Backup, Restore und Disaster Recovery

NetApp Solutions SAP

NetApp
March 11, 2024

Inhalt

Backup, Restore und Disaster Recovery

SAP HANA auf Amazon FSX für NetApp ONTAP – Backup und Recovery mit SnapCenter

TR-4926: SAP HANA auf Amazon FSX für NetApp ONTAP – Backup und Recovery mit SnapCenter

Nils Bauer, NetApp

Dieser technische Bericht enthält die Best Practices für die Datensicherung von SAP HANA auf Amazon FSX für NetApp ONTAP und NetApp SnapCenter. Dieses Dokument behandelt SnapCenter-Konzepte, Konfigurationsempfehlungen und Betriebs-Workflows, einschließlich Konfiguration, Backup-Vorgänge Sowie Restore- und Recovery-Vorgänge durchzuführen.

Unternehmen benötigen heutzutage eine kontinuierliche, unterbrechungsfreie Verfügbarkeit ihrer SAP-Applikationen. Sie erwarten eine konsistente Performance, angesichts ständig wachsender Datenvolumen und bei routinemäßigen Wartungsaufgaben, wie System-Backups. Das Durchführen von Backups von SAP-Datenbanken ist eine wichtige Aufgabe, die erhebliche Auswirkungen auf die Performance des SAP-Produktionssystems haben kann.

Die Backup-Fenster verkürzen sich, während die zu sichernden Daten immer größer werden. Daher ist es schwierig, eine Zeit zu finden, in der Backups mit nur minimalen Auswirkungen auf Geschäftsprozesse durchgeführt werden können. Die Zeit, die zum Wiederherstellen und Wiederherstellen von SAP-Systemen benötigt wird, ist besorgt, da Ausfallzeiten von SAP-Produktions- und nicht produktiven Systemen minimiert werden müssen, um die Kosten für das Unternehmen zu senken.

Backup und Recovery mit Amazon FSX für ONTAP

Mit NetApp Snapshot Technologie können Datenbank-Backups innerhalb von Minuten erstellt werden.

Wie lange es dauert, eine Snapshot Kopie zu erstellen, ist unabhängig von der Größe der Datenbank, da bei Snapshot Kopien keine physischen Datenblöcke auf der Storage-Plattform verschoben werden. Darüber hinaus wirkt sich der Einsatz der Snapshot-Technologie auf das laufende SAP-System nicht auf die Performance aus. Daher können Sie die Erstellung von Snapshot Kopien so planen, dass die Zeiten für Spitzenzeiten oder Batch-Aktivitäten nicht berücksichtigt werden. SAP- und NetApp-Kunden planen in der Regel mehrere Online Snapshot Backups pro Tag, beispielsweise alle sechs Stunden ist üblich. Diese Snapshot Backups werden in der Regel drei bis fünf Tage auf dem primären Storage-System gespeichert, bevor sie entfernt oder zu einem günstigeren Storage verschoben werden, und zwar zur langfristigen Aufbewahrung.

Snapshot Kopien bieten auch wichtige Vorteile für Wiederherstellung und Recovery. Mit der NetApp SnapRestore-Technologie können auf der Grundlage der derzeit verfügbaren Snapshot Kopien eine gesamte Datenbank oder alternativ nur ein Teil einer Datenbank zu einem beliebigen Zeitpunkt wiederhergestellt werden. Solche Wiederherstellungen sind innerhalb von wenigen Sekunden abgeschlossen, unabhängig von der Größe der Datenbank. Da mehrere Online Snapshot Backups tagsüber erstellt werden können, verringert sich die für den Recovery-Prozess erforderliche Zeit erheblich im Vergleich zu einem herkömmlichen Backup-Ansatz nur einmal pro Tag. Da Sie eine Wiederherstellung mit einer Snapshot-Kopie durchführen können, die höchstens ein paar Stunden alt ist (anstatt bis zu 24 Stunden), müssen während des Forward Recovery weniger Transaktions-Logs angewendet werden. Daher reduziert sich die RTO auf mehrere Minuten anstatt auf mehrere Stunden, die bei herkömmlichen Streaming Backups benötigt werden.

Backups von Snapshot-Kopien werden auf demselben Festplattensystem wie die aktiven Online-Daten gespeichert. Daher empfiehlt NetApp, Backups von Snapshot-Kopien als Ergänzung zu verwenden, anstatt Backups an einen sekundären Standort zu ersetzen. Die meisten Restore- und Recovery-Aktionen werden mit SnapRestore auf dem primären Storage-System gemanagt. Restores von einem Sekundärstandort sind nur nötig, wenn das primäre Storage-System, das die Snapshot-Kopien enthält, beschädigt ist. Sie können den sekundären Standort auch verwenden, wenn ein Backup wiederhergestellt werden muss, das am primären Standort nicht mehr verfügbar ist.

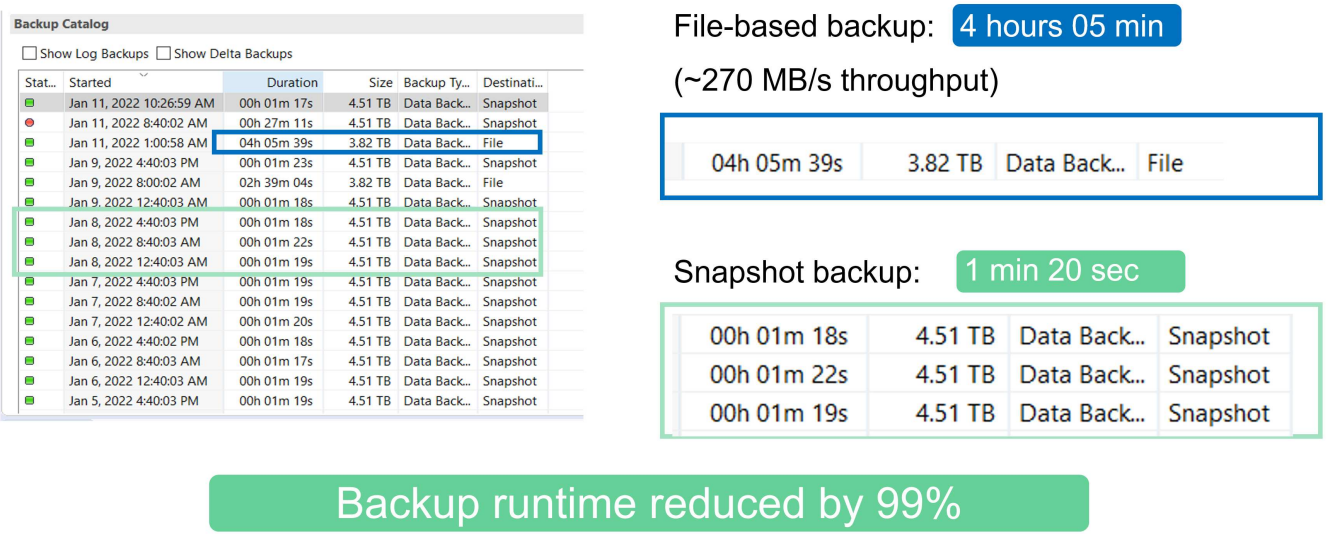
Ein Backup an einen sekundären Standort basiert auf Snapshot-Kopien, die auf dem primären Storage erstellt wurden. Somit werden die Daten direkt aus dem primären Storage-System eingelesen, ohne dass dabei der SAP Datenbankserver belastet wird. Der primäre Storage kommuniziert direkt mit dem sekundären Storage und repliziert mithilfe der NetApp SnapVault Funktion die Backup-Daten am Ziel.

SnapVault bietet im Vergleich zu herkömmlichen Backups deutliche Vorteile. Nach einem anfänglichen Datentransfer, bei dem alle Daten vom Quell- zum Ziel übertragen wurden, werden bei allen nachfolgenden Backups nur die geänderten Blöcke in den sekundären Storage verschoben. Somit werden die Last auf dem primären Storage-System und der Zeitaufwand für ein Vollbackup deutlich reduziert. Da SnapVault nur die geänderten Blöcke am Ziel speichert, belegen alle zusätzlichen vollständigen Datenbank-Backups erheblich weniger Festplattenspeicher.

Laufzeit von Snapshot-Backup- und -Restore-Vorgängen

Die folgende Abbildung zeigt HANA Studio eines Kunden, das Snapshot-Backup-Vorgänge verwendet. Das Bild zeigt, dass die HANA-Datenbank (ca. 4 TB groß) mithilfe der Snapshot Backup-Technologie in 1 Minute und 20 Sekunden und mehr als 4 Stunden bei einem dateibasierten Backup-Vorgang gesichert wird.

Der größte Teil der gesamten Laufzeit des Backup-Workflows ist die Zeit, die zur Ausführung des HANA Backup-Speicherpunktes benötigt wird. Dieser Schritt hängt von der Last der HANA-Datenbank ab. Das Snapshot Backup selbst ist in wenigen Sekunden abgeschlossen.



Vergleich der Recovery-Zeitvorgaben

Dieser Abschnitt enthält einen RTO-Vergleich (Recovery Time Objective) von Datei- und Storage-basierten Snapshot Backups. Das RTO wird durch die Summe der Zeit definiert, die für das Wiederherstellen, Wiederherstellen und Starten der Datenbank benötigt wird.

Benötigte Zeit zum Wiederherstellen der Datenbank

Bei einem dateibasierten Backup hängt die Restore-Zeit von der Größe der Datenbank und der Backup-Infrastruktur ab, die die Restore-Geschwindigkeit in Megabyte pro Sekunde festlegt. Wenn die Infrastruktur beispielsweise einen Restore-Vorgang mit einer Geschwindigkeit von 250 MB/s unterstützt, dauert es etwa 4.5 Stunden, um eine Datenbank mit einer Größe von 4 TB auf der Persistenz wiederherzustellen.

Bei den Backups der Storage Snapshot-Kopien ist die Wiederherstellungszeit unabhängig von der Größe der Datenbank und befindet sich immer im Bereich von einigen Sekunden.

Benötigte Zeit zum Starten der Datenbank

Die Startzeit der Datenbank hängt von der Größe der Datenbank und der Zeit ab, die zum Laden der Daten in den Arbeitsspeicher erforderlich ist. In den folgenden Beispielen wird davon ausgegangen, dass die Daten mit 1000 MBit/s geladen werden können. Das Laden von 4 TB in den Speicher dauert etwa 1 Stunde und 10 Minuten. Die Startzeit ist bei dateibasierten und Snapshot-basierten Restore- und Recovery-Vorgängen gleich.

Benötigte Zeit für das Recovery von Datenbanken

Die Wiederherstellungszeit hängt von der Anzahl der Protokolle ab, die nach der Wiederherstellung angewendet werden müssen. Diese Zahl hängt von der Häufigkeit ab, mit der Daten-Backups erstellt werden.

Bei dateibasierten Daten-Backups wird der Backup-Zeitplan normalerweise einmal pro Tag erstellt. Eine höhere Backup-Frequenz ist normalerweise nicht möglich, da das Backup die Produktions-Performance beeinträchtigt. Daher müssen im schlimmsten Fall alle Protokolle, die während des Tages geschrieben wurden, während der Forward Recovery angewendet werden.

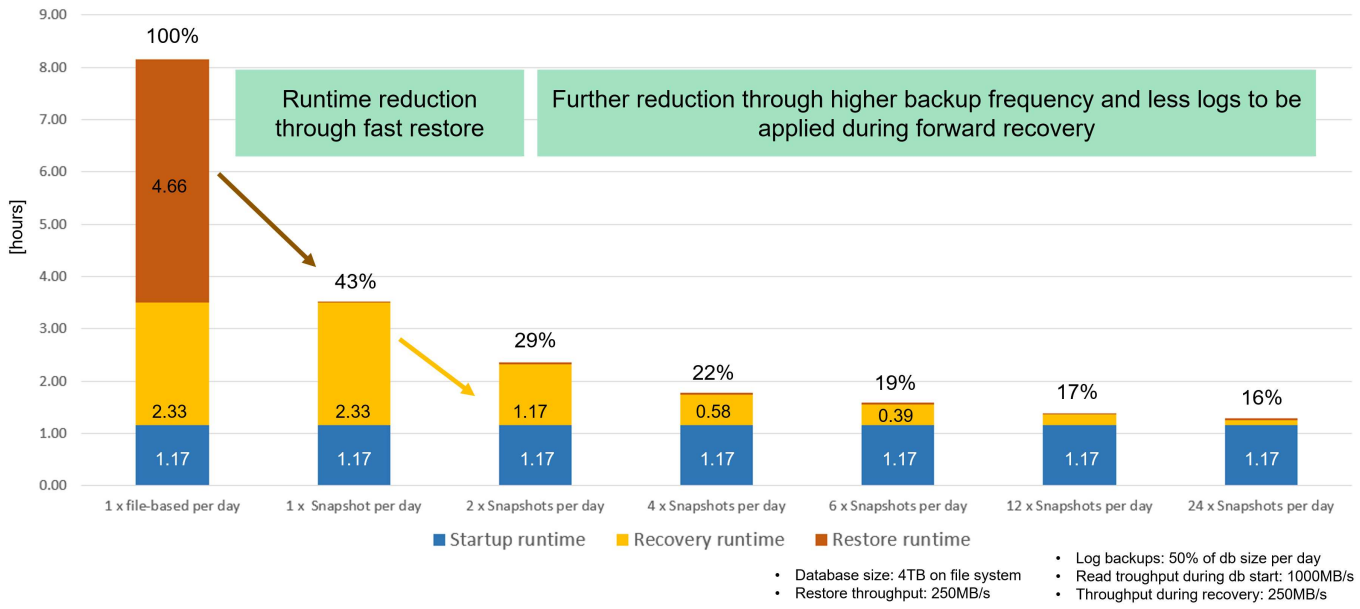
Snapshot Backups werden in der Regel mit höherer Frequenz geplant, da sie nicht die Performance der SAP HANA Datenbank beeinträchtigen. Wenn Snapshot Backups beispielsweise alle sechs Stunden geplant sind, wäre die Recovery-Zeit im schlimmsten Fall ein Viertel der Recovery-Zeit für ein dateibasiertes Backup (6 Stunden / 24 Stunden = .25).

Die folgende Abbildung zeigt einen Vergleich von Restore- und Recovery-Vorgängen mit einem täglichen dateibasierten Backup und Snapshot Backups mit verschiedenen Zeitplänen.

Die ersten beiden Balken zeigen, dass sich auch bei einem einzelnen Snapshot Backup pro Tag die Wiederherstellung und Wiederherstellung dank der Geschwindigkeit des Restore-Vorgangs aus einem Snapshot Backup auf 43 % reduziert. Wenn pro Tag mehrere Snapshot Backups erstellt werden, kann die Laufzeit weiter reduziert werden, da während der Wiederherstellung weniger Protokolle angewendet werden müssen.

Die folgende Abbildung zeigt außerdem, dass vier bis sechs Snapshot Backups pro Tag am sinnvollsten sind, da eine höhere Frequenz keine großen Auswirkungen mehr auf die Gesamtlaufzeit hat.

Restore and Recovery of a 4TB HANA Database (8TB RAM)



Anwendungsfälle und Vorteile beschleunigter Backup- und Klonvorgänge

Die Ausführung von Backups ist ein wichtiger Bestandteil jeder Datensicherungsstrategie. Die Backups werden regelmäßig geplant, um sicherzustellen, dass Sie nach Systemausfällen wiederherstellen können. Dies ist der naheliegende Anwendungsfall, aber auch andere SAP Lifecycle Management-Aufgaben, von denen Beschleunigung von Backup- und Recovery-Vorgängen entscheidend ist.

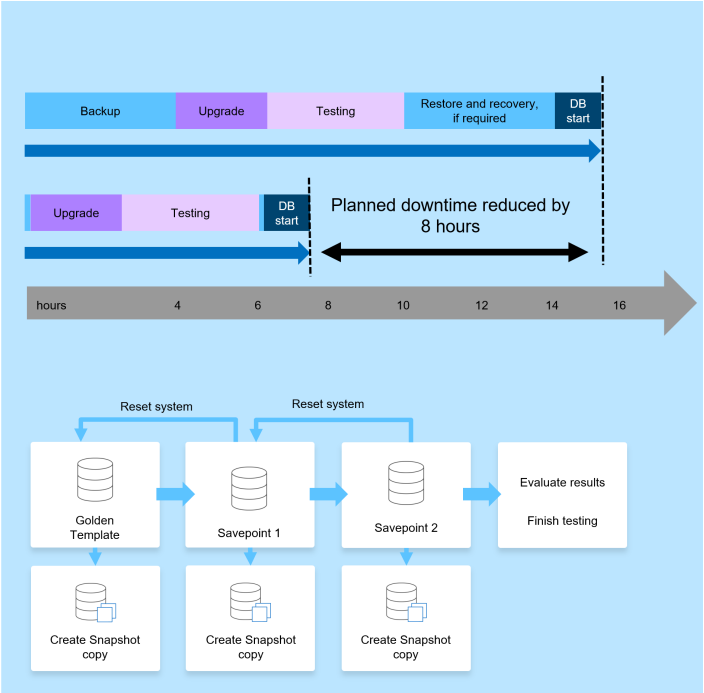
Ein SAP HANA System-Upgrade ist ein Beispiel dafür, wo ein On-Demand-Backup vor dem Upgrade und ein möglicher Restore-Vorgang, wenn das Upgrade fehlschlägt, eine erhebliche Auswirkung auf die gesamte geplante Ausfallzeit hat. Wenn Sie beispielsweise eine Datenbank mit 4 TB verwenden, können Sie die geplanten Ausfallzeiten dank Snapshot-basierter Backup- und Restore-Vorgänge um 8 Stunden reduzieren.

Ein weiteres Anwendungsbeispiel wäre ein typischer Testzyklus, bei dem Tests über mehrere Iterationen mit unterschiedlichen Datensätzen oder Parametern durchgeführt werden müssen. Wenn Sie die schnellen Backup- und Restore-Vorgänge nutzen, können Sie ganz einfach Speicherpunkte innerhalb Ihres Testzyklus erstellen und das System auf jeden dieser vorherigen Speicherpunkte zurücksetzen, wenn ein Test fehlschlägt oder wiederholt werden muss. So können die Tests früher abgeschlossen werden oder es können mehr Tests gleichzeitig durchgeführt werden, und die Testergebnisse werden verbessert.

Use Cases for Backup and Recovery Operations

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

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



Nachdem Snapshot Backups implementiert wurden, können sie für mehrere andere Anwendungsfälle verwendet werden, die Kopien einer HANA-Datenbank benötigen. Mit FSX für ONTAP können Sie ein neues Volume auf Basis des Inhalts jedes verfügbaren Snapshot-Backups erstellen. Die Laufzeit dieses Vorgangs beträgt unabhängig von der Größe des Volumes einige Sekunden.

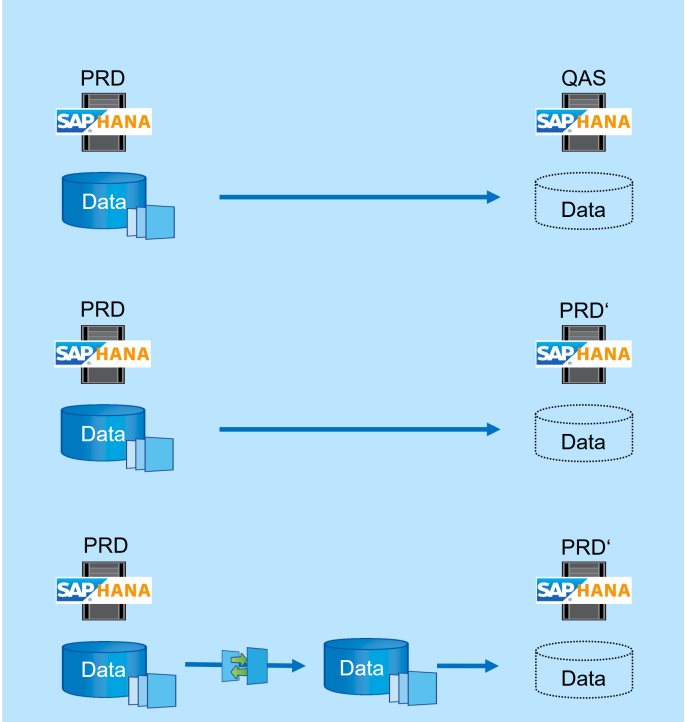
Der beliebteste Anwendungsfall ist SAP Systemaktualisierung, in dem Daten aus dem Produktionssystem in das Test- oder QA-System kopiert werden müssen. Mit der Klonfunktion von FSX für ONTAP lässt sich das Volume für das Testsystem von jeder beliebigen Snapshot Kopie des Produktionssystems in Sekundenschnelle bereitstellen. Das neue Volume muss dann an das Testsystem angeschlossen und die HANA-Datenbank wiederhergestellt werden.

Der zweite Anwendungsfall ist die Erstellung eines Reparatursystems, mit dem eine logische Beschädigung im Produktionssystem bewältigt wird. In diesem Fall wird ein älteres Snapshot Backup des Produktionssystems verwendet, um ein Reparatursystem zu starten, das ein identischer Klon des Produktionssystems mit den Daten ist, bevor die Beschädigung aufgetreten ist. Das Reparatursystem wird dann verwendet, um das Problem zu analysieren und die erforderlichen Daten zu exportieren, bevor sie beschädigt wurden.

Im letzten Anwendungsfall kann ein Disaster-Recovery-Failover-Test ausgeführt werden, ohne die Replizierung zu unterbrechen. Dies hat keinen Einfluss auf RTO und Recovery Point Objective (RPO) des Disaster-Recovery-Setups. Wenn die Daten mithilfe von FSX für ONTAP Replizierung mit NetApp SnapMirror am Disaster Recovery-Standort repliziert werden, stehen am Disaster Recovery-Standort Snapshot Backups der Produktionsumgebung zur Verfügung und können dann für Tests im Disaster Recovery ein neues Volume erstellt werden.

Use Cases for Cloning Operations

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



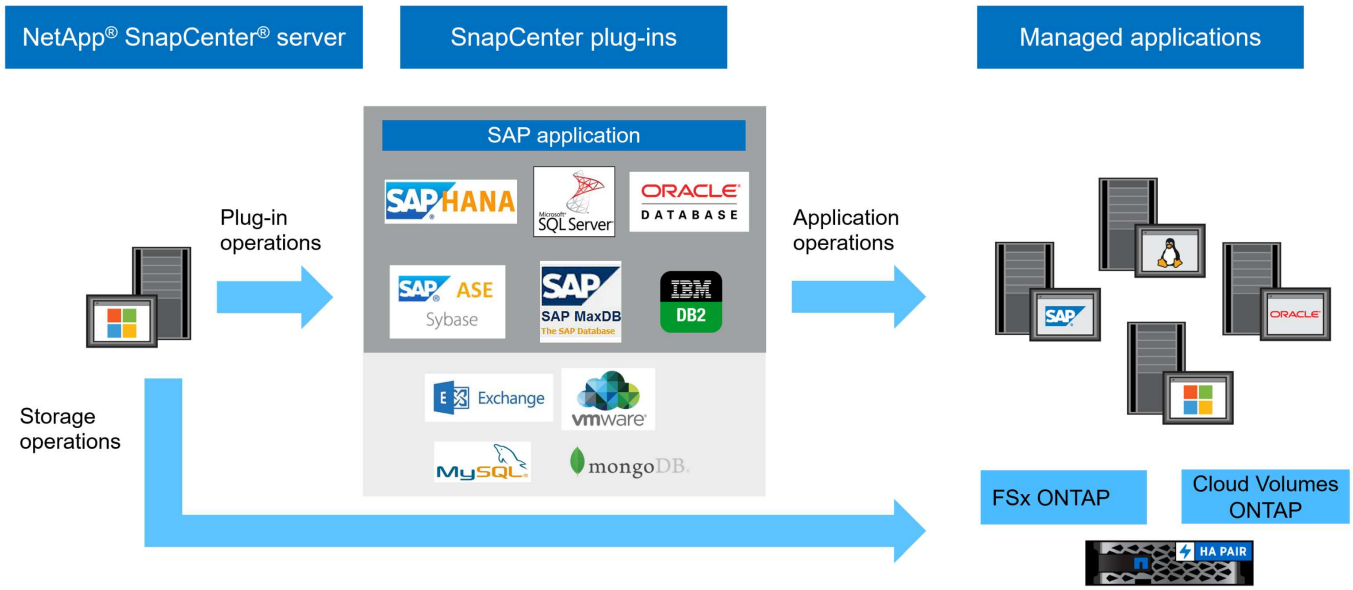
Architektur von SnapCenter

SnapCenter ist eine einheitliche, skalierbare Plattform für applikationskonsistente Datensicherung. SnapCenter bietet zentrale Kontrolle und Überwachung und delegiert die Möglichkeit, dass Benutzer applikationsspezifische Backup-, Restore- und Klonaufgaben managen können. Mit SnapCenter erhalten Datenbank- und Storage-Administratoren ein Tool, mit dem sie Backup-, Wiederherstellungs- und Klonvorgänge für verschiedene Applikationen und Datenbanken managen können.

SnapCenter managt Daten über Endpunkte in der Data-Fabric-Architektur von NetApp hinweg. Daten können mit SnapCenter zwischen lokalen Umgebungen, zwischen lokalen Umgebungen und der Cloud sowie zwischen Private, Hybrid oder Public Clouds repliziert werden.

Komponenten von SnapCenter

SnapCenter umfasst den SnapCenter-Server, das SnapCenter-Plug-in-Paket für Windows und das SnapCenter-Plug-in-Paket für Linux. Jedes Paket enthält SnapCenter-Plug-ins für diverse Applikations- und Infrastrukturkomponenten.



SnapCenter SAP HANA Backup-Lösung

Die SnapCenter Backup-Lösung für SAP HANA umfasst folgende Bereiche:

- Backup-Vorgänge, Planung und Aufbewahrungsmanagement
  - SAP HANA Daten-Backup mit Storage-basierten Snapshot Kopien
  - Backup nicht datenbasierter Volumes mit Storage-basierten Snapshot Kopien (z. B. `/hana/shared`)
  - Integritätsprüfungen der Datenbankblöcke mithilfe eines dateibasierten Backups
  - Die Replizierung an ein externes Backup oder einen Disaster-Recovery-Standort
- Allgemeine Ordnung und Sauberkeit des SAP HANA Backup-Katalogs
  - Für HANA Daten-Backups (Snapshot und dateibasiert)
  - Für HANA-Protokoll-Backups
- Restore- und Recovery-Vorgänge
  - Automatisiertes Restore und Recovery
  - Restore von einzelnen Mandanten für SAP HANA (MDC)-Systeme

Backups von Datenbankdateien werden von SnapCenter in Kombination mit dem Plug-in für SAP HANA ausgeführt. Das Plug-in löst den Speicherpunkt für das SAP HANA Datenbank-Backup aus, sodass die Snapshot Kopien, die auf dem primären Storage-System erstellt werden, auf einem konsistenten Image der SAP HANA Datenbank basieren.

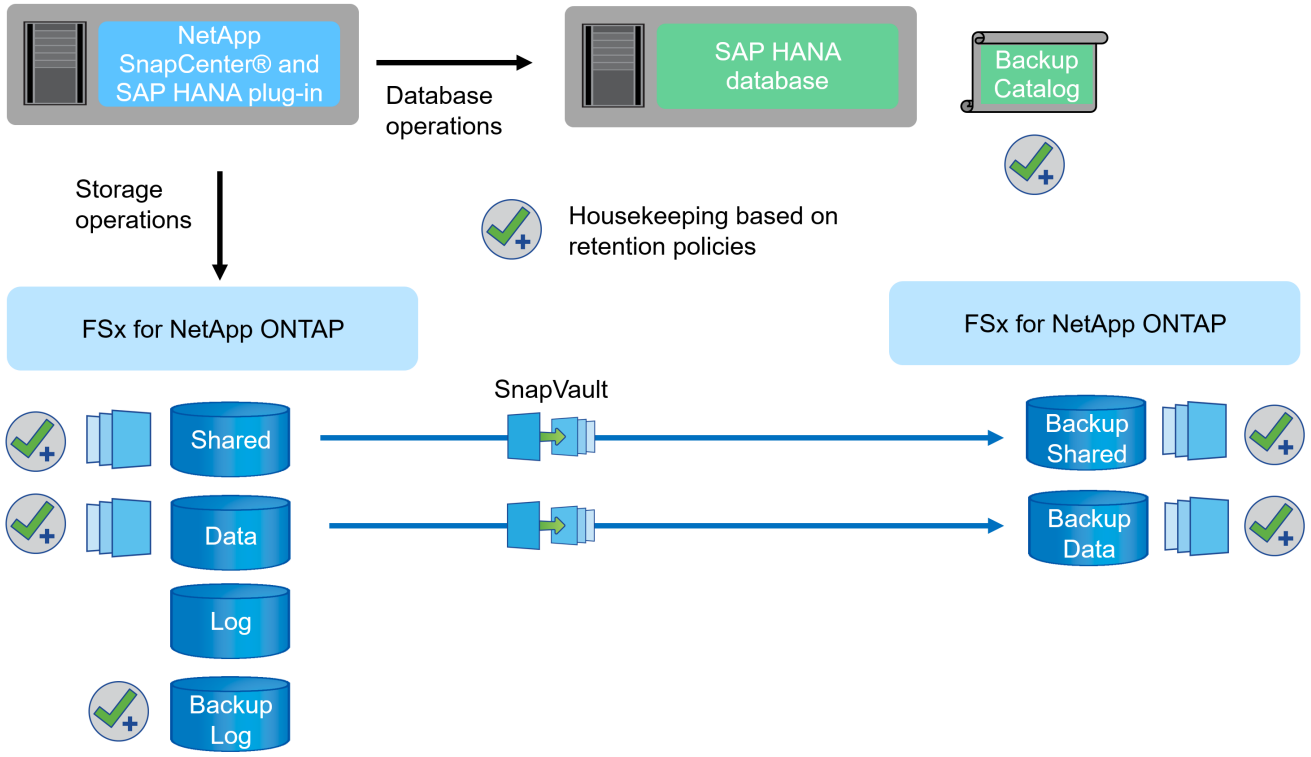
SnapCenter ermöglicht die Replizierung konsistenter Datenbank-Images auf einen externen Backup- oder Disaster-Recovery-Standort mithilfe von SnapVault oder der SnapMirror Funktion. In der Regel werden verschiedene Aufbewahrungsrichtlinien für Backups auf dem primären und externen Backup-Storage definiert. SnapCenter übernimmt die Aufbewahrung im Primärspeicher und ONTAP übernimmt die Aufbewahrung auf dem externen Backup-Storage.

Für ein vollständiges Backup aller mit SAP HANA verbundenen Ressourcen ermöglicht SnapCenter auch das Backup aller nicht datenbezogenen Volumes über das SAP HANA Plug-in mit Storage-basierten Snapshot Kopien. Sie können nicht-Daten-Volumes unabhängig vom Datenbank-Daten-Backup planen, um individuelle Aufbewahrungs- und Sicherungsrichtlinien zu aktivieren.

SAP empfiehlt, Storage-basierte Snapshot-Backups mit einem wöchentlichen dateibasierten Backup zu kombinieren, um eine Integritätsprüfung für Blöcke durchzuführen. Sie können die Integritätsprüfung der Blöcke in SnapCenter ausführen. Basierend auf Ihren konfigurierten Aufbewahrungsrichtlinien managt SnapCenter die allgemeine Ordnung und Sauberkeit der Datendatei-Backups im primären Storage, Backup von Protokolldateien und den SAP HANA Backup-Katalog.

SnapCenter übernimmt die Aufbewahrung auf dem primären Storage, während FSX für ONTAP die sekundäre Backup-Aufbewahrung managt.

Die folgende Abbildung bietet einen Überblick über die SnapCenter Backup- und Aufbewahrungsvorgänge.



Beim Ausführen eines Storage-basierten Snapshot Backups der SAP HANA Datenbank führt SnapCenter die folgenden Aufgaben durch:

1. Erstellung eines SAP HANA Backup-Speicherpunktes, um ein konsistentes Image auf der Persistenzschicht zu erstellen.
2. Erstellt eine Storage-basierte Snapshot Kopie des Daten-Volumes
3. Registrieren des Storage-basierten Snapshot-Backups im SAP HANA Backup-Katalog
4. Gibt den Speicherpunkt für SAP HANA Backup frei.
5. Führt, falls konfiguriert, ein SnapVault oder SnapMirror Update für das Daten-Volume durch
6. Löscht die Storage-Snapshot-Kopien im primären Storage auf der Grundlage der definierten Aufbewahrungsrichtlinien.
7. Löscht die Einträge des SAP HANA Backup-Katalogs, wenn die Backups nicht mehr im primären oder externen Backup-Speicher vorhanden sind.
8. Sobald ein Backup auf Basis der Aufbewahrungsrichtlinie oder manuell gelöscht wurde, löscht SnapCenter auch alle Log-Backups, die älter als das älteste Daten-Backup sind. Log-Backups werden im Dateisystem und im SAP HANA Backup-Katalog gelöscht.

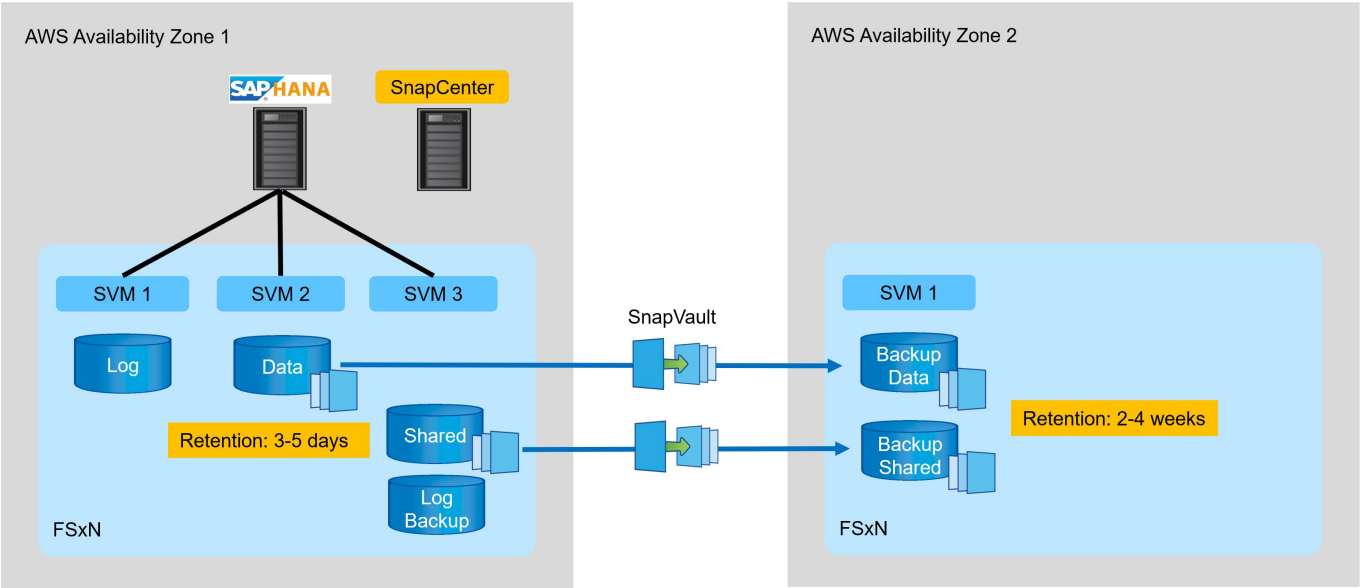
Inhalt des vorliegenden Dokuments

Dieses Dokument beschreibt die gängigste SnapCenter-Konfigurationsoption für ein einzelnes Hostsystem mit einem einzelnen SAP HANA MDC-Mandanten auf FSX für ONTAP. Es sind andere Konfigurationsoptionen möglich und in manchen Fällen auch für bestimmte SAP HANA Systeme erforderlich, beispielsweise für ein mehrere Host-Systeme. Eine ausführliche Beschreibung zu anderen Konfigurationsoptionen finden Sie unter "SnapCenter-Konzepte und Best Practices (netapp.com)".

In diesem Dokument verwenden wir die Amazon Web Services (AWS)-Konsole und die FSX für ONTAP CLI, um die erforderlichen Konfigurationsschritte auf der Storage-Ebene auszuführen. Sie können FSX für ONTAP auch mit NetApp Cloud Manager managen. Dies ist jedoch nicht im Umfang dieses Dokuments enthalten. Informationen zur Verwendung von NetApp Cloud Manager für FSX für ONTAP finden Sie unter "Weitere Informationen zu Amazon FSX für ONTAP (netapp.com)".

Datensicherung Strategie

Die folgende Abbildung zeigt eine typische Backup-Architektur für SAP HANA auf FSX für ONTAP. Das HANA-System befindet sich in der AWS-Verfügbarkeitszone 1 und verwendet ein FSX für ONTAP-Dateisystem innerhalb derselben Verfügbarkeitszone. Snapshot Backup-Vorgänge werden für die Daten und das gemeinsam genutzte Volume der HANA Datenbank ausgeführt. Neben den lokalen Snapshot Backups, die 3-5 Tage aufbewahrt werden, werden Backups auch zur längerfristigen Aufbewahrung auf einen externen Storage repliziert. Der externe Backup-Storage ist ein zweites FSX für ONTAP-Filesystem, das sich in einer anderen AWS-Verfügbarkeitszone befindet. Backups der HANA Daten und des gemeinsam genutzten Volumes werden mit SnapVault in die zweite FSX für ONTAP Filesystem repliziert und 2-3 Wochen aufbewahrt.



Vor dem Konfigurieren von SnapCenter muss die Datensicherungsstrategie auf Basis der RTO- und RPO-Anforderungen der verschiedenen SAP Systeme definiert werden.

Ein gemeinsamer Ansatz besteht in der Definition von Systemtypen wie Systemen für Produktion, Entwicklung, Test oder Sandbox. Alle SAP-Systeme des gleichen Systemtyps haben typischerweise die gleichen Datenschutzparameter.

Folgende Parameter müssen definiert werden:

- Wie oft sollte ein Snapshot Backup ausgeführt werden?
- Wie lange sollten Snapshot Kopien Backups auf dem Primärspeichersystem aufbewahrt werden?

- Wie oft sollte eine Blockintegritätsprüfung ausgeführt werden?
- Sollten die primären Backups auf einen externen Backup-Standort repliziert werden?
- Wie lange sollten die Backups auf dem externen Backup-Storage aufbewahrt werden?

Die folgende Tabelle zeigt ein Beispiel für die Datensicherungsparameter für die Systemtypen: Produktion, Entwicklung und Test. Für das Produktionssystem wurde eine hohe Backup-Frequenz definiert und die Backups werden einmal pro Tag an einen externen Backup-Standort repliziert. Die Testsysteme haben niedrigere Anforderungen und keine Replikation der Backups.

Parameter	**Produktionssysteme auszuführen**	**Entwicklungssysteme**	**Testsysteme**
Sicherungshäufigkeit	Alle 6 Stunden	Alle 6 Stunden	Alle 6 Stunden
Primäre Aufbewahrung	3 Tage	3 Tage	3 Tage
Block-Integritätsprüfung	Einmal in der Woche	Einmal in der Woche	Nein
Replizierung an externe Backup-Standorte	Einmal am Tag	Einmal am Tag	Nein
Externe Backup-Aufbewahrung	2 Wochen	2 Wochen	Keine Angabe

In der folgenden Tabelle werden die Richtlinien aufgeführt, die für die Datensicherheitsparameter konfiguriert werden müssen.

Parameter	**RichtliniengebietsSnap**	**Policy LocalSnapAndSnapVault**	**RichtlinienblockIntegritätsprüfung**
Backup-Typ	Auf Snapshot-Basis	Auf Snapshot-Basis	File-basiert
Zeitplanhäufigkeit	Stündlich	Täglich	Wöchentlich
Primäre Aufbewahrung	Anzahl = 12	Anzahl = 3	Anzahl = 1
SnapVault Replizierung	Nein	Ja.	Keine Angabe

Richtlinie `LocalSnapshot` Werden für Produktions-, Entwicklungs- und Testsysteme verwendet, um lokale Snapshot-Backups mit einer Aufbewahrung von zwei Tagen abzudecken.

In der Konfiguration für den Ressourcenschutz wird der Zeitplan für die Systemtypen unterschiedlich definiert:

- Produktion: Zeitplan alle 4 Stunden.
- Entwicklung: Alle 4 Stunden einplanen.
- Test: Alle 4 Stunden planen.

Richtlinie `LocalSnapAndSnapVault` Wird für die Produktions- und Entwicklungssysteme eingesetzt, um die tägliche Replizierung auf den externen Backup Storage zu decken.

In der Konfiguration für den Ressourcenschutz wird der Zeitplan für die Produktion und Entwicklung definiert:

- Produktion: Zeitplan jeden Tag.
- Entwicklung: Zeitplan jeden Tag.die Politik `BlockIntegrityCheck` Wird für die Produktions- und

Entwicklungssysteme eingesetzt, um die wöchentliche Blockintegritätsprüfung mithilfe eines dateibasierten Backups abzudecken.

In der Konfiguration für den Ressourcenschutz wird der Zeitplan für die Produktion und Entwicklung definiert:

- Produktion: Zeitplan jede Woche.
- Entwicklung: Zeitplan jede Woche.

Für jede einzelne SAP HANA Datenbank, die die externe Backup-Richtlinie nutzt, müssen Sie eine Sicherungsbeziehung auf der Storage-Ebene konfigurieren. Die Sicherungsbeziehung definiert, welche Volumes repliziert werden und wie die Aufbewahrung von Backups im externen Backup-Storage aufbewahrt wird.

Im folgenden Beispiel wird für jedes Produktions- und Entwicklungssystem im externen Backup-Storage eine Aufbewahrung von zwei Wochen definiert.

In diesem Beispiel unterscheiden sich die Sicherungsrichtlinien und die Aufbewahrung von SAP HANA Datenbankressourcen und Ressourcen ohne Datenvolumen.

Beispiel für die Laboreinrichtung

Das folgende Lab-Setup wurde als Beispielkonfiguration für den Rest dieses Dokuments verwendet.

HANA-System-PFX:

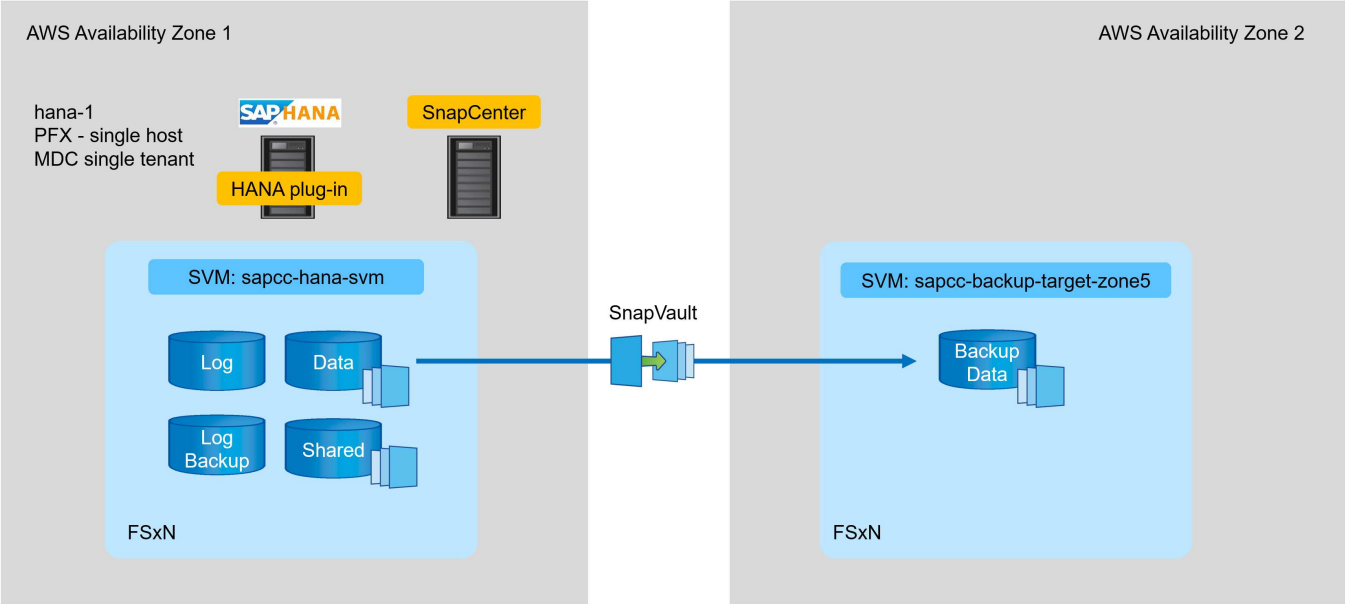
- Ein Host-MDC-System mit einem einzelnen Mandanten
- HANA 2.0 SPS 6, Version 60
- SLES FÜR SAP 15SP3

SnapCenter

- Version 4.6
- Auf einem HANA Datenbank-Host implementiertem HANA und Linux Plug-in

FSX für ONTAP-Dateisysteme:

- Zwei FSX für ONTAP Filesysteme mit einer einzigen Storage Virtual Machine (SVM)
- Jedes FSX für ONTAP-System in einer anderen AWS-Verfügbarkeitszone
- HANA Daten-Volume zur Replizierung in das zweite FSX für ONTAP Filesystem



SnapCenter-Konfiguration

Sie müssen die in diesem Abschnitt aufgeführten Schritte zur Basiskonfiguration von SnapCenter und zum Schutz der HANA-Ressource ausführen.

Übersicht über die Konfigurationsschritte

Führen Sie die folgenden Schritte für die SnapCenter Basiskonfiguration und den Schutz der HANA-Ressource durch. Jeder Schritt wird in den folgenden Kapiteln detailliert beschrieben.

1. Konfiguration des SAP HANA-Backup-Benutzers und des hdbuserstore-Schlüssels Zugriff auf die HANA-Datenbank mit dem hdbsql-Client
2. Konfigurieren Sie den Speicher in SnapCenter. Zugangsdaten für den Zugriff auf FSX für ONTAP SVMs von SnapCenter aus
3. Konfigurieren Sie Anmeldedaten für die Plug-in-Bereitstellung. Wird verwendet, um die erforderlichen SnapCenter-Plug-ins automatisch auf dem HANA-Datenbank-Host zu implementieren und zu installieren.
4. Fügen Sie HANA-Host zu SnapCenter hinzu. Implementierung und Installation der erforderlichen SnapCenter Plug-ins
5. Richtlinien konfigurieren. Definiert den Backup-Typ (Snapshot, Datei), die Aufbewahrung sowie optionale Snapshot Backup-Replizierung.
6. Konfigurieren Sie den Schutz von HANA-Ressourcen. Bereitstellung von hdbuserstore-Schlüsselrichtlinien und -Zeitplänen sowie Anhängen an die HANA-Ressource

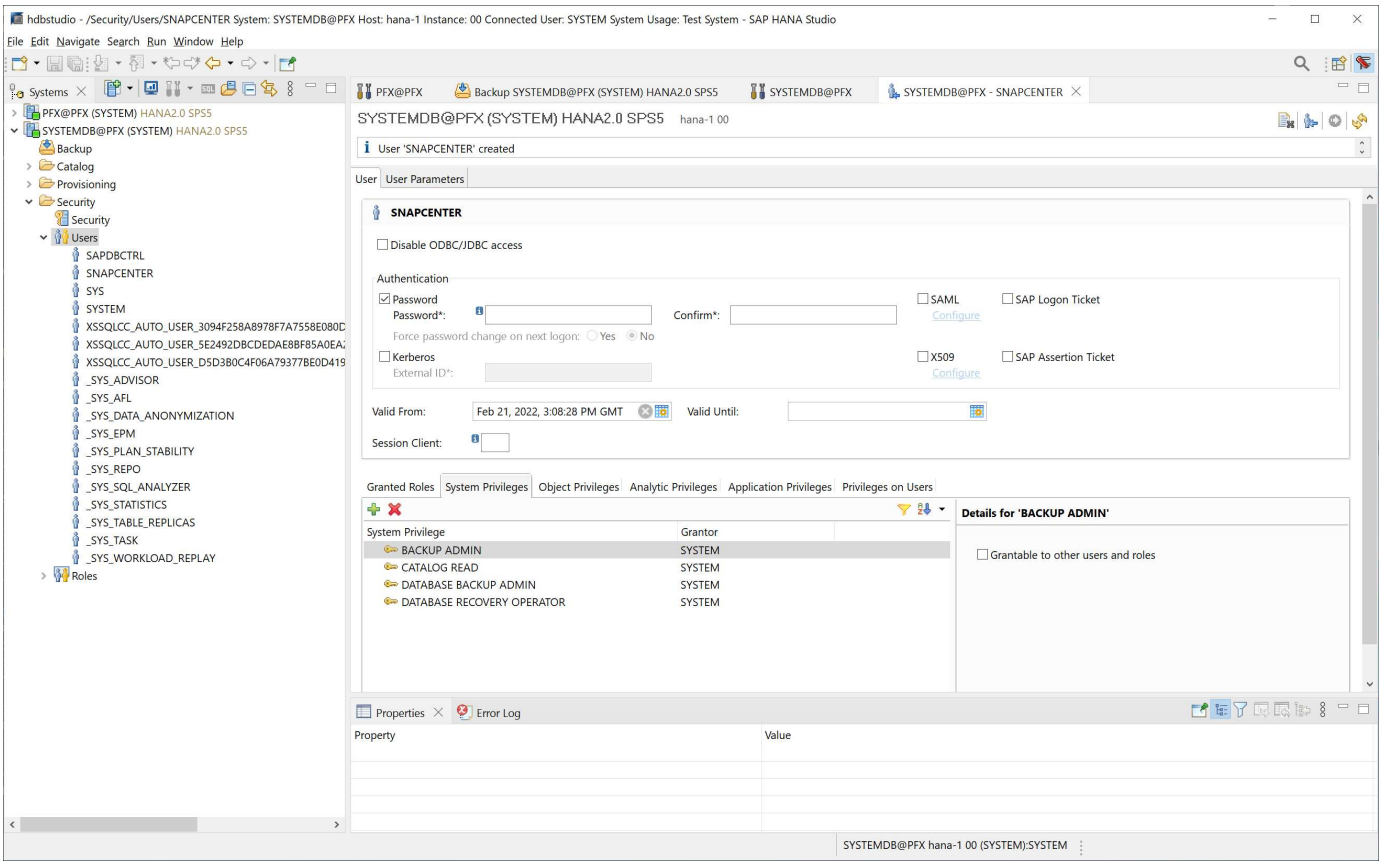
SAP HANA Backup-Benutzer und hdbuserstore-Konfiguration

NetApp empfiehlt, einen dedizierten Datenbankbenutzer in der HANA Datenbank zu konfigurieren, um Backup-Vorgänge mit SnapCenter auszuführen. Im zweiten Schritt wird für diesen Backup-Benutzer ein SAP HANA User Store Key konfiguriert und dieser User Store Key wird bei der Konfiguration des SnapCenter SAP HANA Plug-ins verwendet.

Die folgende Abbildung zeigt das SAP HANA Studio, über das Sie den Backup-Benutzer erstellen können

Die erforderlichen Berechtigungen werden mit HANA 2.0 SPS5 Version geändert: Backup-Admin, Lesevorgang im Katalog, Datenbank-Backup-Administrator und Datenbank-Recovery-Operator. Für ältere Versionen reichen der Backup-Administrator und der Lesevorgang des Katalogs aus.

Für ein SAP HANA MDC-System müssen Sie den Benutzer in der Systemdatenbank erstellen, da alle Backup-Befehle für das System und die Mandantendatenbanken über die Systemdatenbank ausgeführt werden.



Der folgende Befehl wird für die Konfiguration des Benutzerspeichers mit dem verwendet `<sid>adm` Benutzer:

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

SnapCenter verwendet das `<sid>adm` Benutzer zur Kommunikation mit der HANA-Datenbank. Daher müssen Sie den User Store Key mit dem <`sid>adm` Benutzer auf dem Datenbank-Host konfigurieren. In der Regel wird die SAP HANA hdbsql-Client-Software zusammen mit der Datenbank-Server-Installation installiert. Wenn dies nicht der Fall ist, müssen Sie zuerst den hdbclient installieren.

In einer SAP HANA MDC-Einrichtung, Port `3<instanceNo>13` Ist der Standard-Port für den SQL-Zugriff auf die Systemdatenbank und muss in der hdbuserstore-Konfiguration verwendet werden.

Für eine SAP HANA Einrichtung mit mehreren Hosts müssen Sie die Benutzerspeicherschlüssel für alle Hosts konfigurieren. SnapCenter versucht, über jeden der angegebenen Schlüssel eine Verbindung zur Datenbank herzustellen und kann somit unabhängig vom Failover eines SAP HANA Service zu einem anderen Host funktionieren. In unserem Labor-Setup haben wir einen User Store Key für den Benutzer konfiguriert `pfxadm` Für unser System PFX, ein einziges HANA MDC-Host-System mit einem einzelnen Mandanten.

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

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

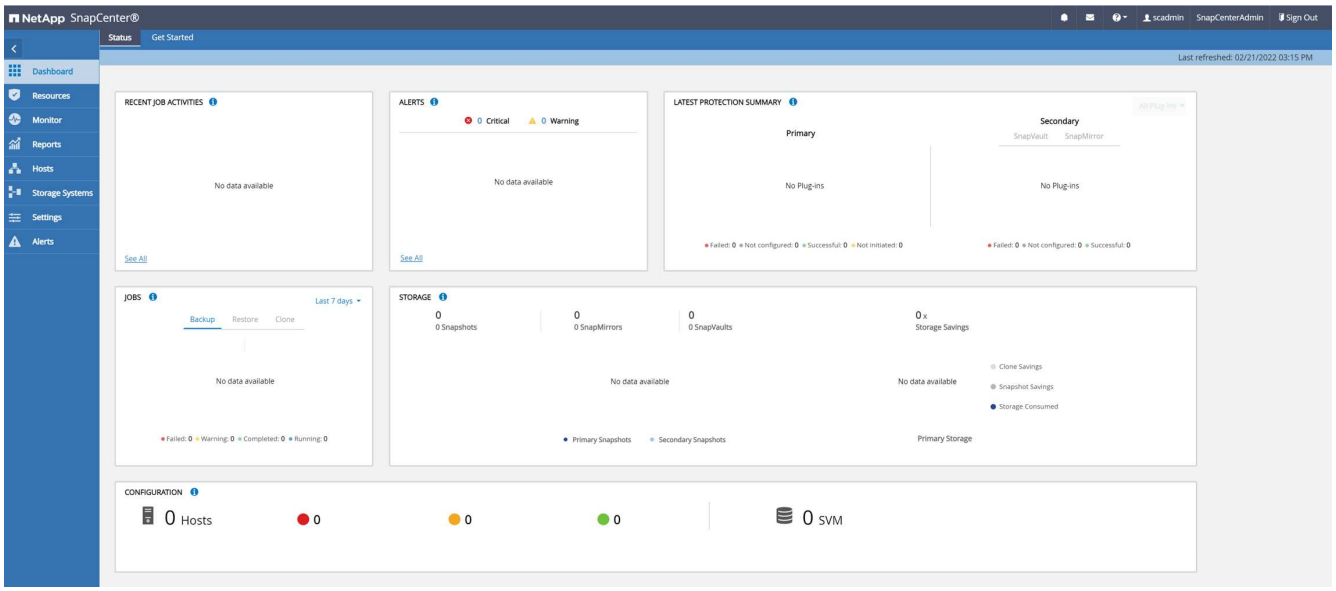
Sie können den Zugriff auf die HANA-Systemdatenbank prüfen, die den Schlüssel mit dem verwendet `hdbsql` Befehl.

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

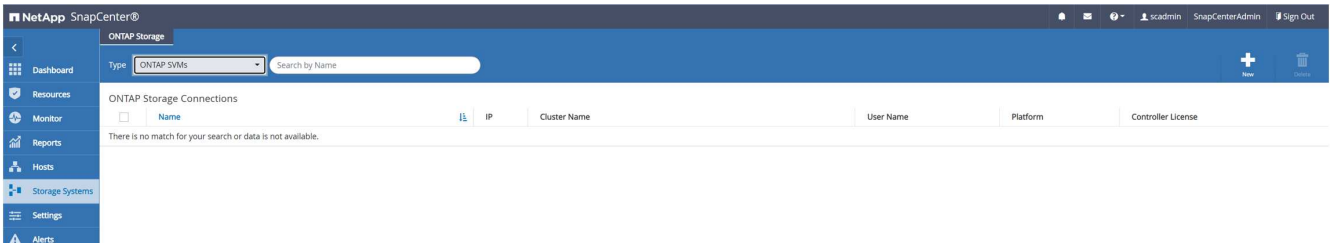
Speicher konfigurieren

Führen Sie diese Schritte aus, um Storage in SnapCenter zu konfigurieren.

1. Wählen Sie in der SnapCenter-Benutzeroberfläche Storage-Systeme aus.

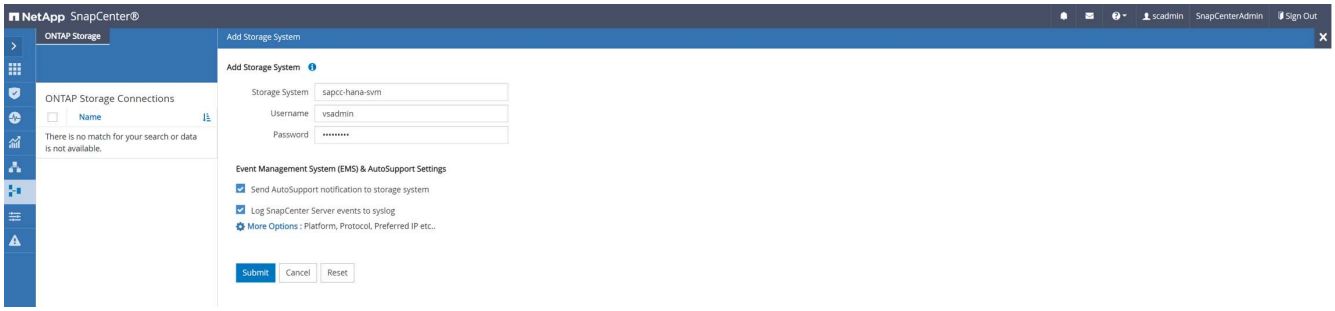


Sie können den Storage-Systemtyp auswählen, der ONTAP SVMs oder ONTAP Cluster sein kann. Im folgenden Beispiel ist das SVM-Management ausgewählt.

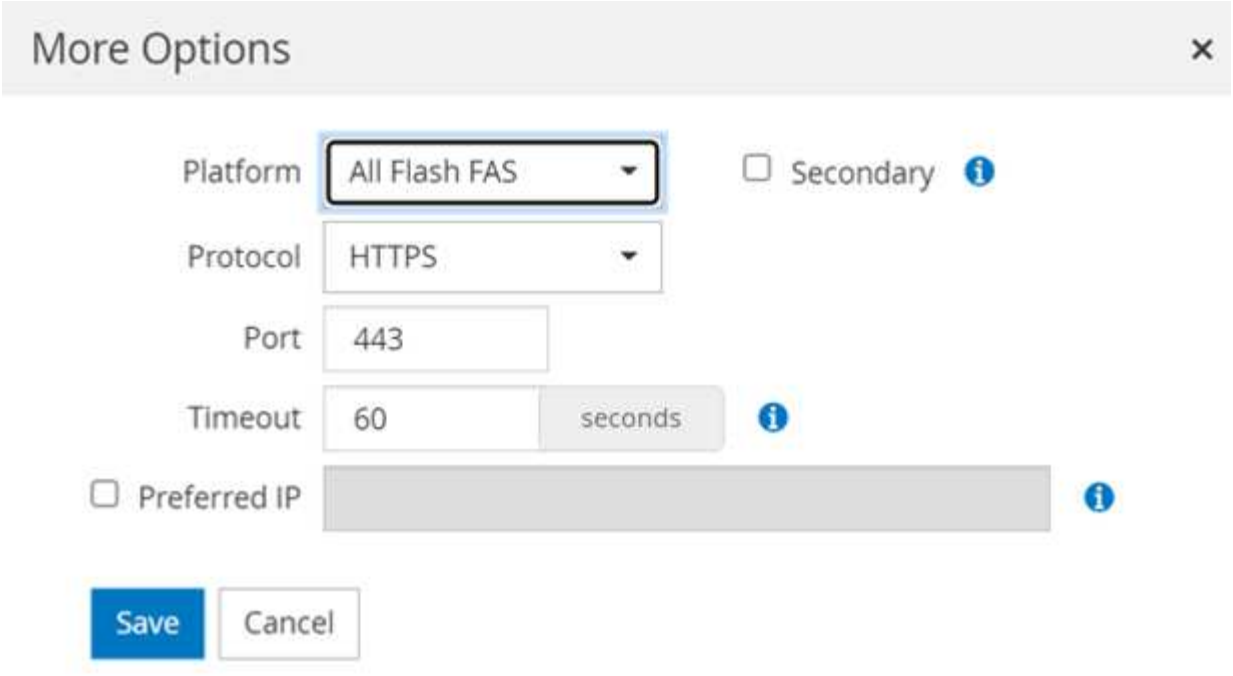


2. Klicken Sie auf Neu, um ein Speichersystem hinzuzufügen und den erforderlichen Hostnamen und die Anmeldeinformationen anzugeben.

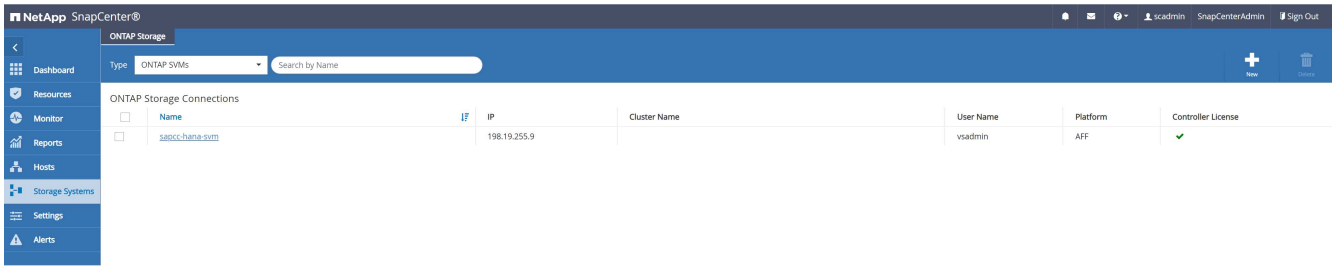
   Der SVM-Benutzer muss nicht wie in der folgenden Abbildung dargestellt vsadmin verwendet werden. In der Regel wird ein Benutzer für die SVM konfiguriert und den erforderlichen Berechtigungen zum Ausführen von Backup- und Restore-Vorgängen zugewiesen. Informationen zu erforderlichen Berechtigungen finden Sie unter "SnapCenter Installationshandbuch" Im Abschnitt „Minimale ONTAP-Berechtigungen erforderlich“.



3. Klicken Sie zum Konfigurieren der Speicherplattform auf Weitere Optionen.
4. Wählen Sie als Storage-System All-Flash FAS aus, um sicherzustellen, dass die Lizenz, die Teil des FSX für ONTAP ist, für SnapCenter verfügbar ist.



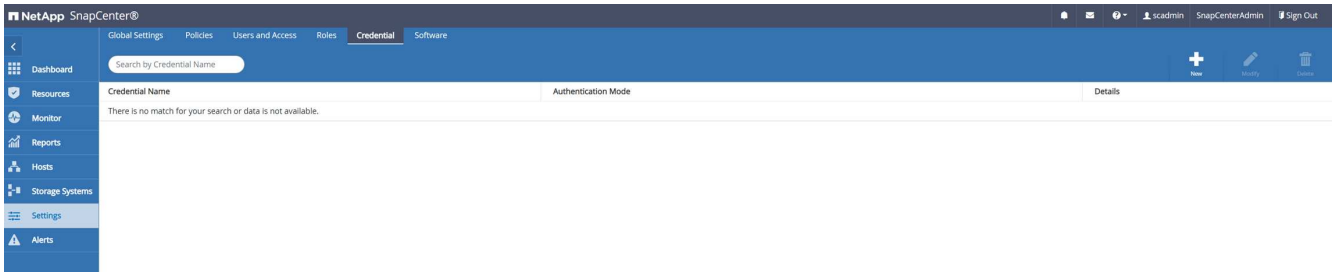
Der SVM `sapcc-hana-svm` Ist jetzt in SnapCenter konfiguriert.



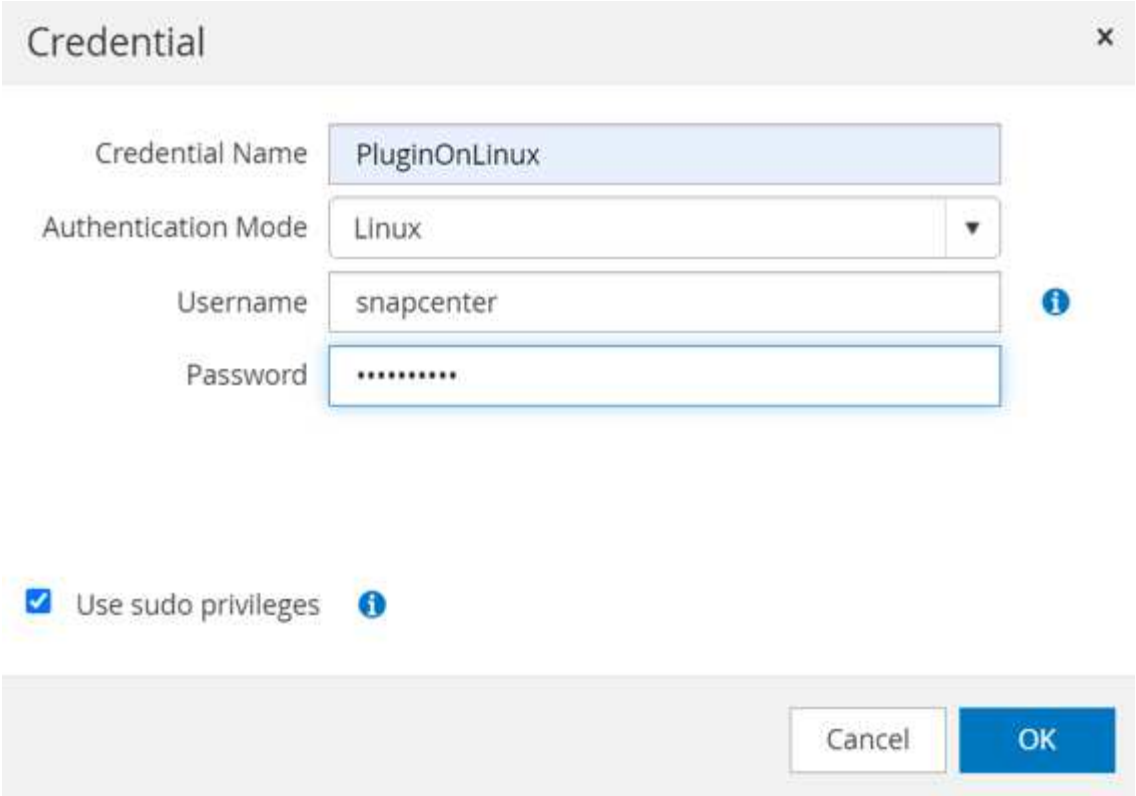
Anmeldedaten für Plug-in-Implementierung erstellen

Damit SnapCenter die erforderlichen Plug-ins auf den HANA-Hosts bereitstellen kann, müssen die Benutzeranmeldeinformationen konfiguriert werden.

1. Gehen Sie zu Einstellungen, wählen Sie Anmeldeinformationen aus, und klicken Sie auf Neu.



2. Im Lab-Setup haben wir einen neuen Benutzer, `snapcenter`, Auf dem HANA-Host, der für die Plug-in-Implementierung verwendet wird. Sie müssen sudo prvileges aktivieren, wie in der folgenden Abbildung dargestellt.




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

Hinzufügen eines SAP HANA-Hosts

Beim Hinzufügen eines SAP HANA-Hosts implementiert SnapCenter die erforderlichen Plug-ins auf dem Datenbank-Host und führt automatische Erkennungsvorgänge aus.

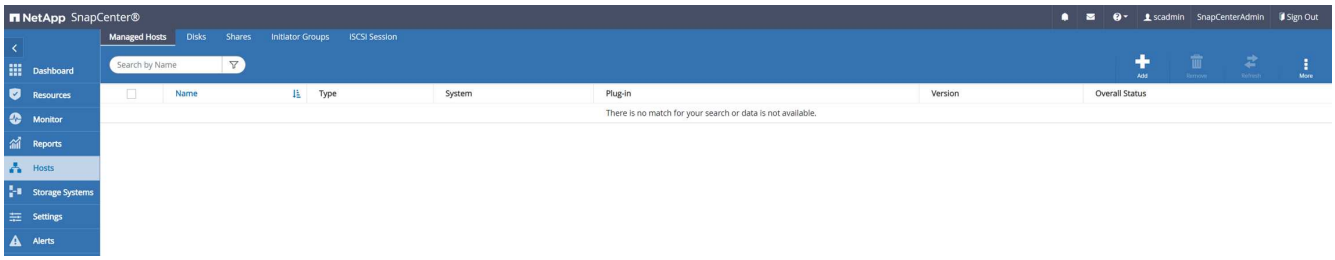
Für das SAP HANA Plug-in ist Java 64-Bit Version 1.8 erforderlich. Java muss auf dem Host installiert sein, bevor der Host zu SnapCenter hinzugefügt wird.

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

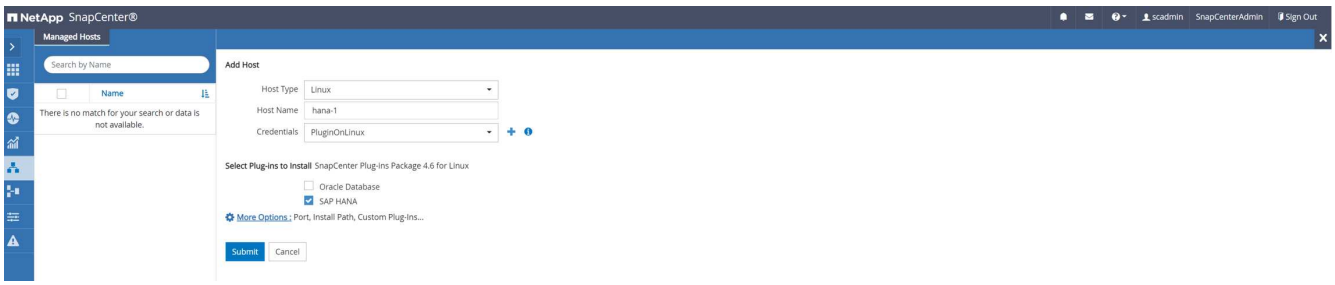
OpenJDK oder Oracle Java wird mit SnapCenter unterstützt.

Gehen Sie wie folgt vor, um den SAP HANA-Host hinzuzufügen:

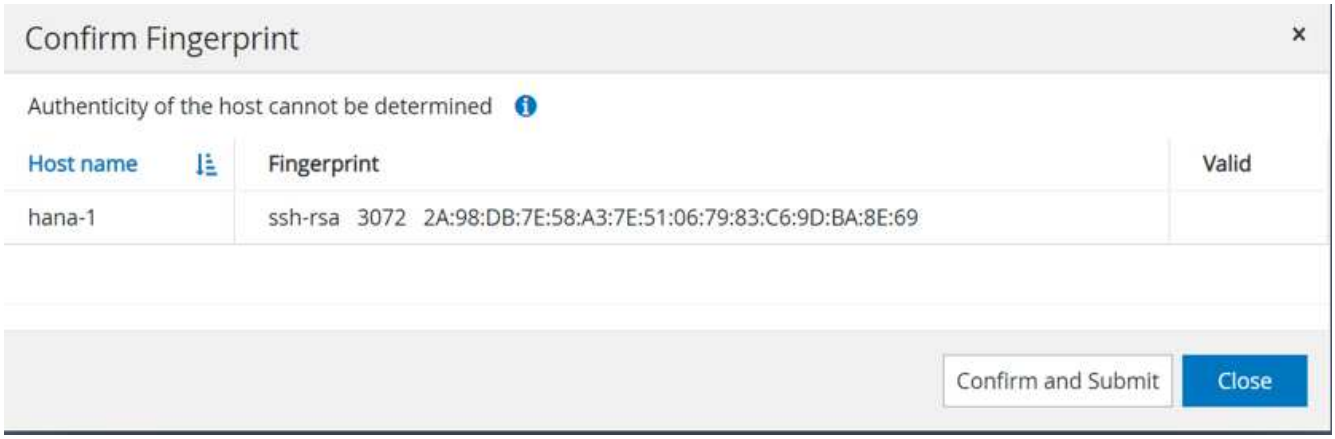
1. Klicken Sie auf der Registerkarte Host auf Hinzufügen.



2. Geben Sie Host-Informationen an, und wählen Sie das zu installierende SAP HANA-Plug-in aus. Klicken Sie Auf Senden.

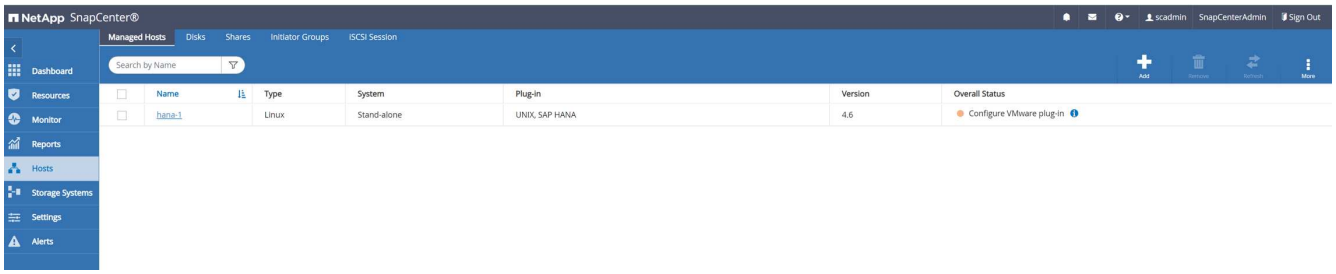


3. Bestätigen Sie den Fingerabdruck.



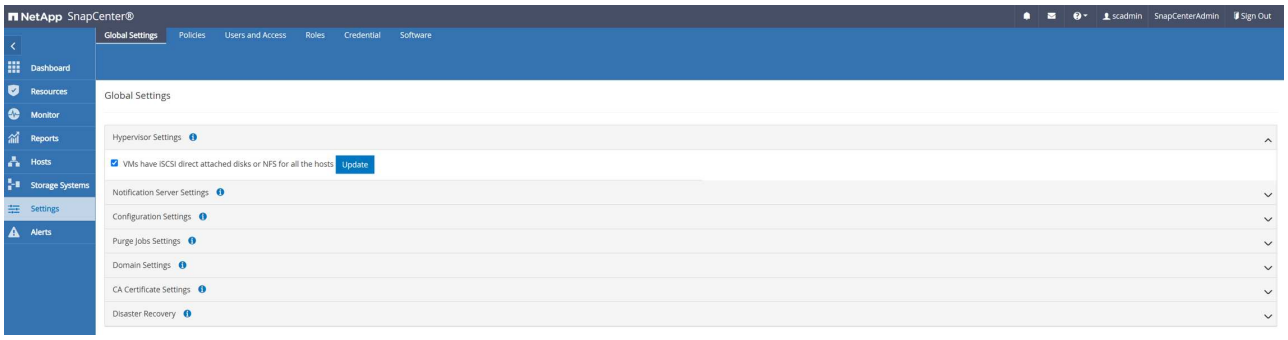
Die Installation des HANA und des Linux Plug-ins wird automatisch gestartet. Nach Abschluss der Installation wird in der Statusspalte des Hosts das VMware Plug-in konfigurieren angezeigt. SnapCenter erkennt, ob das SAP HANA Plug-in in in einer virtualisierten Umgebung installiert ist. Dabei kann es sich um eine VMware Umgebung oder eine Umgebung bei einem Public Cloud-Provider handelt. In diesem Fall zeigt SnapCenter eine Warnung an, um den Hypervisor zu konfigurieren.

Sie können die Warnmeldung mithilfe der folgenden Schritte entfernen.

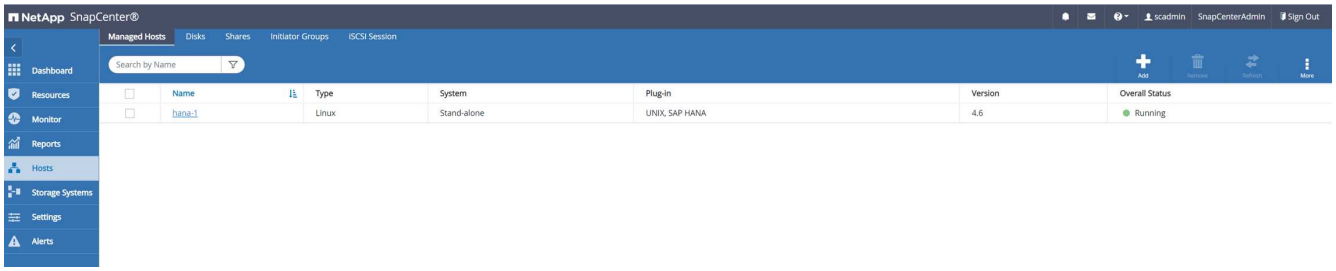


a. Wählen Sie auf der Registerkarte Einstellungen die Option Globale Einstellungen.

b. Wählen Sie für die Hypervisor-Einstellungen die Option VMs mit iSCSI Direct Attached Disks oder NFS für alle Hosts aus, und aktualisieren Sie die Einstellungen.



Der Bildschirm zeigt nun das Linux-Plug-in und das HANA-Plug-in mit dem Status läuft.



Richtlinien konfigurieren

Richtlinien werden normalerweise unabhängig von der Ressource konfiguriert und können von mehreren SAP HANA Datenbanken verwendet werden.

Eine typische Minimalkonfiguration umfasst folgende Richtlinien:

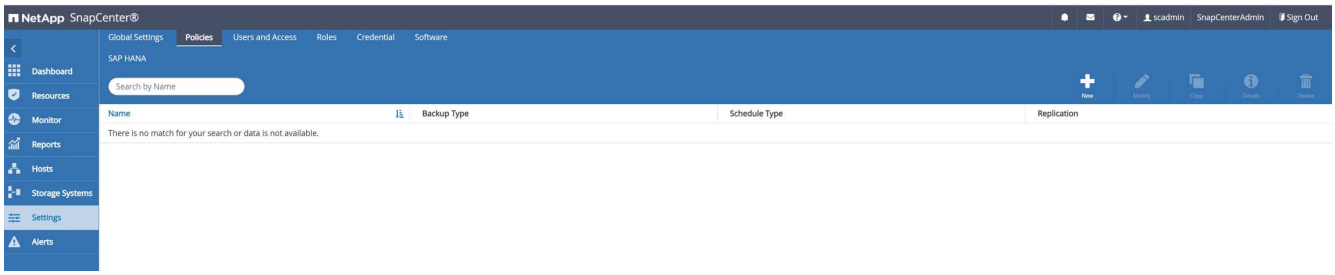
- Richtlinie für stündliche Backups ohne Replikation: `LocalSnap`.
- Richtlinie für wöchentliche Blockintegritätsprüfung über ein dateibasiertes Backup: `BlockIntegrityCheck`.

In den folgenden Abschnitten wird die Konfiguration dieser Richtlinien beschrieben.

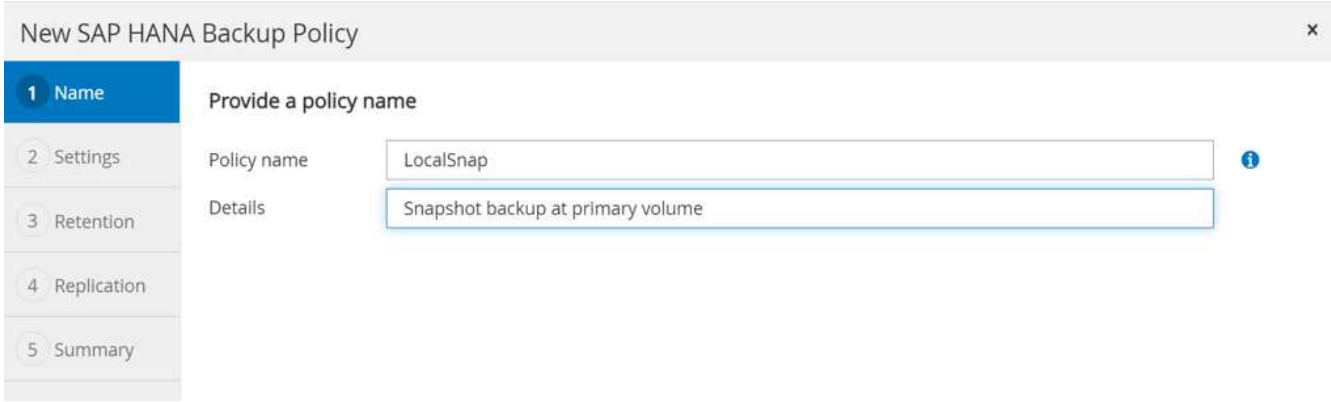
Richtlinien für Snapshot-Backups

Führen Sie diese Schritte aus, um Snapshot Backup-Richtlinien zu konfigurieren.

1. Gehen Sie zu Einstellungen > Richtlinien, und klicken Sie auf Neu.

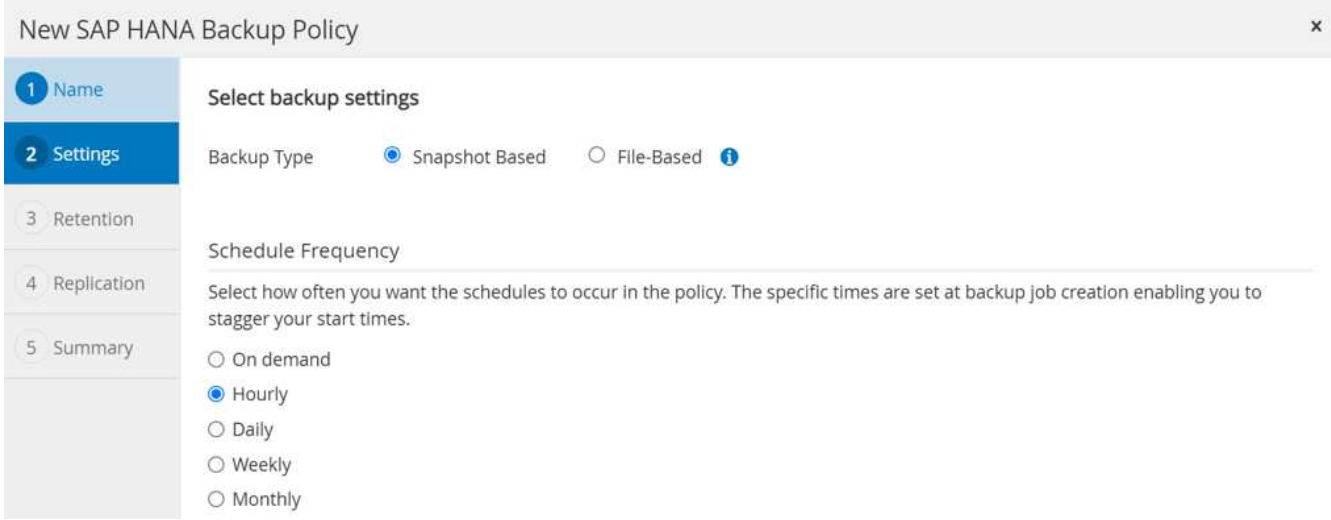


2. Geben Sie den Namen und die Beschreibung der Richtlinie ein. Klicken Sie Auf Weiter.

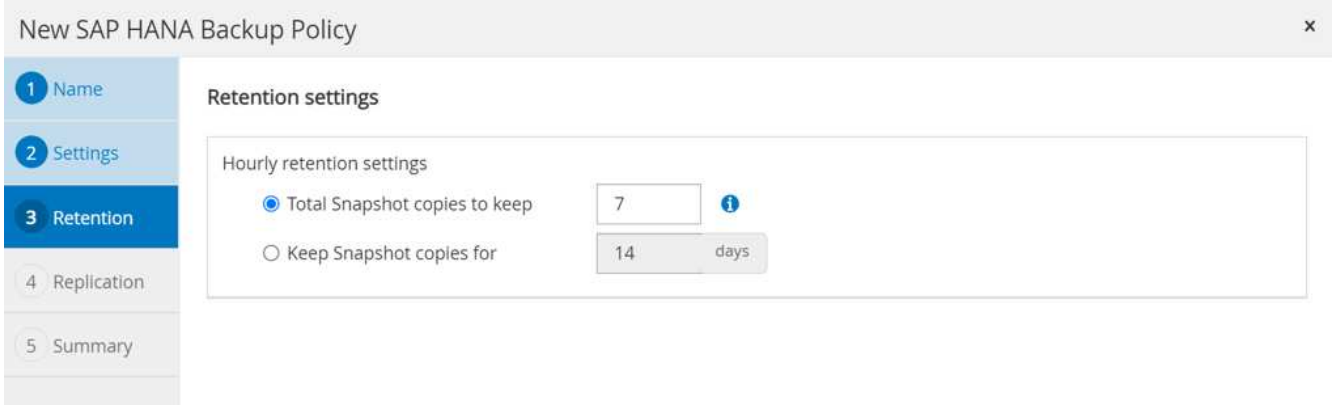


3. Wählen Sie den Backup-Typ als Snapshot-basiert aus und wählen Sie stündlich für die Zeitplanfrequenz aus.

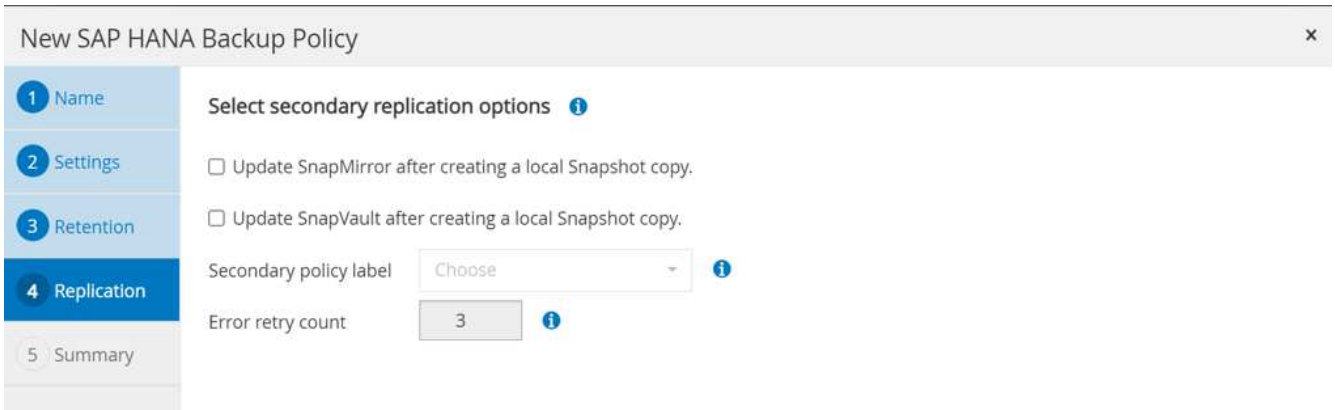
   Der Zeitplan selbst wird später mit der HANA-Ressourcenschutzkonfiguration konfiguriert.

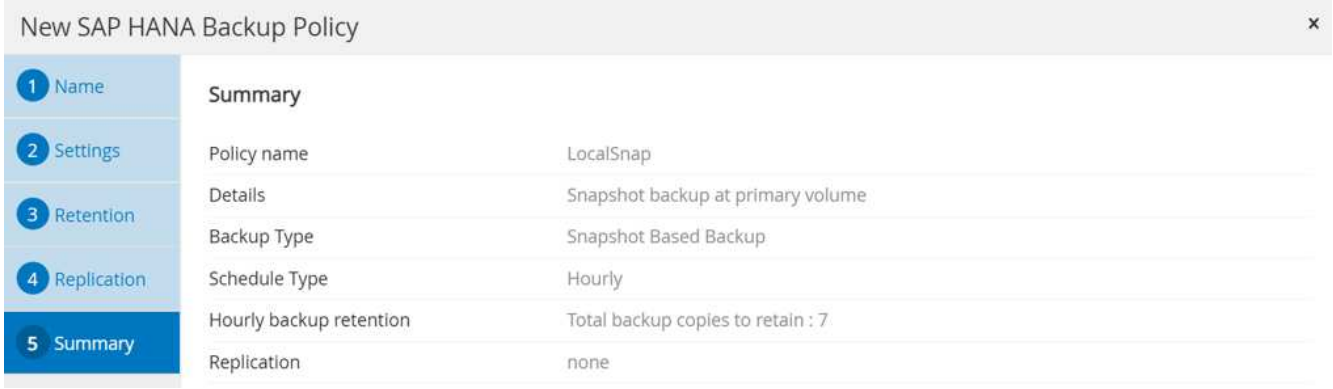


4. Konfigurieren Sie die Aufbewahrungseinstellungen für On-Demand-Backups.

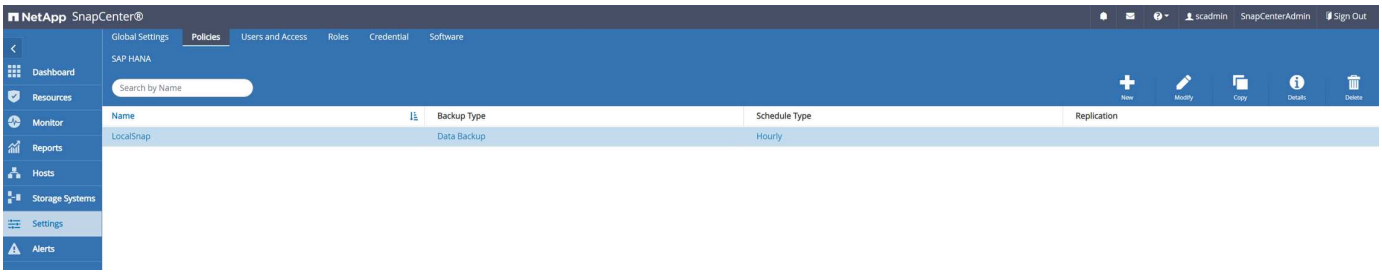


5. Konfigurieren der Replikationsoptionen. In diesem Fall ist kein SnapVault oder SnapMirror Update ausgewählt.





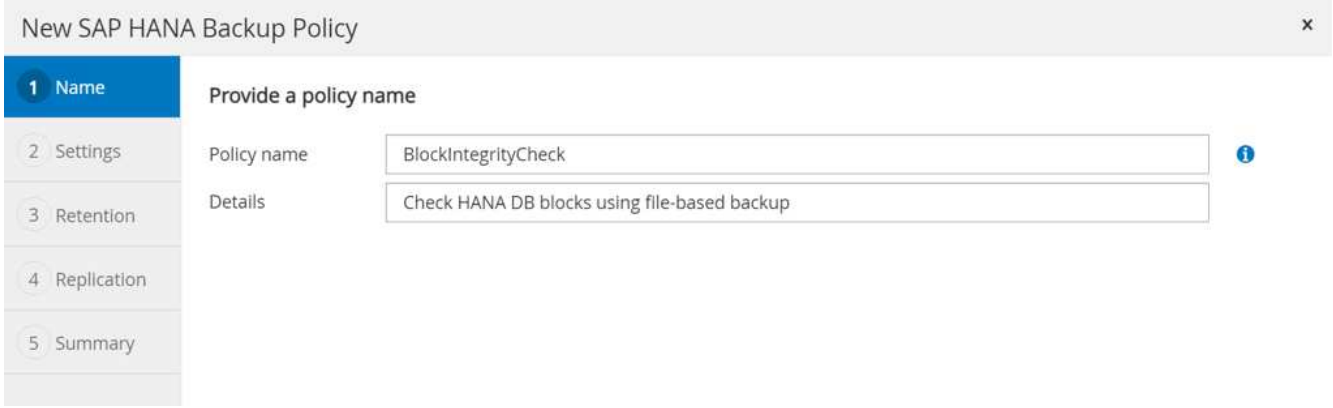
Die neue Richtlinie ist jetzt konfiguriert.



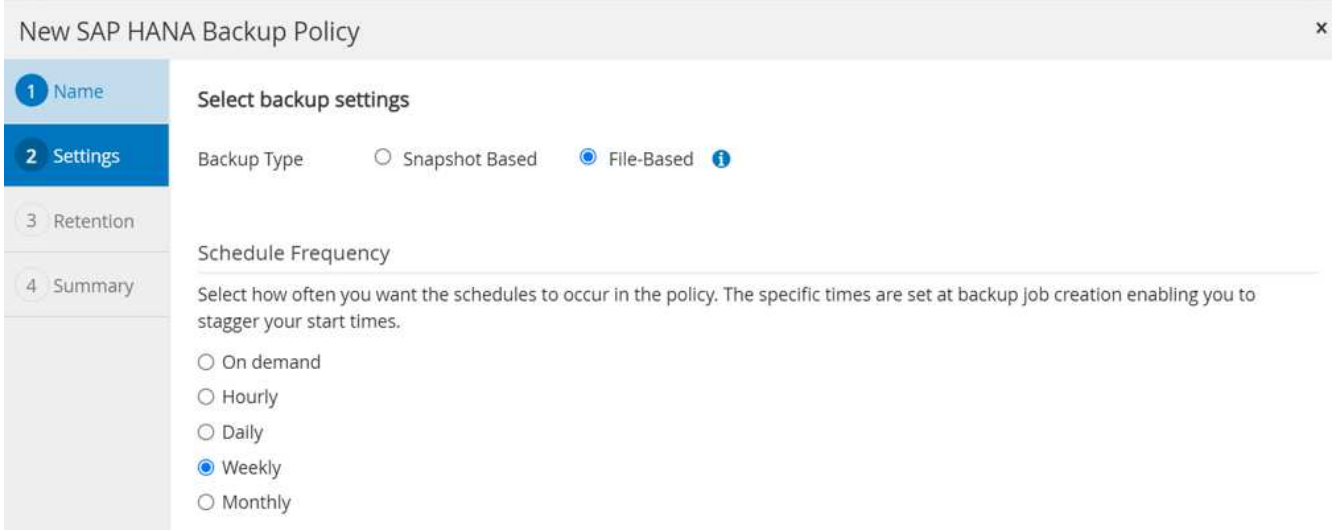
Richtlinie zur Block-Integritätsprüfung

Befolgen Sie diese Schritte, um die Richtlinie zur Integritätsprüfung von Blöcken zu konfigurieren.

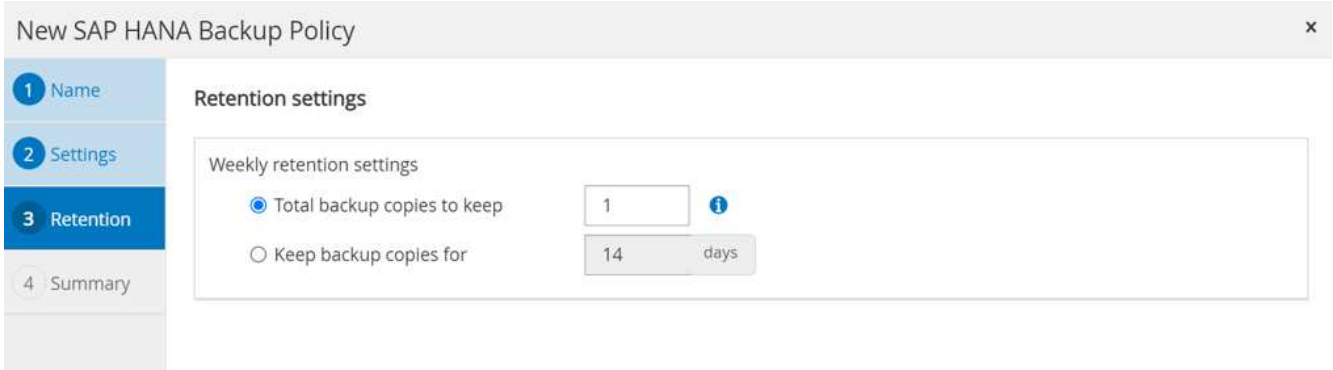
1. Gehen Sie zu Einstellungen > Richtlinien, und klicken Sie auf Neu.
2. Geben Sie den Namen und die Beschreibung der Richtlinie ein. Klicken Sie Auf Weiter.



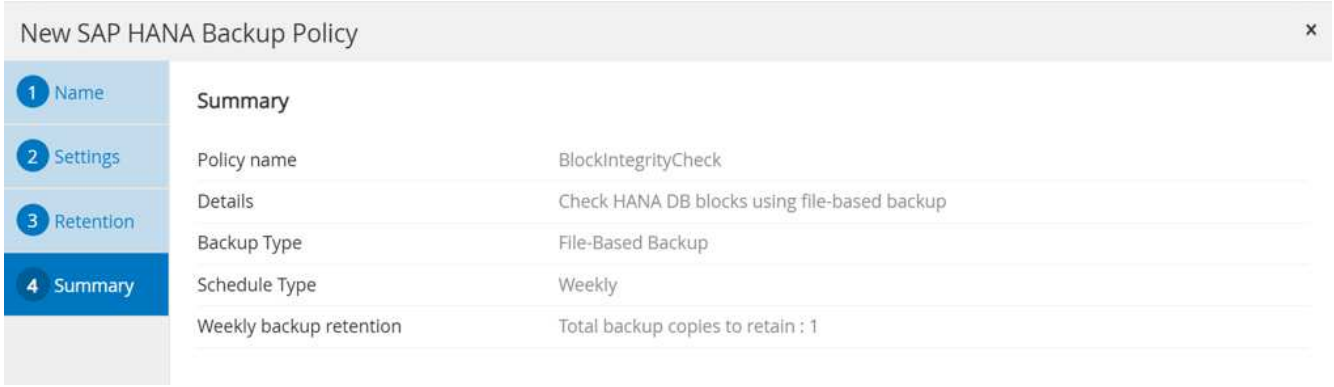
3. Legen Sie den Sicherungstyp auf „File-based“ und „Schedule Frequency“ auf „Weekly“ fest. Der Zeitplan selbst wird später mit der HANA-Ressourcenschutzkonfiguration konfiguriert.

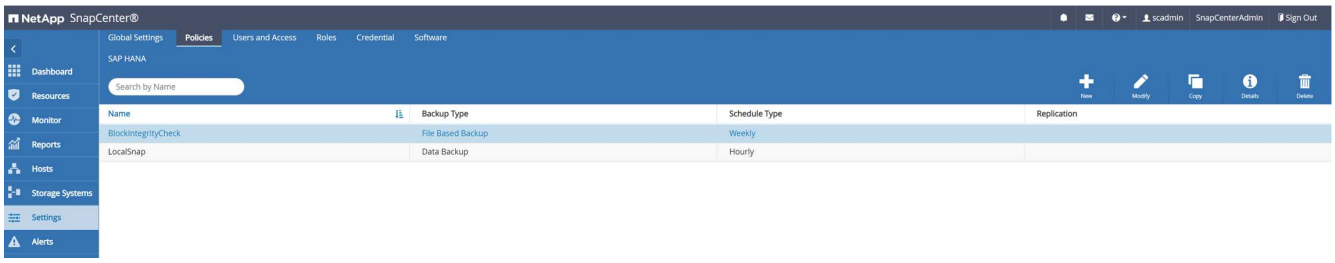


4. Konfigurieren Sie die Aufbewahrungseinstellungen für On-Demand-Backups.



5. Klicken Sie auf der Seite Zusammenfassung auf Fertig stellen.



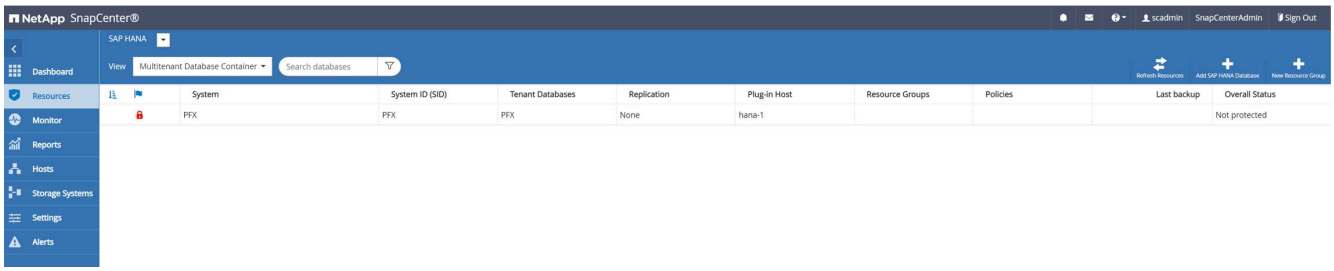


Konfiguration und Sicherung einer HANA-Ressource

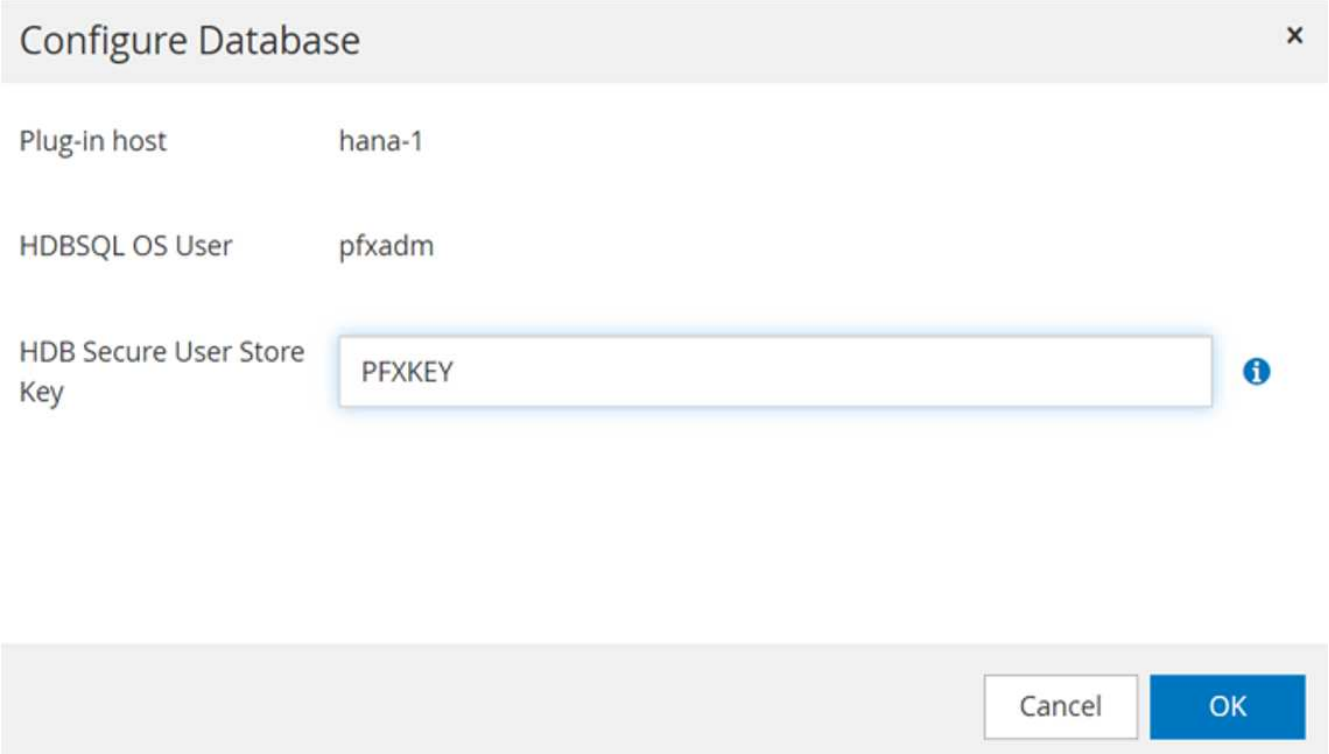
Nach der Plug-in-Installation startet der automatische Erkennungsvorgang der HANA-Ressource automatisch. Im Bildschirm Ressourcen wird eine neue Ressource erstellt, die mit dem roten Vorhängeschloss-Symbol als gesperrt markiert ist. Gehen Sie wie folgt vor, um die neue HANA-Ressource zu konfigurieren und zu schützen:

1. Wählen Sie und klicken Sie auf die Ressource, um mit der Konfiguration fortzufahren.

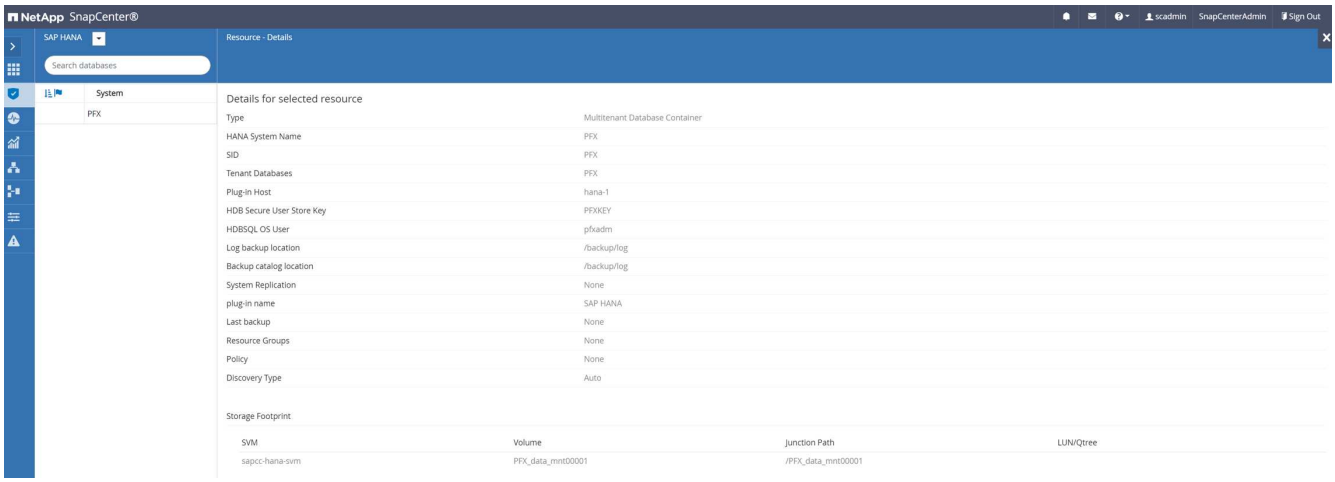
   Sie können den automatischen Erkennungsvorgang auch manuell im Bildschirm Ressourcen auslösen, indem Sie auf Ressourcen aktualisieren klicken.



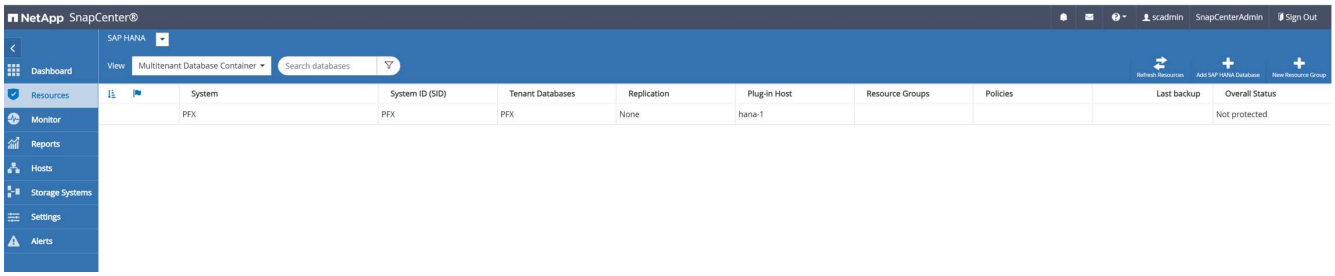
2. Geben Sie den UserStore-Schlüssel für die HANA-Datenbank an.



Der zweite Ebene-Prozess der automatischen Bestandsaufnahme beginnt, bei dem Mandantendaten und Storage-Platzbedarf erfasst werden.

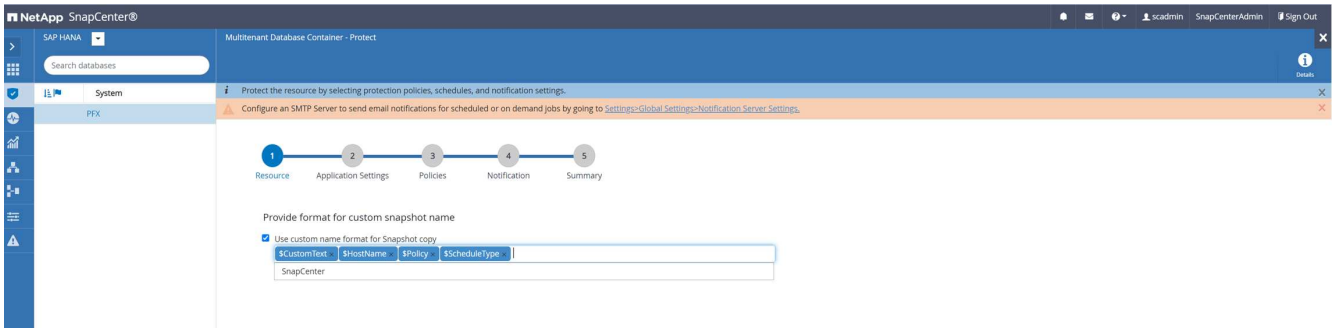


3. Doppelklicken Sie auf der Registerkarte Ressourcen auf die Ressource, um den Ressourcenschutz zu konfigurieren.

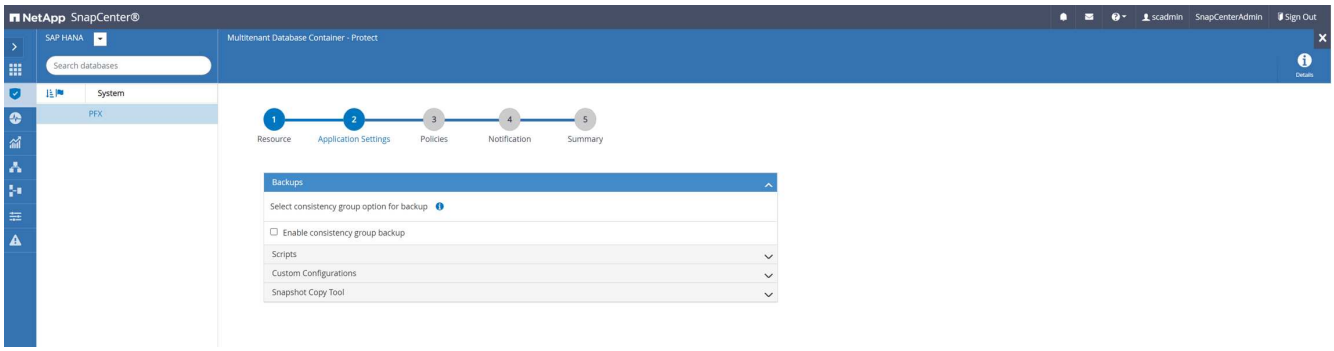


4. Konfigurieren Sie ein benutzerdefiniertes Namensformat für die Snapshot Kopie.

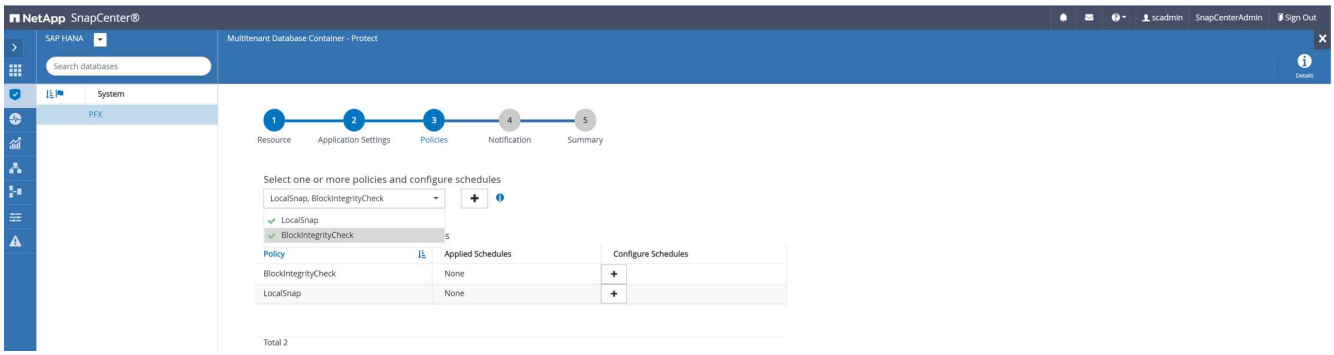
NetApp empfiehlt den Einsatz einer benutzerdefinierten Snapshot Kopie, um schnell ermitteln zu können, mit welcher Richtlinie und welche Zeitplantypen Backups erstellt wurden. Durch Hinzufügen des Zeitplantyps zum Namen der Snapshot Kopie können Sie zwischen geplanten und On-Demand-Backups unterscheiden. Der `schedule name` String für On-Demand-Backups ist leer, während geplante Backups den String enthalten `Hourly`, `Daily`, `or Weekly`.



5. Auf der Seite „Anwendungseinstellungen“ müssen keine spezifischen Einstellungen vorgenommen werden. Klicken Sie Auf Weiter.

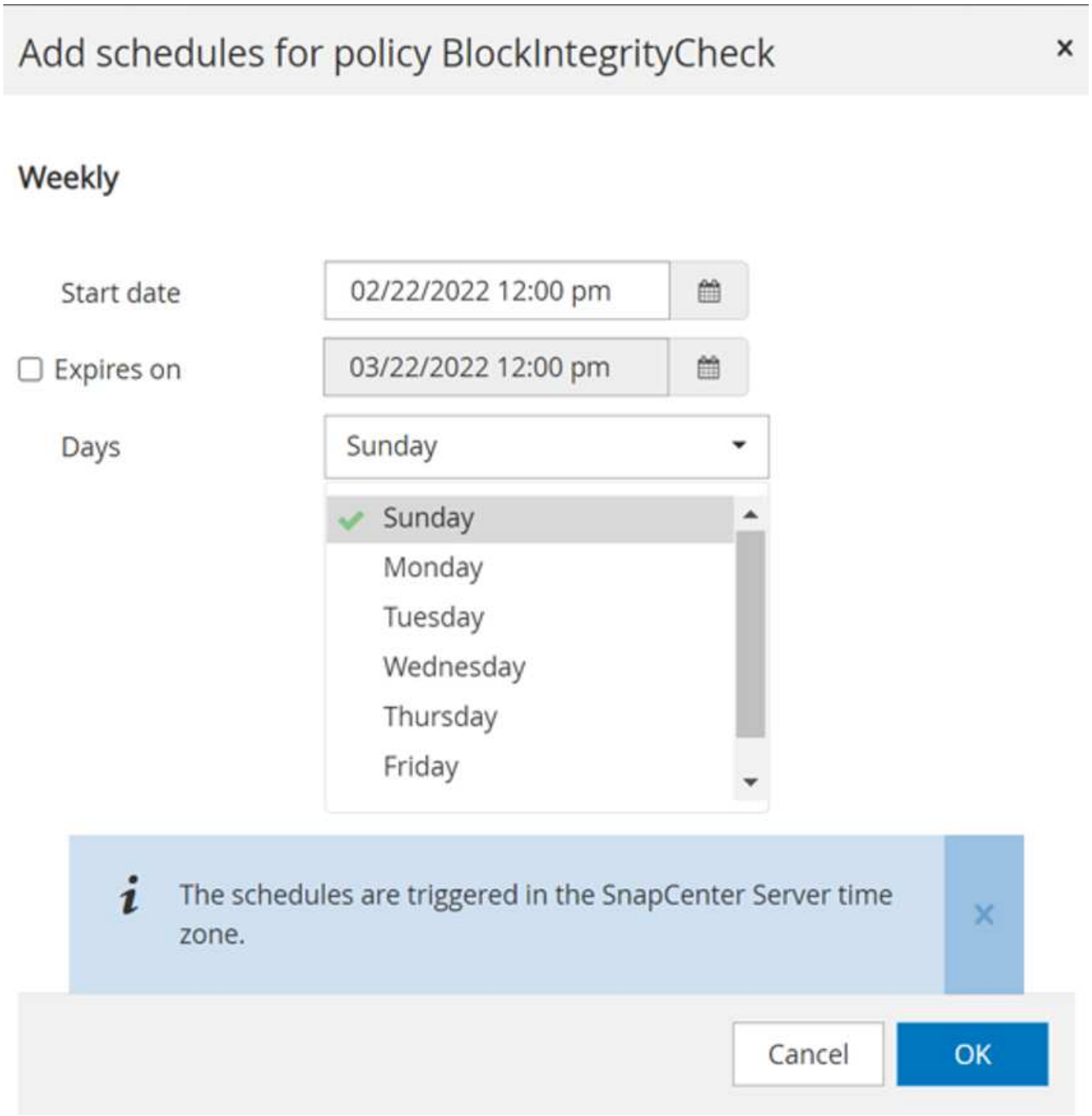


6. Wählen Sie die Richtlinien aus, die der Ressource hinzugefügt werden sollen.



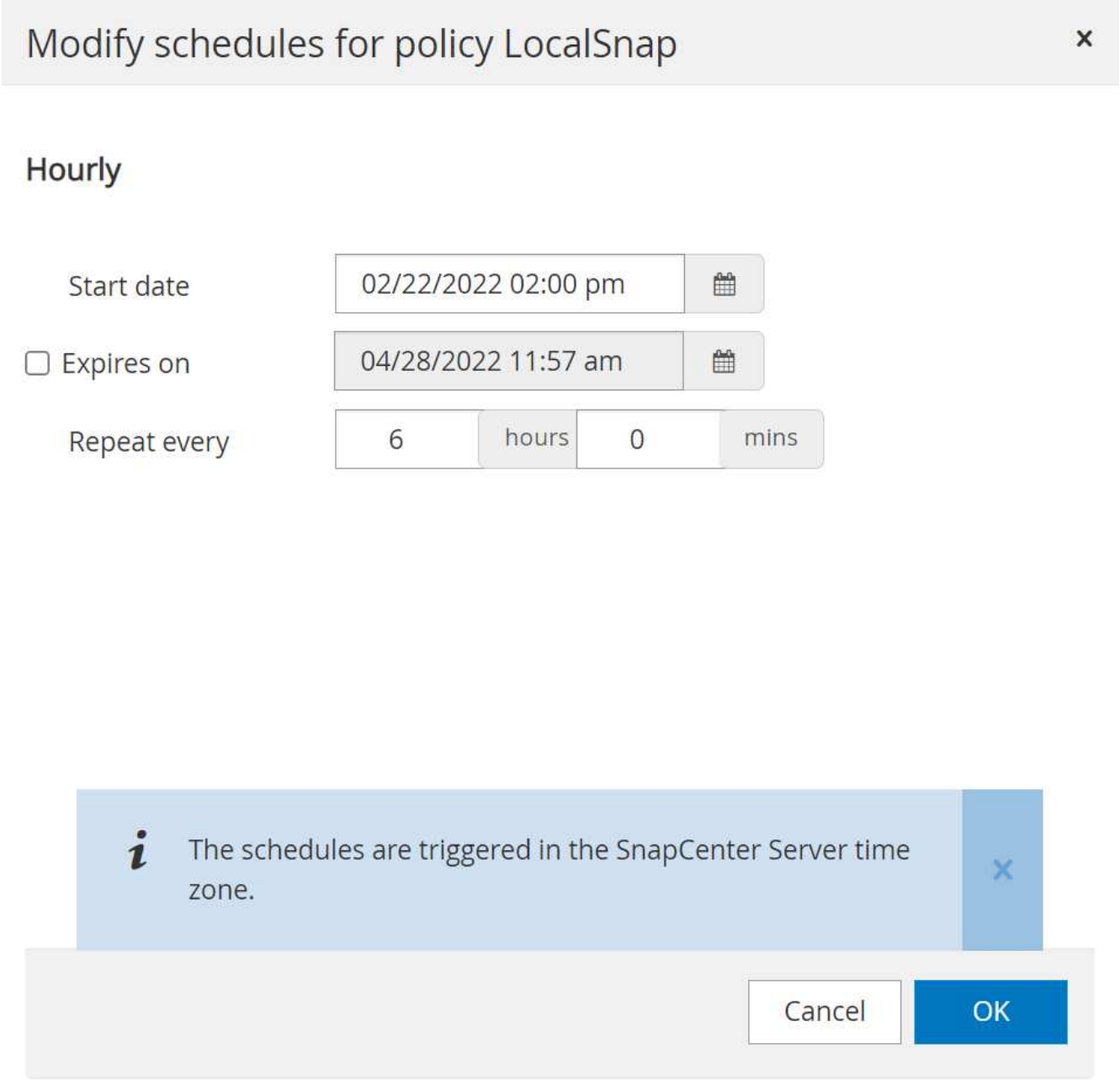
7. Legen Sie den Zeitplan für die Richtlinie zur Integritätsprüfung der Blöcke fest.

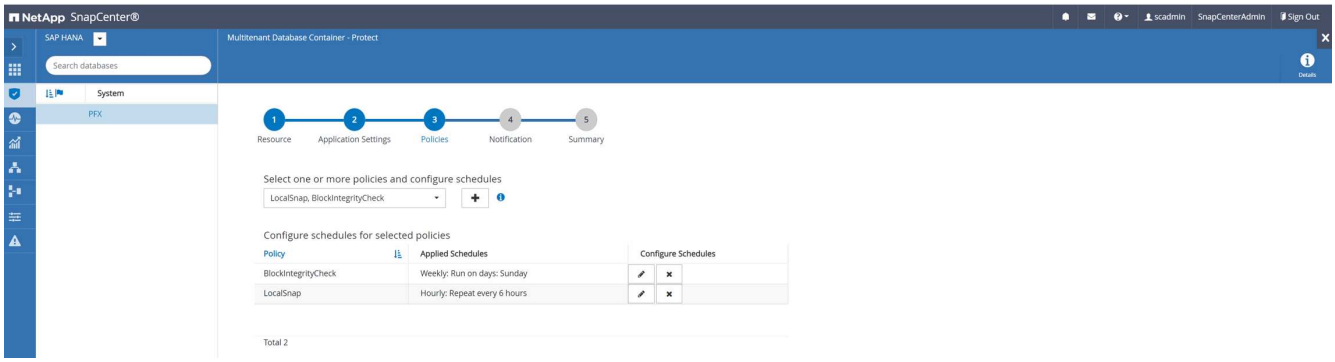
   In diesem Beispiel wird sie für einmal pro Woche festgelegt.



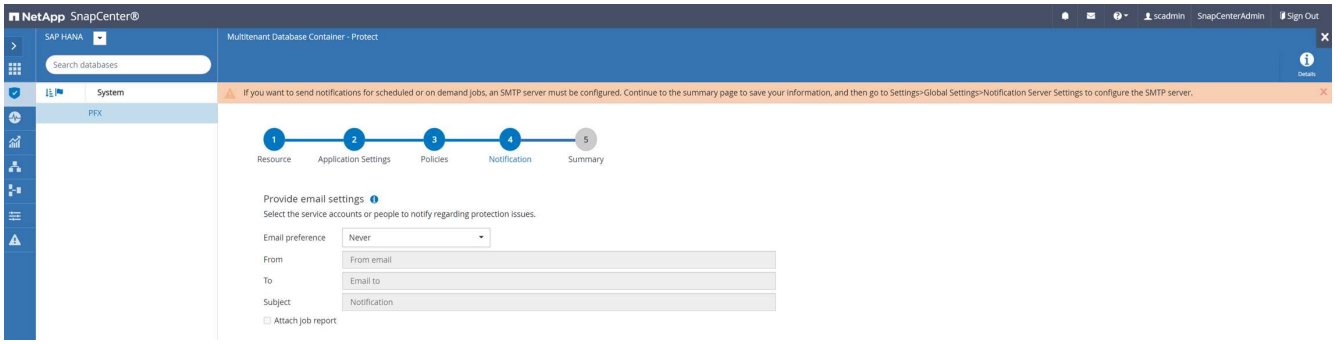
8. Legen Sie den Zeitplan für die lokale Snapshot-Richtlinie fest.

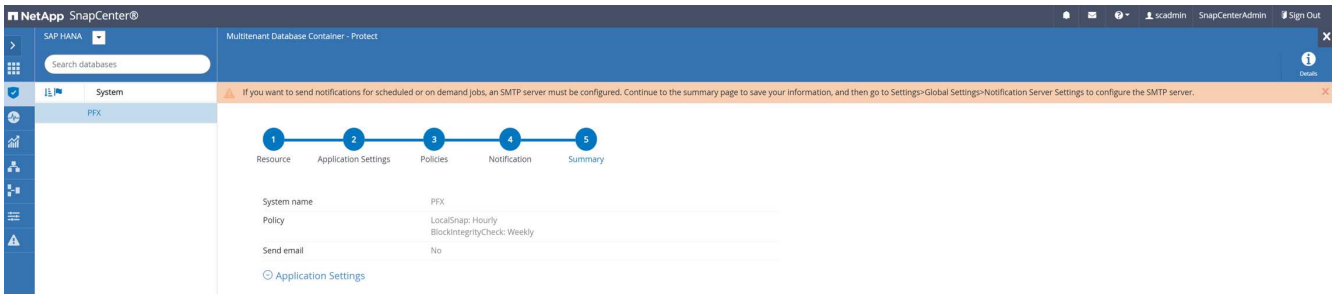
   In diesem Beispiel wird die Einstellung alle 6 Stunden durchgeführt.



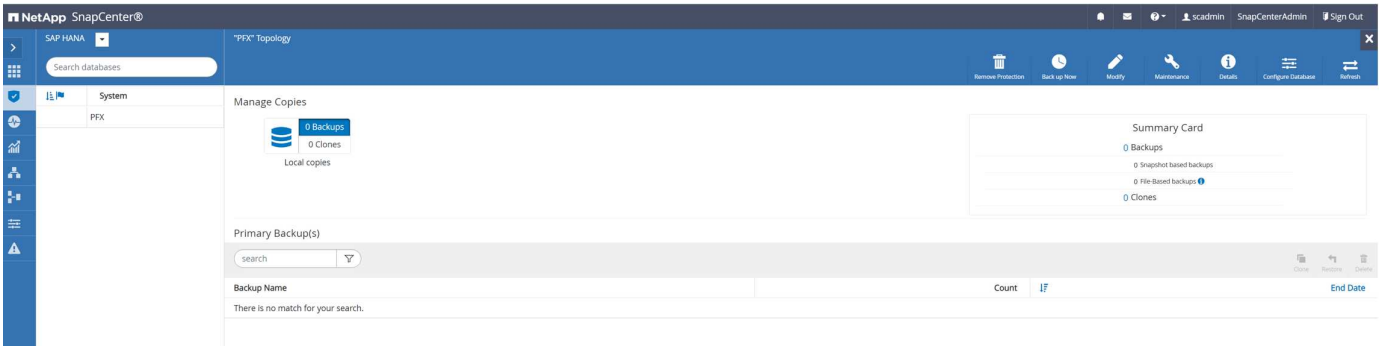


9. Geben Sie Informationen zur E-Mail-Benachrichtigung an.





Die Konfiguration der HANA-Ressourcen ist jetzt abgeschlossen, und Sie können Backups ausführen.



SnapCenter-Backup-Vorgänge

Sie können ein On-Demand-Snapshot-Backup und eine On-Demand-Blockintegritätsprüfung erstellen.

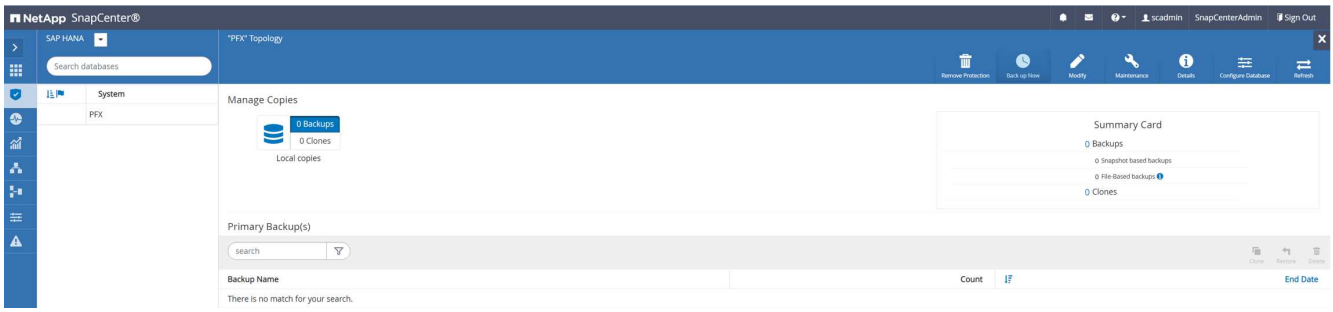
Erstellen Sie ein Snapshot Backup nach Bedarf

Führen Sie die folgenden Schritte aus, um On-Demand Snapshot Backups zu erstellen.

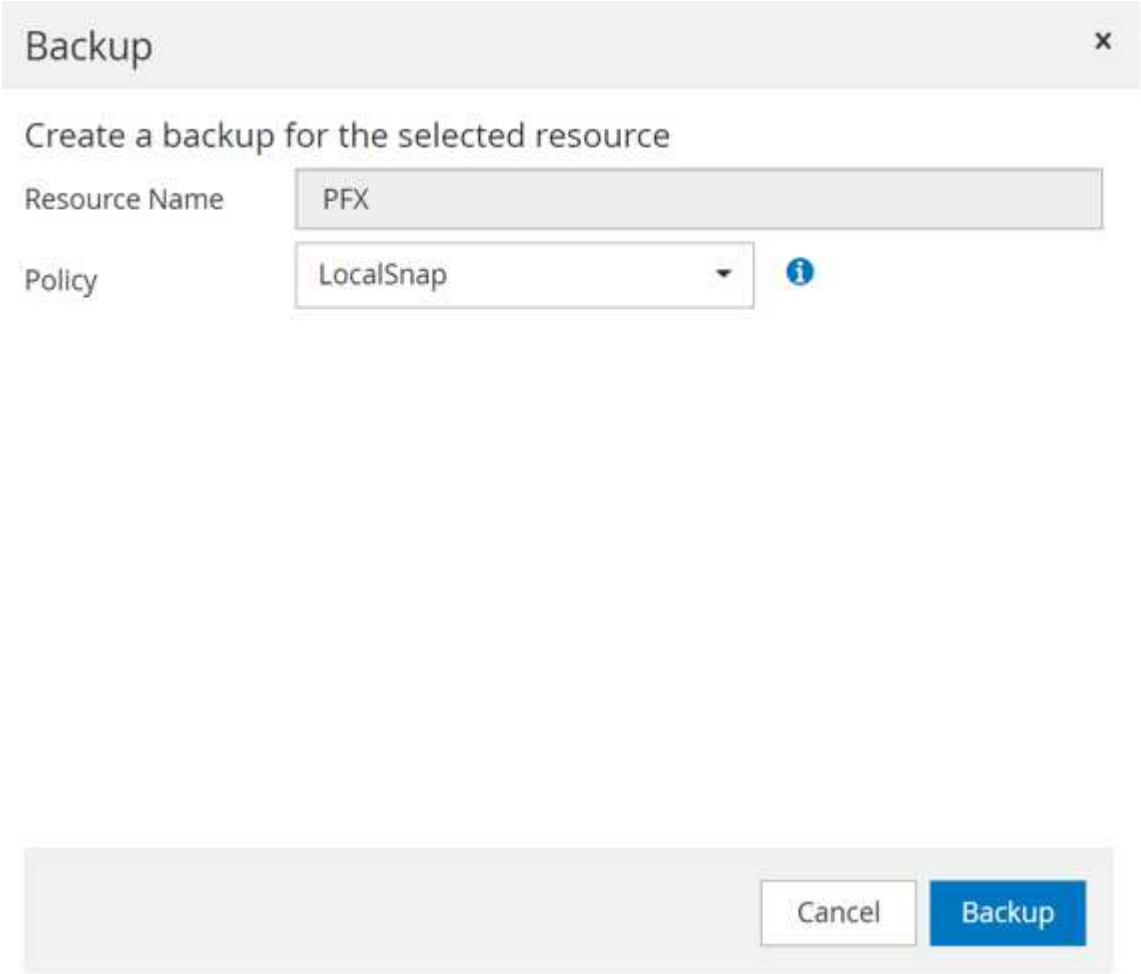
1. Wählen Sie in der Ansicht Ressource die Ressource aus und doppelklicken Sie auf die Zeile, um zur Ansicht Topologie zu wechseln.

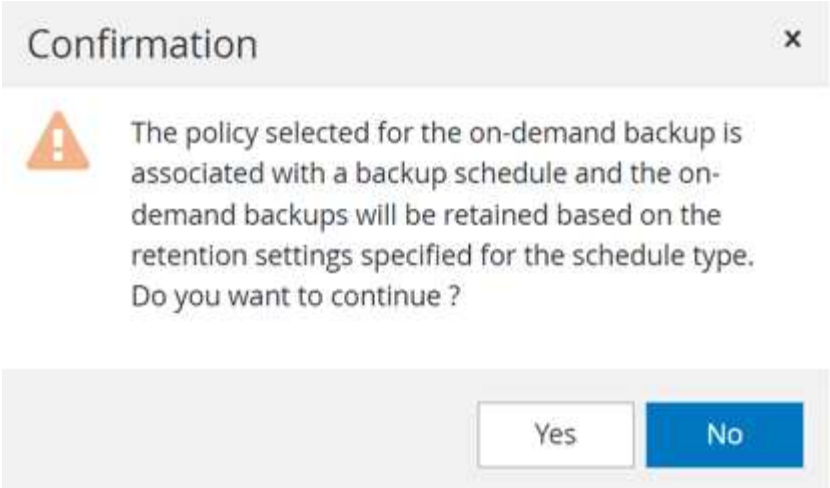
   Die Ansicht RessourcTopologie gibt einen Überblick über alle verfügbaren Backups, die mithilfe von SnapCenter erstellt wurden. Im oberen Bereich dieser Ansicht wird die Backup-Topologie angezeigt, die die Backups des primären Storage (lokale Kopien) und, falls verfügbar, auf dem externen Backup-Storage (Vault-Kopien) anzeigt.

2. Klicken Sie in der oberen Zeile auf das Symbol Jetzt sichern, um ein On-Demand-Backup zu starten.



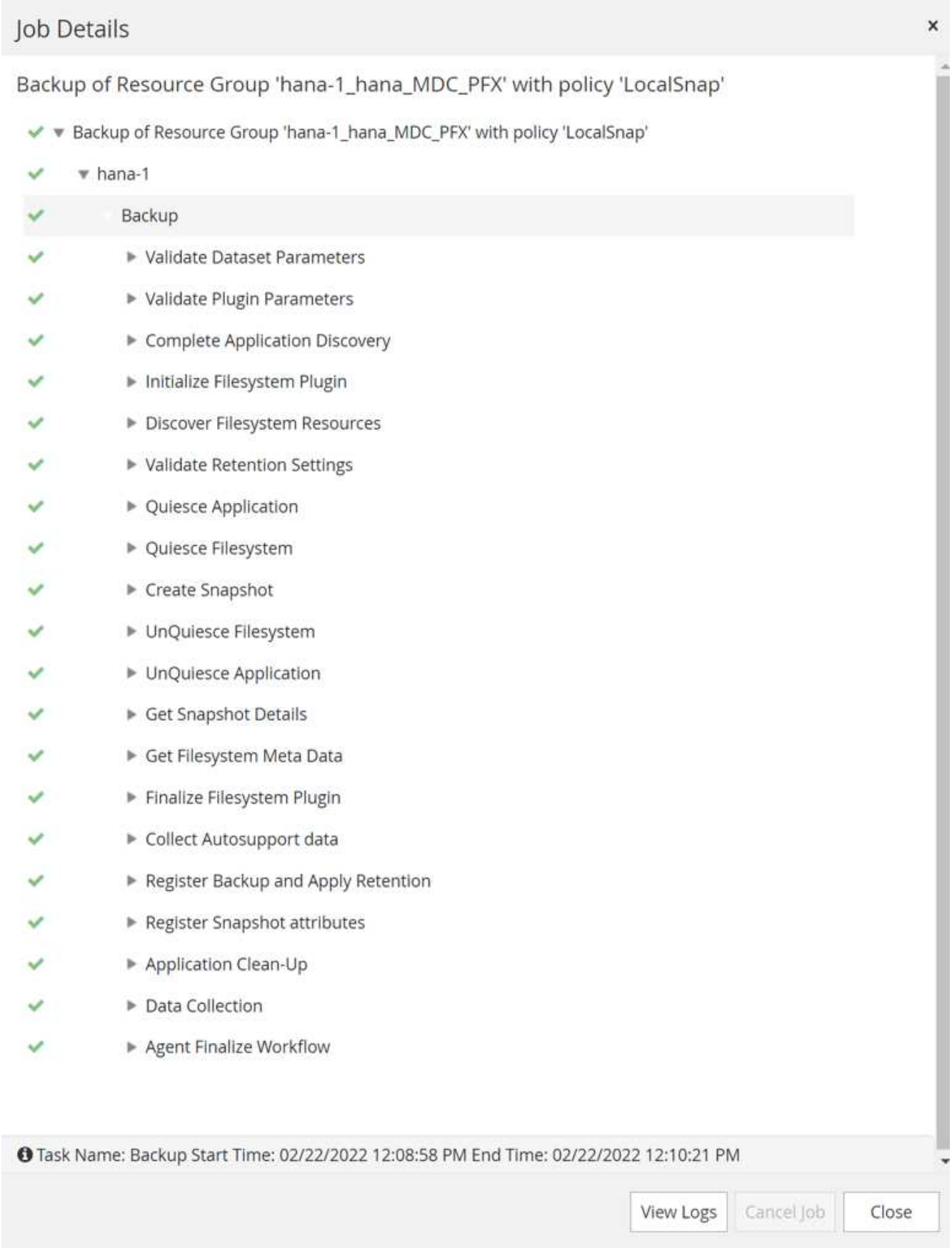
3. Wählen Sie aus der Dropdown-Liste die Backup-Richtlinie aus `LocalSnap`, Und klicken Sie dann auf Backup, um das On-Demand-Backup zu starten.





Ein Protokoll der vorherigen fünf Jobs wird im Aktivitätsbereich unten in der Topologieansicht angezeigt.

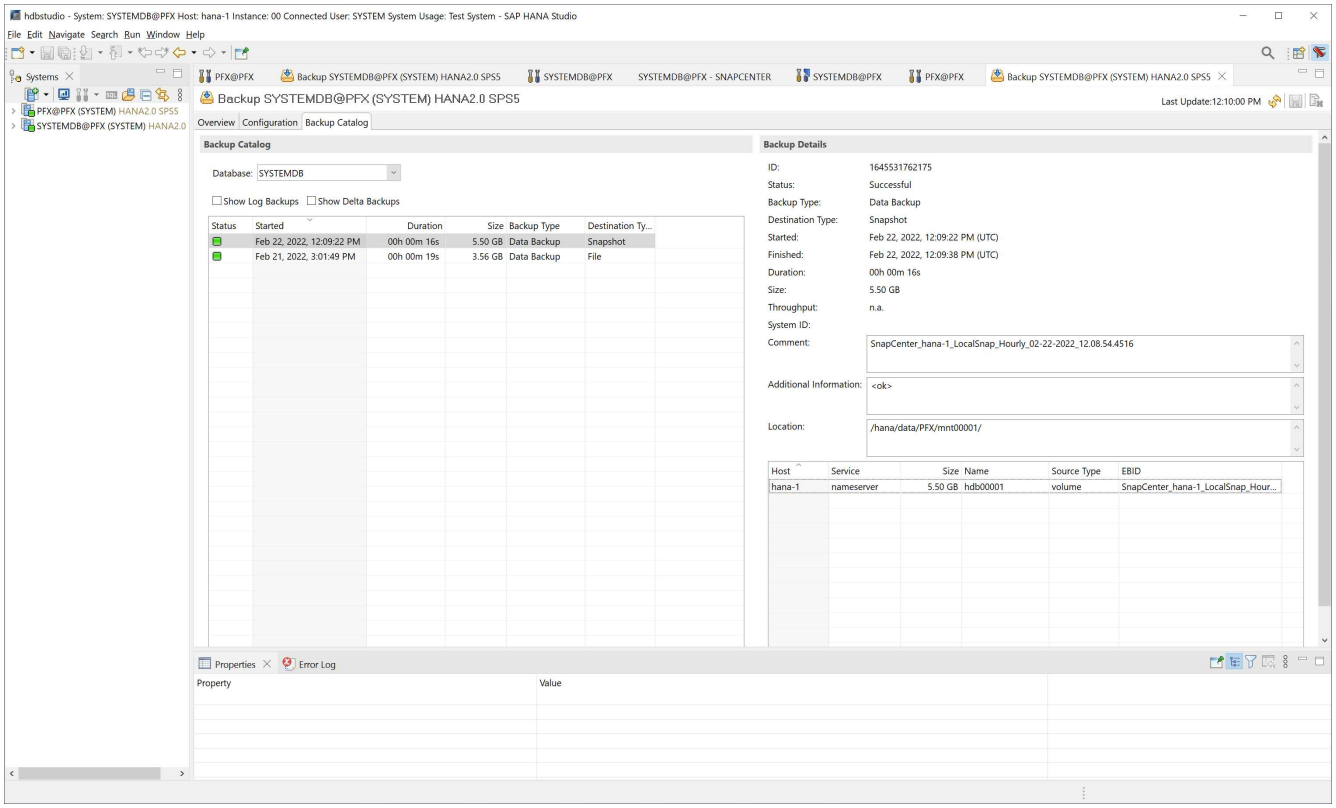
4. Die Jobdetails werden angezeigt, wenn Sie im Aktivitätsbereich auf die Vorgangszeile des Jobs klicken. Sie können ein detailliertes Jobprotokoll öffnen, indem Sie auf Protokolle anzeigen klicken

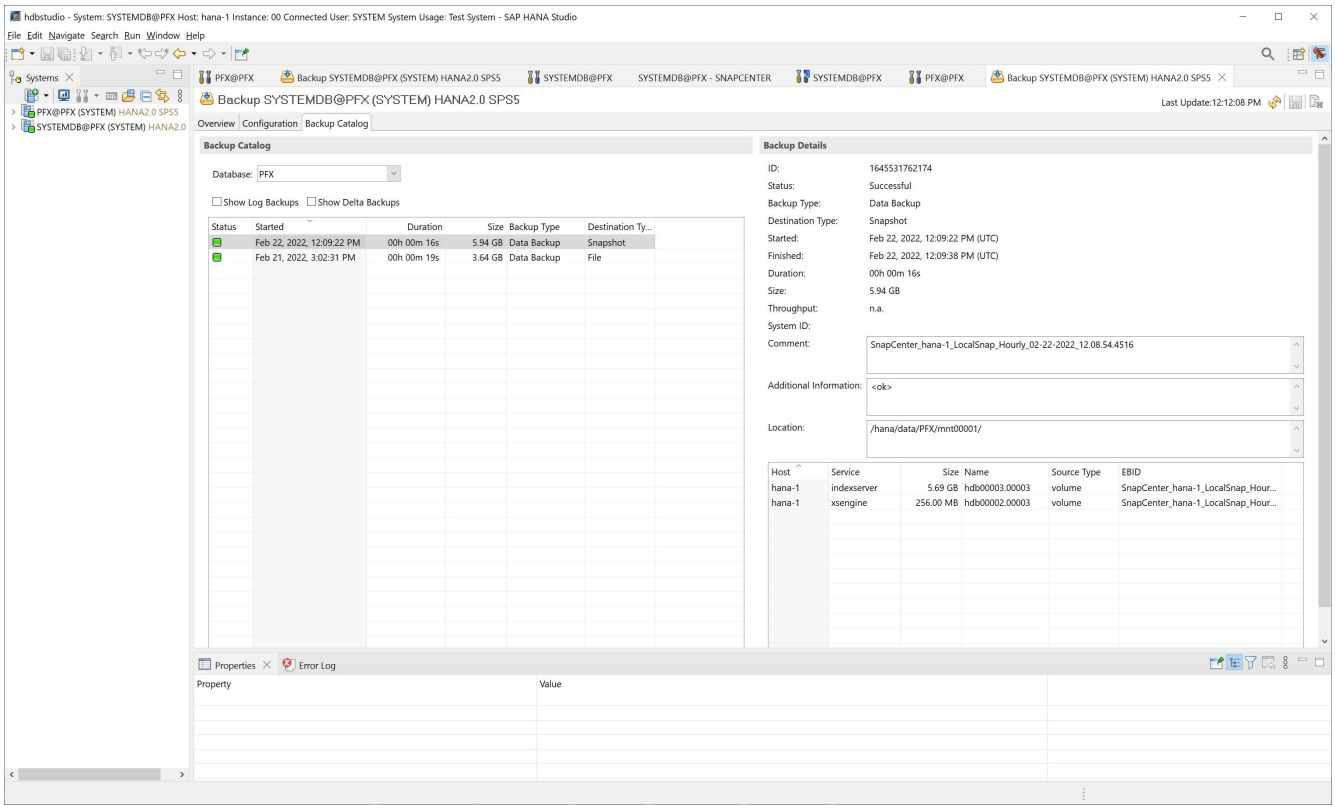


Nach Abschluss des Backups wird in der Topologieansicht ein neuer Eintrag angezeigt. Die Backup-Namen folgen derselben Namenskonvention wie der Snapshot-Name, der im Abschnitt definiert wurde "„Konfigurieren und Schützen einer HANA-Ressource“."

Sie müssen die Topologieansicht schließen und erneut öffnen, um die aktualisierte Backup-Liste anzuzeigen.

Im SAP HANA Backup-Katalog wird der SnapCenter-Backup-Name als A gespeichert `Comment` Außerdem Feld `External Backup ID (EBID)`. Dies ist in der folgenden Abbildung für die Systemdatenbank und in der nächsten Abbildung für die PFX der Mandanten-Datenbank dargestellt.



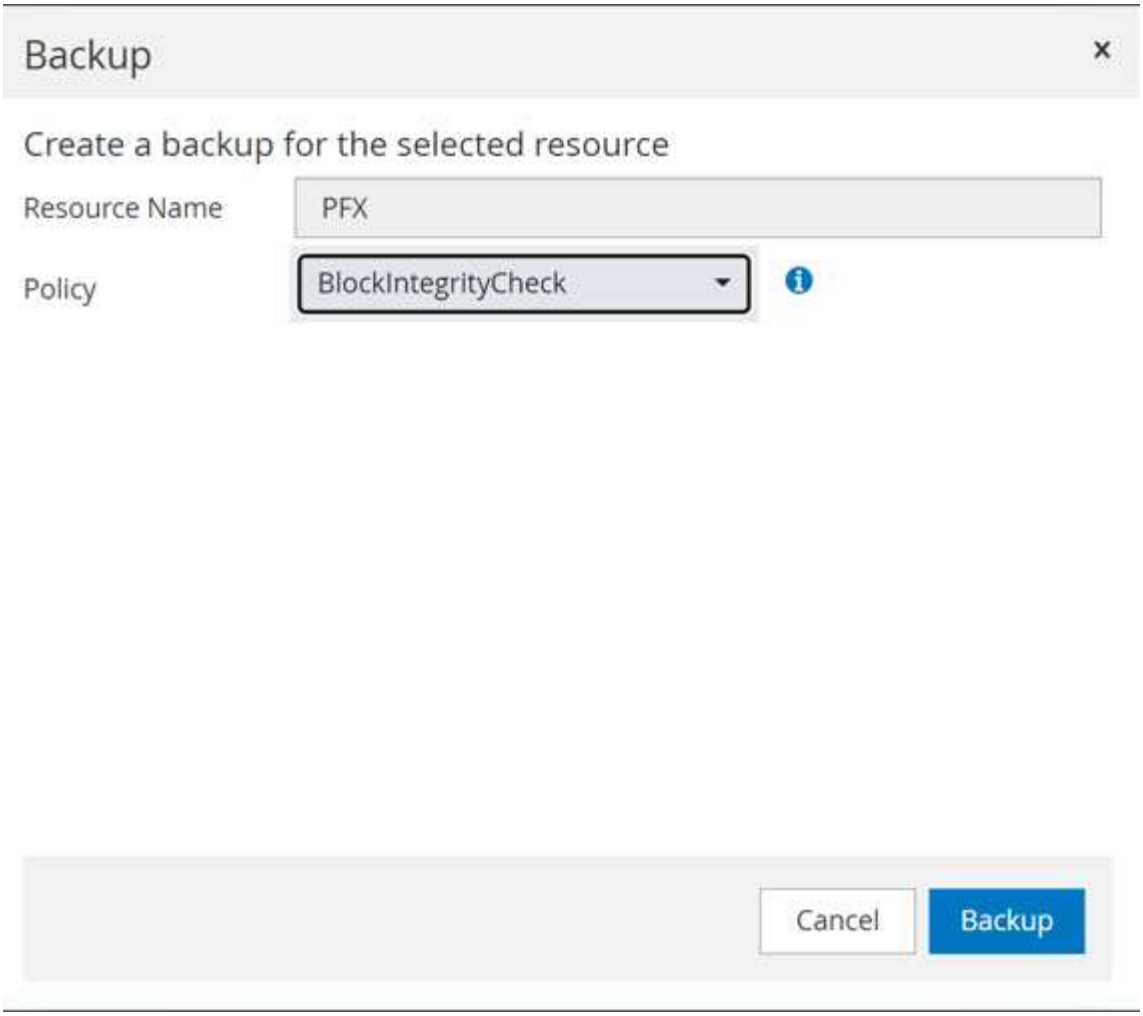


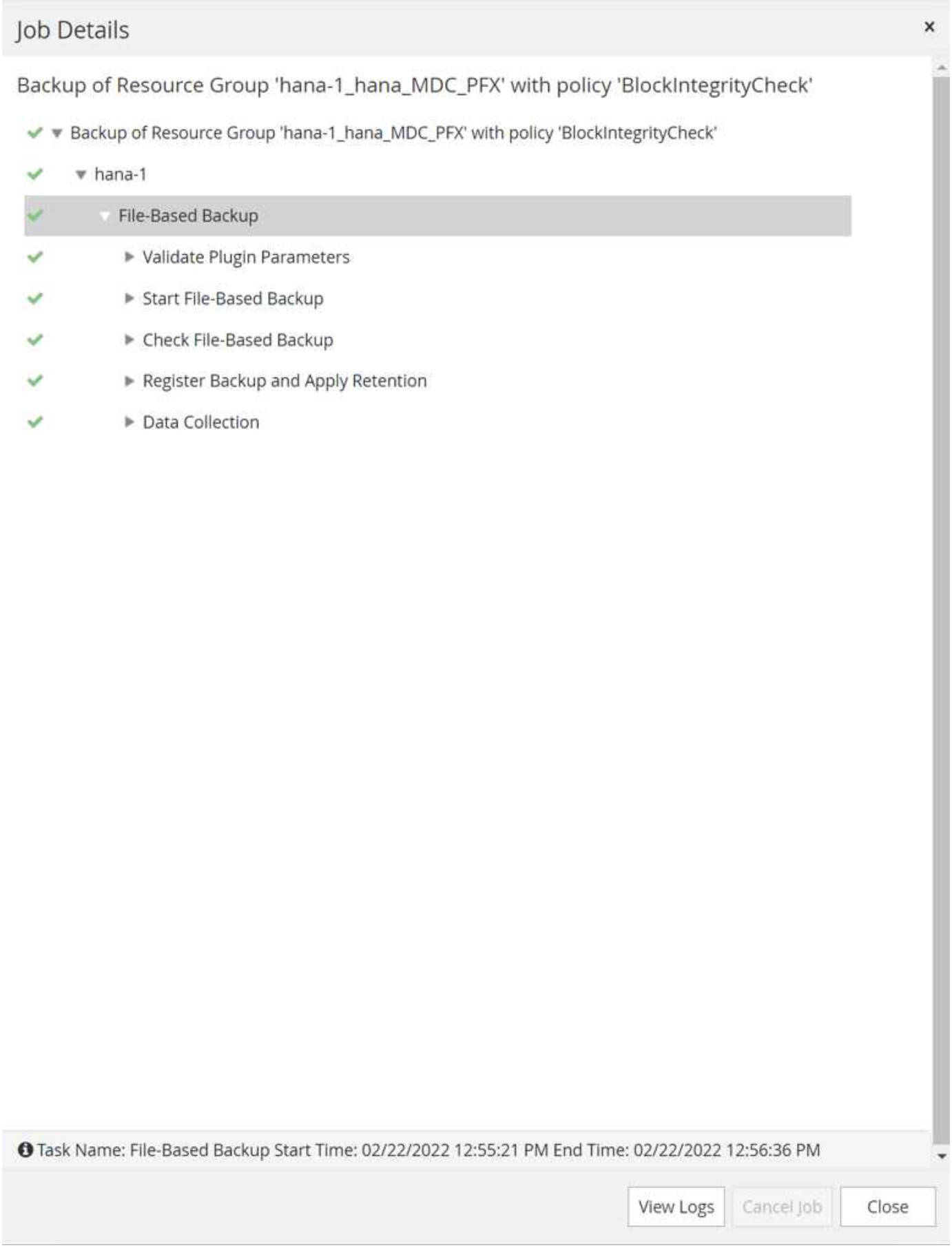
Auf dem FSX für ONTAP Filesystem können Sie die Snapshot-Backups durch eine Verbindung mit der Konsole der SVM auflisten.

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

Erstellung einer bedarfsgerechten Blockintegritätsprüfung

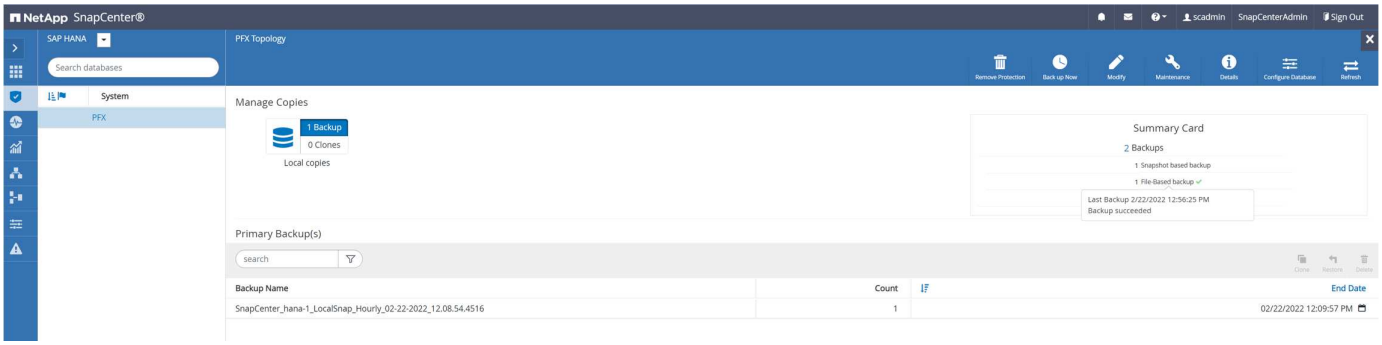
Ein on-Demand Block Integrity Check Vorgang wird auf dieselbe Weise wie ein Snapshot Backup Job ausgeführt, indem die Richtlinie BlockIntegrtyCheck ausgewählt wird. Bei der Planung von Backups mithilfe dieser Richtlinie erstellt SnapCenter eine standardmäßige SAP HANA Datei-Backup für das System und die Mandantendatenbanken.


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

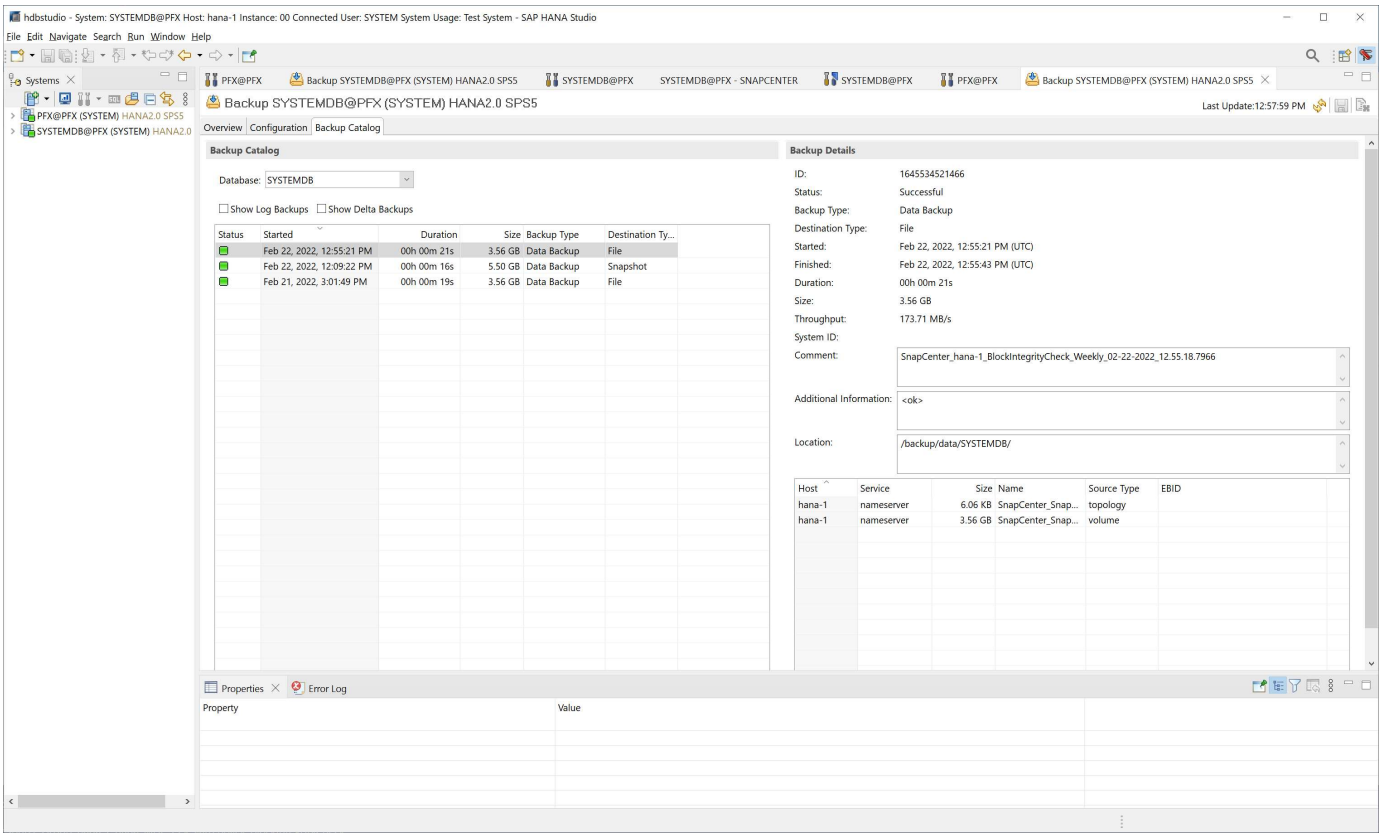


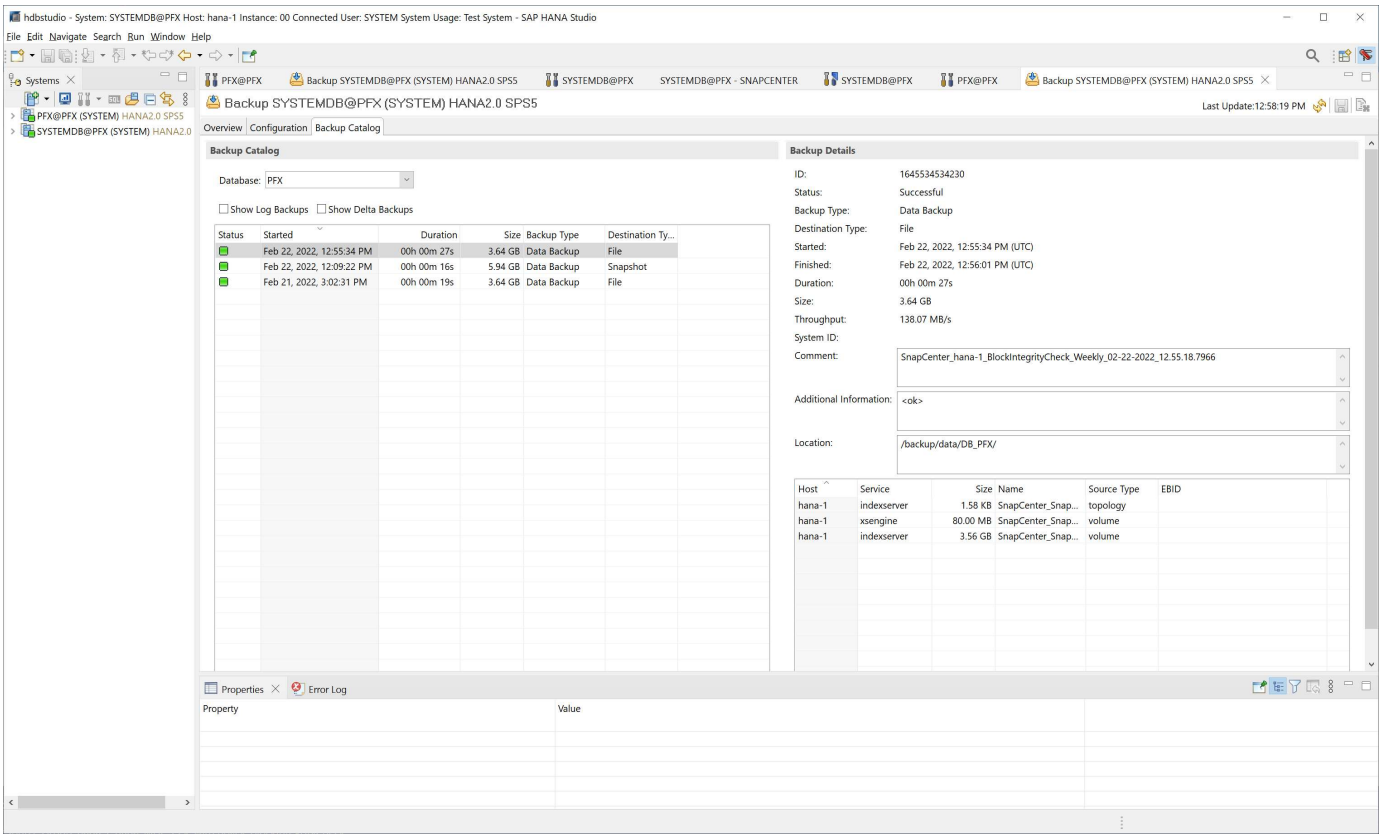
SnapCenter zeigt die Blockintegritätsprüfung nicht auf dieselbe Weise an wie Backups basierend auf

Snapshot-Kopien. Stattdessen zeigt die Übersichtskarte die Anzahl der dateibasierten Backups und den Status des vorherigen Backups an.



