



Backup y recuperación de datos de replicación de sistemas SAP HANA con SnapCenter

NetApp Solutions SAP

NetApp
March 11, 2024

This PDF was generated from <https://docs.netapp.com/es-es/netapp-solutions-sap/backup/saphana-sr-scs-sap-hana-system-replication-overview.html> on March 11, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Backup y recuperación de datos de replicación de sistemas SAP HANA con SnapCenter 1
 - TR-4719: Replicación de sistemas SAP HANA: Backup y recuperación de datos con SnapCenter..... 1
 - Backups de Storage Snapshot y replicación de sistemas SAP 2
 - Opciones de configuración de SnapCenter para la replicación de sistemas SAP..... 4
 - Configuración de SnapCenter 4.6 mediante un grupo de recursos 5
 - Configuración de SnapCenter con un solo recurso 16
 - Restauración y recuperación a partir de un backup creado en el otro host..... 29
 - Dónde encontrar información adicional 34
 - Historial de versiones..... 34

Backup y recuperación de datos de replicación de sistemas SAP HANA con SnapCenter

TR-4719: Replicación de sistemas SAP HANA: Backup y recuperación de datos con SnapCenter

Nils Bauer: NetApp

La replicación de sistemas SAP HANA se suele usar como solución de alta disponibilidad o recuperación ante desastres para bases de datos SAP HANA. La replicación de sistemas SAP HANA ofrece diferentes modos de funcionamiento que puede utilizar en función del caso de uso o los requisitos de disponibilidad.

Existen dos casos de uso principales que pueden combinarse:

- Alta disponibilidad con un objetivo de punto de recuperación (RPO) de cero y un objetivo de tiempo de recuperación (RTO) mínimo mediante un host SAP HANA secundario dedicado.
- Recuperación ante desastres a gran distancia. El host SAP HANA secundario también se puede usar para desarrollo o pruebas durante el funcionamiento normal.

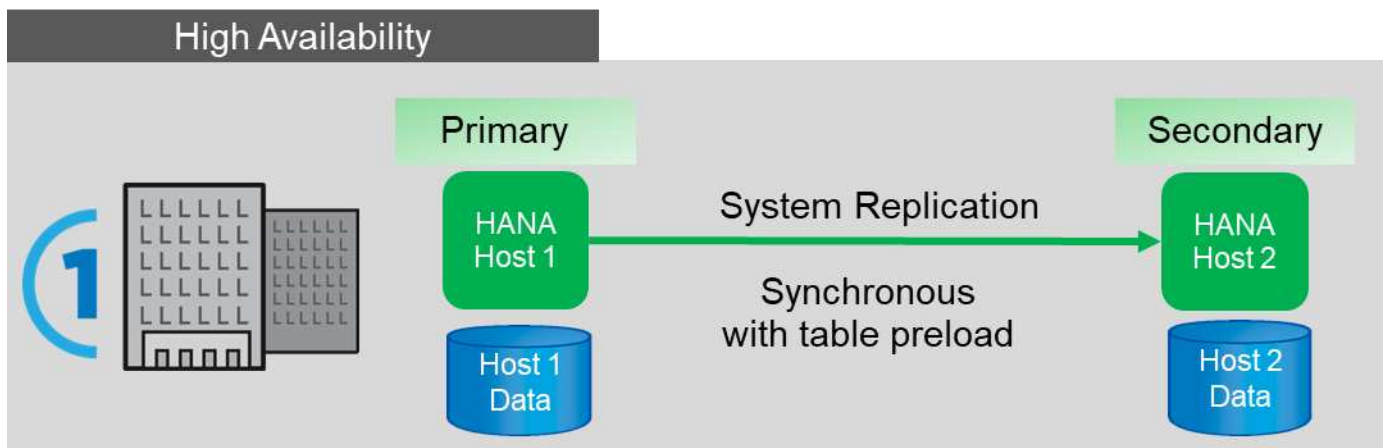
Alta disponibilidad con un objetivo de punto de recuperación de cero y un objetivo de tiempo de recuperación mínimo

La replicación del sistema se configura con la replicación síncrona mediante tablas precargadas en la memoria en el host secundario de SAP HANA. Esta solución de alta disponibilidad se puede usar para solucionar fallos de hardware o software y también para reducir el tiempo de inactividad planificado durante las actualizaciones de software SAP HANA (operaciones de tiempo de inactividad casi cero).

Las operaciones de conmutación por error a menudo se automatizan usando software de clúster de terceros o con un flujo de trabajo de un clic con el software SAP Landscape Management.

Desde la perspectiva de requisito de backup, debe poder crear backups independientemente de qué host de SAP HANA sea primario o secundario. Se usa una infraestructura de backup compartida para restaurar cualquier backup, independientemente del host en el que se haya creado el backup.

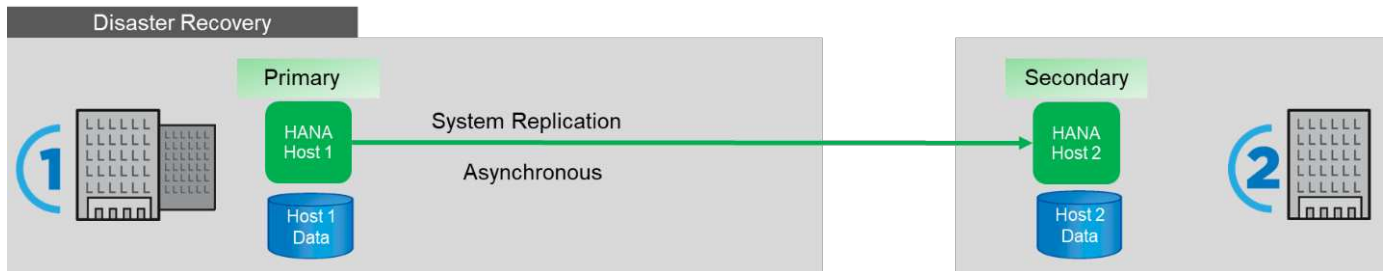
El resto de este documento se centra en operaciones de backup con la replicación de sistemas SAP configurada como solución de alta disponibilidad.



Recuperación ante desastres a gran distancia

La replicación del sistema se puede configurar con la replicación asíncrona sin que la tabla quede precargada en la memoria del host secundario. Esta solución se utiliza para resolver los fallos del centro de datos y, por lo general, las operaciones de conmutación por error se realizan manualmente.

En relación con los requisitos de backup, debe poder crear backups durante el funcionamiento normal en el centro de datos 1 y durante la recuperación ante desastres en el centro de datos 2. Hay una infraestructura de backup independiente disponible en los centros de datos 1 y 2, y las operaciones de backup se activan como parte de la recuperación ante desastres. La infraestructura de backup no suele estar compartida y no es posible realizar una operación de restauración de un backup creado en el otro centro de datos.



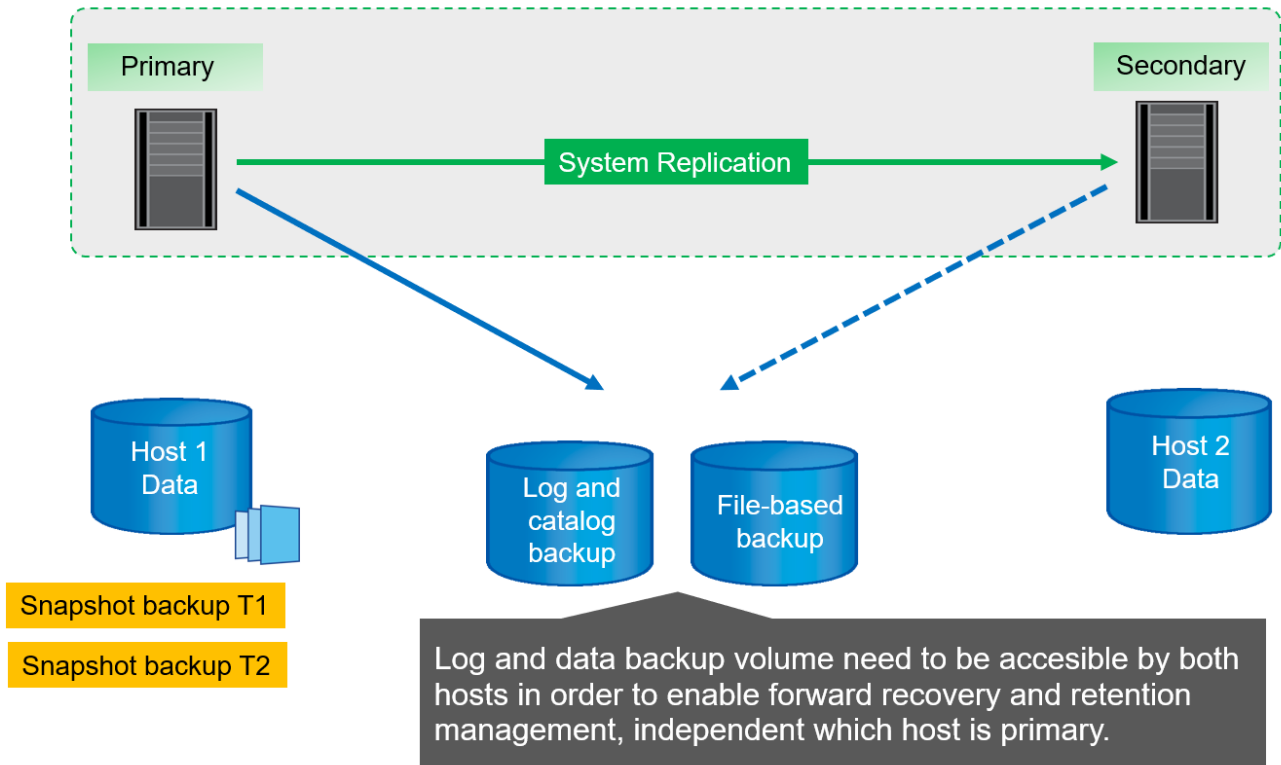
Backups de Storage Snapshot y replicación de sistemas SAP

Las operaciones de backup siempre se realizan en el host SAP HANA principal. Los comandos SQL necesarios para la operación de backup no pueden realizarse en el host SAP HANA secundario.

Para las operaciones de backup de SAP HANA, los hosts SAP HANA primarios y secundarios son una entidad única. Comparten el mismo catálogo de backup SAP HANA y utilizan los backups para la restauración y la recuperación, independientemente de si el backup se creó en el host SAP HANA principal o secundario.

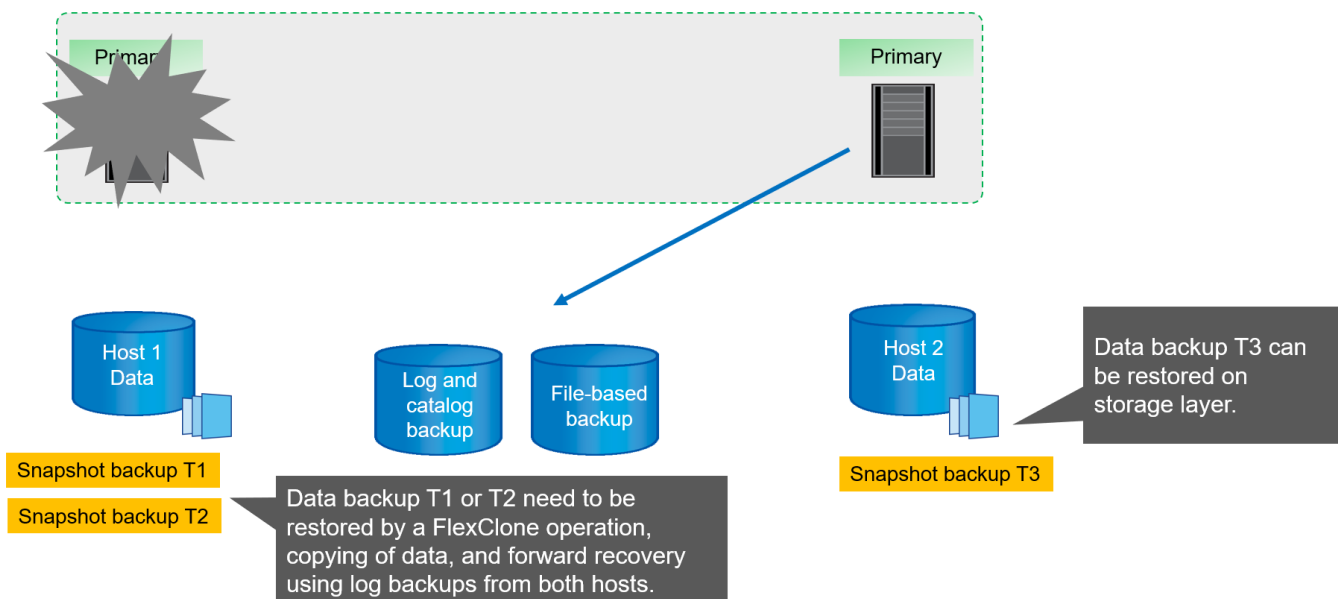
La capacidad de utilizar cualquier backup para restaurar y reenviar recuperaciones mediante backups de registros de ambos hosts requiere una ubicación de backup de registros compartidos a la que ambos hosts puedan acceder. NetApp recomienda la utilización de un volumen de almacenamiento compartido. Sin embargo, también debe separar el destino de la copia de seguridad de registro en subdirectorios dentro del volumen compartido.

Cada host SAP HANA tiene su propio volumen de almacenamiento. Cuando se utiliza una copia Snapshot basada en el almacenamiento para realizar un backup, se crea una copia Snapshot coherente con la base de datos en el volumen de almacenamiento del host SAP HANA principal.



Cuando se realiza una conmutación por error al host 2, el host 2 se convierte en el host primario, los backups se ejecutan en el host 2 y los backups de Snapshot se crean en el volumen de almacenamiento del host 2.

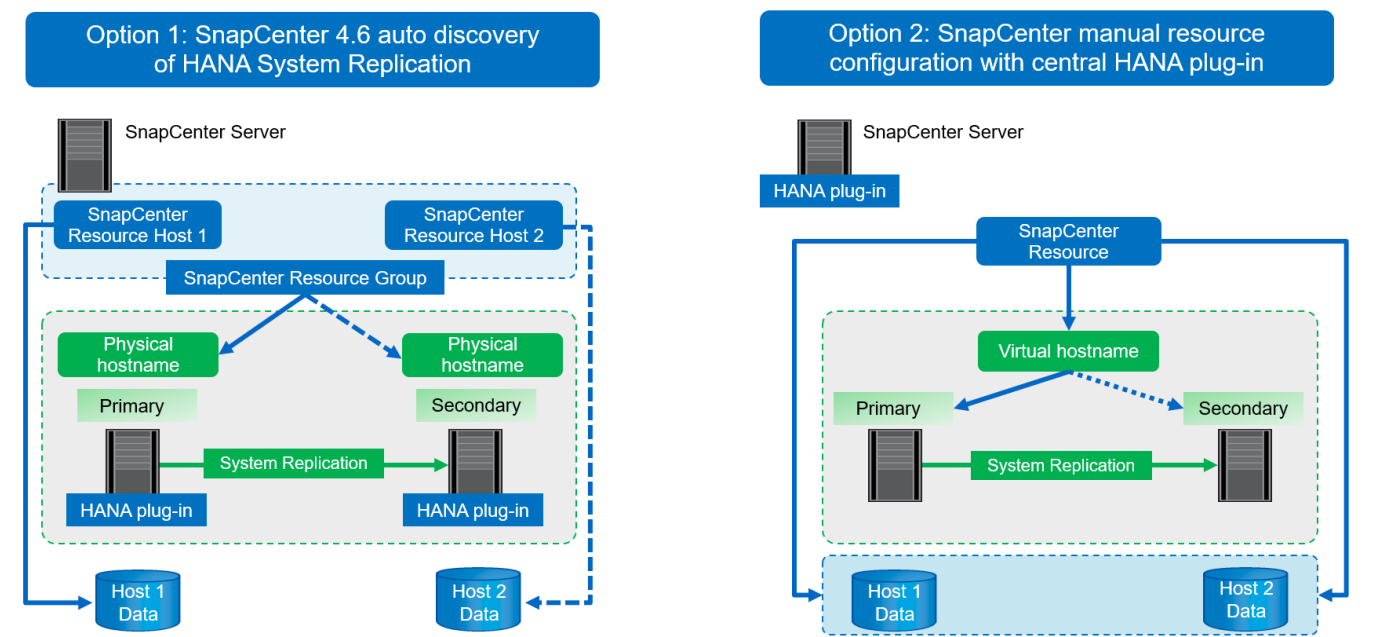
El backup creado en el host 2 se puede restaurar directamente en la capa de almacenamiento. Si se debe usar un backup creado en el host 1, se debe copiar el backup del volumen de almacenamiento del host 1 al volumen de almacenamiento del host 2. La recuperación futura utiliza los backups de registros de ambos hosts.



Opciones de configuración de SnapCenter para la replicación de sistemas SAP

La protección de datos se puede configurar con el software SnapCenter de NetApp en un entorno de replicación de sistemas SAP HANA:

- Un grupo de recursos de SnapCenter que incluye tanto hosts SAP HANA como detección automática con SnapCenter versión 4.6 o posterior.
- Un único recurso de SnapCenter para ambos hosts SAP HANA mediante una dirección IP virtual.



