



Technical Report

SAP HANA backup and recovery with SnapCenter

Nils Bauer, NetApp
February 2022 | TR-4614

Abstract

This technical report provides best practices for SAP HANA data protection with NetApp® SnapCenter®. This document covers SnapCenter concepts, configuration recommendations, and operation workflows, including configuration, backup operations, and restore and recovery operations.

TABLE OF CONTENTS

Overview	6
The NetApp solution	6
Runtime of Snapshot backups	7
Recovery time objective comparison	8
SnapCenter architecture	10
SnapCenter overview	10
SnapCenter components	11
SnapCenter SAP HANA backup solution	11
Solution components	11
Supported SAP HANA releases and configurations	13
SnapCenter 4.6 enhancements	14
SnapCenter concepts and best practices	15
SAP HANA resource configuration options and concepts	15
Deployment options for the SAP HANA plug-in	16
Data protection strategy	21
Backup operations	23
Backup retention management and housekeeping of data and log backups	25
Capacity requirements for Snapshot backups	27
Restore and recovery operations	27
Lab setup used for this report	31
SnapCenter configuration	32
SnapCenter initial configuration	34
Storage system configuration	34
Credentials configuration	36
SAP HANA plug-in installation on a central plug-in host	37
Policy configuration	38
SnapCenter resource-specific configuration for SAP HANA database backups	43
SAP HANA backup user and hdbuserstore configuration	43
Configuration of data protection to off-site backup storage	46
Manual HANA resource configuration	47
Automatic discovery of HANA databases	49
Resource protection configuration	51

Additional configuration steps for Fibre Channel SAN environments	56
SnapCenter resource-specific configuration for nondata volume backups	57
Configuration of nondata volume resources	58
Resource groups	59
Using SnapCenter together with SAP landscape management.....	60
Database backups	60
Identifying SnapCenter backups in SAP HANA Studio	60
Identifying SnapCenter backups on the storage systems.....	63
On-demand database backup at primary storage.....	64
On-demand database backups with SnapVault replication	66
Block integrity check.....	68
Restore and recovery	71
Automated restore and recovery	71
Single tenant restore and recovery operation	77
Restore with manual recovery	87
Advanced configuration and tuning	103
Enable secure communication to HANA database	103
Disable auto discovery on the HANA plug-in host	103
Deactivate automated log backup housekeeping	104
Disable warning when running SAP HANA plug-in on a virtual environment.....	105
Change scheduling frequency of backup synchronization with off-site backup storage	106
Where to find additional information	108
Version history.....	109

LIST OF TABLES

Table 1) Supported HANA configurations for automatic discovery.....	16
Table 2) Supported HANA configurations for manual HANA resource configuration.	16
Table 3) Summary of SAP HANA plug-in deployment options.	20
Table 4) Data protection parameters.....	22
Table 5) Policies based on data protection parameters.	22
Table 6) Restore operation characteristics.....	28
Table 7) Restore and recovery operations, dependent on resource configuration option.	30

LIST OF FIGURES

Figure 1) Backup solution overview.....	7
Figure 2) Customer example of Snapshot backup runtime.....	8
Figure 3) RTO for a 2TB database with file-based backups.....	9
Figure 4) RTO for a 2TB database with Snapshot backups.....	9
Figure 5) RTO comparison: file-based backup versus Snapshot copy backup.....	10
Figure 6) SnapCenter components.....	11
Figure 7) Backup solution overview.....	13
Figure 8) HANA System Replication support with SnapCenter 4.6.....	14
Figure 9) HANA plug-in deployment options dependencies.....	15
Figure 10) SnapCenter communication.....	17
Figure 11) SnapCenter Server as a central HANA plug-in host.....	17
Figure 12) Separate Linux host as a central HANA plug-in host.....	18
Figure 13) HANA plug-in on Individual database hosts.....	19
Figure 14) Mixed plug-in deployment with SnapCenter server as central plug-in host.....	20
Figure 15) Mixed configuration with separate Linux host as central plug-in host.....	20
Figure 16) Overview of HANA Snapshot backup workflow.....	24
Figure 17) Retention management and log backup housekeeping.....	25
Figure 18) Restore and recovery operations for auto discovered resources—MDC single tenant.....	29
Figure 19) Restore and recovery operations for auto discovered resources—MDC multiple tenants.....	30
Figure 20) Restore and recovery operations for manual configured resources.....	30
Figure 21) Lab setup.....	32
Figure 22) Overview of configuration steps and dependencies.....	33
Figure 23) Configured credentials.....	37
Figure 24) Configured hosts.....	38
Figure 25) Policies summary.....	43
Figure 26) Database user for SAP HANA backups.....	44
Figure 27) Protection relationship.....	46
Figure 28) Protection policy.....	47
Figure 29) Configuration of Post Quiesce command.....	57
Figure 30) Nondata volume resources.....	59
Figure 31) SnapCenter topology view.....	61
Figure 32) SAP HANA backup catalog for the system database.....	62
Figure 33) SAP HANA backup catalog for tenant database.....	62
Figure 34) Backups at the primary storage.....	63
Figure 35) Backups at the secondary storage.....	64
Figure 36) Block integrity check.....	69
Figure 37) File-based backup for system database in SAP HANA Studio.....	70
Figure 38) PowerShell command to disable log backup housekeeping.....	105

Figure 39) SnapCenter warning to configure hypervisor.	105
Figure 40) Disable hypervisor settings.	106
Figure 41) Refresh secondary backups.....	107

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.

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 RTO is reduced to several minutes rather than the several hours required for conventional single-cycle tape backups.

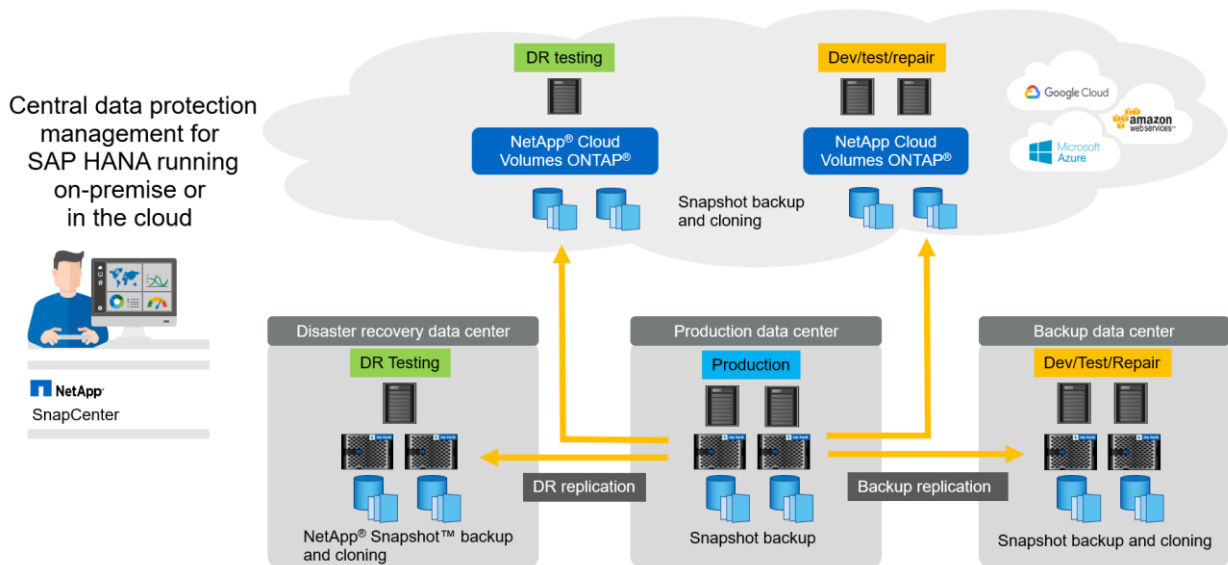
Snapshot copy backups are stored on the same disk system as the active online data. Therefore, NetApp recommends using Snapshot copy backups as a supplement rather than a replacement for backups to a secondary location. Most restore and recovery actions are handled by using SnapRestore on the primary 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.

The solution can also be seamlessly extended to a hybrid cloud operation model. Data replication for disaster recovery or offsite backup purposes can be done from on-premises NetApp ONTAP® systems to Cloud Volumes ONTAP instances running in the cloud. You can use SnapCenter as a central tool to manage the data protection and data replication, independent if the SAP HANA system run on-premises or in the cloud. Figure 1 shows an overview of the backup solution.

Figure 1) Backup solution overview.

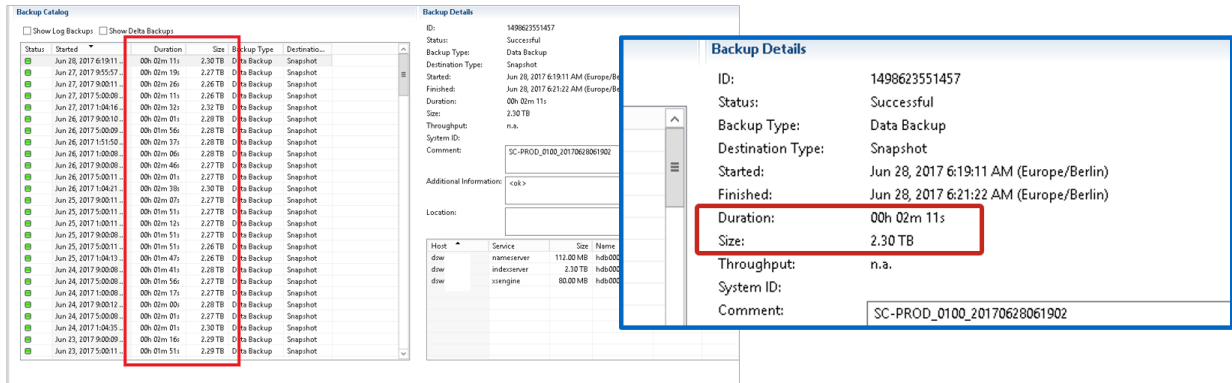


Runtime of Snapshot backups

Figure 2 shows a customer's HANA Studio running SAP HANA on NetApp storage. The customer is using Snapshot copies to back up the HANA database. The image shows that the HANA database (approximately 2.3TB in size) is backed up in 2 minutes and 11 seconds by using Snapshot backup technology.

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

Figure 2) Customer example of Snapshot backup runtime.



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 = $\frac{1}{4}$).

Figure 3 shows an RTO example for a 1TB database when file-based data backups are used. In this example, a backup is taken once per day. The RTO differs depending on when the restore and recovery were performed. If the restore and recovery were performed immediately after a backup was taken, the RTO is primarily based on the restore time, which is 1 hour and 10 minutes in the example. The recovery time increased to 2 hours and 50 minutes when restore and recovery were performed immediately before the next backup was taken, and the maximum RTO was 4 hours and 30 minutes.

Figure 3) RTO for a 2TB database with file-based backups.

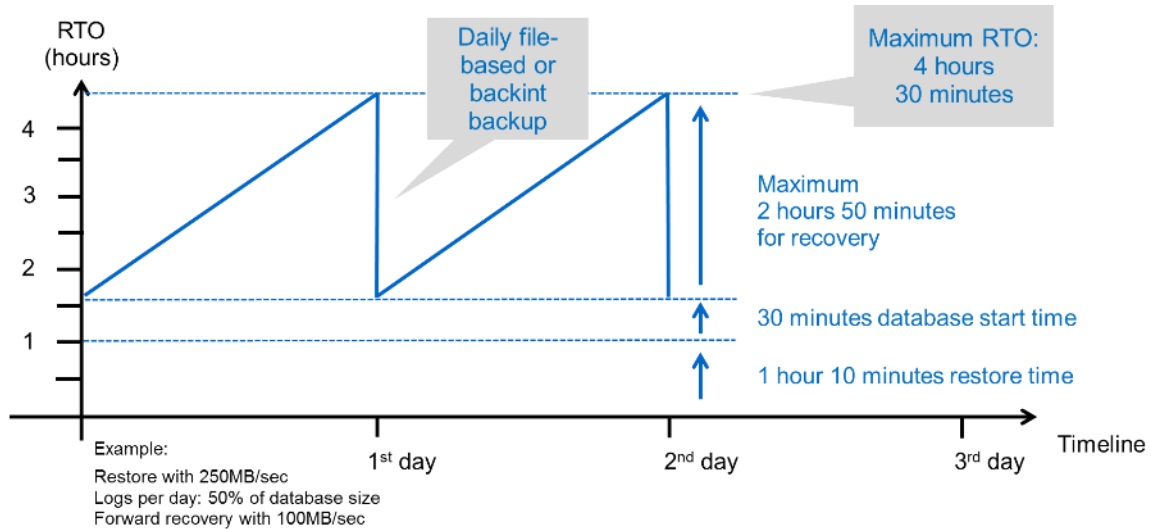


Figure 4 shows an RTO example for a 1TB database when Snapshot backups are used. With storage-based Snapshot backups, the RTO only depends on the database start time and the forward recovery time because the restore is completed in a few seconds, independent of the size of the database. The forward recovery time also increases depending on when the restore and recovery are done, but due to the higher frequency of backups (every six 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 4) RTO for a 2TB database with Snapshot backups.

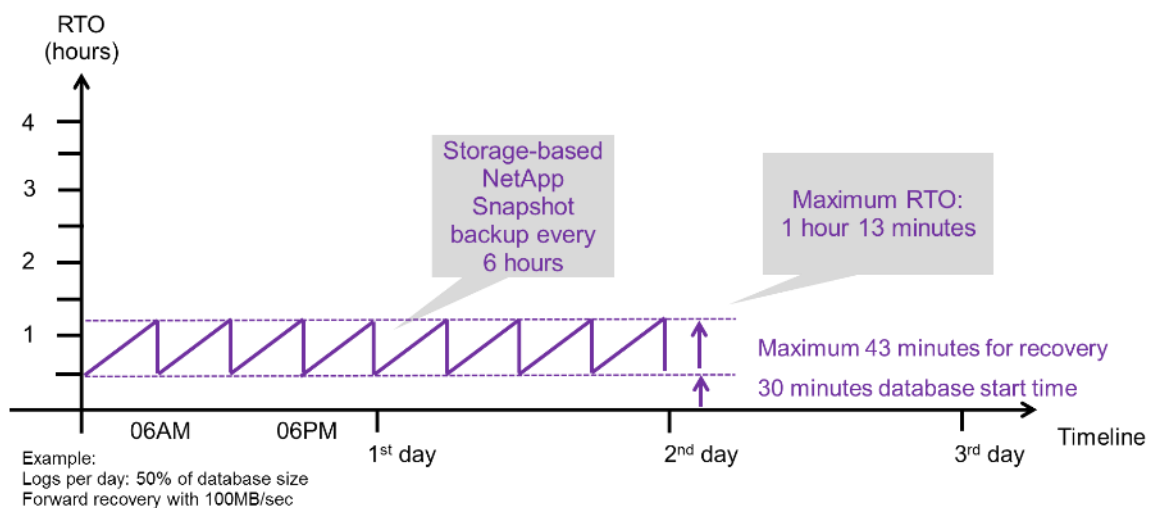
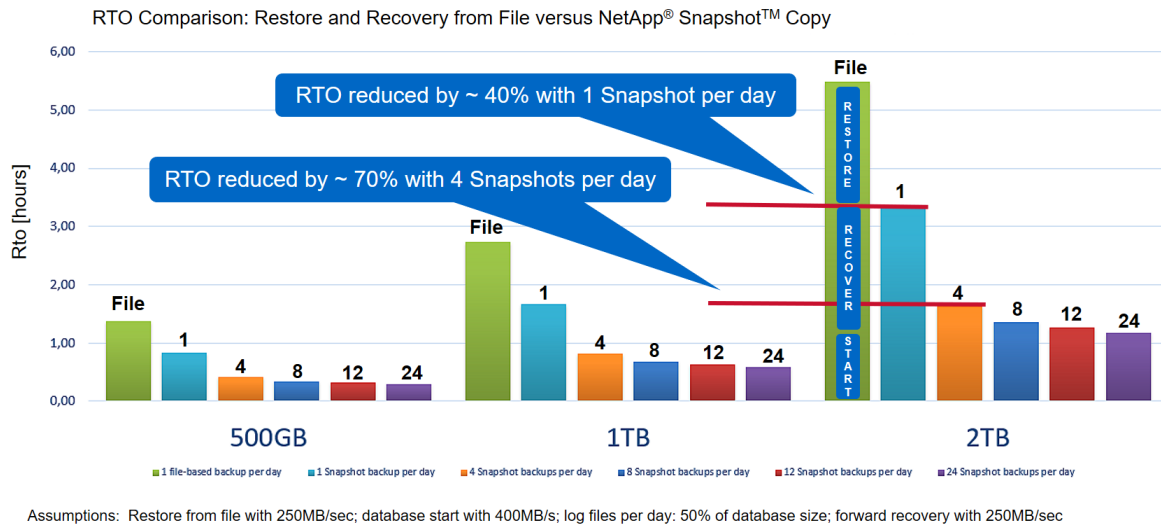


Figure 5 shows an RTO comparison of file-based and storage-based Snapshot backups for different database sizes and different frequencies of Snapshot backups. The green bar shows the file-based backup. The other bars show Snapshot copy backups with different backup frequencies.

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

Figure 5) 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.

SnapCenter architecture

SnapCenter overview

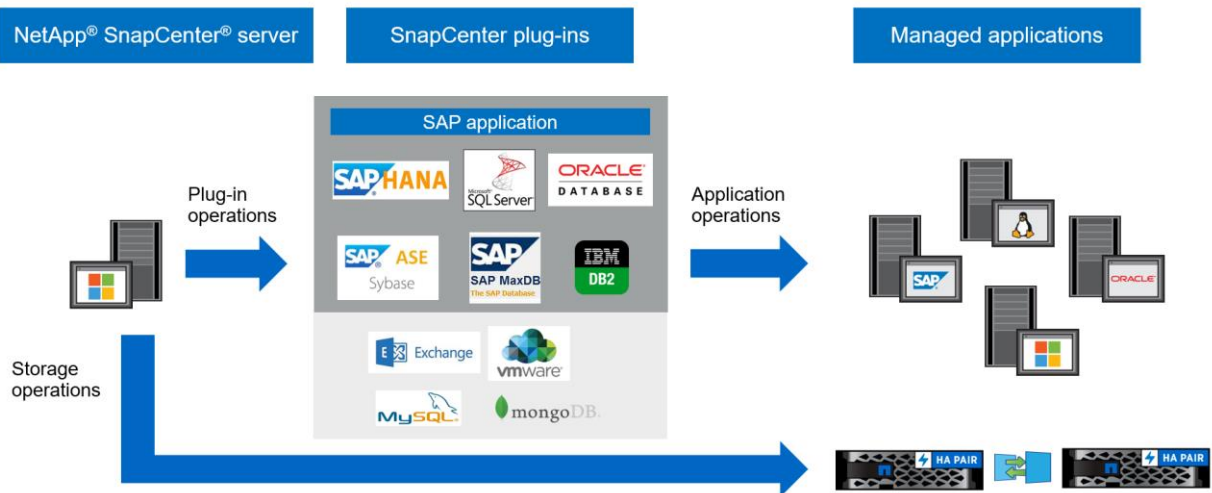
SnapCenter is a unified, scalable platform for application-consistent data protection. SnapCenter provides centralized control and oversight, while delegating the ability for users to manage application-specific backup, restore, and clone jobs. With SnapCenter, database and storage administrators learn a single tool to manage backup, restore, and cloning operations for a variety of applications and databases. SnapCenter manages data across endpoints in the data fabric powered by NetApp. 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.

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.

Figure 6) SnapCenter components.



SnapCenter SAP HANA backup solution

Solution components

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

- SAP HANA data backup with storage-based Snapshot copies:
 - Backup scheduling
 - Retention management
 - Housekeeping of the SAP HANA backup catalog
- Nondata volume (for example, /hana/shared) backup with storage-based Snapshot copies:
 - Backup scheduling
 - Retention management
- Replication to an off-site backup or disaster recovery location:
 - SAP HANA data Snapshot backups
 - Nondata volumes
 - Retention management configured at off-site backup storage
 - Housekeeping of the SAP HANA backup catalog
- Database block integrity checks using a file-based backup:
 - Backup scheduling
 - Retention management
 - Housekeeping of the SAP HANA backup catalog

- Retention management of HANA database log backup:
 - Retention management based on data backup retention
 - Housekeeping of the SAP HANA backup catalog
- Automatic discovery of HANA databases
- Automated restore and recovery
- Single tenant restore operations with SAP HANA multitenant database container (MDC) systems

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 the NetApp SnapMirror® feature. 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:

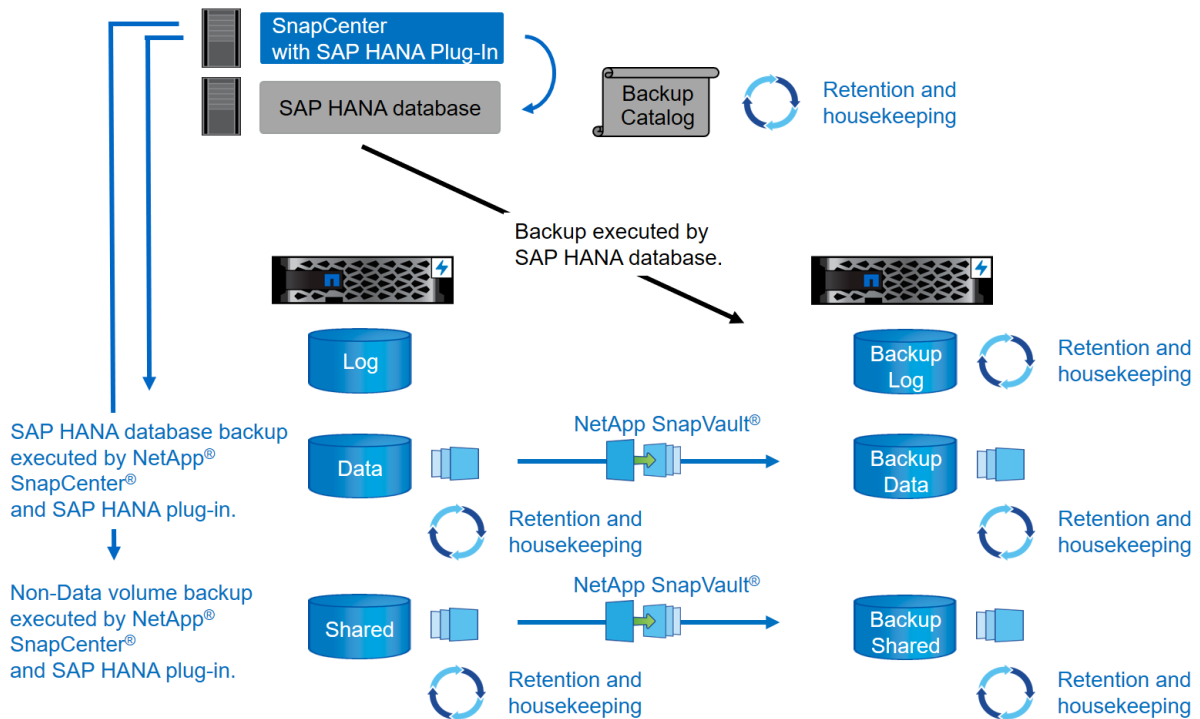
- The log backup is written to a storage system that synchronously mirrors the data to a second location with NetApp MetroCluster™ high-availability (HA) and disaster recovery storage software.
- The log backup destination can be configured on the same primary storage system and then replicated synchronously or 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 7 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.

Figure 7) Backup solution overview.



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 back up 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 or off-site backup 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.

Supported SAP HANA releases and configurations

SnapCenter supports SAP HANA single-host and multiple-host configurations using NFS- or FC-attached NetApp storage systems (AFF and FAS), as well as SAP HANA systems running on Cloud Volumes ONTAP at AWS, Azure, Google Cloud Platform, and AWS FSx ONTAP using NFS.

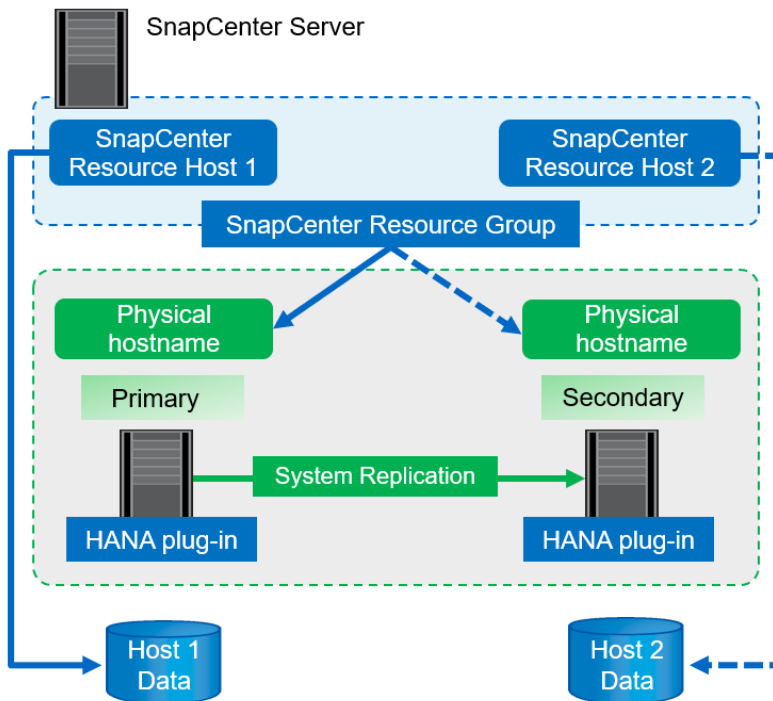
SnapCenter supports the following SAP HANA architectures and releases:

- SAP HANA single container:
 - SAP HANA 1.0 SPS12
- SAP HANA multitenant-database container (MDC) single tenant:
 - SAP HANA 2.0 SPS3 and later
- SAP HANA multitenant-database container (MDC) multiple tenants:
 - SAP HANA 2.0 SPS4 and later

SnapCenter 4.6 enhancements

Starting with release 4.6, SnapCenter supports auto discovery of HANA systems configured in a HANA System Replication relationship. Each host is configured using its physical IP address (host name) and its individual data volume on the storage layer. The two SnapCenter resources are combined in a resource group and SnapCenter automatically identifies which host is primary or secondary and executes the required backup operations accordingly. Retention management for Snapshot and file-based backups created with SnapCenter is done across both hosts to ensure that old backups also get deleted at the current secondary host. Figure 8 shows a high-level overview. For a detailed description of the configuration and operation of HANA System Replication enabled HANA systems in SnapCenter, see [TR-4719: SAP HANA System Replication, Backup and Recovery with SnapCenter](#).

Figure 8) HANA System Replication support with SnapCenter 4.6



SnapCenter concepts and best practices

SAP HANA resource configuration options and concepts

With SnapCenter, the SAP HANA database resource configuration can be done with two different approaches.

- **Manual resource configuration**
HANA resource and storage footprint information must be provided manually.
- **Automatic discovery of HANA resources**
Automatic discovery simplifies the configuration of HANA databases in SnapCenter and enables automated restore and recovery.

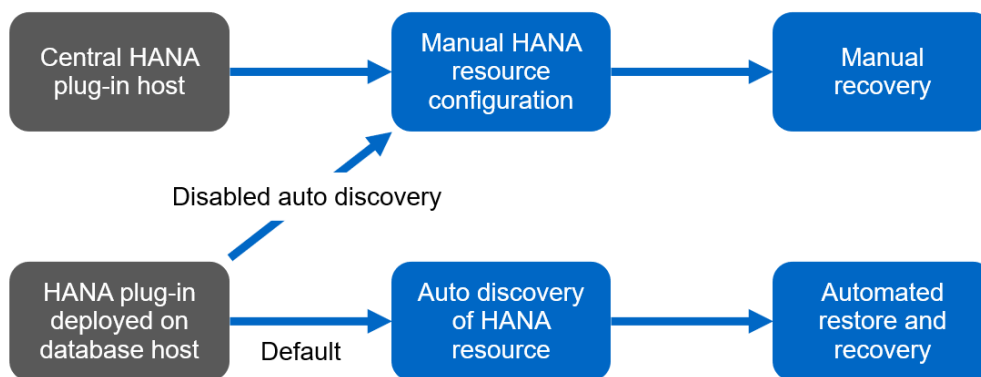
It is important to understand that only HANA database resources in SnapCenter that have been automatically discovered are enabled for automated restore and recovery. HANA database resources that are configured manually in SnapCenter must be recovered manually after a restore operation in SnapCenter.

On the other hand, automatic discovery with SnapCenter is not supported for all HANA architectures and infrastructure configurations. Therefore, HANA landscapes might require a mixed approach, where some HANA systems (HANA multiple host systems) require a manual resource configuration and all others can be configured using automatic discovery.

Automatic discovery and automated restore and recovery depend on the ability to execute OS commands on the database host. Examples of this are file system and storage footprint discovery, and unmount, mount, or LUN discovery operations. These operations are executed with the SnapCenter Linux plug-in, which is automatically deployed together with the HANA plug-in. Therefore, it is pre-requisite to deploy the HANA plug-in on the database host to enable automatic discovery as well as automated restore and recovery. It is also possible to disable the auto discovery after the deployment of the HANA plug-in on the database host. In this instance, the resource will be a manually configured resource.

Figure 9 summarizes the dependencies. More details on the HANA deployment options are covered in the “Deployment options for the SAP HANA plug-in” section.

Figure 9) HANA plug-in deployment options dependencies.



Note: The HANA and Linux plug-ins are currently only available for Intel-based systems. If the HANA databases are running on IBM Power Systems, a central HANA plug-in host must be used.

Supported HANA architectures for automatic discovery and automated recovery

With SnapCenter, automatic discovery and automated restore and recovery is supported for most HANA configurations, with the exception that HANA multiple host systems require a manual configuration.

Table 1) Supported HANA configurations for automatic discovery.

HANA plug-in installed on	HANA architecture	HANA system configuration	Infrastructure
HANA database host	Single host	<ul style="list-style-type: none">• HANA single container• SAP HANA multitenant database containers (MDC) with single or multiple tenants• HANA System Replication	<ul style="list-style-type: none">• Bare metal with NFS• Bare metal with XFS and FC with or without Linux Logical Volume Manager (LVM)• VMware with direct OS NFS mounts

Note: With the current SnapCenter release, HANA MDC systems with multiple tenants are supported for automatic discovery but not for automated restore and recovery.

Supported HANA architectures for manual HANA resource configuration

Manual configuration of HANA resources is supported for all HANA architectures but requires a central HANA plug-in host. The central plug-in host can be the SnapCenter server itself, or a separate Linux or Windows host.

Note: When the HANA plug-in is deployed on the HANA database host, by default, the resource is auto discovered. Auto discovery can be disabled for individual hosts, so that the plug-in can be deployed; for example, on a database host with activated HANA System Replication and a SnapCenter release < 4.6, where auto discovery is not supported. For more information, see the “Disable auto discovery on the HANA plug-in host” section.

Table 2) Supported HANA configurations for manual HANA resource configuration.

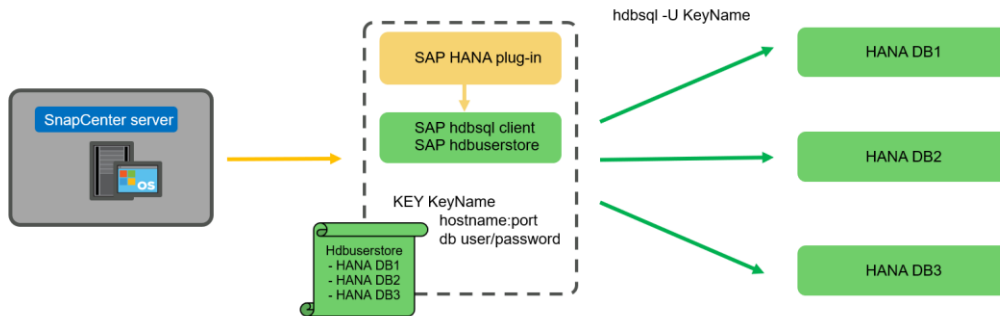
HANA Plug-In installed on	HANA architecture	HANA system configuration	Infrastructure
Central plug-in host (SnapCenter Server or separate Linux host)	Single or multiple host	<ul style="list-style-type: none">• HANA single container• HANA MDC with single or multiple tenants• HANA System Replication	<ul style="list-style-type: none">• Bare metal with NFS• Bare metal with XFS and FC with or without Linux LVM• VMware with direct OS NFS mounts

Deployment options for the SAP HANA plug-in

Figure 10 shows the logical view and the communication between the SnapCenter Server and the 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.

Figure 10) SnapCenter communication.



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 central plug-in host, or the individual SAP HANA database hosts.

SnapCenter server high availability

SnapCenter can be set up in a two-node HA configuration. In such a configuration, a load balancer (for example, F5) is used in an active/passive mode using a virtual IP address pointing to the active SnapCenter host. The SnapCenter repository, the MySQL database, is replicated by SnapCenter between the two hosts so that the SnapCenter data is always in-sync.

