# Table of Contents

SAP HANA backup and recovery on Azure NetApp Files with SnapCenter Service .................................. 1  
   TR-4905: SAP HANA backup and recovery on Azure NetApp Files with SnapCenter Service ............... 1  
The NetApp solution ................................................................................................................................. 2  
SnapCenter Service architecture .......................................................................................................... 6  
SnapCenter Service SAP HANA backup solution .................................................................................. 8  
SnapCenter Service concepts and best practices .................................................................................. 10  
Lab setup used for this report .............................................................................................................. 15  
SnapCenter Service policy configuration ............................................................................................... 16  
SnapCenter Service Snapshot backup configuration .............................................................................. 20  
SAP HANA database Snapshot backups ............................................................................................... 36  
File-based backups and block integrity check ...................................................................................... 44  
Restore and recovery ............................................................................................................................. 46  
Where to find additional information .................................................................................................. 67  
Version history ..................................................................................................................................... 67
This technical report covers best practices for SAP HANA data protection with NetApp SnapCenter Service and Azure NetApp Files. It covers SnapCenter Service concepts, configuration recommendations, and operation workflows, including backup and restore and recovery operations.

Companies today require continuous, uninterrupted availability for their SAP applications. They expect consistent performance levels in the face of ever-increasing volumes of data and the need for routine maintenance tasks such as system backups. Performing backups of SAP databases is a critical task and can have a significant performance effect on the production SAP system.

Backup windows are shrinking, while the amount of data to be backed up is increasing. Therefore, it is difficult to find a time when backups can be performed with minimal effect on business processes. The time needed to restore and recover SAP systems is a concern, because downtime for SAP production and nonproduction systems must be minimized to reduce data loss and cost to the business.

The following points summarize the challenges facing SAP backup and recovery:

- **Performance effects on production SAP systems.** Typically, traditional copy-based backups create a significant performance drain on production SAP systems because of the heavy loads placed on the database server, the storage system, and the storage network.

- **Shrinking backup windows.** Conventional backups can only be made when few dialog or batch activities are in process on the SAP system. The scheduling of backups becomes more difficult when SAP systems are in use around the clock.

- **Rapid data growth.** Rapid data growth and shrinking backup windows require ongoing investment in backup infrastructure. In other words, you must procure additional backup disk space and faster backup networks. You must also cover the ongoing expense of storing and managing these backup assets. Incremental or differential backups can address these issues, but this arrangement results in a very slow, cumbersome, and complex restore process that is harder to verify. Such systems usually increase recovery time objective (RTO) and recovery point objective (RPO) times in ways that are not acceptable to the business.

- **Increasing cost of downtime.** Unplanned downtime of an SAP system typically affects business finances. A significant part of any unplanned downtime is consumed by the requirement to restore and recover the SAP system. Therefore, the desired RTO dictates the design of the backup and recovery architecture.

- **Backup and recovery time for SAP upgrade projects.** The project plan for an SAP upgrade includes at least three backups of the SAP database. These backups significantly reduce the time available for the upgrade process. The decision to proceed is generally based on the amount of time required to restore and recover the database from the previously created backup. Rather than just restoring a system to its previous state, a rapid restore provides more time to solve problems that might occur during an upgrade.

Next: The NetApp solution.
The NetApp solution

You can use Azure NetApp Files NetApp Snapshot technology to create database backups in seconds. The time needed to create a Snapshot copy is independent of the size of the database because a Snapshot copy does not move any physical data blocks on the storage platform. In addition, the use of Snapshot technology has no performance effect on the live SAP system. Therefore, you can schedule the creation of Snapshot copies without considering peak dialog or batch activity periods. SAP on Azure NetApp Files customers typically schedule multiple online Snapshot backups during the day; for example, every four hours is common. These Snapshot backups are typically kept for three to five days on the primary storage system before being removed.

Snapshot copies also provide key advantages for restore and recovery operations. A volume revert operation enables the restoration of an entire database to any point in time, based on the available Snapshot copies. Such restore processes are finished in a few seconds, independent of the size of the database. Because several online Snapshot backups are created during the day, the time needed for the recovery process is significantly reduced relative to a traditional backup approach. Because a restore operation can be performed with a Snapshot copy that is only a few hours old (rather than up to 24 hours), fewer transaction logs must be applied. Therefore, the RTO is reduced to several minutes rather than the several hours required for conventional single-cycle backups.

Snapshot copy backups are stored on the same disk system as the active online data. Therefore, NetApp recommends using Snapshot copy backups as a supplement rather than a replacement for backups to a secondary location. Most restore and recovery actions are handled by using a volume revert operation on the primary storage system. Restores from a secondary location are only necessary if the primary storage system containing the Snapshot copies is damaged. You can use the secondary location if it is necessary to restore a backup that is no longer available from a Snapshot copy.

You can back up to a secondary location by using additional HANA file-based backups. These file-based backups can be scheduled with a much lower frequency, and therefore with less impact on the production system performance.

