



# Protect SAP HANA databases



SnapCenter 4.7

**Second edition (March 2023)**

**© Copyright Lenovo 2022, 2023.**

**LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant to a General Services Administration (GSA) contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.**

# Contents

<b>1. SnapCenter Plug-in for SAP HANA Databases</b>	<b>1</b>
1.1. SnapCenter Plug-in for SAP HANA Database overview	1
1.2. What you can do using the SnapCenter Plug-in for SAP HANA Database	1
1.3. SnapCenter Plug-in for SAP HANA Database features	1
1.4. Storage types supported by SnapCenter Plug-in for SAP HANA Database	3
1.5. Minimum ONTAP privileges required for SAP HANA plug-in	3
1.6. Prepare storage systems for SnapMirror and SnapVault replication for SAP HANA databases	7
1.7. Backup strategy for SAP HANA databases	8
1.7.1. Define a backup strategy for SAP HANA databases	8
1.7.2. Automatic discovery of resources on Linux host	9
1.7.3. Type of backups supported	10
File-Based Backup	10
Snapshot copy based backup	10
1.7.4. How SnapCenter Plug-in for SAP HANA Database uses consistency group Snapshot copies	10
1.7.5. How SnapCenter manages housekeeping of log and data backups	10
1.7.6. Considerations for determining backup schedules for SAP HANA database	11
1.7.7. Number of backup jobs needed for SAP HANA databases	11
1.7.8. Backup naming conventions for Plug-in for SAP HANA databases	11
1.8. Restore and recovery strategy for SAP HANA databases	12
1.8.1. Define a restore and recovery strategy for SAP HANA resources	12
1.8.2. Types of restore strategies supported for manually added SAP HANA resources	12
Complete resource restore	12
File level restore	12
1.8.3. Types of restore strategies supported for automatically discovered SAP HANA databases	13
Complete resource restore	13
Tenant Database	13
1.8.4. Types of restore operations for auto discovered SAP HANA databases	13
Single File SnapRestore is performed in NFS environments for the following scenarios:	13
Single File SnapRestore is performed in SAN environments for the following scenarios:	13
Connect-and-copy based restore is performed in SAN environments for the following scenario:	14
1.8.5. Types of recovery operations supported for SAP HANA databases	14
<b>2. Prepare to install the SnapCenter Plug-in for SAP HANA Database</b>	<b>15</b>
2.1. Installation workflow of SnapCenter Plug-in for SAP HANA Database	15
2.2. Prerequisites for adding hosts and installing SnapCenter Plug-in for SAP HANA Database	15
2.2.1. Windows hosts	16
2.2.2. Linux hosts	16
2.3. Host requirements to install SnapCenter Plug-ins Package for Windows	16
2.4. Host requirements for installing the SnapCenter Plug-ins Package for Linux	17
2.5. Set up credentials for the SnapCenter Plug-in for SAP HANA Database	18

2.6. Configure gMSA on Windows Server 2019 or later . . . . .	21
2.7. Install the SnapCenter Plug-in for SAP HANA Databases . . . . .	22
2.7.1. Add hosts and install plug-in packages on remote hosts . . . . .	22
2.7.2. Install SnapCenter Plug-in Packages for Linux or Windows on multiple remote hosts by using cmdlets . . . . .	26
2.7.3. Install the SnapCenter Plug-in for SAP HANA Database on Linux hosts by using the command-line interface . . . . .	26
2.7.4. Monitor the status of installing Plug-in for SAP HANA . . . . .	27
2.8. Configure CA Certificate . . . . .	28
2.8.1. Generate CA Certificate CSR file . . . . .	28
2.8.2. Import CA certificates . . . . .	29
2.8.3. Get the CA certificate thumbprint . . . . .	29
2.8.4. Configure CA certificate with Windows host plug-in services . . . . .	30
2.8.5. Configure the CA Certificate for the SnapCenter SAP HANA Plug-ins service on Linux host . . . . .	31
Manage password for custom plug-in keystore and alias of the CA signed key pair in use . . . . .	31
Configure root or intermediate certificates to custom plug-in trust-store . . . . .	31
Configure CA signed key pair to custom plug-in trust-store . . . . .	32
Configure certificate revocation list (CRL) for SnapCenter Custom Plug-ins . . . . .	33
2.8.6. Configure the CA Certificate for the SnapCenter SAP HANA Plug-ins service on Windows host . . . . .	33
Manage password for custom plug-in keystore and alias of the CA signed key pair in use . . . . .	33
Configure root or intermediate certificates to custom plug-in trust-store . . . . .	34
Configure CA signed key pair to custom plug-in trust-store . . . . .	35
Configure certificate revocation list (CRL) for SnapCenter Custom Plug-ins . . . . .	35
2.8.7. Enable CA Certificates for plug-ins . . . . .	36
<b>3. Install SnapCenter Plug-in for VMware vSphere . . . . .</b>	<b>37</b>
3.1. Configure the CRL file . . . . .	37
<b>4. Prepare for data protection . . . . .</b>	<b>38</b>
4.1. Prerequisites for using the SnapCenter Plug-in for SAP HANA Database . . . . .	38
4.2. How resources, resource groups, and policies are used for protecting SAP HANA databases . . . . .	38
<b>5. Back up SAP HANA resources . . . . .</b>	<b>40</b>
5.1. Back up SAP HANA resources . . . . .	40
5.2. Configure HDB User Store Key and HDBSQL OS User for the SAP HANA database . . . . .	41
5.3. Discover resources . . . . .	41
5.3.1. Discover the databases automatically . . . . .	41
5.3.2. Add resources manually to the plug-in host . . . . .	43
5.3.3. Create backup policies for SAP HANA databases . . . . .	45
5.3.4. Create resource groups and attach policies . . . . .	48
5.3.5. Back up SAP HANA databases . . . . .	52
5.3.6. Back up resource groups . . . . .	56
5.3.7. Create a storage system connection and a credential using PowerShell cmdlets for SAP HANA database . . . . .	57

5.3.8. Back up databases using PowerShell cmdlets .....	59
5.4. Monitor backup operations .....	62
5.4.1. Monitor SAP HANA databases backup operations .....	62
5.4.2. Monitor data protection operations on SAP HANA databases in the Activity pane .....	63
5.4.3. Cancel backup operations for SAP HANA .....	63
5.4.4. View SAP HANA database backups and clones in the Topology page .....	64
<b>6. Restore SAP HANA Databases</b> .....	<b>66</b>
6.1. Restore workflow .....	66
6.2. Restore and recover a manually added resource backup .....	66
6.3. Restore and recover an auto discovered database backup .....	68
6.4. Restore SAP HANA database using PowerShell cmdlets .....	72
6.5. Restore resources using PowerShell cmdlets .....	74
6.6. Monitor SAP HANA databases restore operations .....	76
<b>7. Clone SAP HANA resource backups</b> .....	<b>78</b>
7.1. Clone workflow .....	78
7.2. Clone a SAP HANA database backup .....	78
7.3. Clone SAP HANA database backups using PowerShell cmdlets .....	80
7.4. Monitor SAP HANA database clone operations .....	82
7.5. Split a clone .....	83
7.6. Delete or split SAP HANA database clones after upgrading SnapCenter .....	84
<b>8. Appendix</b> .....	<b>86</b>
8.1. Contacting support .....	86
8.2. Notices .....	86
8.3. Trademarks .....	87

# Chapter 1. SnapCenter Plug-in for SAP HANA Databases

## 1.1. SnapCenter Plug-in for SAP HANA Database overview

The SnapCenter Plug-in for SAP HANA Database is a host-side component of the Lenovo SnapCenter software that enables application-aware data protection management of SAP HANA databases. The Plug-in for SAP HANA Database automates the backup, restore, and cloning of SAP HANA databases in your SnapCenter environment.

SnapCenter supports single container and multitenant database containers (MDC). You can use the Plug-in for SAP HANA Database in both Windows and Linux environments. The plug-in that is not installed on the HANA database host is known as the centralized host plug-in. The centralized host plug-in can manage multiple HANA databases across different hosts.

When the Plug-in for SAP HANA Database is installed, you can use SnapCenter with Lenovo SnapMirror technology to create mirror copies of backup sets on another volume. You can also use the plug-in with Lenovo SnapVault technology to perform disk-to-disk backup replication for standards compliance.

## 1.2. What you can do using the SnapCenter Plug-in for SAP HANA Database

When you install the Plug-in for SAP HANA Database in your environment, you can use SnapCenter to back up, restore, and clone SAP HANA databases and their resources. You can also perform tasks supporting those operations.

- Add databases.
- Create backups.
- Restore from backups.
- Clone backups.
- Schedule backup operations.
- Monitor backup, restore, and clone operations.
- View reports for backup, restore, and clone operations.

## 1.3. SnapCenter Plug-in for SAP HANA Database features

SnapCenter integrates with the plug-in application and with Lenovo technologies on the storage system. To work with the Plug-in for SAP HANA Database, 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, 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 monitor your environment by configuring SnapCenter to send email alerts.

- **Nondisruptive Lenovo Snapshot copy technology**

SnapCenter uses Lenovo Snapshot copy technology with the Plug-in for SAP HANA Database to back up resources.

Using the Plug-in for SAP HANA Database 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 Lenovo 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 copy feature of ONTAP as part of creating backups.
- Capability to run multiple backups simultaneously across multiple resource hosts

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

- Capability to create Snapshot copies using external commands.
- Support for file-based backup.
- Support for Linux LVM on XFS file system.

