# Back up SAP HANA resources

SnapCenter Software 4.5

NetApp
July 03, 2026

This PDF was generated from https://docs.netapp.com/us-en/snapcenter-45/protect-hana/task_back_up_sap_hana_resources.html on July 03, 2026. Always check docs.netapp.com for the latest.

# Table of Contents

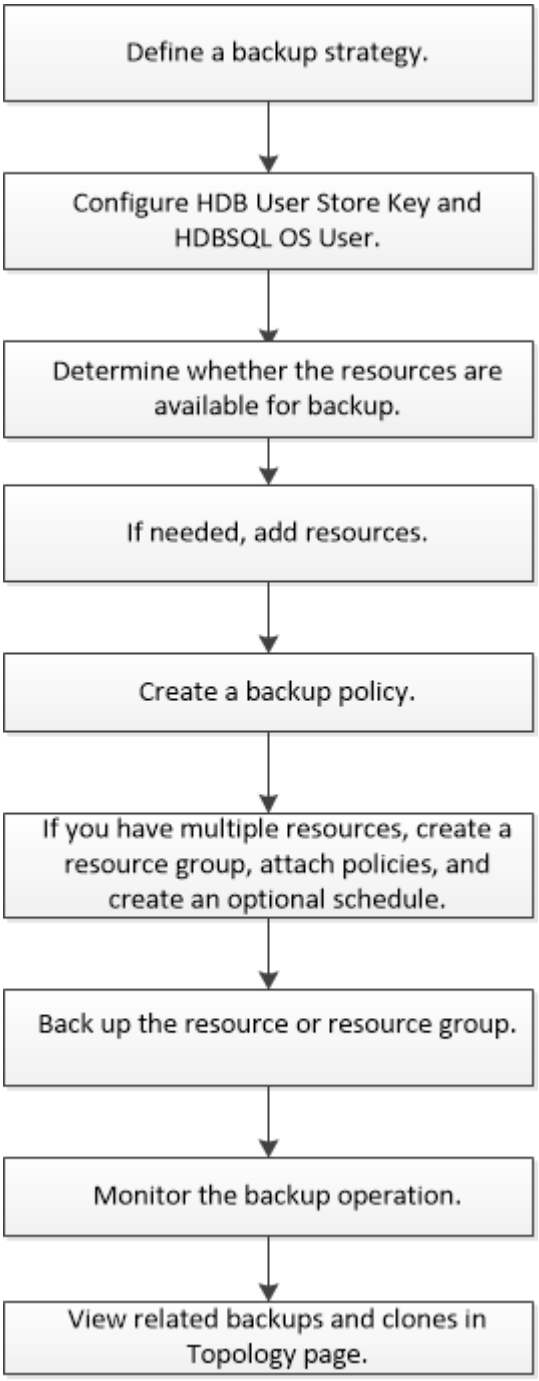

Back up SAP HANA resources . . . 1
- Back up SAP HANA resources . . . 1
- Configure HDB User Store Key and HDBSQL OS User for the SAP HANA database . . . 2
- Discover resources and prepare multitenant database containers for data protection . . . 2
  - Discover the databases automatically . . . 2
  - Prepare multitenant database containers for data protection . . . 4
- Add resources manually to the plug-in host . . . 5
- Create backup policies for SAP HANA databases . . . 6
- Create resource groups and attach policies . . . 9
- Back up SAP HANA databases . . . 13
- Back up resource groups . . . 16
- Create a storage system connection and a credential using PowerShell cmdlets for SAP HANA database . . . 17
- Back up databases using PowerShell cmdlets . . . 18
- Monitor backup operations . . . 22
  - Monitor SAP HANA databases backup operations . . . 22
  - Monitor data protection operations on SAP HANA databases in the Activity pane . . . 23
- Cancel backup operations for SAP HANA . . . 23
- View SAP HANA database backups and clones in the Topology page . . . 24

# Back up SAP HANA resources

## 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. The SnapCenter cmdlet help and the cmdlet reference information contain more information about PowerShell cmdlets. SnapCenter Software Cmdlet Reference Guide.

# 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.

# Discover resources and prepare multitenant database containers for data protection

## 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 NetApp storage and not protected, then Not protected is displayed in the Overall Status column.
   - If the database is on a NetApp 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.

**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

## Prepare multitenant database containers for data protection

For SAP HANA hosts directly registered in SnapCenter, installing or upgrading the SnapCenter Plug-in for SAP HANA Database will trigger an automatic discovery for resources on the host. After installing or upgrading the plug-in, for every multitenant database containers (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.

### About this task

For example, in SnapCenter 4.2, if E90 MDC resource was located on the plug-in host and registered manually, after upgrading to SnapCenter 4.3, another E90 MDC resource with a different GUID will be discovered and registered in SnapCenter.

