Backup, Restore und Disaster Recovery

NetApp solutions for SAP

NetApp
December 16, 2025

Inhalt

Backup, Restore und Disaster Recovery

Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter

Schützen Sie SAP HANA-Systeme mit SnapCenter über ONTAP, Azure NetApp Files und FSx für ONTAP hinweg.

Schützen Sie SAP HANA-Systeme mit NetApp SnapCenter mithilfe von Snapshot-basierten Backups und Datenreplikation. Diese Lösung umfasst die Konfiguration von SnapCenter sowie bewährte Vorgehensweisen für den Betrieb von SAP HANA-Systemen auf ONTAP AFF und ASA -Systemen, Azure NetApp Files und Amazon FSx für ONTAP, einschließlich Backup-Strategien, Konsistenzprüfungen und Wiederherstellungs-Workflows.

Autor: Nils Bauer, NetApp

Weitere anwendungsspezifische Details zu SAP-Systemaktualisierungsvorgängen und SAP-HANA-Systemreplikation finden Sie unter:

- "Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"
- "SAP HANA System Replication – Backup und Recovery mit SnapCenter"

Die besten Vorgehensweisen für die Kombination von SnapCenter -Datenschutz und NetApp SnapMirror ActiveSync werden beschrieben in

- "SAP HANA-Datenschutz und hohe Verfügbarkeit mit SnapCenter SnapMirror Active Sync und VMware Metro Storage Cluster"

Zusätzliche plattformspezifische Dokumentationen zu Best Practices sind verfügbar unter

- "SAP HANA-Datenschutz mit SnapCenter mit VMware VMFS und NetApp ASA -Systemen"
- "SAP HANA auf Amazon FSX für NetApp ONTAP – Backup und Recovery mit SnapCenter"
- "SAP HANA Datensicherung auf Azure NetApp Files with SnapCenter (Blog und Video)"
- "SAP Systemaktualisierung und Klonvorgänge auf Azure NetApp Files mit SnapCenter (Blog und Video)"

Erfahren Sie mehr über den SAP HANA-Datenschutz mit der NetApp Snapshot-Technologie.

Erfahren Sie, wie die NetApp Snapshot-Technologie SAP HANA-Datenbanken mit Backups schützt, die unabhängig von der Datenbankgröße in wenigen Minuten abgeschlossen sind. Lernen Sie Backup- und Wiederherstellungsstrategien kennen, die Snapshot-Kopien, SnapRestore für eine schnelle Wiederherstellung und die Replikation mit SnapVault oder Azure NetApp Files -Backup für einen sekundären Schutz nutzen.

Unternehmen benötigen heutzutage eine kontinuierliche und unterbrechungsfreie Verfügbarkeit ihrer SAP-Anwendungen. Sie erwarten ein gleichbleibendes Leistungsniveau und benötigen angesichts stetig wachsender Datenmengen und des Bedarfs an routinemäßigen Wartungsarbeiten, wie z. B.

Systemsicherungen, einen automatisierten täglichen Betrieb. Die Durchführung von Backups von SAP-Datenbanken ist eine kritische Aufgabe und kann erhebliche Auswirkungen auf die Leistung des produktiven SAP-Systems haben.

Die Backup-Fenster werden immer kleiner, während die Menge der zu sichernden Daten immer größer wird. Daher ist es schwierig, einen Zeitpunkt zu finden, an dem man Datensicherungen durchführen kann, ohne die Geschäftsprozesse wesentlich zu beeinträchtigen. Die für die Wiederherstellung und den Betrieb von SAP-Systemen benötigte Zeit ist ein Grund zur Sorge, da Ausfallzeiten für SAP-Produktions- und Nichtproduktionssysteme minimiert werden müssen, um die Kosten für das Unternehmen zu reduzieren.

Datensicherung und Wiederherstellung mithilfe von Snapshot-Backups

Mit der NetApp Snapshot-Technologie können Sie innerhalb von Minuten Datenbank-Backups erstellen. Die zum Erstellen einer Snapshot-Kopie benötigte Zeit ist unabhängig von der Größe der Datenbank, da bei einer Snapshot-Kopie keine physischen Datenblöcke auf der Speicherplattform verschoben werden. Darüber hinaus hat die Verwendung der Snapshot-Technologie keine Auswirkungen auf die Leistung des laufenden SAP-Systems, da alle Operationen im Speichersystem ausgeführt werden. Daher können Sie die Erstellung von Snapshot-Kopien planen, ohne Spitzenzeiten für Dialoge oder Batch-Aktivitäten berücksichtigen zu müssen. SAP-on- NetApp -Kunden planen typischerweise mehrere Online-Snapshot-Backups über den Tag verteilt; beispielsweise ist ein Abstand von sechs Stunden üblich. Diese Snapshot-Backups werden in der Regel drei bis fünf Tage lang auf dem primären Speichersystem aufbewahrt, bevor sie entfernt oder zur Langzeitarchivierung auf einen günstigeren Speicher ausgelagert werden.

Snapshot-Kopien bieten auch entscheidende Vorteile bei Wiederherstellungs- und Reparaturvorgängen. Bei einer Wiederherstellungsoperation werden die Daten im Dateisystem auf Basis des Zustands einer Sicherung wiederhergestellt. Bei einer Wiederherstellungsoperation wird der Datenbankzustand mithilfe von Datenbankprotokollsicherungen auf einen bestimmten Zeitpunkt zurückgesetzt.

Die NetApp SnapRestore Technologie ermöglicht die Wiederherstellung einer gesamten Datenbank oder alternativ nur eines Teils der Datenbank auf Basis der aktuell verfügbaren Snapshot-Backups. Der Wiederherstellungsprozess ist unabhängig von der Größe der Datenbank in wenigen Sekunden abgeschlossen. Da im Laufe des Tages mehrere Online-Snapshot-Backups erstellt werden können, verkürzt sich die für den Wiederherstellungsprozess benötigte Zeit im Vergleich zu einem herkömmlichen Backup-Ansatz, der nur einmal täglich durchgeführt wird, erheblich. Da Sie eine Wiederherstellung mit einer Snapshot-Kopie durchführen können, die höchstens nur wenige Stunden alt ist (statt bis zu 24 Stunden), müssen bei der Vorwärtswiederherstellung weniger Transaktionsprotokolle angewendet werden. Der Zeitaufwand für Wiederherstellung und Datenrettung wird im Vergleich zu herkömmlichen Streaming-Backups deutlich reduziert.

Da Snapshot-Backups auf demselben Datenträgersystem wie die aktiven Online-Daten gespeichert werden, empfiehlt NetApp, Snapshot-Kopien-Backups eher als Ergänzung denn als Ersatz für Backups an einem sekundären Speicherort zu verwenden. Die meisten Wiederherstellungs- und Reparaturvorgänge werden mithilfe von SnapRestore auf dem primären Speichersystem verwaltet. Die Wiederherstellung von einem sekundären Speicherort ist nur dann erforderlich, wenn das primäre Speichersystem, das die Snapshot-Kopien enthält, nicht verfügbar ist. Sie können die sekundäre Sicherung auch dann verwenden, wenn es notwendig ist, eine Sicherung wiederherzustellen, die auf dem primären Speicher nicht mehr verfügbar ist.

Eine Datensicherung an einem sekundären Speicherort basiert auf Snapshot-Kopien, die auf dem primären Speicher erstellt wurden. Die Daten werden daher direkt aus dem primären Speichersystem gelesen, ohne dass dadurch eine Last auf dem SAP-Datenbankserver und seinem Netzwerk entsteht. Der primäre Speicher kommuniziert direkt mit dem sekundären Speicher und repliziert die Sicherungsdaten mithilfe der SnapVault oder ANF-Sicherungsfunktionalität an das Ziel.

SnapVault und ANF-Backups bieten im Vergleich zu herkömmlichen Backups erhebliche Vorteile. Nach einer ersten Datenübertragung, bei der alle Daten von der Quelle zum Ziel übertragen werden, werden bei allen

nachfolgenden Backups nur die geänderten Blöcke auf den Sekundärspeicher repliziert. Dadurch werden die Belastung des primären Speichersystems und die für eine vollständige Datensicherung benötigte Zeit deutlich reduziert. Da am Zielort nur die geänderten Blöcke gespeichert werden, benötigt jede zusätzliche vollständige Datenbanksicherung deutlich weniger Speicherplatz.

Laufzeit von Snapshot-Backup- und -Restore-Vorgängen

Die folgende Abbildung zeigt HANA Studio eines Kunden, der Snapshot-Backup-Operationen durchführt. Das Bild zeigt, dass die HANA-Datenbank (ca. 4 TB groß) mit der Snapshot-Backup-Technologie in 1 Minute und 20 Sekunden gesichert wird, während eine dateibasierte Sicherung mehr als 4 Stunden dauert.

Den größten Teil der gesamten Laufzeit des Backup-Workflows entfällt auf die Zeit, die für die Ausführung des HANA-Datenbank-Snapshot-Vorgangs benötigt wird. Die Sicherung des Speicher-Snapshots selbst ist unabhängig von der Größe der HANA-Datenbank in wenigen Sekunden abgeschlossen.

[Breite=624, Höhe=267]

Vergleich der Recovery-Zeitvorgaben

Dieser Abschnitt bietet einen Vergleich der Wiederherstellungszeitziele (RTO) von dateibasierten und speicherbasierten Snapshot-Backups. Die RTO (Recovery Time Out) ist definiert als die Summe der Zeit, die für die Wiederherstellung, die Wiederherstellung und den anschließenden Start 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 NetApp Snapshot-Backups ist die Wiederherstellungszeit unabhängig von der Größe der Datenbank und liegt immer im Bereich von wenigen Sekunden.

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 typischerweise in höherer Frequenz geplant, da sie keinen Einfluss auf die Leistung der SAP HANA-Datenbank haben. Wenn beispielsweise Snapshot-Backups alle sechs Stunden geplant sind, müssten im schlimmsten Fall Protokolle für die letzten sechs Stunden angewendet werden, wenn der Fehler unmittelbar vor der Erstellung des nächsten Snapshots auftritt. Für eine tägliche dateibasierte Datensicherung müssten im schlimmsten Fall die Protokolle der letzten 24 Stunden angewendet werden.

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.

Wiederherstellungs- und Recovery-Beispielberechnung

Die folgende Abbildung zeigt einen Vergleich zwischen Wiederherstellungs- und Recovery-Operationen mit einer täglichen dateibasierten Datensicherung und Snapshot-Datensicherungen mit unterschiedlichen 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.

[Breite=624, Höhe=326]

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, wie eine bedarfsgesteuerte Datensicherung vor dem Upgrade und eine mögliche Wiederherstellung im Falle eines Upgrade-Fehlers einen erheblichen Einfluss auf die gesamte geplante Ausfallzeit haben. Am Beispiel einer 4-TB-Datenbank lässt sich die geplante Ausfallzeit um 8 Stunden reduzieren, oder man hat 8 weitere Stunden Zeit für die Analyse und Behebung von Fehlern durch die Verwendung von Snapshot-basierten Sicherungs- und Wiederherstellungsvorgängen.

Ein weiterer Anwendungsfall wäre ein typischer Testzyklus, bei dem die Tests über mehrere Iterationen mit unterschiedlichen Datensätzen oder Parametern durchgeführt werden müssen. Durch die Nutzung der schnellen Sicherungs- und Wiederherstellungsfunktionen können Sie innerhalb Ihres Testzyklus problemlos Speicherpunkte erstellen und das System auf einen dieser vorherigen Speicherpunkte zurücksetzen, falls ein Test fehlschlägt oder wiederholt werden muss. Dadurch können die Tests früher abgeschlossen werden oder es können mehr Tests gleichzeitig durchgeführt werden, was die Testergebnisse verbessert.

[Breite=618, Höhe=279]

Sobald Snapshot-Backups implementiert sind, können sie für zahlreiche weitere Anwendungsfälle genutzt werden, die Kopien einer HANA-Datenbank erfordern. Sie können ein neues Volume auf Basis des Inhalts einer beliebigen verfügbaren Snapshot-Sicherung erstellen. Die Laufzeit dieses Vorgangs beträgt wenige Sekunden, unabhängig von der Größe des Volumens.

Der häufigste Anwendungsfall ist die SAP-Systemaktualisierung, bei der Daten aus dem Produktivsystem in das Test- oder QA-System kopiert werden müssen. Durch die Nutzung der ONTAP oder ANF-Klonfunktion können Sie das Volume für das Testsystem innerhalb weniger Sekunden aus einer beliebigen Snapshot-Kopie des Produktionssystems bereitstellen. Anschließend muss das neue Volume an das Testsystem angebunden und die HANA-Datenbank wiederhergestellt werden.

Der zweite Anwendungsfall ist die Schaffung eines Reparatursystems, das dazu dient, logische Fehler im Produktionssystem zu beheben. In diesem Fall wird ein älteres Snapshot-Backup des Produktionssystems verwendet, um ein Reparatursystem zu starten, das eine identische Kopie des Produktionssystems mit den Daten vor dem Auftreten der Beschädigung darstellt. Anschließend wird das Reparatursystem verwendet, um das Problem zu analysieren und die benötigten Daten zu exportieren, bevor sie beschädigt wurden.

Der letzte Anwendungsfall ist die Möglichkeit, einen Failover-Test im Rahmen der Notfallwiederherstellung durchzuführen, ohne die Replikation zu unterbrechen und somit die RTO und den Recovery Point Objective (RPO) der Notfallwiederherstellungskonfiguration zu beeinflussen. Wenn die Replikation von ONTAP SnapMirror oder die regionsübergreifende Replikation von ANF zur Replikation der Daten an den Disaster-Recovery-Standort verwendet wird, stehen die Produktions-Snapshot-Backups auch am Disaster-Recovery-Standort zur Verfügung und können dann zur Erstellung eines neuen Volumes für Disaster-Recovery-Tests verwendet werden.

[Breite=627, Höhe=328]

Erfahren Sie mehr über die SnapCenter -Architektur.

Erfahren Sie mehr über die SnapCenter -Architektur für den SAP HANA-Datenschutz, einschließlich des SnapCenter -Servers, der Plug-in-Komponenten und der unterstützten Speicherplattformen. SnapCenter bietet eine zentrale Backup-, Wiederherstellungs- und Klonverwaltung für SAP HANA-Datenbanken auf ONTAP -Systemen, Azure NetApp Files und FSx für ONTAP.

SnapCenter ist eine einheitliche Plattform für anwendungskonsistenten Datenschutz. SnapCenter bietet zentrale Steuerung und Überwachung und überlässt es gleichzeitig den Benutzern, anwendungsspezifische Sicherungs-, Wiederherstellungs- und Klonvorgänge selbst zu verwalten. NetApp SnapCenter ist ein einziges Tool, mit dem Datenbank- und Speicheradministratoren Backup-, Wiederherstellungs- und Klonvorgänge für eine Vielzahl von Anwendungen und Datenbanken verwalten können. SnapCenter unterstützt NetApp ONTAP -Speichersysteme sowie Azure NetApp Files und FSx für ONTAP. Mit SnapCenter können Sie außerdem Daten zwischen lokalen Umgebungen, zwischen lokalen Umgebungen und der Cloud sowie zwischen privaten, hybriden oder öffentlichen Clouds replizieren.

SnapCenter umfasst den SnapCenter -Server und die SnapCenter -Plug-ins. Die Plug-ins sind für verschiedene Anwendungen und Infrastrukturkomponenten verfügbar. Der SnapCenter -Server kann entweder unter Windows oder unter Linux ausgeführt werden.

[Breite=601, Höhe=275]

Erfahren Sie mehr über SnapCenter -Backup und -Wiederherstellung für SAP HANA.

SnapCenter bietet umfassende Backup- und Wiederherstellungsfunktionen für SAP HANA-Datenbanken mithilfe von speicherbasierten Snapshot-Kopien, automatisiertem Aufbewahrungsmanagement und Integration mit NetApp ONTAP, Azure NetApp Files und FSx für NetApp ONTAP. Die Lösung unterstützt anwendungskonsistente Datenbanksicherungen, den Schutz von Nicht-Datenvolumes, Blockintegritätsprüfungen und die Replikation auf Sekundärspeicher mittels SnapVault oder ANF-Backup.

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

- Backup-Vorgänge, Planung und Aufbewahrungsmanagement
- SAP HANA Daten-Backup mit Storage-basierten Snapshot Kopien
- Datensicherung ohne Datenvolumen mit speicherbasierten Snapshot-Kopien (z. B. /hana/shared)
- Datenbankblock-Integritätsprüfungsoperationen

    - Verwendung einer dateibasierten Datensicherung
    - mit dem SAP HANA hdbpersdiag-Tool
- Replikation der Snapshot-Sicherung an einen sekundären Sicherungsort
    - Verwendung von SnapVault/ SnapMirror
    - Sicherung mit Azure NetApp Files ANF
- Allgemeine Ordnung und Sauberkeit des SAP HANA Backup-Katalogs
    - für HANA-Datensicherungen (Snapshot und dateibasiert)
    - für HANA-Protokollsicherungen
- Restore- und Recovery-Vorgänge
    - Automatisiertes Restore und Recovery
    - Wiederherstellungsmaßnahmen für einzelne Mandanten

Die Datensicherung der Datenbank erfolgt durch SnapCenter in Kombination mit dem SnapCenter -Plug-in für SAP HANA. Das Plug-in löst einen internen SAP HANA-Datenbank-Snapshot aus, sodass die auf dem Speichersystem erstellten Snapshots auf einem anwendungskonsistenten Abbild der SAP HANA-Datenbank basieren.

SnapCenter ermöglicht die Replikation konsistenter Datenbankabbilder an einen sekundären Sicherungs- oder Notfallwiederherstellungsort mithilfe von SnapVault oder der SnapMirror-Funktion. Typischerweise werden für Backups auf dem primären und dem sekundären Speicher unterschiedliche Aufbewahrungsrichtlinien definiert. SnapCenter übernimmt die Aufbewahrung im primären Speicher, und ONTAP übernimmt die Aufbewahrung im sekundären Backup-Speicher.

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, speicherbasierte Snapshot-Backups mit einer wöchentlichen Konsistenzprüfung der Persistenzschicht zu kombinieren. Sie können die Blockkonsistenzprüfung innerhalb von SnapCenter entweder durch Ausführen einer dateibasierten Sicherung oder durch Ausführen des SAP hdbpersdiag-Tools durchführen.

