



# **SAP HANA System Replication Backup and Recovery with SnapCenter**

**NetApp solutions for SAP**

NetApp  
December 16, 2025

# Table of Contents

SAP HANA System Replication Backup and Recovery with SnapCenter .....	1
TR-4719: SAP HANA System Replication - Backup and Recovery with SnapCenter .....	1
High availability with an RPO of zero and a minimal RTO .....	1
Disaster recovery over a large distance .....	2
Storage Snapshot backups and SAP System Replication .....	2
SnapCenter configuration options for SAP System Replication .....	4
SnapCenter 4.6 configuration using a resource group .....	5
SnapCenter 4.6 configuration of HANA System Replication environments .....	5
Snapshot backup operations .....	9
Block-integrity check operations with file-based backups .....	14
SnapVault replication .....	14
Retention management .....	15
Restore and recovery .....	15
SnapCenter configuration with a single resource .....	16
SnapCenter configuration .....	18
SnapCenter backup operation .....	22
Restore and recovery .....	24
Restore and recovery from a backup created at the other host .....	29
Where to find additional information .....	33
Version history .....	33

# SAP HANA System Replication Backup and Recovery with SnapCenter

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

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.

Author: Nils Bauer, NetApp

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.

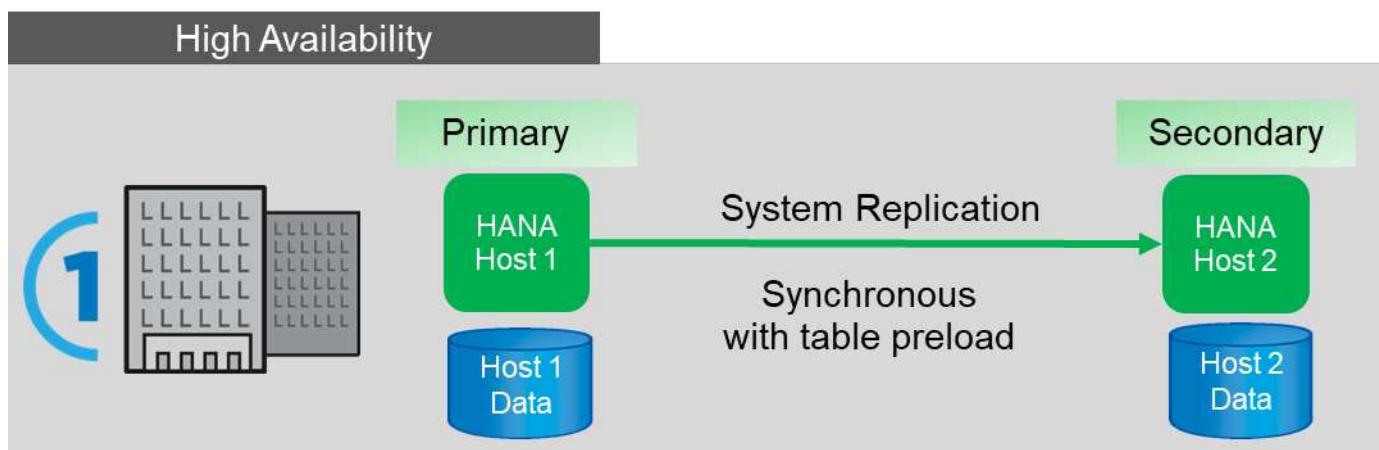
### High availability with an RPO of zero and a minimal RTO

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.

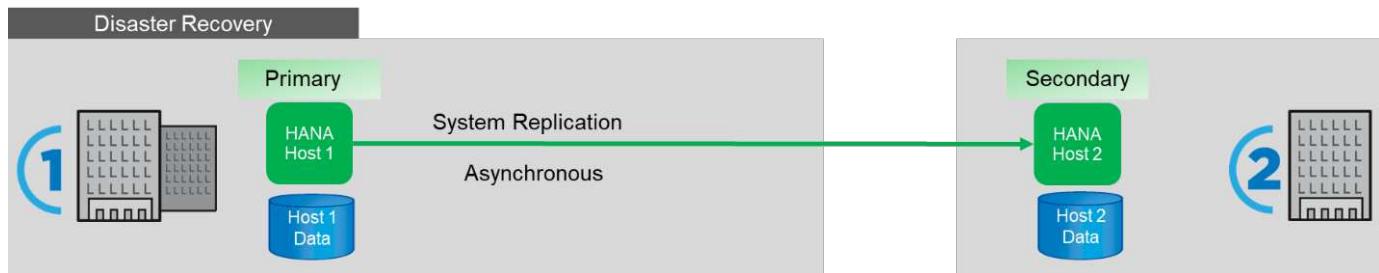
The rest of this document focuses on backup operations with SAP System Replication configured as a high-availability solution.



## 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.



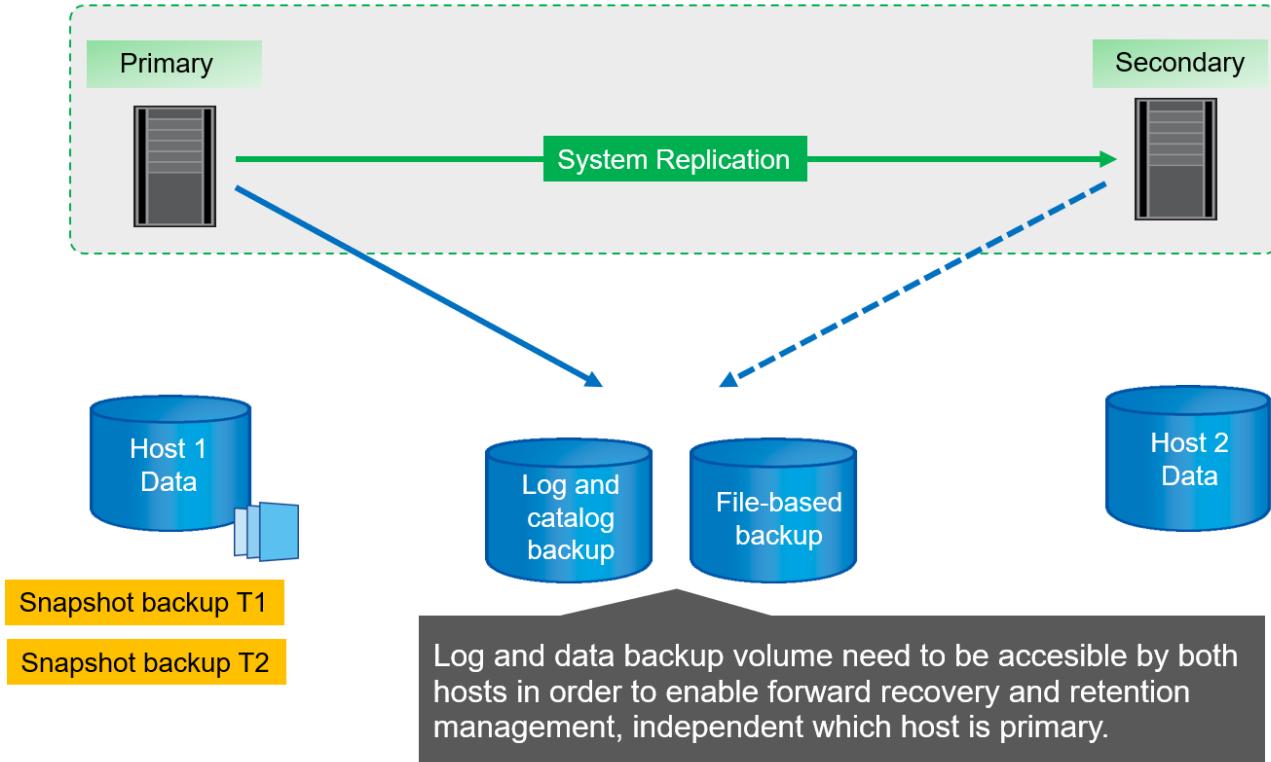
## Storage Snapshot backups and SAP System Replication

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.

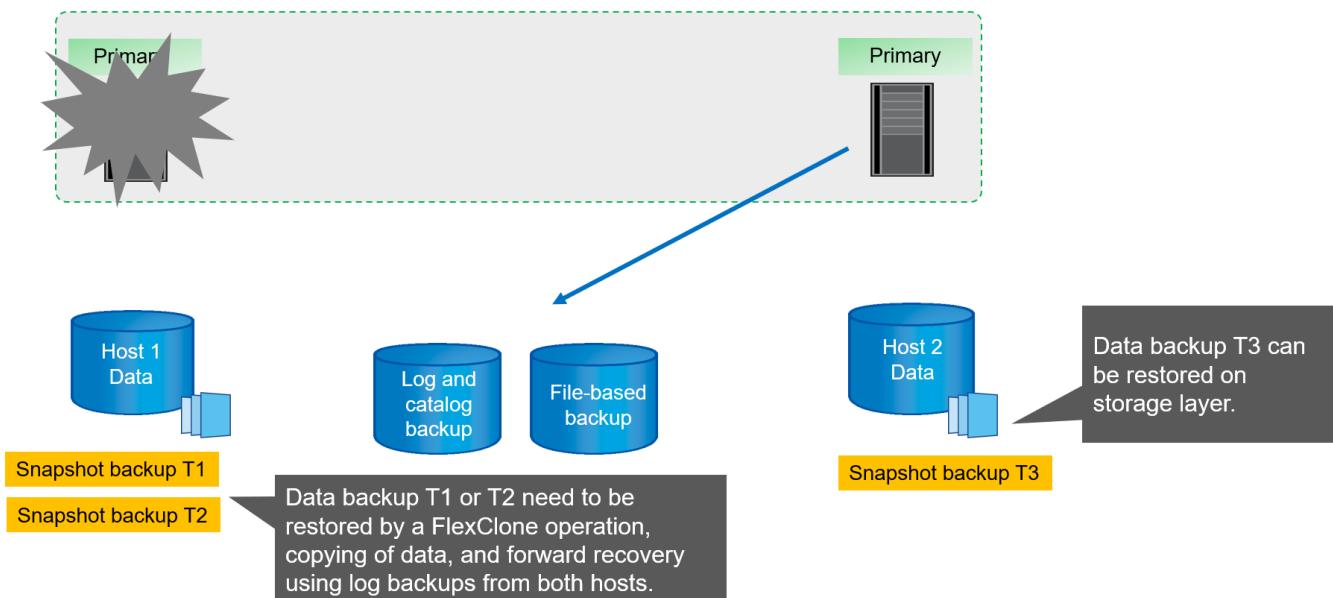
The ability to use any backup for restore and to do forward recovery using log backups from both hosts requires a shared log backup location that is accessible from both hosts. NetApp recommends that you use a shared storage volume. However, you should also separate the log backup destination into subdirectories 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 layer of host 2.

