Backup, Restore and Disaster Recovery

NetApp Solutions SAP

NetApp
December 03, 2023

Table of Contents

Backup, Restore and Disaster Recovery . . . 1
- SAP HANA on Amazon FSx for NetApp ONTAP - Backup and recovery with SnapCenter . . . 1
- SAP HANA backup and recovery with SnapCenter . . . 67
- SAP HANA System Replication Backup and Recovery with SnapCenter . . . 209
- SAP HANA Disaster Recovery with Azure NetApp Files . . . 241
- TR-4646: SAP HANA Disaster Recovery with Storage Replication . . . 282
- TR-4313: SAP HANA Backup and Recovery by Using Snap Creator . . . 283
- TR-4711: SAP HANA Backup and Recovery Using NetApp Storage Systems and Commvault Software . 283
- NVA-1147-DESIGN: SAP HANA on NetApp All SAN Array - Modern SAN, Data Protection, and Disaster Recovery . . . 283

Backup, Restore and Disaster Recovery

SAP HANA on Amazon FSx for NetApp ONTAP - Backup and recovery with SnapCenter

TR-4926: SAP HANA on Amazon FSx for NetApp ONTAP - Backup and recovery with SnapCenter

Nils Bauer, NetApp

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

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

Backup and recovery using Amazon FSx for ONTAP

You can use NetApp Snapshot technology 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. Therefore, you can schedule the creation of Snapshot copies without considering peak dialog or batch activity periods. SAP and NetApp customers typically schedule multiple online Snapshot backups during the day; for example, every six hours is common. These Snapshot backups are typically kept for three to five days on the primary storage system before being removed or tiered to cheaper storage for long term retention.

Snapshot copies also provide key advantages for restore and recovery operations. NetApp SnapRestore technology enables the restoration of an entire database or, alternatively, just a portion of a database to any point in time, based on the currently available Snapshot copies. Such restore processes are finished in a few seconds, independent of the size of the database. Because several online Snapshot backups can be created during the day, the time needed for the recovery process is significantly reduced relative to a traditional once per day backup approach. Because you can perform a restore with a Snapshot copy that is at most only a few hours old (rather than up to 24 hours), fewer transaction logs must be applied during forward recovery. Therefore, the RTO is reduced to several minutes rather than the several hours required for conventional streaming 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 managed 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. You can also use the secondary location if it is necessary to

restore a backup that is no longer available on the primary location.

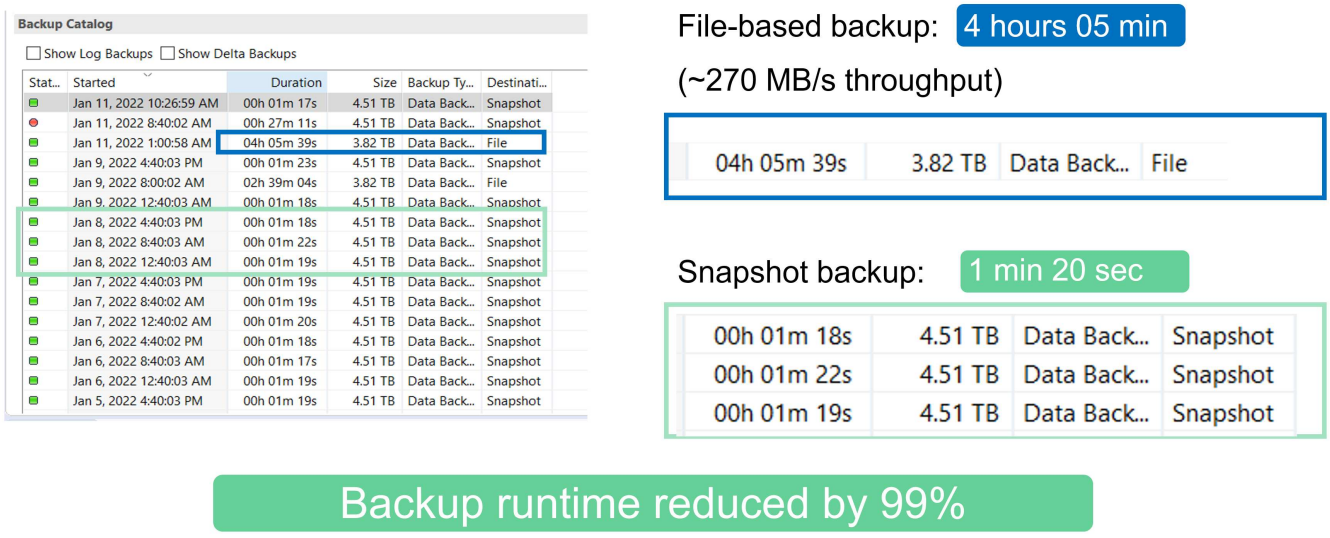
A backup to a secondary location is based on Snapshot copies created on the primary storage. Therefore, the data is read directly from the primary storage system without generating load on the SAP database server. The primary storage communicates directly with the secondary storage and replicates the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

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 move 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, any additional full database backups consume significantly less disk space.

Runtime of Snapshot backup and restore operations

The following figure shows a customer's HANA Studio using Snapshot backup operations. The image shows that the HANA database (approximately 4TB in size) is backed up in 1 minute and 20 seconds by using Snapshot backup technology and more than 4 hours with a file-based backup operation.

The largest part of the overall backup workflow runtime is the time needed to execute the HANA backup save point 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.



Recovery time objective comparison

This section provides a recovery time objective (RTO) comparison of file-based and storage-based Snapshot backups. The RTO is defined by the sum of the time needed to restore, recover, and then start 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 4.5 hours to restore a database 4TB in size on the persistence.

With storage Snapshot copy backups, the restore time is independent of the size of the database and is always in the range of a couple of seconds.

Time needed to start database

The database start time depends on the size of the database and the time needed to load the data into memory. In the following examples, it is assumed that the data can be loaded with 1000MBps. Loading 4TB into memory takes around 1hour and 10 minutes. The start time is the same for a file-based and Snapshot based restore and recovery operations.

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.

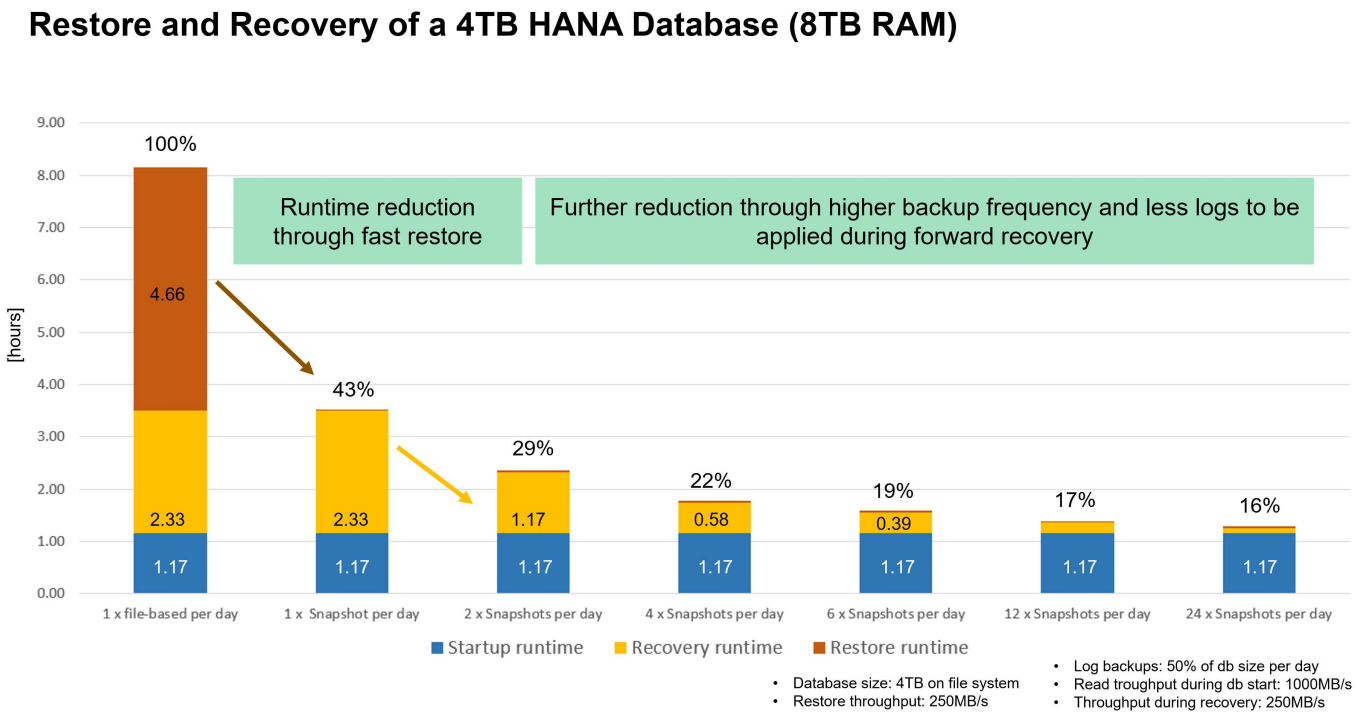
With file-based data backups, the backup schedule is typically once per day. A higher backup frequency is normally not possible, because the backup degrades production performance. Therefore, in the worst case, all the logs that were written during the day must be applied during forward recovery.

Snapshot backups are typically scheduled with a higher frequency because they do not influence the performance of the SAP HANA database. For example, if Snapshot 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 = .25).

The following figure shows a comparison of restore and recovery operations with a daily file-based backup and Snapshot backups with different schedules.

The first two bars show that even with a single Snapshot backup per day, the restore and recovery is reduced to 43% due to the speed of the restore operation from a Snapshot backup. If multiple Snapshot backups per day are created, the runtime can be reduced further because less logs need to be applied during forward recovery.

The following figure also shows that four to six Snapshot backups per day makes the most sense, because a higher frequency does not have a big influence on the overall runtime anymore.



Use cases and values of accelerated backup and cloning operations

Executing backups is a critical part of any data protection strategy. Backups are scheduled on a regular basis to ensure that you can recover from system failures. This is the most obvious use case, but there are also other SAP lifecycle management tasks, where accelerating backup and recovery operations is crucial.

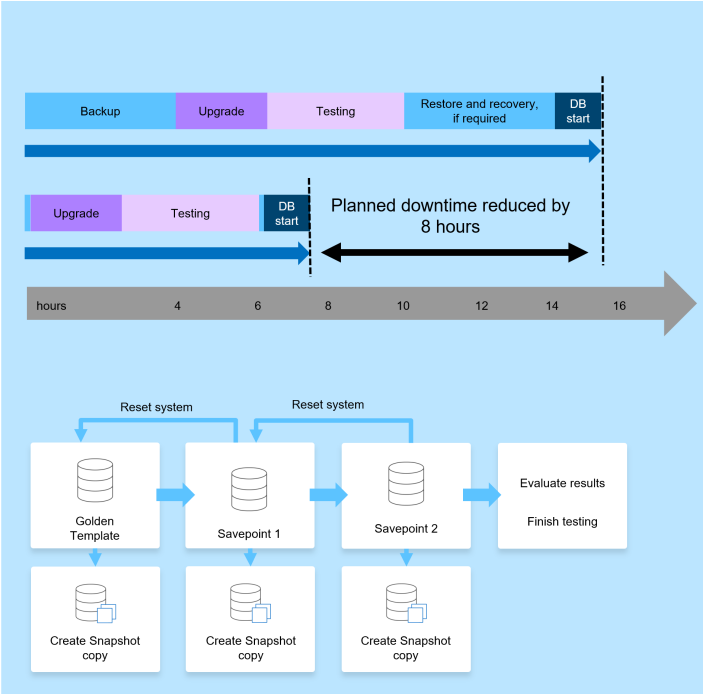
SAP HANA system upgrade is an example of where an on-demand backup before the upgrade and a possible restore operation if the upgrade fails has a significant impact on the overall planned downtime. With the example of a 4TB database, you can reduce the planned downtime by 8 hours by using the Snapshot-based backup and restore operations.

Another use case example would be a typical test cycle, where testing must be done over multiple iterations with different data sets or parameters. When leveraging the fast backup and restore operations, you can easily create save points within your test cycle and reset the system to any of these previous save points if a test fails or needs to be repeated. This enables testing to finish earlier or enables more testing at the same time and improves test results.

Use Cases for Backup and Recovery Operations

- Accelerate HANA system upgrade operations
  - Fast on-demand backup before HANA system upgrade
  - Fast restore operation in case of an upgrade failure
  - Reduction of planned downtime

- Acclerate test cycles
  - Fast creation of savepoints after a successful step
  - Fast reset of system to any savepoint
  - Repeat step until successful



When Snapshot backups have been implemented, they can be used to address multiple other use cases, which require copies of a HANA database. With FSx for ONTAP, you can create a new volume based on the content of any available Snapshot backup. The runtime of this operation is a few seconds, independent of the size of the volume.

The most popular use case is the SAP System Refresh, where data from the production system needs to be copied to the test or QA system. By leveraging the FSx for ONTAP cloning feature, you can provision the volume for the test system from any Snapshot copy of the production system in a matter of seconds. The new volume then must be attached to the test system and the HANA database recovered.

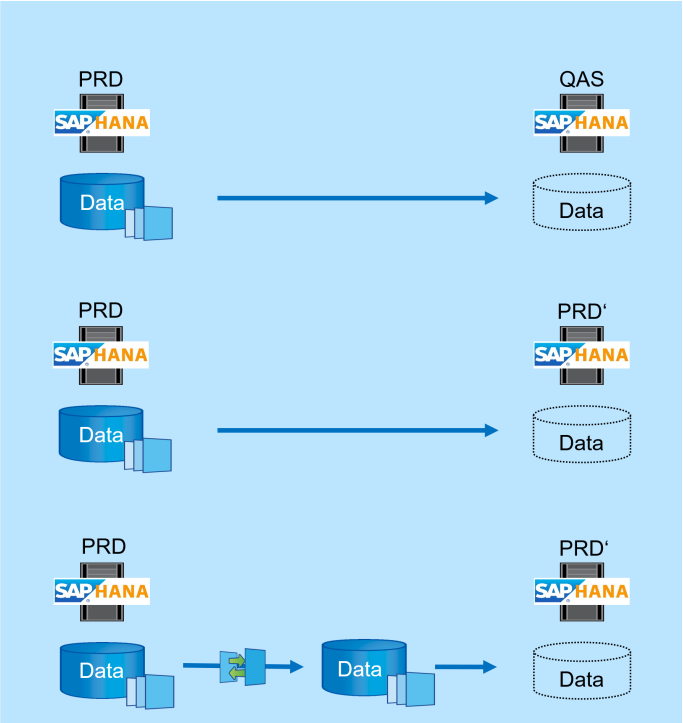
The second use case is the creation of a repair system, which is used to address a logical corruption in the production system. In this case, an older Snapshot backup of the production system is used to start a repair system, which is an identical clone of the production system with the data before the corruption occurred. The repair system is then used to analyze the problem and export the required data before it was corrupted.

The last use case is the ability to run a disaster recover failover test without stopping the replication and therefore without influencing RTO and recovery point objective (RPO) of the disaster recovery setup. When

FSx for ONTAP NetApp SnapMirror replication is used to replicate the data to the disaster recovery site, the production Snapshot backups are available at the disaster recovery site as well and can then be used to create a new volume for disaster recover testing.

Use Cases for Cloning Operations

- SAP System Refresh
  - Fast creation of a new volume based on a production Snapshot backup
  - Attach volume to the test system and recover HANA database with SID change
- Repair System creation to address logical corruption
  - Fast creation of a new volume based on a production Snapshot backup
  - Attach volume to the repair system and recover HANA database w/o SID change
- Disaster Recovery testing
  - Combined with SnapMirror Replication
  - Attach storage clone from a replicated production Snapshot backup to a DR test system



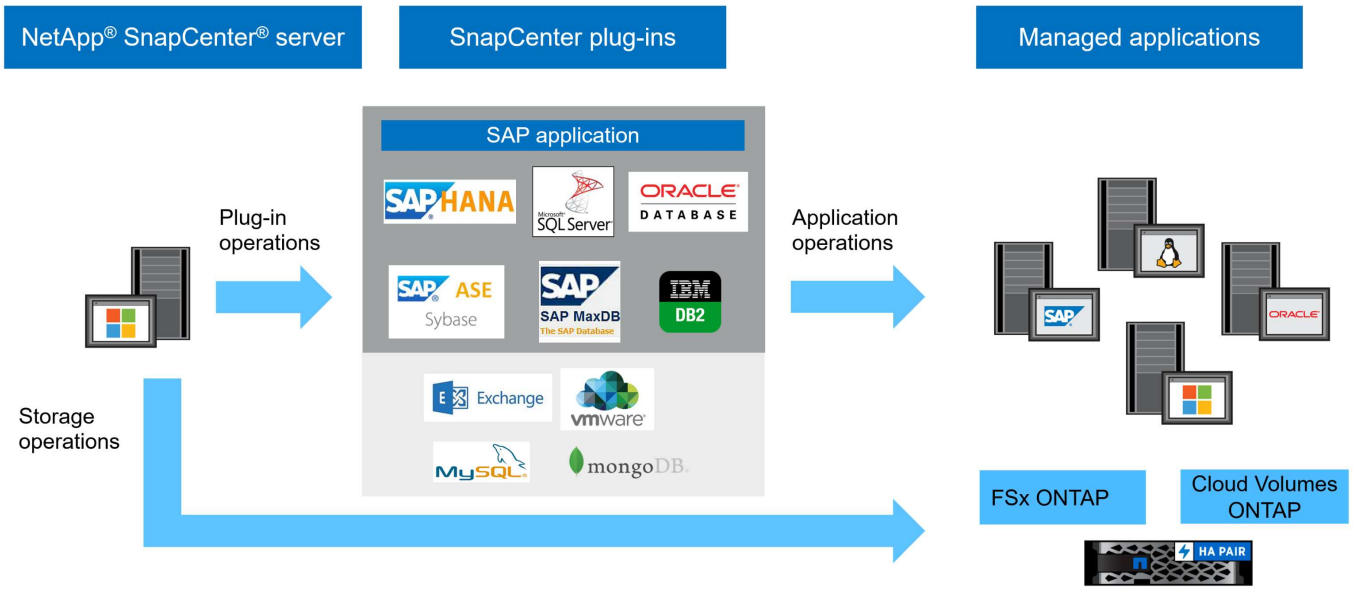
SnapCenter architecture

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-In Package for Linux. Each package contains plug-ins to SnapCenter for various applications and infrastructure components.



SnapCenter SAP HANA backup solution

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

- Backup operations, scheduling, and retention management
  - SAP HANA data backup with storage-based Snapshot copies
  - Non-data volume backup with storage-based Snapshot copies (for example, `/hana/shared`)
  - Database block integrity checks using a file-based backup
  - Replication to an off-site backup or disaster recovery location
- Housekeeping of the SAP HANA backup catalog
  - For HANA data backups (Snapshot and file-based)
  - For HANA log backups
- Restore and recovery operations
  - Automated restore and recovery
  - Single tenant restore operations for SAP HANA (MDC) systems

Database data file backups are executed by SnapCenter in combination with the plug-in for SAP HANA. The plug-in triggers the 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 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.

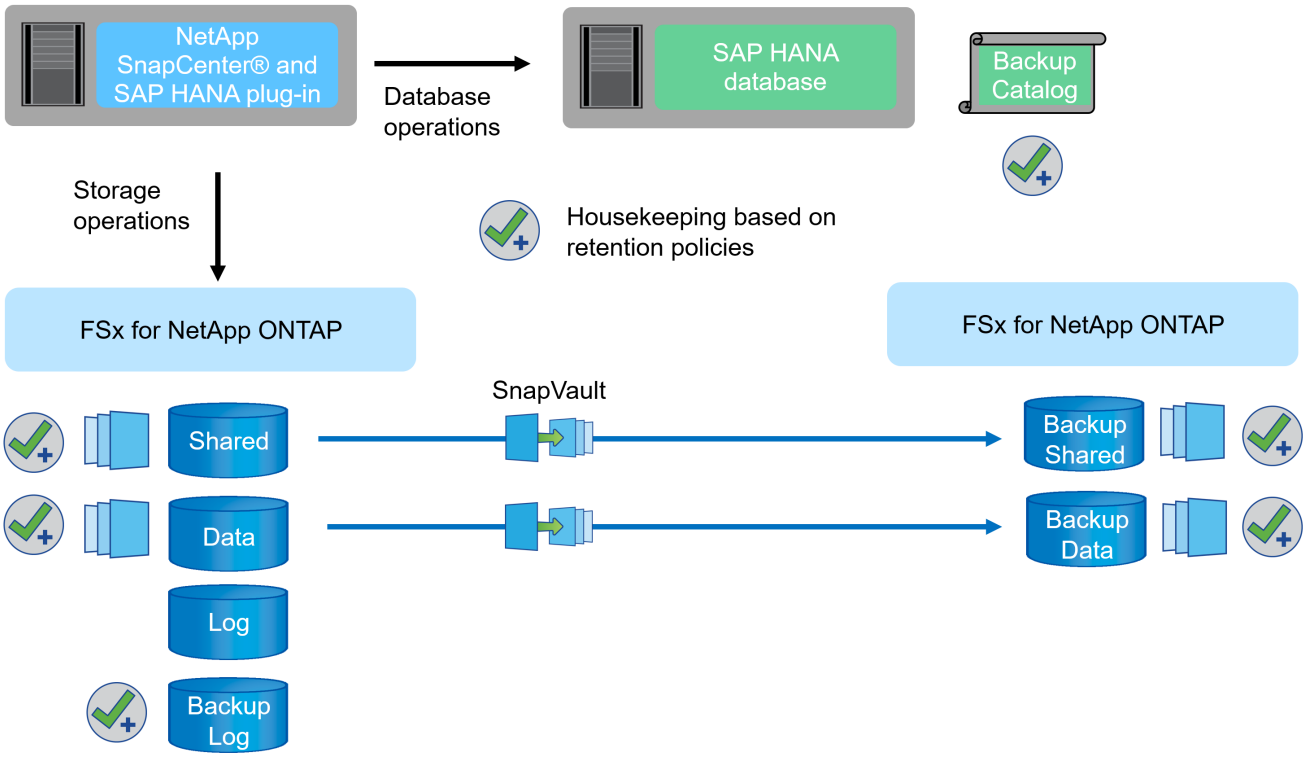
To allow a complete backup of all SAP HANA-related resources, SnapCenter also enables you to back up all non-data volumes by using the SAP HANA plug-in with storage-based Snapshot copies. You can schedule non-data volumes independently from the database data backup to enable individual retention and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

SAP recommends combining storage-based Snapshot backups with a weekly file-based backup to execute a

block integrity check. You can execute the block integrity check from within SnapCenter. Based on your configured retention policies, SnapCenter manages the housekeeping of data file backups at the primary storage, log file backups, and the SAP HANA backup catalog.

SnapCenter handles the retention at primary storage, while FSx for ONTAP manages secondary backup retention.

The following figure shows an overview of the SnapCenter backup and retention management operations.



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

1. Creates an SAP HANA backup save point to create a consistent image on the persistence layer.
2. Creates a storage-based Snapshot copy of the data volume.
3. Registers the storage- based Snapshot back up in the SAP HANA backup catalog.
4. Releases the SAP HANA backup save point.
5. Executes a SnapVault or SnapMirror update for the data volume, if configured.
6. Deletes storage Snapshot copies at the primary storage based on the defined retention policies.
7. Deletes 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 also 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.

Scope of this document

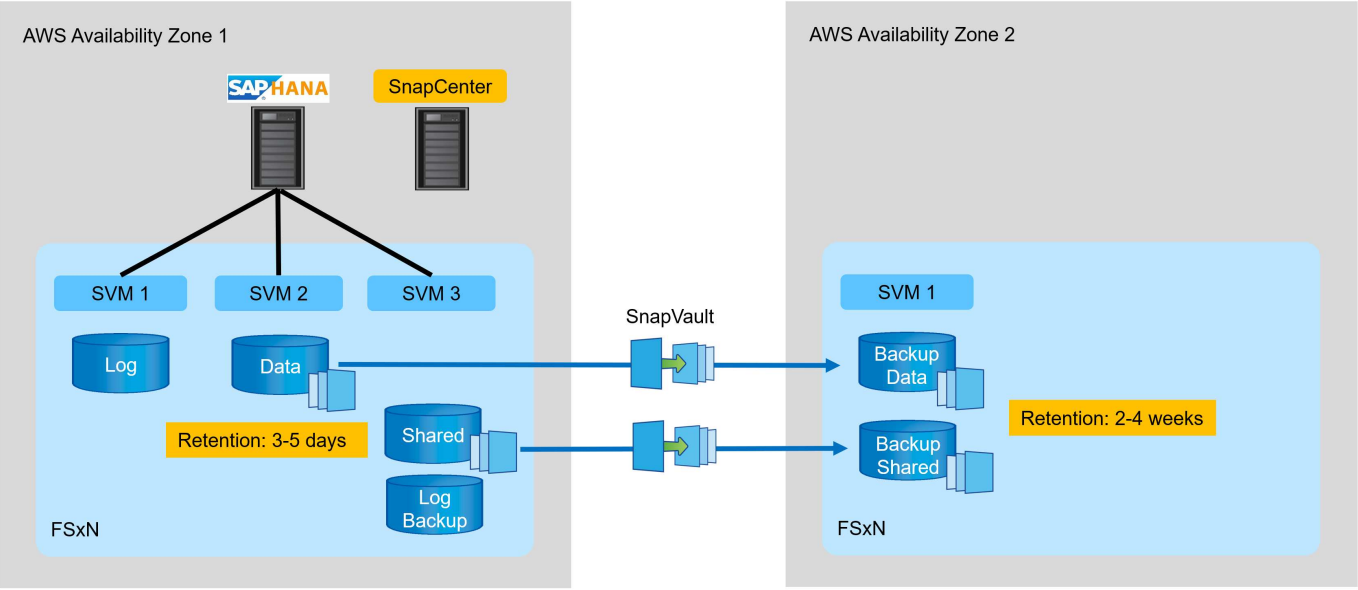
This document describes the most common SnapCenter configuration option for an SAP HANA MDC single host system with a single tenant on FSx for ONTAP. Other configuration options are possible and, in some

cases, required for specific SAP HANA systems, for example, for a multiple host system. For a detailed description about other configuration options, see SnapCenter concepts and best practices (netapp.com).

In this document, we use the Amazon Web Services (AWS) console and the FSx for ONTAP CLI to execute the required configuration steps on the storage layer. You can also use NetApp Cloud Manager to manage FSx for ONTAP, but this is out of scope for this document. For information about using NetApp Cloud Manager for FSx for ONTAP, see Learn about Amazon FSx for ONTAP (netapp.com).

Data protection strategy

The following figure shows a typical backup architecture for SAP HANA on FSx for ONTAP. The HANA system is located in the AWS availability zone 1 and is using an FSx for ONTAP file system within the same availability zone. Snapshot backup operations are executed for the data and the shared volume of the HANA database. In addition to the local Snapshot backups, which are kept for 3-5 days, backups are also replicated to an offsite storage for longer term retention. The offsite backup storage is a second FSx for ONTAP file system located in a different AWS availability zone. Backups of the HANA data and shared volume are replicated with SnapVault to the second FSx for ONTAP file system and are kept for 2-3 weeks.



Before configuring SnapCenter, 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 following parameters must be defined:

- 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?

The following table shows an example of data protection parameters for the system types: production, development, and test. For the production system, a high backup frequency has been defined, and the backups are replicated to an off-site backup site once per day. The test systems have lower requirements and

no replication of the backups.

Parameters	Production systems	Development systems	Test systems
Backup frequency	Every 6 hours	Every 6 hours	Every 6 hours
Primary retention	3 days	3 days	3 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

The following table shows the policies that must be configured for the 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 by 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, you must configure a protection relationship on the storage layer. The protection relationship defines which volumes are replicated and the retention of backups at the off-site backup storage.

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

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

Example lab setup

The following lab setup was used as an example configuration for the rest of this document.

HANA system PFX:

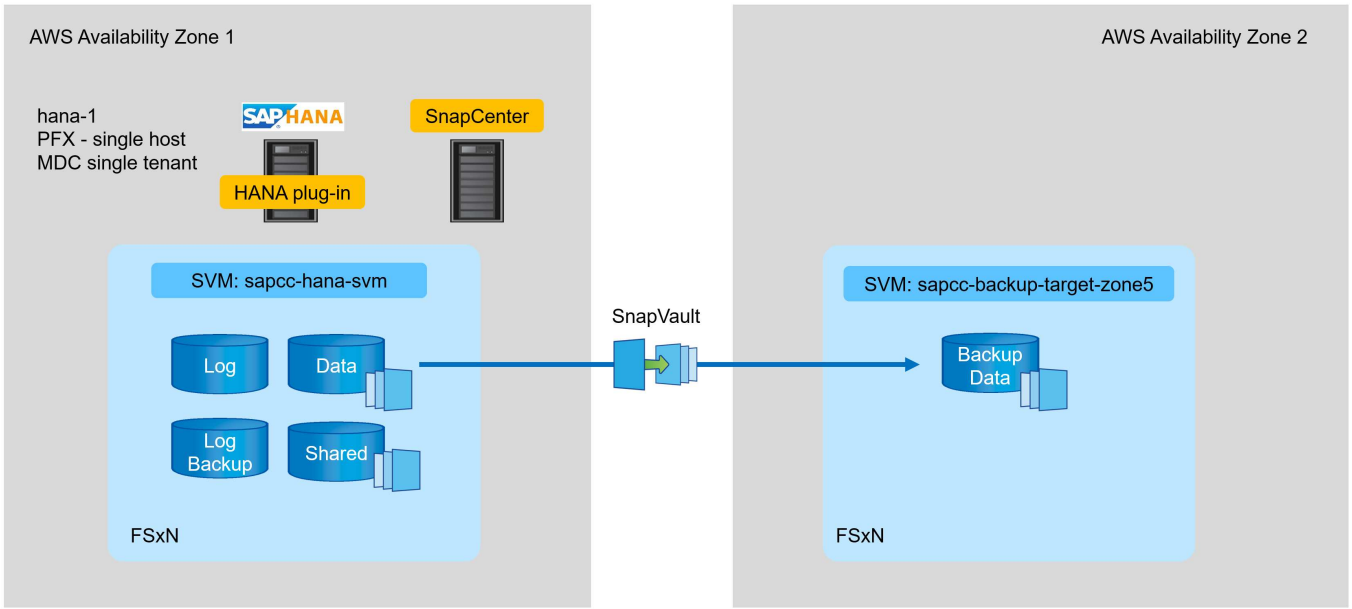
- Single host MDC system with a single tenant
- HANA 2.0 SPS 6 revision 60
- SLES for SAP 15SP3

SnapCenter:

- Version 4.6
- HANA and Linux plug-in deployed on a HANA database host

FSx for ONTAP file systems:

- Two FSx for ONTAP file systems with a single storage virtual machine (SVM)
- Each FSx for ONTAP system in a different AWS availability zone
- HANA data volume replicated to the second FSx for ONTAP file system



SnapCenter configuration

You must perform the steps in this section for base SnapCenter configuration and the protection of the HANA resource.

Overview configuration steps

You must perform the following steps for base SnapCenter configuration and the protection of the HANA resource. Each step is described in detail in the following chapters.

1. Configure SAP HANA backup user and hdbuserstore key. Used to access the HANA database with the hdbsql client.
2. Configure storage in SnapCenter. Credentials to access the FSx for ONTAP SVMs from SnapCenter
3. Configure credentials for plug-in deployment. Used to automatically deploy and install the required SnapCenter plug-ins on the HANA database host.
4. Add HANA host to SnapCenter. Deploys and installs the required SnapCenter plug-ins.
5. Configure policies. Defines the backup operation type (Snapshot, file), retentions, as well asoptional Snapshot backup replication.
6. Configure HANA resource protection. Provide hdbuserstore key and attach policies and schedules to the HANA resource.

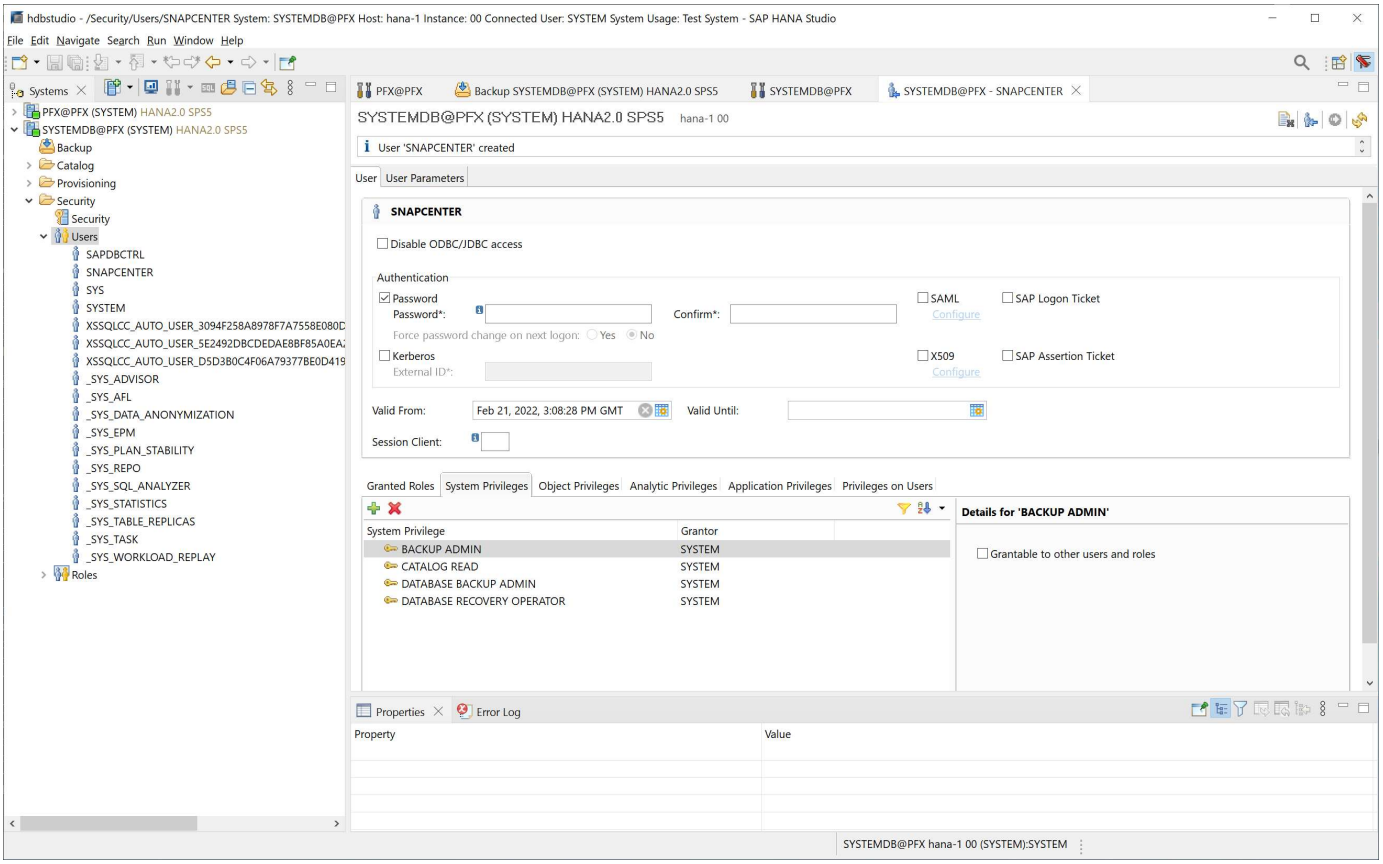
SAP HANA backup user and hdbuserstore configuration

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.

The following figure shows the SAP HANA Studio through which you can create the backup user

The required privileges are 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.

For an SAP HANA MDC system, you must create the user in the system database because all backup commands for the system and the tenant databases are executed by using the system database.



The following command is used for the user store configuration with the `<sid>adm` user:

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

SnapCenter uses the `<sid>adm` user to communicate with the HANA database. Therefore, you must configure the user store key by using the <`sid>adm` user on the database host. Typically, the SAP HANA hdbsql client software is installed together with the database server installation. If this is not the case, you must install the hdbclient first.

In an SAP HANA MDC 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 multiple-host setup, you must configure user store keys for all hosts. SnapCenter tries to connect to the database by using each of the provided keys and can therefore operate independently of a failover of an SAP HANA service to a different host. In our lab setup, we configured a user store key for the user `pfxadm` for our system PFX, which is a single host HANA MDC system with a single tenant.

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbuserstore set PFXKEY hana-1:30013
SNAPCENTER <password>
Operation succeed.
```

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbuserstore list
DATA FILE       : /usr/sap/PFX/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE        : /usr/sap/PFX/home/.hdb/hana-1/SSFS_HDB.KEY
ACTIVE RECORDS  : 7
DELETED RECORDS : 0
KEY PFXKEY
  ENV : hana-1:30013
  USER: SNAPCENTER
KEY PFXSAPDBCTRL
  ENV : hana-1:30013
  USER: SAPDBCTRL
Operation succeed.
```

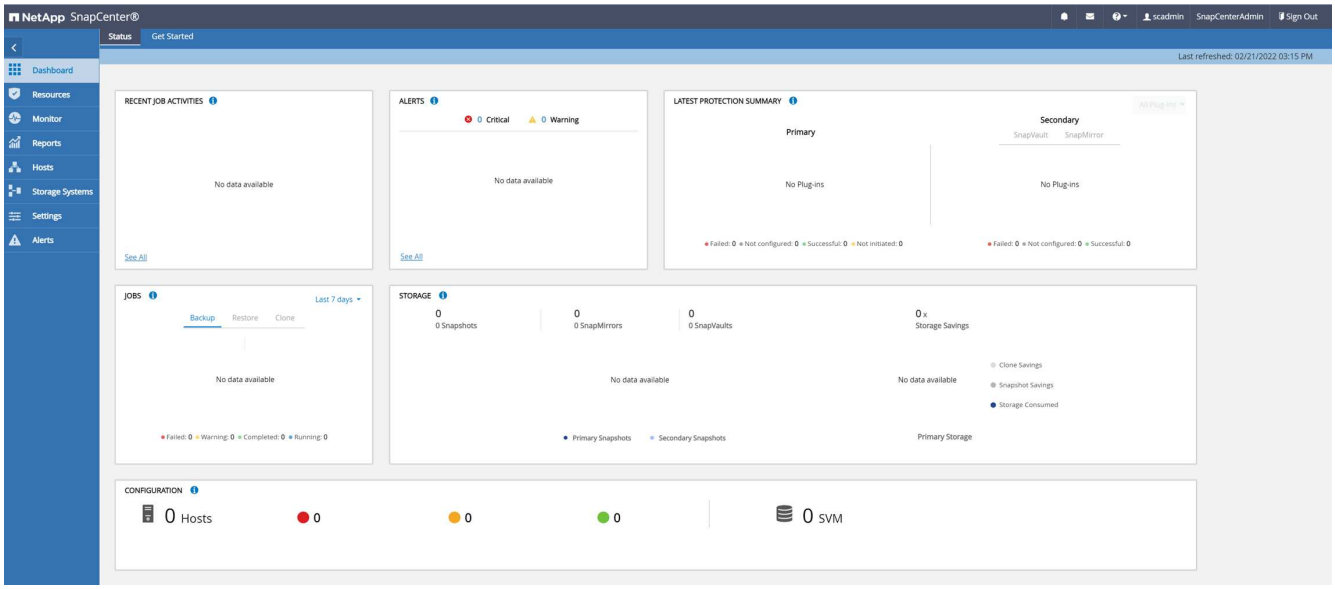
You can check the access to the HANA system database that uses the key with the `hdbsql` command.

```
pfxadm@hana-1:/usr/sap/PFX/home> hdbsql -U PFXKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=>
```

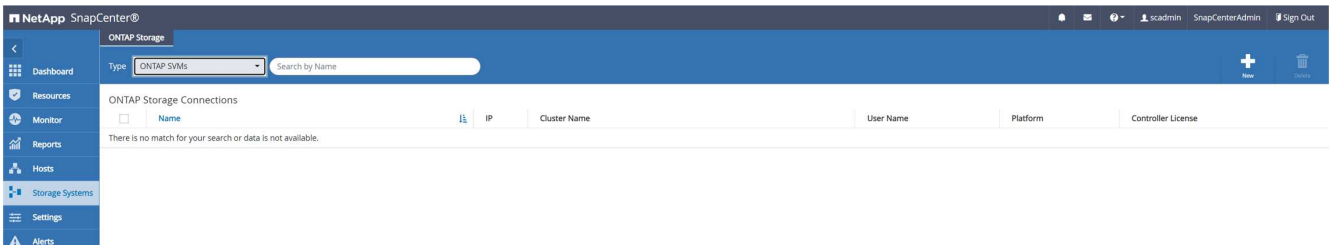
Configure storage

Follow these steps to configure storage in SnapCenter.

1. In the SnapCenter UI, select Storage Systems.

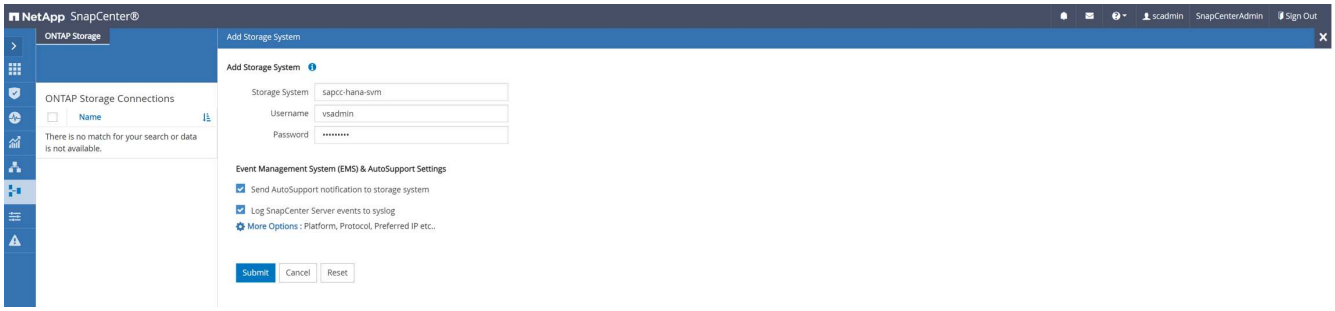


You can select the storage system type, which can be ONTAP SVMs or ONTAP Clusters. In the following example, SVM management is selected.

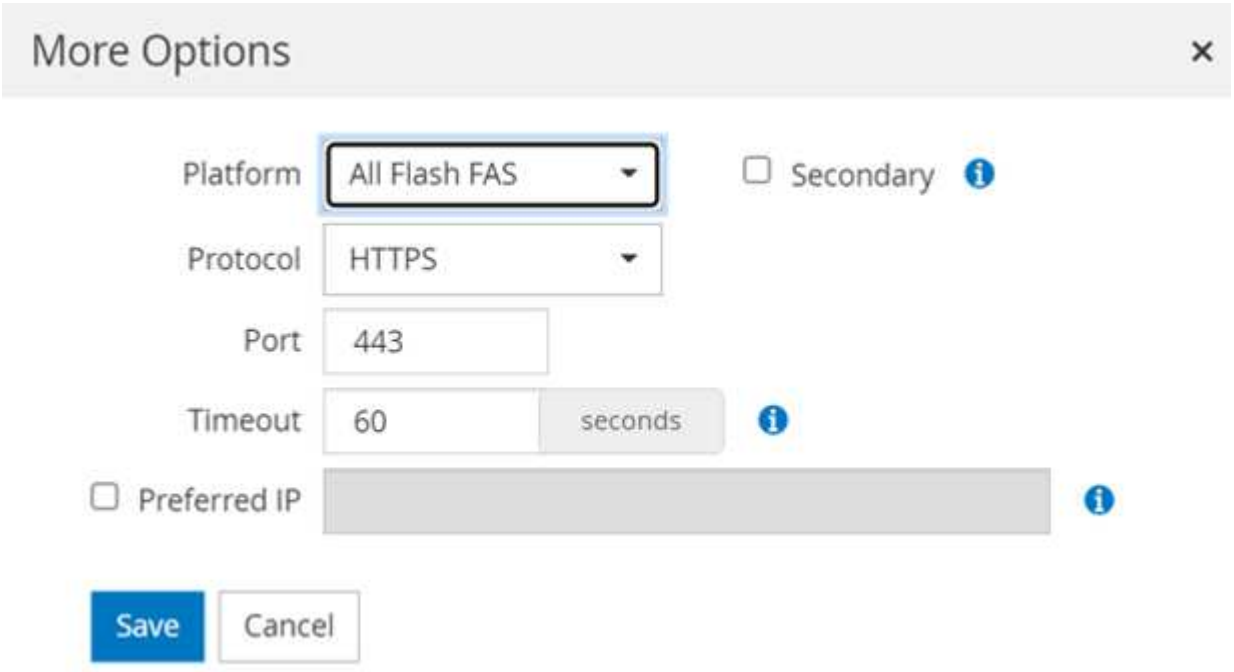


2. To add a storage system and provide the required host name and credentials, click New.

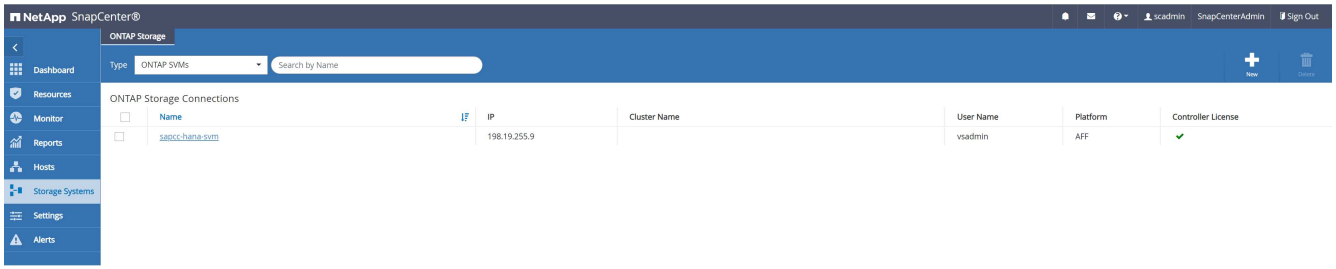
   The SVM user is not required to be the vsadmin user, as shown in the following figure. Typically, a user is configured on the SVM and assigned the required permissions to execute backup and restore operations. For information about required privileges, see SnapCenter Installation Guide in the section titled “Minimum ONTAP privileges required”.



3. To configure the storage platform, click More Options.
4. Select All Flash FAS as the storage system to ensure that the license, which is part of FSx for ONTAP, is available for SnapCenter.



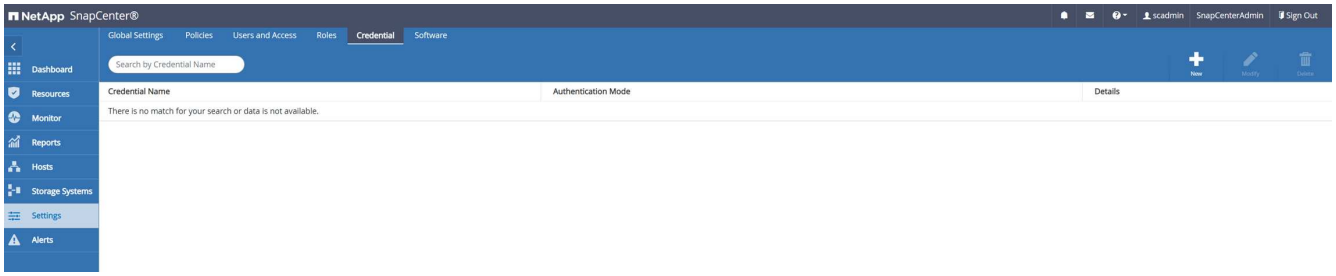
The SVM `sapcc-hana-svm` is now configured in SnapCenter.



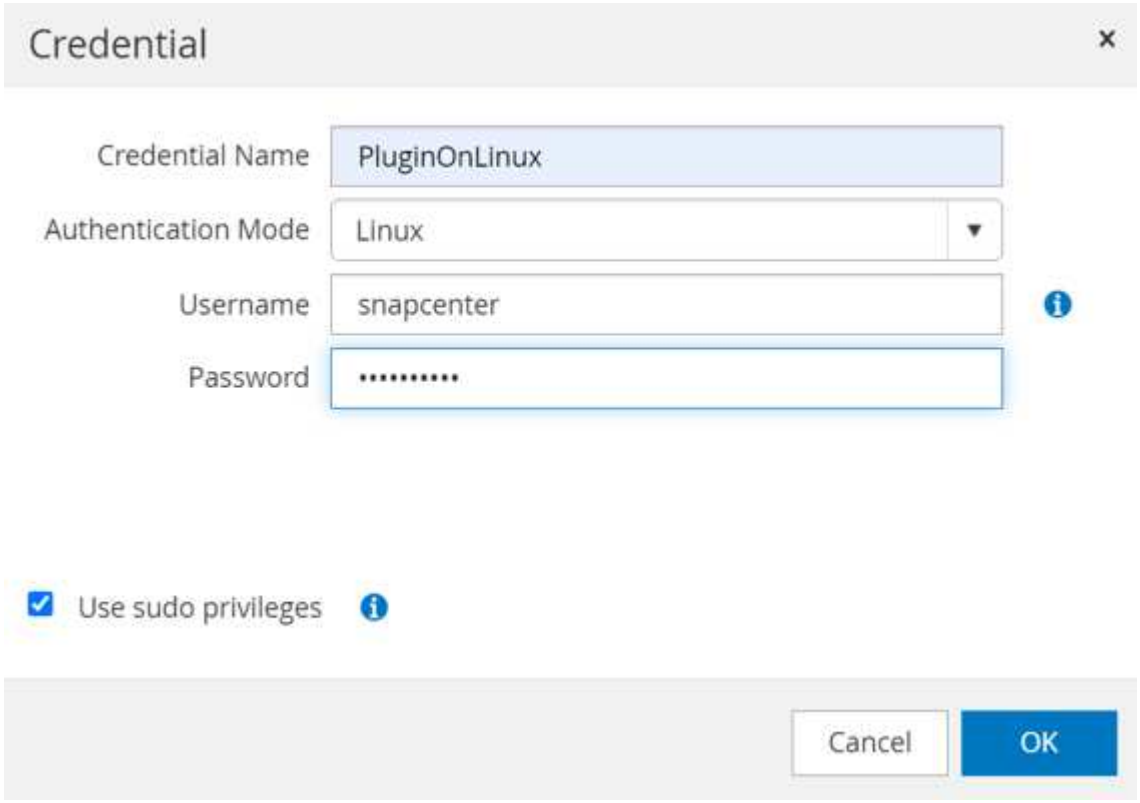
Create credentials for plugin deployment

To enable SnapCenter to deploy the required plug-ins on the HANA hosts, you must configure user credentials.

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



2. In the lab setup, we configured a new user, `snapcenter`, on the HANA host that is used for the plug- in deployment. You must enable sudo prvileges, as shown in the following figure.



```
hana-1:/etc/sudoers.d # cat /etc/sudoers.d/90-cloud-init-users
# Created by cloud-init v. 20.2-8.48.1 on Mon, 14 Feb 2022 10:36:40 +0000
# User rules for ec2-user
ec2-user ALL=(ALL) NOPASSWD:ALL
# User rules for snapcenter user
snapcenter ALL=(ALL) NOPASSWD:ALL
hana-1:/etc/sudoers.d #
```

Add a SAP HANA host

When adding an SAP HANA host, SnapCenter deploys the required plug-ins on the database host and executes auto discovery operations.

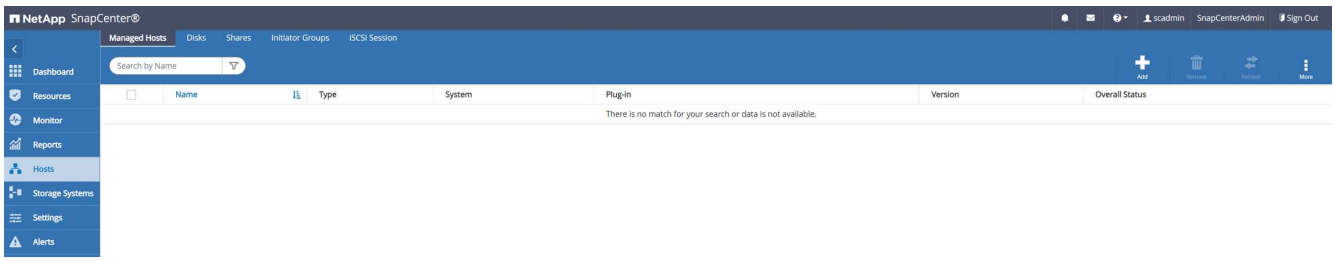
The SAP HANA plug-in requires Java 64-bit version 1.8. Java must be installed on the host before the host is added to SnapCenter.

```
hana-1:/etc/ssh # java -version
openjdk version "1.8.0_312"
OpenJDK Runtime Environment (IcedTea 3.21.0) (build 1.8.0_312-b07 suse-
3.61.3-x86_64)
OpenJDK 64-Bit Server VM (build 25.312-b07, mixed mode)
hana-1:/etc/ssh #
```

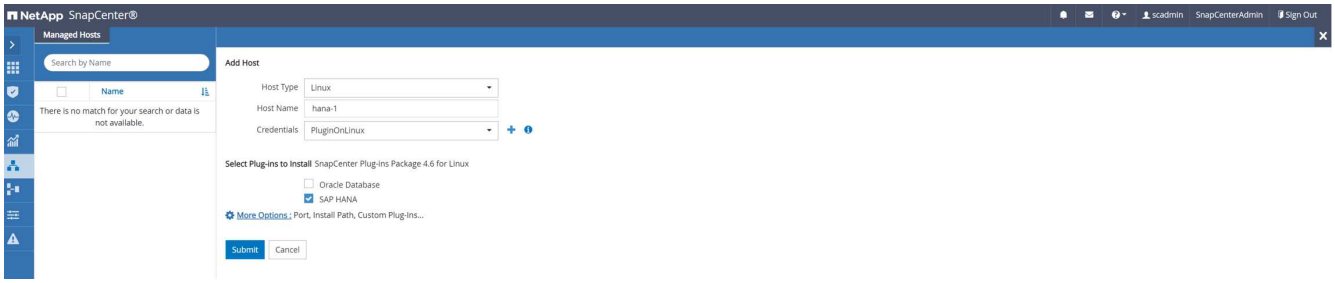
OpenJDK or Oracle Java is supported with SnapCenter.

To add the SAP HANA host, follow these steps:

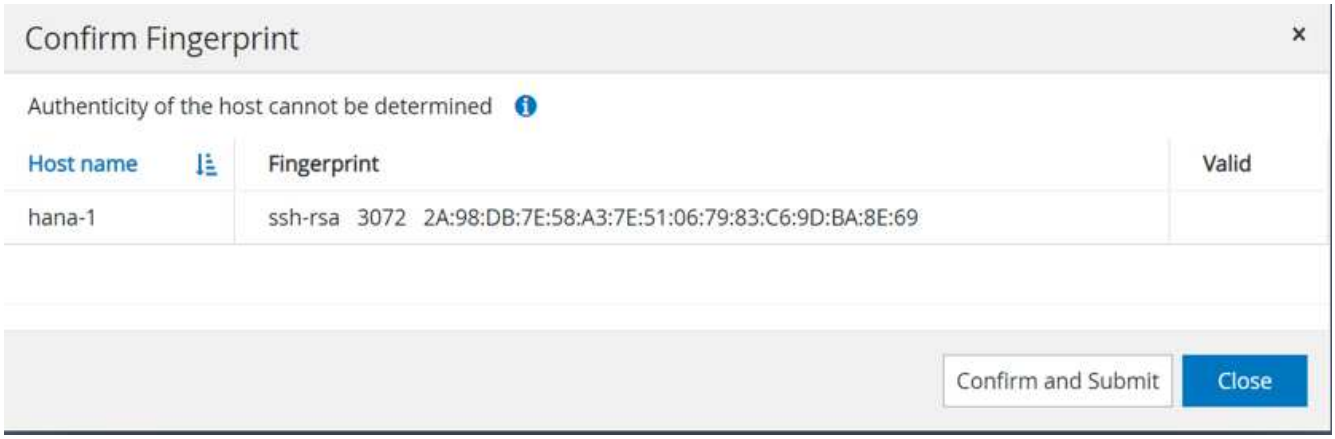
1. From the host tab, click Add.



2. Provide host information and select the SAP HANA plug-in to be installed. Click Submit.

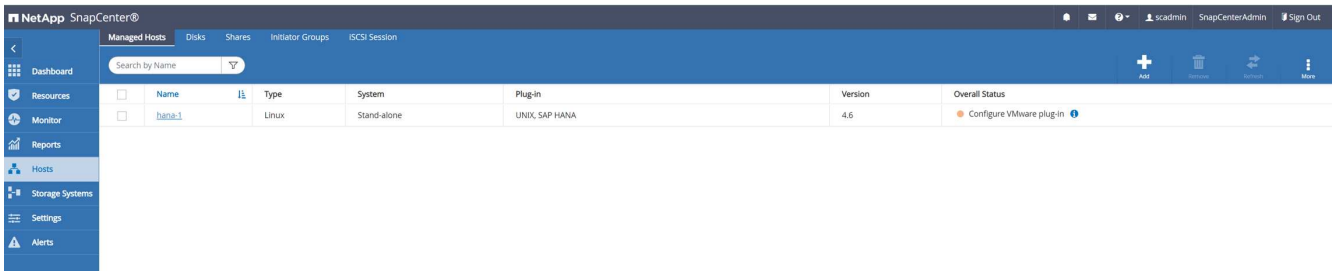


3. Confirm the fingerprint.



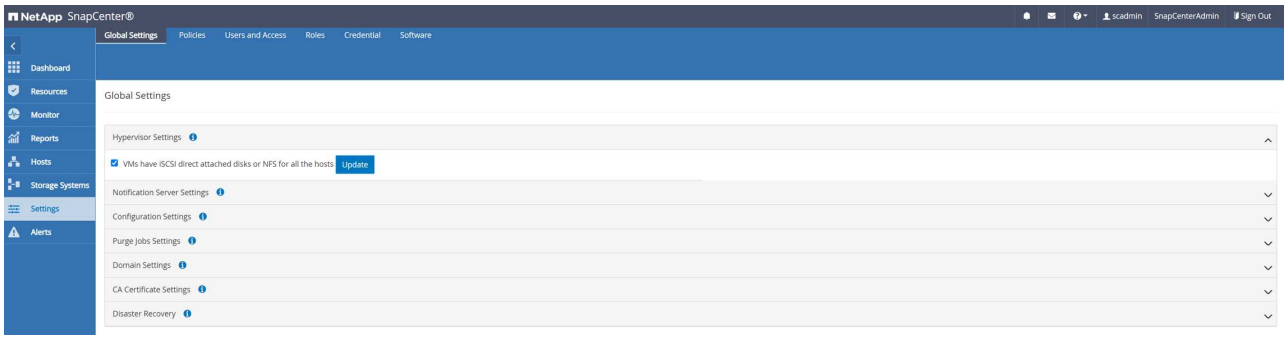
The installation of the HANA and the Linux plug-in starts automatically. When the installation is finished, the status column of the host shows Configure VMware Plug-in. SnapCenter detects if the SAP HANA plug-in is installed on a virtualized environment. This might be a VMware environment or an environment at a public cloud provider. In this case, SnapCenter displays a warning to configure the hypervisor.

You can remove the warning message by using the following steps.

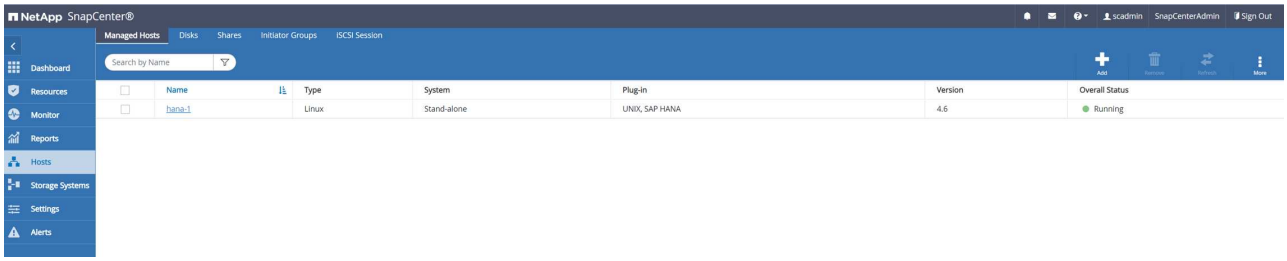


a. From the Settings tab, select Global Settings.

b. For the hypervisor settings, select VMs Have iSCSI Direct Attached Disks or NFS For All the Hosts and update the settings.



The screen now shows the Linux plug-in and the HANA plug-in with the status Running.



Configure policies

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:

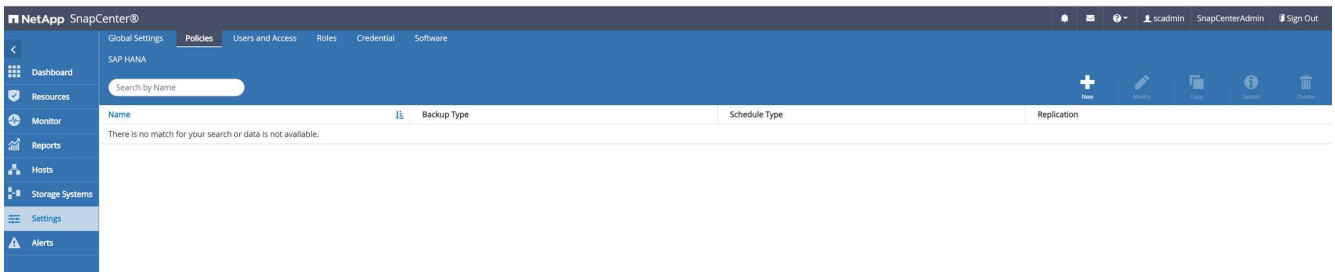
- Policy for hourly backups without replication: `LocalSnap`.
- Policy for weekly block integrity check using a file-based backup: `BlockIntegrityCheck`.

The following sections describe the configuration of these policies.

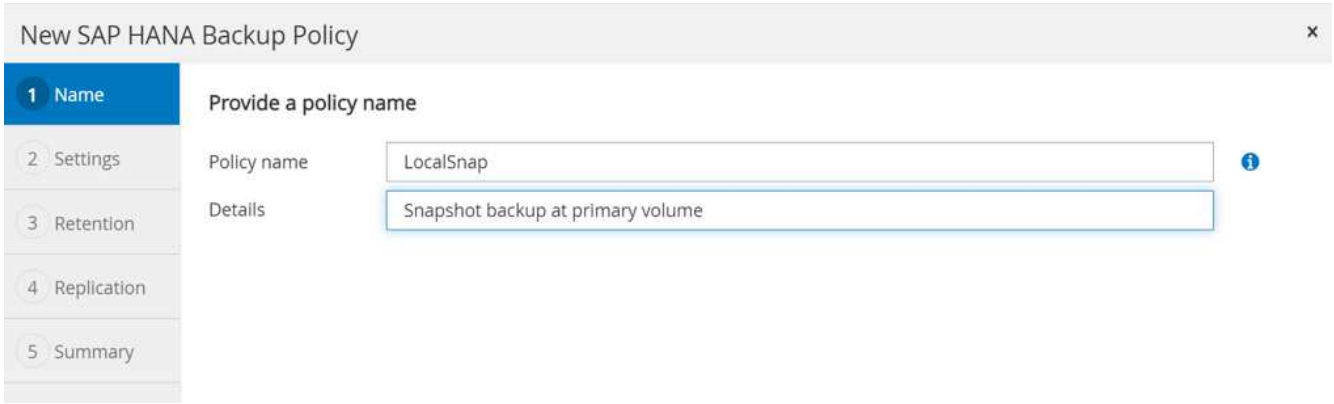
Policy for Snapshot backups

Follow these steps to configure Snapshot backup policies.

1. Go to Settings > Policies and click New.

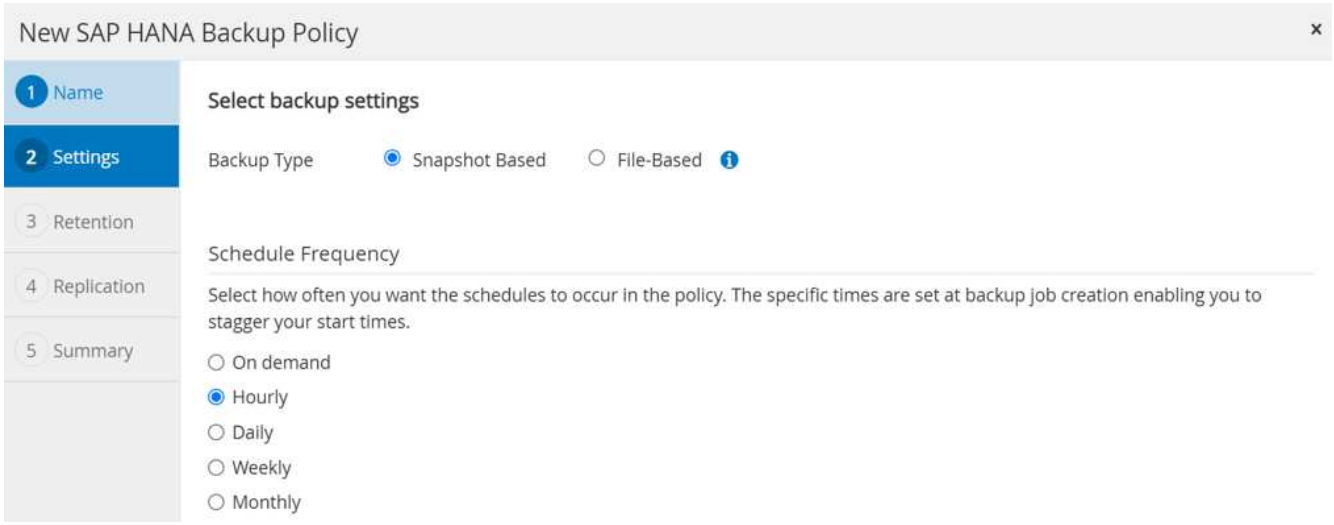


2. Enter the policy name and description. Click Next.

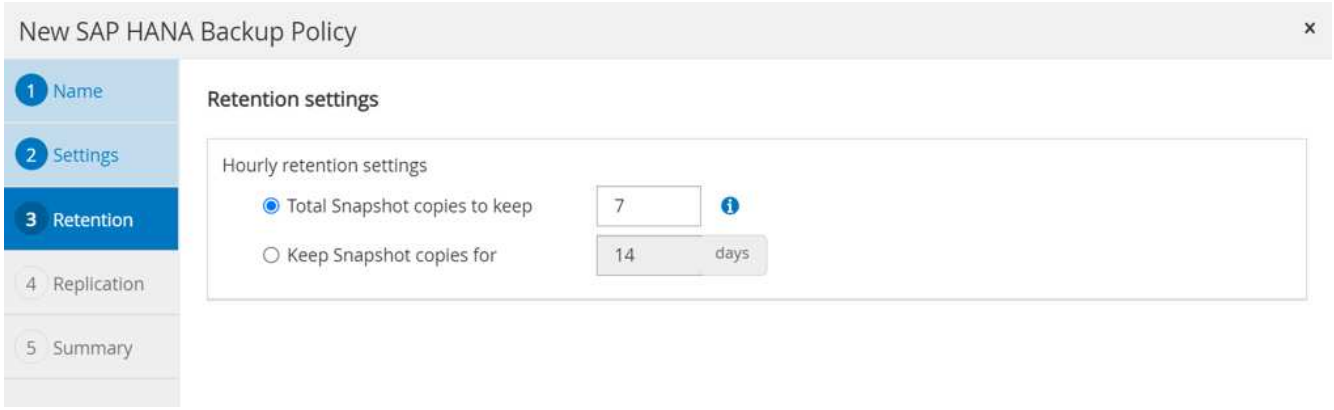


3. Select backup type as Snapshot Based and select Hourly for schedule frequency.

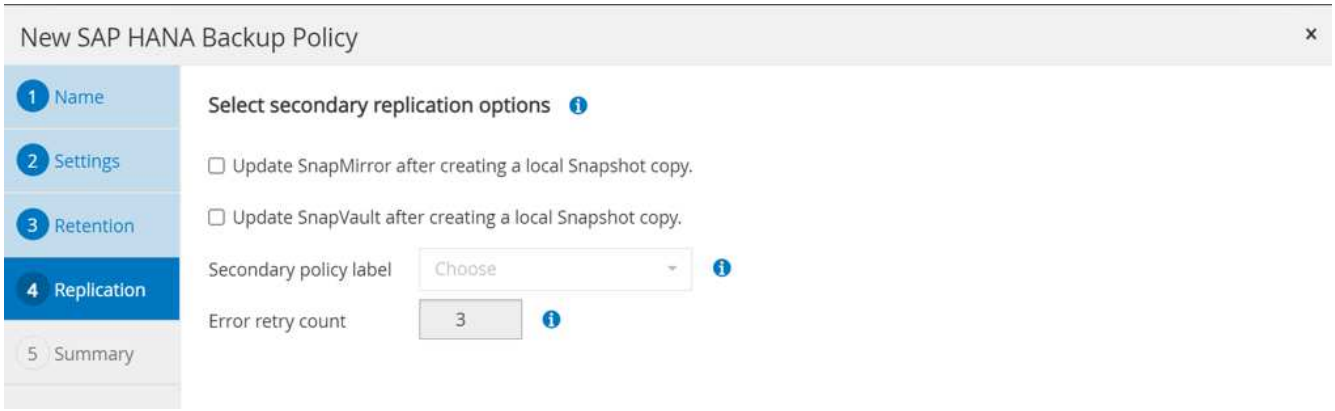
   The schedule itself is configured later with the HANA resource protection configuration.

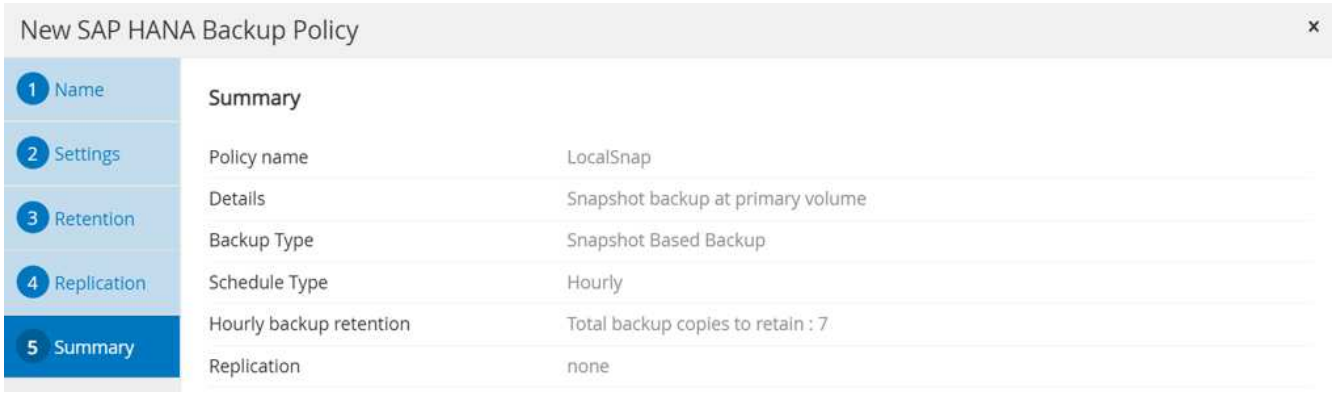


4. Configure the retention settings for on-demand backups.

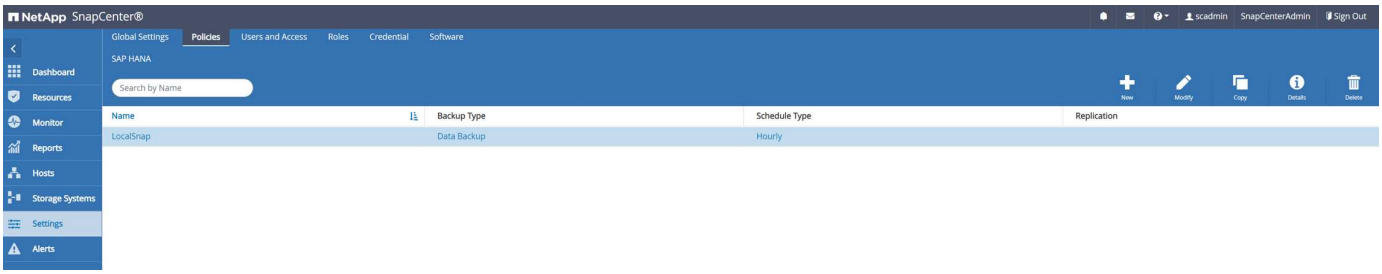


5. Configure the replication options. In this case, no SnapVault or SnapMirror update is selected.





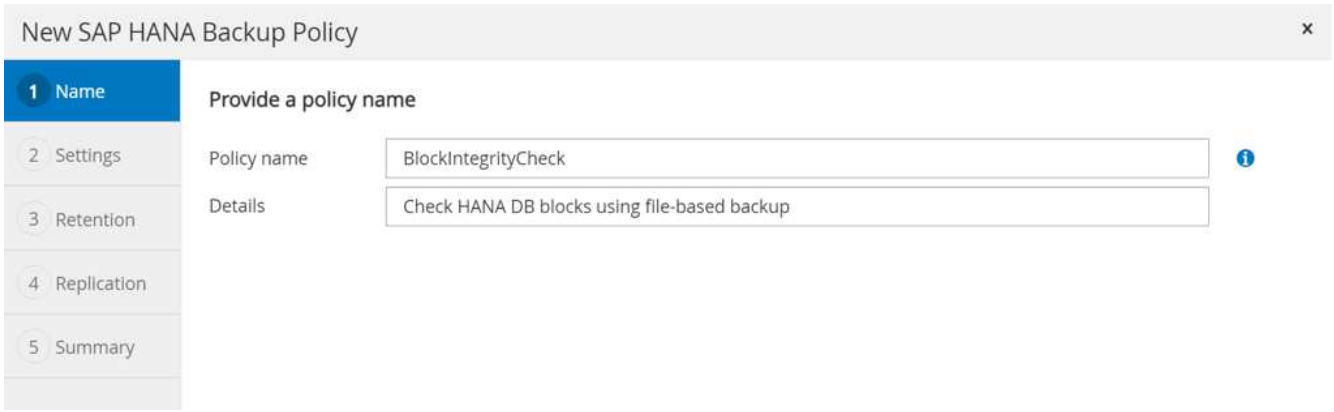
The new policy is now configured.



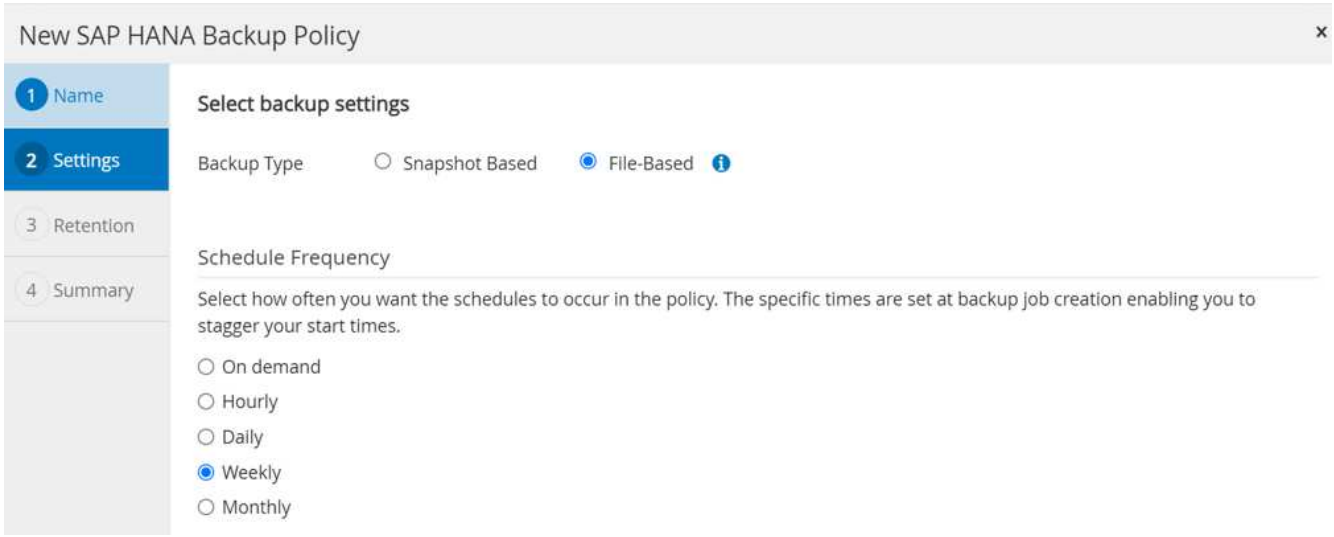
Policy for block integrity check

Follow these steps to configure the block integrity check policy.

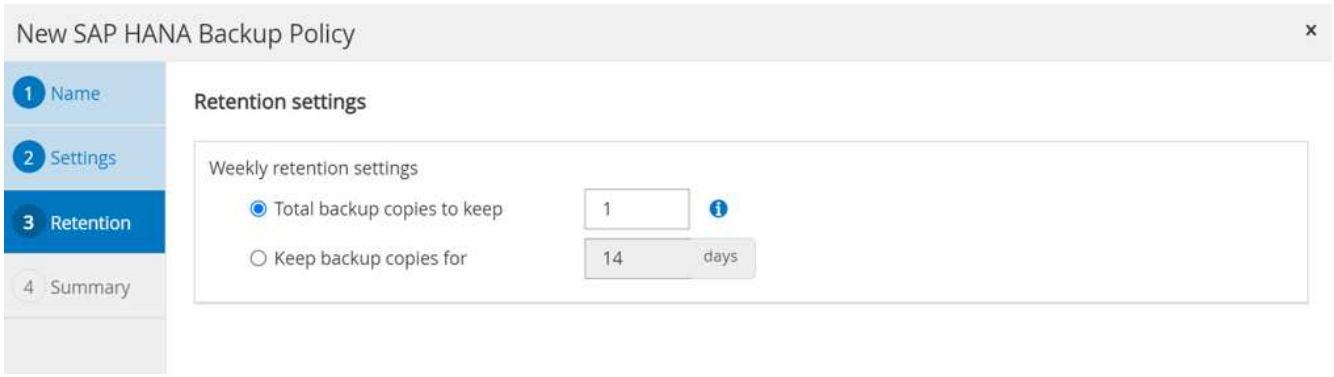
1. Go to Settings > Policies and click New.
2. Enter the policy name and description. Click Next.



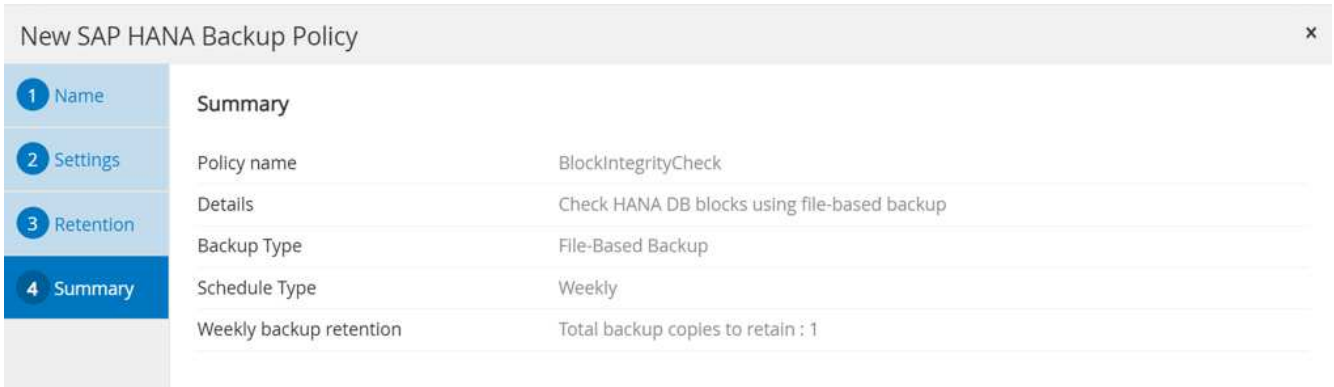
3. Set the backup type to File-Based and schedule frequency to Weekly. The schedule itself is configured later with the HANA resource protection configuration.

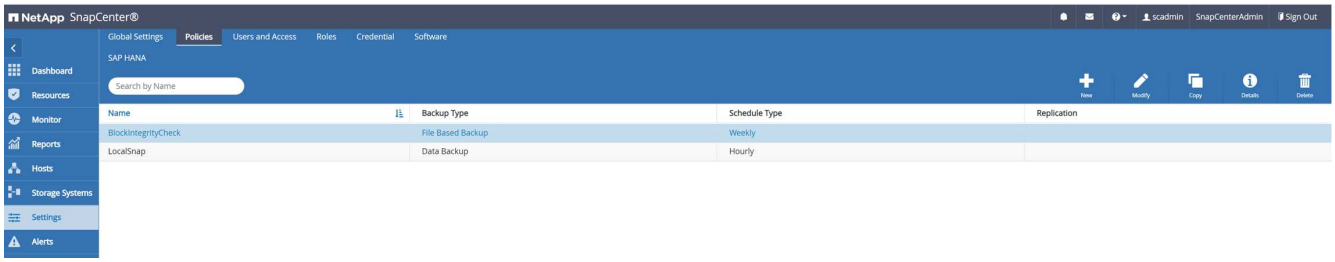


4. Configure the retention settings for on-demand backups.



5. On the Summary page, click Finish.



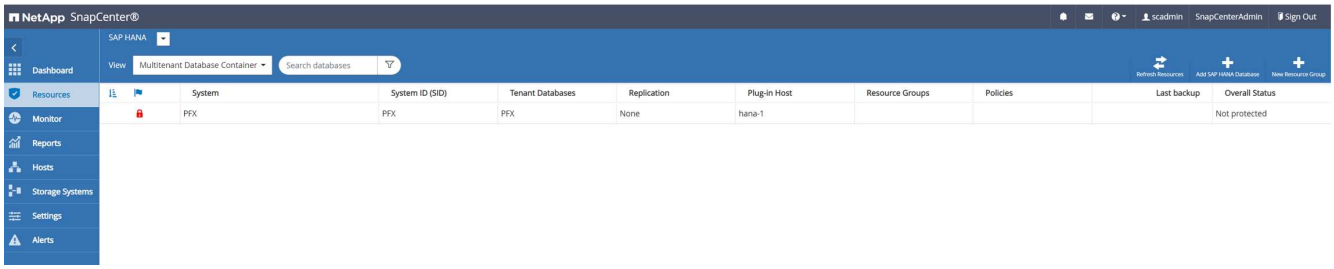


Configure and protect a HANA resource

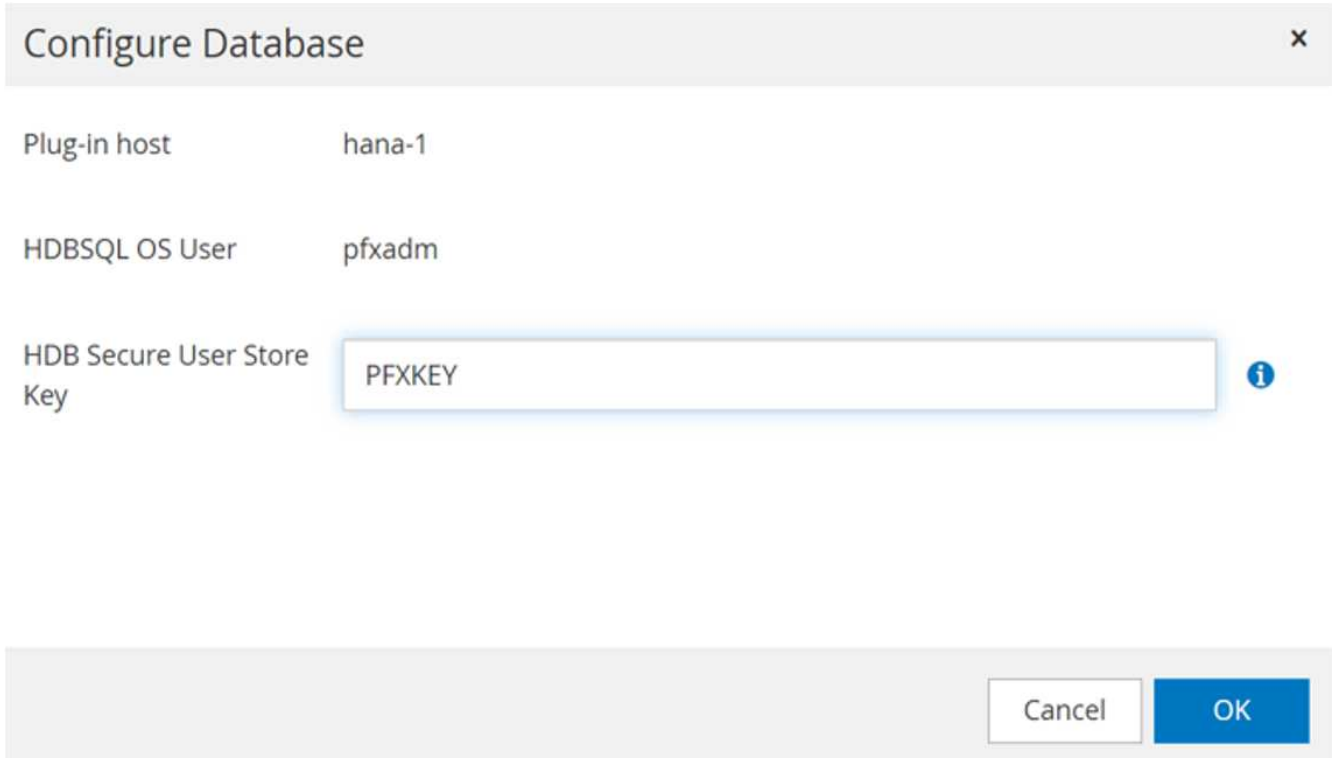
After the plug-in installation, the automatic discovery process of the HANA resource starts automatically. In the Resources screen, a new resource is created, which is marked as locked with the red padlock icon. To configure and protect the new HANA resource, follow these steps:

1. Select and click the resource to continue the configuration.

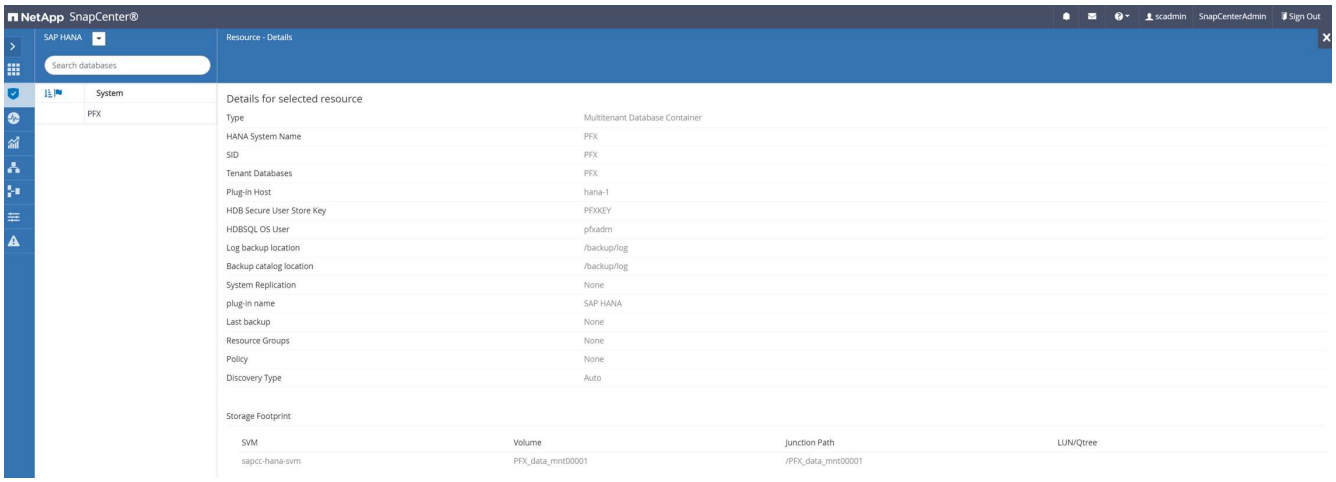
   You can also trigger the automatic discovery process manually within the Resources screen by clicking Refresh Resources.



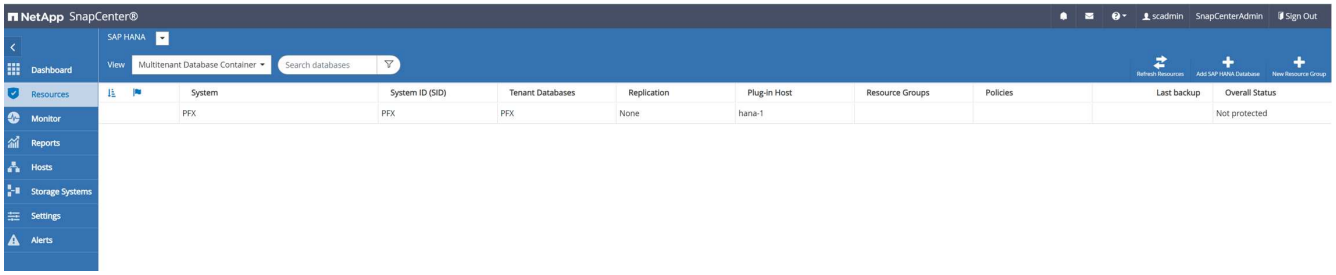
2. Provide the userstore key for the HANA database.



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

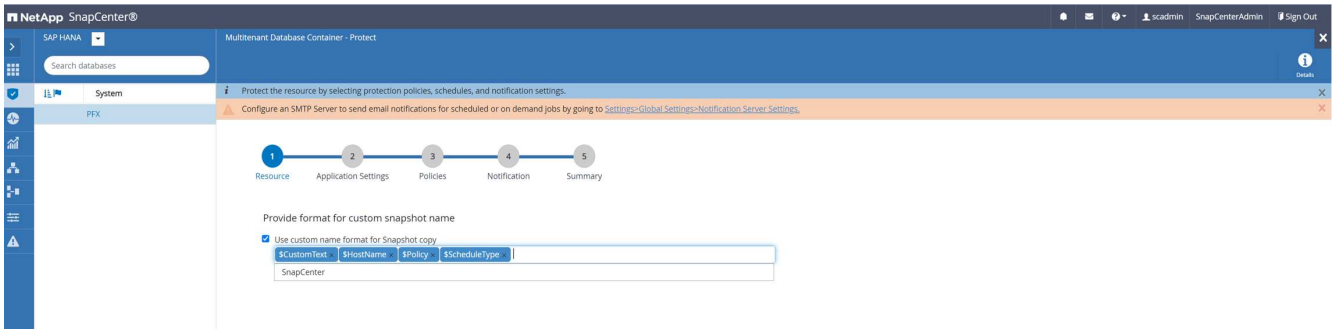


3. From the Resources tab, double click the resource to configure the resource protection.

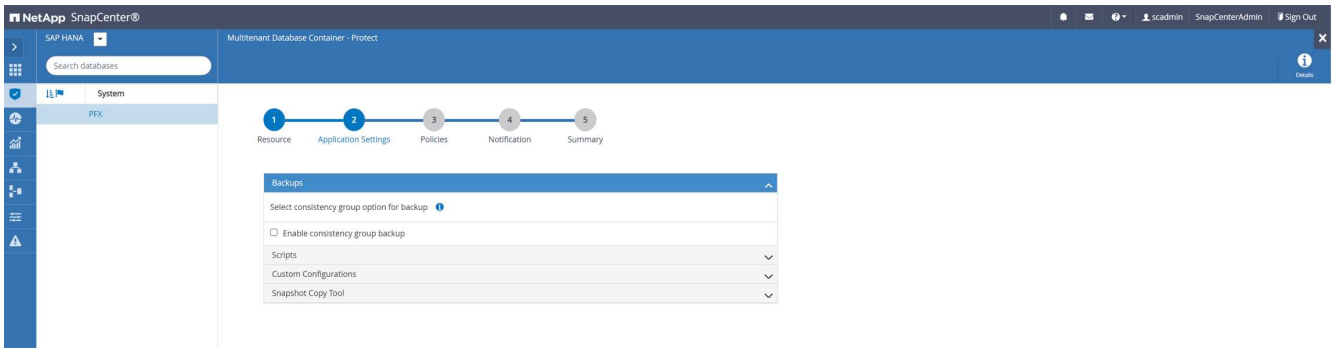


4. Configure a custom name format for the Snapshot copy.

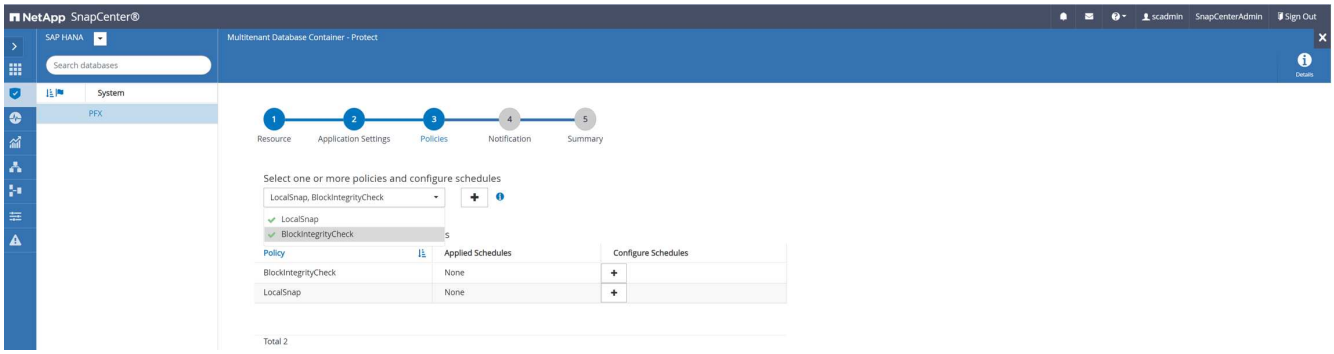
   NetApp recommends using a custom Snapshot copy name to easily identify which backups have been created with which policy and schedule type. By adding the schedule type in the Snapshot copy name, you can distinguish between scheduled and on-demand backups. The `schedule name` string for on-demand backups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



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

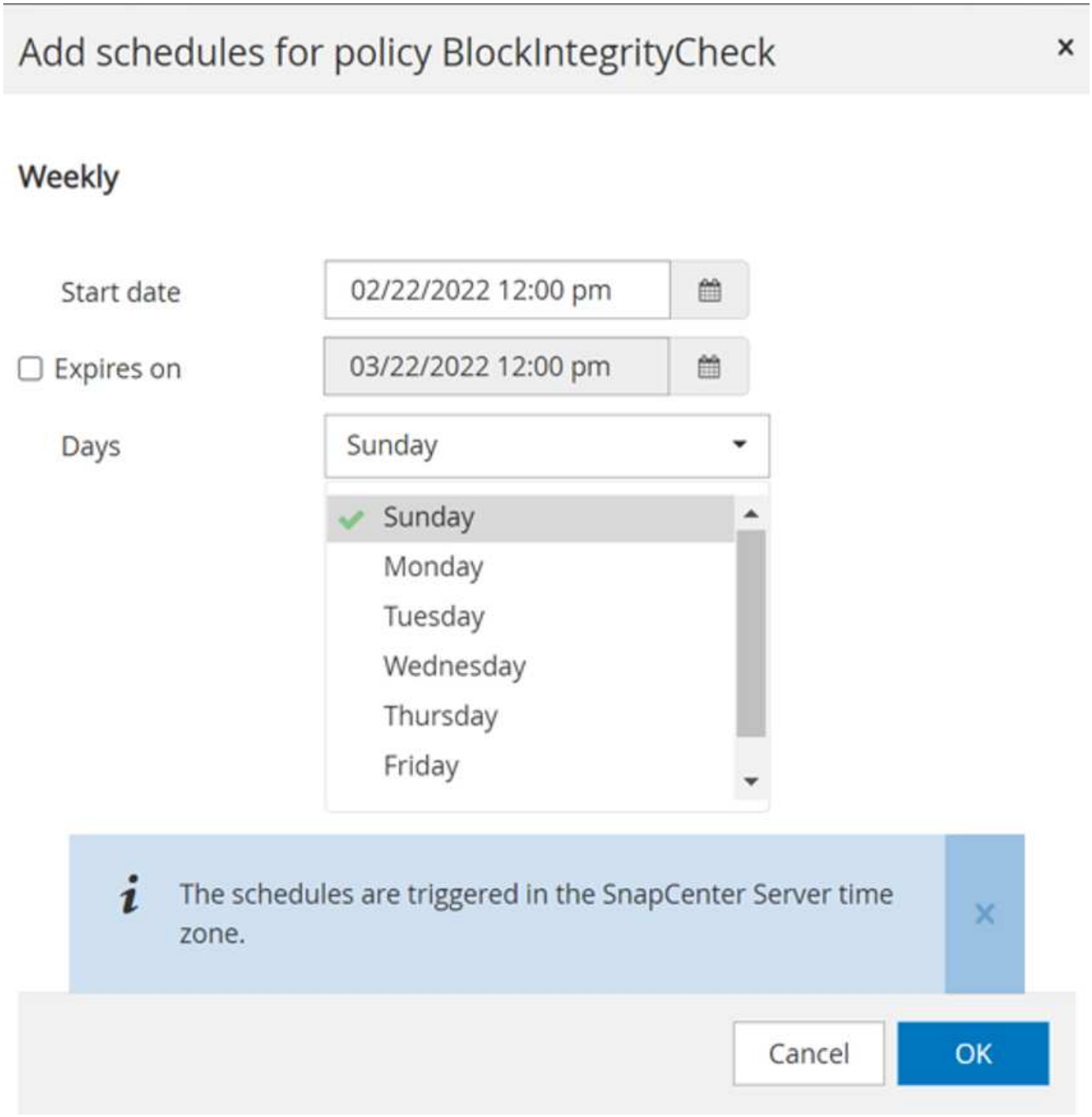


6. Select the policies to be added to the resource.



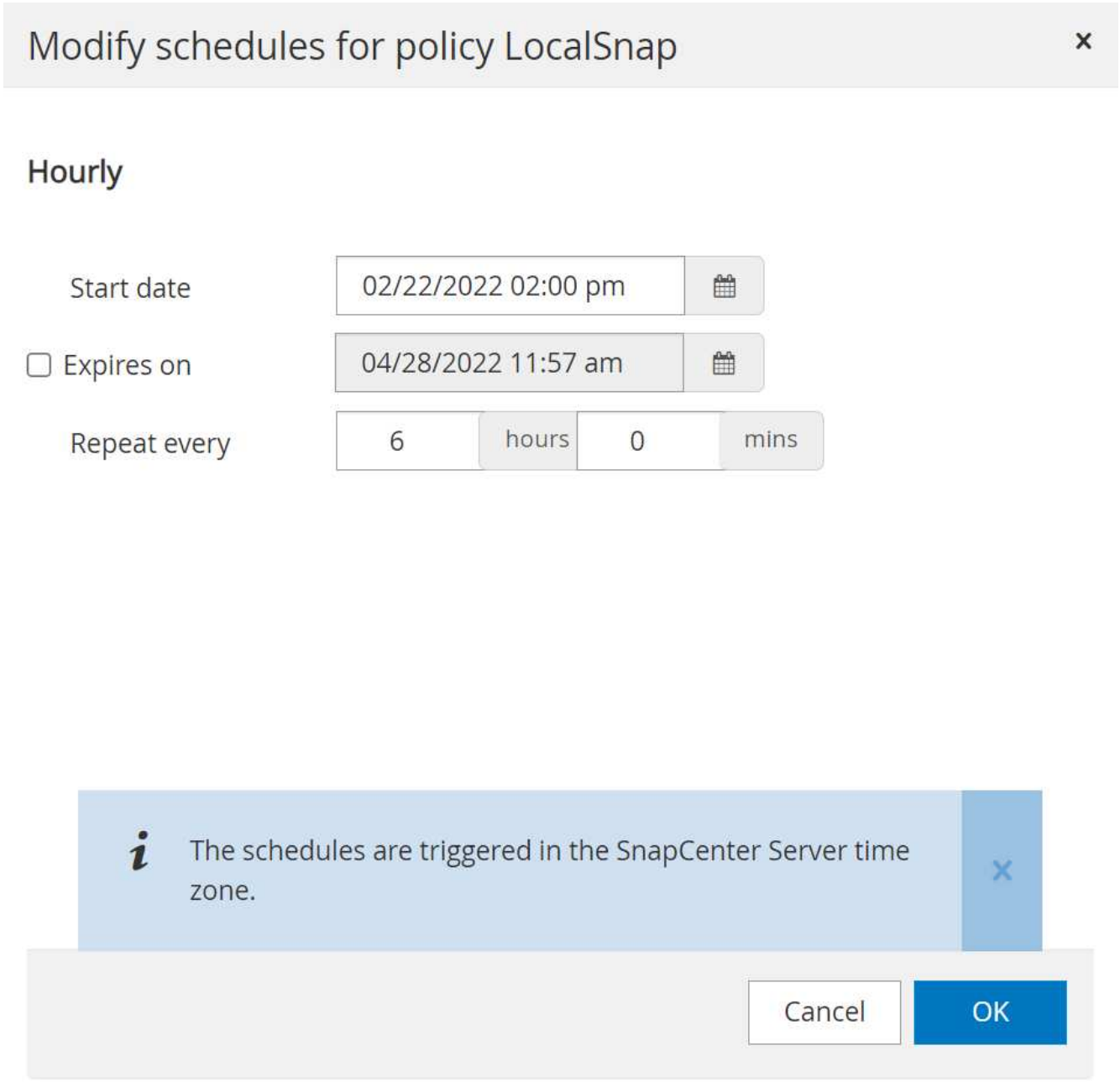
7. Define the schedule for the block integrity check policy.

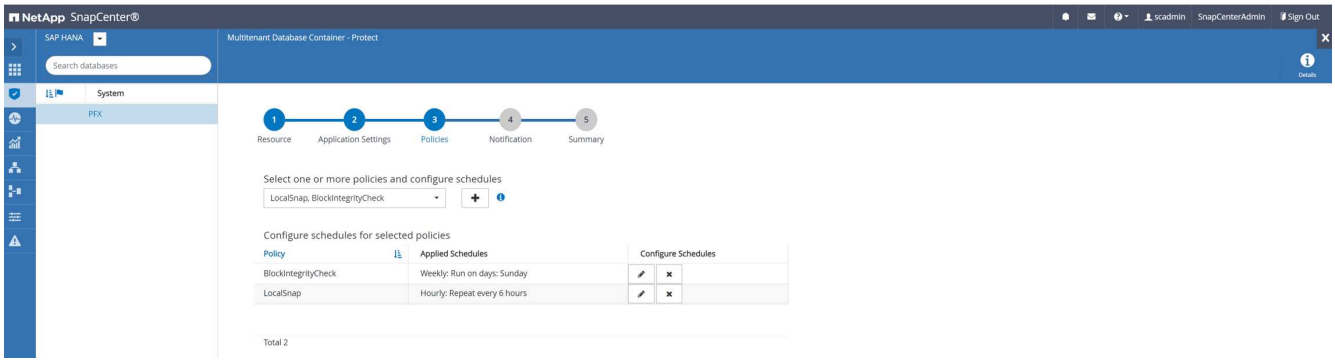
   In this example, it is set for once per week.



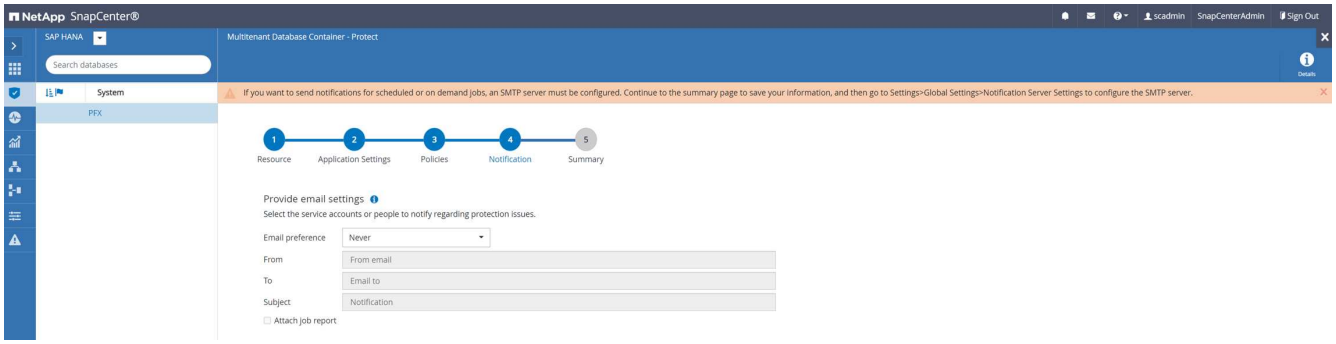
8. Define the schedule for the local Snapshot policy.

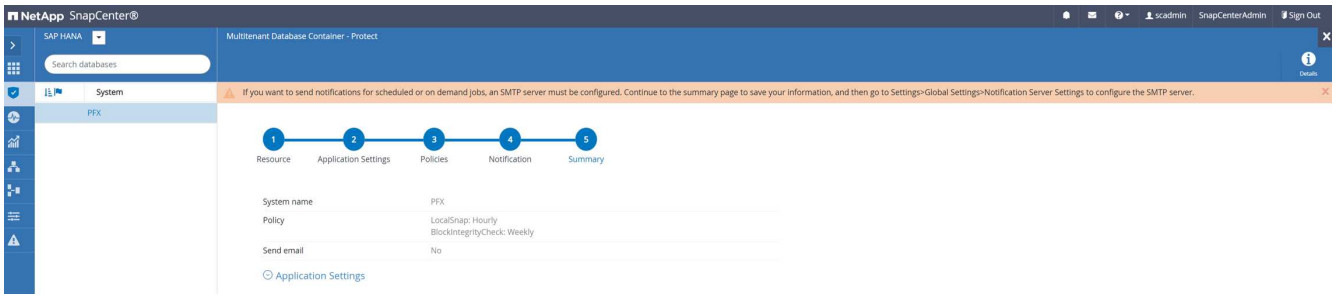
   In this example, it is set for every 6 hours.



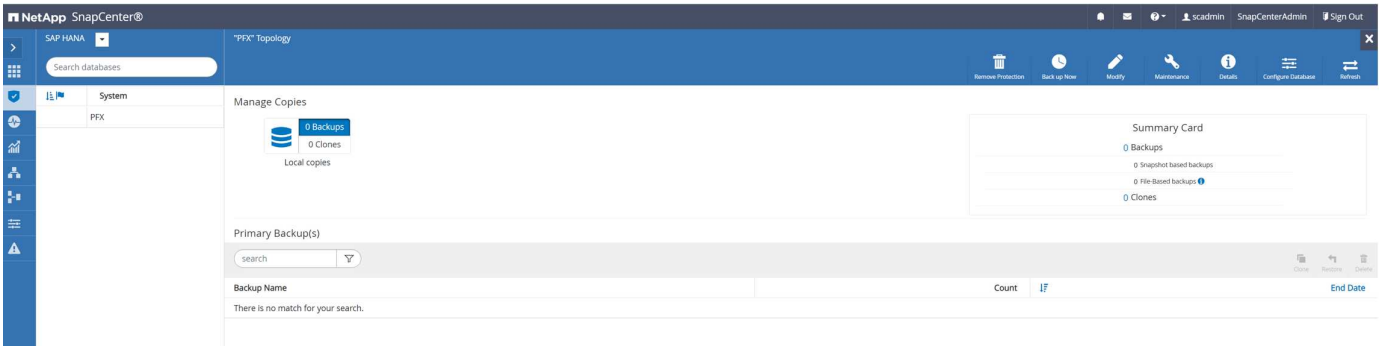


9. Provide information about the email notification.





The HANA resource configuration is now completed, and you can execute backups.



SnapCenter backup operations

You can create an on-demand Snapshot backup and an on-demand block integrity check operation.

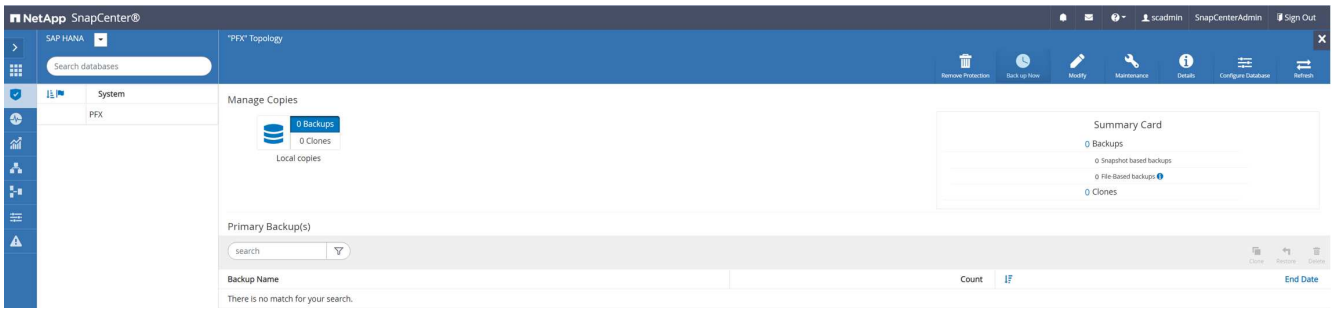
Create an on-demand Snapshot backup

Follow these steps to create on-demand Snapshot backups.

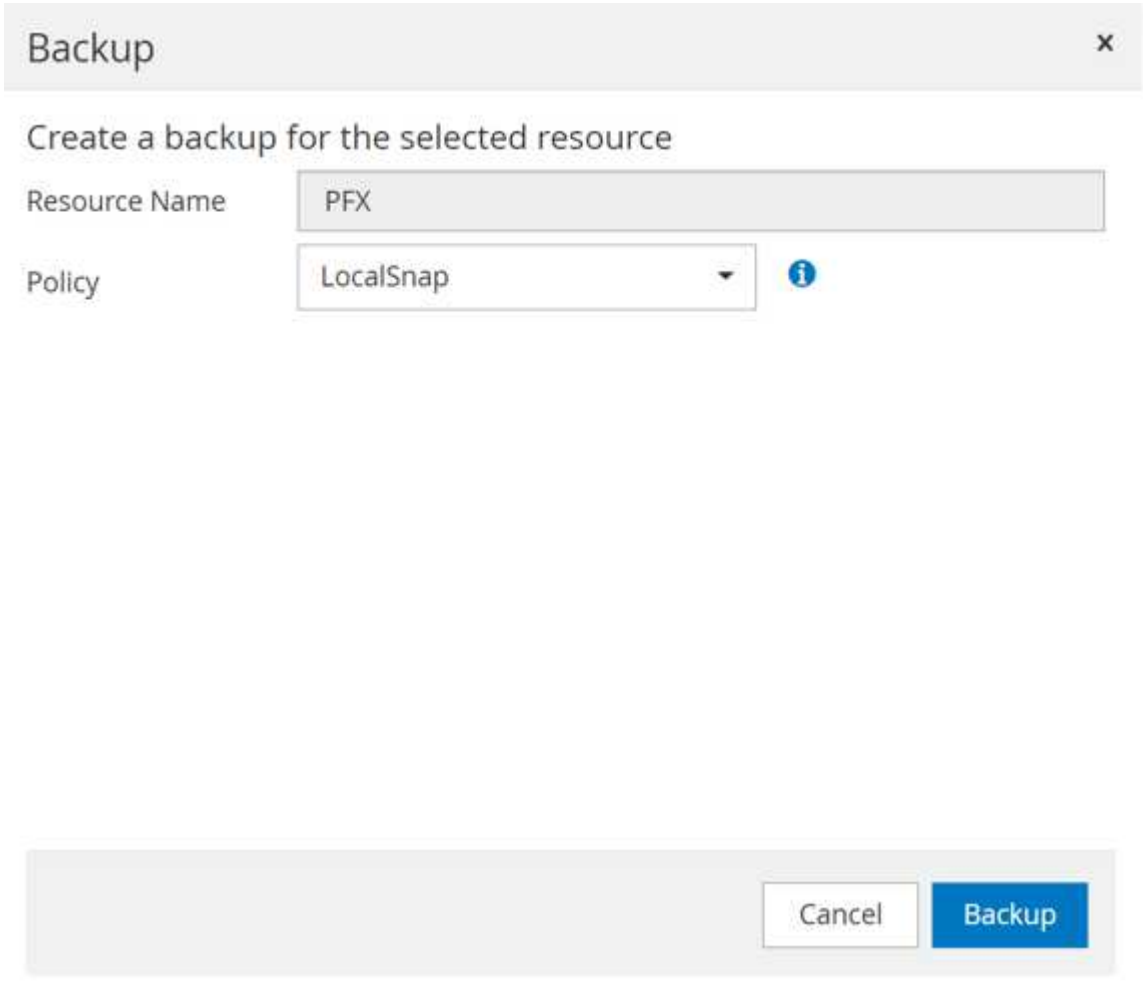
1. In the Resource view, select the resource and double-click the line to switch to the Topology view.

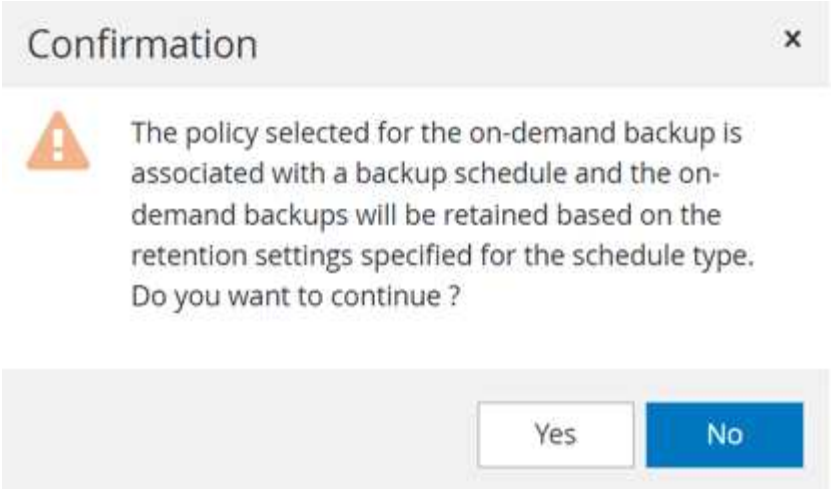
   The Resource Topology view provides an overview of all available backups that have been created by using SnapCenter. The top area of this view displays the backup topology showing the backups on the primary storage (local copies) and, if available, on the off-site backup storage (vault copies).

2. In the top row, select the Back up Now icon to start an on-demand backup.



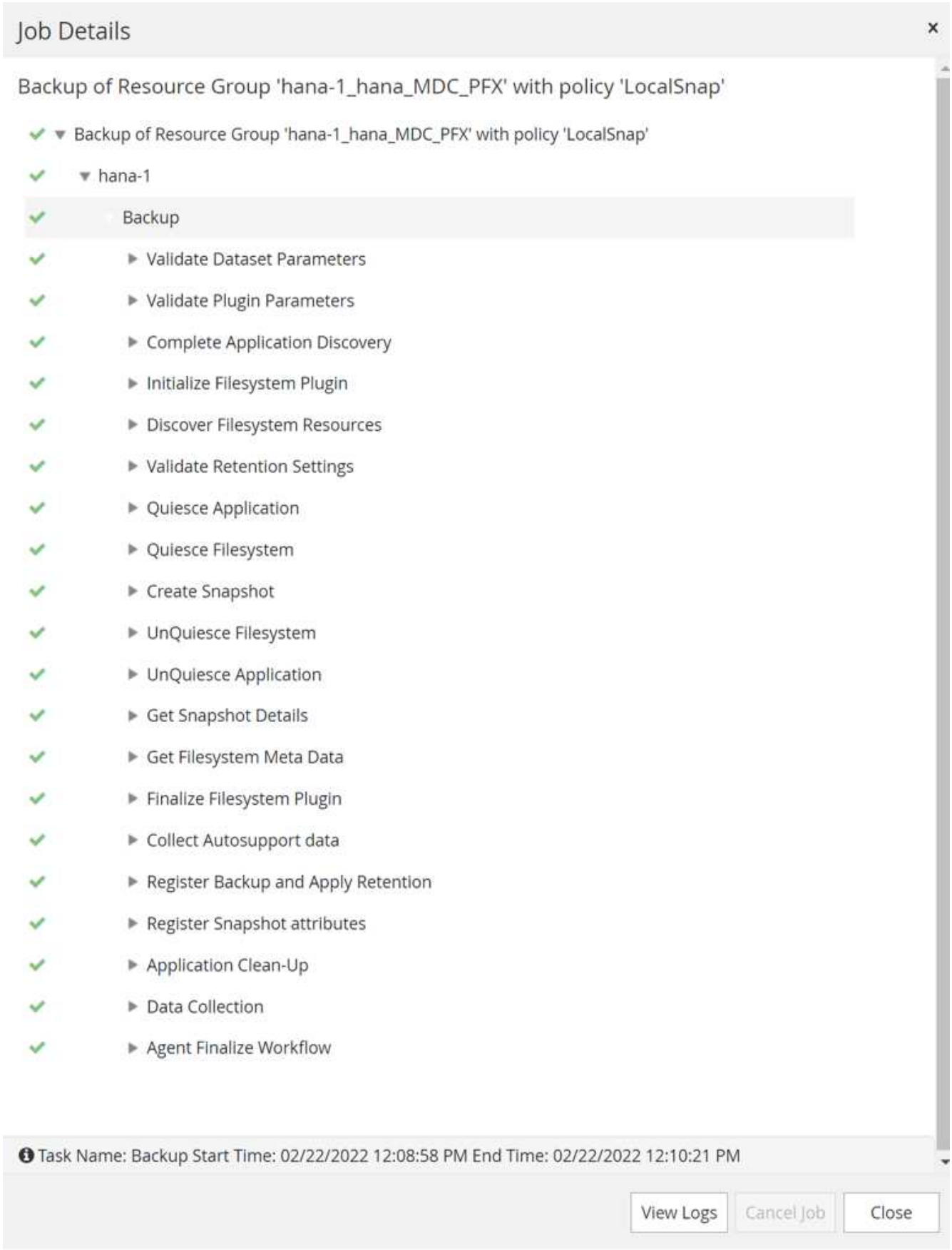
3. From the drop-down list, select the backup policy `LocalSnap`, and then click Backup to start the on-demand backup.





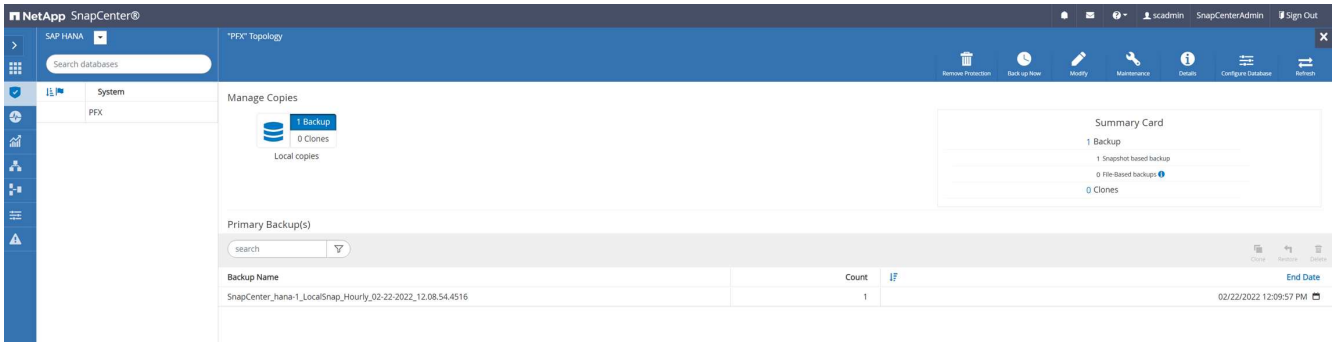
A log of the previous five jobs is shown in the Activity area at the bottom of the Topology view.

4. 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

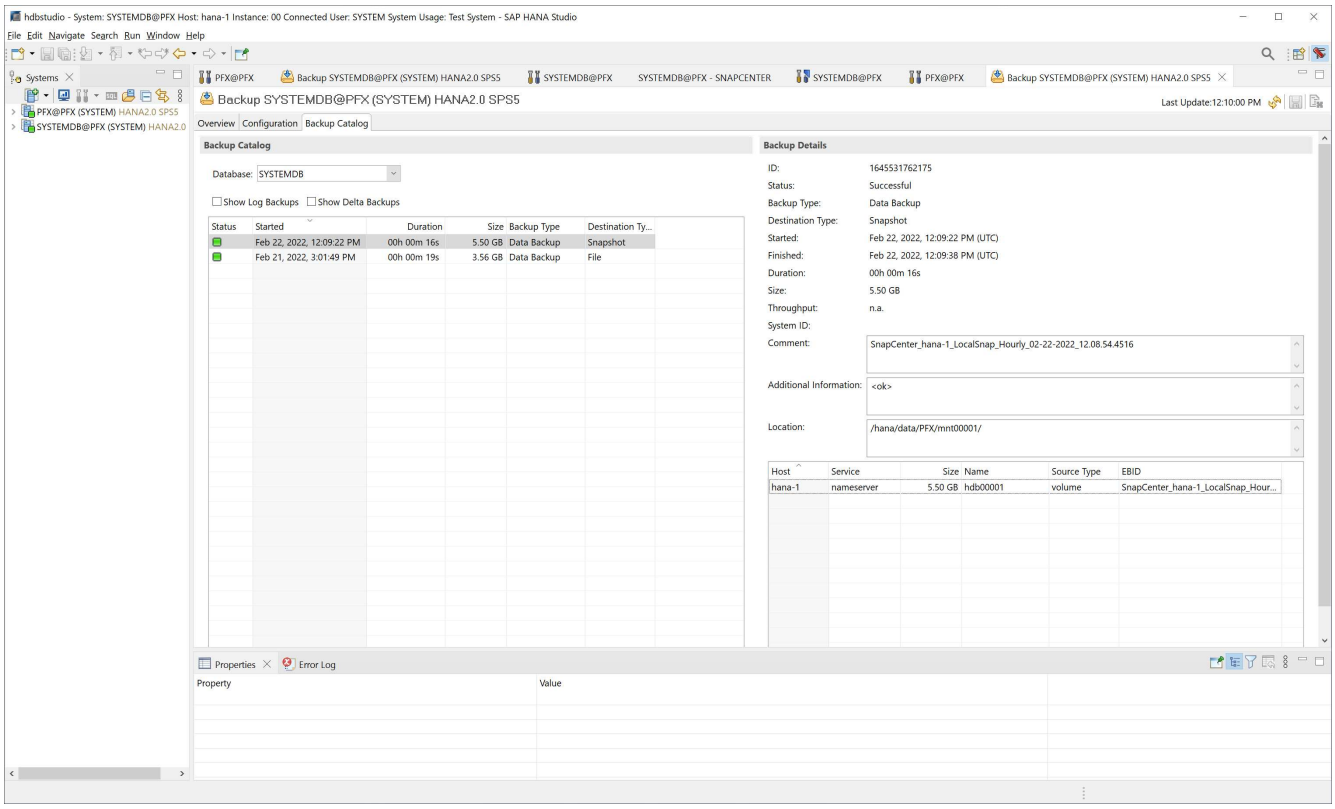


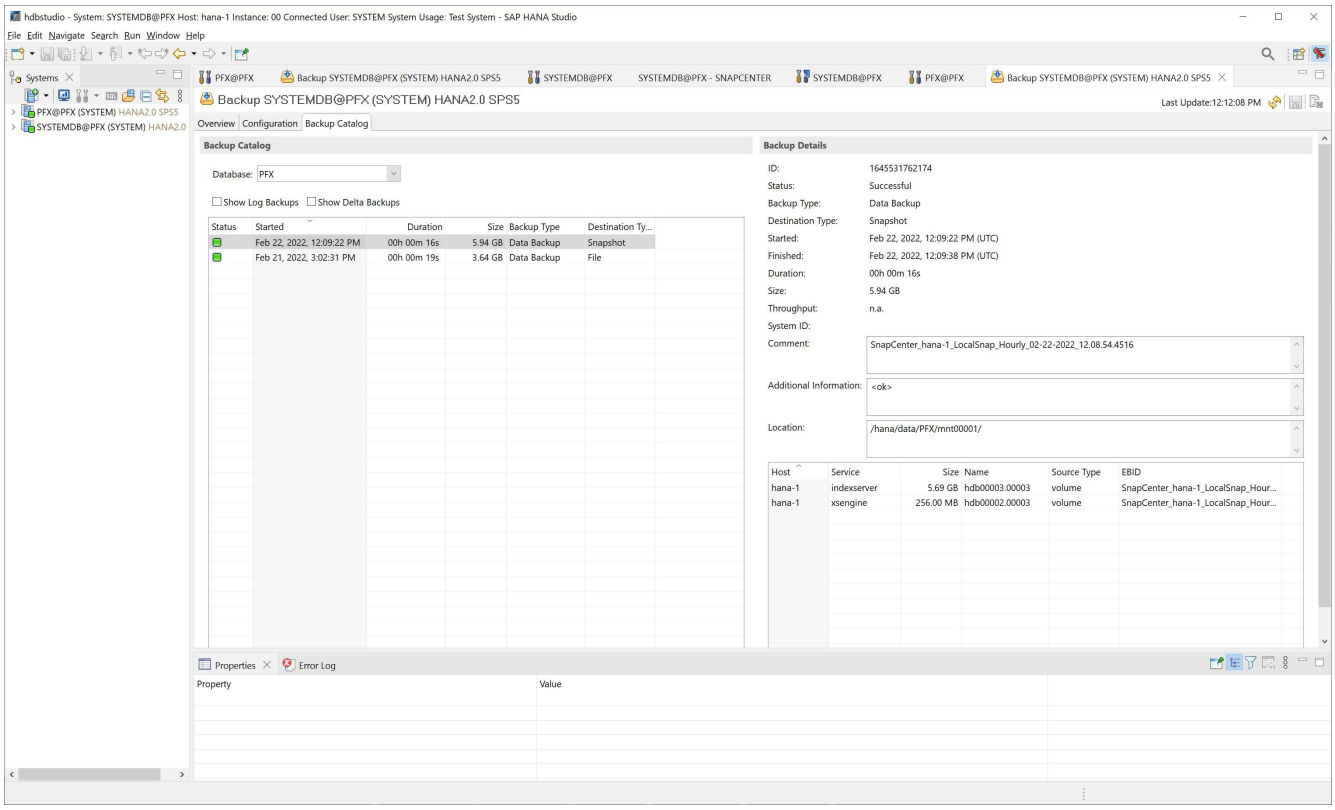
When the backup is finished, a new entry is shown in the topology view. The backup names follow the same naming convention as the Snapshot name defined in the section “Configure and protect a HANA resource”.

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



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 the following figure for the system database and in the next figure for the tenant database PFX.