When Azure NetApp Files Cross Region Replication is used for disaster recovery, all Snapshot backups are also replicated to the disaster recovery site and would then also be available as an offloaded secondary backup. See also TR-4891: SAP HANA disaster recovery with Azure NetApp Files.

You can also offload Snapshot copies for longer term retention to Azure Blob storage using the Azure AzCopy tool. This requires additional scripting outside of SnapCenter Service.

The following figure shows an example of a data protection configuration using Snapshot backups and file-based backups.
Runtime of Snapshot backups

The following figure shows a screenshot of a customer’s HANA Studio running SAP HANA on NetApp storage. The customer is using NetApp Snapshot copies to back up the HANA database. As the figure shows, the HANA database (approximately 2.3TB) is backed up in 2 minutes and 11 seconds by using Snapshot backup technology.

The largest part of the overall backup workflow runtime is the time needed to execute the HANA backup savepoint operation—this step is dependent on the load on the HANA database. The storage Snapshot backup itself always finishes in a couple of seconds.

Recovery Time Objective comparison

This section provides an RTO comparison of file-based and storage-based Snapshot backups. The RTO is defined by the sum of the time needed to restore the database and the time needed to start and recover the database.
Time needed to restore database

With a file-based backup, the restore time depends on the size of the database and backup infrastructure, which defines the restore speed in megabytes per second (MBps). For example, if the infrastructure supports a restore operation at a speed of 250MBps, it takes approximately 1 hour and 10 minutes to restore a database 1TB in size.

With storage Snapshot copy backups, the restore time is independent of the size of the database and is in the range of a couple of seconds when you can perform the restore from primary storage. A restore from a file-based backup is only required in the case of a disaster when the primary storage is no longer available.

Time needed to start database

The database start time depends on the size of the row and column store. For the column store, the start time also depends on how much data is preloaded during the database start. In the following examples, we assume that the start time is 30 minutes. The start time is the same for a file-based restore and recovery and a restore and recovery based on Snapshot copies.

Time needed to recover database

The recovery time depends on the number of logs that must be applied after the restore. This number is determined by the frequency at which data backups are taken.

With file-based data backups, the backup schedule is typically once per day. A higher backup frequency is normally not possible because the backup degrades production performance. Therefore, in the worst case, all the logs that were written during the day must be applied during forward recovery.

Storage Snapshot copy data backups are typically scheduled with a higher frequency because they do not influence the performance of the SAP HANA database. For example, if Snapshot copy backups are scheduled every six hours, the recovery time is, in the worst case, one-fourth of the recovery time for a file-based backup (6 hours / 24 hours = 1/4).

The following figure shows an RTO example for a 1TB database when file-based data backups are used. In this example, a backup is taken once per day. The RTO differs depending on when the restore and recovery were performed. If the restore and recovery were performed immediately after a backup was taken, the RTO is primarily based on the restore time, which is 1 hour and 10 minutes in the example. The recovery time increased to 2 hours and 50 minutes when restore and recovery were performed immediately before the next backup was taken, and the maximum RTO was 4 hours and 30 minutes.
The following figure shows an RTO example for a 1TB database when Snapshot backups are used. With storage-based Snapshot backups, the RTO only depends on the database start time and the forward recovery time because the restore is completed in a few seconds, independent of the size of the database. The forward recovery time also increases depending on when the restore and recovery are done, but due to the higher frequency of backups (every 6 hours in this example), the forward recovery time is 43 minutes at most. In this example, the maximum RTO is 1 hour and 13 minutes.

The following figure shows an RTO comparison of file-based and storage-based Snapshot backups for different database sizes and different frequencies of Snapshot backups. The green bar shows the file-based backup. The other bars show Snapshot copy backups with different backup frequencies.

With a single Snapshot copy data backup per day, the RTO is already reduced by 40% when compared to a file-based data backup. The reduction increases to 70% when four Snapshot backups are taken per day. The figure also shows that the curve goes flat if you increase the Snapshot backup frequency to more than four to six Snapshot backups per day. Our customers, therefore, typically configure four to six Snapshot backups per day.
This graph shows the HANA server RAM size. The database size in memory is calculated to be half of the server RAM size.

The restore and recovery time is calculated based on the following assumptions: the database can be restored at 250MBps; the number of log files per day is 50% of the database size (for example, a 1TB database creates 500MB of log files per day); and a recovery can be performed at 100MBps.

Next: SnapCenter Service architecture.

**SnapCenter Service architecture**

Previous: The NetApp solution.

SnapCenter Service is a unified, scalable platform for application-consistent data protection. SnapCenter Service provides centralized control and oversight, while delegating the ability for users to manage application-specific backup and restore operations.

SnapCenter Service leverages the NetApp Cloud Manager software as a UI and for managing credentials for Azure NetApp Files. The SnapCenter services run within a Kubernetes cluster and communicate with the NetApp Cloud Manager through the Cloud Manager Connector. SnapCenter Service triggers HANA database operations by using the HANA hdbsql client and the Azure NetApp Files storage operation by using the Azure NetApp Files management APIs.