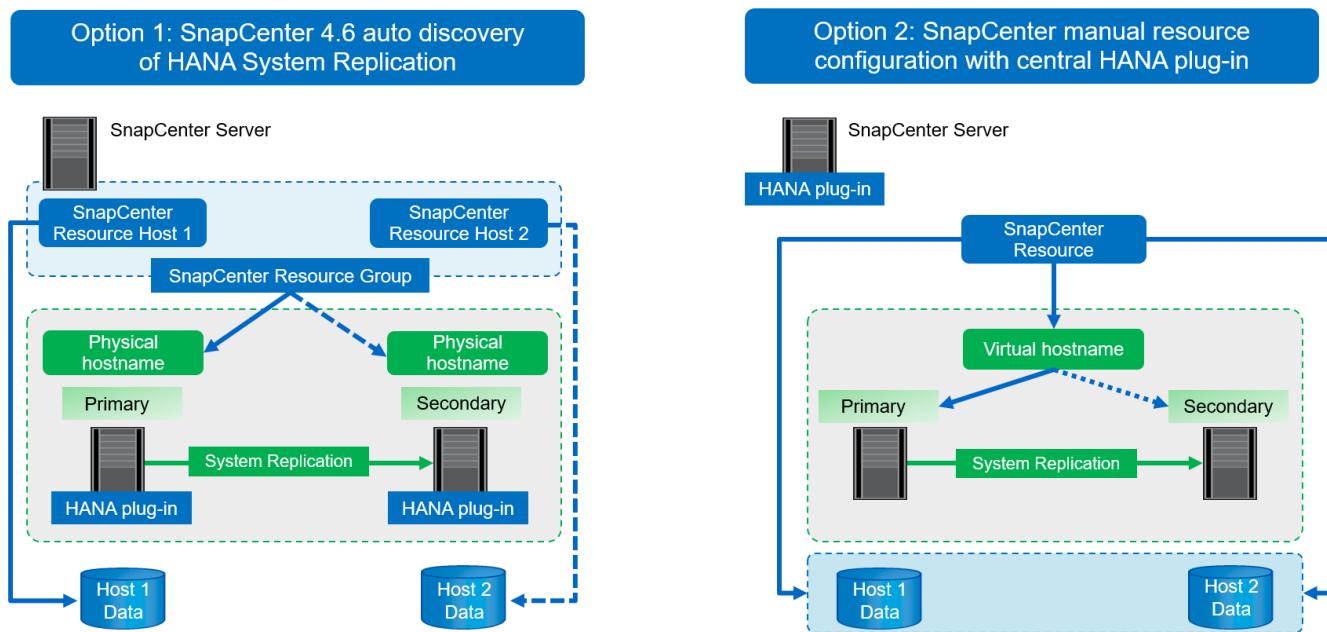
The backup created at host 2 can be restored directly at the storage layer. If you must use a backup created at host 1, then the backup must be copied from the host 1 storage volume to the host 2 storage volume. Forward recovery uses the log backups from both hosts.



# 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.

	<b>Resource group with SnapCenter 4.6</b>	<b>Single SnapCenter resource and virtual IP address</b>
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

	<b>Resource group with SnapCenter 4.6</b>	<b>Single SnapCenter resource and virtual IP address</b>
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.
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.