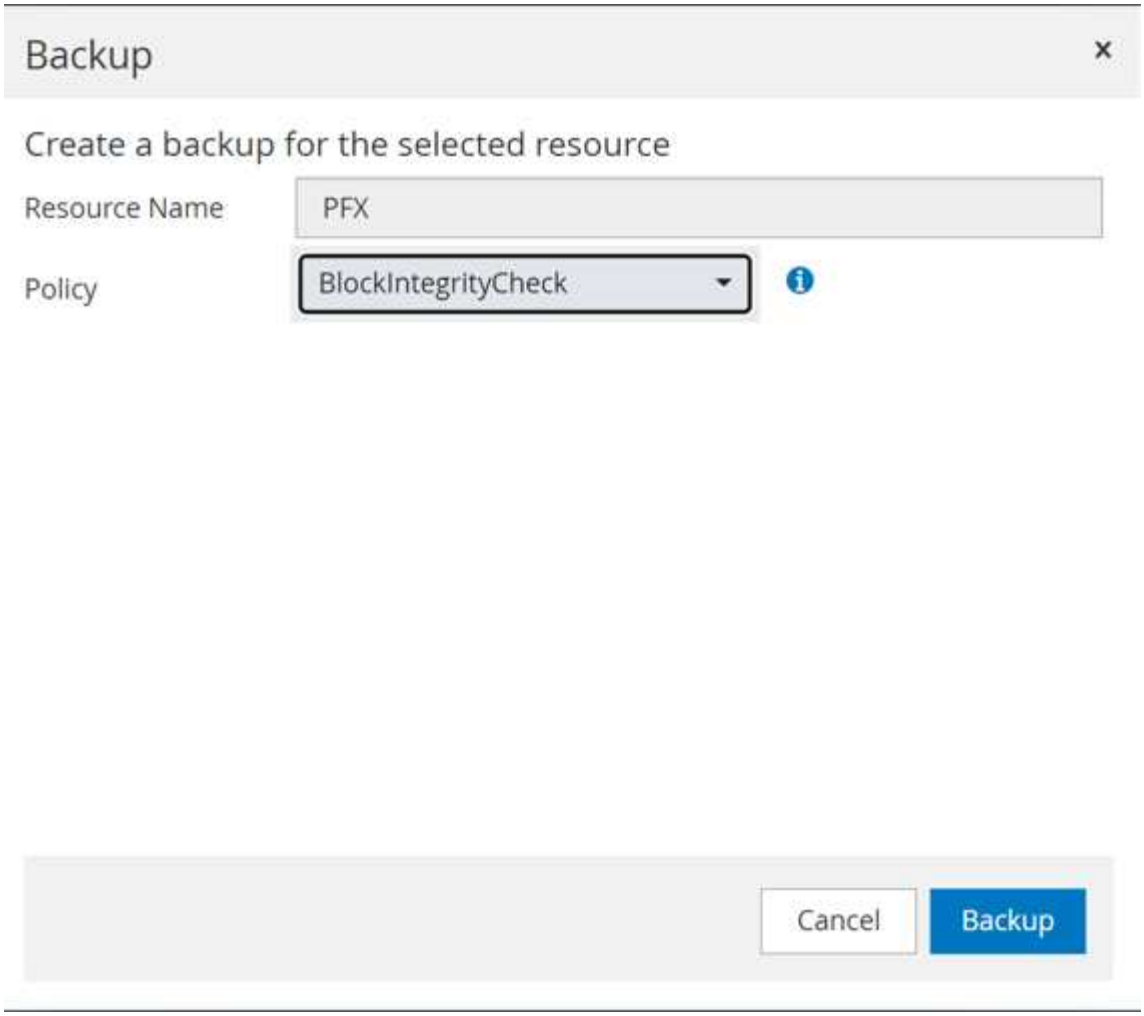


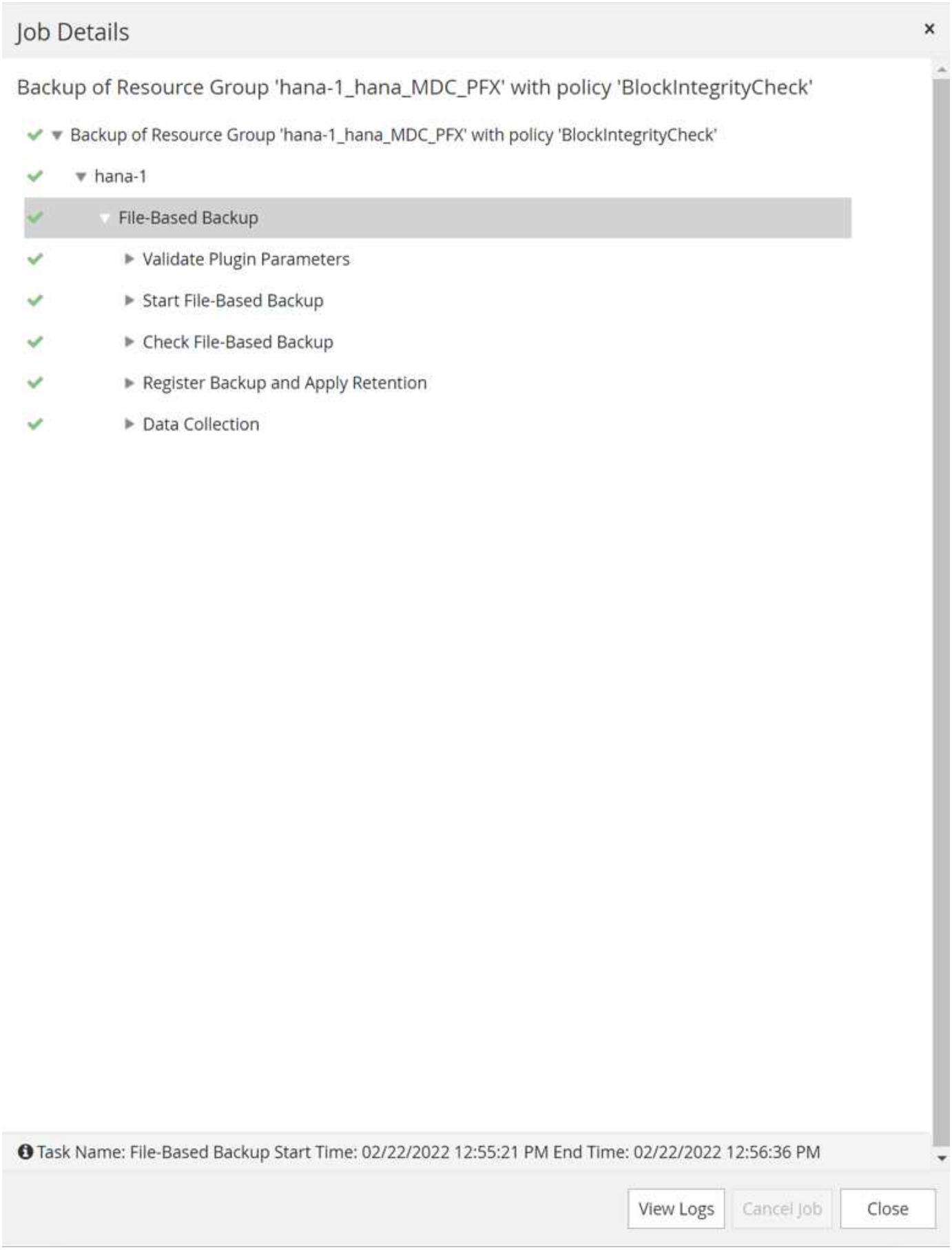
On the FSx for ONTAP file system, you can list the Snapshot backups by connecting to the console of the SVM.

```
sapcc-hana-svm::> snapshot show -volume PFX_data_mnt00001
---Blocks---
Vserver  Volume   Snapshot                                  Size Total%
Used%
-------- -------- ------------------------------------ -------- ------
-----
sapcc-hana-svm
         PFX_data_mnt00001
                  SnapCenter_hana-1_LocalSnap_Hourly_02-22-
2022_12.08.54.4516
                                                       126.6MB     0%
2%
sapcc-hana-svm::>
```

Create an on-demand block integrity check operation

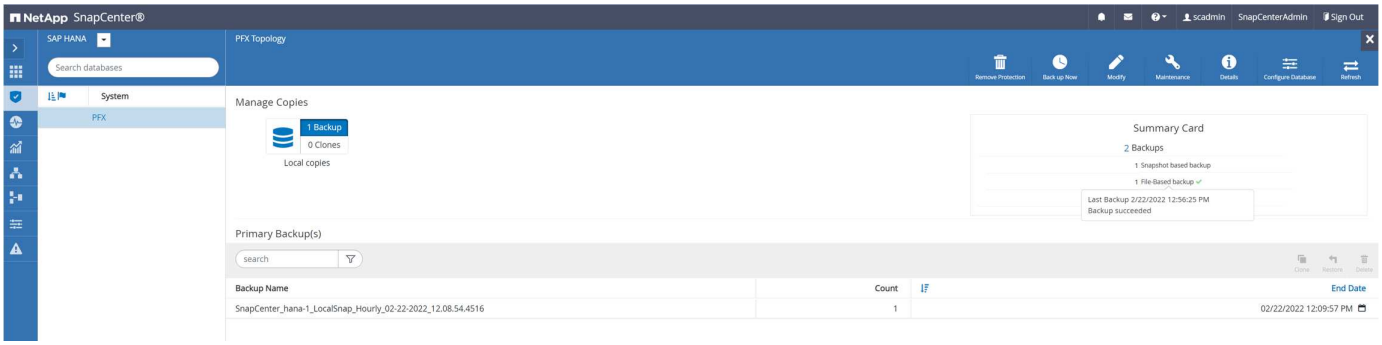
An on-demand block integrity check operation is executed in the same way as a Snapshot backup job, by selecting the policy BlockIntegrityCheck. When scheduling backups using this policy, SnapCenter creates a standard SAP HANA file backup for the system and tenant databases.


Backup
Create a backup for the selected resource
Resource Name
PFX
Policy
BlockIntegrityCheck
Cancel
Backup

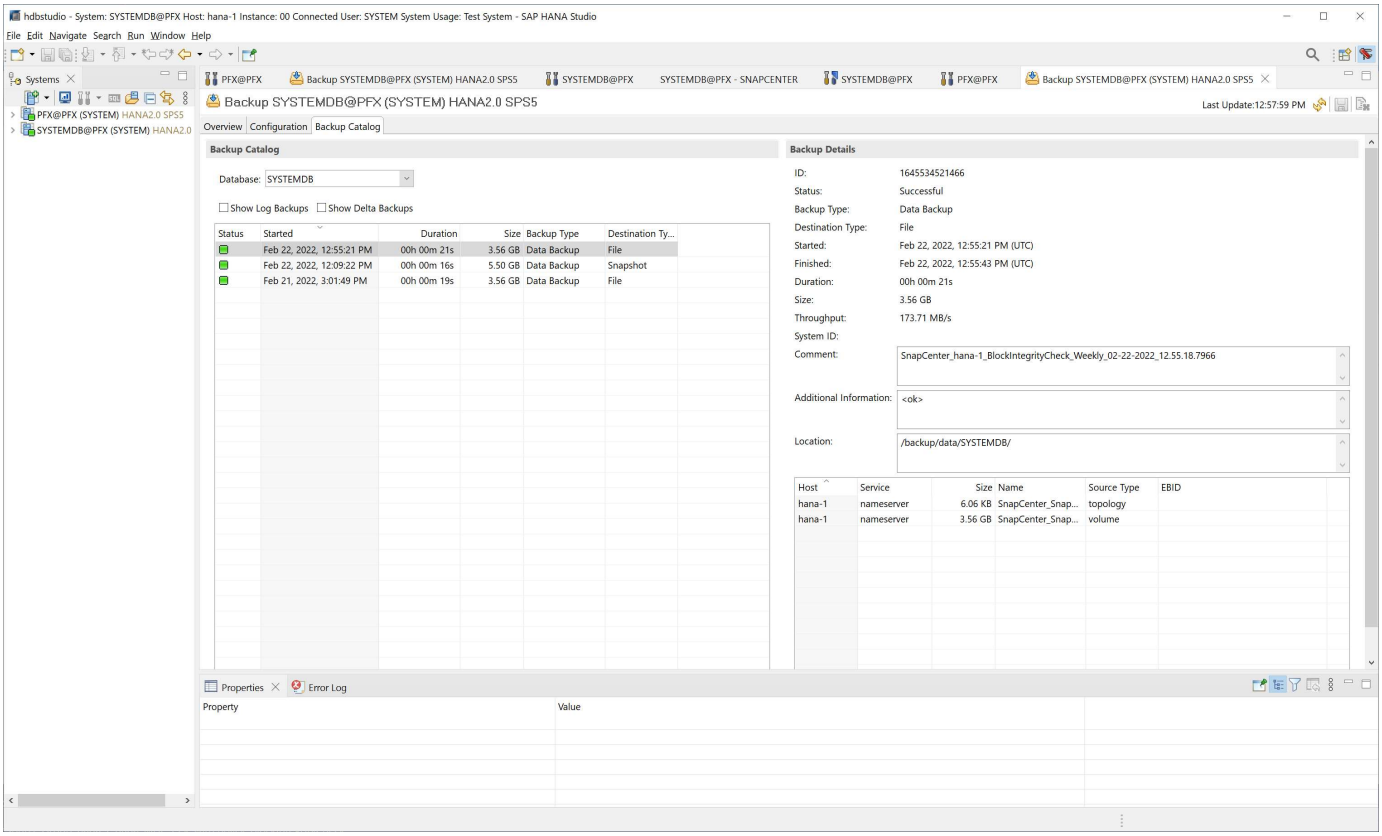


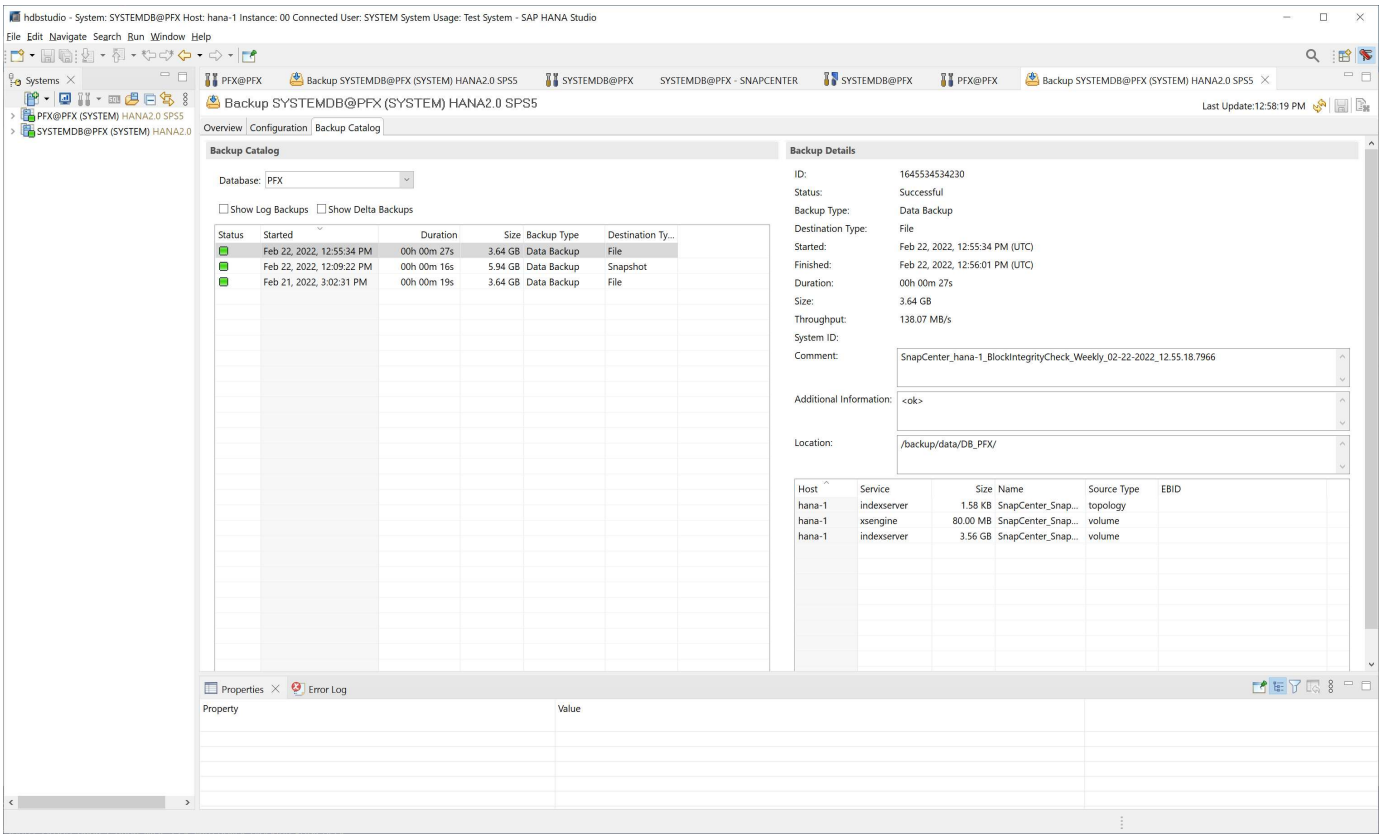
SnapCenter does not display the block integrity check in the same manner as Snapshot copy-based backups.

Instead, the summary card shows the number of file-based backups and the status of the previous backup.



The SAP HANA backup catalog shows entries for both the system and the tenant databases. The following figures show the SnapCenter block integrity check in the backup catalog of the system and the tenant database.





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

```
hana-1:~ # ls -al /backup/data/*
/backup/data/DB_PFX:
total 7665384
drwxr-xr-- 2 pfxadm sapsys       4096 Feb 22 12:56 .
drwxr-xr-x 4 pfxadm sapsys       4096 Feb 21 15:02 ..
-rw-r----- 1 pfxadm sapsys     155648 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_0_1
-rw-r----- 1 pfxadm sapsys   83894272 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_2_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_3_1
-rw-r----- 1 pfxadm sapsys     155648 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_0_1
-rw-r----- 1 pfxadm sapsys   83894272 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_2_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 22 12:56
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_3_1
/backup/data/SYSTEMDB:
total 7500880
drwxr-xr-- 2 pfxadm sapsys       4096 Feb 22 12:55 .
drwxr-xr-x 4 pfxadm sapsys       4096 Feb 21 15:02 ..
-rw-r----- 1 pfxadm sapsys     159744 Feb 21 15:01
COMPLETE_DATA_BACKUP_databackup_0_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 21 15:02
COMPLETE_DATA_BACKUP_databackup_1_1
-rw-r----- 1 pfxadm sapsys     159744 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_0_1
-rw-r----- 1 pfxadm sapsys 3825213440 Feb 22 12:55
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-
2022_12.55.18.7966_databackup_1_1
hana-1:~ #
```

Backup of non-data volumes

The backup of non-data volumes is an integrated part of the SnapCenter and 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 non-data files must be restored, NetApp recommends developing an additional backup strategy for non-data volumes to augment the SAP HANA database backup. Depending on

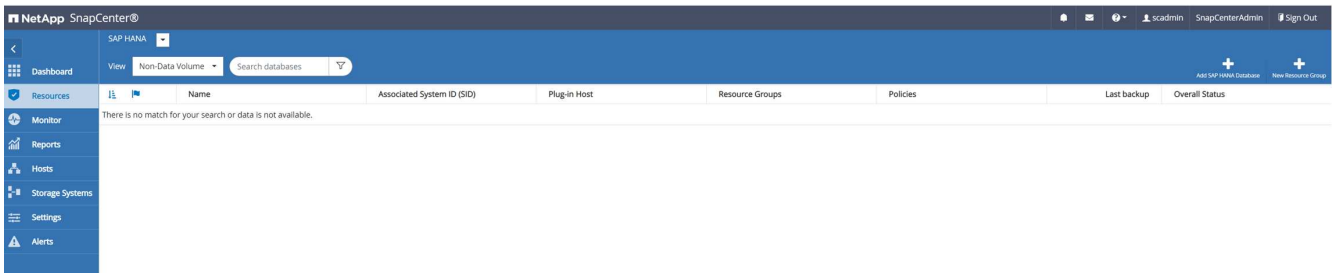
your specific requirements, the backup of non-data volumes might differ in scheduling frequency and retention settings, and you should consider how frequently non-data files are changed. For instance, the HANA volume `/hana/shared` contains executables but also SAP HANA trace files. While executables 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 non-data volume backup enables Snapshot copies of all relevant volumes to be created in a few seconds with the same space efficiency as SAP HANA database backups. The difference is that there is no SQL communication with SAP HANA database required.

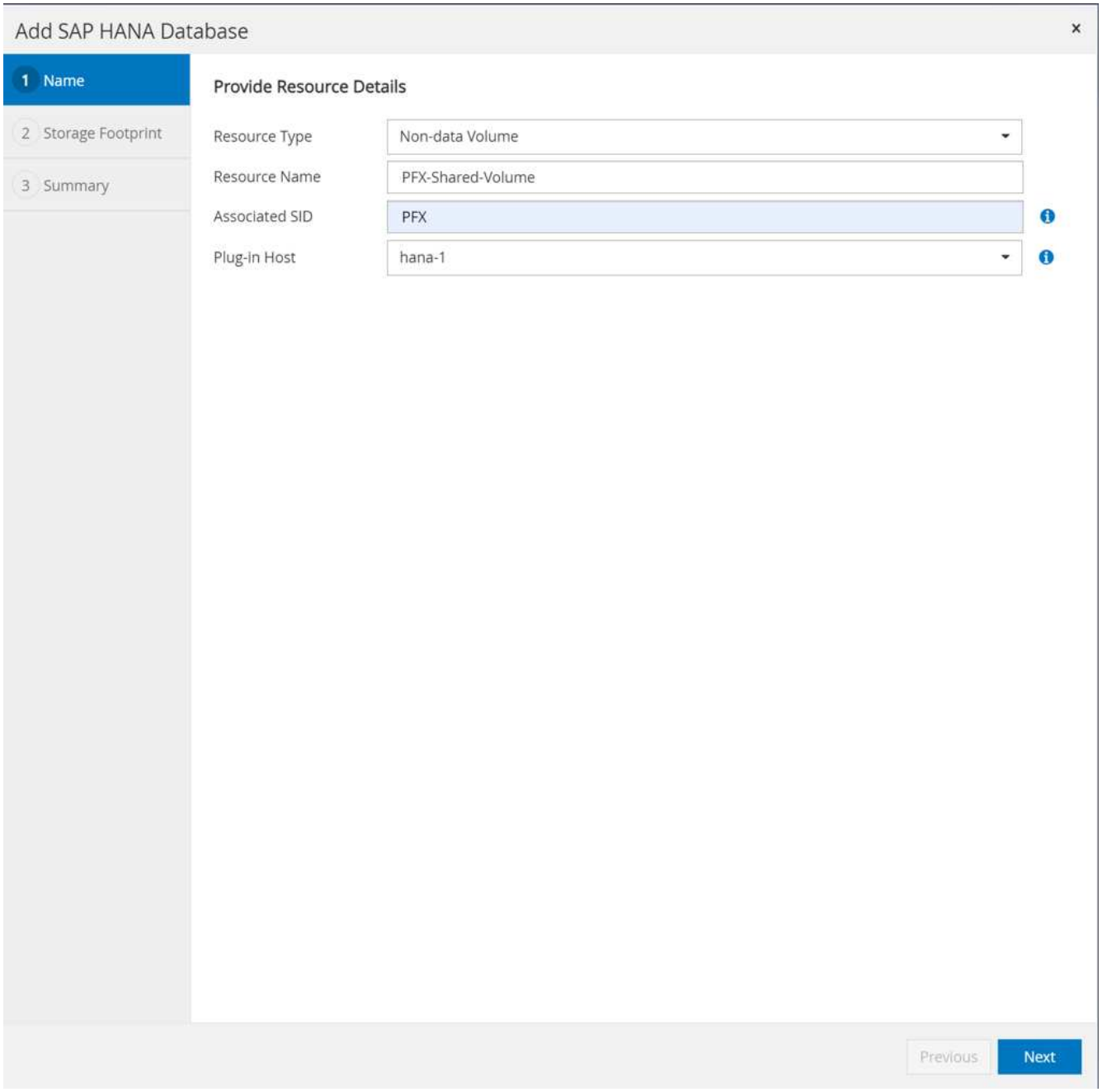
Configure non-data volume resources

Follow these steps to configure non-data volume resources:

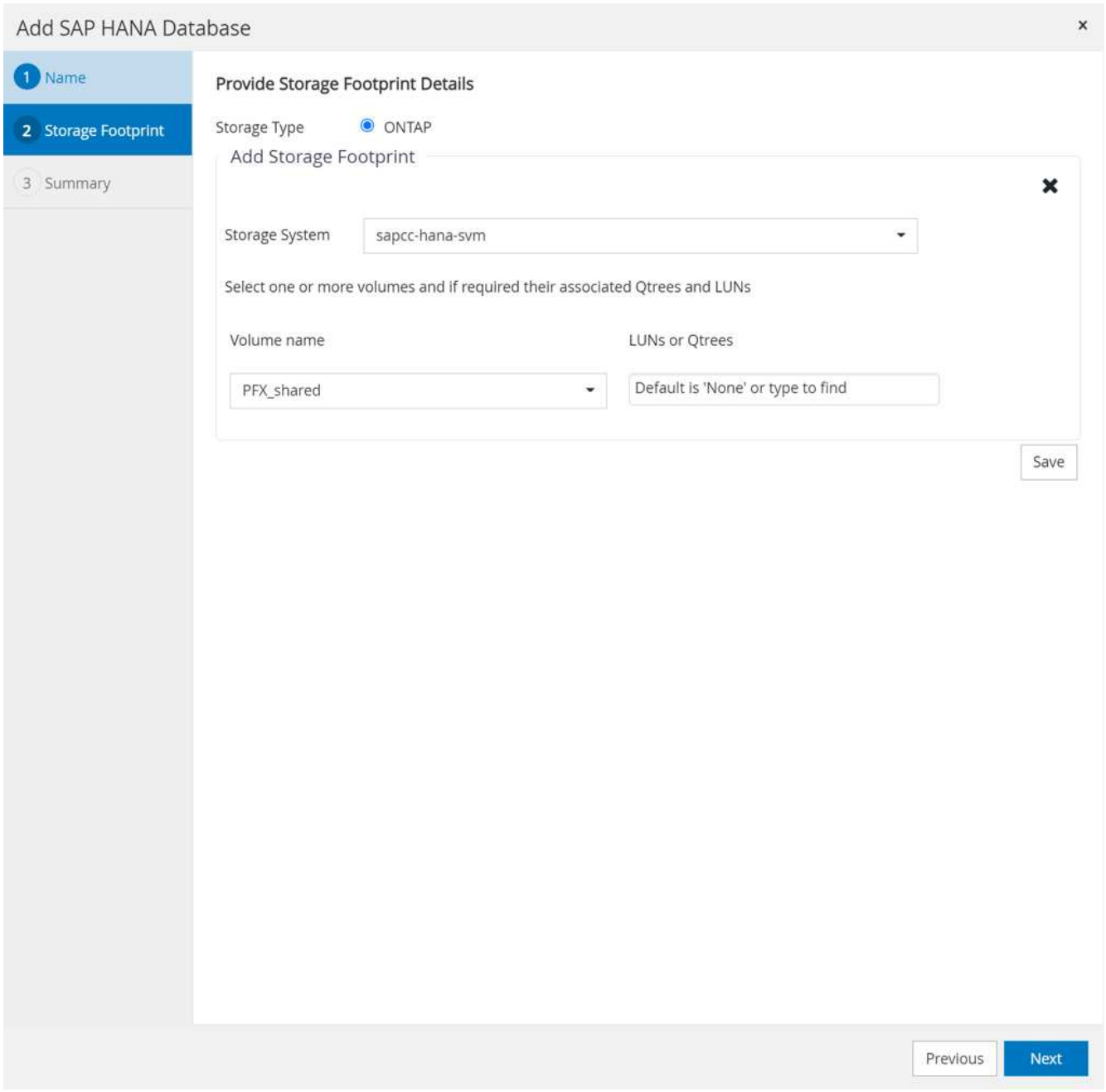
1. From the Resources tab, select Non-Data-Volume and click Add SAP HANA Database.



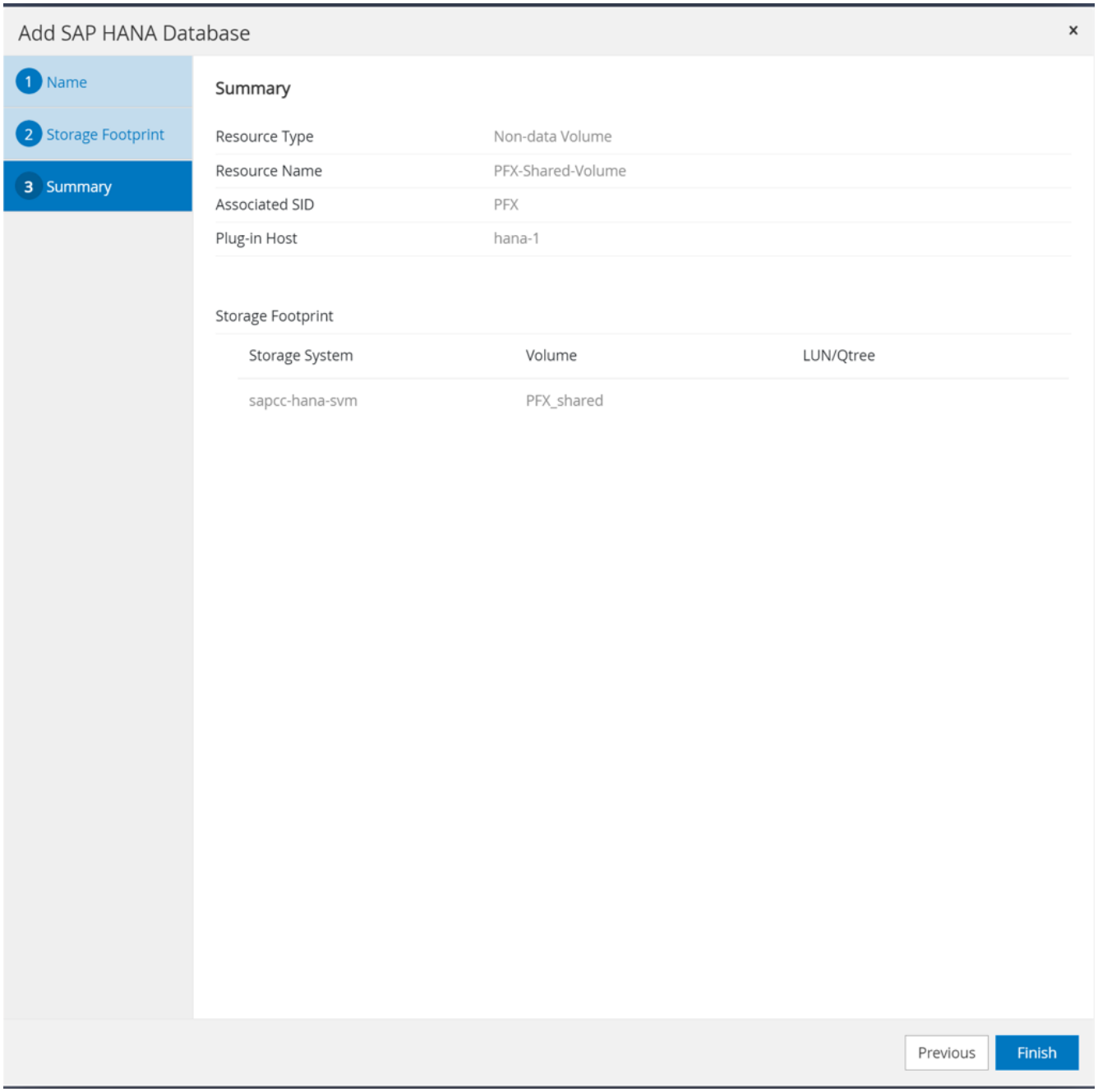
2. In step one of the Add SAP HANA Database dialog, in the Resource Type list, select Non- data Volumes. Specify a name for the resource and the associated SID and the SAP HANA plug-in host that you want to use for the resource, then click Next.



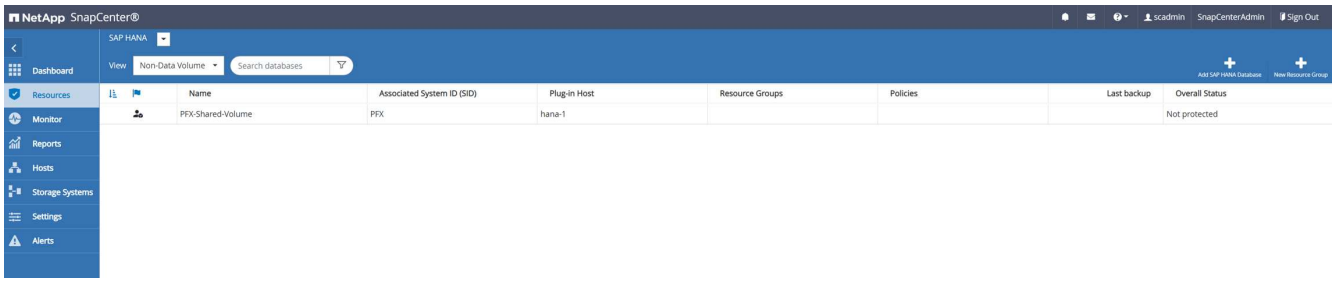
3. Add the SVM and the storage volume as storage footprint, then click Next.



4. To save the settings, in the summary step, click Finish.



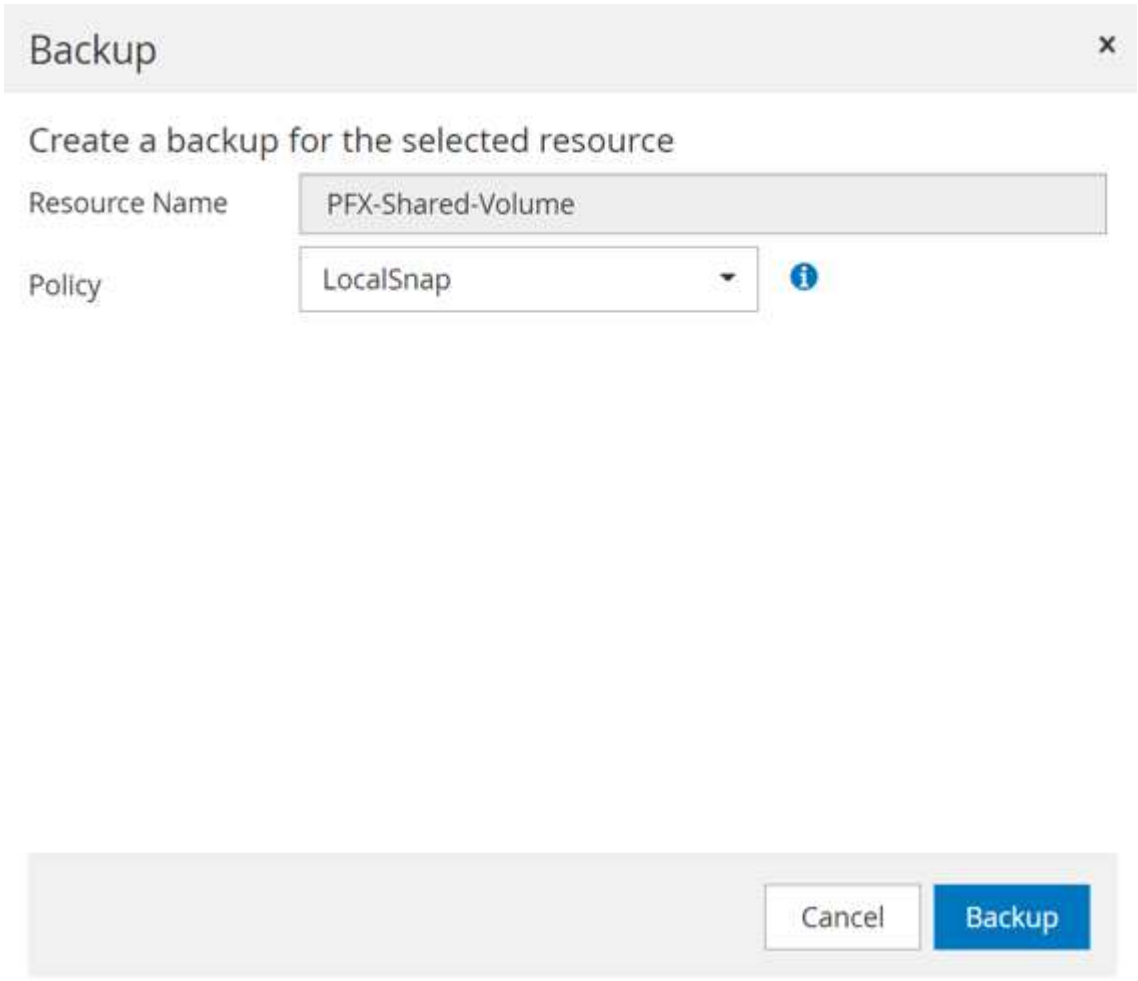
The new non-data volume is now added to SnapCenter. Double click the new resource to execute the resource protection.



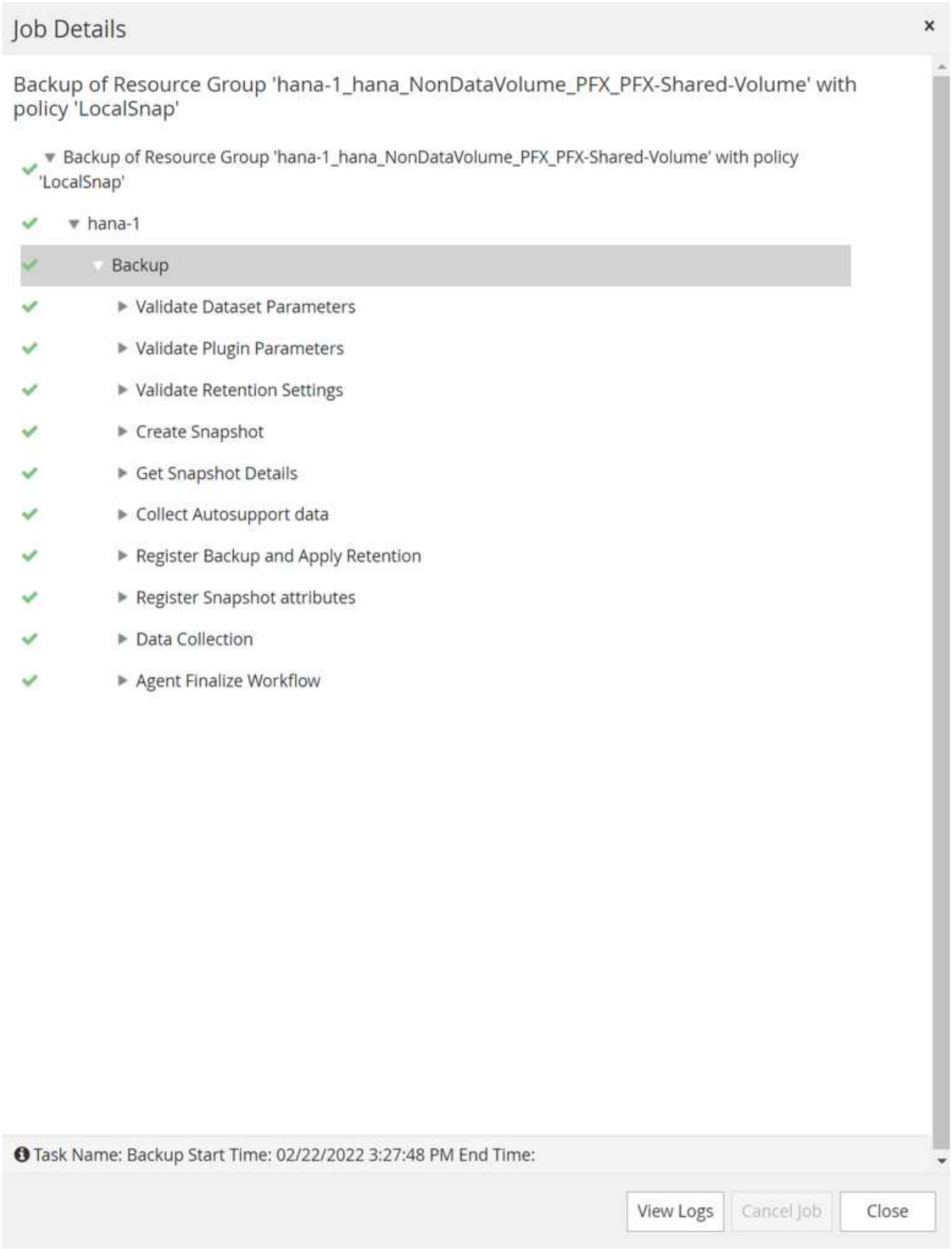
The resource protection is done in the same way as described before with a HANA database resource.

5. You can now execute a backup by clicking on Backup Now.

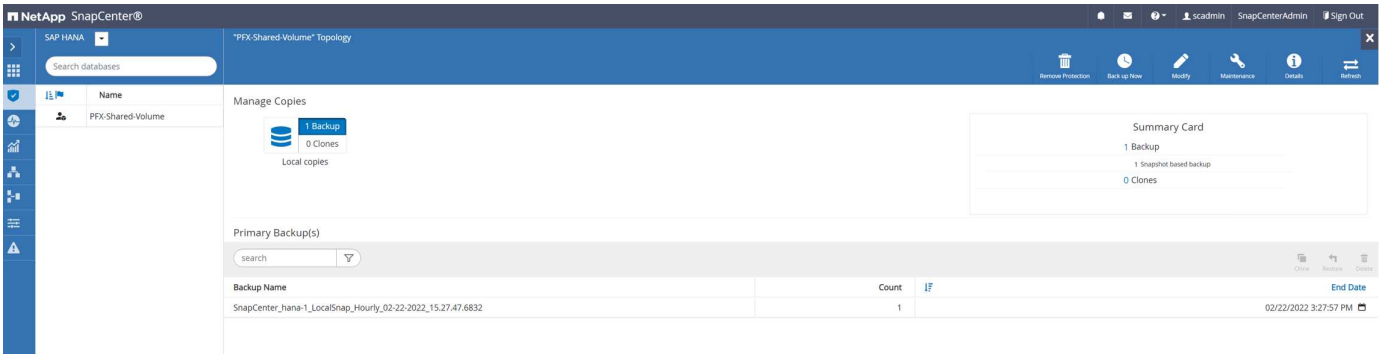
6. Select the policy and start the backup operation.



The SnapCenter job log shows the individual workflow steps.



The new backup is now visible in the resource view of the non- data volume resource.



Restore and recover

With SnapCenter, automated restore and recovery operations are supported for HANA single host MDC systems with a single tenant. For multiple-host systems or MDC systems with multiple tenants, SnapCenter only executes the restore operation and you must perform the recovery manually.

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

1. Select the backup to be used for the restore operation.
2. Select the restore type. Select Complete Restore with Volume Revert or without Volume Revert.
3. Select the recovery type from the following options:
    - To most recent state
    - Point in time
    - To specific data backup
    - No recovery

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

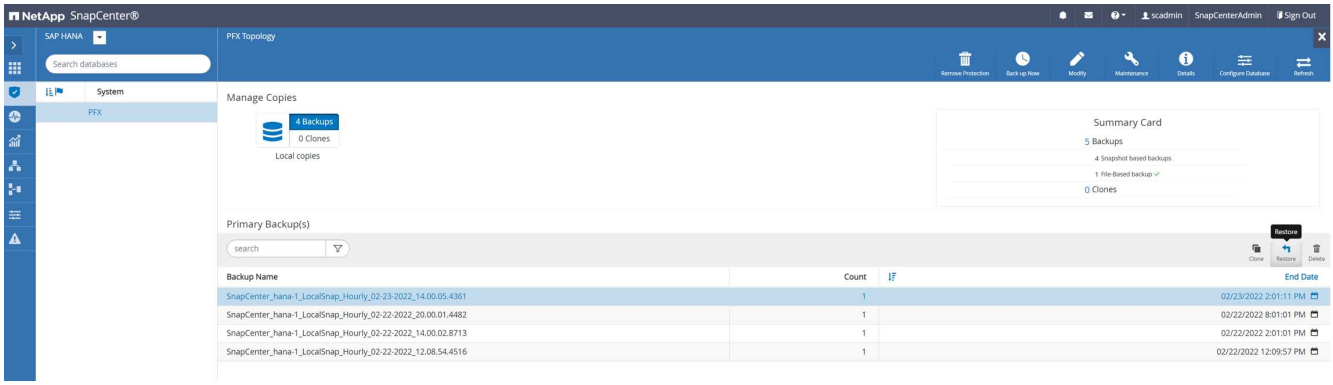
Next, SnapCenter performs the following operations:

1. It stops the HANA database.
2. It restores the database. Depending on the selected restore type, different operations are executed.
    - If Volume Revert is selected, then SnapCenter unmounts the volume, restores the volume by using volume-based SnapRestore on the storage layer, and mounts the volume.
    - If Volume Revert is not selected, then SnapCenter restores all files by using single file SnapRestore operations on the storage layer.
3. It recovers the database:
    a. By recovering the system database
    b. recovering the tenant database
    c. starting the HANA database

      If No Recovery is selected, SnapCenter exits, and you must perform the restore operation for the system and the tenant database manually.

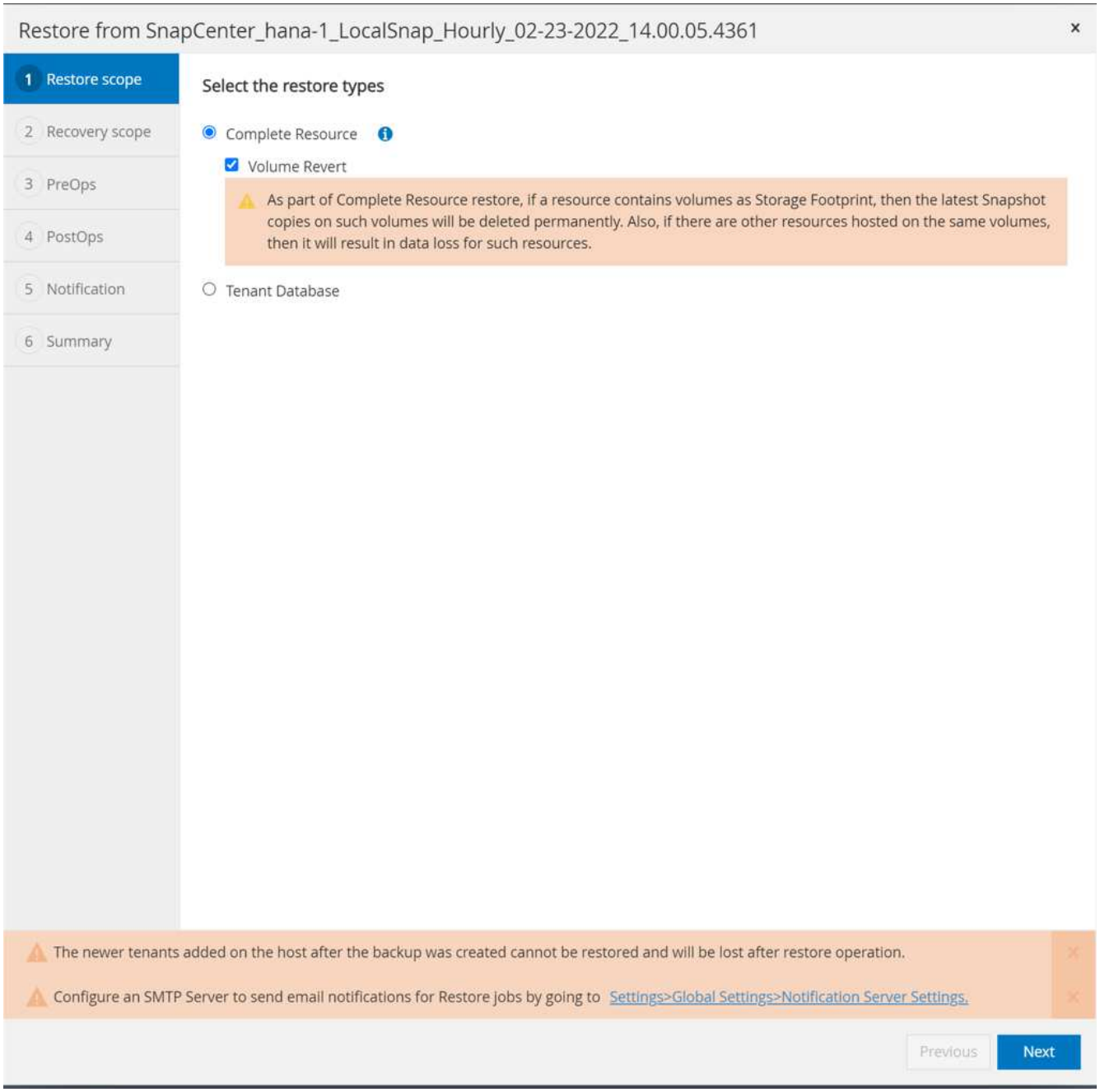
To perform a manual restore operation, follow these steps:

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



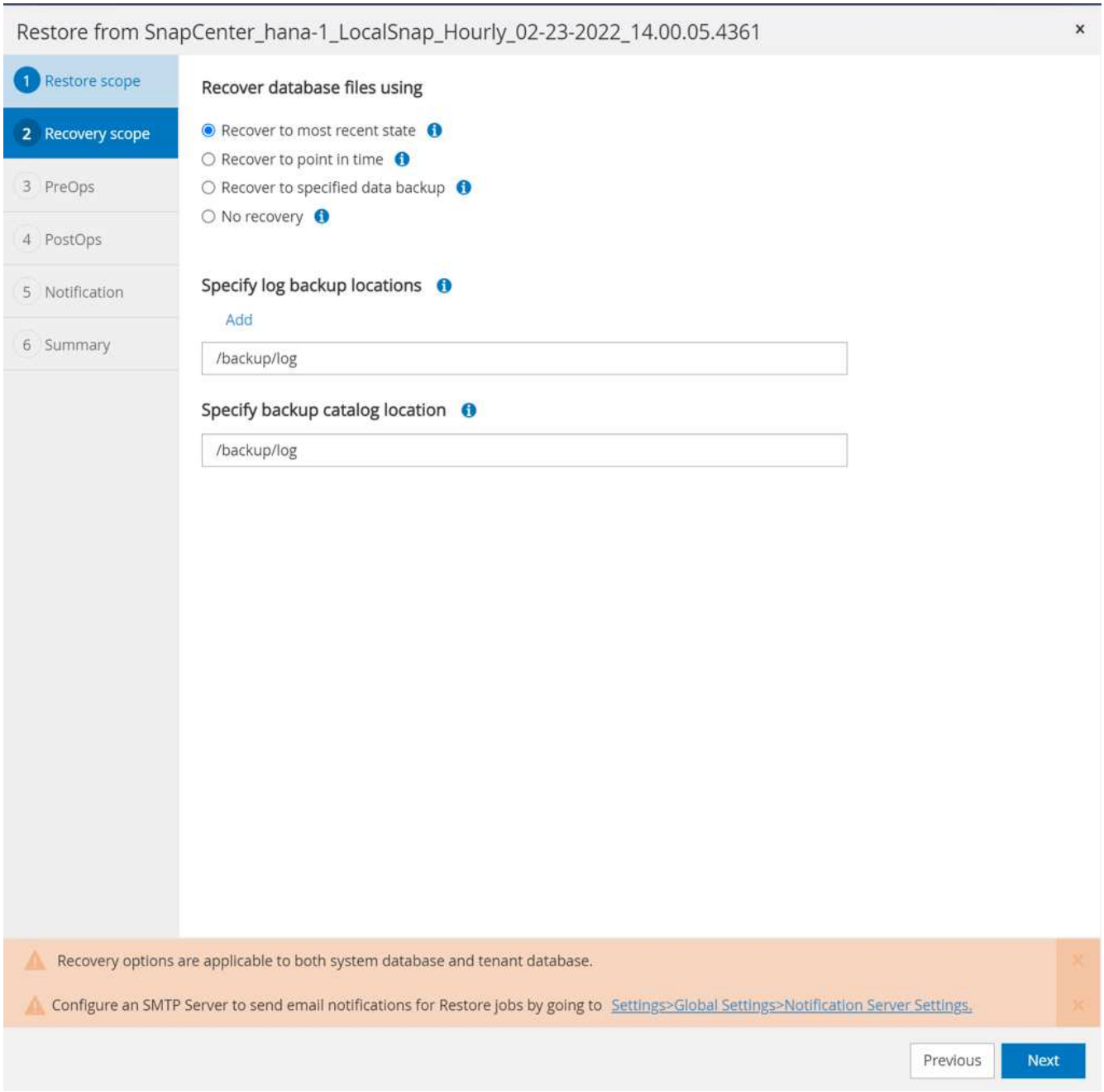
2. Select the restore scope and type.

   The standard scenario for HANA MDC single tenant systems is to use complete resource with volume revert. For a HANA MDC system with multiple tenants, you might want to restore only a single tenant. For more information about the single tenant restore, see Restore and recovery (netapp.com).

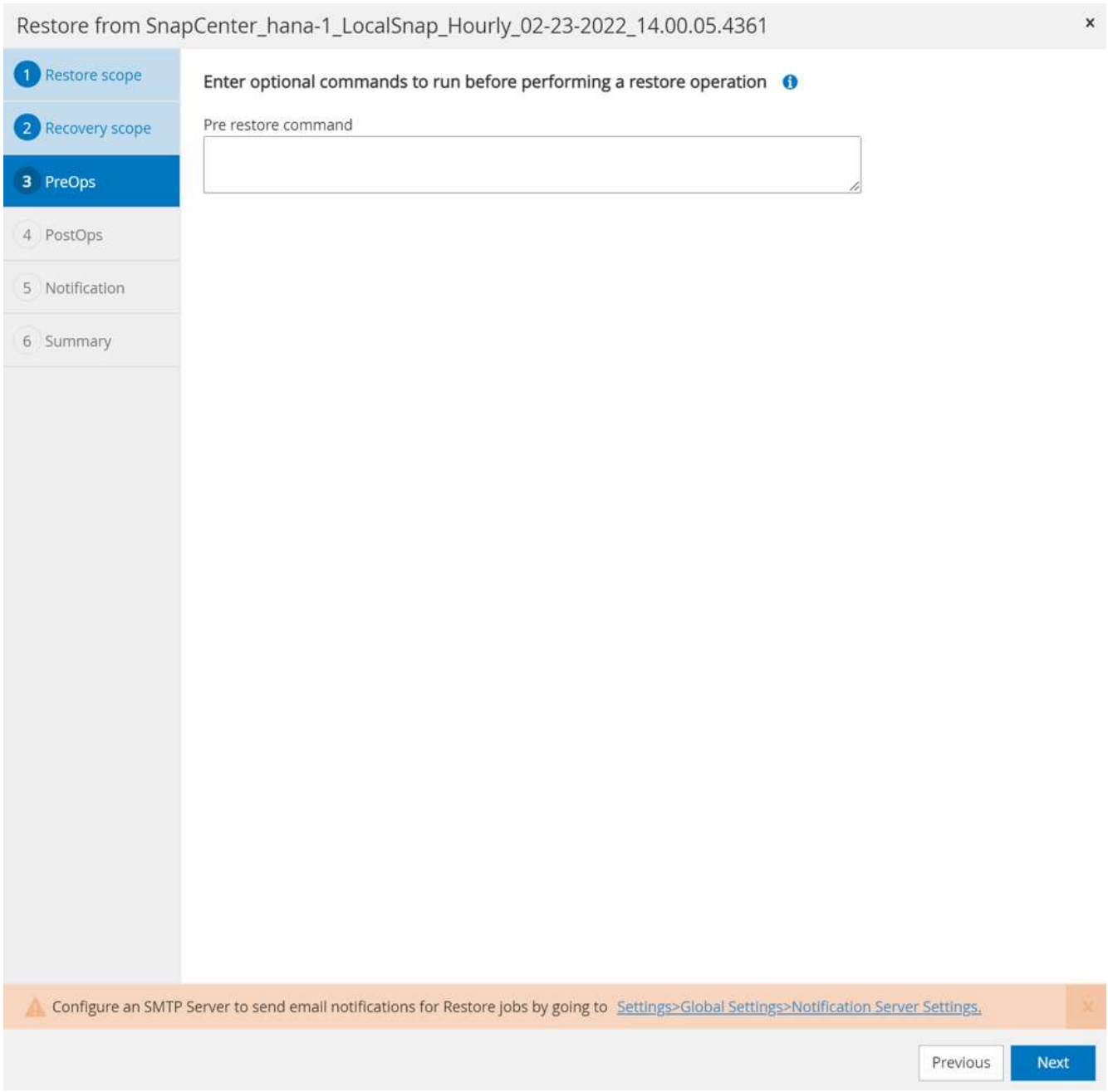


3. Select Recovery Scope and provide the location for log backup and catalog backup.

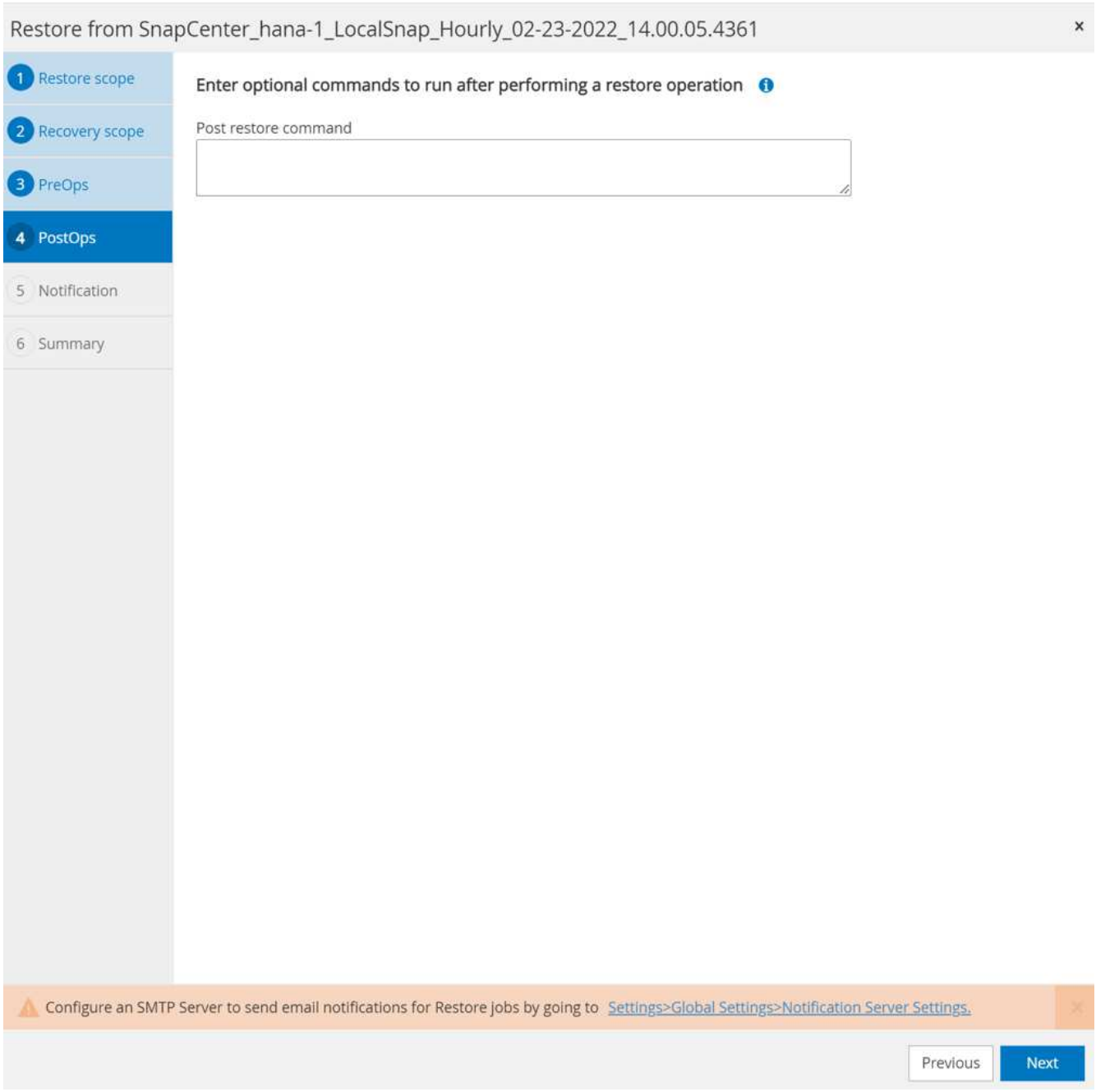
   SnapCenter uses the default path or the changed paths in the HANA global.ini file to prepopulate the log and catalog backup locations.



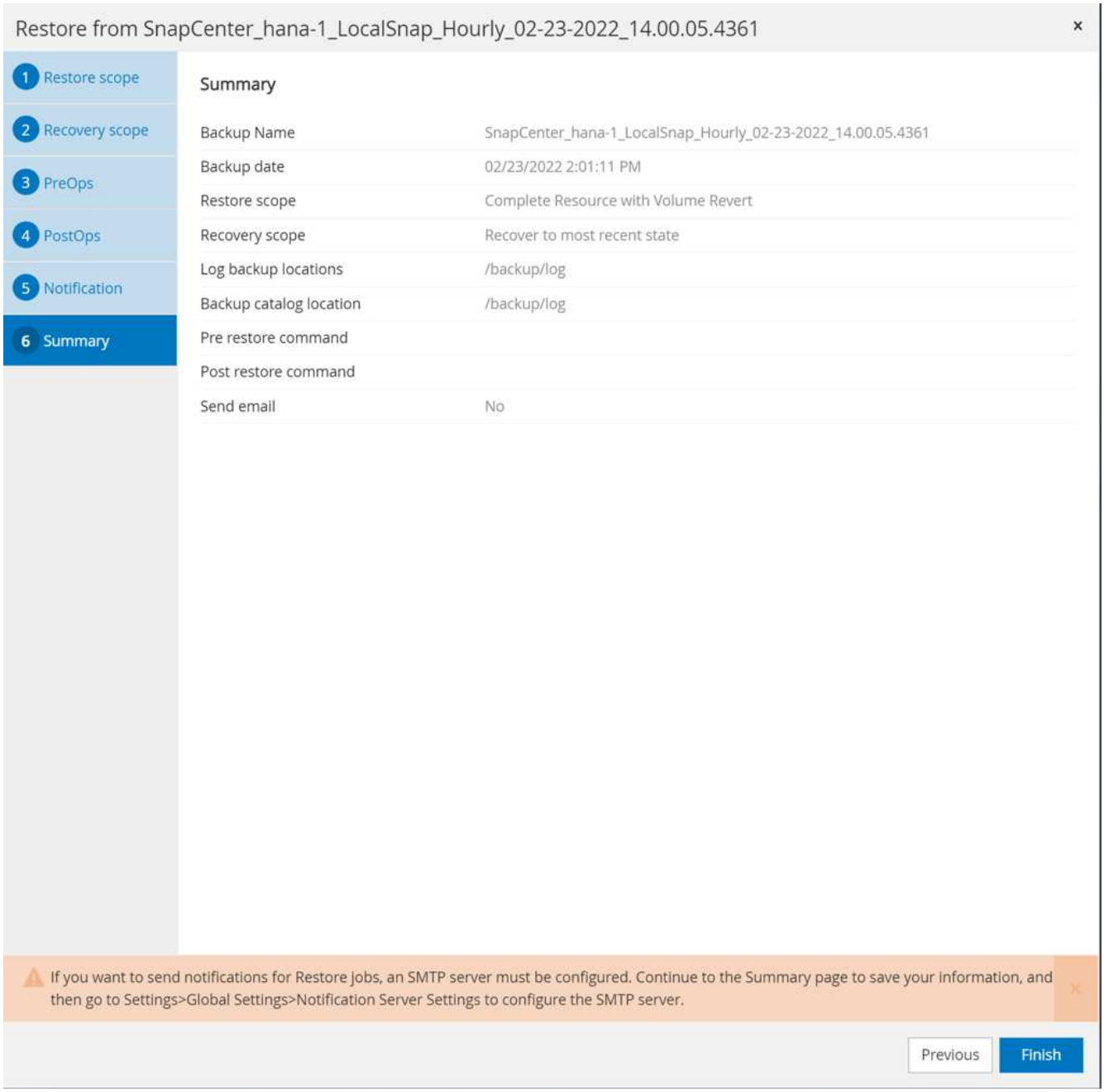
4. Enter the optional pre-restore commands.



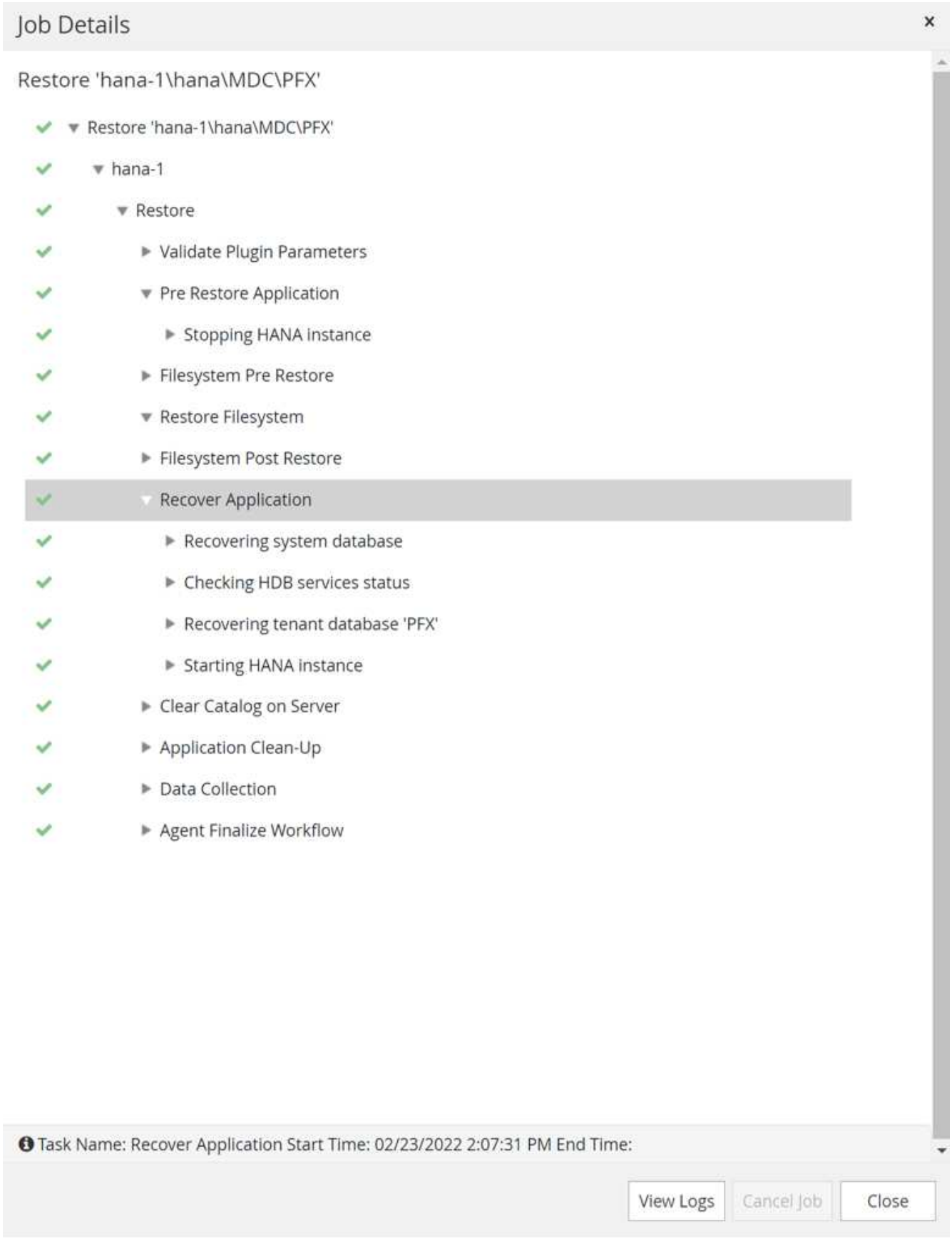
5. Enter the optional post-restore commands.



6. To start the restore and recovery operation, click Finish.



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

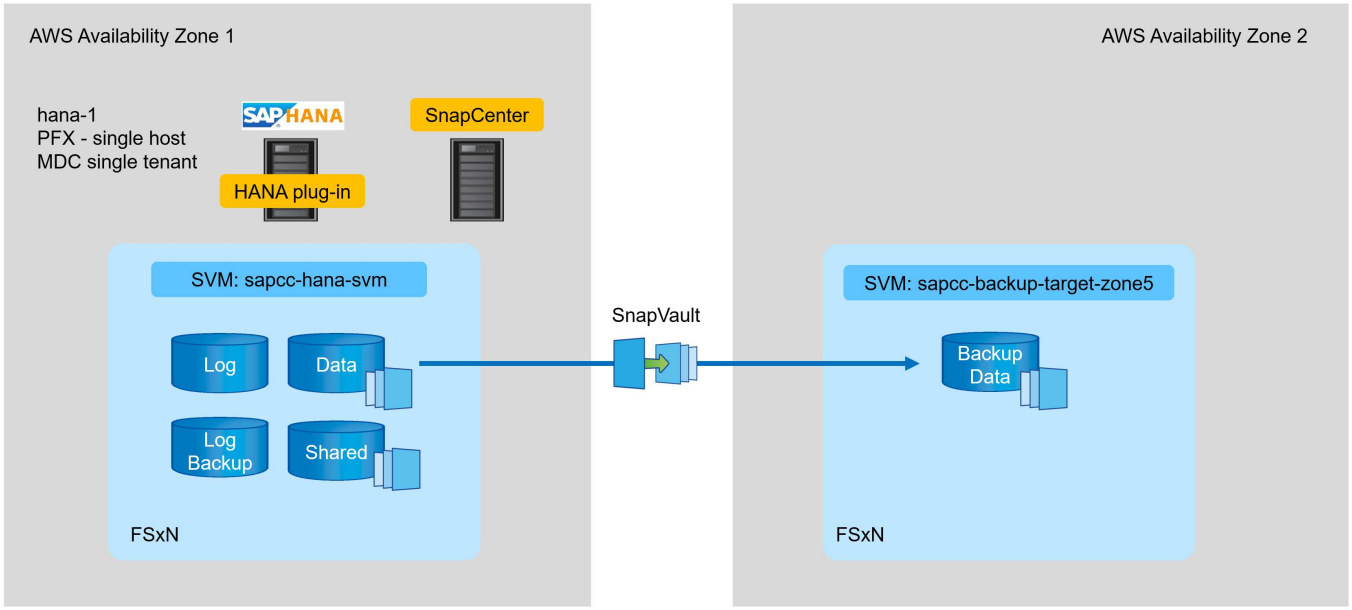

Job Details
Restore 'hana-1\hana\MDC\PFX'
Restore 'hana-1\hana\MDC\PFX'
hana-1
Restore
Validate Plugin Parameters
Pre Restore Application
Stopping HANA instance
Filesystem Pre Restore
Restore Filesystem
Filesystem Post Restore
Recover Application
Recovering system database
Checking HDB services status
Recovering tenant database 'PFX'
Starting HANA instance
Clear Catalog on Server
Application Clean-Up
Data Collection
Agent Finalize Workflow
Task Name: Recover Application Start Time: 02/23/2022 2:07:31 PM End Time:
View Logs
Cancel Job
Close

Backup replication with SnapVault

Overview - Backup replication with SnapVault

In our lab setup, we use a second FSX for ONTAP file system in a second AWS availability zone to showcase the backup replication for the HANA data volume.

As discussed in chapter "Data protection strategy", the replication target must be a second FSx for ONTAP file system in another availability zone to be protected from a failure of the primary FSx for ONTAP file system. Also, the HANA shared volume should be replicated to the secondary FSx for ONTAP file system.



Overview of configuration steps

There are a couple of configuration steps that you must execute on the FSx for ONTAP layer. You can do this either with NetApp Cloud Manager or the FSx for ONTAP command line.

1. Peer FSx for ONTAP file systems. FSx for ONTAP file systems must be peered to allow replication between each other.
2. Peer SVMs. SVMs must be peered to allow replication between each other.
3. Create a target volume. Create a volume at the target SVM with volume type `DP`. Type `DP` is required to be used as a replication target volume.
4. Create a SnapMirror policy. This is used to create a policy for replication with type `vault`.
    a. Add a rule to policy. The rule contains the SnapMirror label and the retention for backups at the secondary site. You must configure the same SnapMirror label later in the SnapCenter policy so that SnapCenter creates Snapshot backups at the source volume containing this label.
5. Create a SnapMirror relationship. Defines the replication relationship between the source and target volume and attaches a policy.
6. Initialize SnapMirror. This starts the initial replication in which the complete source data is transferred to the target volume.

When volume replication configuration is complete, you must configure the backup replication in SnapCenter

as follows:

1. Add the target SVM to SnapCenter.
2. Create a new SnapCenter policy for Snapshot backup and SnapVault replication.
3. Add the policy to HANA resource protection.
4. You can now execute backups with the new policy.

The following chapters describe the individual steps in more detail.

Configure replication relationships on FSx for ONTAP file systems

You can find additional information about SnapMirror configuration options in the ONTAP documentation at SnapMirror replication workflow (netapp.com).

- Source FSx for ONTAP file system: `FsxId00fa9e3c784b6abbb`
- Source SVM: `sapcc-hana-svm`
- Target FSx for ONTAP file system: `FsxId05f7f00af49dc7a3e`
- Target SVM: `sapcc-backup-target-zone5`

Peer FSx for ONTAP file systems

```
FsxId00fa9e3c784b6abbb::> network interface show -role intercluster
            Logical    Status     Network            Current       Current
Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ ------------- -------
----
FsxId00fa9e3c784b6abbb
            inter_1      up/up    10.1.1.57/24
FsxId00fa9e3c784b6abbb-01
                                                                   e0e
true
            inter_2      up/up    10.1.2.7/24
FsxId00fa9e3c784b6abbb-02
                                                                   e0e
true
2 entries were displayed.
```

```
FsxId05f7f00af49dc7a3e::> network interface show -role intercluster
            Logical    Status     Network            Current       Current
Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ ------------- -------
----
FsxId05f7f00af49dc7a3e
            inter_1      up/up    10.1.2.144/24
FsxId05f7f00af49dc7a3e-01
                                                                   e0e
true
            inter_2      up/up    10.1.2.69/24
FsxId05f7f00af49dc7a3e-02
                                                                   e0e
true
2 entries were displayed.
```

```
FsxId05f7f00af49dc7a3e::> cluster peer create -address-family ipv4 -peer
-addrs 10.1.1.57, 10.1.2.7
Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters. To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.
Enter the passphrase:
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command
in the other cluster.
```

`peer-addrs` are cluster IPs of the destination cluster.

```
FsxId00fa9e3c784b6abbb::>  cluster peer create -address-family ipv4 -peer
-addrs  10.1.2.144, 10.1.2.69
Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters. To ensure the authenticity of the peering relationship, use a
        phrase or sequence of characters that would be hard to guess.
Enter the passphrase:
Confirm the passphrase:
FsxId00fa9e3c784b6abbb::>
FsxId00fa9e3c784b6abbb::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
FsxId05f7f00af49dc7a3e    1-80-000011           Available      ok
```

Peer SVMs

```
FsxId05f7f00af49dc7a3e::> vserver peer create -vserver sapcc-backup-
target-zone5 -peer-vserver sapcc-hana-svm -peer-cluster
FsxId00fa9e3c784b6abbb -applications snapmirror
Info: [Job 41] 'vserver peer create' job queued
```

```
FsxId00fa9e3c784b6abbb::> vserver peer accept -vserver sapcc-hana-svm
-peer-vserver sapcc-backup-target-zone5
Info: [Job 960] 'vserver peer accept' job queued
```

```
FsxId05f7f00af49dc7a3e::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
sapcc-backup-target-zone5
            peer-source-cluster
                        peered       FsxId00fa9e3c784b6abbb
                                                       snapmirror
sapcc-hana-svm
```

Create a target volume

You must create the target volume with the type `DP` to flag it as a replication target.

```
FsxId05f7f00af49dc7a3e::> volume create -vserver sapcc-backup-target-zone5
-volume PFX_data_mnt00001 -aggregate aggr1 -size 100GB -state online
-policy default -type DP -autosize-mode grow_shrink -snapshot-policy none
-foreground true -tiering-policy all -anti-ransomware-state disabled
[Job 42] Job succeeded: Successful
```

Create a SnapMirror policy

The SnapMirror policy and the added rule define the retention and the Snapmirror label to identify Snapshots that should be replicated. When creating the SnapCenter policy later, you must use the same label.

```
FsxId05f7f00af49dc7a3e::> snapmirror policy create -policy snapcenter-
policy -tries 8 -transfer-priority normal -ignore-atime false -restart
always -type vault -vserver sapcc-backup-target-zone5
```

```
FsxId05f7f00af49dc7a3e::> snapmirror policy add-rule -vserver sapcc-
backup-target-zone5  -policy snapcenter-policy -snapmirror-label
snapcenter -keep 14
```

```
FsxId00fa9e3c784b6abbb::> snapmirror policy showVserver Policy
Policy Number         Transfer
Name    Name               Type   Of Rules Tries Priority Comment
------- ------------------ ------ -------- ----- -------- ----------
FsxId00fa9e3c784b6abbb
        snapcenter-policy  vault         1     8  normal  -
  SnapMirror Label: snapcenter                          Keep:      14
                                                  Total Keep:      14
```

Create SnapMirror relationship

Now the relation between the source and target volume is defined as well as the type XDP and the policy we created earlier.

```
FsxId05f7f00af49dc7a3e::> snapmirror create -source-path sapcc-hana-
svm:PFX_data_mnt00001 -destination-path sapcc-backup-target-
zone5:PFX_data_mnt00001 -vserver sapcc-backup-target-zone5 -throttle
unlimited -identity-preserve false -type XDP -policy snapcenter-policy
Operation succeeded: snapmirror create for the relationship with
destination "sapcc-backup-target-zone5:PFX_data_mnt00001".
```

Initialize SnapMirror

With this command, the initial replication starts. This is a full transfer of all data from the source volume to the target volume.

```
FsxId05f7f00af49dc7a3e::> snapmirror initialize -destination-path sapcc-
backup-target-zone5:PFX_data_mnt00001 -source-path sapcc-hana-
svm:PFX_data_mnt00001
Operation is queued: snapmirror initialize of destination "sapcc-backup-
target-zone5:PFX_data_mnt00001".
```

You can check the status of the replication with the `snapmirror show` command.

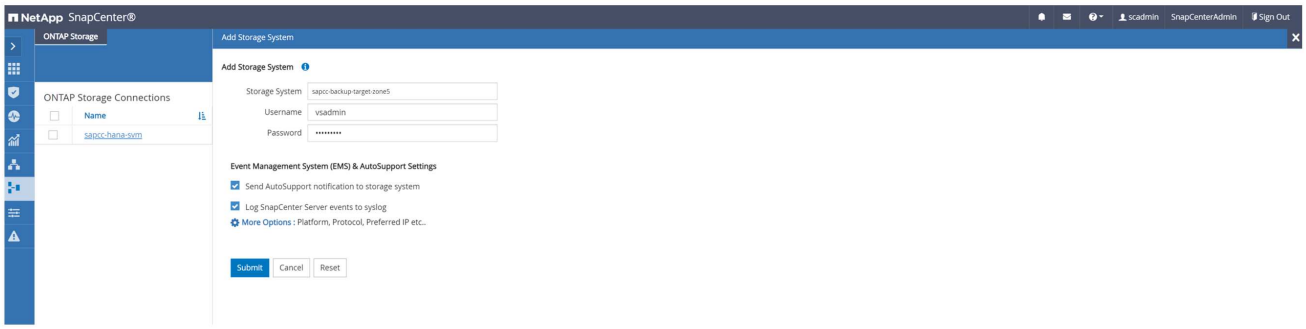
```
FsxId05f7f00af49dc7a3e::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
sapcc-hana-svm:PFX_data_mnt00001
            XDP  sapcc-backup-target-zone5:PFX_data_mnt00001
                             Uninitialized
                                     Transferring   1009MB    true
02/24 12:34:28
```

```
FsxId05f7f00af49dc7a3e::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
sapcc-hana-svm:PFX_data_mnt00001
            XDP  sapcc-backup-target-zone5:PFX_data_mnt00001
                             Snapmirrored
                                     Idle           -         true    -
```

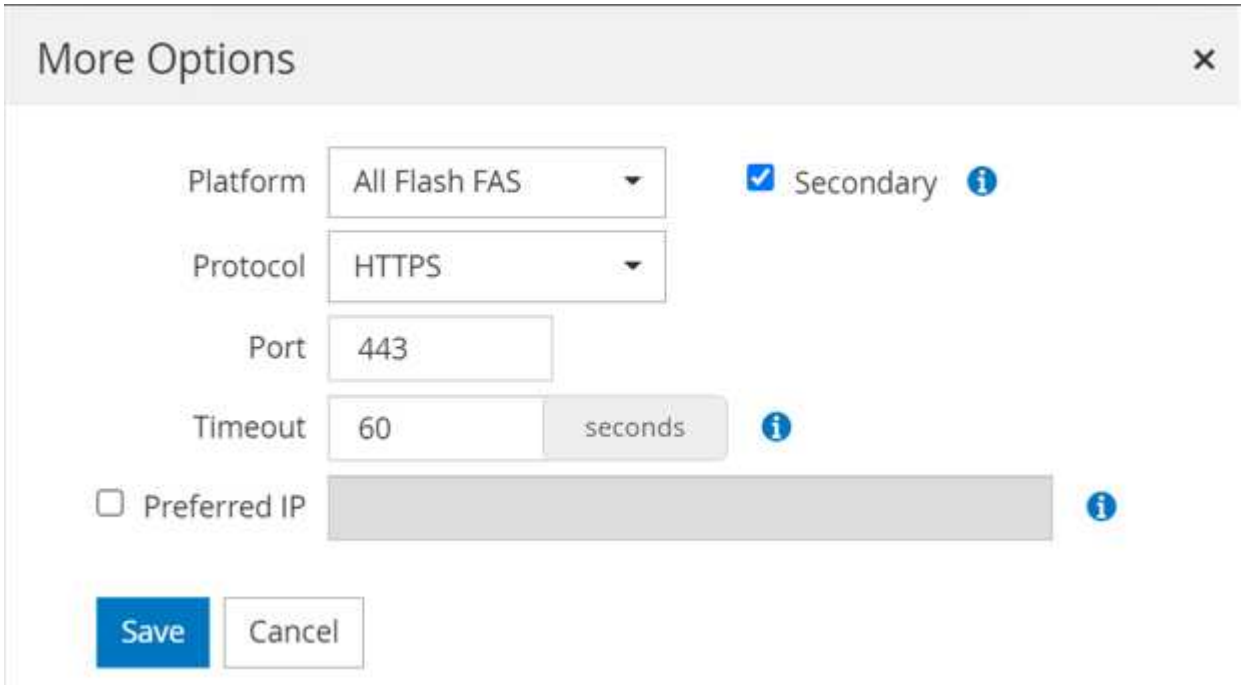
Add a backup SVM to SnapCenter

To add a backup SVM to SnapCenter, follow these steps:

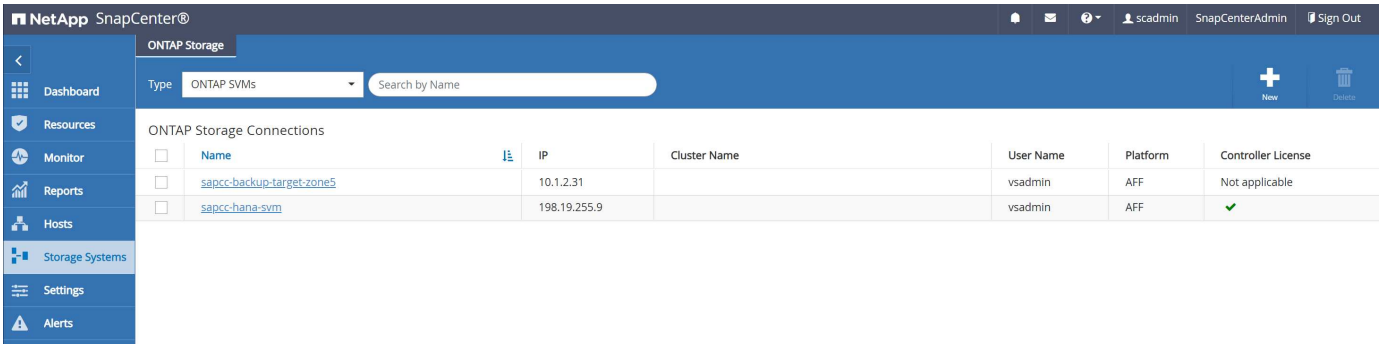
1. Configure the SVM where the SnapVault target volume is located in SnapCenter.



2. On the More Options window, select All Flash FAS as the platform and select Secondary.



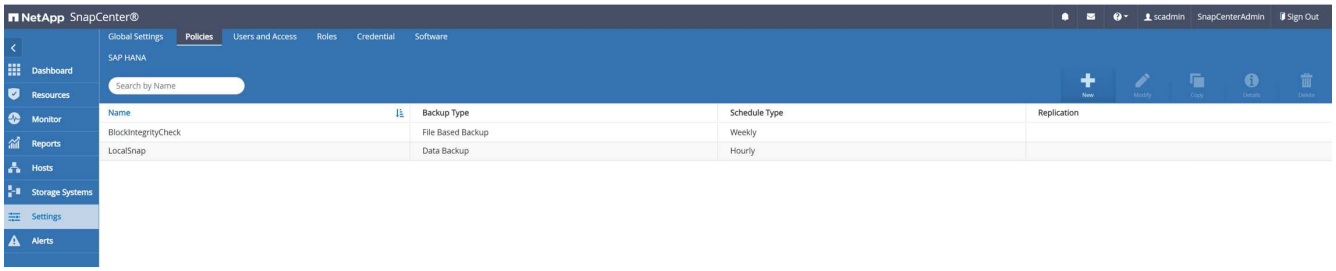
The SVM is now available in SnapCenter.



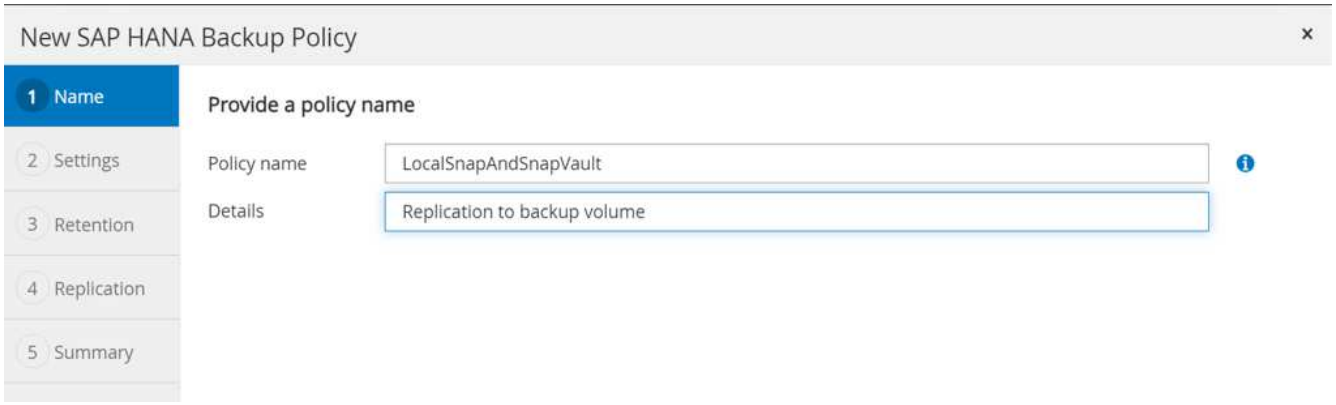
Create a new SnapCenter policy for backup replication

You must configure a policy for the backup replication as follows:

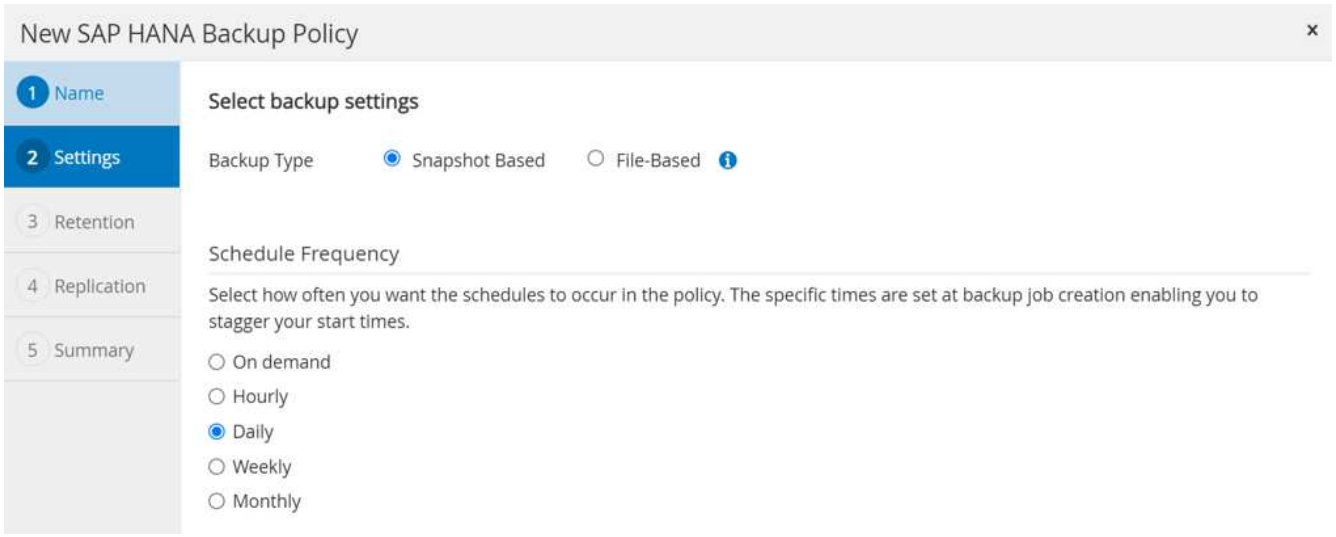
1. Provide a name for the policy.



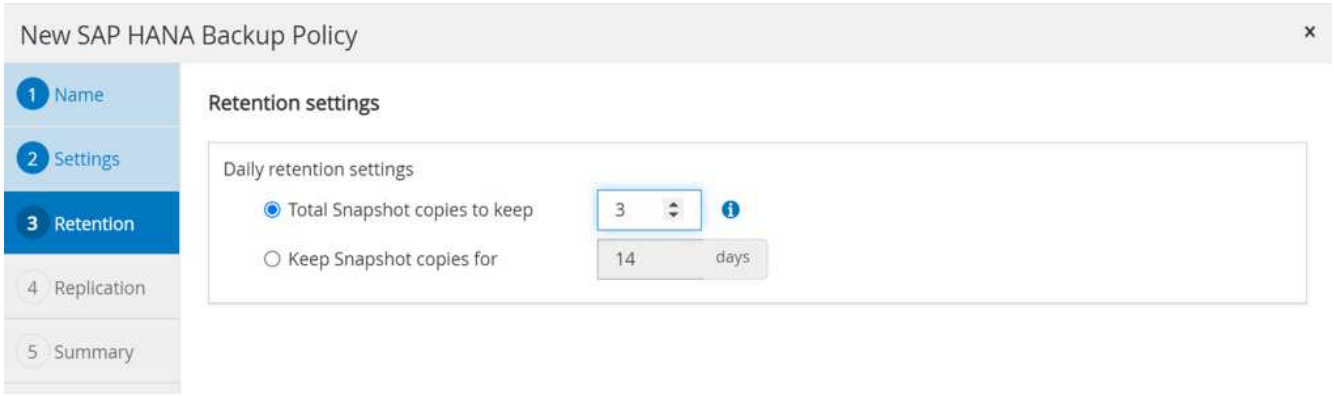
2. Select Snapshot backup and a schedule frequency. Daily is typically used for backup replication.



3. Select the retention for the Snapshot backups.

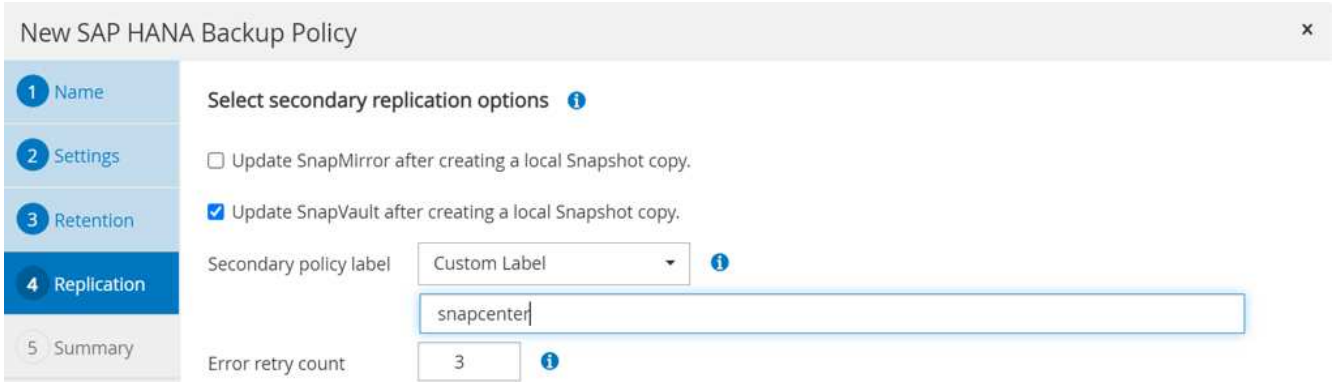


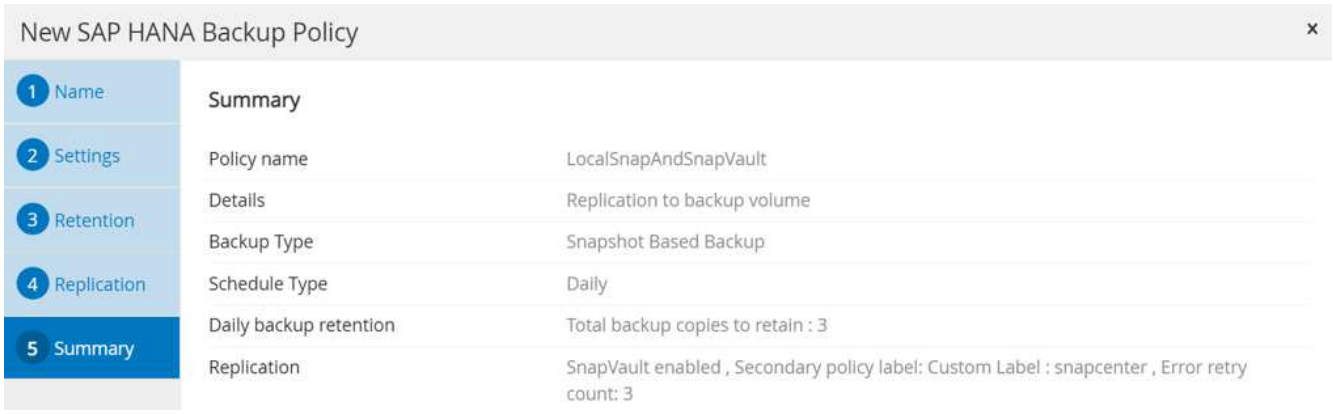
This is the retention for the daily Snapshot backups taken at the primary storage. The retention for secondary backups at the SnapVault target has already been configured previously using the add rule command at the ONTAP level. See “Configure replication relationships on FSx for ONTAP file systems” (xref).



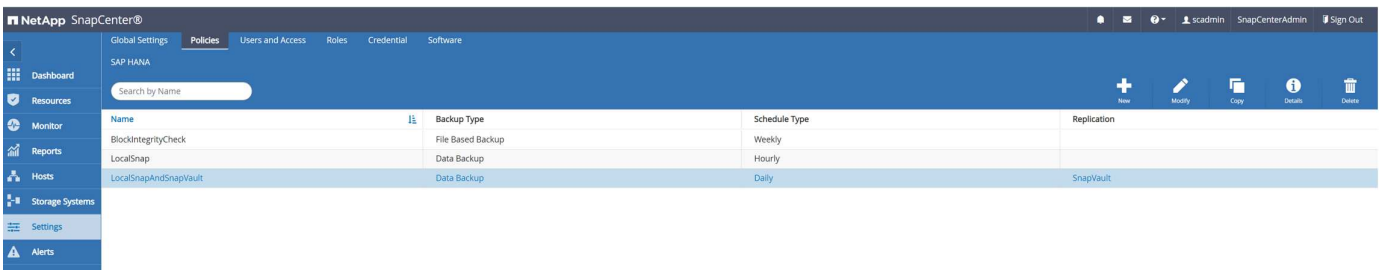
4. Select the Update SnapVault field and provide a custom label.

   This label must match the SnapMirror label provided in the `add rule` command at ONTAP level.



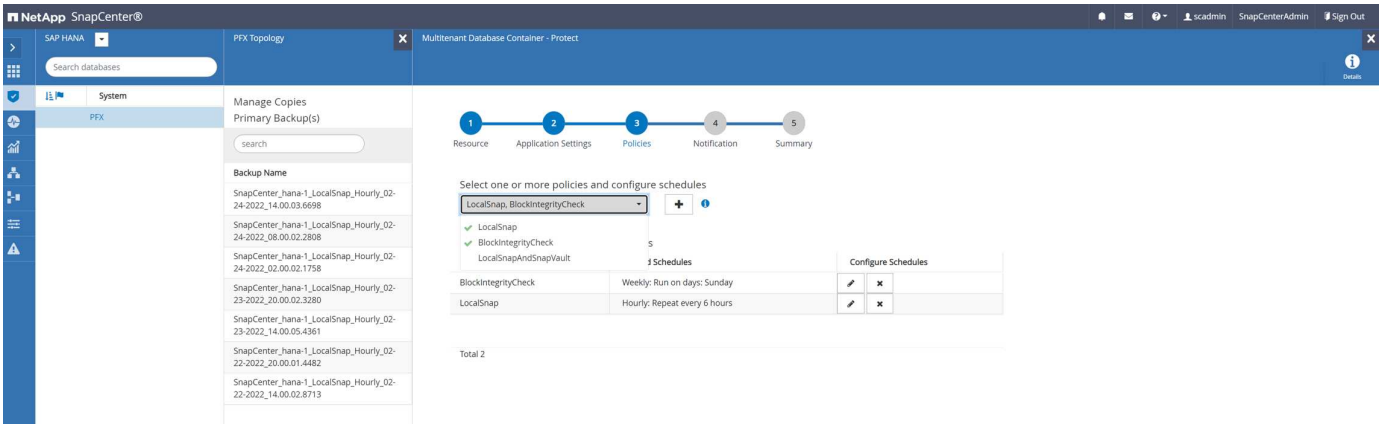


The new SnapCenter policy is now configured.

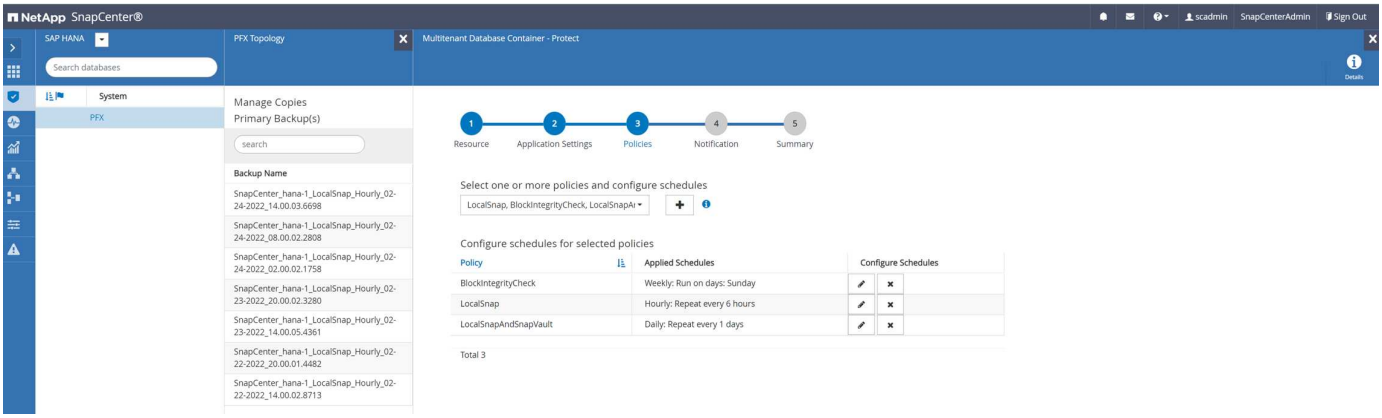


Add a policy to resource protection

You must add the new policy to the HANA resource protection configuration, as shown in the following figure.



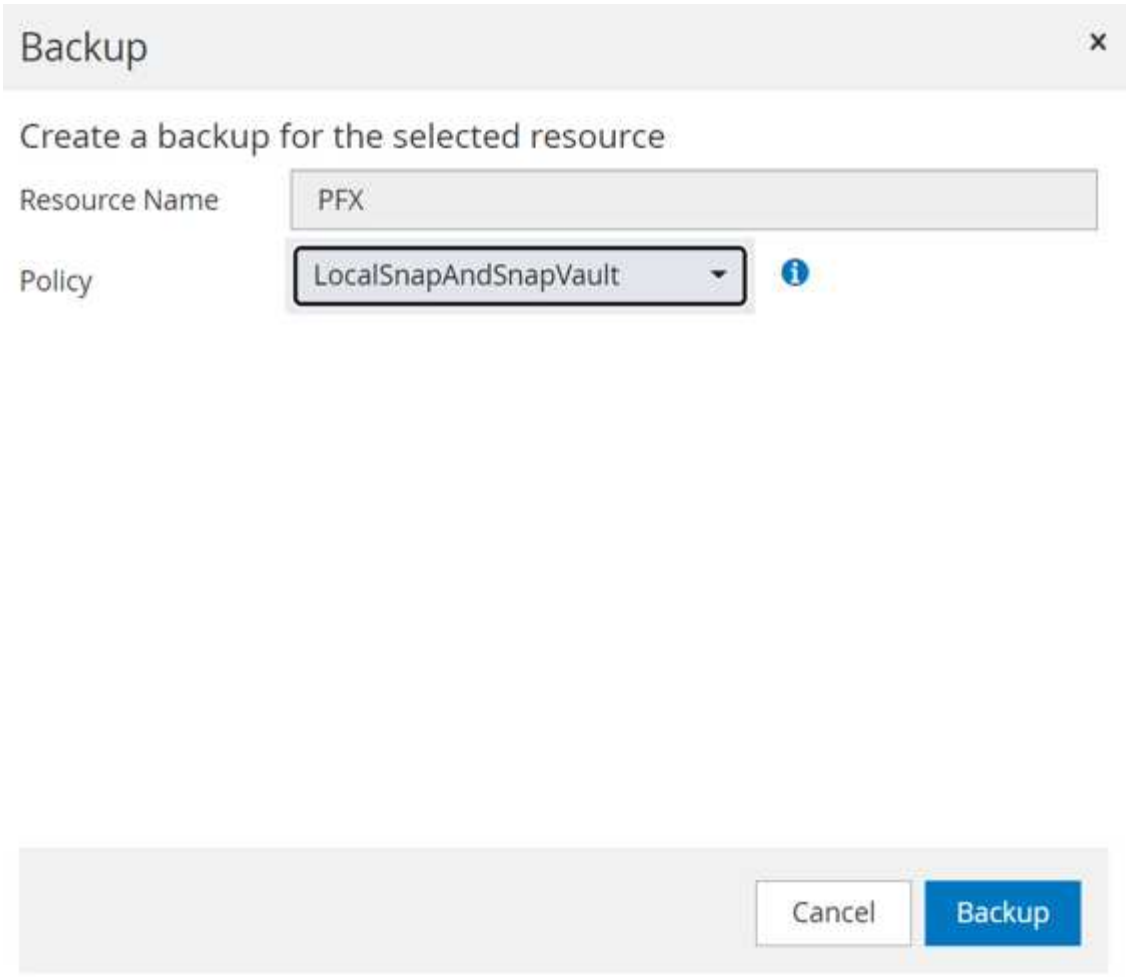
A daily schedule is defined in our setup.



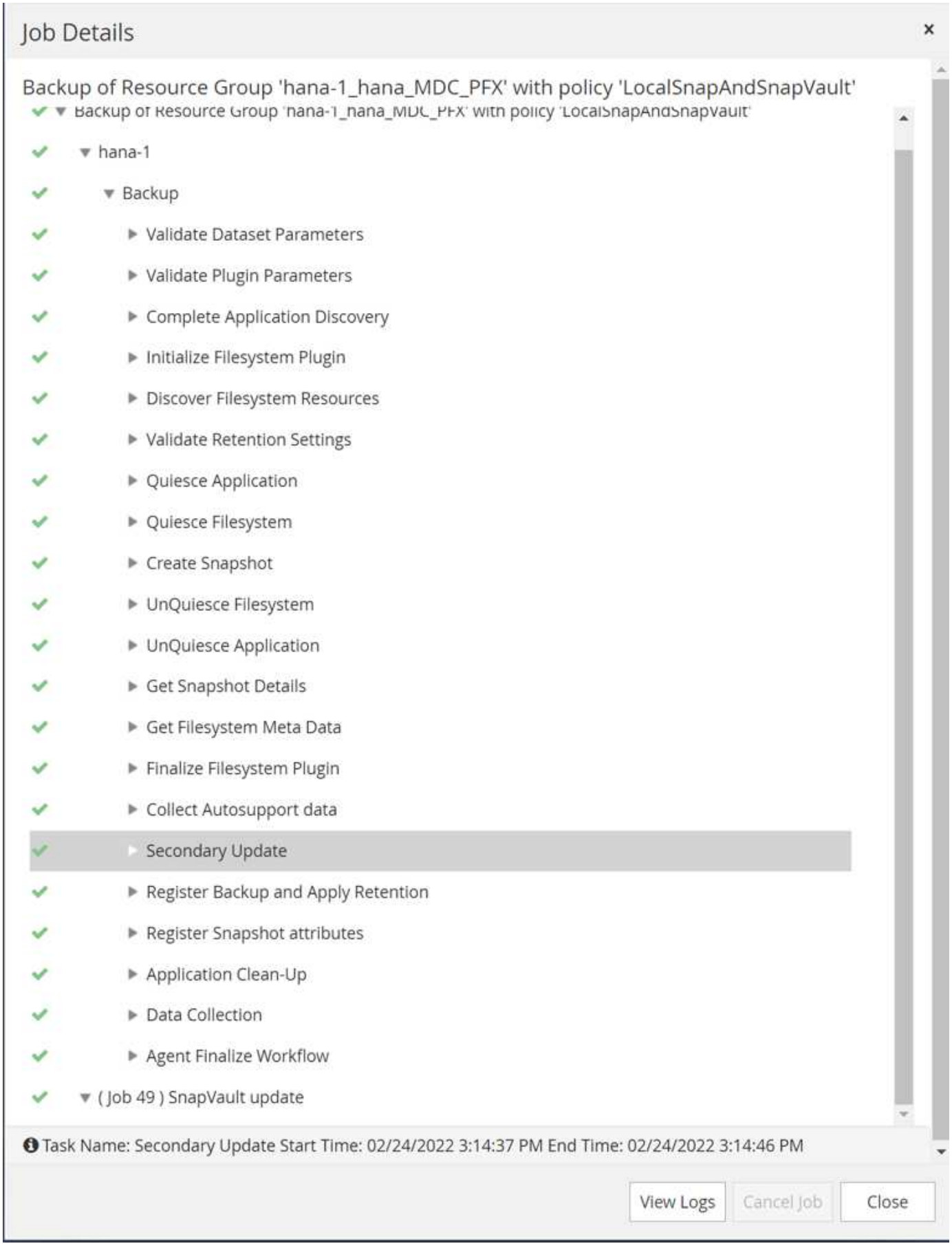
Create a backup with replication

A backup is created in the same way as with a local Snapshot copy.

To create a backup with replication, select the policy that includes the backup replication and click Backup.



Within the SnapCenter job log, you can see the Secondary Update step, which initiates a SnapVault update operation. Replication changed blocks from the source volume to the target volume.



On the FSx for ONTAP file system, a Snapshot on the source volume is created using the SnapMirror label,

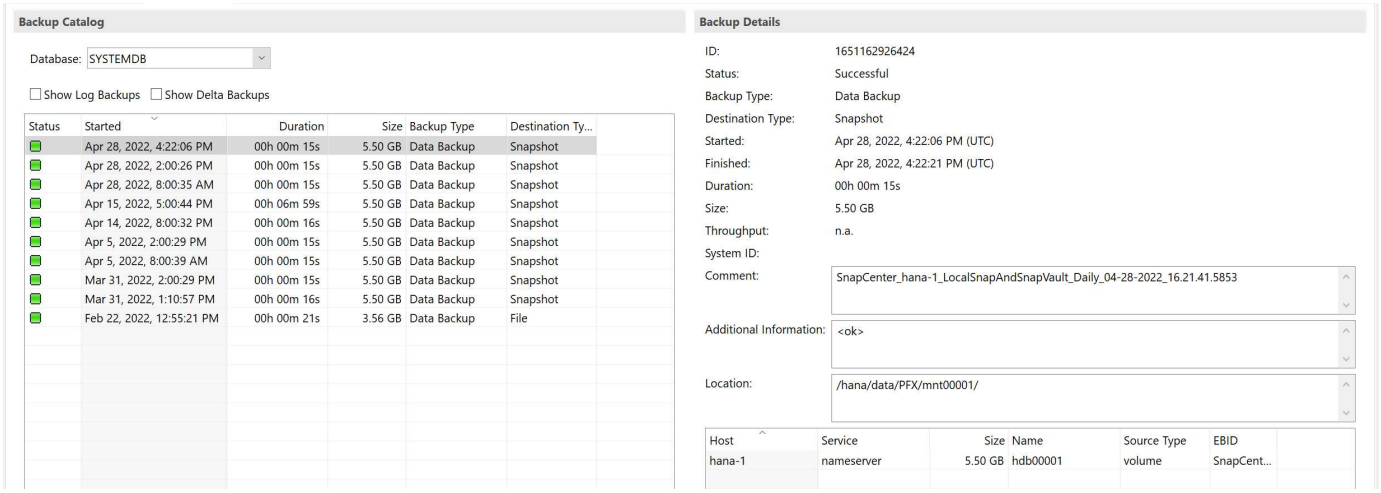
`snapcenter`, as configured in the SnapCenter policy.

```
FsxId00fa9e3c784b6abbb::> snapshot show -vserver sapcc-hana-svm -volume
PFX_data_mnt00001 -fields snapmirror-label
vserver        volume            snapshot
snapmirror-label
-------------- -----------------
-------------------------------------------------------------
----------------
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_03-31-
2022_13.10.26.5482 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_03-31-
2022_14.00.05.2023 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-05-
2022_08.00.06.3380 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-05-
2022_14.00.01.6482 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-14-
2022_20.00.05.0316 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-28-
2022_08.00.06.3629 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-1_LocalSnap_Hourly_04-28-
2022_14.00.01.7275 -
sapcc-hana-svm PFX_data_mnt00001 SnapCenter_hana-
1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853

snapcenter
8 entries were displayed.
```

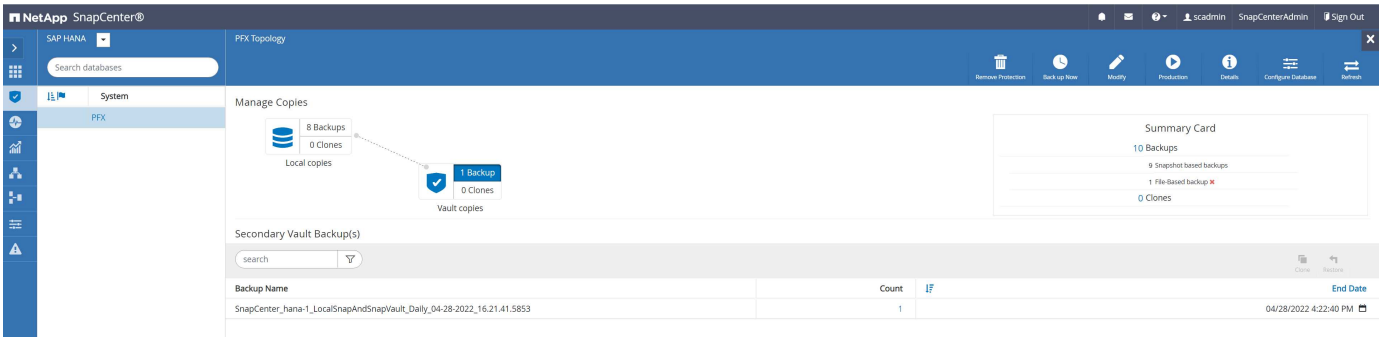
At the target volume, a Snapshot copy with the same name is created.

```
FsxId05f7f00af49dc7a3e::> snapshot show -vserver sapcc-backup-target-zone5
-volume PFX_data_mnt00001 -fields snapmirror-label
vserver                  volume           snapshot
snapmirror-label
------------------------ -----------------
-------------------------------------------------------------------------
----------------
sapcc-backup-target-zone5 PFX_data_mnt00001 SnapCenter_hana-
1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853 snapcenter
FsxId05f7f00af49dc7a3e::>
```

The new Snapshot backup is also listed in the HANA backup catalog.



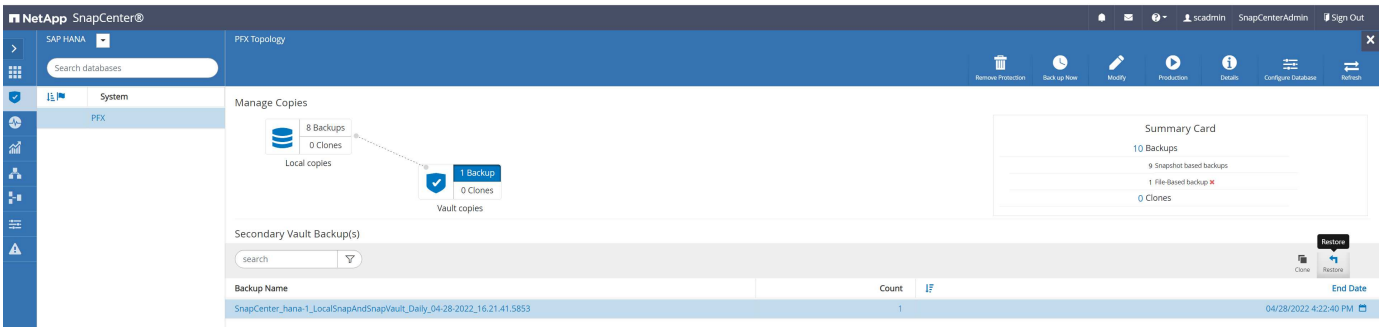
In SnapCenter, you can list the replicated backups by clicking Vault Copies in the topology view.



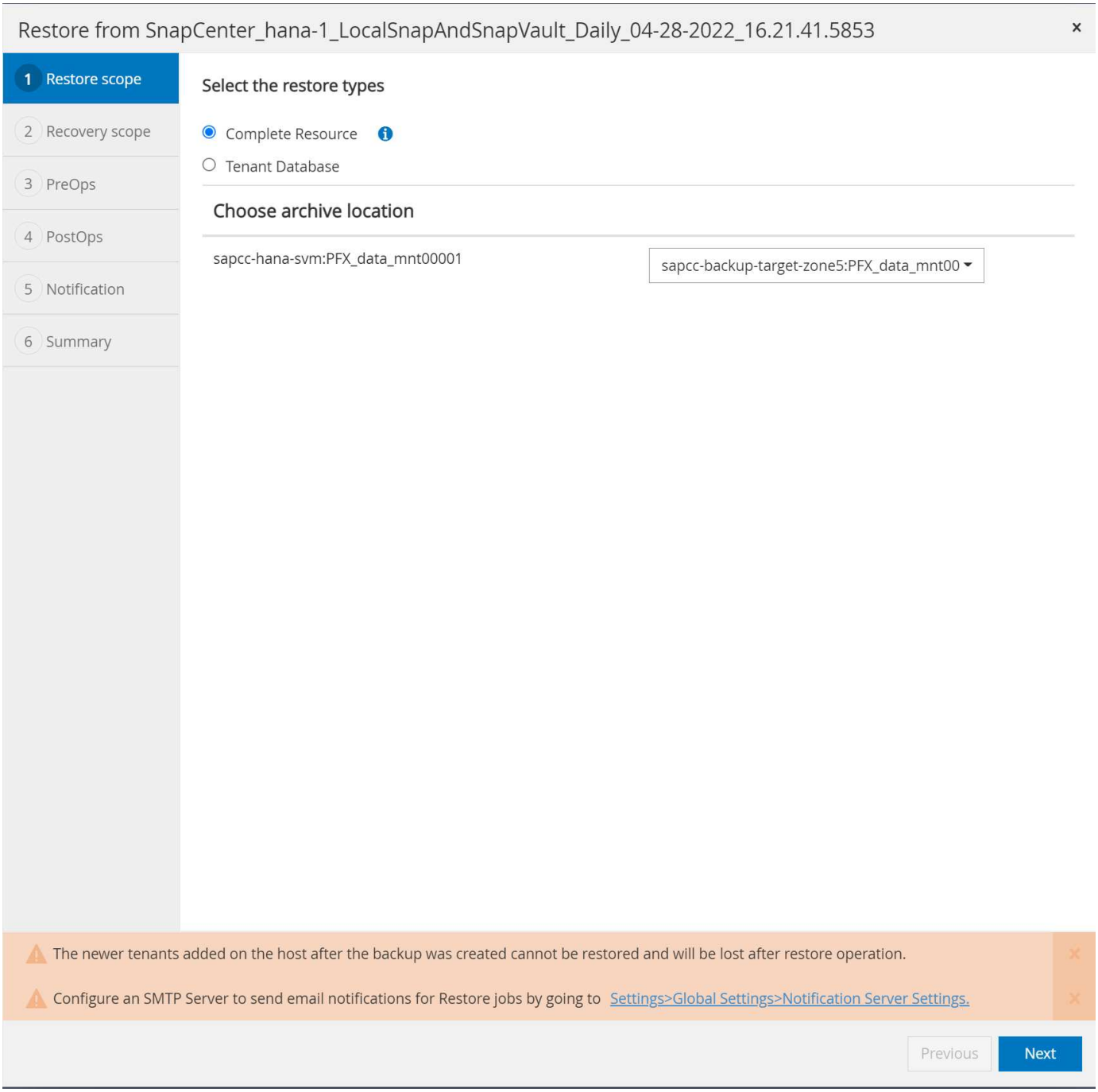
Restore and recover from secondary storage

To restore and recover from secondary storage, follow these steps:

To retrieve the list of all the backups on the secondary storage, in the SnapCenter Topology view, click Vault Copies, then select a backup and click Restore.



The restore dialog shows the secondary locations.



Further restore and recovery steps are identical to those previously covered for a Snapshot backup at the primary storage.

Where to find additional information

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

- FSx for NetApp ONTAP user guide — What is Amazon FSx for NetApp ONTAP?

  https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html

- 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 HANA System Copy and Clone Operations with SnapCenter

  https://www.netapp.com/pdf.html?item=/media/17111-tr4667.pdf

- TR-4719: SAP HANA System Replication — Backup and Recovery with SnapCenter

  https://docs.netapp.com/us-en/netapp-solutions-sap/backup/saphana-sr-scs-sap-hana-system-replication-overview.html

SAP HANA backup and recovery with SnapCenter

TR-4614: SAP HANA backup and recovery with SnapCenter

Nils Bauer, NetApp

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.

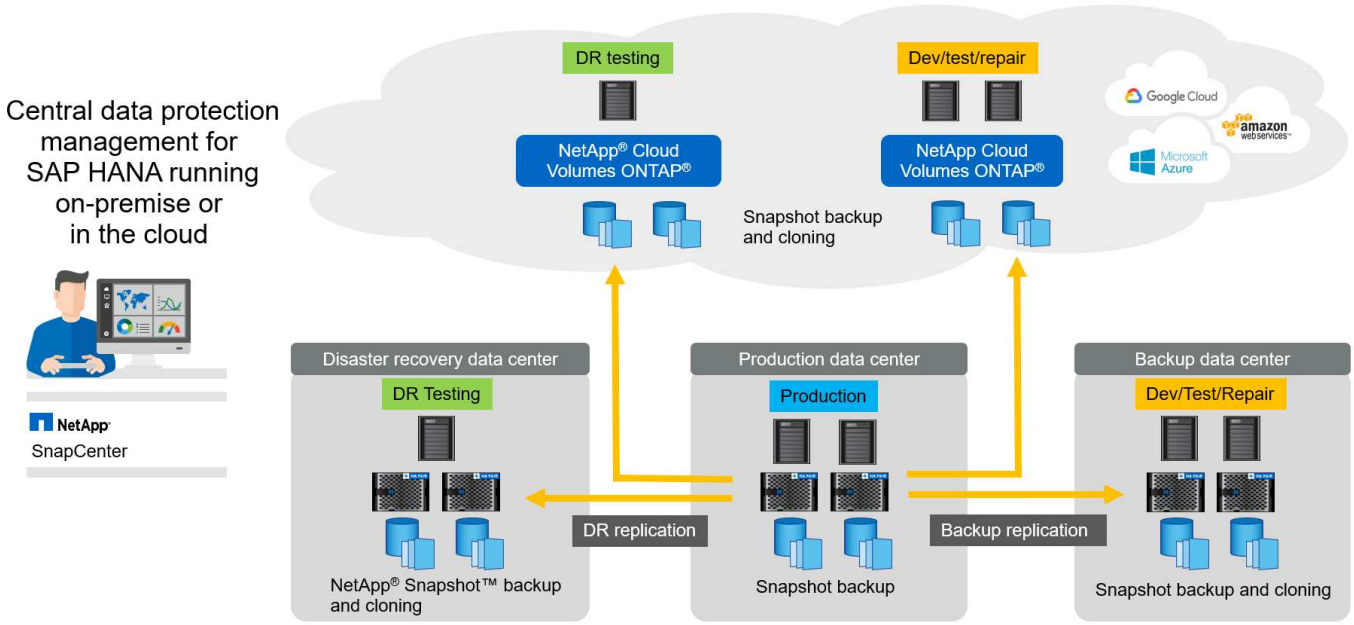
Snapshot copies also provide key advantages for restore and recovery operations. NetApp SnapRestore data recovery software enables the restore of an entire database or, alternatively, a portion of a database to any point in time, based on the available Snapshot copies. Such restore processes are finished 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.

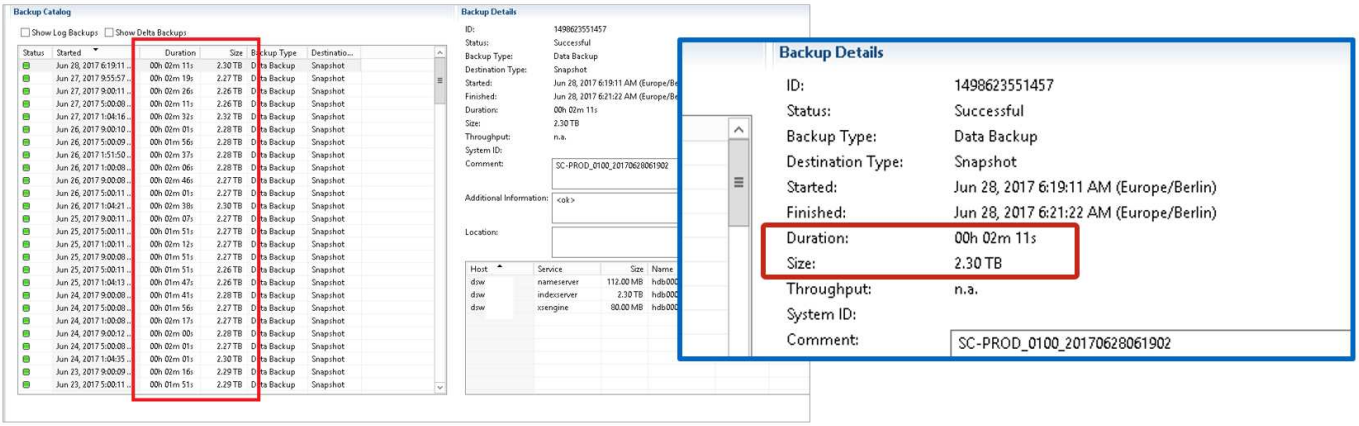
The solution can also be seamlessly extended to a hybrid cloud operation model. Data replication for disaster recovery or offsite backup purposes can be done from on-premises NetApp ONTAP systems to Cloud Volumes ONTAP instances running in the cloud. You can use SnapCenter as a central tool to manage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



Runtime of Snapshot backups

The next screenshot 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.

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.



Recovery time objective comparison

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

Time needed to restore database

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

size.

With storage Snapshot copy backups, the restore time is independent of the size of the database and is in the range of a couple of seconds when the restore can be performed from primary storage. A restore from secondary storage is only required in the case of a disaster when the primary storage is no longer available.

Time needed to start database

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

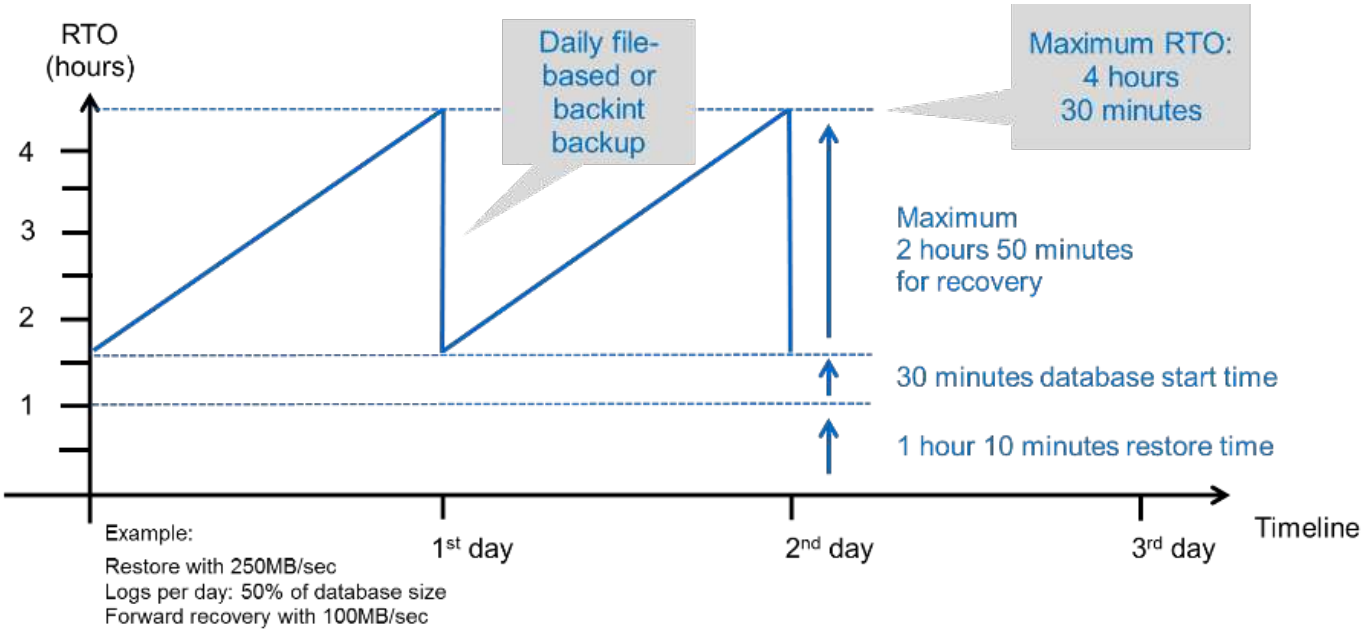
Time needed to recover database

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

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

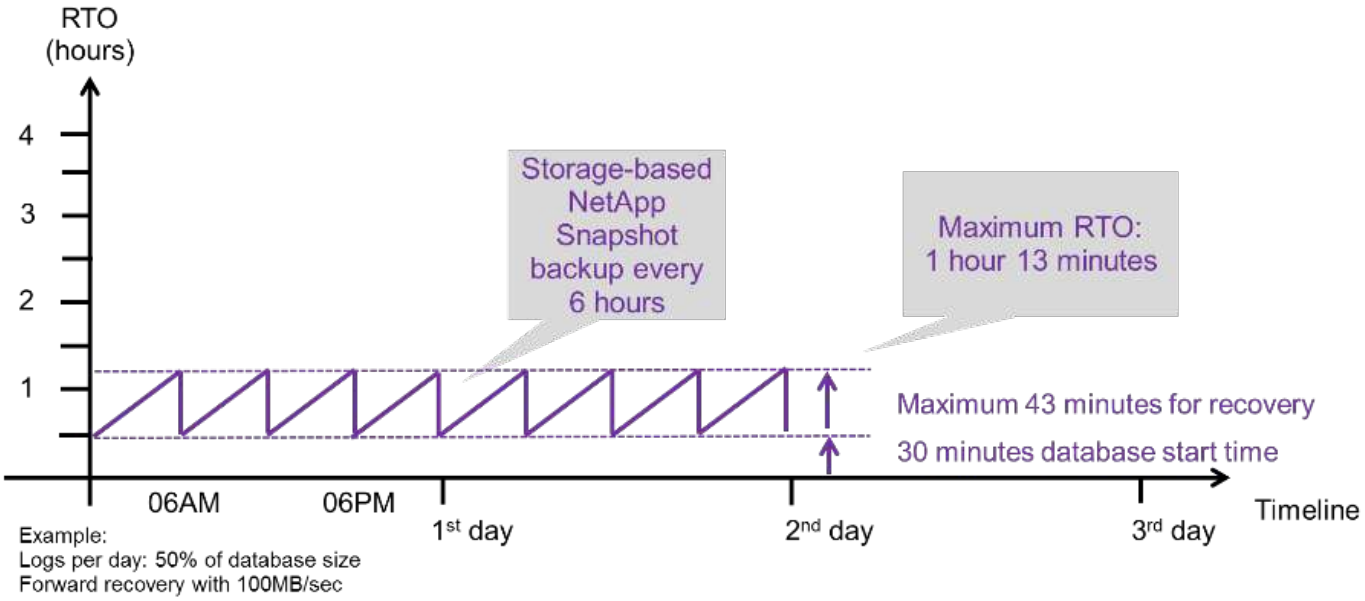
Storage Snapshot copy data backups are typically scheduled with a higher frequency because they do not influence the performance of the SAP HANA database. For example, if Snapshot copy backups are scheduled every six hours, the recovery time would be, in the worst case, one-fourth of the recovery time for a file-based backup (6 hours / 24 hours = ¼).