Basierend auf Ihren konfigurierten Aufbewahrungsrichtlinien verwaltet SnapCenter die Verwaltung von Datendateisicherungen im primären Speicher, Protokolldateisicherungen und des SAP HANA-Sicherungskatalogs.

SnapCenter übernimmt die Aufbewahrung im Primärspeicher, während 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:

- Sicherungsvorgang:
    - Löst einen internen HANA-Datenbank-Snapshot aus, um ein anwendungskonsistentes Abbild auf der Persistenzschicht zu erhalten.
    - Erstellt eine speicherbasierte Snapshot-Sicherung des Datenvolumens

    - Schließt den internen HANA-Datenbank-Snapshot, bestätigt oder bricht den Sicherungsvorgang ab. Dieser Schritt registriert das Backup im HANA-Backup-Katalog.
- Kundenbindungsmanagement:
    - Löscht Speicher-Snapshot-Backups basierend auf der definierten Aufbewahrungsfrist.
    - Löscht Snapshots auf der Speicherebene
    - Löscht Einträge aus dem SAP HANA-Backup-Katalog
    - Löscht alle Protokollsicherungen, die älter als die älteste Datensicherung sind. Protokollsicherungen werden im Dateisystem und im SAP HANA-Sicherungskatalog gelöscht.

[Breite=601, Höhe=285]

Wenn eine sekundäre Datensicherung konfiguriert ist, entweder mit SnapVault/ SnapMirror oder mit ANF-Datensicherung, wird der auf dem primären Datenträger erstellte Snapshot auf den sekundären Datensicherungsspeicher repliziert. SnapCenter verwaltet den HANA-Backup-Katalog sowie die Aufbewahrung von Protokoll-Backups entsprechend der Verfügbarkeit sekundärer Backups.

[Breite=601, Höhe=278]

Erfahren Sie mehr über die von SnapCenter unterstützten Konfigurationen für SAP HANA.

SnapCenter unterstützt eine breite Palette von SAP HANA-Systemarchitekturen und Bereitstellungsszenarien auf On-Premise- und Cloud-Speicherplattformen. Erfahren Sie mehr über unterstützte SAP HANA-Konfigurationen, Plattformkombinationen, Speicherprotokolle und verfügbare Backup- und Wiederherstellungsvorgänge für jede Umgebung.

Unterstützte SAP HANA-Konfigurationen

SnapCenter unterstützt die folgenden HANA-Konfigurationen und -Funktionen:

- SAP HANA Einzelhostsysteme
- SAP HANA-Mehrhostsysteme
    - Erfordert eine zentrale Plug-in-Bereitstellung, wie in beschrieben. "Bereitstellungsoptionen für das SnapCenter -Plug-in für SAP HANA"Die
- SAP HANA MDC-Systeme
    - mit einem oder mit mehreren Mietern
- SAP HANA-Systeme mit mehreren Partitionen
- SAP HANA System Replication
- SAP HANA-Verschlüsselung (Daten, Protokolle, Backups)

Unterstützte Plattform- und Infrastrukturkonfigurationen

SnapCenter unterstützt die folgenden Kombinationen von Host-Plattformen, Dateisystemen und Speicherplattformen.

Hostplattform	SAP HANA Speicheranbindung und Dateisystem	Speicherplattform
VMware	In-Guest-NFS-Mounts	ONTAP AFF
VMware	FC-Datenspeicher mit VMFS + VM mit XFS mit oder ohne Linux LVM	ONTAP AFF oder ASA
KVM	In-Guest-NFS-Mounts	ONTAP AFF
Bare-Metal-Server	NFS-Mounts	ONTAP AFF
Bare-Metal-Server	FC SAN + und XFS mit oder ohne Linux LVM	ONTAP AFF oder ASA (*)
Azure-VM	NFS-Mounts	Azure NetApp Dateien
AWS EC2	NFS-Mounts	FSx für ONTAP

(*): ASA Unterstützung ist ab SnapCenter Version 6.2 verfügbar.

Die HANA- und Linux-Plug-ins sind nur für die Intel-CPU-Plattform verfügbar. Für Linux auf IBM Power muss eine zentrale HANA-Plug-in-Bereitstellung wie beschrieben eingerichtet werden in "Bereitstellungsoptionen für das SnapCenter -Plug-in für SAP HANA"Die

Unterstützte Funktionen und Vorgänge

Abkürzungserklärung

- VBSR: Volume-basiertes SnapRestore + Ein volume-basiertes SnapRestore versetzt das Volume in den Zustand des Snapshots zurück.
- SFSR: Single file SnapRestore + Mit Single file SnapRestore können bestimmte Dateien oder LUNs innerhalb eines Volumes wiederhergestellt werden.

Siehe auch "Arten von Wiederherstellungsvorgängen für automatisch erkannte SAP HANA-Datenbanken"

ONTAP AFF und FSx für ONTAP

Nur Spalte 1 (NFS-Mounts) der folgenden Tabelle ist für FSx für ONTAP relevant.

Betrieb	NFS-Mounts auf Bare-Metal-Systemen oder in Gastsystemen mit VMware oder KVM	FC SAN + Bare Metal	FC-Datenspeicher VMware VMFS
Snapshot-Backup- und Wiederherstellungsvorgänge für die HANA-Datenbank			
Snapshot-Backup	Ja.	Ja.	Ja.
Manipulationssichere Momentaufnahme	Ja.	Ja.	Ja.
Vollständige Wiederherstellung	VBSR oder SFSR (auswählbar)	SFSR der vollständigen LUN	Klonen, einbinden, kopieren

Betrieb	NFS-Mounts auf Bare-Metal-Systemen oder in Gastsystemen mit VMware oder KVM	FC SAN + Bare Metal	FC-Datenspeicher VMware VMFS
Wiederherstellung für Einzelmandanten	SFSR	Klonen, einbinden, kopieren	Klonen, einbinden, kopieren
* SnapVault -Sicherungs- und Wiederherstellungsvorgänge für HANA-Datenbanken*			
SnapVault Replizierung	Ja.	Ja.	Ja.
Manipulationssichere Momentaufnahme	Ja.	Ja.	Ja.
Vollständige Wiederherstellung	Ja.	Ja.	Klonen, einbinden, kopieren
Wiederherstellung für Einzelmandanten	Ja.	Klonen, einbinden, kopieren	Klonen, einbinden, kopieren
HANA-Wiederherstellungsvorgang vom primären Snapshot- oder SnapVault -Ziel			
Automatisierte Wiederherstellung MDC Einzelmandant	Ja.	Ja.	Ja.
Automatisierte Wiederherstellung MDC für mehrere Mandanten	Nein	Nein	Nein
Sichern und Wiederherstellen von Nicht-Datenvolumes			
Snapshot-Backup	Ja.	Ja.	Ja (*)
Wiederherstellen aus Snapshot	VBSR oder SFSR (auswählbar)	SFSR der vollständigen LUN	VBSR (*)
SnapVault Replizierung	Ja.	Ja.	Ja (*)
Wiederherstellung aus SnapVault -Ziel	Ja.	Ja.	Ja (*)
SAP-Systemaktualisierung			
Aus dem primären Snapshot	Ja.	Ja (**)	Ja (**)
Vom SnapVault -Ziel	Ja.	Ja (**)	Ja (**)
HA und DR			
HSR unterstützt Snapshots und SnapVault.	Ja.	Ja.	Ja.
SnapMirror -Replikationsaktualisierungen mit SC	Ja.	Ja.	Ja.
SnapMirror aktive Synchronisierung	NA	Ja.	Ja.

(*): Keine VMware-Integration – Snapshot des Absturzabbilds und vollständige Wiederherstellung des Volumes

(**): Für SnapCenter Versionen < 6.2 sind Workarounds erforderlich.

ONTAP ASA

Betrieb	FC SAN + Bare Metal (*)	FC-Datenspeicher VMware VMFS
Snapshot-Backup- und Wiederherstellungsvorgänge für die HANA-Datenbank		
Snapshot-Backup	Ja.	Ja.
Manipulationssichere Momentaufnahme	Nein	Nein
Vollständige Wiederherstellung	SFSR der vollständigen LUN	Klonen, einbinden, kopieren
Wiederherstellung für Einzelmandanten	Klonen, einbinden, kopieren	Klonen, einbinden, kopieren
* SnapVault -Sicherungs- und Wiederherstellungsvorgänge für HANA-Datenbanken*		
SnapVault Replizierung	Ja.	Ja.
Manipulationssichere Momentaufnahme	Nein	Nein
Vollständige Wiederherstellung	Ja.	Klonen, einbinden, kopieren
Wiederherstellung für Einzelmandanten	Klonen, einbinden, kopieren	Klonen, einbinden, kopieren
HANA-Wiederherstellungsvorgang vom primären Snapshot- oder SnapVault -Ziel		
Automatisierte Wiederherstellung MDC Einzelmandant	Ja.	Ja.
Automatisierte Wiederherstellung MDC für mehrere Mandanten	Nein	Nein
Sichern und Wiederherstellen von Nicht-Datenvolumes		
Snapshot-Backup	Ja (*)	Ja (*)
Wiederherstellen aus Snapshot	SFSR der gesamten LUN (*)	SFSR der gesamten LUN (*)
SnapVault Replizierung	Ja (*)	Ja (*)
Wiederherstellung aus SnapVault -Ziel	Ja (*)	Ja (*)
SAP-Systemaktualisierung		
Aus dem primären Snapshot	Ja (**)	Ja (**)
Vom SnapVault -Ziel	Ja (**)	Ja (**)
HA und DR		
HSR unterstützt Snapshots und SnapVault.	Ja.	Ja.
SnapMirror -Replikationsaktualisierungen, die von SnapCenter ausgelöst werden	Ja.	Ja.
SnapMirror aktive Synchronisierung	Ja.	Ja.

(*): Unterstützung ab SnapCenter Version 6.2

(**): Für SnapCenter Versionen < 6.2 sind Workarounds erforderlich.

Azure NetApp Dateien

Betrieb	NFS-Mounts
Snapshot-Backup- und Wiederherstellungsvorgänge für die HANA-Datenbank	
Snapshot-Backup	Ja.
Manipulationssichere Momentaufnahme	Nein
Vollständige Wiederherstellung vor Ort	Lautstärke zurücksetzen oder SFSR (auswählbar)
Wiederherstellung für Einzelmandanten	SFSR
ANF-Sicherungs- und Wiederherstellungsvorgänge für HANA-Datenbanken	
ANF-Backup-Replikation	Ja.
Manipulationssichere Momentaufnahme	Nein
Vollständige Wiederherstellung vor Ort	Ja.
Wiederherstellung für Einzelmandanten	Ja.
HANA-Wiederherstellungsvorgang aus dem primären Snapshot oder ANF-Backup	
Automatisierte Wiederherstellung MDC Einzelmandant	Ja.
Automatisierte Wiederherstellung MDC für mehrere Mandanten	Nein
Sichern und Wiederherstellen von Nicht-Datenvolumes	
Snapshot-Backup	Ja.
Wiederherstellen aus Snapshot	Lautstärke zurücksetzen
ANF-Backup-Replikation	Ja.
Vollständige Wiederherstellung direkt aus dem ANF-Backup	NEIN (*)
SAP-Systemaktualisierung	
Aus dem primären Snapshot	Ja.
Aus dem ANF-Backup	Ja.
HA und DR	
HSR unterstützt Snapshots und ANF-Backups.	Ja.
Regionsübergreifende Replikationsaktualisierung, ausgelöst durch SnapCenter	Nein

(*): Bei der aktuellen Version muss eine Wiederherstellung über das Azure-Portal oder die Azure CLI durchgeführt werden.

Erfahren Sie mehr über die Datenschutzkonzepte und Best Practices von SnapCenter.

Erfahren Sie mehr über die Bereitstellungsoptionen von SnapCenter , Strategien zum Datenschutz und die Verwaltung der Backup-Aufbewahrung für SAP HANA-Umgebungen. SnapCenter unterstützt die Bereitstellung von Plug-ins auf Datenbank-Hosts oder zentralen Hosts, die automatische Erkennung und manuelle Konfiguration, Konsistenzprüfungen von Blöcken mithilfe dateibasierter Backups oder hdbpersdiag sowie ein umfassendes Aufbewahrungsmanagement über primären und sekundären Speicher hinweg.

Bereitstellungsoptionen für das SnapCenter -Plug-in für SAP HANA

Die folgende Abbildung zeigt die logische Sicht der Kommunikation zwischen dem SnapCenter -Server, der SAP HANA-Datenbank und dem Speichersystem. Der SnapCenter -Server nutzt die HANA- und Linux-Plug-ins zur Kommunikation mit der HANA-Datenbank und den Linux-Betriebssystemen.

[Breite=601, Höhe=199]

Die empfohlene und standardmäßige Bereitstellungsoption für die SnapCenter -Plug-ins ist die Installation auf dem HANA-Datenbankhost. Bei dieser Bereitstellungsoption sind alle im Kapitel „Von SnapCenter unterstützte Konfigurationen“ beschriebenen Konfigurationen und Funktionen gültig. Es gibt einige Ausnahmen, bei denen die SnapCenter -Plug-ins nicht auf dem HANA-Datenbankhost installiert werden können, sondern auf einem zentralen Plug-in-Host konfiguriert werden müssen, bei dem es sich beispielsweise um den SnapCenter -Server selbst handeln kann. Für HANA-Mehrhostsysteme oder HANA-Systeme, die auf der IBM Power-Plattform laufen, ist ein zentraler Plug-in-Host erforderlich. Beide Bereitstellungsoptionen können auch kombiniert werden, z. B. durch die Verwendung des SnapCenter -Servers als zentralen Plug-in-Host für ein System mit mehreren Hosts und die Bereitstellung der Plug-ins auf den HANA-Datenbankhosts für alle anderen HANA-Systeme mit einem einzelnen Host.

In SnapCenter kann eine HANA-Ressource entweder automatisch erkannt oder manuell konfiguriert werden. Ein HANA-System wird standardmäßig automatisch erkannt, sobald die HANA- und Linux-Plug-ins auf dem Datenbankhost bereitgestellt sind. Die automatische Erkennung SnapCenter unterstützt keine mehreren HANA-Installationen auf demselben Host. HANA-Systeme, die über einen zentralen Plug-in-Host verwaltet werden, müssen in SnapCenter manuell konfiguriert werden. Auch Nicht-Datenvolumes sind standardmäßig manuell konfigurierte Ressourcen.

	Plug-in bereitgestellt am	SnapCenter Ressource
HANA-Datenbank	Datenbankhost	Automatisch erkannt
HANA-Datenbank	Zentraler Plug-in-Host	Manuell konfiguriert
Nicht-Datenvolumen	K. A.	Manuell konfiguriert

SnapCenter unterstützt zwar die zentrale Bereitstellung von Plug-ins für HANA-Systeme, es gibt jedoch Einschränkungen hinsichtlich Plattform- und Funktionsunterstützung. Die folgenden Infrastrukturkonfigurationen und -vorgänge werden für HANA-Systeme, die mit einem zentralen Plug-in-Host konfiguriert sind, nicht unterstützt:

- VMware mit FC-Datenspeichern
- SnapMirror aktive Synchronisierung
- SnapCenter Server hohe Verfügbarkeit bei Verwendung als zentraler Plug-in-Host

- Automatische Erkennung von HANA-Systemen
- Automatisierte Wiederherstellung der HANA-Datenbank
- Automatisierte SAP-Systemaktualisierung
- Wiederherstellung für Einzelmandanten

SnapCenter Plug-in für HANA, bereitgestellt auf dem SAP HANA-Datenbankhost

Der SnapCenter Server kommuniziert über das HANA-Plug-in mit den HANA-Datenbanken. Das HANA-Plug-in verwendet die HANA hdbsql-Clientsoftware, um SQL-Befehle an die HANA-Datenbanken auszuführen. Der HANA hdb-Benutzerspeicher dient zur Bereitstellung der Benutzeranmeldeinformationen, des Hostnamens und der Portinformationen für den Zugriff auf die HANA-Datenbanken. Das SnapCenter Linux-Plug-in dient zur Abdeckung aller Host-Dateisystemoperationen sowie zur automatischen Erkennung von Dateisystem- und Speicherressourcen.

Wenn das HANA-Plug-in auf dem HANA-Datenbankhost bereitgestellt wird, wird das HANA-System von SnapCenter automatisch erkannt und in SnapCenter als automatisch erkannte Ressource gekennzeichnet.

[Breite=601, Höhe=304]

Hochverfügbarkeit mit SnapCenter Server

SnapCenter kann in einer HA-Konfiguration mit zwei Knoten eingerichtet werden. Bei einer solchen Konfiguration wird ein Load Balancer (z. B. F5) verwendet, um auf die SnapCenter -Hosts zuzugreifen. 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. Weitere Details zu SnapCenter HA finden Sie unter "Konfigurieren Sie SnapCenter -Server für hohe Verfügbarkeit"Die

[Breite=601, Höhe=307]

Zentraler Plug-in-Host

Wie im vorangegangenen Kapitel bereits erläutert, ist ein zentrales Plug-in erforderlich für

- HANA-Mehrhostsysteme
- HANA-Systeme, die auf IBM Power laufen

Bei Verwendung eines zentralen Plug-in-Hosts müssen das HANA-Plug-in und der SAP HANA hdbsql-Client auf einem Host außerhalb der HANA-Datenbankhosts installiert werden. Bei diesem Host kann es sich um einen beliebigen Windows- oder Linux-Host handeln, beispielsweise den SnapCenter -Server.

> Wenn Sie Ihren SnapCenter -Server unter Windows betreiben, können Sie Ihr Windows-System als zentralen Plug-in-Host verwenden. Wenn Sie Ihren SnapCenter -Server unter Linux betreiben, müssen Sie einen anderen Host als zentralen Plug-in-Host verwenden.

Bei einem HANA-Mehrhostsystem müssen die SAP HANA-Benutzerspeicherschlüssel für alle Worker- und Standby-Hosts auf dem zentralen Plug-in-Host konfiguriert werden. SnapCenter versucht, mit jedem der bereitgestellten Schlüssel eine Verbindung zur Datenbank herzustellen und kann daher unabhängig von einem Failover der Systemdatenbank (HANA-Namensserver) auf einen anderen Host funktionieren.