> The backups associated with the resource of SnapCenter 4.2 and earlier versions must be retained until the expiry of the retention period. After the retention period expires, you can delete the old MDC resource and continue to manage the new auto discovered MDC resource.

`Old MDC resource` is the MDC resource for a plug-in host that was manually added in SnapCenter 4.2 or earlier releases.

Perform the following steps to start using the new resource discovered in SnapCenter 4.3 for data protection operations:

### Steps

1. On the **Resources** page, select the old MDC resource with backups added to the earlier SnapCenter release, and place it in “maintenance mode” from the Topology page.

   If the resource is part of a resource group, place the resource group in “maintenance mode”.

2. Configure the new MDC resource discovered after upgrading to SnapCenter 4.3 by selecting the new resource from the Resources page.

   “New MDC resource” is the newly discovered MDC resource that was discovered once the SnapCenter Server and the plug-in host was upgraded to 4.3. The new MDC resource can be identified as a resource with the same SID as the old MDC resource, for a given host, and with a red padlock icon next to it in the Resources page.

3. Protect the new MDC resource discovered after upgrading to SnapCenter 4.3 by selecting protection policies, schedules, and notification settings.
4. Delete the backups taken in SnapCenter 4.2 or earlier releases based on the retention settings.
5. Delete the resource group from the Topology page.
6. Delete the old MDC resource from the Resources page.

   For example, if the primary Snapshot copies retention period is 7 days and secondary Snapshot copies retention is 45 days, after 45 days are complete and after all the backups are deleted, you must delete the resource group and the old MDC resource.

### Find more information

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

View SAP HANA database backups and clones in the Topology page

# 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.

**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
- HANA System Replication
- Multiple instances on the same host

**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… |
|---|---|
| Resource Type | Enter the resource type. Resource types are Single Container, Multitenant Database Container (MDC), and Non-data Volume. |
| HANA System Name | Enter the descriptive SAP HANA system name. This option is available only if you selected Single Container or MDC resource types. |
| SID | Enter the system ID (SID). The installed SAP HANA system is identified by a single SID. |
| Plug-in Host | Select the plug-in host. |

| For this field… | Do this… |
| --- | --- |
| HDB Secure User Store Keys | Enter the key to connect to the SAP HANA system. The key contains the login information to connect to the database. |
| HDBSQL OS User | Enter the user name for whom the HDB Secure User Store Key is configured. For Windows, it is mandatory for the HDBSQL OS User to be the SYSTEM user. Therefore, you must configure the HDB Secure User Store Key for the SYSTEM user. |

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, plugin 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 the SAP HANA resource has backups associated with it:

- 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

# 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.

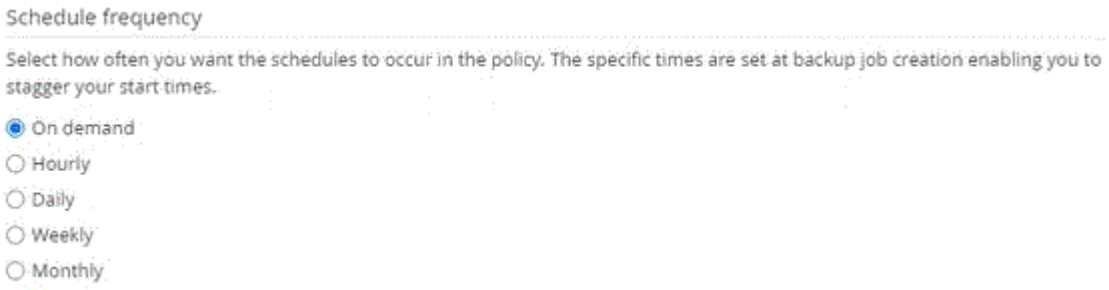
### Steps

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 **File-Based Backup**. Only active tenants are backed up. |
| Create a backup using Snapshot copy technology | Select **Snapshot Based**. |

   - 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.




> ⓘ 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… |
| --- | --- |
| Keep a certain number of Snapshot copies | Select **Total Snapshot copies to keep**, and then specify the number of Snapshot copies that you want to keep.<br><br>If the number of Snapshot copies exceeds the specified number, the Snapshot copies are deleted with the oldest copies deleted first.<br><br>The maximum retention value is 1018 for resources on ONTAP 9.4 or later, and 254 for resources on ONTAP 9.3 or earlier. Backups will fail if retention is set to a value higher than what the underlying ONTAP version supports.<br><br>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. |
| Keep the Snapshot copies for a certain number of days | Select **Keep Snapshot copies for**, and then specify the number of days for which you want to keep the Snapshot copies before deleting them. |

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

| For this field… | Do this… |
| --- | --- |
| **Update SnapMirror after creating a local Snapshot copy** | Select this field to create mirror copies of the backup sets on another volume (SnapMirror replication).<br><br>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. |

| For this field… | Do this… |
| --- | --- |
| **Update SnapVault after creating a local Snapshot copy** | Select this option to perform disk-to-disk backup replication (SnapVault backups). |
| **Secondary policy label** | Select a Snapshot label.<br><br>Depending on the Snapshot copy label that you select, ONTAP applies the secondary Snapshot copy retention policy that matches the label.<br><br>If you have selected **Update SnapMirror after creating a local Snapshot copy**, you can optionally specify the secondary policy label. However, if you have selected **Update SnapVault after creating a local Snapshot copy**, you should specify the secondary policy label. |
| **Error retry count** | 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**.