You can deploy the SnapCenter Service Kubernetes cluster and the Cloud Manager Connector in a separate service vNet or in the same vNet as the SAP HANA systems, as shown in the following two figures.
SnapCenter Service installation requires a minimum of two virtual machines (VMs), one VM for the Cloud Manager Connector and another VM running the Kubernetes cluster in a non-HA configuration. An additional two VMs are required when SnapCenter Service is set up in a high availability (HA) configuration.
SnapCenter Service SAP HANA backup solution

Solution components

The SnapCenter Service backup solution for SAP HANA covers the following areas:

- SAP HANA data backup with storage-based Snapshot copies:
  - Backup scheduling
  - On-demand backups
  - Retention management
  - Housekeeping of the SAP HANA backup catalog
  - Restore operation

- Non-data volume backup with storage-based Snapshot copies
  - SnapCenter differentiates between non-data volumes belonging to a specific HANA system, for example, the HANA shared volume, and global non-data volumes, which do not belong to a specific HANA system, for example, the SAP transport directory.
  - Backup scheduling
  - On-demand backups
  - Retention management
  - Restore operation

- File-based backup for database block integrity checks or backup to a second location:
  - Backup scheduling
  - On-demand backups
Retention management
- Housekeeping of the SAP HANA backup catalog

Retention management of HANA database log backup:
- Retention management based on data backup retention
- Housekeeping of the SAP HANA backup catalog

Snapshot data backups are executed with SnapCenter Service by triggering the SAP HANA database backup savepoint so that the Snapshot copy, which is created on the storage layer, is based on a consistent image of the SAP HANA database.

To enable a complete backup of all SAP HANA-related resources, SnapCenter Service also enables you to back up all non-data volumes with storage-based Snapshot copies. You can schedule non-data volumes independently from the database data backup to enable individual retention and protection policies.

SAP recommends combining storage-based Snapshot backups with a weekly file-based backup to execute a block integrity check. You can execute the block integrity check from within SnapCenter. Block integrity check (file-based) backups are also used to offload backups to a second storage location.

Based on your configurable retention policies, SnapCenter Service manages the housekeeping of data backups, log backups, and the SAP HANA backup catalog.

The following figure summarizes the backup solution.

When executing a storage-based Snapshot backup of non-data volumes, SnapCenter Service performs the following tasks:

1. Creates a storage Snapshot copy of the non-data volume.
2. Deletes storage Snapshot copies based on the defined retention policy.

When executing a storage-based Snapshot backup of the SAP HANA database, SnapCenter Service performs the following tasks:

1. Creates an SAP HANA backup savepoint to create a consistent image on the persistence layer.
2. Creates a storage Snapshot copy of the data volume.
3. Registers the storage Snapshot backup in the SAP HANA backup catalog.
4. Releases the SAP HANA backup savepoint.
5. Deletes storage Snapshot copies based on the defined retention policy.
6. Deletes SAP HANA backup catalog entries based on the defined retention policy.
7. Whenever a data backup has been deleted manually or based on the retention policy, SnapCenter Service deletes all log backups that are older than the oldest data backup. Log backups are deleted on the file system and in the SAP HANA backup catalog.

**Supported SAP HANA releases and configurations**

SnapCenter Service supports SAP HANA single-host and multiple-host configurations attached to Azure NetApp Files volumes.

SnapCenter Service supports the following SAP HANA architectures and releases:

- SAP HANA single container:
  - SAP HANA 1.0 SPS12
- SAP HANA multitenant-database container (MDC) with single or multiple tenants:
  - SAP HANA 2.0 SPS4 and later

Snapshot backup support for MDC systems has been introduced by SAP with HANA 2.0 SP1 for single tenant systems and with HANA 2.0 SPS4 for multiple tenant systems.

The combination of data Snapshot backups with SnapCenter Service and log backups with a backint solution is not supported. Log backups must be configured to be written to a file system.

**SnapCenter Service concepts and best practices**

**Data protection strategy**

Before configuring SnapCenter Service, you must define the data protection strategy based on the RTO and RPO requirements of the various SAP systems.

A common approach is to define system types such as production, development, test, or sandbox systems. All SAP systems of the same system type typically have the same data protection parameters.

You must define the following parameters:

- How often a Snapshot backup is executed
- How long a Snapshot backup is kept
- How often a block integrity check (file-based backups) is executed
- How long a block integrity check backup (file-based backup) is kept?

The following table shows an example of data protection parameters for the system type’s production, development, and test. For the production system, a high backup frequency has been defined, and weekly file-
based backups are executed. The test and the development systems have lower requirements and Snapshot backups are scheduled less often.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Production systems</th>
<th>Development systems</th>
<th>Test systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshot backup frequency</td>
<td>Every 4 hours</td>
<td>Every 6 hours</td>
<td>Every 12 hours</td>
</tr>
<tr>
<td>Snapshot backup retention</td>
<td>3 days</td>
<td>3 days</td>
<td>3 days</td>
</tr>
<tr>
<td>Block integrity check</td>
<td>Once per week</td>
<td>Once per week</td>
<td>Once per week</td>
</tr>
<tr>
<td>Block integrity check</td>
<td>4 weeks</td>
<td>2 weeks</td>
<td>1 week</td>
</tr>
</tbody>
</table>