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



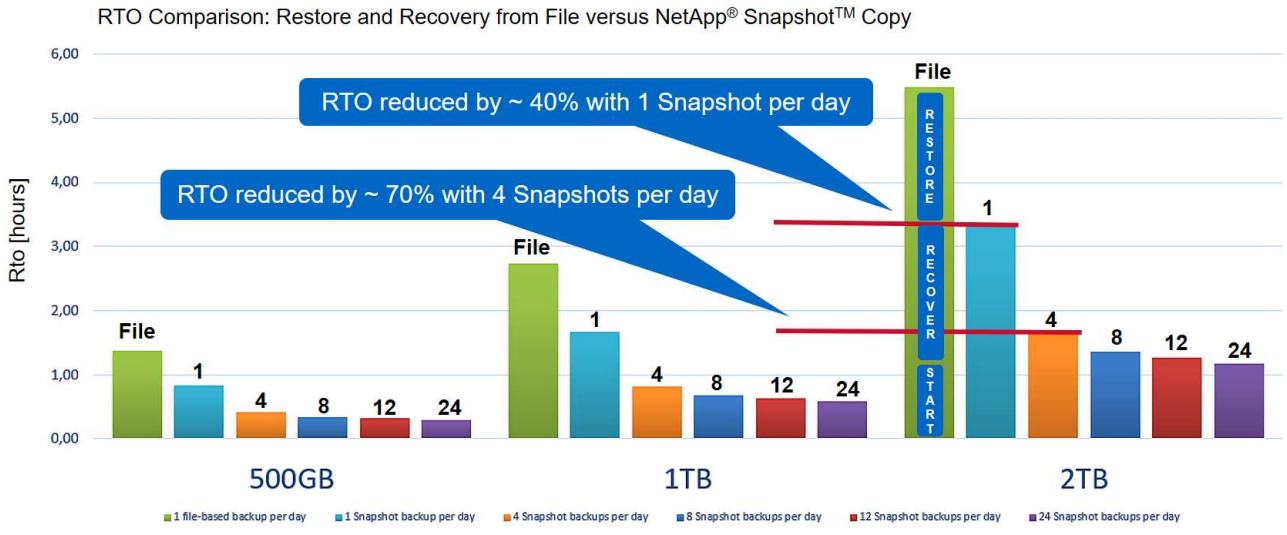
The following figure shows an RTO example for a 1TB database when Snapshot backups are used. With

storage-based Snapshot backups, the RTO only depends on the database start time and the forward recovery time because the restore is completed in a few seconds, independent of the size of the database. The forward recovery time also increases depending on when the restore and recovery are done, but due to the higher frequency of backups (every 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.



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

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



Assumptions: Restore from file with 250MB/sec; database start with 400MB/s; log files per day: 50% of database size; forward recovery with 250MB/sec

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

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

SnapCenter architecture

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.

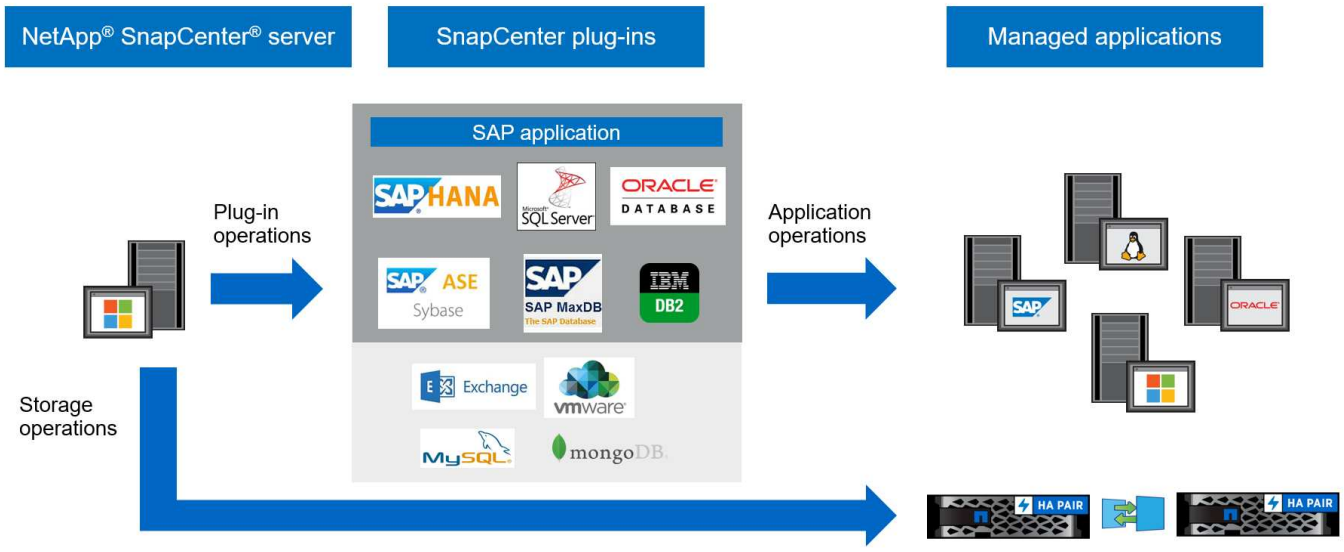
SnapCenter manages data across endpoints in the data fabric powered by NetApp. You can use SnapCenter to replicate data between on-premises environments; between on-premises environments and the cloud; and between private, hybrid, or public clouds.

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.

The following figure depicts SnapCenter components.



SnapCenter SAP HANA backup solution

This section lists the components, supported SAP HANA releases and configurations,

and SnapCenter 4.6 enhancements used in this 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
- Non-data 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
  - Non-data 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 non- data volumes using the SAP HANA plug-in with storage-based Snapshot copies. Non-data volumes can be scheduled independently from the database data backup to enable individual retention and protection policies.

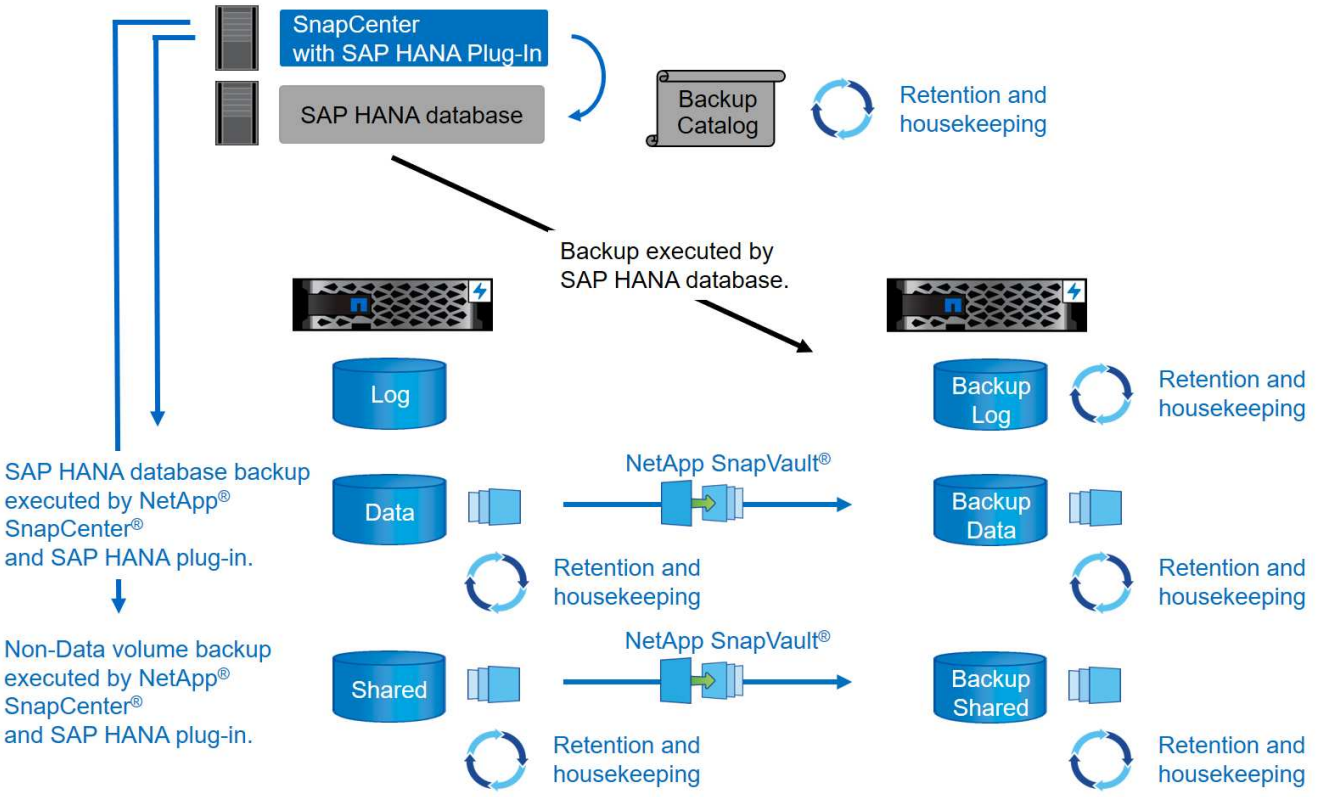
The SAP HANA database automatically executes log backups. Depending on the recovery point objectives, there are several options for the storage location of the log backups:

- 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.

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

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



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

1. Creation of a storage Snapshot copy of the non-data 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

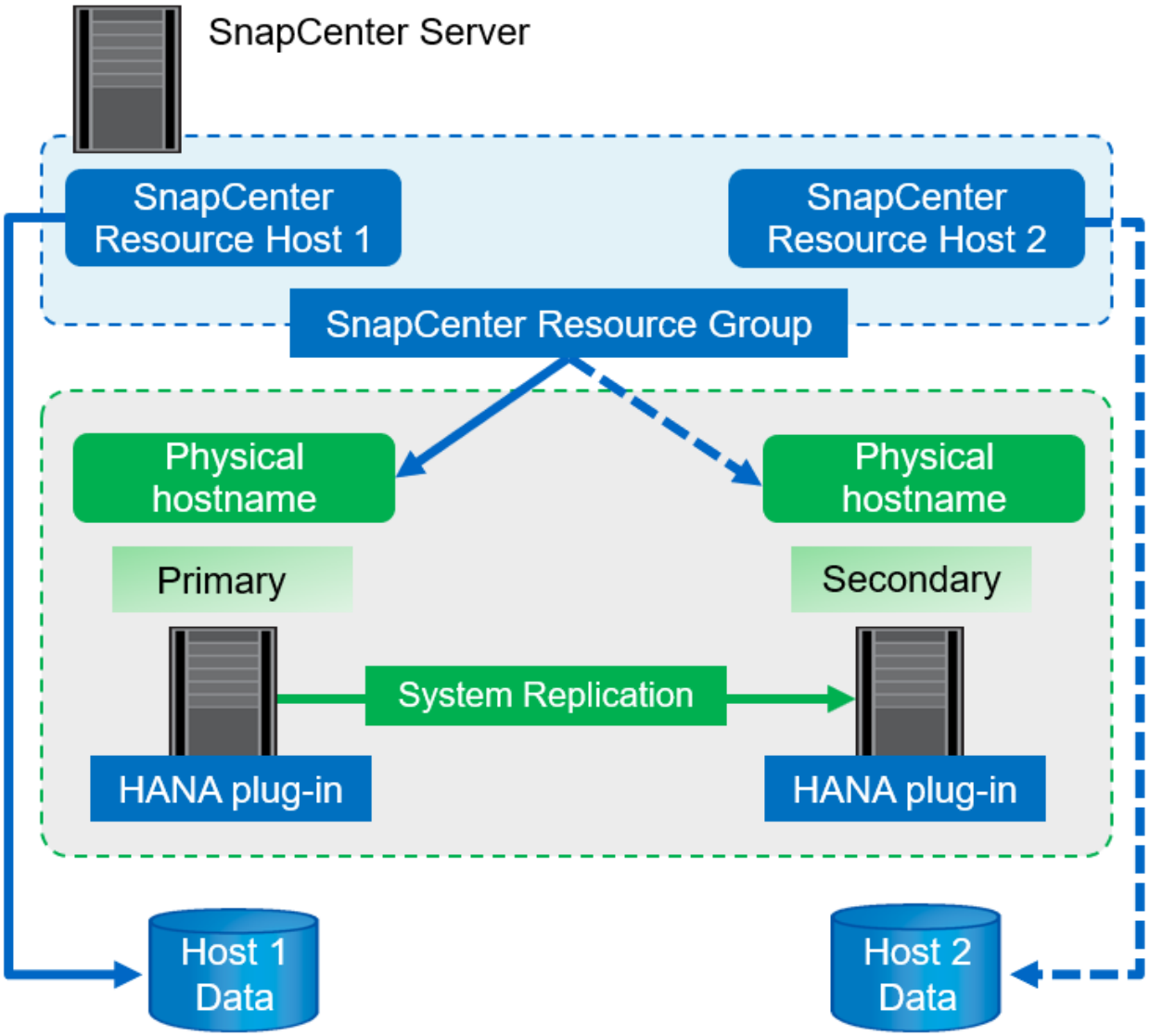
SnapCenter supports SAP HANA single-host and multiple-host configurations using NFS- or FC-attached NetApp storage systems (AFF and FAS), as well as SAP HANA systems running on Cloud Volumes ONTAP at AWS, Azure, the Google Cloud Platform, and AWS FSx ONTAP using NFS.

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 version 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, SnapCenter automatically identifies which host is primary or secondary, and it then executes the required backup operations accordingly. Retention management for Snapshot and file-based backups created with SnapCenter is performed across both hosts to ensure that old backups are also deleted at the current secondary host. The following figure shows a high-level overview. A detailed description of the configuration and operation of HANA System Replication-enabled HANA systems in SnapCenter can be found in TR-4719 SAP HANA System Replication, Backup and Recovery with SnapCenter.



SnapCenter concepts and best practices

This section describes SnapCenter concepts and best practices as they relate to SAP HANA resource configuration and deployment.

SAP HANA resource configuration options and concepts

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

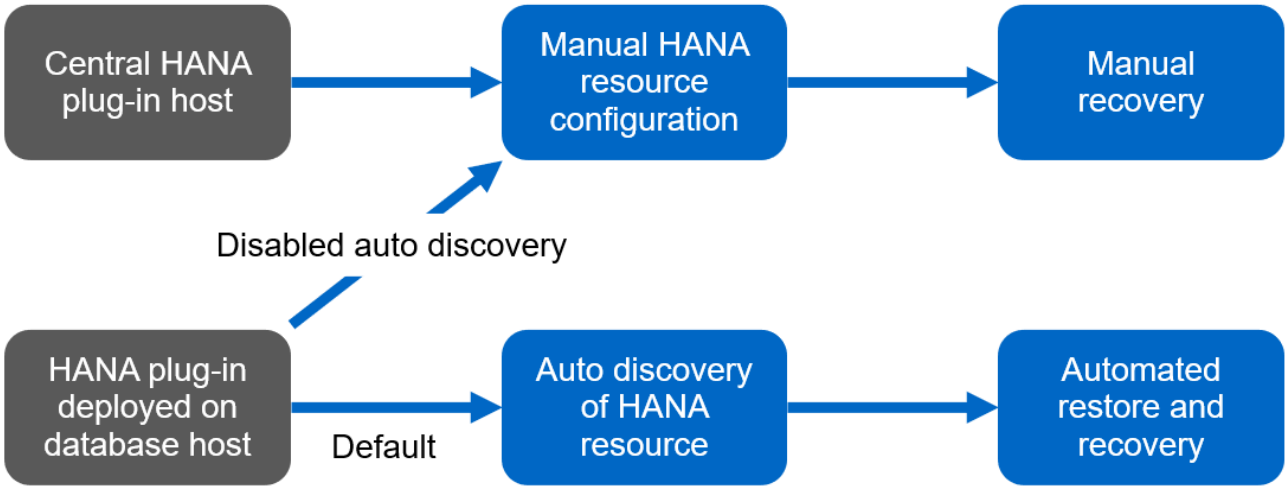
- **Manual resource configuration.** HANA resource and storage footprint information must be provided manually.
- **Automatic discovery of HANA resources.** Automatic discovery simplifies the configuration of HANA databases in SnapCenter and enables automated restore and recovery.

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 in which some HANA systems (HANA multiple host systems) require 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 prerequisite 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.

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



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.

The following table shows supported HANA configurations for automatic discovery.

HANA plug-in installed on:	HANA architecture	HANA system configuration	Infrastructure
HANA database host	Single host	• HANA single container • SAP HANA multitenant database containers (MDC) with single or multiple tenants • HANA System Replication	• Bare metal with NFS • Bare metal with XFS and FC with or without Linux Logical Volume Manager (LVM) • VMware with direct OS NFS mounts

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

Supported HANA architectures for manual HANA resource configuration

Manual configuration of HANA resources is supported for all HANA architectures; however, it 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.

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 section “Disable auto discovery on the HANA plug-in host.”

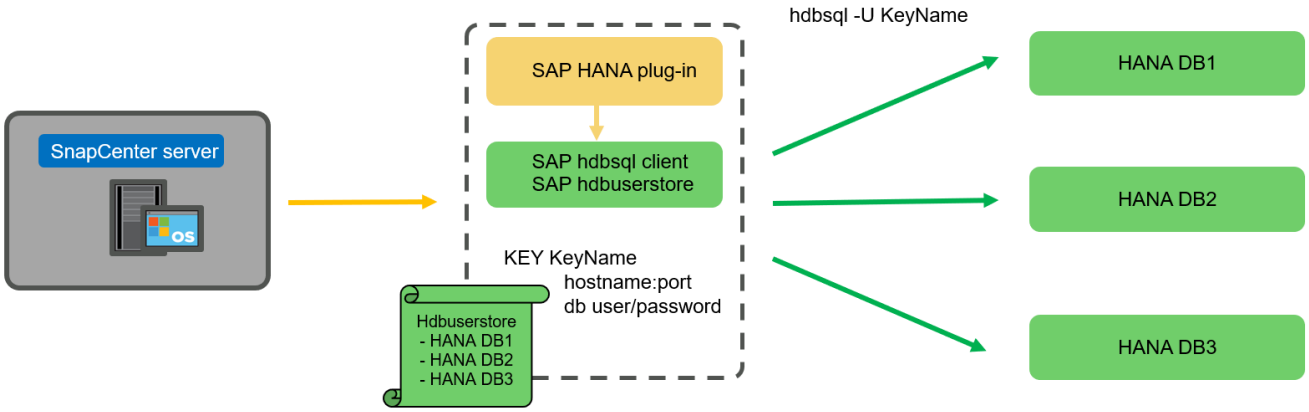
The following table shows supported HANA configurations for manual HANA resource configuration.

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	• HANA single container • HANA MDC with single or multiple tenants • HANA System Replication	• 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

The following figure 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.



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.

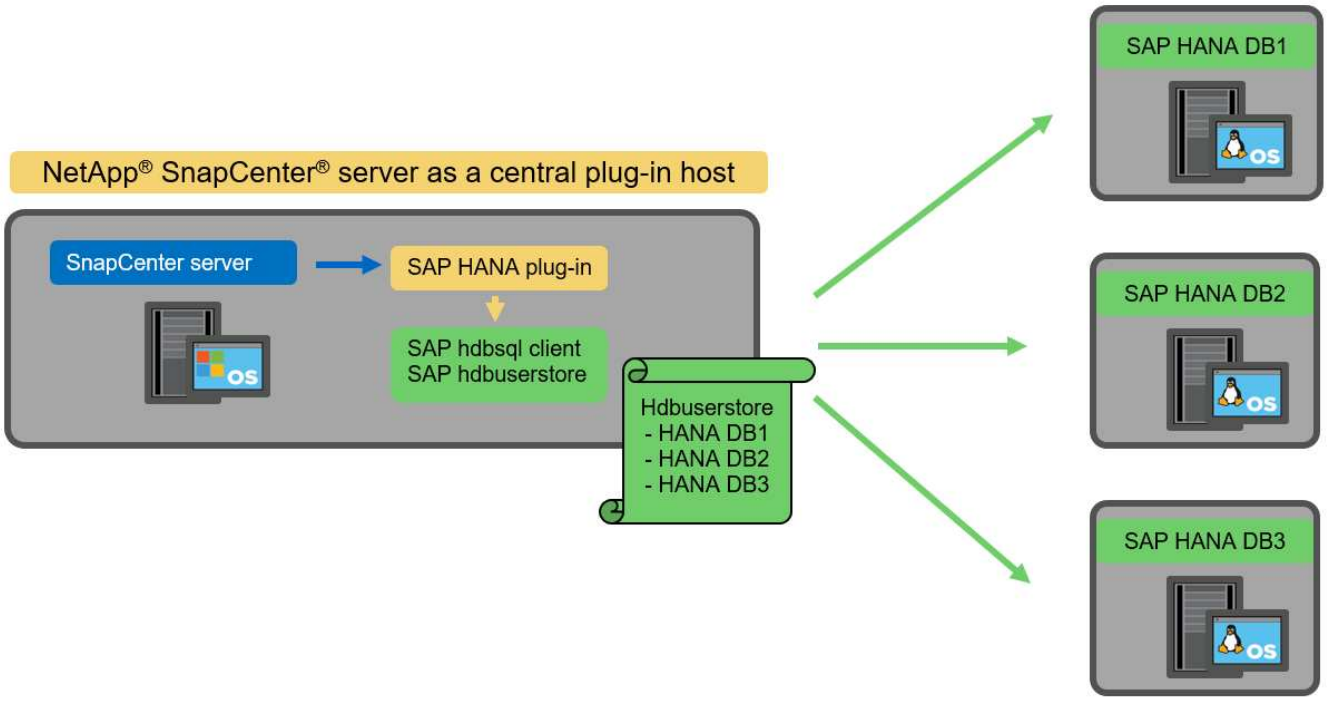
SnapCenter server high availability

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 this NetApp Knowledge Base page.

SnapCenter server as a central HANA plug-in host

The following figure 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.



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.

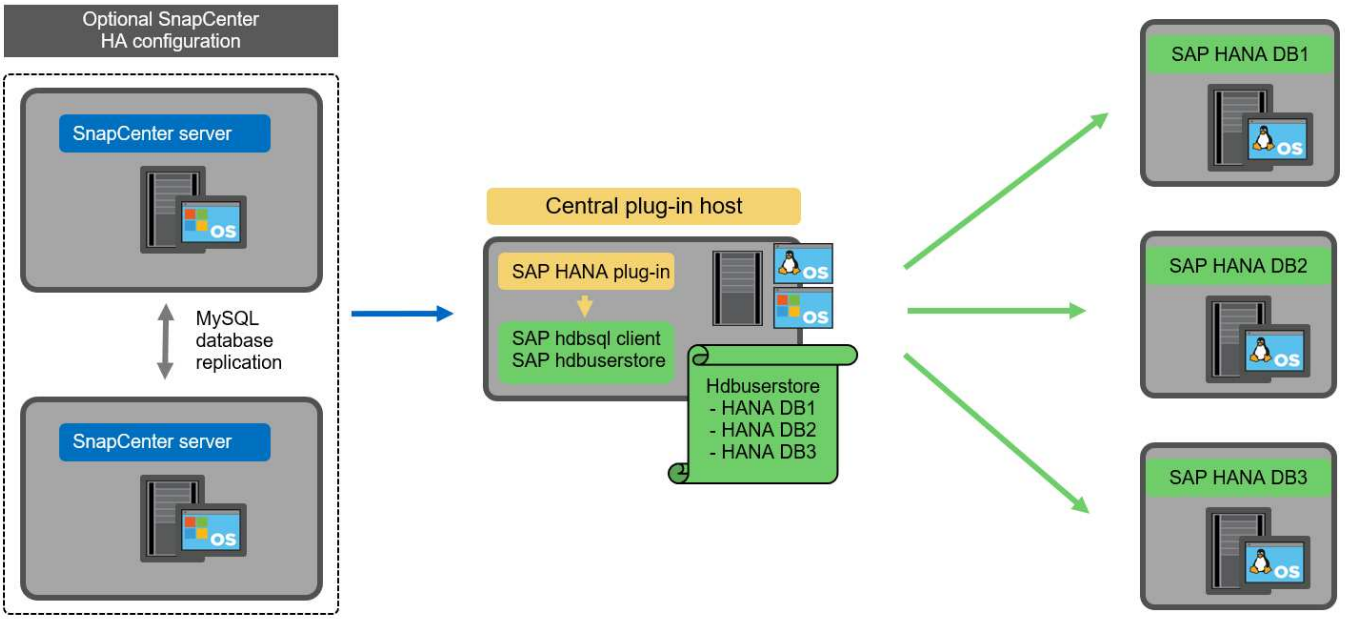
On the other hand, enhanced workflow automation for automatic discovery, automation of restore and recovery, as well as SAP system refresh operations require SnapCenter components to be installed on the database host. When using a central HANA plug-in host, these features are not available.

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

The following figure 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.

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

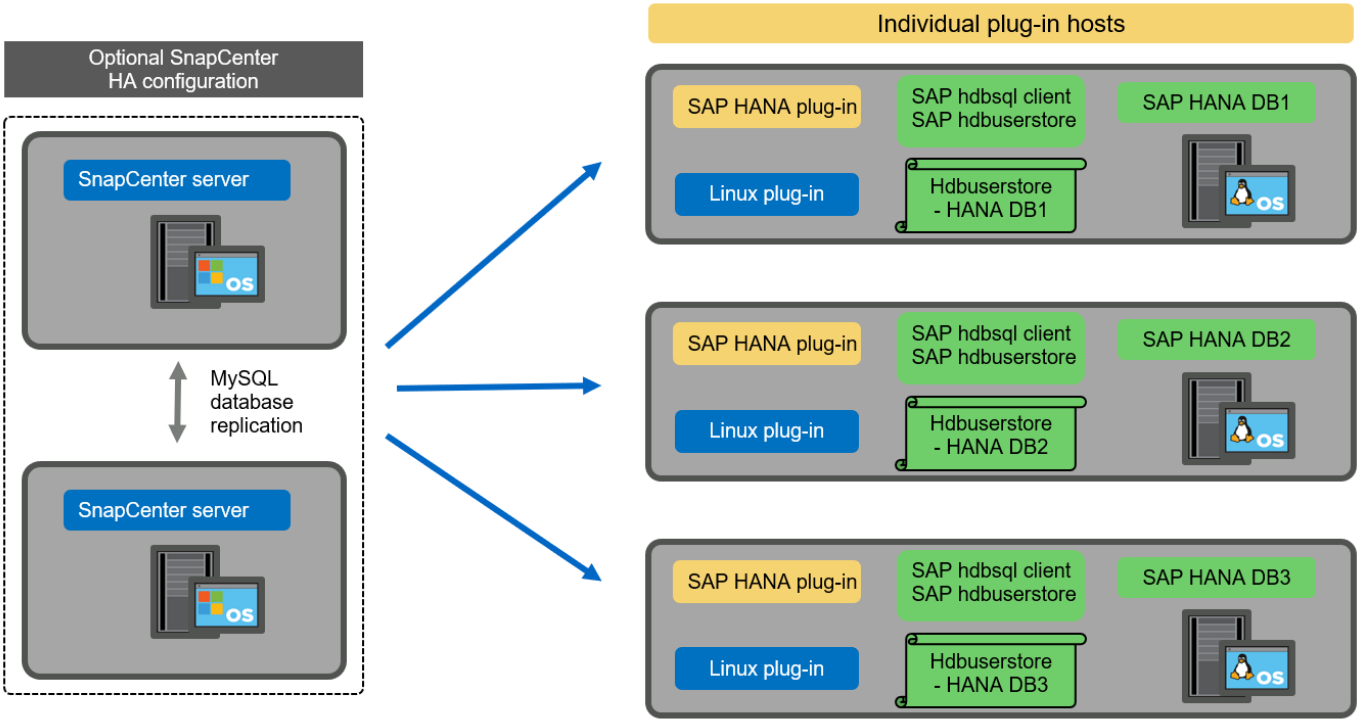


The same restriction regarding feature availability described in the previous section also applies for a separate central plug-in host.

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

The following figure shows a configuration in which the SAP HANA plug-in is installed on each SAP HANA database host.



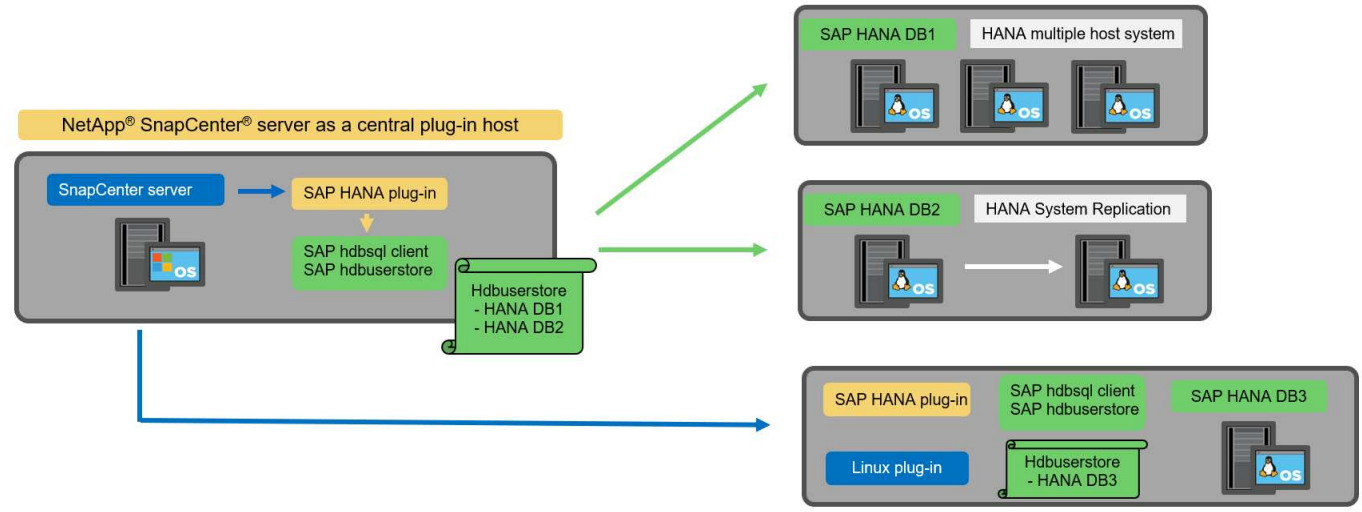
When the HANA plug-in is installed on each individual HANA database host, all features, such as automatic discovery and automated restore and recovery, are available. Also, the SnapCenter server can be set up in an HA configuration.

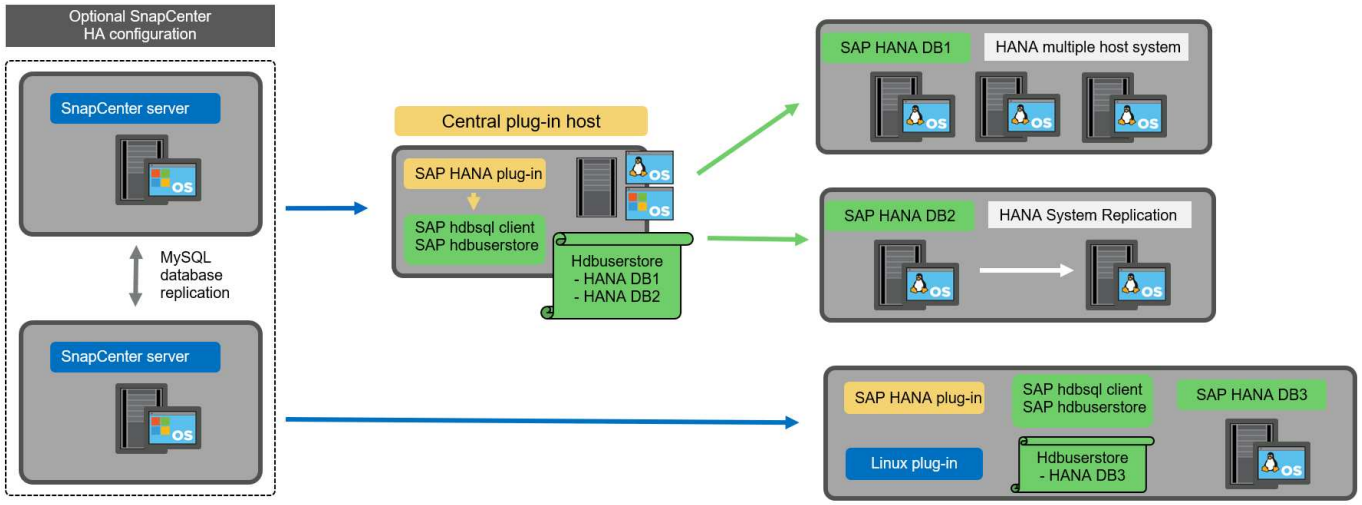
Mixed HANA plug-in deployment

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.

NetApp recommends 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.

The following two figures 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.





Summary and recommendations

In general, NetApp recommends that you deploy the HANA plug-in on each SAP HANA host to enable all

available SnapCenter HANA features and to enhance workflow automation.

> 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-build HA capability, use a separate Linux plug-in host.

The following table summarizes the different deployment options.

Deployment option	Dependencies
Central HANA plug-in host Plug-in installed on SnapCenter server	Pros: * Single HANA plug-in, central HDB user store configuration * No SnapCenter software components required on individual HANA database hosts * Support of all HANA architectures Cons: * 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: * 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: * 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

Deployment option	Dependencies
Individual HANA plug-in host Plug-in installed on HANA database server	Pros: * 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: * 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?

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

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

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

Parameters	PolicyLocalSnap	PolicyLocalSnapAndSnapVault	PolicyBlockIntegrityCheck
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.

In our example, protection policies and retention for SAP HANA database resources and non-data 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.

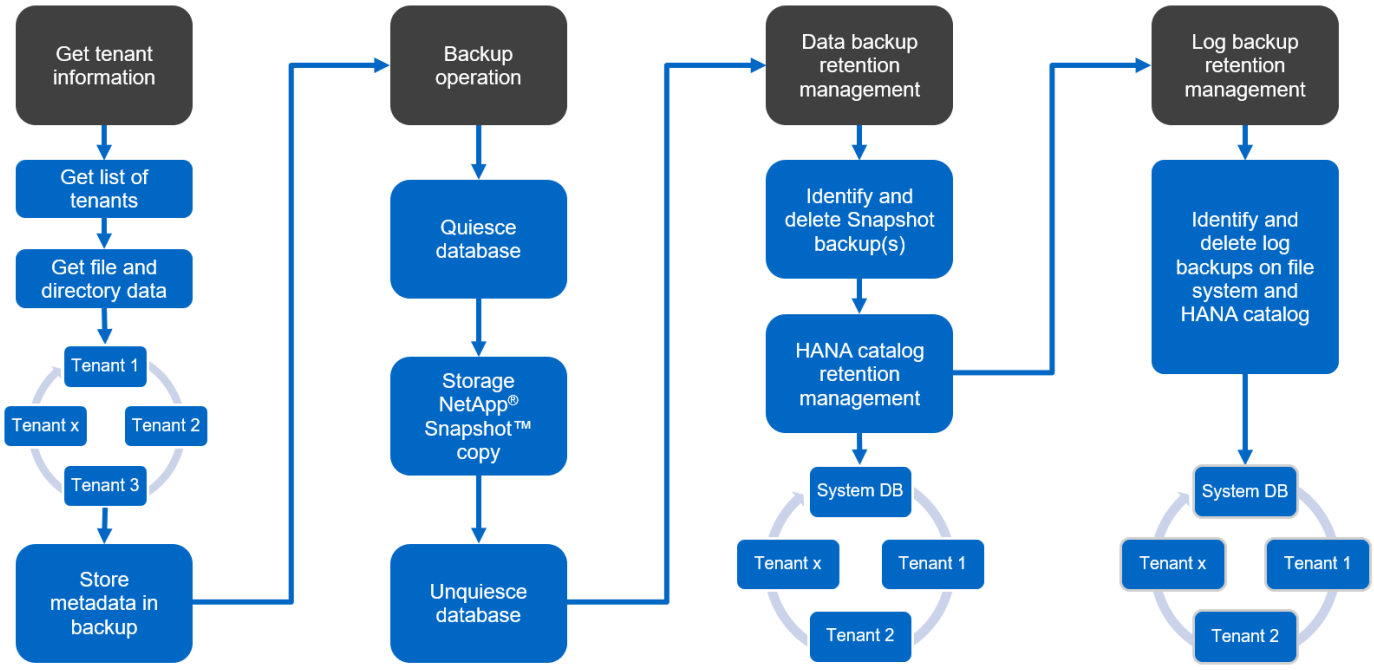
To enable a single tenant restore operation, SnapCenter must know which tenants are included in each Snapshot backup. In addition, it must know which files and directories belong to each tenant included in the Snapshot backup.

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.

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.

The following figure shows an overview of the 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.

   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.

   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.

   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.

    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.

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

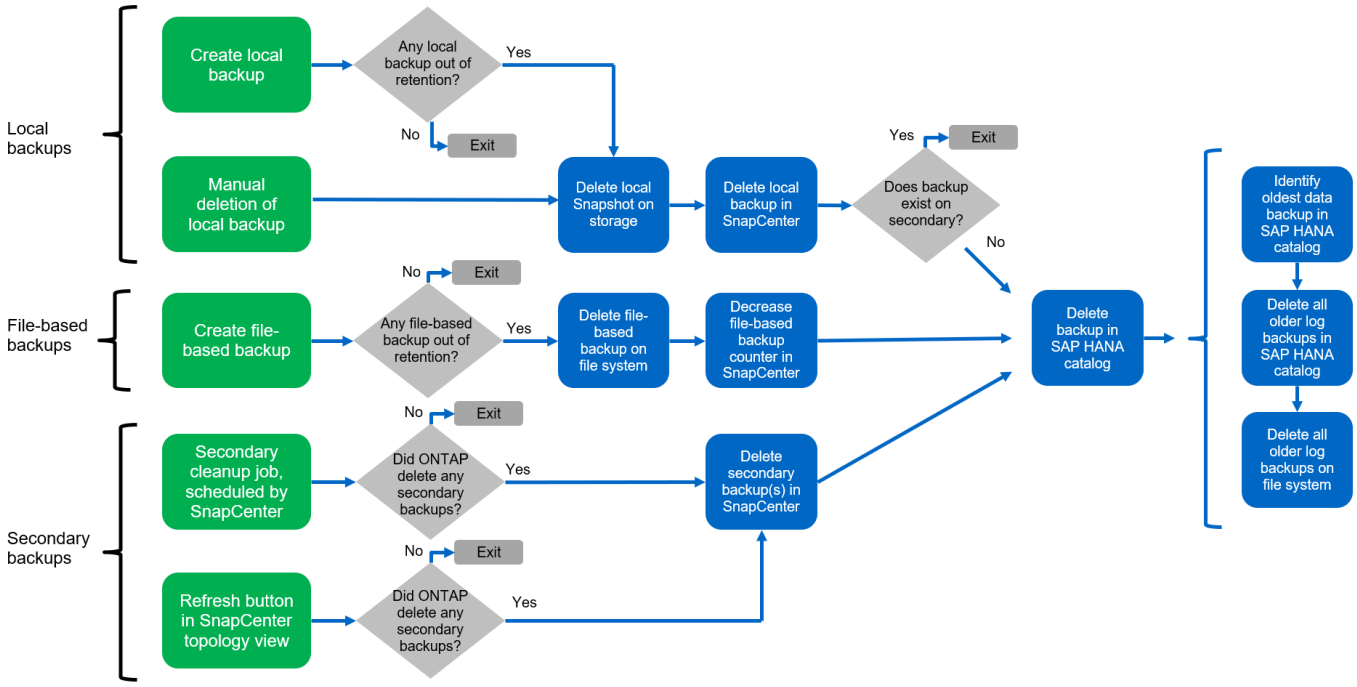
Backup retention management and housekeeping of data and log backups

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

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



Retention management of local backups at the primary storage

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

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

> 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.

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.

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 “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.

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.

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 section "Disable auto discovery on the HANA plug-in host."

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.

- **Restore of the complete resource.** All data of the HANA system is restored. If the HANA system contains one or more tenants, the data of the system database and the data of all tenants are restored.
- **Restore of a single tenant.** Only the data of the selected tenant is 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.

The following table provides a comparison of the different restore methods.

	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.

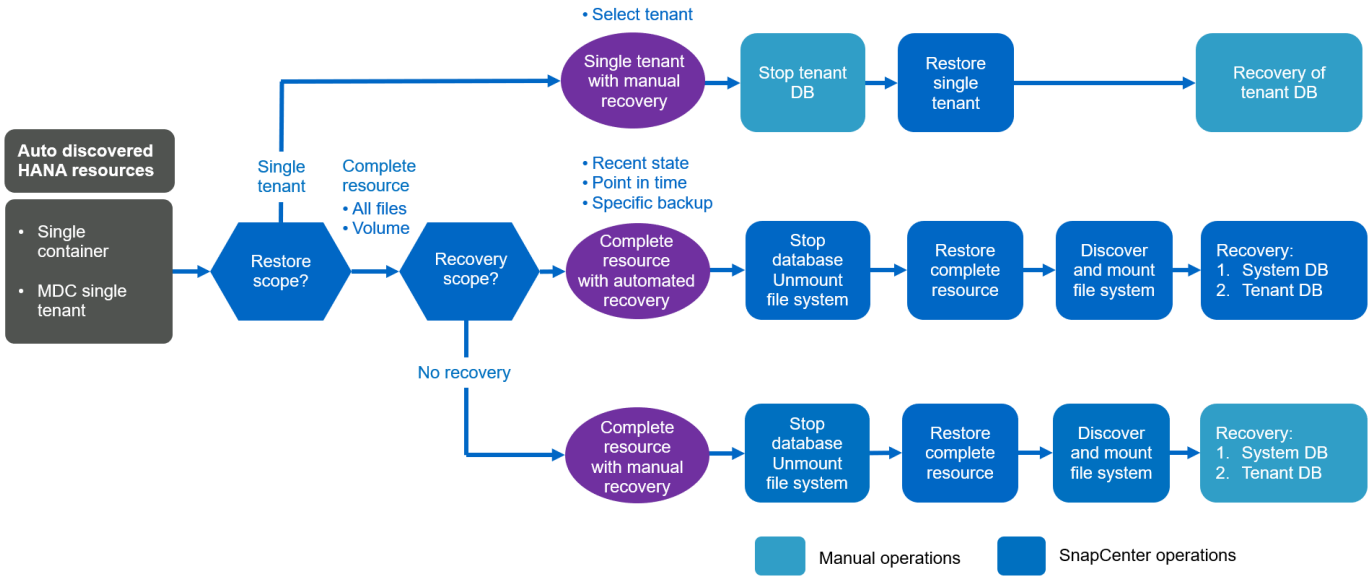
- NFS:
  - Primary storage. File-based SnapRestore operations are executed for all files of the tenant database.
  - Offsite backup storage: SnapVault restore operations are executed for all files of the tenant database.
- SAN:
  - Primary storage. Clone and connect the LUN to the database host and copy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

- **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.

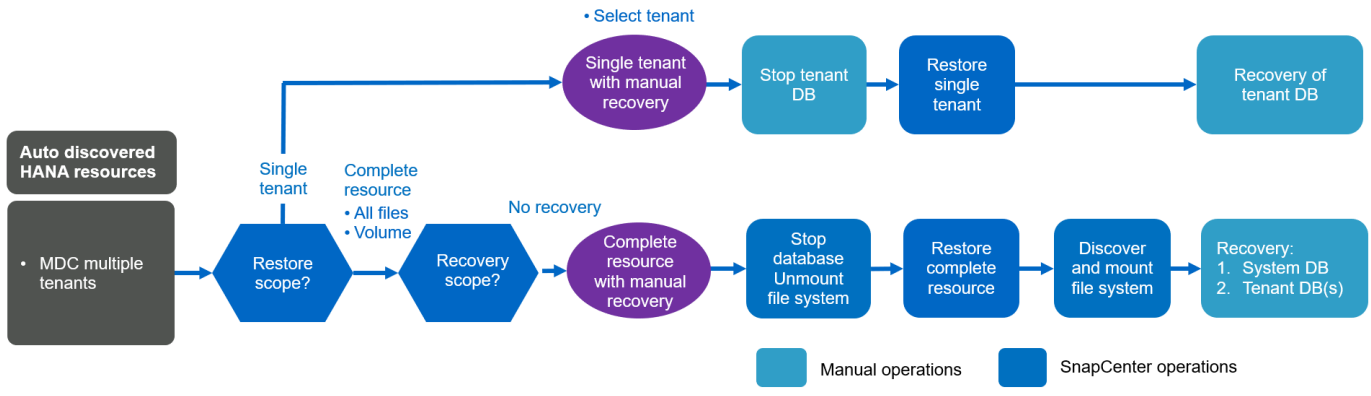


Restore and recovery of automatically discovered HANA MDC multiple tenant systems

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 the following figure:

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

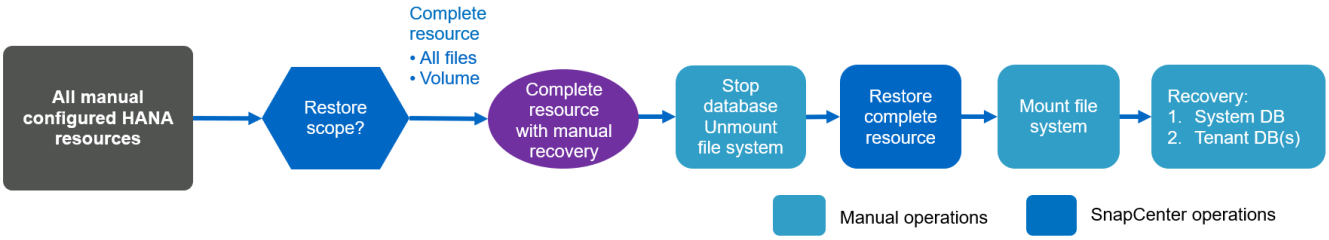
The workflows are the same as described in the previous section.



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 the following figure. The workflow for manual recovery is the same as described in the previous sections.



Summary restore and recovery operations

The following table summarizes the restore and recovery operations depending on the HANA resource configuration in SnapCenter.

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
	• Tenant restore	Manual	Not required	Manual

SnapCenter resource configuration	Restore and recovery options	Stop HANA database	Unmount before, mount after restore operation	Recovery operation
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)
  - Uses NFS as storage protocol
- **SS1.**
  - SAP HANA single-host MDC single tenant system
  - Auto discovered with HANA plug-in installed on HANA database host
  - Uses NFS as storage protocol
- **SM1.**

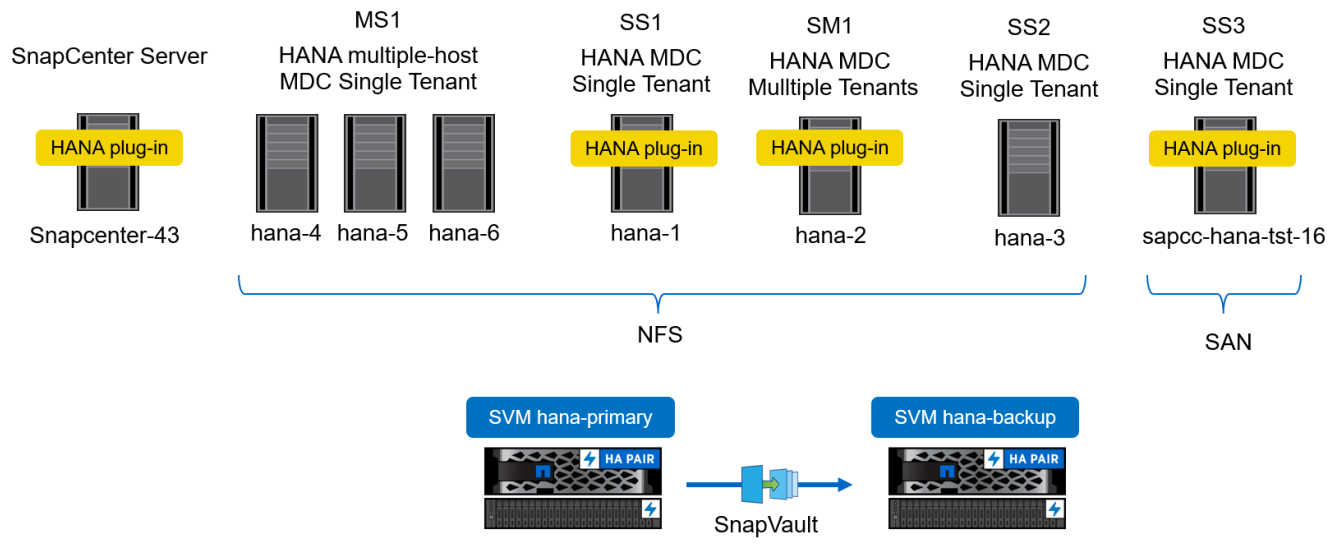
- SAP HANA single-host MDC multiple tenant system
- Auto discovered with HANA plug-in installed on HANA database host
- Uses NFS as storage protocol

- **SS2.**
  - SAP HANA single-host MDC single tenant system
  - Managed with a central plug-in host (SnapCenter Server)
  - Uses NFS as storage protocol
- **SS3.**
  - SAP HANA single-host MDC single tenant system
  - Auto discovered with HANA plug-in installed on HANA database host
  - Uses 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.

The following figure shows the lab setup.

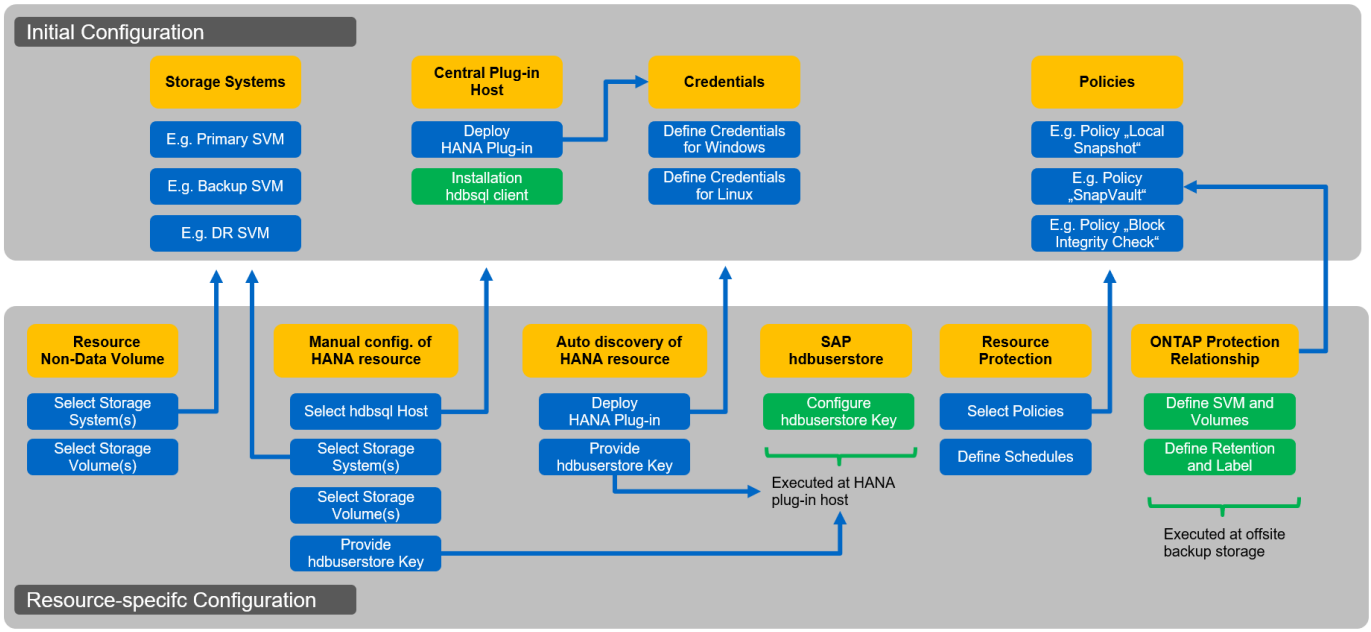


SnapCenter configuration

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.

The following figure 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.



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, primary, off-site backup, and disaster recovery storage.

> Storage cluster credentials can the 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 performed for each SAP HANA database and includes the following configurations:

- SAP HANA non-data volume resource configuration:
  - Storage systems and volumes
- SAP hdbuserstore key configuration:
  - The SAP hdbuserstore key configuration for the specific SAP HANA database must be performed 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.

Initial SnapCenter configuration

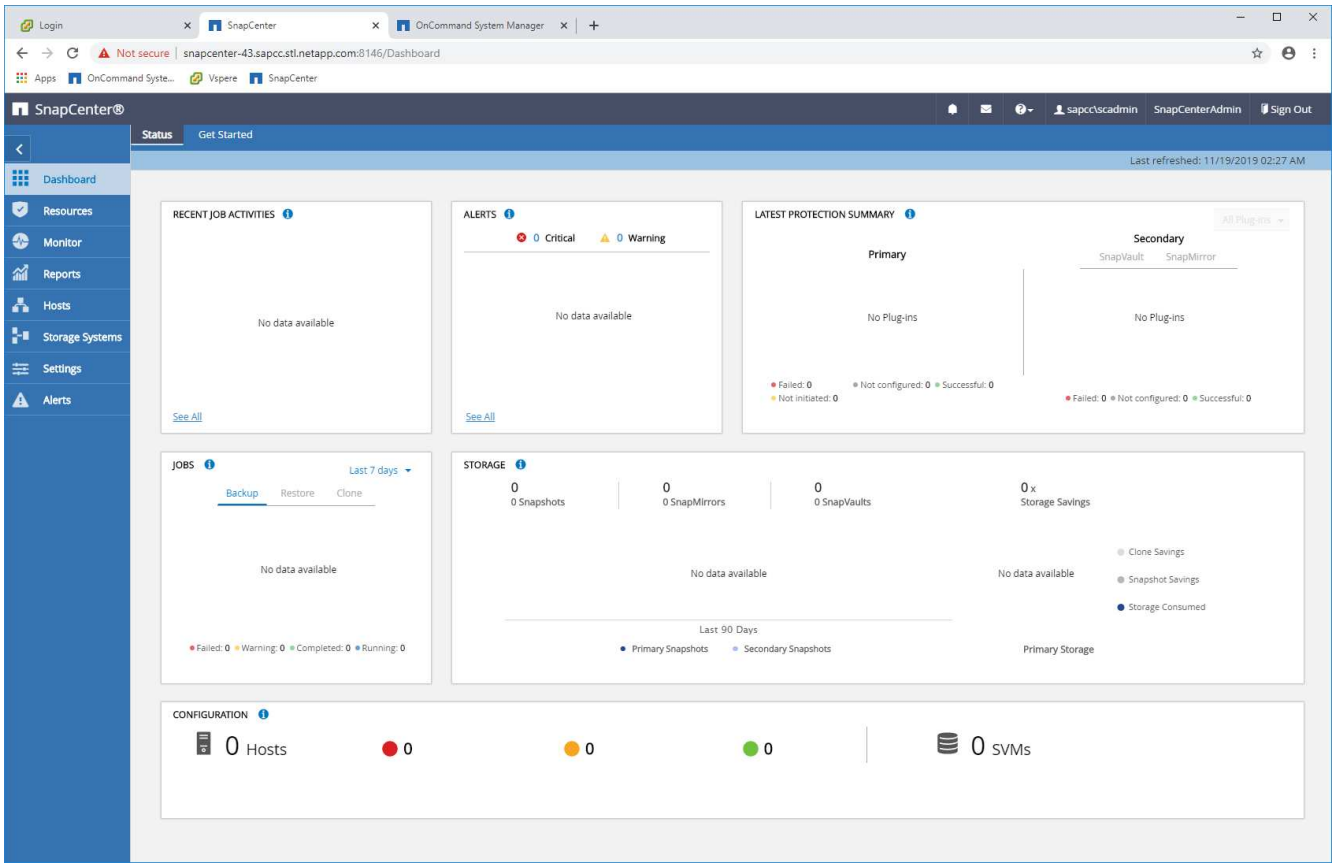
Initial configuration includes the following steps:

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.

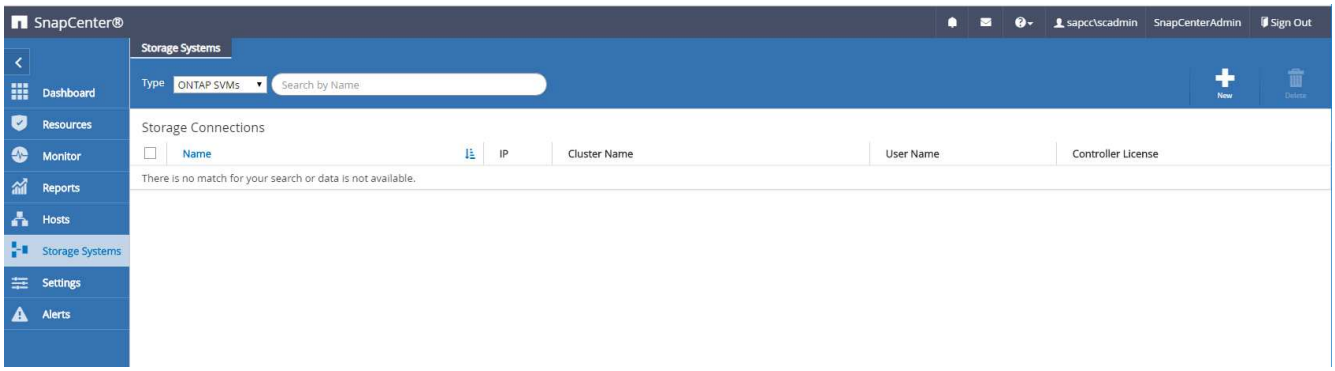
Storage system configuration

1. Log in to the SnapCenter Server GUI.



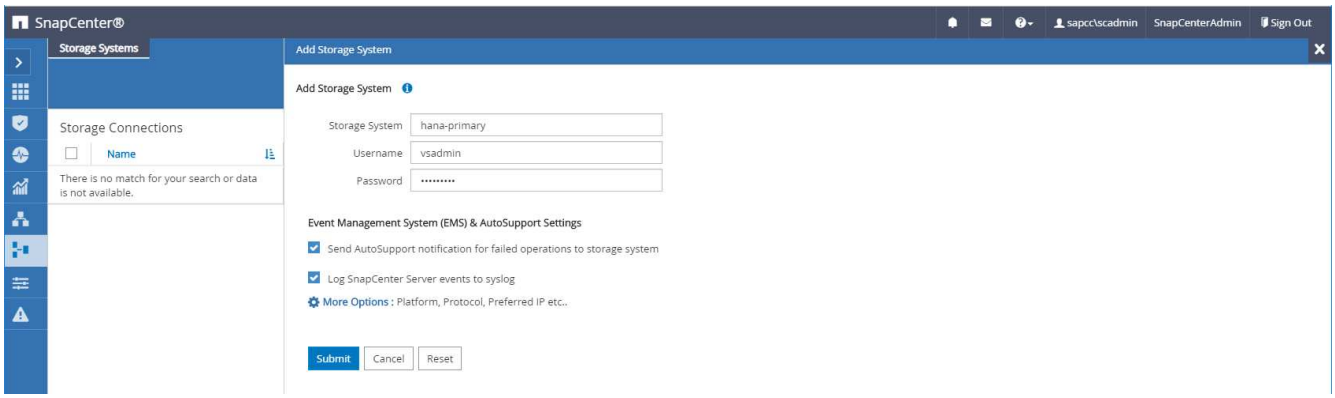
2. Select Storage Systems.

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. SVM management is used in the following example.



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

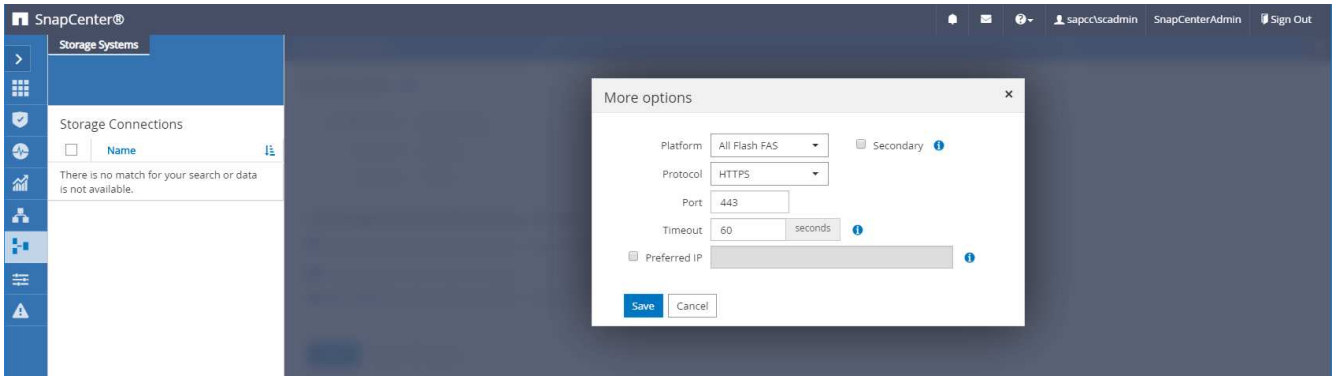
The SVM user is not required to be the vsadmin user, as shown in the screenshot. Typically, a user is configured on the SVM and assigned the required permissions to execute backup and restore operations. Details on required privileges can be found in the SnapCenter Installation Guide in the section titled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



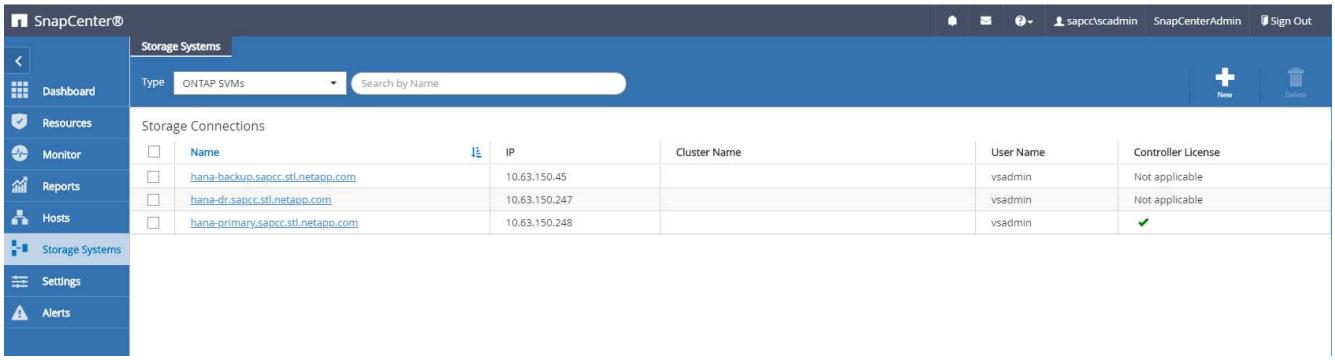
4. Click More Options to configure the storage platform.

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

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

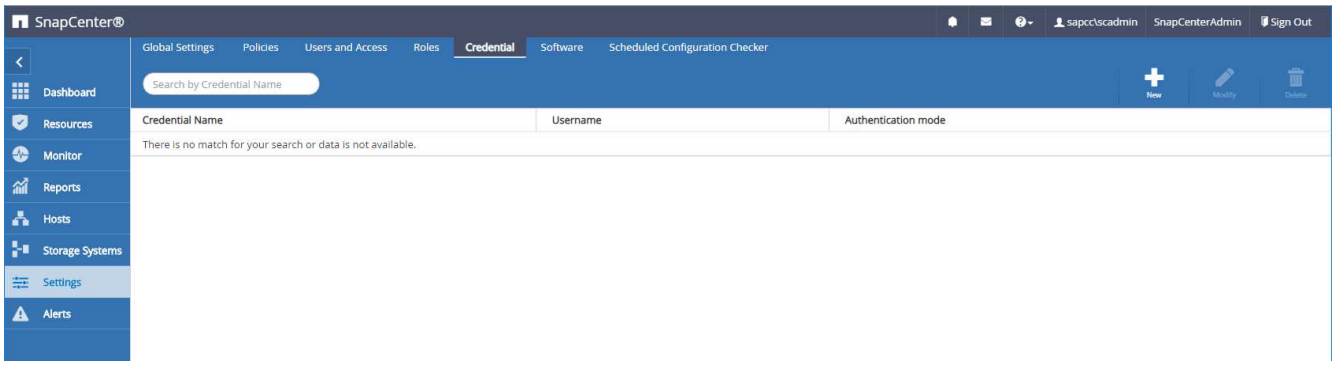


5. Add additional storage systems as required. In our example, an additional offsite backup storage and a disaster recovery storage has been added.

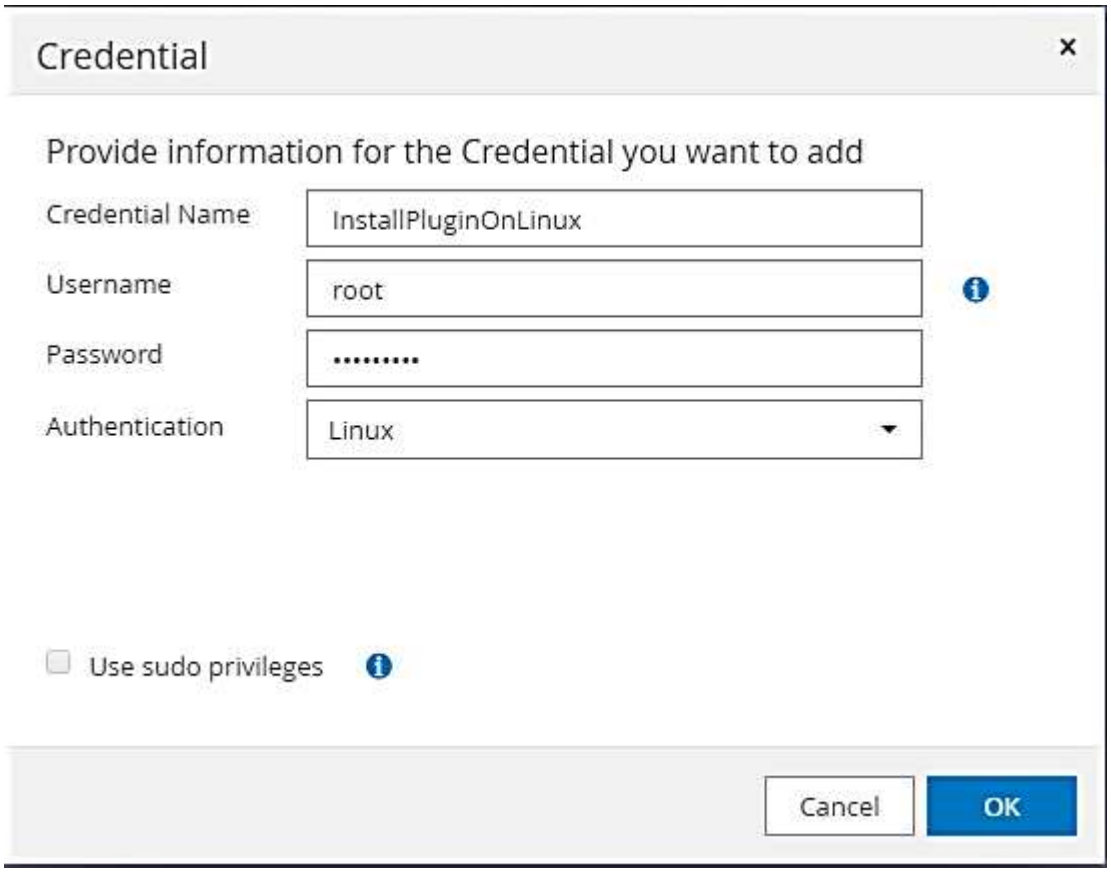


Credentials configuration

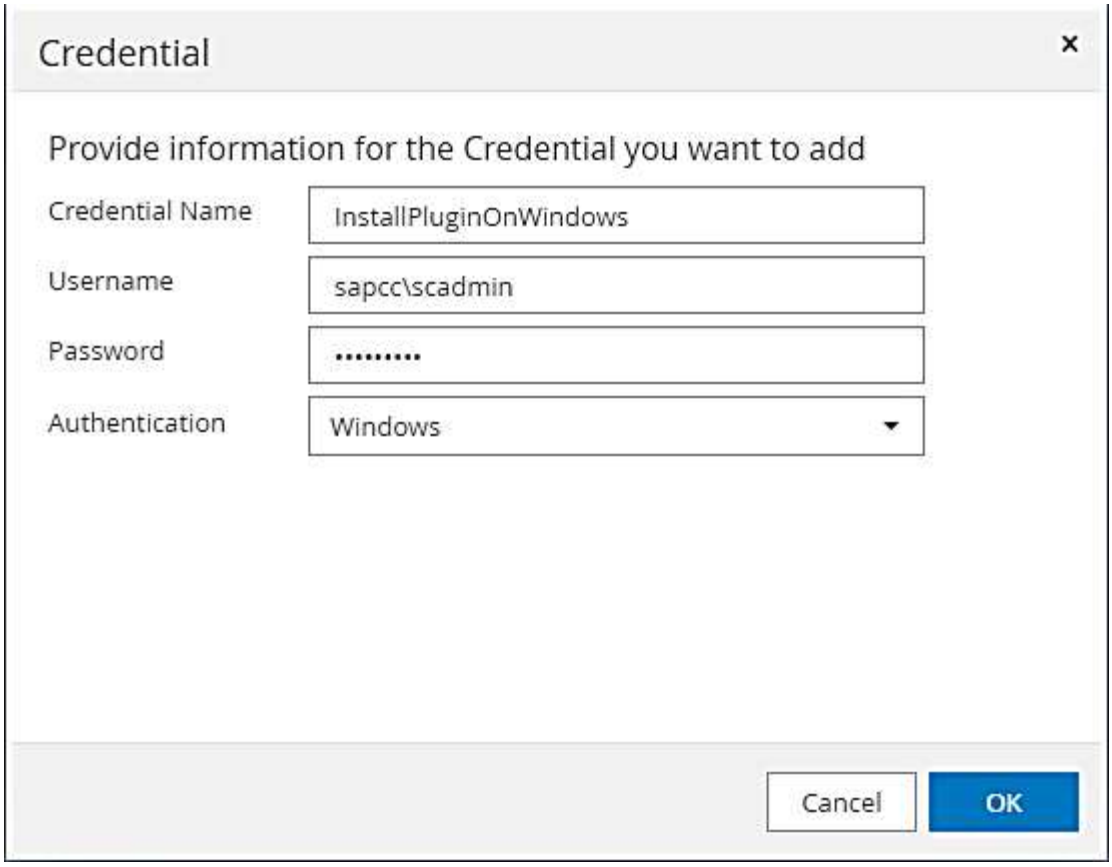
1. Go to Settings, select Credentials, and click New.



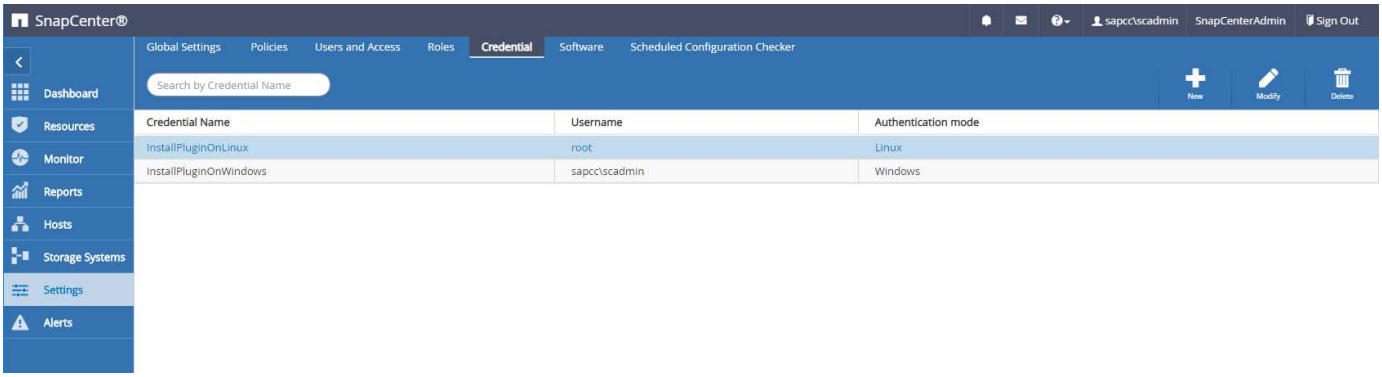
2. Provide the credentials for the user that are used for plug-in installations on Linux systems.



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



The following figure shows the configured credentials.

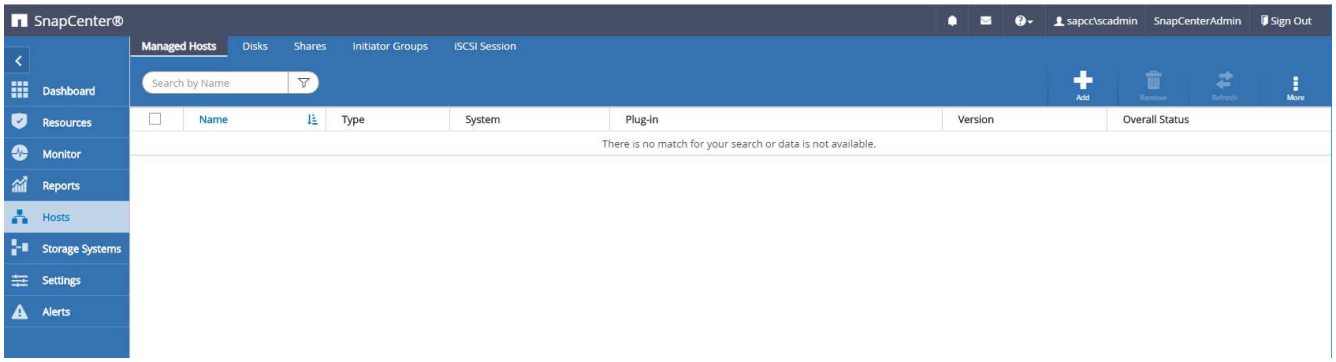


SAP HANA plug-in installation on a central plug-in host

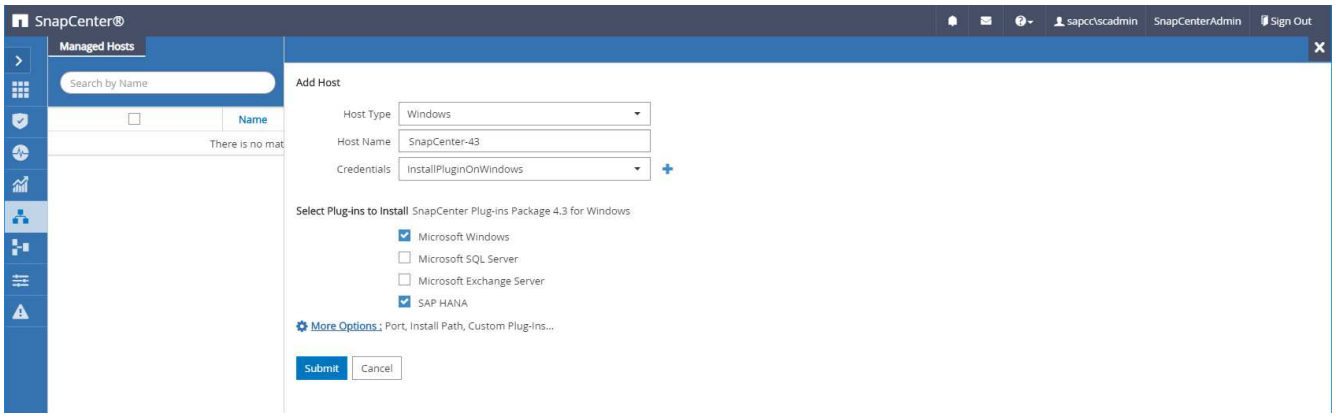
In the lab setup, the SnapCenter Server is also used as a central HANA plug-in host. The Windows host on which SnapCenter Server runs is added as a host, and the SAP HANA plug-in is installed on the Windows host.

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.

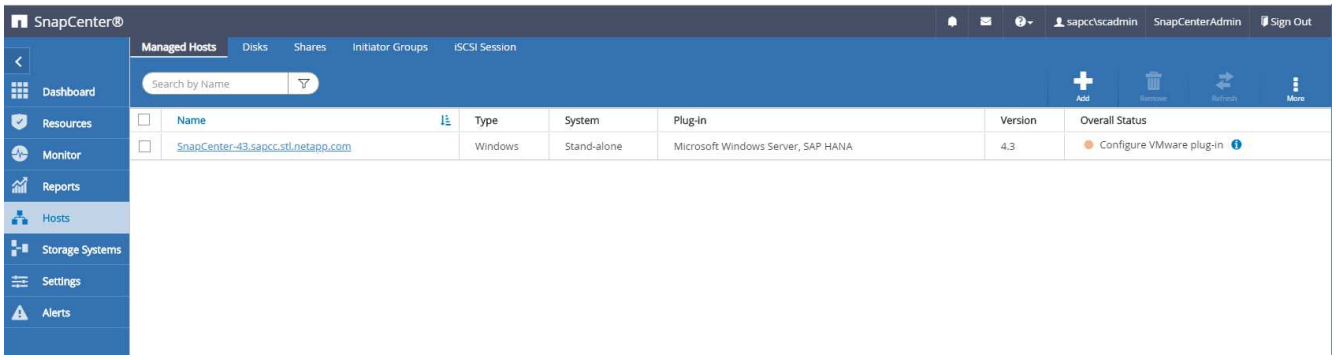
1. Go to Hosts and click Add.



2. Provide the required host information. Click Submit.



The following figure shows all the configured hosts after the HANA plug-in is deployed.



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 section "Data protection strategy," policies are usually configured independently of the resource and can be used by multiple SAP HANA databases.

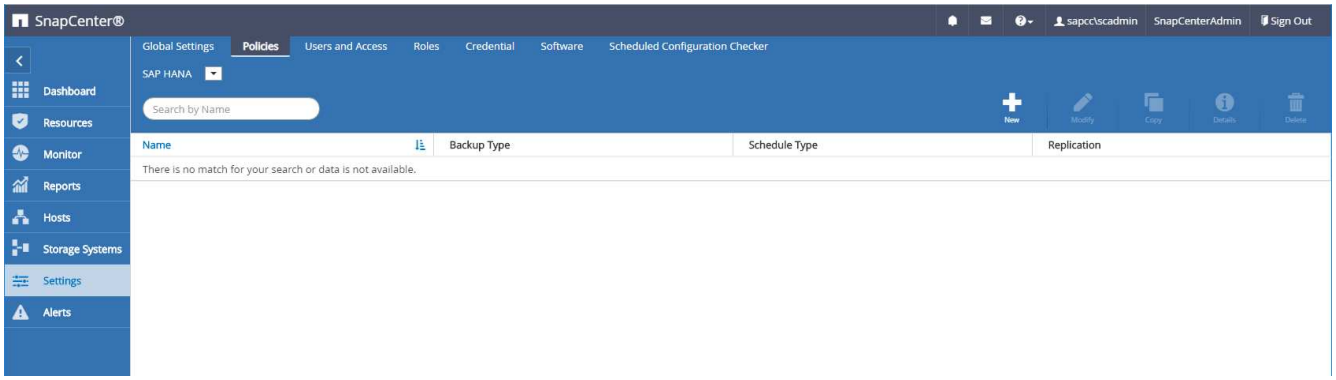
A typical minimum configuration consists of the following policies:

- Policy for hourly backups without replication: `LocalSnap`
- Policy for daily backups with SnapVault replication: `LocalSnapAndSnapVault`
- Policy for weekly block integrity check using a file-based backup: `BlockIntegrityCheck`

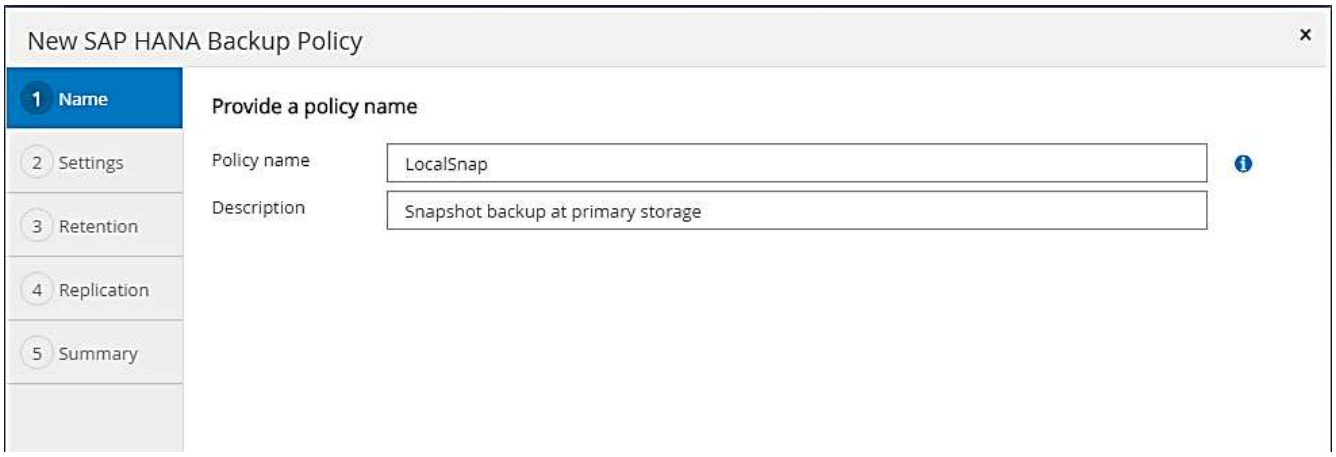
The following sections describe the configuration of these three policies.

Policy for hourly Snapshot backups

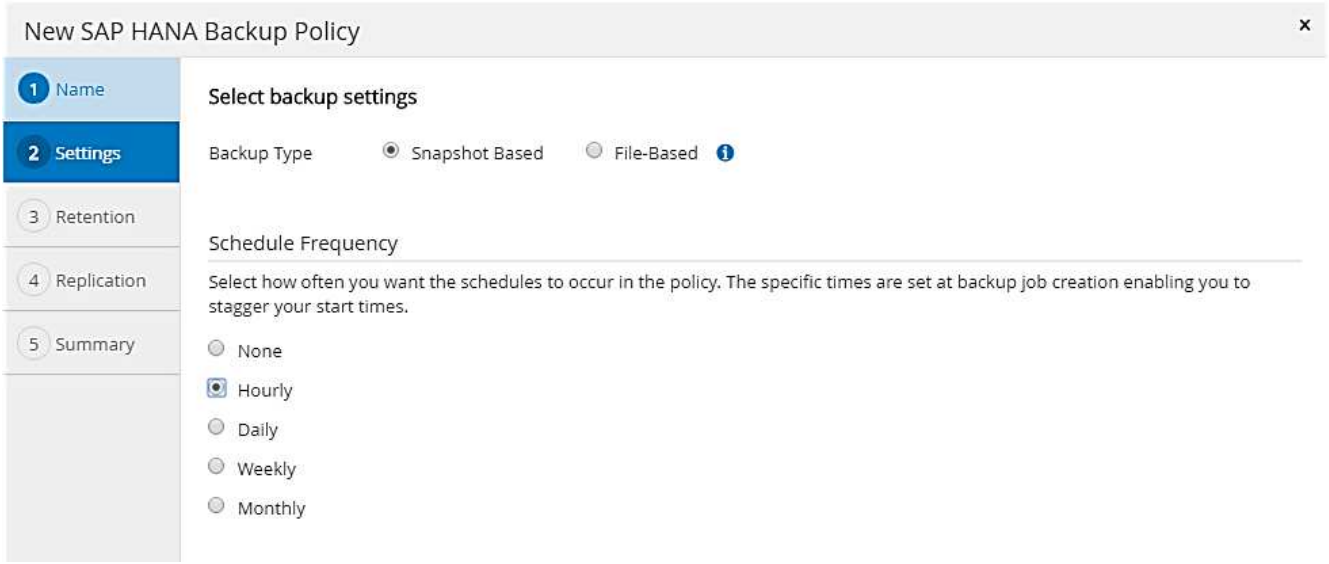
1. Go to Settings > Policies and click New.



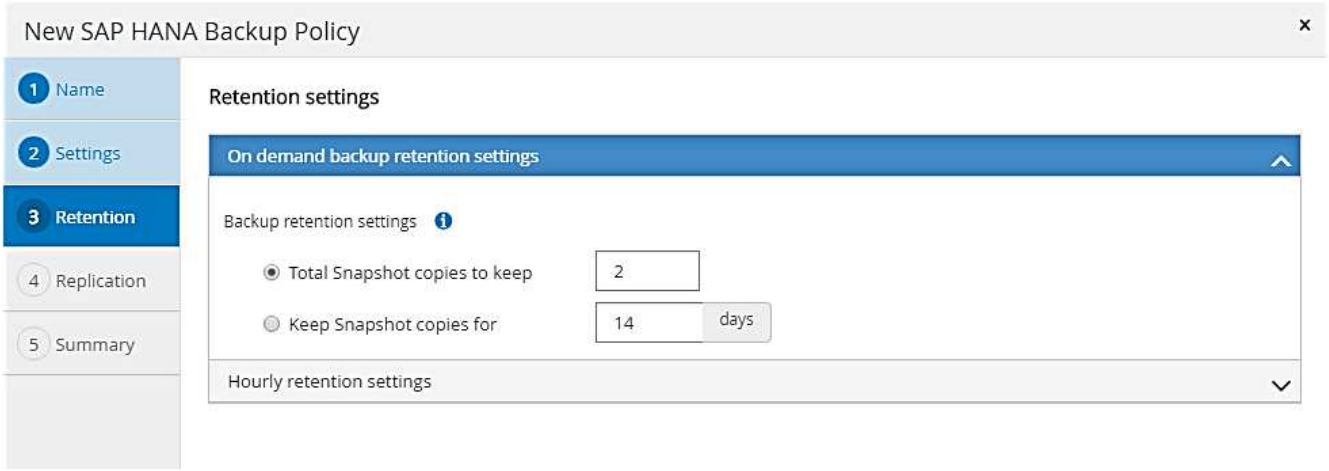
2. Enter the policy name and description. Click Next.



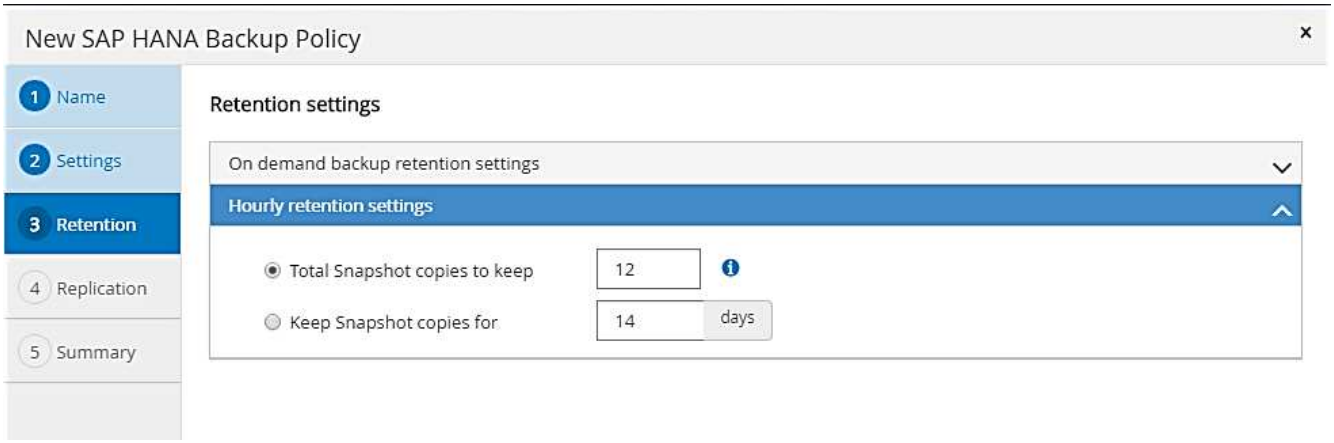
3. Select backup type as Snapshot Based and select Hourly for schedule frequency.



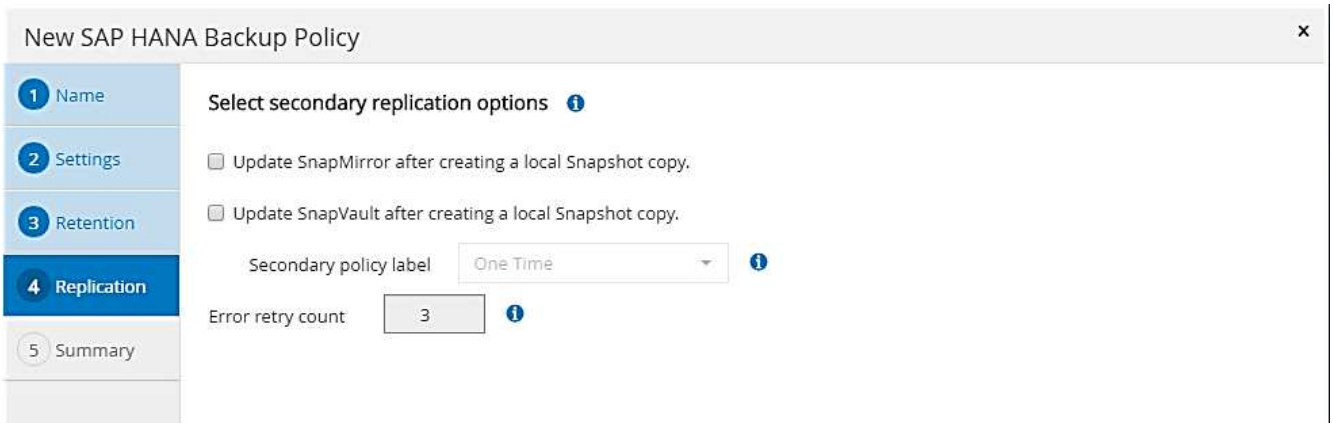
4. Configure the retention settings for on-demand backups.



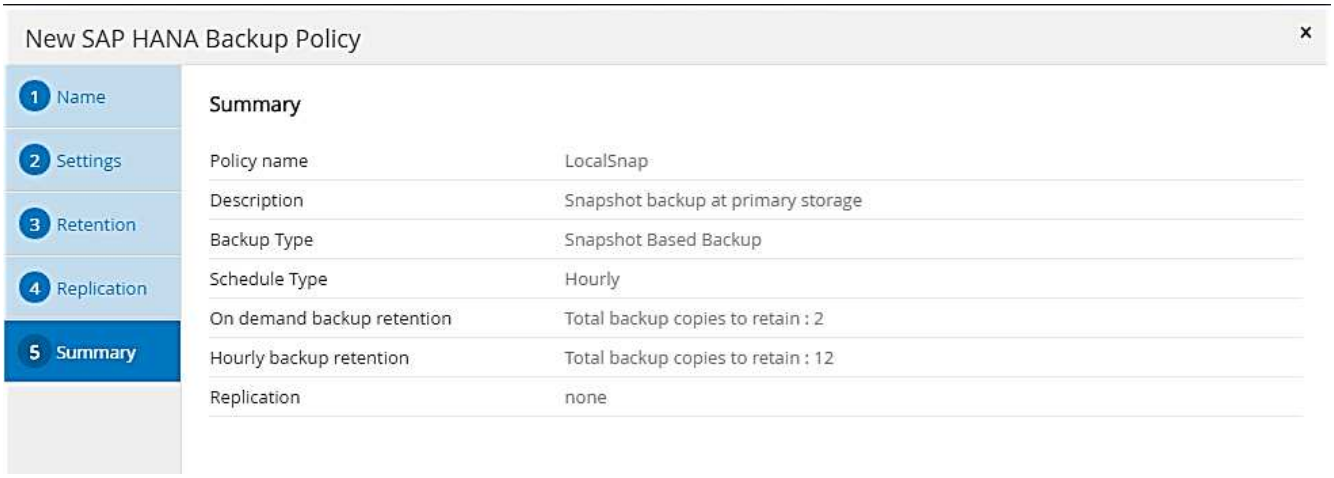
5. Configure the retention settings for scheduled backups.



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

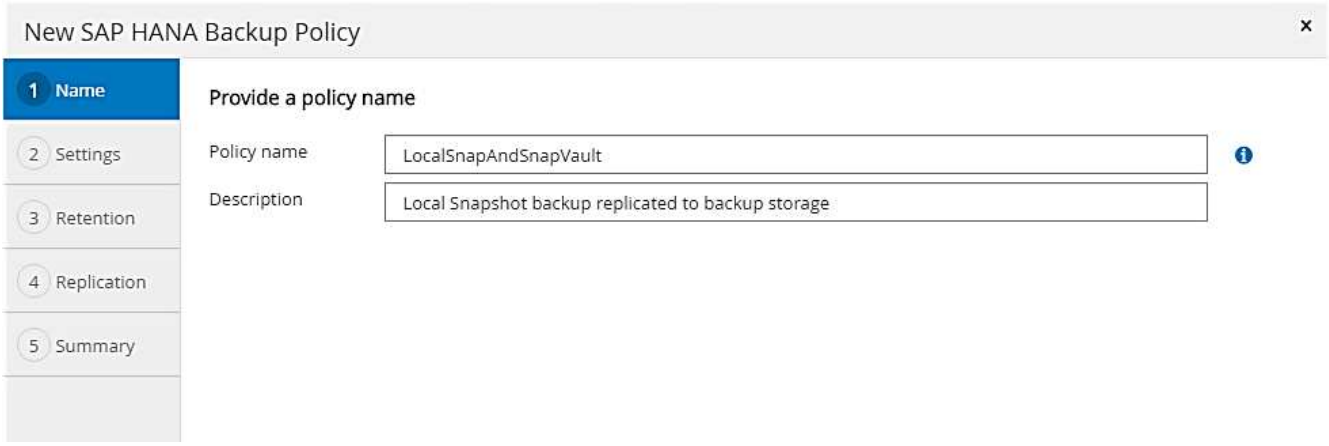


7. On the Summary page, click Finish.

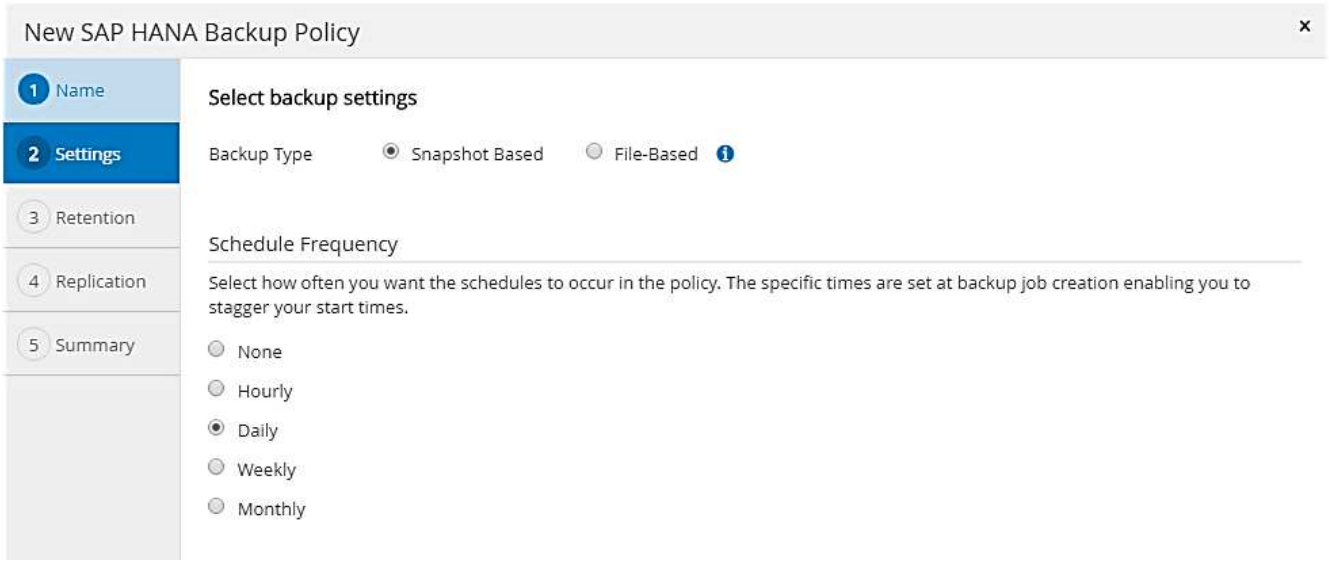


Policy for daily Snapshot backups with SnapVault replication

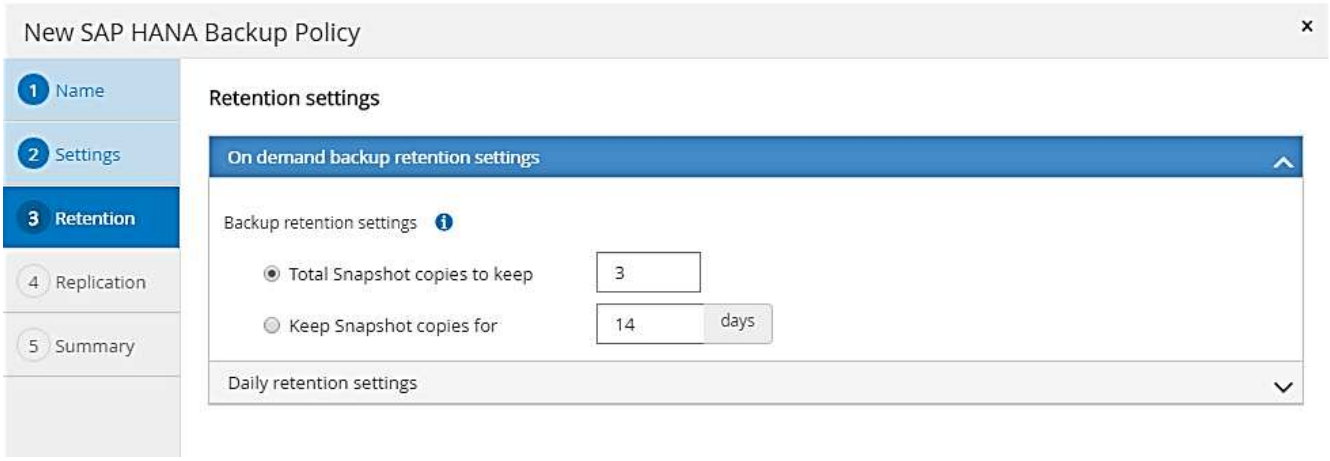
1. Go to Settings > Policies and click New.
2. Enter the policy name and description. Click Next.



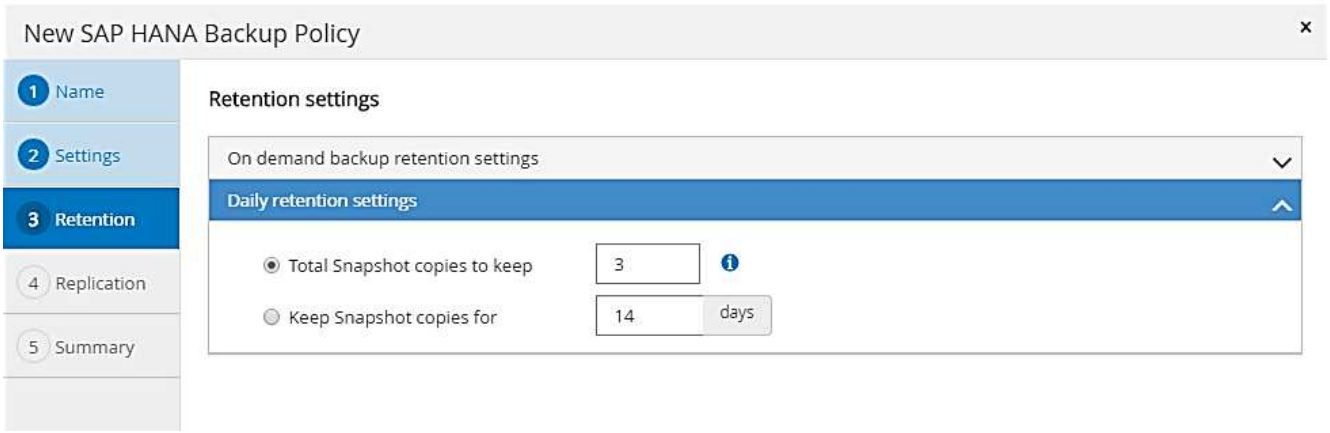
3. Set the backup type to Snapshot Based and the schedule frequency to Daily.



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

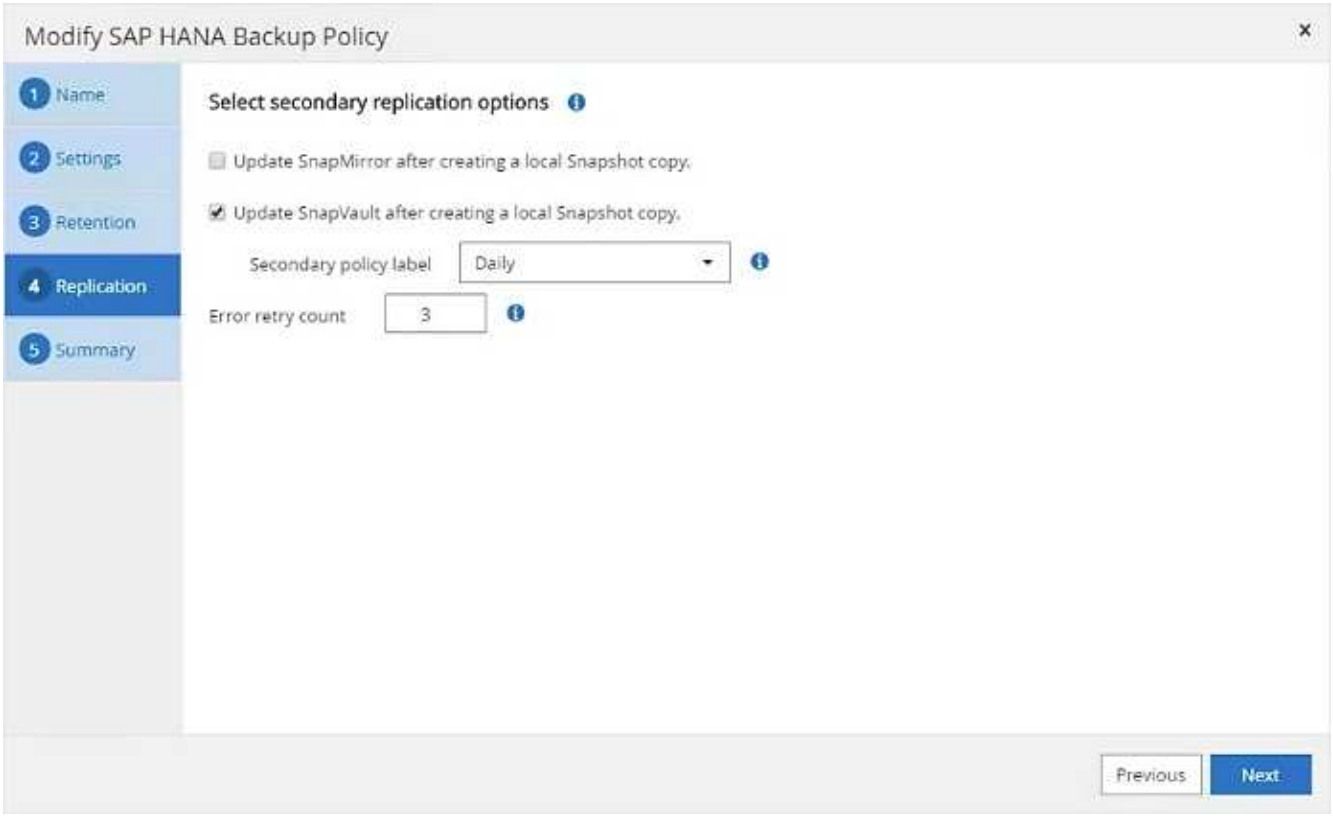


5. Configure the retention settings for scheduled backups.

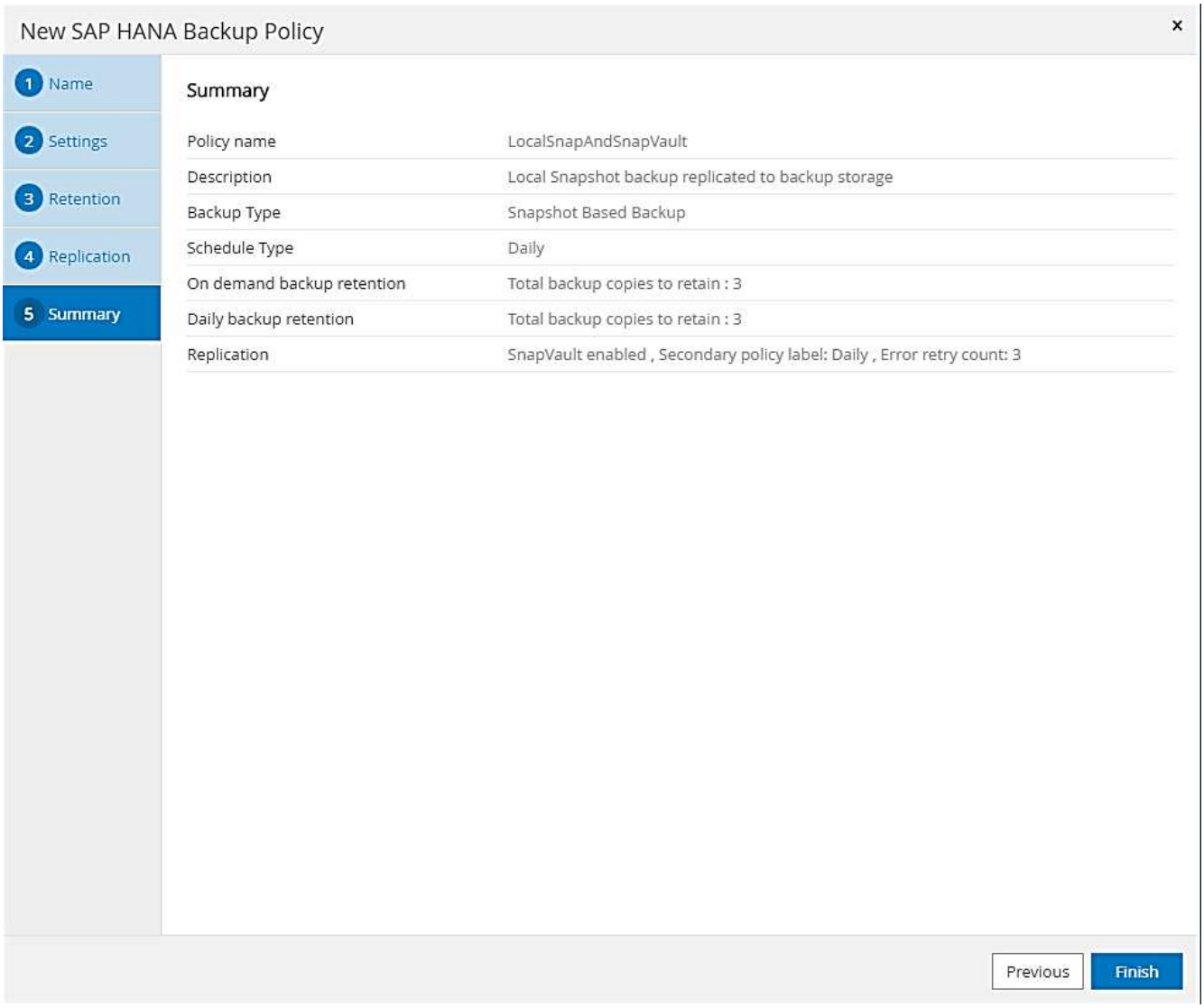


6. Select Update SnapVault after creating a local Snapshot copy.

> The secondary policy label must be the same as the SnapMirror label in the data protection configuration on the storage layer. See the section "Configuration of data protection to off-site backup storage."

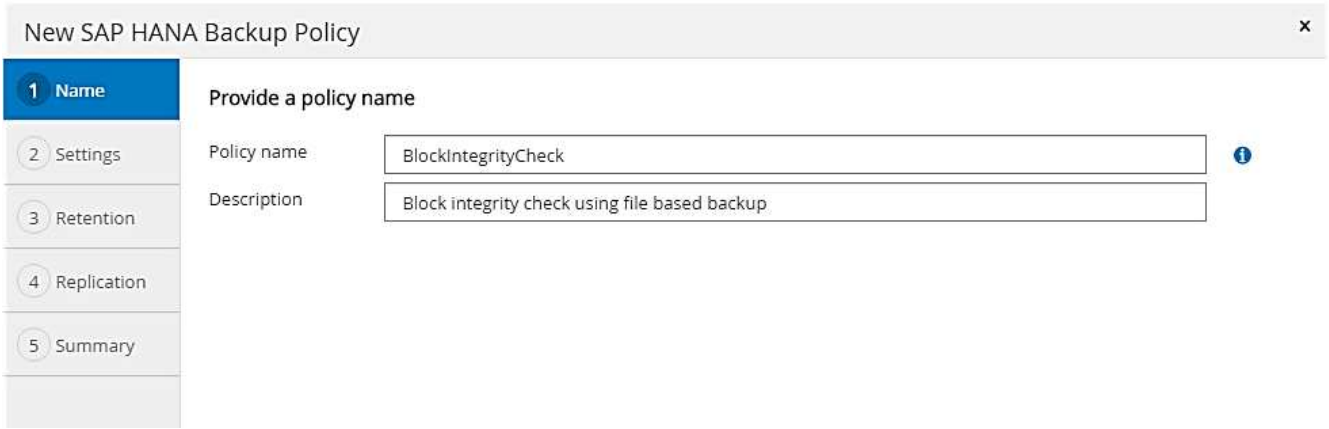


7. On the Summary page, click Finish.

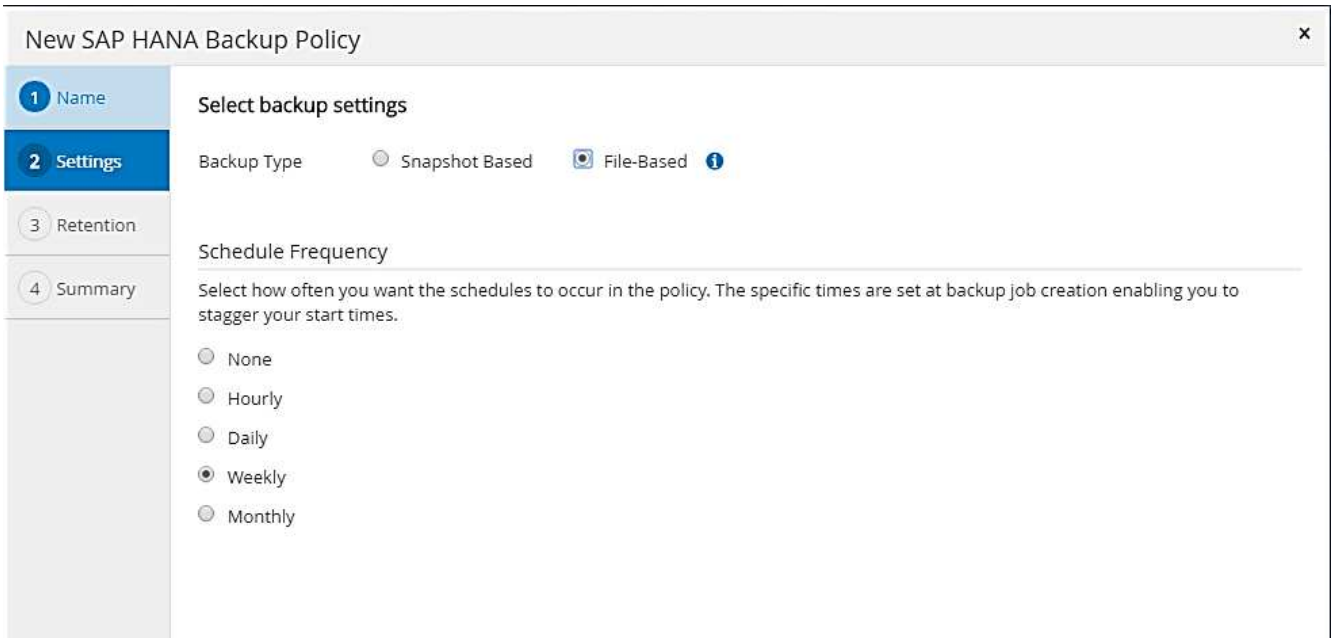


Policy for Weekly Block Integrity Check

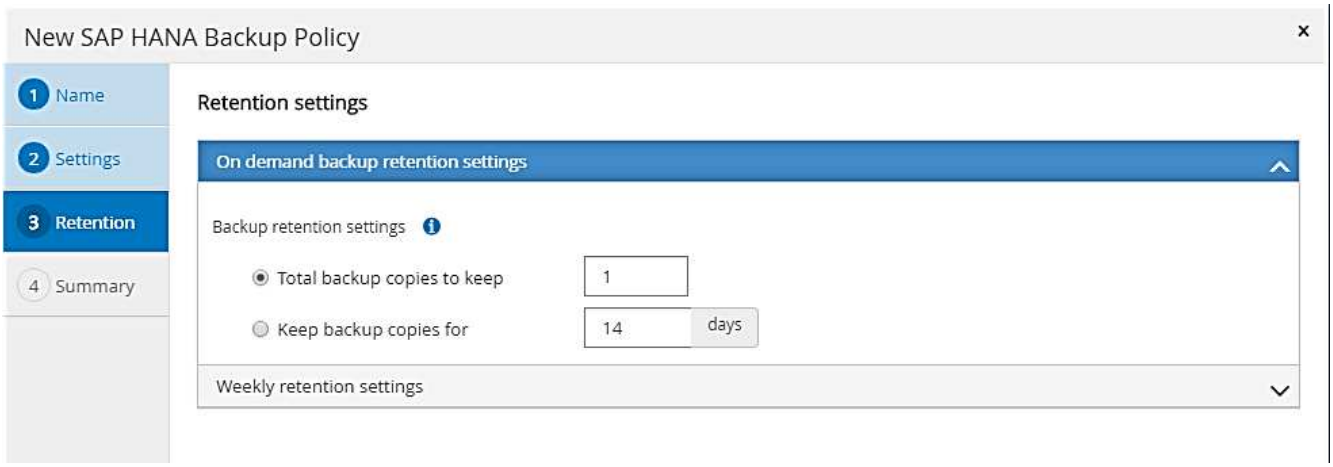
1. Go to Settings > Policies and click New.
2. Enter the policy name and description. Click Next.



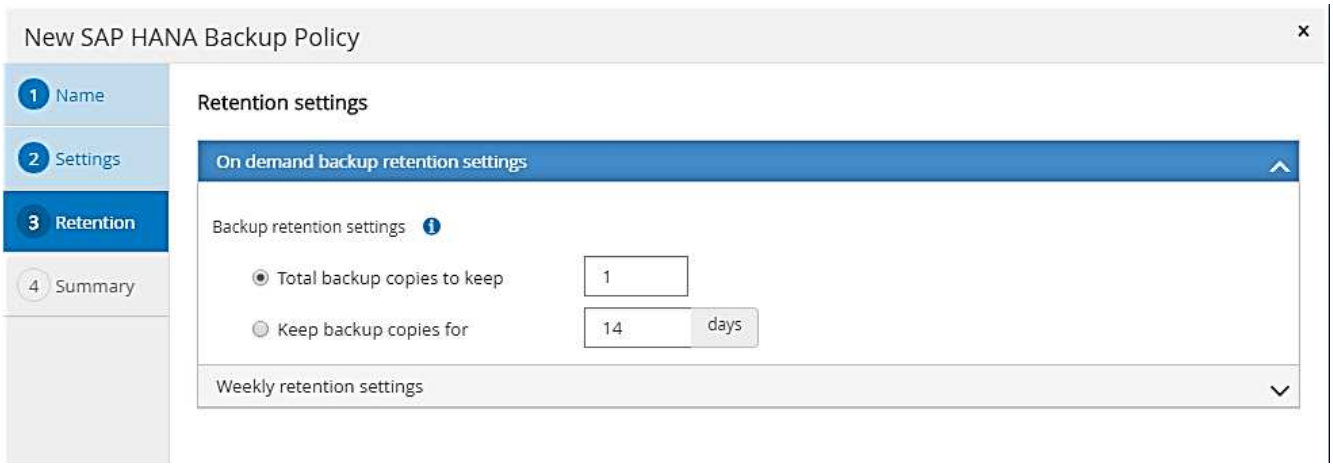
3. Set the backup type to File-Based and schedule frequency to Weekly.



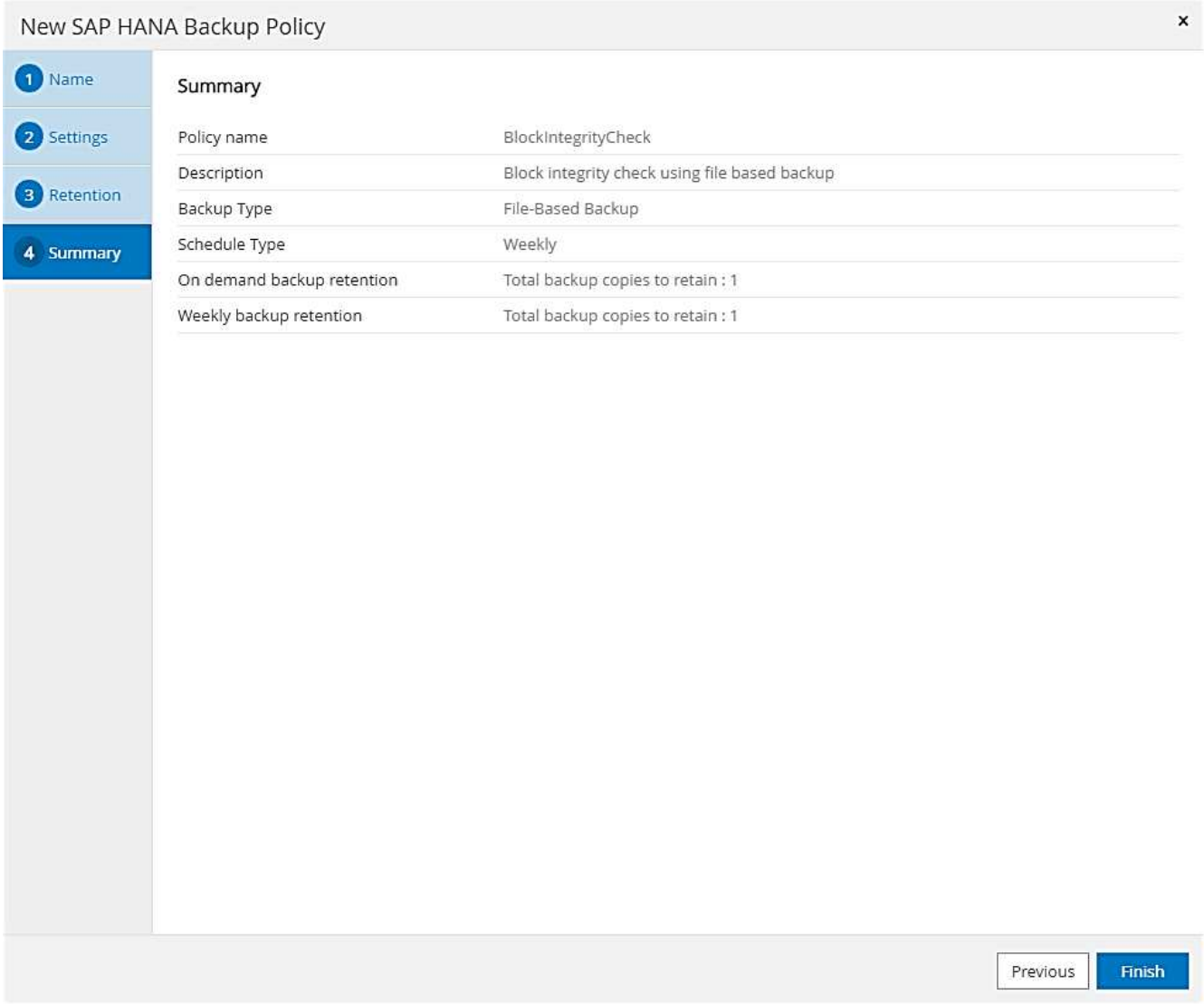
4. Configure the retention settings for on-demand backups.



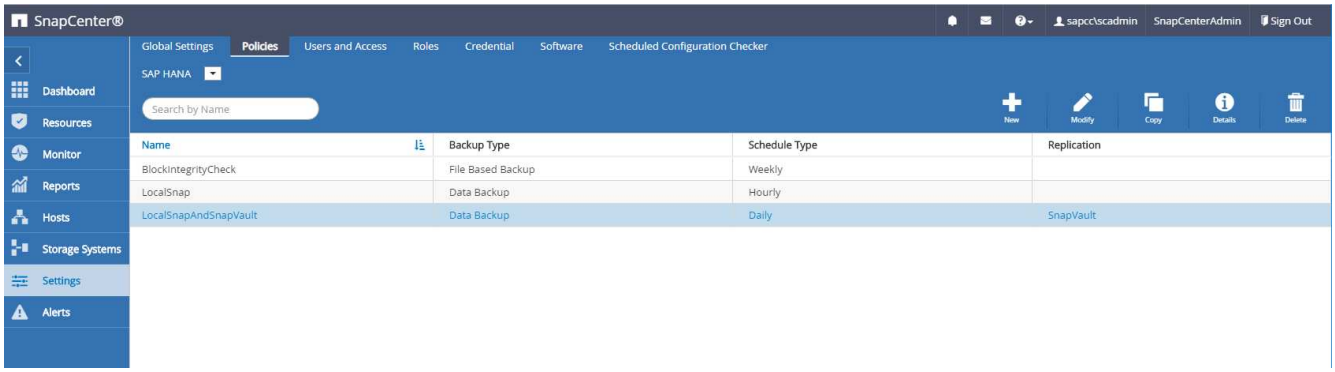
5. Configure the retention settings for scheduled backups.



6. On the Summary page, click Finish.



The following figure shows a summary of the configured policies.



SnapCenter resource-specific configuration for SAP HANA database backups

This section describes the configuration steps for two example configurations.

- **SS2.**
  - Single-host SAP HANA MDC single-tenant system using NFS for storage access

- The resource is 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.**
  - Single-host SAP HANA MDC single-tenant system using NFS for storage access
  - The resource is 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.

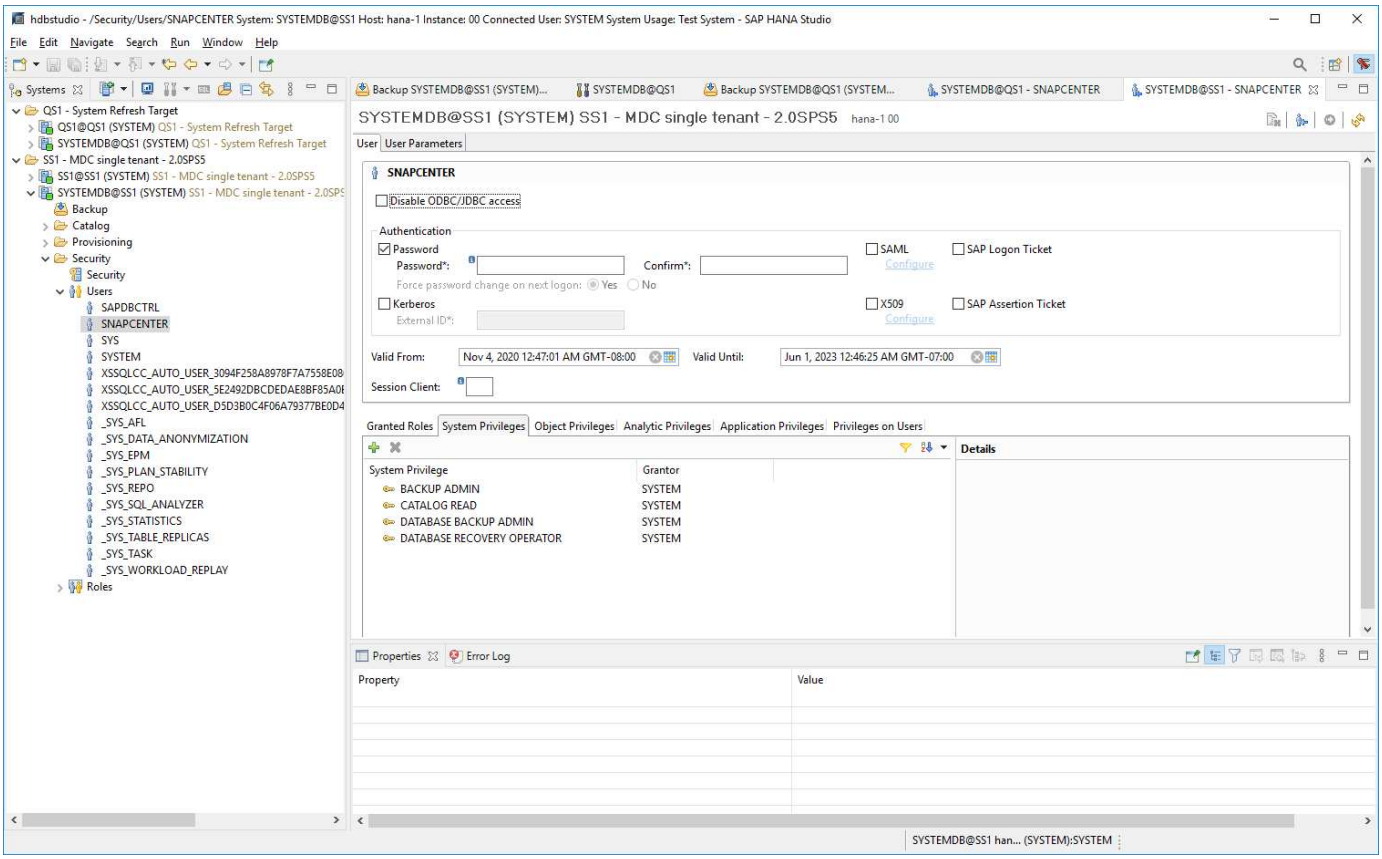
SAP HANA backup user and hdbuserstore configuration

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.