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

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

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

## 1.5. Minimum ONTAP privileges required for SAP HANA 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 9.5 and later
<code>event generate-autosupport-log</code>
<code>job history show</code>
<code>job stop</code>



## All-access commands: Minimum privileges required for ONTAP 9.5 and later

```
lun  
lun create  
lun delete  
lun igroup add  
lun igroup create  
lun igroup delete  
lun igroup rename  
lun igroup show  
lun mapping add-reporting-nodes  
lun mapping create  
lun mapping delete  
lun mapping remove-reporting-nodes  
lun mapping show  
lun modify  
lun move-in-volume  
lun offline  
lun online  
lun persistent-reservation clear  
lun resize  
lun serial  
lun show
```

**All-access commands: Minimum privileges required for ONTAP 9.5 and later**

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

## All-access commands: Minimum privileges required for ONTAP 9.5 and later

```
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
```

**All-access commands: Minimum privileges required for ONTAP 9.5 and later**

```
vserver cifs
vserver cifs share create
vserver cifs share delete
vserver cifs shadowcopy show
vserver cifs share show
vserver cifs show
vserver export-policy
vserver export-policy create
vserver export-policy delete
vserver export-policy rule create
vserver export-policy rule show
vserver export-policy show
vserver iscsi
vserver iscsi connection show
vserver show
```

**Read-only commands: Minimum privileges required for ONTAP 9.5 and later**

```
network interface
network interface show
vserver
```

## 1.6. Prepare storage systems for SnapMirror and SnapVault replication for SAP HANA databases

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 copy 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 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](#).



SnapCenter does not support **sync\_mirror** replication.

## 1.7. Backup strategy for SAP HANA databases

### 1.7.1. Define a backup strategy for SAP HANA databases

Defining a backup strategy before you create your backup jobs helps you to 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 whether you want to create a Snapshot copy-based policy to back up application-

consistent Snapshot copies of the database.

5. Decide whether you want to verify the integrity of the database.
6. Decide whether you want to use Lenovo SnapMirror technology for replication or Lenovo SnapVault technology for long-term retention.
7. Determine the retention period for the Snapshot copies on the source storage system and the SnapMirror destination.
8. Determine whether you want to run any commands before or after the backup operation and provide a prescript or postscript.

### 1.7.2. Automatic discovery of resources on Linux host

Resources are SAP HANA databases and Non-data Volume on the Linux host that are managed by SnapCenter. After installing the SnapCenter Plug-in for SAP HANA Database plug-in, the SAP HANA databases on that Linux host are automatically discovered and displayed on the **Resources** page.

Automatic discovery is supported for the following SAP HANA resources:

- Single containers

After installing or upgrading the plug-in, the single container resources located on a centralized host plug-in will continue as manually added resources.

After installing or upgrading the plug-in, the SAP HANA databases are automatically discovered only on the SAP HANA Linux hosts, which are directly registered into SnapCenter.

- Multitenant database container (MDC)

After installing or upgrading the plug-in, the MDC resources located on a centralized host plug-in will continue as manually added resource.

You must continue to manually add the MDC resources on the centralized host plug-in after upgrading.

For SAP HANA Linux hosts directly registered in SnapCenter, installing or upgrading the plug-in will trigger an automatic discovery for resources on the host. After upgrading the plug-in, for every MDC resource that was located on the plug-in host, another MDC resource will be automatically discovered with a different GUID format and registered in SnapCenter. The new resource will be in locked state.

Automatic discovery is not supported for the following configurations:

- RDM and VMDK layouts



In case the above resources are discovered, the data protection operations are not supported on these resources.

- HANA multiple-host configuration
- Multiple instances on the same host
- Multi-Tier scale out HANA System Replication
- Cascaded replication environment in System Replication mode

### 1.7.3. Type of backups supported

Backup type specifies the type of backup that you want to create. SnapCenter supports File-Based Backup and Snapshot copy-based backup types for SAP HANA databases.

#### File-Based Backup

File-Based Backups verify the integrity of the database. You can schedule the file-based backup operation to occur at specific intervals. Only active tenants are backed up. You cannot restore and clone File-Based backups from SnapCenter.

#### Snapshot copy based backup

Snapshot copy-based backups leverage Lenovo Snapshot copy technology to create online, read-only copies of the volumes on which the SAP HANA databases reside.

### 1.7.4. How SnapCenter Plug-in for SAP HANA Database uses consistency group Snapshot copies

You can use the plug-in to create consistency group Snapshot copies for resource groups. A consistency group is a container that can house multiple volumes so that you can manage them as one entity. A consistency group is simultaneous Snapshot copies of multiple volumes, providing consistent copies of a group of volumes.

You can also specify the wait time for the storage controller to consistently group Snapshot copies. The available wait time options are **Urgent**, **Medium**, and **Relaxed**. You can also enable or disable Write Anywhere File Layout (WAFL) sync during consistent group Snapshot copy operation. WAFL sync improves the performance of a consistency group Snapshot copy.

### 1.7.5. How SnapCenter manages housekeeping of log and data backups

SnapCenter manages the housekeeping of log and data backups on the storage system and file system levels, and within the SAP HANA backup catalog.

The Snapshot copies on the primary or secondary storage and their corresponding entries in the SAP HANA catalog are deleted based on the retention settings. The SAP HANA catalog entries are also deleted during backup and resource group deletion.

### 1.7.6. Considerations for determining backup schedules for SAP HANA database

The most critical factor in determining a backup schedule is the rate of change for the resource. 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).

Backup schedules have two parts, as follows:

- Backup frequency (how often backups are to be performed)

Backup frequency, 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.

- Backup schedules (exactly when backups are to be performed)

Backup schedules 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.

### 1.7.7. Number of backup jobs needed for SAP HANA databases

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).

### 1.7.8. Backup naming conventions for Plug-in for SAP HANA databases

You can either use the default Snapshot copy naming convention or use a customized naming convention. The default backup naming convention adds a timestamp to Snapshot copy names that helps you identify when the copies were created.

The Snapshot copy uses the following default naming convention:

`resourcegroupname_hostname_timestamp`

You should name your backup resource groups logically, as in the following example:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In this example, the syntax elements have the following meanings:

- *dts1* is the resource group name.
- *mach1x88* is the host name.



- 03-12-2015\_23.17.26 is the date and timestamp.

Alternatively, you can specify the Snapshot copy name format while protecting resources or resource groups by selecting **Use custom name format for Snapshot copy**. For example, customtext\_resourcegroup\_policy\_hostname or resourcegroup\_hostname. By default, the time stamp suffix is added to the Snapshot copy name.

## 1.8. Restore and recovery strategy for SAP HANA databases

### 1.8.1. Define a restore and recovery strategy for SAP HANA resources

You must define a strategy before you restore and recover your database so that you can perform restore and recovery operations successfully.

#### Steps

1. Determine the restore strategies supported for manually added SAP HANA resources.
2. Determine the restore strategies supported for auto discovered SAP HANA databases.
3. Decide the type of recovery operations that you want to perform.

### 1.8.2. Types of restore strategies supported for manually added SAP HANA 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 SAP HANA resources. You cannot recover manually added SAP HANA resources.



You cannot recover manually added SAP HANA resources.

#### Complete resource restore

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



If the resource contains volumes or qtrees, the Snapshot copies taken after the Snapshot copy 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

### 1.8.3. Types of restore strategies supported for automatically discovered SAP HANA databases

You must define a strategy before you can successfully perform restore operations using SnapCenter. There are two types of restore strategies for automatically discovered SAP HANA databases.

#### Complete resource restore

- Restores all volumes, qtrees, and LUNs of a resource
  - The **Volume Revert** option should be selected to restore the entire volume.



If the resource contains volumes or qtrees, the Snapshot copies taken after the Snapshot copy 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.

#### Tenant Database

- Restores the tenant database

If **Tenant Database** option is selected, then HANA studio or HANA recovery scripts external to SnapCenter must be used to perform the recovery operation.

### 1.8.4. Types of restore operations for auto discovered SAP HANA databases

SnapCenter supports volume-based SnapRestore (VBSR), Single File SnapRestore, and connect-and-copy restore types for automatically discovered SAP HANA databases.

#### Single File SnapRestore is performed in NFS environments for the following scenarios:

- When the backup selected for restore is taken in SnapCenter 4.5 and higher, and if only the **Complete Resource** option is selected
- For multitenant database containers (MDC), when the backup selected for restore is taken on SnapCenter 4.5 and higher, and the **Tenant Database** option is selected
- When the backup selected is from a SnapMirror or SnapVault secondary location, and the **Complete Resource** option is selected

#### Single File SnapRestore is performed in SAN environments for the following scenarios:

- When backups are taken in SnapCenter 4.5 and higher, and only if the **Complete Resource** option is selected
- When the backup is selected from a SnapMirror or SnapVault secondary location, and the **Complete Resource** option is selected

**Connect-and-copy based restore is performed in SAN environments for the following scenario:**

- For MDC, when the backup selected for restore is taken in SnapCenter 4.5 and higher, and the **Tenant Database** option is selected



**Complete Resource, Volume Revert, and Tenant Database** options are available on the Restore Scope page.

### **1.8.5. Types of recovery operations supported for SAP HANA databases**

SnapCenter enables you to perform different types of recovery operations for SAP HANA databases.

- Recover the database up to the most recent state
- Recover the database up to a specific point in time

You must specify the date and time for recovery.

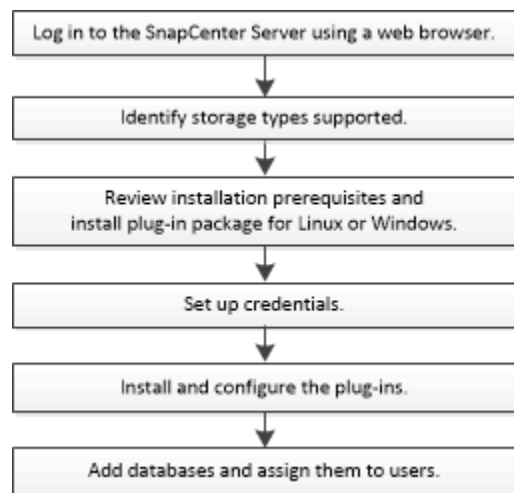
- Recover the database up to a specific data backup

SnapCenter also provides the No recovery option for SAP HANA databases.