[Breite=601, Höhe=314]

Bei mehreren HANA-Systemen auf einem einzigen Host, die von einem zentralen Plug-in-Host verwaltet werden, müssen alle individuellen SAP HANA-Benutzerspeicherschlüssel der HANA-Systeme auf dem zentralen Plug-in-Host konfiguriert werden.

[Breite=601, Höhe=338]

SAP HANA Blockkonsistenzprüfung

SAP empfiehlt, regelmäßige HANA-Blockkonsistenzprüfungen in die gesamte Backup-Strategie aufzunehmen. Bei herkömmlichen dateibasierten Backups wird diese Prüfung bei jedem Backup-Vorgang durchgeführt. Bei Snapshot-Backups muss zusätzlich zu den Snapshot-Backup-Operationen auch die Konsistenzprüfung durchgeführt werden, zum Beispiel einmal pro Woche.

Technisch gesehen gibt es zwei Möglichkeiten, die Blockkonsistenzprüfung durchzuführen.

- Ausführen einer standardmäßigen dateibasierten oder backint-basierten Datensicherung
- Ausführung des HANA-Tools hdbpersdiag, siehe auch "Konsistenzprüfung der Persistenz | SAP-Hilfeportal"

Das HANA-Tool hdbpersdiag ist Bestandteil der HANA-Installation und ermöglicht die Durchführung von Blockkonsistenzprüfungen an einer Offline-HANA-Datenbank. Daher eignet es sich perfekt für die Verwendung in Kombination mit Snapshot-Backups, bei denen vorhandene Snapshot-Backups hdbpersdiag präsentiert werden können.

Beim Vergleich der beiden Ansätze bietet hdbpersdiag deutliche Vorteile gegenüber der dateibasierten Sicherung für HANA-Blockkonsistenzprüfungen. Eine Dimension ist die benötigte Speicherkapazität. Bei dateibasierten Backups muss mindestens die Größe eines Backups für jedes HANA-System verfügbar sein. Wenn Sie beispielsweise 15 HANA-Systeme mit einer Persistenzgröße von 3 TB haben, benötigen Sie zusätzlich 45 TB allein für die Konsistenzprüfungen. Für hdbpersdiag wird keine zusätzliche Speicherkapazität benötigt, da der Vorgang auf einem vorhandenen Snapshot-Backup oder einem FlexClone eines vorhandenen Snapshot-Backups ausgeführt wird. Die zweite Dimension ist die CPU-Auslastung des HANA-Hosts während der Konsistenzprüfung. Eine dateibasierte Datensicherung benötigt CPU-Zyklen auf dem HANA-Datenbankhost, während die hdbpersdiag-Verarbeitung vollständig vom HANA-Host ausgelagert werden kann, wenn sie in Kombination mit einem zentralen Verifizierungshost verwendet wird. Die wichtigsten Merkmale sind in der folgenden Tabelle zusammengefasst.

	Erforderliche Speicherkapazität	CPU- und Netzwerklast auf dem HANA-Host
Dateibasierte Datensicherung	Minimale Datensicherungsgröße 1 x für jedes HANA-System	Hoch
hdbpersdiag verwendet das Snapshot-Verzeichnis auf dem HANA-Host (nur NFS)	Keine	Medium
Zentraler Verifizierungshost, der hdbpersdiag mit FlexClone -Volumes ausführt	Keine	Keine

NetApp empfiehlt die Verwendung von hdbpersdiag zur Durchführung von HANA-Blockkonsistenzprüfungen. Weitere Einzelheiten zur Umsetzung finden sich in Kapitel "Blockkonsistenzprüfungen mit SnapCenter"Die

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?
- Sollen die primären Backups auf einen sekundären Backup-Standort repliziert werden?
- Wie lange sollten die Backups auf dem sekundären Backup-Speicher aufbewahrt werden?

Die folgende Tabelle zeigt ein Beispiel für Datenschutzparameter für die Systemtypen Produktion, Entwicklung und Test. Für das Produktionssystem wurde eine hohe Backup-Frequenz festgelegt, und die Backups werden einmal täglich auf einen sekundären Backup-Standort repliziert. Die Testsysteme haben geringere Anforderungen und es findet keine Replikation der Backups statt.

Parameter	Produktionssysteme auszuführen	Entwicklungssysteme	Testsysteme
Sicherungshäufigkeit	Alle 6 Stunden	Alle 6 Stunden	Alle 12 Stunden
Primäre Aufbewahrung	3 Tage	3 Tage	6 Tage
Block-Integritätsprüfung	Einmal in der Woche	Einmal in der Woche	Nein
Replikation auf sekundären Backup-Standort	Einmal am Tag	Einmal am Tag	Nein
Aufbewahrung der sekundären Datensicherung	2 Wochen	2 Wochen	Nein

Die folgende Tabelle zeigt die Richtlinien und Zeitpläne, die für die oben genannten Datenschutzparameter konfiguriert werden müssten.

Politik	Backup-Typ	Zeitplanhäufigkeit	Primäre Aufbewahrung	SnapVault Replizierung	Sekundäre Retention
LocalSnap	Auf Snapshot-Basis	Alle 6 Stunden	Anzahl=12	Nein	NA
LocalSnap und SnapVault	Auf Snapshot-Basis	Einmal am Tag	Anzahl=2	Ja.	Anzahl=14
SnapAndCallHdbpersdiag	Auf Snapshot-Basis	Einmal in der Woche	Anzahl=2	Nein	NA

Für ONTAP Systeme oder FSx für ONTAP muss in ONTAP eine Datensicherungsbeziehung für die SnapVault Replikation konfiguriert werden, bevor SnapCenter SnapVault Aktualisierungsvorgänge ausführen kann. Die sekundäre Aufbewahrung ist in der ONTAP Schutzrichtlinie definiert.

Für die ANF-Sicherung ist keine zusätzliche Konfiguration außerhalb von SnapCenter erforderlich. Die sekundäre Aufbewahrung der ANF-Backups wird von SnapCenter verwaltet.

In dieser Beispielkonfiguration wird hdbpersdiag für die Blockintegritätsprüfung verwendet. Weitere Einzelheiten finden Sie in Kapitel "Blockkonsistenzprüfungen mit SnapCenter"Die

Die folgende Abbildung fasst die Zeitpläne und die Aufbewahrungsfristen der Backups zusammen. Wird SnapCenter zur Verwaltung der Aufbewahrung von Protokollsicherungen verwendet, werden alle Protokollsicherungen gelöscht, die älter als die älteste Snapshot-Sicherung sind. Mit anderen Worten: Protokollsicherungen werden so lange aufbewahrt, wie es erforderlich ist, um für jede verfügbare Sicherung eine zeitgerechte Wiederherstellung auf den aktuellen Stand zu ermöglichen.

[Breite=601, Höhe=192]

Sicherung der Verschlüsselungs-Root-Schlüssel

Bei Verwendung der HANA-Persistenzverschlüsselung ist es unerlässlich, zusätzlich zu den Standard-Datensicherungen auch Sicherungskopien der Stammschlüssel zu erstellen. Zur Wiederherstellung der HANA-Datenbank im Falle eines Datenverlusts und des Verlusts des HANA-Installationsdateisystems werden Root-Key-Backups benötigt. Weitere Informationen finden Sie unter "SAP HANA Administration Guide"Die

Beachten Sie, dass, wenn ein Stammschlüssel geändert wird, der neue Stammschlüssel nicht zur Wiederherstellung alter HANA-Datenbanksicherungen verwendet werden kann, die zuvor erstellt wurden. Sie benötigen stets den Stammschlüssel, der zum Zeitpunkt der Erstellung des Backups aktiv war.

Backup-Vorgänge

SnapCenter unterstützt Snapshot-Backup-Operationen von HANA MDC-Systemen mit einem oder mehreren Mandanten. SnapCenter unterstützt außerdem zwei verschiedene Wiederherstellungsvorgänge eines HANA MDC-Systems. Sie können entweder das gesamte System, die Systemdatenbank und alle Mandanten wiederherstellen oder nur einen Mandanten. Es gibt einige Voraussetzungen, damit SnapCenter diese Operationen ausführen kann.

In einem MDC-System ist die Mandantenkonfiguration nicht unbedingt statisch. Mieter können hinzugefügt oder gelöscht werden. SnapCenter kann sich nicht auf die Konfiguration verlassen, die beim Hinzufügen der HANA-Datenbank zu SnapCenter ermittelt wird. Um eine Wiederherstellung für einen einzelnen Mandanten zu ermöglichen, muss SnapCenter wissen, welche Mandanten in den einzelnen Snapshot-Backups enthalten sind. Darüber hinaus muss es wissen, welche Dateien und Verzeichnisse zu jedem Mandanten gehören, der in der Snapshot-Sicherung enthalten ist.

Daher ermittelt SnapCenter bei jedem Backup-Vorgang die Mandanteninformationen. Dies umfasst die Mandantennamen und die entsprechenden Datei- und Verzeichnisinformationen. Diese Daten müssen in den Snapshot-Backup-Metadaten gespeichert werden, um eine Wiederherstellung durch einen einzelnen Mandanten zu ermöglichen.

Ein weiterer Schritt der automatischen Anwendungserkennung ist die Erkennung des primären oder

sekundären Knotens der HANA-Systemreplikation (HSR). Wenn ein HANA-System mit HSR konfiguriert ist, muss SnapCenter bei jedem Sicherungsvorgang den primären Knoten identifizieren, damit die Backup-SQL-Befehle auf dem primären HSR-Knoten ausgeführt werden. Siehe auch "SAP HANA System Replication – Backup und Recovery mit SnapCenter"Die

SnapCenter erkennt außerdem die HANA-Datenvolumenkonfiguration und ordnet sie Dateisystem- und Speicherressourcen zu. Mit diesem Ansatz kann SnapCenter Änderungen an der HANA-Volume-Konfiguration verarbeiten, z. B. mehrere Partitionen oder Änderungen an der Speicherkonfiguration wie die Migration von Volumes.

Der nächste Schritt ist die eigentliche Snapshot-Sicherungsoperation. Dieser Schritt umfasst den SQL-Befehl zum Auslösen des HANA-Datenbank-Snapshots, die Sicherung des Speicher-Snapshots und den SQL-Befehl zum Beenden des HANA-Snapshot-Vorgangs. Durch die Verwendung des Befehls „close“ aktualisiert die HANA-Datenbank den Sicherungskatalog der Systemdatenbank und jedes 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.

[Breite=601, Höhe=237]

Backup-Aufbewahrungsverwaltung

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
- Datensicherungen auf dem Sekundärspeicher (SnapVault oder ANF-Backup)
- Daten-Backups im SAP HANA Backup-Katalog
- Protokollsicherungen im SAP HANA-Sicherungskatalog und im Dateisystem

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.

[Breite=601, Höhe=309]

Aufbewahrungsmanagement von lokalen Backups auf dem Primärstorage

SnapCenter übernimmt die Verwaltung von SAP HANA-Datenbanksicherungen und Nicht-Datenvolumensicherungen, indem es Snapshot-Kopien auf dem primären Speicher und im SnapCenter Repository gemäß einer in der SnapCenter -Sicherungsrichtlinie definierten Aufbewahrungsfrist löscht. Die Aufbewahrungsverwaltung ist in jedem Backup-Workflow von SnapCenter enthalten. Lokale Backups auf dem primären Speicher können auch manuell in SnapCenter gelöscht werden.

Aufbewahrungsmanagement von dateibasierten Backups

SnapCenter übernimmt die Verwaltung dateibasierter Backups, indem es die Backups im Dateisystem gemäß einer in der SnapCenter -Backup-Richtlinie definierten Aufbewahrungsfrist löscht. Die Aufbewahrungslogik wird bei jedem Backup-Workflow in SnapCenter ausgeführt.

Aufbewahrungsverwaltung von Backups im Sekundärspeicher (SnapVault)

Die Aufbewahrungsverwaltung der Backups im Sekundärspeicher (SnapVault) wird von ONTAP auf Basis der in der ONTAP Schutzbeziehung definierten Aufbewahrungsfristen übernommen. Um diese Änderungen auf dem Sekundärspeicher im SnapCenter -Repository zu synchronisieren, verwendet SnapCenter einen geplanten Bereinigungsjob. Dieser Bereinigungsvorgang synchronisiert alle Backups des Sekundärspeichers mit dem SnapCenter Repository für alle SnapCenter -Plug-ins und alle Ressourcen.

Die Bereinigung erfolgt standardmäßig einmal pro Woche. Dieser wöchentliche Zeitplan führt zu einer Verzögerung beim Löschen von Backups in SnapCenter und SAP HANA Studio im Vergleich zu den Backups, die bereits im Sekundärspeicher gelöscht wurden. Um diese Unstimmigkeit zu vermeiden, können Kunden den Zeitplan auf eine höhere Frequenz ändern, zum Beispiel einmal täglich. Einzelheiten zur Anpassung des Zeitplans des Bereinigungsauftrags oder zum Auslösen einer manuellen Aktualisierung finden Sie im entsprechenden Kapitel. "Bereinigung sekundärer Backups"Die

Aufbewahrungsverwaltung von Backups auf dem Sekundärspeicher (ANF-Backup)

Die Aufbewahrung von ANF-Backups wird von SnapCenter konfiguriert und verwaltet. SnapCenter übernimmt die Verwaltung der ANF-Backup-Backups, indem es die Backups gemäß einer in der SnapCenter -Backup -Richtlinie definierten Aufbewahrungsfrist löscht. Die Aufbewahrungsverwaltung ist in jedem Backup-Workflow von SnapCenter enthalten.

Aufbewahrungsmanagement von Daten-Backups im SAP HANA Backup-Katalog

Wenn SnapCenter eine Sicherung, einen lokalen Snapshot oder eine dateibasierte Sicherung gelöscht hat oder wenn SnapCenter eine Löschung einer Sicherung auf dem Sekundärspeicher festgestellt hat, wird diese Datensicherung auch im SAP HANA-Sicherungskatalog gelöscht. Bevor SnapCenter den SAP HANA-Katalogeintrag für ein lokales Snapshot-Backup im primären Speicher löscht, prüft es, ob das Backup im sekundären Speicher noch vorhanden ist.

Aufbewahrungsmanagement von Protokoll-Backups

Die SAP HANA-Datenbank erstellt automatisch Log-Backups. Diese Vorgänge erstellen Sicherungsdateien für jeden einzelnen SAP HANA-Dienst in einem in SAP HANA konfigurierten Sicherungsverzeichnis. Protokollsicherungen, die älter als die letzte Datensicherung sind, werden für die zukünftige Wiederherstellung nicht mehr benötigt und können daher gelöscht werden. SnapCenter übernimmt die Verwaltung der Logdateisicherungen sowohl auf Dateisystemebene als auch im SAP HANA-Sicherungskatalog durch die Ausführung der folgenden Schritte:

1. SnapCenter liest den SAP HANA-Backup-Katalog, um die Backup-ID des ältesten erfolgreichen Daten-Backups zu ermitteln.
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 in der Richtlinienkonfiguration eine Aufbewahrungsdauer für On-Demand-Backups definiert ist, wird die Aufräumarbeit nur dann durchgeführt, wenn ein weiteres On-Demand-Backup ausgeführt wird. Daher müssen On-Demand-Backups in SnapCenter in der Regel manuell gelöscht werden, um sicherzustellen, dass diese Backups auch im SAP HANA-Backup-Katalog gelöscht werden und die Protokoll-Backup-Bereinigung nicht auf einem alten On-Demand-Backup basiert.

Die Aufbewahrungsverwaltung für Protokollsicherungen ist standardmäßig aktiviert. Bei Bedarf kann diese Funktion wie im Abschnitt „Automatische Protokollsicherungsverwaltung deaktivieren“ beschrieben deaktiviert werden.

Erfahren Sie mehr über die Konfiguration von SnapCenter für SAP HANA-Umgebungen

Konfigurieren Sie SnapCenter für SAP HANA-Umgebungen mit einem zweiphasigen Ansatz: Erstkonfiguration für gemeinsam genutzte Ressourcen (Anmeldeinformationen, Speichersysteme und Richtlinien) und ressourcenspezifische Konfiguration für einzelne HANA-Systeme (Hostbereitstellung, automatische Erkennung und Schutzeinstellungen).

Die SnapCenter -Konfiguration für eine SAP-HANA-Umgebung mit mehreren HANA-Systemen lässt sich in zwei Hauptbereiche unterteilen:

- Die Ausgangskonfiguration
  - Anmeldeinformationen, Speicher und Richtlinienkonfigurationen. + Diese Einstellungen oder Ressourcen werden typischerweise von mehreren HANA-Systemen genutzt.
- Die HANA-ressourcenspezifische Konfiguration
  - Die Konfiguration von Host, HANA und Ressourcenschutz muss für jedes HANA-System einzeln erfolgen.

Die folgende Abbildung veranschaulicht die verschiedenen Konfigurationskomponenten und ihre Abhängigkeiten.

Alle Konfigurationsschritte werden in den folgenden Abschnitten detailliert beschrieben.

Die Beschreibungen und Screenshots in diesem Dokument basieren auf von SnapCenter automatisch erkannten HANA-Systemen. Zusätzliche oder abweichende Konfigurationsschritte für manuell konfigurierte Ressourcen mit einem zentralen Plug-in-Host werden beschrieben in "Zentrale Plug-in-Host-Konfiguration"Die

[Breite=601, Höhe=319]

Konfigurieren Sie die anfänglichen SnapCenter -Einstellungen für SAP HANA

Konfigurieren Sie die ersten SnapCenter -Einstellungen für SAP HANA-Umgebungen, indem Sie Anmeldeinformationen für Azure-Dienstprinzipale einrichten, Speichersysteme hinzufügen und Richtlinien für Snapshot-Backups, Blockintegritätsprüfungen und sekundäre Replikation erstellen.