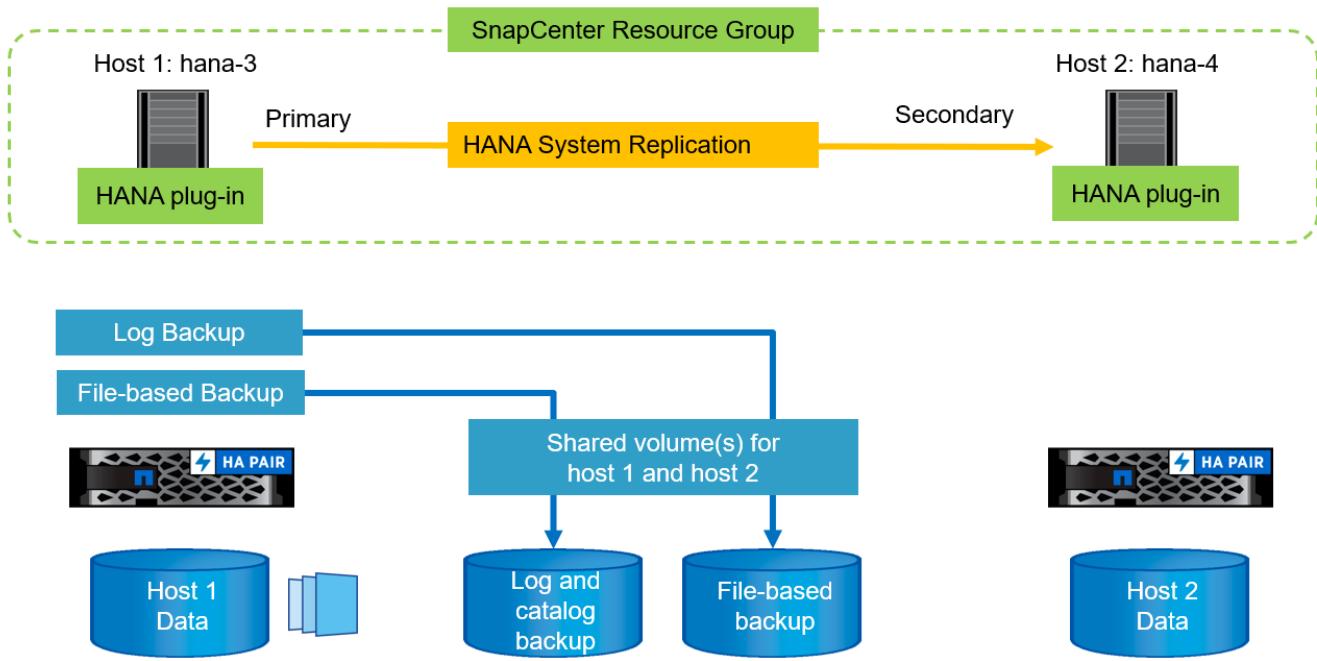
```
ss2adm@hana- 3: / > hdbuserstore set SS2KEY hana- 3:33313 SNAPCENTER
<password>
```

```
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.



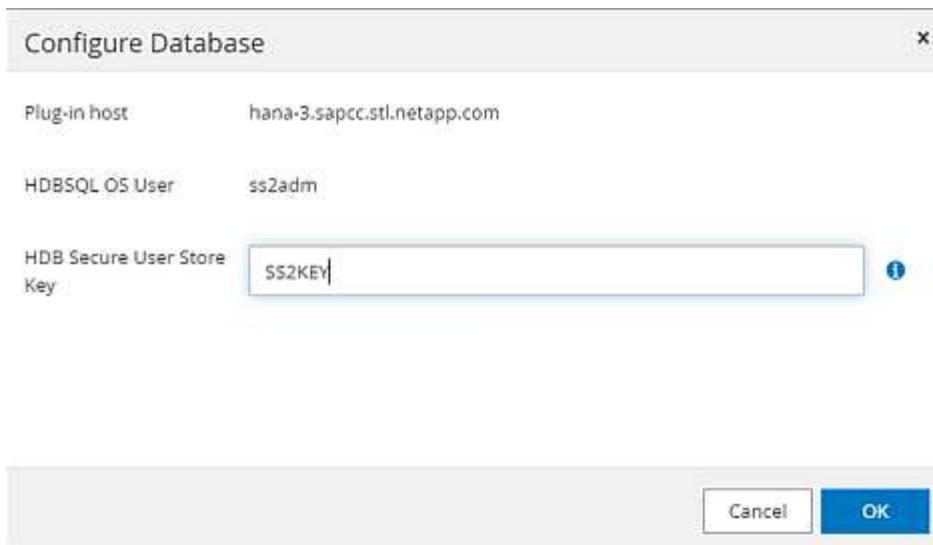
After you have installed the SnapCenter HANA plug-in on both HANA hosts, the HANA systems are shown in the SnapCenter resource view in the same way as other autodiscovered resources. Starting with SnapCenter 4.6, an additional column is displayed that shows the status of HANA system replication (enabled/disabled,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

The screenshot shows the NetApp SnapCenter interface with the "SAP HANA" view selected. The left sidebar includes "Dashboard", "Resources" (selected), "Monitor", "Reports", "Hosts", "Storage Systems", "Settings", and "Alerts". The main table displays two HANA resources:

	System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
1	SS2	SS2	SS2	Enabled (Primary)	hana-3.sapcc.stl.netapp.com				Not protected
2	SS2	SS2	SS2	Enabled (Secondary)	hana-4.sapcc.stl.netapp.com				Not protected

The "Replication" column for both resources is highlighted with a blue oval.

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



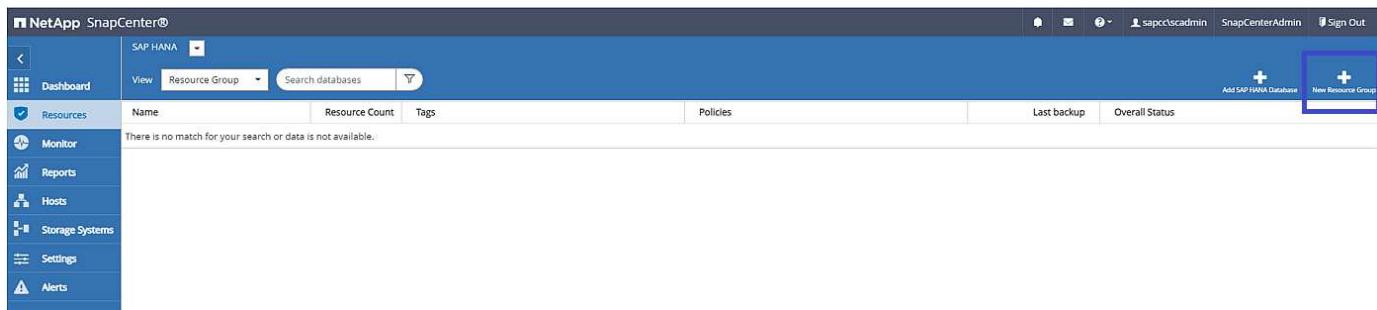
Additional autodiscovery steps are executed, and SnapCenter show the resource details. With SnapCenter 4.6, the system replication status and the secondary server are listed in this view.

System			
System	SS2		
SS2			
Details for selected resource			
Type	Multitenant Database Container		
HANA System Name	SS2		
SID	SS2		
Tenant Databases	SS2		
Plug-in Host	hana-3.sapcc.stl.netapp.com		
HDB Secure User Store Key	SS2KEY		
HDBSQL OS User	ss2adm		
Log backup location	/mnt/backup/SS2		
Backup catalog location	/mnt/backup/SS2		
System Replication	Enabled (Primary)		
Secondary Servers	hana-4		
plugin name	SAP HANA		
Last backup	None		
Resource Groups	None		
Policy	None		
Discovery Type	Auto		
Storage Footprint			
SVM	Volume	Junction Path	LUN/Qtree
hana-primary.sapcc.stl.netapp.com	SS2_data_mnt00001	/SS2_data_mnt00001	

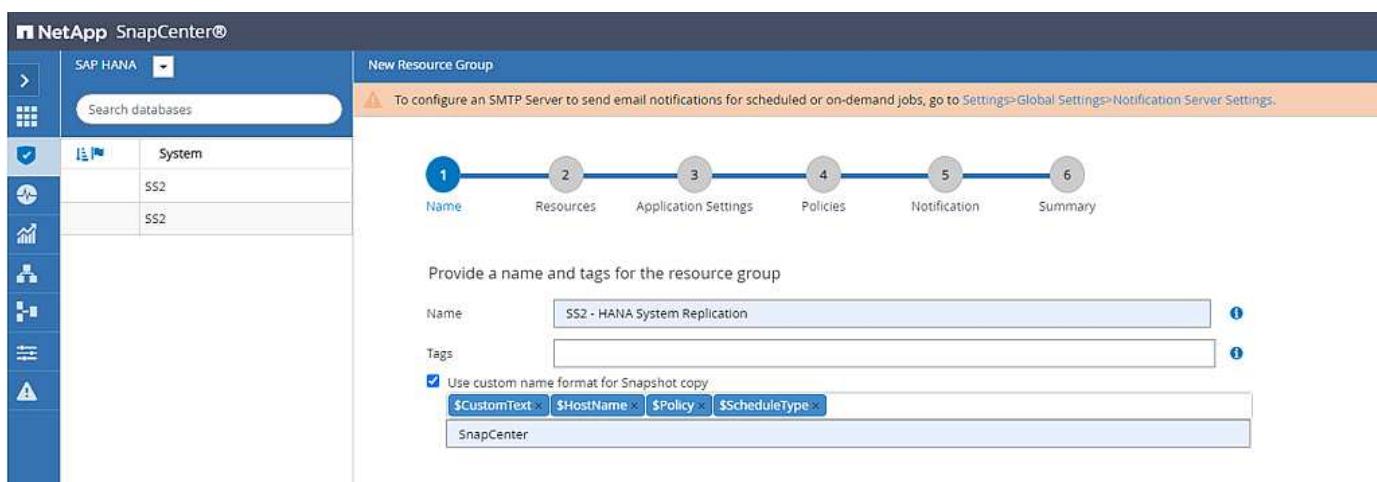
After performing the same steps for the second HANA resource, the autodiscovery process is complete and both HANA resources are configured in SnapCenter.

Resources		System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
SS2	SS2	SS2	SS2	Enabled (Primary)	hana-3.sapcc.stl.netapp.com					Not protected
SS2	SS2	SS2	SS2	Enabled (Secondary)	hana-4.sapcc.stl.netapp.com					Not protected

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.



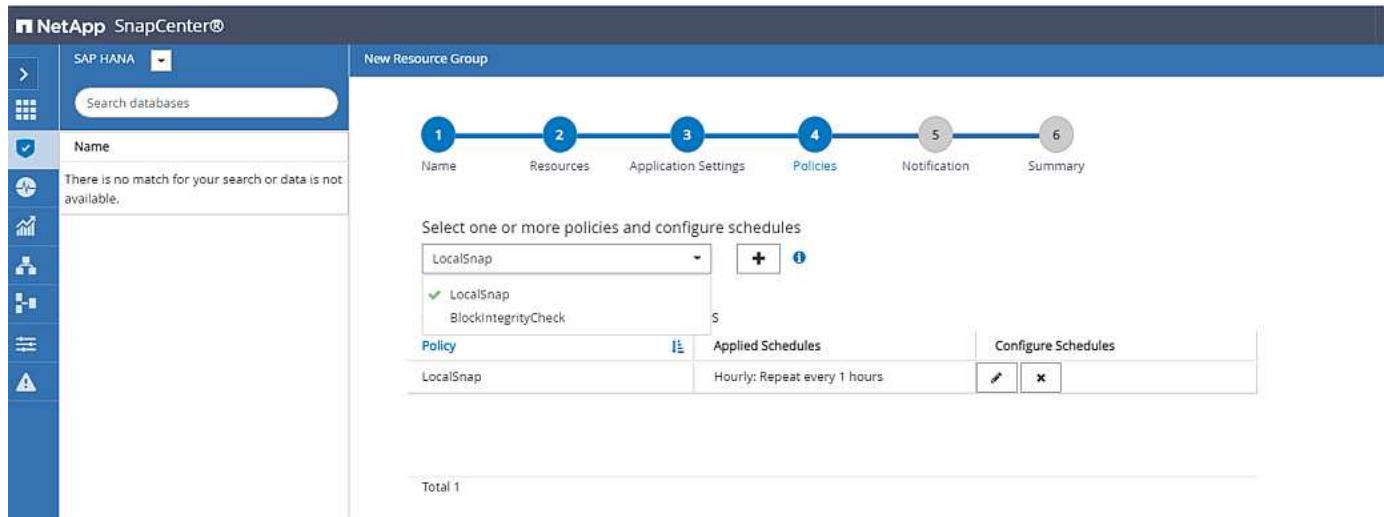
You must add both HANA hosts to the resource group.

&gt;' and '&lt;' are visible between the two lists." data-bbox="75 580 919 910"/&gt;

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.

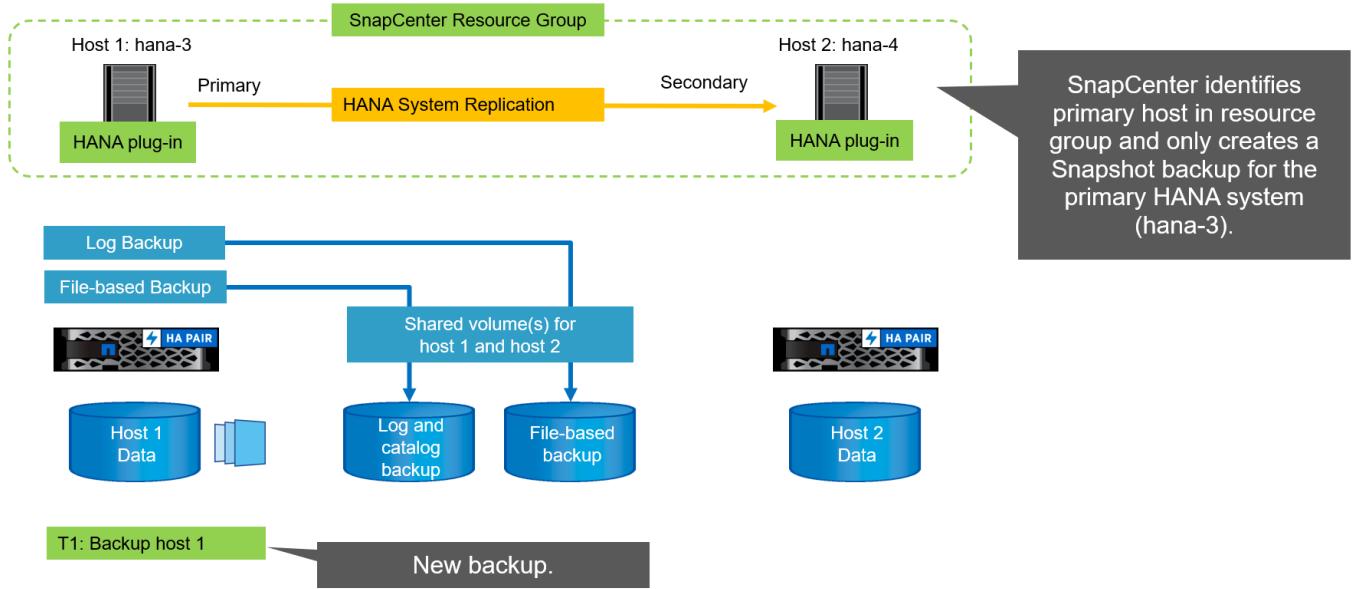


The resource group configuration is now finished and backups can be executed.

