Abstract

This document describes the installation and configuration of the NetApp® backup and recovery solution for SAP HANA. The solution is based on NetApp SnapCenter® and the SnapCenter plug-in for SAP HANA. Backup, restore, and recovery workflows are also covered in the document.
# TABLE OF CONTENTS

1 **Overview** ................................................................................................................................................ 5  
1.1 The NetApp Solution ....................................................................................................................................... 5  
1.2 Runtime of Snapshot Backups ........................................................................................................................ 7  
1.3 Recovery Time Objective Comparison ............................................................................................................ 8  

2 **SnapCenter Architecture** ................................................................................................................... 11  
2.1 SnapCenter Overview ................................................................................................................................... 11  
2.2 SnapCenter Features .................................................................................................................................... 11  
2.3 SnapCenter Components .............................................................................................................................. 11  

3 **SnapCenter SAP HANA Backup Solution** ........................................................................................ 12  
3.1 Solution Components .................................................................................................................................... 12  
3.2 Supported SAP HANA Releases and Configurations ................................................................................... 14  
3.3 Capacity Requirements for Snapshot Backups ............................................................................................. 14  
3.4 SnapCenter 4.0 Enhancements .................................................................................................................... 14  

4 **SnapCenter Installation and Configuration Overview** ........................................................................... 15  
4.1 SnapCenter Installation ................................................................................................................................. 15  
4.2 Deployment Options for the SAP HANA Plug-In ........................................................................................... 15  
4.3 Configuration Steps ...................................................................................................................................... 18  
4.4 Data Protection Strategy ............................................................................................................................... 20  
4.5 Backup Retention Management and Housekeeping of Log Backups ........................................................... 21  

5 **Lab Setup** ............................................................................................................................................ 23  

6 **SnapCenter Initial Configuration** ............................................................................................................ 24  
6.1 Storage System Configuration ...................................................................................................................... 24  
6.2 Run As Credentials Configuration ................................................................................................................. 27  
6.3 Host Configuration and SAP HANA Plug-In Installation ........................................................................ 29  
6.4 SAP HANA hdbsql Client Software Installation and Configuration ......................................................... 31  
6.5 Policy Configuration ...................................................................................................................................... 31  

7 **SnapCenter Resource-Specific Configuration for SAP HANA Database Backups** .............................. 38  
7.1 SAP HANA Backup User and Hdbuserstore Configuration ....................................................................... 38  
7.2 Configuration of Data Protection to Off-Site Backup Storage ..................................................................... 40  
7.3 Resource Configuration ............................................................................................................................... 42  
7.4 Resource Protection Configuration ............................................................................................................. 47  
7.5 Additional Configuration Steps for XFS Environments ............................................................................. 51
8 SnapCenter Resource-Specific Configuration for Nondata Volume Backups ............................................ 52
  8.1 Configuration of Nondata Volume Resources ............................................................................................ 52
  8.2 Data Protection for Nondata Volume Resources ........................................................................................ 54
  8.3 Using SnapCenter Together with SAP Landscape Management .......................................................... 55

9 Database Backups ..................................................................................................................................... 56
  9.1 Backup Workflow for On-Demand and Scheduled Backups .................................................................... 56
  9.2 On-Demand Database Backup at Primary Storage ...................................................................................... 56
  9.3 On-Demand Database Backups with SnapVault Replication ...................................................................... 59
  9.4 Identifying SnapCenter Backups in SAP HANA Studio ............................................................................ 62
  9.5 Identifying SnapCenter Backups on the Storage Systems .......................................................................... 64

10 Block Integrity Check.................................................................................................................................. 66

11 Restore and Recovery .................................................................................................................................. 67
  11.1 Restore and Recovery Workflow Overview ............................................................................................... 68
  11.2 Restore and Recovery from Primary Storage Using Volume-Based Restore ............................................ 68
  11.3 Restore and Recovery from Primary Storage Using File-Level Restore .................................................... 82
  11.4 Restore and Recovery from Off-Site Backup Storage .................................................................................. 84

12 Using Job Monitor for Troubleshooting .................................................................................................... 85

13 Advanced Configuration and Tuning .......................................................................................................... 88
  13.1 Deactivating Automated Log Backup Housekeeping ............................................................................. 88
  13.2 Disable Warning When Running SAP HANA Plug-In on a Virtual Environment ...................................... 89
  13.3 Change Scheduling Frequency of Backup Synchronization with Off-Site Backup Storage .................... 90

Where to Find Additional Information ....................................................................................................... 93

Version History ............................................................................................................................................... 93

LIST OF TABLES
Table 1) Summary of SAP HANA plug-in deployment options .............................................................................. 18
Table 2) Data protection parameters .................................................................................................................. 20
Table 3) Policies based on data protection parameters ..................................................................................... 20

LIST OF FIGURES
Figure 1) Backup solution overview ................................................................................................................ 6
Figure 2) Customer example of Snapshot backup runtime .................................................................................. 7
Figure 3) Backup runtime analysis .................................................................................................................... 8
Figure 4) RTO for a 2TB database with file-based backups ............................................................................. 9
Figure 5) RTO for a 2TB database with Snapshot backups ............................................................................... 10
1 Overview

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 more tape drives, additional backup disk space, and faster backup networks. You must also cover the ongoing expense of storing and managing these tape 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.

1.1 The NetApp Solution

NetApp Snapshot™ technology can be used to create database backups in minutes. 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 because the NetApp Snapshot technology does not move or copy data blocks when the Snapshot copy is created or when data in the active file system is changed. Therefore, the creation of Snapshot copies can be scheduled without considering peak dialog or batch activity periods. SAP and NetApp 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. NetApp SnapRestore® data recovery software enables the restore of an entire database or, alternatively, a portion of a database to any point in time, based on the available Snapshot copies. Such restore processes are finished in a few minutes, 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 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 mean time to recover, which is the time needed for restore and recovery operations, is reduced to several minutes rather than the several hours required for conventional single-cycle tape 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 SnapRestore on the primary storage system. Restores from a secondary location are only necessary if the primary storage system containing the Snapshot copies is damaged. The secondary location can also be used if it is necessary to restore a backup that is no longer available from a Snapshot copy: a month-end backup, for example.

A backup to a secondary location is based on Snapshot copies created on the primary storage. Therefore, the data is read directly from the primary storage system without generating load on the SAP database server. The primary storage communicates directly with the secondary storage and sends the backup data to the destination by using a NetApp SnapVault® disk-to-disk backup.

SnapVault offers significant advantages when compared to traditional backups. After an initial data transfer, in which all data has been transferred from the source to the destination, all subsequent backups copy only the changed blocks to the secondary storage. Therefore, the load on the primary storage system and the time needed for a full backup are significantly reduced. Because SnapVault stores only the changed blocks at the destination, a full database backup requires less disk space.

Backing up data to tape as a long-term backup might still be required. This backup could be, for example, a weekly backup that is kept for a year. In this case, the tape infrastructure can be directly connected to the secondary storage, and data can be written to tape by using the Network Data Management Protocol (NDMP). Figure 1 shows an overview of the backup solution.

Customers who want to avoid investing in an expensive tape infrastructure to fulfill their long-term backup requirements can directly integrate cloud technology to offload the long-term backups to the cloud. This option is not only a very price-competitive alternative but also highly secure and easy to implement. Figure 1 illustrates this option using a NetApp AltaVault™ appliance to transfer the Snapshot copies from the secondary site encrypted, efficiently compressed, and securely stored to cloud storage of your choice. Customers who don’t want to use external cloud storage for archiving can use private object storage such as NetApp StorageGRID® installed in their own data center.

Figure 1) Backup solution overview.
Customers who want to protect their systems from a complete failure of the primary data center can use NetApp SnapMirror® technology together with SnapCenter to complete the data protection strategy described with a disaster recovery data center. Details about how to use SnapCenter for this task are described in TR-4646: SAP HANA Disaster Recovery with Asynchronous Storage Replication.

1.2 Runtime of Snapshot Backups

Figure 2 shows a screenshot of a customer’s HANA Studio running SAP HANA on NetApp storage. The customer is using NetApp Snapshot to back up the HANA database. The screenshot shows that the HANA database (approximately 620GB in size) is backed up in 11 seconds by using Snapshot backup technology.

Figure 2) Customer example of Snapshot backup runtime.

Further analysis of more than 11,000 backup runs demonstrated that more than 80% of the backups were finished in less than 20 seconds. All the backups were finished in less than a minute.
1.3 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. 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 the restore can be performed from primary storage. A restore from secondary storage 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.

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 would be, in the worst case, one-fourth of the recovery time for a file-based backup (6 hours / 24 hours = ¼).

Figure 4 shows an RTO example for a 2TB 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.

Figure 5 shows an RTO example for a 2TB 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.
Figure 5) RTO for a 2TB database with Snapshot backups.