The following table shows the policies that must be configured for the data protection parameters for Snapshot backup operations.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Policy SnapshotEvery4h</th>
<th>Policy SnapshotEvery6h</th>
<th>Policy SnapshotEvery12h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup type</td>
<td>Snapshot copy based</td>
<td>Snapshot copy based</td>
<td>Snapshot copy based</td>
</tr>
<tr>
<td>Schedule type</td>
<td>Hourly</td>
<td>Hourly</td>
<td>Hourly</td>
</tr>
<tr>
<td>Retention</td>
<td>Count = 18</td>
<td>Count = 12</td>
<td>Count = 3</td>
</tr>
<tr>
<td>Backup schedule</td>
<td>Every 4 hours</td>
<td>Every 6 hours</td>
<td>Every 12 hours</td>
</tr>
</tbody>
</table>

The following table shows the policies that must be configured for the data protection parameters for file-based backup operations.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Policy FileBased4Week</th>
<th>Policy FileBased2Weeks</th>
<th>Policy FileBased1Week</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup type</td>
<td>File based</td>
<td>File based</td>
<td>File based</td>
</tr>
<tr>
<td>Schedule type</td>
<td>Weekly</td>
<td>Weekly</td>
<td>Weekly</td>
</tr>
<tr>
<td>Retention</td>
<td>Count = 4</td>
<td>Count = 2</td>
<td>Count = 1</td>
</tr>
<tr>
<td>Backup schedule</td>
<td>Every Sunday</td>
<td>Every Sunday</td>
<td>Every Sunday</td>
</tr>
</tbody>
</table>

**SnapCenter Service policies**

In SnapCenter Service a single protection policy includes the following parameters:

- Backup type
  - Snapshot-based
  - File-based
- Schedule and retention
  - Schedules: Hourly, Daily, Weekly, Monthly. A single policy can have multiple schedules.
  - For each schedule, a start or end time and the frequency is configured.
  - For each schedule, a retention is configured. Retention can be time based, or counter based.
The following figure shows a screenshot of the policy configuration.

Backup operations

SAP introduced the support of Snapshot backups for MDC multiple tenant systems with HANA 2.0 SPS4. In an SAP HANA MDC system, the tenant configuration is not necessarily static. You can add or delete tenants. SnapCenter Service cannot rely on the configuration that is discovered when the HANA database is added to SnapCenter. SnapCenter Service must know which tenants are available at the point in time the backup operation is executed.

Therefore, with each backup operation, the first step in the workflow is to get the tenant information. The next step is the Snapshot backup operation itself. This step includes the SQL command to trigger the HANA backup savepoint, the Azure NetApp Files Snapshot backup, and the SQL command to close the HANA backup savepoint. By using the close command, the HANA database updates the backup catalog of the system database and each tenant.

SAP does not support Snapshot backup operations for MDC systems when one or more tenants are stopped.

For the retention management of data backups and the HANA backup catalog management, SnapCenter Service must execute the catalog delete operations for the system database and all tenant databases that were identified in the first step. In the same way for the log backups, the SnapCenter Service workflow must operate on each tenant that was part of the backup operation.

The following figure shows an overview of the backup workflow.
Backup workflow for Snapshot backups of the HANA database

SnapCenter Service executes the backup of the SAP HANA database in the following sequence:

1. Reads the list of tenants from the HANA database.
2. Stores tenant information in the SnapCenter Service metadata for the backup operation.
3. Triggers an SAP HANA global synchronized backup savepoint to create a consistent database image on the persistence layer.
   
   For an SAP HANA MDC single or multiple tenant system, a synchronized global backup savepoint for the system database and for each tenant database is created.

4. Creates Azure NetApp Files Snapshot copies for all data volumes configured for the HANA system. In our example of a single-host HANA database, there is only one data volume. With an SAP HANA multiple-host database, there are multiple data volumes.

5. Registers the Azure NetApp Files Snapshot backup in the SAP HANA backup catalog.

6. Deletes the SAP HANA backup savepoint.

7. Deletes the Azure NetApp Files Snapshot copies and the backup entries in its database as well as in the SAP HANA backup catalog based on the retention policy defined for backups. HANA backup catalog operations are done for the system database and all tenants.

8. Deletes all log backups on the file system and in the SAP HANA backup catalog that are older than the oldest data backup identified in the SAP HANA backup catalog. These operations are done for the system database and all tenants.

Backup workflow for block integrity check operations

SnapCenter Service executes the block integrity check in the following sequence:

1. Reads the list of tenants from the HANA database.
2. Triggers a file-based backup operation for the system database and each tenant.
3. Deletes file-based backups in its database, on the file system, and in the SAP HANA backup catalog based on the retention policy defined for block integrity check operations. Backup deletion on the file system and HANA backup catalog operations are done for the system database and all tenants.

4. Deletes all log backups on the file system and in the SAP HANA backup catalog that are older than the oldest data backup identified in the SAP HANA backup catalog. These operations are done for the system database and all tenants.