Der SAP HANA-Backup-Katalog zeigt Einträge sowohl für das System als auch für die Mandanten-Datenbanken an. Die folgenden Abbildungen zeigen die Integritätsprüfung der SnapCenter Blöcke im Backup-Katalog des Systems und der Mandanten-Datenbank.





Eine erfolgreiche Überprüfung der Blockintegrität erstellt standardisierte SAP HANA Daten-Backup-Dateien. SnapCenter verwendet den Backup-Pfad, der mit der HANA-Datenbank für dateibasierte Daten-Backup-Vorgänge konfiguriert wurde.

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

Backup nicht datenmengen

Das Backup von nicht-Daten-Volumes ist ein integrierter Teil des SnapCenter und des SAP HANA Plug-ins.

Der Schutz des Datenbank-Daten-Volumes reicht aus, um die SAP HANA Datenbank auf einen bestimmten Zeitpunkt wiederherzustellen, vorausgesetzt, die Ressourcen für die Datenbankinstallation und die erforderlichen Protokolle sind weiterhin verfügbar.

Um das Recovery von Situationen durchzuführen, in denen andere nicht-Datendateien wiederhergestellt

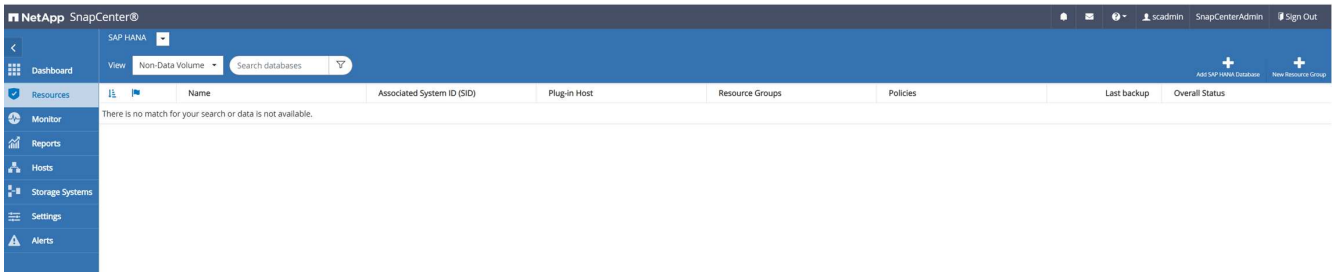
werden müssen, empfiehlt NetApp, eine zusätzliche Backup-Strategie für nicht-Daten-Volumes zu entwickeln, um das SAP HANA Datenbank-Backup zu erweitern. Je nach Ihren spezifischen Anforderungen kann sich das Backup von nicht-Daten-Volumes in den Einstellungen für die Planungsfrequenz und -Aufbewahrung unterscheiden, und Sie sollten bedenken, wie oft nicht-Datendateien geändert werden. Zum Beispiel das HANA Volume `/hana/shared` Enthält ausführbare Dateien, aber auch SAP HANA Trace-Dateien. Zwar ändern sich ausführbare Dateien nur beim Upgrade der SAP HANA Datenbank, doch benötigen die SAP HANA Trace-Dateien möglicherweise eine höhere Backup-Häufigkeit, um Problemsituationen mit SAP HANA zu analysieren.

Dank des nicht-Daten-Volume-Backups von SnapCenter können Snapshot-Kopien aller relevanten Volumes in wenigen Sekunden mit derselben Speichereffizienz erstellt werden wie bei SAP HANA-Datenbank-Backups. Der Unterschied liegt darin, dass keine SQL Kommunikation mit der SAP HANA Datenbank erforderlich ist.

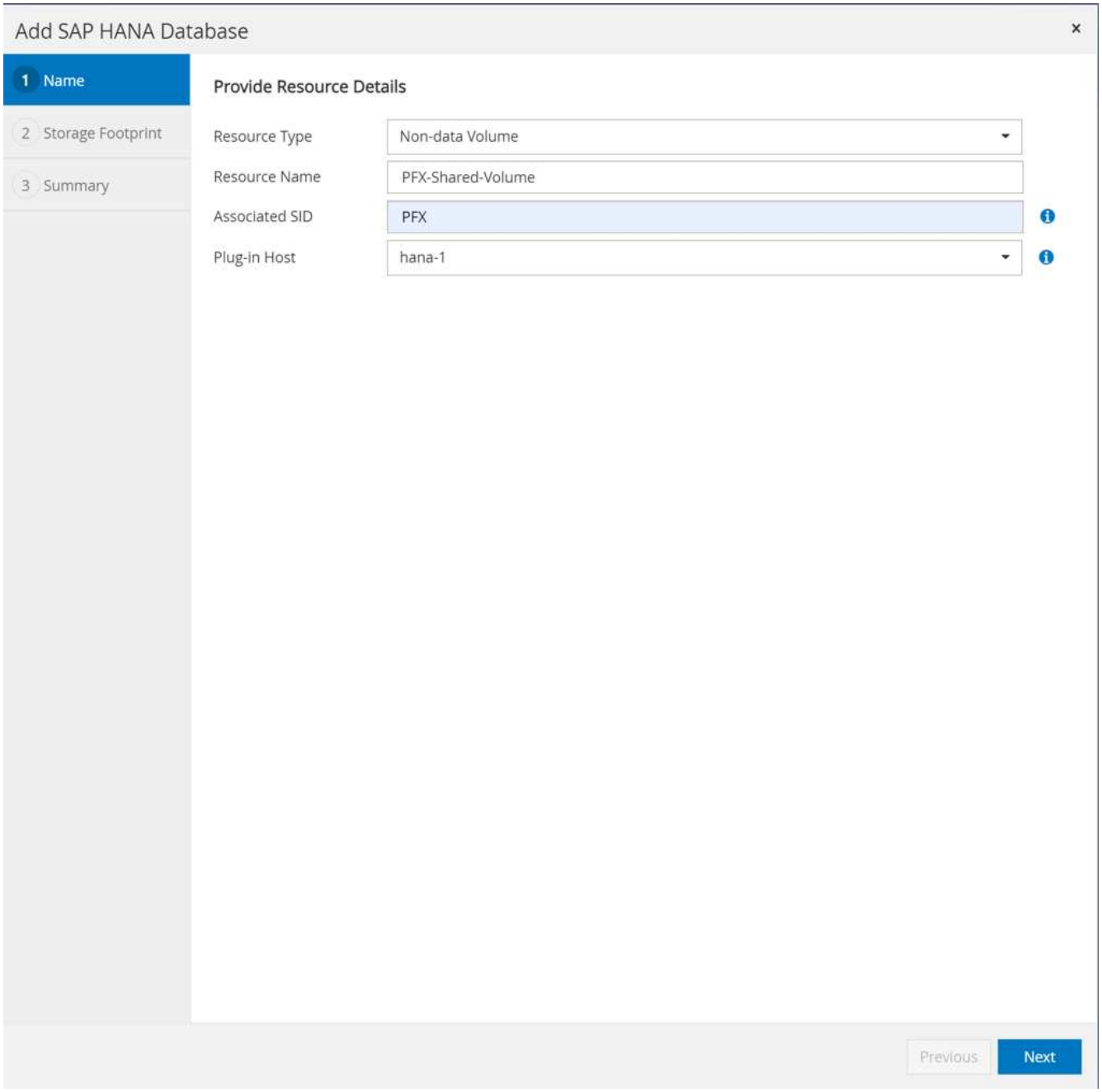
Konfiguration von Ressourcen, die nicht von Datenvolumen stammen

Führen Sie die folgenden Schritte aus, um nicht-Daten-Volume-Ressourcen zu konfigurieren:

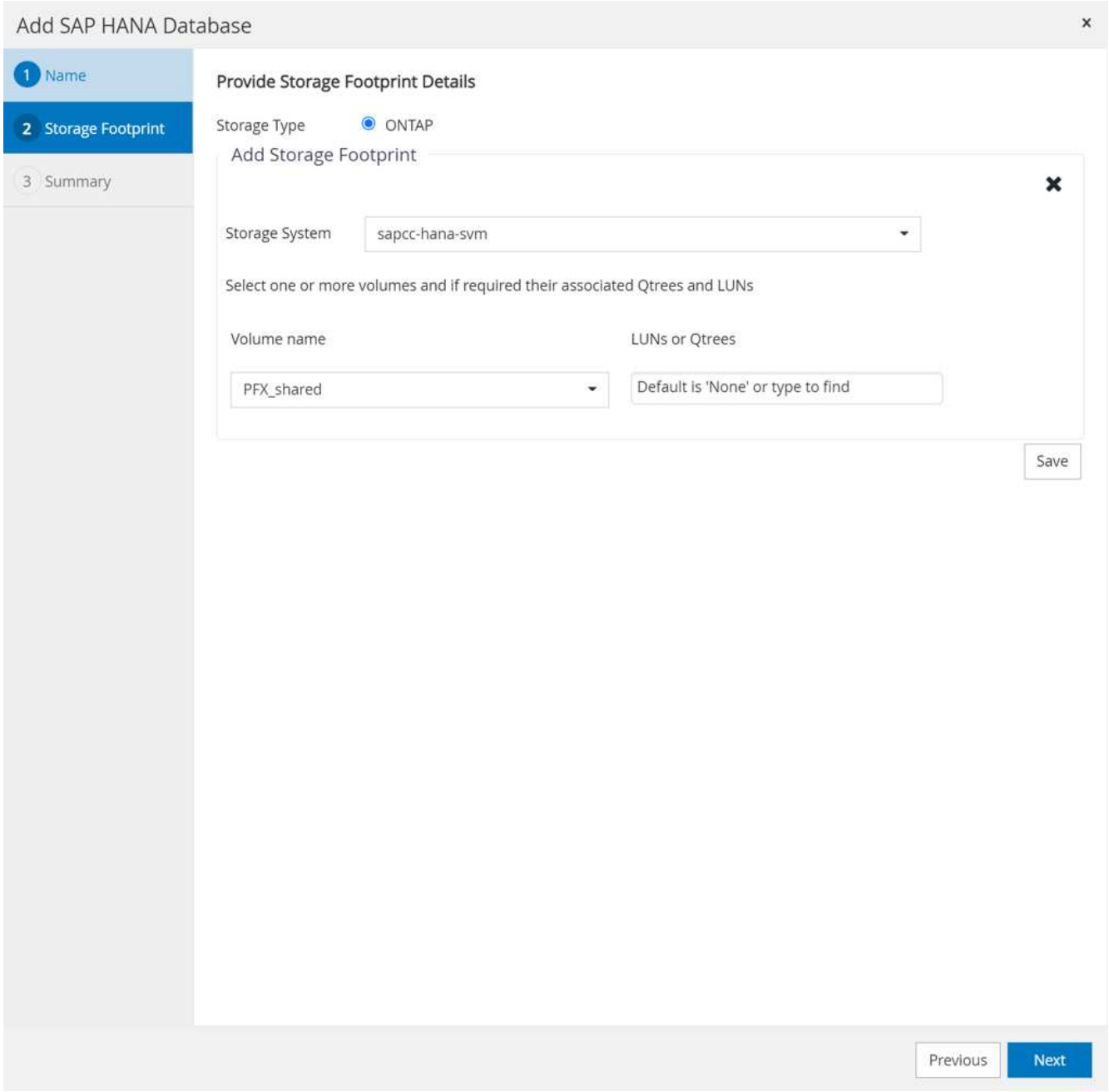
1. Wählen Sie auf der Registerkarte Ressourcen die Option Non-Data-Volume, und klicken Sie auf Add SAP HANA Database.



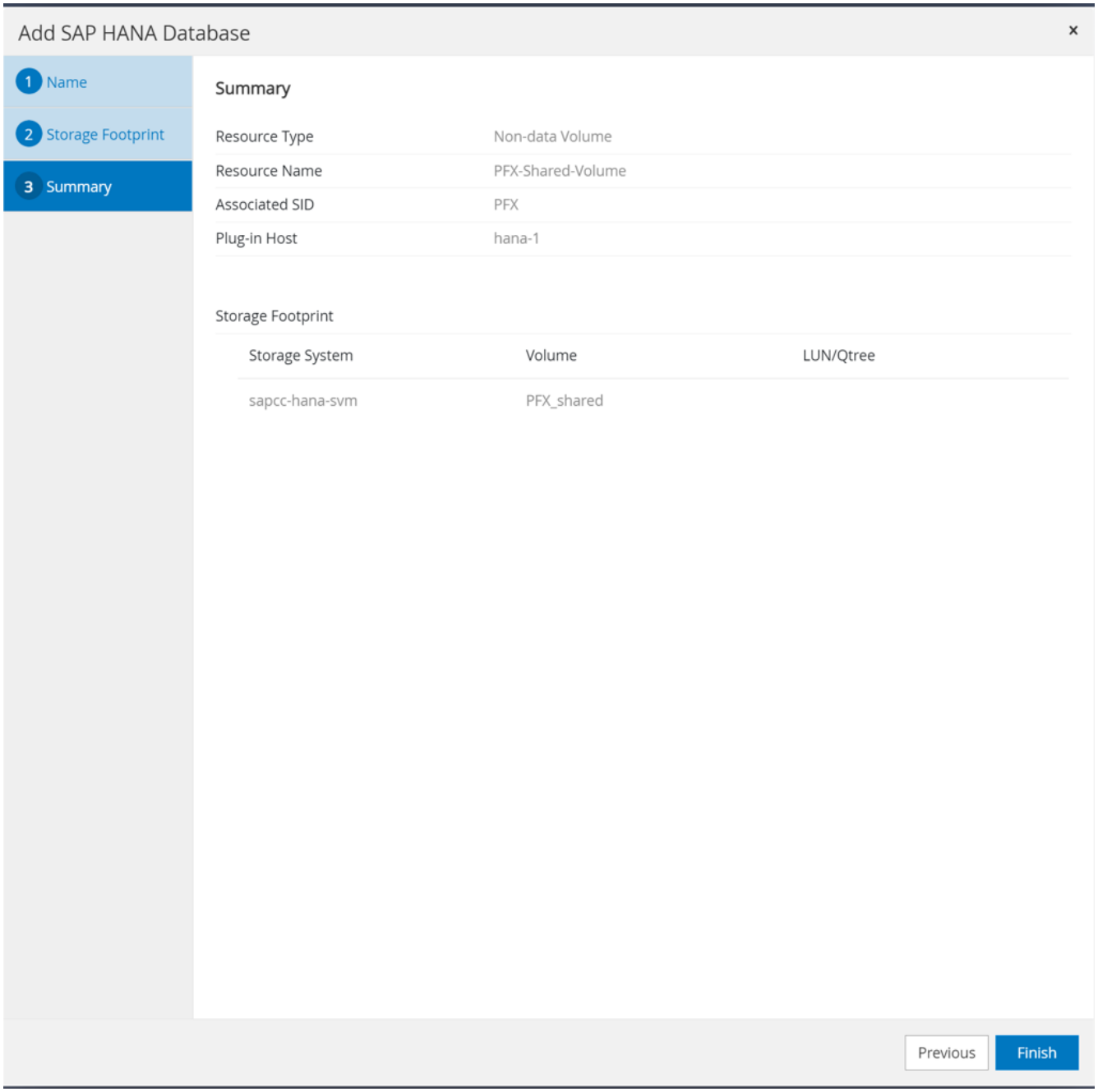
2. Wählen Sie in Schritt 1 des Dialogfelds SAP HANA-Datenbank hinzufügen in der Liste Ressourcentyp die Option nicht-Datenvolumen aus. Geben Sie einen Namen für die Ressource und den zugehörigen SID und den SAP HANA Plug-in-Host an, den Sie für die Ressource verwenden möchten, und klicken Sie dann auf Weiter.



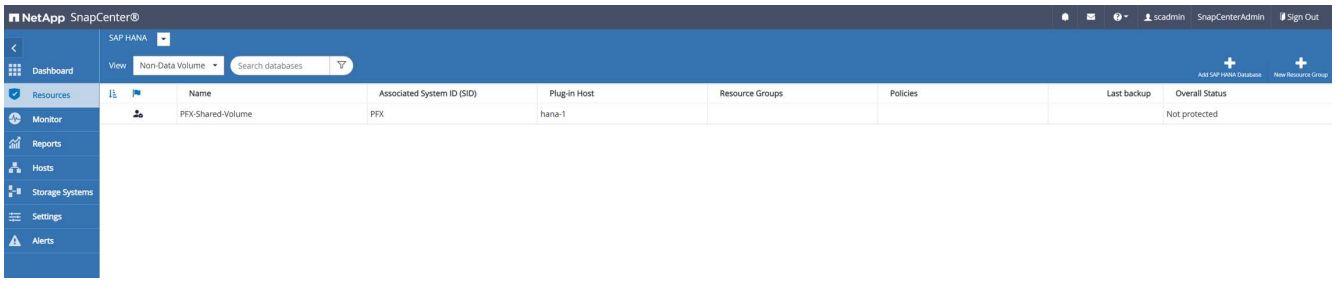
3. Fügen Sie die SVM und das Storage-Volume als Storage-Platzbedarf hinzu und klicken Sie dann auf Weiter.



4. Um die Einstellungen zu speichern, klicken Sie im Zusammenfassungsschritt auf Fertig stellen.



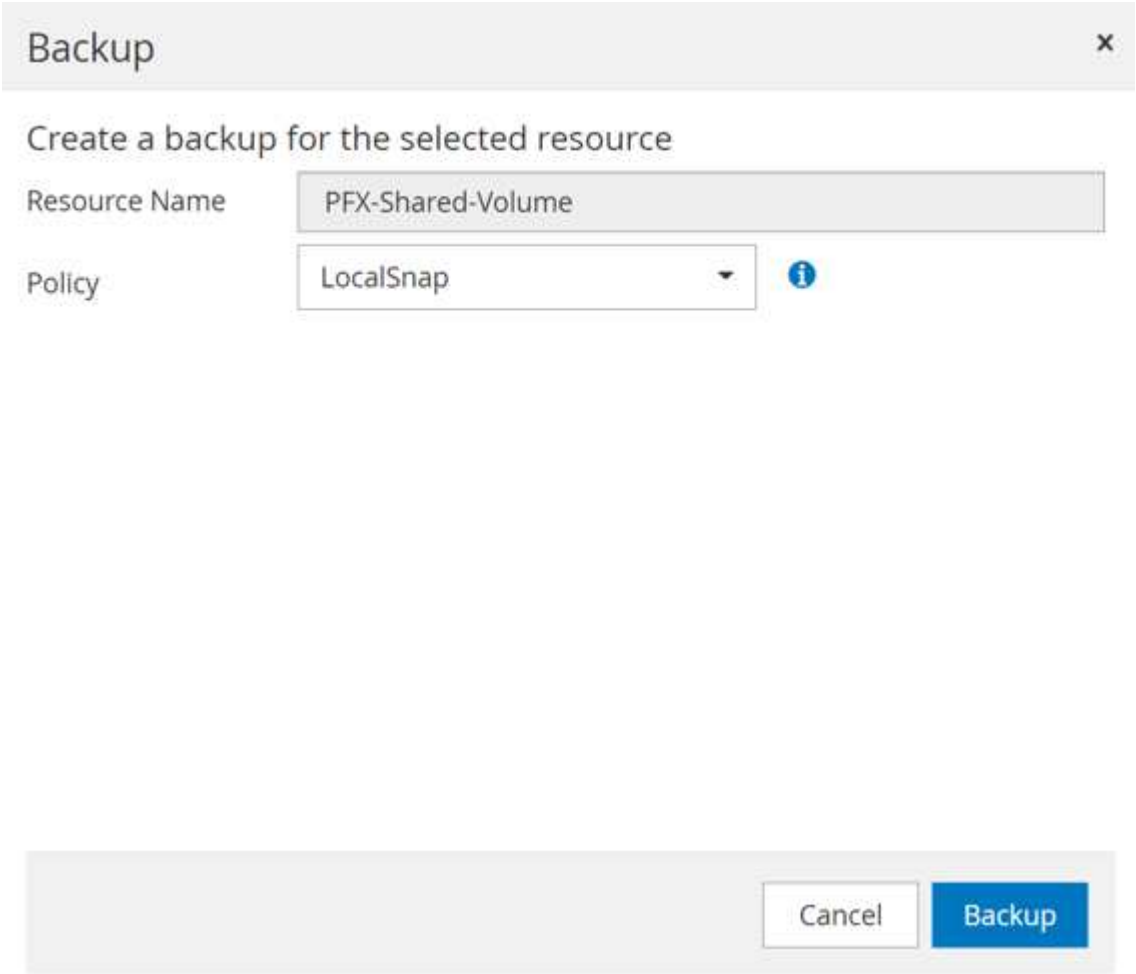
Das neue nicht-Daten-Volume wird nun SnapCenter hinzugefügt. Doppelklicken Sie auf die neue Ressource, um den Ressourcenschutz auszuführen.



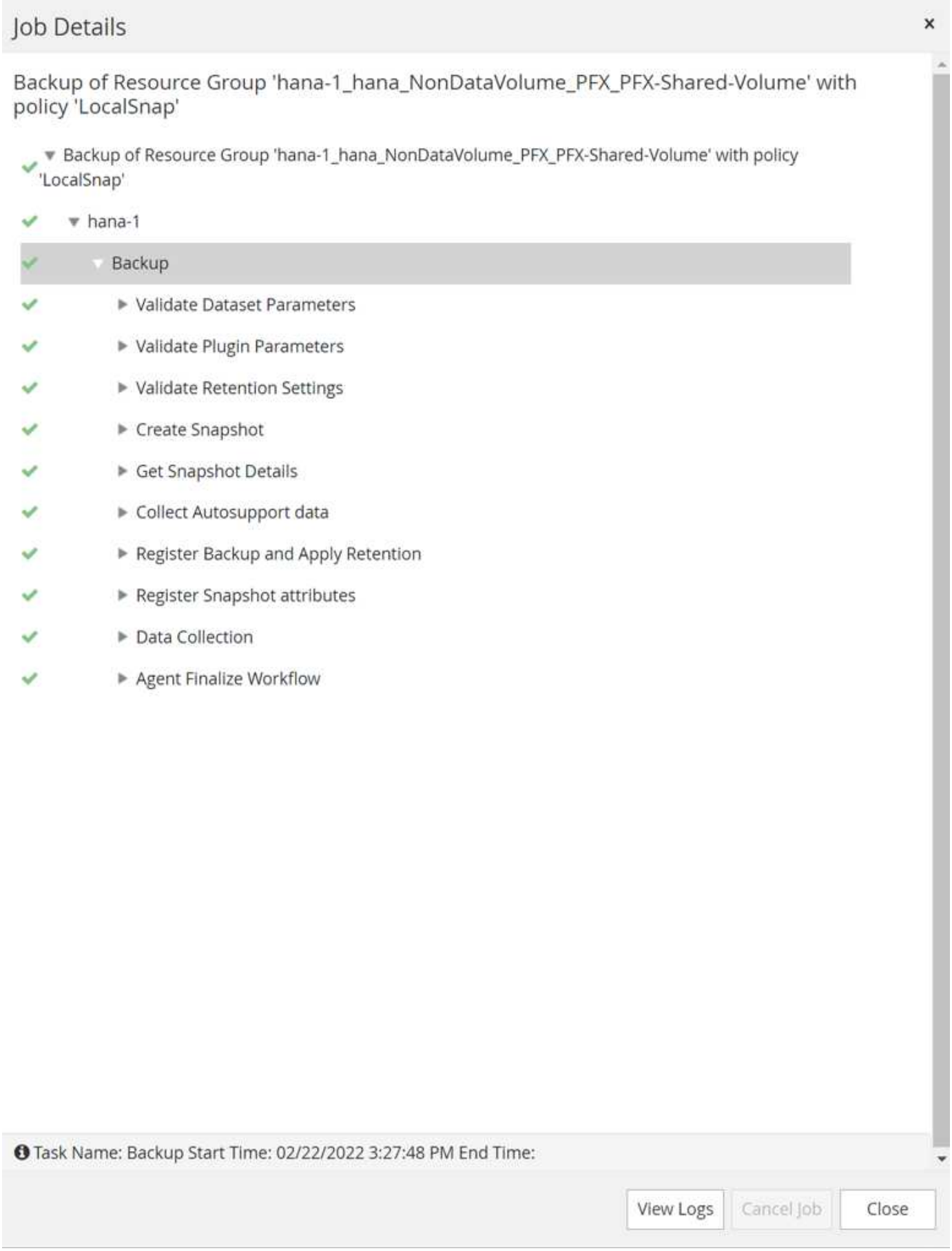
Der Ressourcenschutz erfolgt auf dieselbe Weise wie zuvor bei einer HANA-Datenbankressource.

5. Sie können jetzt ein Backup ausführen, indem Sie auf Jetzt sichern klicken.

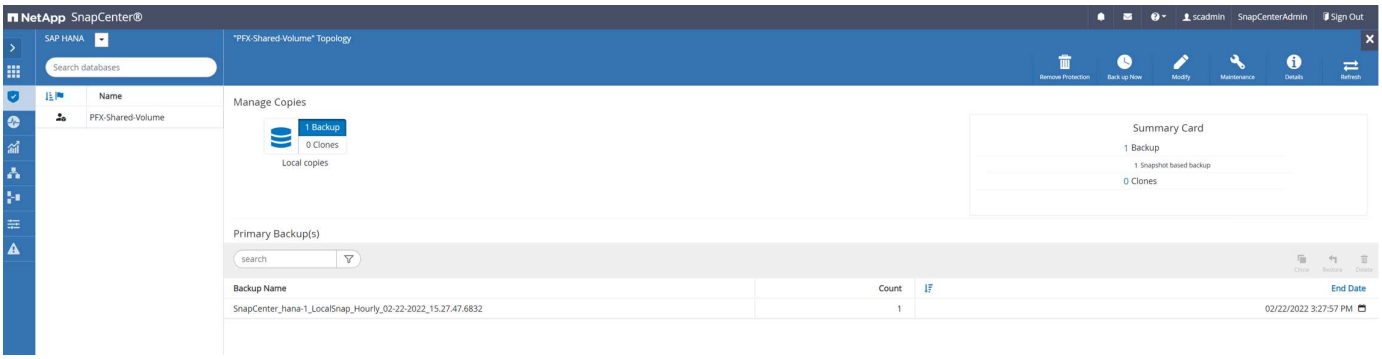
6. Wählen Sie die Richtlinie aus, und starten Sie den Backup-Vorgang.



Das Jobprotokoll von SnapCenter zeigt die einzelnen Workflow-Schritte.



Das neue Backup ist nun in der Ressourcenansicht der Ressource ohne Datenvolumen sichtbar.



Restore und Recovery

Mit SnapCenter werden für HANA-einzelne-Host-MDC-Systeme über einen einzelnen Mandanten automatisierte Restore- und Recovery-Vorgänge unterstützt. Bei Systemen mit mehreren Hosts oder MDC-Systemen mit mehreren Mandanten führt SnapCenter nur den Wiederherstellungsvorgang aus, und Sie müssen die Wiederherstellung manuell durchführen.

Sie können eine automatisierte Wiederherstellung und Operation mit den folgenden Schritten ausführen:

1. Wählen Sie das Backup aus, das für den Wiederherstellungsvorgang verwendet werden soll.
2. Wählen Sie den Wiederherstellungstyp aus. Wählen Sie mit Volume Revert oder ohne Volume Revert die Option Complete Restore.
3. Wählen Sie den Wiederherstellungstyp aus den folgenden Optionen aus:
   - Auf den letzten Stand
   - Zeitpunktgenau
   - Zu einem bestimmten Daten-Backup
   - Keine Wiederherstellung

     Der ausgewählte Wiederherstellungstyp wird für die Wiederherstellung des Systems und der Mandanten-Datenbank verwendet.

Als Nächstes führt SnapCenter die folgenden Operationen durch:

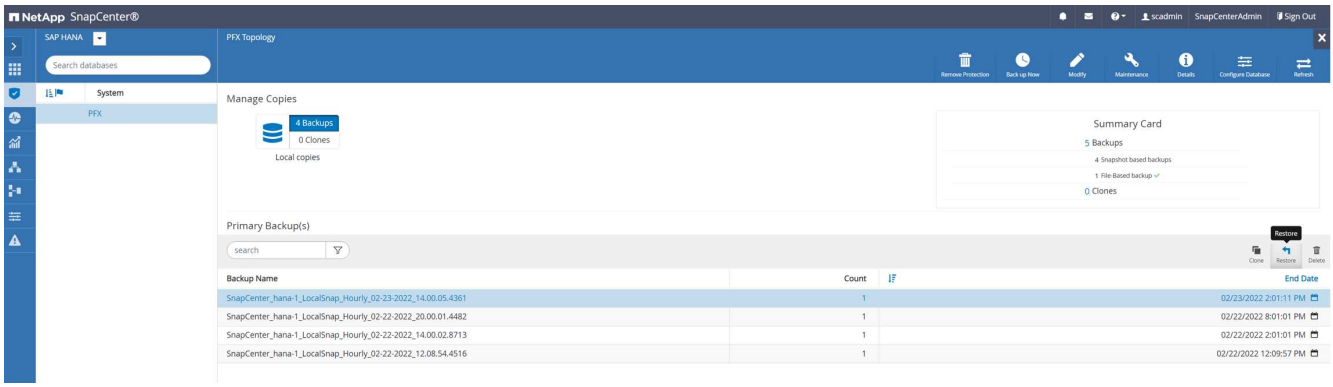
1. Die HANA-Datenbank wird gestoppt.
2. Die Datenbank wird wiederhergestellt. Je nach gewähltem Wiederherstellungstyp werden verschiedene Operationen ausgeführt.
   - Wenn das Zurücksetzen von Volumes ausgewählt wird, hängt SnapCenter das Volume ab, stellt das Volume mithilfe von Volume-basierten SnapRestore auf der Storage-Ebene wieder her und hängt das Volume an.
   - Wenn das Zurücksetzen von Volumes nicht ausgewählt wird, stellt SnapCenter alle Dateien mithilfe einzelner Datei-SnapRestore-Vorgänge auf der Storage-Ebene wieder her.
3. Es stellt die Datenbank wieder her:
   a. Durch Wiederherstellen der Systemdatenbank
   b. Wiederherstellung der Mandantendatenbank
   c. Starten der HANA-Datenbank

     Wenn keine Wiederherstellung ausgewählt ist, wird die SnapCenter beendet, und Sie müssen den

Wiederherstellungsvorgang für das System und die Mandantendatenbank manuell durchführen.

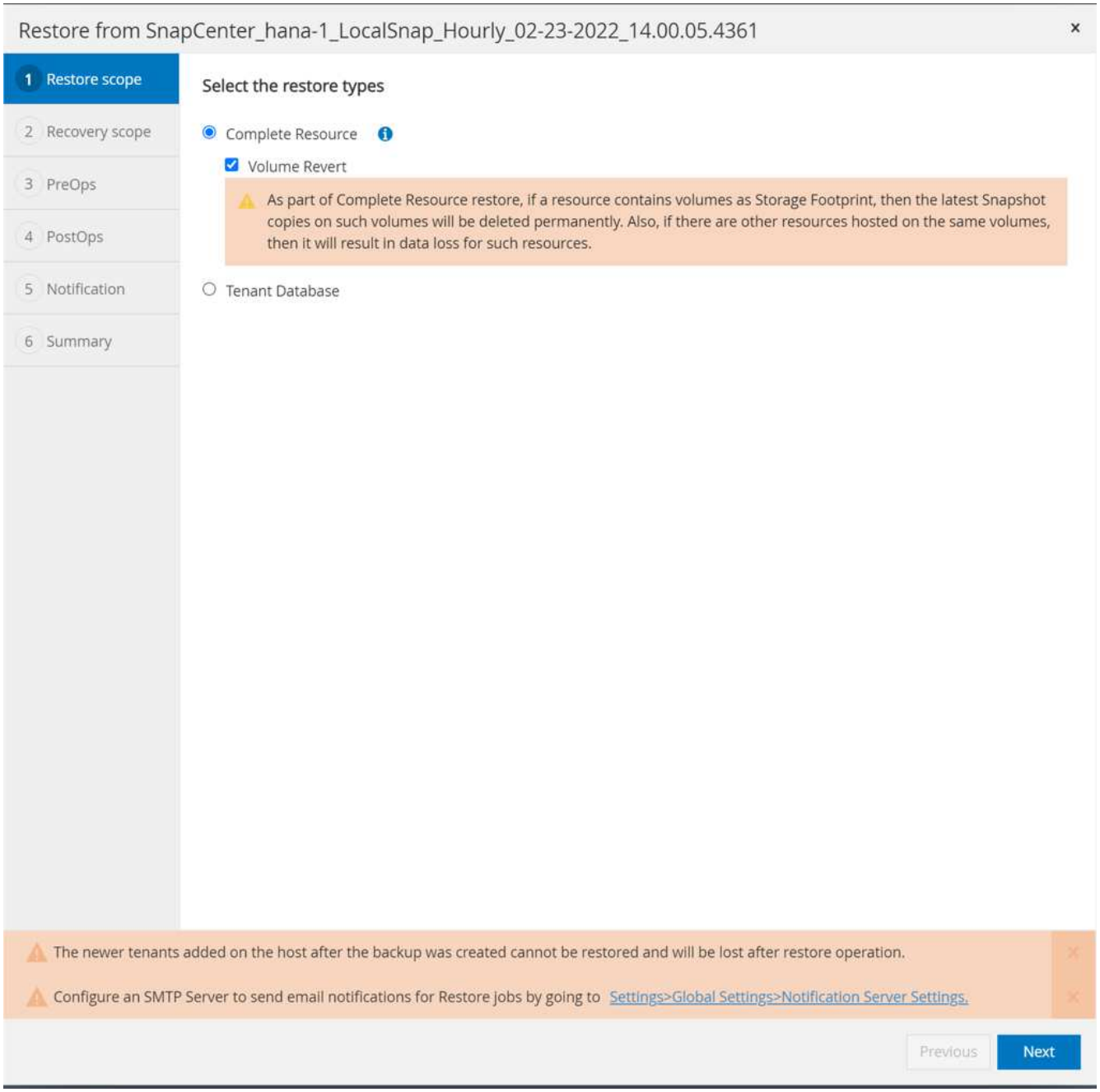
Führen Sie die folgenden Schritte aus, um einen manuellen Wiederherstellungsvorgang durchzuführen:

1. Wählen Sie ein Backup in SnapCenter aus, das für den Wiederherstellungsvorgang verwendet werden soll.



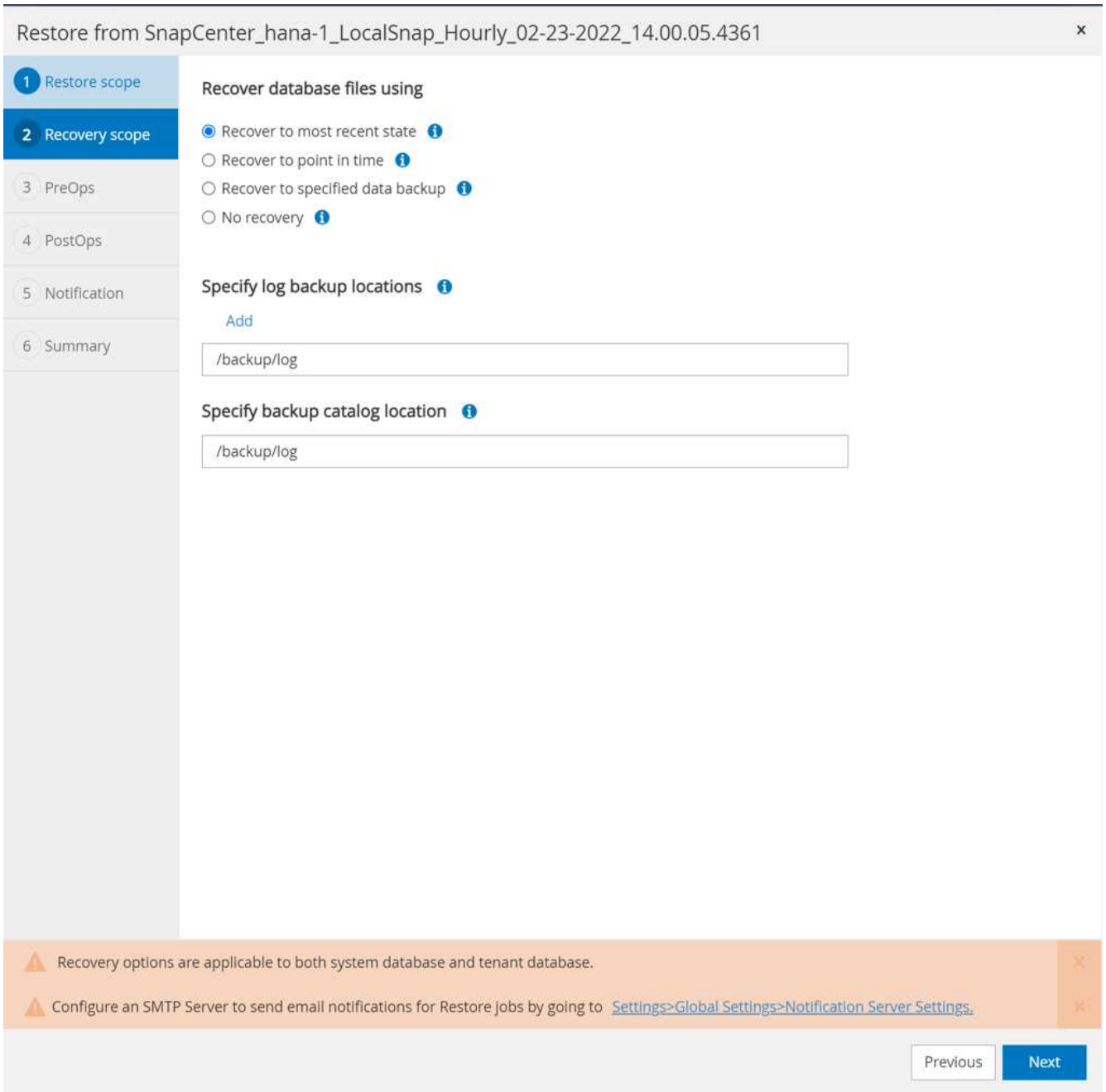
2. Wählen Sie den Umfang und den Typ der Wiederherstellung aus.

   Das Standardszenario für HANA MDC-Einzelmandant-Systeme besteht darin, komplette Ressourcen mit Zurücksetzen des Volumes zu nutzen. Bei einem HANA MDC-System mit mehreren Mandanten möchten Sie möglicherweise nur einen einzelnen Mandanten wiederherstellen. Weitere Informationen zur Wiederherstellung einzelner Mandanten finden Sie unter "Restore und Recovery (netapp.com)".

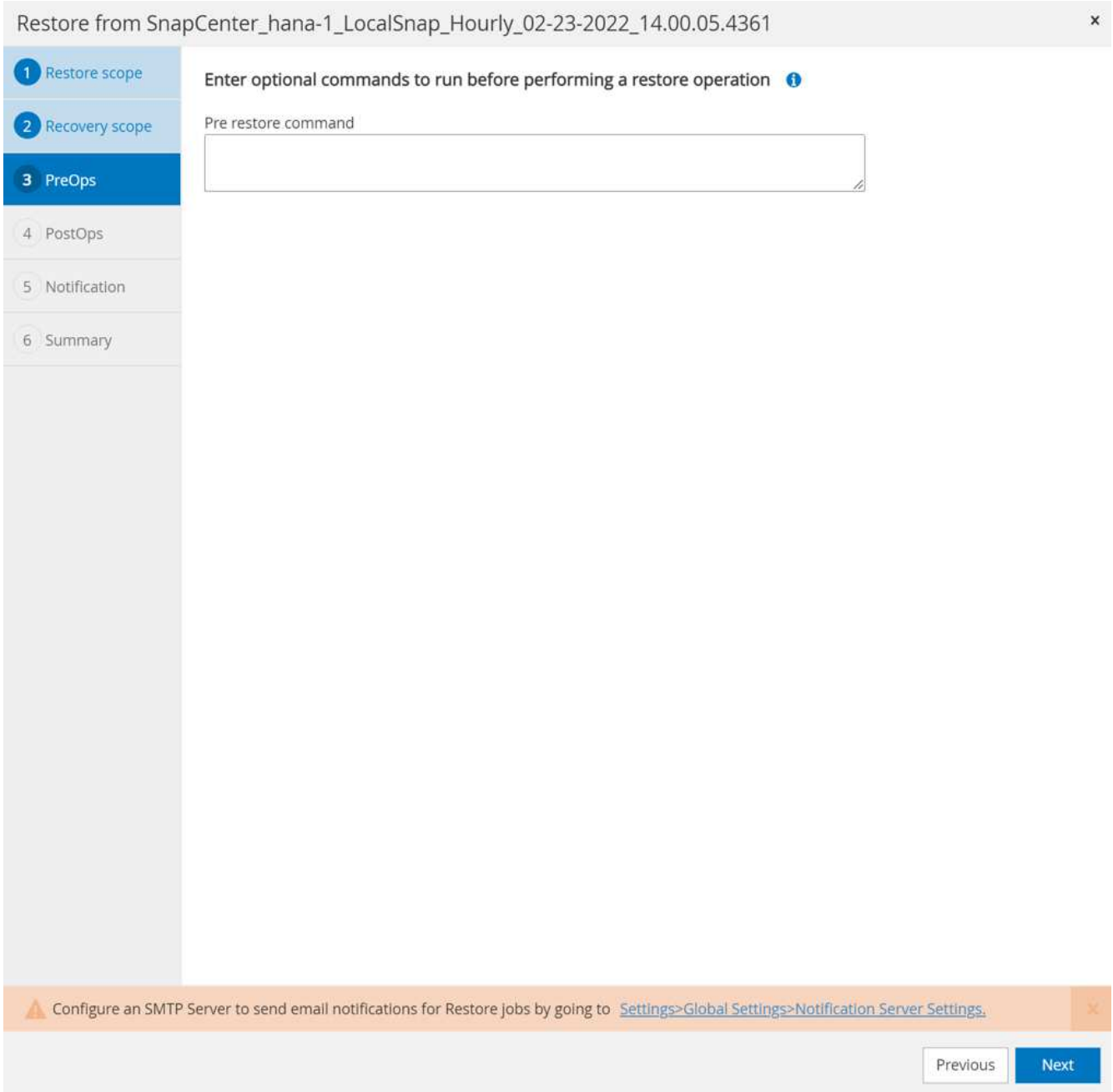


3. Wählen Sie „Recovery Scope“ aus, und stellen Sie den Speicherort für das Backup und das Katalog-Backup bereit.

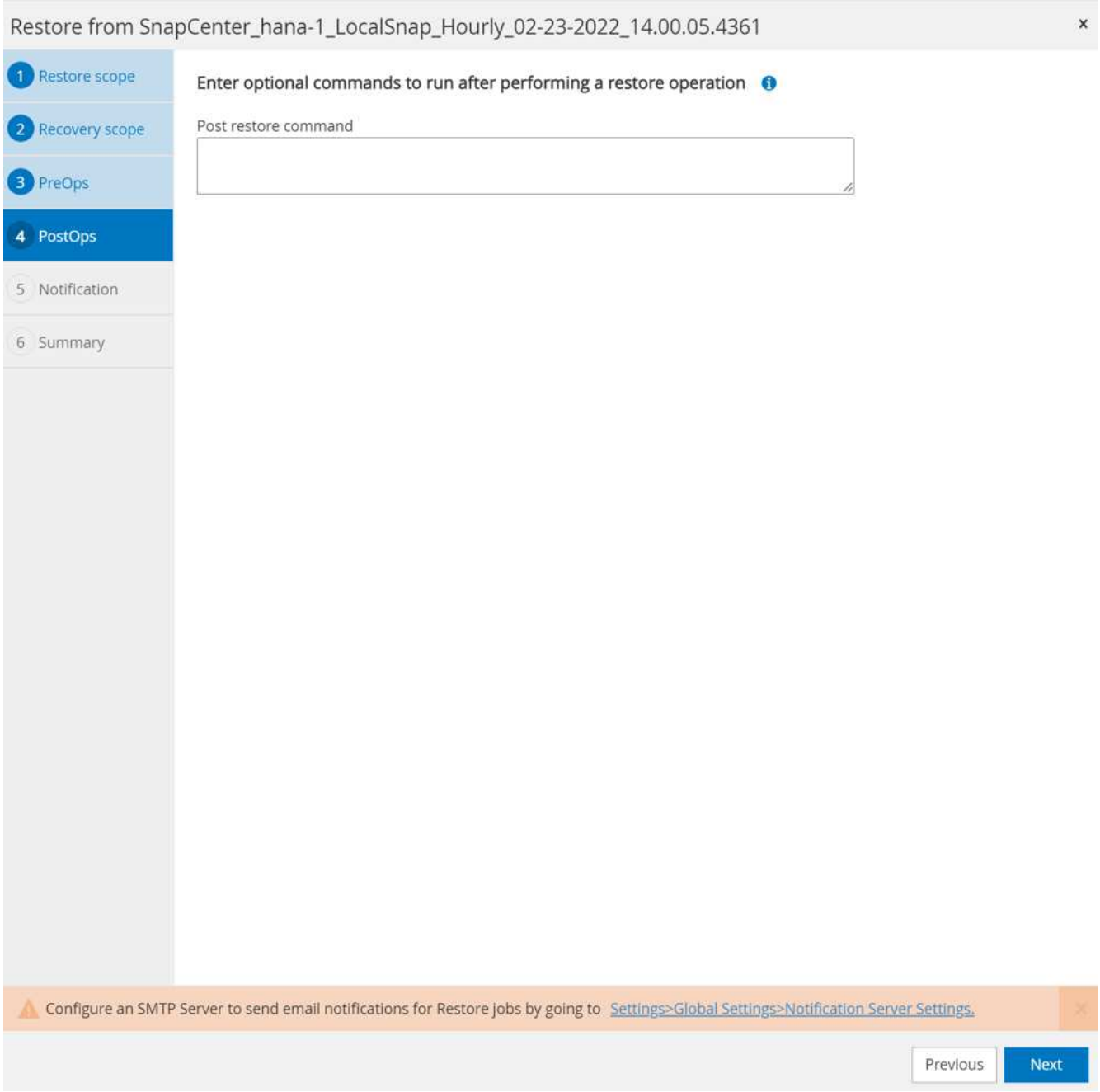
   SnapCenter verwendet den Standardpfad oder die geänderten Pfade in der HANA global.ini-Datei, um die Backup-Speicherorte für das Protokoll und den Katalog auszufüllen.



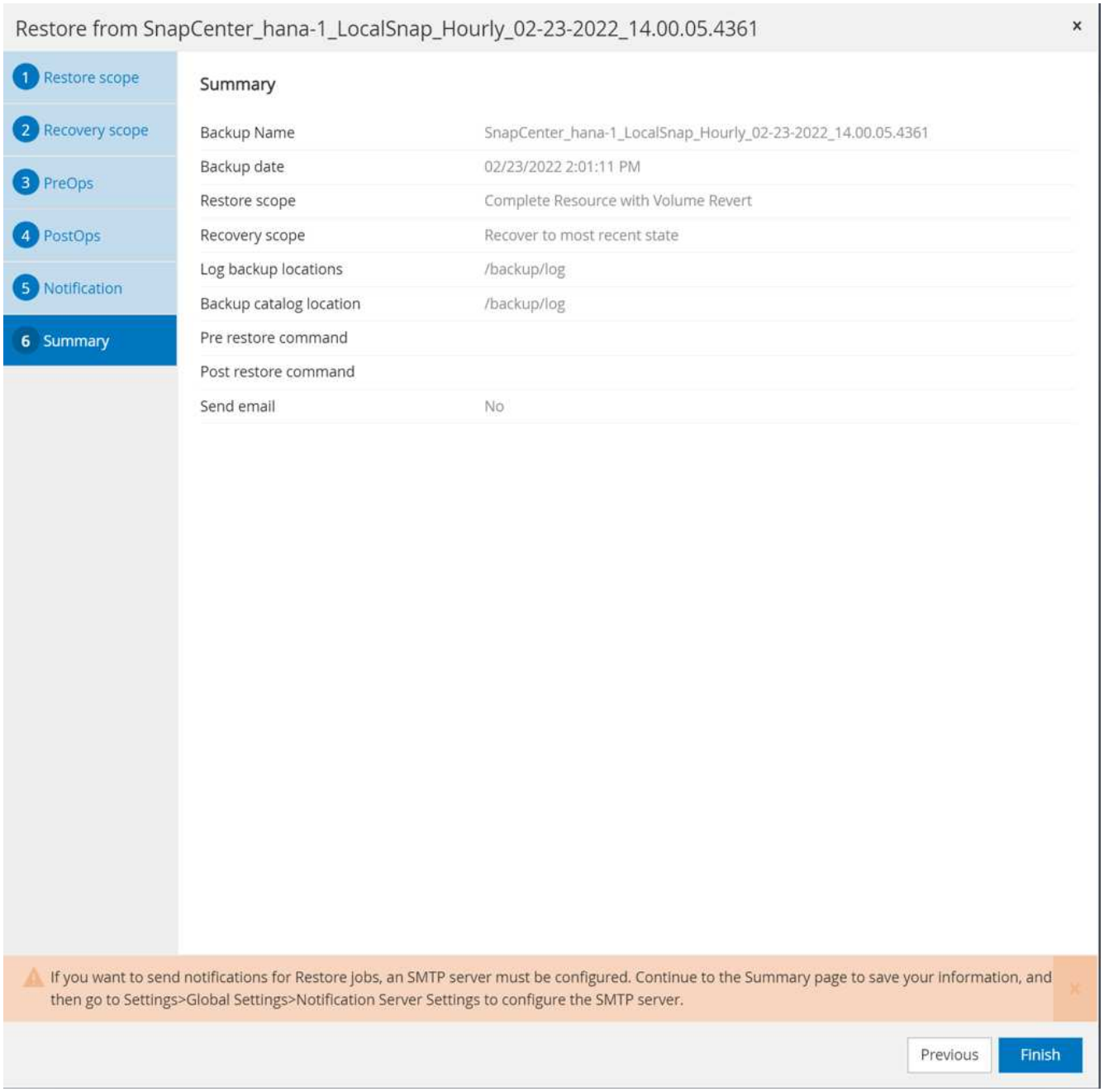
4. Geben Sie die optionalen Befehle vor der Wiederherstellung ein.



5. Geben Sie die optionalen Befehle nach der Wiederherstellung ein.



6. Um den Wiederherstellungs- und Wiederherstellungsvorgang zu starten, klicken Sie auf Fertig stellen.



SnapCenter führt den Wiederherstellungsvorgang und die Wiederherstellung aus. Dieses Beispiel zeigt die Jobdetails des Wiederherstellungsjobs.

Job Details

Restore 'hana-1\hana\MDC\PFX'

- Restore 'hana-1\hana\MDC\PFX'
  - hana-1
    - Restore
      - Validate Plugin Parameters
      - Pre Restore Application
        - Stopping HANA instance
      - Filesystem Pre Restore
      - Restore Filesystem
      - Filesystem Post Restore
      - Recover Application
        - Recovering system database
        - Checking HDB services status
        - Recovering tenant database 'PFX'
        - Starting HANA instance
      - Clear Catalog on Server
      - Application Clean-Up
      - Data Collection
      - Agent Finalize Workflow

Task Name: Recover Application Start Time: 02/23/2022 2:07:31 PM End Time:

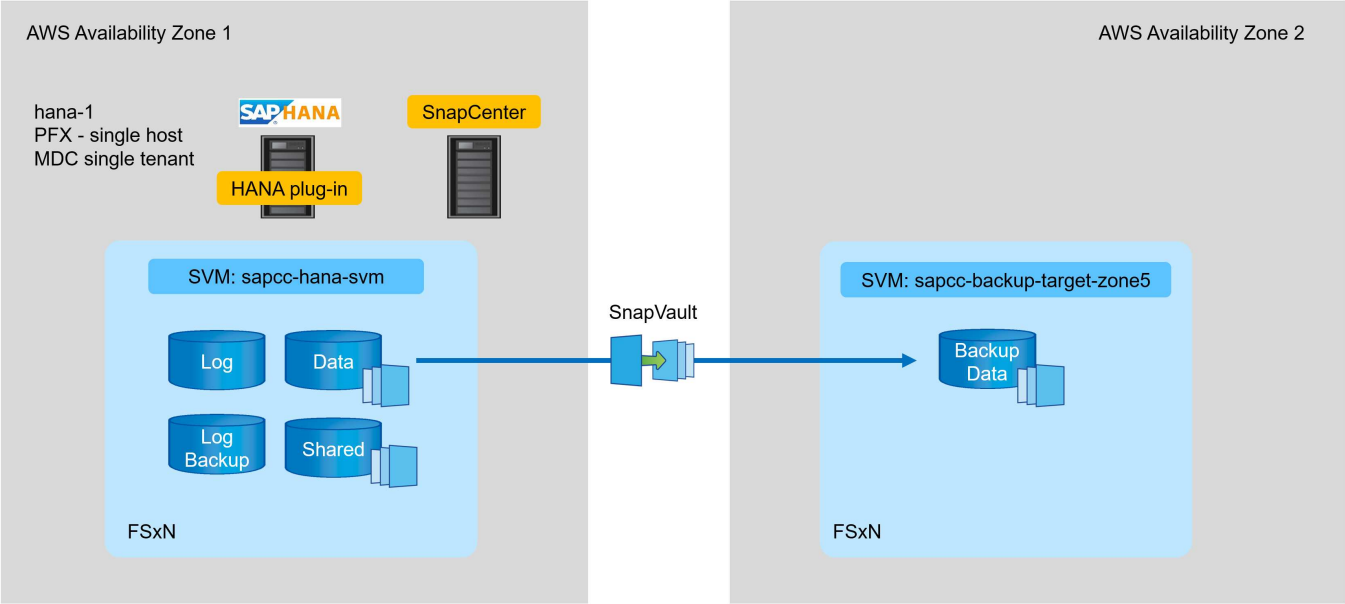
View Logs | Cancel Job | Close

Backup-Replizierung mit SnapVault

Übersicht - Backup-Replikation mit SnapVault

Im Lab-Setup verwenden wir ein zweites FSX für ONTAP-Filesystem in einer zweiten AWS-Verfügbarkeitszone, um die Backup-Replizierung für das HANA-Datenvolumen zu präsentieren.

Wie in Kapitel erläutert "„Datensicherungsstrategie“", Das Replikationsziel muss ein zweites FSX für ONTAP-Dateisystem in einer anderen Verfügbarkeitszone sein, um vor einem Ausfall des primären FSX für ONTAP-Dateisystem geschützt zu werden. Außerdem sollte das gemeinsame HANA-Volume auf das sekundäre FSX für das ONTAP-Dateisystem repliziert werden.



Übersicht über die Konfigurationsschritte

Es gibt einige Konfigurationsschritte, die auf der FSX für ONTAP-Ebene ausgeführt werden müssen. Dies lässt sich entweder mit NetApp Cloud Manager oder über die Befehlszeile des FSX für ONTAP durchführen.

1. Peer-FSX für ONTAP-Filesysteme FSX für ONTAP-Dateisysteme müssen peed werden, um eine Replizierung zwischen beiden zu ermöglichen.
2. Peer-SVMs: SVMs müssen Peering durchgeführt werden, um eine Replizierung zwischen den beiden SVMs zu ermöglichen.
3. Erstellen eines Ziel-Volumes Erstellung eines Volumes in der Ziel-SVM mit Volume-Typ `DP`. Typ `DP` Muss als Ziel-Volume für die Replikation verwendet werden.
4. SnapMirror-Richtlinie erstellen Dies wird verwendet, um eine Policy für Replikation mit Typ zu erstellen `vault`.
    a. Fügen Sie eine Regel zur Richtlinie hinzu. Die Regel enthält das SnapMirror-Etikett und die Aufbewahrung für Backups am sekundären Standort. Sie müssen dasselbe SnapMirror-Label später in der SnapCenter-Richtlinie konfigurieren, damit SnapCenter Snapshot-Backups auf dem Quell-Volume mit diesem Etikett erstellt.
5. SnapMirror Beziehung erstellen Definiert die Replikationsbeziehung zwischen dem Quell- und dem Ziel-Volume und fügt eine Richtlinie hinzu.

6. SnapMirror initialisieren. Damit wird die erste Replikation gestartet, bei der die vollständigen Quelldaten auf das Ziel-Volume übertragen werden.

Wenn die Konfiguration der Volume-Replikation abgeschlossen ist, müssen Sie die Backup-Replikation in SnapCenter wie folgt konfigurieren:

1. Fügen Sie die Ziel-SVM zu SnapCenter hinzu.
2. Erstellen einer neuen SnapCenter-Richtlinie für Snapshot Backup und SnapVault-Replizierung
3. Fügen Sie die Richtlinie zu HANA-Ressourcenschutz hinzu.
4. Sie können jetzt Backups mit der neuen Richtlinie ausführen.

In den folgenden Kapiteln werden die einzelnen Schritte detaillierter beschrieben.

Konfigurieren Sie Replikationsbeziehungen auf FSX für ONTAP-Dateisysteme

Weitere Informationen zur SnapMirror Konfigurationsoptionen finden Sie in der ONTAP-Dokumentation unter "SnapMirror Replizierungs-Workflow (netapp.com)".

- Quell-FSX für ONTAP Dateisystem: `FsxId00fa9e3c784b6abbb`
- Quell-SVM: `sapcc-hana-svm`
- Ziel-FSX für ONTAP Dateisystem: `FsxId05f7f00af49dc7a3e`
- Ziel-SVM: `sapcc-backup-target-zone5`

Peer-FSX für ONTAP-Filesysteme

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

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

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

`peer-addrs` Sind Cluster-IPs des Ziel-Clusters.

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

Peer-SVMs

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

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

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

Erstellen eines Ziel-Volumes

Sie müssen das Ziel-Volume mit dem Typ erstellen `DP` So markieren Sie es als Replikationsziel.

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

SnapMirror-Richtlinie erstellen

Die SnapMirror-Richtlinie und die hinzugefügte Regel definieren die Aufbewahrung und das SnapMirror-Etikett, um die zu replizierenden Snapshots zu identifizieren. Wenn Sie die SnapCenter-Richtlinie später erstellen, müssen Sie dasselbe Etikett verwenden.

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

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

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

SnapMirror Beziehung erstellen

Jetzt wird die Beziehung zwischen dem Quell- und dem Ziel-Volume sowie der Typ XDP und der zuvor erstellten Richtlinie definiert.

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

SnapMirror initialisieren

Mit diesem Befehl wird die erste Replikation gestartet. Bei diesem Vorgang werden alle Daten vom Quell-Volume auf das Ziel-Volume übertragen.

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

Sie können den Status der Replikation mit überprüfen `snapmirror show` Befehl.

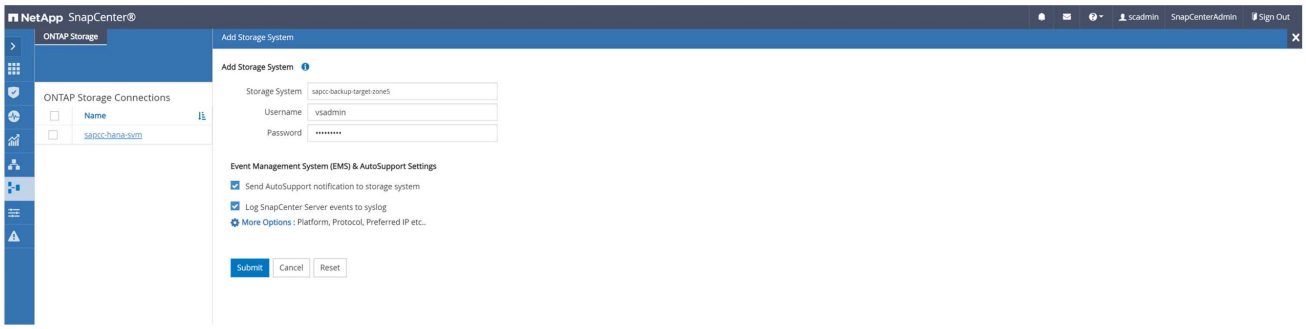
```
FsxId05f7f00af49dc7a3e::> snapmirror show

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

```
FsxId05f7f00af49dc7a3e::> snapmirror show

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

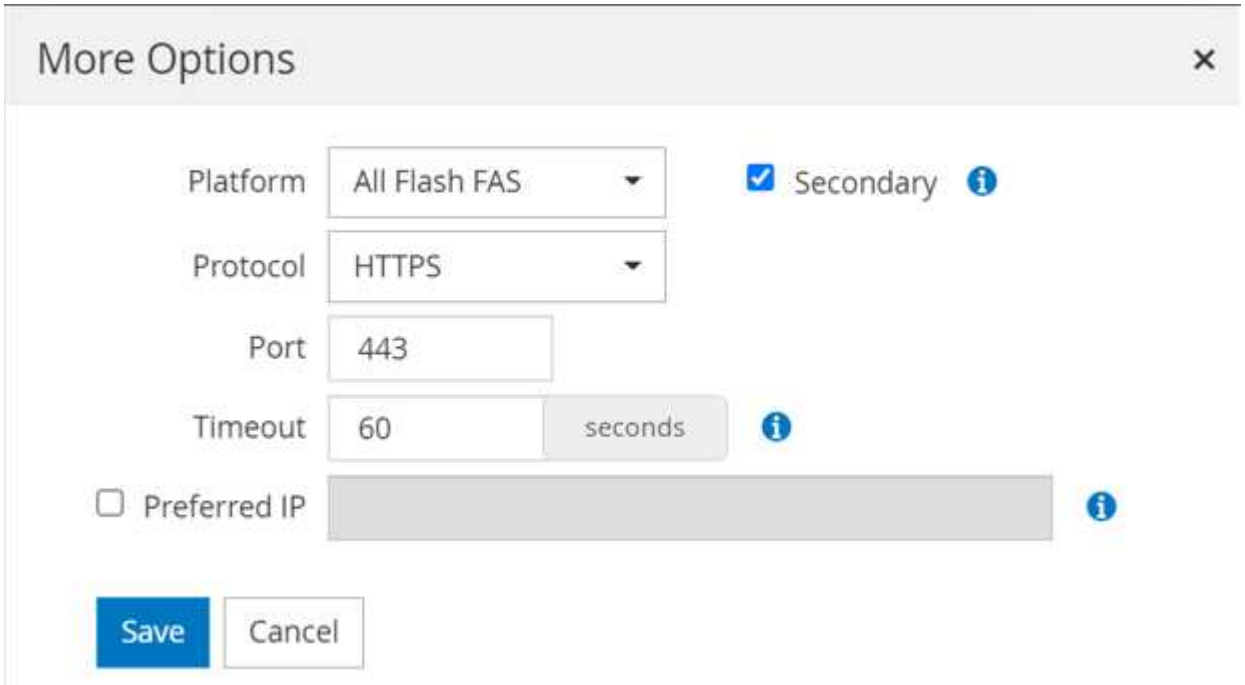
Fügen Sie eine Backup-SVM zu SnapCenter hinzu

So fügen Sie eine Backup-SVM zu SnapCenter hinzu:

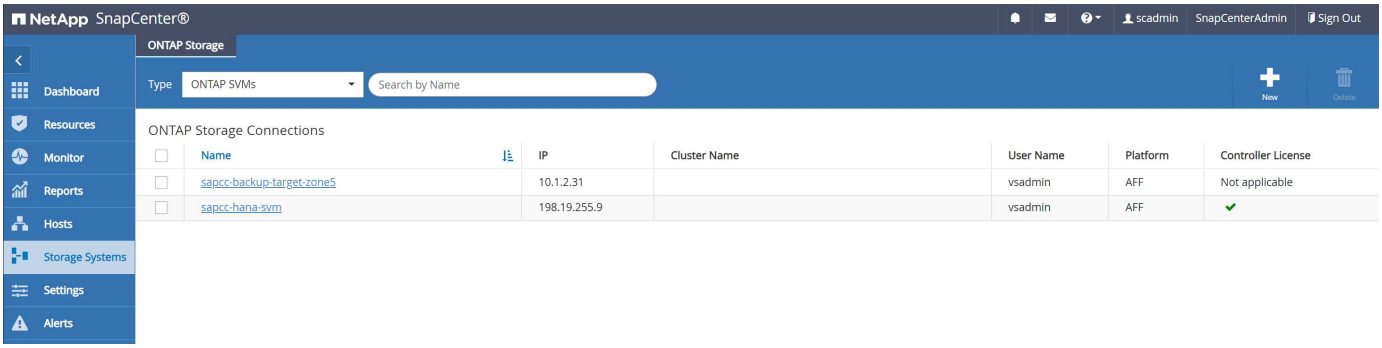
1. Konfigurieren Sie die SVM, auf der sich das SnapVault Ziel-Volume in SnapCenter befindet.



2. Wählen Sie im Fenster Weitere Optionen als Plattform All-Flash-FAS aus, und wählen Sie Sekundär aus.



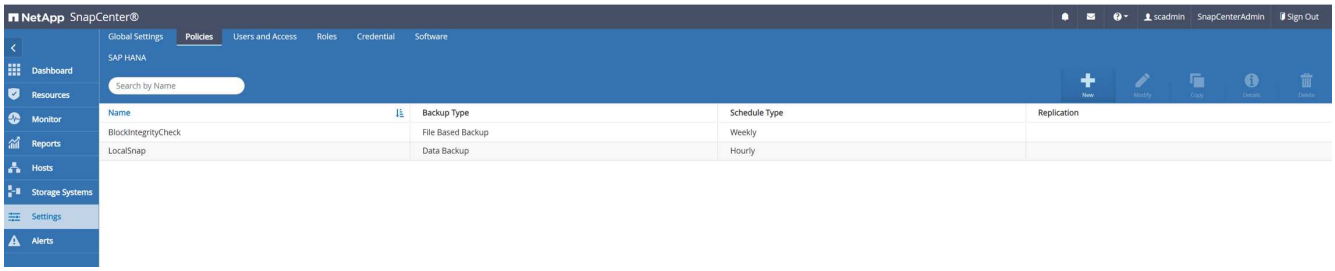
Die SVM ist jetzt in SnapCenter verfügbar.



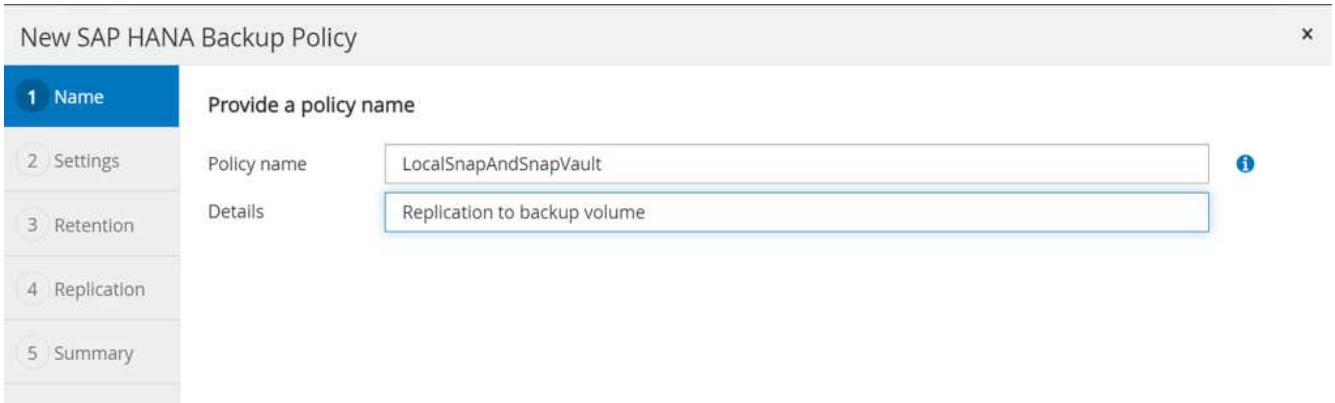
Erstellen einer neuen SnapCenter-Richtlinie für Backup-Replizierung

Sie müssen eine Richtlinie für die Backup-Replikation wie folgt konfigurieren:

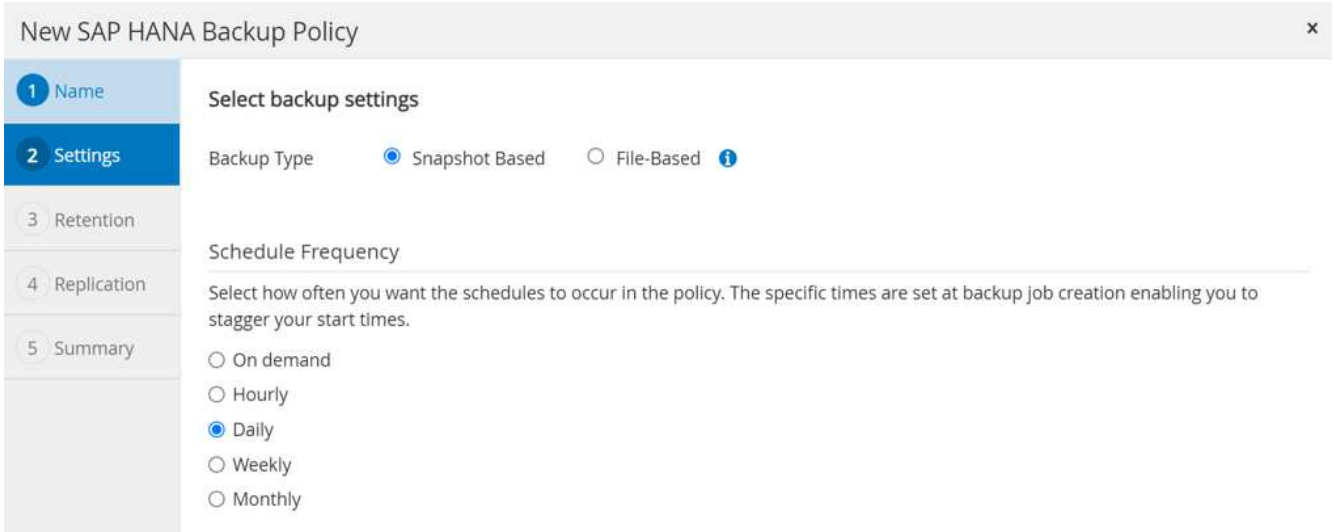
1. Geben Sie einen Namen für die Richtlinie ein.



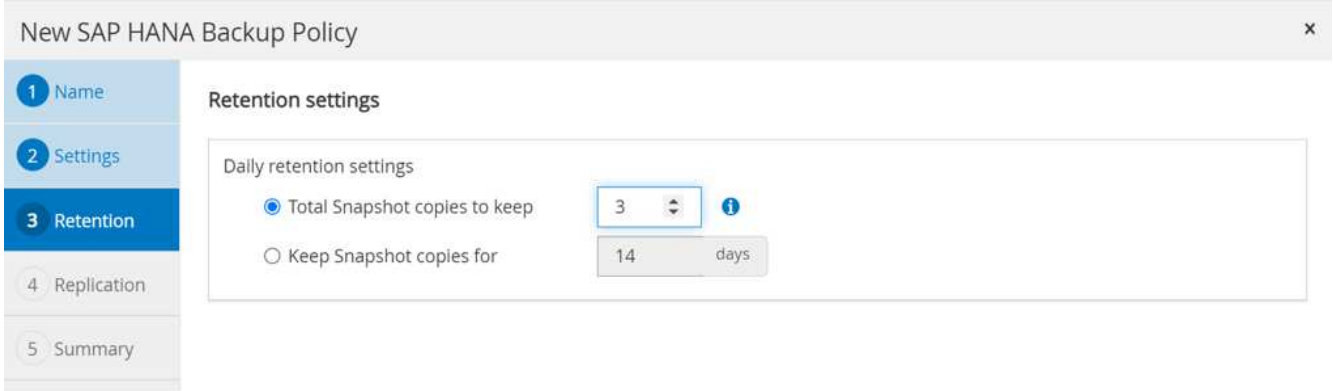
2. Wählen Sie Snapshot Backup und eine Zeitplanfrequenz aus. Für die Backup-Replizierung wird täglich verwendet.



3. Wählen Sie die Aufbewahrung für die Snapshot-Backups aus.

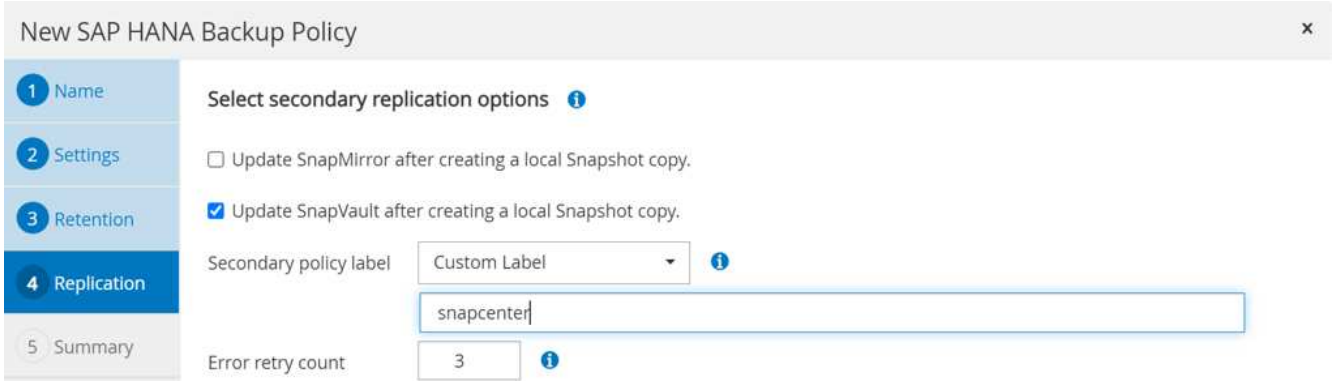


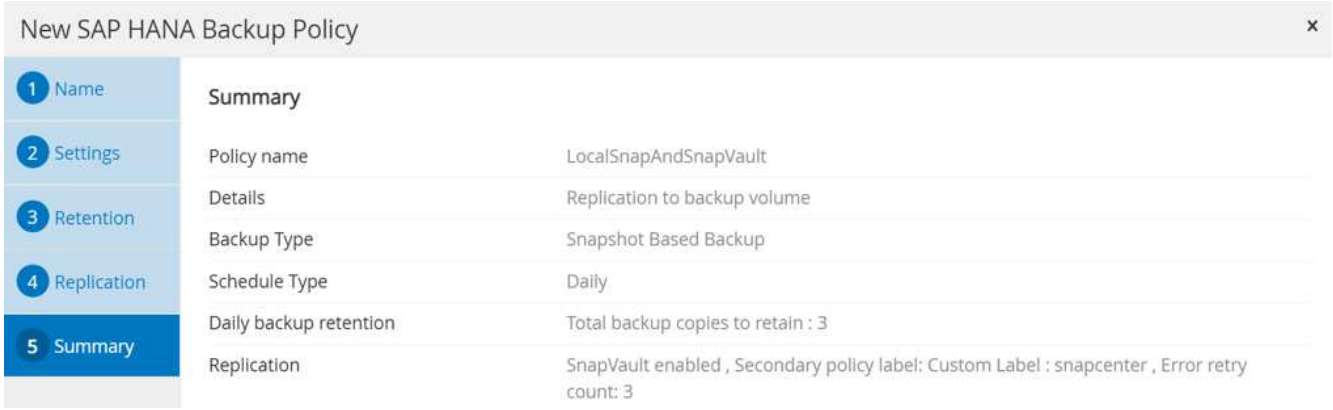
Dies ist die Aufbewahrung für die täglichen Snapshot Backups, die im primären Storage erstellt wurden. Die Aufbewahrung für sekundäre Backups auf dem SnapVault-Ziel wurde bereits mit dem Befehl „Add rule“ auf der ONTAP-Ebene konfiguriert. Siehe „Konfigurieren von Replikationsbeziehungen auf FSX für ONTAP-Dateisysteme“ (xref).



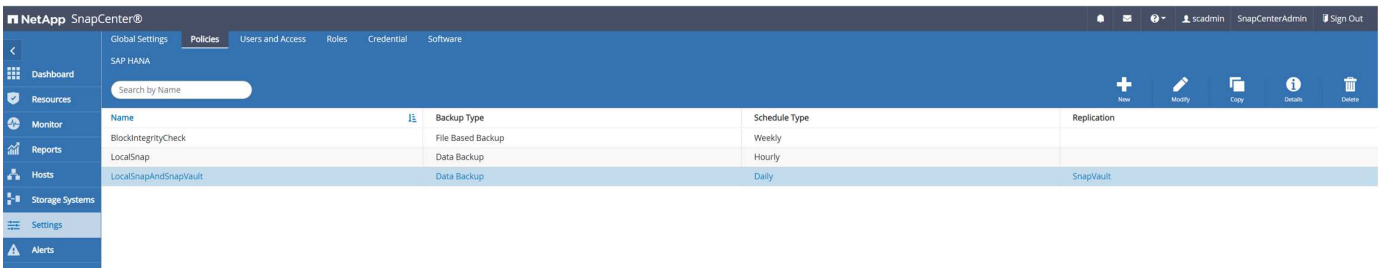
4. Wählen Sie das Feld SnapVault aktualisieren aus, und geben Sie eine benutzerdefinierte Bezeichnung an.

   Dieses Etikett muss mit der SnapMirror-Bezeichnung im übereinstimmen `add rule` Befehl auf ONTAP-Ebene.



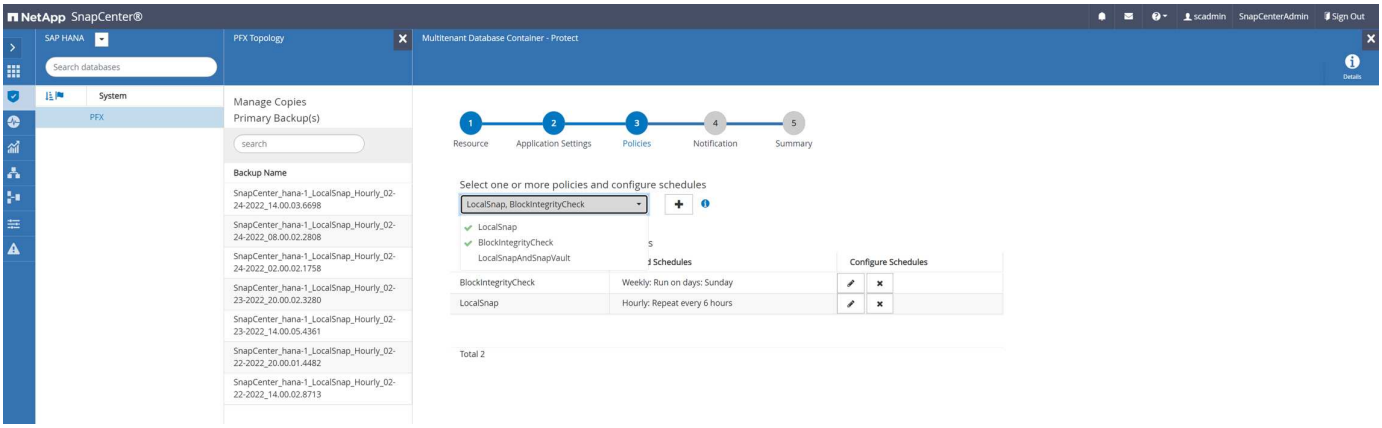


Die neue SnapCenter-Richtlinie ist jetzt konfiguriert.

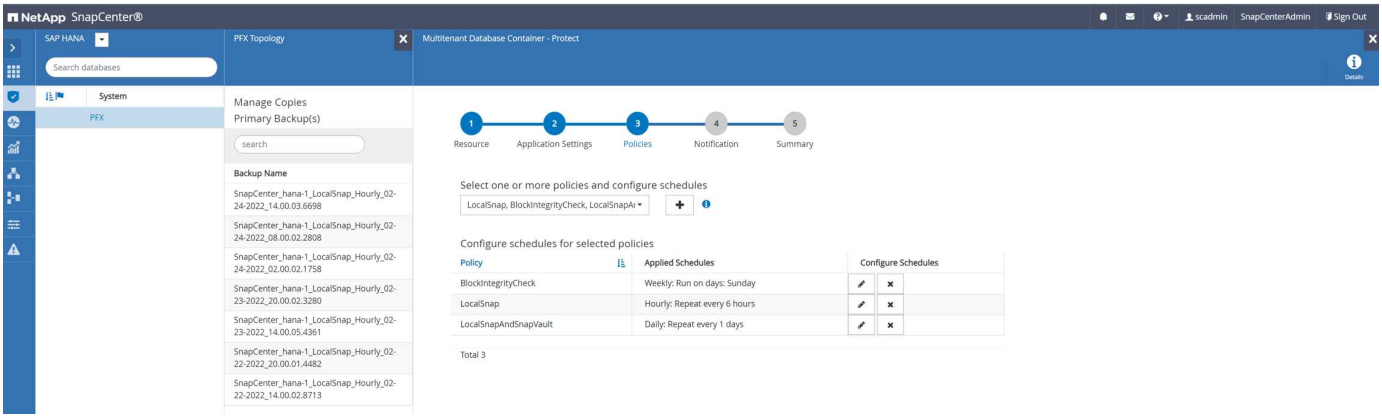


Fügen Sie eine Richtlinie zum Ressourcenschutz hinzu

Sie müssen die neue Richtlinie der HANA-Ressourcenschutzkonfiguration hinzufügen, wie in der folgenden Abbildung dargestellt.



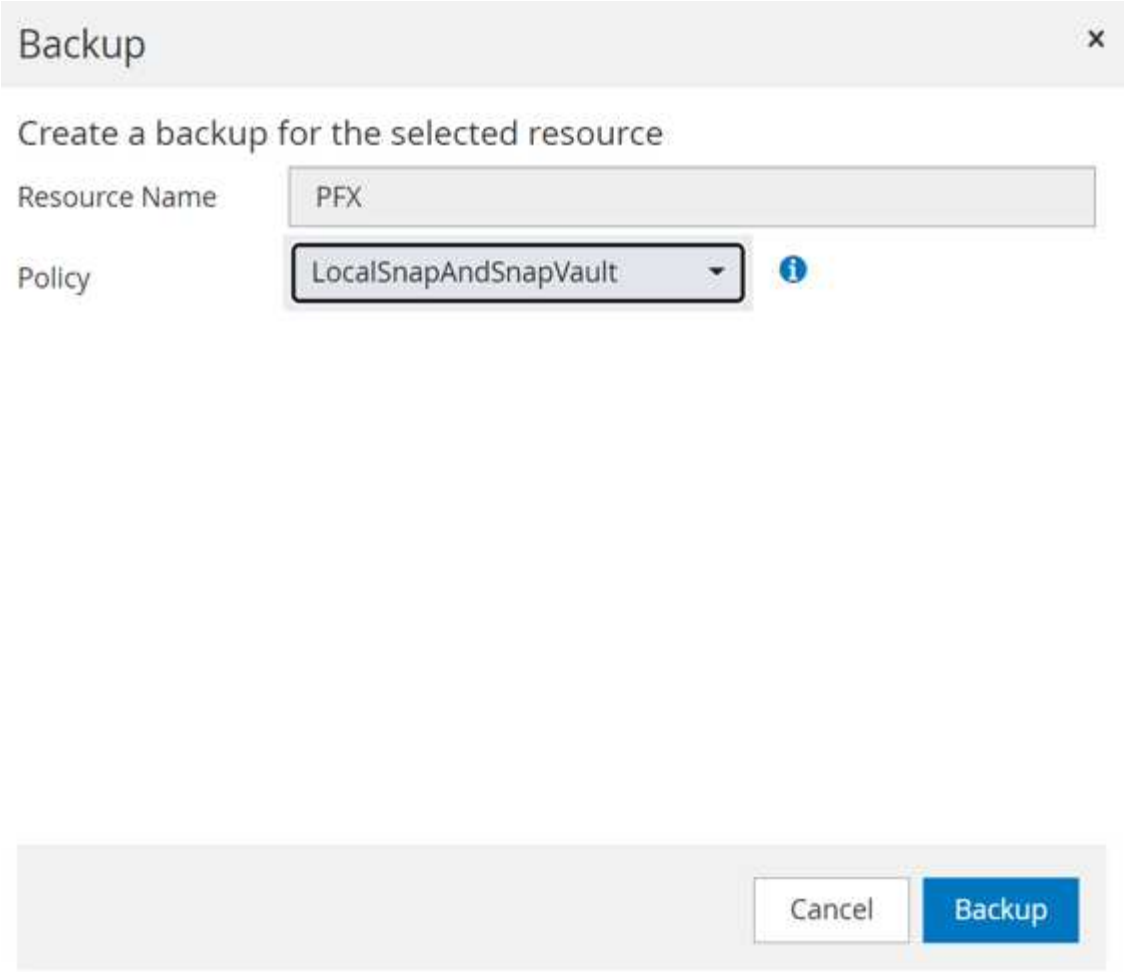
Ein täglicher Zeitplan wird in unserem Setup festgelegt.



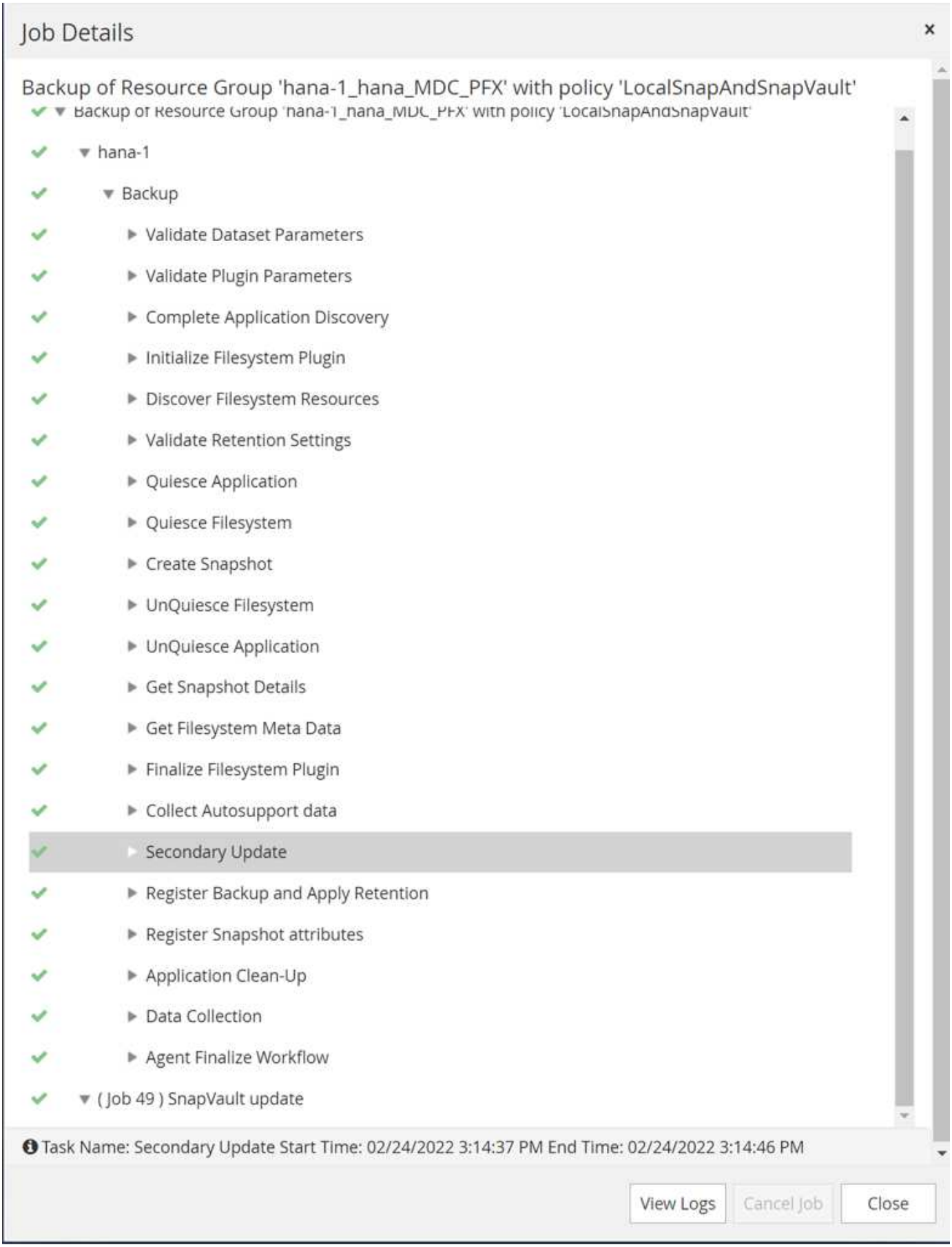
Erstellen Sie ein Backup mit Replikation

Ein Backup wird auf dieselbe Weise wie eine lokale Snapshot Kopie erstellt.

Um ein Backup mit Replikation zu erstellen, wählen Sie die Richtlinie aus, die die Backup-Replikation enthält, und klicken Sie auf Backup.



Im Jobprotokoll von SnapCenter wird der Schritt sekundäre Aktualisierung angezeigt, der einen SnapVault-Aktualisierungsvorgang initiiert. Replizierung hat geänderte Blöcke vom Quell-Volume auf das Ziel-Volume repliziert.



Auf dem FSX für ONTAP Filesystem wird ein Snapshot auf dem Quell-Volume mit dem SnapMirror Label

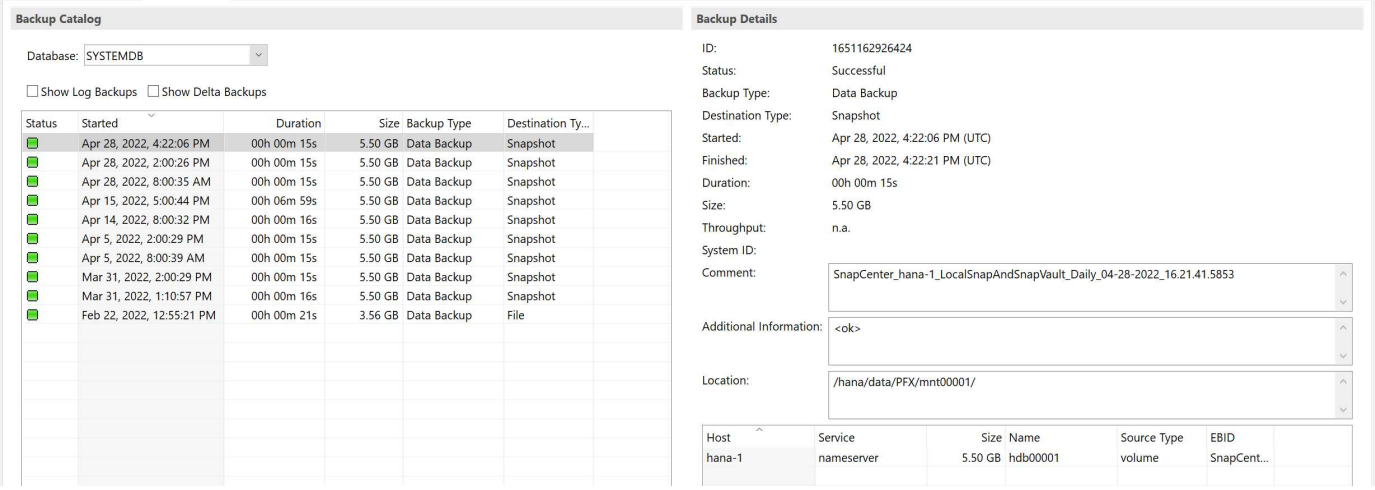
erstellt. `snapcenter`, Wie in der SnapCenter-Richtlinie konfiguriert.