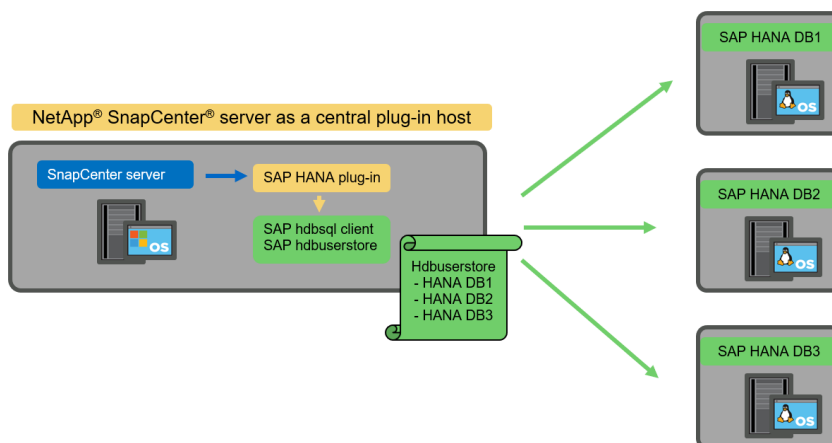
SnapCenter server HA is not supported if the HANA plug-in is installed on the SnapCenter server. If you plan to set up SnapCenter in an HA configuration, do not install the HANA plug-in on the SnapCenter server. More details on SnapCenter HA can be found at

https://kb.netapp.com/app/answers/answer_view/a_id/1096983

SnapCenter server as a central HANA plug-in host

Figure 11 shows a configuration in which the SnapCenter Server is used as a central plug-in host. The SAP HANA plug-in and the SAP hdbsql client software are installed on the SnapCenter Server.

Figure 11) SnapCenter Server as a central HANA plug-in host.



Since the HANA plug-in can communicate with the managed HANA databases using the hdbclient through the network, you do not need to install any SnapCenter components on the individual HANA database hosts. SnapCenter can protect the HANA databases by using a central HANA plug-in host on which all userstore keys are configured for the managed databases.

On the other hand, enhanced workflow automation for automatic discovery, automation of restore and recovery, as well as SAP system refresh operations require SnapCenter components to be installed on the database host. When using a central HANA plug-in host, these features are not available.

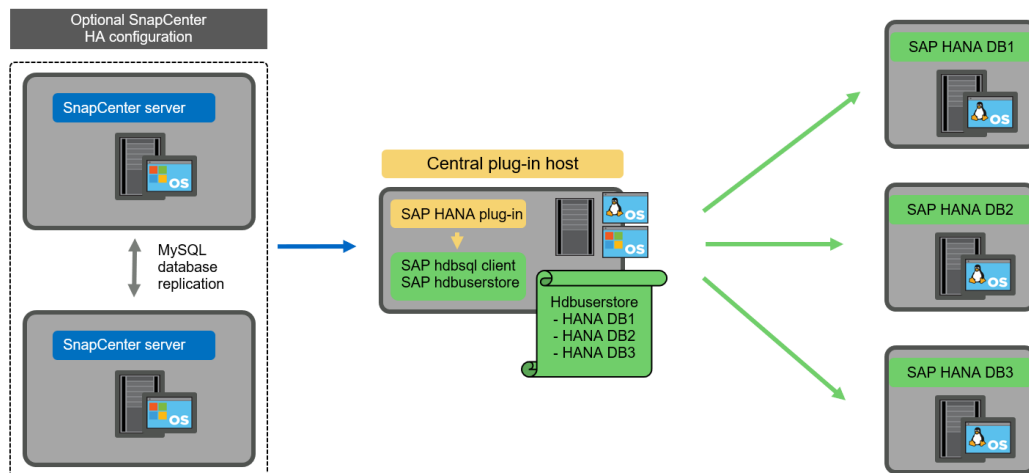
Also, high availability of the SnapCenter server using the in-build HA feature cannot be used when the HANA plug-in is installed on the SnapCenter server. High availability can be achieved using VMware HA if the SnapCenter server is running in a VM within a VMware cluster.

Separate host as a central HANA plug-in host

Figure 12 shows a configuration in which a separate Linux host is used as a central plug-in host. In this case, the SAP HANA plug-in and the SAP hdbsql client software are installed on the Linux host.

Note: The separate central plug-in host can also be a Windows host.

Figure 12) Separate Linux host as a central HANA plug-in host.



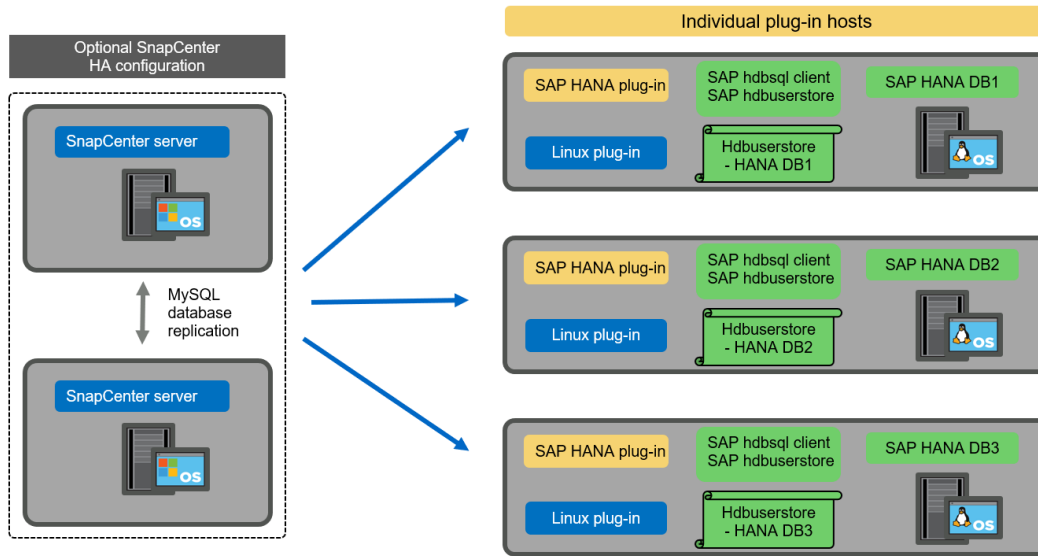
The same restriction regarding feature availability described in the previous section also applies for a separate central plug-in host.

However, with this deployment option the SnapCenter server can be configured with the in-build HA functionality. The central plug-in host must also be HA, for example, by using a Linux cluster solution.

HANA plug-in deployed on individual HANA database hosts

Figure 13 shows a configuration in which the SAP HANA plug-in is installed on each SAP HANA database host.

Figure 13) HANA plug-in on Individual database hosts.



When the HANA plug-in is installed on each individual HANA database host, all features, such as automatic discovery and automated restore and recovery, are available. Also, the SnapCenter server can be set up in an HA configuration

Mixed HANA plug-in deployment

As discussed at the beginning of this section, some HANA system configurations, such as multiple-host systems, require a central plug-in host. Therefore, most SnapCenter configurations require a mixed deployment of the HANA plug-in.

It is recommended that you deploy the HANA plug-in on the HANA database host for all HANA system configurations that are supported for automatic discovery. Other HANA systems, such as multiple-host configurations, should be managed with a central HANA plug-in host.

Figure 14 and Figure 15 show mixed plug-in deployments either with the SnapCenter server or a separate Linux host as a central plug-in host. The only difference between these two deployments is the optional HA configuration.

Figure 14) Mixed plug-in deployment with SnapCenter server as central plug-in host.

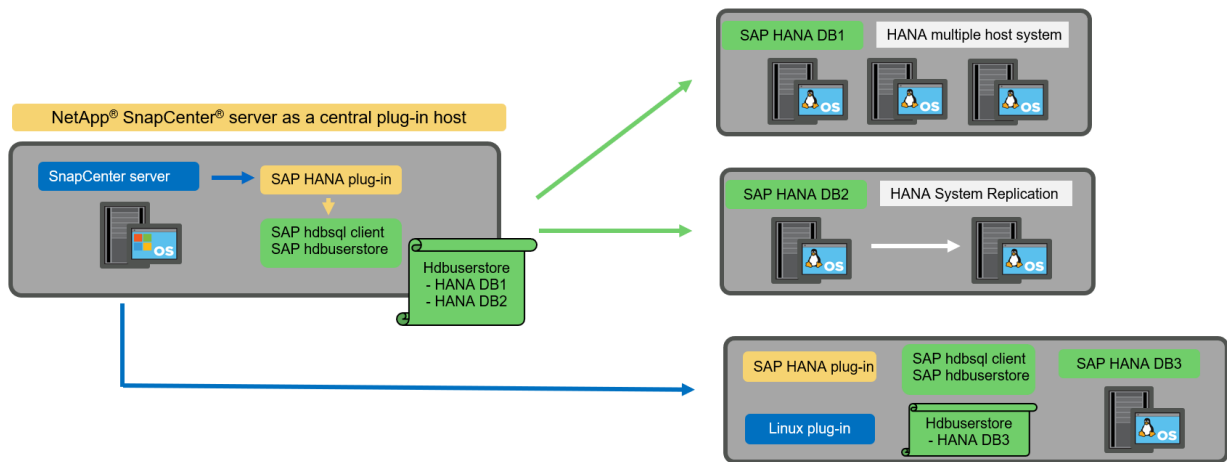
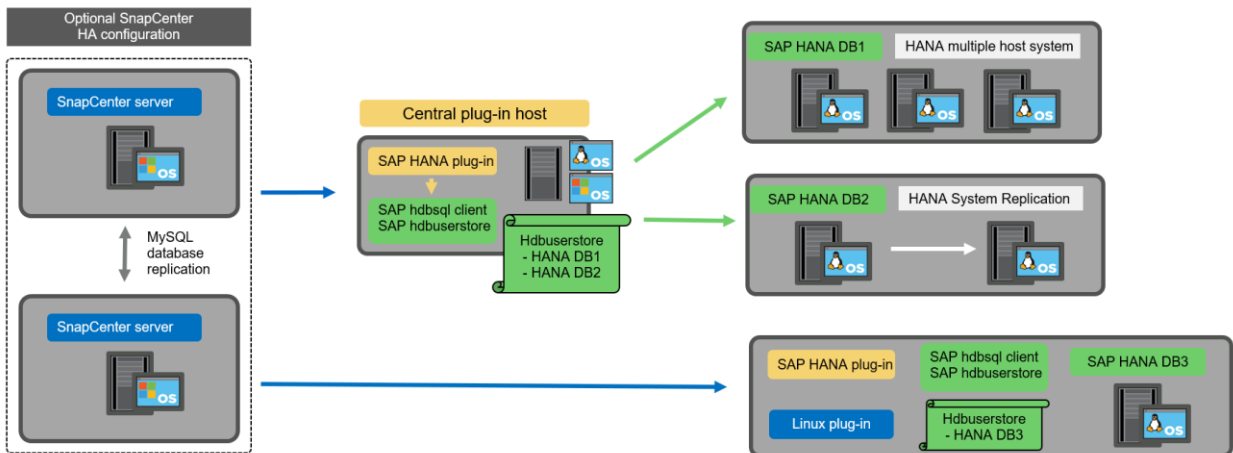


Figure 15) Mixed configuration with separate Linux host as central plug-in host.



Summary and recommendations

In general, it is recommended that you deploy the HANA plug-in on each SAP HANA host to enable all available SnapCenter HANA features and to enhance workflow automation.

Note: The HANA and Linux plug-ins are currently only available for Intel-based systems. If the HANA databases are running on IBM Power Systems, a central HANA plug-in host must be used.

For HANA configurations in which automatic discovery is not supported, such as HANA multiple-host configurations, an additional central HANA plug-in host must be configured. The central plug-in host can be the SnapCenter server if VMware HA can be leveraged for SnapCenter HA. If you plan to use the SnapCenter in-built HA capability, use a separate Linux plug-in host.

Table 3 summarizes the different deployment options.

Table 3) Summary of SAP HANA plug-in deployment options.

Deployment option	Dependencies
Central HANA plug-in host	Pros: <ul style="list-style-type: none"> Single HANA plug-in, central HDB user store configuration

Deployment option	Dependencies
Plug-in installed on SnapCenter server	<ul style="list-style-type: none"> • No SnapCenter software components required on individual HANA database hosts • Support of all HANA architectures Cons: <ul style="list-style-type: none"> • Manual resource configuration • Manual recovery • No single tenant restore support • Any Pre- and post-script steps are executed on the central plug-in host • In-build SnapCenter high availability not supported • Combination of SID and tenant name must be unique across all managed HANA databases • Log backup retention management enabled/disabled for all managed HANA databases
Central HANA plug-in host Plug-in installed on separate Linux or Windows server	Pros: <ul style="list-style-type: none"> • Single HANA plug-in, central HDB user store configuration • No SnapCenter software components required on individual HANA database hosts • Support of all HANA architectures • In-build SnapCenter high availability supported Cons: <ul style="list-style-type: none"> • Manual resource configuration • Manual recovery • No single tenant restore support • Any Pre- and post-script steps are executed on the central plug-in host • Combination of SID and tenant name must be unique across all managed HANA databases • Log backup retention management enabled/disabled for all managed HANA databases
Individual HANA plug-in host Plug-in installed on HANA database server	Pros: <ul style="list-style-type: none"> • Automatic discovery of HANA resources • Automated restore and recovery • Single tenant restore • Pre- and post-script automation for SAP system refresh • In-build SnapCenter high availability supported • Log backup retention management can be enabled/disabled for each individual HANA database Cons: <ul style="list-style-type: none"> • Not supported for all HANA architectures. Additional central plug-in host required for HANA multiple host systems. • HANA plug-in must be deployed on each HANA database hosts

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 4 shows an example of data protection parameters for the system type's production, development, and test. For the production system, a high backup frequency has been defined, and 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 4) Data protection parameters.

Parameters	Production systems	Development systems	Test systems
Backup frequency	Every 4 hours	Every 4 hours	Every 4 hours
Primary retention	2 days	2 days	2 days
Block integrity check	Once per week	Once per week	No
Replication to off-site backup site	Once per day	Once per day	No
Off-site backup retention	2 weeks	2 weeks	Not applicable

Table 5 shows the policies that must be configured for the data protection parameters.

Table 5) Policies based on data protection parameters.

Parameters	Policy LocalSnap	Policy LocalSnapAndSnapVault	Policy BlockIntegrityCheck
Backup type	Snapshot based	Snapshot based	File based
Schedule frequency	Hourly	Daily	Weekly
Primary retention	Count = 12	Count = 3	Count = 1
SnapVault replication	No	Yes	Not applicable

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 protection 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 protection 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 protection 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 must 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 nondata volume resources are not different.

Backup operations

SAP introduced the support of Snapshot backups for MDC multiple tenant systems with HANA 2.0 SPS4. SnapCenter supports Snapshot backup operations of HANA MDC systems with multiple tenants. SnapCenter also supports two different restore operations of a HANA MDC system. You can either restore the complete system, the System DB and all tenants, or you can restore just a single tenant. There are some pre-requisites to enable SnapCenter to execute these operations.

In an MDC System, the tenant configuration is not necessarily static. Tenants can be added or tenants can be deleted. SnapCenter cannot rely on the configuration that is discovered when the HANA database is added to SnapCenter. SnapCenter must know which tenants are available at the point in time the backup operation is executed.

In order to enable a single tenant restore operation, SnapCenter must know which tenants are included in each Snapshot backup. In addition, it is required to know which files and directories belong to each tenant included in the Snapshot backup.

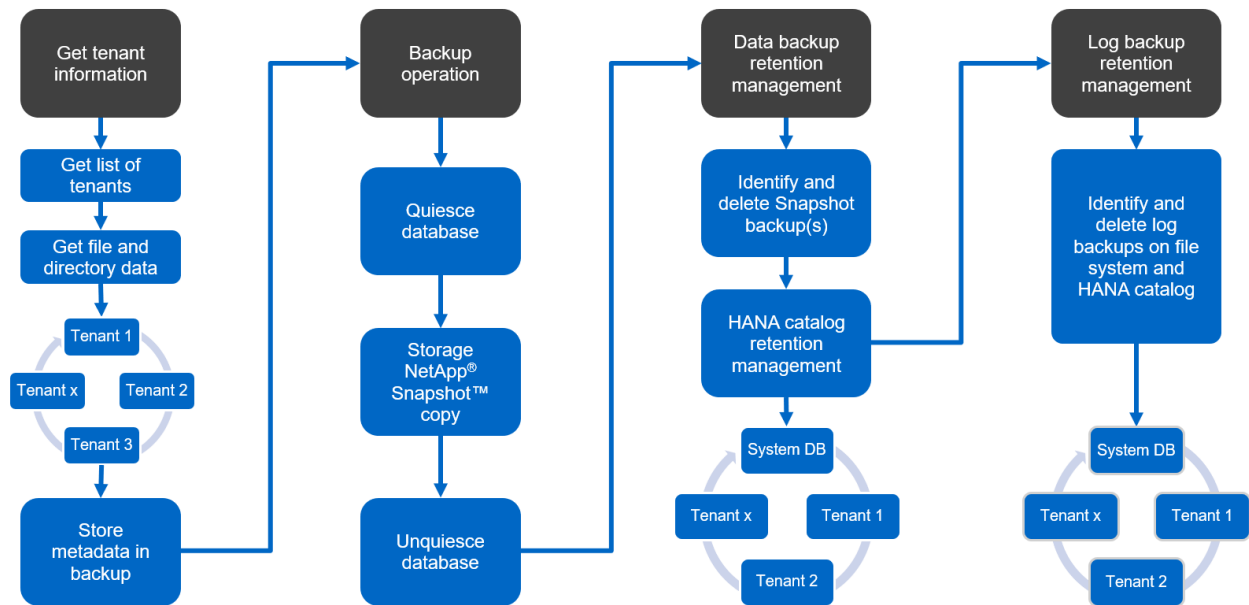
Therefore, with each backup operation, the first step in the workflow is to get the tenant information. This includes the tenant names and the corresponding file and directory information. This data must be stored in the Snapshot backup metadata in order to be able to support a single tenant restore operation. The next step is the Snapshot backup operation itself. This step includes the SQL command to trigger the HANA backup savepoint, the storage Snapshot backup, and the SQL command to close the Snapshot operation. By using the close command, the HANA database updates the backup catalog of the system DB and each tenant.

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

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

Figure 16 shows an overview of the backup workflow.

Figure 16) Overview of HANA Snapshot backup workflow.



Backup workflow for Snapshot backups of the HANA database

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

1. SnapCenter reads the list of tenants from the HANA database.
2. SnapCenter reads the files and directories for each tenant from the HANA database.
3. Tenant information is stored in the SnapCenter metadata for this backup operation.
4. 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 or multiple tenant system, a synchronized global backup save point for the system database, and for each tenant database is created.
5. 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.
6. SnapCenter registers the storage Snapshot backup in the SAP HANA backup catalog.
7. SnapCenter deletes the SAP HANA backup save point.
8. 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.
9. 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. HANA backup catalog operations are done for the system database and all tenants.

Note: If the backup is still available at the secondary storage, the SAP HANA catalog entry is not deleted.
10. 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. These operations are done for the system database and all tenants.

Note: This step is only executed if log backup housekeeping is not disabled.

Backup workflow for block integrity check operations

SnapCenter executes the block integrity check in the following sequence:

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

Note: This step is only executed if log backup housekeeping is not disabled.

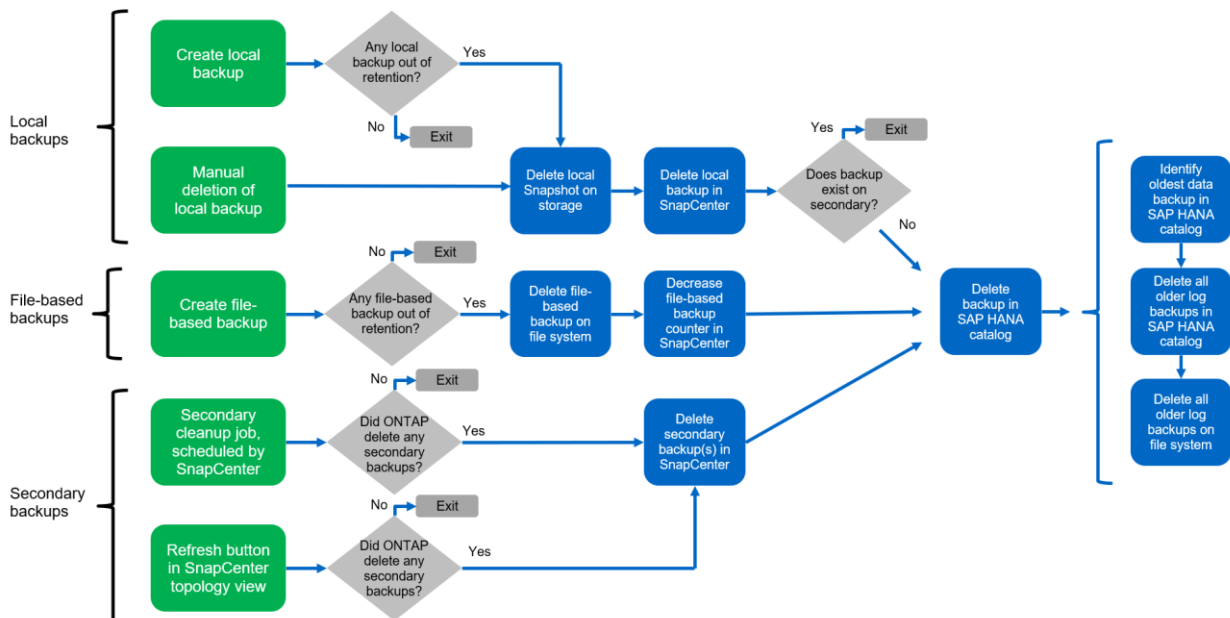
Backup retention management and housekeeping of data and log backups

The data 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 17 provides an overview of the different workflows and the dependencies of each operation. The following sections describe the different operations in detail.

Figure 17) Retention management and log backup housekeeping.



Retention management of local backups at the primary storage

SnapCenter handles the housekeeping of SAP HANA database backups and nondata 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 the section titled “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 the “Disable auto discovery on the HANA plug-in host” section.

Capacity requirements for Snapshot backups

You must consider the higher block change rate on the storage layer relative to the change rate with traditional databases. Due to the HANA table merge process of the column store, the complete table is written to disk, not just the changed blocks.

Data from our customer base shows a daily change rate between 20% and 50% if multiple Snapshot backups are taken during the day. At the SnapVault target, if the replication is done only once per day, the daily change rate is typically smaller.

Restore and recovery operations

Restore operations with SnapCenter

From the HANA database perspective, SnapCenter supports two different restore operations.

1. Restore of the complete resource
All data of the HANA system will be restored. If the HANA system contains one or more tenants, the data of the system database and the data of all tenants are restored.
2. Restore of a single tenant
Only the data of the selected tenant will be restored.

From the storage perspective, the above restore operations must be executed differently depending on the used storage protocol (NFS, or Fibre Channel SAN), the configured data protection (primary storage with or without offsite backup storage), and the selected backup to be used for the restore operation (restore from primary or offsite backup storage).

Restore of complete resource from primary storage

When restoring the complete resource from primary storage, SnapCenter supports two different ONTAP features to execute the restore operation. You can choose between the following two features:

- **Volume-based SnapRestore.** A volume-based SnapRestore reverts the content of the storage volume to the state of the selected Snapshot backup.
 - Volume Revert check box available for auto discovered resources using NFS
 - Complete Resource radio button for manual configured resources
- **File-based SnapRestore.** A file-based SnapRestore, also known as Single File SnapRestore, restores all individual files (NFS), or all LUNs (SAN).
 - Default restore method for auto discovered resources.
Can be changed using the Volume revert check box for NFS

- File level radio button for manual configured resources

Table 6 provides a comparison of the different restore methods.

Table 6) Restore operation characteristics.

	Volume-based SnapRestore	File-based SnapRestore
Speed of restore operation	Very fast, independent of the volume size	Very fast restore operation but uses background copy job on the storage system, which blocks the creation of new Snapshot backups
Snapshot backup history	Restore to an older Snapshot backup, removes all newer Snapshot backups.	No influence
Restore of directory structure	Directory structure is also restored	NFS: 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 SAN: Directory structure is also restored
Resource configured with replication to offsite backup storage	A volume-based restore cannot be done to a Snapshot copy backup that is older than the Snapshot copy used for SnapVault synchronization	Any Snapshot backup can be selected

Restore of complete resource from offsite backup storage

A restore from the offsite backup storage is always executed using a SnapVault restore operation where all files or all LUNs of the storage volume are overwritten with the content of the Snapshot backup.

Restore of a single tenant

Restoring a single tenant requires a file-based restore operation. Depending on the used storage protocol, different restore workflows are executed by SnapCenter.

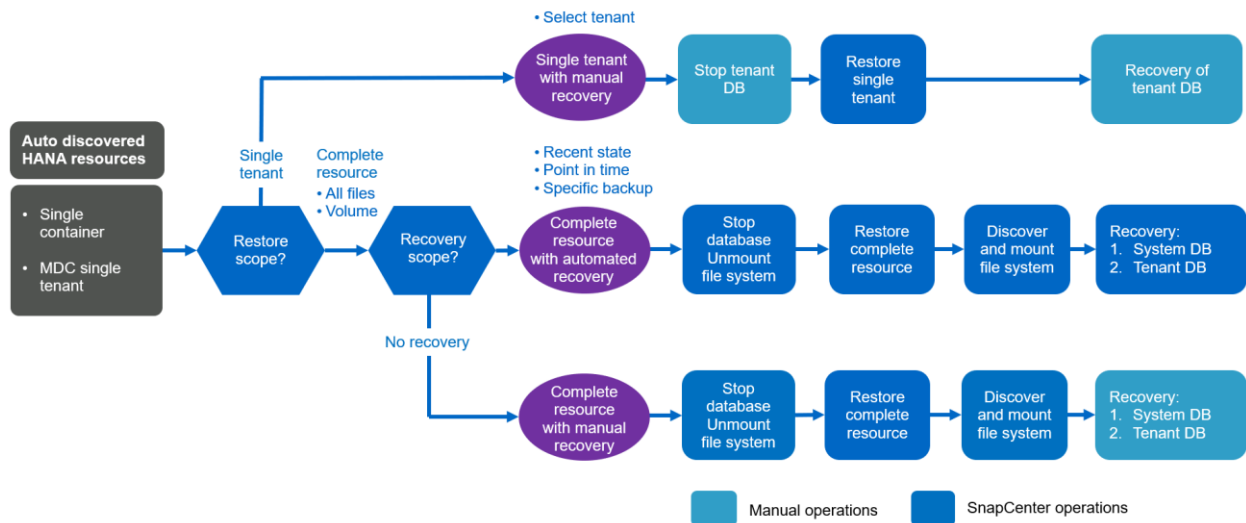
- NFS:
 - Primary storage: File-based SnapRestore operations are executed for all files of the tenant database.
 - Offsite backup storage: SnapVault restore operations are executed for all files of the tenant database.
- SAN:
 - Primary storage: Clone and connect the LUN to the database host and copy all files of the tenant database.
 - Offsite backup storage: Clone and connect the LUN to the database host and copy all files of the tenant database.

Restore and recovery of auto discovered HANA single container and MDC single tenant systems

HANA single container and HANA MDC single tenant systems that have been auto discovered are enabled for automated restore and recovery with SnapCenter. For these HANA systems, SnapCenter supports three different restore and recovery workflows, as shown in Figure 18:

- **Single tenant with manual recovery**
If you select a single tenant restore operation, SnapCenter lists all tenants that are included in the selected Snapshot backup. You must stop and recover the tenant database manually. The restore operation with SnapCenter is done with single file SnapRestore operations for NFS, or clone, mount, copy operations for SAN environments.
- **Complete resource with automated recovery**
If you select a complete resource restore operation and automated recovery, the complete workflow is automated with SnapCenter. SnapCenter supports up to recent state, point in time, or to specific backup recovery operations. The selected recovery operation is used for the system and the tenant database.
- **Complete resource with manual recovery**
If you select No Recovery, SnapCenter stops the HANA database and executes the required file system (unmount, mount) and restore operations. You must recover the system and tenant database manually.

Figure 18) Restore and recovery operations for auto discovered resources—MDC single tenant.



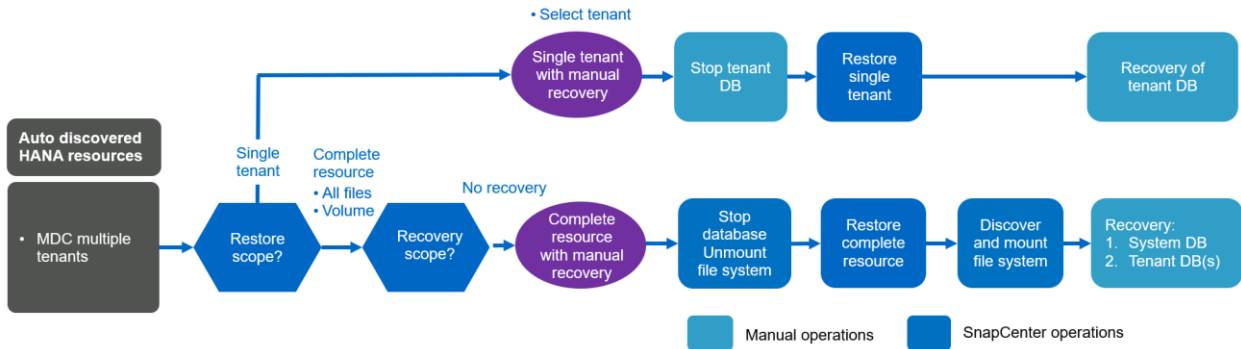
Restore and recovery of automatically discovered HANA MDC multiple tenant systems

Even though HANA MDC systems with multiple tenants can be automatically discovered, automated restore and recovery is not supported with the current SnapCenter release. For MDC systems with multiple tenants, SnapCenter supports two different restore and recovery workflows, as shown in Figure 19:

- Single tenant with manual recovery
- Complete resource with manual recovery

The workflows are the same as described in the previous section.

Figure 19) Restore and recovery operations for auto discovered resources—MDC multiple tenants.

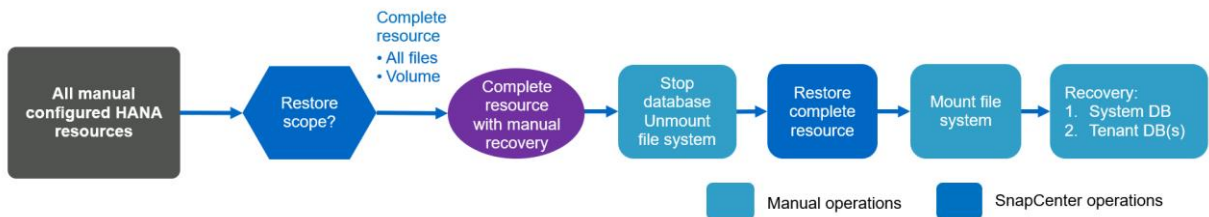


Restore and recovery of manual configured HANA resources

Manual configured HANA resources are not enabled for automated restore and recovery. Also, for MDC systems with single or multiple tenants, a single tenant restore operation is not supported.

For manual configured HANA resources, SnapCenter only supports manual recovery, as shown in Figure 20. The workflow for manual recovery is the same as described in the previous sections.

Figure 20) Restore and recovery operations for manual configured resources.



Summary restore and recovery operations

Table 7 summarizes the restore and recovery operations depending on the HANA resource configuration in SnapCenter.

Table 7) Restore and recovery operations, dependent on resource configuration option.

SnapCenter resource configuration	Restore and recovery options	Stop HANA database	Unmount before, mount after restore operation	Recovery operation
Auto discovered Single container MDC single tenant	Complete resource with either Default (all files) Volume revert (NFS from primary storage only) Automated recovery selected	Automated with SnapCenter	Automated with SnapCenter	Automated with SnapCenter
	Complete resource with either Default (all files) Volume revert (NFS from primary storage only) No recovery selected	Automated with SnapCenter	Automated with SnapCenter	Manual

SnapCenter resource configuration	Restore and recovery options	Stop HANA database	Unmount before, mount after restore operation	Recovery operation
	Tenant restore	Manual	Not required	Manual
Auto discovered MDC multiple tenants	Complete resource with either Default (all files) Volume revert (NFS from primary storage only) Automated recovery not supported	Automated with SnapCenter	Automated with SnapCenter	Manual
	Tenant restore	Manual	Not required	Manual
All manual configured resources	Complete resource (= Volume revert, available for NFS and SAN from primary storage only) File level (all files) Automated recovery not supported	Manual	Manual	Manual

Lab setup used for this report

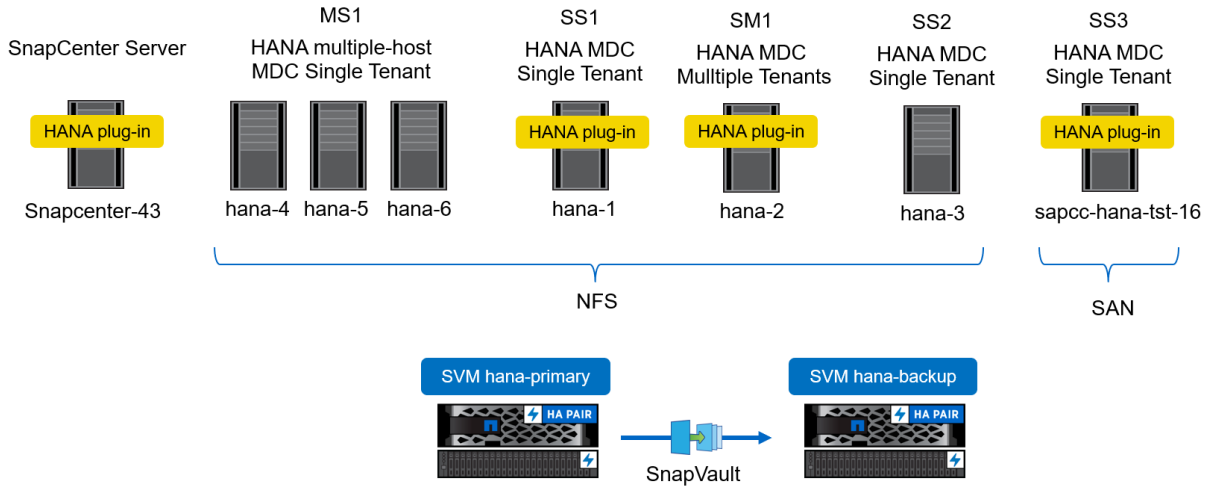
The lab setup used for this technical report includes five different SAP HANA configurations:

- MS1 - SAP HANA multiple host MDC single tenant system
Managed with a central plug-in host (SnapCenter server)
Using NFS as storage protocol
- SS1 – SAP HANA single host MDC single tenant system
Auto discovered with HANA plug-in installed on HANA database host
Using NFS as storage protocol
- SM1 – SAP HANA single host MDC multiple tenant system
Auto discovered with HANA plug-in installed on HANA database host
Using NFS as storage protocol
- SS2 – SAP HANA single host MDC single tenant system
Managed with a central plug-in host (SnapCenter Server)
Using NFS as storage protocol
- SS3 – SAP HANA single host MDC single tenant system
Auto discovered with HANA plug-in installed on HANA database host
Using Fibre Channel SAN as storage protocol

The following sections describe the complete configuration and the backup, restore, and recovery workflows. The description covers local Snapshot backups as well as replication to backup storage using SnapVault. The storage virtual machines (SVMs) are `hana-primary` for the primary storage and `hana-backup` for the off-site backup storage.