Figure 6 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 4 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 4 to 6 Snapshot backups per day. Our customers therefore typically configure 4 to 6 Snapshot backups per day.

Figure 6) RTO comparison: file-based backup versus Snapshot copy backup.

Note: The graph shows the HANA server RAM size. The database size in memory is calculated to be half of the server RAM size.

Note: 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. A recovery can be performed at 100MBps.

2 SnapCenter Architecture

2.1 SnapCenter Overview

SnapCenter is a unified, scalable platform for application-consistent data protection. SnapCenter provides centralized control and oversight, while delegating the ability for users to manage application-specific backup, restore, and clone jobs. With SnapCenter, database and storage administrators learn a single tool to manage backup, restore, and cloning operations for a variety of applications and databases. SnapCenter manages data across endpoints in the NetApp Data Fabric. You can use SnapCenter to replicate data between on-premises environments; between on-premises environments and the cloud; and between private, hybrid, or public clouds.

2.2 SnapCenter Features

SnapCenter enables you to create application-consistent Snapshot copies and to complete data protection operations, including Snapshot copy-based backup, clone, restore, and backup verification operations. SnapCenter provides a centralized management environment, while using role-based access control (RBAC) to delegate data protection and management capabilities to individual application users across your SnapCenter Server and Windows or Linux hosts. SnapCenter includes the following key features:

- A unified and scalable platform across applications and database environments and virtual and nonvirtual storage, powered by SnapCenter Server
- Consistency of features and procedures across plug-ins and environments, supported by the SnapCenter user interface
- RBAC for security and centralized role delegation
- Application-consistent Snapshot copy management, restore, clone, and backup verification support from both primary and secondary destinations (NetApp SnapMirror and SnapVault)
- Remote package installation from the SnapCenter GUI
- Nondisruptive, remote upgrades
- A dedicated SnapCenter repository that provides faster data retrieval
- Load balancing implemented using Microsoft Windows network load balancing (NLB) and application request routing (ARR), with support for horizontal scaling
- Centralized scheduling and policy management to support backup and clone operations
- Centralized reporting, monitoring, and dashboard views

2.3 SnapCenter Components

SnapCenter includes the SnapCenter Server, the SnapCenter Plug-In Package for Windows, and the SnapCenter Plug-Ins Package for Linux. Each package contains plug-ins to SnapCenter for various applications and infrastructure components. The SnapCenter custom plug-ins enable you to create your own plug-ins and protect your application using the same SnapCenter interface.
3 SnapCenter SAP HANA Backup Solution

3.1 Solution Components

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

- **SAP HANA data file backup with storage-based Snapshot copies:**
  - Backup scheduling
  - Replication to an off-site backup or disaster recovery location
  - Retention management
  - Housekeeping of the SAP HANA backup catalog

- **SAP HANA nondata volume backup with storage-based Snapshot copies:**
  - Backup scheduling
  - Replication to an off-site backup or disaster recovery location
  - Retention management

- **Database block integrity checks using a file-based backup:**
  - Backup scheduling
  - Retention management
  - Housekeeping of the SAP HANA backup catalog

- **SAP HANA log file backup with the HANA database log backup functionality:**
  - Retention management
  - Housekeeping of the SAP HANA backup catalog

Database data file backups are executed by SnapCenter in combination with the plug-in for SAP HANA. The plug-in triggers an SAP HANA database backup save point so that the Snapshot copies, which are created on the primary storage system, are based on a consistent image of the SAP HANA database.

SnapCenter enables the replication of consistent database images to an off-site backup or disaster recovery location by using SnapVault or SnapMirror. Typically, different retention policies are defined for backups at primary and at the off-site backup storage. SnapCenter handles the retention at primary storage, and ONTAP® handles the retention at the off-site backup storage.
To allow a complete backup of all SAP HANA-related resources, SnapCenter also allows you to back up all nondata volumes using the SAP HANA plug-in with storage-based Snapshot copies. Nondata volumes can be scheduled independently from the database data backup to enable individual retention and protection policies.

The SAP HANA database automatically executes log backups. Depending on the recovery point objectives, there are several options for the storage location of the log backups:

- The log backup is written to a storage system that synchronously mirrors the data to a second location with NetApp MetroCluster™ high-availability (HA) and disaster recovery storage software.
- The log backup destination can be configured on the same primary storage system and then replicated asynchronously to a secondary storage with SnapMirror.
- The log backup destination can be configured on the same off-site backup storage in which the database backups are replicated with SnapVault. With this configuration, the off-site backup storage has availability requirements like those of the primary storage so that log backups can be written to the off-site backup storage.

SAP recommends combining storage-based Snapshot backups with a weekly file-based backup to execute a block integrity check. The block integrity check can be executed from within SnapCenter. Based on your configurable retention policies, SnapCenter manages the housekeeping of data file backups at the primary storage, log file backups, and the SAP HANA backup catalog.

Note: SnapCenter handles the retention at primary storage, while ONTAP manages secondary backup retention.

Figure 8 shows an overview of the database and log backup configuration, where the log backups are written to an NFS mount of the off-site backup storage.

When executing a storage-based Snapshot backup of nondata volumes, SnapCenter performs the following tasks:
1. Creation of a storage Snapshot copy of the nondata volume.
2. Execution of a SnapVault or SnapMirror update for the data volume, if configured.
3. Deletion of storage Snapshot copies at the primary storage based on the defined retention policy.

When executing a storage-based Snapshot backup of the SAP HANA database, SnapCenter performs the following tasks:
1. Creation of an SAP HANA backup save point to create a consistent image on the persistence layer.
2. Creation of a storage Snapshot copy of the data volume.
3. Registration of the storage Snapshot backup in the SAP HANA backup catalog.
4. Release of the SAP HANA backup save point.
5. Execution of a SnapVault or SnapMirror update for the data volume, if configured.
6. Deletion of storage Snapshot copies at the primary storage based on the defined retention policy.
7. Deletion of SAP HANA backup catalog entries if the backups do not exist anymore at the primary storage.
8. Whenever a backup has been deleted based on the retention policy or manually, SnapCenter 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.

**Note:** The deletion of storage Snapshot copies at the off-site backup storage is executed by NetApp ONTAP, based on the defined retention in the ONTAP protection relationship configuration.

**Note:** The synchronization of backups deleted by ONTAP at the off-site backup storage and the SnapCenter repository is done asynchronously with a cleanup job, which runs once per week in the default configuration. SAP HANA catalog housekeeping and log backup housekeeping for these off-site backups are delayed according to the schedule of the cleanup job.

**Note:** The schedule of the cleanup job can be adapted, if required. For more details, refer to section 13.3, “Change Scheduling Frequency of Backup Synchronization with Off-Site Backup Storage.”

### 3.2 Supported SAP HANA Releases and Configurations

SnapCenter 4.0 supports SAP HANA single-host and multiple-host configurations using NFS- or FC-attached NetApp storage systems (FAS and AFF).

SnapCenter 4.0 supports the following SAP HANA releases:
- SAP HANA single container:
  - SAP HANA 1.0 SPS7 and later
  - SAP HANA 2.0 up to SPS0
- SAP HANA multiple-database container (MDC) single tenant:
  - SAP HANA 2.0 SPS1 and later

**Note:** Storage-based Snapshot backups for SAP HANA MDC with multiple tenants are not supported by SAP.

### 3.3 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 table merge process of the column store, much more data other than just the block changes is written to disk. Data from our customer base shows a daily change rate between 10% and 50%.

### 3.4 SnapCenter 4.0 Enhancements

The following new features and enhancements of SnapCenter 4.0 are important for SAP HANA:
The SAP HANA plug-in now supports the backup of non-data volumes. This allows for a complete backup of all relevant SAP HANA volumes. This feature is required if customers want to use storage-based Snapshot backups created by SnapCenter as a basis for SAP system copy operations with SAP Landscape Management (SAP LaMa). For details about SAP LaMa, see TR-4018: Integrating NetApp ONTAP Systems with SAP Landscape Management.

The operation “restore using file level” has been significantly enhanced to simplify usage for SAP HANA. For details, refer to section 11.3, Error! Reference source not found.."

SnapCenter supports a clone split operation directly from the SnapCenter GUI. For examples of how to use this feature, refer to TR-4667.

4 SnapCenter Installation and Configuration Overview

4.1 SnapCenter Installation

Install the SnapCenter software as instructed in the SnapCenter Software 4.0 Installation and Setup Guide.

4.2 Deployment Options for the SAP HANA Plug-In

Figure 9 shows the logical view and the communication between the SnapCenter Server, NetApp storage, and SAP HANA databases.

The SnapCenter Server communicates through the SAP HANA plug-in with the SAP HANA databases. The SAP HANA plug-in uses the SAP HANA hdbsql client software to execute SQL commands to the SAP HANA databases. The SAP HANA hdbuserstore is used to provide the user credentials, the host name, and the port information to access the SAP HANA databases.