Backup retention management and housekeeping of data and log backups

The data backup retention management and log backup housekeeping can be divided into four main areas, including retention management of the following:

- Snapshot backups
- File-based backups
- Data backups in the SAP HANA backup catalog
- Log backups in the SAP HANA backup catalog and the file system

The following figure provides an overview of the different workflows and the dependencies of each operation. The following sections describe the different operations in detail.

RetentionPolicy of Snapshot backups

SnapCenter Service handles the housekeeping of SAP HANA database backups and non-data volume backups by deleting Snapshot copies on the storage and in the SnapCenter Service repository according to a retention defined in the SnapCenter Service backup policy.

Retention management logic is executed with each backup workflow in SnapCenter.

You can also delete Snapshot backups manually in SnapCenter.

Retention management of file-based backups

SnapCenter Service handles the housekeeping of file-based backups by deleting the backups on the file system according to a retention defined in the SnapCenter Service backup policy.
Retention management logic is executed with each backup workflow in SnapCenter.

**Retention management of data backups within the SAP HANA backup catalog**

When SnapCenter Service deletes any backup (Snapshot or file-based), this data backup is also deleted in the SAP HANA backup catalog.

**Retention management of log backups**

The SAP HANA database automatically creates log backups. These log backup runs create backup files for each individual SAP HANA service in a backup directory configured in SAP HANA.

Log backups older than the latest data backup are no longer required for forward recovery and can be deleted.

SnapCenter Service handles the housekeeping of log file backups on the file system level as well as in the SAP HANA backup catalog by executing the following tasks:

1. Reads the SAP HANA backup catalog to get the backup ID of the oldest successful file-based or Snapshot backup.
2. Deletes all log backups in the SAP HANA catalog and the file system that are older than this backup ID.

SnapCenter Service only handles housekeeping for backups that have been created by SnapCenter. If additional file-based backups are created outside of SnapCenter, you must make sure that the file-based backups are deleted from the backup catalog. If such a data backup is not deleted manually from the backup catalog, it can become the oldest data backup, and older log backups are not deleted until this file-based backup is deleted.

You cannot switch off log backup retention management with the current release of SnapCenter Service.

**Capacity requirements for Snapshot backups**

You must consider the higher block change rate on the storage layer relative to the change rate with traditional databases. Due to the HANA table merge process of the column store, the complete table is written to disk, not just the changed blocks. Data from our customer base shows a daily change rate between 20% and 50% if multiple Snapshot backups are taken during the day.

Next: Lab setup used for this report.

**Lab setup used for this report**

Previous: SnapCenter Service concepts and best practices.

The lab setup used for this report includes the SAP HANA system PR1-SAP HANA single host MDC single tenant system, and the SnapCenter Service components, as shown in the following figure.
As discussed in the section “Data protection strategy,” policies are usually configured independently of the resource and can be used by multiple SAP HANA databases.

A typical minimum configuration consists of the following policies:

- Policy for hourly Snapshot backups.
  
  For example, **SnapshotEvery4h**

- Policy for weekly block integrity check using a file-based backup.

  For example, **BlockIntegrityCheckEverySunday**

The following sections describe the configuration of these two policies.

**Policy for hourly Snapshot backups**

To create a policy for hourly Snapshot backups, follow these steps:

1. Go to Policies and click Add Policy.
2. In the Create Policy screen provide a policy name, backup type, backup naming convention, and schedule and retention details.

For example, in the following figure, for the Snapshot backup, a schedule of every 4 hours and a start time of 10AM is configured. The retention is configured with 18, which is 3 days.
3. In the Custom Backup Name window, you can change the backup naming convention and add a custom prefix.

4. To create the new policy, click Add.
Policy for weekly block integrity check

To create a policy for a weekly block integrity check, follow these steps:

1. Go to Policies and click Add Policy.

2. In the Create Policy screen, provide a policy name, backup type, backup naming convention, and as schedule and retention details.

3. To create the new policy, click Add.

The following figure shows a summary of the configured policies.
SnapCenter Service Snapshot backup configuration overview

SnapCenter Service supports two different Snapshot backup operation types:

- **SAP HANA data backups by using Snapshot operations.**
  
  Backup of the SAP HANA database data volume combining HANA SQL statements for database consistency and backup catalog management with Azure NetApp Files Snapshot operations.

- **Backup of volumes with unstructured data by using Snapshot backup operations.**
  
  Backup of binaries, configuration files, and so on, which do not require any interaction with the HANA database. The backup is executed with an Azure NetApp Files Snapshot backup operation. In SnapCenter Service, two sub-types are used to define whether these volumes belong to a specific HANA system or whether it is a global shared volume used by multiple HANA systems.

  - **Backup of non-data volumes of an SAP HANA database**
    
    Backup of a volume that is associated with a specific HANA system, for example, the HANA shared volume.

  - **Backup of global non-data volumes**
    
    Backup of a volume that is not associated with a specific HANA system, for example, the SAP transport
directory.

In the following sections, the configuration of the three different backup types is described.

Next: Backup configuration of SAP HANA database backups.