## Chapter 2. Prepare to install the SnapCenter Plug-in for SAP HANA Database

### 2.1. Installation workflow of SnapCenter Plug-in for SAP HANA Database

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



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

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

- You must have installed Java 1.8 64-bit on your host.
- You must have installed SAP HANA database interactive terminal (HDBSQL client) on the host.
- For Windows, plug-in Creator Service should be running using the “LocalSystem” windows user, which is the default behavior when Plug-in for SAP HANA Database is installed as domain administrator.
- For Windows, user store keys should be created as SYSTEM user.
- 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. SnapCenter Plug-in for Microsoft Windows will be deployed by default with the SAP HANA plug-in on Windows hosts.
- For Linux host, HDB Secure User Store keys are accessed as HDBSQL OS user.

- SnapCenter Server should have access to the 8145 or custom port of Plug-in for SAP HANA Database host.

### 2.2.1. Windows hosts

- You must have a domain user with local administrator privileges with local login permissions on the remote host.
- While installing Plug-in for SAP HANA Database on a Windows host, SnapCenter Plug-in for Microsoft Windows is installed automatically.
- You must have enabled the password-based SSH connection for the root or non-root user.
- You must have installed Java 1.8 64-bit on your Windows host.

[Java Downloads for All Operating Systems](#)


### 2.2.2. Linux hosts

- You must have enabled the password-based SSH connection for the root or non-root user.
- For SAP HANA databases that are running on a Linux host, while installing Plug-in for SAP HANA Database, SnapCenter Plug-in for UNIX is installed automatically.

## 2.3. 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
Minimum RAM for the SnapCenter plug-in on host	1 GB

Item	Requirements
Minimum install and log space for the SnapCenter plug-in on host	5 GB   <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	<ul style="list-style-type: none"> <li>• Microsoft .NET Framework 4.7.2 or later</li> <li>• Windows Management Framework (WMF) 4.0 or later</li> <li>• PowerShell 4.0 or later</li> </ul>

## 2.4. Host requirements for installing the SnapCenter Plug-ins Package for Linux

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

Item	Requirements
Operating systems	<ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux</li> <li>• SUSE Linux Enterprise Server (SLES)</li> </ul>
Minimum RAM for the SnapCenter plug-in on host	1 GB

Item	Requirements
Minimum install and log space for the SnapCenter plug-in on host	2 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	Java 1.8.x (64-bit) Oracle Java and OpenJDK flavors  If you have upgraded JAVA to the latest version, you must ensure that the JAVA_HOME option located at <code>/var/opt/snapcenter/spl/etc/spl.properties</code> is set to the correct JAVA version and the correct path.

## 2.5. Set up credentials for the SnapCenter Plug-in for SAP HANA Database

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

### About this task

- Linux hosts

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

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

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

- Windows hosts

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

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

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

### Steps

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

Credential

Provide information for the Credential you want to add

Credential Name

Username  **i**

Password


Authentication

Use sudo privileges **i**

Cancel OK

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



For this field...	Do this...
<b>Credential name</b>	Enter a name for the credentials.
<b>User name</b>	<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> <li>• Local administrator (for workgroups only)</li> <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> <p>Do not use double quotes (") or backtick (`) in the passwords. You should not use the less than (&lt;) and exclamation (!) symbols together in passwords. For example, lessthan&lt;!10, lessthan10&lt;!, backtick`12.</p>
<b>Password</b>	Enter the password used for authentication.
<b>Authentication Mode</b>	Select the authentication mode that you want to use.
<b>Use sudo privileges</b>	<p>Select the <b>Use sudo privileges</b> check box if you are creating credentials for a non-root user.</p> <p> Applicable to Linux users only.</p>

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.

## 2.6. Configure gMSA on Windows Server 2019 or later

Windows Server 2019 or later enables you to create a group Managed Service Account (gMSA) that provides automated service account password management from a managed domain account.

### What you will need

- You should have a Windows Server 2019 or later domain controller.
- You should have a Windows Server 2019 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 -EffectiveImmediately`
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.

## 2.7. Install the SnapCenter Plug-in for SAP HANA Databases

### 2.7.1. 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-ins packages. The plug-ins are automatically installed on the remote hosts. You can add a host and install plug-in packages either for an individual host or for a cluster.

#### What you will need

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

- If you are using group Managed Service Account (gMSA), you should configure gMSA with administrative privileges.


[Configure group Managed Service Account on Windows Server 2019 or later for SAP HANA](#)


### About this task

- You cannot add a SnapCenter Server as a plug-in host to another SnapCenter Server.
- For SAP HANA System Replication to discover resources on both primary and secondary systems, it is recommended to add both the primary and the secondary systems using root or sudo user.

### Steps


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



For this field...	Do this...
<b>Host Type</b>	<p>Select the type of host:</p> <ul style="list-style-type: none"> <li>• Windows</li> <li>• Linux</li> </ul> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>The Plug-in for SAP HANA is installed on the HDBSQL client host, and this host can be on either a Windows system or a Linux system.</p> </div>
<b>Host name</b>	<p>Enter the communication host name. Enter the fully qualified domain name (FQDN) or the IP address of the host. SnapCenter depends on the proper configuration of the DNS. Therefore, the best practice is to enter the FQDN.</p> <p>You must configure the HDBSQL client and HDBUserStore on this host.</p>

For this field...	Do this...
<b>Credentials</b>	<p>Either select the credential name that you created or create new credentials. The credential must have administrative rights on the remote host. For details, see the information about creating credentials.</p> <p>You can view details about the credentials by positioning your cursor over the credential name that you provided.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>The credentials authentication mode is determined by the host type that you specify in the Add Host wizard.</p> </div>

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

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

For this field...	Do this...
<b>Port</b>	<p>Either retain the default port number or specify the port number. The default port number is 8145. If the SnapCenter Server was installed on a custom port, that port number will be displayed as the default port.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>If you manually installed the plug-ins and specified a custom port, you must specify the same port. Otherwise, the operation fails.</p> </div>
<b>Installation Path</b>	<p>The Plug-in for SAP HANA is installed on the HDBSQL client host, and this host can be on either a Windows system or a Linux system.</p> <ul style="list-style-type: none"> <li>• For the SnapCenter Plug-ins Package for Windows, the default path is <code>C:\Program Files\Lenovo\SnapCenter WebApp</code>. Optionally, you can customize the path.</li> <li>• For the SnapCenter Plug-ins Package for Linux, the default path is <code>/opt/NetApp/snapcenter</code>. Optionally, you can customize the path.</li> </ul>

For this field...	Do this...
<b>Skip preinstall checks</b>	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.
<b>Use group Managed Service Account (gMSA) to run the plug-in services</b>	<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. Click **Submit**.

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

If the error is related to disk space or RAM, you can update the web.config file located at <C:\Program Files\Lenovo\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 web.config file, you must update the file on both nodes.

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

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



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`.

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

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

#### What you will need

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

#### Steps

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

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running `Get-Help command_name`.

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.

### 2.7.3. Install the SnapCenter Plug-in for SAP HANA Database on Linux hosts by using the command-line interface

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

#### What you will need

- You should install the Plug-in for SAP HANA Database on each of the Linux host where the HDBSQL client resides.
- The Linux host on which you are installing the SnapCenter Plug-in for SAP HANA Database must meet the dependent software, database, and operating system requirements.
- The SnapCenter Plug-in for SAP HANA Database is part of SnapCenter Plug-ins Package for Linux. Before you install SnapCenter Plug-ins Package for Linux, you should have already

installed SnapCenter on a Windows host.

## Steps

1. Copy the SnapCenter Plug-ins Package for Linux installation file (snapcenter\_linux\_host\_plugin.bin) from C:\ProgramData\Lenovo\SnapCenter\PackageRepository to the host where you want to install the Plug-in for SAP HANA Database.

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

2. From the command prompt, navigate to the directory where you copied the installation file.
3. Install the plug-in: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`

- -DPORT specifies the SMCORE HTTPS communication port.
- -DSERVER\_IP specifies the SnapCenter Server IP address.
- -DSERVER\_HTTPS\_PORT specifies the SnapCenter Server HTTPS port.
- -DUSER\_INSTALL\_DIR specifies the directory where you want to install the SnapCenter Plug-ins Package for Linux.
- DINSTALL\_LOG\_NAME specifies the name of the log file.

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

4. Edit the `<installation_directory>/Lenovo/snapcenter/scc/etc/SC_SMS_Services.properties` file, and then add the `PLUGINS_ENABLED = hana:3.0` parameter.
5. Add the host to the SnapCenter Server using the Add-Smhost cmdlet and the required parameters.

The information regarding the parameters that can be used with the command and their descriptions can be obtained by running `Get-Help command_name`.

### 2.7.4. Monitor the status of installing Plug-in for SAP HANA






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**.

## 2.8. Configure CA Certificate

### 2.8.1. Generate CA Certificate CSR file

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

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

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



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

For cluster configurations, the cluster name (virtual cluster FQDN), and the respective host names should be mentioned in the CA certificate. The certificate can be updated by filling the Subject Alternative Name (SAN) field before procuring the certificate. For a wild card certificate

(\*domain.company.com), the certificate will contain all the hostnames of the domain implicitly.

## 2.8.2. 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 Snap-in**.
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 click **Next**. Then, select **Local computer** for computer to manage 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, \*.p7b).

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

## 2.8.3. 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.

## 2.8.4. 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=$certappid="$guid"
```

For example:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$certappid="$guid"
```

## 2.8.5. Configure the CA Certificate for the SnapCenter SAP HANA Plug-ins service on Linux host

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

Custom 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 custom plug-in keystore and alias of the CA signed key pair in use

#### Steps

1. You can retrieve custom plug-in keystore default password from custom 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 custom plug-in keystore and for all the associated alias password of the private key should be same.

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

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

## Steps

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

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

4. Add a root or intermediate certificate:

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

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



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

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

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

## Steps

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

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

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

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.lenovo.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 custom 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 custom plug-in trust-store.