The top screenshot shows the 'SS2 - HANA System Replication Details' page with two hosts listed: 'hana-3.sapcc.stl.netapp.com' and 'hana-4.sapcc.stl.netapp.com'. The bottom screenshot shows the 'Resources' dashboard with two systems listed: 'SS2' and 'SS2'. Both systems are marked as 'Enabled (Primary)' and are associated with 'hana-3.sapcc.stl.netapp.com' and 'hana-4.sapcc.stl.netapp.com' respectively. The 'Resource Groups' and 'Policies' columns show 'SS2 - HANA System Replication' and 'LocalSnap'.

## 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.

Job Details

Backup of Resource Group 'SS2 - HANA System Replication' with policy 'LocalSnap'

✓ ▾ Backup of Resource Group 'SS2 - HANA System Replication' with policy 'LocalSnap'

    ✓ ▾ Refresh HANA replication resources on host(s): hana-3.sapcc.stl.netapp.com, hana-4.sapcc.stl.netapp.com

    ✓ ▾ hana-3.sapcc.stl.netapp.com

    ✓ ▾ Backup

        ✓ ▾ Validate Dataset Parameters

        ✓ ▾ Validate Plugin Parameters

        ✓ ▾ Complete Application Discovery

        ✓ ▾ Initialize Filesystem Plugin

        ✓ ▾ Discover Filesystem Resources

        ✓ ▾ Validate Retention Settings

        ✓ ▾ Quiesce Application

        ✓ ▾ Quiesce Filesystem

        ✓ ▾ Create Snapshot

        ✓ ▾ UnQuiesce Filesystem

        ✓ ▾ UnQuiesce Application

        ✓ ▾ Get Snapshot Details

        ✓ ▾ Get Filesystem Meta Data

        ✓ ▾ Finalize Filesystem Plugin

        ✓ ▾ Collect Autosupport data

        ✓ ▾ Register Backup and Apply Retention

        ✓ ▾ Register Snapshot attributes

        ✓ ▾ Application Clean-Up

Task Name: Backup Start Time: 12/13/2021 8:35:33 AM End Time:

[View Logs](#) [Cancel Job](#) [Close](#)

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

NetApp SnapCenter®

SAP HANA

SS2 - HANA System Replication ...

SS2 Topology

Name: SS2 - HANA System Replication

Manage Copies

1 Backup 0 Clones

Local copies

Primary Backup(s)

Backup Name: SnapCenter\_hana-3\_LocalSnap\_Hourly\_12-13-2021\_08:35:30.7075

Count: 1 End Date: 12/13/2021 8:36:32 AM

Summary Card

1 Backup

1 Snapshot based backup

0 File-Based backups

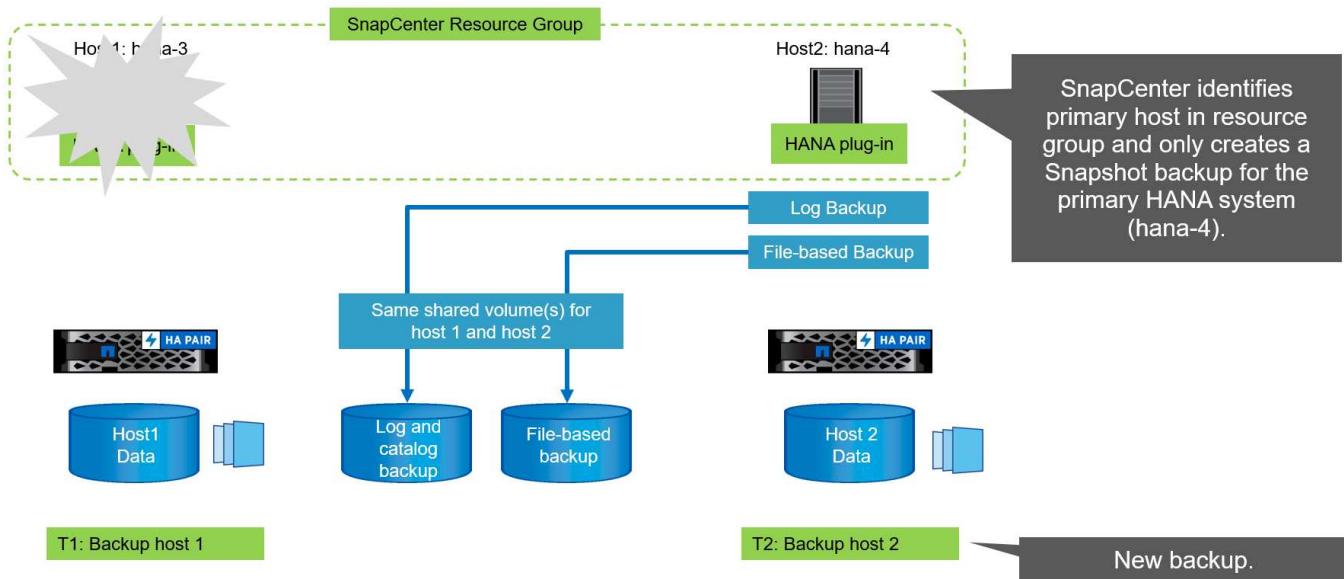
0 Clones

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.

Job Details

Backup of Resource Group 'SS2 - HANA System Replication' with policy 'LocalSnap'

- ✓ ▾ Backup of Resource Group 'SS2 - HANA System Replication' with policy 'LocalSnap'
  - ✓ ▾ Refresh HANA replication resources on host(s): hana-3.sapcc.stl.netapp.com, hana-4.sapcc.stl.netapp.com
  - ✓ ▾ hana-4.sapcc.stl.netapp.com
    - ✓ Backup
    - ✓ ▶ Validate Dataset Parameters
    - ✓ ▶ Validate Plugin Parameters
    - ✓ ▶ Complete Application Discovery
    - ✓ ▶ Initialize Filesystem Plugin
    - ✓ ▶ Discover Filesystem Resources
    - ✓ ▶ Validate Retention Settings
    - ✓ ▶ Quiesce Application
    - ✓ ▶ Quiesce Filesystem
    - ✓ ▶ Create Snapshot
    - ✓ ▶ UnQuiesce Filesystem
    - ✓ ▶ UnQuiesce Application
    - ✓ ▶ Get Snapshot Details
    - ✓ ▶ Get Filesystem Meta Data
    - ✓ ▶ Finalize Filesystem Plugin
    - ✓ ▶ Collect Autosupport data
    - ✓ ▶ Register Backup and Apply Retention
    - ✓ ▶ Register Snapshot attributes
    - ✓ ▶ Application Clean-Up

Task Name: Backup Start Time: 12/13/2021 8:56:44 AM End Time:

[View Logs](#) [Cancel Job](#) [Close](#)

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

NetApp SnapCenter®