The following figure shows the SAP HANA Studio through which the backup user can be created.

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.

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.



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>
```

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>
```

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>
```

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.

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 - ss1adm
ss1adm@hana-1:/usr/sap/SS1/HDB00>
ss1adm@hana-1:/usr/sap/SS1/HDB00>
ss1adm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore set SS1KEY hana-1:30013
SnapCenter password
ss1adm@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
ss1adm@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.

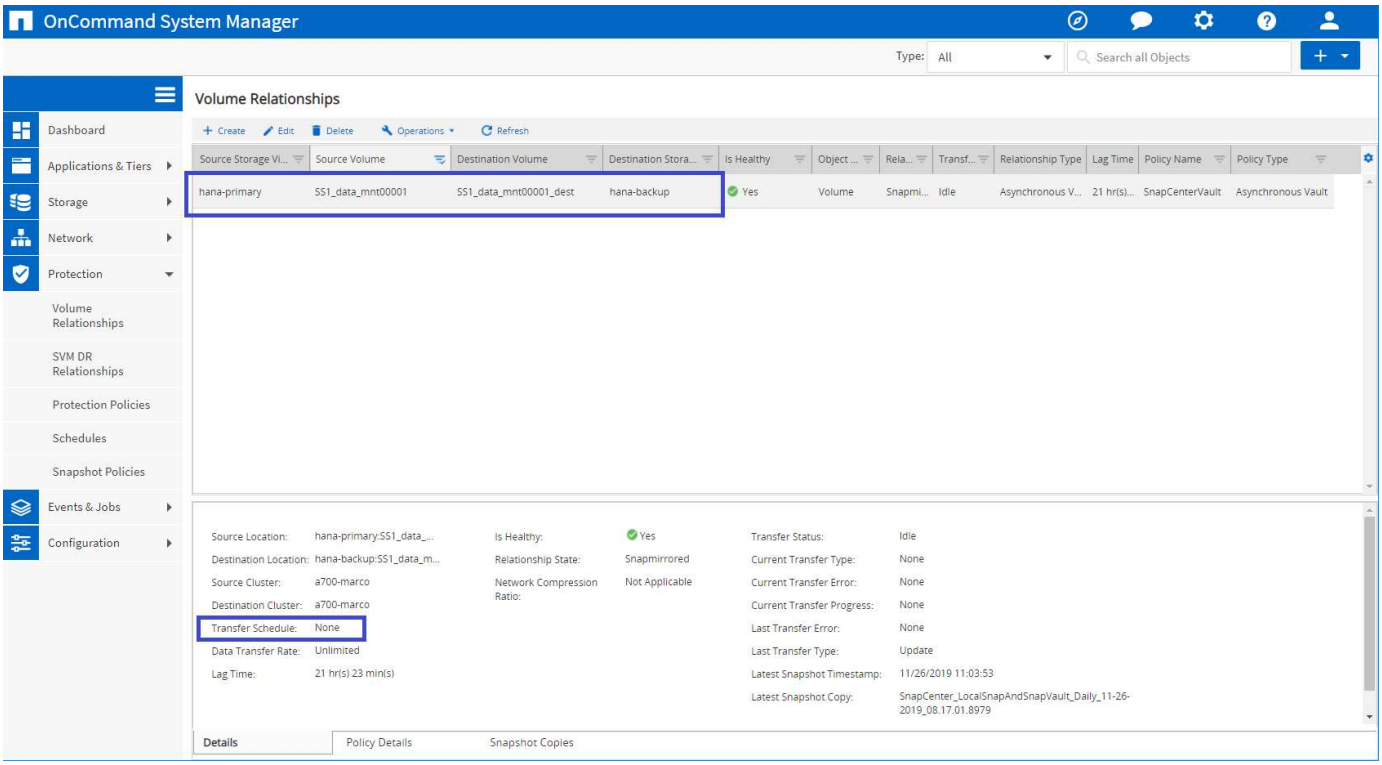
```
hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER
password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE       : 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.

The following figure 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`.

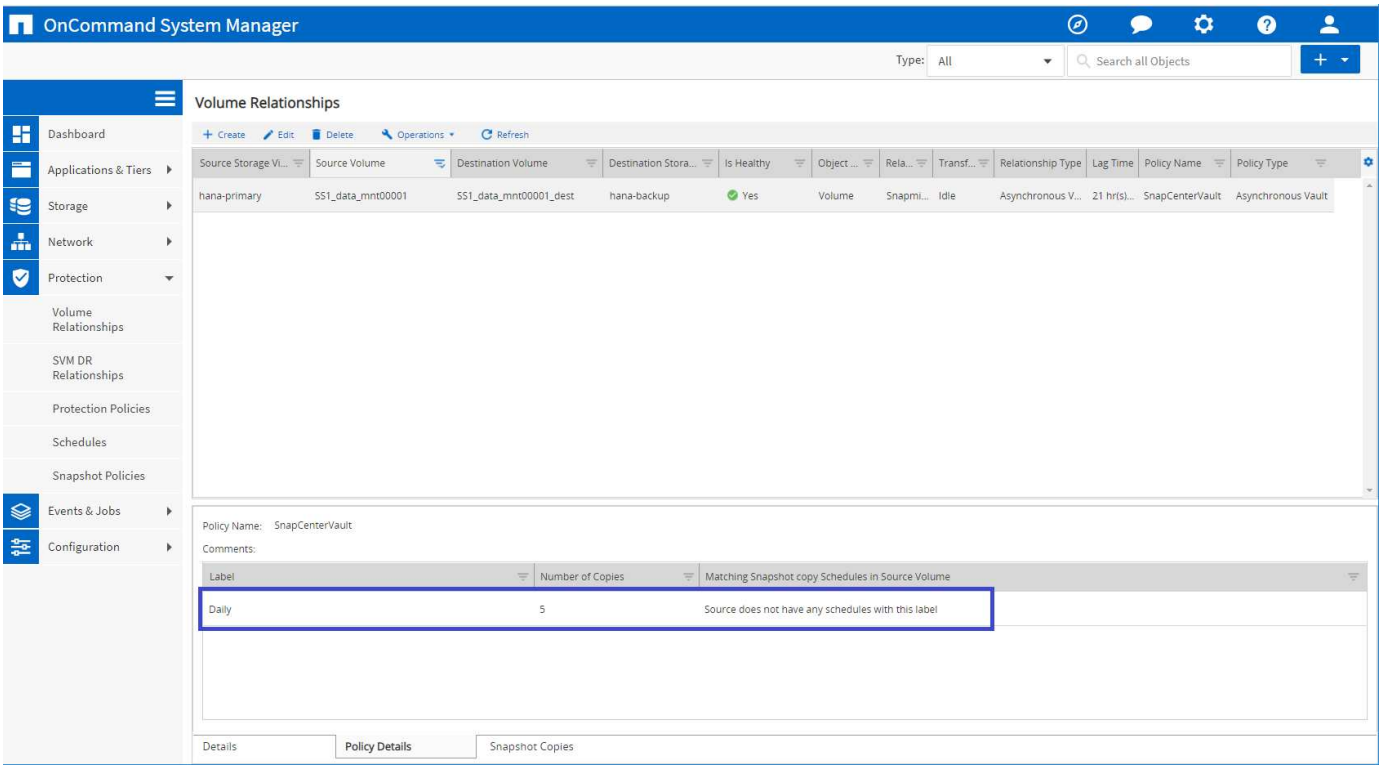
The schedule of the relationship must be set to None, because SnapCenter triggers the SnapVault update.



The following figure 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.

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."

The retention for backups at the off-site backup storage is defined in the policy and controlled by ONTAP.



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.

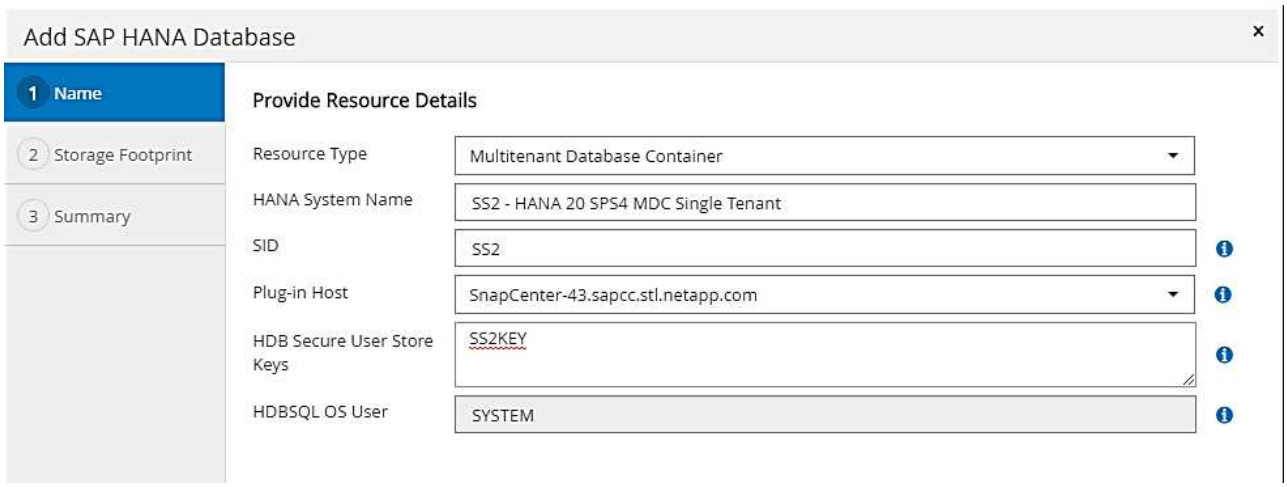
   Select the resource type in our example, Multitenant Database Container.

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

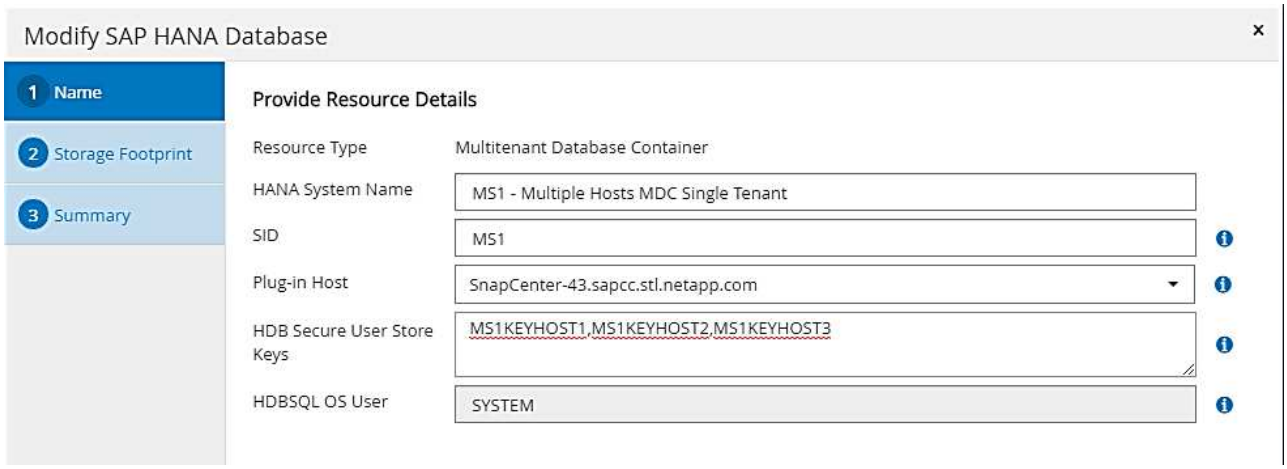
   For our SAP HANA system, the SID is SS2.

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

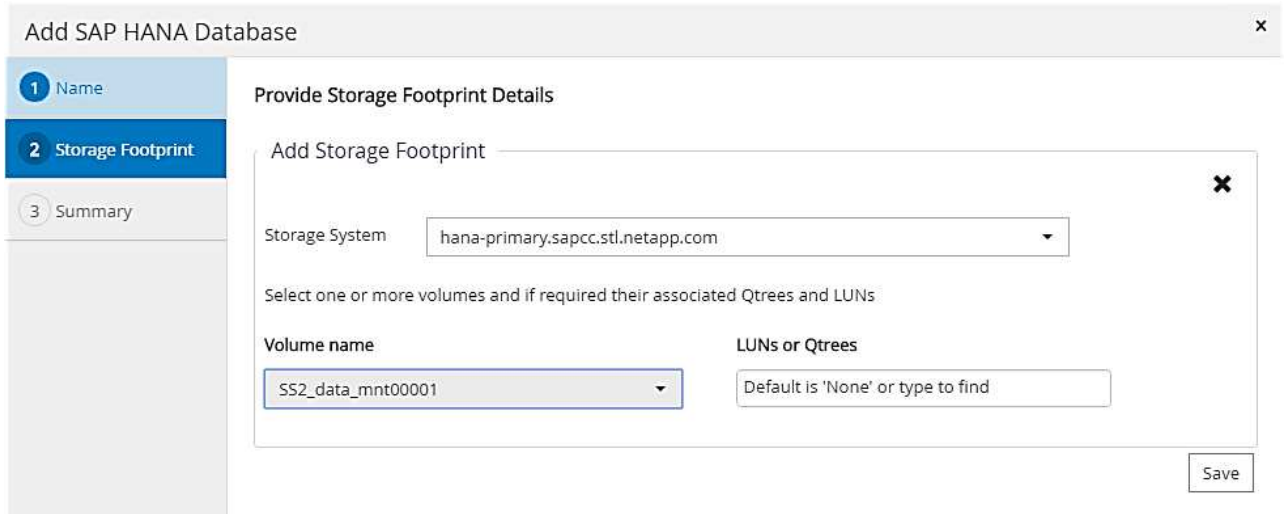
   The hdbuserstore key must match the key that was configured for the HANA database SS2. In our example it is SS2KEY.



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.

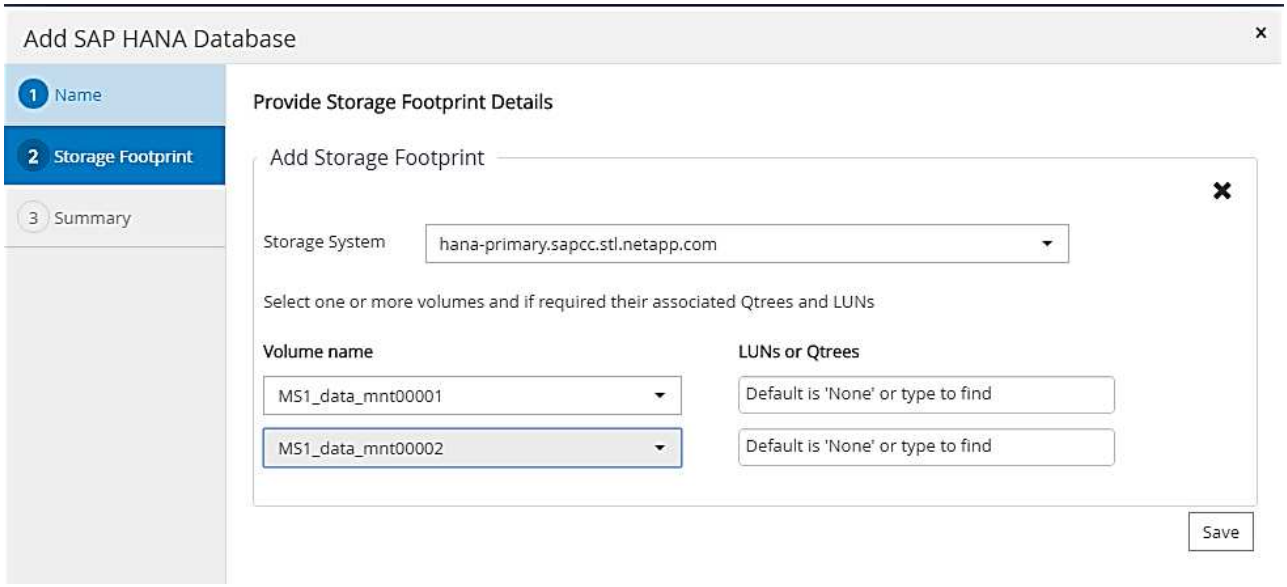


3. Select the required data for the storage system (SVM) and volume name.



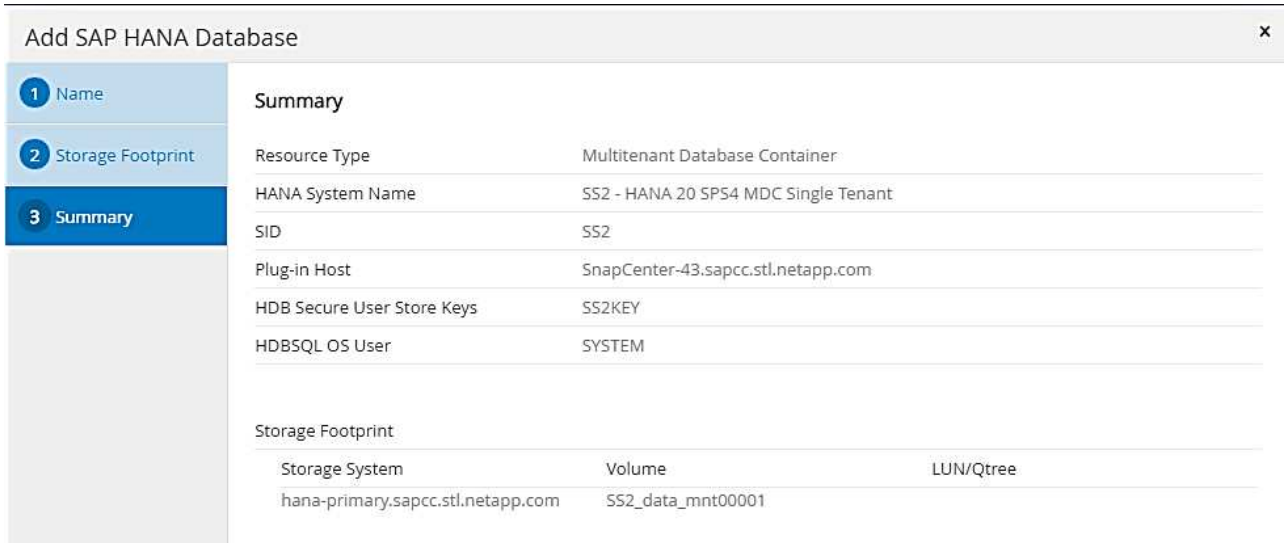
For a Fibre Channel SAN configuration, the LUN needs to be selected as well.

For an SAP HANA multiple-host system, all data volumes of the SAP HANA system must be selected, as shown in the following figure.



The summary screen of the resource configuration is shown.

4. Click Finish to add the SAP HANA database.



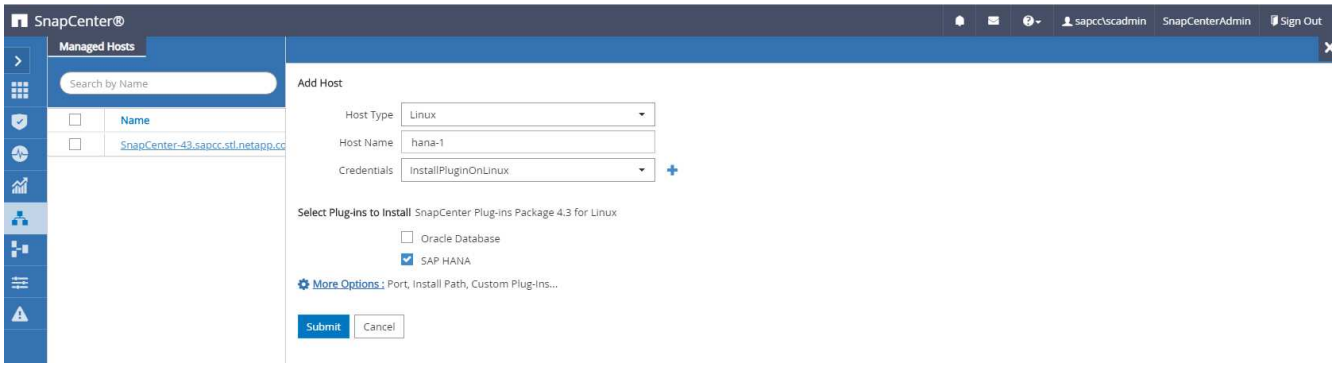
5. When resource configuration is finished, perform the configuration of resource protection as described in the section “Resource protection configuration.”

Automatic discovery of HANA databases

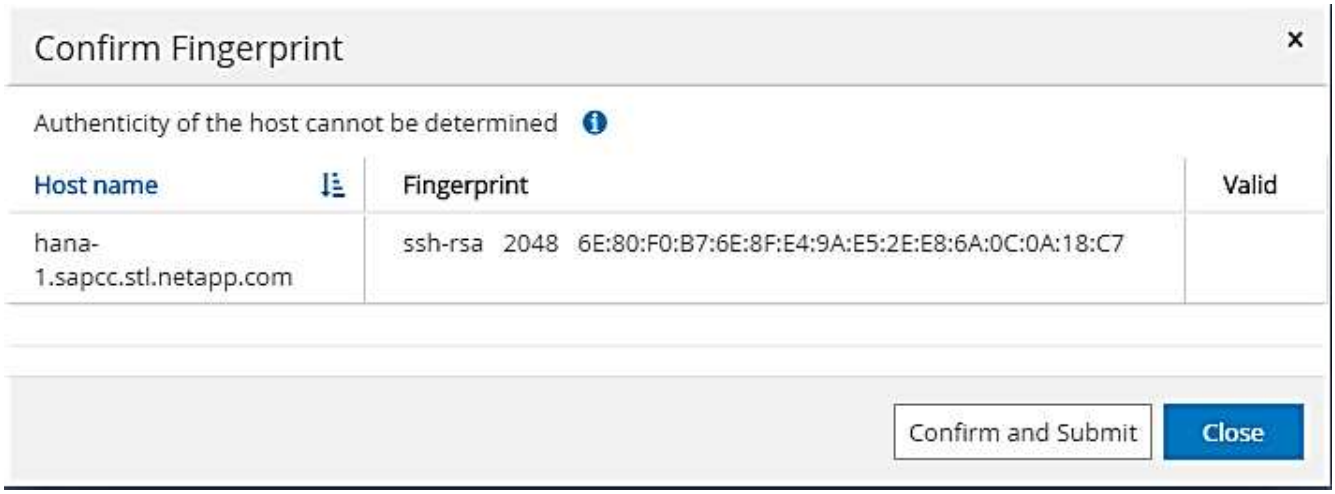
This section describes the automatic discovery of the SAP HANA resource SS1 (single host MDC single tenant system with NFS). All the described steps are identical for a HANA single container, HANA MDC multiple tenants’ systems, and a HANA system using Fibre Channel SAN.

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.

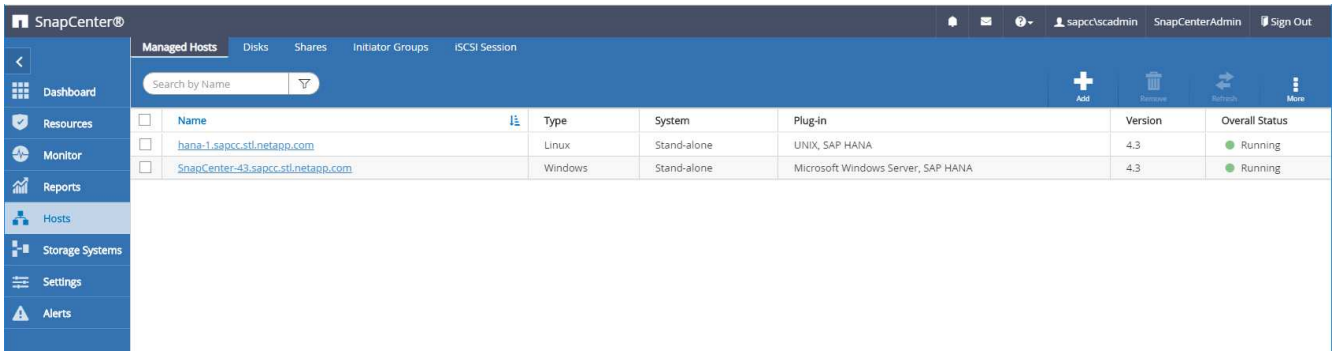
1. From the host tab, click Add.
2. Provide host information and select the SAP HANA plug-in to be installed. Click Submit.



3. Confirm the fingerprint.



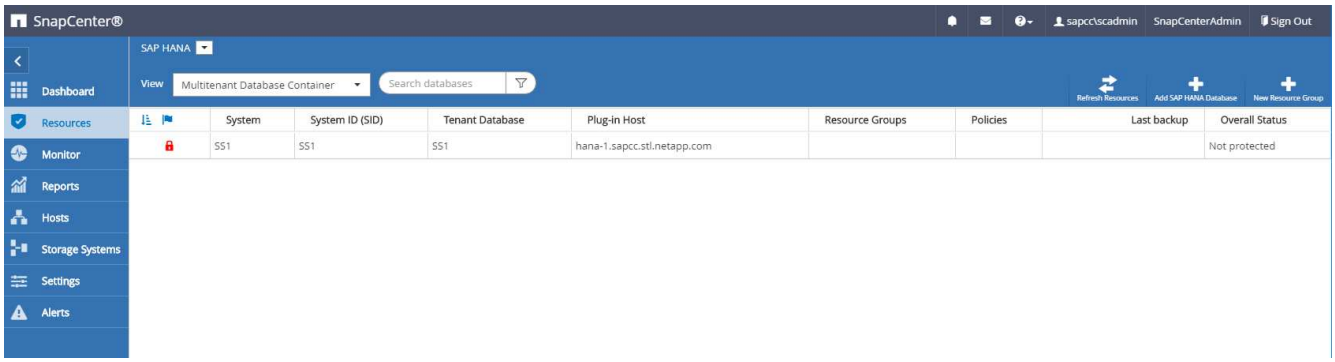
The installation of the HANA plug-in and the Linux plug-in starts automatically. When the installation is finished, the status column of the host shows Running. The screen also shows that the Linux plug-in is installed together with the HANA plug-in.



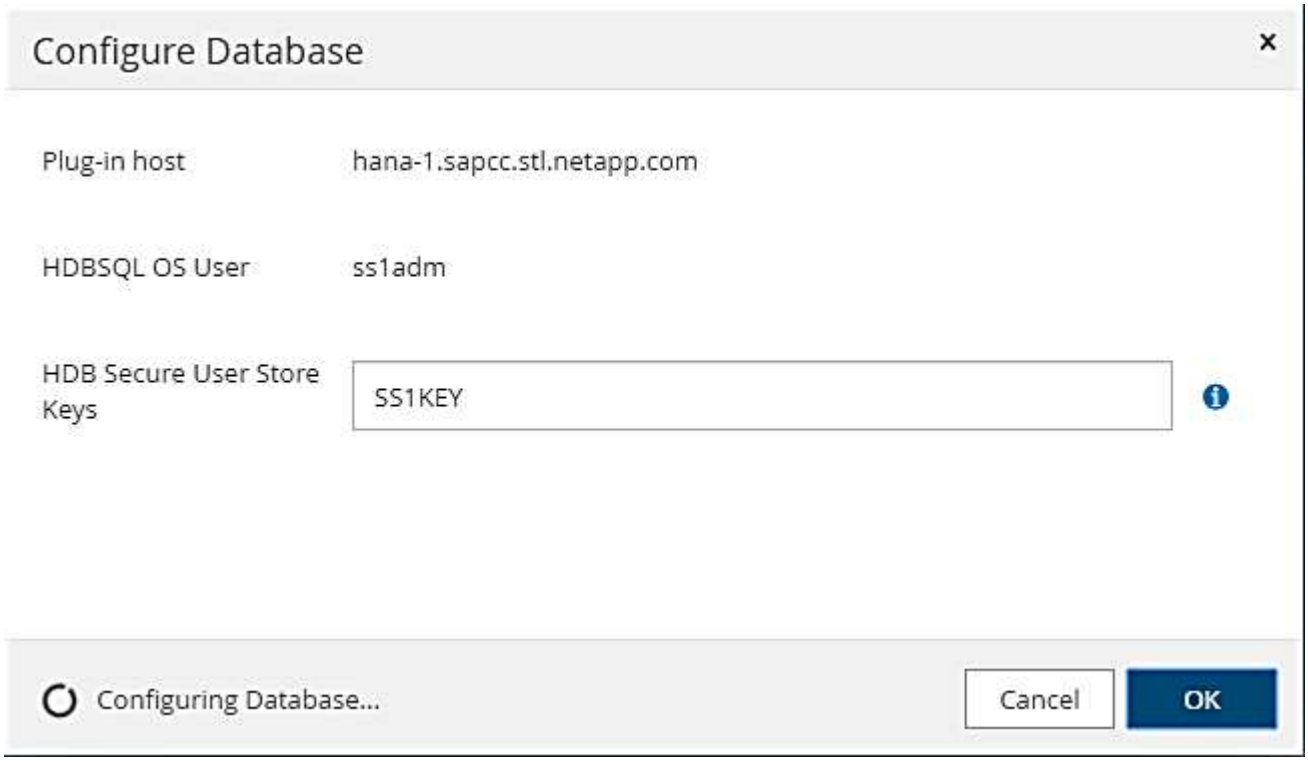
After the plug-in installation, the automatic discovery process of the HANA resource starts automatically. In the Resources screen, a new resource is created, which is marked as locked with the red padlock icon.

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

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

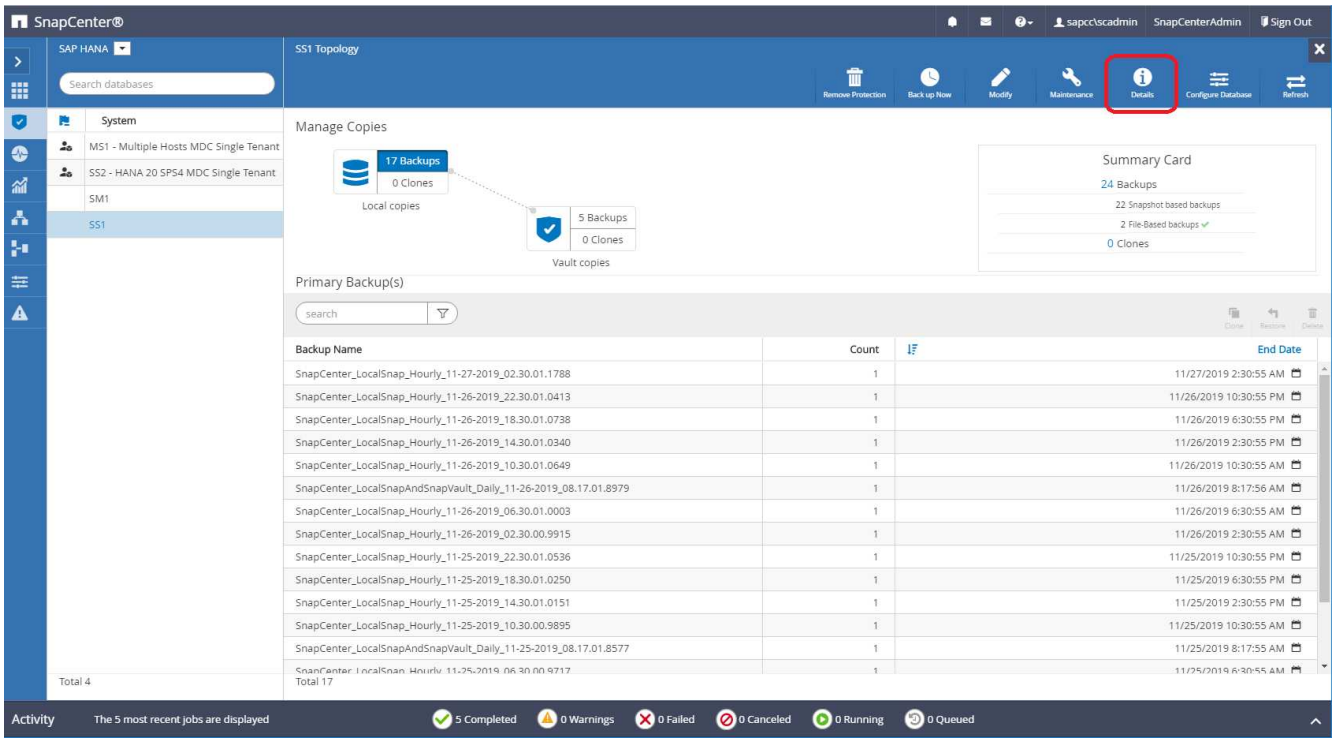


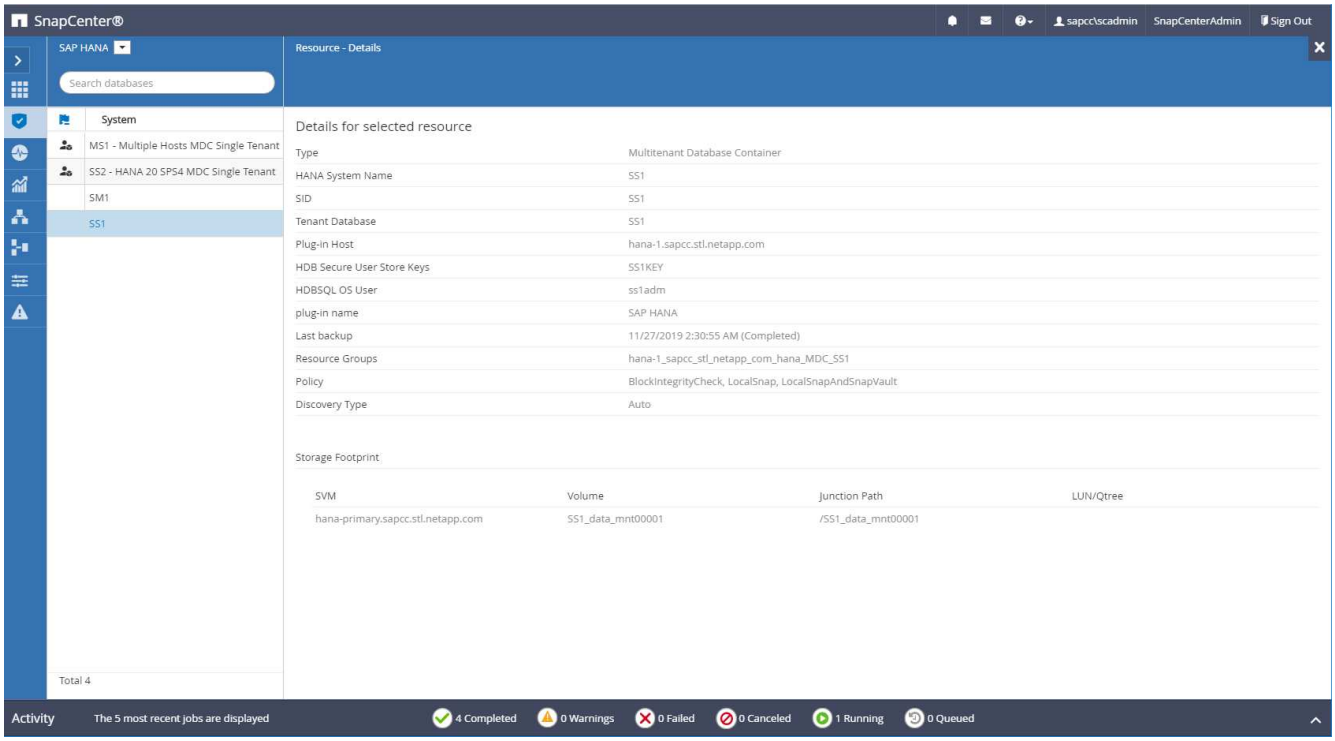
5. Provide the userstore key for the HANA database.



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 following section.

Resource protection configuration

This section describes the resource protection configuration. The resource protection configuration is the same, whether 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.

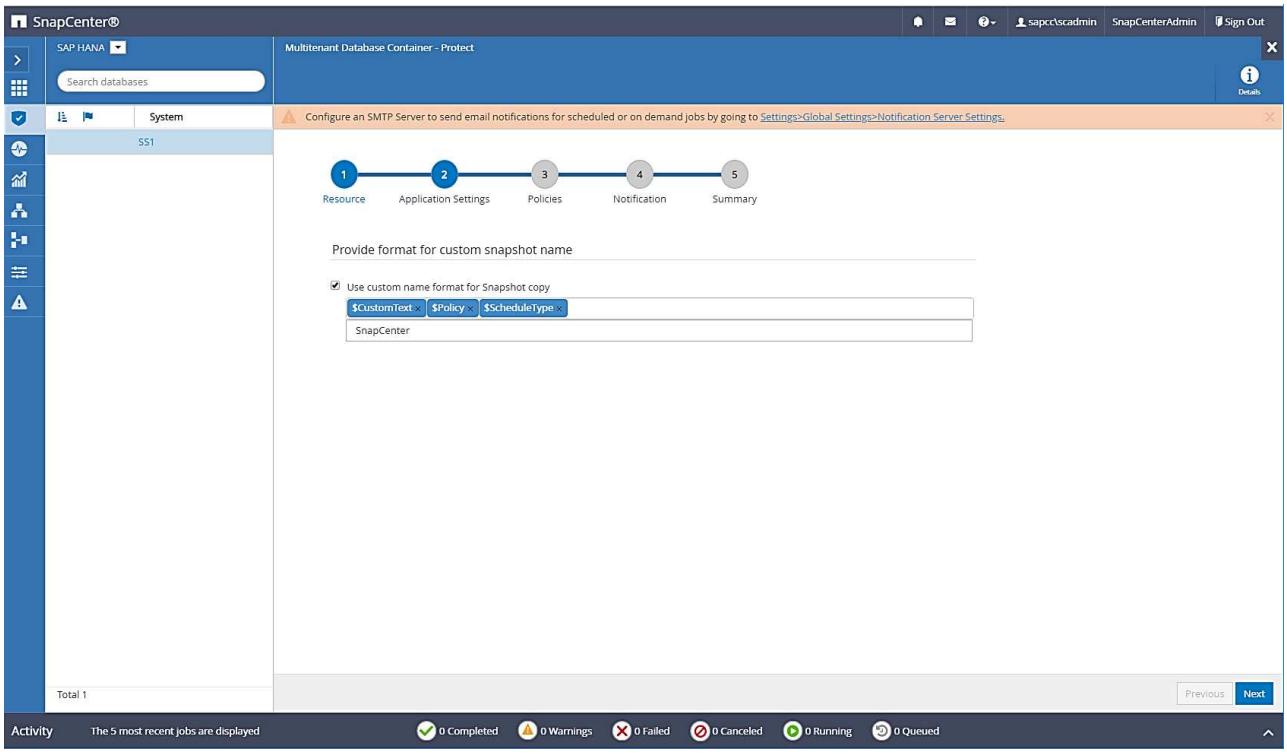
1. From the Resources tab, double-click the resource.
2. Configure a custom name format for the Snapshot copy.

> 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`.

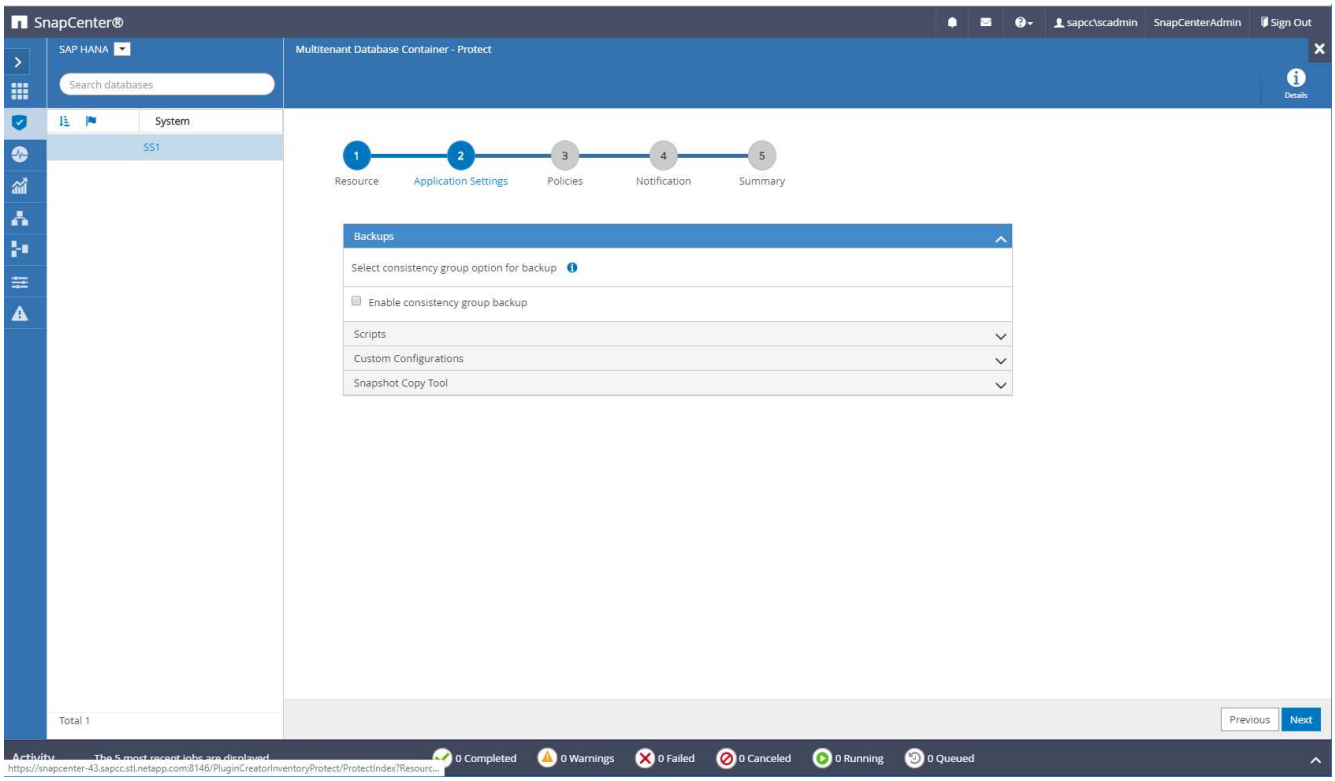
In the configuration shown in the following figure, the backup and Snapshot copy names have the following format:

- 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>`

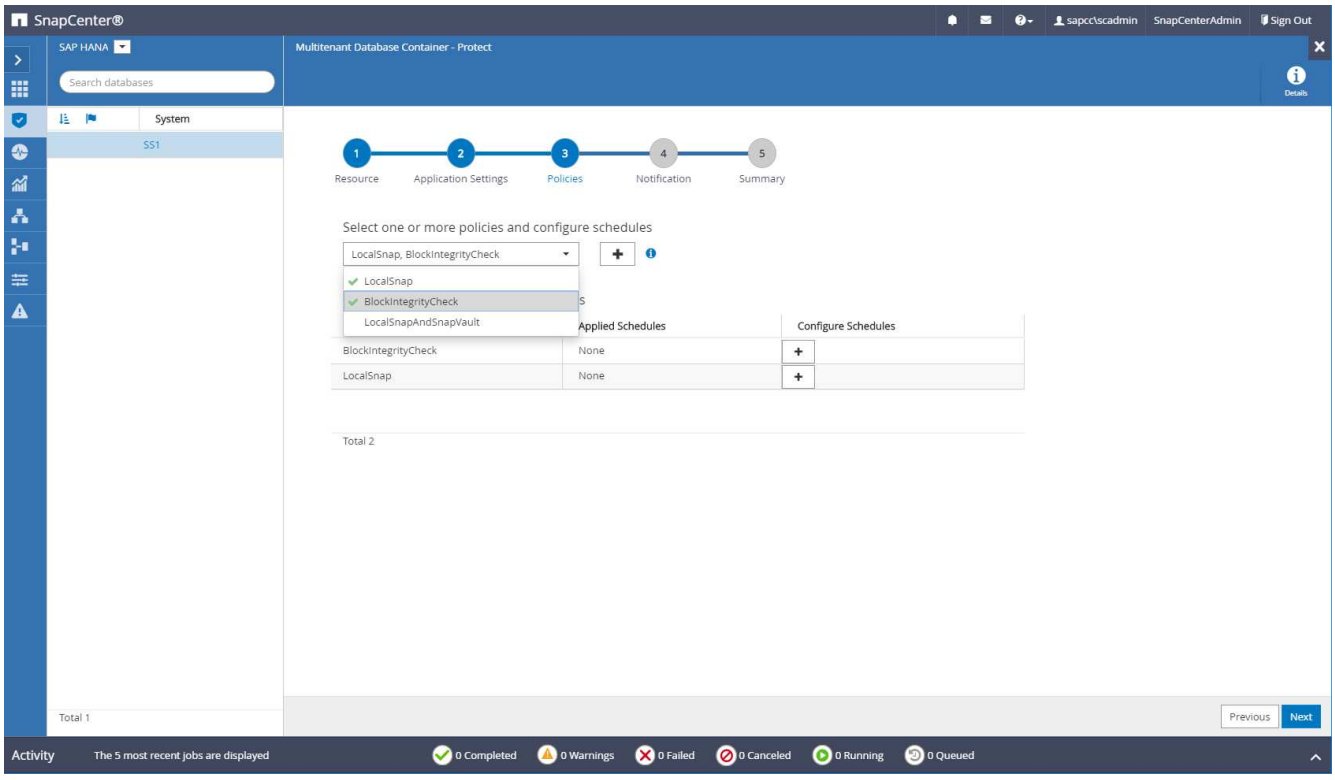
> Even though a retention is defined for on-demand backups in the policy configuration, the housekeeping is only done when another on-demand backup is executed. Therefore, on-demand backups must typically be deleted manually in SnapCenter to make sure that these backups are also deleted in the SAP HANA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



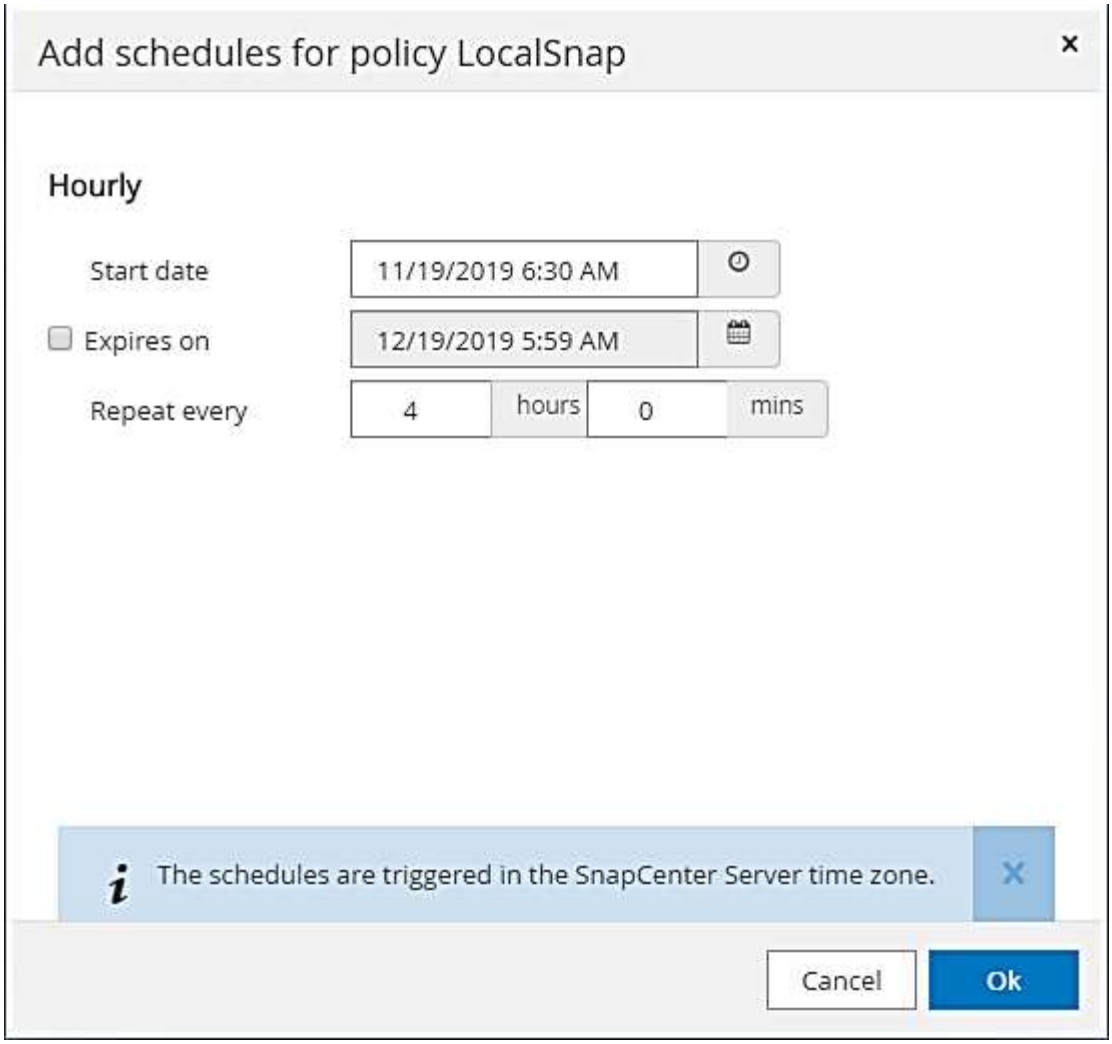
3. No specific setting needs to be made on the Application Settings page. Click Next.



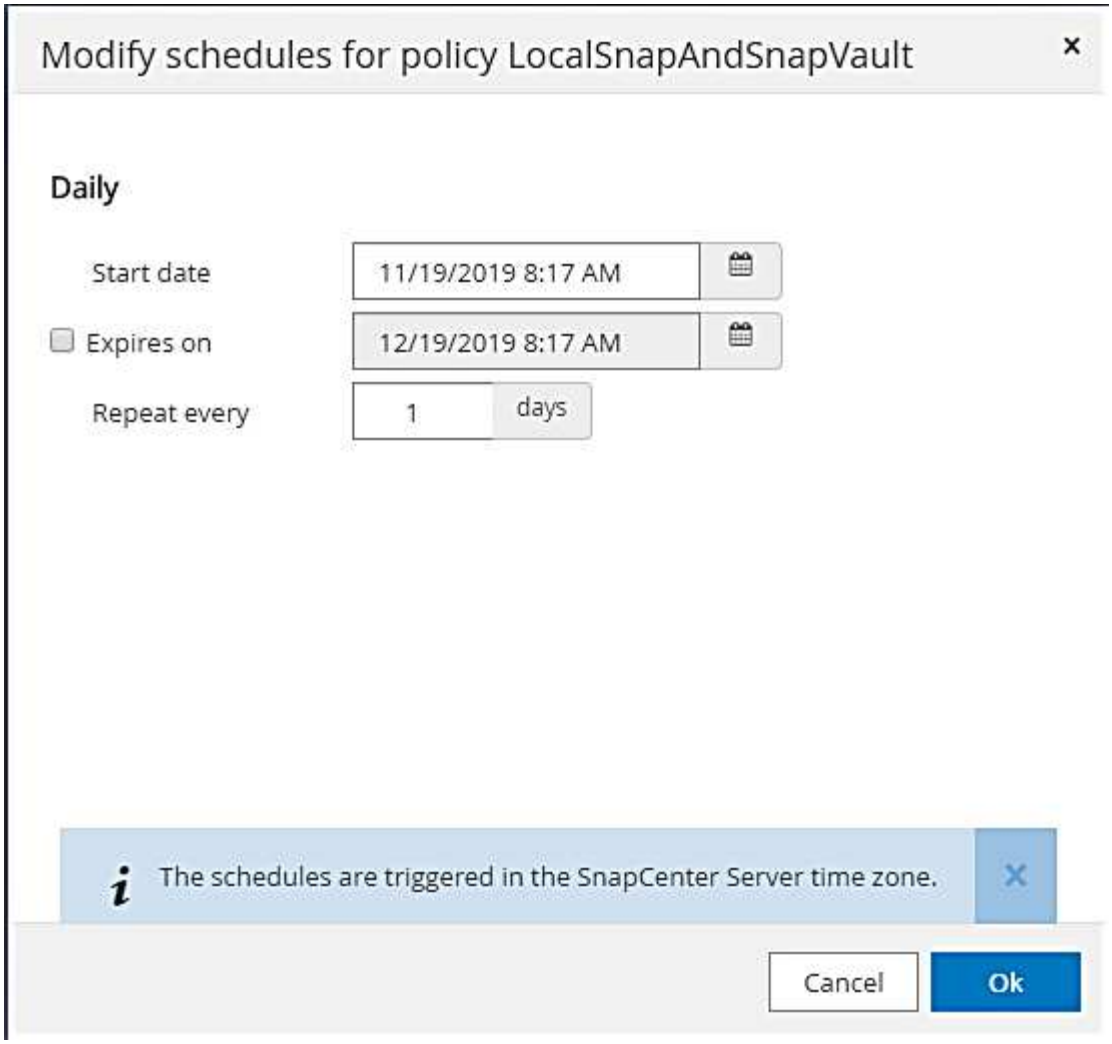
4. Select the policies to add to the resource.



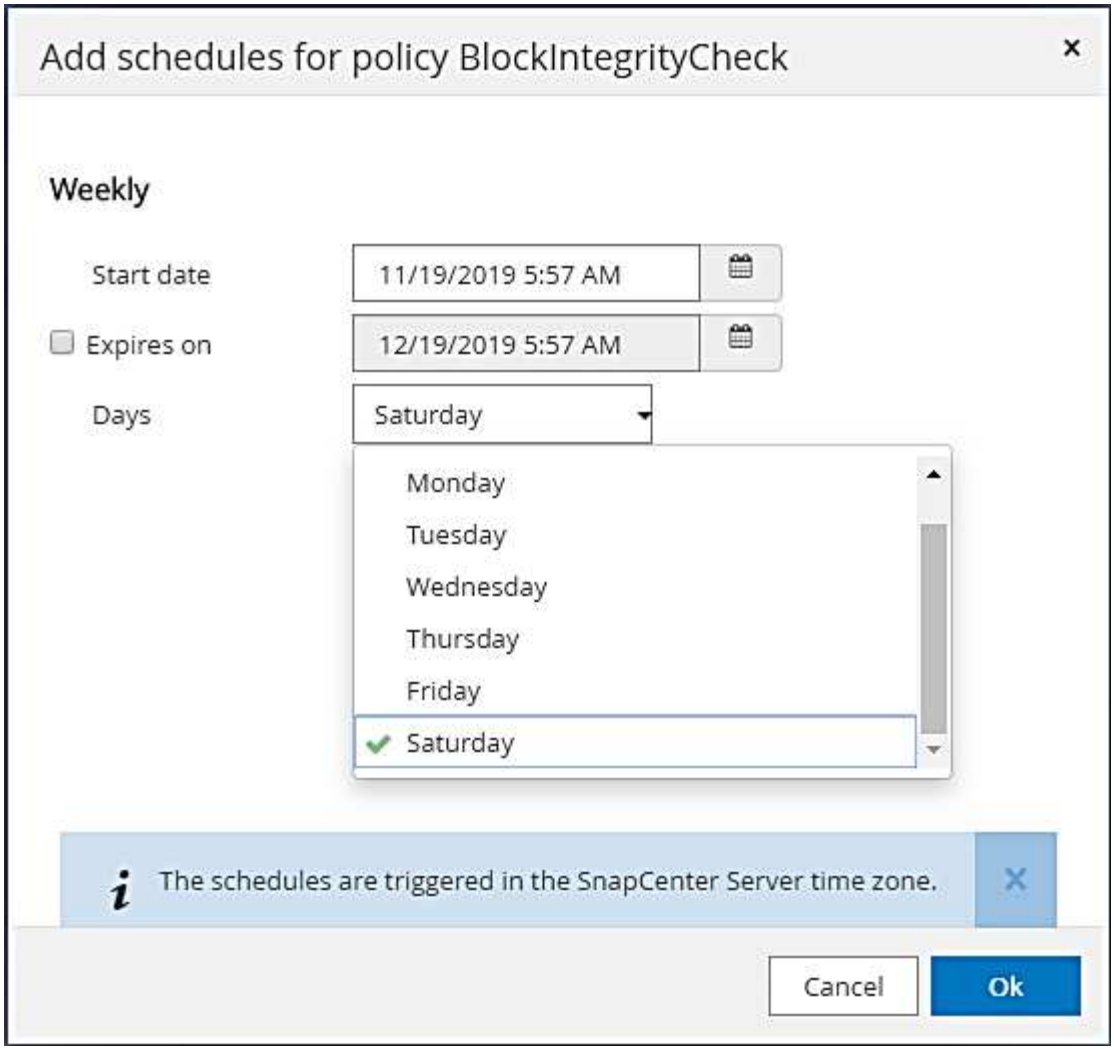
5. Define the schedule for the LocalSnap policy (in this example, every four hours).



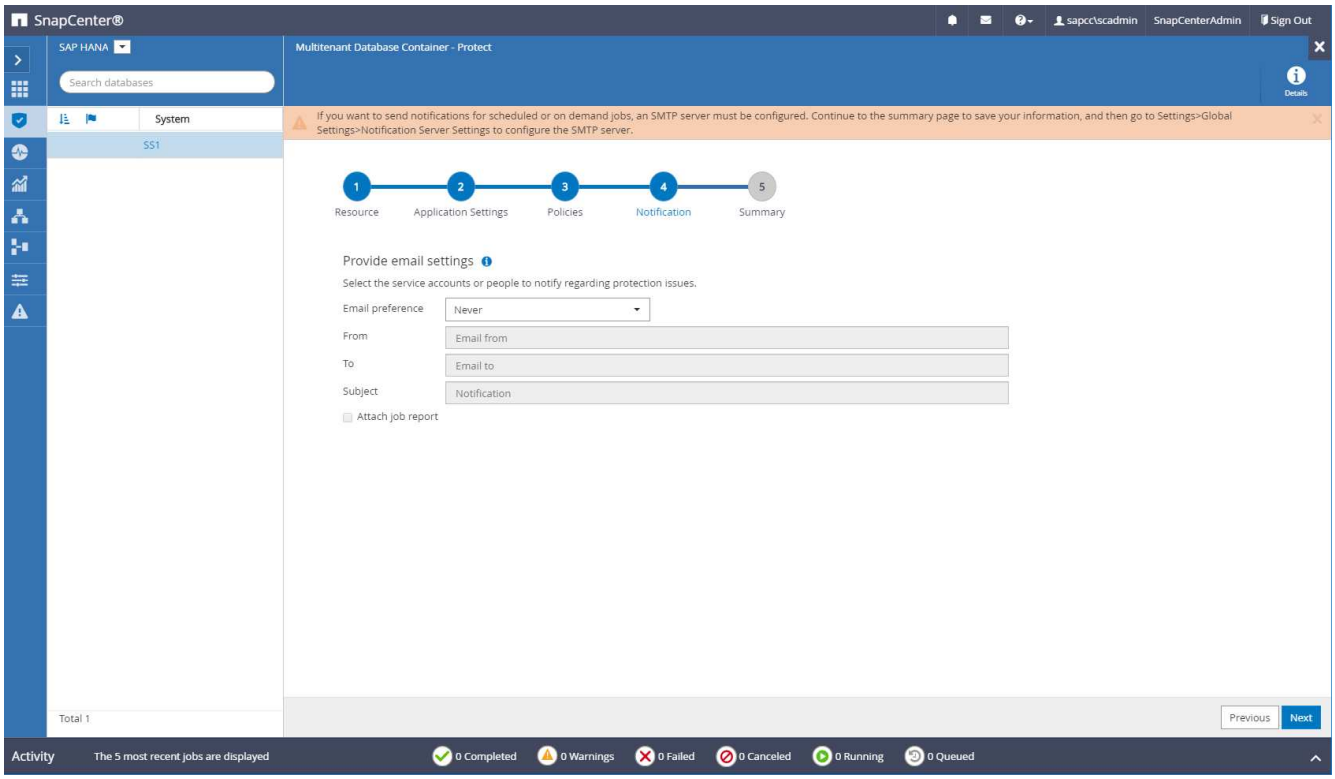
6. Define the schedule for the LocalSnapAndSnapVault policy (in this example, once per day).



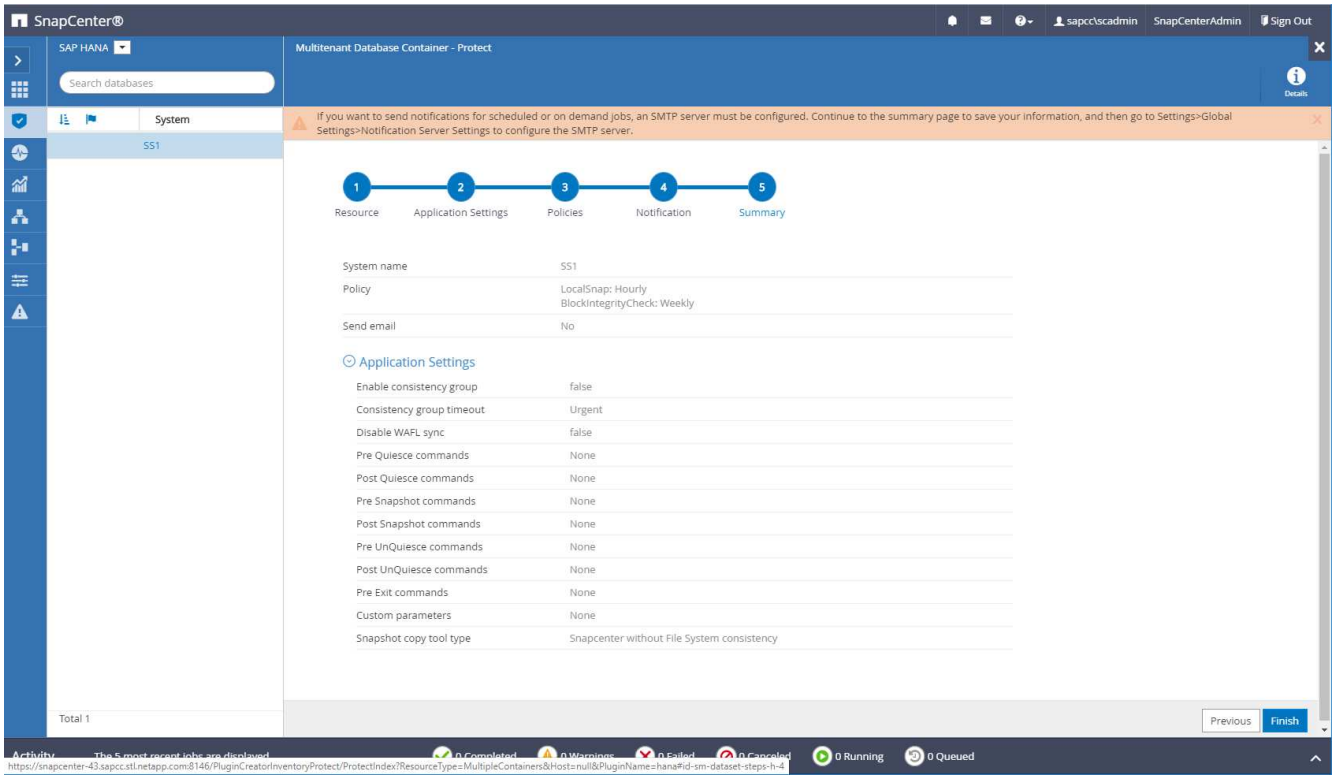
7. Define the schedule for the block integrity check policy (in this example, once per week).



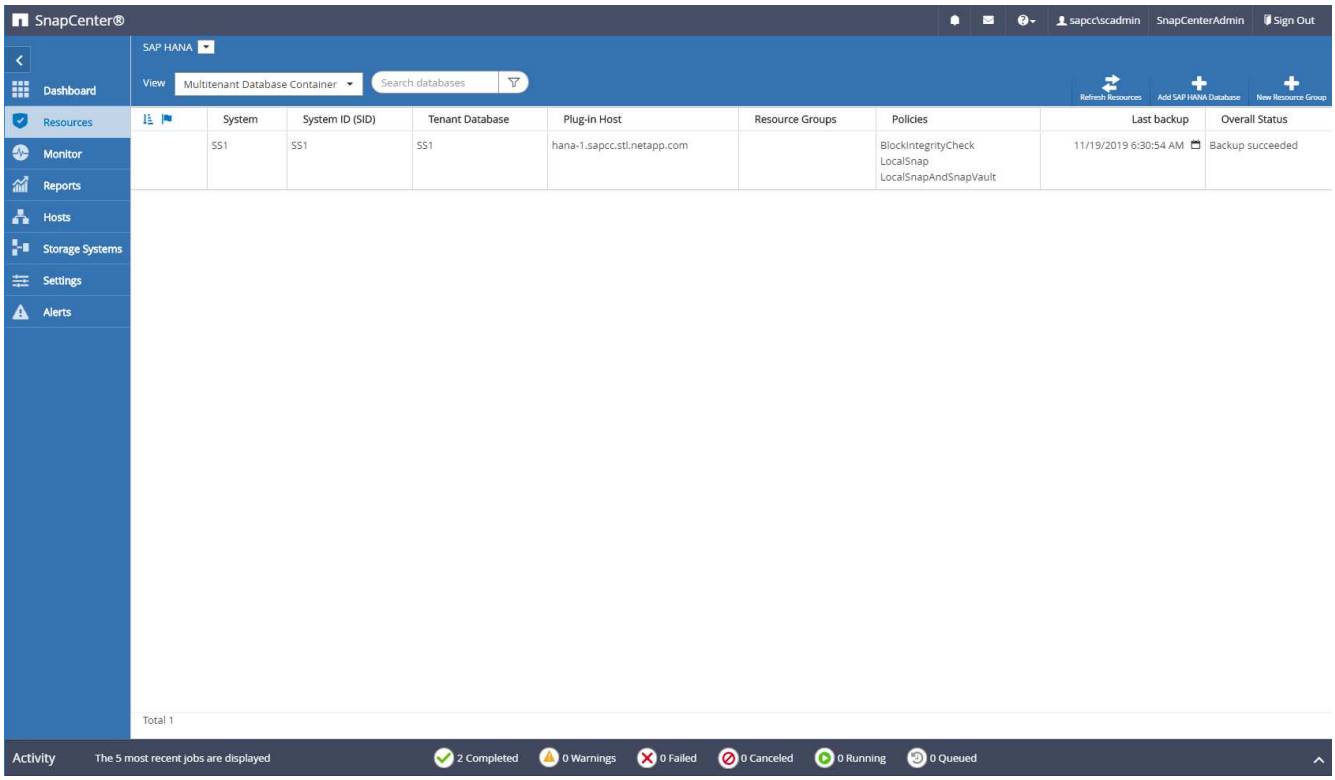
8. Provide information about the email notification.



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.



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.

> 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 as a last step (for example, `/hana/data/SID/mnt00001/hdb00001/snapshot_databackup_0_1`). 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.

> 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.

> 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.

