SAP HANA System Replication Backup und Recovery mit SnapCenter

NetApp solutions for SAP

NetApp
December 10, 2025

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions-sap/backup/hana-sr-scs-system-replication-overview.html on December 10, 2025. Always check docs.netapp.com for the latest.

Inhalt

SAP HANA System Replication Backup und Recovery mit SnapCenter

TR-4719: SAP HANA System Replication – Backup und Recovery mit SnapCenter

SAP HANA System Replication wird häufig als Hochverfügbarkeits- oder Disaster-Recovery-Lösung für SAP HANA Datenbanken verwendet. SAP HANA System Replication bietet verschiedene Betriebsmodi, die Sie je nach Anwendungsfall oder Verfügbarkeitsanforderungen verwenden können.

Autor: Nils Bauer, NetApp

Es gibt zwei primäre Anwendungsfälle, die miteinander kombiniert werden können:

- Hochverfügbarkeit mit einem Recovery Point Objective (RPO) von null und einem minimalen Recovery Time Objective (RTO) unter Verwendung eines dedizierten sekundären SAP HANA-Hosts
- Disaster Recovery über große Entfernungen: Der sekundäre SAP HANA-Host kann auch im normalen Betrieb für Entwicklung oder Tests verwendet werden.

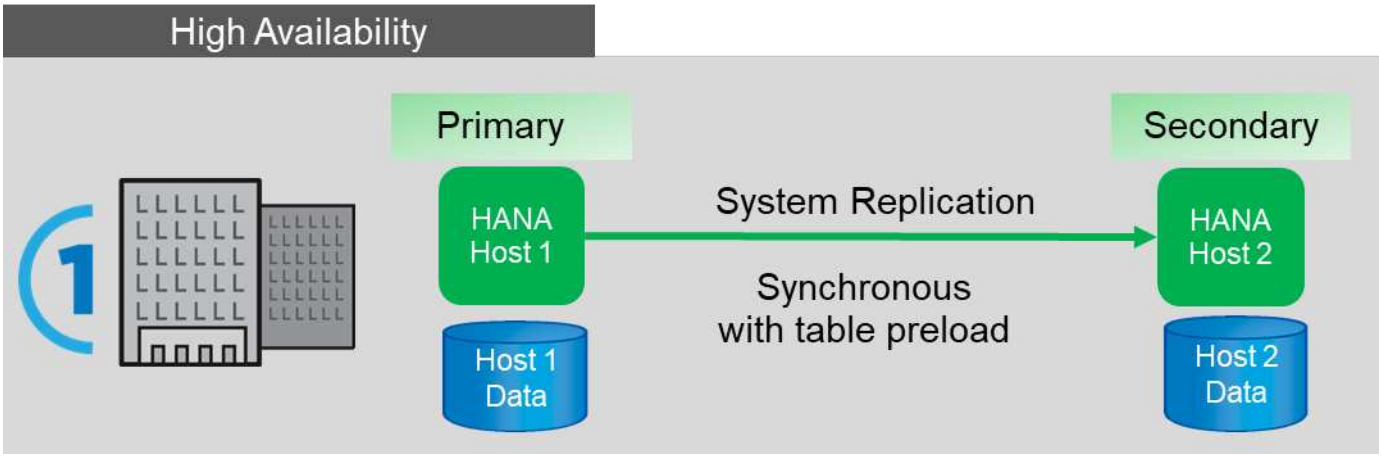
Hochverfügbarkeit ohne RPO und mit minimalem RTO-Aufwand

System Replication ist mit synchroner Replizierung konfiguriert und verwendet Tabellen, die auf dem sekundären SAP HANA-Host vorab in den Speicher geladen sind. Diese Hochverfügbarkeitslösung lässt sich bei Hardware- oder Softwareausfällen einsetzen und reduziert zudem geplante Ausfallzeiten während SAP HANA Software-Upgrades (Betrieb fast ohne Ausfallzeit).

Failover-Vorgänge werden oft mithilfe von Cluster-Software eines Drittanbieters oder mit einem Workflow mit SAP Landscape Management Software mit nur einem Klick automatisiert.

Aus der Perspektive der Backup-Anforderungen müssen Backups erstellt werden können, unabhängig davon, welcher SAP HANA Host primärer oder sekundärer ist. Eine gemeinsam genutzte Backup-Infrastruktur wird verwendet, um alle Backups wiederherzustellen, unabhängig davon, auf welchem Host das Backup erstellt wurde.

Der Rest dieses Dokuments konzentriert sich auf Backup-Vorgänge mit SAP System Replication, konfiguriert als Hochverfügbarkeitslösung.



Disaster Recovery über große Entfernungen

Die Systemreplizierung kann mit asynchroner Replizierung konfiguriert werden, ohne dass Tabelle auf dem sekundären Host vorab in den Speicher geladen wird. Diese Lösung dient der Behebung von Datacenter-Ausfällen. Failover-Vorgänge werden normalerweise manuell durchgeführt.

Hinsichtlich der Backup-Anforderungen müssen Sie in der Lage sein, Backups während des normalen Betriebs in Datacenter 1 und bei Disaster Recovery in Datacenter 2 zu erstellen. In Datacentern 1 und 2 ist eine separate Backup-Infrastruktur verfügbar, Backup-Vorgänge werden als Teil des Disaster Failover aktiviert. Die Backup-Infrastruktur ist in der Regel nicht gemeinsam genutzt und ein Restore eines Backups, das auf dem anderen Datacenter erstellt wurde, ist nicht möglich.

Storage Snapshot Backups und SAP System Replication

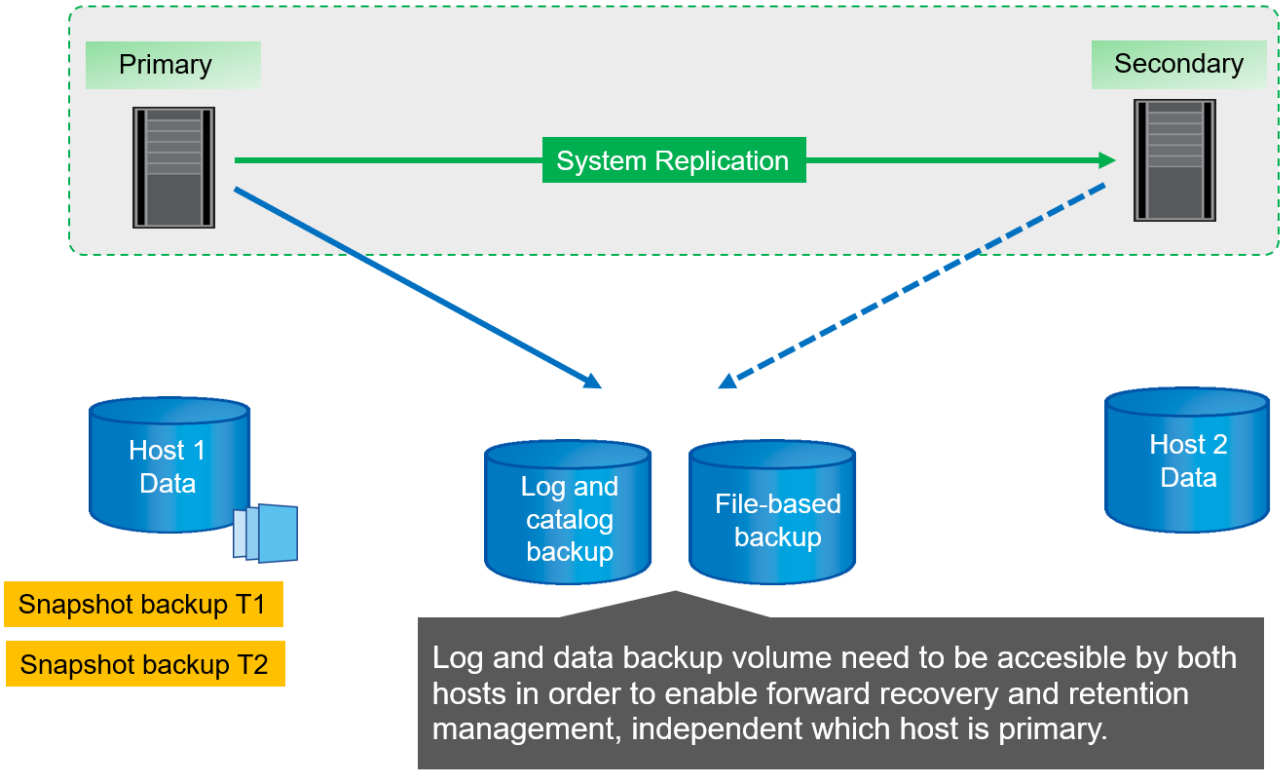
Backup-Vorgänge werden immer auf dem primären SAP HANA-Host durchgeführt. Die erforderlichen SQL-Befehle für den Backup-Vorgang können nicht auf dem sekundären SAP HANA-Host ausgeführt werden.

Für SAP HANA-Backup-Vorgänge sind die primären und sekundären SAP HANA-Hosts eine Einheit. Sie verwenden denselben SAP HANA Backup-Katalog und nutzen die Backups für die Wiederherstellung und das Recovery, unabhängig davon, ob das Backup auf dem primären oder sekundären SAP HANA-Host erstellt wurde.

Da jedes Backup für die Wiederherstellung verwendet und mithilfe von Log-Backups von beiden Hosts durchgeführt werden kann, ist ein gemeinsamer Backup-Ort für Protokolle erforderlich, auf den von beiden Hosts zugegriffen werden kann. NetApp empfiehlt die Verwendung eines Shared Storage Volume. Sie sollten jedoch auch das Ziel der Protokollsicherung in Unterverzeichnisse innerhalb des gemeinsam genutzten Volumes trennen.

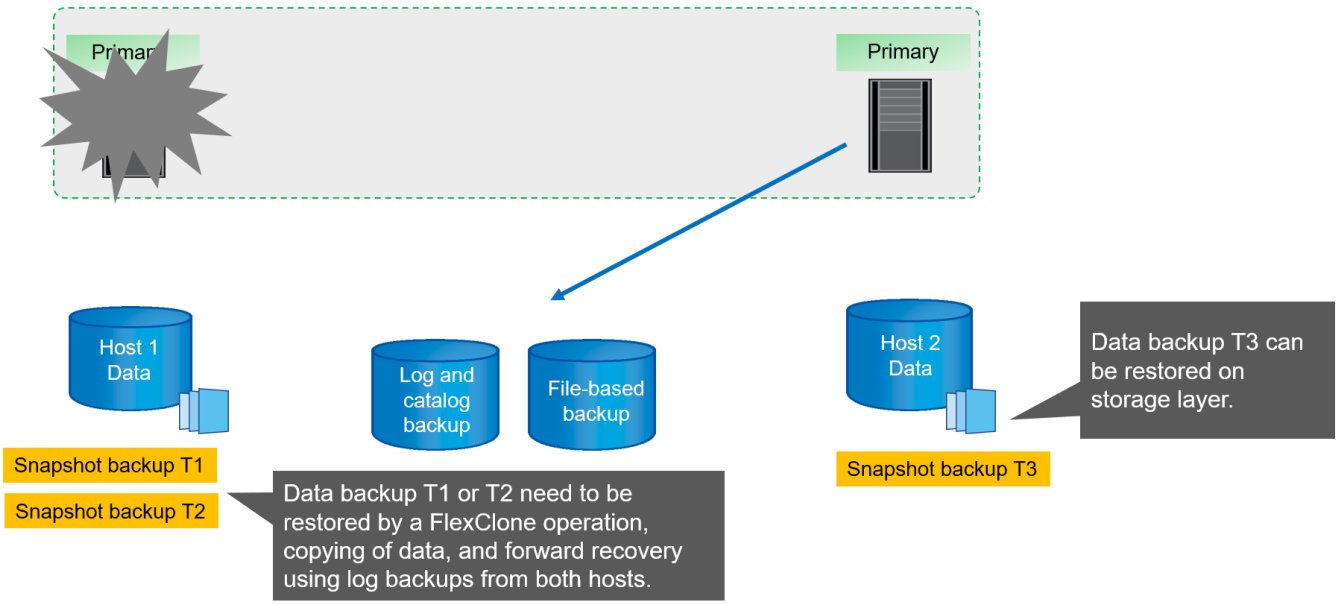
Jeder SAP HANA-Host verfügt über ein eigenes Storage-Volume. Wenn Sie einen Storage-basierten Snapshot

für ein Backup verwenden, wird ein Datenbank-konsistenter Snapshot auf dem Speicher-Volume des primären SAP HANA-Hosts erstellt.



Wenn ein Failover zu Host 2 durchgeführt wird, wird Host 2 zum primären Host, die Backups werden auf Host 2 ausgeführt und Snapshot Backups werden auf dem Storage Volume von Host 2 erstellt.

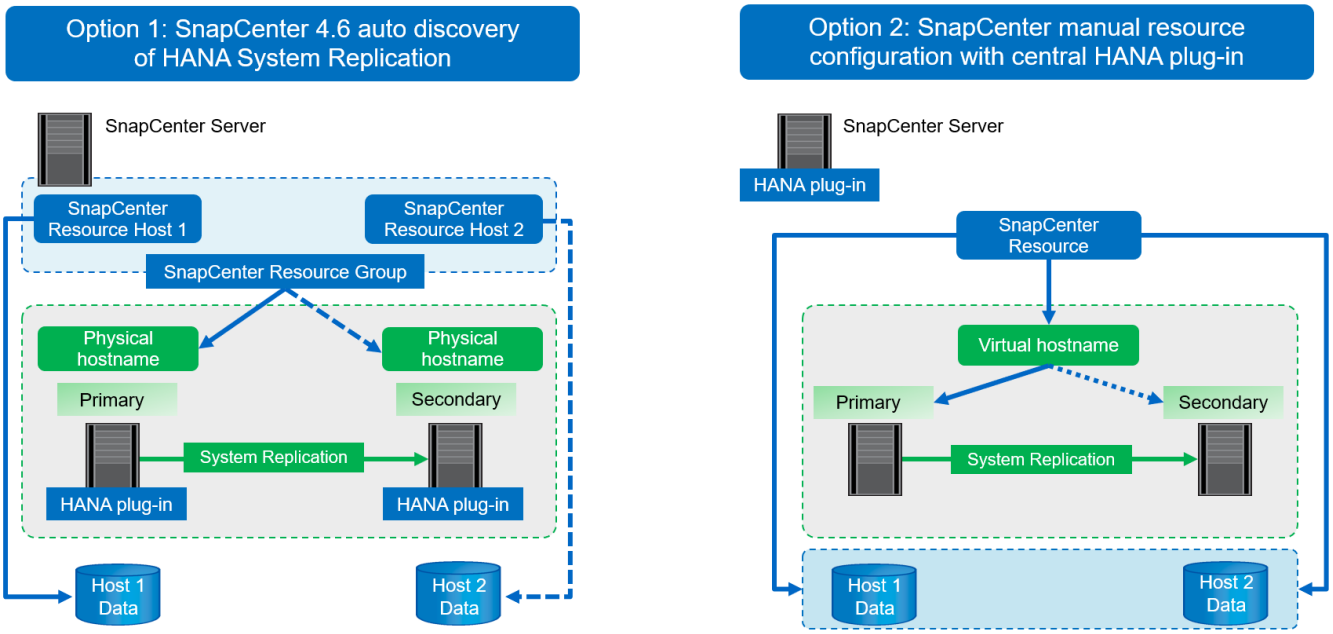
Das auf Host 2 erstellte Backup kann direkt auf der Speicherebene wiederhergestellt werden. Wenn Sie ein Backup verwenden müssen, das auf Host 1 erstellt wurde, muss das Backup vom Host-1-Speicher-Volume auf das Host-2-Speicher-Volume kopiert werden. Die vorwärts-Wiederherstellung verwendet die Protokoll-Backups von beiden Hosts.



SnapCenter Konfigurationsoptionen für SAP System Replication

Es gibt zwei Optionen zur Konfiguration der Datensicherung mit der NetApp SnapCenter Software in einer SAP HANA System Replication Umgebung:

- Eine SnapCenter-Ressourcengruppe, die sowohl SAP HANA-Hosts als auch automatische Erkennung mit SnapCenter Version 4.6 oder höher enthält
- Eine einzige SnapCenter-Ressource für beide SAP HANA-Hosts, die eine virtuelle IP-Adresse verwendet



Ab SnapCenter 4.6 unterstützt SnapCenter die automatische Erkennung von HANA-Systemen, die in einer HANA-System-Replizierungsbeziehung konfiguriert sind. Jeder Host wird mit seiner physischen IP-Adresse (Host-Name) und seinem individuellen Daten-Volume auf der Storage-Ebene konfiguriert. Die beiden SnapCenter Ressourcen werden zu einer Ressourcengruppe kombiniert. SnapCenter erkennt automatisch, welcher Host sich auf einem primären oder sekundären Volume befindet, und führt die erforderlichen Backup-Vorgänge entsprechend aus. Das Aufbewahrungsmanagement für Snapshot und dateibasierte Backups, die durch SnapCenter erstellt wurden, erfolgt über beide Hosts hinweg. So wird sichergestellt, dass alte Backups auch am aktuellen sekundären Host gelöscht werden.

Mit einer Einzelressourcenkonfiguration für beide SAP HANA-Hosts ist die einzelne SnapCenter-Ressource unter Verwendung der virtuellen IP-Adresse der SAP HANA System Replication-Hosts konfiguriert. Beide Datenvolumen der SAP HANA-Hosts sind in der SnapCenter-Ressource enthalten. Da es sich um eine einzelne SnapCenter Ressource handelt, funktioniert das Aufbewahrungsmanagement für Snapshot und dateibasierte Backups, die von SnapCenter erstellt wurden, unabhängig davon, welcher Host derzeit als primärer oder sekundärer Host gilt. Diese Option ist bei allen SnapCenter Versionen möglich.

In der folgenden Tabelle sind die wichtigsten Unterschiede der beiden Konfigurationsoptionen zusammengefasst.

	Ressourcengruppe mit SnapCenter 4.6	Einzelne SnapCenter-Ressource und virtuelle IP-Adresse
Backup-Vorgang (Snapshot und dateibasiert)	Automatische Identifizierung des primären Hosts in der Ressourcengruppe	Virtuelle IP-Adresse automatisch verwenden
Aufbewahrungsmanagement (Snapshot und dateibasiert)	Automatisch auf beiden Hosts ausgeführt	Automatische Verwendung einzelner Ressourcen
Kapazitätsanforderungen des Backups	Backups werden nur auf dem primären Host Volume erstellt	Backups werden immer auf beiden Hosts Volumes erstellt. Das Backup des zweiten Hosts ist nur absturzkonsistent und kann nicht verwendet werden, um eine Rollback durchzuführen.
Wiederherstellungsvorgang	Backups von aktuell aktivem Host stehen für die Wiederherstellung zur Verfügung	Skript zur Vorsicherung erforderlich, um zu ermitteln, welche Backups gültig sind und für die Wiederherstellung verwendet werden können
Recovery-Vorgang	Alle verfügbaren Recovery-Optionen, wie bei jeder automatisch erkannten Ressource	Manuelle Wiederherstellung erforderlich

Im Allgemeinen empfiehlt NetApp, die Konfigurationsoption für Ressourcengruppen mit SnapCenter 4.6 zu verwenden, um HANA Systeme mit aktivierter HANA System Replication zu schützen. Eine einzelne SnapCenter-Ressourcenkonfiguration ist nur erforderlich, wenn der SnapCenter-Operationsansatz auf einem zentralen Plug-in-Host basiert und das HANA-Plug-in nicht auf den HANA-Datenbank-Hosts implementiert ist.

Die beiden Optionen werden in den folgenden Abschnitten näher erläutert.

Konfiguration von SnapCenter 4.6 unter Verwendung einer Ressourcengruppe

SnapCenter 4.6 unterstützt die automatische Erkennung von HANA-Systemen, die mit HANA System Replication konfiguriert sind. SnapCenter 4.6 umfasst die Logik zur Identifizierung primärer und sekundärer HANA-Hosts während des Backup-Betriebs sowie für das Management der Datenaufbewahrung über beide HANA-Hosts hinweg. Darüber hinaus sind jetzt auch automatisierte Wiederherstellungen und Recovery für HANA System Replication-Umgebungen verfügbar.

SnapCenter 4.6-Konfiguration von HANA System Replication-Umgebungen

Die folgende Abbildung zeigt die für dieses Kapitel verwendete Laboreinrichtung. Zwei HANA-Hosts, hana-3 und hana-4, wurden mit HANA System Replication konfiguriert.