Note: The SAP HANA plug-in and the SAP hdbsql client software, which include the hdbuserstore configuration tool, must be installed together on the same host.

The host can be the SnapCenter Server itself, a separate communication host, or the individual SAP HANA database hosts.

Figure 10 shows a configuration in which the SnapCenter Server is used as a central hdbsql communication host. The SAP HANA plug-in and the SAP hdbsql client software are installed on the SnapCenter Server.
Figure 10) Central hdbsql communication host on the SnapCenter Server.

Figure 11 shows a configuration in which a separate Linux host is used as a central hdbsql communication host. In this case, the SAP HANA plug-in and the SAP hdbsql client software are installed on the Linux host.

**Note:** The central communication host could also be a Windows host.

Figure 11) Central hdbsql communication host on a separate Linux server.

Figure 12 shows a configuration in which the SAP HANA plug-in is installed on each SAP HANA database host.
A central hdbsql communication host is required to support failover scenarios with SAP HANA multiple-host configurations. In an SAP HANA multiple-host configuration, a list of hdbuserstore keys is configured. SnapCenter goes through the list and tries to connect to the database. With this approach, the SAP HANA multiple-host system can be managed even if one of the hosts is currently down and the SAP HANA service has failed over to the standby host.

In contrast, the SAP HANA plug-in must be deployed on the SAP HANA target host when an SAP system clone or refresh is executed using SnapCenter. See also TR-4667.

The log backup housekeeping feature is enabled by default. It can only be disabled at the hdbsql communication host level. If there is a requirement to enable this feature on some SAP HANA systems and disable it on the others, then a mixed configuration is required.

The most common deployment is a mixed configuration with a central hdbsql communication host and individual SAP HANA plug-in deployments on the target systems for SAP system clone or refresh if the log backup housekeeping feature needs to be disabled for individual SAP HANA systems.
Table 1 summarizes the different deployment options.

Table 1) Summary of SAP HANA plug-in deployment options.

<table>
<thead>
<tr>
<th>Deployment Option</th>
<th>Installation of SAP HANA Plug-In and SAP hdbsql Client</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central hdbsql communication host</td>
<td>SnapCenter Server</td>
<td>Required deployment to support failover in an SAP HANA multiple-host setup. Log cleanup feature enabled or disabled for all SAP HANA systems using the central communication host.</td>
</tr>
<tr>
<td>Central hdbsql communication host</td>
<td>Separate Linux or Windows server</td>
<td>Required deployment to support failover in an SAP HANA multiple-host setup. Log cleanup feature enabled or disabled for all SAP HANA systems using the central communication host.</td>
</tr>
<tr>
<td>Individual hdbsql communication host</td>
<td>SAP HANA database hosts</td>
<td>Required deployment for the target host to support SAP system clone or refresh workflow. Log cleanup feature can be enabled or disabled for individual SAP HANA systems.</td>
</tr>
<tr>
<td>Mixed configuration</td>
<td>SnapCenter Server or separate Linux or Windows server and SAP HANA database hosts</td>
<td>Supports SAP HANA multiple-host configurations as well as SAP system cloning. Log cleanup feature can be enabled or disabled for individual SAP HANA systems.</td>
</tr>
</tbody>
</table>

### 4.3 Configuration Steps

The SnapCenter configuration can be separated into two main areas:

- **Initial configuration.** Covers generic configurations, independent of an individual SAP HANA database. Configurations such as storage systems, hosts, and policies are selected when executing the resource-specific configurations.

- **Resource-specific configuration.** Covers SAP HANA system-specific configurations and must be done for each SAP HANA system.

Figure 14 provides an overview of the configuration components and their dependencies when a central hdbsql communication host is used. The green boxes show configuration steps that must be done outside of SnapCenter; the blue boxes show the steps that are done using the SnapCenter GUI.
With the initial configuration, the following components are installed and configured:

- **Storage system configuration:**
  - Credential configuration for all SVMs that are used by the SAP HANA systems.
  - Typically, a primary, an off-site backup, and a disaster recovery storage.

- **Run as credential configuration:**
  - Configuration of credentials used to deploy the SAP HANA plug-in on the host.

- **Host configuration (for a central hdbsql communication host):**
  - Configuration of host name, run as credentials, and selection of SAP HANA plug-in to be deployed.
  - Installation of the SAP HANA hdbclient software on the host. The SAP hdbclient software must be installed manually outside of SnapCenter.

- **Policy configuration:**
  - Configuration of backup type, retention, and replication.
  - Typically, at least one policy for local Snapshot copies, one for SnapVault replication, and one for file-based backup is required.

The resource-specific configuration must be done for each SAP HANA database and includes the following configuration steps:

- **SAP hdbuserstore key configuration:**
  - The SAP hdbuserstore key configuration for the specific SAP HANA database must be done on the hdbsql communication host.

- **SAP HANA database resource configuration:**
  - SAP HANA database SID
  - Hdbsql communication host
  - Hdbsql userstore key
  - Storage systems and volumes

- **SAP HANA nondata volume resource configuration:**
  - Storage systems and volumes
• Resource or resource group protection configuration:
  − Selection of required policies
  − Definition of schedules for each policy
• ONTAP data protection configuration:
  − Only required if the backups should be replicated to an off-site backup storage.
  − Definition of relationship and retention.

4.4 Data Protection Strategy

Before configuring SnapCenter and the SAP HANA plug-in, the data protection strategy must be defined 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.

The parameters that must be defined are:
• How often should a Snapshot backup be executed?
• How long should Snapshot copy backups be kept on the primary storage system?
• How often should a block integrity check be executed?
• Should the primary backups be replicated to an off-site backup site?
• How long should the backups be kept at the off-site backup storage?

Table 2 shows an example of data protection parameters for the system types production, development, and test. For the production system, a high backup frequency has been defined, and the backups are replicated to an off-site backup site once per day. The test systems have lower requirements and no replication of the backups.

Table 2) Data protection parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Production Systems</th>
<th>Development Systems</th>
<th>Test Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup frequency</td>
<td>Every 4 hours</td>
<td>Every 4 hours</td>
<td>Every 4 hours</td>
</tr>
<tr>
<td>Primary retention</td>
<td>2 days</td>
<td>2 days</td>
<td>2 days</td>
</tr>
<tr>
<td>Block integrity check</td>
<td>Once per week</td>
<td>Once per week</td>
<td>No</td>
</tr>
<tr>
<td>Replication to off-site backup site</td>
<td>Once per day</td>
<td>Once per day</td>
<td>No</td>
</tr>
<tr>
<td>Off-site backup retention</td>
<td>2 weeks</td>
<td>2 weeks</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 3 shows the policies that must be configured for the data protection parameters.

Table 3) Policies based on data protection parameters.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Policy LocalSnap</th>
<th>Policy LocalSnapAndSnapVault</th>
<th>Policy BlockIntegrityCheck</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup type</td>
<td>Snapshot based</td>
<td>Snapshot based</td>
<td>File based</td>
</tr>
<tr>
<td>Schedule frequency</td>
<td>Hourly</td>
<td>Daily</td>
<td>Weekly</td>
</tr>
<tr>
<td>Primary retention</td>
<td>Count = 12</td>
<td>Count = 2</td>
<td>Count = 1</td>
</tr>
<tr>
<td>SnapVault replication</td>
<td>No</td>
<td>Yes</td>
<td>N/A</td>
</tr>
</tbody>
</table>
The policy `LocalSnapshot` is used for the production, development, and test systems to cover the local Snapshot backups with a retention of two days.

In the resource configuration, the schedule is defined differently for the system types:

- **Production**: Schedule every 4 hours.
- **Development**: Schedule every 4 hours.
- **Test**: Schedule every 4 hours.

The policy `LocalSnapAndSnapVault` is used for the production and development systems to cover the daily replication to the off-site backup storage.

In the resource configuration, the schedule is defined for production and development:

- **Production**: Schedule every day.
- **Development**: Schedule every day.

The policy `BlockIntegrityCheck` is used for the production and development systems to cover the weekly block integrity check using a file-based backup.

In the resource configuration, the schedule is defined for production and development:

- **Production**: Schedule every week.
- **Development**: Schedule every week.

For each individual SAP HANA database that uses the off-site backup policy, a protection relationship needs to be configured on the storage layer. The protection relationship defines which volumes are replicated and the retention of backups at the off-site backup storage.

With our example, for each production and development system, a retention of two weeks is defined at the off-site backup storage.

**Note**: In our example, protection policies and retention for SAP HANA database resources and non-data volume resources are not different.