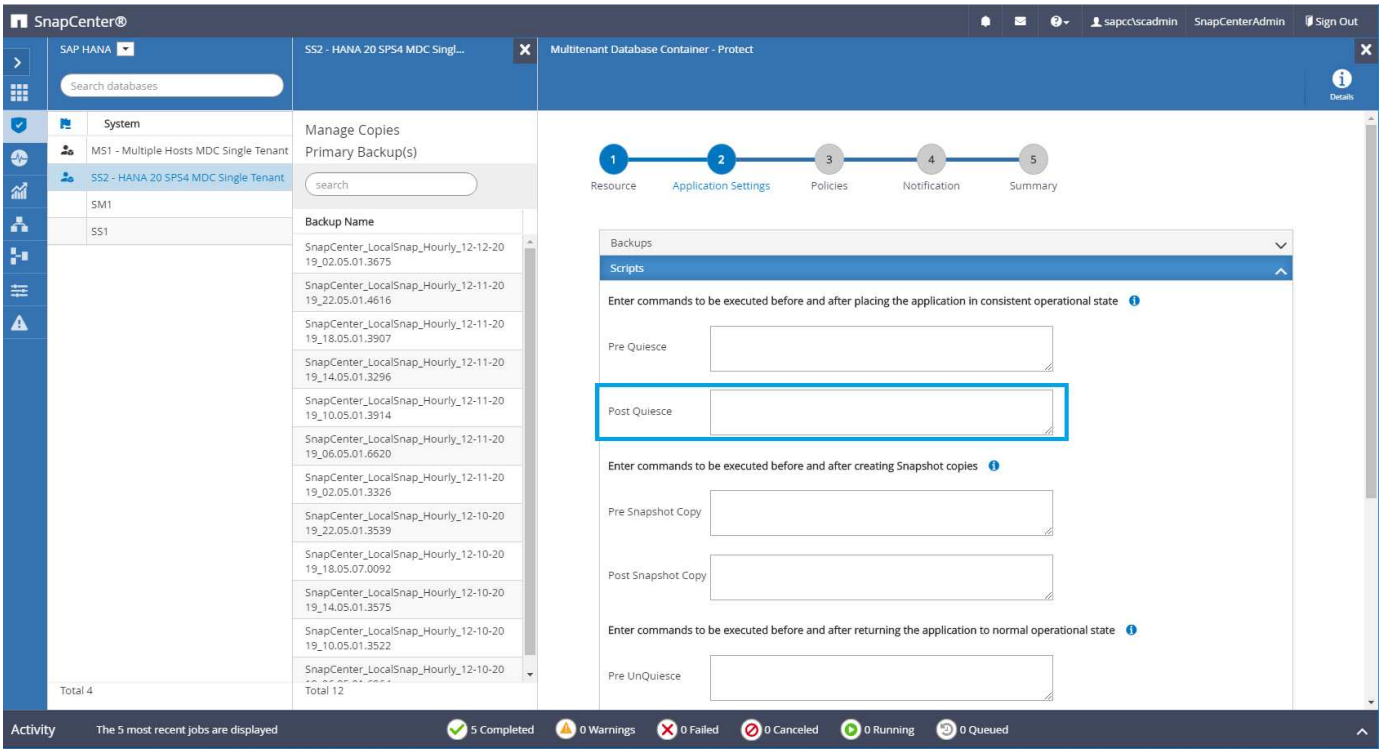
If the SnapCenter server is used as a central HANA plug-in host, a batch file can be used. The batch file must have the following content:

```
@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, you must configure the command `/bin/sleep 60` as the Post Quiesce command in the SnapCenter UI.

The following figure shows the Post Quiesce command within the resource protection configuration screen.



SnapCenter resource-specific configuration for non-data volume backups

The backup of non-data 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.

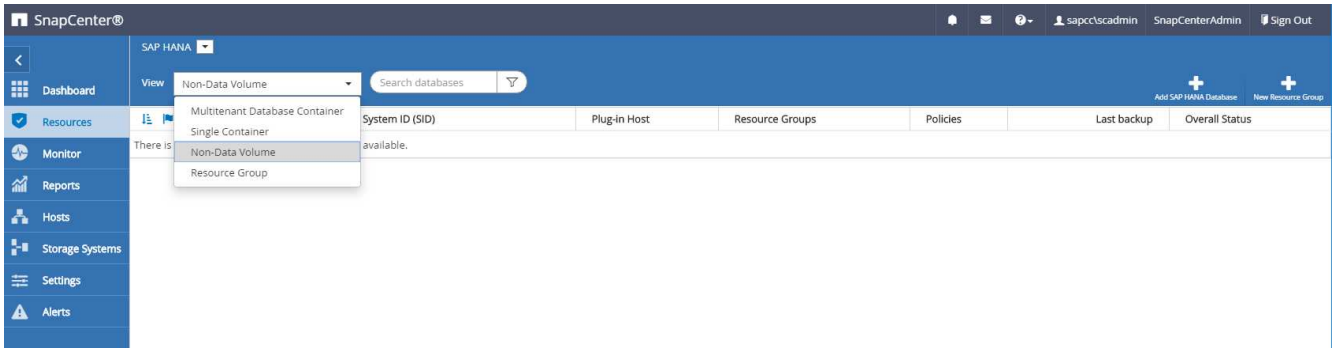
To recover from situations where other non-data files must be restored, NetApp recommends developing an additional backup strategy for non-data volumes to augment the SAP HANA database backup. Depending on your specific requirements, the backup of non-data volumes might differ in scheduling frequency and retention settings, and you should consider how frequently non-data 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 non-data volume backup enables Snapshot copies of all relevant volumes to be created in a few seconds with the same space efficiency as SAP HANA database backups. The difference is that there is no SQL communication with SAP HANA database required.

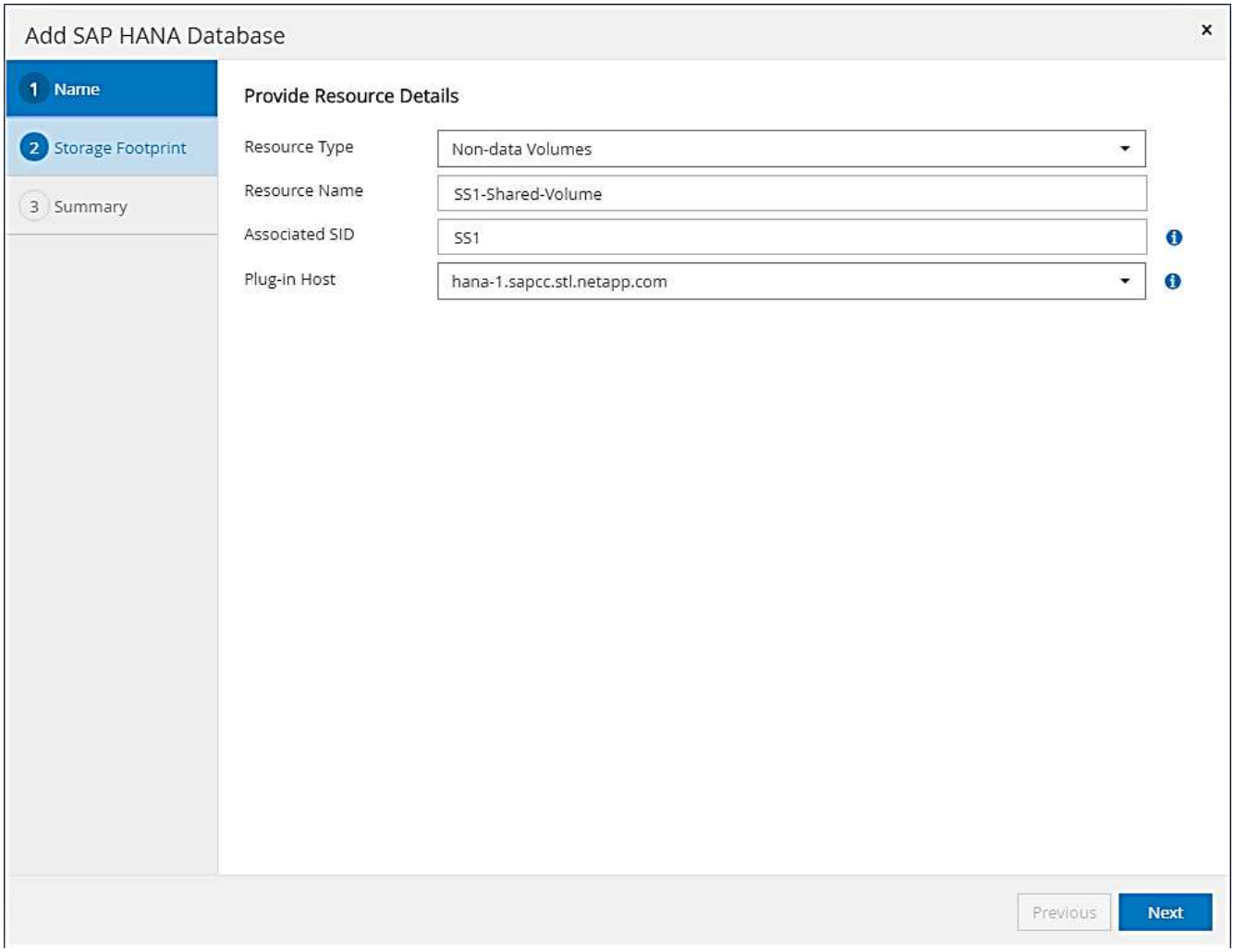
Configuration of non-data volume resources

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

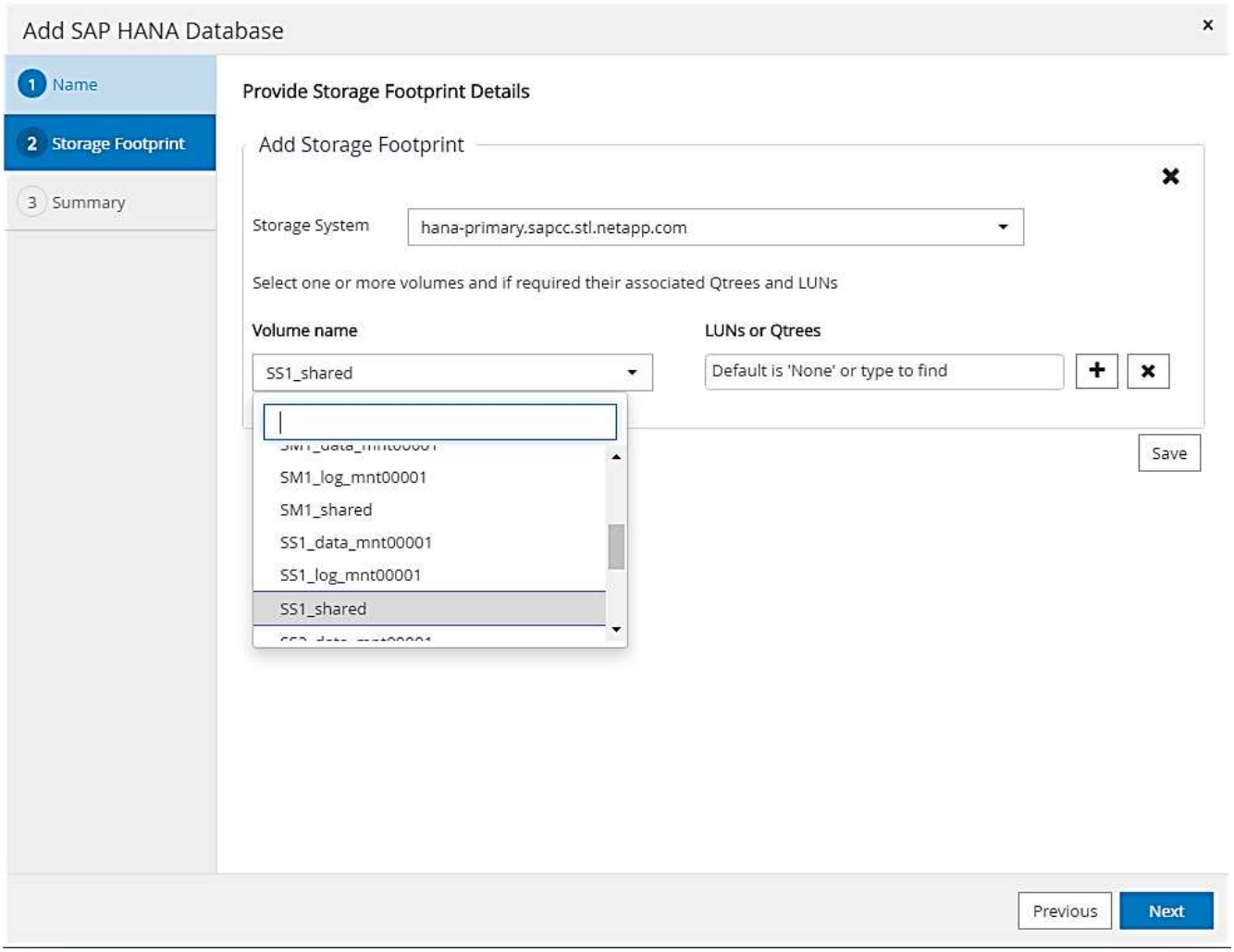
1. From the Resource tab, select Non-Data-Volume and click Add SAP HANA Database.



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.



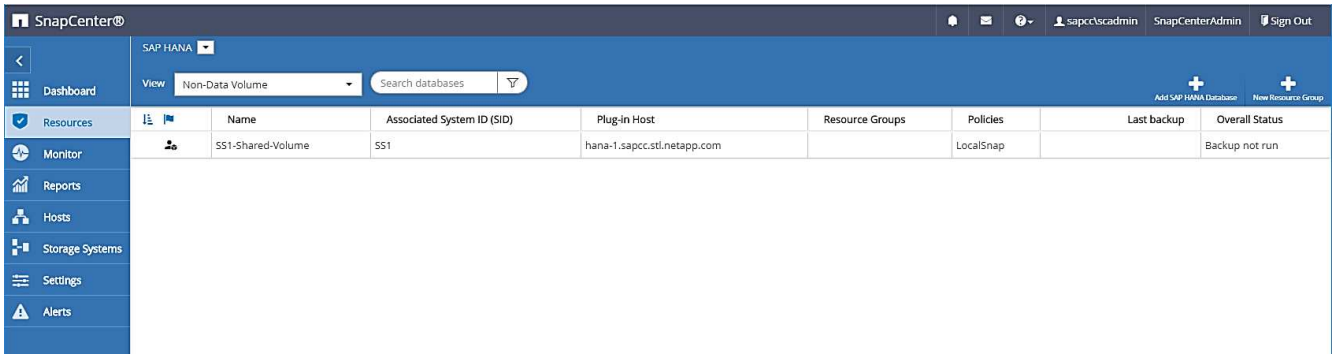
3. Add the SVM and the storage volume as storage footprint, then click Next.



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

> Data protection for a non- data volume resources is identical to the workflow for SAP HANA database resources and can be defined on an individual resource level.

The following figure shows the list of the configured non-data volume resources.



Resource groups

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

Resource groups provide the following features:

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

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.

In normal backup operations, NetApp does not recommend including 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.

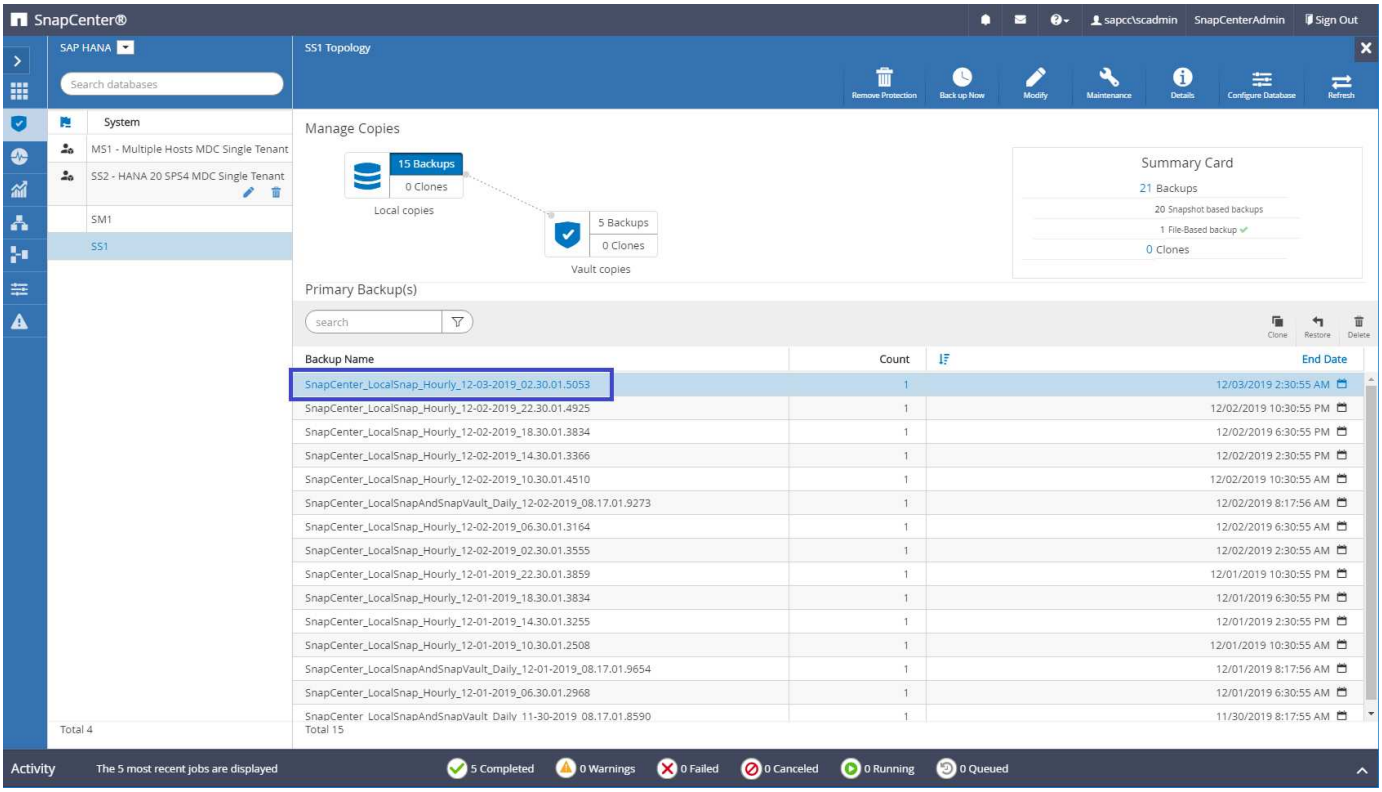
Database backups

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. The following figure shows the backups available on the primary storage and highlights the most recent backup.

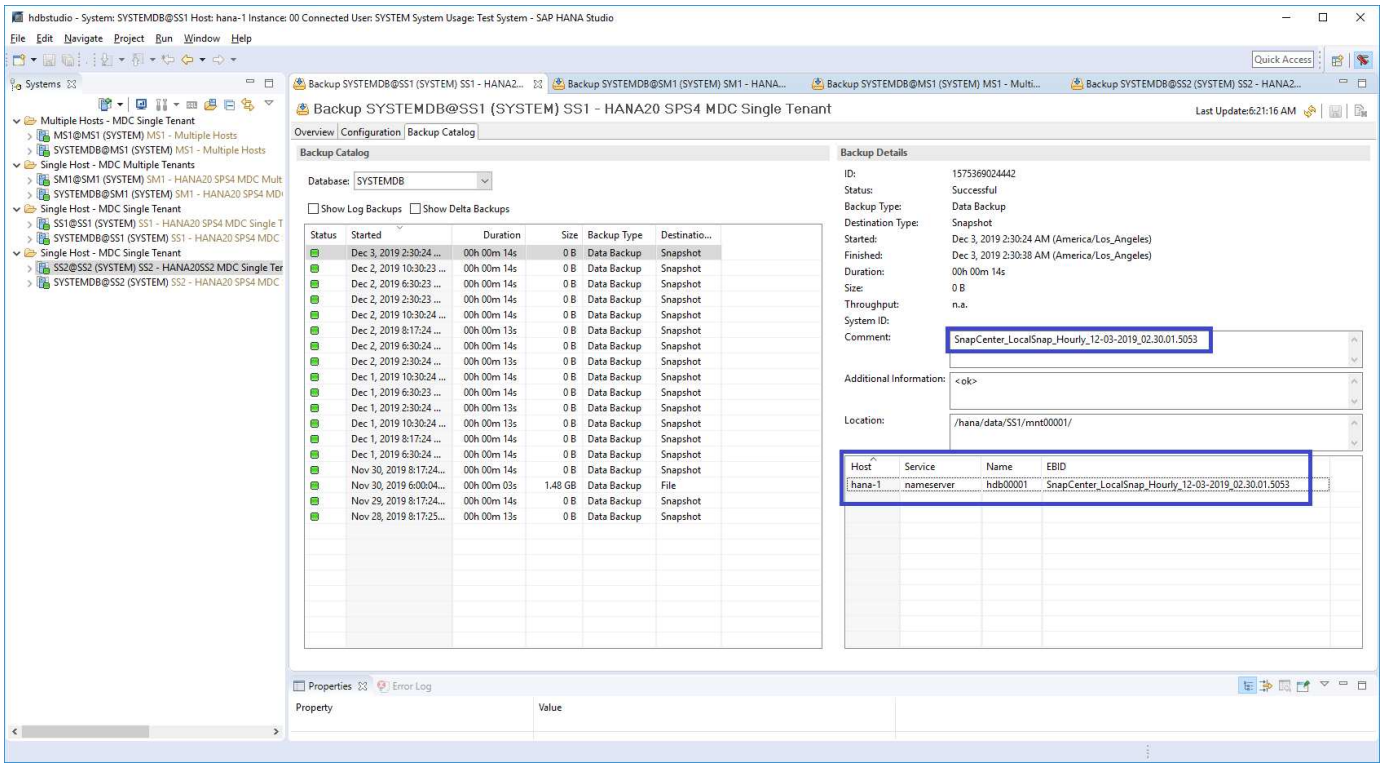


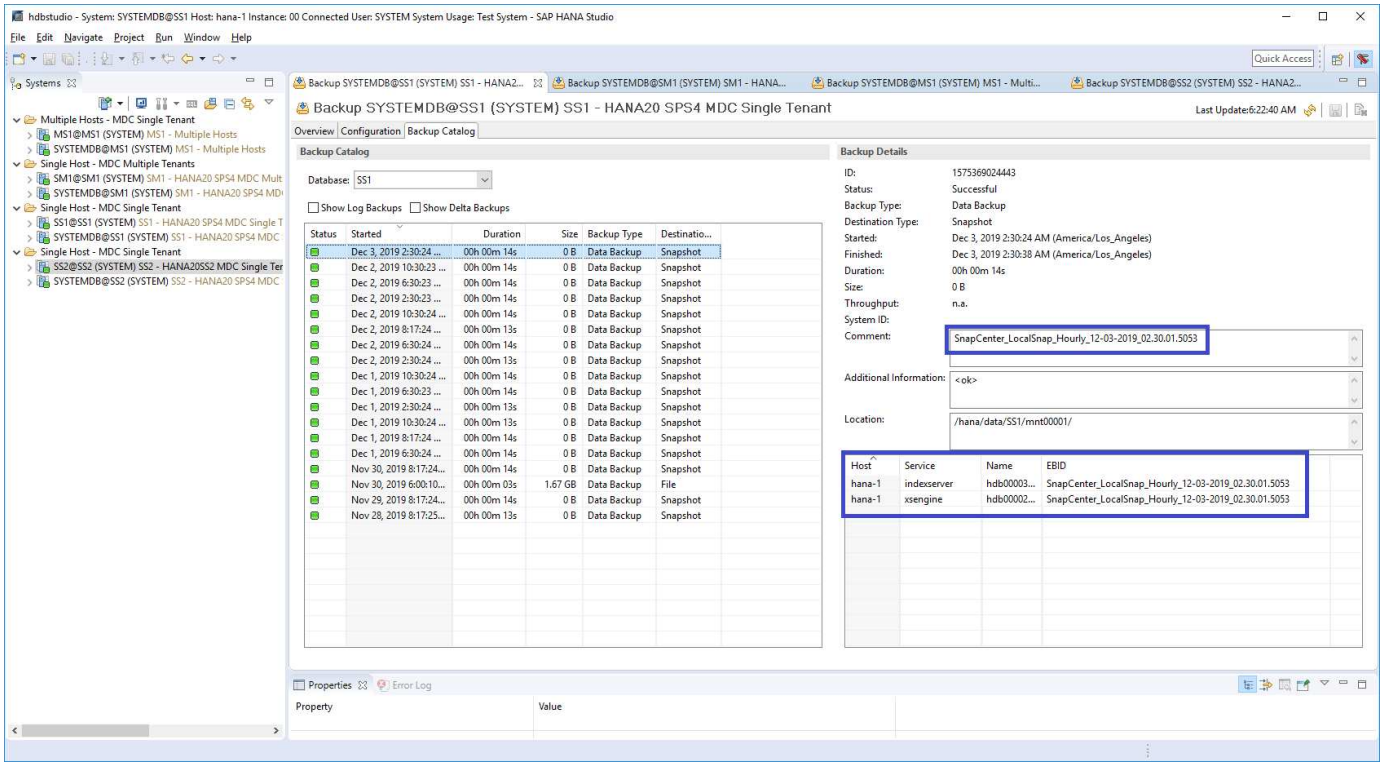
When performing a backup using storage Snapshot copies for an SAP HANA MDC system, a Snapshot copy of the data volume is created. This data volume contains the data of the system database as well as the data of all tenant databases. To reflect this physical architecture, SAP HANA internally performs 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.

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 the following screenshot for the system database and in the screenshot after that for the tenant database SS1. Both figures highlight the SnapCenter backup name stored in the comment field and EBID.

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.

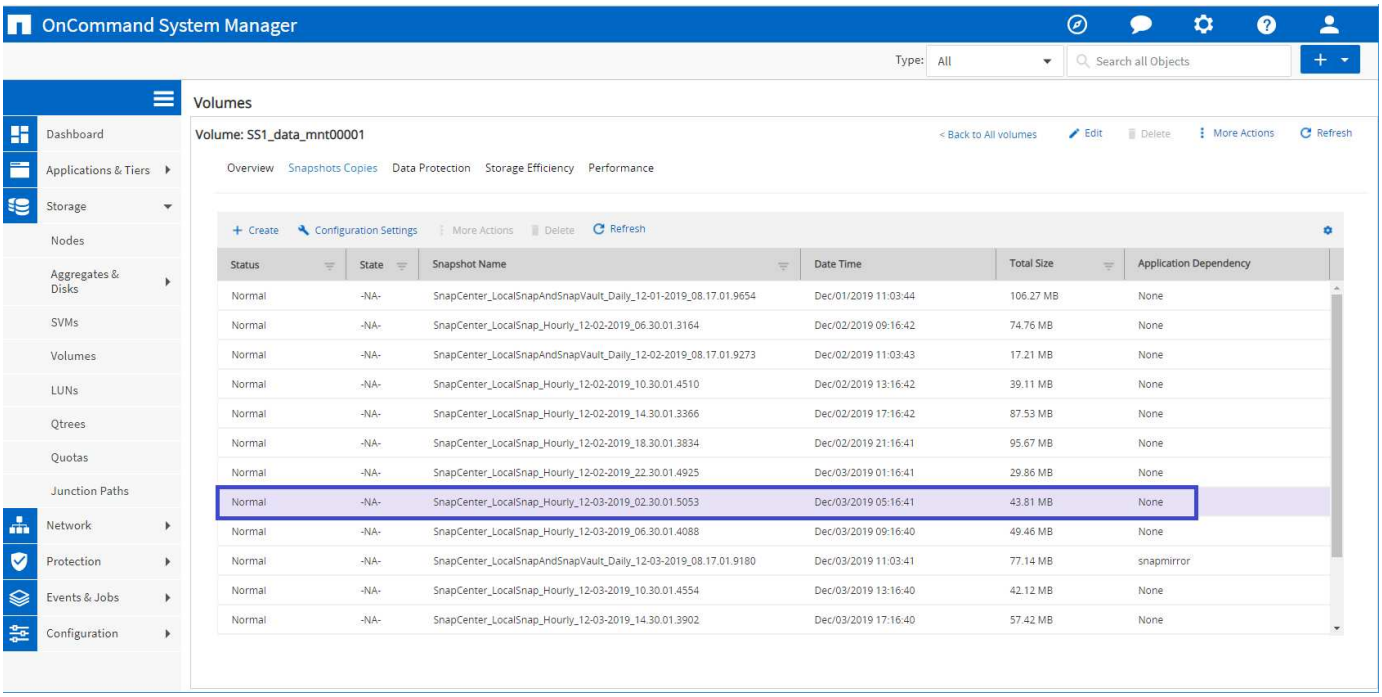




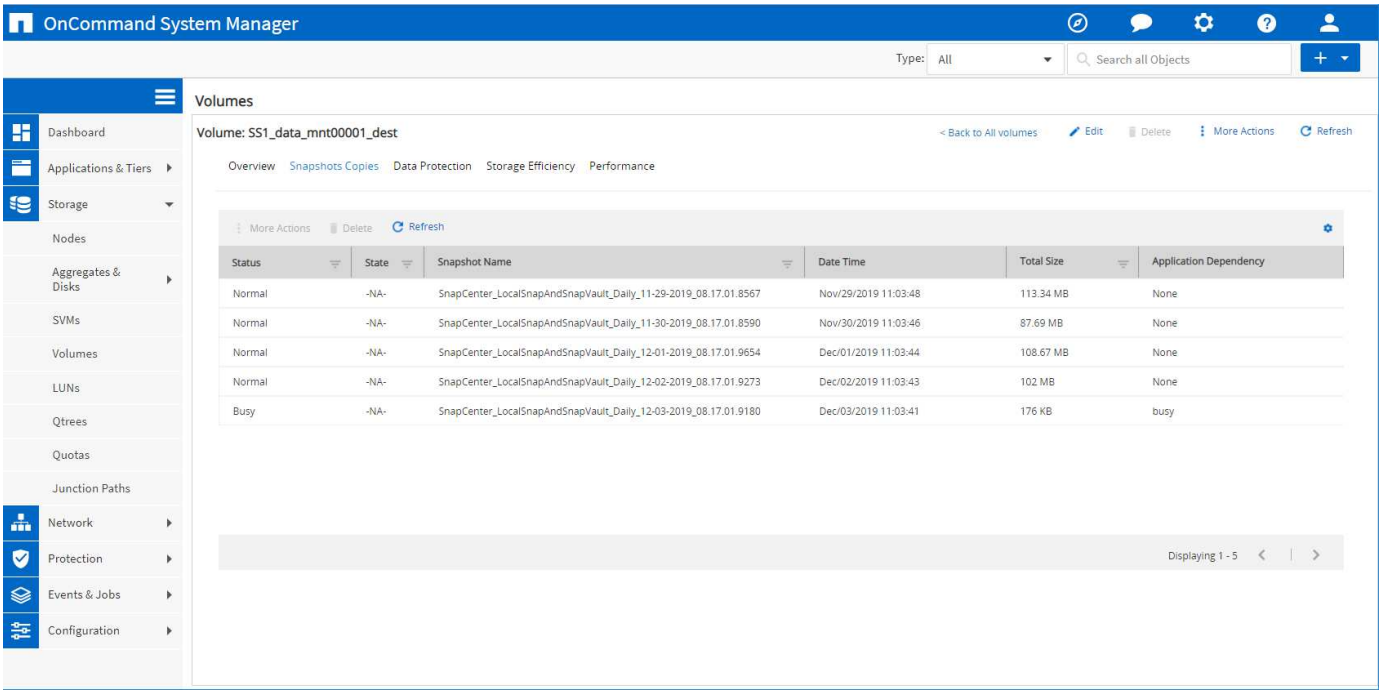
SnapCenter is only aware of its own backups. Additional backups created, for example, with SAP HANA Studio, are visible in the SAP HANA catalog but not in SnapCenter.

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. The following screenshot shows the available backups for the database volume `SS1_data_mnt00001` at the primary storage. The highlighted backup is the backup shown in SnapCenter and SAP HANA Studio in the previous images and has the same naming convention.



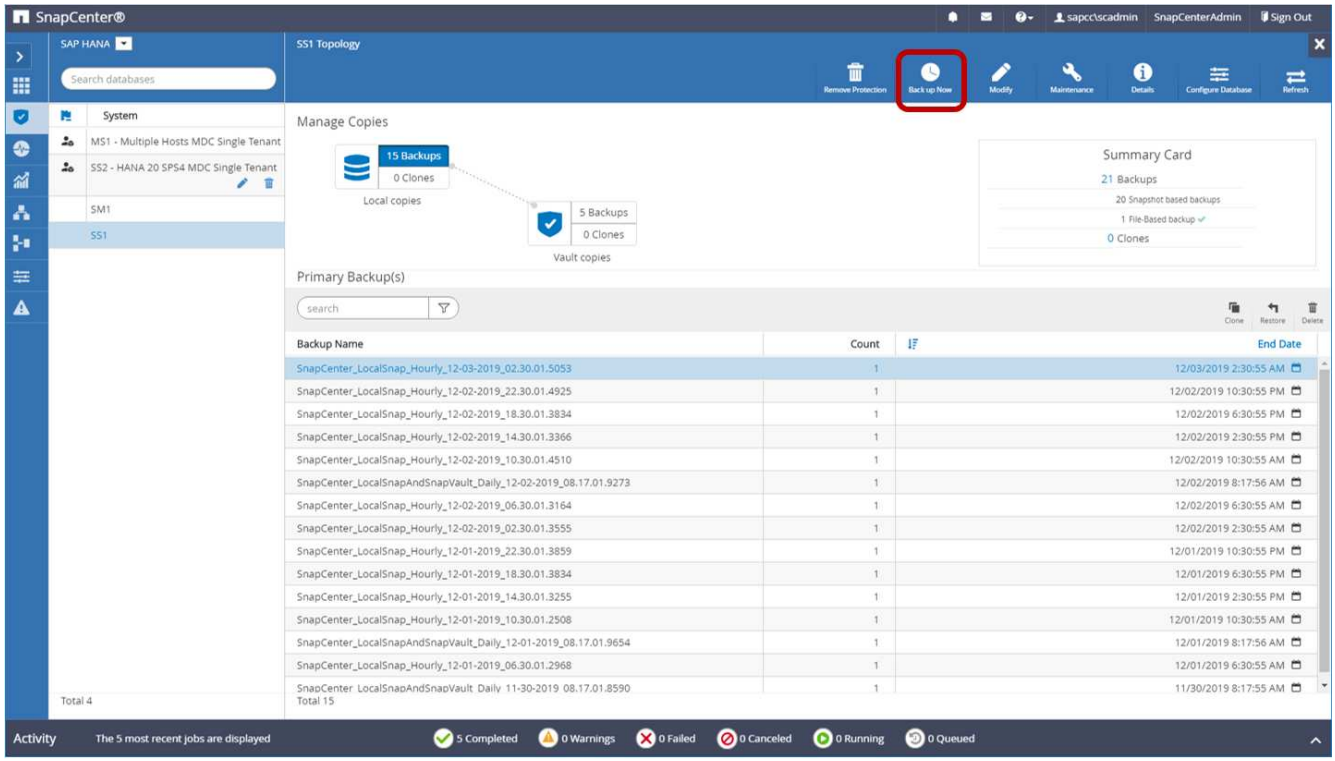
The following screenshot shows the available backups for the replication target volume `hana_SA1_data_mnt00001_dest` at the secondary storage system.



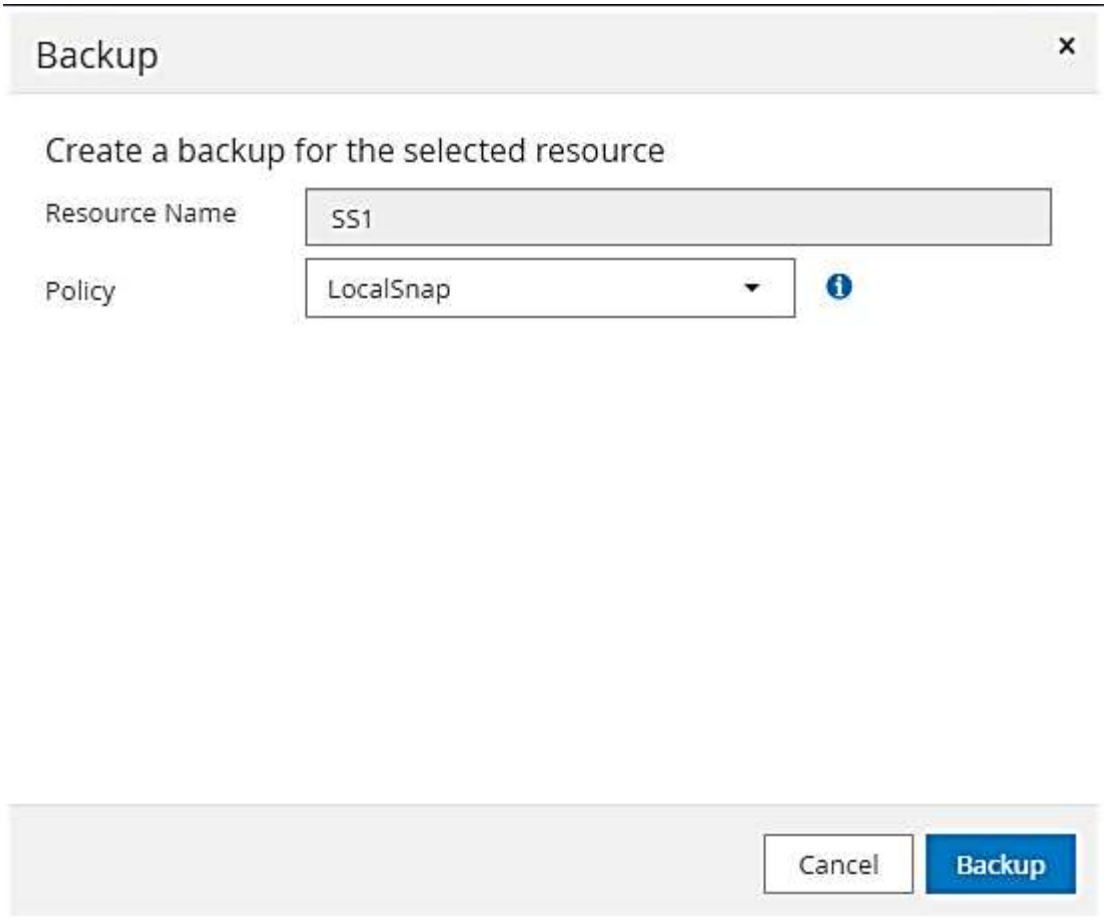
On-demand database backup at primary storage

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).

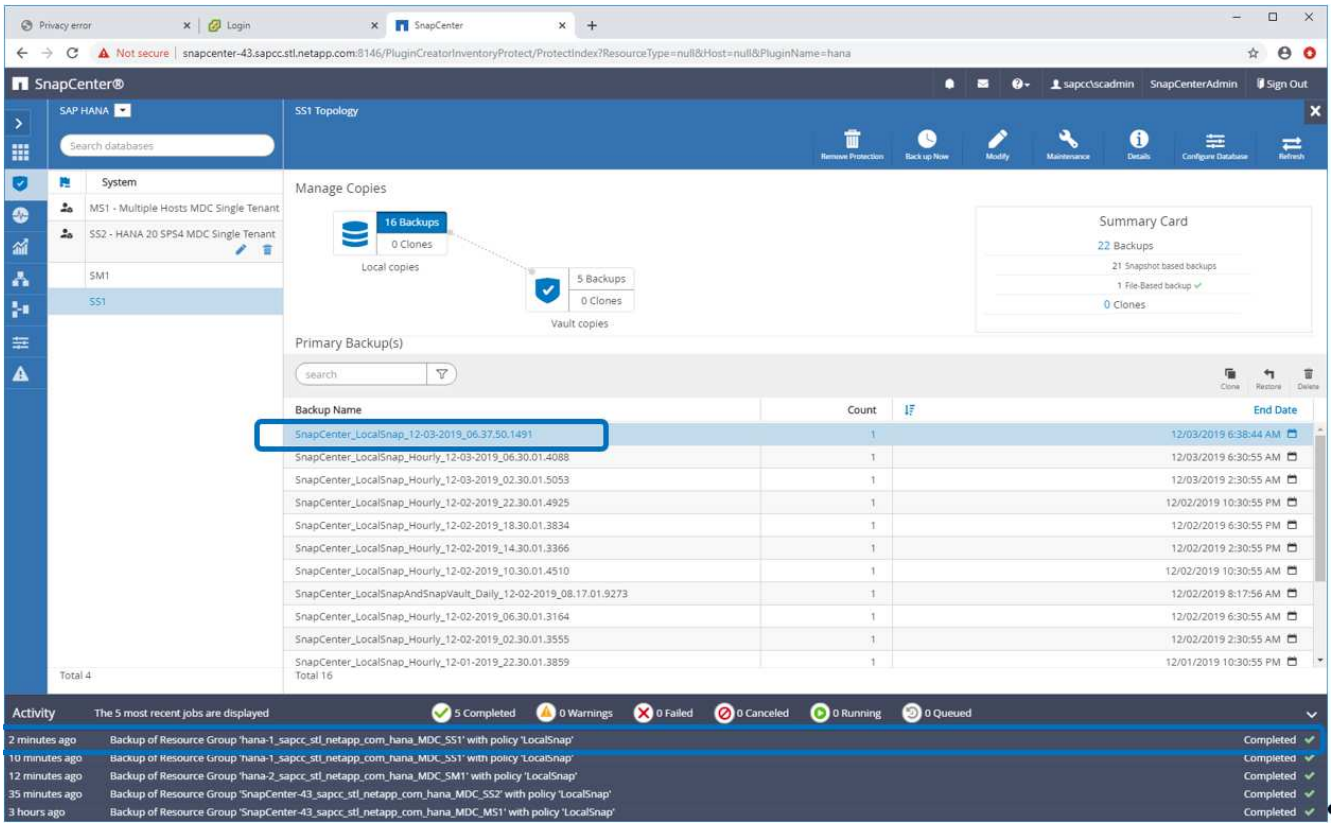


2. In the top row, select the Back up Now icon to start an on-demand backup. From the drop-down list, select the backup policy `LocalSnap` and then click Backup to start the on-demand backup.

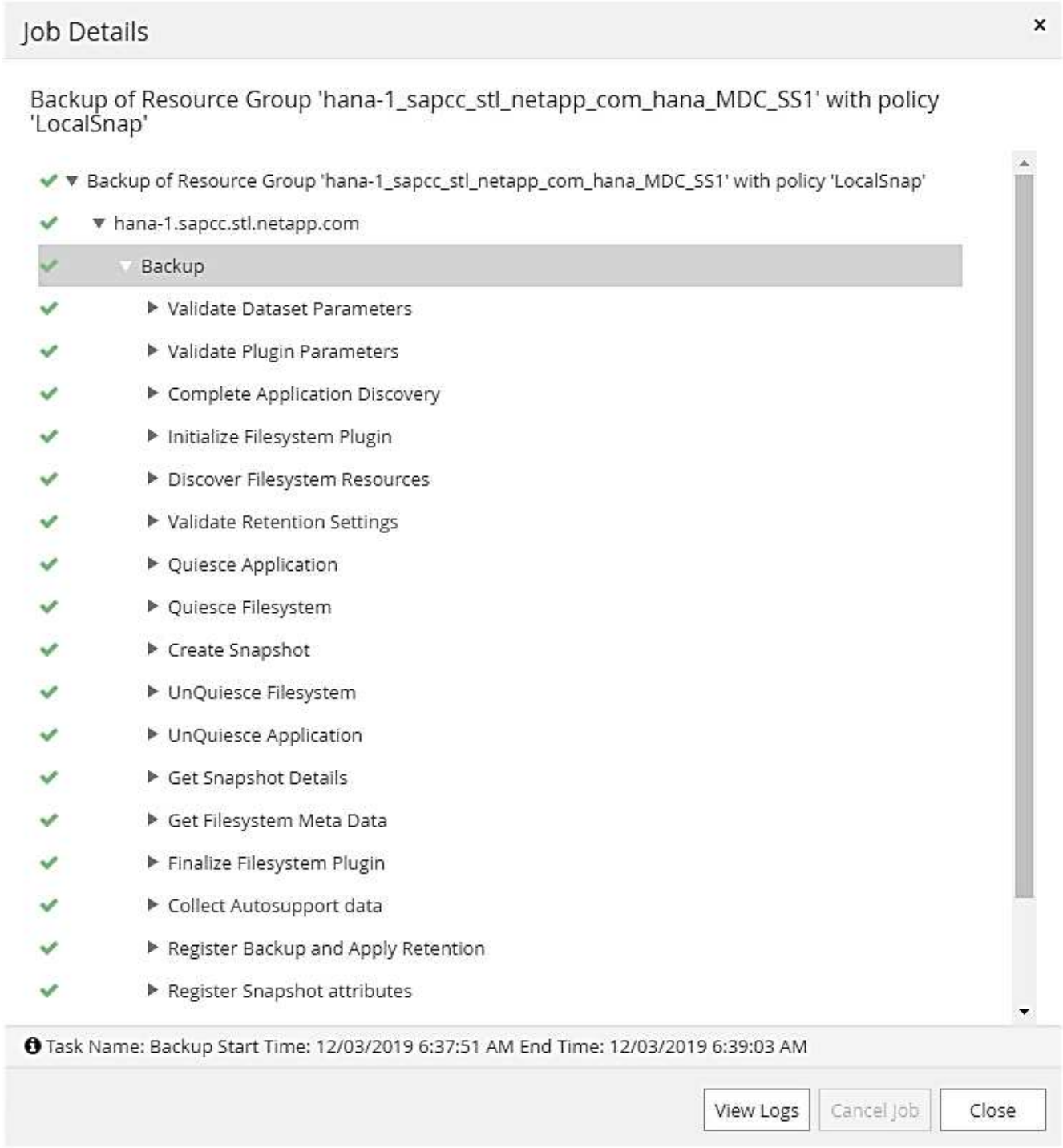


This starts the backup job. A log of the previous five jobs is shown in the Activity area below the topology view. When the backup is finished, a new entry is shown in the topology view. The backup names follow the same naming convention as the Snapshot name defined in the section "Resource protection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

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



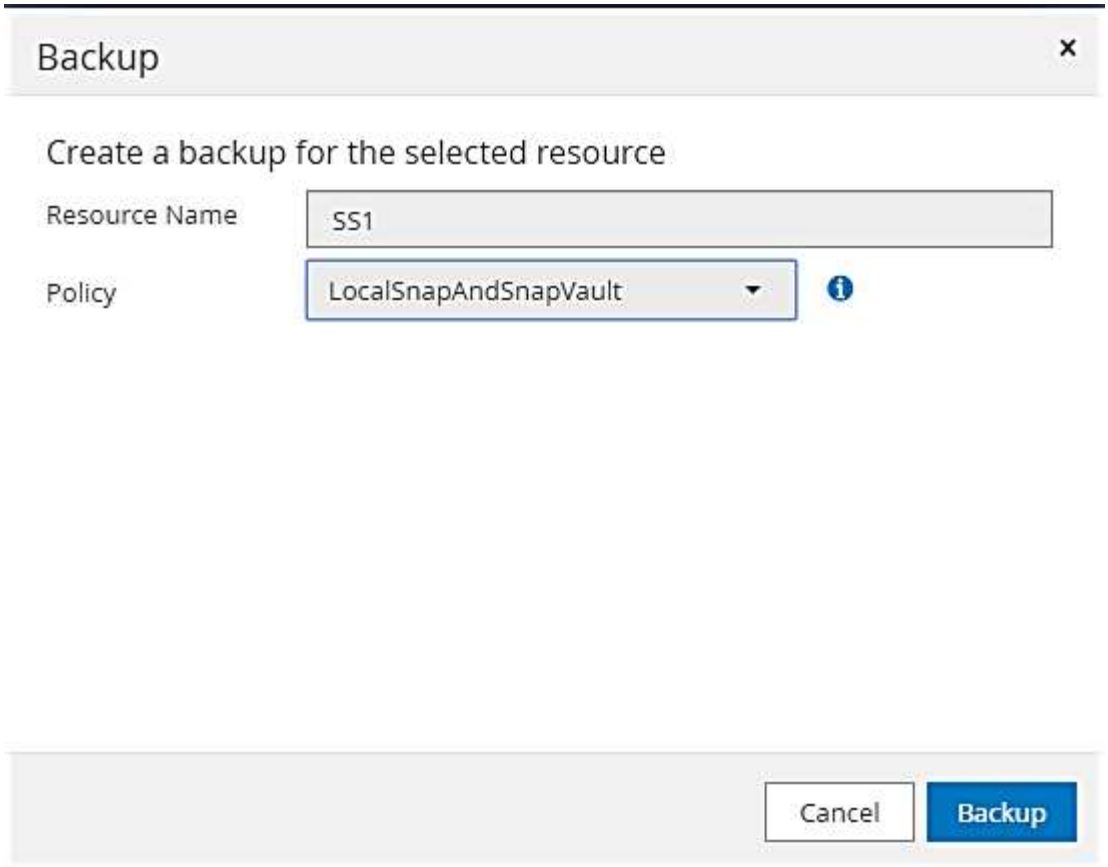
3. The job details are shown when clicking the job's activity line in the Activity area. You can open a detailed job log by clicking View Logs.



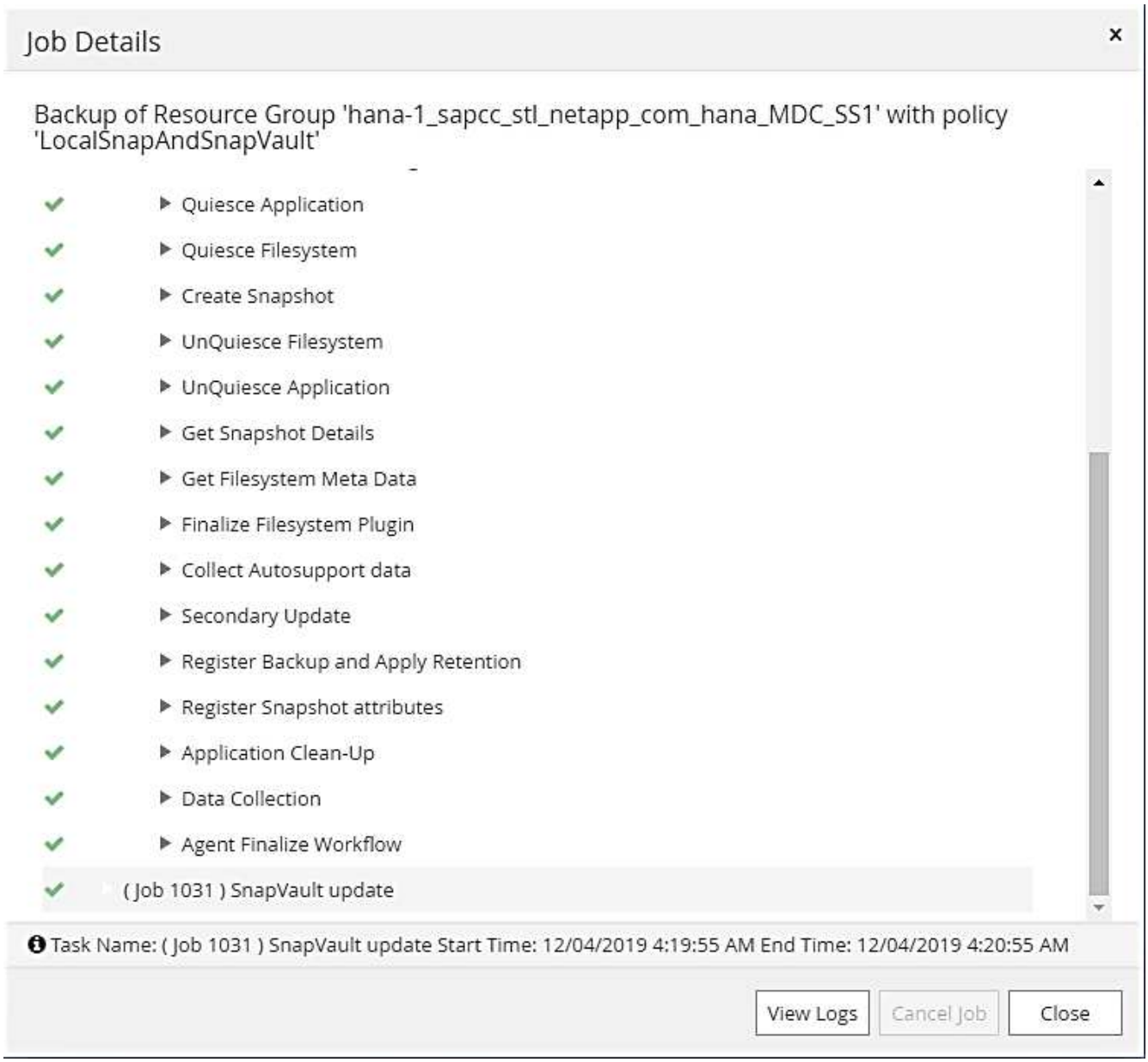
4. In SAP HANA Studio, the new backup is visible in the backup catalog. The same backup name in SnapCenter is also used in the comment and the EBID field in the backup catalog.

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.

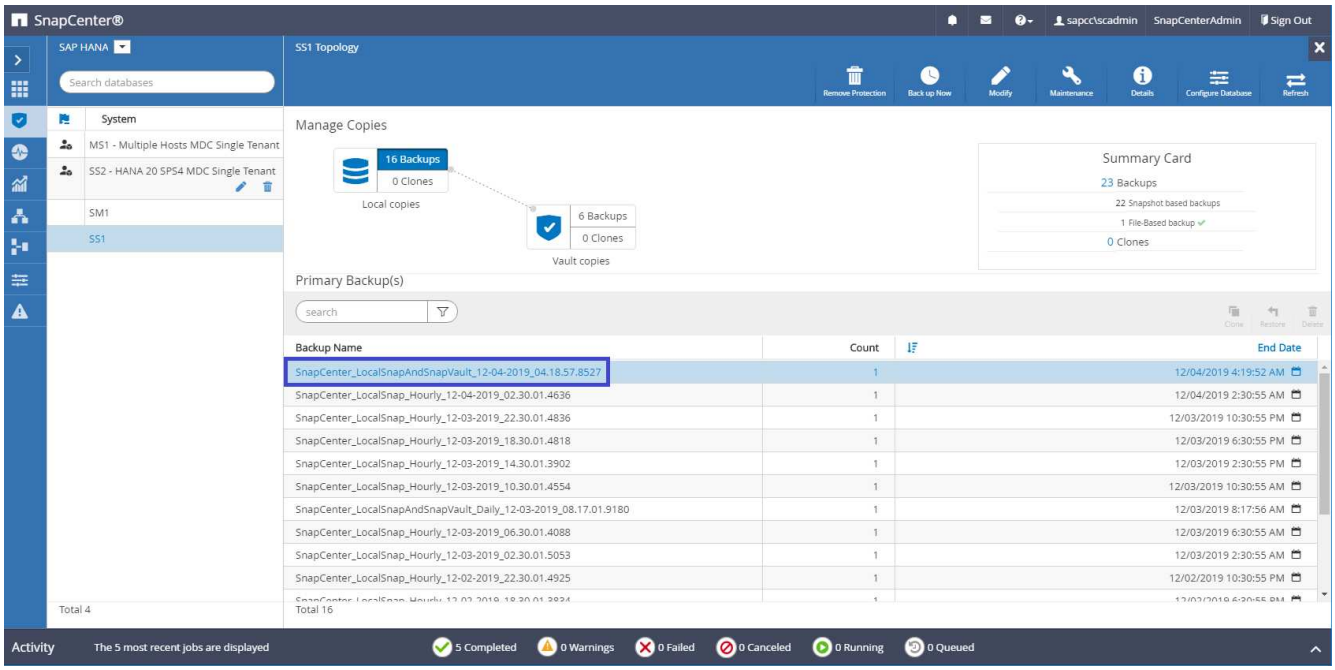


3. The job details are shown when clicking the job's activity line in the Activity area.

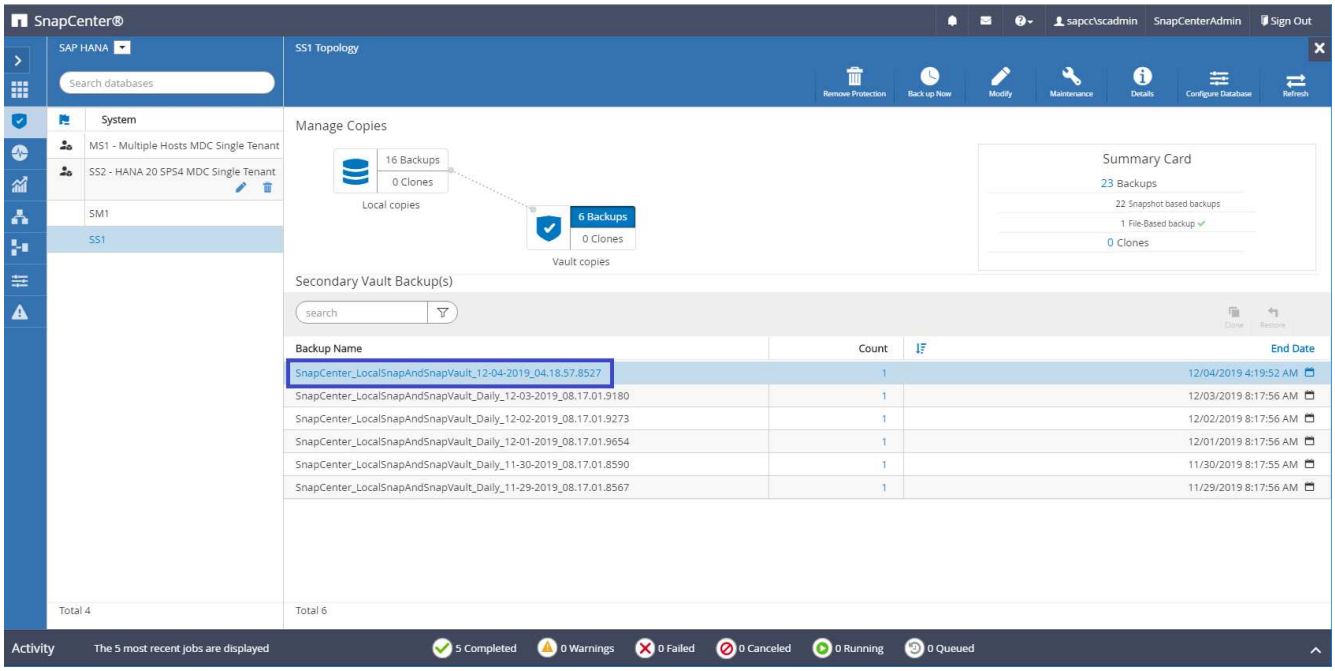


4. When the backup is finished, a new entry is shown in the topology view. The backup names follow the same naming convention as the Snapshot name defined in the section “Resource protection configuration.”

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.



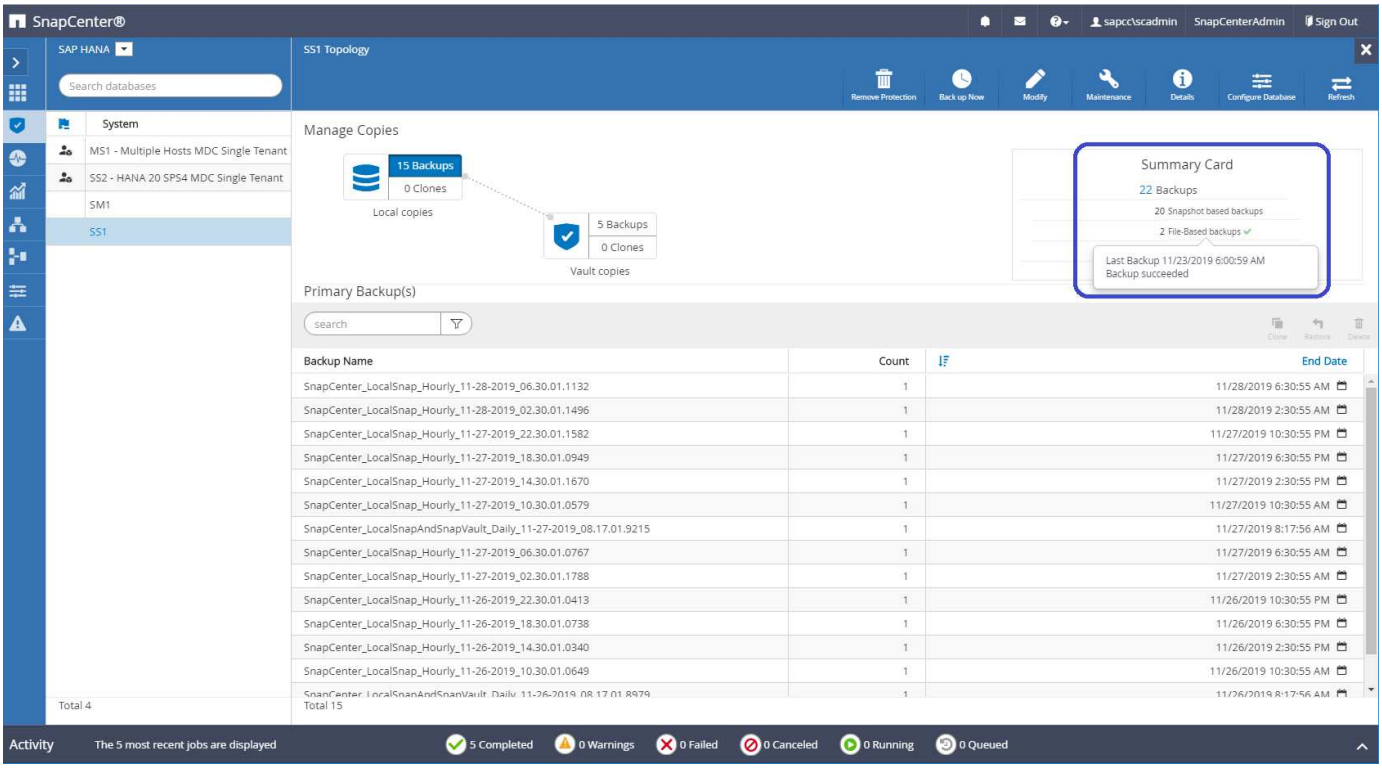
6. In SAP HANA Studio, the new backup is visible in the backup catalog. The same backup name in SnapCenter is also used in the comment and the EBID field in the backup catalog.

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.

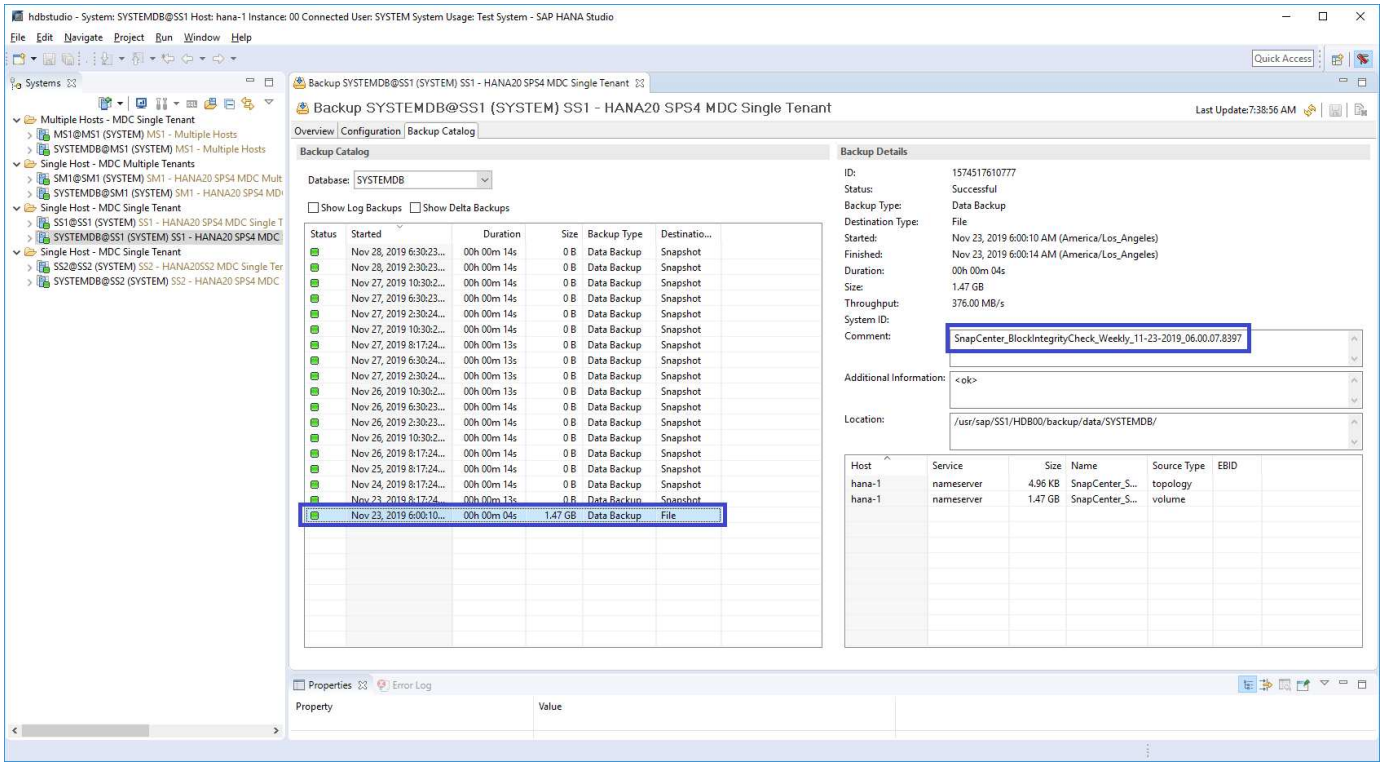
SnapCenter does not display the block integrity check in the same manner as Snapshot copy-based backups. Instead, the summary card shows the number of file-based backups and the status of the previous backup.



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. The following figure shows a SnapCenter block integrity check in the backup catalog of the system database.



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 ss1adm sapsys       4096 Nov 28 10:25 .
drwxr-xr-- 4 ss1adm sapsys       4096 Nov 19 05:11 ..
-rw-r----- 1 ss1adm sapsys     155648 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ss1adm sapsys   83894272 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_2_1
-rw-r----- 1 ss1adm 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 ss1adm sapsys       4096 Nov 28 10:24 .
drwxr-xr-- 4 ss1adm sapsys       4096 Nov 19 05:11 ..
-rw-r----- 1 ss1adm sapsys     159744 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ss1adm 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.

   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

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

Next, SnapCenter performs the following operations:

1. It stops the HANA database.
2. It 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, then SnapCenter unmounts the volume, restores the volume using volume-based SnapRestore on the storage layer, and mounts the volume.
   - If NFS is selected and Volume Revert is not selected, SnapCenter restores all files using single-file SnapRestore operations on the storage layer.
   - If Fibre Channel SAN is selected, then SnapCenter unmounts the LUN(s), restores the LUN(s) using single file SnapRestore operations on the storage layer, and discovers and mounts the LUN(s).
3. It recovers the database:
   a. It recovers the system database.
   b. It recovers the tenant database.

      Or, for HANA single container systems, the recovery is executed in a single step:

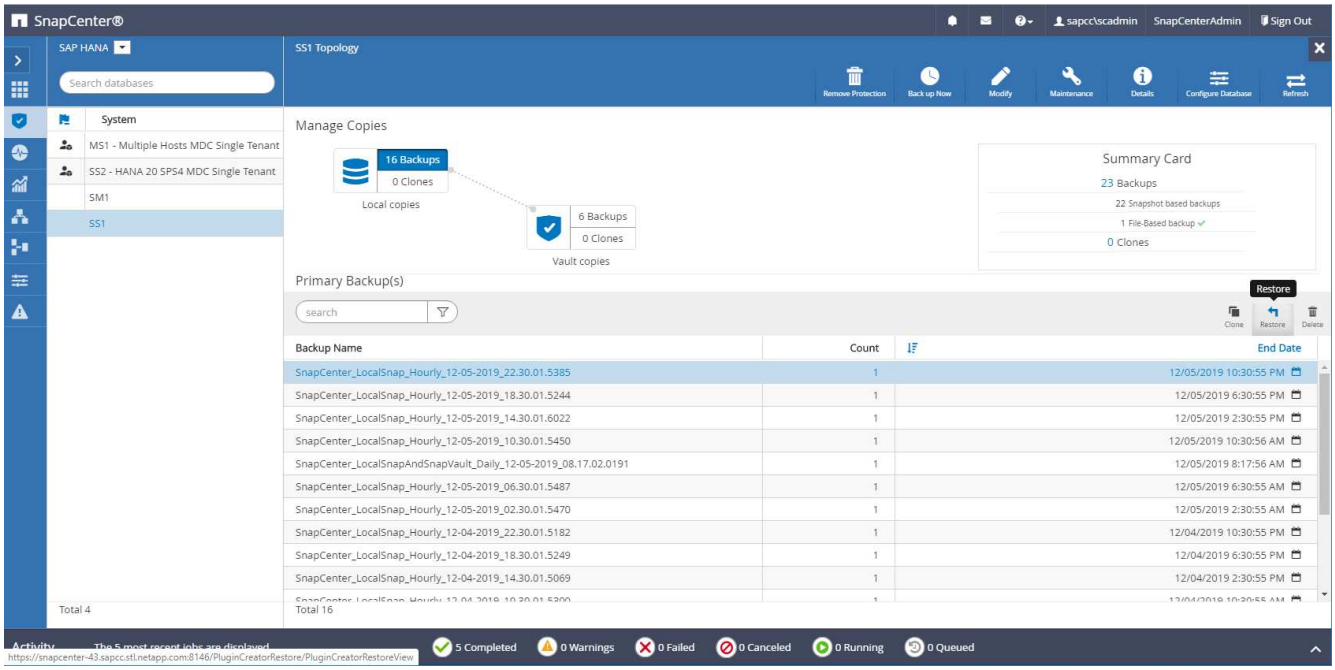
   c. It starts the HANA database.

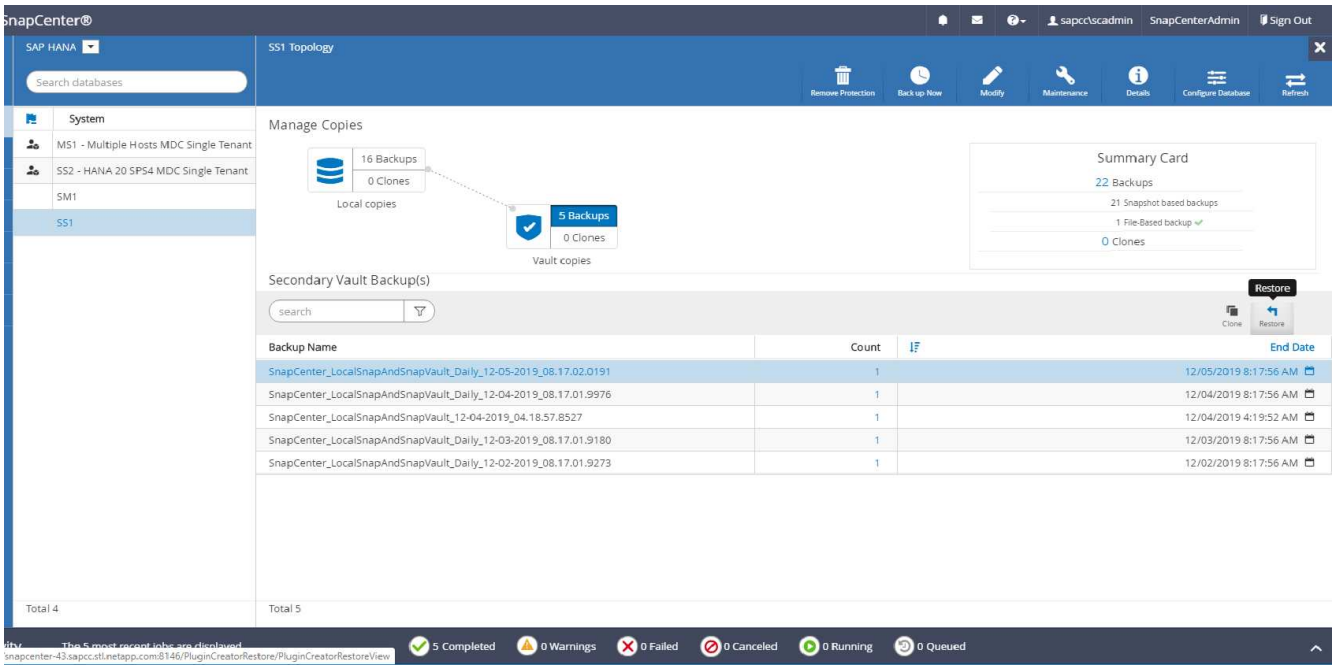
If No Recovery is selected, SnapCenter exits and the recovery operation for the system and the tenant database must be done manually.

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.

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





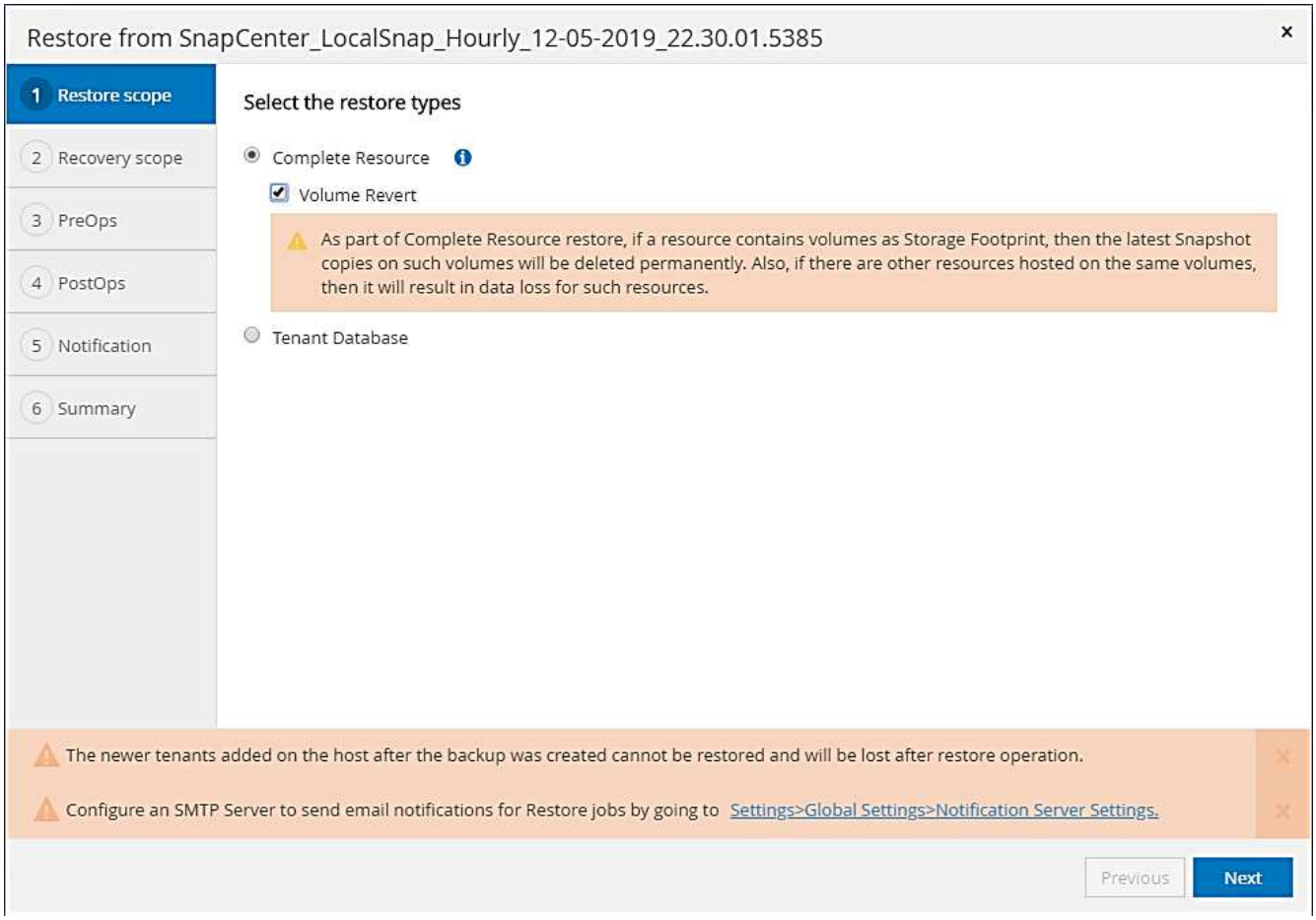
2. Select the restore scope and type.

   The following three screenshots show the restore options for restore from primary with NFS, restore from

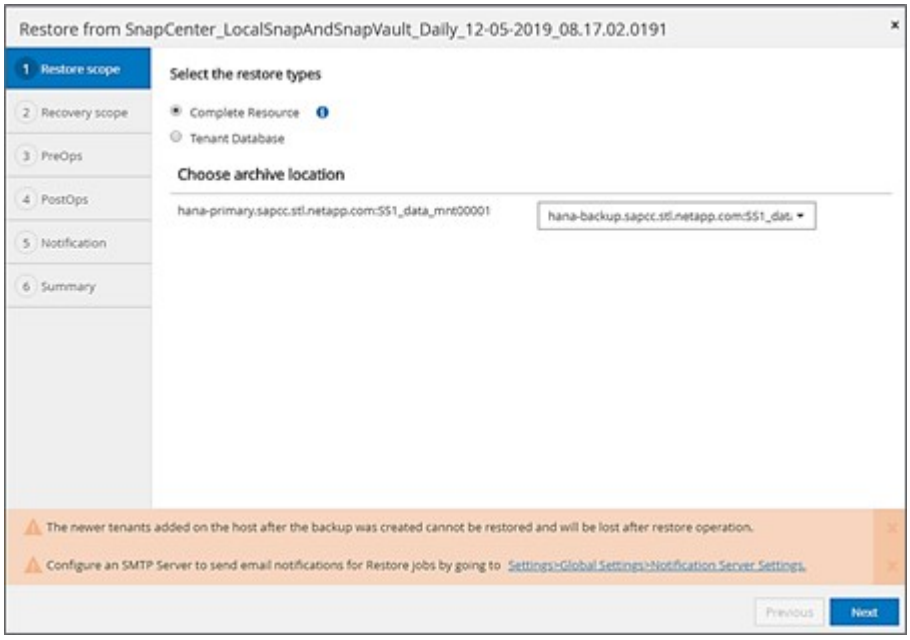
secondary with NFS, and restore from primary with Fibre Channel SAN.

The restore type options for restore from primary storage.

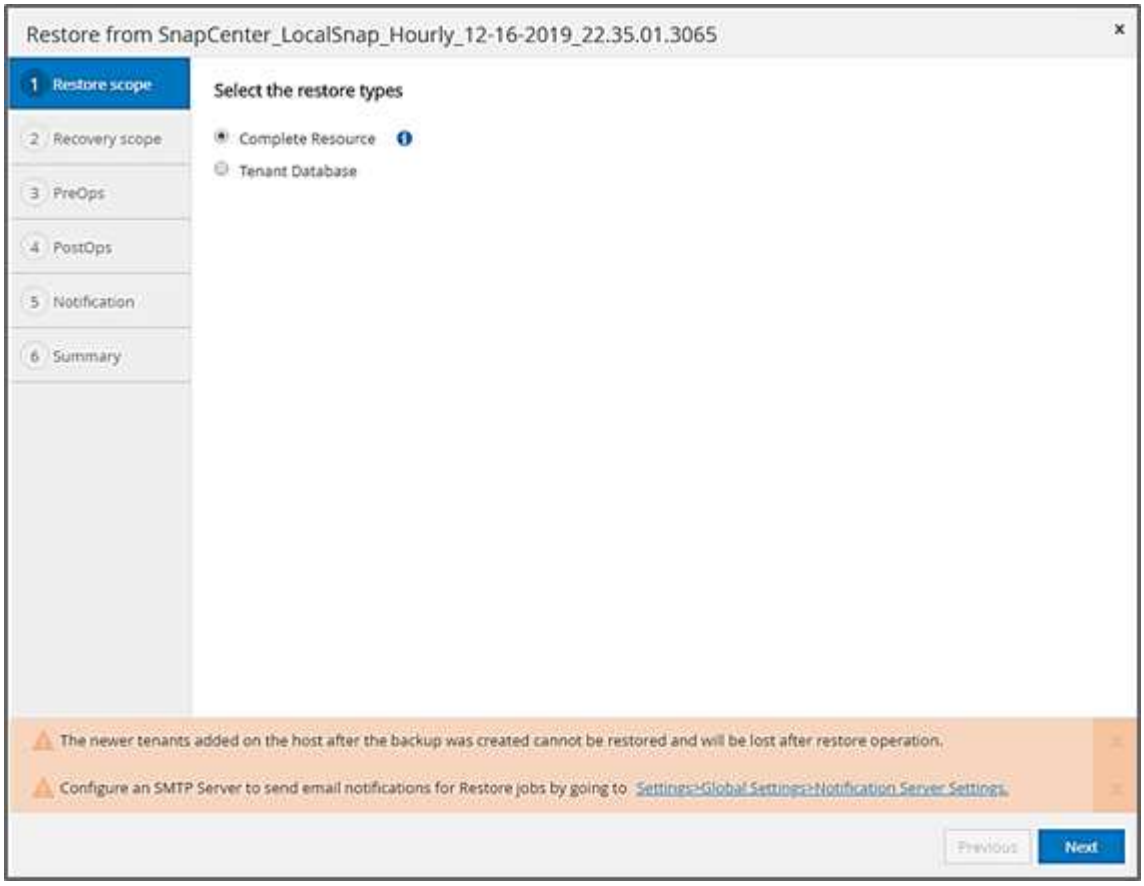
The Volume Revert option is only available for restore operations from primary with NFS.



The restore type options for restore from offsite backup storage.

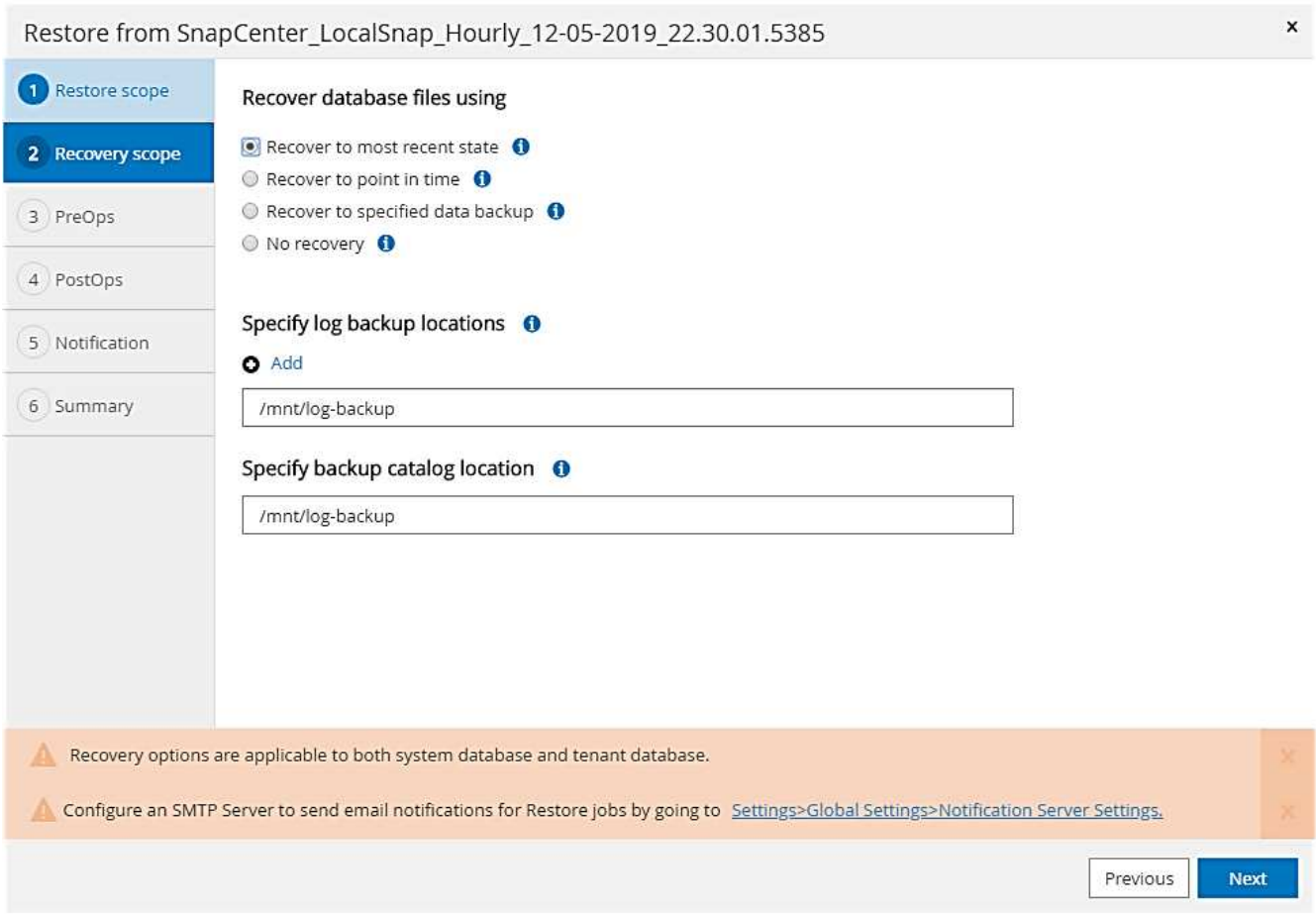


The restore type options for restore from primary storage with Fibre Channel SAN.

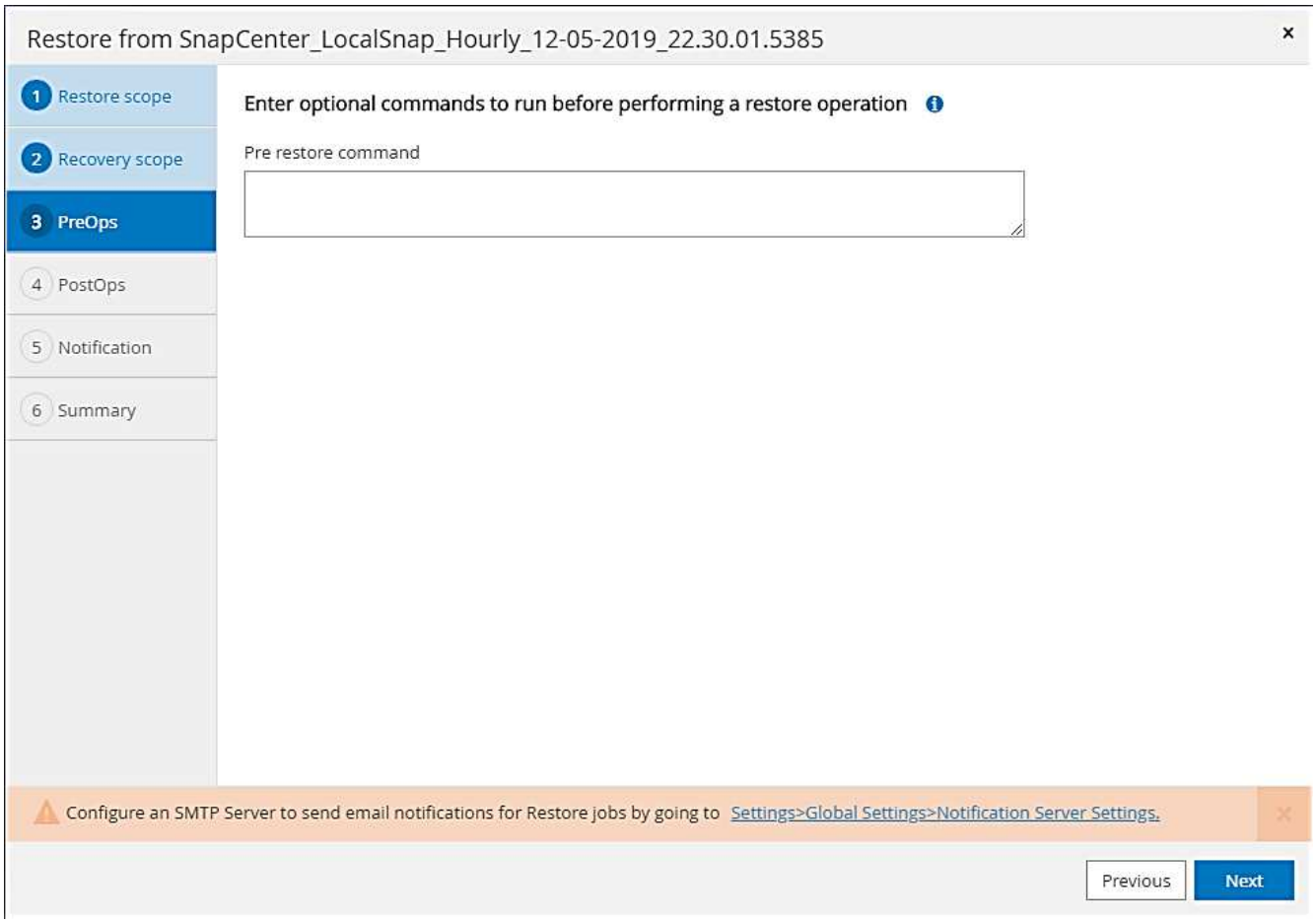


3. Select Recovery Scope and provide the location for log backup and catalog backup.

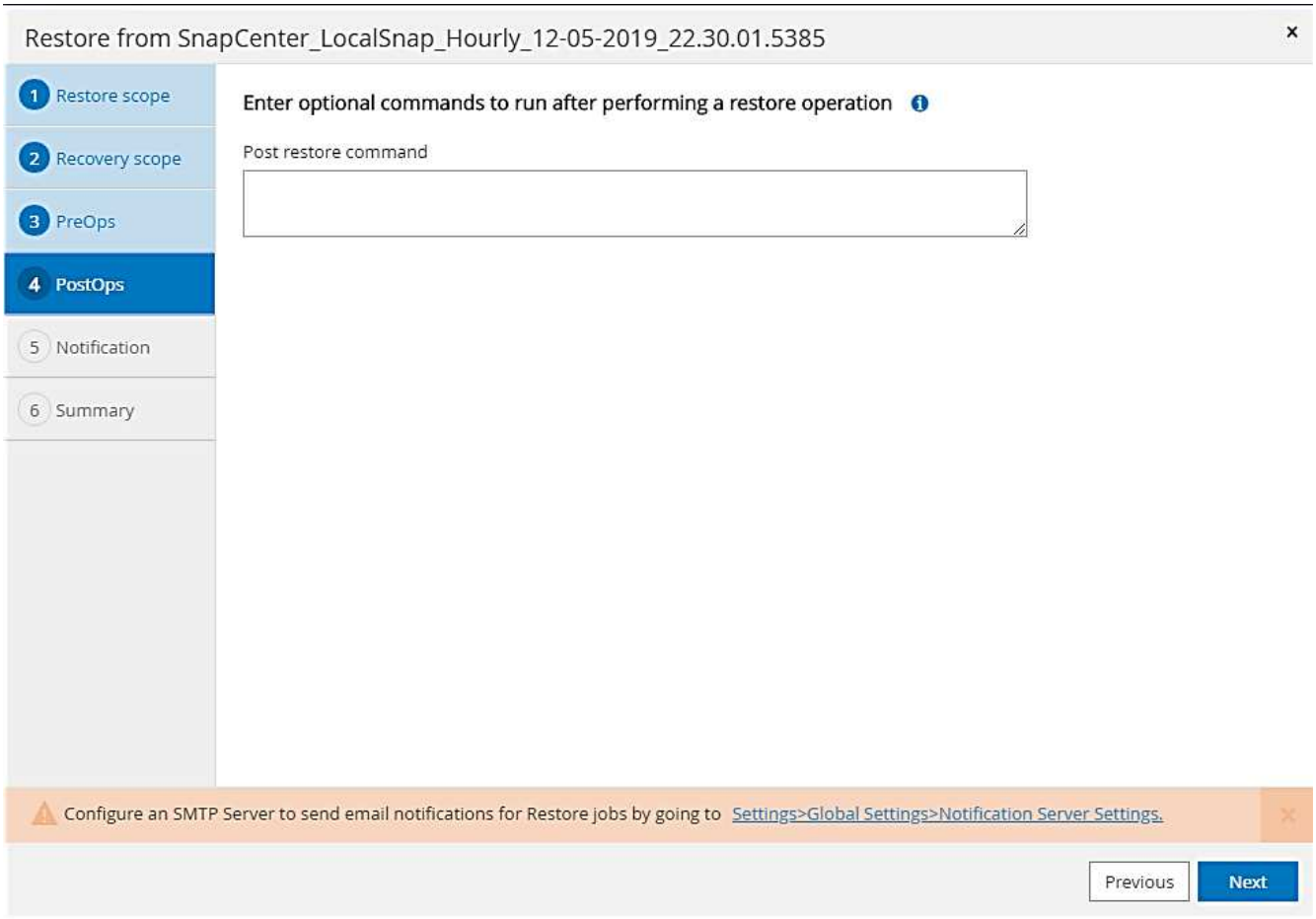
SnapCenter uses the default path or the changed paths in the HANA global.ini file to pre-populate the log and catalog backup locations.



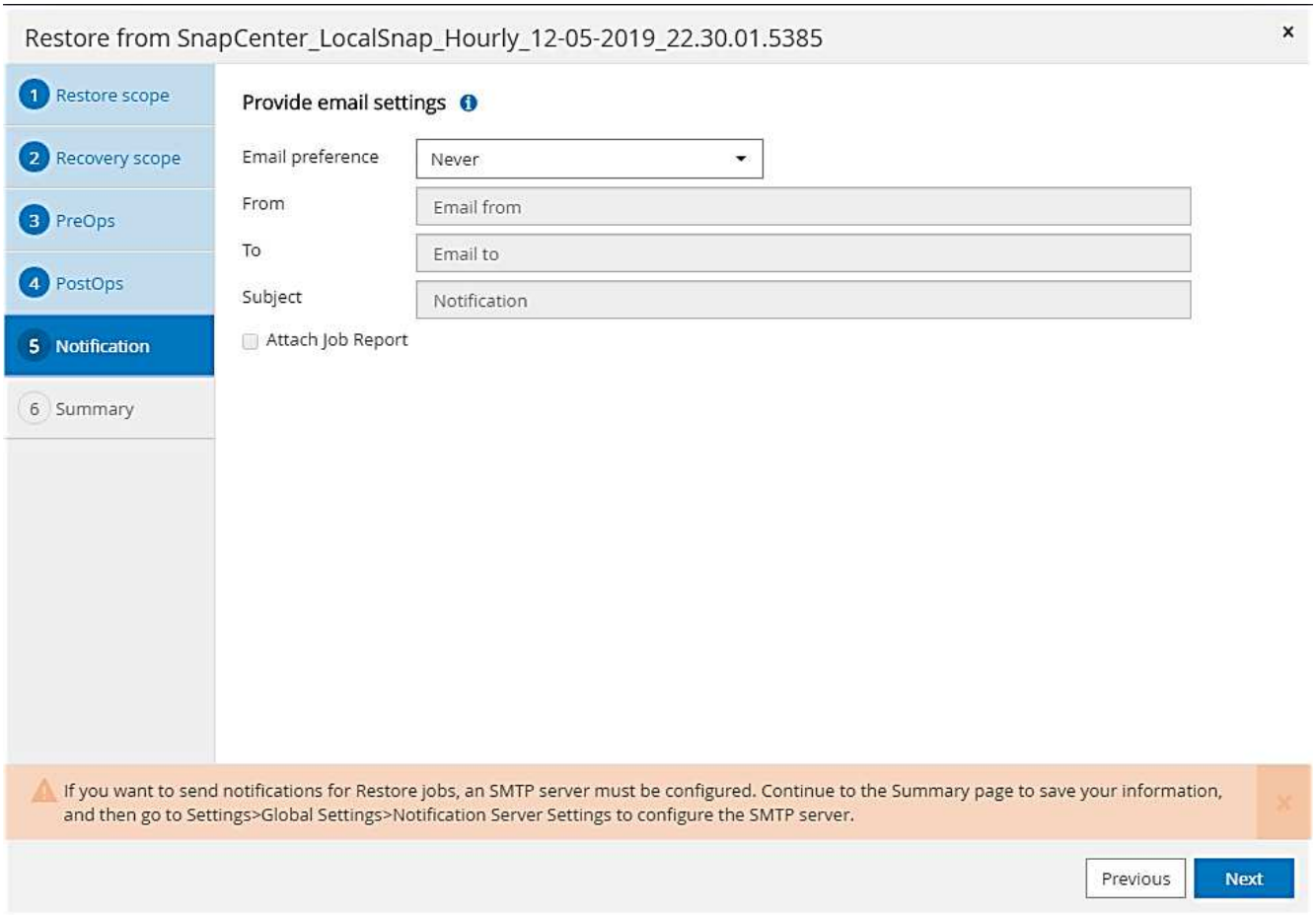
4. Enter the optional prerestore commands.



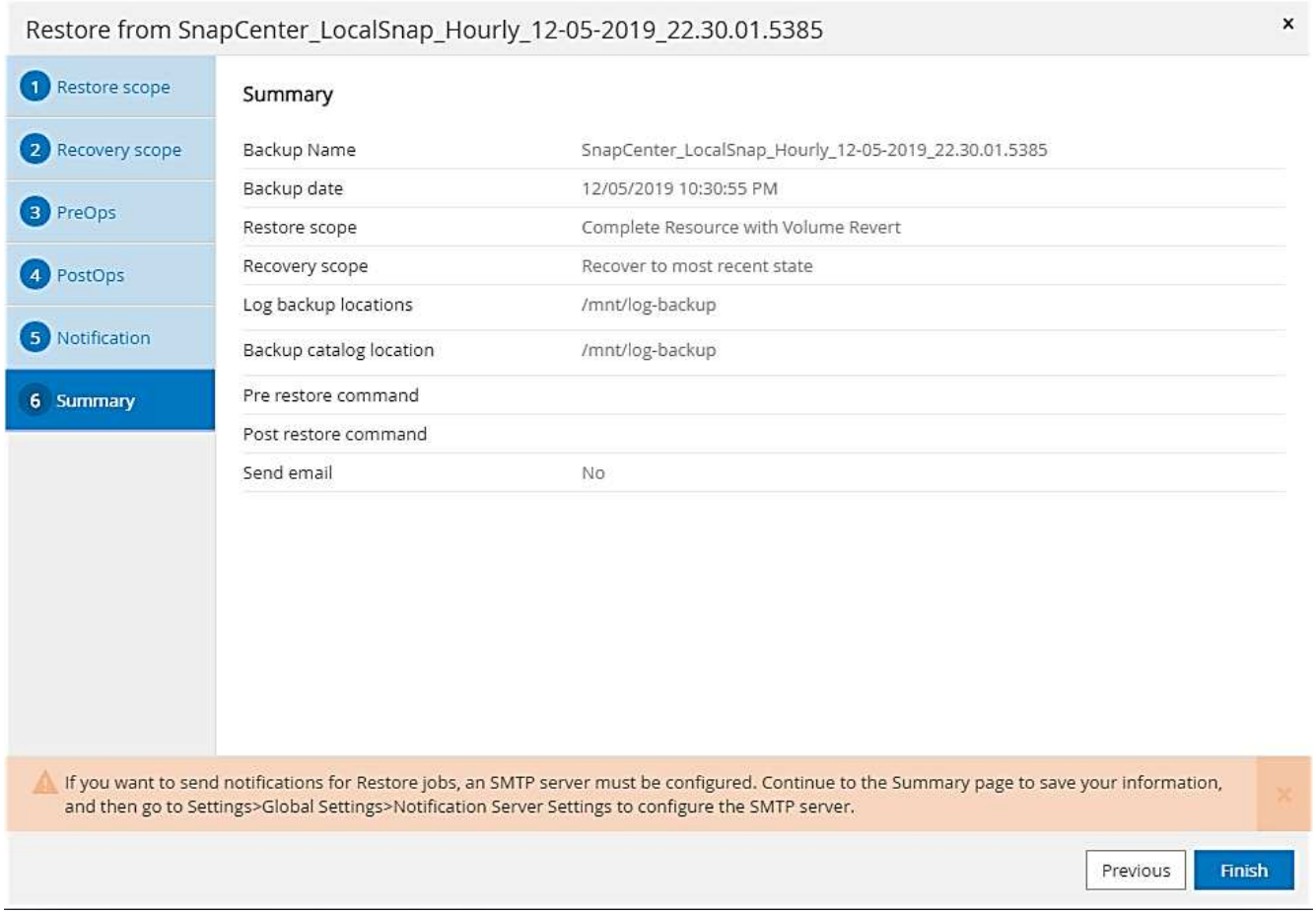
5. Enter the optional post-restore commands.



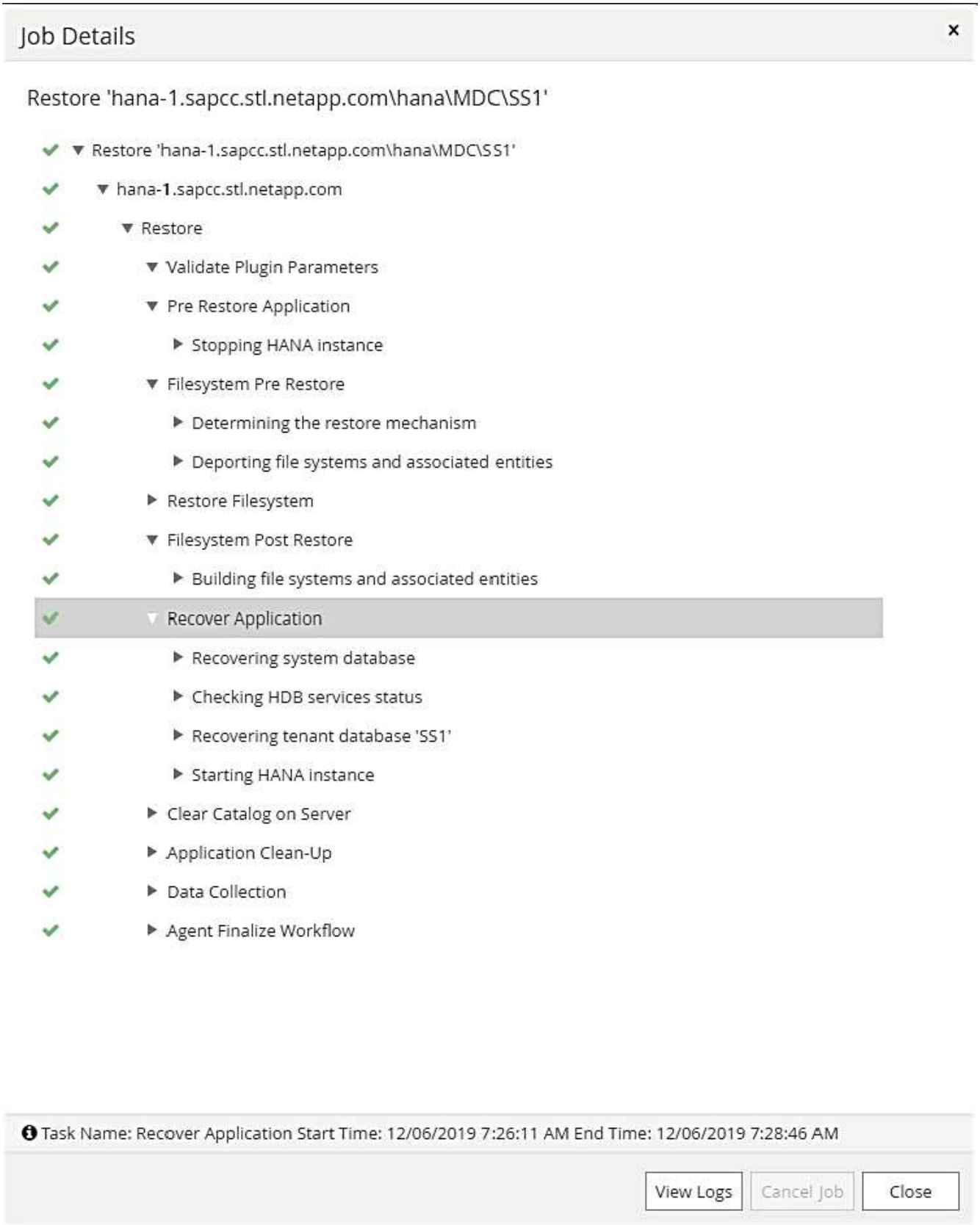
6. Enter the optional email settings.



7. To start the restore operation, click Finish.



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



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:

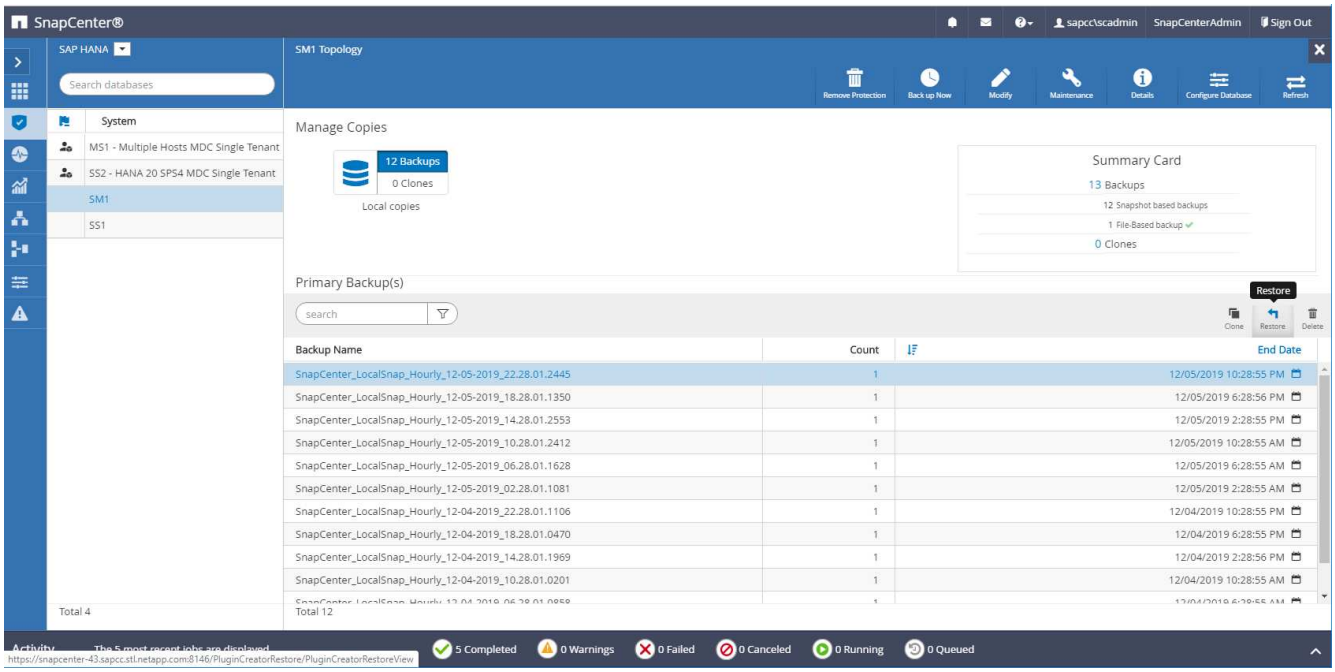
1. Stop the tenant to be restored and recovered.
2. Restore the tenant with SnapCenter.
   - For a restore from primary storage, SnapCenter executes the following operations:
     - **NFS.** Storage Single File SnapRestore operations for all files of the tenant database.
     - **SAN.** Clone and connect 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.

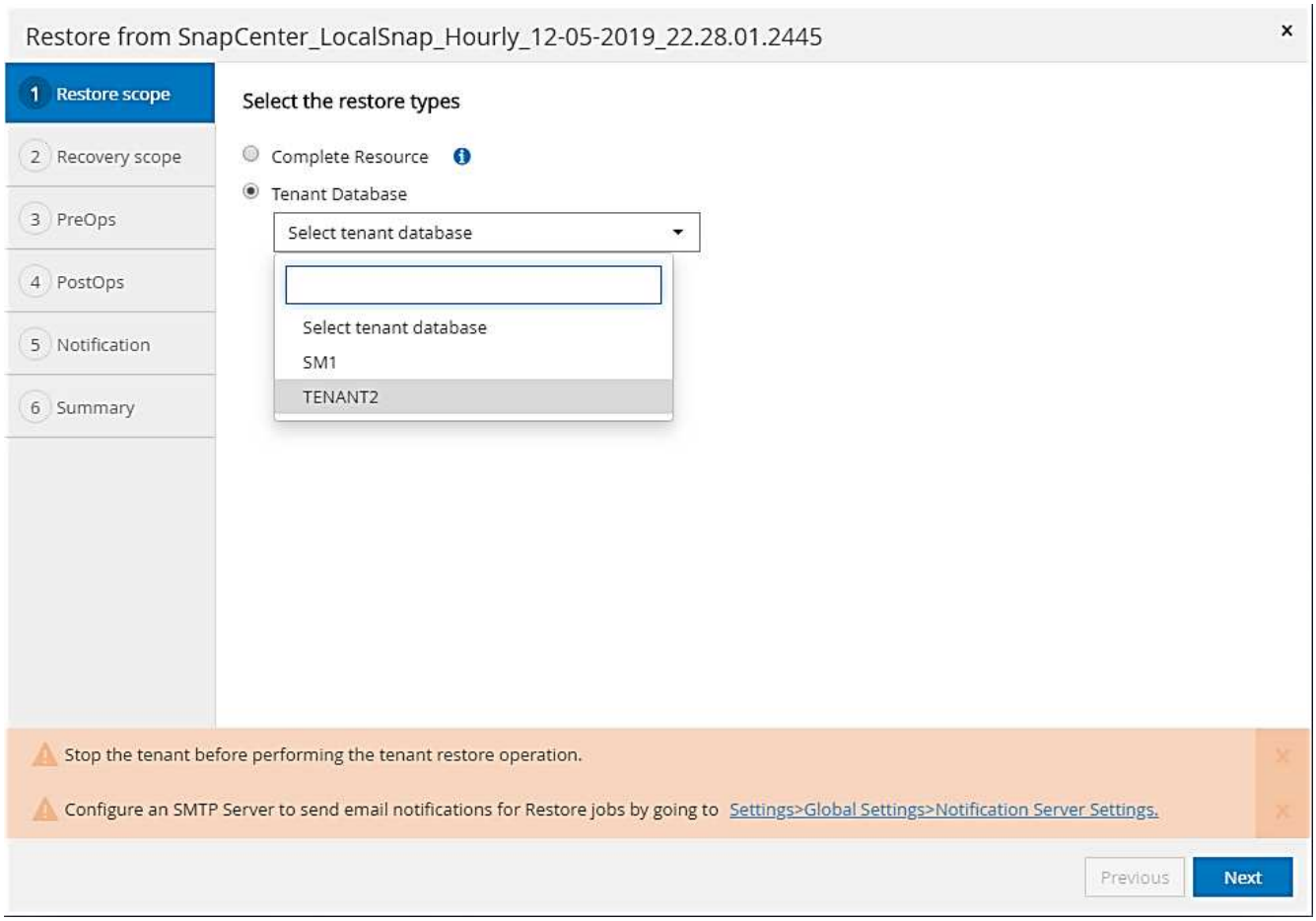
```
sm1adm@hana-2:/usr/sap/SM1/HDB00> hdbsql -U SYSKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql=>
hdbsql SYSTEMDB=> alter system stop database tenant2;
0 rows affected (overall time 14.215281 sec; server time 14.212629 sec)
hdbsql SYSTEMDB=>
```

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

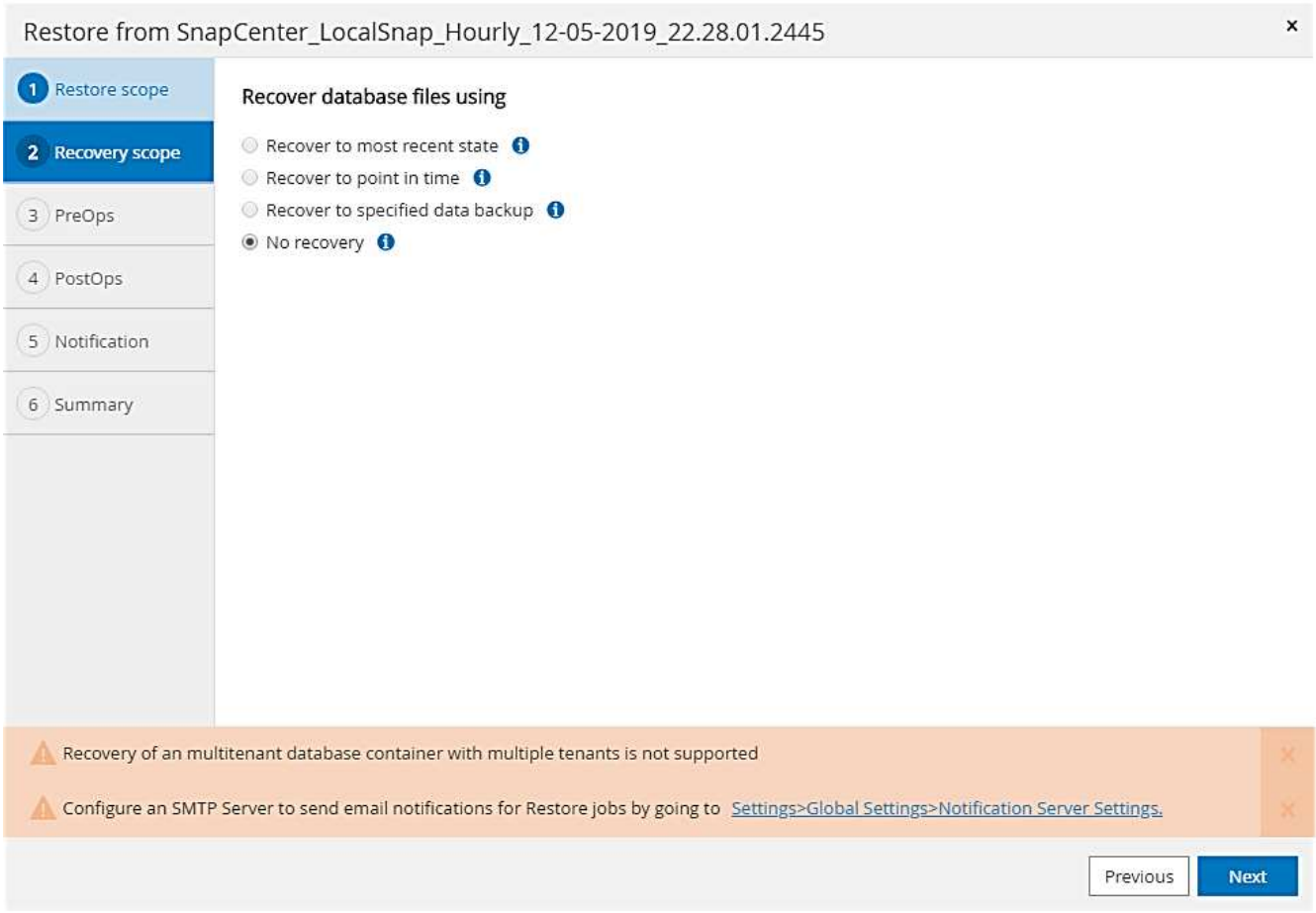


3. Select the tenant to be restored.

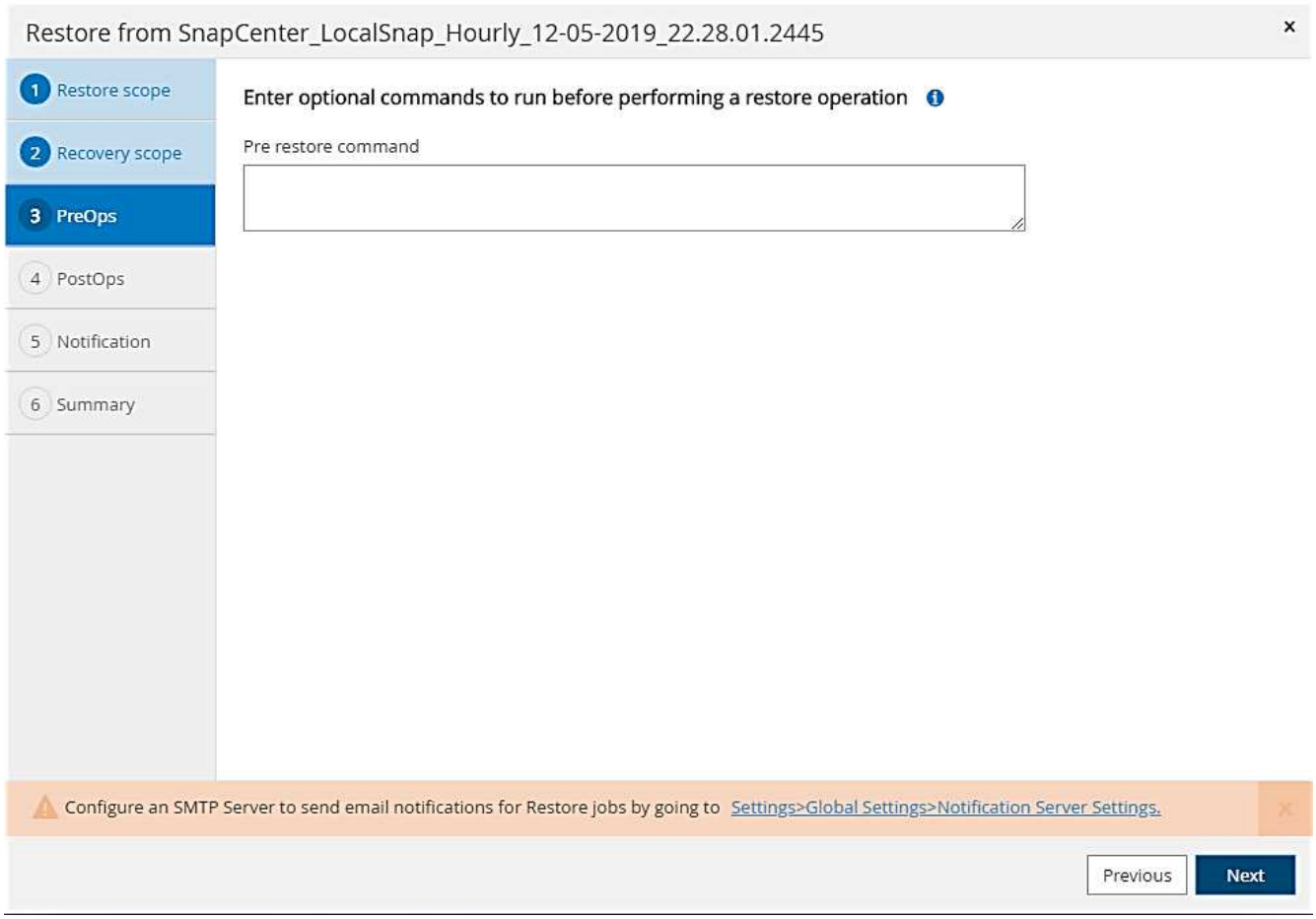
SnapCenter shows a list of all tenants that are included in the selected backup.



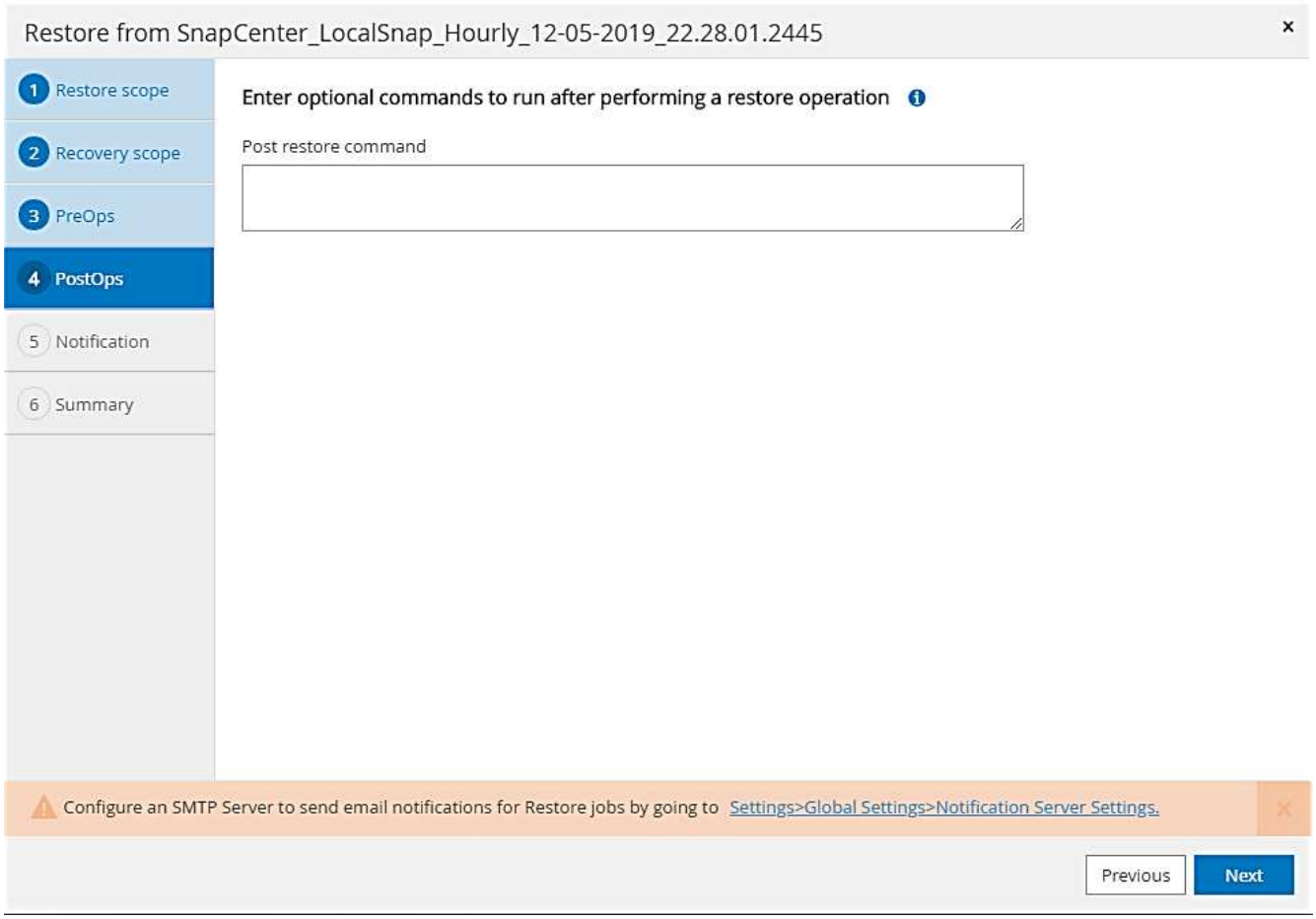
Single-tenant recovery is not supported with SnapCenter 4.3. No Recovery is preselected and cannot be changed.



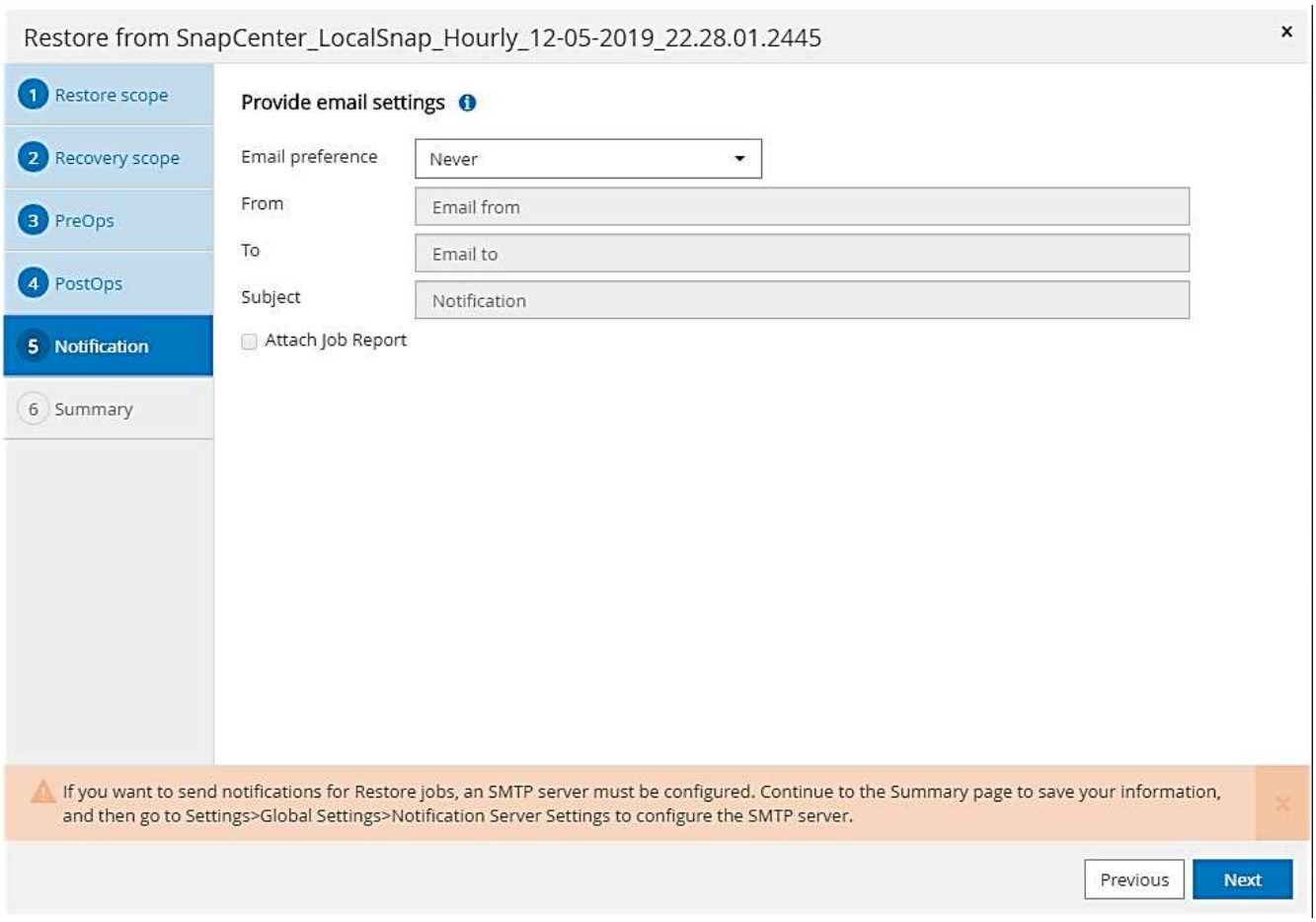
4. Enter the optional prerestore commands.



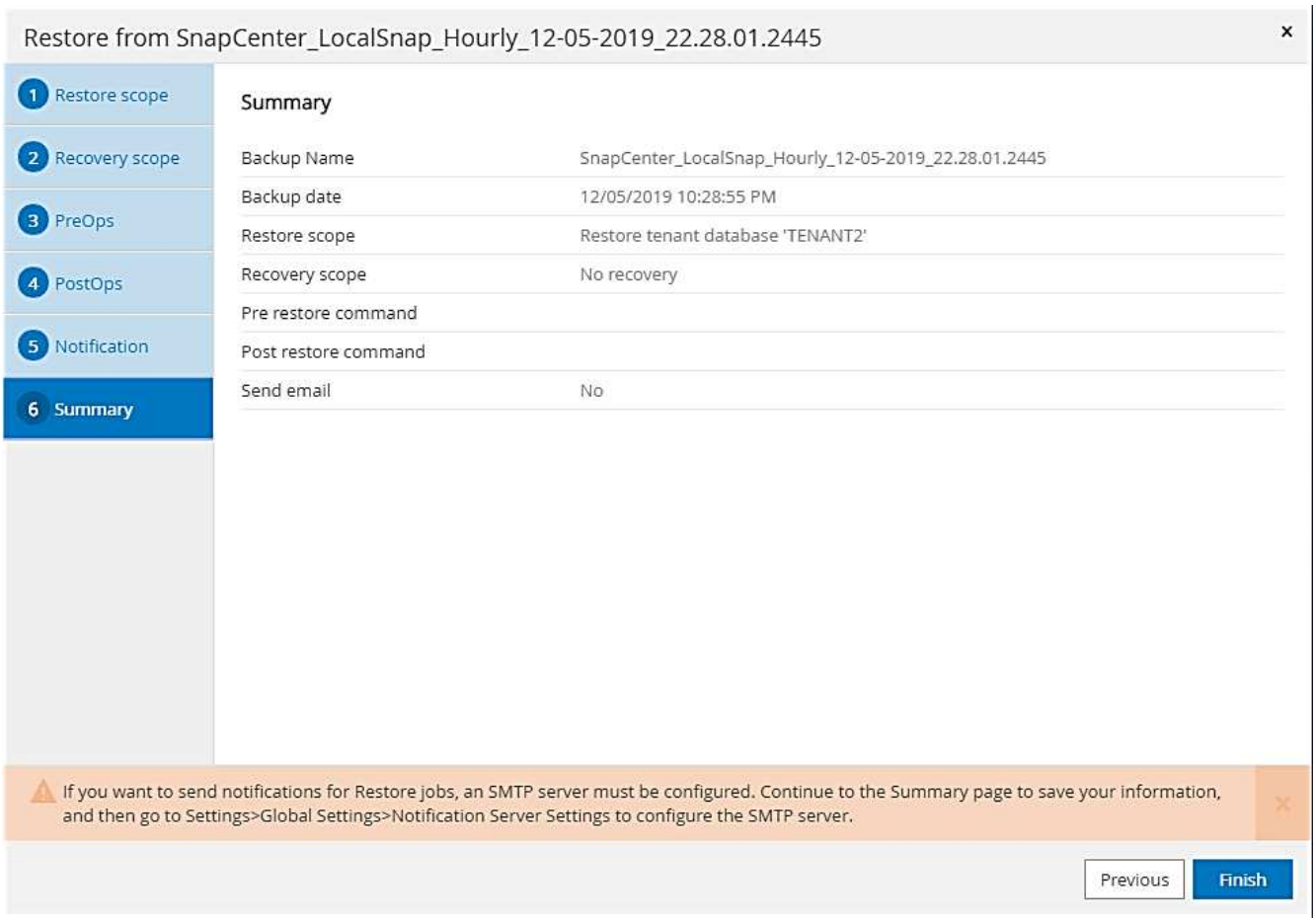
5. Enter optional post-restore commands.



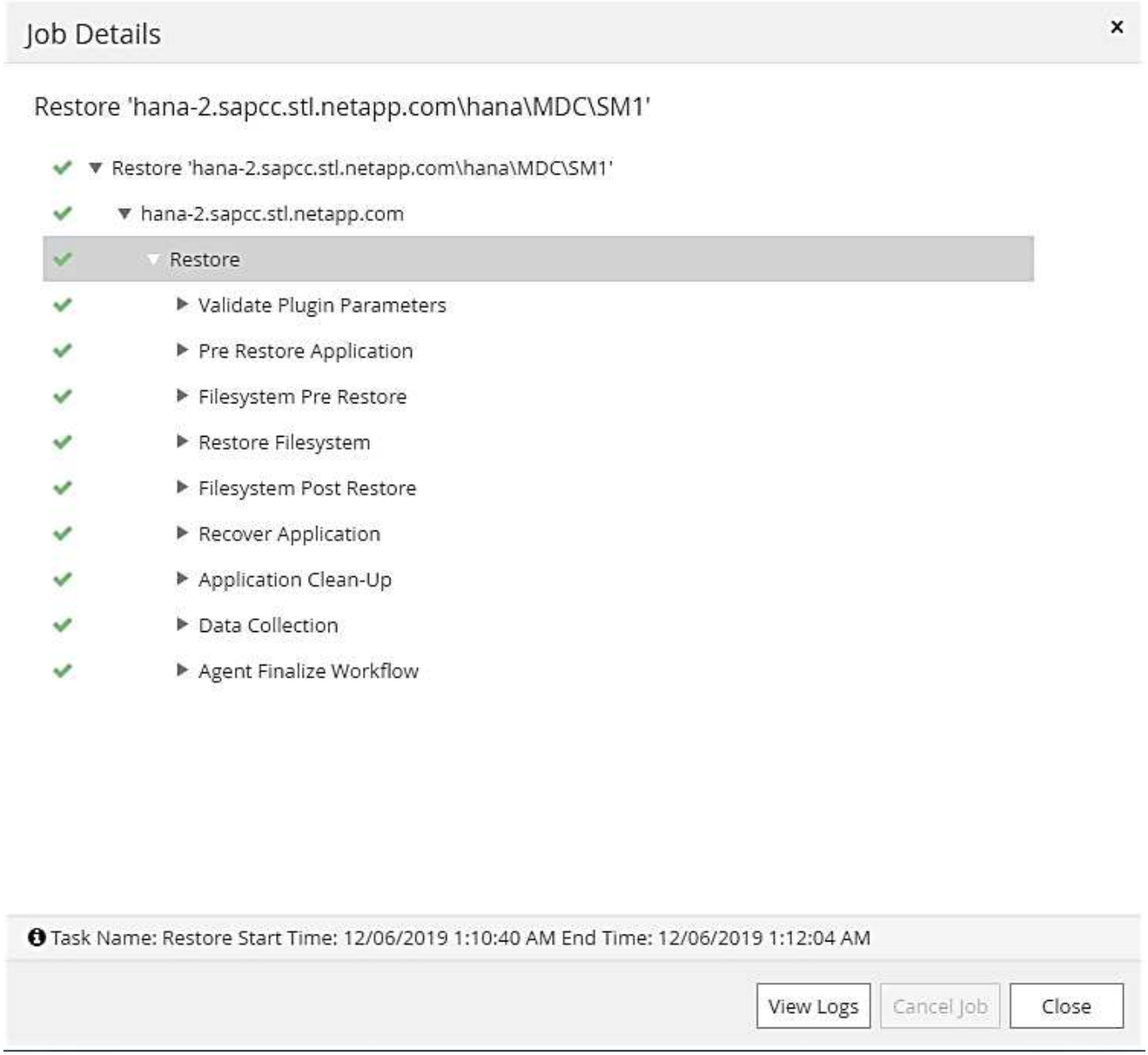
6. Enter the optional email settings.



7. To start the restore operation, click Finish.



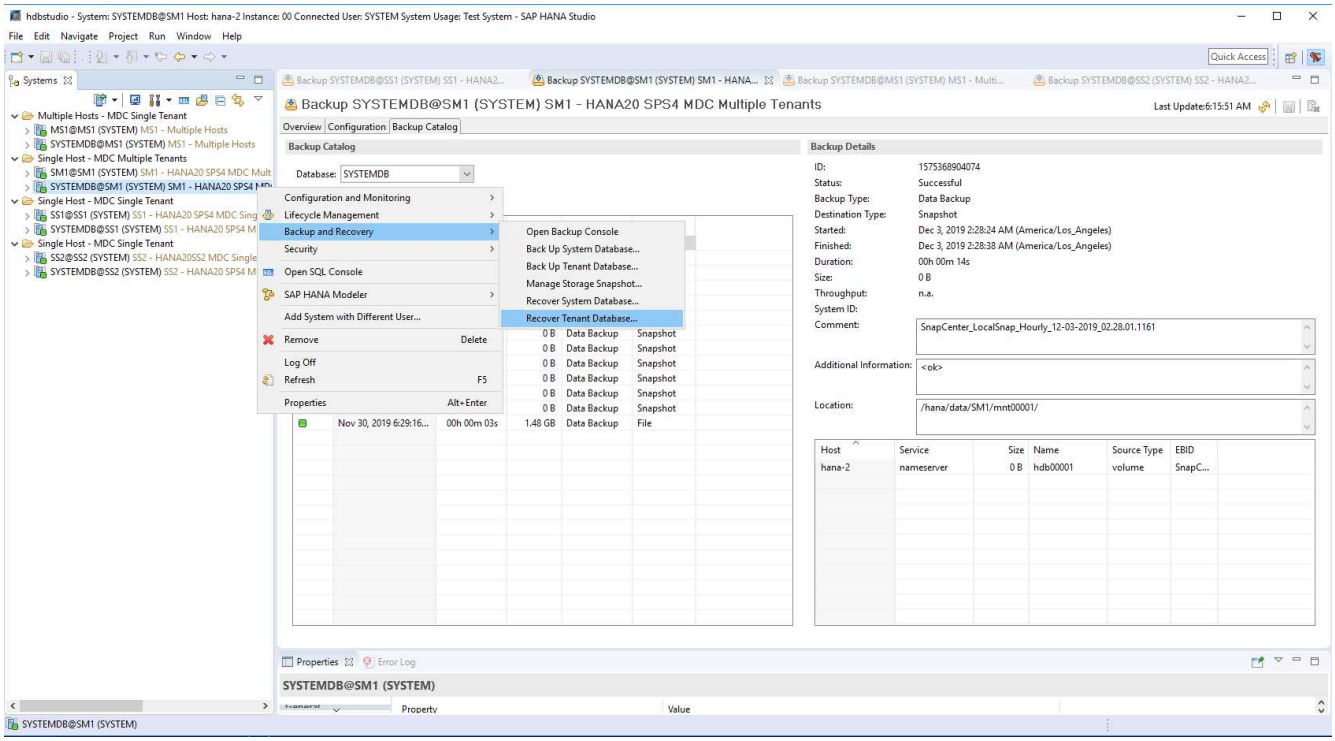
The restore operation is executed by SnapCenter. This example shows the job details of the restore job.



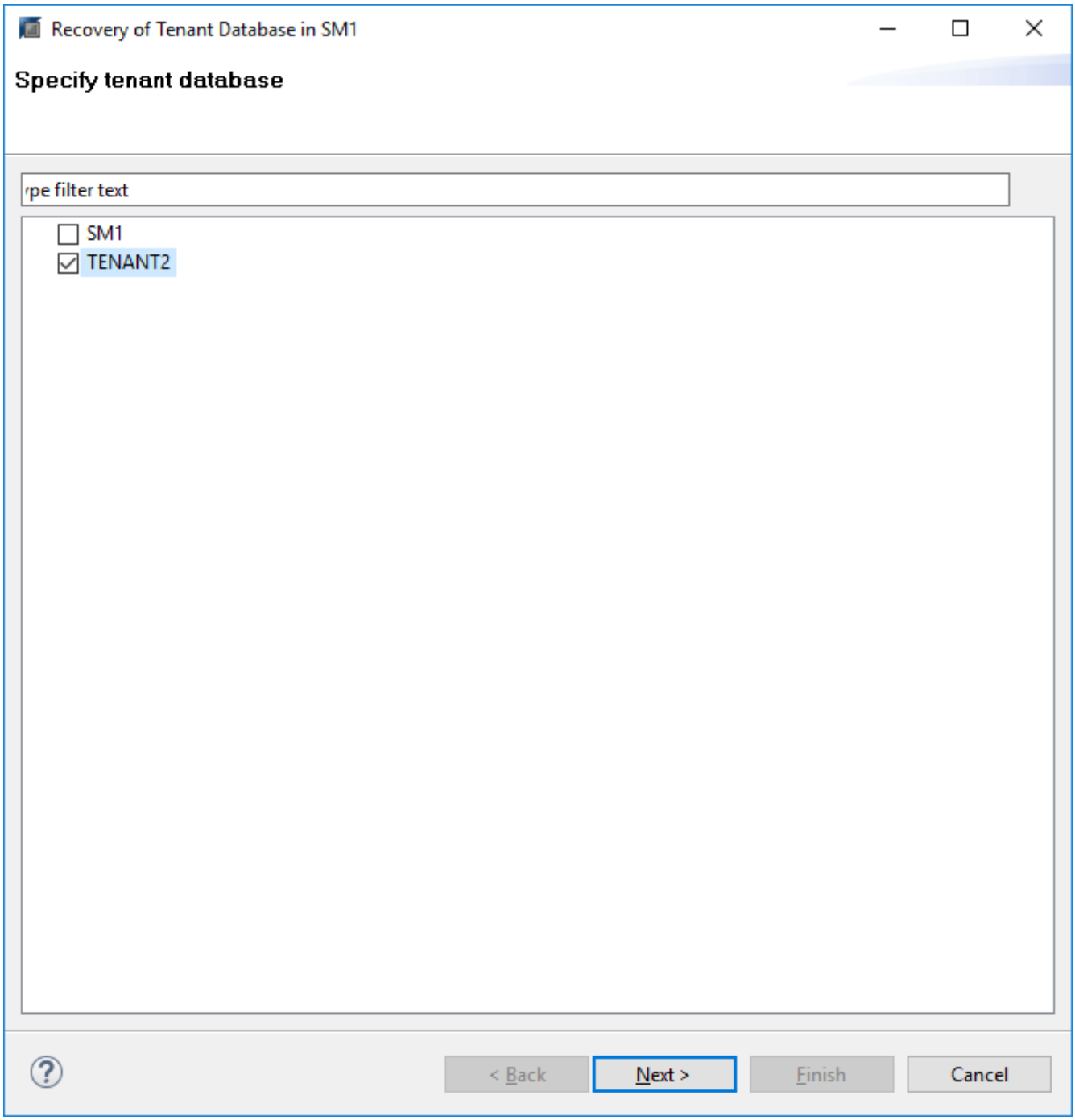
When the tenant restore operation is finished, only the tenant relevant data is restored. On the file system of the HANA database host, the restored data file and the Snapshot backup ID file of the tenant is available.

```
sm1adm@hana-2:/usr/sap/SM1/HDB00> ls -al /hana/data/SM1/mnt00001/*
-rw-r--r-- 1 sm1adm sapsys   17 Dec  6 04:01
/hana/data/SM1/mnt00001/nameserver.lck
/hana/data/SM1/mnt00001/hdb00001:
total 3417776
drwxr-x--- 2 sm1adm sapsys       4096 Dec  6 01:14 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r----- 1 sm1adm sapsys 3758096384 Dec  6 03:59 datavolume_0000.dat
-rw-r----- 1 sm1adm sapsys          0 Nov 20 08:36
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 sm1adm sapsys         36 Nov 20 08:37 landscape.id
/hana/data/SM1/mnt00001/hdb00002.00003:
total 67772
drwxr-xr-- 2 sm1adm sapsys      4096 Nov 20 08:37 .
drwxr-x--- 6 sm1adm sapsys      4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 201441280 Dec  6 03:59 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys         0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
/hana/data/SM1/mnt00001/hdb00002.00004:
total 3411836
drwxr-xr-- 2 sm1adm sapsys       4096 Dec  6 03:57 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 3758096384 Dec  6 01:14 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys          0 Nov 20 09:35
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 sm1adm sapsys     155648 Dec  6 01:14
snapshot_databackup_0_1
/hana/data/SM1/mnt00001/hdb00003.00003:
total 3364216
drwxr-xr-- 2 sm1adm sapsys       4096 Dec  6 01:14 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 3758096384 Dec  6 03:59 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys          0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
sm1adm@hana-2:/usr/sap/SM1/HDB00>
```

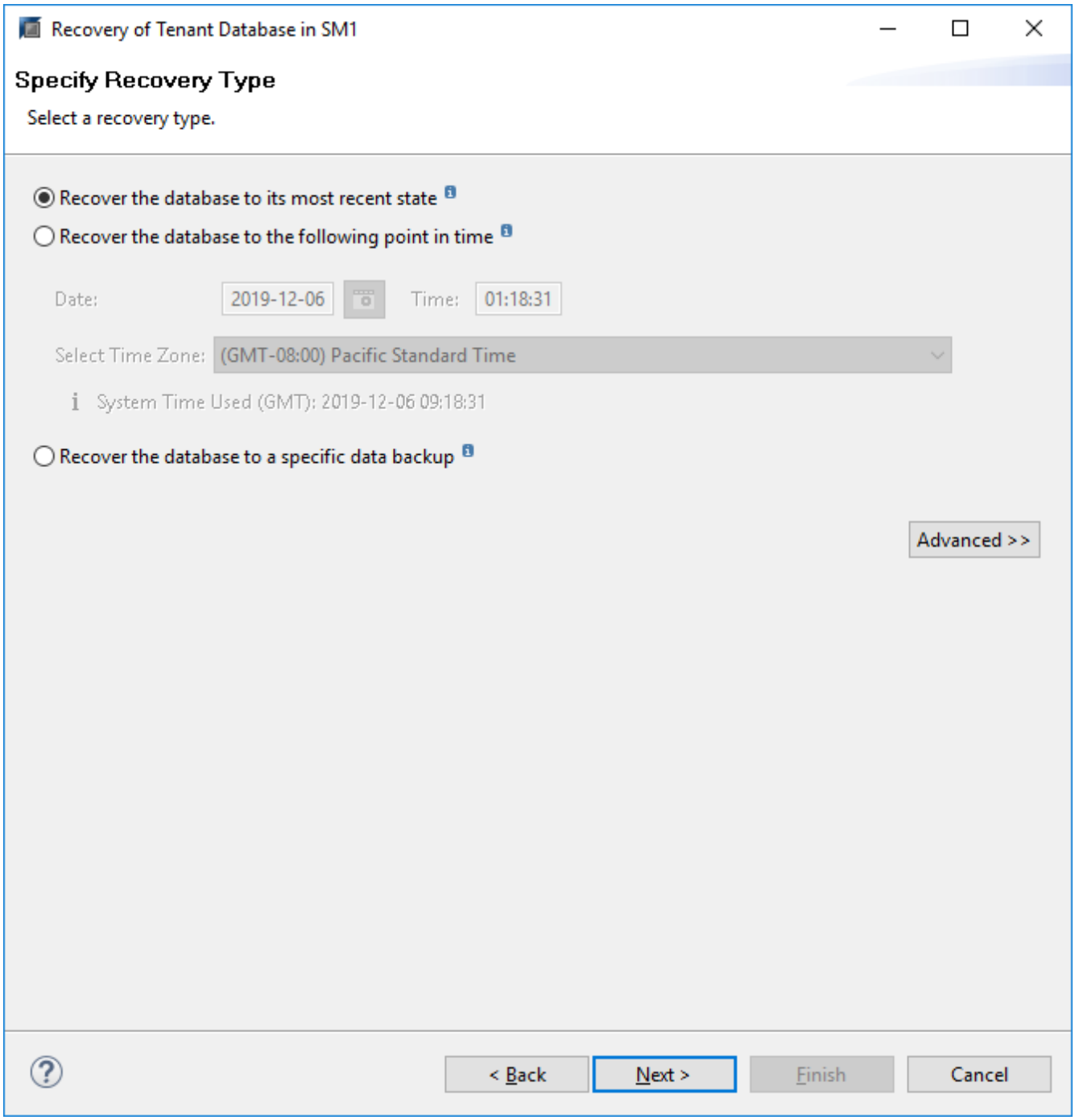
8. Start the recovery with HANA Studio.



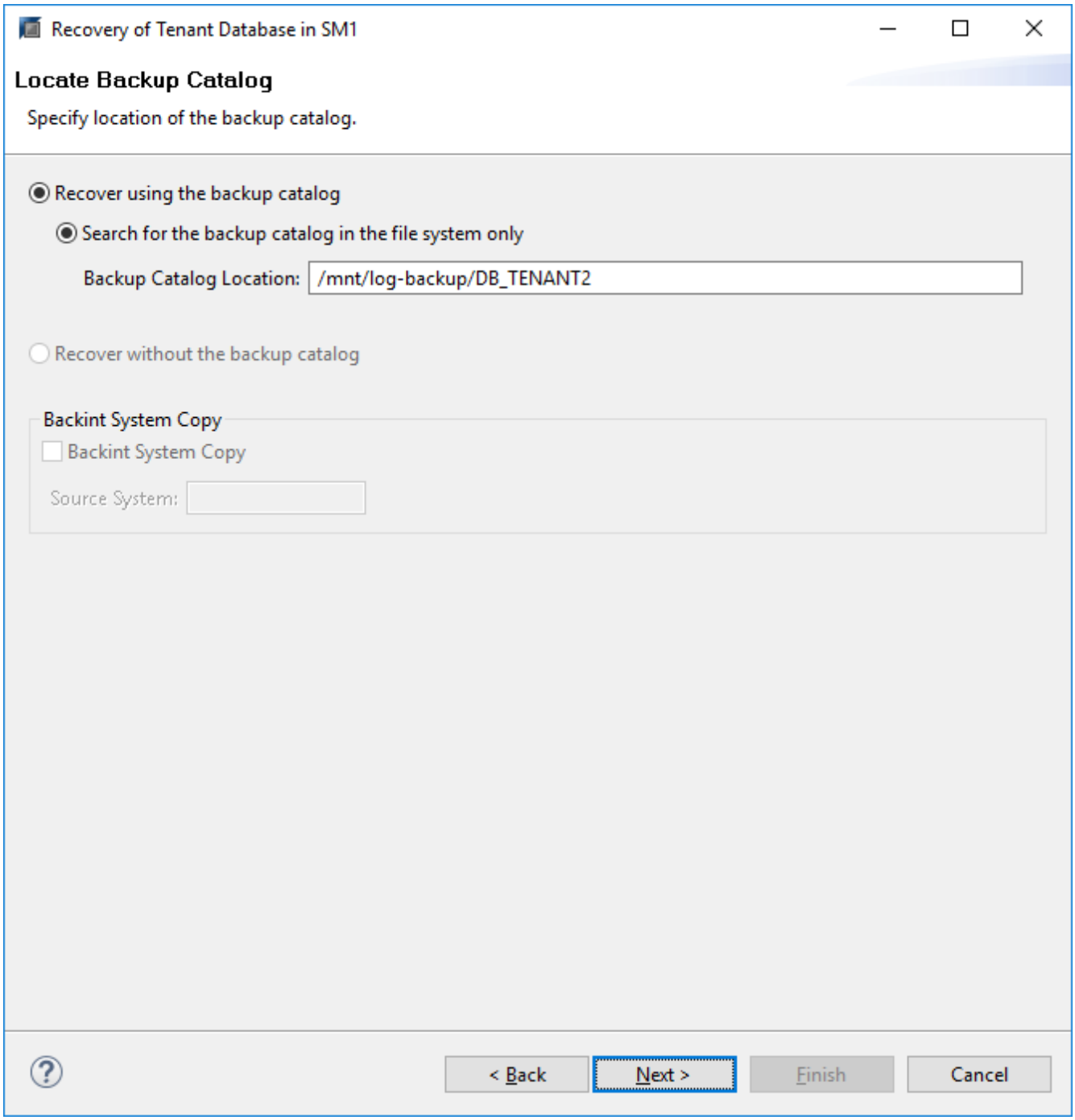
9. Select the tenant.

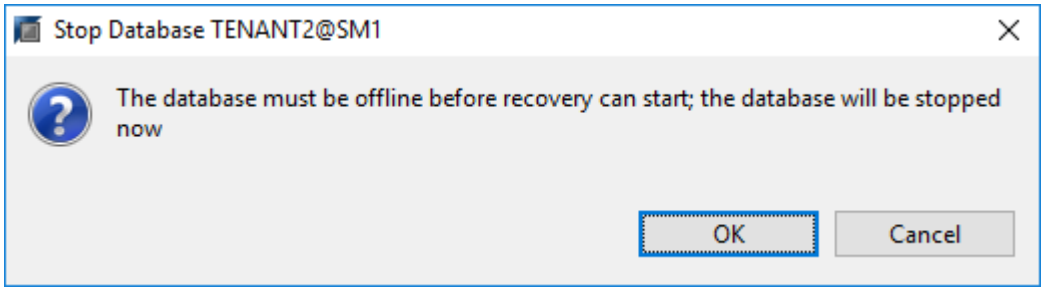


10. Select the recovery type.



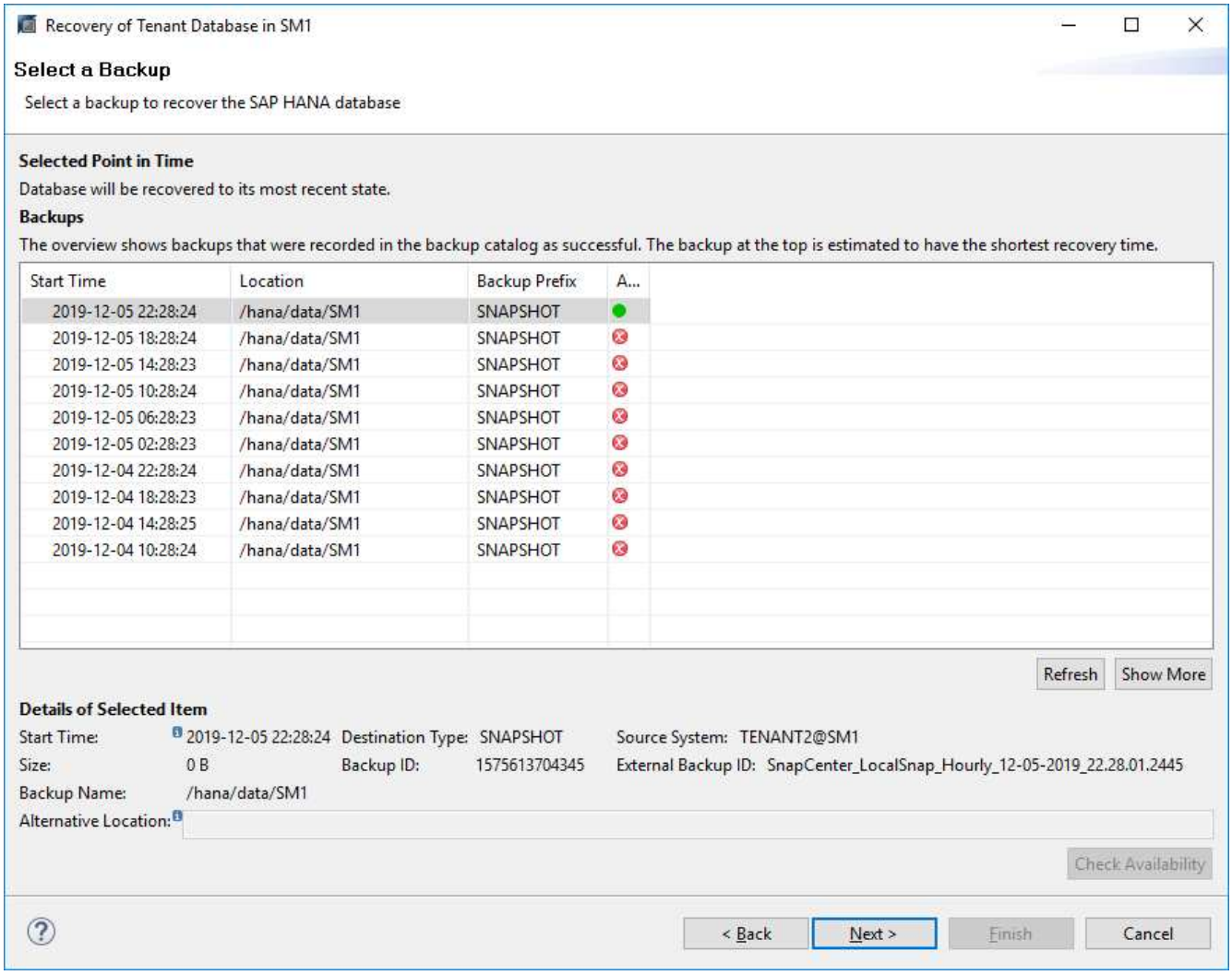
11. Provide the backup catalog location.



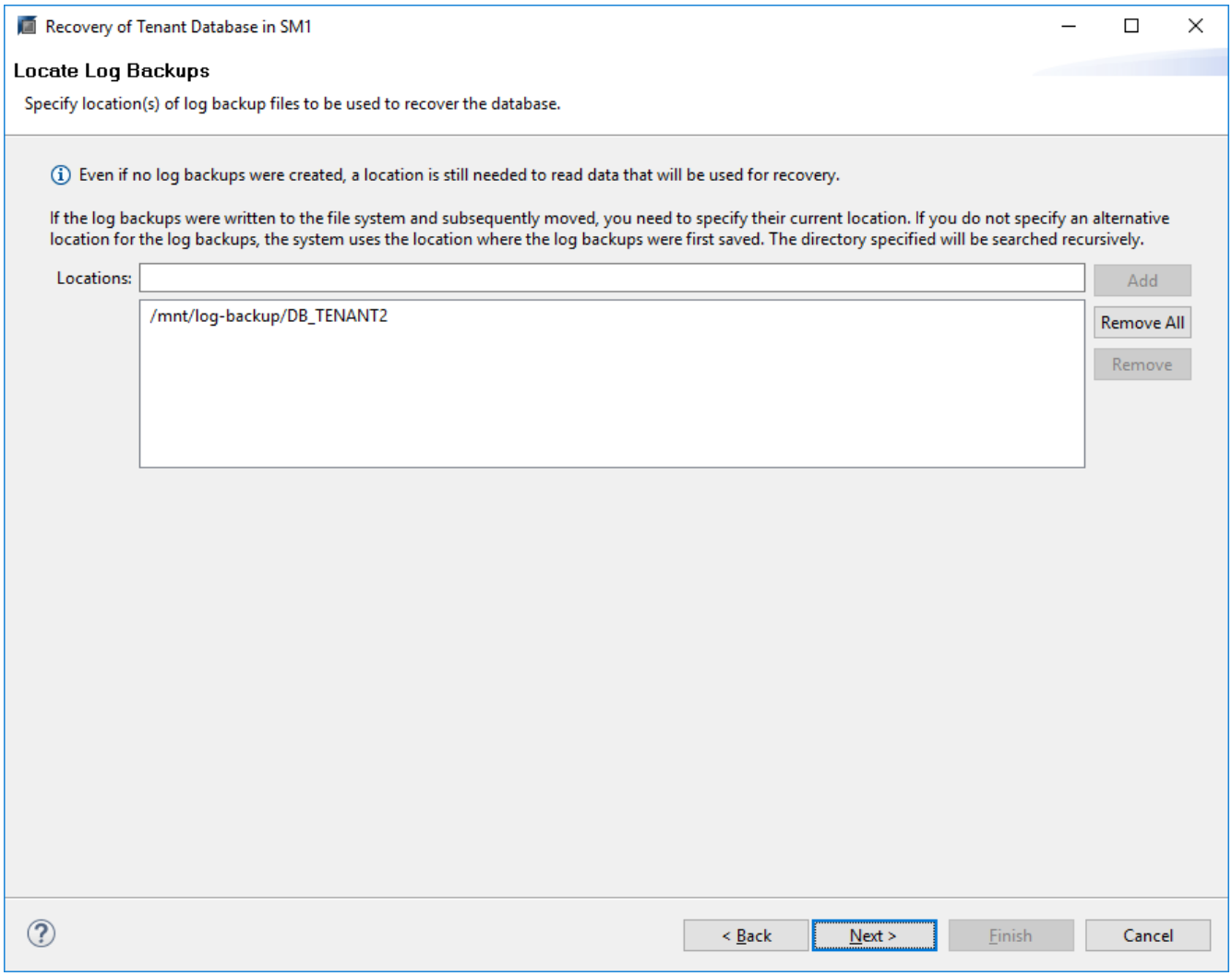


Within the backup catalog, the restored backup is highlighted with a green icon. The external backup ID shows the backup name that was previously selected in SnapCenter.

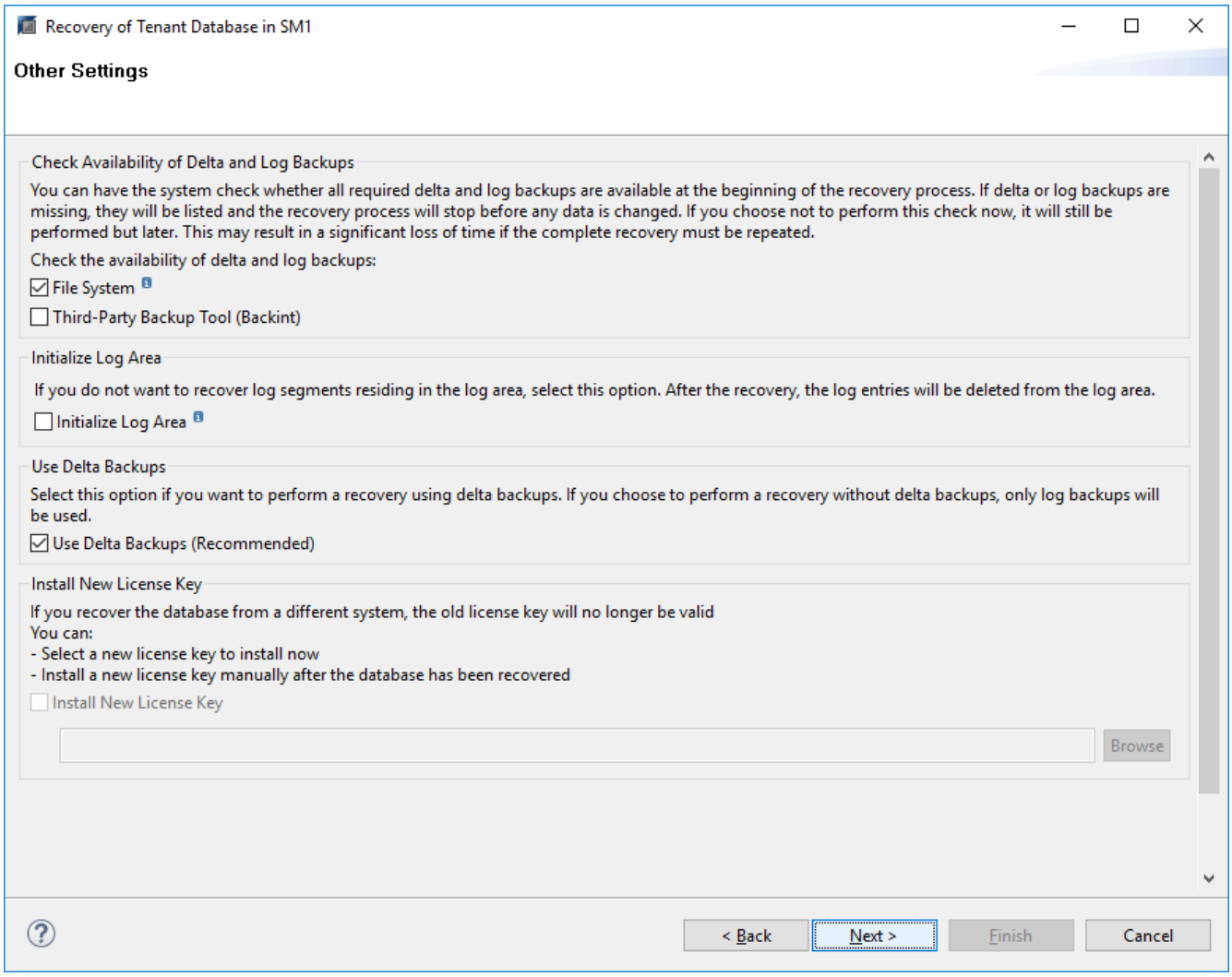
12. Select the entry with the green icon and click Next.



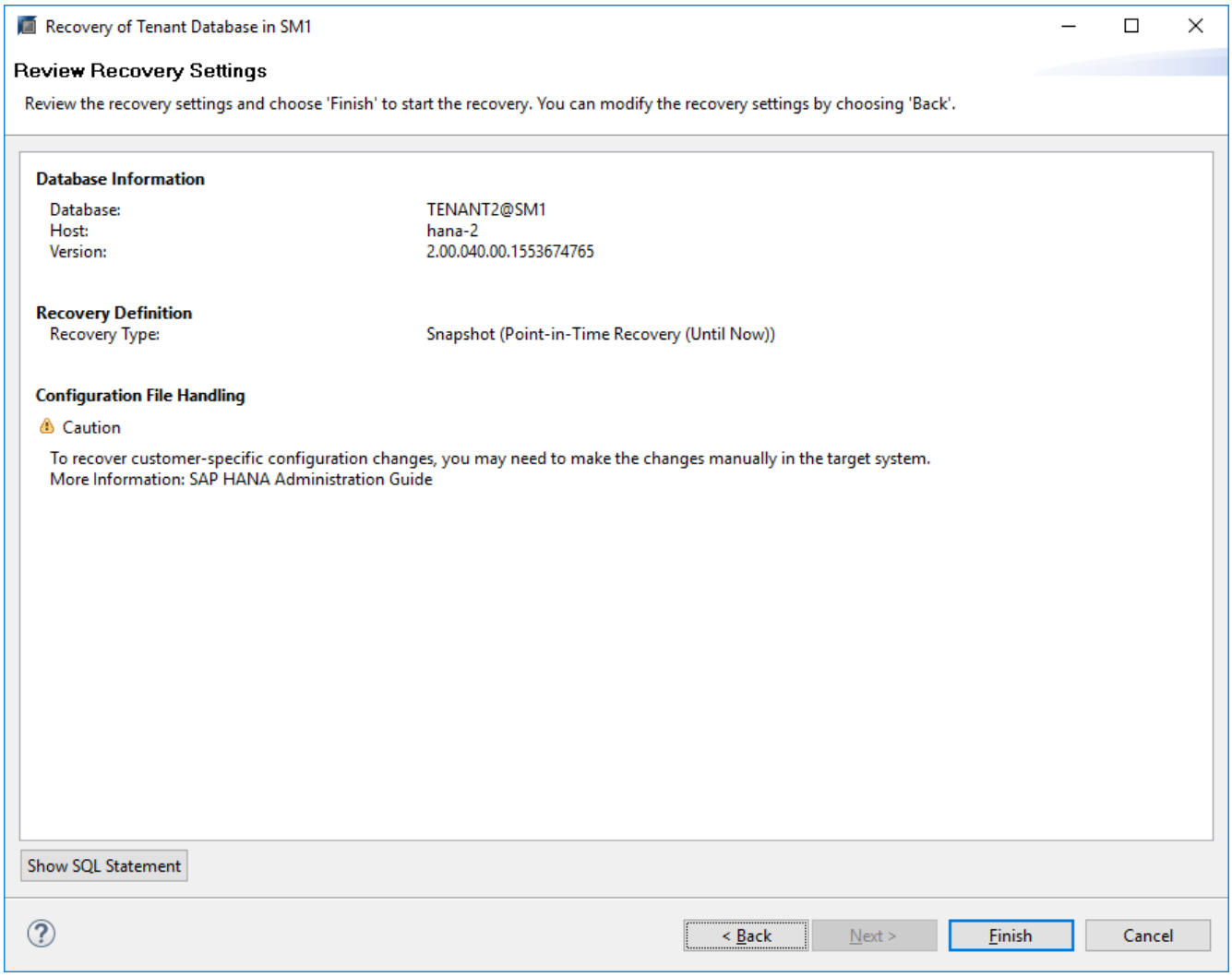
13. Provide the log backup location.

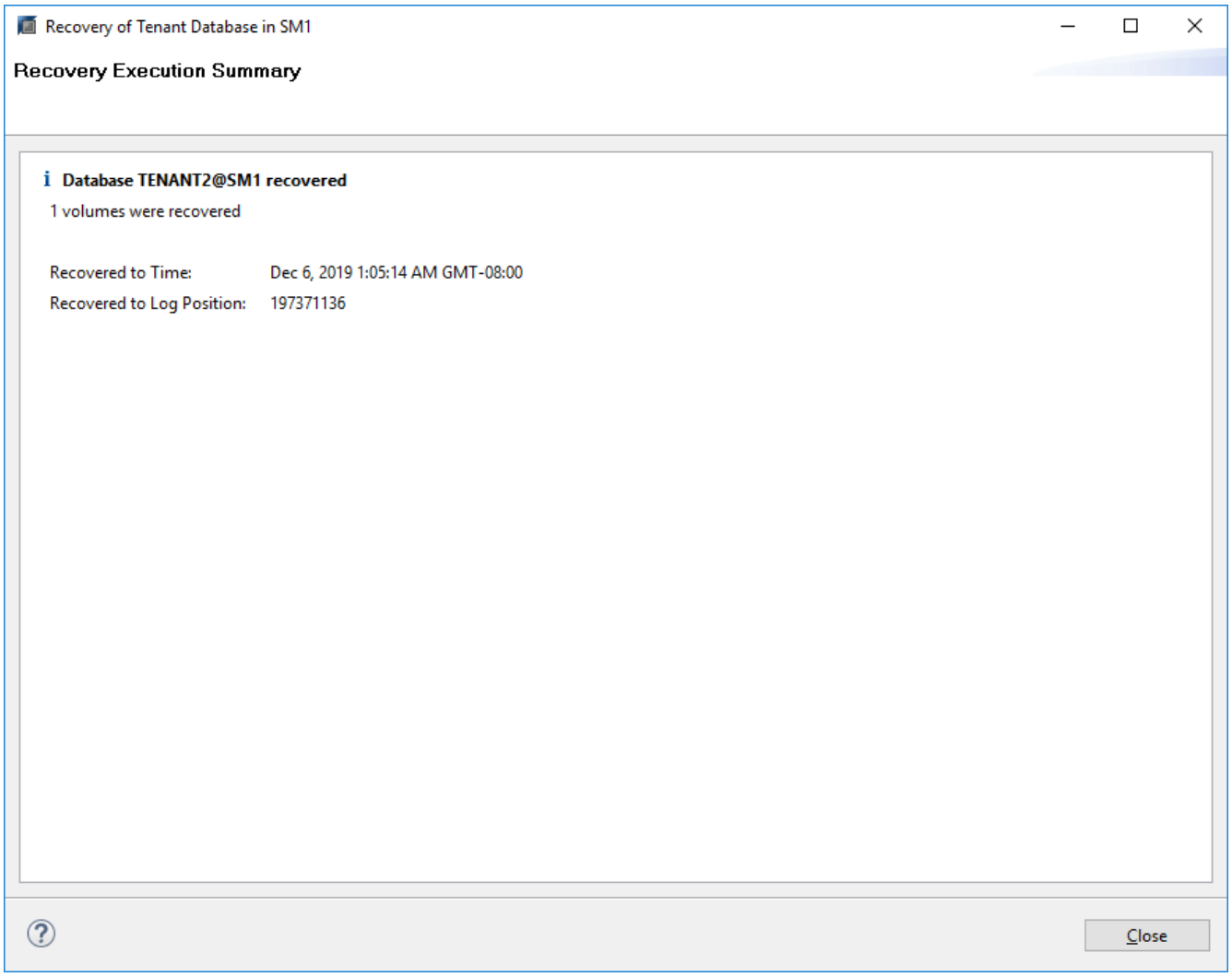


14. Select the other settings as required.



15. Start the tenant recovery operation.


Recovery of Tenant Database in SM1
Review Recovery Settings
Review the recovery settings and choose 'Finish' to start the recovery. You can modify the recovery settings by choosing 'Back'.
Database Information
Database: TENANT2@SM1
Host: hana-2
Version: 2.00.040.00.1553674765
Recovery Definition
Recovery Type: Snapshot (Point-in-Time Recovery (Until Now))
Configuration File Handling
Caution
To recover customer-specific configuration changes, you may need to make the changes manually in the target system.
More Information: SAP HANA Administration Guide
Show SQL Statement
< Back
Next >
Finish
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.

> 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.

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.

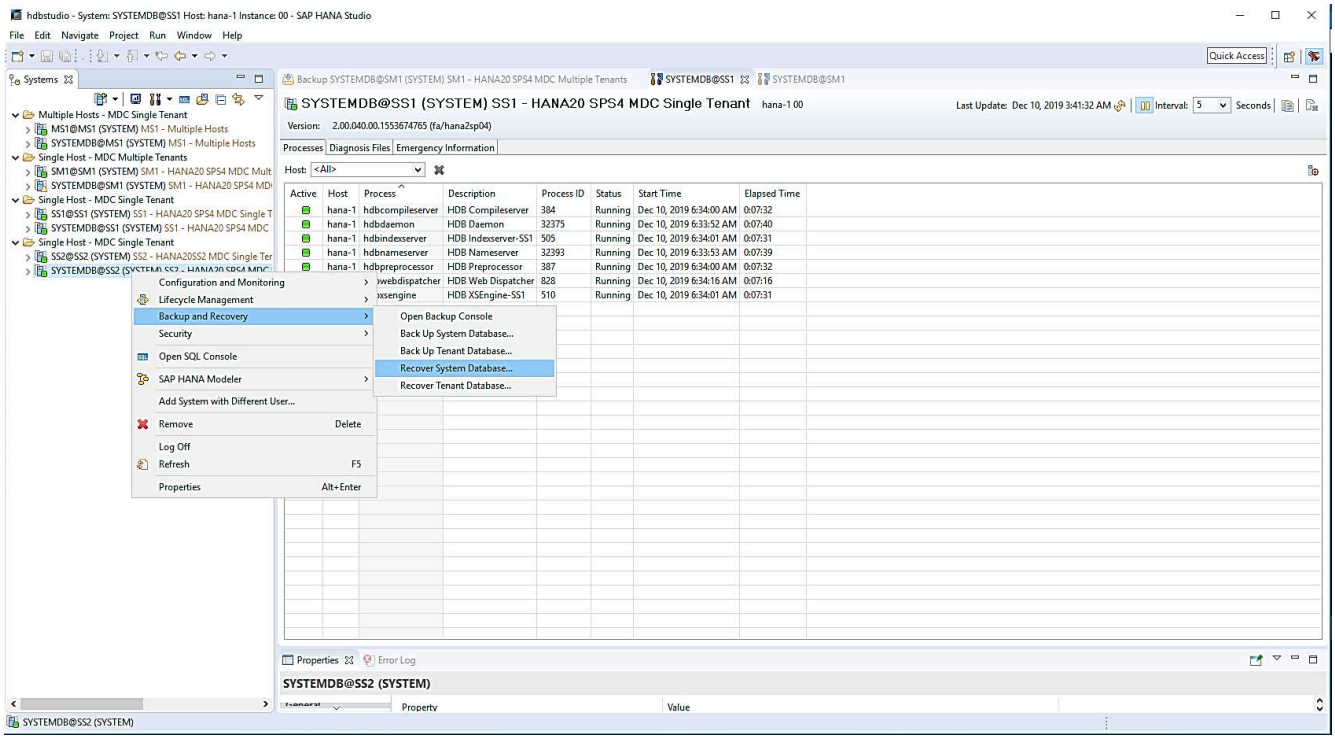
3. Run the recovery process for the system database with SAP HANA Studio:
   a. Click Refresh from the backup list and select the available backup for recovery (indicated with a green icon).
   b. Start the recovery process. After the recovery process is finished, the system database is started.
4. Run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

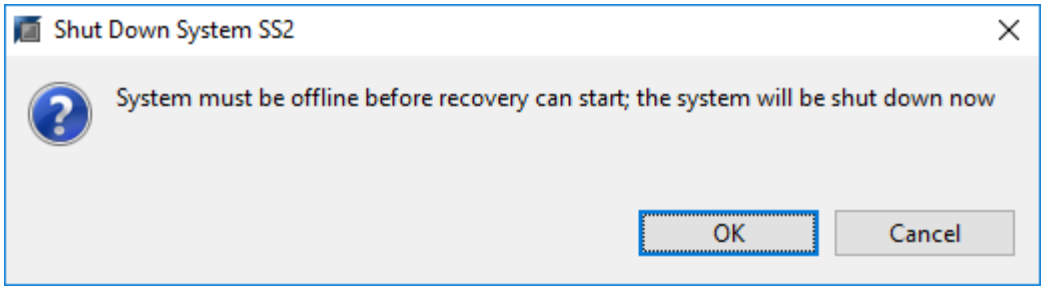
   c. Select this backup and start the recovery process. After the recovery process is finished, the tenant database is started automatically.

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.

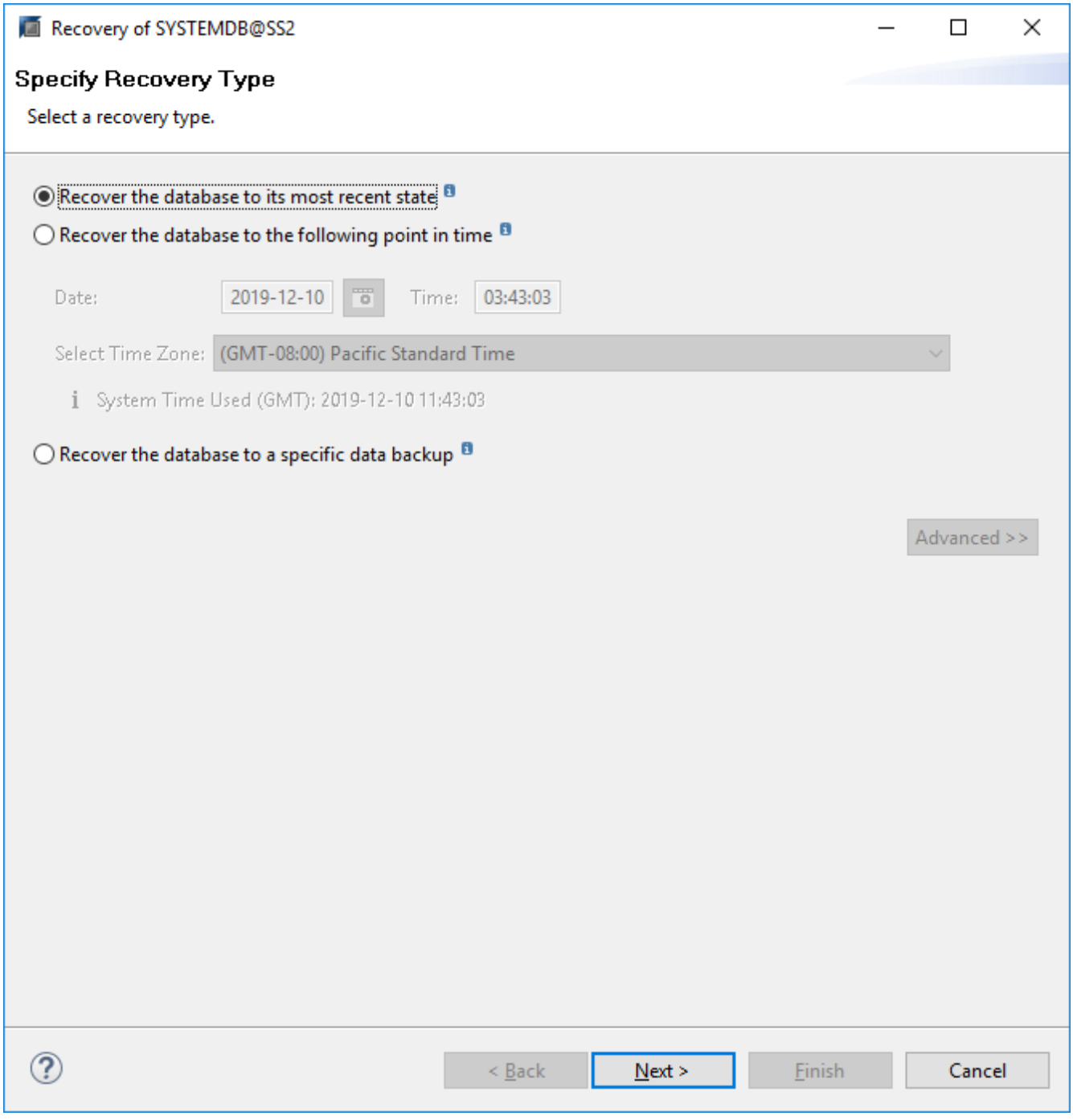


2. Click OK to shut down the SAP HANA database.

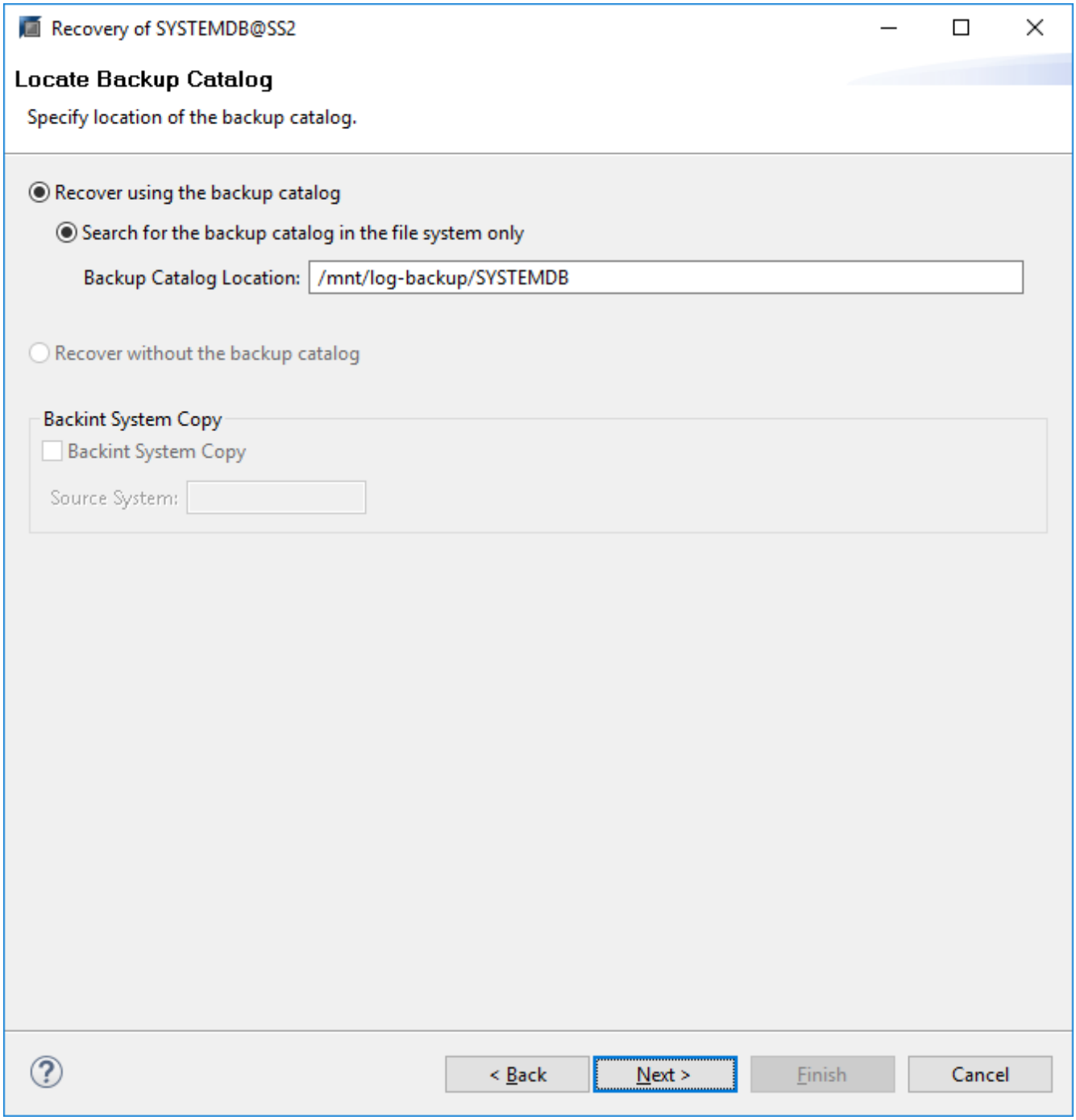


The SAP HANA system shuts down and the recovery wizard is started.

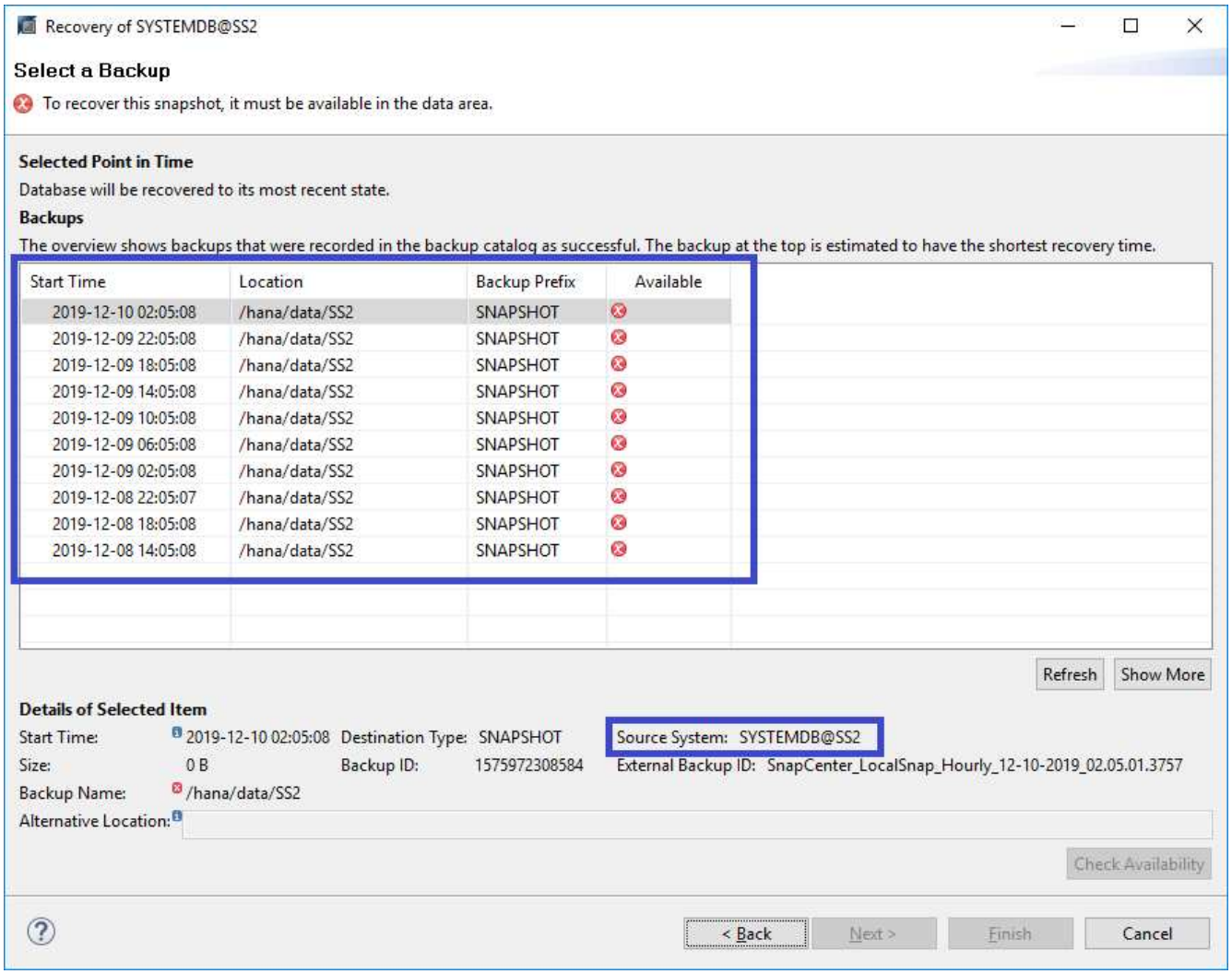
3. Select the recovery type and click Next.



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



5. A list of available backups displays based on the content of the backup catalog. Choose the required backup and note the external backup ID: in our example, the most recent backup.



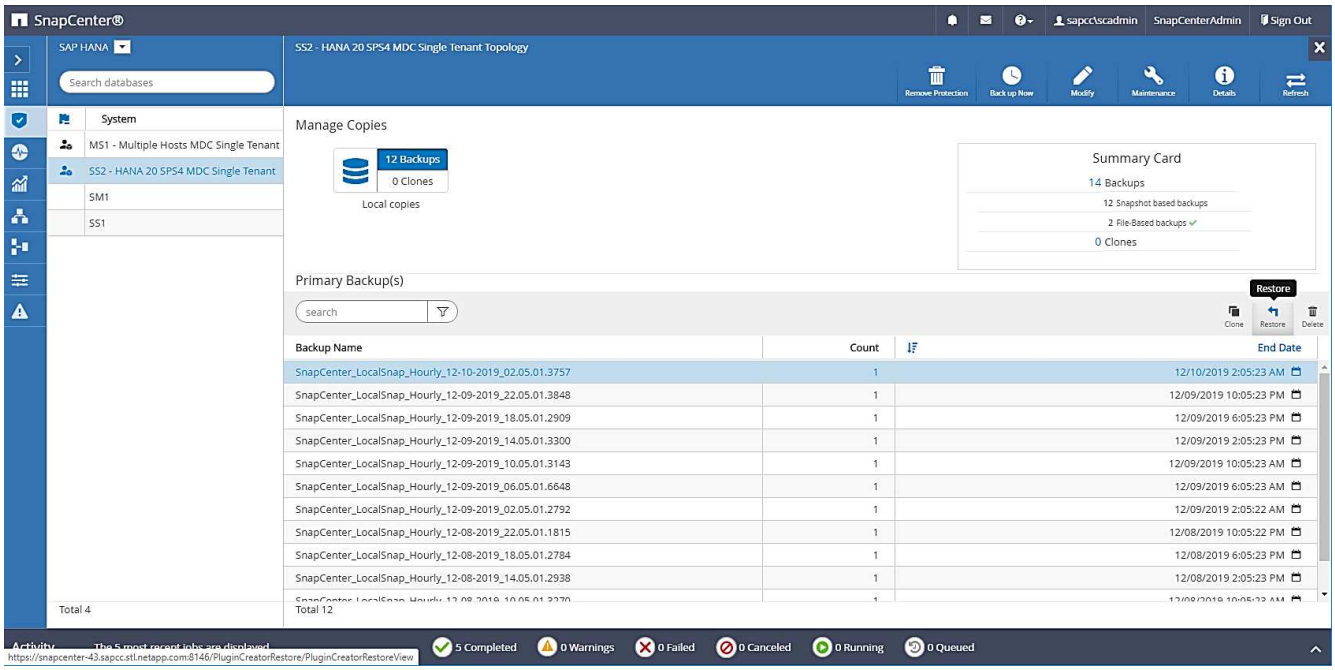
6. Unmount all data volumes.

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

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

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

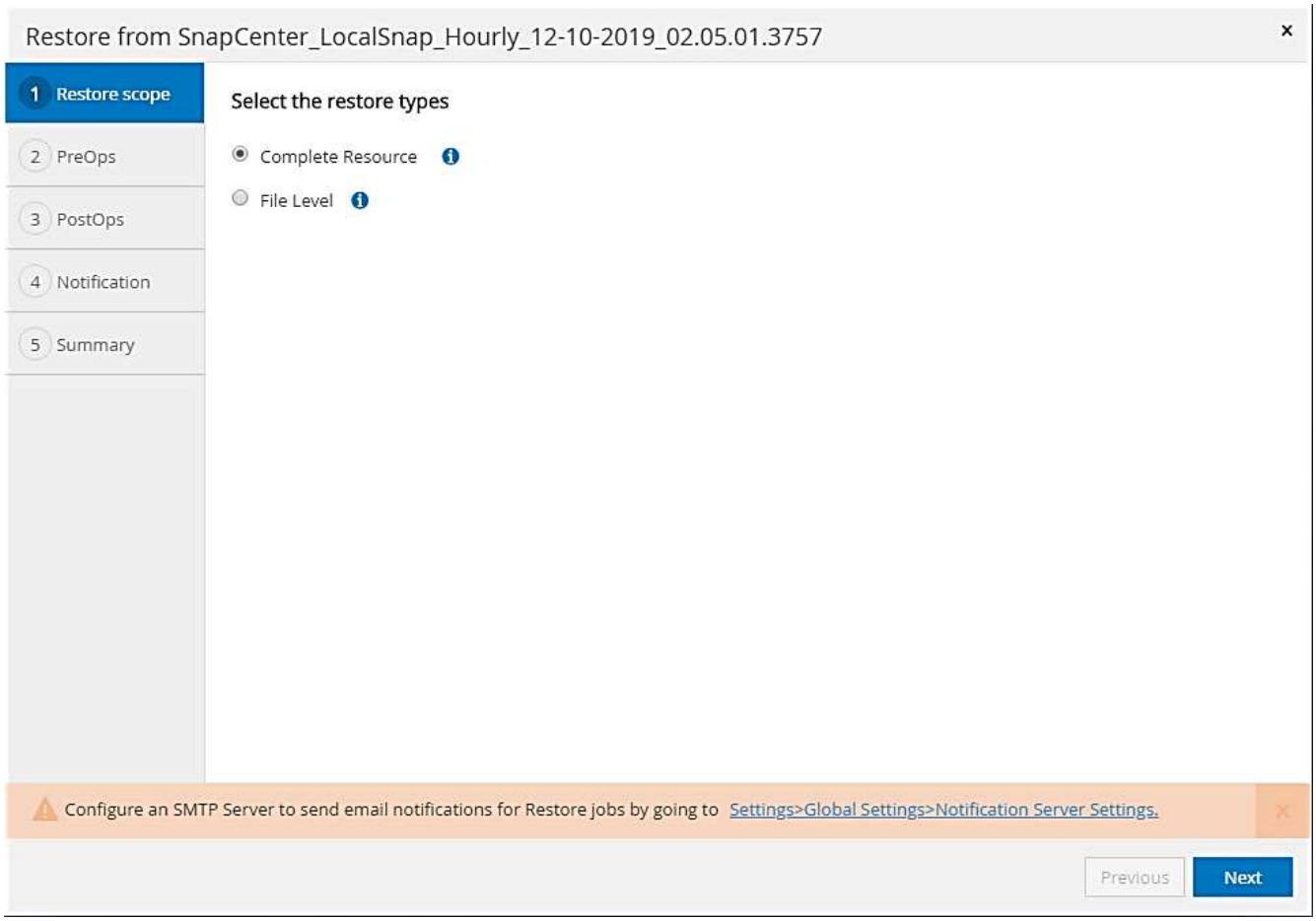
7. From the SnapCenter GUI, select the resource topology view and select the backup that should be restored; in our example, the most recent primary backup. Click the Restore icon to start the restore.



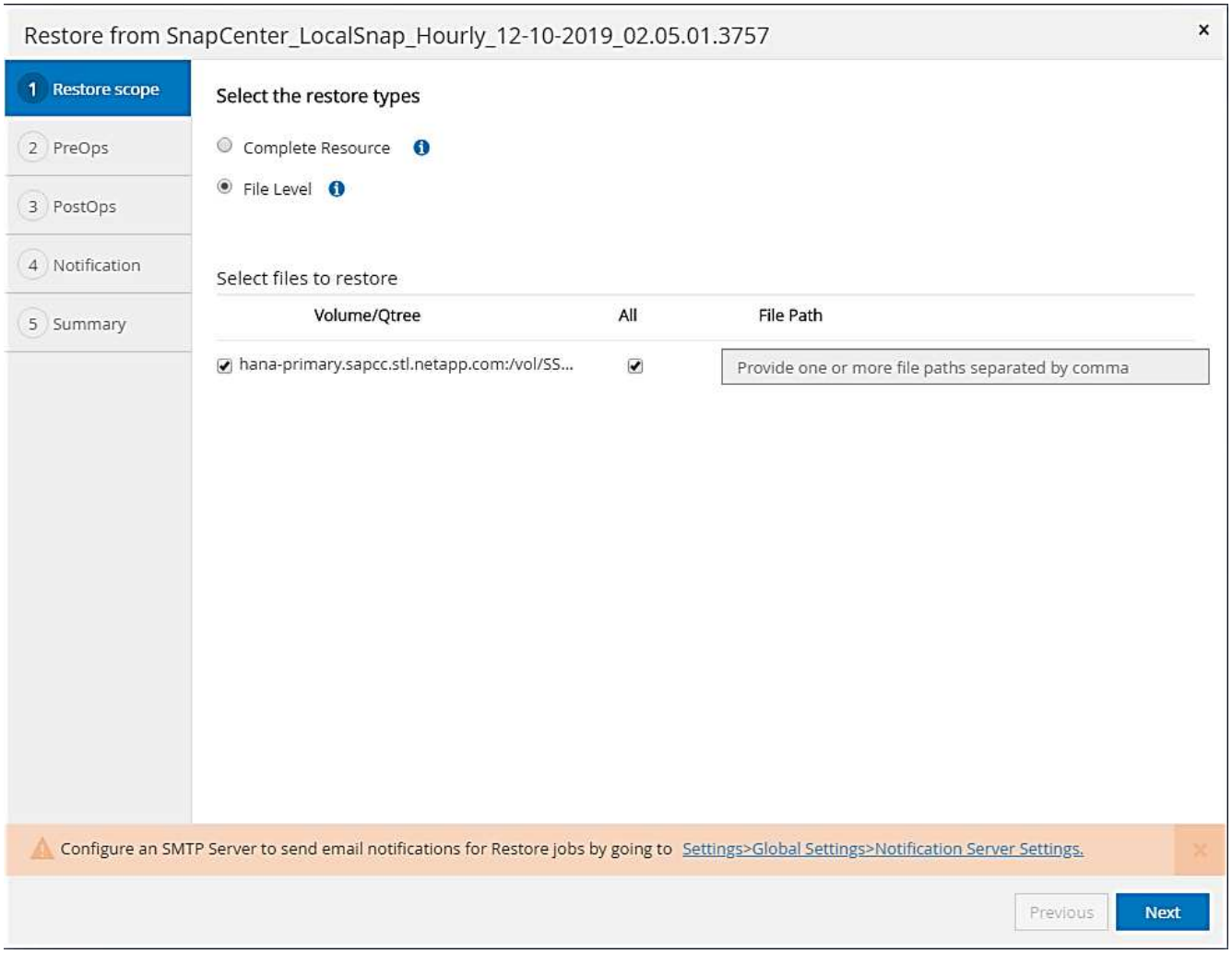
The SnapCenter restore wizard starts.

8. Select the restore type Complete Resource or File Level.

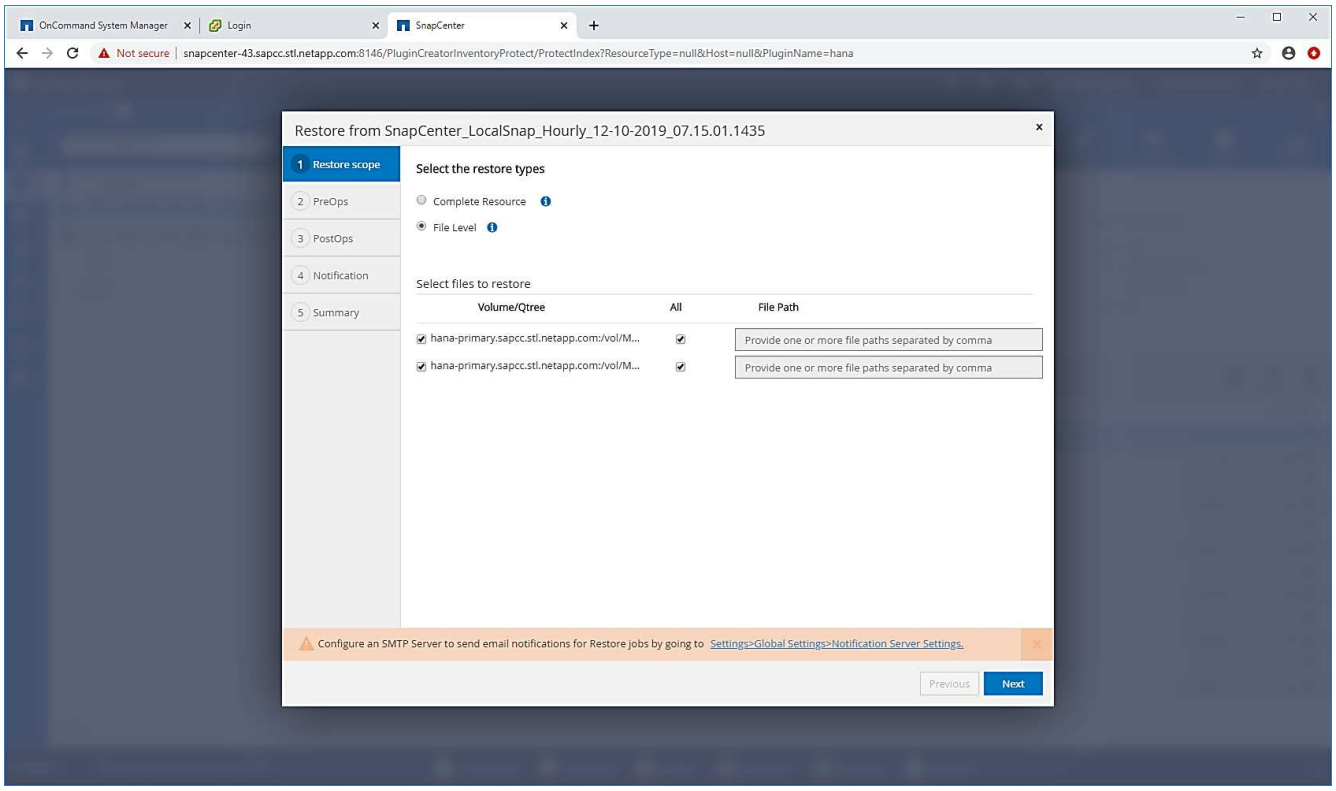
   Select Complete Resource to use a volume-based restore.



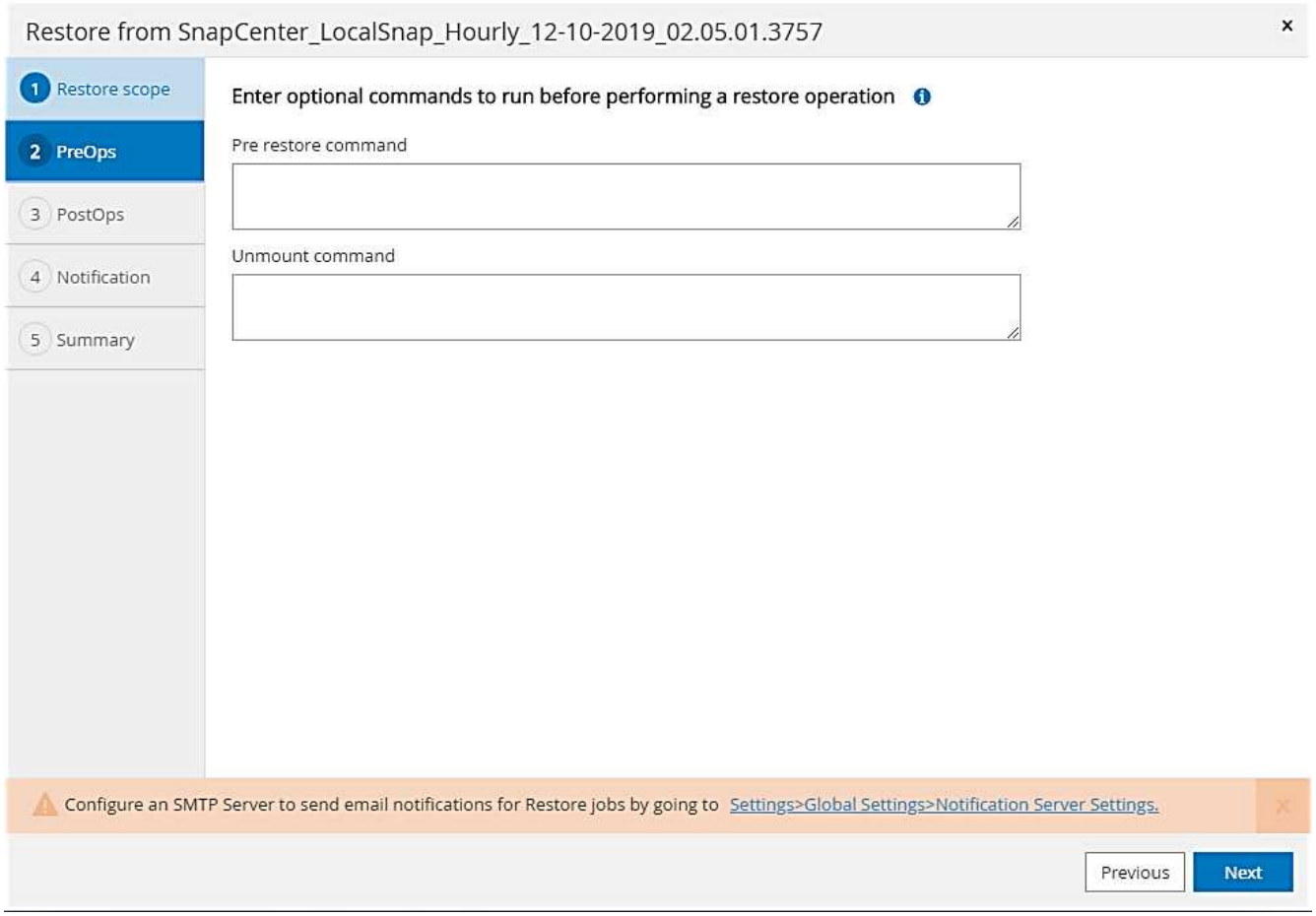
9. Select File Level and All to use a single-file SnapRestore operation for all files.



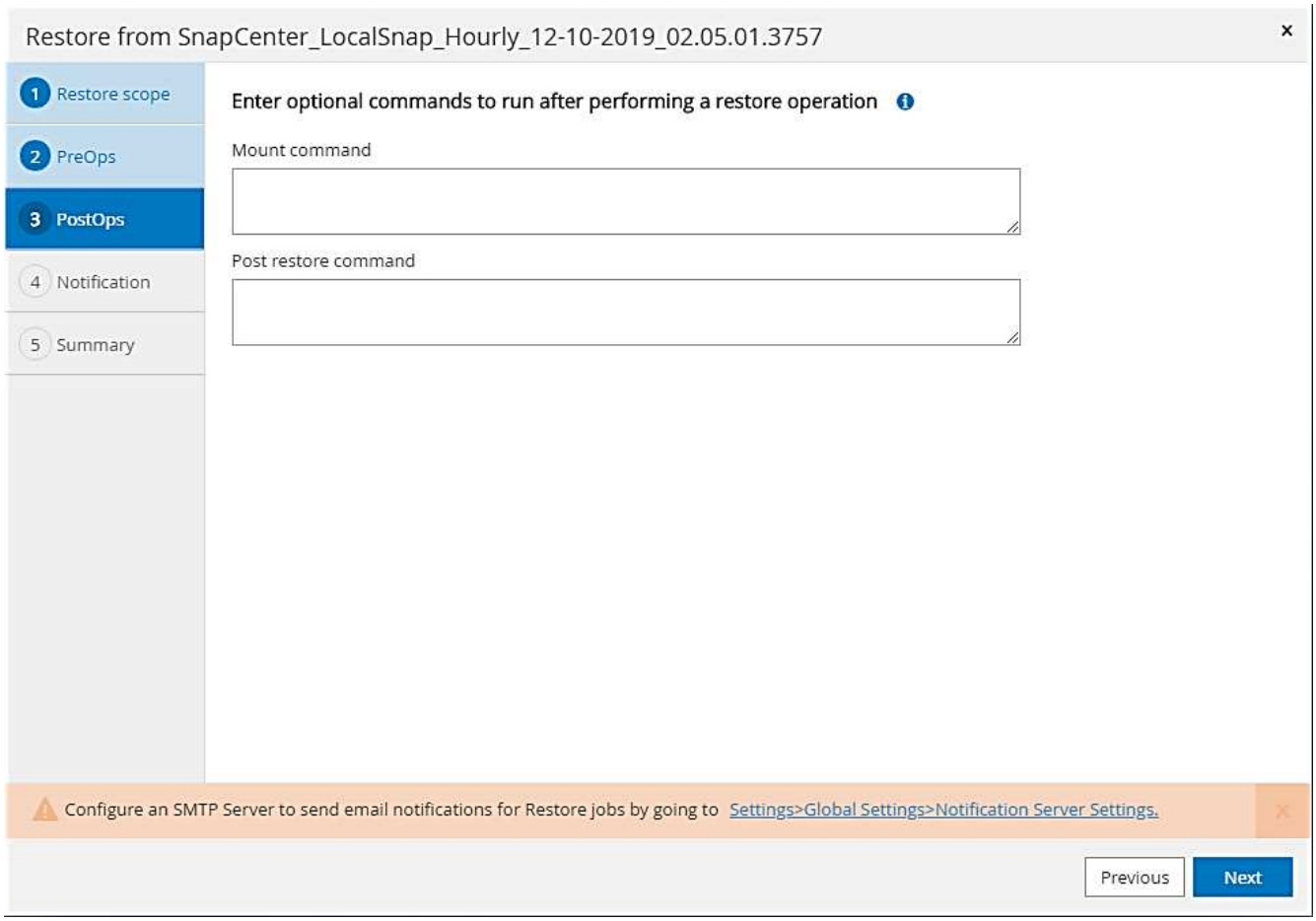
For a file-level restore of a SAP HANA multiple host system, select all the volumes.



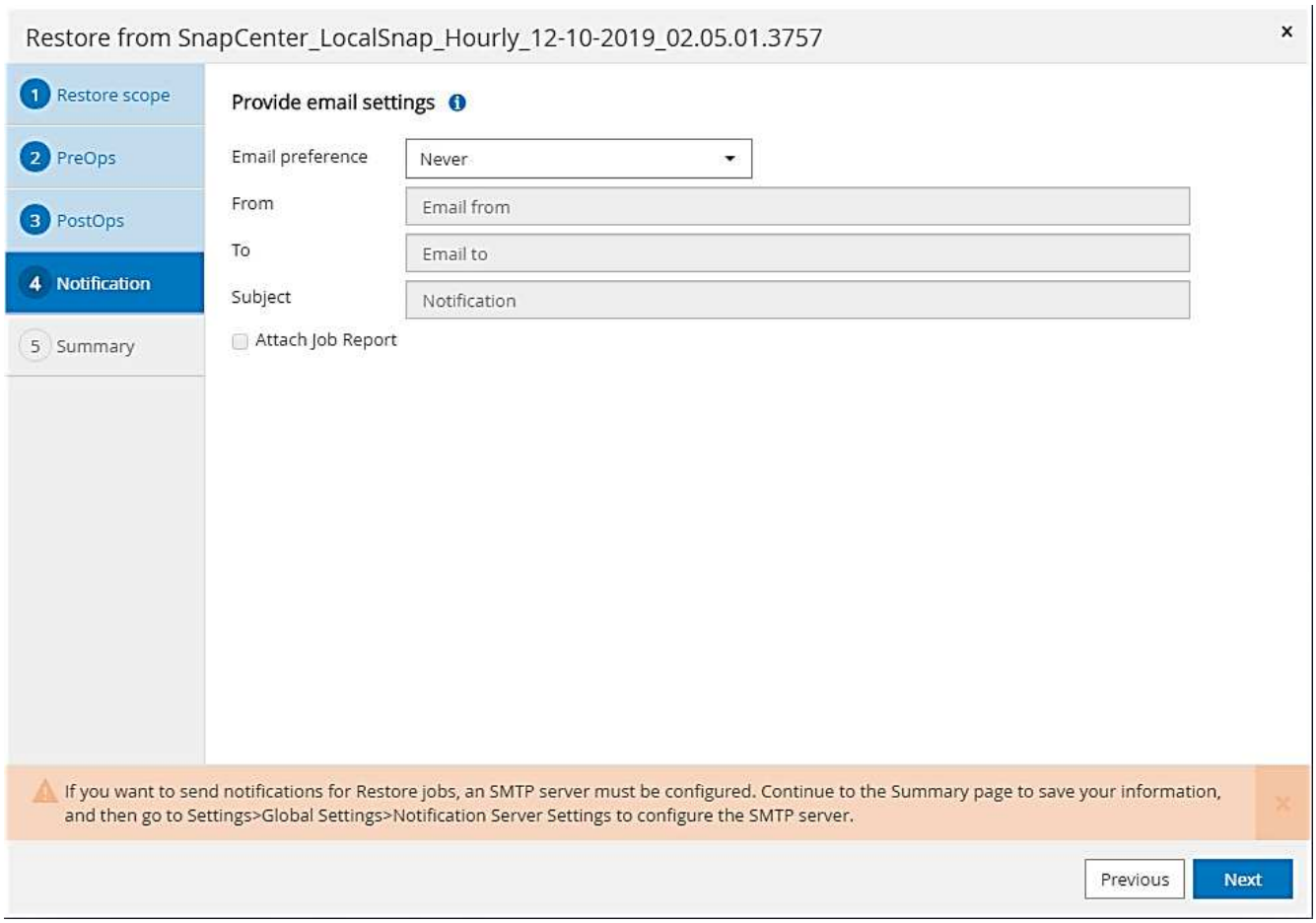
10. (Optional) Specify the commands that should be executed from the SAP HANA plug-in running on the central HANA plug-in host. Click Next.



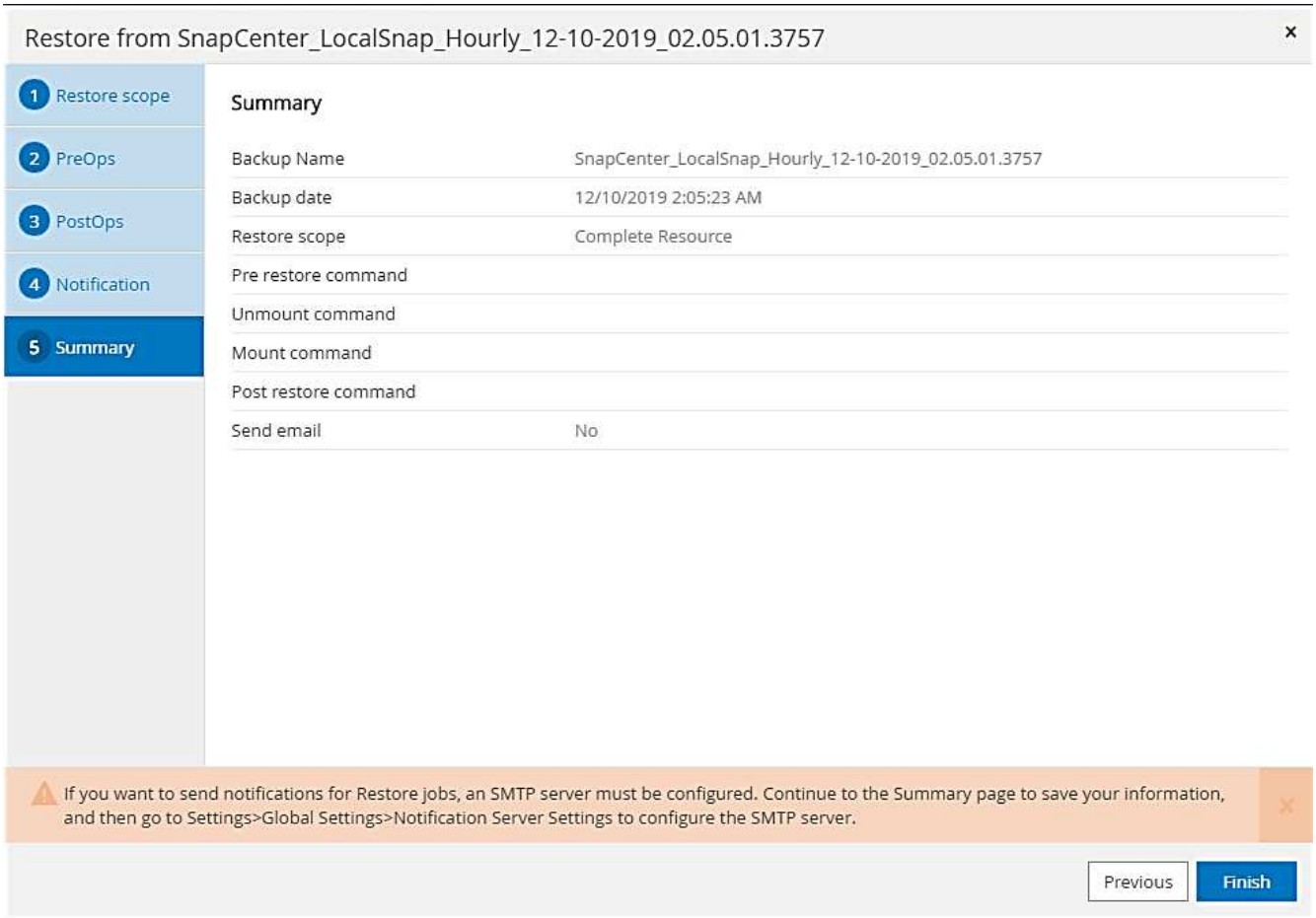
11. Specify the optional commands and click Next.



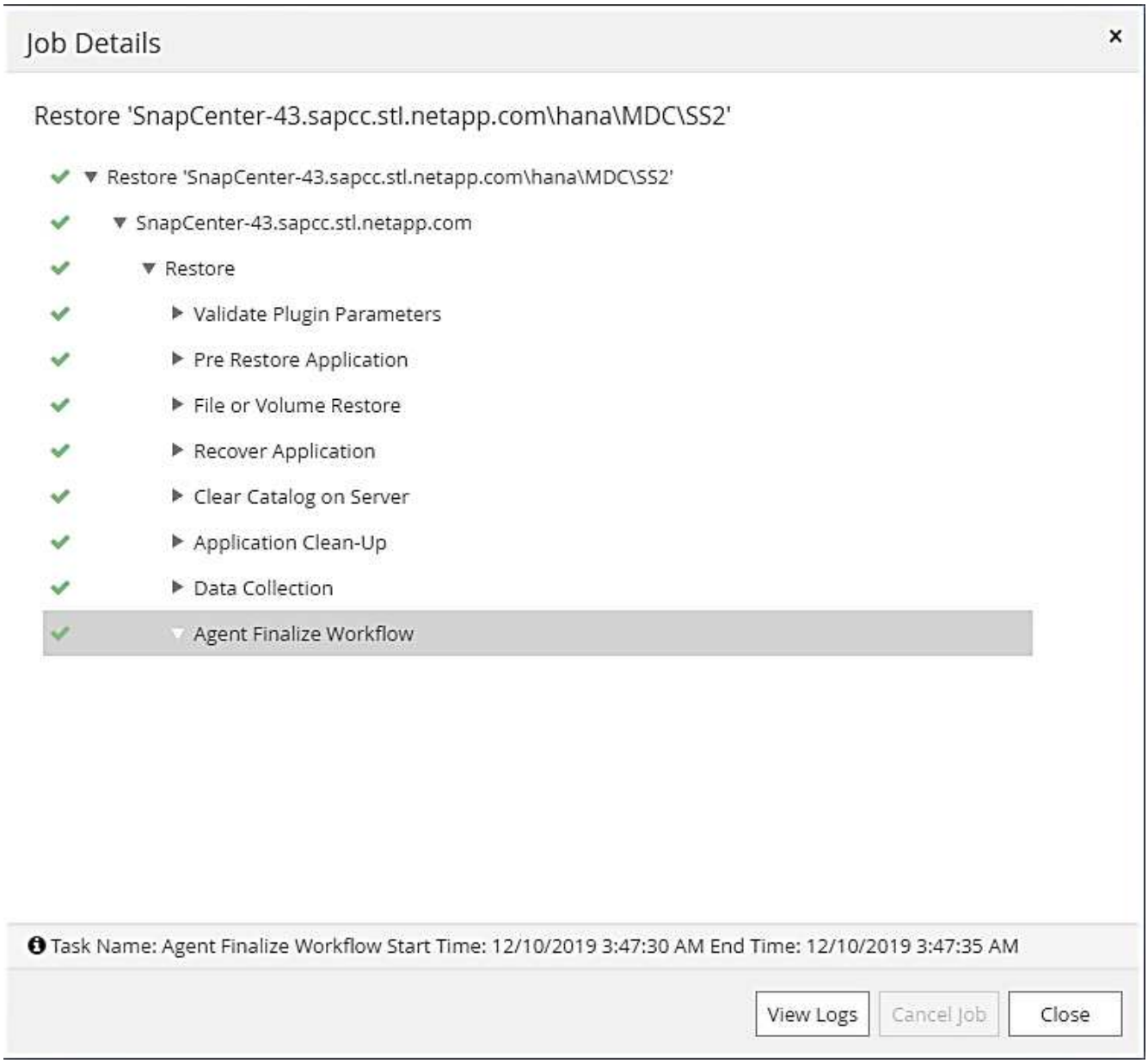
12. Specify the notification settings so that SnapCenter can send a status email and job log. Click Next.



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



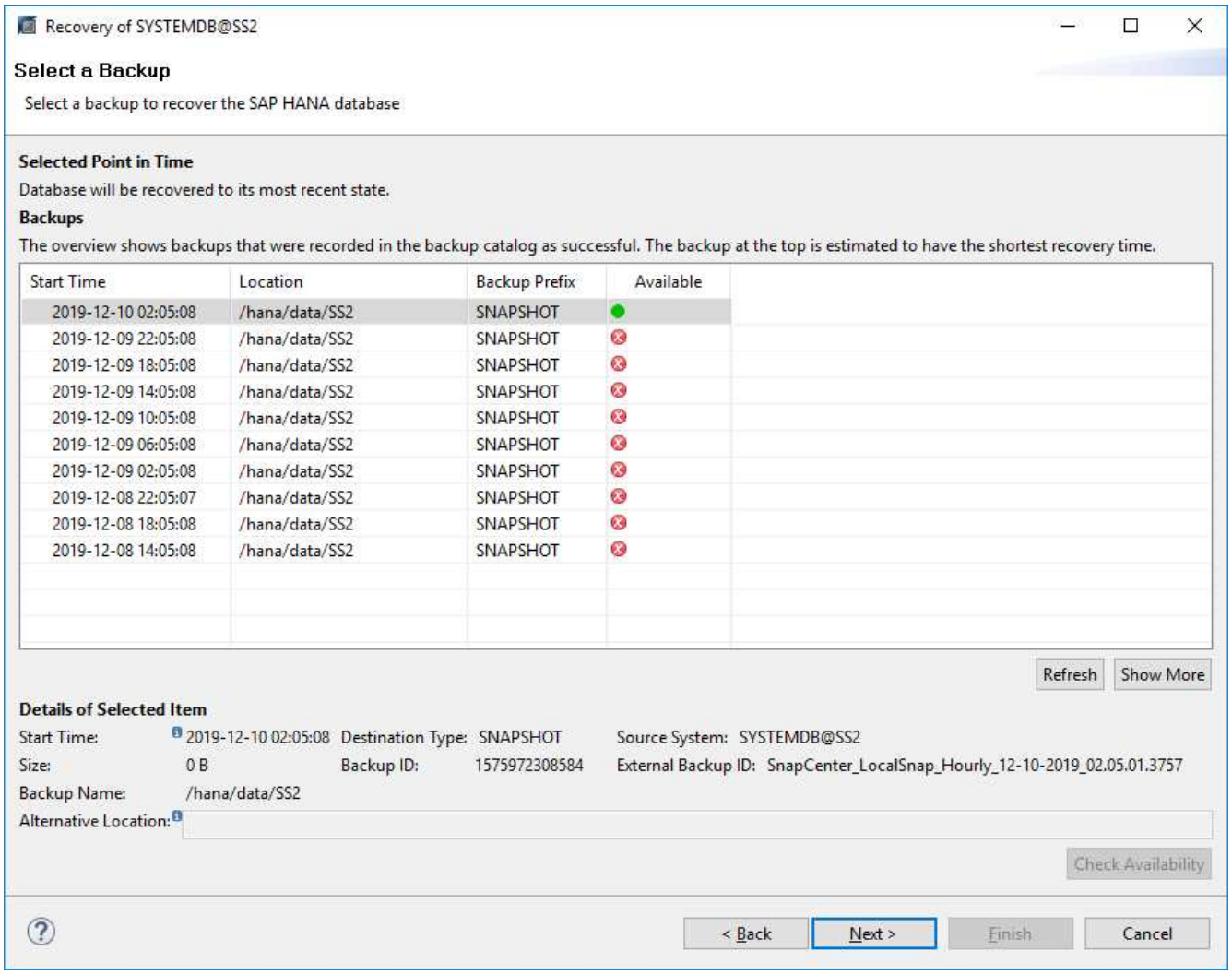
14. The restore job starts, and the job log can be displayed by double-clicking the log line in the activity pane.



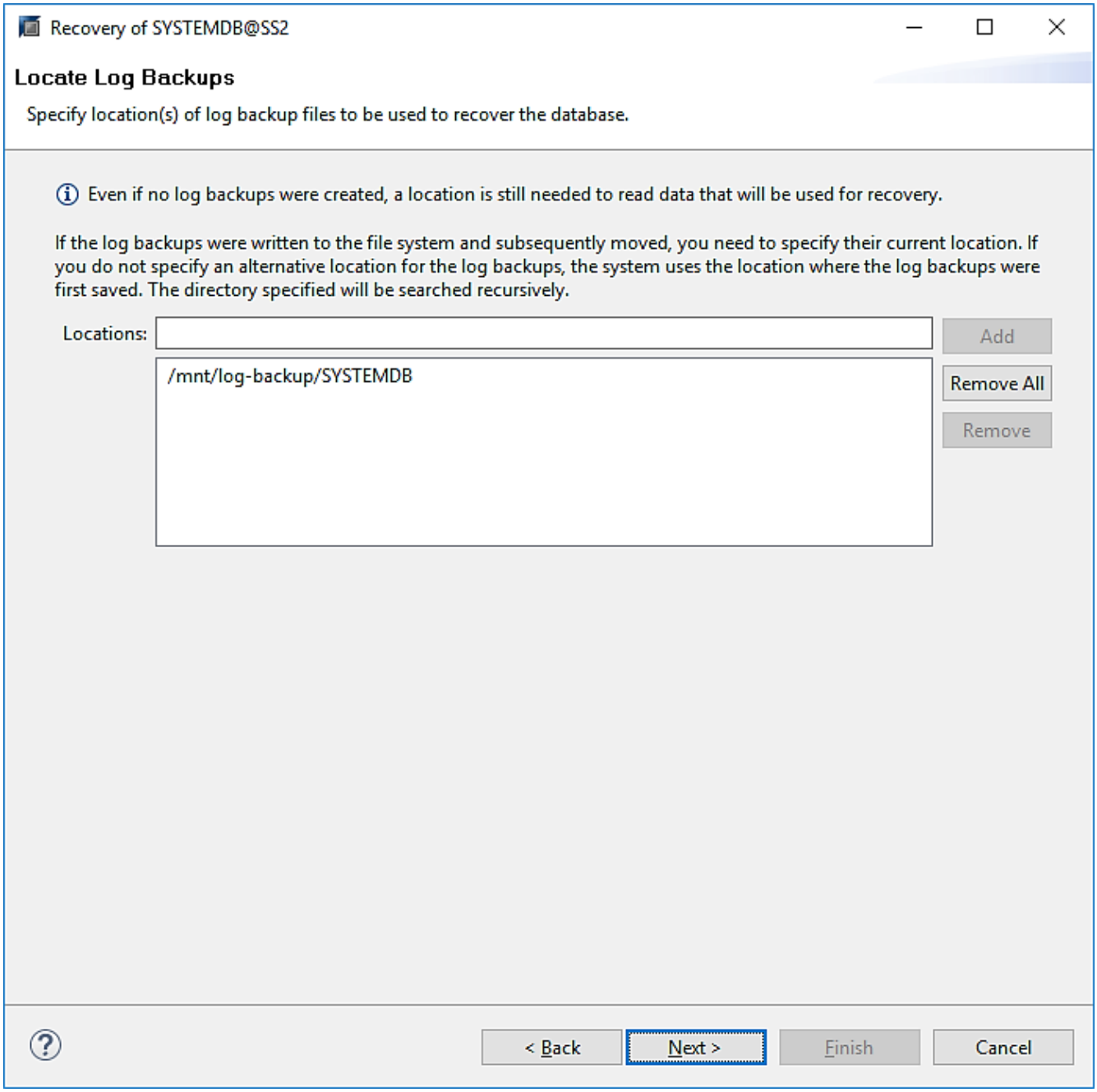
15. Wait until the restore process completes. On each database host, mount all data volumes. In our example, only one volume must be remounted on the database host.

