Protect SAP HANA databases

SnapCenter software

NetApp
January 09, 2026

Table of Contents

Protect SAP HANA databases

Add hosts and install SnapCenter plug-in for SAP HANA database

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

Before you begin

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

- When installing a plug-in on a Windows host, if you specify a credential that is not built-in, or if the user belongs to a local workgroup user, you must disable UAC on the host.

- If you are installing on the centralized host, ensure that the SAP HANA client software is installed on that host and open the required ports on the SAP HANA database host to run the HDB SQL queries remotely.

Steps

1. In the left navigation pane, click **Hosts**.

2. Verify that the **Managed Hosts** tab is selected.

3. Click **Add**.

4. In the Hosts page, perform the following actions:

    a. In the Host Type field, select the host type.

    b. In the Host name field, enter the fully qualified domain name (FQDN) or the IP address of the host.

    c. In the Credentials field, enter the credential that you created.

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

6. (Optional) Click **More Options** and specify the details.

7. Click **Submit**.

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.

9. Monitor the installation progress.

Add SAP HANA database

You should add the SAP HANA database manually.

About this task

Resources need to be added manually if the plug-in is installed on a centralized server. If the SAP HANA plug-in is installed on the HANA database host, then the HANA system is discovered automatically.

ⓘ Automatic discovery is not supported for HANA multi-host configuration, they must be added through centralized plug-in only.

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. In the Resources page, click **Add SAP HANA Database**.

3. In the Provide Resource Details page, perform the following actions:

   a. Enter the resource type either as Single Container, Multitenant Database Container, or Non-data Volume.

   b. Enter the SAP HANA system name.

   c. Enter the system ID (SID).

   d. Select the plug-in host.

   e. Enter the key to connect to the SAP HANA system.

   f. Enter the username for whom the HDB Secure User Store Key is configured.

4. In the Provide Storage Footprint page, select **Azure NetApp Files** as the storage type.

   a. Select the Azure NetApp account.

   b. Select the capacity pool and the associated volumes.

   c. Click **Save**.

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

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.

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 Policy type page, perform the following steps:

   a. Select **Azure NetApp Files** as the storage type.

   b. Select **File-Based** if you want to perform an integrity check of the database.

   c. Select **Snapshot Based** if you want to create a backup using Snapshot technology.

6. In the Snapshot and backup page, perform the following steps:

   a. Select the frequency of the scheduled backup.

   b. Specify the retention settings.

   c. If you want to enable Azure NetApp Files backup, select **Enable backup** and specify the retention settings.

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

Create resource groups and attach SAP HANA backup 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. In the Resources page, click **New Resource Group**.

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

For this field…	Do this…
Name	Enter a name for the resource group.
Tags	Enter one or more labels that will help you later search for the resource group.
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 name.

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

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

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

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

   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**.

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

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

Back up SAP HANA databases running on Azure NetApp Files

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

Steps

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

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

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

4. In 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 name.

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

   a. Select the **Backups** arrow to set additional backup options.

   b. Select the **Scripts** arrow to run pre and post commands for quiesce, Snapshot, and unquiesce operations.

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

   d. Select the **Snapshot Copy Tool > SnapCenter without File System Consistency** to create Snapshots.

   The **File System Consistency** option is applicable only for applications running on Windows hosts.

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

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

   b. Select ➕ 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 select **OK**.

   policy_name is the name of the policy that you selected.

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

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

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

9. Select **Back up Now**.

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

    a. If multiple policies are associated with 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.

11. Select **Backup**.

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

Back up SAP HANA 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.

Steps

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

2. In the Resources page, select **Resource Group** from the **View** list.

3. In the Resource Groups page, select the resource group that you want to back up, and then select **Back up Now**.

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

   a. If multiple policies are associated 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. Select **Backup**.

5. Monitor the operation progress by selecting **Monitor** > **Jobs**.

Restore and recover SAP HANA databases

You can restore and recover data from the backups.

About this task

For Auto discovered HANA systems, if the **Complete Resource** option is selected, then restore is performed using Single File snapshot restore technology. If the **Fast Restore** check box is selected, then Volume Revert technology is used.

For manually added resources, Volume Revert technology is always used.

Steps

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

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

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

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 .

6. In the Restore Scope page, select **Complete Resource**.

   All the configured data volumes of the SAP HANA database are restored.

7. For Auto discovered HANA systems, in the Recovery scope page, perform the following actions:

   a. Select **Recover to most recent state** if you want to recover as close as possible to the current time.

   b. Select **Recover to point in time** if you want to recover to the specified point in time.

   c. Select **Recover to specified data backup** if you want to recover to a specific data backup.

   d. Select **No recovery** if you do not want to recover now.

   e. Specify the log backup locations.

   f. Specify the backup catalog location.

8. In the Pre ops page, enter pre restore and unmount commands to run before performing a restore job.

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

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

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

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

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

Clone SAP HANA database backup

You can use SnapCenter to clone a SAP HANA database using the backup of the database. The clones created are thick clones and are created on the parent capacity pool.

Steps

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

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

3. Select the resource or resource group.

4. From the Manage Copies view, select **Backups** from the primary storage system.

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

6. In the Location page, perform the following actions:

    a. Select the host that has the SAP HANA plug-in installed for managing the cloned HANA system.

       It can be a centralized plug-in host or HANA system host.

       > ⓘ If the HANA plug-in is installed on a centralized host that manages HANA databases on other hosts, while creating or deleting clones, SnapCenter intentionally skips host side operations (mount or unmount filesystem) as the target server is a centralized host. You should use custom pre or post clone scripts to perform mount and unmount operations.

    b. Enter the SAP HANA SID to clone from the existing backups.

    c. Enter IP addresses or the host names on which the cloned volumes will be exported.

    d. If the SAP HANA database ANF volumes are configured in a manual QOS capacity pool, specify the QOS for the cloned volumes.

       If QOS for the cloned volumes is not specified, the QOS of the source volume will be used. If the automatic QOS capacity pool is used, the QOS value specified will be ignored.

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

    a. Enter the commands for pre clone or post clone that should be run before or after the clone operation, respectively.

    b. Enter the mount command to mount a file system to a host.

If the source HANA system is auto discovered and the clone target host plug-in is installed on the SAP HANA host, then SnapCenter automatically unmounts the existing HANA data volumes on the clone target host and mounts the newly cloned HANA data volumes.

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

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

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

> (i) Clone Split is disabled for ANF clones because ANF clone is already an independent volume created from the selected Snapshot.