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

snapcenter
8 entries were displayed.
```

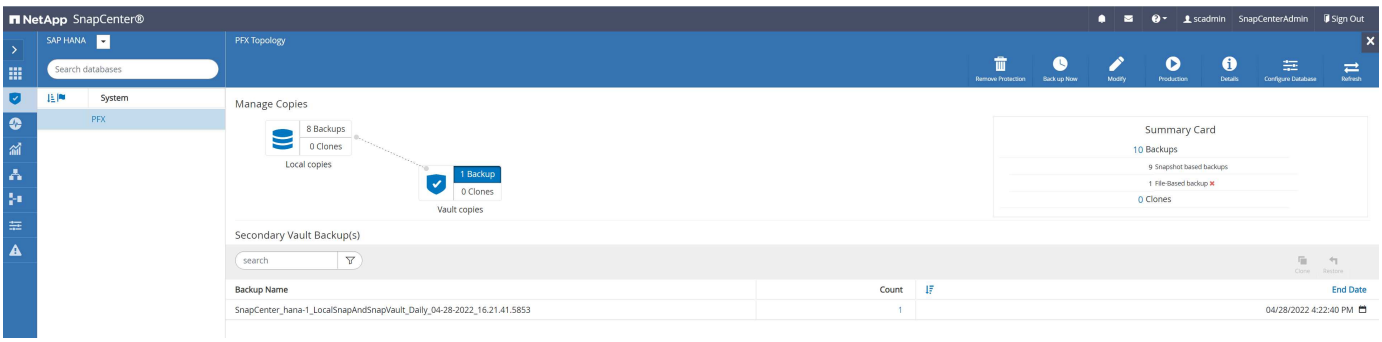
Auf dem Ziel-Volume wird eine Snapshot Kopie mit demselben Namen erstellt.

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

Auch das neue Snapshot-Backup ist im HANA-Backup-Katalog enthalten.



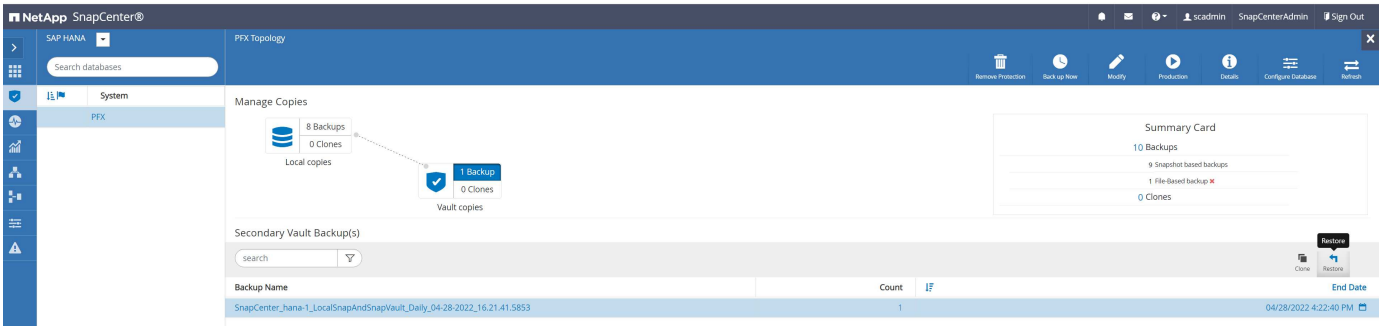
In SnapCenter können Sie die replizierten Backups auflisten, indem Sie in der Topologieansicht auf Vault Kopien klicken.



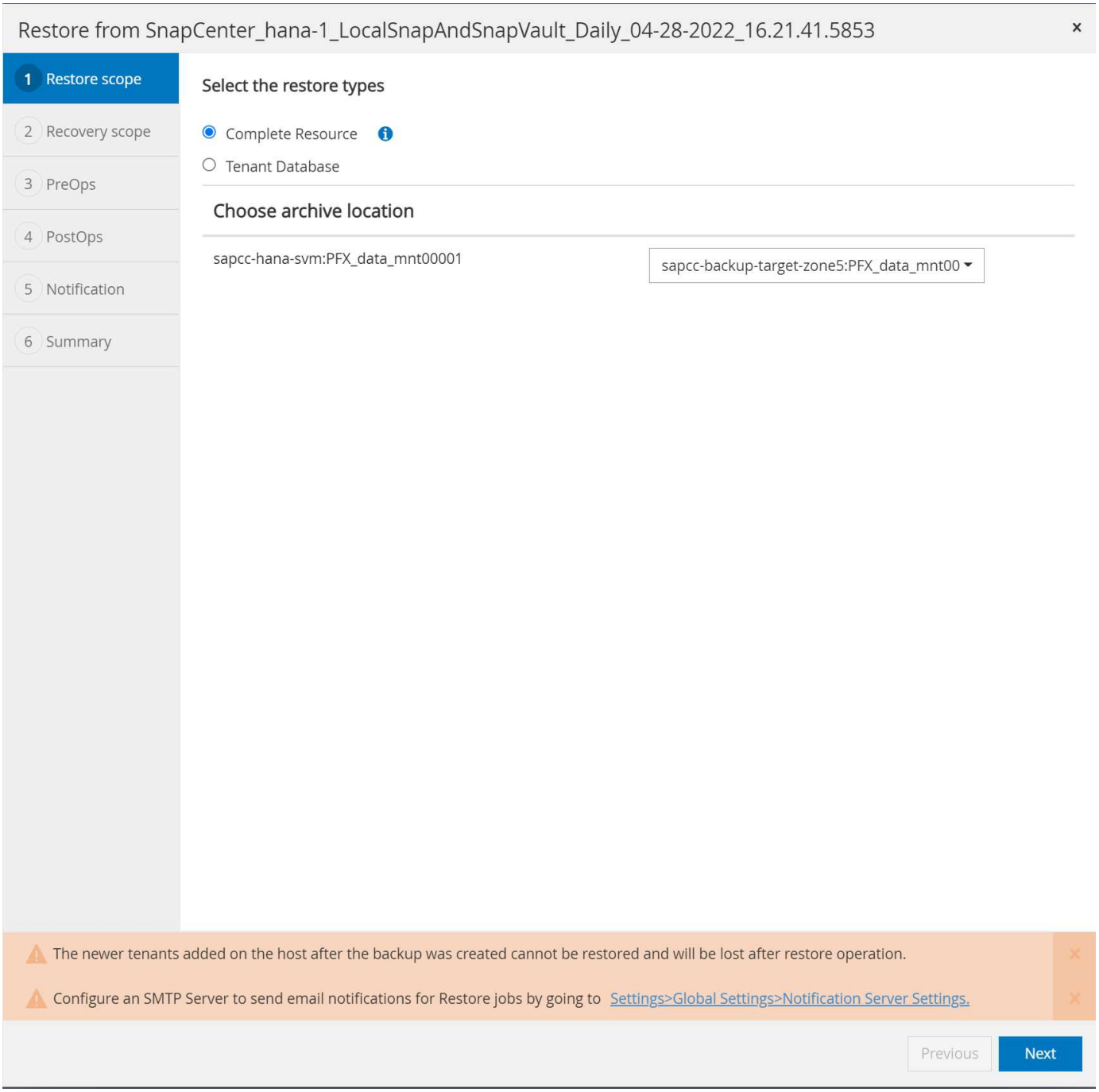
Wiederherstellung im Sekundär-Storage

Führen Sie die folgenden Schritte aus, um im Sekundärspeicher wiederherzustellen und eine Wiederherstellung durchzuführen:

Um die Liste aller Backups auf dem sekundären Storage abzurufen, klicken Sie in der Ansicht SnapCenter Topology auf Vault Kopien, wählen Sie dann ein Backup aus und klicken Sie auf Wiederherstellen.



Das Dialogfeld Wiederherstellen zeigt die sekundären Speicherorte an.



Weitere Restore- und Recovery-Schritte sind mit denen identisch, die bei einem Snapshot Backup im Primärspeicher besprochen wurden.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- FSX für NetApp ONTAP Benutzerhandbuch – Was ist Amazon FSX für NetApp ONTAP?

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

- Ressourcen-Seite zu SnapCenter

"https://www.netapp.com/us/documentation/snapcenter-software.aspx"

- SnapCenter-Softwaredokumentation

  "https://docs.netapp.com/us-en/snapcenter/index.html"

- TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter

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

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

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

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	Mai 2022	Erste Version.

Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter

TR-4614: SAP HANA Backup und Recovery mit SnapCenter

Nils Bauer, NetApp

Unternehmen benötigen heutzutage eine kontinuierliche, unterbrechungsfreie Verfügbarkeit ihrer SAP-Applikationen. Sie erwarten konsistente Performance angesichts stetig wachsender Datenvolumen und bei routinemäßigen Wartungsaufgaben wie System-Backups. Das Durchführen von Backups von SAP-Datenbanken ist eine wichtige Aufgabe, die erhebliche Performance-Auswirkungen auf das SAP-Produktionssystem haben kann.

Die Backup-Fenster schrumpfen, während die zu sichernden Daten immer größer werden. Somit ist es schwierig, mit minimalen Auswirkungen auf Geschäftsprozesse einen Zeitpunkt zu finden, in dem Backups durchgeführt werden können. Die Zeit, die zum Wiederherstellen und Wiederherstellen von SAP-Systemen benötigt wird, ist besorgt, da Ausfallzeiten bei SAP-Produktions- und nicht produktiven Systemen minimiert werden müssen, um Datenverlusten und Kosten für das Unternehmen zu reduzieren.

Folgende Punkte fassen die Herausforderungen zusammen, die mit SAP-Backup und -Recovery zu tun haben:

- **Performance-Auswirkungen auf SAP-Produktionssysteme.** herkömmliche Copy-basierte Backups führen in der Regel aufgrund der hohen Belastungen auf den Datenbankserver, das Storage-System und das Speichernetzwerk zu einer erheblichen Performance-Belastung für SAP-Produktionssysteme.
- **Schrumpfende Backup-Fenster.** herkömmliche Backups können nur vorgenommen werden, wenn nur wenige Dialoge oder Batch-Aktivitäten im SAP-System ausgeführt werden. Wenn SAP Systeme rund um die Uhr im Einsatz sind, gestaltet sich die Planung von Backups schwieriger.
- **Schnelles Datenwachstum.** für ein schnelles Datenwachstum und immer kleiner werdende Backup-Fenster sind laufende Investitionen in die Backup-Infrastruktur erforderlich. Das bedeutet, dass Sie mehr Tape-Laufwerke, zusätzlichen Backup-Speicherplatz und schnellere Backup-Netzwerke beschaffen müssen. Außerdem müssen Sie die laufenden Kosten für die Speicherung und das Management der Tape-

Ressourcen tragen. Inkrementelle oder differenzielle Backups können diese Probleme beheben. Allerdings führt diese Anordnung zu einem sehr langsamen, umständlichen und komplexen Restore-Prozess, der sich schwieriger überprüfen lässt. Derartige Systeme verkürzen in der Regel die Zeiten der Recovery-Zeit (Recovery Time Objective, RTO) und des Recovery-Zeitpunkts (RPO) und sind für das Unternehmen nicht akzeptabel.

- **Steigende Kosten von Ausfallzeiten.** ungeplante Ausfallzeiten eines SAP-Systems haben typischerweise Auswirkungen auf die Geschäftsfinanzen. Die Notwendigkeit der Wiederherstellung des SAP Systems erfordert einen Großteil aller ungeplanten Ausfallzeiten. Daher bestimmt die gewünschte RTO das Design der Backup- und Recovery-Architektur.
- **Backup- und Wiederherstellungszeit für SAP-Upgrade-Projekte.** der Projektplan für ein SAP-Upgrade beinhaltet mindestens drei Backups der SAP-Datenbank. Diese Backups reduzieren die für den Upgrade-Prozess verfügbare Zeit erheblich. Die Entscheidung zum Fortfahren hängt im Allgemeinen von der Zeit ab, die zur Wiederherstellung der Datenbank aus dem zuvor erstellten Backup benötigt wird. Statt ein System in den vorherigen Zustand wiederherzustellen, bietet eine schnelle Wiederherstellung mehr Zeit zur Behebung von Problemen, die bei einem Upgrade auftreten können.

Die Lösung von NetApp

Mit der NetApp Snapshot Technologie können Datenbank-Backups innerhalb von Minuten erstellt werden. Wie lange es dauert, eine Snapshot Kopie zu erstellen, ist unabhängig von der Größe der Datenbank, da bei Snapshot Kopien keine physischen Datenblöcke auf der Storage-Plattform verschoben werden. Weil die NetApp Snapshot Technologie keine Datenblöcke verschiebt oder kopiert, wirkt sie sich nicht auf die Performance des produktiven SAP Systems aus, wenn Snapshot Kopie erstellt oder Daten im aktiven Filesystem geändert werden. Daher kann die Erstellung von Snapshot Kopien ohne die Berücksichtigung von Spitzenzeiten oder Batch-Aktivitäten geplant werden. SAP- und NetApp-Kunden planen normalerweise mehrere Online Snapshot-Backups pro Tag, so dass beispielsweise alle vier Stunden üblich sind. Diese Snapshot Backups werden in der Regel drei bis fünf Tage auf dem primären Storage-System gespeichert, bevor sie entfernt werden.

Snapshot Kopien bieten auch wichtige Vorteile für Wiederherstellung und Recovery. NetApp SnapRestore Daten-Recovery-Software ermöglicht auf der Grundlage von verfügbaren Snapshot Kopien die Wiederherstellung einer gesamten Datenbank oder eines Teils einer Datenbank zu einem beliebigen Zeitpunkt. Solche Wiederherstellungen sind innerhalb von wenigen Minuten abgeschlossen, unabhängig von der Größe der Datenbank. Da mehrere Online Snapshot Backups tagsüber erstellt werden, verringert sich die für den Recovery-Prozess erforderliche Zeit im Vergleich zu einem herkömmlichen Backup-Ansatz deutlich. Da eine Wiederherstellung mit einer Snapshot-Kopie durchgeführt werden kann, die nur wenige Stunden alt ist (und nicht bis zu 24 Stunden), müssen weniger Transaktions-Logs angewendet werden. Daher reduziert sich die RTO auf mehrere Minuten – statt auf mehrere Stunden für herkömmliche Single-Cycle Tape Backups.

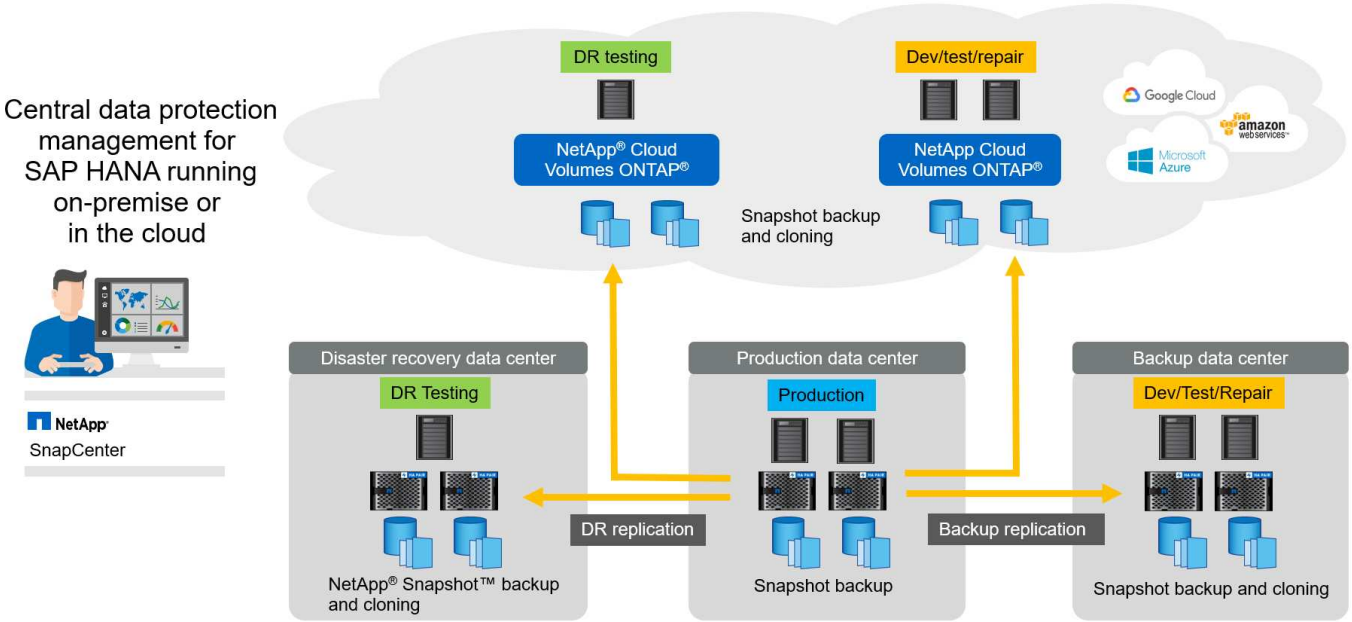
Backups von Snapshot-Kopien werden auf demselben Festplattensystem wie die aktiven Online-Daten gespeichert. Daher empfiehlt NetApp, Backups von Snapshot-Kopien als Ergänzung zu verwenden, anstatt Backups an einen sekundären Standort zu ersetzen. Die meisten Restore- und Recovery-Aktionen werden mithilfe von SnapRestore im primären Storage-System durchgeführt. Restores von einem Sekundärstandort sind nur nötig, wenn das primäre Storage-System, das die Snapshot-Kopien enthält, beschädigt ist. Der sekundäre Standort kann auch verwendet werden, wenn ein Backup, das nicht mehr in einer Snapshot Kopie verfügbar ist, wiederhergestellt werden muss: Ein monatliches Backup.

Ein Backup an einen sekundären Standort basiert auf Snapshot-Kopien, die auf dem primären Storage erstellt wurden. Somit werden die Daten direkt aus dem primären Storage-System eingelesen, ohne dass dabei der SAP Datenbankserver belastet wird. Der primäre Storage kommuniziert direkt mit dem sekundären Storage und sendet mithilfe eines NetApp SnapVault Disk-to-Disk Backups die Backup-Daten an das Ziel.

SnapVault bietet im Vergleich zu herkömmlichen Backups deutliche Vorteile. Nach einem ersten Datentransfer, bei dem alle Daten vom Quell- zum Ziel-Volume übertragen wurden, kopieren bei allen nachfolgenden

Backups nur die geänderten Blöcke in den sekundären Storage. Somit werden die Last auf dem primären Storage-System und der Zeitaufwand für ein Vollbackup deutlich reduziert. Da SnapVault nur die geänderten Blöcke am Ziel speichert, benötigt ein vollständiges Datenbank-Backup weniger Festplattenspeicher.

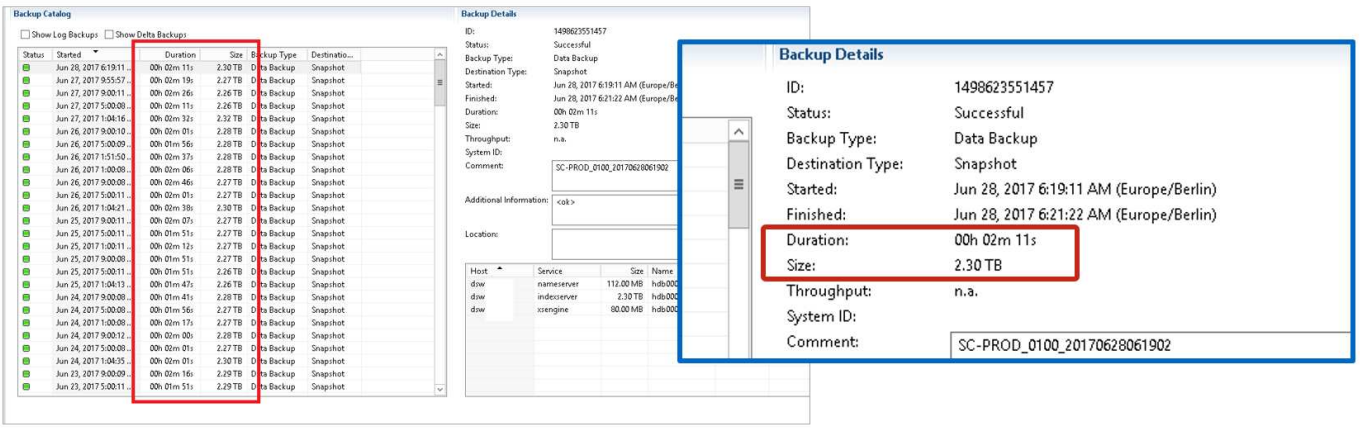
Die Lösung kann zudem nahtlos auf ein Hybrid-Cloud-Betriebsmodell erweitert werden. Die Datenreplizierung für die Disaster Recovery oder für ein externes Backup kann von lokalen NetApp ONTAP Systemen auf Cloud Volumes ONTAP Instanzen in der Cloud durchgeführt werden. SnapCenter kann als zentrales Tool für das Management der Datensicherung und der Datenreplizierung eingesetzt werden – unabhängig davon, ob das SAP HANA System lokal oder in der Cloud ausgeführt wird. Die folgende Abbildung zeigt einen Überblick über die Backup-Lösung.



Laufzeit von Snapshot-Backups

Der nächste Screenshot zeigt ein Kunde im HANA Studio, in dem SAP HANA auf NetApp Storage läuft. Der Kunde erstellt mithilfe von Snapshot Kopien ein Backup der HANA Datenbank. Das Bild zeigt, dass die HANA-Datenbank (ca. 2,3 TB groß) mithilfe der Snapshot-Backup-Technologie in 2 Minuten und 11 Sekunden gesichert wird.

> Der größte Teil der gesamten Laufzeit des Backup-Workflows ist die Zeit, die zur Ausführung des HANA-Backup-Speicherpunktvorgangs benötigt wird. Dieser Schritt hängt von der Last der HANA-Datenbank ab. Das Snapshot Backup selbst ist in wenigen Sekunden abgeschlossen.



Vergleich der Recovery-Zeitvorgaben

Dieser Abschnitt enthält einen RTO-Vergleich von Datei- und Storage-basierten Snapshot-Backups. Das RTO wird durch die Summe der Zeit, die zur Wiederherstellung der Datenbank benötigt wird, und der Zeit definiert, die zum Starten und Wiederherstellen der Datenbank erforderlich ist.

Benötigte Zeit zum Wiederherstellen der Datenbank

Bei einem dateibasierten Backup hängt die Restore-Zeit von der Größe der Datenbank und der Backup-Infrastruktur ab, die die Restore-Geschwindigkeit in Megabyte pro Sekunde festlegt. Wenn die Infrastruktur beispielsweise einen Restore-Vorgang mit einer Geschwindigkeit von 250 MB/s unterstützt, dauert es etwa 1 Stunde und 10 Minuten, um eine Datenbank mit einer Größe von 1 TB wiederherzustellen.

Die Restore-Dauer ist bei Backups der Storage Snapshot Kopien unabhängig von der Größe der Datenbank und liegt im Bereich von einigen Sekunden, wenn die Wiederherstellung im Primärspeicher durchgeführt werden kann. Eine Wiederherstellung aus sekundärem Storage ist nur bei einem Notfall erforderlich, wenn der primäre Storage nicht mehr verfügbar ist.

Benötigte Zeit zum Starten der Datenbank

Die Startzeit der Datenbank hängt von der Größe der Zeile und des Spaltenspeichers ab. Für den Spaltenspeicher hängt die Startzeit auch davon ab, wie viele Daten während des Datenbankstartens vorgeladen werden. In den folgenden Beispielen gehen wir davon aus, dass die Startzeit 30 Minuten beträgt. Die Startzeit ist bei einem dateibasierten Restore und Recovery gleich, sowie bei einem Restore und Recovery auf Basis von Snapshot.

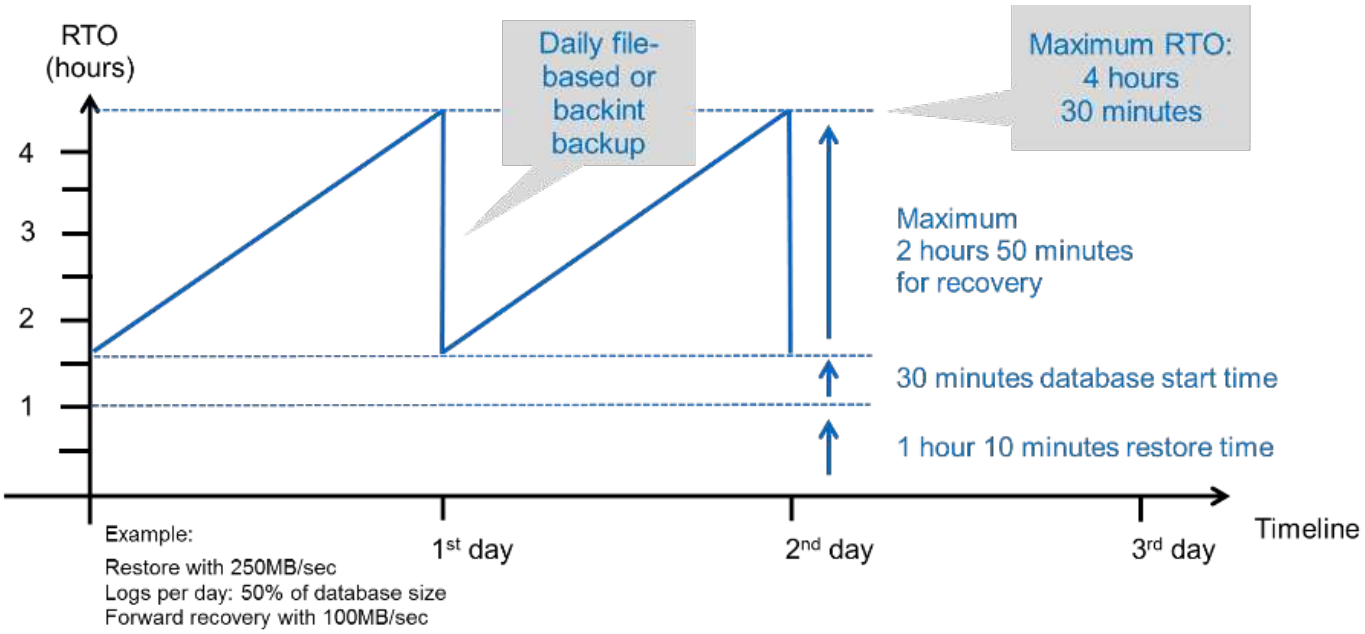
Benötigte Zeit für das Recovery von Datenbanken

Die Wiederherstellungszeit hängt von der Anzahl der Protokolle ab, die nach der Wiederherstellung angewendet werden müssen. Diese Zahl hängt von der Häufigkeit ab, mit der Daten-Backups erstellt werden.

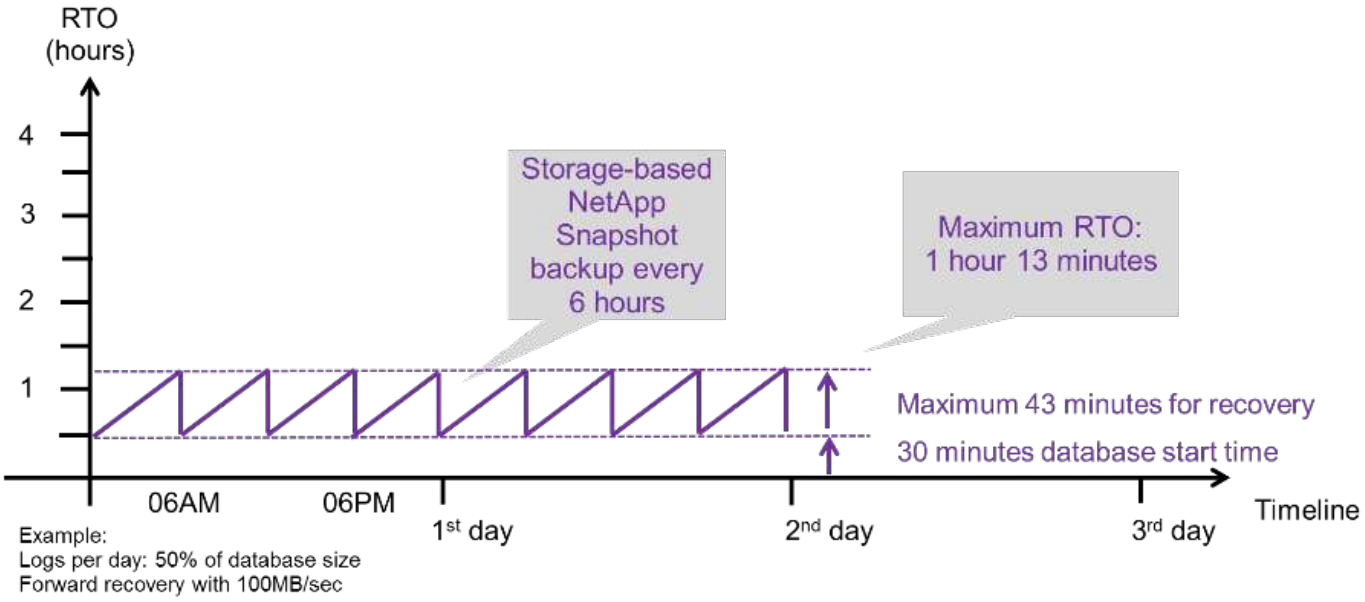
Bei dateibasierten Daten-Backups wird der Backup-Zeitplan normalerweise einmal pro Tag erstellt. Eine höhere Backup-Frequenz ist normalerweise nicht möglich, da das Backup die Produktions-Performance beeinträchtigt. Daher müssen im schlimmsten Fall alle Protokolle, die während des Tages geschrieben wurden, während der Forward Recovery angewendet werden.

Backups von Storage Snapshot Kopien werden in der Regel häufiger geplant, da sie die Performance der SAP HANA Datenbank nicht beeinträchtigen. Wenn beispielsweise alle sechs Stunden Snapshot Kopien Backups geplant werden, wäre die Recovery-Zeit im schlimmsten Fall ein Viertel der Recovery-Zeit für ein dateibasiertes Backup (6 Stunden / 24 Stunden = ¼).

Die folgende Abbildung zeigt ein RTO-Beispiel für eine 1-TB-Datenbank, wenn dateibasierte Daten-Backups verwendet werden. In diesem Beispiel wird ein Backup einmal pro Tag erstellt. Die RTO unterscheidet sich je nach dem Zeitpunkt der Wiederherstellung und des Recovery. Falls die Restore- und Recovery-Vorgänge unmittelbar nach dem Backup durchgeführt wurden, basiert die RTO in erster Linie auf der Restore-Zeit, die in dem Beispiel 1 Stunde und 10 Minuten beträgt. Die Recovery-Zeit stieg auf 2 Stunden und 50 Minuten, wenn Restore und Recovery unmittelbar vor dem nächsten Backup durchgeführt wurden und die maximale RTO 4 Stunden und 30 Minuten betrug.



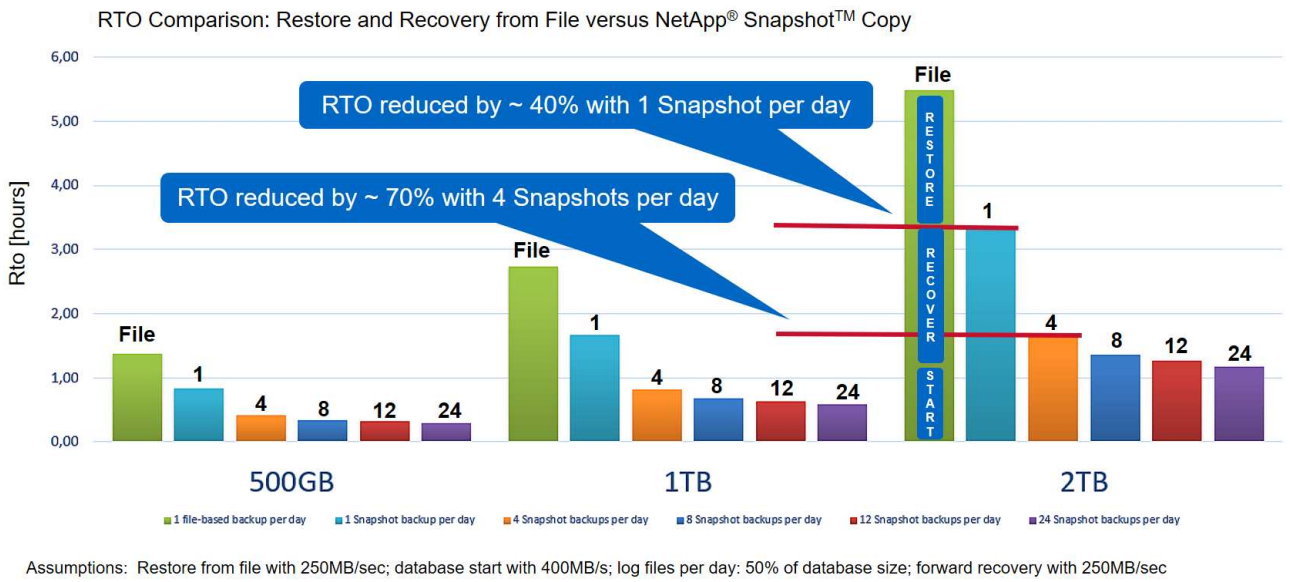
Die folgende Abbildung zeigt ein RTO-Beispiel für eine 1-TB-Datenbank, wenn Snapshot Backups verwendet werden. Bei Storage-basierten Snapshot Backups hängt die RTO nur von der Startzeit der Datenbank und der Wiederherstellungszeit ab, da die Wiederherstellung unabhängig von der Größe der Datenbank in wenigen Sekunden abgeschlossen wurde. Die Recovery-Zeit bis zur Vorwärtszeit wird auch abhängig vom Zeitpunkt der Wiederherstellung und der Wiederherstellung erhöht. Aufgrund der höheren Backup-Häufigkeit (in diesem Beispiel alle sechs Stunden) beträgt die Recovery-Zeit höchstens 43 Minuten. In diesem Beispiel beträgt die maximale RTO 1 Stunde und 13 Minuten.



Die folgende Abbildung zeigt einen RTO-Vergleich von dateibasierten und Storage-basierten Snapshot Backups für unterschiedliche Datenbankgrößen und verschiedene Häufigkeit von Snapshot-Backups. Der grüne Balken zeigt das dateibasierte Backup an. Die anderen Balken zeigen Backups von Snapshot Kopien mit unterschiedlichen Backup-Frequenzen.

Bei einem Daten-Backup pro Tag einer einzelnen Snapshot Kopie ist die RTO im Vergleich zu einem dateibasierten Daten-Backup bereits um 40 % reduziert. Die Reduzierung beträgt 70 %, wenn vier Snapshot-

Backups pro Tag erstellt werden. Die Abbildung zeigt auch, dass die Kurve konstant bleibt, wenn die Snapshot-Backup-Frequenz auf mehr als vier bis sechs Snapshot-Backups pro Tag erhöht wird. Unsere Kunden konfigurieren daher typischerweise vier bis sechs Snapshot Backups pro Tag.



Das Diagramm zeigt die RAM-Größe des HANA-Servers. Die Größe der Datenbank im Arbeitsspeicher wird auf die Hälfte des Server-RAM-Größen berechnet.

Die Restore- und Recovery-Zeit wird anhand folgender Annahmen berechnet. Die Datenbank kann mit 250 MBit/s wiederhergestellt werden. Die Anzahl der Log-Dateien pro Tag beträgt 50 % der Datenbankgröße. Beispielsweise erstellt eine Datenbank mit 1 TB 500MB an Log-Dateien pro Tag. Eine Wiederherstellung kann mit 100 Mbit/s durchgeführt werden.

Architektur von SnapCenter

SnapCenter ist eine einheitliche, skalierbare Plattform für applikationskonsistente Datensicherung. SnapCenter bietet zentrale Kontrolle und Überwachung und delegiert die Möglichkeit, dass Benutzer applikationsspezifische Backup-, Restore- und Klonaufgaben managen können. Mit SnapCenter erhalten Datenbank- und Storage-Administratoren ein Tool, mit dem sie Backup-, Wiederherstellungs- und Klonvorgänge für verschiedene Applikationen und Datenbanken managen können.

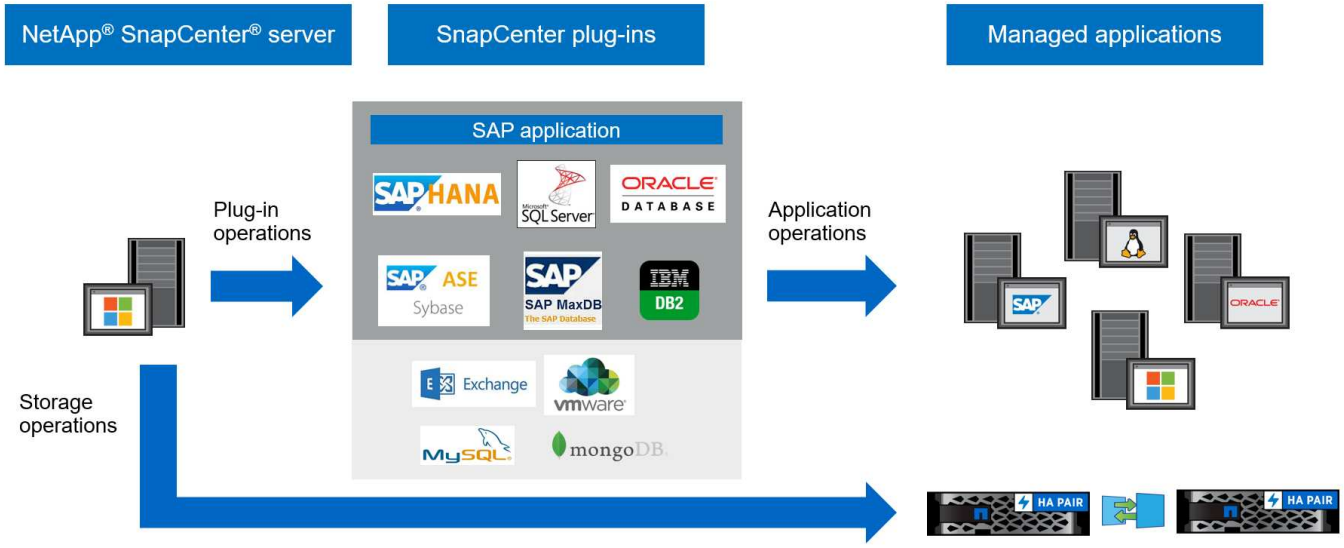
SnapCenter managt Daten über Endpunkte in der Data-Fabric-Architektur von NetApp hinweg. Daten können mit SnapCenter zwischen lokalen Umgebungen, zwischen On-Premises-Umgebungen und der Cloud sowie zwischen Private, Hybrid oder Public Clouds repliziert werden.

Komponenten von SnapCenter

SnapCenter umfasst den SnapCenter-Server, das SnapCenter-Plug-in-Paket für Windows und das SnapCenter-Plug-ins-Paket für Linux. Jedes Paket enthält SnapCenter-Plug-ins für diverse Applikations- und Infrastrukturkomponenten.

Mit den benutzerdefinierten SnapCenter Plug-ins können Sie Ihre eigenen Plug-ins erstellen und Ihre Applikation über dieselbe SnapCenter Oberfläche schützen.

In der folgenden Abbildung sind die SnapCenter Komponenten dargestellt.



SnapCenter SAP HANA Backup-Lösung

In diesem Abschnitt werden die Komponenten, unterstützte SAP HANA-Versionen und -Konfigurationen sowie in dieser Lösung verwendete Verbesserungen von SnapCenter 4.6 aufgeführt.

Lösungskomponenten

Die SnapCenter Backup-Lösung für SAP HANA umfasst folgende Bereiche:

- SAP HANA Daten-Backup mit Storage-basierten Snapshot Kopien:
  - Backup-Planung
  - Retentionmanagement
  - Allgemeine Ordnung und Sauberkeit des SAP HANA Backup-Katalogs
- Nicht-Datenvolumen (z. B. `/hana/shared`) Backup mit Storage-basierten Snapshot Kopien:
  - Backup-Planung
  - Retentionmanagement
- Replizierung an externe Backups oder Disaster-Recovery-Standorte:
  - Backup von SAP HANA Daten-Snapshots
  - Kein Datenvolumen
  - Aufbewahrungsmanagement wird auf externen Backup-Speichern konfiguriert
  - Allgemeine Ordnung und Sauberkeit des SAP HANA Backup-Katalogs
- Integritätsprüfungen der Datenbankblöcke mithilfe eines dateibasierten Backups:
  - Backup-Planung
  - Retentionmanagement
  - Allgemeine Ordnung und Sauberkeit des SAP HANA Backup-Katalogs

- Aufbewahrungsmanagement von HANA-Datenbankprotokoll-Backup:
  - Retentionmanagement basierend auf der Aufbewahrung von Daten-Backups
  - Allgemeine Ordnung und Sauberkeit des SAP HANA Backup-Katalogs
- Automatische Erkennung von HANA-Datenbanken
- Automatisiertes Restore und Recovery
- Restore einzelner Mandanten mit SAP HANA mandantenfähigen Datenbank-Containern (MDC) Systemen

Backups von Datenbankdateien werden von SnapCenter in Kombination mit dem Plug-in für SAP HANA ausgeführt. Das Plug-in löst einen Speicherpunkt für das SAP HANA Datenbank-Backup aus, sodass die Snapshot Kopien, die auf dem primären Storage-System erstellt werden, auf einem konsistenten Image der SAP HANA Datenbank basieren.

SnapCenter ermöglicht die Replizierung konsistenter Datenbank-Images an einen externen Backup- oder Disaster-Recovery-Standort mithilfe von SnapVault oder NetApp SnapMirror. Merkmal: In der Regel werden verschiedene Aufbewahrungsrichtlinien für Backups auf dem primären und externen Backup-Storage definiert. SnapCenter übernimmt die Aufbewahrung im Primärspeicher und ONTAP übernimmt die Aufbewahrung auf dem externen Backup-Storage.

Für ein vollständiges Backup aller mit SAP HANA verbundenen Ressourcen ermöglicht SnapCenter zudem das Backup aller nicht aus Daten stammenden Volumes über das SAP HANA Plug-in mit Storage-basierten Snapshot Kopien. Nicht vorhandene Datenvolumen können unabhängig vom Datenbank-Daten-Backup geplant werden, um individuelle Aufbewahrungs- und Sicherungsrichtlinien zu ermöglichen.

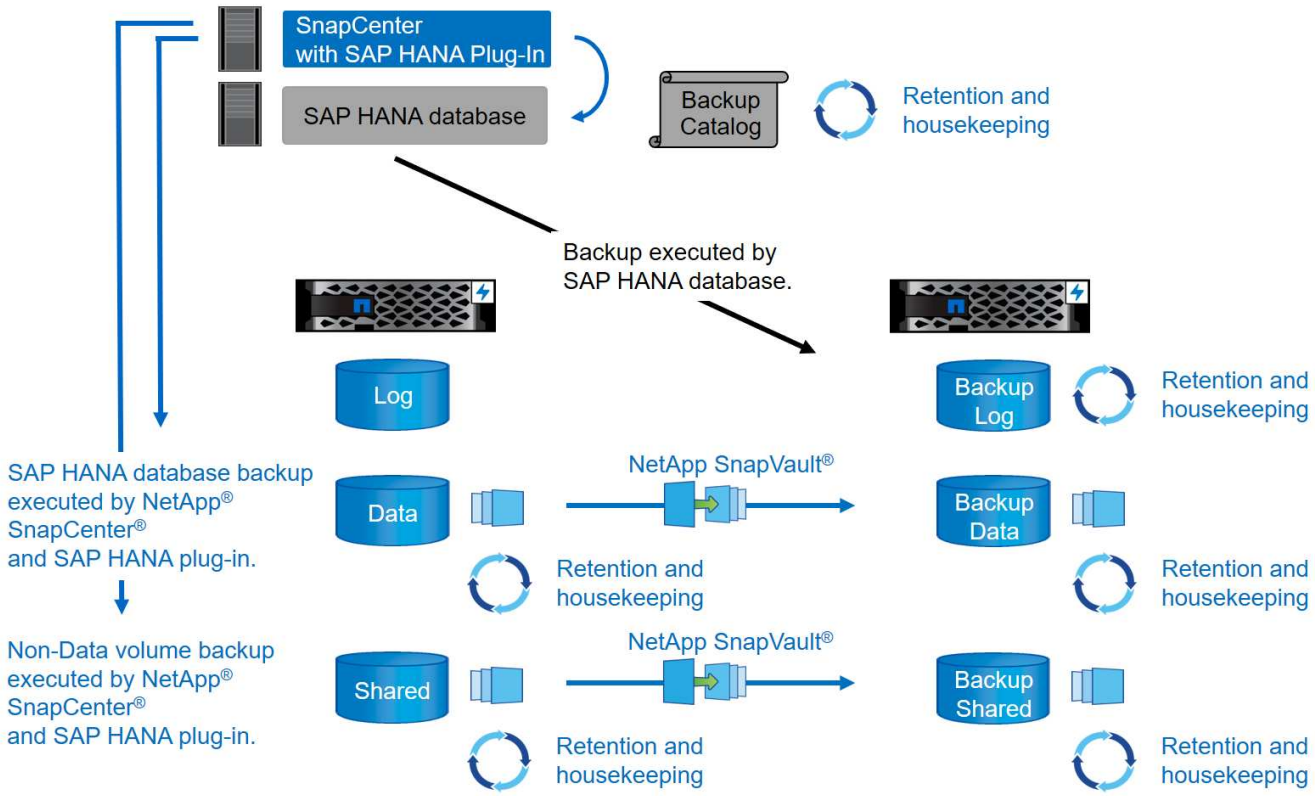
Die SAP HANA Datenbank führt automatisch Protokoll-Backups aus. Abhängig von den Vorgaben für Recovery-Zeitpunkte gibt es mehrere Optionen für den Speicherort der Log-Backups:

- Das Protokoll-Backup wird auf ein Storage-System geschrieben, das die Daten mithilfe der NetApp MetroCluster Storage-Software (HA) und Disaster Recovery synchron an einen zweiten Standort spiegelt.
- Das Protokoll-Backup-Ziel kann auf demselben primären Storage-System konfiguriert und dann mit SnapMirror synchron oder asynchron auf einen sekundären Storage repliziert werden.
- Das Backup-Ziel für das Protokoll kann auf demselben externen Backup-Storage konfiguriert werden, in dem die Datenbank-Backups mit SnapVault repliziert werden. Mit dieser Konfiguration stellt der externe Backup-Storage Verfügbarkeitsanforderungen wie den des primären Storage dar, sodass Log-Backups auf den externen Backup-Storage geschrieben werden können.

SAP empfiehlt, Storage-basierte Snapshot-Backups mit einem wöchentlichen dateibasierten Backup zu kombinieren, um eine Integritätsprüfung für Blöcke durchzuführen. Die Blockintegritätsprüfung kann innerhalb von SnapCenter ausgeführt werden. Basierend auf Ihren konfigurierbaren Aufbewahrungsrichtlinien managt SnapCenter die allgemeine Ordnung und Sauberkeit der Datendatei-Backups auf dem Primärspeicher, Backup von Protokolldateien und den SAP HANA Backup-Katalog.

> SnapCenter übernimmt die Aufbewahrung im Primärspeicher, während ONTAP die sekundäre Backup-Aufbewahrung managt.

Die folgende Abbildung zeigt eine Übersicht über die Datenbank- und Backup-Protokollierungs-Konfiguration, bei der die Protokoll-Backups auf einen NFS Mount des externen Backup-Storage geschrieben werden.



Bei der Ausführung eines Storage-basierten Snapshot-Backups von Volumes ohne Daten führt SnapCenter die folgenden Aufgaben aus:

1. Erstellung einer Storage-Snapshot-Kopie des nicht-Daten-Volumes
2. Ausführung eines SnapVault- oder SnapMirror-Updates für das Daten-Volume, falls konfiguriert
3. Löschen von Storage-Snapshot-Kopien im primären Storage auf Grundlage der festgelegten Aufbewahrungsrichtlinie.

Beim Ausführen eines Storage-basierten Snapshot Backups der SAP HANA Datenbank führt SnapCenter die folgenden Aufgaben durch:

1. Erstellung eines SAP HANA-Speicherpunktes für Backups, um ein konsistentes Image auf der Persistenzschicht zu erstellen.
2. Erstellung einer Storage-Snapshot-Kopie des Daten-Volumes
3. Registrierung des Storage-Snapshot-Backups im SAP HANA-Backup-Katalog
4. Veröffentlichung des Speicherpunktes SAP HANA Backup
5. Ausführung eines SnapVault- oder SnapMirror-Updates für das Daten-Volume, falls konfiguriert
6. Löschen von Storage-Snapshot-Kopien im primären Storage auf Grundlage der festgelegten Aufbewahrungsrichtlinie.
7. Löschen der Einträge des SAP HANA Backup-Katalogs, wenn die Backups nicht mehr im primären oder externen Backup-Speicher vorhanden sind.
8. Sobald ein Backup auf Grundlage der Aufbewahrungsrichtlinie oder manuell gelöscht wurde, löscht SnapCenter alle Log-Backups, die älter als das älteste Daten-Backup sind. Log-Backups werden im Dateisystem und im SAP HANA Backup-Katalog gelöscht.

Unterstützte SAP HANA-Versionen und -Konfigurationen

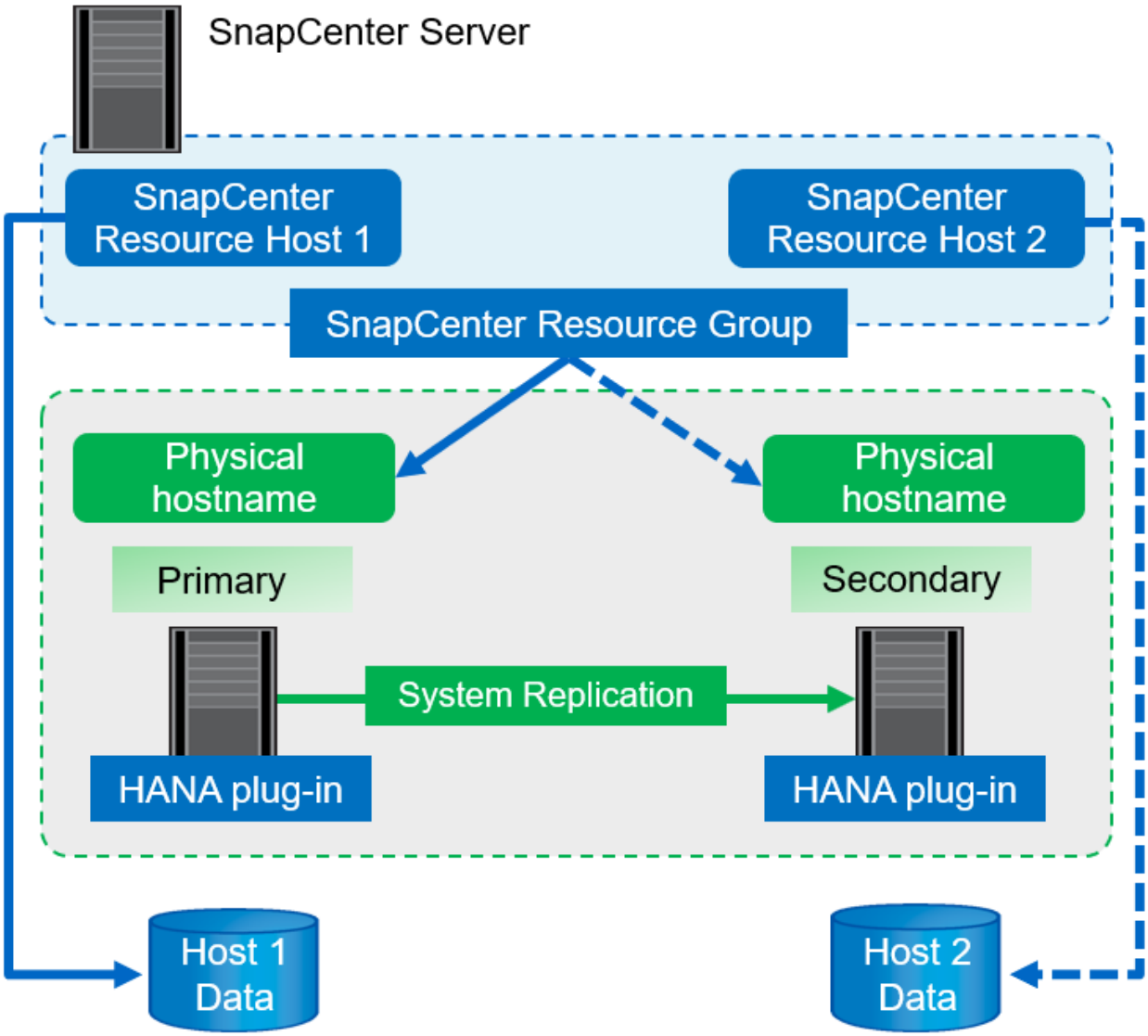
SnapCenter unterstützt SAP HANA Einzel- und Konfigurationen für mehrere Hosts über NFS- oder FC-Attached NetApp Storage-Systeme (AFF und FAS) sowie SAP HANA Systeme, die auf Cloud Volumes ONTAP bei AWS, Azure, der Google Cloud Platform und AWS FSX ONTAP über NFS ausgeführt werden.

SnapCenter unterstützt die folgenden SAP HANA-Architekturen und -Releases:

- SAP HANA Single-Container: SAP HANA 1.0 SPS12
- SAP HANA mandantenfähige Datenbank-Container (MDC) mit einem Mandanten: SAP HANA 2.0 SPS3 und höher
- SAP HANA mandantenfähige Datenbank-Container (MDC) mehrere Mandanten: SAP HANA 2.0 SPS4 und höher

Verbesserungen von SnapCenter 4.6

Ab Version 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 in einer Ressourcengruppe kombiniert, SnapCenter erkennt automatisch, welcher Host sich auf einem primären oder sekundären Server befindet, und führt dann die erforderlichen Backup-Vorgänge entsprechend aus. Das Aufbewahrungsmanagement für Snapshot und dateibasierte Backups, die mit SnapCenter erstellt wurden, erfolgt über beide Hosts hinweg, sodass sichergestellt ist, dass alte Backups auch am aktuellen sekundären Host gelöscht werden. Die folgende Abbildung bietet einen allgemeinen Überblick. Eine detaillierte Beschreibung der Konfiguration und des Betriebs von HANA System Replication fähigen HANA-Systemen in SnapCenter finden Sie unter "TR-4719 SAP HANA System Replication, Backup und Recovery mit SnapCenter".



SnapCenter-Konzepte und Best Practices

In diesem Abschnitt werden die SnapCenter-Konzepte und Best Practices im Zusammenhang mit der Konfiguration und Implementierung von SAP HANA-Ressourcen beschrieben.

Optionen und Konzepte für die Konfiguration von SAP HANA Ressourcen

Mit SnapCenter kann die Konfiguration von SAP HANA Datenbankressourcen mit zwei verschiedenen Ansätzen durchgeführt werden.

- **Manuelle Ressourcenkonfiguration.** HANA Ressourcen- und Speicherplatzinformationen müssen manuell bereitgestellt werden.
- **Automatische Erkennung von HANA-Ressourcen.** Automatische Erkennung vereinfacht die Konfiguration von HANA-Datenbanken in SnapCenter und ermöglicht automatisiertes Restore und Recovery.

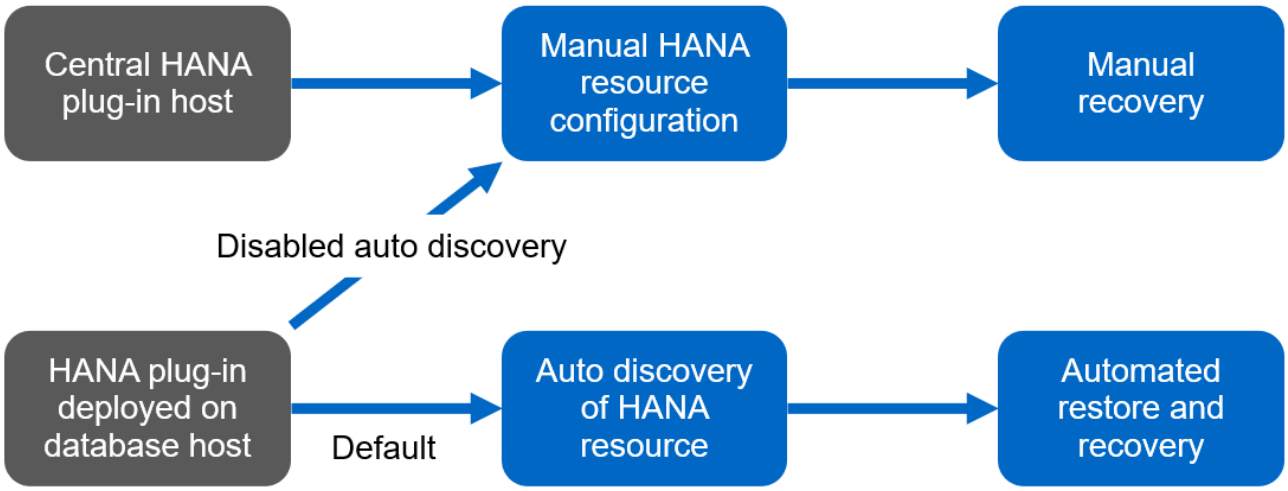
Dabei ist es wichtig zu wissen, dass nur HANA-Datenbankressourcen in SnapCenter aktiviert sind, die

automatisch erkannt wurden, für automatisierte Wiederherstellungen und Recoverys. HANA-Datenbankressourcen, die in SnapCenter manuell konfiguriert sind, müssen nach einer Wiederherstellung in SnapCenter manuell wiederhergestellt werden.

Andererseits wird die automatische Erkennung mit SnapCenter nicht für alle HANA-Architekturen und Infrastrukturkonfigurationen unterstützt. Daher erfordern HANA-Landschaften einen gemischten Ansatz, bei dem für einige HANA-Systeme (HANA mehrere Hostsysteme) eine manuelle Ressourcenkonfiguration erforderlich ist, und alle anderen Systeme können mithilfe der automatischen Erkennung konfiguriert werden.

Die automatische Erkennung und die automatisierte Wiederherstellung und Wiederherstellung hängen von der Möglichkeit ab, OS-Befehle auf dem Datenbank-Host auszuführen. Beispiele hierfür sind die Ermittlung des Platzbedarfs für Filesystem und Storage sowie die Unmount-, Mount- oder LUN-Erkennung. Diese Vorgänge werden mit dem SnapCenter Linux Plug-in ausgeführt, das gemeinsam mit dem HANA-Plug-in automatisch implementiert wird. Daher ist es Voraussetzung, das HANA-Plug-in auf dem Datenbank-Host zu implementieren, um automatische Erkennung sowie automatisiertes Restore und Recovery zu ermöglichen. Es ist auch möglich, die automatische Erkennung nach der Bereitstellung des HANA-Plug-ins auf dem Datenbank-Host zu deaktivieren. In diesem Fall handelt es sich bei der Ressource um eine manuell konfigurierte Ressource.

In der folgenden Abbildung sind die Abhängigkeiten zusammengefasst. Weitere Einzelheiten zu den HANA-Implementierungsoptionen finden Sie im Abschnitt „Bereitstellungsoptionen für das SAP HANA-Plug-in“.



Die HANA- und Linux-Plug-ins sind derzeit nur für Systeme mit Intel-Technik verfügbar. Falls die HANA-Datenbanken auf IBM Power Systems laufen, muss ein zentraler HANA-Plug-in-Host verwendet werden.

Unterstützte HANA-Architekturen für automatisches Discovery und automatisiertes Recovery

Mit SnapCenter werden automatische Erkennung und automatisierte Wiederherstellung und Recovery für die meisten HANA-Konfigurationen unterstützt, mit der Ausnahme, dass für HANA mehrere Host-Systeme eine manuelle Konfiguration erforderlich ist.

Die folgende Tabelle zeigt die unterstützten HANA-Konfigurationen für die automatische Erkennung.

HANA-Plug-in installiert auf:	HANA-Architektur	HANA-Systemkonfiguration	Infrastruktur
HANA Datenbank-Host	Einzelner Host	• HANA-einzelner Container • Mandantenfähige SAP HANA Datenbank-Container (MDC) mit einzelnen oder mehreren Mandanten • HANA System Replication	• Bare Metal mit NFS • Bare Metal mit XFS und FC mit oder ohne Linux Logical Volume Manager (LVM) • VMware mit direkt-Betriebssystem-NFS-Mounts

HANA MDC-Systeme mit mehreren Mandanten werden für automatische Erkennung unterstützt, nicht jedoch für automatisiertes Restore und Recovery mit der aktuellen SnapCenter-Version.

Unterstützte HANA-Architekturen für manuelle HANA-Ressourcenkonfiguration

Die manuelle Konfiguration von HANA-Ressourcen wird für alle HANA-Architekturen unterstützt, erfordert jedoch einen zentralen HANA-Plug-in-Host. Der zentrale Plug-in-Host kann der SnapCenter-Server selbst oder ein separater Linux- oder Windows-Host sein.

Wenn das HANA-Plug-in auf dem HANA-Datenbank-Host implementiert wird, wird die Ressource standardmäßig automatisch erkannt. Die automatische Erkennung kann für einzelne Hosts deaktiviert werden, sodass das Plug-in bereitgestellt werden kann. Beispielsweise auf einem Datenbank-Host mit aktivierter HANA-Systemreplizierung und einer SnapCenter-Version < 4.6, bei der die automatische Erkennung nicht unterstützt wird. Weitere Informationen finden Sie im Abschnitt "„Automatische Erkennung auf dem HANA-Plug-in-Host deaktivieren.“"

Die folgende Tabelle zeigt die unterstützten HANA-Konfigurationen für die manuelle HANA-Ressourcenkonfiguration.

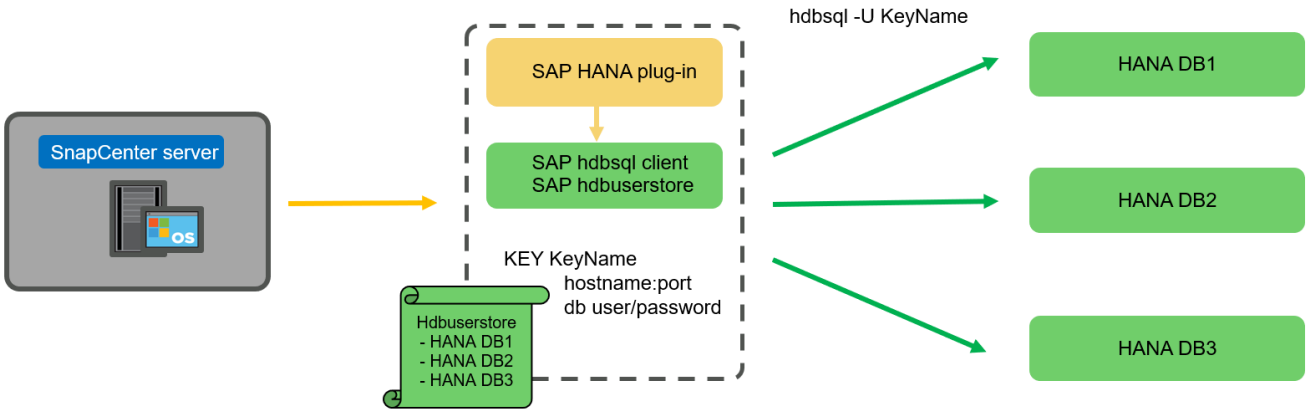
HANA-Plug-in installiert auf:	HANA-Architektur	HANA-Systemkonfiguration	Infrastruktur
Zentraler Plug-in-Host (SnapCenter-Server oder separater Linux-Host)	Single oder mehrere Hosts	• HANA-einzelner Container • HANA MDC mit einzelnen oder mehreren Mandanten • HANA System Replication	• Bare Metal mit NFS • Bare Metal mit XFS und FC mit oder ohne Linux LVM • VMware mit direkt-Betriebssystem-NFS-Mounts

Implementierungsoptionen für das SAP HANA Plug-in

Die folgende Abbildung zeigt die logische Ansicht und die Kommunikation zwischen dem SnapCenter Server und den SAP HANA Datenbanken.

Der SnapCenter-Server kommuniziert über das SAP HANA Plug-in mit den SAP HANA Datenbanken. Das

SAP HANA Plug-in nutzt die SAP HANA hdbsql-Client-Software, um SQL-Befehle an die SAP HANA-Datenbanken auszuführen. Der SAP HANA hdbuserstore wird verwendet, um die Benutzeranmeldeinformationen, den Hostnamen und die Portinformationen für den Zugriff auf die SAP HANA-Datenbanken bereitzustellen.



Das SAP HANA-Plug-in und die SAP-hdbsql-Client-Software, zu der auch das hdbuserstore-Konfigurationstool gehört, müssen auf demselben Host zusammen installiert werden.

Der Host kann entweder der SnapCenter-Server selbst, ein separater zentraler Plug-in-Host oder die einzelnen SAP HANA Datenbank-Hosts sein.

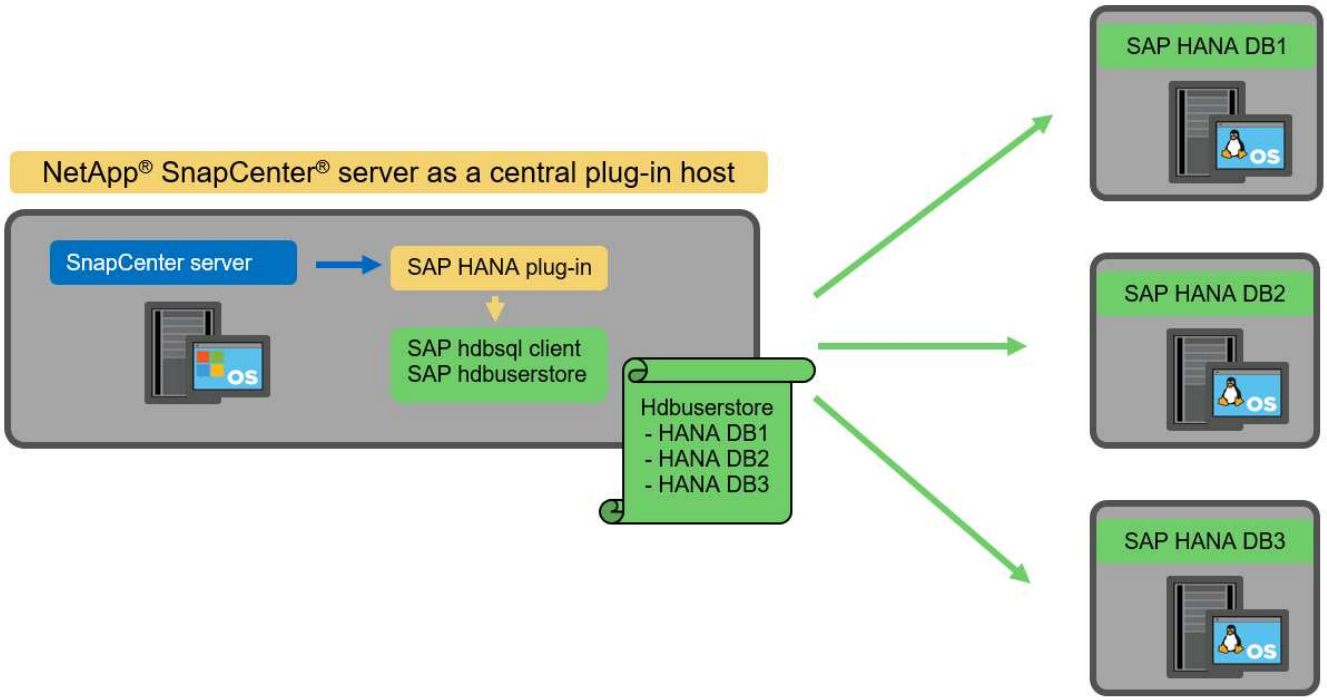
Hochverfügbarkeit mit SnapCenter Server

SnapCenter kann in einer HA-Konfiguration mit zwei Nodes eingerichtet werden. In dieser Konfiguration wird ein Load Balancer (z. B. F5) unter Verwendung einer virtuellen IP-Adresse verwendet, die auf den aktiven SnapCenter-Host verweist. Das SnapCenter-Repository (die MySQL-Datenbank) wird von SnapCenter zwischen den beiden Hosts repliziert, sodass die SnapCenter-Daten immer synchron sind.

SnapCenter Server HA wird nicht unterstützt, wenn das HANA-Plug-in auf dem SnapCenter-Server installiert ist. Wenn Sie SnapCenter in einer HA-Konfiguration einrichten möchten, installieren Sie das HANA Plug-in nicht auf dem SnapCenter Server. Weitere Informationen zur SnapCenter HA finden Sie unter diesem "NetApp Knowledge Base Seite".

SnapCenter Server als zentraler HANA Plug-in-Host

Die folgende Abbildung zeigt eine Konfiguration, in der der SnapCenter-Server als zentraler Plug-in-Host verwendet wird. Das SAP HANA Plug-in und die SAP hdbsql-Client-Software sind auf dem SnapCenter-Server installiert.



Da das HANA-Plug-in mit den gemanagten HANA-Datenbanken über den hdbclient über das Netzwerk kommunizieren kann, müssen keine SnapCenter-Komponenten auf den einzelnen HANA-Datenbank-Hosts installiert werden. SnapCenter kann die HANA-Datenbanken über einen zentralen HANA Plug-in-Host sichern, auf dem alle Benutzerspeicherschlüssel für die gemanagten Datenbanken konfiguriert sind.

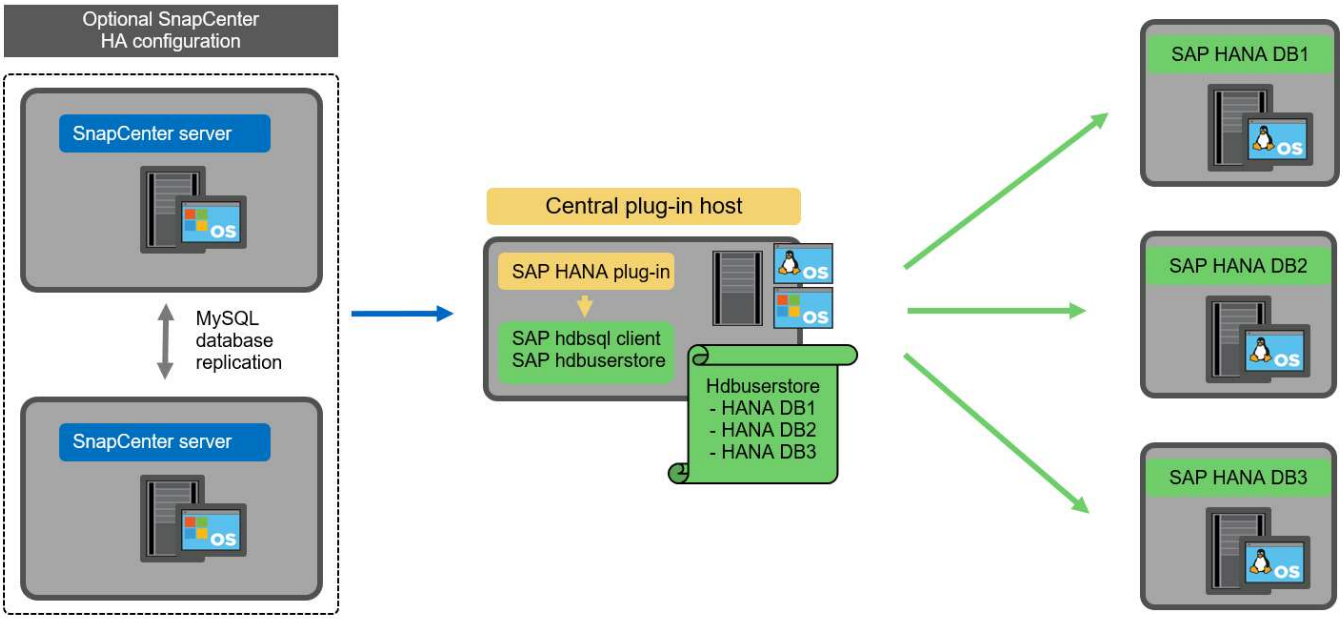
Um dagegen die Workflow-Automatisierung für die automatische Erkennung, die Automatisierung von Wiederherstellung und Wiederherstellung sowie die Aktualisierung von SAP Systemen zu verbessern, müssen auf dem Datenbank-Host SnapCenter Komponenten installiert werden. Bei Verwendung eines zentralen HANA-Plug-in-Hosts sind diese Funktionen nicht verfügbar.

Darüber hinaus kann die Hochverfügbarkeit des SnapCenter-Servers mit der in-Build-HA-Funktion nicht verwendet werden, wenn das HANA-Plug-in auf dem SnapCenter-Server installiert ist. Hochverfügbarkeit kann mit VMware HA erzielt werden, wenn der SnapCenter Server auf einer VM innerhalb eines VMware Clusters ausgeführt wird.

Separater Host als zentraler HANA Plug-in-Host

Die folgende Abbildung zeigt eine Konfiguration, in der ein separater Linux-Host als zentraler Plug-in-Host verwendet wird. In diesem Fall sind das SAP HANA Plug-in und die SAP hdbsql-Client-Software auf dem Linux-Host installiert.

> Der separate zentrale Plug-in-Host kann auch ein Windows-Host sein.

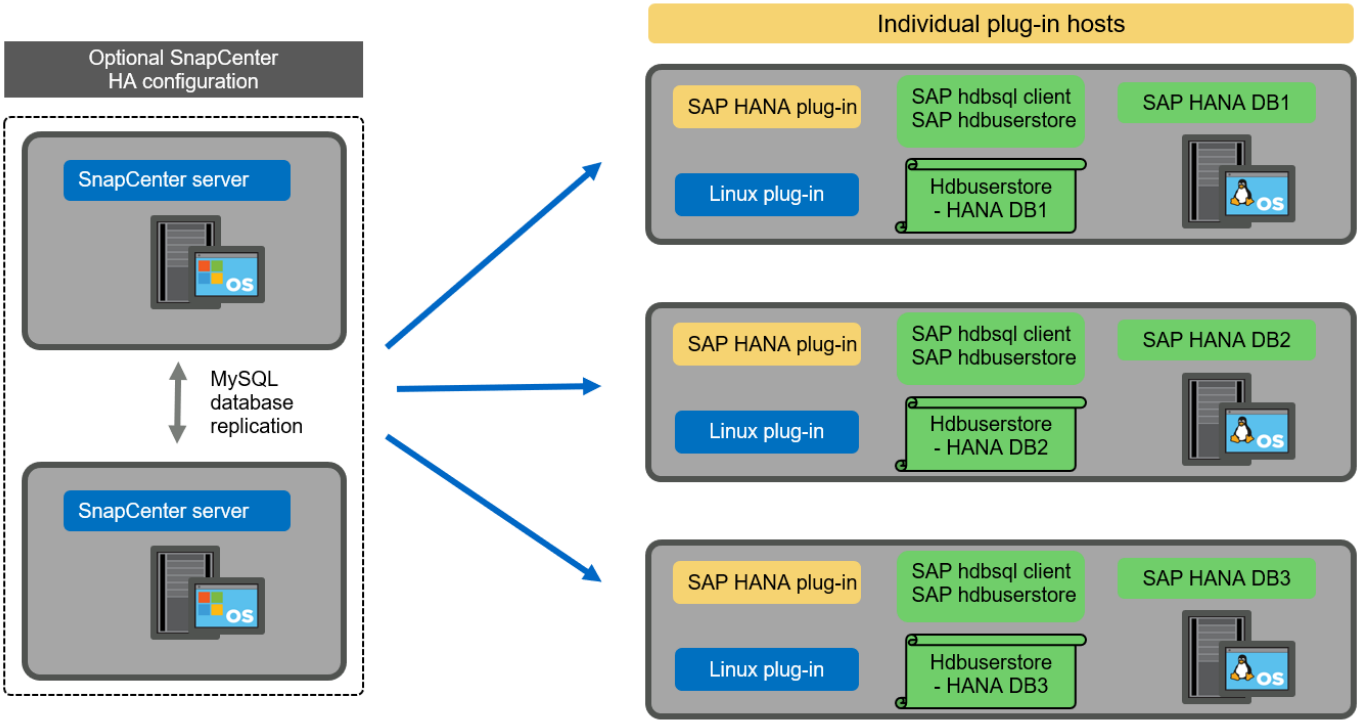


Die gleiche Einschränkung hinsichtlich der im vorherigen Abschnitt beschriebenen Funktionsverfügbarkeit gilt auch für einen separaten zentralen Plug-in Host.

Bei dieser Implementierungsoption kann der SnapCenter Server jedoch mit den in-Build-HA-Funktionen konfiguriert werden. Auch der zentrale Plug-in-Host muss HA sein, beispielsweise durch Verwendung einer Linux-Cluster-Lösung.

Auf einzelnen HANA-Datenbank-Hosts implementiertem HANA Plug-in

Die folgende Abbildung zeigt eine Konfiguration, in der das SAP HANA Plug-in auf jedem SAP HANA Datenbank-Host installiert ist.



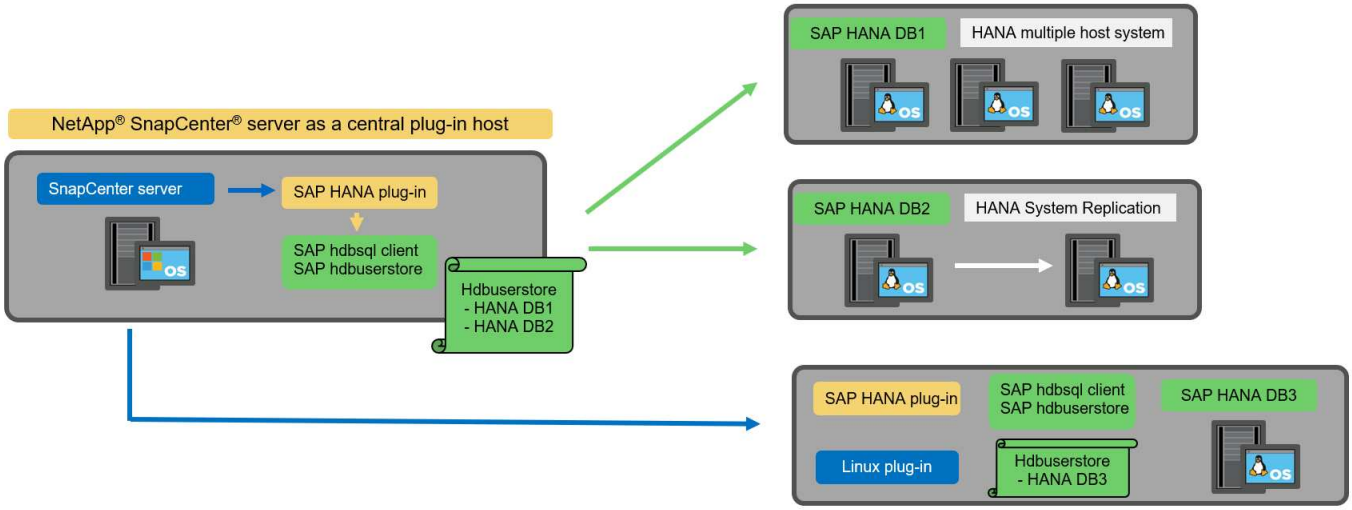
Wird das HANA-Plug-in auf jedem einzelnen HANA-Datenbank-Host installiert, sind alle Funktionen verfügbar, beispielsweise automatische Erkennung, automatisiertes Restore und Recovery. Zudem kann der SnapCenter Server in einer HA-Konfiguration eingerichtet werden.

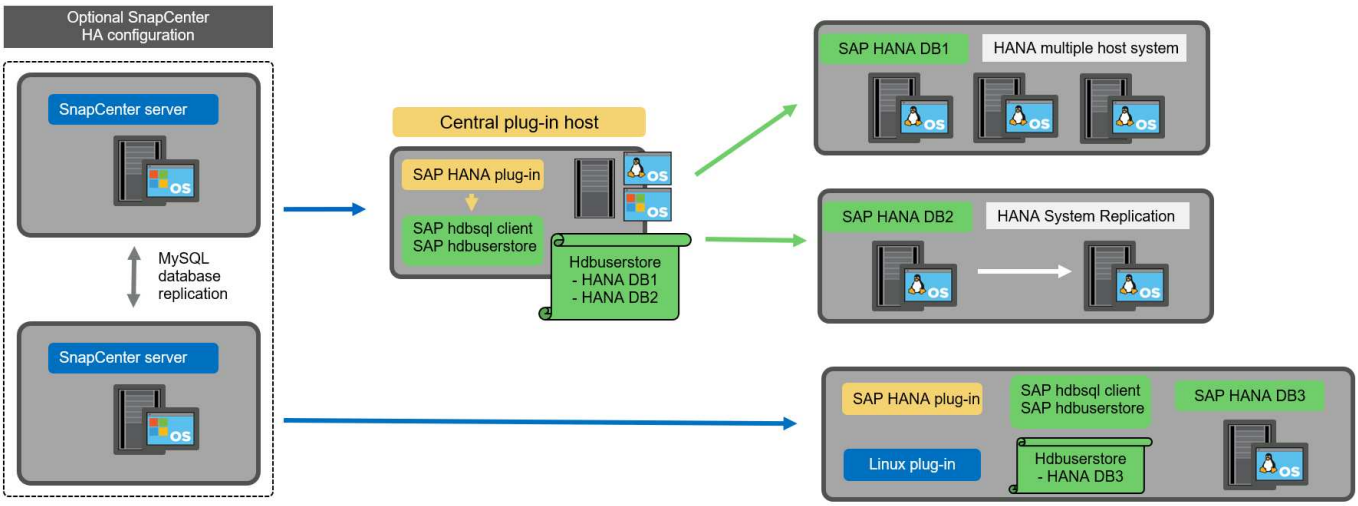
Plug-in-Implementierung für heterogene HANA

Wie zu Beginn dieses Abschnitts erläutert, erfordern einige HANA-Systemkonfigurationen, wie z. B. Systeme mit mehreren Hosts, einen zentralen Plug-in-Host. Daher erfordern die meisten SnapCenter Konfigurationen eine gemischte Implementierung des HANA Plug-ins.

NetApp empfiehlt, das HANA Plug-in auf dem HANA-Datenbank-Host für alle HANA-Systemkonfigurationen zu implementieren, die zur automatischen Erkennung unterstützt werden. Andere HANA-Systeme, wie beispielsweise Konfigurationen mit mehreren Hosts, sollten mit einem zentralen HANA Plug-in-Host gemanagt werden.

Die folgenden beiden Abbildungen zeigen gemischte Plug-in-Bereitstellungen entweder mit dem SnapCenter-Server oder einem separaten Linux-Host als zentralen Plug-in-Host. Der einzige Unterschied zwischen diesen beiden Implementierungen ist die optionale HA-Konfiguration.





Zusammenfassung und Empfehlungen

Im Allgemeinen empfiehlt NetApp die Implementierung des HANA Plug-ins auf jedem SAP HANA Host, um alle verfügbaren SnapCenter HANA Funktionen zu aktivieren und die Workflow-Automatisierung zu verbessern.

> Die HANA- und Linux-Plug-ins sind derzeit nur für Systeme mit Intel-Technik verfügbar. Falls die HANA-Datenbanken auf IBM Power Systems laufen, muss ein zentraler HANA-Plug-in-Host verwendet werden.

Für HANA-Konfigurationen, bei denen keine automatische Erkennung wie HANA-Konfigurationen mit mehreren Hosts unterstützt wird, muss ein zusätzlicher zentraler HANA-Plug-in-Host konfiguriert werden. Der zentrale Plug-in-Host kann der SnapCenter Server sein, wenn VMware HA für SnapCenter HA genutzt werden kann. Wenn Sie die im Build-HA-Funktion von SnapCenter verwenden möchten, verwenden Sie einen separaten Linux-Plug-in-Host.

In der folgenden Tabelle sind die verschiedenen Implementierungsoptionen aufgeführt.

Implementierungsoptionen	Abhängigkeiten
Zentrales HANA-Plug-in-Host-Plug-in auf SnapCenter-Server installiert	Vorteile: * Single HANA Plug-in, zentrale HDB User Store-Konfiguration * auf einzelnen HANA-Datenbank-Hosts werden keine SnapCenter-Softwarekomponenten benötigt * Unterstützung aller HANA-Architekturen Cons: * Manuelle Ressourcenkonfiguration * Manuelle Wiederherstellung * keine Unterstützung für die Wiederherstellung einzelner Mandanten * Alle Pre- und Post-Script-Schritte werden auf dem zentralen Plug-in-Host ausgeführt * in-Build SnapCenter Hochverfügbarkeit nicht unterstützt * Kombination von SID und Mandantenname muss für alle verwalteten HANA-Datenbanken eindeutig sein * Protokoll Für alle gemanagten HANA-Datenbanken ist das Backup-Aufbewahrungsmanagement aktiviert/deaktiviert
Zentrales HANA-Plug-in-Host-Plug-in auf separatem Linux- oder Windows-Server installiert	Vorteile: * Single HANA Plug-in, zentrale HDB User Store-Konfiguration * Keine SnapCenter Software-Komponenten erforderlich auf einzelnen HANA-Datenbank-Hosts * Unterstützung aller HANA-Architekturen * in-Build SnapCenter Hochverfügbarkeit unterstützt Cons: * Manuelle Ressourcenkonfiguration * Manuelle Wiederherstellung * keine Unterstützung für die Wiederherstellung einzelner Mandanten * Alle Pre- und Post-Script-Schritte werden auf dem zentralen Plug-in-Host ausgeführt * Kombination von SID und Mandantenname muss für alle verwalteten HANA-Datenbanken eindeutig sein * Protokoll Backup Aufbewahrungsmanagement aktiviert/deaktiviert für alle gemanagt HANA-Datenbanken

Implementierungsoptionen	Abhängigkeiten
Auf dem HANA-Datenbankserver wird ein individuelles HANA-Plug-in-Host-Plug-in installiert	Vorteile: * Automatische Bestandsaufnahme von HANA-Ressourcen * automatisierte Wiederherstellung und Recovery * Wiederherstellung einzelner Mandanten * vorab- und Postscript-Automatisierung für SAP Systemaktualisierung * in-Build SnapCenter Hochverfügbarkeit unterstützt * Backup-Aufbewahrungsmanagement für Protokoll kann für jede einzelne HANA-Datenbank aktiviert/deaktiviert werden Cons: * Nicht unterstützt für alle HANA-Architekturen. Zusätzlicher zentraler Plug-in-Host für HANA mehrere Host-Systeme erforderlich * HANA-Plug-in muss auf jedem HANA-Datenbank-Host implementiert werden

Datensicherung Strategie

Vor der Konfiguration von SnapCenter und dem SAP HANA Plug-in muss die Datensicherungsstrategie auf Grundlage der RTO- und RPO-Anforderungen der verschiedenen SAP Systeme definiert werden.

Ein gemeinsamer Ansatz besteht in der Definition von Systemtypen wie Systemen für Produktion, Entwicklung, Test oder Sandbox. Alle SAP-Systeme des gleichen Systemtyps haben typischerweise die gleichen Datenschutzparameter.

Folgende Parameter müssen definiert werden:

- Wie oft sollte ein Snapshot Backup ausgeführt werden?
- Wie lange sollten Snapshot Kopien Backups auf dem Primärspeichersystem aufbewahrt werden?
- Wie oft sollte eine Blockintegritätsprüfung ausgeführt werden?
- Sollten die primären Backups auf einen externen Backup-Standort repliziert werden?
- Wie lange sollten die Backups auf dem externen Backup-Storage aufbewahrt werden?

Die folgende Tabelle zeigt ein Beispiel für die Datenschutzparameter für die Produktion, Entwicklung und Prüfung des Systemtyps. Für das Produktionssystem wurde eine hohe Backup-Frequenz definiert und die Backups werden einmal pro Tag an einen externen Backup-Standort repliziert. Die Testsysteme haben niedrigere Anforderungen und keine Replikation der Backups.

Parameter	Produktionssysteme auszuführen	Entwicklungssysteme	Testsysteme
Sicherungshäufigkeit	Alle 4 Stunden	Alle 4 Stunden	Alle 4 Stunden
Primäre Aufbewahrung	2 Tage	2 Tage	2 Tage
Block-Integritätsprüfung	Einmal in der Woche	Einmal in der Woche	Nein
Replizierung an externe Backup-Standorte	Einmal am Tag	Einmal am Tag	Nein
Externe Backup-Aufbewahrung	2 Wochen	2 Wochen	Keine Angabe

In der folgenden Tabelle werden die Richtlinien aufgeführt, die für die Datensicherheitsparameter konfiguriert

werden müssen.

Parameter	RichtlinienLocalSnap	RichtlinieLocalSnapAndSnapVault	RichtlinienBlockIntegritätPrüfung
Backup-Typ	Auf Snapshot-Basis	Auf Snapshot-Basis	File-basiert
Zeitplanhäufigkeit	Stündlich	Täglich	Wöchentlich
Primäre Aufbewahrung	Anzahl = 12	Anzahl = 3	Anzahl = 1
SnapVault Replizierung	Nein	Ja.	Keine Angabe

Richtlinie `LocalSnapshot` Werden für Produktions-, Entwicklungs- und Testsysteme verwendet, um lokale Snapshot-Backups mit einer Aufbewahrung von zwei Tagen abzudecken.

In der Konfiguration für den Ressourcenschutz wird der Zeitplan für die Systemtypen unterschiedlich definiert:

- **Produktion.** Zeitplan alle 4 Stunden.
- **Entwicklung** Zeitplan alle 4 Stunden.
- **Test.** Zeitplan alle 4 Stunden.

Richtlinie `LocalSnapAndSnapVault` Wird für die Produktions- und Entwicklungssysteme eingesetzt, um die tägliche Replizierung auf den externen Backup Storage zu decken.

In der Konfiguration für den Ressourcenschutz wird der Zeitplan für die Produktion und Entwicklung definiert:

- **Produktion.** Zeitplan jeden Tag.
- **Entwicklung.** Zeitplan jeden Tag.

Richtlinie `BlockIntegrityCheck` Wird für die Produktions- und Entwicklungssysteme verwendet, um die wöchentliche Blockintegritätsprüfung mithilfe eines dateibasierten Backups abzudecken.

In der Konfiguration für den Ressourcenschutz wird der Zeitplan für die Produktion und Entwicklung definiert:

- **Produktion.** Zeitplan jede Woche.
- **Entwicklung.** Zeitplan jede Woche.

Für jede einzelne SAP HANA Datenbank, die die externe Backup-Richtlinie nutzt, muss auf der Storage-Ebene eine Sicherungsbeziehung konfiguriert werden. Die Sicherungsbeziehung definiert, welche Volumes repliziert werden und wie die Aufbewahrung von Backups im externen Backup-Storage aufbewahrt wird.

Mit unserem Beispiel wird für jedes Produktions- und Entwicklungssystem im externen Backup-Storage eine Aufbewahrung von zwei Wochen definiert.

> In unserem Beispiel sind die Sicherungsrichtlinien und die Aufbewahrung von SAP HANA-Datenbankressourcen und die nicht-Datenvolumen-Ressourcen nicht anders.

Backup-Vorgänge

SAP führte die Unterstützung von Snapshot Backups für MDC-Mehrmandantensysteme mit HANA 2.0 SPS4 ein. SnapCenter unterstützt Snapshot-Backup-Vorgänge von HANA MDC-Systemen mit mehreren Mandanten. SnapCenter unterstützt außerdem zwei verschiedene Wiederherstellungsvorgänge eines HANA MDC-Systems. Sie können entweder das komplette System, die System-DB und alle Mandanten wiederherstellen

oder nur einen einzelnen Mandanten wiederherstellen. Es gibt einige Voraussetzungen, wenn SnapCenter die Ausführung dieser Vorgänge ermöglicht.

In einem MDC-System ist die Mandantenkonfiguration nicht unbedingt statisch. Mandanten können hinzugefügt oder Mandanten gelöscht werden. SnapCenter kann sich nicht auf die Konfiguration verlassen, die beim Hinzufügen der HANA-Datenbank zu SnapCenter erkannt wird. SnapCenter muss wissen, welche Mandanten zum Zeitpunkt der Ausführung des Backup-Vorgangs verfügbar sind.

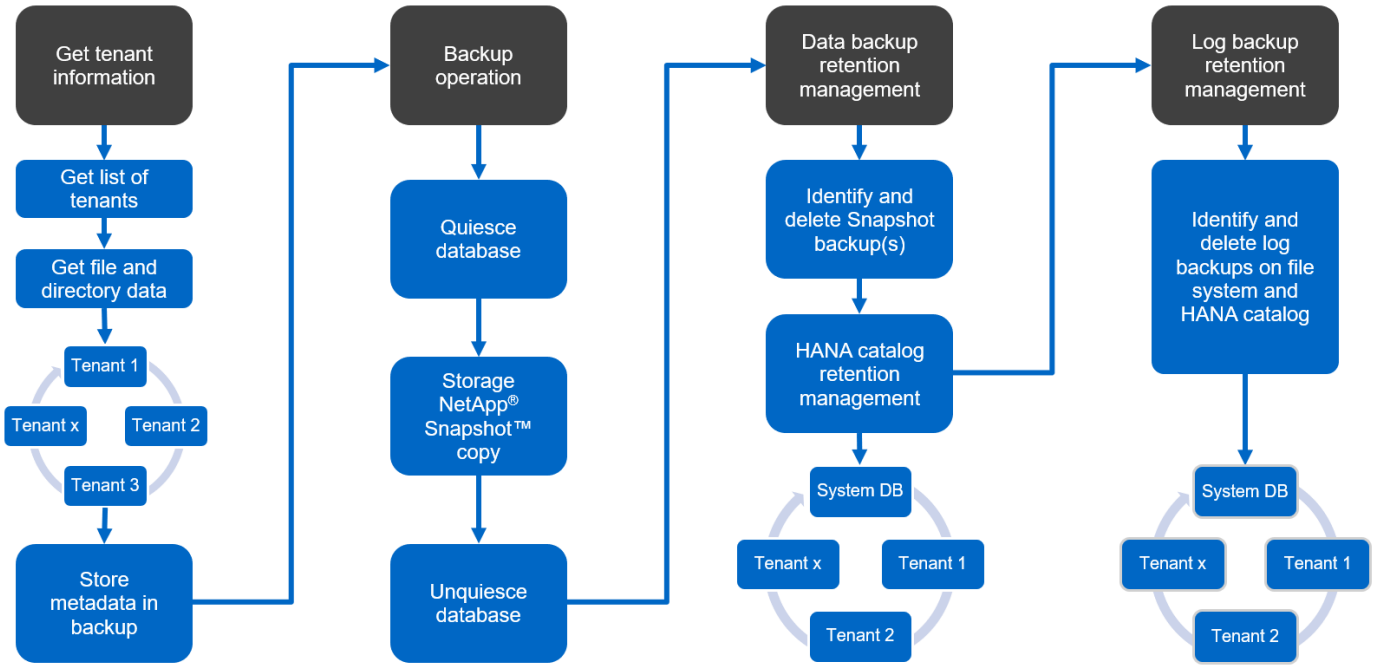
Um eine einzelne Mandanten-Wiederherstellung zu ermöglichen, muss SnapCenter wissen, welche Mandanten in jedem Snapshot-Backup enthalten sind. Zusätzlich muss die IT wissen, welche Dateien und Verzeichnisse zu den einzelnen Mandanten im Snapshot Backup gehören.

Somit müssen bei jedem Backup-Vorgang die Mandantendaten angezeigt werden. Dazu gehören die Mandantennamen und die entsprechenden Datei- und Verzeichnisinformationen. Diese Daten müssen in den Snapshot Backup-Metadaten gespeichert werden, um eine Wiederherstellung eines einzelnen Mandanten zu unterstützen. Der nächste Schritt ist der Snapshot-Backup-Vorgang selbst. Dieser Schritt umfasst den SQL-Befehl, um den HANA-Backup-Speicherpunkt auszulösen, das Storage-Snapshot-Backup und den SQL-Befehl zum Schließen des Snapshot-Vorgangs. Mit dem Befehl close aktualisiert die HANA-Datenbank den Backup-Katalog der System-DB und aller Mandanten.

> SAP unterstützt keine Snapshot Backup-Vorgänge für MDC-Systeme, wenn ein oder mehrere Mandanten angehalten werden.

Für das Aufbewahrungsmanagement von Daten-Backups und das HANA-Backup-Katalogmanagement muss SnapCenter die Kataloglösch-Operationen für die Systemdatenbank und alle Mandantendatenbanken ausführen, die im ersten Schritt identifiziert wurden. Auf dieselbe Weise für die Log-Backups muss der SnapCenter-Workflow auf jedem Mandanten laufen, der Teil des Backup-Vorgangs war.

Die folgende Abbildung zeigt einen Überblick über den Backup-Workflow.



Backup-Workflow für Snapshot-Backups der HANA-Datenbank

SnapCenter sichert die SAP HANA-Datenbank in folgender Reihenfolge:

1. SnapCenter liest die Liste der Mandanten aus der HANA-Datenbank vor.
2. SnapCenter liest die Dateien und Verzeichnisse für jeden Mandanten aus der HANA-Datenbank vor.
3. Informationen zu Mandanten werden bei diesem Backup in den Metadaten von SnapCenter gespeichert.
4. SnapCenter löst einen globalen, synchronisierten Speicherpunkt für Backups von SAP HANA aus, um ein konsistentes Datenbank-Image auf der Persistenzschicht zu erstellen.

   Für ein SAP HANA MDC-System mit einem oder mehreren Mandanten wird ein synchronisierter globaler Backup-Speicherpunkt für die Systemdatenbank und für jede Mandantendatenbank erstellt.

5. SnapCenter erstellt Storage-Snapshot-Kopien für alle Daten-Volumes, die für die Ressource konfiguriert sind. In unserem Beispiel einer HANA-Datenbank mit einem einzigen Host gibt es nur ein Daten-Volume. Bei einer SAP HANA Datenbank mit mehreren Hosts sind mehrere Daten-Volumes vorhanden.
6. Das Storage Snapshot Backup wird von SnapCenter im SAP HANA Backup-Katalog registriert.
7. SnapCenter löscht den Speicherpunkt für SAP HANA-Backups.
8. SnapCenter startet ein SnapVault- oder SnapMirror-Update für alle konfigurierten Daten-Volumes in der Ressource.

   Dieser Schritt wird nur ausgeführt, wenn die ausgewählte Richtlinie eine SnapVault- oder SnapMirror-Replizierung umfasst.

9. SnapCenter löscht die Storage-Snapshot-Kopien und die Backup-Einträge in seiner Datenbank sowie im SAP HANA Backup-Katalog basierend auf der Aufbewahrungsrichtlinie, die für Backups im primären Storage definiert ist. HANA-Backup-Katalogvorgänge werden für die Systemdatenbank und alle Mandanten ausgeführt.

   Ist das Backup noch auf dem sekundären Speicher verfügbar, wird der SAP HANA-Katalogeintrag nicht gelöscht.

10. SnapCenter löscht alle Log-Backups auf dem Filesystem und im SAP HANA-Backup-Katalog, die älter als die älteste im SAP HANA-Backup-Katalog identifizierte Datensicherung sind. Diese Vorgänge werden für die Systemdatenbank und alle Mandanten durchgeführt.

    Dieser Schritt wird nur ausgeführt, wenn die allgemeine Ordnung der Protokollsicherung nicht deaktiviert ist.

Backup-Workflow für die Überprüfung der Blockintegrität

SnapCenter führt die Integritätsprüfung der Blöcke in folgender Reihenfolge aus:

1. SnapCenter liest die Liste der Mandanten aus der HANA-Datenbank vor.
2. SnapCenter löst einen dateibasierten Backup-Vorgang für die Systemdatenbank und jeden Mandanten aus.
3. SnapCenter löscht dateibasierte Backups in seiner Datenbank, im Filesystem und im SAP HANA-Backup-Katalog basierend auf der Aufbewahrungsrichtlinie, die für die Überprüfung der Blockintegrität definiert ist. Das Löschen des Backups im Filesystem und der HANA-Backup-Katalog werden für die Systemdatenbank und alle Mandanten durchgeführt.
4. SnapCenter löscht alle Log-Backups auf dem Filesystem und im SAP HANA-Backup-Katalog, die älter als

die älteste im SAP HANA-Backup-Katalog identifizierte Datensicherung sind. Diese Vorgänge werden für die Systemdatenbank und alle Mandanten durchgeführt.

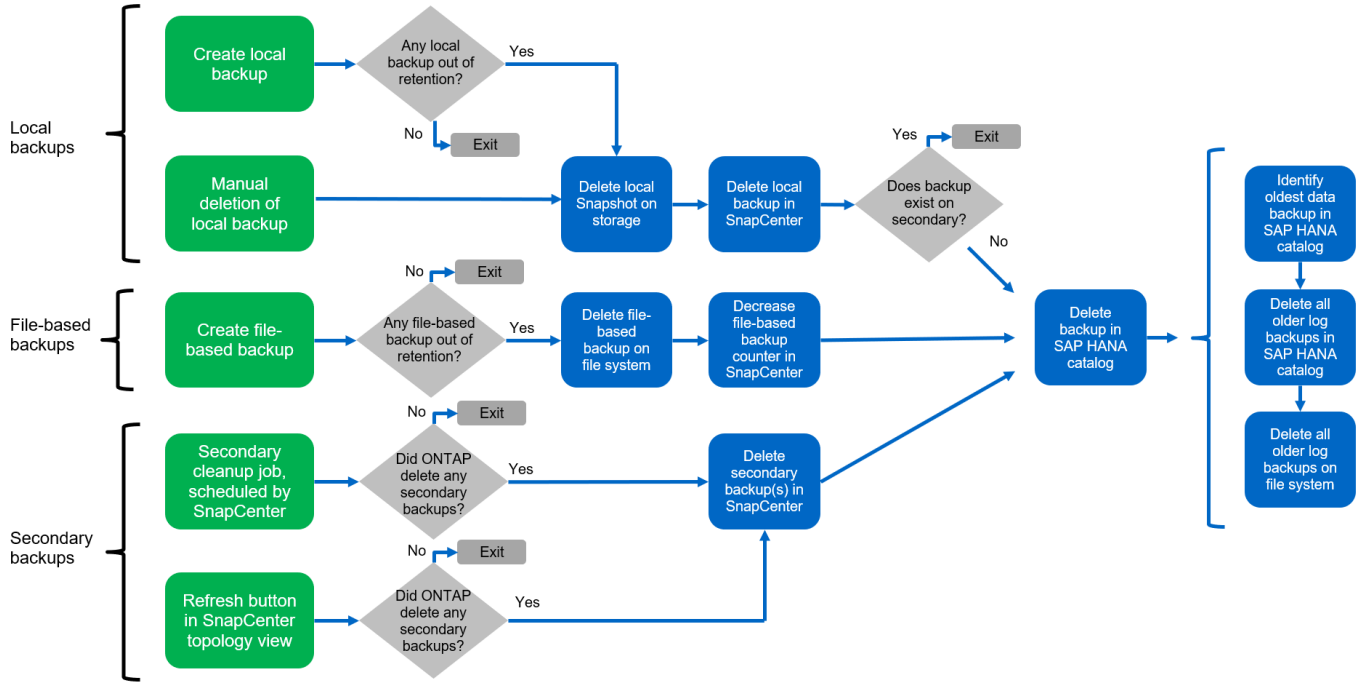
> Dieser Schritt wird nur ausgeführt, wenn die allgemeine Ordnung der Protokollsicherung nicht deaktiviert ist.

Management der Backup-Aufbewahrung und allgemeine Ordnung der Daten und Backup-Protokollierung

Das Management der Daten-Backup-Aufbewahrung und die allgemeine Ordnung der Backup-Protokollierung können in fünf Hauptbereiche unterteilt werden, einschließlich Aufbewahrungsmanagement von:

- Lokale Backups im primären Storage
- Dateibasierten Backups
- Backups im sekundären Storage
- Daten-Backups im SAP HANA Backup-Katalog
- Protokollierung von Backups im SAP HANA Backup-Katalog und im Filesystem

Die folgende Abbildung bietet einen Überblick über die verschiedenen Workflows und die Abhängigkeiten jedes einzelnen Vorgangs. In den folgenden Abschnitten werden die verschiedenen Operationen im Detail beschrieben.



Aufbewahrungsmanagement von lokalen Backups auf dem Primärstorage

SnapCenter übernimmt die allgemeine Ordnung und Sauberkeit von SAP HANA Datenbank-Backups und Backups nicht-Daten-Volumes, indem Snapshot Kopien im primären Storage und im SnapCenter Repository gemäß einer in der SnapCenter Backup-Richtlinie definierten Aufbewahrung gelöscht werden.

Die Aufbewahrungsmanagement-Logik wird mit jedem Backup Workflow in SnapCenter ausgeführt.

> Beachten Sie, dass SnapCenter das Aufbewahrungsmanagement für sowohl geplante als auch On-Demand-Backups individuell übernimmt.

Lokale Backups im Primärspeicher können auch manuell in SnapCenter gelöscht werden.

Aufbewahrungsmanagement von dateibasierten Backups

SnapCenter übernimmt die allgemeine Ordnung und Sauberkeit der dateibasierten Backups, indem die Backups auf dem Filesystem gemäß einer in der SnapCenter Backup Policy definierten Aufbewahrung gelöscht werden.

Die Aufbewahrungsmanagement-Logik wird mit jedem Backup Workflow in SnapCenter ausgeführt.

> Beachten Sie, dass SnapCenter das Aufbewahrungsmanagement individuell für geplante oder On-Demand Backups handhabt.

Aufbewahrungsmanagement von Backups im sekundären Storage

Das Aufbewahrungsmanagement von Backups im sekundären Storage wird durch ONTAP verarbeitet, basierend auf der in der ONTAP-Sicherungsbeziehung definierten Aufbewahrung.

Zur Synchronisierung dieser Änderungen auf dem sekundären Storage im SnapCenter-Repository verwendet SnapCenter einen geplanten Bereinigungsauftrag. Dieser Bereinigungsjob synchronisiert alle sekundären Storage-Backups mit dem SnapCenter Repository für alle SnapCenter Plug-ins und alle Ressourcen.

Der Bereinigungsjob wird standardmäßig einmal pro Woche geplant. Dieser wöchentliche Zeitplan führt zu einer Verzögerung beim Löschen von Backups in SnapCenter und SAP HANA Studio im Vergleich zu den Backups, die bereits auf dem Sekundärspeicher gelöscht wurden. Um diese Inkonsistenz zu vermeiden, können Kunden den Zeitplan beispielsweise einmal pro Tag auf eine höhere Frequenz ändern.

> Der Bereinigungsauftrag kann auch manuell für eine einzelne Ressource ausgelöst werden, indem Sie in der Topologieansicht der Ressource auf die Schaltfläche „Aktualisieren“ klicken.

Details dazu, wie der Zeitplan des Bereinigungsjobs angepasst wird oder wie eine manuelle Aktualisierung ausgelöst wird, finden Sie im Abschnitt "„Change Scheduling Frequency of Backup Synchronization with off-Site Backup Storage“."

Aufbewahrungsmanagement von Daten-Backups im SAP HANA Backup-Katalog

Hat SnapCenter ein Backup, lokale Snapshots oder dateibasierte Backups gelöscht oder das Backup im sekundären Storage identifiziert, so wird dieses Daten-Backup auch im SAP HANA Backup-Katalog gelöscht.

Bevor der SAP HANA-Katalogeintrag für ein lokales Snapshot Backup im primären Storage gelöscht wird, überprüft SnapCenter, ob das Backup noch im sekundären Storage vorhanden ist.

Aufbewahrungsmanagement von Protokoll-Backups

Die SAP HANA Datenbank erstellt automatisch Protokoll-Backups. Diese Backup-Durchläufe für das Protokoll erstellen Backup-Dateien für jeden einzelnen SAP HANA Service in einem in SAP HANA konfigurierten Backup-Verzeichnis.

Log-Backups, die älter als die aktuelle Datensicherung sind, werden für die zukünftige Wiederherstellung nicht mehr benötigt und können daher gelöscht werden.

SnapCenter übernimmt die allgemeine Ordnung und Sauberkeit der Log-Datei-Backups auf Filesystem-Ebene sowie im SAP HANA Backup-Katalog, indem Sie die folgenden Schritte durchführen:

1. SnapCenter liest den SAP HANA-Backup-Katalog, um die Backup-ID des ältesten erfolgreichen dateibasierten oder Snapshot-Backups zu erhalten.
2. SnapCenter löscht alle Log-Backups im SAP HANA-Katalog und das Filesystem, die älter als diese Backup-ID sind.

> SnapCenter kümmert sich nur um die allgemeine Ordnung und Sauberkeit der Backups, die von SnapCenter erstellt wurden. Falls zusätzliche dateibasierte Backups außerhalb von SnapCenter erstellt werden, müssen Sie sicherstellen, dass die dateibasierten Backups aus dem Backup-Katalog gelöscht werden. Wird eine solche Datensicherung nicht manuell aus dem Backup-Katalog gelöscht, kann sie zur ältesten Datensicherung werden, und ältere Log-Backups werden erst gelöscht, wenn diese dateibasierte Sicherung gelöscht wird.

> Obwohl eine Aufbewahrung für On-Demand-Backups in der Richtlinienkonfiguration definiert wird, wird die allgemeine Ordnung und Sauberkeit nur dann ausgeführt, wenn ein weiteres On-Demand-Backup ausgeführt wird. Daher müssen On-Demand-Backups in der Regel manuell in SnapCenter gelöscht werden, um sicherzustellen, dass diese Backups auch im SAP HANA Backup-Katalog gelöscht werden und die allgemeine Ordnung der Protokollbackups nicht auf einem alten On-Demand-Backup basiert.

Das Backup-Aufbewahrungsmanagement für Protokolle ist standardmäßig aktiviert. Falls erforderlich, kann diese deaktiviert werden, wie im Abschnitt beschrieben "„Automatische Erkennung auf dem HANA-Plug-in-Host deaktivieren.“"

Kapazitätsanforderungen für Snapshot Backups

Dabei müssen Sie die höhere Blockänderungsrate auf Storage-Ebene in Relation zur Änderungsrate bei herkömmlichen Datenbanken berücksichtigen. Aufgrund des HANA-Tabellen-Zusammenführungsprozesses des Spaltenspeichers wird die komplette Tabelle auf die Festplatte geschrieben, nicht nur die geänderten Blöcke.

Die Daten unseres Kundenstamms zeigen eine tägliche Änderungsrate zwischen 20 % und 50 %, wenn mehrere Snapshot-Backups während des Tages erstellt werden. Wenn beim SnapVault-Ziel die Replizierung nur einmal pro Tag durchgeführt wird, ist die tägliche Änderungsrate in der Regel kleiner.

Restore- und Recovery-Vorgänge

Wiederherstellung von Vorgängen mit SnapCenter

Aus Sicht der HANA-Datenbank unterstützt SnapCenter zwei verschiedene Restore-Vorgänge.

- **Wiederherstellung der gesamten Ressource.** Alle Daten des HANA-Systems sind wiederhergestellt. Enthält das HANA-System einen oder mehrere Mandanten, werden die Daten der Systemdatenbank und die Daten aller Mandanten wiederhergestellt.
- **Restore eines einzelnen Mieters.** nur die Daten des ausgewählten Mieters werden wiederhergestellt.

In Bezug auf Storage müssen die oben genannten Restore-Vorgänge unterschiedlich durchgeführt werden, abhängig vom verwendeten Storage-Protokoll (NFS oder Fibre Channel SAN), der konfigurierten Datensicherung (Primärstorage mit oder ohne externen Backup-Storage). Und das ausgewählte Backup, das für den Wiederherstellungsvorgang verwendet werden soll (Wiederherstellung vom primären oder externen Backup-Storage).

Wiederherstellung vollständiger Ressourcen aus dem primären Storage

Beim Wiederherstellen der gesamten Ressource aus dem primären Speicher unterstützt SnapCenter zwei verschiedene ONTAP Funktionen zum Ausführen des Wiederherstellungsvorgangs. Sie können zwischen den folgenden beiden Funktionen wählen:

- **Volume-basierte SnapRestore.** Ein Volume-basierter SnapRestore setzt den Inhalt des Speichervolumens in den Status des ausgewählten Snapshot Backups zurück.
  - Das Kontrollkästchen zur Zurücksetzen von Volumes ist verfügbar für automatisch erkannte Ressourcen mithilfe von NFS.
  - Aktivieren Sie das Optionsfeld „Ressource“ für manuell konfigurierte Ressourcen.
- **File-Based SnapRestore.** ein dateibasierter SnapRestore, auch als Single File SnapRestore bekannt, stellt alle einzelnen Dateien (NFS) oder alle LUNs (SAN) wieder her.
  - Standardwiederherstellungsmethode für automatisch erkannte Ressourcen. Kann mit dem Kontrollkästchen Volume zurücksetzen für NFS geändert werden.
  - Optionsfeld auf Dateiebene für manuell konfigurierte Ressourcen.

Die folgende Tabelle enthält einen Vergleich der verschiedenen Wiederherstellungsmethoden.

	Volume-basierte SnapRestore	File-basiertes SnapRestore
Geschwindigkeit der Wiederherstellung	Sehr schnell, unabhängig von der Volume-Größe	Sehr schnelle Restore-Prozesse, nutzt aber Hintergrundkopiejobs für das Storage-System, wodurch die Erstellung neuer Snapshot Backups blockiert wird
Snapshot Backup-Verlauf	Wiederherstellung auf ein älteres Snapshot-Backup, entfernt alle neueren Snapshot-Backups.	Kein Einfluss
Wiederherstellung der Verzeichnisstruktur	Verzeichnisstruktur wird ebenfalls wiederhergestellt	NFS: Stellt nur die einzelnen Dateien wieder her, nicht die Verzeichnisstruktur. Wenn auch die Verzeichnisstruktur verloren geht, muss sie manuell erstellt werden, bevor der Wiederherstellungsvorgang ausgeführt wird.auch die Verzeichnisstruktur wird wiederhergestellt
Für die Konfiguration der Ressource ist die Replizierung auf einen externen Backup-Storage eingerichtet	Eine Wiederherstellung auf Volume-Basis kann nicht an einem Backup der Snapshot Kopie durchgeführt werden, das älter als die Snapshot Kopie ist, die für die SnapVault-Synchronisierung verwendet wird	Ein beliebiges Snapshot Backup kann ausgewählt werden

Wiederherstellung kompletter Ressourcen von externen Backup-Speichern

Eine Wiederherstellung über den externen Backup-Speicher wird immer mithilfe einer SnapVault-Wiederherstellung durchgeführt, bei der alle Dateien oder alle LUNs des Storage-Volumes mit dem Inhalt des

Snapshot-Backups überschrieben werden.

Wiederherstellung eines einzelnen Mandanten

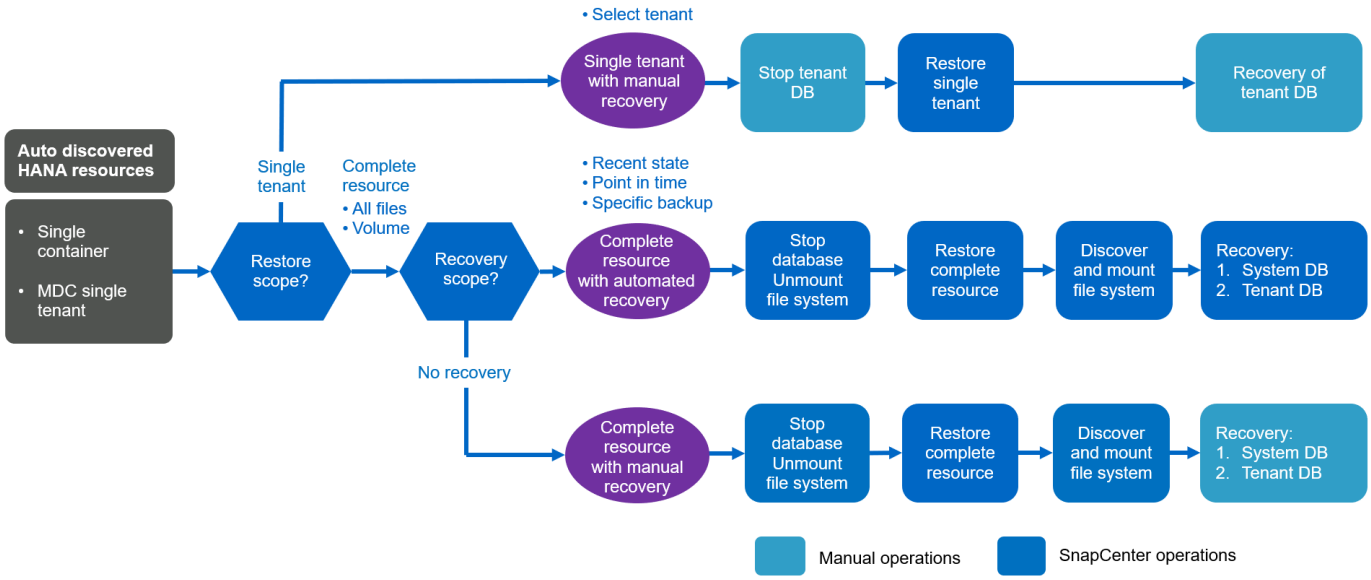
Die Wiederherstellung eines einzelnen Mandanten erfordert eine dateibasierte Wiederherstellung. Je nach verwendetem Storage-Protokoll werden verschiedene Restore-Workflows von SnapCenter ausgeführt.

- NFS
  - Primärspeicher. Dateibasierte SnapRestore-Vorgänge werden für alle Dateien der Mandanten-Datenbank ausgeführt.
  - Externer Backup-Storage: Für alle Dateien der Mandanten-Datenbank werden SnapVault Restore-Vorgänge durchgeführt.
- SAN
  - Primärspeicher. Klonen und Verbinden der LUN mit dem Datenbank-Host und Kopieren aller Dateien der Mandanten-Datenbank.
  - Externer Backup-Storage: Klonen und Verbinden der LUN mit dem Datenbank-Host und Kopieren aller Dateien der Mandanten-Datenbank.

Wiederherstellung und Recovery von automatisch erkannten HANA-Einzelcontainern und MDC-Einzelmandanten-Systemen

HANA-einzelner Container und HANA MDC-Einzelmandanten-Systeme, die automatisch erkannt wurden, sind für die automatisierte Wiederherstellung und das automatisierte Recovery mit SnapCenter aktiviert. Für diese HANA-Systeme unterstützt SnapCenter drei verschiedene Restore- und Recovery-Workflows, wie in der folgenden Abbildung dargestellt:

- **Einzelner Mandant mit manueller Wiederherstellung.** bei Auswahl eines einzelnen Mandanten führt SnapCenter alle Mandanten auf, die im ausgewählten Snapshot-Backup enthalten sind. Sie müssen die Mandantendatenbank manuell anhalten und wiederherstellen. Der Restore-Vorgang mit SnapCenter wird mit einzelnen Datei-SnapRestore-Vorgängen für NFS oder Klon-, Mount- und Kopiervorgängen in SAN-Umgebungen durchgeführt.
- **Komplette Ressource mit automatisierter Wiederherstellung.** Wenn Sie einen kompletten Ressourcenwiederherstellungsvorgang und eine automatisierte Wiederherstellung auswählen, wird der gesamte Workflow mit SnapCenter automatisiert. SnapCenter unterstützt den aktuellen Zustand, zeitpunktgenaue oder bestimmte Backup Recovery-Vorgänge. Der ausgewählte Wiederherstellungsvorgang wird für das System und die Mandantendatenbank verwendet.
- **Vollständige Ressource mit manueller Wiederherstellung.** Wenn Sie No Recovery wählen, stoppt SnapCenter die HANA-Datenbank und führt das erforderliche Dateisystem (unmount, Mount) und Restore Operationen aus. Sie müssen die System- und die Mandantendatenbank manuell wiederherstellen.

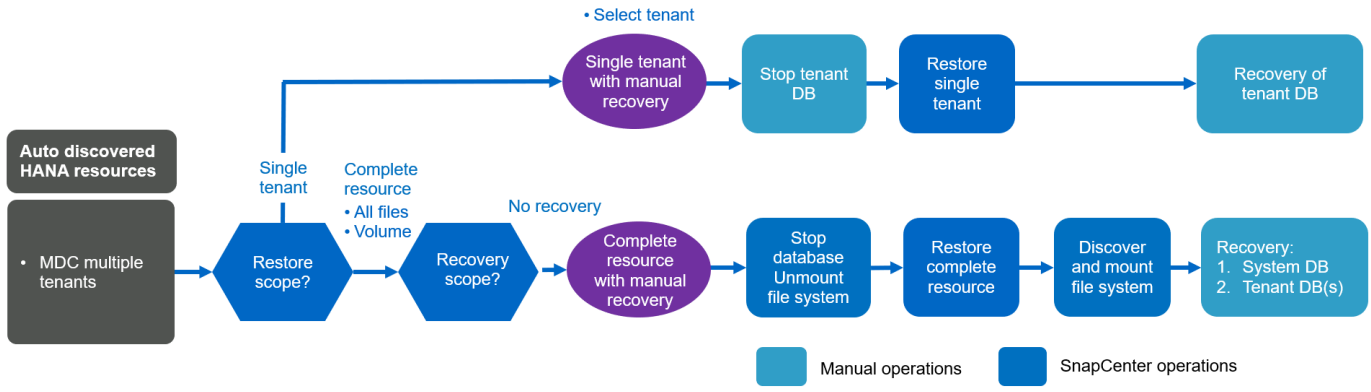


Wiederherstellung und Wiederherstellung von automatisch erkannten HANA MDC-Systemen mit mehreren Mandanten

Obwohl HANA MDC-Systeme mit mehreren Mandanten automatisch erkannt werden können, wird die automatisierte Wiederherstellung und Wiederherstellung mit der aktuellen SnapCenter-Version nicht unterstützt. Bei MDC-Systemen mit mehreren Mandanten unterstützt SnapCenter zwei verschiedene Wiederherstellungs- und Recovery-Workflows, wie in der folgenden Abbildung dargestellt:

- Ein einzelner Mandant mit manueller Recovery
- Ressource mit manueller Wiederherstellung abschließen

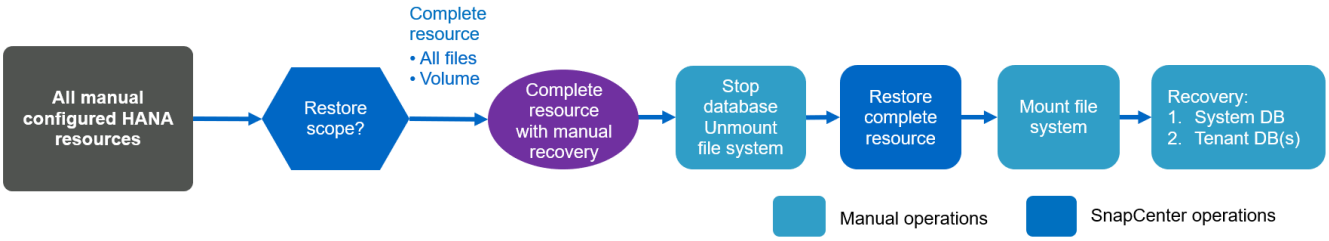
Die Workflows sind die gleichen wie im vorherigen Abschnitt beschrieben.



Wiederherstellung und Recovery von manuellen konfigurierten HANA-Ressourcen

Manuelle konfigurierte HANA-Ressourcen sind für automatisiertes Restore und Recovery nicht aktiviert. Zudem wird bei MDC-Systemen mit einzelnen oder mehreren Mandanten kein Restore-Vorgang eines einzelnen Mandanten unterstützt.

Bei manuell konfigurierten HANA-Ressourcen unterstützt SnapCenter nur eine manuelle Recovery, wie in der folgenden Abbildung dargestellt. Der Workflow für die manuelle Wiederherstellung ist der gleiche wie in den vorherigen Abschnitten beschrieben.



Zusammenfassung von Restore- und Recovery-Vorgängen

In der folgenden Tabelle sind die Restore- und Recovery-Vorgänge abhängig von der Konfiguration der HANA-Ressourcen in SnapCenter zusammengefasst.

Konfiguration von SnapCenter-Ressourcen	Wiederherstellungs- und Recovery-Optionen	Stoppen Sie die HANA Datenbank	Vorher unmounten, nach Wiederherstellungsvorgang mounten	Recovery-Vorgang
Automatisch erkannte Einzelcontainer MDC Einzelmandant	• Füllen Sie die Ressource mit entweder aus • Standard (alle Dateien) • Volume-Zurücksetzen (NFS nur aus Primärspeicher) • Automatische Wiederherstellung ausgewählt	Automatisiert mit SnapCenter	Automatisiert mit SnapCenter	Automatisiert mit SnapCenter
	• Füllen Sie die Ressource mit entweder aus • Standard (alle Dateien) • Volume-Zurücksetzen (NFS nur aus Primärspeicher) • Keine Wiederherstellung ausgewählt	Automatisiert mit SnapCenter	Automatisiert mit SnapCenter	Manuell
	• Wiederherstellung von Mandanten	Manuell	Nicht erforderlich	Manuell

Konfiguration von SnapCenter-Ressourcen	Wiederherstellungs- und Recovery-Optionen	Stoppen Sie die HANA Datenbank	Vorher unmounten, nach Wiederherstellungsvorgang mounten	Recovery-Vorgang
Automatisch erkannte MDC mehrere Mandanten	• Füllen Sie die Ressource mit entweder aus • Standard (alle Dateien) • Volume-Zurücksetzen (NFS nur aus Primärspeicher) • Automatisierte Wiederherstellung wird nicht unterstützt	Automatisiert mit SnapCenter	Automatisiert mit SnapCenter	Manuell
	• Wiederherstellung von Mandanten	Manuell	Nicht erforderlich	Manuell
Alle manuell konfigurierten Ressourcen	• Komplette Ressource (= Volume revert, verfügbar für NFS und SAN nur auf Basis des Primärspeichers) • Dateiebene (alle Dateien) • Automatisierte Wiederherstellung wird nicht unterstützt	Manuell	Manuell	Manuell

Lab-Einrichtung für diesen Bericht

Die für diesen technischen Bericht verwendete Lab-Einrichtung umfasst fünf verschiedene SAP HANA-Konfigurationen:

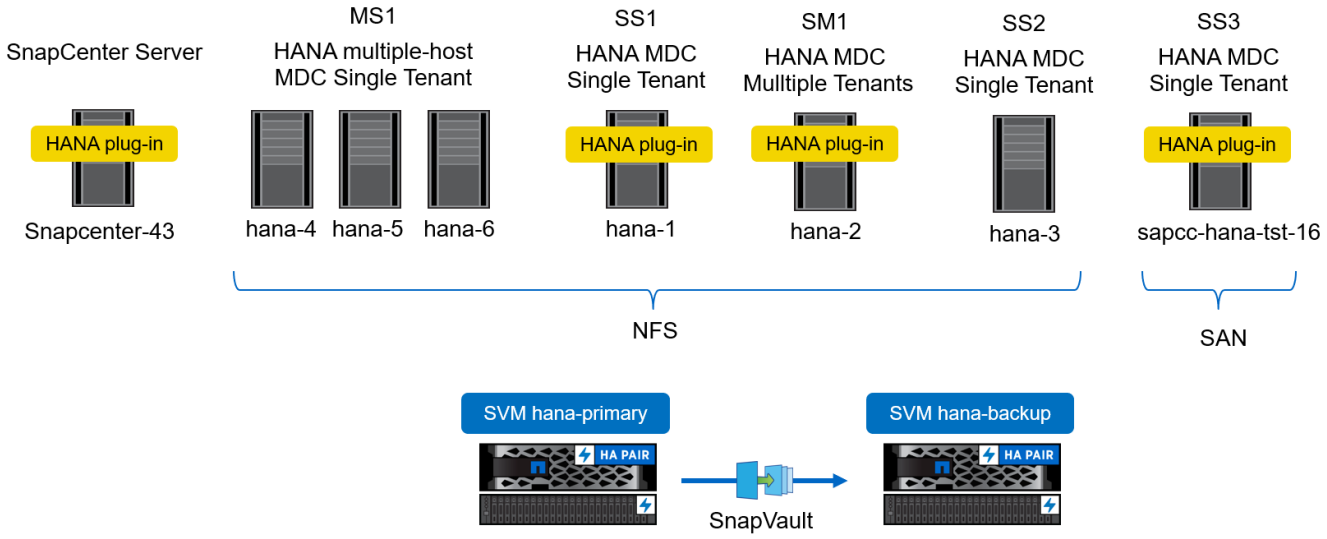
- **MS1.**
  - SAP HANA MDC-Einzelmandant-System mit mehreren Hosts
  - Management über einen zentralen Plug-in-Host (SnapCenter Server)

    - Verwendet NFS als Storage-Protokoll
- **SS1.**
    - SAP HANA Single-Host-MDC-Einzelmandant-System
    - Automatisch erkannt mit installiertem HANA-Plug-in auf HANA-Datenbank-Host
    - Verwendet NFS als Storage-Protokoll
- **SM1.**
    - SAP HANA MDC-Mandantensystem mit einem Host
    - Automatisch erkannt mit installiertem HANA-Plug-in auf HANA-Datenbank-Host
    - Verwendet NFS als Storage-Protokoll
- **SS2.**
    - SAP HANA Single-Host-MDC-Einzelmandant-System
    - Management über einen zentralen Plug-in-Host (SnapCenter-Server)
    - Verwendet NFS als Storage-Protokoll
- **SS3.**
    - SAP HANA Single-Host-MDC-Einzelmandant-System
    - Automatisch erkannt mit installiertem HANA-Plug-in auf HANA-Datenbank-Host
    - Verwendet Fibre Channel SAN als Storage-Protokoll

In den folgenden Abschnitten werden die vollständige Konfiguration sowie die Workflows für Backup, Wiederherstellung und Recovery beschrieben. Die Beschreibung behandelt lokale Snapshot Backups sowie die Replizierung auf Backup Storage mit SnapVault. Die Storage Virtual Machines (SVMs) sind `hana-primary` Für den primären Storage und `hana-backup` Für die externe Backup-Speicherung.

Der SnapCenter-Server wird als zentraler HANA-Plug-in-Host für die HANA-Systeme MS1 und SS2 verwendet.

Die folgende Abbildung zeigt die Laboreinrichtung.

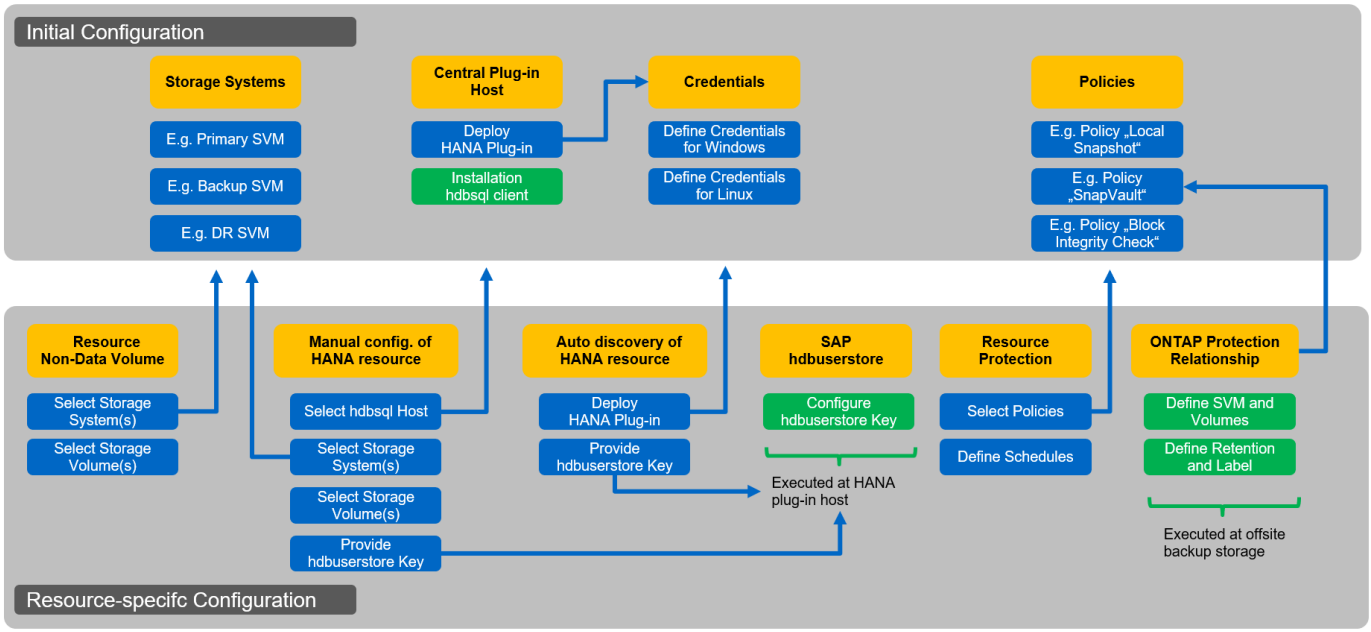


SnapCenter-Konfiguration

Die SnapCenter Konfiguration lässt sich in zwei Hauptbereiche trennen:

- **Erstkonfiguration.** umfasst allgemeine Konfigurationen, unabhängig von einer einzelnen SAP HANA Datenbank. Konfigurationen wie Storage-Systeme, zentrale HANA-Plug-in-Hosts und Richtlinien, die bei Ausführung der ressourcenspezifischen Konfigurationen ausgewählt werden.
- **Ressourcenspezifische Konfiguration.** umfasst SAP HANA systemspezifische Konfigurationen und muss für jede SAP HANA Datenbank durchgeführt werden.

Die folgende Abbildung bietet einen Überblick über die Konfigurationskomponenten und ihre Abhängigkeiten. Die grünen Felder zeigen Konfigurationsschritte, die außerhalb von SnapCenter ausgeführt werden müssen. Die blauen Felder zeigen die Schritte auf, die über die SnapCenter-Benutzeroberfläche ausgeführt werden.



Bei der Erstkonfiguration werden die folgenden Komponenten installiert und konfiguriert:

- **Storage-System.** Credential-Konfiguration für alle SVMs, die von den SAP HANA Systemen verwendet werden: In der Regel primärer Storage, externer Backup- und Disaster Recovery-Storage.

> Die auch Storage-Cluster-Anmeldedaten können anstelle einzelner SVM-Anmeldedaten konfiguriert werden.

- **Anmeldeinformationen** Konfiguration von Anmeldeinformationen, die zur Bereitstellung des SAP HANA-Plug-ins auf den Hosts verwendet werden.
- **Hosts (für zentrale HANA-Plug-in-Hosts).** Bereitstellung von SAP HANA-Plug-in. Installation der SAP HANA hdbclient-Software auf dem Host. Die SAP hdbclient-Software muss manuell installiert werden.
- **Richtlinien.** Konfiguration von Backup-Typ, Aufbewahrung und Replikation. In der Regel sind mindestens eine Richtlinie für lokale Snapshot-Kopien, eine für SnapVault-Replizierung und eine für dateibasiertes Backup erforderlich.

Die ressourcenspezifische Konfiguration muss für jede SAP HANA Datenbank durchgeführt werden und umfasst die folgenden Konfigurationen:

- Konfiguration der nicht datenvolumenlosen SAP HANA-Ressource:
  - Storage-Systeme und Volumes
- SAP hdbuserstore Schlüsselkonfiguration:
  - Die SAP hdbuserstore Schlüsselkonfiguration für die spezifische SAP HANA Datenbank muss entweder auf dem zentralen Plug-in-Host oder auf dem HANA-Datenbank-Host erfolgen, je nachdem, wo das HANA-Plug-in bereitgestellt wird.
- Automatisch erkannte SAP HANA Datenbankressourcen:
  - Implementierung des SAP HANA Plug-ins auf dem Datenbank-Host
  - Geben Sie den hdbuserstore-Schlüssel an
- Manuelle Konfiguration der SAP HANA-Datenbankressourcen:
  - SAP HANA Datenbank-SID, Plug-in-Host, hdbuserstore-Schlüssel, Storage-Systeme und Volumes
- Konfiguration für Ressourcenschutz:
  - Auswahl der erforderlichen Richtlinien
  - Definition von Zeitplänen für die einzelnen Richtlinien
- Konfiguration der ONTAP Datensicherung:
  - Nur erforderlich, wenn die Backups in einen externen Backup-Storage repliziert werden sollen.
  - Definition von Beziehung und Aufbewahrung

Erstkonfiguration von SnapCenter

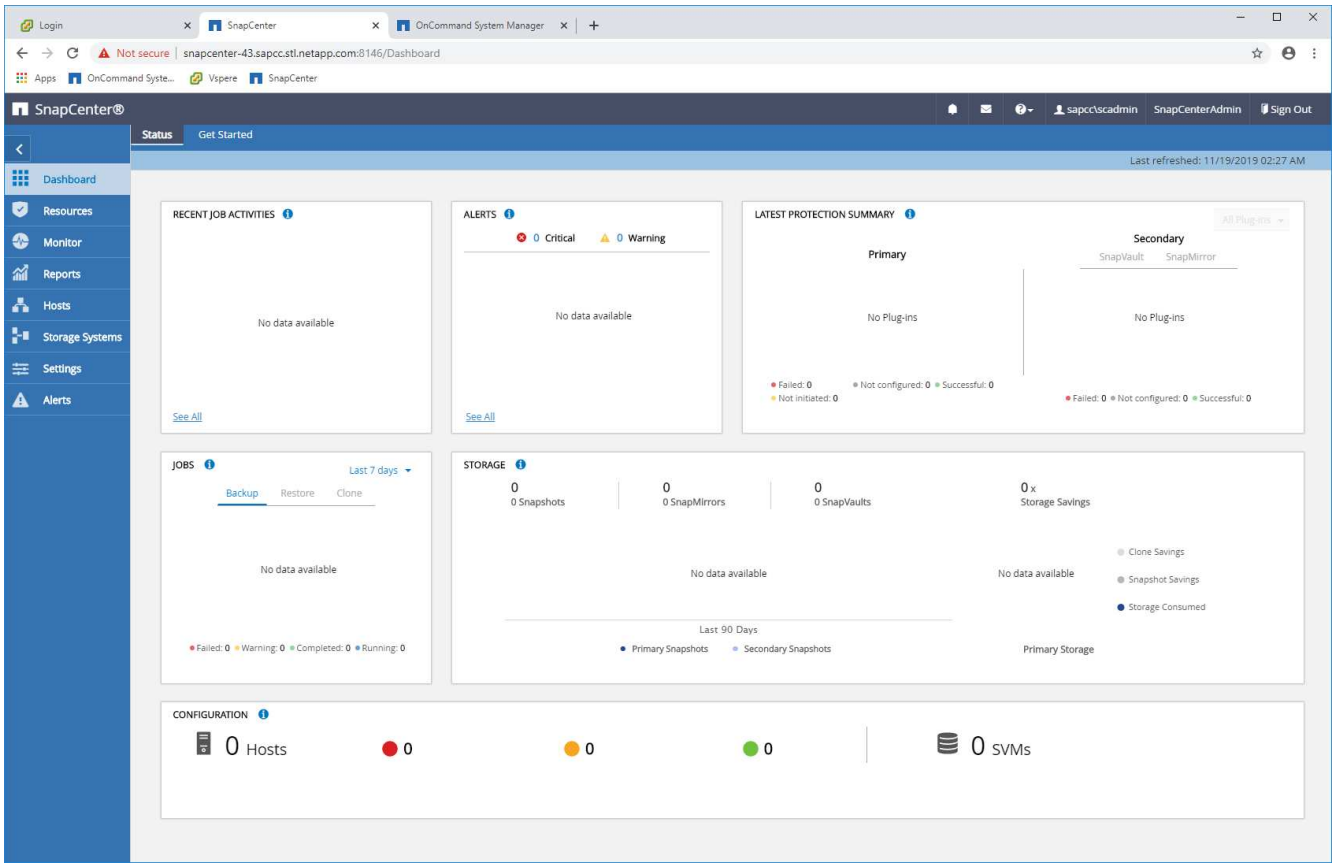
Die Erstkonfiguration umfasst die folgenden Schritte:

1. Konfiguration des Storage-Systems
2. Konfiguration von Anmeldeinformationen für die Plug-in-Installation
3. Für einen zentralen HANA-Plug-in-Host:
   a. Host-Konfiguration und SAP HANA Plug-in-Implementierung
   b. Installation und Konfiguration der SAP HANA hdbsql Client-Software
4. Konfiguration von Richtlinien

In den folgenden Abschnitten werden die ersten Konfigurationsschritte beschrieben.

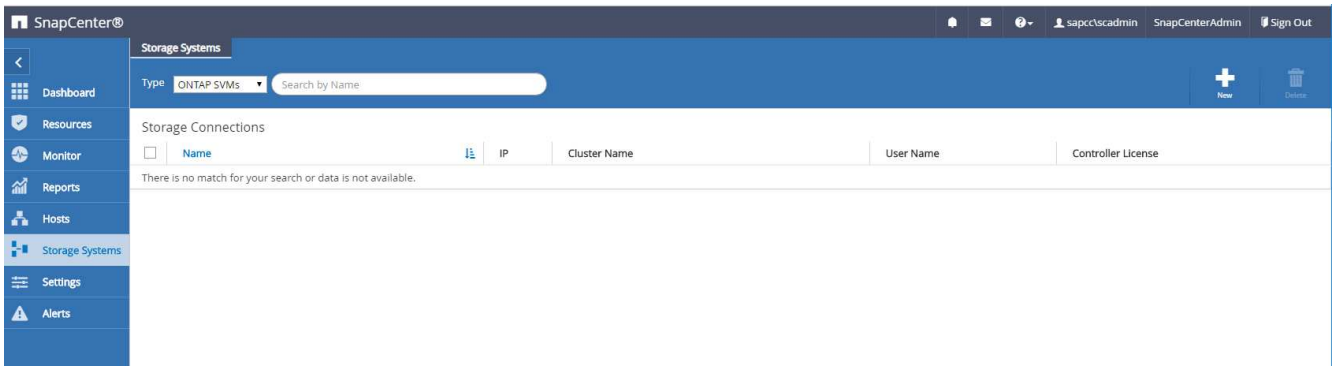
Konfiguration des Storage-Systems

1. Melden Sie sich bei der SnapCenter-ServerGUI an.



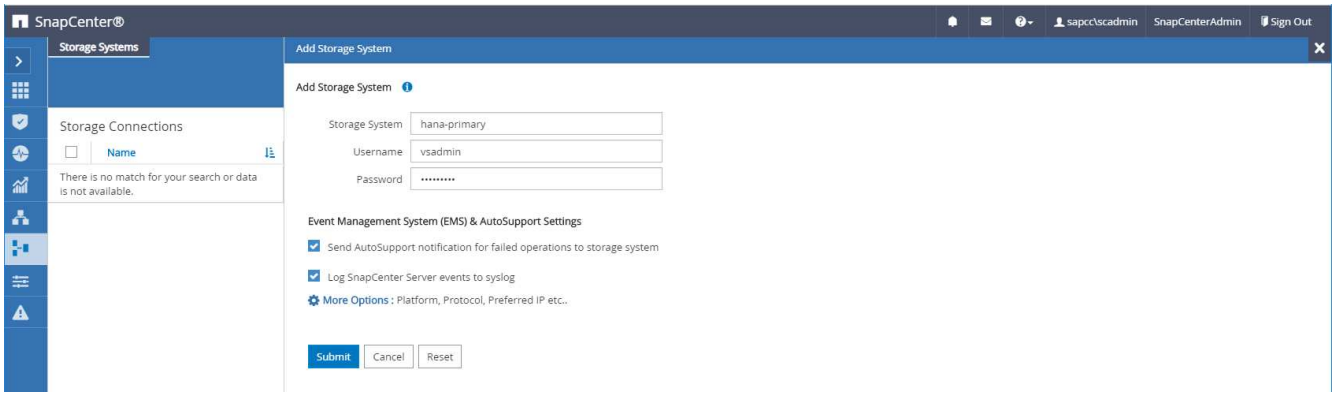
2. Wählen Sie Storage Systems Aus.

> Im Bildschirm können Sie den Storage-System-Typ auswählen, der ONTAP SVMs oder ONTAP Cluster sein kann. Wenn Sie die Storage-Systeme auf SVM-Ebene konfigurieren, müssen Sie für jede SVM eine Management-LIF konfiguriert haben. Alternativ können Sie einen SnapCenter-Managementzugriff auf Cluster-Ebene verwenden. Das SVM-Management wird im folgenden Beispiel verwendet.



3. Klicken Sie auf Neu, um ein Speichersystem hinzuzufügen und den erforderlichen Hostnamen und die erforderlichen Anmeldeinformationen anzugeben.

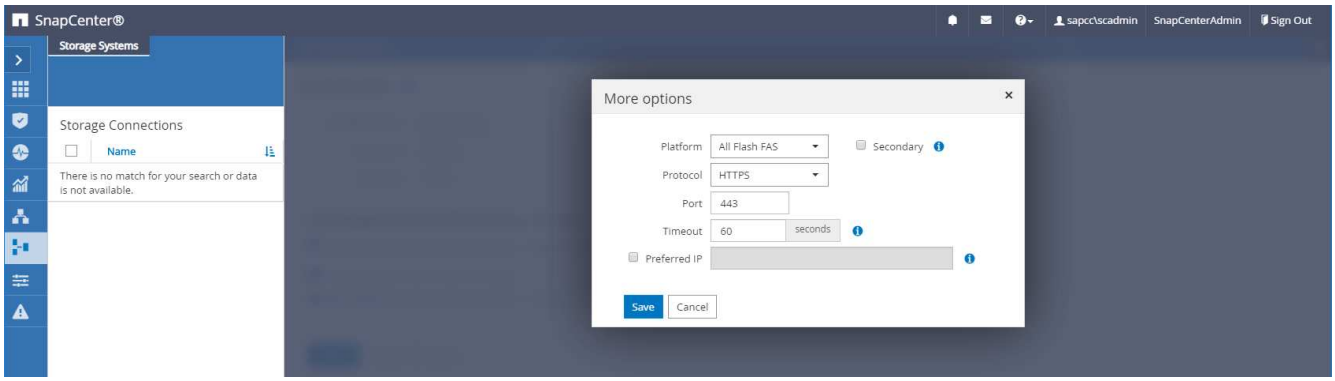
> Der SVM-Benutzer muss nicht der vsadmin-Benutzer sein, wie in dem Screenshot dargestellt. In der Regel wird ein Benutzer für die SVM konfiguriert und den erforderlichen Berechtigungen zum Ausführen von Backup- und Restore-Vorgängen zugewiesen. Einzelheiten zu den erforderlichen Berechtigungen finden Sie im "SnapCenter Installationshandbuch" Im Abschnitt „Minimale ONTAP-Berechtigungen erforderlich“.



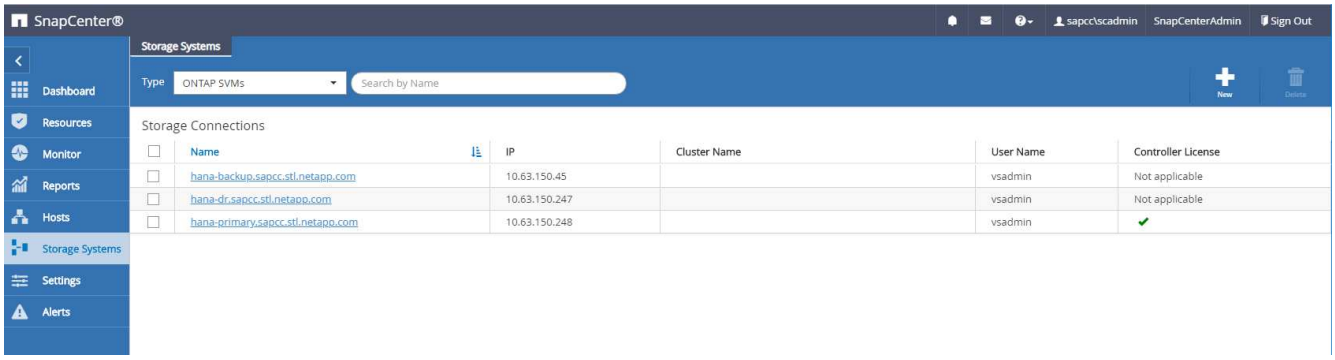
4. Klicken Sie auf Mehr Optionen, um die Storage-Plattform zu konfigurieren.

   Als Storage-Plattform können FAS, AFF, ONTAP Select oder Cloud Volumes ONTAP verwendet werden.

   > Wählen Sie bei einem System, das als SnapVault- oder SnapMirror-Ziel verwendet wird, das sekundäre Symbol aus.

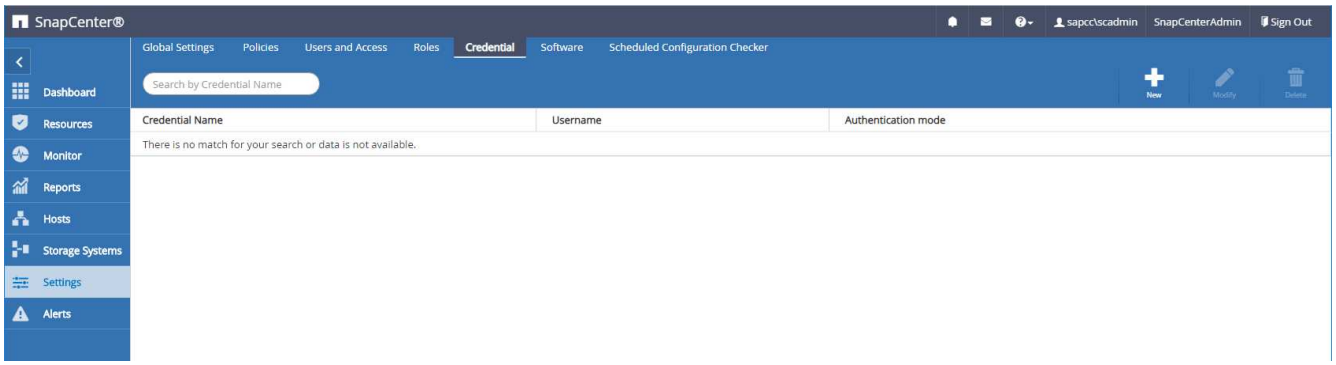


5. Fügen Sie bei Bedarf zusätzliche Storage-Systeme hinzu. Beispielsweise wurde ein zusätzlicher externer Backup-Storage und eine Disaster Recovery-Storage hinzugefügt.

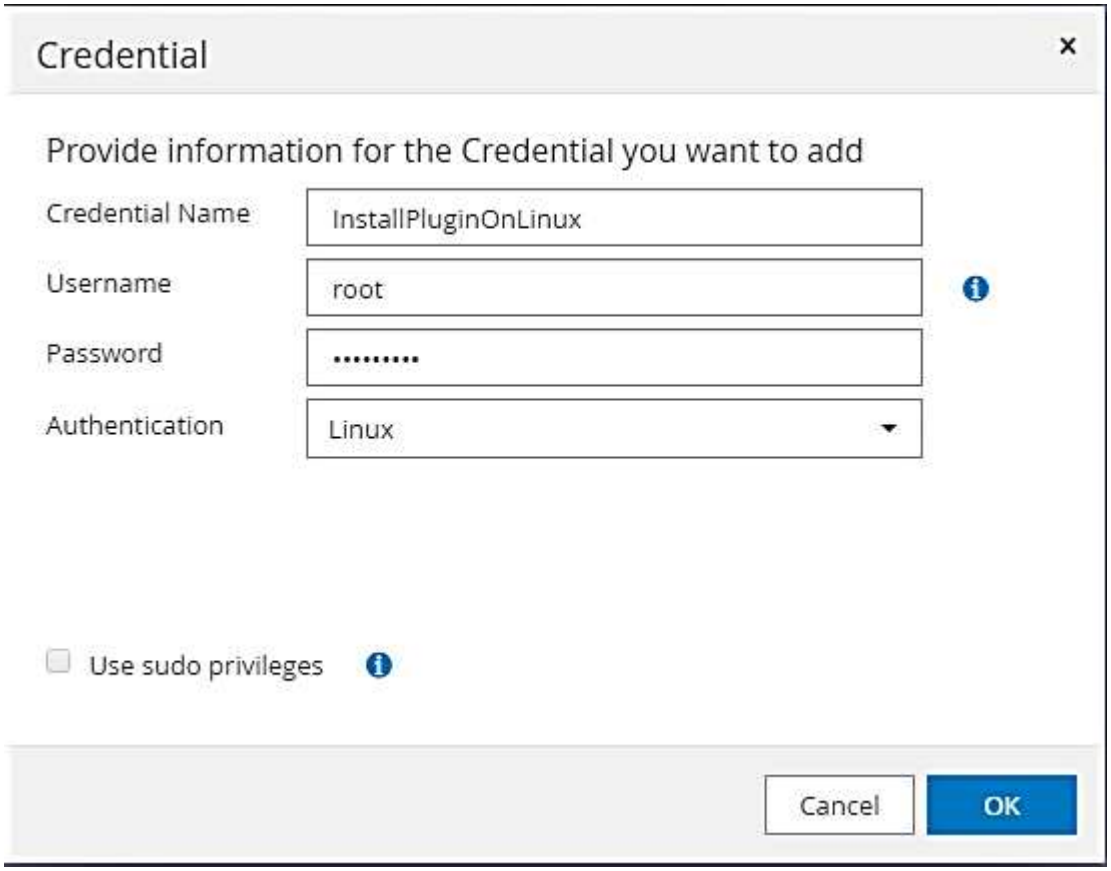


Konfiguration von Anmeldeinformationen

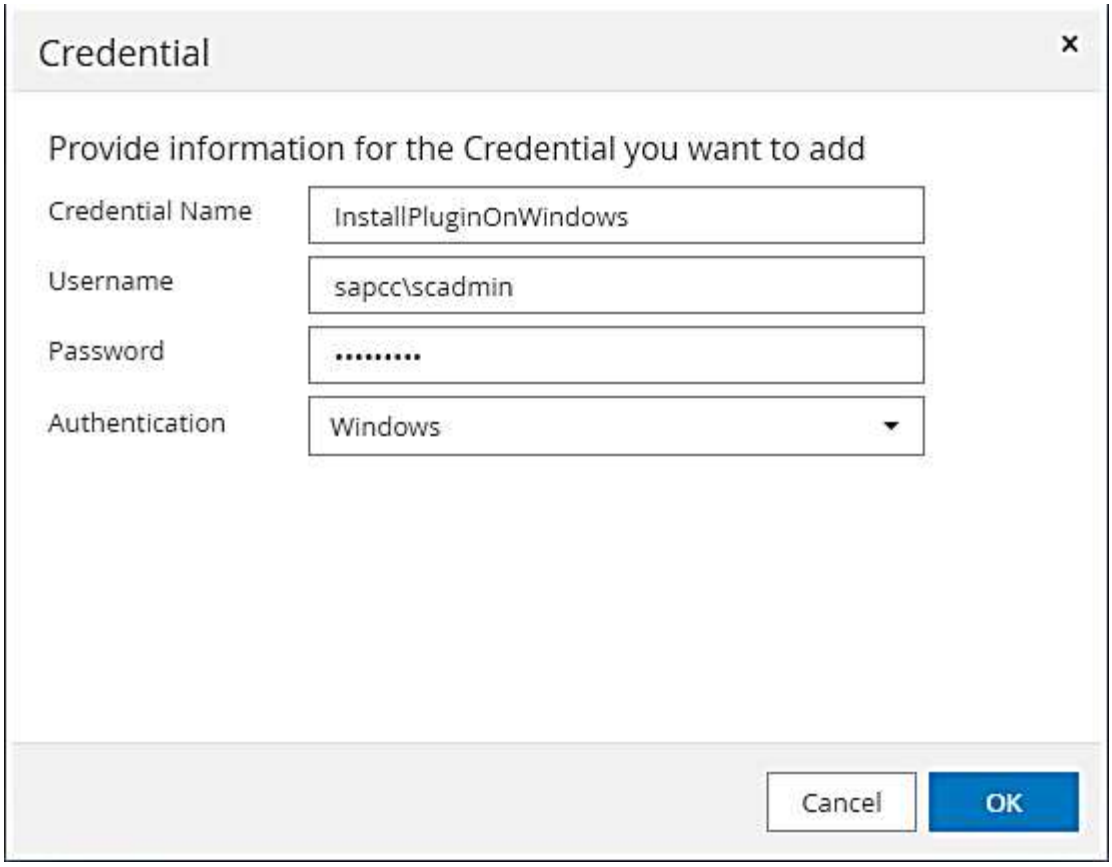
1. Gehen Sie zu Einstellungen, wählen Sie Anmeldeinformationen aus, und klicken Sie auf Neu.



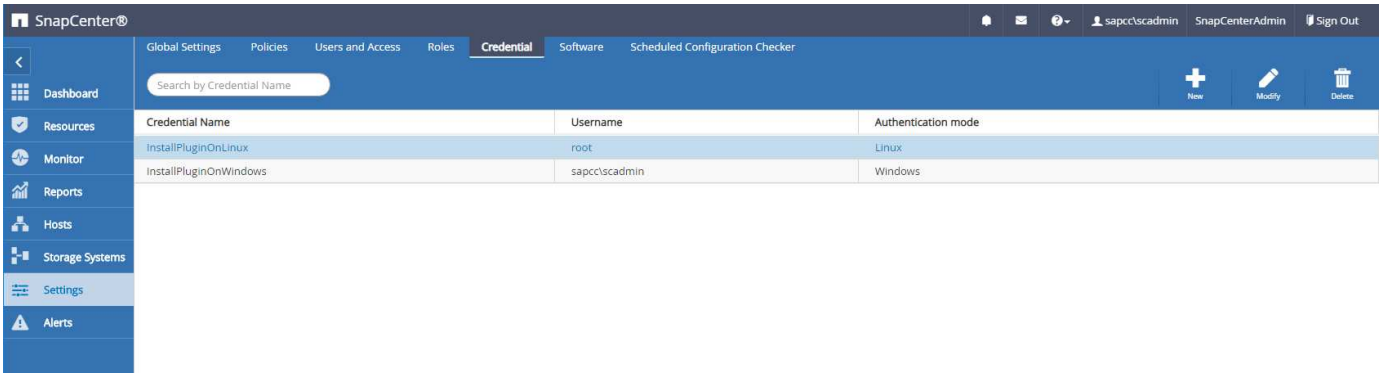
2. Geben Sie die Anmeldeinformationen für den Benutzer an, der für Plug-in-Installationen auf Linux-Systemen verwendet wird.



3. Geben Sie die Anmeldeinformationen für den Benutzer an, der für Plug-in-Installationen auf Windows-Systemen verwendet wird.



Die folgende Abbildung zeigt die konfigurierten Anmeldedaten.

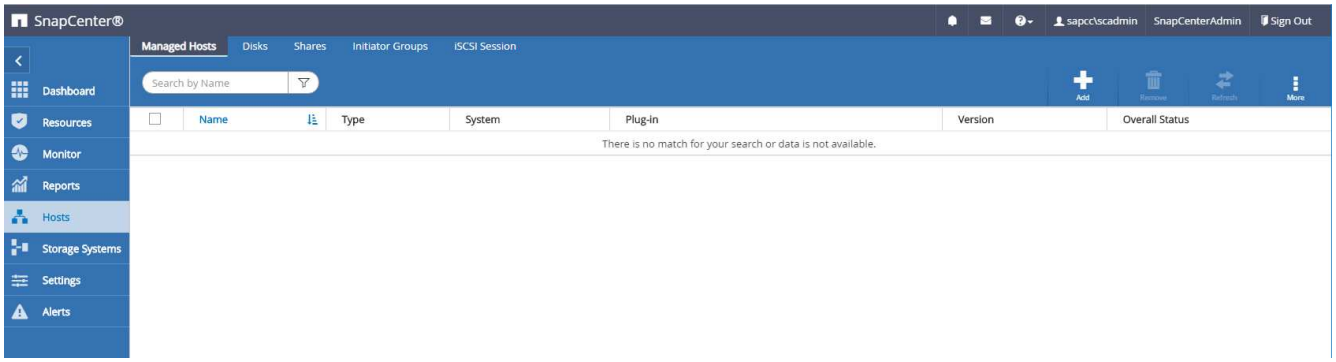


SAP HANA Plug-in-Installation auf einem zentralen Plug-in-Host

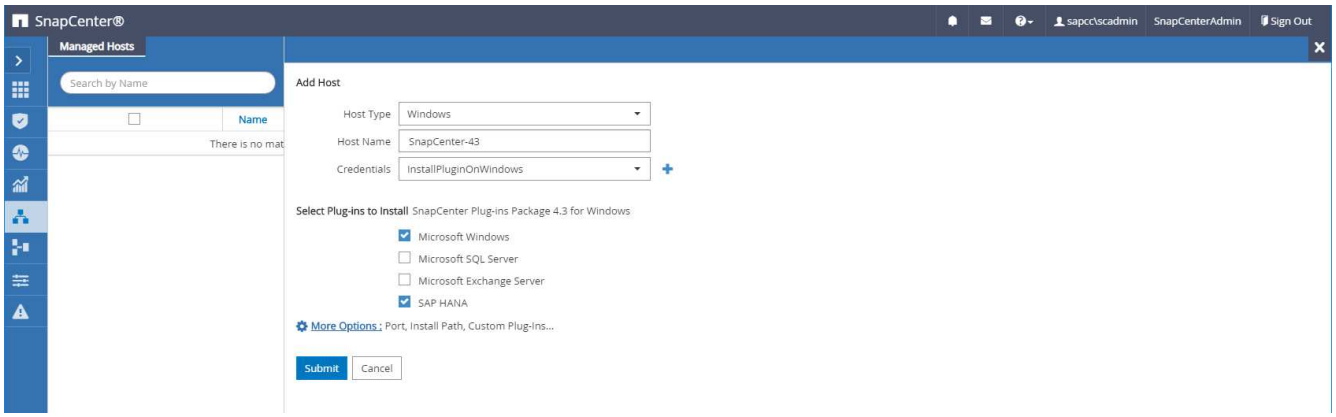
Bei der Lab-Einrichtung wird der SnapCenter-Server auch als zentraler HANA-Plug-in-Host verwendet. Der Windows-Host, auf dem SnapCenter Server ausgeführt wird, wird als Host hinzugefügt, und das SAP HANA-Plug-in ist auf dem Windows-Host installiert.

> Für das SAP HANA Plug-in ist Java 64-Bit Version 1.8 erforderlich. Vor der Bereitstellung des SAP HANA Plug-ins muss Java auf dem Host installiert sein.

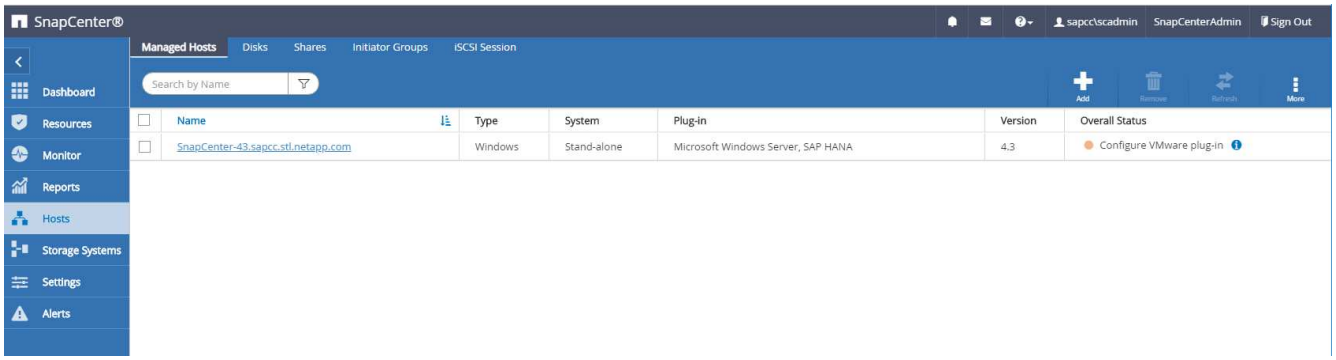
1. Gehen Sie zu Hosts und klicken Sie auf Hinzufügen.



2. Geben Sie die erforderlichen Hostinformationen ein. Klicken Sie Auf Senden.



Die folgende Abbildung zeigt alle konfigurierten Hosts, die nach der Implementierung des HANA-Plug-ins konfiguriert wurden.



Installation und Konfiguration der SAP HANA hdbsql Client-Software

Die SAP HANA hdbsql-Client-Software muss auf dem gleichen Host installiert sein, auf dem das SAP HANA-Plug-in installiert ist. Die Software kann von heruntergeladen werden "SAP-Supportportal".

Der während der Ressourcenkonfiguration konfigurierte HDBSQL OS-Benutzer muss in der Lage sein, die ausführbare Datei hdbsql auszuführen. Der Pfad zur ausführbaren Datei hdbsql muss im konfiguriert werden `hana.properties` Datei:

- Windows:

```
C:\More C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in
Creator\etc\hana.properties
HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql.exe
```

- Linux

```
cat /opt/NetApp/snapcenter/scc/etc/hana.properties
HANA_HDBSQL_CMD=/usr/sap/hdbclient/hdbsql
```

Konfiguration von Richtlinien

Wie im Abschnitt beschrieben "„Datensicherungsstrategie“," Richtlinien werden normalerweise unabhängig von der Ressource konfiguriert und können von mehreren SAP HANA Datenbanken verwendet werden.

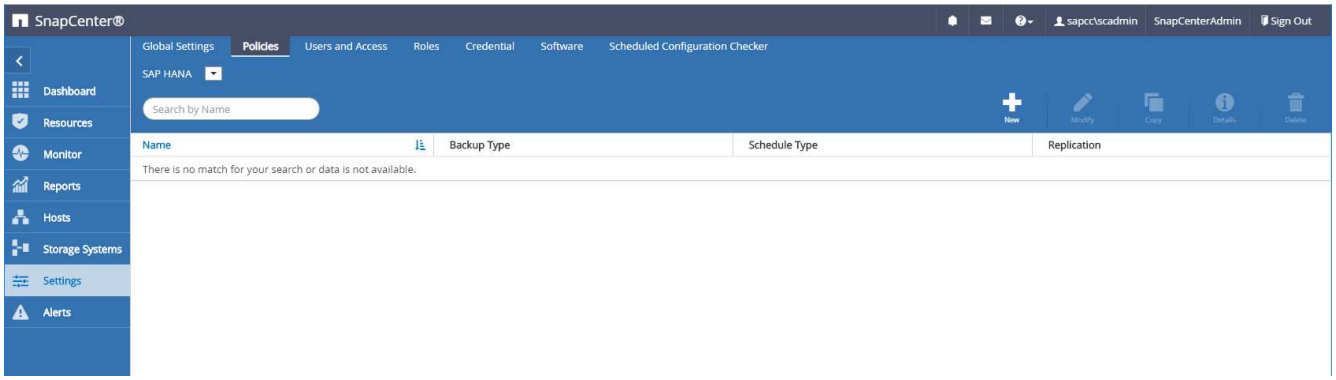
Eine typische Minimalkonfiguration umfasst folgende Richtlinien:

- Richtlinie für stündliche Backups ohne Replikation: `LocalSnap`
- Richtlinie für tägliche Backups mit SnapVault-Replikation: `LocalSnapAndSnapVault`
- Richtlinie für wöchentliche Blockintegritätsprüfung über ein dateibasiertes Backup: `BlockIntegrityCheck`

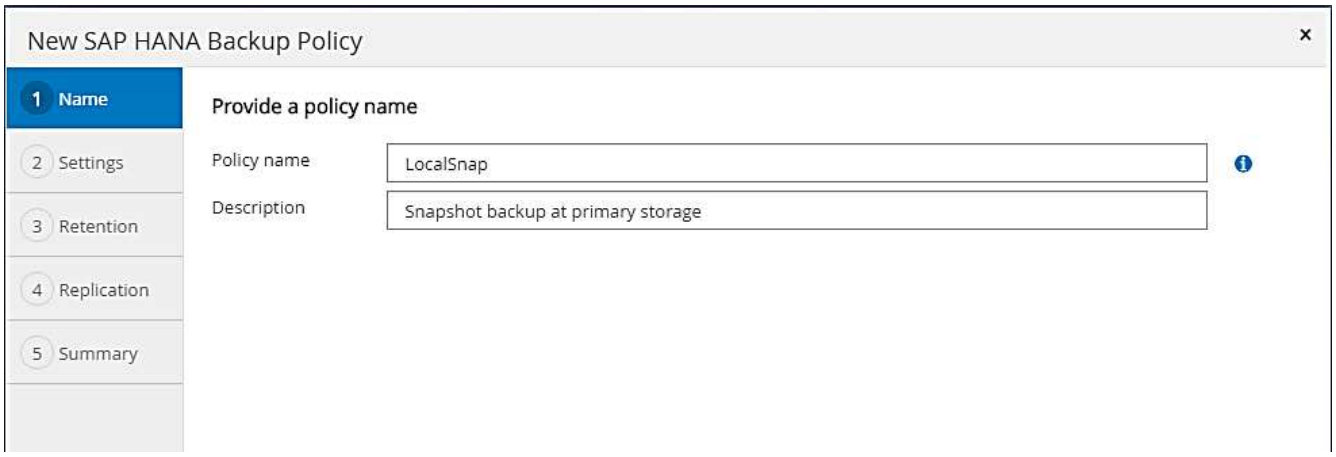
In den folgenden Abschnitten wird die Konfiguration dieser drei Richtlinien beschrieben.

Richtlinie für stündliche Snapshot Backups

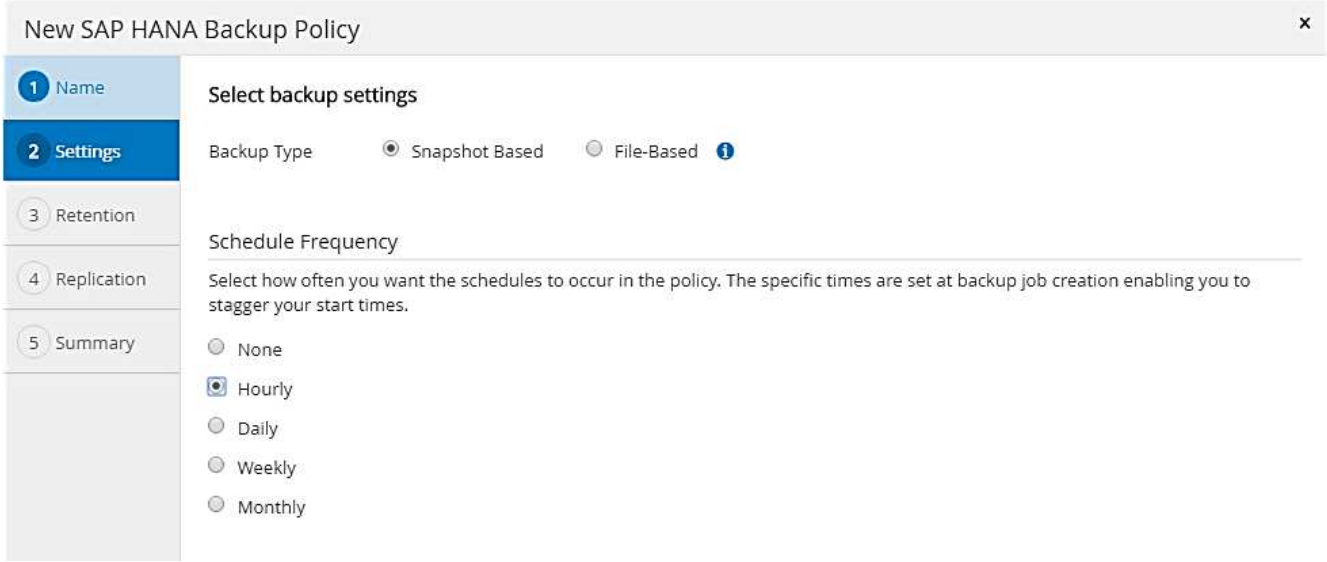
1. Gehen Sie zu Einstellungen > Richtlinien, und klicken Sie auf Neu.



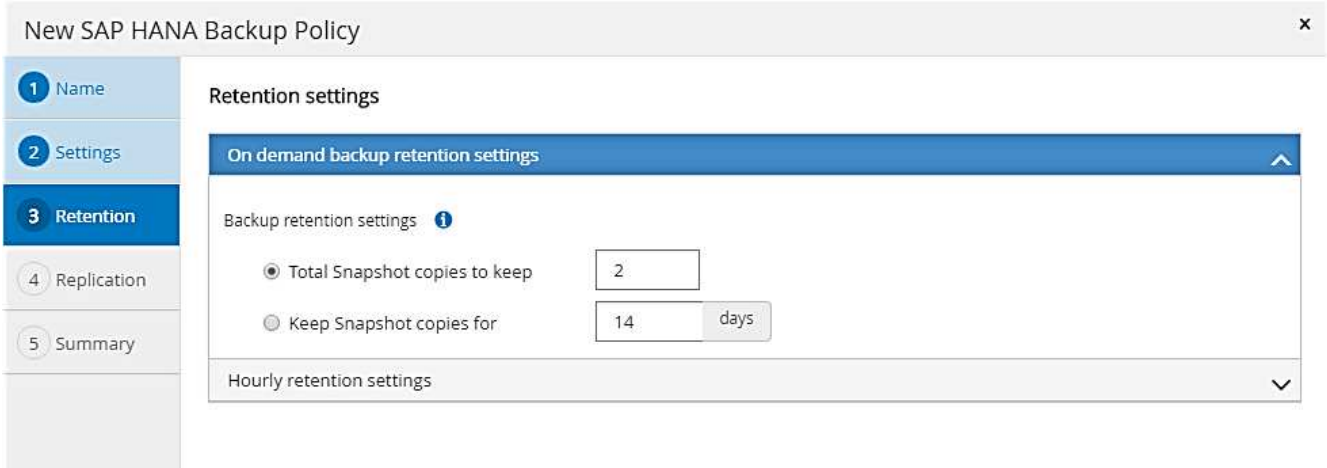
2. Geben Sie den Namen und die Beschreibung der Richtlinie ein. Klicken Sie Auf Weiter.



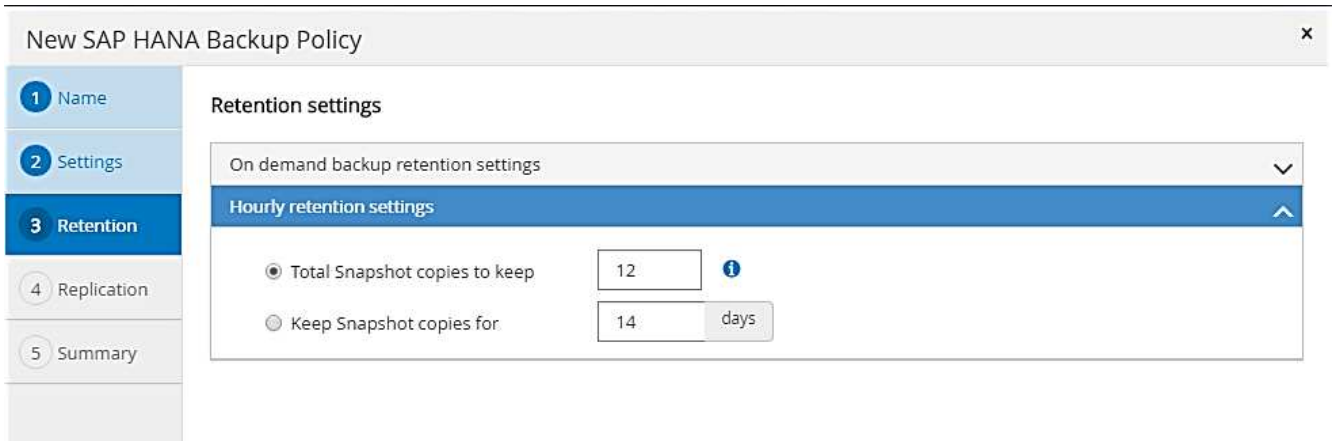
3. Wählen Sie den Backup-Typ als Snapshot-basiert aus und wählen Sie stündlich für die Zeitplanfrequenz aus.



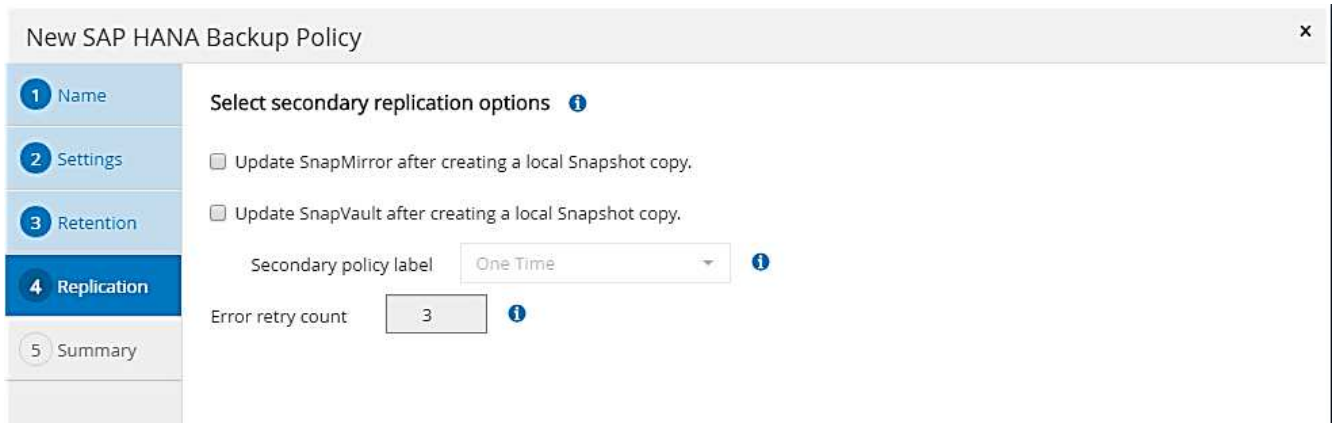
4. Konfigurieren Sie die Aufbewahrungseinstellungen für On-Demand-Backups.



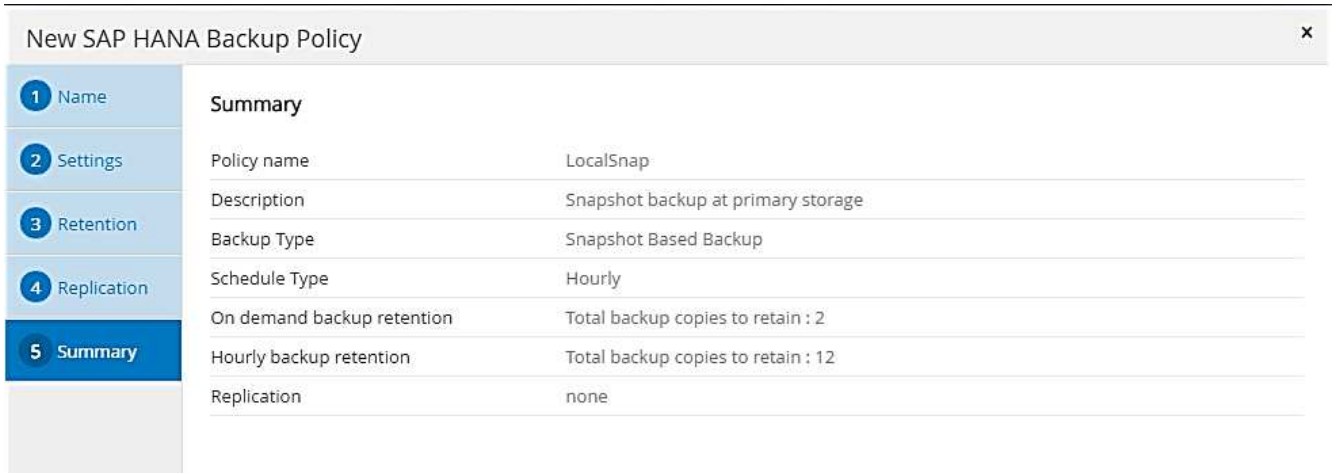
5. Konfigurieren Sie die Aufbewahrungseinstellungen für geplante Backups.



6. Konfigurieren der Replikationsoptionen. In diesem Fall ist kein SnapVault oder SnapMirror Update ausgewählt.

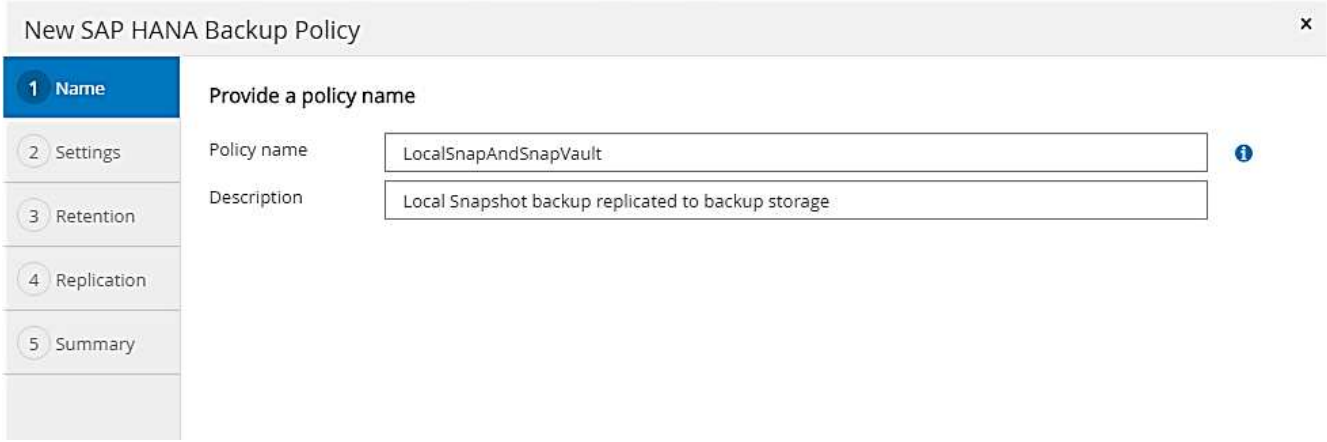


7. Klicken Sie auf der Seite Zusammenfassung auf Fertig stellen.

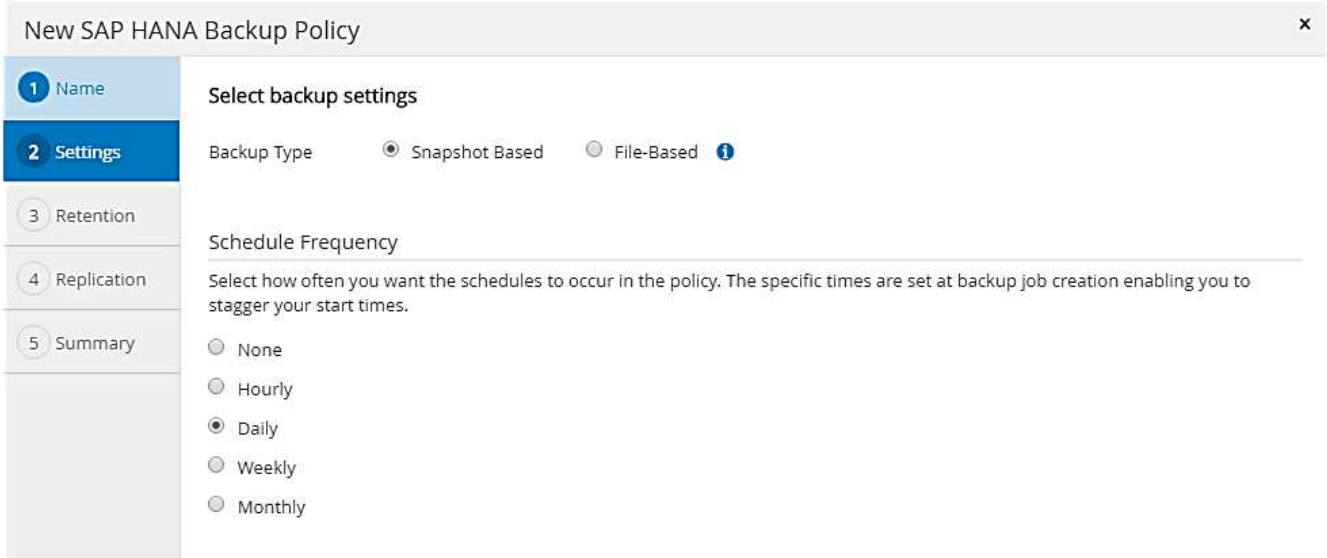


Richtlinie für tägliche Snapshot Backups mit SnapVault Replizierung

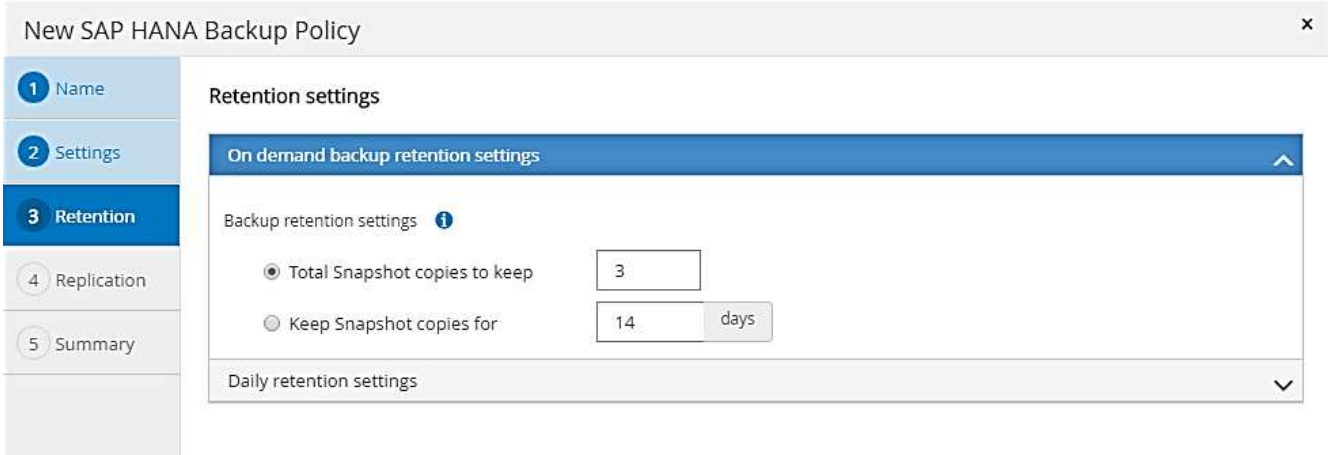
1. Gehen Sie zu Einstellungen > Richtlinien, und klicken Sie auf Neu.
2. Geben Sie den Namen und die Beschreibung der Richtlinie ein. Klicken Sie Auf Weiter.



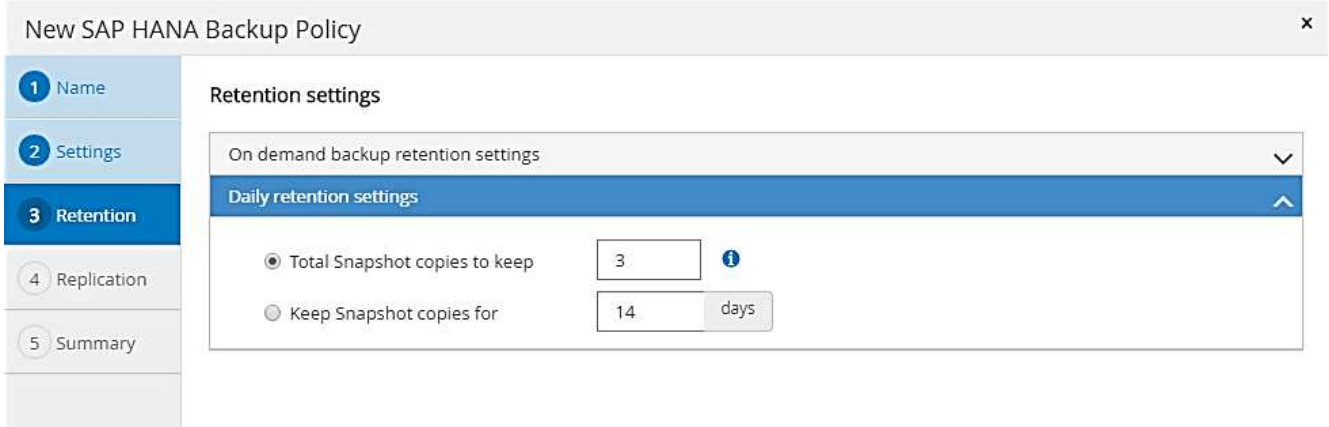
3. Legen Sie den Backup-Typ auf Snapshot-basiert und die Zeitplanfrequenz auf täglich fest.



4. Konfigurieren Sie die Aufbewahrungseinstellungen für On-Demand-Backups.

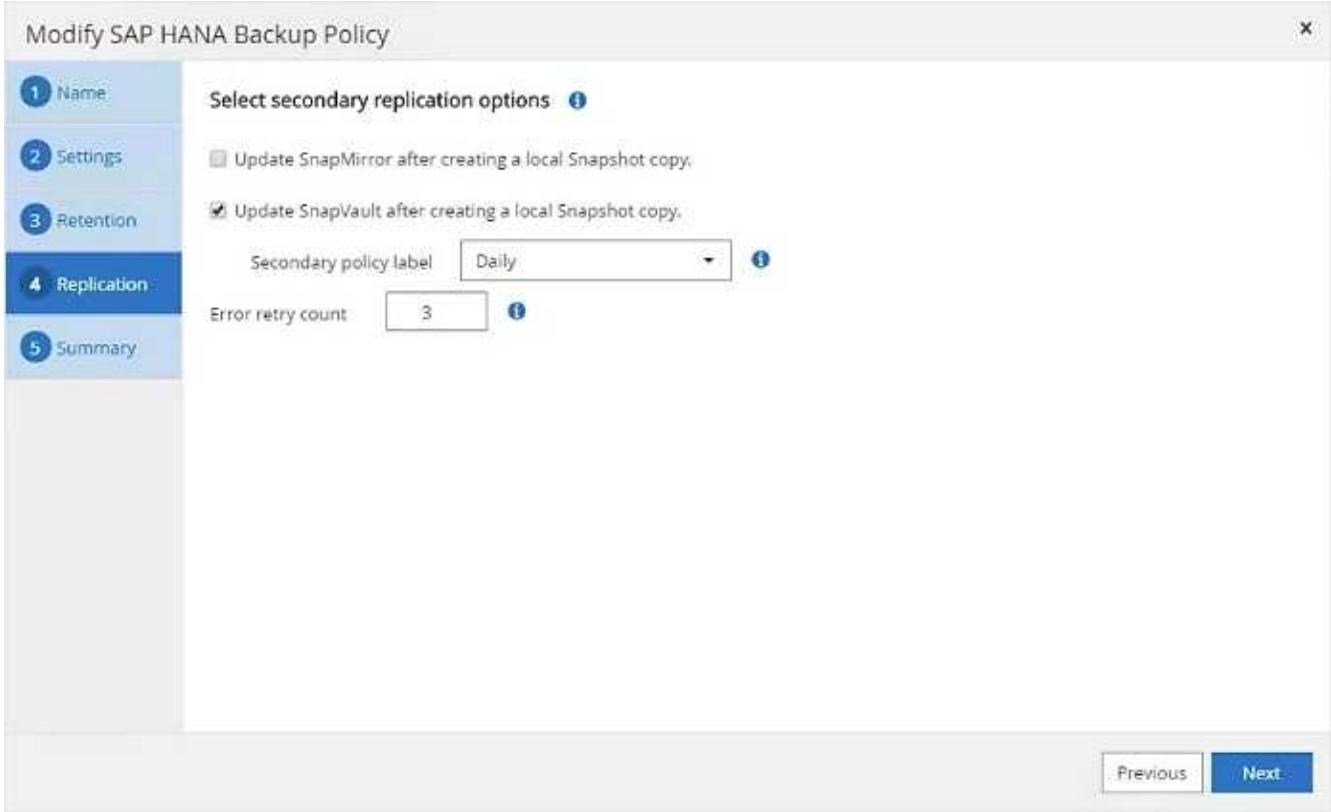


5. Konfigurieren Sie die Aufbewahrungseinstellungen für geplante Backups.

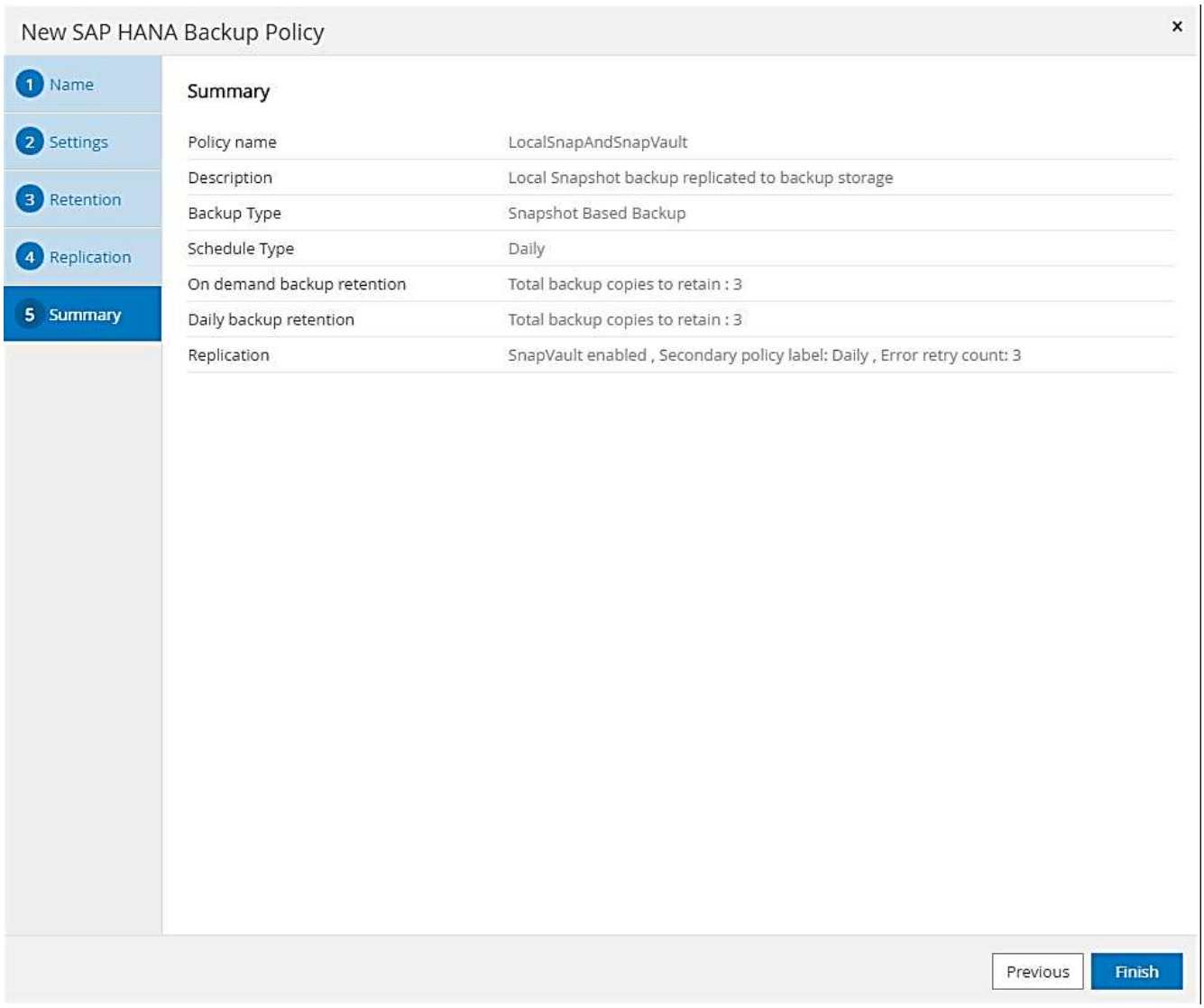


6. Wählen Sie SnapVault aktualisieren aus, nachdem Sie eine lokale Snapshot-Kopie erstellt haben.

> Das sekundäre Richtlinienetikett muss mit dem SnapMirror Etikett in der Datensicherungskonfiguration auf der Storage-Ebene identisch sein. Siehe Abschnitt "„Konfiguration von Datenschutz auf externen Backup-Speicher“."

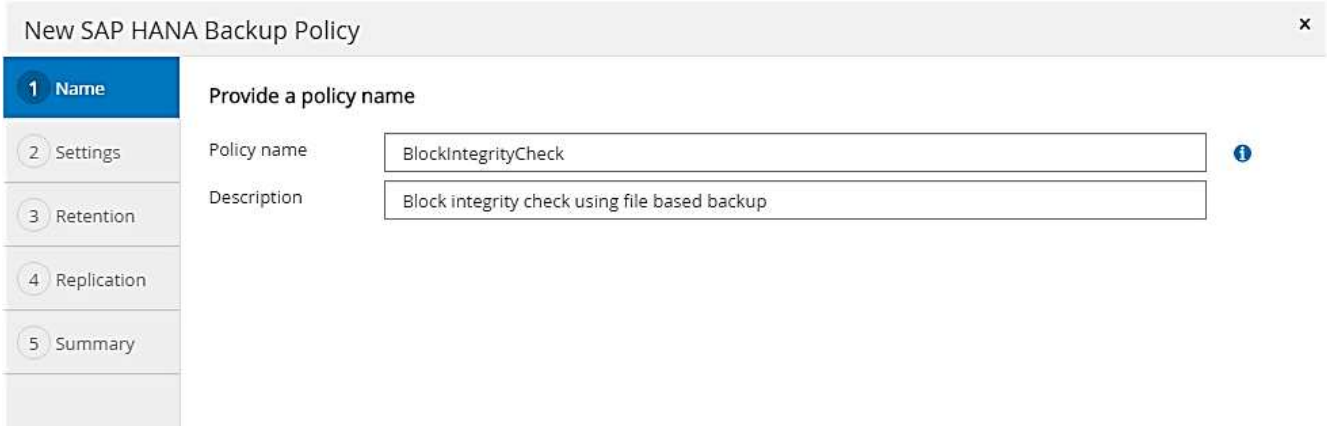


7. Klicken Sie auf der Seite Zusammenfassung auf Fertig stellen.

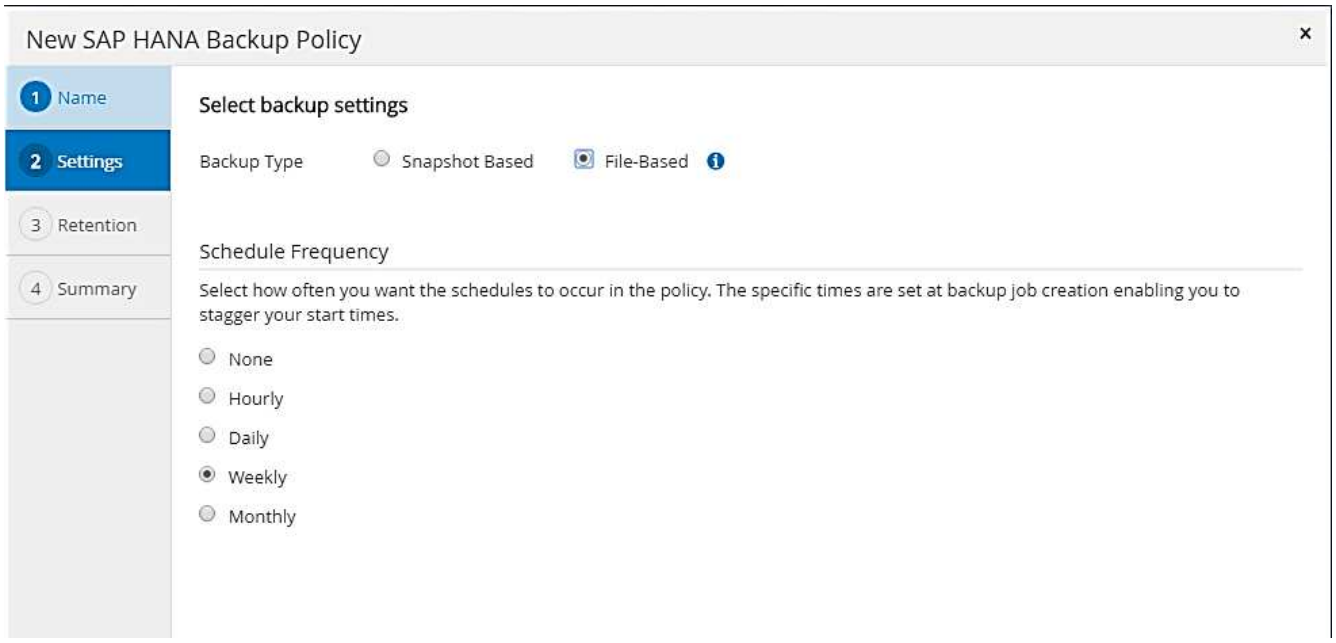


Richtlinie für die wöchentliche Blockintegritätsprüfung

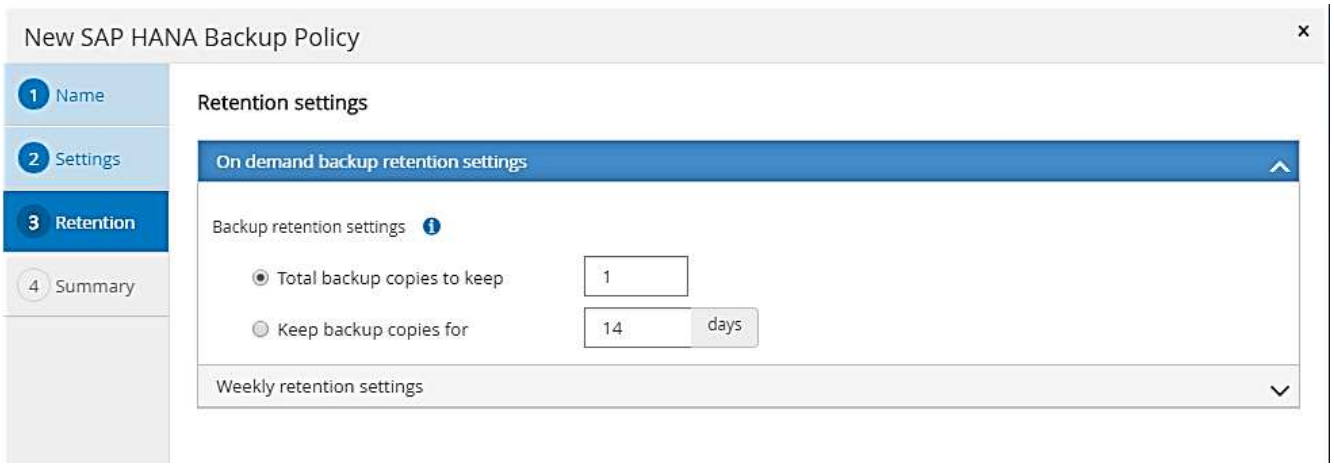
1. Gehen Sie zu Einstellungen > Richtlinien, und klicken Sie auf Neu.
2. Geben Sie den Namen und die Beschreibung der Richtlinie ein. Klicken Sie Auf Weiter.



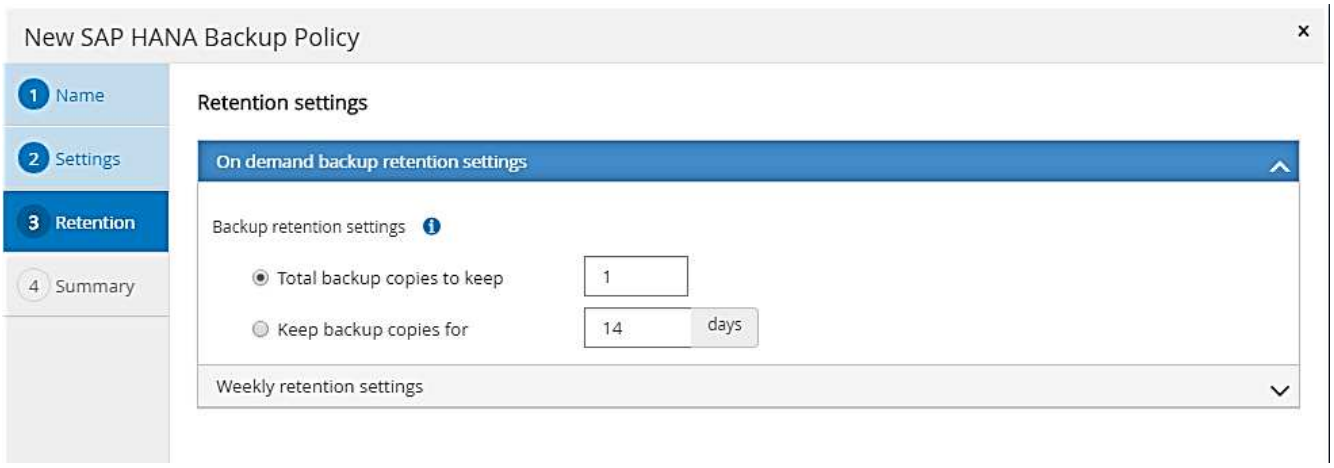
3. Legen Sie den Sicherungstyp auf „File-based“ und „Schedule Frequency“ auf „Weekly“ fest.



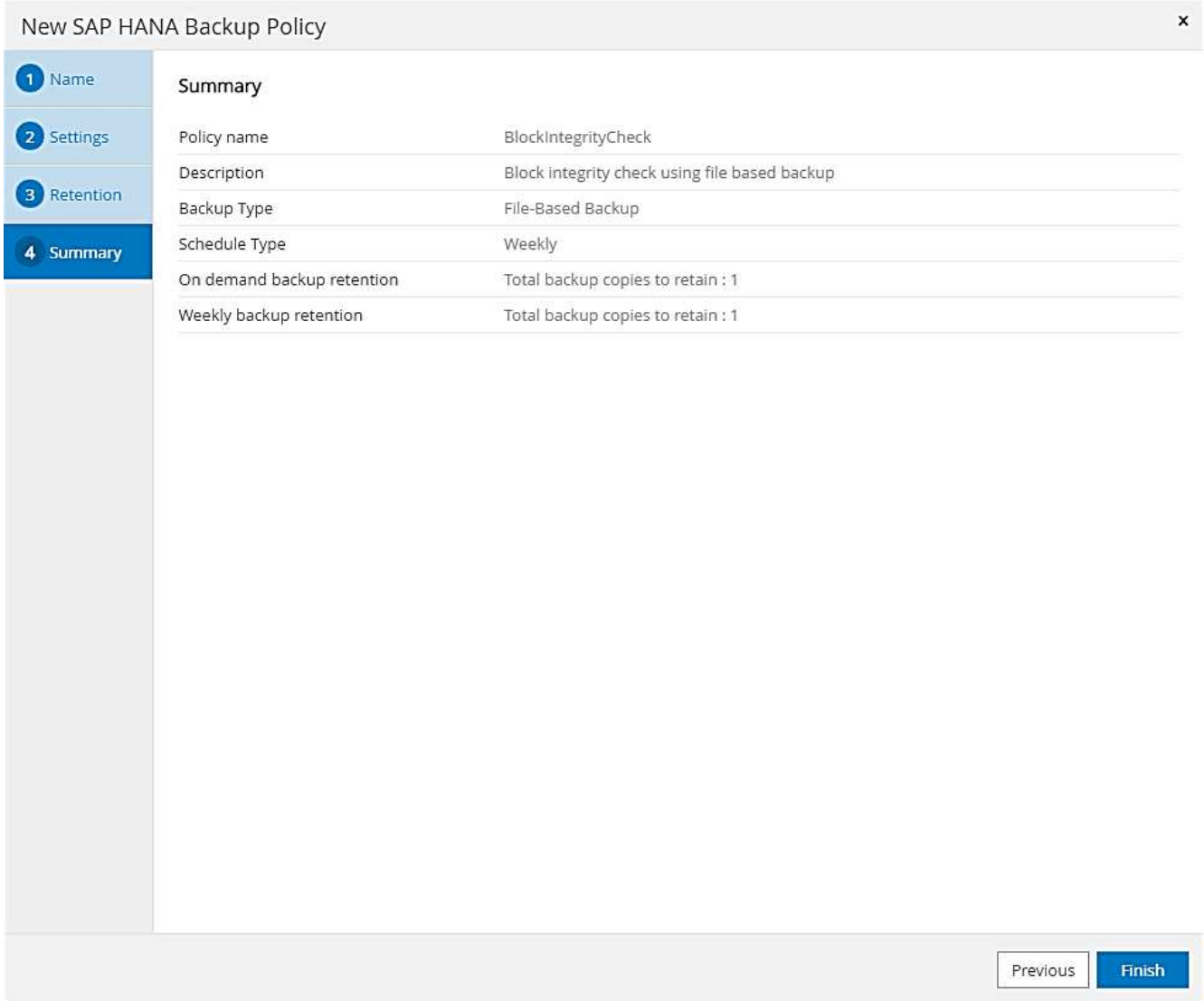
4. Konfigurieren Sie die Aufbewahrungseinstellungen für On-Demand-Backups.



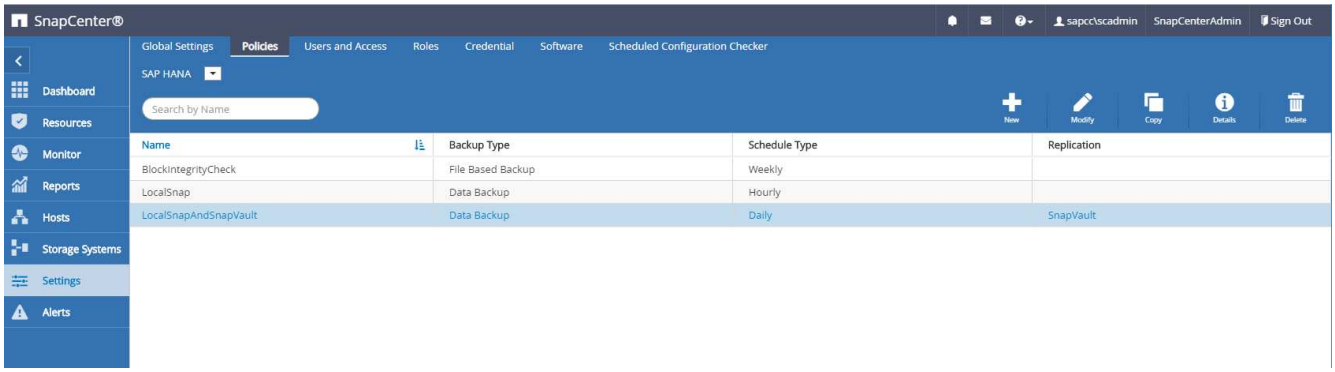
5. Konfigurieren Sie die Aufbewahrungseinstellungen für geplante Backups.



6. Klicken Sie auf der Seite Zusammenfassung auf Fertig stellen.



Die folgende Abbildung zeigt eine Zusammenfassung der konfigurierten Richtlinien.



Ressourcenspezifische SnapCenter Konfiguration für SAP HANA Datenbank-Backups

In diesem Abschnitt werden die Konfigurationsschritte für zwei Beispielkonfigurationen beschrieben.

- **SS2.**
  - SAP HANA MDC, ein mandantenfähiges Single-Host-System mit NFS für Storage-Zugriff
  - Die Ressource wird manuell in SnapCenter konfiguriert.
  - Die Ressource ist so konfiguriert, lokale Snapshot Backups zu erstellen und mithilfe eines wöchentlichen dateibasierten Backups die Blockintegritätsprüfungen für die SAP HANA Datenbank durchzuführen.
- **SS1.**
  - SAP HANA MDC, ein mandantenfähiges Single-Host-System mit NFS für Storage-Zugriff
  - Die Ressource wird mit SnapCenter automatisch erkannt.
  - Die Ressource ist so konfiguriert, dass sie lokale Snapshot Backups erstellt, mithilfe von SnapVault auf einen externen Backup-Storage repliziert und mithilfe eines wöchentlichen dateibasierten Backups die Blockintegritätsprüfungen für die SAP HANA Datenbank durchführt.

Die Unterschiede zwischen einem SAN-Attached Storage, einem Single-Container oder einem System mit mehreren Hosts werden in den entsprechenden Konfigurations- oder Workflow-Schritten wiedergegeben.

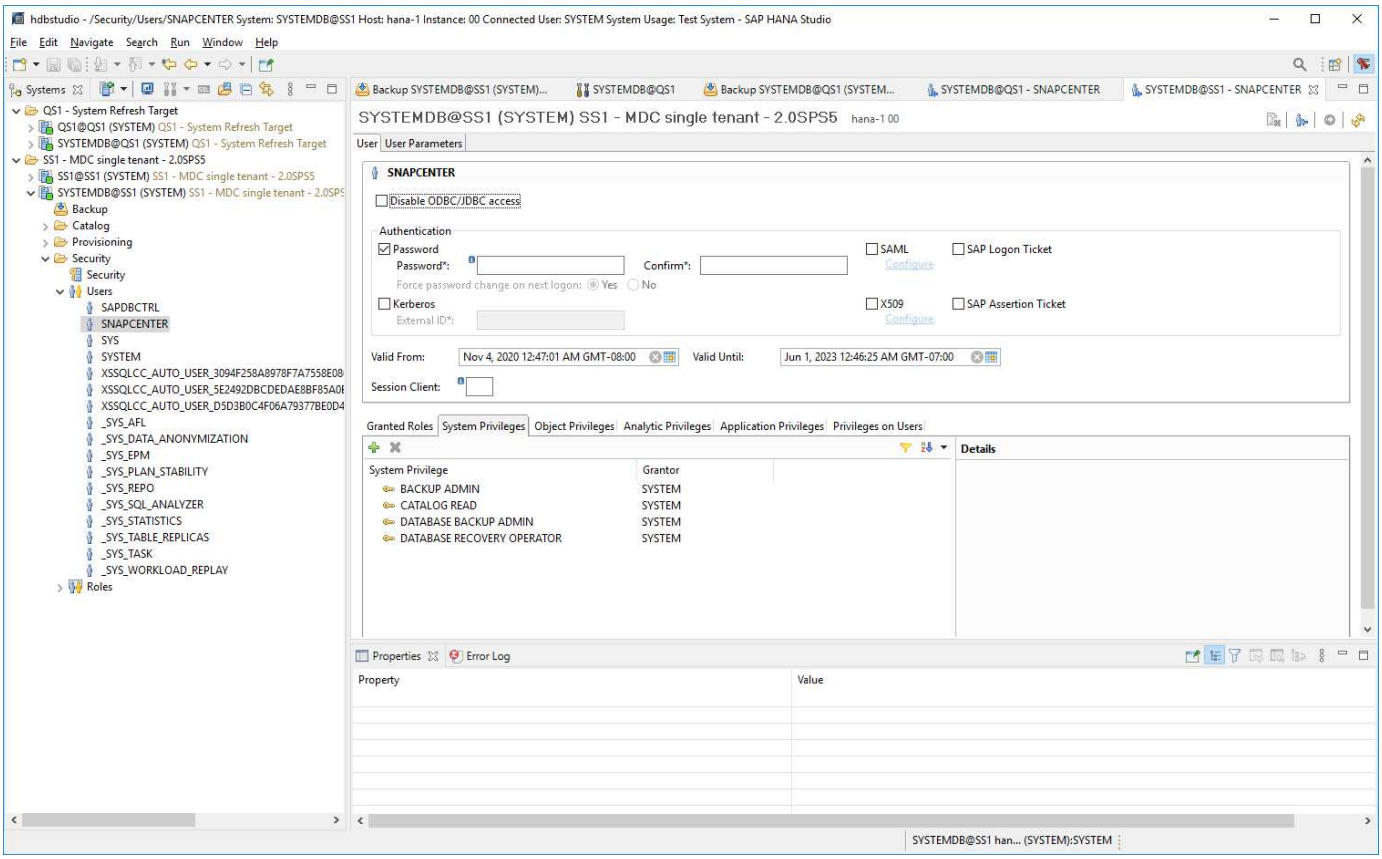
SAP HANA Backup-Benutzer und hdbuserstore-Konfiguration

NetApp empfiehlt, einen dedizierten Datenbankbenutzer in der HANA Datenbank zu konfigurieren, um Backup-Vorgänge mit SnapCenter auszuführen. Im zweiten Schritt wird für diesen Backup-Benutzer ein SAP HANA User Store Key konfiguriert und dieser User Store Key wird bei der Konfiguration des SnapCenter SAP HANA Plug-ins verwendet.

Die folgende Abbildung zeigt das SAP HANA Studio, über das der Backup-Benutzer erstellt werden kann.

> Die erforderlichen Berechtigungen wurden mit HANA 2.0 SPS5 Version geändert: Backup-Admin, Lesevorgang für den Katalog, Datenbank-Backup-Administrator und Datenbank-Recovery-Operator. Für ältere Versionen reichen der Backup-Administrator und der Lesevorgang des Katalogs aus.

> Bei einem SAP HANA MDC-System muss der Benutzer in der Systemdatenbank erstellt werden, da alle Backup-Befehle für das System und die Mandantendatenbanken über die Systemdatenbank ausgeführt werden.



Beim HANA-Plug-in-Host, auf dem das SAP HANA-Plug-in und der SAP-hdbsql-Client installiert sind, muss ein Benutzerspeicherschlüssel konfiguriert werden.

Userstore-Konfiguration auf dem SnapCenter-Server, der als zentraler HANA-Plug-in-Host verwendet wird

Wenn das SAP HANA-Plug-in und der SAP-hdbsql-Client unter Windows installiert sind, führt der lokale Systembenutzer die hdbsql-Befehle aus und wird standardmäßig in der Ressourcenkonfiguration konfiguriert. Da es sich bei dem Systembenutzer nicht um einen Anmeldesbenutzer handelt, muss die Konfiguration des Benutzerspeichers mit einem anderen Benutzer und mit der ausgeführt werden `-u <User>` Option.

```
hdbuserstore.exe -u SYSTEM set <key> <host>:<port> <database user>
<password>
```

> Die SAP HANA hdbclient-Software muss zuerst auf dem Windows-Host installiert sein.

Konfiguration des Benutzerspeichers auf einem separaten Linux-Host, der als zentraler HANA-Plug-in-Host verwendet wird

Wenn das SAP HANA-Plug-in und der SAP-hdbsql-Client auf einem separaten Linux-Host installiert sind, wird der folgende Befehl für die User-Store-Konfiguration verwendet, wobei der Benutzer in der Ressourcenkonfiguration definiert ist:

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

Die SAP HANA hdbclient-Software muss zuerst auf dem Linux-Host installiert sein.

UserStore-Konfiguration auf dem HANA-Datenbank-Host

Wenn das SAP HANA-Plug-in auf dem HANA-Datenbank-Host bereitgestellt wird, wird der folgende Befehl für die User Store-Konfiguration mit dem verwendet `<sid>adm` Benutzer:

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

SnapCenter verwendet das `<sid>adm` Benutzer zur Kommunikation mit der HANA-Datenbank. Daher muss der User Store Key mit dem <`sid>adm` Benutzer auf dem Datenbank-Host konfiguriert werden.

In der Regel wird die SAP HANA hdbsql-Client-Software zusammen mit der Datenbank-Server-Installation installiert. Wenn dies nicht der Fall ist, muss der hdbclient zuerst installiert werden.

Konfiguration des Benutzerspeichers abhängig von der HANA Systemarchitektur

In einer SAP HANA MDC-Einzelmandant-Einrichtung, Port `3<instanceNo>13` Ist der Standard-Port für den SQL-Zugriff auf die Systemdatenbank und muss in der hdbuserstore-Konfiguration verwendet werden.

Für eine SAP HANA-Installation mit einem Container ist Port erforderlich `3<instanceNo>15` Ist der Standard-Port für den SQL-Zugriff auf den Indexserver und muss in der hdbuserstore-Konfiguration verwendet werden.

Für eine SAP HANA Einrichtung mit mehreren Hosts müssen die Benutzerspeicherschlüssel für alle Hosts konfiguriert werden. SnapCenter versucht mit jedem der angegebenen Schlüssel eine Verbindung zur Datenbank herzustellen und kann somit unabhängig vom Failover eines SAP HANA Service zu einem anderen Host funktionieren.

Anwendungskonfigurationsbeispiele

Im Lab-Setup wird eine gemischte SAP HANA Plug-in-Implementierung verwendet. Das HANA-Plug-in wird für einige HANA-Systeme auf dem SnapCenter-Server installiert und für andere Systeme auf den einzelnen HANA-Datenbankservern implementiert.

SAP HANA System SS1, MDC Einzelmieter, Instanz 00

Das HANA-Plug-in wurde auf dem Datenbank-Host implementiert. Daher muss der Schlüssel auf dem Datenbank-Host mit dem Benutzer ss1adm konfiguriert werden.