SAP HANA SS2 - HANA System Replication ... SS2 Topology

System Resource Name SS2

Manage Copies 1 Backup 0 Clones Local copies

Summary Card 1 Backup 1 Snapshot-based backup 0 File-based backups 0 Clones

Primary Backup(s)

Backup Name	Count	End Date
SnapCenter_hana-4_LocalSnap_Hourly_12-13-2021_08:56:42.1331	1	12/13/2021 8:57:41 AM

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.

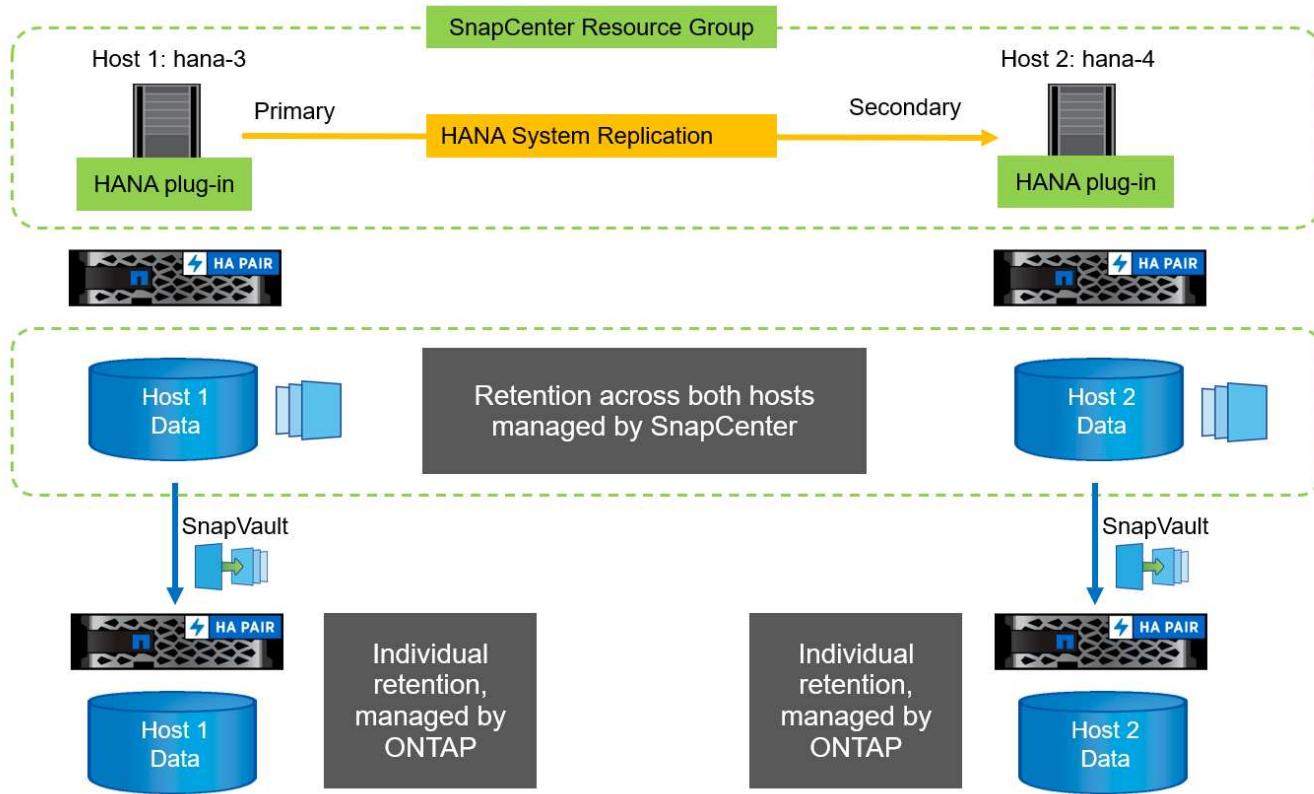


If a takeover to the secondary host is not performed for a long time, the number of changed blocks for the first SnapVault update at the secondary host will be high.

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 be 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.



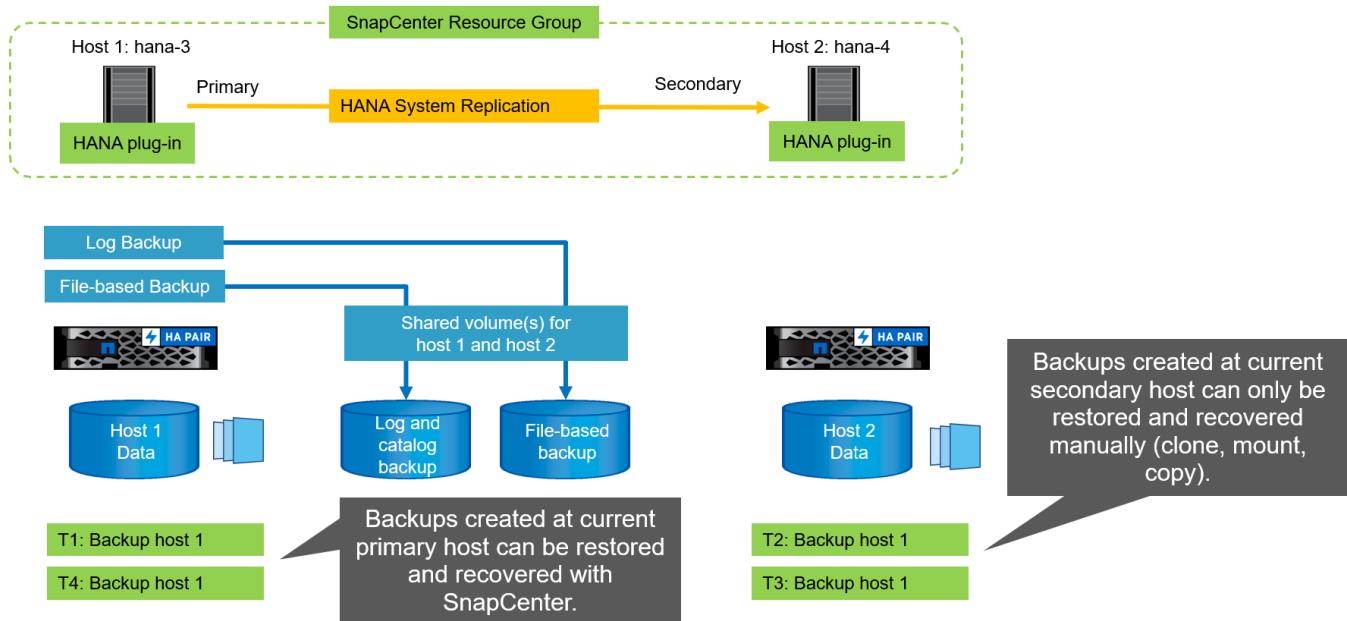
## Retention management

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 [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

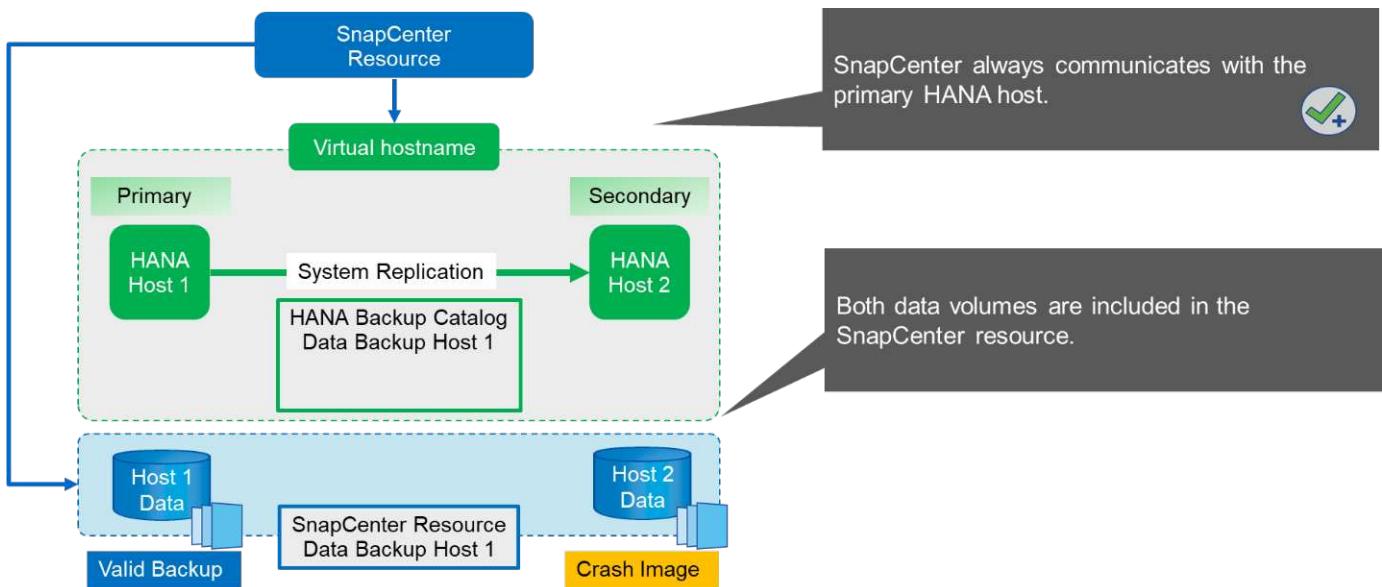
A SnapCenter resource is configured with the virtual IP address (host name) of the HANA System Replication environment. With this approach, SnapCenter always communicates with the primary host, regardless of whether host 1 or host 2 is primary. The data volumes of both SAP HANA hosts are included in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

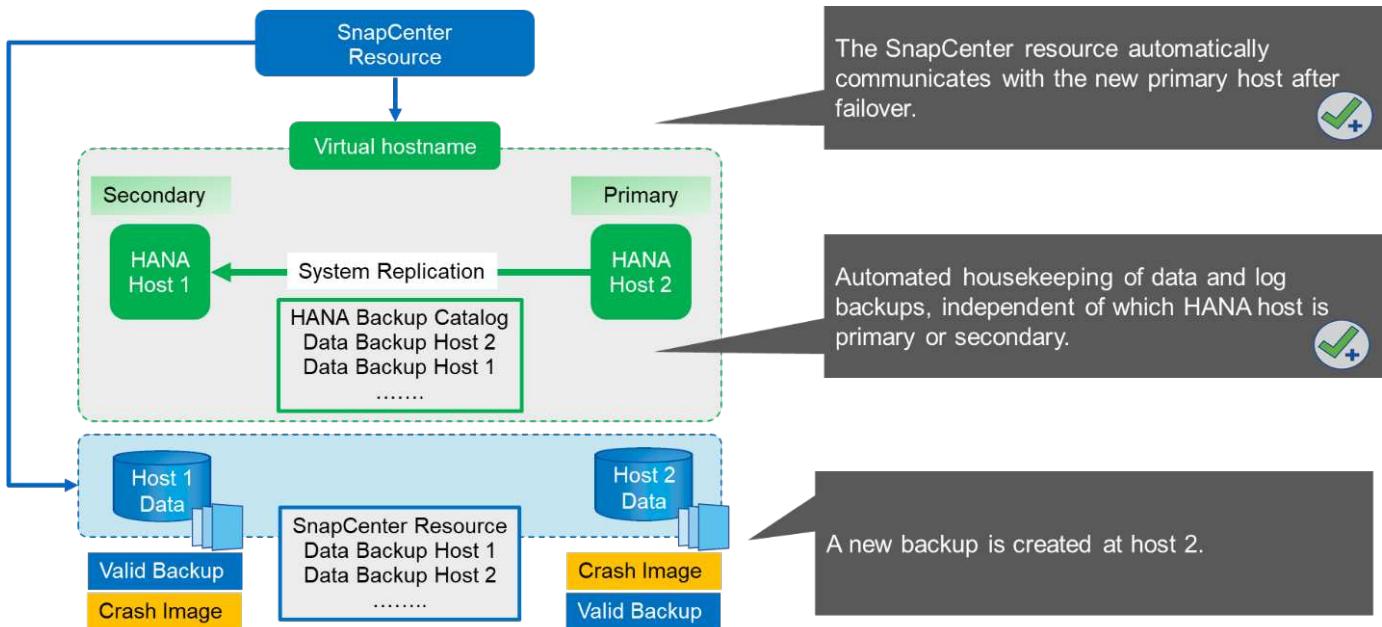
When a backup is executed with host 1 as the primary host, a database-consistent Snapshot backup is created at the data volume of host 1. Because the data volume of host 2 is part of the SnapCenter resource, another Snapshot copy is created for this volume. This Snapshot copy is not database consistent;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

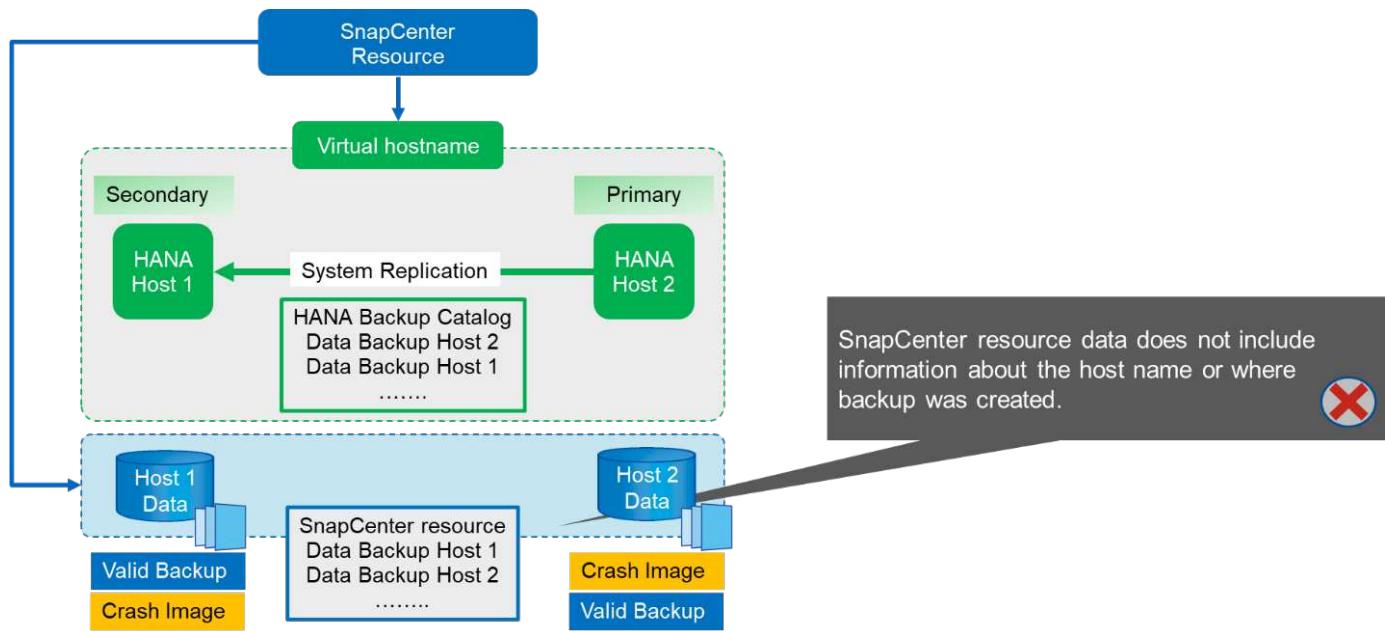


As discussed in the section [Storage Snapshot Backups and SAP System Replication](#), a restore operation with storage-based Snapshot backups is different, depending on which backup must be restored. It is important to identify which host the backup was created at to determine if the restore can be performed 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

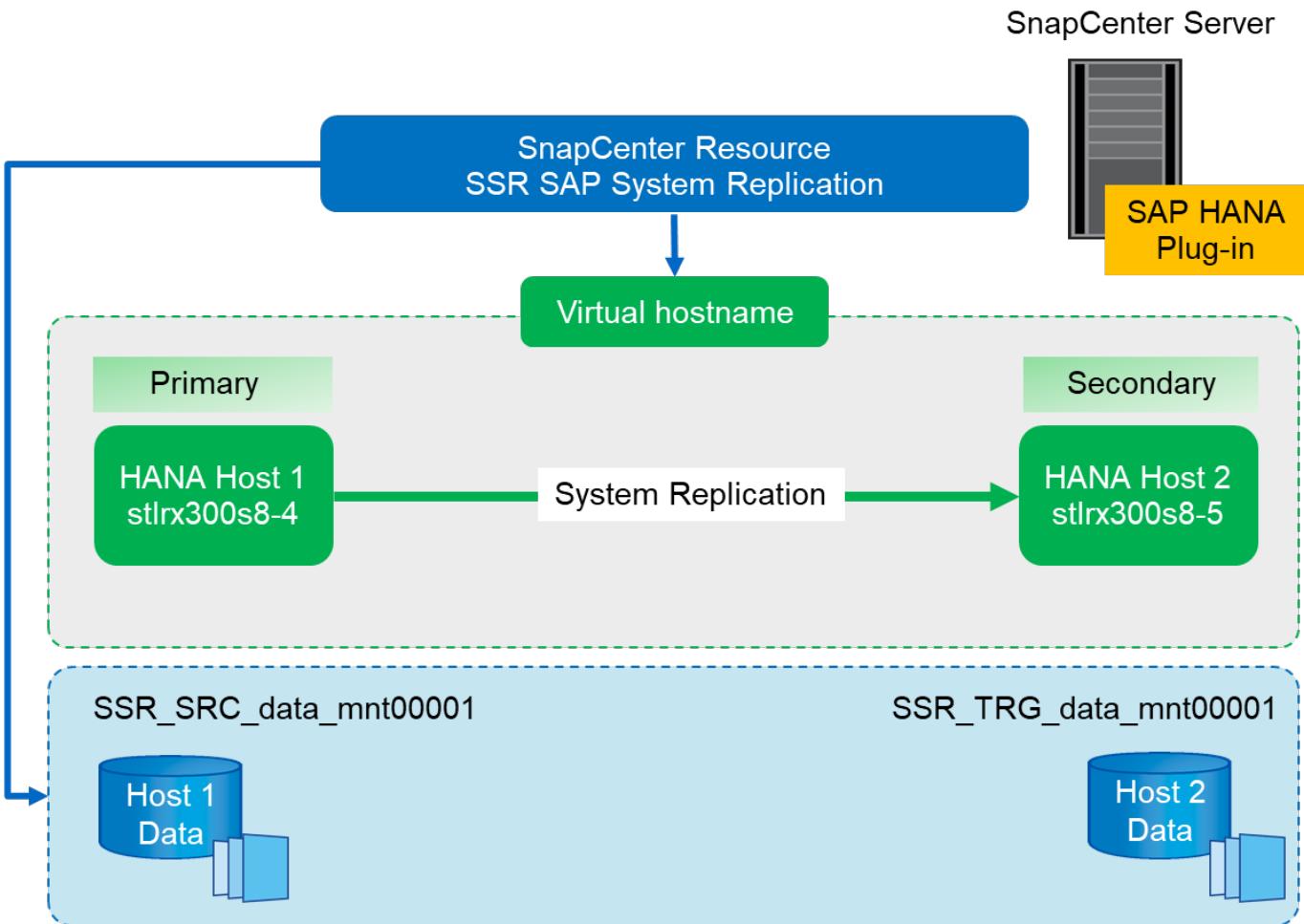
identify which host is currently the primary SAP HANA host.

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.

Add SAP HANA Database

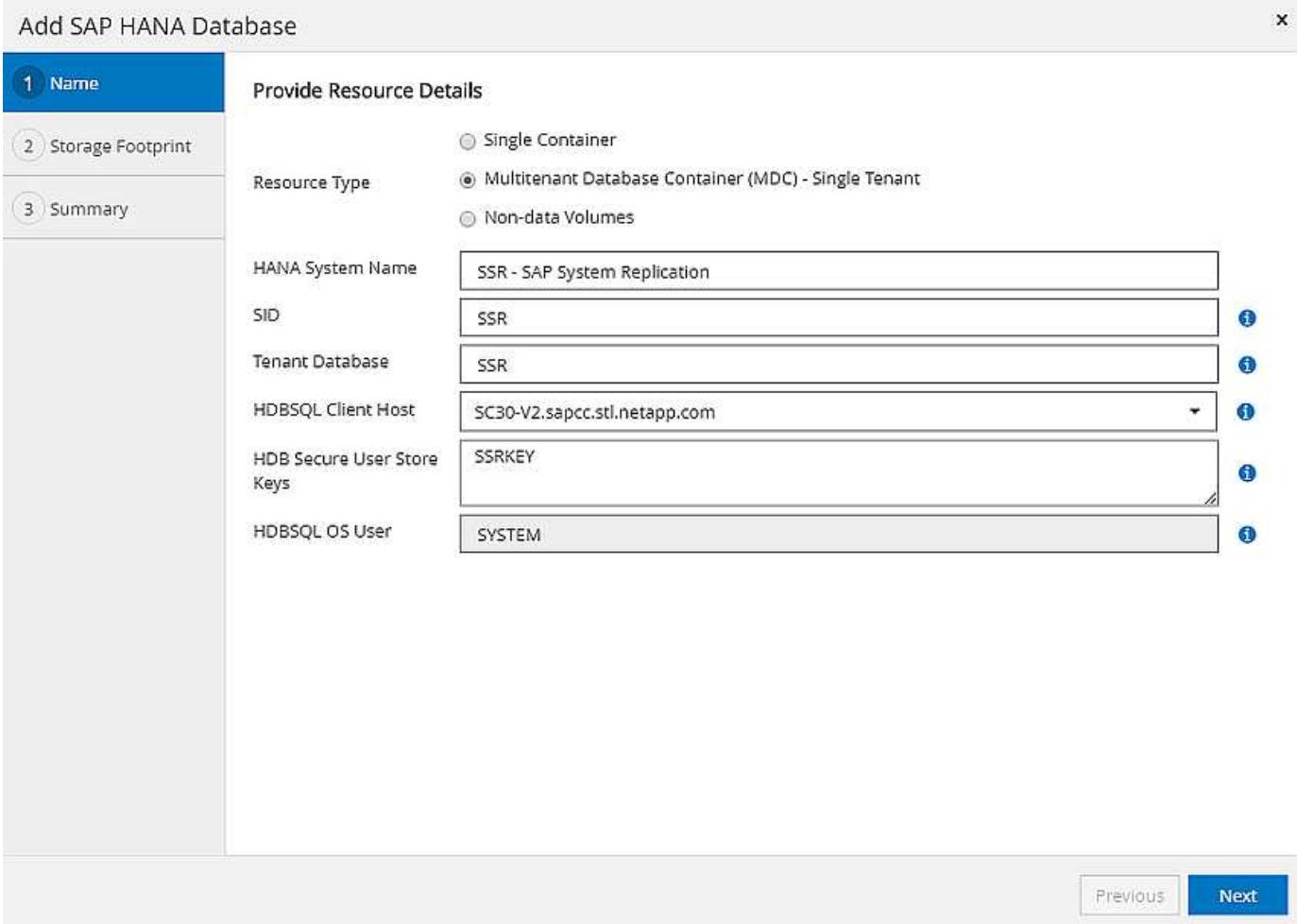
**1 Name**

**Provide Resource Details**

Resource Type  Multitenant Database Container (MDC) - Single Tenant  Single Container  Non-data Volumes

HANA System Name	SSR - SAP System Replication
SID	SSR
Tenant Database	SSR
HDBSQL Client Host	SC30-V2.sapcc.sti.netapp.com
HDB Secure User Store Keys	SSRKEY
HDBSQL OS User	SYSTEM

**Previous** **Next**



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

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Resource Settings

4 Summary

Provide Storage Footprint Details

Storage Systems for storage footprint

hana

Modify hana

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

Volume Name	LUNs or Qtrees
SSR_TRG_data_mnt00001	Default is 'None' or type to find
SSR_SRC_data_mnt00001	Default is 'None' or type to find

Save

Previous

Next

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
```

