



# **Protect applications using NetApp supported plug-ins**

## **SnapCenter software**

NetApp  
January 09, 2026

This PDF was generated from [https://docs.netapp.com/us-en/snapcenter/protect-nsp/netapp\\_supported\\_plugins\\_overview.html](https://docs.netapp.com/us-en/snapcenter/protect-nsp/netapp_supported_plugins_overview.html) on January 09, 2026. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Table of Contents

Protect applications using NetApp supported plug-ins .....	1
NetApp supported plug-ins .....	1
NetApp supported plug-ins overview .....	1
What you can do with the NetApp supported plug-ins .....	1
NetApp supported plug-ins features .....	2
Storage types supported by NetApp supported plug-ins .....	3
Minimum ONTAP privileges required for NetApp supported plug-in .....	3
Prepare storage systems for SnapMirror and SnapVault replication for NetApp supported plug-ins .....	5
Define a backup strategy .....	6
Backup strategy for NetApp supported plug-ins .....	7
Types of restore strategies supported for manually added NetApp supported plug-in resources .....	7
Prepare to install NetApp supported plug-ins .....	8
Installation workflow of SnapCenter NetApp supported plug-ins .....	8
Prerequisites for adding hosts and installing Plug-ins package for Windows, Linux, or AIX .....	8
Host requirements to install SnapCenter Plug-ins Package for Windows .....	13
Host requirements for installing the SnapCenter Plug-ins Package for Linux and AIX .....	13
Set up credentials for NetApp supported plug-ins .....	14
Configure gMSA on Windows Server 2016 or later .....	16
Install the NetApp supported plug-ins .....	17
Configure CA Certificate .....	23
Prepare for data protection .....	31
Prerequisites for using the NetApp supported plug-ins .....	31
How resources, resource groups, and policies are used for protecting NetApp supported plug-in resources .....	31
Back up NetApp supported plug-ins resources .....	32
Back up NetApp supported plug-ins resources .....	32
Add resources to NetApp supported plug-ins .....	33
Create policies for NetApp supported plug-in resources .....	37
Create resource groups and attach policies .....	41
Create resource groups and enable secondary protection for resources on ASA r2 systems .....	44
Create a storage system connection and a credential using PowerShell cmdlets .....	46
Back up individual NetApp supported plug-ins resources .....	47
Back up resource groups of NetApp supported plug-in resources .....	52
Monitor NetApp supported plug-in resources backup operations .....	53
Cancel backup operations for NetApp supported plug-ins .....	54
View NetApp supported plug-ins resource related backups and clones in the Topology page .....	55
Restore NetApp supported plug-ins resources .....	56
Restore NetApp supported plug-in resources .....	56
Restore a resource backup .....	57
Monitor NetApp supported plug-in resources restore operations .....	61
Clone NetApp supported plug-ins resource backups .....	62
Clone NetApp supported plug-ins resource backups .....	62
Clone from a backup .....	63



# Protect applications using NetApp supported plug-ins

## NetApp supported plug-ins

### NetApp supported plug-ins overview

You can use the NetApp supported plug-ins like MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB, and Storage plug-in for applications that you use and then use SnapCenter to backup, restore, or clone these applications. Your NetApp supported plug-ins act as host-side components of the NetApp SnapCenter Software, enabling application-aware data protection and management of resources.

When NetApp supported plug-ins are installed, you can use SnapCenter with NetApp SnapMirror technology to create mirror copies of backup sets on another volume and use NetApp SnapVault technology to perform disk-to-disk backup replication. The NetApp supported plug-ins can be used in both Windows and Linux environments.



SnapCenterCLI does not support NetApp supported plug-ins commands.

NetApp provides the Storage plug-in to perform data protection operations of the data volume on the ONTAP storage using the plug-in framework built into SnapCenter.

You can install the NetApp supported plug-ins from the Add Host page.

#### [Add hosts and install plug-in packages on remote hosts.](#)



SnapCenter support policy will cover support for the plug-in framework, core engine, and the associated APIs. Support will not cover the plug-in source code and the associated scripts built on the plug-in framework.

### What you can do with the NetApp supported plug-ins

You can use the NetApp supported plug-ins like MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB, and Storage plug-in for data protection operations.

- Add resources such as databases, instances, documents, or tablespaces.
- Create backups.
- Restore from backups.
- Clone backups.
- Schedule backup operations.
- Monitor backup, restore, and clone operations.
- View reports for backup, restore, and clone operations.

You can use the NetApp supported plug-ins for data protection operations.

- Take consistency group Snapshots of the storage volumes across ONTAP clusters.
- Backup custom applications using the built in pre and post scripting framework

You can backup ONTAP volume, LUN, or a Qtree.

- Update Snapshots taken on the primary to an ONTAP secondary, leveraging the existing replication relationship (SnapVault/SnapMirror/unified replication) using SnapCenter policy

ONTAP primary and secondary can be ONTAP FAS, AFF, ASA, ONTAP Select, or Cloud Volumes ONTAP.

- Recover complete ONTAP volume, LUN, or files.

You should provide the respective file path manually as the browse or indexing features are not built into the product.

Qtree or directory restore is not supported but you can clone and export only the Qtree if the backup scope is defined at a Qtree level.

## NetApp supported plug-ins features

SnapCenter integrates with the plug-in application and with NetApp technologies on the storage system. To work with NetApp supported plug-ins like MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB, and Storage plug-in you use the SnapCenter graphical user interface.

- **Unified graphical user interface**

The SnapCenter interface provides standardization and consistency across plug-ins and environments. The SnapCenter interface enables you to complete consistent backup, restore, recovery, and clone operations across plug-ins, use centralized reporting, use at-a-glance dashboard views, set up role-based access control (RBAC), and monitor jobs across all plug-ins.

- **Automated central administration**

You can schedule backup operations, configure policy-based backup retention, and perform restore operations. You can also proactively monitor your environment by configuring SnapCenter to send email alerts.

- **Nondisruptive NetApp Snapshot technology**

SnapCenter uses NetApp Snapshot technology with the NetApp supported plug-ins to back up resources. Snapshots consume minimal storage space.

The NetApp supported plug-ins also offers the following benefits:

- Support for backup, restore, and clone workflows
- RBAC-supported security and centralized role delegation

You can also set the credentials so that the authorized SnapCenter users have application-level permissions.

- Creation of space-efficient and point-in-time copies of resources for testing or data extraction by using

## NetApp FlexClone technology

A FlexClone license is required on the storage system where you want to create the clone.

- Support for the consistency group (CG) Snapshot feature of ONTAP as part of creating backups.
- Capability to run multiple backups simultaneously across multiple resource hosts

In a single operation, Snapshots are consolidated when resources in a single host share the same volume.

- Capability to create Snapshot using external commands.
- Capability to create file system consistent Snapshots in Windows environments.

## Storage types supported by NetApp supported 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 NetApp supported plug-ins.

Machine	Storage type
Physical and NFS direct mounts on the VM hosts (VMDKs and RDM LUNs are not supported.)	FC-connected LUNs
Physical and NFS direct mounts on the VM hosts (VMDKs and RDM LUNs are not supported.)	iSCSI-connected LUNs
Physical and NFS direct mounts on the VM hosts (VMDKs and RDM LUNs are not supported.)	NFS-connected volumes
VMware ESXi	vVol datastores on both NFS and SAN  vVol datastore can only be provisioned with ONTAP Tools for VMware vSphere.

## Minimum ONTAP privileges required for NetApp supported plug-in

The minimum ONTAP privileges that are required vary according to the SnapCenter plug-ins you are using for data protection.

- All-access commands: Minimum privileges required for ONTAP 9.12.1 and later
  - event generate-autosupport-log
  - job history show
  - job stop
  - lun attribute show
  - lun create
  - lun delete
  - lun geometry

- lun igrup add
- lun igrup create
- lun igrup delete
- lun igrup rename
- lun igrup 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 resize
- lun serial
- lun show
- network interface
- 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
- snapmirror list-destinations
- version
- 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
- vserver cifs
- vserver cifs share create
- vserver cifs share delete
- vserver cifs shadowcopy show
- vserver cifs share show
- vserver cifs show
- vserver export-policy create
- vserver export-policy delete
- vserver export-policy rule create
- vserver export-policy rule show
- vserver export-policy show
- vserver iscsi connection show
- vserver show

- Read-only commands: Minimum privileges required for ONTAP 8.3.0 and later
  - network interface

## Prepare storage systems for SnapMirror and SnapVault replication for NetApp supported plug-ins

You can use a SnapCenter plug-in with ONTAP SnapMirror technology to create mirror copies of backup sets on another volume, and with ONTAP SnapVault technology to perform disk-to-disk backup replication for standards compliance and other governance-

related purposes. Before you perform these tasks, you must configure a data-protection relationship between the source and destination volumes and initialize the relationship.

SnapCenter performs the updates to SnapMirror and SnapVault after it completes the Snapshot operation. SnapMirror and SnapVault updates are performed as part of the SnapCenter job; do not create a separate ONTAP schedule.



If you are coming to SnapCenter from a NetApp SnapManager product and are satisfied with the data protection relationships you have configured, you can skip this section.

A data protection relationship replicates data on primary storage (the source volume) to secondary storage (the destination volume). When you initialize the relationship, ONTAP transfers the data blocks referenced on the source volume to the destination volume.



SnapCenter does not support cascade relationships between SnapMirror and SnapVault volumes (**Primary > Mirror > Vault**). You should use fanout relationships.

SnapCenter supports the management of version-flexible SnapMirror relationships. For details about version-flexible SnapMirror relationships and how to set them up, see the [ONTAP documentation](#).

## Define a backup strategy

Defining a backup strategy before you create your backup jobs ensures that you have the backups that you require to successfully restore or clone your resources. Your service-level agreement (SLA), recovery time objective (RTO), and recovery point objective (RPO) largely determine your backup strategy.

### About this task

An SLA defines the level of service that is expected and addresses many service-related issues, including the availability and performance of the service. RTO is the time by which a business process must be restored after a disruption in service. RPO defines the strategy for the age of the files that must be recovered from backup storage for regular operations to resume after a failure. SLA, RTO, and RPO contribute to the data protection strategy.

### Steps

1. Determine when you should back up your resources.
2. Decide how many backup jobs you require.
3. Decide how to name your backups.
4. Decide if you want Consistency Group Snapshots and decide on appropriate options for deleting Consistency Group Snapshots.
5. Decide whether you want to use NetApp SnapMirror technology for replication or NetApp SnapVault technology for long term retention.
6. Determine the retention period for the Snapshots on the source storage system and the SnapMirror destination.
7. Determine if you want to run any commands before or after the backup operation and provide a prescript or postscript.

## Backup strategy for NetApp supported plug-ins

### Backup schedules of NetApp supported plug-in resources

The most critical factor in determining a backup schedule is the rate of change for the resource. The more often you back up your resources, the fewer archive logs SnapCenter has to use for restoring, which can result in faster restore operations.

You might back up a heavily used resource every hour, while you might back up a rarely used resource once a day. Other factors include the importance of the resource to your organization, your service-level agreement (SLA) and your recovery point objective (RPO).

SLA defines the level of service expected and addresses many service-related issues, including the availability and performance of service. RPO defines the strategy for the age of the files that must be recovered from backup storage for regular operations to resume after a failure. SLA and RPO contribute to the data protection strategy.

Backup schedules have two parts, as follows:

- Backup frequency

Backup frequency (how often backups are to be performed), also called schedule type for some plug-ins, is part of a policy configuration. For example, you might configure the backup frequency as hourly, daily, weekly or monthly. You can access policies in the SnapCenter GUI by clicking **Settings > Policies**.