### 4.5 Backup Retention Management and Housekeeping of Log Backups

The backup retention management and log backup housekeeping can be divided into five main areas, including retention management of:

- **Local backups at the primary storage**
- **File-based backups**
- **Backups at the secondary storage**
- **Data backups in the SAP HANA backup catalog**
- **Log backups in the SAP HANA backup catalog and the file system**

Figure 15 provides an overview of the different workflows and the dependencies of each operation. The following chapters describe the different operations in detail.
Retention Management of Local Backups at the Primary Storage
SnapCenter handles the housekeeping of SAP HANA database backups and non-data volume backups by deleting Snapshot copies on the primary storage and in the SnapCenter repository according to a retention defined in the SnapCenter backup policy.

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

Note: Be aware that SnapCenter handles retention management individually for both scheduled and on-demand backups.

Local backups at the primary storage can also be deleted manually in SnapCenter.

Retention Management of File-Based Backups
SnapCenter handles the housekeeping of file-based backups by deleting the backups on the file system according to a retention defined in the SnapCenter backup policy.

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

Note: Be aware that SnapCenter handles retention management individually for scheduled or on-demand backups.

Retention Management of Backups at the Secondary Storage
The retention management of backups at the secondary storage is handled by ONTAP, based on the retention defined in the ONTAP protection relationship.

To synchronize these changes on the secondary storage in the SnapCenter repository, SnapCenter uses a scheduled cleanup job. This cleanup job synchronizes all secondary storage backups with the SnapCenter repository for all SnapCenter plug-ins and all resources.

The cleanup job is scheduled once per week by default. This weekly schedule results in a delay with deleting backups in SnapCenter and SAP HANA Studio when compared with the backups that have already been deleted at the secondary storage. To avoid this inconsistency, customers can change the schedule to a higher frequency, for example, once per day.
Note: The cleanup job can also be triggered manually for an individual resource by clicking the refresh button in the topology view of the resource.

For details about how to adapt the schedule of the cleanup job or how to trigger a manual refresh, refer to section 13.3, “Change Scheduling Frequency of Backup Synchronization with Off-Site Backup Storage.”

Retention Management of Data Backups Within the SAP HANA Backup Catalog

When SnapCenter has deleted any backup, local Snapshot or file based, or has identified the backup deletion at the secondary storage, this data backup is also deleted in the SAP HANA backup catalog.

Before deleting the SAP HANA catalog entry for a local Snapshot backup at the primary storage, SnapCenter checks if the backup still exists at the secondary storage.

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 therefore be deleted.

SnapCenter 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 steps:

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

**Note:** SnapCenter 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.

**Note:** Even though a retention is defined for on-demand backups in the policy configuration, the housekeeping is only done when another on-demand backup is executed. Therefore, on-demand backups typically must be deleted manually in SnapCenter to make sure that these backups are also deleted in the SAP HANA backup catalog and that log backup housekeeping is not based on an old on-demand backup.

Log backup retention management is enabled by default. If required, it can be disabled as described in section 13.1, “Deactivating Automated Log Backup Housekeeping.”

5 Lab Setup

The lab setup used for this document includes four different SAP HANA configurations:

- SAP HANA MDC single-tenant systems:
  - SP1 single host using NFS
  - FP1 single host using SAN
- NF2 multiple host using NFS
- SAP HANA single-container system:
  - P01 using NFS
The following sections describe the complete configuration and the backup, restore, and recovery workflows for the SAP HANA MDC single-tenant system SP1, which uses NFS as the storage access protocol.

The differences for a SAN-attached, a single container, or a multiple-host system are reflected in the corresponding configuration or workflow steps.

The description covers local Snapshot backups as well as replication to backup storage using SnapVault. The storage virtual machines (SVMs) are hana for the primary storage and backup for the off-site backup storage.

The SnapCenter Server is used as a central hdbsql communication host. The SAP HANA plug-in and the SAP hdbsql client are installed on the SnapCenter Server.

Figure 16 shows the lab setup.

Figure 16) Lab setup.

6 SnapCenter Initial Configuration

The initial configuration includes the following steps:

1. Storage system configuration.
2. Run as credentials configuration.
3. For a central communication host:
   a. Host configuration and SAP HANA plug-in deployment
   b. SAP HANA hdbsql client software installation and configuration
4. Policies configuration.

The sections that follow describe the initial configuration steps.

6.1 Storage System Configuration

1. Log in to the SnapCenter Server GUI.
2. From the Get Started tab, select Add storage connection and licensing.

3. Click New to add a storage system.
4. Select the storage type ONTAP SVM and provide the required host name and credentials. 

**Note:** The SVM user is not required to be the "vsadmin" user, as shown in the screenshot. Typically, a user is configured on the SVM and assigned the required permissions to execute backup and restore operations.

5. Add additional storage systems as required.
6.2 Run As Credentials Configuration

1. Go to Settings, select Run As Credentials, and click New.

2. Provide the credentials for the user, which are used for plug-in installations on Linux systems.
3. Provide the credentials for the user, which are used for plug-in installations on Windows systems.

Figure 17 shows the configured run as credentials.
6.3 Host Configuration and SAP HANA Plug-In Installation

In the lab setup, the SnapCenter Server is used as the central hdbsql communication host. The Windows host, on which SnapCenter Server runs, is added as a host, and the SAP HANA plug-in is installed on the Windows host.

Note: The SAP HANA plug-in is based on Java. Java 64-bit version 1.8 or later needs to be installed on the host on which the SAP HANA plug-in is deployed.

1. Go to Hosts and click Add.

2. Provide the required host information. Click Next.
3. Click Next on the installed plug-ins page.

4. Select the SnapCenter plug-in for SAP HANA. Click Next.

5. Click Next on the Summary page. The SAP HANA plug-in is deployed on the host.

Figure 18 show all the configured hosts in our lab environment.
6.4 SAP HANA hdbsql Client Software Installation and Configuration

The SAP HANA hdbsql client software must be installed on the same host on which the SAP HANA plug-in is installed. The software can be downloaded from the SAP Support Portal.

The HDBSQL OS user configured during the resource configuration must be able to run the hdbsql executable. The path to the hdbsql executable must be configured in the `hana.properties` file.

- **Windows:**
  
  ```
  C:\More C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\hana.properties
  HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql.exe
  ```

- **Linux:**
  
  ```
  cat /opt/NetApp/snapcenter/scc/etc/hana.properties
  HANA_HDBSQL_CMD=/usr/sap/hdbclient/hdbsql
  ```

**Note:** If the HANA plug-in was installed at the SAP HANA database host, the hdbsql client software is typically already installed. If the recommended user `<sid>adm` is configured as the hdbsql OS user in the SnapCenter resource configuration, these steps are not required because the hdbsql executable can be run directly due to the $PATH configuration of the `<sid>anm` user.

6.5 Policy Configuration

As discussed in “Error! Reference source not found.,” 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 backups without replication: `LocalSnap`
- Policy for daily backups with SnapVault replication: `LocalSnapAndSnapVault`
- Policy for weekly block integrity check using a file-based backup: `BlockIntegrityCheck`

The following sections describe the configuration of these three policies.
Policy for Hourly Snapshot Backups Without Replication

1. Go to Settings > Policies and click New.
2. Enter the policy name and description. Click Next.

3. Select backup type as Snapshot Based and select Hourly for schedule frequency.

4. Configure the retention settings for on-demand backups.
5. Configure the retention settings for scheduled backups.

6. Configure the replication options. In this case, no SnapVault or SnapMirror update is selected.

7. Click Finish on the Summary page.
Policy for Daily Snapshot Backups with SnapVault Replication

1. Go to Settings > Policies and click New.
2. Enter the policy name and description. Click Next.

3. Set the backup type to Snapshot Based and the schedule frequency to Daily.

4. Configure the retention settings for on-demand backups.
5. Configure the retention settings for scheduled backups.

6. Select Update SnapVault after creating a local Snapshot copy.

   **Note:** The secondary policy label must be the same as the SnapMirror label in the data protection configuration on the storage layer. Refer to section 7.2, “Configuration of Data Protection to Off-Site Backup Storage.”

7. Click Finish on the Summary page.
Policy for Weekly Block Integrity Check Using File-Based Backup

1. Go to Settings > Policies and click New.
2. Enter the policy name and description. Click Next.
3. Set the backup type to File-Based and schedule frequency to Weekly.
4. Configure the retention settings for on-demand backups.
5. Configure the retention settings for scheduled backups.

6. Click Finish on the Summary page.

Figure 19 shows a summary of the configured policies.
7 SnapCenter Resource-Specific Configuration for SAP HANA Database Backups

This section describes an example configuration for the SAP HANA system SP1, an SAP HANA MDC single-tenant setup using NFS for storage access. The resource is configured to create local Snapshot backups, replicate to an off-site backup storage using SnapVault, and perform block integrity checks for the SAP HANA database using a weekly file-based backup.

The differences for a SAN-attached, single-container, or multiple-host system are reflected in the corresponding configuration or workflow steps.