A partir de SnapCenter 4.6, SnapCenter admite la detección automática de sistemas HANA configurados en una relación de replicación del sistema HANA. Cada host se configura usando su dirección IP física (nombre de host) y su volumen de datos individual en la capa de almacenamiento. Los dos recursos de SnapCenter se combinan en un grupo de recursos, y SnapCenter identifica automáticamente qué host es primario o secundario y ejecuta las operaciones de backup necesarias en consecuencia. La gestión de retención de Snapshot y los backups basados en archivos creados por SnapCenter se realiza en ambos hosts para garantizar que los backups antiguos también se eliminan en el host secundario actual.

Con una configuración de un solo recurso para ambos hosts SAP HANA, el recurso único de SnapCenter se configura usando la dirección IP virtual de los hosts SAP HANA System Replication. Los dos volúmenes de datos de los hosts SAP HANA se incluyen en el recurso SnapCenter. Dado que se trata de un solo recurso de SnapCenter, la gestión de retención de Snapshot y los backups basados en archivos creados por SnapCenter funciona independientemente de qué host representa actualmente un recurso primario o secundario. Estas opciones son posibles con todas las versiones de SnapCenter.

En la tabla siguiente se resumen las principales diferencias de las dos opciones de configuración.

| | Grupo de recursos con SnapCenter 4.6 | Recurso único de SnapCenter y dirección IP virtual |
|---|--|--|
| Operación de backup (basado en archivos y Snapshot) | Identificación automática de host primario en el grupo de recursos | Usar automáticamente la dirección IP virtual |

| | Grupo de recursos con SnapCenter 4.6 | Recurso único de SnapCenter y dirección IP virtual |
|--|--|--|
| Gestión de retención (basada en archivos y Snapshot) | Se ejecutan automáticamente en ambos hosts | Utilice automáticamente un solo recurso |
| Requisitos de capacidad para backups | Los backups solo se crean en el volumen de host primario | Siempre se crean backups en ambos volúmenes de host. El backup del segundo host solo es coherente con los fallos y no se puede utilizar para realizar una reversión. |
| Operación de restauración | Los backups del host activo actual están disponibles para la operación de restauración | Se requiere un script previo al backup para identificar qué backups son válidos y se pueden usar para la restauración |
| Operación de recuperación | Todas las opciones de recuperación disponibles, igual que para cualquier recurso detectado automáticamente | Requiere recuperación manual |



En general, NetApp recomienda usar la opción de configuración de grupo de recursos con SnapCenter 4.6 para proteger los sistemas HANA con replicación de sistema HANA habilitada. Usar una sola configuración de recursos de SnapCenter solo es necesaria si el enfoque de la operación de SnapCenter se basa en un host del plugin central y el plugin de HANA no se implementa en los hosts de la base de datos HANA.

Las dos opciones se tratan en detalle en las siguientes secciones.

Configuración de SnapCenter 4.6 mediante un grupo de recursos

SnapCenter 4.6 admite la detección automática para los sistemas HANA configurados con la replicación de sistemas HANA. SnapCenter 4.6 incluye la lógica para identificar hosts HANA primarios y secundarios durante las operaciones de backup y también gestiona la gestión de retención en ambos hosts HANA. Además, la restauración y recuperación automatizadas ahora también están disponibles para los entornos de replicación de sistemas HANA.

Configuración de SnapCenter 4.6 de entornos de replicación de sistemas HANA

La siguiente figura muestra la configuración de laboratorio utilizada en este capítulo. Dos hosts HANA, hana-3 y hana-4, fueron configurados con HANA System Replication.

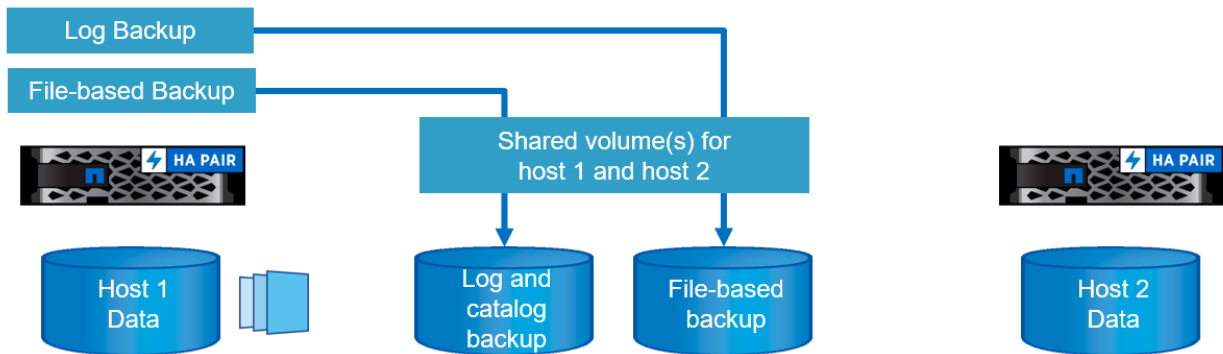
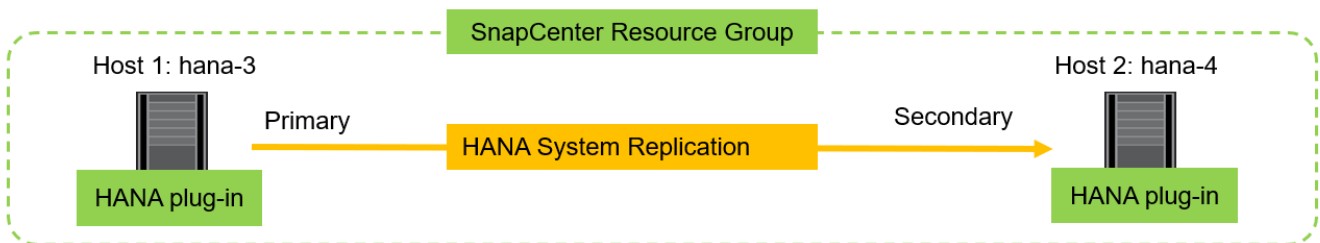
Se creó un usuario de base de datos "SnapCenter" para la base de datos del sistema HANA con los privilegios necesarios para ejecutar operaciones de backup y recuperación (consulte "[Backup y recuperación de datos de SAP HANA con SnapCenter](#)"). Debe configurarse una clave de almacenamiento de usuario de HANA en ambos hosts que utilice el usuario de base de datos anterior.

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

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

Desde una perspectiva de alto nivel, debe realizar los siguientes pasos para configurar la replicación del sistema HANA en SnapCenter.

1. Instale el complemento HANA en el host primario y secundario. Se ejecuta la detección automática y se detecta el estado de replicación del sistema HANA en cada host primario o secundario.
2. Ejecutar SnapCenter `configure database` y proporcione el `hdbuserstore` clave. Se ejecutan más operaciones de detección automática.
3. Cree un grupo de recursos, incluidos tanto los hosts como configurar la protección.



Después de instalar el plugin de SnapCenter HANA en ambos hosts HANA, los sistemas HANA se muestran en la vista de recursos de SnapCenter de la misma manera que otros recursos de detección automática. A partir de SnapCenter 4.6, se muestra una columna adicional que muestra el estado de la replicación del sistema HANA (habilitada/deshabilitada, primaria/secundaria).

| NetApp SnapCenter® | | | | | | | | | |
|---|--------|-----------------|------------------|---------------------|-----------------------------|-----------------|----------|-------------|----------------|
| SAP HANA | | | | | | | | | |
| View: Multitenant Database Container Search databases | | | | | | | | | |
| Resources | System | System ID (SID) | Tenant Databases | Replication | Plug-in Host | Resource Groups | Policies | Last backup | Overall Status |
| Monitor | SS2 | SS2 | SS2 | Enabled (Primary) | hana-3.sapcc.stl.netapp.com | | | | Not protected |
| Reports | SS2 | SS2 | SS2 | Enabled (Secondary) | hana-4.sapcc.stl.netapp.com | | | | Not protected |

Al hacer clic en el recurso, SnapCenter solicita la clave de almacenamiento de usuario de HANA para el sistema HANA.

Configure Database

Plug-in host

hana-3.sapcc.stl.netapp.com

HDBSQL OS User

ss2adm

HDB Secure User Store Key

SS2KEY

Cancel

OK

Se ejecutan pasos adicionales de detección automática y SnapCenter muestra los detalles del recurso. Con SnapCenter 4.6, el estado de la replicación del sistema y el servidor secundario se muestran en esta vista.

NetApp SnapCenter

SAP HANA

Search databases

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

plug-in 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 | |

Activity

The 5 most recent jobs are displayed

0 Completed

0 Warnings

0 Failed

0 Canceled

0 Running

0 Queued

Tras realizar los mismos pasos para el segundo recurso HANA, se completa el proceso de detección automática y ambos recursos HANA se configuran en SnapCenter.

NetApp SnapCenter®

SAP HANA

View: Multitenant Database Container Search databases

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

Para los sistemas habilitados con replicación del sistema HANA, debe configurar un grupo de recursos de SnapCenter, incluidos ambos recursos de HANA.

NetApp SnapCenter®

SAP HANA

View: Resource Group Search databases

| Name | Resource Count | Tags | Policies | Last backup | Overall Status |
|---|----------------|------|----------|-------------|----------------|
| There is no match for your search or data is not available. | | | | | |

NetApp recomienda usar un formato de nombre personalizado para el nombre de Snapshot, que debe incluir el nombre de host, la política y la programación.

NetApp SnapCenter®

SAP HANA

Search databases

New Resource Group

To configure an SMTP Server to send email notifications for scheduled or on-demand jobs, go to Settings>Global Settings>Notification Server Settings.

1 Name 2 Resources 3 Application Settings 4 Policies 5 Notification 6 Summary

Provide a name and tags for the resource group

Name: SS2 - HANA System Replication

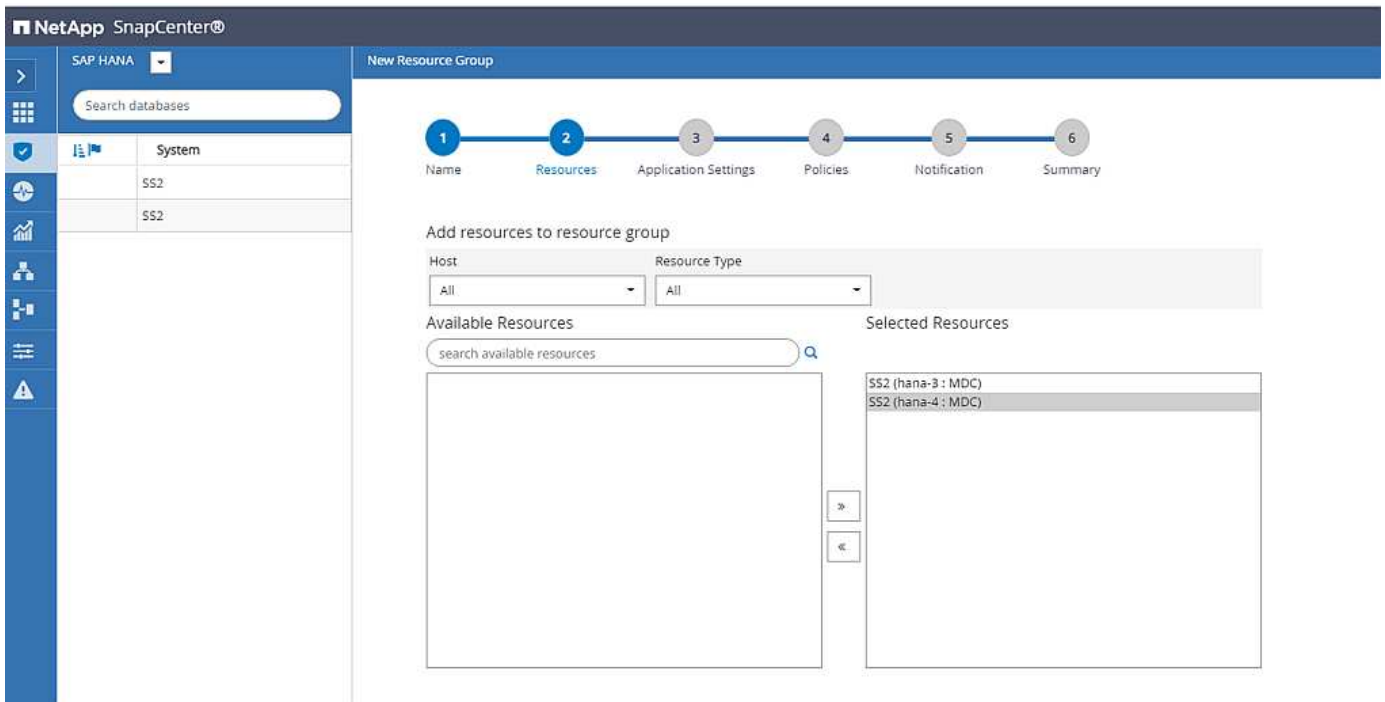
Tags:

☒ Use custom name format for Snapshot copy

\$CustomText x \$HostName x \$Policy x \$ScheduleType x

SnapCenter

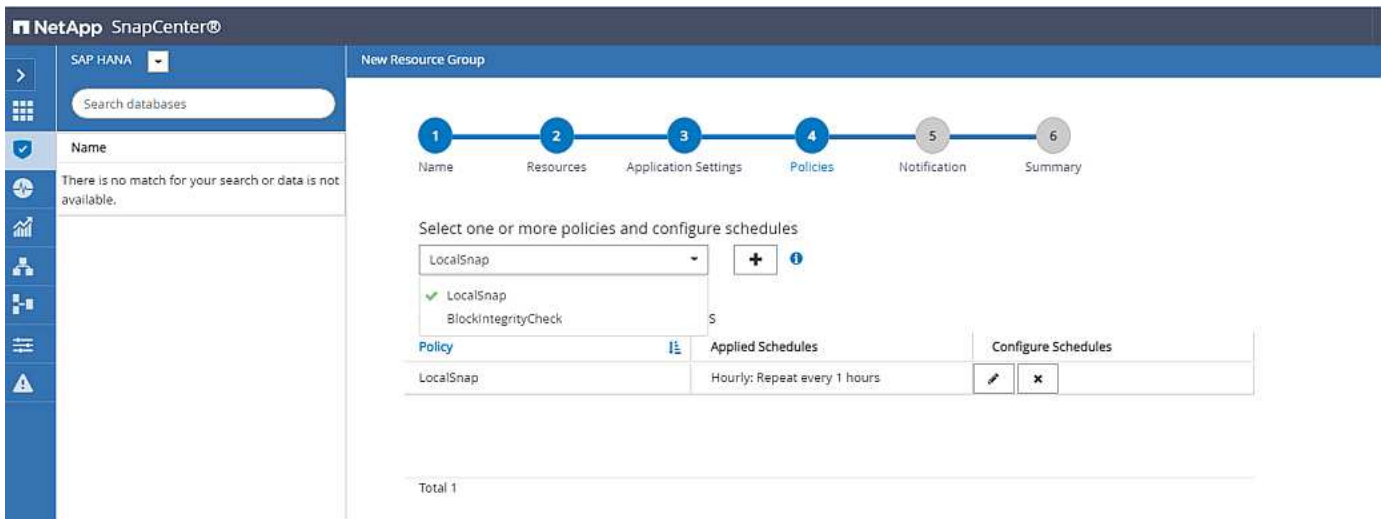
Debe añadir ambos hosts HANA al grupo de recursos.



Las políticas y las programaciones se configuran para el grupo de recursos.



La retención definida en la política se usa en ambos hosts HANA. Si, por ejemplo, se define una retención de 10 en la política, la suma de los backups de ambos hosts se usa como criterios para la eliminación de un backup. SnapCenter elimina el backup más antiguo de forma independiente si se creó en el host primario o secundario actual.



La configuración del grupo de recursos ahora termina y se pueden ejecutar los backups.