- Backup schedules

Backup schedules (exactly when backups are to be performed) are part of a resource or resource group configuration. For example, if you have a resource group that has a policy configured for weekly backups, you might configure the schedule to back up every Thursday at 10:00 p.m. You can access resource group schedules in the SnapCenter GUI by clicking **Resources**, then selecting the appropriate plug-in, and clicking **View > Resource Group**.

### Number of backup jobs needed

Factors that determine the number of backup jobs that you need include the size of the resource, the number of volumes used, the rate of change of the resource, and your Service Level Agreement (SLA).

The number of backup jobs that you choose typically depends on the number of volumes on which you placed your resources. For example, if you placed a group of small resources on one volume and a large resource on another volume, you might create one backup job for the small resources and one backup job for the large resource.

### Types of restore strategies supported for manually added NetApp supported plug-in resources

You must define a strategy before you can successfully perform restore operations using SnapCenter. There are two types of restore strategies for manually added NetApp supported plug-in resources.



You cannot recover manually added NetApp supported plug-in resources.

## Complete resource restore

- Restores all volumes, qtrees, and LUNs of a resource



If the resource contains volumes or qtrees, the Snapshots taken after the Snapshot selected for restore on such volumes or qtrees are deleted and cannot be recovered. Also, if any other resource is hosted on the same volumes or qtrees, then that resource is also deleted.

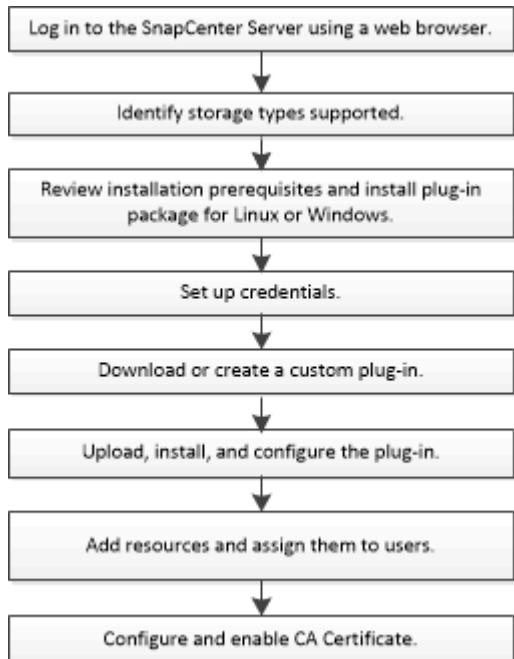
## File level restore

- Restores files from volumes, qtrees, or directories
- Restores only the selected LUNs

# Prepare to install NetApp supported plug-ins

## Installation workflow of SnapCenter NetApp supported plug-ins

You should install and set up SnapCenter NetApp supported plug-ins if you want to protect NetApp supported plug-in resources.



## Prerequisites for adding hosts and installing Plug-ins package for Windows, Linux, or AIX

Before you add a host and install the plug-ins packages, you must complete all the requirements. The NetApp supported plug-ins are supported on Windows, Linux, and AIX environments.



Storage and Oracle applications are supported on AIX.

- You must have installed Java 11 on your Linux, Windows, or AIX host.



IBM Java is not supported on Windows and Linux 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 NetApp supported plug-ins like MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB, and Storage plug-in must be available on the client host from where the add host operation is performed.

## General

If you are using iSCSI, the iSCSI service should 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.
- You must manually choose SnapCenter Plug-in for Microsoft Windows.

[Download JAVA for Windows](#)

### Linux and AIX hosts



Storage and Oracle applications are supported on AIX.

- You must have enabled the password-based SSH connection for the root or non-root user.
- You must have installed Java 11 on your Linux host.

If you are using Windows Server 2019 or Windows Server 2016 for the SnapCenter Server host, you must install Java 11.

[Download JAVA for Linux](#)

[Download JAVA for AIX](#)

- 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.



Ensure that you are using Sudo version 1.8.7 or later.

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```

*LINUX\_USER* is the name of the non-root user that you created.

You can obtain the *checksum\_value* from the **sc\_unix\_plugins\_checksum.txt** file, which is located at:

- *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc\_unix\_plugins\_checksum.txt* if SnapCenter Server is installed on Windows host.
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc\_unix\_plugins\_checksum.txt* if SnapCenter Server is installed on Linux host.



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

## AIX Host requirements

You should ensure that the host meets the requirements before installing the SnapCenter Plug-ins Package for AIX.



Storage and Oracle applications are supported on AIX.



SnapCenter Plug-in for UNIX which is part of the SnapCenter Plug-ins Package for AIX, does not support concurrent volume groups.

Item	Requirements
Operating systems	AIX 7.1 or later
Minimum RAM for the SnapCenter plug-in on host	4 GB

Item	Requirements
Minimum install and log space for the SnapCenter plug-in on host	<p>2 GB</p> <p></p> <p>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	<p>Java 11 IBM Java</p> <p>If you have upgraded JAVA to the latest version, you must ensure that the JAVA_HOME option located at /var/opt/snapcenter/spl/etc/spl.properties is set to the correct JAVA version and the correct path.</p>

#### Configure sudo privileges for non-root users for AIX host

SnapCenter 4.4 and later allows a non-root user to install the SnapCenter Plug-ins Package for AIX and to start the plug-in process. The plug-in processes will be running as an effective non-root user. You should configure sudo privileges for the non-root user to provide access to several paths.

#### What you will need

- Sudo version 1.8.7 or later.
- 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:

- `/home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/custom_location/NetApp/snapcenter/spl/bin/spl`

## Steps

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

```
Cmnd_Alias HPPACMD = sha224:checksum_value== /home/  
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,  
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,  
/opt/NetApp/snapcenter/spl/bin/spl  
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/  
AIX_USER/.sc_netapp/AIX_Prechecks.sh  
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config  
_Check.sh  
Cmnd_Alias SCCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/bin/sc_command_executor  
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,  
CONFIGCHECKCMD, SCCMD  
Defaults: LINUX_USER env_keep += "IATEMPDIR"  
Defaults: LINUX_USER env_keep += "JAVA_HOME"  
Defaults: AIX_USER !visiblepw  
Defaults: AIX_USER !requiretty
```



If you are having a RAC setup, along with the other allowed commands, you should add the following to the `/etc/sudoers` file: '`/<crs_home>/bin/olsnodes`'

You can obtain the value of `crs_home` from the `/etc/oracle/olr.loc` file.

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

You can obtain the `checksum_value` from the **sc\_unix\_plugins\_checksum.txt** file, which is located at:

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` if SnapCenter Server is installed on Windows host.
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` if SnapCenter Server is installed on Linux host.



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

## 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	Microsoft Windows  For the latest information about supported versions, see <a href="#">NetApp Interoperability Matrix Tool</a> .
Minimum RAM for the SnapCenter plug-in on host	1 GB
Minimum install and log space for the SnapCenter plug-in on host	5 GB   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.
Required software packages	<ul style="list-style-type: none"><li>ASP.NET Core Runtime 8.0.12 (and all subsequent 8.0.x patches) Hosting Bundle</li><li>PowerShell Core 7.4.2</li><li>Java 11 Oracle Java and OpenJDK</li></ul> For .NET specific troubleshooting information, see <a href="#">SnapCenter upgrade or install fails for legacy systems that do not have internet connectivity</a> .

## Host requirements for installing the SnapCenter Plug-ins Package for Linux and AIX

You should ensure that the host meets the requirements before installing the SnapCenter Plug-ins Package for Linux or AIX.



Storage and Oracle applications are supported on AIX.

Item	Requirements
Operating systems	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• Oracle Linux</li> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul>
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></p> <p>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	<p>Java 11 Oracle Java or OpenJDK</p> <p>If you have upgraded JAVA to the latest version, you must ensure that the JAVA_HOME option located at /var/opt/snapcenter/spl/etc/spl.properties is set to the correct JAVA version and the correct path.</p>

For the latest information about supported versions, see the [NetApp Interoperability Matrix Tool](#)

## Set up credentials for NetApp supported 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.

### Before you begin

- Linux or AIX hosts

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

- NetApp supported 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**.

## About this task

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**.
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"><li>• Domain administrator or any member of the administrator group</li></ul> <p>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:</p> <ul style="list-style-type: none"><li>◦ <i>NetBIOS\UserName</i></li><li>◦ <i>Domain FQDN\UserName</i></li></ul> <ul style="list-style-type: none"><li>• Local administrator (for workgroups only)</li></ul> <p>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: <i>UserName</i></p>

For this field...	Do this...
Password	Enter the password used for authentication.
Authentication Type	Select the authentication type that you want to use.
Use sudo privileges	<p>Select the <b>Use sudo privileges</b> check box if you are creating credentials for a non-root user.</p> <div style="display: flex; align-items: center; justify-content: space-between;"> <span></span> <span>Applicable to Linux and AIX users only.</span> </div>

5. Click **OK**.

After you finish setting up the credentials, you might want to assign credential maintenance to a user or group of users on the User and Access page.

## Configure gMSA on Windows Server 2016 or later

Windows Server 2016 or later enables you to create a group Managed Service Account (gMSA) that provides automated service account password management from a managed domain account.

### Before you begin

- You should have a Windows Server 2016 or later domain controller.
- You should have a Windows Server 2016 or later host, which is a member of the domain.

### Steps

1. Create a KDS root key to generate unique passwords for each object in your gMSA.
2. For each domain, run the following command from the Windows domain controller: `Add-KDSRootKey -Effectivelmmediately`
3. Create and configure your gMSA:
  - a. Create a user group account in the following format:

domainName\accountName\$

- b. Add computer objects to the group.
- c. Use the user group you just created to create the gMSA.

For example,

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
```

- d. Run `Get-ADServiceAccount` command to verify the service account.

4. Configure the gMSA on your hosts:

- a. Enable the Active Directory module for Windows PowerShell on the host where you want to use the gMSA account.

To do this, run the following command from PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name           Name           Install
State
-----
-----
[ ] Active Directory Domain Services  AD-Domain-Services  Available

PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success  Restart Needed  Exit Code      Feature Result
-----  -----  -----  -----
True      No            Success        {Active Directory Domain
Services, Active ...}

WARNING: Windows automatic updating is not enabled. To ensure that
your newly-installed role or feature is
automatically updated, turn on Windows Update.
```

- b. Restart your host.
- c. Install the gMSA on your host by running the following command from the PowerShell command prompt: `Install-AdServiceAccount <gMSA>`
- d. Verify your gMSA account by running the following command: `Test-AdServiceAccount <gMSA>`

5. Assign the administrative privileges to the configured gMSA on the host.

6. Add the Windows host by specifying the configured gMSA account in the SnapCenter Server.

SnapCenter Server will install the selected plug-ins on the host and the specified gMSA will be used as the service log on account during the plug-in installation.

## Install the NetApp supported plug-ins

### Add hosts and install 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 should 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.
- If you are using group Managed Service Account (gMSA), you should configure gMSA with administrative privileges.

[Configure group Managed Service Account on Windows Server 2016 or later for custom applications](#)

- For Windows host, you must ensure that you select SnapCenter Plug-in for Windows.

#### About this task

- You cannot add a SnapCenter Server as a plug-in host to another SnapCenter Server.
- If you install plug-ins on a cluster (WSFC), the plug-ins are installed on all of the nodes of the cluster.

#### Steps

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

For this field...	Do this...
Host Type	<p>Select the host type:</p> <ul style="list-style-type: none"> <li>• Windows</li> <li>• Linux</li> <li>• AIX</li> </ul> <p> The NetApp supported plug-ins can be used in Windows, Linux, and AIX environments.</p> <p> Storage and Oracle applications are supported on AIX.</p>

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> 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.

You can install the following plug-ins from the list:

- MongoDB
- ORASCPM (displayed as Oracle Applications)
- SAP ASE
- SAP MaxDB
- Storage

6. (Optional) Select **More Options** to install the other plug-ins.