7.1 SAP HANA Backup User and Hdbuserstore Configuration

NetApp recommends configuring a dedicated database user in the HANA database to run the backup operations with SnapCenter. In the second step, an SAP HANA user store key is configured for this backup user, and this user store key is used in the configuration of the SnapCenter SAP HANA plug-in.

Figure 20 shows a screenshot of the SAP HANA Studio through which the backup user can be created. The backup user must have backup admin and catalog read privileges.

Note: For an SAP HANA MDC system, the user must be created in the system database because all backup commands for the system and the tenant database are executed using the system database.
At the hdbsql communication host, on which the SAP HANA plug-in and the SAP hdbsql client are installed, a user store key is configured for all database hosts that belong to the SAP HANA system. The user store key is configured with the OS user that is defined in the resource configuration, as described in section 7.3, "Resource Configuration."

If the SAP HANA plug-in and the SAP hdbsql client are installed on Windows, the local system user executes the hdbsql commands and is configured by default in the resource configuration. Because the system user is not a logon user, the user store configuration must be done with a different user and the \-u <User>\ option.

```
hdbuserstore.exe -u SYSTEM set <key> <host>:<port> <database user> <password>
```

If the SAP HANA plug-in and SAP hdbsql client are installed on Linux, the following command is used for the user store configuration with the user defined in the resource configuration:

```
hdbuserstore set <key> <host>:<port> <database user> <password>
```

**Note:** In an SAP HANA MDC single-tenant setup, port 3<instanceNo>13 is the standard port for SQL access to the system database and must be used in the hdbuserstore configuration.

**Note:** 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 hdbuserstore configuration.

**Note:** For an SAP HANA multiple-host setup, user store keys for all hosts must be configured. SnapCenter tries to connect to the database using each of the provided keys and can therefore operate independently of a failover of an SAP HANA service to a different host.

In the lab setup, the SAP HANA plug-in and the SAP hdbsql client were installed on the SnapCenter Windows host. The user store keys for the SAP HANA systems are configured by running the following commands:

- SAP HANA system SP1, MDC single tenant, instance 00:
7.2 Configuration of Data Protection to Off-Site Backup Storage

The configuration of the data protection relation as well as the initial data transfer must be executed before replication updates can be managed by SnapCenter.

Figure 21 shows the configured protection relationship for the used SAP HANA system SP1. With our example, the source volume `SP1_data_mnt00001` at the SVM `hana` is replicated to the SVM `backup` and the target volume `hana_SP1_data_mnt00001_vault`.

Note: The schedule of the relationship must be set to None because SnapCenter triggers the SnapVault update.
Figure 21 shows the protection policy. The protection policy used for the protection relationship defines the SnapMirror label, as well as the retention of backups at the secondary storage. In our example, the used label is **Daily**, and the retention is set to **3**.

**Note:** The SnapMirror label in the policy being created must match the label defined in the SnapCenter policy configuration. For details, refer to “Policy for Daily Snapshot Backups with SnapVault Replication.”

**Note:** The retention for backups at the off-site backup storage is defined in the policy and controlled by ONTAP.
7.3 Resource Configuration

The following screenshots show the configuration of existing resources. The required input is the same if a new resource is added to SnapCenter.

1. From the Resources tab, select SAP HANA and click Add SAP HANA Database.
2. Enter the information for configuring the SAP HANA database and click Next.
   - Select the resource type, in our example, MDC – Single Tenant.
   - For our SAP HANA system, the SID and the tenant database name are SP1.
   - The HDBSQL client host in our example is the SnapCenter Server.
   - The hdbuserstore key must match the key that was configured previously. In our example, it is SP1KEY.

Note: The configuration screen for an SAP HANA single-container system does not include the tenant database name. All other parameters are identical.
### Modify SAP HANA Database

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Type</td>
<td>Single Container, Multi-tenant Database Container (MDC), Single Tenant, Non-data Volume</td>
</tr>
<tr>
<td>HANA System Name</td>
<td>MDC single tenant—MTP—multiple host</td>
</tr>
<tr>
<td>SID</td>
<td>T123</td>
</tr>
<tr>
<td>HDBSQL Client Host</td>
<td>&lt;host_name&gt;</td>
</tr>
<tr>
<td>HDB SQL Secure User Store Keys</td>
<td>&lt;keys&gt;</td>
</tr>
<tr>
<td>HDBSQL OS User</td>
<td>&lt;username&gt;</td>
</tr>
</tbody>
</table>

**Note:** For an SAP HANA multiple-host system, the hdbuserstore keys for all hosts must be included, as shown in the following figure.

3. Select the required data for the storage system (SVM) and volume name.
**Note:** For an SAP HANA multiple-host system, all data volumes of the SAP hana system must be selected, as shown in the following figure.

4. Enter the parameter for file-based backup and click Next.
**Note:** The backup location is a path accessible from the SAP HANA database host. If the location input field is left empty, the path for file-based backups configured in the SAP HANA database is used. This is the recommended configuration.

### Modify SAP HANA Database

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Review</td>
</tr>
<tr>
<td>2</td>
<td>Storage Format</td>
</tr>
<tr>
<td>3</td>
<td>Resource Settings</td>
</tr>
<tr>
<td>4</td>
<td>Summary</td>
</tr>
</tbody>
</table>

#### Summary

- **Resource Type:** Multitenant Database Container (MDC) - Single Tenant
- **SID:** SAP
- **Version:** 1900
- **HANA Client Host:** SCS V225aptd6سفر.Netapp.com
- **HANA Secure User Store Name:** SPROXY
- **HANA OS User Name:** SYSTEM
- **Storage System:** SPS
- **Volume:** HLAV001
- **File Backup Prefix:** SnapCenter_
- **File Backup Path:**

5. The summary screen of the resource configuration is shown. Click Finish to add the SAP HANA database.
### 7.4 Resource Protection Configuration

The following screenshots show the configuration of existing resources. The required input is the same if a new resource is added to SnapCenter.

1. In the Resources tab, double-click the resource.
2. Configure a custom name format for the Snapshot copy.

**Note:** NetApp recommends using a custom Snapshot copy name to easily identify which backups have been created with which policy and with which schedule type. By adding the schedule type in the Snapshot copy name, you can distinguish between scheduled and on-demand backups. The schedule name string for on-demand backups is empty, while scheduled backups include the string Hourly, Daily, or Weekly.

In the configuration shown in the following figure, the backup and Snapshot copy names have the following format:

- **Scheduled hourly backup:** SnapCenter_LocalSnap_Hourly_<time_stamp>
- **Scheduled daily backup:** SnapCenter_LocalSnapAndSnapVault_Daily_<time_stamp>
- **On-demand hourly backup:** SnapCenter_LocalSnap_<time_stamp>
- **On-demand daily backup:** SnapCenter_LocalSnapAndSnapVault_<time_stamp>

**Note:** Even though a retention is defined for on-demand backups in the policy configuration, the housekeeping is only done when another on-demand backup is executed. Therefore, on-demand backups must typically be deleted manually in SnapCenter to make sure that these backups are also deleted in the SAP HANA backup catalog and that the log backup housekeeping is not based on an old on-demand backup.

3. In the Snapshot Copy Tool configuration, select SnapCenter without file system consistency and click Next.
4. Select the policies that should be added to the resource.

5. Define the schedule for the LocalSnap policy: with our example, every 4 hours.
6. Define the schedule for the LocalSnapAndSnapVault policy: with our example, once per day.

7. Define the schedule for the block integrity check policy: with our example, once per week.

8. Provide information about email notification.
9. Click Finish on the Summary page.

10. On-demand backups can now be created in the topology screen. The scheduled backups are executed based on the configuration set.
7.5 Additional Configuration Steps for XFS Environments

Additional configuration steps are required for environments in which the SAP HANA systems are using the XFS file system.

When a global synchronized backup save point is triggered by SnapCenter in SAP HANA, SAP HANA writes the file /hana/data/SID/mnt00001/hdb00001/snapshot_databackup_0_1 as a last step. This file is part of the data volume on the storage and is therefore part of the storage Snapshot copy. This file is mandatory when performing a recovery in a situation in which the backup is restored. Due to metadata caching with the XFS file system on the Linux host, the file is not immediately visible at the storage layer. The standard XFS configuration for metadata caching is 30 seconds.

In SnapCenter, you must configure a postquiesce command that waits until the XFS metadata cache is flushed to the disk layer.

The actual configuration of the metadata caching can be checked by using the following command:

```
stlrx300s8-2:/ # sysctl -A | grep xfssyncd_centisecs
fs.xfs.xfssyncd_centisecs = 3000
```

NetApp recommends using a wait time that is twice the value of the `fs.xfs.xfssyncd_centisecs` parameter. Because the default value is 30 seconds, set the sleep command to 60 seconds.