# 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.

**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… |
| --- | --- |
| Name | Enter a name for the resource group.<br><br>The resource group name should not exceed 250 characters. |
| Tags | Enter one or more labels that will help you later search for the resource group.<br><br>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. |
| Use custom name format for Snapshot copy | Select this check box, and enter a custom name format that you want to use for the Snapshot copy name.<br><br>For example, customtext_resource group_policy_hostname or resource group_hostname. By default, a timestamp is appended to the Snapshot copy name. |

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… |
| --- | --- |
| Afford time to wait for Consistency Group Snapshot operation to complete | Select **Urgent**, **Medium**, or **Relaxed** to specify the wait time for Snapshot copy operation to complete.<br><br>Urgent = 5 seconds, Medium = 7 seconds, and Relaxed = 20 seconds. |
| Disable WAFL Sync | Select this to avoid forcing a WAFL consistency point. |

b. Click the **Scripts** arrow 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. |
| ARCHIVE_LOG_RETENTION | number_of_days | Specifies the number of days the archive logs are retained.<br><br>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. |

| Parameter | Setting | Description |
|---|---|---|
| ARCHIVE_LOG_EXT | file_extension | Specifies the archive log file extension length.<br><br>For example, if the archive log is log_backup_0_0_0_0.16151855 1942 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.<br><br>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 **SnapCenter with File System Consistency**.<br><br>This option is not applicable for SnapCenter Plug-in for SAP HANA Database. |
| SnapCenter to create a storage level Snapshot copy | Select **SnapCenter without File System Consistency**. |
| To enter the command to be executed on the host to create Snapshot copies. | Select **Other**, 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**.

# 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.
- If you want to create a file-based backup when one or more tenant databases are down, set the ALLOW_FILE_BASED_BACKUP_IFINACTIVE_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

### 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… |
| --- | --- |
| Afford time to wait for "Consistency Group Snapshot" operation to complete | Select **Urgent**, or **Medium**, or **Relaxed** to specify the wait time for Snapshot copy operation to finish. Urgent = 5 seconds, Medium = 7 seconds, and Relaxed = 20 seconds. |
| Disable WAFL Sync | 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 **SnapCenter without File System Consistency**. |
| SnapCenter to use the plug-in for Windows to put the file system into a consistent state and then create a Snapshot copy | Select **SnapCenter with File System Consistency**. |
| To enter the command to create a Snapshot copy | Select **Other**, 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.

      For information, see: Unable to detect SnapMirror or SnapVault relationship after MetroCluster failover

    - If you are backing up application data on VMDKs and the Java heap size for the SnapCenter Plug-in for VMware vSphere is not large enough, the backup might fail.

      To increase the Java heap size, locate the script file */opt/netapp/init_scripts/scvservice*. In that script, the *do_start method* command starts the SnapCenter VMware plug-in service. Update that command to the following: *Java -jar -Xmx8192M -Xms4096M*

# 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**.

# 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 NetApp storage”.

- Storage system names should be unique.

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

**Steps**

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

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

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*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

# 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.netapp.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.sccore.test.com";"Uid"="SID"},@{"Host"="sccore
linux62.sccore.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.sccore.test.com";"Uid"="H11";"PluginName"="han
a"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="MDC\H31";"PluginName
"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"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*. Alternatively, you can also refer to the SnapCenter Software Cmdlet Reference Guide.

# Monitor backup operations

## Monitor SAP HANA databases backup operations

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

### About this task

The following icons appear on the Jobs page and indicate the corresponding state of the operations:

- In progress
- Completed successfully
- Failed

- Completed with warnings or could not start due to warnings
- Queued
- Canceled

**Steps**

1. In the left navigation pane, click **Monitor**.
2. In the Monitor page, click **Jobs**.
3. 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.

## 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.

# 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 |
|---|---|
| Monitor page | a. In the left navigation pane, click **Monitor** > **Jobs**.<br>b. Select the operation, and then click **Cancel Job**. |
| Activity pane | a. After initiating the backup operation, click on the Activity pane to view the five most recent operations.<br>b. Select the operation.<br>c. On the Job Details page, click **Cancel Job**. |

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

# 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.

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 .

## Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

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

## Trademark information

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