For this field...	Do this...
Port	<p>Either retain the default port number, or specify the port number.</p> <p>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> 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 NetApp supported plug-ins can be installed on either a Windows system or Linux system.</p> <ul style="list-style-type: none"> <li>For the SnapCenter Plug-ins Package for Windows, the default path is C:\Program Files\NetApp\SnapCenter.</li> </ul> <p>Optionally, you can customize the path.</p> <ul style="list-style-type: none"> <li>For SnapCenter Plug-ins Package for Linux and SnapCenter Plug-ins Package for AIX, the default path is /opt/NetApp/snapcenter.</li> </ul> <p>Optionally, you can customize the path.</p>
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>
Use group Managed Service Account (gMSA) to run the plug-in services	<p>For Windows host, select this check box if you want to use group Managed Service Account (gMSA) to run the plug-in services.</p> <p> Provide the gMSA name in the following format: domainName\accountName\$.</p> <p> gMSA will be used as a log on service account only for SnapCenter Plug-in for Windows service.</p>

## 7. Select **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.



In an HA setup, if you are updating SnapManager.Web.UI.dll.config, you must update the file on both nodes and restart the SnapCenter App Pool.

Windows default path is C:\Program Files\NetApp\SnapCenter\WebApp\SnapManager.Web.UI.dll.config

Linux default path is

/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config

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



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.

## Install SnapCenter Plug-in Packages for Linux, Windows, or AIX on multiple remote hosts by using cmdlets

You can install the SnapCenter Plug-in Packages for Linux, Windows, or AIX 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.



Storage and Oracle applications are supported on AIX.

### 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 [SnapCenter Software 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.

## Install the NetApp supported plug-ins on Linux hosts by using the command-line interface

You should install the NetApp supported plug-ins 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 NetApp supported plug-ins 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 NetApp supported plug-ins.

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.

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

The information regarding the parameters that can be used with the command and their descriptions can be obtained by running `Get-Help command_name`. Alternatively, you can also refer to the [SnapCenter Software Cmdlet Reference Guide](#).

5. Log in to SnapCenter and upload the NetApp supported plug-in from the UI or by using PowerShell cmdlets.

You can upload the NetApp supported plug-in from the UI by referring to [Add hosts and install plug-in packages on remote hosts](#) section.

The SnapCenter cmdlet help and the cmdlet reference information contain more information about PowerShell cmdlets.

[SnapCenter Software Cmdlet Reference Guide](#).

## Monitor the status of installing NetApp supported plug-ins

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. In 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**.

## Configure CA Certificate

### Generate CA Certificate CSR file

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

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



CA Certificate RSA key length must be minimum 3072 bits.

For information to generate a CSR, see [How to generate CA Certificate CSR file](#).



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

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

### Import CA certificates

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

#### Steps

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

In this wizard window...	Do the following...
Import Private Key	Select the option <b>Yes</b> , import the private key, and then click <b>Next</b> .
Import File Format	Make no changes; click <b>Next</b> .
Security	Specify the new password to be used for the exported certificate, and then click <b>Next</b> .
Completing the Certificate Import Wizard	Review the summary, and then click <b>Finish</b> to start the import.



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

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

### Get the CA certificate thumbprint

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

#### Steps

1. Perform the following on the GUI:

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

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

2. Perform the following from PowerShell:

- a. Run the following command to list the thumbprint of the installed certificate and identify the recently installed certificate by the subject name.

```
Get-ChildItem -Path Cert:\LocalMachine\My
```

- b. Copy the thumbprint.

### Configure CA certificate with Windows host plug-in services

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

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

#### Steps

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

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

For example:

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

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

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

For example:

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

## Configure the CA Certificate for the NetApp supported plug-ins service on Linux host

You should manage the password of the plug-ins keystore and its certificate, configure the CA certificate, configure root or intermediate certificates to the plug-ins trust-store, and configure CA signed key pair to plug-ins trust-store with SnapCenter plug-ins service to activate the installed digital certificate.

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

### Manage password for plug-in keystore and alias of the CA signed key pair in use

#### Steps

1. You can retrieve plug-in keystore default password from plug-in agent property file.

It is the value corresponding to the key 'KEYSTORE\_PASS'.

2. Change the keystore password:

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

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

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

Update the same for the key KEYSTORE\_PASS in `agent.properties` file.

4. Restart the service after changing the password.



>Password for plug-in keystore and for all the associated alias password of the private key should be same.

## Configure root or intermediate certificates to plug-in trust-store

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

#### Steps

1. Navigate to the folder containing the plug-in keystore: `/opt/NetApp/snapcenter/scc/etc`.
2. Locate the file 'keystore.jks'.

3. List the added certificates in the keystore:

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

4. Add a root or intermediate certificate:

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

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



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

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

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

#### Steps

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

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

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

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

5. List the added certificates in the keystore.

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

6. Verify that the keystore contains the alias corresponding to the new CA certificate, which was added to the keystore.

7. Change the added private key password for CA certificate to the keystore password.

Default plug-in keystore password is the value of the key KEYSTORE\_PASS in agent.properties file.

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

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

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

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

Update this value against the key SCC\_CERTIFICATE\_ALIAS.

10. Restart the service after configuring the CA signed key pair to plug-in trust-store.

#### Configure certificate revocation list (CRL) for plug-ins

##### About this task

- SnapCenter Plug-ins will search for the CRL files in a pre-configured directory.
- Default directory for the CRL files for SnapCenter Plug-ins is ' opt/NetApp/snapcenter/scc/etc/crl'.

##### Steps

1. You can modify and update the default directory in agent.properties file against the key CRL\_PATH.

You can place more than one CRL file in this directory. The incoming certificates will be verified against each CRL.

#### Configure the CA Certificate for the NetApp supported plug-ins service on Windows host

You should manage the password of the plug-ins keystore and its certificate, configure the CA certificate, configure root or intermediate certificates to the plug-ins trust-store, and configure CA signed key pair to plug-ins trust-store with SnapCenter plug-ins service to activate the installed digital certificate.

The plug-ins uses the file *keystore.jks*, which is located at *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc* both as its trust-store and key-store.

##### Manage password for plug-in keystore and alias of the CA signed key pair in use

##### Steps

1. You can retrieve plug-in keystore default password from plug-in agent property file.

It is the value corresponding to the key KEYSTORE\_PASS.

2. Change the keystore password:

*keytool -storepasswd -keystore keystore.jks*



If the "keytool" command is not recognized on the Windows command prompt, replace the keytool command with its complete path.

*C:\Program Files\Java\<jdk\_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks*

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

*keytool -keypasswd -alias "alias\_name\_in\_cert" -keystore keystore.jks*

Update the same for the key KEYSTORE\_PASS in *agent.properties* file.

4. Restart the service after changing the password.



Password for plug-in keystore and for all the associated alias password of the private key should be same.

#### Configure root or intermediate certificates to plug-in trust-store

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

##### Steps

1. Navigate to the folder containing the plug-in keystore *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Locate the file 'keystore.jks'.
3. List the added certificates in the keystore:

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

4. Add a root or intermediate certificate:

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

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



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

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

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

##### Steps

1. Navigate to the folder containing the plug-in keystore *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Locate the file *keystore.jks*.
3. List the added certificates in the keystore:

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

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

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

5. List the added certificates in the keystore.

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

6. Verify that the keystore contains the alias corresponding to the new CA certificate, which was added to the keystore.

7. Change the added private key password for CA certificate to the keystore password.

Default plug-in keystore password is the value of the key KEYSTORE\_PASS in agent.properties file.

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

8. Configure the alias name from CA certificate in *agent.properties* file.

Update this value against the key `SCC_CERTIFICATE_ALIAS`.

9. Restart the service after configuring the CA signed key pair to plug-in trust-store.

#### Configure certificate revocation list (CRL) for SnapCenter plug-ins

##### About this task

- To download the latest CRL file for the related CA certificate see [How to update certificate revocation list file in SnapCenter CA Certificate](#).
- SnapCenter plug-ins will search for the CRL files in a pre-configured directory.
- Default directory for the CRL files for SnapCenter plug-ins is '`C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\crl`'.

##### Steps

1. You can modify and update the default directory in *agent.properties* file against the key `CRL_PATH`.
2. You can place more than one CRL file in this directory.

The incoming certificates will be verified against each CRL.

#### Enable CA Certificates for plug-ins

You should configure the CA certificates and deploy the CA certificates in the SnapCenter Server and the corresponding plug-in hosts. You should enable the CA certificate validation for the plug-ins.

##### Before you begin

- You can enable or disable the CA certificates using the run `Set-SmCertificateSettings` cmdlet.
- You can display the certificate status for the plug-ins using the `Get-SmCertificateSettings`.

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

##### Steps

1. In the left navigation pane, click **Hosts**.
2. In the Hosts page, click **Managed Hosts**.
3. Select single or multiple plug-in hosts.
4. Click **More options**.
5. Select **Enable Certificate Validation**.

##### After you finish

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

-  indicates that the CA certificate is neither enabled nor assigned to the plug-in host.
-  indicates that the CA certificate is successfully validated.

-  indicates that the CA certificate could not be validated.
-  indicates that the connection information could not be retrieved.



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

## Prepare for data protection

### Prerequisites for using the NetApp supported plug-ins

Before you use SnapCenter NetApp supported plug-ins, the SnapCenter administrator must install and configure the SnapCenter Server and perform the prerequisite tasks.

- Install and configure SnapCenter Server.
- Log in to SnapCenter Server.
- Configure the SnapCenter environment by adding storage system connections and creating credentials, if applicable.
- Add hosts, and install and upload the plug-ins.
- If applicable, install Java 11 on the plug-in host.
- If you have multiple data paths (LIFs) or a dNFS configuration, you can perform the following using the SnapCenter CLI on the database host:
  - By default, all the IP addresses of the database host are added to the NFS storage export policy in storage virtual machine (SVM) for the cloned volumes. If you want to have a specific IP address or restrict to a subset of the IP addresses, run the `Set-PreferredHostIPsInStorageExportPolicy` CLI.
  - If you have multiple data paths (LIFs) in SVMs, SnapCenter chooses the appropriate data path (LIF) for mounting the NFS cloned volume. However, if you want to specify a specific data path (LIF), you must run the `Set-SvmPreferredDataPath` CLI. The information regarding the parameters that can be used with the command and their descriptions can be obtained by running `Get-Help command_name`. Alternatively, you can also refer to the [SnapCenter Software Command Reference Guide](#).
- Set up SnapMirror and SnapVault, if you want backup replication.
- Ensure that port 9090 is not used by any other application on the host.

Port 9090 must be reserved for use by NetApp supported plug-ins in addition to the other ports required by SnapCenter.

### How resources, resource groups, and policies are used for protecting NetApp supported plug-in resources

Before you use SnapCenter, it is helpful to understand basic concepts related to the backup, clone, and restore operations you want to perform. You interact with resources, resource groups, and policies for different operations.

- Resources are typically databases, Windows file systems, or VMs that you back up or clone with SnapCenter.
- A SnapCenter resource group, is a collection of resources on a host or cluster.

When you perform an operation on a resource group, you perform that operation on the resources defined

in the resource group according to the schedule you specify for the resource group.

You can back up on demand a single resource or a resource group. You also can perform scheduled backups for single resources and resource groups.

- The policies specify the backup frequency, copy retention, replication, scripts, and other characteristics of data protection operations.

When you create a resource group, you select one or more policies for that group. You can also select a policy when you perform a backup on demand for a single resource.