```
hana-1:/ # su - ss1adm
ss1adm@hana-1:/usr/sap/SS1/HDB00>
ss1adm@hana-1:/usr/sap/SS1/HDB00>
ss1adm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore set SS1KEY hana-1:30013
SnapCenter password
ss1adm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore list
DATA FILE       : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE        : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.KEY
KEY SS1KEY
  ENV : hana-1:30013
  USER: SnapCenter
KEY SS1SAPDBCTRLSS1
  ENV : hana-1:30015
  USER: SAPDBCTRL
ss1adm@hana-1:/usr/sap/SS1/HDB00>
```

- SAP HANA System MS1, Multihost MDC Einzelmandant, Instanz 00*

Für HANA sind mehrere Hostsysteme ein zentraler Plug-in-Host erforderlich, in unserem Setup haben wir den SnapCenter Server verwendet. Daher muss die Konfiguration des Benutzerspeichers auf dem SnapCenter-Server ausgeführt werden.

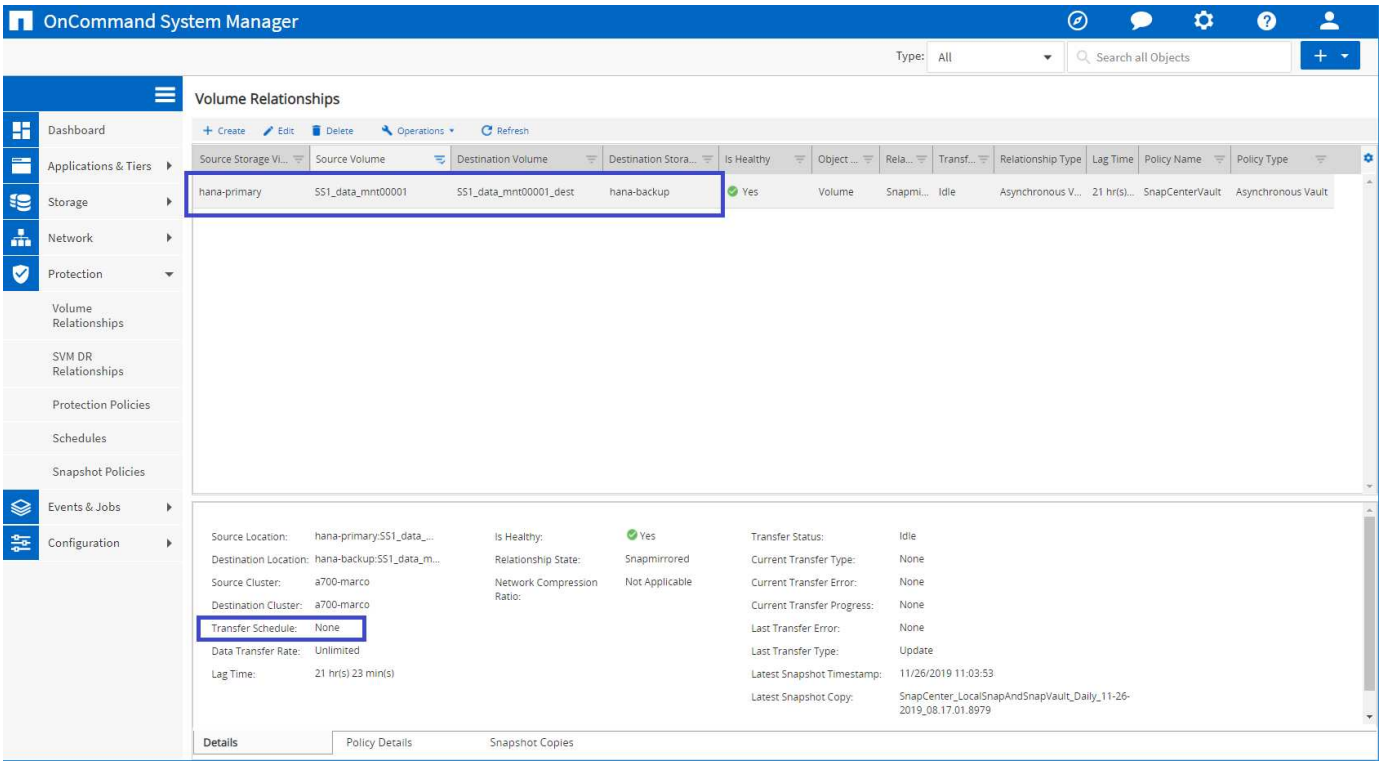
```
hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER
password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE       : C:\ProgramData\.hdb\SNAPCENTER-43\S-1-5-18\SSFS_HDB.DAT
KEY FILE        : C:\ProgramData\.hdb\SNAPCENTER-43\S-1-5-18\SSFS_HDB.KEY
KEY MS1KEYHOST1
  ENV : hana-4:30013
  USER: SNAPCENTER
KEY MS1KEYHOST2
  ENV : hana-5:30013
  USER: SNAPCENTER
KEY MS1KEYHOST3
  ENV : hana-6:30013
  USER: SNAPCENTER
KEY SS2KEY
  ENV : hana-3:30013
  USER: SNAPCENTER
C:\Program Files\sap\hdbclient>
```

Konfiguration der Datensicherung auf externen Backup-Storage

Die Konfiguration der Datensicherungsbeziehung sowie der anfängliche Datentransfer müssen ausgeführt werden, bevor Replizierungs-Updates von SnapCenter gemanagt werden können.

Die folgende Abbildung zeigt die konfigurierte Sicherungsbeziehung für das SAP HANA-System SS1. Mit unserem Beispiel das Quellvolumen `SS1_data_mnt00001` Bei der SVM `hana-primary` Wird auf die SVM repliziert `hana-backup` Und das Ziel-Volume `SS1_data_mnt00001_dest`.

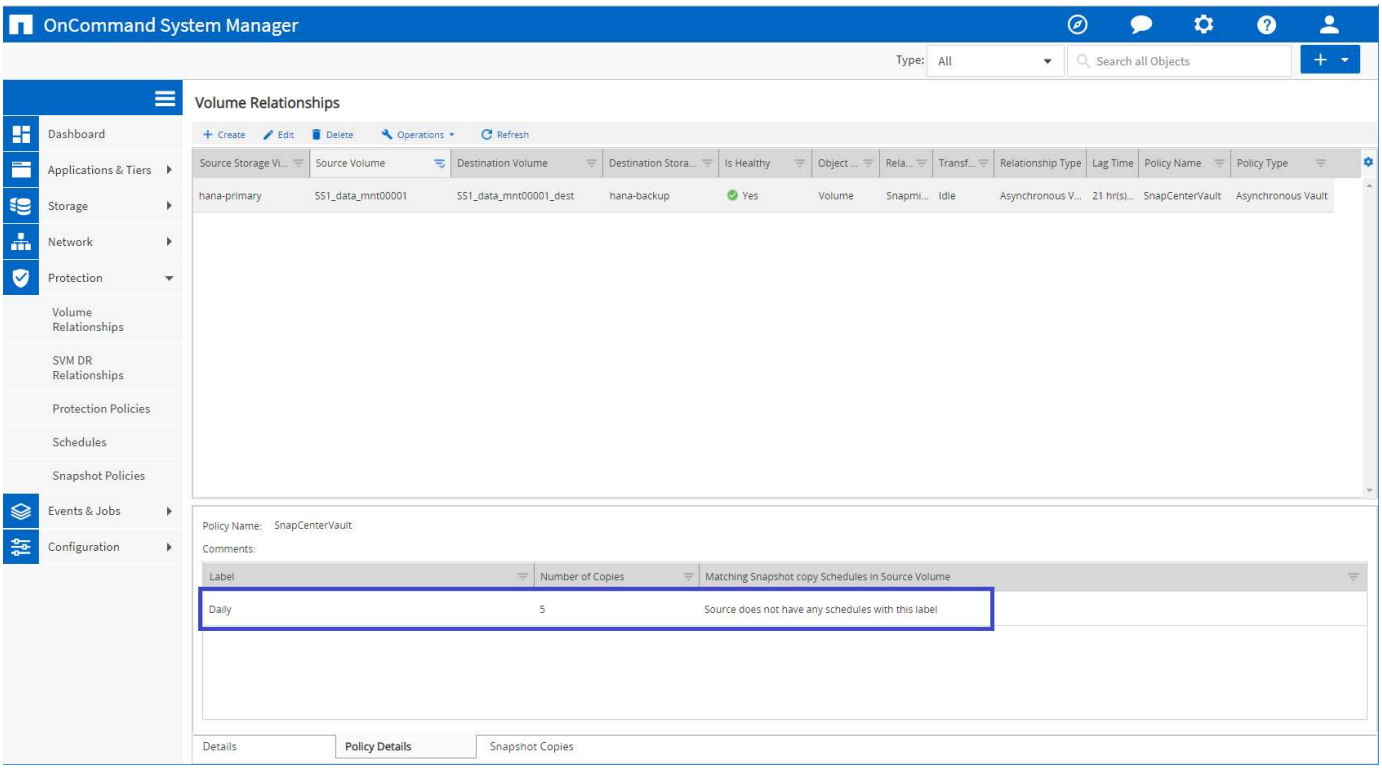
> Der Zeitplan für die Beziehung muss auf „Keine“ gesetzt werden, da SnapCenter das SnapVault Update auslöst.



Die folgende Abbildung zeigt die Sicherungsrichtlinie. Die Sicherungsrichtlinie, die für die Schutzbeziehung verwendet wird, definiert das SnapMirror-Label und die Aufbewahrung von Backups im sekundären Storage. In unserem Beispiel ist das verwendete Etikett `Daily`, Und die Aufbewahrung ist auf 5 eingestellt.

> Das SnapMirror-Label in der erstellten Richtlinie muss mit der in der Konfiguration der SnapCenter-Richtlinie definierten Beschriftung übereinstimmen. Weitere Informationen finden Sie unter „Richtlinie für tägliche Snapshot Backups mit SnapVault Replizierung.“

> Die Aufbewahrung für Backups im externen Backup-Storage wird in der Richtlinie definiert und durch ONTAP gesteuert.



Manuelle Konfiguration der HANA-Ressourcen

In diesem Abschnitt wird die manuelle Konfiguration der SAP HANA-Ressourcen SS2 und MS1 beschrieben.

- SS2 ist ein MDC-Einzelmandant-System mit einem Host
- MS1 ist ein MDC-Einzelmandant-System mit mehreren Hosts.

a. Wählen Sie auf der Registerkarte Ressourcen SAP HANA aus, und klicken Sie auf Add SAP HANA Database.

b. Geben Sie die Informationen zum Konfigurieren der SAP HANA-Datenbank ein, und klicken Sie auf Weiter.

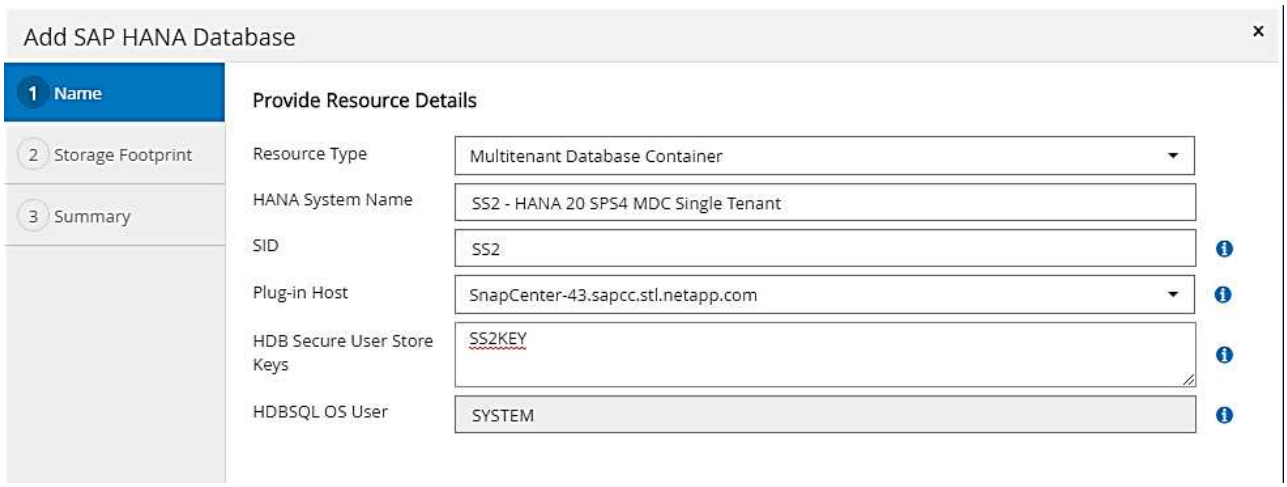
   Wählen Sie in unserem Beispiel den Ressourcentyp Multitenant Database Container aus.

   > Für ein HANA-System mit einem einzelnen Container muss der Ressourcentyp Single Container ausgewählt werden. Alle anderen Konfigurationsschritte sind identisch.

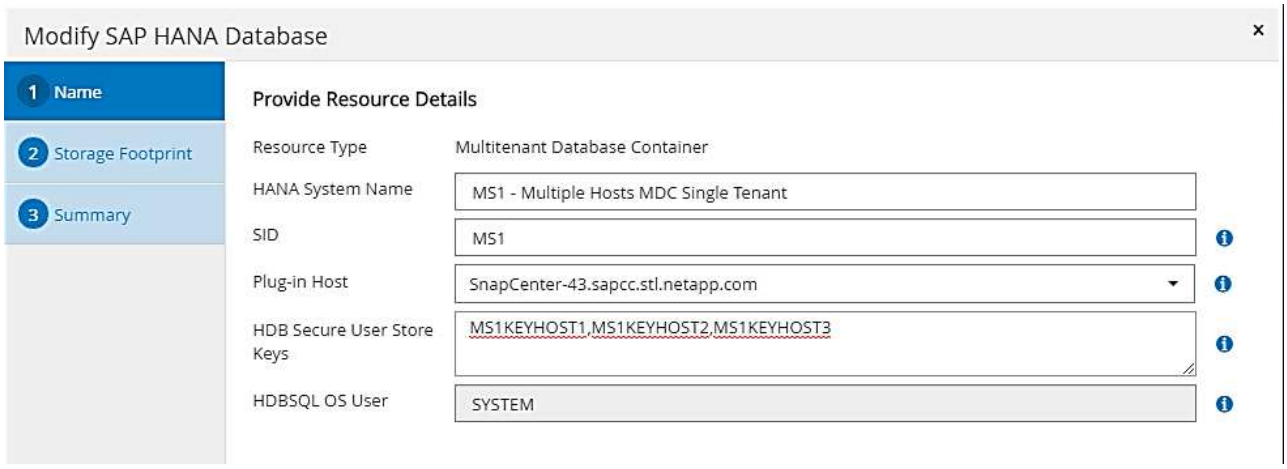
   Für unser SAP HANA System ist SID SS2.

   Der HANA-Plug-in-Host in unserem Beispiel ist der SnapCenter-Server.

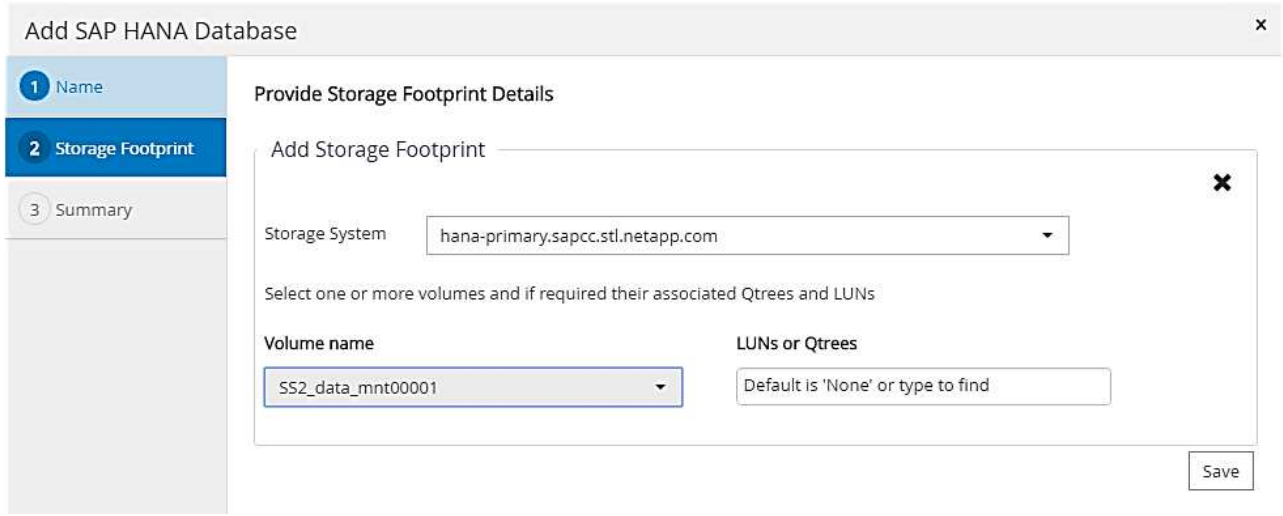
   Der hdbuserstore-Schlüssel muss mit dem Schlüssel übereinstimmen, der für die HANA-Datenbank SS2 konfiguriert wurde. In unserem Beispiel ist es SS2KEY.



Bei einem SAP HANA-System mit mehreren Hosts müssen die hdbuserstore-Schlüssel für alle Hosts enthalten sein, wie in der folgenden Abbildung dargestellt. SnapCenter versucht, eine Verbindung mit der ersten Taste in der Liste herzustellen, und setzt den anderen Fall fort, falls der erste Schlüssel nicht funktioniert. Dies ist zur Unterstützung von HANA Failover in einem System mit mehreren Hosts mit Worker und Standby-Hosts erforderlich.

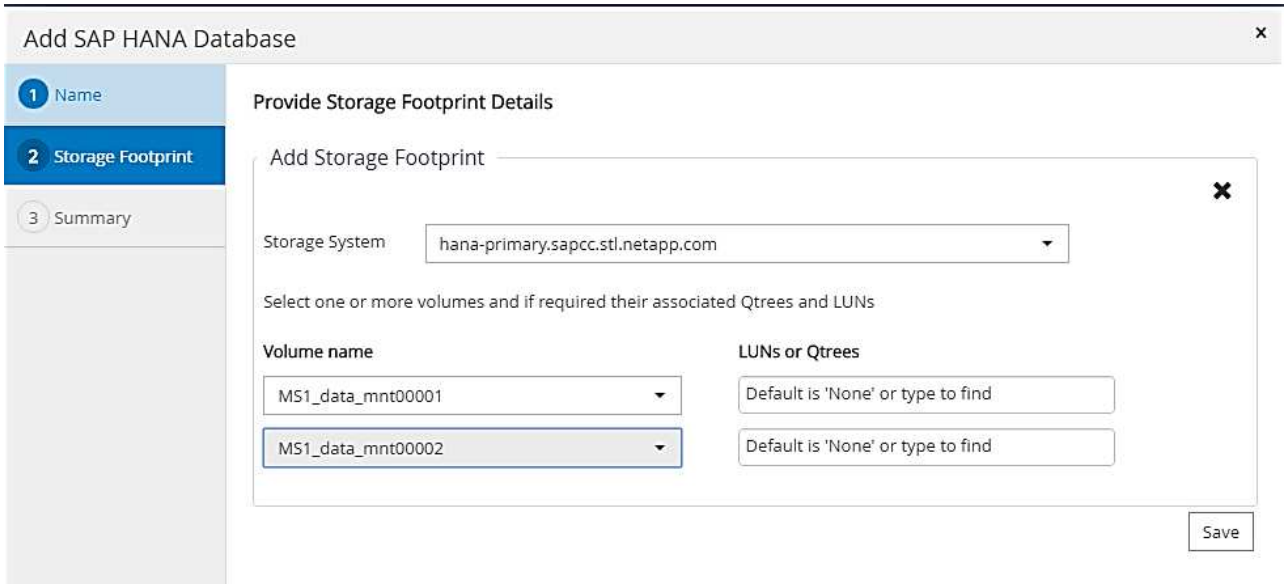


c. Wählen Sie die erforderlichen Daten für das Storage-System (SVM) und den Volume-Namen aus.



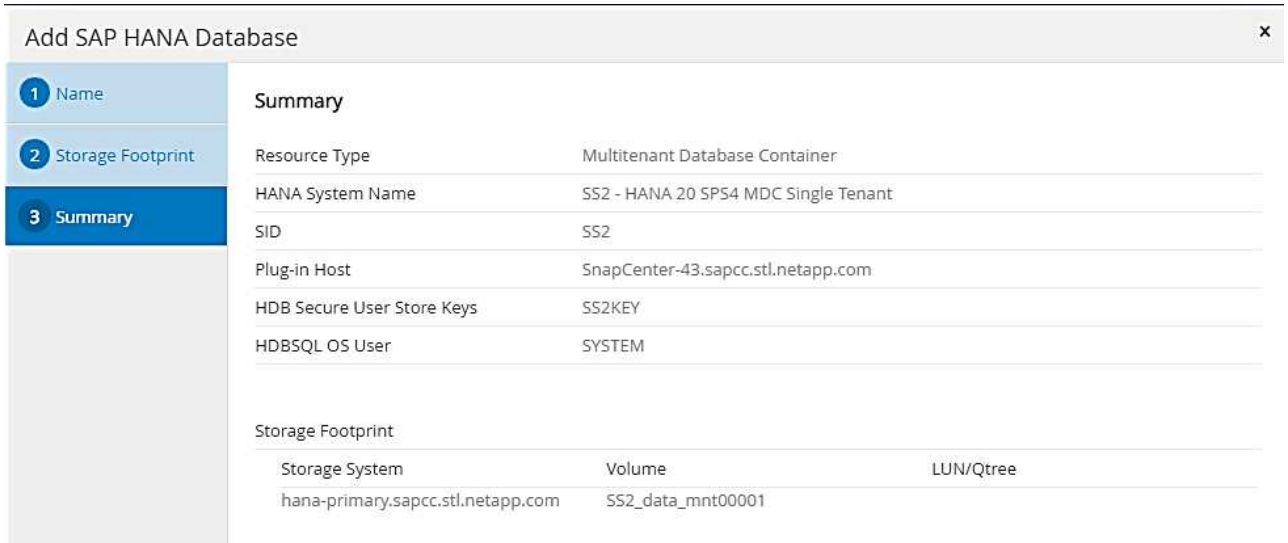
Für eine Fibre-Channel-SAN-Konfiguration muss auch die LUN ausgewählt werden.

Bei einem SAP HANA-System mit mehreren Hosts müssen alle Datenvolumen des SAP HANA Systems ausgewählt werden, wie in der folgenden Abbildung dargestellt.



Der Übersichtsbildschirm der Ressourcenkonfiguration wird angezeigt.

a. Klicken Sie auf Fertig stellen, um die SAP HANA-Datenbank hinzuzufügen.



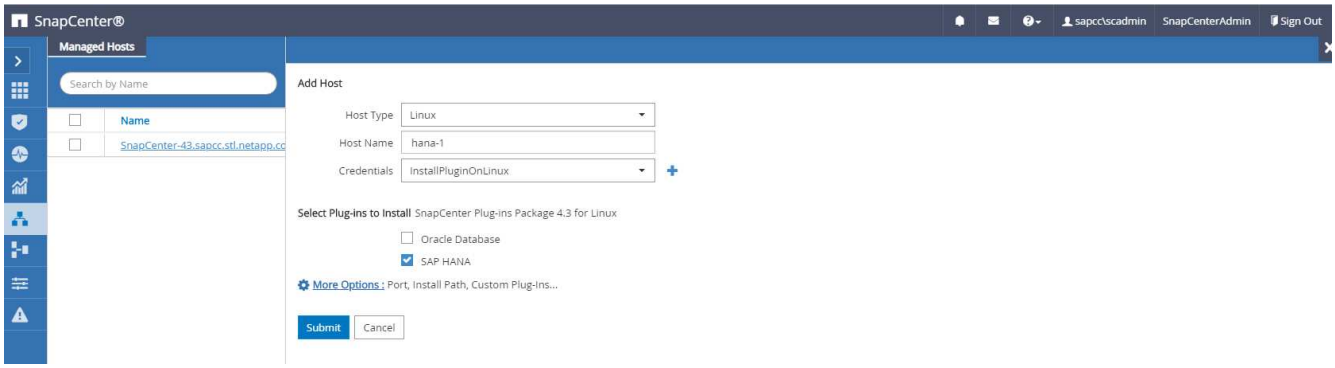
b. Wenn die Ressourcenkonfiguration abgeschlossen ist, führen Sie die Konfiguration des Ressourcenschutzes durch, wie im Abschnitt „ beschriebenKonfiguration für Ressourcenschutz.“

Automatische Erkennung von HANA-Datenbanken

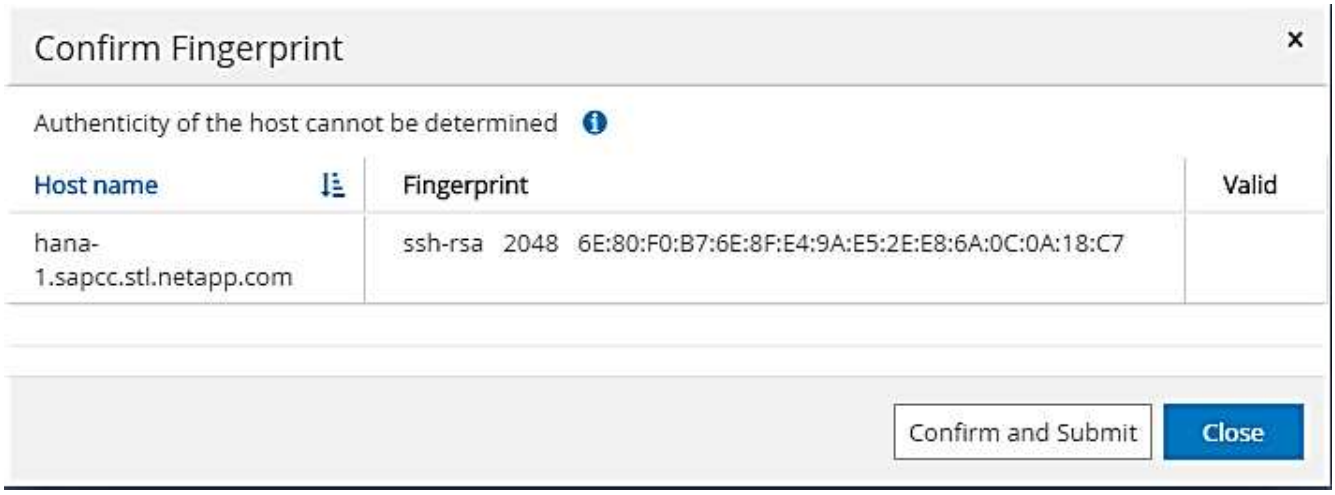
In diesem Abschnitt wird die automatische Erkennung der SAP HANA-Ressource SS1 (Single-Host-MDC-Einzelmandant-System mit NFS) beschrieben. Alle beschriebenen Schritte sind identisch mit einem HANA-Einzelcontainer, HANA-MDC-Systemen mehrerer Mandanten und einem HANA-System, das Fibre Channel-SAN verwendet.

Für das SAP HANA Plug-in ist Java 64-Bit Version 1.8 erforderlich. Java muss auf dem Host installiert sein, bevor das SAP HANA Plug-in bereitgestellt wird.

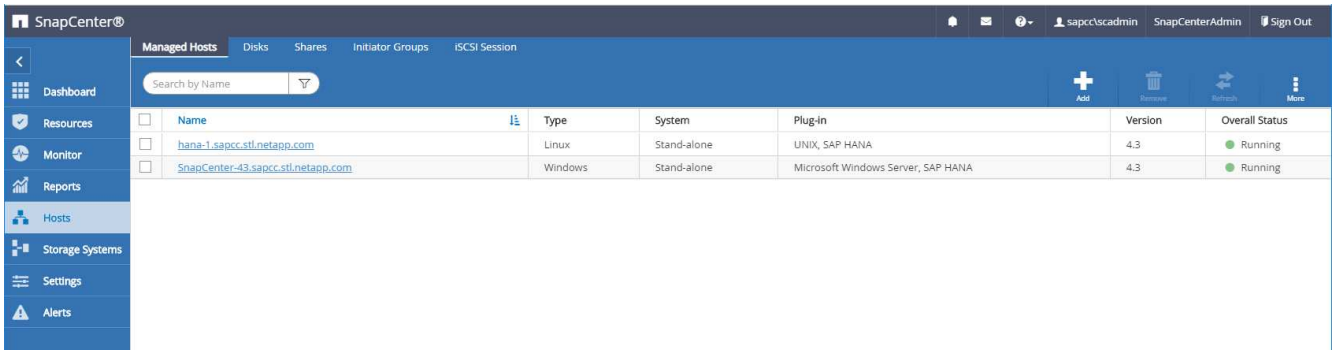
1. Klicken Sie auf der Registerkarte Host auf Hinzufügen.
2. Geben Sie Host-Informationen an, und wählen Sie das zu installierende SAP HANA-Plug-in aus. Klicken Sie Auf Senden.



3. Bestätigen Sie den Fingerabdruck.



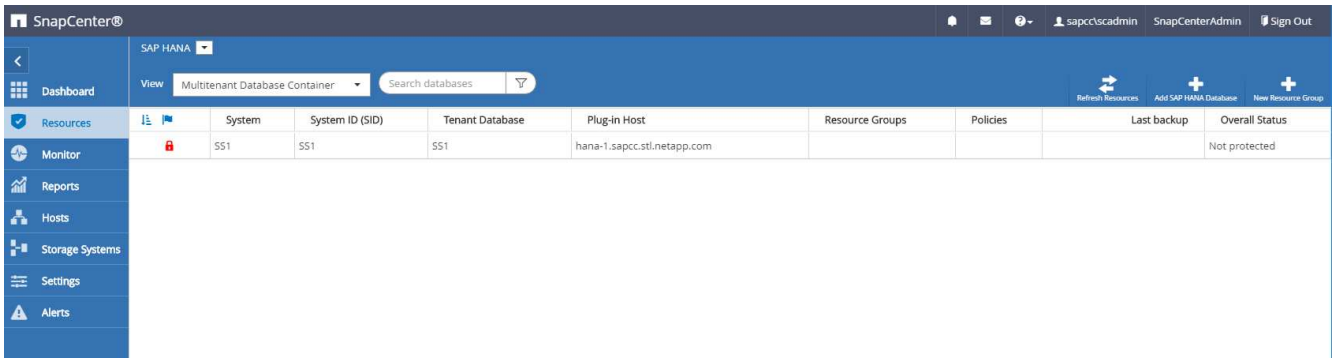
Die Installation des HANA-Plug-ins und des Linux-Plug-ins wird automatisch gestartet. Nach Abschluss der Installation wird in der Statusspalte des Hosts die Ausführung angezeigt. Der Bildschirm zeigt auch, dass das Linux-Plug-in zusammen mit dem HANA-Plug-in installiert wird.



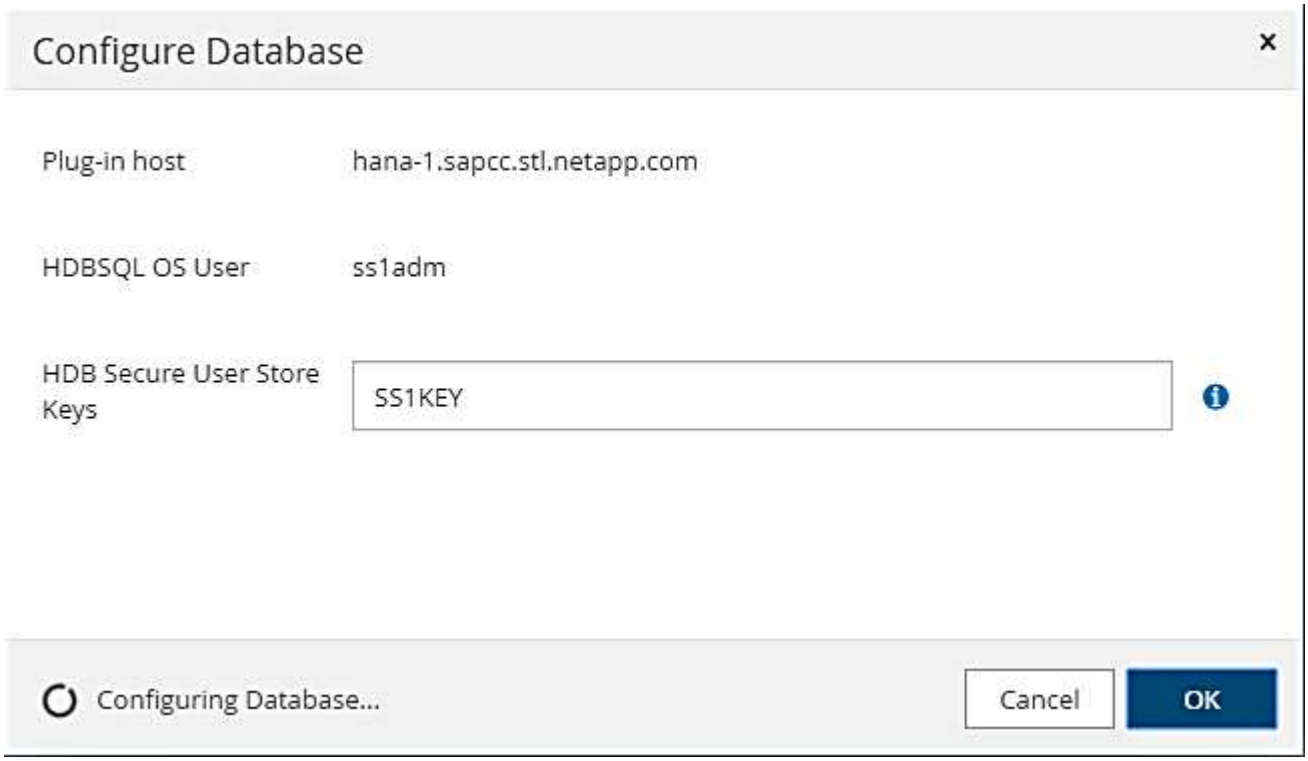
Nach der Plug-in-Installation startet der automatische Erkennungsvorgang der HANA-Ressource automatisch. Im Bildschirm Ressourcen wird eine neue Ressource erstellt, die mit dem roten Vorhängeschloss-Symbol als gesperrt markiert ist.

4. Wählen Sie und klicken Sie auf die Ressource, um mit der Konfiguration fortzufahren.

> Sie können den automatischen Erkennungsvorgang auch manuell im Bildschirm Ressourcen auslösen, indem Sie auf Ressourcen aktualisieren klicken.

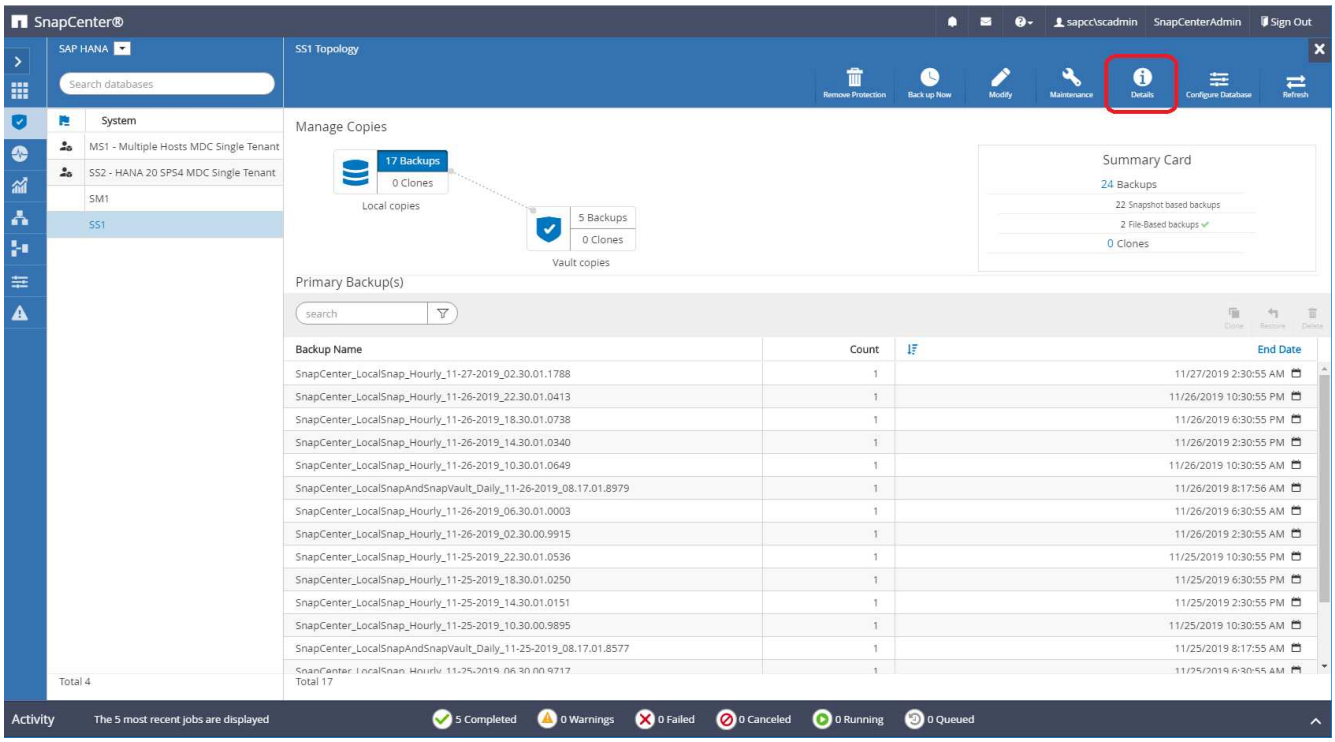


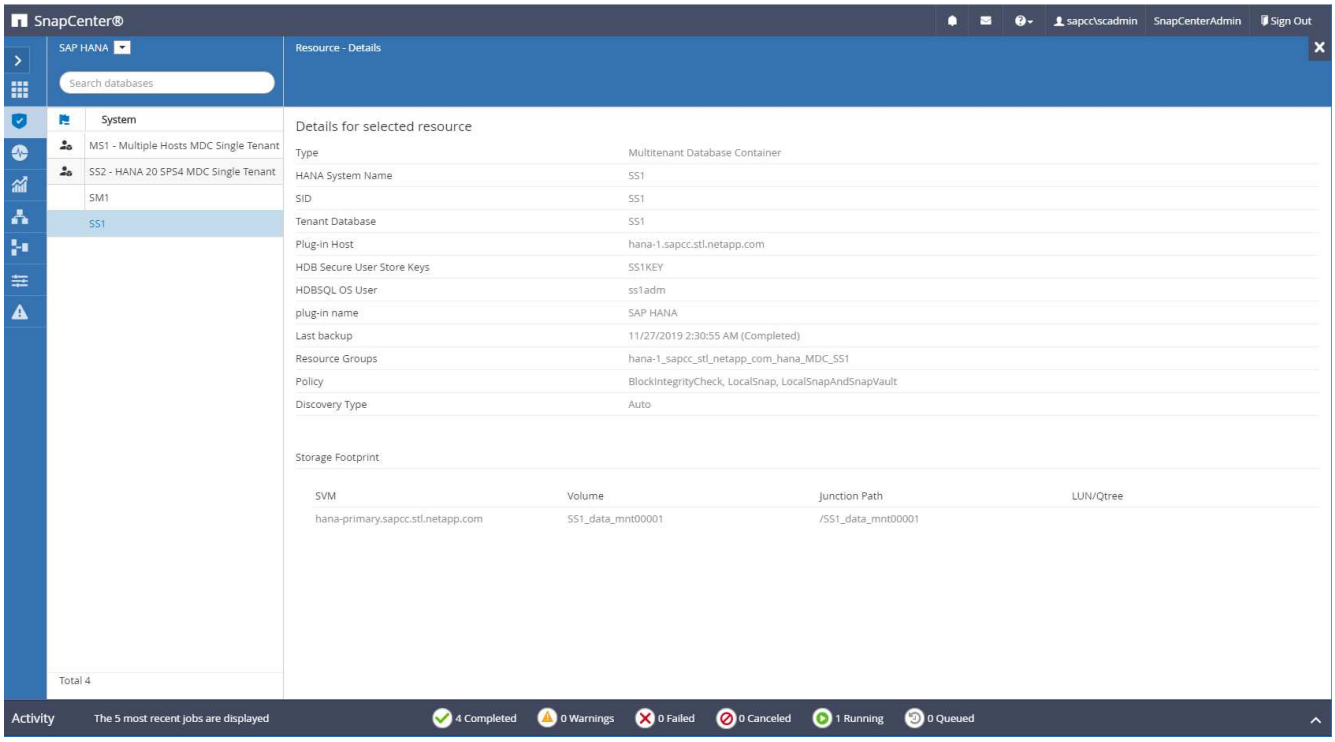
5. Geben Sie den UserStore-Schlüssel für die HANA-Datenbank an.



Der zweite Ebene-Prozess der automatischen Bestandsaufnahme beginnt, bei dem Mandantendaten und Storage-Platzbedarf erfasst werden.

6. Klicken Sie auf Details, um die Konfigurationsinformationen der HANA-Ressource in der Ansicht der Ressourcentopologie anzuzeigen.





Wenn die Ressourcenkonfiguration abgeschlossen ist, muss die Konfiguration des Ressourcenschutzes wie im folgenden Abschnitt beschrieben ausgeführt werden.

Konfiguration für Ressourcenschutz

In diesem Abschnitt wird die Konfiguration für den Ressourcenschutz beschrieben. Die Ressourcenschutzkonfiguration ist dieselbe, unabhängig davon, ob die Ressource automatisch erkannt oder manuell konfiguriert wurde. Und ist für alle HANA-Architekturen, einzelne oder mehrere Hosts, einzelnen Container oder MDC-Systeme identisch.

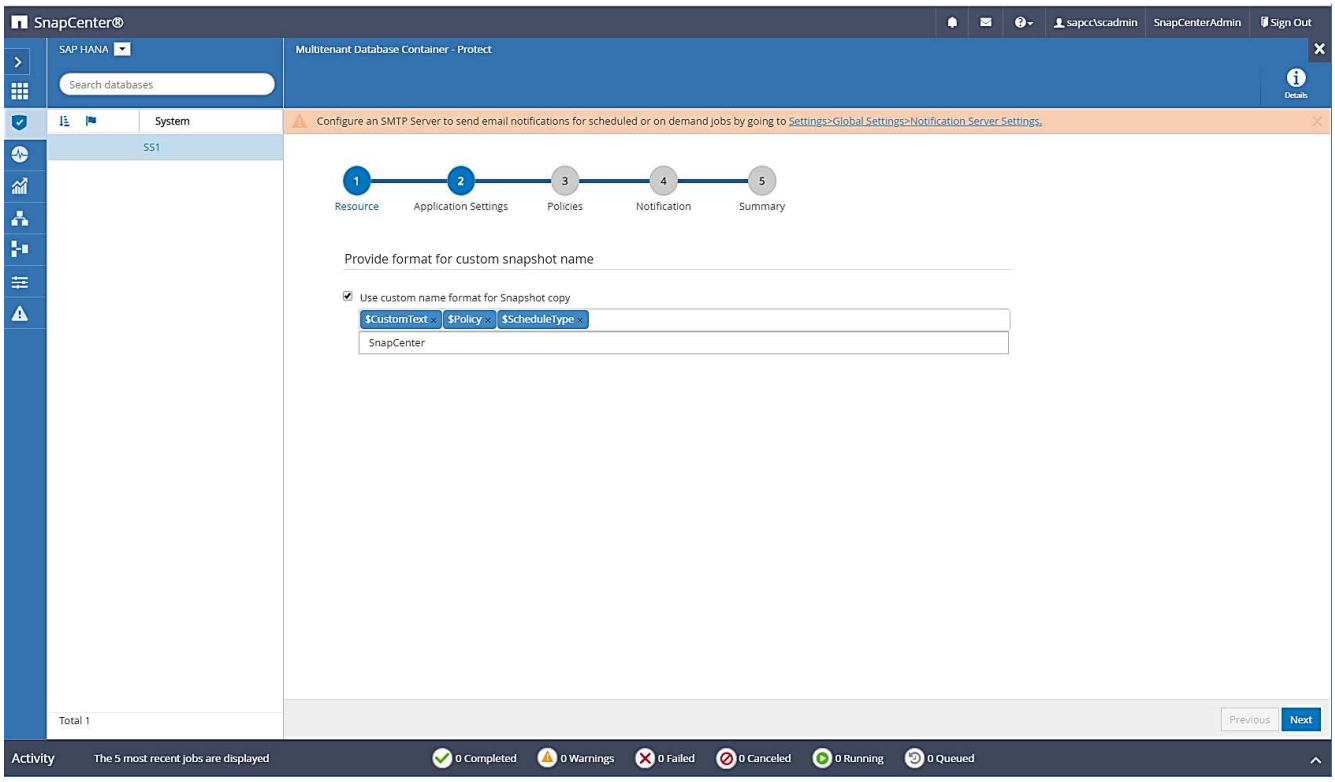
1. Doppelklicken Sie auf der Registerkarte Ressourcen auf die Ressource.
2. Konfigurieren Sie ein benutzerdefiniertes Namensformat für die Snapshot Kopie.

> NetApp empfiehlt den Einsatz einer benutzerdefinierten Snapshot Kopie, um schnell ermitteln zu können, mit welcher Richtlinie und welche Zeitplantypen Backups erstellt wurden. Durch Hinzufügen des Zeitplantyps zum Namen der Snapshot Kopie können Sie zwischen geplanten und On-Demand-Backups unterscheiden. Der `schedule name` String für On-Demand-Backups ist leer, während geplante Backups den String enthalten `Hourly`, `Daily`, `or Weekly`.

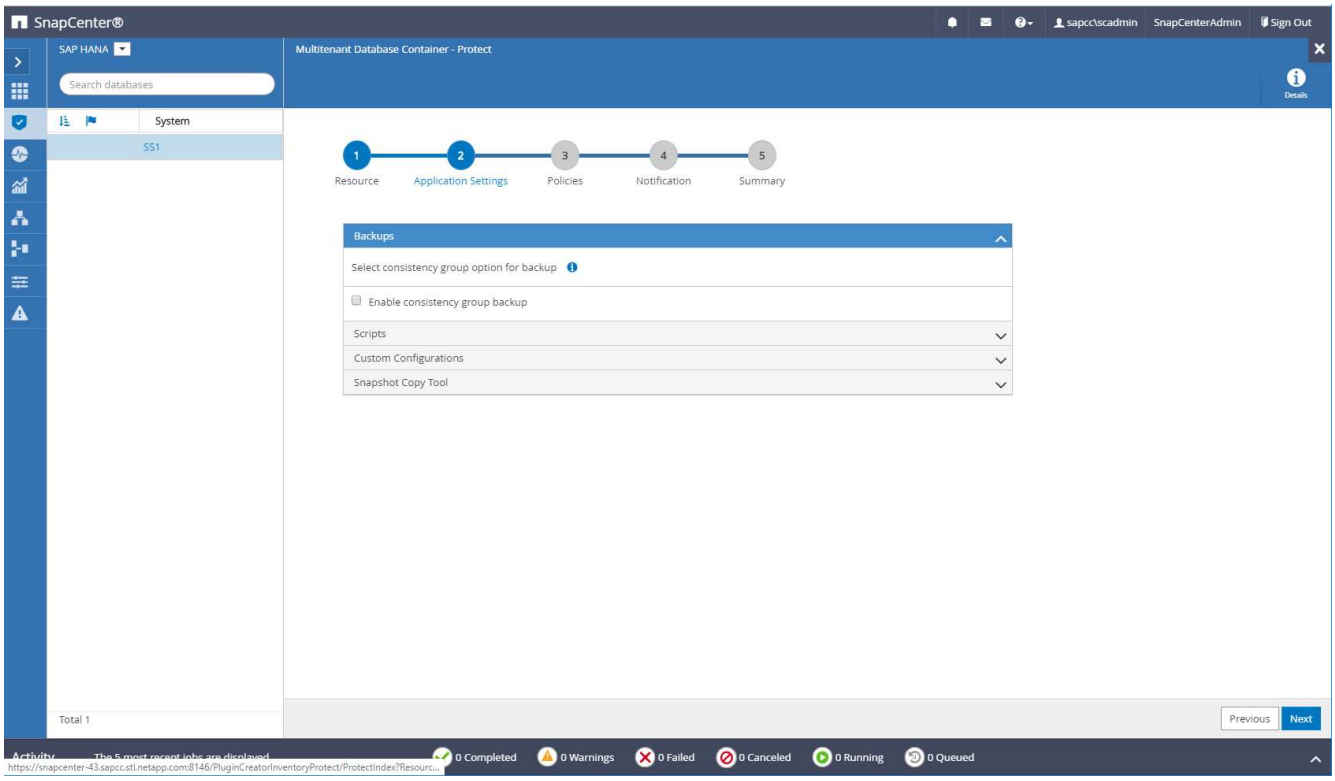
In der Konfiguration der folgenden Abbildung haben die Namen von Backup- und Snapshot-Kopien das folgende Format:

- Stündliches Backup geplant: `SnapCenter_LocalSnap_Hourly_<time_stamp>`
- Täglich geplantes Backup: `SnapCenter_LocalSnapAndSnapVault_Daily_<time_stamp>`
- Stündliches On-Demand-Backup: `SnapCenter_LocalSnap_<time_stamp>`
- Tägliches On-Demand Backup: `SnapCenter_LocalSnapAndSnapVault_<time_stamp>`

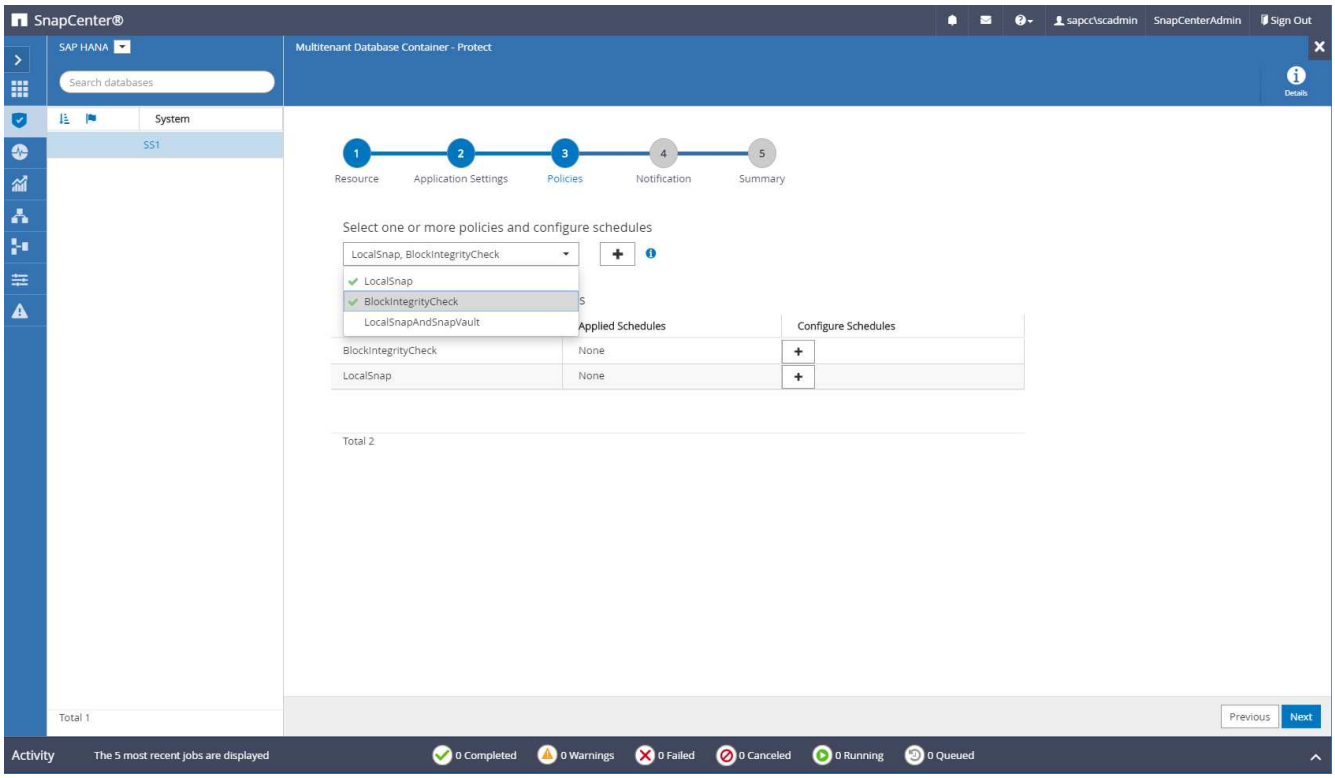
> Obwohl eine Aufbewahrung für On-Demand-Backups in der Richtlinienkonfiguration definiert wird, wird die allgemeine Ordnung und Sauberkeit nur dann ausgeführt, wenn ein weiteres On-Demand-Backup ausgeführt wird. Daher müssen On-Demand-Backups in der Regel manuell in SnapCenter gelöscht werden, um sicherzustellen, dass diese Backups auch im SAP HANA Backup-Katalog gelöscht werden und dass die allgemeine Ordnung der Protokollsicherung nicht auf einem alten On-Demand-Backup basiert.



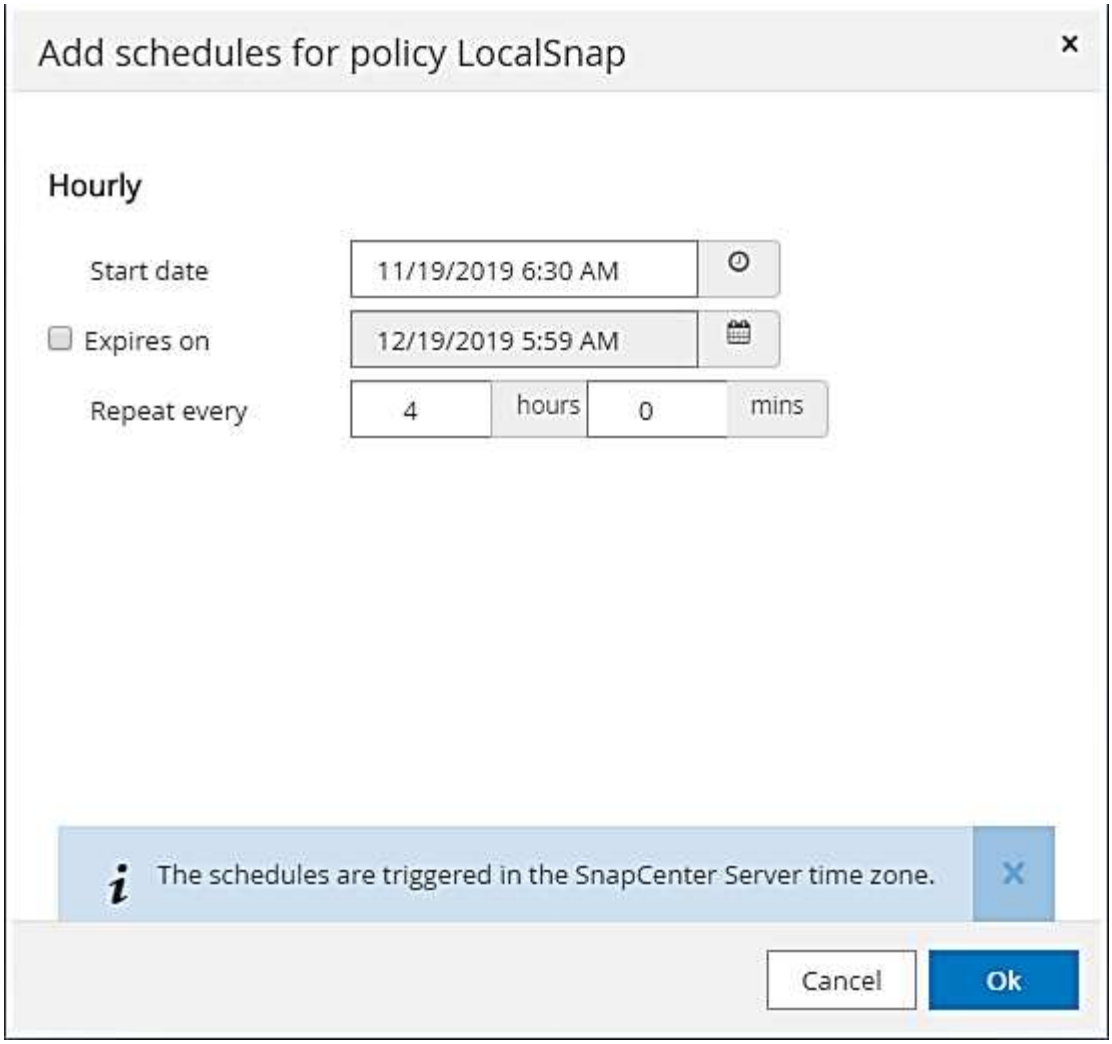
3. Auf der Seite „Anwendungseinstellungen“ müssen keine spezifischen Einstellungen vorgenommen werden. Klicken Sie Auf Weiter.



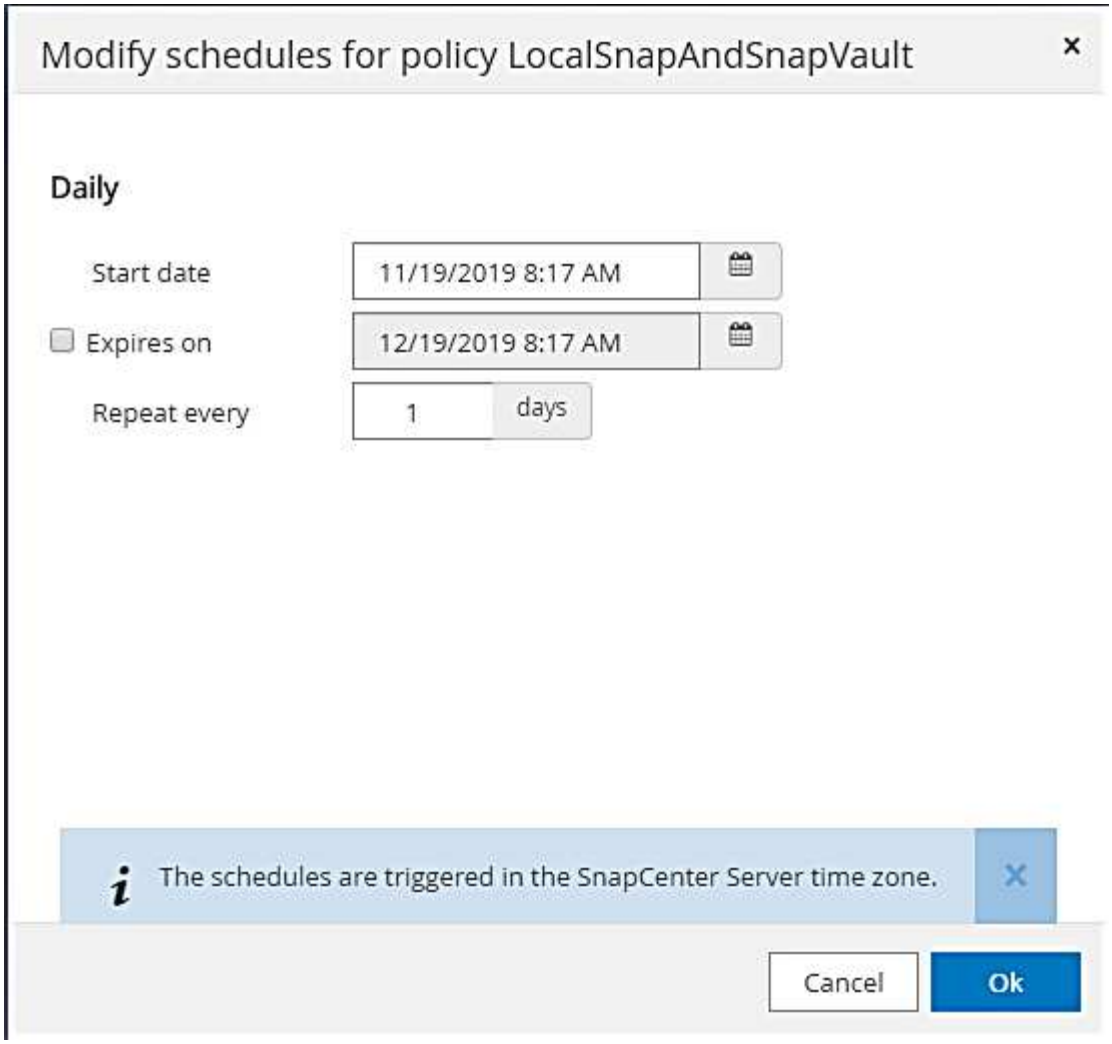
4. Wählen Sie die Richtlinien aus, die der Ressource hinzugefügt werden sollen.



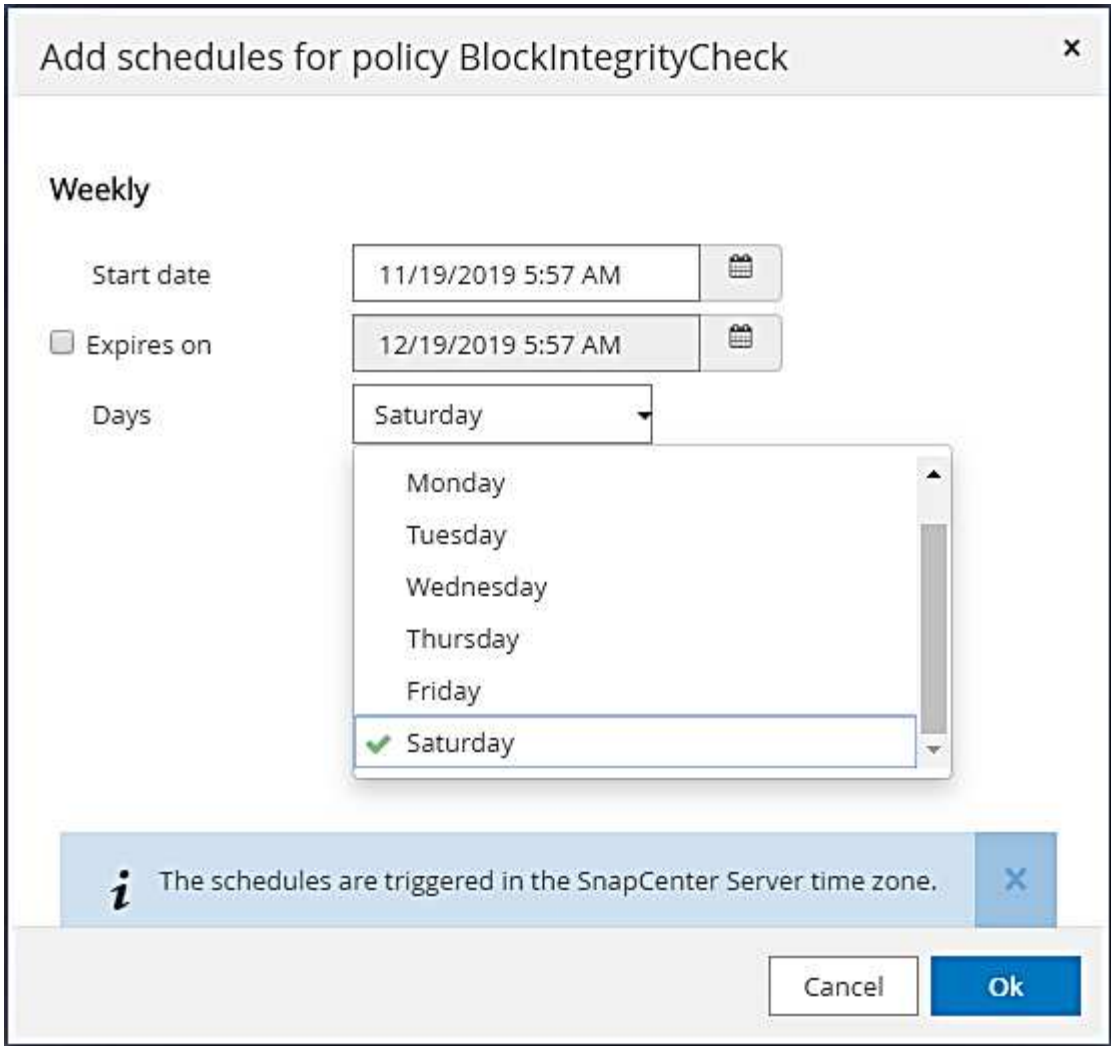
5. Legen Sie den Zeitplan für die LocalSnap-Richtlinie fest (in diesem Beispiel alle vier Stunden).



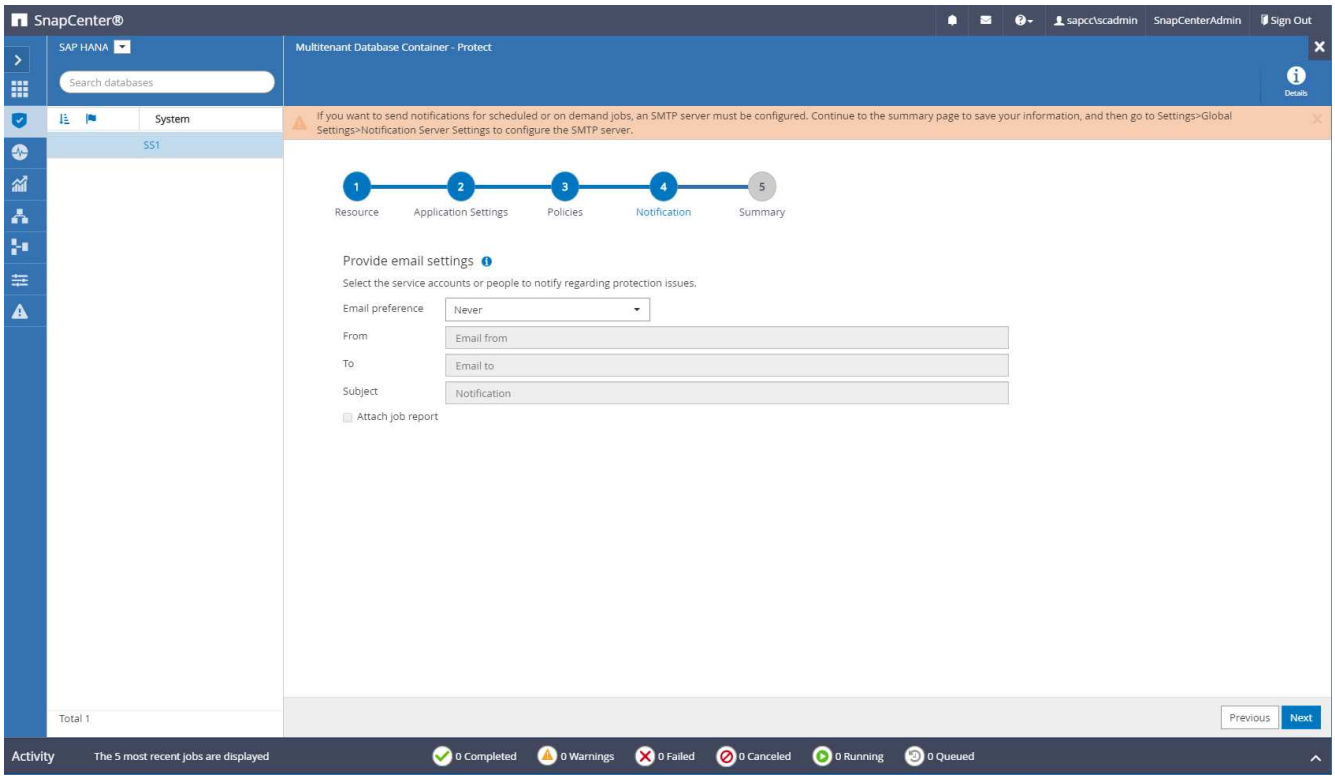
6. Legen Sie den Zeitplan für die LocalSnapAndSnapVault-Richtlinie fest (in diesem Beispiel einmal pro Tag).



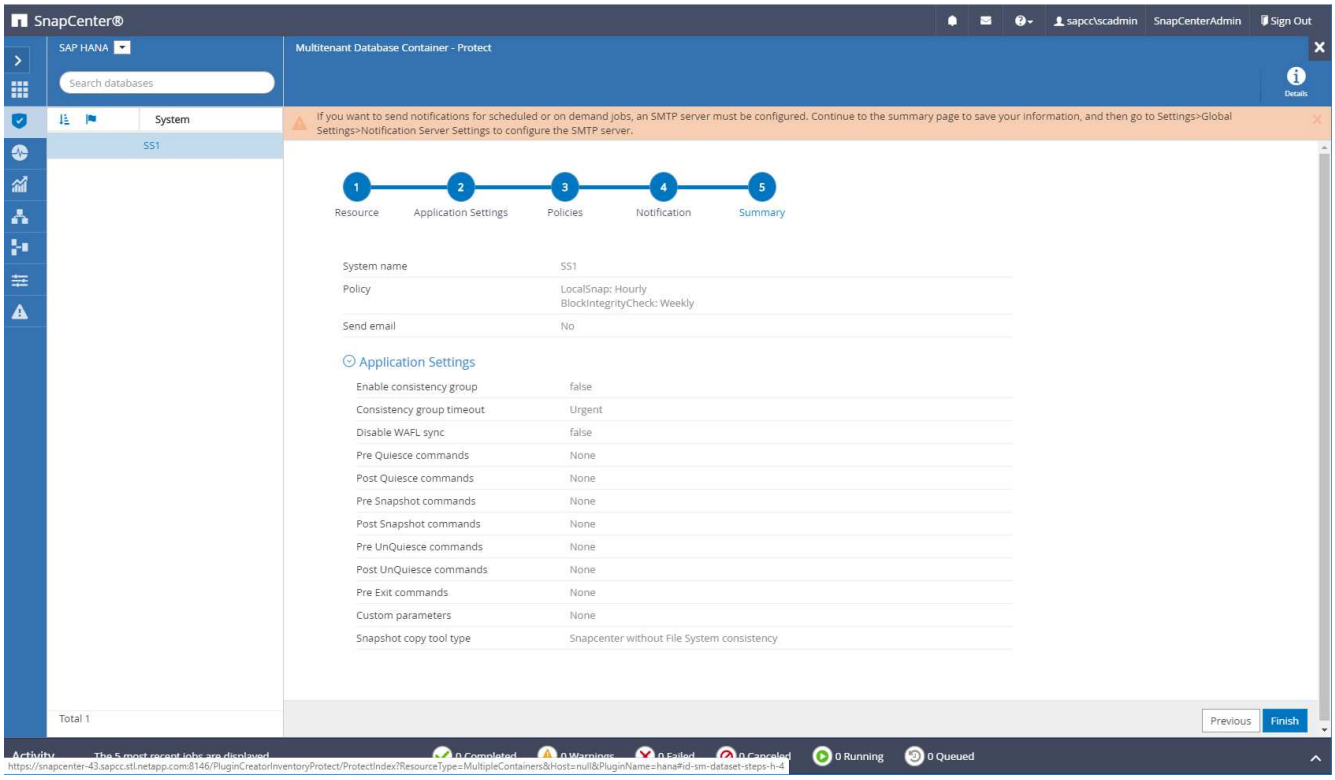
7. Legen Sie den Zeitplan für die Richtlinie zur Integritätsprüfung der Blöcke fest (in diesem Beispiel einmal pro Woche).



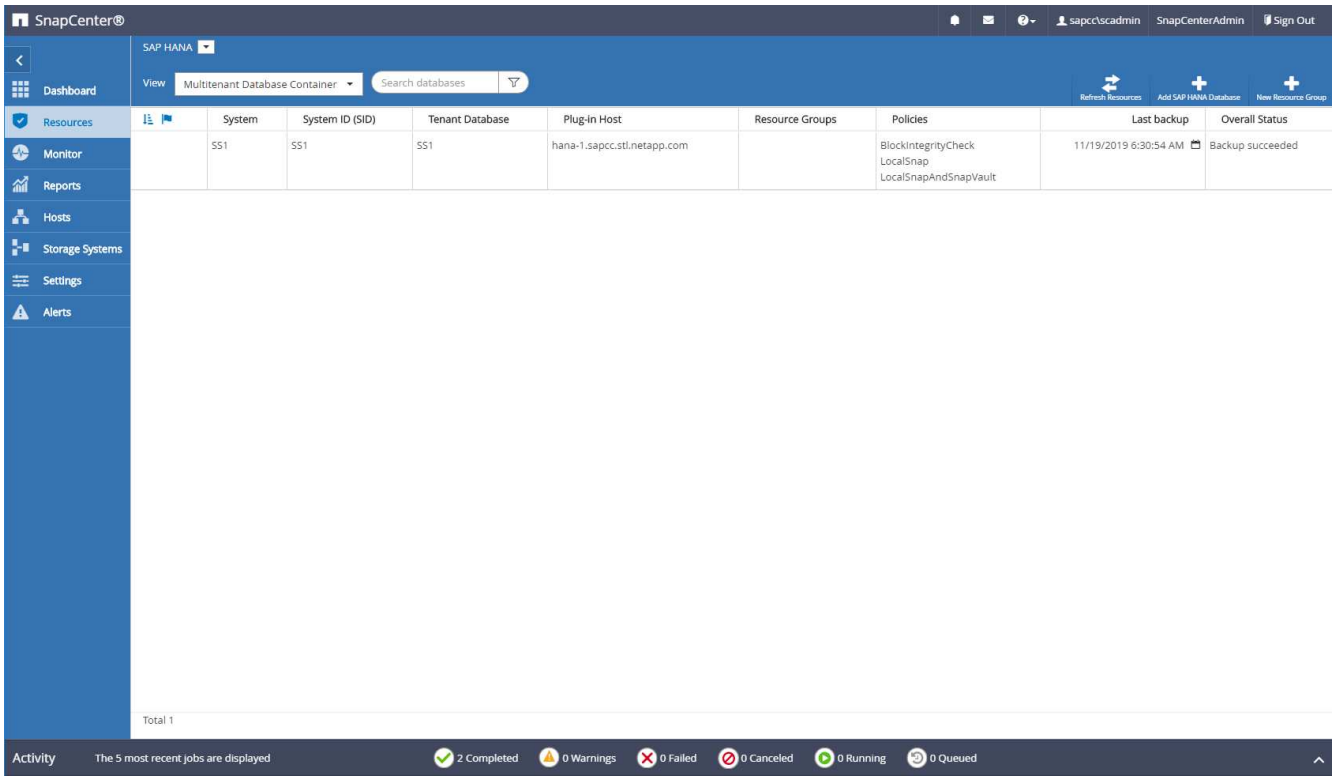
8. Geben Sie Informationen zur E-Mail-Benachrichtigung an.



9. Klicken Sie auf der Seite Zusammenfassung auf Fertig stellen.



10. On-Demand-Backups können jetzt auf der Topologieseite erstellt werden. Die geplanten Backups werden basierend auf den Konfigurationseinstellungen ausgeführt.



Zusätzliche Konfigurationsschritte für Fibre Channel SAN-Umgebungen

Je nach HANA-Version und HANA-Plug-in-Implementierung sind für Umgebungen, in denen die SAP HANA-Systeme Fibre Channel und das XFS-Dateisystem nutzen, zusätzliche Konfigurationsschritte erforderlich.

> Diese zusätzlichen Konfigurationsschritte sind nur für HANA-Ressourcen erforderlich, die in SnapCenter manuell konfiguriert werden. Außerdem wird es nur für HANA 1.0 und HANA 2.0-Versionen bis SPS2 benötigt.

Wenn der Speicherpunkt für ein HANA Backup von SnapCenter in SAP HANA ausgelöst wird, schreibt SAP HANA als letzter Schritt Snapshot-ID-Dateien für jeden Mandanten und Datenbankservice (z. B. `/hana/data/SID/mnt00001/hdb00001/snapshot_databackup_0_1`). Diese Dateien sind Teil des Daten-Volumes im Storage und sind daher Teil der Storage-Snapshot-Kopie. Diese Datei ist bei der Durchführung einer Recovery in einer Situation, in der das Backup wiederhergestellt wird, obligatorisch. Durch Metadaten-Caching mit dem XFS-Dateisystem auf dem Linux-Host wird die Datei auf der Speicherebene nicht sofort sichtbar. Die standardmäßige XFS-Konfiguration für das Metadaten-Caching beträgt 30 Sekunden.

> Mit HANA 2.0 SPS3 änderte SAP den Schreibvorgang dieser Snapshot ID-Dateien in synchron, sodass es kein Problem ist, Metadaten-Caching zu verwenden.

> Wird bei SnapCenter 4.3 das HANA Plug-in auf dem Datenbank-Host bereitgestellt, führt das Linux Plug-in vor dem Auslösen des Storage-Snapshots einen Dateisystemputz-Vorgang auf dem Host durch. In diesem Fall stellt das Metadaten-Caching keine Probleme dar.

In SnapCenter müssen Sie ein konfigurieren `postquiesce` Befehl, der wartet, bis der XFS-Metadatencache auf die Festplattenebene gespeichert wird.

Die tatsächliche Konfiguration des Metadaten-Caching kann mit folgendem Befehl überprüft werden:

```
stlrx300s8-2:/ # sysctl -A | grep xfssyncd_centisecs
fs.xfs.xfssyncd_centisecs = 3000
```

NetApp empfiehlt, die Wartezeit auf eine doppelt so hohe Wartezeit von zu verwenden `fs.xfs.xfssyncd_centisecs` Parameter. Da der Standardwert 30 Sekunden beträgt, setzen Sie den Befehl „Sleep“ auf 60 Sekunden.

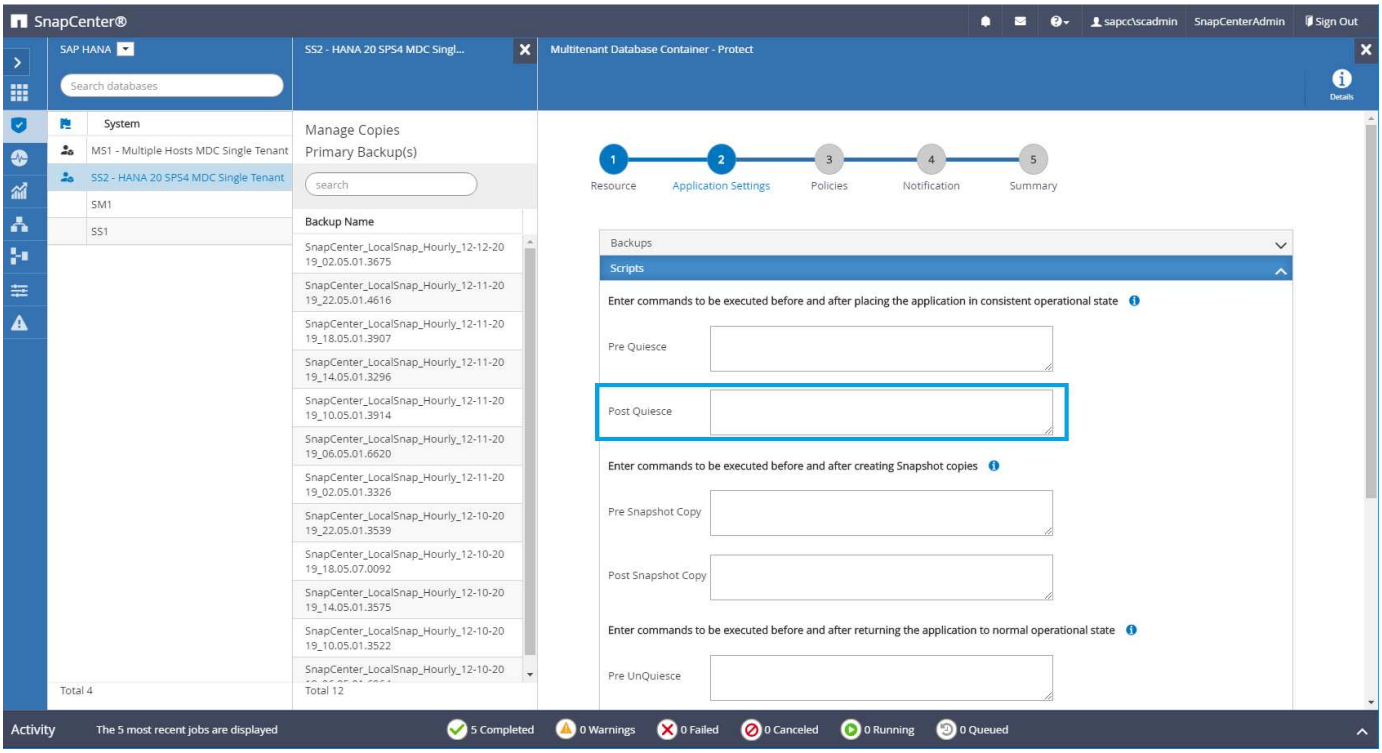
Wird der SnapCenter-Server als zentraler HANA-Plug-in-Host genutzt, kann eine Batch-Datei verwendet werden. Die Batch-Datei muss folgenden Inhalt haben:

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

Die Batch-Datei kann z.B. als gespeichert werden `C:\Program Files\NetApp\Wait60Sec.bat`. In der Ressourcenschutzkonfiguration muss die Batch-Datei als Post Quiesce-Befehl hinzugefügt werden.

Wenn ein separater Linux-Host als zentraler HANA-Plug-in-Host verwendet wird, müssen Sie den Befehl konfigurieren `/bin/sleep 60` Als Post-Quiesce-Befehl in der SnapCenter-UI.

Die folgende Abbildung zeigt den Befehl Post Quiesce im Konfigurationsbildschirm für Ressourcenschutz.



Ressourcenspezifische SnapCenter Konfiguration für Backups außerhalb von Datenvolumen

Das Backup von nicht-Daten-Volumes ist ein integrierter Teil des SAP HANA Plug-ins. Der Schutz des Datenbankdatenvolumens reicht aus, um die SAP HANA Datenbank zu

einem bestimmten Zeitpunkt wiederherzustellen, vorausgesetzt, die Ressourcen zur Datenbankinstallation und die erforderlichen Protokolle sind weiterhin verfügbar.

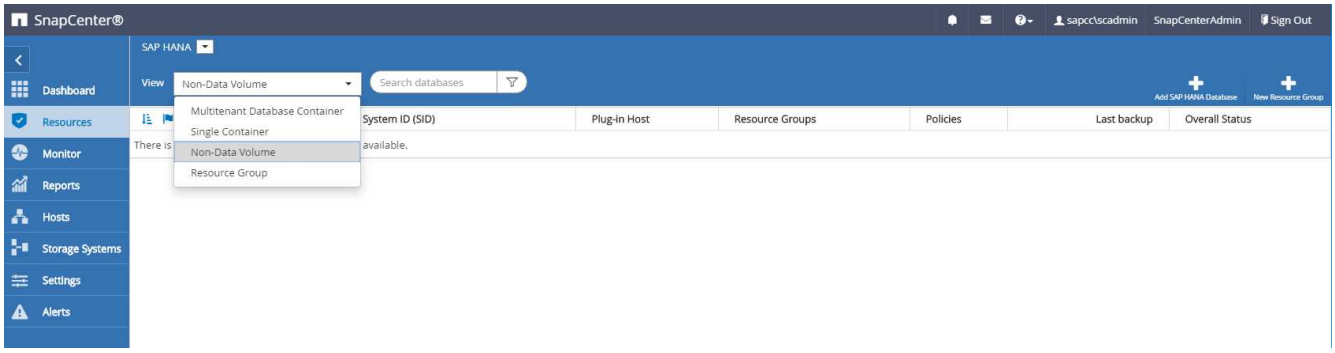
Um das Recovery von Situationen durchzuführen, in denen andere nicht-Datendateien wiederhergestellt werden müssen, empfiehlt NetApp, eine zusätzliche Backup-Strategie für nicht-Daten-Volumes zu entwickeln, um das SAP HANA Datenbank-Backup zu erweitern. Je nach Ihren spezifischen Anforderungen kann sich das Backup von nicht-Daten-Volumes in den Einstellungen für die Planungsfrequenz und -Aufbewahrung unterscheiden, und Sie sollten bedenken, wie oft nicht-Datendateien geändert werden. Zum Beispiel das HANA Volume `/hana/shared` Enthält ausführbare Dateien, aber auch SAP HANA Trace-Dateien. Zwar ändern sich ausführbare Dateien nur beim Upgrade der SAP HANA Datenbank, doch benötigen die SAP HANA Trace-Dateien möglicherweise eine höhere Backup-Häufigkeit, um Problemsituationen mit SAP HANA zu analysieren.

Dank des nicht-Daten-Volume-Backups von SnapCenter können Snapshot-Kopien aller relevanten Volumes in wenigen Sekunden mit derselben Speichereffizienz erstellt werden wie bei SAP HANA-Datenbank-Backups. Der Unterschied liegt darin, dass keine SQL Kommunikation mit der SAP HANA Datenbank erforderlich ist.

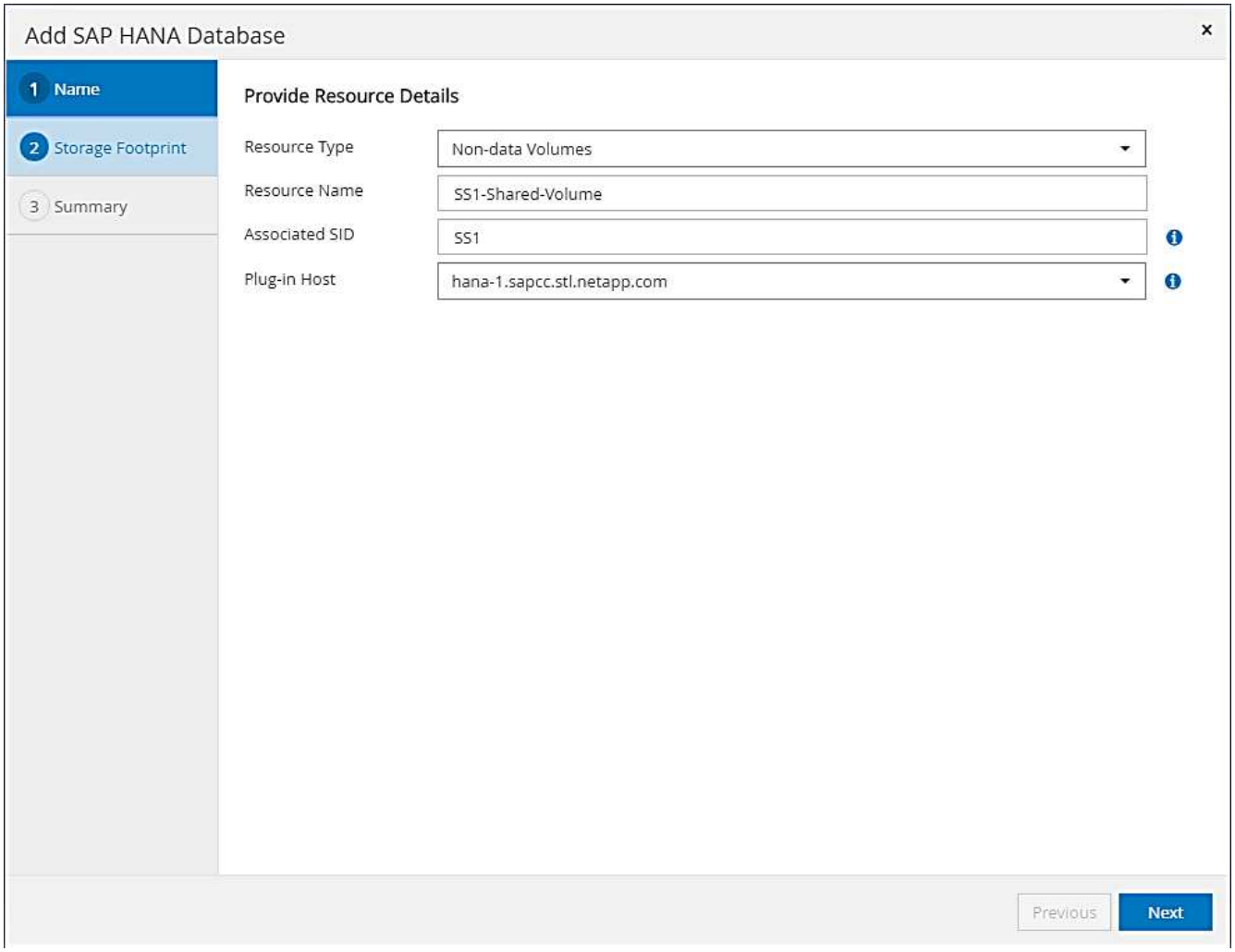
Konfiguration von Ressourcen, die nicht vom Datenvolumen stammen

In diesem Beispiel wollen wir die nicht-Daten-Volumes der SAP HANA Datenbank SS1 schützen.

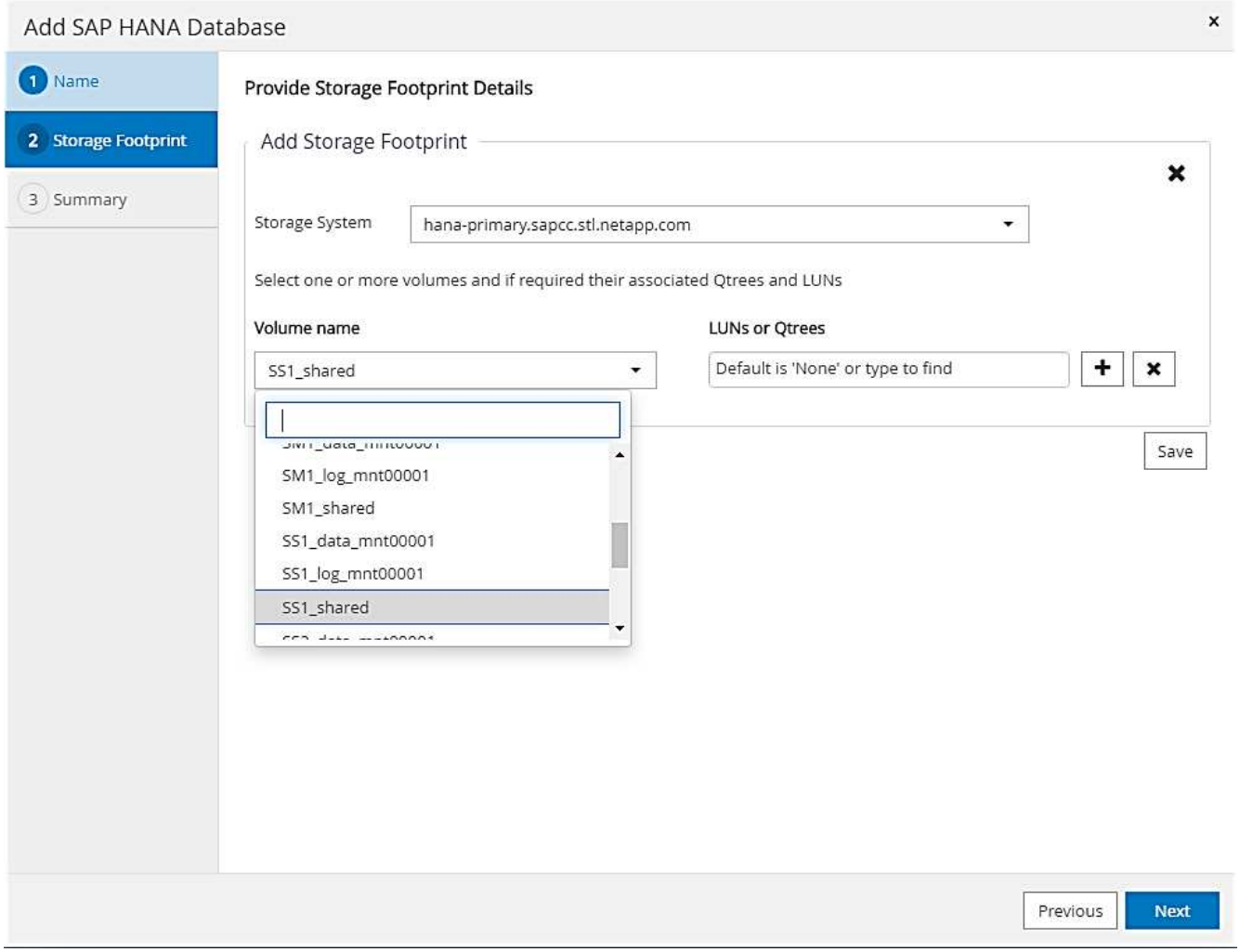
1. Wählen Sie auf der Registerkarte Ressource die Option nicht-Daten-Volume aus, und klicken Sie auf SAP HANA-Datenbank hinzufügen.



2. Wählen Sie in Schritt 1 des Dialogfelds SAP HANA-Datenbank hinzufügen in der Liste Ressourcentyp die Option nicht-Daten-Volumes aus. Geben Sie einen Namen für die Ressource und den zugehörigen SID und den SAP HANA Plug-in-Host an, den Sie für die Ressource verwenden möchten, und klicken Sie dann auf Weiter.



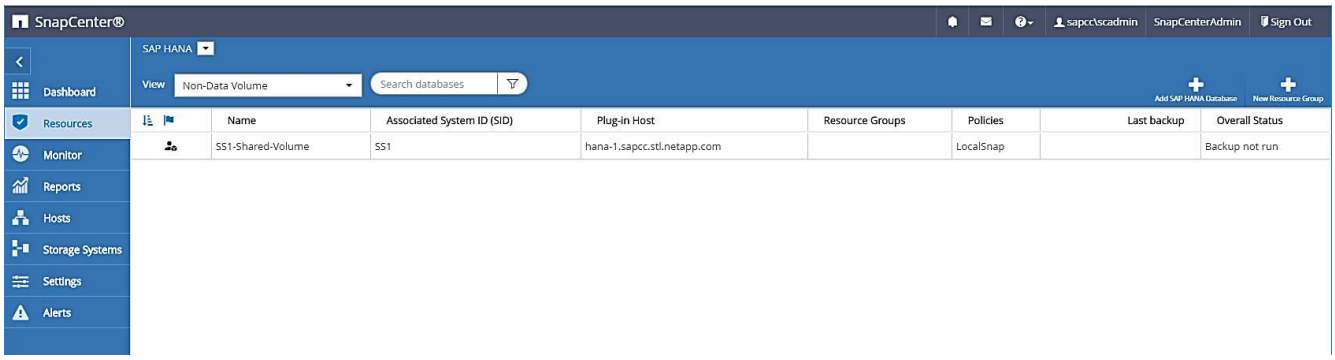
3. Fügen Sie die SVM und das Storage-Volume als Storage-Platzbedarf hinzu und klicken Sie dann auf Weiter.



4. Klicken Sie im Übersichtsschritt auf Fertig stellen, um die Einstellungen zu speichern.
5. Wiederholen Sie diese Schritte für alle erforderlichen nicht-Daten-Volumes.
6. Setzen Sie die Schutzkonfiguration der neuen Ressource fort.

> Die Datensicherung für nicht-Daten-Volume-Ressourcen ist identisch mit dem Workflow für SAP HANA Datenbankressourcen und kann auf individueller Ressourcenebene definiert werden.

Die folgende Abbildung zeigt eine Liste der konfigurierten Ressourcen, die keine Daten-Volumes enthalten.



Ressourcengruppen

Ressourcengruppen können den Schutz mehrerer Ressourcen bequem definieren, für die dieselben Sicherungsrichtlinien und denselben Zeitplan erforderlich sind. Einzelne Ressourcen, die zu einer Ressourcengruppe gehören, können weiterhin auf individueller Ebene geschützt werden.

Ressourcengruppen bieten die folgenden Funktionen:

- Sie können einer Ressourcengruppe mindestens eine Ressource hinzufügen. Alle Ressourcen müssen zum gleichen SnapCenter-Plug-in gehören.
- Der Schutz kann auf Ressourcengruppenebene definiert werden. Alle Ressourcen in der Ressourcengruppe verwenden die gleiche Richtlinie und den gleichen Zeitplan, wenn sie geschützt sind.
- Alle Backups im SnapCenter Repository und die Storage-Snapshot-Kopien haben denselben Namen wie im Ressourcenschutz definiert.
- Wiederherstellungsvorgänge werden auf nur einer Ressourcenebene und nicht als Teil einer Ressourcengruppe angewendet.
- Wenn Sie das Backup einer Ressource, die auf Ressourcengruppenebene erstellt wurde, mit SnapCenter löschen, wird dieses Backup für alle Ressourcen der Ressourcengruppe gelöscht. Das Backup wird gelöscht, das Backup aus dem SnapCenter Repository zu löschen und die Storage Snapshot Kopien zu löschen.
- Der Hauptanwendungsfall für Ressourcengruppen ist, wenn ein Kunde Backups verwenden möchte, die mit SnapCenter für das Systemklonen mit SAP Landscape Management erstellt wurden. Dies wird im nächsten Abschnitt beschrieben.

Nutzen Sie SnapCenter in Kombination mit dem SAP Landscape Management

Mit SAP Landscape Management (SAP Lama) können Kunden komplexe SAP Systemlandschaften in On-Premises-Datacentern und in Systemen, die in der Cloud ausgeführt werden, managen. SAP Lama ermöglicht zusammen mit dem NetApp Storage Services Connector (SSC) Storage-Vorgänge wie das Klonen und die Replizierung für SAP-Systemklone, Kopier- und Aktualisierungs-Anwendungsfälle mithilfe der Snapshot- und FlexClone-Technologie. Damit können Sie eine SAP Systemkopie auf Basis der Storage-Klontechnologie vollständig automatisieren und gleichzeitig die erforderliche SAP Nachbearbeitung erzielen. Weitere Informationen zu den Lösungen von NetApp für SAP Lama finden Sie unter "TR-4018: Integration von NetApp ONTAP-Systemen in SAP Landscape Management".

NetApp SSC und SAP Lama können On-Demand Snapshot-Kopien direkt mit NetApp SSC erstellen, können aber auch mithilfe von SnapCenter erstellte Snapshot-Kopien nutzen. Um SnapCenter Backups als Basis für Systemklonungs- und Kopiervorgänge bei SAP Lama zu nutzen, müssen folgende Voraussetzungen erfüllt werden:

- SAP Lama verlangt, dass alle Volumes in das Backup einbezogen werden; dazu gehören SAP HANA-Daten, Protokolle und gemeinsam genutzte Volumes.
- Alle Storage-Snapshot-Namen müssen identisch sein.
- Storage-Snapshot-Namen müssen mit VCM beginnen.

> Bei normalen Backup-Vorgängen empfiehlt NetApp nicht, das Protokoll-Volume einzubeziehen. Wenn Sie das Protokoll-Volume aus einem Backup wiederherstellen, werden die letzten aktiven Redo-Protokolle überschrieben und die Wiederherstellung der Datenbank in den letzten letzten Status verhindert.

SnapCenter Ressourcengruppen erfüllen alle diese Anforderungen. In SnapCenter werden drei Ressourcen

konfiguriert: Je eine Ressource für das Daten-Volume, das Protokoll-Volume und das gemeinsam genutzte Volume. Die Ressourcen werden einer Ressourcengruppe zugeordnet, und der Schutz wird dann auf Ressourcengruppenebene definiert. Im Ressourcengruppenschutz muss der benutzerdefinierte Snapshot-Name zu Beginn mit VCM definiert werden.

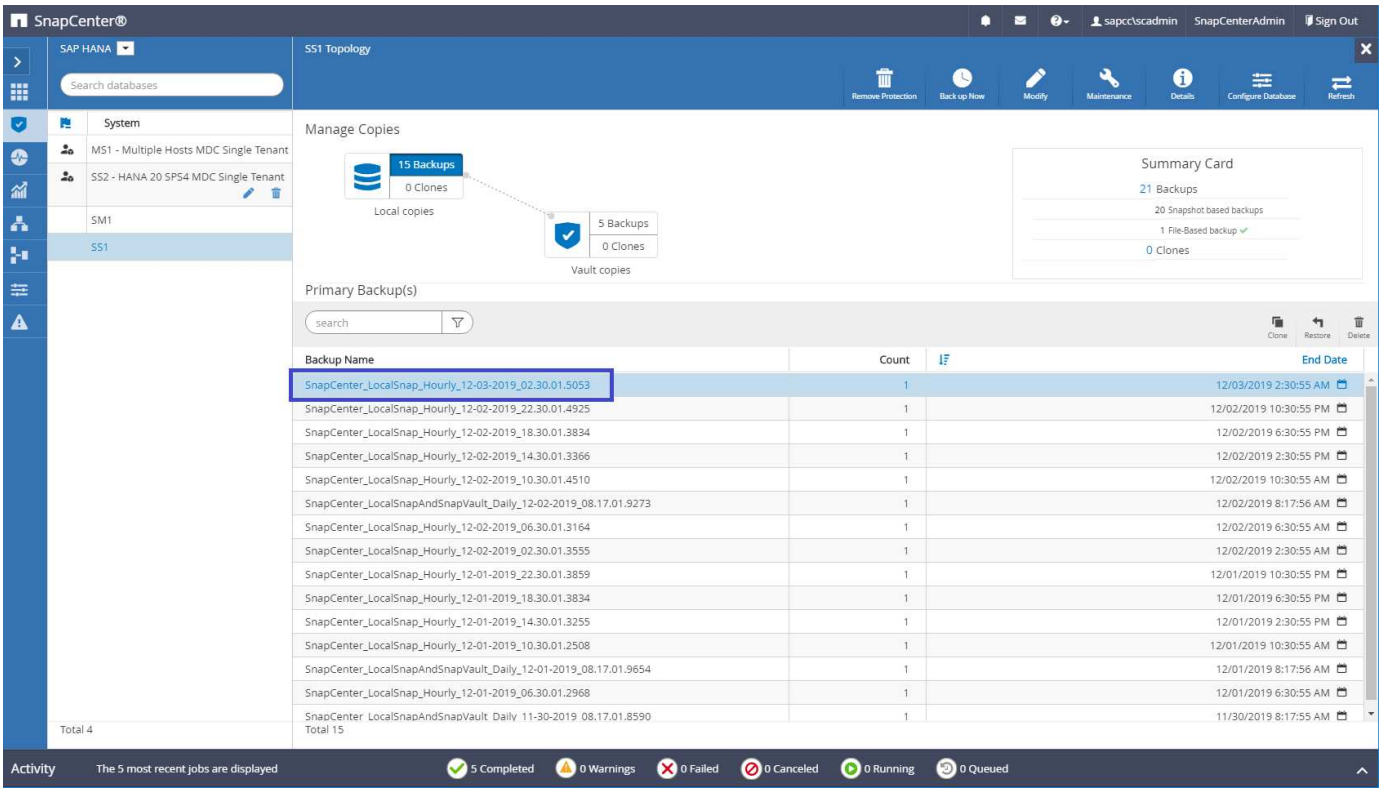
Datenbank-Backups

In SnapCenter werden Datenbank-Backups normalerweise mithilfe der Zeitpläne ausgeführt, die in der Ressourcenschutzkonfiguration der einzelnen HANA-Datenbanken definiert sind.

Ein On-Demand-Datenbank-Backup kann entweder über die SnapCenter GUI, eine PowerShell Befehlszeile oder REST-APIs durchgeführt werden.

Identifizierung von SnapCenter Backups in SAP HANA Studio

In der Topologie der SnapCenter Ressourcen wird eine Liste der mit SnapCenter erstellten Backups angezeigt. Die folgende Abbildung zeigt die auf dem primären Storage verfügbaren Backups und hebt das neueste Backup hervor.

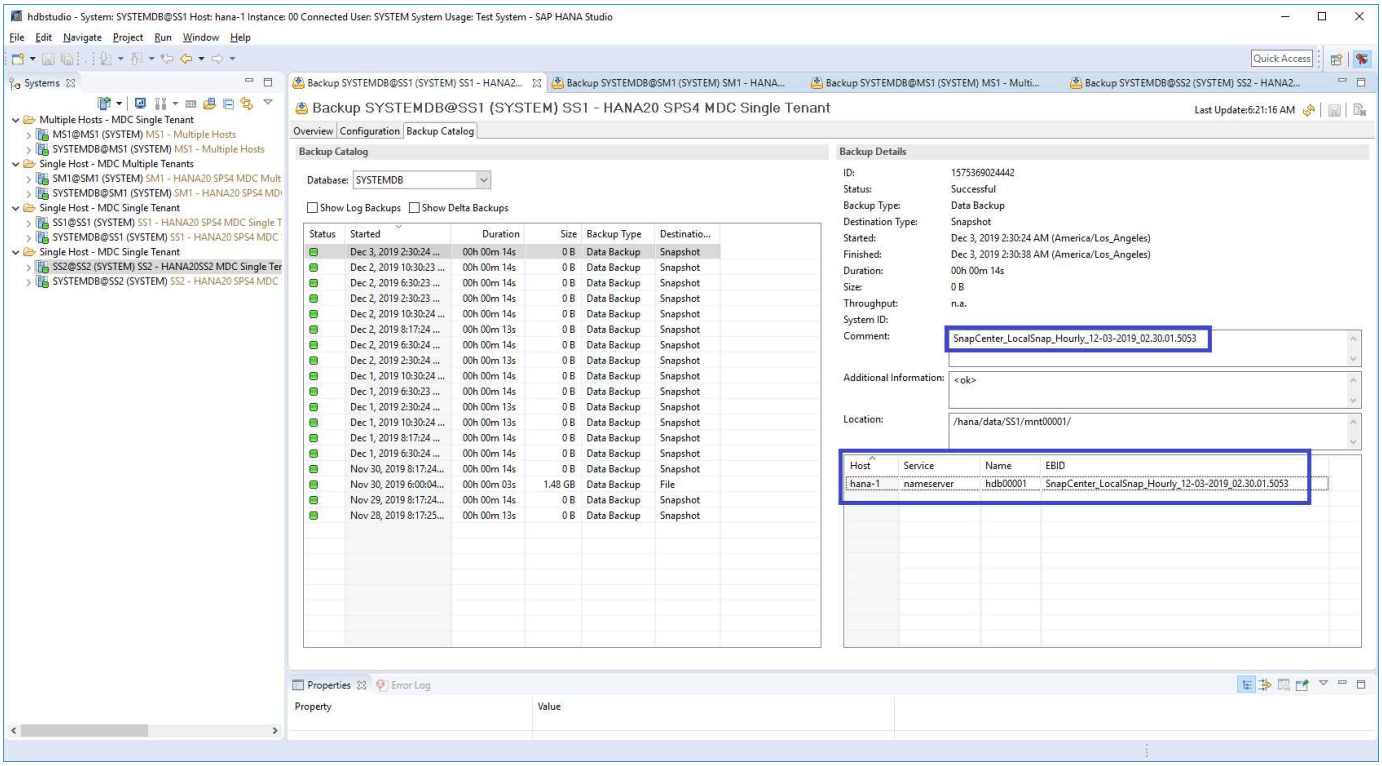


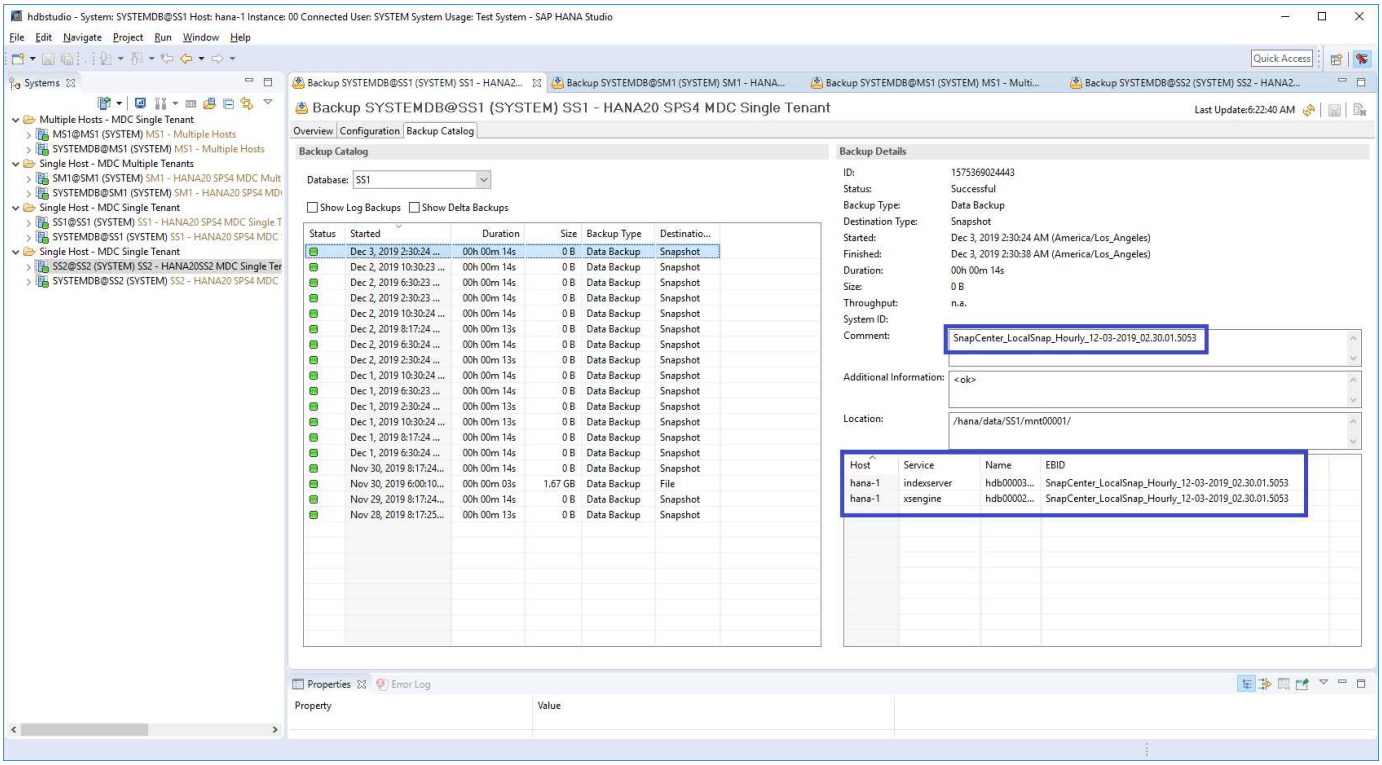
Bei einem Backup mit Storage Snapshot Kopien für ein SAP HANA MDC System wird eine Snapshot Kopie des Daten-Volumes erstellt. Dieses Daten-Volume enthält die Daten der Systemdatenbank sowie die Daten aller Mandantendatenbanken. Zur Berücksichtigung dieser physischen Architektur führt SAP HANA intern ein kombiniertes Backup der Systemdatenbank sowie aller Mandantendatenbanken durch, wenn SnapCenter ein Snapshot Backup auslöst. Das führt zu mehreren separaten Backup-Einträgen im SAP HANA Backup-Katalog: Einer für die Systemdatenbank und einer für jede Mandantendatenbank.

> Bei SAP HANA Single-Container-Systemen enthält das Datenbank-Volume nur die einzige Datenbank, und es gibt nur einen Eintrag im SAP HANA Backup-Katalog.

Im SAP HANA Backup-Katalog wird der SnapCenter-Backup-Name als A gespeichert `Comment` Außerdem Feld `External Backup ID (EBID)`. Dies wird im folgenden Screenshot für die Systemdatenbank und in dem Screenshot danach für die Mandanten-Datenbank SS1 dargestellt. Beide Abbildungen zeigen den im Kommentarfeld gespeicherten SnapCenter Backup-Namen und EBID.

> Die HANA 2.0 SPS4 Version (Revision 40 und 41) zeigt für Snapshot-basierte Backups immer eine Sicherungsgröße von null. Das wurde mit Revision 42 behoben. Weitere Informationen finden Sie im SAP-Hinweis "https://launchpad.support.sap.com/#/notes/2795010".

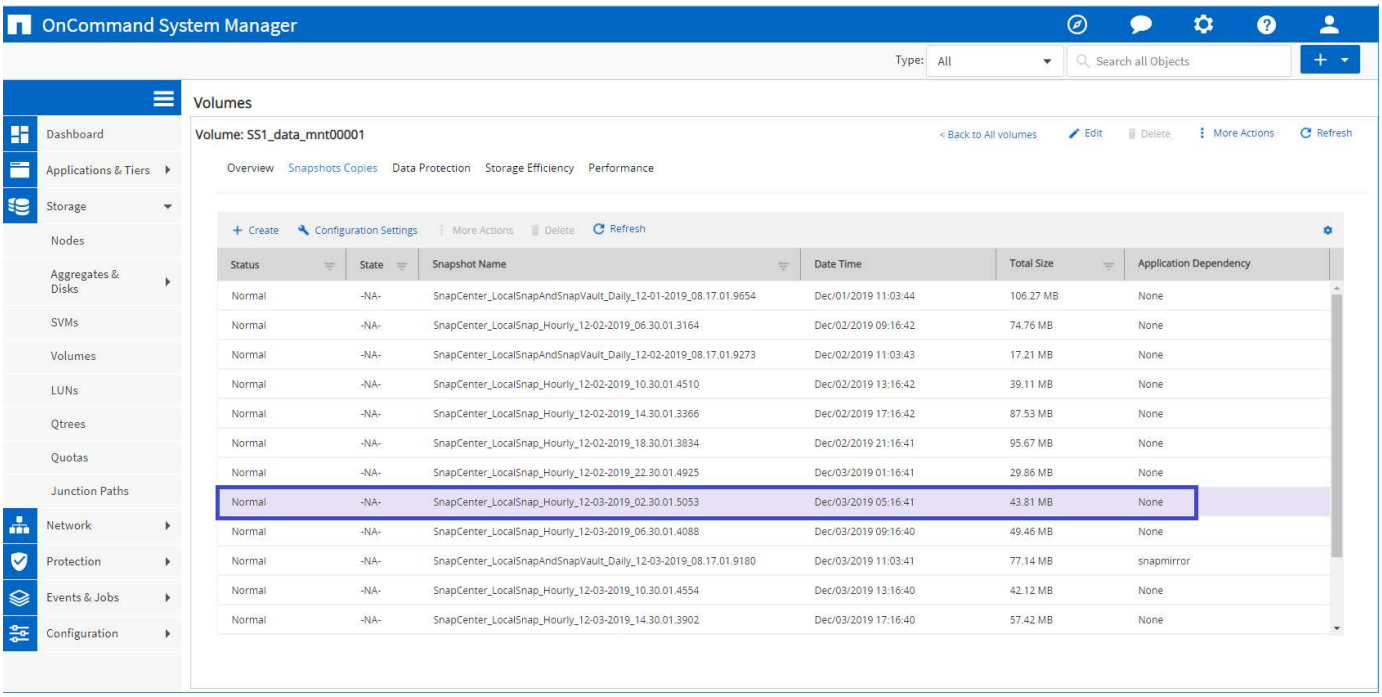




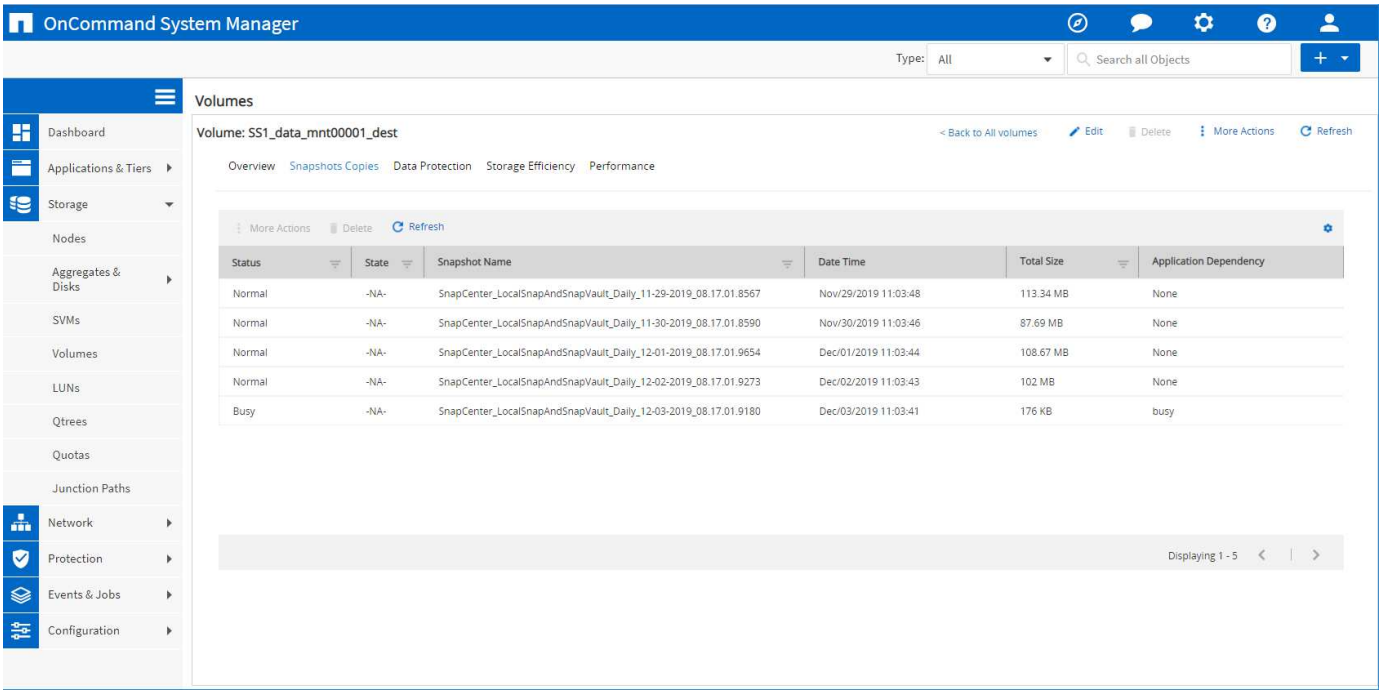
SnapCenter ist nur sich seiner eigenen Backups bewusst. Zusätzliche Backups, die beispielsweise mit SAP HANA Studio erstellt wurden, sind im SAP HANA Katalog sichtbar, jedoch nicht im SnapCenter.

Ermitteln von SnapCenter Backups auf den Storage-Systemen

Verwenden Sie NetApp OnCommand System Manager, um die Backups auf Storage-Ebene anzuzeigen, und wählen Sie das Datenbank-Volume in der Ansicht „SVM – Volume“ aus. Auf der unteren Registerkarte Snapshot Kopien werden die Snapshot Kopien des Volume angezeigt. Der folgende Screenshot zeigt die verfügbaren Backups für das Datenbank-Volume `SS1_data_mnt00001` Auf dem primären Storage. Das hervorgehobene Backup ist der in den vorherigen Bildern in SnapCenter und SAP HANA Studio angezeigte Backup mit derselben Namenskonvention.



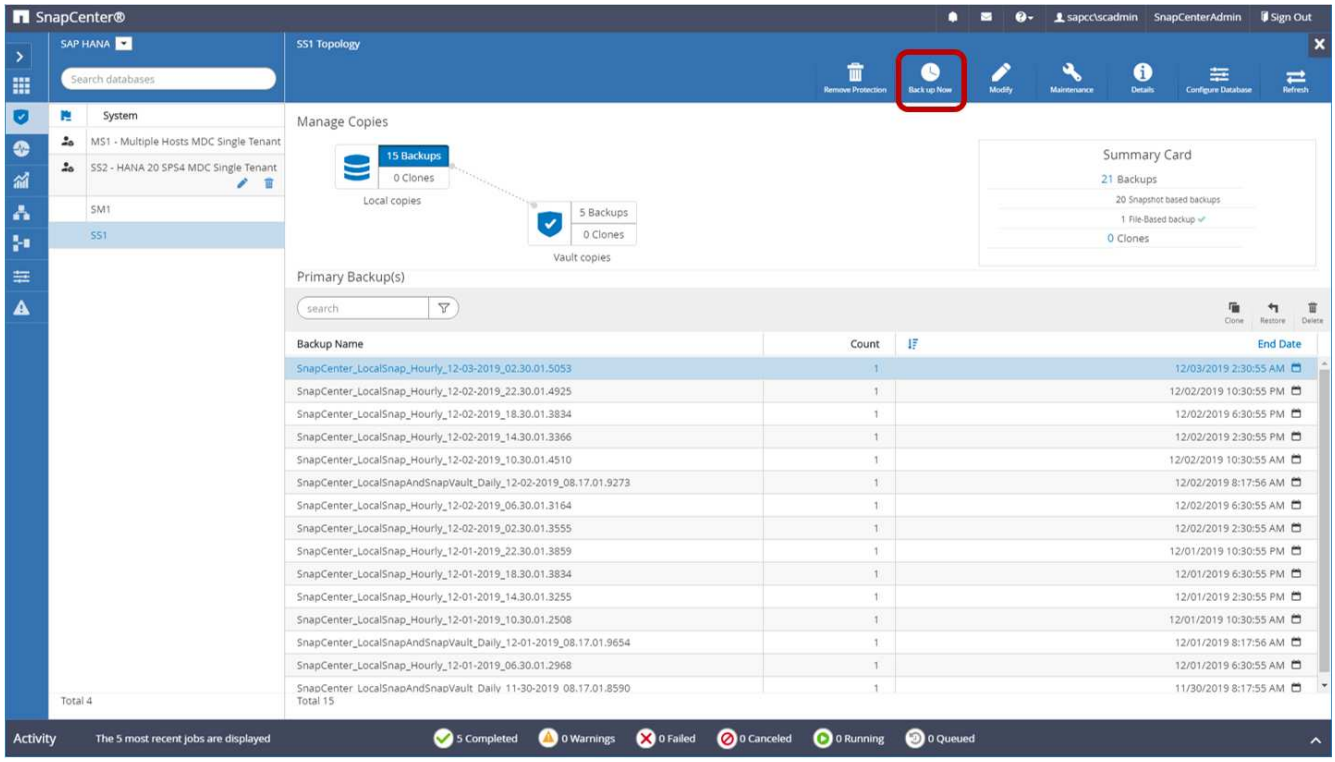
Der folgende Screenshot zeigt die verfügbaren Backups für das Replikationsziel-Volume `hana_SA1_data_mnt00001_dest` Auf dem sekundären Storage-System.



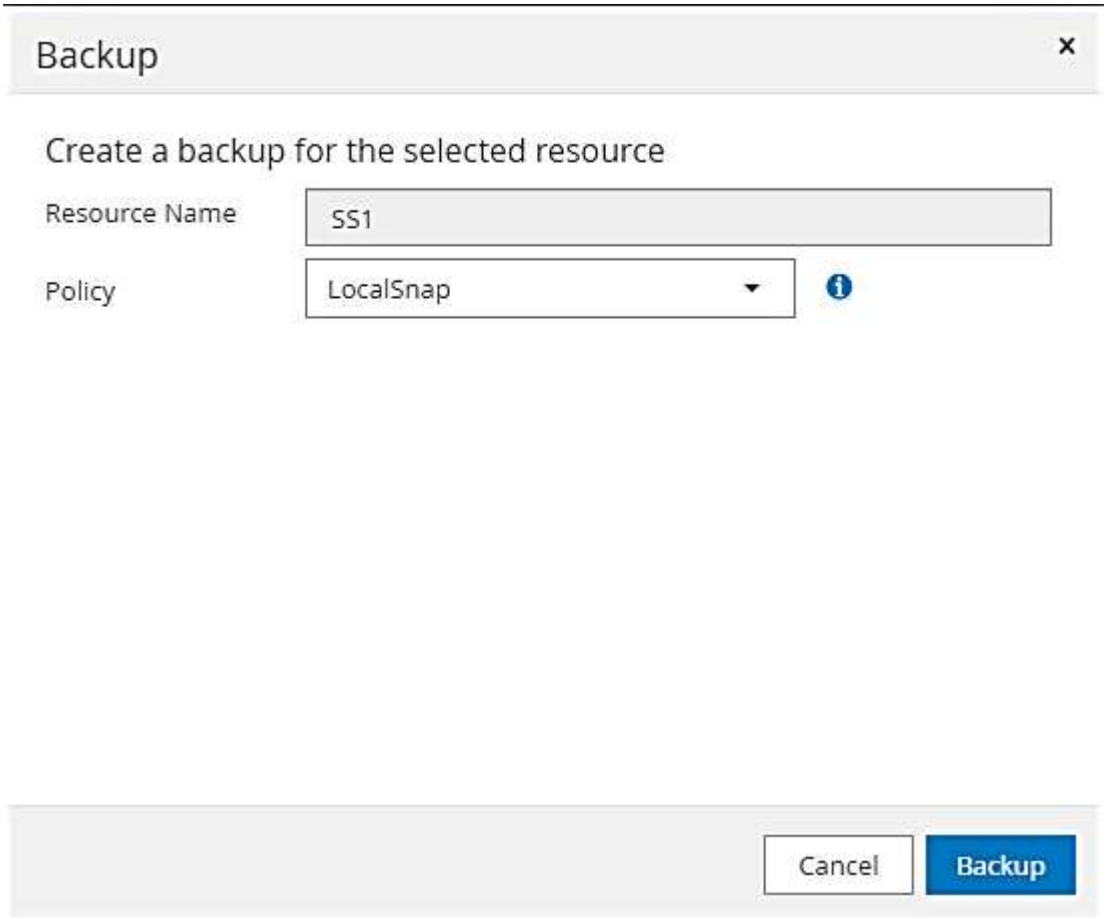
On-Demand-Datenbank-Backup auf dem Primärspeicher

1. Wählen Sie in der Ressourcenansicht die Ressource aus, und doppelklicken Sie auf die Linie, um zur Topologieansicht zu wechseln.

   Die Ansicht „Ressourcentopologie“ bietet einen Überblick über alle verfügbaren Backups, die mit SnapCenter erstellt wurden. Im oberen Bereich dieser Ansicht wird die Backup-Topologie angezeigt, die Backups im primären Storage (lokale Kopien) und, sofern verfügbar, im externen Backup-Storage (Vault-Kopien) angezeigt.

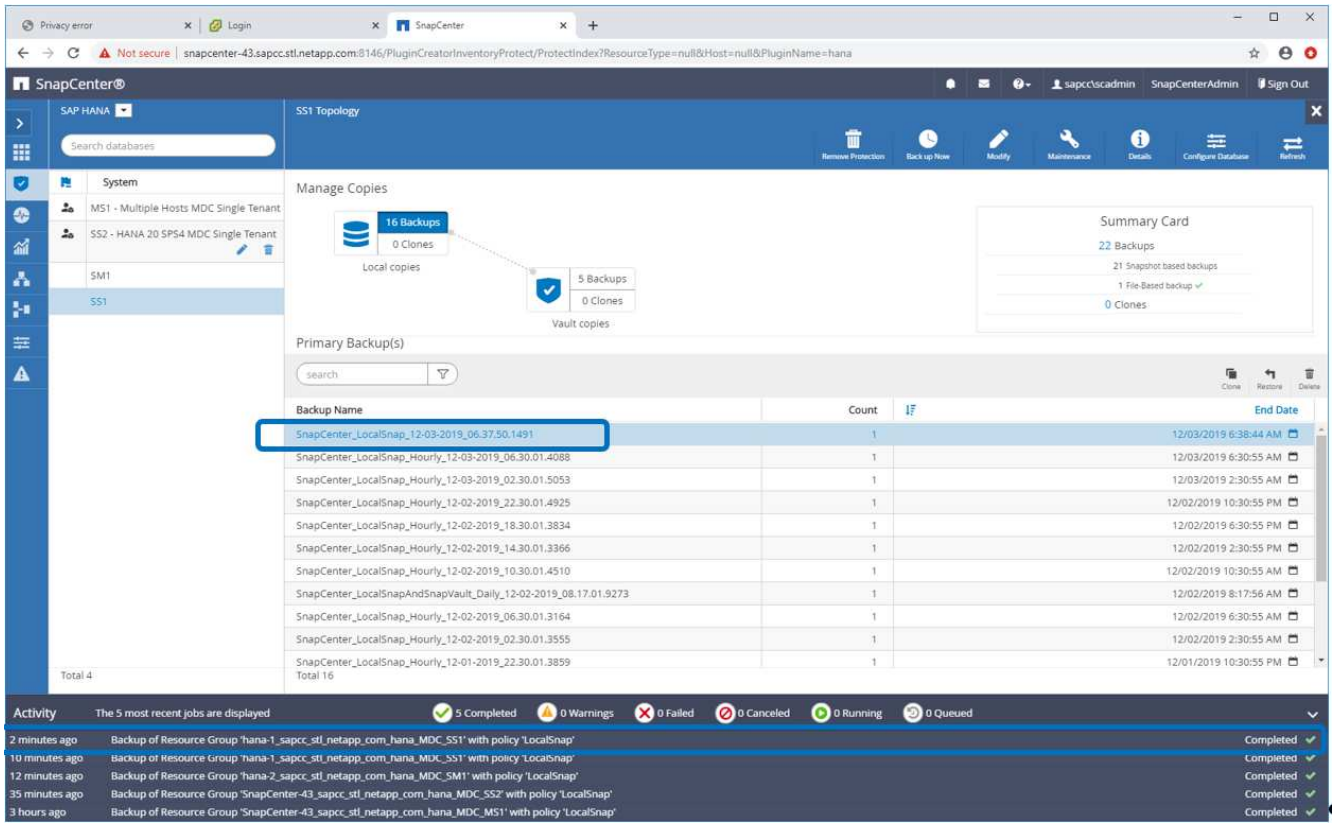


2. Klicken Sie in der oberen Zeile auf das Symbol Jetzt sichern, um ein On-Demand-Backup zu starten. Wählen Sie aus der Dropdown-Liste die Backup-Richtlinie aus `LocalSnap` Anschließend auf Backup klicken, um das On-Demand-Backup zu starten.

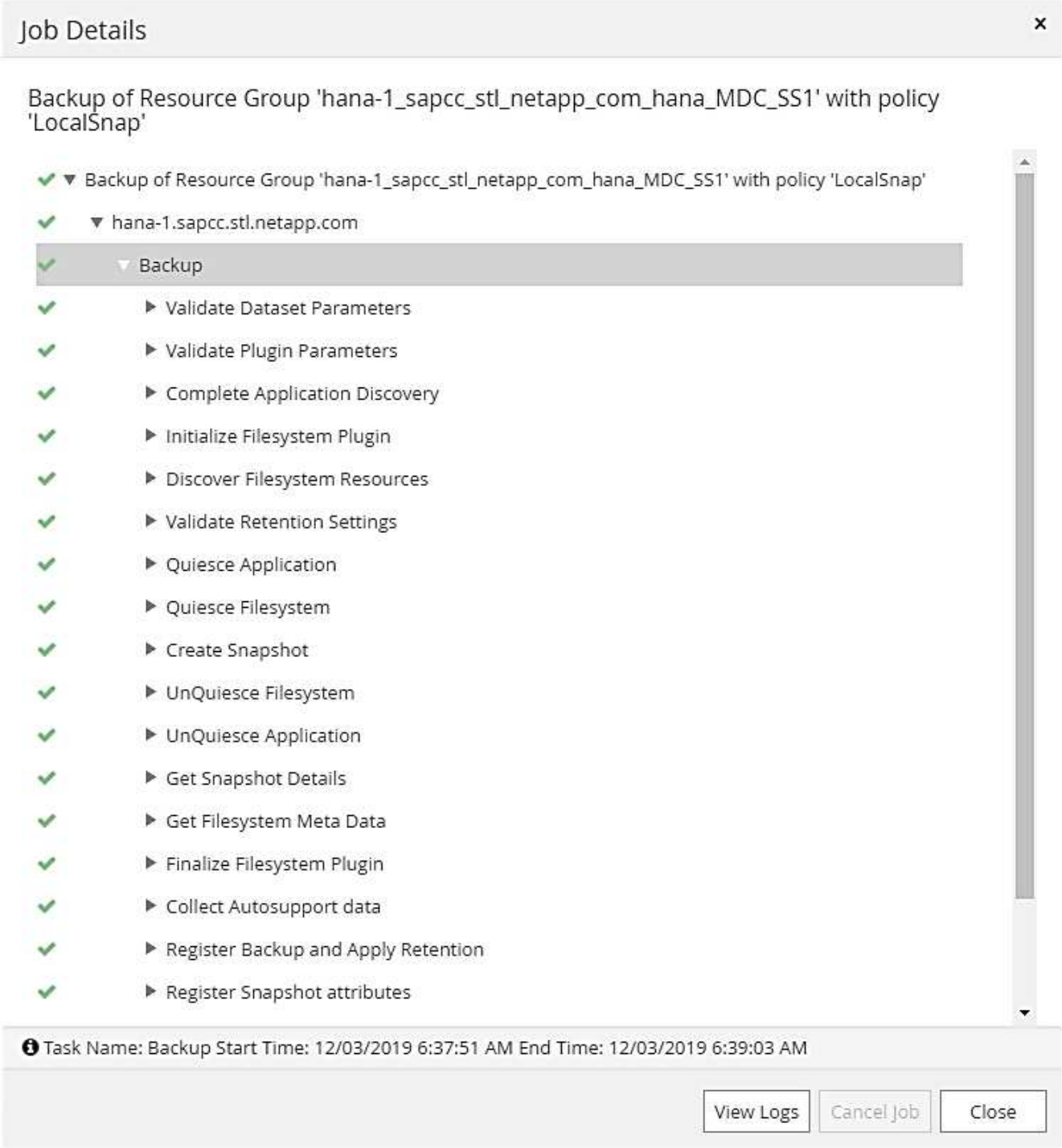


Dies startet den Sicherungsauftrag. Ein Protokoll der vorherigen fünf Jobs wird im Aktivitätsbereich unterhalb der Topologieansicht angezeigt. Nach Abschluss des Backups wird in der Topologieansicht ein neuer Eintrag angezeigt. Die Backup-Namen folgen derselben Namenskonvention wie der Snapshot-Name, der im Abschnitt definiert wurde "„Konfiguration des Ressourcenschutzes“."

> Sie müssen die Topologieansicht schließen und erneut öffnen, um die aktualisierte Backup-Liste anzuzeigen.



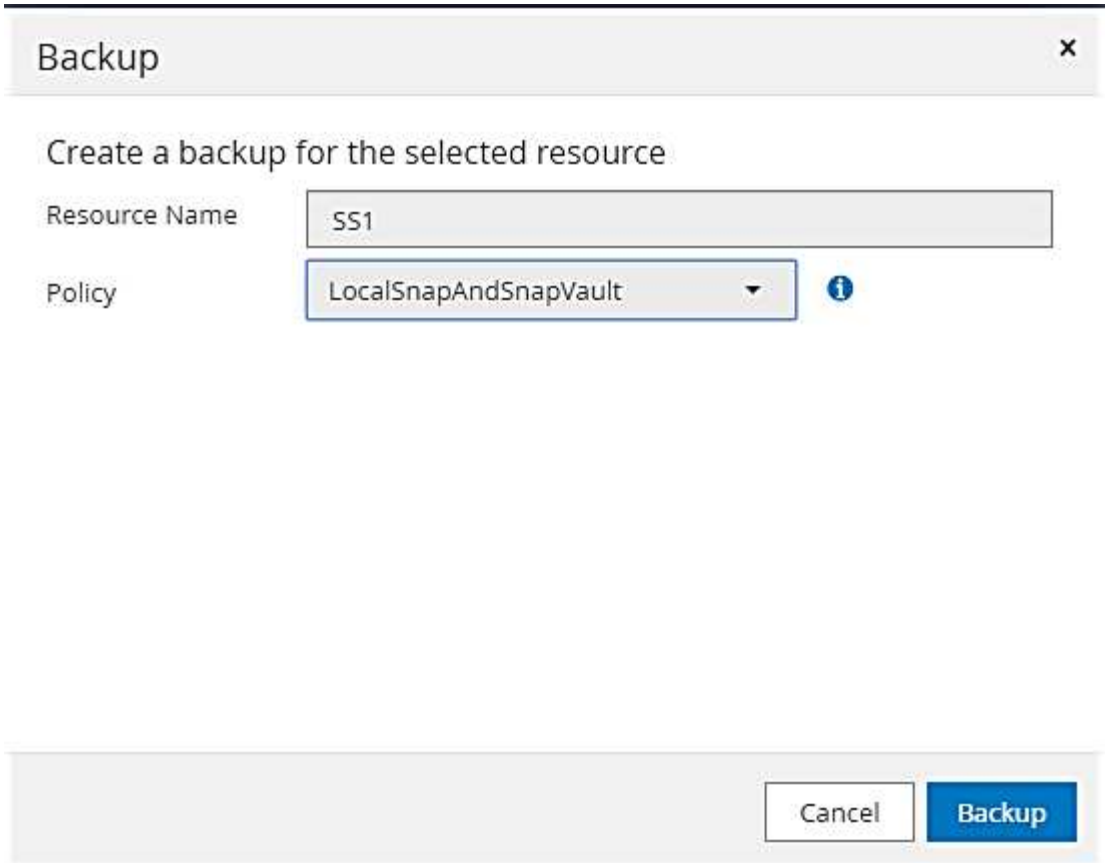
3. Die Jobdetails werden angezeigt, wenn Sie im Aktivitätsbereich auf die Vorgangszeile des Jobs klicken. Sie können ein detailliertes Jobprotokoll öffnen, indem Sie auf Protokolle anzeigen klicken.



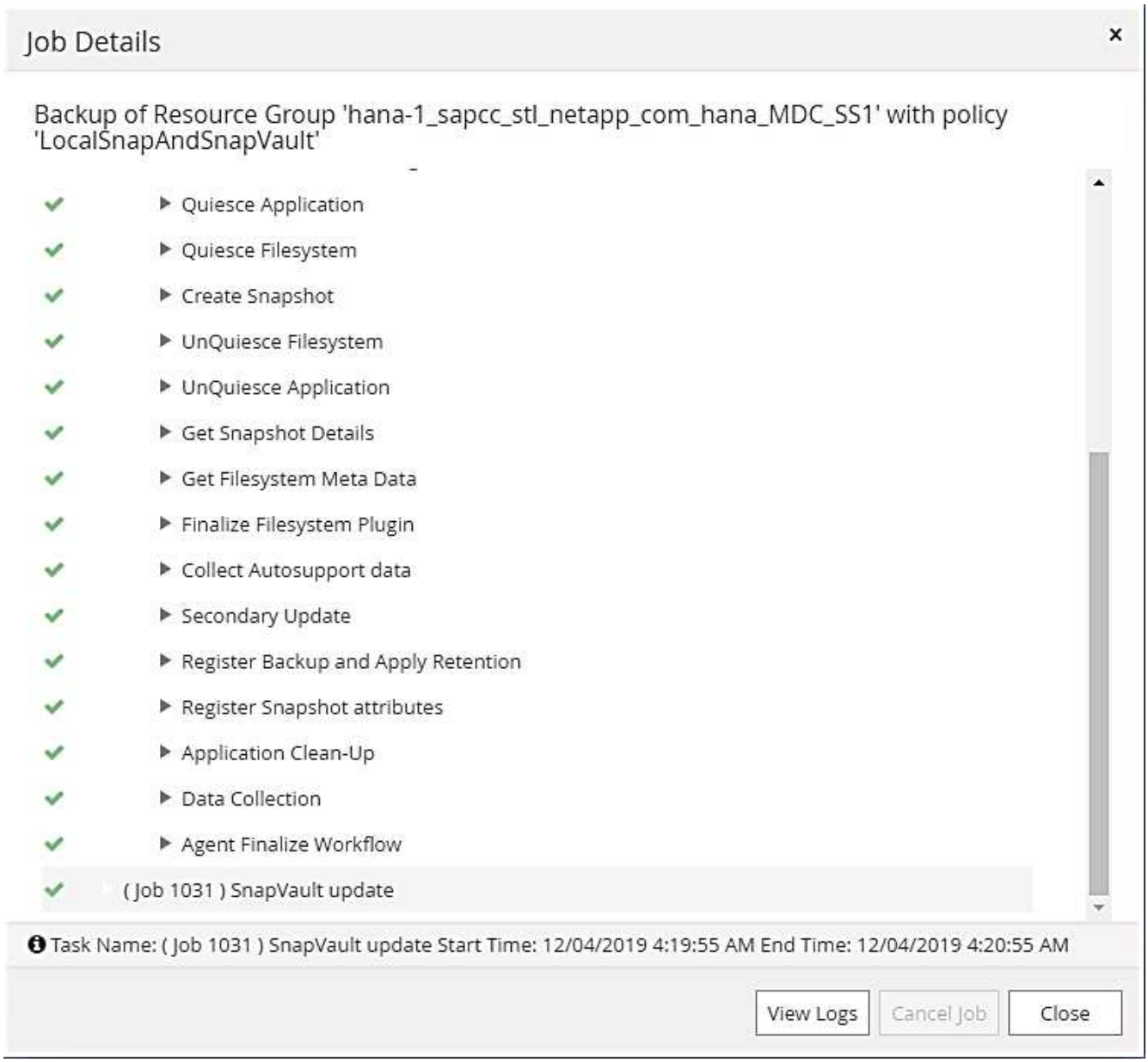
4. Im SAP HANA Studio ist das neue Backup im Backup-Katalog sichtbar. Derselbe Backup-Name in SnapCenter wird auch im Kommentar und im EBID-Feld im Backup-Katalog verwendet.

On-Demand-Datenbank-Backups mit SnapVault Replizierung

1. Wählen Sie in der Ressourcenansicht die Ressource aus, und doppelklicken Sie auf die Linie, um zur Topologieansicht zu wechseln.
2. Klicken Sie in der oberen Zeile auf das Symbol Jetzt sichern, um ein On-Demand-Backup zu starten. Wählen Sie aus der Dropdown-Liste die Backup-Richtlinie aus `LocalSnapAndSnapVault`, Dann klicken Sie auf Backup, um das On-Demand-Backup zu starten.

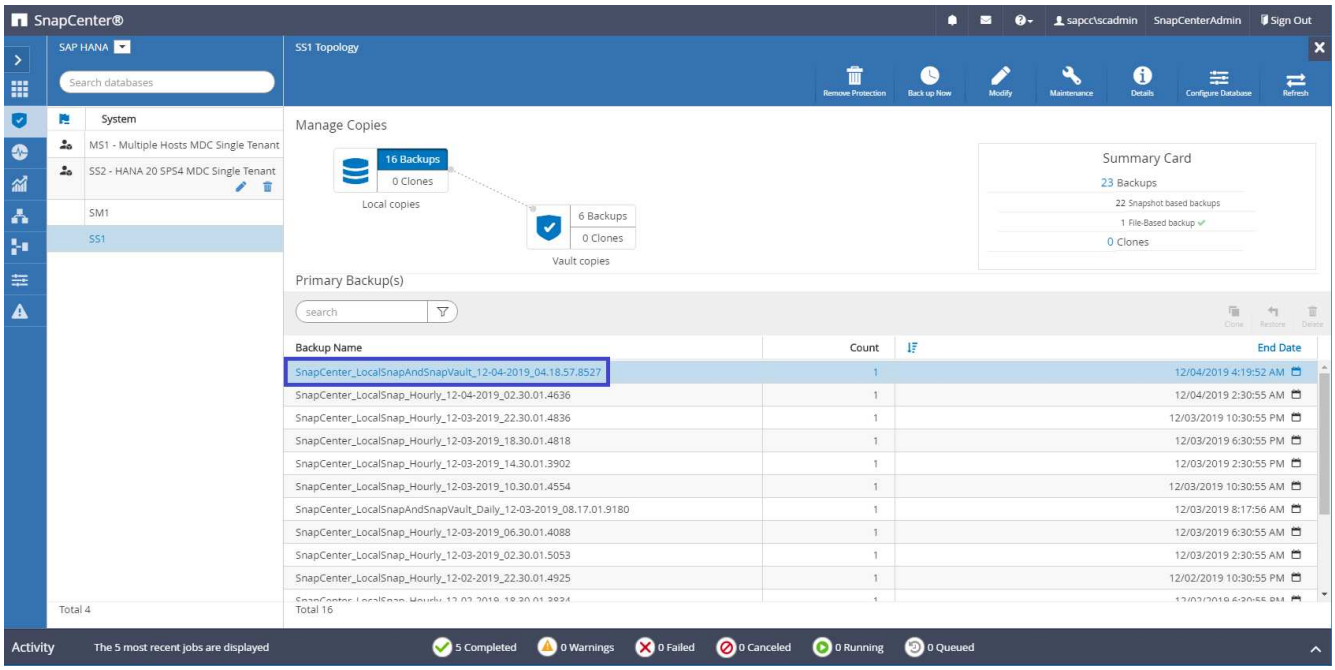


3. Die Jobdetails werden angezeigt, wenn Sie im Aktivitätsbereich auf die Vorgangszeile des Jobs klicken.

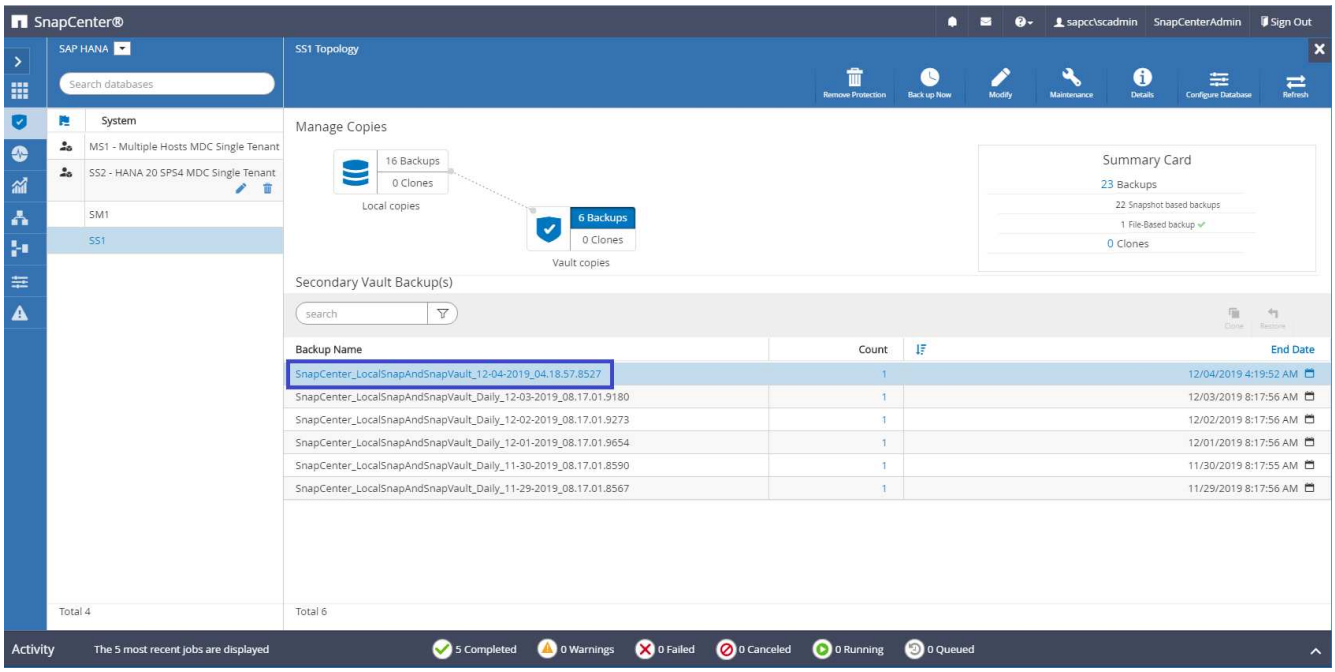


4. Nach Abschluss des Backups wird in der Topologieansicht ein neuer Eintrag angezeigt. Die Backup-Namen folgen derselben Namenskonvention wie der Snapshot-Name, der im Abschnitt definiert wurde "„Konfiguration des Ressourcenschutzes“."

> Sie müssen die Topologieansicht schließen und erneut öffnen, um die aktualisierte Backup-Liste anzuzeigen.



5. Durch Auswahl von Vault Kopien werden Backups im sekundären Storage angezeigt. Der Name des replizierten Backups entspricht dem Backup-Namen im primären Storage.



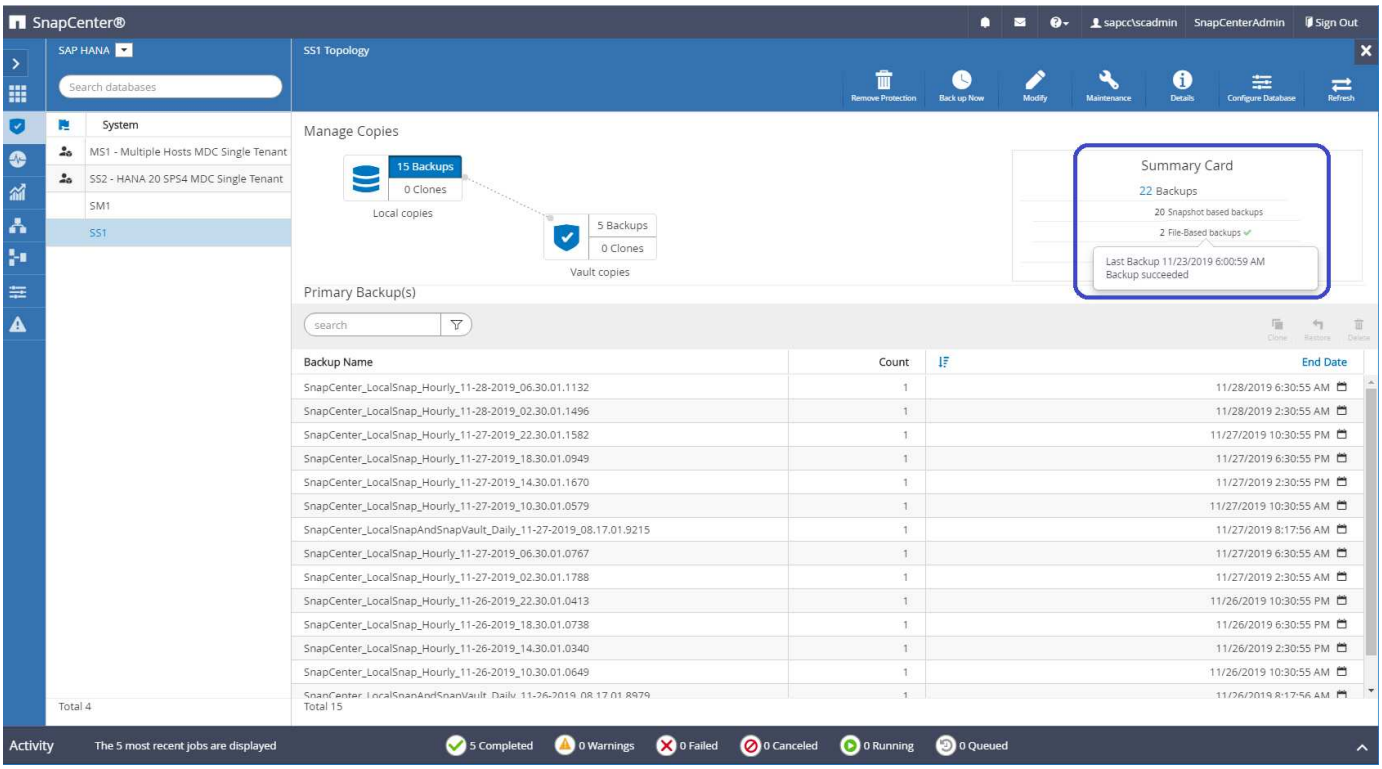
6. Im SAP HANA Studio ist das neue Backup im Backup-Katalog sichtbar. Derselbe Backup-Name in SnapCenter wird auch im Kommentar und im EBID-Feld im Backup-Katalog verwendet.

Block-Integritätsprüfung

SAP empfiehlt, Storage-basierte Snapshot-Backups mit einem wöchentlichen dateibasierten Backup zu kombinieren, um eine Integritätsprüfung für Blöcke durchzuführen. SnapCenter unterstützt die Ausführung einer Block-Integritätsprüfung, indem eine Richtlinie verwendet wird, in der das dateibasierte Backup als Backup-Typ ausgewählt wird.

Bei der Planung von Backups mithilfe dieser Richtlinie erstellt SnapCenter eine standardmäßige SAP HANA Datei-Backup für das System und die Mandantendatenbanken.

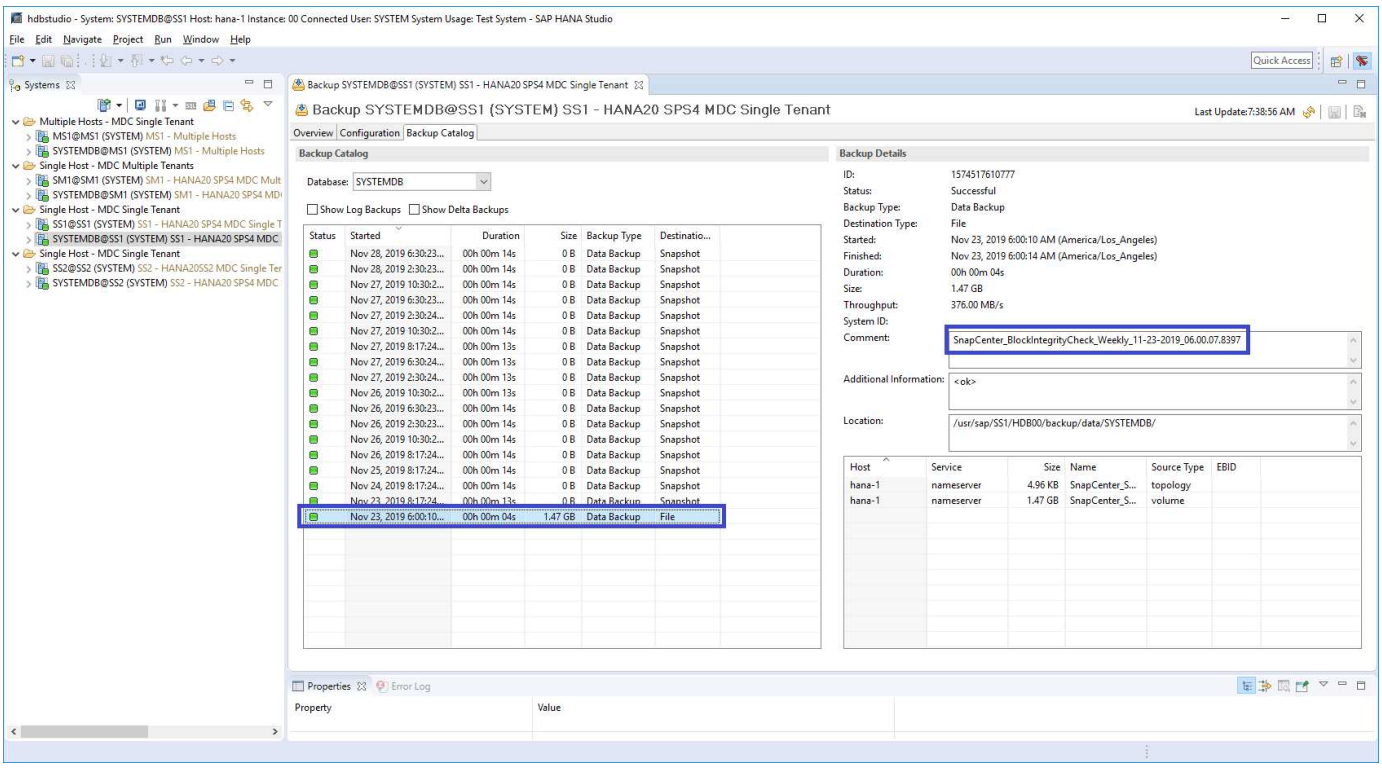
SnapCenter zeigt die Blockintegritätsprüfung nicht auf dieselbe Weise an wie Backups basierend auf Snapshot-Kopien. Stattdessen zeigt die Übersichtskarte die Anzahl der dateibasierten Backups und den Status des vorherigen Backups an.



Ein Backup zur Block-Integritätsprüfung kann nicht mithilfe der SnapCenter UI gelöscht werden, er kann jedoch mithilfe von PowerShell Befehlen gelöscht werden.

```
PS C:\Users\scadmin> Get-SmBackupReport -Resource SS1
SmBackupId                : 9
SmJobId                   : 42
StartDateTime             : 11/19/2019 8:26:32 AM
EndDateTime               : 11/19/2019 8:27:33 AM
Duration                  : 00:01:00.7652030
CreatedDateTime           : 11/19/2019 8:27:24 AM
Status                    : Completed
ProtectionGroupName       : hana-1_sapcc_stl_netapp_com_hana_MDC_SS1
SmProtectionGroupId       : 1
PolicyName                : BlockIntegrityCheck
SmPolicyId                : 5
BackupName                : SnapCenter_BlockIntegrityCheck_11-19-
2019_08.26.33.2913
VerificationStatus        : NotApplicable
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
PluginCode                : SCC
PluginName                : hana
JobTypeId                 : 0
JobHost                   :

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

Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"): y


BackupResult : {}
Result       : SMCoreContracts.SMResult
TotalCount   : 0
DisplayCount : 0
Context      :
Job          : SMCoreContracts.SmJob



PS C:\Users\scadmin>
```

Der SAP HANA-Backup-Katalog zeigt Einträge sowohl für das System als auch für die Mandanten-Datenbanken an. Die folgende Abbildung zeigt eine SnapCenter-Blockintegritätsprüfung im Backup-Katalog der Systemdatenbank.



Eine erfolgreiche Überprüfung der Blockintegrität erstellt standardisierte SAP HANA Daten-Backup-Dateien. SnapCenter verwendet den Backup-Pfad, der in der HANA-Datenbank für dateibasierte Daten-Backup-Vorgänge konfiguriert wurde.