The SnapCenter Server is used as a central HANA plug-in host for the HANA systems MS1 and SS2. Figure 21 shows the lab setup.

Figure 21) Lab setup.



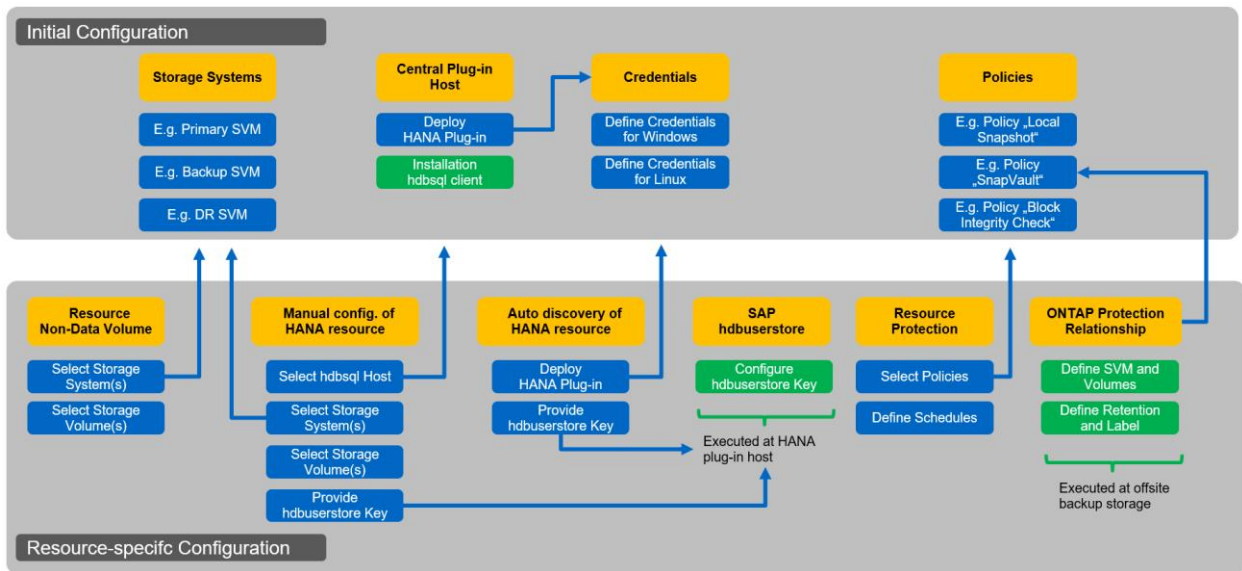
SnapCenter configuration

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, central HANA plug-in hosts, and policies, which 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 database.

Figure 22 provides an overview of the configuration components and their dependencies. 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.

Figure 22) Overview of configuration steps and dependencies.



With the initial configuration, the following components are installed and configured:

- **Storage system.** 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.
Note: Storage cluster credentials can also be configured instead of individual SVM credentials.
- **Credentials.** Configuration of credentials used to deploy the SAP HANA plug-in on the hosts.
- **Hosts (for central HANA plug-in hosts).** Deployment of SAP HANA plug-in. Installation of the SAP HANA hdbclient software on the host. The SAP hdbclient software must be installed manually.
- **Policies.** 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 configurations:

- SAP HANA nondata volume resource configuration:
 - Storage systems and volumes
- SAP hdbuserstore key configuration:
 - The SAP hdbuserstore key configuration for the specific SAP HANA database must be done either on the central plug-in host, or on the HANA database host, depending on where the HANA plug-in is deployed.
- Auto discovered SAP HANA database resources:
 - Deployment of SAP HANA plug-in on database host
 - Provide hdbuserstore key
- Manual SAP HANA database resource configuration:
 - SAP HANA database SID, plug-in host, hdbuserstore key, storage systems and volumes
- Resource 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.

SnapCenter initial configuration

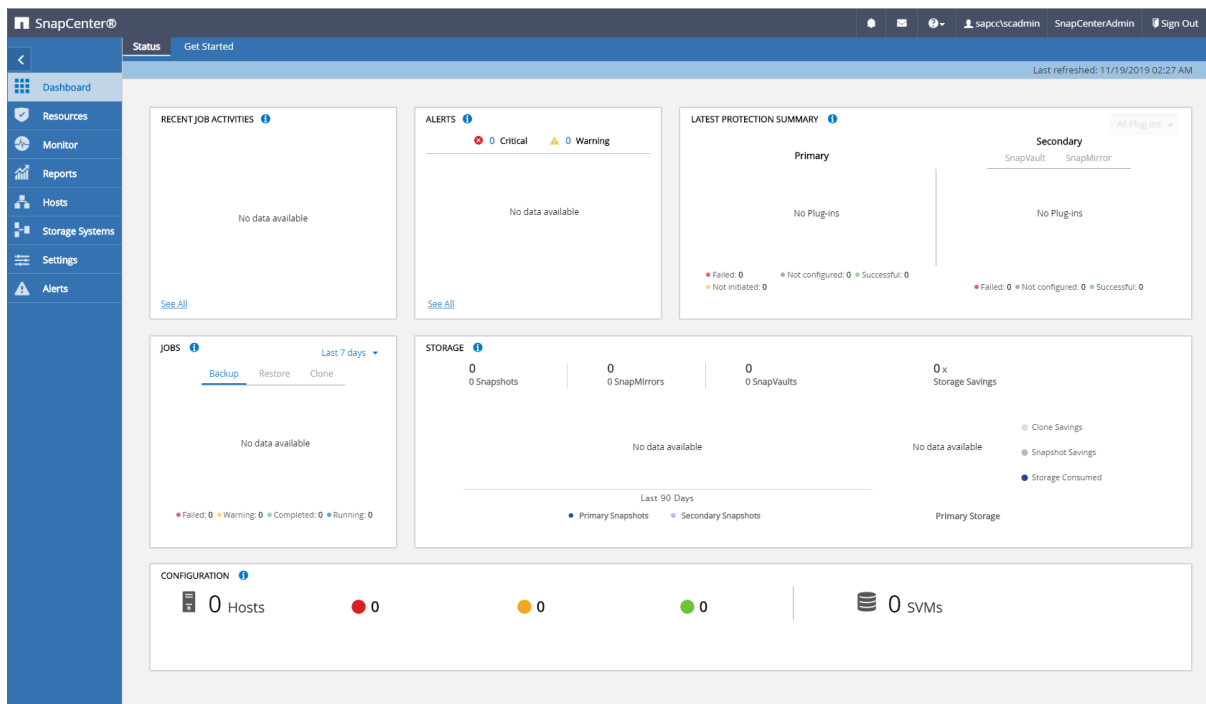
The initial configuration includes the following steps:

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

The following sections describe the initial configuration steps.

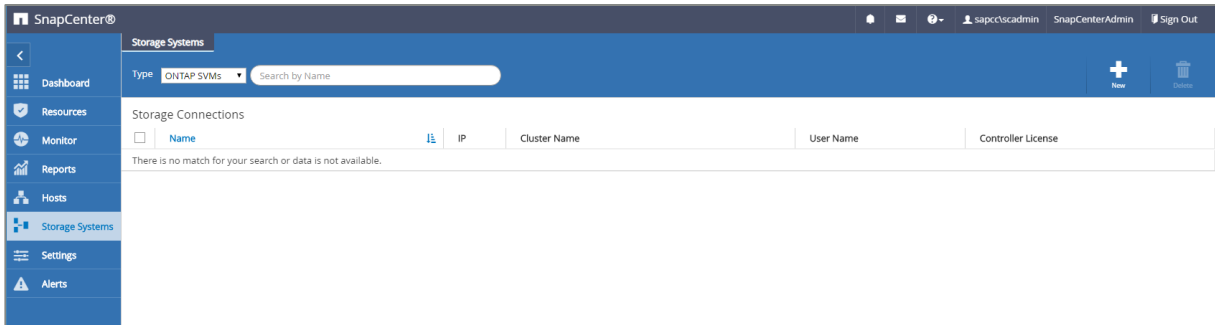
Storage system configuration

1. Log in to the SnapCenter Server GUI.



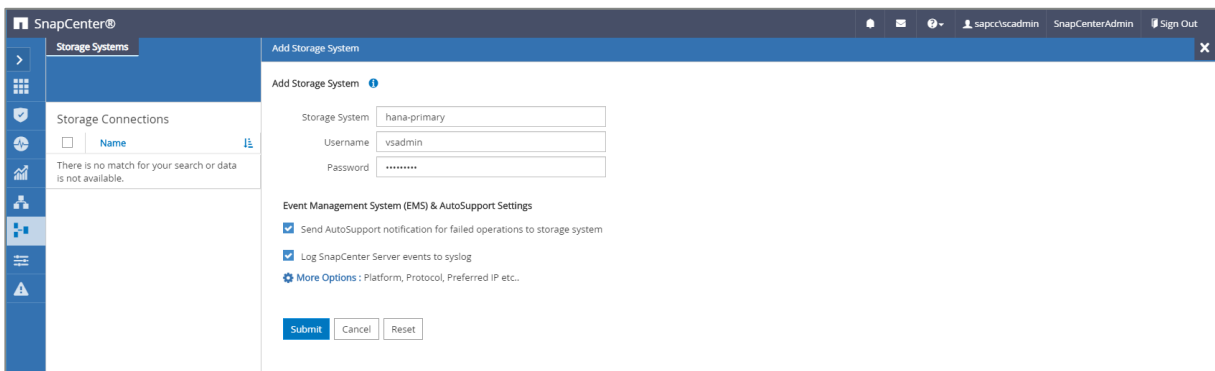
2. Select Storage Systems.

Note: In the screen, you can select the storage system type, which can be ONTAP SVMs or ONTAP Clusters. If you configure the storage systems on SVM level, you need to have a management LIF configured for each SVM. As an alternative, you can use a SnapCenter management access on cluster level. With the following example, SVM management is used.



- Click New to add a storage system and provide the required host name and credentials.

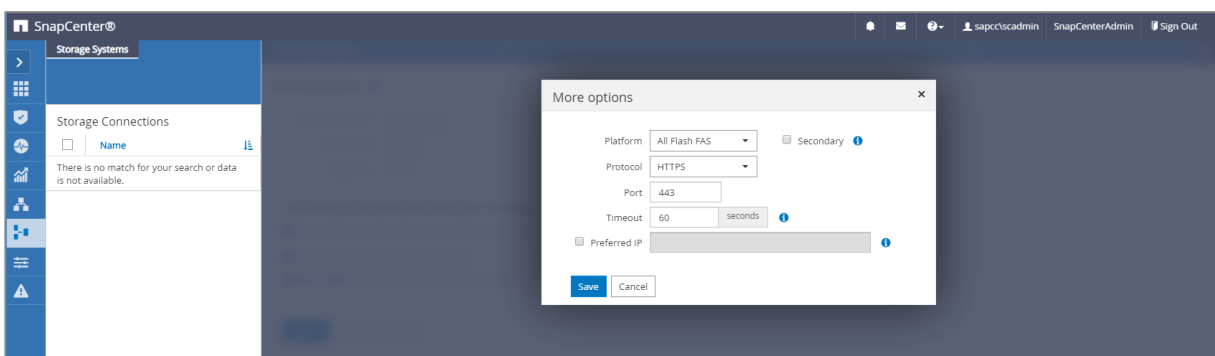
Note: The SVM user is not required to be the vsadmin user, as shown in the screenshot. Typically, a user is configured on the SVM and assigned the required permissions to execute backup and restore operations. Details on required privileges can be found in the [SnapCenter Installation Guide](#) in the section titled “Minimum ONTAP privileges required”.



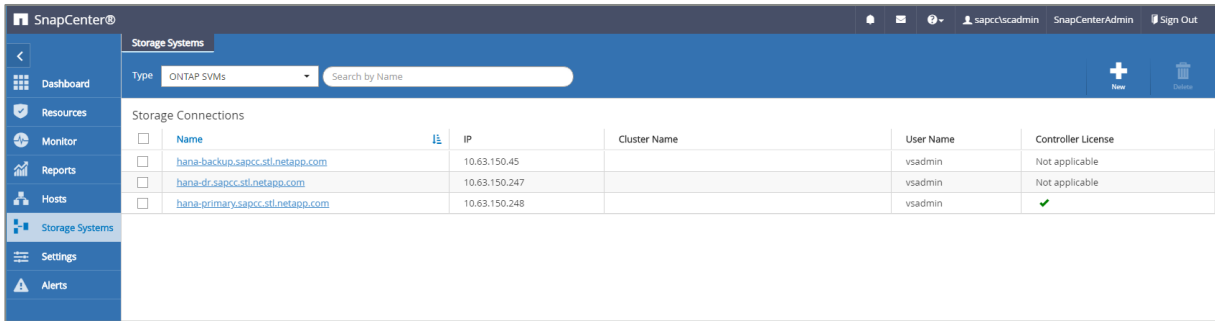
- Click More Options to configure the storage platform.

Storage platform can be FAS, AFF, ONTAP Select or Cloud Volumes ONTAP.

Note: For a system used as a SnapVault or SnapMirror target, select the Secondary icon.

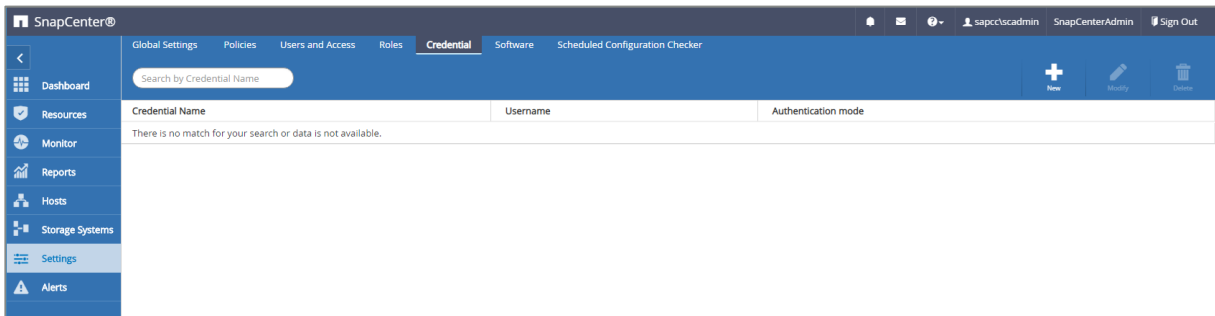


- Add additional storage systems as required.
In our example, an additional offsite backup storage and a disaster recovery storage has been added.



Credentials configuration

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



2. Provide the credentials for the user that are used for plug-in installations on Linux systems.

The 'Credential' dialog box is shown with the following fields:

- Credential Name: InstallPluginOnLinux
- Username: root
- Password: (masked with dots)
- Authentication: Linux
- Use sudo privileges: (unchecked)

Buttons: Cancel, OK

3. Provide the credentials for the user that are used for plug-in installations on Windows systems.

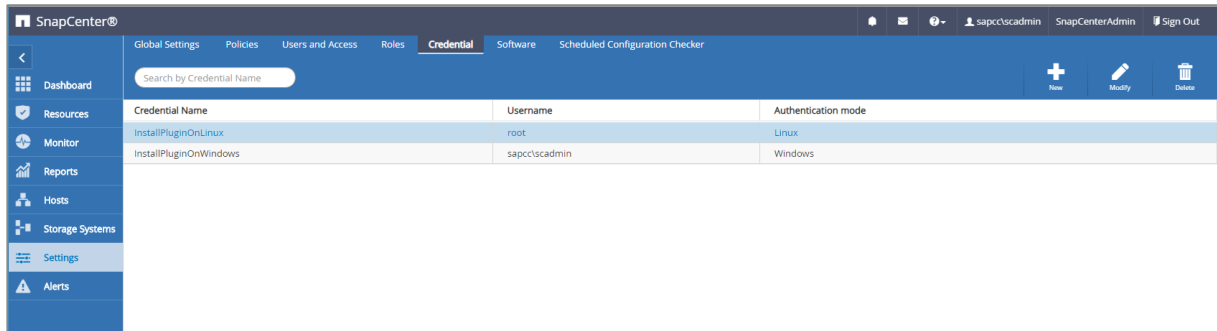
The 'Credential' dialog box is shown with the following fields:

- Credential Name: InstallPluginOnWindows
- Username: sapcc/scadmin
- Password: (masked with dots)
- Authentication: Windows

Buttons: Cancel, OK

Figure 23 shows the configured credentials.

Figure 23) Configured credentials.



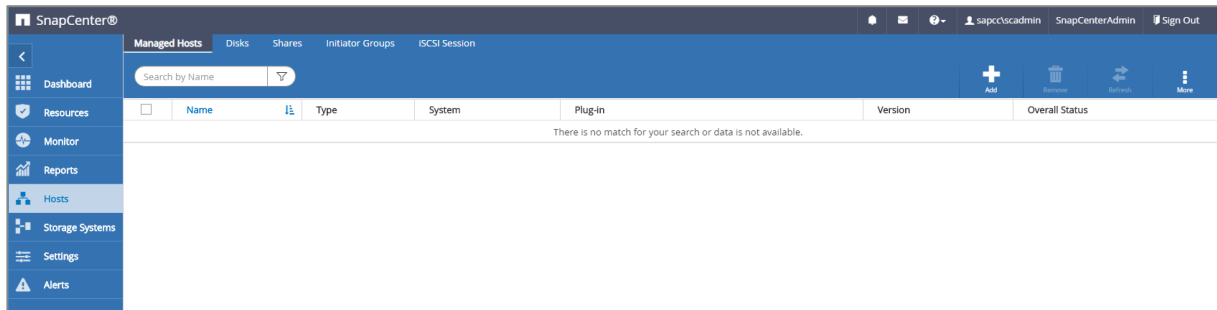
Credential Name	Username	Authentication mode
InstallPluginOnLinux	root	Linux
InstallPluginOnWindows	sapcc\scadmin	Windows

SAP HANA plug-in installation on a central plug-in host

In the lab setup, the SnapCenter Server is also used as a central HANA plug-in 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.

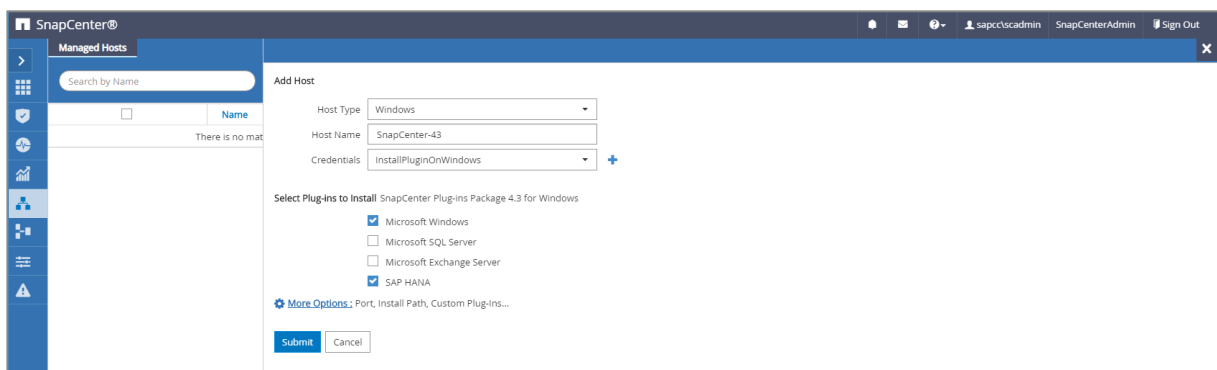
Note: The SAP HANA plug-in requires Java 64-bit version 1.8. Java needs to be installed on the host before the SAP HANA plug-in is deployed.

1. Go to Hosts and click Add.



Name	Type	System	Plug-in	Version	Overall Status
There is no match for your search or data is not available.					

2. Provide the required host information. Click Submit.



Host Type: Windows

Host Name: SnapCenter-43

Credentials: InstallPluginOnWindows

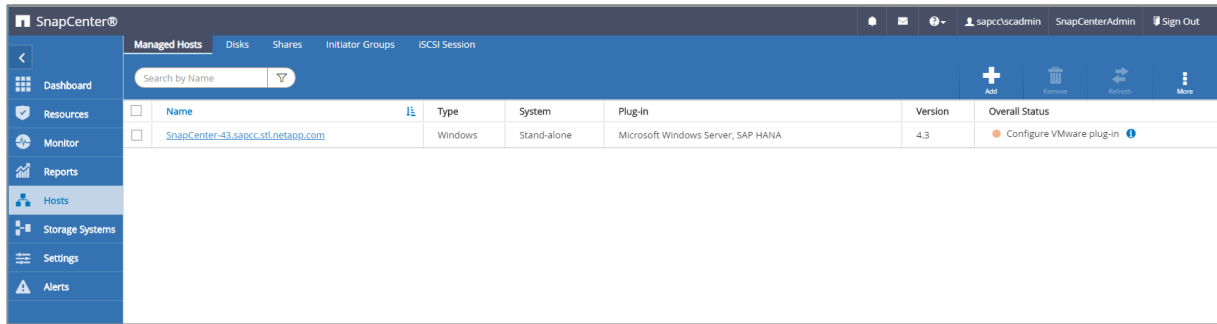
Select Plug-ins to install: SnapCenter Plug-ins Package 4.3 for Windows

- ☒ Microsoft Windows
- ☐ Microsoft SQL Server
- ☐ Microsoft Exchange Server
- ☒ SAP HANA

[More Options](#): Port, Install Path, Custom Plug-ins...

Figure 24 shows all the configured hosts after the HANA plug-in is deployed.

Figure 24) Configured hosts.



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
```

Policy configuration

As discussed in the “Data protection strategy” section, policies are usually configured independently of the resource and can be used by multiple SAP HANA databases.

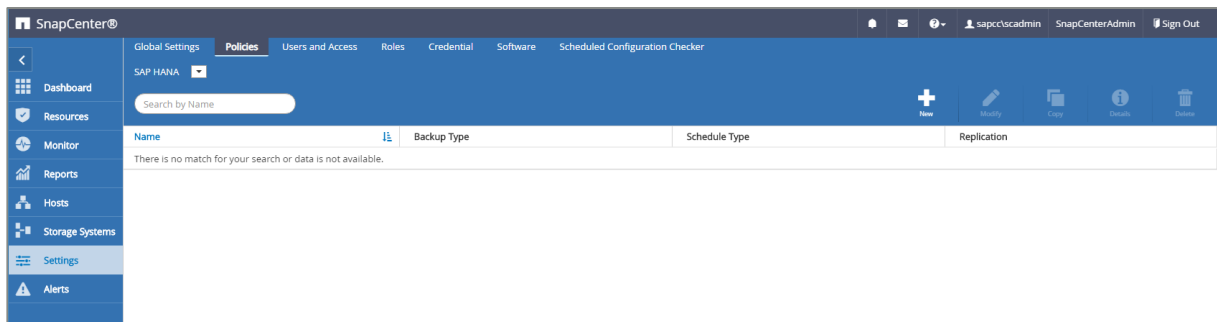
A typical minimum configuration consists of the following policies:

- 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

1. Go to Settings > Policies and click New.



2. Enter the policy name and description. Click Next.

New SAP HANA Backup Policy

1 Name Provide a policy name

2 Settings Policy name LocalSnap

3 Retention Description Snapshot backup at primary storage

4 Replication

5 Summary

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

New SAP HANA Backup Policy

1 Name Select backup settings

2 Settings Backup Type ☒ Snapshot Based ☐ File-Based

3 Retention Schedule Frequency

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

5 Summary ☐ None ☒ Hourly ☐ Daily ☐ Weekly ☐ Monthly

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

New SAP HANA Backup Policy

1 Name Retention settings

2 Settings On demand backup retention settings

3 Retention Backup retention settings

4 Replication ☒ Total Snapshot copies to keep 2

5 Summary ☐ Keep Snapshot copies for 14 days

Hourly retention settings

5. Configure the retention settings for scheduled backups.

New SAP HANA Backup Policy

1 Name Retention settings

2 Settings On demand backup retention settings

3 Retention Hourly retention settings

4 Replication ☒ Total Snapshot copies to keep 12

5 Summary ☐ Keep Snapshot copies for 14 days

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

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select secondary replication options

☐ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label: One Time

Error retry count: 3

7. On the Summary page, click Finish.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Summary

Policy name	LocalSnap
Description	Snapshot backup at primary storage
Backup Type	Snapshot Based Backup
Schedule Type	Hourly
On demand backup retention	Total backup copies to retain : 2
Hourly backup retention	Total backup copies to retain : 12
Replication	none

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.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Provide a policy name

Policy name: LocalSnapAndSnapVault

Description: Local Snapshot backup replicated to backup storage

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

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select backup settings

Backup Type: ☒ Snapshot Based ☐ File-Based

Schedule Frequency

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

☐ None

☐ Hourly

☒ Daily

☐ Weekly

☐ Monthly

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

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Retention settings

On demand backup retention settings

Backup retention settings

☒ Total Snapshot copies to keep 3

☐ Keep Snapshot copies for 14 days

Daily retention settings

5. Configure the retention settings for scheduled backups.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Retention settings

On demand backup retention settings

Daily retention settings

☒ Total Snapshot copies to keep 3

☐ Keep Snapshot copies for 14 days

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 the section titled "Configuration of data protection to off-site backup storage."

Modify SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select secondary replication options

☐ Update SnapMirror after creating a local Snapshot copy.

☒ Update SnapVault after creating a local Snapshot copy.

Secondary policy label Daily

Error retry count 3

7. On the Summary page, click Finish.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Summary

Policy name	LocalSnapAndSnapVault
Description	Local Snapshot backup replicated to backup storage
Backup Type	Snapshot Based Backup
Schedule Type	Daily
On demand backup retention	Total backup copies to retain : 3
Daily backup retention	Total backup copies to retain : 3
Replication	SnapVault enabled , Secondary policy label: Daily , Error retry count: 3

Policy for Weekly Block Integrity Check

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

New SAP HANA Backup Policy

1 Name Provide a policy name

2 Settings Policy name BlockIntegrityCheck

3 Retention Description Block integrity check using file based backup

4 Replication

5 Summary

3. Set the backup type to File-Based and schedule frequency to Weekly.

New SAP HANA Backup Policy

1 Name

2 Settings Select backup settings

Backup Type ☐ Snapshot Based ☒ File-Based

3 Retention

4 Summary

Schedule Frequency

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

☐ None

☐ Hourly

☐ Daily

☒ Weekly

☐ Monthly

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

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention Retention settings

4 Summary

On demand backup retention settings

Backup retention settings

☒ Total backup copies to keep 1

☐ Keep backup copies for 14 days

Weekly retention settings

5. Configure the retention settings for scheduled backups.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention Retention settings

4 Summary

On demand backup retention settings

Backup retention settings

☒ Total backup copies to keep 1

☐ Keep backup copies for 14 days

Weekly retention settings

6. On the Summary page, click Finish.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary Summary

Policy name BlockIntegrityCheck

Description Block integrity check using file based backup

Backup Type File-Based Backup

Schedule Type Weekly

On demand backup retention Total backup copies to retain : 1

Weekly backup retention Total backup copies to retain : 1

Figure 25 shows a summary of the configured policies.

Figure 25) Policies summary.

Name	Backup Type	Schedule Type	Replication
BlockIntegrityCheck	File Based Backup	Weekly	
LocalSnap	Data Backup	Hourly	
LocalSnapAndSnapVault	Data Backup	Daily	SnapVault

SnapCenter resource-specific configuration for SAP HANA database backups

This section describes the configuration steps for two example configurations.

- SS2, a single host SAP HANA MDC single-tenant system using NFS for storage access
The resource will be manually configured in SnapCenter.
The resource is configured to create local Snapshot backups and perform block integrity checks for the SAP HANA database using a weekly file-based backup.
- SS1, a single host SAP HANA MDC single-tenant system using NFS for storage access
The resource will be auto discovered with SnapCenter.
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, a single-container, or a multiple-host system are reflected in the corresponding configuration or workflow steps.

SAP HANA backup user and hdbuserstore configuration

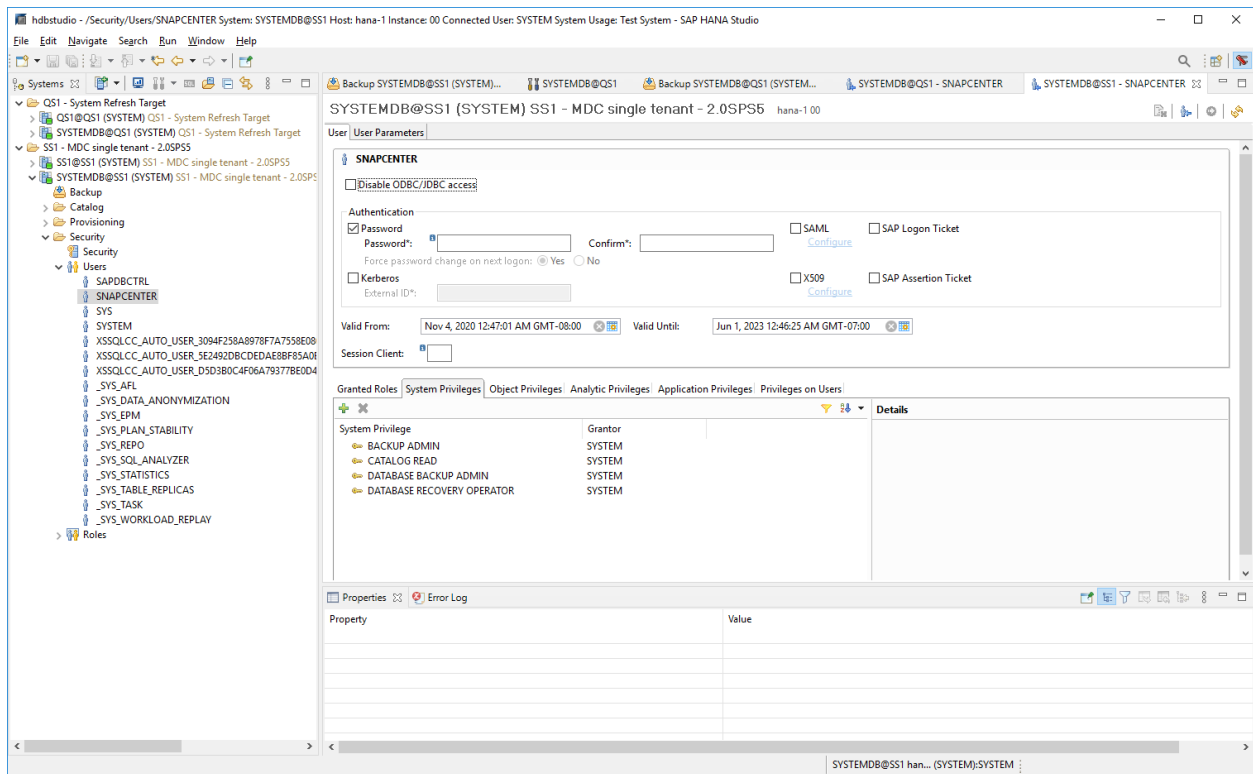
NetApp recommends configuring a dedicated database user in the HANA database to run the backup operations with SnapCenter. In the second step, an SAP HANA user store key is configured for this backup user, and this user store key is used in the configuration of the SnapCenter SAP HANA plug-in.

Figure 26 shows the SAP HANA Studio through which the backup user can be created.

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

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 databases are executed using the system database.

Figure 26) Database user for SAP HANA backups.



At the HANA plug-in host, on which the SAP HANA plug-in and the SAP hdbsql client are installed, a userstore key must be configured.

Userstore configuration on the SnapCenter server used as a central HANA plug-in host

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>
```

Note: The SAP HANA hdbclient software must be first installed on the Windows host.

Userstore configuration on a separate Linux host used as a Central HANA plug-in host

If the SAP HANA plug-in and SAP hdbsql client are installed on a separate Linux host, 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: The SAP HANA hdbclient software must be first installed on the Linux host.