```
mount /hana/data/SP1/mnt00001
```

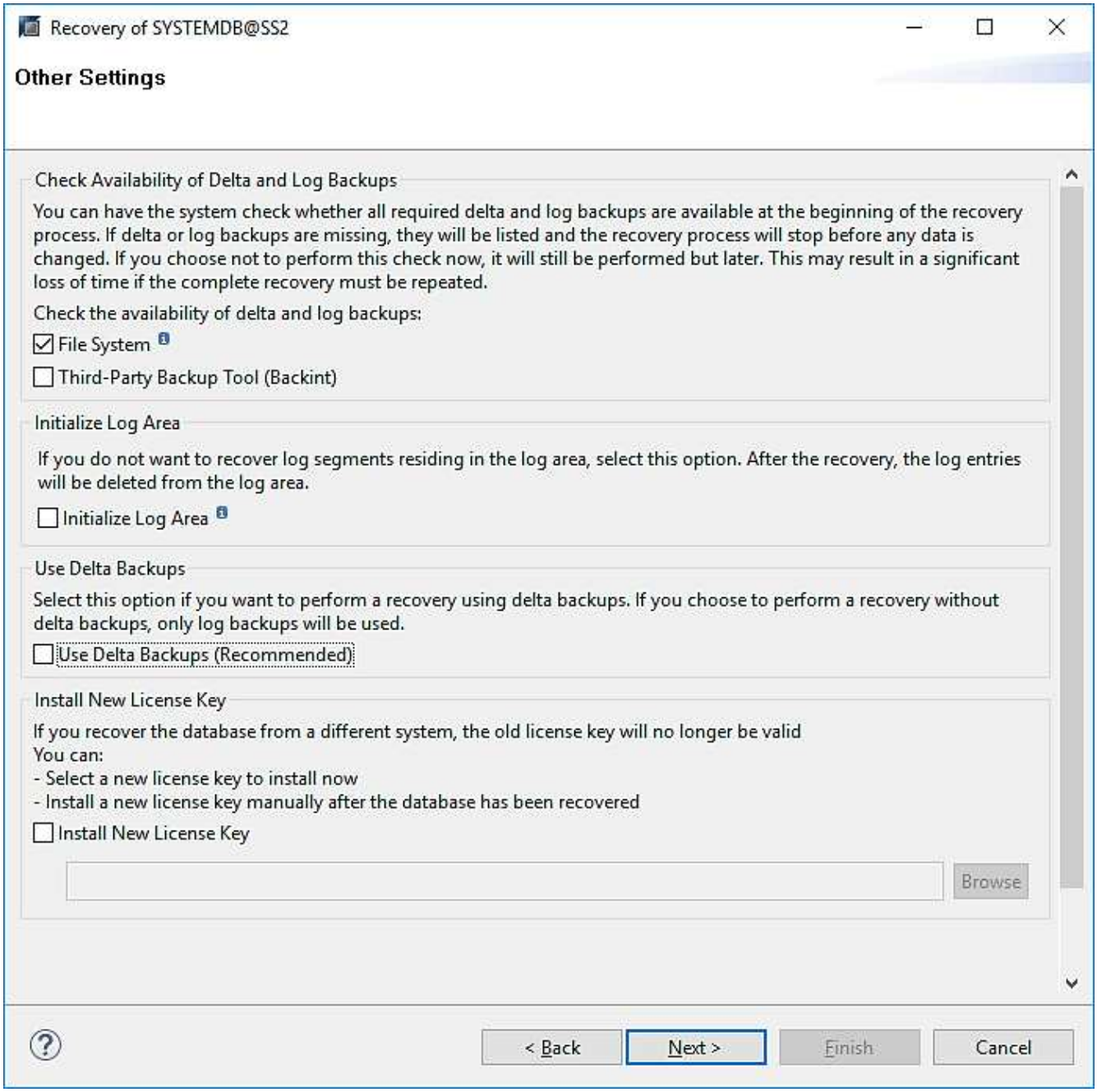
16. Go to SAP HANA Studio and click Refresh to update the list of available backups. The backup that was restored with SnapCenter is shown with a green icon in the list of backups. Select the backup and click Next.



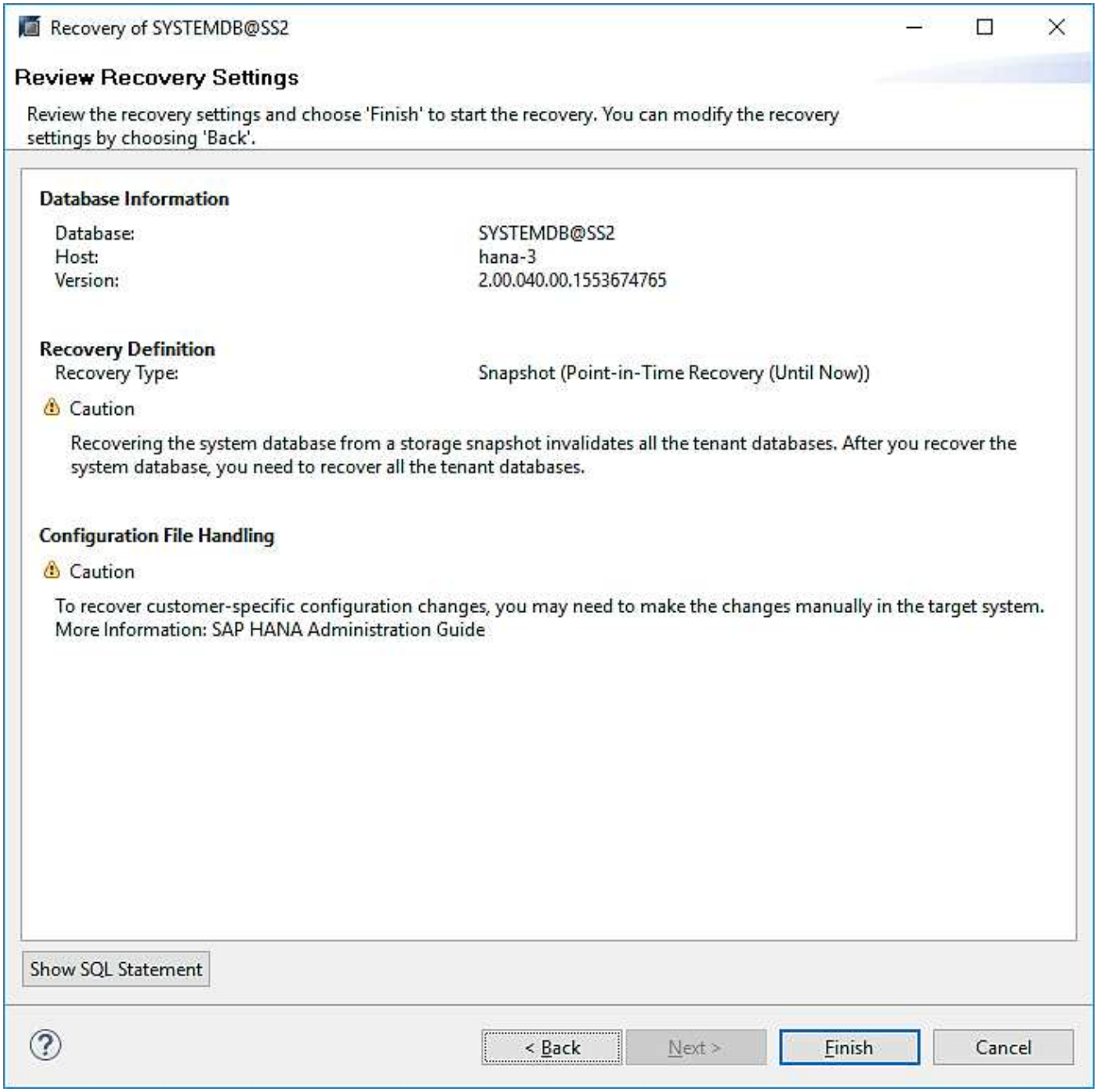
17. Provide the location of the log backups. Click Next.



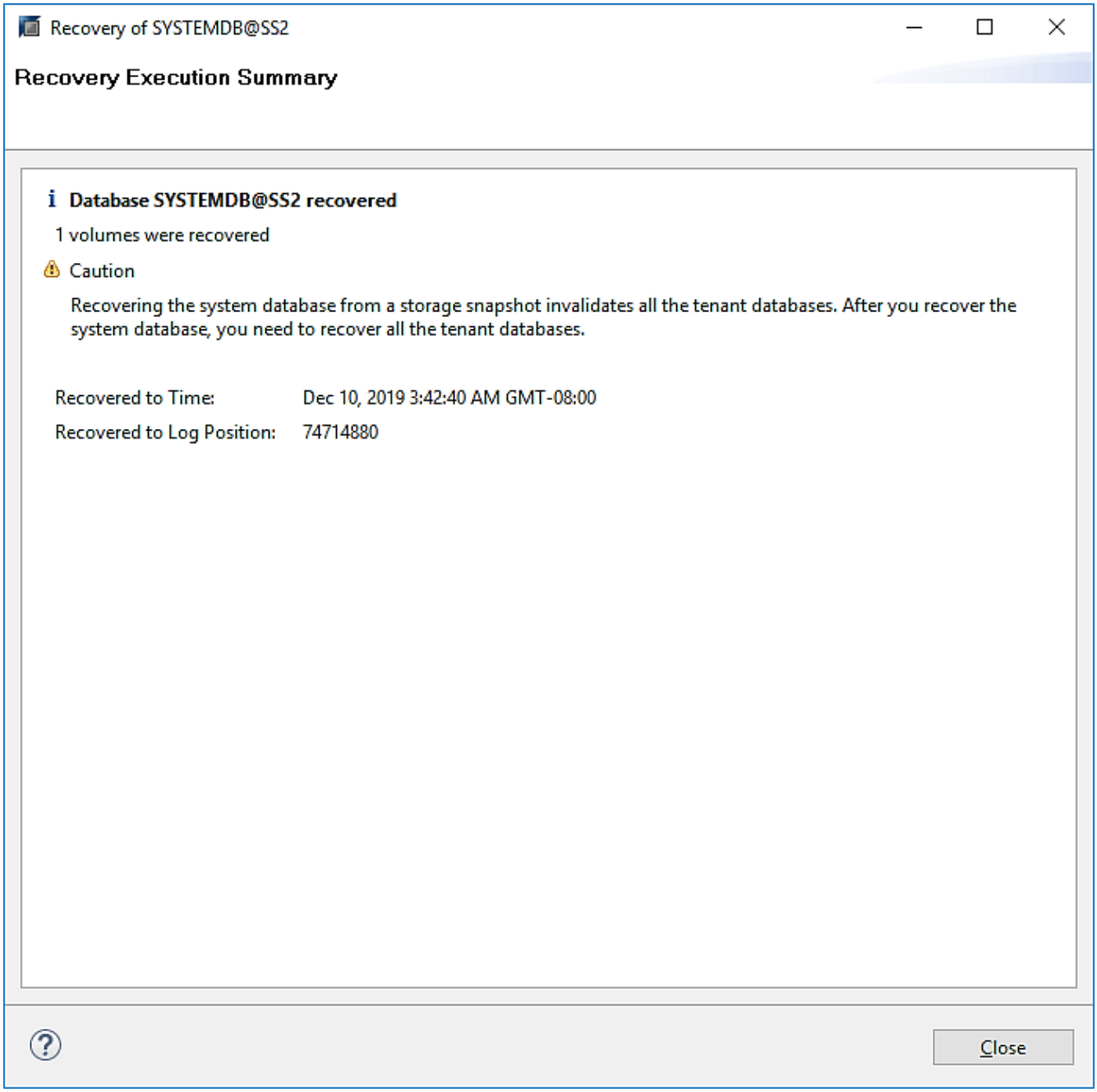
18. Select other settings as required. Make sure Use Delta Backups is not selected. Click Next.



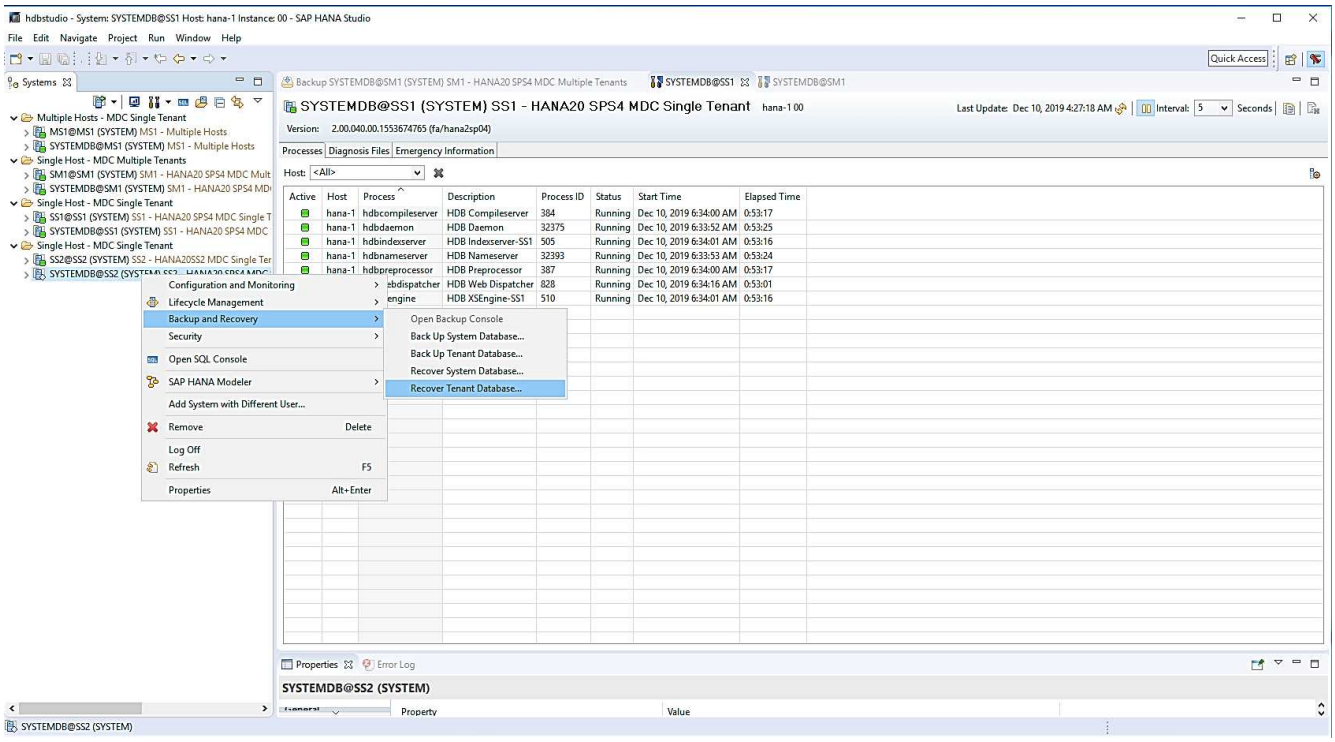
19. Review the recovery settings and click Finish.



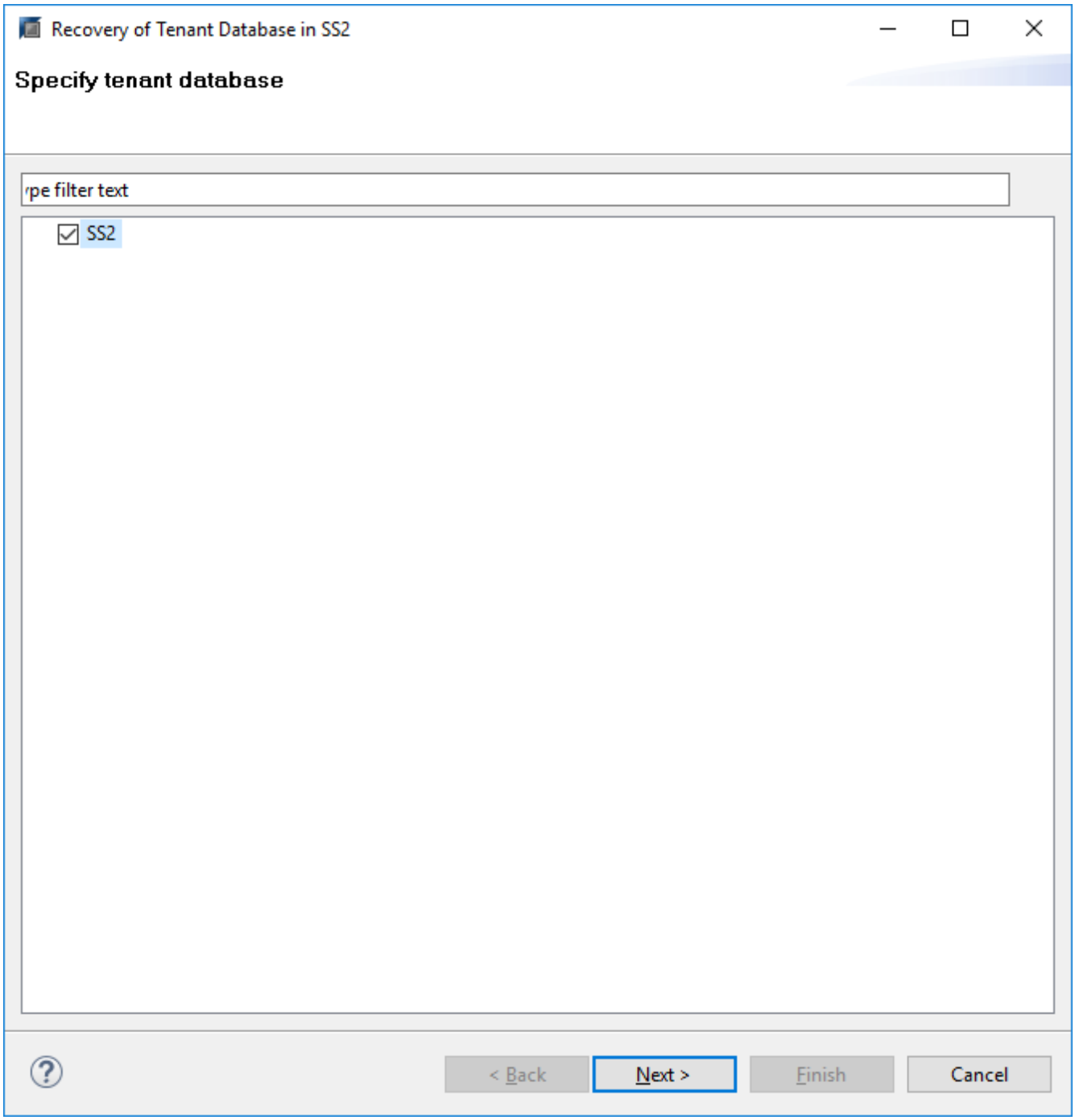
20. The recovery process starts. Wait until the recovery of the system database completes.



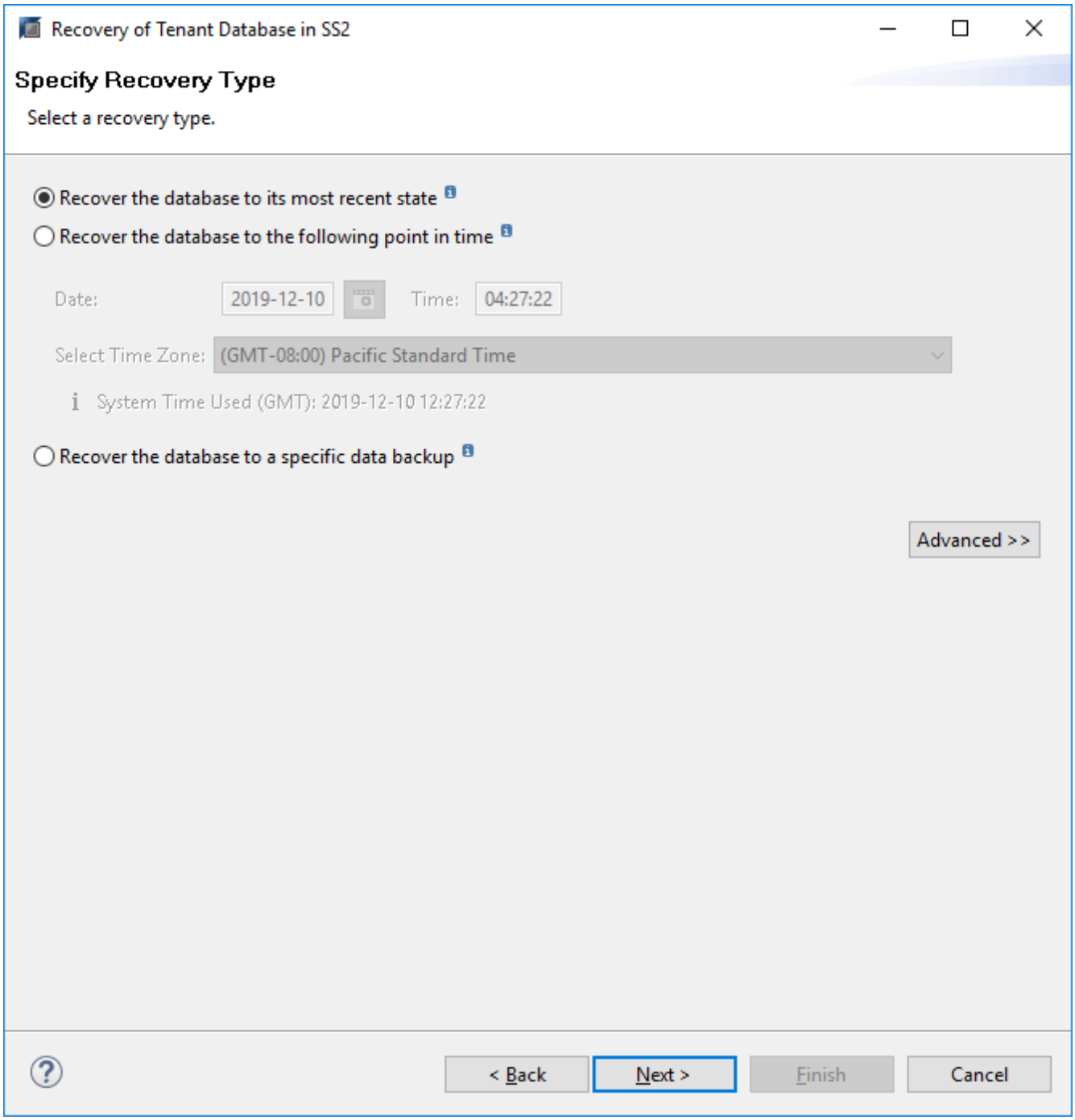
21. In SAP HANA Studio, select the entry for the system database and start Backup Recovery - Recover Tenant Database.



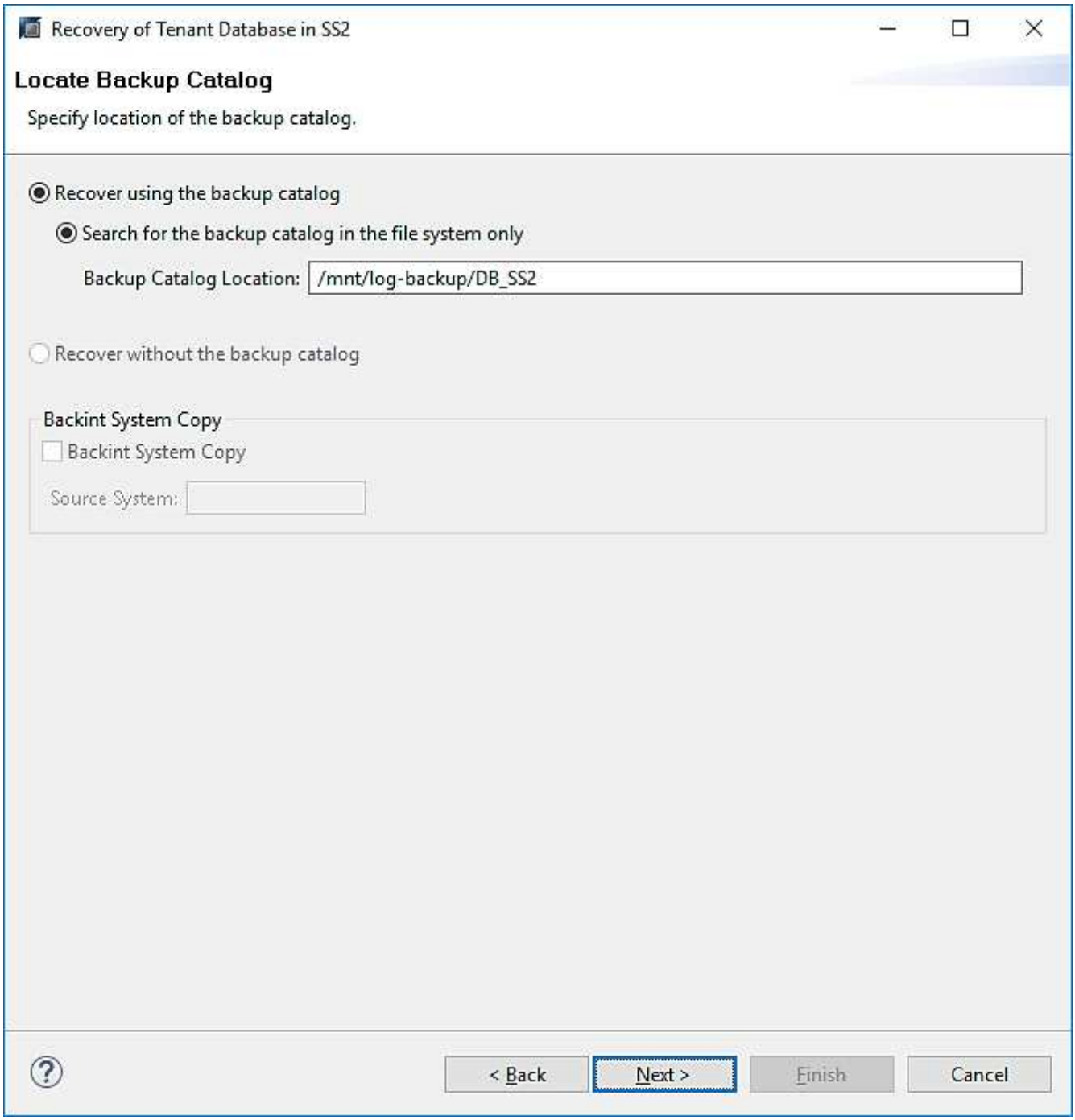
22. Select the tenant to recover and click Next.



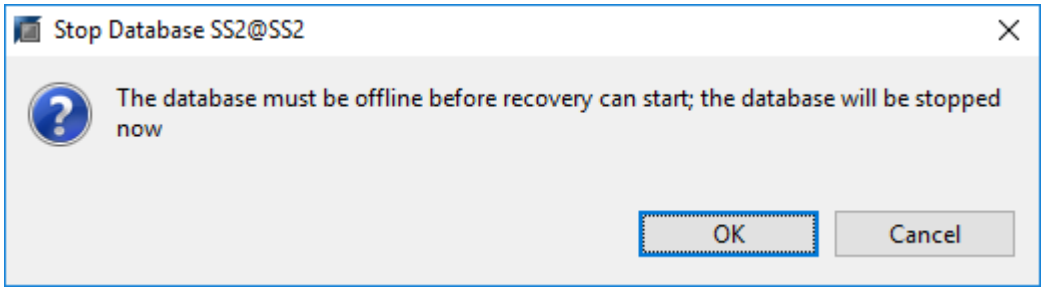
23. Specify the recovery type and click Next.



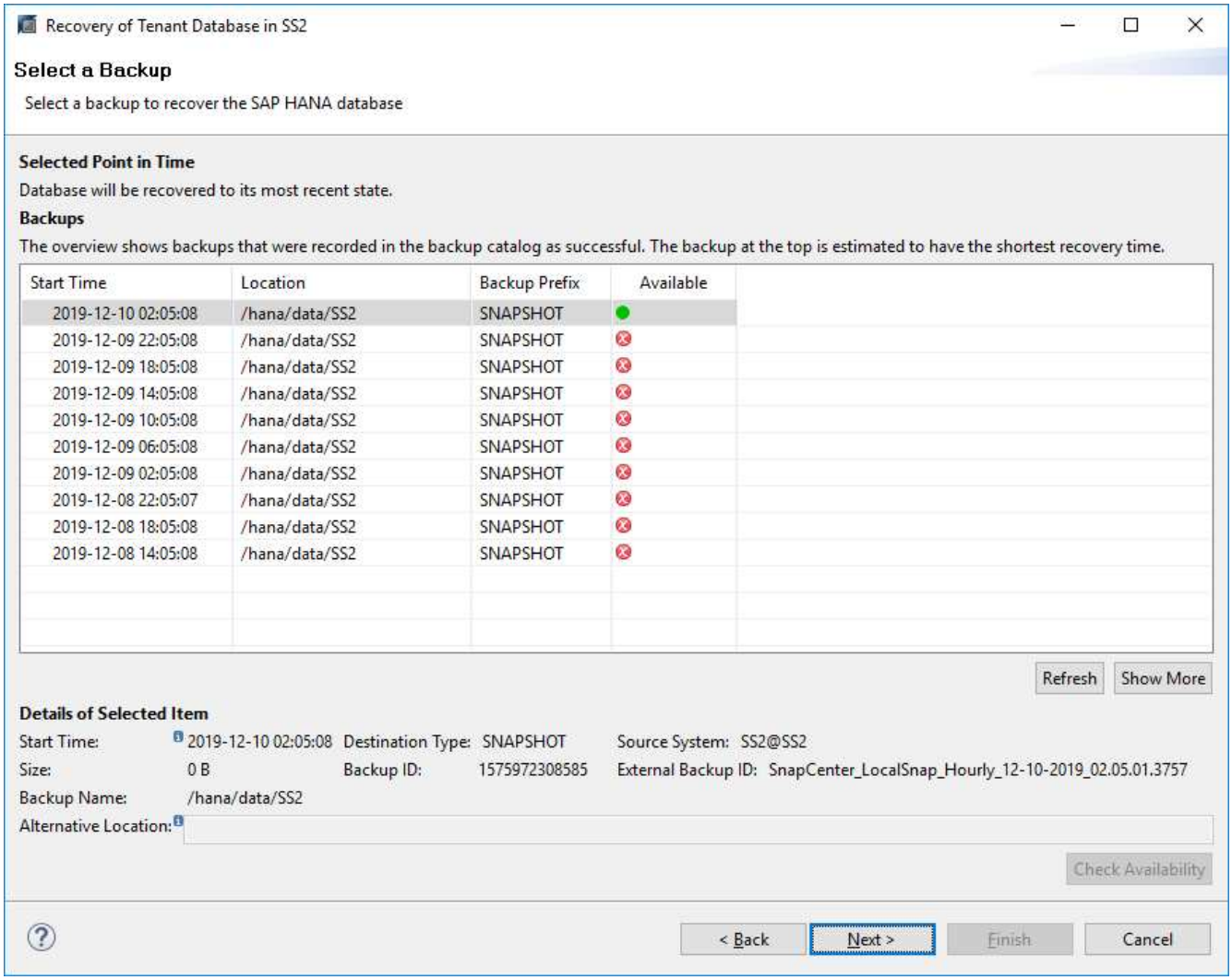
24. Confirm the backup catalog location and click Next.



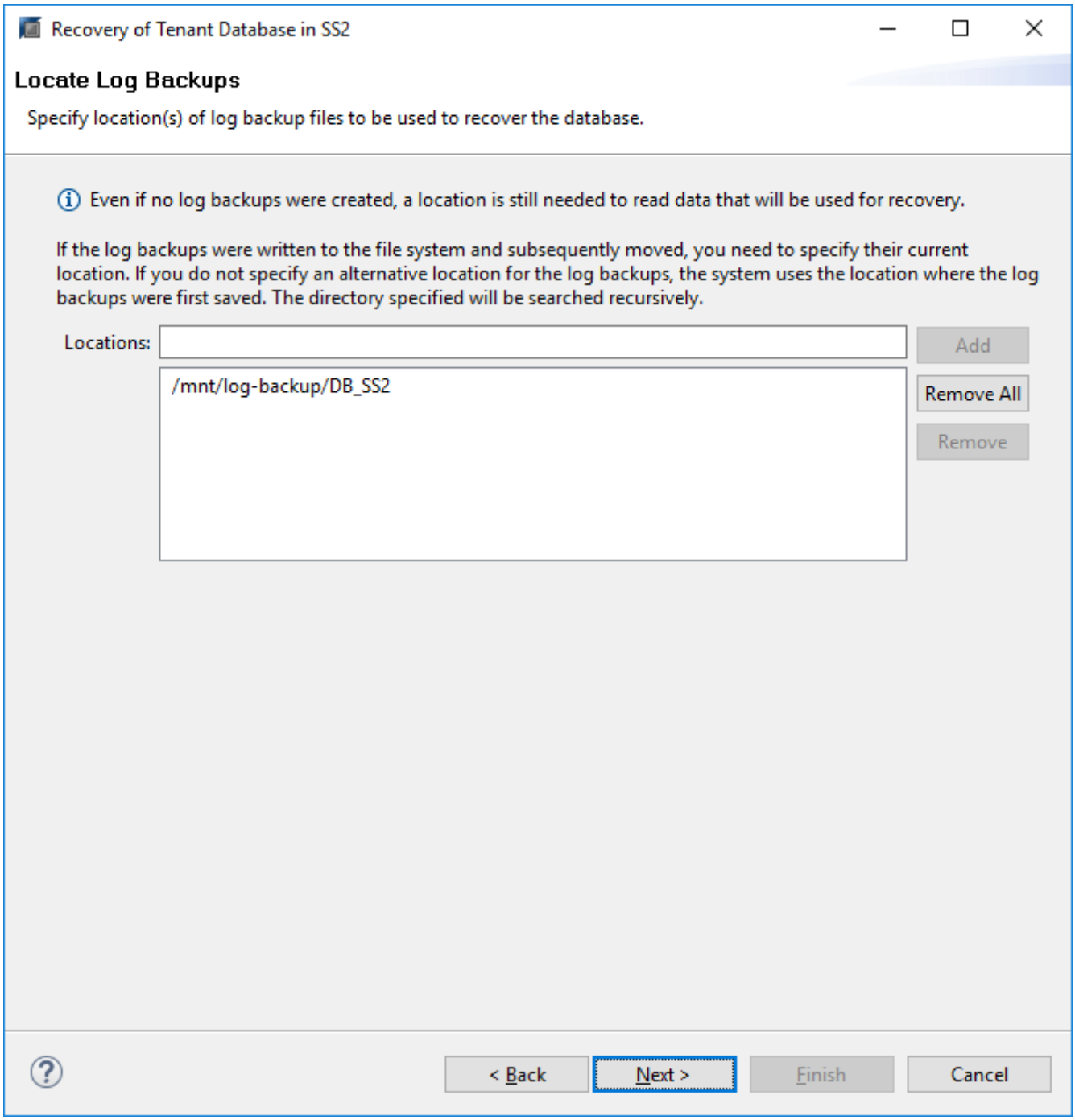
25. Confirm that the tenant database is offline. Click OK to continue.



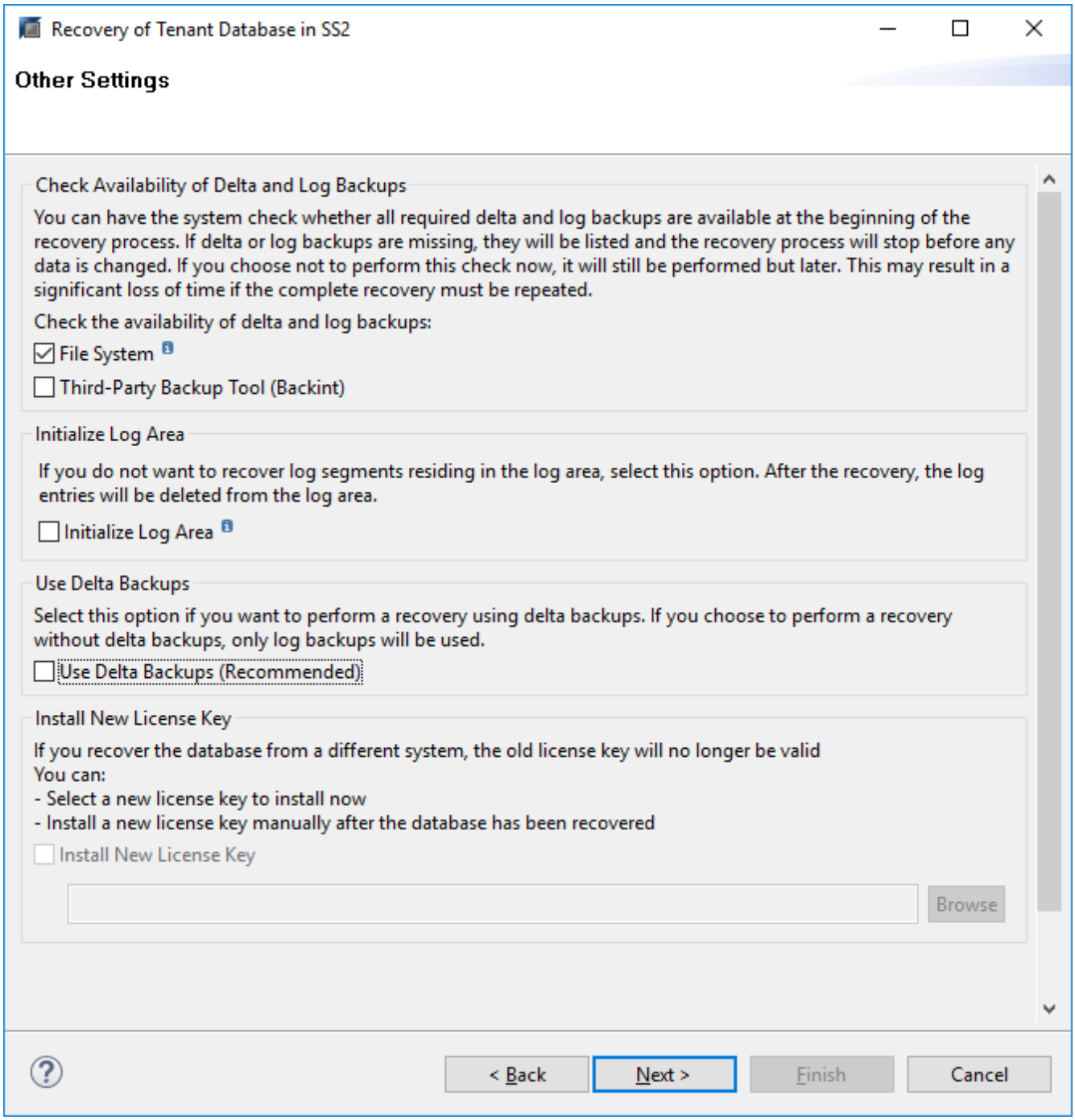
26. Because the restore of the data volume has occurred before the recovery of the system database, the tenant backup is immediately available. Select the backup highlighted in green and click Next.



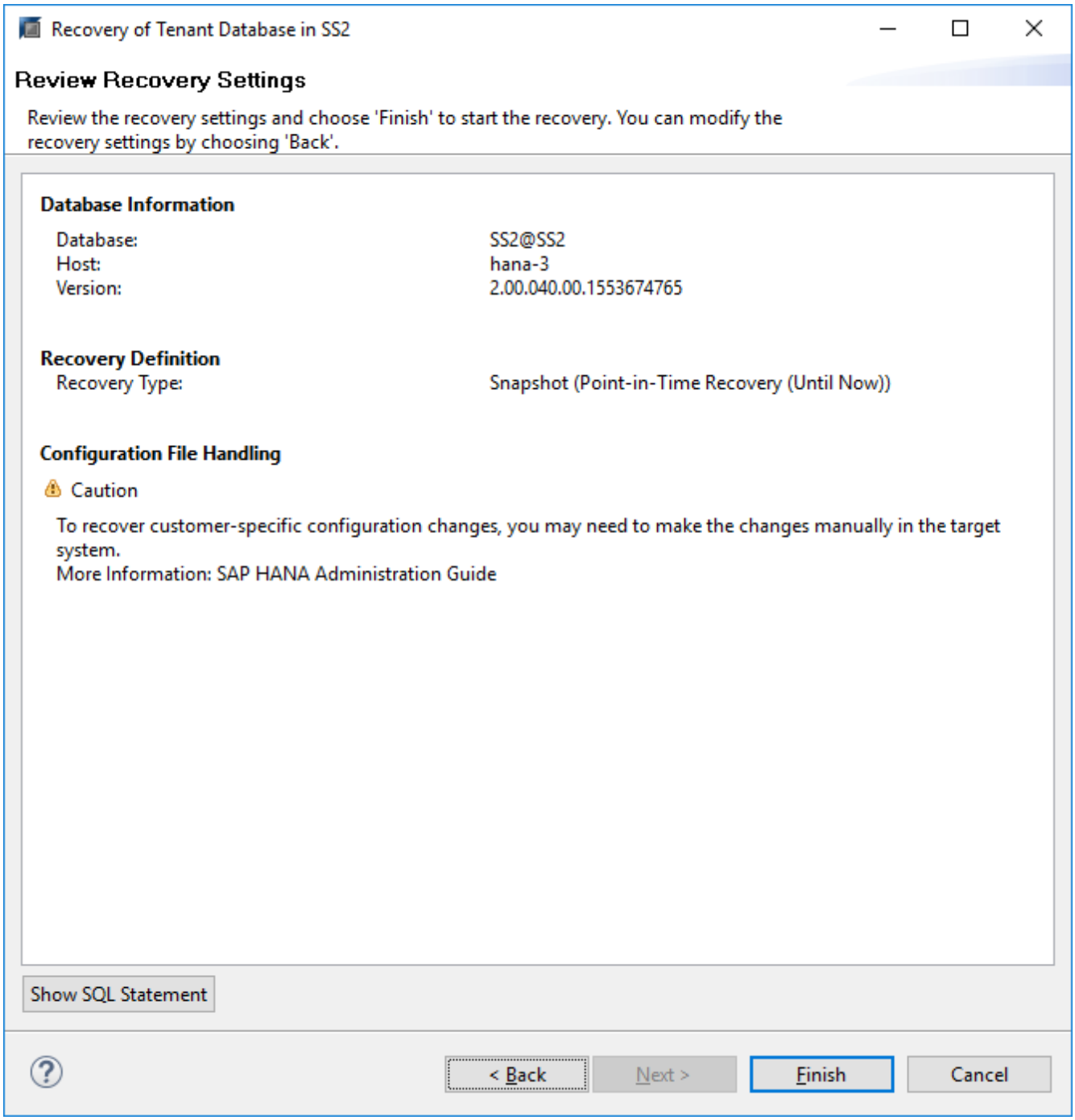
27. Confirm the log backup location and click Next.



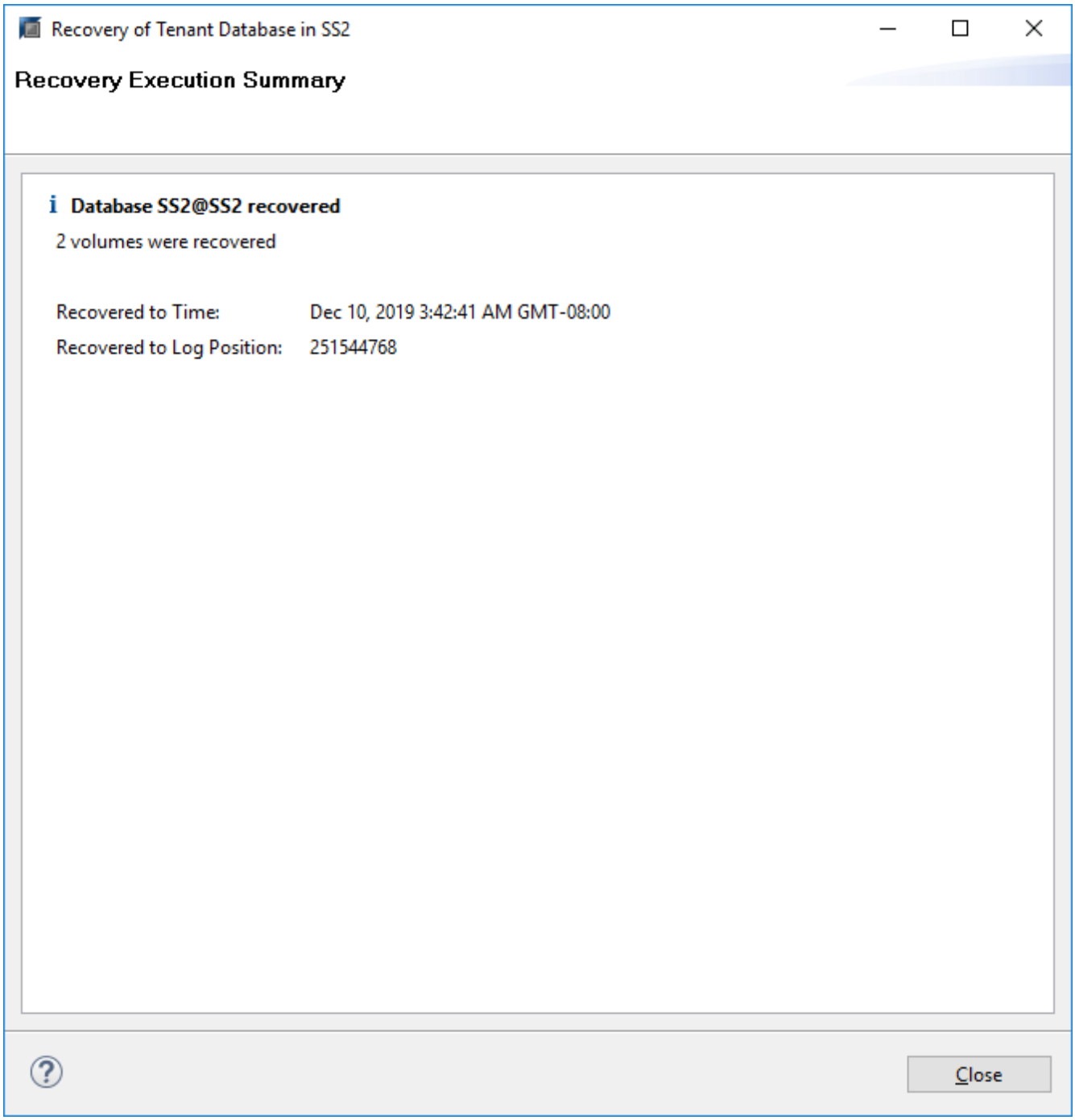
28. Select other settings as required. Make sure Use Delta Backups is not selected. Click Next.



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.

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.

> 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 %*
```

> 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.

```
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 username 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 is as follows:

```
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 is 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:

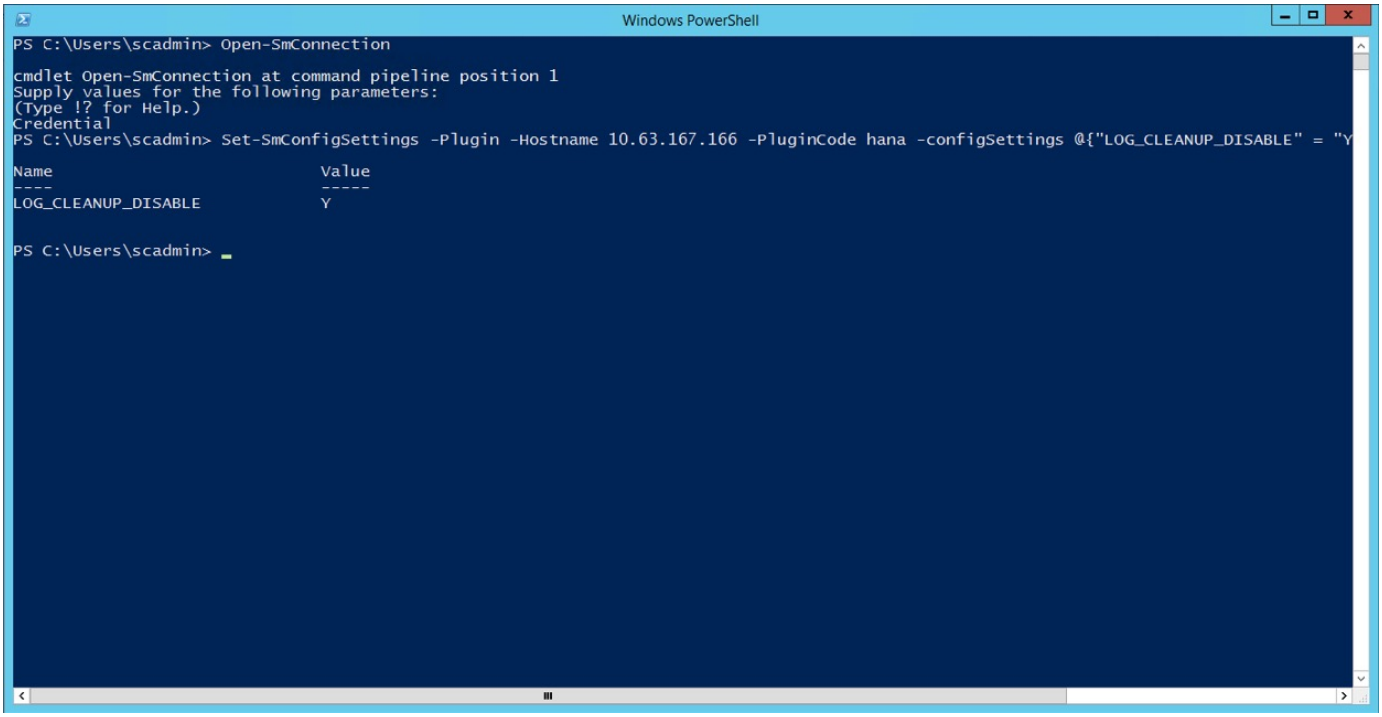
- For the Hdbsql communication host on Windows, the `hana.property` file is located at `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc`.

- For the Hdbsql communication host on Linux, the `hana.property` file is located at `/opt/NetApp/snapcenter/scc/etc`.

Use the PowerShell command

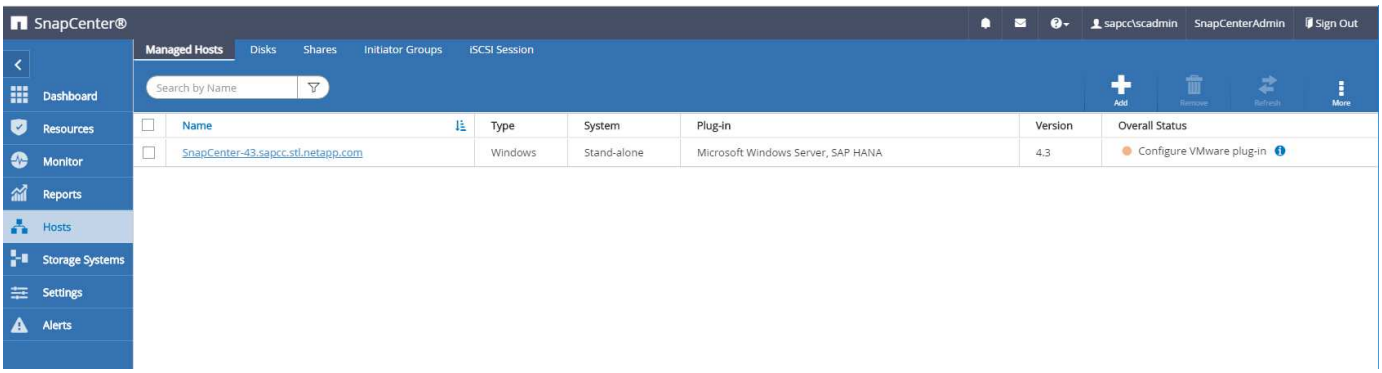
A second option to configure these settings is using a SnapCenter PowerShell command.

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 the following figure).



Disable warning when running SAP HANA plug-in on a virtual environment

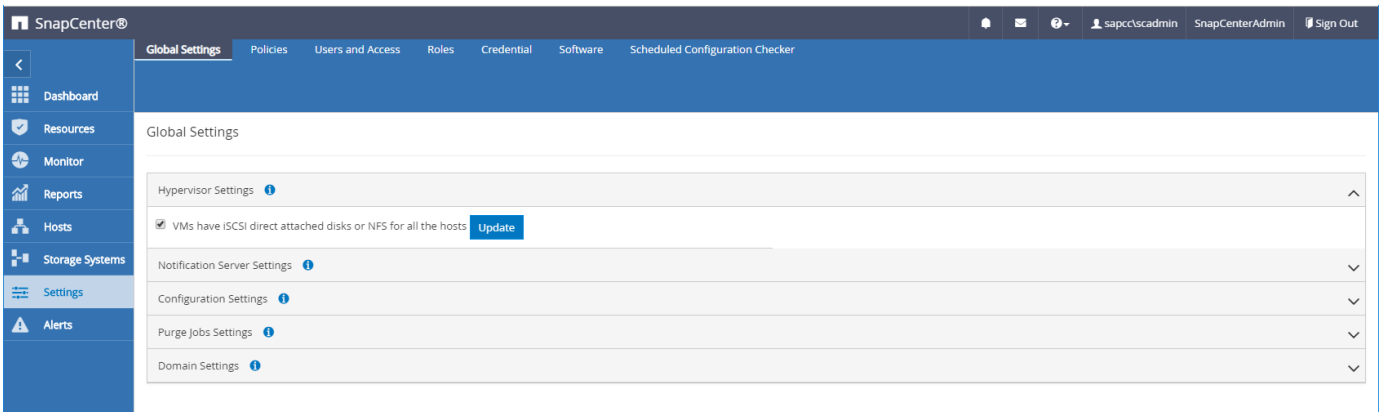
SnapCenter detects if the SAP HANA plug-in is installed on a virtualized environment. This could be a VMware environment or a SnapCenter installation at a public cloud provider. In this case, SnapCenter displays a warning to configure the hypervisor, as shown in the following figure.



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.



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

As described in the 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.

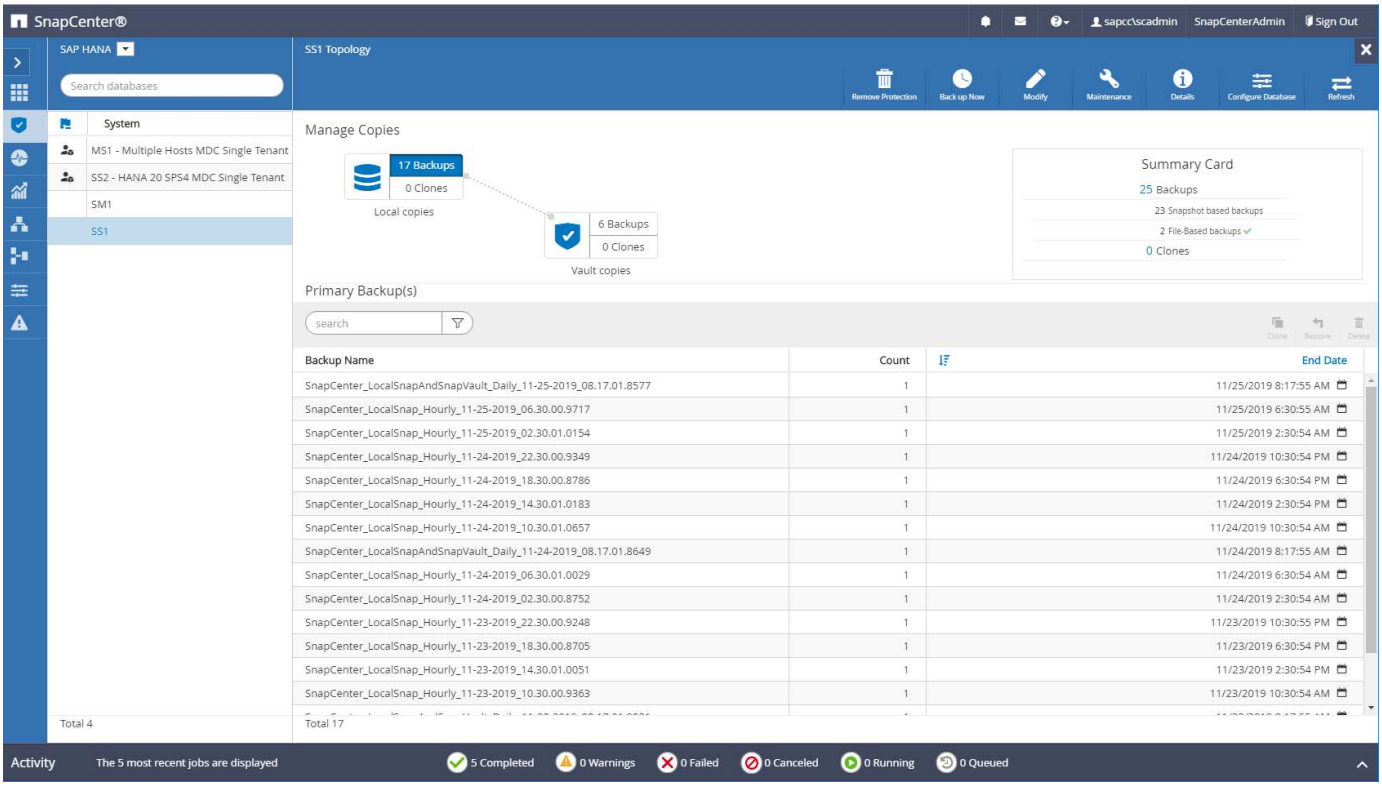
Until this scheduled cleanup has finished, SAP HANA and SnapCenter might still show backups that have already been deleted from the off-site backup storage.

> 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

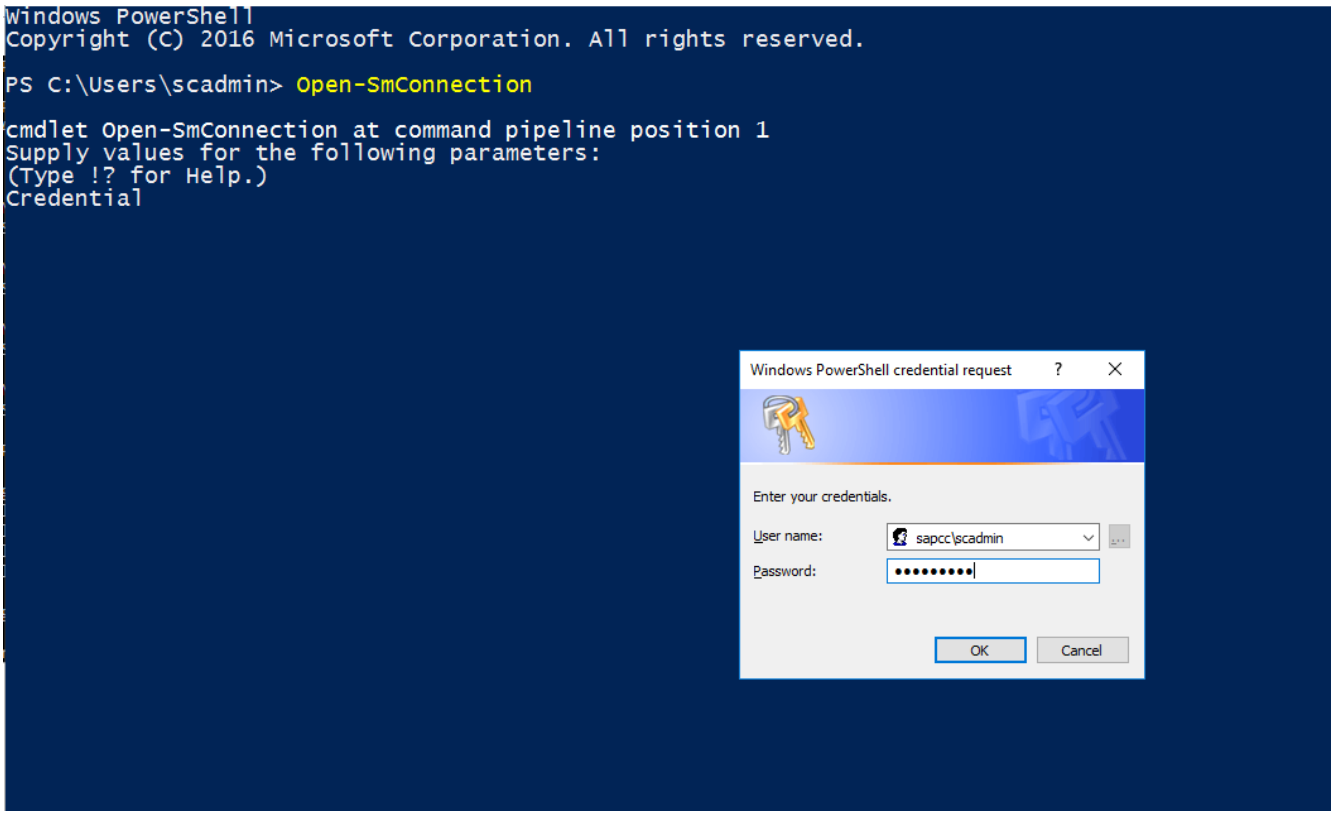
In the topology view of a resource, SnapCenter displays the backups on the off-site backup storage when selecting the secondary backups, as shown in the following screenshot. SnapCenter executes a cleanup operation with the Refresh icon to synchronize the backups for this resource.



Change the frequency of the SnapCenter cleanup job

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

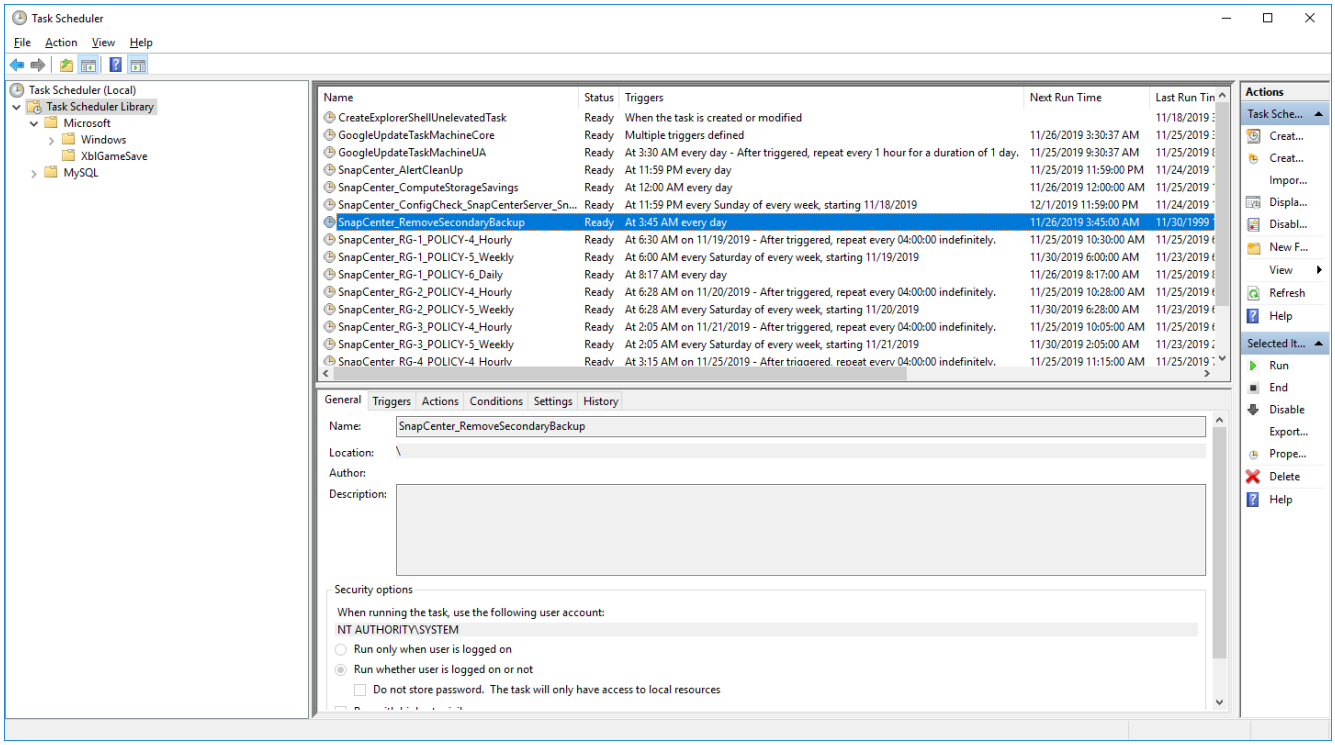
1. Start a PowerShell command window on the SnapCenter Server.
2. Open the connection to the SnapCenter Server and enter the SnapCenter administrator credentials in the login window.



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
DaysoftheMonth        :
MonthsofTheYear       :
DaysInterval          : 1
DaysOfTheWeek         :
AllowDefaults         : False
ReplaceJobIfExist     : False
UserName              :
Password              :
SchedulerType         : Daily
RepeatTask_Every_Hour :
IntervalDuration      :
EndTime               :
LocalScheduler        : False
AppType               : False
AuthMode              :
SchedulerSQLInstance  : 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/pdf.html?item=/media/17111-tr4667pdf.pdf

- TR-4719: SAP HANA System Replication, Backup and Recovery with SnapCenter

  https://www.netapp.com/pdf.html?item=/media/17030-tr4719pdf.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/pdf.html?item=/media/8584-tr4646pdf.pdf

SAP HANA System Replication Backup and Recovery with SnapCenter

TR-4719: SAP HANA System Replication - Backup and Recovery with SnapCenter

Nils Bauer, NetApp

SAP HANA System Replication is commonly used as a high-availability or disaster-recovery solution for SAP HANA databases. SAP HANA System Replication provides different operating modes that you can use depending on the use case or availability requirements.

There are two primary use cases that can be combined:

- High availability with a recovery point objective (RPO) of zero and a minimal recovery time objective (RTO) using a dedicated secondary SAP HANA host.
- Disaster recovery over a large distance. The secondary SAP HANA host can also be used for development or testing during normal operation.

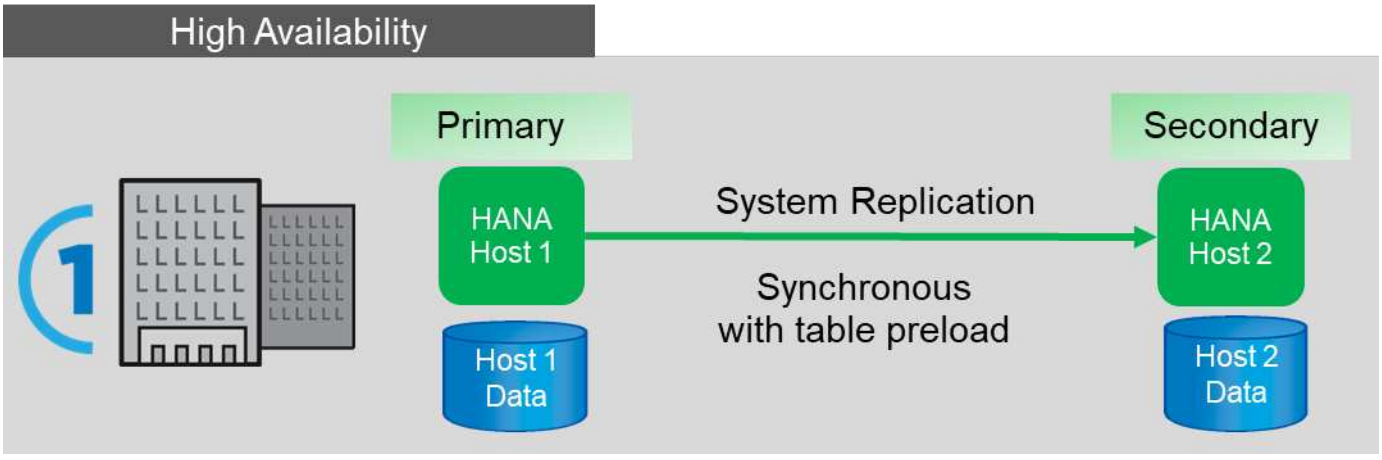
High availability with an RPO of zero and a minimal RTO

System Replication is configured with synchronous replication using tables preloaded into memory at the secondary SAP HANA host. This high-availability solution can be used to address hardware or software failures and also to reduce planned downtime during SAP HANA software upgrades (near- zero downtime operations).

Failover operations are often automated by using third-party cluster software or with a one-click workflow with SAP Landscape Management software.

From a backup requirement perspective, you must be able to create backups independent of which SAP HANA host is primary or secondary. A shared backup infrastructure is used to restore any backup, regardless of which host the backup has been created on.

The rest of this document focuses on backup operations with SAP System Replication configured as a high-availability solution.



Disaster recovery over a large distance

System replication can be configured with asynchronous replication with no table preloaded into memory at the secondary host. This solution is used to address data center failures, and failover operations are typically

performed manually.

Regarding backup requirements, you must be able to create backups during normal operation in data center 1 and during disaster recovery in data center 2. A separate backup infrastructure is available in data centers 1 and 2, and backup operations are activated as a part of disaster failover. The backup infrastructure is typically not shared, and a restore operation of a backup that was created at the other data center is not possible.

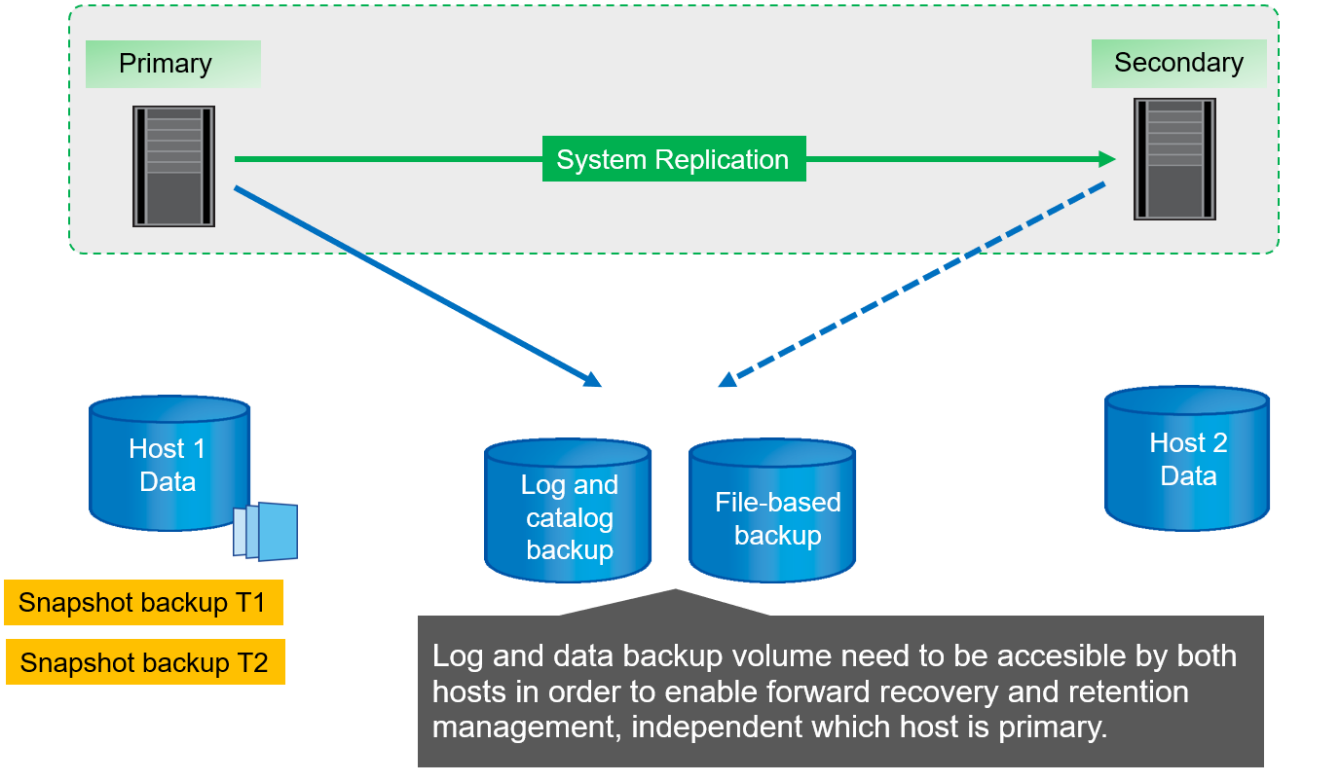
Storage Snapshot backups and SAP System Replication

Backup operations are always performed at the primary SAP HANA host. The required SQL commands for the backup operation cannot be performed at the secondary SAP HANA host.

For SAP HANA backup operations, the primary and secondary SAP HANA hosts are a single entity. They share the same SAP HANA backup catalog and they use backups for restore and recovery, regardless of whether the backup was created at the primary or secondary SAP HANA host.

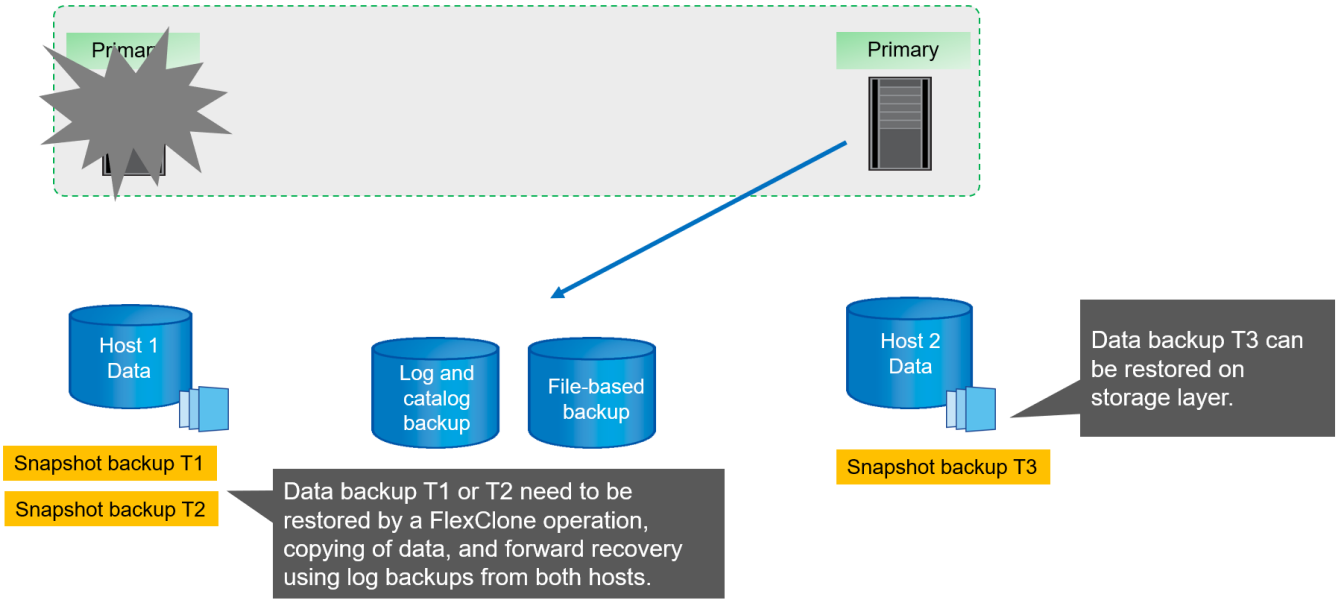
The ability to use any backup for restore and to do forward recovery using log backups from both hosts requires a shared log backup location that is accessible from both hosts. NetApp recommends that you use a shared storage volume. However, you should also separate the log backup destination into subdirectories within the shared volume.

Each SAP HANA host has its own storage volume. When you use a storage-based Snapshot to perform a backup, a database- consistent Snapshot is created on the primary SAP HANA host's storage volume.



When a failover to host 2 is performed, host 2 becomes the primary host, the backups are executed at host 2, and Snapshot backups are created at the storage volume of host 2.

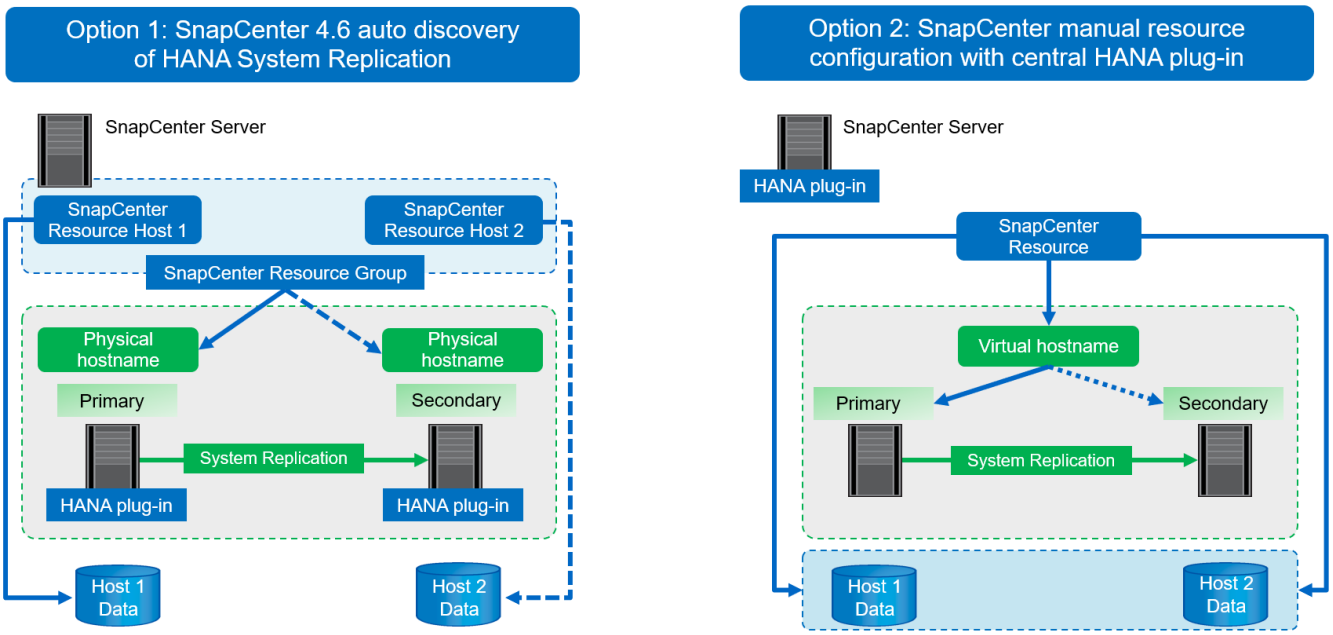
The backup created at host 2 can be restored directly at the storage layer. If you must use a backup created at host 1, then the backup must be copied from the host 1 storage volume to the host 2 storage volume. Forward recovery uses the log backups from both hosts.



SnapCenter configuration options for SAP System Replication

There are two options for configuring data protection with NetApp SnapCenter software in an SAP HANA System Replication environment:

- A SnapCenter resource group including both SAP HANA hosts and auto discovery with SnapCenter version 4.6 or higher.
- A single SnapCenter resource for both SAP HANA hosts using a virtual IP address.



Starting with SnapCenter 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 by SnapCenter is performed across both hosts to ensure that old backups also get deleted at the current secondary host.

With a single-resource configuration for both SAP HANA hosts, the single SnapCenter resource is configured using the virtual IP address of the SAP HANA System Replication hosts. Both data volumes of the SAP HANA hosts are included in the SnapCenter resource. Because it is a single SnapCenter resource, retention management for Snapshot and file-based backups created by SnapCenter works independent of which host is currently primary or secondary. This options is possible with all SnapCenter releases.

The following table summarizes the key differences of the two configuration options.

	Resource group with SnapCenter 4.6	**Single SnapCenter resource and virtual IP address**
Backup operation (Snapshot and file-based)	Automatic identification of primary host in resource group	Automatically use virtual IP address
Retention management (Snapshot and file-based)	Automatically executed across both hosts	Automatically use single resource
Backup capacity requirements	Backups are only created at primary host volume	Backups are always created at both hosts volumes. The backup of the second host is only crash consistent and cannot be used to do a roll forward.

	Resource group with SnapCenter 4.6	Single SnapCenter resource and virtual IP address
Restore operation	Backups from current active host are available for restore operation	Pre-backup script required to identify which backups are valid and can be used for restore
Recovery operation	All recovery options available, same as for any auto-discovered resource	Manual recovery required

In general, NetApp recommends using the resource group configuration option with SnapCenter 4.6 to protect HANA systems with enabled HANA System Replication. Using a single SnapCenter resource configuration is only required if the SnapCenter operation approach is based on a central plug-in host and the HANA plug-in is not deployed on the HANA database hosts.

The two options are discussed in detail in the following sections.

SnapCenter 4.6 configuration using a resource group

SnapCenter 4.6 supports auto discovery for HANA systems configured with HANA System Replication. SnapCenter 4.6 includes the logic to identify primary and secondary HANA hosts during backup operations and also handles retention management across both HANA hosts. In addition, automated restore and recovery is now also available for HANA System Replication environments.

SnapCenter 4.6 configuration of HANA System Replication environments

The following figure shows the lab setup used for this chapter. Two HANA hosts, hana-3 and hana-4, were configured with HANA System Replication.

A database user “SnapCenter” was created for the HANA system database with the required privileges to execute backup and recovery operations (see SAP HANA Backup and Recovery with SnapCenter). A HANA user store key must be configured at both hosts using the above database user.

```
ss2adm@hana- 3: / > hdbuserstore set SS2KEY hana- 3:33313 SNAPCENTER
<password>
```

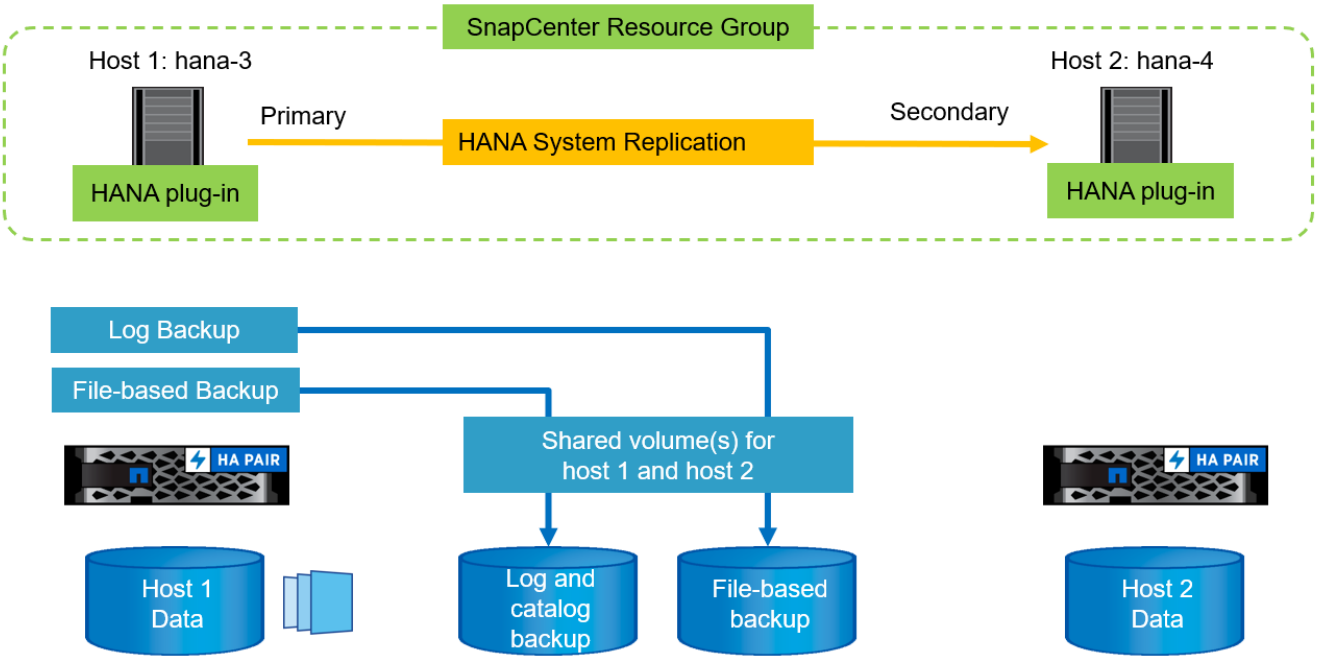
```
ss2adm@hana- 4:/ > hdbuserstore set SS2KEY hana-4:33313 SNAPCENTER
<password>
```

From a high-level perspective, you must perform the following steps to set up HANA System Replication within SnapCenter.

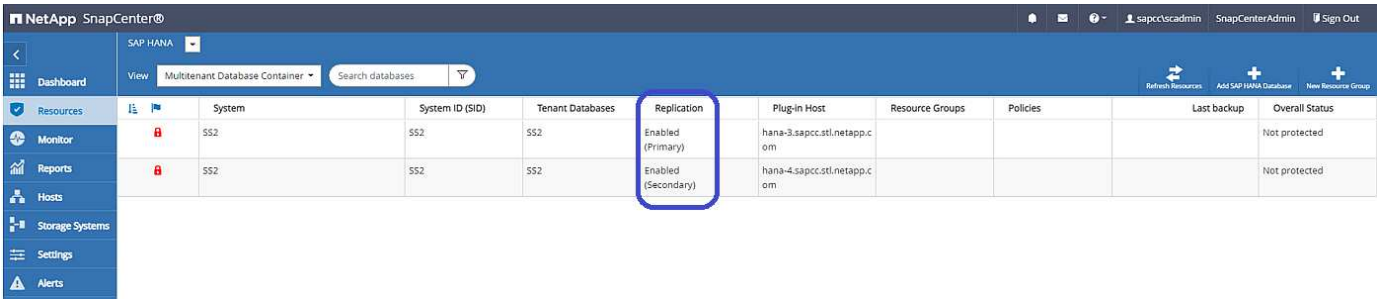
1. Install the HANA plugin on the primary and secondary host. Autodiscovery is executed and the HANA System Replication status is detected for each primary or secondary host.
2. Execute SnapCenter `configure database` and provide the `hdbuserstore` key. Further autodiscovery

operations are executed.

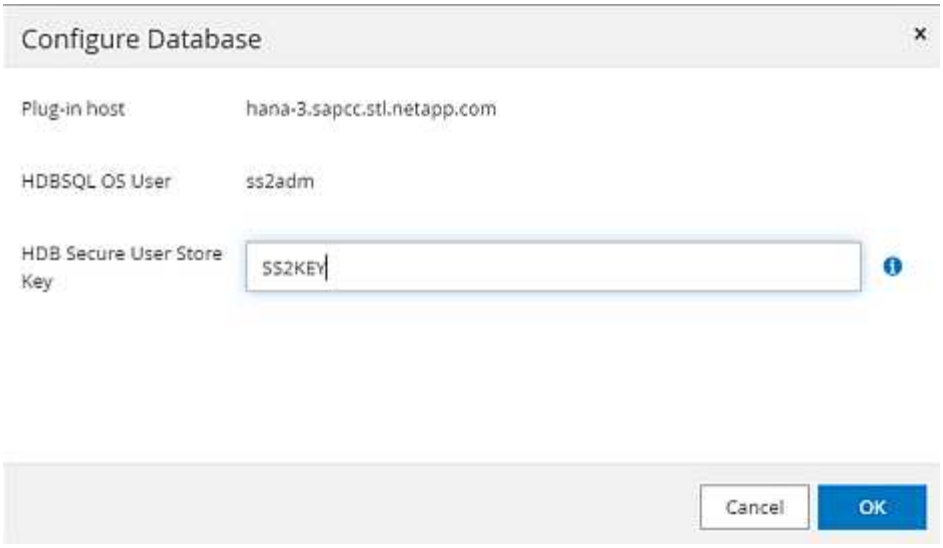
3. Create a resource group, including both hosts and configure protection.