Die Erstkonfiguration von SnapCenter umfasst die folgenden Schritte:

1. Konfiguration von Anmeldeinformationen
   a. Bei HANA-Systemen, die mit Azure NetApp Files (ANF) konfiguriert sind, muss ein Dienstprinzipal vorbereitet und anschließend in SnapCenter konfiguriert werden.
   b. Für die automatisierte Installation des HANA-Plug-ins auf den HANA-Datenbankhosts müssen Host-Zugangsdaten angegeben werden.
2. Konfiguration des Storage-Systems
   a. Bei HANA-Systemen, die mit ANF konfiguriert sind, können die erforderlichen NetApp -Konten ausgewählt und der SnapCenter -Konfiguration hinzugefügt werden.
   b. Für ONTAP oder FSx for ONTAP Speichersysteme können entweder SVMs oder der komplette Speichercluster zu SnapCenter hinzugefügt werden.
3. Konfiguration von Richtlinien
   a. Richtlinien für Snapshot-basierte Backups sowie für Blockintegritätsprüfungen können sowohl für ANF als auch für ONTAP und FSx for ONTAP Speichersysteme konfiguriert werden.
   b. Richtlinien für manipulationssichere Snapshots und sekundäre Backups mit SnapVault oder SnapMirror können nur für ONTAP und FSx for ONTAP Speichersysteme konfiguriert werden.
   c. Für HANA-Systeme, die mit ANF konfiguriert sind, kann eine Richtlinie Folgendes umfassen: "ANF-Backup"Die

> Die gleichen Snapshot-Backup-Richtlinien können sowohl für HANA-Datenbanken als auch für Nicht-Datenvolumes, z. B. das HANA Shared Volume, verwendet werden.

Die folgende Abbildung fasst die Konfigurationsabschnitte zusammen.

[Breite=601, Höhe=158]

Die folgenden Kapitel beschreiben die ersten Konfigurationsschritte.

Konfiguration von Anmeldeinformationen

Anmeldeinformationen für die HANA-Plug-in-Bereitstellung

Die Anmeldeinformationen werden im Abschnitt „Einstellungen“ und durch Auswahl der Registerkarte „Anmeldeinformationen“ konfiguriert. Anmeldeinformationen können durch Klicken auf das +-Symbol hinzugefügt werden.

[Breite=601, Höhe=118]

NetApp empfiehlt, auf allen HANA-Datenbankhosts einen Benutzer (z. B. scuser) zu konfigurieren und die sudo-Berechtigungen wie beschrieben einzurichten. "Voraussetzungen für das Hinzufügen von Hosts und die Installation des SnapCenter -Plug-ins für die SAP HANA-Datenbank"Die

[Breite=287, Höhe=247]

Anmeldeinformationen für Azure NetApp Files

Es muss ein Azure-Dienstprinzipal vorbereitet werden, der es SnapCenter ermöglicht, die erforderlichen Operationen für die ANF-Volumes auszuführen. Das folgende Beispiel zeigt die minimal erforderlichen Berechtigungen, die unbedingt enthalten sein müssen.

```
    "assignableScopes": [
        "/subscriptions/xxx"
    ],
    "createdBy": "xxx",
    "createdOn": "2025-05-07T07:12:14.451483+00:00",
    "description": "Restricted Access for SnapCenter ",
    "id":
"/subscriptions/xxx/providers/Microsoft.Authorization/roleDefinitions/xxx"
,
    "name": "xxx",
    "permissions": [
        {
            "actions": [
            "Microsoft.NetApp/register/action",
            "Microsoft.NetApp/unregister/action",
            "Microsoft.NetApp/netAppAccounts/read",
            "Microsoft.NetApp/netAppAccounts/getKeyVaultStatus/action",
            "Microsoft.NetApp/netAppAccounts/migrateEncryption/action",
            "Microsoft.NetApp/netAppAccounts/transitionToCmk/action",
            "Microsoft.NetApp/netAppAccounts/capacityPools/read",
            "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
            "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/revert/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/poolChange/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/finalizeRelocation/
action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/revertRelocation/ac
tion",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/breakFileLocks/acti
on",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/getGroupIdListForLd
```

```
apUser/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/backups/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/backups/restoreFile
s/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/delete",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/restoreFi
les/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/getMetad
ata/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/volumeQuotaRules/re
ad",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/latestRestoreStatus
/current/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/mountTargets/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/restoreStatus/read"
,
            "Microsoft.NetApp/netAppAccounts/snapshotPolicies/read",
            "Microsoft.NetApp/netAppAccounts/snapshotPolicies/write",

"Microsoft.NetApp/netAppAccounts/snapshotPolicies/listVolumes/read",

"Microsoft.NetApp/netAppAccounts/snapshotPolicies/volumes/read",
            "Microsoft.NetApp/netAppAccounts/volumeGroups/read",
            "Microsoft.NetApp/netAppAccounts/volumeGroups/write",
            "Microsoft.NetApp/locations/checknameavailability/action",
            "Microsoft.NetApp/locations/checkfilepathavailability/action",
            "Microsoft.NetApp/locations/operationresults/read",
            "Microsoft.NetApp/Operations/read",
            "Microsoft.Resources/resources/read",
```

```
            "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
            "Microsoft.Network/virtualNetworks/read",
            "Microsoft.Network/virtualNetworks/subnets/read",
            "Microsoft.Network/virtualNetworks/write",
            "Microsoft.Network/virtualNetworks/subnets/write",
            "Microsoft.NetApp/netAppAccounts/backupVaults/read",
            "Microsoft.NetApp/netAppAccounts/backupVaults/write",
            "Microsoft.NetApp/netAppAccounts/backupVaults/backups/read",
            "Microsoft.NetApp/netAppAccounts/backupVaults/backups/write",
            "Microsoft.NetApp/netAppAccounts/backupVaults/backups/delete",

"Microsoft.NetApp/netAppAccounts/backupVaults/backups/restoreFiles/action"
            ],
            "condition": null,
            "conditionVersion": null,
            "dataActions": [],
            "notActions": [],
            "notDataActions": []
        }
    ],
    "roleName": "SnapCenter-Restricted-Access",
    "roleType": "CustomRole",
    "type": "Microsoft.Authorization/roleDefinitions",
    "updatedBy": "xxx",
    "updatedOn": "2025-05-07T07:12:14.451483+00:00"
}
```

Die Anmeldeinformationen werden im Abschnitt „Einstellungen“ und durch Auswahl der Registerkarte „Anmeldeinformationen“ konfiguriert. Die Zugangsdaten werden durch Klicken auf das Plus-Symbol konfiguriert.

[Breite=601, Höhe=116]

Im folgenden Bildschirm muss ein Name für die Anmeldeinformationen angegeben und der Authentifizierungsmodus „Azure-Anmeldeinformationen“ ausgewählt werden. Anschließend müssen Mandanten-ID, Client-ID und Client-Geheimschlüssel konfiguriert werden.

[Breite=252, Höhe=246]

Konfiguration des Storage-Systems

ONTAP Systeme und FSx für ONTAP

Ein ONTAP System oder FSx für ONTAP kann zu SnapCenter hinzugefügt werden, indem entweder Cluster-Zugangsdaten oder Zugangsdaten für jede benötigte SVM angegeben werden. Wenn die Cluster-Zugangsdaten angegeben werden, werden alle SVMs des Clusters zu SnapCenter hinzugefügt.

In unserem Laboraufbau haben wir die Speichercluster zu SnapCenter hinzugefügt. ONTAP Cluster werden im Abschnitt „Speichersysteme“ konfiguriert, indem die Registerkarte „ONTAP -Speicher“ und der Clustertyp „ONTAP“ ausgewählt werden. Ein neuer Cluster wird durch Anklicken des Plus-Symbols hinzugefügt.

[Breite=601, Höhe=117]

Im folgenden Bildschirm müssen Sie die Anmeldeinformationen für einen Clusterbenutzer angeben.

> Der Cluster-Benutzer admin sollte nicht verwendet werden. Stattdessen sollte ein neuer Benutzer mit den erforderlichen Berechtigungen erstellt werden, wie in beschrieben. "Erstellen Sie ONTAP Clusterrollen mit minimalen Berechtigungen"Die für das ASA -System erforderlichen Berechtigungen finden Sie unter "Erstellen Sie ONTAP Clusterrollen für ASA R2-Systeme"Die

[Breite=299, Höhe=176]

SVMs werden im Abschnitt „Speichersysteme“ konfiguriert, indem die Registerkarte „ONTAP -Speicher“ und der Typ „ONTAP SVMS“ ausgewählt werden. Eine neue SVM wird durch Klicken auf das +-Symbol hinzugefügt.

Im folgenden Bildschirm müssen Sie die Anmeldeinformationen für einen Clusterbenutzer angeben.

> Der SVM-Benutzer vsadmin sollte nicht verwendet werden. Stattdessen sollte ein neuer Benutzer mit den erforderlichen Berechtigungen erstellt werden, wie in beschrieben. "Erstellen Sie SVM-Rollen mit minimalen Berechtigungen"Die für das ASA -System erforderlichen Berechtigungen finden Sie unter "Erstellen Sie SVM-Rollen für ASA R2-Systeme"Die

> Der DNS-Name für die SVM muss mit dem im ONTAP System konfigurierten SVM-Namen übereinstimmen.

[Breite=331, Höhe=199]

Azure NetApp Dateien

Nachdem die ANF-Zugangsdaten konfiguriert wurden, können ANF NetApp Konten zu SnapCenter hinzugefügt werden. NetApp Konten werden im Abschnitt „Speichersysteme“ und durch Auswahl der Registerkarte „Azure NetApp Files“ konfiguriert. Ein neues NetApp -Konto wird durch Klicken auf das Plus-Symbol hinzugefügt.

[Breite=601, Höhe=117]

Nach Auswahl der ANF-Anmeldeinformationen und des Abonnements kann ein NetApp -Konto zu SnapCenter hinzugefügt werden.

[Breite=401, Höhe=176]

Speicherkonfiguration bei Verwendung von SnapMirror ActiveSync

Spezifische Schritte zur Speicherkonfiguration werden beschrieben unter "Speicherkonfiguration mit SnapMirror ActiveSync"Die

Konfiguration von Richtlinien

Wie im Abschnitt „Datenschutzstrategie“ erläutert, werden Richtlinien in der Regel unabhängig von der Ressource konfiguriert und können für mehrere SAP HANA-Systeme verwendet werden.

Eine typische Minimalkonfiguration umfasst folgende Richtlinien:

- Richtlinie für stündliche Backups ohne Replikation
- Richtlinie für tägliche Backups mit SnapVault oder ANF-Backup-Replikation
- Richtlinie für die wöchentliche Überprüfung der Blockintegrität
  - Verwendung einer dateibasierten Datensicherung
  - mit dem HANA-Tool hdbpersdiag

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

Die Richtlinien werden im Abschnitt „Einstellungen“ und durch Auswahl der Registerkarte „Richtlinien“ konfiguriert. Eine neue Richtlinie wird durch Klicken auf das Plus-Symbol konfiguriert. Die beiden folgenden Screenshots zeigen die Liste der Richtlinien für HANA-Systeme, die mit Azure NetApp Files betrieben werden, sowie eine zweite Liste für HANA-Systeme, die mit ONTAP -Speichersystemen oder FSx für ONTAP betrieben werden.

[Breite=601, Höhe=133]

[Breite=601, Höhe=138]

Snapshot-Backups mit ONTAP -Systemen und FSx für ONTAP

Snapshot-Backup-Richtlinien für ONTAP Systeme oder FSx für ONTAP können einen lokalen Snapshot mit Replikations- oder Snapshot-Sperrvorgängen (manipulationssicherer Snapshot) kombinieren. Dieses Beispiel zeigt eine Richtlinie mit Replikation auf einen sekundären Speicher mithilfe von SnapVault.

Geben Sie einen Namen für die Versicherungspolice und optional eine Beschreibung an.

[Breite=376, Höhe=103]

Wählen Sie den ONTAP Speichertyp und den Snapshot-Richtlinienbereich aus.

[Breite=385, Höhe=97]

Für diese Richtlinie wurde ein täglicher Zeitplan konfiguriert. Es wird täglich ein Snapshot erstellt, und die Snapshot-Änderungen werden mithilfe von SnapVault auf den sekundären Speicher repliziert.

Der Zeitplan selbst ist mit der individuellen HANA-Ressourcenschutzkonfiguration konfiguriert.

Die in der Richtlinie konfigurierte Aufbewahrungsdauer gilt nur für die primären Snapshots. Die Aufbewahrung im SnapVault Ziel wird mit der ONTAP Replikationsbeziehung für die einzelnen Volumes der HANA-Datenbank konfiguriert, wie in Kapitel [Kapitelnummer einfügen] beschrieben. "SAP HANA Snapshot-Sicherungsvorgänge"Die Die in der Richtlinie konfigurierte Snapshot-Bezeichnung muss mit der in der ONTAP Replikationsbeziehung konfigurierten Bezeichnung übereinstimmen.

Die Snapshot-Sperre (manipulationssichere Snapshots) kann durch Anklicken der Kontrollkästchen und Festlegen des Sperrzeitraums aktiviert werden. Diese Funktion erfordert eine SnapLock -Lizenz auf dem Speichersystem und die Konfiguration der Compliance-Uhr.

Eine Richtlinie, die nur lokale Snapshots berücksichtigt, würde mit einem stündlichen Zeitplan und durch Deaktivierung des Kontrollkästchens „SnapVault aktualisieren“ konfiguriert.

[Breite=378, Höhe=352]

Die Übersichtsseite zeigt die konfigurierten Parameter an.

[Breite=385, Höhe=119]

Snapshot-Backups mit Azure NetApp Files

Die Snapshot-Sicherungsrichtlinien für Azure NetApp Files können einen lokalen Snapshot mit einer ANF-Sicherung kombinieren, die die Snapshot-Daten in Azure Blob repliziert. Dieses Beispiel zeigt eine Richtlinie, die für die Replikation mit ANF-Backup verwendet wird.

Geben Sie einen Namen für die Versicherungspolice und optional eine Beschreibung an.

[Breite=356, Höhe=95]

Wählen Sie den Speichertyp „Azure NetApp Files“ und den Richtlinienbereich für Snapshots aus.

[Breite=360, Höhe=102]

Für diese Richtlinie wurde ein täglicher Zeitplan konfiguriert. Es wird täglich ein Snapshot erstellt, und die Snapshot-Änderungen werden mithilfe von ANF Backup in den Backup-Tresor repliziert.

Der Zeitplan selbst ist mit der individuellen HANA-Ressourcenschutzkonfiguration konfiguriert.

Die in der Richtlinie konfigurierte Snapshot-Aufbewahrungsdauer gilt für die primären Snapshots auf dem ANF-Volume. Die Aufbewahrungsdauer für das ANF-Backup wird mit den Backup-Aufbewahrungseinstellungen konfiguriert.

Eine Richtlinie, die nur lokale Snapshots vorsieht, würde mit einem stündlichen Zeitplan und durch Deaktivierung des Kontrollkästchens „Backup aktivieren“ konfiguriert.

[Breite=373, Höhe=361]

Die Übersichtsseite zeigt die konfigurierten Parameter an.

[Breite=376, Höhe=138]

Blockintegritätsprüfungsvorgänge für alle Plattformen

HANA-Tool hdbpersdiag

Einzelheiten werden in Kapitel 1 beschrieben. "Blockkonsistenzprüfungen mit SnapCenter"Die

Dateibasierte Datensicherung

Geben Sie einen Namen für die Versicherungspolice und optional eine Beschreibung an.

[Breite=346, Höhe=95]

Wählen Sie je nach Ihrer Konfiguration den Speichertyp ONTAP oder Azure NetApp Files und anschließend den Richtlinienbereich „Dateibasiert“.

[Breite=357, Höhe=98]

Wie bereits besprochen, wird empfohlen, die Blockintegritätsprüfung einmal pro Woche durchzuführen. Daher wird ein Wochenplan gewählt.

Der Zeitplan selbst ist mit der individuellen HANA-Ressourcenschutzkonfiguration konfiguriert.

Das Dateisystem, in dem die dateibasierte Sicherung gespeichert wird, muss über ausreichend Kapazität für eine Sicherung mehr verfügen als in den Aufbewahrungseinstellungen definiert ist, da SnapCenter die alte Sicherung löscht, nachdem die neue erstellt wurde. In diesem Beispiel wird Speicherplatz für zwei Backups benötigt, wobei nur ein Backup aufbewahrt werden soll. Die minimale konfigurierbare Aufbewahrungsdauer beträgt null.

[Breite=351, Höhe=173]

Die Übersichtsseite zeigt die konfigurierten Parameter an.

[Breite=366, Höhe=101]

Richtlinienkonfiguration bei Verwendung von SnapMirror ActiveSync

Die einzelnen Schritte zur Richtlinienkonfiguration werden im Dokument beschrieben. "Richtlinienkonfiguration SnapMirror Active Sync"Die

SnapCenter Ressourcen für einzelne SAP HANA-Datenbanken konfigurieren

Konfigurieren Sie einzelne SAP HANA-Datenbanken in SnapCenter , indem Sie Backup-Benutzer und Benutzerspeicherschlüssel erstellen, die Speicherreplikation für sekundäre Backups einrichten, das HANA-Plug-in für die automatische Erkennung bereitstellen und den Ressourcenschutz mit Richtlinien und Zeitplänen konfigurieren.

Die Konfiguration einer HANA-Datenbank in SnapCenter erfolgt in folgenden Schritten:

1. In der HANA-Systemdatenbank muss ein SnapCenter Backup-Benutzer konfiguriert und auf dem HANA-Datenbankhost ein SAP-HANA-Benutzerspeicherschlüssel eingerichtet werden.
2. Wenn eine Datenreplikation auf einen Sekundärspeicher erforderlich ist, muss die ONTAP -Speicherreplikation für das HANA-Datenvolume konfiguriert werden.
3. Das SnapCenter HANA-Plug-in muss auf dem HANA-Datenbankhost bereitgestellt werden.
    a. Der automatische Erkennungsprozess wird gestartet
    b. Der SAP HANA-Benutzerspeicherschlüssel muss in SnapCenter konfiguriert werden.
    c. Die zweite Phase der automatischen Erkennung wird gestartet und die HANA-Ressource wird von SnapCenter automatisch hinzugefügt.
4. Der HANA-Ressourcenschutz muss für die neu hinzugefügte HANA-Ressource konfiguriert werden.

Die anfängliche SnapCenter -Konfiguration, wie im vorherigen Thema beschrieben. "Erstkonfiguration von SnapCenter" Dies muss zuerst erfolgen, da während der Konfiguration der HANA-Datenbankressourcen Anmeldeinformationen, Speichersysteme und Richtlinien benötigt werden. Die folgende Abbildung fasst die Schritte und Abhängigkeiten zusammen.