NetApp SnapCenter®

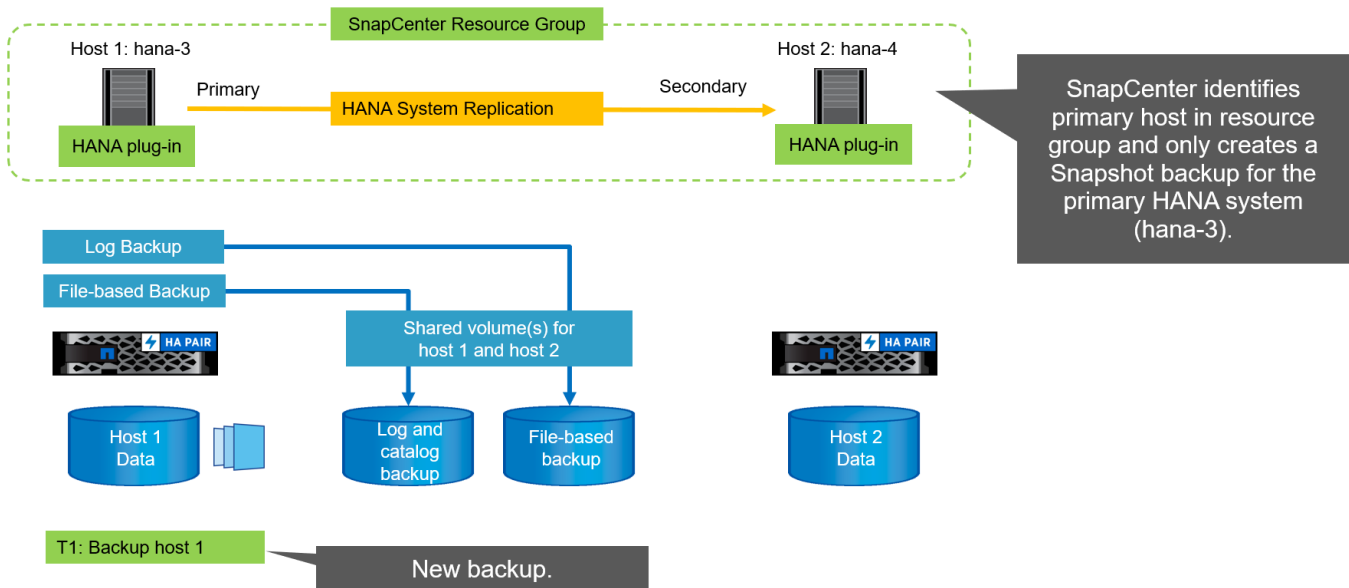
</

NetApp SnapCenter®

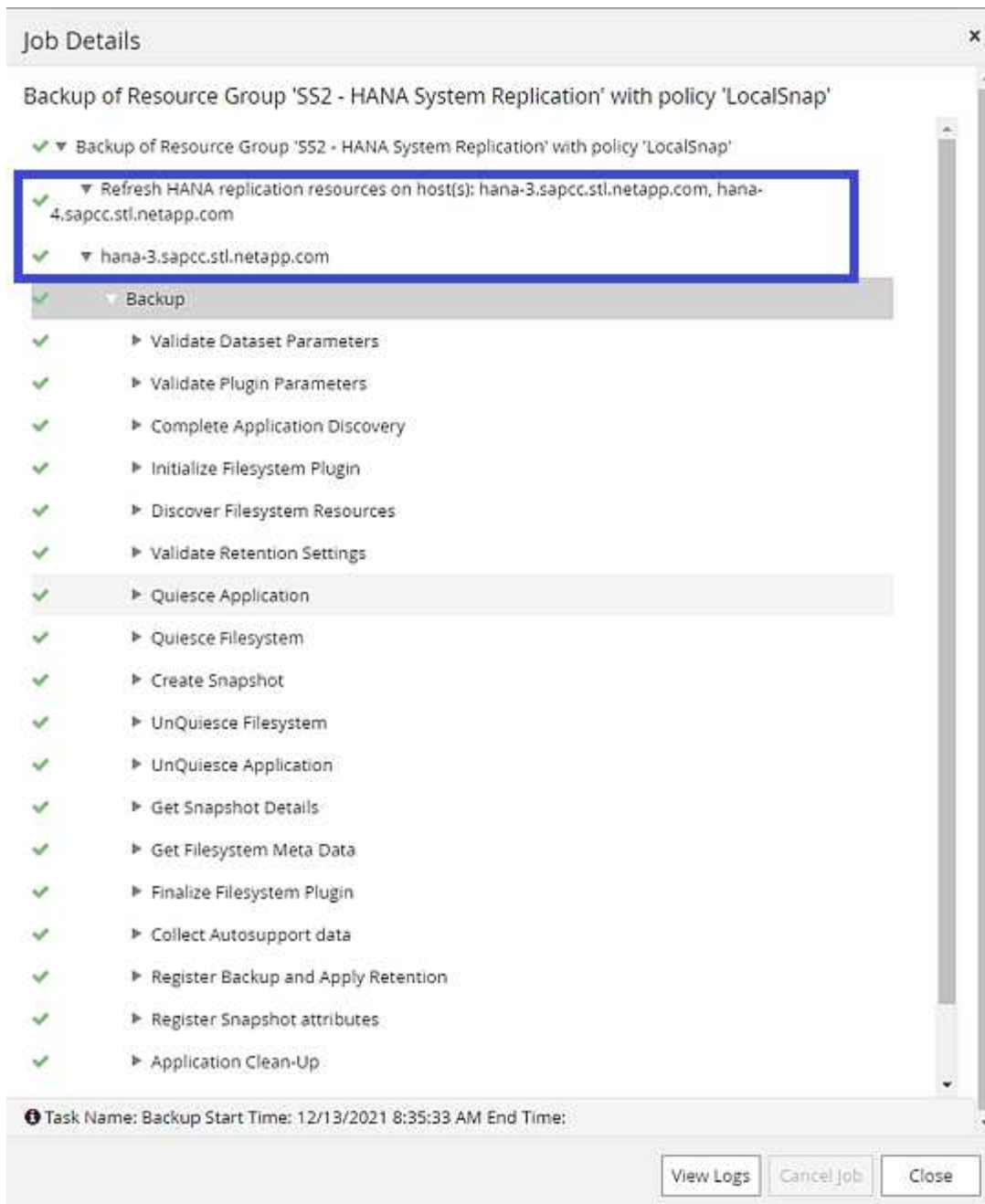
</

Operaciones de backup de Snapshot

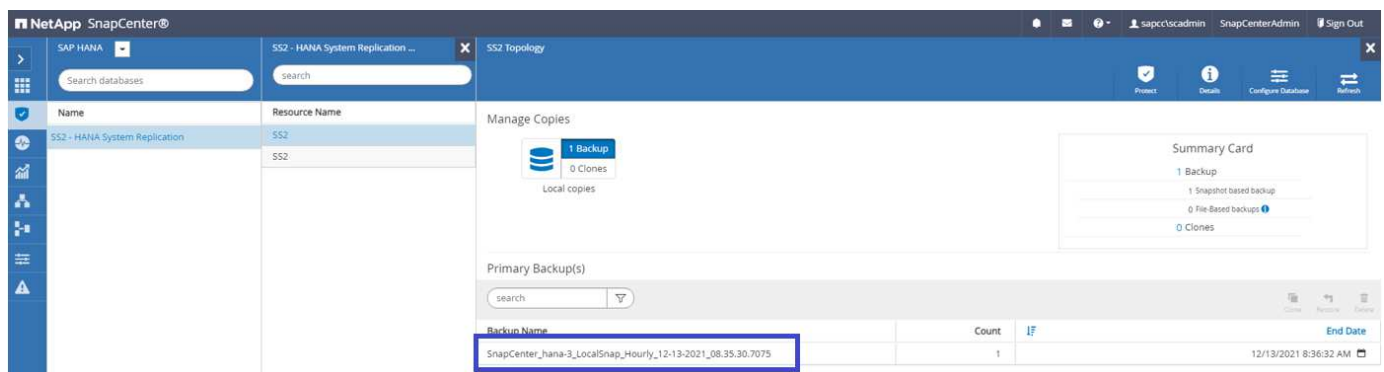
Cuando se ejecuta una operación de backup del grupo de recursos, SnapCenter identifica el host primario y solo activa un backup en el host primario. Esto significa que solo se hará copia Snapshot del volumen de datos del host primario. En nuestro ejemplo, hana-3 es el host primario actual y se ejecuta un backup en este host.



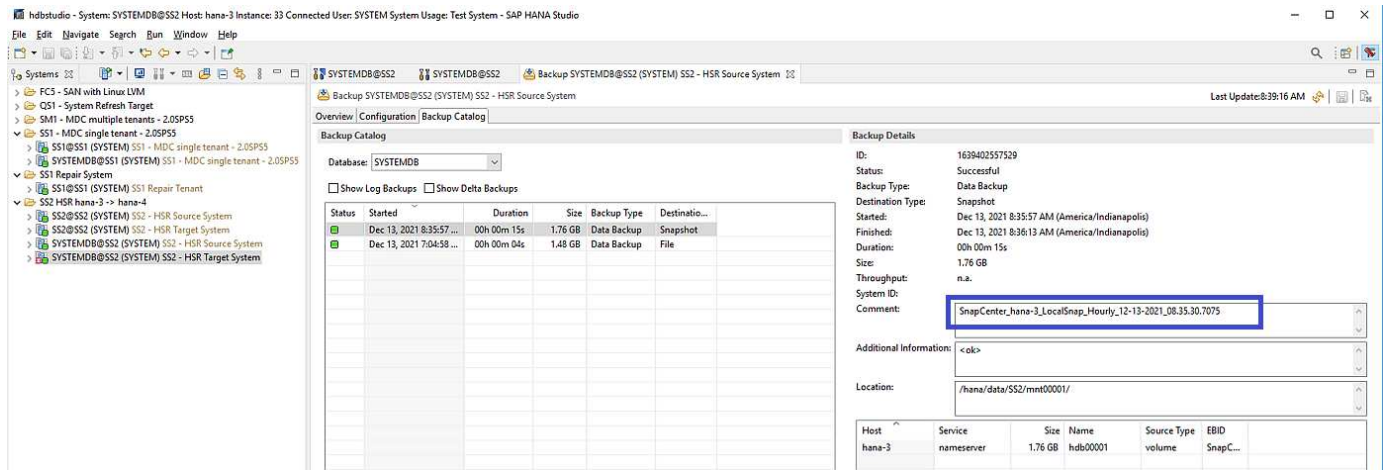
El registro de trabajos de SnapCenter muestra la operación de identificación y la ejecución del backup en el host primario actual hana-3.



Ahora se ha creado un backup de Snapshot en el recurso HANA principal. El nombre de host incluido en el nombre de backup muestra hana-3.



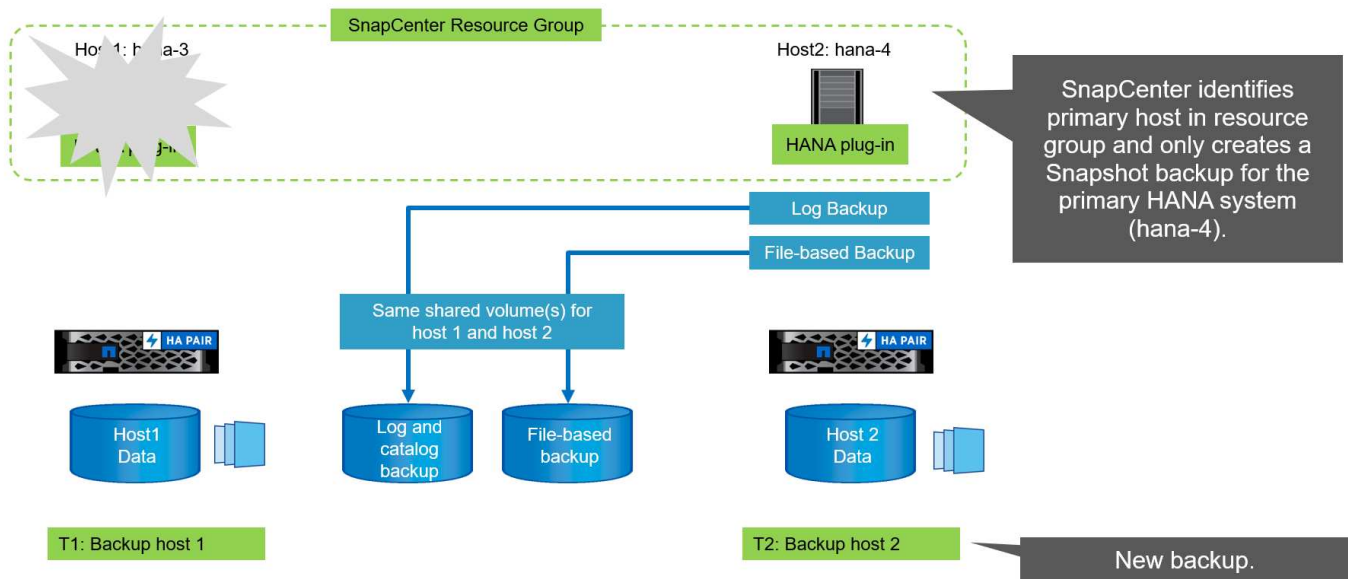
El mismo backup Snapshot también se puede ver en el catálogo de backup de HANA.



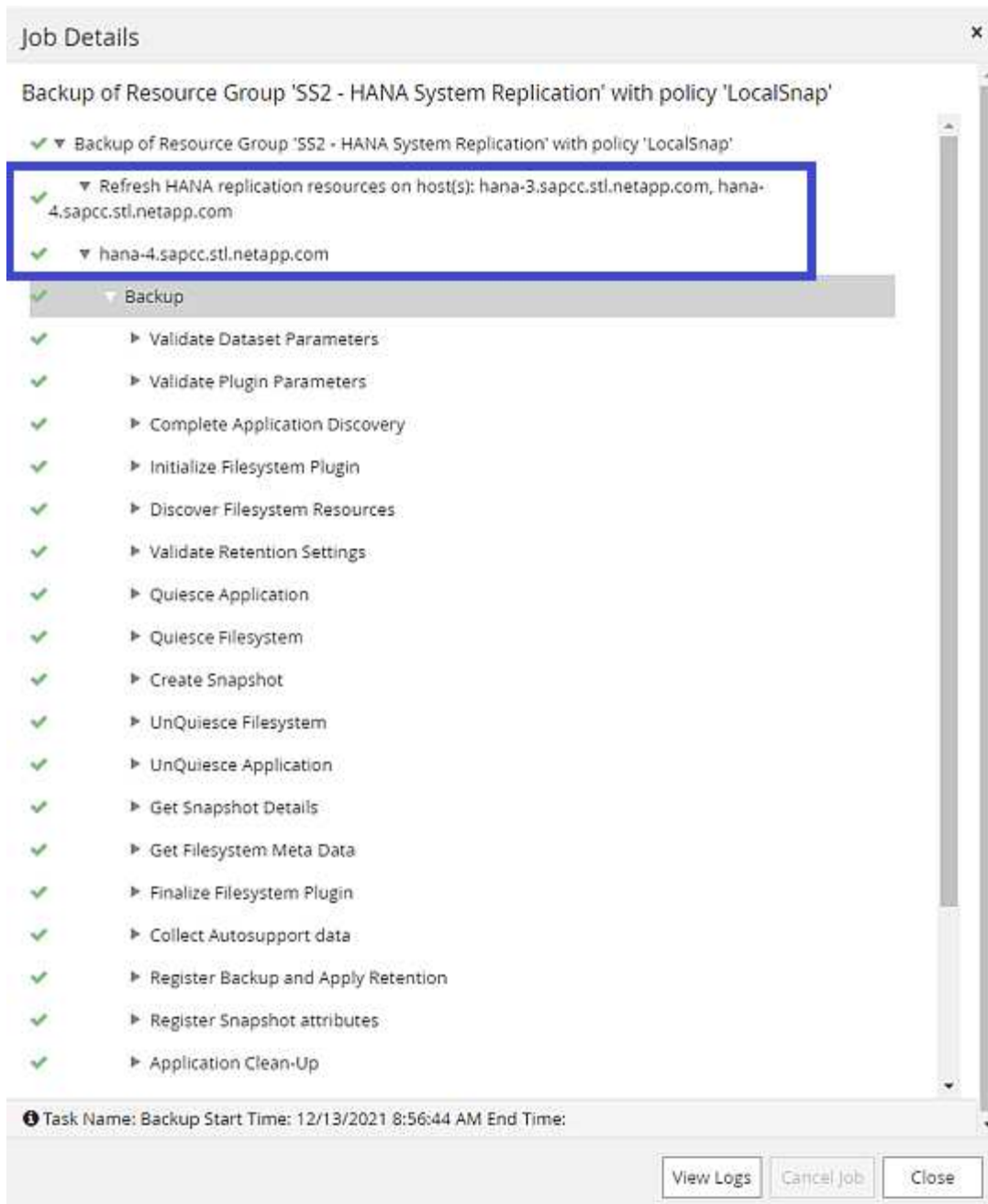
Si se ejecuta una operación de toma de control, otros backups de SnapCenter ahora identifican el host secundario anterior (hana-4) como primario; la operación de backup se ejecuta en hana-4. De nuevo, solo se crea una copia de Snapshot del nuevo host primario (hana-4).



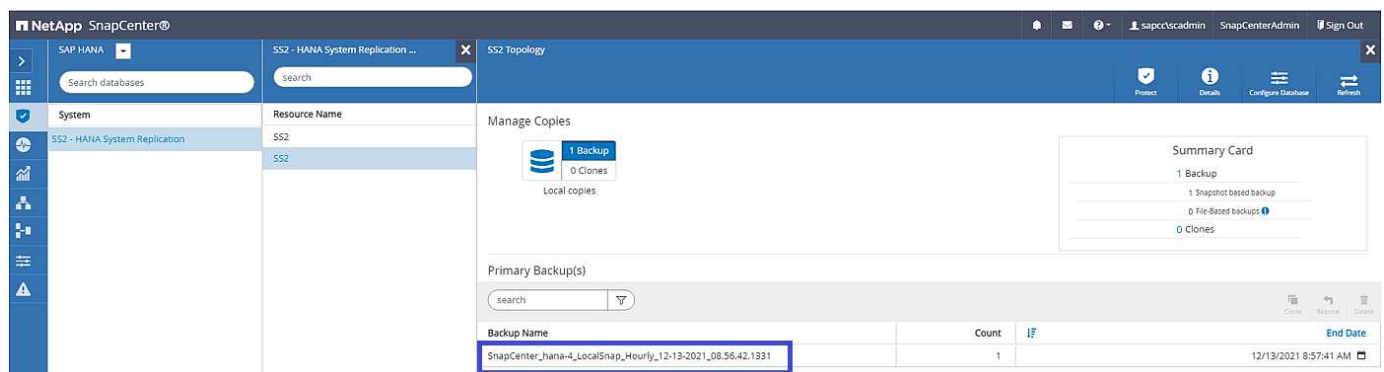
La lógica de identificación de SnapCenter solo cubre situaciones en las que los hosts HANA se encuentran en una relación primaria-secundaria o cuando uno de los hosts HANA está sin conexión.