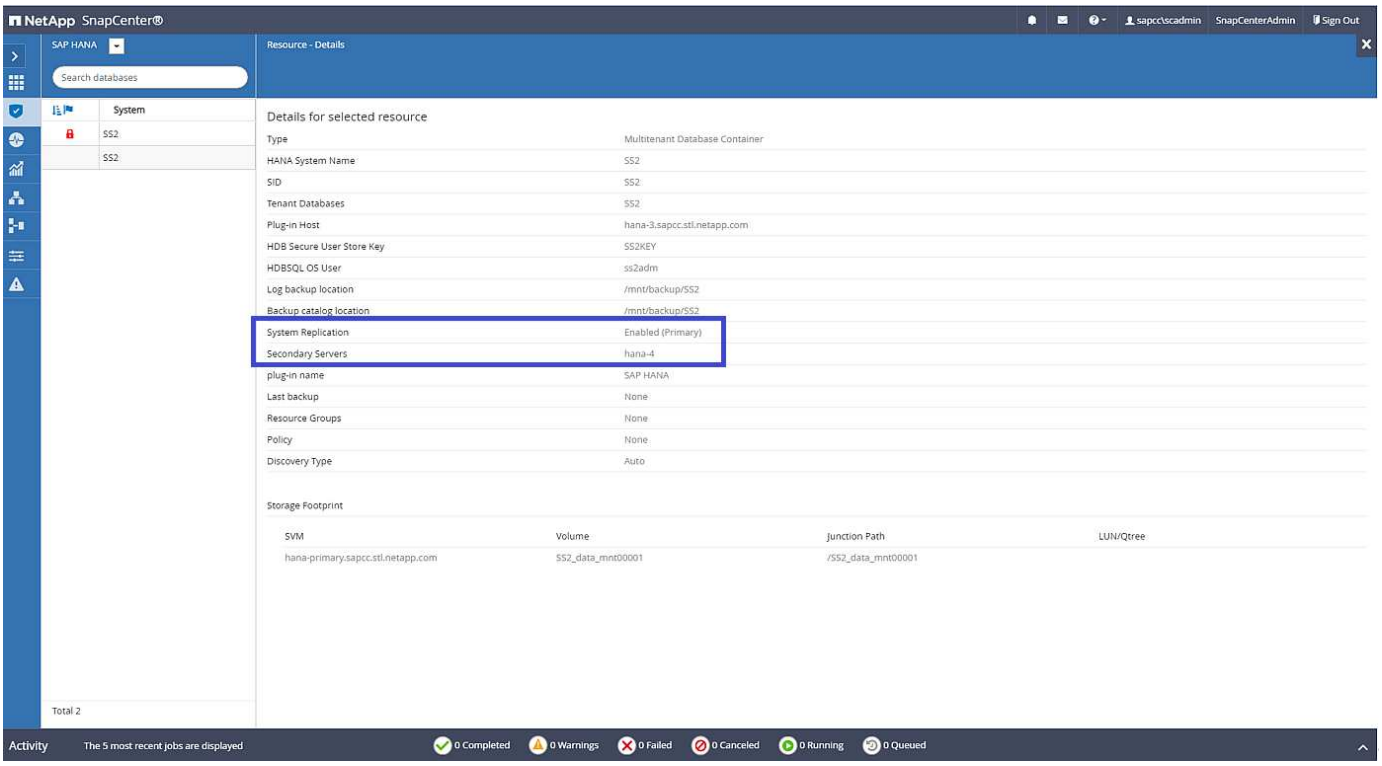
After you have installed the SnapCenter HANA plug-in on both HANA hosts, the HANA systems are shown in the SnapCenter resource view in the same way as other autodiscovered resources. Starting with SnapCenter 4.6, an additional column is displayed that shows the status of HANA system replication (enabled/disabled, primary/secondary).



By clicking the resource, SnapCenter requests the HANA user store key for the HANA system.

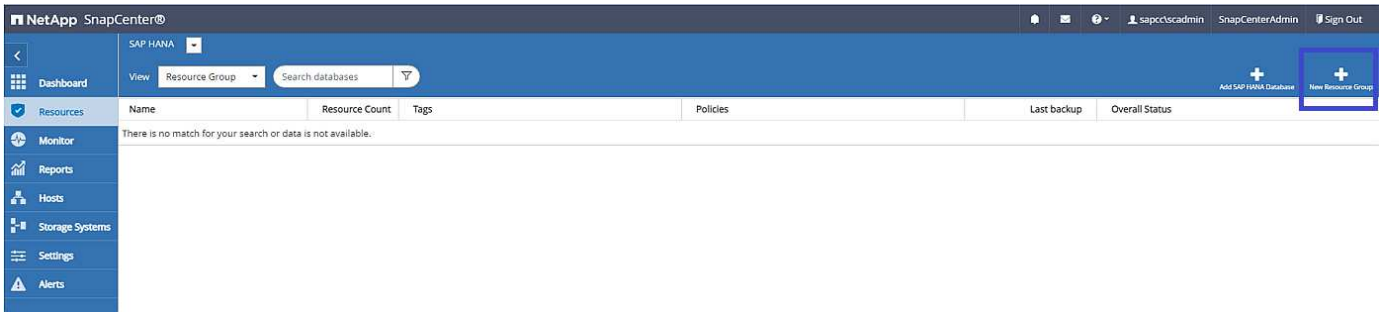


Additional autodiscovery steps are executed, and SnapCenter show the resource details. With SnapCenter 4.6, the system replication status and the secondary server are listed in this view.

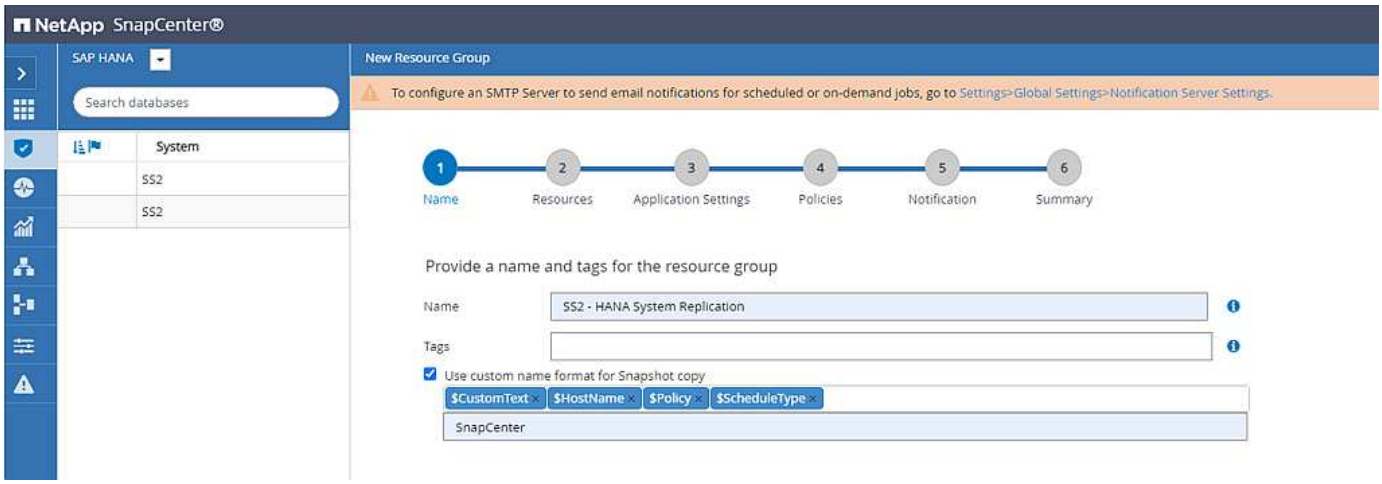


After performing the same steps for the second HANA resource, the autodiscovery process is complete and both HANA resources are configured in SnapCenter.

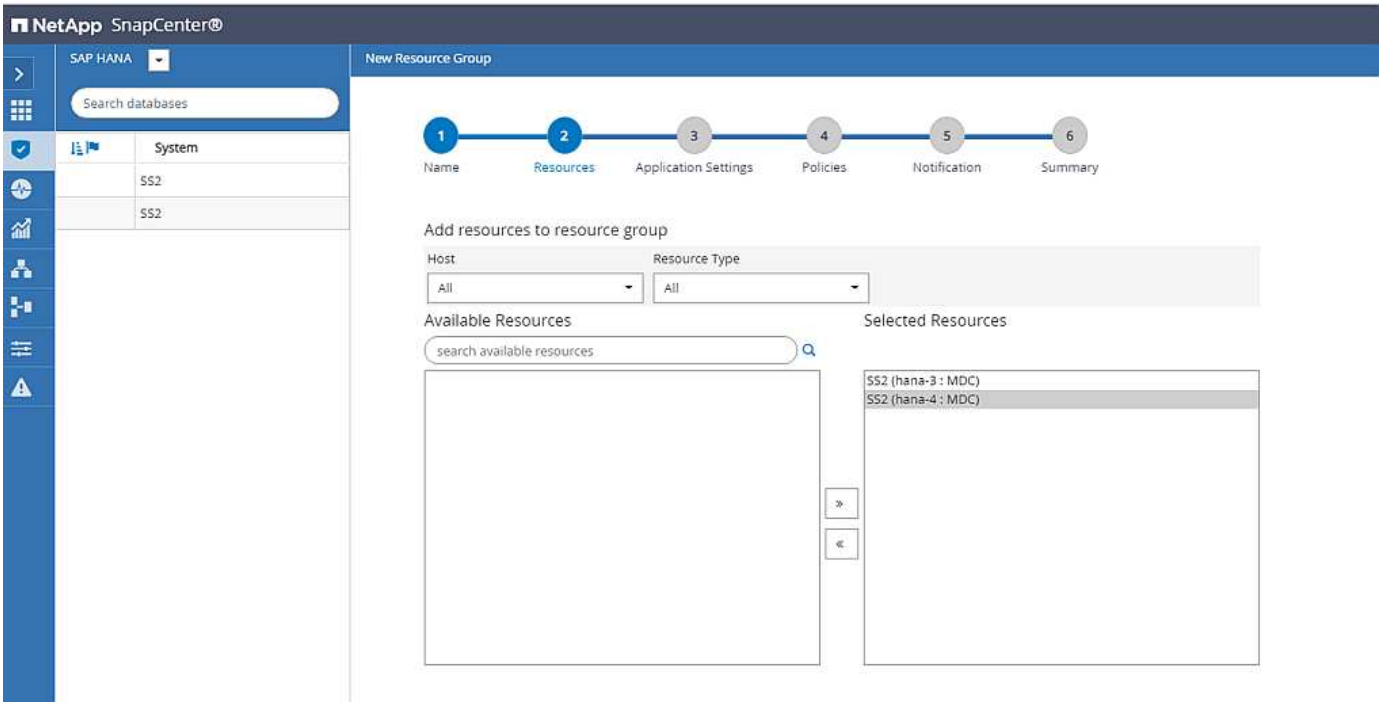
For HANA System Replication- enabled systems, you must configure a SnapCenter resource group, including both HANA resources.



NetApp recommends using a custom name format for the Snapshot name, which should include the hostname, the policy, and the schedule.

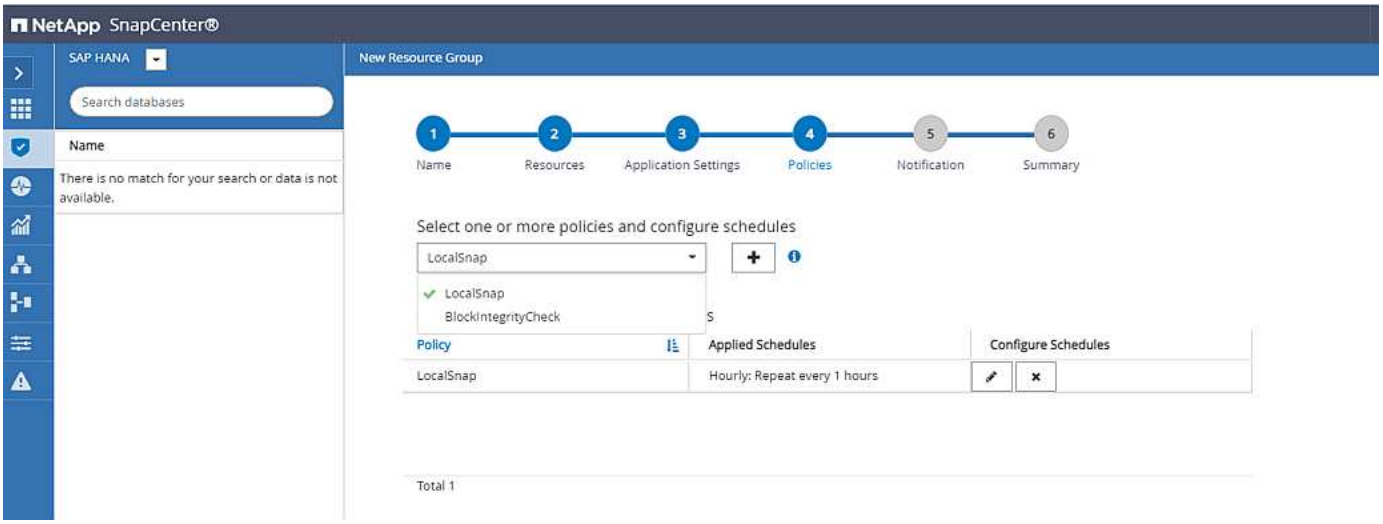


You must add both HANA hosts to the resource group.

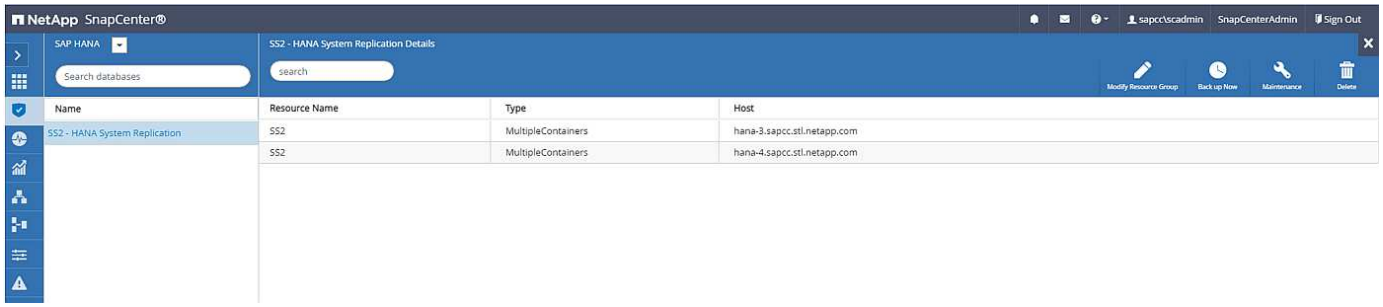


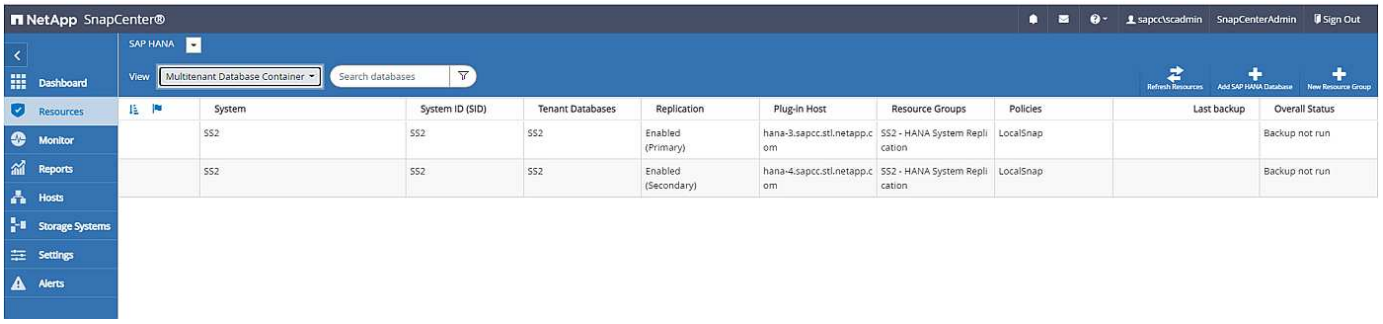
Policies and schedules are configured for the resource group.

> The retention defined in the policy is used across both HANA hosts. If, for example, a retention of 10 is defined in the policy, the sum of backups of both hosts is used as a criteria for backup deletion. SnapCenter deletes the oldest backup independently if it has been created at the current primary or secondary host.



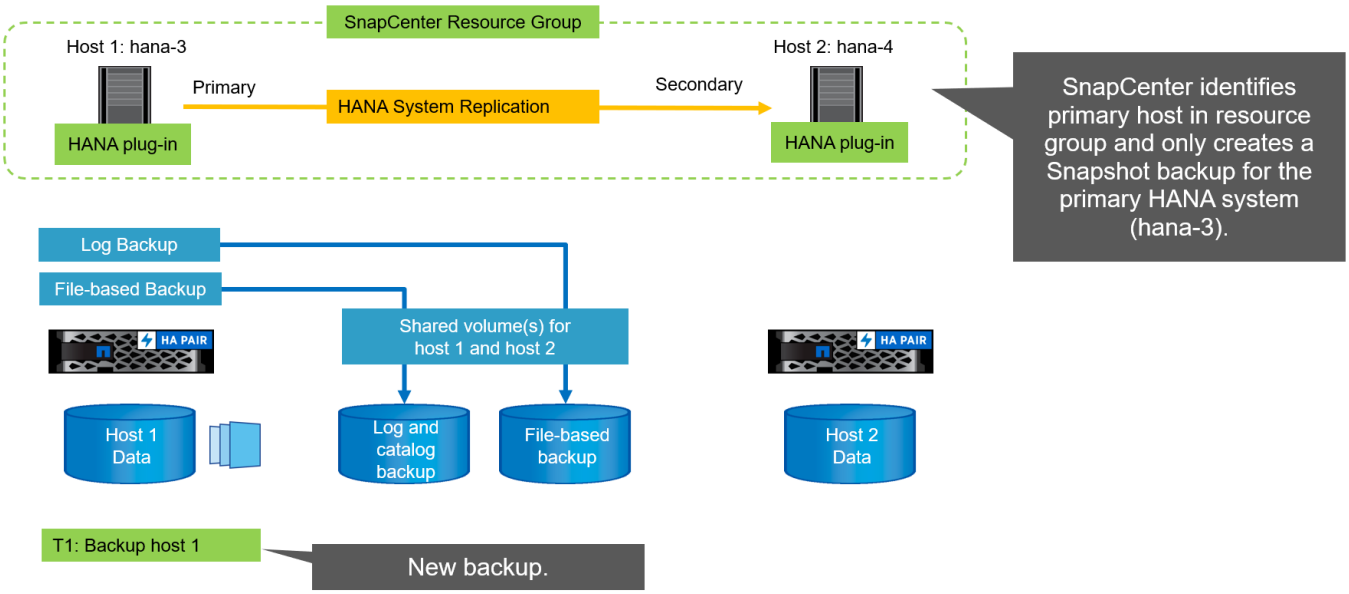
The resource group configuration is now finished and backups can be executed.



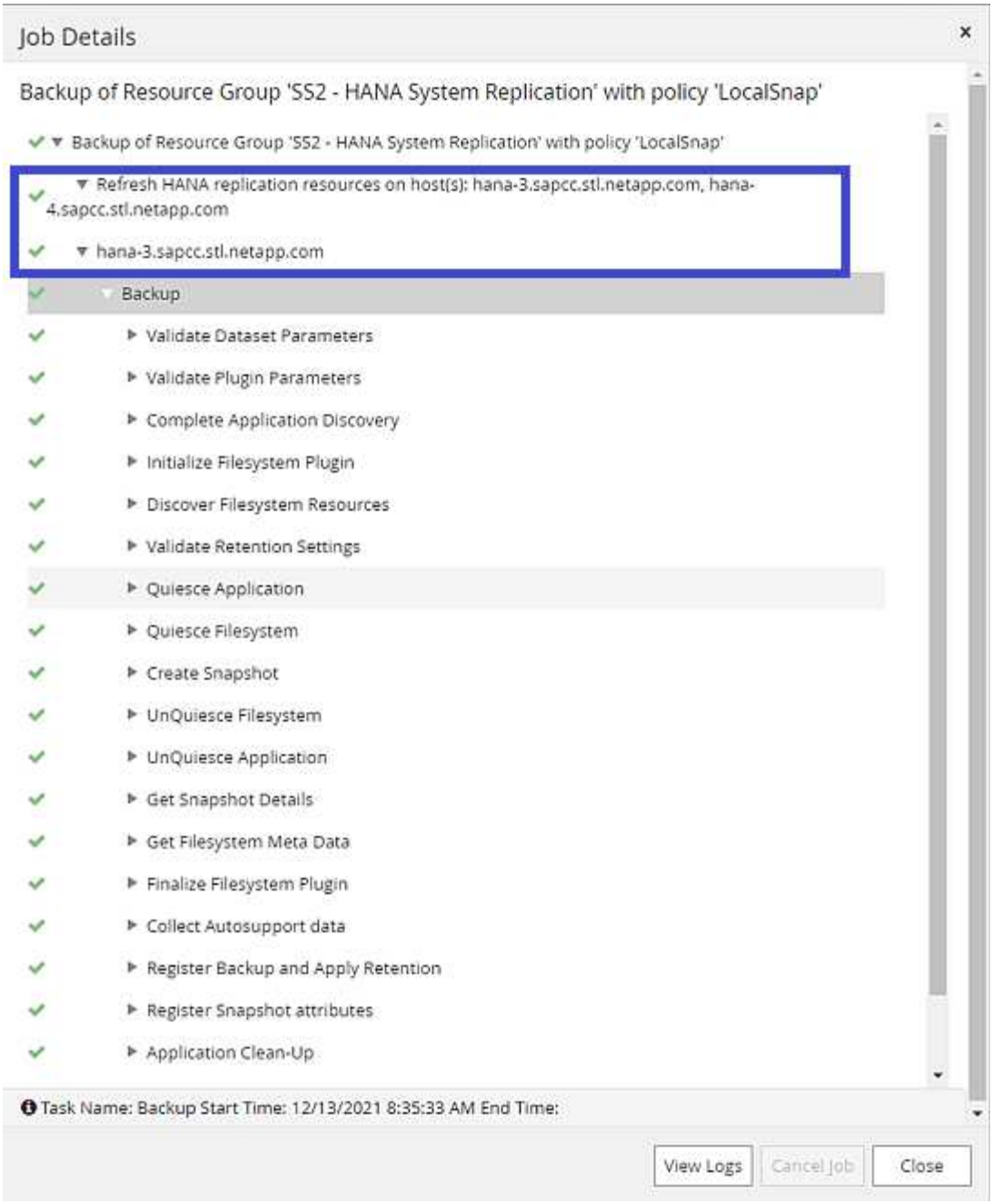


Snapshot backup operations

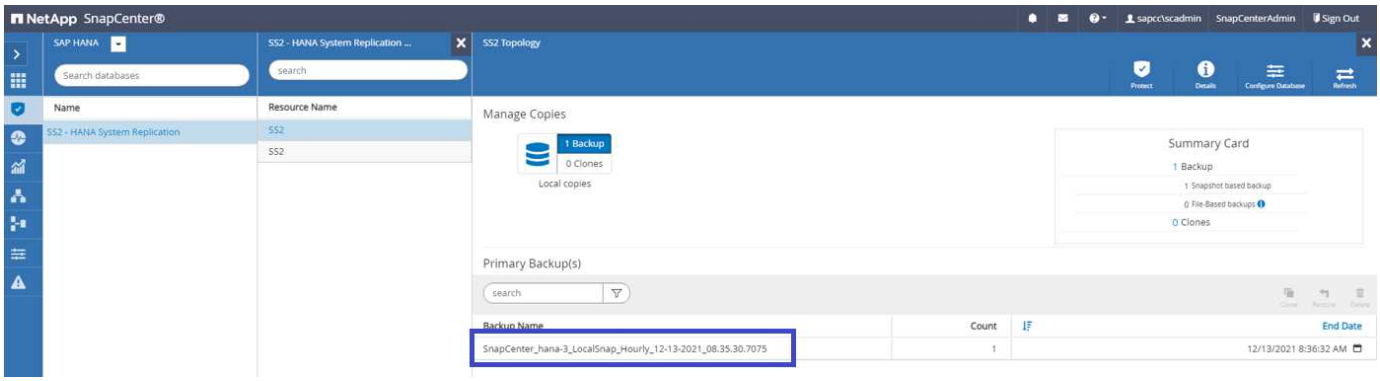
When a backup operation of the resource group is executed, SnapCenter identifies which host is primary and only triggers a backup at the primary host. This means, only the data volume of the primary host will be snapshotted. In our example, hana-3 is the current primary host and a backup is executed at this host.



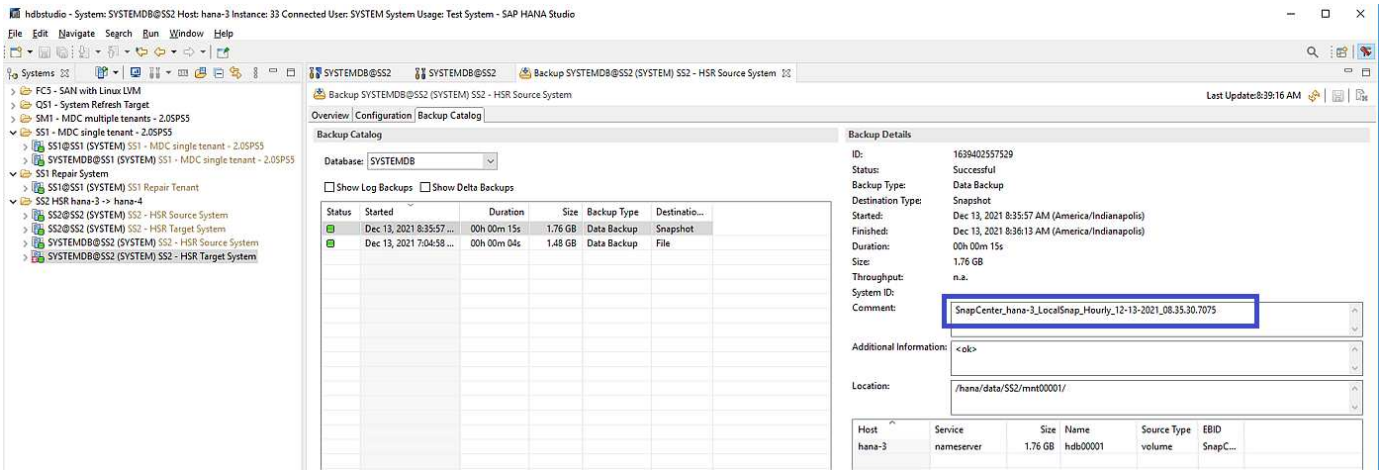
The SnapCenter job log shows the identification operation and the execution of the backup at the current primary host hana-3.



A Snapshot backup has now been created at the primary HANA resource. The hostname included in the backup name shows hana-3.

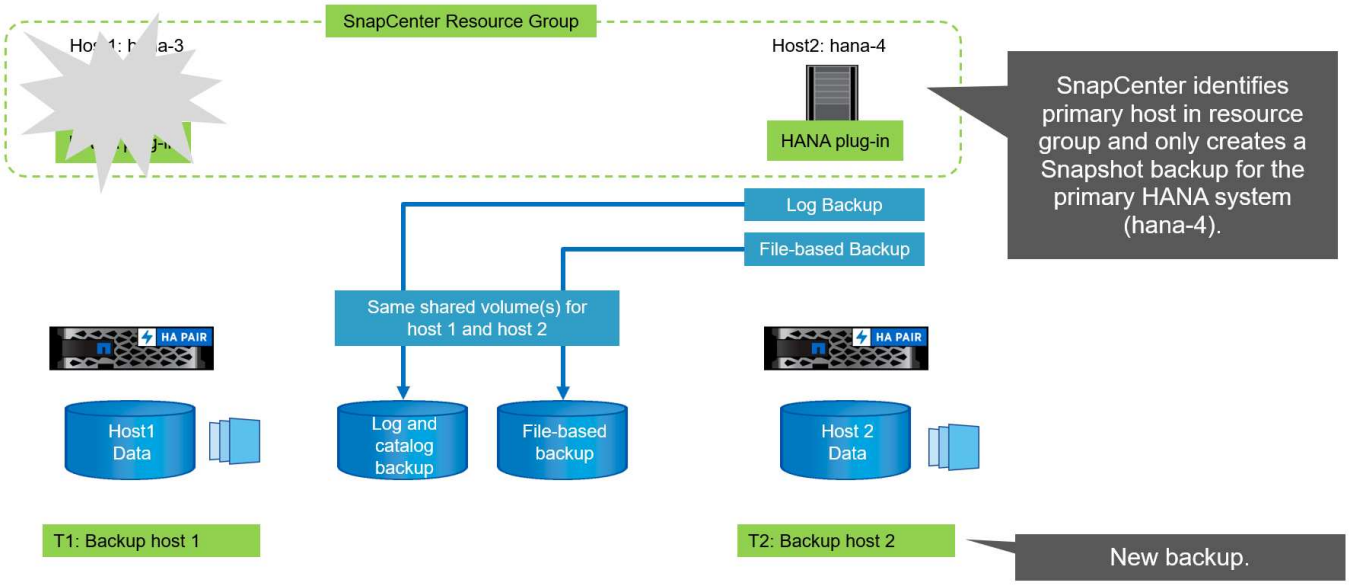


The same Snapshot backup is also visible in the HANA backup catalog.

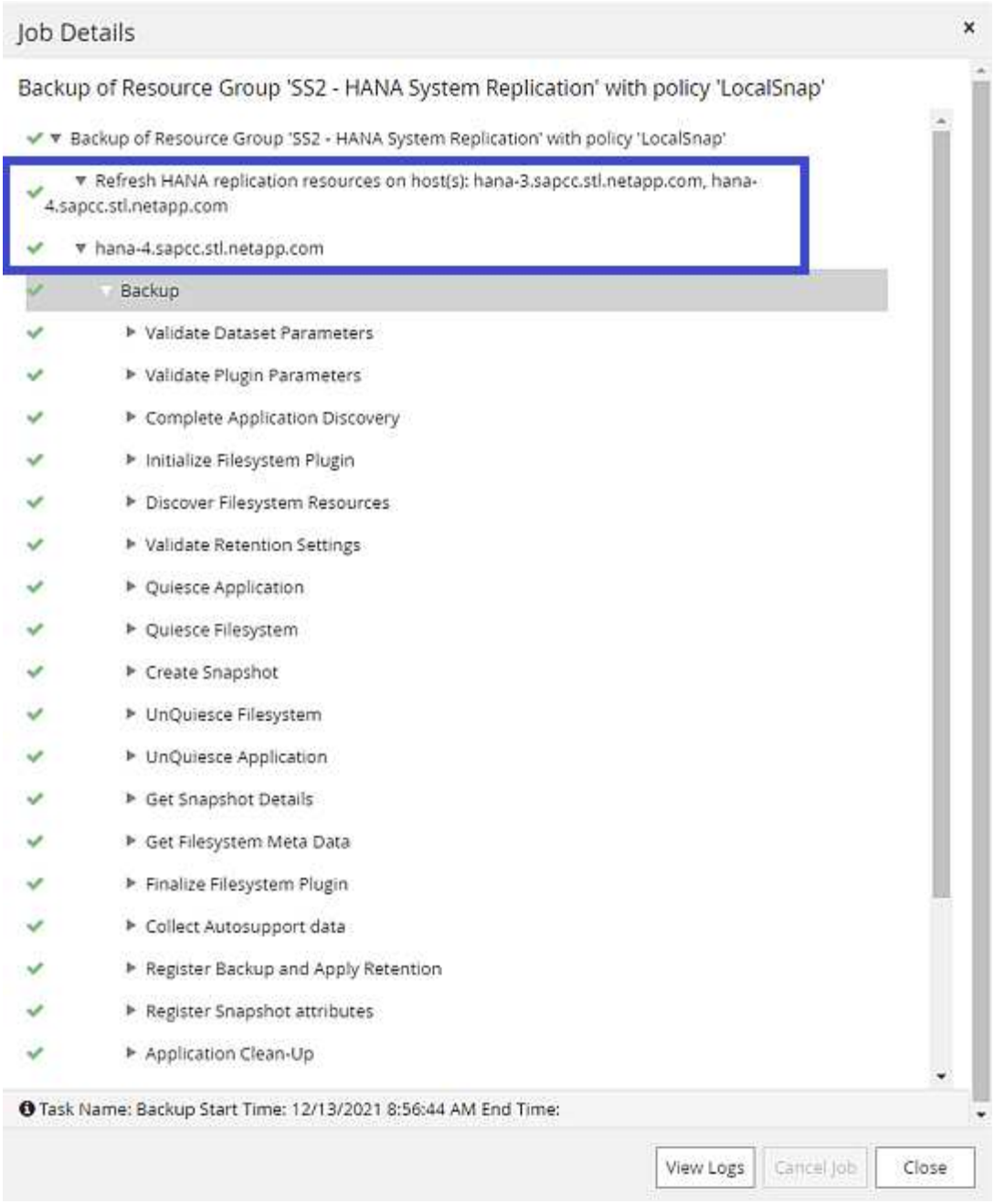


If a takeover operation is executed, further SnapCenter backups now identify the former secondary host (hana-4) as primary, and the backup operation is executed at hana-4. Again, only the data volume of the new primary host (hana-4) is snapshotted.

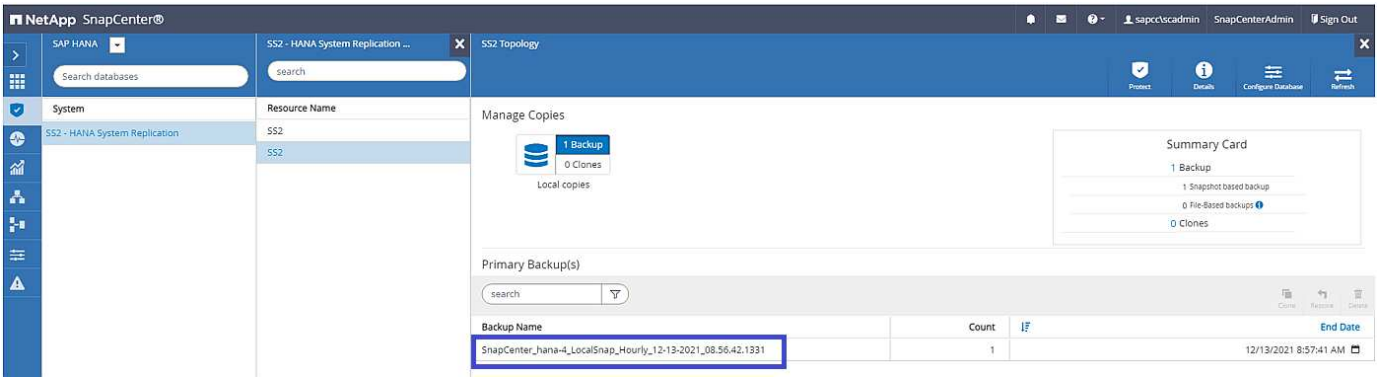
> The SnapCenter identification logic only covers scenarios in which the HANA hosts are in a primary-secondary relation or when one of the HANA hosts is offline.



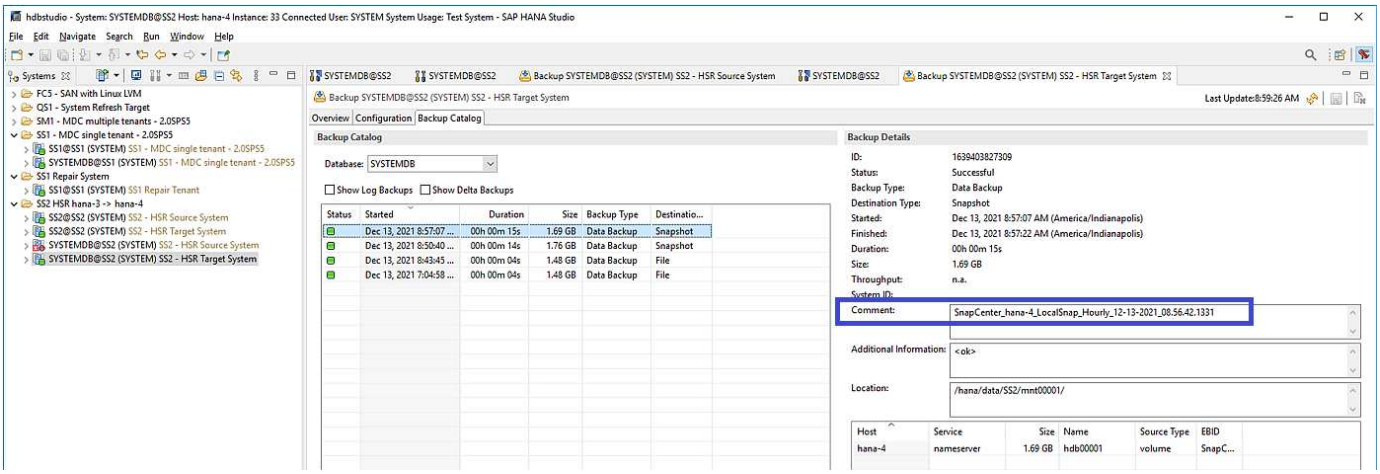
The SnapCenter job log shows the identification operation and the execution of the backup at the current primary host hana-4.



A Snapshot backup has now been created at the primary HANA resource. The hostname included in the backup name shows hana-4.



The same Snapshot backup is also visible in the HANA backup catalog.



Block-integrity check operations with file-based backups

SnapCenter 4.6 uses the same logic as described for Snapshot backup operations for block-integrity check operations with file-based backups. SnapCenter identifies the current primary HANA host and executes the file-based backup for this host. Retention management is also performed across both hosts, so the oldest backup is deleted regardless of which host is currently the primary.

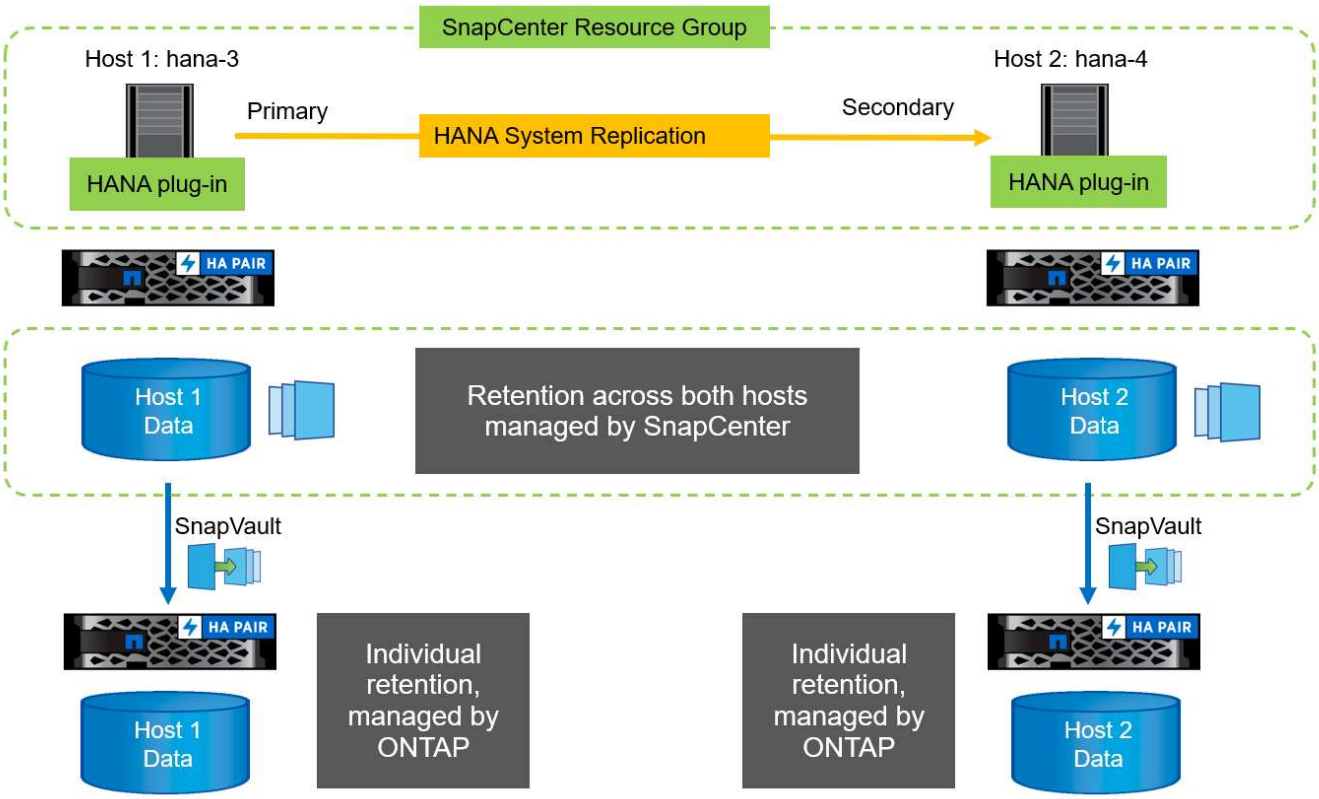
SnapVault replication

To allow transparent backup operations without manual interaction in case of a takeover and independent of which HANA host is currently the primary host, you must configure a SnapVault relationship for the data volumes of both hosts. SnapCenter executes a SnapVault update operation for the current primary host with each backup run.

> If a takeover to the secondary host is not performed for a long time, the number of changed blocks for the first SnapVault update at the secondary host will be high.

Since the retention management at the SnapVault target is managed outside of SnapCenter by ONTAP, the retention can't be handled across both HANA hosts. Therefore backups that have been created before a takeover are not deleted with backup operations at the former secondary. These backups remain until the former primary becomes primary again. So that these backups do not block the retention management of log backups, they must deleted manually either at the SnapVault target or within the HANA backup catalog.

> A cleanup of all SnapVault Snapshot copies is not possible, because one Snapshot copy is blocked as a synchronization point. If the latest Snapshot copy needs to be deleted as well, the SnapVault replication relationship must be deleted. In this case, NetApp recommends deleting the backups in the HANA backup catalog to unblock log backup retention management.



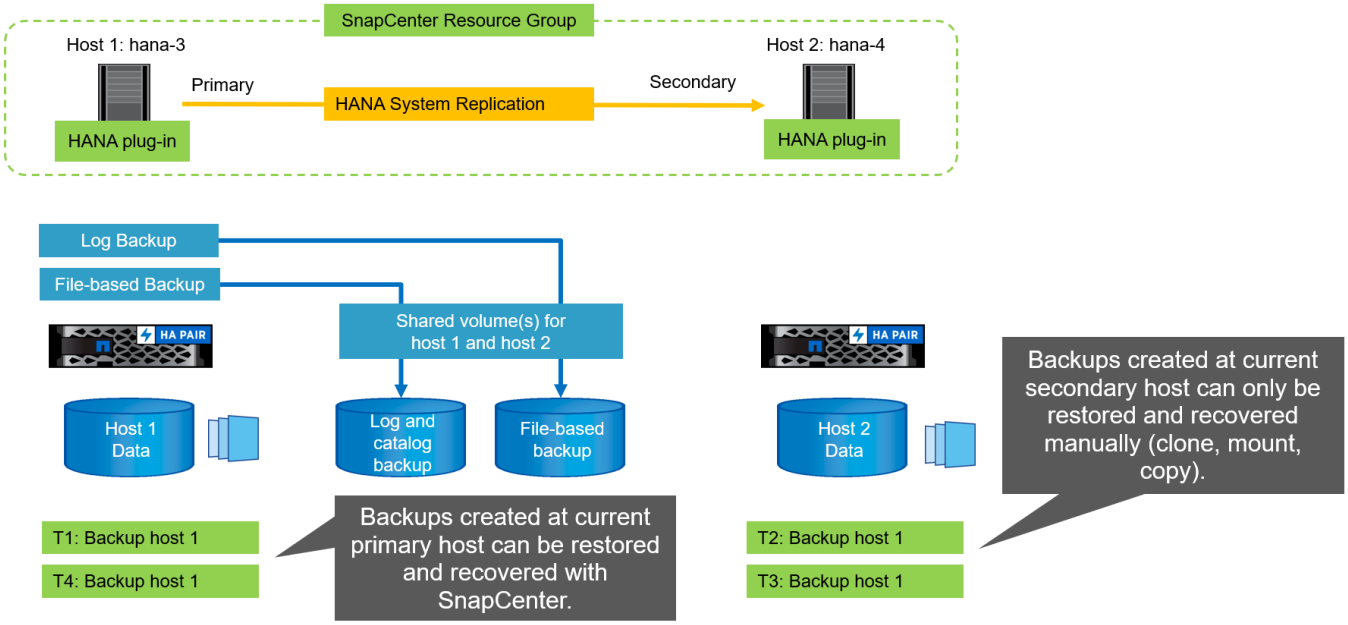
Retention management

SnapCenter 4.6 manages retention for Snapshot backups, block-integrity check operations, HANA backup catalog entries, and log backups (if not disabled) across both HANA hosts, so it doesn't matter which host is currently primary or secondary. Backups (data and log) and entries in the HANA catalog are deleted based on the defined retention, regardless of whether a delete operation is necessary on the current primary or secondary host. In other words, no manual interaction is required if a takeover operation is performed and/or the replication is configured in the other direction.

If SnapVault replication is part of the data protection strategy, manual interaction is required for specific scenarios, as described in the section [SnapVault Replication].

Restore and recovery

The following figure depicts a scenario in which multiple takeovers have been executed and Snapshot backups have been created at both sites. With the current status, the host hana-3 is the primary host and the latest backup is T4, which has been created at host hana-3. If you need to perform a restore and recovery operation, the backups T1 and T4 are available for restore and recovery in SnapCenter. The backups, which have been created at host hana-4 (T2, T3), can't be restored using SnapCenter. These backups must be copied manually to the data volume of hana-3 for recovery.



Restore and recovery operations for a SnapCenter 4.6 resource group configuration are identical to an autodiscovered non-System Replication setup. All options for restore and automated recovery are available. For further details, see the technical report TR-4614: SAP HANA Backup and Recovery with SnapCenter.

A restore operation from a backup that was created at the other host is described in the section Restore and Recovery from a Backup Created at the Other Host.

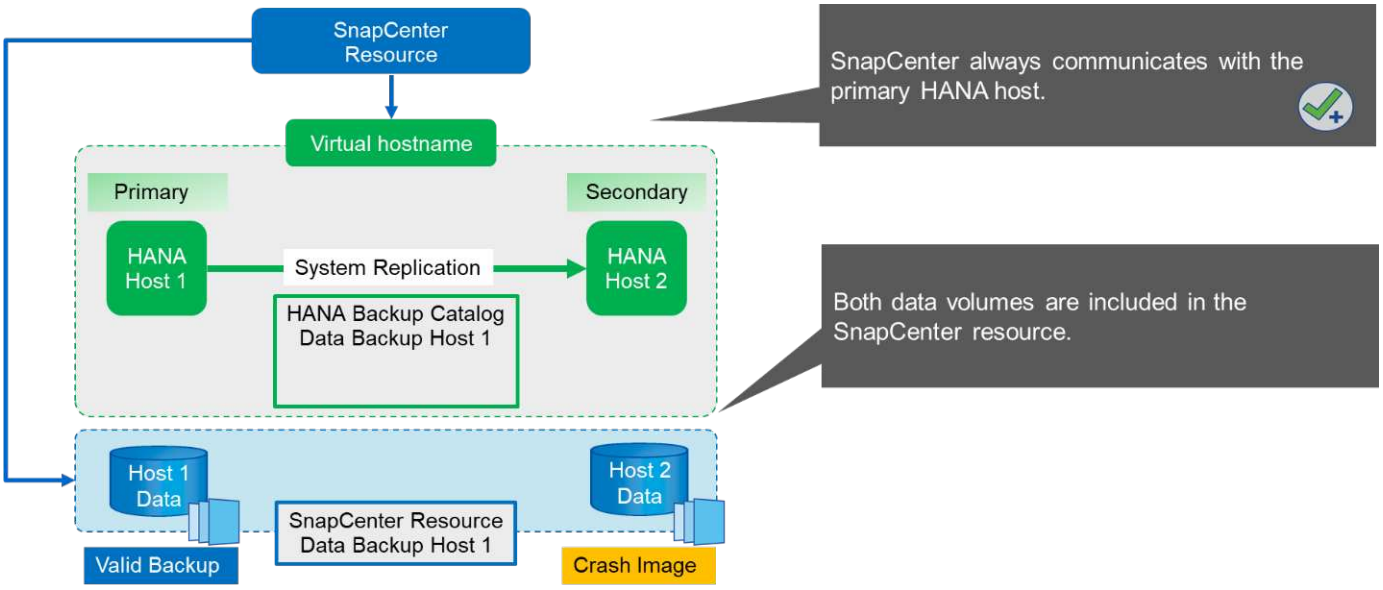
SnapCenter configuration with a single resource

A SnapCenter resource is configured with the virtual IP address (host name) of the HANA System Replication environment. With this approach, SnapCenter always communicates with the primary host, regardless of whether host 1 or host 2 is primary. The data volumes of both SAP HANA hosts are included in the SnapCenter resource.

> We assume that the virtual IP address is always bound to the primary SAP HANA host. The failover of the virtual IP address is performed outside SnapCenter as part of the HANA System Replication failover workflow.

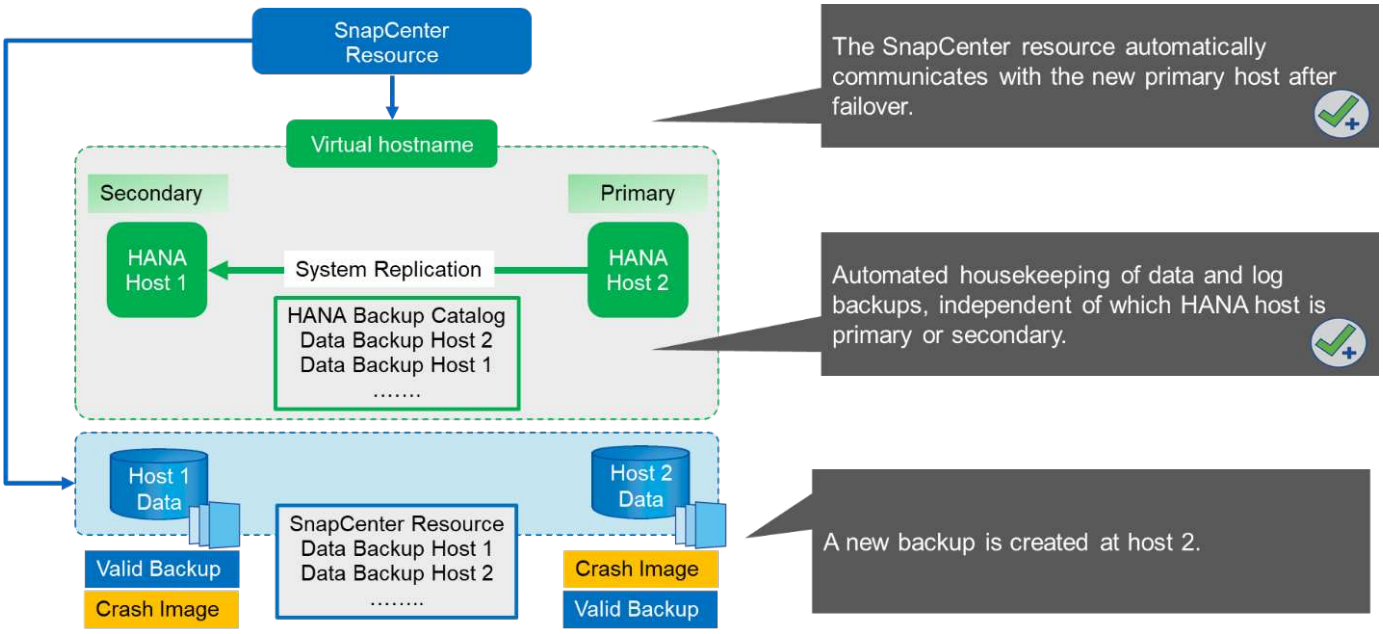
When a backup is executed with host 1 as the primary host, a database-consistent Snapshot backup is created at the data volume of host 1. Because the data volume of host 2 is part of the SnapCenter resource, another Snapshot copy is created for this volume. This Snapshot copy is not database consistent; rather, it is just a crash image of the secondary host.

The SAP HANA backup catalog and the SnapCenter resource includes the backup created at host 1.



The following figure shows the backup operation after failover to host 2 and replication from host 2 to host 1. SnapCenter automatically communicates with host 2 by using the virtual IP address configured in the SnapCenter resource. Backups are now created at host 2. Two Snapshot copies are created by SnapCenter: a database-consistent backup at the data volume at host 2 and a crash image Snapshot copy at the data volume at host 1. The SAP HANA backup catalog and the SnapCenter resource now include the backup created at host 1 and the backup created at host 2.

Housekeeping of data and log backups is based on the defined SnapCenter retention policy, and backups are deleted regardless of which host is primary or secondary.

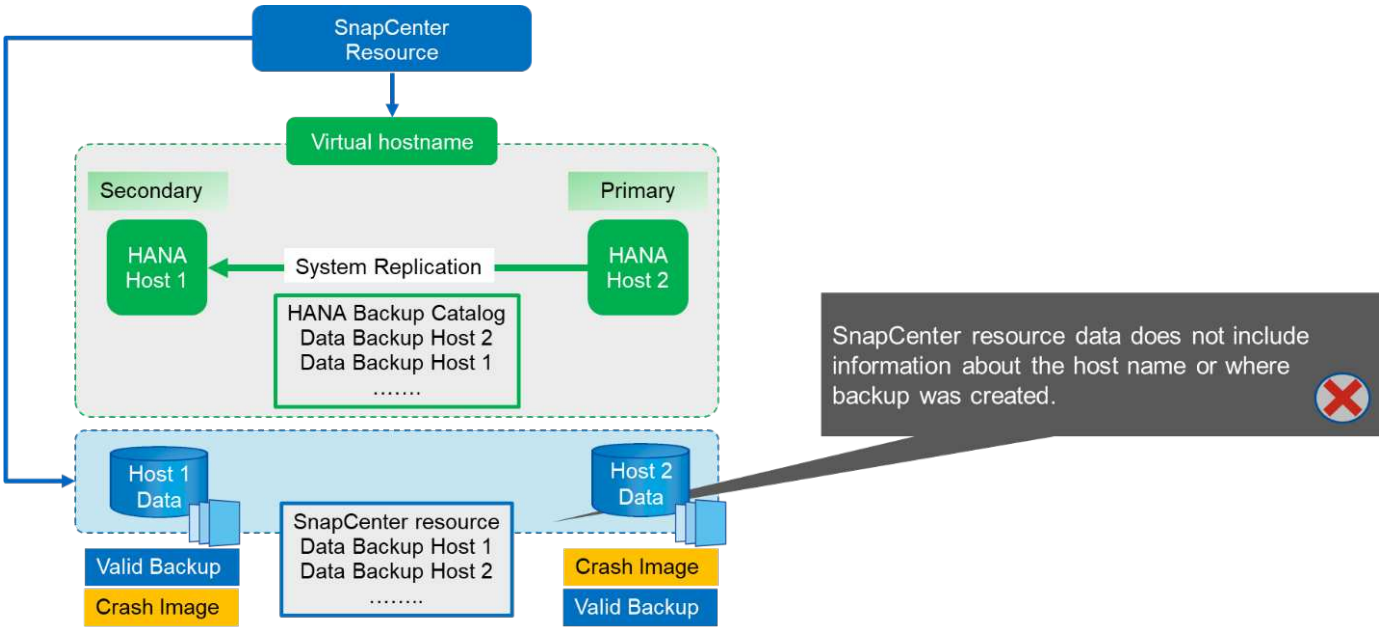


As discussed in the section Storage Snapshot Backups and SAP System Replication, a restore operation with storage-based Snapshot backups is different, depending on which backup must be restored. It is important to identify which host the backup was created at to determine if the restore can be performed at the local storage volume, or if the restore must be performed at the other host's storage volume.

With single-resource SnapCenter configuration, SnapCenter is not aware of where the backup was created. Therefore, NetApp recommends that you add a prebackup script to the SnapCenter backup workflow to

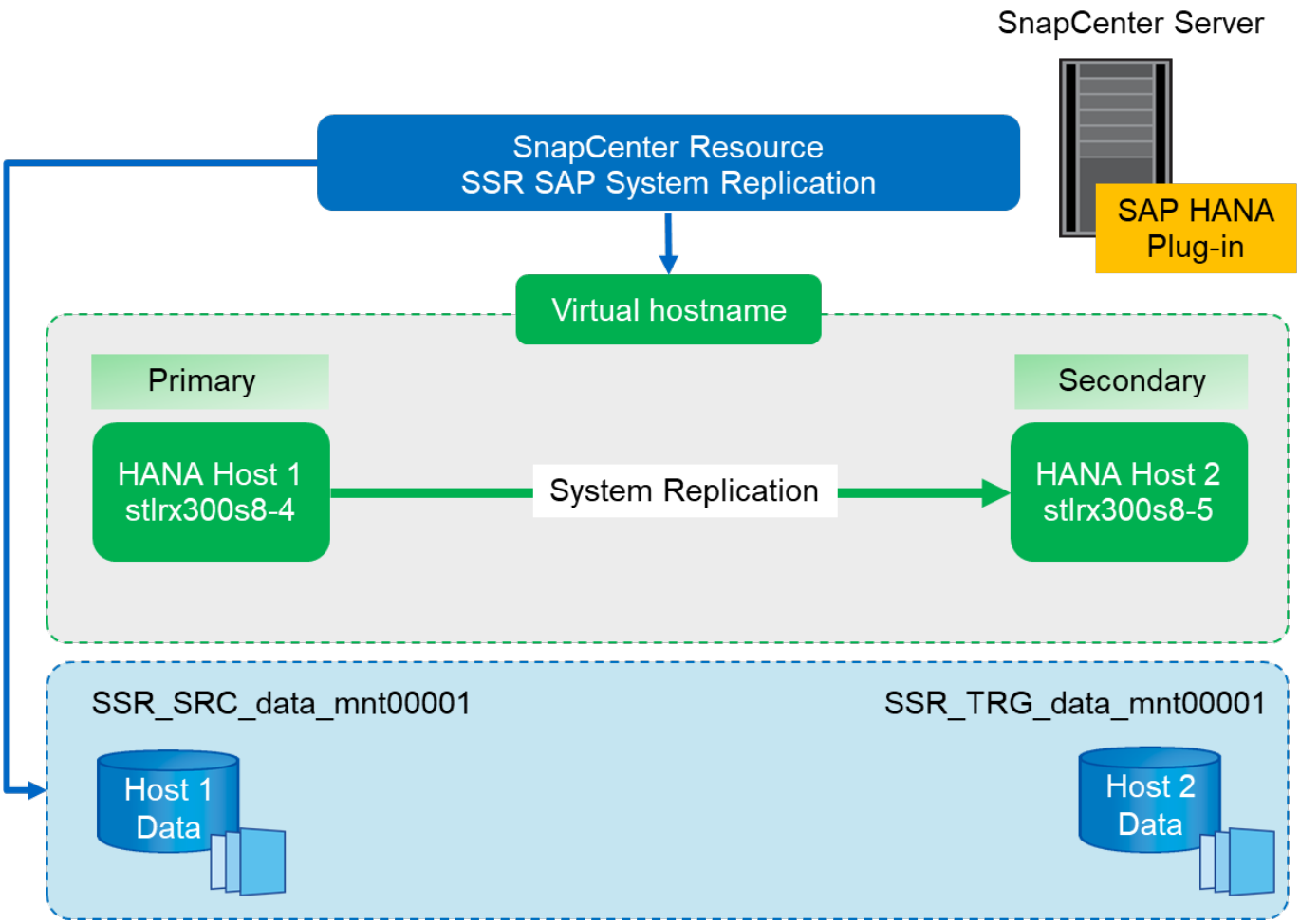
identify which host is currently the primary SAP HANA host.

The following figure depicts identification of the backup host.



SnapCenter configuration

The following figure shows the lab setup and an overview of the required SnapCenter configuration.



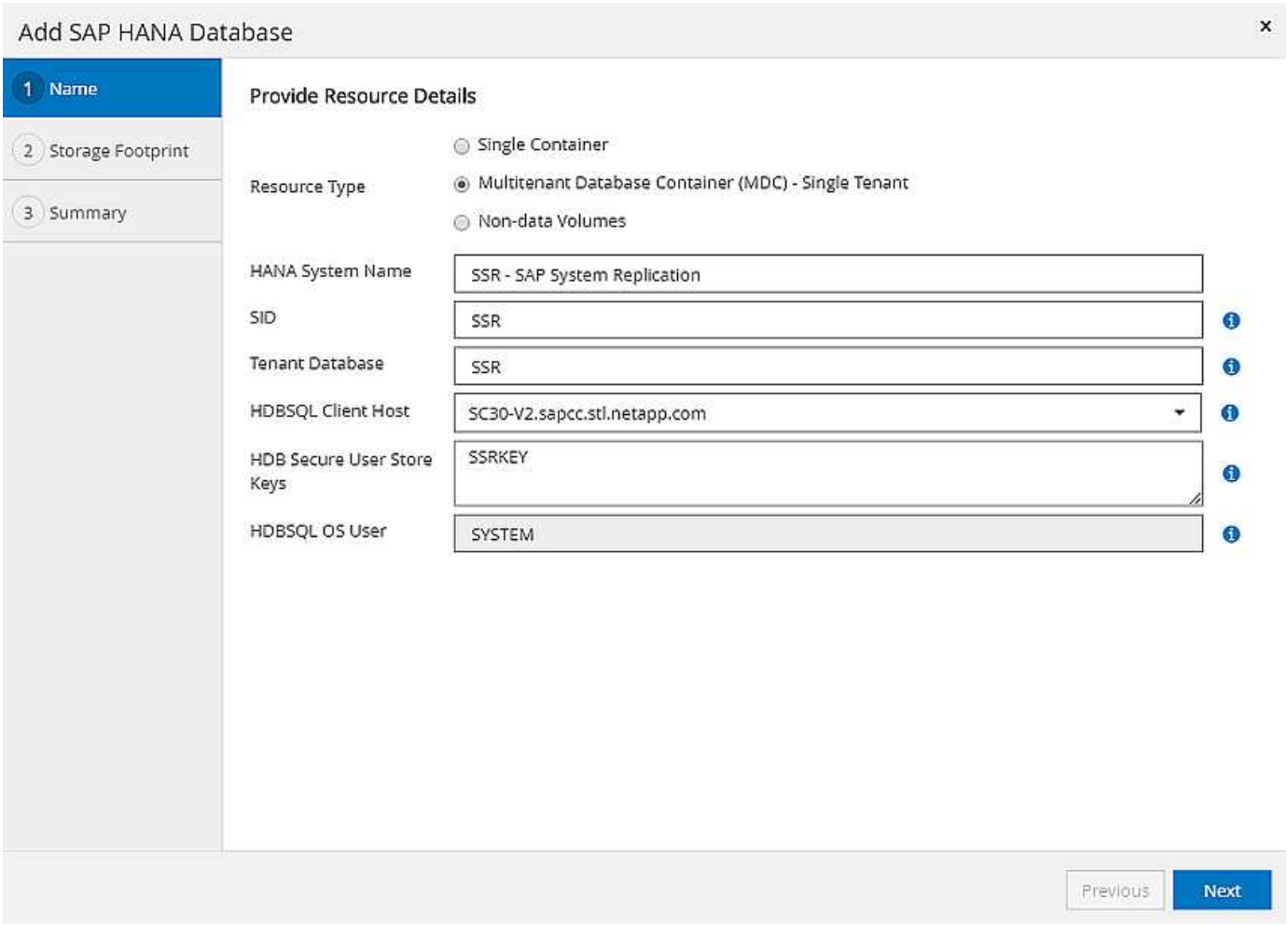
To perform backup operations regardless of which SAP HANA host is primary and even when one host is down, the SnapCenter SAP HANA plug-in must be deployed on a central plug-in host. In our lab setup, we used the SnapCenter server as a central plug-in host, and we deployed the SAP HANA plug-in on the SnapCenter server.

A user was created in the HANA database to perform backup operations. A user store key was configured at the SnapCenter server on which the SAP HANA plug-in was installed. The user store key includes the virtual IP address of the SAP HANA System Replication hosts (`ssr-vip`).

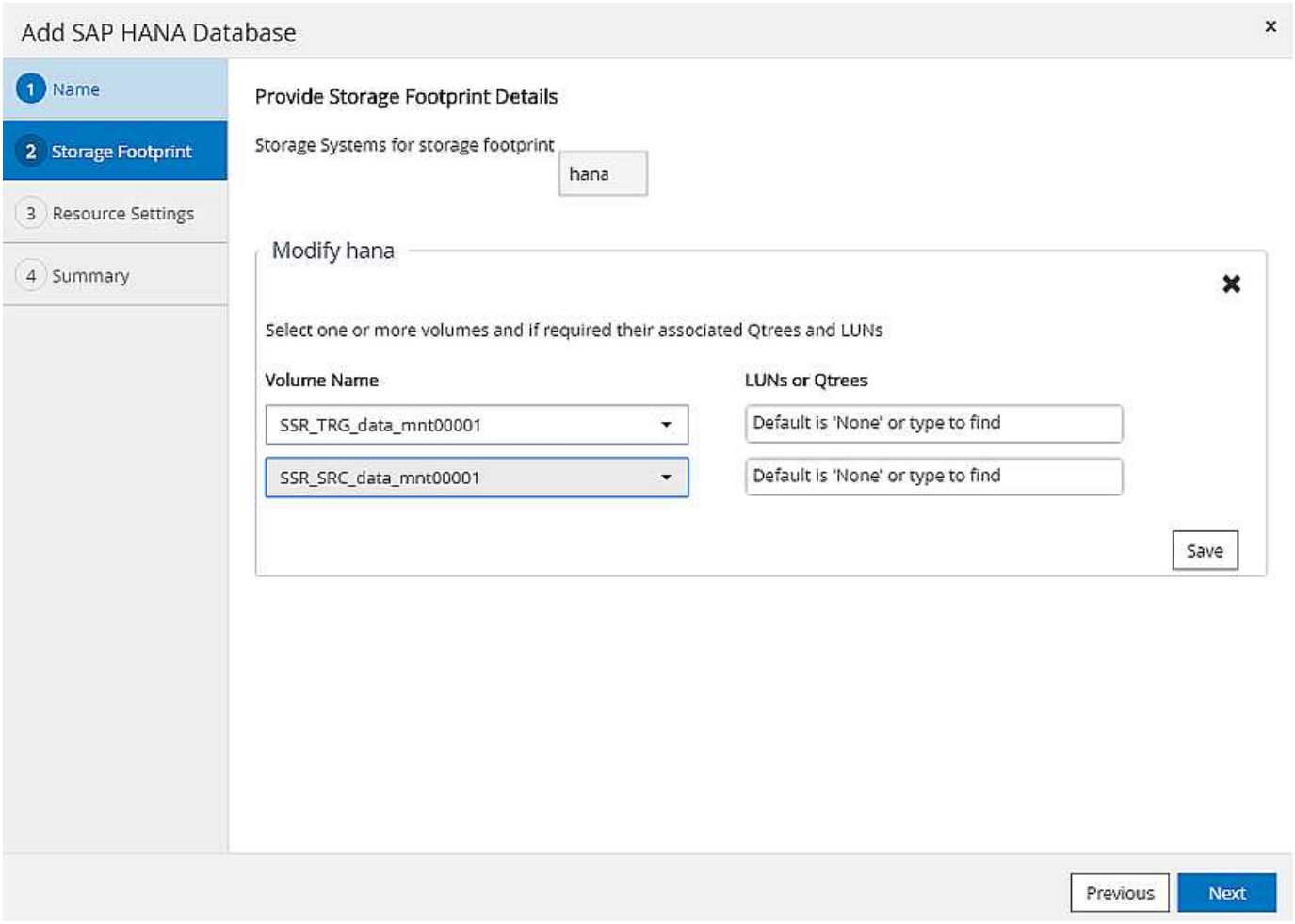
```
hdbuserstore.exe -u SYSTEM set SSRKEY ssr-vip:31013 SNAPCENTER <password>
```

You can find more information about SAP HANA plug-in deployment options and user store configuration in the technical report TR-4614: SAP HANA Backup and Recovery with SnapCenter.

In SnapCenter, the resource is configured as shown in the following figure using the user store key, configured before, and the SnapCenter server as the `hdbsql` communication host.

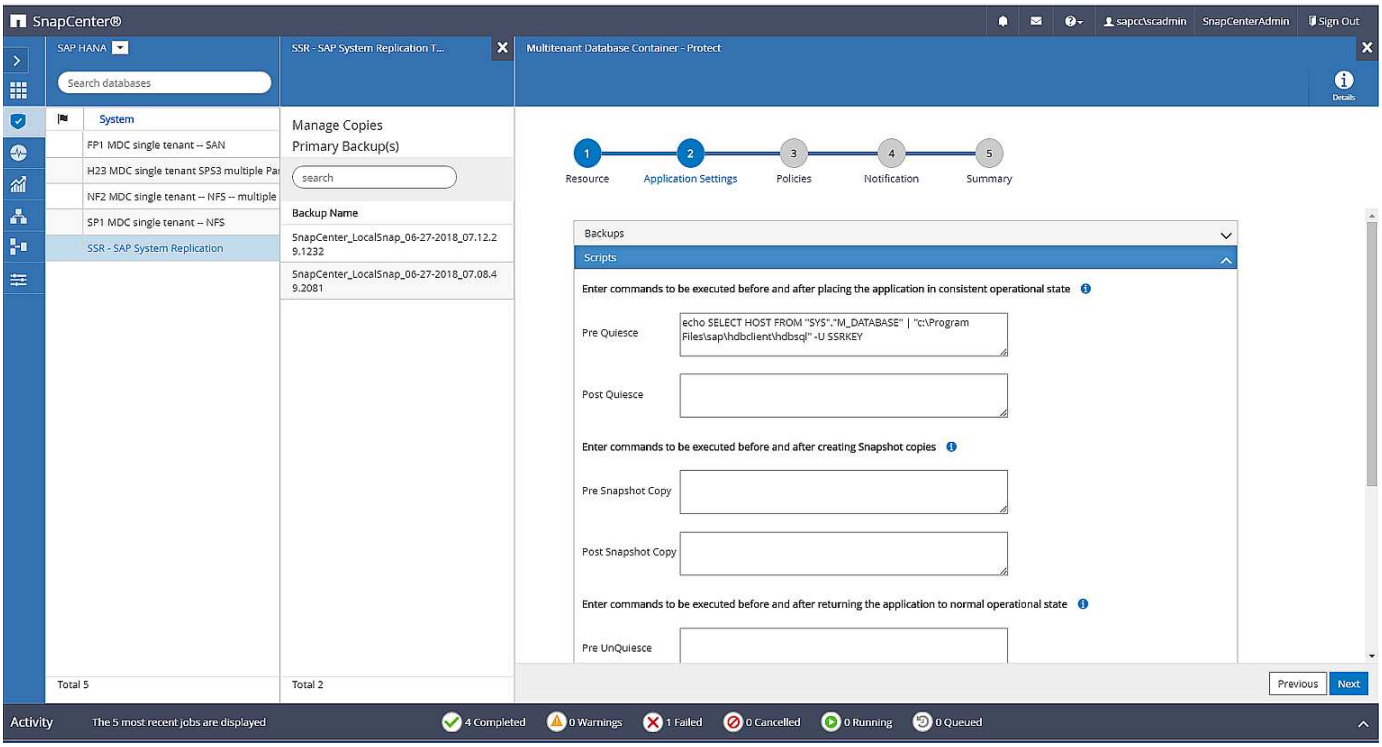


The data volumes of both SAP HANA hosts are included in the storage footprint configuration, as the following figure shows.



As discussed before, SnapCenter is not aware of where the backup was created. NetApp therefore recommends that you add a pre- backup script in the SnapCenter backup workflow to identify which host is currently the primary SAP HANA host. You can perform this identification using a SQL statement that is added to the backup workflow, as the following figure shows.

```
Select host from "SYS".M_DATABASE
```

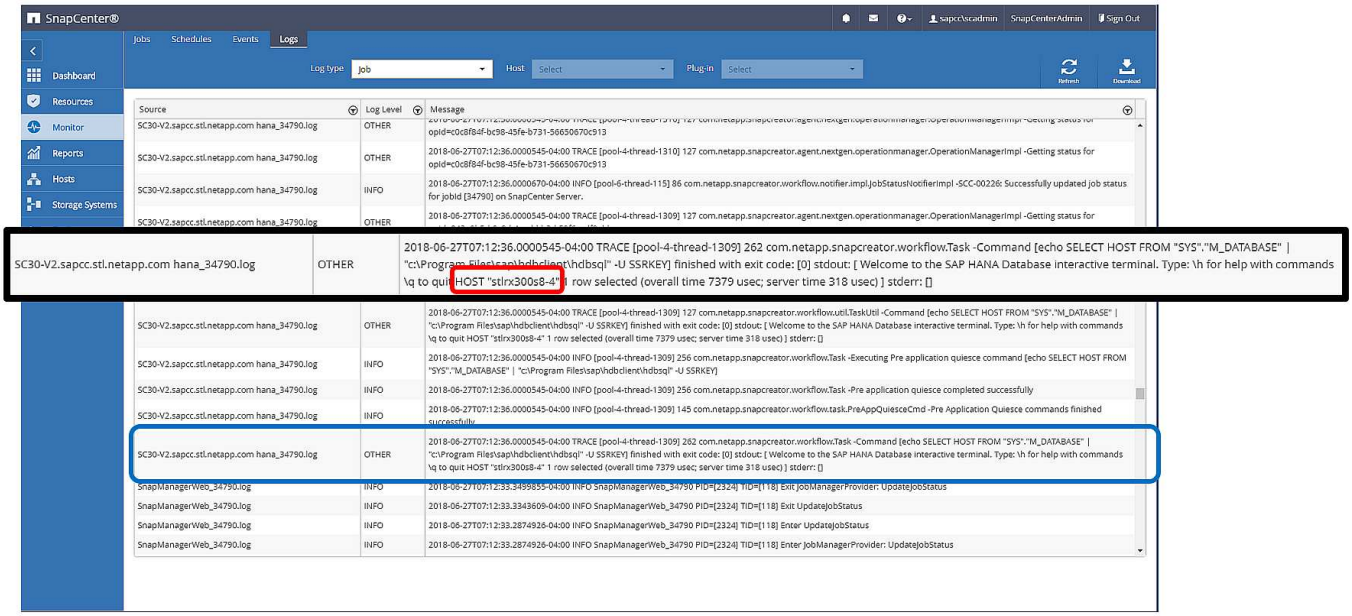


SnapCenter backup operation

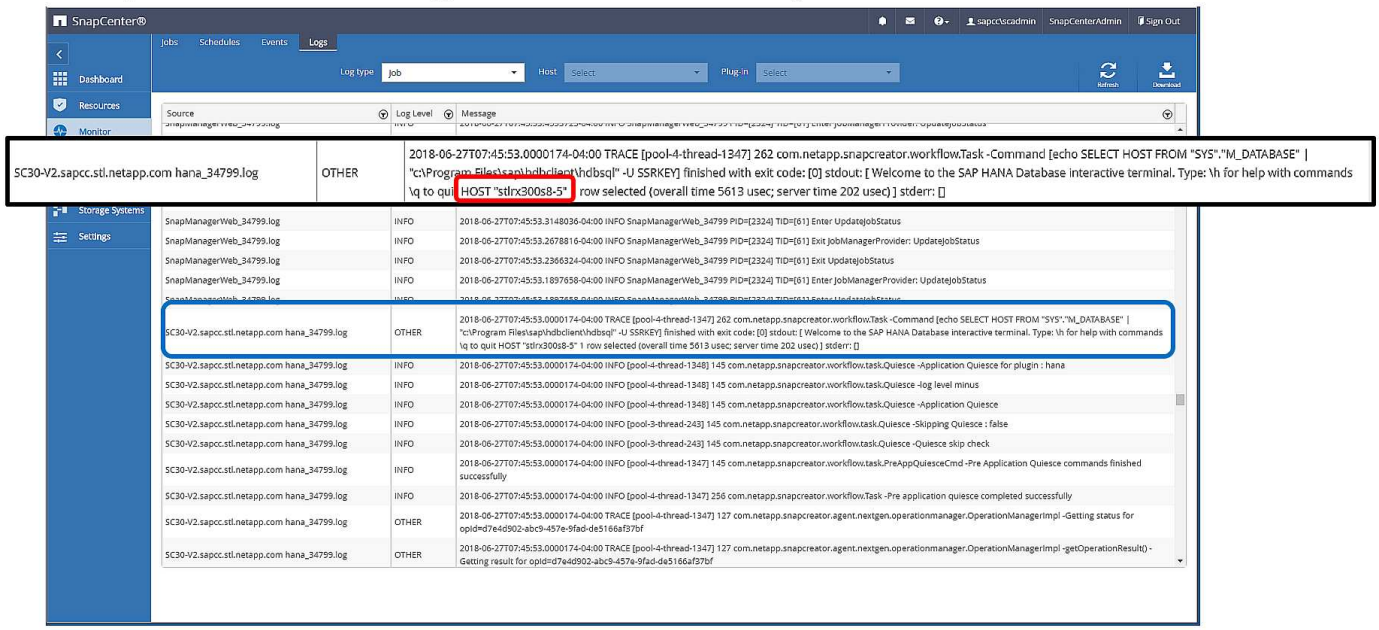
Backup operations are now executed as usual. Housekeeping of data and log backups is performed independent of which SAP HANA host is primary or secondary.

The backup job logs include the output of the SQL statement, which allows you to identify the SAP HANA host where the backup was created.

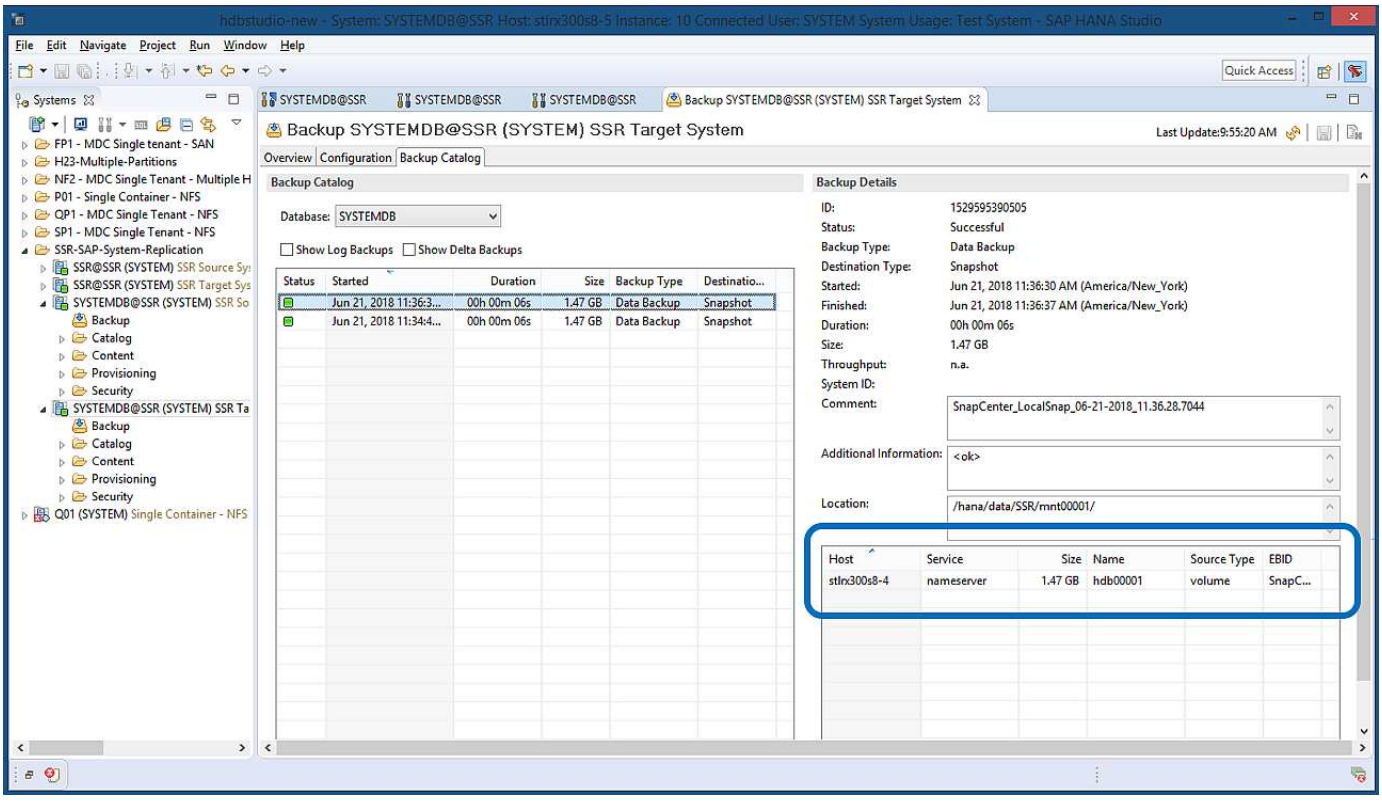
The following figure shows the backup job log with host 1 as the primary host.



This figure shows the backup job log with host 2 as the primary host.



The following figure shows the SAP HANA backup catalog in SAP HANA Studio. When the SAP HANA database is online, the SAP HANA host where the backup was created is visible in SAP HANA Studio.



The SAP HANA backup catalog on the file system, which is used during a restore and recovery operation, does not include the host name where the backup was created. The only way to identify the host when the database is down is to combine the backup catalog entries with the `backup.log` file of both SAP HANA hosts.

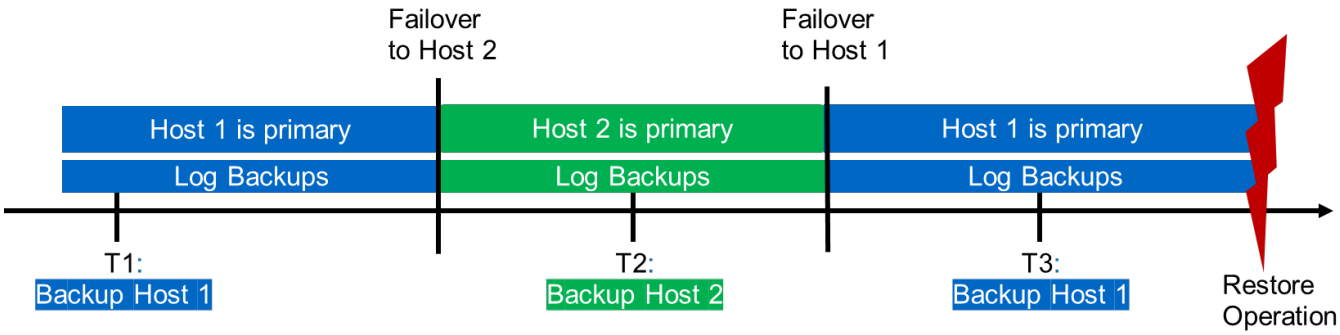
Restore and recovery

As discussed before, you must be able to identify where the selected backup was created to define the required restore operation. If the SAP HANA database is still online, you can use SAP HANA Studio to identify the host at which the backup was created. If the database is offline, the information is only available in the SnapCenter backup job log.

The following figure illustrates the different restore operations depending on the selected backup.

If a restore operation must be performed after timestamp T3 and host 1 is the primary, you can restore the backup created at T1 or T3 by using SnapCenter. These Snapshot backups are available at the storage volume attached to host 1.

If you need to restore using the backup created at host 2 (T2), which is a Snapshot copy at the storage volume of host 2, the backup needs to be made available to host 1. You can make this backup available by creating a NetApp FlexClone copy from the backup, mounting the FlexClone copy to host 1, and copying the data to the original location.



Restore Operation With	
Backup T1	SnapCenter
Backup T2	Create FlexClone from „Backup host 2“, mount and copy
Backup T3	SnapCenter

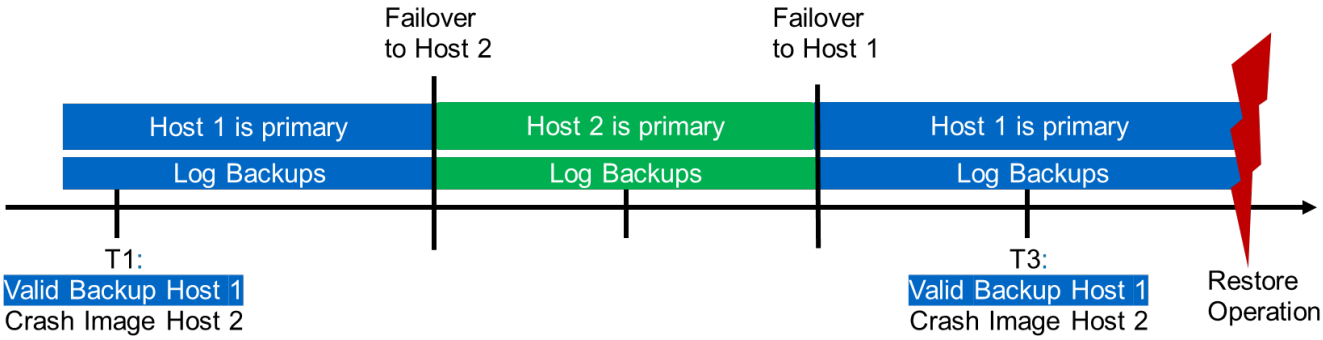
With a single SnapCenter resource configuration, Snapshot copies are created at both storage volumes of both SAP HANA System Replication hosts. Only the Snapshot backup that is created at the storage volume of the primary SAP HANA host is valid to use for forward recovery. The Snapshot copy created at the storage volume of the secondary SAP HANA host is a crash image that cannot be used for forward recovery.

A restore operation with SnapCenter can be performed in two different ways:

- Restore only the valid backup
- Restore the complete resource, including the valid backup and the crash imageThe following sections discuss the two different restore operations in more detail.

A restore operation from a backup that was created at the other host is described in the section Restore and Recovery from a Backup Created at the Other Host.

The following figure depicts restore operations with a single SnapCenter resource configuration.

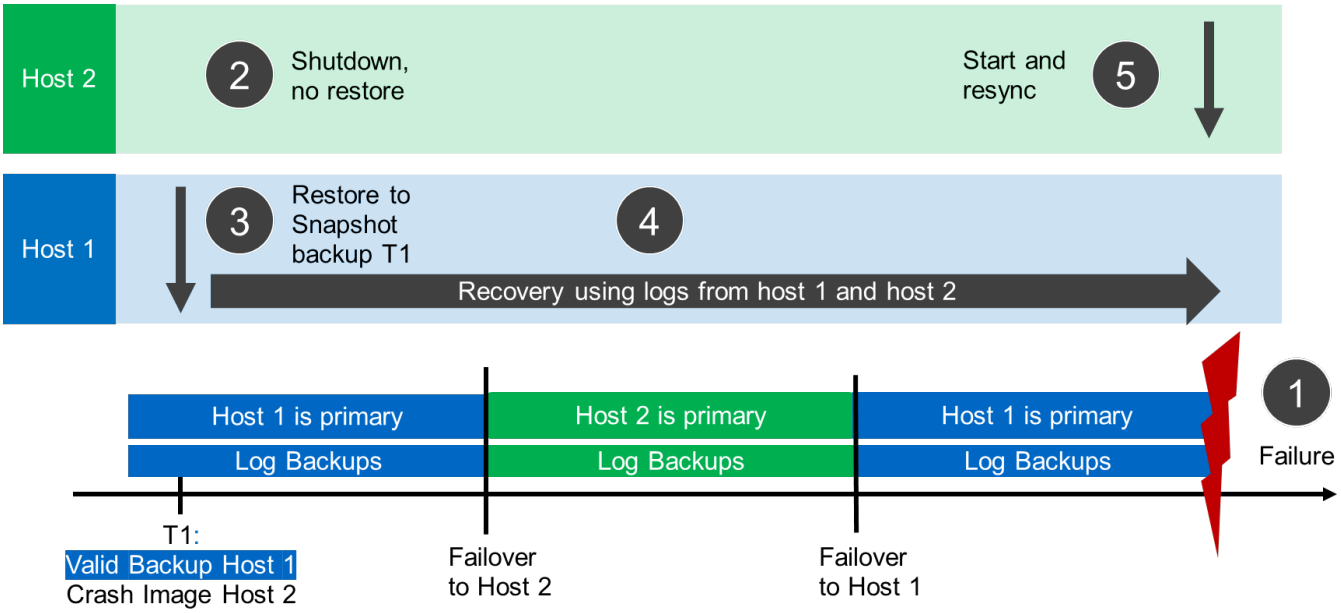


SnapCenter restore of the valid backup only

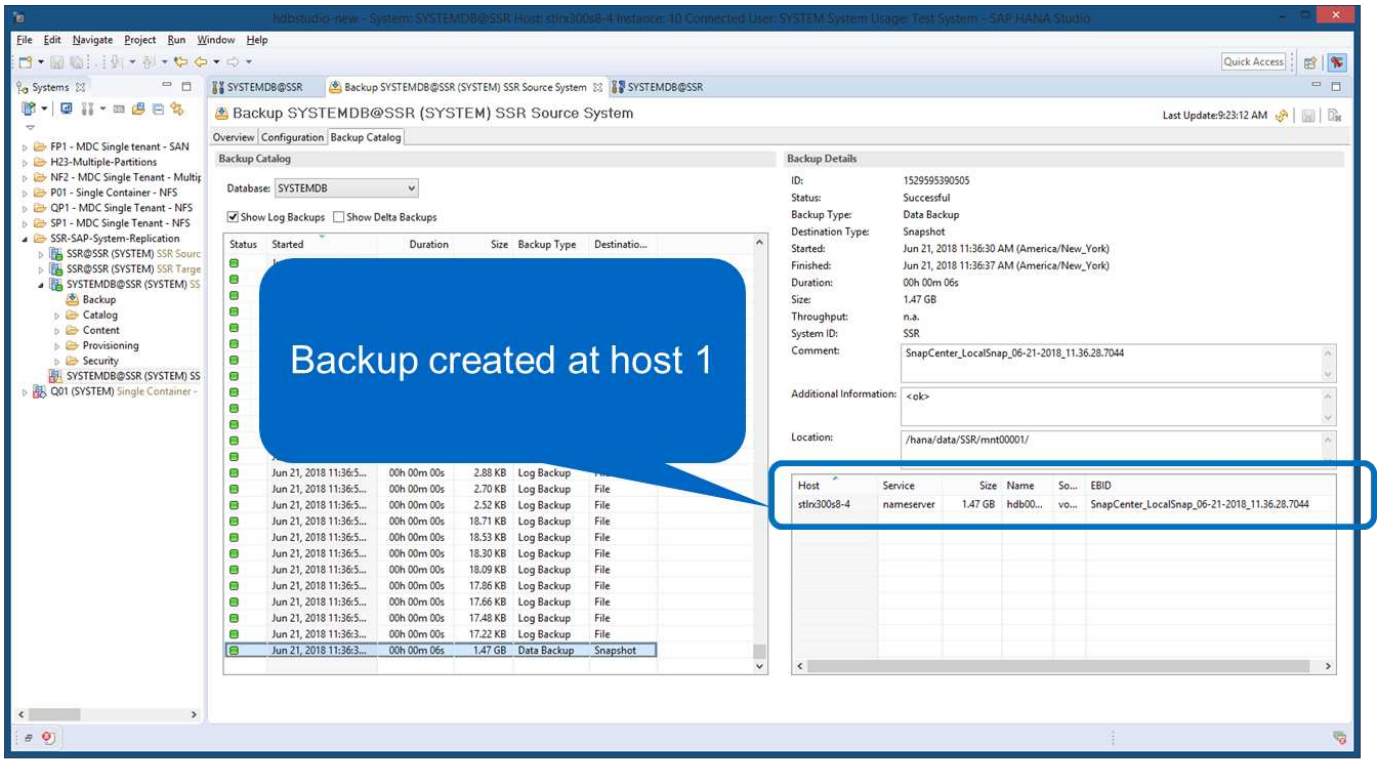
The following figure shows an overview of the restore and recovery scenario described in this section.

A backup has been created at T1 at host 1. A failover has been performed to host 2. After a certain point in time, another failover back to host 1 was performed. At the current point in time, host 1 is the primary host.

1. A failure occurred and you must restore to the backup created at T1 at host 1.
2. The secondary host (host 2) is shut down, but no restore operation is executed.
3. The storage volume of host 1 is restored to the backup created at T1.
4. A forward recovery is performed with logs from host 1 and host 2.
5. Host 2 is started, and a system replication resynchronization of host 2 is automatically started.



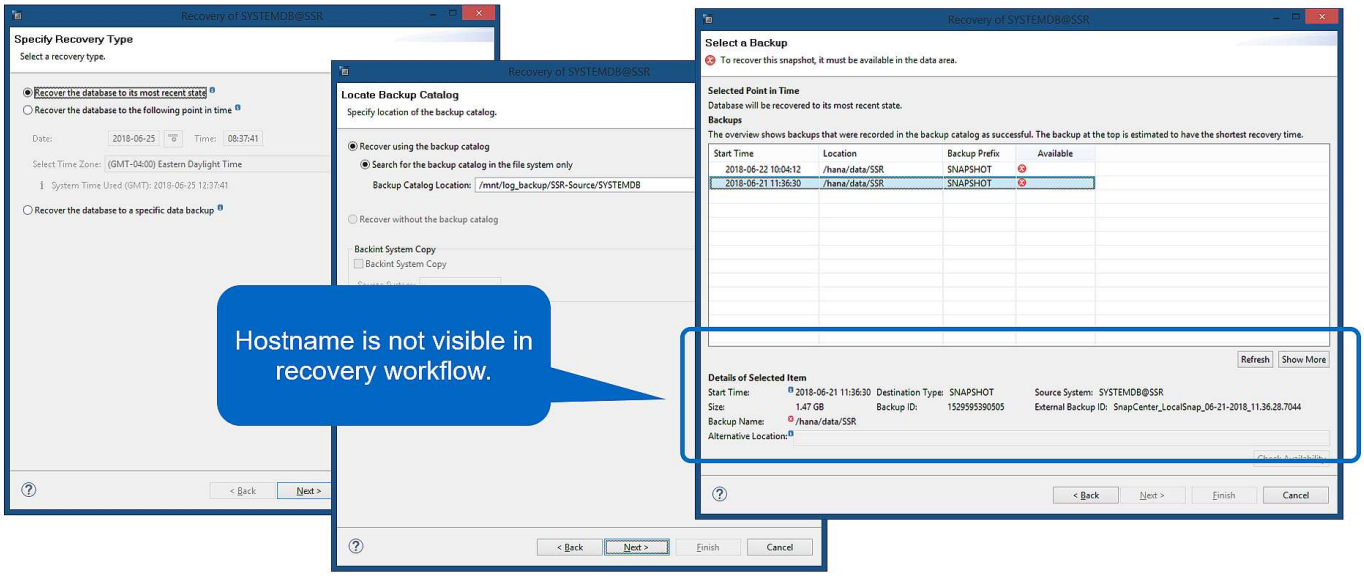
The following figure shows the SAP HANA backup catalog in SAP HANA Studio. The highlighted backup shows the backup created at T1 at host 1.



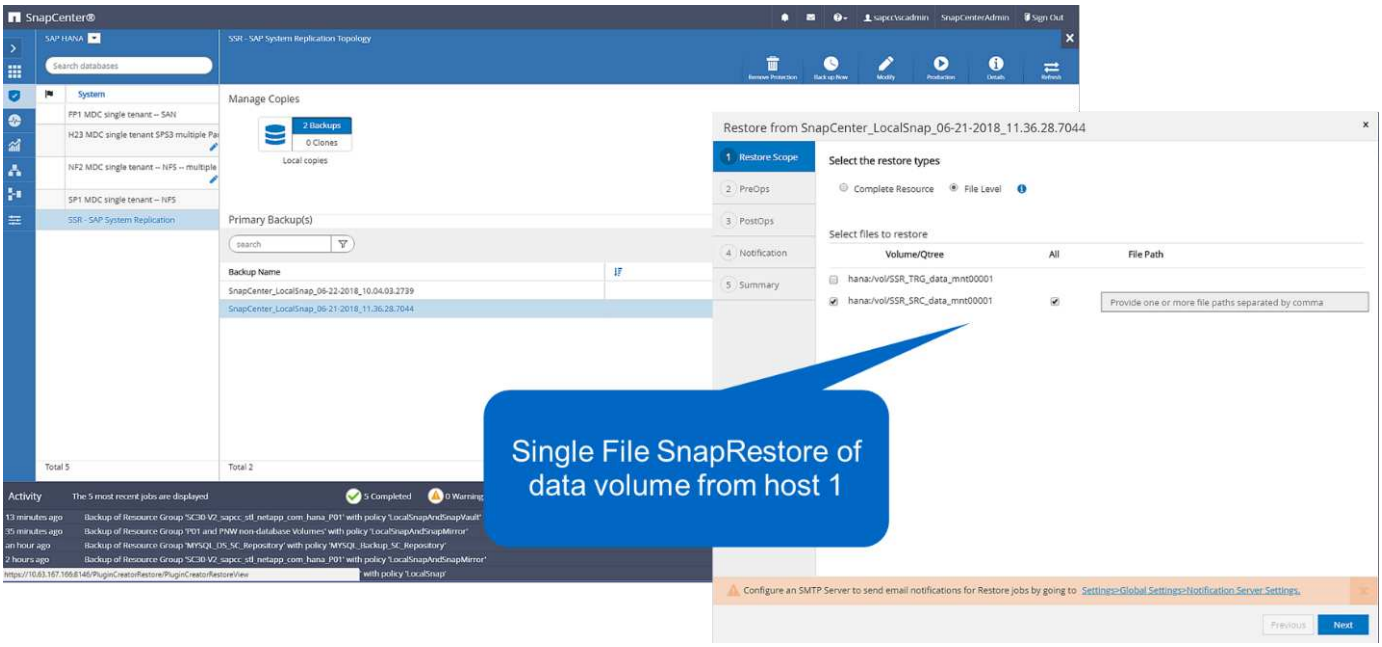
25

A restore and recovery operation is started in SAP HANA Studio. As the following figure shows, the name of the host where the backup was created is not visible in the restore and recovery workflow.

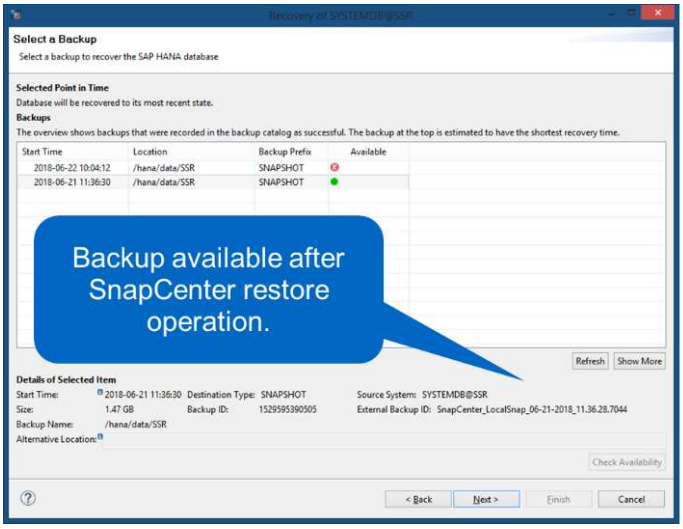
In our test scenario, we were able to identify the correct backup (the backup created at host 1) in SAP HANA Studio when the database was still online. If the database is not available, you must check the SnapCenter backup job log to identify the right backup.

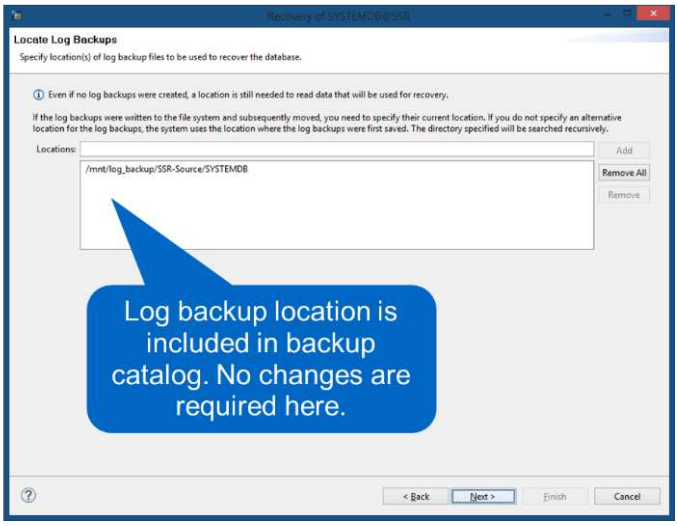


In SnapCenter, the backup is selected and a file-level restore operation is performed. On the file-level restore screen, only the host 1 volume is selected so that only the valid backup is restored.



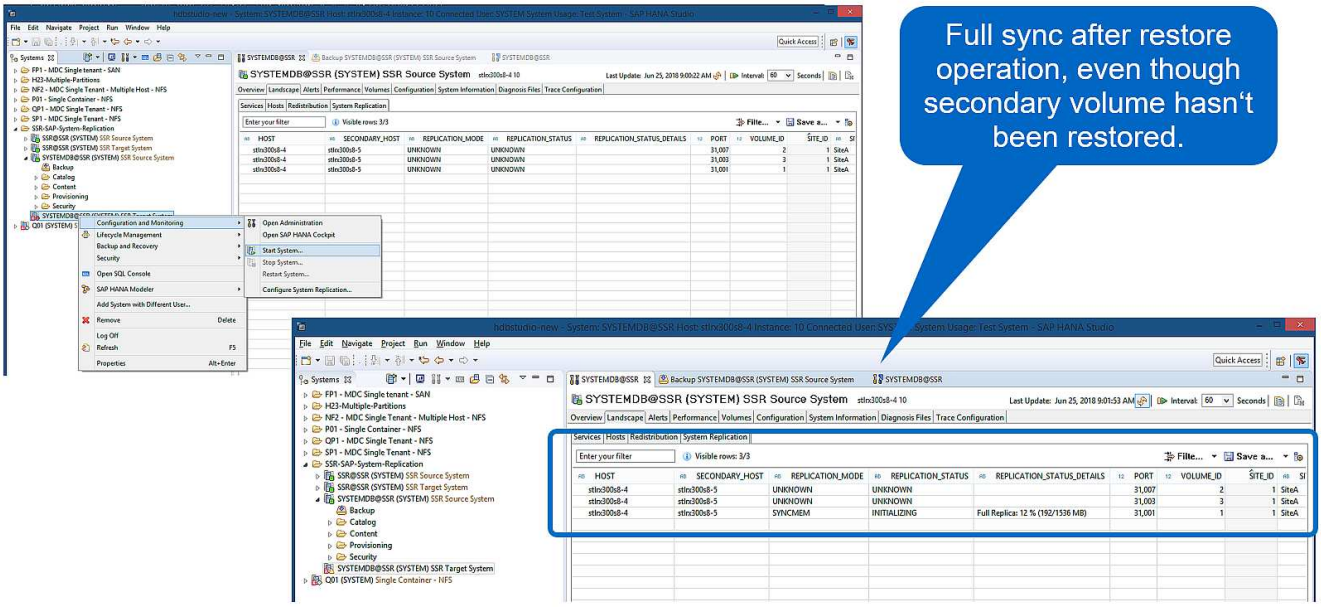
After the restore operation, the backup is highlighted in green in SAP HANA Studio. You don't have to enter an additional log backup location, because the file path of log backups of host 1 and host 2 are included in the backup catalog.





After forward recovery has finished, the secondary host (host 2) is started and SAP HANA System Replication resynchronization is started.

Even though the secondary host is up-to-date (no restore operation was performed for host 2), SAP HANA executes a full replication of all data. This behavior is standard after a restore and recovery operation with SAP HANA System Replication.

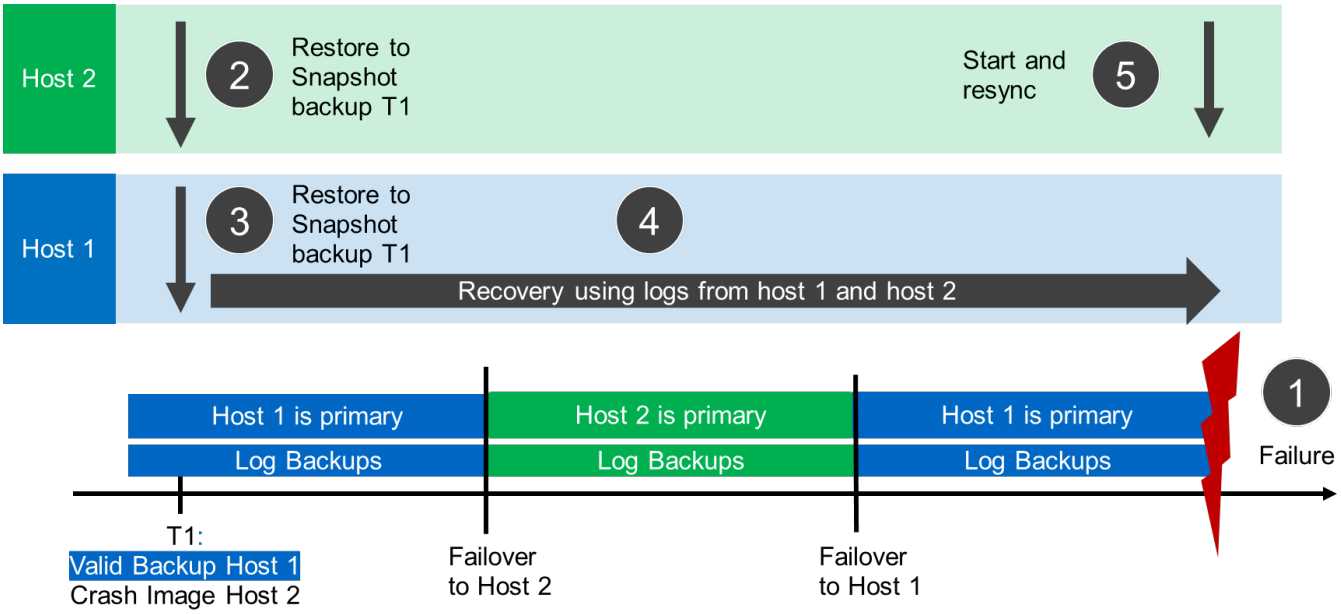


SnapCenter restore of valid backup and crash image

The following figure shows an overview of the restore and recovery scenario described in this section.

A backup has been created at T1 at host 1. A failover has been performed to host 2. After a certain point in time, another failover back to host 1 was performed. At the current point in time, host 1 is the primary host.

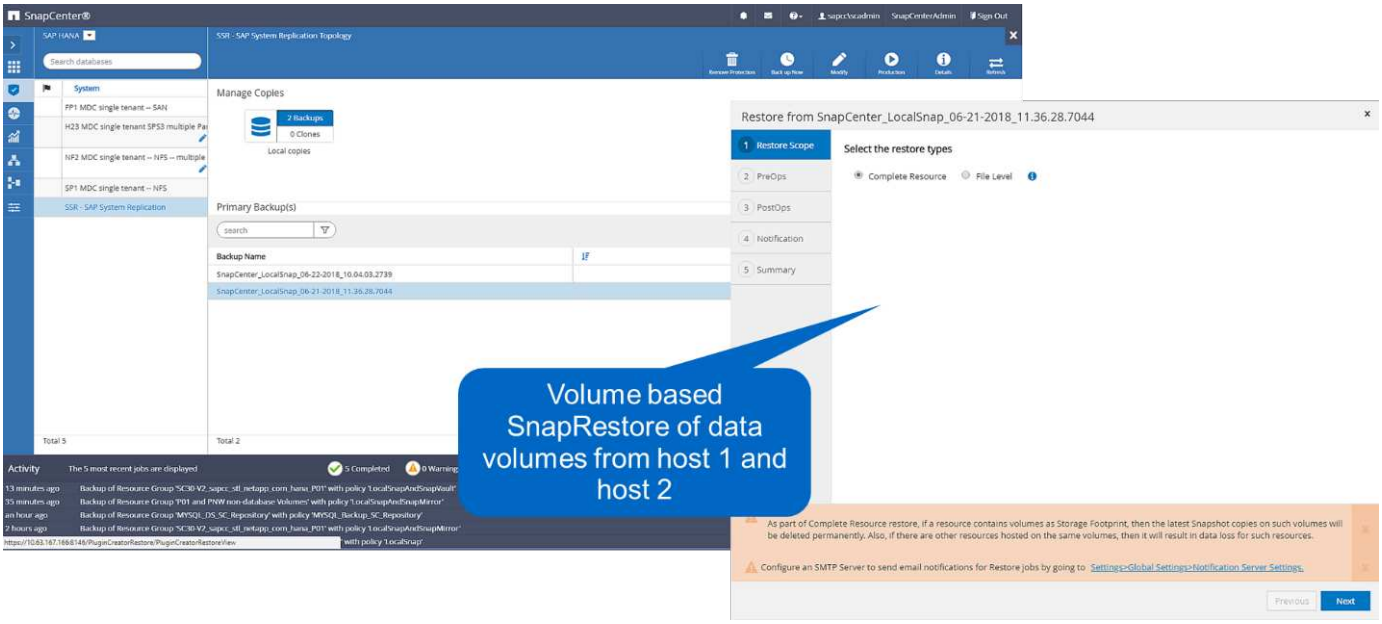
1. A failure occurred and you must restore to the backup created at T1 at host 1.
2. The secondary host (host 2) is shut down and the T1 crash image is restored.
3. The storage volume of host 1 is restored to the backup created at T1.
4. A forward recovery is performed with logs from host 1 and host 2.
5. Host 2 is started and a system replication resynchronization of host 2 is automatically started.



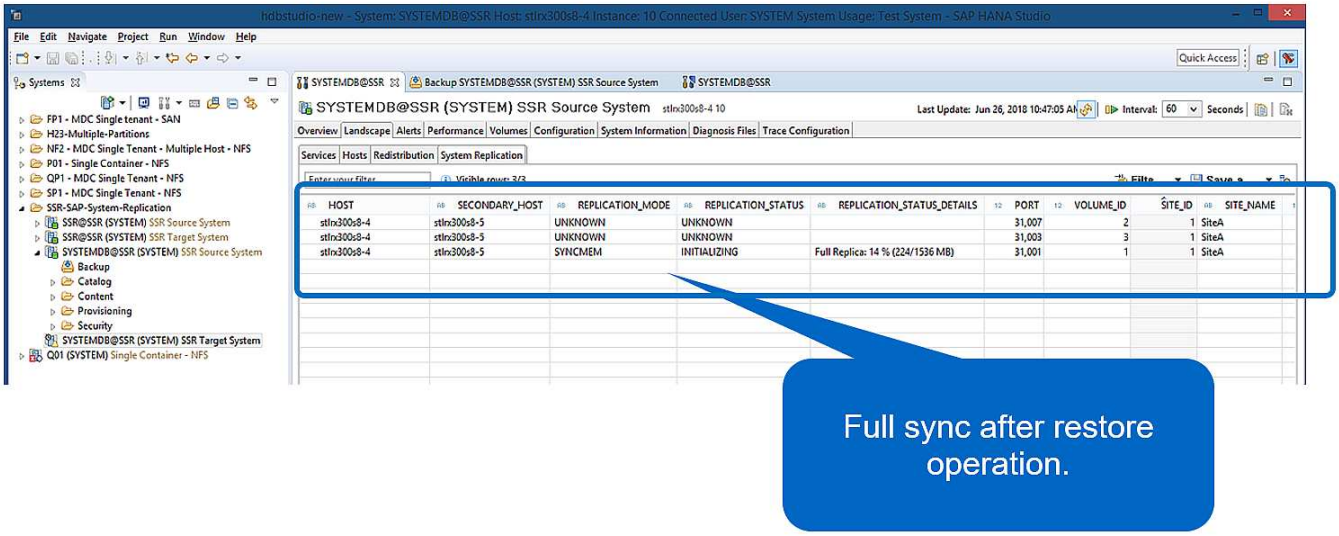
The restore and recovery operation with SAP HANA Studio is identical to the steps described in the section

SnapCenter restore of the valid backup only.

To perform the restore operation, select Complete Resource in SnapCenter. The volumes of both hosts are restored.



After forward recovery has been completed, the secondary host (host 2) is started and SAP HANA System Replication resynchronization is started. Full replication of all data is executed.



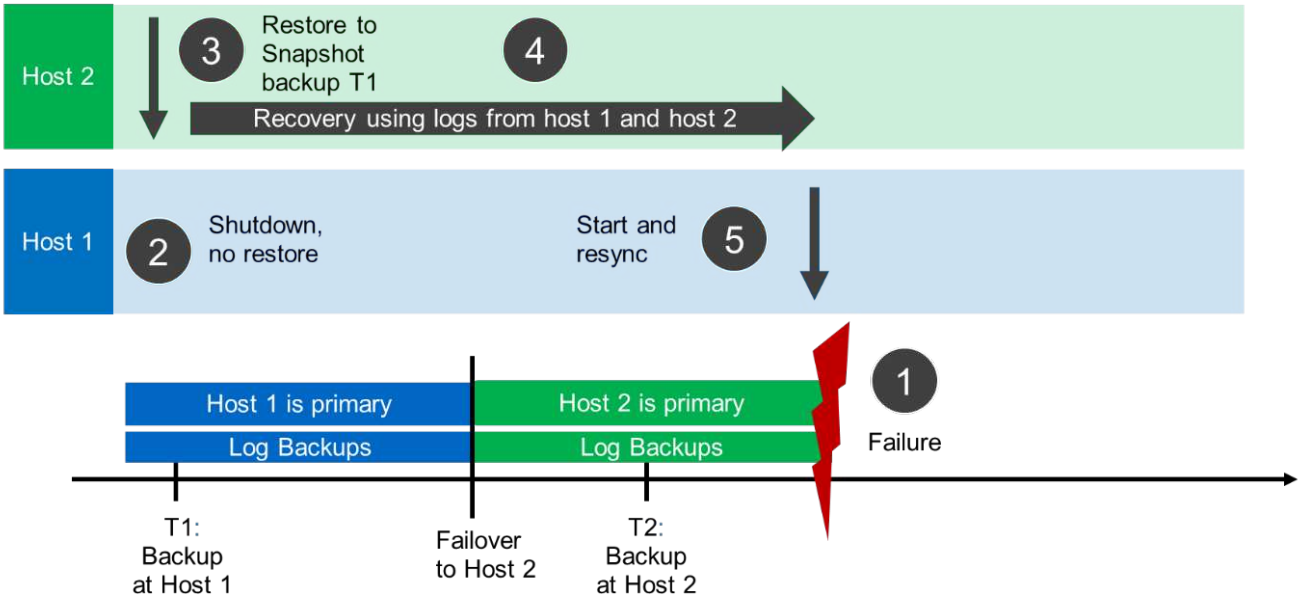
Restore and recovery from a backup created at the other host

A restore operation from a backup that has been created at the other SAP HANA host is a valid scenario for both SnapCenter configuration options.

The following figure shows an overview of the restore and recovery scenario described in this section.

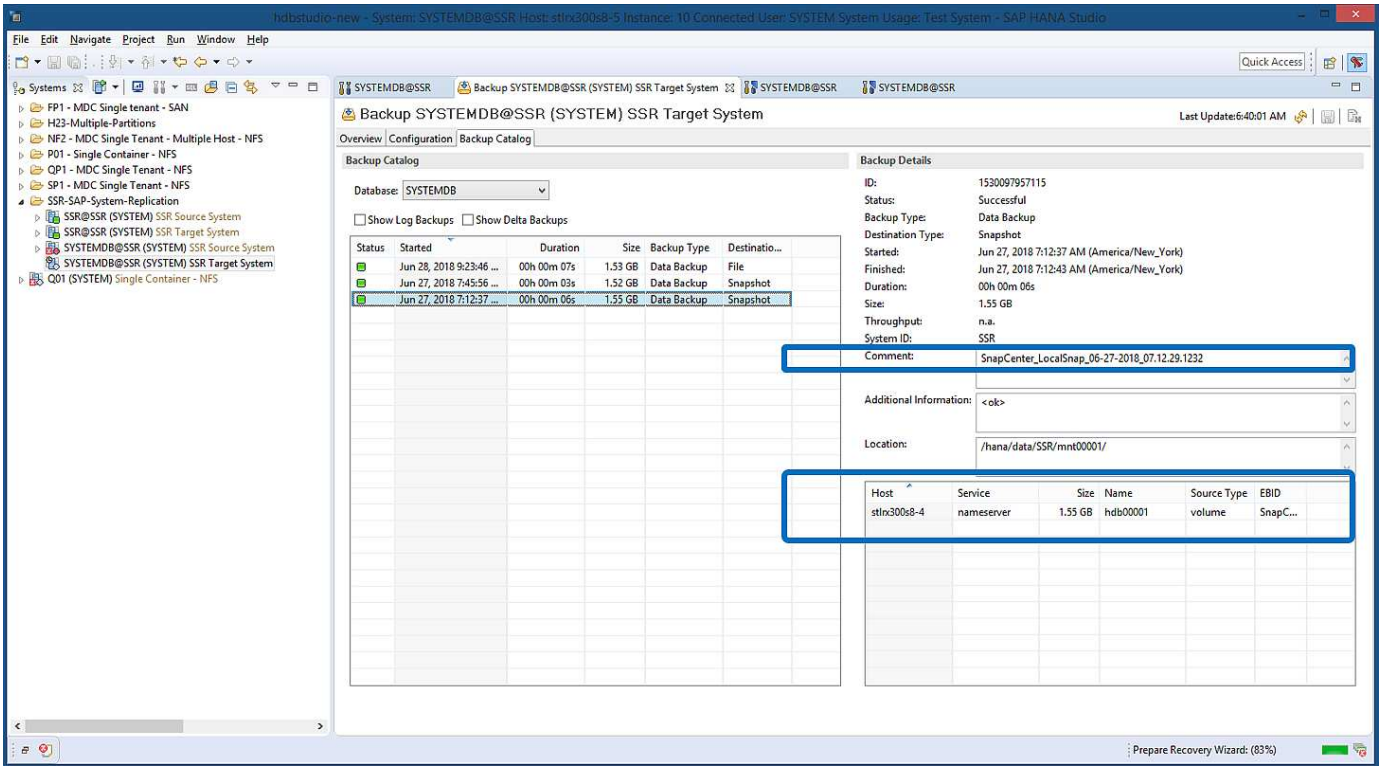
A backup has been created at T1 at host 1. A failover has been performed to host 2. At the current point in time, host 2 is the primary host.

1. A failure occurred and you must restore to the backup created at T1 at host 1.
2. The primary host (host 1) is shut down.
3. The backup data T1 of host 1 is restored to host 2.
4. A forward recovery is performed using logs from host 1 and host 2.
5. Host 1 is started, and a system replication resynchronization of host 1 is automatically started.



31

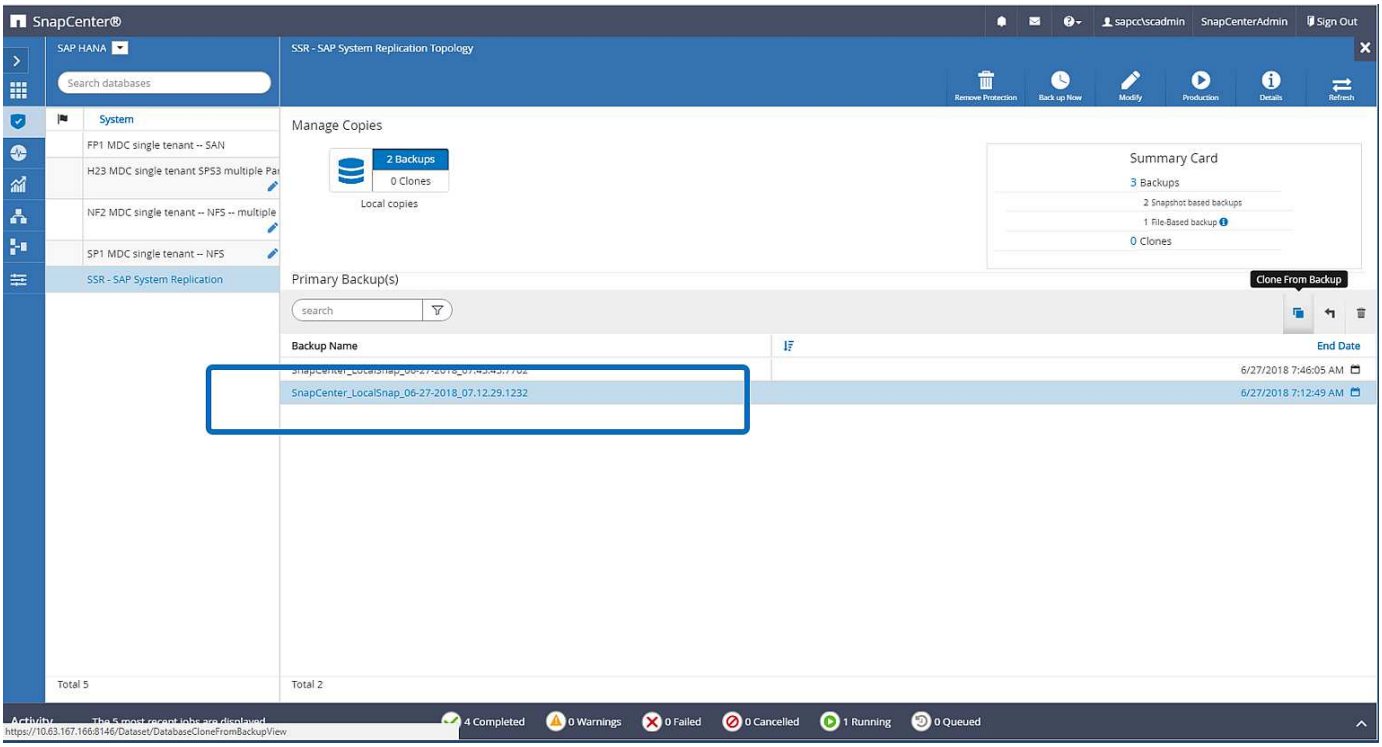
The following figure shows the SAP HANA backup catalog and highlights the backup, created at host 1, that was used for the restore and recovery operation.



The restore operation involves the following steps:

1. Create a clone from the backup created at host 1.
2. Mount the cloned volume at host 2.
3. Copy the data from the cloned volume to the original location.

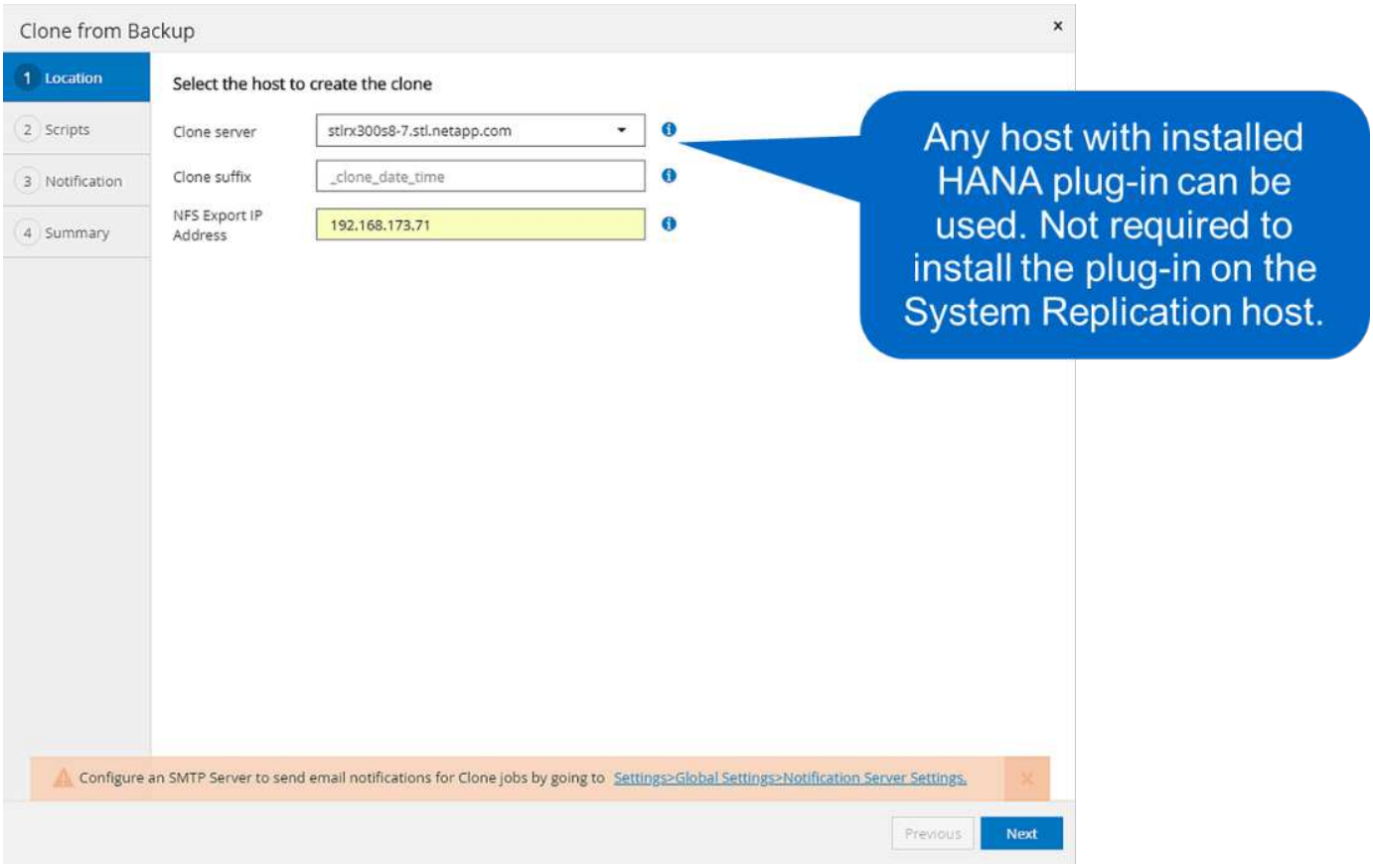
In SnapCenter, the backup is selected and the clone operation is started.



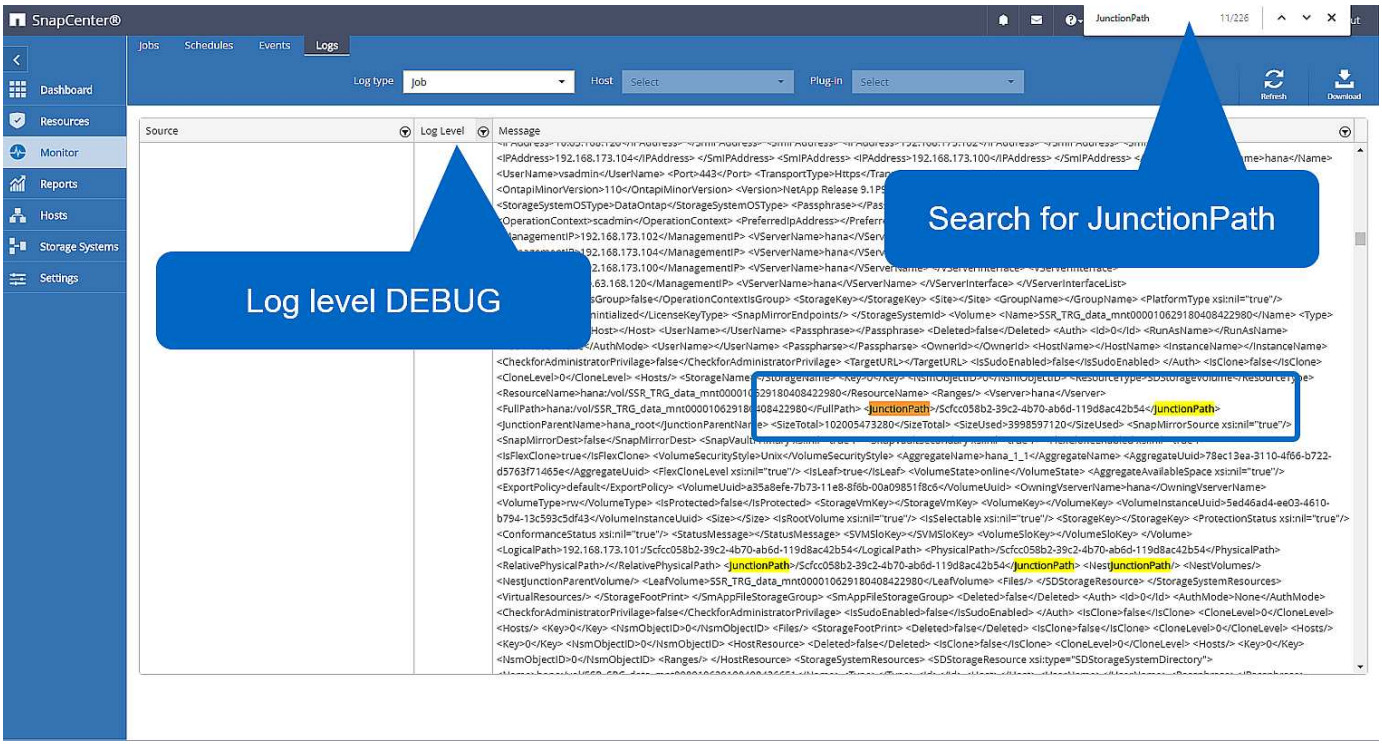
You must provide the clone server and the NFS export IP address.

> In a SnapCenter single-resource configuration, the SAP HANA plug-in is not installed at the database host. To execute the SnapCenter clone workflow, any host with an installed HANA plug-in can be used as a clone server.