Für die HANA-Systemdatenbank wurde ein Datenbankbenutzer namens „SnapCenter“ mit den erforderlichen Berechtigungen zum Ausführen von Sicherungs- und Wiederherstellungsvorgängen erstellt (siehe "Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter"). Auf beiden Hosts muss ein HANA-

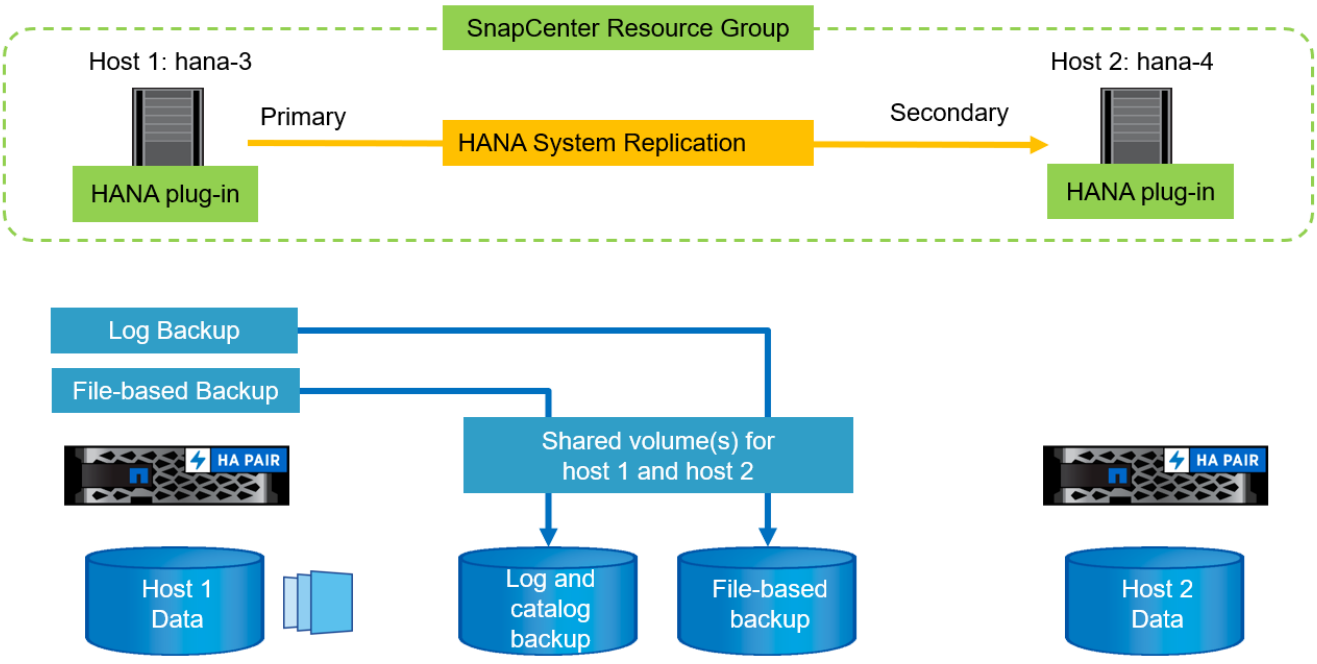
Benutzerspeicherschlüssel unter Verwendung des oben genannten Datenbankbenutzers konfiguriert werden.

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

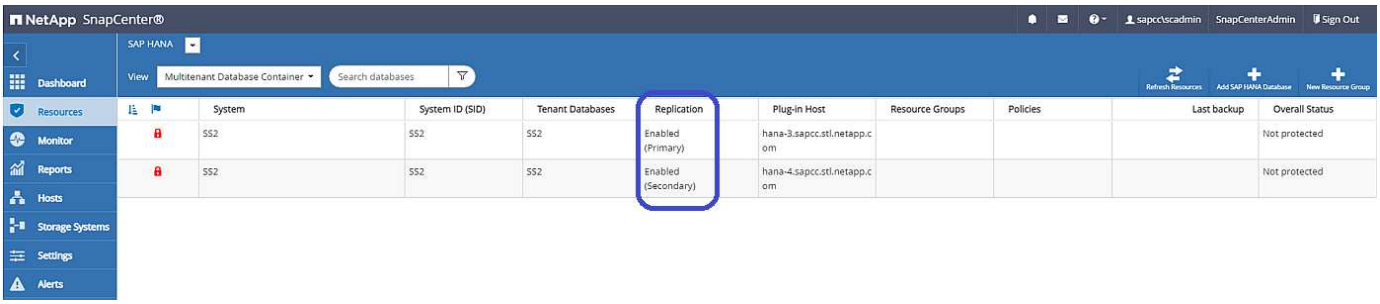
```
ss2adm@hana- 4:/ > hdbuserstore set SS2KEY hana-4:33313 SNAPCENTER
<password>
```

Aus einer übergeordneten Sicht müssen Sie die folgenden Schritte durchführen, um HANA System Replication in SnapCenter einzurichten.

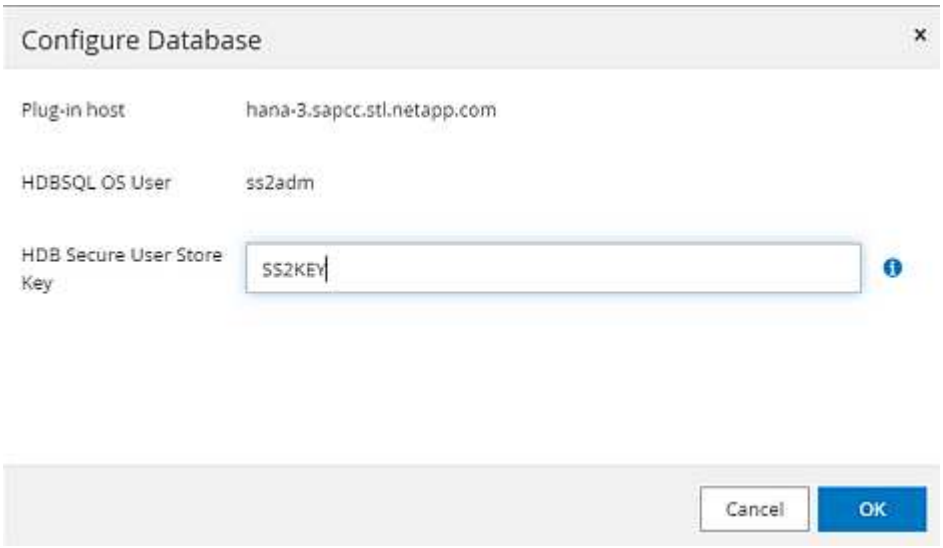
1. Das HANA-Plug-in wird auf dem primären und sekundären Host installiert. Die automatische Ermittlung wird ausgeführt und der Status der HANA-Systemreplizierung wird für jeden primären oder sekundären Host erkannt.
2. Ausführen von SnapCenter `configure database` Und stellen die bereit `hdbuserstore` Taste. Weitere automatische Erkennungsvorgänge werden ausgeführt.
3. Erstellen Sie eine Ressourcengruppen, einschließlich beider Hosts, und konfigurieren Sie den Schutz.



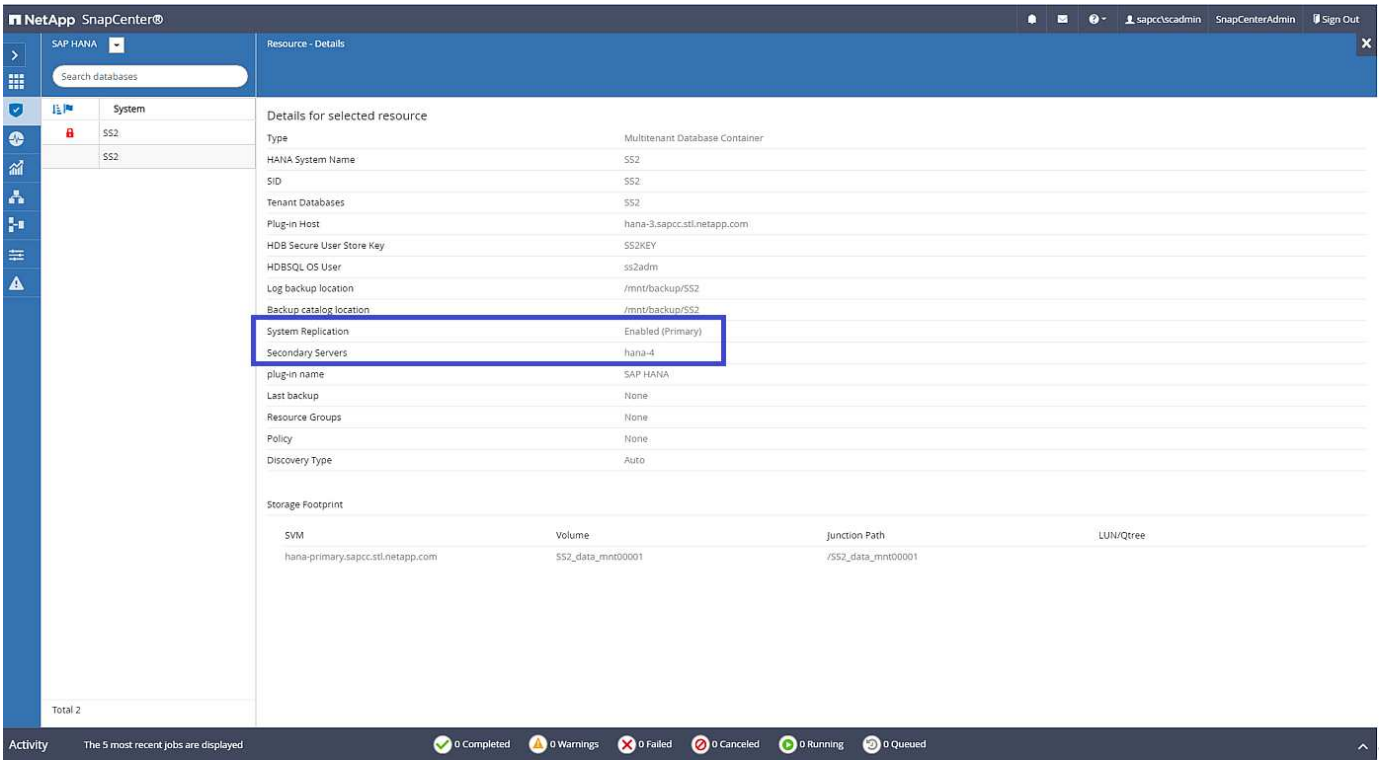
Nachdem Sie das SnapCenter HANA Plug-in auf beiden HANA-Hosts installiert haben, werden die HANA-Systeme in der Ansicht der SnapCenter-Ressourcen wie andere automatisch erkannte Ressourcen angezeigt. Ab SnapCenter 4.6 wird eine zusätzliche Spalte angezeigt, in der der Status der HANA-Systemreplizierung (aktiviert/deaktiviert, primär/sekundär) angezeigt wird.



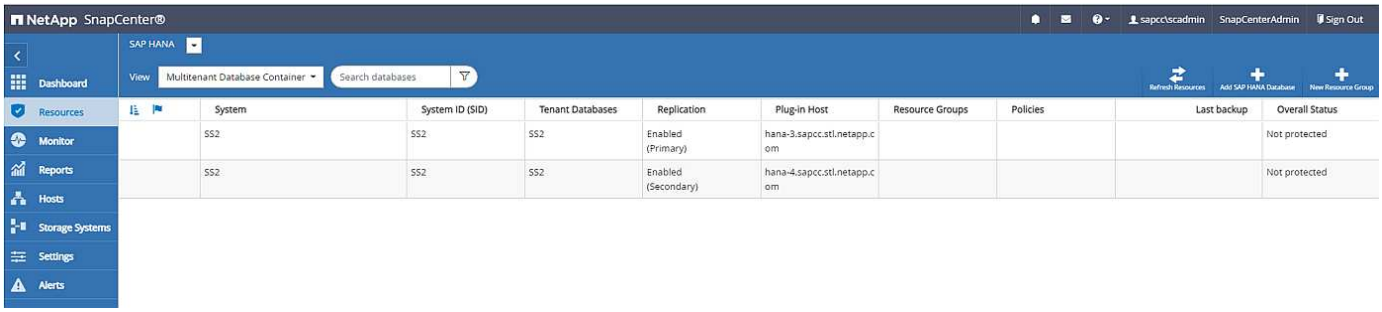
Durch Klicken auf die Ressource fordert SnapCenter den HANA-Benutzerspeicherschlüssel für das HANA-System an.



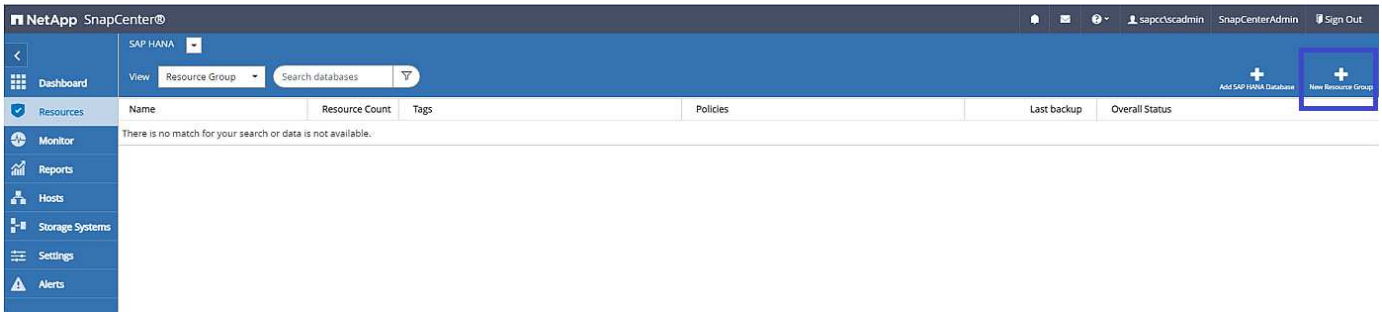
Weitere Schritte zur automatischen Ermittlung werden ausgeführt, und SnapCenter zeigen die Ressourcendetails an. In SnapCenter 4.6 werden der Replikationsstatus des Systems und der sekundäre Server in dieser Ansicht aufgelistet.



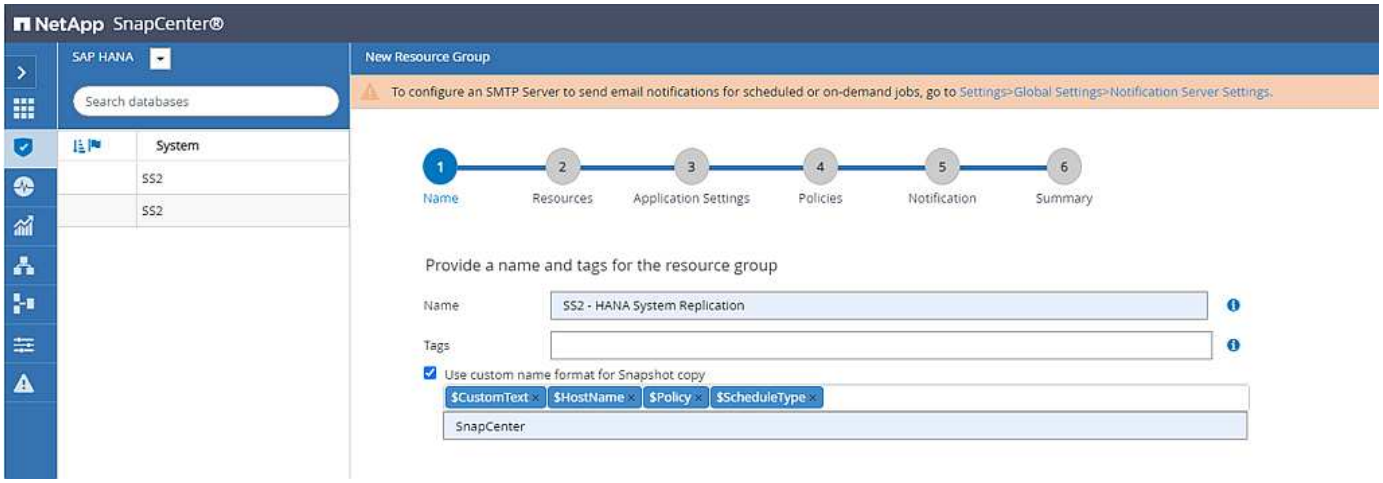
Nach Durchführung der gleichen Schritte für die zweite HANA-Ressource ist die automatische Ermittlung abgeschlossen, und beide HANA-Ressourcen werden in SnapCenter konfiguriert.



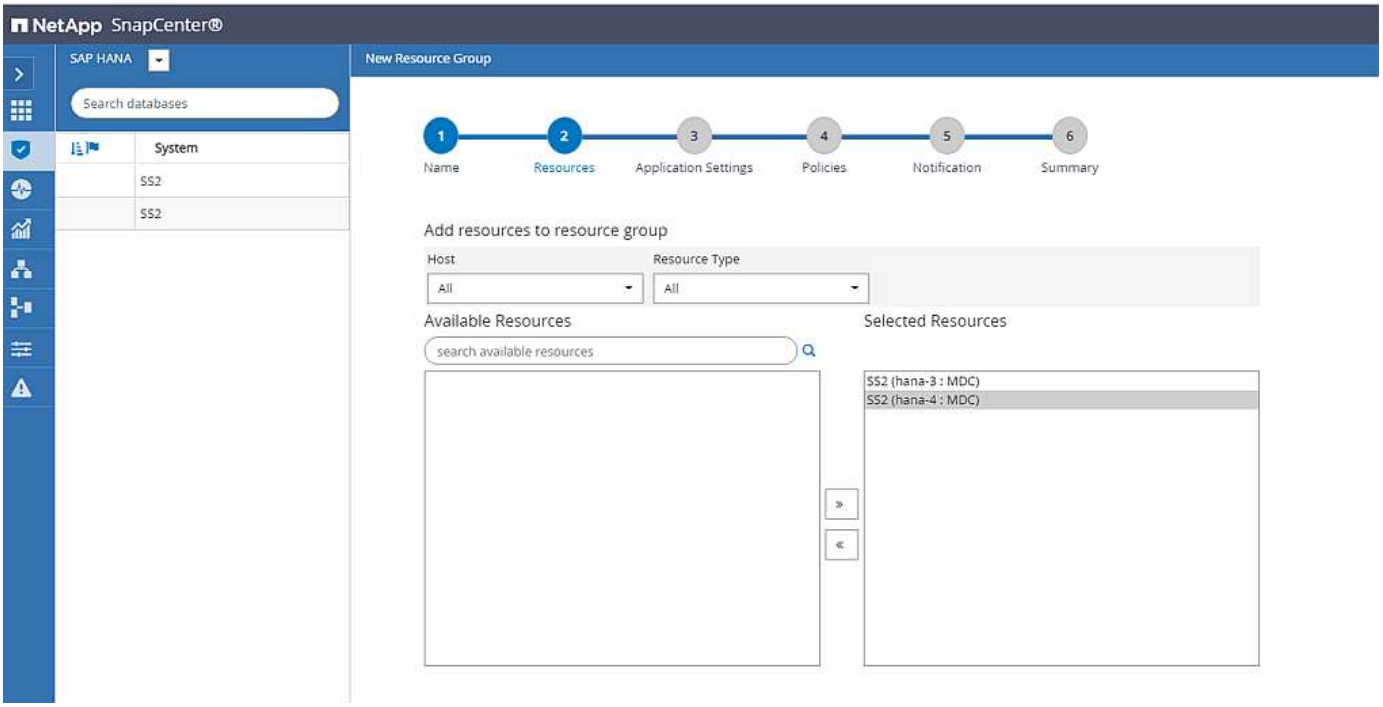
Für HANA System Replication-fähige Systeme müssen Sie eine SnapCenter-Ressourcengruppe, einschließlich beider HANA-Ressourcen, konfigurieren.



NetApp empfiehlt die Verwendung eines benutzerdefinierten Namensformats für den Snapshot-Namen. Dieser sollte den Hostnamen, die Richtlinie und den Zeitplan enthalten.

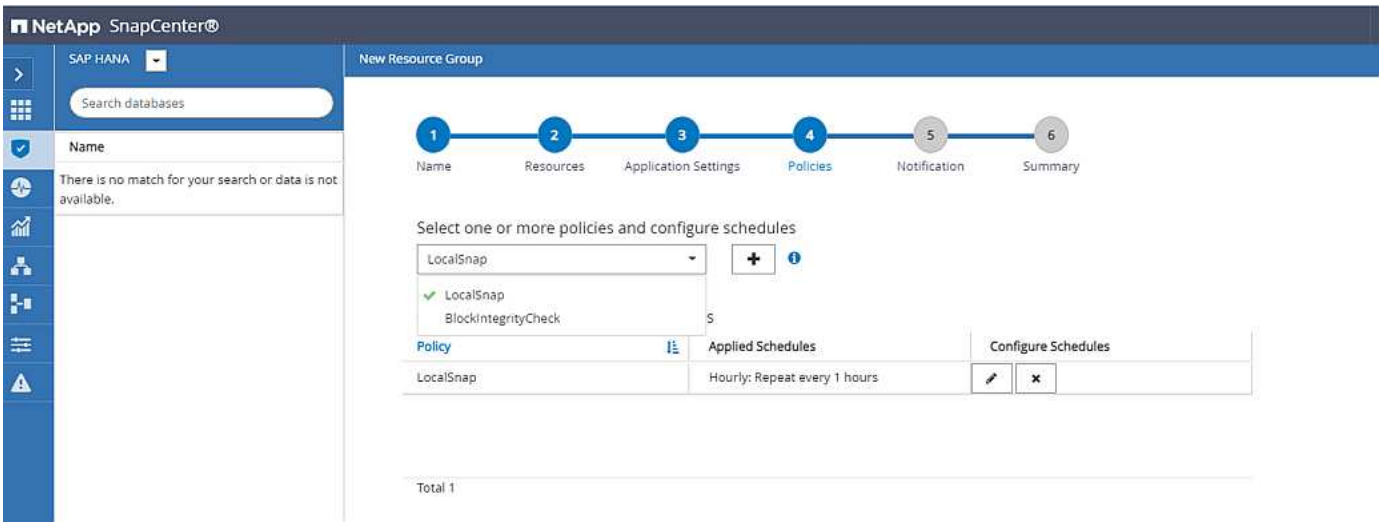


Sie müssen der Ressourcengruppe beide HANA-Hosts hinzufügen.