Userstore configuration on the HANA database host

If the SAP HANA plug-in is deployed on the HANA database host, the following command is used for the user store configuration with the `<sid>adm` user:

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

Note: SnapCenter uses the <sid>adm user to communicate with the HANA database. Therefore, the user store key must be configured using the <sid>adm user on the database host.

Note: Typically, the SAP HANA hdbsql client software is installed together with the database server installation. If this is not the case, the hdbclient must be installed first.

Userstore configuration depending on HANA system architecture

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.

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.

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.

Userstore configuration examples

In the lab setup, a mixed SAP HANA plug-in deployment is used. The HANA plug-in is installed on the SnapCenter Server for some HANA systems and deployed on the individual HANA database servers for other systems.

SAP HANA system SS1, MDC single tenant, instance 00:

The HANA plug-in has been deployed on the database host. Therefore, the key must be configured on the database host with the user ss1adm.

```
hana-1:/ # su - ssladm
ssladm@hana-1:/usr/sap/SS1/HDB00>
ssladm@hana-1:/usr/sap/SS1/HDB00>
ssladm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore set SS1KEY hana-1:30013 SnapCenter password
ssladm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore list
DATA FILE      : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE       : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.KEY

KEY SS1KEY
  ENV : hana-1:30013
  USER: SnapCenter
KEY SS1SAPDBCTRLSS1
  ENV : hana-1:30015
  USER: SAPDBCTRL
ssladm@hana-1:/usr/sap/SS1/HDB00>
```

SAP HANA system MS1, multiple-host MDC single tenant, instance 00:

For HANA multiple host systems, a central plug-in host is required, in our setup we used the SnapCenter Server. Therefore, the user store configuration must be done on the SnapCenter Server.

```
hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE      : C:\ProgramData\.hdb\SNAPCENTER-43\S-1-5-18\SSFS_HDB.DAT
KEY FILE       : C:\ProgramData\.hdb\SNAPCENTER-43\S-1-5-18\SSFS_HDB.KEY

KEY MS1KEYHOST1
  ENV : hana-4:30013
  USER: SNAPCENTER
KEY MS1KEYHOST2
  ENV : hana-5:30013
  USER: SNAPCENTER
```

```

KEY MS1KEYHOST3
  ENV : hana-6:30013
  USER: SNAPCENTER
KEY SS2KEY
  ENV : hana-3:30013
  USER: SNAPCENTER
C:\Program Files\sap\hdbclient>

```

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 27 shows the configured protection relationship for the SAP HANA system SS1. With our example, the source volume `SS1_data_mnt00001` at the SVM `hana-primary` is replicated to the SVM `hana-backup` and the target volume `SS1_data_mnt00001_dest`.

Note: The schedule of the relationship must be set to `None`, because SnapCenter triggers the SnapVault update.

Figure 27) Protection relationship.

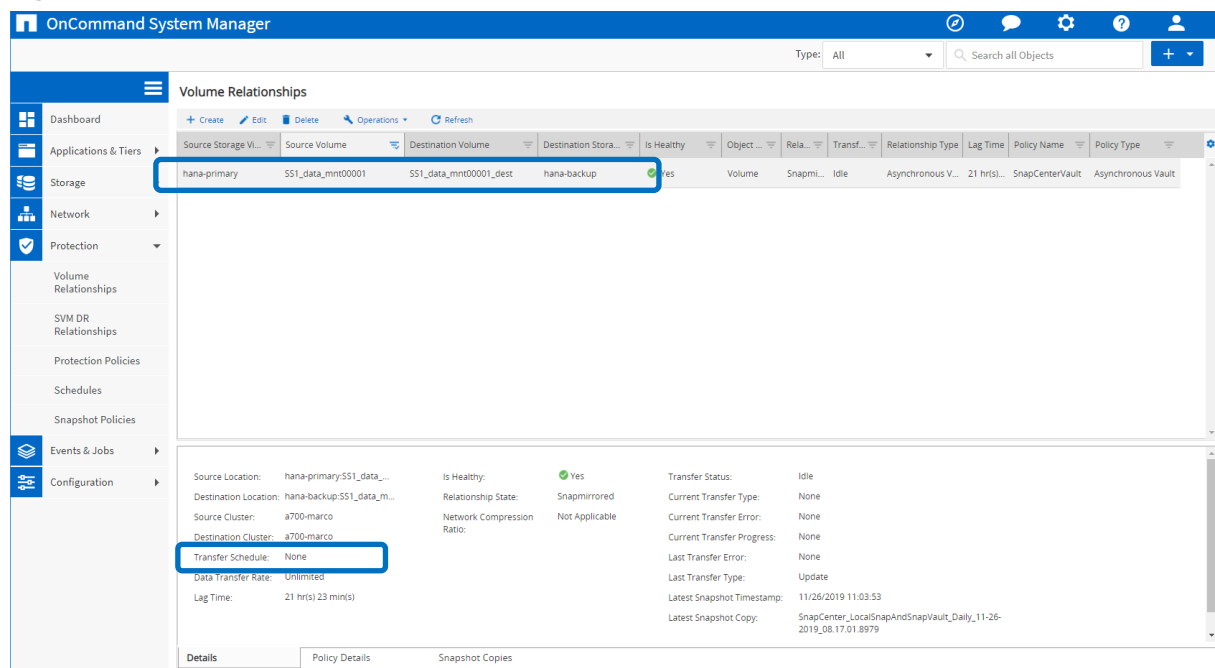
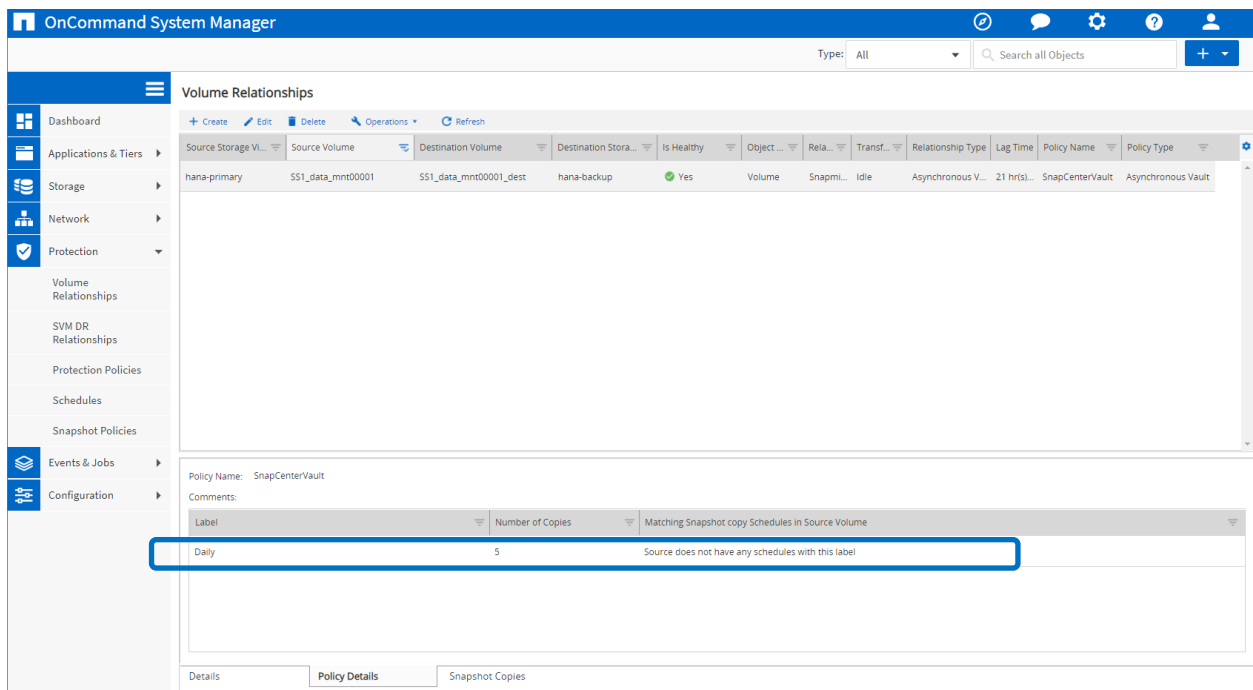


Figure 28 shows the protection policy. The protection policy used for the protection relationship defines the SnapMirror label, as well as the retention of backups at the secondary storage. In our example, the used label is `Daily`, and the retention is set to 5.

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.

Figure 28) Protection policy.



Manual HANA resource configuration

This section describes the manual configuration of the SAP HANA resources SS2 and MS1.

- SS2 is a single host MDC single tenant system
 - MS1 is a multiple-host MDC single tenant system.
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, Multitenant Database Container.

Note: For a HANA single container system, the resource type Single Container must be selected. All the other configuration steps are identical.

For our SAP HANA system, the SID is SS2.

The HANA plug-in host in our example is the SnapCenter Server.

The hdbuserstore key must match the key that was configured for the HANA database SS2. In our example it is SS2KEY.

The screenshot shows the 'Add SAP HANA Database' dialog box. The 'Name' tab is selected, showing the 'Provide Resource Details' section. The form contains the following fields and values:

Field	Value
Resource Type	Multitenant Database Container
HANA System Name	SS2 - HANA 20 SP54 MDC Single Tenant
SID	SS2
Plug-in Host	SnapCenter-43.sapcc.stl.netapp.com
HDB Secure User Store Keys	SS2KEY
HDBSQL OS User	SYSTEM

Note: For an SAP HANA multiple-host system, the hdbuserstore keys for all hosts must be included, as shown in the following figure. SnapCenter will try to connect with the first key in

the list, and will continue with the other case, in case the first key does not work. This is required to support HANA failover in a multiple-host system with worker and standby hosts.

Modify SAP HANA Database

1 Name

Provide Resource Details

Resource Type: Multitenant Database Container

HANA System Name: MS1 - Multiple Hosts MDC Single Tenant

SID: MS1

Plug-in Host: SnapCenter-43.sapcc.stl.netapp.com

HDB Secure User Store Keys: MS1KEYHOST1,MS1KEYHOST2,MS1KEYHOST3

HDBSQL OS User: SYSTEM

3. Select the required data for the storage system (SVM) and volume name.

Add SAP HANA Database

2 Storage Footprint

Provide Storage Footprint Details

Add Storage Footprint

Storage System: hana-primary.sapcc.stl.netapp.com

Select one or more volumes and if required their associated Qtrees and LUNs

Volume name: SS2_data_mnt00001

LUNs or Qtrees: Default is 'None' or type to find

Save

Note: For a Fibre Channel SAN configuration, the LUN needs to be selected as well.

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.

Add SAP HANA Database

2 Storage Footprint

Provide Storage Footprint Details

Add Storage Footprint

Storage System: hana-primary.sapcc.stl.netapp.com

Select one or more volumes and if required their associated Qtrees and LUNs

Volume name: MS1_data_mnt00001, MS1_data_mnt00002

LUNs or Qtrees: Default is 'None' or type to find

Save

The summary screen of the resource configuration is shown.

4. Click Finish to add the SAP HANA database.

Add SAP HANA Database

3 Summary

Summary

Resource Type: Multitenant Database Container

HANA System Name: SS2 - HANA 20 SPS4 MDC Single Tenant

SID: SS2

Plug-in Host: SnapCenter-43.sapcc.stl.netapp.com

HDB Secure User Store Keys: SS2KEY

HDBSQL OS User: SYSTEM

Storage Footprint

Storage System	Volume	LUN/Qtree
hana-primary.sapcc.stl.netapp.com	SS2_data_mnt00001	

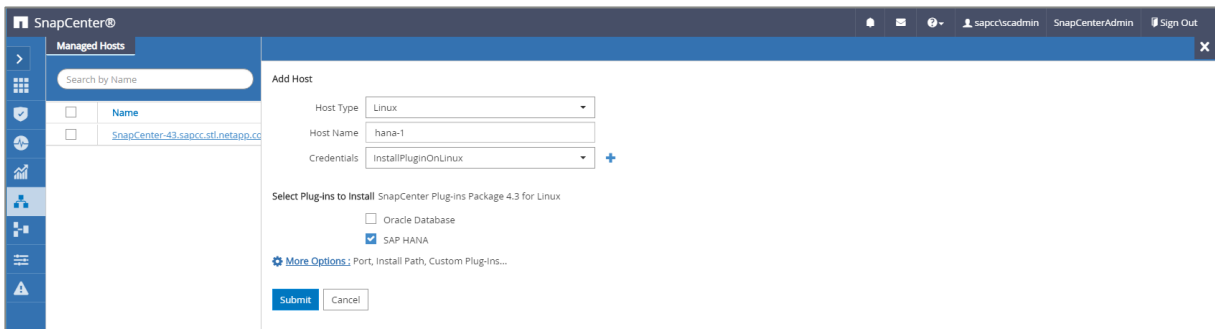
- When the resource configuration is finished, the resource protection configuration must be executed as described in the “Resource protection configuration” section.

Automatic discovery of HANA databases

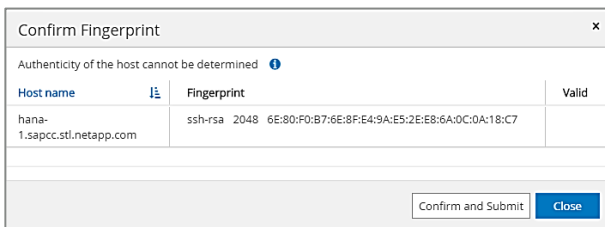
This section describes the automatic discovery of the SAP HANA resource SS1 (Single host MDC single tenant system with NFS). All the described steps are identical for HANA single container, HANA MDC multiple tenants’ systems, and HANA system using Fibre Channel SAN.

Note: The SAP HANA plug-in requires Java 64-bit version 1.8. Java must be installed on the host before the SAP HANA plug-in is deployed.

- From the host tab, click Add.
- Provide host information and select SAP HANA plug-in to be installed. Click Submit.

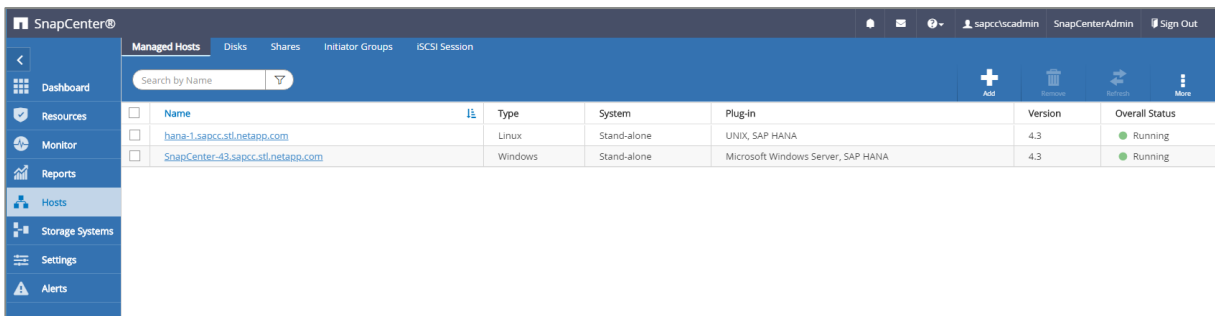


- Confirm the fingerprint.



Host name	Fingerprint	Valid
hana-1.sapcc.stl.netapp.com	ssh-rsa 2048 6E:80:F0:B7:6E:8F:E4:9A:E5:2E:E8:6A:0C:0A:18:C7	

The installation of the HANA and the Linux plug-in starts automatically. When the installation is finished, the status column of the host shows Running. The screen also shows that the Linux plug-in is installed together with the HANA plug-in.

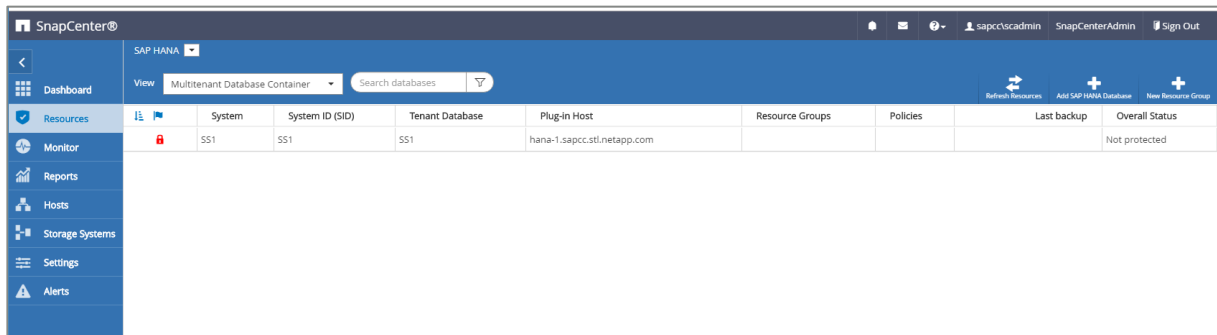


Name	Type	System	Plug-in	Version	Overall Status
hana-1.sapcc.stl.netapp.com	Linux	Stand-alone	UNIX, SAP HANA	4.3	Running
SnapCenter-43.sapcc.stl.netapp.com	Windows	Stand-alone	Microsoft Windows Server, SAP HANA	4.3	Running

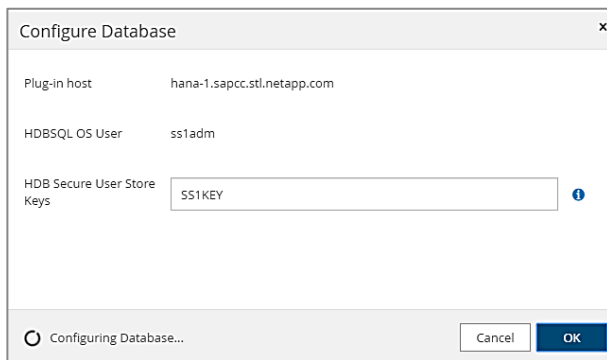
After the plug-in installation, the automatic discovery process of the HANA resource starts automatically. In the Resources screen, a new resource is created, which is marked as locked with the red padlock icon.

- Select and click on the resource to continue the configuration.

Note: You can also trigger the automatic discovery process manually within the Resources screen, by clicking Refresh Resources.

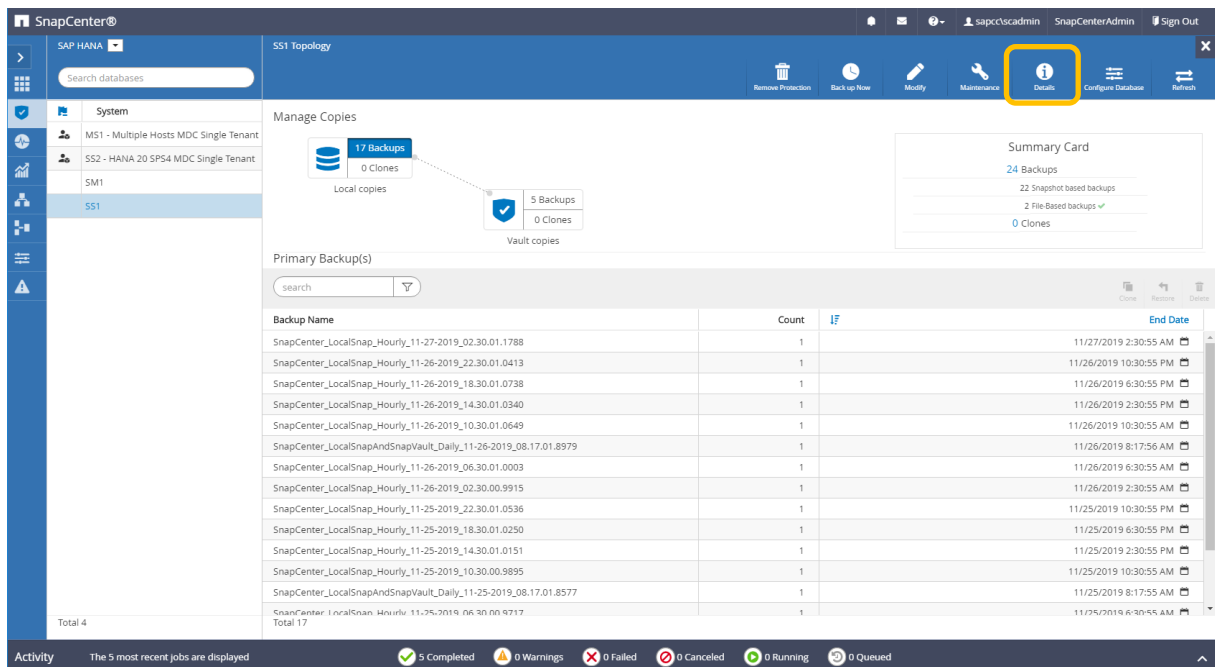


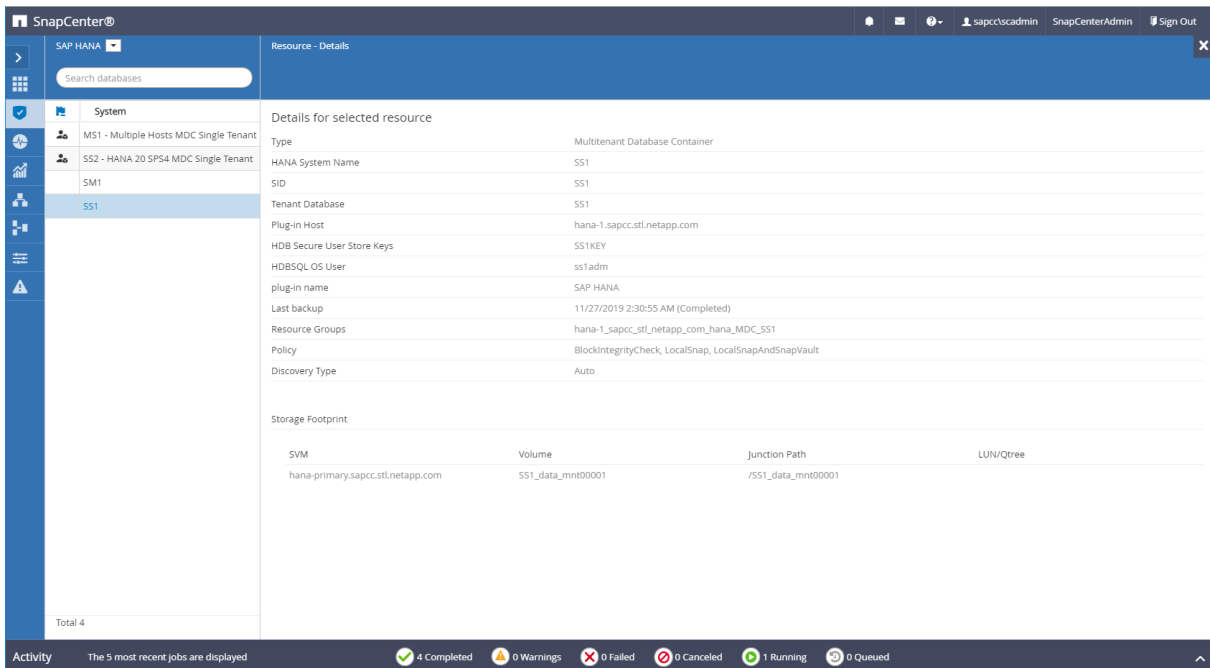
5. Provide the userstore key for the HANA database.



The second level automatic discovery process starts in which tenant data and storage footprint information is discovered.

6. Click Details to review the HANA resource configuration information in the resource topology view.





When the resource configuration is finished, the resource protection configuration must be executed as described in the “Resource protection configuration” section.

Resource protection configuration

This section describes the resource protection configuration. The resource protection configuration is the same, independent if the resource has been auto discovered, or configured manually. It is also identical for all HANA architectures, single or multiple hosts, single container, or MDC systems.

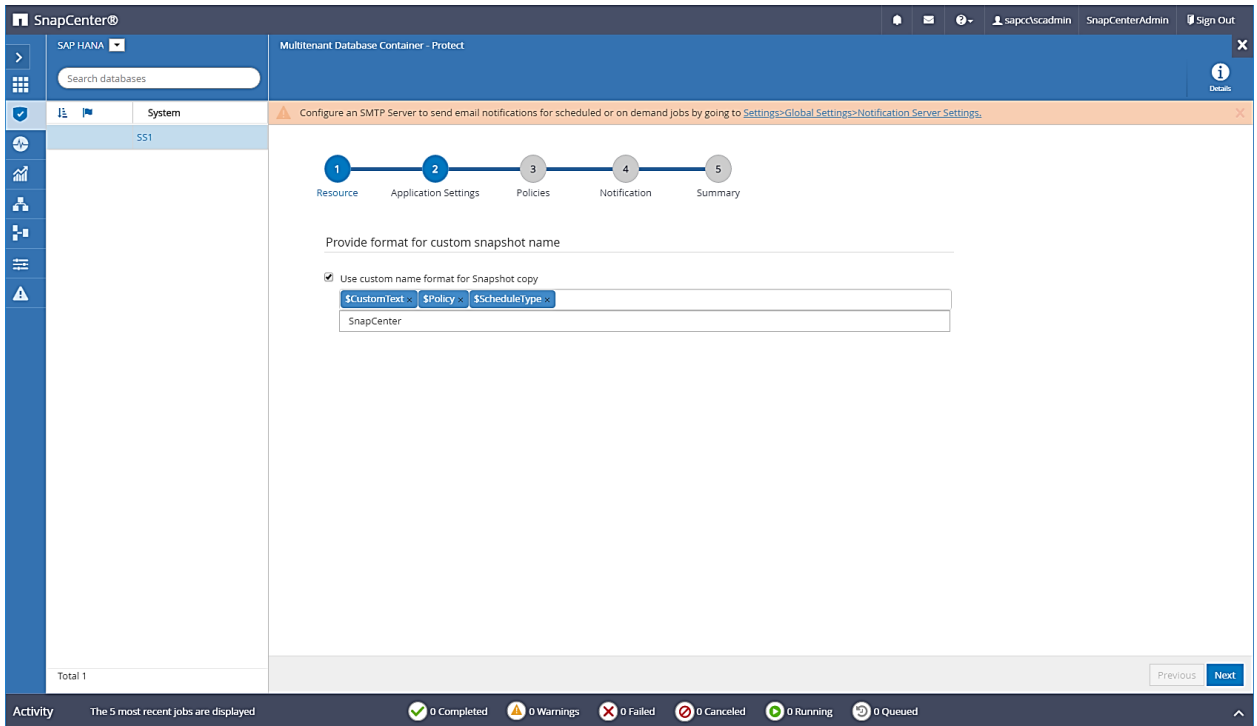
1. From the Resources tab, double-click the resource.
2. Configure a custom name format for the Snapshot copy.

Note: NetApp recommends using a custom Snapshot copy name to easily identify which backups have been created with which policy and 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`.

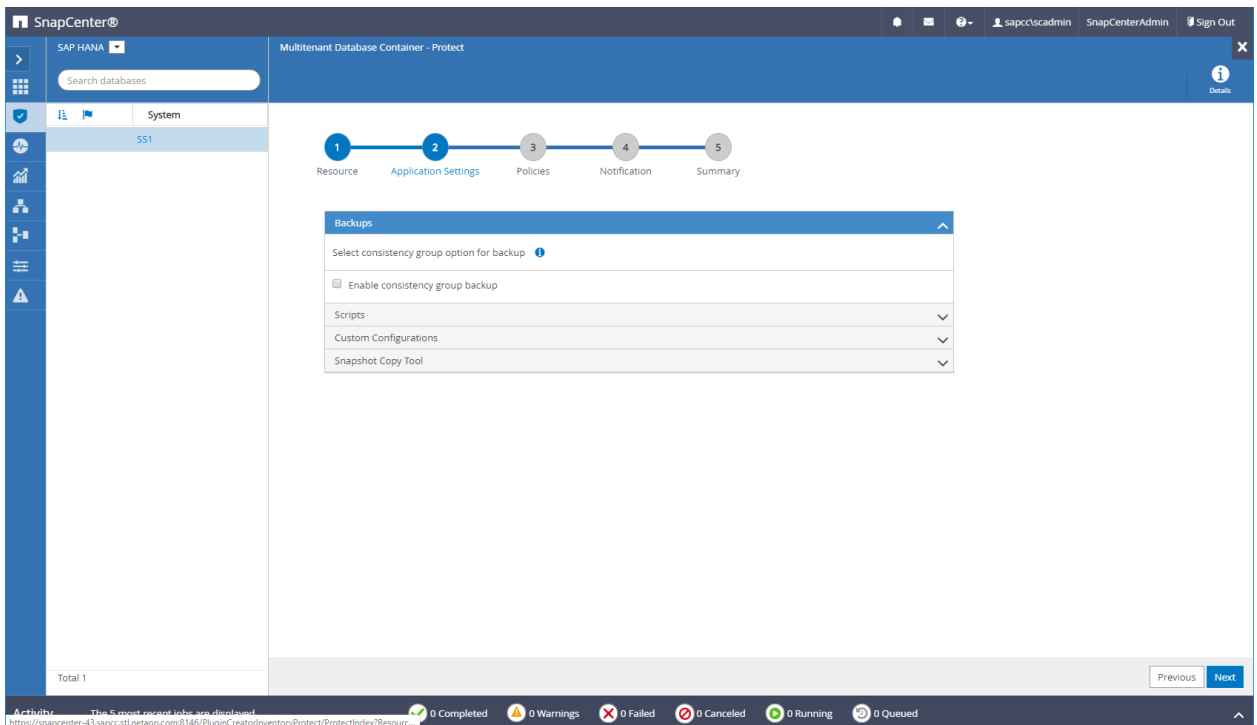
In the configuration shown in the following figure, the backup and Snapshot copy names have the following format:

- 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>`

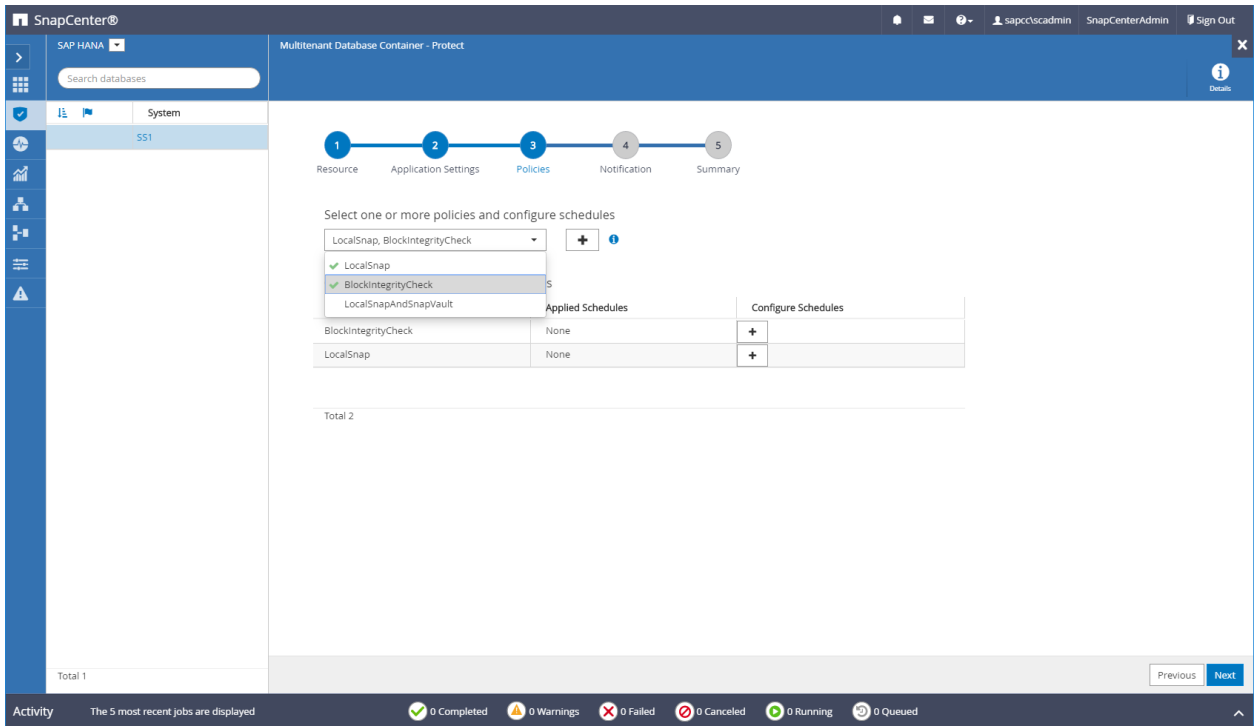
Note: Even though a retention is defined for on-demand backups in the policy configuration, the housekeeping is only done when another on-demand backup is executed. Therefore, on-demand backups must typically be deleted manually in SnapCenter to make sure that these backups are also deleted in the SAP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



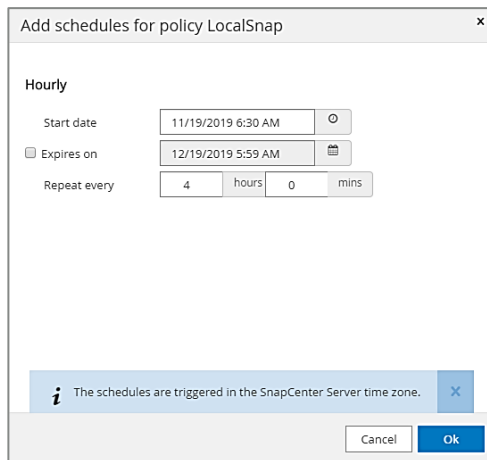
3. No specific setting needs to be made on the Application Settings page. Click Next.