Backup configuration of SAP HANA database backups

Previous: SnapCenter Service Snapshot backup configuration overview.

This section describes the configuration steps for a single host SAP HANA MDC single-tenant system PR1. The steps are identical for an MDC system with multiple tenants. The differences for a single-container or a multiple-host system are reflected in the corresponding configuration steps.

SAP HANA backup user

NetApp recommends configuring a dedicated database user in the HANA database to run the backup operations with SnapCenter Service. During the HANA system configuration in SnapCenter Service, an HANA database user store key is configured for this backup user, and this user store key is used to communicate with the HANA system.

The following figure shows a screenshot of SAP HANA Studio through which you can create the backup user.

The required privileges changed in the SAP HANA 2.0 SPS5 release: backup admin, catalog read, database backup admin, and database recovery operator is required. For earlier releases, backup admin and catalog read are sufficient.

For an SAP HANA MDC system, with single or multiple tenants, you must create the user in the system database because all backup commands for the system and the tenant databases are executed by using the system database.
SAP HANA system configuration in SnapCenter Service

To configure the SAP HANA system PR1 in SnapCenter Service, follow these steps:

1. Go to SAP HANA Systems and click Add.
2. In the System Details screen, select the system type, HANA Single Container, or Multitenant Database Container. Provide the SID of the HANA system and enter any text of your choosing as a system name.
3. To add a HANA database user store key, Click Add Keys.
4. Enter the information for configuring the user store key for the HANA database. You can provide any name as the key name.

The system details include the IP address and the port to communicate with the system database using the hdbsql client. In an SAP HANA MDC single-tenant setup, port 3<instanceNo>13 is the standard port for SQL access to the system database. For an SAP HANA single-container setup, port 3<instanceNo>15 is the standard port for SQL access to the index server and must be used in the configuration. For an SAP HANA multiple-host setup, you must configure user store keys for all hosts. SnapCenter Service tries to connect to the database by using each of the provided keys and can therefore operate independently of a failover of an SAP HANA service to a different host.

You must provide the username and password for the database user in the system database that was previously configured. SnapCenter automatically creates a user store key by using this information and uses the key to communicate with the HANA database.

5. To continue, click Add.
6. To proceed to the storage footprint configuration, click Continue.

7. Enter the information for the storage volumes of the HANA system.

   Select the working environment and the NetApp account that is used for the Azure NetApp Files volumes of the HANA system. Select the data volume of your HANA system, for example, PR1_data_mnt00001.
For an SAP HANA multiple-host system, you must select the data volumes of all HANA hosts belonging to the system.

8. Click Continue.
9. To add the HANA system, click Add.

10. To continue with the protection configuration, click Proceed.
The screen displays all the policies that have been configured in SnapCenter Service.

11. Select the policies that you want to assign. For example, the policies `SnapshotEvery4h` and `BlockIntegrityCheckEverySunday` that were previously created are selected.

12. To assign the policies to the HANA system, click Protect.
The HANA systems overview screen shows the HANA system and the assigned policies.

Next: Backup configuration of SAP HANA non-data volumes.
Backup configuration of SAP HANA non-data volumes

The backup of non-data volumes is an integrated part of the SnapCenter Service. Protecting the database data volume is sufficient to restore and recover the SAP HANA database to a given point in time provided that the database installation resources and the required logs are still available.

To recover from situations where other non-data files must be restored, NetApp recommends developing an additional backup strategy for these volumes to augment the SAP HANA database backup. Depending on your specific requirements, the backup of non-data volumes might differ in scheduling frequency and retention settings, and you should consider how frequently files are changed. For instance, the HANA volume `/hana/shared` contains executables but also SAP HANA trace files. Although executables only change when the SAP HANA database is upgraded, the SAP HANA trace files might need a higher backup frequency to support analyzing problem situations with SAP HANA.

A SnapCenter Service non-data volume backup enables Snapshot copies of all relevant volumes to be created in a few seconds with the same space efficiency as SAP HANA database backups. The difference is that there is no SQL communication with the SAP HANA database required.

The following steps show how to protect the HANA shared volume of the SAP HANA database PR1.

1. In the SAP HANA Systems view, select Add Non-Data Volumes in the context menu on the right of the screen.

2. Click Add Storage.
3. Select the HANA shared volume and click Add Storage.
4. To add the non-data volume, click Add.

The SAP HANA Systems overview now shows a second icon in the protection column, which indicates that a non-data volume was added to the HANA system.
5. In the context menu on the right, select Protect > Non-Data Volumes.

6. Assign a policy to the non-data volume. In the following example, the `SnapshotEvery4h` policy is assigned to the HANA shared volume.
Backup configuration of global non-data volumes

To set the backup configuration of global non-data volumes, follow these steps:

1. Go to SAP HANA Systems and click Add.
2. In the System Details screen, select the system type, Global Non-Data Volume. You can provide a comma-separated list of SIDs, which are associated with the global volume. Enter a system name of your choosing and click Continue.
3. Select the volume and click Continue.