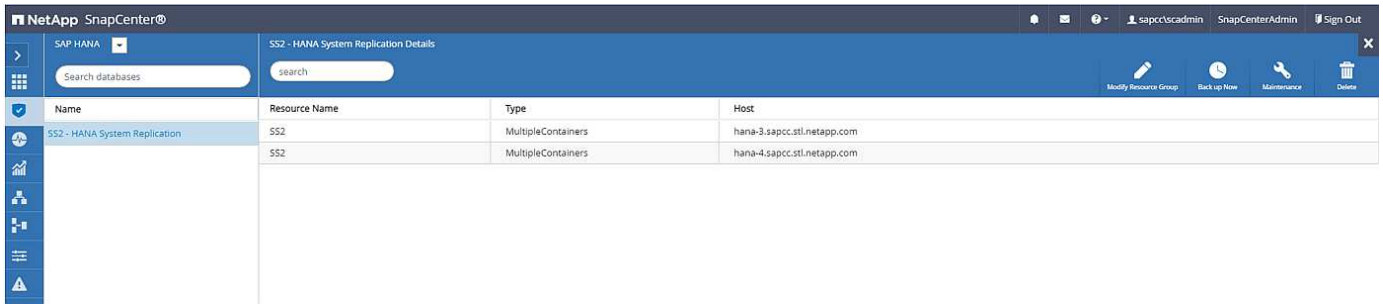


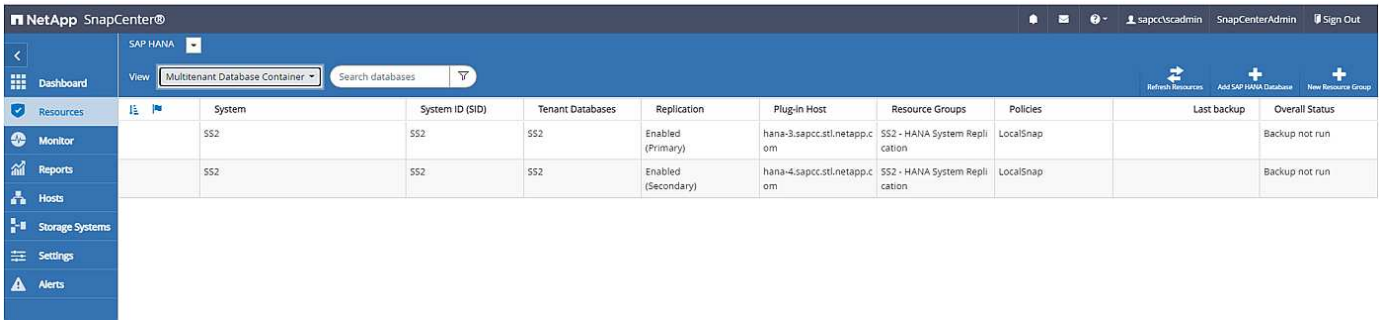
Die Richtlinien und Zeitpläne für die Ressourcengruppe werden konfiguriert.

Die in der Richtlinie definierte Aufbewahrung wird für beide HANA-Hosts verwendet. Wenn z. B. eine Aufbewahrung von 10 in der Richtlinie definiert ist, wird die Summe der Backups beider Hosts als Kriterien für das Löschen von Backups verwendet. SnapCenter löscht das älteste Backup unabhängig davon, wenn es auf dem aktuellen primären oder sekundären Host erstellt wurde.



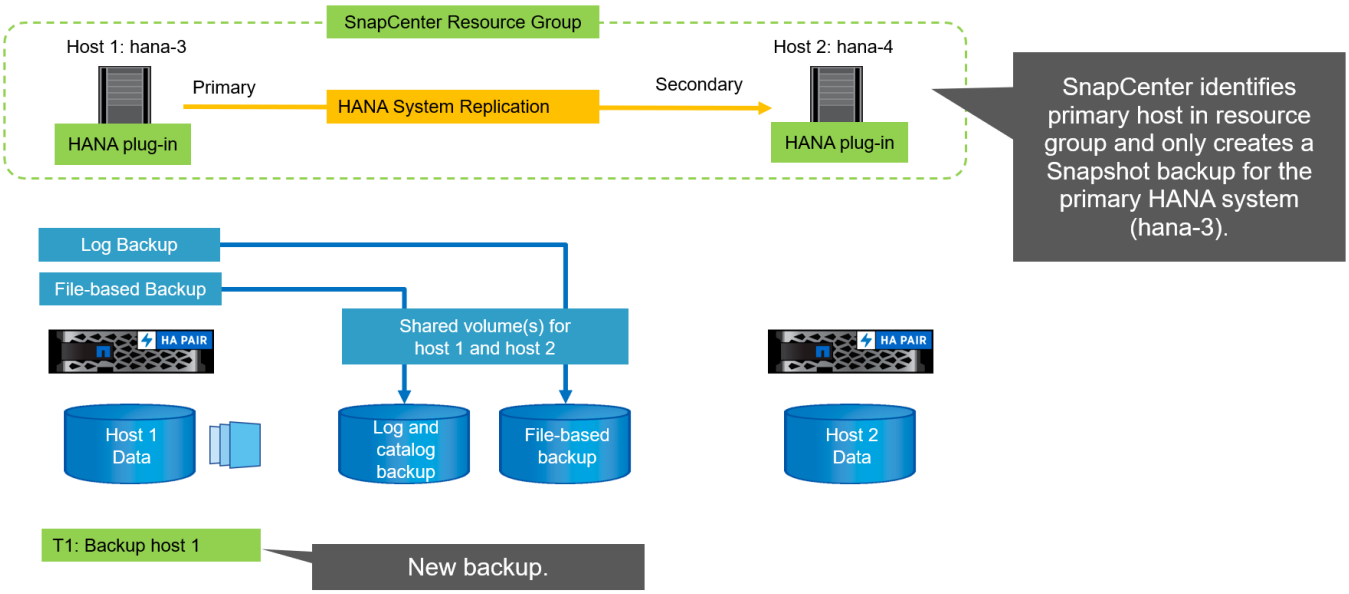
Die Konfiguration der Ressourcengruppe ist jetzt abgeschlossen und Backups können ausgeführt werden.



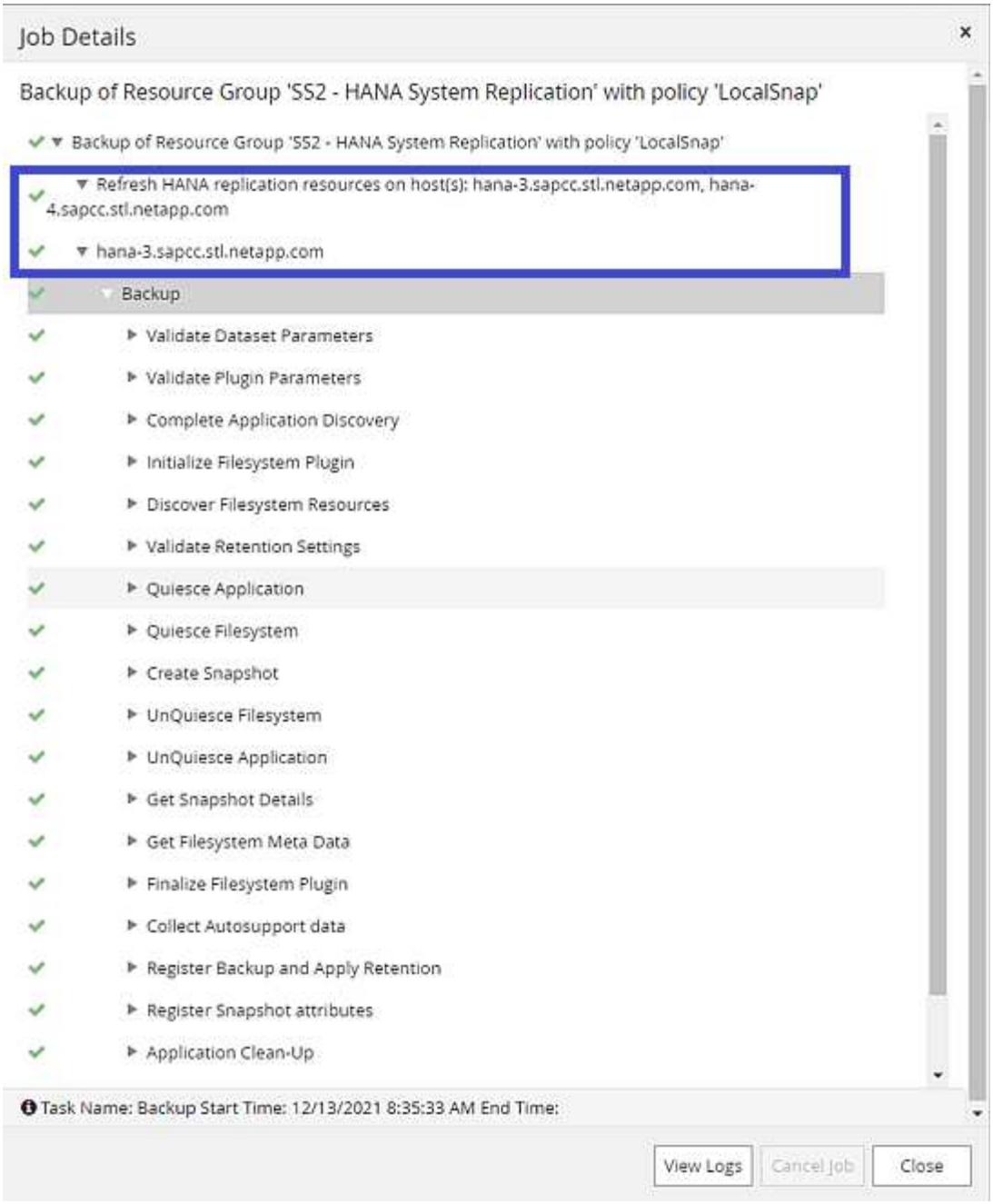


Snapshot-Backup-Vorgänge

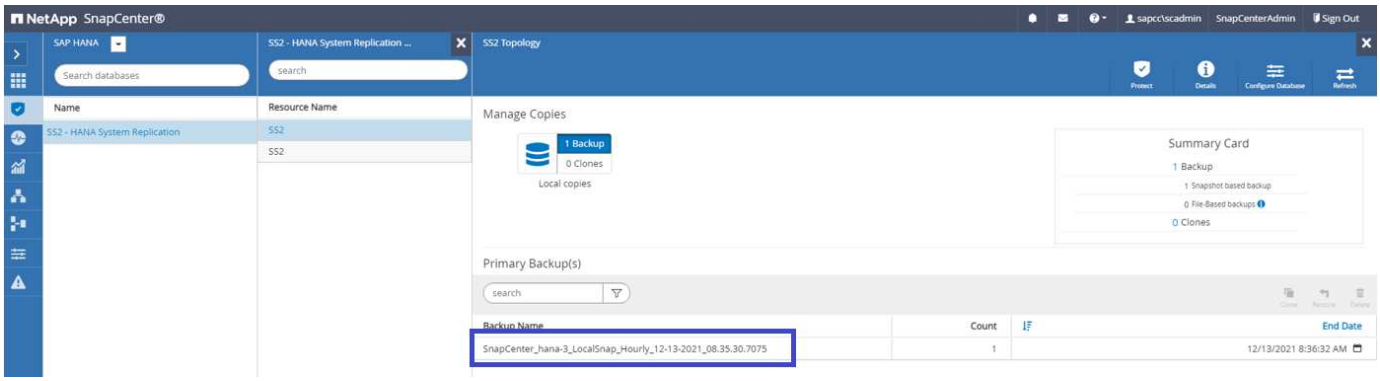
Wenn ein Backup-Vorgang der Ressourcengruppe ausgeführt wird, identifiziert SnapCenter den primären Host und löst nur ein Backup auf dem primären Host aus. Das bedeutet, dass nur das Daten-Volume des primären Hosts mit Snapshots erstellt werden wird. in unserem Beispiel ist hana-3 der aktuelle primäre Host und ein Backup wird auf diesem Host ausgeführt.



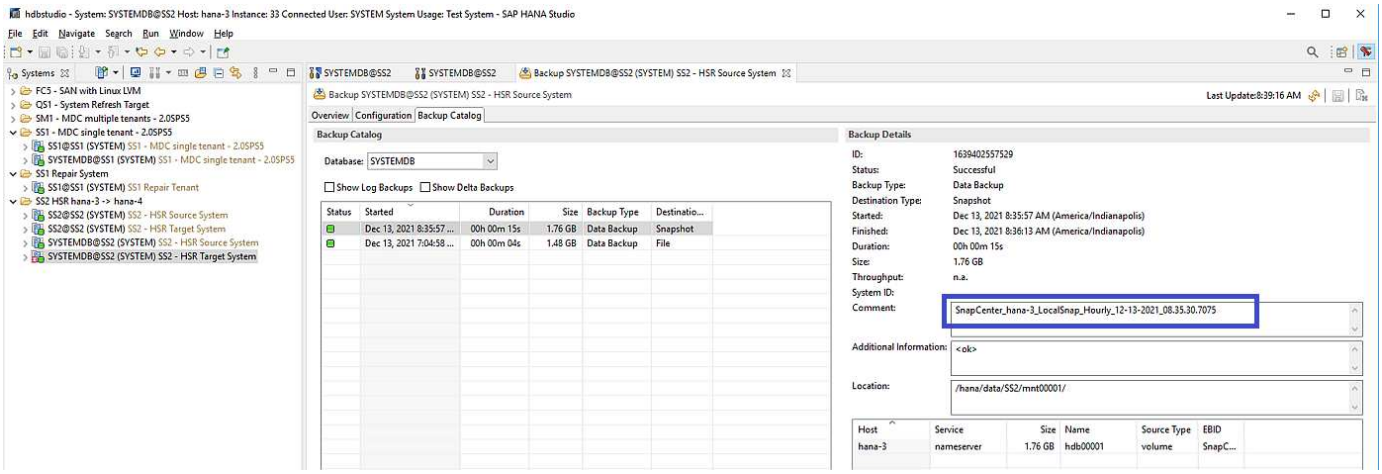
Das SnapCenter-Jobprotokoll zeigt den Identifizierungsvorgang und die Ausführung des Backups auf dem aktuellen primären Host hana-3.



Ein Snapshot-Backup wurde jetzt auf der primären HANA-Ressource erstellt. Der im Backup-Namen enthaltene Hostname zeigt hana-3.

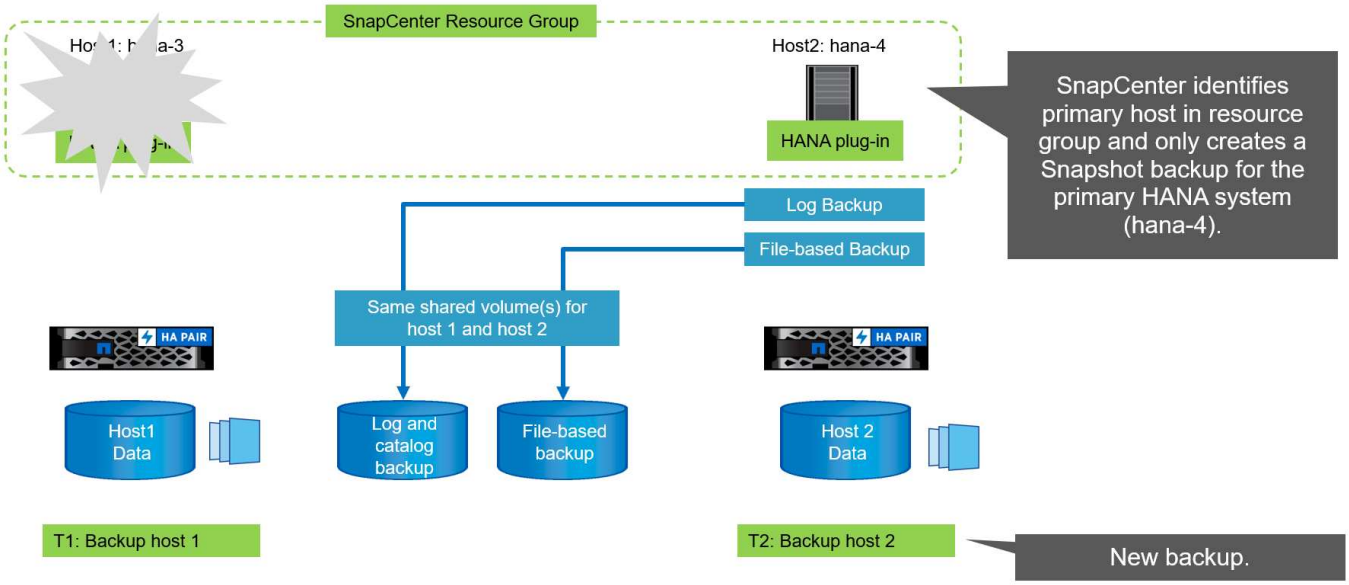


Das Snapshot-Backup ist auch im HANA-Backup-Katalog sichtbar.

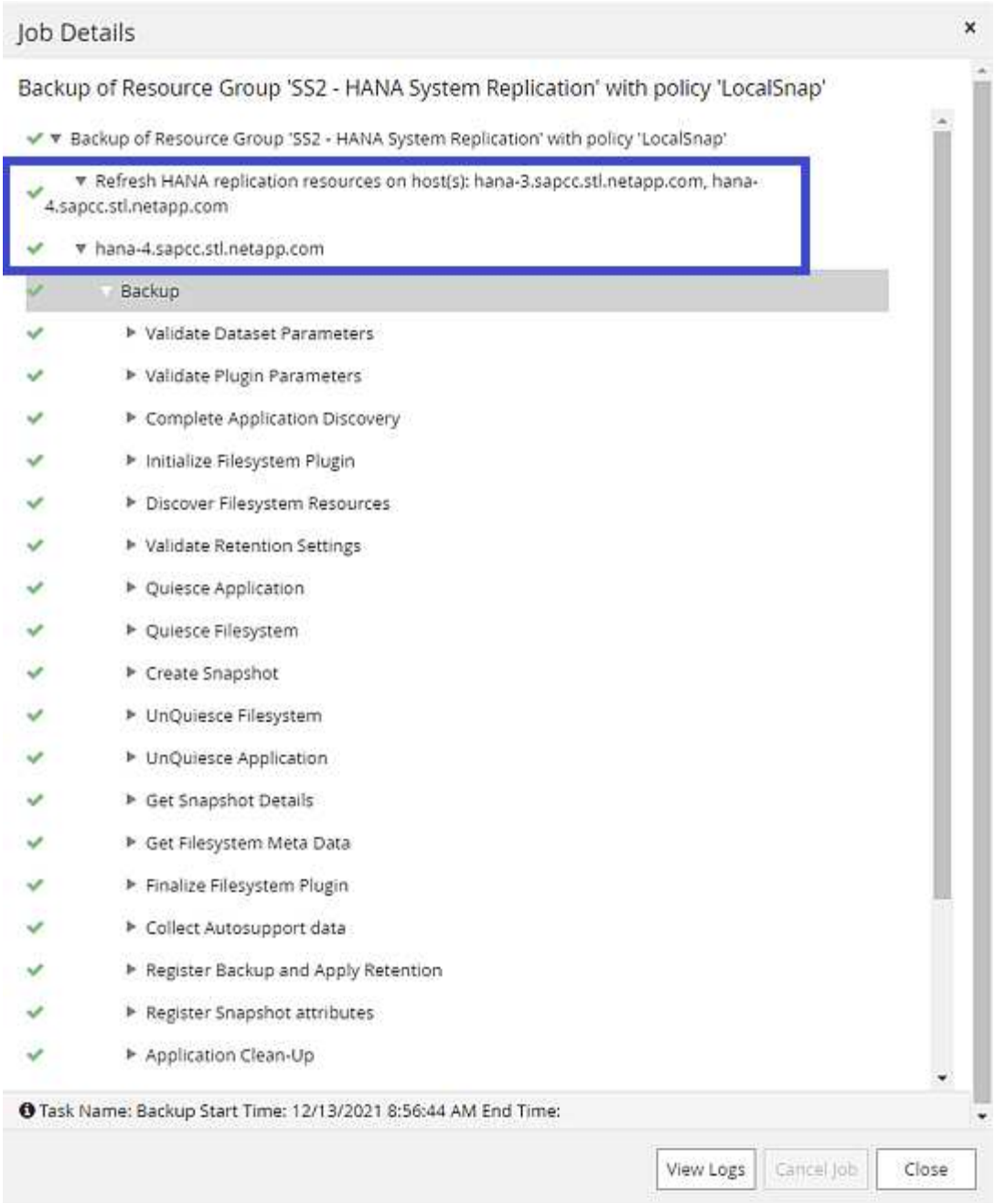


Falls ein Übernahmevorgang ausgeführt wird, identifizieren weitere SnapCenter Backups jetzt den früheren sekundären Host (hana-4) als primär und der Backup-Vorgang wird auf hana-4 ausgeführt. Erneut wird nur das Daten-Volume des neuen primären Hosts (hana-4) mit Snapshots erstellt.