4. Select the policies that should be added to the resource.



5. Define the schedule for the LocalSnap policy; in this example, it's every four hours.



6. Define the schedule for the LocalSnapAndSnapVault policy; in this example, it's once per day.

Modify schedules for policy LocalSnapAndSnapVault

Daily

Start date: 11/19/2019 8:17 AM

☐ Expires on: 12/19/2019 8:17 AM

Repeat every: 1 days

i The schedules are triggered in the SnapCenter Server time zone.

Cancel Ok

7. Define the schedule for the block integrity check policy; in this example, it's once per week.

Add schedules for policy BlockIntegrityCheck

Weekly

Start date: 11/19/2019 5:57 AM

☐ Expires on: 12/19/2019 5:57 AM

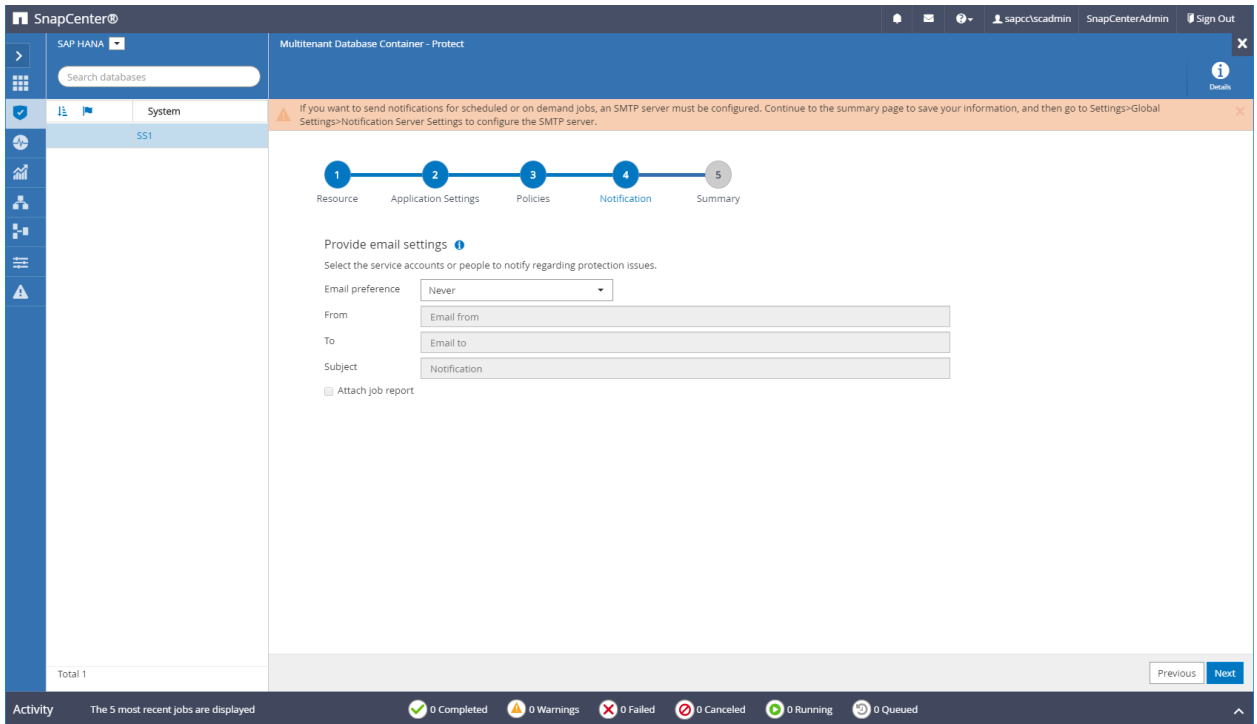
Days: Saturday

Monday
Tuesday
Wednesday
Thursday
Friday
✓ Saturday

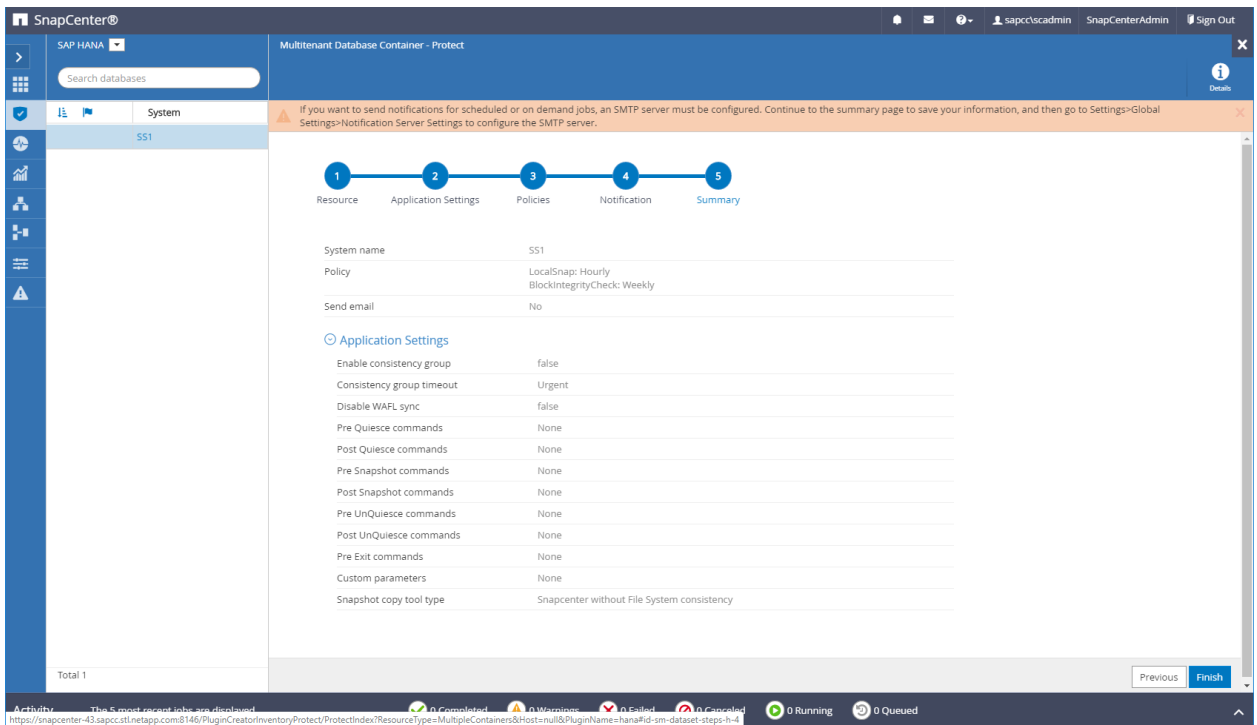
i The schedules are triggered in the SnapCenter Server time zone.

Cancel Ok

8. Provide information about the email notification.



9. On the Summary page, click Finish.



10. On-demand backups can now be created on the topology page. The scheduled backups are executed based on the configuration settings.

System	System ID (SID)	Tenant Database	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
SS1	SS1	SS1	hana-1.sapcc.stl.netapp.com		BlockIntegrityCheck LocalSnap LocalSnapAndSnapVault	11/19/2019 6:30:54 AM	Backup succeeded

Total 1

Activity: The 5 most recent jobs are displayed. 2 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, 0 Queued.

Additional configuration steps for Fibre Channel SAN environments

Depending on the HANA release and the HANA plug-in deployment, additional configuration steps are required for environments in which the SAP HANA systems are using Fibre Channel and the XFS file system.

Note: These additional configuration steps are only required for HANA resources, which are configured manually in SnapCenter. It is also only required for HANA 1.0 releases and HANA 2.0 releases up to SPS2.

When a HANA backup save point is triggered by SnapCenter in SAP HANA, SAP HANA writes Snapshot ID files for each tenant and database service, for example, `/hana/data/SID/mnt00001/hdb00001/snapshot_databackup_0_1` as a last step. These files are part of the data volume on the storage and are 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.

Note: With HANA 2.0 SPS3, SAP changed the write operation of these Snapshot ID files to synchronously so that metadata caching is not a problem.

Note: With SnapCenter 4.3, if the HANA plug-in is deployed on the database host, the Linux plug-in executes a file system flush operation on the host before the storage Snapshot is triggered. In this case, the metadata caching is not a problem.

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 SnapCenter server is used as a central HANA plug-in host, a batch file can be used. The batch file must have the following content:

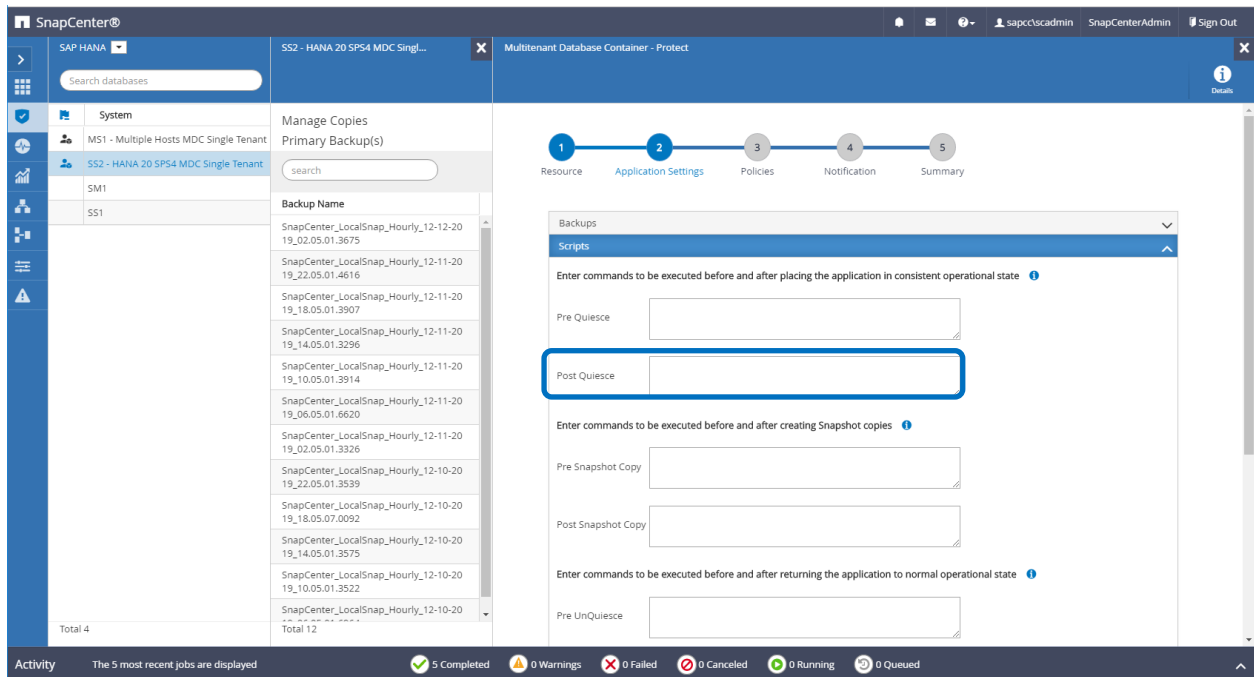
```
@echo off
waitfor AnyThing /t 60 2>NUL
Exit /b 0
```

The batch file can be saved, for example, as `C:\Program Files\NetApp\Wait60Sec.bat`. In the resource protection configuration, the batch file must be added as Post Quiesce command.

If a separate Linux host is used as a central HANA plug-in host, the command `/bin/sleep 60` must be configured as Post Quiesce command in the SnapCenter UI.

Figure 29 shows the Post Quiesce command within the resource protection configuration screen.

Figure 29) Configuration of Post Quiesce command.



SnapCenter resource-specific configuration for nondata volume backups

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

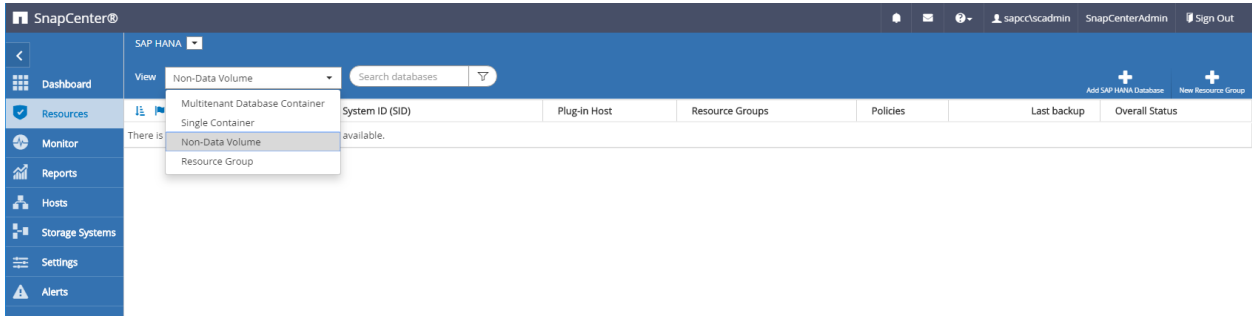
To recover from situations where other nondata files must be restored, NetApp recommends developing an additional backup strategy for nondata volumes to augment the SAP HANA database backup. Depending on your specific requirements, the backup of nondata volumes might differ in scheduling frequency and 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 database required.

Configuration of nondata volume resources

In this example, we want to protect the nondata volumes of the SAP HANA database SS1.

1. From the Resource tab, select Non-Data-Volume and click Add SAP HANA Database.



2. In step one of the Add SAP HANA Database dialog, in the Resource Type list, select Non-data Volumes. 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 click Next.

3. Add the SVM and the storage volume as storage footprint, then click Next.

Add SAP HANA Database

1 Name
2 **Storage Footprint**
3 Summary

Provide Storage Footprint Details

Add Storage Footprint

Storage System: hana-primary.sapcc.stl.netapp.com

Select one or more volumes and if required their associated Qtrees and LUNs

Volume name: SS1_shared

LUNs or Qtrees: Default is 'None' or type to find

Save

Previous Next

4. In the summary step, click Finish to save the settings.
5. Repeat these steps for all the required nondata volumes.
6. Continue with the protection configuration of the new resource.

Note: Data protection for a nondata volume resources is identical to the workflow for SAP HANA database resources and can be defined on an individual resource level.

Figure 30 shows the list of the configured nondata volume resources.

Figure 30) Nondata volume resources.

Name	Associated System ID (SID)	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
SS1-Shared-Volume	SS1	hana-1.sapcc.stl.netapp.com		LocalSnap		Backup not run

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.

Using SnapCenter together with SAP landscape management

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 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 be included in the backup; this includes: SAP HANA data, log and shared 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 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 VCM at the beginning.

Database backups

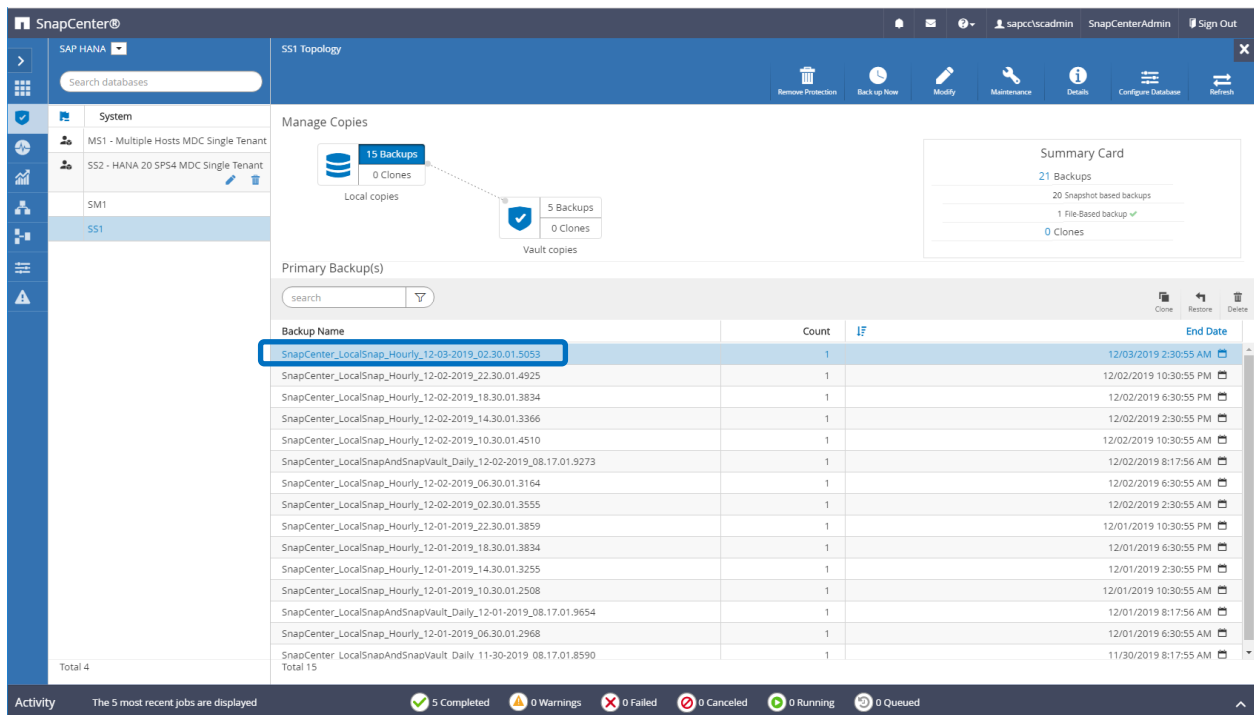
In SnapCenter, database backups are typically executed using the schedules defined within the resource protection configuration of each HANA database.

On-demand database backup can be performed by using either the SnapCenter GUI, a PowerShell command line, or REST APIs.

Identifying SnapCenter backups in SAP HANA Studio

The SnapCenter resource topology shows a list of backups created using SnapCenter. Figure 31 shows the backups available on the primary storage and highlights the most recent backup.

Figure 31) SnapCenter topology view.



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

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 32 for the system database and in Figure 33 for the tenant database SS1. Both figures highlight the SnapCenter backup name stored in the comment field and EBID.

Note: The HANA 2.0 SPS4 (revision 40 and 41) release always shows a backup size of zero for Snapshot-based backups. This was fixed with revision 42. For more information, see the SAP Note <https://launchpad.support.sap.com/#/notes/2795010>.

Figure 32) SAP HANA backup catalog for the system database.

Backup SYSTEMDB@SS1 (SYSTEM) SS1 - HANA20 SP54 MDC Single Tenant

Database: SYSTEMDB

Backup Catalog

Status	Started	Duration	Size	Backup Type	Destination...
Dec 3, 2019 2:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 10:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 6:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 2:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 10:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 8:17:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 2, 2019 6:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 2:30:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 1, 2019 10:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 1, 2019 6:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 1, 2019 2:30:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 1, 2019 10:30:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 1, 2019 8:17:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Nov 30, 2019 8:17:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Nov 30, 2019 6:00:04 ...	00h 00m 03s	1.40 GB	Data Backup	File	
Nov 29, 2019 8:17:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Nov 28, 2019 8:17:25 ...	00h 00m 13s	0 B	Data Backup	Snapshot	

Backup Details

ID: 1575369024442

Status: Successful

Backup Type: Data Backup

Destination Type: Snapshot

Started: Dec 3, 2019 2:30:24 AM (America/Los_Angeles)

Finished: Dec 3, 2019 2:30:38 AM (America/Los_Angeles)

Duration: 00h 00m 14s

Size: 0 B

Throughput: n.a.

System ID: n.a.

Comment: SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053

Additional Information: <ok>

Location: /hana/data/SS1/rmt00001/

Host	Service	Name	EBID
hana-1	nameserver	hdb00001	SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053

Figure 33) SAP HANA backup catalog for tenant database.

Backup SYSTEMDB@SS1 (SYSTEM) SS1 - HANA20 SP54 MDC Single Tenant

Database: SS1

Backup Catalog

Status	Started	Duration	Size	Backup Type	Destination...
Dec 3, 2019 2:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 10:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 6:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 2:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 10:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 8:17:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 2, 2019 6:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 2:30:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 1, 2019 10:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 1, 2019 6:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 1, 2019 2:30:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 1, 2019 10:30:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 1, 2019 8:17:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 1, 2019 6:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Nov 30, 2019 8:17:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Nov 30, 2019 6:00:10 ...	00h 00m 03s	1.67 GB	Data Backup	File	
Nov 29, 2019 8:17:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Nov 28, 2019 8:17:25 ...	00h 00m 13s	0 B	Data Backup	Snapshot	

Backup Details

ID: 1575369024443

Status: Successful

Backup Type: Data Backup

Destination Type: Snapshot

Started: Dec 3, 2019 2:30:24 AM (America/Los_Angeles)

Finished: Dec 3, 2019 2:30:38 AM (America/Los_Angeles)

Duration: 00h 00m 14s

Size: 0 B

Throughput: n.a.

System ID: n.a.

Comment: SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053

Additional Information: <ok>

Location: /hana/data/SS1/rmt00001/

Host	Service	Name	EBID
hana-1	indexserver	hdb00003...	SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053
hana-1	xsengine	hdb00002...	SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053

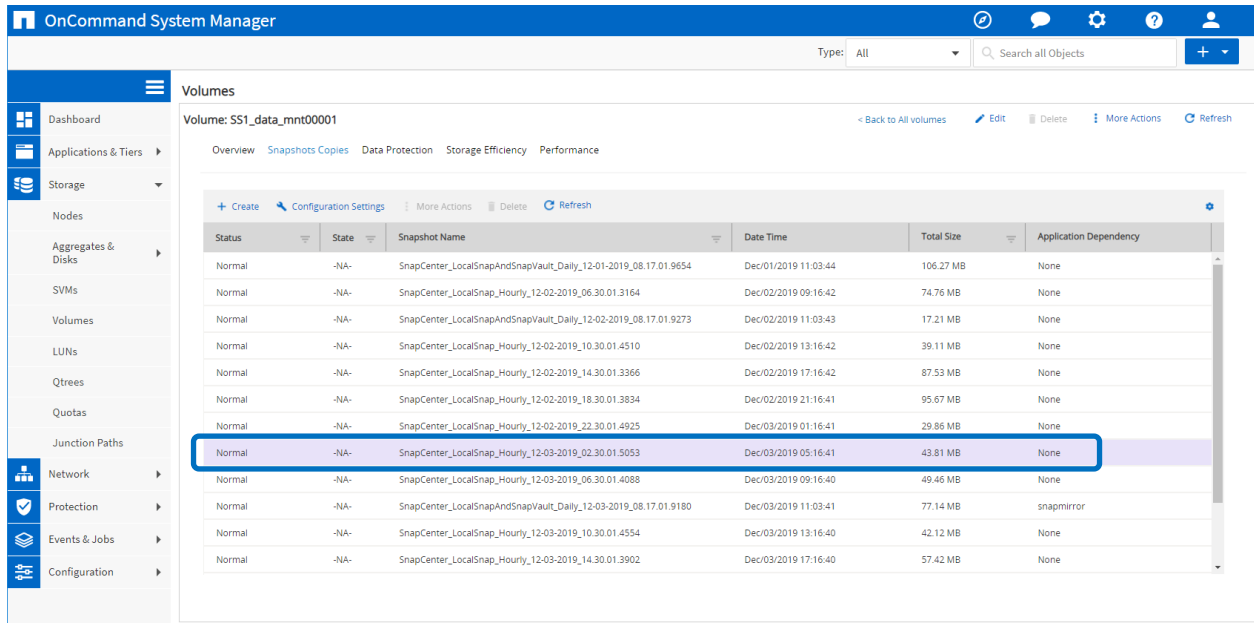
Note: SnapCenter is only aware of its own backups. Additional backups created, for example, with SAP HANA Studio, are visible in the SAP HANA catalog but not in SnapCenter.

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 34 shows the available backups for the database volume

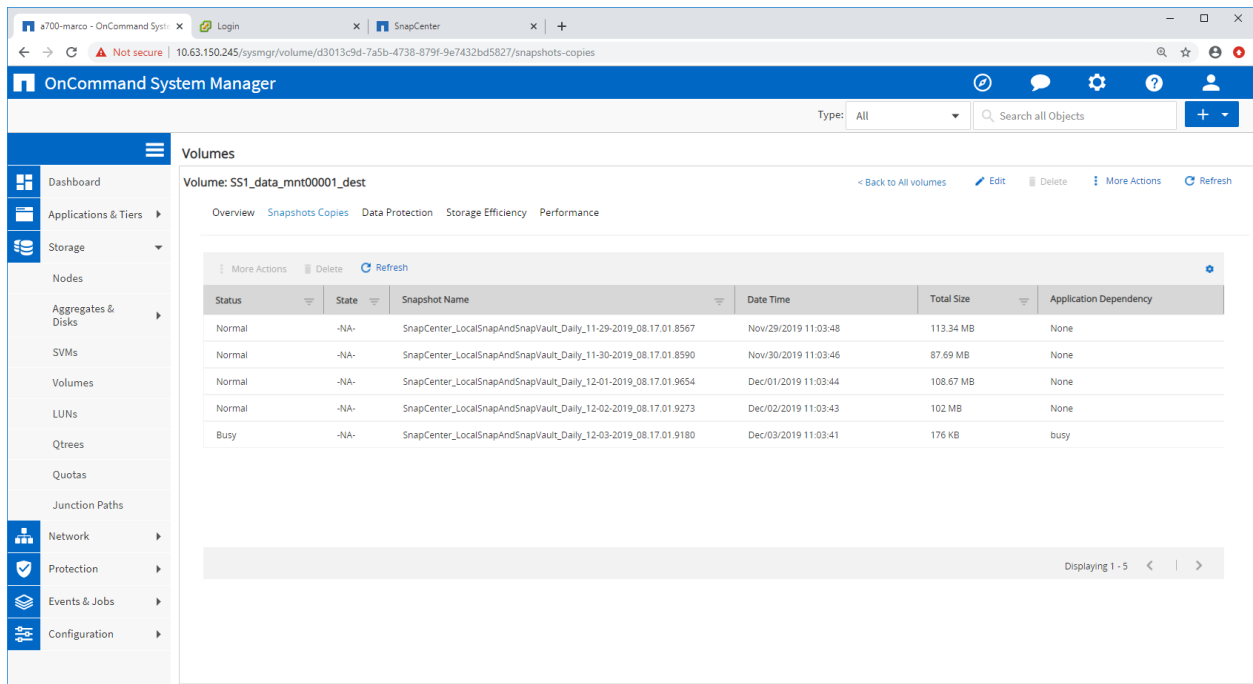
SS1_data_mnt00001 at the primary storage. Figure 35 shows the available backups for the replication target volume hana_SA1_data_mnt00001_dest at the secondary storage system. The highlighted backup is the backup shown in SnapCenter and SAP HANA Studio in the previous images and has the same naming convention.

Figure 34) Backups at the primary storage.



Status	State	Snapshot Name	Date Time	Total Size	Application Dependency
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-01-2019_08.17.01.9654	Dec/01/2019 11:03:44	106.27 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_06.30.01.3164	Dec/02/2019 09:16:42	74.76 MB	None
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08.17.01.9273	Dec/02/2019 11:03:43	17.21 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_10.30.01.4510	Dec/02/2019 13:16:42	39.11 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_14.30.01.3366	Dec/02/2019 17:16:42	87.53 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_18.30.01.3834	Dec/02/2019 21:16:41	95.67 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_22.30.01.4925	Dec/03/2019 01:16:41	29.86 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-03-2019_02.30.01.5053	Dec/03/2019 05:16:41	43.81 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-03-2019_06.30.01.4088	Dec/03/2019 09:16:40	49.46 MB	None
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-03-2019_08.17.01.9180	Dec/03/2019 11:03:41	77.14 MB	snapmirror
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-03-2019_10.30.01.4554	Dec/03/2019 13:16:40	42.12 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-03-2019_14.30.01.3902	Dec/03/2019 17:16:40	57.42 MB	None

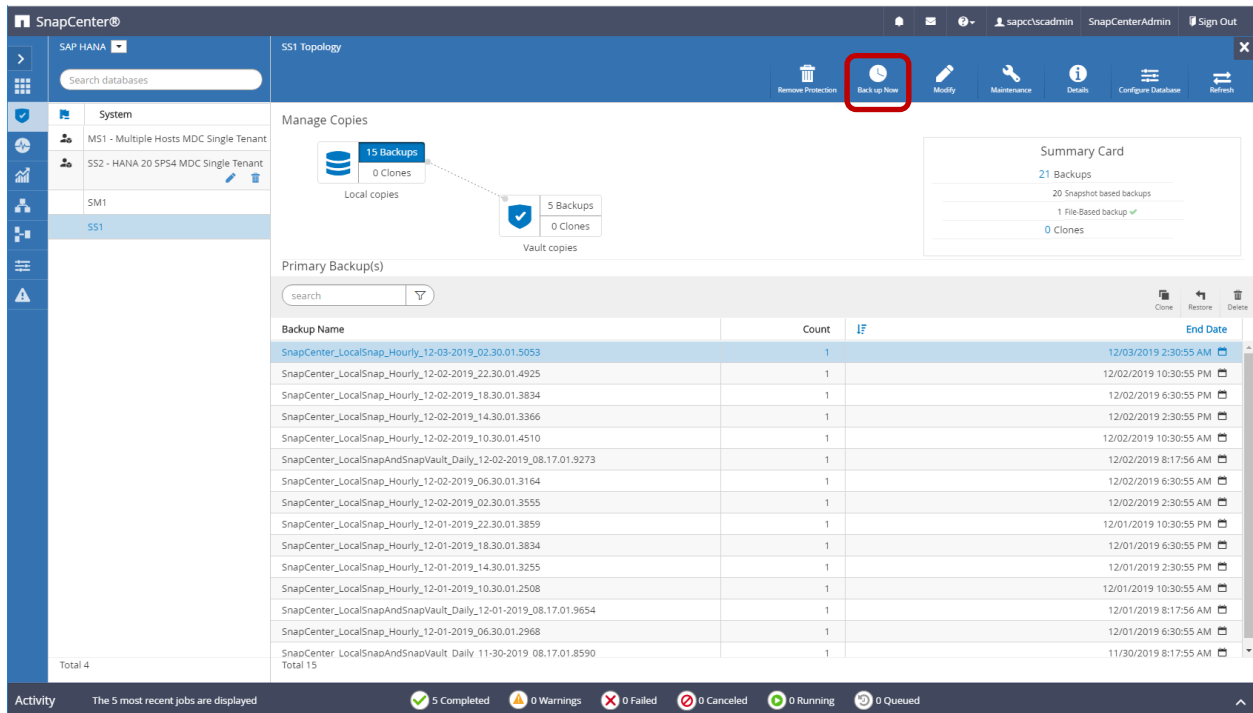
Figure 35) Backups at the secondary storage.



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 have been 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).



- 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 then click Backup to start the on-demand backup.

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 the “Resource protection configuration” section.

Note: You must close and reopen the topology view to see the updated backup list.

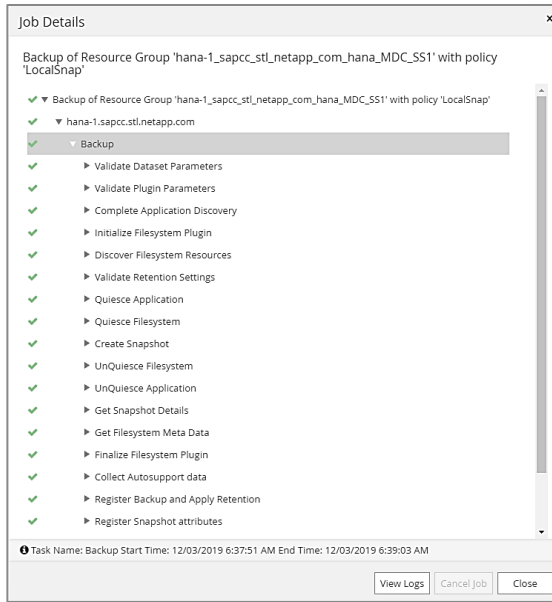
The screenshot shows the SnapCenter web interface. The top navigation bar includes 'SAP HANA', 'SS1 Topology', and various action icons like 'Remove Protection', 'Back up Now', 'Modify', 'Maintenance', 'Details', 'Configure Database', and 'Refresh'. The main content area is divided into two sections: 'Manage Copies' and 'Primary Backup(s)'. The 'Manage Copies' section shows a diagram with 'Local copies' (16 Backups, 0 Clones) and 'Vault copies' (5 Backups, 0 Clones). The 'Primary Backup(s)' section contains a table of backup jobs.