If the hdbsql communication host runs on Windows, a batch file can be used. The batch file must have the following content:

```
@echo off
waitfor AnyThing /t 60 2>NUL
Exit /b 0
```

In our lab setup, the batch file is saved as `C:\Program Files\NetApp\Wait60Sec.bat`. In the resource protection configuration, the Post Quiesce command is configured as shown in Figure 23.

![Figure 23) Configuration of postquiesce command in Windows.](image)
If the hdbsql communication host runs on Linux or the SAP HANA plug-in has been installed on the SAP HANA database host, the command `/bin/sleep 60` must be configured as a Post Quiesce command in the SnapCenter UI.

8 SnapCenter Resource-Specific Configuration for Nondata Volume Backups

In SnapCenter 4.0, the backup of nondata volumes is an integrated part of the SAP HANA plug-in. Protecting the database volume or database LUN, as shown in section 7.4, “Resource Protection Configuration,” 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 nondata files must be restored, NetApp recommends developing an additional backup strategy for nondata volumes to augment the SAP HANA database backup. Depending on your specific requirements, the backup of nondata volumes might differ in scheduling frequency and retention settings, and you should consider how frequently nondata files are changed. For instance, the HANA volume `/hana/shared` contains executables but also SAP HANA trace files. While 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.

SnapCenter nondata 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 SAP HANA, and no entry is required in the SAP HANA backup catalog.

8.1 Configuration of Nondata Volume Resources

In the example, we want to protect the nondata volumes of the SAP HANA database P01. The SAP HANA database P01 is used for the SAP NetWeaver system PNW application servers and therefore is a perfect example for adding “all” relevant nondata volumes to be protected. This means it includes not only the nondata volumes of SAP HANA database P01, but also the application server volumes from the PNW instance that connects to this database. See Figure 24.
In our example, we create a single nondata resource for every nondata volume.

1. In the Resource tab, select the “Add SAP HANA Database” button.

2. In step one of the “Add SAP HANA Database” dialog, select Non-data Volumes as resource type. Specify a name for the resource and the associated SID and the SAP HANA Plug-in host you want to use for the resource, then select Next.

3. Add the storage virtual machine and the storage volume as storage footprint and select Next.
4. In the summary step, select Finish to save the settings.
5. Repeat these steps for all required nondata volumes.

Figure 25 shows the list of the configured nondata volume resources.

Figure 25) Nondata volume resources.

8.2 Data Protection for Nondata Volume Resources

Data protection for a nondata volume resource is identical to the workflow for SAP HANA database resources and can be defined on an individual resource level. This provides the most flexibility with respect to policies and schedules for nondata volume resources.
Resource Groups

Resource groups are a convenient way to define the protection of multiple resources that require the same protection policies and schedule. Single resources that are part of a resource group can still be protected on an individual level.

Resource groups provide the following features:

- You can add one or more resources to a resource group. All resources must belong to the same SnapCenter plug-in.
- Protection can be defined on a resource group level. All resources in the resource group use the same policy and schedule when protected.
- All backups in the SnapCenter repository and the storage Snapshot copies have the same name defined in the resource protection.
- Restore operations are applied on a single resource level, not as part of a resource group.
- When using SnapCenter to delete the backup of a resource that was created on a resource group level, this backup is deleted for all resources in the resource group. Deleting the backup includes deleting the backup from the SnapCenter repository as well as deleting the storage Snapshot copies.
- The main use case for resource groups is when a customer wants to use backups created with SnapCenter for system cloning with SAP Landscape Management. This is described in the next section.

8.3 Using SnapCenter Together with SAP Landscape Management

Note: With SAP Landscape Management (SAP LaMa), customers can manage complex SAP system landscapes in on-premises data centers as well as in systems that are running in the cloud. SAP LaMa, together with NetApp Storage Services Connector (SSC), can execute storage operations such as cloning and replication for SAP system clone, copy, and refresh use cases using NetApp Snapshot and FlexClone® technology. This allows you to completely automate an SAP system copy based on storage cloning technology while also including the required SAP postprocessing. For more details about NetApp’s solutions for SAP LaMa, refer to TR-4018: Integrating NetApp ONTAP Systems with SAP Landscape Management.

NetApp SSC and SAP LaMa can create on-demand Snapshot copies directly using NetApp SSC, but they can also utilize Snapshot copies that have been created using SnapCenter. To utilize SnapCenter backups as the basis for system clone and copy operations with SAP LaMa, the following prerequisites must be met:

- SAP LaMa requires that all volumes are included in the backup; this includes:
  - SAP HANA data volumes
  - SAP HANA shared volume
  - SAP HANA log volumes
- All storage Snapshot names must be identical.
- Storage Snapshot names must start with “VCM.”

Note: In normal backup operations, it is not recommended to include the log volume. If you restore the log volume from a backup, it overwrites the last active redo logs and thus prevents the recovery of the database to the last recent state.

SnapCenter resource groups meet all these requirements. Three resources are configured in SnapCenter: one resource each for the data volume, the log volume, and the shared volume. The resources are put into a resource group, and the protection is then defined on the resource group level. In the resource group protection, the custom Snapshot name must be defined with the required “VCM” at the beginning.
9 Database Backups

A database backup can be performed by using either the SnapCenter GUI, a PowerShell command line, or REST APIs. In this report, the SnapCenter GUI is used for backup and restore operations.

Note: The backup workflows in the following sections are illustrated using an SAP HANA MDC single-tenant system SP1. This system is configured with the resource name SP1 MDC single tenant.

9.1 Backup Workflow for On-Demand and Scheduled Backups

SnapCenter backs up the SAP HANA database in the following sequence:

1. SnapCenter triggers an SAP HANA global synchronized backup save point to create a consistent database image on the persistence layer.
   
   Note: For an SAP HANA MDC single-tenant system, a synchronized global backup save point for both databases, the system database, and the tenant database is created.

2. SnapCenter creates storage Snapshot copies for all data volumes configured for the resource. 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.

3. SnapCenter registers the storage Snapshot backup in the SAP HANA backup catalog.

4. SnapCenter deletes the SAP HANA backup save point.

5. SnapCenter starts a SnapVault or SnapMirror update for all configured data volumes in the resource.
   
   Note: This step is only executed if the selected policy includes a SnapVault or SnapMirror replication.

6. SnapCenter deletes the storage 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 at the primary storage.
   
   Note: If the backup is still available at the secondary storage, the SAP HANA catalog entry does not get deleted.

7. SnapCenter 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.
   
   Note: This step is only executed if log backup housekeeping has not been disabled.

9.2 On-Demand Database Backup at Primary Storage

1. In the resource view, select the resource and double-click the line to switch to the topology view.

   The resource topology view provides an overview of all available backups that are created using SnapCenter. The top area of this view displays the backup topology, showing the backups on the primary storage (local copies) and if available on the off-site backup storage (vault copies).
2. In the top row, select the Back up Now icon to start an on-demand backup. From the drop-down list, select the backup policy `LocalSnap` and start the on-demand backup with the Backup button.

![Backup Screen](Image)

Create a backup for the selected resource

<table>
<thead>
<tr>
<th>Resource Name</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP1 MDC single tenant – NFS</td>
<td>LocalSnap</td>
</tr>
</tbody>
</table>

![Backup Button](Image)

3. This starts the backup job. A log of the previous five jobs is shown in the Activity area below the topology view. When the backup is finished, a new entry is shown in the topology view. The backup names follow the same naming convention as the Snapshot name defined in section 7.4, “Resource Protection Configuration.”

**Note:** You must close and reopen the topology view to see the updated backup list.
4. The job details are shown when clicking the job’s activity line in the Activity area. A detailed job log can be opened by clicking the View logs button.
5. In SAP HANA Studio, the new backup is visible in the backup catalog. The same backup name in SnapCenter is also used in the comment and the EBID field in the backup catalog.

**Note:** The screenshot shows the backup catalog of the SYSTEMDB. The identical backup entry is also written to the backup catalog of the tenant database.

9.3 On-Demand Database Backups with SnapVault Replication

1. In the resource view, select the resource and double-click the line to switch to the topology view.
2. In the top row, select the Back up Now icon to start an on-demand backup. From the drop-down list, select the backup policy `LocalSnapAndSnapVault` and start the on-demand backup with the Backup button.

3. The job details are shown when clicking the job's activity line in the Activity area.
4. When the backup is finished, a new entry is shown in the topology view. The backup names follow the same naming convention as the Snapshot name defined in section 7.4, “Resource Protection Configuration.”

**Note:** You must close and reopen the topology view to see the updated backup list.
5. By selecting Vault copies, backups at the secondary storage are shown. The name of the replicated backup is identical to the backup name at the primary storage.

**Note:** To get an updated view of the secondary backups, the refresh button on the upper-right side of the topology view must be clicked.
6. In SAP HANA Studio, the new backup is visible in the backup catalog. The same backup name in SnapCenter is also used in the comment and the EBID field in the backup catalog.