+
In a SnapCenter configuration with separate resources, the HANA database host is selected as a clone server, and a mount script is used to mount the clone to the target host.



To determine the junction path that is required to mount the cloned volume, check the job log of the cloning job, as the following figure shows.



The cloned volume can now be mounted.

```
stlrx300s8-5:/mnt/tmp # mount 192.168.173.101:/Scc373da37-00ff-4694-b1e1-
8153dbd46caf /mnt/tmp
```

The cloned volume contains the data of the HANA database.

```
stlrx300s8-5:/mnt/tmp/# ls -al
drwxr-x--x 2 ssradm sapsys 4096 Jun 27 11:12 hdb00001
drwx------ 2 ssradm sapsys 4096 Jun 21 09:38 hdb00002.00003
drwx------ 2 ssradm sapsys 4096 Jun 27 11:12 hdb00003.00003
-rw-r--r-- 1 ssradm sapsys   22 Jun 27 11:12 nameserver.lck
```

The data is copied to the original location.

```
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00001 /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00002.00003/ /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00003.00003/ /hana/data/SSR/mnt00001/
```

The recovery with SAP HANA Studio is performed as described in the section SnapCenter restore of the valid backup only.

Where to find additional information

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

- SAP HANA Backup and Recovery with SnapCenter

  https://www.netapp.com/us/media/tr-4614.pdf

- Automating SAP HANA System Copy and Clone Operations with SnapCenter

  https://docs.netapp.com/us-en/netapp-solutions-sap/lifecycle/sc-copy-clone-introduction.html

- SAP HANA Disaster Recovery with Storage Replication

  https://www.netapp.com/us/media/tr-4646.pdf

SAP HANA Disaster Recovery with Azure NetApp Files

TR-4891: SAP HANA disaster recovery with Azure NetApp Files

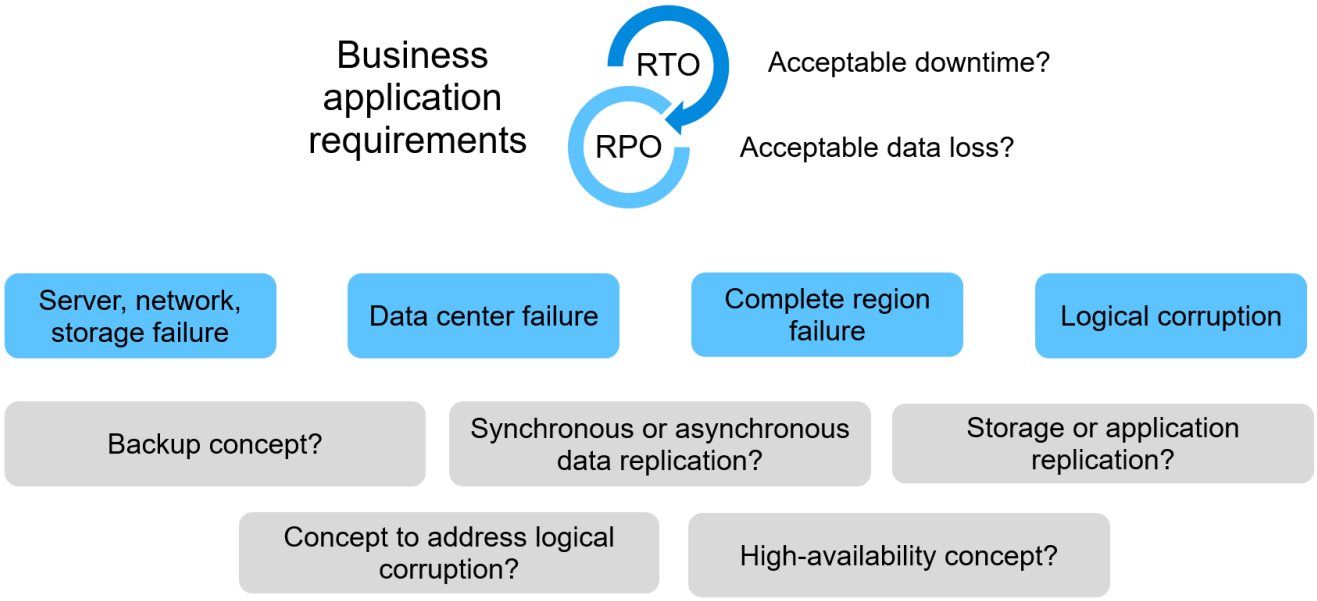
Nils Bauer, NetApp
Ralf Klahr, Microsoft

Studies have shown that business application downtime has a significant negative impact on the business of enterprises. In addition to the financial impact, downtime can also damage the company's reputation, staff

morale, and customer loyalty. Surprisingly, not all companies have a comprehensive disaster recovery policy.

Running SAP HANA on Azure NetApp Files (ANF) gives customers access to additional features that extend and improve the built-in data protection and disaster recovery capabilities of SAP HANA. This overview section explains these options to help customers select options that support their business needs.

To develop a comprehensive disaster recovery policy, customers must understand the business application requirements and technical capabilities they need for data protection and disaster recovery. The following figure provides an overview of data protection.



Business application requirements

There are two key indicators for business applications:

- The recovery point objective (RPO), or the maximum tolerable data loss
- The recovery time objective (RTO), or the maximum tolerable business application downtime

These requirements are defined by the kind of application used and the nature of your business data. The RPO and the RTO might differ if you are protecting against failures at a single Azure region. They might also differ if you are preparing for catastrophic disasters such as the loss of a complete Azure region. It is important to evaluate the business requirements that define the RPO and RTO, because these requirements have a significant impact on the technical options that are available.

High availability

The infrastructure for SAP HANA, such as virtual machines, network, and storage, must have redundant components to make sure that there is no single point of failure. MS Azure provides redundancy for the different infrastructure components.

To provide high availability on the compute and application side, standby SAP HANA hosts can be configured for built-in high availability with an SAP HANA multiple-host system. If a server or an SAP HANA service fails, the SAP HANA service fails over to the standby host, which causes application downtime.

If application downtime is not acceptable in the case of server or application failure, you can also use SAP HANA system replication as a high-availability solution that enables failover in a very short time frame. SAP

customers use HANA system replication not only to address high availability for unplanned failures, but also to minimize downtime for planned operations, such as HANA software upgrades.

Logical corruption

Logical corruption can be caused by software errors, human errors, or sabotage. Unfortunately, logical corruption often cannot be addressed with standard high-availability and disaster recovery solutions. As a result, depending on the layer, application, file system, or storage where the logical corruption occurred, RTO and RPO requirements can sometimes not be fulfilled.

The worst case is a logical corruption in an SAP application. SAP applications often operate in a landscape in which different applications communicate with each other and exchange data. Therefore, restoring and recovering an SAP system in which a logical corruption has occurred is not the recommended approach. Restoring the system to a point in time before the corruption occurred results in data loss, so the RPO becomes larger than zero. Also, the SAP landscape would no longer be in sync and would require additional postprocessing.

Instead of restoring the SAP system, the better approach is to try to fix the logical error within the system, by analyzing the problem in a separate repair system. Root cause analysis requires the involvement of the business process and application owner. For this scenario, you create a repair system (a clone of the production system) based on data stored before the logical corruption occurred. Within the repair system, the required data can be exported and imported to the production system. With this approach, the productive system does not need to be stopped, and, in the best-case scenario, no data or only a small fraction of data is lost.

The required steps to setup a repair system are identical to a disaster recovery testing scenario described in this document. The described disaster recovery solution can therefore easily be extended to address logical corruption as well.

Backups

Backups are created to enable restore and recovery from different point-in-time datasets. Typically, these backups are kept for a couple of days to a few weeks.

Depending on the kind of corruption, restore and recovery can be performed with or without data loss. If the RPO must be zero, even when the primary and backup storage is lost, backup must be combined with synchronous data replication.

The RTO for restore and recovery is defined by the required restore time, the recovery time (including database start), and the loading of data into memory. For large databases and traditional backup approaches, the RTO can easily be several hours, which might not be acceptable. To achieve very low RTO values, a backup must be combined with a hot-standby solution, which includes preloading data into memory.

In contrast, a backup solution must address logical corruption, because data replication solutions cannot cover all kinds of logical corruption.

Synchronous or asynchronous data replication

The RPO primarily determines which data replication method you should use. If the RPO must be zero, even when the primary and backup storage is lost, the data must be replicated synchronously. However, there are technical limitations for synchronous replication, such as the distance between two Azure regions. In most cases, synchronous replication is not appropriate for distances greater than 100km due to latency, and therefore this is not an option for data replication between Azure regions.

If a larger RPO is acceptable, asynchronous replication can be used over large distances. The RPO in this case is defined by the replication frequency.

HANA system replication with or without data preload

The startup time for an SAP HANA database is much longer than that of traditional databases because a large amount of data must be loaded into memory before the database can provide the expected performance. Therefore, a significant part of the RTO is the time needed to start the database. With any storage-based replication as well as with HANA System Replication without data preload, the SAP HANA database must be started in case of failover to the disaster recovery site.

SAP HANA system replication offers an operation mode in which the data is preloaded and continuously updated at the secondary host. This mode enables very low RTO values, but it also requires a dedicated server that is only used to receive the replication data from the source system.

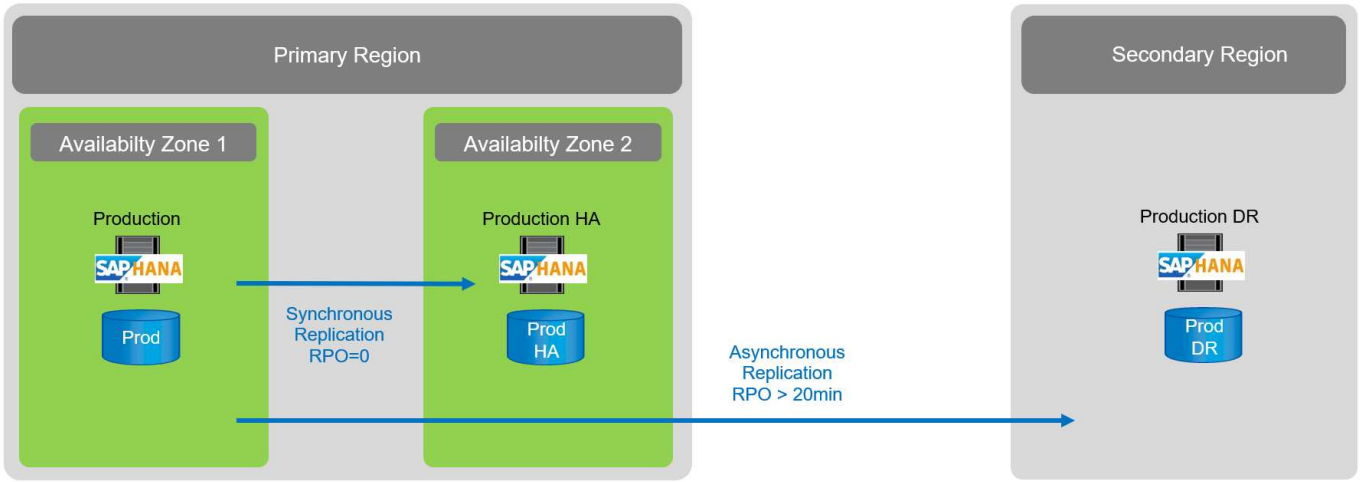
Disaster recovery solution comparison

A comprehensive disaster recovery solution must enable customers to recover from a complete failure of the primary site. Therefore, data must be transferred to a secondary site, and a complete infrastructure is necessary to run the required production SAP HANA systems in case of a site failure. Depending on the availability requirements of the application and the kind of disaster you want to be protected from, a two-site or three-site disaster recovery solution must be considered.

The following figure shows a typical configuration in which the data is replicated synchronously within the same Azure region into a second availability zone. The short distance allows you to replicate the data synchronously to achieve an RPO of zero (typically used to provide HA).

In addition, data is also replicated asynchronously to a secondary region to be protected from disasters, when the primary region is affected. The minimum achievable RPO depends on the data replication frequency, which is limited by the available bandwidth between the primary and the secondary region. A typical minimal RPO is in the range of 20 minutes to multiple hours.

This document discusses different implementation options of a two- region disaster recovery solution.



SAP HANA System Replication

SAP HANA System Replication works at the database layer. The solution is based on an additional SAP HANA system at the disaster recovery site that receives the changes from the primary system. This secondary system must be identical to the primary system.

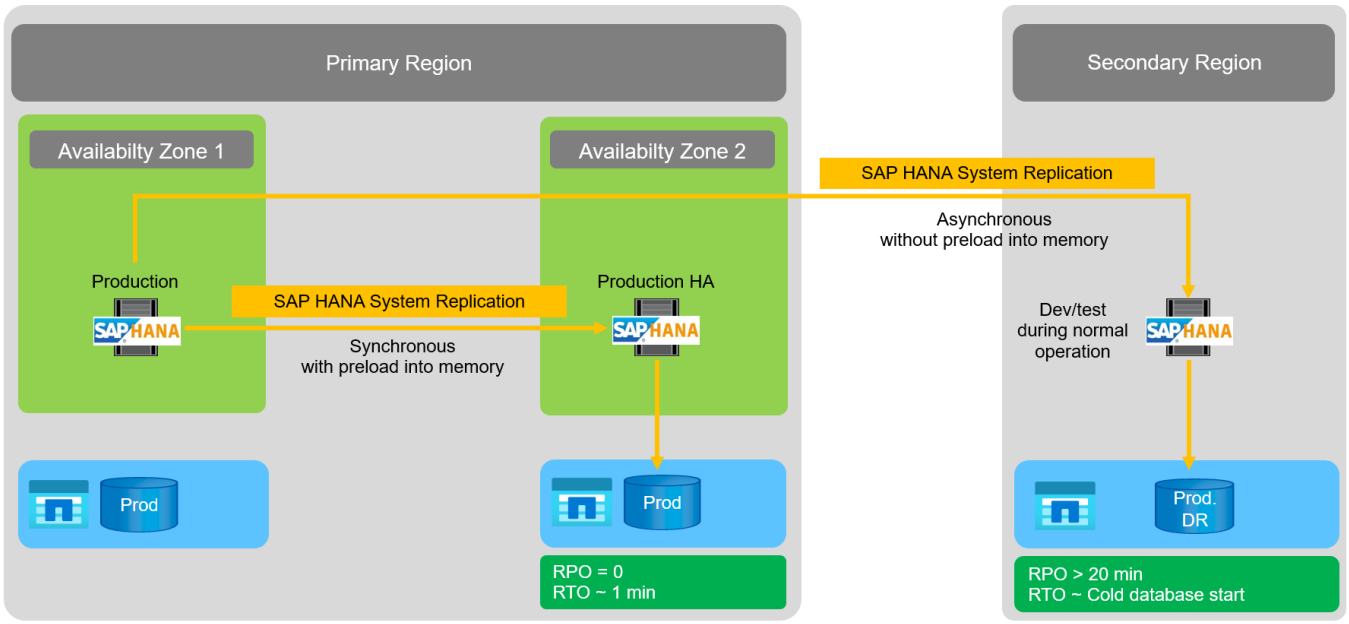
SAP HANA System Replication can be operated in one of two modes:

- With data preloaded into memory and a dedicated server at the disaster recovery site:
  - The server is used exclusively as an SAP HANA System Replication secondary host.
  - Very low RTO values can be achieved because the data is already loaded into memory and no database start is required in case of a failover.
- Without data preloaded into memory and a shared server at the disaster recovery site:
  - The server is shared as an SAP HANA System Replication secondary and as a dev/test system.
  - RTO depends mainly on the time required to start the database and load the data into memory.

For a full description of all configuration options and replication scenarios, see the SAP HANA Administration Guide.

The following figure shows the setup of a two-region disaster recovery solution with SAP HANA System Replication. Synchronous replication with data preloaded into memory is used for local HA in the same Azure region, but in different availability zones. Asynchronous replication without data preloaded is configured for the remote disaster recovery region.

The following figure depicts SAP HANA System Replication.



SAP HANA System Replication with data preloaded into memory

Very low RTO values with SAP HANA can be achieved only with SAP HANA System Replication with data preloaded into memory. Operating SAP HANA System Replication with a dedicated secondary server at the disaster recovery site allows an RTO value of approximately 1 minute or less. The replicated data is received and preloaded into memory at the secondary system. Because of this low failover time, SAP HANA System Replication is also often used for near-zero-downtime maintenance operations, such as HANA software

upgrades.

Typically, SAP HANA System Replication is configured to replicate synchronously when data preload is chosen. The maximum supported distance for synchronous replication is in the range of 100km.

SAP System Replication without data preloaded into memory

For less stringent RTO requirements, you can use SAP HANA System Replication without data preloaded. In this operational mode, the data at the disaster recovery region is not loaded into memory. The server at the DR region is still used to process SAP HANA System Replication running all the required SAP HANA processes. However, most of the server's memory is available to run other services, such as SAP HANA dev/test systems.

In the event of a disaster, the dev/test system must be shut down, failover must be initiated, and the data must be loaded into memory. The RTO of this cold standby approach depends on the size of the database and the read throughput during the load of the row and column store. With the assumption that the data is read with a throughput of 1000MBps, loading 1TB of data should take approximately 18 minutes.

SAP HANA disaster recovery with ANF Cross-Region Replication

ANF Cross-Region Replication is built into ANF as a disaster recovery solution using asynchronous data replication. ANF Cross-Region Replication is configured through a data protection relationship between two ANF volumes on a primary and a secondary Azure region. ANF Cross-Region Replication updates the secondary volume by using efficient block delta replications. Update schedules can be defined during the replication configuration.

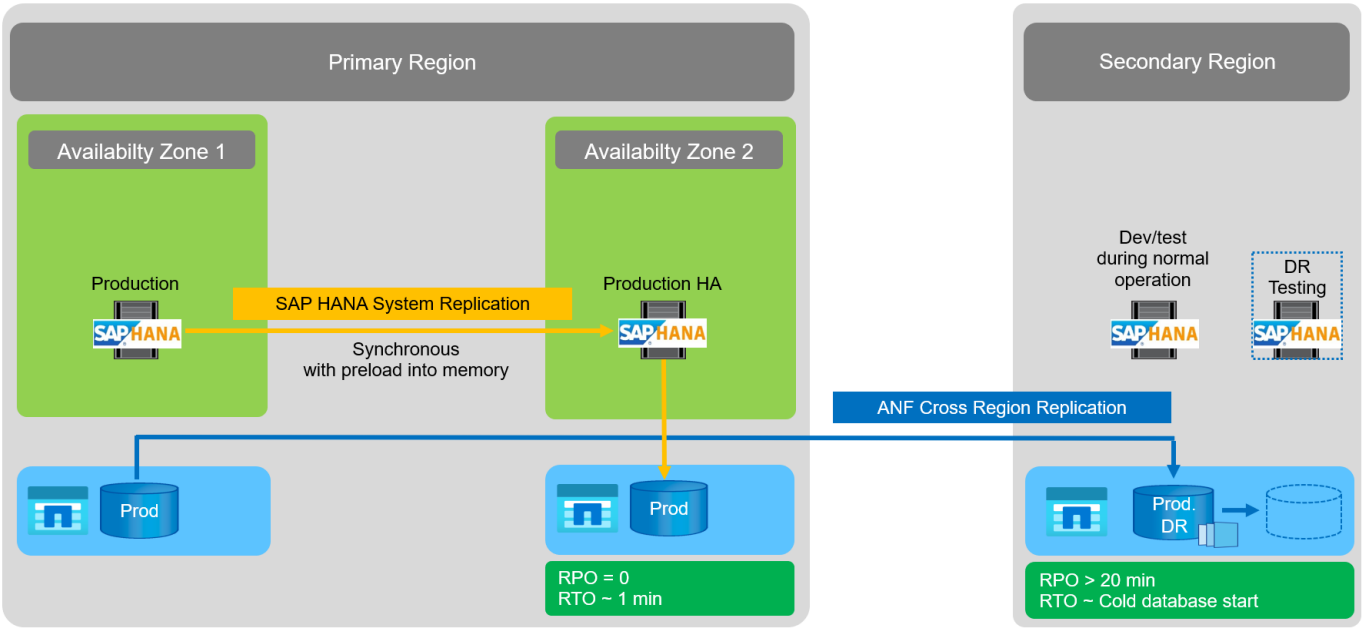
The following figure shows a two- region disaster recovery solution example, using ANF Cross- Region Replication. In this example the HANA system is protected with HANA System Replication within the primary region as discussed in the previous chapter. The replication to a secondary region is performed using ANF cross region replication. The RPO is defined by the replication schedule and replication options.

The RTO depends mainly on the time needed to start the HANA database at the disaster recovery site and to load the data into memory. With the assumption that the data is read with a throughput of 1000MB/s, loading 1TB of data would take approximately 18 minutes. Depending on the replication configuration, forward recovery is required as well and will add to the total RTO value.

More details on the different configuration options are provided in chapter Configuration options for cross region replication with SAP HANA.

The servers at the disaster recovery sites can be used as dev/test systems during normal operation. In case of a disaster, the dev/test systems must be shut down and started as DR production servers.

ANF Cross-Region Replication allows you to test the DR workflow without impacting the RPO and RTO. This is accomplished by creating volume clones and attaching them to the DR testing server.



Summary of disaster recovery solutions

The following table compares the disaster recovery solutions discussed in this section and highlights the most important indicators.

The key findings are as follows:

- If a very low RTO is required, SAP HANA System Replication with preload into memory is the only option.
  - A dedicated server is required at the DR site to receive the replicated data and load the data into memory.
- In addition, storage replication is needed for the data that resides outside of the database (for example shared files, interfaces, and so on).
- If RTO/RPO requirements are less strict, ANF Cross-Region Replication can also be used to:
  - Combine database and nondatabase data replication.
  - Cover additional use cases such as disaster recovery testing and dev/test refresh.
  - With storage replication the server at the DR site can be used as a QA or test system during normal operation.
- A combination of SAP HANA System Replication as an HA solution with RPO=0 with storage replication for long distance makes sense to address the different requirements.

The following table provides a comparison of disaster recovery solutions.

	Storage replication	SAP HANA system replication	
	Cross-region replication	**With data preload**	**Without data preload**
RTO	Low to medium, depending on database startup time and forward recovery	Very low	Low to medium, depending on database startup time

	Storage replication	SAP HANA system replication	
RPO	RPO > 20min asynchronous replication	RPO > 20min asynchronous replication RPO=0 synchronous replication	RPO > 20min asynchronous replication RPO=0 synchronous replication
Servers at DR site can be used for dev/test	Yes	No	Yes
Replication of nondatabase data	Yes	No	No
DR data can be used for refresh of dev/test systems	Yes	No	No
DR testing without affecting RTO and RPO	Yes	No	No

ANF Cross-Region Replication with SAP HANA

ANF Cross-Region Replication with SAP HANA

Application agnostic information on Cross-Region Replication can be found at Azure NetApp Files documentation | Microsoft Docs in the concepts and how- to guide sections.

Configuration options for Cross-Region Replication with SAP HANA

The following figure shows the volume replication relationships for an SAP HANA system using ANF Cross-Region Replication. With ANF Cross-Region Replication, the HANA data and the HANA shared volume must be replicated. If only the HANA data volume is replicated, typical RPO values are in the range of one day. If lower RPO values are required, the HANA log backups must be also replicated for forward recovery.

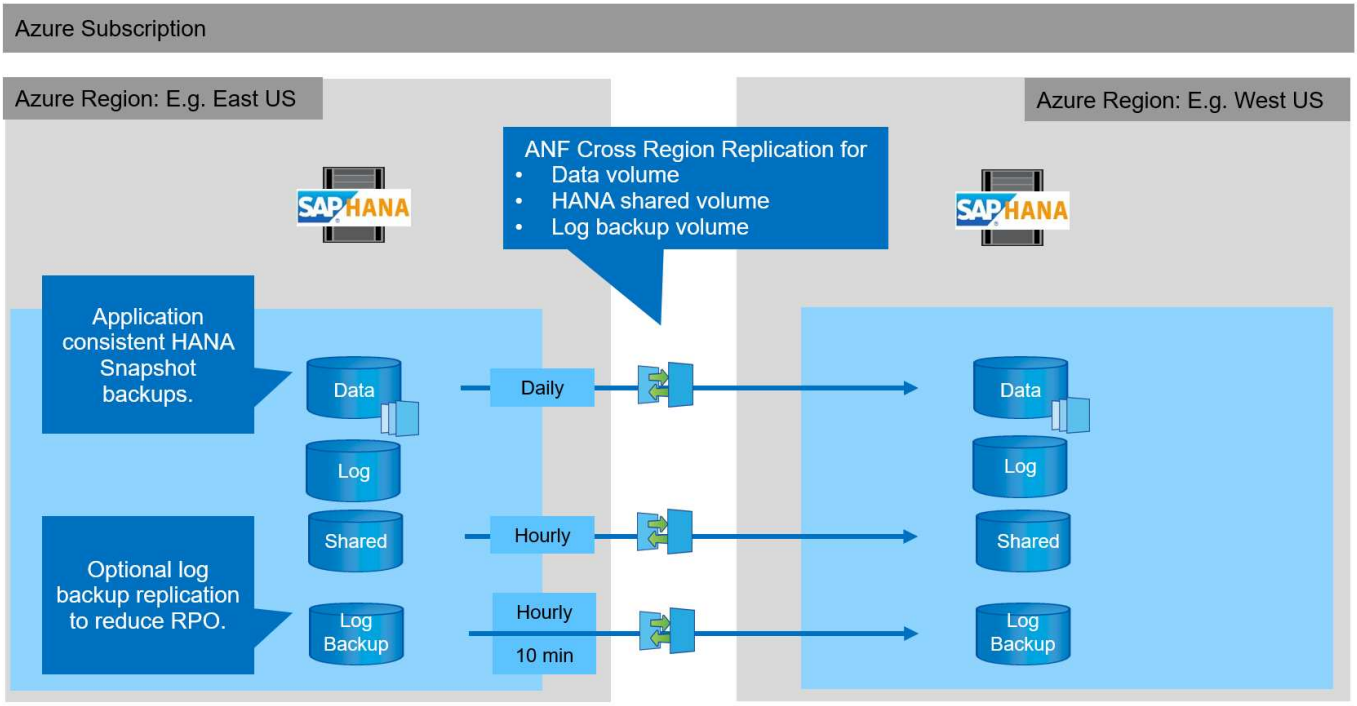
ⓘ The term “log backup” used in this document includes the log backup and the HANA backup catalog backup. The HANA backup catalog is required to execute forward recovery operations.

ⓘ The following description and the lab setup focus on the HANA database. Other shared files, for example the SAP transport directory would be protected and replicated in the same way as the HANA shared volume.

To enable HANA save-point recovery or forward recovery using the log backups, application-consistent data Snapshot backups must be created at the primary site for the HANA data volume. This can be done for example with the ANF backup tool AzAcSnap (see also What is Azure Application Consistent Snapshot tool for Azure NetApp Files | Microsoft Docs). The Snapshot backups created at the primary site are then replicated to the DR site.

In the case of a disaster failover, the replication relationship must be broken, the volumes must be mounted to the DR production server, and the HANA database must be recovered, either to the last HANA save point or with forward recovery using the replicated log backups. The chapter Disaster recovery failover, describes the required steps.

The following figure depicts the HANA configuration options for cross-region replication.



With the current version of Cross-Region Replication, only fixed schedules can be selected, and the actual replication update time cannot be defined by the user. Available schedules are daily, hourly and every 10 minutes. Using these schedule options, two different configurations make sense depending on the RPO requirements: data volume replication without log backup replication and log backup replication with different schedules, either hourly or every 10 minutes. The lowest achievable RPO is around 20 minutes. The following table summarizes the configuration options and the resulting RPO and RTO values.

	Data volume replication	Data and log backup volume replication	Data and log backup volume replication
CRR schedule data volume	Daily	Daily	Daily
CRR schedule log backup volume	n/a	Hourly	10 min
Max RPO	24 hours + Snapshot schedule (e.g., 6 hours)	1 hour	2 x 10 min
Max RTO	Primarily defined by HANA startup time	HANA startup time + recovery time	HANA startup time + recovery time
Forward recovery	NA	Logs for the last 24 hours + Snapshot schedule (e.g., 6 hours)	Logs for the last 24 hours + Snapshot schedule (e.g., 6 hours)

Requirements and best practices

Microsoft Azure does not guarantee the availability of a specific virtual machine (VM) type upon creation or when starting a deallocated VM. Specifically, in case of a region failure, many clients might require additional VMs at the disaster recovery region. It is therefore

recommended to actively use a VM with the required size for disaster failover as a test or QA system at the disaster recovery region to have the required VM type allocated.

For cost optimization it makes sense to use an ANF capacity pool with a lower performance tier during normal operation. The data replication does not require high performance and could therefore use a capacity pool with a standard performance tier. For disaster recovery testing, or if a disaster failover is required, the volumes must be moved to a capacity pool with a high-performance tier.

If a second capacity pool is not an option, the replication target volumes should be configured based on capacity requirements and not on performance requirements during normal operations. The quota or the throughput (for manual QoS) can then be adapted for disaster recovery testing in the case of disaster failover.

Further information can be found at Requirements and considerations for using Azure NetApp Files volume cross-region replication | Microsoft Docs.

Lab setup

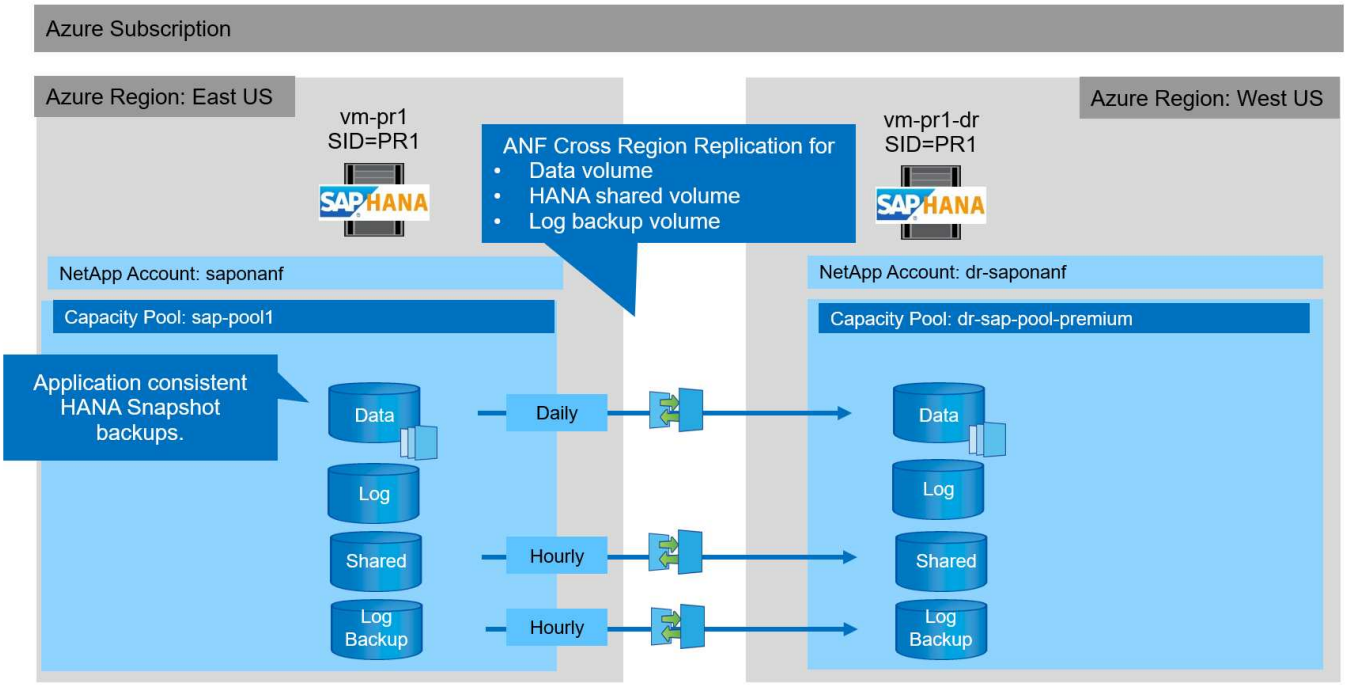
Solution validation has been performed with an SAP HANA single-host system. The Microsoft AzAcSnap Snapshot backup tool for ANF has been used to configure HANA application-consistent Snapshot backups. A daily data volume, hourly log backup, and shared volume replication were all configured. Disaster recover testing and failover was validated with a save point as well as with forward recovery operations.

The following software versions have been used in the lab setup:

- Single host SAP HANA 2.0 SPS5 system with a single tenant
- SUSE SLES for SAP 15 SP1
- AzAcSnap 5.0

A single capacity pool with manual QoS has been configured at the DR site.

The following figure depicts the lab setup.

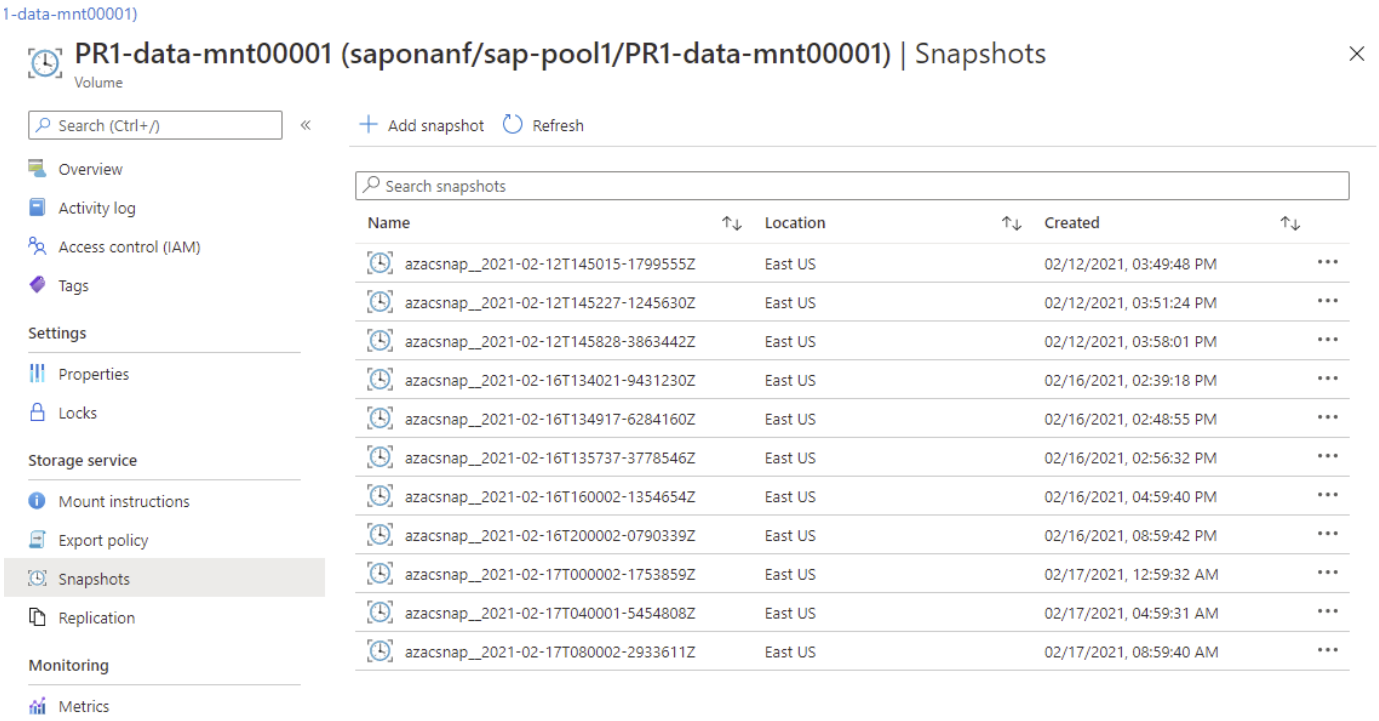


Snapshot backup configuration with AzAcSnap

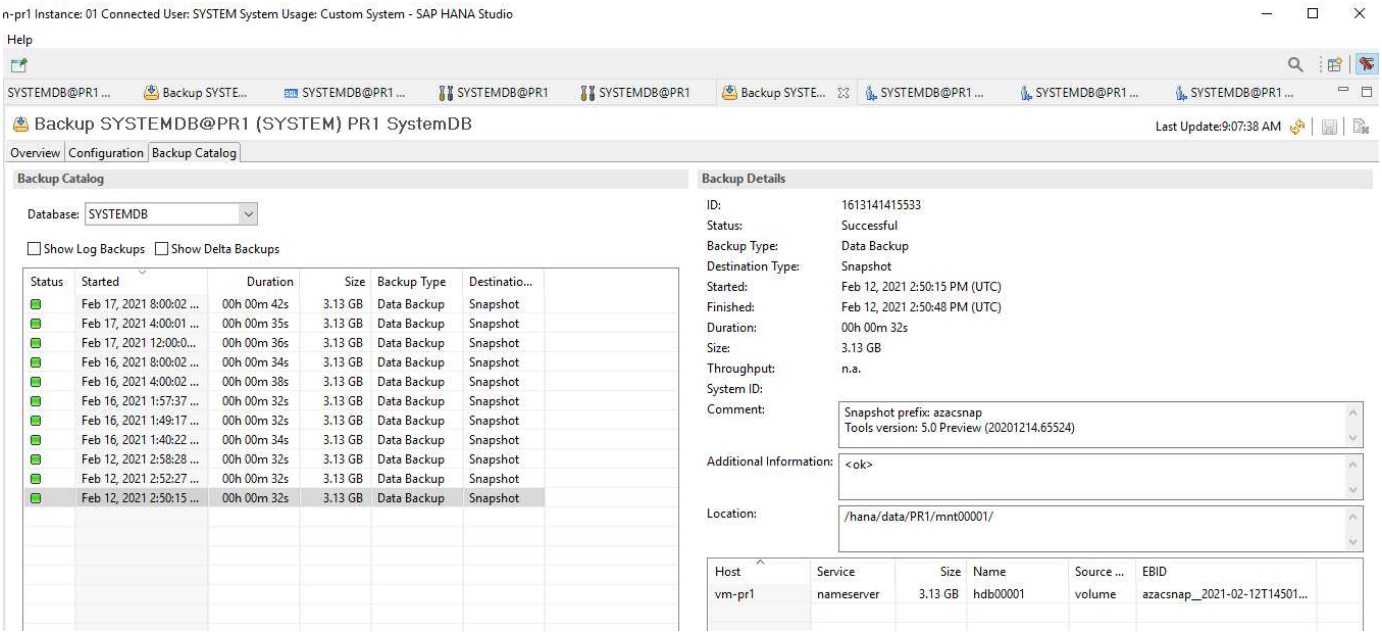
At the primary site, AzAcSnap was configured to create application-consistent Snapshot backups of the HANA system PR1. These Snapshot backups are available at the ANF data volume of the PR1 HANA system, and they are also registered in the SAP HANA backup catalog, as shown in the following two figures. Snapshot backups were scheduled for every 4 hours.

With the replication of the data volume using ANF Cross-Region Replication, these Snapshot backups are replicated to the disaster recovery site and can be used to recover the HANA database.

The following figure shows the Snapshot backups of the HANA data volume.



The following figure shows the SAP HANA backup catalog.



Configuration steps for ANF Cross-Region Replication

A few preparation steps must be performed at the disaster recovery site before volume replication can be configured.

- A NetApp account must be available and configured with the same Azure subscription as the source.
- A capacity pool must be available and configured using the above NetApp account.
- A virtual network must be available and configured.
- Within the virtual network, a delegated subnet must be available and configured for use with ANF.

Protection volumes can now be created for the HANA data, the HANA shared and the HANA log backup volume. The following table shows the configured destination volumes in our lab setup.

> To achieve the best latency, the volumes must be placed close to the VMs that run the SAP HANA in case of a disaster failover. Therefore, the same pinning process is required for the DR volumes as for any other SAP HANA production system.

HANA volume	Source	Destination	Replication schedule
HANA data volume	PR1-data-mnt00001	PR1-data-mnt00001-sm-dest	Daily
HANA shared volume	PR1-shared	PR1-shared-sm-dest	Hourly
HANA log/catalog backup volume	hanabackup	hanabackup-sm-dest	Hourly

For each volume, the following steps must be performed:

1. Create a new protection volume at the DR site:
    a. Provide the volume name, capacity pool, quota, and network information.

b. Provide the protocol and volume access information.
c. Provide the source volume ID and a replication schedule.
d. Create a target volume.

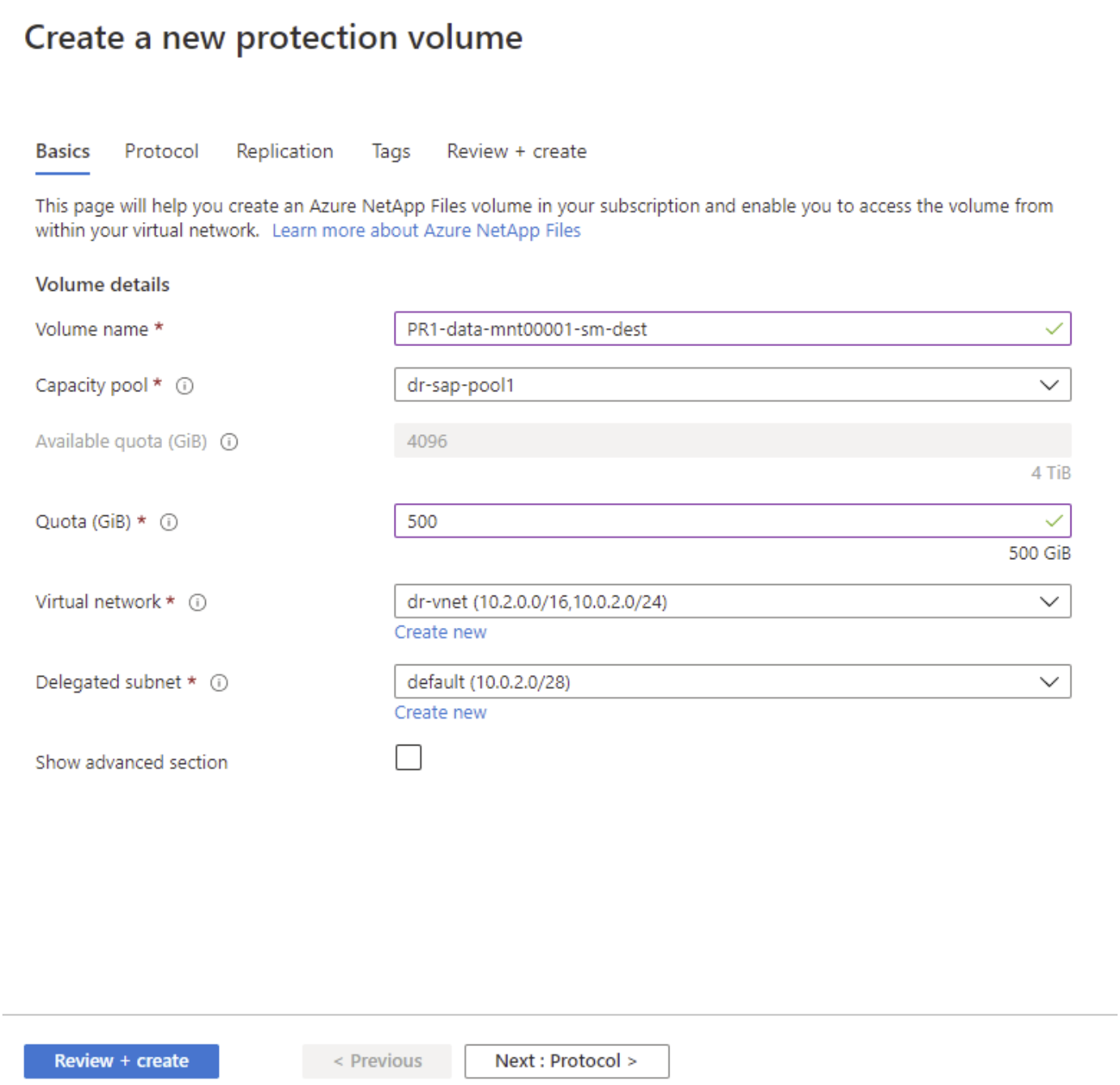
2. Authorize replication at the source volume.
    - Provide the target volume ID.

The following screenshots show the configuration steps in detail.

At the disaster recovery site, a new protection volume is created by selecting volumes and clicking Add Data Replication. Within the Basics tab, you must provide the volume name, capacity pool and network information.

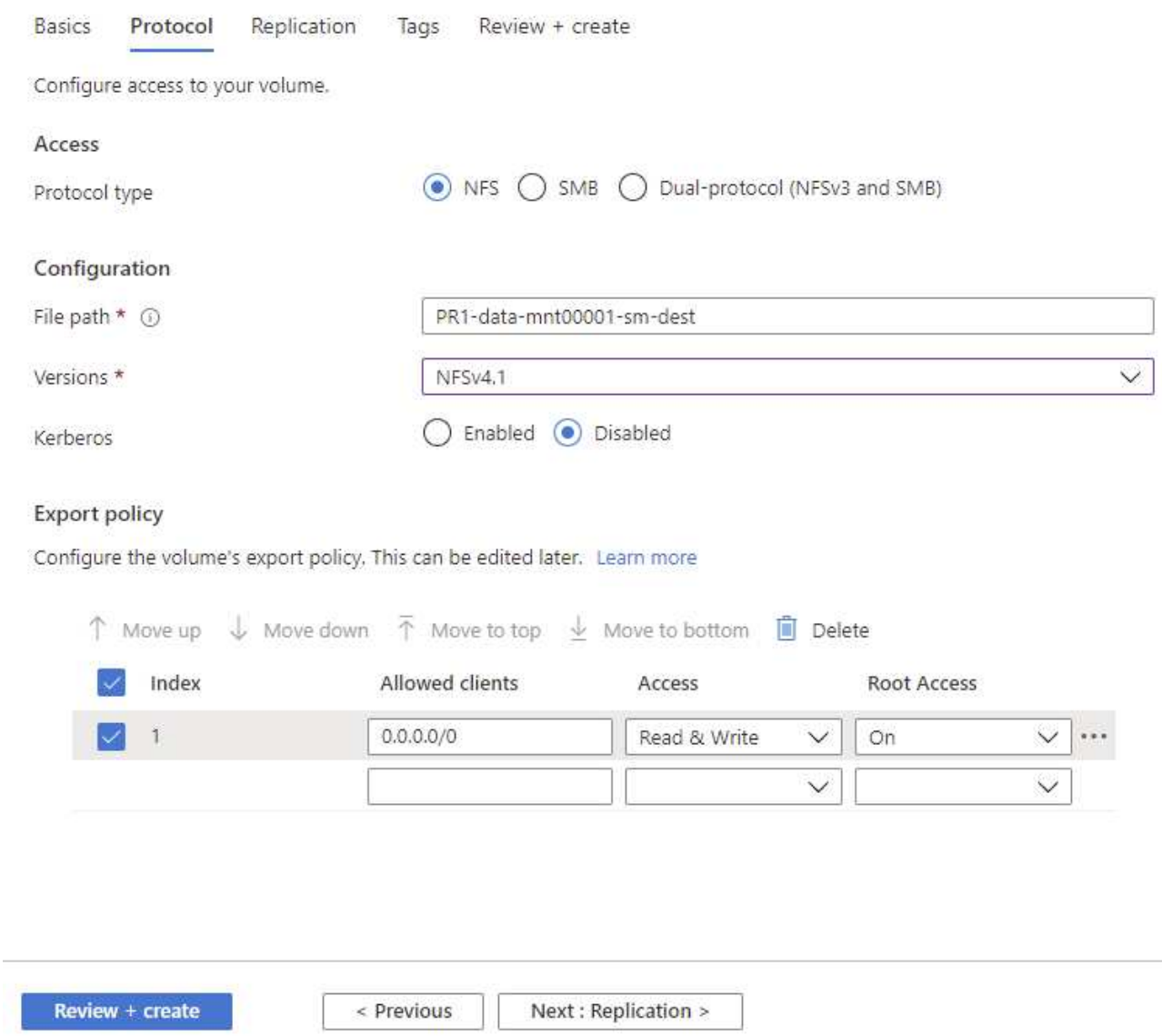
The quota of the volume can be set based on capacity requirements, because volume performance does not have an effect on the replication process. In the case of a disaster recovery failover, the quota must be adjusted to fulfill the real performance requirements.

If the capacity pool has been configured with manual QoS, you can configure the throughput in addition to the capacity requirements. Same as above, you can configure the throughput with a low value during normal operation and increase it in case of a disaster recovery failover.



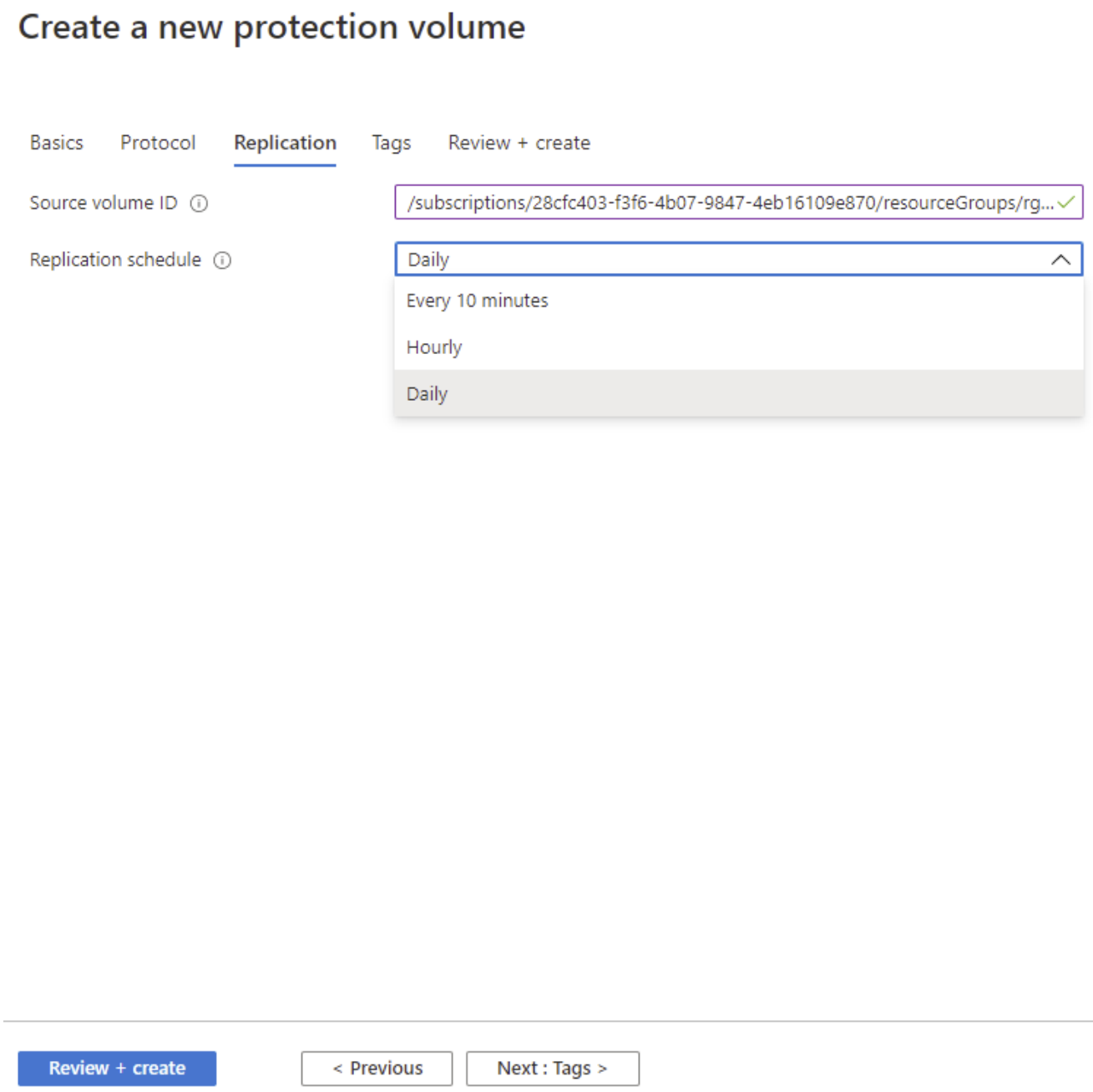
In the Protocol tab, you must provide the network protocol, the network path, and the export policy.

The protocol must be the same as the protocol used for the source volume.



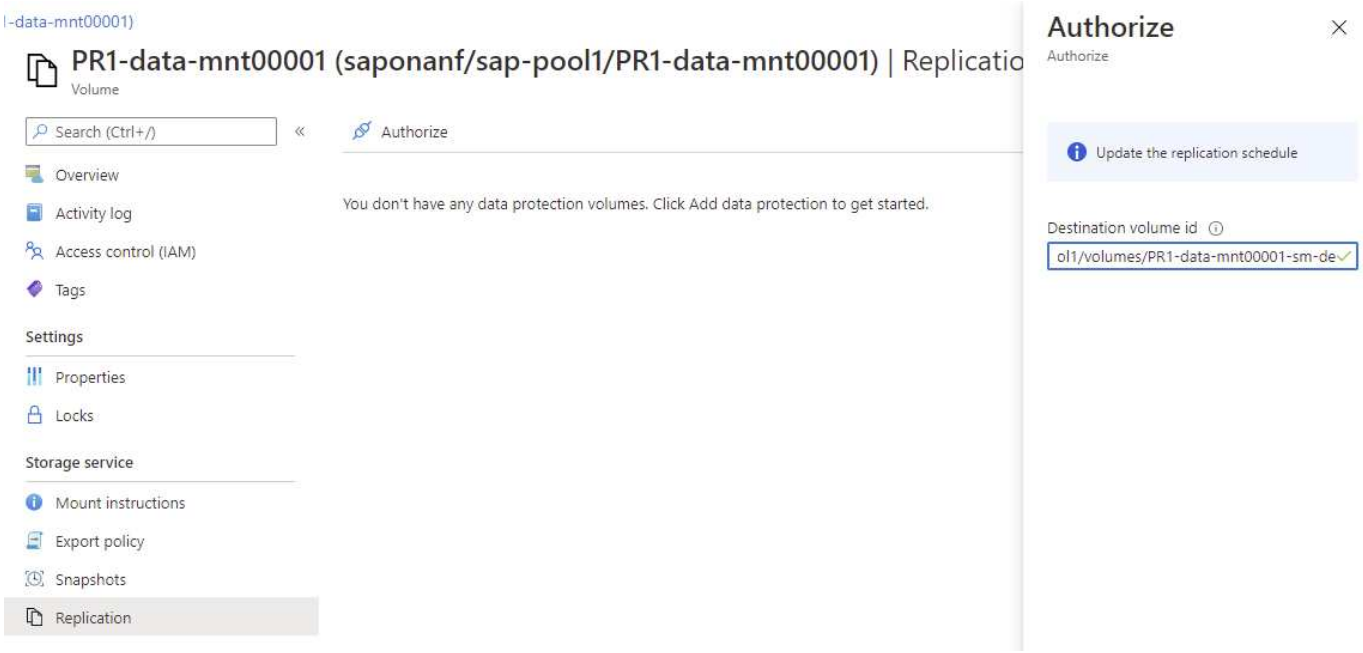
Within the Replication tab, you must configure the source volume ID and the replication schedule. For data volume replication, we configured a daily replication schedule for our lab setup.

The source volume ID can be copied from the Properties screen of the source volume.



As a final step, you must authorize replication at the source volume by providing the ID of the target volume.

You can copy the destination volume ID from the Properties screen of the destination volume.



The same steps must be performed for the HANA shared and the log backup volume.

Monitoring ANF Cross-Region Replication

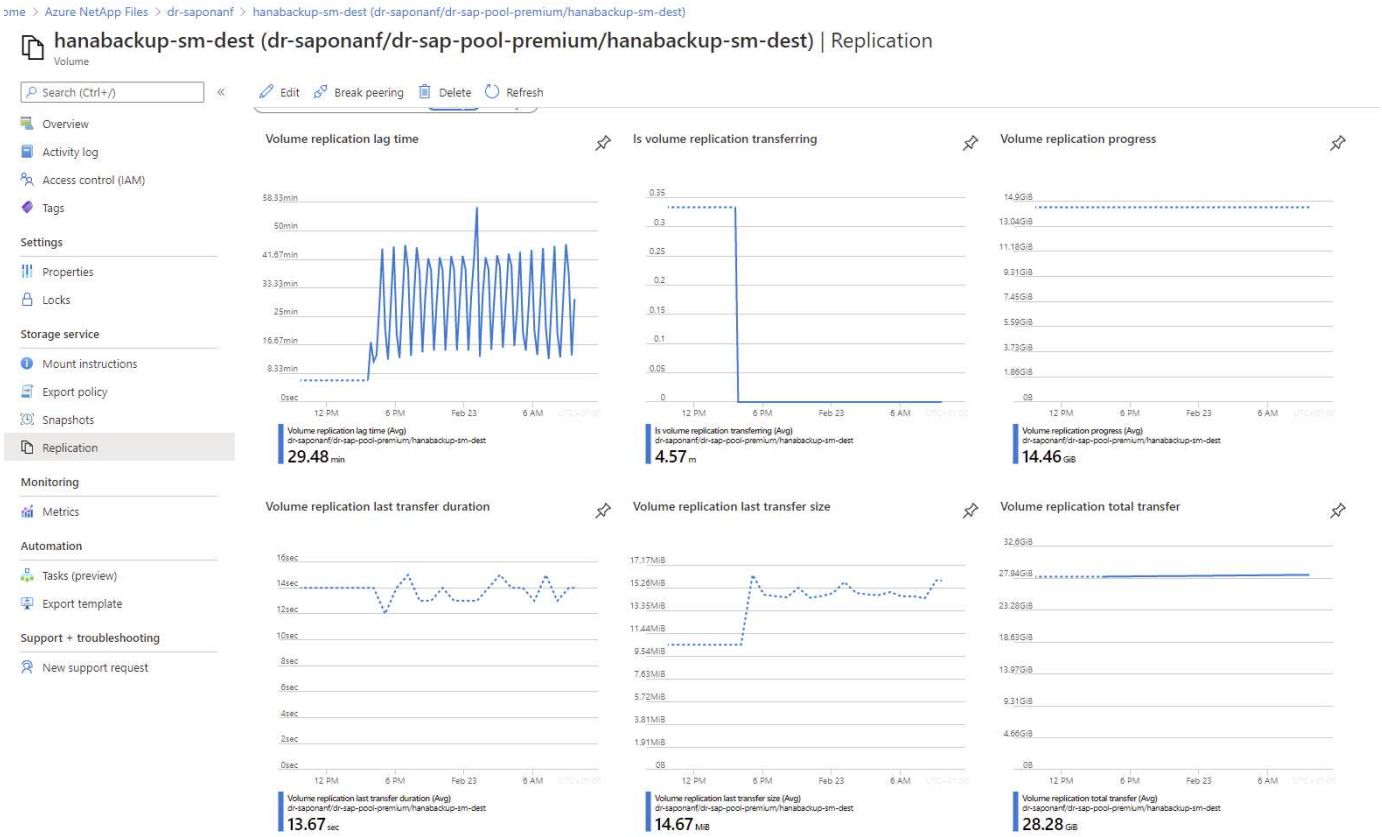
The following three screenshots show the replication status for the data, log backup, and shared volumes.

The volume replication lag time is a useful value to understand RPO expectations. For example, the log backup volume replication shows a maximum lag time of 58 minutes, which means that the maximum RPO has the same value.

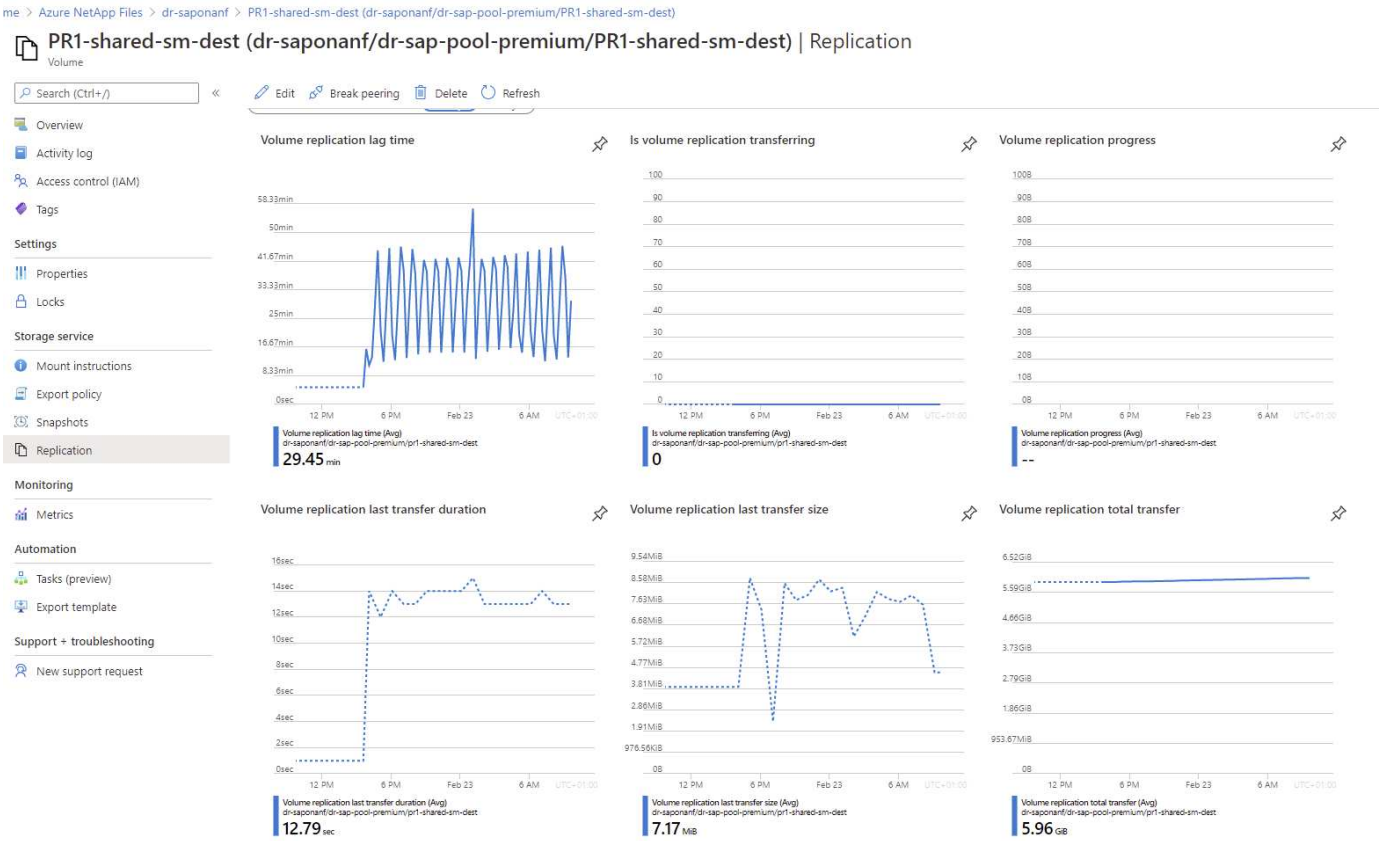
The transfer duration and transfer size provide valuable information on bandwidth requirements and change the rate of the replicated volume.

The following screenshot shows the replication status of HANA data volume.

The following screenshot shows the replication status of HANA log backup volume.



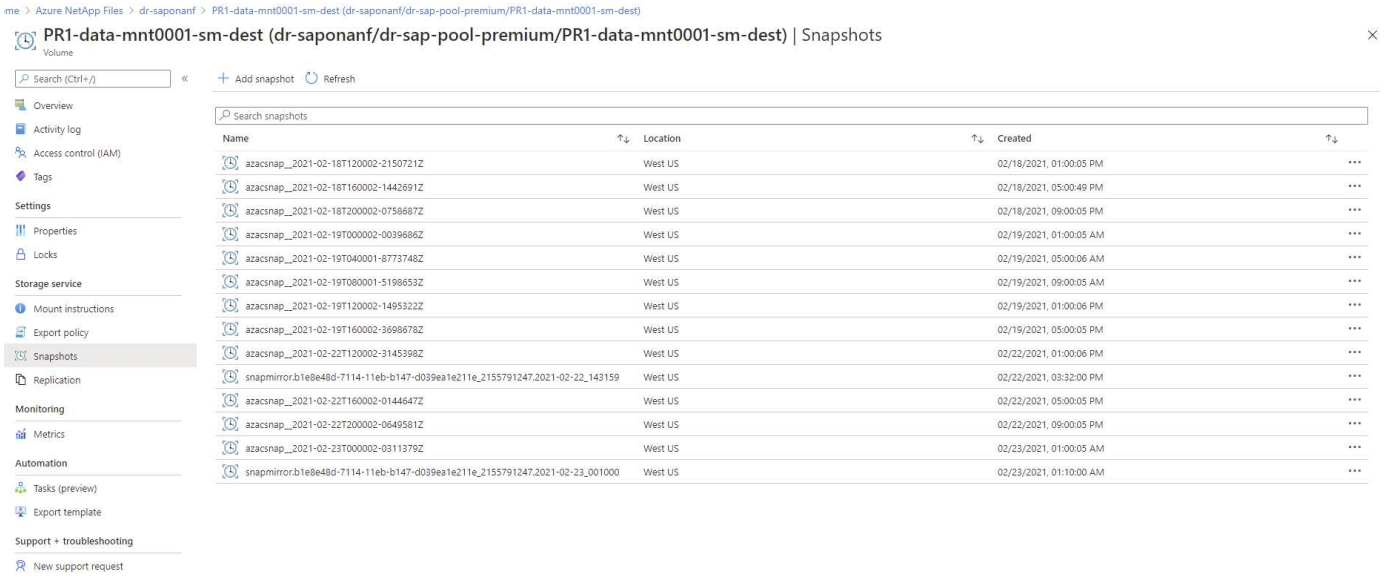
The following screenshot shows the replication status of HANA shared volume.



Replicated snapshot backups

With each replication update from the source to the target volume, all block changes that happened between the last and the current update are replicated to the target volume. This also includes the snapshots, which have been created at the source volume. The following screenshot shows the snapshots available at the target volume. As already discussed, each of the snapshots created by the AzAcSnap tool are application-consistent images of the HANA database that can be used to execute either a savepoint or a forward recovery.

Within the source and the target volume, SnapMirror Snapshot copies are created as well, which are used for resync and replication update operations. These Snapshot copies are not application consistent from the HANA database perspective; only the application-consistent snapshots created via AzaCSnap can be used for HANA recovery operations.



Disaster recovery testing

Disaster Recovery Testing

To implement an effective disaster recovery strategy, you must test the required workflow. Testing demonstrates whether the strategy works and whether the internal documentation is sufficient, and it also allows administrators to train on the required procedures.

ANF Cross-Region Replication enables disaster recovery testing without putting RTO and RPO at risk. Disaster recovery testing can be done without interrupting data replication.

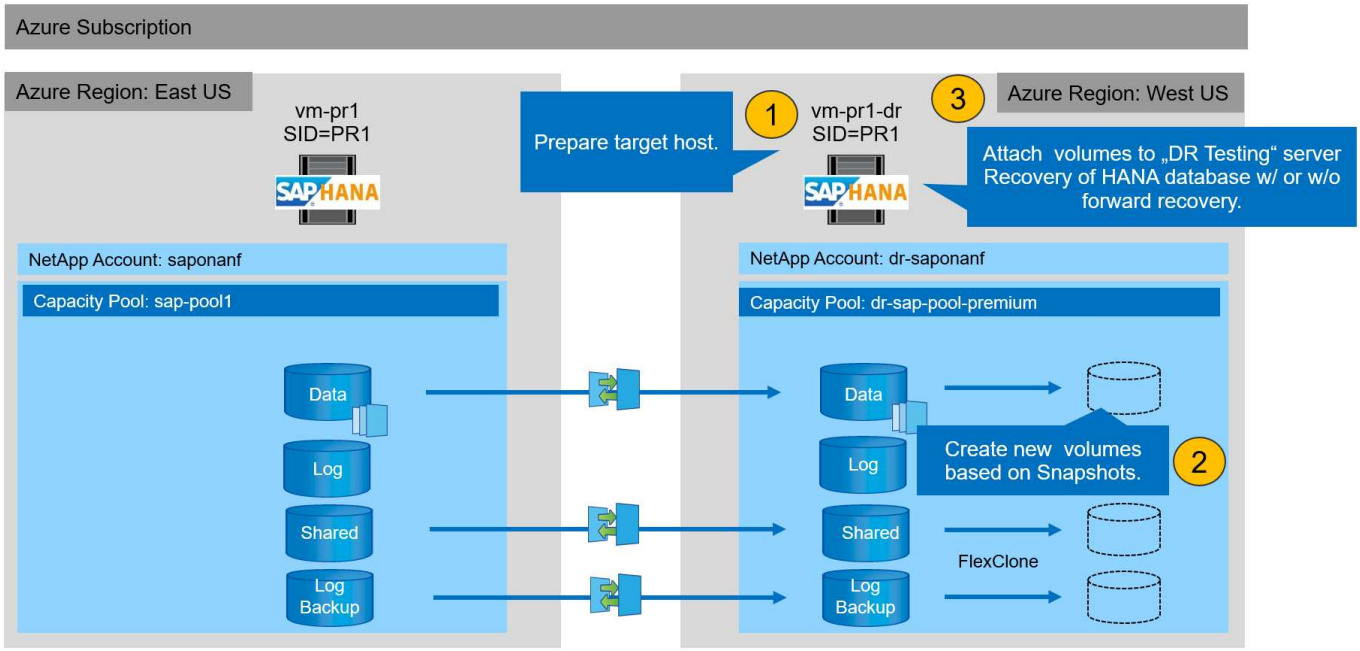
The disaster recovery testing workflow leverages the ANF feature set to create new volumes based on existing Snapshot backups at the disaster recovery target. See How Azure NetApp Files snapshots work | Microsoft Docs.

Depending on whether log backup replication is part of the disaster recovery setup or not, the steps for disaster recovery are slightly different. This section describes the disaster recovery testing for data-backup-only replication as well as for data volume replication combined with log backup volume replication.

To perform disaster recovery testing, complete the following steps:

1. Prepare the target host.
2. Create new volumes based on Snapshot backups at the disaster recovery site.
3. Mount the new volumes at the target host.
4. Recover the HANA database.
    - Data volume recovery only.
    - Forward recovery using replicated log backups.

The following subsections describe these steps in detail.



Prepare the target host

This section describes the preparation steps required at the server that is used for disaster recovery failover testing.

During normal operation, the target host is typically used for other purposes, for example as a HANA QA or test system. Therefore, most of these steps must be run when disaster failover testing is performed. On the other hand, the relevant configuration files, like `/etc/fstab` and `/usr/sap/sapservices`, can be prepared and then put into production by simply copying the configuration file. The disaster recovery testing procedure ensures that the relevant prepared configuration files are configured correctly.

The target host preparation also includes shutting down the HANA QA or test system, as well as stopping all services using `systemctl stop sapinit`.

Target server host name and IP address

The host name of the target server must be identical to the host name of the source system. The IP address can be different.

> Proper fencing of the target server must be established so that it cannot communicate with other systems. If proper fencing is not in place, then the cloned production system might exchange data with other production systems, resulting in logically corrupted data.

Install required software

The SAP host agent software must be installed at the target server. For more information, see the SAP Host Agent at the SAP help portal.

> If the host is used as a HANA QA or test system, the SAP host agent software is already installed.

Configure users, ports, and SAP services

The required users and groups for the SAP HANA database must be available at the target server. Typically, central user management is used; therefore, no configuration steps are necessary at the target server. The required ports for the HANA database must be configured at the target hosts. The configuration can be copied from the source system by copying the `/etc/services` file to the target server.

The required SAP services entries must be available at the target host. The configuration can be copied from the source system by copying the `/usr/sap/sapservices` file to the target server. The following output shows the required entries for the SAP HANA database used in the lab setup.

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
limit.descriptors=1048576
```

Prepare HANA log volume

Because the HANA log volume is not part of the replication, an empty log volume must exist at the target host. The log volume must include the same subdirectories as the source HANA system.

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root   root   4096 Feb 19 16:20 .
drwxr-xr-x 3 root   root     22 Feb 18 13:38 ..
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

Prepare log backup volume

Because the source system is configured with a separate volume for the HANA log backups, a log backup volume must also be available at the target host. A volume for the log backups must be configured and mounted at the target host.

If log backup volume replication is part of the disaster recovery setup, a new volume based on a snapshot is mounted at the target host, and it is not necessary to prepare an additional log backup volume.

Prepare file system mounts

The following table shows the naming conventions used in the lab setup. The volume names of the new volumes at the disaster recovery site are included in `/etc/fstab`. These volume names are used in the volume creation step in the next section.

HANA PR1 volumes	New volume and subdirectories at disaster recovery site	Mount point at target host
Data volume	PR1-data-mnt00001-sm-dest-clone	/hana/data/PR1/mnt00001
Shared volume	PR1-shared-sm-dest-clone/shared PR1-shared-sm-dest-clone/usr-sap-PR1	/hana/shared /usr/sap/PR1
Log backup volume	hanabackup-sm-dest-clone	/hanabackup

The mount points listed in this table must be created at the target host.

Here are the required `/etc/fstab` entries.

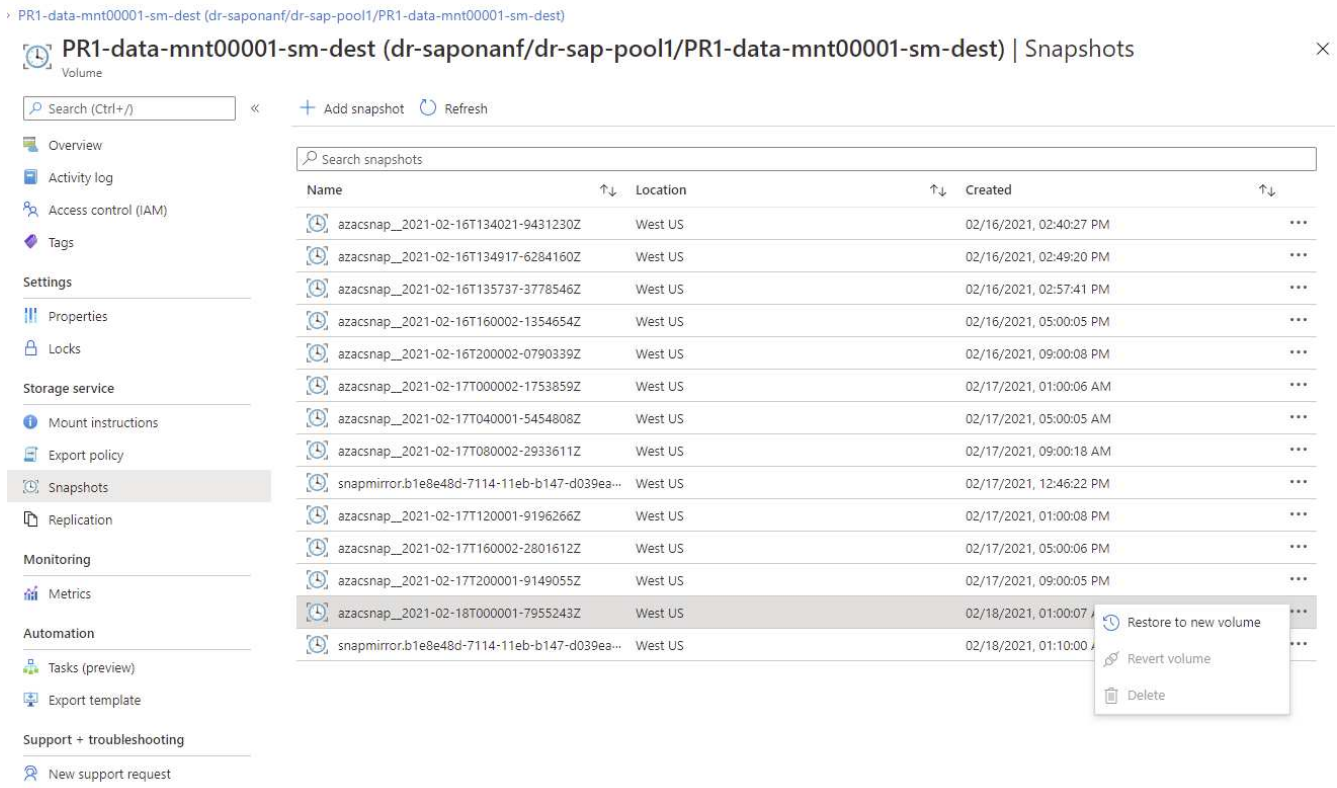
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt00001-sm-dest-clone /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest-clone/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-shared-sm-dest-clone/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest-clone    /hanabackup nfs
rw,vers=3,hard,timeo=600,rsize=262144,wsize=262144,nconnect=8,bg,noatime,n
olock 0 0
```

Create new volumes based on snapshot backups at the disaster recovery site

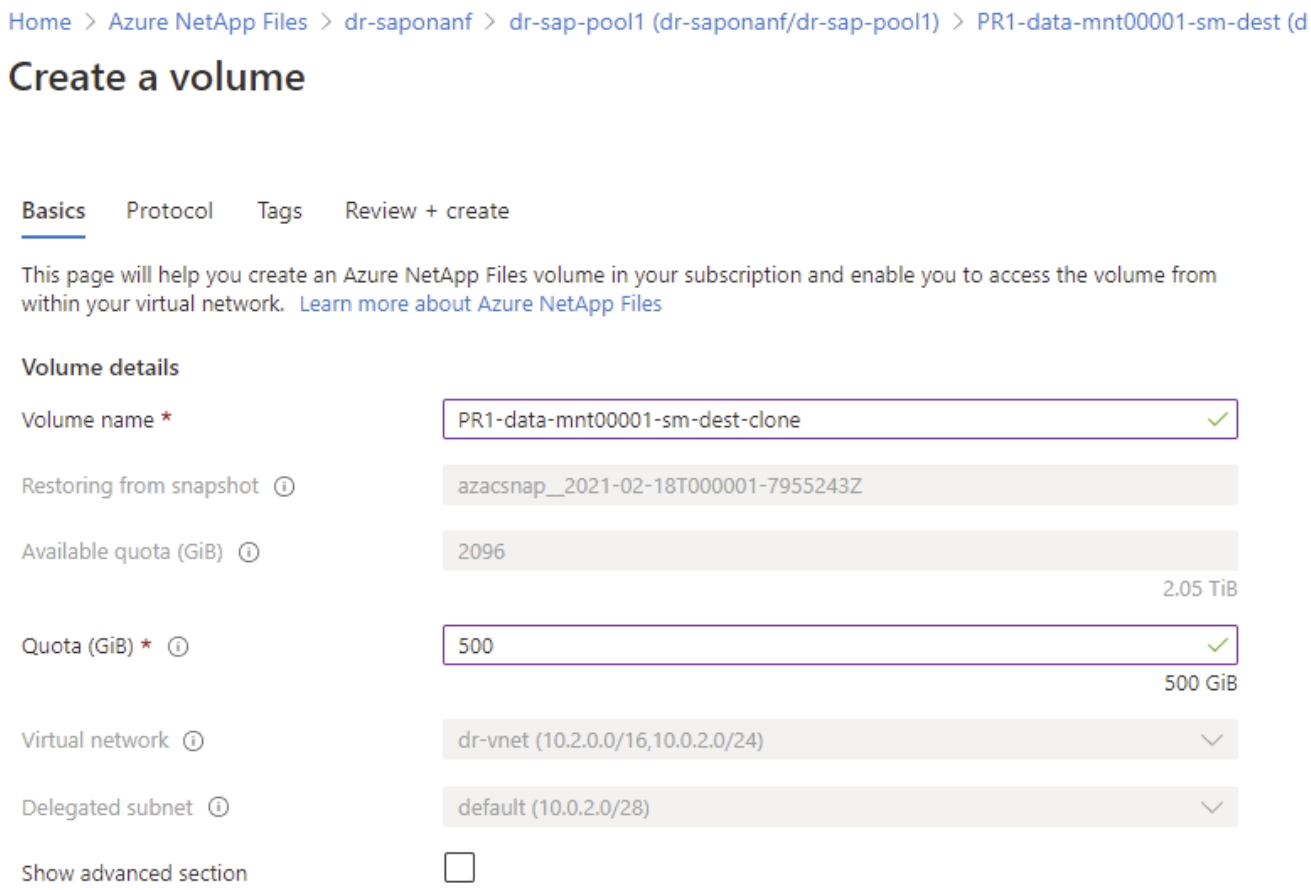
Depending on the disaster recovery setup (with or without log backup replication), two or three new volumes based on snapshot backups must be created. In both cases, a new volume of the data and the HANA shared volume must be created.

A new volume of the log backup volume must be created if the log backup data is also replicated. In our example, data and the log backup volume have been replicated to the disaster recovery site. The following steps use the Azure Portal.

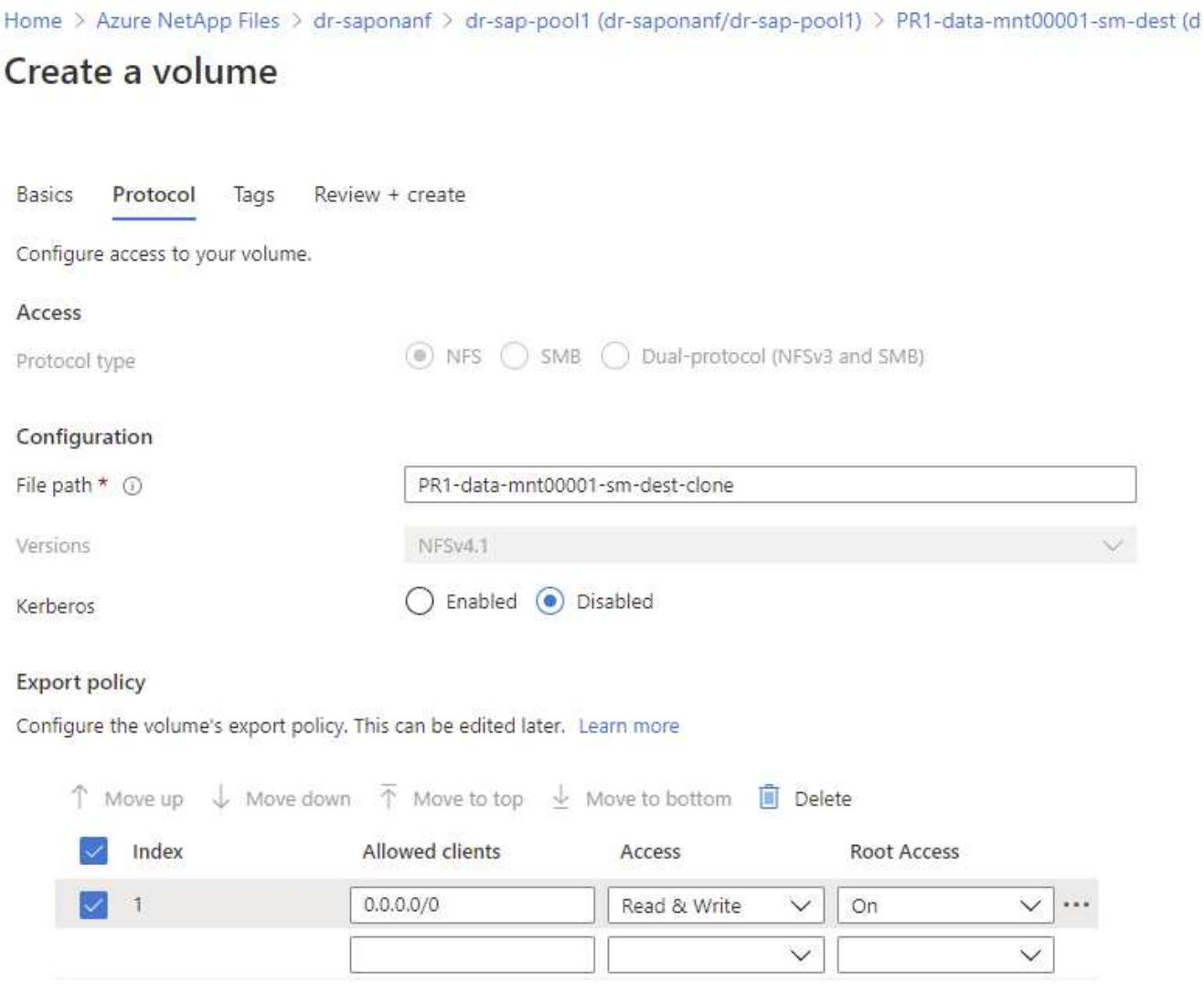
1. One of the application-consistent snapshot backups is selected as a source for the new volume of the HANA data volume. Restore to New Volume is selected to create a new volume based on the snapshot backup.



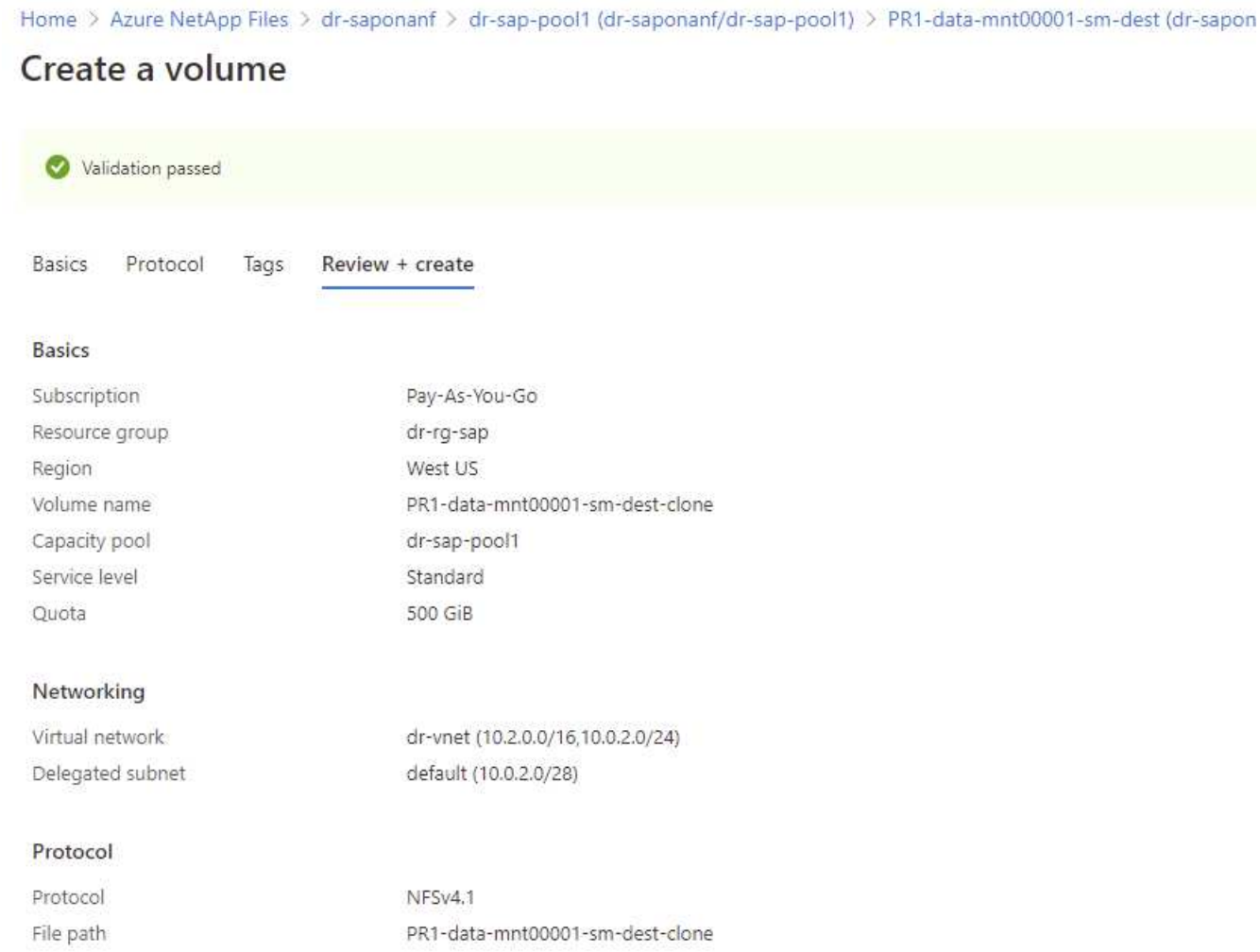
2. The new volume name and quota must be provided in the user interface.



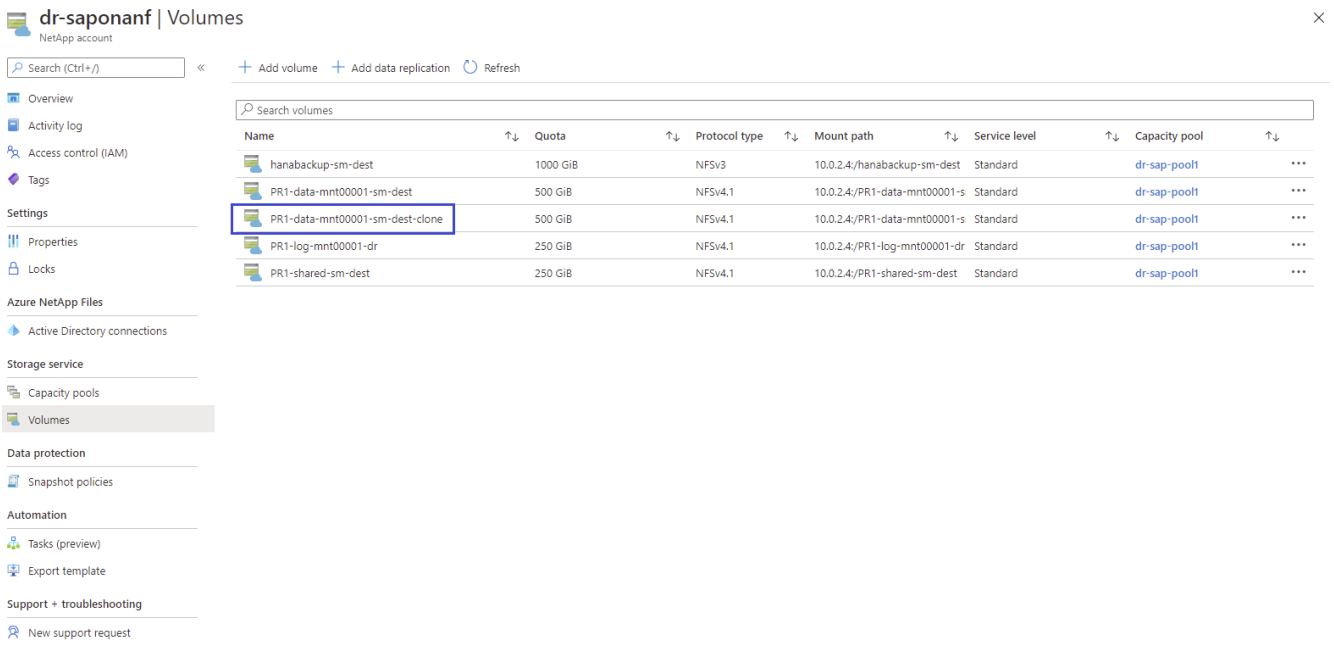
3. Within the protocol tab, the file path and export policy are configured.



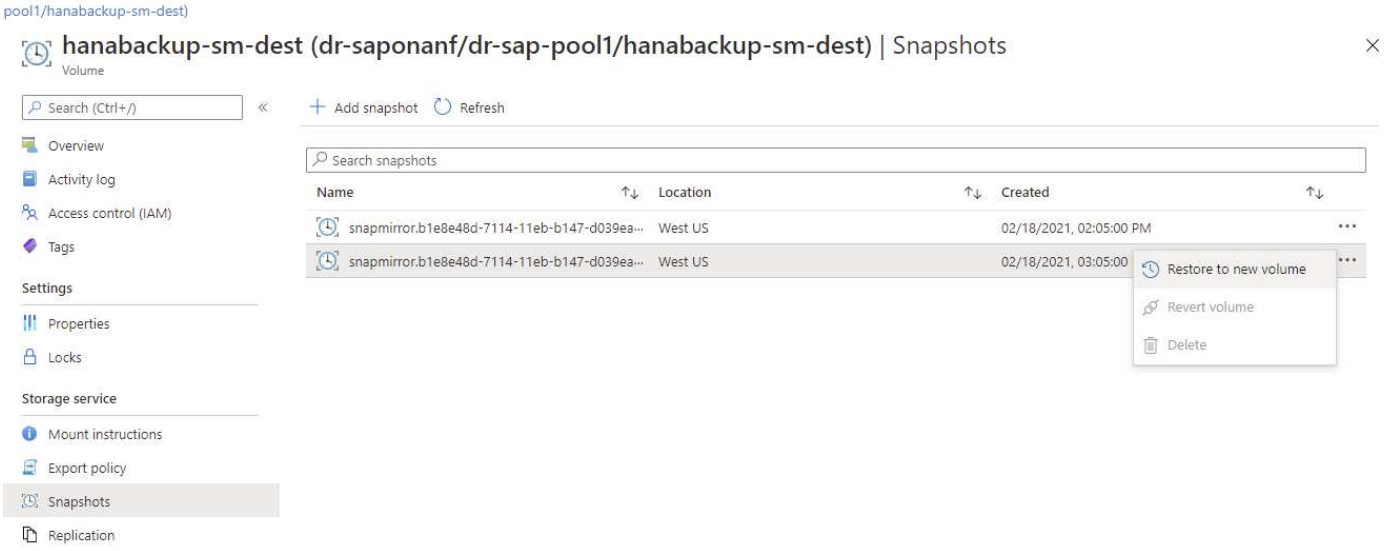
4. The Create and Review screen summarizes the configuration.



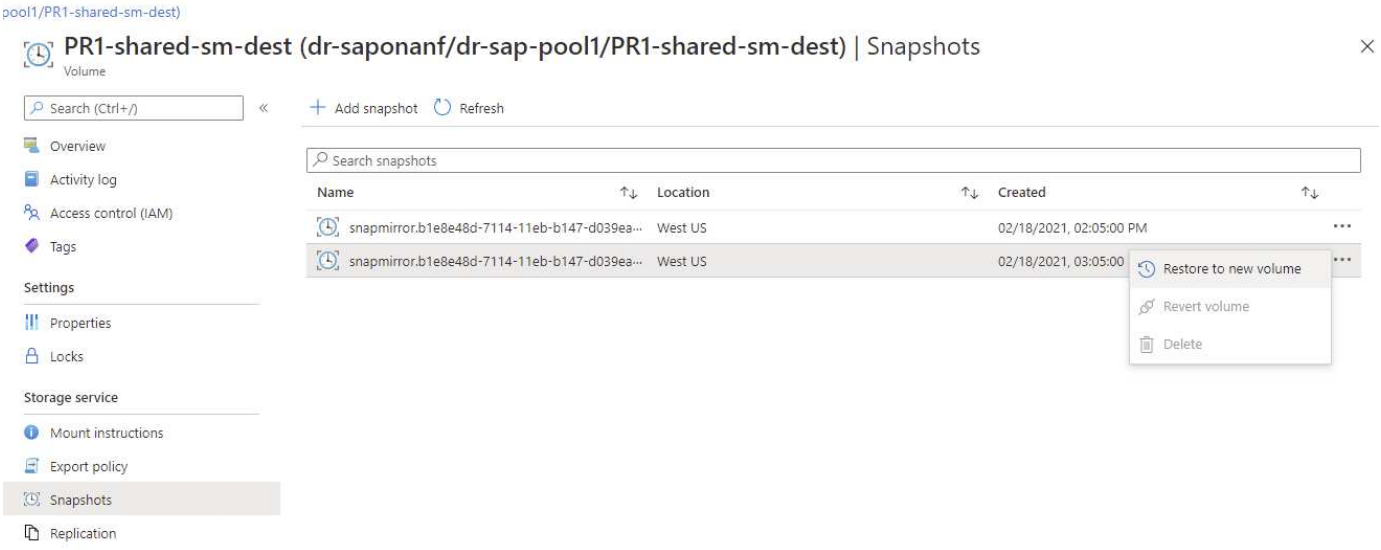
5. A new volume has now been created based on the HANA snapshot backup.



The same steps must now be performed for the HANA shared and the log backup volume as shown in the following two screenshots. Since no additional snapshots have been created for the HANA shared and log backup volume, the newest SnapMirror Snapshot copy must be selected as the source for the new volume. This is unstructured data, and the SnapMirror Snapshot copy can be used for this use case.



The following screenshot shows the HANA shared volume restored to new volume.



If a capacity pool with a low performance tier has been used, the volumes must now be moved to a capacity pool that provides the required performance.

All three new volumes are now available and can be mounted at the target host.

Mount the new volumes at the target host

The new volumes can now be mounted at the target host, based on the `/etc/fstab` file created before.

```
vm-pr1:~ # mount -a
```

The following output shows the required file systems.

```
vm-pr1:/hana/data/PR1/mnt00001/hdb00001 # df
Filesystem                                          1K-blocks     Used
Available Use% Mounted on
devtmpfs                                              8190344        8
8190336   1% /dev
tmpfs                                                12313116        0
12313116   0% /dev/shm
tmpfs                                                 8208744    17292
8191452   1% /run
tmpfs                                                 8208744        0
8208744   0% /sys/fs/cgroup
/dev/sda4                                            29866736  2438052
27428684   9% /
/dev/sda3                                             1038336   101520
936816  10% /boot
/dev/sda2                                              524008     1072
522936   1% /boot/efi
/dev/sdb1                                            32894736    49176
31151560   1% /mnt
tmpfs                                                 1641748        0
1641748   0% /run/user/0
10.0.2.4:/PR1-log-mnt00001-dr                    107374182400      256
107374182144   1% /hana/log/PR1/mnt00001
10.0.2.4:/PR1-data-mnt00001-sm-dest-clone      107377026560  6672640
107370353920   1% /hana/data/PR1/mnt00001
10.0.2.4:/PR1-shared-sm-dest-clone/hana-shared 107377048320 11204096
107365844224   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest-clone/usr-sap-PR1 107377048320 11204096
107365844224   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest-clone             107379429120 35293440
107344135680   1% /hanabackup
```

HANA database recovery

The following shows the steps for HANA database recovery

Start the required SAP services.

```
vm-pr1:~ # systemctl start sapinit
```

The following output shows the required processes.

```
vm-pr1:/ # ps -ef | grep sap
root     23101     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm   23191     1  3 11:29 ?        00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm   23202     1  5 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root     23292     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root     23359  2597  0 11:29 pts/1    00:00:00 grep --color=auto sap
```

The following subsections describe the recovery process with and without forward recovery using the replicated log backups. The recovery is executed using the HANA recovery script for the system database and hdbsql commands for the tenant database.

Recovery to latest HANA data volume backup savepoint

The recovery to the latest backup savepoint is executed with the following commands as user pr1adm:

- System database

```
recoverSys.py --command "RECOVER DATA USING SNAPSHOT CLEAR LOG”
```

- Tenant database

```
Within hdbsql: RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
```

You can also use HANA Studio or Cockpit to execute the recovery of the system and the tenant database.

The following command output show the recovery execution.

System database recovery

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py
--command="RECOVER DATA USING SNAPSHOT CLEAR LOG"
[139702869464896, 0.008] >> starting recoverSys (at Fri Feb 19 14:32:16
2021)
[139702869464896, 0.008] args: ()
[139702869464896, 0.009] keys: {'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 14:32:16 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 14:32:16
stopped system: 2021-02-19 14:32:16
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 14:32:21
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T14:32:56+00:00  P0027646      177bab4d610 INFO    RECOVERY
RECOVER DATA finished successfully
recoverSys finished successfully: 2021-02-19 14:32:58
[139702869464896, 42.017] 0
[139702869464896, 42.017] << ending recoverSys, rc = 0 (RC_TEST_OK), after
42.009 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>
```

Tenant database recovery

If a user store key has not been created for the pr1adm user at the source system, a key must be created at the target system. The database user configured in the key must have privileges to execute tenant recovery operations.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>
```

The tenant recovery is now executed with hdbsql.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
0 rows affected (overall time 66.973089 sec; server time 66.970736 sec)
hdbsql SYSTEMDB=>
```

The HANA database is now up and running, and the disaster recovery workflow for the HANA database has been tested.

Recovery with forward recovery using log/catalog backups

Log backups and the HANA backup catalog are being replicated from the source system.

The recovery using all available log backups is executed with the following commands as user pr1adm:

- System database

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- Tenant database

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```

> To recover using all available logs, you can just use any time in the future as the timestamp in the recovery statement.

You can also use HANA Studio or Cockpit to execute the recovery of the system and the tenant database.

The following command output show the recovery execution.

System database recovery

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING
SNAPSHOT"
[140404915394368, 0.008] >> starting recoverSys (at Fri Feb 19 16:06:40
2021)
[140404915394368, 0.008] args: ()
[140404915394368, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 16:06:40 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 16:06:40
stopped system: 2021-02-19 16:06:41
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 16:06:46
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T16:07:19+00:00  P0009897      177bb0b4416 INFO    RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
19T15:17:33+00:00, reached log position 38272960
recoverSys finished successfully: 2021-02-19 16:07:20
[140404915394368, 39.757] 0
[140404915394368, 39.758] << ending recoverSys, rc = 0 (RC_TEST_OK), after
39.749 secs
```

Tenant database recovery

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit

hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 63.791121 sec; server time 63.788754 sec)

hdbsql SYSTEMDB=>
```

The HANA database is now up and running, and the disaster recovery workflow for the HANA database has been tested.

Check consistency of latest log backups

Because log backup volume replication is performed independently of the log backup process executed by the SAP HANA database, there might be open, inconsistent log backup files at the disaster recovery site. Only the latest log backup files might be inconsistent, and those files should be checked before a forward recovery is performed at the disaster recovery site using the `hdbbackupcheck` tool.

If the `hdbbackupcheck` tool reports an error for the latest log backups, the latest set of log backups must be removed or deleted.

```
pr1adm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

The check must be executed for the latest log backup files of the system and the tenant database.

If the `hdbbackupcheck` tool reports an error for the latest log backups, the latest set of log backups must be removed or deleted.

Disaster recovery failover

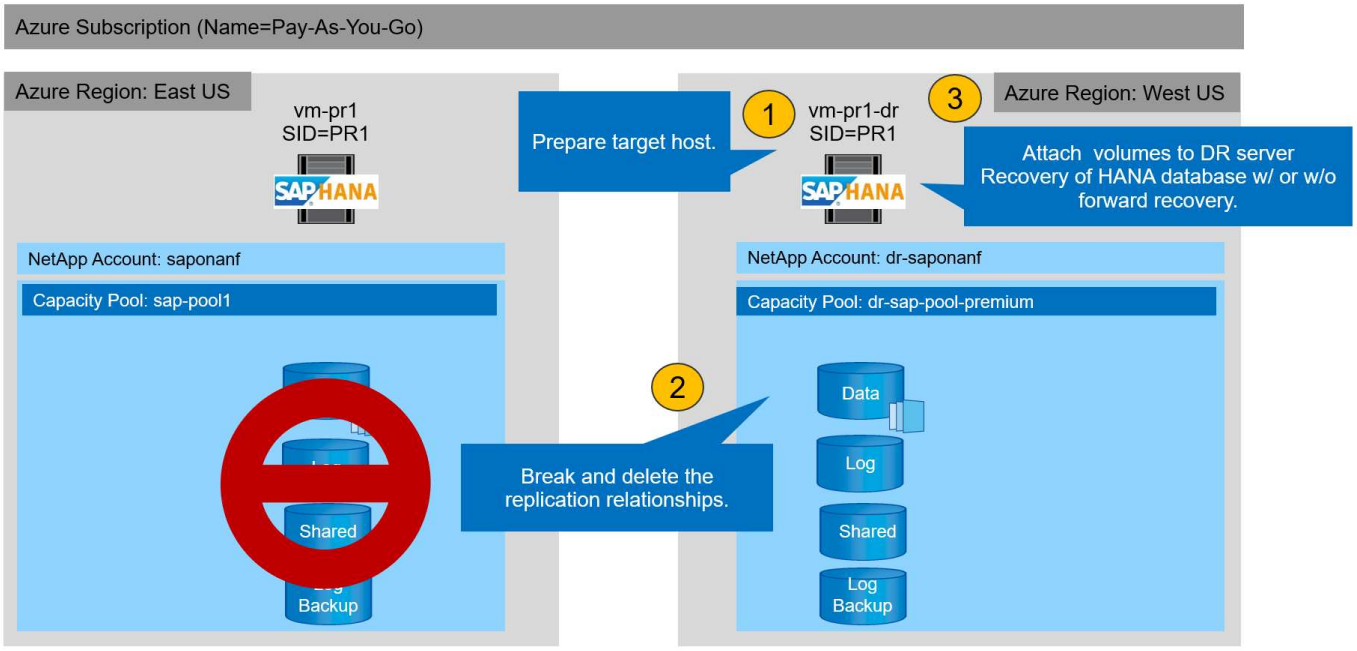
Disaster recovery failover

Depending on whether the log backup replication is part of the disaster recovery setup, the steps for disaster recovery are slightly different. This section describes the disaster recovery failover for data-backup-only replication as well as for data volume replication combined with log backup volume replication.

To execute disaster recovery failover, complete these steps:

1. Prepare the target host.
2. Break and delete the replication relationships.
3. Restore the data volume to the latest application- consistent snapshot backup.
4. Mount the volumes at the target host.
5. Recover the HANA database.
    - Data volume recovery only.
    - Forward recovery using replicated log backups.

The following subsections describe these steps in detail, and the following figure depicts disaster failover testing.



Prepare the target host

This section describes the preparation steps required at the server that is used for the disaster recovery failover.

During normal operation, the target host is typically used for other purposes, for example, as a HANA QA or test system. Therefore, most of the described steps must be executed when disaster failover testing is executed. On the other hand, the relevant configuration files, like `/etc/fstab` and `/usr/sap/sapservices`, can be prepared and then put in production by simply copying the configuration file. The disaster recovery failover procedure ensures that the relevant prepared configuration files are configured correctly.

The target host preparation also includes shutting down the HANA QA or test system as well as stopping all services using `systemctl stop sapinit`.

Target server host name and IP address

The host name of the target server must be identical to the host name of the source system. The IP address can be different.

Proper fencing of the target server must be established so that it cannot communicate with other systems. If proper fencing is not in place, then the cloned production system might exchange data with other production systems, resulting in logically corrupted data.

Install required software

The SAP host agent software must be installed at the target server. For full information, see the SAP Host Agent at the SAP help portal.

If the host is used as a HANA QA or test system, the SAP host agent software is already installed.

Configure users, ports, and SAP services

The required users and groups for the SAP HANA database must be available at the target server. Typically, central user management is used; therefore, no configuration steps are necessary at the target server. The required ports for the HANA database must be configured at the target hosts. The configuration can be copied from the source system by copying the `/etc/services` file to the target server.

The required SAP services entries must be available at the target host. The configuration can be copied from the source system by copying the `/usr/sap/sapservices` file to the target server. The following output shows the required entries for the SAP HANA database used in the lab setup.

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
limit.descriptors=1048576
```

Prepare HANA log volume

Because the HANA log volume is not part of the replication, an empty log volume must exist at the target host. The log volume must include the same subdirectories as the source HANA system.

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root   root   4096 Feb 19 16:20 .
drwxr-xr-x 3 root   root     22 Feb 18 13:38 ..
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

Prepare log backup volume

Because the source system is configured with a separate volume for the HANA log backups, a log backup volume must also be available at the target host. A volume for the log backups must be configured and mounted at the target host.

If log backup volume replication is part of the disaster recovery setup, the replicated log backup volume is mounted at the target host, and it is not necessary to prepare an additional log backup volume.

Prepare file system mounts

The following table shows the naming conventions used in the lab setup. The volume names at the disaster recovery site are included in `/etc/fstab`.

HANA PR1 volumes	Volume and subdirectories at disaster recovery site	Mount point at target host
Data volume	PR1-data-mnt00001-sm-dest	/hana/data/PR1/mnt00001
Shared volume	PR1-shared-sm-dest/shared PR1-shared-sm-dest/usr-sap-PR1	/hana/shared /usr/sap/PR1
Log backup volume	hanabackup-sm-dest	/hanabackup

The mount points from this table must be created at the target host.

Here are the required `/etc/fstab` entries.

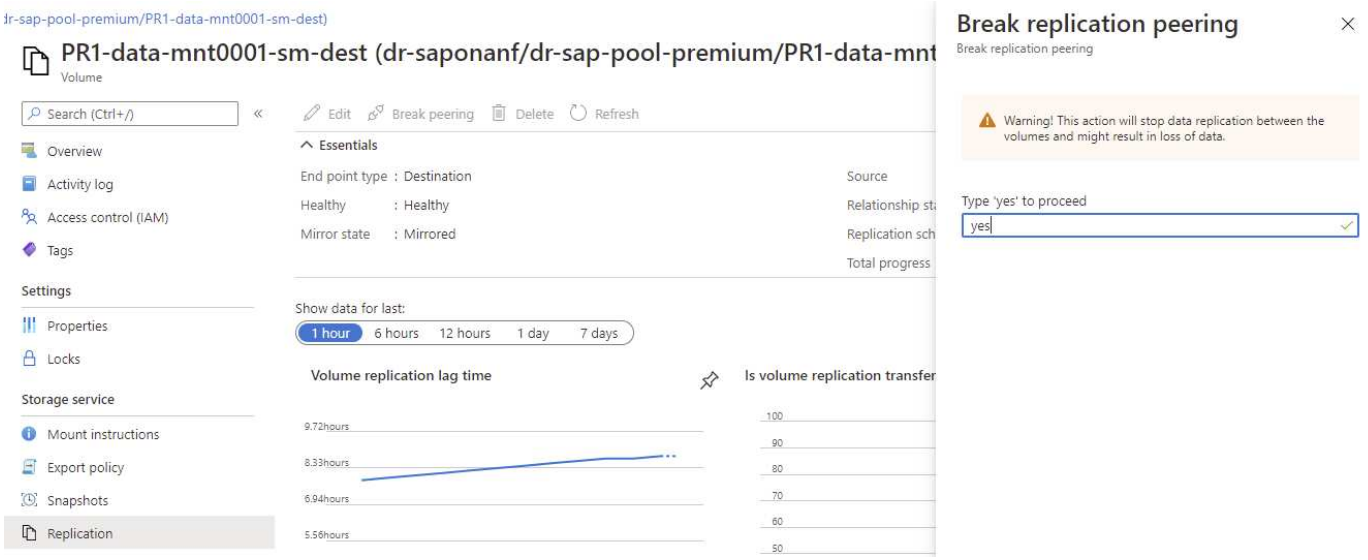
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest    /hanabackup nfs
rw,vers=3,hard,timeo=600,rsize=262144,wsize=262144,nconnect=8,bg,noatime,n
olock 0 0
```

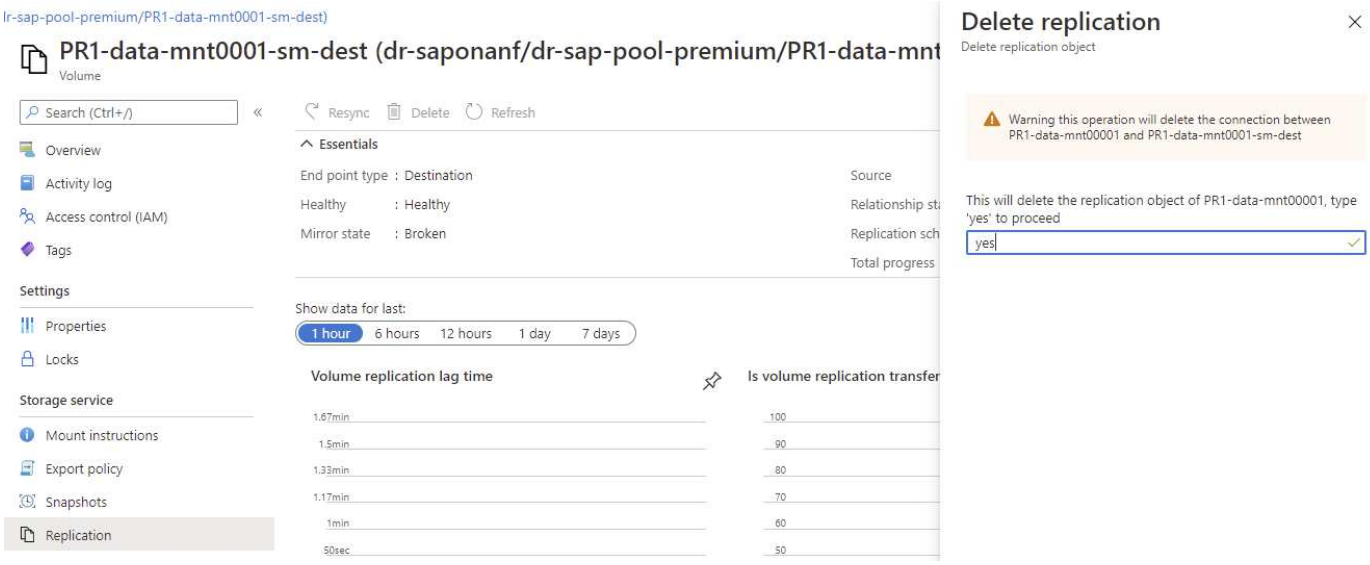
Break and delete replication peering

In case of a disaster failover, the target volumes must be broken off so that the target host can mount the volumes for read and write operations.

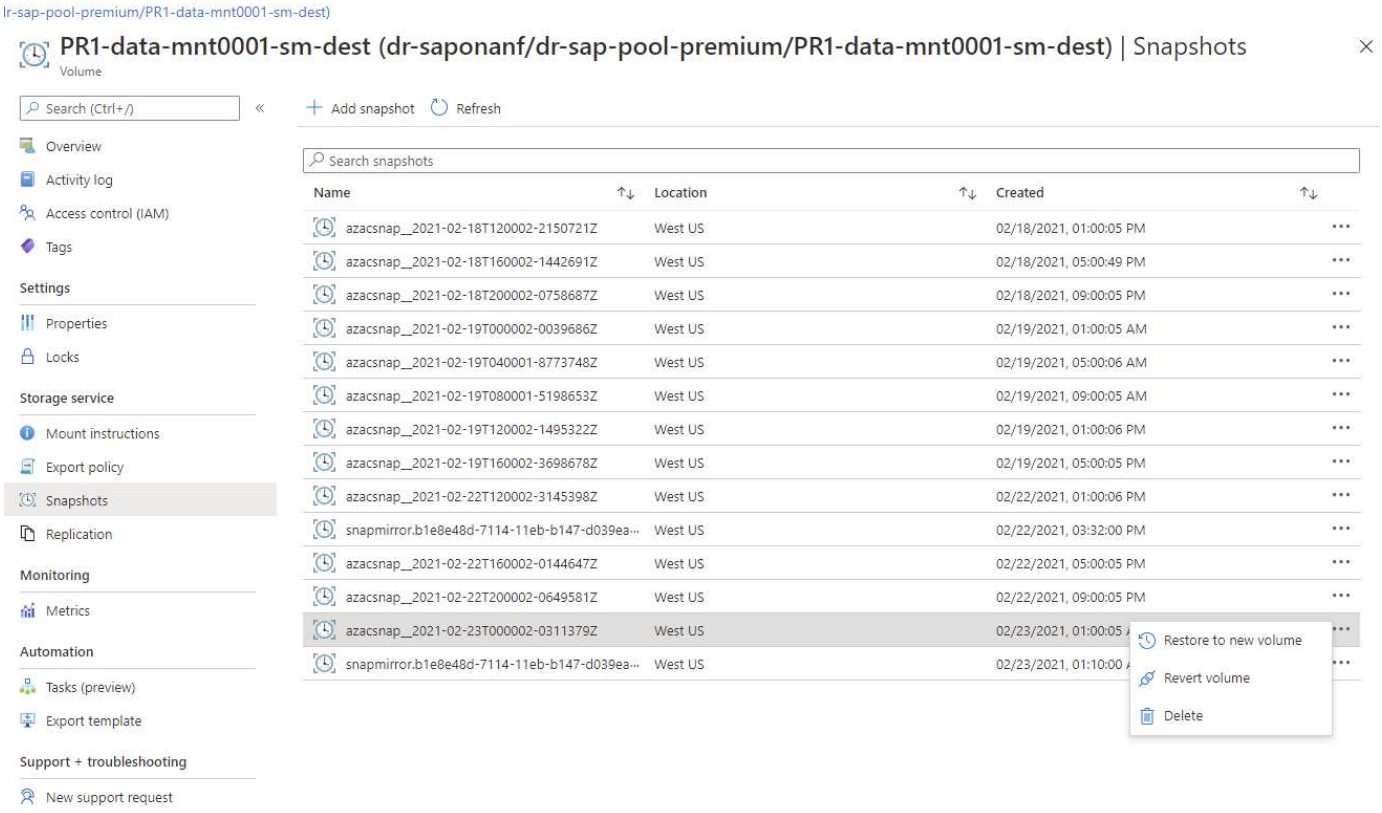
For the HANA data volume, you must restore the volume to the latest HANA snapshot backup created with AzAcSnap. This volume revert operation is not possible if the latest replication snapshot is marked as busy due to the replication peering. Therefore, you must also delete the replication peering.

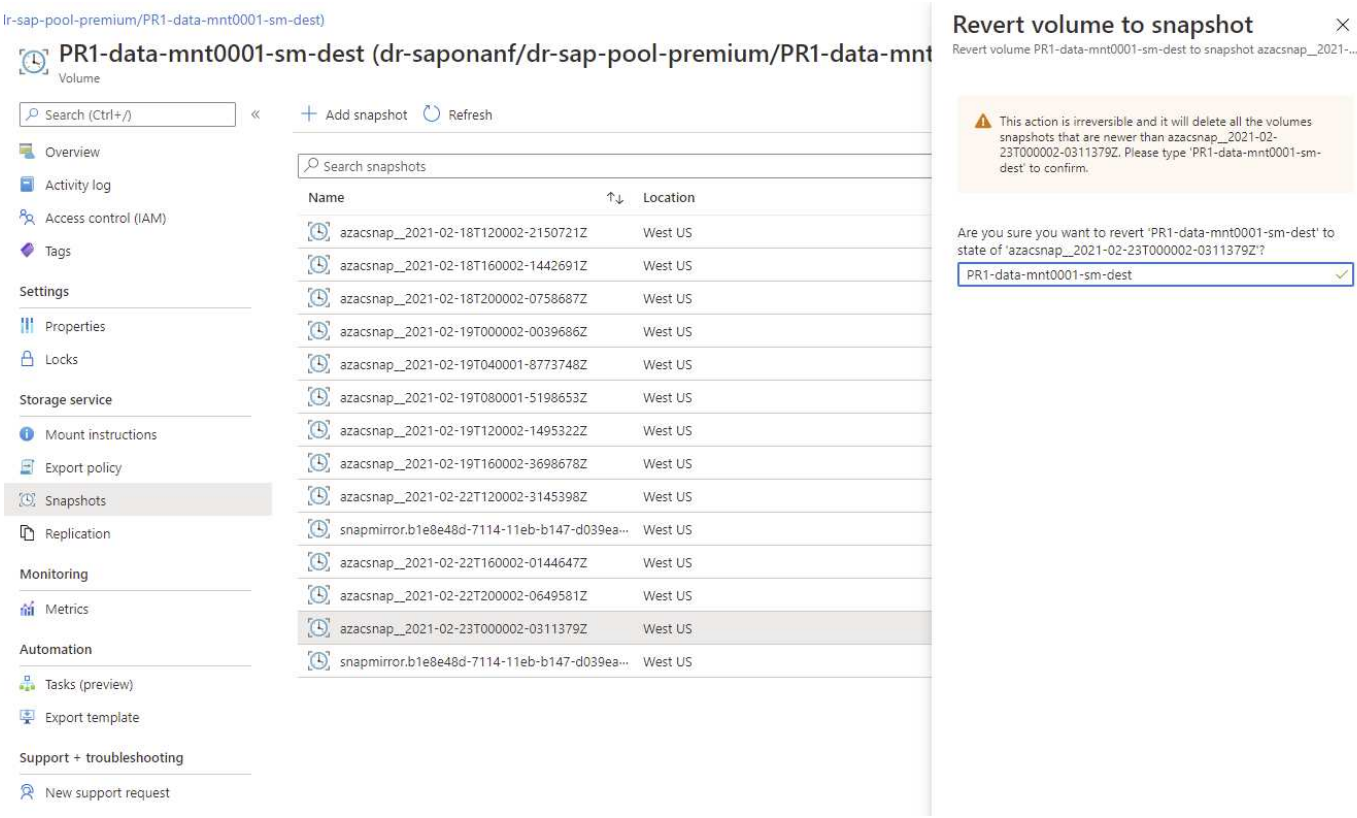
The next two screenshots show the break and delete peering operation for the HANA data volume. The same operations must be performed for the log backup and the HANA shared volume as well.





Since replication peering was deleted, it is possible to revert the volume to the latest HANA snapshot backup. If peering is not deleted, the selection of revert volume is grayed out and is not selectable. The following two screenshots show the volume revert operation.





After the volume revert operation, the data volume is based on the consistent HANA snapshot backup and can now be used to execute forward recovery operations.

If a capacity pool with a low performance tier has been used, the volumes must now be moved to a capacity pool that can provide the required performance.

Mount the volumes at the target host

The volumes can now be mounted at the target host, based on the `/etc/fstab` file created before.

```
vm-pr1:~ # mount -a
```

The following output shows the required file systems.

```
vm-pr1:~ # df
Filesystem                                      1K-blocks     Used
Available Use% Mounted on
devtmpfs                                          8201112        0
8201112   0% /dev
tmpfs                                            12313116        0
12313116   0% /dev/shm
tmpfs                                             8208744     9096
8199648   1% /run
tmpfs                                             8208744        0
8208744   0% /sys/fs/cgroup
/dev/sda4                                        29866736  2543948
27322788   9% /
/dev/sda3                                         1038336    79984
958352   8% /boot
/dev/sda2                                          524008     1072
522936   1% /boot/efi
/dev/sdb1                                        32894736    49180
31151556   1% /mnt
10.0.2.4:/PR1-log-mnt00001-dr                107374182400     6400
107374176000   1% /hana/log/PR1/mnt00001
tmpfs                                             1641748        0
1641748   0% /run/user/0
10.0.2.4:/PR1-shared-sm-dest/hana-shared     107377178368 11317248
107365861120   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1     107377178368 11317248
107365861120   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest                 107379678976 35249408
107344429568   1% /hanabackup
10.0.2.4:/PR1-data-mnt0001-sm-dest           107376511232  6696960
107369814272   1% /hana/data/PR1/mnt00001
vm-pr1:~ #
```

HANA database recovery

The following are steps for HANA database recovery.

Start the required SAP services.

```
vm-pr1:~ # systemctl start sapinit
```

The following output shows the required processes.

```
vm-pr1:/ # ps -ef | grep sap
root     23101     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm   23191     1  3 11:29 ?        00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm   23202     1  5 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root     23292     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root     23359  2597  0 11:29 pts/1    00:00:00 grep --color=auto sap
```

The following subsections describe the recovery process with forward recovery using the replicated log backups. The recovery is executed using the HANA recovery script for the system database and hdbsql commands for the tenant database.

The commands to execute a recovery to the latest data savepoint is described in chapter Recovery to latest HANA Data Volume Backup Savepoint.

Recovery with forward recovery using log backups

The recovery using all available log backups is executed with the following commands as user pr1adm:

- System database

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- Tenant database

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```

To recover using all available logs, you can use any time in the future as the timestamp in the recovery statement.

You can also use HANA Studio or Cockpit to execute the recovery of the system and the tenant database.

The following command output show the recovery execution.

System database recovery

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-24 00:00:00' CLEAR LOG USING
SNAPSHOT"
[139792805873472, 0.008] >> starting recoverSys (at Tue Feb 23 12:05:16
2021)
[139792805873472, 0.008] args: ()
[139792805873472, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-24 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-23 12:05:16 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-23 12:05:17
stopped system: 2021-02-23 12:05:18
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-23 12:05:23
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-23T12:07:53+00:00  P0012969      177cec93d51 INFO    RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
23T09:03:11+00:00, reached log position 43123520
recoverSys finished successfully: 2021-02-23 12:07:54
[139792805873472, 157.466] 0
[139792805873472, 157.466] << ending recoverSys, rc = 0 (RC_TEST_OK),
after 157.458 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>
```

Tenant database recovery

If a user store key has not been created for the pr1adm user at the source system, a key must be created at the target system. The database user configured in the key must have privileges to execute tenant recovery operations.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>
```

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-24
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 98.740038 sec; server time 98.737788 sec)
hdbsql SYSTEMDB=>
```

Check consistency of latest log backups

Because log backup volume replication is performed independently of the log backup process executed by the SAP HANA database, there might be open, inconsistent log backup files at the disaster recovery site. Only the latest log backup files might be inconsistent, and those files should be checked before a forward recovery is performed at the disaster recovery site using the `hdbbackupcheck` tool.

```
pr1adm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

The check must be executed for the latest log backup files of the System and the tenant database.

If the `hdbbackupcheck` tool reports an error for the latest log backups, the latest set of log backups must be removed or deleted.

TR-4646: SAP HANA Disaster Recovery with Storage Replication

Nils Bauer, NetApp

TR-4646 is an overview of the options for disaster recovery protection for SAP HANA. It includes detailed setup information and a use case description of a three-site disaster recovery solution based on synchronous and asynchronous NetApp SnapMirror Storage replication. The described solution uses NetApp SnapCenter with the SAP HANA plug-in to manage database consistency.

https://www.netapp.com/pdf.html?item=/media/8584-tr4646pdf.pdf

TR-4313: SAP HANA Backup and Recovery by Using Snap Creator

: hardbreaks:
:icons: font
:linkattrs:
:relative_path: ./backup/
:imagesdir: /tmp/d20231203-6435-uf6p21/source/./backup/./../media/

Nils Bauer, NetApp

TR-4313 describes the installation and configuration of the NetApp backup and recovery solution for SAP HANA. The solution is based on the NetApp Snap Creator framework and the Snap Creator plug-in for SAP HANA. This solution is supported with the certified Cisco SAP HANA multinode appliance in combination with NetApp storage. This solution is also supported with single-node and multinode SAP HANA systems in tailored data center integration (TDI) projects.

https://www.netapp.com/pdf.html?item=/media/19779-tr-4313.pdf

TR-4711: SAP HANA Backup and Recovery Using NetApp Storage Systems and Commvault Software

Marco Schoen, NetApp

Dr. Tristan Daude, Commvault Systems

TR-4711 describes the design of a NetApp and Commvault solution for SAP HANA, which includes Commvault IntelliSnap snapshot management technology and NetApp Snapshot technology. The solution is based on NetApp storage and the Commvault data protection suite.

https://www.netapp.com/pdf.html?item=/media/17050-tr4711pdf.pdf

NVA-1147-DESIGN: SAP HANA on NetApp All SAN Array - Modern SAN, Data Protection, and Disaster Recovery

Nils Bauer, Roland Wartenberg, Darryl Clinkscales, Daniel Hohman, Marco Schöen, Steve Botkin, Michael Peppers, Vidula Aiyer, Steve Collins, Pavan Jhamnani, Lee Dorrier, NetApp

Jim Zucchero, Naem Saafein, Ph.D., Broadcom Brocade

This NetApp Verified Architecture covers modernizing SAP systems and operations for SAP HANA on NetApp All SAN Array (ASA) storage systems with Brocade FC SAN Fabric. It includes backup and recovery, disaster recovery, and data protection. The solution leverages NetApp SnapCenter to automate SAP HANA backup, restore and recovery, as well as cloning workflows. Disaster recovery configuration, testing, and failover scenarios are described using synchronous NetApp SnapMirror data replication software. Additionally, SAP Data Protection with CommVault is outlined.

https://www.netapp.com/pdf.html?item=/media/10235-nva-1147-design.pdf

Copyright information

Trademark information