x

## 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.

Host	Service	Size	Name	Source Type	EBID
strlx300s8-4	nameserver	1.47 GB	hdb0001	volume	SnapC...

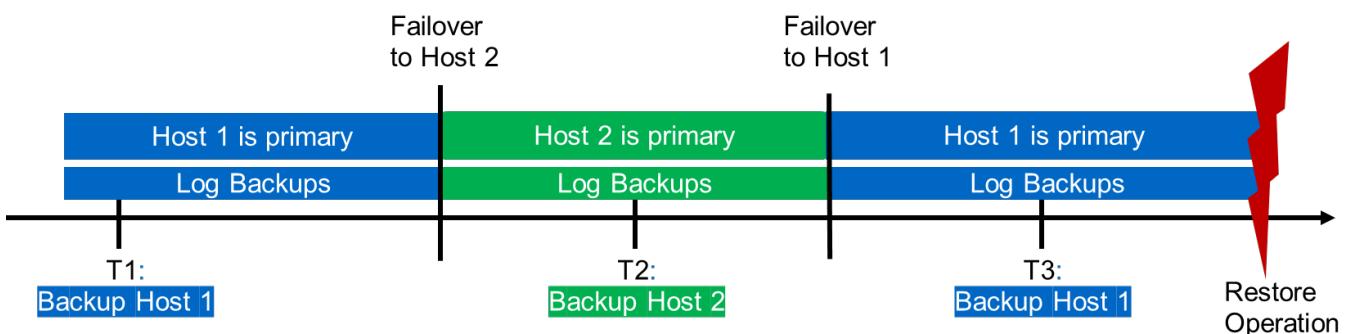
## Restore and recovery

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

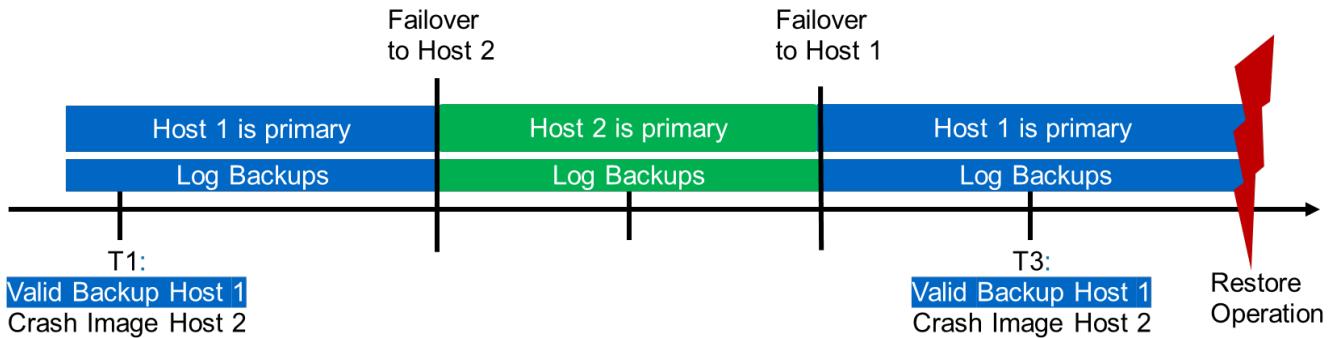
With a single SnapCenter resource configuration, Snapshot copies are created at both storage volumes of both SAP HANA System Replication hosts. Only the Snapshot backup that is created at the storage volume of the primary SAP HANA host is valid to use for forward recovery. The Snapshot copy created at 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 image. The 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.