```
hana-1:/usr/sap/SS1/HDB00/backup/data # ls -al *
DB_SS1:
total 1710840
drwxr-xr-- 2 ss1adm sapsys       4096 Nov 28 10:25 .
drwxr-xr-- 4 ss1adm sapsys       4096 Nov 19 05:11 ..
-rw-r----- 1 ss1adm sapsys     155648 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ss1adm sapsys   83894272 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_2_1
-rw-r----- 1 ss1adm sapsys 1660952576 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_3_1
SYSTEMDB:
total 1546340
drwxr-xr-- 2 ss1adm sapsys       4096 Nov 28 10:24 .
drwxr-xr-- 4 ss1adm sapsys       4096 Nov 19 05:11 ..
-rw-r----- 1 ss1adm sapsys     159744 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ss1adm sapsys 1577066496 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_1_1
```

Restore und Recovery

In den folgenden Abschnitten werden die Wiederherstellungs- und Recovery-Workflows von drei verschiedenen Szenarien und Beispielkonfigurationen beschrieben.

- Automatisierte Wiederherstellung und Wiederherstellung:
  - Automatisch ermittelte HANA-System SS1
  - SAP HANA ein einzelner Host, MDC ein Mandantensystem mit NFS
- Restore und Recovery einzelner Mandanten:
  - Automatisch ermittelte HANA-System SM1
  - SAP HANA einzelner Host, MDC mandantenfähiges System mit NFS
- Wiederherstellung mit manueller Wiederherstellung:
  - Manuell konfiguriertes HANA-System SS2
  - SAP HANA einzelner Host, MDC mandantenfähiges System mit NFS

In den folgenden Abschnitten werden die Unterschiede zwischen einem einzelnen SAP HANA Host und mehreren Hosts sowie in HANA-Systemen mit Fibre Channel-SAN-Anbindung hervorgehoben.

Die Beispiele zeigen, dass SAP HANA Studio als Tool zur manuellen Wiederherstellung dient. Sie können

auch SAP HANA Cockpit oder HANA SQL Statements verwenden.

Automatisiertes Restore und Recovery

Bei SnapCenter 4.3 werden automatisierte Restore- und Recovery-Vorgänge für einzelne HANA-Container oder MDC-Mandantensysteme unterstützt, die von SnapCenter automatisch erkannt wurden.

Sie können eine automatisierte Wiederherstellung und Operation mit den folgenden Schritten ausführen:

1. Wählen Sie das Backup aus, das für den Wiederherstellungsvorgang verwendet werden soll. Das Backup kann aus den folgenden Speicheroptionen ausgewählt werden:
   - Primärspeicher
   - Externer Backup-Storage (SnapVault Ziel)
2. Wählen Sie den Wiederherstellungstyp aus. Wählen Sie mit Volume Revert oder ohne Volume Revert die Option Complete Restore.

   > Die Option Volume Revert ist nur für die Wiederherstellung von Vorgängen im primären Storage und, wenn die HANA Datenbank NFS als Storage-Protokoll verwendet.

3. Wählen Sie den Wiederherstellungstyp aus den folgenden Optionen aus:
   - Auf den letzten Stand
   - Zeitpunktgenau
   - Zu einem bestimmten Daten-Backup
   - Keine Wiederherstellung

   > Der ausgewählte Wiederherstellungstyp wird für die Wiederherstellung des Systems und der Mandanten-Datenbank verwendet.

Als Nächstes führt SnapCenter die folgenden Operationen durch:

1. Die HANA-Datenbank wird gestoppt.
2. Die Datenbank wird wiederhergestellt.

   Abhängig vom ausgewählten Wiederherstellungstyp und dem verwendeten Storage-Protokoll werden verschiedene Operationen ausgeführt.

   - Wenn die Option „NFS“ und „Volume revert“ ausgewählt sind, hängt SnapCenter das Volume ab, stellt das Volume mithilfe von Volume-basierten SnapRestore auf der Storage-Ebene wieder her und hängt das Volume an.
   - Wenn NFS ausgewählt ist und die Volume-Zurücksetzung nicht ausgewählt ist, stellt SnapCenter alle Dateien mithilfe von SnapRestore-Vorgängen mit einer einzigen Datei auf der Storage-Ebene wieder her.
   - Wenn Fibre Channel SAN ausgewählt ist, hängt SnapCenter die LUN(s) ab, stellt die LUN(s) anhand einzelner Datei-SnapRestore-Vorgänge auf der Storage-Ebene wieder her und erkennt und hängt die LUN(s) an.
3. Es stellt die Datenbank wieder her:
   a. Es stellt die Systemdatenbank wieder her.

b. Die Mandantendatenbank wird wiederhergestellt.

   Bei HANA-Systemen mit einzelnen Containern erfolgt die Recovery in einem Schritt:

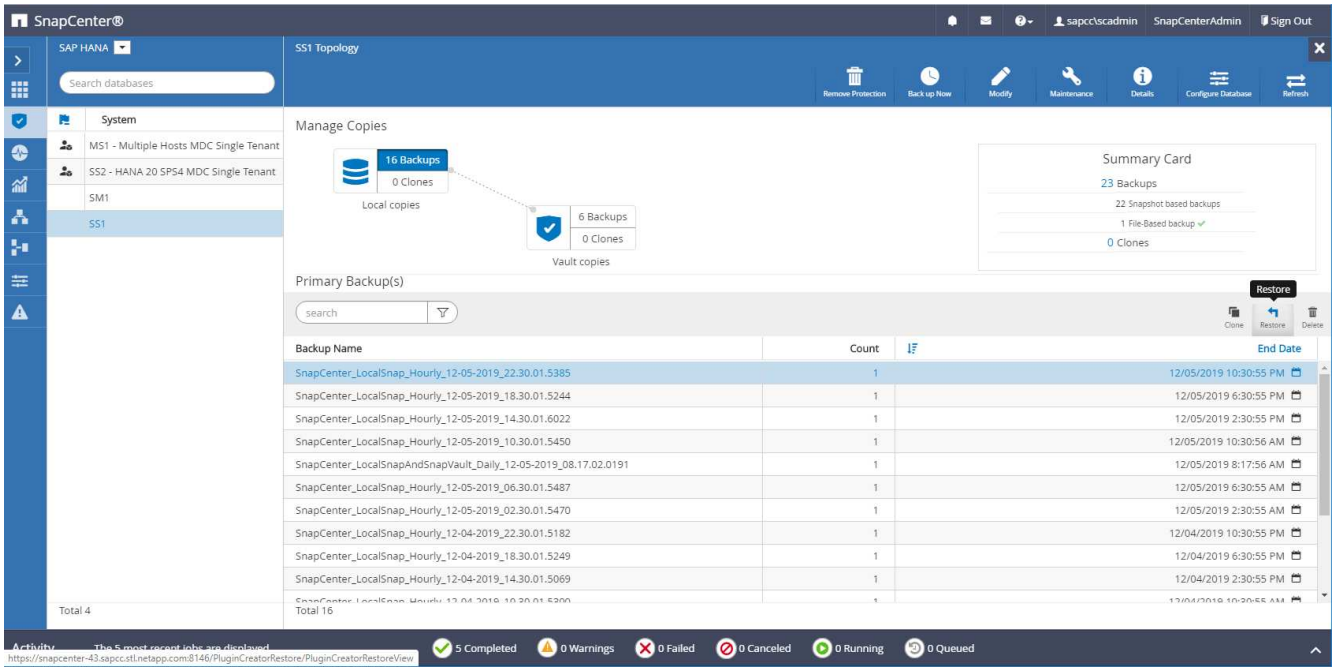
c. Es startet die HANA-Datenbank.

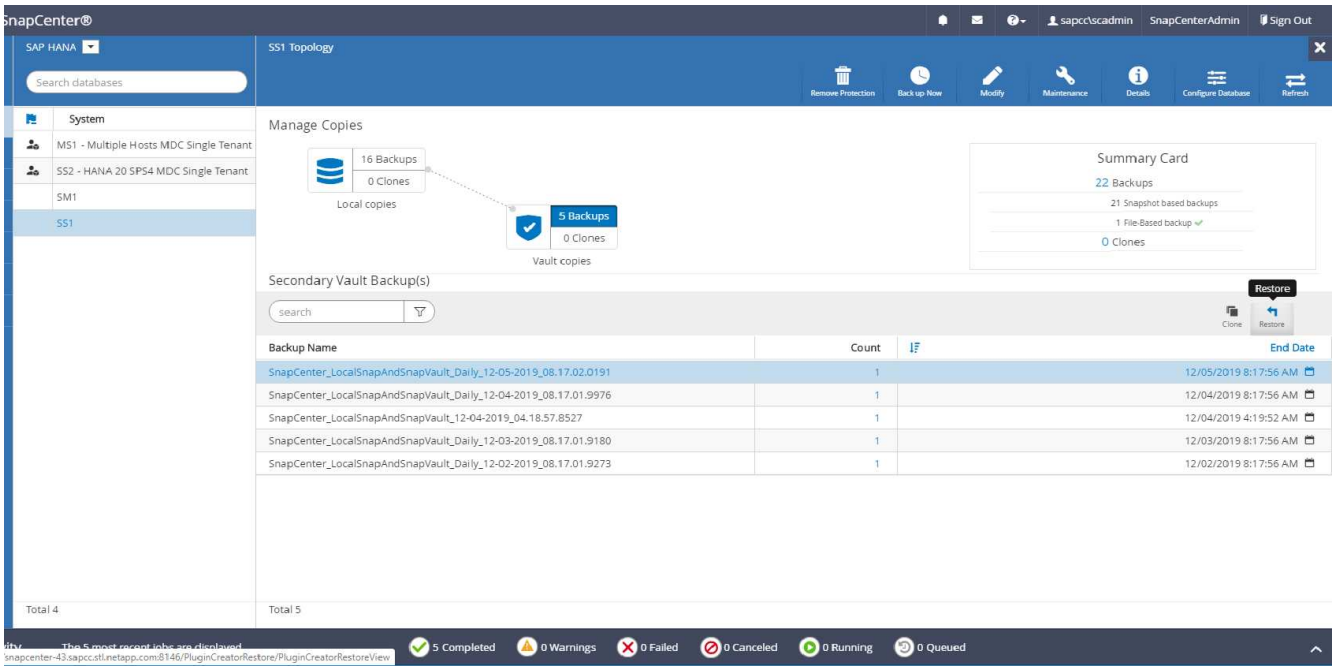
> Wenn keine Wiederherstellung ausgewählt ist, beendet SnapCenter und der Wiederherstellungsvorgang für das System, die Mandantendatenbank muss manuell durchgeführt werden.

Dieser Abschnitt enthält die Schritte für den automatisierten Restore- und Recovery-Vorgang des automatisch erkannten HANA-Systems SS1 (SAP HANA einzelner Host, MDC einzelnes Mandantensystem mit NFS).

1. Wählen Sie ein Backup in SnapCenter aus, das für den Wiederherstellungsvorgang verwendet werden soll.

   > Sie können Restores von primärem oder externem Backup-Storage wählen.



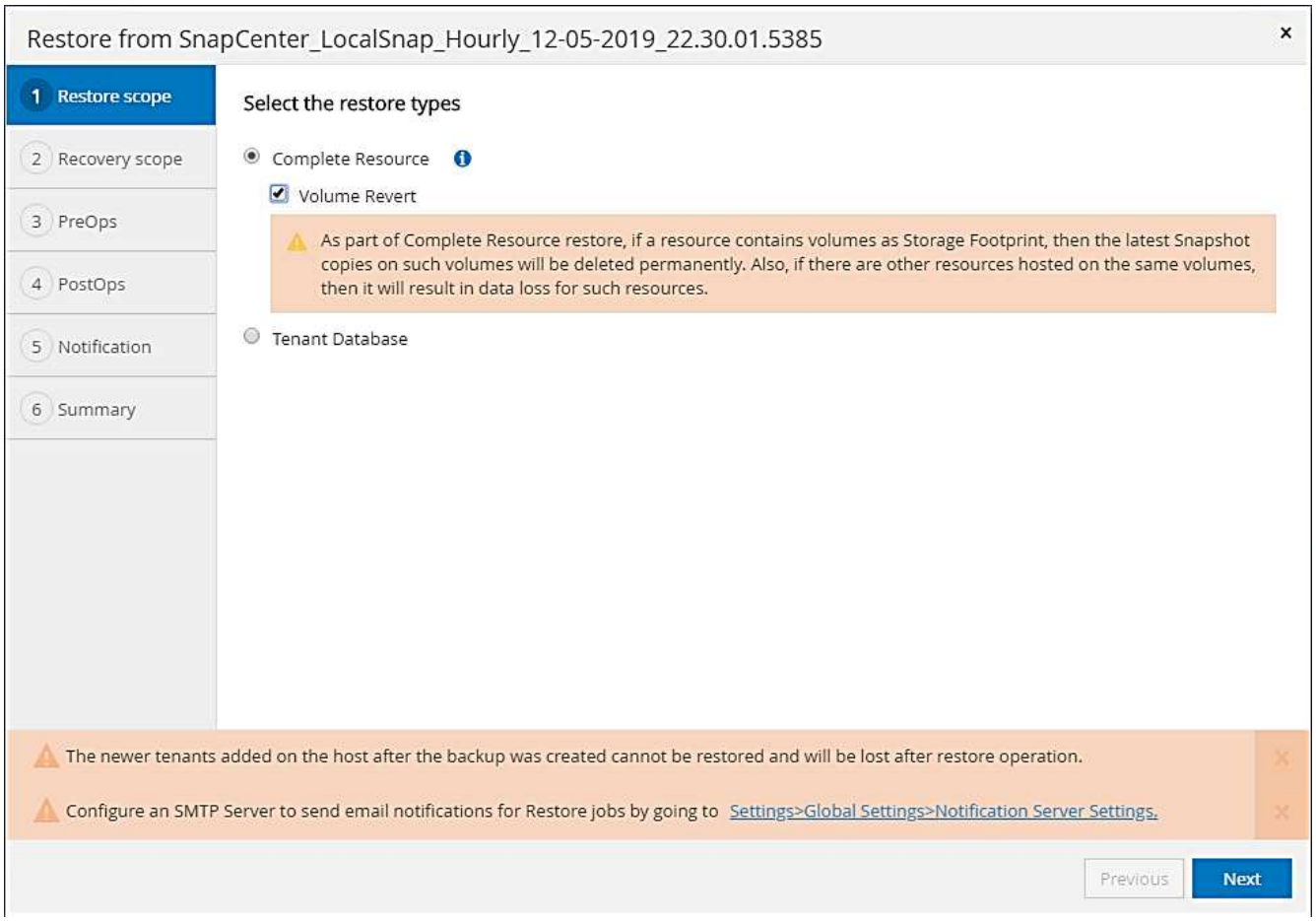


2. Wählen Sie den Umfang und den Typ der Wiederherstellung aus.

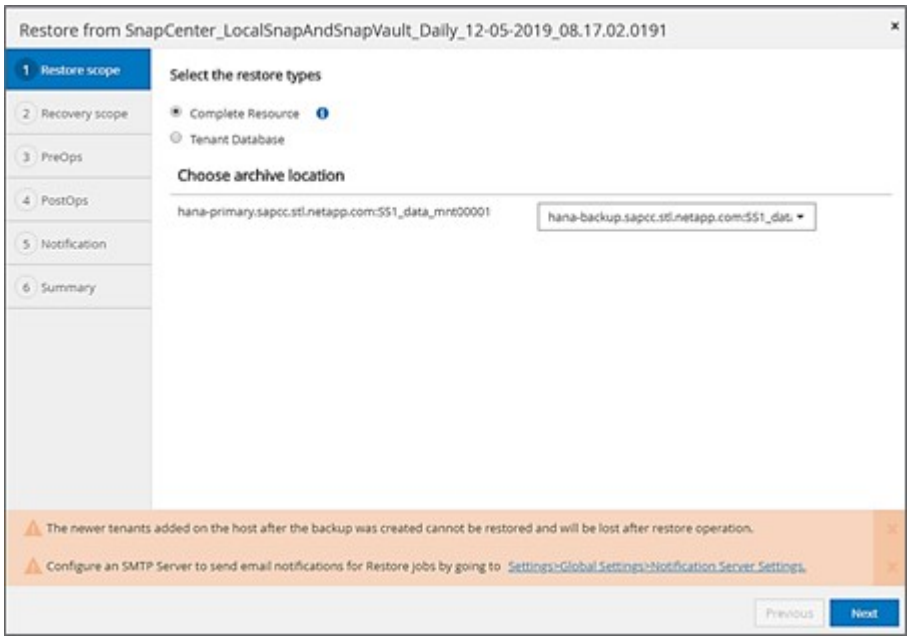
   Die folgenden drei Screenshots zeigen die Restore-Optionen für die Wiederherstellung vom primären Volume mit NFS, die Wiederherstellung vom sekundären mit NFS und die Wiederherstellung vom primären Speicher mit Fibre Channel SAN.

   Die Restore-Optionen für die Wiederherstellung aus dem primären Speicher.

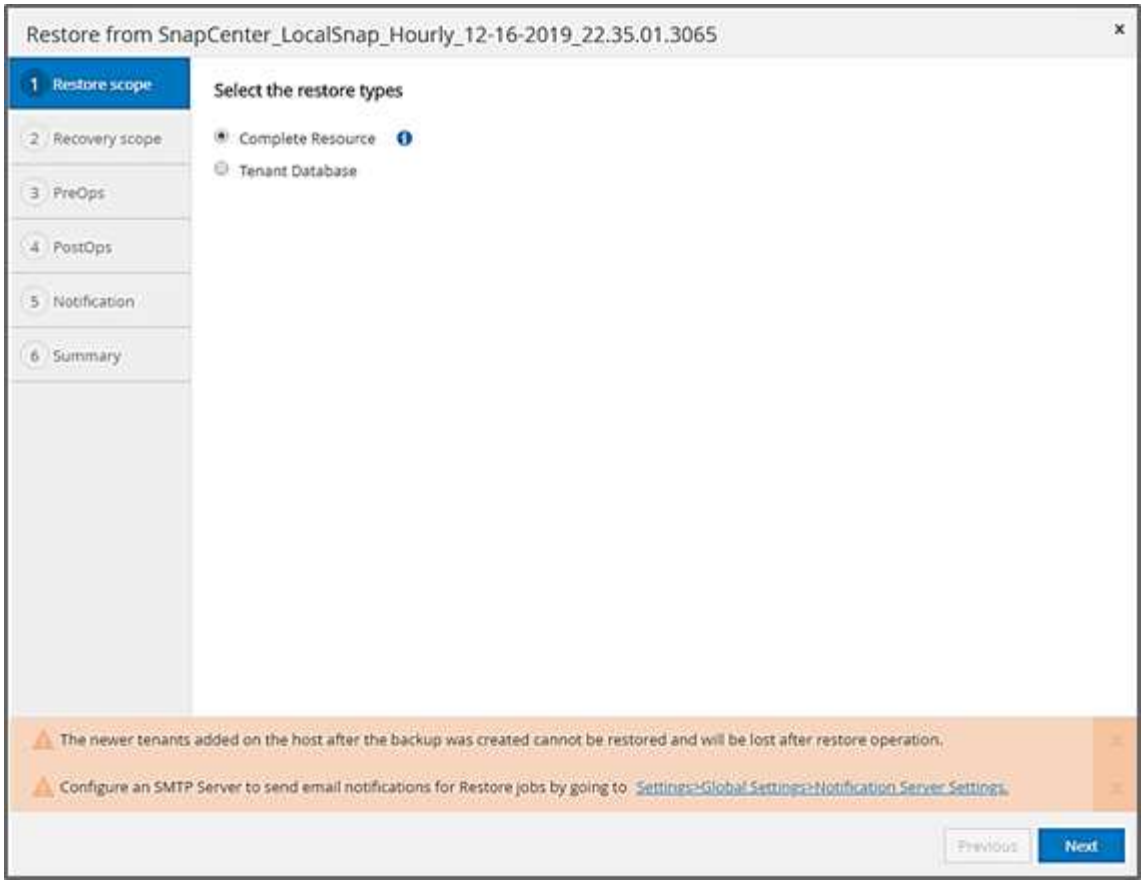
   > Die Option zur Umrüstung von Volumes ist nur für die Wiederherstellung von Vorgängen von Primärquelle mit NFS verfügbar.



Die Wiederherstellungsoptionen für die Wiederherstellung von einem externen Backup-Speicher.

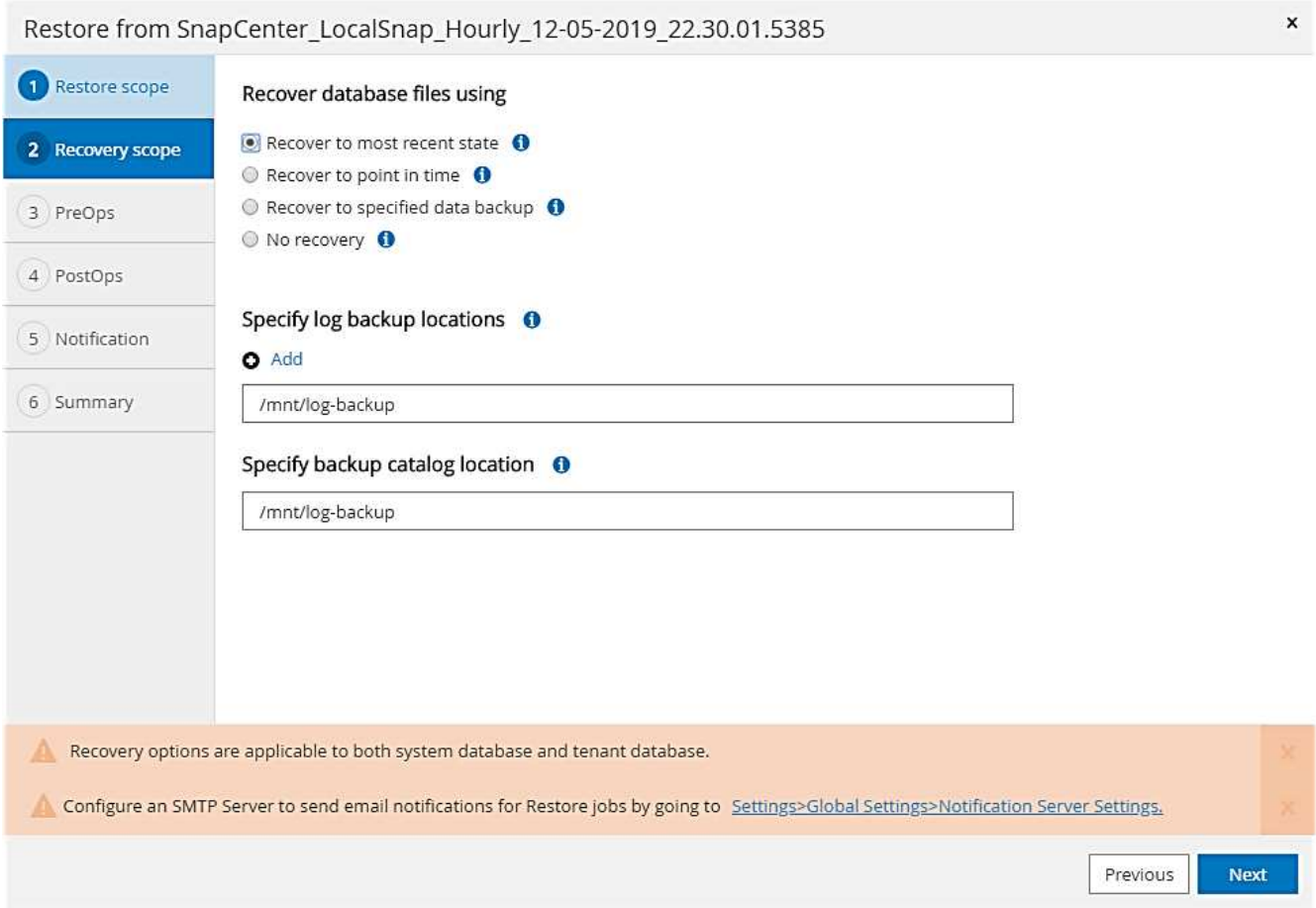


Die Wiederherstellungsoptionen für die Wiederherstellung aus dem primären Speicher mit Fibre Channel SAN.

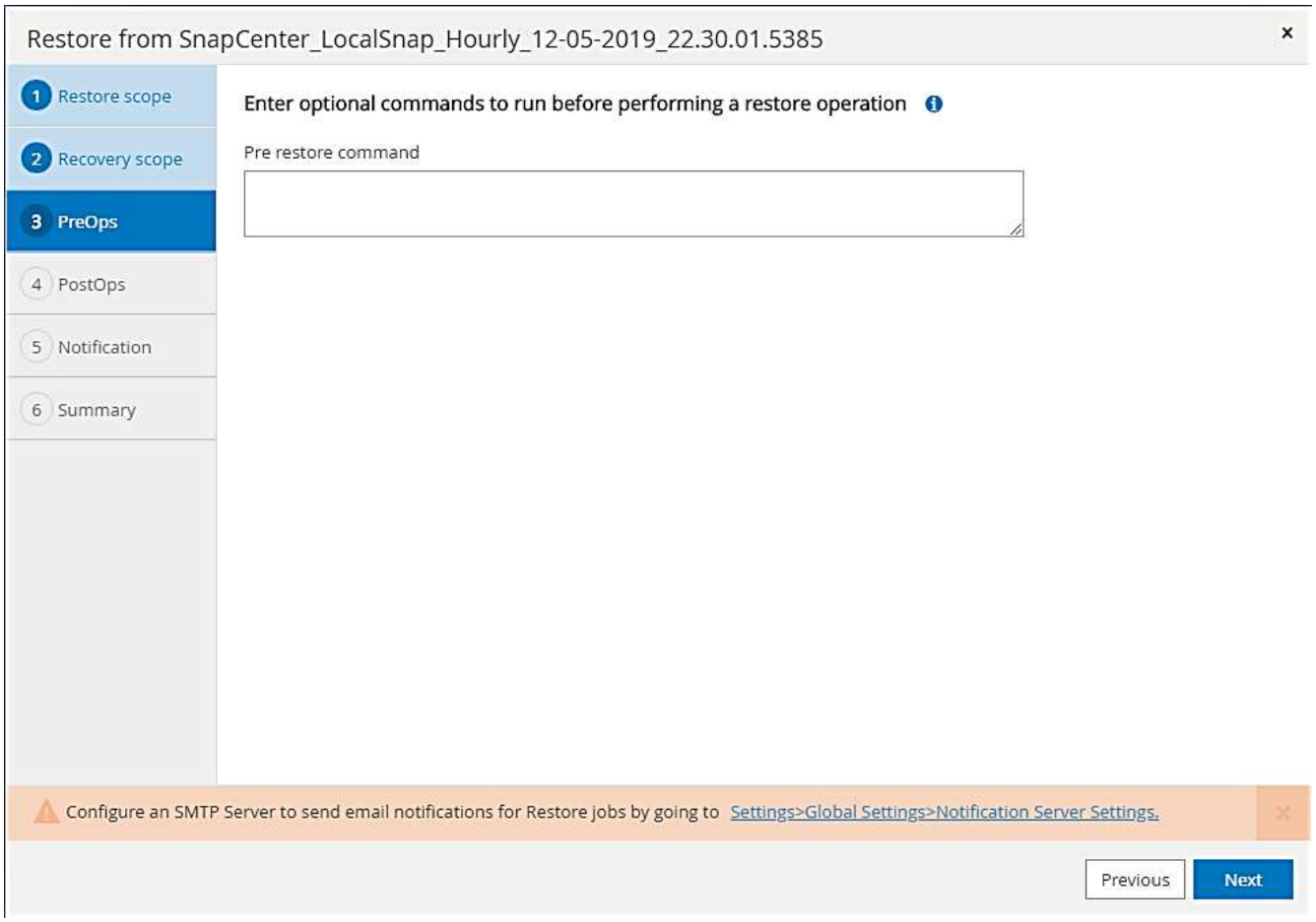


3. Wählen Sie „Recovery Scope“ aus, und stellen Sie den Speicherort für das Backup und das Katalog-Backup bereit.

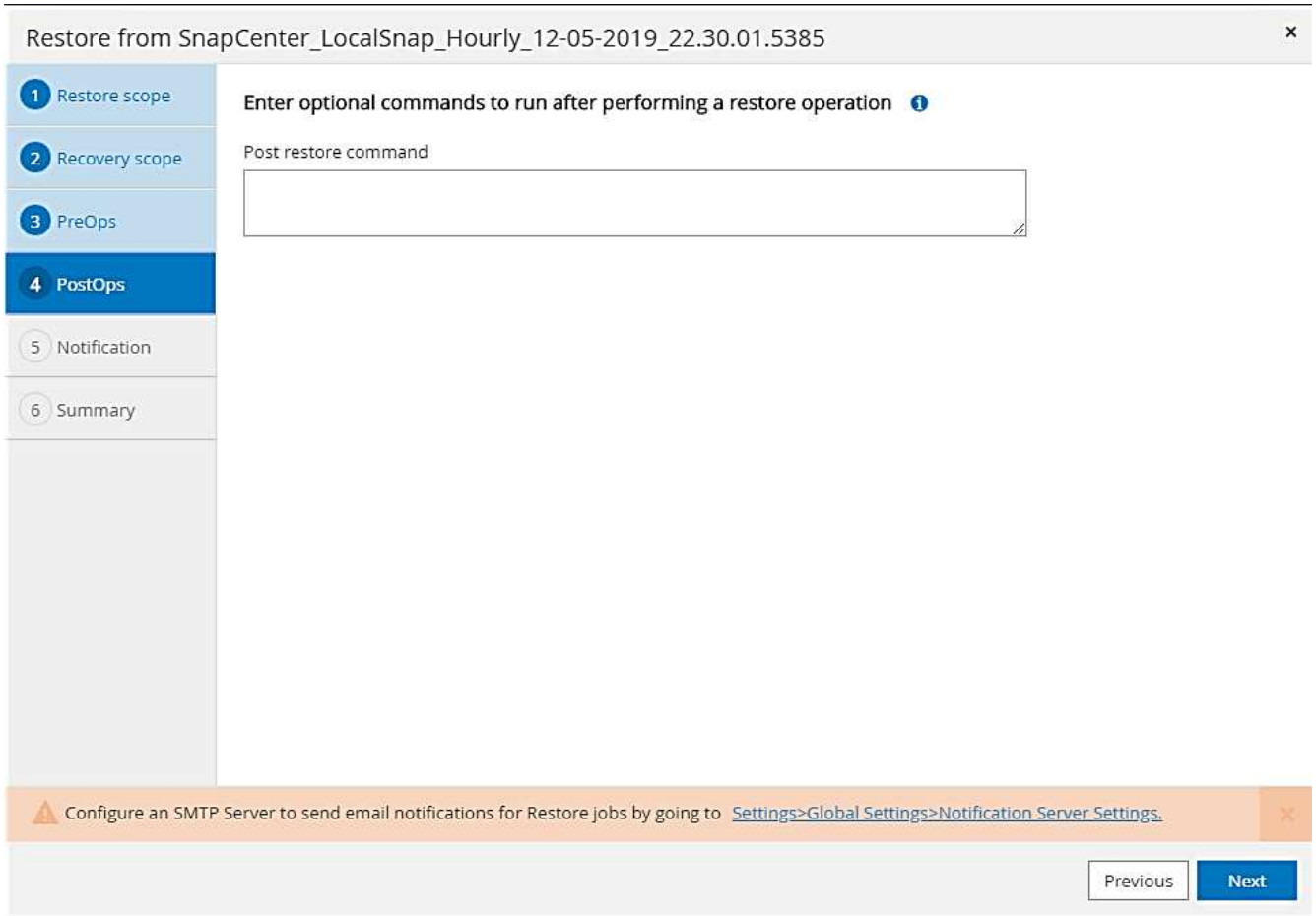
> SnapCenter verwendet den Standardpfad oder die geänderten Pfade in der HANA global.ini-Datei, um die Backup-Standorte für das Protokoll und den Katalog vorab aufzufüllen.



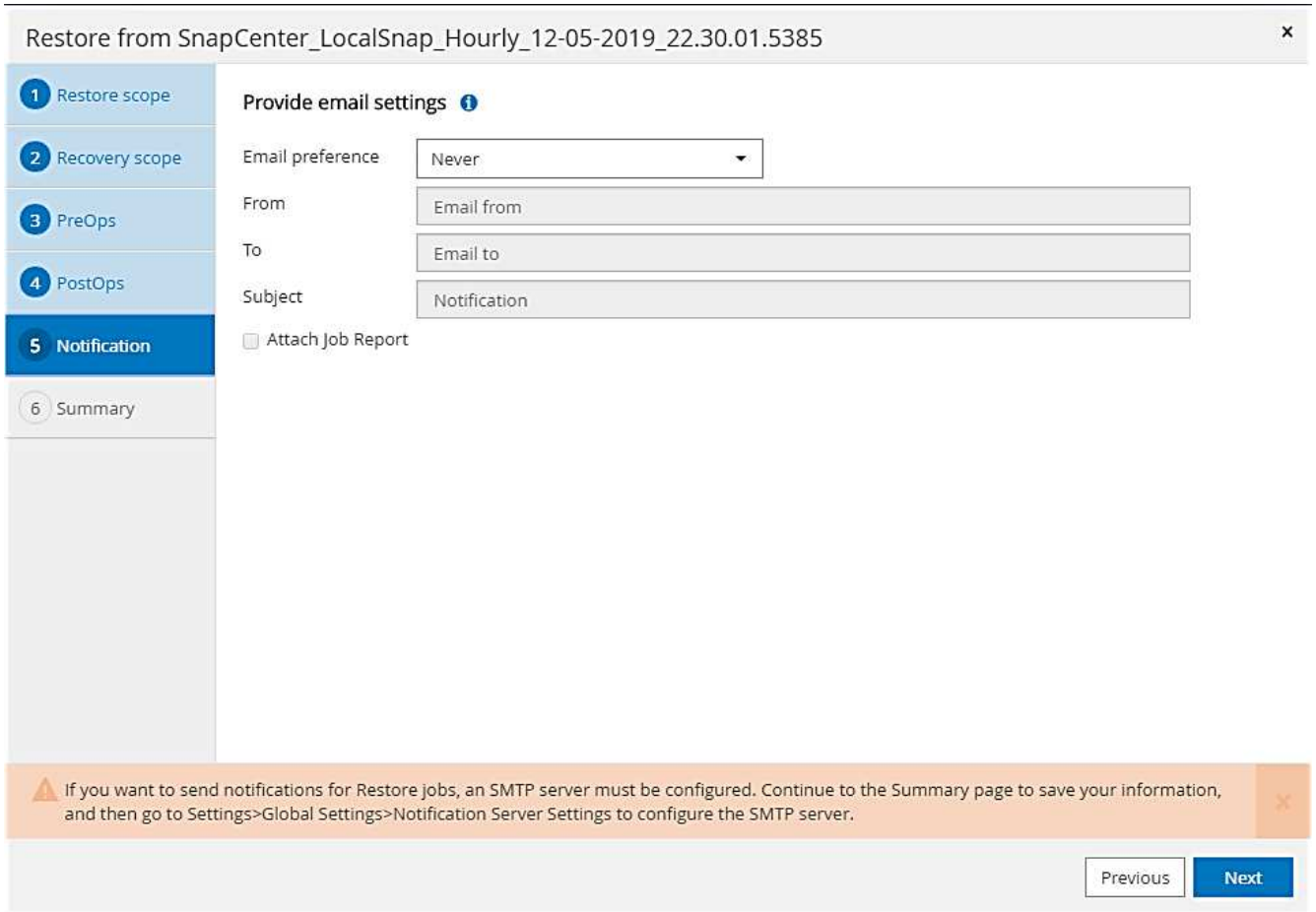
4. Geben Sie die optionalen Befehle zur Vorratspeicher ein.



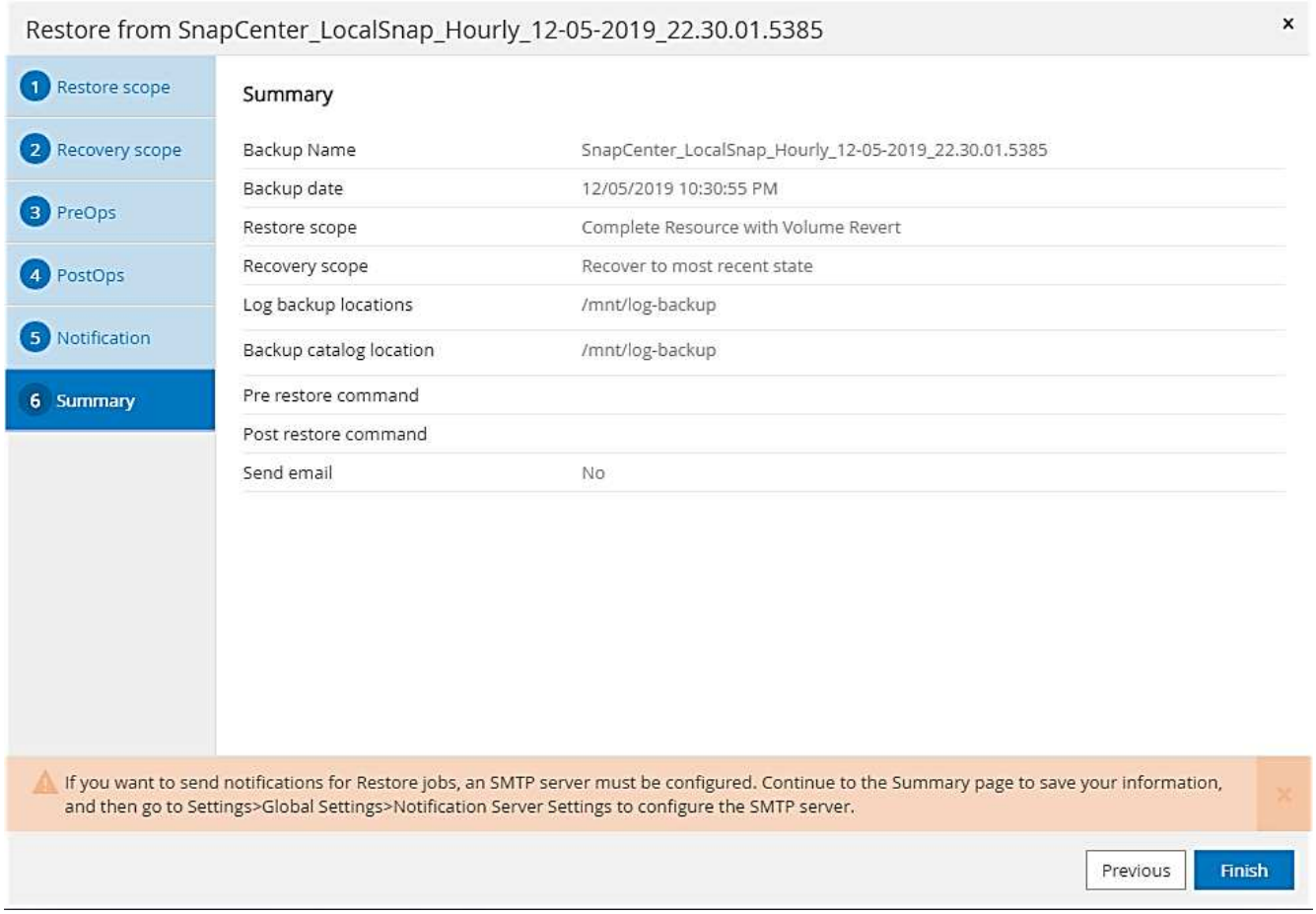
5. Geben Sie die optionalen Befehle nach der Wiederherstellung ein.



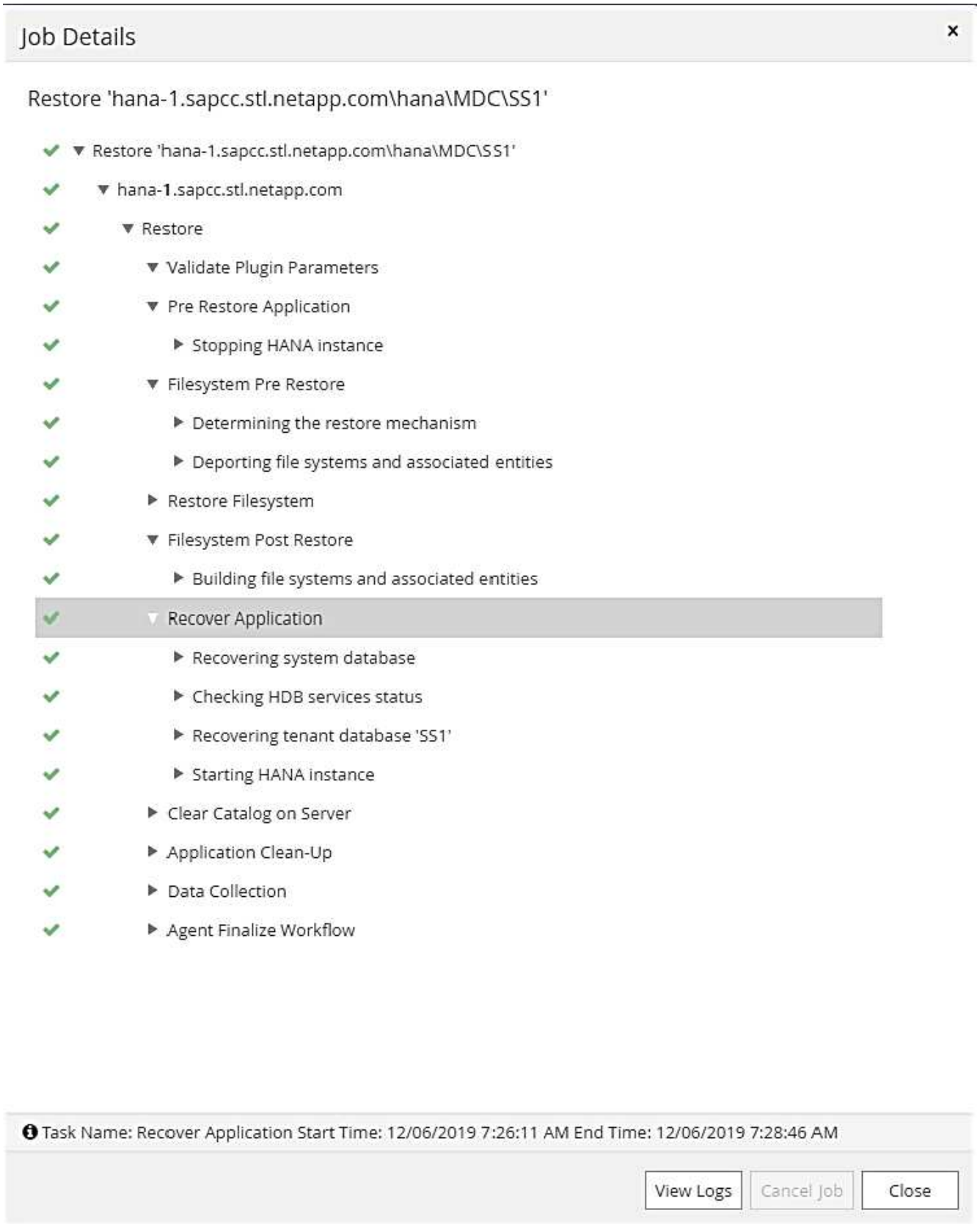
6. Geben Sie die optionalen E-Mail-Einstellungen ein.



7. Um den Wiederherstellungsvorgang zu starten, klicken Sie auf Fertig stellen.



8. SnapCenter führt den Wiederherstellungsvorgang und die Wiederherstellung aus. Dieses Beispiel zeigt die Jobdetails des Wiederherstellungsjobs.



Restore- und Recovery-Vorgang für einzelne Mandanten

Mit SnapCenter 4.3 werden Restore-Vorgänge für einzelne Mandanten für HANA MDC-Systeme mit einem einzelnen Mandanten oder mit mehreren Mandanten, die von SnapCenter automatisch erkannt wurden, unterstützt.

Sie können eine Restore- und Recovery-Operation mit nur einem Mandanten durchführen:

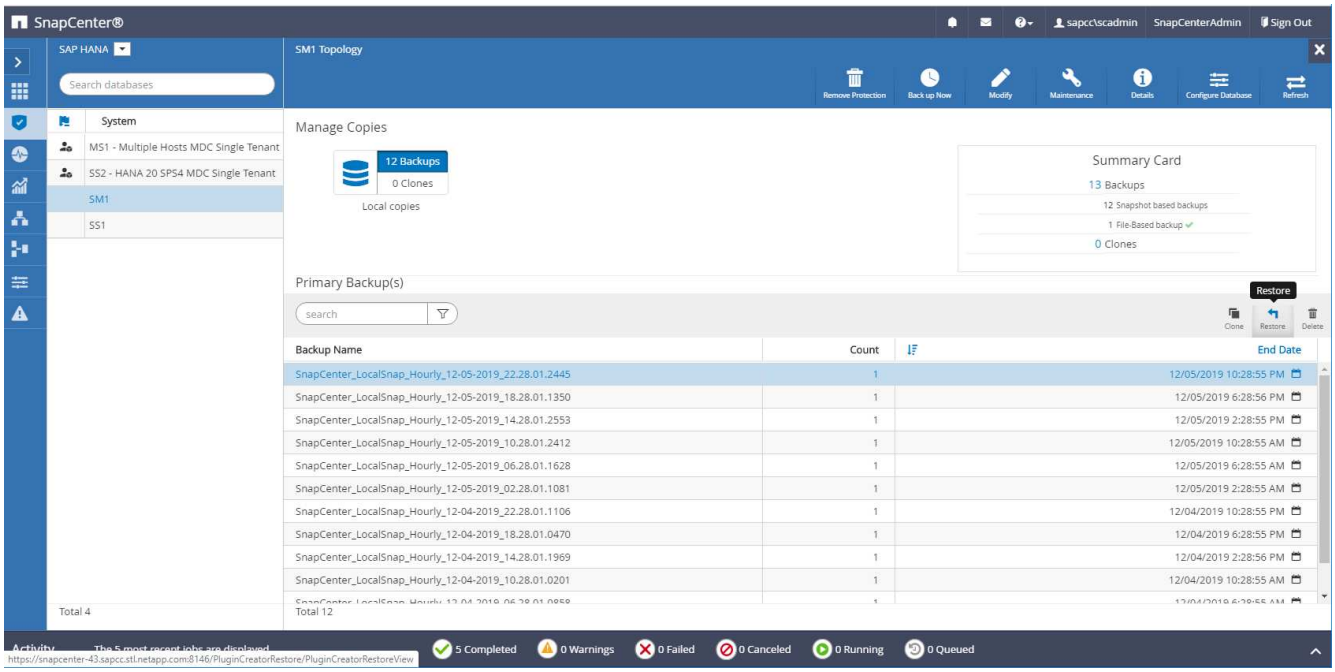
1. Stoppen Sie den Mieter wiederhergestellt werden.
2. Stellen Sie den Mandanten mit SnapCenter wieder her.
   - Bei einer Wiederherstellung vom primären Speicher führt SnapCenter folgende Operationen aus:
     - **NFS.** Speicher einzelne Datei SnapRestore Operationen für alle Dateien der Mandanten-Datenbank.
     - **SAN.** Klonen und verbinden Sie die LUN mit dem Datenbank-Host und kopieren Sie alle Dateien der Mandanten-Datenbank.
   - Bei einer Wiederherstellung vom sekundären Storage führt SnapCenter folgende Operationen aus:
     - **NFS.** Speicher-SnapVault Wiederherstellen von Vorgängen für alle Dateien der Mandanten-Datenbank
     - **SAN.** Klonen und verbinden Sie die LUN mit dem Datenbank-Host und kopieren Sie alle Dateien der Mandanten-Datenbank
3. Stellen Sie den Mandanten mit HANA Studio, Cockpit oder SQL-Anweisung wieder her.

Dieser Abschnitt enthält die Schritte für den Restore- und Recovery-Vorgang vom primären Storage des automatisch erkannten HANA-Systems SM1 (SAP HANA Single-Host, MDC Multiple-Tenant-System via NFS). Aus Benutzereingangsperspektive sind die Workflows bei Restores aus sekundärem oder bei einer Wiederherstellung in einem Fibre Channel SAN-Setup identisch.

1. Beenden Sie die Mandantendatenbank.

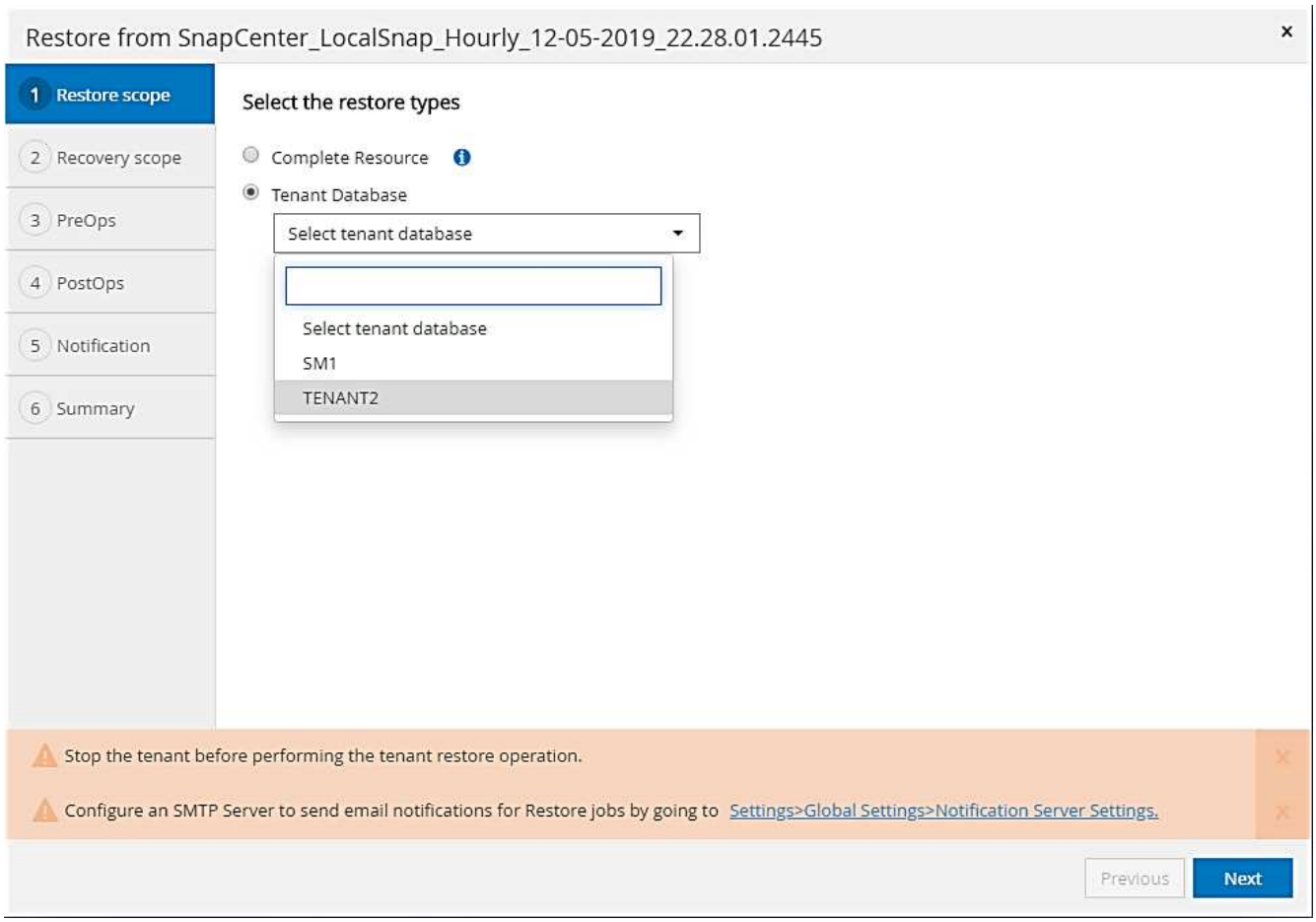
```
sm1adm@hana-2:/usr/sap/SM1/HDB00> hdbsql -U SYSKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql=>
hdbsql SYSTEMDB=> alter system stop database tenant2;
0 rows affected (overall time 14.215281 sec; server time 14.212629 sec)
hdbsql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

2. Wählen Sie ein Backup in SnapCenter aus, das für den Wiederherstellungsvorgang verwendet werden soll.



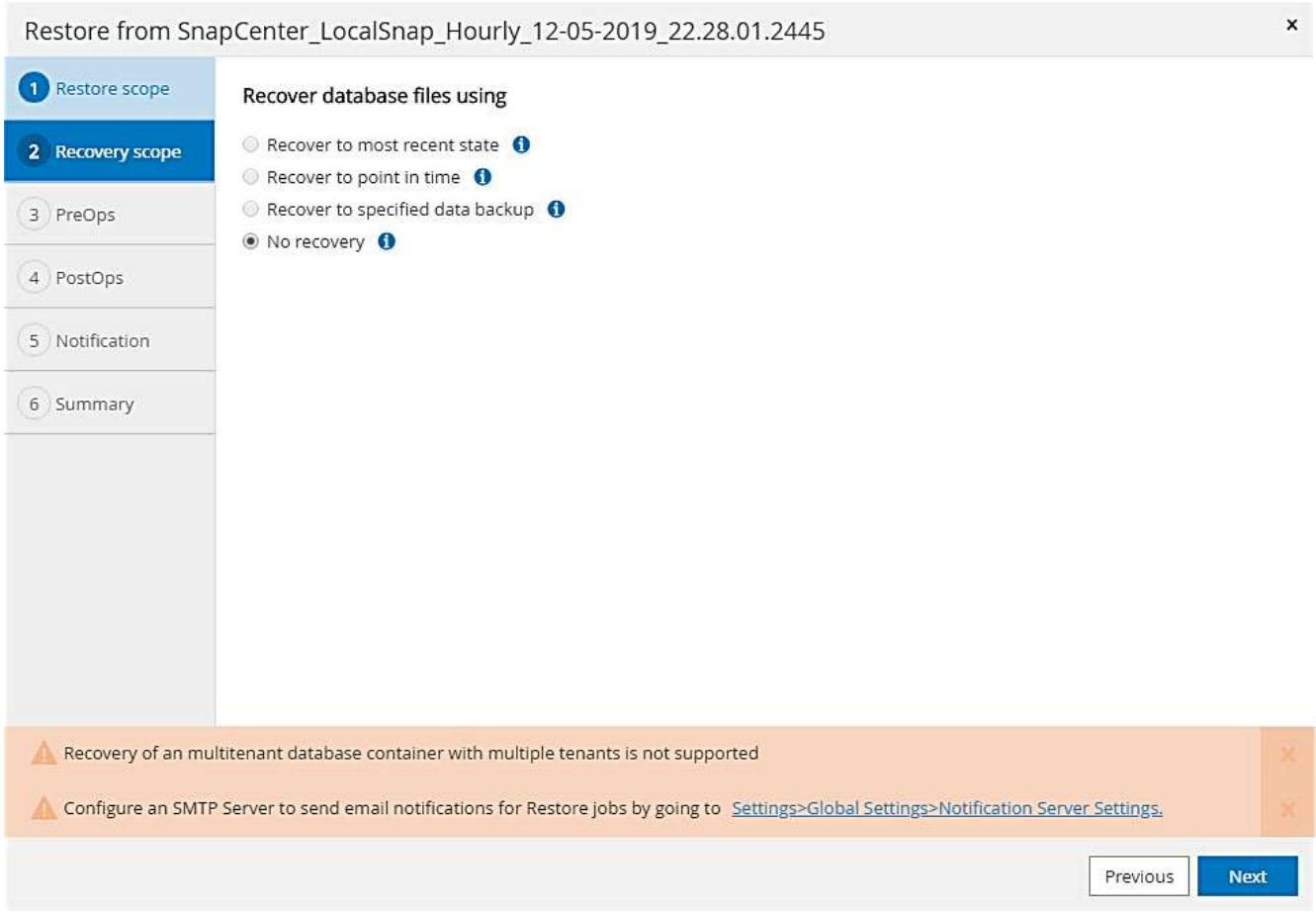
3. Wählen Sie den wiederherzustellenden Mandanten aus.

> SnapCenter zeigt eine Liste aller Mandanten an, die im ausgewählten Backup enthalten sind.

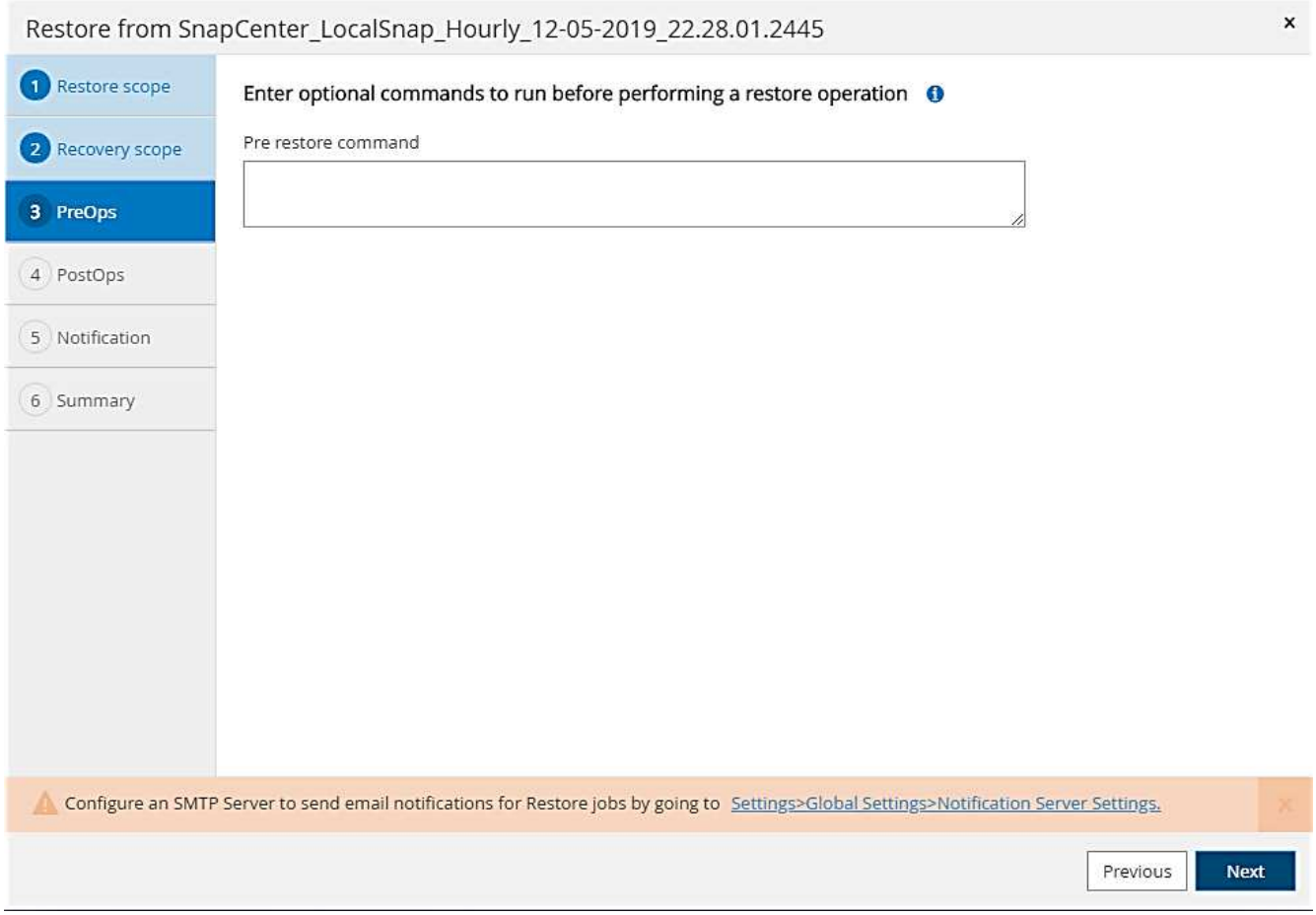


Die Recovery einzelner Mandanten wird mit SnapCenter 4.3 nicht unterstützt. Keine Wiederherstellung ist

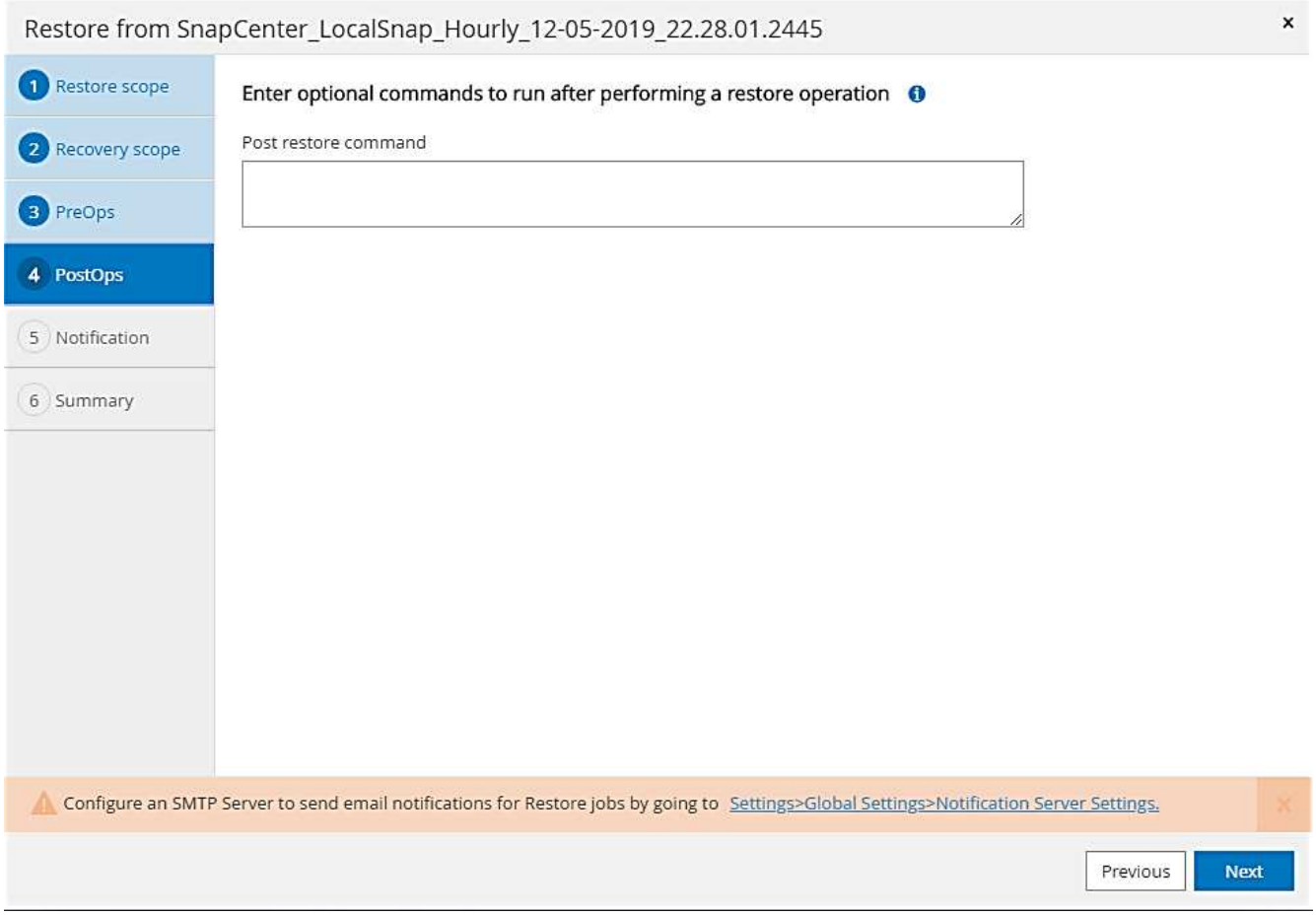
vorausgewählt und kann nicht geändert werden.



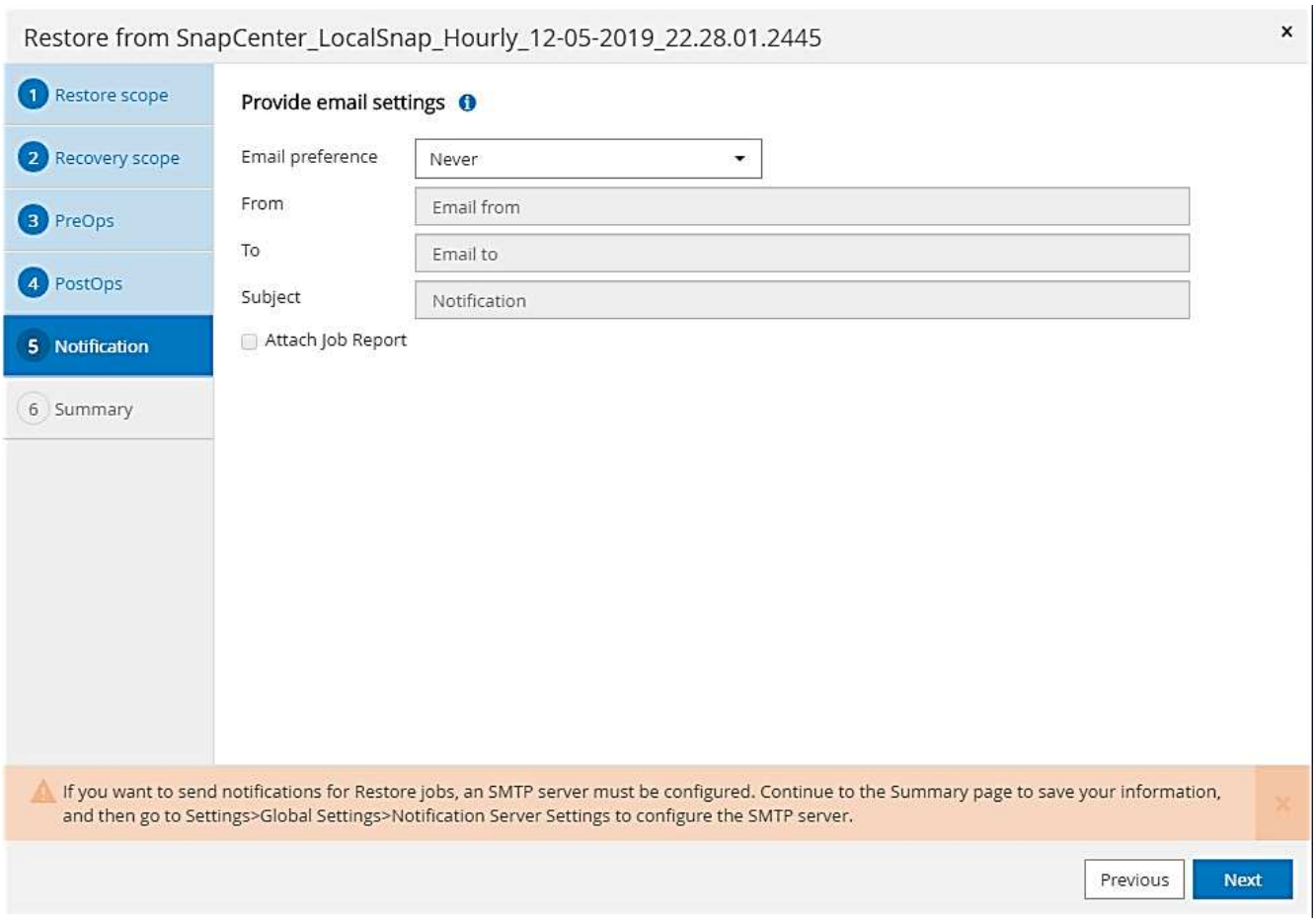
4. Geben Sie die optionalen Befehle zur Vorratspeicher ein.



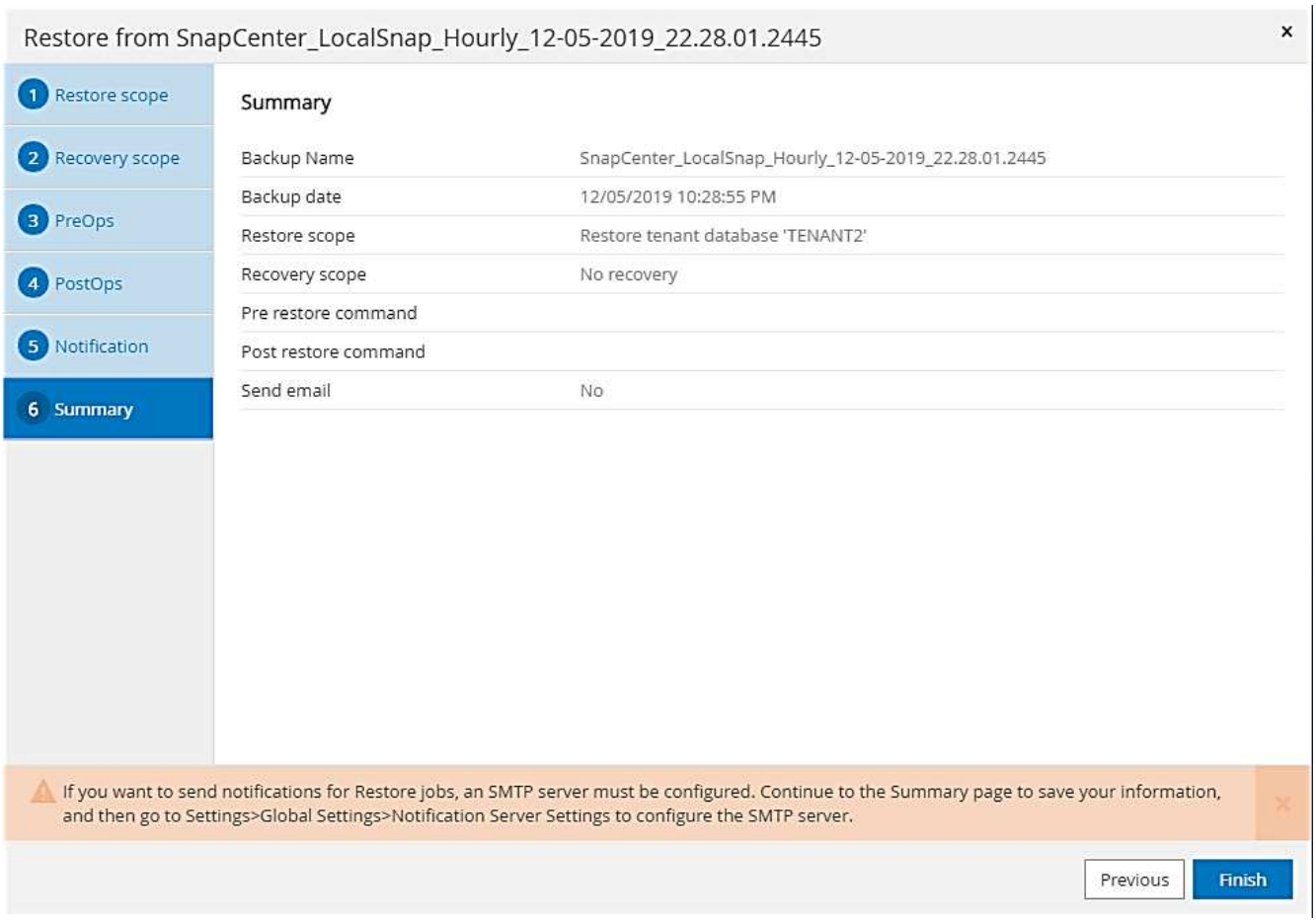
5. Geben Sie optionale Befehle nach der Wiederherstellung ein.



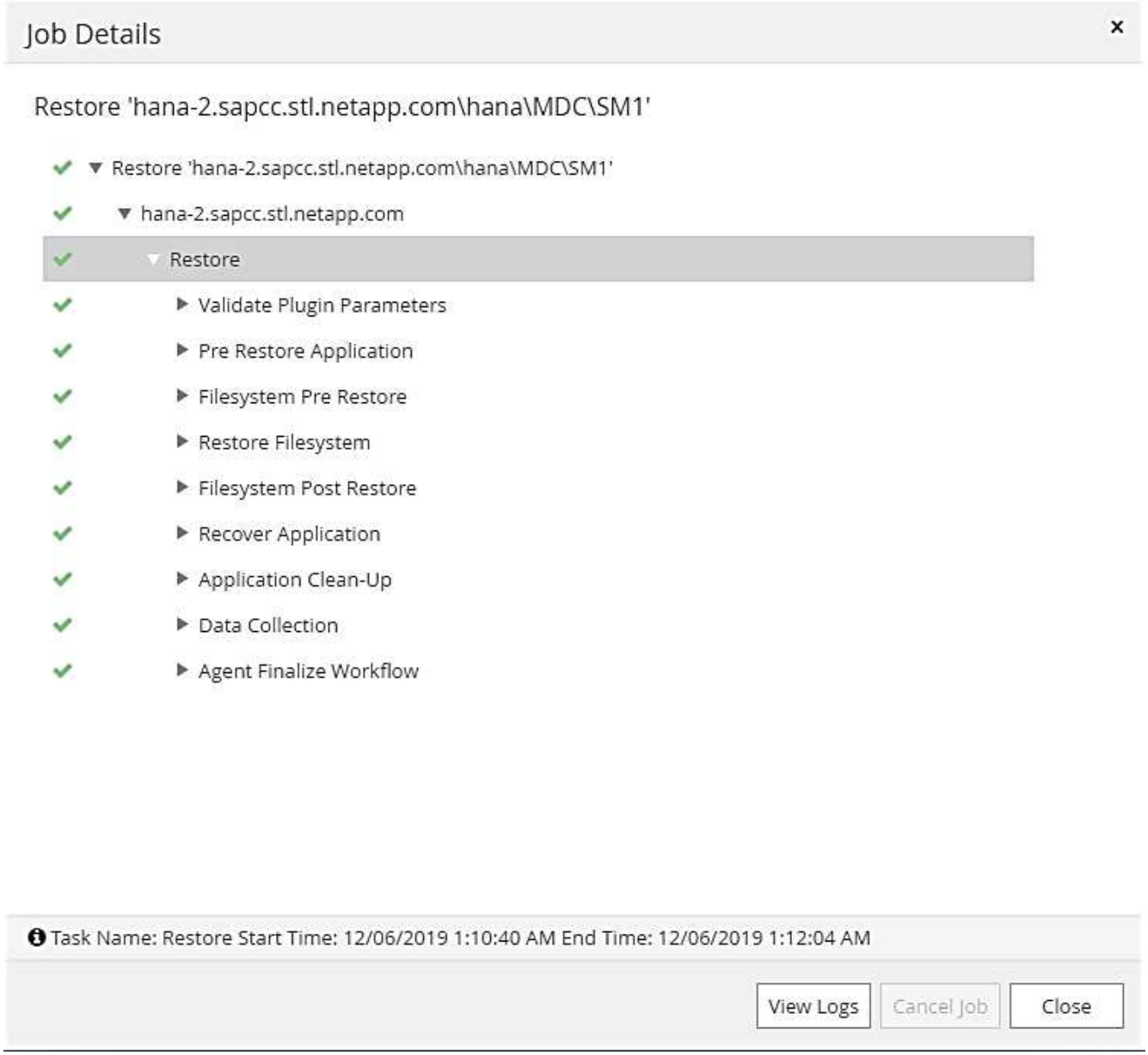
6. Geben Sie die optionalen E-Mail-Einstellungen ein.



7. Um den Wiederherstellungsvorgang zu starten, klicken Sie auf Fertig stellen.



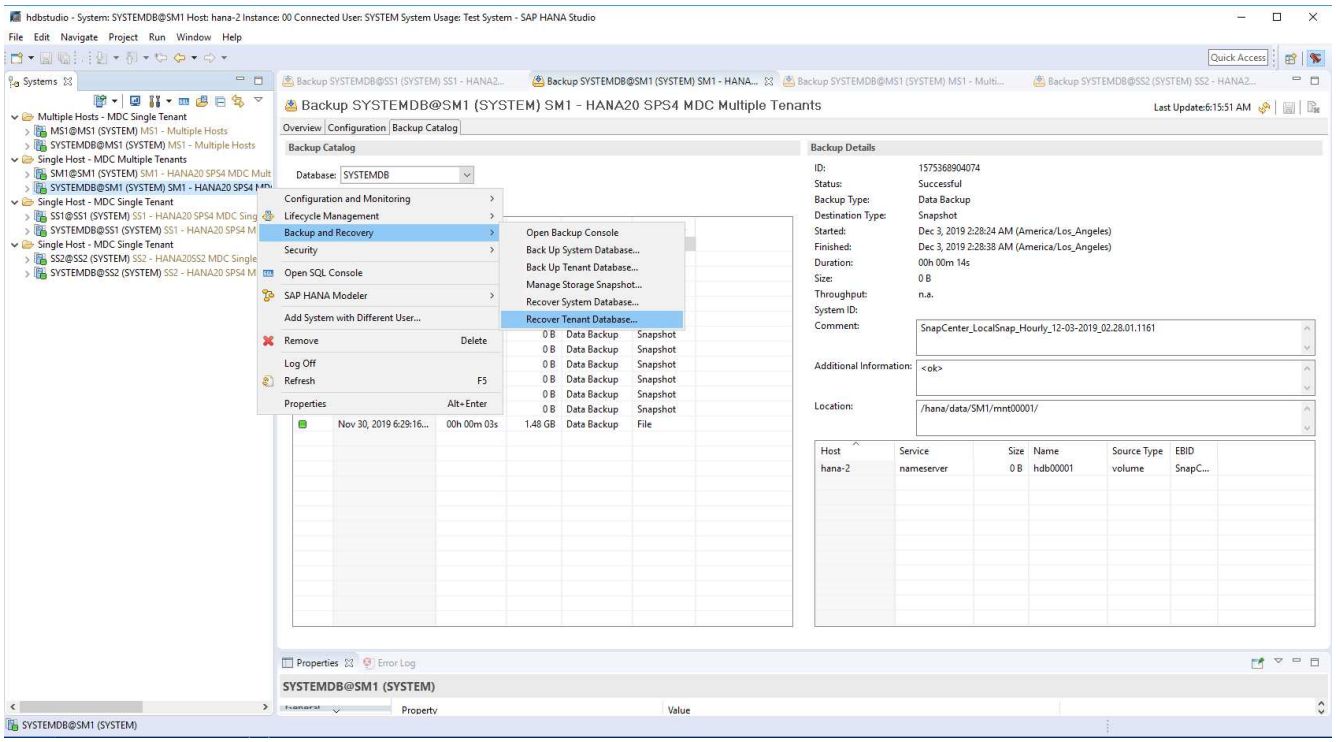
Der Wiederherstellungsvorgang wird von SnapCenter ausgeführt. Dieses Beispiel zeigt die Jobdetails des Wiederherstellungsjobs.



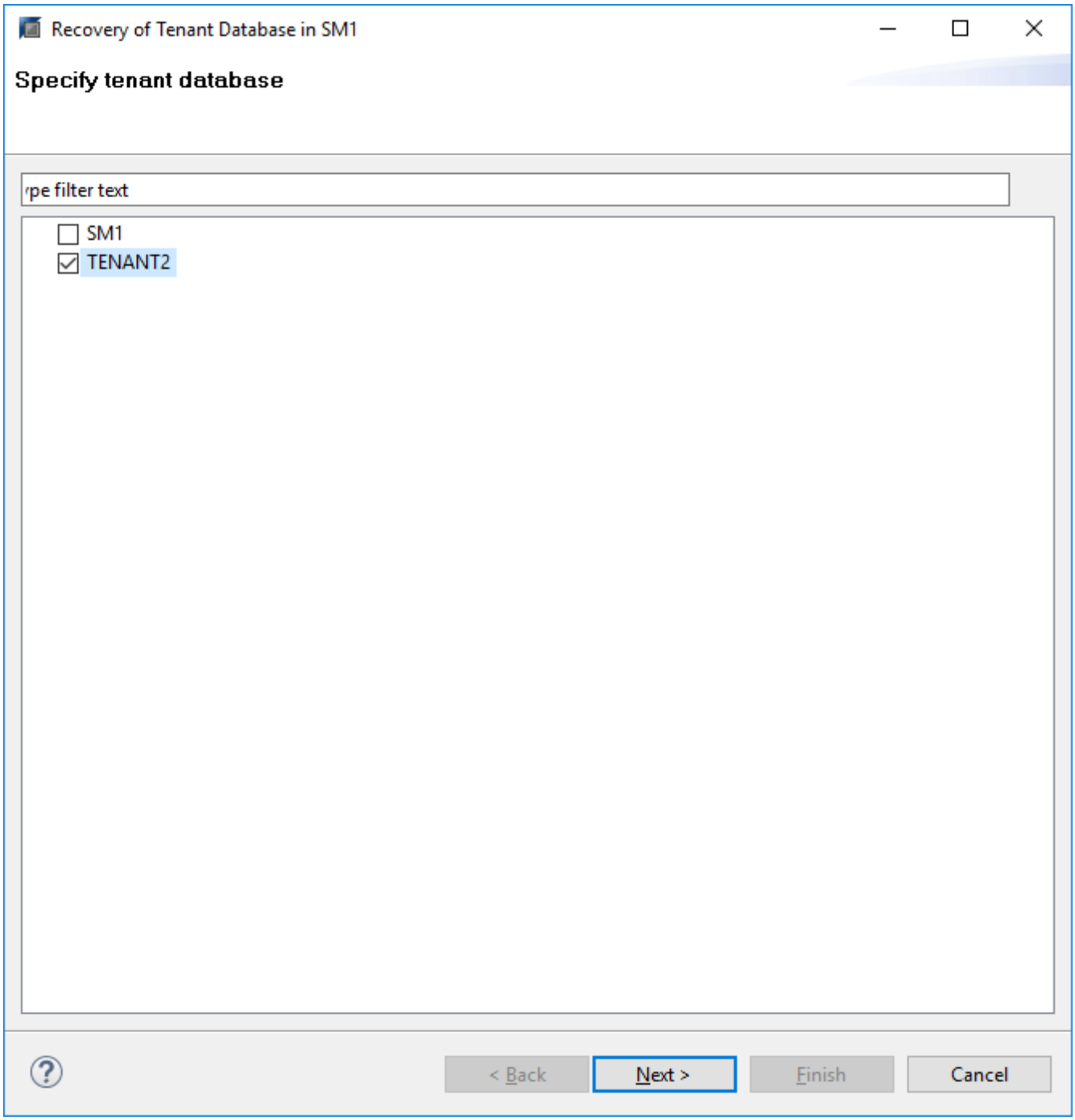
Nach Abschluss der Mandantenwiederherstellung werden nur die mandantenrelevanten Daten wiederhergestellt. Auf dem Filesystem des HANA-Datenbank-Hosts sind die wiederhergestellte Datendatei und die Snapshot Backup ID-Datei des Mandanten verfügbar.

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

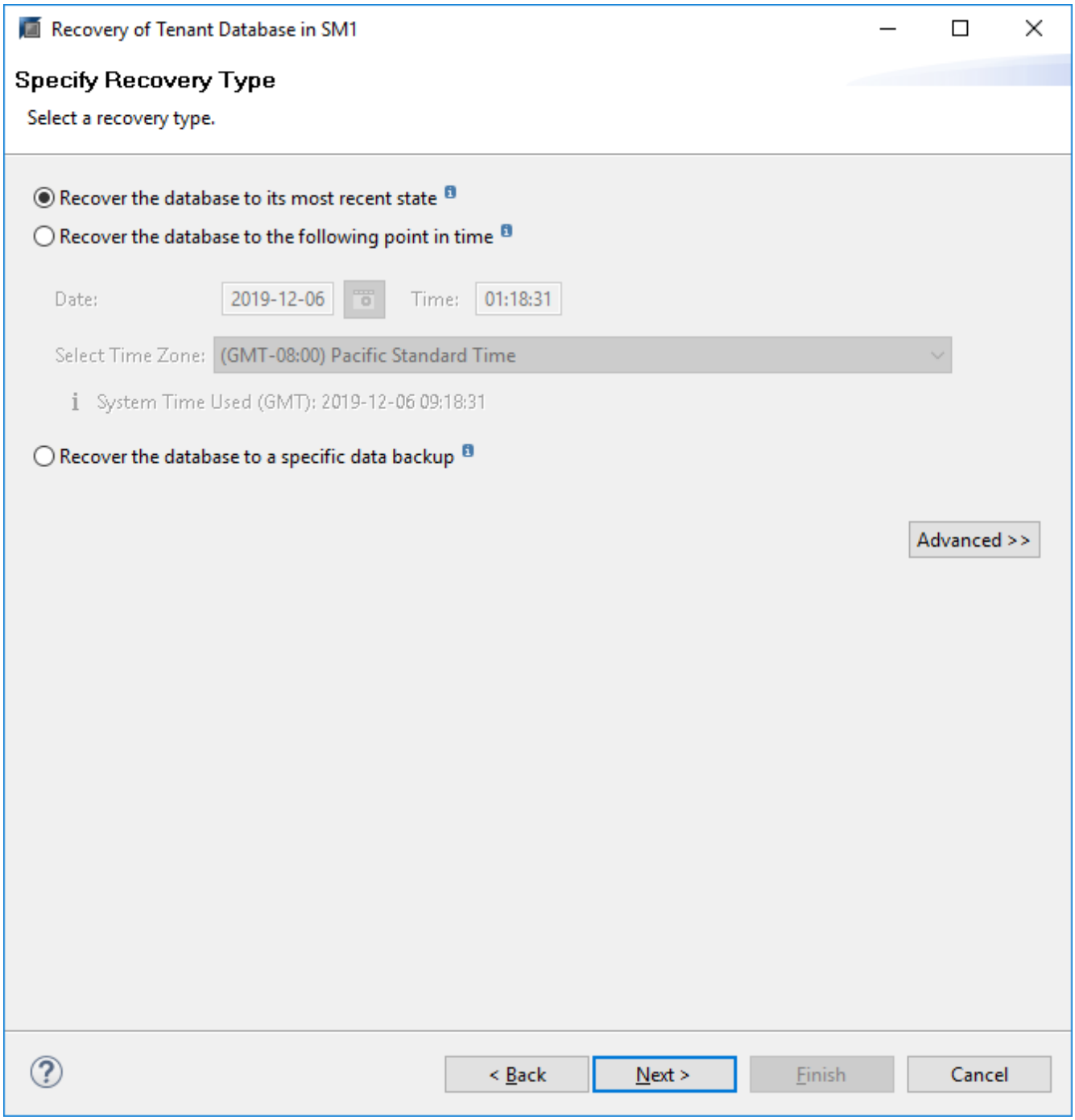
8. Starten Sie die Recovery mit HANA Studio.



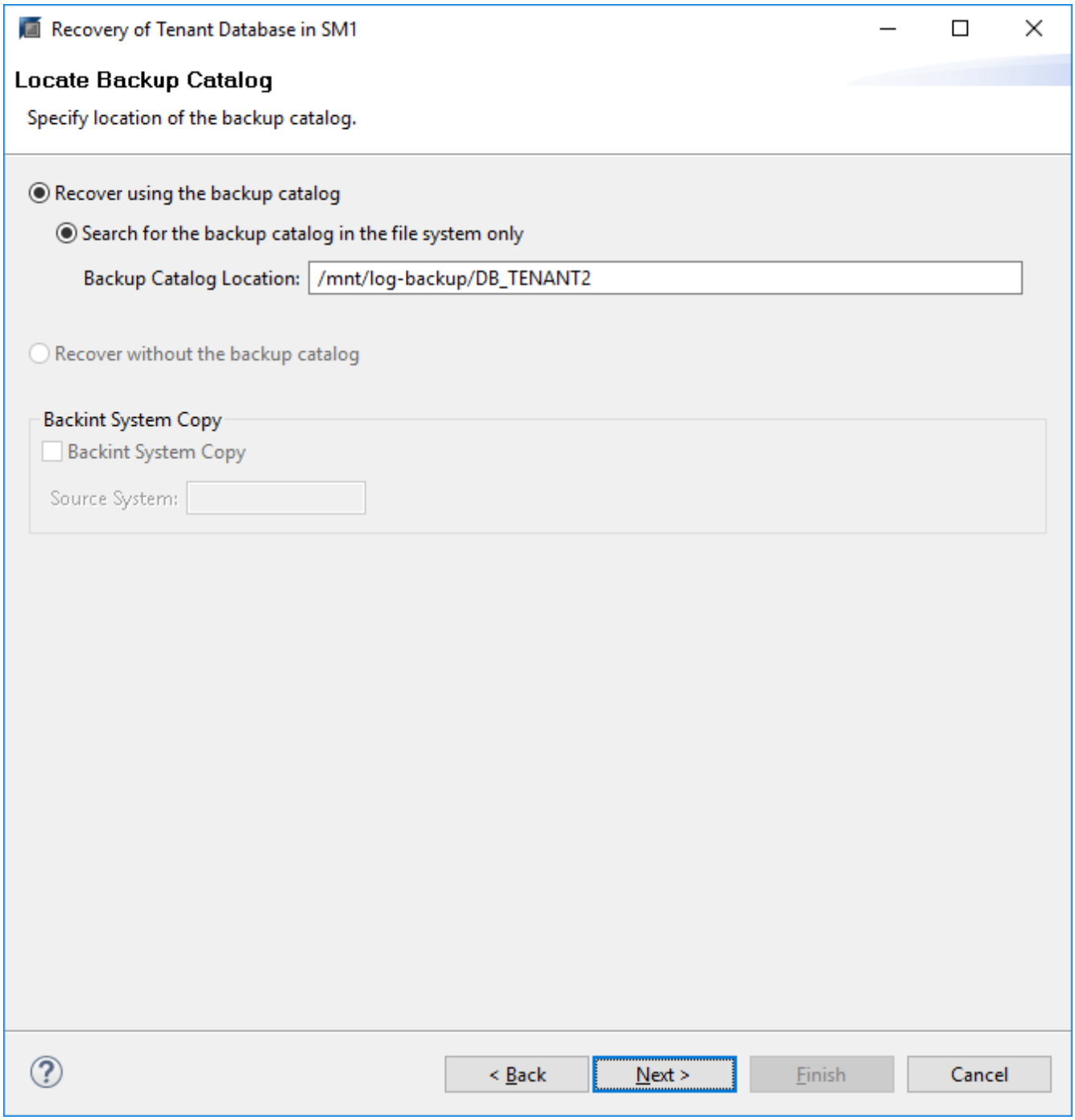
9. Wählen Sie den Mandanten aus.

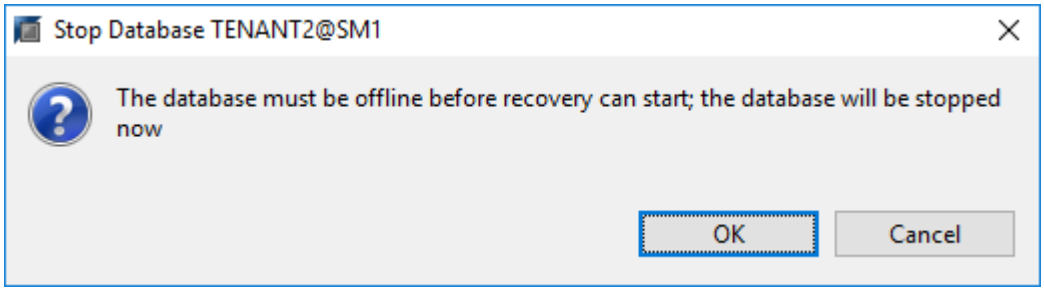


10. Wählen Sie den Wiederherstellungstyp aus.



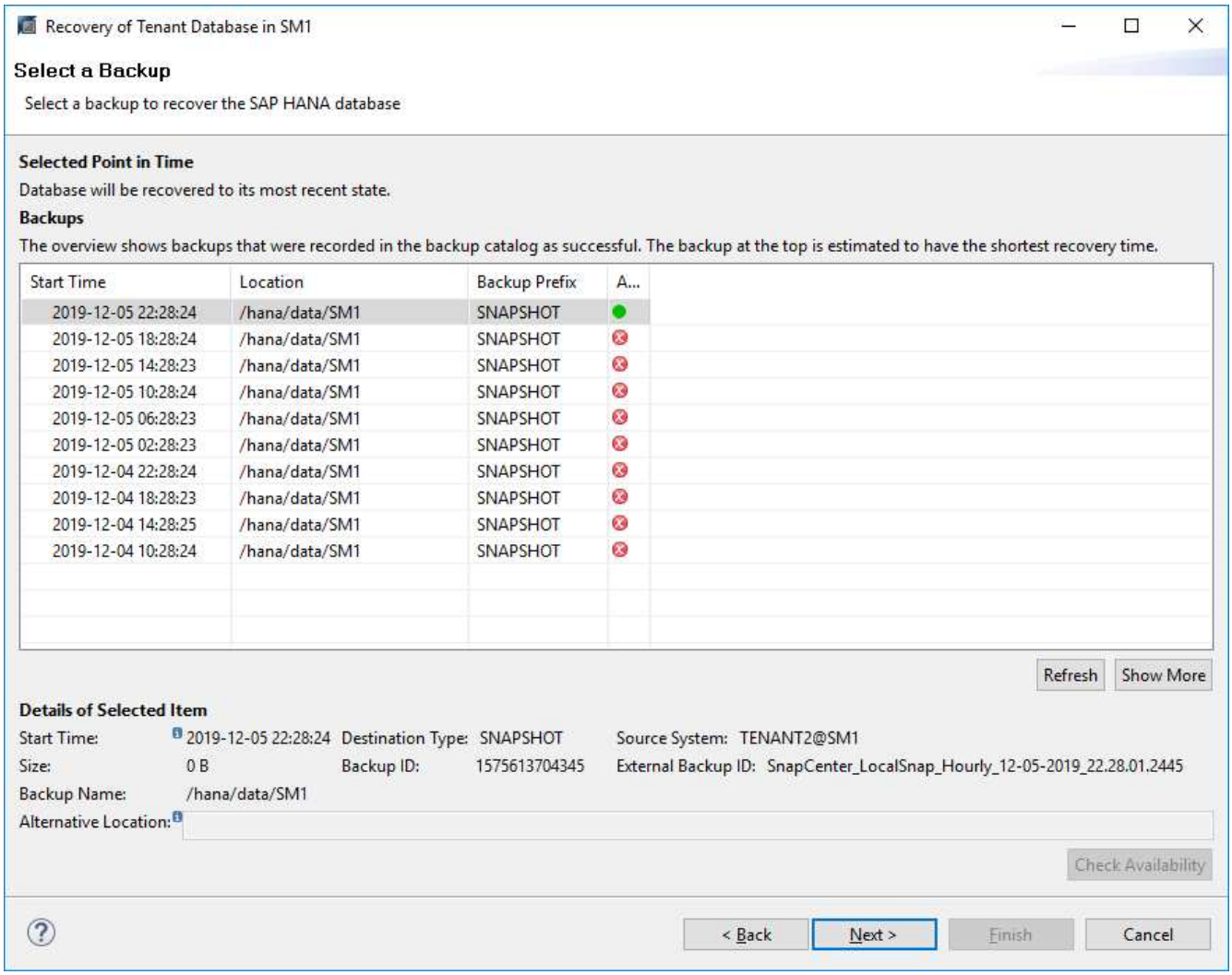
11. Stellen Sie den Speicherort des Backup-Katalogs bereit.



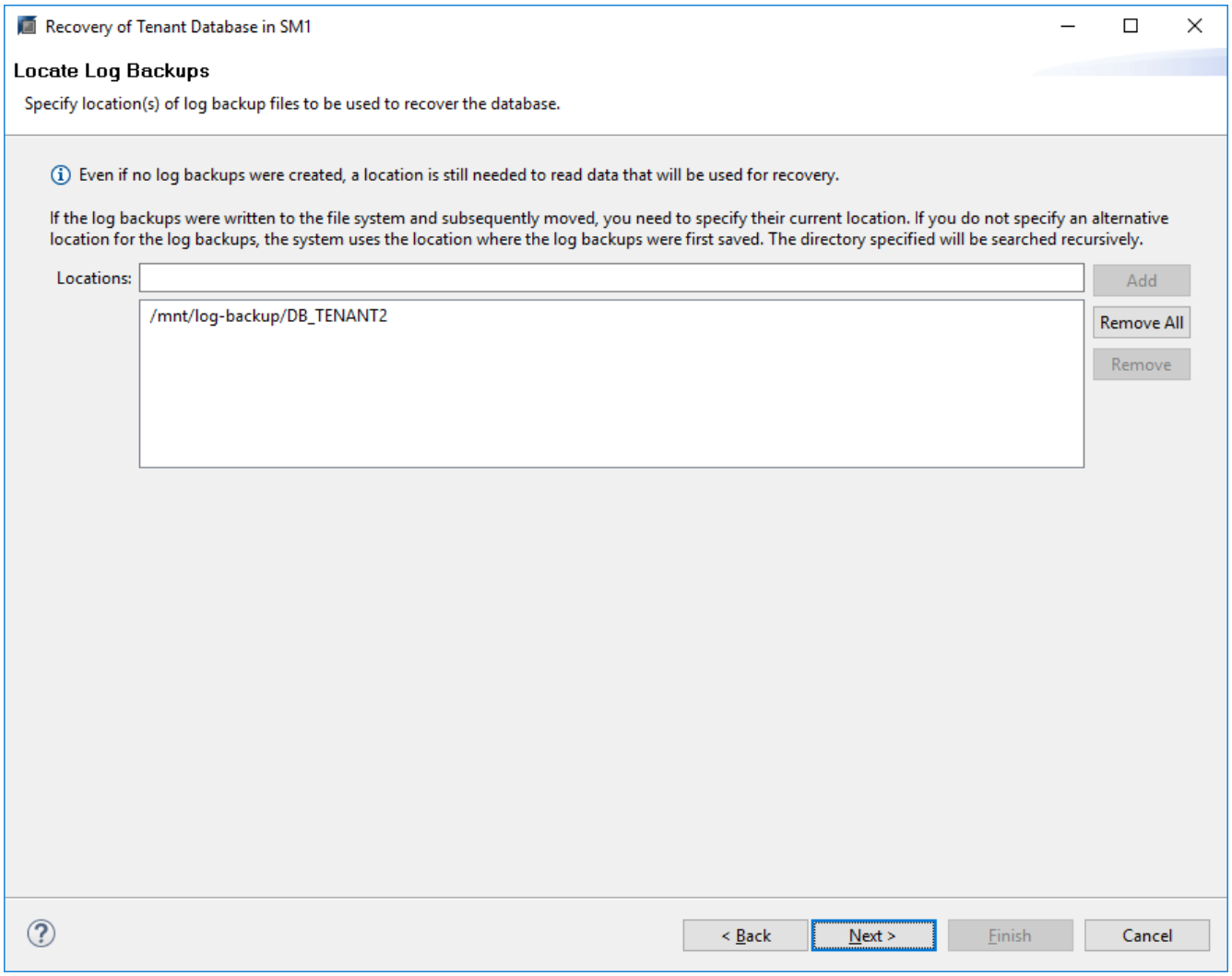


Im Backup-Katalog wird das wiederhergestellte Backup mit einem grünen Symbol hervorgehoben. Die externe Backup-ID zeigt den Backup-Namen an, der zuvor in SnapCenter ausgewählt wurde.

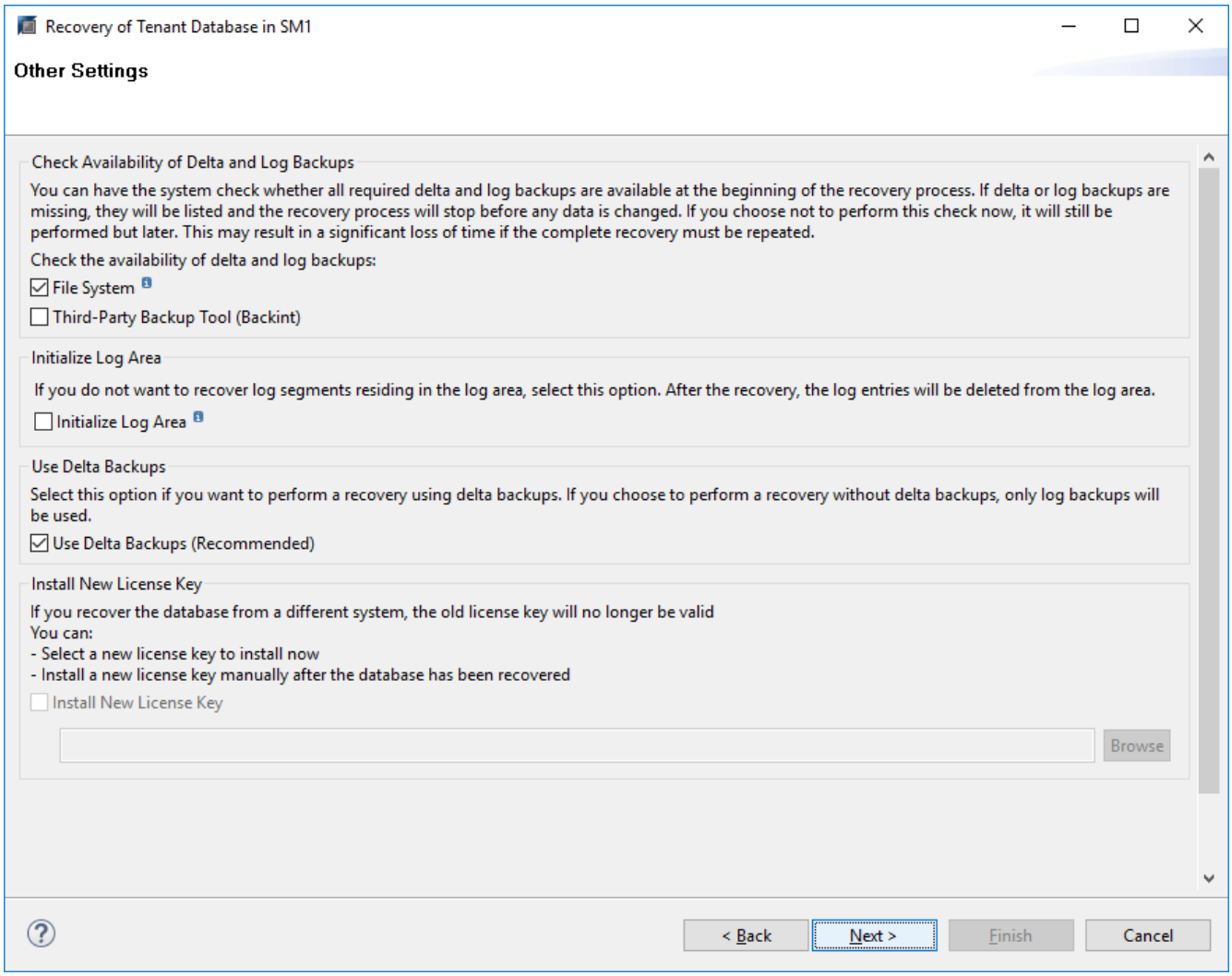
12. Wählen Sie den Eintrag mit dem grünen Symbol aus, und klicken Sie auf Weiter.



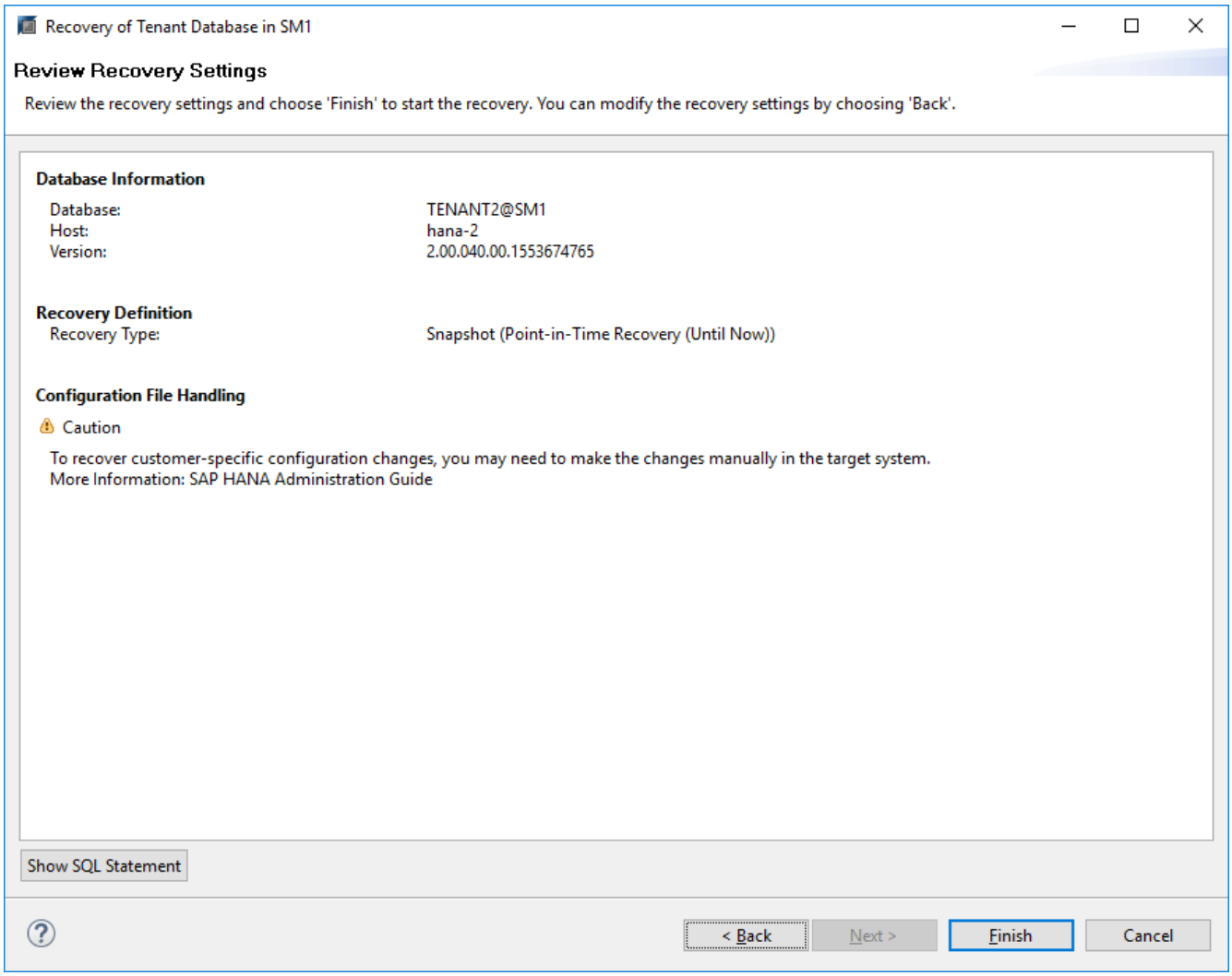
13. Geben Sie den Backup-Speicherort für das Protokoll an.

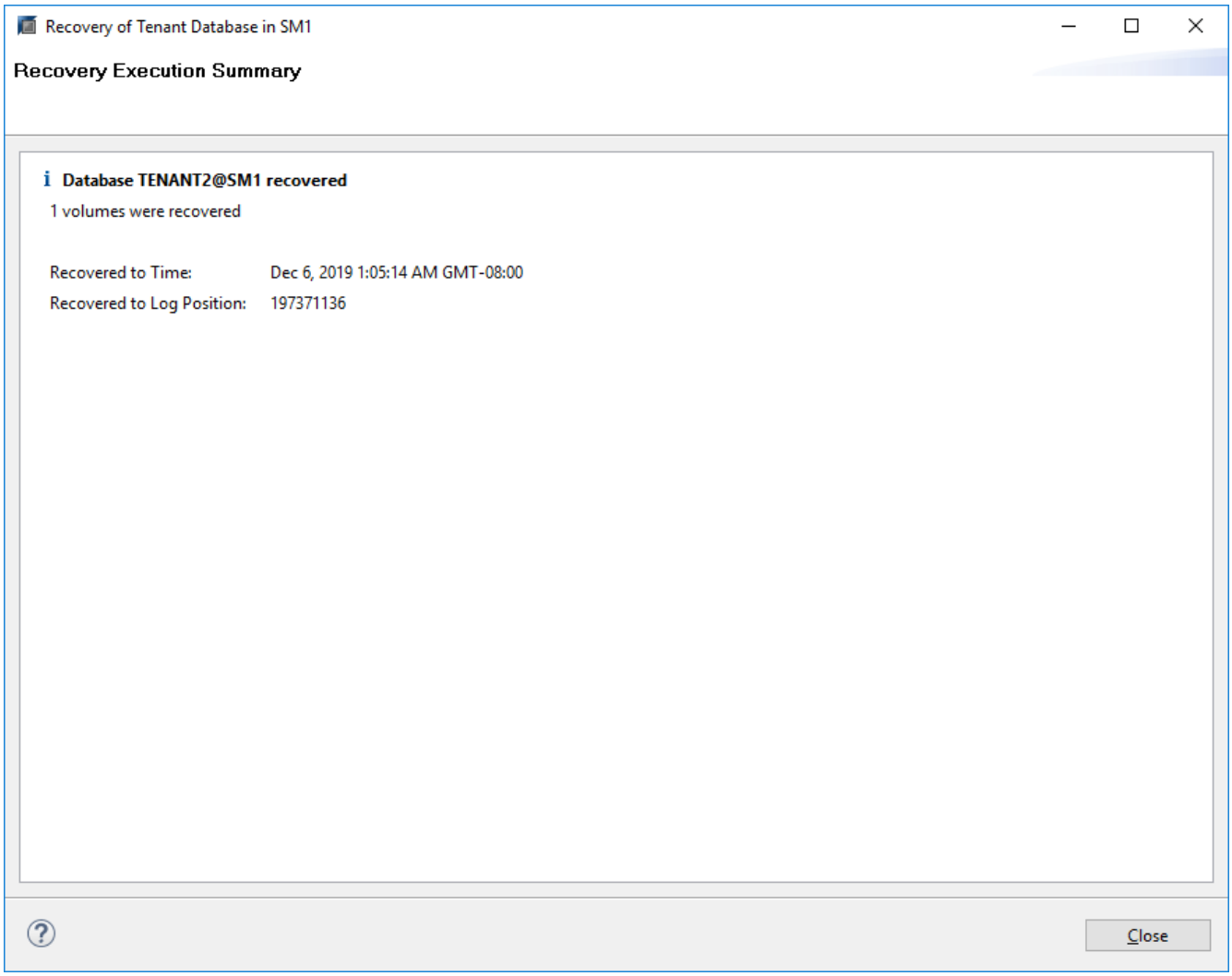


14. Wählen Sie die anderen Einstellungen nach Bedarf aus.



15. Starten Sie den Recovery-Vorgang des Mandanten.


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



Manuelle Wiederherstellung

Gehen Sie wie folgt vor, um ein SAP HANA MDC-Einzelmandant-System mit SAP HANA Studio und SnapCenter wiederherzustellen:

1. Vorbereitung des Restore- und Recovery-Prozesses mit SAP HANA Studio:
   a. Wählen Sie Recover System Database und bestätigen Sie das Herunterfahren des SAP HANA-Systems.
   b. Wählen Sie den Wiederherstellungstyp und den Speicherort für die Protokollsicherung aus.
   c. Es wird eine Liste der Daten-Backups angezeigt. Wählen Sie Backup, um die externe Backup-ID anzuzeigen.
2. Führen Sie den Wiederherstellungsprozess mit SnapCenter aus:
   a. Wählen Sie in der Topologieansicht der Ressource lokale Kopien aus, die aus dem primären Storage oder Vault-Kopien wiederhergestellt werden sollen, wenn Sie eine Wiederherstellung aus einem externen Backup-Storage durchführen möchten.
   b. Wählen Sie das SnapCenter Backup aus, das mit der externen Backup-ID oder dem Kommentarfeld aus SAP HANA Studio übereinstimmt.
   c. Starten Sie den Wiederherstellungsprozess.

> Wenn eine Volume-basierte Wiederherstellung aus dem primären Speicher ausgewählt wird, müssen die Daten-Volumes vor der Wiederherstellung von allen SAP HANA-Datenbank-Hosts abgehängt und nach Abschluss des Wiederherstellungsprozesses erneut gemountet werden.

> Bei einer SAP HANA-Konfiguration mit mehreren Hosts mit FC werden die Unmount- und Mount-Vorgänge im Rahmen des Shutdown- und Startvorgangs der Datenbank vom SAP HANA-Namensserver ausgeführt.

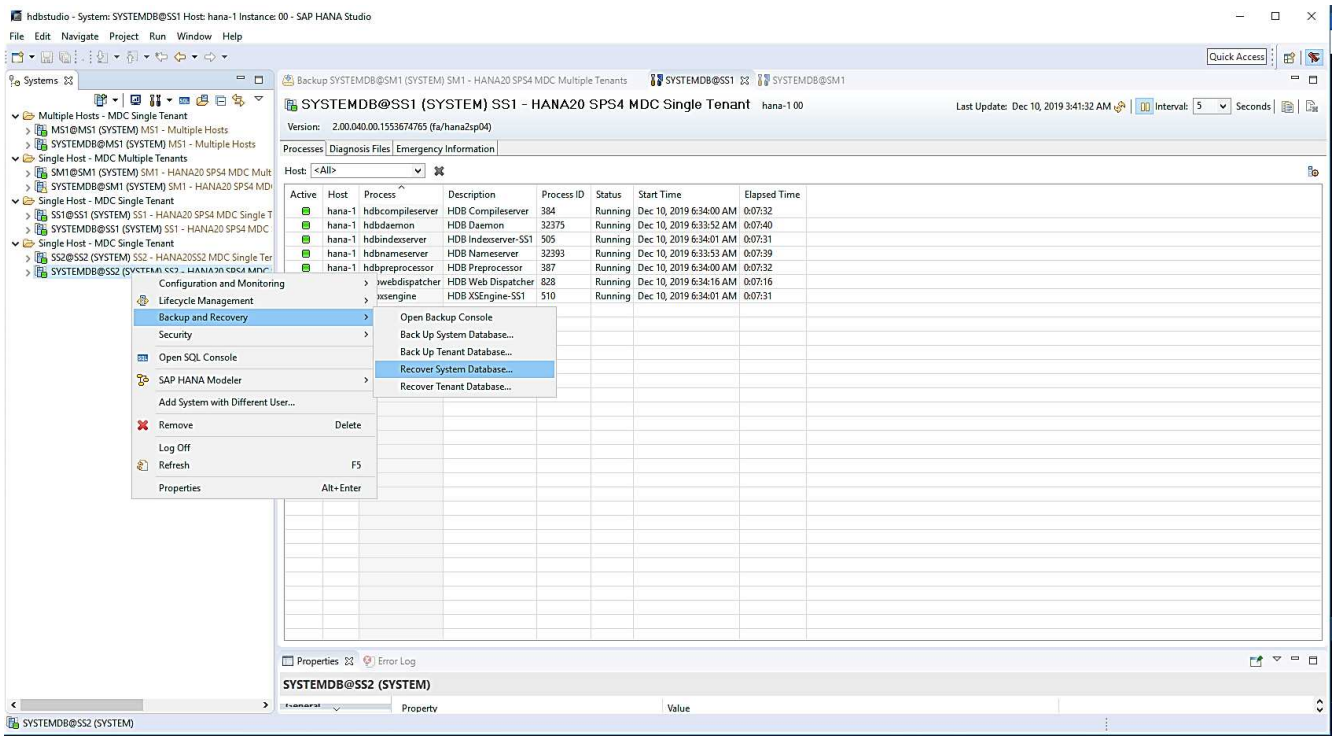
3. Führen Sie den Recovery-Prozess für die Systemdatenbank mit SAP HANA Studio aus:
   a. Klicken Sie in der Backup-Liste auf Aktualisieren, und wählen Sie das verfügbare Backup für die Recovery aus (wird durch ein grünes Symbol angezeigt).
   b. Starten Sie den Wiederherstellungsprozess. Nach Abschluss des Wiederherstellungsprozesses wird die Systemdatenbank gestartet.
4. Führen Sie den Recovery-Prozess für die Mandantendatenbank mit SAP HANA Studio aus:
   a. Wählen Sie die Option „Tenant Database wiederherstellen“ und wählen Sie den Mieter aus, der wiederhergestellt werden soll.
   b. Wählen Sie den Wiederherstellungstyp und den Speicherort für die Protokollsicherung aus.

      Es wird eine Liste der Daten-Backups angezeigt. Da das Daten-Volume bereits wiederhergestellt ist, wird das Mandanten-Backup als verfügbar angezeigt (in grün).

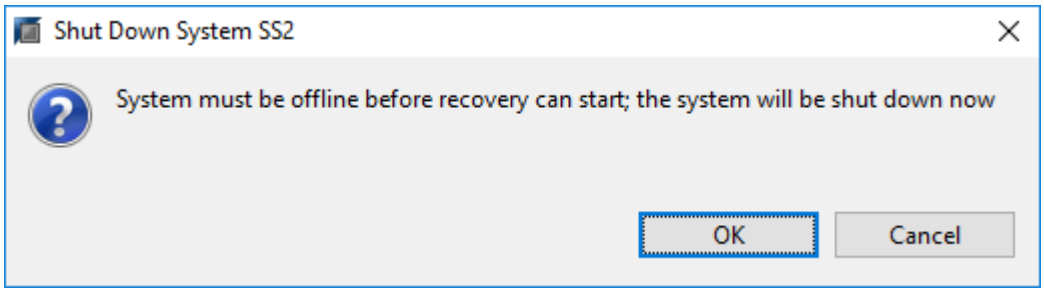
   c. Wählen Sie dieses Backup aus, und starten Sie den Wiederherstellungsprozess. Nach Abschluss des Recovery-Prozesses wird die Mandantendatenbank automatisch gestartet.

Im folgenden Abschnitt werden die Schritte der Wiederherstellungs- und Wiederherstellungsvorgänge des manuell konfigurierten HANA-Systems SS2 beschrieben (SAP HANA einzelner Host, MDC-Mehrmandantensystem mit NFS).

1. Wählen Sie in SAP HANA Studio die Option Systemdatenbank wiederherstellen aus, um die Wiederherstellung der Systemdatenbank zu starten.

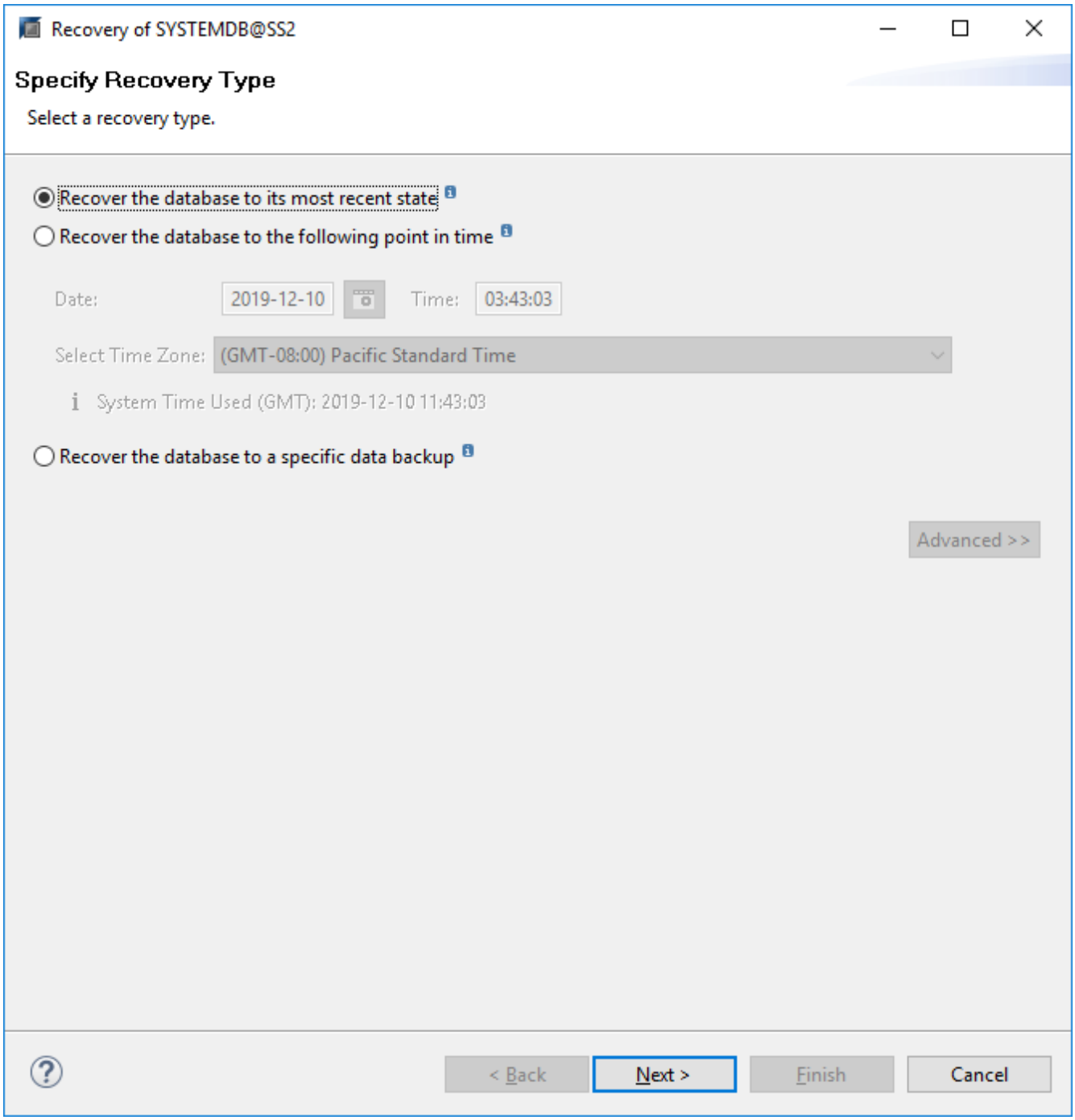


2. Klicken Sie auf OK, um die SAP HANA-Datenbank herunterzufahren.

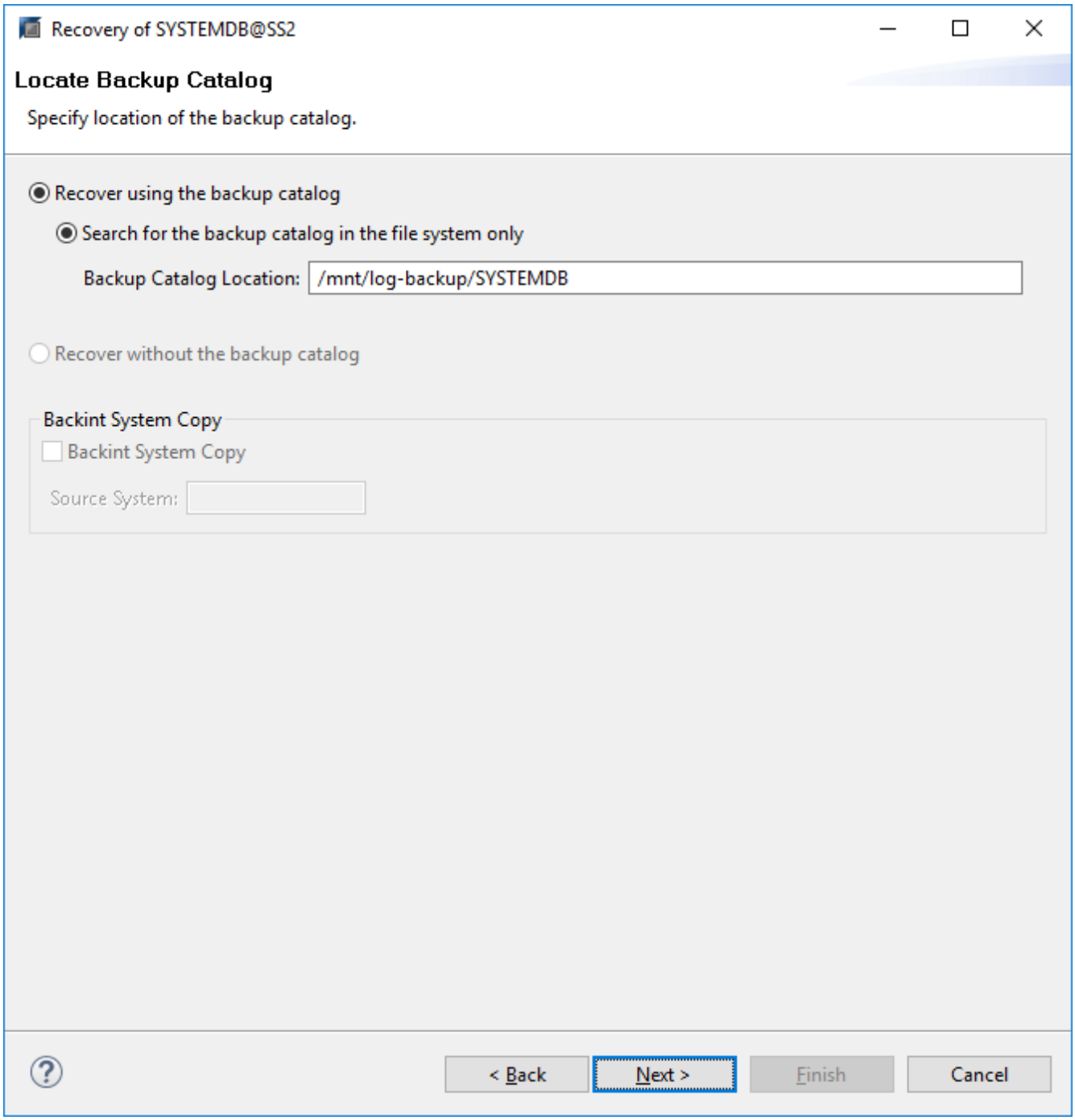


Das SAP HANA-System wird heruntergefahren und der Wiederherstellungsassistent wird gestartet.

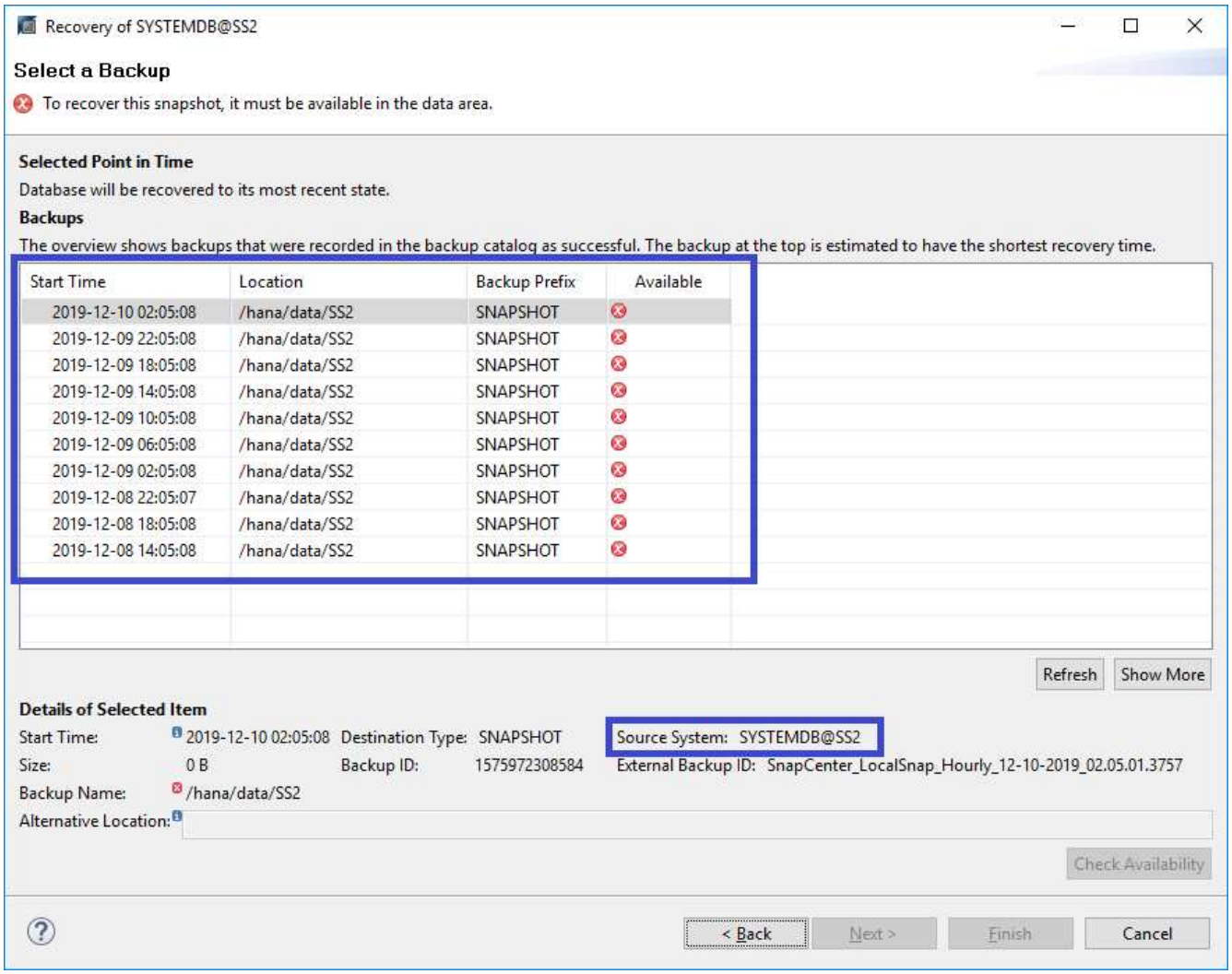
3. Wählen Sie den Wiederherstellungstyp aus, und klicken Sie auf Weiter.



4. Geben Sie den Speicherort des Backup-Katalogs an, und klicken Sie auf Weiter.



5. Eine Liste der verfügbaren Backups wird basierend auf dem Inhalt des Backup-Katalogs angezeigt. Wählen Sie das gewünschte Backup und notieren Sie sich die externe Backup ID: In unserem Beispiel das aktuellste Backup.



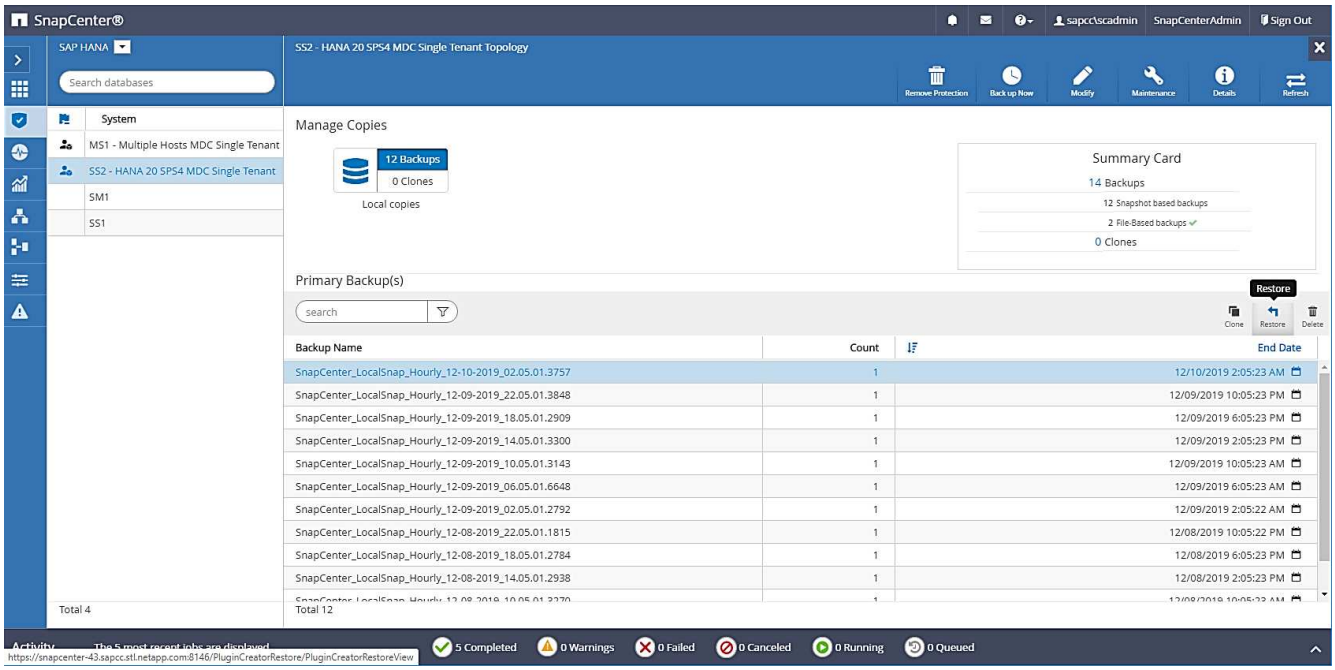
6. Heben Sie die Bereitstellung aller Daten-Volumes auf.

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

> Bei einem SAP HANA mehrere Host-System mit NFS müssen alle Daten-Volumes auf jedem Host abgehängt werden.

> Bei einer SAP HANA-Konfiguration mit mehreren Hosts mit FC wird der Unmount-Vorgang im Rahmen des Herunterfahrens vom SAP HANA-Namensserver ausgeführt.

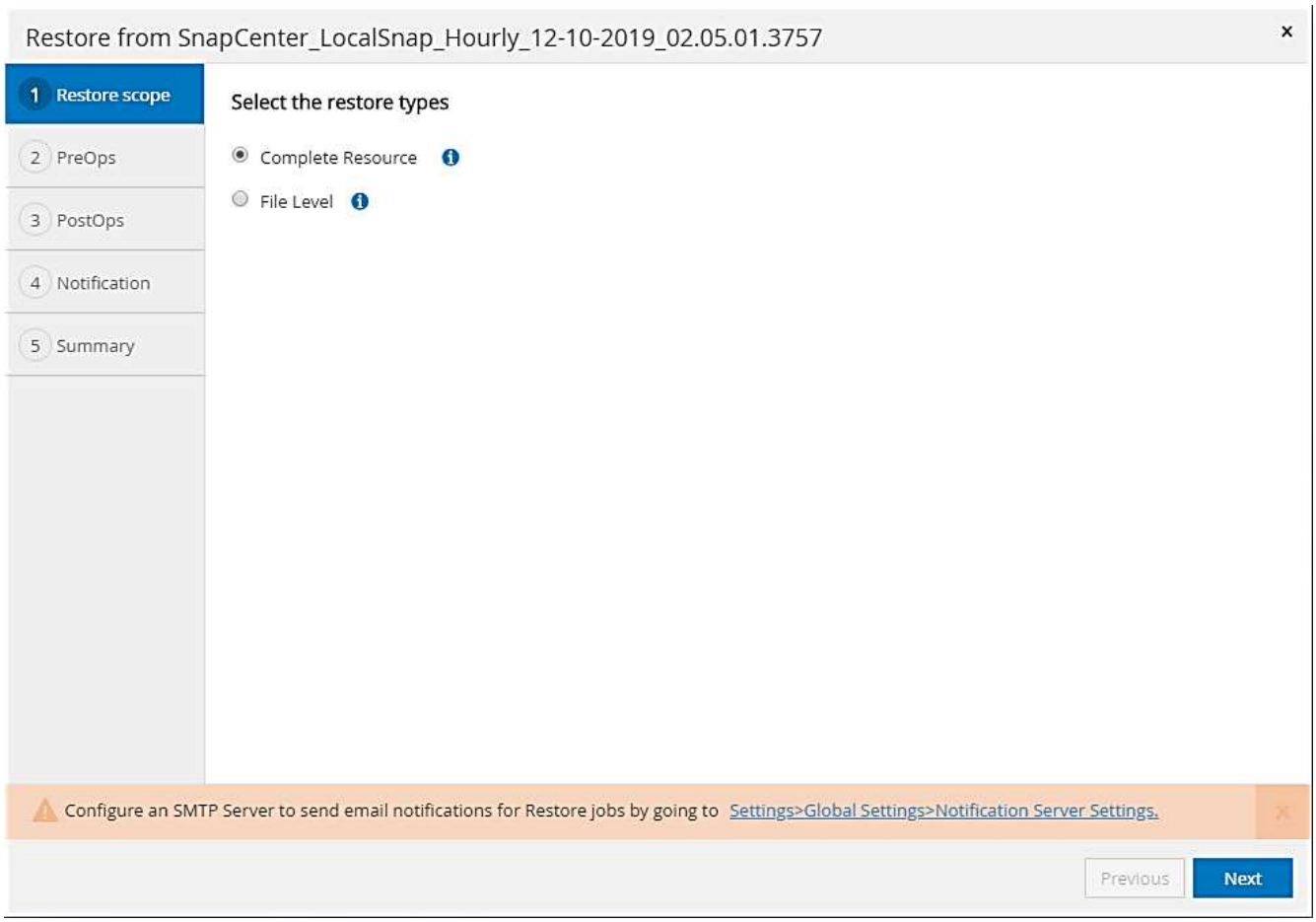
7. Wählen Sie in der SnapCenter GUI die Ansicht der Ressourcen-Topologie aus und wählen Sie das Backup aus, das wiederhergestellt werden soll, beispielsweise das aktuellste primäre Backup. Klicken Sie auf das Symbol Wiederherstellen, um die Wiederherstellung zu starten.



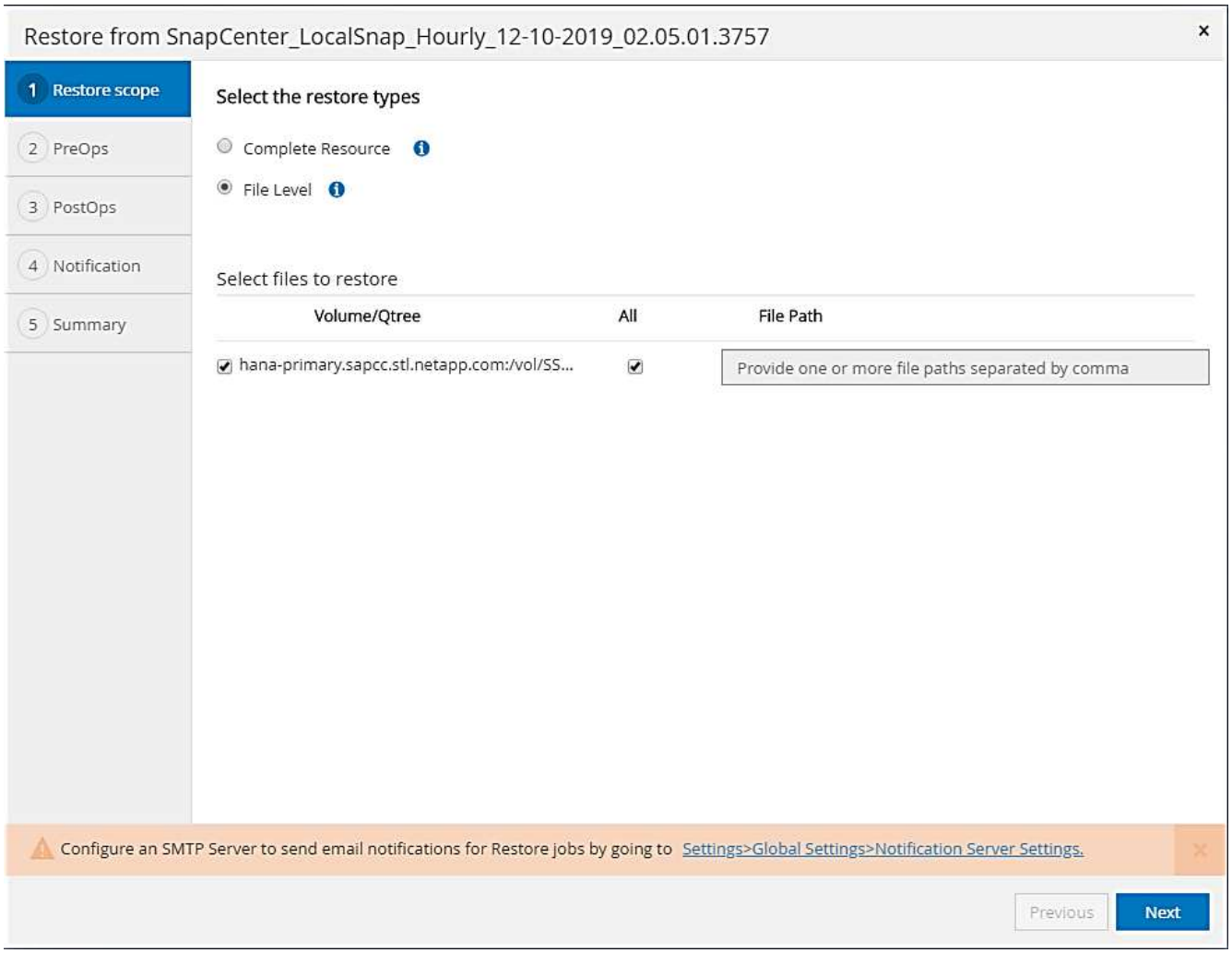
Der SnapCenter-Wiederherstellungsassistent wird gestartet.

8. Wählen Sie den Wiederherstellungstyp Complete Resource or File Level aus.

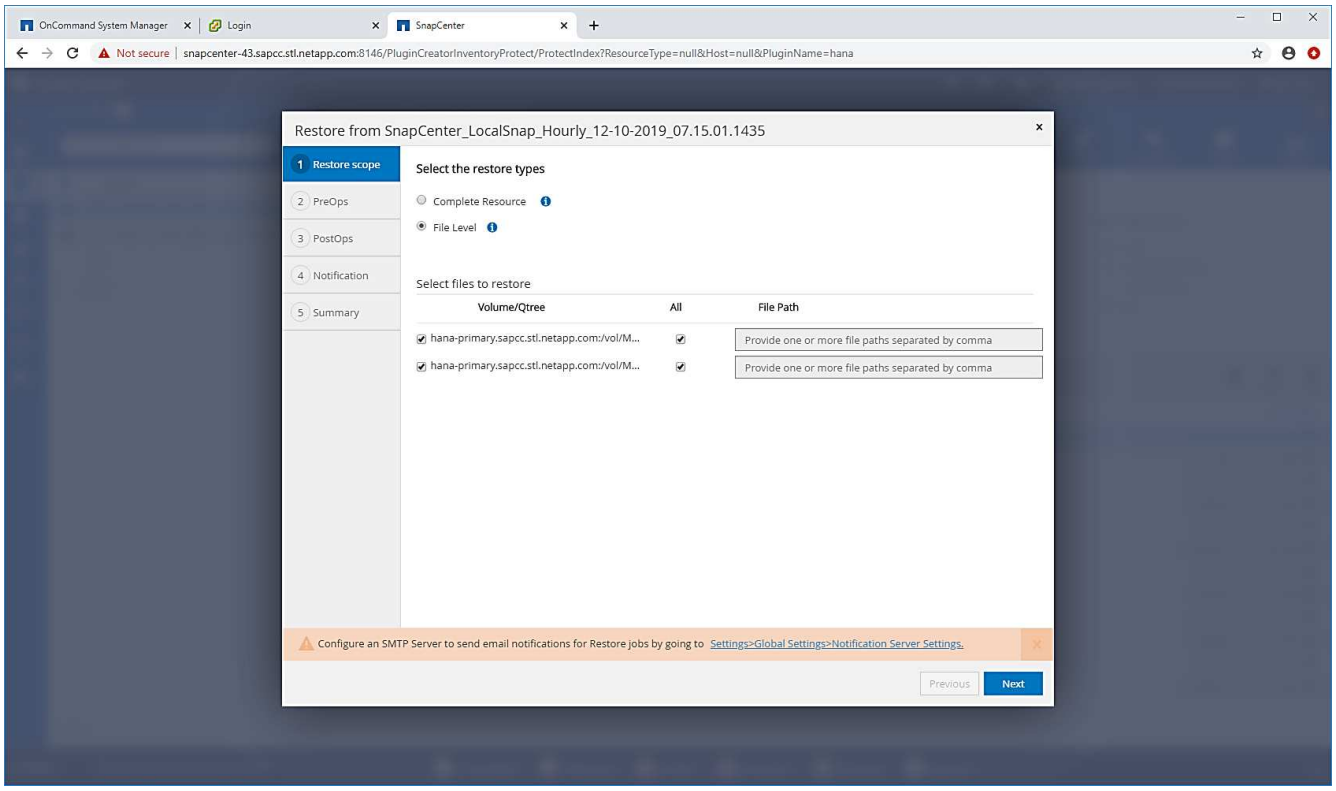
   Wählen Sie „Complete Resource“ aus, um eine Volume-basierte Wiederherstellung zu verwenden.



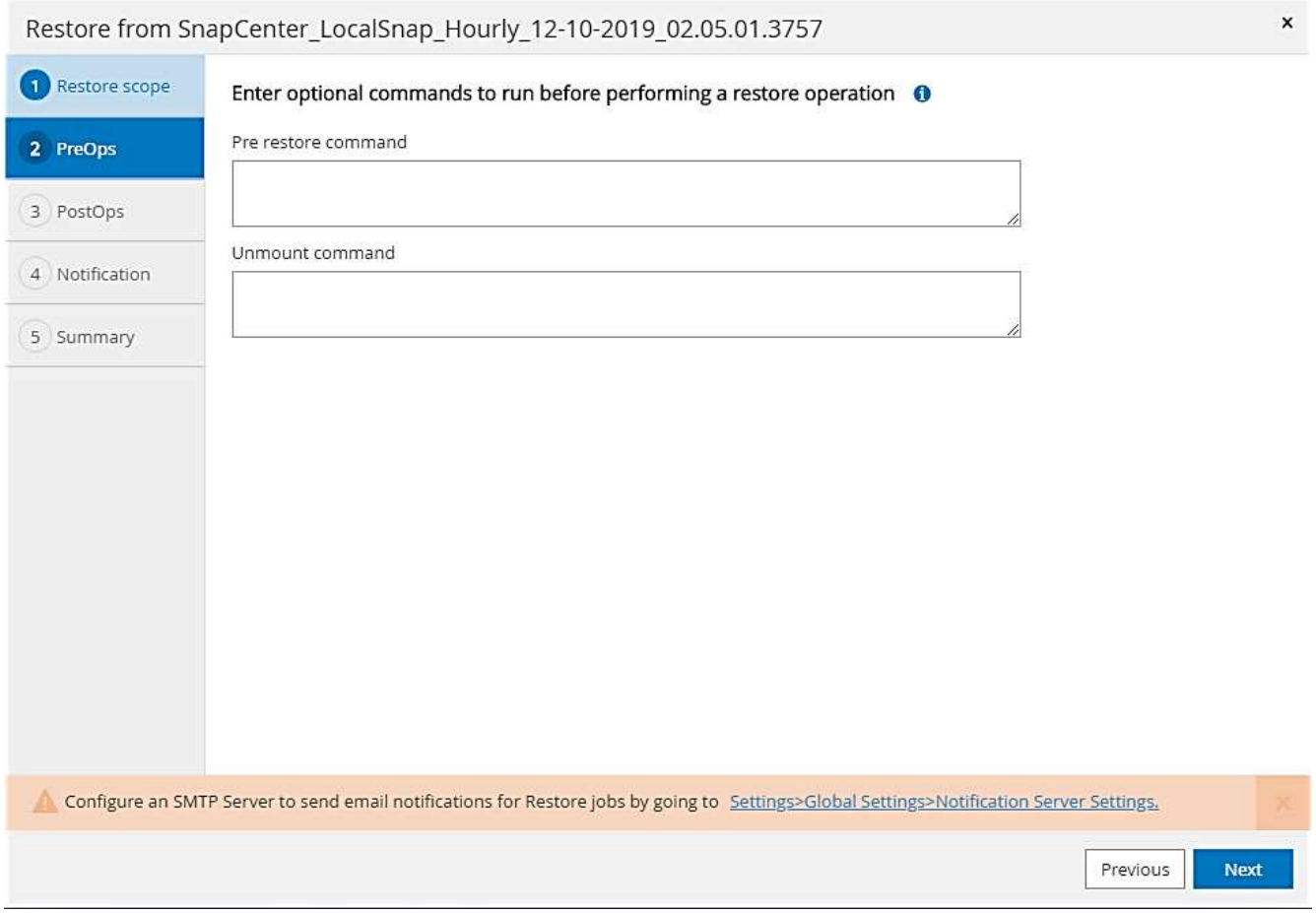
9. Wählen Sie Dateiebene und Alle, um einen SnapRestore-Vorgang mit einer einzigen Datei für alle Dateien zu verwenden.



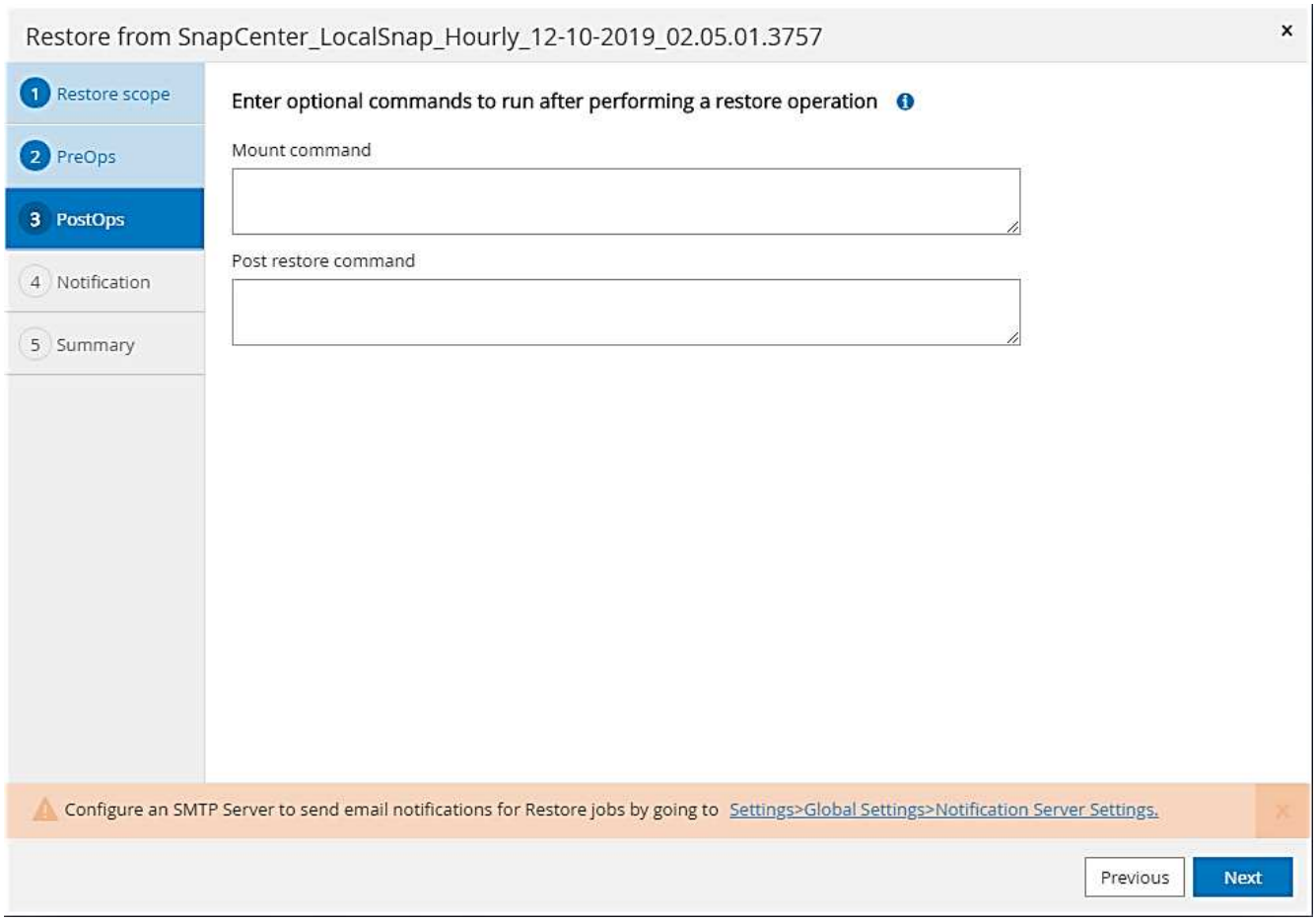
Wählen Sie für eine Wiederherstellung auf Dateiebene eines SAP HANA-Host-Systems mit mehreren Hosts alle Volumes aus.



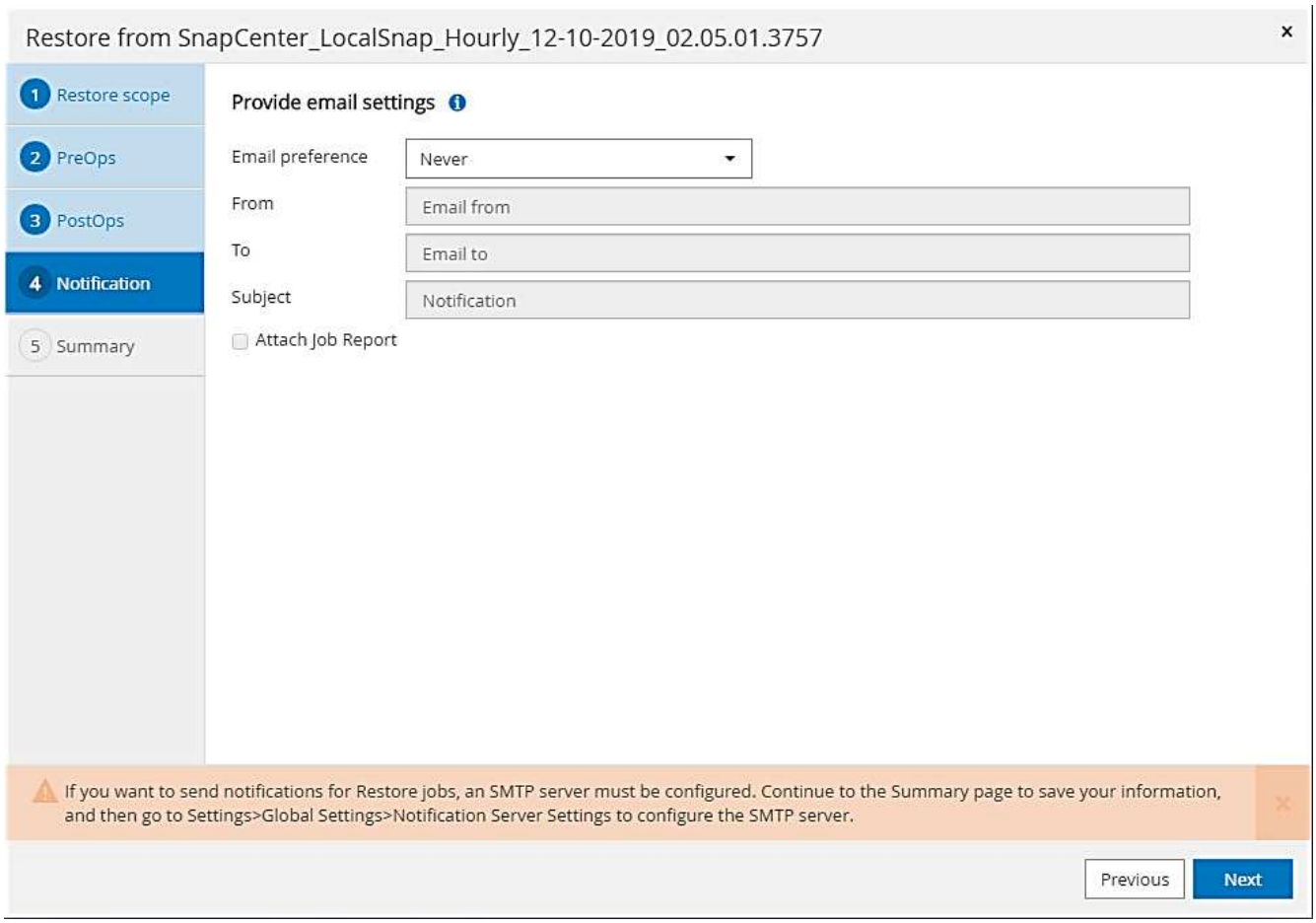
10. (Optional) Geben Sie die Befehle an, die aus dem SAP HANA-Plug-in ausgeführt werden sollen, das auf dem zentralen HANA-Plug-in-Host ausgeführt wird. Klicken Sie Auf Weiter.



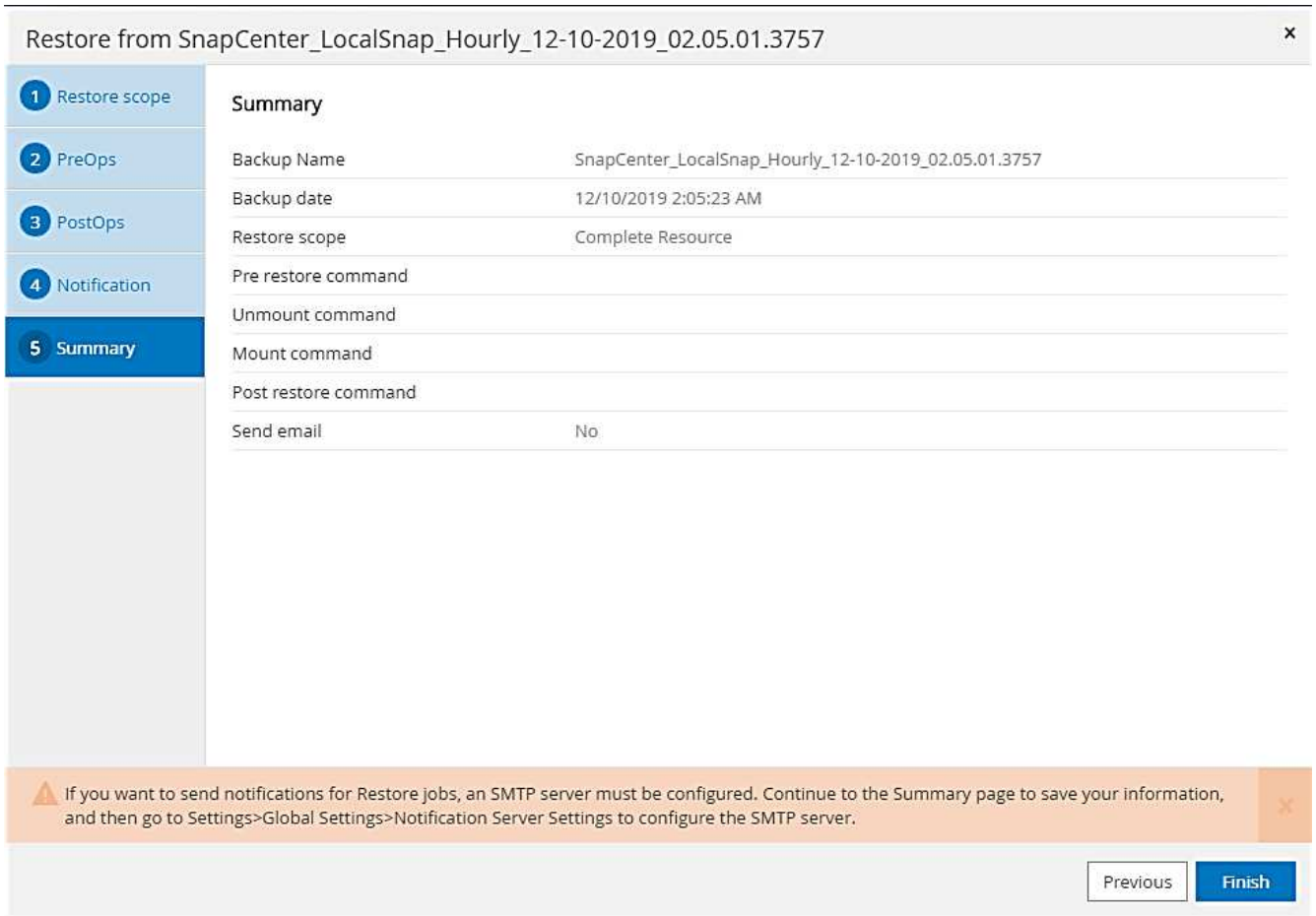
11. Geben Sie die optionalen Befehle an, und klicken Sie auf Weiter.



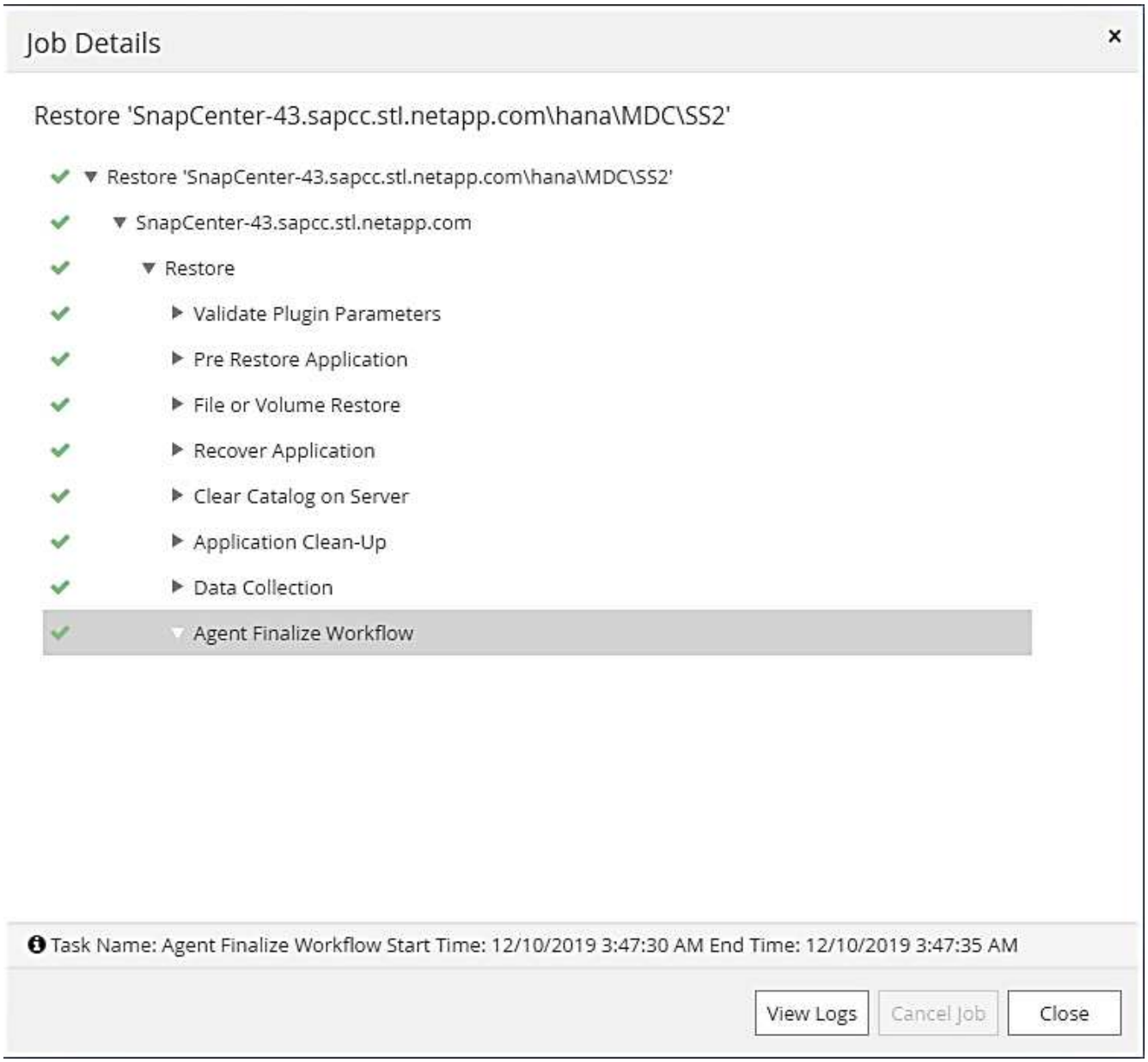
12. Geben Sie die Benachrichtigungseinstellungen an, damit SnapCenter eine Status-E-Mail und ein Jobprotokoll senden kann. Klicken Sie Auf Weiter.



13. Überprüfen Sie die Zusammenfassung und klicken Sie auf Fertig stellen, um die Wiederherstellung zu starten.



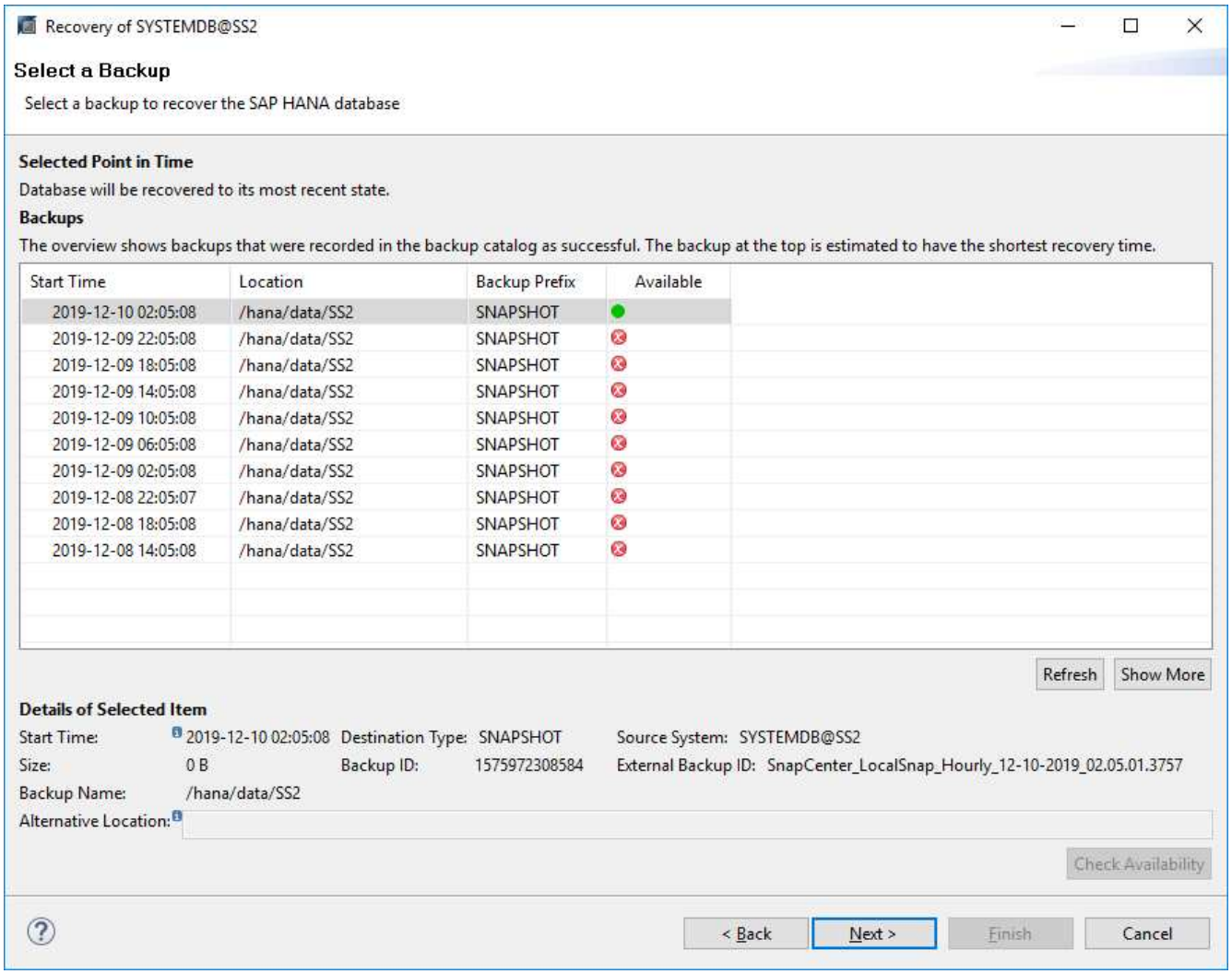
14. Der Wiederherstellungsauftrag wird gestartet, und das Jobprotokoll kann durch Doppelklicken auf die Protokollzeile im Aktivitätsfenster angezeigt werden.



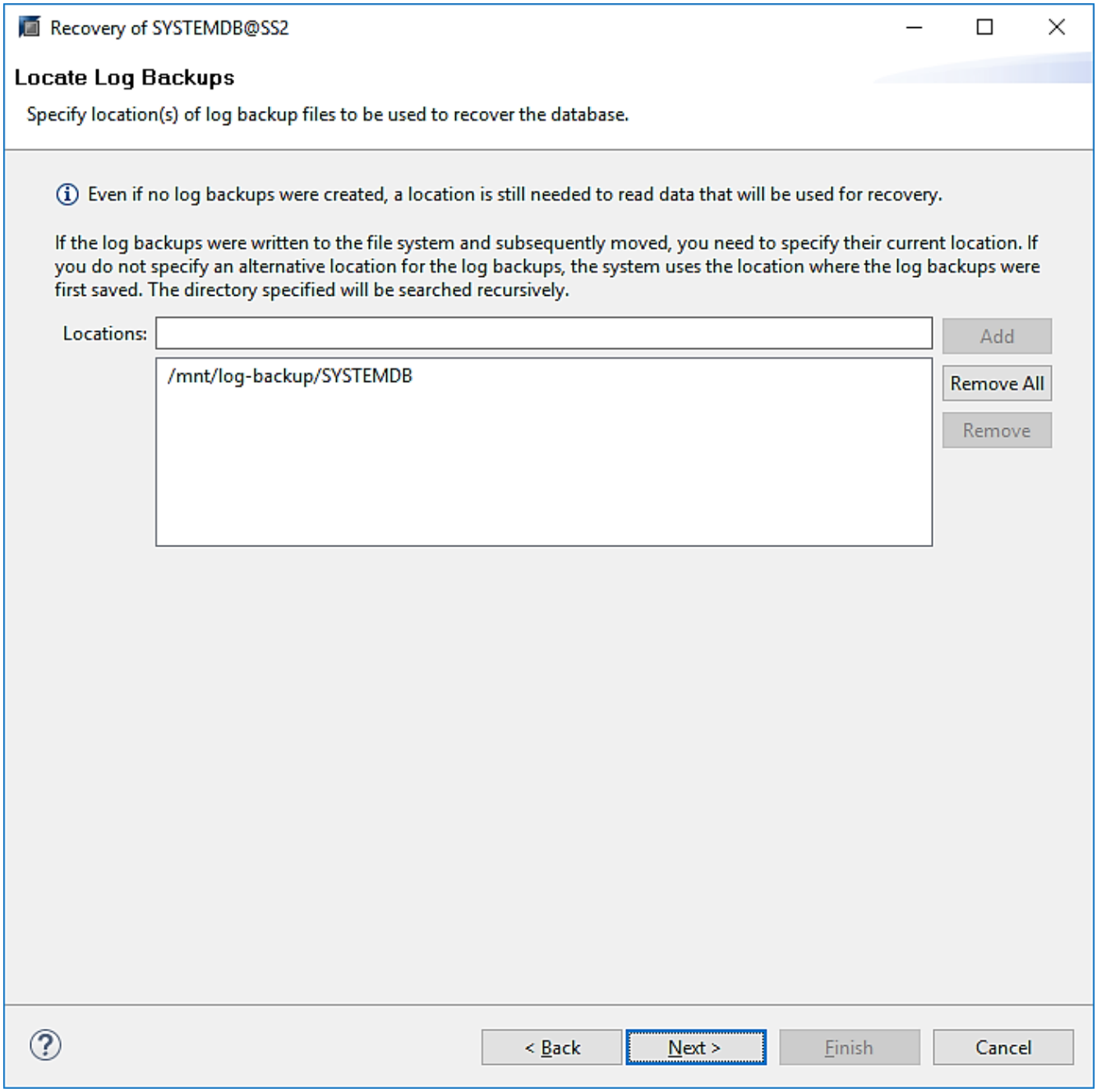
15. Warten Sie, bis der Wiederherstellungsvorgang abgeschlossen ist. Mounten Sie auf jedem Datenbank-Host alle Daten-Volumes. In unserem Beispiel muss nur ein Volume auf dem Datenbank-Host neu eingebunden werden.