**Note:** The screenshot shows the backup catalog of the SYSTEMDB. The identical backup entry is also written to the backup catalog of the tenant database.

9.4 Identifying SnapCenter Backups in SAP HANA Studio

The SnapCenter resource topology shows a list of backups created using SnapCenter. Figure 26 shows the backups available on the primary storage and highlights the most recent backup.
When performing a backup using storage Snapshot copies for an SAP HANA MDC single-tenant database, a Snapshot copy of the data volume is created. This data volume contains the data of the system database as well as the tenant database. To reflect this physical architecture, SAP HANA internally performs a combined backup of the system database as well as the tenant database whenever SnapCenter triggers a Snapshot backup. This results in two separate backup entries in the SAP HANA backup catalog: one for the system database and the other for the tenant database.

**Note:** 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 backup name is stored as a Comment field as well as External Backup ID (EBID). This is shown in Figure 27 for the system database and in Figure 28 for the tenant database SP1. Both figures highlight the SnapCenter backup name stored in the comment field and EBID.
Figure 27) SAP HANA backup catalog for the system database.

Figure 28) SAP HANA studio backup catalog for tenant SP1.

Note: SnapCenter only displays its own backups. Additional backups created, for example, with SAP HANA Studio, are visible in the SAP HANA catalog but not in SnapCenter.

9.5 Identifying SnapCenter Backups on the Storage Systems

To view the backups on the storage layer, use NetApp OnCommand® System Manager and select the database volume in the SVM - Volume view. The lower Snapshot Copies tab displays the Snapshot
copies of the volume. Figure 29 shows the available backups for the database volume SP1_data_mnt00001 at the primary storage. Figure 30 shows the available backups for the replication target volume hana_SP1_data_mnt00001_vault at the secondary storage system. The highlighted backup is the backup shown in SnapCenter and SAP HANA Studio in the previous screenshots and has the same naming convention.

Figure 29) Backups at the primary storage.

Figure 30) Backups at the secondary storage.
10 Block Integrity Check

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

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

SnapCenter does not display the block integrity check in the same manner as Snapshot copy-based backups. Instead, the summary card shows the number of file-based backups and the status of the previous backup.

Figure 31) Block integrity check.

The SAP HANA backup catalog shows entries for both the system and the tenant databases. Figure 32 shows a SnapCenter block integrity check in the backup catalog of the system database.
On the backup path defined in SAP HANA Studio or in the specific path defined in the policy, a successful block integrity check creates standard SAP HANA data backup files.

The backup names follow the naming convention defined in the resource protection by adding the prefix defined in the backup policy for the block integrity check.

```
stlrx300s8-8:~ # ls -al /hana/shared/SP1/HDB00/backup/data/DB_SP1/
total 3125408
  drwxr-x--x 2 sp1adm sapsys  4096 Feb  4  07:01 .
  drwxr-x--x 4 sp1adm sapsys  4096 Feb  4  07:01 ..
-rw-r----- 1 sp1adm sapsys 155648 Feb  4  07:00 SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_02-04-2018_07.00.02.7276_databackup_0_1
-rw-r----- 1 sp1adm sapsys  83894272 Feb  4  07:00 SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_02-04-2018_07.00.02.7276_databackup_2_1
-rw-r----- 1 sp1adm sapsys 3103793152 Feb  4  07:01 SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_02-04-2018_07.00.02.7276_databackup_3_1
```

```
stlrx300s8-8:~ # ls -al /hana/shared/SP1/HDB00/backup/data/SYSTEMDB/
total 2812872
  drwxr-x--x 2 spladm sapsys  4096 Feb  4  07:01 .
  drwxr-x--x 4 spladm sapsys  4096 Feb  4  07:01 ..
-rw-r----- 1 spladm sapsys  155648 Feb  4  07:00 SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_02-04-2018_07.00.02.7276_databackup_0_1
-rw-r----- 1 spladm sapsys  2868912128 Feb  4  07:00 SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_02-04-2018_07.00.02.7276_databackup_1_1
```

11 Restore and Recovery

Restore and recovery of an SAP HANA database are done using SnapCenter and SAP HANA Studio or SAP HANA Cockpit:

- SnapCenter is used to restore the database volumes.
• SAP HANA Studio or SAP HANA Cockpit is used to recover the SAP HANA database.

Note: For the recovery of an SAP HANA MDC single-tenant database, two subsequent recoveries must be executed. The system database needs to be recovered first, followed by the tenant database. The following examples use SAP HANA Studio for the recovery process.

11.1 Restore and Recovery Workflow Overview
To restore and recover an SAP HANA MDC single-tenant system using SAP HANA Studio and SnapCenter, complete the following steps:

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

2. To perform the restore process with SnapCenter:
   a. In the topology view of the resource, select Local Copies to restore from primary storage or Vault Copies if you want to restore from an off-site backup storage.
   b. Select the SnapCenter backup that matches the external backup ID or comment field from SAP HANA Studio.
   c. Start the restore process.

Note: If a volume-based restore from primary storage is chosen, the data volumes must be unmounted from all SAP HANA database hosts before the restore and mounted again after the restore process is finished.

Note: In an SAP HANA multiple-host setup with FC, the unmount and mount operations are executed by the SAP HANA name server as part of the shutdown and startup process of the database.

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

3. To 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.
   c. A list of data backups displays. Because the data volume has already been restored, the tenant backup is indicated as available (in green).
   d. Select this backup and start the recovery process. After the recovery process is finished, the tenant database is started automatically.

11.2 Restore and Recovery from Primary Storage Using Volume-Based Restore
The fastest method of restore is the volume-based restore from primary storage. However, when SnapVault protection is active and backups from primary storage must be restored that are older than the Snapshot copy used for SnapVault synchronization, SnapCenter prevents the restore operation because of the busy Snapshot copy at the storage layer. In this case, only a file-level restore can be executed.

Note: When using volume restore from an older backup on the primary storage, all newer Snapshot copy backups are not available anymore at the storage layer. SnapCenter also deletes these backups in its own database. However, SnapCenter won’t be able to delete the backups in the SAP HANA backup catalog because the SAP HANA database is not online currently. To
To start a volume-based restore and recovery, complete the following steps:

1. In SAP HANA Studio, select the Recover System Database option to start the recovery of the system database for the SAP HANA MDC single-tenant system with SID SP1.

2. Click OK to shut down the SAP HANA database.

The SAP HANA system shuts down to start the recovery wizard.

3. Select the recovery type and click Next.
4. Provide the location of the backup catalog and click Next.
5. A list of available backups displays based on the content of the backup catalog. Choose the required backup and note the external backup ID: in our example, the most recent backup.

6. On each database host, unmount all data volumes. In our example, only one volume must be unmounted on the single-host SAP HANA system.

   umount /hana/data/SP1/mnt00001

   **Note:** In an SAP HANA multiple-host setup with FC, the unmount operation is executed by the SAP HANA name server as a part of the shutdown process.

7. From the SnapCenter GUI, select the resource topology view and select the backup that should be restored: in our example, the most recent primary backup. Click the restore icon to start the restore.
The SnapCenter restore wizard starts.

8. Select the restore type Complete Resource to use a volume-based restore. Click Next to continue.

9. (Optional) Specify commands that should be executed from the SAP HANA plug-in running on the hdbsql communication host. Click Next.

10. Specify the optional commands and click Next.
11. Specify the notification settings so that SnapCenter can send a status email and job log. Click Next.

12. Review the summary and click Finish to start the restore.
13. The restore job starts, and the job log can be displayed by double-clicking the log line in the activity pane.

14. Wait until the restore process completes. On each database host, mount all data volumes. In our example, only one volume must be remounted on the database host.
mount /hana/data/SP1/mnt00001

15. Go to SAP HANA Studio and click Refresh to update the list of available backups. The backup that was restored with SnapCenter is shown with a green icon in the list of backups. Select the backup and click Next.

16. Provide the location of the log backups. Click Next.

17. Select other settings as required. Make sure Use Delta Backups is not selected. Click Next.
18. Review the recovery settings and click Finish.

19. The recovery process starts. Wait until the recovery of the system database completes.
20. In SAP HANA Studio, select the entry for the system database and start Backup Recovery - Recover Tenant Database.

21. Select the tenant to recover and click Next.
22. Specify the recovery type and click Next.
23. Confirm the backup catalog location and click Next.

![Locate Backup Catalog](image)

24. Confirm that the tenant database is offline. Click OK to continue.

![Stop Database SP1@SP1](image)

25. Because the restore of the data volume has occurred before the recovery of the system database, the tenant backup is immediately available. Select the backup highlighted in green and click Next.
26. Confirm the log backup location and click Next.
27. Select other settings as required. Make sure Use Delta Backups is not selected. Click Next.