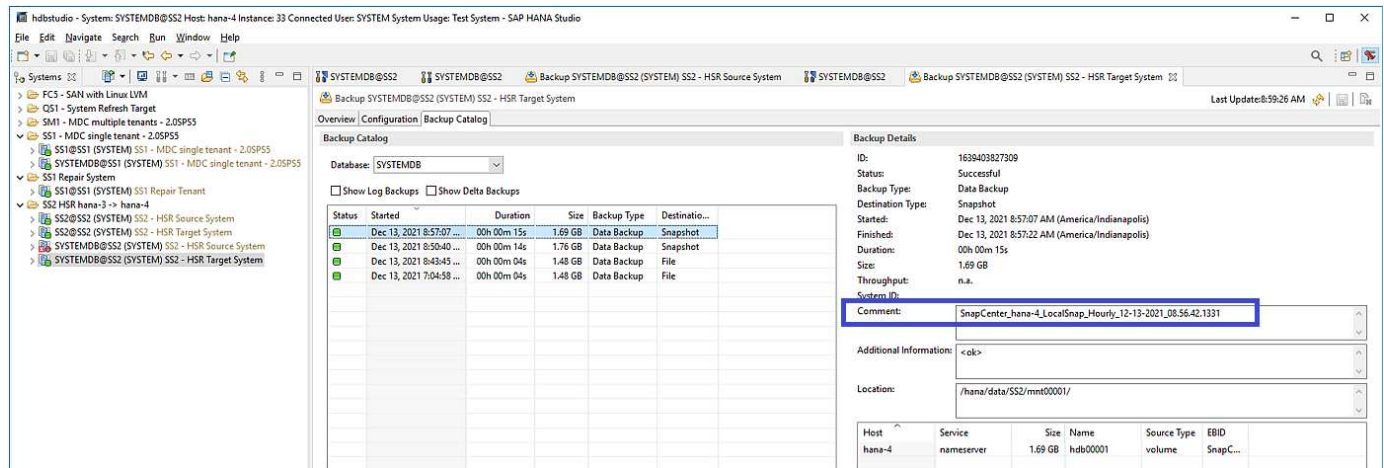
El registro de trabajos de SnapCenter muestra la operación de identificación y la ejecución del backup en el host primario actual hana-4.



Ahora se ha creado un backup de Snapshot en el recurso HANA principal. El nombre de host incluido en el nombre de backup muestra hana-4.



El mismo backup Snapshot también se puede ver en el catálogo de backup de HANA.



Operaciones de comprobación de integridad de bloques con backups basados en archivos

SnapCenter 4.6 usa el mismo lógico que se describe para las operaciones de backup de Snapshot para operaciones de comprobación de integridad de bloques con backups basados en archivos. SnapCenter identifica el host HANA primario actual y ejecuta el backup basado en archivos para este host. La gestión de retención también se realiza en ambos hosts, de modo que el backup más antiguo se elimina independientemente de qué host sea actualmente el primario.

Replicación SnapVault

Para permitir operaciones de backup transparentes sin interacción manual en el caso de toma de control e independiente del host HANA que actualmente es el host primario, debe configurar una relación de SnapVault para los volúmenes de datos de ambos hosts. SnapCenter ejecuta una operación de actualización de SnapVault para el host primario actual con cada ejecución de backup.

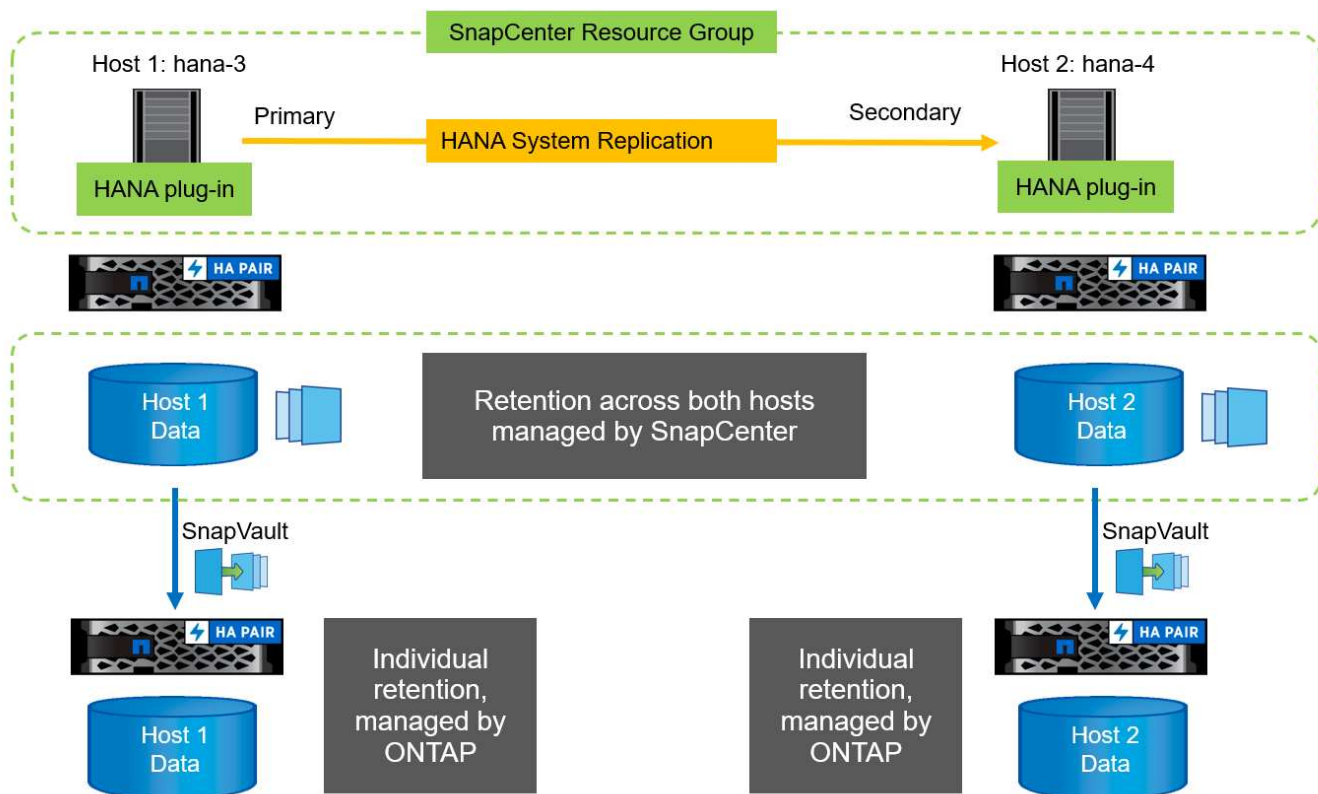


Si no se realiza una toma de control en el host secundario durante mucho tiempo, la cantidad de bloques modificados para la primera actualización de SnapVault en el host secundario será alta.

Como ONTAP gestiona la gestión de retención en el destino de SnapVault fuera de SnapCenter, esta retención no se puede manejar entre ambos hosts HANA. Por lo tanto, los backups que se crearon antes de la toma de control no se eliminan con operaciones de backup en el secundario anterior. Estos backups permanecen hasta que la primera copia vuelve a ser primaria. Para que estos backups no bloqueen la gestión de retención de los backups de registros, deben eliminarse manualmente en el destino SnapVault o en el catálogo de backup de HANA.



No es posible limpiar todas las copias snapshot de SnapVault porque una copia snapshot está bloqueada como punto de sincronización. Si también es necesario eliminar la última copia de Snapshot, se debe eliminar la relación de replicación de SnapVault. En este caso, NetApp recomienda eliminar los backups en el catálogo de backup de HANA para desbloquear la gestión de la retención de backup de registros.



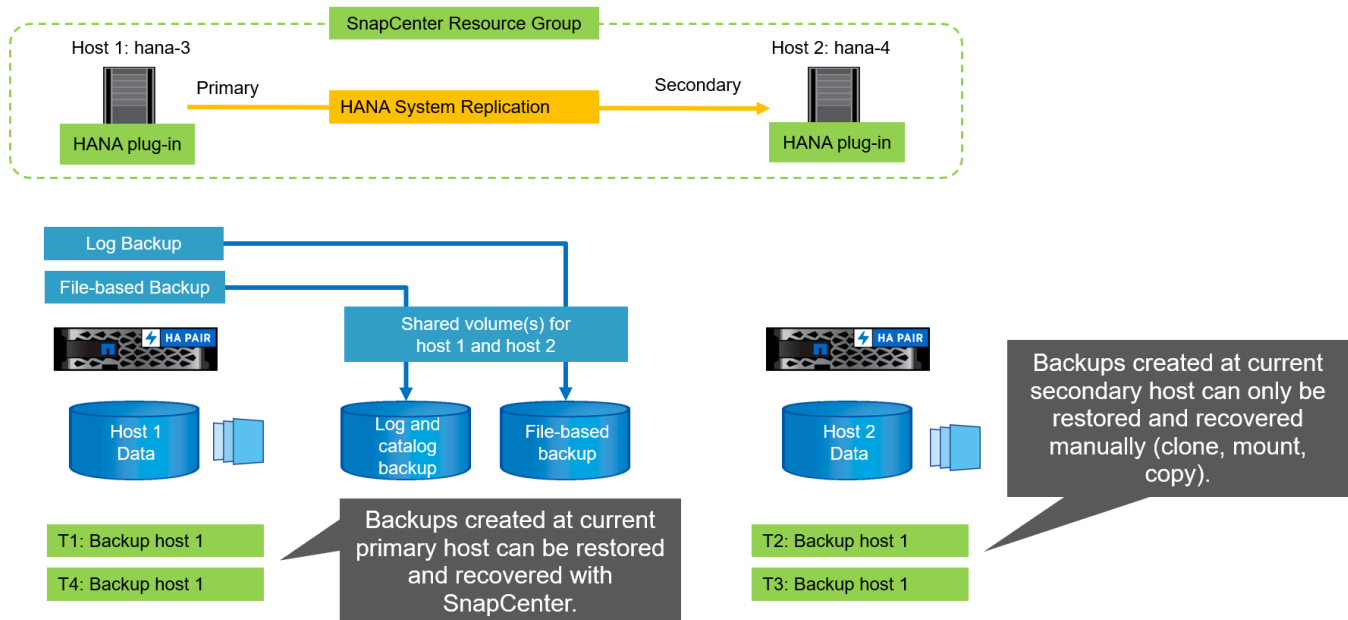
Gestión de retención

SnapCenter 4.6 gestiona la retención de backups de Snapshot, operaciones de comprobación de integridad de bloques, entradas de catálogo de backup de HANA y backups de registros (si no están deshabilitados) en ambos hosts HANA, por lo que no importa qué host sea actualmente primario o secundario. Los backups (datos y registro) y las entradas en el catálogo HANA se eliminan de acuerdo con la retención definida, independientemente de si es necesaria una operación de eliminación en el host primario o secundario actual. Es decir, no es necesaria ninguna interacción manual si se realiza una operación de toma de control y/o si la replicación se configura en la otra dirección.

Si la replicación de SnapVault forma parte de la estrategia de protección de datos, es necesario realizar la interacción manual para situaciones específicas, como se describe en la sección [\[SnapVault Replication\]](#).

Restauración y recuperación

La siguiente figura muestra una situación en la que se han ejecutado varias adquisiciones y se han creado backups de Snapshot en ambos sitios. Con el estado actual, el host hana-3 es el host principal y el último backup es T4, que se ha creado en el host hana-3. Si necesita realizar una restauración y recuperación de datos, los backups T1 y T4 están disponibles para su restauración y recuperación en SnapCenter. Los backups, que se crearon en el host hana-4 (T2, T3), no se pueden restaurar mediante SnapCenter. Estos backups deben copiarse manualmente en el volumen de datos de hana-3 para la recuperación.



Las operaciones de restauración y recuperación de una configuración de grupos de recursos de SnapCenter 4.6 son idénticas a la configuración de replicación sin sistema que se haya detectado automáticamente. Todas las opciones de restauración y recuperación automatizada están disponibles. Si quiere más información, consulte el informe técnico "[TR-4614: Backup y recuperación de datos de SAP HANA con SnapCenter](#)".

Una operación de restauración a partir de un backup que se creó en el otro host se describe en la sección "[Restauración y recuperación a partir de un backup creado en el otro host](#)".

Configuración de SnapCenter con un solo recurso

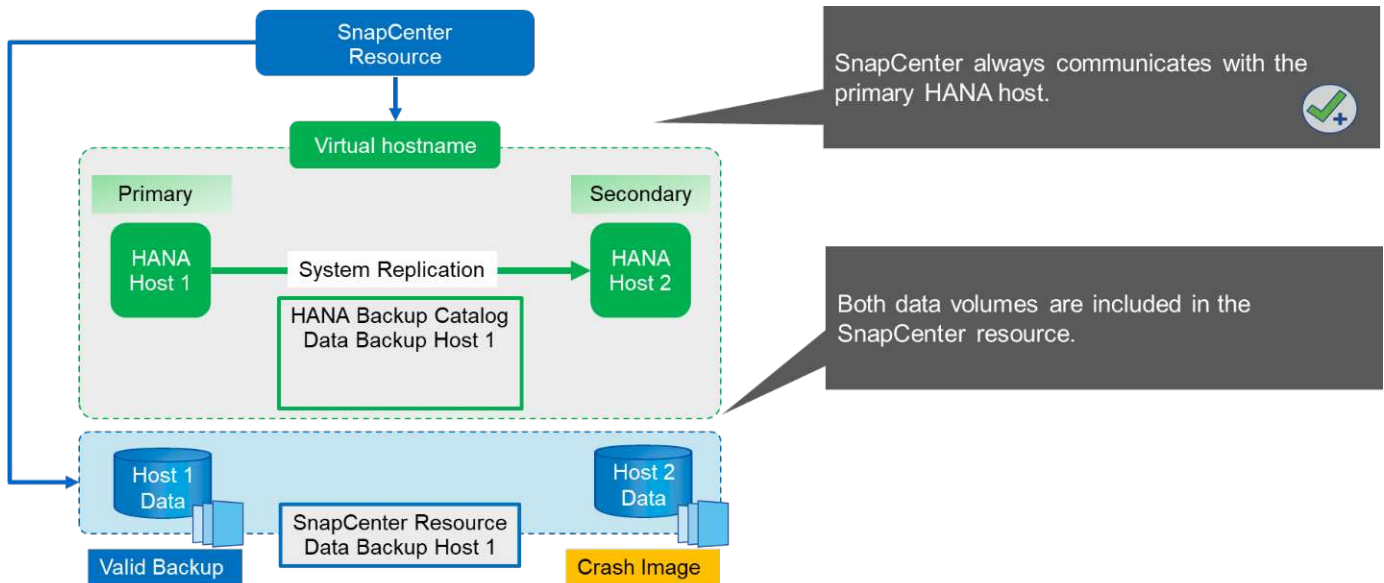
Un recurso de SnapCenter se configura con la dirección IP virtual (nombre de host) del entorno de replicación del sistema HANA. Con este método, SnapCenter siempre se comunica con el host primario, independientemente de si el host 1 o el host 2 son primarios. Los volúmenes de datos de ambos hosts SAP HANA se incluyen en el recurso SnapCenter.



Asumimos que la dirección IP virtual siempre está vinculada al host SAP HANA principal. La conmutación al nodo de respaldo de la dirección IP virtual se realiza fuera de SnapCenter como parte del flujo de trabajo de conmutación al nodo de respaldo de la replicación del sistema HANA.

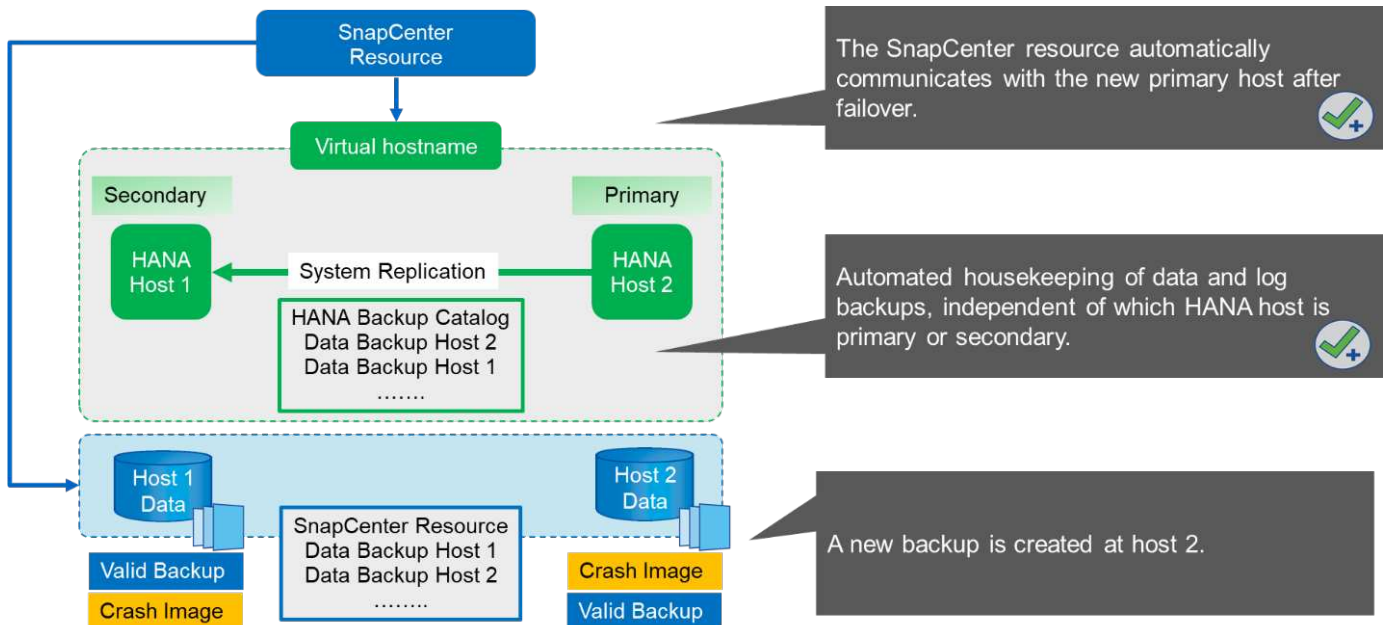
Cuando se ejecuta un backup con el host 1 como host primario, se crea un backup de Snapshot coherente con la base de datos en el volumen de datos del host 1. Debido a que el volumen de datos del host 2 forma parte del recurso de SnapCenter, se crea otra copia de Snapshot para este volumen. Esta copia Snapshot no es coherente con la base de datos, sino que es solo una imagen con los fallos del host secundario.