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

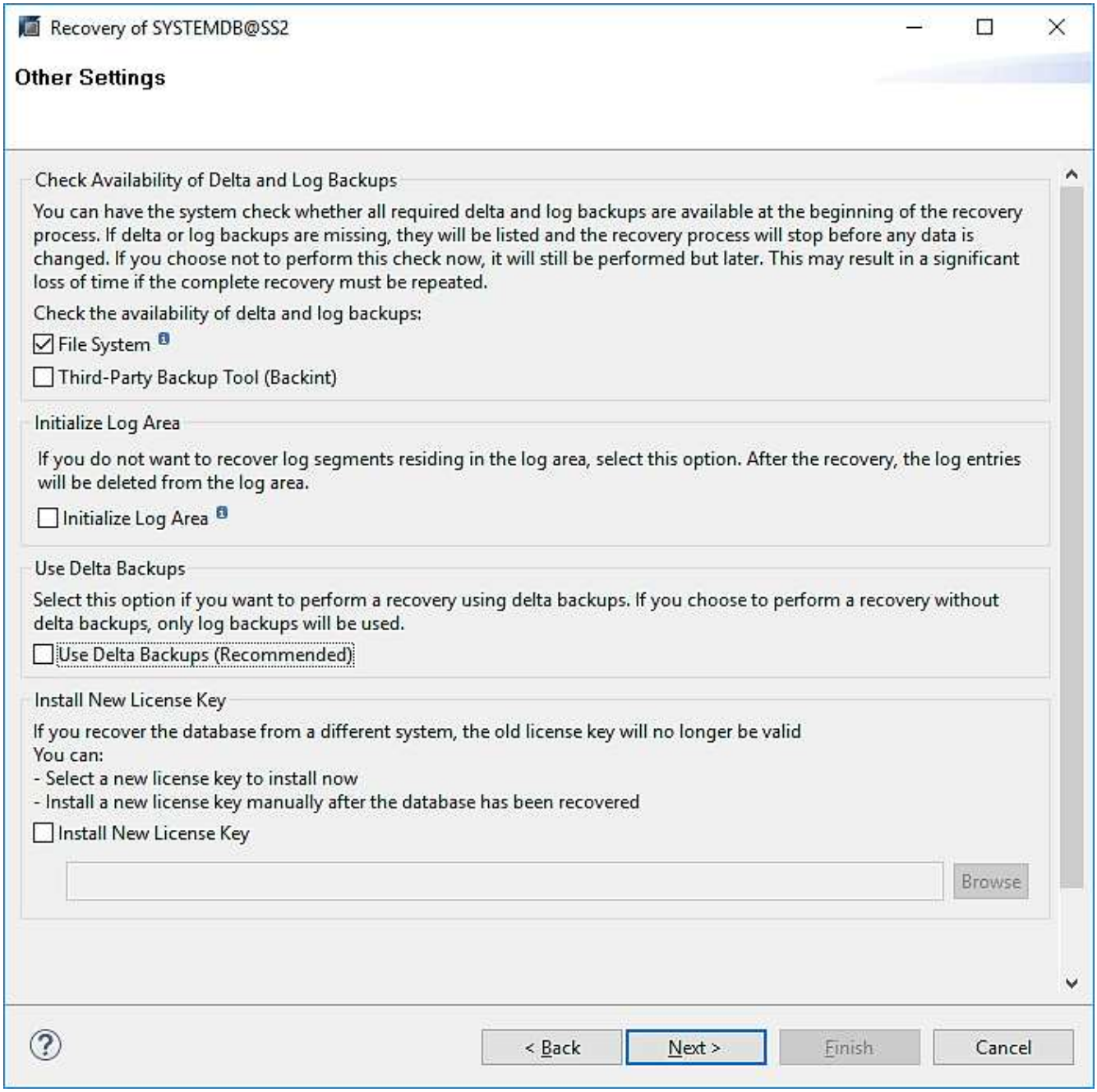
16. Gehen Sie zu SAP HANA Studio und klicken Sie auf Aktualisieren, um die Liste der verfügbaren Backups zu aktualisieren. Das mit SnapCenter wiederhergestellte Backup wird durch ein grünes Symbol in der Liste der Backups angezeigt. Wählen Sie das Backup aus, und klicken Sie auf Weiter.



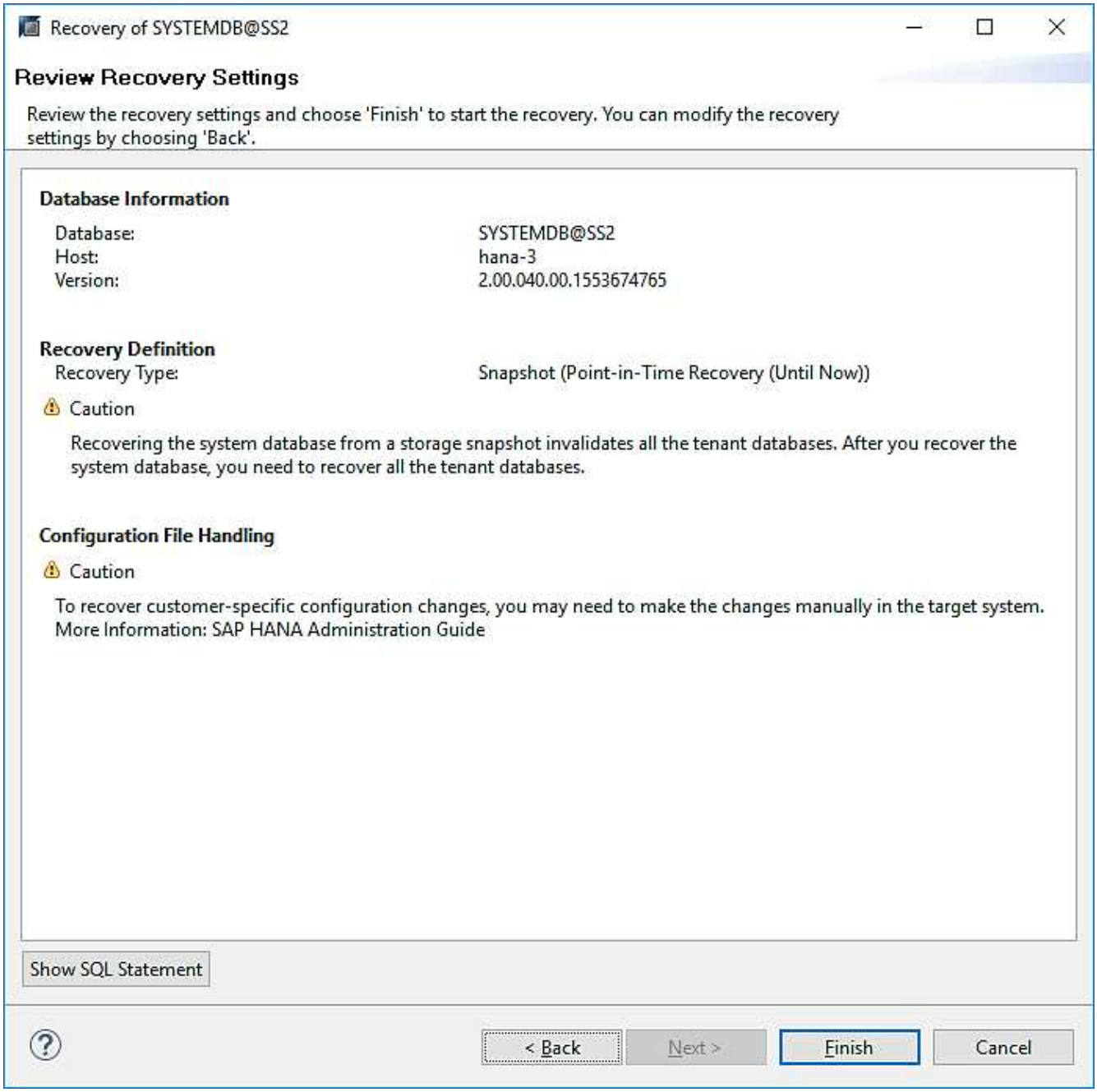
17. Stellen Sie den Speicherort der Protokoll-Backups bereit. Klicken Sie Auf Weiter.



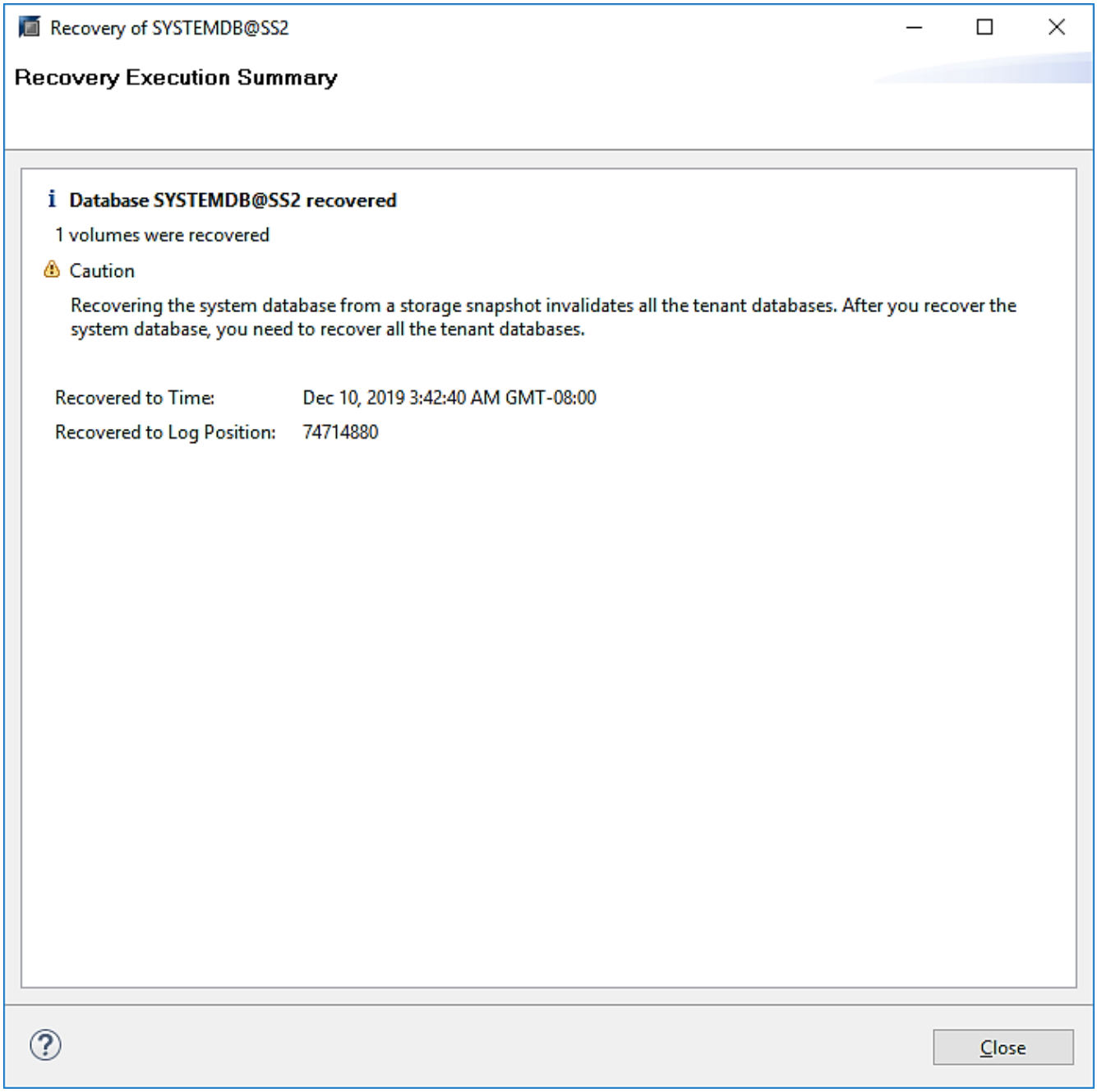
18. Wählen Sie je nach Bedarf andere Einstellungen aus. Stellen Sie sicher, dass Delta-Backups verwenden nicht ausgewählt ist. Klicken Sie Auf Weiter.



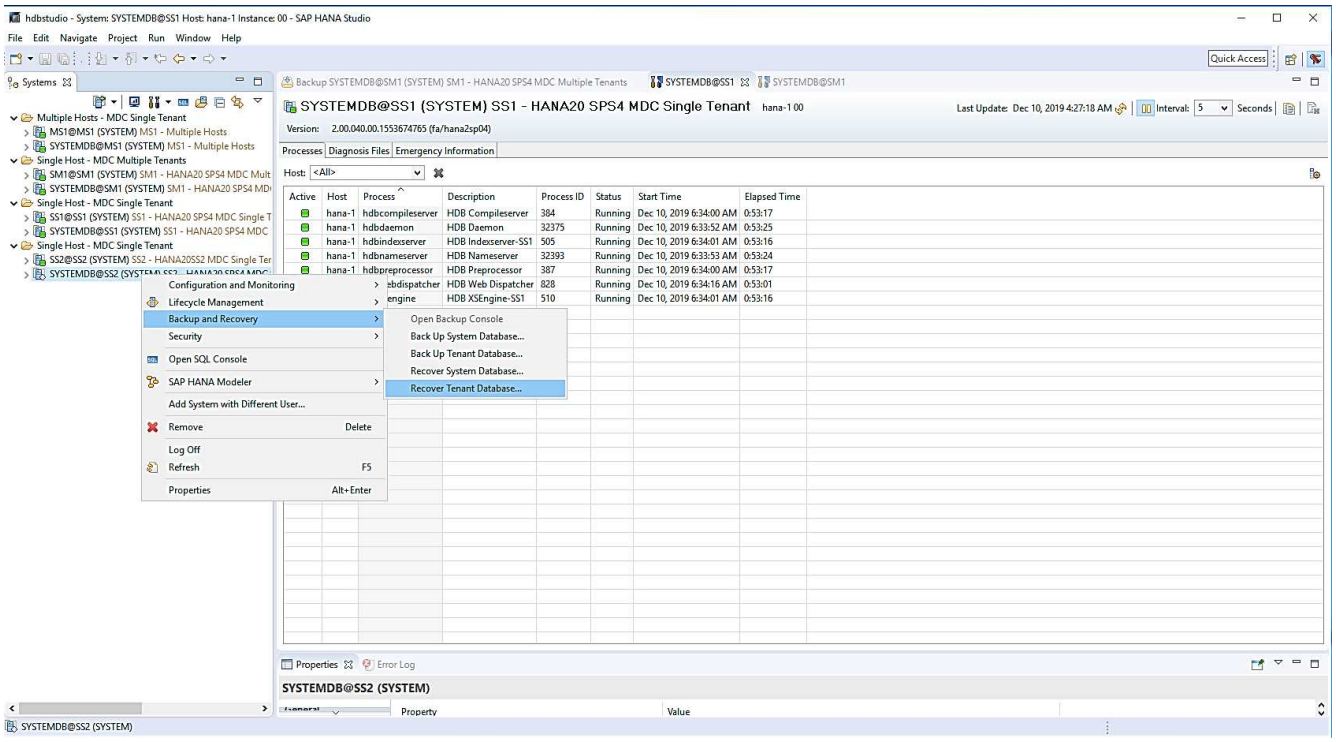
19. Überprüfen Sie die Wiederherstellungseinstellungen, und klicken Sie auf Fertig stellen.



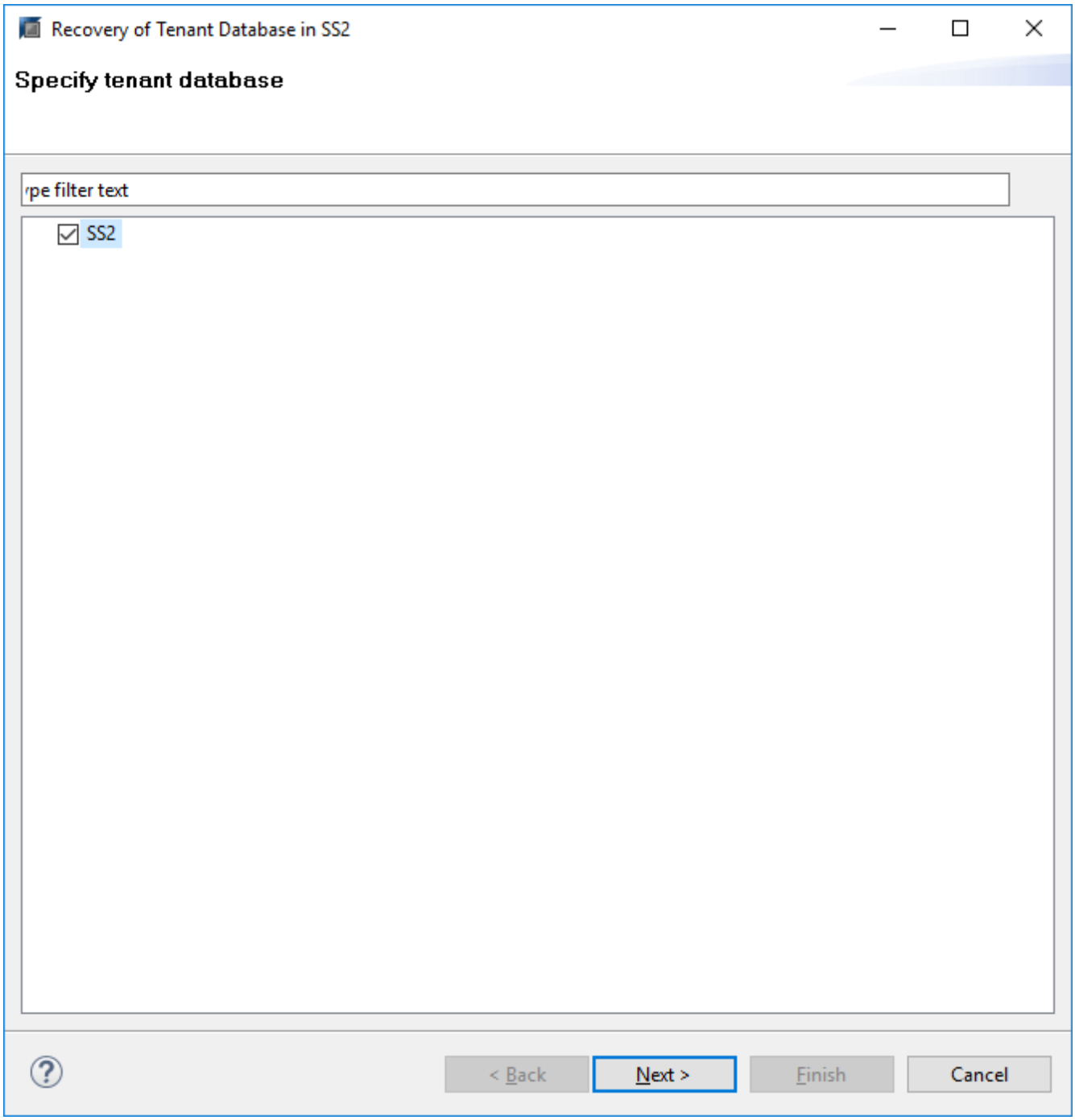
20. Der Wiederherstellungsprozess wird gestartet. Warten Sie, bis die Wiederherstellung der Systemdatenbank abgeschlossen ist.



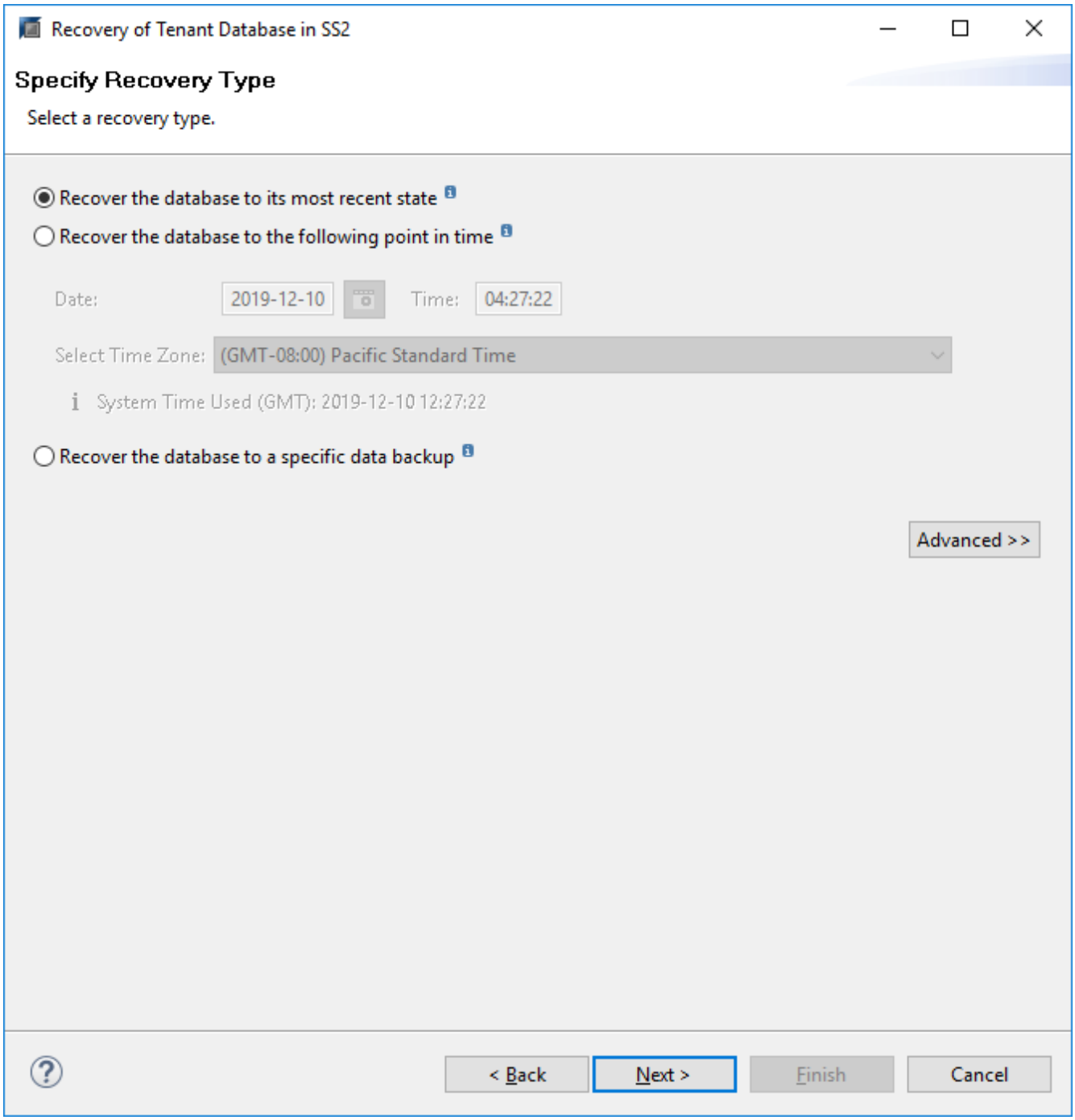
21. Wählen Sie in SAP HANA Studio den Eintrag für die Systemdatenbank aus, und starten Sie Backup Recovery - Rcover Tenant Database.



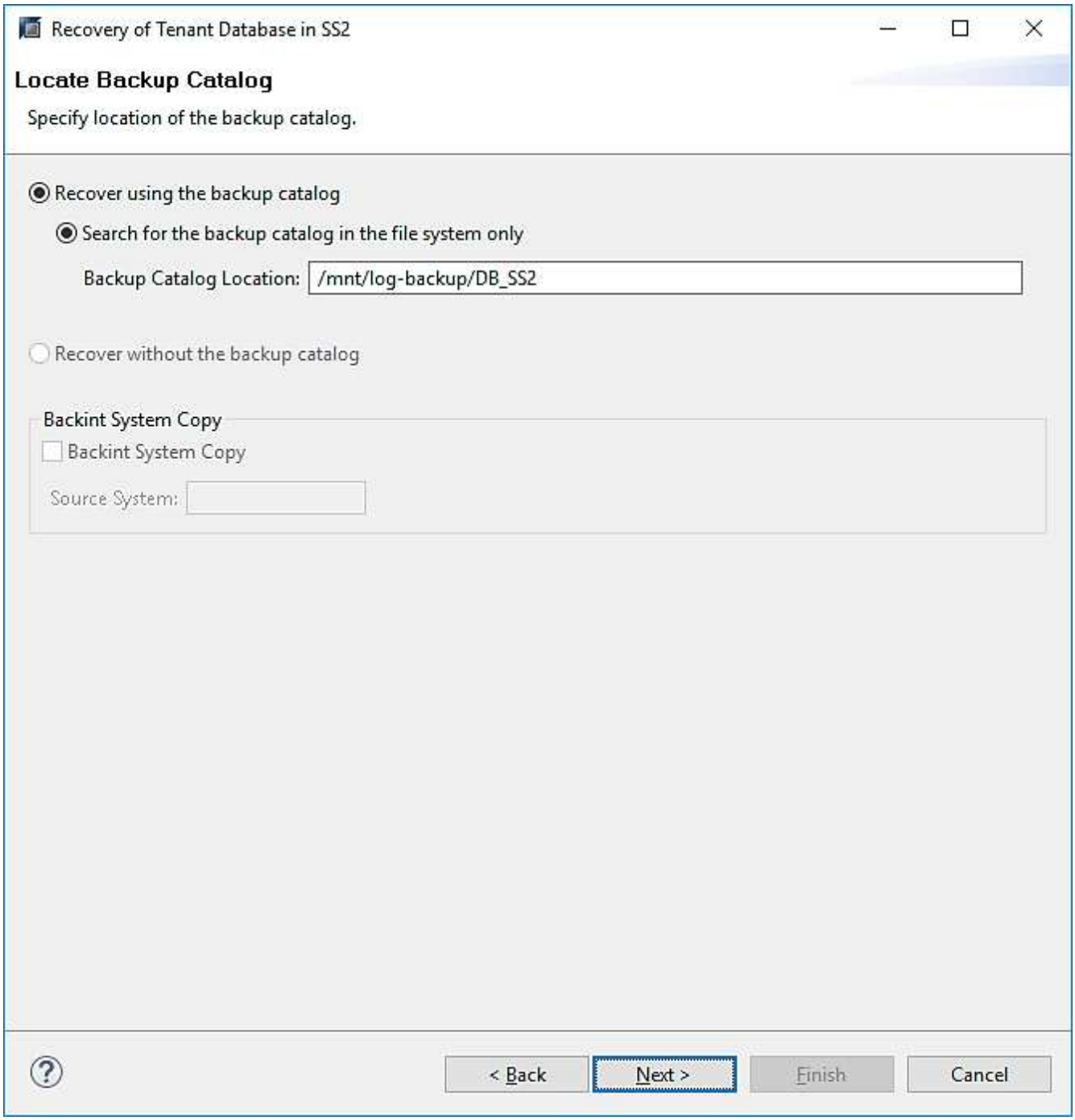
22. Wählen Sie den zu wiederherzuenden Mieter aus, und klicken Sie auf Weiter.



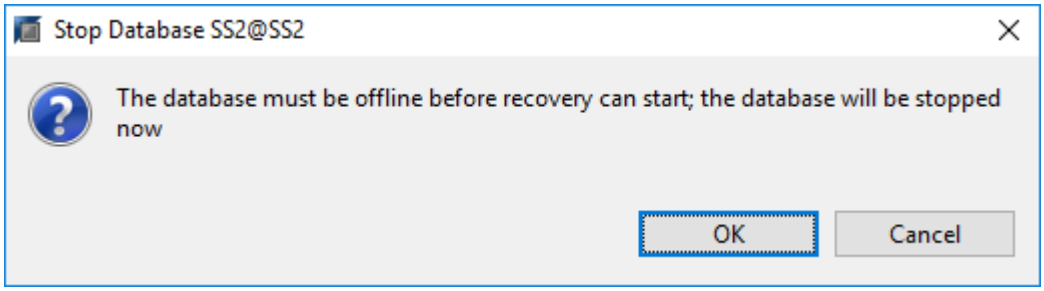
23. Geben Sie den Wiederherstellungstyp an, und klicken Sie auf Weiter.



24. Bestätigen Sie den Speicherort des Backup-Katalogs, und klicken Sie auf Weiter.

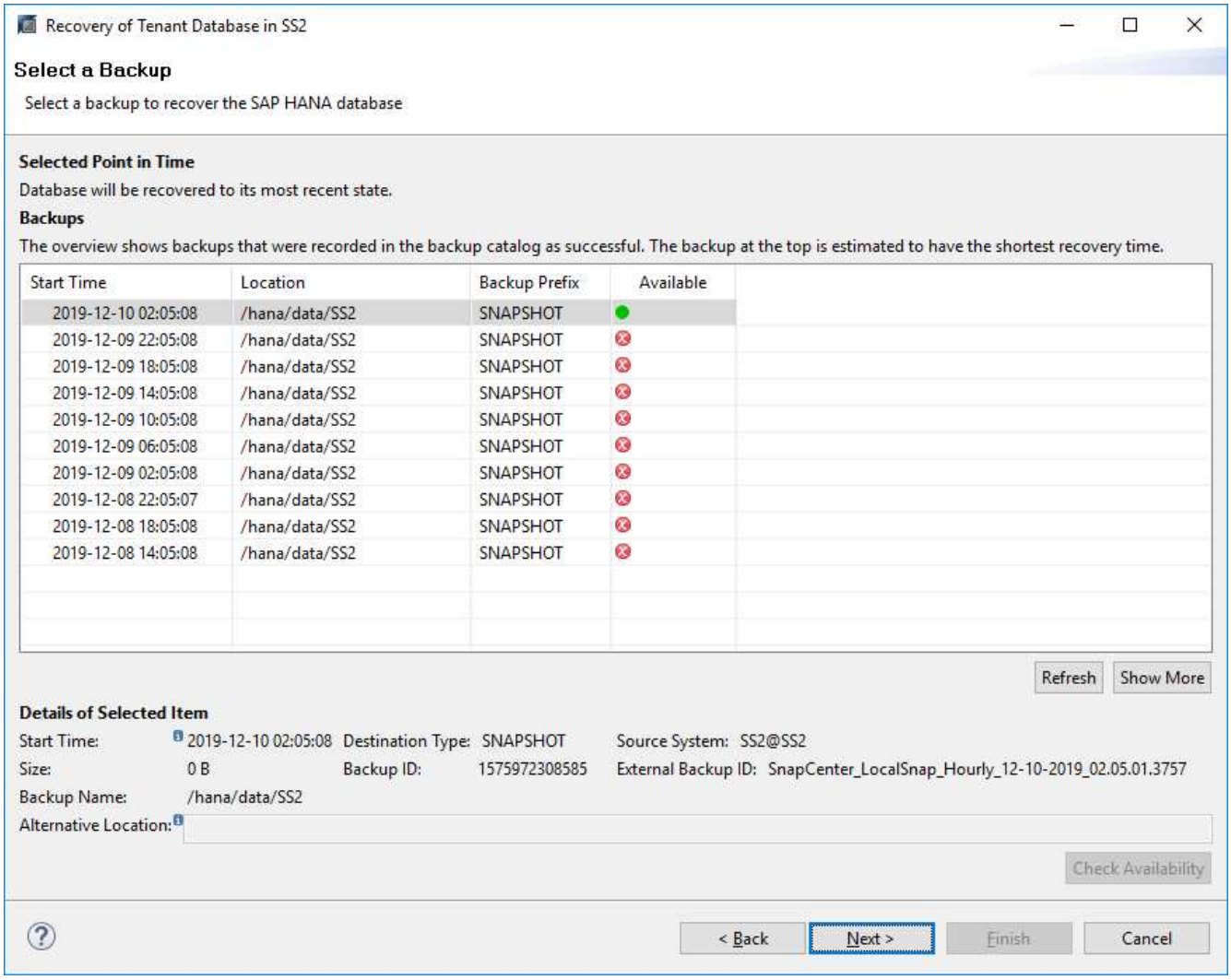


25. Vergewissern Sie sich, dass die Mandantendatenbank offline ist. Klicken Sie auf OK, um fortzufahren.

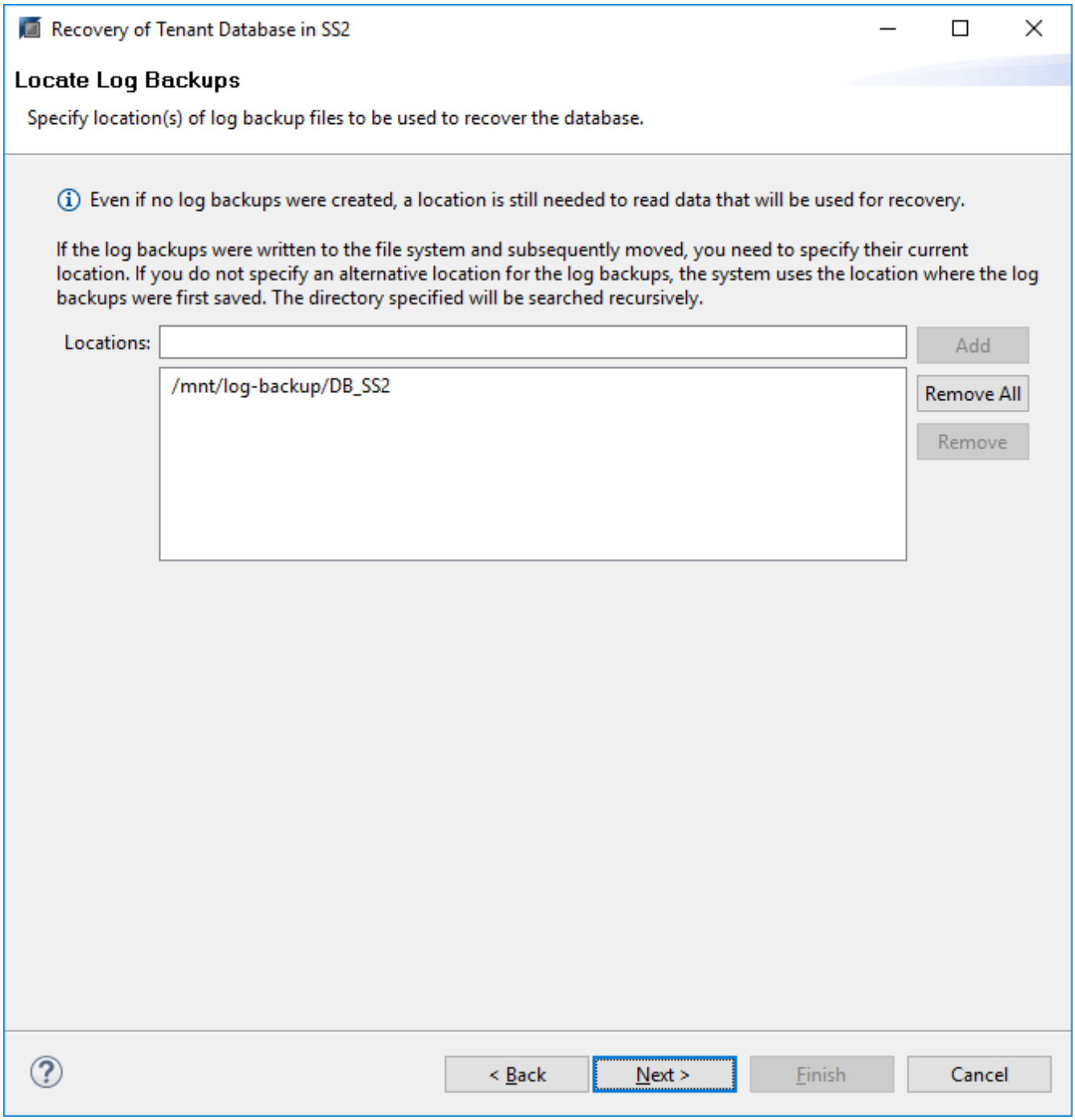


26. Da die Wiederherstellung des Daten-Volumes vor der Wiederherstellung der Systemdatenbank erfolgt ist, ist das Mandanten-Backup sofort verfügbar. Wählen Sie das grün markierte Backup aus, und klicken Sie

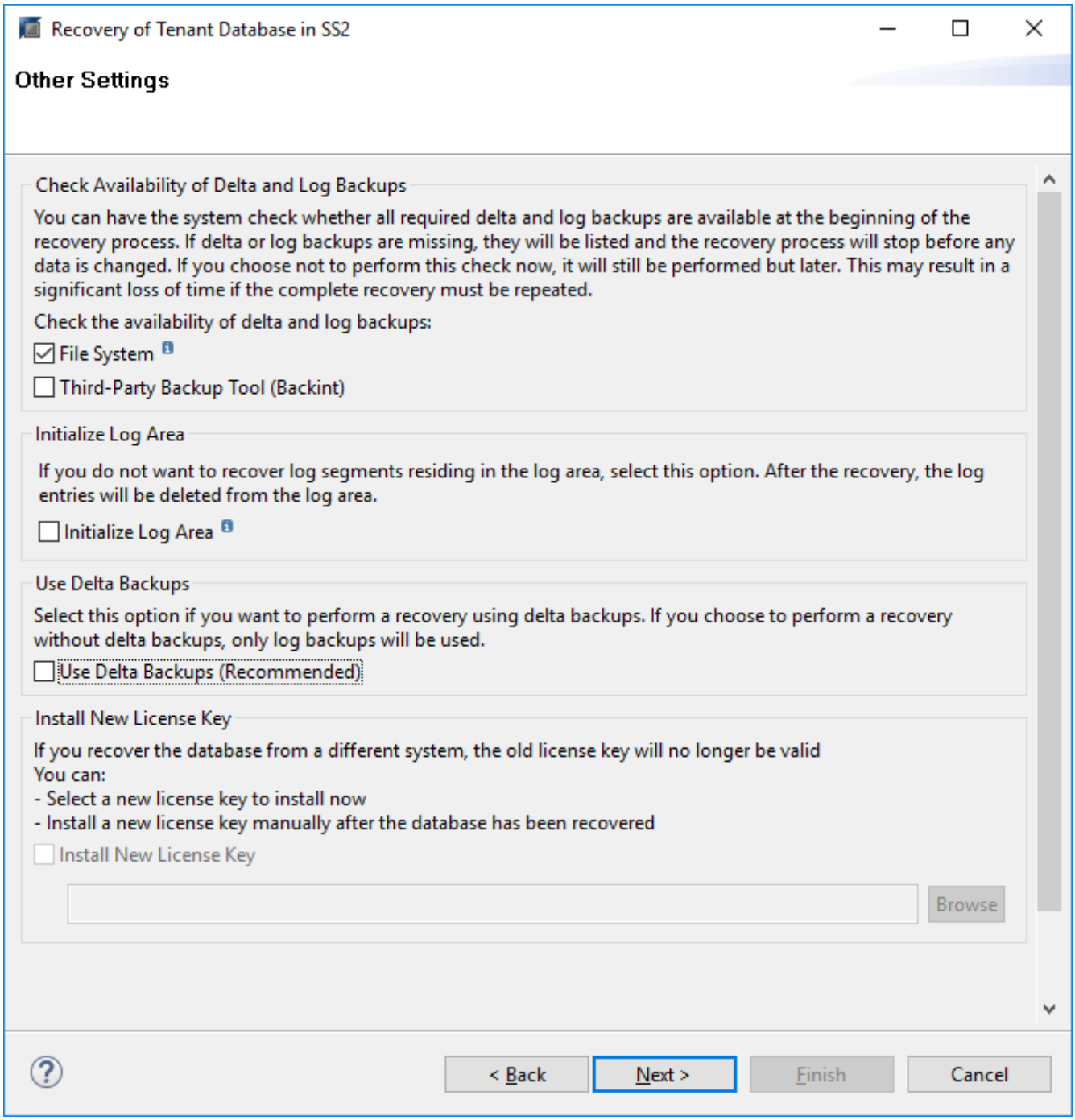
auf Weiter.



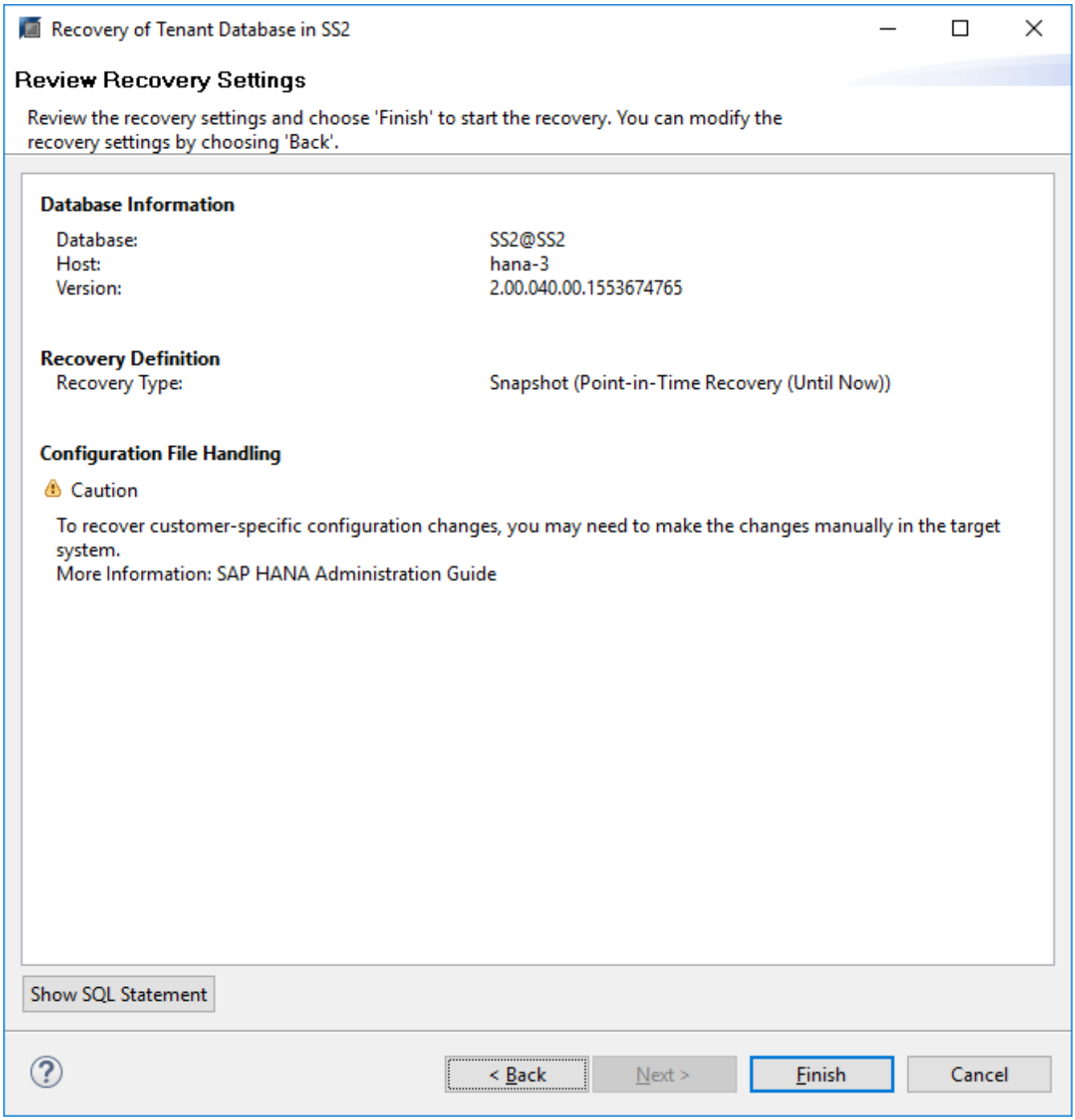
27. Bestätigen Sie den Speicherort für die Protokollsicherung und klicken Sie auf Weiter.



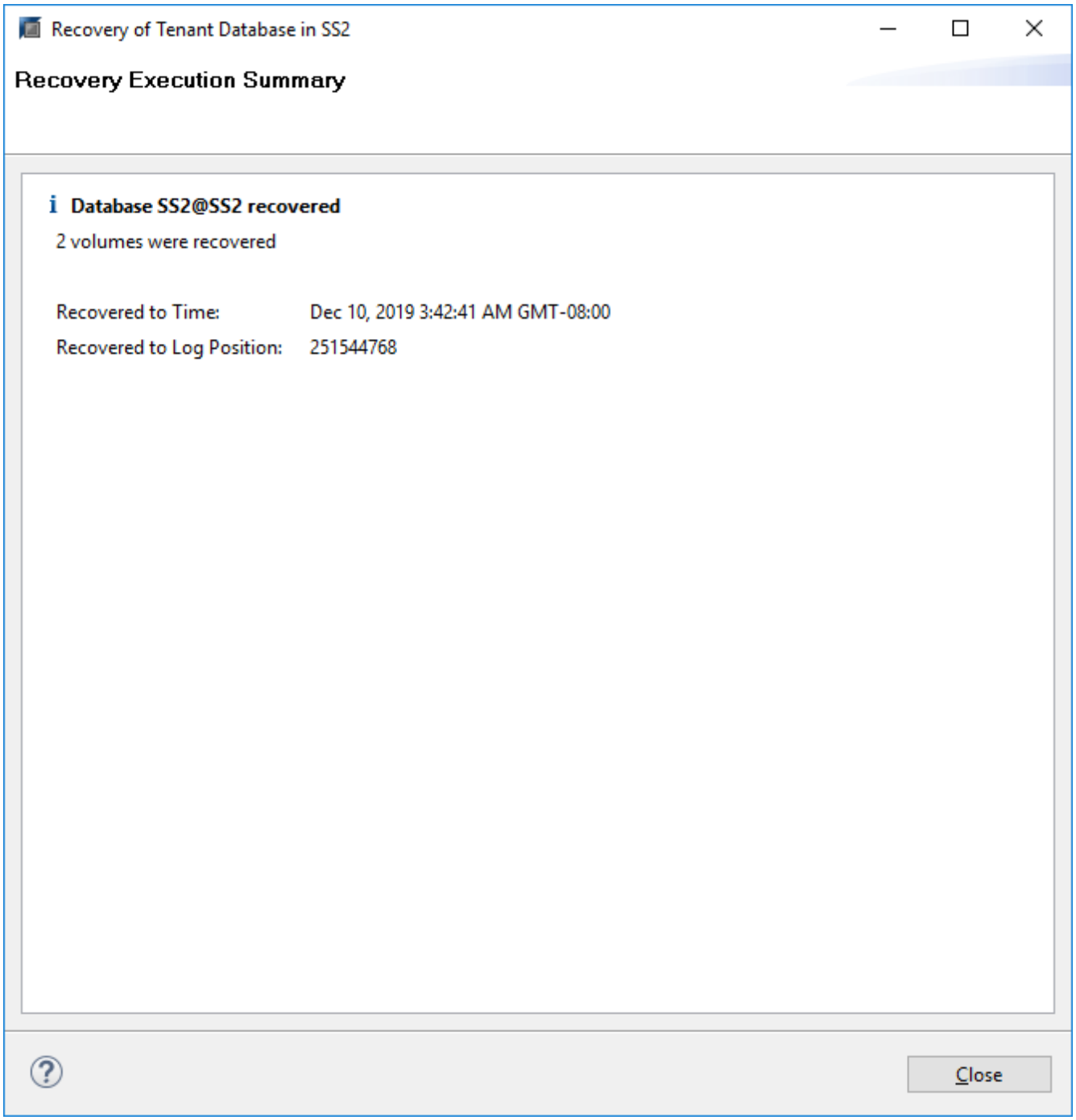
28. Wählen Sie je nach Bedarf andere Einstellungen aus. Stellen Sie sicher, dass Delta-Backups verwenden nicht ausgewählt ist. Klicken Sie Auf Weiter.



29. Überprüfen Sie die Wiederherstellungseinstellungen und starten Sie den Wiederherstellungsprozess der Mandantendatenbank, indem Sie auf Fertig stellen klicken.



30. Warten Sie, bis die Wiederherstellung abgeschlossen ist und die Mandantendatenbank gestartet wird.



Das SAP HANA System ist betriebsbereit.

> Bei einem SAP HANA MDC-System mit mehreren Mandanten müssen Sie die Schritte 20 bis 29 für jeden Mandanten wiederholen.

Erweiterte Konfiguration und Optimierung

In diesem Abschnitt werden Konfigurations- und Tuning-Optionen beschrieben, mit denen Kunden das SnapCenter Setup an ihre spezifischen Anforderungen anpassen können. Möglicherweise gelten nicht alle Einstellungen für alle Kundenszenarien.

Sichere Kommunikation mit HANA-Datenbank ermöglichen

Sind die HANA-Datenbanken mit sicherer Kommunikation konfiguriert `hdbsql` Der von SnapCenter ausgeführte Befehl muss zusätzliche Befehlszeilenoptionen verwenden. Dies kann mit einem Wrapper-Skript erreicht werden, das aufruft `hdbsql` Mit den erforderlichen Optionen.

> Es gibt verschiedene Optionen zur Konfiguration der SSL-Kommunikation. In den folgenden Beispielen wird die einfachste Client-Konfiguration mit der Befehlszeilenoption beschrieben, bei der keine Server-Zertifikatvalidierung durchgeführt wird. Wenn eine Zertifikatvalidierung auf Server- und/oder Client-Seite erforderlich ist, sind unterschiedliche hdbsql-Befehlszeilenoptionen erforderlich, und Sie müssen die PSE-Umgebung entsprechend konfigurieren, wie im SAP HANA Security Guide beschrieben.

Anstatt die zu konfigurieren `hdbsql` Ausführbar in `hana.properties` Dateien, das Wrapper-Skript wird hinzugefügt.

Für einen zentralen HANA-Plug-in-Host auf dem SnapCenter-Windows-Server müssen Sie den folgenden Inhalt in hinzufügen `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\hana.properties`.

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

Das Wrapper-Skript `hdbsql-ssl.cmd` Anrufe `hdbsql.exe` Mit den erforderlichen Befehlszeilenoptionen.

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

> Der `-e - ssltrustcert` Hdbsql-Befehlszeilenoption funktioniert auch für HANA-Systeme, bei denen SSL nicht aktiviert ist. Diese Option kann daher auch mit einem zentralen HANA-Plug-in-Host verwendet werden, auf dem nicht alle HANA-Systeme SSL aktiviert oder deaktiviert haben.

Wenn das HANA-Plug-in auf einzelnen HANA-Datenbank-Hosts implementiert wird, muss die Konfiguration auf jedem Linux-Host entsprechend vorgenommen werden.

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

Das Wrapper-Skript `hdbsqls` Anrufe `hdbsql` Mit den erforderlichen Befehlszeilenoptionen.

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

Deaktivieren Sie die automatische Erkennung auf dem HANA-Plug-in-Host

Gehen Sie wie folgt vor, um die automatische Erkennung auf dem HANA-Plug-in-Host zu deaktivieren:

1. Öffnen Sie auf dem SnapCenter-Server PowerShell. Stellen Sie eine Verbindung zum SnapCenter-Server her, indem Sie das ausführen `Open- SmConnection` Geben Sie im Anmeldefenster den Benutzernamen und das Passwort an.
2. Um die automatische Erkennung zu deaktivieren, führen Sie den aus `Set- SmConfigSettings` Befehl.

   Für einen HANA-Host `hana-2`, Der Befehl lautet wie folgt:

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

3. Überprüfen Sie die Konfiguration, indem Sie den ausführen `Get- SmConfigSettings` Befehl.

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

   Die Konfiguration wird in die Agent-Konfigurationsdatei auf dem Host geschrieben und ist nach einem Plug-in-Upgrade mit SnapCenter weiterhin verfügbar.

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

Deaktivieren der automatischen Backup-Organisation für Protokolle

Die allgemeine Ordnung und Sauberkeit der Protokollsicherung ist standardmäßig aktiviert und kann auf der HANA-Plug-in-Hostebene deaktiviert werden. Es gibt zwei Optionen, um diese Einstellungen zu ändern.

Bearbeiten Sie die Datei hana.property

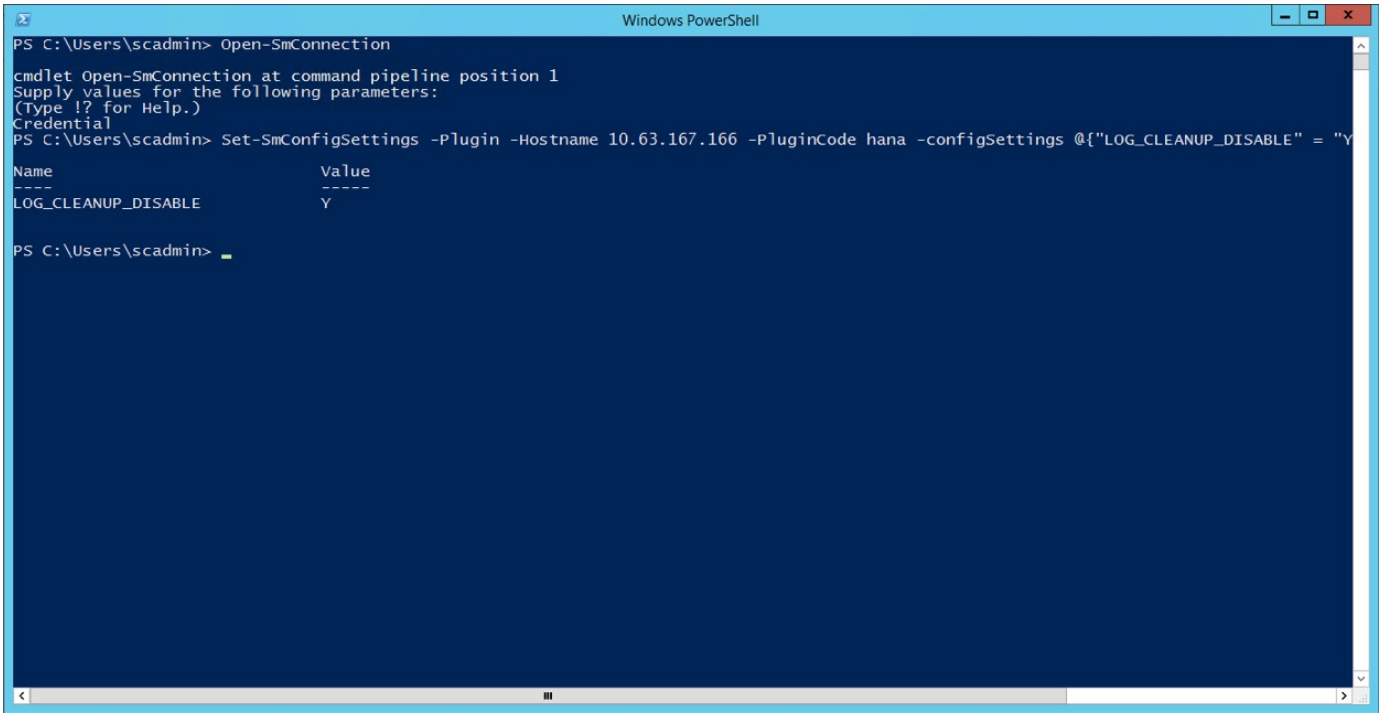
Einschließlich des Parameters `LOG_CLEANUP_DISABLE = Y` Im `hana.property` Die Konfigurationsdatei deaktiviert die allgemeine Ordnung und Sauberkeit der Protokollsicherung für alle Ressourcen, die diesen SAP HANA Plug-in-Host als Kommunikationshost verwenden:

- Für den Hdbsql Kommunikations-Host unter Windows, die `hana.property` Datei befindet sich unter `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc`.
- Für den Hdbsql-Kommunikations-Host unter Linux, die `hana.property` Datei befindet sich unter `/opt/NetApp/snapcenter/scc/etc`.

Verwenden Sie den PowerShell-Befehl

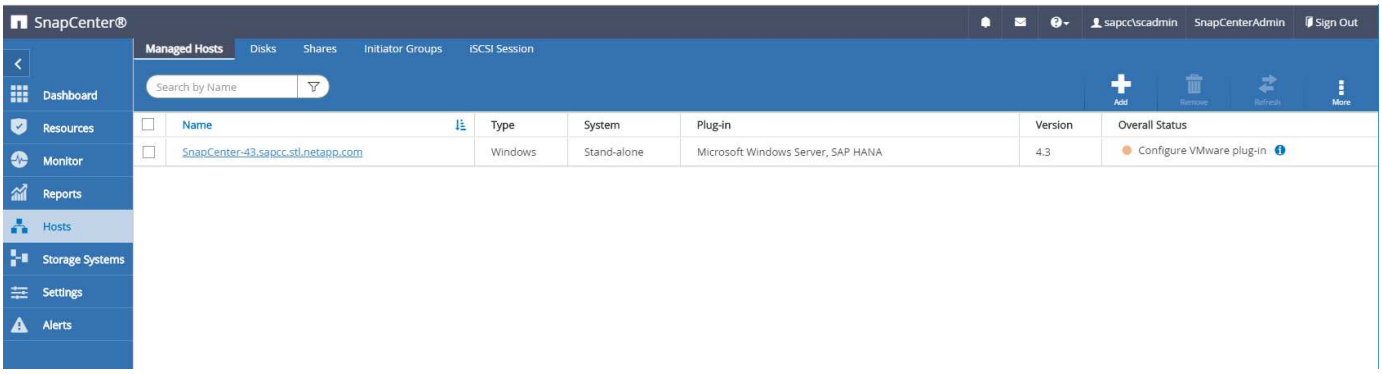
Eine zweite Option zum Konfigurieren dieser Einstellungen ist der SnapCenter PowerShell Befehl.

1. Öffnen Sie auf dem SnapCenter-Server eine PowerShell. Stellen Sie mit dem Befehl eine Verbindung zum SnapCenter-Server her `Open- SmConnection` Und geben Sie im Anmeldefenster den Benutzernamen und das Passwort an.
2. Mit dem Befehl `Set- SmConfigSettings -Plugin - HostName <pluginhostname> - PluginCode hana - configSettings @{"LOG_CLEANUP_DISABLE" = "Y"}`, Die Änderungen werden für den SAP HANA Plug-in-Host konfiguriert `<pluginhostname>` Durch den IP- oder Host-Namen angegeben (siehe folgende Abbildung).



Deaktivieren Sie die Warnung beim Ausführen des SAP HANA-Plug-ins in einer virtuellen Umgebung

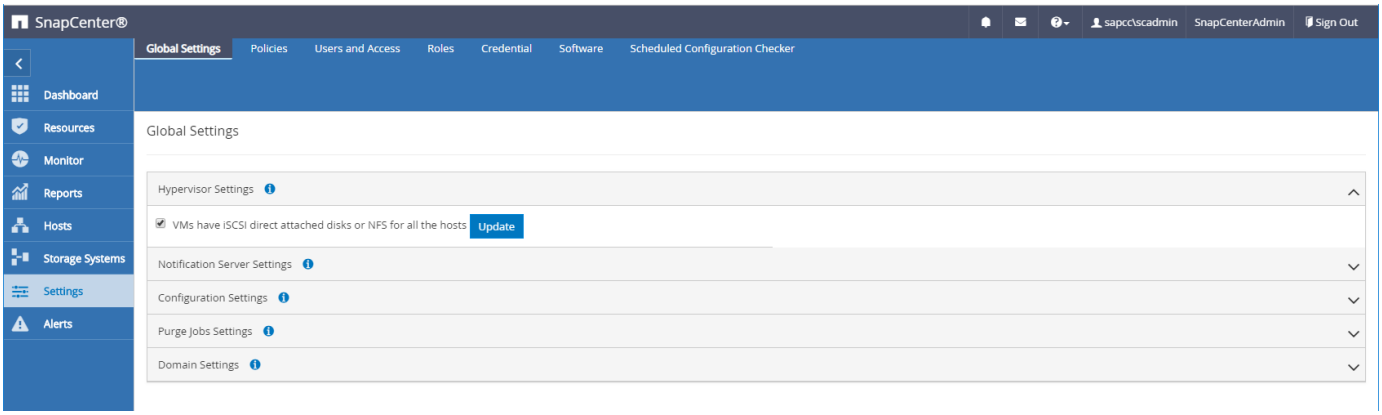
SnapCenter erkennt, ob das SAP HANA Plug-in in in einer virtualisierten Umgebung installiert ist. Dabei kann es sich um eine VMware Umgebung oder eine SnapCenter Installation bei einem Public Cloud Provider handelt. In diesem Fall zeigt SnapCenter eine Warnung für die Konfiguration des Hypervisors an, wie in der folgenden Abbildung dargestellt.



Diese Warnung kann global unterdrückt werden. In diesem Fall kennt SnapCenter virtualisierte Umgebungen nicht und weist daher keine derartigen Warnungen auf.

Um SnapCenter zu konfigurieren, um diese Warnung zu unterdrücken, muss die folgende Konfiguration angewendet werden:

1. Wählen Sie auf der Registerkarte Einstellungen die Option Globale Einstellungen.
2. Wählen Sie für die Hypervisor-Einstellungen die Option VMs mit iSCSI Direct Attached Disks oder NFS für alle Hosts aus, und aktualisieren Sie die Einstellungen.



Ändern Sie die Häufigkeit der Backup-Synchronisierung mit externen Backup-Storage

Wie im Abschnitt beschrieben "„Retention Management von Backups auf dem Sekundärspeicher“," Das Aufbewahrungsmanagement von Daten-Backups auf einer externen Backup-Ablage wird durch ONTAP übernommen. SnapCenter prüft regelmäßig, ob ONTAP Backups auf dem externen Backup-Storage gelöscht hat. Dazu wird ein Bereinigungsauftrag mit einem wöchentlichen Standardzeitplan ausgeführt.

Der SnapCenter-Bereinigungsauftrag löscht Backups im SnapCenter-Repository sowie im SAP HANA-Backup-Katalog, wenn gelöschte Backups im externen Backup-Speicher identifiziert wurden.

Der Bereinigungsauftrag führt auch die allgemeine Ordnung und Sauberkeit der SAP HANA-Log-Backups aus.

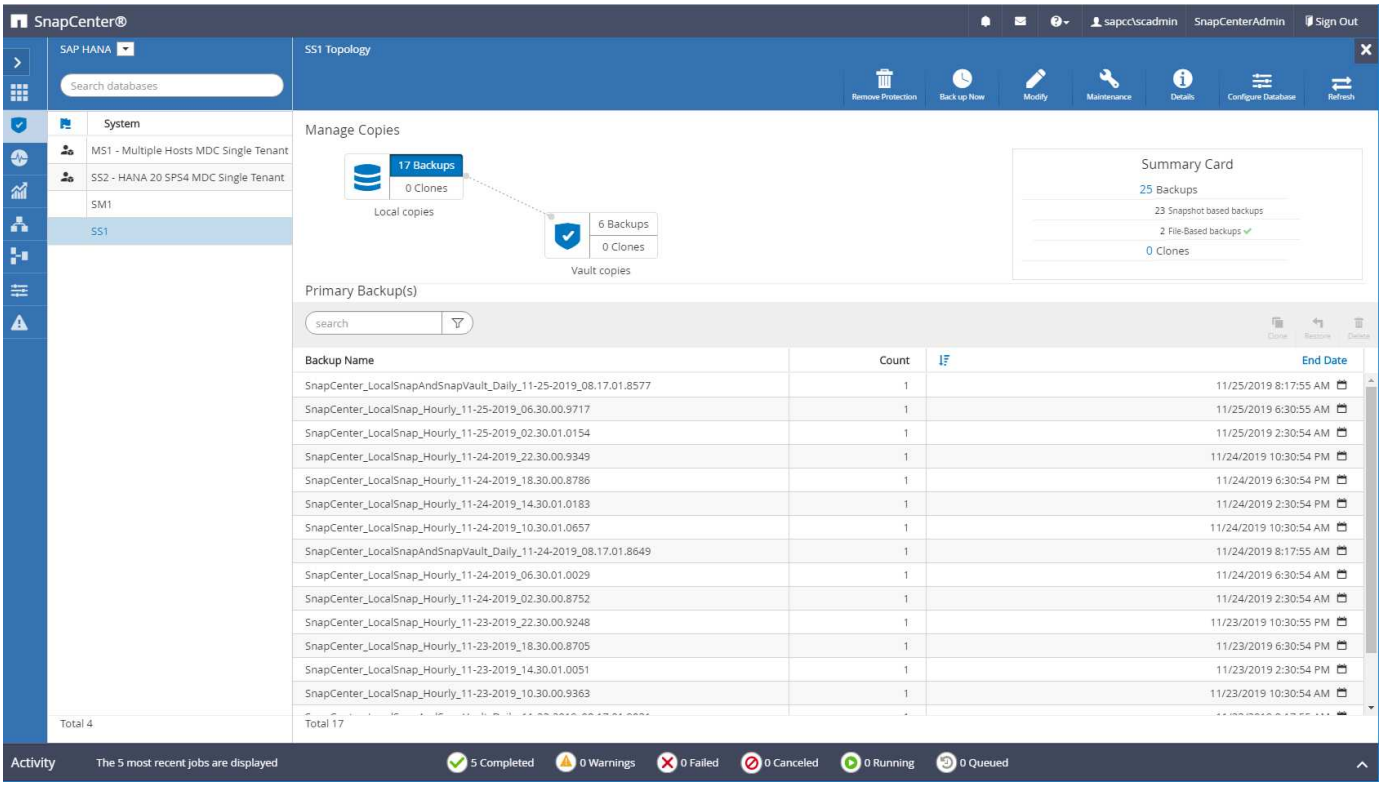
Bis diese geplante Bereinigung beendet ist, zeigen SAP HANA und SnapCenter noch Backups an, die bereits aus dem externen Backup-Storage gelöscht wurden.

> Dies kann zu zusätzlichen Protokoll-Backups führen, die aufbewahrt werden, selbst wenn die entsprechenden Storage-basierten Snapshot Backups auf dem externen Backup Storage bereits gelöscht wurden.

In den folgenden Abschnitten werden zwei Möglichkeiten beschrieben, um diese temporäre Diskrepanz zu vermeiden.

Manuelle Aktualisierung auf Ressourcenebene

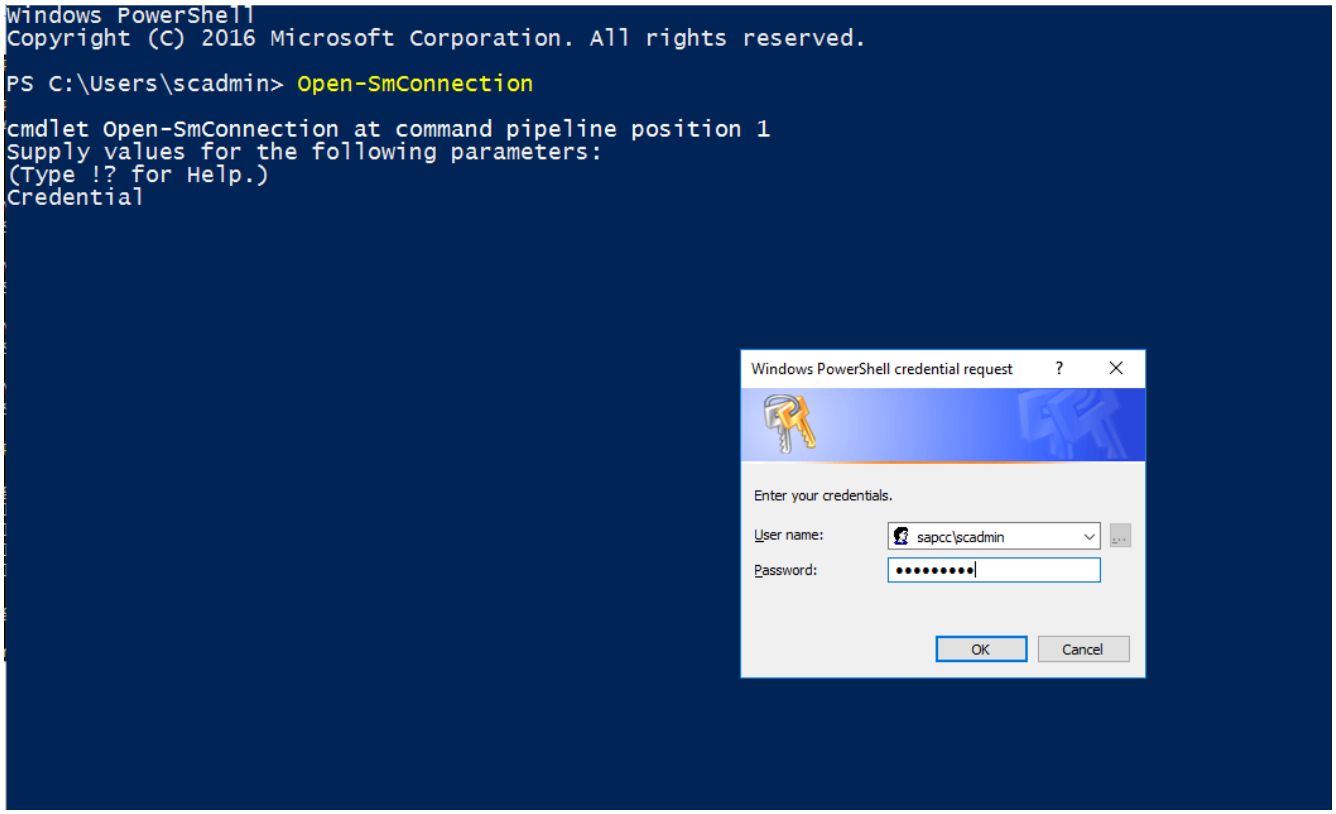
In der Topologieansicht einer Ressource zeigt SnapCenter bei der Auswahl der sekundären Backups die Backups auf dem externen Backup-Speicher an, wie im folgenden Screenshot dargestellt. SnapCenter führt eine Bereinigung mit dem Symbol „Aktualisieren“ aus, um die Backups für diese Ressource zu synchronisieren.



Ändern Sie die Häufigkeit des SnapCenter-Bereinigungsjobs

SnapCenter führt den Bereinigungsjob aus `SnapCenter_RemoveSecondaryBackup` Standardmäßig werden alle Ressourcen wöchentlich unter Verwendung des Windows-Arbeitsplanungsmechanismus verwendet. Dies kann mit einem SnapCenter PowerShell Cmdlet geändert werden.

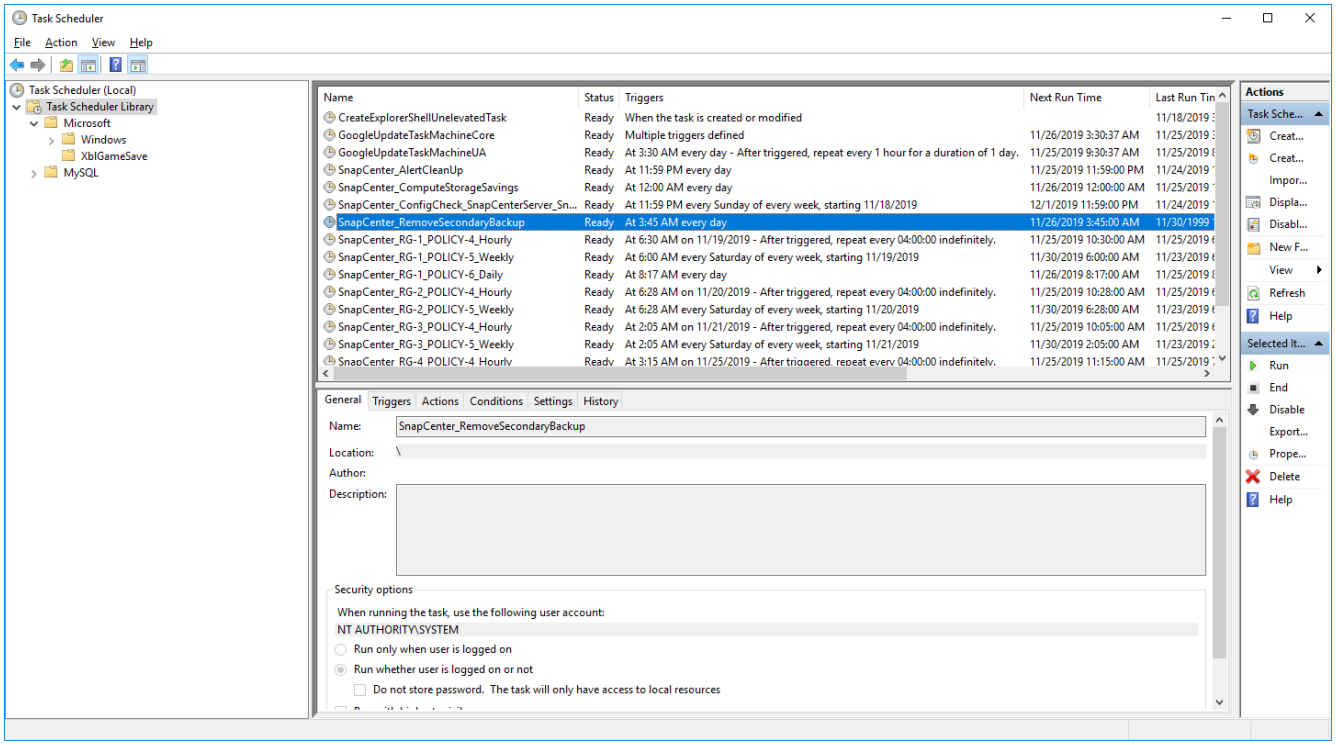
1. Starten Sie ein PowerShell Befehlsfenster auf dem SnapCenter-Server.
2. Öffnen Sie die Verbindung zum SnapCenter-Server, und geben Sie im Anmeldefenster die Anmeldedaten des SnapCenter-Administrators ein.



3. Um den Zeitplan von einer Woche auf eine tägliche Basis zu ändern, verwenden Sie das Cmdlet `Set-SmSchedule`.

```
PS C:\Users\scadmin> Set-SmSchedule -ScheduleInformation
@{"ScheduleType"="Daily";"StartTime"="03:45 AM";"DaysInterval"=
"1"} -TaskName SnapCenter_RemoveSecondaryBackup
TaskName              : SnapCenter_RemoveSecondaryBackup
Hosts                 : {}
StartTime             : 11/25/2019 3:45:00 AM
DaysoftheMonth        :
MonthsofTheYear       :
DaysInterval          : 1
DaysOfTheWeek         :
AllowDefaults         : False
ReplaceJobIfExist     : False
UserName              :
Password              :
SchedulerType         : Daily
RepeatTask_Every_Hour :
IntervalDuration      :
EndTime               :
LocalScheduler        : False
AppType               : False
AuthMode              :
SchedulerSQLInstance  : SMCoreContracts.SmObject
MonthlyFrequency      :
Hour                  : 0
Minute                : 0
NodeName              :
ScheduleID            : 0
RepeatTask_Every_Mins :
CronExpression        :
CronOffsetInMinutes   :
StrStartTime          :
StrEndTime            :
PS C:\Users\scadmin> Check the configuration using the Windows Task
Scheduler.
```

4. Sie können die Job-Eigenschaften im Windows Task Scheduler überprüfen.



Wo finden Sie weitere Informationen und Versionsverlauf

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- Seite „SnapCenter Ressourcen“

  "https://www.netapp.com/us/documentation/snapcenter-software.aspx"

- SnapCenter-Softwaredokumentation

  "https://docs.netapp.com/us-en/snapcenter/index.html"

- TR-4667: Automatisierung von SAP Systemkopien mit dem SnapCenter

  https://www.netapp.com/pdf.html?item=/media/17111-tr4667pdf.pdf

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

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

- TR-4018: Integration von NetApp ONTAP-Systemen in SAP Landscape Management

  https://www.netapp.com/pdf.html?item=/media/17195-tr4018pdf.pdf

- TR-4646: SAP HANA Disaster Recovery with Storage Replication

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

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	Juli 2017	• Erste Version.
Version 1.1	September 2017	• Der Abschnitt „Erweiterte Konfiguration und Anpassung“ wurde hinzugefügt. • Kleinere Korrekturen.
Version 2.0	März 2018	• Updates zu SnapCenter 4.0: Neue Ressource für das Datenvolumen Verbesserte SnapRestore-Operation einer einzelnen Datei
Version 3.0	Januar 2020	• Der Abschnitt „SnapCenter-Konzepte und Best-Practices“ wurde hinzugefügt. • Updates zu SnapCenter 4.3: Automatische Erkennung Automatisiertes Restore und Recovery Unterstützung für HANA MDC mehrere Mandanten Wiederherstellung eines Mandanten
Version 3.1	Juli 2020	• Kleinere Aktualisierungen und Korrekturen: NFSv4-Unterstützung mit SnapCenter 4.3.1 Konfiguration der SSL-Kommunikation Zentrale Plug-in-Implementierung für Linux auf IBM Power
Version 3.2	November 2020	• Die erforderlichen Benutzerberechtigungen für die Datenbank für HANA 2.0 SPS5 wurden hinzugefügt.
Version 3.3	Mai 2021	• Der Abschnitt SSL-hdbsql-Konfiguration wurde aktualisiert. • Linux LVM-Unterstützung hinzugefügt.

Version	Datum	Versionsverlauf des Dokuments
Version 3.4	August 2021	• Die Konfigurationsbeschreibung für die automatische Ermittlung deaktivieren wurde hinzugefügt.
Version 3.5	Februar 2022	• Kleinere Updates zu SnapCenter 4.6 und Unterstützung von automatischer Erkennung für HANA-Systeme mit Systemreplizierung

BlueXP Backup and Recovery for SAP HANA – Cloud-Objekt-Storage als Backup-Ziel

BlueXP Backup and Recovery for SAP HANA – Cloud-Objekt-Storage als Backup-Ziel

Überblick

In diesem Dokument wird beschrieben, wie Sie SAP HANA für die Datensicherung mit NetApp BlueXP einrichten und konfigurieren – von lokalen bis hin zu Cloud-basierten Objektspeichern. Sie deckt den Backup- und Recovery-Teil der Lösung von BlueXP ab. Diese Lösung ist eine Erweiterung der lokalen SAP HANA Backup-Lösung mit NetApp Snap Center und bietet eine kostengünstige Möglichkeit für die langfristige Archivierung von SAP HANA-Backups in Cloud-basiertem Objekt-Storage. Außerdem bietet sie optionales Tiering von Objekt-Storage in Archiv-Storage wie AWS Glacier/Deep Glacier, Microsoft Azure Blob Archive und GCP Archive Storage.

Die Einrichtung und Konfiguration der lokalen SAP HANA Backup- und Recovery-Lösung wird in beschrieben "TR-4614: SAP HANA Backup und Recovery mit SnapCenter (netapp.com)".

In dieser TR wird nur beschrieben, wie Sie die lokale SnapCenter-basierte SAP HANA Backup- und Recovery-Lösung mit BlueXP Backup und Recovery für SAP HANA erweitern können. Dabei kommen z. B. AWS S3 Objekt-Storage zum Einsatz. Das Setup und die Konfiguration mit Microsoft Azure und GCP-Objekt-Storage statt AWS S3 ist ähnlich, wird in diesem Dokument aber nicht beschrieben.

BlueXP Backup- und Recovery-Architektur

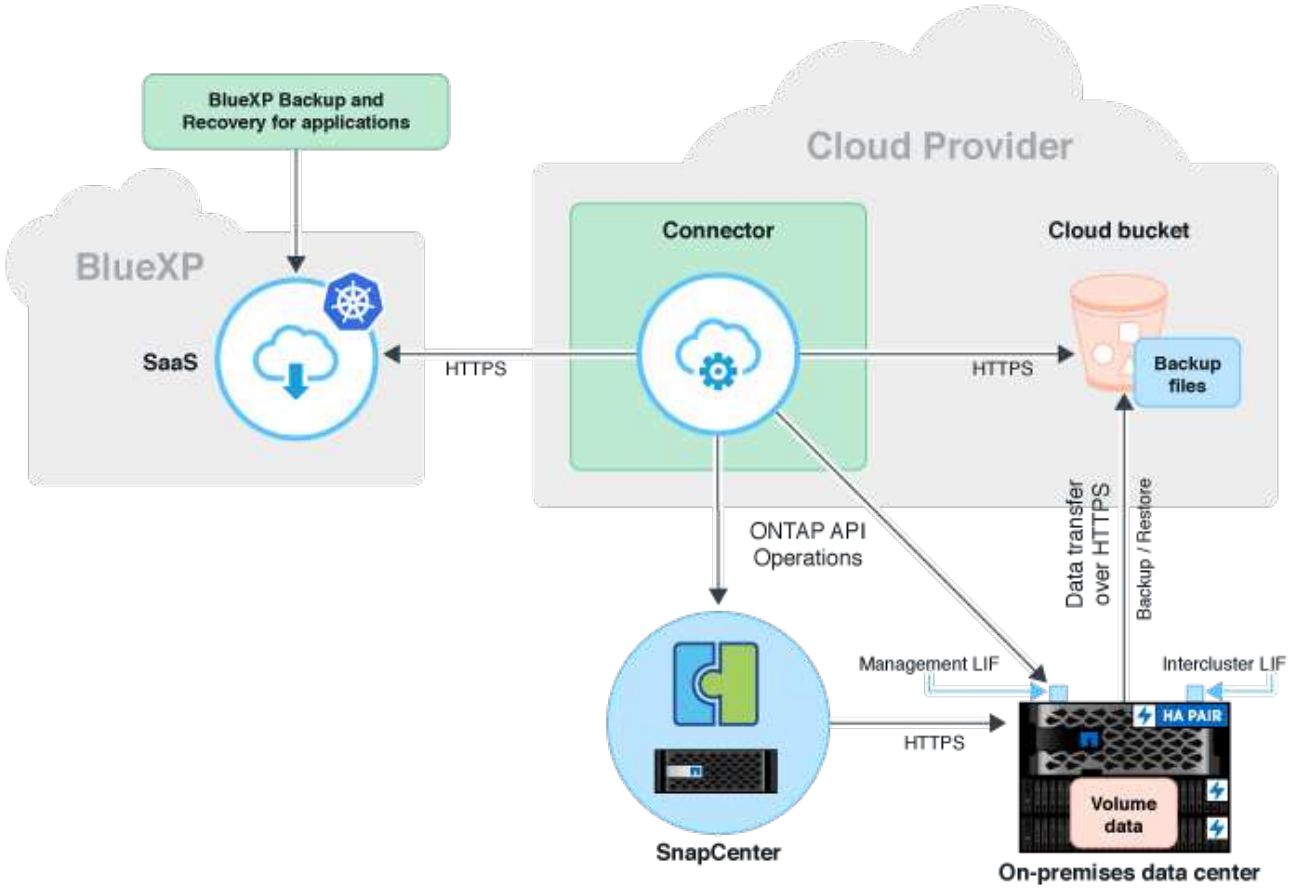
BlueXP Backup und Recovery ist eine SaaS-Lösung mit Datensicherungsfunktionen für Applikationen, die auf NetApp On-Premises-Storage in der Cloud ausgeführt werden. SAP HANA wird mithilfe von NetApp Storage effizient, applikationskonsistent und richtlinienbasiert gesichert. Darüber hinaus ermöglicht BlueXP Backup- und Recovery-Funktionen zentrale Kontrolle und Übersicht. Gleichzeitig werden Benutzern das Management applikationsspezifischer Backup- und Restore-Vorgänge delegiert.

BlueXP Backup und Recovery läuft in NetApp BlueXP als SaaS und nutzt das Framework und die UI. Das BlueXP Arbeitsumgebungs-Framework wird verwendet, um die Zugangsdaten für NetApp ONTAP auf Basis des lokalen Storage und des NetApp SnapCenter Servers zu konfigurieren und zu managen.

Ein BlueXP Connector muss innerhalb des virtuellen Netzwerks des Kunden implementiert werden. Es ist eine

Verbindung zwischen der lokalen Umgebung und der Cloud-Umgebung erforderlich, z. B. eine Site-to-Site-VPN-Verbindung. Die Kommunikation zwischen den NetApp-SaaS-Komponenten und der Kundenumgebung erfolgt ausschließlich über den Konnektor. Der Connector führt die Storage-Vorgänge mithilfe der ONTAP und SnapCenter Management-APIs aus.

Der Datentransfer zwischen dem lokalen Storage und dem Cloud-Bucket ist vollständig gesichert mit AES-256-Bit-Verschlüsselung im Ruhezustand, TLS/HTTPS-Verschlüsselung bei der Übertragung und CMK-Unterstützung (Customer Managed Key).
Die gesicherten Daten werden in einem unveränderlichen und nicht löschbaren WORM-Zustand gespeichert. Die einzige Möglichkeit, auf die Daten aus dem Objekt-Storage zuzugreifen, besteht darin, sie in NetApp ONTAP-basiertem Storage wiederherzustellen, einschließlich NetApp CVO.



Überblick über die Installations- und Konfigurationsschritte

Die erforderlichen Installations- und Konfigurationsschritte lassen sich in drei Bereiche aufteilen. Voraussetzung ist, dass die SAP HANA-Backup-Konfiguration im NetApp Snap Center konfiguriert ist. Für die Einrichtung von Snap Center für SAP HANA in erster Linie auf "SnapCenter-Konfiguration (netapp.com)".

1. Installation und Konfiguration von NetApp BlueXP Komponenten

   Muss einmal während der ersten Einrichtung der Datensicherungslösung durchgeführt werden.

2. Vorbereitungsschritte bei NetApp SnapCenter.

   Muss für jede SAP HANA-Datenbank durchgeführt werden, die geschützt werden sollte.

3. Konfigurationsschritte bei BlueXP Backup und Recovery.

   Muss für jede SAP HANA-Datenbank durchgeführt werden, die geschützt werden sollte.

Installation und Konfiguration von NetApp BlueXP Hybrid-Applikations-Backup

Die Installation und Konfiguration der NetApp BlueXP Komponenten finden Sie in "Sichern Sie Ihre On-Premises-Applikationsdaten in der NetApp Dokumentation".

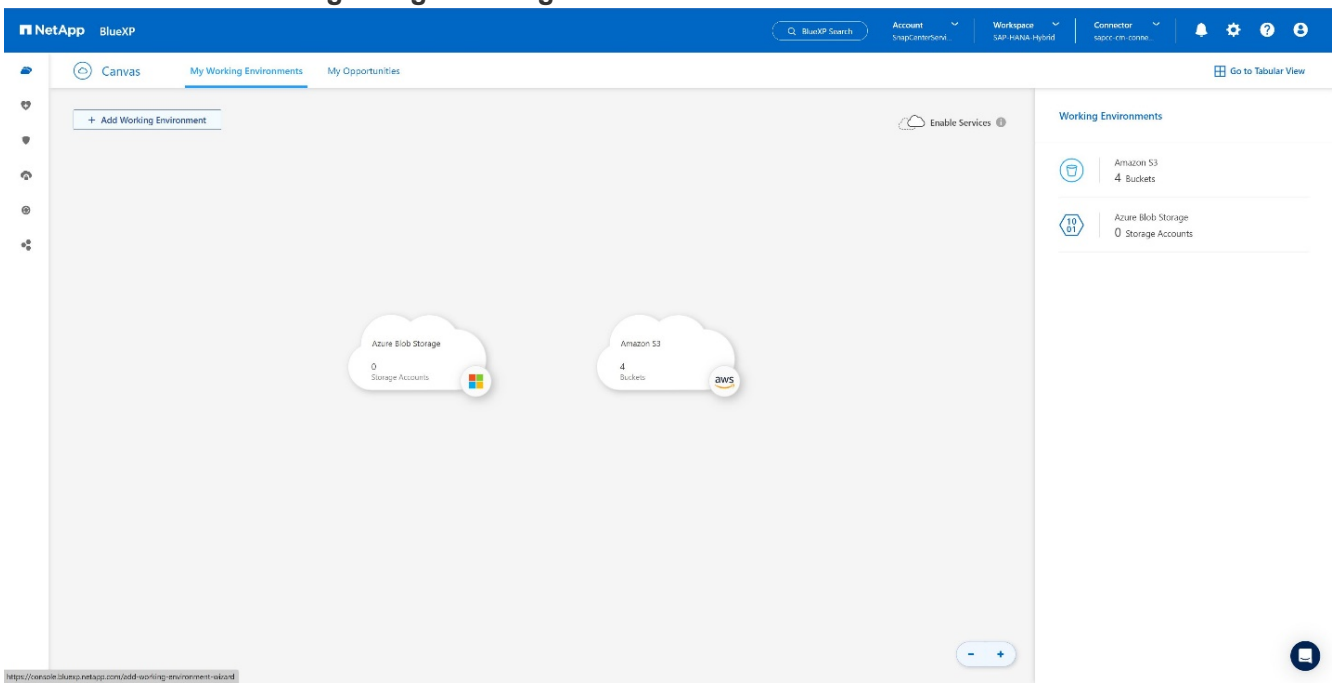
1. Melden Sie sich bei BlueXP an und richten Sie ein NetApp Konto ein unter https://bluexp.netapp.com/.
2. Implementieren Sie den BlueXP Connector in Ihrer Umgebung. Beschreibung ist verfügbar unter "Weitere Informationen zu Steckverbindern finden Sie in der NetApp-Dokumentation".
3. Cloud-Backup-Lizenz bei BlueXP hinzufügen/kaufen: https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-licensing-cloud-backup.html.
4. Schaffen Sie eine Arbeitsumgebung für Ihre On-Premises-Umgebung in NetApp und Ihr Cloud-Ziel in BlueXP durch Hinzufügen Ihres lokalen Storage.
5. Erstellen einer neuen Objektspeicher-Beziehung für den On-Premises-Storage in einen AWS S3 Bucket
6. SAP HANA-Systemressource bei SnapCenter konfigurieren
7. Fügen Sie Snap Center zu Ihrer Arbeitsumgebung hinzu.
8. Erstellen Sie eine Richtlinie für Ihre Umgebung.
9. Sicherung Ihres SAP HANA-Systems

Konfigurieren von BlueXP Backup und Recovery für SAP HANA

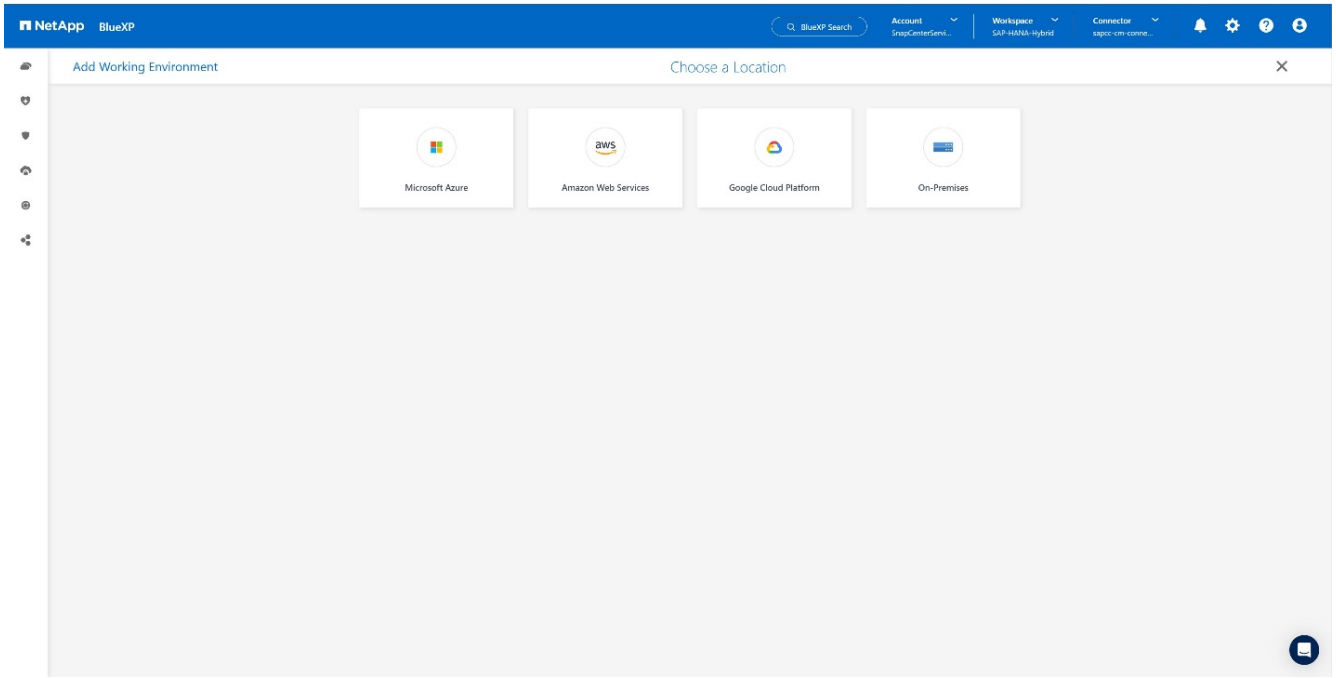
Arbeitsumgebung für BlueXP erstellen

Fügen Sie das lokale Storage-System zu Ihrer Arbeitsumgebung hinzu.

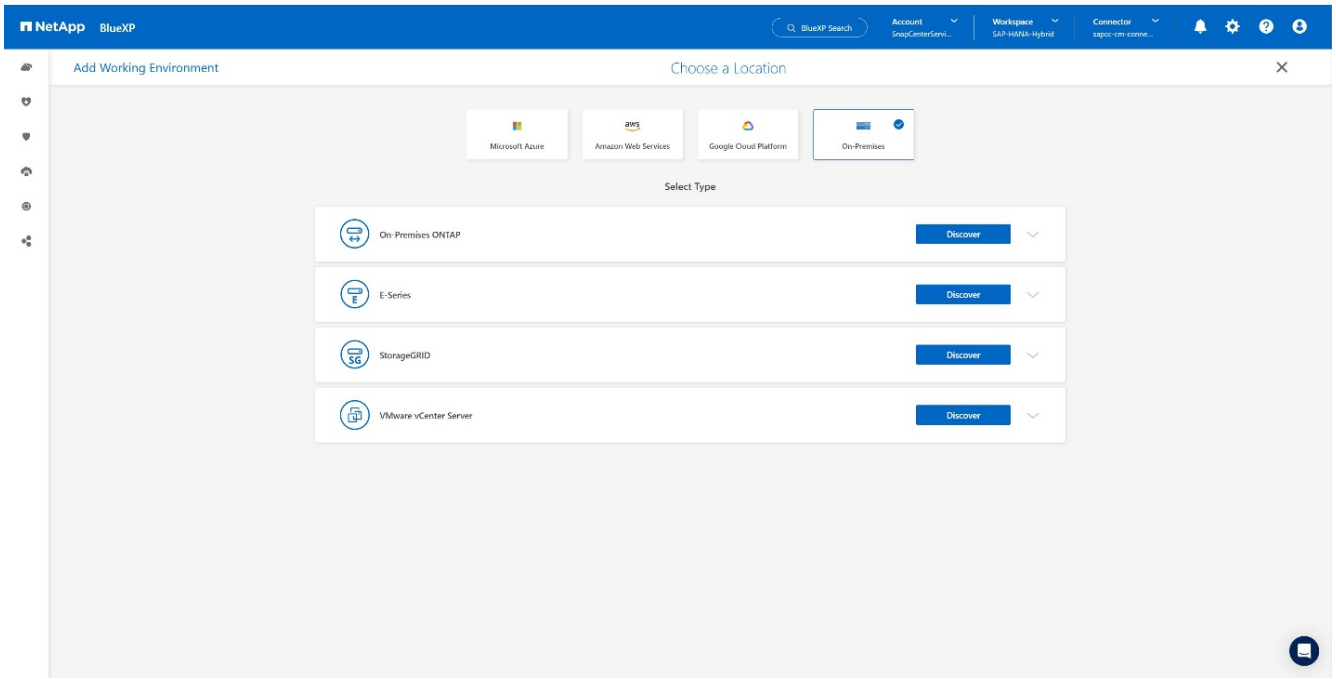
1. Wählen Sie im linken Menü **Storage** → **Canvas** → **My Working** Umgebung.
2. Drücken Sie **+ Arbeitsumgebung Hinzufügen**.



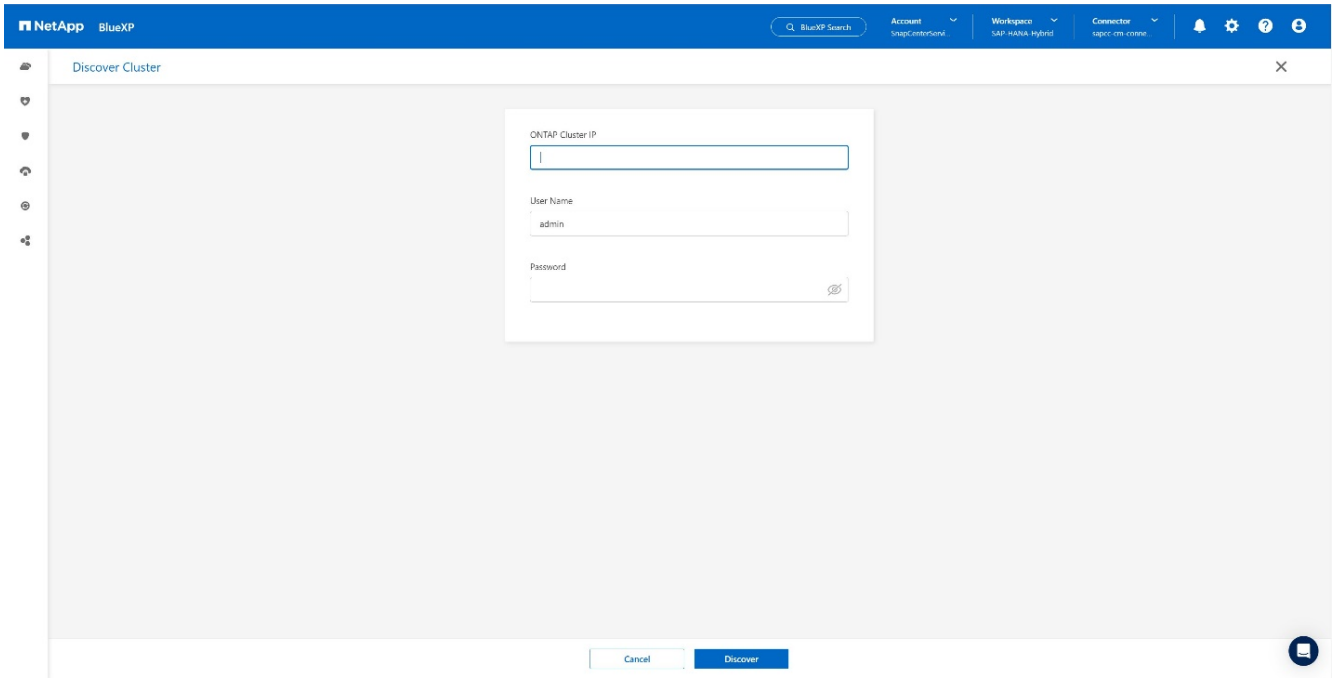
3. Wählen Sie **On-Premises**.



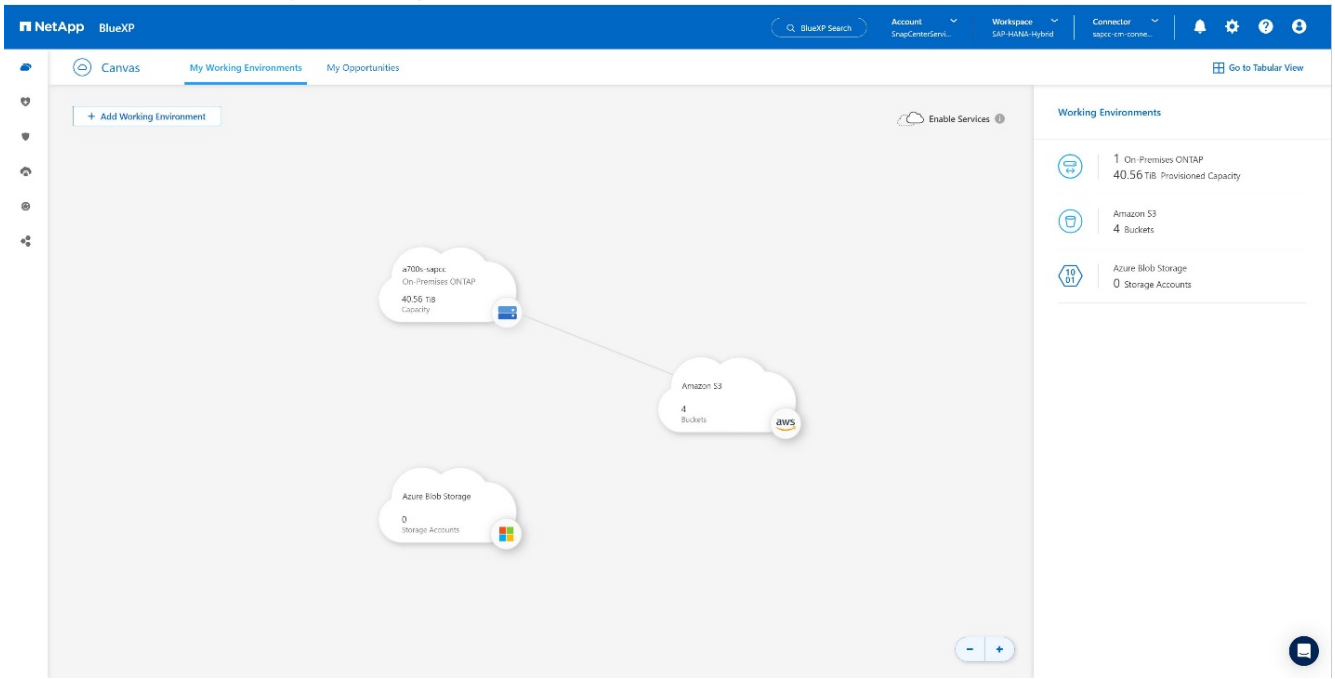
4. Wählen Sie **Entdecken Sie die On-Premises-ONTAP**.



5. Geben Sie die IP-Adresse des ONTAP-Clusters und das Passwort ein und drücken Sie **Discover**.



6. Der ONTAP Cluster ist jetzt verfügbar.

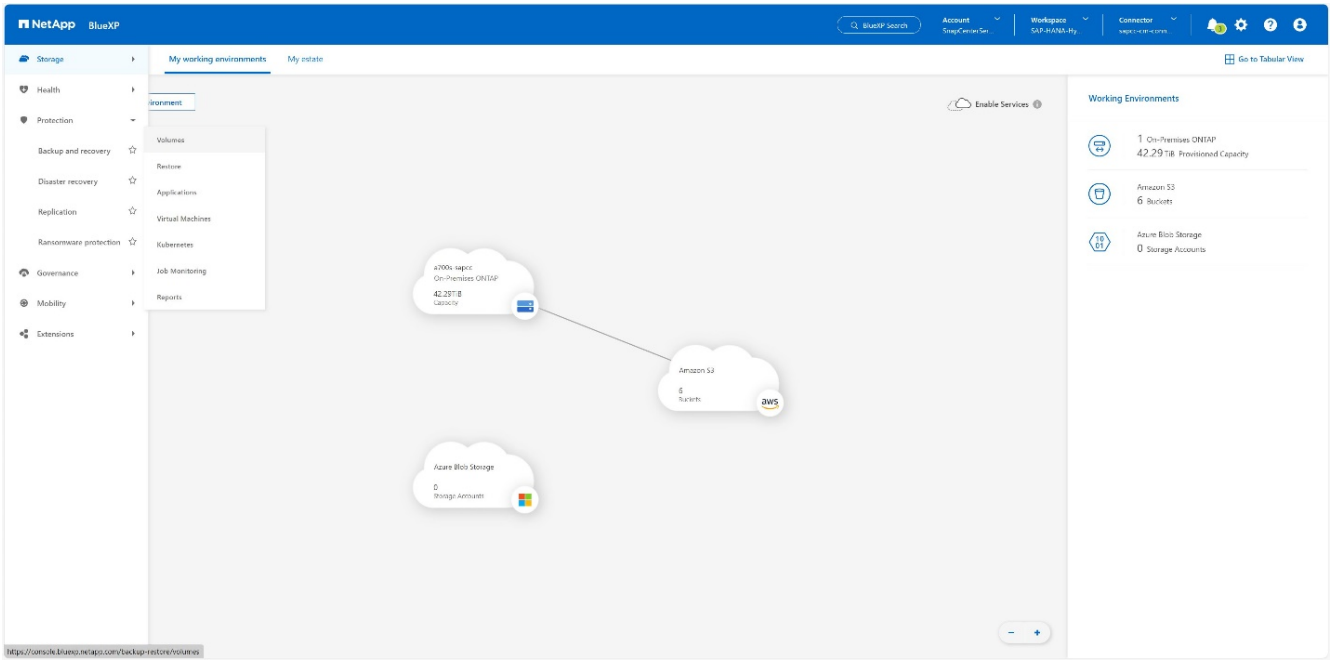


Erstellen einer Beziehung zwischen dem lokalen Storage-System und einem Objekt-Storage-Bucket

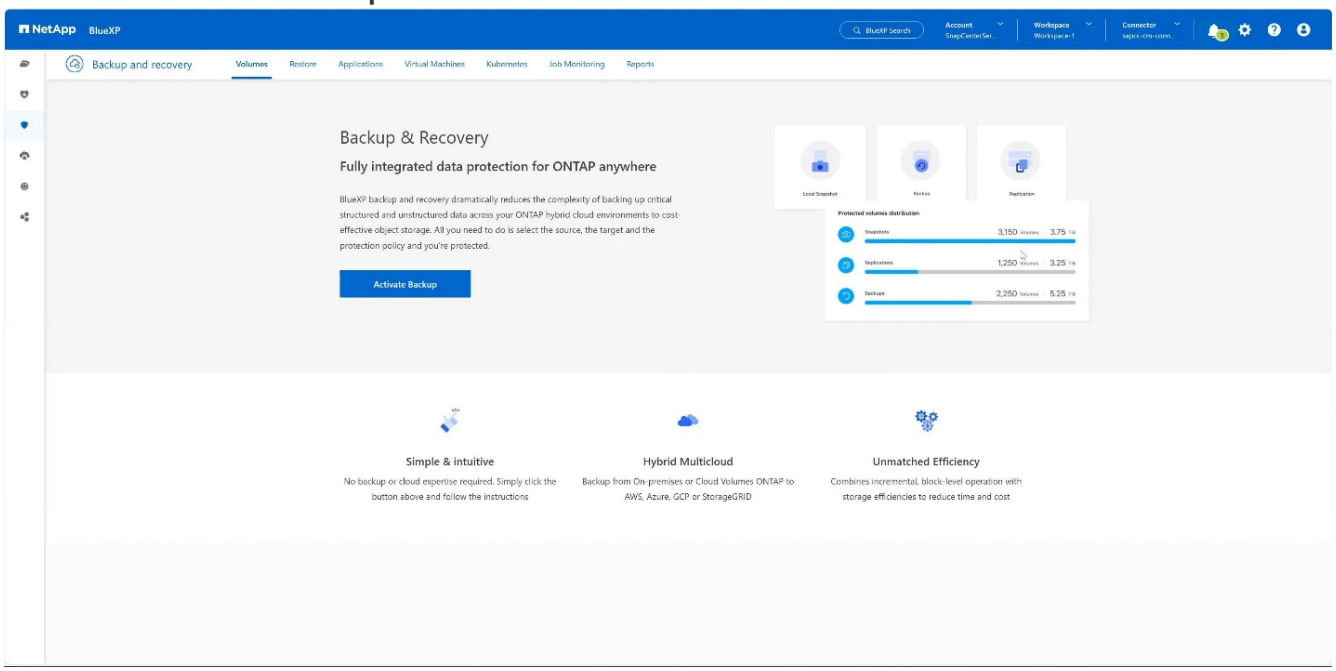
Die Beziehung zwischen dem On-Premises-Storage und dem S3-Bucket wird entweder ein Backup für ein Volume oder ein Backup einer Applikation erstellt. Soll ein vorhandenes Standort-zu-Standort-VPN für die Übertragung der Daten von On-Premises zu S3 verwendet werden, muss ein Volume-Backup zum Erstellen der Beziehung zwischen dem lokalen Storage und dem S3-Bucket verwendet werden, während VPC-Endpunkte verwendet werden müssen.
Bei Erstellung dieser Dokumentation bietet der Applikations-Backup-Workflow keine VPC-Endpunkte für den Zugriff auf S3 Buckets.
Siehe "Gateway-Endpunkte für Amazon S3 – Amazon Virtual Private Cloud" Einrichten von VPC-Endpunkten für S3 innerhalb der VPC

So erstellen Sie ein erstes Volume-Backup:

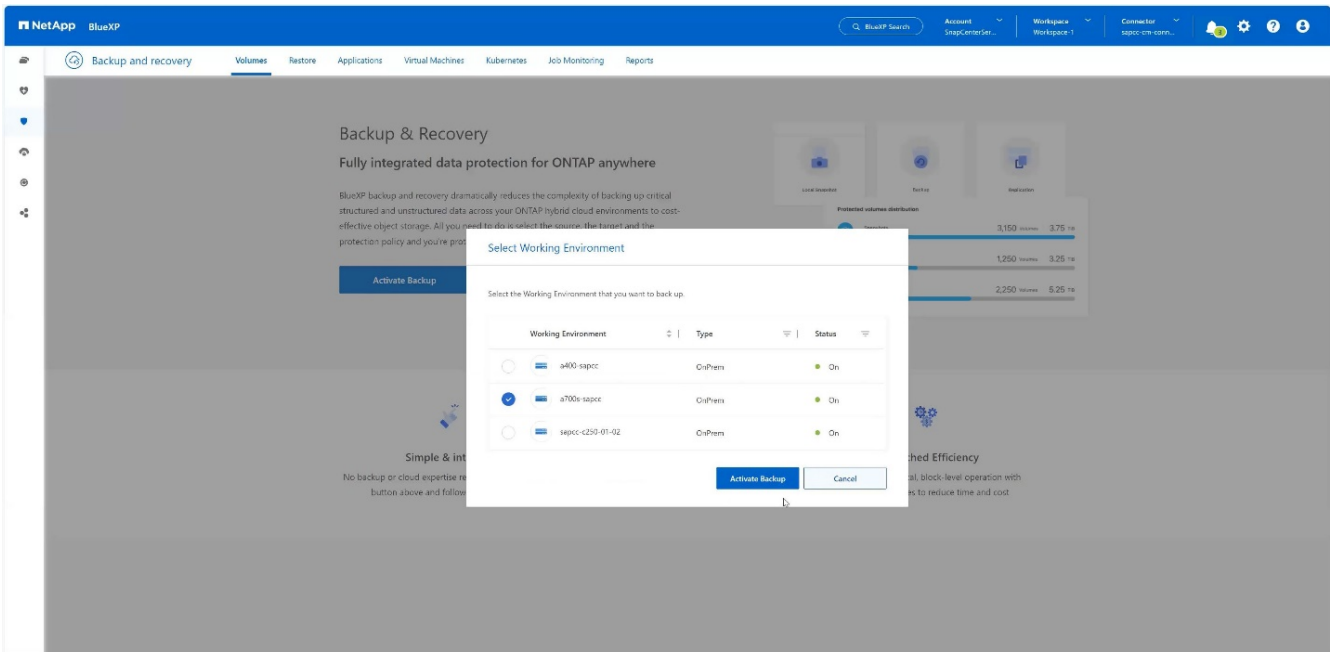
1. Navigieren Sie über **Protection** zu **Backup und Recovery** und wählen Sie **Volumes**.



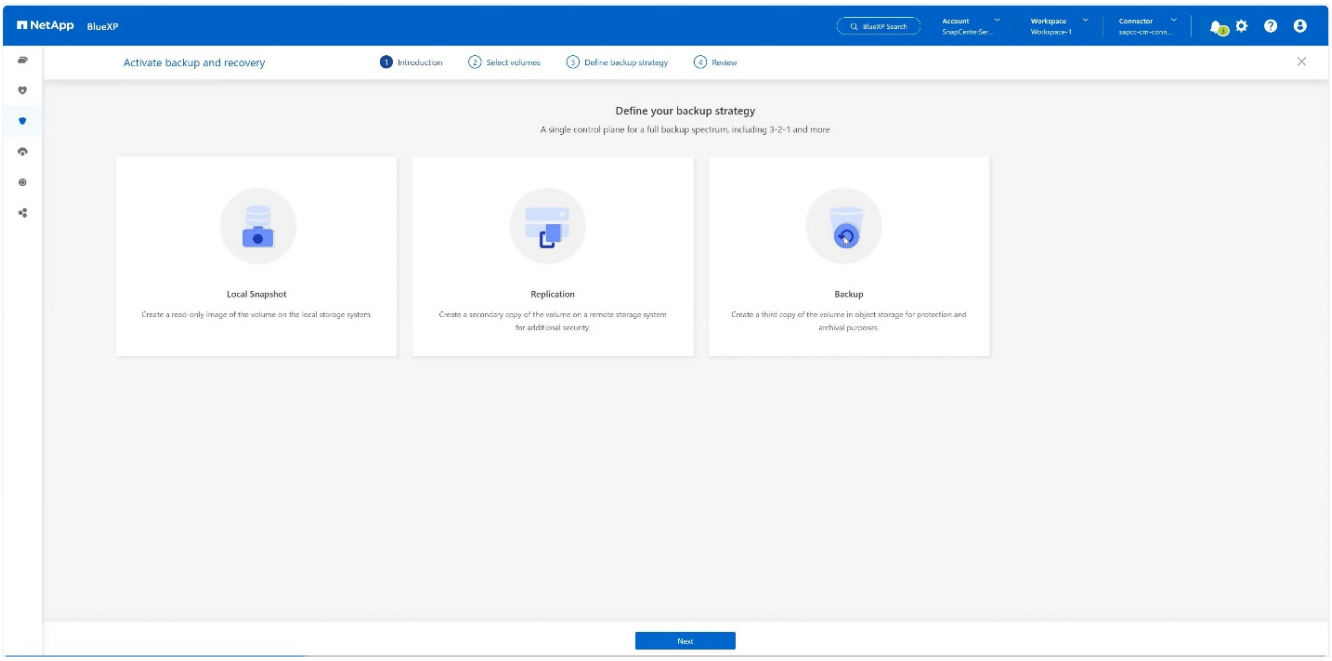
2. Drücken Sie die Taste **Backup aktivieren**.



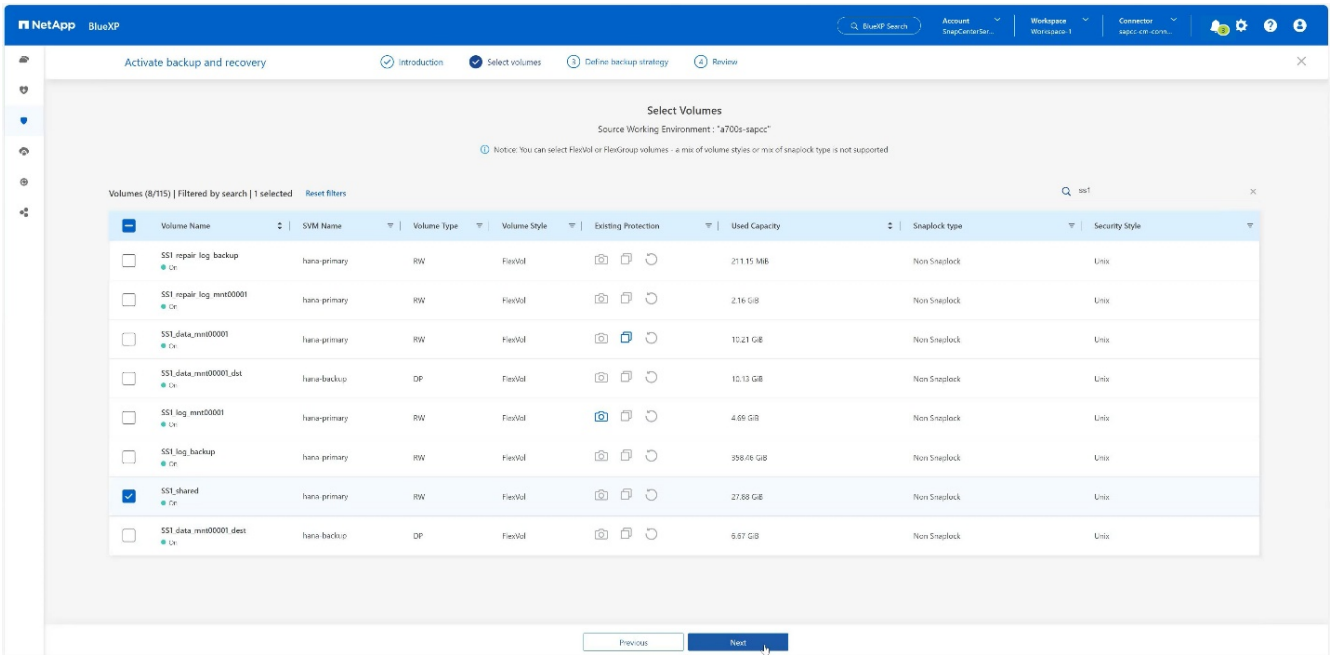
3. Wählen Sie das gewünschte lokale Speichersystem aus und klicken Sie auf **Backup aktivieren**.



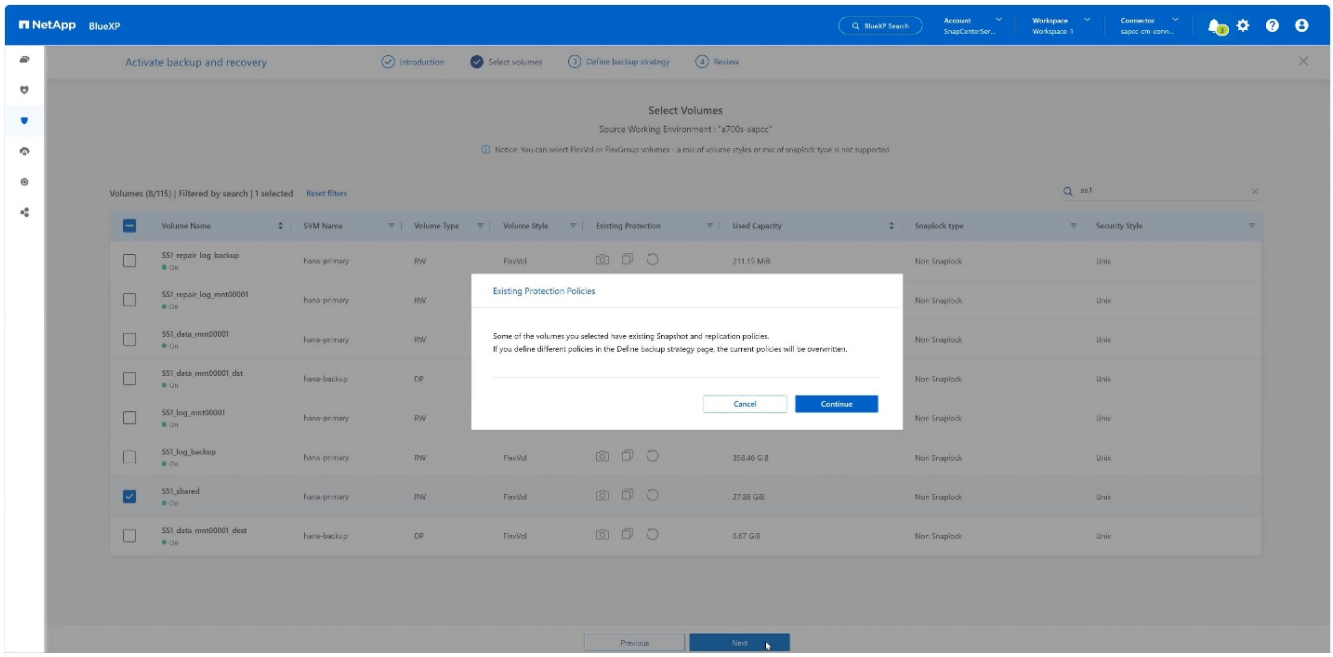
4. Wählen Sie **Backup**.



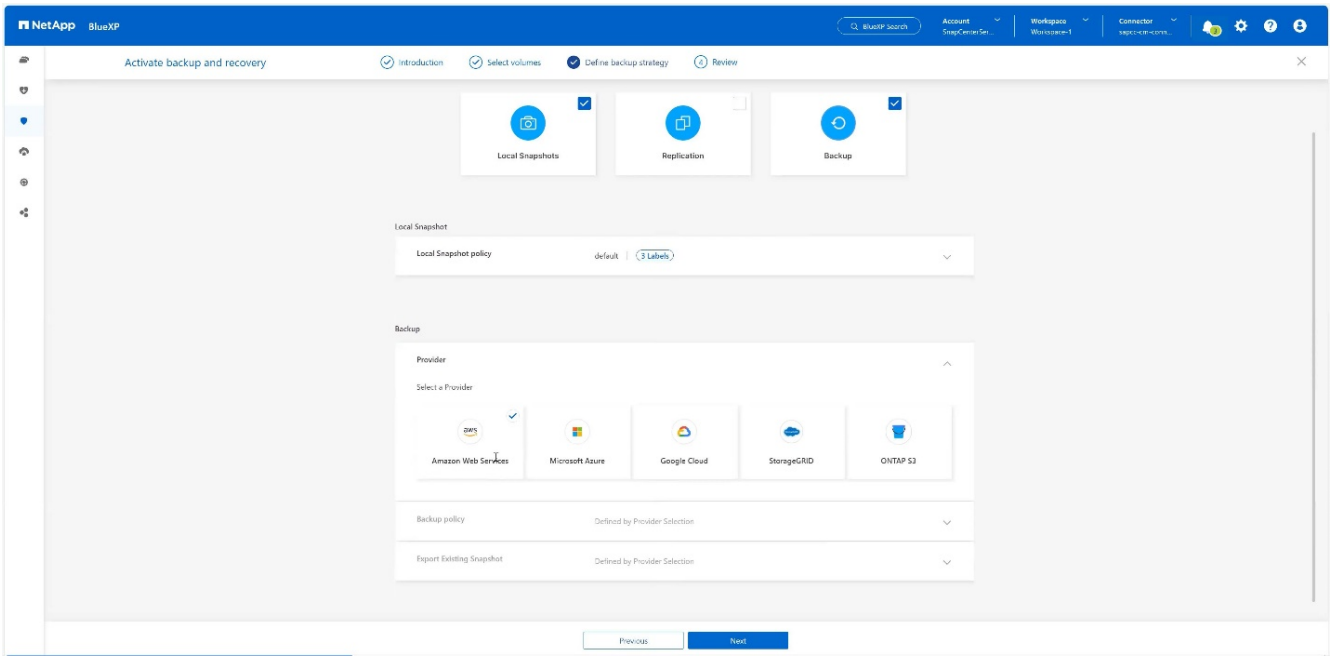
5. Wählen Sie ein Volume, das auf derselben SVM wie Ihre SAP HANA-Datendateien gespeichert ist, und drücken Sie **Weiter**. In diesem Beispiel wurde das Volume für /hana/shared ausgewählt.



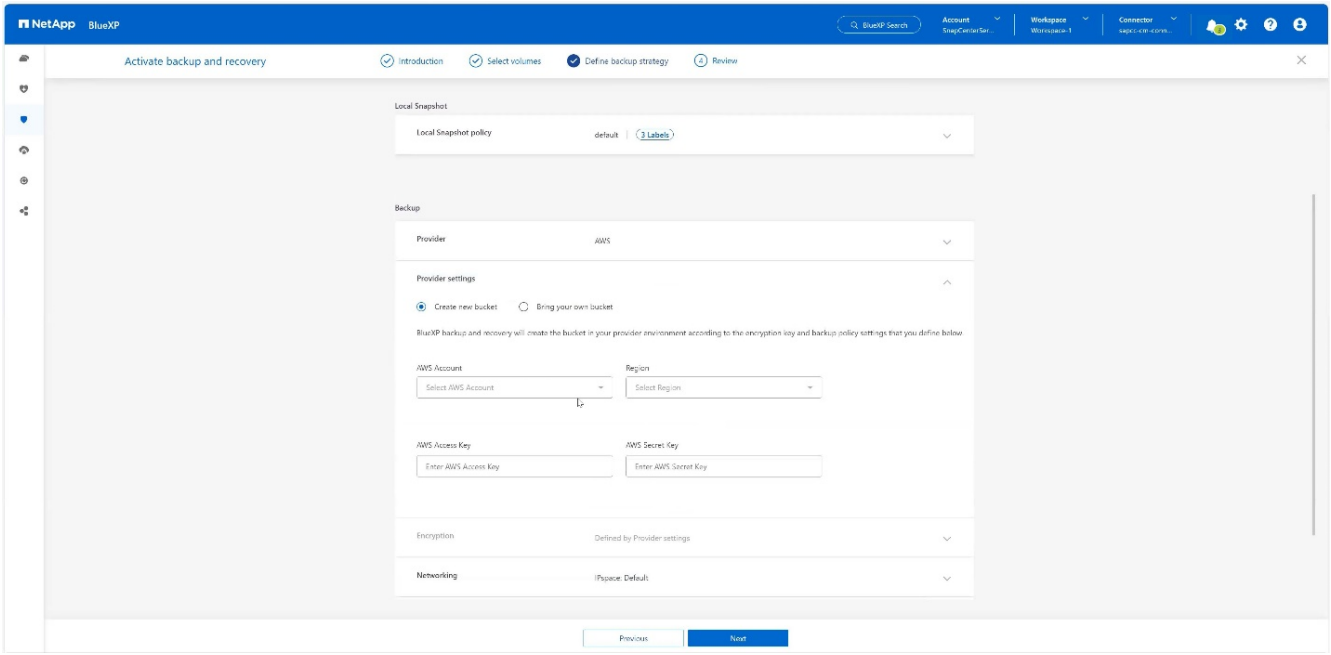
6. **Weiter**, wenn eine bestehende Richtlinie vorhanden ist.



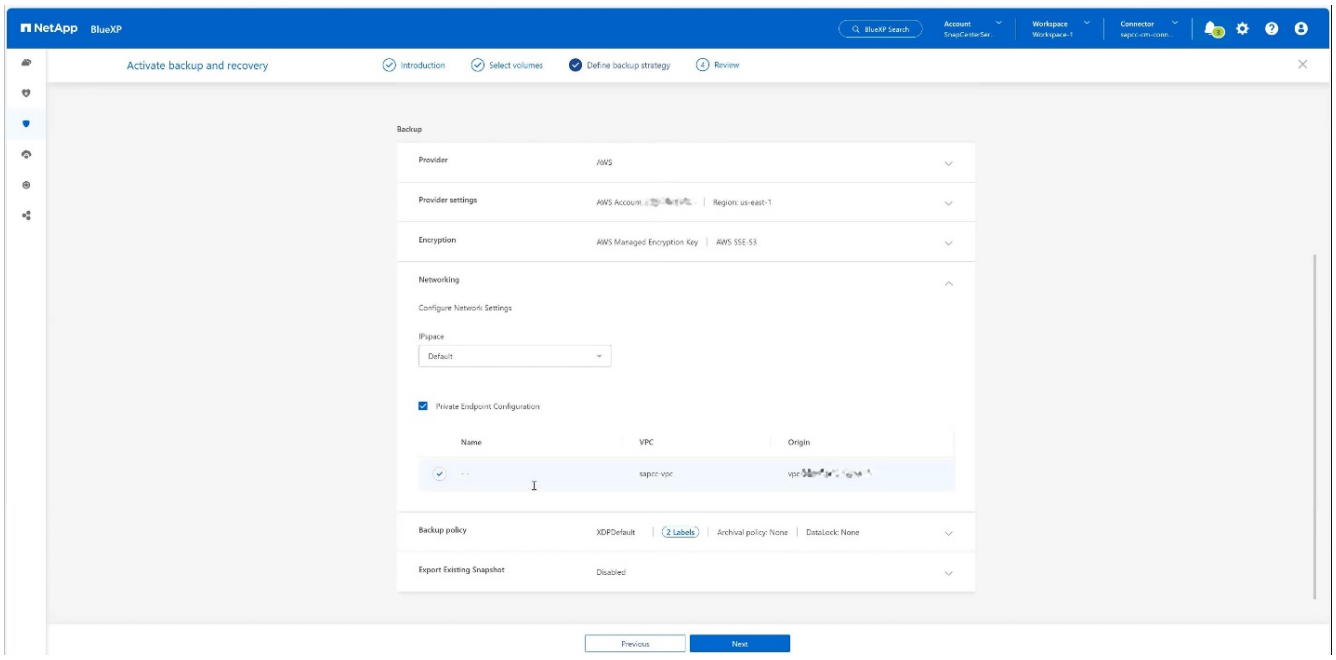
7. Aktivieren Sie die Option **Backup** und wählen Sie Ihren gewünschten Backup-Anbieter. In diesem Beispiel AWS.
   Lassen Sie die Option für bereits vorhandene Richtlinien aktiviert.
   Deaktivieren Sie die Optionen, die Sie nicht verwenden möchten.



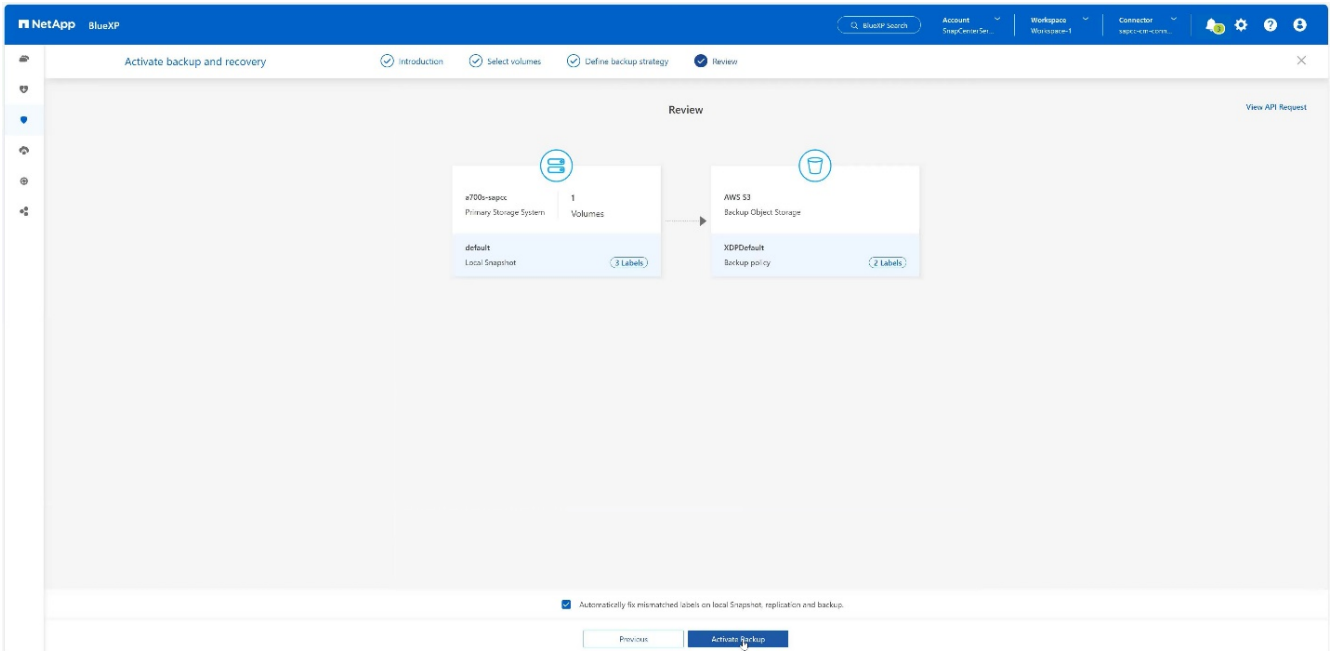
8. Erstellen Sie einen neuen Bucket, oder wählen Sie einen vorhandenen Bucket aus. Stellen Sie Ihre AWS-Kontoeinstellungen, den regio, Ihren Zugriffsschlüssel und den geheimen Schlüssel bereit. Drücken Sie **Weiter**.



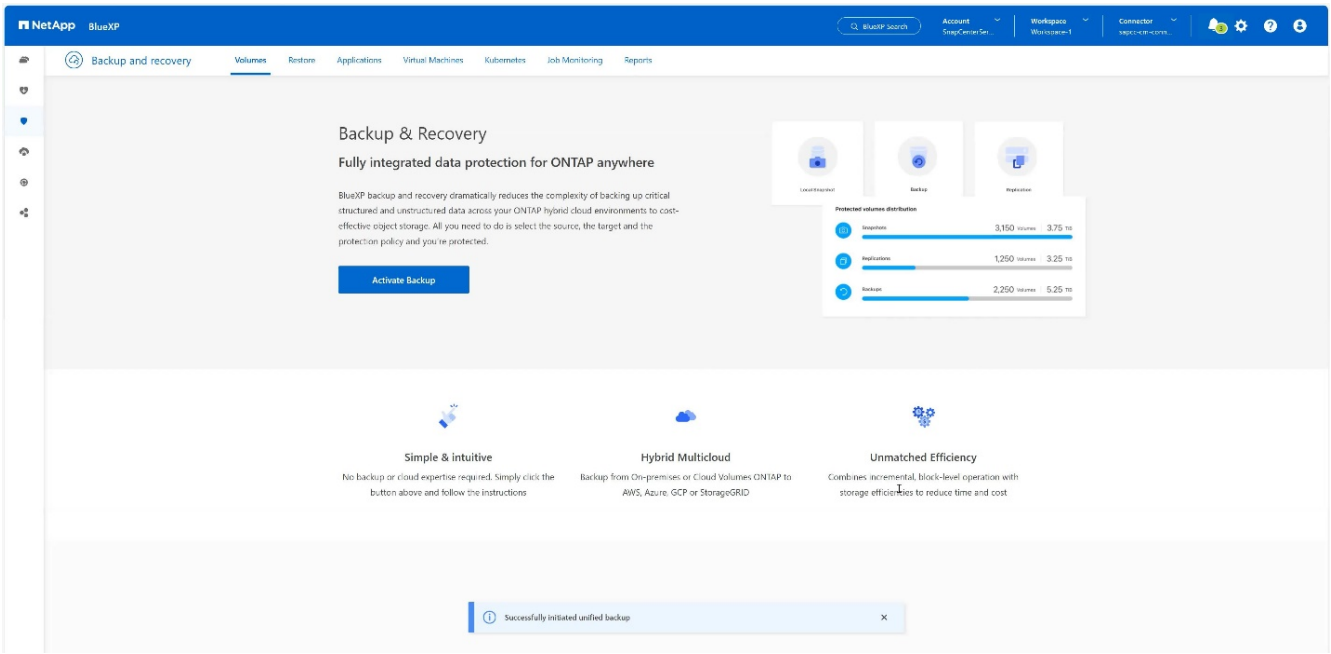
9. Wählen Sie den korrekten IPspace Ihres lokalen Storage-Systems aus, wählen Sie **Privat Endpoint Configuration** aus und wählen Sie den VPC-Endpunkt für S3 aus. Drücken Sie **Weiter**.



10. Überprüfen Sie Ihre Konfiguration und drücken Sie **Sicherung aktivieren**.

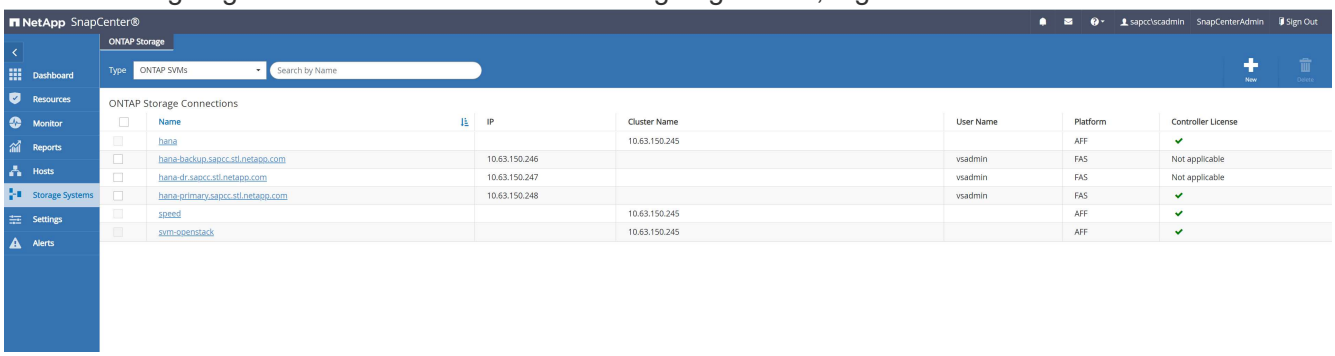


11. Die Sicherung wurde erfolgreich initiiert.

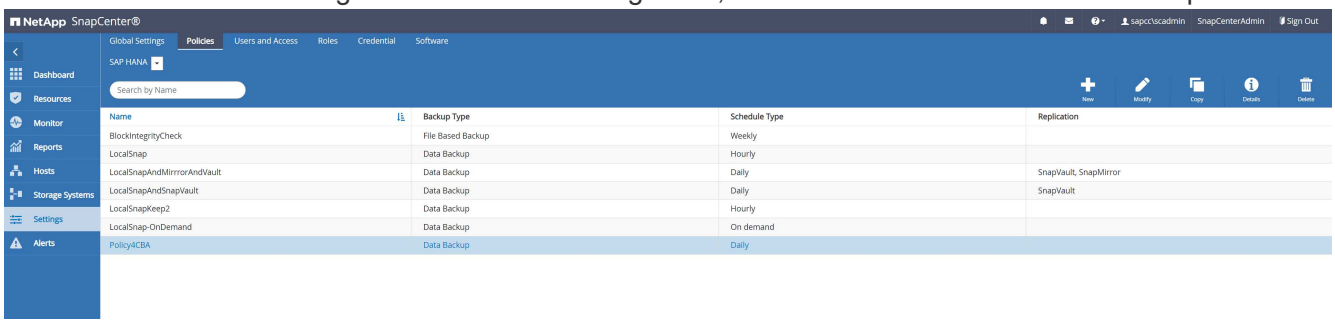


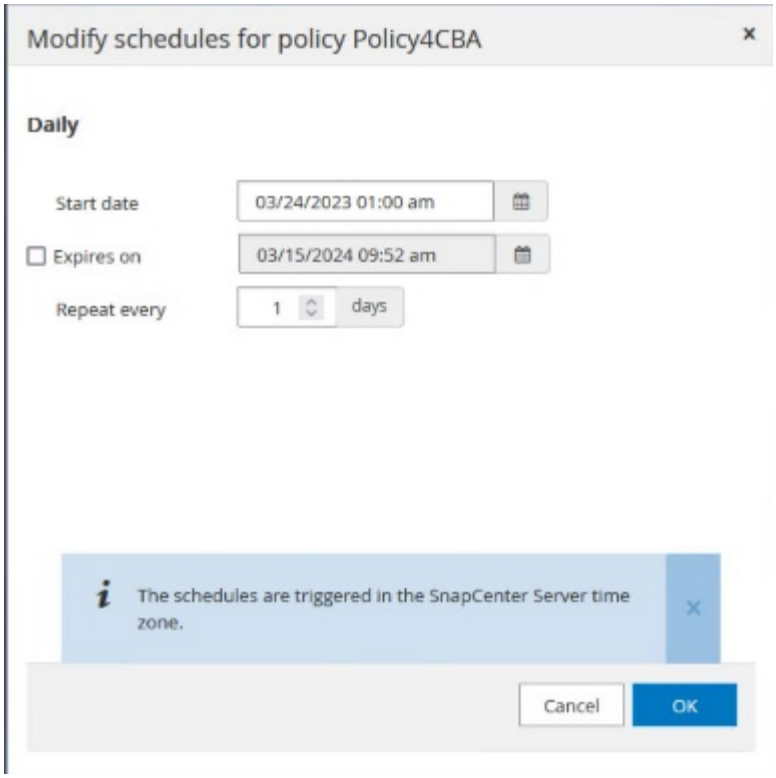
Konfigurieren Sie die SAP HANA-Systemressource bei SnapCenter

1. Prüfen Sie, ob die SVM (in diesem Beispiel hana), in der Ihr SAP HANA-System gespeichert ist, über den Cluster hinzugefügt wurde. Wenn nur die SVM hinzugefügt wurde, fügen Sie das Cluster hinzu.

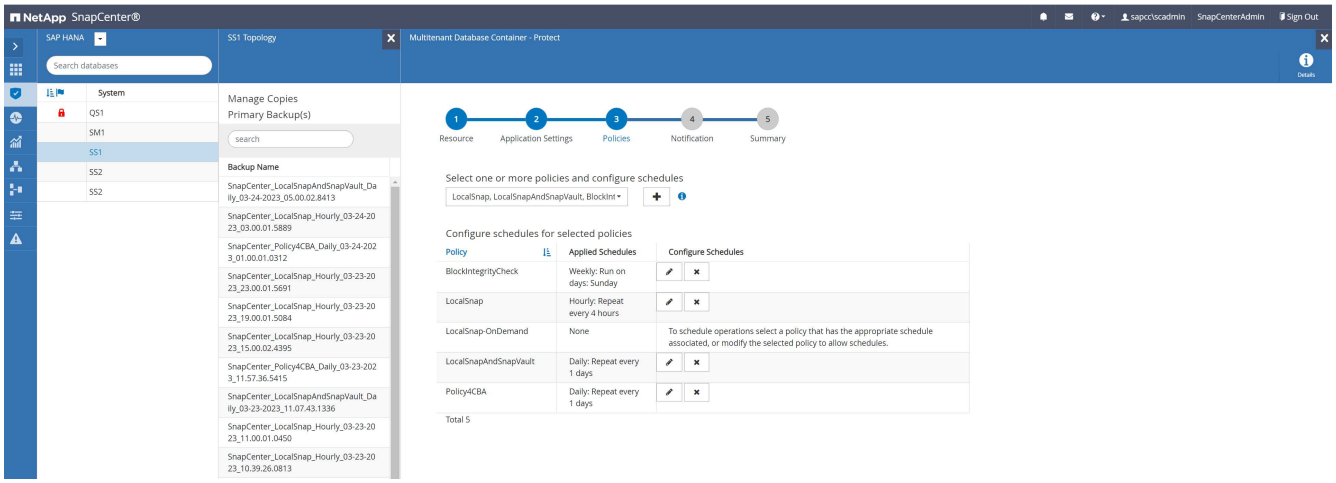


2. Definieren Sie eine Planungsrichtlinie mit einem täglichen, wöchentlichen oder monatlichen Zeitplan.

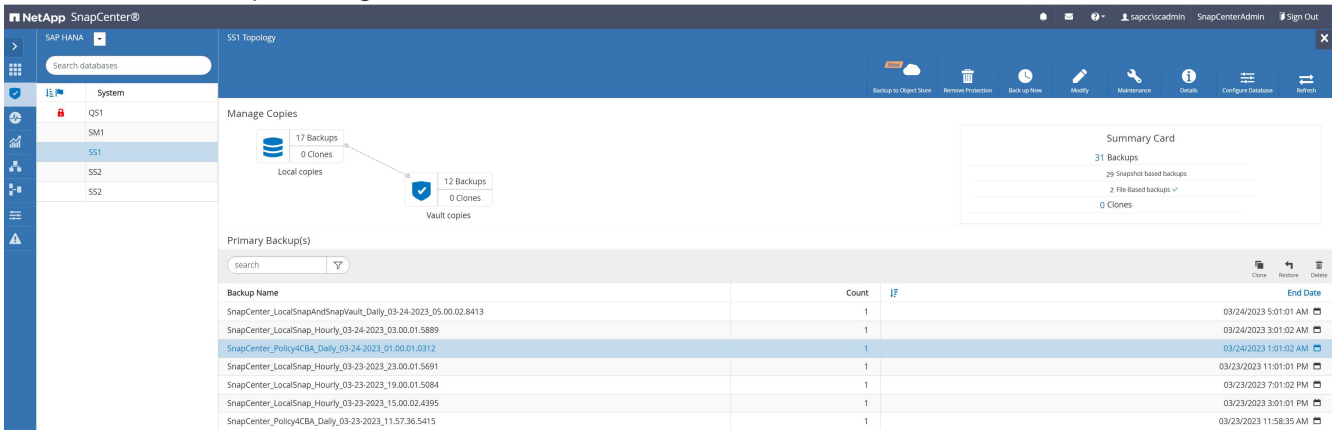




3. Fügen Sie die neue Richtlinie zu Ihrem SAP HANA-System hinzu und weisen Sie einen täglichen Zeitplan zu.

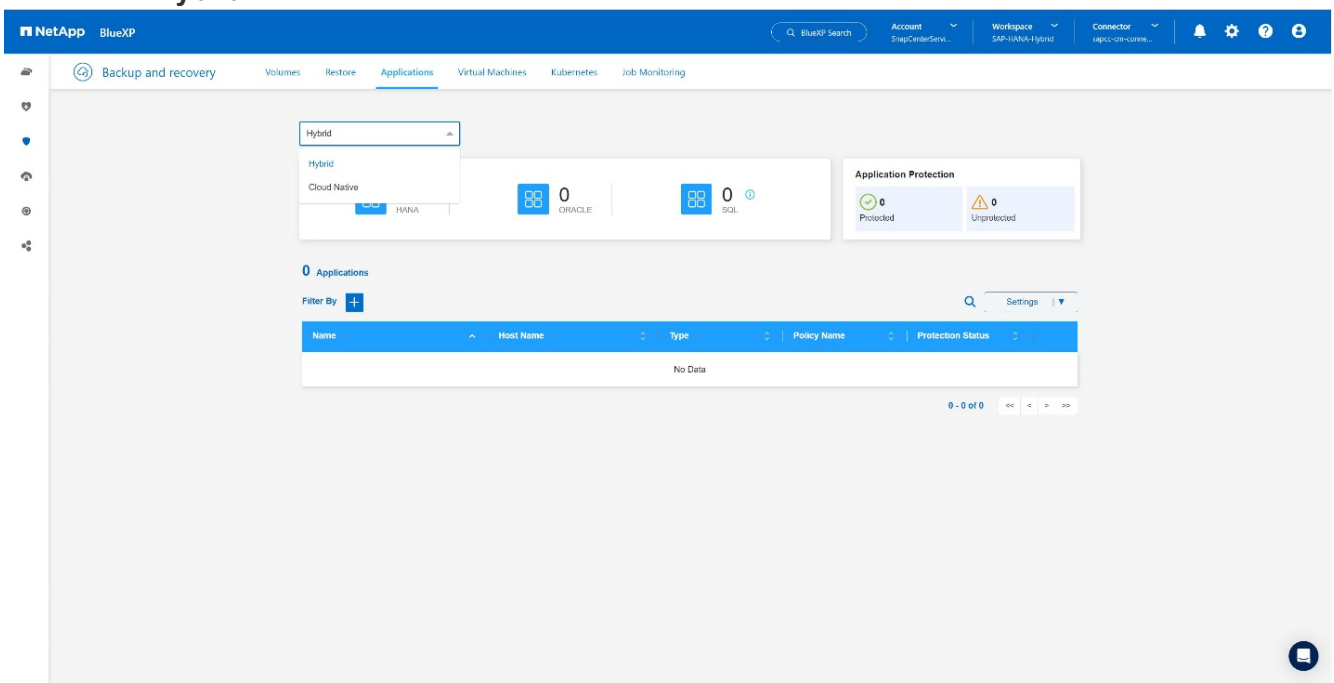


4. Nach der Konfiguration sind neue Backups mit dieser Richtlinie verfügbar, nachdem die Richtlinie gemäß dem definierten Zeitplan ausgeführt wurde.

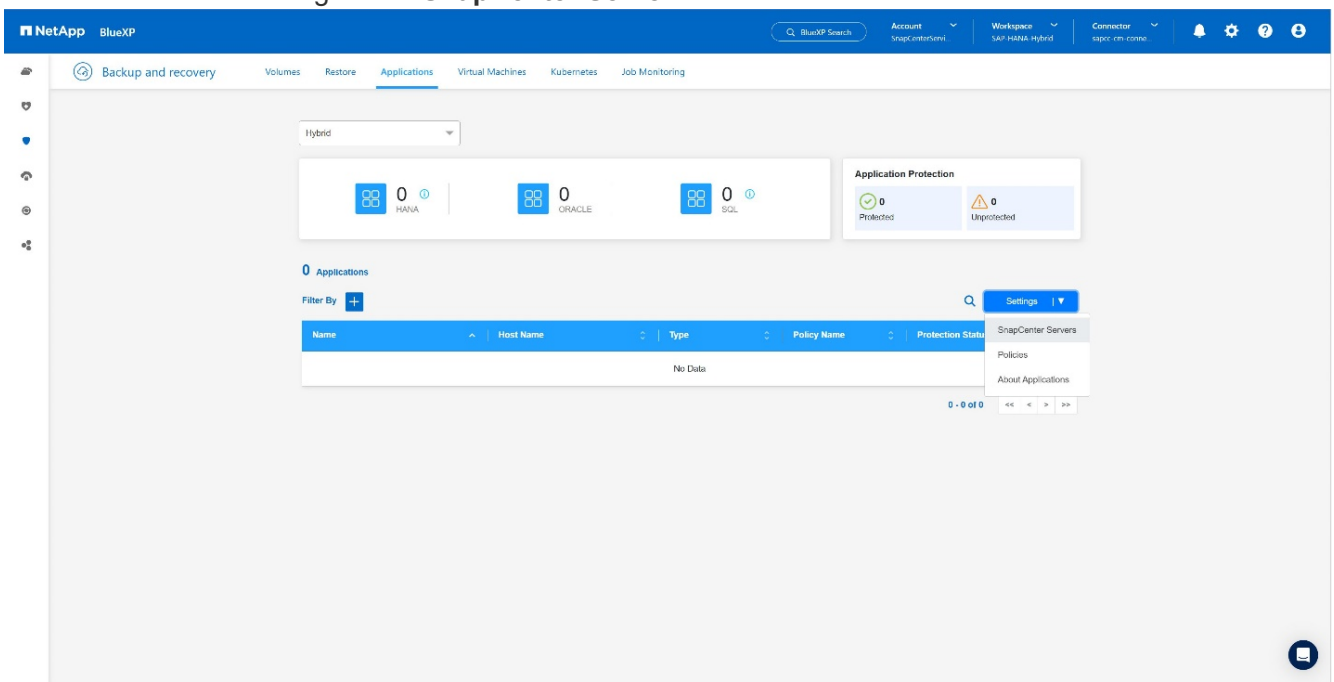


Hinzufügen von SnapCenter zur BlueXP Arbeitsumgebung

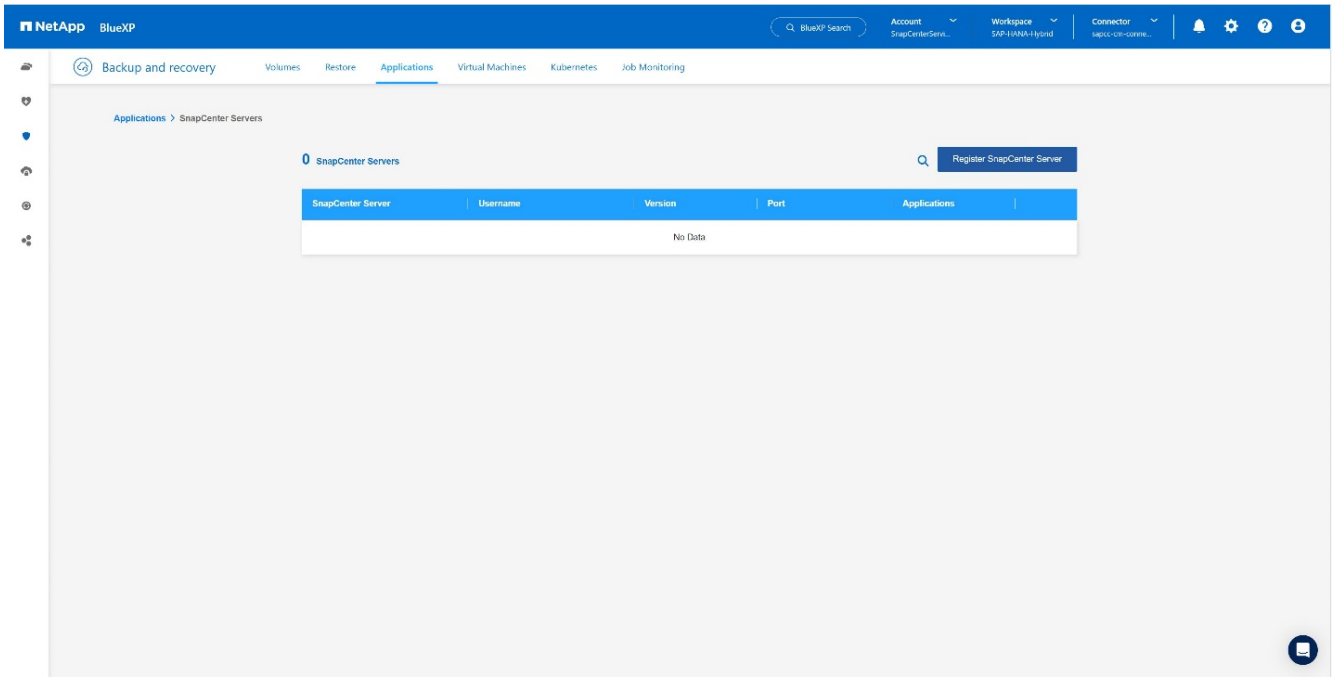
1. Wählen Sie im linken Menü **Schutz** → **Sicherung und Wiederherstellung** → **Anwendungen**.
2. Wählen Sie **Hybrid** aus dem Pulldown-Menü.



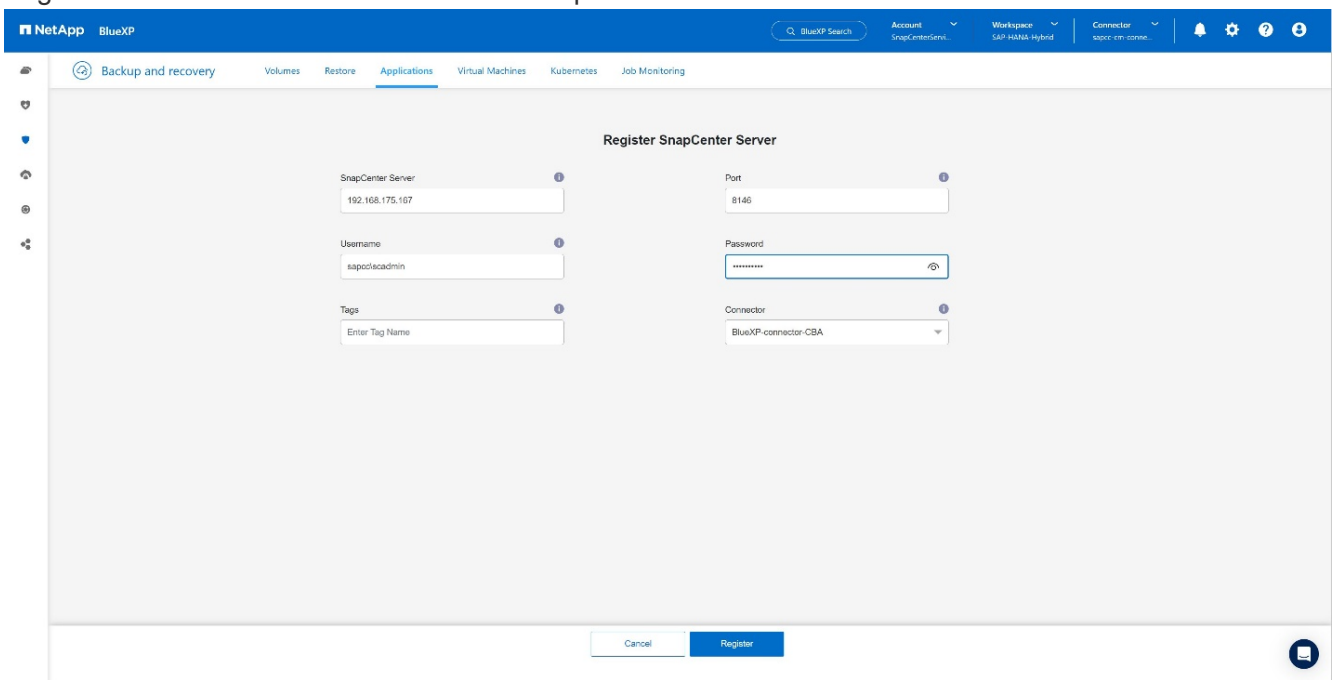
3. Wählen Sie im Einstellungsmenü **SnapCenter Server**.



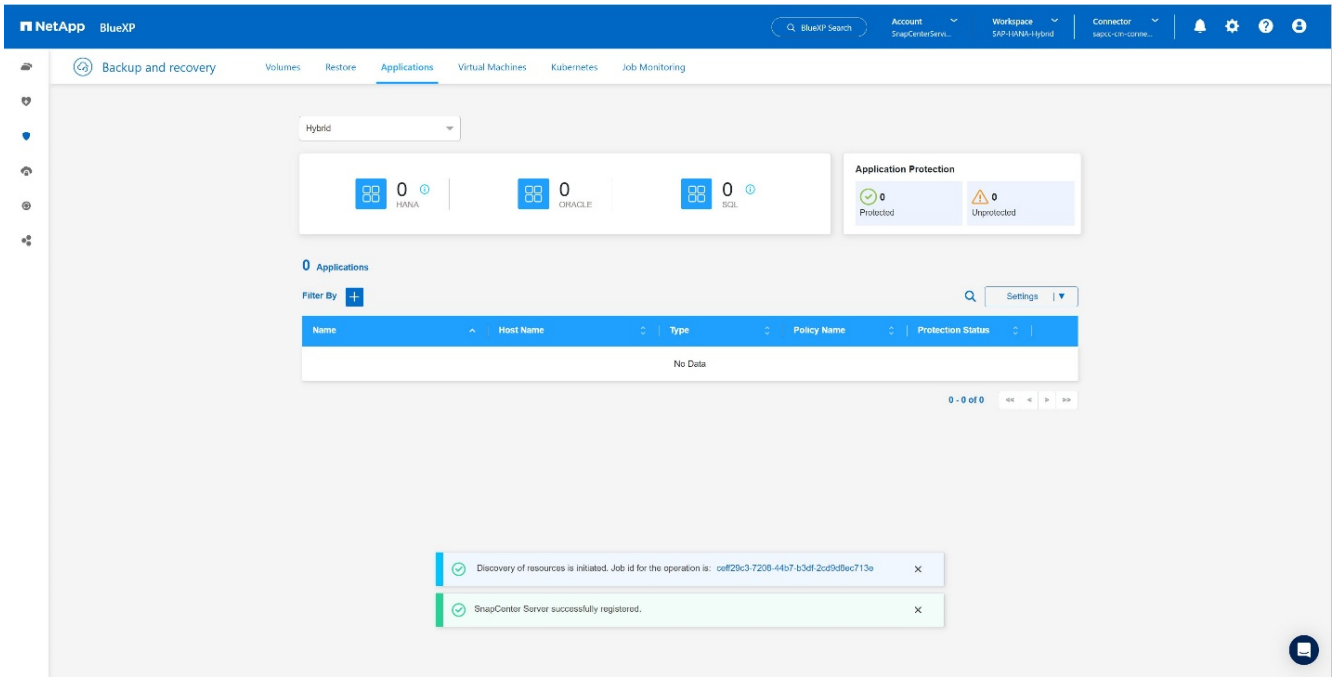
4. Registrieren Sie den SnapCenter-Server.



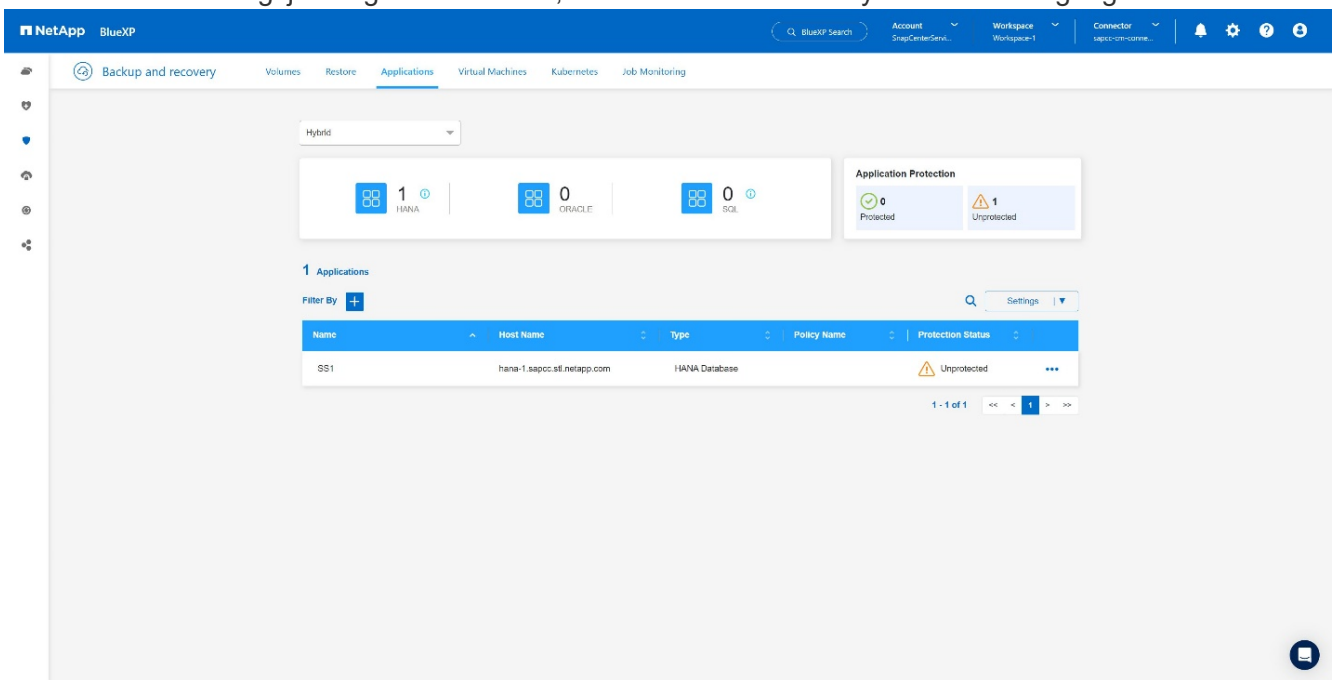
5. Fügen Sie die Anmeldeinformationen des SnapCenter-Servers hinzu.