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

### About this task

- SnapCenter Custom Plug-ins will search for the CRL files in a pre-configured directory.
- Default directory for the CRL files for SnapCenter Custom 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.

## 2.8.6. Configure the CA Certificate for the SnapCenter SAP HANA Plug-ins service on Windows host

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

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

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

### Steps

1. You can retrieve custom plug-in keystore default password from custom 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 custom plug-in keystore and for all the associated alias password of the private key should be same.

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

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

### Steps

1. Navigate to the folder containing the custom plug-in keystore `C:\Program Files\Lenovo\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 custom plug-in trust-store.



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

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

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

### Steps

1. Navigate to the folder containing the custom plug-in keystore `C:\Program Files\Lenovo\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.lenovo.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 custom 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 custom plug-in trust-store.

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

### About this task

- SnapCenter Custom Plug-ins will search for the CRL files in a pre-configured directory.
- Default directory for the CRL files for SnapCenter Custom Plug-ins is `C:\Program Files\Lenovo\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.

### 2.8.7. 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.

#### What you will need

- 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`.

#### 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.

## Chapter 3. Install SnapCenter Plug-in for VMware vSphere

If your database is stored on virtual machines (VMs), or if you want to protect VMs and datastores, you must deploy the SnapCenter Plug-in for VMware vSphere virtual appliance.

### 3.1. Configure the CRL file

SnapCenter Plug-in for VMware vSphere looks for the CRL files in a pre-configured directory. Default directory of the CRL files for SnapCenter Plug-in for VMware vSphere is */opt/netapp/config/crl*.

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

## Chapter 4. Prepare for data protection

### 4.1. Prerequisites for using the SnapCenter Plug-in for SAP HANA Database

Before you use SnapCenter Plug-in for SAP HANA Database, 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.
- Install Java 1.7 or Java 1.8 on your Linux or Windows host.

You must set the Java path in the environmental path variable of the host machine.

- Set up SnapMirror and SnapVault, if you want backup replication.
- Install the HDBSQL client on the host where you will install the Plug-in for SAP HANA Database.

Configure the user store keys for the SAP HANA nodes that you will manage through this host.

- For SAP HANA database 2.0 SPS 05, if you are using a SAP HANA database user account, ensure that you have the following permissions to perform backup, restore, and clone operations in SnapCenter Server:
  - Backup admin
  - Catalog read
  - Database backup admin
  - Database recovery operator

### 4.2. How resources, resource groups, and policies are used for protecting SAP HANA databases

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 SAP HANA databases that you back up or clone with SnapCenter.
- A SnapCenter resource group, is a collection of resources on a host.

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, 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.

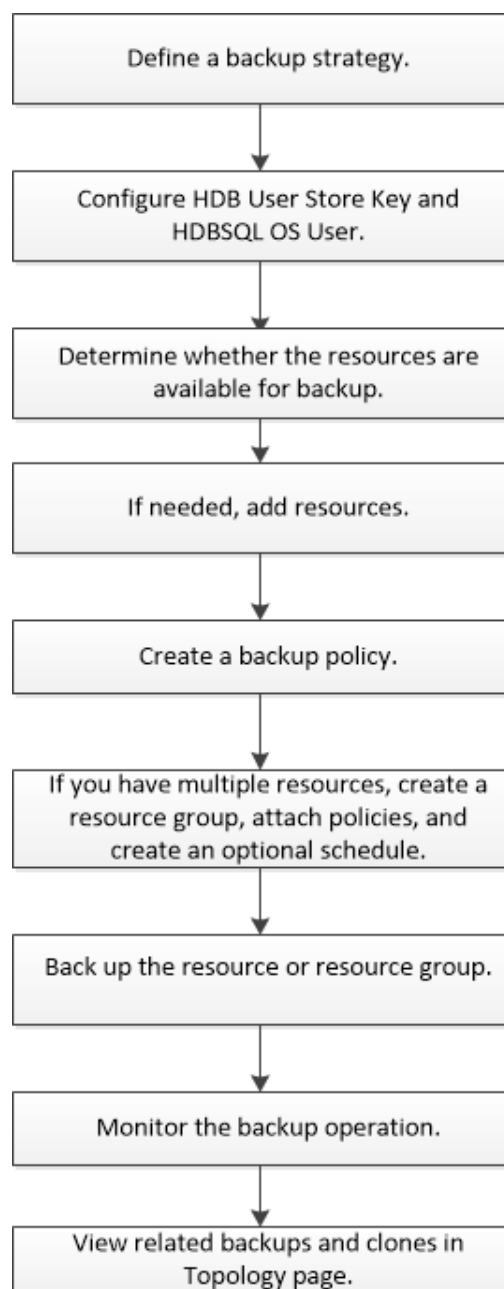
Think of a resource group as defining what you want to protect and when you want to protect it in terms of day and time. Think of a policy as defining how you want to protect it. If you are backing up all databases, for example, you might create a resource group that includes all of the databases in 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 full backup daily.

## Chapter 5. Back up SAP HANA resources

### 5.1. Back up SAP HANA resources

You can either create a backup of a resource (database) or resource group. The backup workflow includes planning, identifying the databases 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.



## 5.2. Configure HDB User Store Key and HDBSQL OS User for the SAP HANA database

You must configure HDB User Store Key and HDBSQL OS User to perform data protection operations on SAP HANA databases.

### What you will need

- If the SAP HANA database does not have the HDB Secure User Store Key and HDB SQL OS User configured, a red padlock icon appears only for the autodiscovered resources. If during a subsequent discovery operation, the configured HDB Secure User Store Key was found to be incorrect or did not provide access to the database itself, then the red padlock icon will reappear.
- You must configure the HDB Secure User Store Key and the HDB SQL OS user to be able to protect the database or add it to a resource group to perform data protection operations.
- You must configure HDB SQL OS User to access the system database. If HDB SQL OS User is configured to access only tenant database, the discovery operation will fail.

### Steps

1. In the left navigation pane, click **Resources** and then select SnapCenter Plug-in for SAP HANA Database from the list.
2. In the **Resources** page, select the resource type from the **View** list.
3. (Optional) Click  and select the host name.  
You can then click  to close the filter pane.
4. Select the database, and then click **Configure Database**.
5. In the **Configure database settings** section, enter HDB Secure User Store Key.



The Plug-in host name is displayed and HDB SQL OS User is automatically populated to <sid>adm.

6. Click **OK**.

You can modify the database configuration from the **Topology** page.

## 5.3. Discover resources

### 5.3.1. Discover the databases automatically

Resources are SAP HANA databases and Non-data Volume on the Linux host

that are managed by SnapCenter. You can add these resources to resource groups to perform data protection operations after you discover the SAP HANA databases that are available.

### What you will need


- You must have already completed tasks such as installing the SnapCenter Server, adding HDB User Store Key, adding hosts, and setting up the storage system connections.
- You must have configured the HDB Secure User Store Key and HDB SQL OS user on the Linux host.
  - You must configure the HDB User Store Key with SID adm user. For example, for HANA system with A22 as the SID, the HDB User Store Key must be configured with a22adm.
- SnapCenter Plug-in for SAP HANA Database does not support automatic discovery of the resources residing on RDM/VMDK virtual environments. You must provide the storage information for virtual environments while adding the databases manually.

### About this task

After installing the plug-in, all the resources on that Linux host are automatically discovered and displayed on the **Resources** page.

The automatically discovered resources cannot be modified or deleted.

### Steps

1. In the left navigation pane, click **Resources**, and then select the Plug-in for SAP HANA Database from the list.
2. On the **Resources** page, select the resource type from the View list.
3. (Optional) Click , and then select the host name.

You can then click  to close the filter pane.

4. Click **Refresh Resources** to discover the resources available on the host.

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

- If the database is on a Lenovo storage and not protected, then Not protected is displayed in the Overall Status column.
- If the database is on a Lenovo storage system and protected, and if there is no backup operation performed, then Backup not run is displayed in the Overall Status column. The status will otherwise change to Backup failed or Backup succeeded based on the last backup status.



If the SAP HANA database does not have a HDB Secure User Store Key configured, a red padlock icon appears next to the resource. If during a subsequent discovery operation, the configured HDB Secure User Store Key was found to be incorrect or did not provide access to the database itself, then the red padlock icon will reappear.



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

### After you finish

You must configure the HDB Secure User Store Key and HDBSQL OS User to be able to protect the database or add it to the resource group to perform data protection operations.

[Configure HDB User Store Key and HDBSQL OS User for the SAP HANA database](#)

### 5.3.2. Add resources manually to the plug-in host

Automatic discovery is not supported for certain HANA instances. You must add these resources manually.

#### What you will need

- You must have completed tasks such as installing the SnapCenter Server, adding hosts, setting up storage system connections, and adding HDB User Store Key.
- For SAP HANA system replication, it is recommended to add all the resources of that HANA system into one resource group and take a resource group backup. This ensures a seamless backup during takeover-failback mode.

[Create resource groups and attach policies.](#)

#### About this task

Automatic discovery is not supported for the following configurations:

- RDM and VMDK layouts



In case the above resources are discovered, the data protection operations are not supported on these resources.

- HANA multiple-host configuration
- Multiple instances on the same host
- Multi-Tier scale out HANA System Replication
- Cascaded replication environment in System Replication mode


#### Steps



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

For this field...	Do this...
<b>Resource Type</b>	Enter the resource type. Resource types are Single Container, Multitenant Database Container (MDC), and Non-data Volume.
<b>HANA System Name</b>	Enter the descriptive SAP HANA system name. This option is available only if you selected Single Container or MDC resource types.
<b>SID</b>	Enter the system ID (SID). The installed SAP HANA system is identified by a single SID.
<b>Plug-in Host</b>	Select the plug-in host.
<b>HDB Secure User Store Keys</b>	Enter the key to connect to the SAP HANA system. The key contains the login information to connect to the database.
<b>HDBSQL OS User</b>	Enter the user name for whom the HDB Secure User Store Key is configured. For Windows, it is mandatory for the HDBSQL OS User to be the SYSTEM user. Therefore, you must configure the HDB Secure User Store Key for the SYSTEM user.