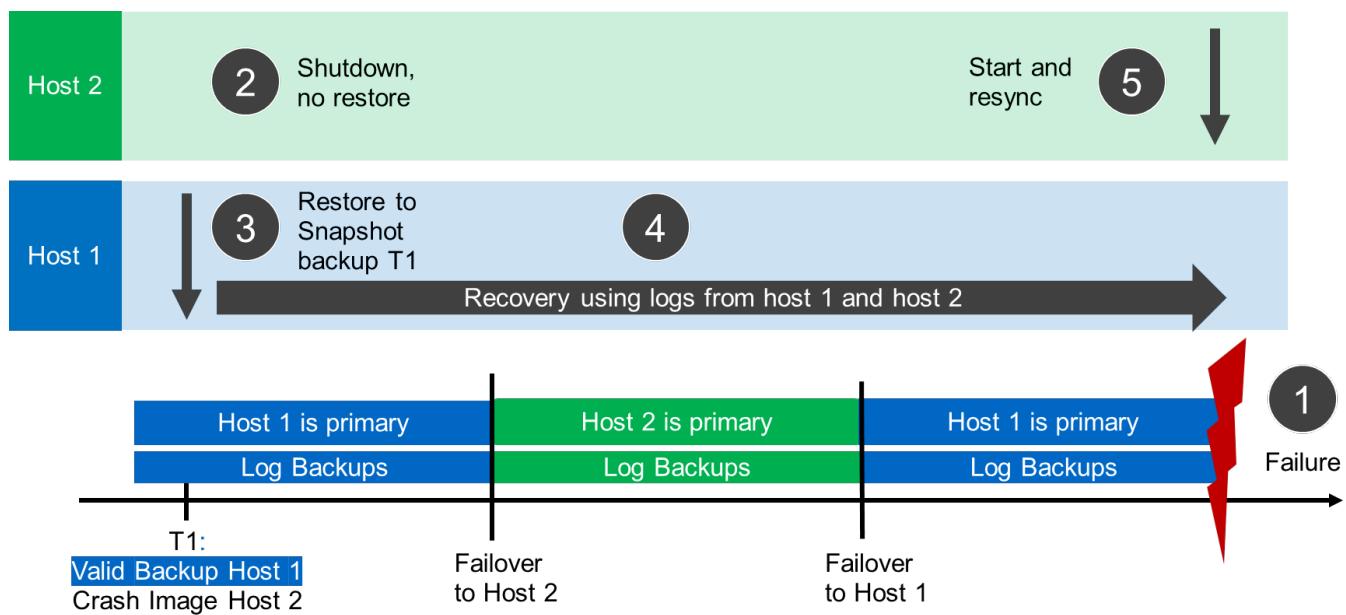


### SnapCenter restore of the valid backup only

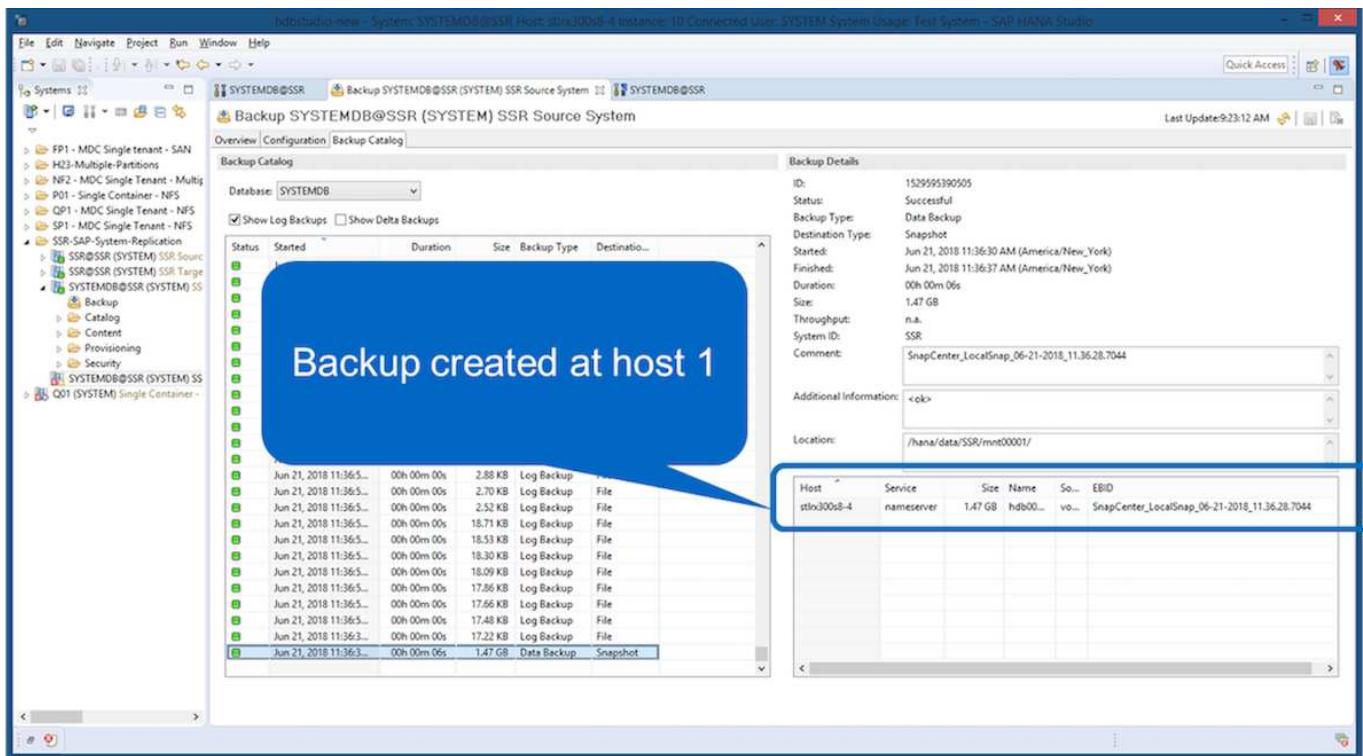
The following figure shows an overview of the restore and recovery scenario described in this section.

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.



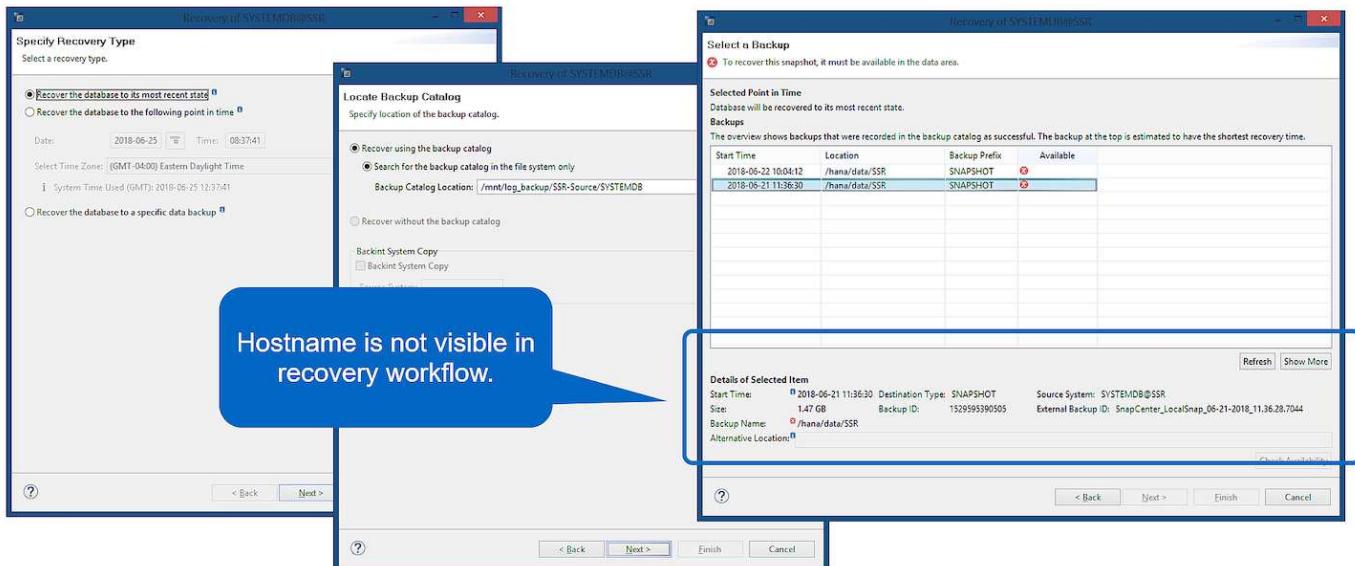
The following figure shows the SAP HANA backup catalog in SAP HANA Studio. The highlighted backup shows the backup created at T1 at host 1.



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.

i 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.

26

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.



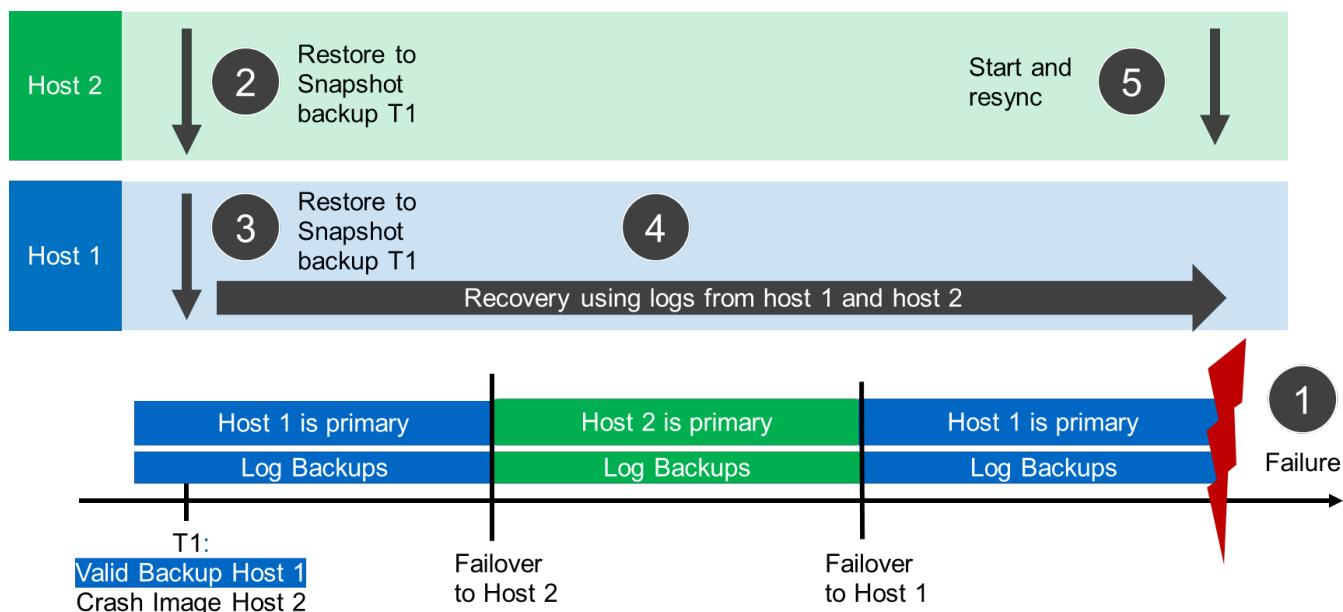
Even though the secondary host is up-to-date (no restore operation was performed for host 2), SAP HANA executes a full replication of all data. This behavior is standard after a restore and recovery operation with SAP HANA System Replication.

## 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.

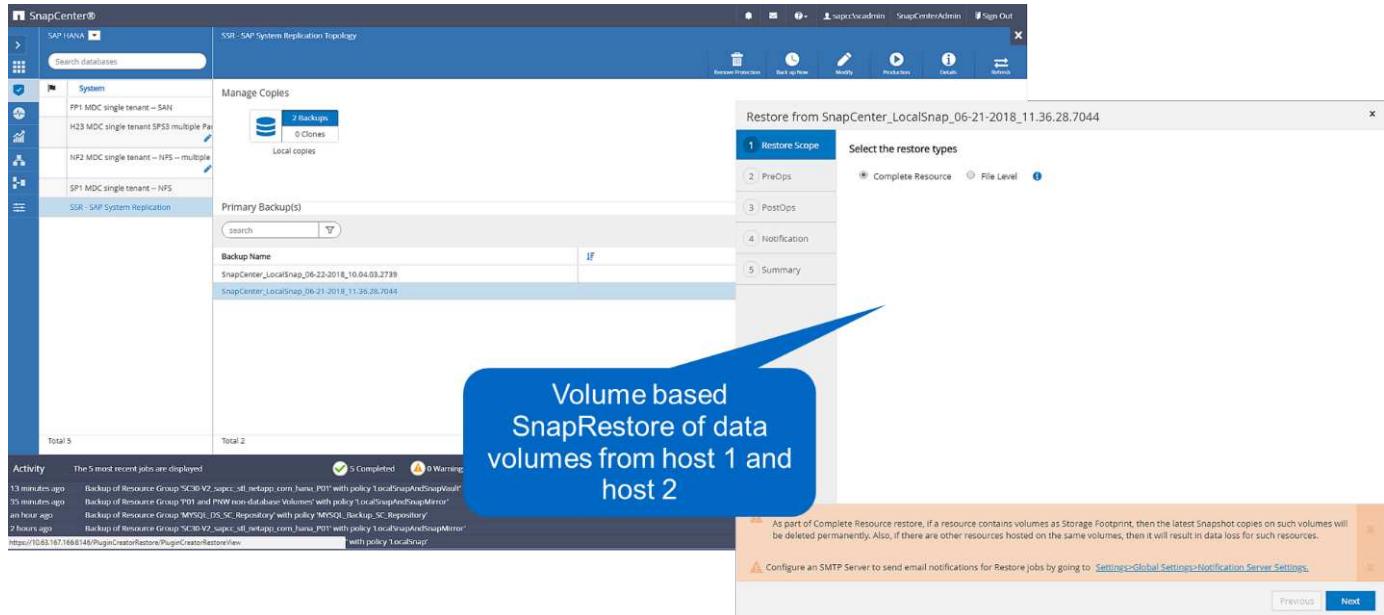
1. A failure occurred and you must restore to the backup created at T1 at host 1.
2. The secondary host (host 2) is shut down and the T1 crash image is restored.
3. The storage volume of host 1 is restored to the backup created at T1.
4. A forward recovery is performed with logs from host 1 and host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