6. Die SnapCenter-Server wurden hinzugefügt, und Daten werden erkannt.

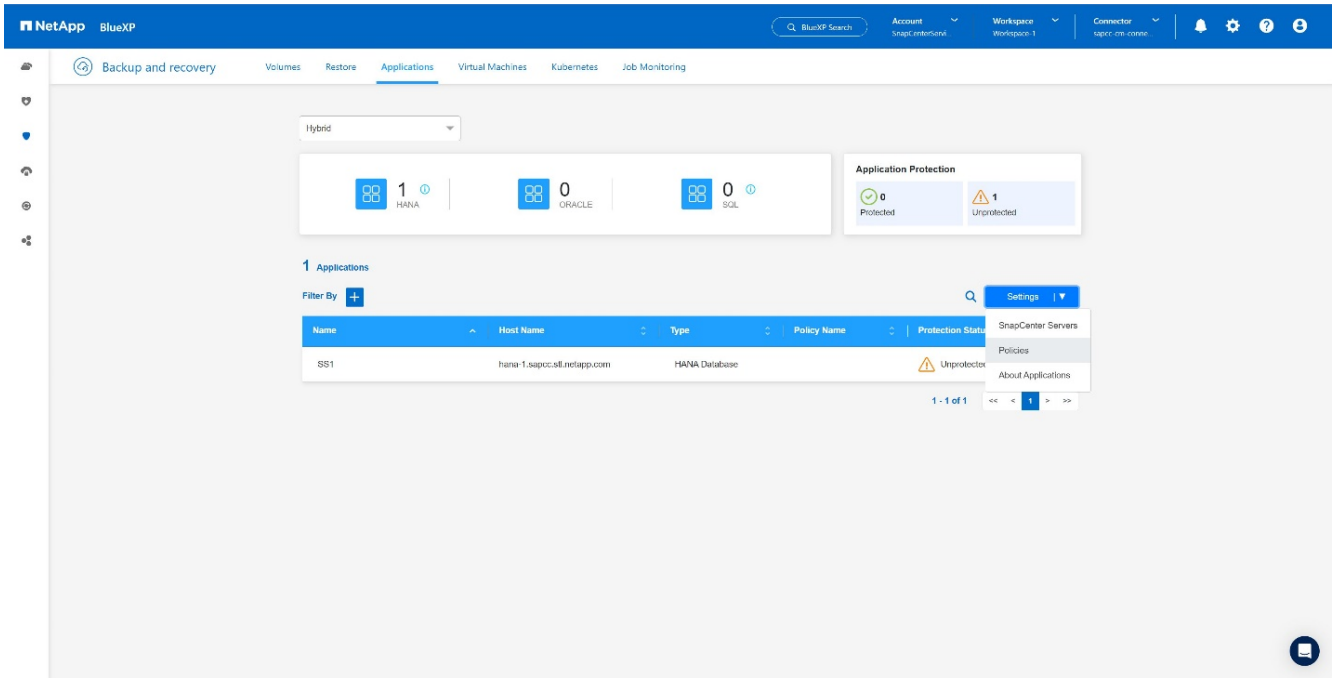


7. Sobald der Ermittlungsjob abgeschlossen ist, steht das SAP HANA-System zur Verfügung.

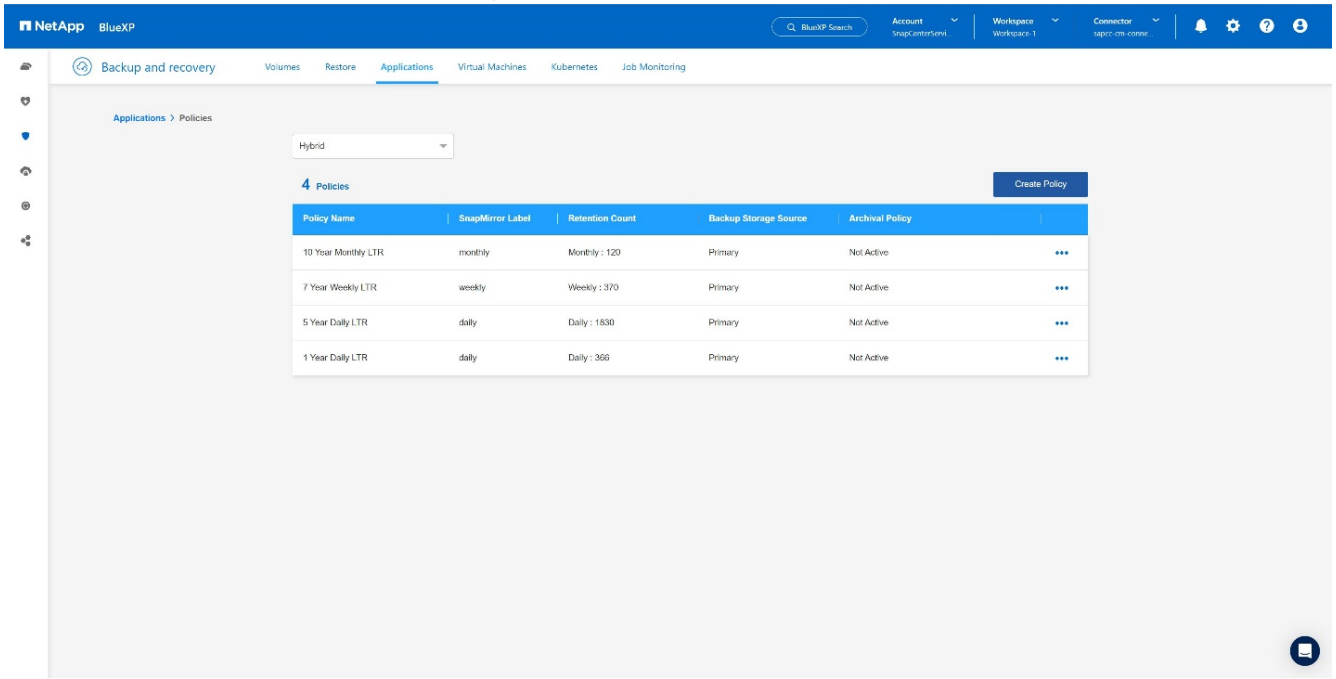


Erstellen einer Backup-Richtlinie für Anwendungsbackups

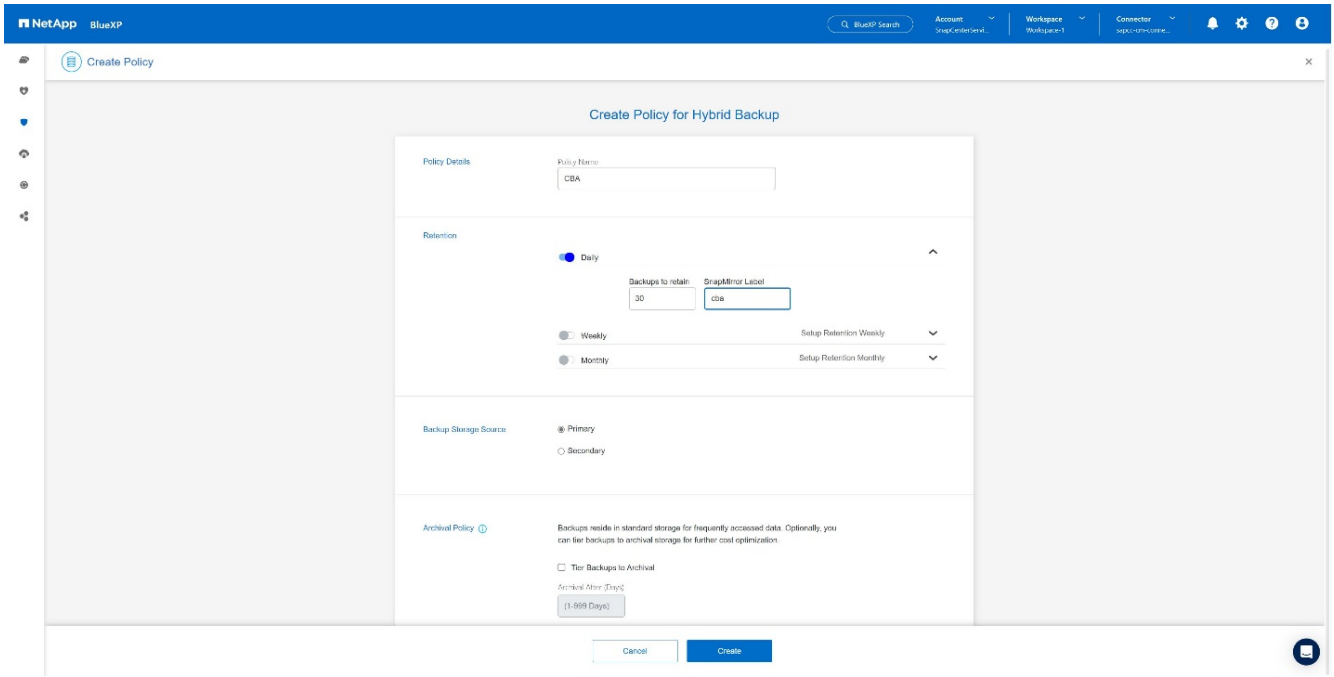
1. Wählen Sie im Einstellungsmenü **Policies** aus.



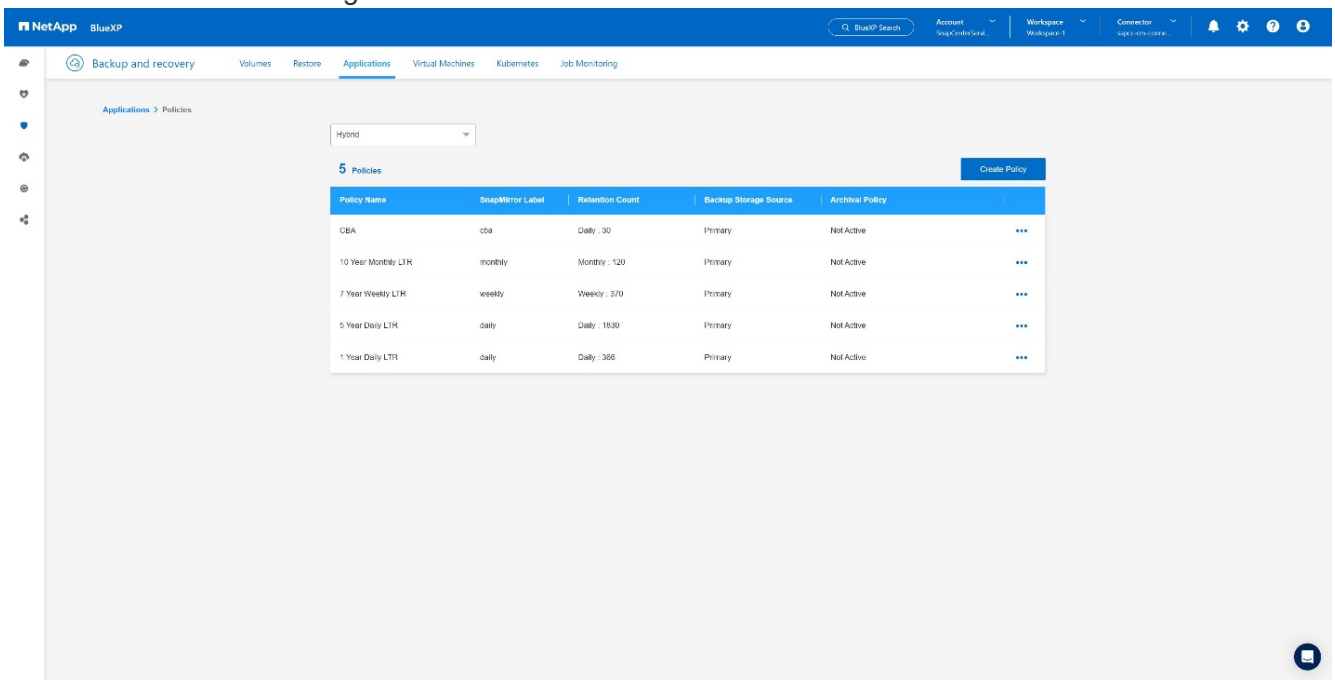
2. Erstellen Sie eine neue Richtlinie, falls gewünscht, indem Sie auf **Richtlinie erstellen** klicken.



3. Geben Sie den Richtliniennamen an, das gewünschte SnapMirror-Label, wählen Sie Ihre gewünschten Optionen aus und drücken Sie **Create**.

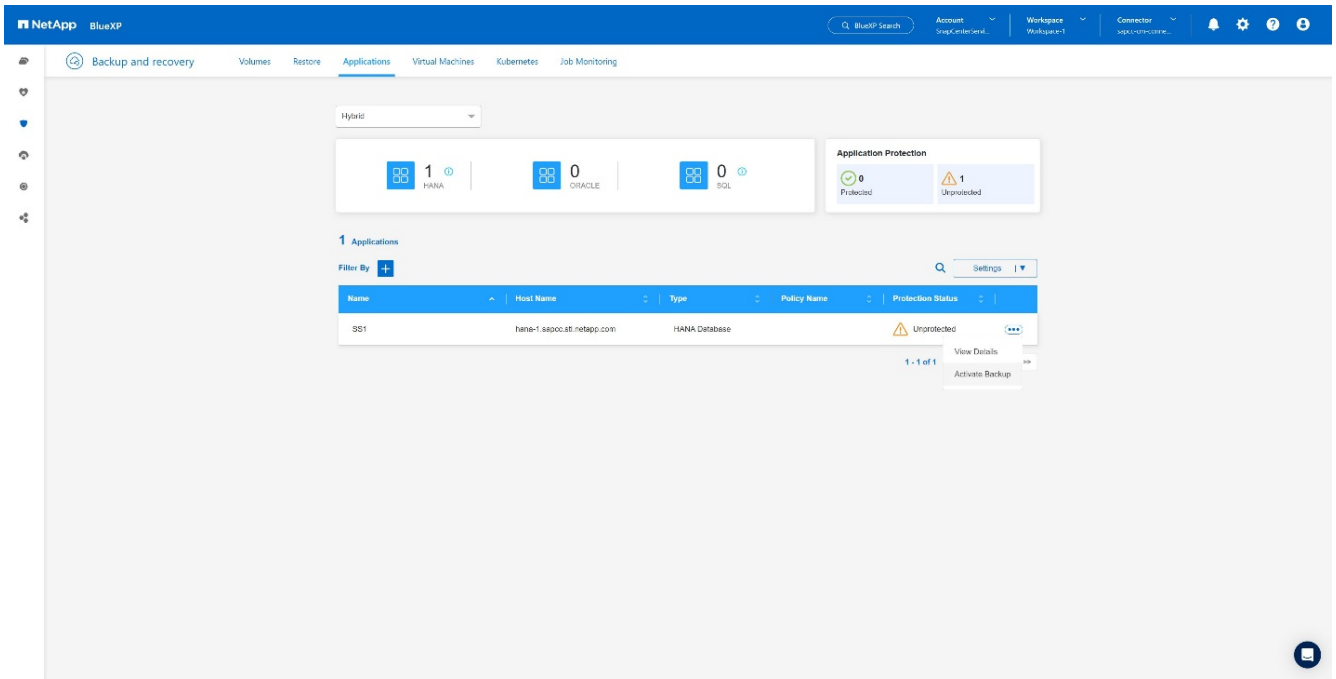


4. Die neue Richtlinie ist verfügbar.

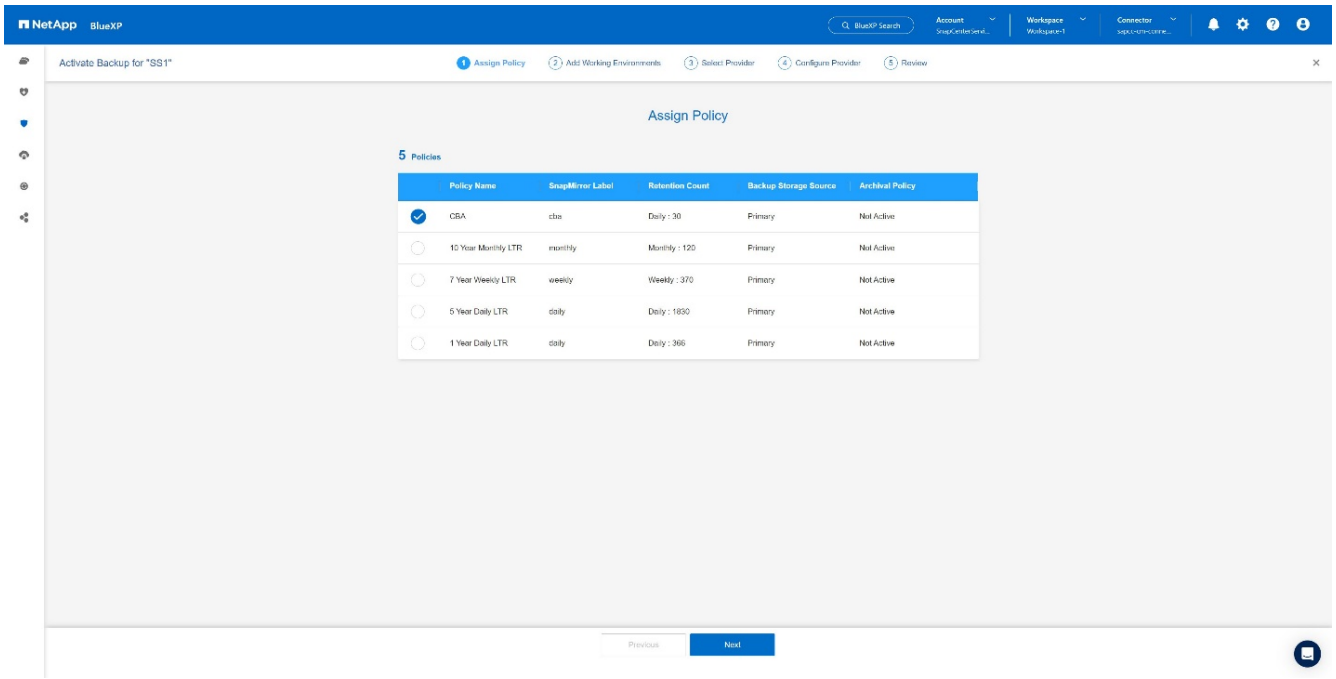


Sicherung der SAP HANA-Datenbank mit Cloud Backup für Applikationen

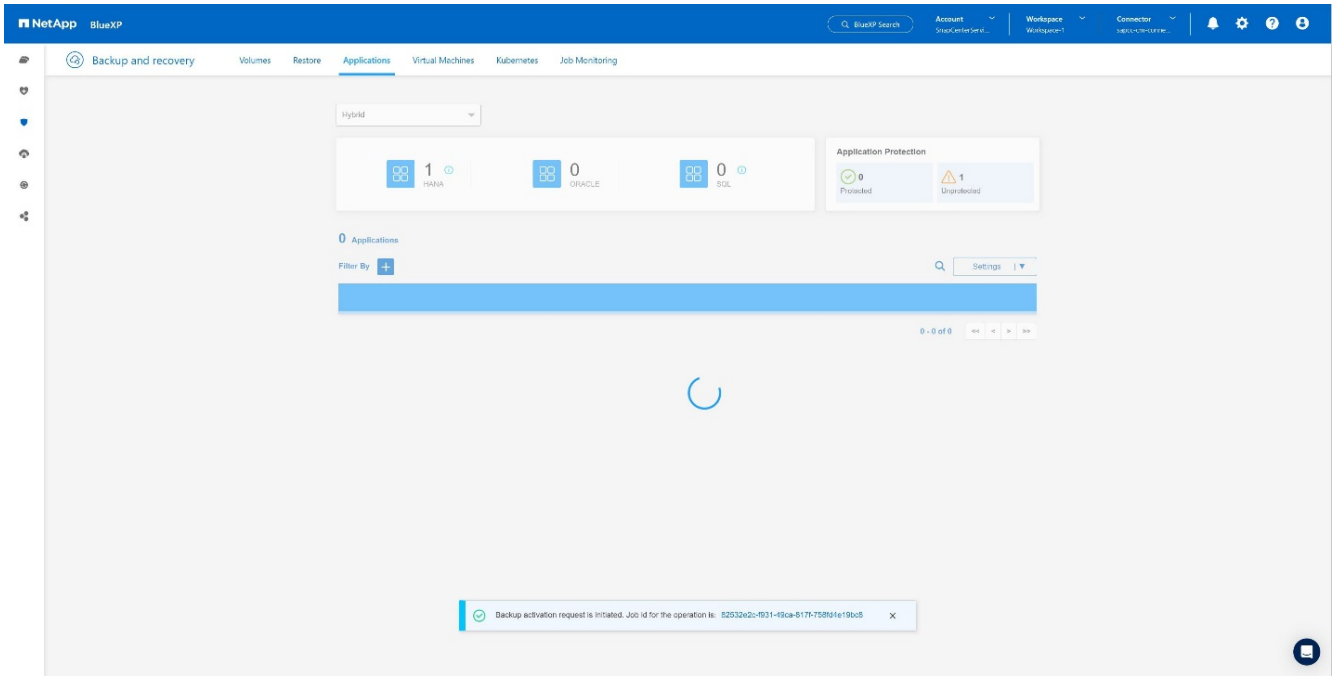
1. Wählen Sie **Backup aktivieren** für das SAP HANA-System.



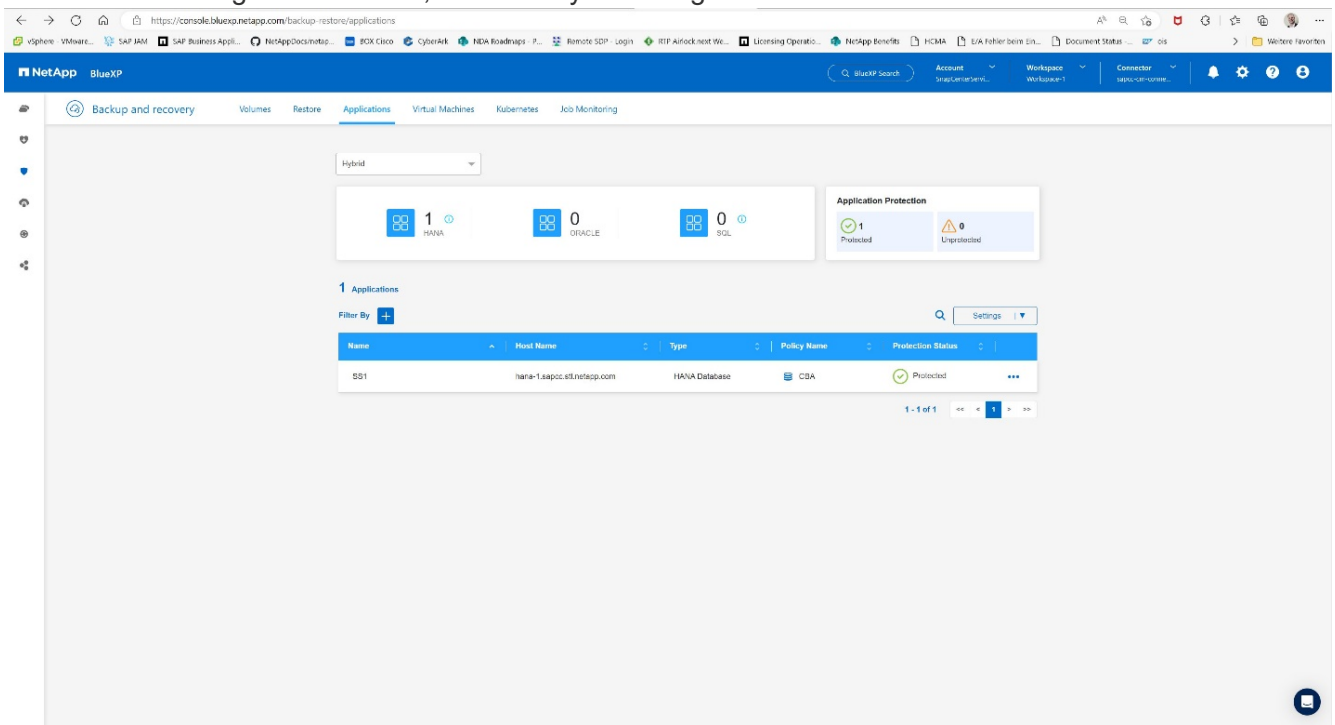
2. Wählen Sie die zuvor erstellte Richtlinie aus und klicken Sie auf **Weiter**.



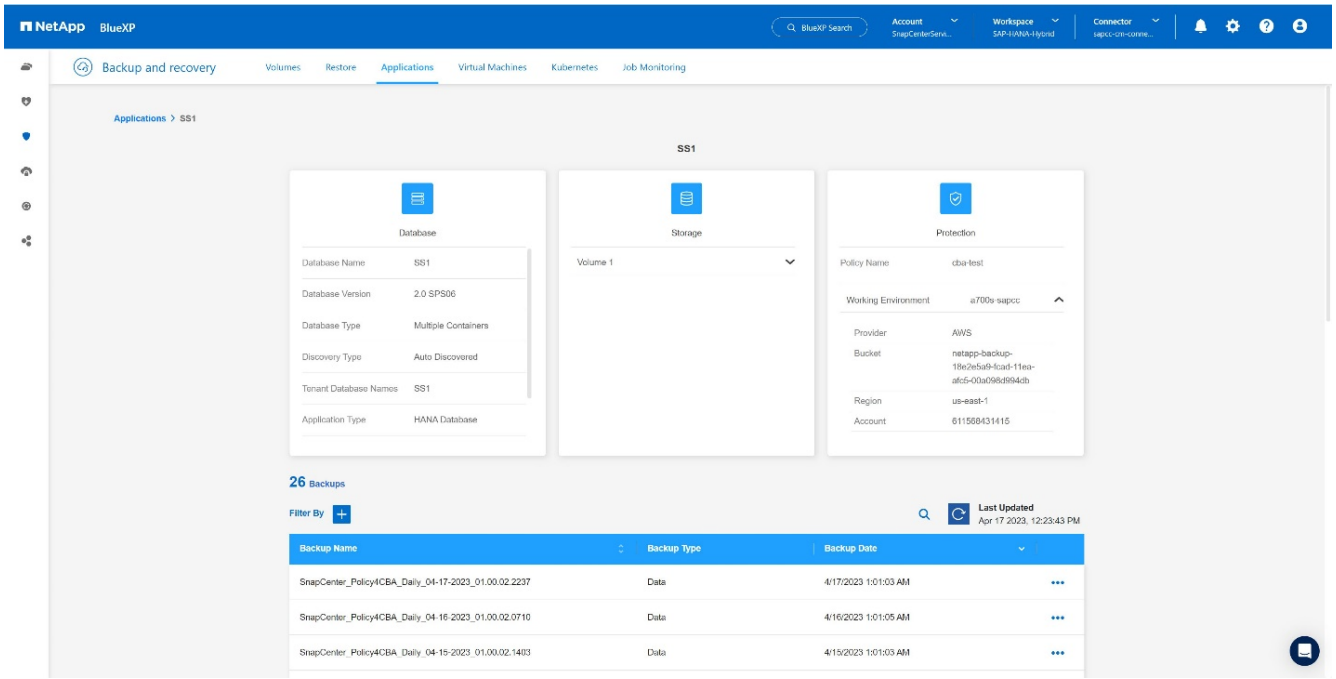
3. Da das Speichersystem und der Konnektor im Voraus konfiguriert haben, wird das Backup aktiviert.



4. Sobald der Job abgeschlossen ist, wird das System aufgelistet.



5. Nach einiger Zeit werden die Backups in der Detailansicht des SAP HANA Systems aufgelistet. Eine tägliche Sicherung wird am nächsten Tag aufgelistet.

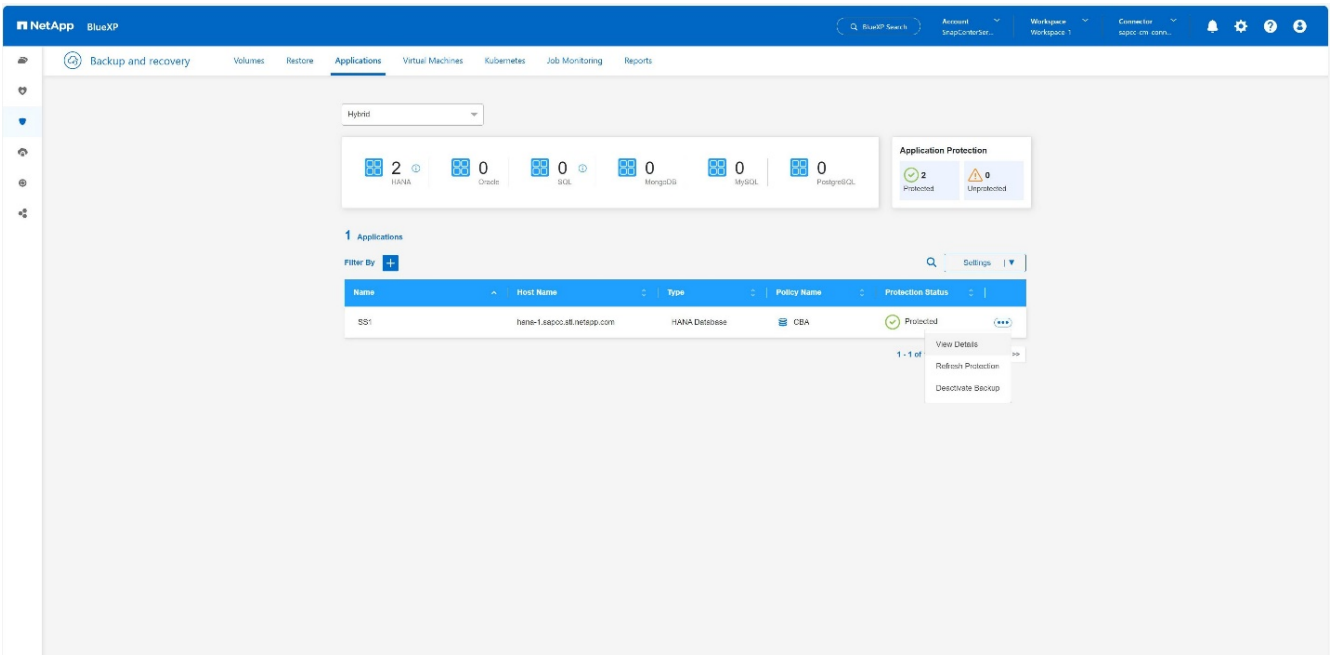


In einigen Umgebungen kann es notwendig sein, vorhandene Planungseinstellungen der snapmirror Quelle zu entfernen. Führen Sie dazu den folgenden Befehl am Quell-ONTAP-System aus: *snapmirror modify -Destination-path <hana-cloud-svm>:<SID_data_mnt00001>_copy -schedule ""* .

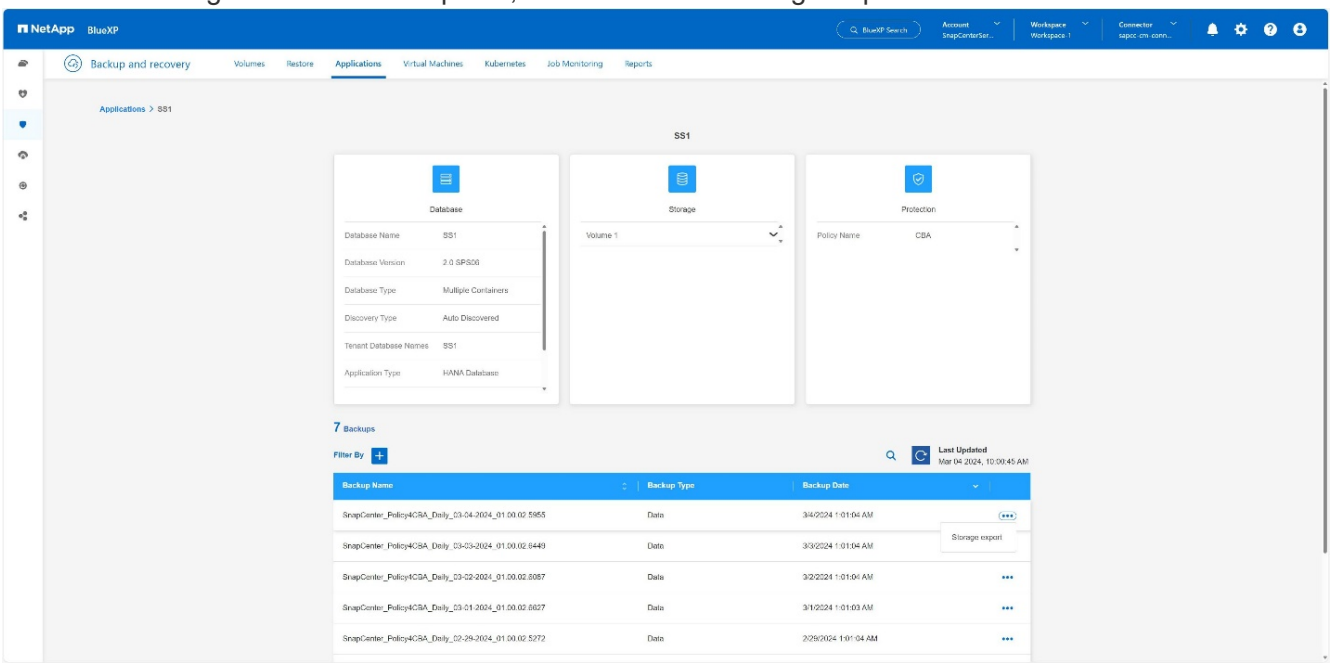
Wiederherstellung von SAP HANA BlueXP Backup

Eine Wiederherstellung aus dem Backup kann nur mit einem On-Premises-NetApp ONTAP-basierten Storage-System oder NetApp CVO in der Cloud erfolgen. Eine Wiederherstellung kann wie folgt durchgeführt werden:

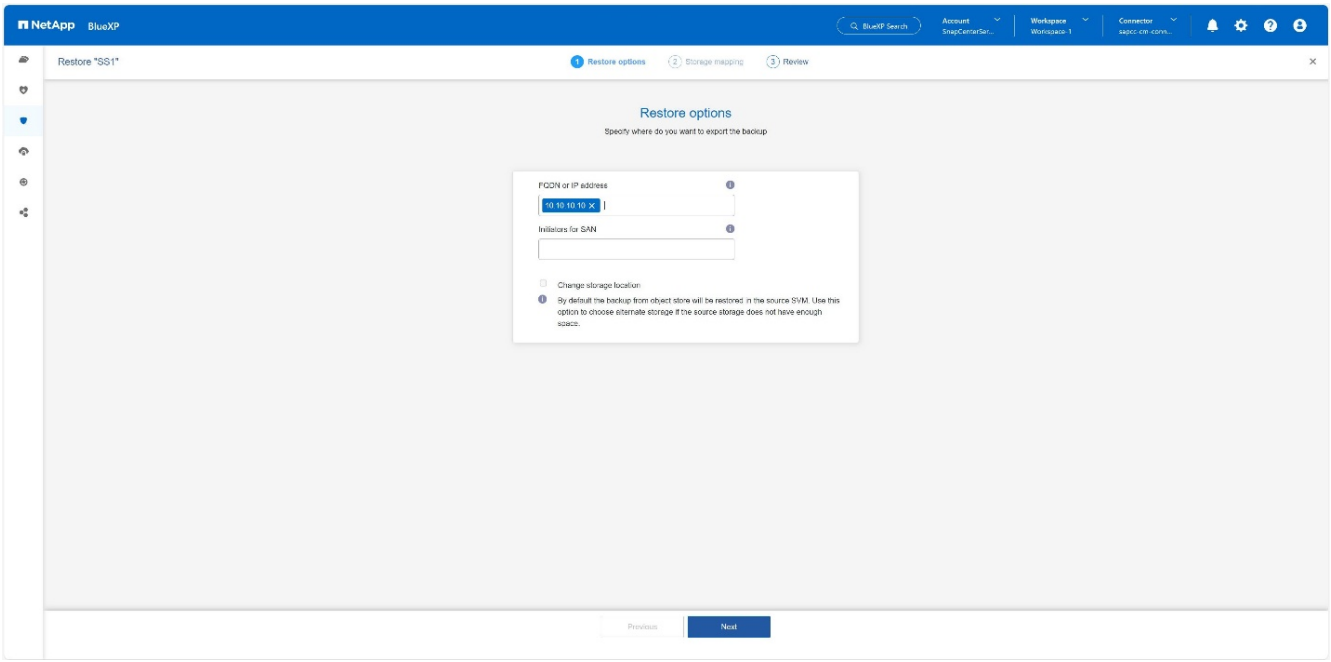
1. Klicken Sie in der Benutzeroberfläche von BlueXP auf **Schutz** > **Backup und Recovery** > **Anwendungen** und wählen Sie Hybrid.
2. Wählen Sie im Feld **Filtern nach** den Filter **Typ** und wählen Sie aus der Dropdown- Liste **HANA** aus.
3. Klicken Sie auf **View Details** für die Datenbank, die Sie wiederherstellen möchten.



4. Wählen Sie das gewünschte Backup aus, und wählen Sie Storage Export.



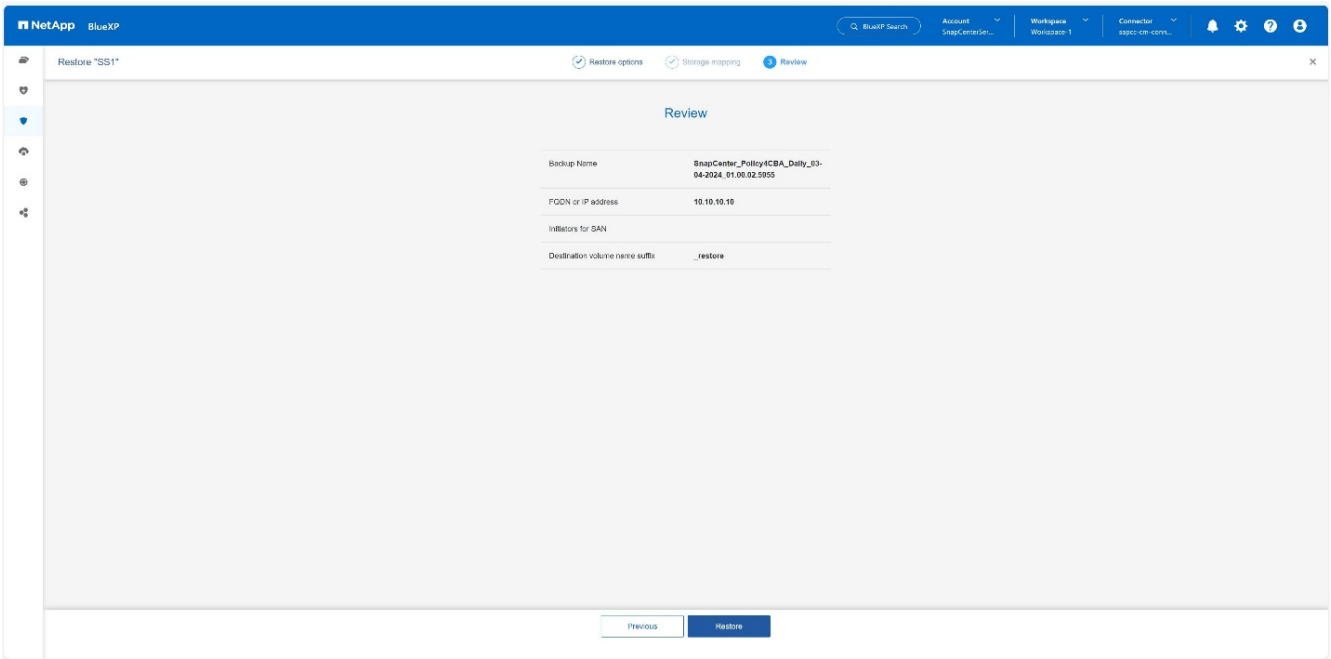
5. Geben Sie die gewünschten Optionen an:



a. Geben Sie in der NAS-Umgebung den FQDN oder die IP-Adresse des Hosts an, auf den die aus dem Objektspeicher wiederhergestellten Volumes exportiert werden sollen.

b. Geben Sie in der SAN-Umgebung die Initiatoren des Hosts an, dem die LUNs der aus dem Objektspeicher wiederhergestellten Volumes zugeordnet werden sollen.

6. Wenn sich der Snapshot im Archiv-Speicher befindet, wählen Sie die Priorität für die Wiederherstellung der Daten aus dem Archiv-Speicher aus.
7. Wenn nicht genügend Speicherplatz auf dem Quellspeicher vorhanden ist oder der Quellspeicher nicht verfügbar ist, wählen Sie **Speicherort ändern**.
8. Wenn Sie **Speicherort ändern** auswählen, können Sie ein Suffix an das Ziel-Volume anhängen. Wenn Sie das Kontrollkästchen nicht aktiviert haben, wird standardmäßig **_restore** an das Zielvolume angehängt. Klicken Sie Auf **Weiter**.
9. Wenn Sie Speicherort ändern ausgewählt haben, geben Sie die Details zum alternativen Speicherort an, in denen die vom Objektspeicher wiederhergestellten Daten auf der Seite Speicherzuordnung gespeichert werden, und klicken Sie auf **Weiter**.
10. Überprüfen Sie die Details und klicken Sie auf * Wiederherstellen*.



Dieser Vorgang führt nur den Speicherexport des wiederhergestellten Backups für den angegebenen Host aus. Sie müssen das Dateisystem manuell am Host mounten und die Datenbank aufrufen. Nach der Nutzung des Volumes kann der Speicheradministrator das Volume aus dem ONTAP-Cluster löschen.

Zusätzliche Informationen und Versionsverlauf

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- NetApp BlueXP Backup- und Recovery-Produktdokumentation
  "Sichern Sie Ihre On-Premises-Applikationsdaten in der NetApp Dokumentation"
- SAP HANA Backup und Recovery mit SnapCenter
  https://docs.netapp.com/us-en/netapp-solutions-sap/backup/saphana-br-scs-overview.html#the-netapp-solution

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	März 2024	Ausgangsversion

Siehe "Interoperabilitäts-Matrix-Tool (IMT)" Überprüfen Sie auf der NetApp Support-Website, ob die in diesem Dokument angegebenen Produktversionen und Funktionen in Ihrer IT-Umgebung unterstützt werden. Das NetApp IMT definiert die Produktkomponenten und -Versionen, die für von NetApp unterstützte Konfigurationen verwendet werden können. Die spezifischen Ergebnisse hängen von der Installation des jeweiligen Kunden gemäß den technischen Daten ab.

SAP HANA System Replication Backup und Recovery mit SnapCenter

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

Nils Bauer, NetApp

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.

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.

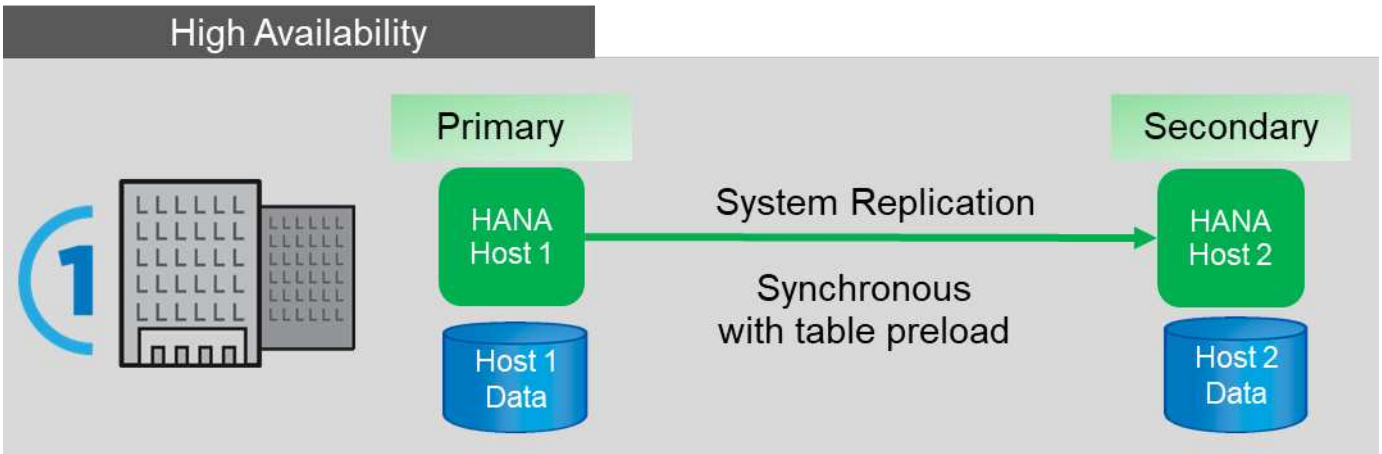
Hochverfügbarkeit ohne RPO und mit minimalem RTO-Aufwand

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.

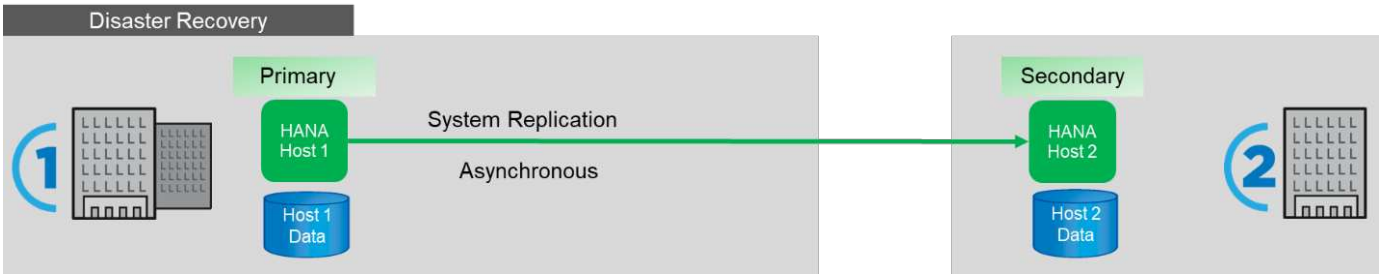
Der Rest dieses Dokuments konzentriert sich auf Backup-Vorgänge mit SAP System Replication, konfiguriert als Hochverfügbarkeitslösung.



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.



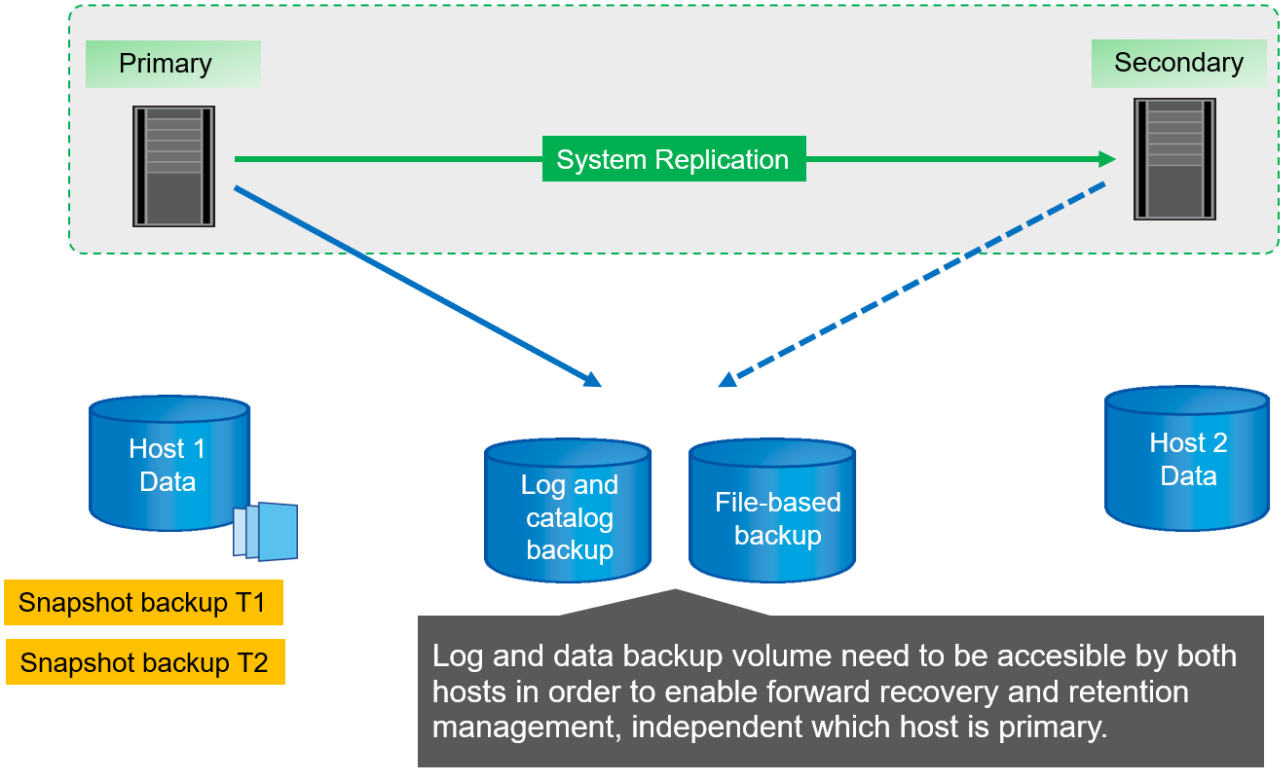
Storage Snapshot Backups und SAP System Replication

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.

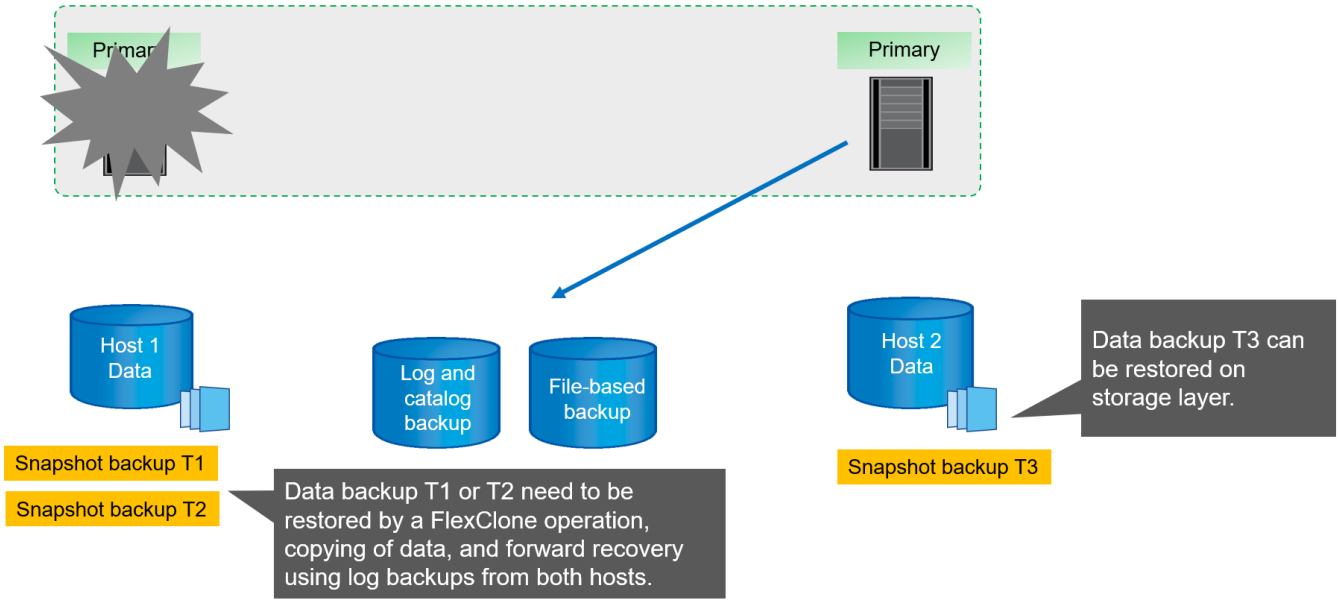
Da jedes Backup für die Wiederherstellung verwendet und mithilfe von Log-Backups von beiden Hosts durchgeführt werden kann, ist ein gemeinsamer Backup-Ort für Protokolle erforderlich, auf den von beiden Hosts zugegriffen werden kann. NetApp empfiehlt die Verwendung eines Shared Storage Volume. Sie sollten 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.

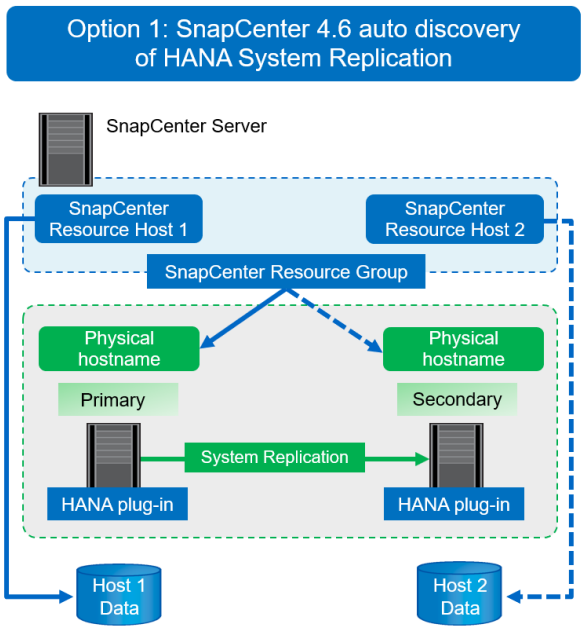


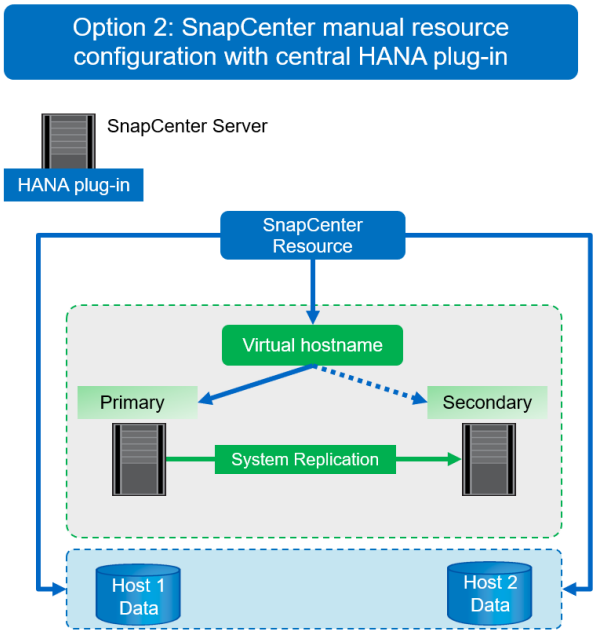
SnapCenter Konfigurationsoptionen für SAP System Replication

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

	Ressourcengruppe mit SnapCenter 4.6	Einzelne SnapCenter-Ressource und virtuelle IP-Adresse
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.

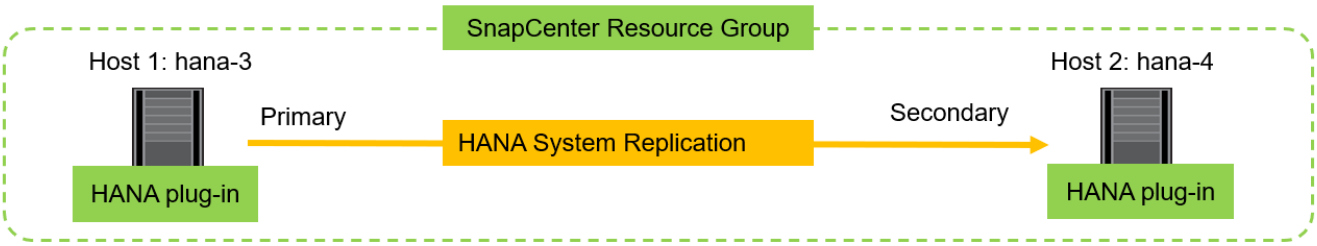
Für die HANA-Systemdatenbank wurde ein Datenbankbenutzer „SnapCenter“ mit den erforderlichen Berechtigungen zum Ausführen von Backup- und Recovery-Vorgängen erstellt (siehe "Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter"). Ein HANA-Benutzerspeicherschlüssel muss auf beiden Hosts mit dem oben genannten Datenbankbenutzer konfiguriert sein.

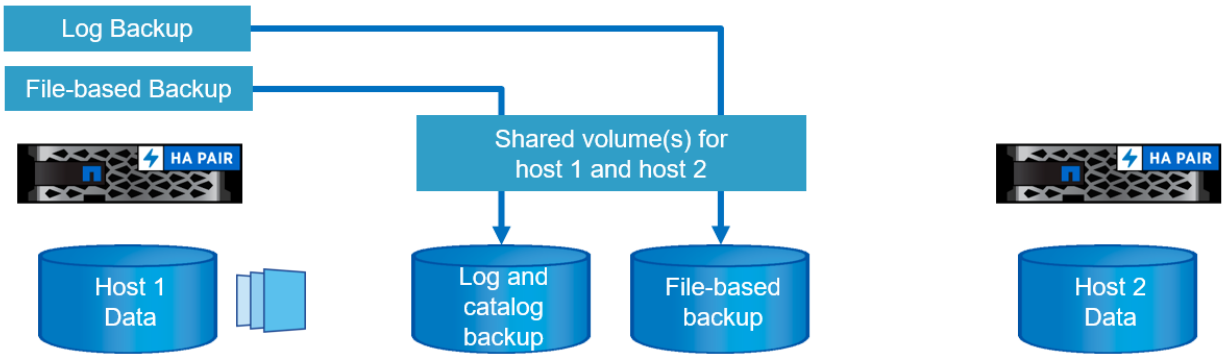
```
ss2adm@hana- 3: / > hdbuserstore set SS2KEY hana- 3:33313 SNAPCENTER
<password>
```

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

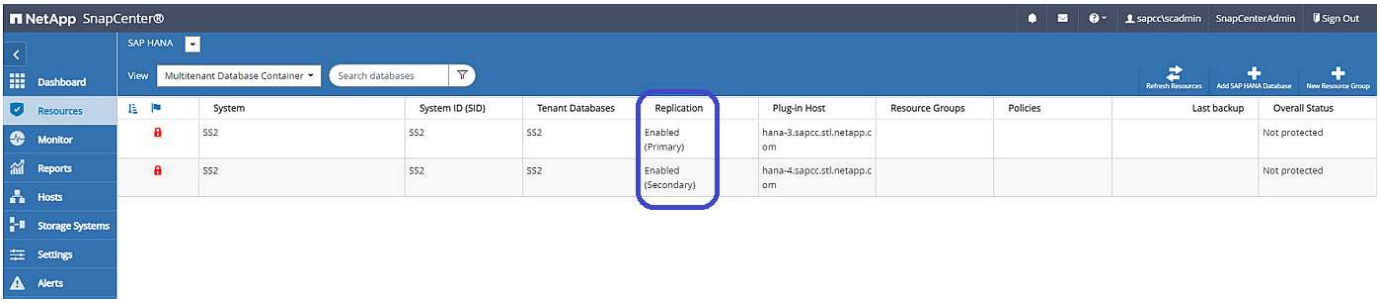
Aus einer übergeordneten Sicht müssen Sie die folgenden Schritte durchführen, um HANA System Replication in SnapCenter einzurichten.

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.

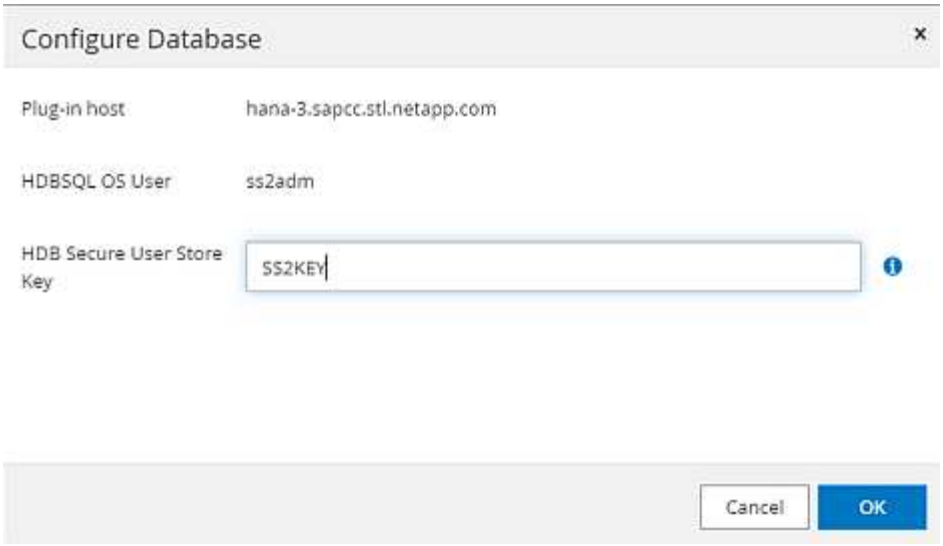




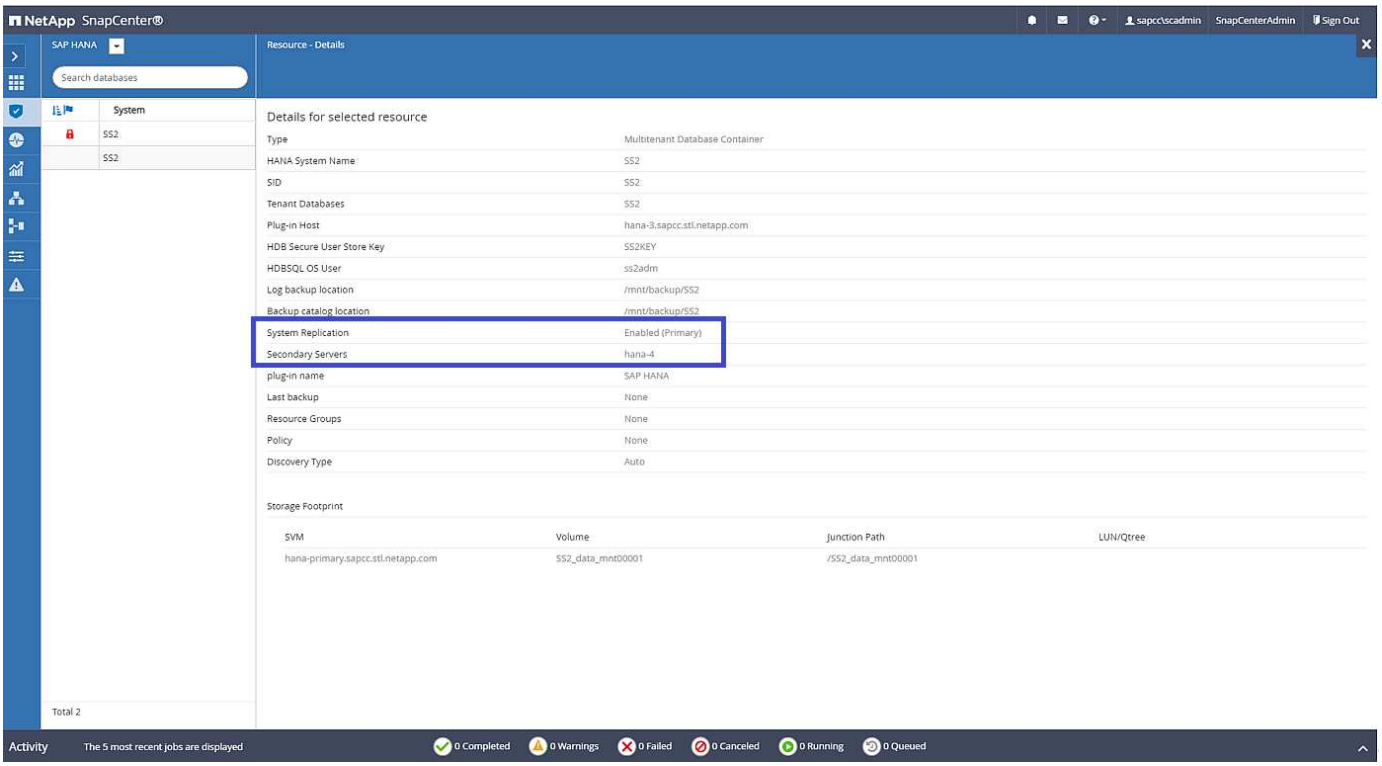
Nachdem Sie das SnapCenter HANA Plug-in auf beiden HANA-Hosts installiert haben, werden die HANA-Systeme in der Ansicht der SnapCenter-Ressourcen wie andere automatisch erkannte Ressourcen angezeigt. Ab SnapCenter 4.6 wird eine zusätzliche Spalte angezeigt, in der der Status der HANA-Systemreplizierung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



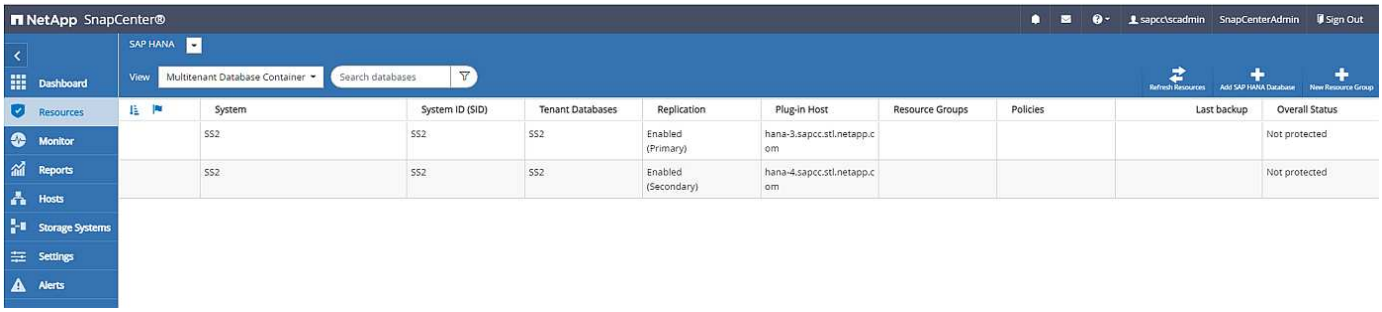
Durch Klicken auf die Ressource fordert SnapCenter den HANA-Benutzerspeicherschlüssel für das HANA-System an.



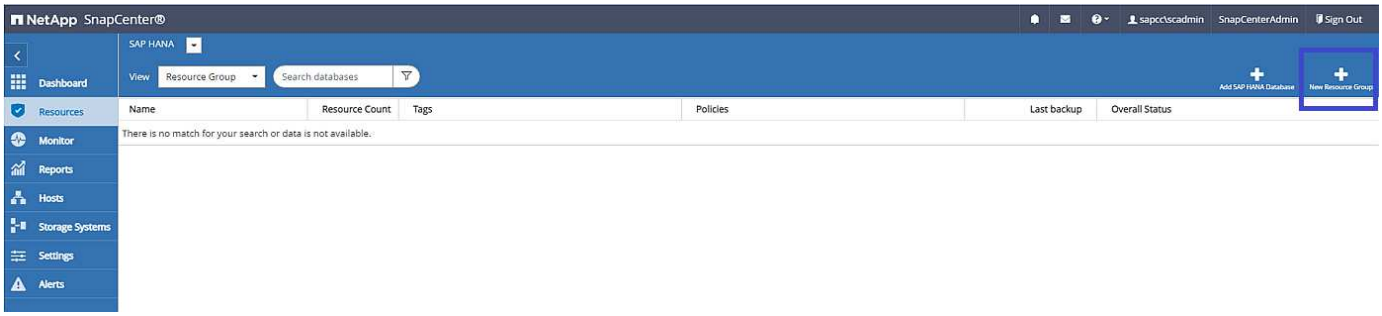
Weitere Schritte zur automatischen Ermittlung werden ausgeführt, und SnapCenter zeigen die Ressourcendetails an. In SnapCenter 4.6 werden der Replikationsstatus des Systems und der sekundäre Server in dieser Ansicht aufgelistet.



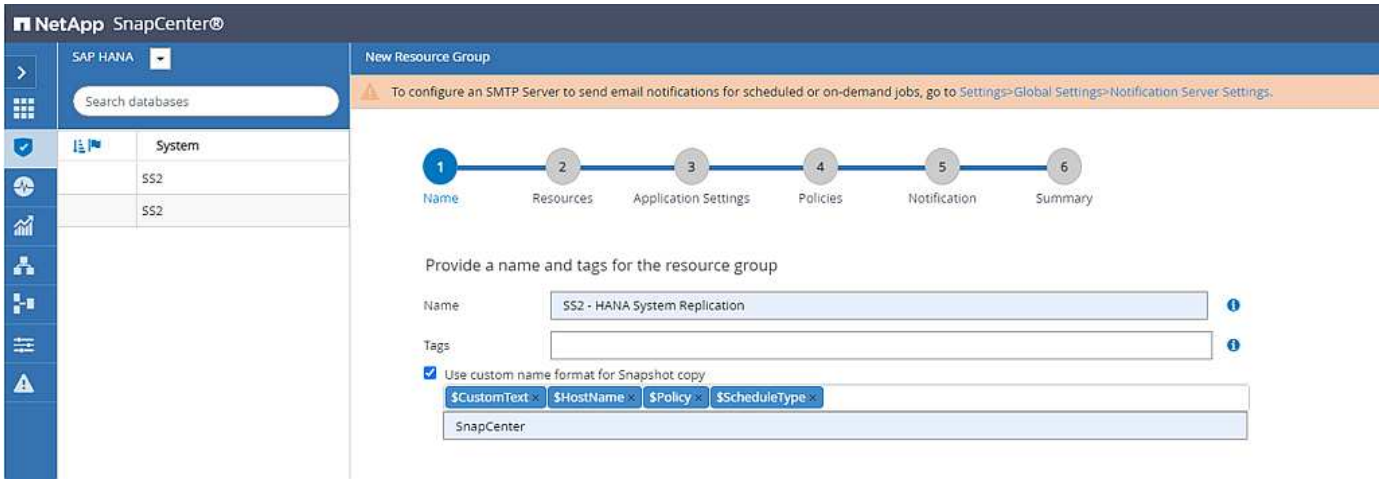
Nach Durchführung der gleichen Schritte für die zweite HANA-Ressource ist die automatische Ermittlung abgeschlossen, und beide HANA-Ressourcen werden in SnapCenter konfiguriert.



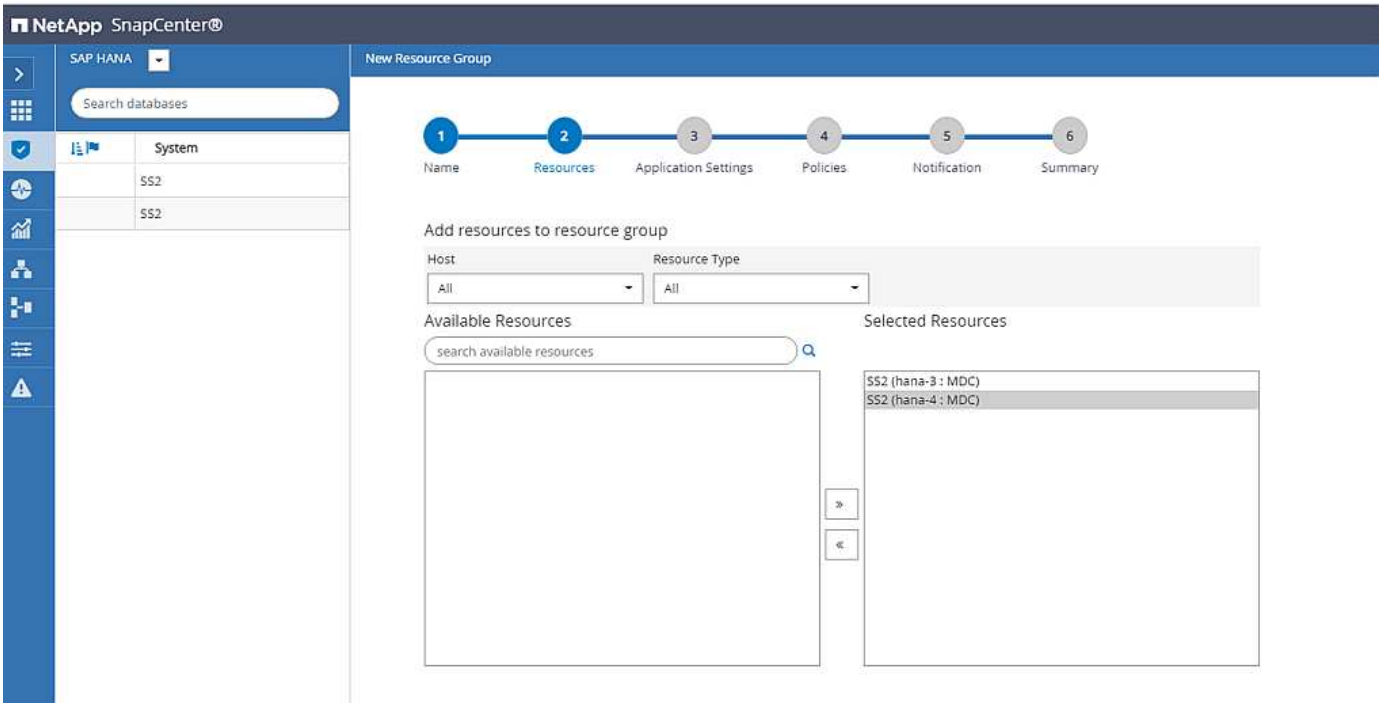
Für HANA System Replication-fähige Systeme müssen Sie eine SnapCenter-Ressourcengruppe, einschließlich beider HANA-Ressourcen, konfigurieren.



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

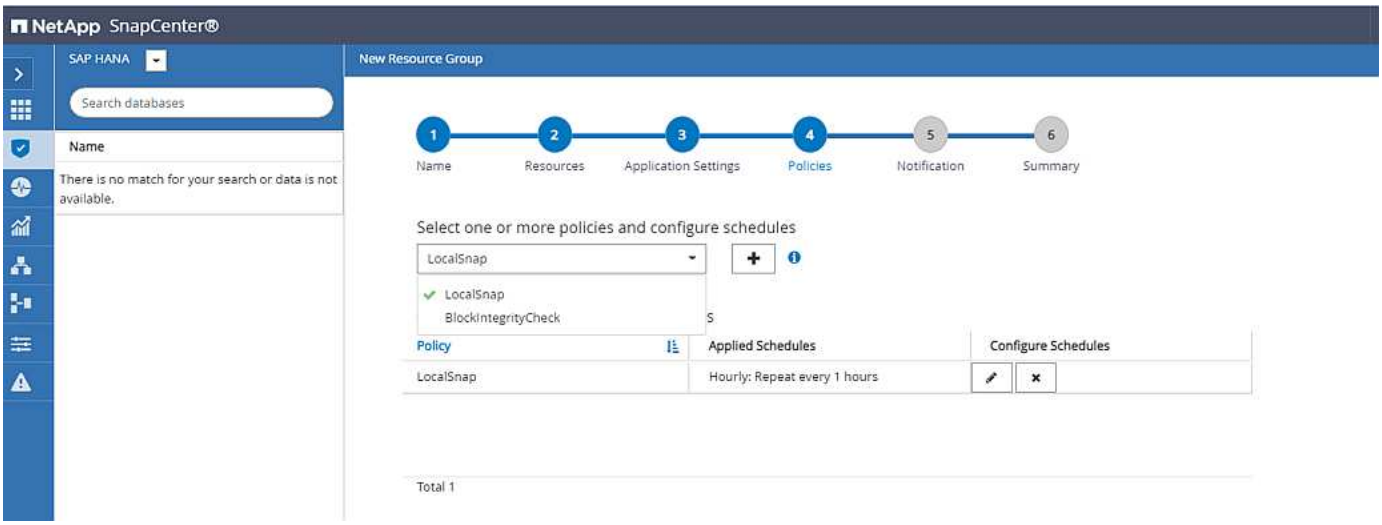


Sie müssen der Ressourcengruppe beide HANA-Hosts hinzufügen.

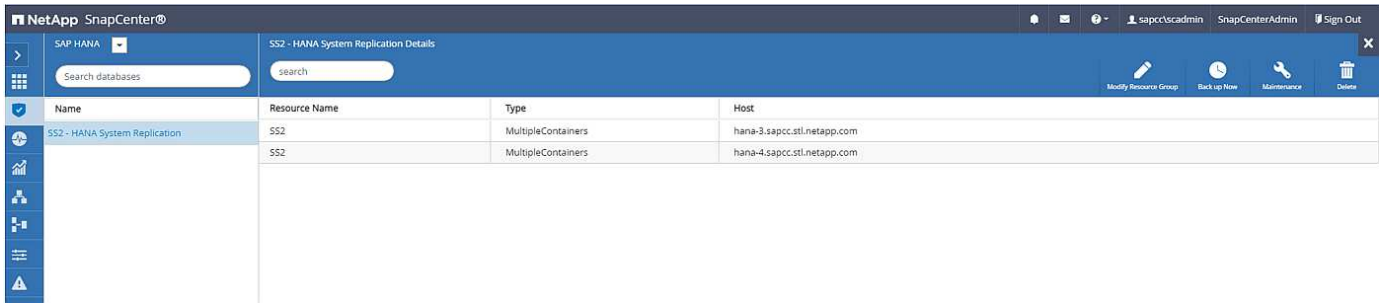


Die Richtlinien und Zeitpläne für die Ressourcengruppe werden konfiguriert.

> 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.

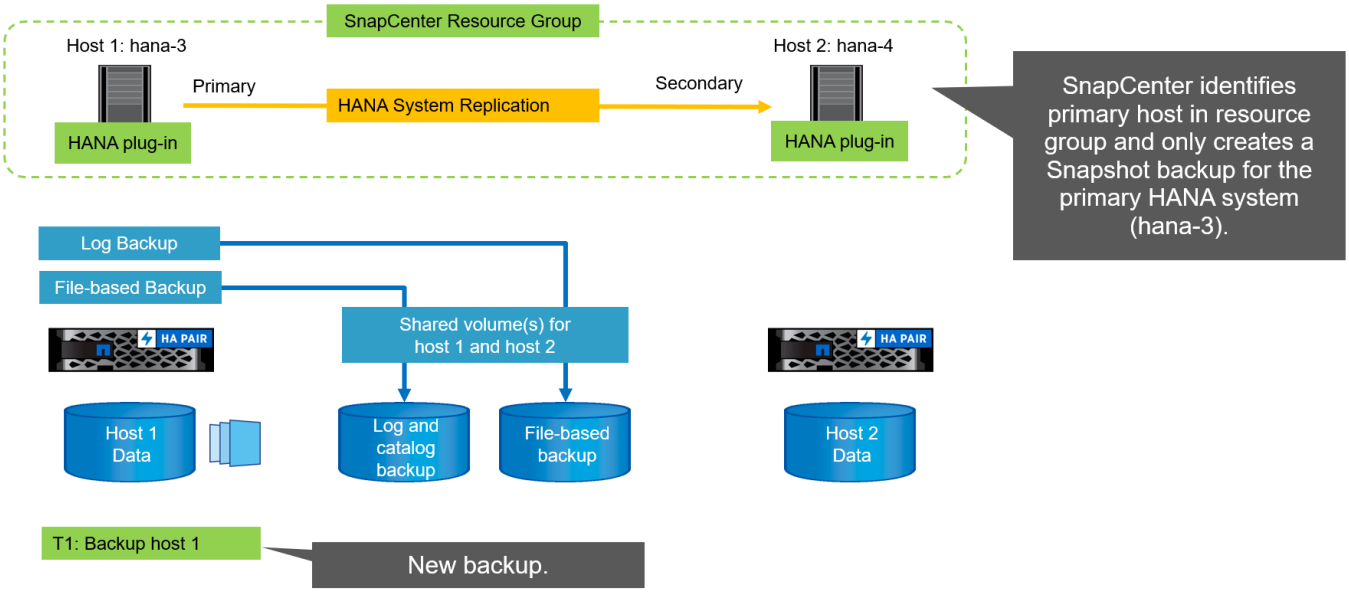


Die Konfiguration der Ressourcengruppe ist jetzt abgeschlossen und Backups können ausgeführt werden.

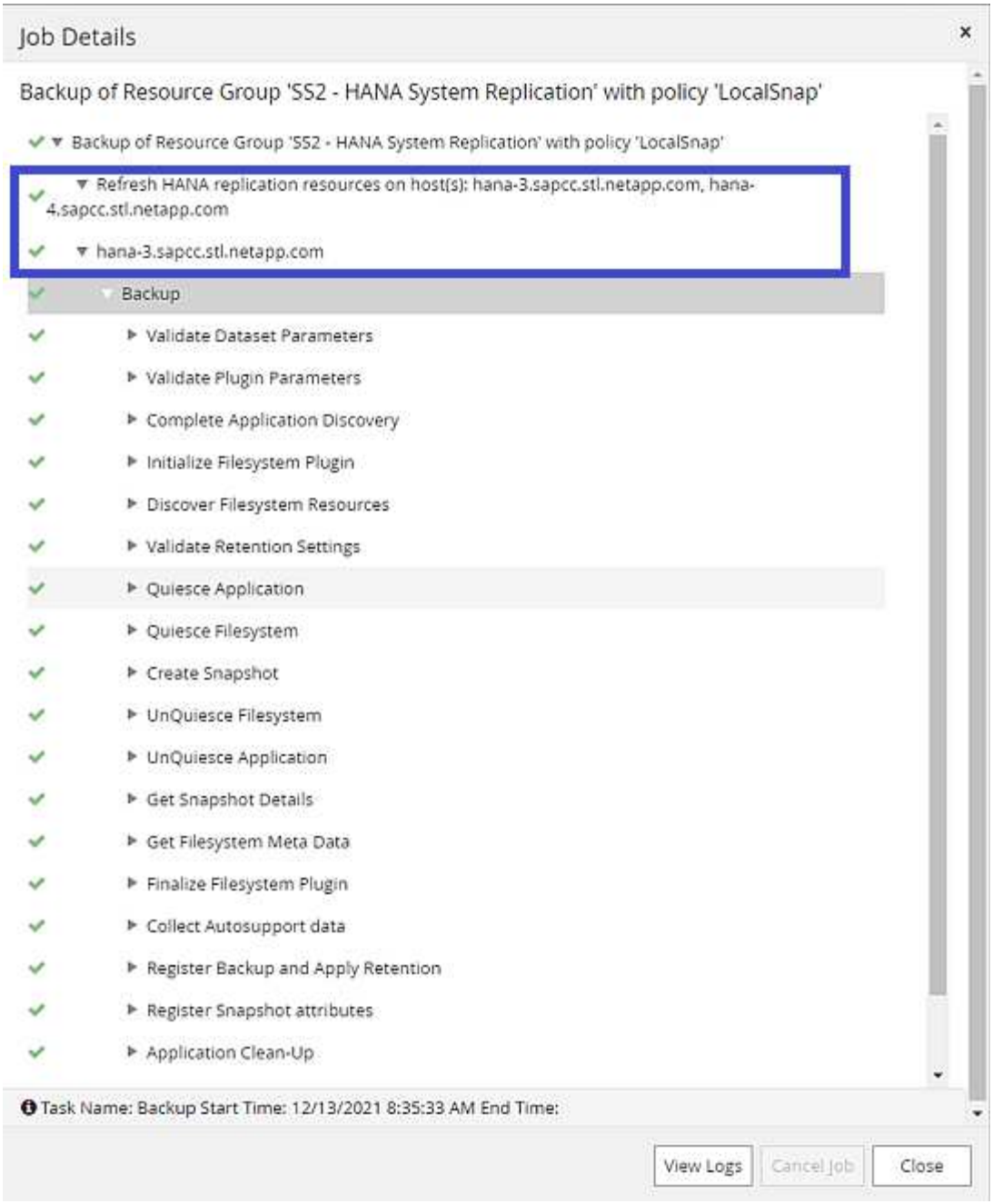


Snapshot-Backup-Vorgänge

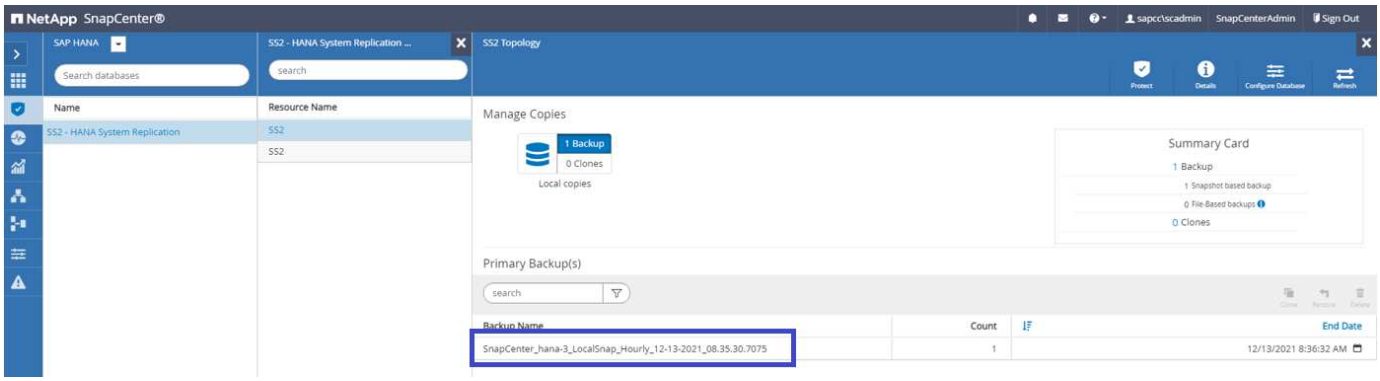
Wenn ein Backup-Vorgang der Ressourcengruppe ausgeführt wird, identifiziert SnapCenter den primären Host und löst nur ein Backup auf dem primären Host aus. Das bedeutet, dass nur das Daten-Volume des primären Hosts mit Snapshots erstellt werden wird. in unserem Beispiel ist hana-3 der aktuelle primäre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



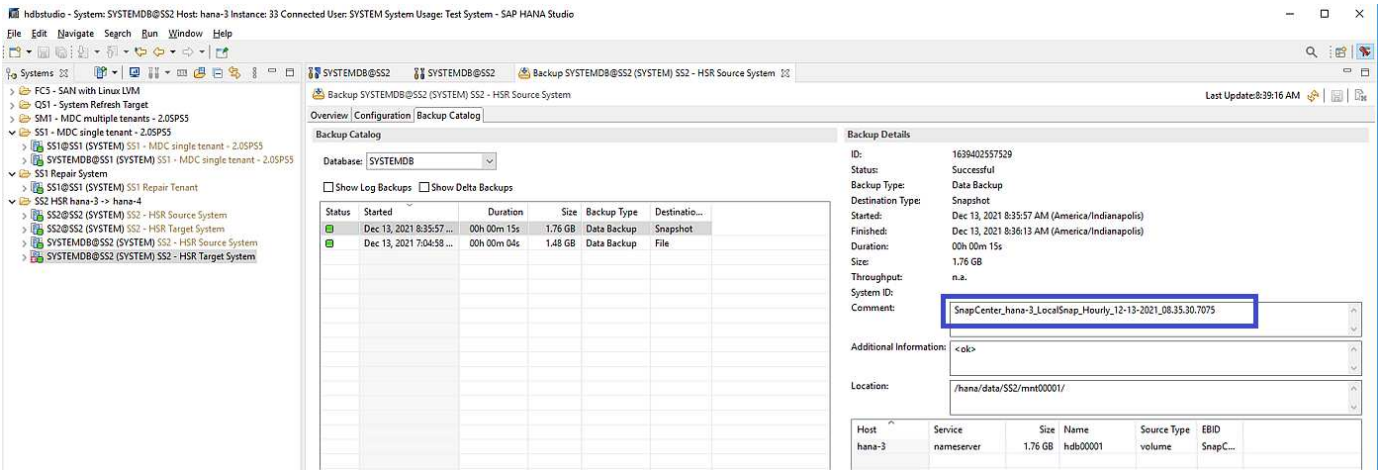
Das SnapCenter-Jobprotokoll zeigt den Identifizierungsvorgang und die Ausführung des Backups auf dem aktuellen primären Host hana-3.



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

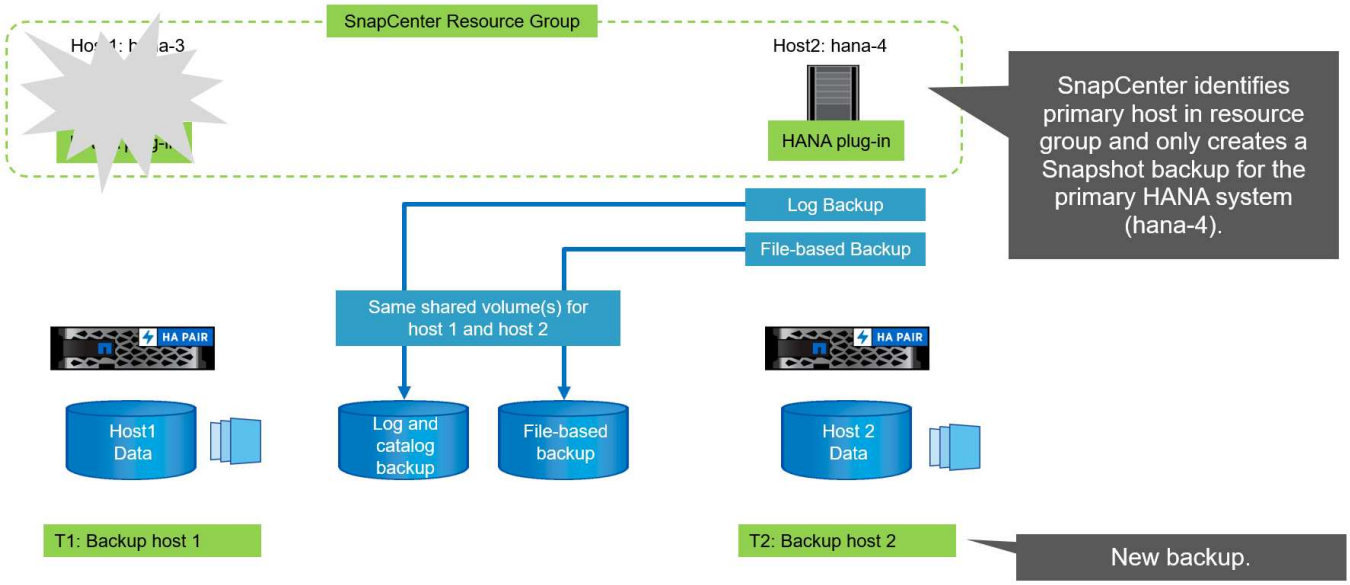


Das Snapshot-Backup ist auch im HANA-Backup-Katalog sichtbar.

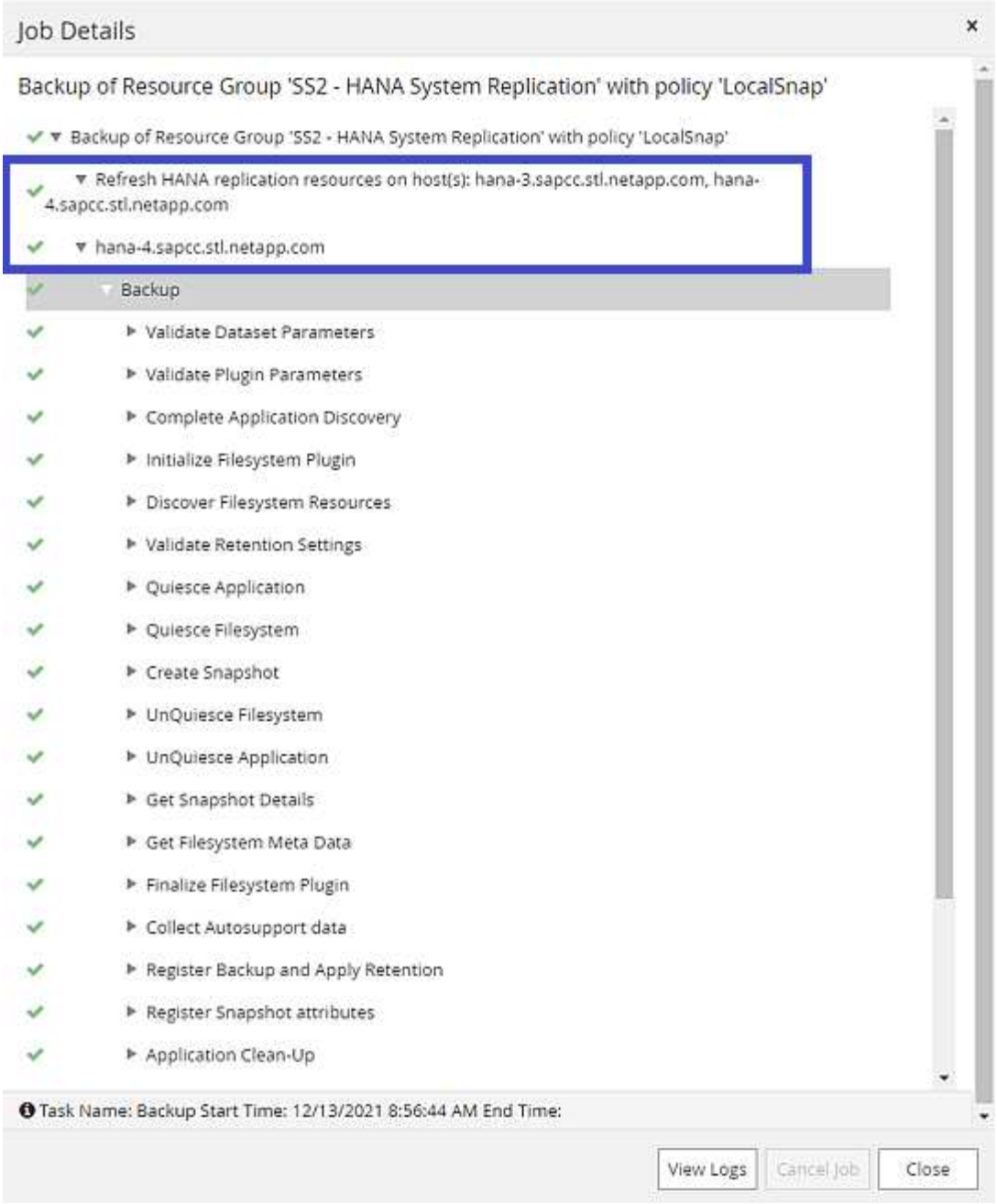


Falls ein Übernahmevorgang ausgeführt wird, identifizieren weitere SnapCenter Backups jetzt den früheren sekundären Host (hana-4) als primär und der Backup-Vorgang wird auf hana-4 ausgeführt. Erneut wird nur das Daten-Volume des neuen primären Hosts (hana-4) mit Snapshots erstellt.

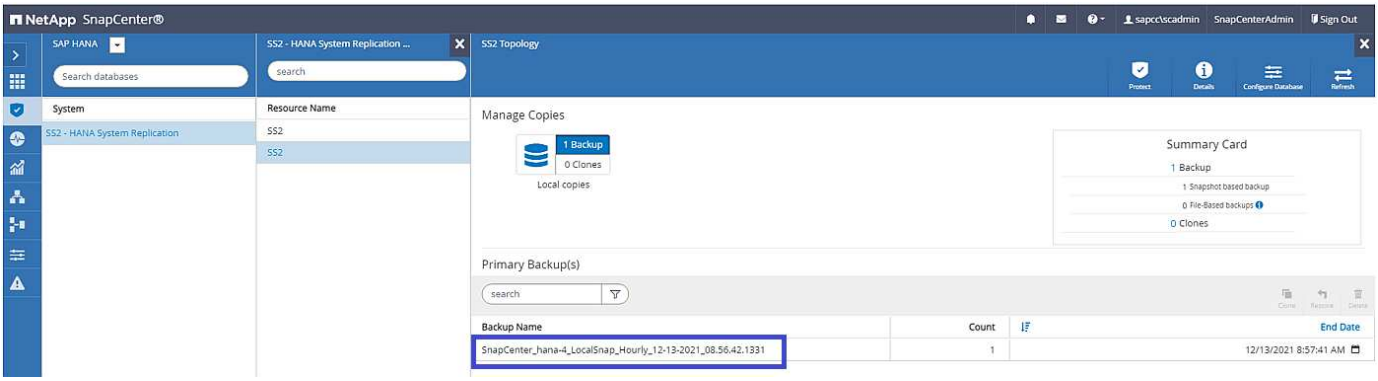
> Die SnapCenter-Identifizierungslogik deckt nur Szenarien ab, in denen sich die HANA-Hosts in einer primären/sekundären Beziehung befinden oder wenn einer der HANA-Hosts offline ist.



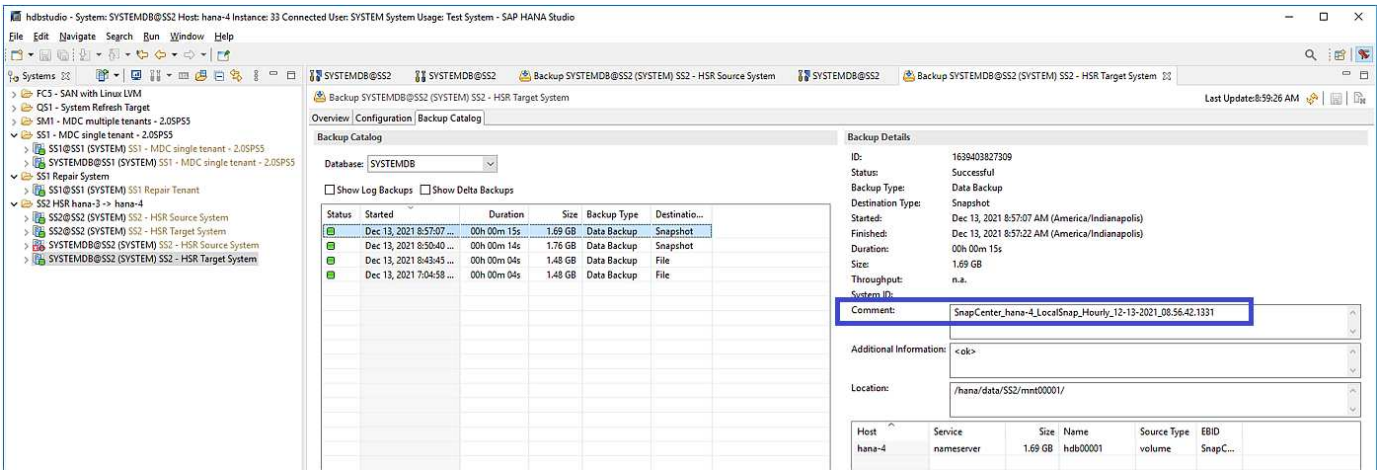
Das SnapCenter-Jobprotokoll zeigt den Identifizierungsvorgang und die Ausführung des Backups auf dem aktuellen primären Host hana-4.



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.

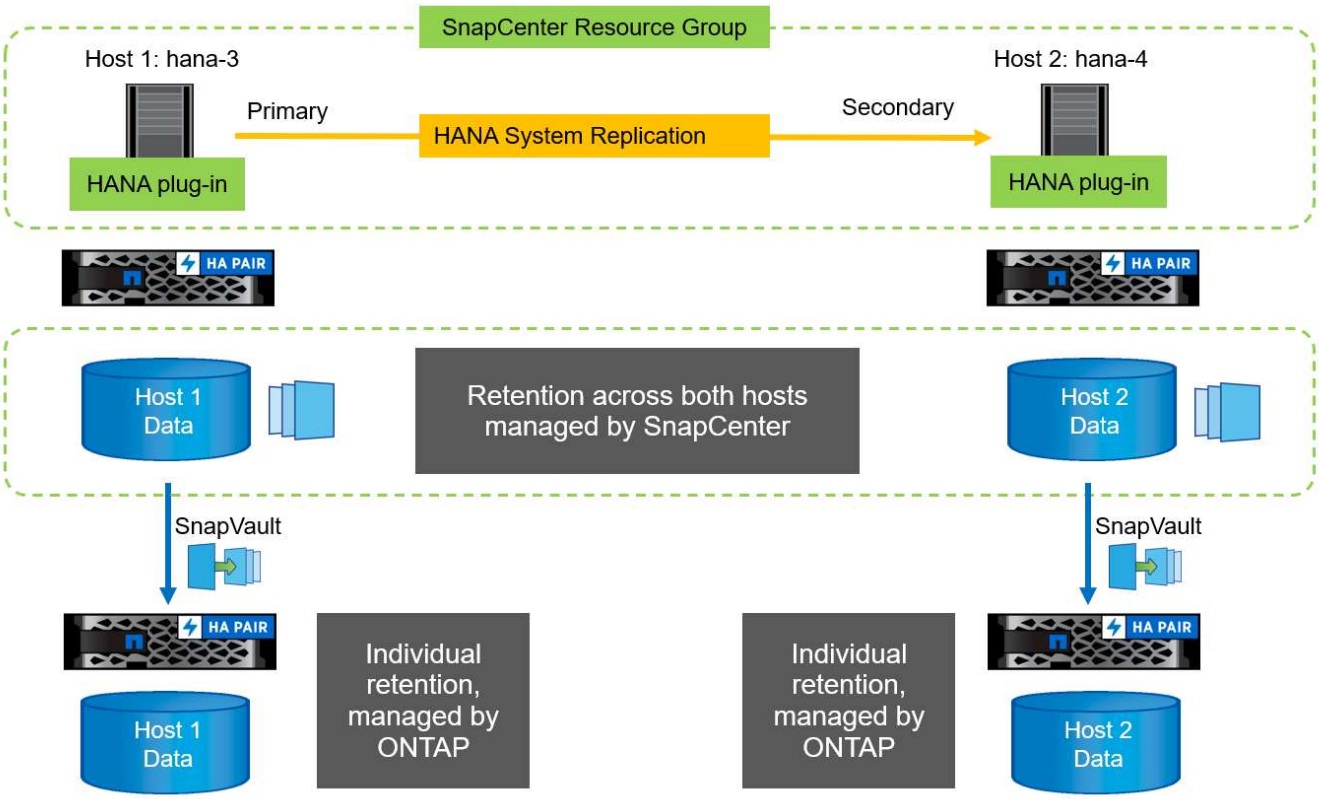
SnapVault Replizierung

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.



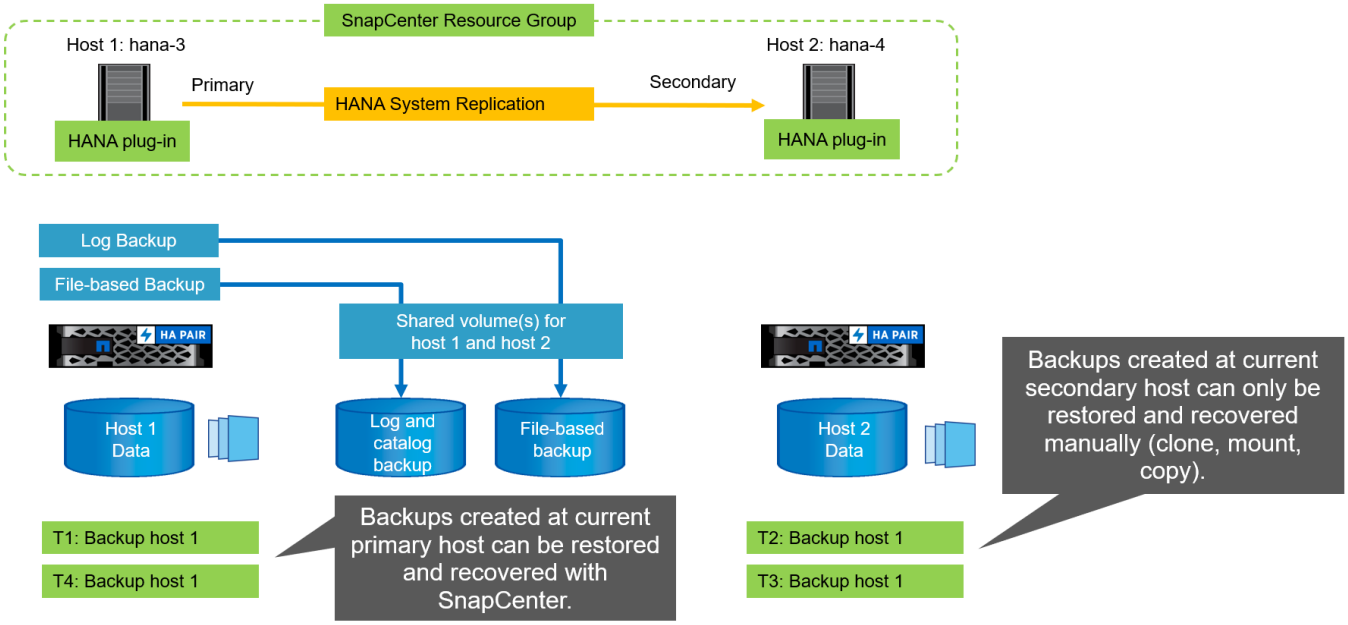
Retentionmanagement

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 SnapVault Replizierung Teil der Datensicherungsstrategie ist, ist für spezifische Szenarien eine manuelle Interaktion erforderlich, wie im Abschnitt beschrieben [SnapVault Replication].

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 Recovery-Vorgänge für eine SnapCenter 4.6-Ressourcengruppe sind identisch mit einer automatisch erkannten Konfiguration, die nicht vom System stammt. Alle Optionen für Restores und automatisiertes Recovery sind verfügbar. Weitere Einzelheiten finden Sie im technischen Bericht "TR-4614: SAP HANA Backup and Recovery with SnapCenter".

Eine Wiederherstellung 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".

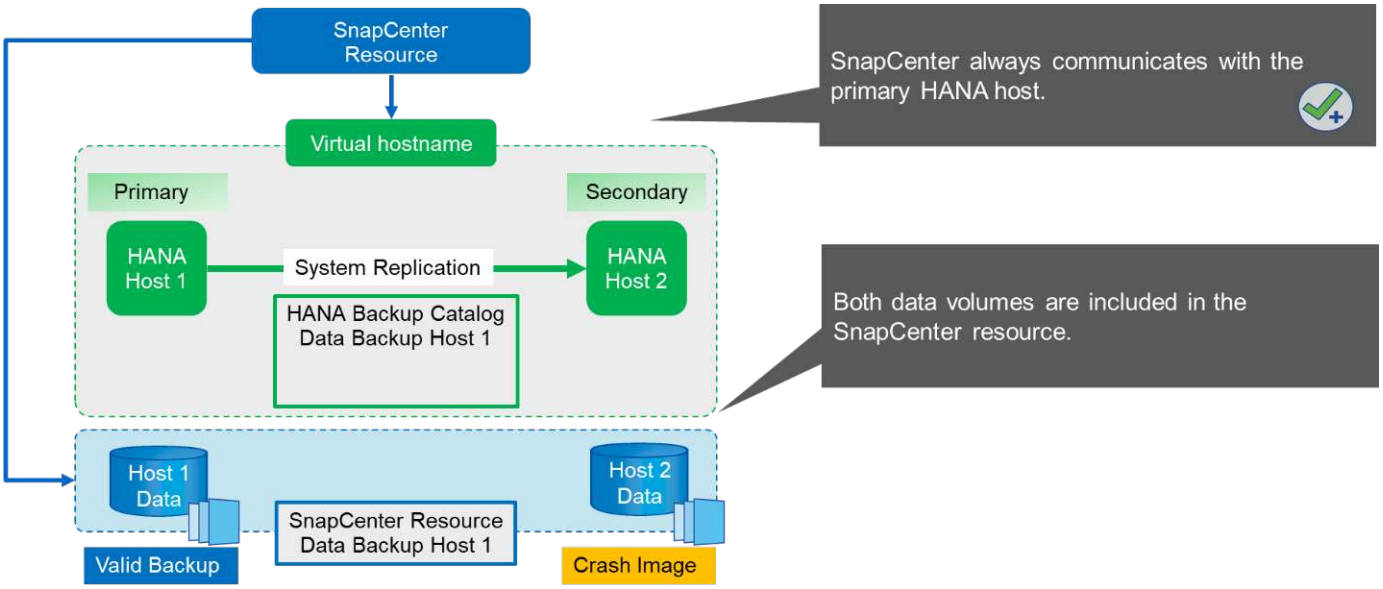
SnapCenter Konfiguration mit einer einzigen Ressource

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.

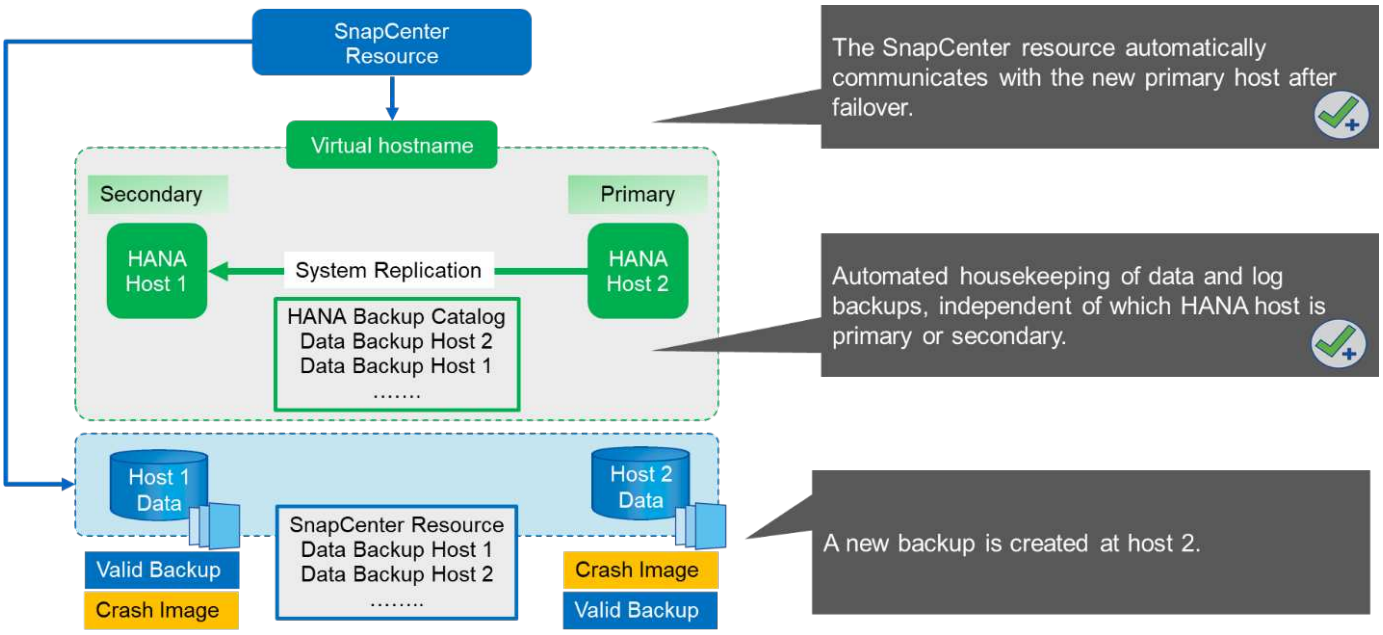
Wird ein Backup mit Host 1 als primärer Host ausgeführt, wird ein datenbankkonsistentes Snapshot-Backup auf dem Datenvolumen von Host 1 erstellt. Da das Daten-Volume des Hosts 2 Teil der SnapCenter Ressource ist, wird für dieses Volume eine weitere Snapshot Kopie erstellt. Diese Snapshot Kopie ist nicht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

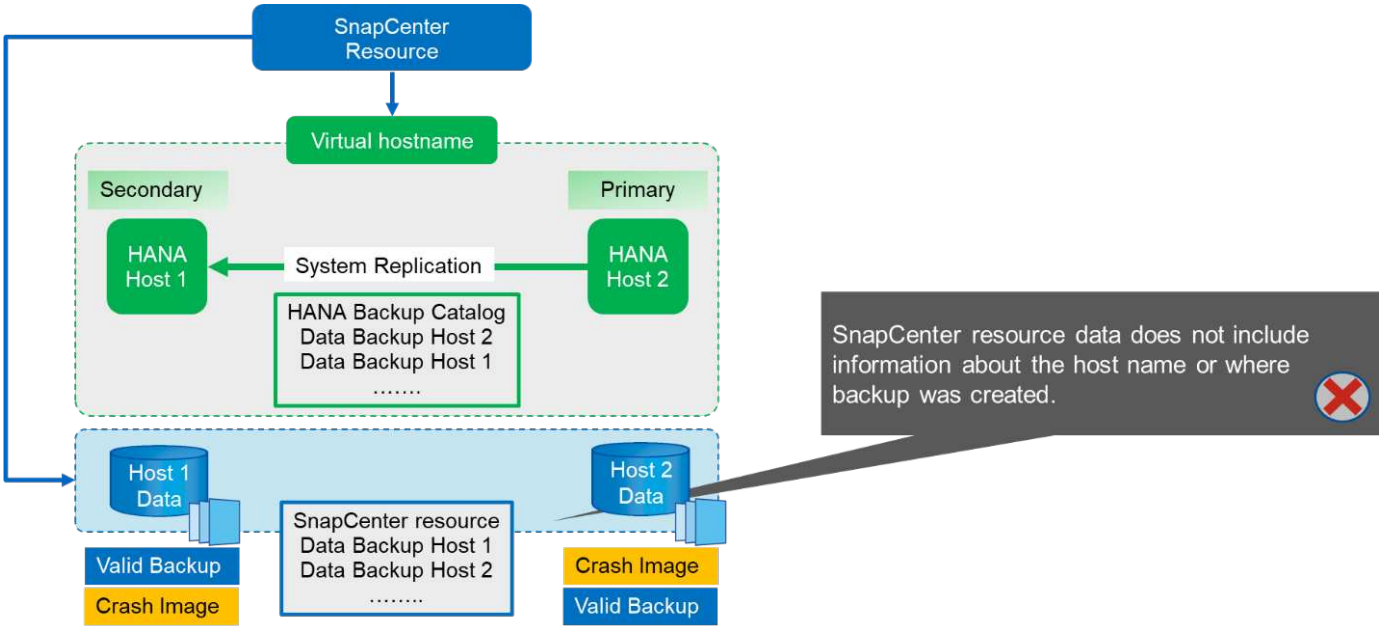
Die allgemeine Ordnung und Sauberkeit der Daten- und Log-Backups basiert auf der definierten SnapCenter-Aufbewahrungsrichtlinie und die Backups werden unabhängig vom primären oder sekundären Host gelöscht.



Wie im Abschnitt beschrieben "Storage Snapshot Backups und SAP System Replication", Eine Wiederherstellungsfunktion mit Storage-basierten Snapshot-Backups ist unterschiedlich, 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.

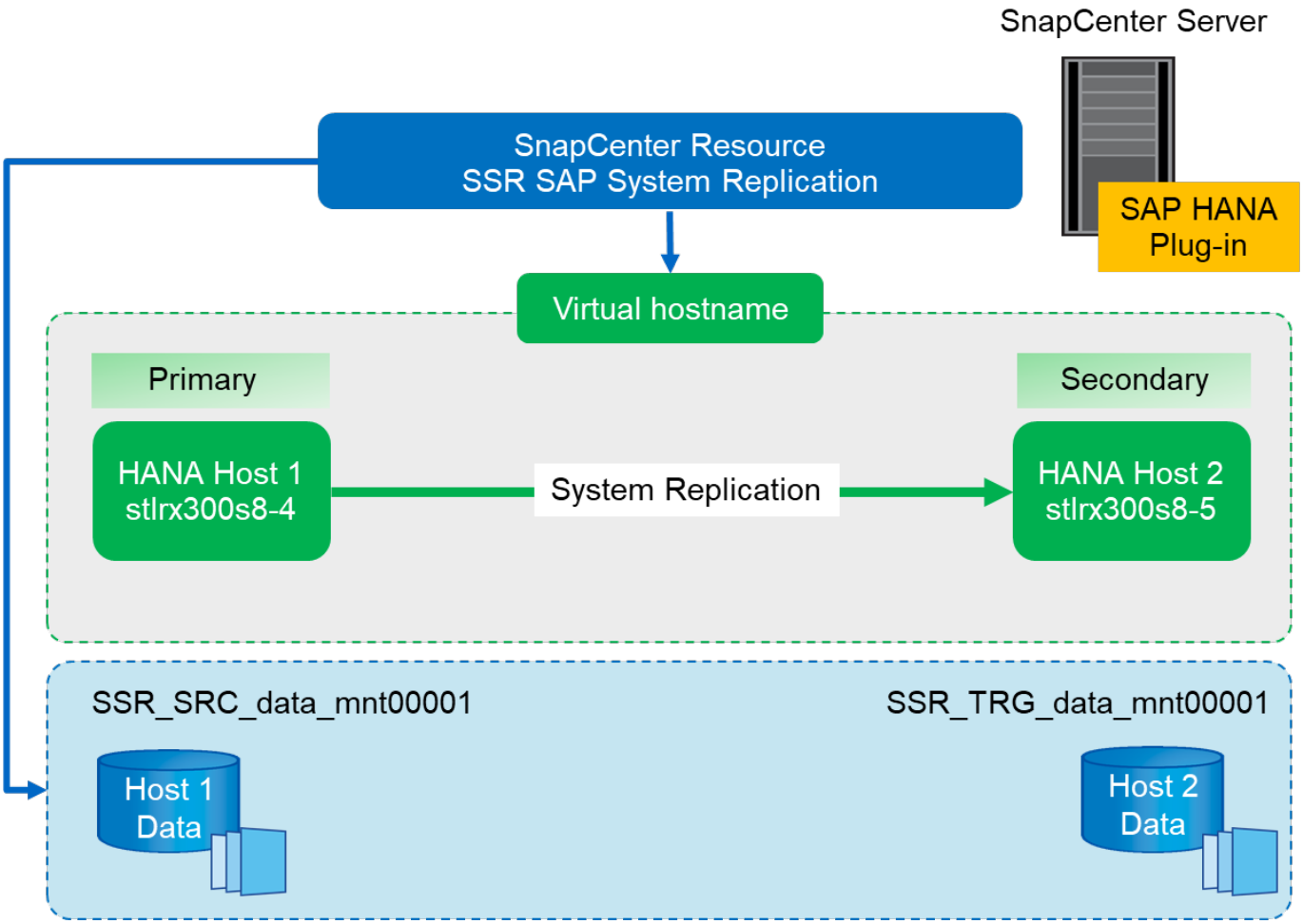
Bei einer SnapCenter-Konfiguration mit nur einem Mitarbeiter ist SnapCenter nicht bewusst, wo das Backup erstellt wurde. NetApp empfiehlt daher, dem SnapCenter Backup-Workflow ein Pre-Backup-Skript hinzuzufügen, um zu ermitteln, welcher Host derzeit der primäre SAP HANA-Host ist.

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.



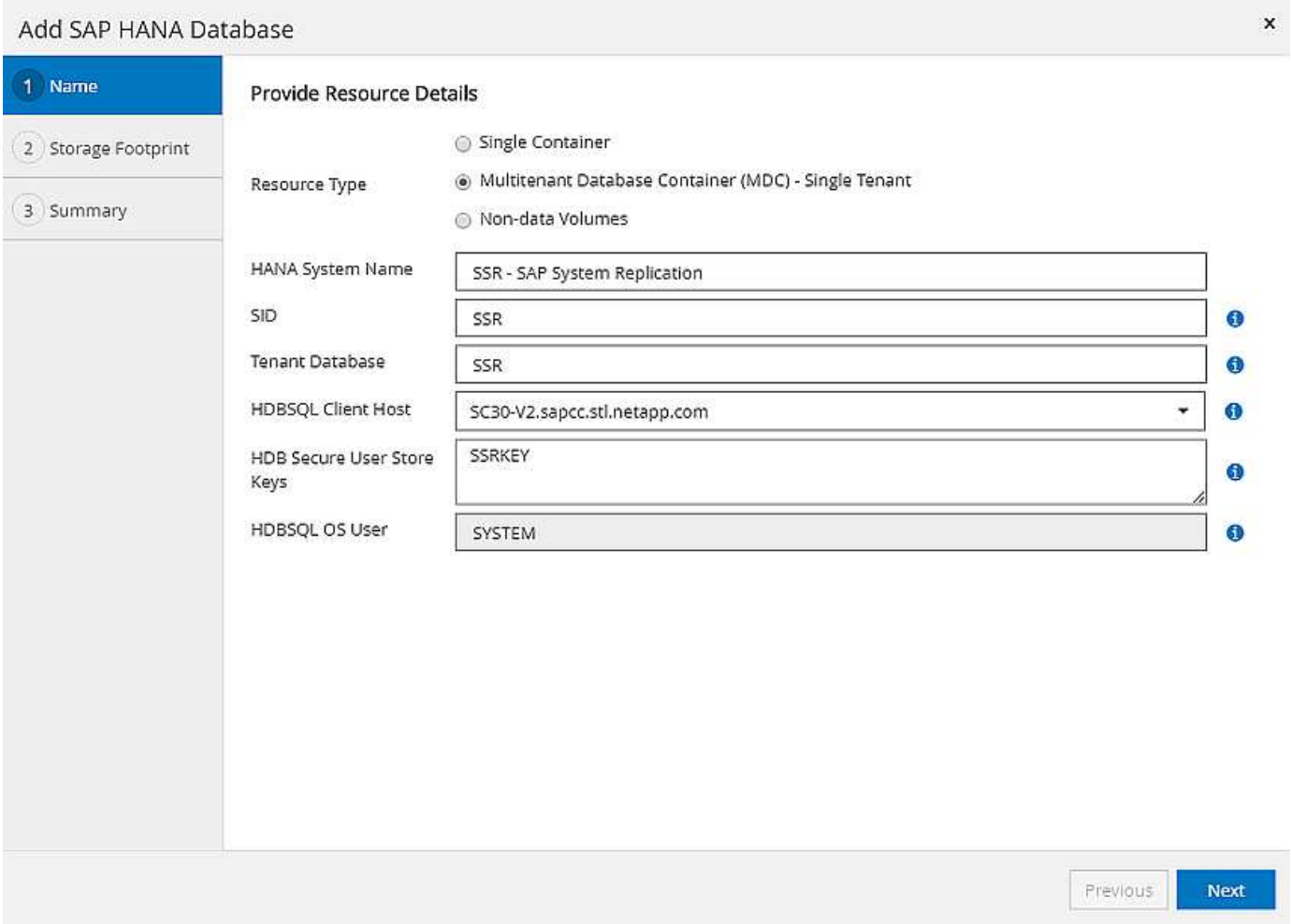
Um Backup-Vorgänge unabhängig davon durchzuführen, welcher SAP HANA Host primär ist und selbst wenn ein Host ausfällt, muss das SnapCenter SAP HANA Plug-in auf einem zentralen Plug-in-Host implementiert werden. In unserer Lab-Einrichtung wurde der SnapCenter Server als zentraler Plug-in-Host verwendet,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

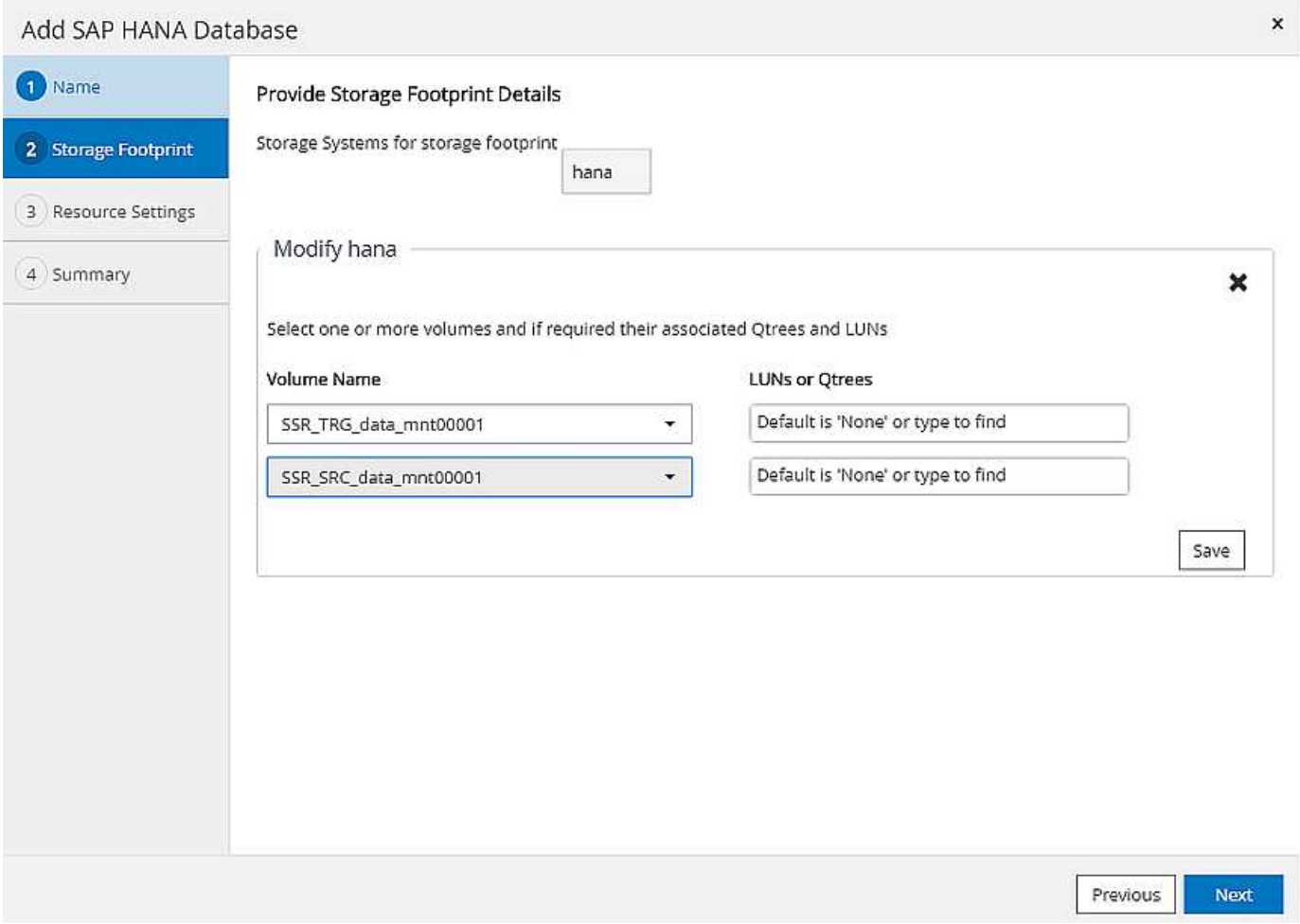
```
hdbuserstore.exe -u SYSTEM set SSRKEY ssr-vip:31013 SNAPCENTER <password>
```

Weitere Informationen zu SAP HANA Plug-in-Implementierungsoptionen und User-Store-Konfiguration finden Sie im technischen Bericht TR-4614: "Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter".

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.

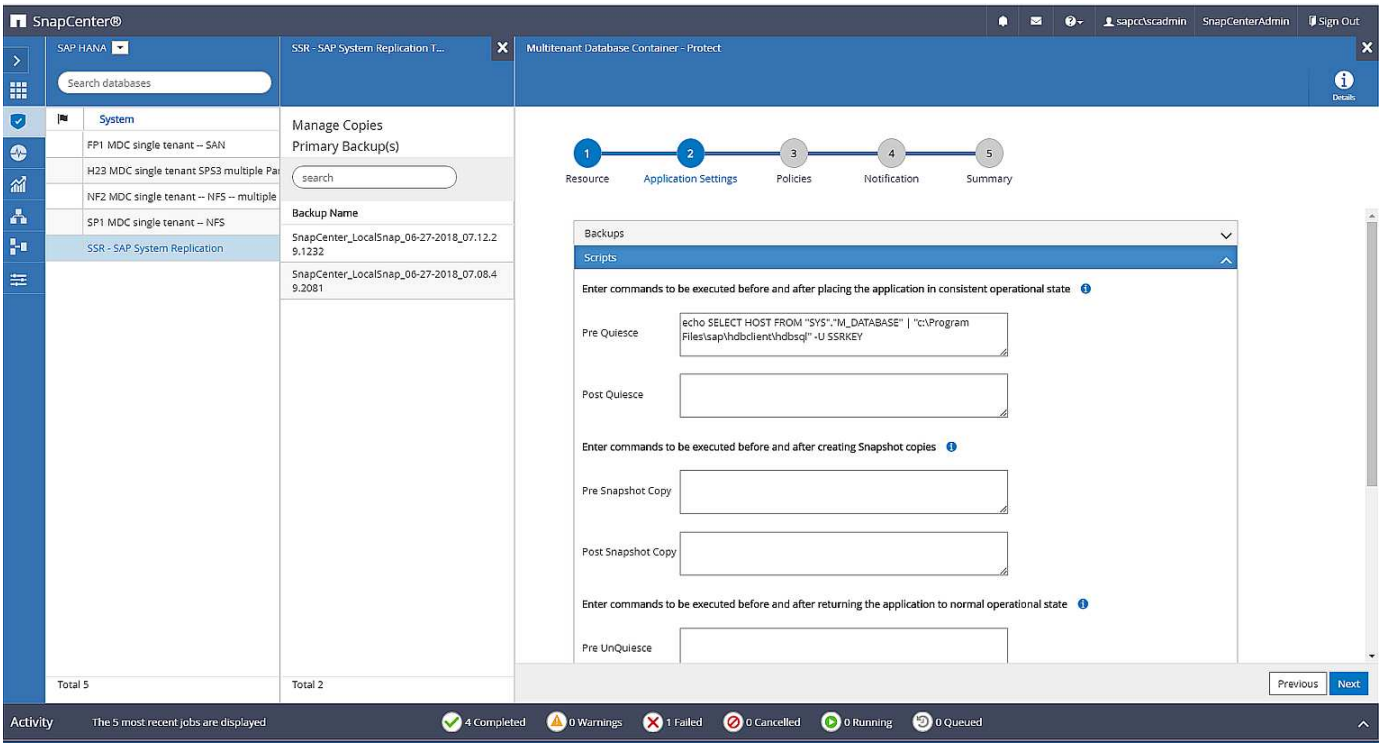


Die Datenvolumen der beiden SAP HANA-Hosts sind in der Storage-Platzbedarf-Konfiguration enthalten, wie die folgende Abbildung zeigt.