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

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

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

The databases are displayed along with information such as the SID, plug-in host, associated resource groups and policies, and overall status.

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

## [Add a user or group and assign role and assets](#)

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

You cannot modify the following if there are backups associated with the SAP HANA resource:

- Multitenant database containers (MDC): SID, or HDBSQL Client (plug-in) Host
- Single Container: SID or HDBSQL Client (plug-in) Host
- Non-data Volume: Resource name, Associated SID, or Plug-in Host

### **5.3.3. Create backup policies for SAP HANA databases**

Before you use SnapCenter to back up SAP HANA database resources, you must create a backup policy for the resource or resource group that you want to back up. A backup policy is a set of rules that governs how you manage, schedule, and retain backups.

#### **What you will need**

- You must have defined your backup strategy.

For details, see the information about defining a data protection strategy for SAP HANA databases.

- You must have prepared for data protection by completing tasks such as installing SnapCenter, adding hosts, setting up storage system connections, and adding resources.
- The SnapCenter administrator must have assigned the SVMs for both the source and destination volumes to you if you are replicating Snapshot copies to a mirror or vault.

Additionally, you can specify replication, script, and application settings in the policy. These options saves time when you want to reuse the policy for another resource group.

#### **About this task**

- SAP HANA System Replication
  - You can protect the primary SAP HANA system and all the data protection operations can be performed.
  - You can protect the secondary SAP HANA system, but the backups cannot be created.

After the failover, all the data protection operation can be performed as the secondary SAP HANA system becomes the primary SAP HANA system.

You cannot create a backup for SAP HANA data volume, but SnapCenter continues to protect the Non-data Volumes (NDV).

## 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 description.
5. In the **Settings** page, perform the following steps:

- Choose backup type:

If you want to...	Do this...
Perform an integrity check of the database	Select <b>File-Based Backup</b> . Only active tenants are backed up.
Create a backup using Snapshot copy technology	Select <b>Snapshot Based</b> .

- 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 also enables you to assign different backup schedules to each policy.

### Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

- On demand
- Hourly
- Daily
- Weekly
- Monthly




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


- 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 **Retention** page, specify the retention settings for the backup type and the schedule type selected in the Backup Type page:

If you want to...	Then...
<p>Keep a certain number of Snapshot copies</p>	<p>Select <b>Total Snapshot copies to keep</b>, and then specify the number of Snapshot copies that you want to keep.</p> <p>If the number of Snapshot copies exceeds the specified number, the Snapshot copies are deleted with the oldest copies deleted first.</p> <p><b>NOTE:</b> The maximum retention value is 1018 for resources on ONTAP 9.5 or later. Backups will fail if retention is set to a value higher than what the underlying ONTAP version supports.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;">  <p>For Snapshot copy-based backups, 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 copy is the reference Snapshot copy for the SnapVault relationship until a newer Snapshot copy is replicated to the target.</p> </div> <p><b>NOTE:</b> For SAP HANA system replication, it is recommended to add all the resources of the SAP HANA system into one resource group. This ensures that the right number of backups are retained.</p> <p><b>NOTE:</b> For SAP HANA System Replication, the total Snapshot copies taken will be equal to the retention set for the resource group. The removal of the oldest Snapshot copy is based on which node the oldest Snapshot copy is located. For example, the retention is set to 7 for a resource group with SAP HANA System Replication primary and SAP HANA System Replication secondary. You can take a maximum of 7 Snapshot copies at a time including both SAP HANA System Replication primary and SAP HANA System Replication secondary.</p>
<p>Keep the Snapshot copies for a certain number of days</p>	<p>Select <b>Keep Snapshot copies for</b>, and then specify the number of days for which you want to keep the Snapshot copies before deleting them.</p>

7. For Snapshot copy-based backups, specify the replication settings in the **Replication** page:

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, the Snapshot copy created on the primary will not be transferred to the destination, but will be listed in the destination. If this Snapshot copy is selected from the destination to perform a restore operation, then the Secondary Location is not available for the selected vaulted/mirrored backup error message is displayed.</p>
<b>Update SnapVault after creating a local Snapshot copy</b>	Select this option to perform disk-to-disk backup replication (SnapVault backups).
<b>Secondary policy label</b>	<p>Select a Snapshot label.</p> <p>Depending on the Snapshot copy label that you select, ONTAP applies the secondary Snapshot copy retention policy that matches the label.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> If you have selected <b>Update SnapMirror after creating a local Snapshot copy</b>, you can optionally specify the secondary policy label. However, if you have selected <b>Update SnapVault after creating a local Snapshot copy</b>, you should specify the secondary policy label.</p> </div>
<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 Snapshot copies on the secondary storage.

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

#### 5.3.4. 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. A resource group enables you to back up all the data that is associated with a given application simultaneously. A resource


group is required for any data protection job. 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.

### About this task

To create SAP HANA system replication backups, it is recommended to add all the resources of the SAP HANA system into one resource group. This ensures a seamless backup during takeover-failback mode.

### Steps

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

For this field...	Do this...
<b>Name</b>	<p>Enter a name for the resource group.</p> <div style="display: flex; align-items: center;">  <p>The resource group name should not exceed 250 characters.</p> </div>
<b>Tags</b>	<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 resource groups associated with the HR tag.</p>
<b>Use custom name format for Snapshot copy</b>	<p>Select this check box, and enter a custom name format that you want to use for the Snapshot copy name.</p> <p>For example, customtext_resource_group_policy_hostname or resource_group_hostname. By default, a timestamp is appended to the Snapshot copy name.</p>

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

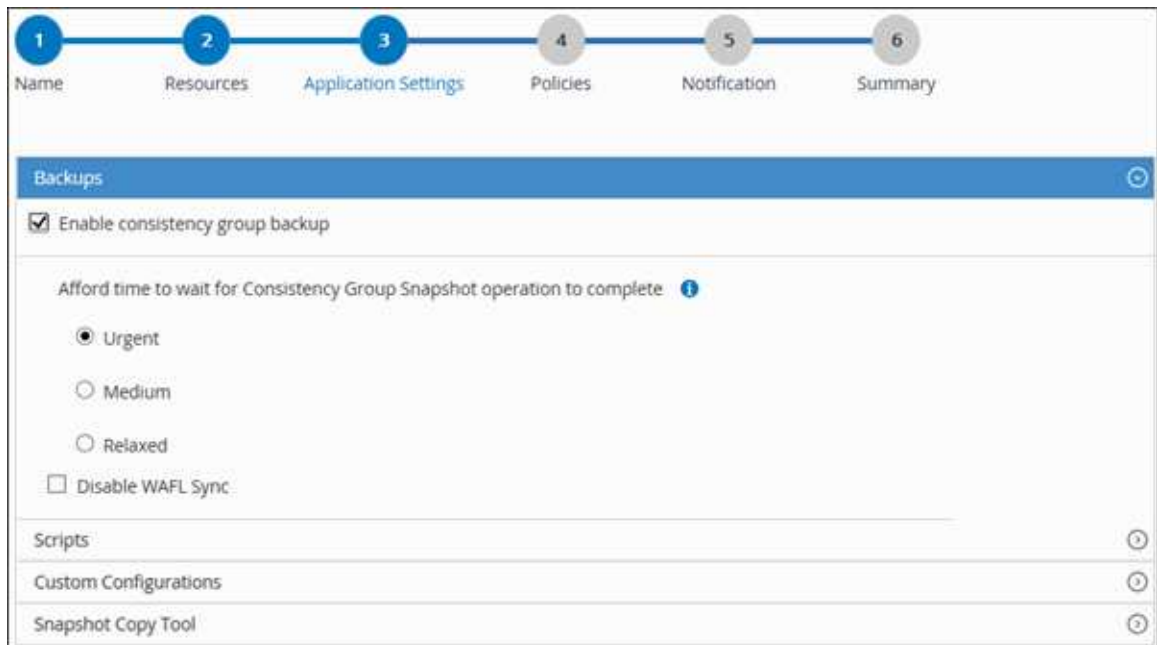
This helps to filter information on the screen.

5. Select the resources from the **Available Resources** section, and then click the right arrow to move them to the **Selected Resources** section.

6. On the **Application Settings** page, do the following:
  - a. Click the **Backups** arrow to set additional backup options:

Enable consistency group backup and perform the following tasks:

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



- b. Click the **Scripts** arrow and enter the pre and post commands for quiesce, Snapshot copy, and unquiesce operations. You can also enter the pre commands to be executed before exiting in the event of a failure.
  - c. Click 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.

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



The custom key-value pairs are supported for SAP HANA Linux plug-in systems and not supported for SAP HANA database registered as a centralized windows plug-in.

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



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 copy. For Linux resources, this option is not applicable.	Select <b>SnapCenter with File System Consistency</b> .  This option is not applicable for SnapCenter Plug-in for SAP HANA Database.
SnapCenter to create a storage level Snapshot copy	Select <b>SnapCenter without File System Consistency</b> .
To enter the command to be executed on the host to create Snapshot copies.	Select <b>Other</b> , and then enter the command to be executed on the host to create a Snapshot copy.


7. On 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  .

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

- b. In the Configure Schedules column, click  for the policy you want to configure.
- 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.

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

8. On 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. The SMTP server must be configured in **Settings > Global Settings**.

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

### 5.3.5. Back up SAP HANA databases

If a resource is not yet part of any resource group, you can back up the resource from the **Resources** page.

## What you will need

- 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.
- For Snapshot copy based backup operation, ensure that all the tenant databases are valid and active.
- To create SAP HANA system replication backups, it is recommended to add all the resources of the SAP HANA system into one resource group. This ensures a seamless backup during takeover-failback mode.

[Create resource groups and attach policies.](#)

### [Back up resource groups](#)

- If you want to create a file-based backup when one or more tenant databases are down, set the `ALLOW_FILE_BASED_BACKUP_IF_INACTIVE_TENANTS_PRESENT` parameter to **YES** in the HANA properties file using `Set-SmConfigSettings` cmdlet.