El catálogo de backup de SAP HANA y el recurso SnapCenter incluyen el backup creado en el host 1.



En la figura siguiente se muestra la operación de backup después de la conmutación al host 2 y la replicación del host 2 al host 1. SnapCenter se comunica automáticamente con el host 2 mediante la dirección IP virtual configurada en el recurso SnapCenter. Ahora se crean backups en el host 2. SnapCenter crea dos copias de Snapshot: Un backup coherente con la base de datos en el volumen de datos en el host 2 y una copia Snapshot de imagen tras bloqueo en el volumen de datos en el host 1. El catálogo de backup de SAP HANA y el recurso SnapCenter ahora incluyen el backup creado en el host 1 y el backup creado en el host 2.

El mantenimiento de backups de datos y registros se basa en la política de retención de SnapCenter definida, y los backups se eliminan independientemente del host primario o secundario.

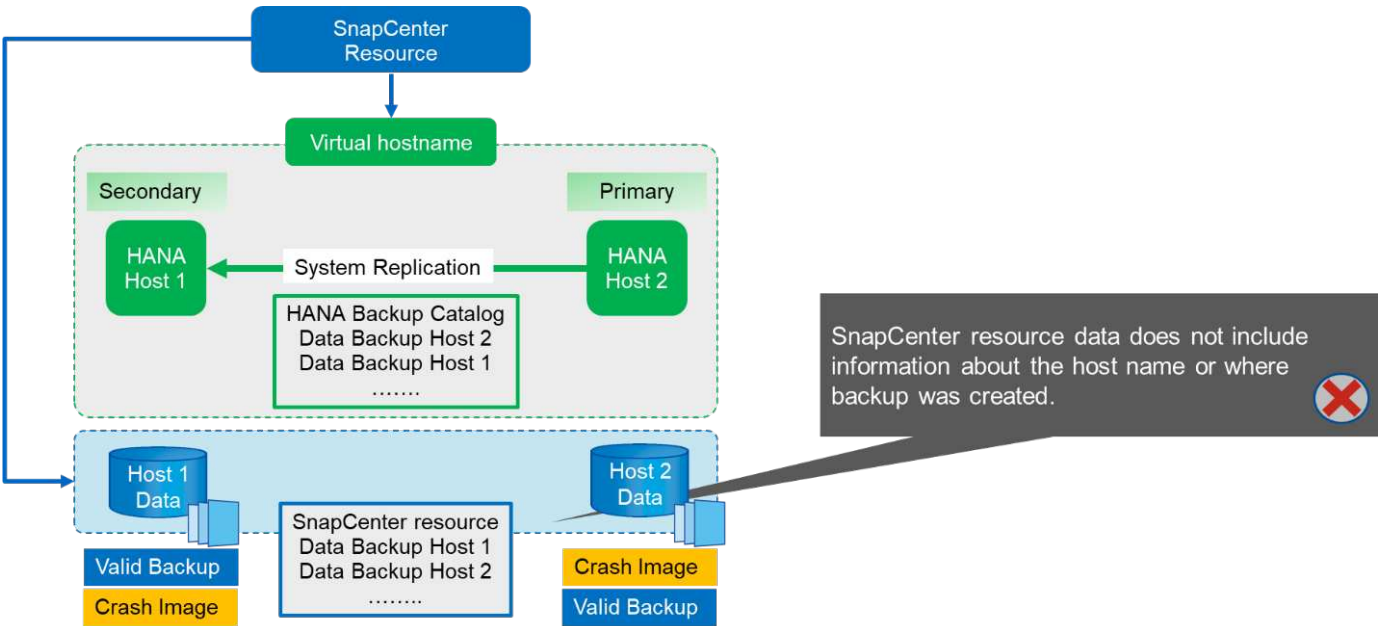


Como se explica en la sección "[Backups de Storage Snapshot y replicación de sistemas SAP](#)", Una operación de restauración con copias de seguridad Snapshot basadas en almacenamiento es diferente, dependiendo de qué copia de seguridad se deba restaurar. Es importante identificar en qué host se creó la copia de seguridad para determinar si la restauración puede realizarse en el volumen de almacenamiento local o si la restauración debe realizarse en el volumen de almacenamiento del otro host.

Con la configuración de SnapCenter para un solo recurso, SnapCenter no sabe dónde se creó el backup. Por

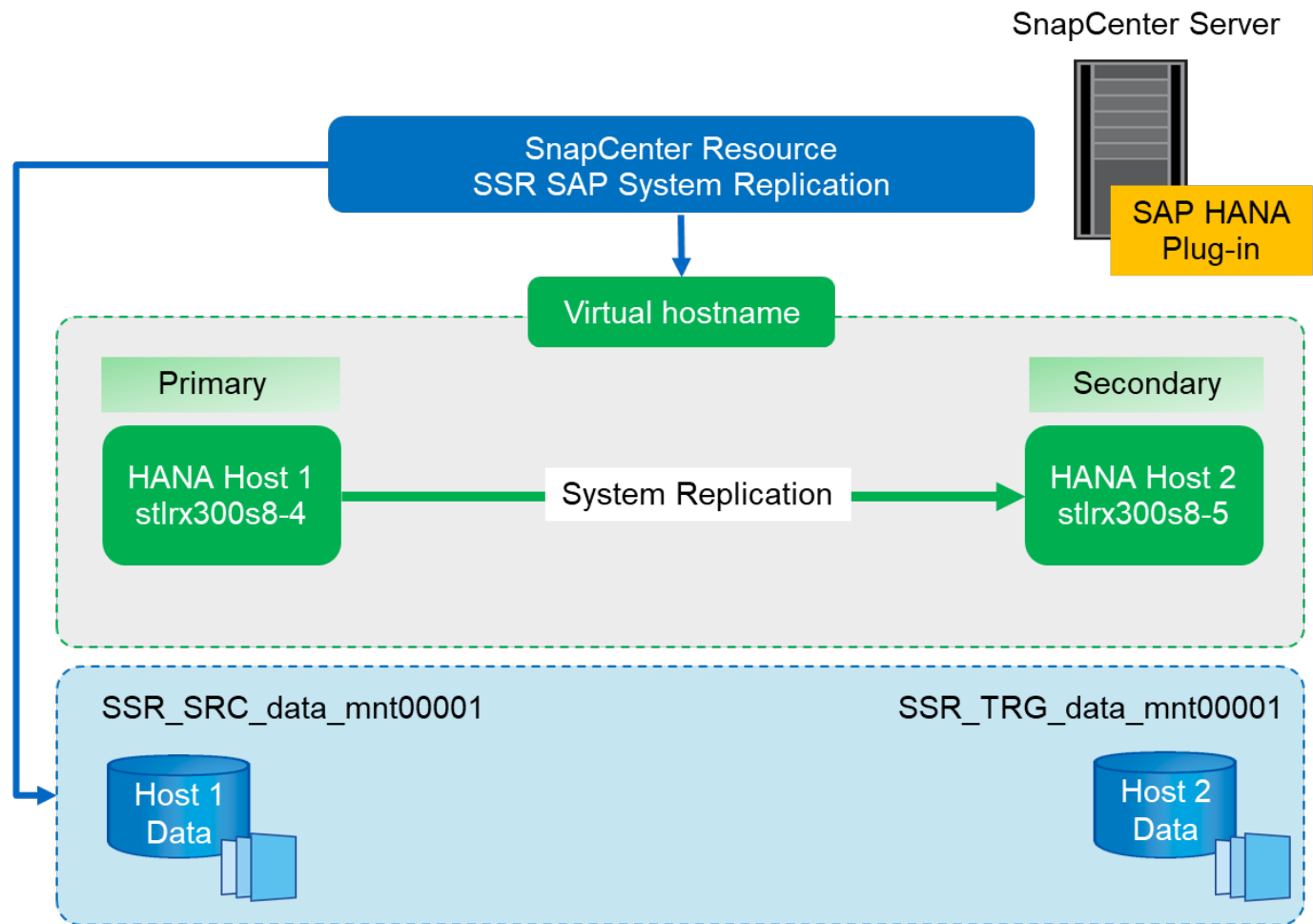
lo tanto, NetApp recomienda añadir una secuencia de comandos de prebackup al flujo de trabajo de backup de SnapCenter para identificar qué host es actualmente el host SAP HANA principal.

La siguiente figura muestra la identificación del host de backup.



Configuración de SnapCenter

La siguiente figura muestra la configuración del laboratorio y una descripción general de la configuración de SnapCenter necesaria.



Para realizar operaciones de backup independientemente del host de SAP HANA principal e incluso cuando uno de los hosts está inactivo, se debe poner en marcha el plugin SAP HANA de SnapCenter en un host de plugin central. En nuestra configuración de laboratorio, utilizamos el servidor SnapCenter como host de complementos central e implementamos el complemento SAP HANA en el servidor SnapCenter.

Se creó un usuario en la base de datos HANA para realizar operaciones de backup. Se configuró una clave de almacenamiento de usuario en el servidor SnapCenter en el que se instaló el complemento SAP HANA. La clave de almacenamiento de usuario incluye la dirección IP virtual de los hosts SAP HANA System Replication (ssr-vip).

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

Puede encontrar más información sobre las opciones de puesta en marcha del complemento SAP HANA y la configuración del almacén de usuario en el informe técnico TR-4614: ["Backup y recuperación de datos de SAP HANA con SnapCenter"](#).

En SnapCenter, el recurso se configura como se muestra en la siguiente figura utilizando la clave de almacenamiento de usuario, configurada antes y el servidor SnapCenter como el hdbsql host de comunicación.

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Resource Details

☐ Single Container

☒ Multitenant Database Container (MDC) - Single Tenant

☐ Non-data Volumes

Resource Type

HANA System Name

SSR - SAP System Replication

SID

SSR

Tenant Database

SSR

HDBSQL Client Host

SC30-V2.sapcc.stl.netapp.com

HDB Secure User Store Keys

SSRKEY

HDBSQL OS User

SYSTEM

Previous

Next

Los volúmenes de datos de ambos hosts SAP HANA se incluyen en la configuración de espacio de almacenamiento, tal y como se muestra en la siguiente figura.

20

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

SSR_TRG_data_mnt00001

SSR_SRC_data_mnt00001

LUNs or Qtrees

Default is 'None' or type to find

Default is 'None' or type to find

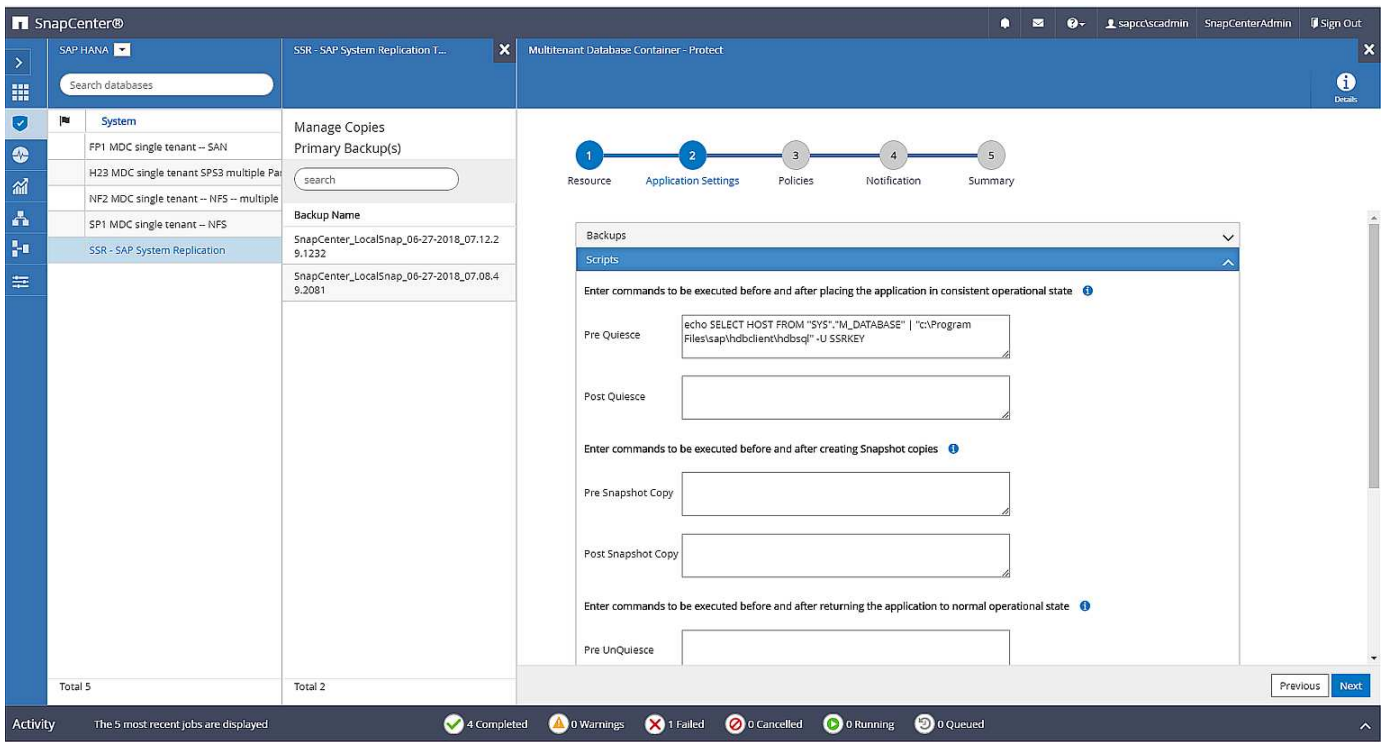
Save

Previous

Next

Como se ha explicado anteriormente, SnapCenter no sabe dónde se creó el backup. NetApp, por lo tanto, recomienda añadir una secuencia de comandos previa al backup en el flujo de trabajo de SnapCenter para identificar qué host es actualmente el host SAP HANA principal. Puede realizar esta identificación con una sentencia SQL que se agrega al flujo de trabajo de backup, tal y como se muestra en la siguiente figura.

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

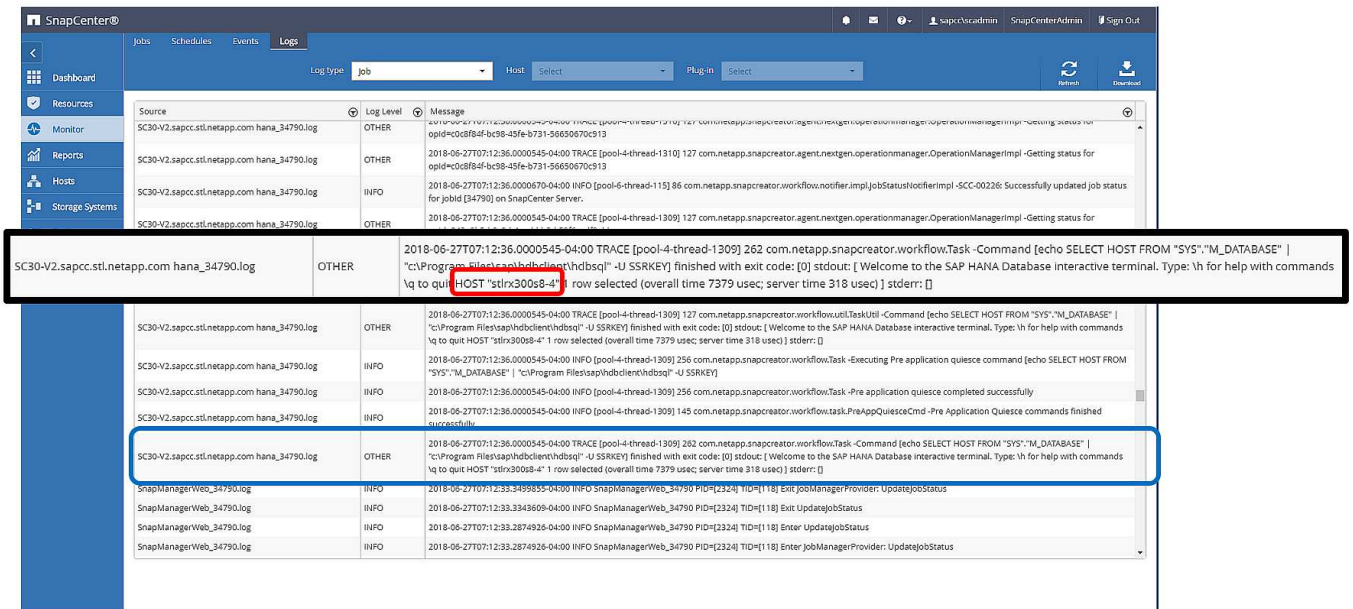



Operación de backup de SnapCenter

Las operaciones de backup ahora se ejecutan de la forma habitual. El mantenimiento de backups de datos y registros se realiza independientemente del host SAP HANA principal o secundario.