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
```

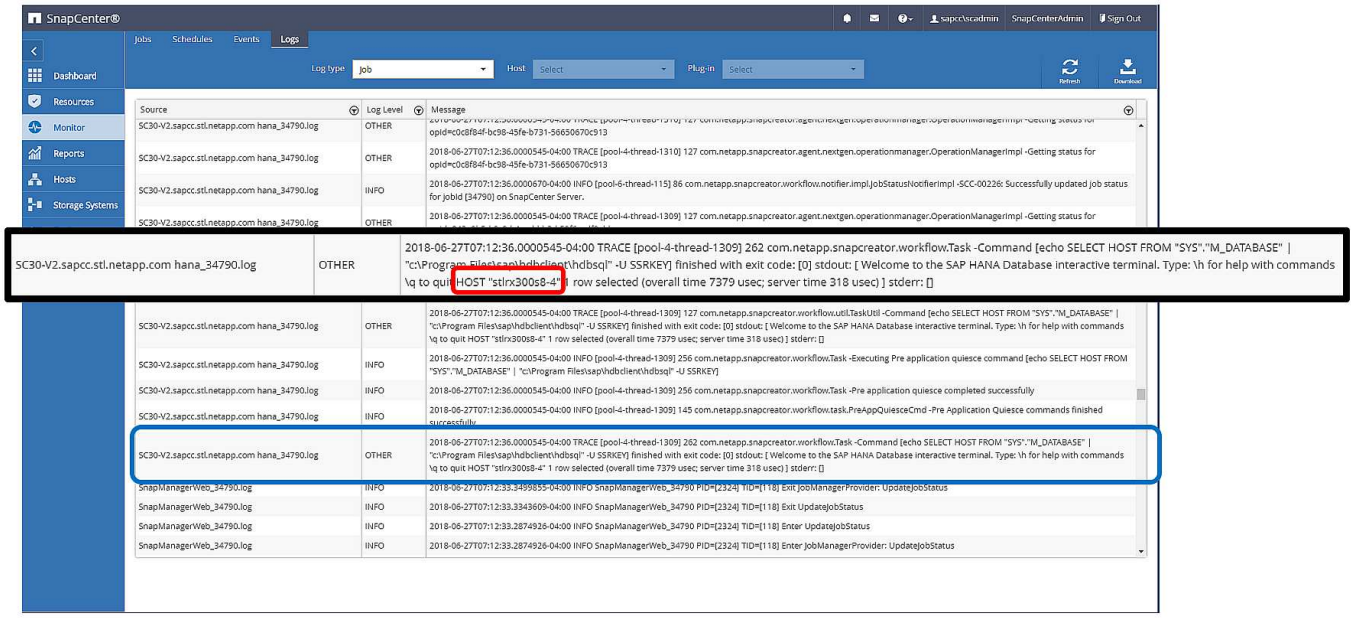


SnapCenter Backup-Vorgang

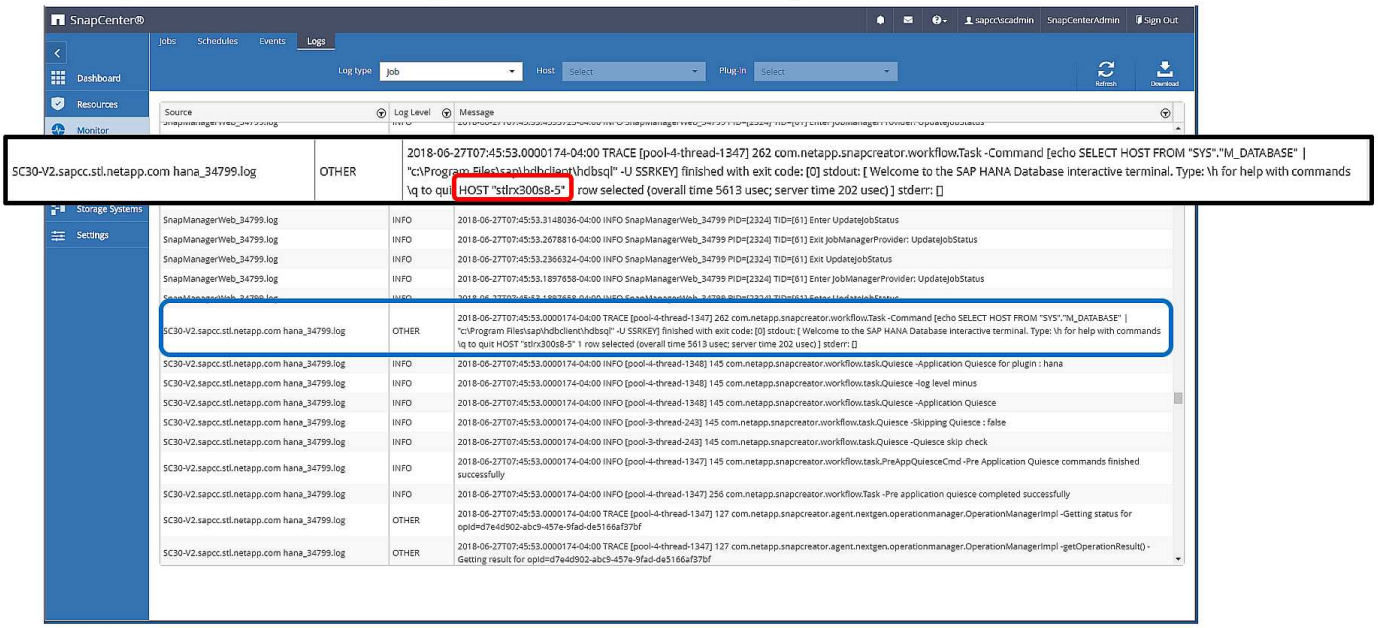
Backup-Vorgänge werden jetzt wie gewohnt ausgeführt. Die allgemeine Ordnung und Sauberkeit der Daten und Log-Backups wird unabhängig davon durchgeführt, welcher SAP HANA-Host primärer oder sekundärer ist.

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.

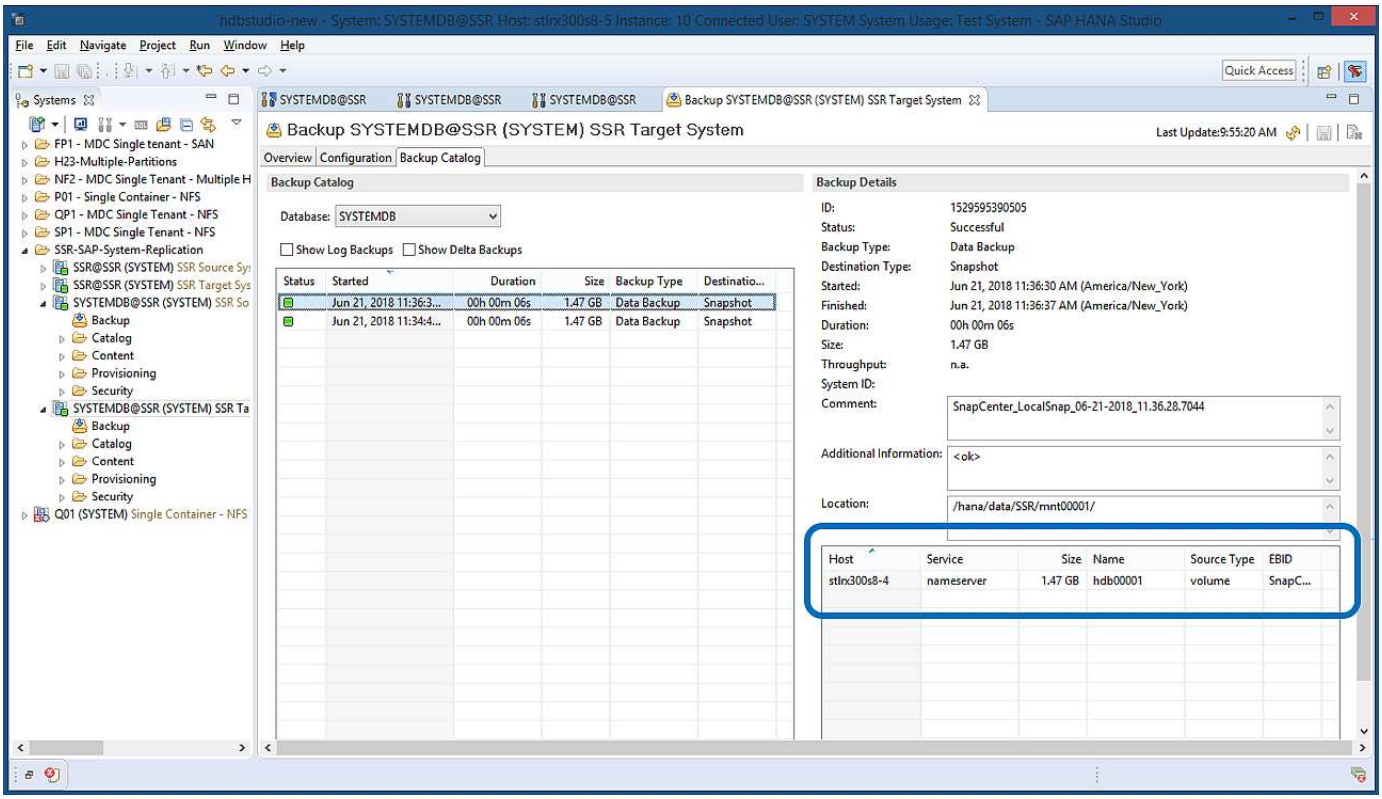


Diese Abbildung zeigt das Backup-Jobprotokoll mit Host 2 als primärer Host.



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.



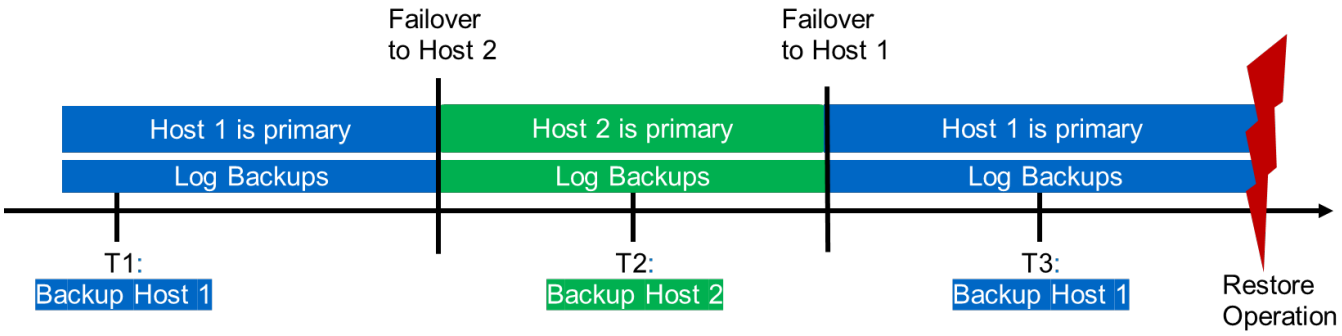
Restore und Recovery

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

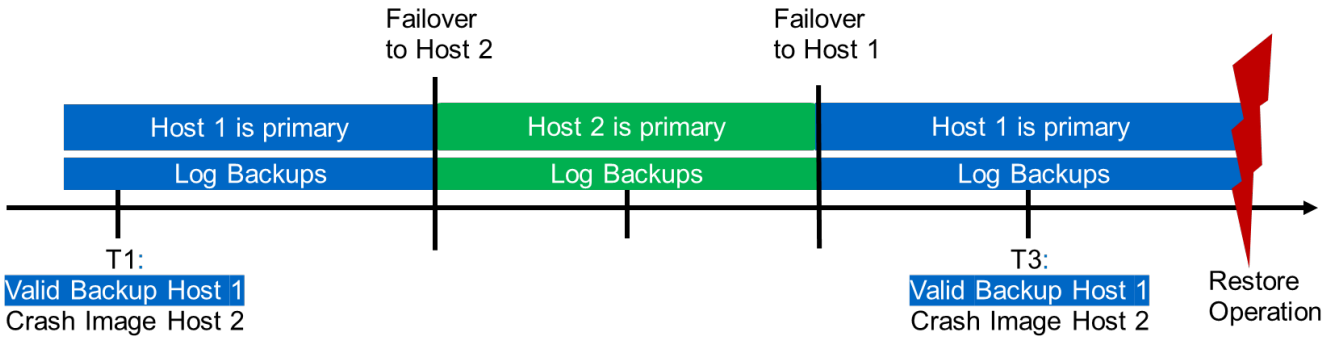
Mit einer einzelnen SnapCenter Ressourcenkonfiguration werden Snapshot Kopien auf beiden Storage-Volumes sowohl von SAP HANA System Replication Hosts erstellt. Nur das Snapshot-Backup, das auf dem Storage-Volume des primären SAP HANA-Hosts erstellt wird, ist für die zukünftige Recovery gültig. Die auf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

Eine Wiederherstellung 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.

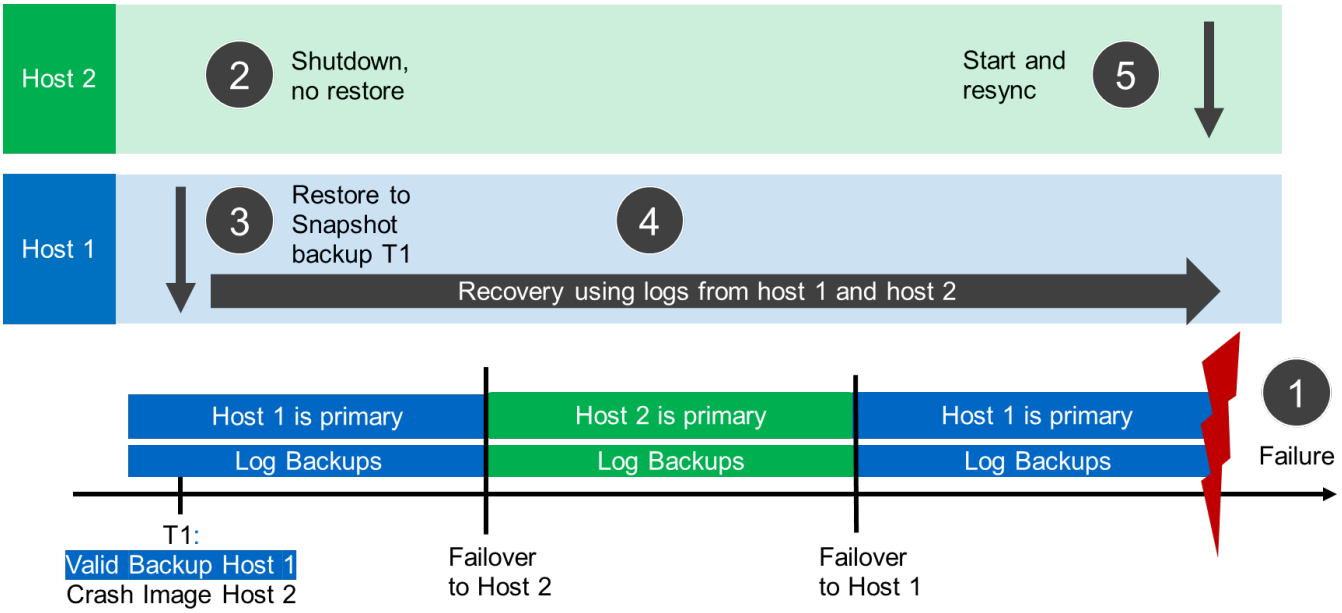


SnapCenter Restore nur für gültige Backups

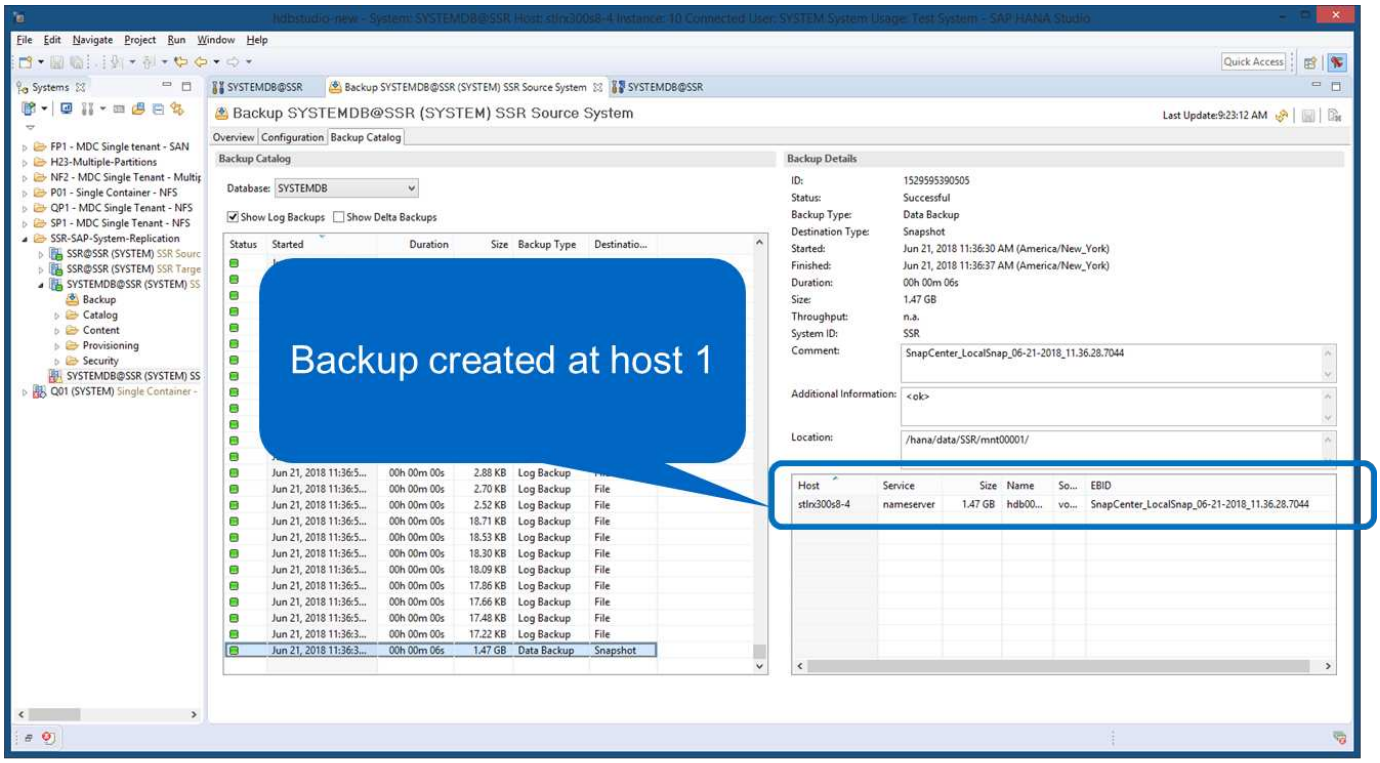
Die folgende Abbildung zeigt einen Überblick über das in diesem Abschnitt beschriebene Wiederherstellungsszenario.

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.



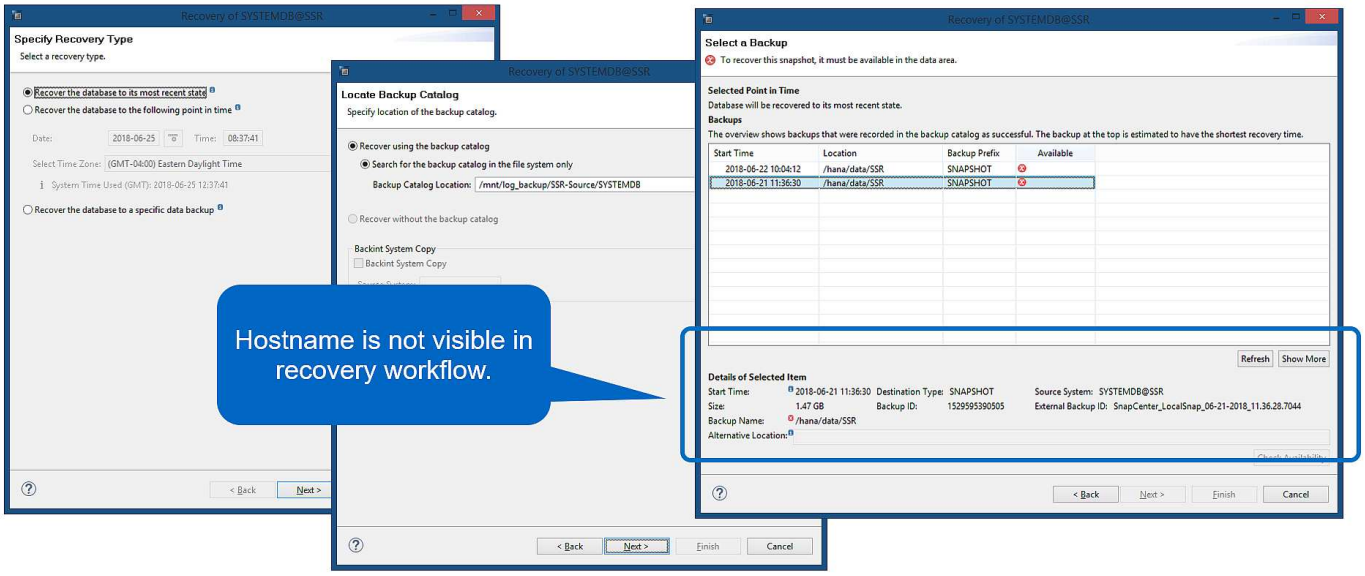
Die folgende Abbildung zeigt den SAP HANA Backup-Katalog in SAP HANA Studio. Die hervorgehobene Sicherung zeigt die Sicherung, die am T1 bei Host 1 erstellt wurde.



25

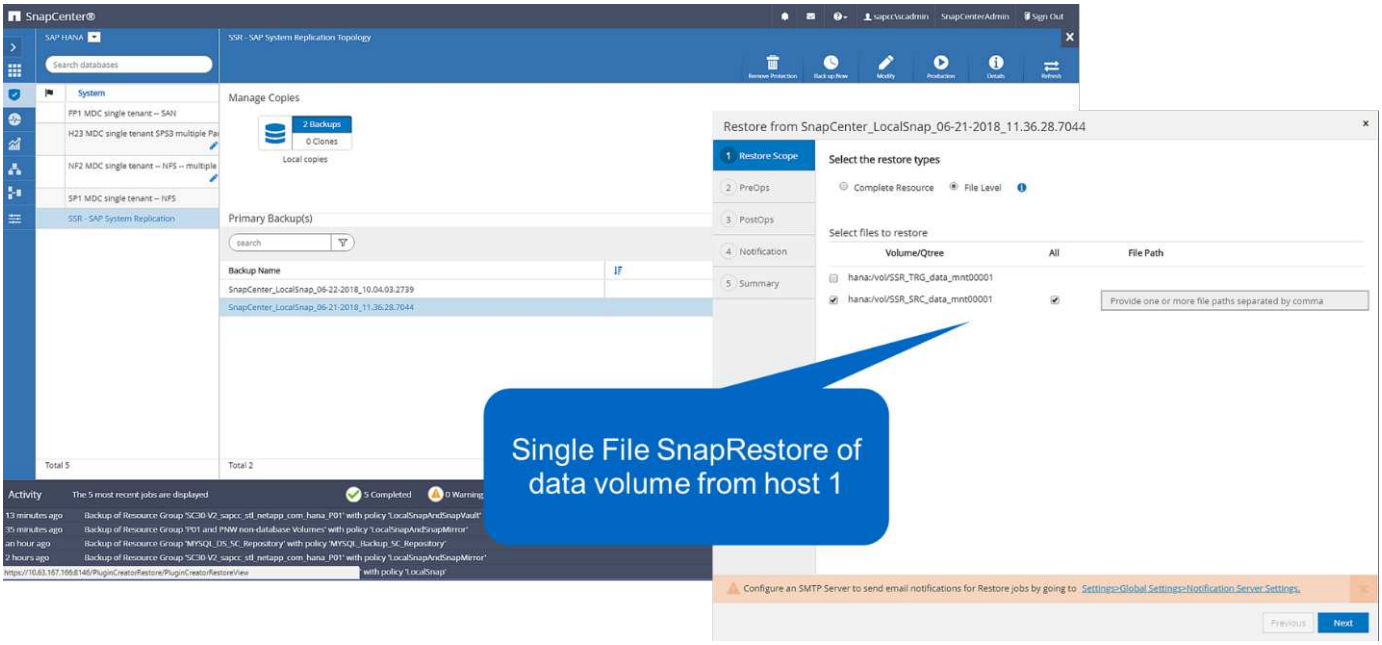
Im SAP HANA Studio wird eine Wiederherstellung gestartet. Wie die folgende Abbildung zeigt, ist der Name des Hosts, auf dem das Backup erstellt wurde, im Wiederherstellungsworkflow nicht sichtbar.

> 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.

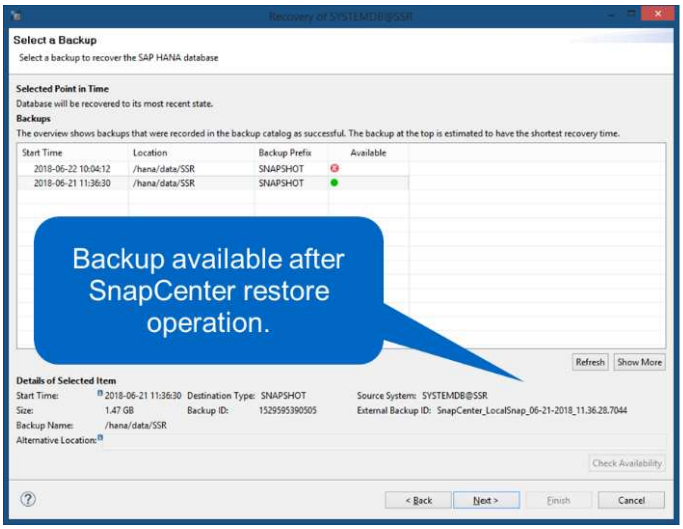


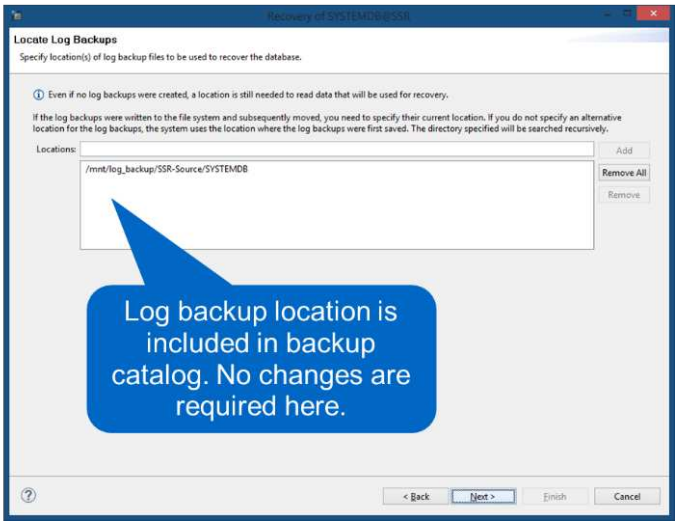
In SnapCenter wird das Backup ausgewählt und ein Restore-Vorgang auf Dateiebene durchgeführt. Auf dem Bildschirm Wiederherstellung auf Dateiebene wird nur das Host 1 Volume ausgewählt, sodass nur das gültige

Backup wiederhergestellt wird.



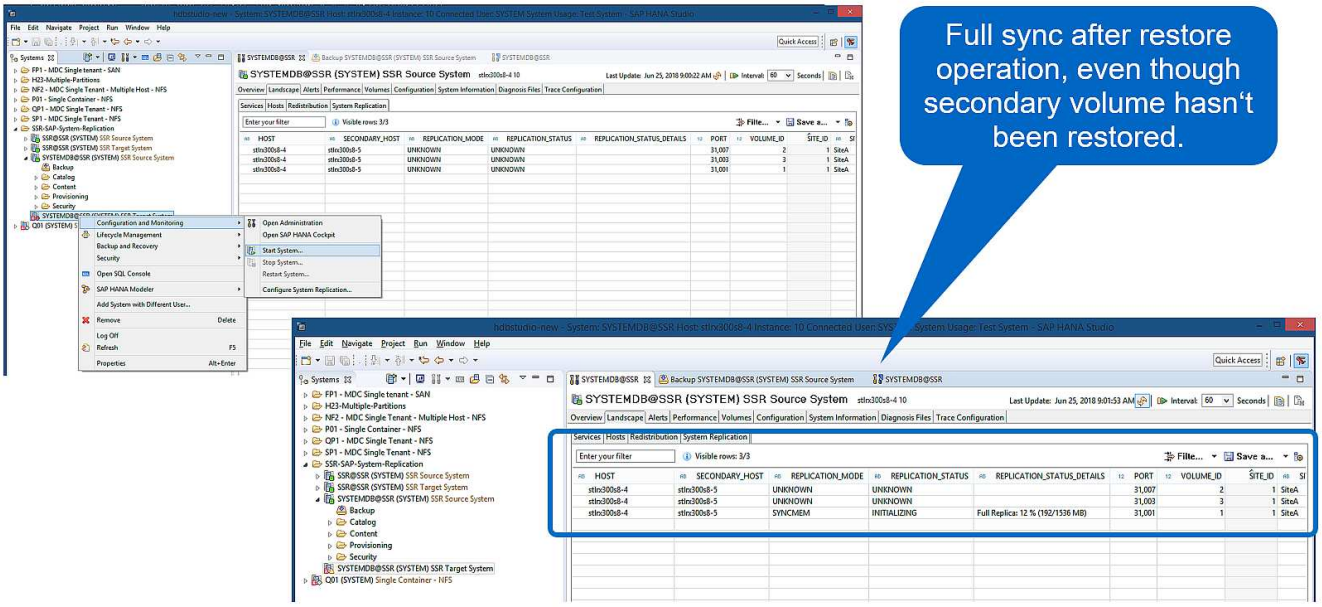
Nach der Wiederherstellung wird das Backup in SAP HANA Studio grün hervorgehoben. Sie müssen nicht einen zusätzlichen Log-Backup-Speicherort eingeben, weil der Dateipfad der Log-Backups von Host 1 und Host 2 im Backup-Katalog enthalten sind.





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.

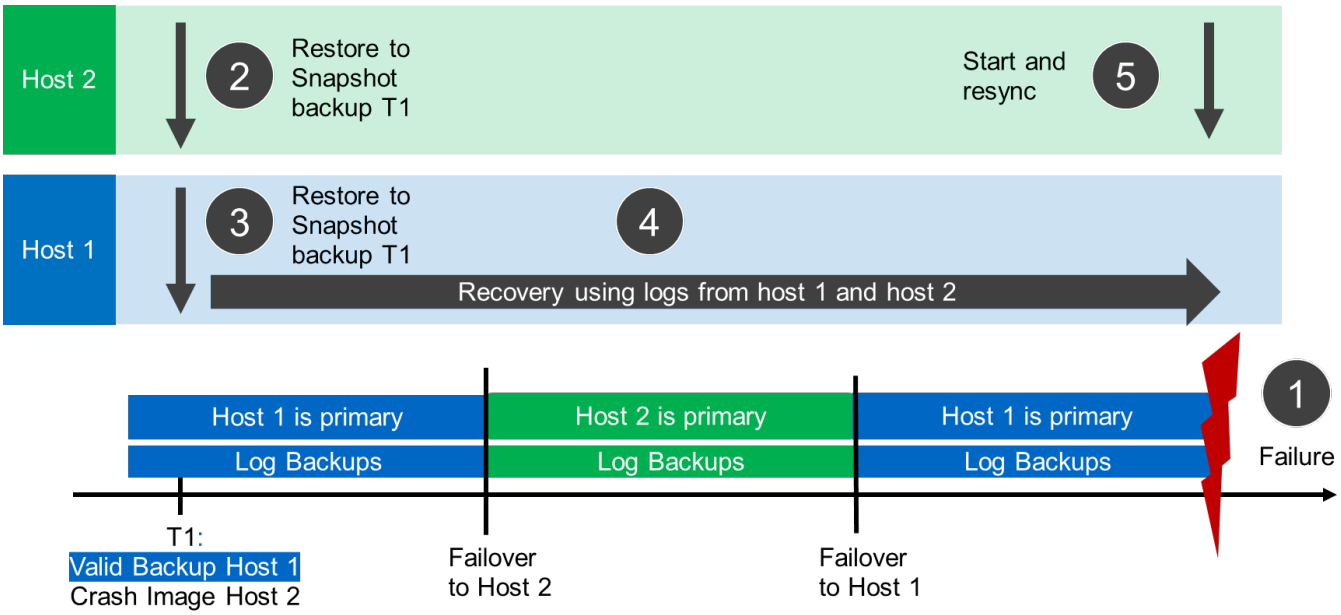


SnapCenter Restore von gültigem Backup- und Crash-Image

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

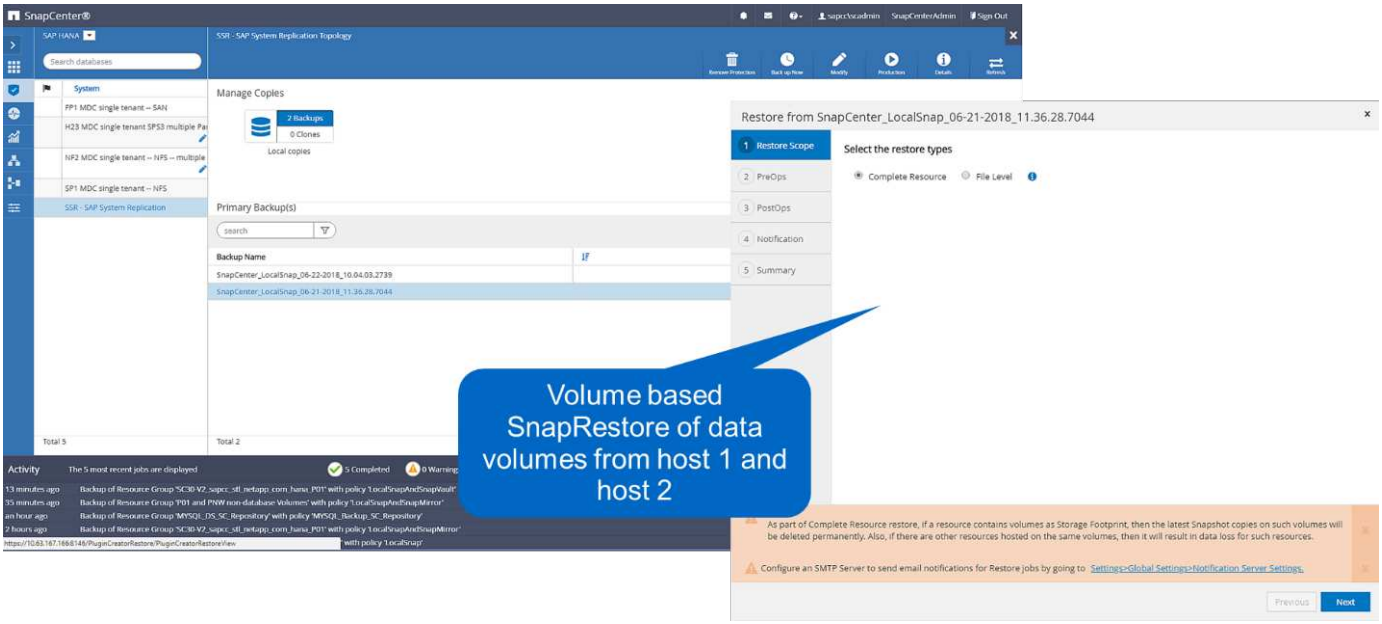
Bei T1 am Host 1 wurde ein Backup erstellt. Ein Failover wurde an Host 2 durchgeführt. Nach einem bestimmten Zeitpunkt wurde ein weiteres Failover zurück zu Host 1 durchgeführt. Zum aktuellen Zeitpunkt ist Host 1 der primäre Host.

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.

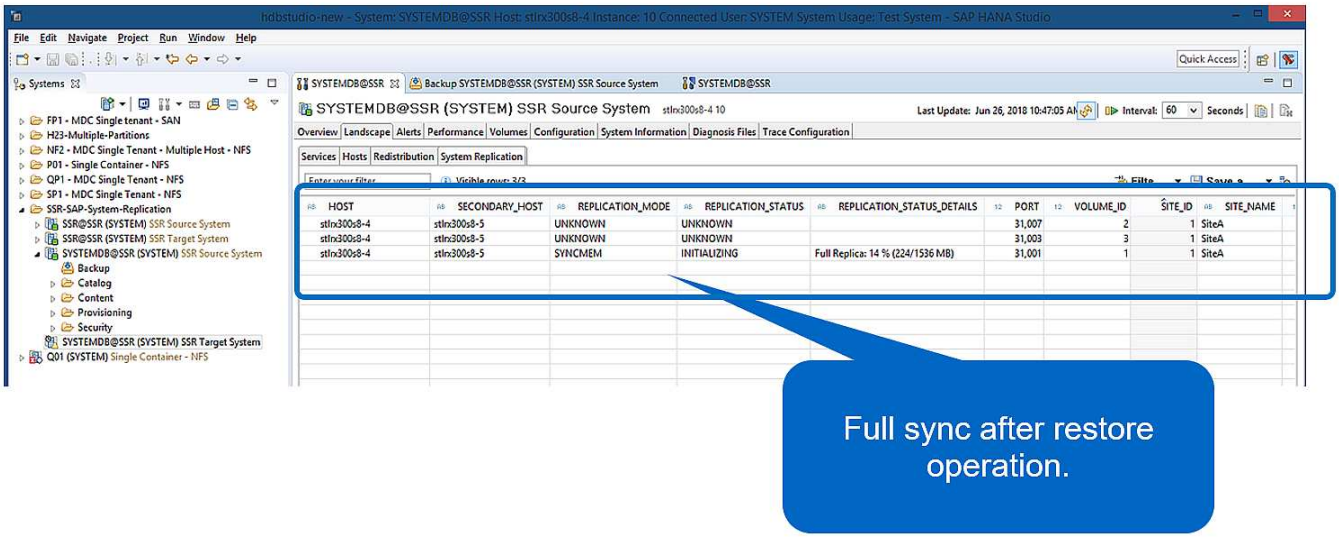


Der Restore- und Recovery-Vorgang mit SAP HANA Studio entspricht den im Abschnitt beschriebenen Schritten "SnapCenter Restore nur für gültige Backups".

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.



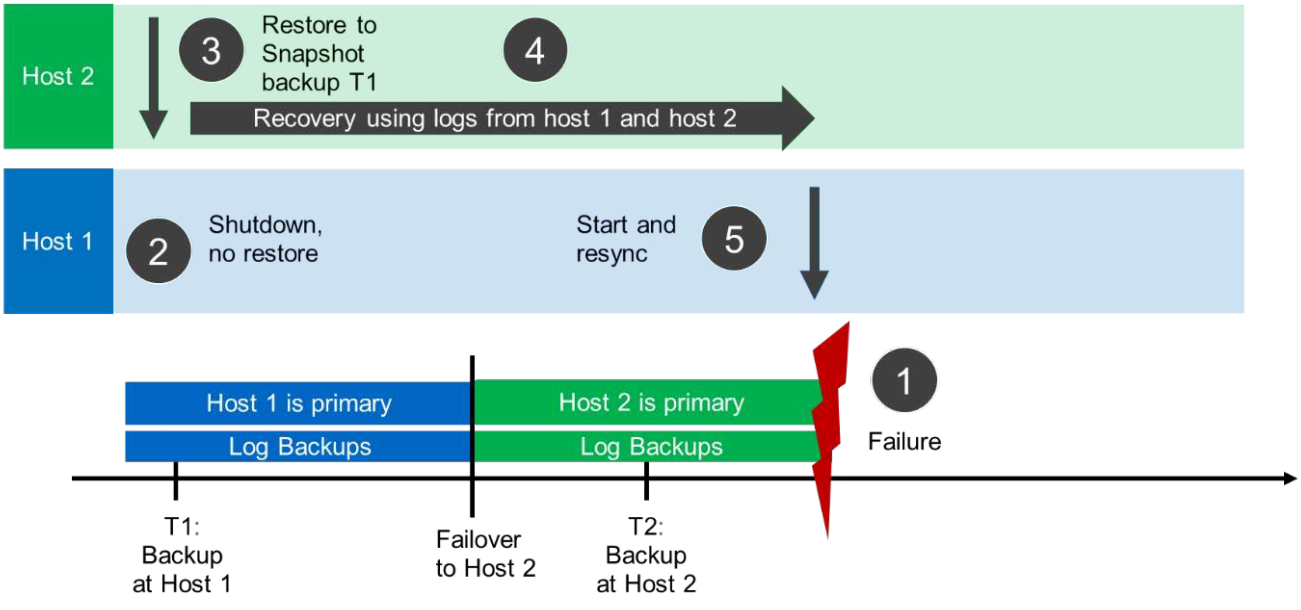
Wiederherstellung und Recovery von einem auf dem anderen Host erstellten Backup

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

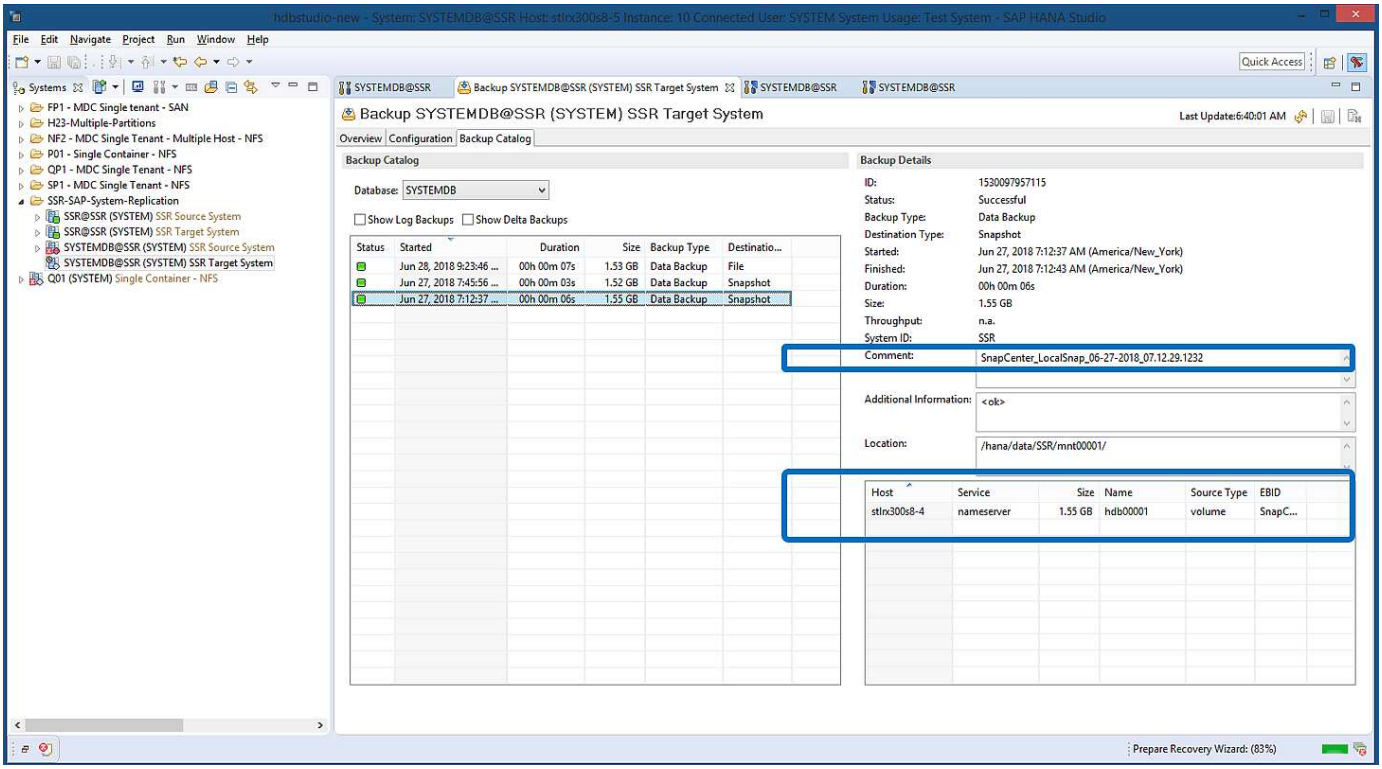
Die folgende Abbildung zeigt einen Überblick über das in diesem Abschnitt beschriebene Wiederherstellungsszenario.

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.



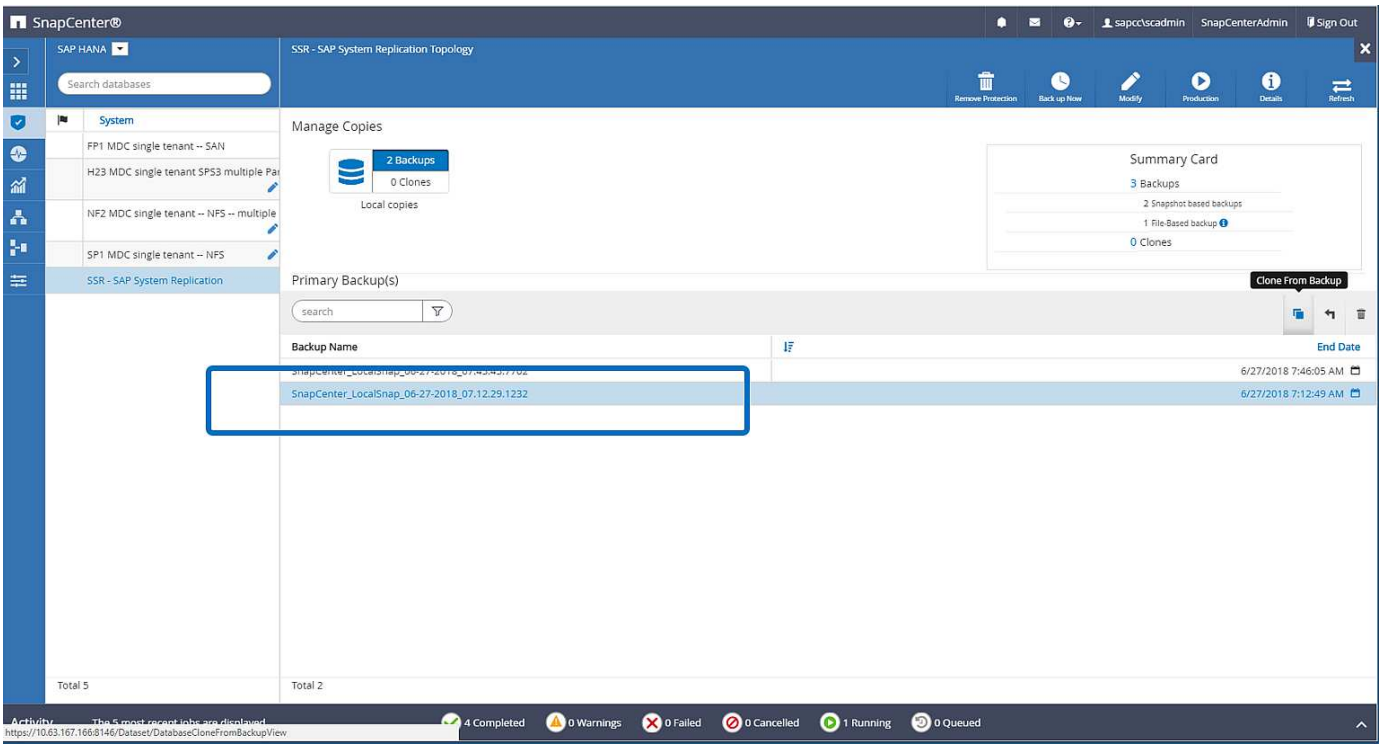
Die folgende Abbildung zeigt den SAP HANA Backup-Katalog und hebt das auf Host 1 erstellte Backup hervor, das für den Restore- und Recovery-Vorgang verwendet wurde.



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.

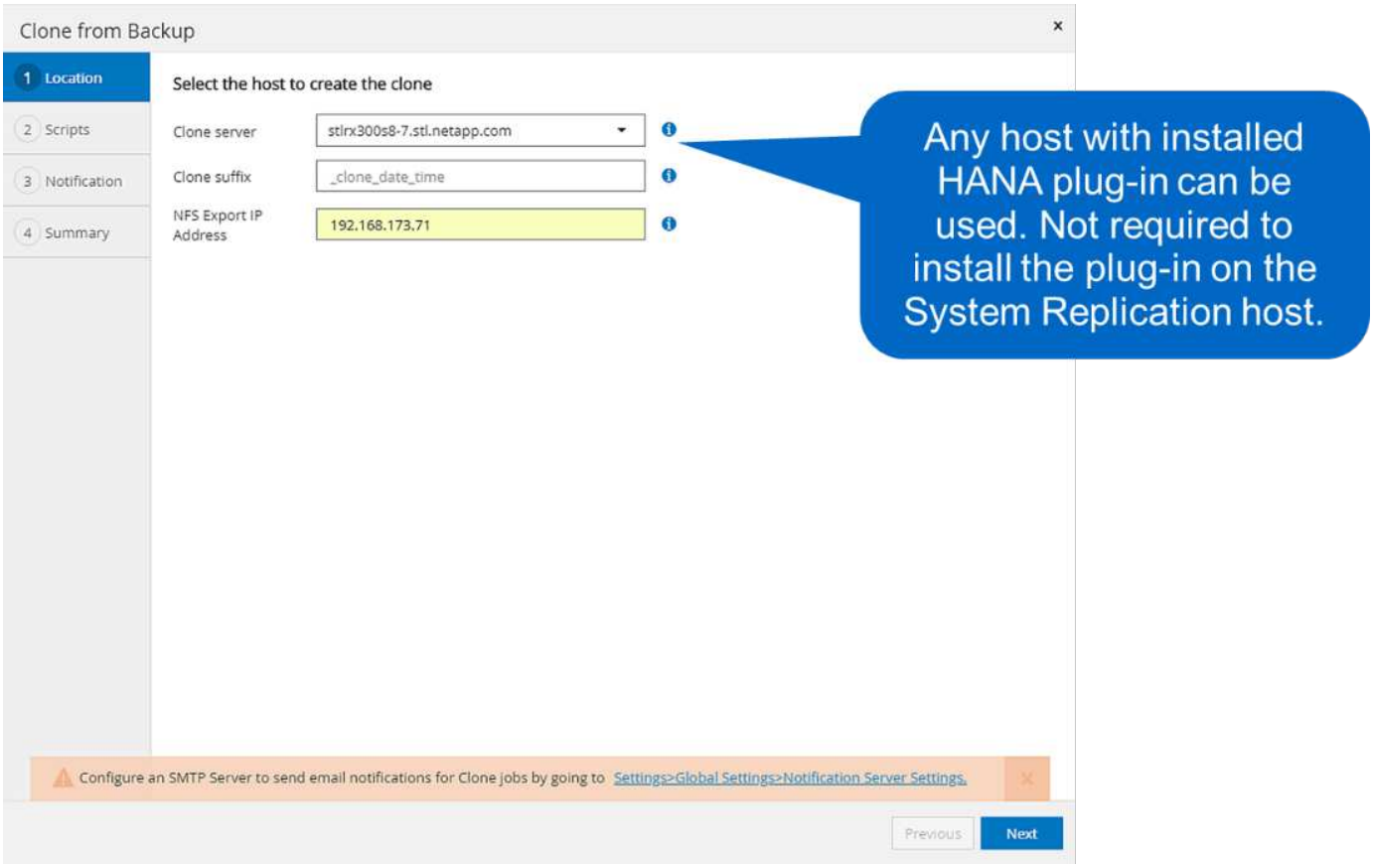
In SnapCenter wird das Backup ausgewählt und der Klonvorgang gestartet.



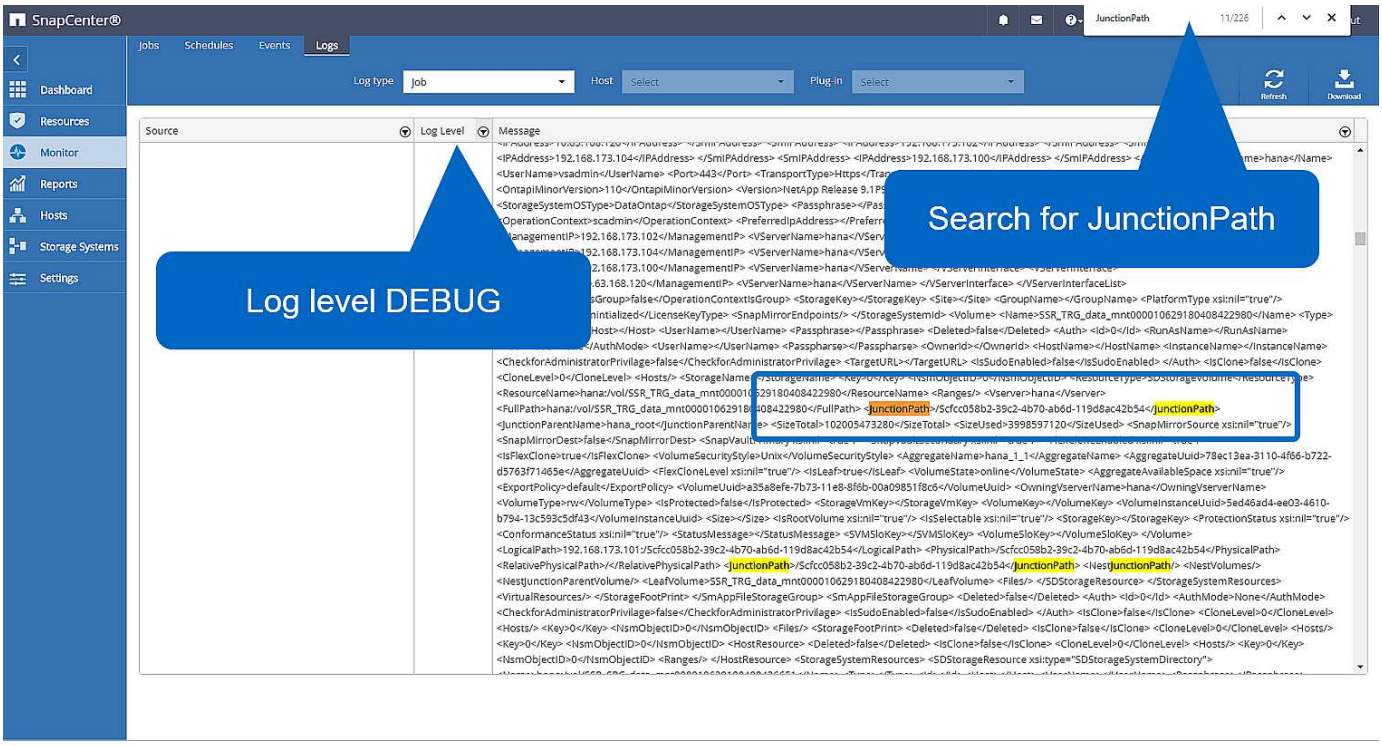
Sie müssen den Klon-Server und die NFS-Export-IP-Adresse angeben.

> 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 Recovery mit SAP HANA Studio wird wie im Abschnitt beschrieben durchgeführt "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

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

- Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter

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

- Technischer Bericht: SAP HANA Disaster Recovery with Storage Replication

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

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

Technischer Bericht: SAP HANA Disaster Recovery with Azure NetApp Files

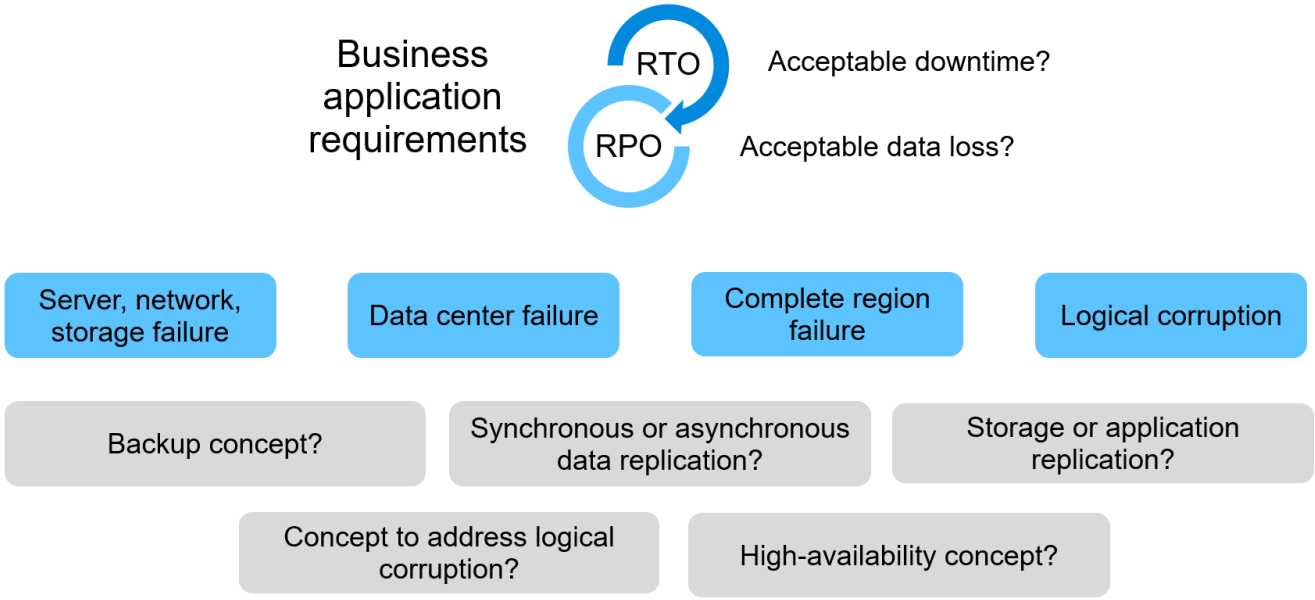
TR-4891: SAP HANA Disaster Recovery mit Azure NetApp Files

Nils Bauer, NetApp Ralf Klahr, Microsoft

Studien haben gezeigt, dass Ausfallzeiten von Business-Applikationen erhebliche negative Auswirkungen auf das Geschäft von Unternehmen haben. Neben den finanziellen Auswirkungen können Ausfallzeiten auch den Ruf des Unternehmens, die Arbeitsmoral des Personals und die Kundenbindung schädigen. Überraschenderweise haben nicht alle Unternehmen eine umfassende Disaster Recovery-Richtlinie.

Wenn SAP HANA auf Azure NetApp Files (ANF) läuft, erhalten Kunden Zugriff auf zusätzliche Funktionen, mit denen die integrierte Datensicherung und Disaster Recovery-Funktionen von SAP HANA erweitert und verbessert werden können. In der Übersicht werden die folgenden Optionen erläutert, mit denen Kunden Optionen auswählen können, die ihre geschäftlichen Anforderungen unterstützen.

Zur Entwicklung einer umfassenden Disaster Recovery-Richtlinie müssen Kunden die Anforderungen ihrer Business-Applikationen und die technischen Funktionen kennen, die sie für Datensicherung und Disaster Recovery benötigen. Die folgende Abbildung bietet einen Überblick über die Datensicherung.



Anforderungen von Business-Applikationen

Für Geschäftsanwendungen gibt es zwei wichtige Indikatoren:

- Der Recovery-Zeitpunkt (Recovery Point Objective, RPO) oder der maximal tolerierbare Datenverlust
- Die Recovery-Zeitvorgabe (Recovery Time Objective, RTO) bzw. die maximal tolerierbare Ausfallzeit von Business-Applikationen

Diese Anforderungen werden durch die Art der verwendeten Applikation und die Art der Geschäftsdaten definiert. RPO und RTO können unterschiedlich sein, wenn Sie vor Ausfällen in einer einzelnen Azure Region schützen. Sie können auch voneinander abweichen, wenn Sie sich auf katastrophale Katastrophen wie den Verlust einer kompletten Azure-Region vorbereiten. Es ist wichtig, die geschäftlichen Anforderungen zu

bewerten, die RPO und RTO definieren, da diese Anforderungen erhebliche Auswirkungen auf die verfügbaren technischen Optionen haben.

Hochverfügbarkeit

Die Infrastruktur für SAP HANA wie Virtual Machines, Netzwerk und Storage muss über redundante Komponenten verfügen, um sicherzustellen, dass es keinen Single Point of Failure gibt. MS Azure bietet Redundanz für die verschiedenen Infrastrukturkomponenten.

Um auf der Computing- und Applikationsseite Hochverfügbarkeit zu gewährleisten, können Standby-SAP HANA-Hosts mit einem SAP HANA System mit mehreren Hosts für integrierte Hochverfügbarkeit konfiguriert werden. Wenn ein Server oder ein SAP HANA-Service ausfällt, erfolgt ein Failover des SAP HANA-Service auf den Standby-Host, was zu einem Ausfall von Applikationen führt.

Wenn eine Applikationsausfallzeit im Falle eines Server- oder Applikationsausfalls nicht akzeptabel ist, kann auch die SAP HANA Systemreplizierung als Hochverfügbarkeitslösung eingesetzt werden, die Failover in einem sehr kurzen Zeitrahmen ermöglicht. SAP-Kunden nutzen HANA-Systemreplizierung, um Hochverfügbarkeit bei ungeplanten Ausfällen sicherzustellen, aber auch die Ausfallzeiten bei geplanten Vorgängen wie HANA-Software-Upgrades zu minimieren.

Logische Beschädigung

Logische Beschädigungen können durch Softwarefehler, menschliche Fehler oder Sabotage verursacht werden. Leider können logische Beschädigungen oft nicht mit standardmäßigen Hochverfügbarkeits- und Disaster Recovery-Lösungen behoben werden. Daher können in manchen Fällen RTO- und RPO-Anforderungen in Abhängigkeit von der Ebene, der Applikation, dem File-System oder dem Storage mit der logischen Beschädigung nicht erfüllt werden.

Schlimmstenfalls ist die SAP-Applikation beschädigt oder logisch. SAP Applikationen laufen oft in einer Landschaft, in der verschiedene Applikationen miteinander kommunizieren und Daten austauschen. Daher wird die Wiederherstellung eines SAP-Systems, bei dem eine logische Beschädigung aufgetreten ist, nicht empfohlen. Das Wiederherstellen des Systems zu einem Zeitpunkt vor der Beschädigung führt zu Datenverlusten, sodass die RPO größer als null ist. Außerdem würde die SAP-Landschaft nicht mehr synchron sein und eine zusätzliche Nachbearbeitung erfordern.

Anstatt das SAP-System wiederherzustellen, ist es besser, den logischen Fehler innerhalb des Systems zu beheben, indem das Problem in einem separaten Reparatursystem analysiert wird. Zur Ursachenanalyse ist die Einbindung des Geschäftsprozesses und der Applikationseigentümer erforderlich. Für dieses Szenario erstellen Sie ein Reparatursystem (ein Klon des Produktionssystems) auf Basis der Daten, die vor dem Auftreten der logischen Beschädigung gespeichert wurden. Innerhalb des Reparatursystems können die erforderlichen Daten exportiert und in das Produktionssystem importiert werden. Bei diesem Ansatz muss das produktive System nicht gestoppt werden, und im besten Fall gehen keine Daten oder nur ein Bruchteil der Daten verloren.

> Die zum Einrichten eines Reparatursystems erforderlichen Schritte sind mit einem in diesem Dokument beschriebenen Disaster-Recovery-Testszenario identisch. Somit kann die beschriebene Disaster Recovery-Lösung problemlos auf logische Beschädigungen erweitert werden.

Backups

Backups werden erstellt, um Restores und Recovery von unterschiedlichen zeitpunktgenauen Datensätzen zu ermöglichen. In der Regel werden diese Backups einige Tage bis einige Wochen aufbewahrt.

Je nach Art der Beschädigung können Restores und Recovery mit oder ohne Datenverlust durchgeführt werden. Wenn das RPO null beträgt, selbst bei einem Verlust des Primär- und Backup-Storage, muss das Backup mit der synchronen Datenreplizierung kombiniert werden.

Die RTO für Restore und Recovery wird durch die erforderliche Wiederherstellungszeit, die Recovery-Zeit (einschließlich Datenbankstart) und das Laden der Daten in den Arbeitsspeicher definiert. Bei großen Datenbanken und herkömmlichen Backup-Ansätzen kann die RTO problemlos mehrere Stunden betragen, was unter Umständen nicht akzeptabel ist. Um eine sehr geringe RTO-Werte zu erzielen, muss ein Backup mit einer Hot-Standby-Lösung kombiniert werden, die das Vorladen von Daten in den Speicher beinhaltet.

Eine Backup-Lösung muss dagegen die logische Beschädigung beheben, da Datenreplizierungslösungen nicht alle Arten von logischen Beschädigungen abdecken können.

Synchrone oder asynchrone Datenreplizierung

Der RPO bestimmt hauptsächlich, welche Datenreplizierungsmethode Sie verwenden sollten. Bei einem RPO von null muss auch bei einem Ausfall des primären und des Backup-Storage die Daten synchron repliziert werden. Allerdings gibt es technische Einschränkungen bei der synchronen Replizierung, beispielsweise die Entfernung zwischen zwei Azure Regionen. In den meisten Fällen ist synchrone Replizierung aufgrund von Latenz bei Entfernungen von mehr als 100 km nicht geeignet. Daher ist diese Lösung keine Option für die Datenreplizierung zwischen Azure Regionen.

Wenn ein größerer RPO-Wert akzeptabel ist, kann die asynchrone Replizierung über große Entfernungen hinweg verwendet werden. Der RPO in diesem Fall wird durch die Replizierungsfrequenz definiert.

HANA System-Replizierung mit oder ohne vorab geladen

Die Startzeit einer SAP HANA-Datenbank ist wesentlich länger als die von herkömmlichen Datenbanken, da eine große Datenmenge in den Arbeitsspeicher geladen werden muss, bevor die Datenbank die erwartete Performance liefern kann. Daher ist ein großer Teil der RTO die Zeit, die zum Starten der Datenbank benötigt wird. Mit jeder Storage-basierten Replizierung sowie mit HANA System Replication ohne vorab geladen werden, muss die SAP HANA-Datenbank für den Failover zum Disaster-Recovery-Standort gestartet werden.

Die SAP HANA Systemreplizierung bietet einen Betriebsmodus, in dem die Daten vorgeladen und kontinuierlich am sekundären Host aktualisiert werden. Dieser Modus ermöglicht sehr niedrige RTO-Werte, benötigt aber auch einen dedizierten Server, der nur für den Empfang der Replizierungsdaten vom Quellsystem verwendet wird.

Disaster-Recovery-Lösungsvergleich

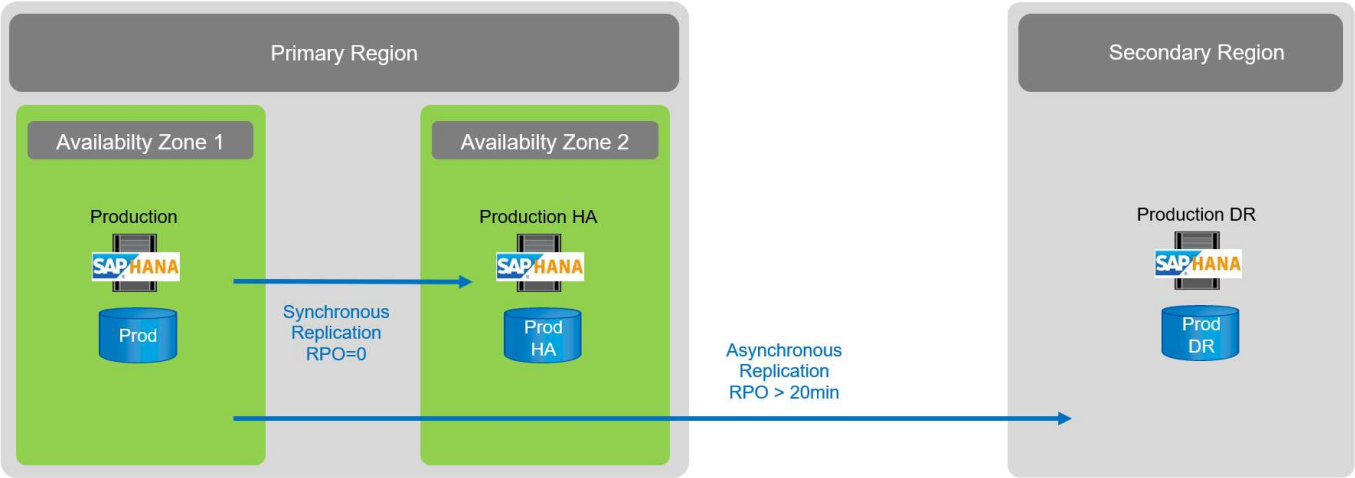
Eine umfassende Disaster Recovery-Lösung muss Kunden nach einem vollständigen Ausfall des primären Standorts die Wiederherstellung ermöglichen. Daher müssen die Daten an einen sekundären Standort übertragen werden und eine komplette Infrastruktur ist erforderlich, um bei einem Standortausfall die erforderlichen SAP HANA Produktionssysteme auszuführen. Abhängig von den Verfügbarkeitsanforderungen der Applikation und der Art des zu schützenden Disaster ist eine Disaster Recovery-Lösung mit zwei oder drei Standorten zu berücksichtigen.

Die folgende Abbildung zeigt eine typische Konfiguration, bei der die Daten innerhalb derselben Azure-Region synchron in eine zweite Verfügbarkeitszone repliziert werden. Durch die kurze Entfernung können Sie die Daten synchron replizieren und ein RPO von null (normalerweise HA-Bereitstellung) erreichen.

Darüber hinaus werden Daten asynchron in eine sekundäre Region repliziert, um sie vor Ausfällen zu

schützen, wenn die primäre Region betroffen ist. Der erzielbare MindestRPO hängt von der Datenreplizierungsfrequenz ab, die durch die verfügbare Bandbreite zwischen dem primären und dem sekundären Bereich begrenzt ist. Ein typischer minimaler RPO liegt im Bereich von 20 Minuten bis mehreren Stunden.

Dieses Dokument erläutert verschiedene Implementierungsoptionen für eine Disaster Recovery-Lösung für zwei Regionen.



SAP HANA System Replication

SAP HANA System Replication arbeitet auf Datenbankebene. Die Lösung basiert auf einem zusätzlichen SAP HANA-System am Disaster-Recovery-Standort, das die Änderungen vom Primärsystem empfängt. Dieses sekundäre System muss mit dem Primärsystem identisch sein.

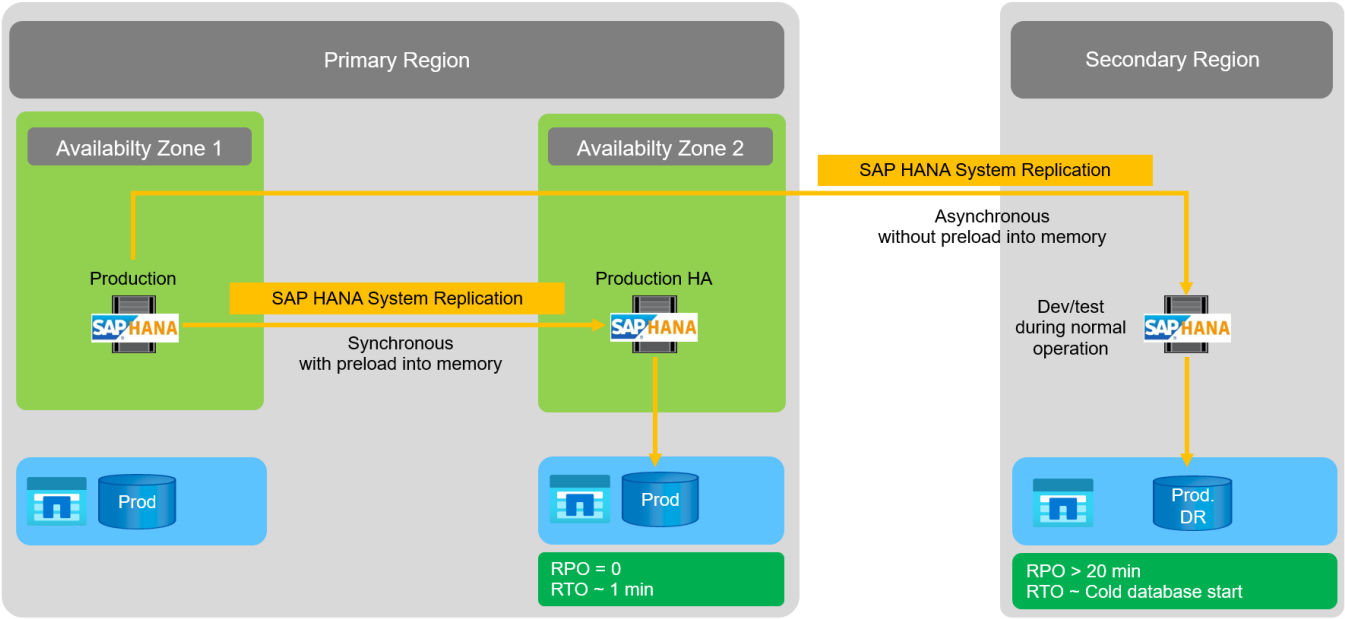
SAP HANA System Replication kann in einem von zwei Modi betrieben werden:

- Mit vorab in den Arbeitsspeicher geladenen Daten und einem dedizierten Server am Disaster-Recovery-Standort:
  - Der Server wird ausschließlich als sekundärer SAP HANA System Replication Host verwendet.
  - Sehr geringe RTO-Werte können erzielt werden, weil die Daten bereits in den Speicher geladen sind und bei einem Failover kein Datenbankstart erforderlich ist.
- Ohne Daten, die vorab in den Arbeitsspeicher geladen sind und einen gemeinsam genutzten Server am Disaster Recovery-Standort nutzen:
  - Der Server wird als sekundäres SAP HANA System Replication und als Entwicklungs-/Testsystem gemeinsam genutzt.
  - RTO hängt hauptsächlich von der Zeit ab, die zum Starten der Datenbank und Laden der Daten in den Arbeitsspeicher benötigt wird.

Eine vollständige Beschreibung aller Konfigurationsoptionen und Replikationsszenarien finden Sie im "SAP HANA Administration Guide".

Die folgende Abbildung zeigt das Setup einer Disaster-Recovery-Lösung für zwei Regionen mit SAP HANA System Replication. Die synchrone Replizierung mit vorab in den Speicher geladenen Daten wird für lokale HA in derselben Azure-Region verwendet, allerdings in verschiedenen Verfügbarkeitszonen. Die asynchrone Replizierung ohne vorab geladene Daten wird für die Remote Disaster-Recovery-Region konfiguriert.

Die folgende Abbildung zeigt die SAP HANA System Replication.



SAP HANA System Replication mit vorab in den Speicher geladenen Daten

Sehr geringe RTO-Werte mit SAP HANA können nur mit SAP HANA System Replication erreicht werden, wobei Daten vorab in den Speicher geladen sind. Der Betrieb von SAP HANA System Replication mit einem dedizierten sekundären Server am Disaster-Recovery-Standort ermöglicht einen RTO-Wert von maximal einer Minute. Die replizierten Daten werden empfangen und im sekundären System vorgeladen. Aus diesem Grund wird SAP HANA System Replication häufig auch für Wartungsvorgänge ohne Ausfallzeiten eingesetzt, beispielsweise für HANA-Software-Upgrades.

In der Regel ist SAP HANA System Replication so konfiguriert, dass sie synchron repliziert wird, wenn eine vorab-Datenlast ausgewählt wird. Die maximal unterstützte Entfernung bei synchroner Replizierung liegt im Bereich von 100 km.

SAP System Replication ohne vorab in den Speicher geladene Daten

Für weniger strenge RTO-Anforderungen kann SAP HANA System Replication ohne vorab geladene Daten verwendet werden. In diesem Betriebsmodus werden die Daten der Disaster-Recovery-Region nicht in den Arbeitsspeicher geladen. Der Server in der DR-Region wird weiterhin zur Verarbeitung von SAP HANA System Replication verwendet, auf dem alle erforderlichen SAP HANA-Prozesse ausgeführt werden. Der Großteil des Serverspeichers ist jedoch für andere Dienste verfügbar, wie zum Beispiel SAP HANA Entwicklungs-/Testsysteme.

Bei einem Notfall muss das Entwicklungs-/Testsystem heruntergefahren, der Failover initiiert und die Daten in den Arbeitsspeicher geladen werden. Das RTO dieses Cold-Standby-Ansatzes hängt von der Größe der Datenbank und dem Lesedurchsatz während der Last des Zeilen- und Spaltenspeichers ab. Mit der Annahme, dass die Daten mit einem Durchsatz von 1000 MBit/s gelesen werden, dass das Laden von 1 TB Daten ungefähr 18 Minuten dauert.

Technischer Bericht: SAP HANA Disaster Recovery with ANF Cross-Region Replication

ANF Cross-Region Replication ist in ANF als Disaster-Recovery-Lösung mit asynchroner Datenreplizierung integriert. ANF regionsübergreifende Replizierung wird über eine Datensicherungsbeziehung zwischen zwei ANF-Volumes in einer primären und einer sekundären Azure-Region konfiguriert. ANF-Cross-Region Replication aktualisiert das sekundäre Volume mithilfe effizienter Block-Delta-Replikationen. Update-Zeitpläne können während der Replikationskonfiguration definiert werden.

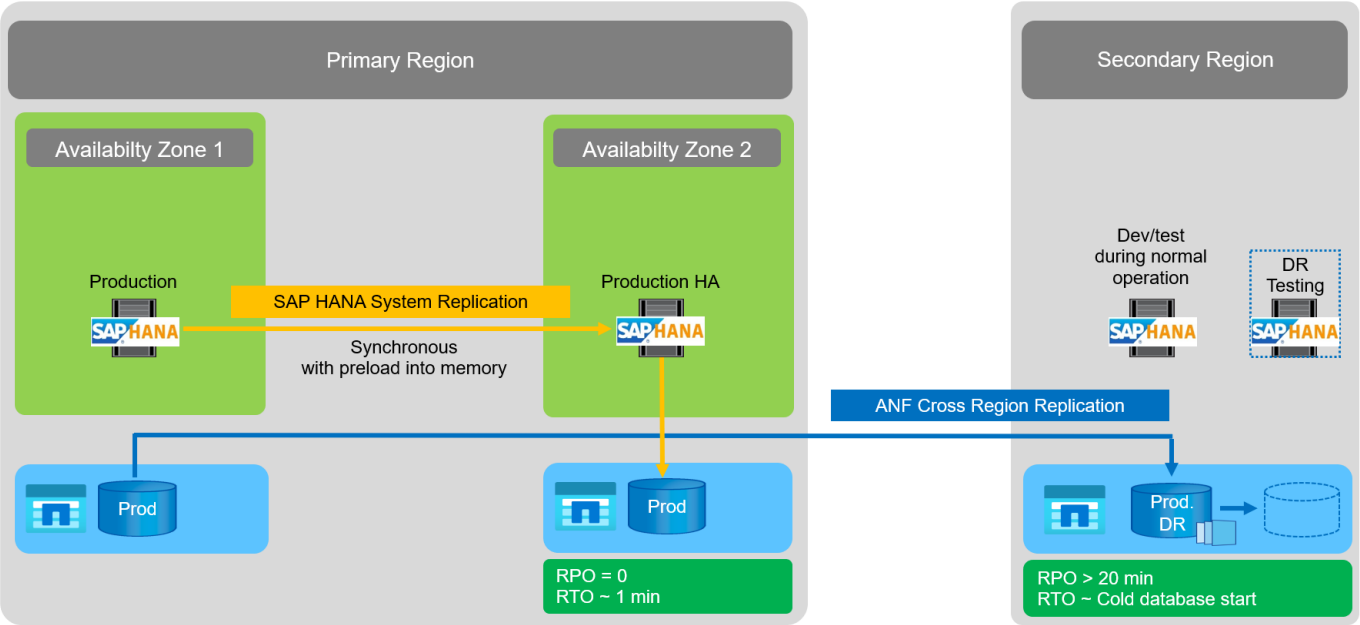
Die folgende Abbildung zeigt ein Beispiel für eine Disaster-Recovery-Lösung für zwei Regionen mithilfe von ANF-bereichsübergreifender Replizierung. In diesem Beispiel ist das HANA-System mit HANA System Replication innerhalb der primären Region geschützt, wie im vorherigen Kapitel erläutert. Die Replikation in eine sekundäre Region wird mittels ANF-bereichsübergreifender Replikation durchgeführt. Der RPO-Wert wird durch den Replizierungszeitplan und die Replizierungsoptionen definiert.

Das RTO hängt hauptsächlich von der Zeit ab, die zum Starten der HANA-Datenbank am Disaster-Recovery-Standort und zum Laden der Daten in den Arbeitsspeicher benötigt wird. Mit der Annahme, dass die Daten mit einem Durchsatz von 1000 MB/s gelesen werden, dass das Laden von 1 TB Daten ungefähr 18 Minuten dauert. Je nach Replizierungskonfiguration ist auch Recovery-Prozesse erforderlich und wird der RTO-Gesamtwert steigern.

Weitere Details zu den verschiedenen Konfigurationsoptionen finden Sie in Kapitel "Konfigurationsoptionen für regionsübergreifende Replizierung mit SAP HANA".

Die Server an den Disaster-Recovery-Standorten können als Entwicklungs-/Testsysteme im normalen Betrieb eingesetzt werden. Bei einem Notfall müssen die Entwicklungs-/Testsysteme heruntergefahren und als DR-Produktionsserver gestartet werden.

Mit der standortübergreifenden ANF Replizierung können Sie den DR-Workflow testen, ohne dass RPO und RTO beeinträchtigt werden. Dazu werden Volume-Klone erstellt und an den DR-Testserver angeschlossen.



Zusammenfassung der Disaster Recovery-Lösungen

In der folgenden Tabelle werden die in diesem Abschnitt beschriebenen Disaster-Recovery-Lösungen verglichen und die wichtigsten Kennzahlen hervorgehoben.

Die wichtigsten Ergebnisse:

- Ist ein sehr niedriges RTO erforderlich, ist SAP HANA System Replication mit vorab-Load in den Speicher die einzige Option.
  - Am DR-Standort ist ein dedizierter Server erforderlich, um die replizierten Daten zu erhalten und die Daten in den Arbeitsspeicher zu laden.
- Darüber hinaus ist eine Storage-Replizierung für die Daten erforderlich, die sich außerhalb der Datenbank

befinden (z. B. gemeinsam genutzte Dateien, Schnittstellen usw.).

- Bei einer geringeren RTO/RPO-Anforderung kann auch eine regionale ANF-Replizierung verwendet werden, um:
  - Kombinieren Sie Datenreplizierung außerhalb von Datenbanken.
  - Behandeln Sie zusätzliche Anwendungsfälle wie Disaster-Recovery-Tests und Aktualisierungen von Entwicklung/Tests.
  - Bei der Storage-Replizierung kann der Server am DR-Standort im normalen Betrieb als QA- oder Testsystem verwendet werden.
- Eine Kombination aus SAP HANA System Replication als HA-Lösung mit RPO=0 mit Storage-Replizierung für große Entfernungen ist sinnvoll, um die unterschiedlichen Anforderungen zu erfüllen.

In der folgenden Tabelle werden die Disaster-Recovery-Lösungen verglichen.

	Storage-Replizierung	**SAP HANA Systemreplizierung**	
	Regionenübergreifende Replikation	* Mit Datenvorladung*	**Ohne Datenvorladung**
RTO	Gering bis mittel; abhängig von der Startzeit der Datenbank und der Vorwärtswiederherstellung	Sehr niedrig	Gering bis mittel; abhängig von der Datenbank-Startzeit
RPO	RPO > 20 Min. Asynchrone Replizierung	RPO > 20 Min. Asynchrone Replikation RPO = 0 synchrone Replizierung	RPO > 20 Min. Asynchrone Replikation RPO = 0 synchrone Replizierung
Server am DR-Standort können für Entwicklung/Test genutzt werden	Ja.	Nein	Ja.
Replizierung von nicht aus Datenbanken stammenden Daten	Ja.	Nein	Nein
DR-Daten können zur Aktualisierung von Entwicklungs-/Testsystemen genutzt werden	Ja.	Nein	Nein
DR-Tests ohne Auswirkungen auf RTO und RPO	Ja.	Nein	Nein

ANF: Regionale Replizierung mit SAP HANA

ANF: Regionale Replizierung mit SAP HANA

Anwendungsunabhängige Informationen zur bereichsübergreifenden Replikation finden Sie unter "Azure NetApp Files Dokumentation – Microsoft Docs" In den Konzepten und Anleitungen.

Konfigurationsoptionen für Regionalreplizierung mit SAP HANA

Die folgende Abbildung zeigt die Volume-Replizierungsbeziehungen für ein SAP HANA-System mit ANF-bereichsübergreifender Replizierung. Bei ANF-Cross-Region Replication müssen die HANA-Daten und das gemeinsame HANA-Volume repliziert werden. Wenn nur das HANA-Daten-Volume repliziert wird, liegen die typischen RPO-Werte im Bereich von einem Tag. Wenn niedrigere RPO-Werte erforderlich sind, müssen die HANA-Protokoll-Backups auch für die zukünftige Recovery repliziert werden.

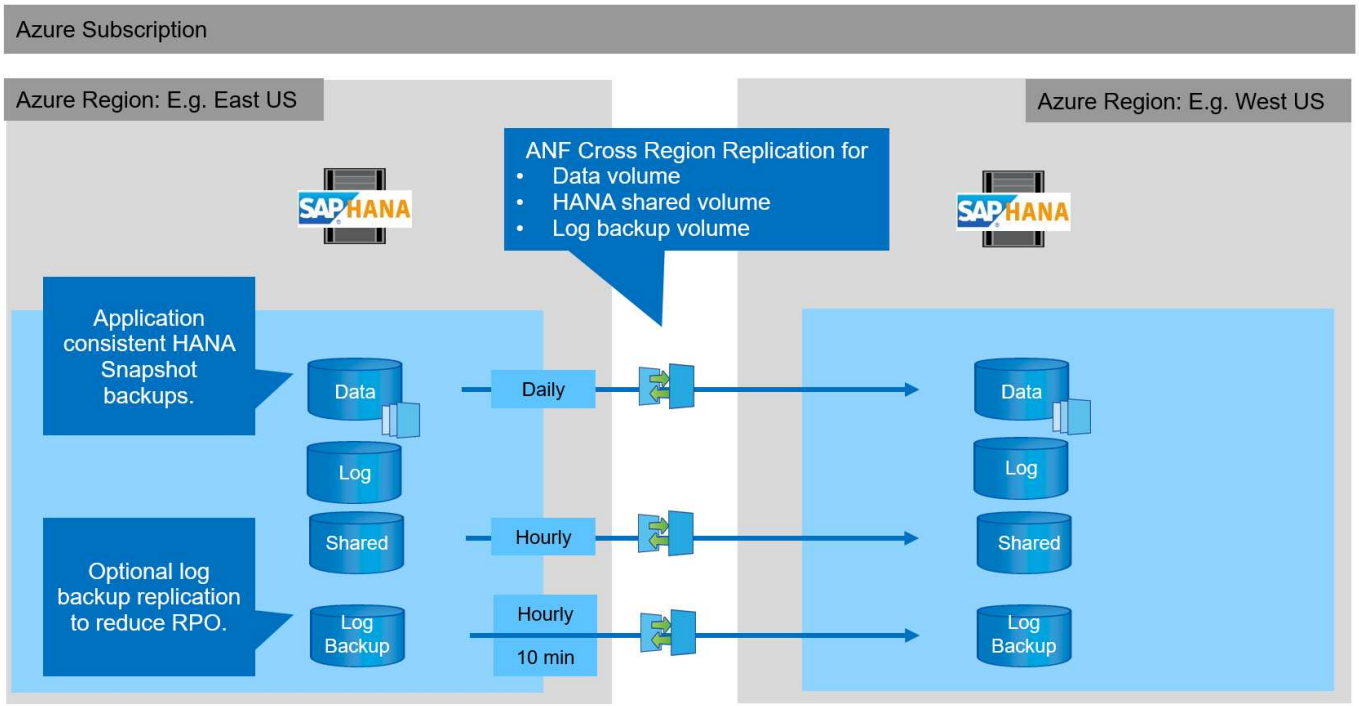
> Der in diesem Dokument verwendete Begriff „Protokollsicherung“ umfasst die Protokollsicherung und die Sicherung des HANA-Backup-Katalogs. Der HANA-Backup-Katalog ist erforderlich, um Recovery-Vorgänge durchzuführen.

> Die folgende Beschreibung und der Schwerpunkt der Laboreinrichtung sind auf die HANA-Datenbank. Andere gemeinsam genutzte Dateien, zum Beispiel das SAP-Transportverzeichnis, würden auf die gleiche Weise gesichert und repliziert werden wie das freigegebene HANA-Volume.

Für die HANA-Speicherpunktwiederherstellung oder Forward-Recovery mit den Backup-Protokollen müssen am primären Standort für das HANA-Daten-Volume applikationskonsistente Snapshot Backups erstellt werden. Dies kann zum Beispiel mit dem ANF-Backup-Tool AzAcSnap (siehe auch "Was ist Azure Application konsistente Snapshot Tool für Azure NetApp Files Microsoft Docs"). Die am primären Standort erstellten Snapshot Backups werden anschließend am DR-Standort repliziert.

Bei einem Disaster Failover muss die Replizierungsbeziehung beschädigt werden, die Volumes müssen auf dem DR-Produktionsserver eingebunden werden, und die HANA-Datenbank muss wiederhergestellt werden, entweder zum letzten HANA-Speicherpunkt oder bei einer Forward-Recovery mit den replizierten Log-Backups. Kapitel "Disaster-Recovery-Failover", Beschreibt die erforderlichen Schritte.

In der folgenden Abbildung sind die HANA-Konfigurationsoptionen für die regionsübergreifende Replizierung dargestellt.



Mit der aktuellen Version der Cross-Region-Replikation können nur feste Zeitpläne ausgewählt werden, und die tatsächliche Replikationsaktualisierungszeit kann nicht vom Benutzer definiert werden. Verfügbare Termine sind täglich, stündlich und alle 10 Minuten. Bei Verwendung dieser Zeitplanoptionen sind zwei verschiedene Konfigurationen je nach RPO-Anforderungen sinnvoll: Daten-Volume-Replizierung ohne Backup-Replizierung bei Protokolldaten sowie Backup-Replizierung mit verschiedenen Zeitplänen entweder stündlich oder alle 10 Minuten. Die niedrigste mögliche RPO beträgt etwa 20 Minuten. In der folgenden Tabelle sind die Konfigurationsoptionen sowie die resultierenden RPO- und RTO-Werte zusammengefasst.

	Replizierung von Daten-Volumes	**Replizierung von Daten und Backup Volumes protokollieren**	**Replizierung von Daten und Backup Volumes protokollieren**
CRR-Volumen planen	Täglich	Täglich	Täglich
CRR-Protokoll Backup-Volumen planen	k. A.	Stündlich	10 Min
Max. RPO	24 Stunden + Snapshot Zeitplan (z. B. 6 Stunden)	1 Stunde	2 x 10 Min
Max RTO	In erster Linie durch die HANA-Startzeit definiert	+ HANA Startzeit + Wiederherstellungszeit+	+ HANA Startzeit + Wiederherstellungszeit+
Wiederherstellung vorwärts	NA	Logs der letzten 24 Stunden + Snapshot Zeitplan (z.B. 6 Stunden)	Logs der letzten 24 Stunden + Snapshot Zeitplan (z.B. 6 Stunden)

Anforderungen und Best Practices

Microsoft Azure übernimmt keine Garantie für die Verfügbarkeit eines bestimmten VM-Typs (Virtual Machine) bei der Erstellung oder beim Starten einer nicht zugewiesenen VM. Insbesondere im Falle eines regionalen Ausfalls benötigen viele Clients möglicherweise zusätzliche VMs in der Disaster Recovery-Region. Daher wird

empfohlen, eine VM mit der erforderlichen Größe für Disaster Failover aktiv als Test- oder QA-System in der Disaster Recovery-Region zu verwenden, um den erforderlichen VM-Typ zugewiesen zu haben.

Es empfiehlt sich, einen ANF-Kapazitätspool mit einer niedrigeren Performance Tier im normalen Betrieb zu verwenden, um eine Kostenoptimierung zu ermöglichen. Die Datenreplizierung erfordert keine hohe Performance und kann daher einen Kapazitäts-Pool mit einer Standard-Performance-Tier verwenden. Bei Disaster-Recovery-Tests oder bei einem Ausfall muss die Volume in einen Kapazitäts-Pool mit einer hochperformanten Tier verschoben werden.

Wenn ein zweiter Kapazitäts-Pool keine Option ist, sollten die Ziel-Volumes für die Replizierung auf Basis der Kapazitätsanforderungen konfiguriert werden und nicht auf die Performance-Anforderungen während des normalen Betriebs. Das Kontingent oder der Durchsatz (für manuelle QoS) kann dann für Disaster-Recovery-Tests angepasst werden, falls ein Notfall besteht.

Weitere Informationen finden Sie unter "Anforderungen und Überlegungen für die Verwendung von Azure NetApp Files-Volume-regionsübergreifende Replikation mit Microsoft Docs".

Laboreinrichtung

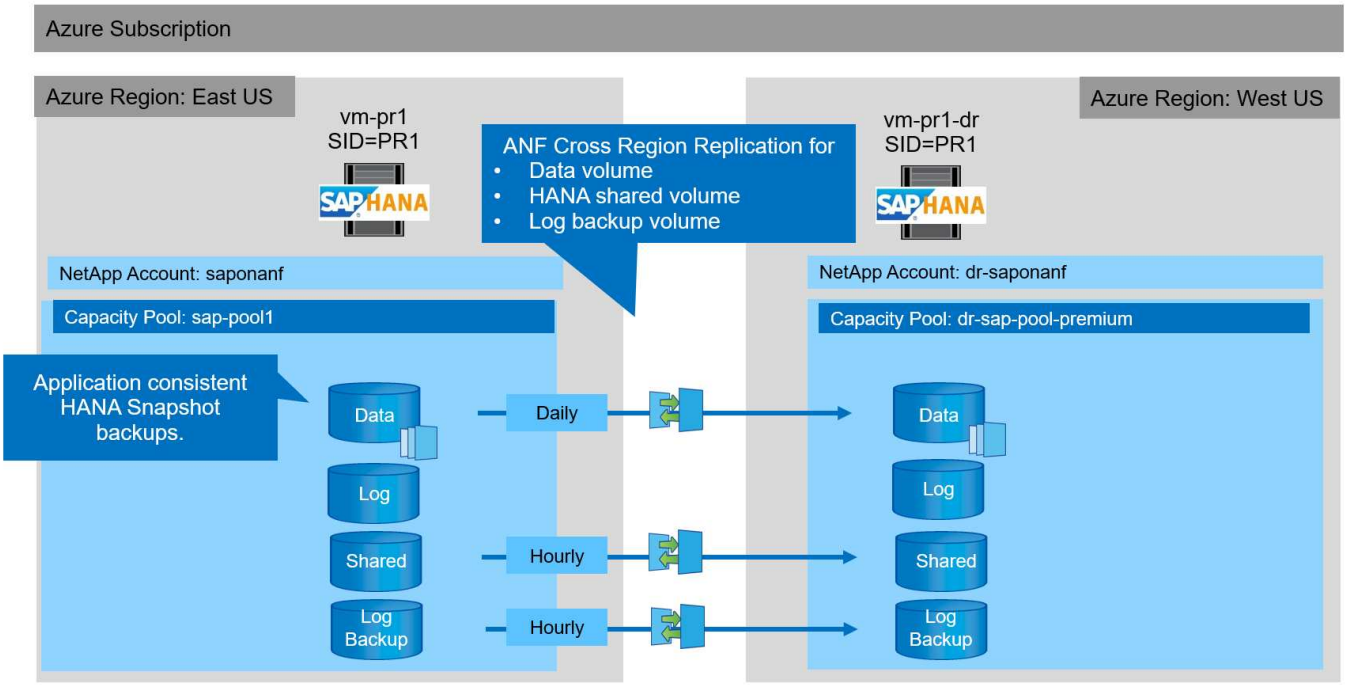
Die Lösungsvalidierung wurde mit einem Single-Host-System für SAP HANA durchgeführt. Das Microsoft AzAcSnap Snapshot Backup-Tool für ANF wurde verwendet, um applikationskonsistente HANA Snapshot Backups zu konfigurieren. Es wurden ein tägliches Datenvolumen, ein stündliches Log Backup und die gemeinsame Volume-Replizierung konfiguriert. Disaster Recovery-Tests und Failover wurden mit einem Speicherpunkt sowie bei vorwärts gerichteten Recovery-Vorgängen validiert.

Die folgenden Softwareversionen wurden für die Laboreinrichtung verwendet:

- Ein einziges Host-System SAP HANA 2.0 SPS5 mit einem einzelnen Mandanten
- SUSE SLES FÜR SAP 15 SP1
- AzAcSnap 5.0

Am DR-Standort wurde ein einzelner Kapazitäts-Pool mit manueller QoS konfiguriert.

Die folgende Abbildung zeigt die Laboreinrichtung.

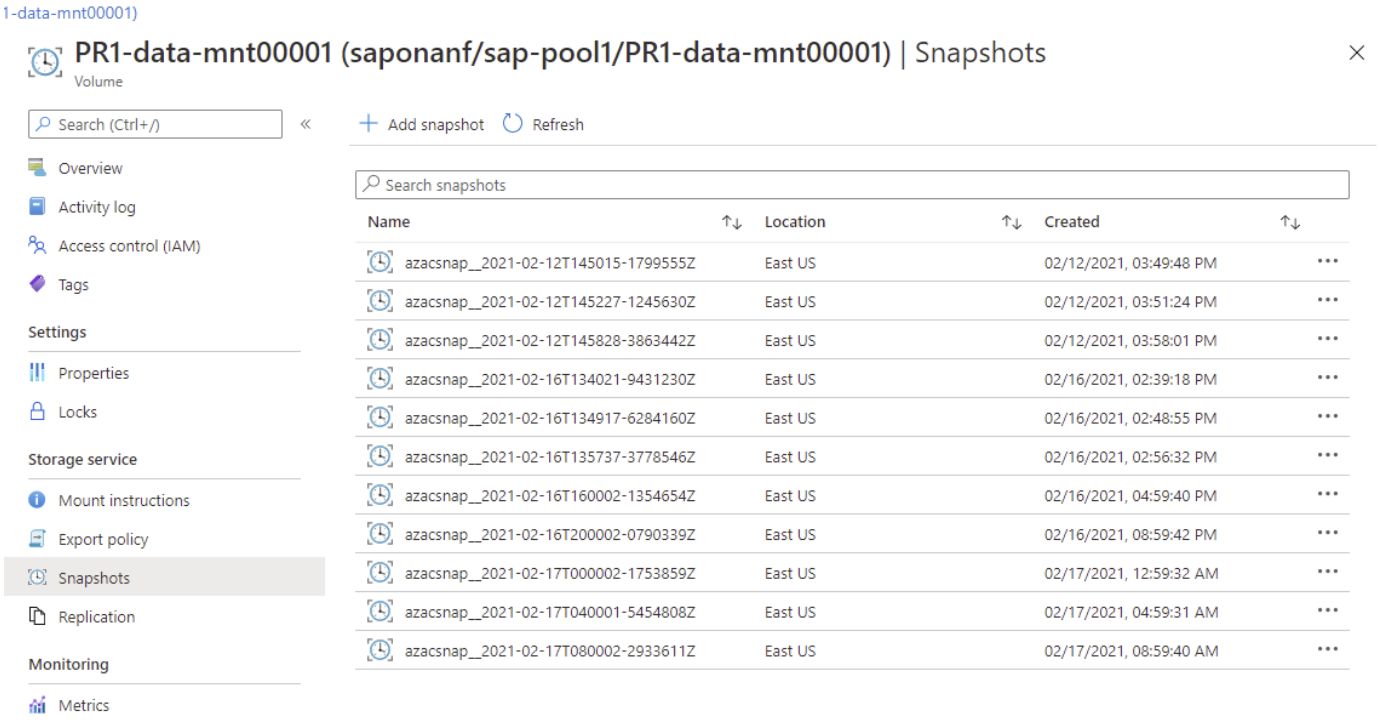


Snapshot Backup-Konfiguration mit AzAcSnap

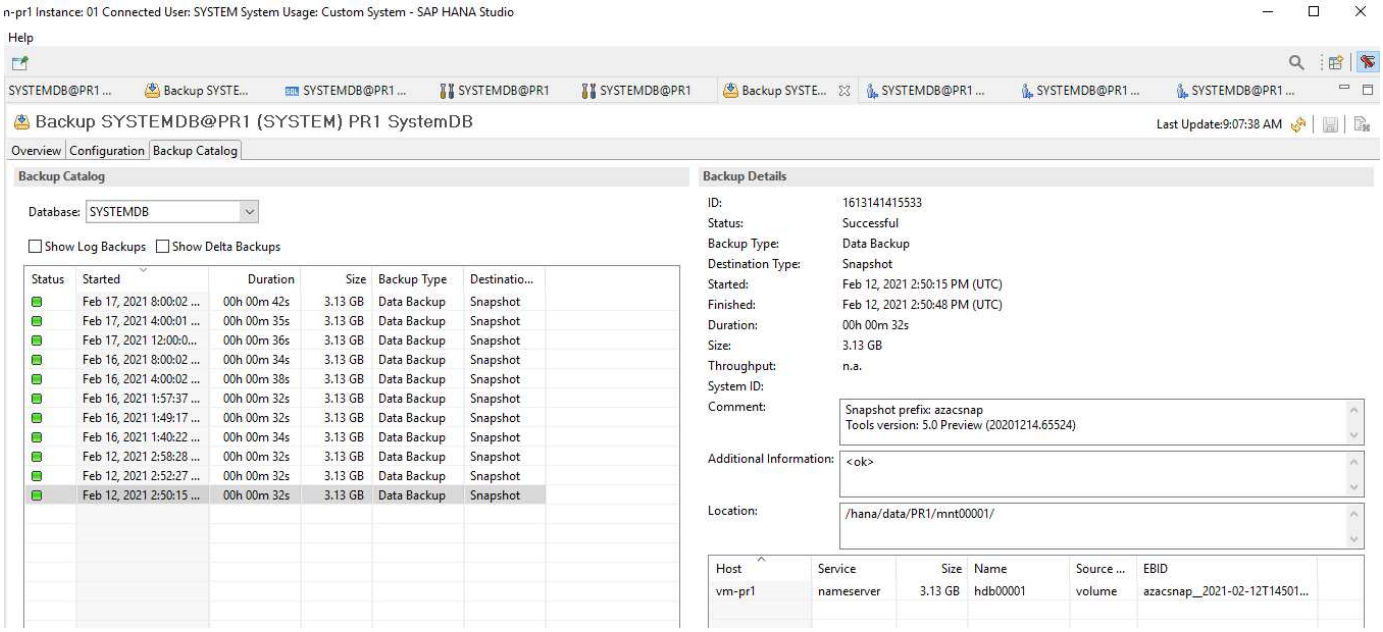
Am primären Standort wurde AzAcSnap für die Erstellung applikationskonsistenter Snapshot-Backups des HANA-Systems PR1 konfiguriert. Diese Snapshot-Backups sind im ANF-Datenvolumen des PR1 HANA Systems verfügbar und sind auch im SAP HANA Backup-Katalog registriert, wie in den beiden folgenden Abbildungen dargestellt. Snapshot Backups wurden alle 4 Stunden geplant.

Bei der Replizierung des Daten-Volumes mithilfe von ANF Cross-Region Replication werden diese Snapshot-Backups am Disaster Recovery-Standort repliziert und können zur Wiederherstellung der HANA-Datenbank verwendet werden.

Die folgende Abbildung zeigt die Snapshot Backups des HANA Daten-Volumes.



Die folgende Abbildung zeigt den SAP HANA-Backup-Katalog.



Konfigurationsschritte für ANF-bereichsübergreifende Replikation

Am Disaster Recovery-Standort sind einige Vorbereitungsschritte durchzuführen, bevor die Volume-Replizierung konfiguriert werden kann.

- Ein NetApp Konto muss verfügbar und mit demselben Azure Abonnement wie die Quelle konfiguriert sein.
- Ein Kapazitäts-Pool muss über das oben genannte NetApp Konto verfügbar und konfiguriert sein.
- Ein virtuelles Netzwerk muss verfügbar und konfiguriert sein.
- Innerhalb des virtuellen Netzwerks muss ein delegiertes Subnetz zur Verwendung mit ANF verfügbar und

konfiguriert sein.

Protection Volumes können nun für HANA-Daten, HANA Shared IT und das HANA-Log-Backup-Volume erstellt werden. Die folgende Tabelle zeigt die konfigurierten Ziel-Volumes in unserer Laboreinrichtung.

> Um eine optimale Latenz zu erzielen, müssen die Volumes in der Nähe der VMs platziert werden, die im Falle eines Disaster-Failover den SAP HANA ausführen. Daher ist für die DR-Volumes derselbe Pinning-Prozess wie für jedes andere SAP HANA-Produktionssystem erforderlich.

HANA Volume	Quelle	Ziel	Replizierungsplan
HANA-Datenvolumen	PR1-Data-mnt00001	PR1-Data-mnt00001-SM-dest	Täglich
HANA Shared Volume	PR1 freigegeben	PR1-shared-SM-dest	Stündlich
HANA-Protokoll-/Katalogbackup-Volume	Hanabackup	Hanabackup-SM-dest	Stündlich

Für jedes Volume müssen folgende Schritte durchgeführt werden:

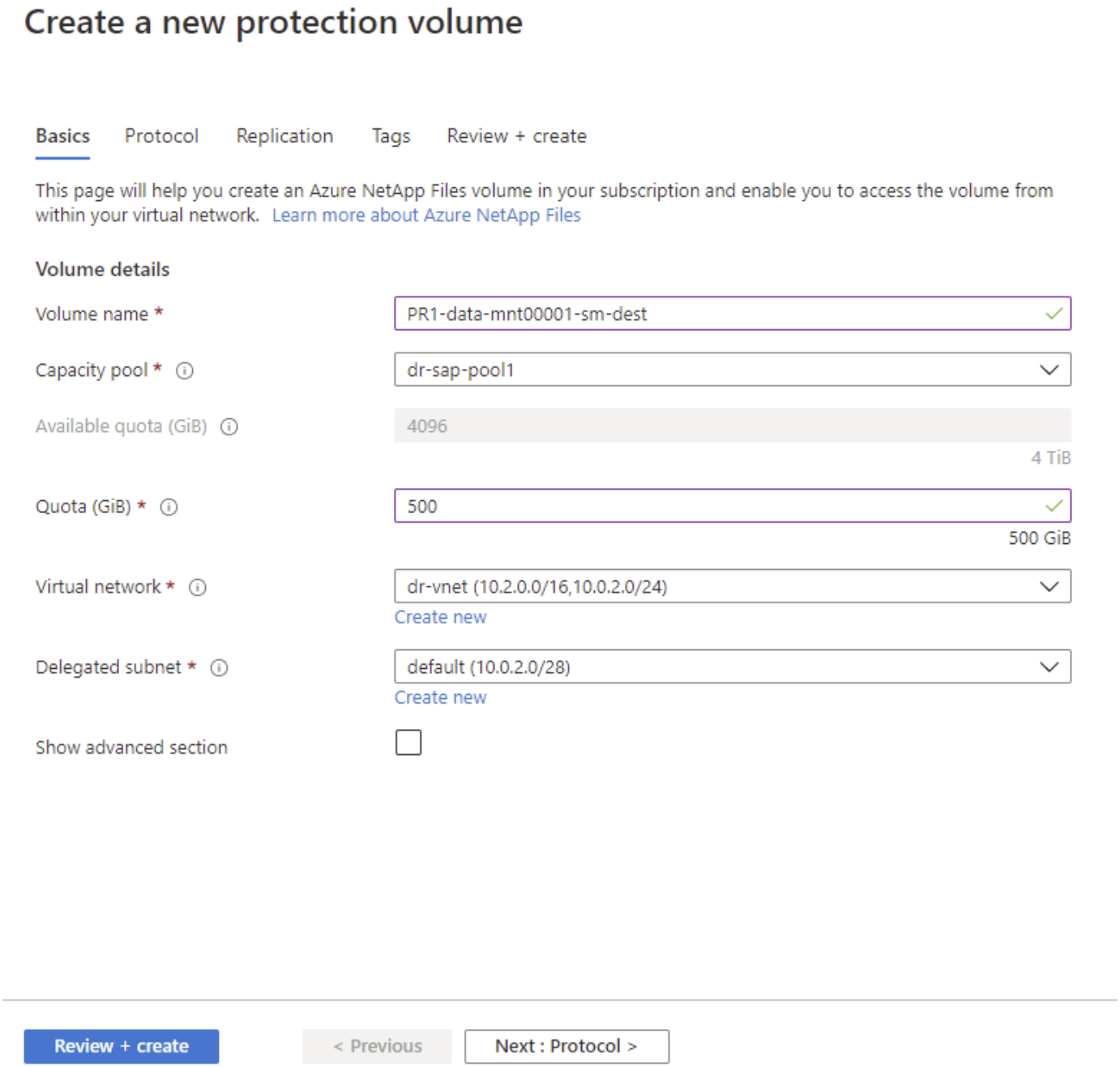
1. Erstellen eines neuen Sicherungs-Volumes am DR-Standort:
   a. Stellen Sie Volume-Namen, den Kapazitäts-Pool, die Quota- und Netzwerkinformationen bereit.
   b. Bereitstellen der Zugriffsinformationen für Protokolle und Volumes
   c. Geben Sie die Quell-Volume-ID und einen Replizierungsplan an.
   d. Erstellen eines Ziel-Volumes
2. Autorisieren Sie die Replikation auf dem Quell-Volume.
   - Geben Sie die ID des Zielvolumens an.

Die folgenden Screenshots zeigen die Konfigurationsschritte im Detail.

Am Disaster Recovery-Standort wird ein neues Datensicherungs-Volume erstellt, indem Sie Volumes auswählen und auf Datenreplizierung hinzufügen klicken. Auf der Registerkarte „Grundlagen“ müssen Sie den Namen des Volumes, den Kapazitäts-Pool und die Netzwerkinformationen angeben.

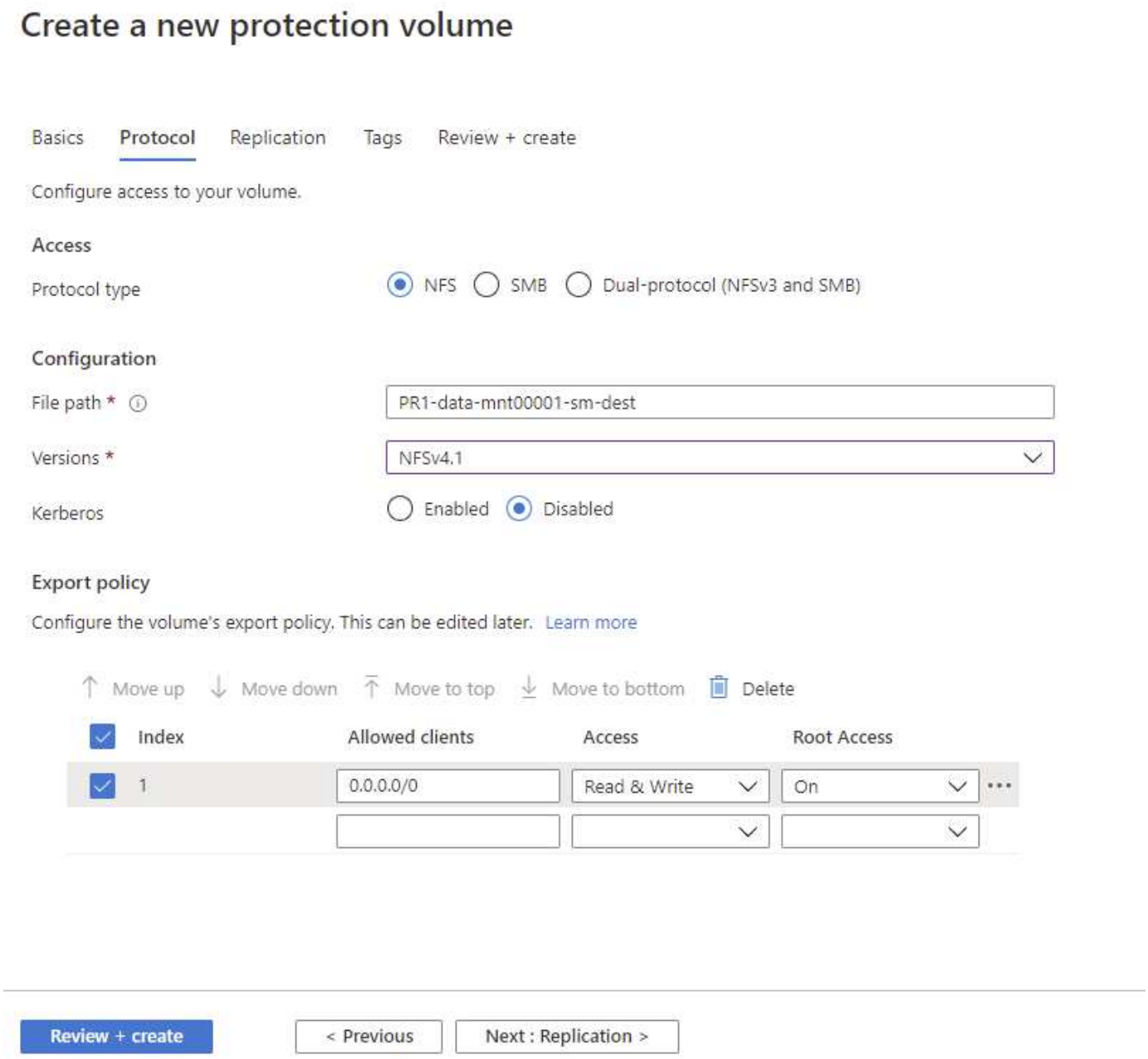
> Das Kontingent kann auf Basis der Kapazitätsanforderungen festgelegt werden, da die Volume-Performance sich nicht auf den Replizierungsprozess auswirkt. Bei einem Disaster Recovery-Failover muss die Quote an die tatsächlichen Performance-Anforderungen angepasst werden.

> Wenn der Kapazitäts-Pool mit manueller QoS konfiguriert wurde, können Sie den Durchsatz zusätzlich zu den Kapazitätsanforderungen konfigurieren. Wie oben angegeben können Sie den Durchsatz auch im normalen Betrieb mit niedrigem Wert konfigurieren und im Falle eines Disaster Recovery Failover diesen erhöhen.



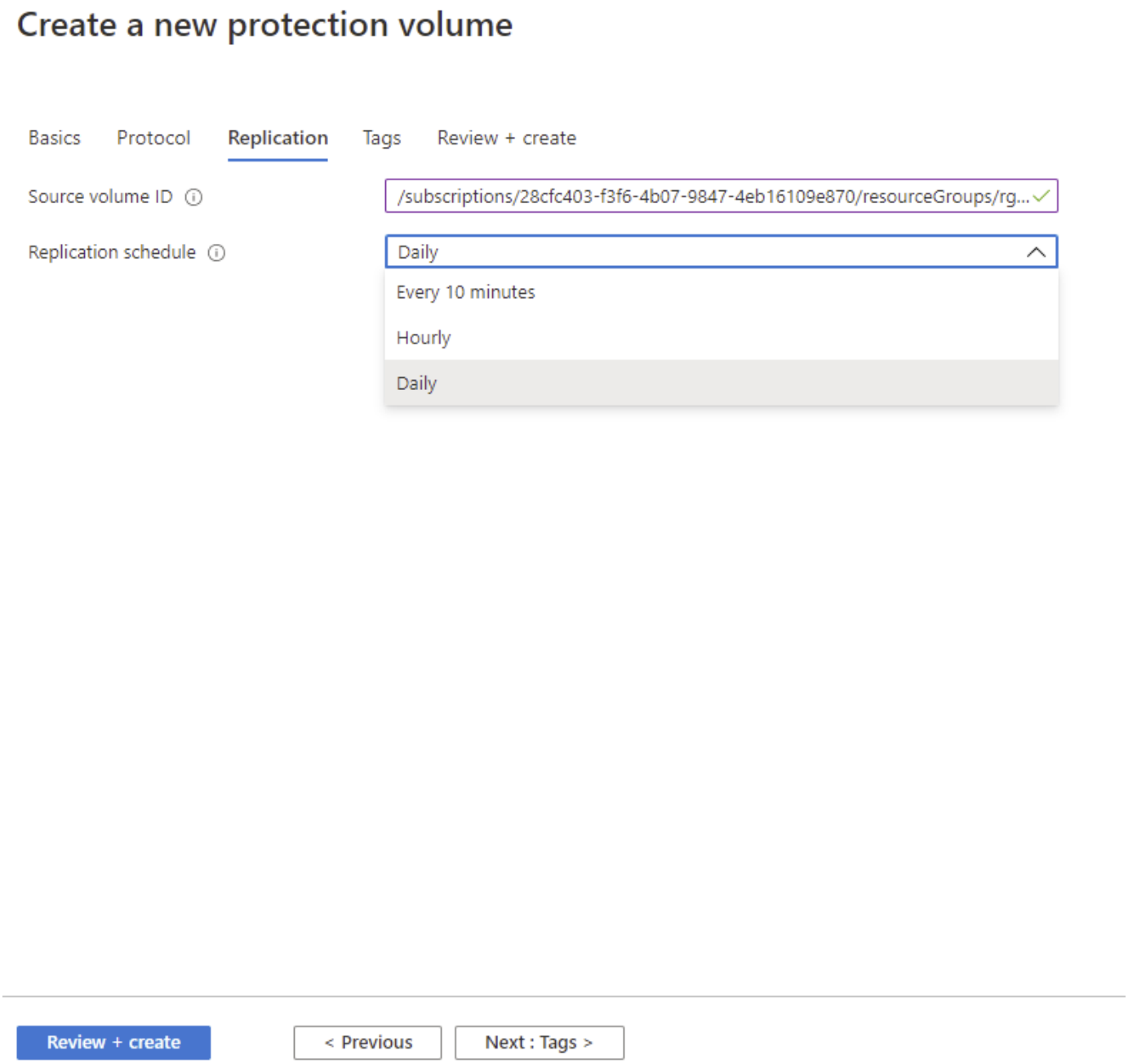
Auf der Registerkarte Protokoll müssen Sie das Netzwerkprotokoll, den Netzwerkpfad und die Exportrichtlinie angeben.

> Das Protokoll muss dasselbe sein wie das für das Quell-Volume verwendete Protokoll.



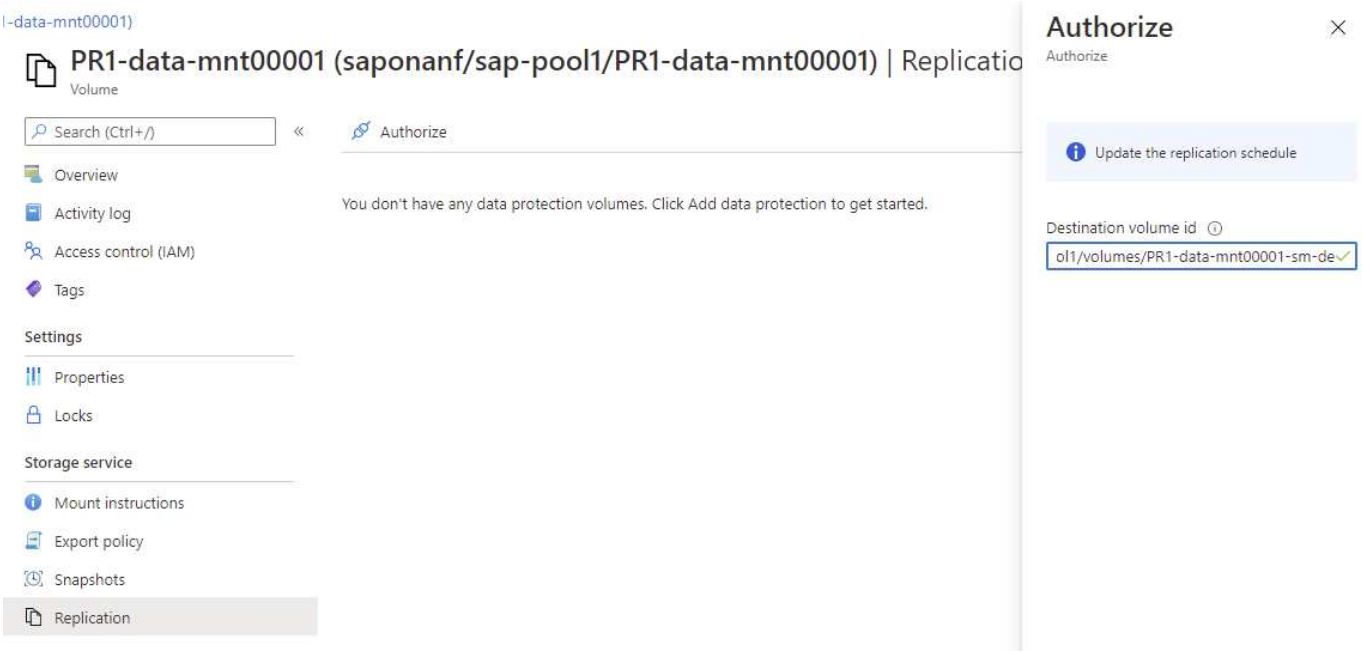
Auf der Registerkarte „Replikation“ müssen Sie die Quell-Volume-ID und den Replizierungsplan konfigurieren. Für die Datenreplizierung mit Daten-Volumes haben wir einen täglichen Replizierungszeitplan für unsere Einrichtung im Labor konfiguriert.

Die Quell-Volume-ID kann vom Bildschirm Eigenschaften des Quell-Volumes kopiert werden.



Als letzter Schritt müssen Sie die Replikation am Quell-Volume durch Angabe der ID des Ziel-Volume autorisieren.

> Sie können die Ziel-Volume-ID vom Bildschirm Eigenschaften des Ziel-Volumes kopieren.



Für das freigegebene HANA und das Protokoll-Backup-Volume müssen dieselben Schritte durchgeführt werden.

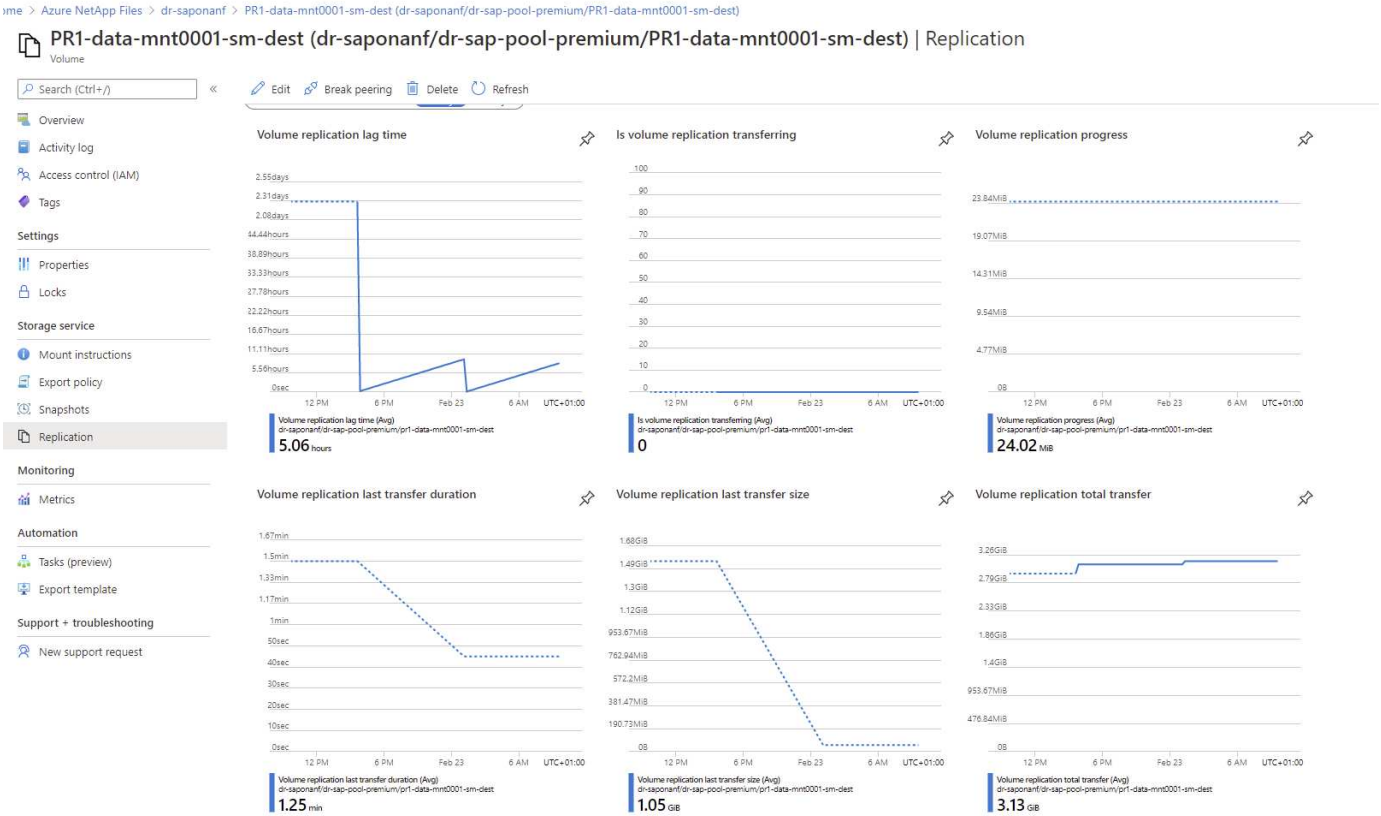
Überwachung der standortübergreifenden ANF-Replikation

Die folgenden drei Screenshots zeigen den Replikationsstatus für die Daten, Backup-Protokollierung und gemeinsam genutzte Volumes.

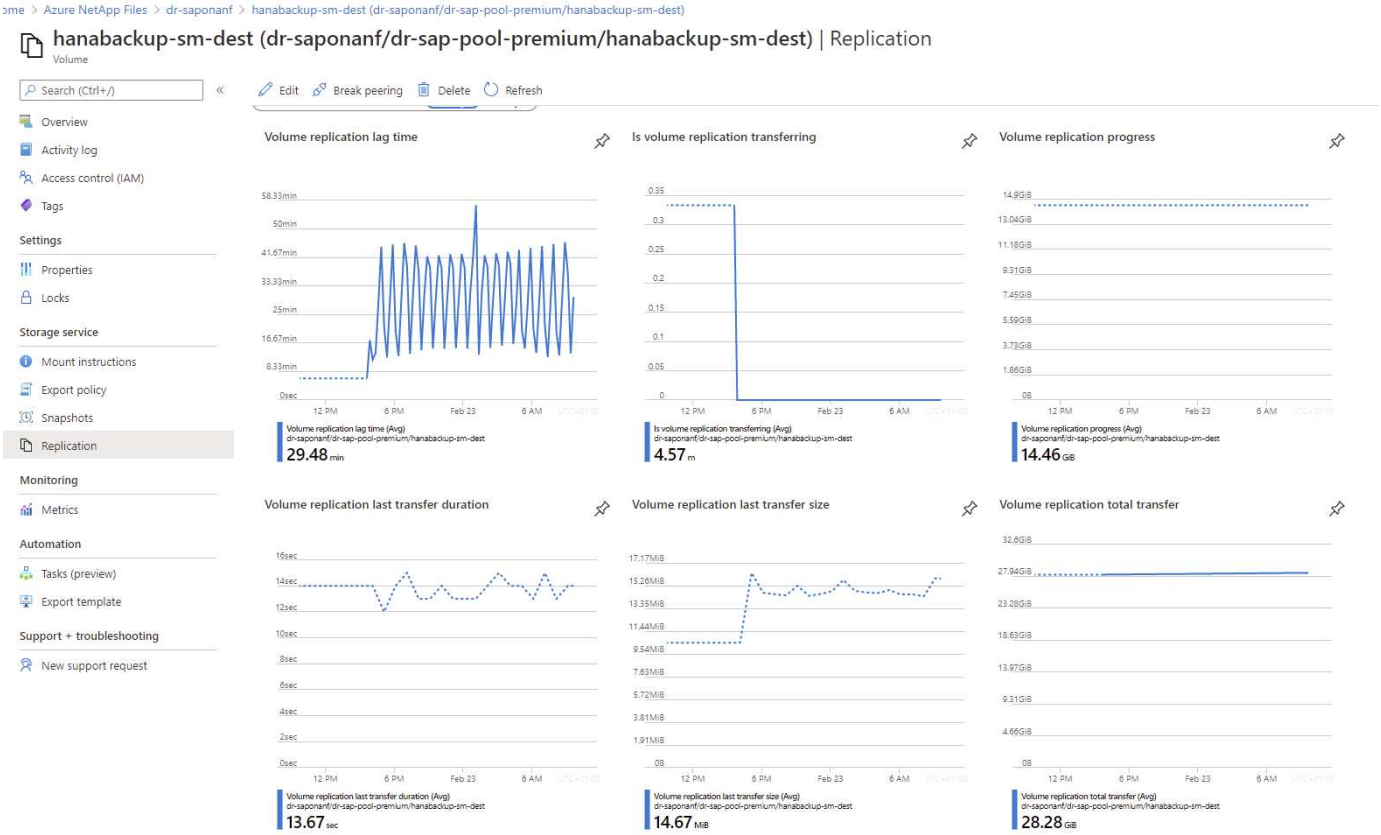
Die Verzögerung bei der Volume-Replizierung ist ein nützlicher Wert, um die RPO-Erwartungen zu verstehen. Beispielsweise zeigt die Replizierung des Backup-Volumes für das Protokoll eine maximale Verzögerungszeit von 58 Minuten, das heißt, dass der maximale RPO den gleichen Wert hat.

Die Übertragungsdauer und Übertragungsgröße bieten wertvolle Informationen zu den Bandbreitenanforderungen und ändern die Rate des replizierten Volumes.

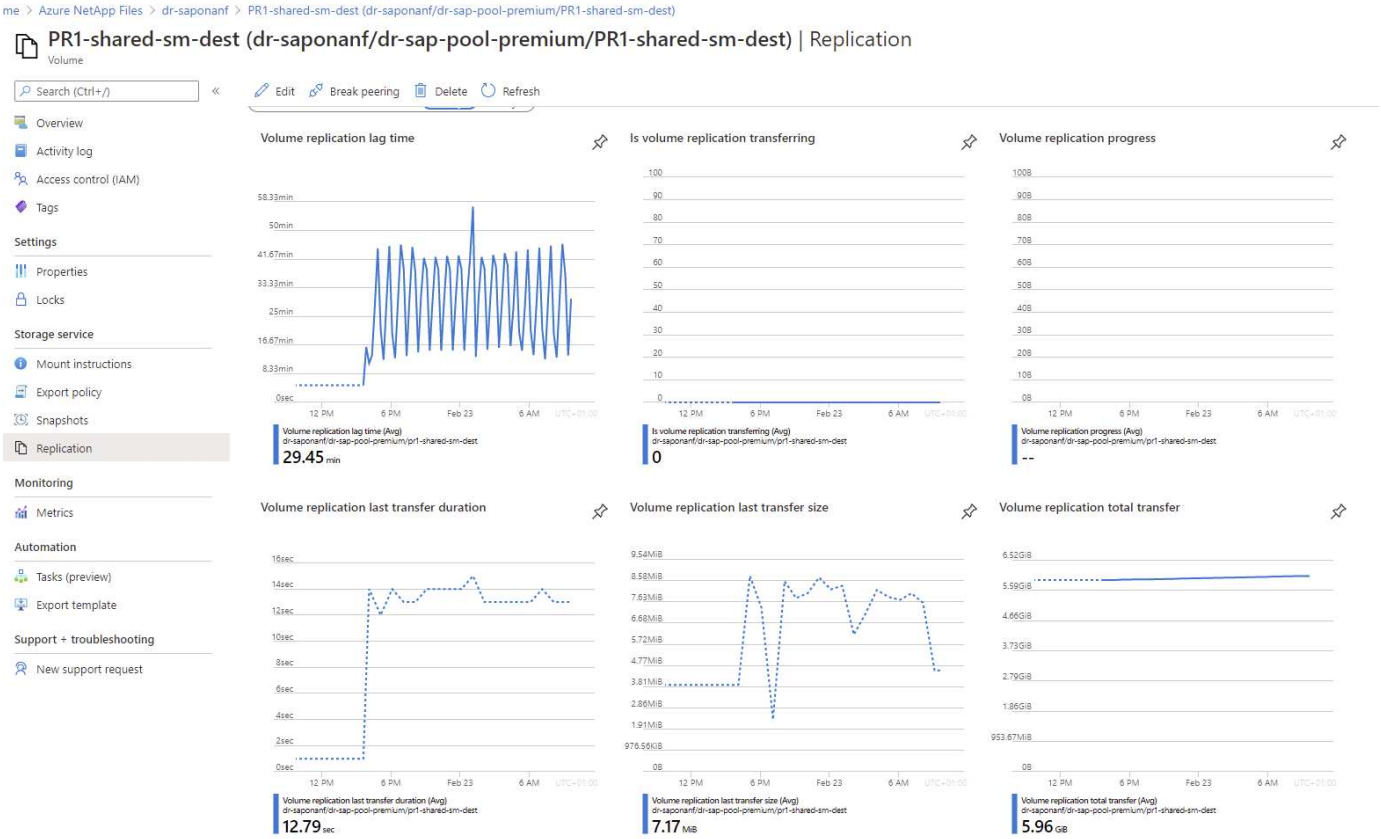
Der folgende Screenshot zeigt den Replizierungsstatus eines HANA Daten-Volumes.



Der folgende Screenshot zeigt den Replizierungsstatus eines HANA-Protokoll-Backup-Volumes.



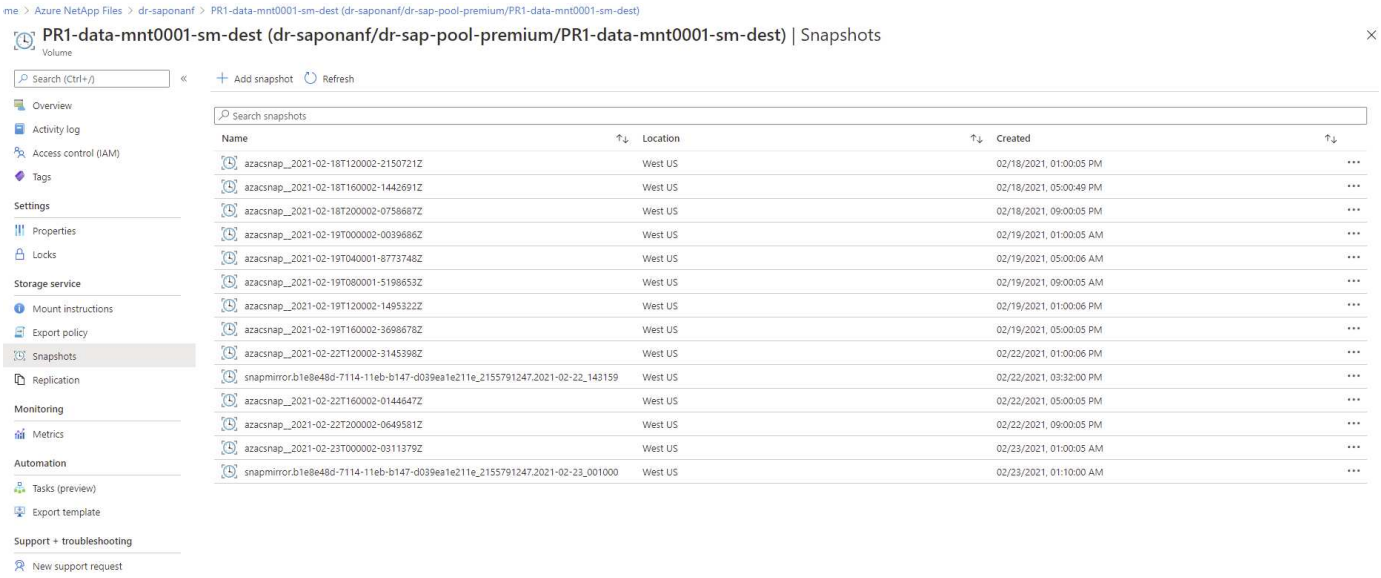
Der folgende Screenshot zeigt den Replizierungsstatus von einem Shared HANA Volume.



Replizierte Snapshot Backups

Bei jedem Replizierungs-Update vom Quell- zum Ziel-Volume werden alle Blockänderungen, die zwischen dem letzten und dem aktuellen Update stattgefunden haben, auf das Ziel-Volume repliziert. Dies umfasst auch die Snapshots, die auf dem Quell-Volume erstellt wurden. Der folgende Screenshot zeigt die Snapshots, die auf dem Zielvolume verfügbar sind. Wie bereits erwähnt, sind alle Snapshots, die vom Tool AzAcSnap erstellt wurden, applikationskonsistente Images der HANA Datenbank, die zur Ausführung eines Speicherpunktes oder einer vorwärts gerichteten Recovery verwendet werden können.

> Innerhalb des Quell- und Ziel-Volume werden auch SnapMirror Snapshot Kopien erstellt, die für Resynchronisierung und Replizierungs-Updates verwendet werden. Diese Snapshot-Kopien sind aus Sicht der HANA-Datenbank nicht applikationskonsistent. Bei HANA-Recovery-Vorgängen können nur die über AzaCSnap erstellten applikationskonsistenten Snapshots verwendet werden.



Disaster Recovery-Tests

Disaster Recovery-Tests

Um eine effiziente Disaster Recovery-Strategie zu implementieren, müssen Sie den erforderlichen Workflow testen. Der Test zeigt, ob die Strategie funktioniert und ob die interne Dokumentation ausreichend ist, und ermöglicht es Administratoren auch, die erforderlichen Verfahren zu trainieren.

Die regionale ANF Replizierung ermöglicht Disaster-Recovery-Tests ohne Risiko für RTO und RPO. Disaster-Recovery-Tests können ohne Unterbrechung der Datenreplizierung durchgeführt werden.

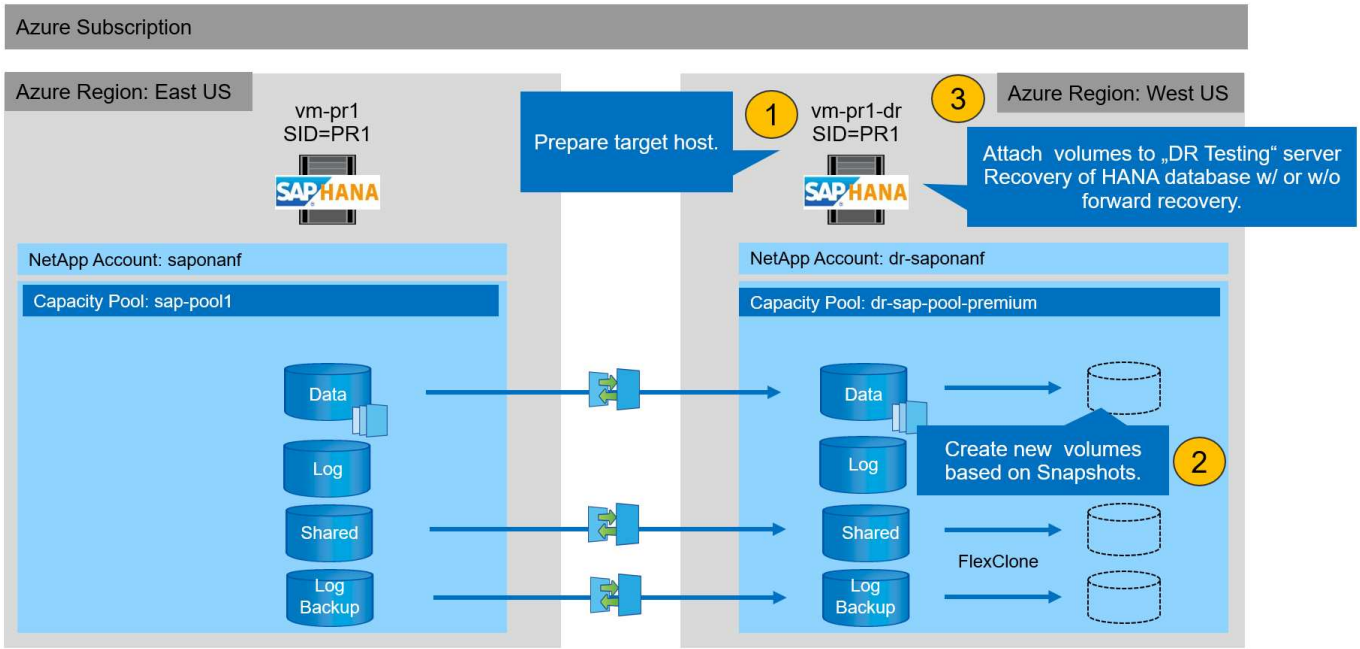
Der Workflow für Disaster Recovery-Tests nutzt die ANF-Funktionen, um auf Basis vorhandener Snapshot-Backups am Disaster-Recovery-Ziel neue Volumes zu erstellen. Siehe "Wie Azure NetApp Files Snapshots funktionieren - Microsoft Docs".

Je nachdem, ob die Backup-Replizierung des Protokolls Bestandteil der Disaster Recovery-Einrichtung ist oder nicht, unterscheiden sich die Schritte für die Disaster Recovery leicht. In diesem Abschnitt werden die Disaster Recovery-Tests für die reine Daten-Backup-Replizierung sowie für die Replizierung von Daten-Volumes in Kombination mit der Replizierung des Backup-Volumes für das Protokoll beschrieben.

Gehen Sie wie folgt vor, um Disaster-Recovery-Tests durchzuführen:

1. Bereiten Sie den Zielhost vor.
2. Erstellen neuer Volumes auf Basis von Snapshot Backups am Disaster-Recovery-Standort
3. Mounten Sie die neuen Volumes am Ziel-Host.
4. Stellen Sie die HANA Datenbank wieder her.
    - Nur Daten-Volume-Recovery.
    - Recovery mit replizierten Protokoll-Backups vorführen.

In den folgenden Abschnitten werden diese Schritte detailliert beschrieben.



Bereiten Sie den Zielhost vor

Dieser Abschnitt beschreibt die auf dem Server erforderlichen Vorbereitungsschritte für das Disaster-Recovery-Failover-Testen.

Im normalen Betrieb wird der Zielhost normalerweise für andere Zwecke verwendet, beispielsweise als HANA QA- oder Testsystem. Daher müssen die meisten dieser Schritte ausgeführt werden, wenn Disaster Failover-Tests durchgeführt werden. Zum anderen die relevanten Konfigurationsdateien, wie `/etc/fstab` Und `/usr/sap/sapservices`, Kann vorbereitet und dann in die Produktion durch einfaches Kopieren der Konfigurationsdatei gesetzt werden. Das Testverfahren für die Disaster Recovery stellt sicher, dass die relevanten, vorbereiteten Konfigurationsdateien korrekt konfiguriert sind.

Die Vorbereitung des Ziel-Hosts umfasst auch das Herunterfahren des HANA QA- oder Testsystems sowie das Anhalten aller Services mit `systemctl stop sapinit`.

Hostname und IP-Adresse des Zielservers

Der Hostname des Zielservers muss mit dem Hostnamen des Quellsystems identisch sein. Die IP-Adresse kann unterschiedlich sein.

> Ein ordnungsgemäßes Fechten des Zielservers muss eingerichtet werden, damit er nicht mit anderen Systemen kommunizieren kann. Wenn keine ordnungsgemäße Fechten vorhanden sind, kann das geklonte Produktionssystem Daten mit anderen Produktionssystemen austauschen, was zu logisch beschädigten Daten führt.

Installieren Sie die erforderliche Software

Die SAP-Hostagent-Software muss auf dem Zielserver installiert sein. Weitere Informationen finden Sie im "SAP Host Agent" Im SAP-Hilfeportal.

> Wenn der Host als HANA QA- oder Testsystem verwendet wird, ist die SAP-Hostagent-Software bereits installiert.

Konfiguration von Benutzern, Ports und SAP-Diensten

Die erforderlichen Anwender und Gruppen für die SAP HANA-Datenbank müssen auf dem Zielserver verfügbar sein. In der Regel wird die zentrale Benutzerverwaltung verwendet. Daher sind keine Konfigurationsschritte auf dem Zielserver erforderlich. Die erforderlichen Ports für die HANA-Datenbank müssen auf den Ziel-Hosts konfiguriert sein. Die Konfiguration kann durch Kopieren des aus dem Quellsystem kopiert werden `/etc/services` Datei auf dem Zielserver.

Die erforderlichen SAP Services-Einträge müssen auf dem Zielhost verfügbar sein. Die Konfiguration kann durch Kopieren des aus dem Quellsystem kopiert werden `/usr/sap/sapservices` Datei auf dem Zielserver. Die folgende Ausgabe zeigt die erforderlichen Einträge für die im Lab-Setup verwendete SAP HANA-Datenbank.

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

HANA-Protokollvolumen vorbereiten

Da das HANA-Protokoll-Volume nicht Teil der Replikation ist, muss auf dem Ziel-Host ein leeres Protokoll-Volume vorhanden sein. Das Protokoll-Volume muss dieselben Unterverzeichnisse enthalten wie das Quell-HANA-System.

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

Erstellen des Backup-Volumes für das Protokoll

Da das Quellsystem für die HANA-Protokoll-Backups mit einem separaten Volume konfiguriert ist, muss auch ein Protokoll-Backup-Volume auf dem Zielhost verfügbar sein. Ein Volume für die Protokoll-Backups muss konfiguriert und auf dem Ziel-Host gemountet werden.

Wenn die Replikation des Protokoll-Backup-Volumes Teil der Disaster Recovery-Einrichtung ist, wird ein neues Volume auf Basis eines Snapshots auf dem Zielhost gemountet und es ist nicht erforderlich, ein zusätzliches Protokoll-Backup-Volume vorzubereiten.

Bereiten Sie Dateisystemeinhängungen vor

In der folgenden Tabelle sind die Namenskonventionen aufgeführt, die für das Lab-Setup verwendet werden. Die Volume-Namen der neuen Volumes am Disaster-Recovery-Standort sind in enthalten `/etc/fstab`. Diese

Volume-Namen werden im nächsten Abschnitt im Schritt zur Volume-Erstellung verwendet.

HANA PR1-Volumes	Neues Volume und neue Unterverzeichnisse am Disaster Recovery-Standort	Bereitstellungspunkt am Zielhost
Datenvolumen	PR1-Data-mnt00001-SM-dest-Clone	/hana/Data/PR1/mnt00001
Freigegebenes Volume	PR1-shared-sm-dest-Clone/shared PR1-shared-SM-dest-Clone/usr-sap-PR1	/hana/shared /usr/sap/PR1
Backup-Volume protokollieren	Hanabackup-sm-dest-Clone	/Hanabackup

Die in dieser Tabelle aufgeführten Mount-Punkte müssen auf dem Zielhost erstellt werden.

Hier sind die erforderlichen `/etc/fstab` Einträge.

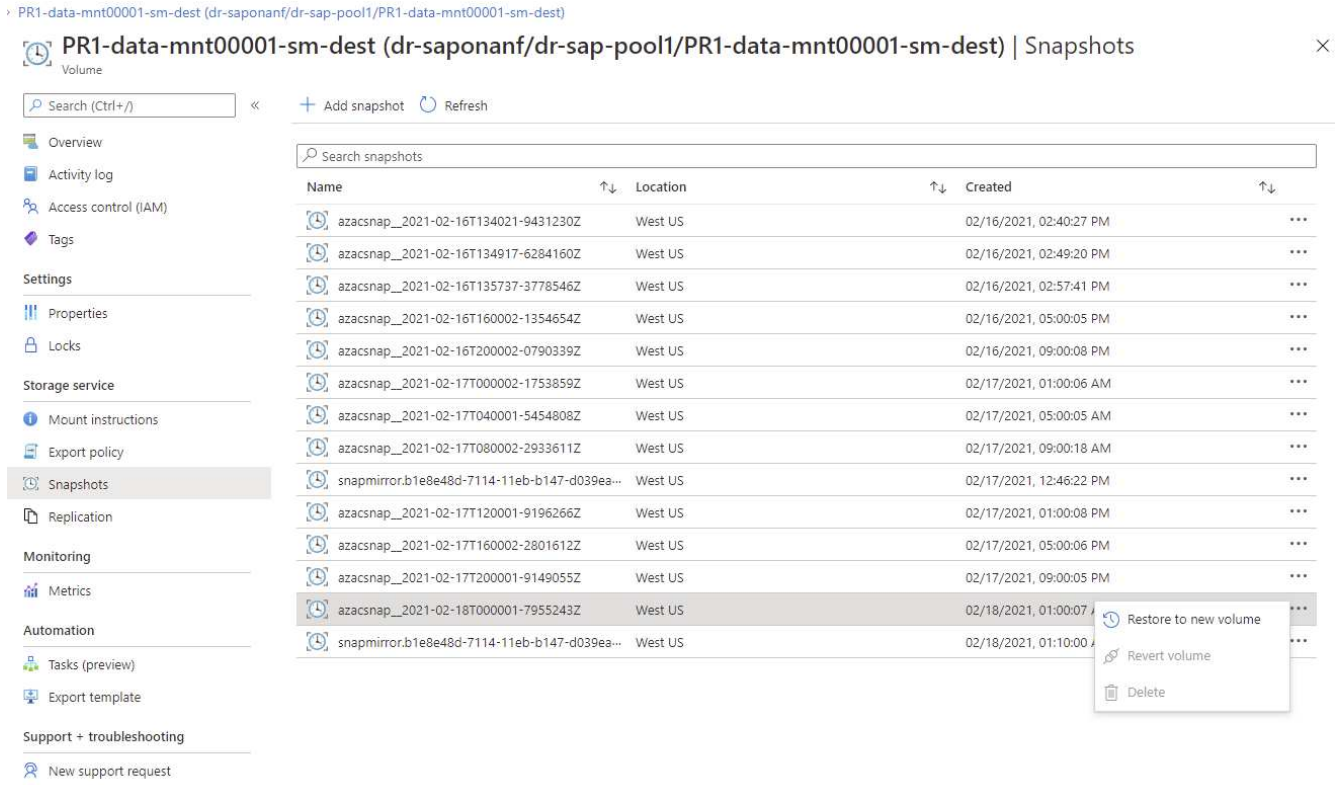
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt00001-sm-dest-clone /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa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

Erstellen Sie neue Volumes auf Basis von Snapshot-Backups am Disaster-Recovery-Standort

Abhängig vom Disaster Recovery Setup (mit oder ohne Log-Backup-Replikation) müssen zwei oder drei neue Volumes auf der Basis von Snapshot-Backups erstellt werden. In beiden Fällen muss ein neues Volume der Daten und das gemeinsame HANA Volume erstellt werden.

Wenn auch die Backup-Daten für das Protokoll repliziert werden, muss ein neues Volume des Backup-Volumes erstellt werden. In unserem Beispiel wurden die Daten und das Protokoll-Backup-Volume an den Disaster Recovery-Standort repliziert. In den folgenden Schritten wird das Azure-Portal verwendet.

1. Eines der applikationskonsistenten Snapshot-Backups wird als Quelle für das neue Volume des HANA-Daten-Volumes ausgewählt. Restore to New Volume ist ausgewählt, um ein neues Volume basierend auf der Snapshot-Sicherung zu erstellen.



2. Der neue Volume-Name und die neue Quote müssen in der Benutzeroberfläche angegeben werden.

Home > Azure NetApp Files > dr-saponanf > dr-sap-pool1 (dr-saponanf/dr-sap-pool1) > PR1-data-mnt00001-sm-dest (d

Create a volume

Basics Protocol Tags Review + create

This page will help you create an Azure NetApp Files volume in your subscription and enable you to access the volume from within your virtual network. Learn more about Azure NetApp Files

Volume details

Volume name *	PR1-data-mnt00001-sm-dest-clone
Restoring from snapshot	azacsnap__2021-02-18T000001-7955243Z
Available quota (GiB)	2096 2.05 TiB
Quota (GiB) *	500 500 GiB
Virtual network	dr-vnet (10.2.0.0/16,10.0.2.0/24)
Delegated subnet	default (10.0.2.0/28)
Show advanced section	☐

3. Auf der Registerkarte Protokoll werden der Dateipfad und die Exportrichtlinie konfiguriert.

Home > Azure NetApp Files > dr-saponanf > dr-sap-pool1 (dr-saponanf/dr-sap-pool1) > PR1-data-mnt00001-sm-dest (d

Create a volume

Basics | **Protocol** | Tags | Review + create

Configure access to your volume.

Access

Protocol type: (•) NFS ( ) SMB ( ) Dual-protocol (NFSv3 and SMB)

Configuration

File path * ⓘ: PR1-data-mnt00001-sm-dest-clone

Versions: NFSv4.1

Kerberos: ( ) Enabled (•) Disabled

Export policy

Configure the volume's export policy. This can be edited later. Learn more

↑ Move up ↓ Move down ↑ Move to top ↓ Move to bottom 🗑 Delete

☑ Index	Allowed clients	Access	Root Access
☑ 1	0.0.0.0/0	Read & Write	On

4. Der Bildschirm Erstellen und Prüfen fasst die Konfiguration zusammen.

Home > Azure NetApp Files > dr-saponanf > dr-sap-pool1 (dr-saponanf/dr-sap-pool1) > PR1-data-mnt00001-sm-dest (dr-sapon

Create a volume

Validation passed

Basics Protocol Tags **Review + create**

Basics

Subscription	Pay-As-You-Go
Resource group	dr-rg-sap
Region	West US
Volume name	PR1-data-mnt00001-sm-dest-clone
Capacity pool	dr-sap-pool1
Service level	Standard
Quota	500 GiB

Networking

Virtual network	dr-vnet (10.2.0.0/16,10.0.2.0/24)
Delegated subnet	default (10.0.2.0/28)

Protocol

Protocol	NFSv4.1
File path	PR1-data-mnt00001-sm-dest-clone

5. Auf Basis des HANA-Snapshot-Backups wurde jetzt ein neues Volume erstellt.

dr-saponanf | Volumes
NetApp account

Search (Ctrl+/)

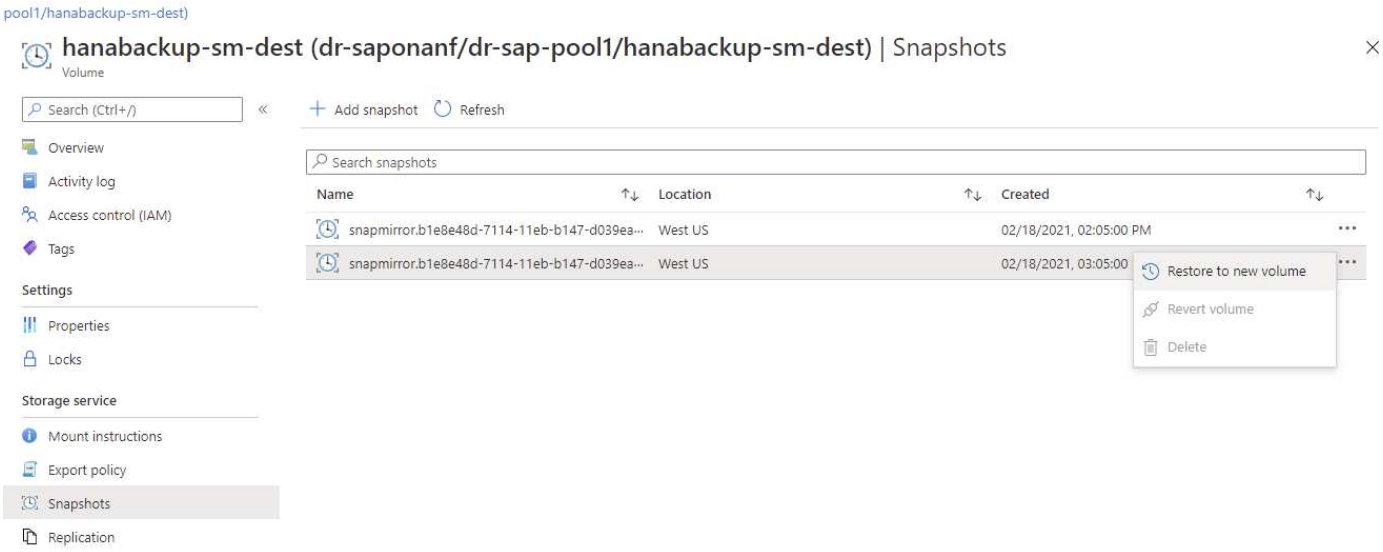
Overview
Activity log
Access control (IAM)
Tags
Settings
Properties
Locks
Azure NetApp Files
Active Directory connections
Storage service
Capacity pools
Volumes
Data protection
Snapshot policies
Automation
Tasks (preview)
Export template
Support + troubleshooting
New support request

Add volume | Add data replication | Refresh

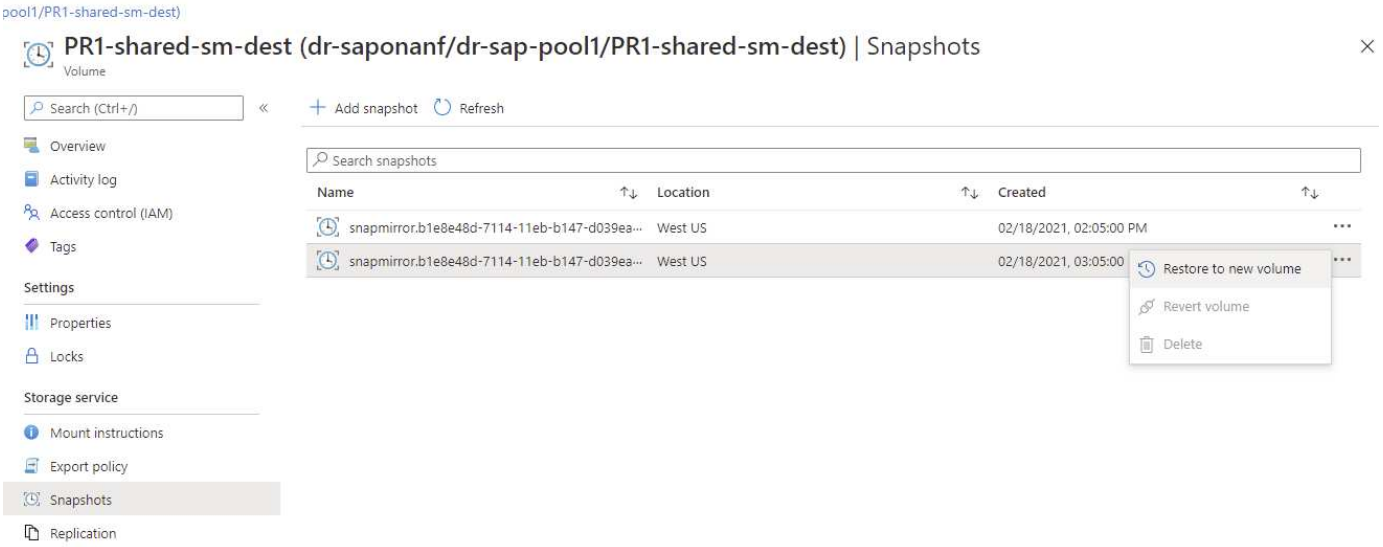
Search volumes

Name	Quota	Protocol type	Mount path	Service level	Capacity pool
hanabackup-sm-dest	1000 GiB	NFSv3	10.0.2.4:/hanabackup-sm-dest	Standard	dr-sap-pool1
PR1-data-mnt00001-sm-dest	500 GiB	NFSv4.1	10.0.2.4:/PR1-data-mnt00001-s	Standard	dr-sap-pool1
PR1-data-mnt00001-sm-dest-clone	500 GiB	NFSv4.1	10.0.2.4:/PR1-data-mnt00001-s	Standard	dr-sap-pool1
PR1-log-mnt00001-dr	250 GiB	NFSv4.1	10.0.2.4:/PR1-log-mnt00001-dr	Standard	dr-sap-pool1
PR1-shared-sm-dest	250 GiB	NFSv4.1	10.0.2.4:/PR1-shared-sm-dest	Standard	dr-sap-pool1

Die gleichen Schritte müssen nun für das freigegebene HANA und das Protokoll-Backup-Volumen, wie in den folgenden beiden Screenshots dargestellt, durchgeführt werden. Da keine zusätzlichen Snapshots für das HANA Shared-Backup-Volume und das Log-Backup-Volume erstellt wurden, muss die neueste SnapMirror Snapshot Kopie als Quelle für das neue Volume ausgewählt werden. Das sind unstrukturierte Daten, und die SnapMirror Snapshot Kopie kann für diesen Anwendungsfall genutzt werden.



Der folgende Screenshot zeigt das HANA Shared Volume, das auf dem neuen Volume wiederhergestellt ist.



Wenn ein Kapazitäts-Pool mit einer Tier mit niedriger Performance verwendet wurde, müssen die Volumes nun in einen Kapazitäts-Pool verschoben werden, der die erforderliche Performance bietet.

Alle drei neuen Volumes sind jetzt verfügbar und können auf dem Zielhost eingebunden werden.

Mounten Sie die neuen Volumes am Ziel-Host

Die neuen Volumes können jetzt auf Basis des auf dem Zielhost eingebunden werden `/etc/fstab` Datei zuvor erstellt.

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

Die folgende Ausgabe zeigt die erforderlichen Dateisysteme.

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

HANA Datenbank-Recovery

Im Folgenden werden die Schritte für das HANA-Datenbank-Recovery aufgeführt

Starten Sie die erforderlichen SAP-Dienste.

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

Die folgende Ausgabe zeigt die erforderlichen Prozesse.

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

In den folgenden Abschnitten wird der Recovery-Prozess mit und ohne Forward Recovery mit den replizierten Log-Backups beschrieben. Die Recovery wird mit dem HANA-Recovery-Skript für die Systemdatenbank und hdbsql-Befehle für die Mandanten-Datenbank ausgeführt.

Recovery zum aktuellen Backup-Speicherpunkt für das HANA-Datenvolumen

Die Wiederherstellung zum neuesten Backup savepoint wird mit folgenden Befehlen als User pr1adm ausgeführt:

- Systemdatenbank

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

- Mandantendatenbank

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

Sie können auch HANA Studio oder Cockpit verwenden, um die Wiederherstellung des Systems und der Mandanten-Datenbank auszuführen.

Die folgende Befehlsausgabe zeigt die Ausführung der Wiederherstellung.

Recovery der Systemdatenbank

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

Recovery von Mandanten-Datenbanken

Wenn für den Benutzer pr1adm am Quellsystem kein Benutzerspeicherschlüssel erstellt wurde, muss auf dem Zielsystem ein Schlüssel erstellt werden. Der im Schlüssel konfigurierte Datenbankbenutzer muss über Berechtigungen zur Ausführung von Mandanten-Recovery-Vorgängen verfügen.

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

Die Mandantenwiederherstellung wird jetzt mit hdbsql ausgeführt.

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

Die HANA-Datenbank ist jetzt betriebsbereit, und der Disaster-Recovery-Workflow für die HANA-Datenbank wurde getestet.

Recovery mit vorwärtsgerichteten Recovery mithilfe von Log-/Katalog-Backups

Log-Backups und der HANA-Backup-Katalog werden aus dem Quellsystem repliziert.

Die Wiederherstellung mit allen verfügbaren Log-Backups wird mit den folgenden Befehlen als Benutzer pr1adm ausgeführt:

- Systemdatenbank

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

- Mandantendatenbank

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

> Um eine Wiederherstellung mit allen verfügbaren Protokollen durchzuführen, können Sie jederzeit als Zeitstempel in der Recovery-Anweisung verwenden.

Sie können auch HANA Studio oder Cockpit verwenden, um die Wiederherstellung des Systems und der Mandanten-Datenbank auszuführen.

Die folgende Befehlsausgabe zeigt die Ausführung der Wiederherstellung.

Recovery der Systemdatenbank

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

Recovery von Mandanten-Datenbanken

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

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

hdbsql SYSTEMDB=>
```

Die HANA-Datenbank ist jetzt betriebsbereit, und der Disaster-Recovery-Workflow für die HANA-Datenbank wurde getestet.

Überprüfen Sie die Konsistenz der neuesten Protokoll-Backups

Da die Volume-Replizierung für das Protokoll unabhängig vom von dem von der SAP HANA Datenbank ausgeführten Backup-Prozess durchgeführt wird, können am Disaster Recovery-Standort inkonsistente Backup-Dateien für Protokolle vorhanden sein. Nur die letzten Backup-Dateien für Protokolle sind möglicherweise inkonsistent und diese Dateien sollten überprüft werden, bevor eine Weiterleitung der Recovery am Disaster Recovery-Standort mithilfe der erfolgt `hdbbackupcheck` Werkzeug.

Wenn der `hdbbackupcheck` Tool meldet Fehler bei den letzten Protokollsicherungen muss der neueste Satz von Protokollsicherungen entfernt oder gelöscht werden.

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

Die Prüfung muss für die aktuellen Log-Backup-Dateien des Systems und der Mandanten-Datenbank ausgeführt werden.

Wenn der `hdbbackupcheck` Tool meldet Fehler bei den letzten Protokollsicherungen muss der neueste Satz von Protokollsicherungen entfernt oder gelöscht werden.

Disaster-Recovery-Failover

Disaster-Recovery-Failover

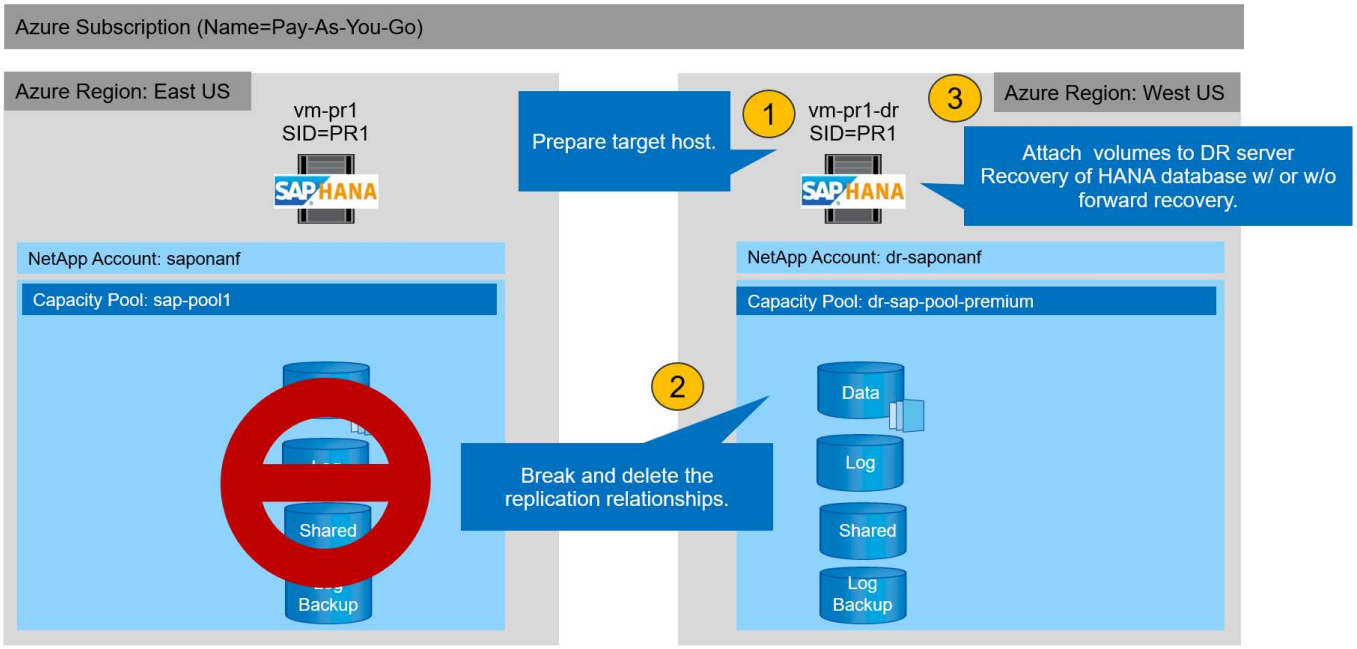
Je nachdem, ob die Backup-Replizierung des Protokolls Teil der Disaster Recovery-Einrichtung ist, unterscheiden sich die Schritte für Disaster Recovery leicht. In diesem Abschnitt wird das Disaster Recovery Failover für die reine Daten-Backup-Replizierung sowie für die Replizierung von Daten-Volumes in Kombination mit der Replizierung des Backup-Volumes für das Protokoll beschrieben.

Um Disaster Recovery-Failover auszuführen, gehen Sie wie folgt vor:

1. Bereiten Sie den Zielhost vor.
2. Brechen Sie die Replikationsbeziehungen auf und löschen Sie sie.
3. Wiederherstellung des Datenvolumens im letzten applikationskonsistenten Snapshot-Backup
4. Mounten Sie die Volumes am Ziel-Host.
5. Stellen Sie die HANA Datenbank wieder her.
    - Nur Daten-Volume-Recovery.
    - Recovery mit replizierten Protokoll-Backups vorführen.

In den folgenden Abschnitten werden diese Schritte detailliert beschrieben und die folgende Abbildung zeigt

Disaster-Failover-Tests.



Bereiten Sie den Zielhost vor

In diesem Abschnitt werden die Vorbereitungsschritte beschrieben, die auf dem Server für das Disaster-Recovery-Failover erforderlich sind.

Im normalen Betrieb wird der Zielhost normalerweise für andere Zwecke verwendet, beispielsweise als HANA QA- oder Testsystem. Daher müssen die meisten der beschriebenen Schritte bei der Ausführung von Disaster Failover-Tests ausgeführt werden. Zum anderen die relevanten Konfigurationsdateien, wie `/etc/fstab` Und `/usr/sap/sapservices`, Kann vorbereitet werden und dann in die Produktion durch einfaches Kopieren der Konfigurationsdatei. Das Disaster Recovery-Failover-Verfahren stellt sicher, dass die relevanten vorbereiteten Konfigurationsdateien korrekt konfiguriert sind.

Die Vorbereitung des Ziel-Hosts umfasst auch das Herunterfahren des HANA QA- oder Testsystems sowie das Anhalten aller Services mit `systemctl stop sapinit`.

Hostname und IP-Adresse des Zielservers

Der Hostname des Zielservers muss mit dem Hostnamen des Quellsystems identisch sein. Die IP-Adresse kann unterschiedlich sein.

> Ein ordnungsgemäßes Fechten des Zielservers muss eingerichtet werden, damit er nicht mit anderen Systemen kommunizieren kann. Wenn keine ordnungsgemäße Fechten vorhanden sind, kann das geklonte Produktionssystem Daten mit anderen Produktionssystemen austauschen, was zu logisch beschädigten Daten führt.

Installieren Sie die erforderliche Software

Die SAP-Hostagent-Software muss auf dem Zielserver installiert sein. Ausführliche Informationen finden Sie im "SAP Host Agent" Im SAP-Hilfeportal.

Wenn der Host als HANA QA- oder Testsystem verwendet wird, ist die SAP-Hostagent-Software bereits installiert.

Konfiguration von Benutzern, Ports und SAP-Diensten

Die erforderlichen Anwender und Gruppen für die SAP HANA-Datenbank müssen auf dem Zielserver verfügbar sein. In der Regel wird die zentrale Benutzerverwaltung verwendet. Daher sind keine Konfigurationsschritte auf dem Zielserver erforderlich. Die erforderlichen Ports für die HANA-Datenbank müssen auf den Ziel-Hosts konfiguriert sein. Die Konfiguration kann durch Kopieren des aus dem Quellsystem kopiert werden `/etc/services` Datei auf dem Zielserver.

Die erforderlichen SAP Services-Einträge müssen auf dem Zielhost verfügbar sein. Die Konfiguration kann durch Kopieren des aus dem Quellsystem kopiert werden `/usr/sap/sapservices` Datei auf dem Zielserver. Die folgende Ausgabe zeigt die erforderlichen Einträge für die im Lab-Setup verwendete SAP HANA-Datenbank.

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

HANA-Protokollvolumen vorbereiten

Da das HANA-Protokoll-Volume nicht Teil der Replikation ist, muss auf dem Ziel-Host ein leeres Protokoll-Volume vorhanden sein. Das Protokoll-Volume muss dieselben Unterverzeichnisse enthalten wie das Quell-HANA-System.

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

Erstellen des Backup-Volumes für das Protokoll

Da das Quellsystem für die HANA-Protokoll-Backups mit einem separaten Volume konfiguriert ist, muss auch ein Protokoll-Backup-Volume auf dem Zielhost verfügbar sein. Ein Volume für die Protokoll-Backups muss konfiguriert und auf dem Ziel-Host gemountet werden.

Wenn die Protokollsicherung Teil der Disaster Recovery-Einrichtung ist, wird das replizierte Backup-Volume für das Protokoll auf dem Zielhost gemountet und es ist nicht erforderlich, ein zusätzliches Protokoll-Backup-Volume vorzubereiten.

Bereiten Sie Dateisystemeinhängungen vor

In der folgenden Tabelle sind die Namenskonventionen aufgeführt, die für das Lab-Setup verwendet werden. Die Volume-Namen am Disaster-Recovery-Standort sind in enthalten `/etc/fstab`.

HANA PR1-Volumes	Volumes und Unterverzeichnisse am Disaster Recovery-Standort	Bereitstellungspunkt am Zielhost
Datenvolumen	PR1-Data-mnt00001-SM-dest	/hana/Data/PR1/mnt00001
Freigegebenes Volume	PR1-shared-sm-dest/shared PR1-shared-SM-dest/usr-sap-PR1	/hana/shared /usr/sap/PR1
Backup-Volume protokollieren	Hanabackup-SM-dest	/Hanabackup

Die Mount-Punkte aus dieser Tabelle müssen auf dem Zielhost erstellt werden.

Hier sind die erforderlichen `/etc/fstab` Einträge.

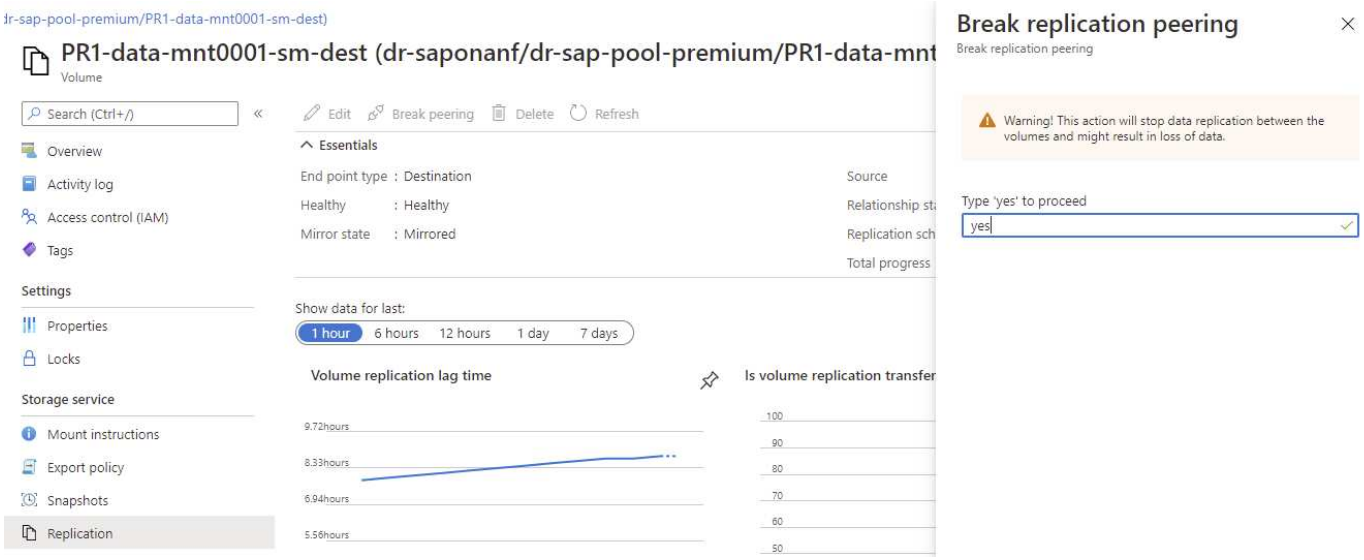
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa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

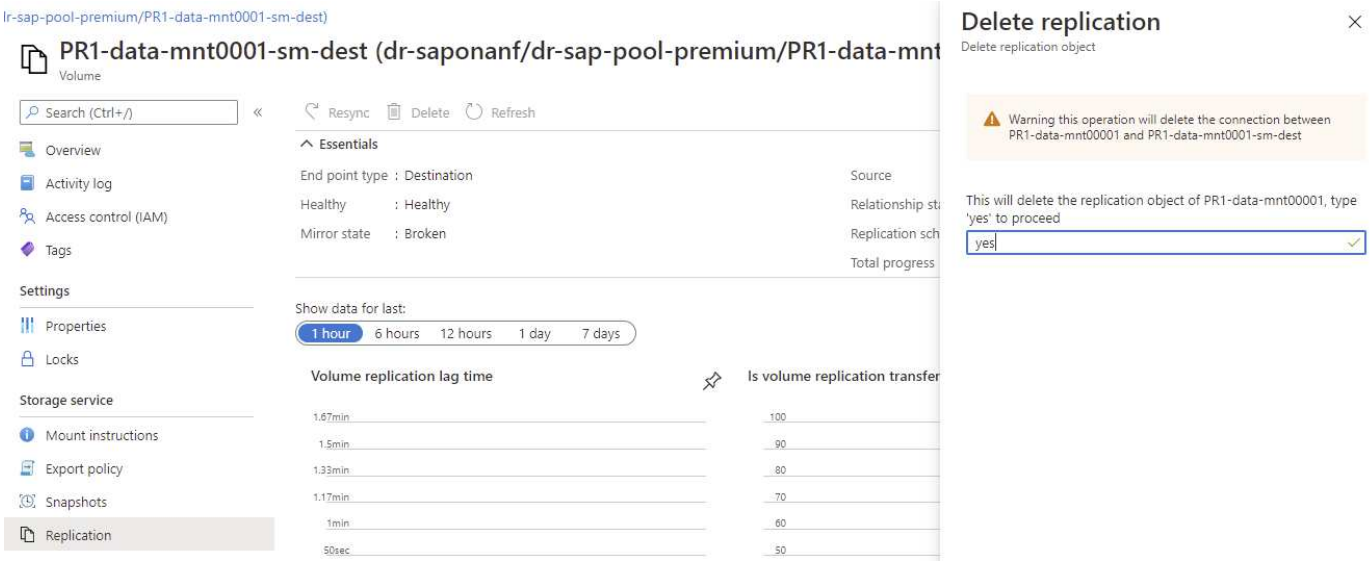
Peering der Replizierung unterbrechen und löschen

Im Falle eines Disaster-Failovers müssen die Ziel-Volumes unterbrochen werden, damit der Zielhost die Volumes für Lese- und Schreibvorgänge mounten kann.

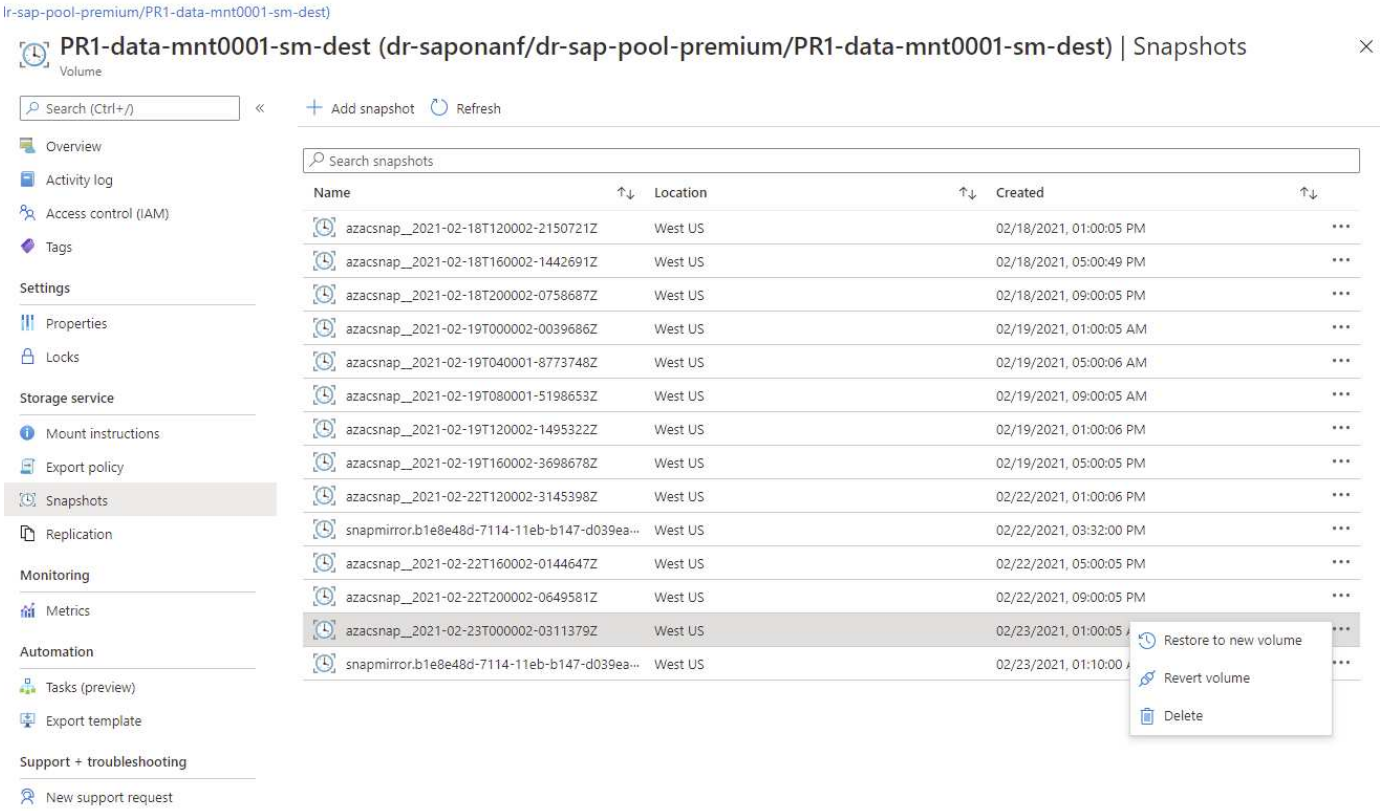
Für das HANA Daten-Volume müssen Sie das aktuelle HANA Snapshot-Backup wiederherstellen, das mit AzAcSnap erstellt wurde. Dieser Vorgang zum Zurücksetzen des Volumes ist nicht möglich, wenn der neueste ReplikationssSnapshot aufgrund des Replication Peering als belegt markiert wird. Deshalb müssen Sie auch das Replication Peering löschen.

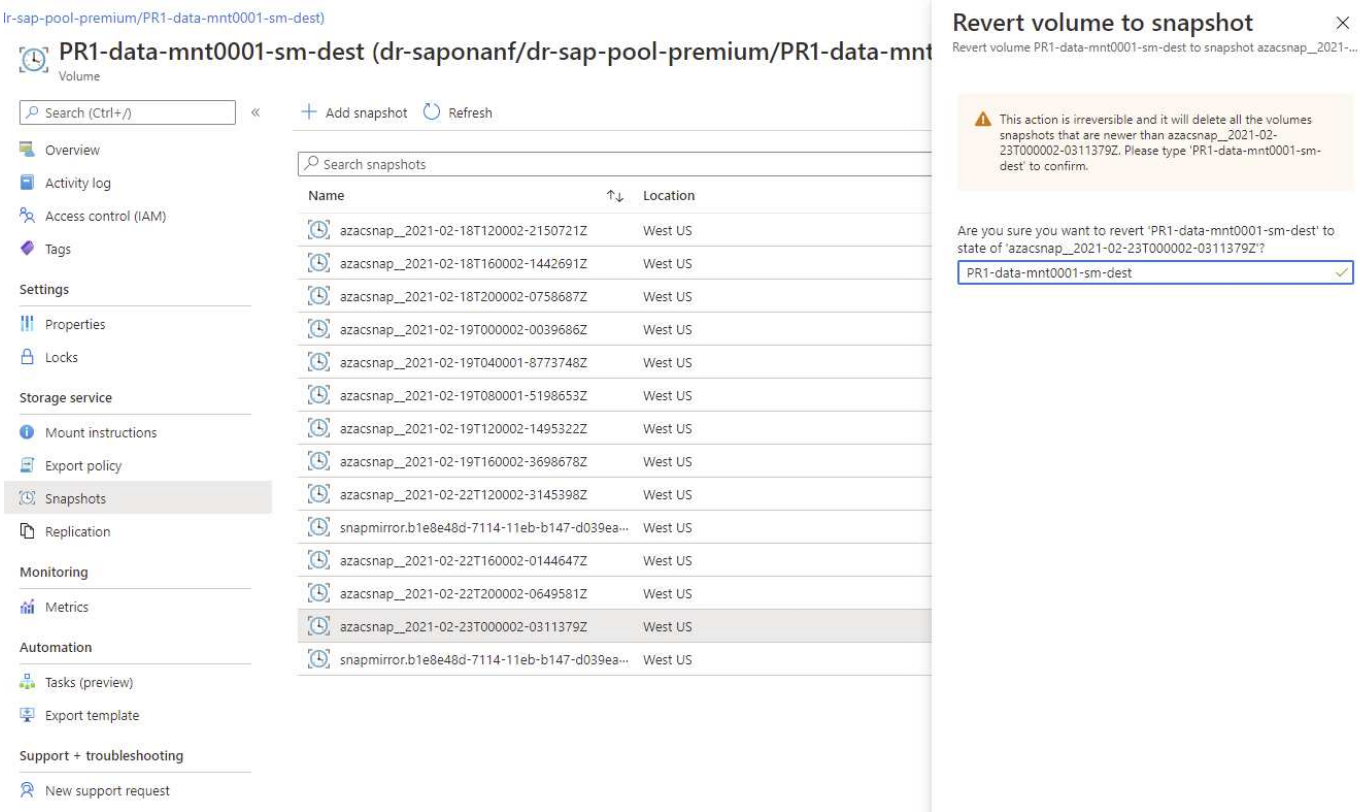
Die nächsten beiden Screenshots zeigen den Break and delete Peering-Vorgang für das HANA-Datenvolumen. Dieselben Vorgänge müssen auch für das Log-Backup und das gemeinsame HANA-Volume durchgeführt werden.





Da Replication Peering gelöscht wurde, ist es möglich, das Volume auf das neueste HANA Snapshot Backup zurückzusetzen. Wenn Peering nicht gelöscht wird, wird die Auswahl des Revert-Volumes ausgegraut und ist nicht wählbar. Die folgenden zwei Screenshots zeigen den Vorgang zur Zurücksetzen des Volumens.





Nach der Wiederherstellung des Volumes basiert das Daten-Volume auf einem konsistenten HANA-Snapshot-Backup und kann nun für Recovery-Vorgänge genutzt werden.

Wenn ein Kapazitäts-Pool mit einer Tier mit niedriger Performance verwendet wurde, müssen die Volumes nun in einen Kapazitäts-Pool verschoben werden, der die erforderliche Performance bietet.

Mounten Sie die Volumes am Ziel-Host

Die Volumes können jetzt auf der Grundlage des auf dem Zielhost eingebunden werden `/etc/fstab` Datei zuvor erstellt.

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

Die folgende Ausgabe zeigt die erforderlichen Dateisysteme.

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

HANA Datenbank-Recovery

Die folgenden Schritte sind für das HANA-Datenbank-Recovery beschrieben.

Starten Sie die erforderlichen SAP-Dienste.

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

Die folgende Ausgabe zeigt die erforderlichen Prozesse.

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

In den folgenden Abschnitten wird der Recovery-Prozess mit der vorwärts gerichteten Recovery mit den replizierten Protokoll-Backups beschrieben. Die Recovery wird mit dem HANA-Recovery-Skript für die Systemdatenbank und hdbsql-Befehle für die Mandanten-Datenbank ausgeführt.

Die Befehle zur Ausführung einer Wiederherstellung zum neuesten Speicherpunkt von Daten werden in Kapitel beschrieben "Recovery zum neuesten HANA Daten-Volume-Backup-Speicherpunkt".

Recovery mit vorwärtsgerichteten Recovery mithilfe von Log-Backups

Die Wiederherstellung mit allen verfügbaren Log-Backups wird mit den folgenden Befehlen als Benutzer pr1adm ausgeführt:

- Systemdatenbank

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

- Mandantendatenbank

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

> Um die Wiederherstellung mit allen verfügbaren Protokollen zu ermöglichen, können Sie jederzeit als Zeitstempel in der Wiederherstellungsanweisung verwenden.

Sie können auch HANA Studio oder Cockpit verwenden, um die Wiederherstellung des Systems und der Mandanten-Datenbank auszuführen.

Die folgende Befehlsausgabe zeigt die Ausführung der Wiederherstellung.

Recovery der Systemdatenbank

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

Recovery von Mandanten-Datenbanken

Wenn für den Benutzer pr1adm am Quellsystem kein Benutzerspeicherschlüssel erstellt wurde, muss auf dem Zielsystem ein Schlüssel erstellt werden. Der im Schlüssel konfigurierte Datenbankbenutzer muss über Berechtigungen zur Ausführung von Mandanten-Recovery-Vorgängen verfügen.

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

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

Überprüfen Sie die Konsistenz der neuesten Protokoll-Backups

Da die Volume-Replizierung für das Protokoll unabhängig vom von dem von der SAP HANA Datenbank ausgeführten Backup-Prozess durchgeführt wird, können am Disaster Recovery-Standort inkonsistente Backup-Dateien für Protokolle vorhanden sein. Nur die letzten Backup-Dateien für Protokolle sind möglicherweise inkonsistent und diese Dateien sollten überprüft werden, bevor eine Weiterleitung der Recovery am Disaster Recovery-Standort mithilfe der erfolgt `hdbbackupcheck` Werkzeug.

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

Die Prüfung muss für die aktuellen Log-Backup-Dateien des Systems und der Mandanten-Datenbank ausgeführt werden.

Wenn der `hdbbackupcheck` Tool meldet Fehler bei den letzten Protokollsicherungen muss der neueste Satz von Protokollsicherungen entfernt oder gelöscht werden.

Aktualisierungsverlauf

An dieser Lösung wurden seit ihrer ersten Veröffentlichung folgende technische Änderungen vorgenommen:

Version	Datum	Zusammenfassung aktualisieren
Version 1.0	April 2021	Ausgangsversion

TR-4646: SAP HANA Disaster Recovery with Storage Replication

Nils Bauer, NetApp

Der TR-4646 bietet einen Überblick über die Optionen für Disaster-Recovery-Schutz für SAP HANA. Sie enthält detaillierte Setup-Informationen und eine Beschreibung des Anwendungsfalls für eine Disaster-Recovery-Lösung an drei Standorten, die auf synchroner und asynchroner NetApp SnapMirror Storage-Replizierung basiert. Bei der beschriebenen Lösung wird NetApp SnapCenter mit dem SAP HANA Plug-in

eingesetzt, um die Datenbankkonsistenz zu managen.

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

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

Nils Bauer, NetApp

TR-4313 beschreibt die Installation und Konfiguration der NetApp Backup- und Recovery-Lösung für SAP HANA. Die Lösung basiert auf dem NetApp Snap Creator Framework und dem Snap Creator Plug-in für SAP HANA. Diese Lösung wird durch die zertifizierte Cisco SAP HANA Multinode Appliance in Kombination mit NetApp Storage unterstützt. Unterstützt wird diese Lösung auch durch SAP HANA-Systeme mit einem Node und mehreren Knoten in TDI-Projekten (Tailored Datacenter Integration).

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

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

Marco Schoen, NetApp

Dr. Tristan Daude, Commvault Systems

TR-4711 beschreibt das Design einer NetApp und CommVault Lösung für SAP HANA, die CommVault IntelliSnap Snapshot-Managementtechnologie und NetApp Snapshot Technologie umfasst. Die Lösung basiert auf NetApp Storage und der CommVault Datensicherungssuite.

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

NVA-1147-DESIGN: SAP HANA auf NetApp All-SAN-Array: Modernes SAN, Datensicherung und Disaster Recovery

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

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

Diese NetApp Verified Architecture deckt die Modernisierung von SAP-Systemen und Betriebsabläufe für SAP HANA auf NetApp All SAN-Array (ASA) Storage-Systemen mit Brocade FC SAN Fabric ab. Sie umfasst Backup und Recovery, Disaster Recovery und Datensicherung. Die Lösung nutzt NetApp SnapCenter, um Backup, Restore und Recovery von SAP HANA sowie die Klon-Workflows zu automatisieren. Konfiguration, Tests und Failover-Szenarien von Disaster Recovery werden mit synchroner NetApp SnapMirror Datenreplizierungssoftware beschrieben. Darüber hinaus wird SAP Data Protection mit CommVault beschrieben.

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