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

- For pre and post commands for quiesce, Snapshot copy, and unquiesce operations, you should check if the commands exist in the command list available on the plug-in host from the following paths:



For Windows: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt`

For Linux: `/var/opt/snapcenter/scc/allowed_commands_list.txt`



If the commands do not exist in the command list, then the operation will fail.

## Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. On the **Resource** 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. On the **Resource** page, select **Use custom name format for Snapshot copy**, and then enter a

custom name format that you want to use for the Snapshot copy name.

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

5. On the **Application Settings** page, do the following:

- Click the **Backups** arrow to set additional backup options:

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

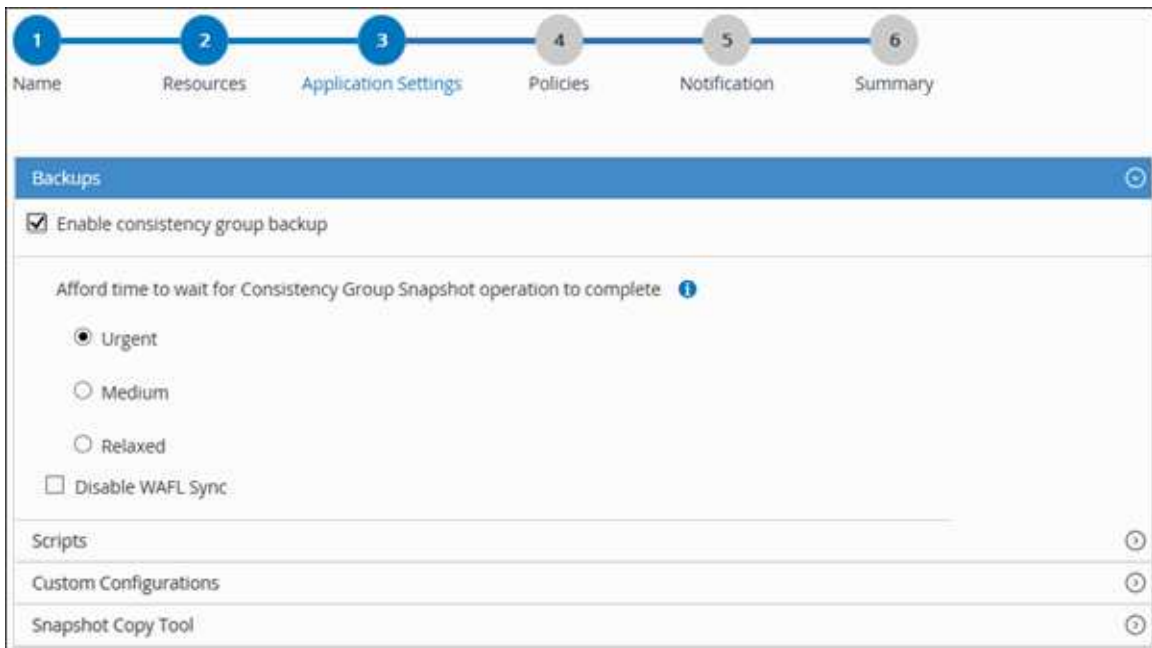
For this field...	Do this...
<b>Afford time to wait for "Consistency Group Snapshot" operation to complete</b>	Select <b>Urgent</b> , or <b>Medium</b> , or <b>Relaxed</b> to specify the wait time for Snapshot copy operation to finish. Urgent = 5 seconds, Medium = 7 seconds, and Relaxed = 20 seconds.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

- Click the **Scripts** arrow to run pre and post commands for quiesce, Snapshot copy, and unquiesce operations.

You can also run pre commands before exiting the backup operation. Prescripts and postscripts are run in the SnapCenter Server.

- Click the **Custom Configurations** arrow, and then enter the custom value pairs required for all jobs using this resource.
- Click the **Snapshot Copy Tool** arrow to select the tool to create Snapshot copies:

If you want...	Then...
SnapCenter to create a storage-level Snapshot copy	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 create a Snapshot copy	Select <b>SnapCenter with File System Consistency</b> .
To enter the command to create a Snapshot copy	Select <b>Other</b> , and then enter the command to create a Snapshot copy.




6. On 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**.

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

The configured schedules are listed in the Applied Schedules column.

7. On 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. On the **Backup** page, perform the following steps:
  - a. If you 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**.

- In MetroCluster configurations, SnapCenter might not be able to detect a protection relationship after a 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`

### 5.3.6. Back up resource groups

A resource group is a collection of resources on a host. A backup operation on the resource group is performed on all resources defined in the resource group.

#### What you will need



- You must have created a resource group with a policy attached.
- 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.

#### About this task

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.

#### 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 then 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 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**.

### 5.3.7. Create a storage system connection and a credential using PowerShell cmdlets for SAP HANA database

You must create a storage virtual machine (SVM) connection and a credential before using PowerShell cmdlets to back up, restore, or clone SAP HANA databases.

#### What you will need

- 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 Lenovo storage”.

- Storage system names should be unique.

SnapCenter does not support multiple storage systems with the same name on different clusters. Each storage system that is supported by SnapCenter should have a unique name and a unique data LIF IP address.

#### Steps

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

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

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

cmdlet.

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

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

This example shows how to create a new credential named FinanceAdmin with Windows credentials:

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

4. Add the SAP HANA communication host to SnapCenter Server.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName FinanceAdmin -PluginCode  
hana
```

5. Install the package and the SnapCenter Plug-in for SAP HANA Database on the host.

For Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana
```

For Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana -FilesystemCode scw  
-RunAsName FinanceAdmin
```

6. Set the path to the HDBSQL client.

For Windows:

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode hana -configSettings  
@{"HANA_HDBSQL_CMD" = "C:\Program Files\sap\hdbclient\hdbsql.exe"}
```

For Linux:

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com -PluginCode hana  
-configSettings @{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running `Get-Help command_name`.

### 5.3.8. Back up databases using PowerShell cmdlets

Backing up a database includes establishing a connection with the SnapCenter Server, adding resources, adding a policy, creating a backup resource group, and backing up.

#### What you will need

- You must have prepared the PowerShell environment to execute the PowerShell cmdlets.
- You must have added the storage system connection and created a credential.

#### 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.lenovo.com:8146\
```

The username and password prompt is displayed.

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

This example shows how to add a SAP HANA database of SingleContainer type:

```
C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA' -DatabaseName H10  
-ResourceType SingleContainer -StorageFootPrint  
(@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary"}) -SID 'H10'  
-filebackuppath '/tmp/HanaFileLog' -userstorekeys 'HS10' -osdbuser 'h10adm' -filebackupprefix  
'H10_'
```

This example shows how to add a SAP HANA database of MultipleContainers type:

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com' -PluginCode 'HANA'  
-DatabaseName MDC_MT -ResourceType MultipleContainers -StorageFootPrint  
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.netapp.com"}) -sid 'A12'  
-userstorekeys 'A12KEY' -TenantType 'MultiTenant'
```

This example shows how to create a non-data volume resource:

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sccore.test.com' -PluginCode 'hana' -ResourceName  
NonDataVolume -ResourceType NonDataVolume -StorageFootPrint  
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"}) -sid 'S10'
```

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

This example creates a backup policy for a Snapshot copy-based backup:



```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType Backup -PluginPolicyType hana
-BackupType SnapShotBasedBackup
```

This example creates a backup policy for a File-Based backup:

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup -PluginPolicyType hana
-BackupType FileBasedBackup
```

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

This example protects a single container resource:

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies hana_snapshotbased, hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="SID"} -Description test
-usesnapcenterwithoutfilesystemconsistency
```

This example protects a multiple containers resource:

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies hana_snapshotbased, hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="MDC\SID"} -Description test
-usesnapcenterwithoutfilesystemconsistency
```

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

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources' -Resources
@(@{"Host"="sccorelinux61.sscore.test.com";"UId"="SID"},@{"Host"="sccorelinux62.sscore.test.com"
;"UId"="MDC\SID"})
-Policies hana_snapshotbased, hana_Filebased -usesnapcenterwithoutfilesystemconsistency
-plugincode 'HANA'
```

This example creates a non-data volume resource group:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows' -Resources
@(@{"Host"="SNAPCENTERN42.sscore.test.com";"UId"="H11";"PluginName"="hana"},@{"Host"="SNAPCENTER
N42.sscore.test.com";"UId"="MDC\H31";"PluginName"="hana"},@{"Host"="SNAPCENTERN42.sscore.test.co
m";"UId"="NonDataVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies hanaprimary
```

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

This example shows how to backup a resource group:

```
C:\PS> New-SMBackup -ResourceGroupName  
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources' -Policy hana_snapshotbased
```

This example backs up a protected resource:

```
C:\PS> New-SMBackup -Resources @{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}  
-Policy hana_Filebased
```

6. Monitor the job status (running, completed, or failed) by using the `Get-smJobSummaryReport` cmdlet.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Monitor the backup job details like backup ID, backup name to perform restore or clone operation by using the `Get-SmBackupReport` cmdlet.

```
PS C:\> Get-SmBackupReport -JobId 351  
Output:  
BackedUpObjects      : {DB1}  
FailedObjects        : {}  
IsScheduled          : False  
HasMetadata          : False  
SmBackupId           : 269  
SmJobId              : 2361  
StartDateTime        : 10/4/2016 11:20:45 PM  
EndDateTime          : 10/4/2016 11:21:32 PM  
Duration             : 00:00:46.2536470  
CreatedDateTime      : 10/4/2016 11:21:09 PM  
Status               : Completed  
ProtectionGroupName  : Verify_ASUP_Message_windows  
SmProtectionGroupId  : 211  
PolicyName           : test2  
SmPolicyId           : 20  
BackupName           : Verify_ASUP_Message_windows_scc54_10-04-2016_23.20.46.2758  
VerificationStatus   : NotVerified  
VerificationStatuses :  
SmJobError           :  
BackupType           : SCC_BACKUP  
CatalogingStatus     : NotApplicable  
CatalogingStatuses  :  
ReportDataCreatedDateTime :
```

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running `Get-Help command_name.`







## 5.4. Monitor backup operations

### 5.4.1. Monitor SAP HANA databases backup operations


You can monitor the progress of different backup operations by using the SnapCenter\*Jobs\* 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. On 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. On the **Job Details** page, click **View logs**.