Backup Name	Count	IF	End Date
SnapCenter_LocalSnap_12-03-2019_06:37:50.1491	1		12/03/2019 6:38:44 AM
SnapCenter_LocalSnap_Hourly_12-03-2019_06:30:01.4088	1		12/03/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053	1		12/03/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_22:30:01.4925	1		12/02/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_18:30:01.3834	1		12/02/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_14:30:01.3366	1		12/02/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_10:30:01.4510	1		12/02/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08:17:01.9273	1		12/02/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_06:30:01.3164	1		12/02/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_02:30:01.3555	1		12/02/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-01-2019_22:30:01.3859	1		12/01/2019 10:30:55 PM
Total 4	Total 16		

Below the table is the 'Activity' section, which shows the 5 most recent jobs. The first job is highlighted:

Time Ago	Job Description	Status
2 minutes ago	Backup of Resource Group 'hana-1_sapcc_stl_netapp_com_hana_MDC_SS1' with policy 'LocalSnap'	Completed
10 minutes ago	Backup of Resource Group 'hana-1_sapcc_stl_netapp_com_hana_MDC_SS1' with policy 'LocalSnap'	Completed
12 minutes ago	Backup of Resource Group 'hana-2_sapcc_stl_netapp_com_hana_MDC_SM1' with policy 'LocalSnap'	Completed
35 minutes ago	Backup of Resource Group 'SnapCenter-43_sapcc_stl_netapp_com_hana_MDC_SS2' with policy 'LocalSnap'	Completed
3 hours ago	Backup of Resource Group 'SnapCenter-43_sapcc_stl_netapp_com_hana_MDC_MS1' with policy 'LocalSnap'	Completed

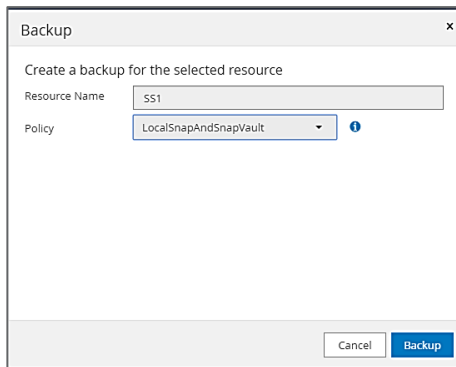
- The job details are shown when clicking the job's activity line in the Activity area.
You can open a detailed job log by clicking View Logs.



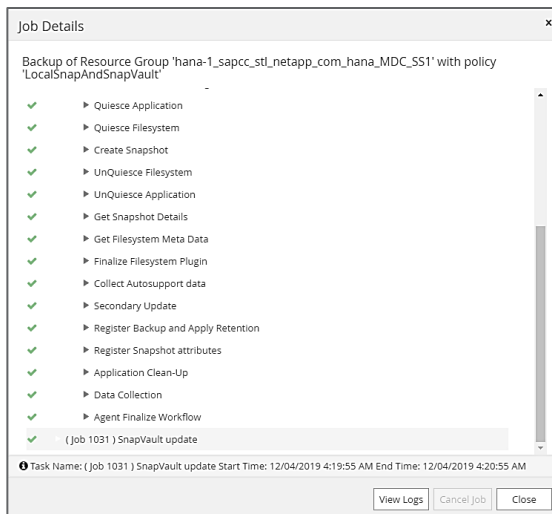
4. In SAP HANA Studio, the new backup is visible in the backup catalog. The same backup name in SnapCenter is also used in the comment and the EBID field in the backup catalog.

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 Backup Now icon to start an on-demand backup. From the drop-down list, select the backup policy `LocalSnapAndSnapVault`, then click Backup to start the on-demand backup.

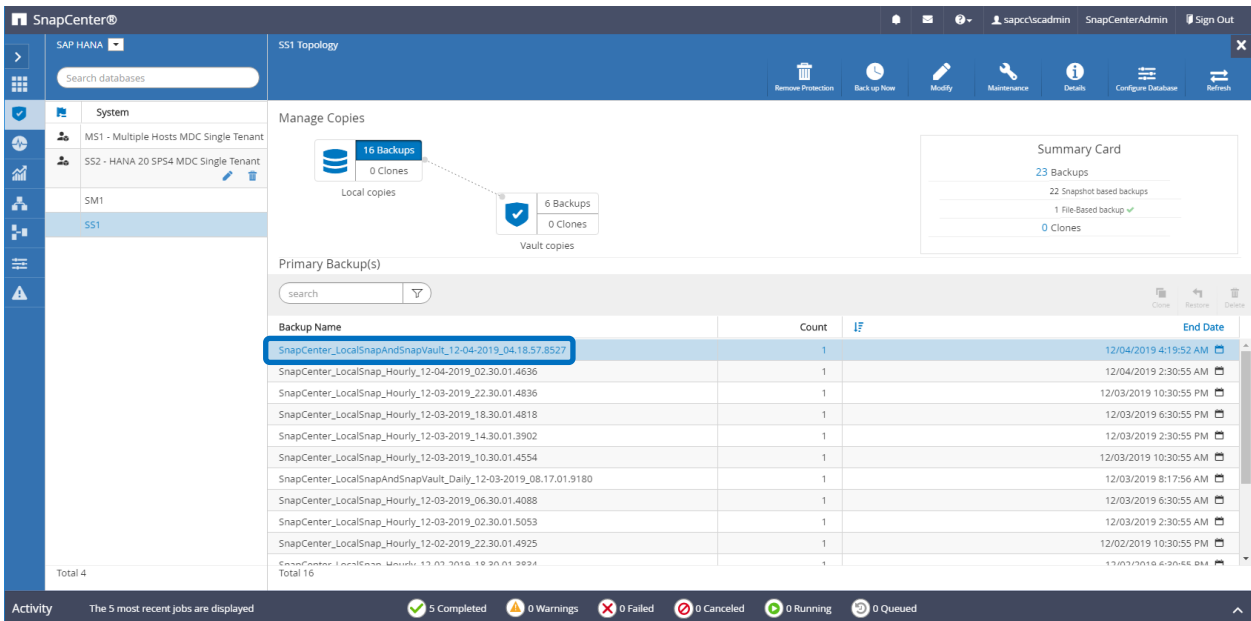


3. The job details are shown when clicking the job's activity line in the Activity area.



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 the “Resource protection configuration” section.

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.

The screenshot displays the SnapCenter interface for SAP HANA. The left sidebar shows the 'System' section with a list of tenants: 'MS1 - Multiple Hosts MDC Single Tenant', 'SS2 - HANA 20 SP54 MDC Single Tenant', 'SM1', and 'SS1'. The main content area is titled 'SS1 Topology' and 'Manage Copies'. It features a diagram showing 'Local copies' (16 Backups, 0 Clones) and 'Vault copies' (6 Backups, 0 Clones). A 'Summary Card' on the right provides statistics: 23 Backups, 22 Snapshot based backups, 1 File Based backup, and 0 Clones. Below the diagram is a table of 'Secondary Vault Backup(s)'. The table has three columns: 'Backup Name', 'Count', and 'End Date'. The first row is highlighted, showing the backup name 'SnapCenter_LocalSnapAndSnapVault_12-04-2019_04.18.57.8527' with a count of 1 and an end date of '12/04/2019 4:19:52 AM'. The table lists several other backups with counts of 1 and end dates ranging from 12/03/2019 to 11/29/2019. At the bottom, an 'Activity' bar shows the status of recent jobs: 5 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, and 0 Queued.

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.

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 36) Block integrity check.

The screenshot shows the SnapCenter interface for managing backups. On the left, a sidebar lists system components like 'MS1 - Multiple Hosts MDC Single Tenant' and 'SS1'. The main area is titled 'Manage Copies' and shows a visual representation of backup copies: 15 Local copies and 5 Vault copies. A 'Summary Card' on the right provides a high-level overview: 22 Backups, 20 Snapshot based backups, and 2 File-Based backups. Below this, a table lists individual backup entries with columns for Backup Name, Count, and End Date. The bottom of the interface features an 'Activity' bar indicating 'The 5 most recent jobs are displayed' with a status summary: 5 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, and 0 Queued.

A block integrity check backup cannot be deleted using the SnapCenter UI, but it can be deleted using PowerShell commands.

```
PS C:\Users\scadmin> Get-SmBackupReport -Resource SS1
```

```
SmBackupId          : 9
SmJobId             : 42
StartDateTime        : 11/19/2019 8:26:32 AM
EndDateTime          : 11/19/2019 8:27:33 AM
Duration             : 00:01:00.7652030
CreatedDateTime       : 11/19/2019 8:27:24 AM
Status               : Completed
ProtectionGroupName   : hana-1_sapcc_stl_netapp_com_hana_MDC_SS1
SmProtectionGroupId   : 1
PolicyName            : BlockIntegrityCheck
SmPolicyId            : 5
BackupName            : SnapCenter_BlockIntegrityCheck_11-19-2019_08.26.33.2913
VerificationStatus     : NotApplicable
VerificationStatuses  :
SmJobError            :
BackupType            : SCC_BACKUP
CatalogingStatus      : NotApplicable
CatalogingStatuses    :
ReportDataCreatedDateTime :
PluginCode             : SCC
PluginName             : hana
JobTypeId             : 0
JobHost               :
```

```
PS C:\Users\scadmin> Remove-SmBackup -BackupIds 9
```

```
Remove-SmBackup
```

```
Are you sure want to remove the backup(s).
```

```
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
```

```
BackupResult : {}
```

```

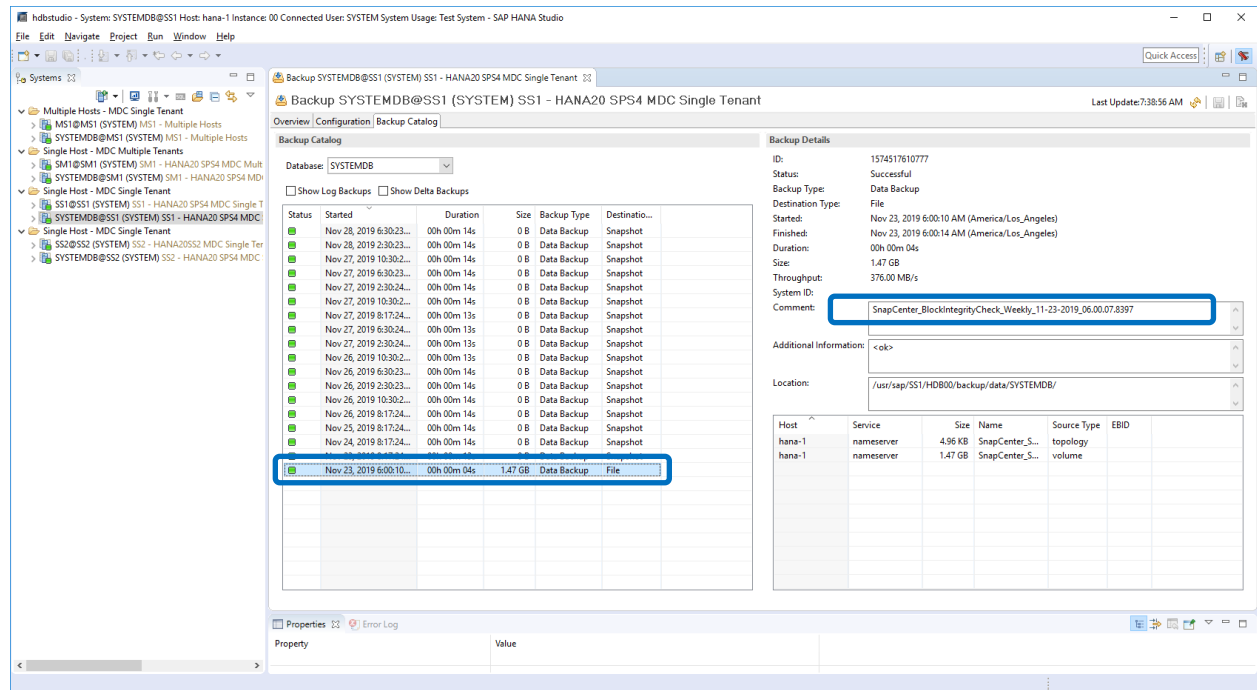
Result      : SMCoreContracts.SMResult
TotalCount  : 0
DisplayCount : 0
Context     :
Job         : SMCoreContracts.SmJob

```

```
PS C:\Users\scadmin>
```

The SAP HANA backup catalog shows entries for both the system and the tenant databases. Figure 37 shows a SnapCenter block integrity check in the backup catalog of the system database.

Figure 37) File-based backup for system database in SAP HANA Studio.



A successful block integrity check creates standard SAP HANA data backup files. SnapCenter uses the backup path that has been configured in the HANA database for file-based data backup operations.

```

hana-1:/usr/sap/SS1/HDB00/backup/data # ls -al *
DB_SS1:
total 1710840
drwxr-xr-- 2 ssladm sapsys      4096 Nov 28 10:25 .
drwxr-xr-- 4 ssladm sapsys      4096 Nov 19 05:11 ..
-rw-r----- 1 ssladm sapsys 155648 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ssladm sapsys 83894272 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-2019_06.00.07.8397_databackup_2_1
-rw-r----- 1 ssladm sapsys 1660952576 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-2019_06.00.07.8397_databackup_3_1

SYSTEMDB:
total 1546340
drwxr-xr-- 2 ssladm sapsys      4096 Nov 28 10:24 .
drwxr-xr-- 4 ssladm sapsys      4096 Nov 19 05:11 ..
-rw-r----- 1 ssladm sapsys 159744 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ssladm sapsys 1577066496 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-2019_06.00.07.8397_databackup_1_1

```

Restore and recovery

The following sections describe the restore and recovery workflows of three different scenarios and example configurations.

- Automated restore and recovery:
 - Auto discovered HANA system SS1
SAP HANA single host, MDC single tenant system using NFS
- Single tenant restore and recovery:
 - Auto discovered HANA system SM1
SAP HANA single host, MDC multiple tenant system using NFS
- Restore with manual recovery:
 - Manual configured HANA system SS2
SAP HANA single host, MDC multiple tenant system using NFS

In the following sections, the differences between SAP HANA single host and multiple hosts and Fibre Channel SAN attached HANA systems are highlighted.

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

Automated restore and recovery

With SnapCenter 4.3, automated restore and recovery operations are supported for HANA single container or MDC single tenant systems that have been auto discovered by SnapCenter.

You can execute an automated restore and recovery operation with the following steps:

1. Select the backup to be used for the restore operation. The backup can be selected from the following storage options:
 - Primary storage
 - Offsite backup storage (SnapVault target)
2. Select the restore type. Select Complete Restore with Volume Revert or without Volume Revert.
Note: The Volume Revert option is only available for restore operations from primary storage and if the HANA database is using NFS as the storage protocol.
3. Select the recovery type from the following options:
 - To most recent state
 - Point in time
 - To specific data backup
 - No recovery

Note: The selected recovery type is used for the recovery of the system and the tenant database.

Next, SnapCenter performs the following operations:

1. Stops the HANA database.
2. Restores the database.

Depending on the selected restore type and the used storage protocol, different operations are executed.

- If NFS and Volume Revert are selected, SnapCenter:
 - a. Unmounts the volume
 - b. Restores the volume using volume-based SnapRestore on the storage layer

- c. Mounts the volume
 - If NFS is selected and Volume Revert is not selected, SnapCenter:
 - a. Restores all files using single file SnapRestore operations on the storage layer
 - If Fibre Channel SAN is selected, SnapCenter:
 - a. Unmounts the LUN(s)
 - b. Restores the LUN(s) using single file SnapRestore operations on the storage layer
 - c. Discovers and mounts the LUN(s)
 3. Recovers the database:
 - a. Recovers the system database
 - b. Recovers the tenant database
- Or, for HANA single container systems, the recovery is done in a single step:
- a. Starts the HANA database

Note: If No Recovery is selected, SnapCenter exits and the recovery operation for the system and the tenant database must be done manually.

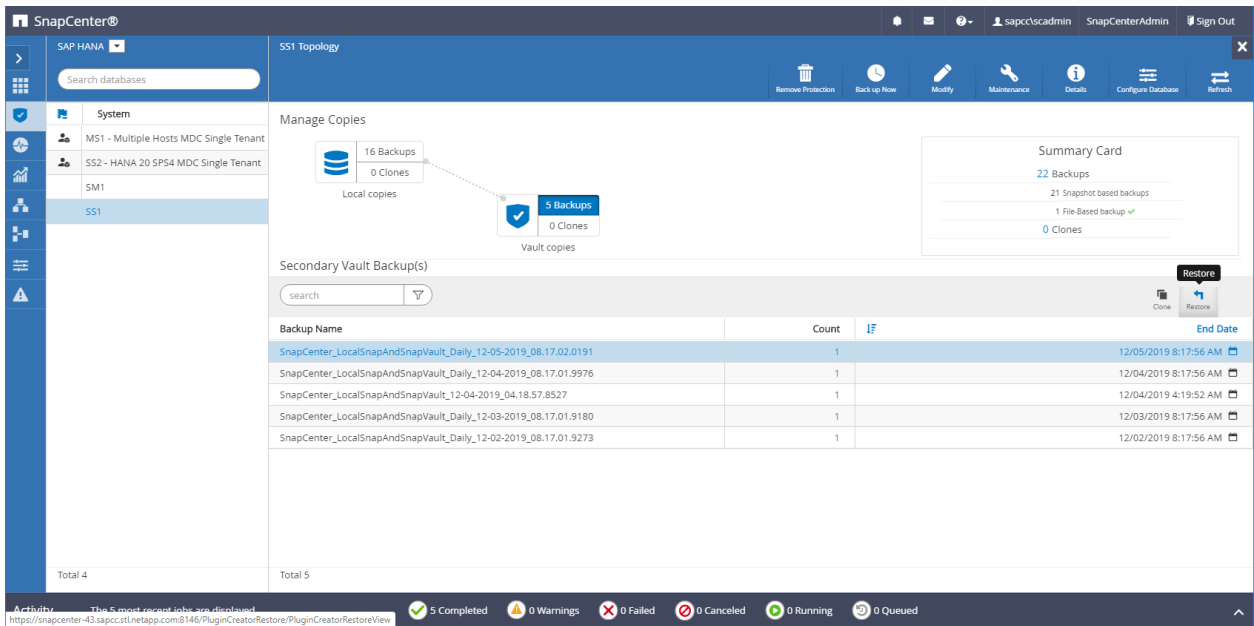
This section provides the steps for the automated restore and recovery operation of the auto discovered HANA system SS1 (SAP HANA single host, MDC single tenant system using NFS).

1. Select a backup in SnapCenter to be used for the restore operation.

Note: You can select restore from primary or from offsite backup storage.

The screenshot shows the SnapCenter web interface for managing SAP HANA backups. The left sidebar shows the navigation menu with 'System' selected. The main area displays the 'Manage Copies' section for system 'SS1'. It shows a hierarchy of backups: 16 Backups (Local copies) and 6 Backups (Vault copies). A 'Summary Card' on the right provides a high-level overview: 23 Backups, 22 Snapshot based backups, 1 File-based backup, and 0 Clones. Below this, a table lists individual backups with their names, counts, and end dates. The bottom status bar shows the overall system health: 5 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, and 0 Queued.

Backup Name	Count	End Date
SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385	1	12/05/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-05-2019_18.30.01.5244	1	12/05/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-05-2019_14.30.01.6022	1	12/05/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-05-2019_10.30.01.5450	1	12/05/2019 10:30:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-05-2019_08.17.02.0191	1	12/05/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-05-2019_06.30.01.5487	1	12/05/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-05-2019_02.30.01.5470	1	12/05/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-04-2019_22.30.01.5182	1	12/04/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-04-2019_18.30.01.5249	1	12/04/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-04-2019_14.30.01.5069	1	12/04/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-04-2019_10.30.01.5300	1	12/04/2019 10:30:55 AM
Total 4	Total 16	

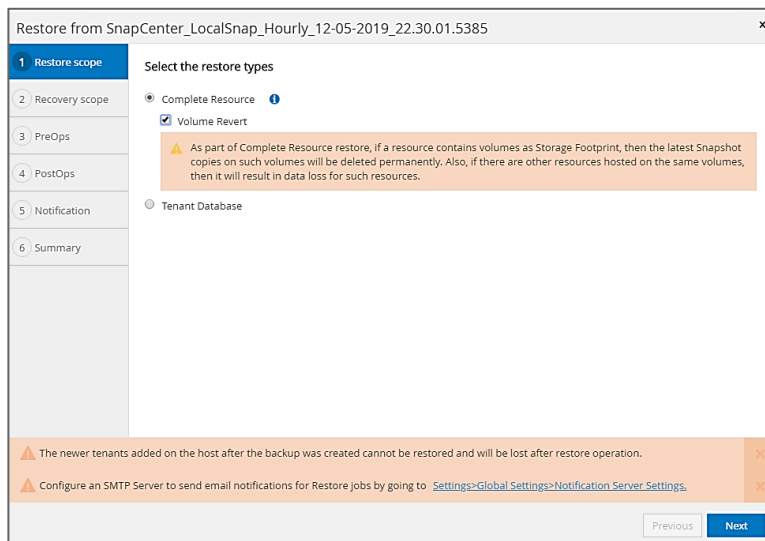


2. Select the restore scope and type.

The following three screenshots show the restore options for restore from primary with NFS, restore from secondary with NFS, and restore from primary with Fibre Channel SAN.

The restore type options for restore from primary storage.

Note: The Volume Revert option is only available for restore operations from primary with NFS.



The restore type options for restore from offsite backup storage.

Restore from SnapCenter_LocalSnapAndSnapVault_Daily_12-05-2019_08.17.02.0191

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☒ Complete Resource ⓘ

☐ Tenant Database

Choose archive location

hana-primary.sapcc.stf.netapp.com:SS1_data_mre00001

hana-backup.sapcc.stf.netapp.com:SS1_data

The newer tenants added on the host after the backup was created cannot be restored and will be lost after restore operation.

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous Next

The restore type options for restore from primary storage with Fibre Channel SAN.

Restore from SnapCenter_LocalSnap_Hourly_12-16-2019_22.35.01.3065

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☒ Complete Resource ⓘ

☐ Tenant Database

The newer tenants added on the host after the backup was created cannot be restored and will be lost after restore operation.

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous Next

3. Select Recovery Scope and provide the location for log backup and catalog backup.

Note: SnapCenter uses the default path or the changed paths in the HANA global.ini file to pre-populate the log and catalog backup locations.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope
2 Recovery scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Recover database files using

☒ Recover to most recent state ⓘ
☐ Recover to point in time ⓘ
☐ Recover to specified data backup ⓘ
☐ No recovery ⓘ

Specify log backup locations ⓘ

Add

Specify backup catalog location ⓘ

Recovery options are applicable to both system database and tenant database.

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous Next

4. Enter the optional prerestore commands.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope
2 Recovery scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Enter optional commands to run before performing a restore operation ⓘ

Pre restore command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous Next

5. Enter the optional post-restore commands.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope
2 Recovery scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Enter optional commands to run after performing a restore operation ⓘ
Post restore command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous
Next

6. Enter the optional email settings.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope
2 Recovery scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Provide email settings ⓘ
Email preference: Never
From: Email from
To: Email to
Subject: Notification
☐ Attach Job Report

If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous
Next

7. To start the restore operation, click Finish.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Summary

Backup Name	SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385
Backup date	12/05/2019 10:30:55 PM
Restore scope	Complete Resource with Volume Revert
Recovery scope	Recover to most recent state
Log backup locations	/mnt/log-backup
Backup catalog location	/mnt/log-backup
Pre restore command	
Post restore command	
Send email	No

If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous

Finish

- SnapCenter executes the restore and recovery operation. This example shows the job details of the restore and recovery job.

Job Details

Restore 'hana-1.sapcc.stl.netapp.com\hana\MDC\SS1'

▼ Restore 'hana-1.sapcc.stl.netapp.com\hana\MDC\SS1'

▼ hana-1.sapcc.stl.netapp.com

▼ Restore

▼ Validate Plugin Parameters

▼ Pre Restore Application

▶ Stopping HANA instance

▼ Filesystem Pre Restore

▶ Determining the restore mechanism

▶ Deporting file systems and associated entities

▶ Restore Filesystem

▼ Filesystem Post Restore

▶ Building file systems and associated entities

▼ Recover Application

▶ Recovering system database

▶ Checking HDB services status

▶ Recovering tenant database 'SS1'

▶ Starting HANA instance

▶ Clear Catalog on Server

▶ Application Clean-Up

▶ Data Collection

▶ Agent Finalize Workflow

Task Name: Recover Application Start Time: 12/06/2019 7:26:11 AM End Time: 12/06/2019 7:28:46 AM

View Logs

Cancel Job

Close

Single tenant restore and recovery operation

With SnapCenter 4.3, single tenant restore operations are supported for HANA MDC systems with a single tenant or with multiple tenants that have been auto discovered by SnapCenter.

You can perform a single tenant restore and recovery operation with the following steps:

77

SAP HANA backup and recovery with SnapCenter

© 2022 NetApp, Inc. All rights reserved.

1. Stop the tenant to be restored and recovered
2. Restore the tenant with SnapCenter
 - For a restore from primary storage, SnapCenter executes the following operations:
 - NFS: Storage Single File SnapRestore operations for all files of the tenant database
 - SAN: Clone and connect the LUN to the database host, and copy all files of the tenant database
 - For a restore from secondary storage, SnapCenter executes the following operations:
 - NFS: Storage SnapVault Restore operations for all files of the tenant database
 - SAN: Clone and connect the LUN to the database host, and copy all files of the tenant database
3. Recover the tenant with HANA Studio, Cockpit, or SQL statement

This section provides the steps for the restore and recovery operation from the primary storage of the auto discovered HANA system SM1 (SAP HANA single host, MDC multiple tenant system using NFS). From the user input perspective, the workflows are identical for a restore from secondary or a restore in a Fibre Channel SAN setup.

1. Stop the tenant database.

```
smladm@hana-2:/usr/sap/SM1/HDB00> hdbsql -U SYSKEY

Welcome to the SAP HANA Database interactive terminal.

Type:  \h for help with commands
       \q to quit

hdbsql=>
hdbsql SYSTEMDB=> alter system stop database tenant2;
0 rows affected (overall time 14.215281 sec; server time 14.212629 sec)

hdbsql SYSTEMDB=>
```

2. Select a backup in SnapCenter to be used for the restore operation

The screenshot displays the SnapCenter web interface. On the left, a sidebar shows the navigation menu with options like 'System', 'MS1 - Multiple Hosts MDC Single Tenant', 'SS2 - HANA 20 SP54 MDC Single Tenant', 'SM1', and 'SS1'. The main area is titled 'Manage Copies' and shows a 'Summary Card' with '13 Backups' and '0 Clones'. Below this, a table lists 'Primary Backup(s)' with columns for 'Backup Name', 'Count', 'if', and 'End Date'. The table contains 12 rows of backup information, including names like 'SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445' and their respective counts and end dates. At the bottom, there is an 'Activity' bar showing the status of various jobs: 5 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, and 0 Queued.

3. Select the tenant to be restored.

Note: SnapCenter shows a list of all tenants that are included in the selected backup.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope
2 Recovery scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Select the restore types

☐ Complete Resource
☒ Tenant Database

Select tenant database

Select tenant database
SM1
TENANT2

Stop the tenant before performing the tenant restore operation.

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous
Next

Single tenant recovery is not supported with SnapCenter 4.3. No Recovery is preselected and cannot be changed.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope
2 Recovery scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Recover database files using

☐ Recover to most recent state
☐ Recover to point in time
☐ Recover to specified data backup
☒ No recovery

Recovery of a multitenant database container with multiple tenants is not supported

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous
Next

4. Enter the optional prerestore commands.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope
2 Recovery scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Enter optional commands to run before performing a restore operation ⓘ

Pre restore command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous Next

5. Enter optional post-restore commands.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope
2 Recovery scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Enter optional commands to run after performing a restore operation ⓘ

Post restore command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous Next

6. Enter the optional email settings.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope
2 Recovery scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Provide email settings

Email preference
Never

From
Email from

To
Email to

Subject
Notification

☐ Attach Job Report

⚠ If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous
Next

7. To start the restore operation, click Finish.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope
2 Recovery scope
3 PreOps
4 PostOps
5 Notification
6 Summary

Summary

Backup Name
SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

Backup date
12/05/2019 10:28:55 PM

Restore scope
Restore tenant database 'TEHANTZ'

Recovery scope
No recovery

Pre restore command

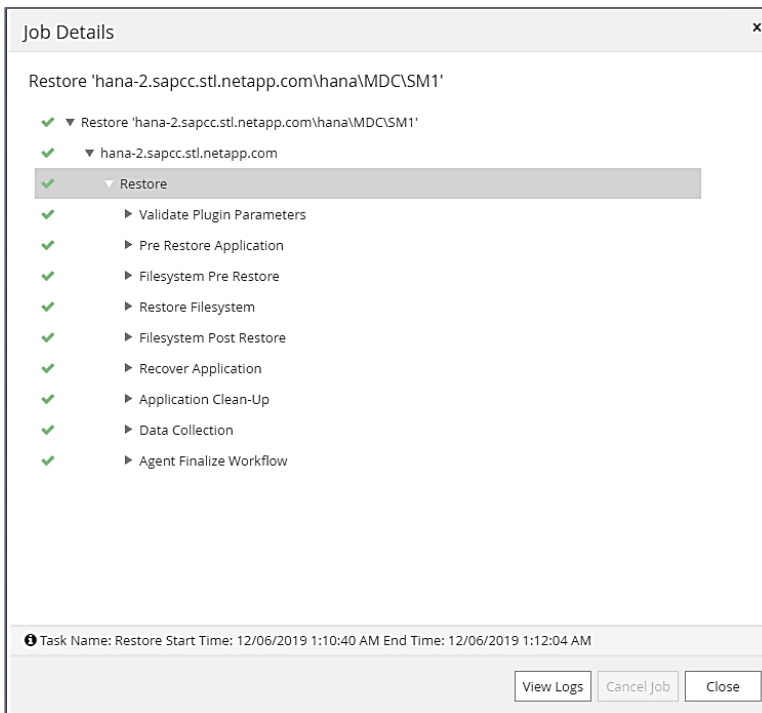
Post restore command

Send email
No

⚠ If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous
Finish

The restore operation is executed by SnapCenter. This example shows the job details of the restore job.



Note: When the tenant restore operation is finished, only the tenant relevant data is restored. On the file system of the HANA database host, the restored data file and the Snapshot backup ID file of the tenant is available.

```
smladm@hana-2:/usr/sap/SM1/HDB00> ls -al /hana/data/SM1/mnt00001/*
-rw-r--r-- 1 smladm sapsys 17 Dec 6 04:01 /hana/data/SM1/mnt00001/nameserver.lck

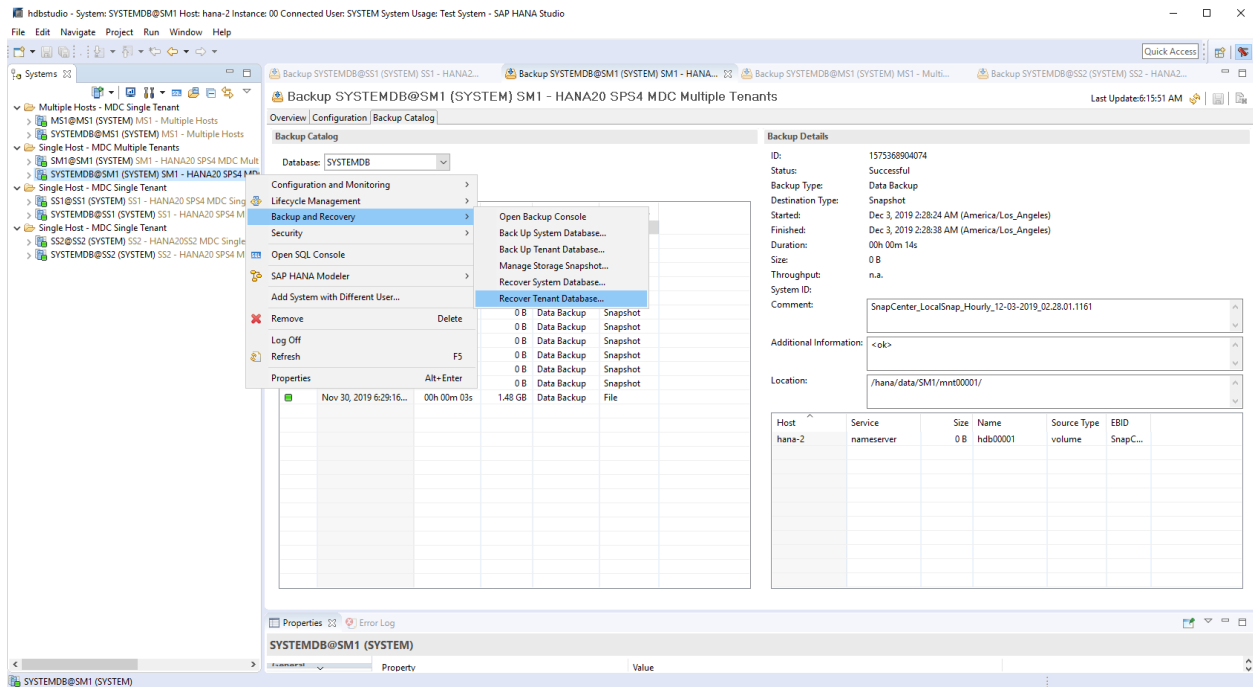
/hana/data/SM1/mnt00001/hdb00001:
total 3417776
drwxr-x--- 2 smladm sapsys 4096 Dec 6 01:14 .
drwxr-x--- 6 smladm sapsys 4096 Nov 20 09:35 ..
-rw-r----- 1 smladm sapsys 3758096384 Dec 6 03:59 datavolume_0000.dat
-rw-r----- 1 smladm sapsys 0 Nov 20 08:36 __DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 smladm sapsys 36 Nov 20 08:37 landscape.id

/hana/data/SM1/mnt00001/hdb00002.00003:
total 67772
drwxr-xr-- 2 smladm sapsys 4096 Nov 20 08:37 .
drwxr-x--- 6 smladm sapsys 4096 Nov 20 09:35 ..
-rw-r--r-- 1 smladm sapsys 201441280 Dec 6 03:59 datavolume_0000.dat
-rw-r--r-- 1 smladm sapsys 0 Nov 20 08:37 __DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__

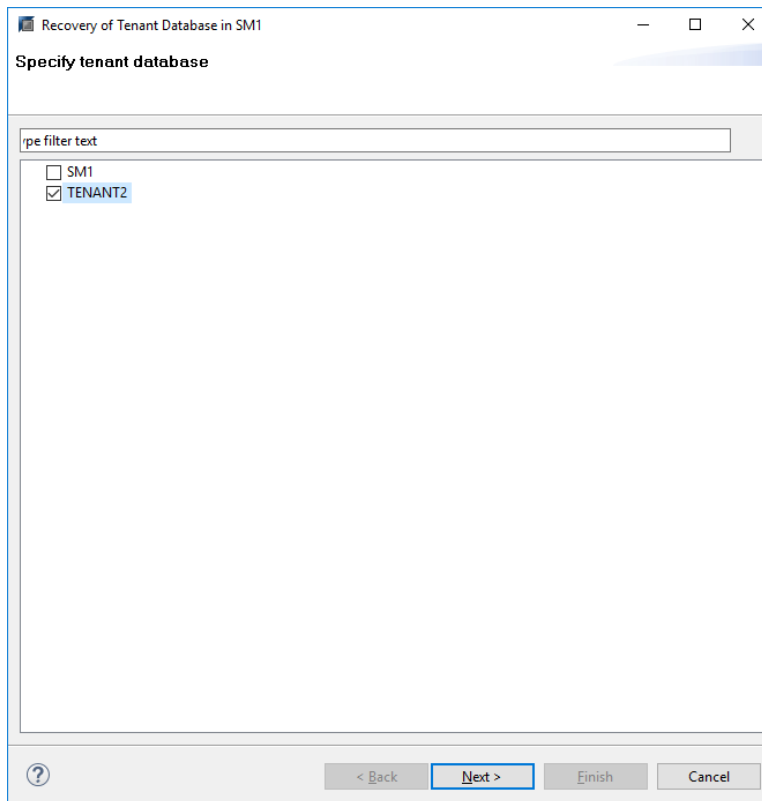
/hana/data/SM1/mnt00001/hdb00002.00004:
total 3411836
drwxr-xr-- 2 smladm sapsys 4096 Dec 6 03:57 .
drwxr-x--- 6 smladm sapsys 4096 Nov 20 09:35 ..
-rw-r--r-- 1 smladm sapsys 3758096384 Dec 6 01:14 datavolume_0000.dat
-rw-r--r-- 1 smladm sapsys 0 Nov 20 09:35 __DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 smladm sapsys 155648 Dec 6 01:14 snapshot_databackup_0_1

/hana/data/SM1/mnt00001/hdb00003.00003:
total 3364216
drwxr-xr-- 2 smladm sapsys 4096 Dec 6 01:14 .
drwxr-x--- 6 smladm sapsys 4096 Nov 20 09:35 ..
-rw-r--r-- 1 smladm sapsys 3758096384 Dec 6 03:59 datavolume_0000.dat
-rw-r--r-- 1 smladm sapsys 0 Nov 20 08:37 __DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
smladm@hana-2:/usr/sap/SM1/HDB00>
```

8. Start the recovery with HANA Studio.



9. Select the tenant.



10. Select the recovery type.

Recovery of Tenant Database in SM1

Specify Recovery Type

Select a recovery type.