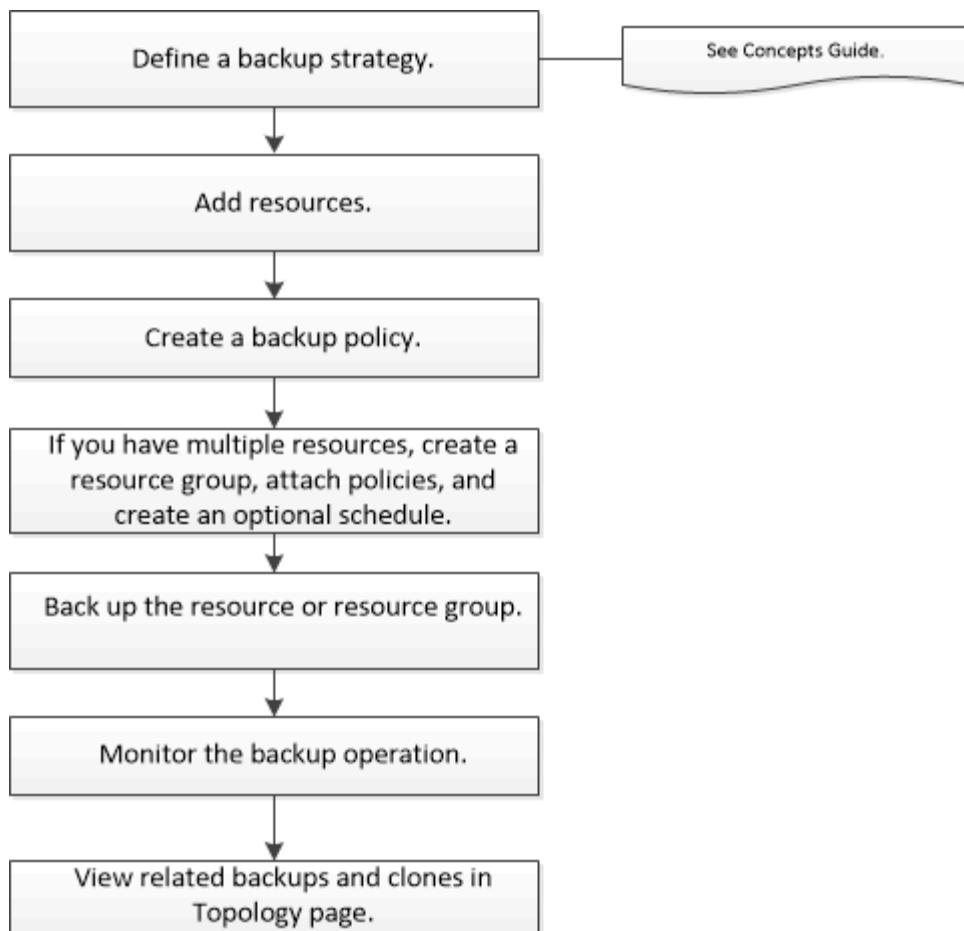
Think of a resource group as defining *what* you want to protect and when you want to protect it in terms of day and time. Think of a policy as defining *how* you want to protect it. If you are backing up all databases or backing up all file systems of a host, for example, you might create a resource group that includes all the databases or all the file systems in the host. You could then attach two policies to the resource group: a daily policy and an hourly policy. When you create the resource group and attach the policies, you might configure the resource group to perform a File-Based backup daily and another schedule that performs Snapshot based backup hourly.

## **Back up NetApp supported plug-ins resources**

### **Back up NetApp supported plug-ins resources**

The backup workflow includes planning, identifying the resources for backup, managing backup policies, creating resource groups and attaching policies, creating backups, and monitoring the operations.

The following workflow shows the sequence in which you must perform the backup operation:



You can also use PowerShell cmdlets manually or in scripts to perform backup, restore, and clone operations. For detailed information about PowerShell cmdlets, use the SnapCenter cmdlet help or see the [SnapCenter Software Cmdlet Reference Guide](#)

## Add resources to NetApp supported 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 uploaded the plug-ins to SnapCenter Server.

### Steps

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

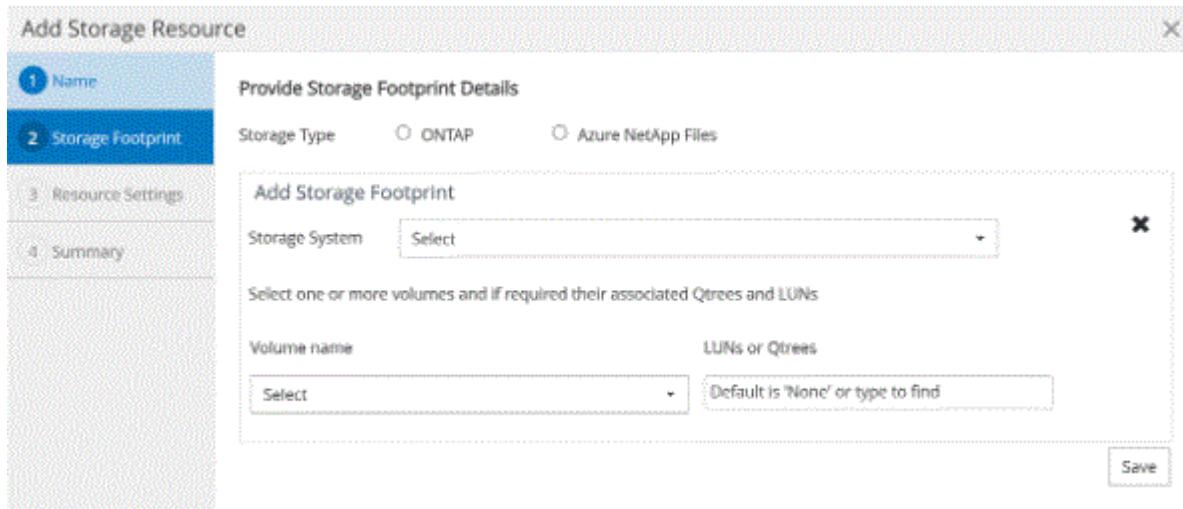
For this field...	Do this...
Host name	Select the host.
Type	Select the type. Type is user defined as per the plug-in description file. For example, database and instance.  In case the type selected has a parent, enter the details of the parent. For example, if the type is Database and the parent is Instance, enter the details of the Instance.
Credential name	Select Credential or create a new credential.
Mount Paths	Enter the mount paths where the resource is mounted. This is applicable only for a Windows host.

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

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



NetApp supported plug-ins does not support automatic discovery of the resources. The storage details of physical and virtual environments are also not discovered automatically. 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.



Ensure that the custom keys name is in uppercase.

## Resource settings i

Custom key-value pairs for MySQL plug-in

Name	Value	
HOST	localhost	<span style="border: 1px solid #ccc; padding: 2px;">X</span>
PORT	3306	<span style="border: 1px solid #ccc; padding: 2px;">X</span>
MASTER_SLAVE	NO	<span style="border: 1px solid #ccc; padding: 2px;">+</span> <span style="border: 1px solid #ccc; padding: 2px;">X</span>

For the respective plug-in parameters, refer [Parameters to configure the resource](#)

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

## Result

The resources are displayed along with information such as type, host or cluster name, associated resource groups and policies, and overall status.



You must refresh the resources if the databases are renamed outside of SnapCenter.

## 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 NetApp supported plug-ins resource has backups associated with it, the following fields cannot be modified: resource name, resource type, and host name.

## Parameters to configure the resource

If you are adding the plug-ins manually, you can use the following parameters to configure the resource in the Resource Settings page.

### Plug-in for MongoDB

Resource Settings:

- MONGODB\_APP\_SERVER=(for resource type as sharded cluster) or MONGODB\_REPLICASET\_SERVER=(for resource type as replicaset)
- OPLOG\_PATH=(Optional parameter in case it is provided from MongoDB.propertiesfile)
- MONGODB\_AUTHENTICATION\_TYPE= (PLAIN for LDAP Authentication and None for others)

You must provide the following parameters needs to be provided in MongoDB.properties file:

- DISABLE\_STARTING\_STOPPING\_SERVICES=
  - N if the start/stop services are performed by the plug-in.
  - Y if start/\*\*stop services are performed by the user.
  - Optional parameter as default value is set to N.

- OPLOG\_PATH\_= (Optional parameter in case it is already provided as custom key-value pair in SnapCenter).

#### Plug-in for MaxDB

Resource Settings:

- XUSER\_ENABLE (Y|N) enables or disables the use of an xuser for MaxDB so that a password is not required for the database user.
- HANDLE\_LOGWRITER (Y|N) executes suspend logwriter (N) or resume logwriter (Y) operations.
- DBMCLICMD (path\_to\_dbmcli\_cmd) specifies the path to the MaxDB dbmcli command. If not set, dbmcli on the search path is used.



For Windows environment, the path must be within double-quotes ("...").

- SQLCLICMD (path\_to\_sqlcli\_cmd) specifies the path to the MaxDB sqlcli command. If the path is not set, sqlcli is used on the search path.
- MAXDB\_UPDATE\_HIST\_LOG (Y|N) instructs the MaxDB backup program whether it should update the MaxDB history log.
- MAXDB\_CHECK\_SNAPSHOT\_DIR : Example, SID1:directory[,directory...]; [SID2:directory[,directory...]] checks that a Snap Creator Snapshot copy operation is successful and ensures that the snapshot is created.

This applies to NFS only. The directory must point to the location that contains the .snapshot directory. Multiple directories can be included in a comma-separated list.

In MaxDB 7.8 and later versions, the database backup request is marked Failed in the backup history.

- MAXDB\_BACKUP\_TEMPLATES: Specifies a backup template for each database.

The template must exist and be an external type of backup template. To enable snapshot integration for MaxDB 7.8 and later, you must have MaxDB background server functionality and already configured MaxDB backup template of the EXTERNAL type.

- MAXDB\_BG\_SERVER\_PREFIX: Specifies the prefix for the background server name.

If the MAXDB\_BACKUP\_TEMPLATES parameter is set, you must also set the MAXDB\_BG\_SERVER\_PREFIX parameter. If you do not set the prefix, the default value na\_bg\_ is used.

#### Plug-in for SAP ASE

Resource Settings:

- SYBASE\_SERVER (data\_server\_name) specifies the Sybase data server name (-S option on isql command). For example, p\_test.
- SYBASE\_DATABASES\_EXCLUDE (db\_name) allows databases to be excluded if the "ALL" construct is used.

You can specify multiple databases by using a semicolon-separated list. For example: pubs2;test\_db1.

- SYBASE\_USER: user\_name specifies the operating system user who can run the isql command.

Required for UNIX. This parameter is required if the user running the Snap Creator Agent start and stop commands (usually the root user) and the user running the isql command are different.

- SYBASE\_TRAN\_DUMP db\_name:directory\_path enables you to perform a Sybase transaction dump after creating a snapshot. For example, pubs2:/sybasedumps/ pubs2

You must specify each database requiring a transaction dump.

- SYBASE\_TRAN\_DUMP\_COMPRESS (Y|N ) enables or disables native Sybase transaction dump compression.
- SYBASE\_ISQL\_CMD (For example, /opt/sybase/OCS-15\_0/bin/isql) defines the path to the isql command.
- SYBASE\_EXCLUDE\_TEMPDB (Y|N) allows you to auto exclude user created temporary databases.

#### Plug-in for Oracle applications (ORASCPM)

Resource Settings:

- SQLPLUS\_CMD specifies the path to SQLplus.
- ORACLE\_DATABASES lists the Oracle databases to be backed up and corresponding user (database:user).
- CNTL\_FILE\_BACKUP\_DIR specifies the directory for control file back up.
- ORA\_TEMP specifies the directory for temporary files.
- ORACLE\_HOME specifies the directory where the Oracle software is installed.
- ARCHIVE\_LOG\_ONLY specifies whether to back up the archive logs or not.
- ORACLE\_BACKUPMODE specifies whether to perform online or offline backup.
- ORACLE\_EXPORT\_PARAMETERS specifies whether the environment variables defined above should be re-exported while running `/bin/su <user running sqlplus> -c sqlplus /nolog <cmd>`. This is typically the case, when the user who is running sqlplus has not set all environment variables necessary to connect to the database using `connect / as sysdba`.