Los registros de trabajos de backup incluyen el resultado de la declaración SQL, que permite identificar el host SAP HANA donde se creó el backup.

En la siguiente figura, se muestra el registro del trabajo de backup con el host 1 como host primario.



En esta figura, se muestra el registro de la tarea de backup con el host 2 como host primario.

The screenshot shows the SAP HANA Studio Logs window. The log entry for 'SC30-V2.sapcc.stl.netapp.com hana_34799.log' is highlighted. The log message is as follows:

```
2018-06-27T07:45:53.0000174-04:00 TRACE [pool-4-thread-1347] 262 com.netapp.snapcreator.workflow.Task -Command [echo SELECT HOST FROM *SYS*."M_DATABASE" | "c:\Program Files\sql\hdbclient\hdbsql" -U SSRKEY] finished with exit code: [0] stdout: [Welcome to the SAP HANA Database Interactive terminal. Type: \h for help with commands \q to quit HOST "stlx3008-5" 1 row selected (overall time 5613 usec; server time 202 usec) ] stderr: []
```

La siguiente figura muestra el catálogo de backup de SAP HANA en SAP HANA Studio. Cuando la base de datos SAP HANA está en línea, el host SAP HANA donde se creó el backup es visible en SAP HANA Studio.



El catálogo de backup de SAP HANA en el sistema de archivos, que se usa durante una operación de restauración y recuperación, no incluye el nombre de host donde se creó el backup. La única manera de identificar el host cuando la base de datos está inactiva es combinar las entradas del catálogo de backup con la backup . log Archivo de ambos hosts SAP HANA.

The screenshot shows the SAP HANA Studio Backup Catalog window. The backup details for the SYSTEMDB database are displayed. The backup was created on Jun 21, 2018, 11:36:30 AM (America/New_York) and is a Data Backup Snapshot. The backup size is 1.47 GB. The backup location is /hana/data/SSR/rmnt00001/. The backup details table shows the host stlx3008-4, service nameserver, size 1.47 GB, name hdb00001, source type volume, and EBID SnapC...

| Host | Service | Size | Name | Source Type | EBID |
|------------|------------|---------|----------|-------------|----------|
| stlx3008-4 | nameserver | 1.47 GB | hdb00001 | volume | SnapC... |

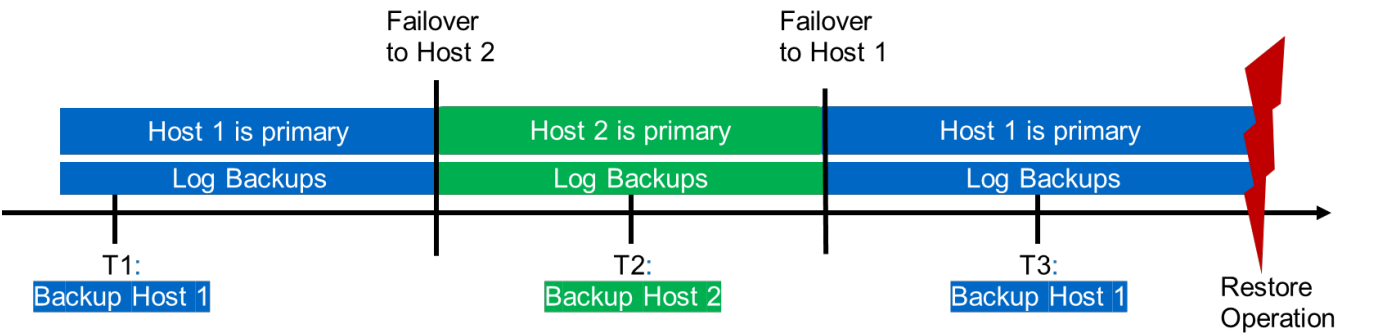
Restauración y recuperación

Como hemos visto anteriormente, es necesario poder identificar dónde se creó el backup seleccionado para definir la operación de restauración necesaria. Si la base de datos SAP HANA sigue conectada, puede usar SAP HANA Studio para identificar el host en el que se creó el backup. Si la base de datos está sin conexión, la información solo está disponible en el registro de trabajos de backup de SnapCenter.

En la siguiente figura, se ilustran las diferentes operaciones de restauración en función del backup seleccionado.

Si se debe realizar una operación de restauración después de que la Marca de tiempo T3 y el host 1 sea el primario, puede restaurar el backup creado en T1 o T3 mediante SnapCenter. Estos backups de Snapshot están disponibles en el volumen de almacenamiento conectado al host 1.

Si tiene que restaurar con el backup creado en el host 2 (T2), que es una copia Snapshot en el volumen de almacenamiento del host 2, debe estar disponible para el host 1. Puede hacer que este backup esté disponible creando una copia de FlexClone de NetApp desde el backup, montando la copia de FlexClone en el host 1 y copiando los datos en la ubicación original.



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

Con una configuración única de recursos de SnapCenter, se crean copias de Snapshot en ambos volúmenes de almacenamiento de los hosts de replicación del sistema SAP HANA. Solo el backup de Snapshot que se crea en el volumen de almacenamiento del host SAP HANA primario es válido para la recuperación futura. La copia Snapshot creada en el volumen de almacenamiento del host SAP HANA secundario es una imagen de bloqueo que no se puede utilizar para una recuperación posterior.

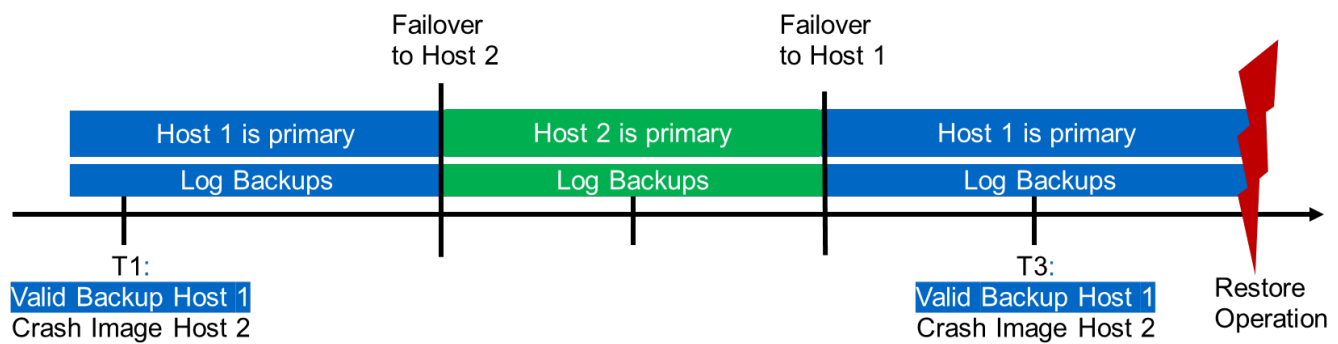
La operación de restauración con SnapCenter se puede ejecutar de dos formas distintas:

- Restaure únicamente la copia de seguridad válida
- Restaurar el recurso completo, incluida la copia de seguridad válida y la imagen de bloqueo.en las siguientes secciones se tratan con más detalle las dos operaciones de restauración diferentes.

Una operación de restauración a partir de un backup que se creó en el otro host se describe en la sección ["Restauración y recuperación a partir de un backup creado en el otro host"](#).

En la siguiente figura, se muestran las operaciones de restauración con una configuración de recursos único

de SnapCenter.

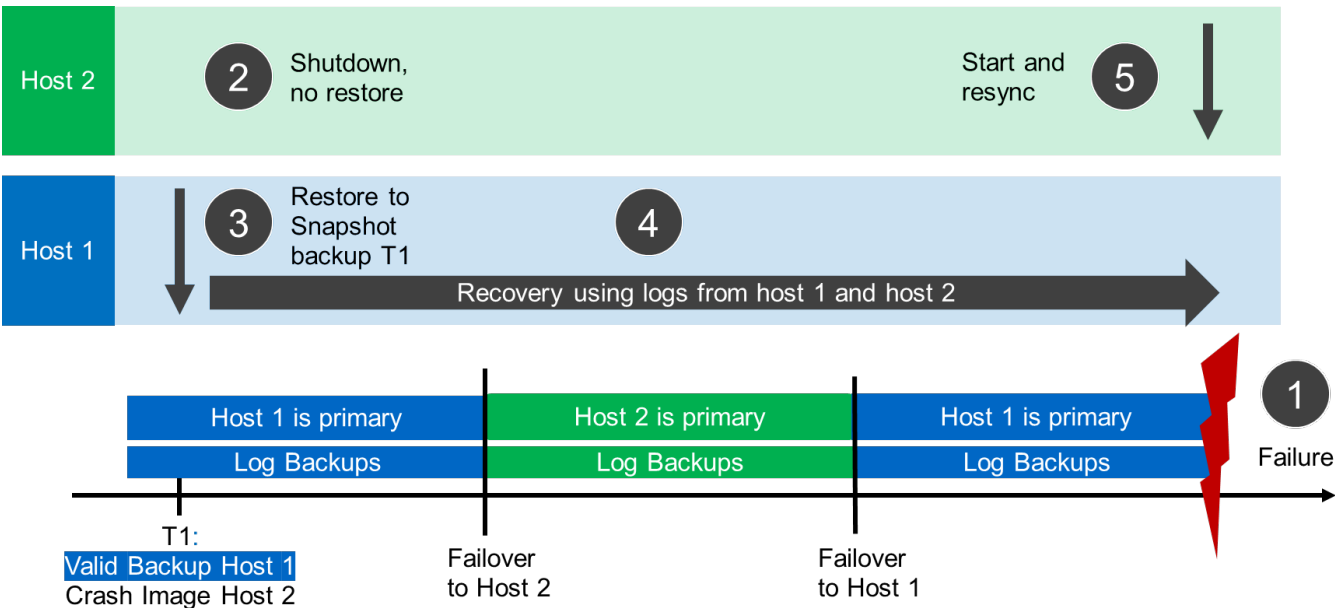


Restauración SnapCenter únicamente del backup válido

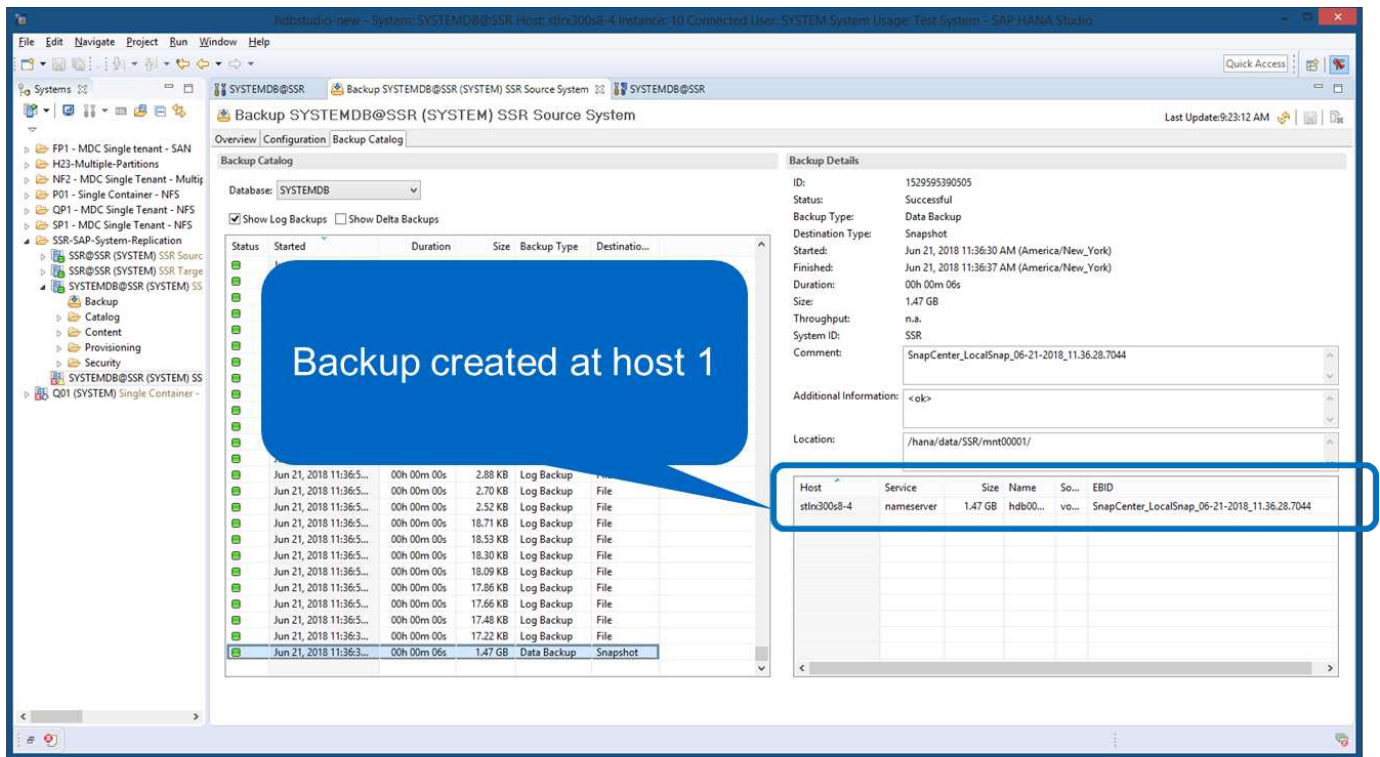
La siguiente figura muestra información general sobre el escenario de restauración y recuperación descrito en esta sección.

Se ha creado un backup en T1 en el host 1. Se ha realizado una conmutación por error al host 2. Después de un momento específico, se ejecutó otro conmutación por error al host 1. En el momento actual, el host 1 es el host primario.

- 1. Se ha producido un fallo y debe restaurar al backup creado en T1 en el host 1.
- 2. El host secundario (host 2) se apaga, pero no se ejecuta ninguna operación de restauración.
- 3. El volumen de almacenamiento del host 1 se restaura al backup creado en T1.
- 4. Se realiza una recuperación de reenvío con registros del host 1 y del host 2.
- 5. Se ha iniciado el host 2 y se inicia automáticamente una resincronización de replicación del sistema del host 2.



La siguiente figura muestra el catálogo de backup de SAP HANA en SAP HANA Studio. El backup resaltado muestra el backup creado en T1 en el host 1.

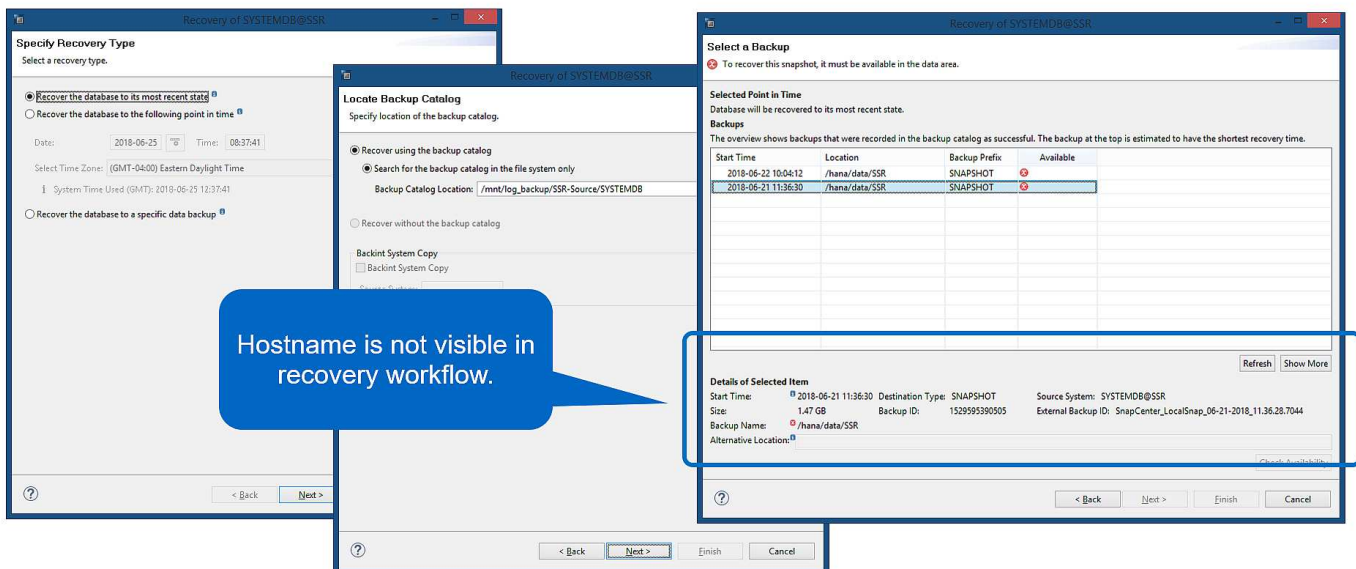


25

Se inicia una operación de restauración y recuperación en SAP HANA Studio. Tal y como se muestra en la siguiente figura, el nombre del host donde se creó el backup no se puede ver en el flujo de trabajo de restauración y recuperación.