28. Review the recovery settings and start the recovery process of the tenant database by clicking Finish.
29. Wait until the recovery has finished and the tenant database is started.

The SAP HANA system is up and running.

11.3 Restore and Recovery from Primary Storage Using File-Level Restore

A restore operation using file-level restore is required if a restore that is based on an older backup than the Snapshot copy used for SnapVault synchronization needs to be executed. A file-level restore also has the advantage that no Snapshot backups are deleted when you are not restoring to the most recent backup. A file-level restore is done by copying all files from the Snapshot backup on the storage layer. This operation takes more time compared to a volume restore.

Note: A file-level restore only restores the individual files, not the directory structure. If the directory structure is also lost, it must be created manually, before executing the restore operation.

The restore and recovery workflow steps using a file-level restore are almost identical to the restore and recovery workflow steps using a volume-based restore operation described in section 11.2, “Restore and Recovery from Primary Storage Using Volume-Based Restore.” The following sections highlight the steps that are different.

File-Level Restore with an NFS Setup

Note: With a file-level restore, the mount and unmount operations of the data volume are not required.

The most common use case for an SAP HANA restore is to restore all files of the database. To simplify this operation, SnapCenter allows you to select all files in the restore workflow, as shown in Figure 33).
In an SAP HANA multiple-host configuration, all volumes must be selected together with the “All” check box, as shown in Figure 34.

After the restore is completed, the recovery is done using SAP HANA Studio in the same way as described in section 11.2, “Restore and Recovery from Primary Storage Using Volume-Based Restore.”
File-Level Restore with an FC Setup

Before the restore operation is started, the LUN needs to be unmounted at the SAP HANA database server.

Note: The mount and unmount operations of the target LUNs are not required for a multiple-host SAP HANA database.

Figure 35 shows the restore screen in SnapCenter. Select the LUNs to be restored. In our case, for the SAP HANA single-host system, only one LUN is stored in the data volume. In an SAP HANA multiple-host setup, multiple LUNs must be selected.

Figure 35) File-level restore with an FC setup.

After the restore is finished, the restored LUN needs to be mounted at the SAP HANA database server. The recovery is done using SAP HANA Studio in the same manner as described in section 11.2, “Restore and Recovery from Primary Storage Using Volume-Based Restore.”

11.4 Restore and Recovery from Off-Site Backup Storage

The restore and recovery workflow is like the volume restore workflow described in section 11.2, “Restore and Recovery from Primary Storage Using Volume-Based Restore.” However, instead of restoring from the primary site, the data is restored from the off-site backup site.

Note: In a volume restore operation from the off-site backup site, the mount and unmount operations of the target volume are not required.

1. From the SnapCenter GUI, select the resource topology view and select the secondary vault backup from where you want to restore. Click the Restore icon to start the workflow.
2. Verify that the correct source volume is selected. Click Next.

After the restore completes, the recovery is done using SAP HANA Studio in a manner similar to that described in section 11.2, “Restore and Recovery from Primary Storage Using Volume-Based Restore.”

12 Using Job Monitor for Troubleshooting

Every operation such as backup and restore creates an entry in the Job Monitoring section.

1. Click the Monitor tab in the main menu to view the job monitor.
2. In the job monitor, you can use the filter to search for text fragments. As an example, we analyze a problem that occurred during a block integrity check operation. Searching for the string block filters the job logs.

3. Double-click the job line to open the job details. Drill down to the erroneous step to display the error message.
4. In most cases, this helps to identify the issue. Clicking the View logs button switches to the log view of this. You can filter the logs, for example, to display only the error messages to further analyze the situation.

In our example, the job details and job logs indicate a connection problem to the SAP HANA database, which was offline when SnapCenter tried to start the block integrity check.
13 Advanced Configuration and Tuning

This chapter describes configuration and tuning options that customers may use to adapt the SnapCenter setup to their specific needs. Not all the settings may apply for all customer scenarios.

13.1 Deactivating Automated Log Backup Housekeeping

Log backup housekeeping is enabled by default and can be disabled on the hdbsql communication host level. There are two options to change these settings.

Editing the hana.property File

Including the parameter LOG_CLEANUP_DISABLE = Y in the hana.property configuration file disables the log backup housekeeping for all resources using this SAP HANA plug-in host as communication host:

- For the Hdbsql communication host on Windows, the hana.property file is located at C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc.
- For the Hdbsql communication host on Linux, the hana.property file is located at /opt/NetApp/snapcenter/scc/etc.

Using PowerShell Command

A second option to configure these settings is using a SnapCenter PowerShell command.

1. On the SnapCenter server, open a PowerShell. Connect to the SnapCenter server using the command "Open-SmConnection" and specify user name and password in the opening login popup window.

2. With the command `Set-SmConfigSettings -Plugin -HostName <pluginhostname> -PluginCode hana -configSettings @{"LOG_CLEANUP_DISABLE" = "Y"}`, the changes are configured for the SAP HANA plug-in host <pluginhostname> specified by ip or hostname (see Figure 36).

Figure 36) PowerShell cmd to disable log backup housekeeping.
13.2 Disable Warning When Running SAP HANA Plug-In on a Virtual Environment

SnapCenter detects if the SAP HANA plug-in is installed on a virtualized environment. In this case, SnapCenter displays a warning to configure the hypervisor, as shown in Figure 37.

Figure 37) SnapCenter warning to configure hypervisor.

For customers that are interested in protecting only their SAP HANA databases and do not plan to use SnapCenter features to protect virtualized environments, it is possible to suppress this warning globally. In this case, SnapCenter is not aware of virtualized environments, and thus it does not show these warnings.

To configure SnapCenter to suppress this warning, the following configuration must be applied:

1. On the Settings tab, select Global Settings.
2. For the hypervisor settings, select “VMs have iSCSI direct attached disks or NFS for all the hosts” and update the settings.
13.3 Change Scheduling Frequency of Backup Synchronization with Off-Site Backup Storage

As described in section 4.5, “Backup Retention Management and Housekeeping of Log Backups,” retention management of data backups to an off-site backup storage is handled by ONTAP. SnapCenter periodically checks if ONTAP has deleted backups at the off-site backup storage by running a cleanup job with a weekly default schedule.

The SnapCenter cleanup job deletes backups in the SnapCenter repository as well as in the SAP HANA backup catalog if any deleted backups at the off-site backup storage have been identified.

The cleanup job also executes the housekeeping of SAP HANA log backups.

Until this scheduled cleanup has finished, SAP HANA and SnapCenter might still show backups that have already been deleted from the off-site backup storage.

Note: This might result in additional log backups that are kept, even if the corresponding storage-based Snapshot backups on the off-site backup storage have already been deleted.

The following sections describe two ways to avoid this temporary discrepancy.

Manual Refresh on Resource Level

In the topology view of a resource, SnapCenter displays the backups on the off-site backup storage when selecting the secondary backups, as shown in Figure 39. SnapCenter executes a cleanup operation with the Refresh icon to synchronize the backups for this resource.
Change the Frequency of the SnapCenter Cleanup Job

SnapCenter executes the cleanup job SnapCenter_RemoveSecondaryBackup by default for all resources on a weekly basis using the Windows task scheduling mechanism. This can be changed using a SnapCenter PowerShell cmdlet.

1. Start a PowerShell command window on the SnapCenter Server.
2. Open the connection to the SnapCenter Server using the host name and port of your SnapCenter Server and enter the SnapCenter administrator credentials in the login pop-up window.

   ```powershell
   Open-smconnection -SMSbaseurl https://sc30-v2.sapcc.stl.netapp.com:8146/
   ```

3. To change the schedule from a weekly to a daily basis, use the cmdlet Set-SmSchedule.
4. Check the configuration using the Windows Task Scheduler.

For more information, refer to the SnapCenter 4.0 Cmdlet Reference Guide.
Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites:

- TR-4018: Integrating NetApp ONTAP Systems with SAP Landscape Management
- TR-4646: SAP HANA Disaster Recovery with Asynchronous Storage Replication
- SnapCenter Software 4.0 Installation and Setup Guide
- NetApp Documentation Centers: https://mysupport.netapp.com/info/web/ECMLP2557637.html
- SnapCenter 4.0 Cmdlet Reference Guide
- SAP Support Portal

Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Document Version History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>July 2017</td>
<td>Initial version</td>
</tr>
<tr>
<td>Version 1.1</td>
<td>September 2017</td>
<td>- Added section 12, “Advanced Configuration and Tuning”</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Minor corrections</td>
</tr>
<tr>
<td>Version 2.0</td>
<td>March 2018</td>
<td>Updates to cover SnapCenter 4.0:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- New data volume resource</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Improved SFSR operation</td>
</tr>
</tbody>
</table>
Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Copyright © 2017–2018 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.

TR-4614-0717