## Create policies for NetApp supported plug-in resources

Before you use SnapCenter to back up NetApp supported plug-in specific resources, you must create a backup policy for the resource or resource group that you want to back up.

#### Before you begin

- You should have defined your backup strategy.

For details, see the information about defining a data protection strategy for NetApp supported plug-ins.

- You should have prepared for data protection.

Preparing for data protection includes tasks such as installing SnapCenter, adding hosts, creating storage system connections, and adding resources.

- The storage virtual machines (SVMs) should be assigned to you for mirror or vault operations.

The SnapCenter administrator must have assigned the SVMs for both the source and destination volumes to you if you are replicating Snapshots to a mirror or vault.

- You should have manually added the resources that you want to protect.

## About this task

- A backup policy is a set of rules that governs how you manage, schedule, and retain backups. Additionally, you can specify replication, script, and application settings.
- Specifying options in a policy saves time when you want to reuse the policy for another resource group.
- SnapLock
  - If 'Retain the backup copies for a specific number of days' option is selected, then the SnapLock retention period must be lesser than or equal to the mentioned retention days.
  - Specifying a Snapshot locking period prevents deletion of the Snapshots until the retention period expires. This could lead to retaining a larger number of Snapshots than the count specified in the policy.
  - For ONTAP 9.12.1 and below version, the clones created from the SnapLock Vault Snapshots as part of restore will inherit the SnapLock Vault expiry time. Storage admin should manually cleanup the clones post the SnapLock expiry time.



Primary SnapLock settings are managed in SnapCenter backup policy and the secondary SnapLock settings are managed by ONTAP.

## Steps

1. In the left navigation pane, click **Settings**.
2. In the Settings page, click **Policies**.
3. Click **New**.
4. In the Name page, enter the policy name and details.
5. In the Policy type page, perform the following:
  - a. Select storage type.
  - b. In the Custom backup settings section, provide any specific backup settings that have to be passed to the plug-in in key-value format.

You can provide multiple key-values to be passed to the plug-in.
6. In the Snapshot and Replication page, perform the following steps:
  - a. Specify the schedule type by selecting **On demand**, **Hourly**, **Daily**, **Weekly**, or **Monthly**.



You can specify the schedule (start date, end date, and frequency) for the backup operation while creating a resource group. This enables you to create resource groups that share the same policy and backup frequency, but enables you to assign different backup schedules to each policy.



If you have scheduled for 2:00 a.m., the schedule will not be triggered during daylight saving time (DST).

- b. In the Snapshot settings section, specify the retention settings for the backup type and the schedule type selected in the **Backup Type** page:

If you want to...	Then...
Keep a certain number of Snapshots	<p>Select <b>Copies to keep</b>, and then specify the number of Snapshots that you want to keep.</p> <p>If the number of Snapshots exceeds the specified number, the Snapshots are deleted with the oldest copies deleted first.</p> <p> You must set the retention count to 2 or higher if you plan to enable SnapVault replication. If you set the retention count to 1, the retention operation might fail because the first Snapshot is the reference Snapshot for the SnapVault relationship until a newer Snapshot is replicated to the target.</p> <p> The maximum retention value is 1018. Backups will fail if retention is set to a value higher than what the underlying ONTAP version supports.</p>
Keep the Snapshots for a certain number of days	Select <b>Retain copies for</b> , and then specify the number of days for which you want to keep the Snapshots before deleting them.
Snapshot copy locking period	<p>Select <b>Snapshot copy locking period</b>, and specify days, months, or years.</p> <p>SnapLock retention period should be less than 100 years.</p>

c. Select a Policy label.



You can assign SnapMirror labels to primary snapshots for remote replication, allowing the primary snapshots to offload the snapshot replication operation from SnapCenter to ONTAP secondary systems. This can be done without enabling SnapMirror or SnapVault option in the policy page.

7. In the Select secondary replication options section, select one or both of the following secondary replication options:

For this field...	Do this...
<b>Update SnapMirror after creating a local Snapshot copy</b>	<p>Select this field to create mirror copies of the backup sets on another volume (SnapMirror replication).</p> <p>If the protection relationship in ONTAP is of type Mirror and Vault and if you select only this option, Snapshot created on the primary will not be transferred to the destination, but will be listed in the destination. If this Snapshot is selected from the destination to perform a restore operation, then the following error message is displayed: Secondary Location is not available for the selected vaulted/mirrored backup.</p> <p>During secondary replication, the SnapLock expiry time loads the primary SnapLock expiry time.</p> <p>Clicking the <b>Refresh</b> button in the Topology page refreshes the secondary and primary SnapLock expiry time that are retrieved from ONTAP.</p> <p>See <a href="#">View NetApp supported plug-ins resource related backups and clones in the Topology page</a>.</p>
<b>Update SnapVault after creating a local Snapshot copy</b>	<p>Select this option to perform disk-to-disk backup replication (SnapVault backups).</p> <p>During secondary replication, the SnapLock expiry time loads the primary SnapLock expiry time.</p> <p>Clicking the <b>Refresh</b> button in the Topology page refreshes the secondary and primary SnapLock expiry time that are retrieved from ONTAP.</p> <p>When SnapLock is configured only on the secondary from ONTAP known as SnapLock Vault, clicking the <b>Refresh</b> button in the Topology page refreshes the locking period on the secondary that is retrieved from ONTAP.</p> <p>For more information on SnapLock Vault see <a href="#">Commit Snapshots to WORM on a vault destination</a>.</p> <p>See <a href="#">View NetApp supported plug-ins resource related backups and clones in the Topology page</a>.</p>
<b>Error retry count</b>	Enter the maximum number of replication attempts that can be allowed before the operation stops.



You should configure SnapMirror retention policy in ONTAP for the secondary storage to avoid reaching the maximum limit of Snapshots on the secondary storage.

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

## Create resource groups and attach policies

A resource group is the container to which you must add resources that you want to back up and protect. It enables you to back up all the data that is associated with a given application simultaneously. You must also attach one or more policies to the resource group to define the type of data protection job that you want to perform.

### Steps

1. In the left navigation pane, select **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, select New Resource Group.
3. In the Name page, perform the following actions:

For this field...	Do this...
Name	<p>Enter a name for the resource group.</p> <p>Note: The resource group name should not exceed 250 characters.</p>
Tags	<p>Enter one or more labels that will help you later search for the resource group.</p> <p>For example, if you add HR as a tag to multiple resource groups, you can later find all the resource groups associated with the HR tag.</p>
Use custom name format for Snapshot copy	<p>Select this check box, and enter a custom name format that you want to use for the Snapshot name.</p> <p>For example, <i>customtext_resource group_policy_hostname</i> or <i>resource group_hostname</i>. By default, a timestamp is appended to the Snapshot name.</p>

4. Optional: In the Resources page, select a host name from the **Host** drop-down list and the resource type from the **Resource Type** drop-down list.

This helps to filter information on the screen.

5. Select the resources from the **Available Resources** section, and then select the right arrow to move them to the **Selected Resources** section.
6. Optional: In the **Application Settings** page, do the following:
  - a. Select the Backups arrow to set additional backup options:

Enable consistency group backup and perform the following tasks:

For this field...	Do this...
Afford time to wait for Consistency Group Snapshot operation to complete	Select Urgent, Medium, or Relaxed to specify the wait time for Snapshot operation to complete.  Urgent = 5 seconds, Medium = 7 seconds, and Relaxed = 20 seconds.
Disable WAFL Sync	Select this to avoid forcing a WAFL consistency point.

- b. Select the Scripts arrow and enter the pre and post commands for quiesce, Snapshot, and unquiesce operations. You can also enter the pre commands to be executed before exiting in the event of a failure.
- c. Select the Custom Configurations arrow and enter the custom key-value pairs required for all data protection operations using this resource.

Parameter	Setting	Description
ARCHIVE_LOG_ENABLE	(Y/N)	Enables the archive log management to delete the archive logs.
ARCHIVE_LOG_RETENTION	number_of_days	Specifies the number of days the archive logs are retained.  This setting must be equal to or greater than NTAP_SNAPSHOT_RETENTIONS.
ARCHIVE_LOG_DIR	change_info_directory/logs	Specifies the path to the directory that contains the archive logs.
ARCHIVE_LOG_EXT	file_extension	Specifies the archive log file extension length.  For example, if the archive log is log_backup_0_0_0_0.161518551942 9 and if the file_extension value is 5, then the extension of the log will retain 5 digits, which is 16151.

Parameter	Setting	Description
ARCHIVE_LOG_RECURSIVE_SE ARCH	(Y/N)	<p>Enables the management of archive logs within subdirectories.</p> <p>You should use this parameter if the archive logs are located under subdirectories.</p>

d. Select the **Snapshot Copy Tool** arrow to select the tool to create Snapshots:

If you want...	Then...
SnapCenter to use the plug-in for Windows and put the file system into a consistent state before creating a Snapshot. For Linux resources, this option is not applicable.	<p>Select <b>SnapCenter with File System Consistency</b>.</p> <p>This option is not applicable for SnapCenter Plug-in for SAP HANA Database.</p>
SnapCenter to create a storage level Snapshot	Select <b>SnapCenter without File System Consistency</b> .
To enter the command to be executed on the host to create Snapshots.	Select <b>Other</b> , and then enter the command to be executed on the host to create a Snapshot.

7. In the Policies page, perform the following steps:

a. Select one or more policies from the drop-down list.



You can also create a policy by selecting .

The policies are listed in the **Configure schedules for selected policies** section.

b.

In the **Configure Schedules** column, select  for the policy you want to configure.

c. In the Add schedules for policy *policy\_name* dialog box, configure the schedule and select OK.

Where *policy\_name* is the name of the policy that you have selected.

The configured schedules are listed in the Applied Schedules column. Third party backup schedules are not supported when they overlap with SnapCenter backup schedules.

8. From the **Email preference** drop-down list on the **Notification** page, select the scenarios in which you want to send the emails.

You must also specify the sender and receiver email addresses, and the subject of the email. The SMTP server must be configured in **Settings > Global Settings**.

9. Review the summary, and then select **Finish**.

## Create resource groups and enable secondary protection for resources on ASA r2 systems

You should create the resource group to add the resources that are on ASA r2 systems. You can also provision the secondary protection while creating the resource group.

### Before you begin

- You should ensure that you are not adding both ONTAP 9.x resources and ASA r2 resources to the same resource group.
- You should ensure that you do not have a database with both ONTAP 9.x resources and ASA r2 resources.

### About this task

- The secondary protection is available only if the logged-in user is assigned to the role that has the **SecondaryProtection** capability enabled.
- If you enabled secondary protection, the resource group is put into maintenance mode while creating the primary and secondary consistency groups. After the primary and secondary consistency groups are created, the resource group is put out of maintenance mode.
- SnapCenter does not support secondary protection for a clone resource.

### Steps

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

2. In the Resources page, click **New Resource Group**.

3. In the Name page, perform the following actions:

a. Enter a name for the resource group in the Name field.



The resource group name should not exceed 250 characters.

b. Enter one or more labels in the Tag field to help you search for the resource group later.

For example, if you add HR as a tag to multiple resource groups, you can later find all resource groups associated with the HR tag.

c. Select this check box, and enter a custom name format that you want to use for the Snapshot name.

For example, customtext\_resource group\_policy\_hostname or resource group\_hostname. By default, a timestamp is appended to the Snapshot name.

d. Specify the destinations of the archive log files that you do not want to back up.



You should use the exact same destination as it was set in the application including prefix, if needed.