☒ Recover the database to its most recent state [?]
☐ Recover the database to the following point in time [?]

Date: Time:
 Select Time Zone:

ⓘ System Time Used (GMT): 2019-12-06 09:18:31

☐ Recover the database to a specific data backup [?]

Advanced >>

? < Back Next > Finish Cancel

11. Provide the backup catalog location.

Recovery of Tenant Database in SM1

Locate Backup Catalog

Specify location of the backup catalog.

☒ Recover using the backup catalog

☒ Search for the backup catalog in the file system only

Backup Catalog Location:

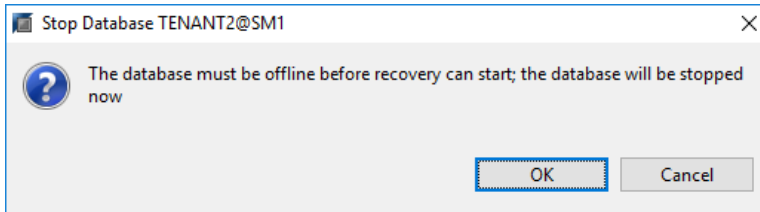
☐ Recover without the backup catalog

Backint System Copy

☐ Backint System Copy

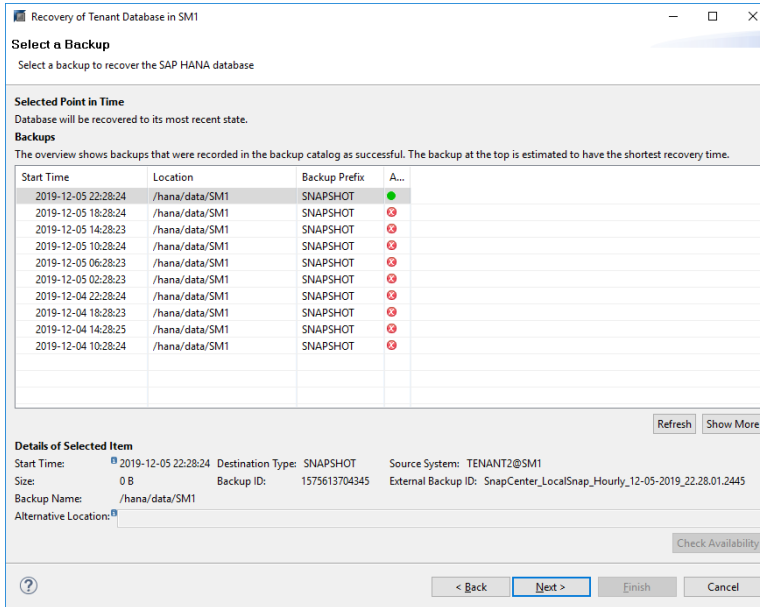
Source System:

? < Back Next > Finish Cancel

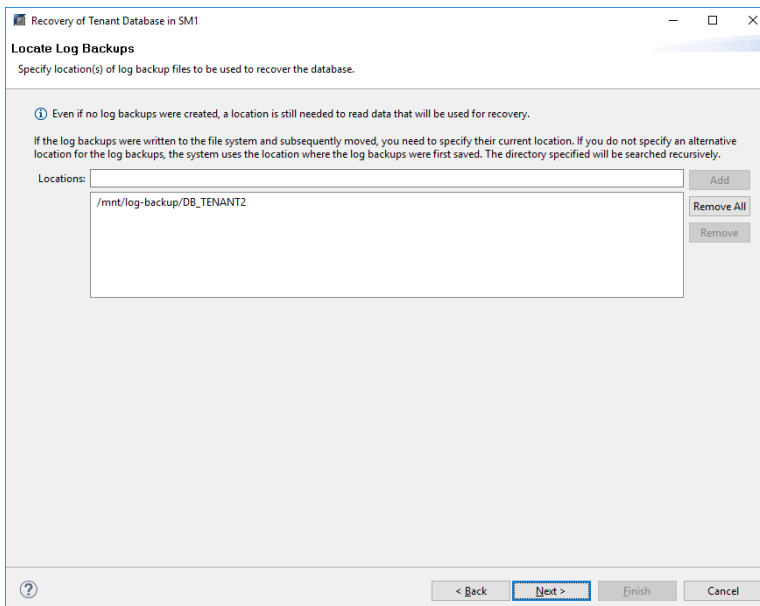


Within the backup catalog, the restored backup is highlighted with a green icon. The external backup ID shows the backup name that was previously selected in SnapCenter.

12. Select the entry with the green icon and click Next.



13. Provide the log backup location.



14. Select the other settings as required.

The screenshot shows the 'Other Settings' window of the 'Recovery of Tenant Database in SM1' wizard. The window contains several sections with checkboxes and text instructions:

- Check Availability of Delta and Log Backups:** A text block explaining that the system can check for available delta and log backups at the start of the recovery process. It includes a checkbox for 'File System' (checked) and 'Third-Party Backup Tool (Backint)' (unchecked).
- Initialize Log Area:** A text block explaining that log segments in the log area will be deleted after recovery. It includes a checkbox for 'Initialize Log Area' (unchecked).
- Use Delta Backups:** A text block explaining that delta backups are used for recovery. It includes a checkbox for 'Use Delta Backups (Recommended)' (checked).
- Install New License Key:** A text block explaining that the old license key will no longer be valid. It includes a checkbox for 'Install New License Key' (unchecked) and a 'Browse' button.

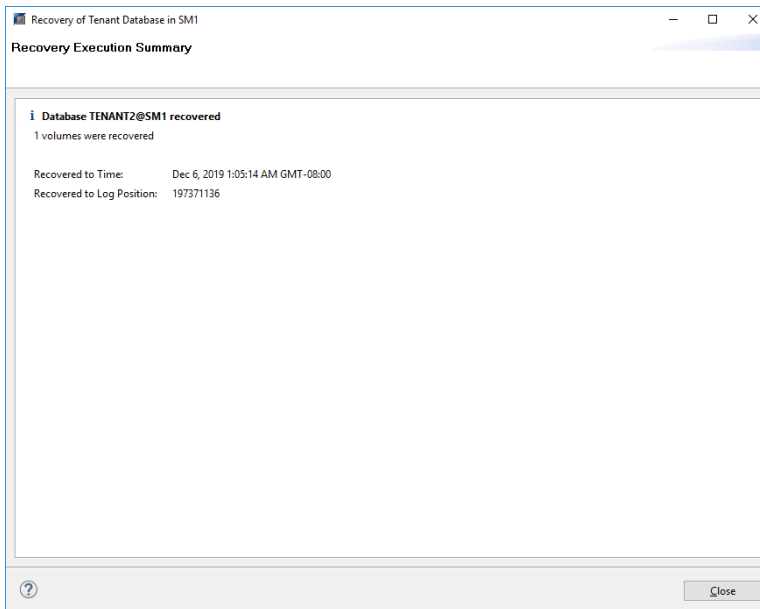
At the bottom, there are navigation buttons: '< Back', 'Next >' (highlighted), 'Finish', and 'Cancel'.

15. Start the tenant recovery operation.

The screenshot shows the 'Review Recovery Settings' window of the 'Recovery of Tenant Database in SM1' wizard. The window displays a summary of the recovery settings:

- Database Information:** A table showing the database name 'TENANT2@SM1', host 'hana-2', and version '2.00.040.00.1553674765'.
- Recovery Definition:** A table showing the recovery type 'Snapshot (Point-in-Time Recovery (Until Now))'.
- Configuration File Handling:** A section with a 'Caution' icon and text stating that customer-specific configuration changes may need to be made manually in the target system. It includes a link to 'More Information: SAP HANA Administration Guide'.

At the bottom, there is a 'Show SQL Statement' button and navigation buttons: '< Back', 'Next >', 'Finish' (highlighted), and 'Cancel'.



Restore with manual recovery

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

1. 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. 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.

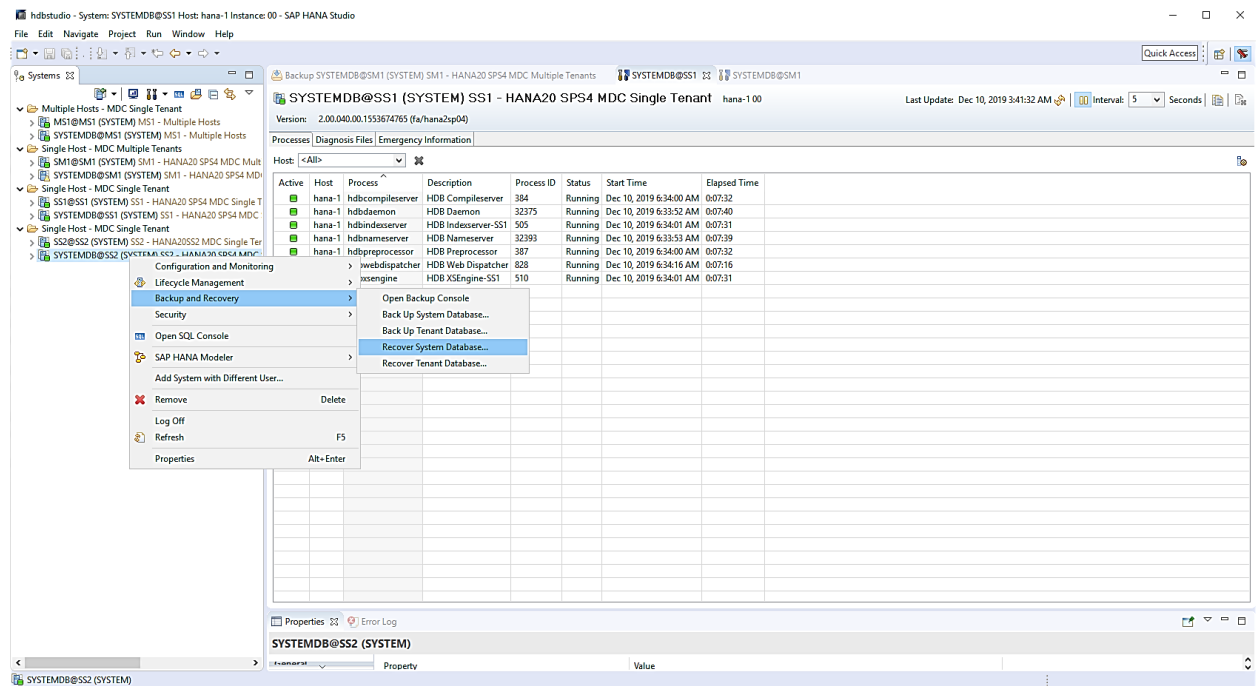
3. Run the recovery process for the system database with SAP HANA Studio:
 - a. Click Refresh from the backup list and select the available backup for recovery (indicated with a green icon).
 - b. Start the recovery process. After the recovery process is finished, the system database is started.
4. Run the recovery process for the tenant database with SAP HANA Studio:
 - a. Select Recover Tenant Database and select the tenant to be recovered.
 - b. Select the recovery type and the log backup location.

A list of data backups displays. Because the data volume has already been restored, the tenant backup is indicated as available (in green).

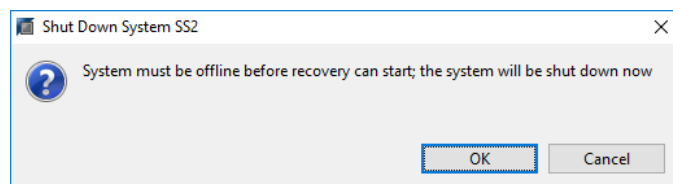
- c. Select this backup and start the recovery process. After the recovery process is finished, the tenant database is started automatically.

The following section describes the steps of the restore and recovery operations of the manually configured HANA system SS2 (SAP HANA single host, MDC multiple tenant system using NFS).

1. In SAP HANA Studio, select the Recover System Database option to start the recovery of the system database.



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



The SAP HANA system shuts down and the recovery wizard is started.

3. Select the recovery type and click Next.

Recovery of SYSTEMDB@SS2

Specify Recovery Type

Select a recovery type.

☒ Recover the database to its most recent state [?]

☐ Recover the database to the following point in time [?]

Date: Time:

Select Time Zone:

ⁱ System Time Used (GMT): 2019-12-10 11:43:03

☐ Recover the database to a specific data backup [?]

Advanced >>

[?] < Back **Next >** Finish Cancel

4. Provide the location of the backup catalog and click Next.

Recovery of SYSTEMDB@SS2

Locate Backup Catalog

Specify location of the backup catalog.

☒ Recover using the backup catalog

☒ Search for the backup catalog in the file system only

Backup Catalog Location:

☐ Recover without the backup catalog

Backint System Copy

☐ Backint System Copy

Source System:

[?] < Back **Next >** Finish Cancel

- 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.

Recovery of SYSTEMDB@SS2

Select a Backup

To recover this snapshot, it must be available in the data area.

Selected Point in Time
Database will be recovered to its most recent state.

Backups
The overview shows backups that were recorded in the backup catalog as successful. The backup at the top is estimated to have the shortest recovery time.

Start Time	Location	Backup Prefix	Available
2019-12-10 02:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 22:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 18:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 14:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 10:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 06:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 02:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-08 22:05:07	/hana/data/SS2	SNAPSHOT	✗
2019-12-08 18:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-08 14:05:08	/hana/data/SS2	SNAPSHOT	✗

Details of Selected Item

Start Time: 2019-12-10 02:05:08 Destination Type: SNAPSHOT Source System: SYSTEMDB@SS2

Size: 0 B Backup ID: 1575972308584 External Backup ID: SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

Backup Name: /hana/data/SS2

Alternative Location:

Buttons: Refresh, Show More, Check Availability, < Back, Next >, Finish, Cancel

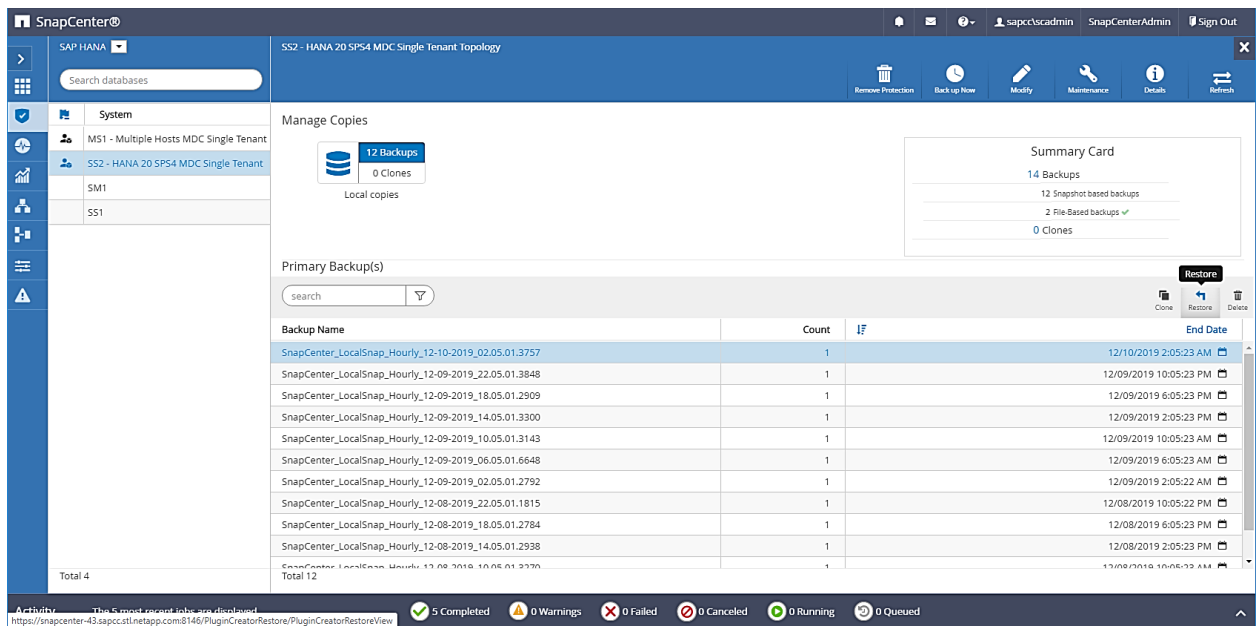
- Unmount all data volumes.

```
umount /hana/data/SS2/mnt00001
```

Note: For an SAP HANA multiple host system with NFS, all data volumes on each host must be unmounted.

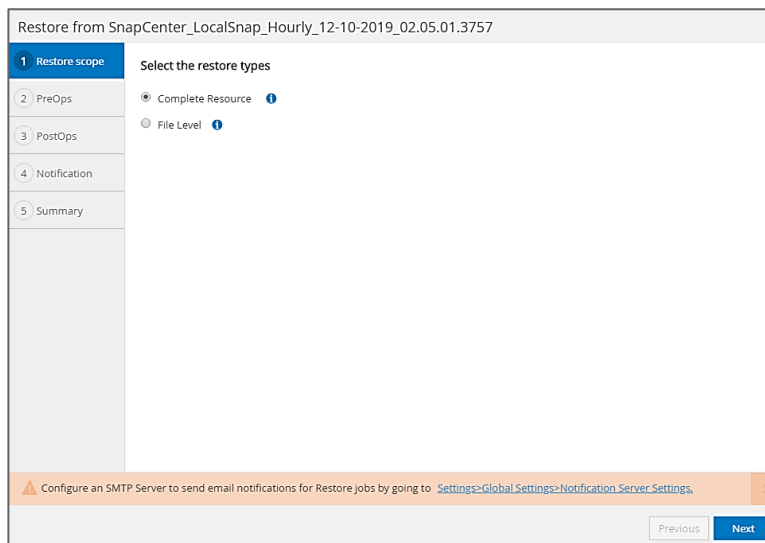
Note: In an SAP HANA multiple-host setup with FC, the unmount operation is executed by the SAP HANA name server as a part of the shutdown process.

- 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 or File Level.
Select Complete Resource to use a volume-based restore.



9. Select File Level and All to use a single file SnapRestore operation for all files.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Select the restore types

Complete Resource

File Level

Select files to restore

Volume/Qtree	All	File Path
<input checked="" type="checkbox"/> hana-primary.sapcc.stl.netapp.com/vol/SS...	<input checked="" type="checkbox"/>	<div>Provide one or more file paths separated by comma</div>

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

PreviousNext

Note: For a file-level restore of a SAP HANA multiple host system, select all the volumes.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_07.15.01.1435

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Select the restore types

Complete Resource

File Level

Select files to restore

Volume/Qtree	All	File Path
<input checked="" type="checkbox"/> hana-primary.sapcc.stl.netapp.com/vol/M...	<input checked="" type="checkbox"/>	<div>Provide one or more file paths separated by comma</div>
<input checked="" type="checkbox"/> hana-primary.sapcc.stl.netapp.com/vol/M...	<input checked="" type="checkbox"/>	<div>Provide one or more file paths separated by comma</div>

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

PreviousNext

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

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope
2 PreOps
3 PostOps
4 Notification
5 Summary

Enter optional commands to run before performing a restore operation ⓘ

Pre restore command

Unmount command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous Next

11. Specify the optional commands and click Next.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope
2 PreOps
3 PostOps
4 Notification
5 Summary

Enter optional commands to run after performing a restore operation ⓘ

Mount command

Post restore command

Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings](#).

Previous Next

12. Specify the notification settings so that SnapCenter can send a status email and job log. Click Next.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope
2 PreOps
3 PostOps
4 Notification
5 Summary

Provide email settings

Email preference: Never

From: Email from

To: Email to

Subject: Notification

☐ Attach Job Report

If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

PreviousNext

13. Review the summary and click Finish to start the restore.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope
2 PreOps
3 PostOps
4 Notification
5 Summary

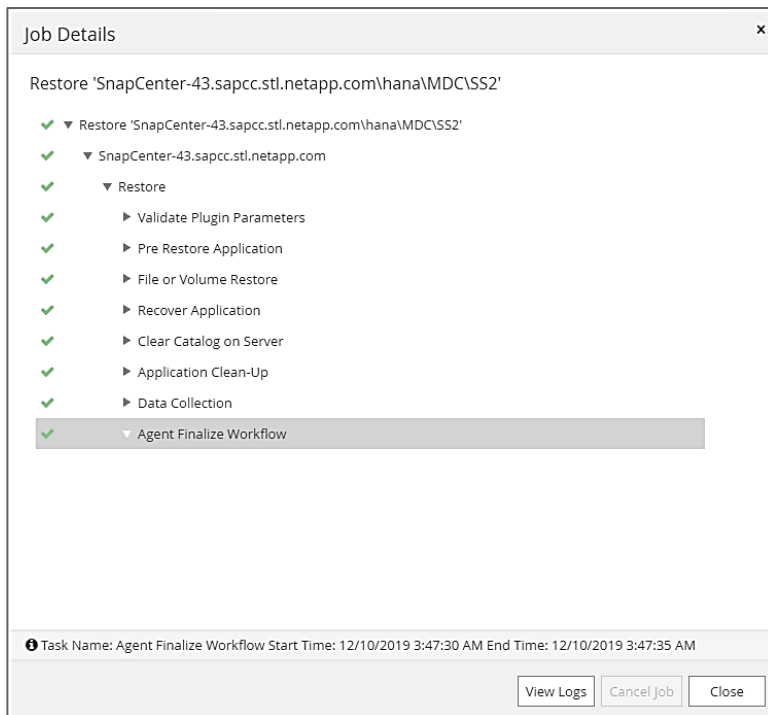
Summary

Backup Name: SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757
Backup date: 12/10/2019 2:05:23 AM
Restore scope: Complete Resource
Pre restore command
Unmount command
Mount command
Post restore command
Send email: No

If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

PreviousFinish

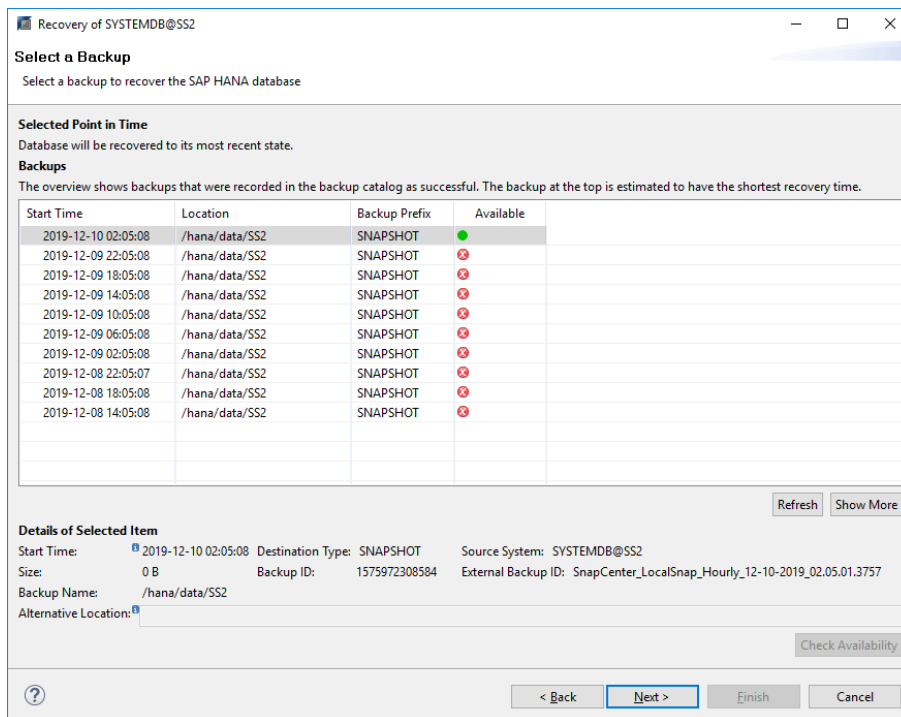
14. The restore job starts, and the job log can be displayed by double-clicking the log line in the activity pane.