Die folgende Abbildung veranschaulicht die verschiedenen Konfigurationskomponenten und Abhängigkeiten.

[Breite=601, Höhe=315] In den folgenden Abschnitten finden Sie eine detaillierte Beschreibung der erforderlichen Konfigurationsschritte.

SAP HANA Backup-Benutzer- und SAP HANA Benutzerspeicherkonfiguration

NetApp empfiehlt, in der HANA-Datenbank einen dedizierten Benutzer zu konfigurieren, der die Backup-Vorgänge mit SnapCenter ausführt. Im zweiten Schritt wird für diesen Backup-Benutzer ein SAP HANA-Benutzerspeicherschlüssel konfiguriert, und der SAP HANA-Benutzerspeicherschlüssel wird in der SnapCenter -Konfiguration bereitgestellt.

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

Der Backup-Benutzer muss mit den Berechtigungen Backup-Admin, Katalog-Lesen, Datenbank-Backup-Admin und Datenbank-Wiederherstellungsoperator konfiguriert werden.

Der Backup-Benutzer muss in der Systemdatenbank angelegt werden, da alle Backup-Befehle für die System- und Mandantendatenbanken über die Systemdatenbank ausgeführt werden.

[Breite=601, Höhe=382]

SAP HANA-Benutzerspeicherkonfiguration auf dem HANA-Datenbankhost

SnapCenter verwendet den Benutzer <sid>adm zur Kommunikation mit der HANA-Datenbank. Daher muss der SAP HANA-Benutzerspeicherschlüssel mit dem Benutzer <sid>adm auf dem Datenbankhost konfiguriert werden.

hdbuserstore set <key-name> <host>:<port> <database user> <password>

Bei einem SAP HANA MDC-System ist der Port der HANA-Systemdatenbank 3<instanceNo>13.

SAP HANA Benutzerspeicherkonfigurationsbeispiele

Die Ausgabe zeigt den Schlüssel SS1KEY an, der für das HANA-System mit der Instanznummer = 00 konfiguriert wurde.

```
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 SS1SAPDBCTRL
ENV : hana-1:30013
USER: SAPDBCTRL
KEY SS1KEY
ENV : hana-1:30013
USER: SNAPCENTER
KEY SYSTEMKEY
ENV : hana-1:30013
USER: SYSTEM
ACTIVE RECORDS : 10
DELETED RECORDS : 15
NUMBER OF COMPLETE KEY: 3
Operation succeed.
ss1adm@hana-1:/usr/sap/SS1/HDB00>
```

Die Ausgabe zeigt den Schlüssel SM1KEY an, der für das HANA-System mit der Instanznummer = 12 konfiguriert wurde.

```
sm1adm@hana-2:/usr/sap/SM1/HDB12> hdbuserstore list
DATA FILE : /usr/sap/SM1/home/.hdb/hana-2/SSFS_HDB.DAT
KEY FILE : /usr/sap/SM1/home/.hdb/hana-2/SSFS_HDB.KEY
KEY SM1SAPDBCTRL
ENV : hana-2:31213
USER: SAPDBCTRL
KEY SM1KEY
ENV : hana-2:31213
USER: SNAPCENTER
ACTIVE RECORDS : 7
DELETED RECORDS : 9
NUMBER OF COMPLETE KEY: 2
Operation succeed.
sm1adm@hana-2:/usr/sap/SM1/HDB12>
```

Speicherreplikationskonfiguration

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

Die folgenden Screenshots zeigen eine Konfiguration mit dem ONTAP System Manager. Bei FSx für ONTAP -Systemen muss die Replikation mithilfe der ONTAP CLI wie beschrieben durchgeführt werden unter "Übersicht - Backup-Replikation mit SnapVault"Die

Die folgende Abbildung zeigt die konfigurierte Schutzbeziehung für das Datenvolumen des SAP HANA-

Systems SS1. In diesem Beispiel wird das Quellvolume SS1_data_mnt00001 auf dem SVM hana-primary auf das SVM hana-backup und das Zielvolume SS1_data_mnt00001_dst repliziert.

[Breite=601, Höhe=183]

Die folgende Abbildung zeigt die Schutzrichtlinie, die für diesen Laboraufbau erstellt wurde. Die für die Schutzbeziehung verwendete Schutzrichtlinie definiert das SnapMirror -Label sowie die Aufbewahrung von Backups auf dem Sekundärspeicher. In diesem Beispiel lautet die verwendete Bezeichnung „Täglich“ und die Aufbewahrungsdauer ist auf 5 eingestellt.

Die Bezeichnung „SnapMirror“ in der Replikationsrichtlinie muss mit der in der SnapCenter -Richtlinienkonfiguration definierten Bezeichnung übereinstimmen.

Der Zeitplan der Beziehung muss auf „Keine“ gesetzt werden, da SnapCenter die SnapVault Aktualisierung als Teil des Sicherungsvorgangs auf Basis des zuvor erstellten anwendungskonsistenten Snapshots auslöst.

Die Aufbewahrungsdauer für Backups auf dem sekundären Backup-Speicher wird in der Richtlinie definiert und von ONTAP gesteuert.

[Breite=601, Höhe=180]

ANF-Backup-Konfiguration

Für die ANF-Datensicherung sind keine besonderen Vorbereitungen erforderlich. Sobald die erste Sicherung mit aktiviertem ANF-Backup ausgeführt wird, erstellt SnapCenter einen Azure-Sicherungstresor mit dem Namen snapcenter-vault. Dieser Backup-Tresor wird dann von allen nachfolgenden ANF-Backup-Operationen verwendet, die von SnapCenter ausgeführt werden.

[Breite=601, Höhe=227]

Bereitstellung des SnapCenter -Plug-ins für SAP HANA

Die Anforderungen an den Host sind aufgelistet unter "Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux"Die

Die Bereitstellung des HANA-Plug-ins erfolgt durch Klicken auf die Schaltfläche „Hinzufügen“ im Abschnitt „Hosts“ der SnapCenter Benutzeroberfläche.

[Breite=601, Höhe=145]

Im Bildschirm „Host hinzufügen“ müssen Sie den Hosttyp und -namen sowie die Anmeldeinformationen angeben, die für den Bereitstellungsprozess verwendet werden sollen. Darüber hinaus muss das SAP HANA-Plug-in ausgewählt werden. Mit einem Klick auf „Absenden“ wird der Bereitstellungsprozess gestartet.

Für diese Beschreibung haben wir keinen neuen Host hinzugefügt, sondern zeigen die Konfiguration bestehender Hosts in SnapCenter.

[Breite=601, Höhe=154]

HANA-Autoerkennung

Sobald die Bereitstellung des HANA-Plug-ins abgeschlossen ist, wird der automatische Erkennungsprozess gestartet. In der ersten Phase werden nur die Grundeinstellungen ermittelt und SnapCenter erstellt eine neue Ressource, die im Ressourcenbereich der Benutzeroberfläche mit einem roten Vorhängeschloss gekennzeichnet wird.

[Breite=601, Höhe=169]

Beim Anklicken der Ressource werden Sie nach dem SAP HANA-Benutzerspeicherschlüssel für diese HANA-Datenbank gefragt.

[Breite=316, Höhe=180]

Nach der Bereitstellung des Schlüssels beginnt die zweite Phase des automatischen Erkennungsprozesses. Der automatische Erkennungsprozess ermittelt alle Mandantendatenbanken im HANA-System, die Konfigurationsdetails für Protokoll- und Katalogsicherungen sowie die Replikationsrollen des HANA-Systems. Darüber hinaus werden die Speicherbedarfsdetails automatisch ermittelt. Diese Einstellungen können überprüft werden, indem man eine Ressource auswählt und auf die Schaltfläche „Details“ klickt.

Dieser automatische Erkennungsprozess wird bei jedem Sicherungsvorgang ausgeführt, sodass alle Änderungen am HANA-System, die für den Sicherungsvorgang relevant sind, automatisch erkannt werden.

[Breite=601, Höhe=219]

Konfiguration für Ressourcenschutz

Der Bildschirm zur Konfiguration des Ressourcenschutzes wird durch Anklicken einer Ressource geöffnet, nachdem der automatische Erkennungsprozess abgeschlossen ist. Die Screenshots in dieser Dokumentation zeigen die Schutzkonfiguration einer bestehenden Ressource.

Konfigurieren Sie ein benutzerdefiniertes Namensformat für den Snapshot. NetApp empfiehlt die Verwendung eines benutzerdefinierten Snapshot-Namens, um leicht erkennen zu können, welche Backups mit welchem Richtlinien- und Zeitplantyp erstellt wurden.

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

- Geplante stündliche Datensicherung: + SnapCenter_<Hostname>_LocalSnap_Hourly_<Zeitstempel>
- Geplante tägliche Sicherung: + SnapCenter_<Hostname>_LocalSnapAndSnapVault_Daily_<Zeitstempel>

[Breite=601, Höhe=294]

Im nächsten Bildschirm können Skripte konfiguriert werden, die in verschiedenen Schritten des Backup-Workflows ausgeführt werden sollen.

[Breite=601, Höhe=294]

Nun werden Richtlinien mit den Ressourcen verknüpft und Zeitpläne definiert.

In diesem Beispiel haben wir Folgendes konfiguriert:

- Wöchentliche Überprüfung der Blockintegrität, jeden Sonntag

- Eine lokale Snapshot-Sicherung, alle 4 Stunden
- Tägliche Snapshot-Sicherung mit SnapVault -Replikation einmal täglich

[Breite=601, Höhe=294]

E-Mail-Benachrichtigungen können konfiguriert werden.

[Breite=601, Höhe=294]

Sobald die Konfiguration des Ressourcenschutzes abgeschlossen ist, werden die geplanten Backups gemäß den definierten Einstellungen ausgeführt.

Konfigurieren Sie SnapCenter so, dass es Nicht-Datenvolumes sichert.

Konfigurieren Sie SnapCenter so, dass auch Nicht-Datenvolumes wie ausführbare Dateien, Konfigurationsdateien, Protokolldateien und Anwendungsserverdaten gesichert werden.

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.

Für die Wiederherstellung von Daten, die nicht mit der Datenverarbeitung zusammenhängen, empfiehlt NetApp die Entwicklung einer zusätzlichen Backup-Strategie für Nicht-Daten-Volumes, um das Backup der SAP HANA-Datenbank zu ergänzen. Je nach Ihren spezifischen Anforderungen können sich die Sicherungsintervalle und Aufbewahrungseinstellungen für Nicht-Datenvolumes unterscheiden. Sie sollten außerdem berücksichtigen, wie häufig Nicht-Datendateien geändert werden. Das HANA-Volume /hana/shared enthält beispielsweise ausführbare Dateien, Konfigurationsdateien, aber auch SAP HANA-Tracedateien. Während sich die ausführbaren Dateien nur bei einem Upgrade der SAP HANA-Datenbank ändern, benötigen die SAP HANA-Konfigurations- und Trace-Dateien möglicherweise eine höhere Sicherungsfrequenz. Auch SAP-Anwendungsserver-Volumes können mit SnapCenter durch die Verwendung von Nicht-Daten-Volume-Backups geschützt werden.

Mit der SnapCenter Funktion zur Sicherung von Nicht-Daten-Volumes können Snapshot-Kopien aller relevanten Volumes in wenigen Sekunden erstellt werden, und zwar mit der gleichen Speicherplatzeffizienz wie bei SAP HANA-Datenbanksicherungen. Der Unterschied besteht darin, dass keine Interaktion mit der SAP HANA-Datenbank erforderlich ist.

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

[Breite=601, Höhe=173]

[Breite=601, Höhe=112]

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.

[Breite=332, Höhe=310]

Wählen Sie für ONTAP -Systeme und FSx für ONTAP den Speichertyp ONTAP aus und fügen Sie die SVM(s) und das/die Speichervolumen als Speicher-Footprint hinzu. Klicken Sie anschließend auf Weiter.

[Breite=332, Höhe=312]

Wählen Sie für ANF den Speichertyp Azure NetApp Files aus, wählen Sie das NetApp -Konto und den Kapazitätspool aus und fügen Sie die ANF-Volumes als Speicherfläche hinzu. Klicken Sie anschließend auf Weiter.

[Breite=350, Höhe=337]

Klicken Sie im Übersichtsschritt auf Fertig stellen, um die Einstellungen zu speichern.

Wiederholen Sie diese Schritte für alle benötigten Nicht-Datenvolumes. Fahren Sie mit der Schutzkonfiguration der neuen Ressource fort.

> Die Konfiguration des Datenschutzes für Nicht-Datenvolumenressourcen ist identisch mit dem Workflow für SAP HANA-Datenbankressourcen und kann auf Ebene einer einzelnen Ressource definiert werden.

SnapCenter Zentral-Plug-in-Host für SAP HANA konfigurieren

Setzen Sie das SnapCenter HANA-Plug-in auf einem zentralen Host ein, um SAP HANA-Mehrhostsysteme oder HANA-Systeme auf IBM Power zu unterstützen. Dieses Verfahren umfasst die Installation des Plug-ins auf einem Windows- oder Linux-Host, die Konfiguration des SAP HANA hdbsql-Clients und die Einrichtung von Benutzerspeicherschlüsseln für jedes geschützte HANA-System.

Wie in "Bereitstellungsoptionen für das SnapCenter -Plug-in für SAP HANA"Das HANA-Plug-in kann außerhalb der HANA-Datenbank eingesetzt werden, um eine zentrale Plug-in-Konfiguration zu unterstützen, die für SAP HANA Multi-Host-Systeme oder SAP HANA on IBM Power-Umgebungen erforderlich ist.

Als zentraler Plug-in-Host kann jeder Windows- oder Linux-Host verwendet werden, typischerweise wird jedoch der SnapCenter -Server selbst als zentraler Plug-in-Host eingesetzt.

Die Konfiguration eines zentralen Plug-in-Hosts umfasst die folgenden Schritte:

- SnapCenter HANA-Plug-in-Bereitstellung
- SAP HANA hdbsql Client Installation und Konfiguration
- Die SAP HANA-Benutzerspeicherkonfiguration für jedes HANA-System wird durch den zentralen Plug-in-Host geschützt.

SnapCenter HANA-Plug-in-Bereitstellung

Die Anforderungen an den Host sind aufgelistet unter "Hostanforderungen für die Installation des SnapCenter Plug-Ins-Pakets für Linux"Die

Der zentrale Plug-in-Host wird als Host hinzugefügt, und das SAP HANA-Plug-in wird auf dem Host installiert. Der folgende Screenshot zeigt die Plug-in-Bereitstellung auf einem SnapCenter -Server unter Windows.

1. Gehen Sie zu Hosts und klicken Sie auf Hinzufügen.
2. Geben Sie die erforderlichen Hostinformationen ein. Klicken Sie Auf Senden.

[Breite=601, Höhe=166]

Installation und Konfiguration der SAP HANA hdbsql Client-Software

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

Der während der HANA-Ressourcenkonfiguration konfigurierte hdbsql-Betriebssystembenutzer muss in der Lage sein, die hdbsql-Executable auszuführen. Der Pfad zur ausführbaren Datei hdbsql muss in der Datei hana.properties oder in den Suchpfadparametern (%PATH%, $PATH) des Betriebssystembenutzers konfiguriert werden.

Zentraler Plug-in-Host unter 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
```

Zentraler Plugin-Host unter Linux:

```
cat /opt/NetApp/snapcenter/scc/etc/hana.properties

HANA_HDBSQL_CMD=/usr/sap/hdbclient/hdbsql
```

SAP HANA-Benutzerspeicherkonfiguration für einen zentralen Plug-in-Host

Für jedes HANA-System, das vom zentralen Plug-in-Host verwaltet wird, muss ein SAP HANA-Benutzerspeicherschlüssel konfiguriert werden. Bevor der Schlüssel auf dem zentralen Plug-in-Host konfiguriert werden kann, muss ein Datenbankbenutzer wie beschrieben erstellt werden. "SAP HANA Backup-Benutzer- und SAP HANA Benutzerspeicherkonfiguration"Die

Wenn das SAP HANA-Plug-in und der SAP hdbsql-Client unter Windows installiert sind, führt der lokale Systembenutzer die hdbsql-Befehle aus und ist standardmäßig in der Ressourcenkonfiguration konfiguriert. Da der Systembenutzer kein Anmeldebenutzer ist, muss die Konfiguration des SAP HANA-Benutzerspeichers mit einem anderen Benutzer unter Verwendung der Option -u <Benutzer> durchgeführt werden.

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

Bei einer SAP HANA-Umgebung mit mehreren Hosts müssen die SAP HANA-Benutzerspeicherschlüssel für alle Hosts konfiguriert werden. SnapCenter versucht, mit jedem der bereitgestellten Schlüssel eine Verbindung zur Datenbank herzustellen und kann daher unabhängig von einem Failover der Systemdatenbank (HANA-Namensserver) auf einen anderen Host funktionieren. Für alle Worker- und Standby-Hosts ist ein SAP HANA-Benutzerspeicherschlüssel konfiguriert. Der HANA-Datenbankbenutzer, in diesem Beispiel SNAPCENTER, ist der Benutzer, der in der Systemdatenbank konfiguriert wurde.