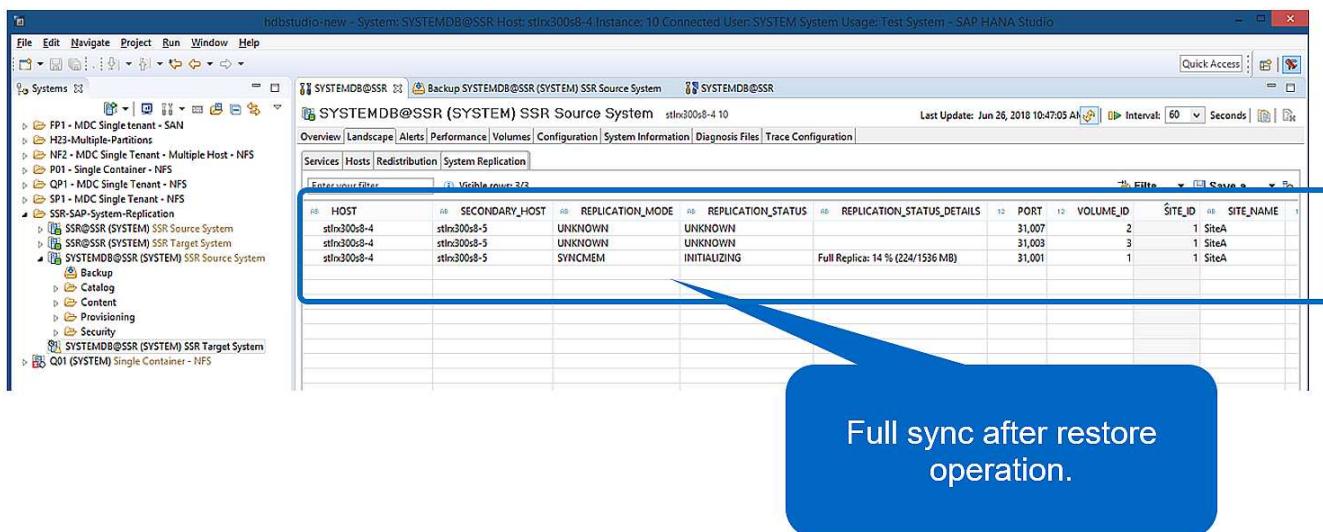
The restore and recovery operation with SAP HANA Studio is identical to the steps described in the section

## 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

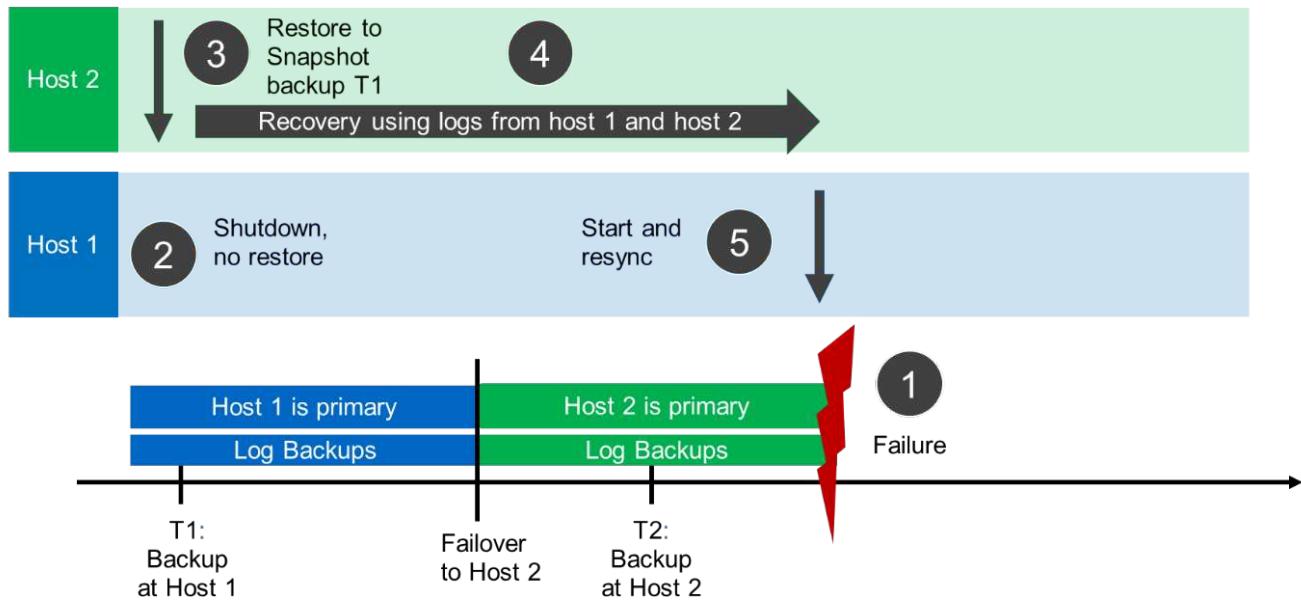
A restore operation from a backup that has been created at the other SAP HANA host is a valid scenario for both SnapCenter configuration options.

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 screenshot shows the SAP HANA Backup Catalog for the SYSTEMDB@SSR database. The catalog lists three backups:

Status	Started	Duration	Size	Backup Type	Destination
Success	Jun 28, 2018 9:23:46 AM	00h 00m 07s	1.55 GB	Data Backup	File
Success	Jun 27, 2018 7:45:56 AM	00h 00m 03s	1.52 GB	Data Backup	Snapshot
Success	Jun 27, 2018 7:12:37 AM	00h 00m 06s	1.55 GB	Data Backup	Snapshot

**Backup Details:**

- ID: 153009795715
- Status: Successful
- Backup Type: Data Backup
- Destination Type: Snapshot
- Started: Jun 27, 2018 7:12:37 AM (America/New\_York)
- Finished: Jun 27, 2018 7:12:43 AM (America/New\_York)
- Duration: 00h 00m 06s
- Size: 1.55 GB
- Throughput: n.a.
- System ID: SSR
- Comment: SnapCenter\_LocalSnap\_06-27-2018\_07.12.29.1232

**Additional Information:** <ok>

**Location:** /hana/data/SSR/mnt0001/

**Host:**

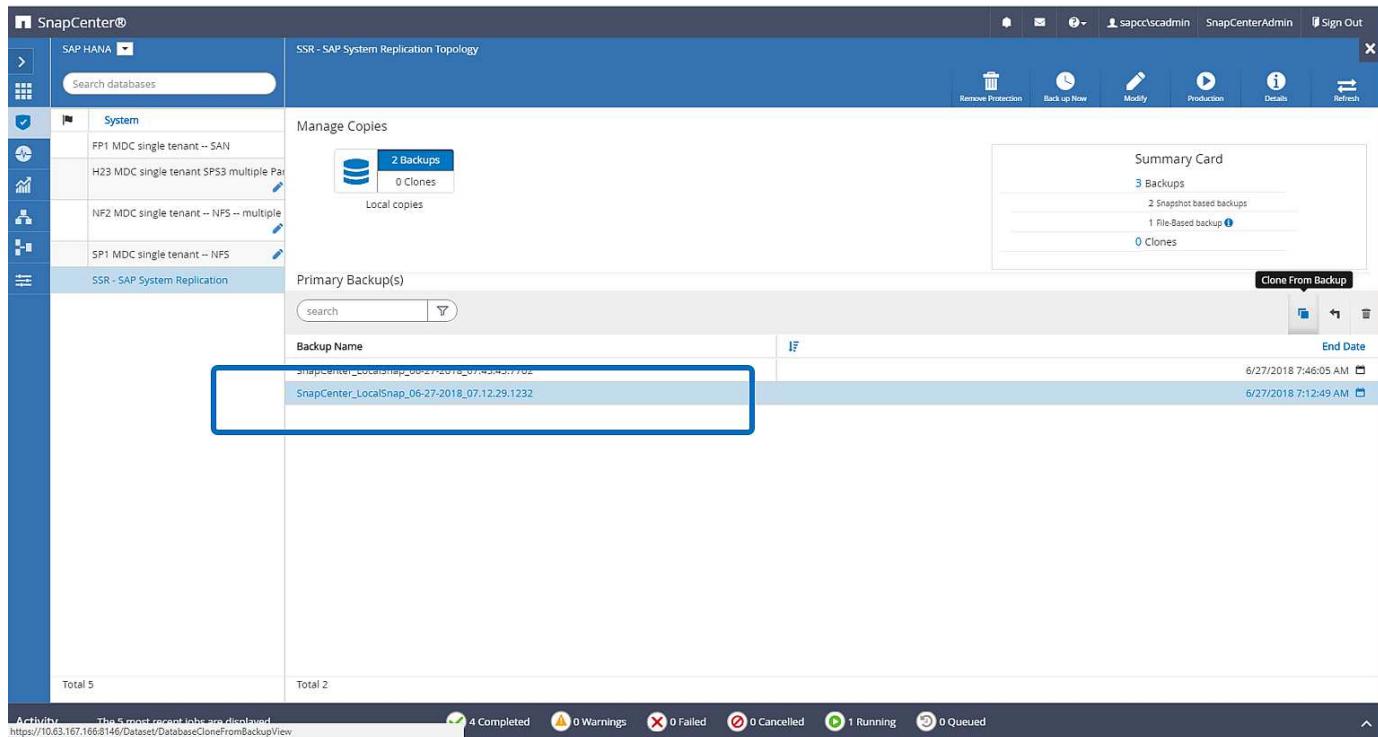
Host	Service	Size	Name	Source Type	EBID
stln3008-4	nameserver	1.55 GB	hdb00001	volume	SnapC...

30

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.



The screenshot shows the SnapCenter interface for managing SAP HANA backups. The left sidebar shows a tree structure with 'System' and 'SSR - SAP System Replication' selected. The main pane displays 'Manage Copies' with '2 Backups' and '0 Clones'. The 'Primary Backup(s)' table lists two backups. The second backup, 'SnapCenter\_LocalSnap\_06-27-2018\_07.12.29.1232', is highlighted with a blue box. On the right, a 'Summary Card' shows '3 Backups' (2 Snapshot based backups, 1 File-Based backup) and '0 Clones'. A 'Clone From Backup' button is located in the top right of the main pane.

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.

Clone from Backup

1 Location      2 Scripts      3 Notification      4 Summary

Select the host to create the clone

Clone server: stirx300s8-7.stl.netapp.com

Clone suffix: \_clone\_date\_time

NFS Export IP Address: 192.168.173.71

Any host with HANA can be used. Note: install the System R

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

Previous      Next

Any host with installed HANA plug-in can be used. Not required to install the plug-in on the System Replication 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](#)
- [Automating SAP HANA System Copy and Clone Operations with SnapCenter](#)
- SAP HANA Disaster Recovery with Storage Replication

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

## Version history

Version History:

Version	Date	Document Version History
Version 1.0	October 2018	Initial version
Version 2.0	January 2022	Update to cover SnapCenter 4.6 HANA System Replication support

## Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

**LIMITED RIGHTS LEGEND:** Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.