4. In the Resources page, select the database host name from the **Host** drop-down list.



The resources are listed in the Available Resources section only if the resource is discovered successfully. If you have recently added resources, they will appear on the list of available resources only after you refresh your resource list.

5. Select the ASA r2 resources from the Available Resources section and move them to the Selected

Resources section.

6. In the Application Settings page, select the backup option.

7. In the Policies page, perform the following steps:

- Select one or more policies from the drop-down list.



You can also create a policy by clicking .

In the Configure schedules for selected policies section, the selected policies are listed.

b.

Click  in the Configure Schedules column for the policy for which you want to configure a schedule.

c. In the Add schedules for policy *policy\_name* window, configure the schedule, and then click **OK**.

Where, *policy\_name* is the name of the policy that you have selected.

The configured schedules are listed in the Applied Schedules column.

Third party backup schedules are not supported when they overlap with SnapCenter backup schedules.

8. If the secondary protection is enabled for the policy that you have selected, then Secondary Protection page is displayed and you need to perform the following steps:

- Select the type of the replication policy.



Synchronous replication policy is not supported.

- Specify the consistency group suffix that you want to use.

c. From the Destination Cluster and Destination SVM drop-downs select the peered cluster and SVM that you want to use.



The cluster and SVM peering is not supported by SnapCenter. You should use System Manager or ONTAP CLIs to perform cluster and SVM peering.



If the resources are already protected outside of SnapCenter, those resources will be displayed in the Secondary Protected Resources section.

1. On the Verification page, perform the following steps:

a. Click **Load locators** to load the SnapMirror or SnapVault volumes to perform verification on secondary storage.

b.

Click  in the Configure Schedules column to configure the verification schedule for all the schedule types of the policy.

c. In the Add Verification Schedules *policy\_name* dialog box, perform the following actions:

If you want to...	Do this...
Run verification after backup	Select <b>Run verification after backup</b> .
Schedule a verification	Select <b>Run scheduled verification</b> and then select the schedule type from the drop-down list.

- d. Select **Verify on secondary location** to verify your backups on secondary storage system.
- e. Click **OK**.

The configured verification schedules are listed in the Applied Schedules column.

2. In the Notification page, from the **Email preference** drop-down list, select the scenarios in which you want to send the emails.

You must also specify the sender and receiver email addresses, and the subject of the email. If you want to attach the report of the operation performed on the resource group, select **Attach Job Report**.



For email notification, you must have specified the SMTP server details using the either the GUI or the PowerShell command Set-SmSmtpServer.

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

## Create a storage system connection and a credential using PowerShell cmdlets

You must create a storage virtual machine (SVM) connection and a credential before using PowerShell cmdlets to perform data protection operations.

### Before you begin

- You should have prepared the PowerShell environment to execute the PowerShell cmdlets.
- 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 management LIF IP address.

### Steps

1. Initiate a PowerShell Core connection session by using the Open-SmConnection cmdlet.

This example opens a PowerShell session:

```
PS C:\> Open-SmConnection
```

2. Create a new connection to the storage system by using the Add-SmStorageConnection cmdlet.

This example creates a new storage system connection:

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Create a new credential by using the Add-SmCredential cmdlet.

This example creates a new credential named FinanceAdmin with Windows credentials:

```
PS C:\> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command\_name*. Alternatively, you can also refer to the [SnapCenter Software Cmdlet Reference Guide](#).

## Back up individual NetApp supported plug-ins resources

If an individual NetApp supported plug-ins resource is not part of any resource group, you can back up the resource from the Resources page. You can back up the resource on demand, or, if the resource has a policy attached and a schedule configured, then backups occur automatically according to the schedule.

### Before you begin

- You must have created a backup policy.
- If you want to back up a resource that has a SnapMirror relationship with a secondary storage, the ONTAP role assigned to the storage user should include the “snapmirror all” privilege. However, if you are using the “vsadmin” role, then the “snapmirror all” privilege is not required.

## SnapCenter UI

### Steps

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

2. In the Resources page, filter resources from the **View** drop-down list based on resource type.

Click  , and then select the host name and the resource type to filter the resources. You can then click  to close the filter pane.

3. Click the resource that you want to back up.

4. In the Resource page, if you want to use a custom name, select the **Use custom name format for Snapshot copy** check box , and then enter a custom name format for the Snapshot name.

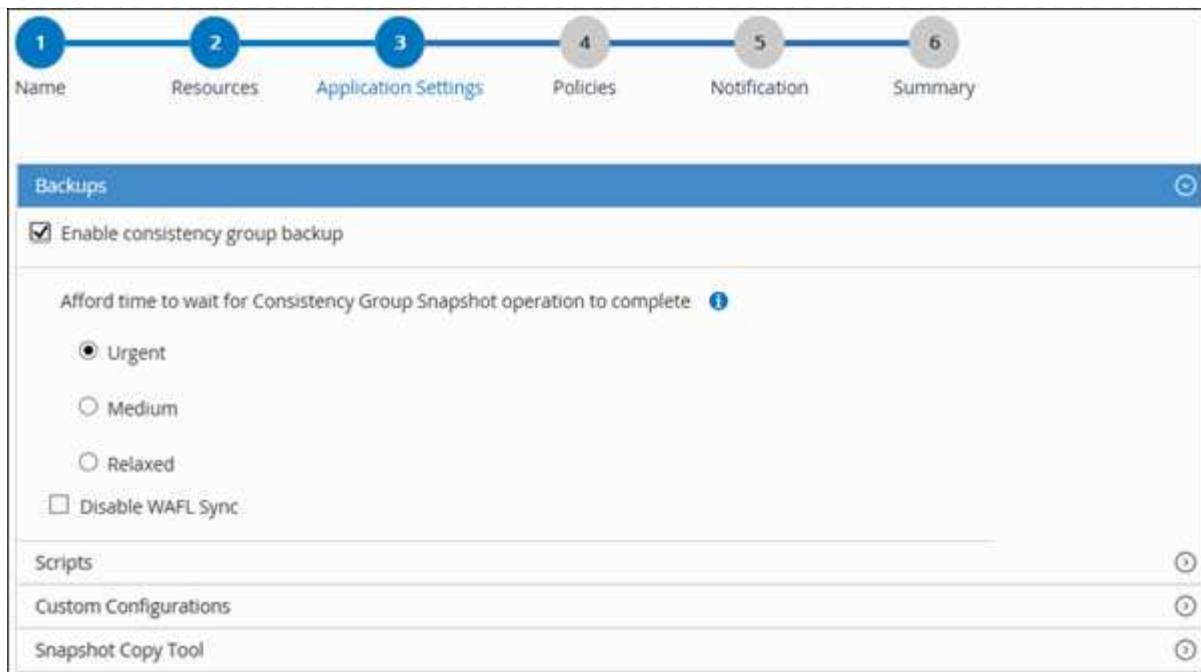
For example, *customtext\_policy\_hostname* or *resource\_hostname*. By default, a timestamp is appended to the Snapshot name.

5. In the Application Settings page, do the following:

a. Click the **Backups** arrow to set additional backup options:

Enable consistency group backup, if needed, and perform the following tasks:

For this field...	Do this...
Afford time to wait for Consistency Group Snapshot operation to complete	Select Urgent, Medium, or Relaxed to specify the wait time for Snapshot operation to complete.  Urgent = 5 seconds, Medium = 7 seconds, and Relaxed = 20 seconds.
Disable WAFL Sync	Select this to avoid forcing a WAFL consistency point.



b. Click the **Scripts** arrow to run pre and post commands for quiesce, Snapshot, and unquiesce operations. You can also run pre commands before exiting the backup operation.

Prescripts and postscripts are run in the SnapCenter Server.

c. Click the **Custom Configurations** arrow, and then enter the custom value pairs required for all jobs using this resource.

d. Click the **Snapshot Copy Tool** arrow to select the tool to create Snapshots:

If you want...	Then...
SnapCenter to take a storage level Snapshot	Select <b>SnapCenter without File System Consistency</b> .
SnapCenter to use the plug-in for Windows to put the file system into a consistent state and then take a Snapshot	Select <b>SnapCenter with File System Consistency</b> .
To enter the command to create a Snapshot	Select <b>Other</b> , and then enter the command to create a Snapshot.

6. In the Policies page, perform the following steps:

a. Select one or more policies from the drop-down list.



You can also create a policy by clicking .

In the Configure schedules for selected policies section, the selected policies are listed.

b. Click  in the Configure Schedules column for the policy for which you want to configure a

schedule.

- c. In the Add schedules for policy *policy\_name* dialog box, configure the schedule, and then click **OK**.

Where, *policy\_name* is the name of the policy that you have selected.

The configured schedules are listed in the Applied Schedules column.

7. In the Notification page, from the **Email preference** drop-down list, select the scenarios in which you want to send the emails.

You must also specify the sender and receiver email addresses, and the subject of the email. SMTP must also be configured in **Settings > Global Settings**.

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

The resources topology page is displayed.

9. Click **Back up Now**.

10. In the Backup page, perform the following steps:

- a. If you have applied multiple policies to the resource, from the **Policy** drop-down list, select the policy that you want to use for backup.

If the policy selected for the on-demand backup is associated with a backup schedule, the on-demand backups will be retained based on the retention settings specified for the schedule type.

- b. Click **Backup**.

11. Monitor the operation progress by clicking **Monitor > Jobs**.

## PowerShell cmdlets

### Steps

1. Initiate a connection session with the SnapCenter Server for a specified user by using the Open-SmConnection cmdlet.

```
Open-smconnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\\
```

The username and password prompt is displayed.

2. Add resources by using the Add-SmResources cmdlet.

This example adds resources:

```
Add-SmResource -HostName 'scc55.sccore.test.com' -PluginCode  
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database  
-StorageFootPrint (  
@{ "VolumeName"="qtree_voll_scc55_sccore_test_com"; "QTREENAME"="qtree  
Vol1"; "StorageSystem"="vserver_scauto_primary" }) -Instance QTREE1
```

3. Create a backup policy by using the Add-SmPolicy cmdlet.

This example creates a new backup policy:

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'  
-PluginPolicyType DummyPlugin -description 'testPolicy'
```

4. Add a new resource group to SnapCenter by using the Add-SmResourceGroup cmdlet.

This example creates a new resource group with the specified policy and resources:

```
Add-SmResourceGroup -ResourceGroupName  
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'  
-Resources  
@(@{"Host"="scc55.sccore.test.com";"Uid"="QTREE2";"PluginName"="Dumm  
yPlugin"},@{"Host"="scc55.sccore.test.com";"Uid"="QTREE";"PluginName"  
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'  
-usesnapcenterwithoutfilesystemconsistency
```

5. Initiate a new backup job by using the New-SmBackup cmdlet.

```
New-SMBackup -DatasetName  
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy  
test2
```

6. View the status of the backup job by using the Get-SmBackupReport cmdlet.

This example displays a job summary report of all jobs that were run on the specified date:

```

Get-SmBackupReport -JobId 149

BackedUpObjects          : {QTREE2, QTREE}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 1
SmJobId                  : 149
StartTime                : 1/15/2024 1:35:17 AM
EndTime                  : 1/15/2024 1:36:19 AM
Duration                 : 00:01:02.4265750
CreatedDateTime           : 1/15/2024 1:35:51 AM
Status                   : Completed
ProtectionGroupName       :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows
SmProtectionGroupId       : 1
PolicyName                : test2
SmPolicyId                : 4
BackupName                :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows_scc55_01-
15-2024_01.35.17.4467
VerificationStatus         : NotApplicable
VerificationStatuses       :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus           : NotApplicable
CatalogingStatuses         :
ReportDataCreatedDateTime :
PluginCode                : SCC
PluginName                : DummyPlugin
PluginDisplayName           : DummyPlugin
JobTypeId                  :
JobHost                   : scc55.sccore.test.com

```

## Back up resource groups of NetApp supported plug-in resources

You can back up a resource group on demand from the Resources page. If a resource group has a policy attached and a schedule configured, then backups occur automatically according to the schedule.