```
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-61\S-1-5-18\SSFS_HDB.DAT
KEY FILE : C:\ProgramData\.hdb\SNAPCENTER-61\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>
```

Manuelle HANA-Ressourcenkonfiguration

Eine manuell konfigurierte HANA-Systemressource wird in SnapCenter erstellt, indem in der Ressourcenansicht auf die Schaltfläche „Hinzufügen“ geklickt wird.

[Breite=601, Höhe=189]

Im nächsten Bildschirm müssen Sie einige Systemparameter angeben.

- Plug-in-Host: Der zentrale Plug-in-Host muss ausgewählt werden.
- SAP HANA Benutzerspeicherschlüssel: Bei einem HANA-System mit einem einzelnen Host muss der Schlüsselname angegeben werden, der auf dem zentralen Plug-in-Host vorbereitet wurde. Bei einem HANA-System mit mehreren Hosts muss eine durch Kommas getrennte Liste aller Schlüssel für das System angegeben werden.
- HDBSQL-Betriebssystembenutzer: Wenn der zentrale Plug-in-Host unter Windows läuft, wird der Benutzer automatisch als SYSTEM-Benutzer vorausgewählt. Andernfalls muss der Benutzer angegeben werden, der für den SAP HANA-Benutzerspeicherschlüssel verwendet wurde.

[Breite=384, Höhe=357]

Als nächstes muss der Speicherbedarf konfiguriert werden. Alle ONTAP oder ANF-Volumes, die zum HANA-System gehören, müssen hier hinzugefügt werden.

[Breite=385, Höhe=359]

Die Konfiguration des Ressourcenschutzes kann nun auf die gleiche Weise wie bei automatisch erkannten HANA-Systemen erfolgen.

Erfahren Sie mehr über Sicherungsvorgänge für SAP HANA Snapshots in SnapCenter.

Führen Sie SAP HANA Snapshot-Backups mit SnapCenter durch. Erfahren Sie mehr über Datenbank-Snapshot-Backups, Blockintegritätsprüfungen, Backups von Nicht-Datenvolumes und Backup-Replikation mit SnapVault oder Azure NetApp Files Backup.

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.

SnapCenter unterstützt die folgenden Sicherungsvorgänge.

- HANA-Datenbank-Snapshot-Sicherungsvorgänge
- Blockintegritätsprüfungsoperationen
- Snapshot-Backups von Nicht-Datenvolumes
- Backup-Replikation mit SnapVault oder ANF-Backup für HANA-Datenbanken oder Nicht-Datenvolumen-Backups

In den folgenden Abschnitten werden die verschiedenen Operationen für Einzelhost-HANA-Systeme beschrieben, die von SnapCenter (HANA-Plug-in, das auf dem HANA-Datenbankhost bereitgestellt wird) automatisch erkannt wurden.

SAP HANA Snapshot-Backups in SnapCenter

Die SnapCenter -Ressourcentopologie zeigt die Liste der von SnapCenter erstellten Backups. Die folgende Abbildung zeigt die auf dem primären Speicher verfügbaren Backups und hebt das aktuellste Backup hervor.

[Breite=601, Höhe=293]

Die Backups im Sekundärspeicher können durch Anklicken des Symbols „Vault-Kopien“ aufgelistet werden.

[Breite=601, Höhe=294]

Der folgende Screenshot zeigt die Liste der Backups für das System SM1, für das manipulationssichere Snapshots konfiguriert wurden.

[Breite=601, Höhe=293]

SAP HANA Snapshot-Backups in SAP HANA Studio

Bei der Durchführung einer Datensicherung mittels Speichersnapshots für ein SAP HANA MDC-System wird eine Snapshot-Kopie des Datenvolumes erstellt. Dieses Datenvolumen enthält die Daten der Systemdatenbank sowie die Daten aller Mandantendatenbanken. Um diese physische Architektur abzubilden, führt SAP HANA intern immer dann einen kombinierten internen Datenbank-Snapshot der Systemdatenbank sowie aller Mandantendatenbanken durch, wenn SnapCenter eine Snapshot-Sicherung auslöst. Dies führt zu mehreren separaten Backup-Einträgen im SAP HANA Backup-Katalog: einem für die Systemdatenbank und einem für jede Mandantendatenbank.

Im SAP HANA Backup-Katalog wird der Name des SnapCenter -Backups als Kommentarfeld sowie als externe Backup-ID (EBID) gespeichert. Dies wird im folgenden Screenshot für die Systemdatenbank und im darauffolgenden Screenshot für die Mandantendatenbank SS1 gezeigt. In beiden Abbildungen werden der im Kommentarfeld gespeicherte SnapCenter -Backup-Name und die EBID hervorgehoben.

[Breite=601, Höhe=289]

[Breite=601, Höhe=296]

SnapCenter kennt nur seine eigenen Backups. Zusätzliche Backups, die beispielsweise mit SAP HANA Studio erstellt wurden, sind im SAP HANA-Katalog sichtbar, jedoch nicht in SnapCenter. Auch direkt auf dem Speichersystem erstellte Snapshots sind in SnapCenter nicht sichtbar.

SAP HANA Snapshot-Backups auf der Speicherschicht

Um die Backups auf der Speicherebene anzuzeigen, können Sie den NetApp System Manager verwenden und das Datenbankvolume auswählen. Der folgende Screenshot zeigt die verfügbaren Backups für das Datenbankvolume SS1_data_mnt00001 auf dem primären Speicher. Das hervorgehobene Backup ist das Backup, das in SnapCenter und SAP HANA Studio in den vorherigen Bildern angezeigt wird und die gleiche Namenskonvention aufweist.

[Breite=601, Höhe=294]

Der folgende Screenshot zeigt die verfügbaren Backups für das Replikationszielvolume hana_SS1_data_mnt00001_dest auf dem sekundären Speichersystem.

[Breite=601, Höhe=294]

SAP HANA Snapshot-Backups mit ANF

Der folgende Screenshot zeigt die Topologieansicht eines HANA-Systems mit Azure NetApp Files. Für dieses HANA-System wurden sowohl lokale Snapshot-Backups als auch Backup-Replikation mittels ANF-Backup konfiguriert.

[Breite=601, Höhe=303]

Die Snapshot-Backups auf dem ANF-Volume können über das Azure-Portal aufgelistet werden.

[Breite=601, Höhe=258]

Durch Klicken auf das Sicherungssymbol können Sie die Sicherungen auflisten, die mit ANF Backup repliziert wurden.

[Breite=601, Höhe=304]

ANF-Backups können auch im Azure-Portal aufgelistet werden.

[Breite=601, Höhe=216]

Snapshot-Backups von Nicht-Datenvolumes

Die SnapCenter -Ressourcentopologie zeigt die Liste der Backups für Nicht-Datenvolumes an. In der folgenden Abbildung sind die Backups des gemeinsam genutzten HANA-Volumes aufgelistet.

[Breite=601, Höhe=294]

Backup-Workflow für HANA-Datenbanksicherungen

Der Backup-Workflow für ein HANA-Datenbank-Snapshot-Backup besteht aus drei Hauptabschnitten.

- Automatische Erkennung
  - Anwendungserkennung, z. B.
    - SnapCenter erkennt alle Änderungen an der Mandantenkonfiguration.
    - SnapCenter erkennt den primären Replikationsknoten des HANA-Systems.
  - Dateisystem- und Speichererkennung, z. B.
    - SnapCenter erkennt jegliche Änderungen in der Volumenkonfiguration.
    - SnapCenter erkennt HANA-Konfigurationen mit mehreren Partitionen
- HANA- und Snapshot-Backup-Operationen
  - Trigger HANA-Datenbank-Snapshot
  - Speicher-Snapshot erstellen
  - Bestätigen Sie den HANA-Datenbank-Snapshot und registrieren Sie die Sicherung im HANA-Sicherungskatalog.
- Retentionmanagement
  - Snapshot-Backups basierend auf der definierten Aufbewahrungsdauer löschen in
    - SnapCenter -Repository
    - Storage
    - HANA-Backup-Katalog
  - Verwaltung der Aufbewahrung von Protokollsicherungen
    - Protokollsicherungen im Dateisystem und im HANA-Sicherungskatalog löschen

[Breite=339, Höhe=475]

Backup-Workflow für Nicht-Datenvolumes

Bei einem Nicht-Daten-Volume besteht der Backup-Workflow aus der Snapshot-Operation und der Aufbewahrungsverwaltungsoperation.

[Breite=329, Höhe=404]

Bereinigung sekundärer Backups

Wie in beschrieben "Aufbewahrungsmanagement für sekundäre Backups"Die Aufbewahrungsverwaltung von Datensicherungen auf einem sekundären Sicherungsspeicher wird von ONTAP übernommen. SnapCenter prüft regelmäßig, ob ONTAP Backups auf dem sekundären Backup-Speicher gelöscht hat, indem es wöchentlich einen Bereinigungsauftrag ausführt.

Der SnapCenter -Bereinigungsjob löscht Backups sowohl im SnapCenter -Repository als auch im SAP HANA-Backup-Katalog, falls gelöschte Backups im sekundären Backup-Speicher identifiziert wurden.

[Breite=601, Höhe=158]

[Breite=267, Höhe=330]

Bis zum Abschluss dieser planmäßigen Bereinigung werden in SAP HANA und SnapCenter weiterhin Backups angezeigt, die bereits aus dem sekundären Backup-Speicher gelöscht wurden. Dies führt dazu, dass zusätzliche Protokollsicherungen aufbewahrt werden, selbst wenn die entsprechenden speicherbasierten Snapshot-Sicherungen auf dem sekundären Sicherungsspeicher bereits gelöscht wurden. NetApp empfiehlt, den Zeitplan von wöchentlich auf täglich umzustellen, um die Aufbewahrung von Protokollsicherungen zu vermeiden, da diese nicht mehr erforderlich sind.

Ändern Sie die Häufigkeit des SnapCenter-Bereinigungsjobs

SnapCenter führt standardmäßig wöchentlich den Bereinigungsauftrag SnapCenter_RemoveSecondaryBackup für alle Ressourcen aus. Dies kann mithilfe eines SnapCenter PowerShell-Cmdlets geändert werden.

```
SnapCenterPS C:\> Open-SmConnection

Enter username/password
User: sapcc\scadmin
Password for user sapcc\scadmin: **********

SnapCenterPS C:\> Set-SmSchedule -ScheduleInformation
@{"ScheduleType"="Daily";"StartTime"="03:45 AM";"DaysInterval"="1"}
-TaskName SnapCenter_RemoveSecondaryBackup

TaskName : SnapCenter_RemoveSecondaryBackup
Hosts : {}
StartTime : 8/25/2025 3:45:00 AM
DaysoftheMonth :
MonthsofTheYear :
DaysInterval : 1
DaysOfTheWeek :
AllowDefaults : False
ReplaceJobIfExist : False
UserName :
Password :
SchedulerType : Daily
RepeatTask_Every_Hour : 1
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 :
ScheduleCategory :
PolicyId : 0
PolicyName :
ProtectionGroupId : 0
ProtectionGroupName :
PluginCode : NONE
PolicyType : None
ReportTriggerName :
PolicyScheduleId : 0
HoursOfTheDay :
DayStartTime :
MinuteOffset : ZeroMinutes
SnapMirrorLabel :
BackupType :
SnapCenterPS C:\>
```

Die Konfiguration kann auch in der Ansicht „Überwachung – Zeitpläne“ in der SnapCenter Benutzeroberfläche überprüft werden.

[Breite=601, Höhe=257]

Manuelle Aktualisierung auf Ressourcenebene

Bei Bedarf kann in der Topologieansicht einer Ressource auch eine manuelle Bereinigung der sekundären Backups durchgeführt werden. SnapCenter zeigt die Backups auf dem sekundären Backup-Speicher an, wenn die sekundären Backups ausgewählt werden, wie im folgenden Screenshot dargestellt. SnapCenter führt mit dem Symbol „Aktualisieren“ einen Bereinigungsvorgang durch, um die Backups für diese Ressource zu synchronisieren.

[Breite=601, Höhe=291]

Führen Sie SAP HANA-Blockkonsistenzprüfungen mit SnapCenter durch.

Führen Sie SAP HANA-Blockkonsistenzprüfungen mit dem SAP hdbpersdiag-Tool oder durch Ausführen dateibasierter Backups durch. Erfahren Sie mehr über Konfigurationsoptionen wie den Zugriff auf das lokale Snapshot-Verzeichnis, zentrale Verifizierungshosts mit FlexClone -Volumes und die SnapCenter -Integration für Planung und Automatisierung.

Die folgende Tabelle fasst die wichtigsten Parameter zusammen, die Ihnen bei der Entscheidung helfen, welche Methode für Blockkonsistenzprüfungen am besten für Ihre Umgebung geeignet ist.

	HANA hdbpersdiag-Tool verwendet lokales Snapshot-Verzeichnis	HANA hdbpersdiag-Tool mit zentralem Verifizierungshost	Dateibasierte Datensicherung
Unterstützte Konfigurationen	Nur NFS Bare-Metal-, ANF-, FSx ONTAP, VMware- oder KVM-Gastsystem-Einbindungen	Alle Protokolle und Plattformen	Alle Protokolle und Plattformen
CPU-Auslastung auf dem HANA-Host	Medium	Keine	Hoch
Netzwerkauslastung am HANA-Host	Hoch	Keine	Hoch
Laufzeit	Nutzt den vollen Lesedurchsatz des Speichervolumens aus	Nutzt den vollen Lesedurchsatz des Speichervolumens aus	Typischerweise begrenzt durch den Schreibdurchsatz des Zielsystems
Kapazitätsanforderungen	Keine	Keine	Mindestens 1 x Backup-Größe pro HANA-System
SnapCenter Integration	Backup-Skript	Klon erstellen und Skript für die Nachbearbeitung des Klonvorgangs, Klon löschen	Eingebaute Funktion
Terminplanung	SnapCenter Planer	PowerShell-Skript zur Ausführung des Workflows zum Erstellen und Löschen von Klonen, extern geplant	SnapCenter Planer

In den folgenden Kapiteln werden die Konfiguration und Ausführung der verschiedenen Optionen für Blockkonsistenzprüfungsoperationen beschrieben.

Konsistenzprüfungen mit hdbpersdiag unter Verwendung des lokalen Snapshot-Verzeichnisses

Innerhalb von SnapCenter wird eine spezielle Richtlinie für hdbpersdiag-Operationen mit einem Tagesplan und einer Aufbewahrungsfrist von zwei Tagen erstellt. Wir verwenden keinen wöchentlichen Zeitplan, da wir dann mindestens 2 Snapshot-Backups hätten (minimale Aufbewahrungsdauer = 2), von denen eines bis zu zwei Wochen alt wäre.

Innerhalb der SnapCenter Ressourcenschutzkonfiguration des HANA-Systems wird ein Post-Backup-Skript hinzugefügt, das das Tool hdbpersdiag ausführt. Da das Skript nach der Datensicherung auch mit jeder anderen für die Ressource konfigurierten Richtlinie aufgerufen wird, müssen wir im Skript überprüfen, welche Richtlinie aktuell aktiv ist. Innerhalb des Skripts prüfen wir auch den aktuellen Wochentag und führen die hdbpersdiag-Operation nur einmal pro Woche, nämlich sonntags, aus. Anschließend wird HANA hdbpersdiag für jedes Datenvolume im entsprechenden hdb*-Verzeichnis des aktuellen Snapshot-Sicherungsverzeichnisses aufgerufen. Wenn die Konsistenzprüfung mit hdbpersdiag einen Fehler meldet, wird der SnapCenter -Auftrag als fehlgeschlagen markiert.

Das Beispielskript call-hdbpersdiag.sh wird im vorliegenden Zustand bereitgestellt und ist nicht vom NetApp -Support abgedeckt. Sie können das Skript per E-Mail an ng-sapcc@netapp.com anfordern.

Die folgende Abbildung zeigt das übergeordnete Konzept der Konsistenzprüfungsimplementierung.

[Breite=601, Höhe=248]

Als ersten Schritt müssen Sie den Zugriff auf das Snapshot-Verzeichnis erlauben, damit das Verzeichnis """.snapshot" auf dem HANA-Datenbankhost sichtbar ist.

- ONTAP -Systeme und FSX für ONTAP: Sie müssen den Parameter für den Zugriff auf das Snapshot-Verzeichnis konfigurieren.
- ANF: Sie müssen den Volume-Parameter „Snapshot-Pfad ausblenden“ konfigurieren.

Als nächsten Schritt müssen Sie eine Richtlinie konfigurieren, die mit dem Namen übereinstimmt, der im Post-Backup-Skript verwendet wird. Für unser Skriptbeispiel muss der Name SnapAndCallHdbpersdiag lauten. Wie bereits erwähnt, wird ein Tagesplan verwendet, um zu vermeiden, dass alte Snapshots mit einem Wochenplan zusammengehalten werden.

[Breite=414, Höhe=103]

[Breite=424, Höhe=108]

[Breite=433, Höhe=336]

Innerhalb der Ressourcenschutzkonfiguration wird das Skript für die Nachsicherung hinzugefügt und die Richtlinie der Ressource zugewiesen.[Breite=601, Höhe=294]

[Breite=601, Höhe=281]

Schließlich muss das Skript in der Datei allowed_commands.config auf dem HANA-Host konfiguriert werden.

```
hana-1:/ # cat /opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/hdbpersdiag/call-hdbpersdiag.sh
```

Die Snapshot-Sicherungsoperation wird nun einmal täglich ausgeführt, und das Skript sorgt dafür, dass die hdbpersdiag-Prüfung nur einmal wöchentlich, nämlich sonntags, durchgeführt wird.

Das Skript ruft hdbpersdiag mit der Befehlszeilenoption „-e“ auf, die für die Datenvolume-Verschlüsselung erforderlich ist. Wenn die HANA-Datenvolumenverschlüsselung nicht verwendet wird, muss der Parameter entfernt werden.

Die folgende Ausgabe zeigt die Protokolldatei des Skripts:

```
20251024055824###hana-1###call-hdbpersdiag.sh: Current policy is
SnapAndCallHdbpersdiag
20251024055824###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
```

```
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001
20251024055827###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001/ (4.8 GB,
5100273664 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (94276 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251024055827###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001.
20251024055827###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003
20251024055828###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003/
(320.0 MB, 335544320 bytes)
```

```
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (4099 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
UndoContainerDirectory OK
DRLoadedTable OK
20251024055828###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003.
20251024055828###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003
20251024055833###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003/
(4.6 GB, 4898947072 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
Static Converter Pages OK
RowStore Converter Pages OK
Logical Pages (100817 pages) OK
Logical Pages Linkage OK
```

```
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
DRLoadedTable OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251024055833###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003.
20251024060048###hana-1###call-hdbpersdiag.sh: Current policy is
LocalSnapAndSnapVault, consistency check is only done with Policy
SnapAndCallHdbpersdiag
20251024080048###hana-1###call-hdbpersdiag.sh: Current policy is
LocalSnap, consistency check is only done with Policy SnapAndHdbpersdiag
```

Konsistenzprüfungen mit hdbpersdiag unter Verwendung eines zentralen Verifizierungshosts

Die folgende Abbildung zeigt eine Übersicht über die Lösungsarchitektur und den Arbeitsablauf. Mit einem zentralen Verifizierungshost kann die Konsistenz mehrerer unterschiedlicher HANA-Systeme überprüft werden. Die Lösung nutzt die SnapCenter -Workflows zum Erstellen und Löschen von Klonen, um ein geklontes Volume aus dem HANA-System, das überprüft werden soll, an den Verifizierungshost anzuhängen. Ein Post-Clone-Skript wird verwendet, um das HANA hdbpersdiag-Tool auszuführen. Im zweiten Schritt wird der SnapCenter -Workflow zum Löschen von Klonen verwendet, um das geklonte Volume auszuhängen und zu löschen.

> Wenn die HANA-Systeme mit Datenvolumenverschlüsselung konfiguriert sind, müssen die Verschlüsselungsstammschlüssel des Quell-HANA-Systems auf dem Verifizierungshost importiert werden, bevor hdbpersdiag ausgeführt wird. Siehe auch "Importieren gesicherter Stammschlüssel vor der Datenbankwiederherstellung | SAP-Hilfeportal"

[Breite=601, Höhe=257]

Das HANA-Tool hdbpersdiag ist in jeder HANA-Installation enthalten, steht aber nicht als eigenständiges Tool zur Verfügung. Daher muss der zentrale Verifizierungshost durch die Installation eines normalen HANA-Systems vorbereitet werden.

Erste einmalige Vorbereitungsschritte:

- Installation eines SAP-HANA-Systems, das als zentraler Verifizierungshost verwendet werden soll
- Konfiguration des SAP HANA-Systems in SnapCenter
  - Bereitstellung des SnapCenter SAP HANA-Plug-ins auf dem Verifizierungshost. Das SAP HANA-System wird von SnapCenter automatisch erkannt.
- Die erste hdbpersdiag-Operation nach der Erstinstallation wird mit folgenden Schritten vorbereitet:
  - Herunterfahren des Ziel-SAP HANA-Systems
  - SAP HANA-Datenvolumen unmounten.

Sie müssen die Skripte, die auf dem Zielsystem ausgeführt werden sollen, der Konfigurationsdatei „SnapCenter allowed commands“ hinzufügen.