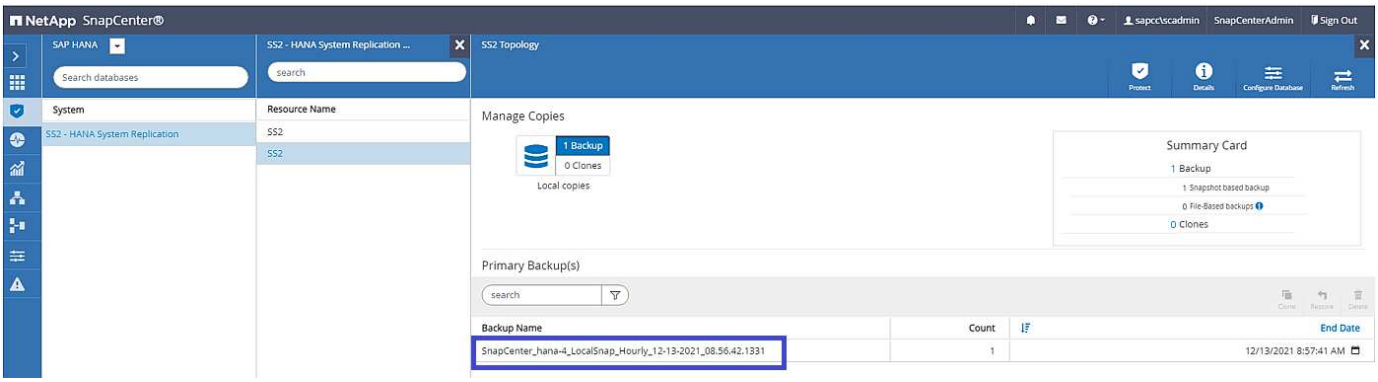
Die SnapCenter-Identifizierungslogik deckt nur Szenarien ab, in denen sich die HANA-Hosts in einer primären/sekundären Beziehung befinden oder wenn einer der HANA-Hosts offline ist.



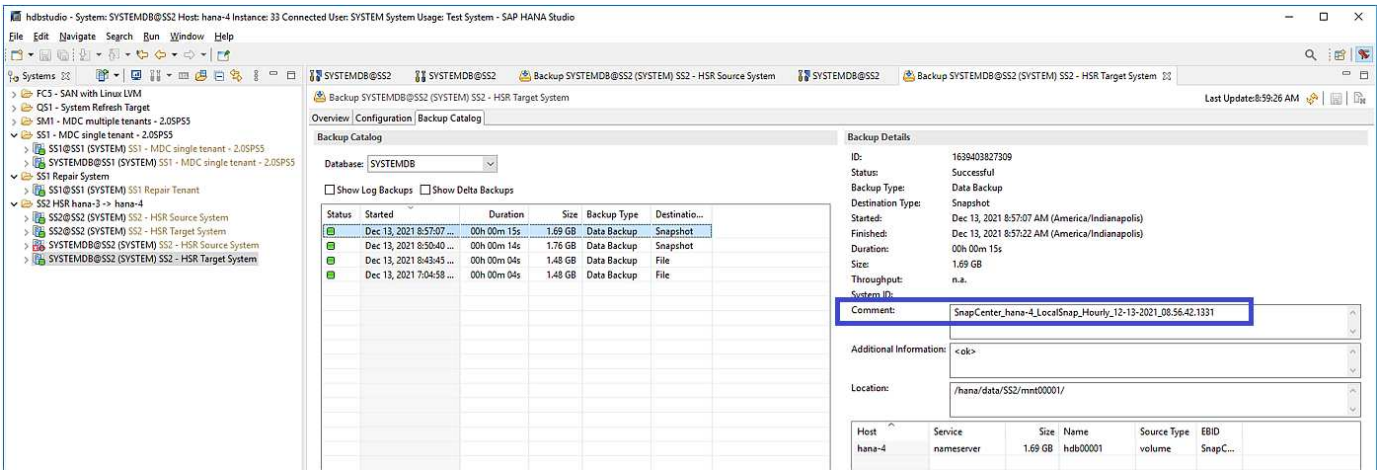
Das SnapCenter-Jobprotokoll zeigt den Identifizierungsvorgang und die Ausführung des Backups auf dem aktuellen primären Host hana-4.



Ein Snapshot-Backup wurde jetzt auf der primären HANA-Ressource erstellt. Der im Backup-Namen enthaltene Hostname zeigt hana-4.



Das Snapshot-Backup ist auch im HANA-Backup-Katalog sichtbar.



Block-Integritätsprüfung mit dateibasierten Backups

SnapCenter 4.6 verwendet dieselbe Logik wie für Snapshot Backup-Vorgänge bei dateibasierten Backups beschrieben zur Überprüfung der Blockintegrität. SnapCenter identifiziert den aktuellen primären HANA-Host und führt das dateibasierte Backup für diesen Host aus. Das Aufbewahrungsmanagement wird auch auf beiden Hosts durchgeführt, sodass das älteste Backup unabhängig davon, welcher Host sich derzeit im primären System befindet, gelöscht wird.

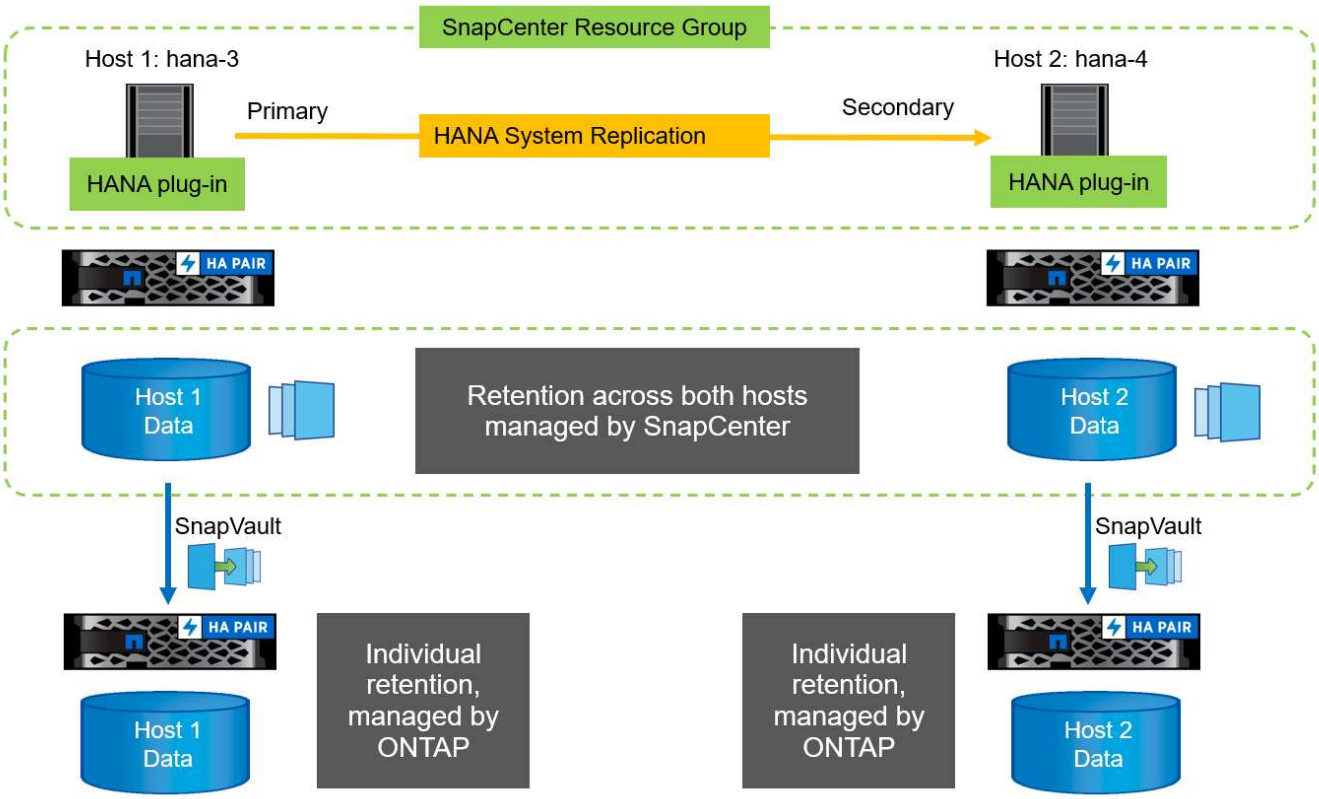
SnapVault Replizierung

Damit transparente Backup-Vorgänge ohne manuelle Interaktion möglich sind, muss im Falle einer Übernahme und unabhängig davon, dass der HANA-Host derzeit der primäre Host ist, eine SnapVault-Beziehung für die Daten-Volumes beider Hosts konfiguriert werden. SnapCenter führt bei jedem Backup-Durchlauf einen SnapVault Update-Vorgang für den aktuellen primären Host durch.

> Wenn ein Takeover an den sekundären Host nicht für lange Zeit ausgeführt wird, ist die Anzahl der geänderten Blöcke für das erste SnapVault Update am sekundären Host hoch.

Da die Retention Management am SnapVault-Ziel außerhalb von SnapCenter durch ONTAP verwaltet wird, kann die Aufbewahrung nicht über beide HANA-Hosts abgewickelt werden. Daher werden Backups, die vor einem Takeover erstellt wurden, nicht mit Backup-Vorgängen auf dem ehemaligen Sekundärstandort gelöscht. Diese Backups bleiben so lange erhalten, bis der frühere primäre wieder auf den primären Speicher zurückgeht. Damit diese Backups das Aufbewahrungsmanagement von Log-Backups nicht blockieren, müssen sie entweder am SnapVault-Ziel oder im HANA-Backup-Katalog manuell gelöscht werden.

> Eine Bereinigung aller SnapVault Snapshot-Kopien ist nicht möglich, da eine Snapshot-Kopie als Synchronisierungspunkt gesperrt wird. Wenn auch die neueste Snapshot Kopie gelöscht werden muss, muss die SnapVault Replizierungsbeziehung gelöscht werden. In diesem Fall empfiehlt NetApp, die Backups im HANA-Backup-Katalog zu löschen, um das Backup-Aufbewahrungsmanagement für das Protokoll abzulösen.



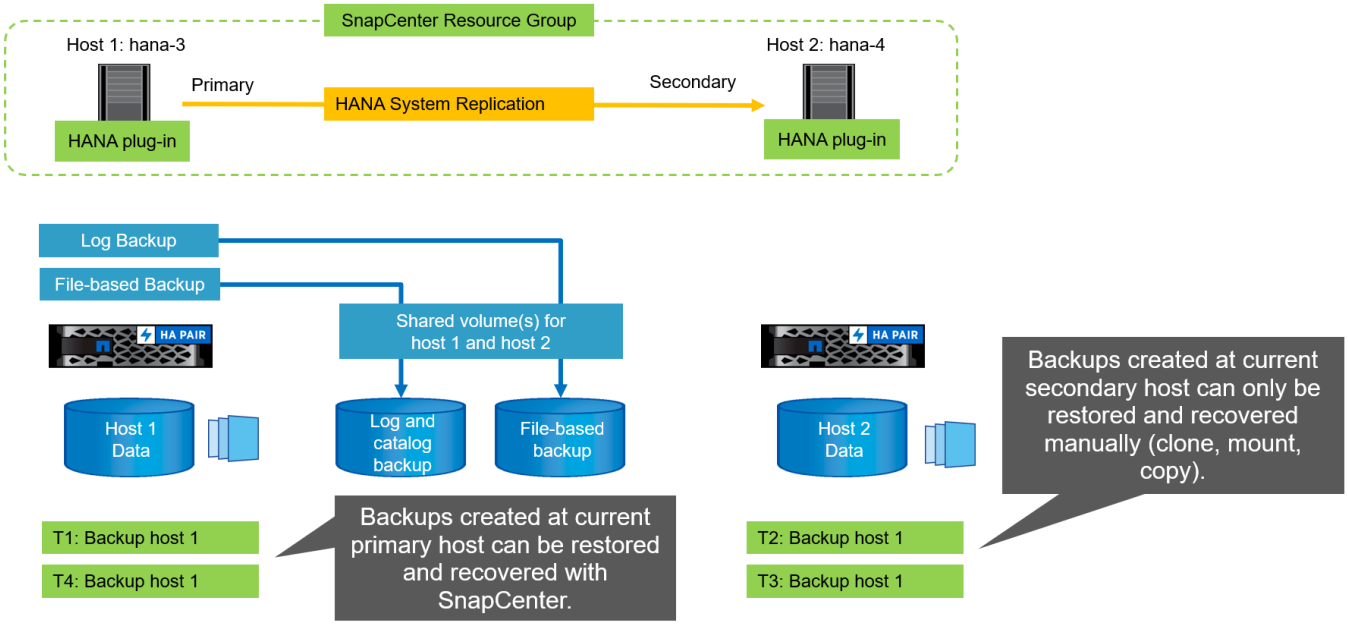
Retentionmanagement

SnapCenter 4.6 verwaltet Aufbewahrung für Snapshot-Backups, Block-Integrität-Check Operationen, HANA Backup-Katalog Einträge, und Log-Backups (wenn nicht deaktiviert) über beide HANA-Hosts, so ist es egal, welcher Host derzeit primär oder sekundär ist. Backups (Daten und Protokoll) und Einträge im HANA-Katalog werden basierend auf der definierten Aufbewahrung gelöscht, unabhängig davon, ob ein Löschvorgang auf dem aktuellen primären oder sekundären Host erforderlich ist. Das bedeutet, dass keine manuelle Interaktion erforderlich ist, wenn ein Übernahmemodus durchgeführt wird und/oder die Replizierung in andere Richtung konfiguriert wird.

Wenn die SnapVault-Replizierung Teil der Datensicherungsstrategie ist, ist für bestimmte Szenarien eine manuelle Interaktion erforderlich, wie in Abschnitt beschrieben "SnapVault-Replizierung"

Restore und Recovery

Die folgende Abbildung zeigt ein Szenario, in dem mehrere Übernahmen ausgeführt und Snapshot Backups an beiden Standorten erstellt wurden. Mit dem aktuellen Status ist der Host hana-3 der primäre Host und das neueste Backup T4, das auf Host hana-3 erstellt wurde. Wenn Sie einen Restore- und Recovery-Vorgang durchführen müssen, sind die Backups T1 und T4 für die Wiederherstellung im SnapCenter verfügbar. Die Backups, die auf dem Host hana-4 (T2, T3) erstellt wurden, können mit SnapCenter nicht wiederhergestellt werden. Diese Backups müssen zur Wiederherstellung manuell auf das Datenvolumen von hana-3 kopiert werden.



Die Wiederherstellungs- und Instandsetzungsvorgänge für eine SnapCenter 4.6-Ressourcengruppenkonfiguration sind identisch mit denen einer automatisch erkannten Konfiguration ohne Systemreplikation. Alle Optionen zur Wiederherstellung und automatisierten Datenrettung stehen zur Verfügung. Weitere Einzelheiten finden Sie im technischen Bericht. "Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter"Die

Ein Wiederherstellungsvorgang aus einem Backup, das auf dem anderen Host erstellt wurde, wird im Abschnitt beschrieben"Wiederherstellung aus einem Backup, das auf dem anderen Host erstellt wurde".

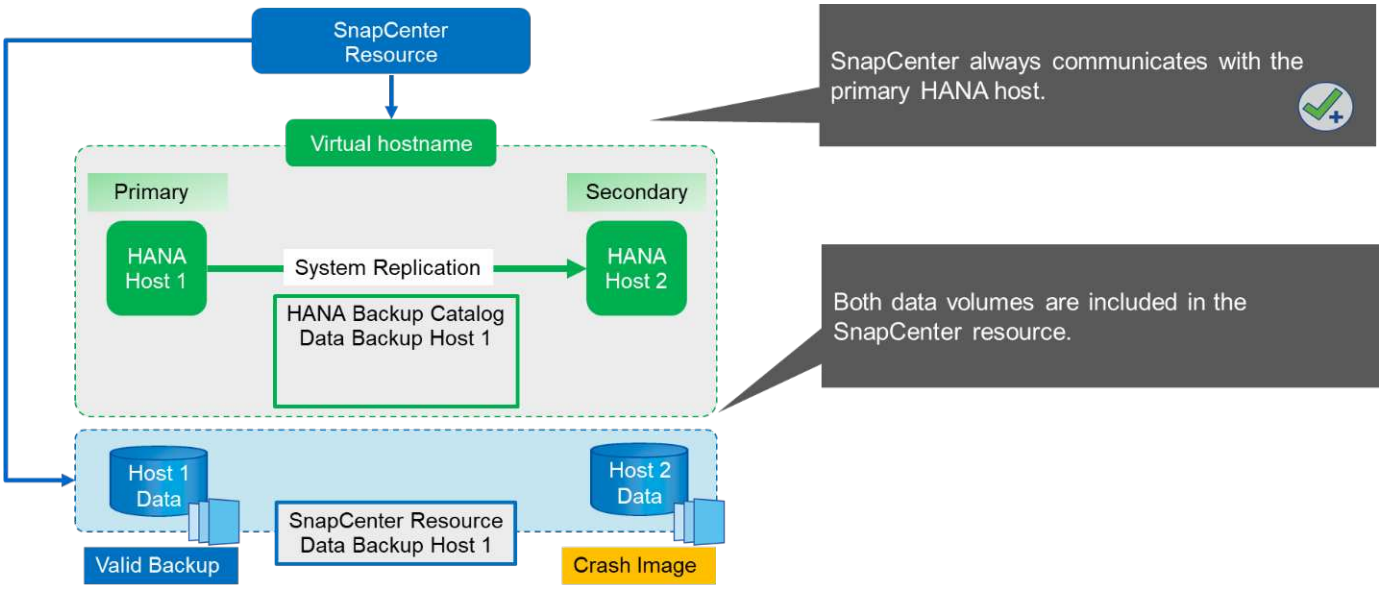
SnapCenter Konfiguration mit einer einzigen Ressource

Eine SnapCenter-Ressource wird mit der virtuellen IP-Adresse (Hostname) der HANA System Replication-Umgebung konfiguriert. Bei diesem Ansatz kommuniziert SnapCenter immer mit dem primären Host, unabhängig davon, ob Host 1 oder Host 2 der primäre Host ist. Die Datenvolumen beider SAP HANA-Hosts sind in der SnapCenter Ressource enthalten.

Wir gehen davon aus, dass die virtuelle IP-Adresse immer an den primären SAP HANA-Host gebunden ist. Das Failover der virtuellen IP-Adresse erfolgt außerhalb von SnapCenter im Rahmen des Failover-Workflows zur HANA-Systemreplizierung.

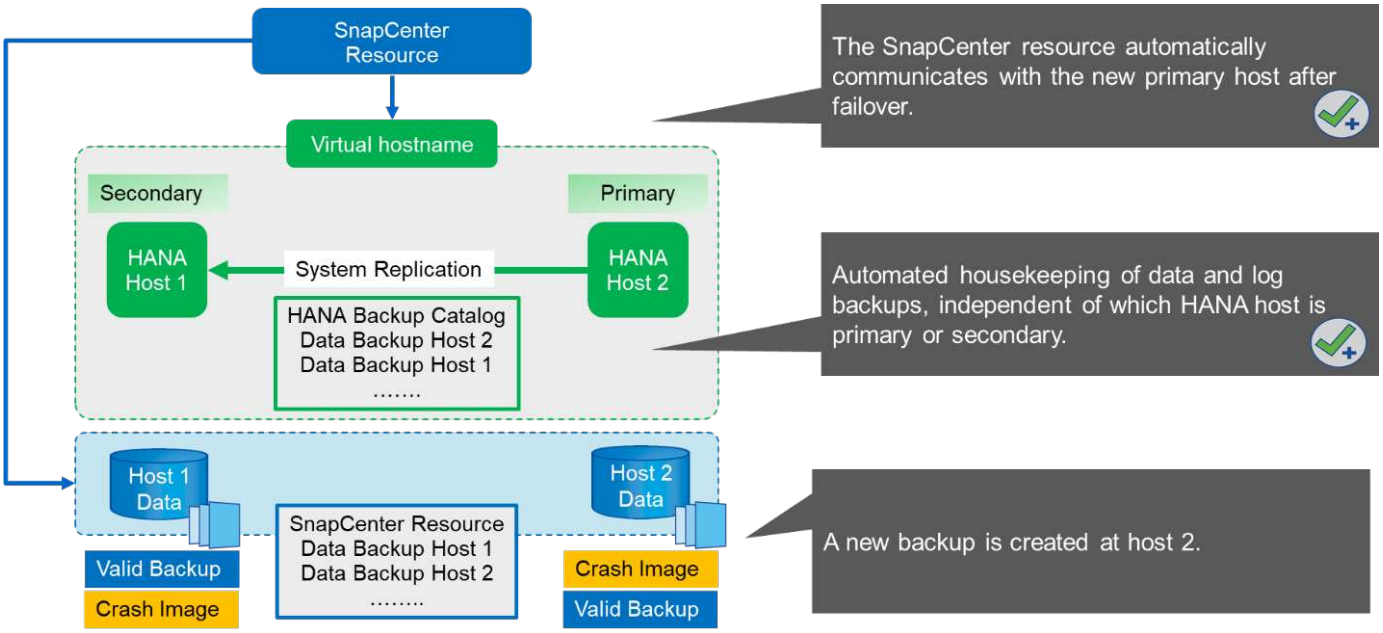
Wird ein Backup mit Host 1 als primärer Host ausgeführt, wird ein datenbankkonsistentes Snapshot-Backup auf dem Datenvolumen von Host 1 erstellt. Da das Daten-Volume des Hosts 2 Teil der SnapCenter Ressource ist, wird für dieses Volume eine weitere Snapshot Kopie erstellt. Diese Snapshot Kopie ist nicht datenbankkonsistent, sondern nur ein Crash-Image des sekundären Hosts.

Der SAP HANA Backup-Katalog und die SnapCenter-Ressource umfassen das auf Host 1 erstellte Backup.