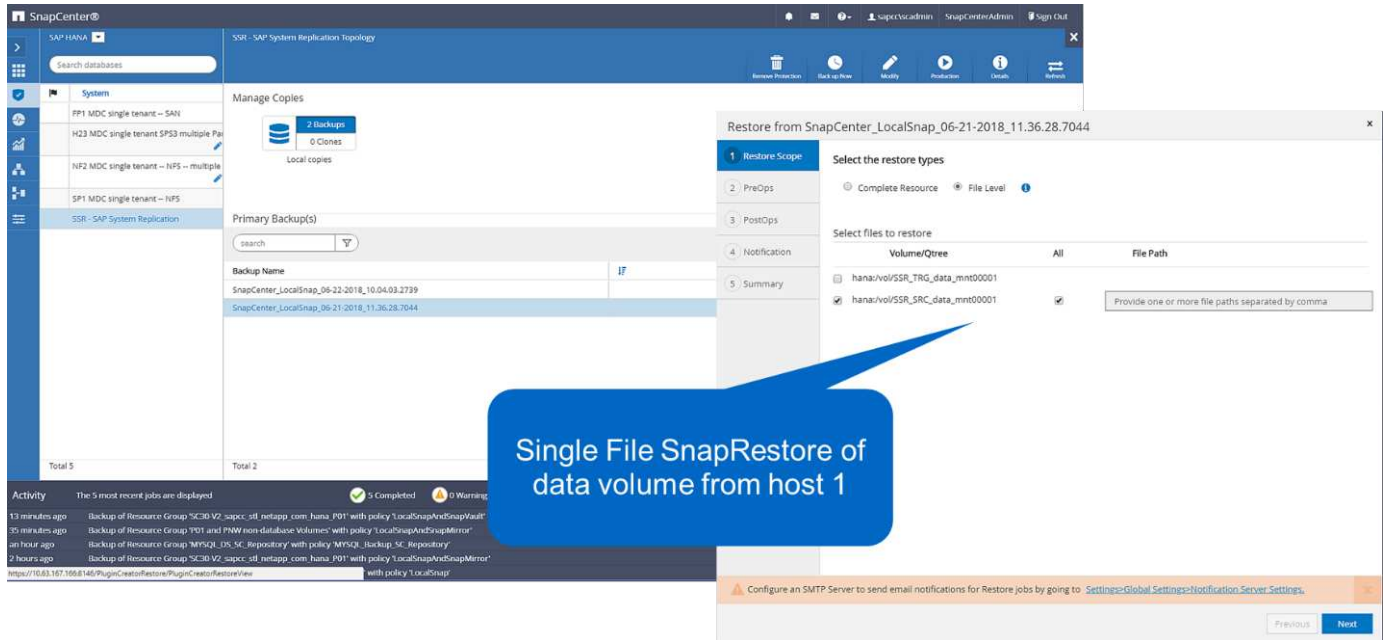


En nuestro supuesto de prueba, pudimos identificar el backup correcto (el backup creado en el host 1) en SAP HANA Studio cuando la base de datos seguía activa. Si la base de datos no está disponible, debe comprobar el registro de los trabajos de backup de SnapCenter para identificar el backup correcto.

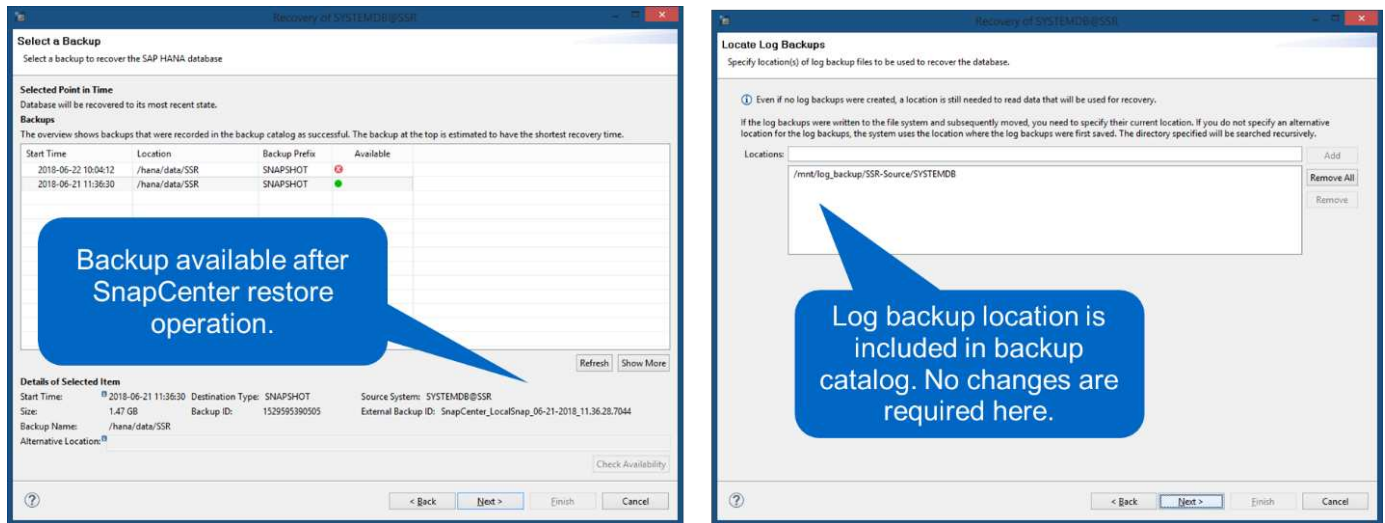


En SnapCenter, se selecciona el backup y se ejecuta una operación de restauración a nivel de archivo. En la

pantalla de restauración del nivel de archivos, solo se selecciona el volumen host 1 para restaurar únicamente el backup válido.



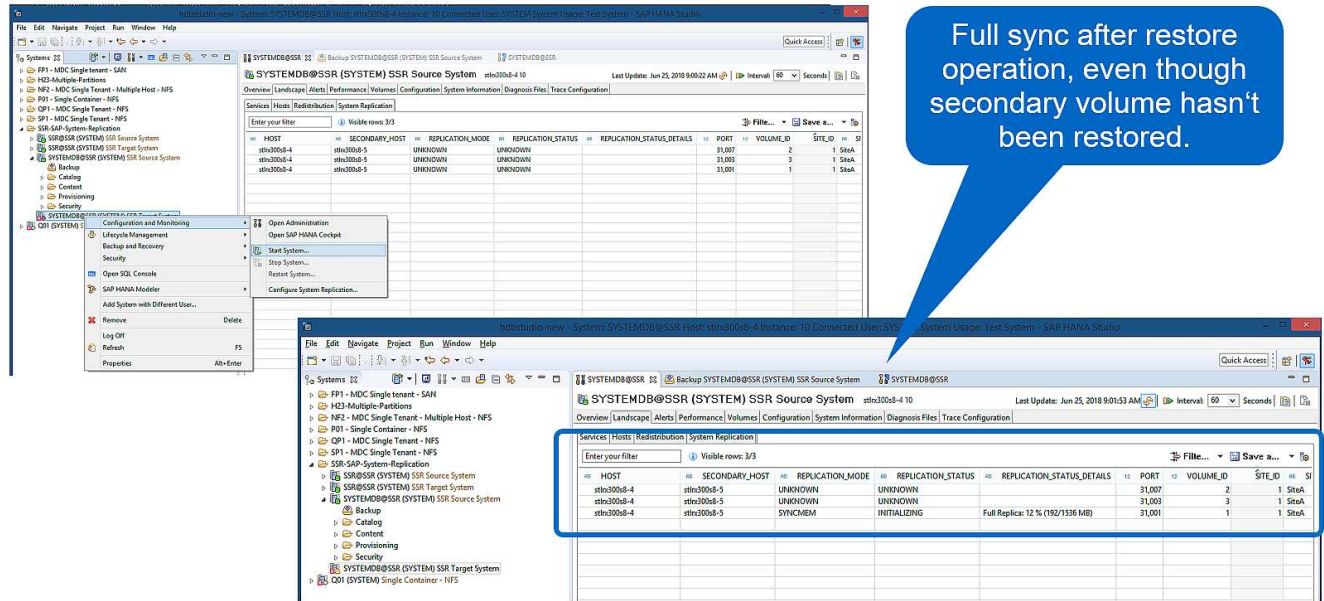
Después de la operación de restauración, el backup se resalta en verde en SAP HANA Studio. No es necesario introducir una ubicación de backup de registros adicional, ya que la ruta de acceso del archivo de los backups de registros del host 1 y del host 2 están incluidos en el catálogo de copias de seguridad.



Una vez finalizada la recuperación, se inicia el host secundario (host 2) y se inicia la resincronización de replicación de sistemas SAP HANA.



Aunque el host secundario esté actualizado (no se ejecutó ninguna operación de restauración para el host 2), SAP HANA ejecuta una replicación completa de todos los datos. Este comportamiento es estándar después de una operación de restauración y recuperación con la replicación de sistemas SAP HANA.

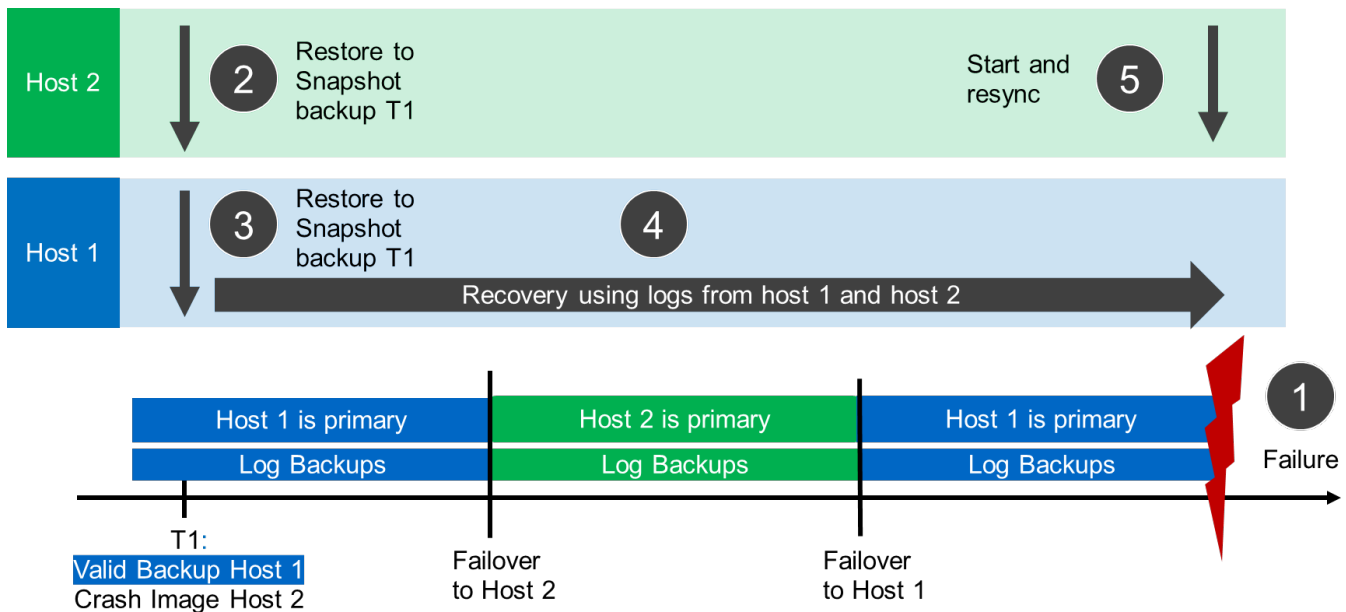


Restauración SnapCenter de una imagen de bloqueo y backup válida

La siguiente figura muestra información general sobre el escenario de restauración y recuperación descrito en esta sección.

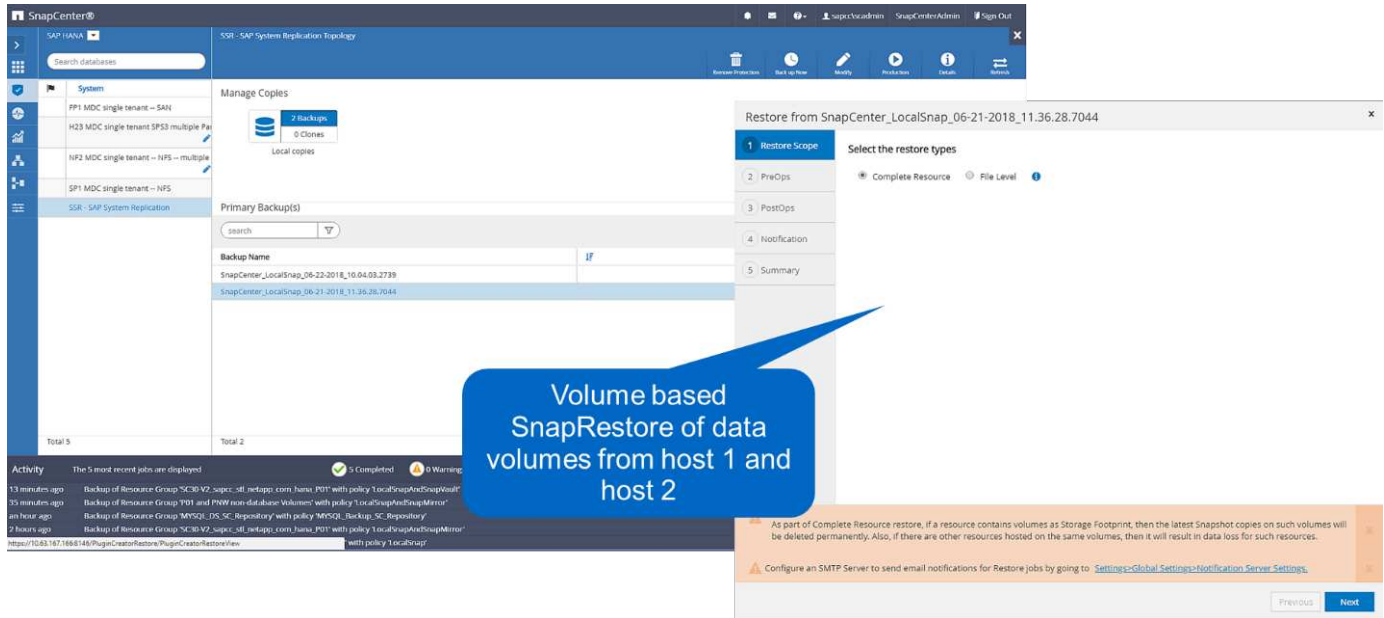
Se ha creado un backup en T1 en el host 1. Se ha realizado una conmutación por error al host 2. Después de un momento específico, se ejecutó otro conmutación por error al host 1. En el momento actual, el host 1 es el host primario.

1. Se ha producido un fallo y debe restaurar al backup creado en T1 en el host 1.
2. El host secundario (host 2) se apaga y se restaura la imagen de fallo T1.
3. El volumen de almacenamiento del host 1 se restaura al backup creado en T1.
4. Se realiza una recuperación de reenvío con registros del host 1 y del host 2.
5. El host 2 se inicia y se inicia automáticamente una resincronización de replicación del sistema del host 2.

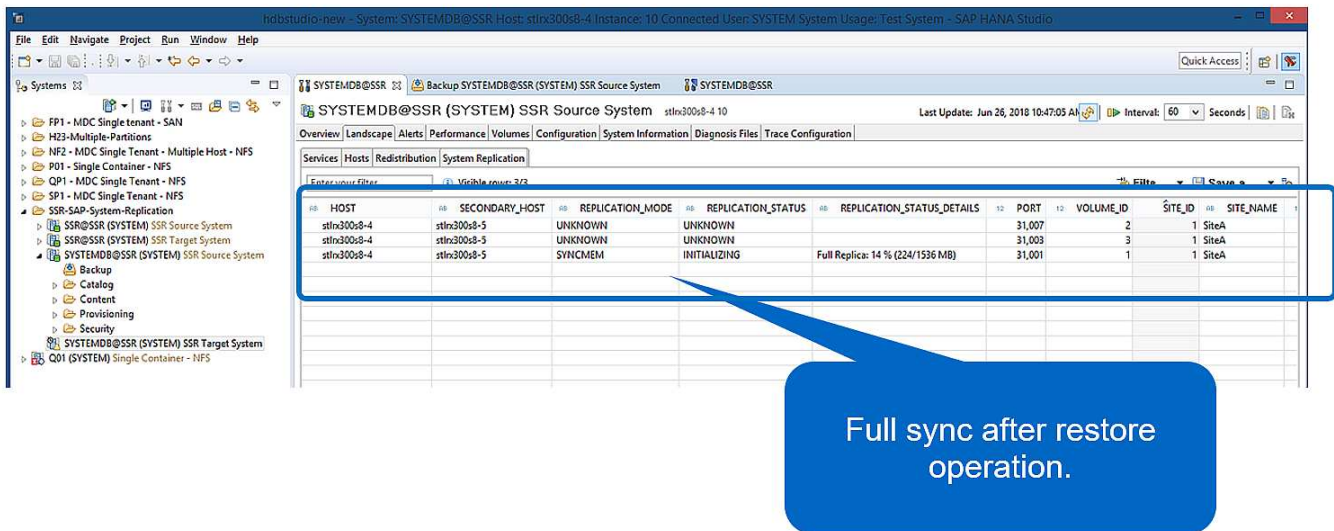


La operación de restauración y recuperación con SAP HANA Studio es idéntica a los pasos descritos en la sección "[Restauración SnapCenter únicamente del backup válido](#)".