```
hana-7:/mnt/sapcc-share/hdbpersdiag # cat
/opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/hdbpersdiag/call-hdbpersdiag-flexclone.sh
```

Das Beispielskript call-hdbpersdiag-flexclone.sh wird ohne Gewährleistung bereitgestellt und ist nicht vom NetApp -Support abgedeckt. Sie können das Skript per E-Mail an ng-sapcc@netapp.com anfordern.

Manuelle Workflow-Ausführung

In den meisten Fällen wird die Konsistenzprüfung als geplanter Vorgang ausgeführt, wie im nächsten Kapitel beschrieben. Kenntnisse über den manuellen Arbeitsablauf sind jedoch hilfreich, um die Parameter zu verstehen, die für den automatisierten Prozess verwendet werden.

Der Workflow zum Erstellen eines Klons wird gestartet, indem man eine Sicherung aus dem System auswählt, die überprüft werden soll, und anschließend auf „Aus Sicherung klonen“ klickt.

[Breite=601, Höhe=247]

Im nächsten Bildschirm müssen der Hostname, die SID und die Speichernetzwerkschnittstelle des Verifizierungshosts angegeben werden.

Es ist wichtig, immer die SID des auf dem Verifizierungshost installierten HANA-Systems zu verwenden, da der Workflow sonst fehlschlägt.

[Breite=431, Höhe=115]

Im nächsten Bildschirm müssen Sie das Skript call-hdbpersdiag-fleclone.sh als Post-Clone-Befehl hinzufügen.

[Breite=442, Höhe=169]

Wenn der Workflow gestartet wird, erstellt SnapCenter ein geklontes Volume basierend auf dem ausgewählten Snapshot-Backup und bindet es auf dem Verifizierungshost ein.

Hinweis: Die unten stehende Beispielausgabe basiert auf HANA-Systemen, die NFS als Speicherprotokoll verwenden. Bei HANA-Systemen, die FC- oder VMware VMDKs verwenden, wird das Gerät auf die gleiche Weise unter /hana/data/SID/mnt00001 eingebunden.

```
hana-7:/mnt/sapcc-share/hdbpersdiag # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 16G 8.0K 16G 1% /dev
tmpfs 25G 0 25G 0% /dev/shm
tmpfs 16G 474M 16G 3% /run
tmpfs 16G 0 16G 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 9.0G 48G 16% /
/dev/mapper/system-root 60G 9.0G 48G 16% /home
/dev/mapper/system-root 60G 9.0G 48G 16% /.snapshots
/dev/mapper/system-root 60G 9.0G 48G 16% /root
/dev/mapper/system-root 60G 9.0G 48G 16% /opt
/dev/mapper/system-root 60G 9.0G 48G 16% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 9.0G 48G 16% /srv
/dev/mapper/system-root 60G 9.0G 48G 16% /usr/local
/dev/mapper/system-root 60G 9.0G 48G 16% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 9.0G 48G 16% /var
/dev/mapper/system-root 60G 9.0G 48G 16% /tmp
/dev/sda1 500M 5.1M 495M 2% /boot/efi
192.168.175.117:/QS1_shared/usr-sap 251G 15G 236G 6% /usr/sap/QS1
192.168.175.86:/sapcc_share 1.4T 858G 568G 61% /mnt/sapcc-share
192.168.175.117:/QS1_log_mnt00001 251G 335M 250G 1% /hana/log/QS1/mnt00001
192.168.175.117:/QS1_shared/shared 251G 15G 236G 6% /hana/shared
tmpfs 3.2G 20K 3.2G 1% /run/user/467
tmpfs 3.2G 0 3.2G 0% /run/user/0
192.168.175.117:/SS2_data_mnt00001_Clone_10292511250337819 250G 6.4G 244G
3% /hana/data/QS1/mnt00001
```

Die folgende Ausgabe zeigt die Protokolldatei des Post-Clone-Befehls call-hdbpersdiag-flexclone.sh.

```
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag for source system SS2.
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Clone mounted at
/hana/data/QS1/mnt00001.
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00001
20251029112600###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00001/ (3.1 GB, 3361128448 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
```

```
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (65388 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251029112600###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00001.
20251029112601###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00002.00003
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00002.00003/ (288.0 MB, 301989888 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (4099 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
UndoContainerDirectory OK
DRLoadedTable OK
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00002.00003.
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00003.00003
20251029112606###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
```

```
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00003.00003/ (3.7 GB, 3942645760 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
Static Converter Pages OK
RowStore Converter Pages OK
Logical Pages (79333 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
DRLoadedTable OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251029112606###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00003.00003.
```

Das Skript ruft hdbpersdiag mit der Befehlszeilenoption „-e“ auf, die für die Datenvolume-Verschlüsselung erforderlich ist. Wenn die HANA-Datenvolumenverschlüsselung nicht verwendet wird, muss der Parameter entfernt werden. Wenn das Post-Clone-Skript abgeschlossen ist, ist auch der SnapCenter -Job beendet.

[Breite=279, Höhe=344]

Als nächsten Schritt führen wir den SnapCenter -Workflow zum Löschen von Klonen aus, um den Verifizierungshost zu bereinigen und das FlexClone -Volume zu löschen.

In der Topologieansicht des Quellsystems wählen wir den Klon aus und klicken auf die Schaltfläche „Löschen“.

[Breite=601, Höhe=165]

SnapCenter wird nun das geklonte Volume vom Verifizierungshost aushängen und das geklonte Volume auf dem Speichersystem löschen.

SnapCenter Workflow-Automatisierung mithilfe von PowerShell-Skripten

Im vorherigen Abschnitt wurden die Workflows zum Erstellen und Löschen von Klonen mithilfe der SnapCenter -Benutzeroberfläche ausgeführt. Alle Workflows können auch mit PowerShell-Skripten oder REST-API-Aufrufen ausgeführt werden, was eine weitere Automatisierung ermöglicht. Im folgenden Abschnitt wird ein

einfaches PowerShell-Skriptbeispiel zur Ausführung der SnapCenter -Workflows zum Erstellen und Löschen von Klonen beschrieben.

> Die Beispielskripte call-hdbpersdiag-flexclone.sh und clone-hdbpersdiag.ps1 werden ohne Gewährleistung bereitgestellt und sind nicht vom NetApp Support abgedeckt. Sie können die Skripte per E-Mail an ng-sapcc@netapp.com anfordern.

Das PowerShell-Beispielskript führt den folgenden Arbeitsablauf aus.

- Suchen Sie anhand des Befehlszeilenparameters SID und des Quellhosts nach dem neuesten Snapshot-Backup.
- Führt den SnapCenter -Klon-Erstellungsworkflow unter Verwendung des im vorherigen Schritt definierten Snapshot-Backups aus. Die Zielhostinformationen und die hdbpersdiag-Informationen werden im Skript definiert. Das Skript call-hdbpersdiag-flexclone.sh ist als Post-Clone-Skript definiert und wird auf dem Zielhost ausgeführt.
  - $result = New-SmClone -AppPluginCode hana -BackupName $backupName -Resources @{"Host"="$sourceHost";"UID"="$uid"} -CloneToInstance "$verificationHost" -NFSExportIPs $exportIpTarget -CloneUid $targetUid -PostCloneCreateCommands $postCloneScript
- Führt den SnapCenter -Klon-Lösch-Workflow aus. Der folgende Text zeigt die Ausgabe des Beispielskripts, das auf dem SnapCenter -Server ausgeführt wurde.

Der folgende Text zeigt die Ausgabe des Beispielskripts, das auf dem SnapCenter -Server ausgeführt wurde.

```
C:\Users\scadmin>pwsh -command "c:\netapp\clone-hdbpersdiag.ps1 -sid SS2
-sourceHost hana-3.sapcc.stl.netapp.com"
Starting verification
Connecting to SnapCenter
Validating clone/verification request - check for already existing clones
Get latest back for [SS2] on host [hana-3.sapcc.stl.netapp.com]
Found backup name [SnapCenter_hana-3_LocalSnapKeep2_Hourly_11-21-
2025_07.56.27.5547]
Creating clone from backup [hana-
3.sapcc.stl.netapp.com/SS2/SnapCenter_hana-3_LocalSnapKeep2_Hourly_11-21-
2025_07.56.27.5547]: [hana-7.sapcc.stl.netapp.com/QS1]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Running]
waiting for job [169851] - [Completed]
Removing clone [SS2 - HANA System Replication__clone__169851_MDC_SS2_07-
09-2025_07.44.09]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Running]
waiting for job [169854] - [Completed]
Verification completed

C:\Users\scadmin>
```

Das Skript ruft hdbpersdiag mit der Befehlszeilenoption „-e“ auf, die für die Datenvolume-Verschlüsselung erforderlich ist. Wenn die HANA-Datenvolumenverschlüsselung nicht verwendet wird, muss der Parameter entfernt werden.

Die folgende Ausgabe zeigt die Protokolldatei des Skripts call-hdbpersdiag-flexclone.sh.

```
20251121085720###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag for source system SS2.
20251121085720###hana-7###call-hdbpersdiag-flexclone.sh: Clone mounted at
/hana/data/QS1/mnt00001.
```

```
20251121085720###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00001
20251121085723###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
  #0 /hana/data/QS1/mnt00001/hdb00001/ (3.1 GB, 3361128448 bytes)
Tips:
  Type 'help' for help on the available commands
  Use 'TAB' for command auto-completion
  Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
                      Default Anchor Page OK
                             Restart Page OK
                   Default Converter Pages OK
                  RowStore Converter Pages OK
              Logical Pages (65415 pages) OK
                    Logical Pages Linkage OK
Checking entries from restart page...
                       ContainerDirectory OK
                  ContainerNameDirectory OK
                  FileIDMappingContainer OK
                  UndoContainerDirectory OK
                             LobDirectory OK
                     MidSizeLobDirectory OK
                             LobFileIDMap OK
20251121085723###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00001.
20251121085723###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00002.00003
20251121085724###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
  #0 /hana/data/QS1/mnt00001/hdb00002.00003/ (288.0 MB, 301989888 bytes)
Tips:
  Type 'help' for help on the available commands
  Use 'TAB' for command auto-completion
  Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
                      Default Anchor Page OK
                             Restart Page OK
                   Default Converter Pages OK
                  RowStore Converter Pages OK
```

```
              Logical Pages (4099 pages) OK
                   Logical Pages Linkage OK
Checking entries from restart page...
                  UndoContainerDirectory OK
                           DRLoadedTable OK
20251121085724###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00002.00003.
20251121085724###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00003.00003
20251121085729###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
  #0 /hana/data/QS1/mnt00001/hdb00003.00003/ (3.7 GB, 3942645760 bytes)
Tips:
  Type 'help' for help on the available commands
  Use 'TAB' for command auto-completion
  Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
                     Default Anchor Page OK
                            Restart Page OK
                 Default Converter Pages OK
                  Static Converter Pages OK
                RowStore Converter Pages OK
             Logical Pages (79243 pages) OK
                   Logical Pages Linkage OK
Checking entries from restart page...
                      ContainerDirectory OK
                  ContainerNameDirectory OK
                  FileIDMappingContainer OK
                  UndoContainerDirectory OK
                            LobDirectory OK
                           DRLoadedTable OK
                     MidSizeLobDirectory OK
                            LobFileIDMap OK
20251121085729###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00003.00003.
hana-7:/mnt/sapcc-share/hdbpersdiag #
```

Dateibasierte Datensicherung

SnapCenter unterstützt die Durchführung einer Blockintegritätsprüfung mithilfe einer Richtlinie, bei der dateibasierte Sicherung als Sicherungstyp ausgewählt ist.

Bei der Planung von Backups mithilfe dieser Richtlinie erstellt SnapCenter ein standardmäßiges SAP HANA-Datei-Backup für das System und alle 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.

[Breite=601, Höhe=293]

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.

[Breite=601, Höhe=293]

Bei einer erfolgreichen Blockintegritätsprüfung werden standardmäßige SAP HANA-Datensicherungsdateien erstellt.

[Breite=351, Höhe=433]

SnapCenter verwendet den in der HANA-Datenbank für dateibasierte Datensicherungsvorgänge konfigurierten Sicherungspfad.

```
hana-1:/hana/shared/SS1/HDB00/backup/data # ls -al *
DB_SS1:
total 3717564
drwxr-xr-- 2 ss1adm sapsys 4096 Aug 22 11:03 .
drwxr-xr-- 4 ss1adm sapsys 4096 Jul 27 2022 ..
-rw-r----- 1 ss1adm sapsys 159744 Aug 17 05:32 SnapCenter_SnapCenter_hana-
1_BlockIntegrityCheck_Weekly_08-17-2025_05.32.00.4493_databackup_0_1
-rw-r----- 1 ss1adm sapsys 83898368 Aug 17 05:32
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_08-17-
2025_05.32.00.4493_databackup_2_1
-rw-r----- 1 ss1adm sapsys 3707777024 Aug 17 05:32
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_08-17-
2025_05.32.00.4493_databackup_3_1
SYSTEMDB:
total 3339236
drwxr-xr-- 2 ss1adm sapsys 4096 Aug 22 11:03 .
drwxr-xr-- 4 ss1adm sapsys 4096 Jul 27 2022 ..
-rw-r----- 1 ss1adm sapsys 163840 Aug 17 05:32 SnapCenter_SnapCenter_hana-
1_BlockIntegrityCheck_Weekly_08-17-2025_05.32.00.4493_databackup_0_1