Die folgende Abbildung zeigt den Backup-Vorgang nach dem Failover auf Host 2 und die Replizierung von Host 2 zu Host 1. SnapCenter kommuniziert automatisch mit Host 2, indem die in der SnapCenter-Ressource konfigurierte virtuelle IP-Adresse verwendet wird. Backups werden jetzt auf Host 2 erstellt. Von SnapCenter werden zwei Snapshot-Kopien erstellt: Ein datenbankkonsistentes Backup auf dem Daten-Volume bei Host 2 und eine Snapshot-Kopie des Crash-Images am Daten-Volume beim Host 1. Der SAP HANA-Backup-Katalog und die SnapCenter-Ressource enthalten nun das bei Host 1 erstellte Backup und das auf Host 2 erstellte Backup.

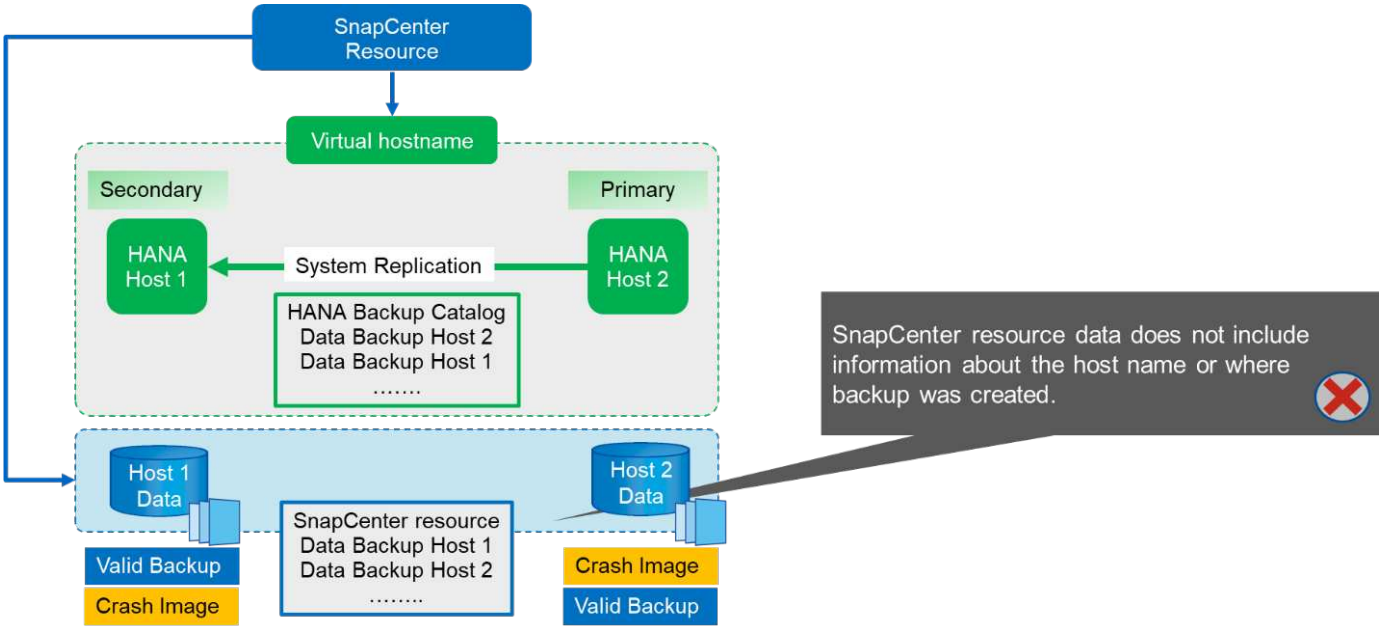
Die allgemeine Ordnung und Sauberkeit der Daten- und Log-Backups basiert auf der definierten SnapCenter-Aufbewahrungsrichtlinie und die Backups werden unabhängig vom primären oder sekundären Host gelöscht.



Wie im Abschnitt erläutert"Storage Snapshot Backups und SAP System Replication", unterscheidet sich ein Restore-Vorgang mit Storage-basierten Snapshot Backups, je nachdem, welches Backup wiederhergestellt werden muss. Es ist wichtig zu ermitteln, auf welchem Host das Backup erstellt wurde, um festzustellen, ob die Wiederherstellung auf dem lokalen Speichervolumen durchgeführt werden kann, oder ob die Wiederherstellung auf dem Speichervolumen des anderen Hosts durchgeführt werden muss.

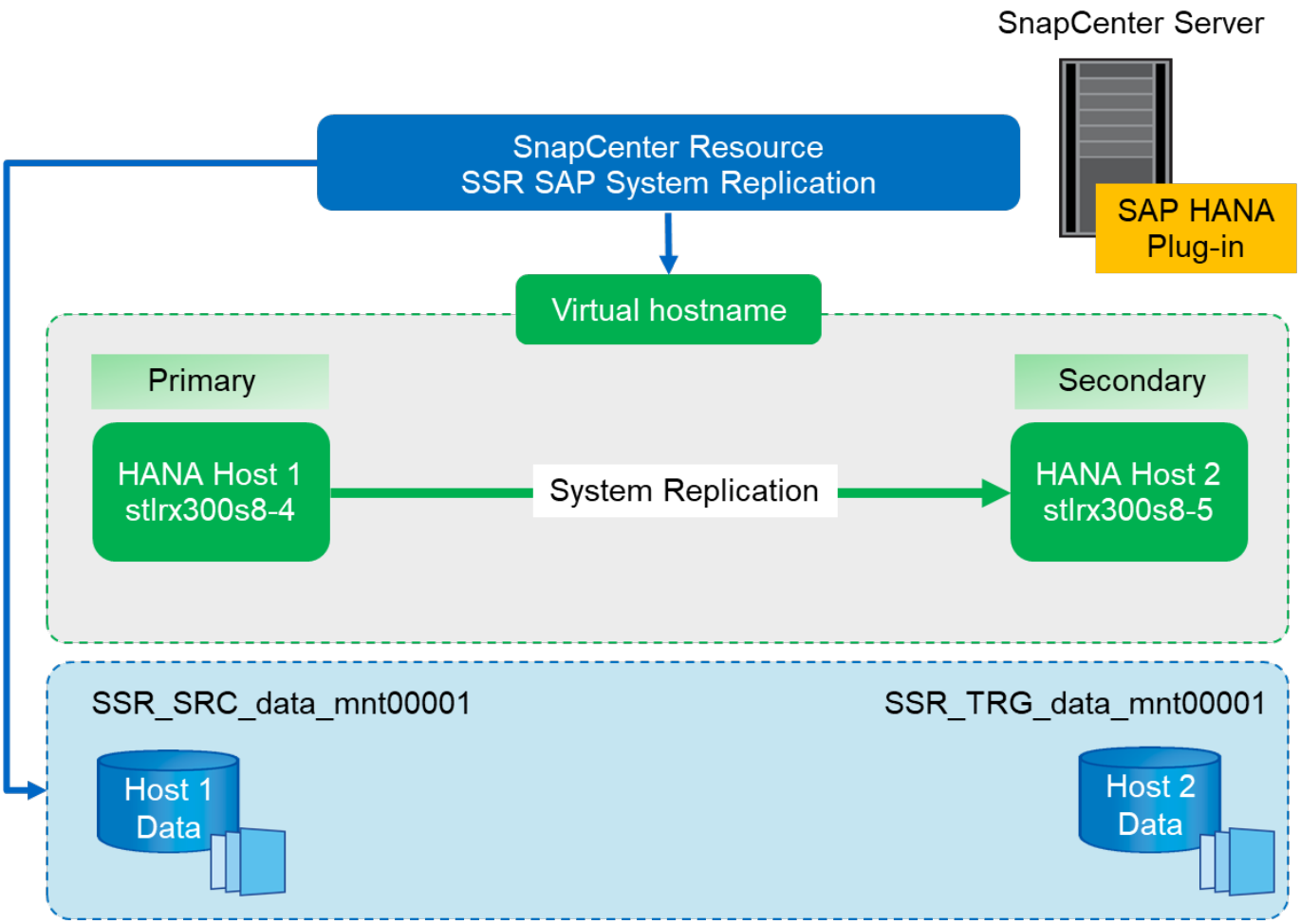
Bei einer SnapCenter-Konfiguration mit nur einem Mitarbeiter ist SnapCenter nicht bewusst, wo das Backup erstellt wurde. NetApp empfiehlt daher, dem SnapCenter Backup-Workflow ein Pre-Backup-Skript hinzuzufügen, um zu ermitteln, welcher Host derzeit der primäre SAP HANA-Host ist.

Die folgende Abbildung zeigt die Identifikation des Backup-Hosts.



SnapCenter-Konfiguration

Die folgende Abbildung zeigt das Lab-Setup und eine Übersicht über die erforderliche SnapCenter-Konfiguration.



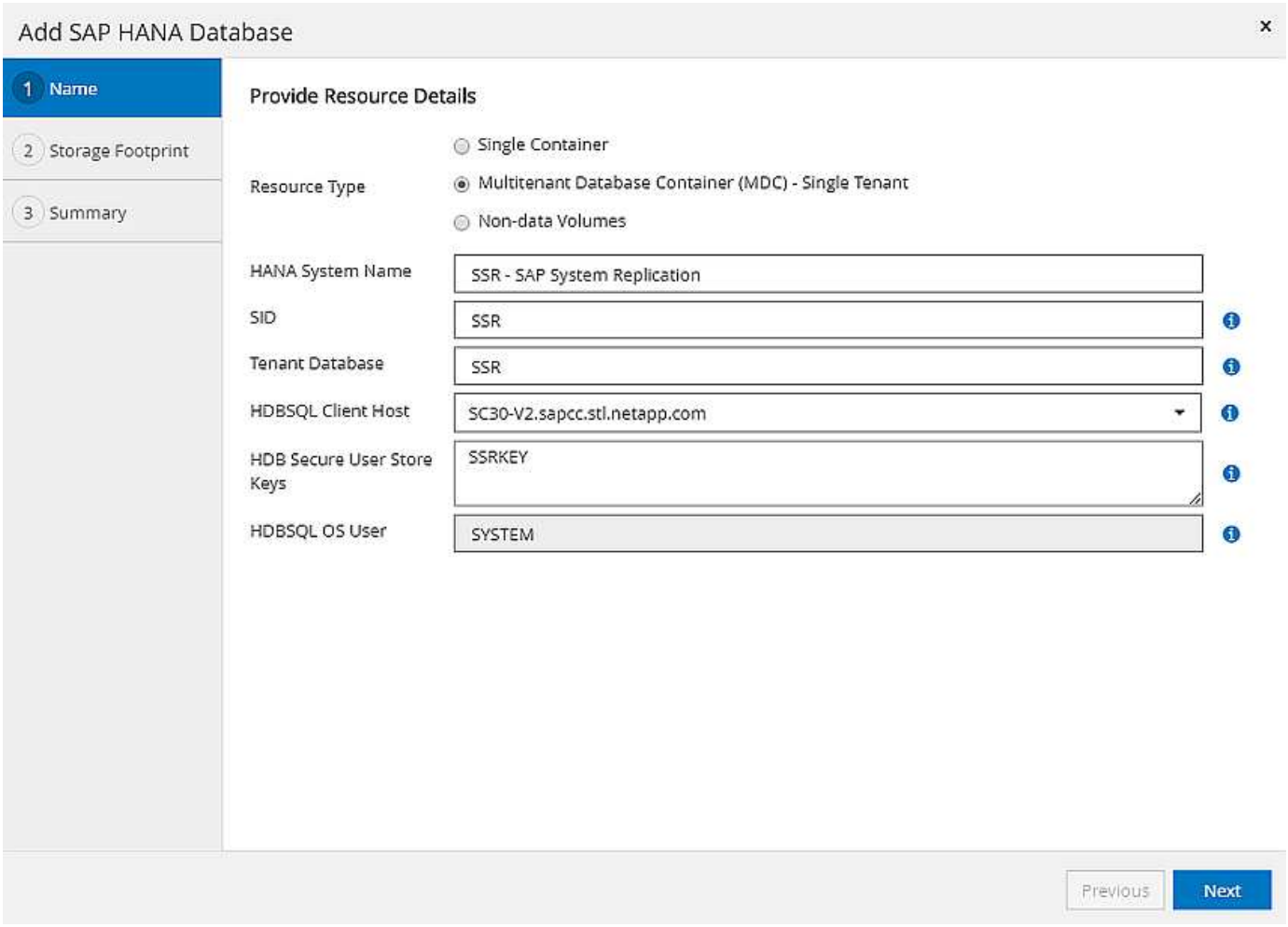
Um Backup-Vorgänge unabhängig davon durchzuführen, welcher SAP HANA Host primär ist und selbst wenn ein Host ausfällt, muss das SnapCenter SAP HANA Plug-in auf einem zentralen Plug-in-Host implementiert werden. In unserer Lab-Einrichtung wurde der SnapCenter Server als zentraler Plug-in-Host verwendet, und wir haben das SAP HANA Plug-in auf dem SnapCenter Server implementiert.

In der HANA-Datenbank wurde ein Benutzer erstellt, um Backup-Vorgänge durchzuführen. Auf dem SnapCenter-Server, auf dem das SAP HANA-Plug-in installiert wurde, wurde ein User-Store-Schlüssel konfiguriert. Der Benutzerspeicherschlüssel enthält die virtuelle IP-Adresse der SAP HANA System Replication Hosts (`ssr-vip`).

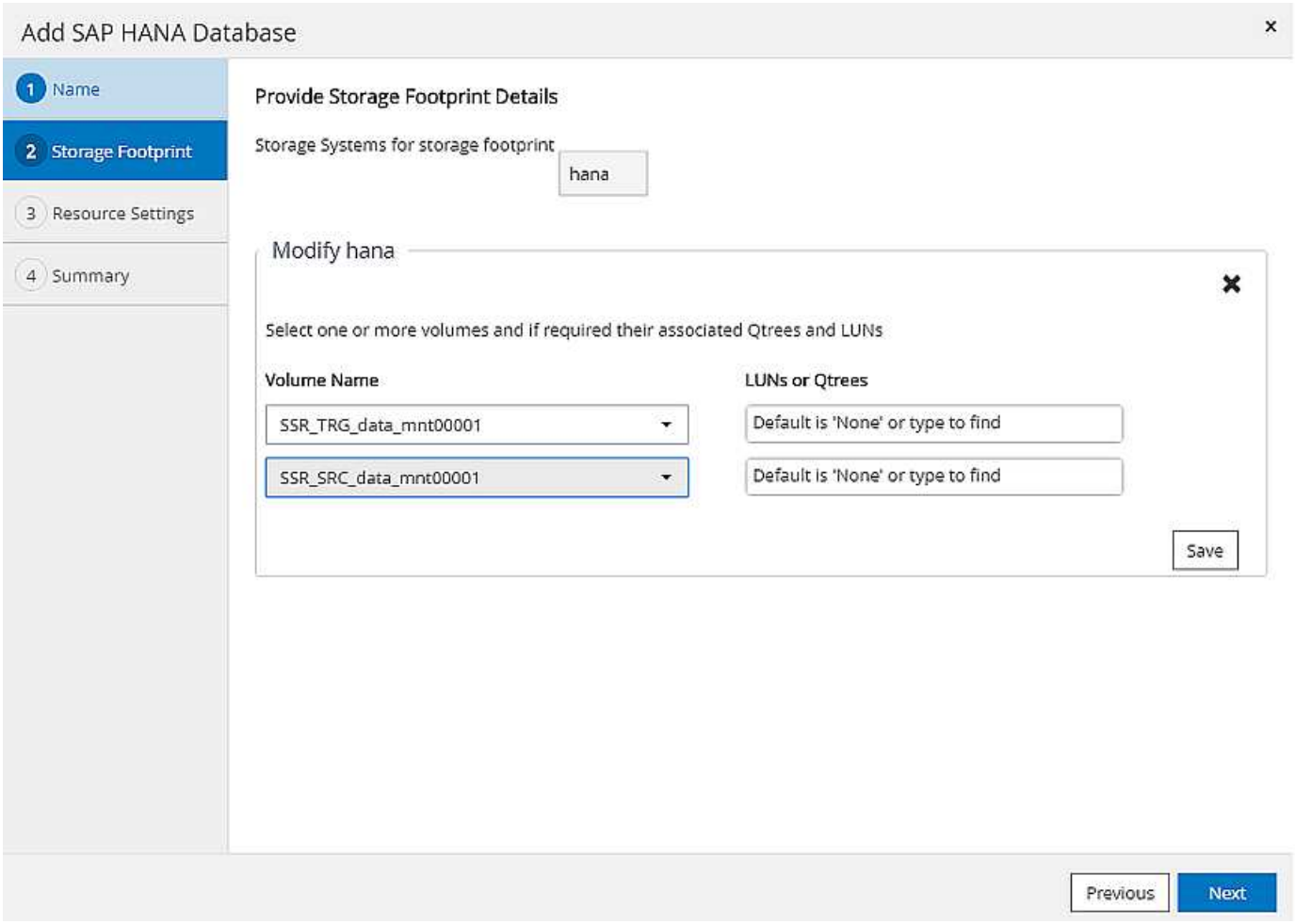
```
hdbuserstore.exe -u SYSTEM set SSRKEY ssr-vip:31013 SNAPCENTER <password>
```

Weitere Informationen zu den Bereitstellungsoptionen für SAP HANA-Plug-ins und zur Konfiguration des Benutzerspeichers finden Sie im technischen Bericht TR-4614: "Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter"Die

In SnapCenter wird die Ressource wie in der folgenden Abbildung dargestellt mit dem Benutzer-Speicherschlüssel konfiguriert, vorher konfiguriert, und dem SnapCenter-Server als der konfiguriert `hdbsql` Kommunikations-Host.

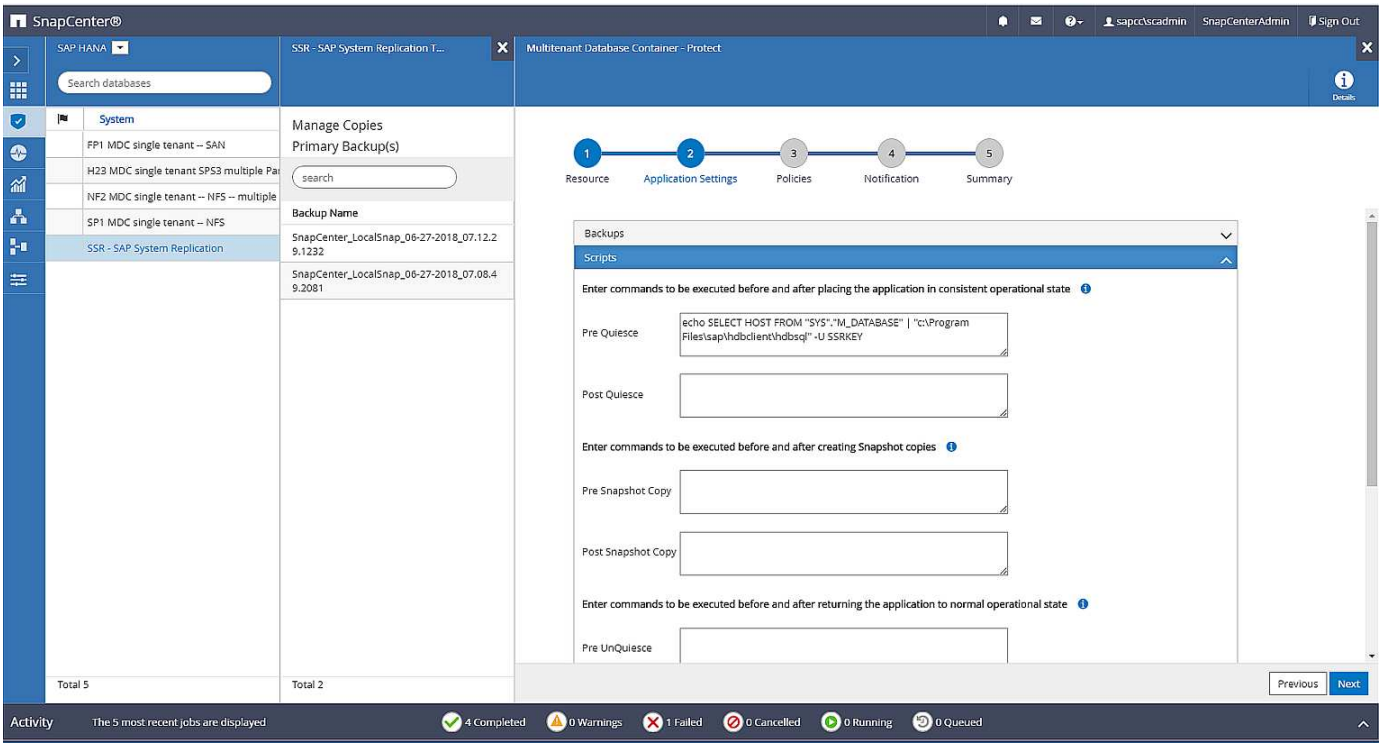


Die Datenvolumen der beiden SAP HANA-Hosts sind in der Storage-Platzbedarf-Konfiguration enthalten, wie die folgende Abbildung zeigt.



Wie zuvor bereits besprochen, ist bei SnapCenter nicht bekannt, wo das Backup erstellt wurde. NetApp empfiehlt daher, ein Skript vor dem Backup im SnapCenter Backup Workflow hinzuzufügen, um zu ermitteln, welcher Host derzeit der primäre SAP HANA Host ist. Sie können diese Identifizierung mithilfe einer SQL-Anweisung durchführen, die dem Backup-Workflow hinzugefügt wird, wie die folgende Abbildung zeigt.