4. Click Continue.
5. Click Add.

6. To configure the protection, click Proceed.
7. Select the policy and click Protect.

8. Transport Directory now displays in the list of HANA systems as a global non-data volume.
With SnapCenter Service, database backups are typically executed by using the schedules defined within the policies. You can also perform on-demand database backups by using either the SnapCenter Service UI or REST APIs.

**Identify SnapCenter Service data backups in SAP HANA Studio**

In the context menu of the SAP HANA Systems view, select View Backups to open the backup overview.
The backup overview shows a list of backups created by using SnapCenter Service. The following figure shows the backups available and highlights the most recent backup.

When performing a backup by using storage Snapshot copies for an SAP HANA MDC system, a Snapshot copy of the data volume is created. This data volume contains the data of the system database as well as the data of all tenant databases. To reflect this physical architecture, SAP HANA internally performs a combined backup of the system database and all tenant databases whenever SnapCenter Service triggers a Snapshot backup. This results in multiple separate backup entries in the SAP HANA backup catalog: one for the system database and one for each tenant database.
For SAP HANA single-container systems, the database volume contains only the single database, and there is only one entry in SAP HANA’s backup catalog.

In the SAP HANA backup catalog, the SnapCenter Service backup name is stored in the Comment field and the External Backup ID (EBID) field. The following figures show the system database and the tenant database PR1. Both figures highlight the SnapCenter Service backup name stored in the Comment field and EBID field.
SnapCenter Service is only aware of its own backups. Additional backups created, for example, with SAP HANA Studio, are visible in the SAP HANA catalog but not in SnapCenter Service.

Identify SnapCenter Service backups on the Azure NetApp Files volume

The same name, which is used as backup name in SnapCenter Service, is also used as the Snapshot backup name on the Azure NetApp Files volume. The following figure shows the Azure portal and the Snapshot backups for the database data volume.

List non-data volume backups

In the backup view of the HANA system, select Non-Data Volumes to display the list of backups for the non-data volume, as shown in the following figure.
On the Azure NetApp Files volume for HANA shared, the Snapshot copies have the same name as in SnapCenter Service.

On-demand database backup

To create an on-demand database backup, follow these steps:

1. In the SAP HANA Systems view, select On-Demand Backup in the context menu. You also can select either Data Volume or Non-Data Volume. For the database backup, you must select Data Volume.
2. In the On-Demand Backup dialog, select either Policy: None, or one of the policies that you have assigned to the HANA system.

If you select policy None, you can define a specific retention that must be used for this specific backup. If you select a policy, which is assigned to the HANA system, the same retention is applied to this backup as for the scheduled backups using this policy.

In the following example, the existing policy is selected.
3. To start the backup workflow, click Create Backup.

A screen displays the job ID of the backup operation.

4. To open the job detail screen, click the job ID.
Job Monitor displays the different workflow steps, the runtime of the steps, and the total operation runtime. In the following example, the backup operation takes 19 seconds.

Next: File-based backups and block integrity check.
File-based backups and block integrity check

Previous: SAP HANA database Snapshot backups.

SAP recommends combining storage-based snapshot backups with a weekly file-based backup to execute a block integrity check. SnapCenter Service supports the execution of a block integrity check by using a policy in which file-based backup is selected as the backup type.

File-based backups are also used to have secondary backup copies in addition to the snapshot backups on the HANA data volume. You can use these file-based backups for restore and recovery operations in case of a complete loss of the primary data volume.

When scheduling backups using this policy, SnapCenter Service creates a standard SAP HANA file backup for the system and all tenant databases.

SnapCenter Service does not display the file-based backups in the same manner as snapshot-based backups. Instead, only the last file-based backup is listed. Success or failure of file-based backups are visible in the Job Monitor view.

The SAP HANA backup catalog shows entries for both the system and the tenant databases. The following figure shows a SnapCenter Service block integrity check in the backup catalog of the system database.
A successful block integrity check creates standard SAP HANA data backup files. SnapCenter Service uses the backup path that has been configured in the HANA database for file-based data backup operations.
vm-pr1:/hanabackup/PR1/file # ls -al *

DB_PR1:
total 1743736
drwxr-xr-- 2 pr1adm sapsys 4096 Jun 6 05:12 .
drwxr-x--- 4 pr1adm sapsys 4096 Jan 31 18:59 ..
-rw-r----- 1 pr1adm sapsys 155648 Jun 6 05:00
SnapCenter_SCS_PR1_BlockIntegrityCheckEverySunday_Weekly_2021_06_06_05_00_00_databackup_0_1
-rw-r----- 1 pr1adm sapsys 83894272 Jun 6 05:01
SnapCenter_SCS_PR1_BlockIntegrityCheckEverySunday_Weekly_2021_06_06_05_00_00_databackup_2_1
-rw-r----- 1 pr1adm sapsys 1694507008 Jun 6 05:02
SnapCenter_SCS_PR1_BlockIntegrityCheckEverySunday_Weekly_2021_06_06_05_00_00_databackup_3_1

SYSTEMDB:
total 1562788
drwxr-xr-- 2 pr1adm sapsys 4096 Jun 6 05:12 .
drwxr-x--- 4 pr1adm sapsys 4096 Jan 31 18:59 ..
-rw-r----- 1 pr1adm sapsys 159744 Jun 6 05:00
SnapCenter_SCS_PR1_BlockIntegrityCheckEverySunday_Weekly_2021_06_06_05_00_00_databackup_0_1
-rw-r----- 1 pr1adm sapsys 1593843712 Jun 6 05:02
SnapCenter_SCS_PR1_BlockIntegrityCheckEverySunday_Weekly_2021_06_06_05_00_00_databackup_1_1

---

**Restore and recovery using file-based backups**

You must do a restore and recovery operation of a file-based backup outside of SnapCenter by using the standard HANA recovery operations with HANA Studio or HANA Cockpit.