### Before you begin

- You must have created a resource group with a policy attached.
- If you want to back up a resource that has a SnapMirror relationship to secondary storage, the ONTAP role assigned to the storage user should include the “snapmirror all” privilege. However, if you are using the

“vsadmin” role, then the “snapmirror all” privilege is not required.

## 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 **Resource Group** from the **View** list.

You can search the resource group either by entering the resource group name in the search box or by clicking  and selecting the tag. You can then click  to close the filter pane.

3. In the Resource Groups page, select the resource group that you want to back up, and then click **Back up Now**.
4. In the Backup page, perform the following steps:
  - a. If you have associated multiple policies with the resource group, from the **Policy** drop-down list, select the policy that you want to use for backup.  
If the policy selected for the on-demand backup is associated with a backup schedule, the on-demand backups will be retained based on the retention settings specified for the schedule type.
  - b. Click **Backup**.
5. Monitor the operation progress by clicking **Monitor > Jobs**.
  - In MetroCluster configurations, SnapCenter might not be able to detect a protection relationship after a failover.

### [Unable to detect SnapMirror or SnapVault relationship after MetroCluster failover](#)

- If you are backing up application data on VMDKs and the Java heap size for the SnapCenter Plug-in for VMware vSphere is not large enough, the backup might fail. To increase the Java heap size, locate the script file `/opt/netapp/init_scripts/scvservice`. In that script, the `do_start` method command starts the SnapCenter VMware plug-in service. Update that command to the following: `Java -jar -Xmx8192M -Xms4096M`.

## Monitor NetApp supported plug-in resources backup operations

You can monitor the progress of different backup operations by using the SnapCenterJobs page. You might want to check the progress 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 corresponding state of the operations:

-  In progress
-  Completed successfully
-  Failed
-  Completed with warnings or could not start due to warnings
-  Queued
-  Canceled

## Steps

1. In the left navigation pane, click **Monitor**.
2. In the Monitor page, click **Jobs**.
3. In the Jobs page, perform the following steps:
  - a. Click  to filter the list so that only backup operations are listed.
  - b. Specify the start and end dates.
  - c. From the **Type** drop-down list, select **Backup**.
  - d. From the **Status** drop-down, select the backup status.
  - e. Click **Apply** to view the operations completed successfully.
4. Select a backup job, and then click **Details** to view the job details.



Though the backup job status displays  , when you click on job details you might see that some of the child tasks of the backup operation are still in progress or marked with warning signs.

5. In the Job Details page, click **View logs**.

The **View logs** button displays the detailed logs for the selected operation.

## Cancel backup operations for NetApp supported plug-ins

You can cancel backup operations that are queued.

### What you will need

- You must be logged in as the SnapCenter Admin or job owner to cancel operations.
- You can cancel a backup operation from either the **Monitor** page or the **Activity** pane.
- You cannot cancel a running backup operation.
- You can use the SnapCenter GUI, PowerShell cmdlets, or CLI commands to cancel the backup operations.
- The **Cancel Job** button is disabled for operations that cannot be canceled.
- If you selected **All members of this role can see and operate on other members objects** in Users\Groups page while creating a role, you can cancel the queued backup operations of other members while using that role.

### Steps

1. Perform one of the following actions:

From the...	Action
Monitor page	<ol style="list-style-type: none"> <li>a. In the left navigation pane, click <b>Monitor &gt; Jobs</b>.</li> <li>b. Select the operation, and then click <b>Cancel Job</b>.</li> </ol>

From the...	Action
Activity pane	<ol style="list-style-type: none"> <li data-bbox="855 160 1496 255">a. After initiating the backup operation, click  on the Activity pane to view the five most recent operations.</li> <li data-bbox="855 276 1155 308">b. Select the operation.</li> <li data-bbox="855 329 1416 361">c. In the Job Details page, click <b>Cancel Job</b>.</li> </ol>

The operation is canceled, and the resource is reverted to the previous state.

## View NetApp supported plug-ins resource related backups and clones in the Topology page

When you are preparing to back up or clone a resource, you might find it helpful to view a graphical representation of all backups and clones on the primary and secondary storage. In the Topology page, you can see all of the backups and clones that are available for the selected resource or resource group. You can view the details of those backups and clones, and then select them to perform data protection operations.

### About this task

You can review the following icons in the Manage Copies view to determine whether the backups and clones are available on the primary or secondary storage (Mirror copies or Vault copies).

-  displays the number of backups and clones that are available on the primary storage.
-  displays the number of backups and clones that are mirrored on the secondary storage using SnapMirror technology.
-  Clones of a backup of a version-flexible mirror on a mirror-vault type volume are displayed in the topology view but the mirror backup count in the topology view does not include the version-flexible backup.
-  displays the number of backups and clones that are replicated on the secondary storage using SnapVault technology.

The number of backups displayed includes the backups deleted from the secondary storage. For example, if you have created 6 backups using a policy to retain only 4 backups, the number of backups displayed are 6.



Clones of a backup of a version-flexible mirror on a mirror-vault type volume are displayed in the topology view but the mirror backup count in the topology view does not include the version-flexible backup.

## Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, either select the resource or resource group from the **View** drop-down list.
3. Select the resource either from the resource details view or from the resource group details view.

If the resource is protected, the topology page of the selected resource is displayed.

4. Review the Summary card to see a summary of the number of backups and clones available on the primary and secondary storage.

The Summary Card section displays the total number of backups and clones.

Clicking the refresh button starts a query of the storage to display an accurate count.

If SnapLock enabled backup is taken, then clicking the **Refresh** button refreshes the primary and secondary SnapLock expiry time retrieved from ONTAP. A weekly schedule also refreshes the primary and secondary SnapLock expiry time retrieved from ONTAP.

When the application resource is spread across multiple volumes, the SnapLock expiry time for the backup will be the longest SnapLock expiry time that is set for a Snapshot in a volume. The longest SnapLock expiry time is retrieved from ONTAP.

After on demand backup, by clicking the **Refresh** button refreshes the details of backup or clone.

5. In the Manage Copies view, click **Backups** or **Clones** from the primary or secondary storage to see details of a backup or clone.

The details of the backups and clones are displayed in a table format.

6. Select the backup from the table, and then click the data protection icons to perform restore, clone, rename, and delete operations.



You cannot rename or delete backups that are on the secondary storage system.



You cannot rename the backups that are on the primary storage system.

7. If you want to delete a clone, then select the clone from the table and click to delete the clone.

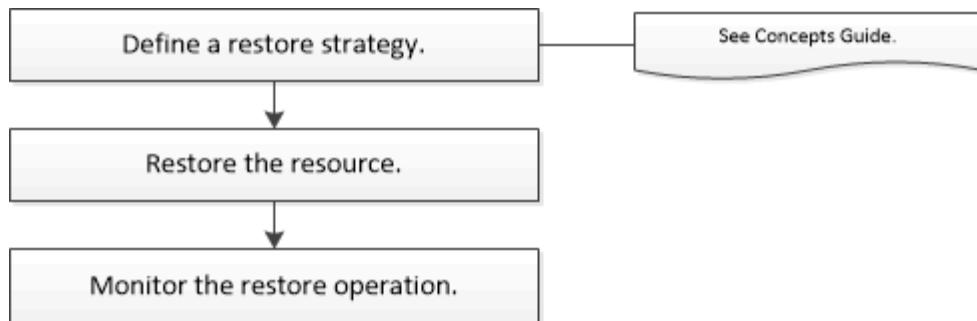
## Restore NetApp supported plug-ins resources

### Restore NetApp supported plug-in resources

The restore and recovery workflow includes planning, performing the restore operations, and monitoring the operations.

#### About this task

The following workflow shows the sequence in which you must perform the restore operation:



You can also use PowerShell cmdlets manually or in scripts to perform backup, restore, and clone operations. For information about PowerShell cmdlets, use the SnapCenter cmdlet help or see the [SnapCenter Software Cmdlet Reference Guide](#).

## Restore a resource backup

You can use SnapCenter to restore resources. The capabilities of the restore operations depends upon the plug-in that you use.

### Before you begin

- You must have backed up the resource or resource groups.
- The SnapCenter administrator must have assigned you the storage virtual machines (SVMs) for both the source volumes and destination volumes if you are replicating Snapshots to a mirror or vault.
- You must have cancelled any backup operation that is currently in progress for the resource or resource group you want to restore.

### About this task

- The default restore operation only restores storage objects. Restore operations at the application level can only be performed if the NetApp supported plug-in provides that capability.
- For ONTAP 9.12.1 and below version, the clones created from the SnapLock Vault Snapshots as part of restore will inherit the SnapLock Vault expiry time. Storage admin should manually cleanup the clones post the SnapLock expiry time.

## SnapCenter UI

### Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the Resources page, filter resources from the **View** drop-down list based on resource type.

The resources are displayed along with information such as type, host or cluster name, associated resource groups and policies, and status.



Although a backup might be for a resource group, when you restore, you must select the individual resources you want to restore.

If the resource is not protected, *Not protected* is displayed in the **Overall Status** column.

The status *Not protected* in the **Overall Status** column can mean either that the resource is not protected, or that the resource was backed up by a different user.

3. Select the resource or select a resource group and then select a resource in that group.

The resource topology page is displayed.

4. From the **Manage Copies** view, select **Backups** either from the primary or secondary (mirrored or vaulted) storage systems.
5. In the Primary backup(s) table, select the backup that you want to restore from, and then click .

Primary Backup(s)	
Backup Name	End Date
rg1_scpr0191683001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. In the Restore Scope page, select either **Complete Resource** or **File Level**.

- a. If you selected **Complete Resource**, the resource backup is restored.

If the resource contains volumes or qtrees as Storage Footprint, then newer Snapshots on such volumes or qtrees are deleted and cannot be recovered. Also, if any other resource is hosted on same volumes or qtrees, then that resource is also deleted.

- b. If you selected **File Level**, then you can either select **All**, or select volumes or qtrees, and then enter the path related to the volumes or qtrees that are selected separated by commas.
      - You can select multiple volumes and qtrees.
      - If resource type is LUN, entire LUN is restored. You can select multiple LUNs.  
NOTE: If you select **All**, all the files on the volumes, qtrees, or LUNs are restored.
  7. In the **Pre ops** page, enter pre restore and unmount commands to run before performing a restore job.
  8. In the **Post ops** page, enter mount and post restore commands to run after performing a restore job.
  9. In the **Notification** page, from the **Email preference** drop-down list, select the scenarios in which you

want to send the emails.

You must also specify the sender and receiver email addresses, and the subject of the email. SMTP must also be configured in the **Settings > Global Settings** page.

10. Review the summary, and then click **Finish**.
11. Monitor the operation progress by clicking **Monitor > Jobs**.

## PowerShell cmdlets

### Steps

1. Initiate a connection session with the SnapCenter Server for a specified user by using the Open-SmConnection cmdlet.

```
PS C:\> Open-Smconnection
```

2. Retrieve the information about the one or more backups that you want to restore by using the Get-SmBackup and Get-SmBackupReport cmdlets.

This example displays information about all available backups:

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupType	BackupTime
1	Payroll Dataset_vise-f6_08...	Full Backup	8/4/2015 11:02:32
2	Payroll Dataset_vise-f6_08...	Full Backup	8/4/2015 11:23:17

This example displays detailed information about the backup from January 29th 2015 to February 3rd, 2015:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime "2/3/2015"

SmBackupId      : 113
SmJobId        : 2032
StartTime       : 2/2/2015 6:57:03 AM
EndTime         : 2/2/2015 6:57:11 AM
Duration        : 00:00:07.3060000
CreatedDateTime : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName      : Vault
SmPolicyId      : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId        : 2183
StartTime       : 2/2/2015 1:02:41 PM
EndTime         : 2/2/2015 1:02:38 PM
Duration        : -00:00:03.2300000
CreatedDateTime : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName      : Vault
SmPolicyId      : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore data from the backup by using the `Restore-SmBackup` cmdlet.