Para realizar la operación de restauración, seleccione Complete Resource en SnapCenter. Se restauran los volúmenes de ambos hosts.



Una vez finalizada la recuperación futura, se inicia el host secundario (host 2) y se inicia la resincronización de replicación de sistemas SAP HANA. Se ejecuta una replicación completa de todos los datos.



Restauración y recuperación a partir de un backup creado en el otro host

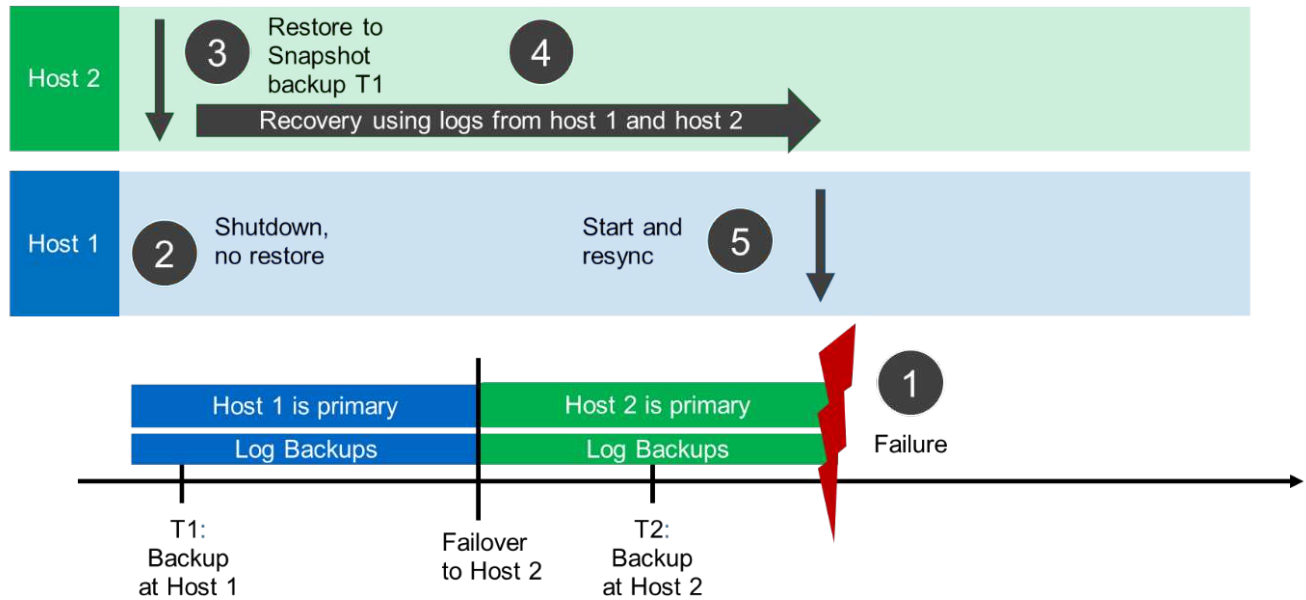
Una operación de restauración a partir de un backup que se creó en el otro host SAP HANA es un escenario válido para ambas opciones de configuración de SnapCenter.

La siguiente figura muestra información general sobre el escenario de restauración y recuperación descrito en

esta sección.

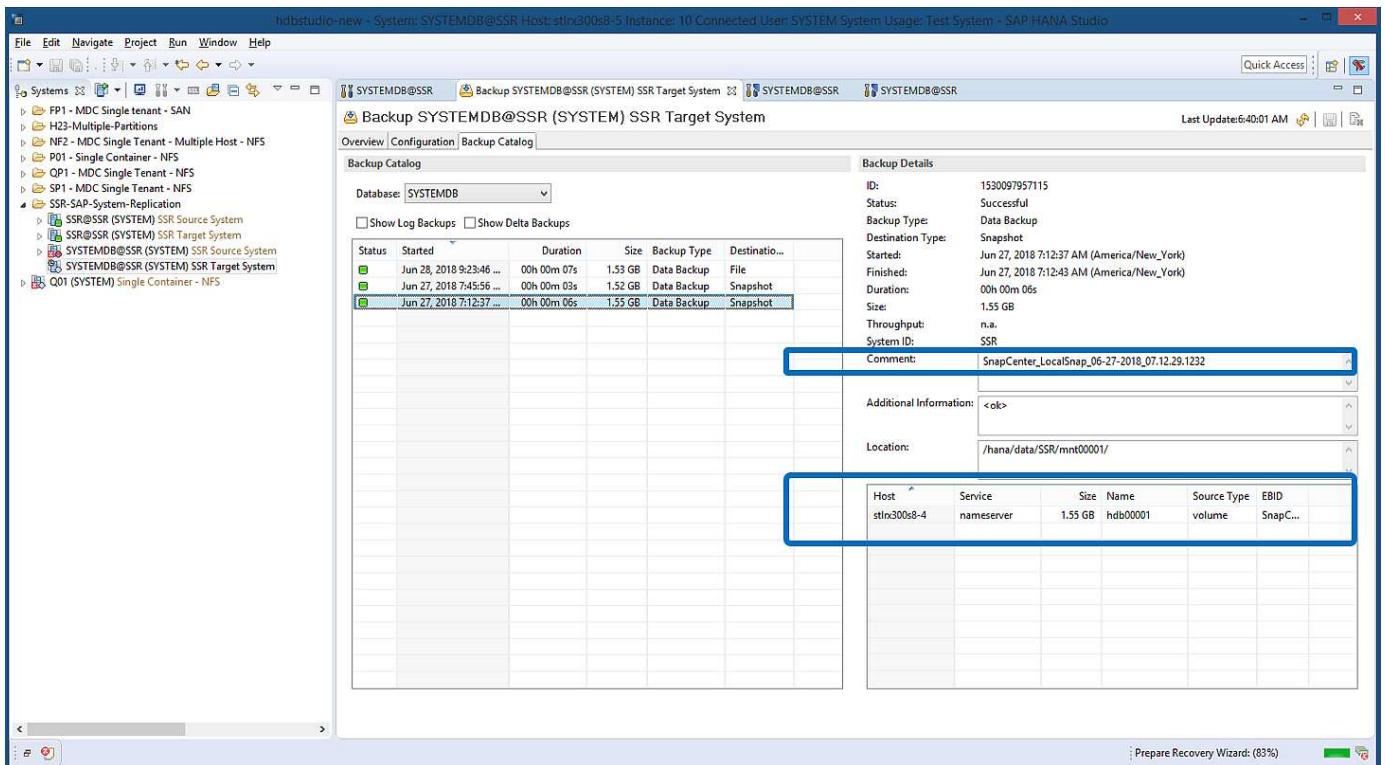
Se ha creado un backup en T1 en el host 1. Se ha realizado una conmutación por error al host 2. En el momento actual, el host 2 es el host primario.

1. Se ha producido un fallo y debe restaurar al backup creado en T1 en el host 1.
2. El host primario (host 1) se apaga.
3. Los datos de backup T1 del host 1 se restauran en el host 2.
4. La recuperación futura se realiza con registros del host 1 y del host 2.
5. Se inicia el host 1 y se inicia automáticamente una resincronización de replicación del sistema del host 1.



31

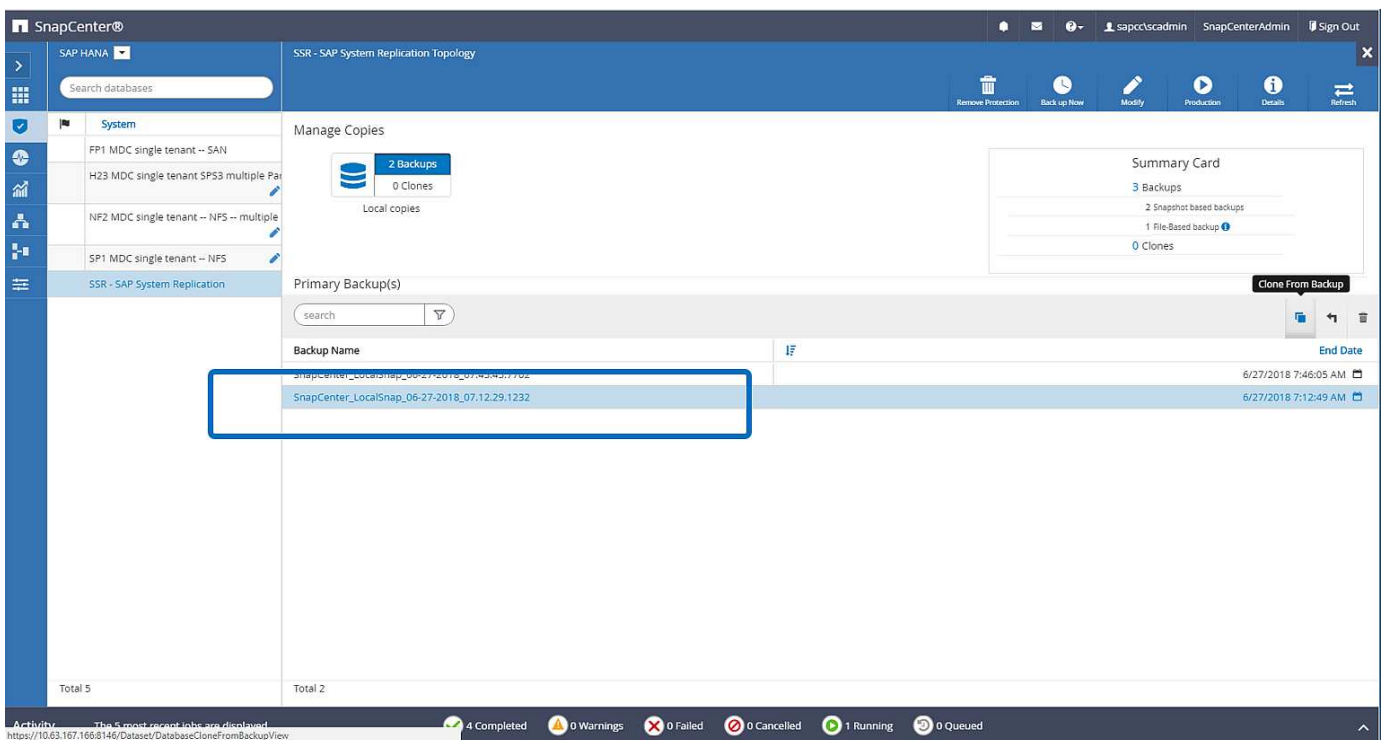
En la siguiente figura, se muestra el catálogo de backup de SAP HANA y se destaca el backup, creado en el host 1, que se utilizó para la operación de restauración y recuperación.



La operación de restauración conlleva los siguientes pasos:

1. Crear un clon desde el backup creado en el host 1.
2. Monte el volumen clonado en el host 2.
3. Copie los datos del volumen clonado en la ubicación original.

En SnapCenter, se selecciona el backup y se inicia la operación de clonado.



Debe proporcionar el servidor de clonado y la dirección IP de exportación de NFS.



En una configuración de recurso único de SnapCenter, el plugin de SAP HANA no está instalado en el host de base de datos. Para ejecutar el flujo de trabajo de clonado de SnapCenter, cualquier host con un plugin de HANA instalado se puede usar como servidor de clones.

+ en una configuración de SnapCenter con recursos independientes, el host de la base de datos HANA se selecciona como servidor de clones y se utiliza un script de montaje para montar el clon en el host de destino.

Clone from Backup

1 Location

Select the host to create the clone

Clone server: stlr300s8-7.stl.netapp.com

Clone suffix: _clone_date_time

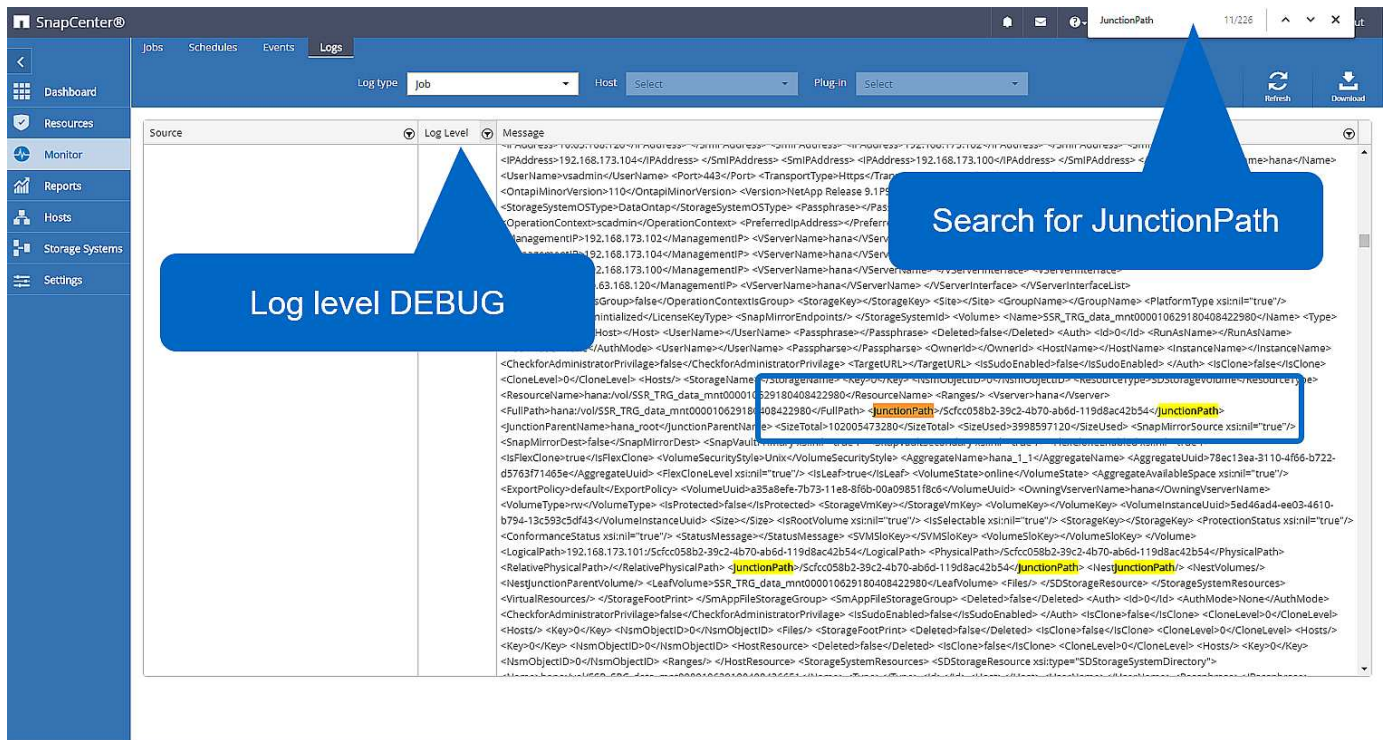
NFS Export IP Address: 192.168.173.71

Any host with installed HANA plug-in can be used. Not required to install the plug-in on the System Replication host.

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

Previous Next

Para determinar la ruta de unión necesaria para montar el volumen clonado, compruebe el registro de trabajos del trabajo de clonado, como se muestra en la siguiente figura.



Ahora el volumen clonado puede montarse.

```
stlrx300s8-5:/mnt/tmp # mount 192.168.173.101:/Sc373da37-00ff-4694-b1e1-8153dbd46caf /mnt/tmp
```

El volumen clonado contiene los datos de la base de datos HANA.

```
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
```

Los datos se copian en la ubicación original.

```
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/
```

La recuperación con SAP HANA Studio se realiza tal y como se describe en la sección "[Restauración SnapCenter únicamente del backup válido](#)".

Dónde encontrar información adicional

Si quiere obtener más información sobre la información descrita en este documento, consulte los siguientes documentos:

- Backup y recuperación de datos de SAP HANA con SnapCenter

["https://www.netapp.com/us/media/tr-4614.pdf"](https://www.netapp.com/us/media/tr-4614.pdf)

- Automatización de las operaciones de copia y clonado del sistema SAP HANA con SnapCenter

["https://docs.netapp.com/us-en/netapp-solutions-sap/lifecycle/sc-copy-clone-introduction.html"](https://docs.netapp.com/us-en/netapp-solutions-sap/lifecycle/sc-copy-clone-introduction.html)

- Recuperación ante desastres de SAP HANA con replicación de almacenamiento

["https://www.netapp.com/us/media/tr-4646.pdf"](https://www.netapp.com/us/media/tr-4646.pdf)

Historial de versiones

| Versión | Fecha | Historial de versiones del documento |
|-------------|-----------------|---|
| Versión 1.0 | Octubre de 2018 | Versión inicial |
| Versión 2.0 | Enero de 2022 | Actualización para cubrir el soporte de replicación del sistema SnapCenter 4.6 HANA |

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.