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

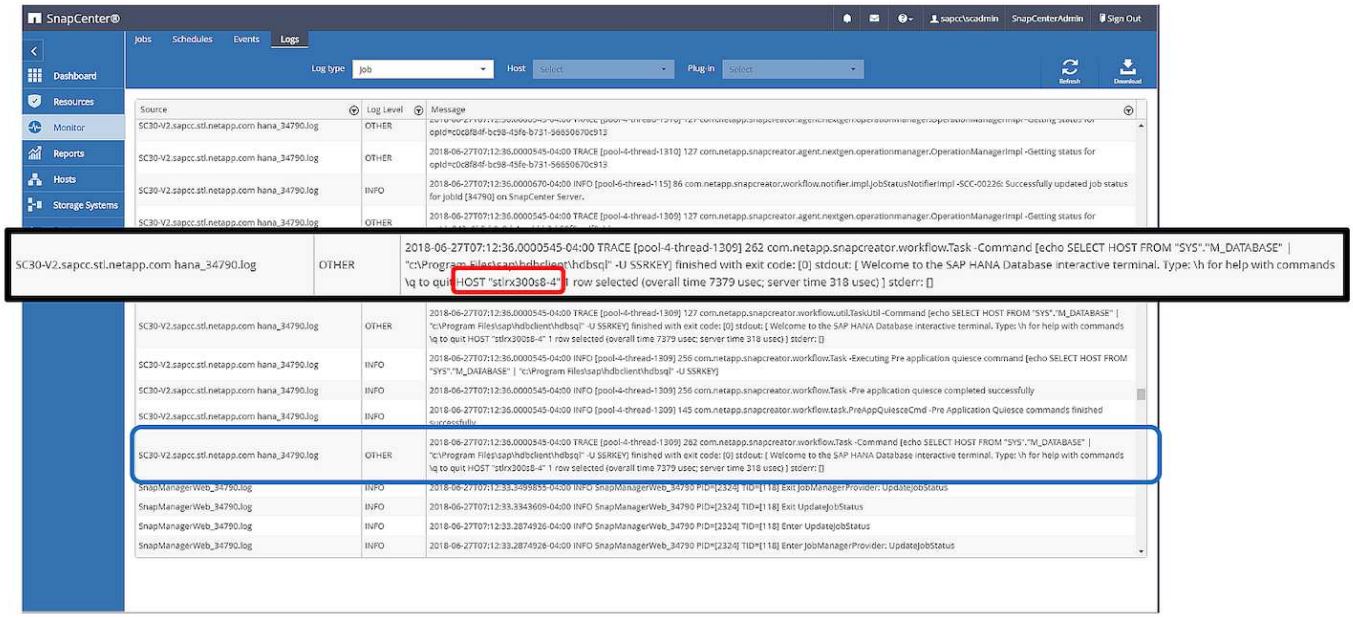


SnapCenter Backup-Vorgang

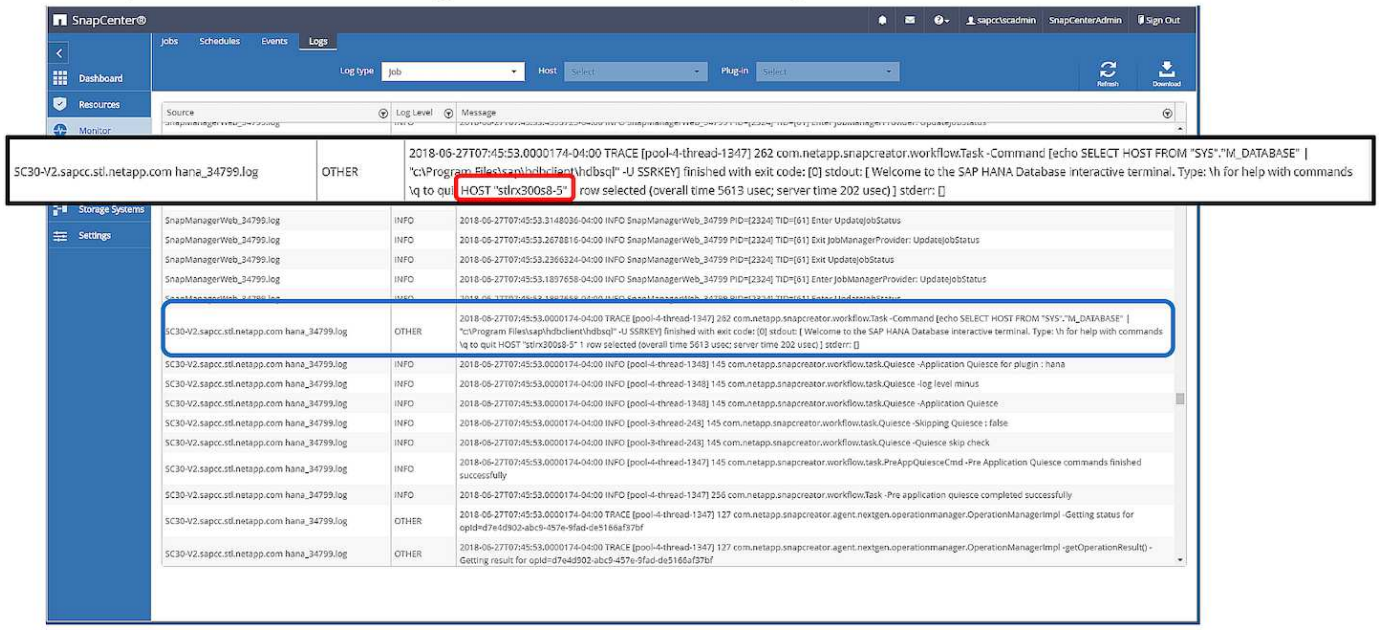
Backup-Vorgänge werden jetzt wie gewohnt ausgeführt. Die allgemeine Ordnung und Sauberkeit der Daten und Log-Backups wird unabhängig davon durchgeführt, welcher SAP HANA-Host primärer oder sekundärer ist.

Die Backup-Jobprotokolle enthalten die Ausgabe der SQL-Anweisung, mit der Sie den SAP HANA-Host identifizieren können, auf dem das Backup erstellt wurde.

Die folgende Abbildung zeigt das Backup-Jobprotokoll mit Host 1 als primärer Host.

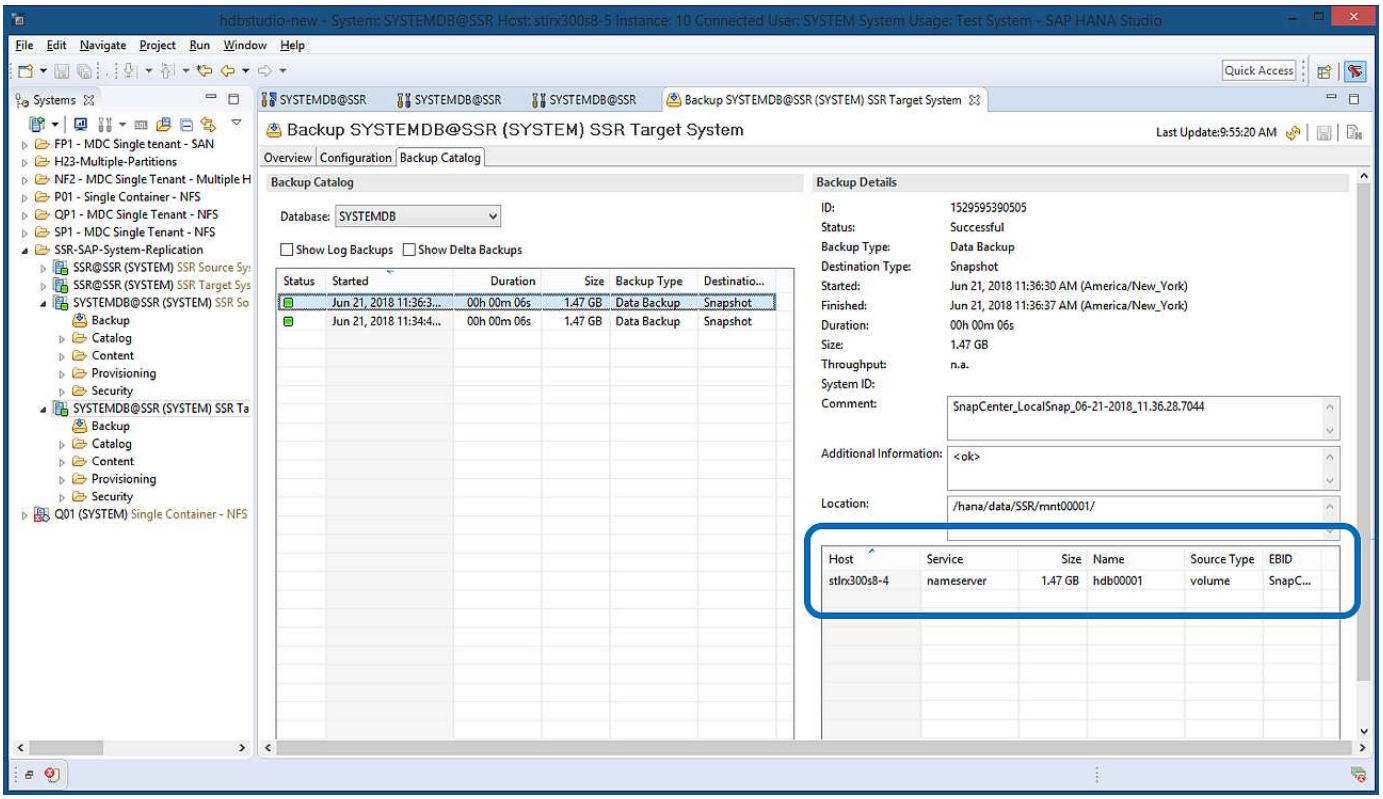


Diese Abbildung zeigt das Backup-Jobprotokoll mit Host 2 als primärer Host.



Die folgende Abbildung zeigt den SAP HANA Backup-Katalog in SAP HANA Studio. Ist die SAP HANA-Datenbank online, ist der SAP HANA-Host, auf dem das Backup erstellt wurde, im SAP HANA Studio sichtbar.

Der SAP HANA-Backup-Katalog auf dem Filesystem, der während eines Restore- und Recovery-Vorgangs verwendet wird, enthält nicht den Host-Namen, in dem das Backup erstellt wurde. Der einzige Weg, um den Host zu identifizieren, wenn die Datenbank ausfällt, ist die Kombination der Backup-Katalog-Einträge mit dem `backup.log` Datei beider SAP HANA-Hosts.



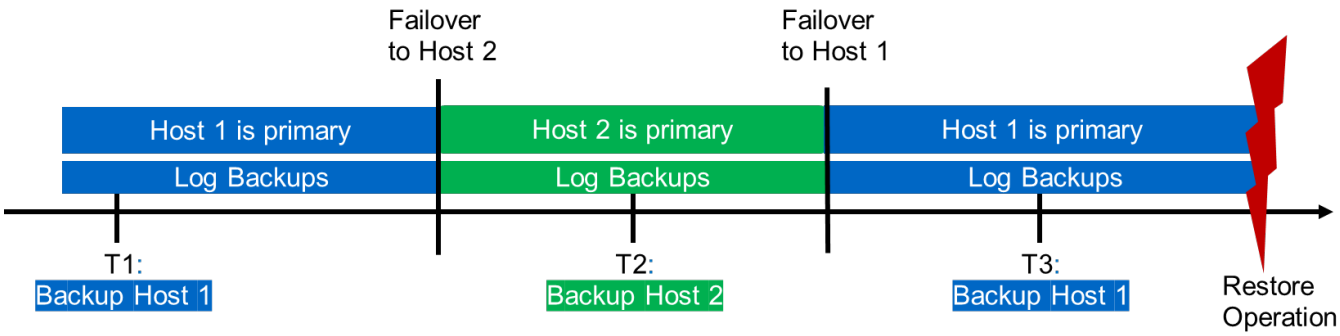
Restore und Recovery

Wie bereits besprochen, müssen Sie feststellen können, wo das ausgewählte Backup erstellt wurde, um den erforderlichen Wiederherstellungsvorgang zu definieren. Wenn die SAP HANA Datenbank noch online ist, kann mit SAP HANA Studio der Host identifiziert werden, auf dem das Backup erstellt wurde. Wenn die Datenbank offline ist, sind die Informationen nur im SnapCenter-Backup-Jobprotokoll verfügbar.

Die folgende Abbildung zeigt die verschiedenen Wiederherstellungsvorgänge je nach ausgewähltem Backup.

Wenn ein Wiederherstellungsvorgang nach dem Zeitstempel T3 ausgeführt werden muss und Host 1 der primäre ist, können Sie das bei T1 oder T3 erstellte Backup mithilfe von SnapCenter wiederherstellen. Diese Snapshot-Backups sind auf dem an Host 1 angebundenen Storage Volume verfügbar.

Wenn Sie mithilfe des Backup wiederherstellen müssen, der am Host 2 (T2) erstellt wurde, eine Snapshot-Kopie im Storage Volume von Host 2 ist, muss der Backup für den Host 1 zur Verfügung gestellt werden. Sie können dieses Backup zur Verfügung stellen, indem Sie eine NetApp FlexClone Kopie aus dem Backup erstellen, die FlexClone Kopie in Host 1 mounten und die Daten am ursprünglichen Speicherort kopieren.



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

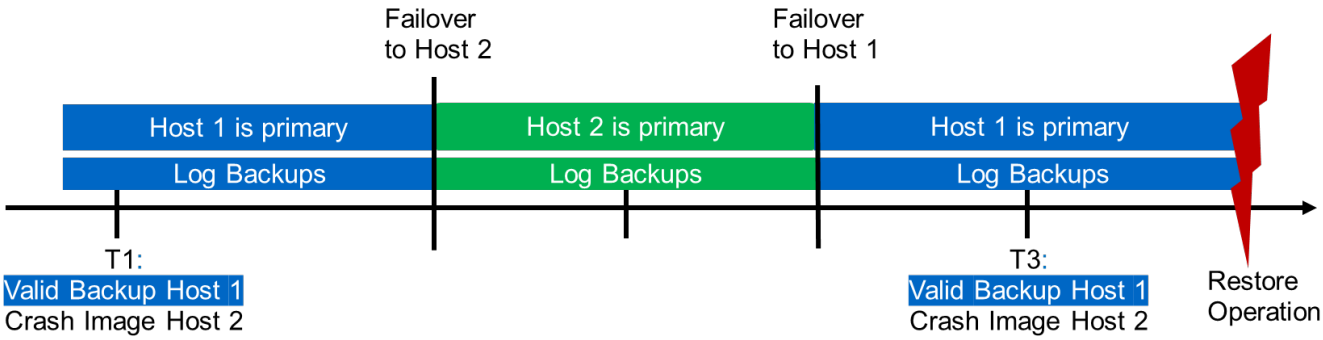
Mit einer einzelnen SnapCenter Ressourcenkonfiguration werden Snapshot Kopien auf beiden Storage-Volumes sowohl von SAP HANA System Replication Hosts erstellt. Nur das Snapshot-Backup, das auf dem Storage-Volume des primären SAP HANA-Hosts erstellt wird, ist für die zukünftige Recovery gültig. Die auf dem Storage Volume des sekundären SAP HANA-Hosts erstellte Snapshot Kopie ist ein Crash-Image, das nicht für die zukünftige Recovery verwendet werden kann.

Eine Wiederherstellung mit SnapCenter kann auf zwei verschiedene Arten durchgeführt werden:

- Stellen Sie nur das gültige Backup wieder her
- Stellen Sie die komplette Ressource einschließlich des gültigen Backups und des Crash-imageIn den folgenden Abschnitten werden die beiden verschiedenen Wiederherstellungsvorgänge näher erläutert.

Ein Wiederherstellungsvorgang aus einem Backup, das auf dem anderen Host erstellt wurde, wird im Abschnitt beschrieben"Wiederherstellung aus einem Backup, das auf dem anderen Host erstellt wurde".

Die folgende Abbildung zeigt die Wiederherstellungen mit einer einzelnen SnapCenter Ressourcenkonfiguration.

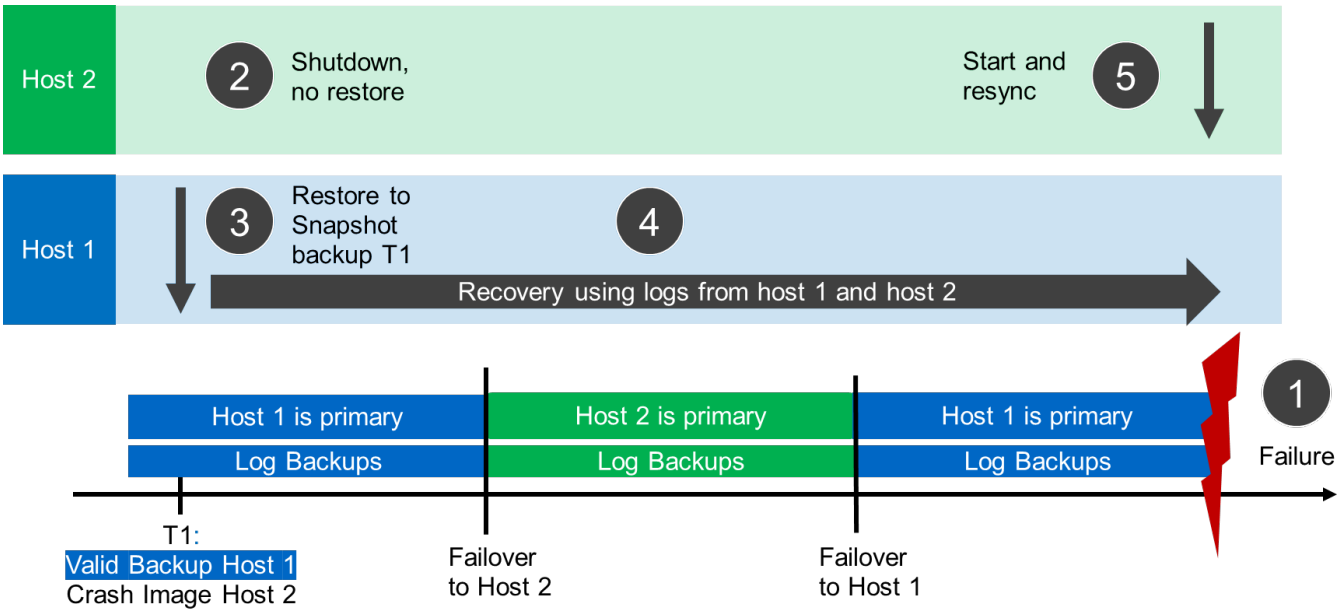


SnapCenter Restore nur für gültige Backups

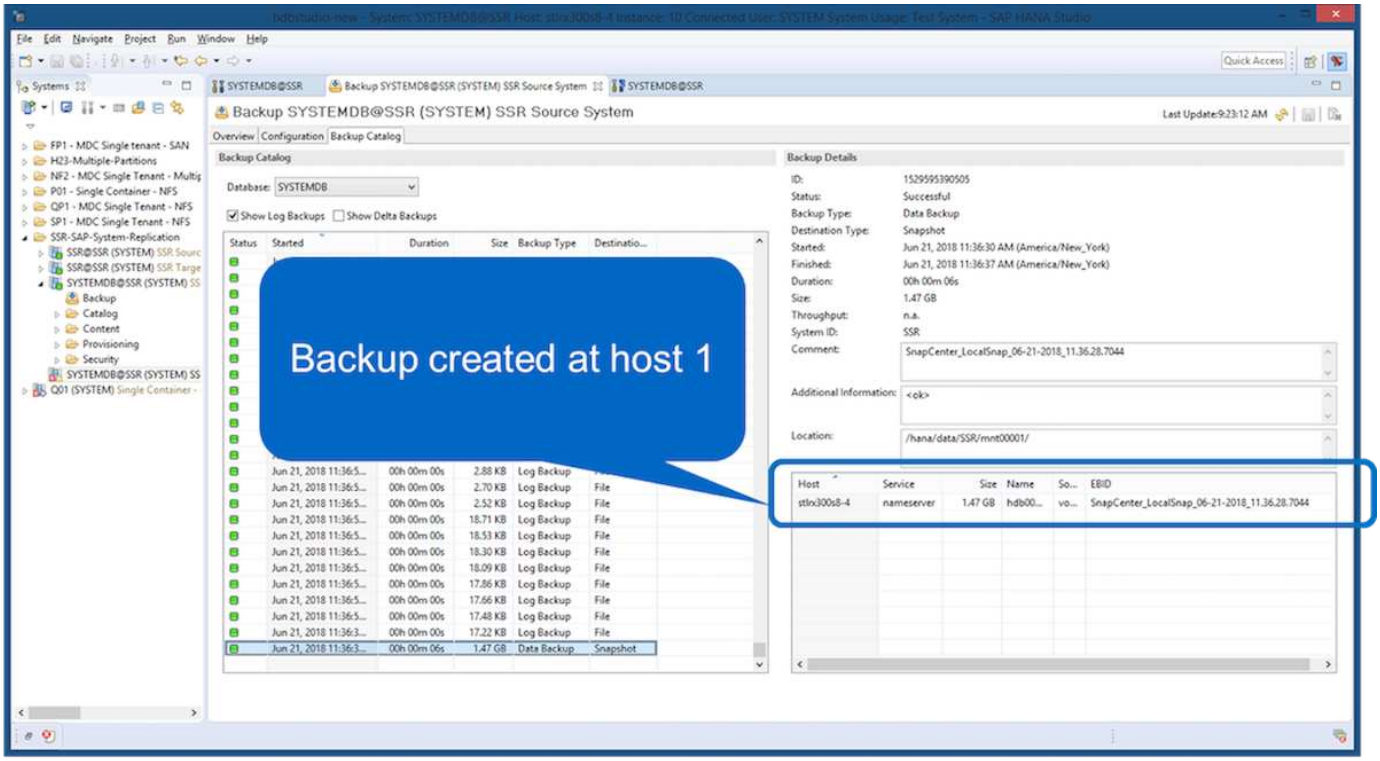
Die folgende Abbildung zeigt einen Überblick über das in diesem Abschnitt beschriebene Wiederherstellungsszenario.