Next: Restore and recovery.

**Restore and recovery**

Previous: File-based backups and block integrity check.

The following section describes the restore and recovery workflows for a HANA MDC single-host, single tenant system. The differences for a multiple host system are described.

The examples show SAP HANA Studio as a tool to execute manual recovery. You can also use SAP HANA Cockpit or HANA SQL statements for the recovery operations.

To restore and recover an SAP HANA MDC single-tenant system using SAP HANA Studio and SnapCenter Service, complete the following steps:

1. Prepare the restore and recovery process with SAP HANA Studio:
   a. Select Recover System Database and confirm the shutdown of the SAP HANA system.
b. Select the recovery type and the log backup location.
   
   The list of data backups displays.
   
   c. Select the relevant backup to see the external backup ID.

2. Unmount the HANA data volumes.

3. Perform the restore process with SnapCenter Service:
   
   a. In the Backup view, select the backup that matches the external backup ID or comment field from SAP
      HANA Studio.
   
   b. To start the restore operation, select Restore in the context menu.

4. Mount the HANA data volumes.

5. Run the recovery process for the system database with SAP HANA Studio:
   
   a. Click Refresh from the backup list and select the available backup for recovery (indicated with a green
      icon).
   
   b. Start the recovery operation.
       
       After the recovery operation is finished, the system database is started.

6. Run the recovery process for the tenant database with SAP HANA Studio:
   
   a. Select Recover Tenant Database and select the tenant to be recovered.
   
   b. Select the recovery type and the log backup location.
       
       A list of data backups displays. Because the data volume has already been restored, the tenant backup
       indicates as available (in green).
   
   c. Select the backup and start the recovery process. After the recovery process is finished, the tenant
       database is started automatically.

The following steps describe the restore and recovery operations of HANA system PR1:

1. To start the recovery of the system database, in SAP HANA Studio, go to Backup and Recovery Recover
   System Database option.
2. Select the recovery type and click Next.
3. Provide the location of the backup catalog and click Next.
4. A list of available backups is displayed based on the content of the HANA backup catalog. Choose the required backup and note the external backup ID, for example, as shown in the following screenshot, the most recent backup.
5. Unmount all data volumes.

```bash
umount /hana/data/PR1/mnt00001
```

For an SAP HANA multiple host system, you must unmount all the data volumes on each host.

6. From the SnapCenter Service UI, select View Backups in the context menu of the SAP HANA Systems view.

7. To start the restore operation, in the Backup view, select the most recent backup, which also shows in HANA Studio, and select Restore in the context menu.
8. To confirm the restore operation, click Yes, Restore.

The SnapCenter Service job log shows the progress of the restore operation.
9. Wait until the restore process completes. On each database host, mount all the data volumes. In the following example, you must remount only one volume on the database host:

`mount /hana/data/SP1/mnt00001`

10. To update the list of available backups, go to SAP HANA Studio and click Refresh. The backup that was restored with SnapCenter Service is shown with a green icon in the list of backups. Select the backup and click Next.
11. Provide the location of the log backups. Click Next.
12. Select other settings as required. Make sure Use Delta Backups is not selected. Click Next.
13. Review the recovery settings and click Finish.
The recovery process starts. Wait until the recovery of the system database completes.
14. In SAP HANA Studio, select the entry for the system database and go to Backup and Recovery Recover Tenant Database.
15. Select the tenant to recover and click Next.
16. Specify the recovery type and click Next.
17. Confirm the backup catalog location and click Next.
18. Confirm that the tenant database is offline. Click OK to continue.

Because the restore of the data volume has occurred before the recovery of the system database, the tenant backup is immediately available.
19. Select the backup highlighted in green and click Next.

20. Confirm the log backup location and click Next.
21. Select other settings as required. Make sure Use Delta Backups is not selected. Click Next.
22. Review the recovery settings and start the recovery process of the tenant database by clicking Finish.
23. Wait until the recovery has finished and the tenant database is started.
The SAP HANA system is up and running.

For an SAP HANA MDC system with multiple tenants, you must repeat steps 15 to 24 for each tenant.

Next: Where to find additional information.

Where to find additional information

Previous: Restore and recovery.

To learn more about the information that is described in this document, review the following documents and/or websites:


Next: Version history.

Version history

Previous: Additional information.
<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Document version history</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>October 2021</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>