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id : 2368
StartTime : 10/4/2016 11:22:02 PM
EndTime :
IsCancellable : False
IsRestartable : False
IsCompleted : False
IsVisible : True
IsScheduled : False
PercentageCompleted : 0
Description :
Status : Queued
Owner :
Error :
Priority : None
Tasks : { }
ParentJobID : 0
EventId : 0
JobTypeID :
ApisJobKey :
ObjectId : 0
PluginCode : NONE
PluginName :

```

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running *Get-Help command\_name*. Alternatively, you can also refer to the [SnapCenter Software Cmdlet Reference Guide](#).

## Monitor NetApp supported plug-in resources restore operations

You can monitor the progress of different SnapCenter restore operations by using the Jobs page. You might want to check the progress of an operation to determine when it is complete or if there is an issue.

### About this task

Post-restore states describe the conditions of the resource after a restore operation and any further restore actions that you can take.

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
-  Canceled

## Steps

1. In the left navigation pane, click **Monitor**.
2. In the **Monitor** page, click **Jobs**.
3. In the **Jobs** page, perform the following steps:
  - a. Click  to filter the list so that only restore operations are listed.
  - b. Specify the start and end dates.
  - c. From the **Type** drop-down list, select **Restore**.
  - d. From the **Status** drop-down list, select the restore status.
  - e. Click **Apply** to view the operations that have been completed successfully.
4. Select the restore job, and then click **Details** to view the job details.
5. In the **Job Details** page, click **View logs**.

The **View logs** button displays the detailed logs for the selected operation.

# Clone NetApp supported plug-ins resource backups

## Clone NetApp supported plug-ins resource backups

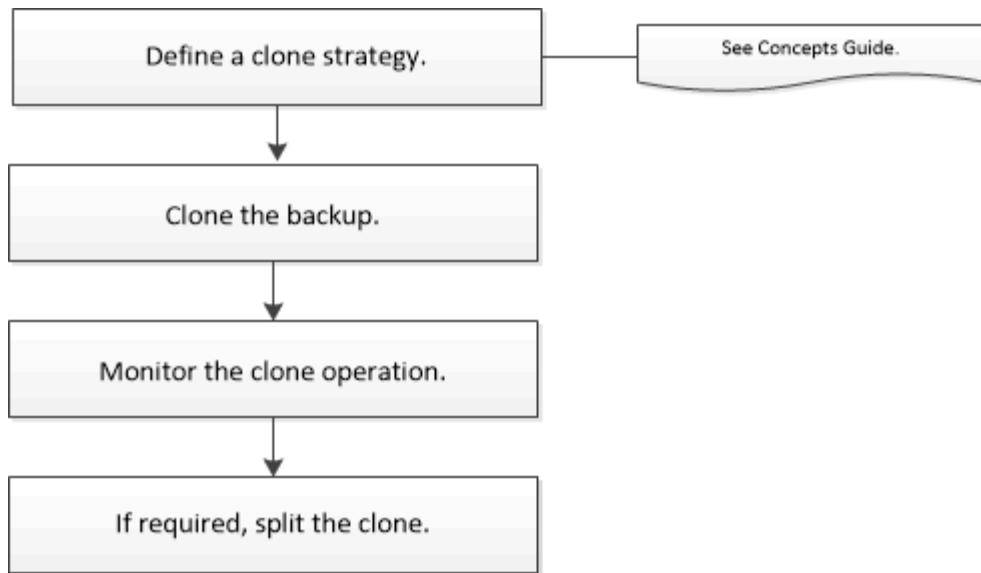
The clone workflow includes performing the clone operation and monitoring the operation.

### About this task

You might clone resource backups for the following reasons:

- To test functionality that has to be implemented using the current resource structure and content during application development cycles
- For data extraction and manipulation tools when populating data warehouses
- To recover data that was mistakenly deleted or changed

The following workflow shows the sequence in which you must perform the clone operation:



You can also use PowerShell cmdlets manually or in scripts to perform backup, restore, and clone operations. For detailed information about PowerShell cmdlets, use the SnapCenter cmdlet help or see the [SnapCenter Software Cmdlet Reference Guide](#).

## Clone from a backup

You can use SnapCenter to clone a backup. You can clone from primary or secondary backup. The capabilities of the clone operations depends upon the plug-in that you use.

### Before you begin

- You must have backed up the resources or resource group.
- The default clone operation only clones storage objects. Clone operations at the application level can only be performed if the NetApp supported plug-in provides that capability.
- You should ensure that the aggregates hosting the volumes should be in the assigned aggregates list of the storage virtual machine (SVM).

### About this task

For ONTAP 9.12.1 and below version, the clones created from the SnapLock Vault Snapshots as part of restore will inherit the SnapLock Vault expiry time. Storage admin should manually cleanup the clones post the SnapLock expiry time.

## SnapCenter UI

### Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. In the **Resources** page, filter resources from the **View** drop-down list based on resource type.

The resources are displayed along with information such as type, host or cluster name, associated resource groups and policies, and status.

3. Select the resource or resource group.

You must select a resource if you select a resource group.

The resource or resource group topology page is displayed.

4. From the Manage Copies view, select **Backups** either from the primary or secondary (mirrored or vaulted) storage systems.

5. Select the data backup from the table, and then click .

6. In the Locations page, perform the following:

For this field...	Do this...
Clone server	<p>By default, the source host is populated.</p> <p>If you want to specify a different host, select the host on which the clone should be mounted and the plug-in is installed.</p>
Clone suffix	<p>This is mandatory when the clone destination is the same as the source.</p> <p>Enter a suffix that will be appended to the newly cloned resource name. The suffix ensures that the cloned resource is unique on the host.</p> <p>For example, rs1_clone. If you are cloning to the same host as the original resource, you must provide a suffix to differentiate the cloned resource from the original resource; otherwise, the operation fails.</p>

If the resource selected is a LUN and if you are cloning from a secondary backup, then the destination volumes are listed. Single source can have multiple destination volumes.

7. In the **Settings** page, perform the following:

For this field...	Do this...
Initiator name	Enter the host initiator name, which is either a IQDN or WWPN.

For this field...	Do this...
Igroup protocol	Select Igroup protocol.



Settings page is displayed only if the storage type is LUN.

8. In the Scripts page, enter the commands for pre clone or post clone that should be run before or after the clone operation, respectively. Enter the mount command to mount a file system to a host.

For example:

- Pre clone command: delete existing databases with the same name
- Post clone command: verify a database or start a database.

Mount command for a volume or qtree on a Linux machine:  
`mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>`

9. In the **Notification** page, from the **Email preference** drop-down list, select the scenarios in which you want to send the emails.

You must also specify the sender and receiver email addresses, and the subject of the email.

10. Review the summary and click **Finish**.

11. Monitor the operation progress by clicking **Monitor > Jobs**.

## PowerShell cmdlets

### Steps

1. Initiate a connection session with the SnapCenter Server for a specified user by using the Open-SmConnection cmdlet.

```
Open-SmConnection -SMSbaseurl
https://snapctr.demo.netapp.com:8146/
```

2. List the backups that can be cloned using the Get-SmBackup or Get-SmResourceGroup cmdlet.

This example displays information about all available backups:

```
C:\PS>PS C:\> Get-SmBackup

BackupId          BackupName
BackupTime        BackupType
-----
-----          -----
1                Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32
AM                Full Backup
2                Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17
AM
```

This example displays information about a specified resource group:

```
PS C:\> Get-SmResourceGroup

Description          :
CreationTime        : 10/10/2016 4:45:53 PM
ModificationTime    : 10/10/2016 4:45:53 PM
EnableEmail         : False
EmailSMTPServer    :
EmailFrom          :
EmailTo             :
EmailSubject        :
EnableSysLog        : False
ProtectionGroupType: Backup
EnableAsupOnFailure: False
Policies            : {}
HostResourceMaping : {}
Configuration       :

SMCoreContracts.SmCloneConfiguration
LastBackupStatus    : Completed
VerificationServer  :
EmailBody           :
EmailNotificationPreference: Never
VerificationServerInfo  :
SchedulerSQLInstance:
CustomText          :
CustomSnapshotFormat:
SearchResources     : False
ByPassCredential   : False
IsCustomSnapshot   :
MaintenanceStatus  : Production
PluginProtectionGroupTypes: {SMSQL}
Tag                 :
IsInternal          : False
EnableEmailAttachment: False
VerificationSettings: {}
Name                : NFS_DB
Type                : Group
Id                 : 2
Host               :
UserName           :
Passphrase          :
Deleted             : False
Auth                : SMCoreContracts.SmAuth
IsClone             : False
CloneLevel          : 0
```

```

    Hosts : 
    StorageName : 
    ResourceGroupNames : 
    PolicyNames : 

    Description : 
    CreationTime : 10/10/2016 4:51:36 PM
    ModificationTime : 10/10/2016 5:27:57 PM
    EnableEmail : False
    EmailSMTPServer : 
    EmailFrom : 
    EmailTo : 
    EmailSubject : 
    EnableSysLog : False
    ProtectionGroupType : Backup
    EnableAsupOnFailure : False
    Policies : {}
    HostResourceMaping : {}
    Configuration : 

SMCoreContracts.SmCloneConfiguration
    LastBackupStatus : Failed
    VerificationServer : 
    EmailBody : 
    EmailNotificationPreference : Never
    VerificationServerInfo : 
    SchedulerSQLInstance : 
    CustomText : 
    CustomSnapshotFormat : 
    SearchResources : False
    ByPassRunAs : False
    IsCustomSnapshot : 
    MaintenanceStatus : Production
    PluginProtectionGroupTypes : {SMSQL}
    Tag : 
    IsInternal : False
    EnableEmailAttachment : False
    VerificationSettings : {}
    Name : Test
    Type : Group
    Id : 3
    Host : 
    UserName : 
    Passphrase : 
    Deleted : False
    Auth : SMCoreContracts.SmAuth
    IsClone : False

```

CloneLevel	:	0
Hosts	:	
StorageName	:	
ResourceGroupNames	:	
PolicyNames	:	

3. Initiate a clone operation from a clone resource group or an existing backup using the New-SmClone cmdlet.

This example creates a clone from a specified backup with all logs:

```
New-SmClone -BackupName
Verify_delete_clone_on_qtree_windows_scc54_10-04-2016_19.05.48.0886
-Resources @{"Host"="scc54.sccore.test.com";"Uid"="QTREE1"} -
CloneToInstance scc54.sccore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sccore.test.com' -igroupprotocol 'mixed'
```

4. View the status of the clone job by using the Get-SmCloneReport cmdlet.

This example displays a clone report for the specified job ID:

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartTime : 8/3/2015 2:43:02 PM
EndTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper_clone_08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError :
```

## Monitor NetApp supported plug-in resource clone operations

You can monitor the progress of SnapCenter clone operations by using the **Jobs** page. You might want to check the progress of an operation 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
- Canceled

### Steps

1. In the left navigation pane, click **Monitor**.
2. In the **Monitor** page, click **Jobs**.
3. In the **Jobs** page, perform the following steps:
  - a. Click to filter the list so that only clone operations are listed.
  - b. Specify the start and end dates.
  - c. From the **Type** drop-down list, select **Clone**.
  - d. From the **Status** drop-down list, select the clone status.
  - e. Click **Apply** to view the operations that are completed successfully.
4. Select the clone job, and then click **Details** to view the job details.
5. In the Job Details page, click **View logs**.

## Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—with prior written permission of the copyright owner.

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

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

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

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

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

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

## Trademark information

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