Bei T1 am Host 1 wurde ein Backup erstellt. Ein Failover wurde an Host 2 durchgeführt. Nach einem bestimmten Zeitpunkt wurde ein weiteres Failover zurück zu Host 1 durchgeführt. Zum aktuellen Zeitpunkt ist Host 1 der primäre Host.

1. Es ist ein Fehler aufgetreten, und Sie müssen das am T1 erstellte Backup am Host 1 wiederherstellen.
2. Der sekundäre Host (Host 2) wird heruntergefahren, aber es wird kein Wiederherstellungsvorgang ausgeführt.
3. Das Speichervolumen von Host 1 wird auf dem bei T1 erstellten Backup wiederhergestellt.
4. Eine vorwärts gerichteten Wiederherstellung wird mit Protokollen von Host 1 und Host 2 durchgeführt.
5. Host 2 wird gestartet, und die Neusynchronisierung der Systemreplizierung von Host 2 wird automatisch gestartet.



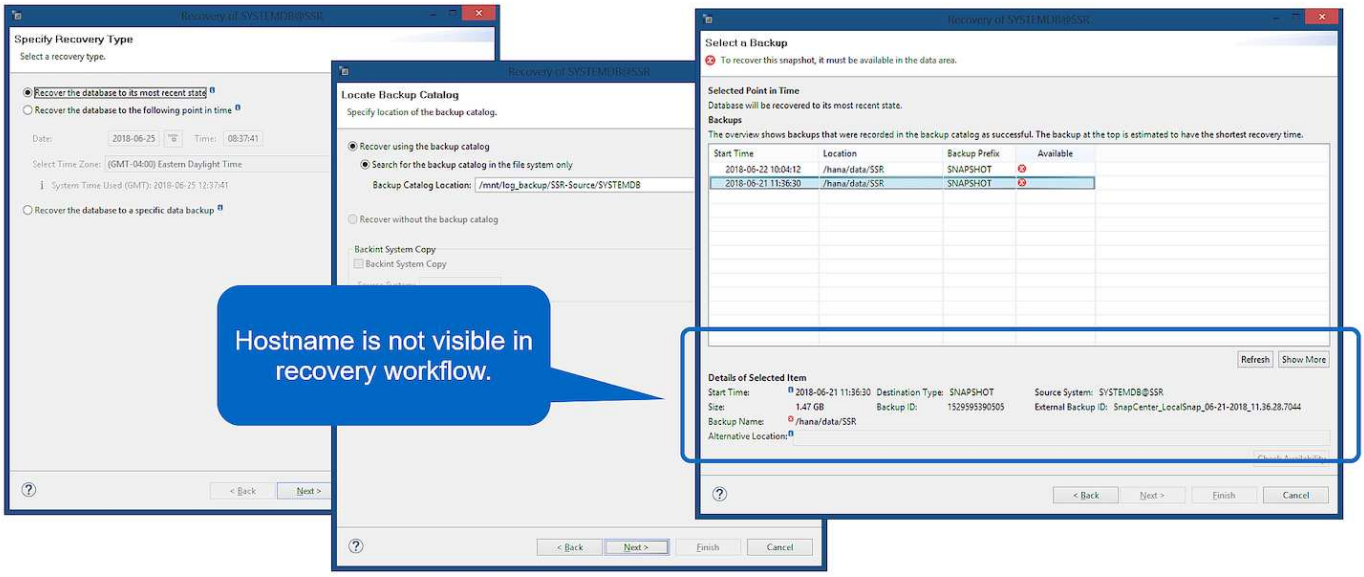
Die folgende Abbildung zeigt den SAP HANA Backup-Katalog in SAP HANA Studio. Die hervorgehobene Sicherung zeigt die Sicherung, die am T1 bei Host 1 erstellt wurde.



25

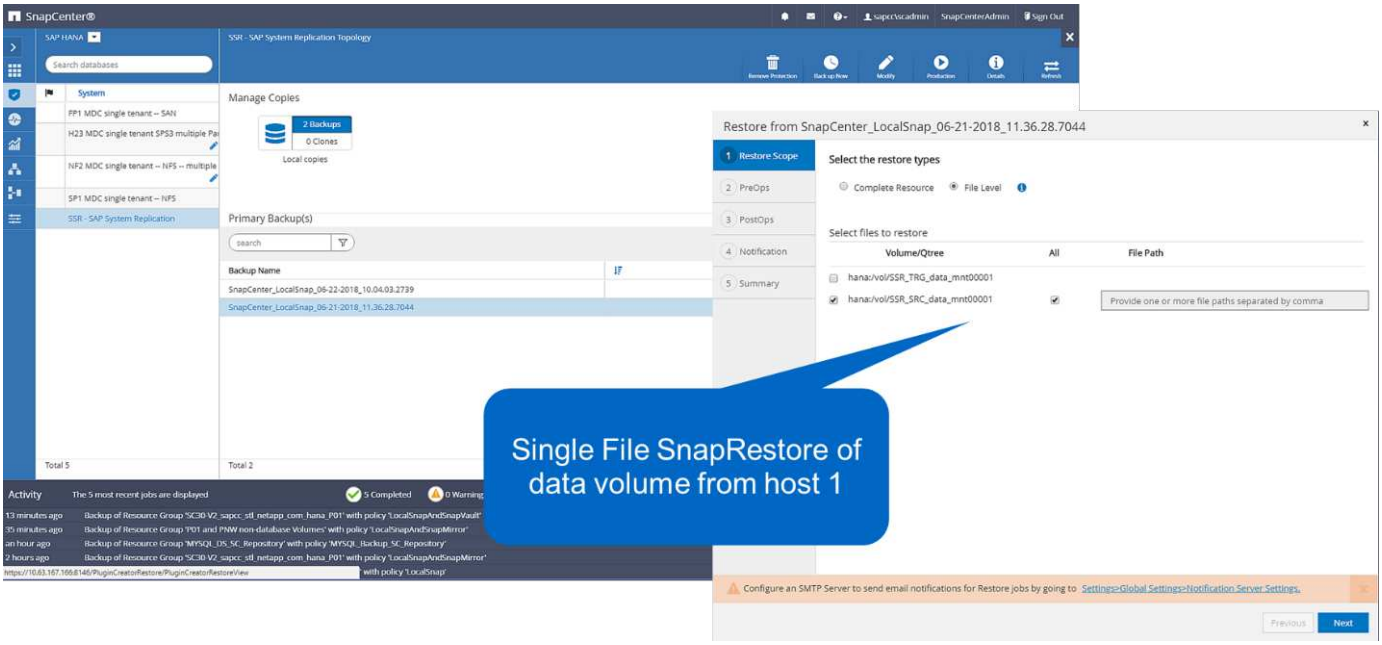
Im SAP HANA Studio wird eine Wiederherstellung gestartet. Wie die folgende Abbildung zeigt, ist der Name des Hosts, auf dem das Backup erstellt wurde, im Wiederherstellungsworkflow nicht sichtbar.

In unserem Testszenario waren wir in der Lage, das richtige Backup (das Backup beim Host 1 erstellt wurde) in SAP HANA Studio zu identifizieren, als die Datenbank noch online war. Wenn die Datenbank nicht verfügbar ist, müssen Sie das SnapCenter Backup-Jobprotokoll prüfen, um das richtige Backup zu finden.

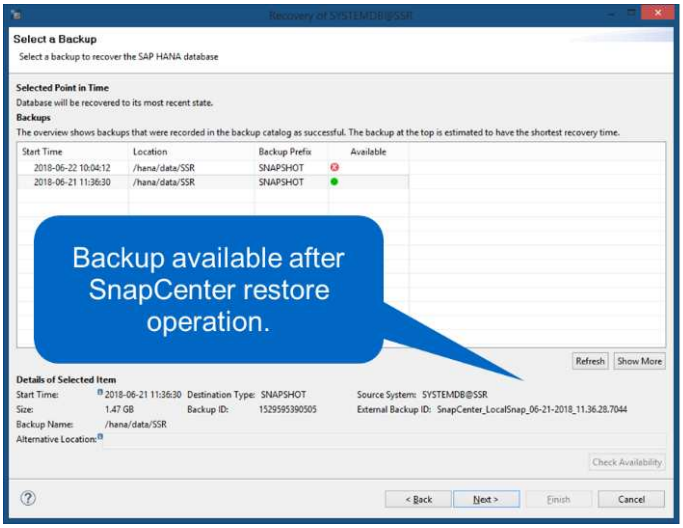


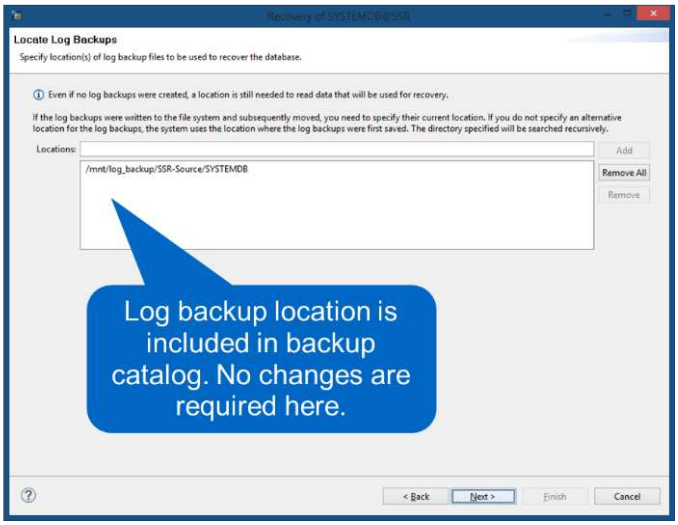
In SnapCenter wird das Backup ausgewählt und ein Restore-Vorgang auf Dateiebene durchgeführt. Auf dem Bildschirm Wiederherstellung auf Dateiebene wird nur das Host 1 Volume ausgewählt, sodass nur das gültige

Backup wiederhergestellt wird.



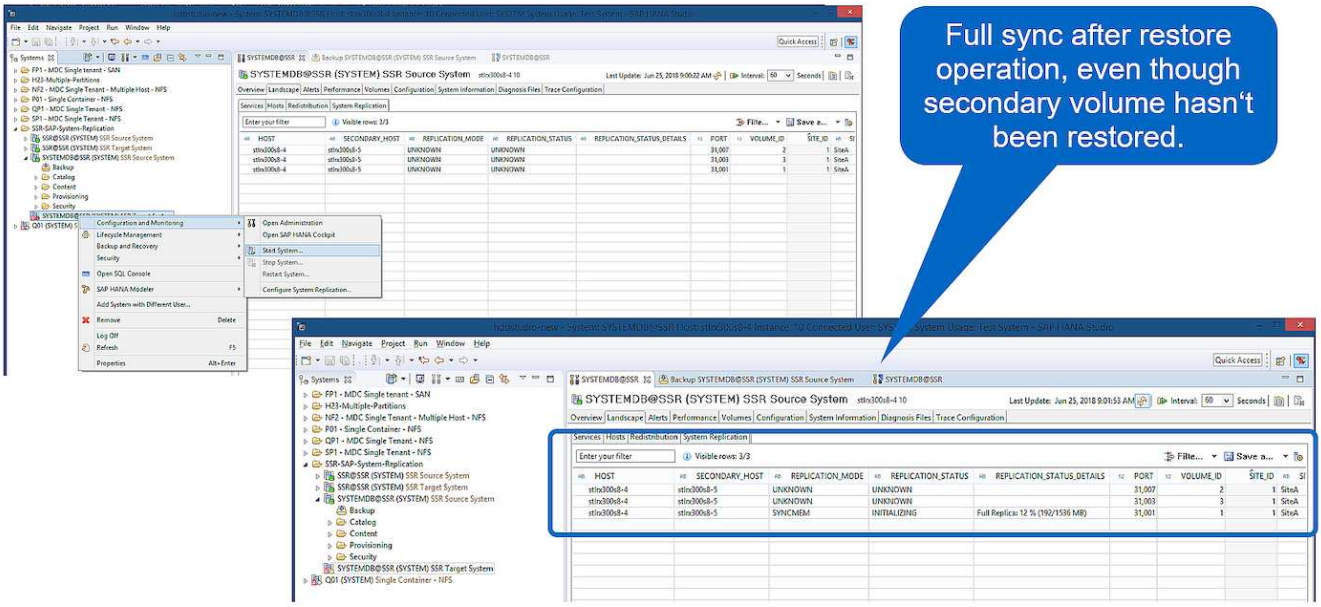
Nach der Wiederherstellung wird das Backup in SAP HANA Studio grün hervorgehoben. Sie müssen nicht einen zusätzlichen Log-Backup-Speicherort eingeben, weil der Dateipfad der Log-Backups von Host 1 und Host 2 im Backup-Katalog enthalten sind.





Nach Abschluss der vorwärts gerichteten Recovery wird der sekundäre Host (Host 2) gestartet und die Resynchronisierung der SAP HANA System Replication gestartet.

Obwohl der sekundäre Host aktuell ist (kein Restore-Vorgang für Host 2 durchgeführt), führt SAP HANA eine vollständige Replizierung aller Daten durch. Dieses Verhalten ist Standard nach einem Restore- und Recovery-Vorgang mit SAP HANA System Replication.

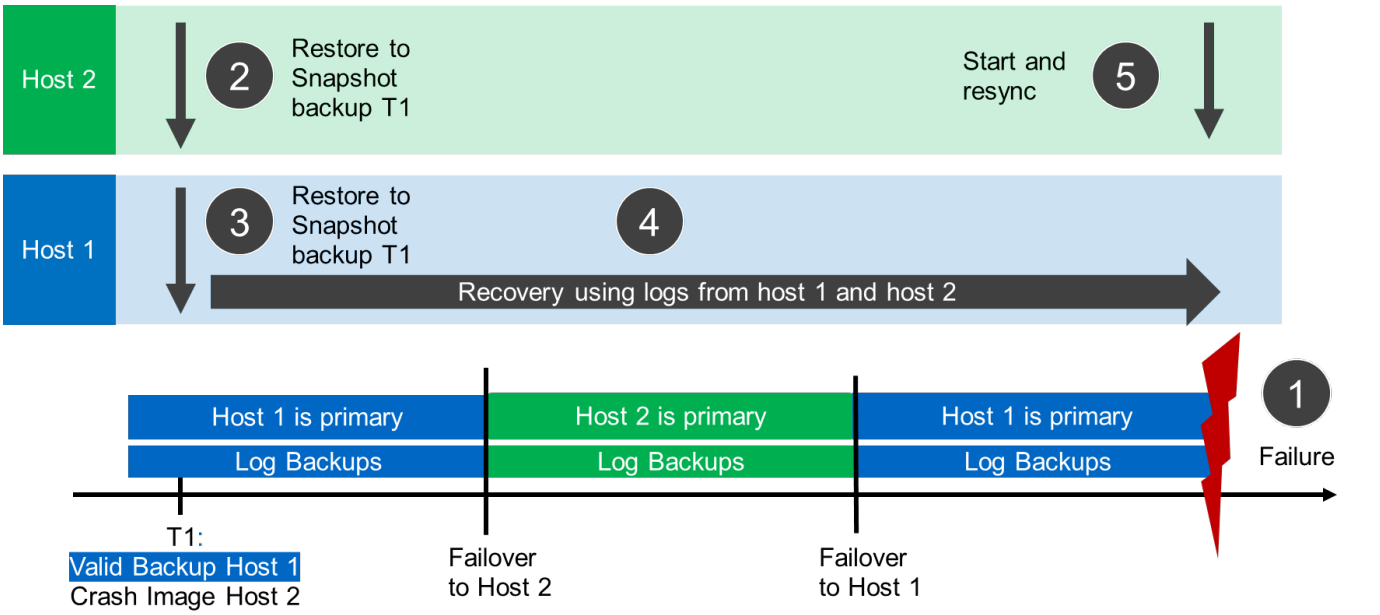


SnapCenter Restore von gültigem Backup- und Crash-Image

Die folgende Abbildung zeigt einen Überblick über das in diesem Abschnitt beschriebene Wiederherstellungsszenario.

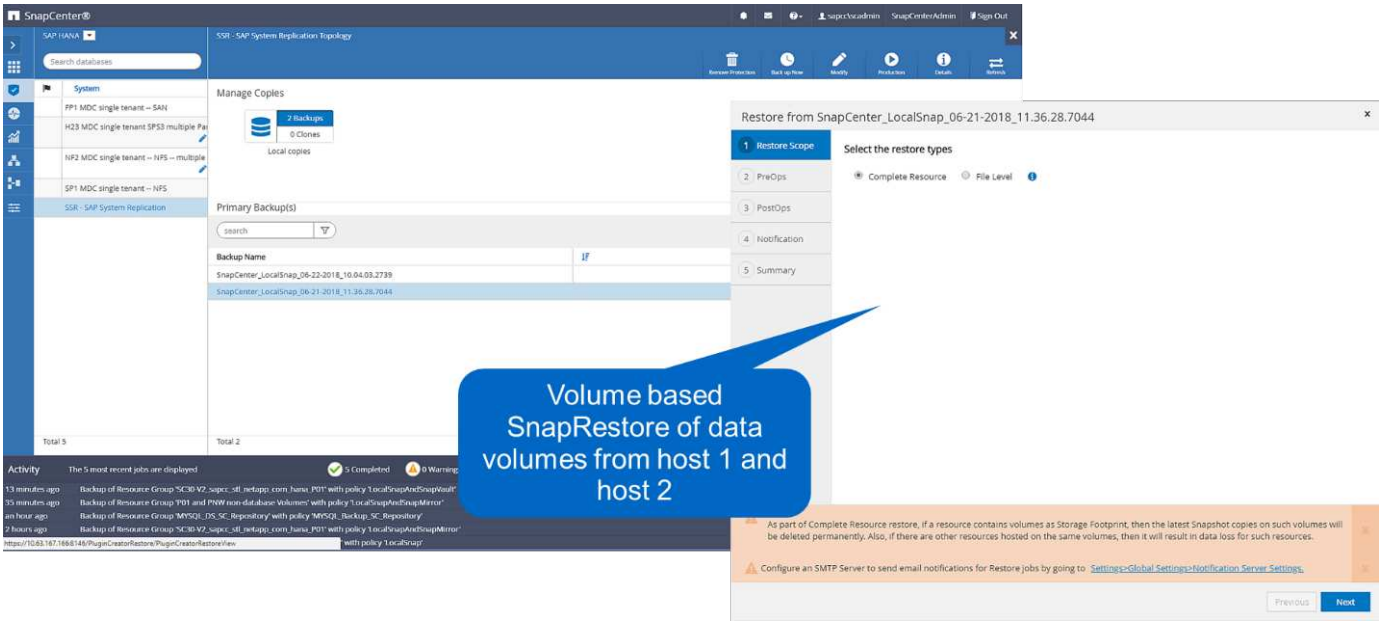
Bei T1 am Host 1 wurde ein Backup erstellt. Ein Failover wurde an Host 2 durchgeführt. Nach einem bestimmten Zeitpunkt wurde ein weiteres Failover zurück zu Host 1 durchgeführt. Zum aktuellen Zeitpunkt ist Host 1 der primäre Host.

1. Es ist ein Fehler aufgetreten, und Sie müssen das am T1 erstellte Backup am Host 1 wiederherstellen.
2. Der sekundäre Host (Host 2) wird heruntergefahren und das T1-Absturzabbild wird wiederhergestellt.
3. Das Speichervolumen von Host 1 wird auf dem bei T1 erstellten Backup wiederhergestellt.
4. Eine vorwärts gerichteten Wiederherstellung wird mit Protokollen von Host 1 und Host 2 durchgeführt.
5. Host 2 wird gestartet und eine Resynchronisierung der Systemreplizierung von Host 2 wird automatisch gestartet.