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

### 5.4.2. Monitor data protection operations on SAP HANA databases in the Activity pane

The **Activity** pane displays the five most recent operations performed. The **Activity** pane also displays when the operation was initiated and the status of the operation.

The **Activity** pane displays information regarding backup, restore, clone, and scheduled backup operations. If you are using Plug-in for SQL Server or Plug-in for Exchange Server, the **Activity** pane also displays information about the reseed operation.

#### Steps

1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. Click  on the **Activity** pane to view the five most recent operations.

When you click one of the operations, the operation details are listed in the Job Details page.

### 5.4.3. Cancel backup operations for SAP HANA

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
<b>Monitor</b> page	<ol style="list-style-type: none"><li>a. In the left navigation pane, click <b>Monitor</b> &gt; <b>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>After initiating the backup operation, click  on the <b>Activity</b> pane to view the five most recent operations.</li> <li>Select the operation.</li> <li>On the Job Details page, click <b>Cancel Job</b>.</li> </ol>




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

#### 5.4.4. View SAP HANA database 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.

##### 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.
-  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 created 6 backups using a policy to retain only 4 backups, the number of backups displayed is 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.



For SAP HANA system replication primary resources, the restore and delete operations are supported and for secondary resources, the clone operation is supported.

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.

## 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 File-Based backups, Snapshot copy backups, and clones.

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

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, and delete operations.



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

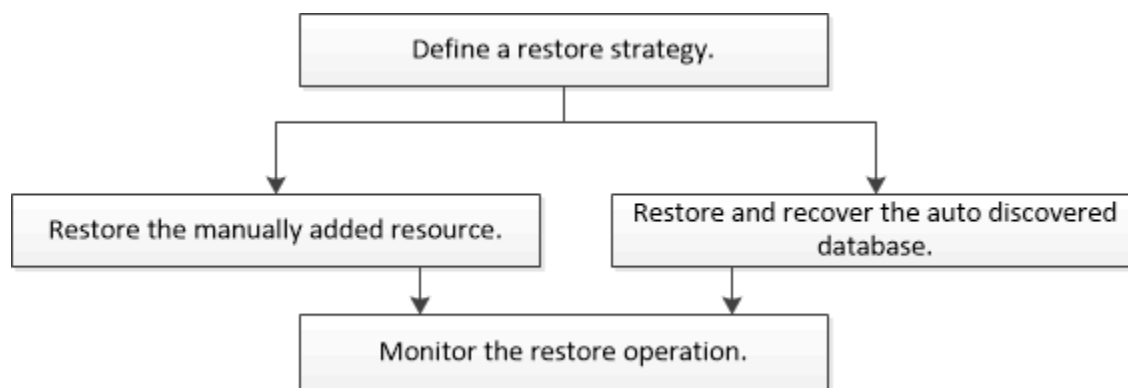
7. If you want to delete a clone, select the clone from the table, and then click .
8. If you want to split a clone, select the clone from the table, and then click .

## Chapter 6. Restore SAP HANA Databases

### 6.1. Restore workflow

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

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.

### 6.2. Restore and recover a manually added resource backup

You can use SnapCenter to restore and recover data from one or more backups.

#### What you will need

- You must have backed up the resource or resource groups.
- You must have canceled any backup operation that is currently in progress for the resource or resource group that you want to restore.
- For pre restore, post restore, mount, and unmount commands, you should check if the commands exist in the command list available on the plug-in host from the following paths:

For Windows: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt`

For Linux: `/var/opt/snapcenter/scc/allowed_commands_list.txt`



If the commands do not exist in the command list, then the operation will fail.

#### About this task

File-based backup copies cannot be restored from SnapCenter.

## Steps

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

The resources are displayed along with type, host, 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. This 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_scispr0191683001_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 select **Complete Resource**, all of the configured data volumes of the SAP HANA database are restored.

If the resource contains volumes or qtrees, the Snapshot copies taken after the Snapshot copy selected for restore 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 select **File Level**, then you can either select **All** or select the specific volumes or qtrees, and then enter the path related to those volumes or qtrees, separated by commas



- You can select multiple volumes and qtrees.
- If the resource type is LUN, the entire LUN is restored.

You can select multiple LUNs.



If you select **All**, all the files on the volumes, qtrees, or LUNs are restored.

7. On the **Pre ops** page, enter pre restore and unmount commands to run before performing a restore job.

Unmount commands are not available for auto discovered resources.

8. On the **Post ops** page, enter mount and post restore commands to run after performing a restore job.

Mount commands are not available for auto discovered resources.

9. On 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 on the **Settings > Global Settings** page.

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

## 6.3. Restore and recover an auto discovered database backup

You can use SnapCenter to restore and recover data from one or more backups.

### What you will need

- You must have backed up the resource or resource groups.
- You must have canceled any backup operation that is currently in progress for the resource or resource group that you want to restore.
- For pre restore, post restore, mount, and unmount commands, you should check if the commands exist in the command list available on the plug-in host from the following paths:

For Windows: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt`

For Linux: `/var/opt/snapcenter/scc/allowed_commands_list.txt`



If the commands do not exist in the command list, then the operation will fail.

### About this task

File-based backup copies cannot be restored from SnapCenter.

### Steps

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

The resources are displayed along with type, host, 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. This 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_scopr0191683001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. In the **Restore Scope** page, select **Complete Resource** to restore the configured data volumes of the SAP HANA database.



You can select either **Complete Resource** (with or without **Volume Revert**), or **Tenant Database**.

Recovery operation is not supported by SnapCenter Server for multiple tenants when user

selects either the **Tenant Database** or **Complete Restore** option. You must use HANA studio or HANA python script to perform the recovery operation.

- a. Select **Volume Revert** if you want to restore the entire volume.

This option is available for backups taken in SnapCenter 4.5 and later versions in NFS environments.

If the resource contains volumes or qtrees, the Snapshot copies taken after the Snapshot copy 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. This is applicable when **Complete Resource** with **Volume Revert** option is selected for restore.

- b. Select **Tenant Database**.

This option is available only for MDC resources.

Ensure to stop the tenant database before performing the restore operation.

If you select **Tenant Database** option, you must use HANA studio or use HANA recovery scripts external to SnapCenter to perform recovery operation.

- 7. On the **Recovery scope** page, select one of the following options:

If you...	Do this...
Want to recover as close as possible to the current time	<p>Select <b>Recover to most recent state</b>. For single container resources specify one or more log and catalog backup locations.</p> <p>For multitenant database container (MDC) resources specify one or more log backup locations and the backup catalog location.</p> <p>For MDC resources, the path should contain both system database and tenant database logs.</p>

If you...	Do this...
Want to recover to the specified point in time	<p>Select <b>Recover to point in time</b>.</p> <p>a. Select the time zone.</p> <p>Browser timezone is populated by default.</p> <p>The selected time zone along with the input time is converted to absolute GMT.</p> <p>b. Enter date and time. For example, the HANA Linux host is located in Sunnyvale, CA and the user in Raleigh, NC is recovering the logs in to SnapCenter.</p> <p>The time difference between both these locations is 3 hours, and since the user has logged in from Raleigh, NC, the default browser time zone that will be selected in the GUI is GMT-04:00.</p> <p>If the user wants to perform a recovery to 5 a.m. Sunnyvale, CA, then the user has to set the browser time zone to the HANA Linux host time zone, which is GMT-07:00 and specify the date and time as 5:00 a.m.</p> <p>For single container resources specify one or more log and catalog backup locations.</p> <p>For MDC resources, specify one or more log backup locations and the backup catalog location.</p> <p>For MDC resources, the path should contain both system database and tenant database logs.</p>
Want to recover to a specific data backup	Select <b>Recover to specified data backup</b> .
Do not want to recover	Select <b>No recovery</b> . You must perform the recovery operation manually from the HANA studio.

You can recover only those backups that are taken after upgrading to SnapCenter 4.5 and higher, provided both the host and the plug-in are upgraded to SnapCenter 4.5 and higher, and the backups selected for restore are taken after the resource is converted or discovered as auto discovered resource.

- On the **Pre ops** page, enter pre restore and unmount commands to run before performing a restore job.

Unmount commands are not available for auto discovered resources.

9. On the **Post ops** page, enter mount and post restore commands to run after performing a restore job.

Mount commands are not available for auto discovered resources.

10. On 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 on the **Settings > Global Settings** page.

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

## 6.4. Restore SAP HANA database using PowerShell cmdlets

Restoring a SAP HANA database backup includes initiating a connection session with the SnapCenter Server, listing the backups and retrieving backup information, and restoring a backup.

### What you will need

You must have prepared the PowerShell environment to execute the 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.lenovo.com:8146/
```

2. Identify the backup that you want to restore by using the `Get-SmBackup` and `Get-SmBackupReport` cmdlets.

This example shows that there are two backups available for the restore:

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

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

```
SmBackupId      : 113
SmJobId         : 2032
StartDateTime   : 2/2/2015 6:57:03 AM
EndDateTime     : 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_SCSPPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId         : 2183
StartDateTime   : 2/2/2015 1:02:41 PM
EndDateTime     : 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_SCSPPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

### 3. Start the recovery process in the HANA studio.

The database is shut down.