- 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
```

- 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.



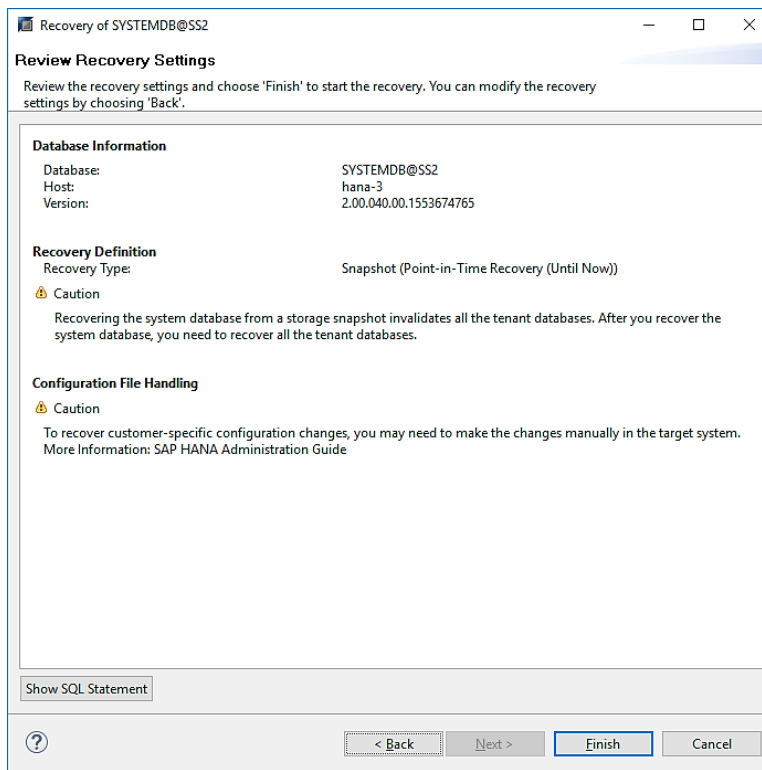
17. Provide the location of the log backups. Click Next.

The screenshot shows a window titled "Recovery of SYSTEMDB@SS2" with a sub-header "Locate Log Backups". Below the sub-header is the instruction "Specify location(s) of log backup files to be used to recover the database." A help icon and text explain that a location is needed even if no backups were created, and that the system searches recursively if no alternative location is specified. A text input field labeled "Locations:" contains the path "/mnt/log-backup/SYSTEMDB". To the right of the input field are three buttons: "Add", "Remove All", and "Remove". At the bottom of the window are four buttons: "< Back", "Next >" (highlighted with a blue border), "Finish", and "Cancel".

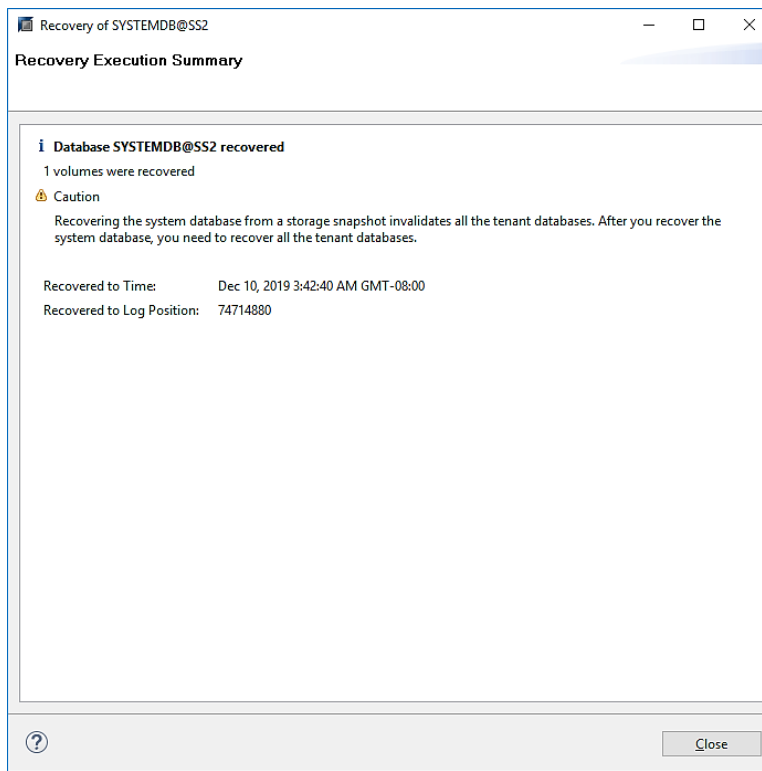
18. Select other settings as required. Make sure Use Delta Backups is not selected. Click Next.

The screenshot shows a window titled "Recovery of SYSTEMDB@SS2" with a sub-header "Other Settings". The main content area has a scroll bar and contains several sections: "Check Availability of Delta and Log Backups" with explanatory text and checkboxes for "File System" (checked) and "Third-Party Backup Tool (Backint)" (unchecked); "Initialize Log Area" with explanatory text and an unchecked "Initialize Log Area" checkbox; "Use Delta Backups" with explanatory text and an unchecked "Use Delta Backups (Recommended)" checkbox; and "Install New License Key" with explanatory text, a list of options, and an unchecked "Install New License Key" checkbox with a "Browse" button. At the bottom of the window are four buttons: "< Back", "Next >" (highlighted with a blue border), "Finish", and "Cancel".

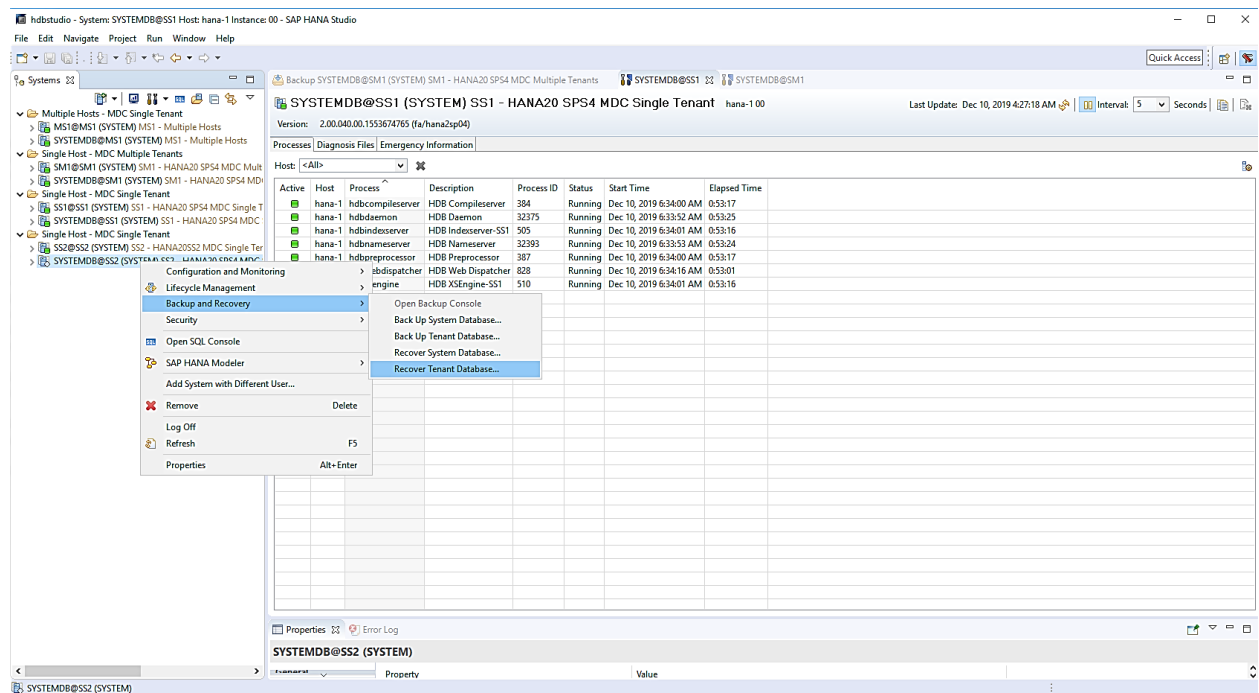
19. Review the recovery settings and click Finish.



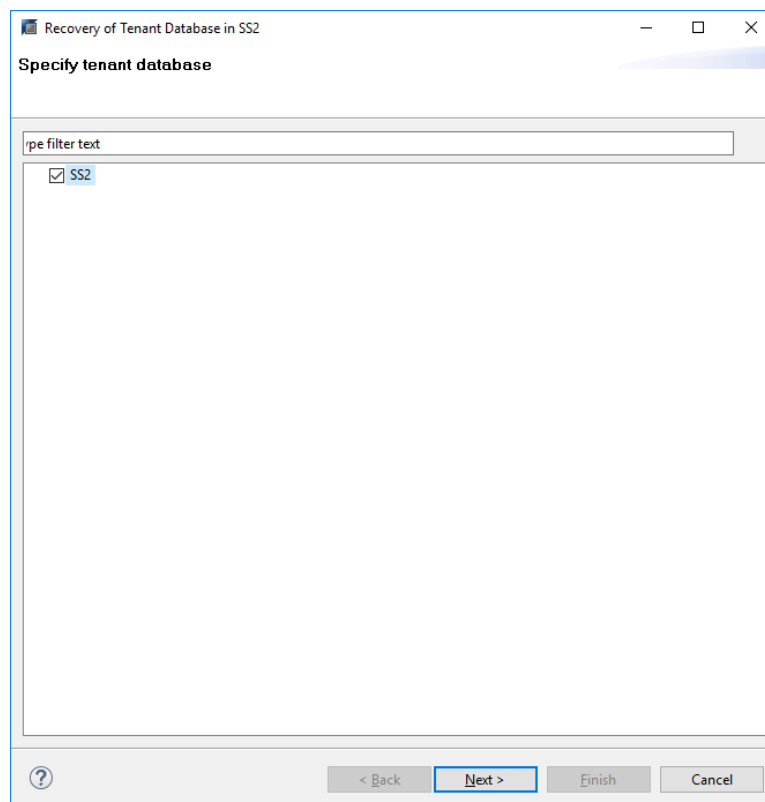
20. The recovery process starts. Wait until the recovery of the system database completes.



21. In SAP HANA Studio, select the entry for the system database and start Backup Recovery - Recover Tenant Database.



22. Select the tenant to recover and click Next.



23. Specify the recovery type and click Next.

Recovery of Tenant Database in SS2

Specify Recovery Type

Select a recovery type.

☒ Recover the database to its most recent state [?]
☐ Recover the database to the following point in time [?]

Date: Time:

Select Time Zone:

ⓘ System Time Used (GMT): 2019-12-10 12:27:22

☐ Recover the database to a specific data backup [?]

24. Confirm the backup catalog location and click Next.

Recovery of Tenant Database in SS2

Locate Backup Catalog

Specify location of the backup catalog.

☒ Recover using the backup catalog

☒ Search for the backup catalog in the file system only

Backup Catalog Location:

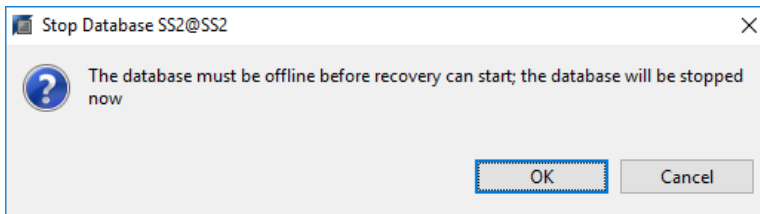
☐ Recover without the backup catalog

Backint System Copy

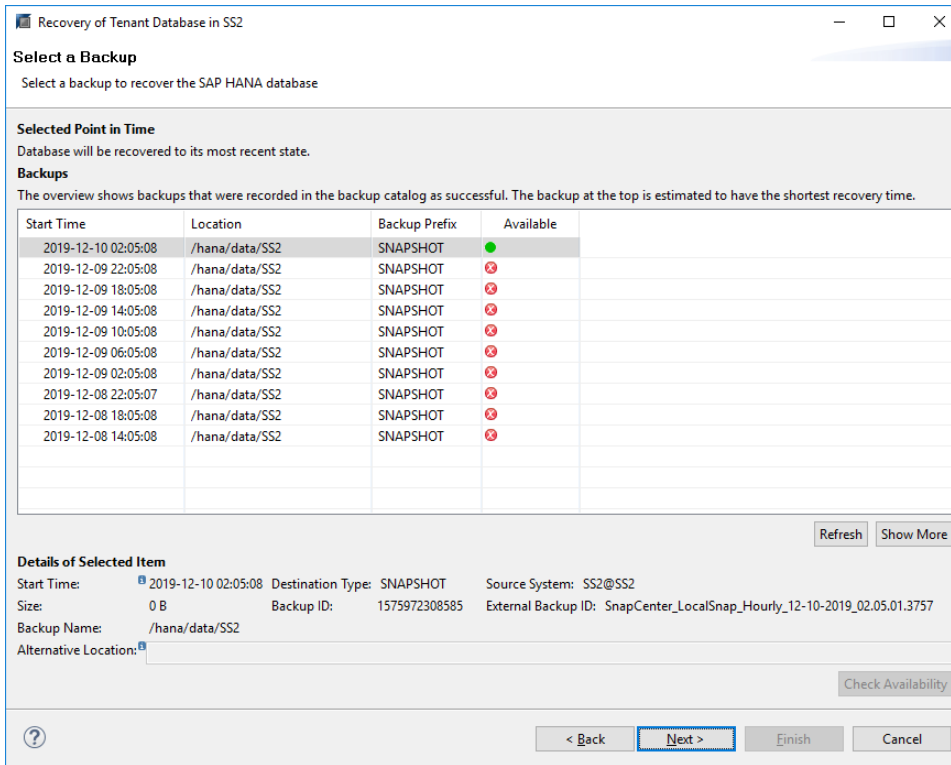
☐ Backint System Copy

Source System:

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



26. 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.



27. Confirm the log backup location and click Next.

Recovery of Tenant Database in SS2

Locate Log Backups

Specify location(s) of log backup files to be used to recover the database.

? Even if no log backups were created, a location is still needed to read data that will be used for recovery.

If the log backups were written to the file system and subsequently moved, you need to specify their current location. If you do not specify an alternative location for the log backups, the system uses the location where the log backups were first saved. The directory specified will be searched recursively.

Locations:

28. Select other settings as required. Make sure Use Delta Backups is not selected. Click Next.

Recovery of Tenant Database in SS2

Other Settings

Check Availability of Delta and Log Backups

You can have the system check whether all required delta and log backups are available at the beginning of the recovery process. If delta or log backups are missing, they will be listed and the recovery process will stop before any data is changed. If you choose not to perform this check now, it will still be performed but later. This may result in a significant loss of time if the complete recovery must be repeated.

Check the availability of delta and log backups:

☒ File System **?**

☐ Third-Party Backup Tool (Backint)

Initialize Log Area

If you do not want to recover log segments residing in the log area, select this option. After the recovery, the log entries will be deleted from the log area.

☐ Initialize Log Area **?**

Use Delta Backups

Select this option if you want to perform a recovery using delta backups. If you choose to perform a recovery without delta backups, only log backups will be used.

☐ Use Delta Backups (Recommended)

Install New License Key

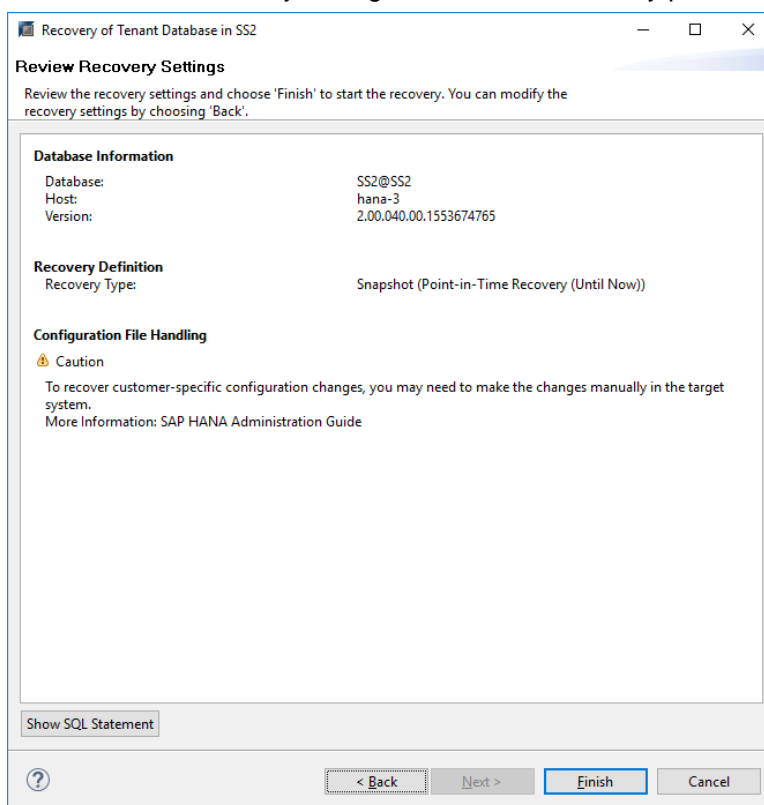
If you recover the database from a different system, the old license key will no longer be valid

You can:

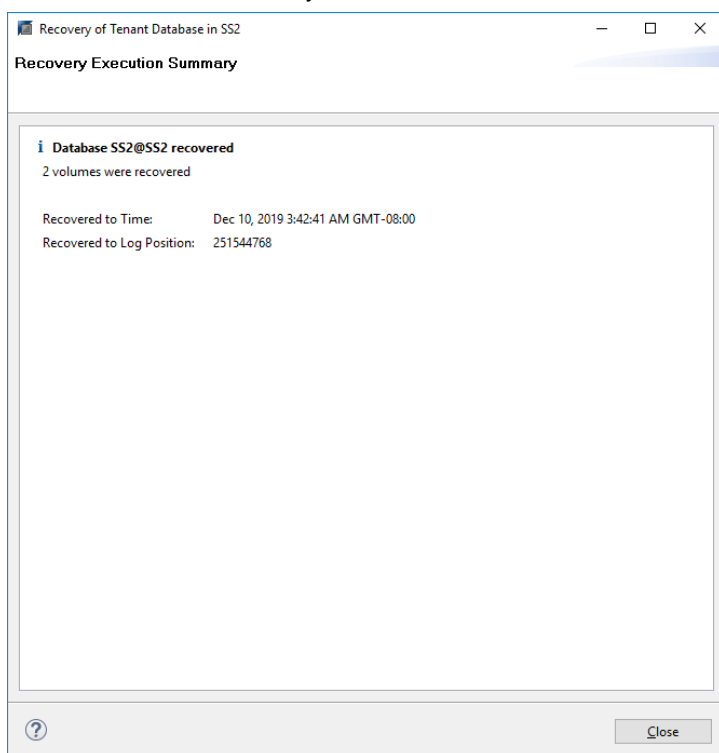
- Select a new license key to install now
- Install a new license key manually after the database has been recovered

☐ Install New License Key

29. Review the recovery settings and start the recovery process of the tenant database by clicking Finish.



30. Wait until the recovery has finished and the tenant database is started.



The SAP HANA system is up and running.

Note: For an SAP HANA MDC system with multiple tenants, you must repeat steps 20–29 for each tenant.

Advanced configuration and tuning

This section 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.

Enable secure communication to HANA database

If the HANA databases are configured with secure communication, the `hdbsql` command that is executed by SnapCenter must use additional command-line options. This can be achieved by using a wrapper script which calls `hdbsql` with the required options.

Note: There are various options to configure the SSL communication. In the following examples, the simplest client configuration is described using the command line option, where no server certificate validation is done. If certificate validation on server and/or client side is required, different `hdbsql` command line options are needed, and you must configure the PSE environment accordingly as described in the SAP HANA Security Guide.

Instead of configuring the `hdbsql` executable in the `hana.properties` files, the wrapper script is added.

For a central HANA plug-in host on the SnapCenter Windows server, you must add the following content in `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\hana.properties`.

```
HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql-ssl.cmd
```

The wrapper script `hdbsql-ssl.cmd` calls `hdbsql.exe` with the required command-line options.

```
@echo off
"C:\Program Files\sap\hdbclient\hdbsql.exe" -e -ssltrustcert %*
```

Note: The `-e -ssltrustcert hdbsql` command-line option also works for HANA systems where SSL is not enabled. This option can therefore also be used with a central HANA plug-in host, where not all HANA systems have SSL enabled or disabled.

If the HANA plug-in is deployed on individual HANA database hosts, the configuration must be done on each Linux host accordingly.

In the file `/opt/NetApp/snapcenter/scc/etc/hana.properties`, you must add the following content.

```
HANA_HDBSQL_CMD = /usr/sap/SM1/HDB12/exe/hdbsqls
```

The wrapper script `hdbsqls` calls `hdbsql` with the required command-line options.

```
#!/bin/bash
/usr/sap/SM1/HDB12/exe/hdbsql -e -ssltrustcert $*
```

Disable auto discovery on the HANA plug-in host

To disable autodiscovery on the HANA plug-in host, complete the following steps:

1. On the SnapCenter Server, open PowerShell. Connect to the SnapCenter Server by running the `Open-SmConnection` command and specify the user name and password in the opening login window.

2. To disable auto discovery, run the `Set-SmConfigSettings` command.

For a HANA host `hana-2`, the command would be:

```
PS C:\Users\administrator.SAPCC> Set-SmConfigSettings -Agent -Hostname hana-2 -configSettings @{"DISABLE_AUTO_DISCOVERY"="true"}

Name                               Value
----                               -
DISABLE_AUTO_DISCOVERY            true

PS C:\Users\administrator.SAPCC>
```

3. Verify the configuration by running the `Get-SmConfigSettings` command.

```
PS C:\Users\administrator.SAPCC> Get-SmConfigSettings -Agent -Hostname hana-2 -key all
Key: CUSTOMPLUGINS_OPERATION_TIMEOUT_IN_MSEC      Value: 3600000      Details: Plug-in API
operation Timeout
Key: CUSTOMPLUGINS_HOSTAGENT_TO_SERVER_TIMEOUT_IN_SEC  Value: 1800        Details: Web Service
API Timeout
Key: CUSTOMPLUGINS_ALLOWED_CMDS                    Value: *;           Details: Allowed Host
OS Commands
Key: DISABLE_AUTO_DISCOVERY                        Value: true         Details:
Key: PORT                                           Value: 8145        Details: Port for
server communication
PS C:\Users\administrator.SAPCC>
```

The configuration is written to the agent configuration file on the host and will be still available after a plug-in upgrade with SnapCenter.

```
hana-2:/opt/NetApp/snapcenter/scc/etc # cat /opt/NetApp/snapcenter/scc/etc/agent.properties |
grep DISCOVERY
DISABLE_AUTO_DISCOVERY = true
hana-2:/opt/NetApp/snapcenter/scc/etc #
```

Deactivate automated log backup housekeeping

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

Edit 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:

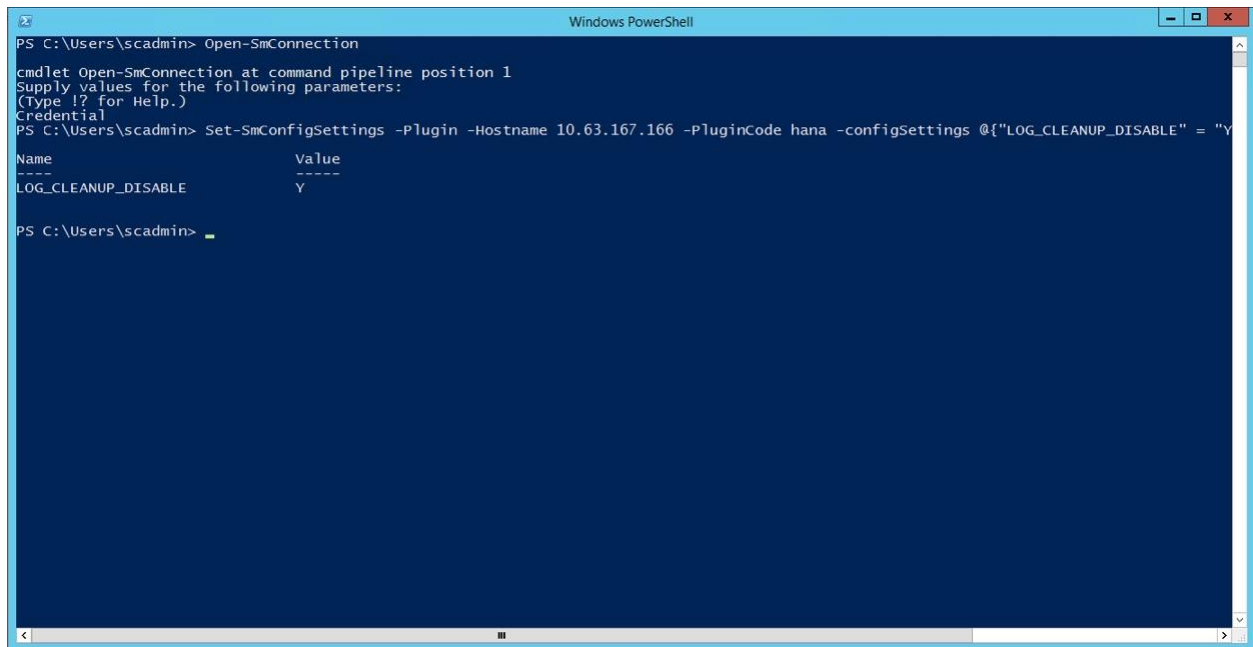
- For the Hdbsql communication host on Windows, the `hana.property` file is located at `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc`.
- For the Hdbsql communication host on Linux, the `hana.property` file is located at `/opt/NetApp/snapcenter/scc/etc`.

Use the 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 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 the IP or host name (see Figure 38).

Figure 38) PowerShell command to disable log backup housekeeping.



```
PS C:\Users\scadmin> Open-SmConnection
cmdlet Open-SmConnection at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
Credential
PS C:\Users\scadmin> Set-SmConfigSettings -Plugin -Hostname 10.63.167.166 -PluginCode hana -configSettings @{LOG_CLEANUP_DISABLE} = "Y"

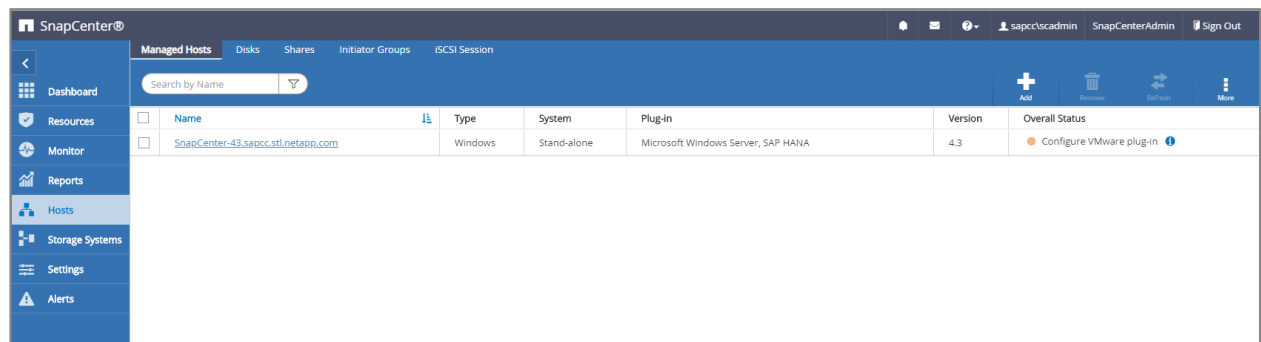
Name                Value
-----
LOG_CLEANUP_DISABLE Y

PS C:\Users\scadmin>
```

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. This could be a VMware environment or a SnapCenter installation at a public cloud provider. In this case, SnapCenter displays a warning to configure the hypervisor, as shown in Figure 39.

Figure 39) SnapCenter warning to configure hypervisor.

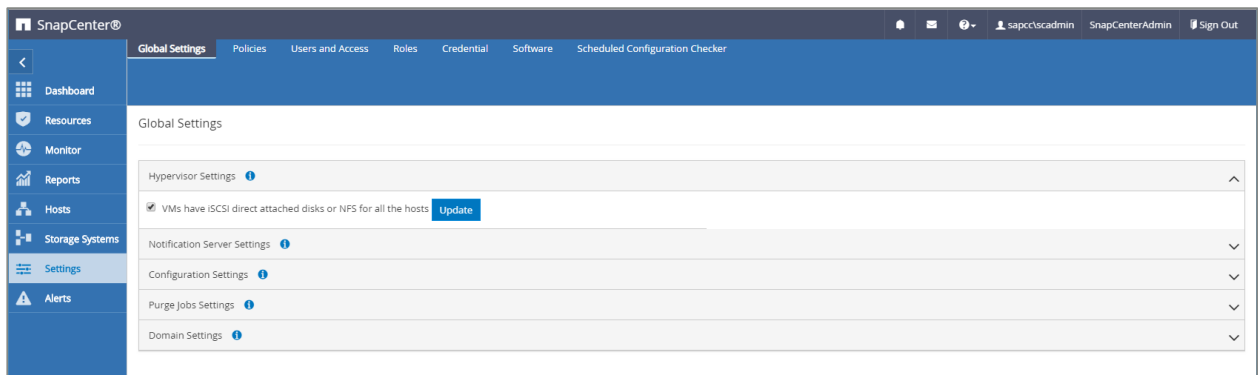


It is possible to suppress this warning globally. In this case, SnapCenter is not aware of virtualized environments, and therefore, does not show these warnings.

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

1. From 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.

Figure 40) Disable hypervisor settings.



Change scheduling frequency of backup synchronization with off-site backup storage

As described in section “Retention management of backups at the secondary storage”, 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.

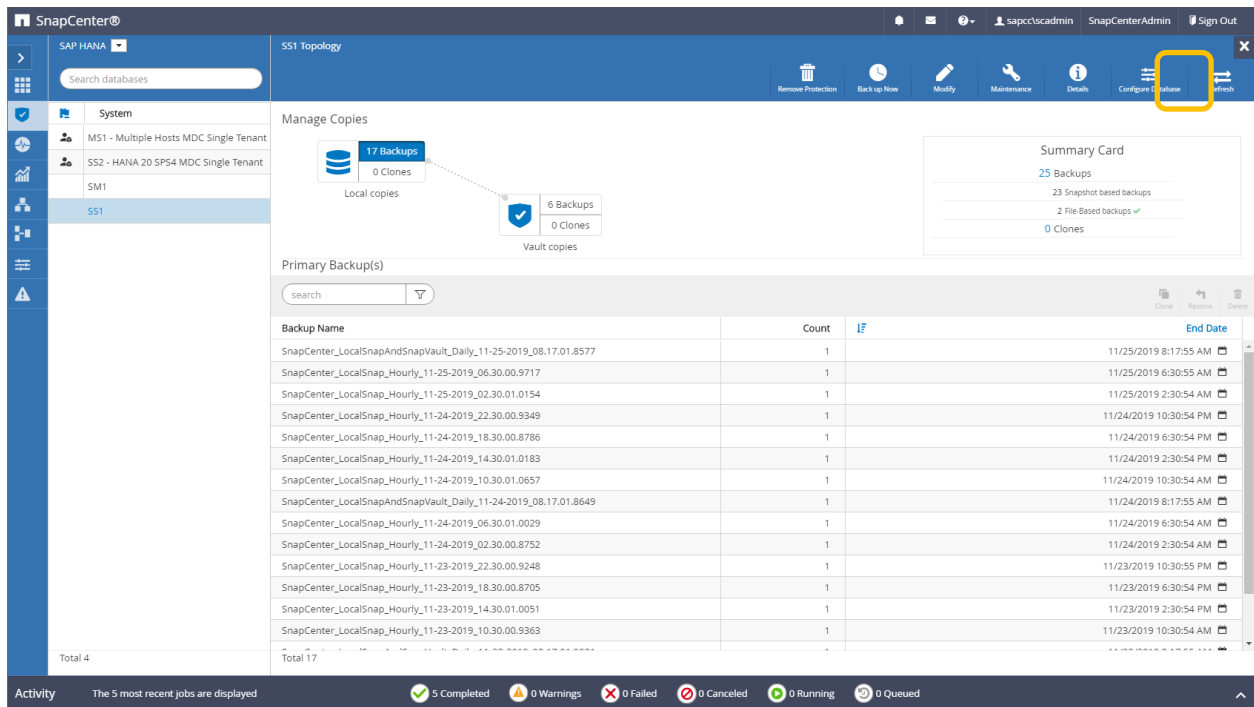
Note: This might result in additional log backups that are kept, even if the corresponding storage-based Snapshot backups on the off-site backup storage have already been deleted.

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 41. SnapCenter executes a cleanup operation with the Refresh icon to synchronize the backups for this resource.

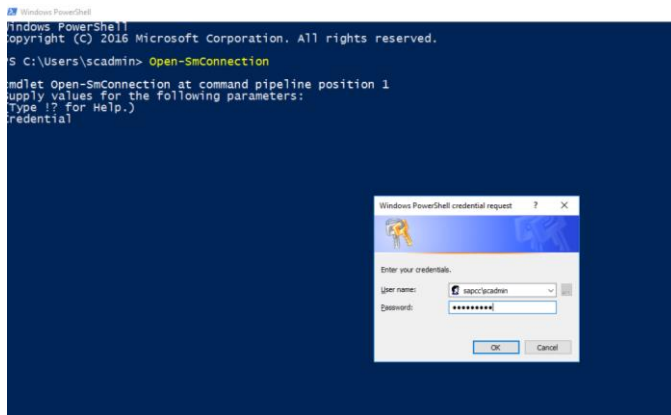
Figure 41) Refresh secondary backups.



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 and enter the SnapCenter administrator credentials in the login window.



3. To change the schedule from a weekly to a daily basis, use the cmdlet `Set-SmSchedule`.

```
PS C:\Users\scadmin> Set-SmSchedule -ScheduleInformation
@{"ScheduleType"="Daily";"StartTime"="03:45 AM";"DaysInterval"=
"1"} -TaskName SnapCenter_RemoveSecondaryBackup
```

```
TaskName : SnapCenter_RemoveSecondaryBackup
```

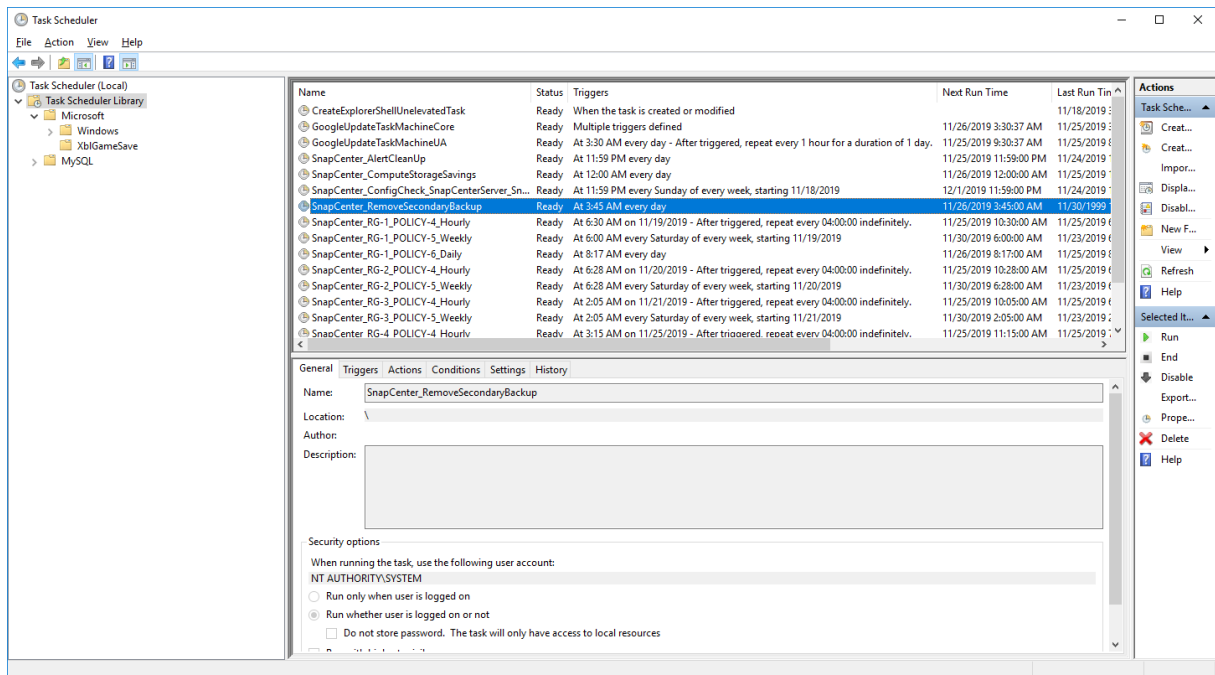
```

Hosts                : {}
StartTime            : 11/25/2019 3:45:00 AM
DaysOfMonth          : 
MonthsofTheYear      : 
DaysInterval         : 1
DaysOfTheWeek        : 
AllowDefaults        : False
ReplaceJobIfExists   : False
UserName             : 
Password             : 
SchedulerType        : Daily
RepeatTask_Every_Hour : 
IntervalDuration     : 
EndTime              : 
LocalScheduler       : False
AppType              : False
AuthMode             : 
SchedulersSQLInstance : SMCoreContracts.SmObject
MonthlyFrequency     : 
Hour                 : 0
Minute               : 0
NodeName             : 
ScheduleID           : 0
RepeatTask_Every_Mins : 
CronExpression       : 
CronOffsetInMinutes  : 
StrStartTime         : 
StrEndTime           : 

```

PS C:\Users\scadmin> Check the configuration using the Windows Task Scheduler.

4. You can check the job properties in Windows task scheduler.



Where to find additional information

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

- SnapCenter Resources Page
<https://www.netapp.com/us/documentation/snapcenter-software.aspx>
- SnapCenter Software Documentation
<https://docs.netapp.com/us-en/snapcenter/index.html>
- TR-4667: Automating SAP System Copies Using the SnapCenter
<https://www.netapp.com/us/media/tr-4667.pdf>
- TR-4719: SAP HANA System Replication, Backup and Recovery with SnapCenter
<https://www.netapp.com/us/media/tr-4719.pdf>
- TR-4018: Integrating NetApp ONTAP Systems with SAP Landscape Management
<https://www.netapp.com/pdf.html?item=/media/17195-tr4018pdf.pdf>
- TR-4646: SAP HANA Disaster Recovery with Storage Replication
<https://www.netapp.com/us/media/tr-4646.pdf>

Version history

Version	Date	Document version history
Version 1.0	July 2017	<ul style="list-style-type: none"> • Initial release.
Version 1.1	September 2017	<ul style="list-style-type: none"> • Added the “Advanced Configuration and Tuning” section. • Minor corrections.
Version 2.0	March 2018	<ul style="list-style-type: none"> • Updates to cover SnapCenter 4.0: <ul style="list-style-type: none"> – New data volume resource – Improved Single File SnapRestore operation
Version 3.0	January 2020	<ul style="list-style-type: none"> • Added the “SnapCenter Concepts and Best Practices” section. • Updates to cover SnapCenter 4.3: <ul style="list-style-type: none"> – Automatic discovery – Automated restore and recovery – Support of HANA MDC multiple tenants – Single tenant restore operation
Version 3.1	July 2020	<ul style="list-style-type: none"> • Minor updates and corrections: <ul style="list-style-type: none"> – NFSv4 support with SnapCenter 4.3.1 – Configuration of SSL communication – Central plug-in deployment for Linux on IBM Power
Version 3.2	November 2020	<ul style="list-style-type: none"> • Added the required database user privileges for HANA 2.0 SPS5.
Version 3.3	May 2021	<ul style="list-style-type: none"> • Updated the SSL hdbsql configuration section. • Added Linux LVM support.
Version 3.4	August 2021	<ul style="list-style-type: none"> • Added the disable auto discovery configuration description.
Version 3.5	February 2022	<ul style="list-style-type: none"> • Minor updates to cover SnapCenter 4.6 and auto discovery support for HANA System Replication enabled HANA systems.

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 © 2022 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

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-4614-0222