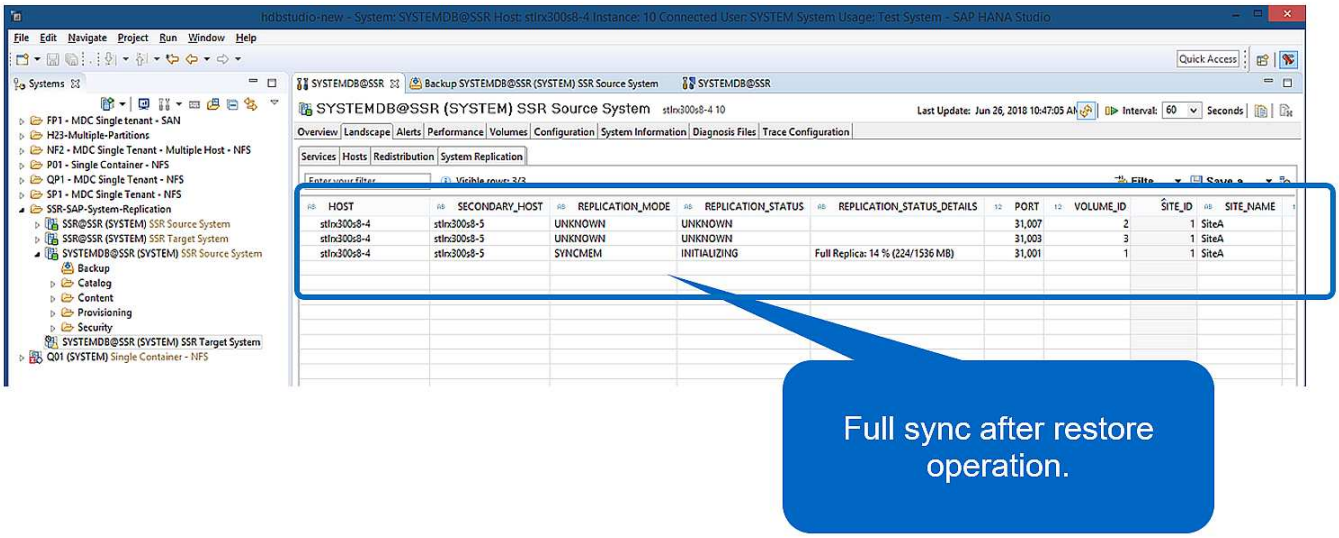


Der Wiederherstellungs- und Wiederherstellungsvorgang mit SAP HANA Studio ist identisch mit den im Abschnitt beschriebenen Schritten "SnapCenter Restore nur für gültige Backups".

Um den Wiederherstellungsvorgang durchzuführen, wählen Sie in SnapCenter die Option Ressource abschließen. Die Volumes beider Hosts werden wiederhergestellt.



Nach Abschluss der erweiterten Recovery wird der sekundäre Host (Host 2) gestartet und die Resynchronisierung von SAP HANA System Replication gestartet. Eine vollständige Replizierung aller Daten wird durchgeführt.



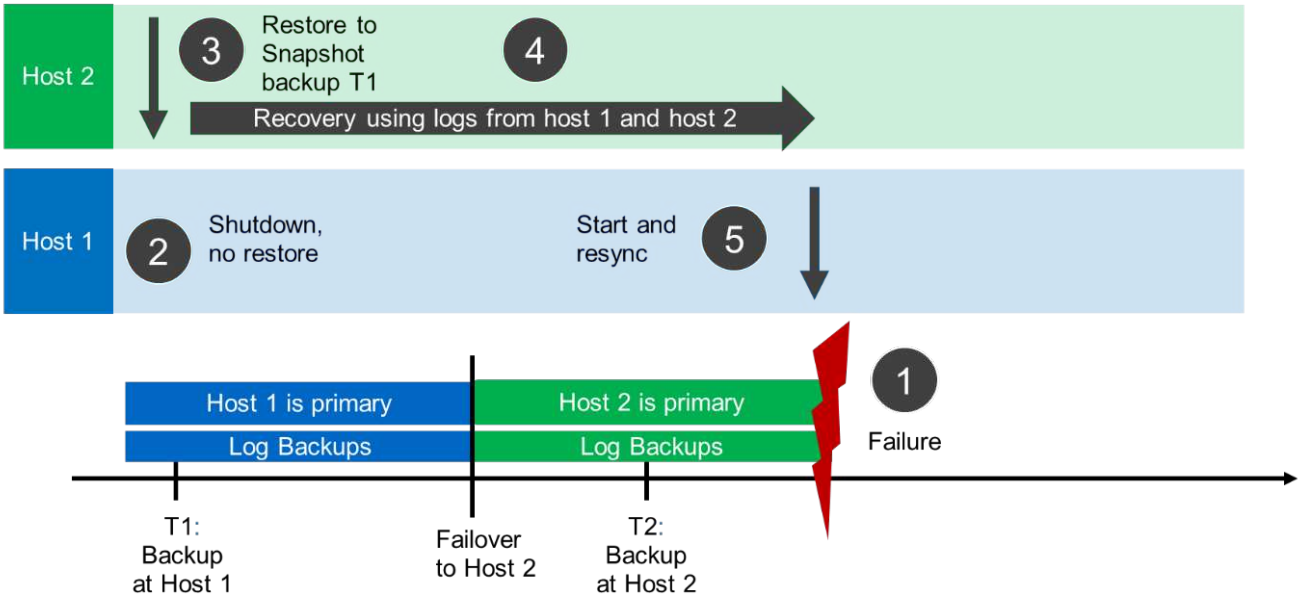
Wiederherstellung und Recovery von einem auf dem anderen Host erstellten Backup

Ein Restore-Vorgang aus einem Backup, das auf dem anderen SAP HANA-Host erstellt wurde, ist ein gültiges Szenario für beide SnapCenter-Konfigurationsoptionen.

Die folgende Abbildung zeigt einen Überblick über das in diesem Abschnitt beschriebene Wiederherstellungsszenario.

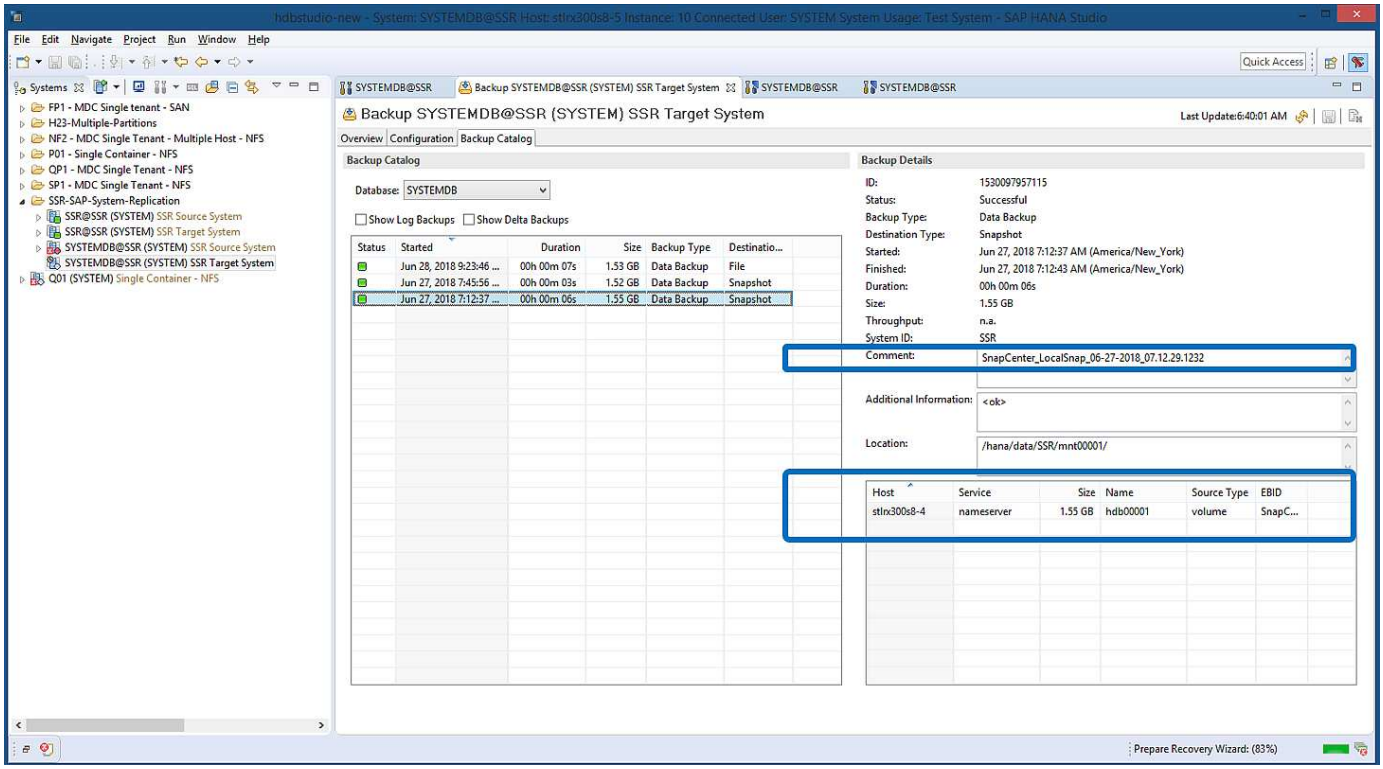
Bei T1 am Host 1 wurde ein Backup erstellt. Ein Failover wurde an Host 2 durchgeführt. Zum aktuellen Zeitpunkt ist Host 2 der primäre Host.

1. Es ist ein Fehler aufgetreten, und Sie müssen das am T1 erstellte Backup am Host 1 wiederherstellen.
2. Der primäre Host (Host 1) wird heruntergefahren.
3. Die Backup-Daten T1 von Host 1 wird auf Host 2 wiederhergestellt.
4. Eine Weiterleitung der Recovery erfolgt mithilfe von Protokollen von Host 1 und Host 2.
5. Host 1 wird gestartet, und die Neusynchronisierung der Systemreplizierung von Host 1 wird automatisch gestartet.



31

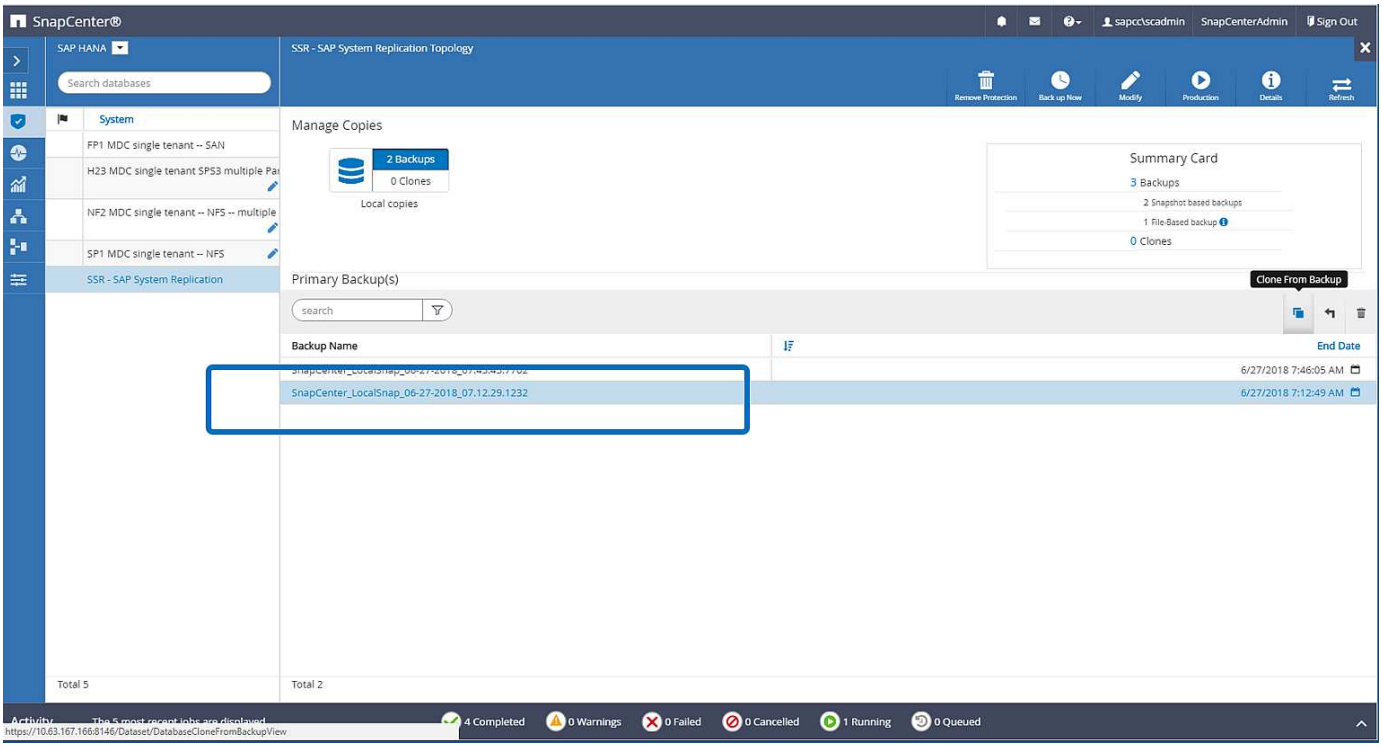
Die folgende Abbildung zeigt den SAP HANA Backup-Katalog und hebt das auf Host 1 erstellte Backup hervor, das für den Restore- und Recovery-Vorgang verwendet wurde.



Die Wiederherstellung umfasst die folgenden Schritte:

1. Erstellen Sie einen Klon aus dem Backup, das auf Host 1 erstellt wurde.
2. Mounten Sie das geklonte Volume unter Host 2.
3. Kopieren Sie die Daten vom geklonten Volume in den ursprünglichen Speicherort.

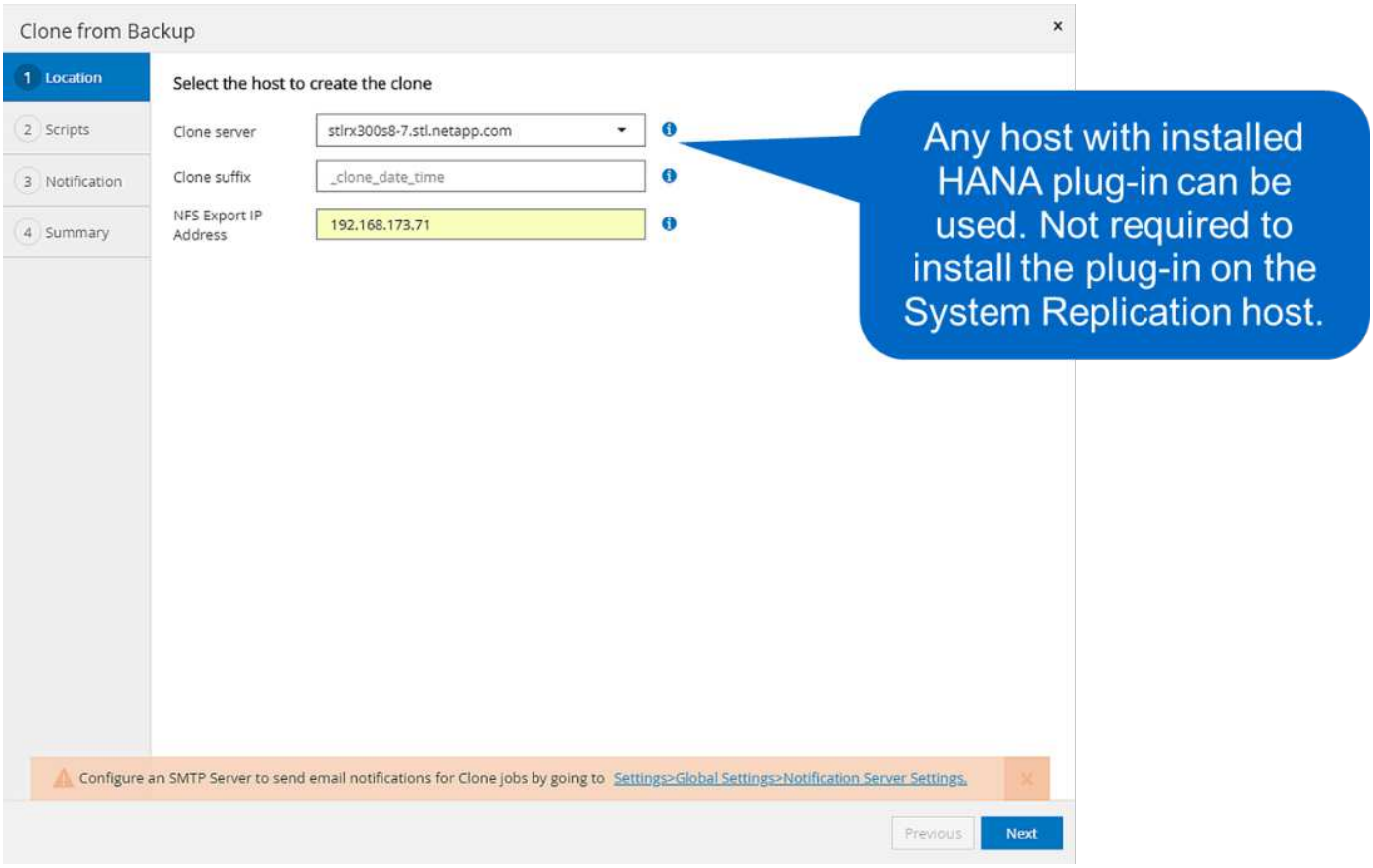
In SnapCenter wird das Backup ausgewählt und der Klonvorgang gestartet.



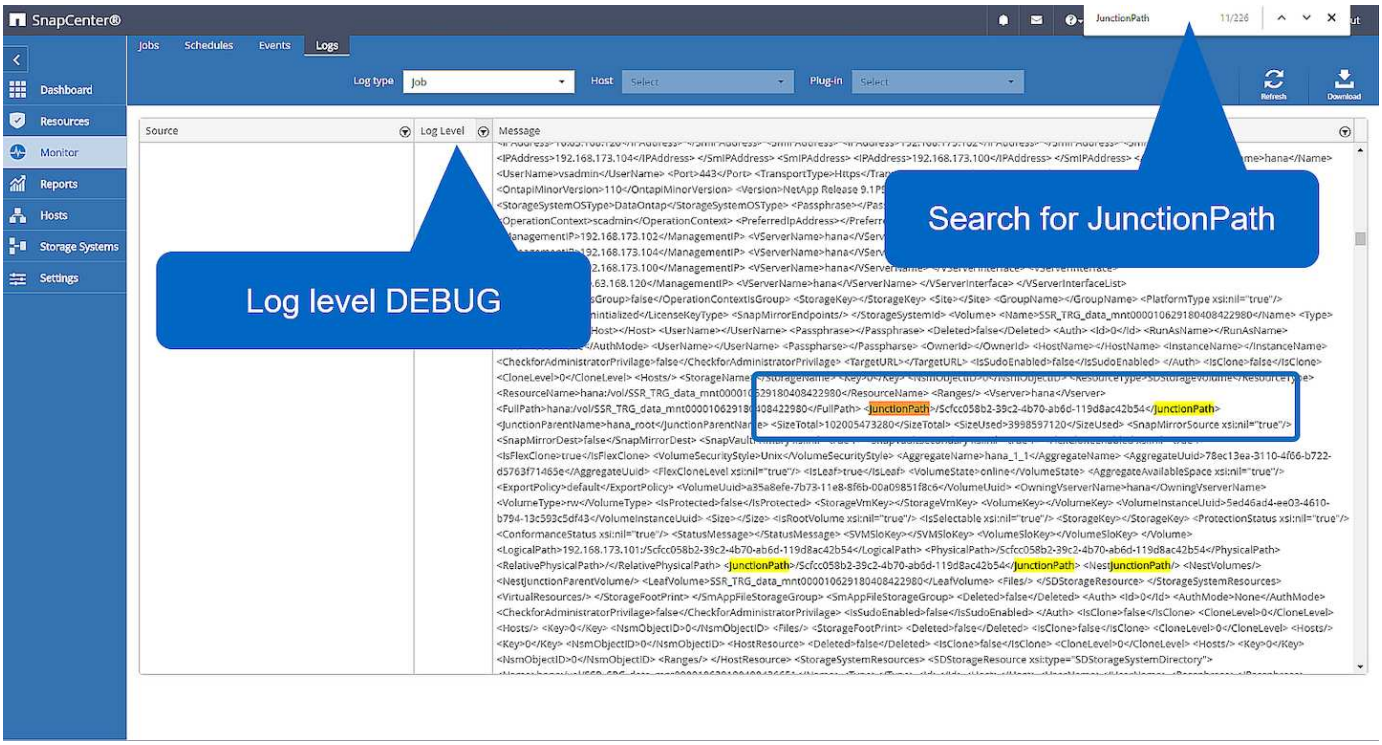
Sie müssen den Klon-Server und die NFS-Export-IP-Adresse angeben.

Bei einer SnapCenter-Konfiguration mit einer Einzelressource ist das SAP HANA-Plug-in nicht auf dem Datenbank-Host installiert. Zum Ausführen des SnapCenter Clone Workflows kann jeder Host mit einem installierten HANA-Plug-in als Klon-Server verwendet werden.

+ in einer SnapCenter-Konfiguration mit separaten Ressourcen wird der HANA-Datenbank-Host als Klon-Server ausgewählt, und ein Mount-Skript wird verwendet, um den Klon auf dem Ziel-Host zu mounten.



Um den Verbindungspfad zu bestimmen, der zum Mounten des geklonten Volume erforderlich ist, prüfen Sie das Jobprotokoll des Klonjobs, wie in der folgenden Abbildung dargestellt.



Das geklonte Volume kann jetzt angehängt werden.

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

Das geklonte Volume enthält die Daten der HANA-Datenbank.

```
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
```

Die Daten werden an den ursprünglichen Speicherort kopiert.

```
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/
```

Die Wiederherstellung mit SAP HANA Studio erfolgt wie im Abschnitt beschrieben"SnapCenter Restore nur für gültige Backups".

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten:

- "Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter"
- "Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"
- Technischer Bericht: SAP HANA Disaster Recovery with Storage Replication

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

Versionsverlauf

Versionsverlauf:

Version	Datum	Versionsverlauf Des Dokuments
Version 1.0	Oktober 2018	Ausgangsversion
Version 2.0	Januar 2022	Update zur Unterstützung von SnapCenter 4.6 HANA System Replication

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.