### 4. Restore data from the backup by using the Restore-SmBackup cmdlet.



AppObjectId is "Host\Plugin\UID", where UID = SID is for single container type resource and UID = MDC\SID is for multiple containers resource. You can get the ResourceId from the Get-smResources cmdlet.

```
Get-smResources -HostName cn24.sccore.test.com -PluginCode HANA
```

This example shows how to restore the database from the primary storage:

```
Restore-SmBackup -PluginCode HANA -AppObjectId cn24.sccore.test.com\hana\H10 -BackupId 3
```

This example shows how to restore the database from the secondary storage:

```
Restore-SmBackup -PluginCode 'HANA' -AppObjectId cn24.sscore.test.com\hana\H10 -BackupId 399
-Confirm:$false -Archive @( @{"Primary"="<Primary
Vserver>:<PrimaryVolume>";"Secondary"="<Secondary Vserver>:<SecondaryVolume>"})
```

The backups will be available in HANA studio for recovery.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running `Get-Help command_name`.

## 6.5. Restore resources using PowerShell cmdlets

Restoring a resource backup includes initiating a connection session with the SnapCenter Server, listing the backups and retrieving backup information, and restoring a backup.

You must have prepared the PowerShell environment to execute the 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.lenovo.com:8146/
```

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:

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

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

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

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

```
SmBackupId      : 113
SmJobId         : 2032
StartDateTime   : 2/2/2015 6:57:03 AM
EndDateTime     : 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
StartDateTime   : 2/2/2015 1:02:41 PM
EndDateTime     : 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.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269 -Confirm:$false
output:
Name           : Restore 'scc54.sscore.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`.





## 6.6. Monitor SAP HANA databases 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. On the **Job Details** page, click **View logs**.

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



After the volume based restore operation, the backup metadata is deleted from the SnapCenter repository but the backup catalog entries remain in SAP HANA catalog. Though the restore job status displays  , you should click on job details to see the warning sign of some of the child tasks. Click on the warning sign and delete the indicated backup catalog entries.

## Chapter 7. Clone SAP HANA resource backups

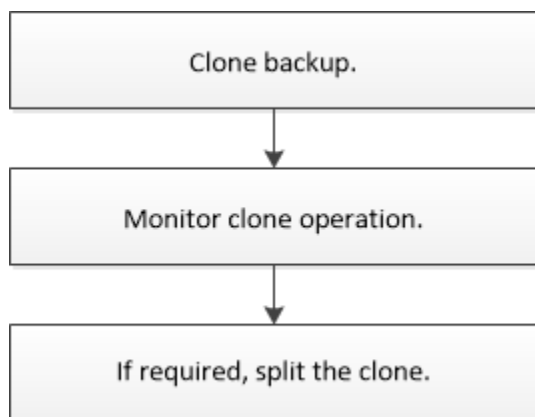
### 7.1. Clone workflow

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

#### About this task

- You can clone on the source SAP HANA server.
- 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.

### 7.2. Clone a SAP HANA database backup

You can use SnapCenter to clone a backup. You can clone from primary or secondary backup.

#### What you will need

- You should have backed up the resources or resource group.
- You should ensure that the aggregates hosting the volumes should be in the assigned aggregates list of the storage virtual machine (SVM).
- You cannot clone file-based backups.

- The target clone server should have the same SAP HANA instance SID that is provided in the Target Clone SID field.
- For pre clone or post clone commands, you should check if the commands exist in the command list available on the plug-in host from the following paths:

For Windows: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt`

For Linux: `/var/opt/snapcenter/scc/allowed_commands_list.txt`



If the commands do not exist in the command list, then the operation will fail.

**About this task** For information about clone split operation limitations, see [ONTAP 9 Logical Storage Management Guide](#).

### Steps


1. In the left navigation pane, click **Resources**, and then select the appropriate plug-in from the list.
2. On 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, 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. On the **Location** page, perform the following actions:

For this field...	Do this...
<b>Plug-in host</b>	Select the host on which the clone should be mounted and the plug-in is installed.
<b>Target Clone SID</b>	Enter the SAP HANA instance ID to clone from the existing backups.
<b>NFS Export IP Address</b>	Enter IP addresses or the host names on which the cloned volumes will be exported.

For this field...	Do this...
<b>iSCSI Initiator</b>	Enter iSCSI initiator name of the host to which the LUNs are exported. This option is available only if you selected LUN resource type.
<b>Protocol</b>	Enter the LUN protocol. This option is available only if you selected LUN resource type.

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



Before cloning, you must ensure that the iSCSI initiator or the FCP is present and are configured and logged into alternate hosts.

7. On the **Scripts** page, perform the following steps:



The scripts are run on the plug-in host.

- a. Enter the commands for pre clone or post clone that should be run before or after the clone operation, respectively.
  - Pre clone command: delete existing databases with the same name
  - Post clone command: verify a database or start a database.
- b. Enter the mount command to mount a file system to a host.

Mount command for a volume or qtree on a Linux machine:

Example for NFS:

```
mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt
```

8. On 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.

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

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

### 7.3. Clone SAP HANA database backups using PowerShell cmdlets

The clone workflow includes planning, performing the clone operation, and

monitoring the operation.

You must have prepared the PowerShell environment to execute the PowerShell cmdlets.

The information regarding the parameters that can be used with the cmdlet and their descriptions can be obtained by running `Get-Help command_name`.

## 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.lenovo.com:8146/
```

2. Retrieve the backups to perform the clone operation by using the `Get-SmBackup` cmdlet.

This example shows that two backups are available for cloning:

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

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

3. Initiate a clone operation from an existing backup and specify the NFS export IP addresses on which the cloned volumes are exported.

This example shows that the backup to be cloned has an `NFSEXPORtIPs` address of 10.232.206.169:

```
New-SmClone -AppPluginCode hana -BackupName scscore1_sscore_test_com_hana_H73_scscore1_06-07-2017_02.54.29.3817 -Resources @{"Host"="scscore1.sscore.test.com";"Uid"="H73"}  
-CloneToInstance shivsc4.sscore.test.com -mountcommand 'mount 10.232.206.169:%hana73data_Clone  
/hana83data' -preclonecreatecommands '/home/scripts/scpre_clone.sh' -postclonecreatecommands  
'/home/scripts/scpost_clone.sh'
```



If `NFSEXPORtIPs` is not specified, the default is exported to the clone target host.

4. Verify that the backups were cloned successfully by using the `Get-SmCloneReport` cmdlet to view the clone job details.

You can view details such as clone ID, start date and time, end date and time.

```

PS C:\> Get-SmCloneReport -JobId 186

SmCloneId      : 1
SmJobId        : 186
StartDateTime  : 8/3/2015 2:43:02 PM
EndDateTime    : 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     :







```

## 7.4. Monitor SAP HANA database 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**.

## 7.5. Split a clone

You can use SnapCenter to split a cloned resource from the parent resource. The clone that is split becomes independent of the parent resource.

### About this task

- You cannot perform the clone split operation on an intermediate clone.

For example, after you create clone1 from a database backup, you can create a backup of clone1, and then clone this backup (clone2). After you create clone2, clone1 is an intermediate clone, and you cannot perform the clone split operation on clone1. However, you can perform the clone split operation on clone2.

After splitting clone2, you can perform the clone split operation on clone1 because clone1 is no longer the intermediate clone.

- When you split a clone, the backup copies and clone jobs of the clone are deleted.
- For information about clone split operation limitations, see [ONTAP 9 Logical Storage Management Guide](#).
- Ensure that the volume or aggregate on the storage system is online.

### Steps


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

Option	Description
For database applications	Select <b>Database</b> from the View list.
For file systems	Select <b>Path</b> from the View list.

3. Select the appropriate resource from the list.

The resource topology page is displayed.



4. From the Manage Copies view, select the cloned resource (for example, the database or LUN), and then click .
5. Review the estimated size of the clone that is to be split and the required space available on the aggregate, and then click **Start**.
6. Monitor the operation progress by clicking **Monitor > Jobs**.

The clone split operation stops responding if the SMCore service restarts. You should run the Stop-SmJob cmdlet to stop the clone split operation, and then retry the clone split operation.

If you want a longer poll time or shorter poll time to check whether the clone is split or not, you can change the value of *CloneSplitStatusCheckPollTime* parameter in *SMCoreServiceHost.exe.config* file to set the time interval for SMCore to poll for the status of the clone split operation. The value is in milliseconds and the default value is 5 minutes.

For example:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

The clone split start operation fails if backup, restore, or another clone split is in progress. You should restart the clone split operation only after the running operations are complete.

## 7.6. Delete or split SAP HANA database clones after upgrading SnapCenter

After upgrading to SnapCenter 4.5 and higher, you will no longer see the clones. You can delete the clone or split the clones from the Topology page of the resource from which the clones were created.

### About this task

If you want to locate the storage footprint of the hidden clones, run the following command: `Get-SmClone -ListStorageFootprint`



### Steps

1. Delete the backups of the cloned resources by using the remove-smbbackup cmdlet.
2. Delete the resource group of the cloned resources by using the remove-smresourcegroup cmdlet.
3. Remove the protection of the cloned resource by using the remove-smprotectresource cmdlet.
4. Select the parent resource from the **Resources** page.

The resource topology page is displayed.

5. From the **Manage Copies** view, select the clones either from the primary or secondary

(mirrored or replicated) storage systems.

6. Select the clones, and then click  to delete clones or click  to split the clones.
7. Click **OK**.

## Chapter 8. Appendix

### 8.1. Contacting support

You can contact Support to obtain help for your issue.

You can receive hardware service through a Lenovo Authorized Service Provider. To locate a service provider authorized by Lenovo to provide warranty service, go to <https://datacentersupport.lenovo.com/serviceprovider> and use filter searching for different countries. For Lenovo support telephone numbers, see <https://datacentersupport.lenovo.com/supportphonenumber> for your region support details.

### 8.2. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

Lenovo (United States), Inc.  
8001 Development Drive  
Morrisville, NC 27560  
U.S.A.  
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information

contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

### **8.3. Trademarks**

LENOVO, LENOVO logo, and THINKSYSTEM are trademarks of Lenovo. All other trademarks are the property of their respective owners. © 2022 Lenovo.

**Lenovo**