-rw-r----- 1 ss1adm sapsys 3405787136 Aug 17 05:32
SnapCenter_SnapCenter_hana-1_BlockIntegrityCheck_Weekly_08-17-
2025_05.32.00.4493_databackup_1_1
```

Wiederherstellung und Datenrettung von SAP HANA-Datenbanken mit SnapCenter

Wiederherstellung und Instandsetzung von SAP HANA-Systemen mit SnapCenter mittels automatisierter oder manueller Wiederherstellungsoptionen. Dies umfasst vollständige

Systemwiederherstellungen, Wiederherstellungen einzelner Mandanten für HANA-Datenbanken auf ONTAP, Azure NetApp Files und FSx für ONTAP.

SnapCenter unterstützt die folgenden Wiederherstellungs- und Reparaturvorgänge.

- SAP HANA MDC-Systeme mit einem einzigen Mandanten
  - Vollständig automatisierte Wiederherstellung und Datenrettung
  - Vollständig automatisierte Wiederherstellung und manuelle Wiederherstellung (auswählbar)
- SAP HANA MDC-Systeme mit mehreren Mandanten
  - Die durchgängige automatisierte Wiederherstellung muss manuell durchgeführt werden.
- Wiederherstellung eines einzelnen Mandanten
  - Die durchgängige automatisierte Wiederherstellung muss manuell durchgeführt werden.

Die automatische Wiederherstellung wird nur unterstützt, wenn das HANA-Plug-in auf dem HANA-Datenbankhost bereitgestellt ist und das HANA-System von SnapCenter automatisch erkannt wurde. Bei einer zentralen Plug-in-Host-Konfiguration muss die Wiederherstellung nach dem Wiederherstellungsvorgang mit SnapCenter manuell durchgeführt werden.

Die Wiederherstellung vom primären ANF-Volume wird unterstützt. Die Wiederherstellung aus einem ANF-Backup wird noch nicht unterstützt. Eine Wiederherstellung direkt am Speicherort oder eine Wiederherstellung auf ein neues Volume aus einer ANF-Sicherung muss manuell über das Azure-Portal oder die CLI durchgeführt werden.

Automatisierte Wiederherstellung und Recovery für SAP HANA MDC-Systeme mit einem einzigen Mandanten

Ein Wiederherstellungsvorgang wird eingeleitet, indem in der Ressourcentopologieansicht eine Snapshot-Sicherung ausgewählt und anschließend auf „Wiederherstellen“ geklickt wird.

[Breite=601, Höhe=294]

Bei HANA-Systemen mit NFS on ANF, FSx for ONTAP oder ONTAP -Speichersystemen können Sie die vollständige Wiederherstellung mit oder ohne Wiederherstellung der primären Volume-Snapshots auswählen.

- Die vollständige Ressourcenwiederherstellung ohne Volumenrücksetzung verwendet Single File SnapRestore (SFSR), um alle Dateien der Datenbank wiederherzustellen.
- Die vollständige Ressource mit Volume-Wiederherstellung verwendet eine volumebasierte Wiederherstellungsoperation (VBSR), um das gesamte Volume auf den Zustand des ausgewählten Snapshots zurückzusetzen.

Die Funktion „Volume-Revert“ kann nicht verwendet werden, wenn Sie einen Snapshot wiederherstellen müssen, der älter ist als der aktive SnapVault oder SnapMirror -Replikations -Snapshot.

Bei einer Volume-Wiederherstellung werden alle Snapshot-Backups gelöscht, die neuer sind als der für die Wiederherstellung ausgewählte Snapshot.

Eine Wiederherstellung mit SFSR ist fast so schnell wie eine Volume-Wiederherstellung, blockiert jedoch alle Snapshot-Operationen, bis der Hintergrundprozess die Metadatenoperationen abgeschlossen hat.

[Breite=300]

Bei HANA-Systemen auf Bare-Metal-Hosts mit FC-SAN wird ein Volume Revert (VBSR) nicht unterstützt; stattdessen wird für den Wiederherstellungsvorgang immer SFSR verwendet. Für HANA-Systeme, die auf VMware mit VMFS laufen, wird ein Klon-, Mount- und Kopiervorgang verwendet.

[Breite=345, Höhe=325]

Für eine Wiederherstellung aus einer sekundären Sicherung müssen Sie den Archivspeicherort auswählen.

[Breite=345, Höhe=323]

Mit dem Wiederherstellungsbereich können Sie eine Wiederherstellung „zum letzten Zustand“, „zu einem bestimmten Zeitpunkt“ oder „zu einem Sicherungspunkt“ auswählen, ohne Protokollsicherungen zu verwenden. Wenn Sie „Keine Wiederherstellung“ auswählen, führt SnapCenter lediglich den Wiederherstellungsvorgang aus, die eigentliche Wiederherstellung muss jedoch wie beschrieben manuell durchgeführt werden. "Manuelle Wiederherstellung mit HANA Studio"Die

SnapCenter verwendet die in SAP HANA konfigurierten Pfade für die Speicherorte der Protokollsicherung und der Katalogsicherung. Wenn Sie gestaffelte Backups an einem zusätzlichen Speicherort haben, können Sie diese zusätzlichen Pfade hinzufügen.

[Breite=346, Höhe=324]

Optional können Sie Skripte für die Zeit vor und nach der Wiederherstellung hinzufügen.

[Breite=348, Höhe=326]

[Breite=359, Höhe=335]

Durch Klicken auf „Fertigstellen“ im Übersichtsbildschirm wird der Wiederherstellungs- und Instandsetzungsvorgang gestartet.

[Breite=361, Höhe=336]

Der Wiederherstellungs- und Instandsetzungsprozess lässt sich in drei Hauptabschnitte unterteilen.

- Herunterfahren des HANA-Systems
- Wiederherstellungsvorgang
  - Dateisystemspezifische Vorbereitungen, z. B. Aushängevorgang
  - Snapshot-Wiederherstellungsvorgang
  - Dateisystemspezifische Nachbearbeitungsoperationen, z. B. Mount-Operationen
- HANA-Wiederherstellung
  - Recovery der Systemdatenbank
  - Recovery von Mandanten-Datenbanken

[Breite=357, Höhe=439]

Manuelle Wiederherstellung mit HANA Studio

Um ein SAP HANA MDC-System mit einem oder mehreren Mandanten mithilfe von SAP HANA Studio und SnapCenter wiederherzustellen und zu sichern, führen Sie die folgenden Schritte aus:

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 aus und geben Sie den Speicherort des Sicherungskatalogs an.
   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, um Daten vom primären Speicher wiederherzustellen, oder „Vault-Kopien“, wenn Sie Daten von einem sekundären Sicherungsspeicher wiederherstellen 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.
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.
   c. Es wird eine Liste der Daten-Backups angezeigt. Da das Daten-Volume bereits wiederhergestellt ist, wird das Mandanten-Backup als verfügbar angezeigt (in grün).
   d. Wählen Sie dieses Backup aus, und starten Sie den Wiederherstellungsprozess. Nach Abschluss des Recovery-Prozesses wird die Mandantendatenbank automatisch gestartet.
5. Bei einem HANA-System mit mehreren Mandanten wiederholen Sie Schritt 4 für jeden Mandanten.

Eine manuelle Wiederherstellung mit SAP HANA Cockpit erfolgt mit den gleichen Schritten.

Im folgenden Abschnitt werden die Schritte der Wiederherstellungs- und Recovery-Operationen eines SAP HANA MDC-Systems mit einem einzelnen Mandanten beschrieben.

Wählen Sie in HANA Studio „Sicherung und Wiederherstellung“ und anschließend „Systemdatenbank wiederherstellen“.

[Breite=450, Höhe=368]

Bestätigen Sie den Herunterfahrvorgang; dies ist nur erforderlich, wenn das HANA-System noch läuft.

[Breite=349, Höhe=83]

Wiederherstellungsvorgang auswählen. In diesem Beispiel möchten wir zum letzten vorherigen Zustand zurückkehren.

[Breite=345, Höhe=359]

Geben Sie einen alternativen Speicherort für den Katalog an.

[Breite=343, Höhe=356]

HANA Studio listet die aktuellsten im HANA-Backup-Katalog gespeicherten Backups auf.

Es wird eine Liste der verfügbaren Backups basierend auf dem Inhalt des Backup-Katalogs angezeigt. Wählen Sie das gewünschte Backup aus und notieren Sie sich die externe Backup-ID: in diesem Beispiel das aktuellste Backup.

[Breite=391, Höhe=283]

Wählen Sie in der SnapCenter Benutzeroberfläche die Ressourcentopologieansicht und anschließend die wiederherzustellende Sicherung aus, in diesem Beispiel die aktuellste primäre Sicherung. Klicken Sie auf das Symbol „Wiederherstellen“, um die Wiederherstellung zu starten.

[Breite=601, Höhe=294]

Der SnapCenter -Wiederherstellungsassistent wird gestartet. Wählen Sie als Wiederherstellungstyp „Vollständige Ressourcen- und Volumenwiederherstellung“, um eine volumenbasierte Wiederherstellung durchzuführen.

[Breite=346, Höhe=325]

Wählen Sie „Keine Wiederherstellung“, um die Wiederherstellungsvorgänge vom SnapCenter -Workflow auszuschließen.

[Breite=358, Höhe=336]

Klicken Sie auf Fertigstellen, um den Wiederherstellungsvorgang zu starten.

[Breite=361, Höhe=339]

SnapCenter führt jetzt den Wiederherstellungsvorgang aus.

- Dateisystemspezifische Vorbereitungen, z. B. Aushängevorgang
- Snapshot-Wiederherstellungsvorgang
- Dateisystemspezifische Nachbearbeitungsoperationen, z. B. Mount-Operationen

[Breite=322, Höhe=398]

Wenn der Snapshot von SnapCenter wiederhergestellt wurde, ist eine snapshot_databackup_0_1-Datei im Unterverzeichnis system and tenant database des HANA-Datenvolumes verfügbar. Diese Datei wurde von der HANA-Datenbank während der Erstellung des HANA-Datenbank-Snapshots erstellt. HANA löscht die Datei, sobald der Sicherungsvorgang abgeschlossen ist, sodass die Dateien nur noch innerhalb der Snapshot-Sicherung sichtbar sind. Diese Dateien werden für jede Wiederherstellungsoperation benötigt. Nach der Wiederherstellung werden die Dateien von der HANA-Datenbank gelöscht.

```
hana-1:~ # cd /hana/data/SS1/mnt00001/
hana-1:/hana/data/SS1/mnt00001 # ls -al *
-rw-r--r-- 1 ss1adm sapsys 16 Aug 26 06:00 nameserver.lck
hdb00001:
total 4992236
drwxr-x--- 2 ss1adm sapsys 4096 Aug 26 06:00 .
drwxr-x--- 5 ss1adm sapsys 4096 Aug 26 06:00 ..
-rw-r----- 1 ss1adm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 ss1adm sapsys 5100273664 Aug 26 06:00 datavolume_0000.dat
-rw-r----- 1 ss1adm sapsys 36 Aug 25 10:30 landscape.id
-rw-r----- 1 ss1adm sapsys 163840 Aug 26 06:00 snapshot_databackup_0_1
hdb00002.00003:
total 201420
drwxr-xr-- 2 ss1adm sapsys 4096 Nov 3 2020 .
drwxr-x--- 5 ss1adm sapsys 4096 Aug 26 06:00 ..
-rw-r--r-- 1 ss1adm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r--r-- 1 ss1adm sapsys 335544320 Aug 26 06:00 datavolume_0000.dat
hdb00003.00003:
total 4803140
drwxr-xr-- 2 ss1adm sapsys 4096 Aug 26 06:00 .
drwxr-x--- 5 ss1adm sapsys 4096 Aug 26 06:00 ..
-rw-r--r-- 1 ss1adm sapsys 0 Nov 3 2020
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r--r-- 1 ss1adm sapsys 4898947072 Aug 26 06:00 datavolume_0000.dat
-rw-r----- 1 ss1adm sapsys 159744 Aug 26 06:00 snapshot_databackup_0_1
hana-1:/hana/data/SS1/mnt00001 #
```

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 nun in der Backup-Liste mit einem grünen Symbol angezeigt. Wählen Sie die Sicherung aus und klicken Sie auf Weiter.

[Breite=400, Höhe=290]

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

SAP HANA Studio verwendet die in SAP HANA konfigurierten Pfade für die Speicherorte der Protokollsicherung und der Katalogsicherung. Wenn Sie gestaffelte Backups an einem zusätzlichen Speicherort haben, können Sie diese zusätzlichen Pfade hinzufügen.

[Breite=465, Höhe=296]

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

[Breite=466, Höhe=296]

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

Durch Klicken auf „SQL-Anweisung anzeigen“ zeigt HANA Studio den SQL-Befehl an, der für den Wiederherstellungsvorgang ausgeführt wird.

[Breite=464, Höhe=295]

Der Genesungsprozess beginnt. Warten Sie, bis die Wiederherstellung der Systemdatenbank abgeschlossen ist.

[Breite=376, Höhe=239]

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

[Breite=476, Höhe=315]

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

[Breite=342, Höhe=355]

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

[Breite=343, Höhe=356]

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

[Breite=342, Höhe=355]

Bestätigen Sie, dass die Mandantendatenbank heruntergefahren wurde.

[Breite=348, Höhe=85]

Da die Wiederherstellung des Datenvolumens vor der Wiederherstellung der Systemdatenbank erfolgte, ist die Mandantensicherung sofort verfügbar. Wählen Sie die grün markierte Sicherung aus und klicken Sie auf Weiter.

[Breite=433, Höhe=349]

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

> SAP HANA Studio verwendet die in SAP HANA konfigurierten Pfade für die Speicherorte der Protokollsicherung und der Katalogsicherung. Wenn Sie gestaffelte Backups an einem zusätzlichen Speicherort haben, können Sie diese zusätzlichen Pfade hinzufügen.

[Breite=384, Höhe=310]

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

[Breite=384, Höhe=310]

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

Durch Klicken auf „SQL-Anweisung anzeigen“ zeigt HANA Studio den SQL-Befehl an, der für den Wiederherstellungsvorgang ausgeführt wird.

[Breite=380, Höhe=307]

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

[Breite=378, Höhe=305]

Sobald die Mandantenwiederherstellung abgeschlossen ist, ist das SAP HANA-System betriebsbereit.

Bei einem SAP HANA MDC-System mit mehreren Mandanten muss die Mandantenwiederherstellung für jeden Mandanten wiederholt werden.

Manuelle Wiederherstellung mit SQL-Befehlen

Sie können auch SQL-Anweisungen zur Wiederherstellung des HANA-Systems verwenden.

Zuerst müssen Sie die Systemdatenbank wiederherstellen.

```
HDBSettings.sh recoverSys.py --command="RECOVER DATABASE UNTIL TIMESTAMP
'2026-08-26 10:55:49' USING CATALOG PATH ('mnt/log-backup/SYSTEMDB') USING
LOG PATH ('mnt/log-backup/SYSTEMDB') USING SNAPSHOT"
```

Als zweiten Schritt müssen Sie eine Verbindung zur Systemdatenbank herstellen und die Wiederherstellung der Mandantendatenbank(en) starten. In diesem Beispiel ist die Mandantendatenbank SS1.

```
hdbsql SYSTEMDB=> RECOVER DATABASE FOR SS1 UNTIL TIMESTAMP '2026-08-26
10:55:49' USING CATALOG PATH ('mnt/log-backup/DB_SS1') USING LOG PATH
('mnt/log-backup/DB_SS1') USING SNAPSHOT
```

Wiederherstellung und Recovery für einzelne Mandanten

Die Wiederherstellung und der Recovery-Vorgang für einen einzelnen Mandanten mit SnapCenter ähneln sehr dem im vorherigen Thema beschriebenen Workflow. "Manuelle Wiederherstellung mit HANA Studio"Die

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 „Mandantendatenbank wiederherstellen“ und bestätigen Sie das Herunterfahren der Mandantendatenbank.
   b. Wählen Sie den Wiederherstellungstyp aus und geben Sie den Speicherort des Sicherungskatalogs an.
   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, um Daten vom primären Speicher wiederherzustellen, oder „Vault-Kopien“, wenn Sie Daten von einem sekundären Sicherungsspeicher wiederherstellen 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 des Mandanten.

3. Führen Sie den Recovery-Prozess für die Mandantendatenbank 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 Mandantendatenbank gestartet.

Wiederherstellung von Nicht-Datenvolumes

Ein Wiederherstellungsvorgang für ein Nicht-Datenvolume wird gestartet, indem in der Topologieansicht der Nicht-Datenvolume-Ressource eine Snapshot-Sicherung ausgewählt und anschließend auf „Wiederherstellen“ geklickt wird.

[Breite=601, Höhe=294]

Bei Nicht-Datenvolumes mit NFS kann eine vollständige Ressourcenwiederherstellung (VBSR) oder eine Wiederherstellung auf Dateiebene (SFSR) ausgewählt werden. Bei der Wiederherstellung auf Dateiebene können entweder alle oder einzelne Dateien für den Wiederherstellungsvorgang definiert werden.

[Breite=369, Höhe=344]

Erweiterte SnapCenter Optionen für SAP HANA konfigurieren

Konfigurieren Sie erweiterte SnapCenter -Einstellungen für SAP HANA-Umgebungen, einschließlich der Unterdrückung von VMware-Warnmeldungen für NFS-Mounts im Gastsystem, der Deaktivierung der automatischen Protokollsicherungsverwaltung und der Aktivierung der SSL-Verschlüsselung für HANA-Datenbankverbindungen.

Warnmeldung bei virtualisierten Umgebungen und Gast-Mounts

Bei der Verwendung von beispielsweise VMware mit NFS-Einbindungen im Gastsystem gibt SnapCenter eine Warnmeldung aus, dass das SnapCenter VMware-Plug-in verwendet werden sollte. Da das VMware-Plug-in für In-Guest-Mounts nicht erforderlich ist, kann die Warnmeldung ignoriert und deaktiviert werden. Um SnapCenter so zu konfigurieren, dass diese Warnung unterdrückt wird, 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.

[Breite=601, Höhe=176]

Deaktivieren der automatischen Backup-Organisation für Protokolle

Die Protokollsicherungsverwaltung ist standardmäßig aktiviert und kann auf Hostebene des HANA-Plug-ins deaktiviert werden. Verwenden Sie den PowerShell-Befehl:

Der Befehl Set-SmConfigSettings -Plugin -HostName <pluginhostname> -PluginCode hana -configSettings @{"LOG_CLEANUP_DISABLE" = "Y"} deaktiviert die Protokollsicherungsverwaltung für diesen SAP HANA-

Host.

Sichere Kommunikation mit HANA-Datenbank ermöglichen

Wenn die HANA-Datenbanken für eine sichere Kommunikation konfiguriert sind, muss der von SnapCenter ausgeführte hdbsql-Befehl zusätzliche Befehlszeilenoptionen verwenden.

Es gibt verschiedene Möglichkeiten, die SSL-Kommunikation zu konfigurieren. Standardmäßig verwendet SnapCenter die Befehlszeilenoption -e ssltrustcert hdbsql. Mit dieser Option wird SSL-Kommunikation ohne Serverzertifikatsvalidierung durchgeführt. Diese Option funktioniert auch für HANA-Systeme, bei denen SSL nicht aktiviert ist.

Wenn eine Zertifikatsvalidierung auf Server- und/oder Clientseite erforderlich ist, werden unterschiedliche hdbsql-Befehlszeilenoptionen benötigt, und Sie müssen die PSE-Umgebung entsprechend konfigurieren, wie im SAP HANA Security Guide beschrieben.

Dies kann durch die Verwendung eines Wrapper-Skripts erreicht werden, das hdbsql mit den erforderlichen Optionen aufruft. Anstatt die hdbsql-Executable in den hana.properties-Dateien zu konfigurieren, wird das Wrapper-Skript hinzugefügt.

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

Das Wrapper-Skript hdbsqls ruft hdbsql mit den erforderlichen Befehlszeilenoptionen auf.

```
#/bin/bash
/usr/sap/SM1/HDB12/exe/hdbsql <command line options> $*
```

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

Um die automatische Erkennung auf dem HANA-Plug-in-Host zu deaktivieren, führen Sie die folgenden Schritte aus:

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

Für einen HANA-Host hana-2 lautet der Befehl 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>

Verify the configuration by running the Get- SmConfigSettings command.

PS C:\Users\administrator.SAPCC> Get-SmConfigSettings -Agent -Hostname
hana-2 -key all

Key: CUSTOMPLUGINS_OPERATION_TIMEOUT_IN_MSEC Value: 3600000 Details: Plug-
in API operation Timeout

Key: CUSTOMPLUGINS_HOSTAGENT_TO_SERVER_TIMEOUT_IN_SEC Value: 1800 Details:
Web Service API Timeout

Key: CUSTOMPLUGINS_ALLOWED_CMDS Value: *; Details: Allowed Host OS
Commands

Key: DISABLE_AUTO_DISCOVERY Value: true Details:

Key: PORT Value: 8145 Details: Port for server communication

PS C:\Users\administrator.SAPCC>
```

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 #
```

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

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.

Autor: Nils Bauer, NetApp

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.

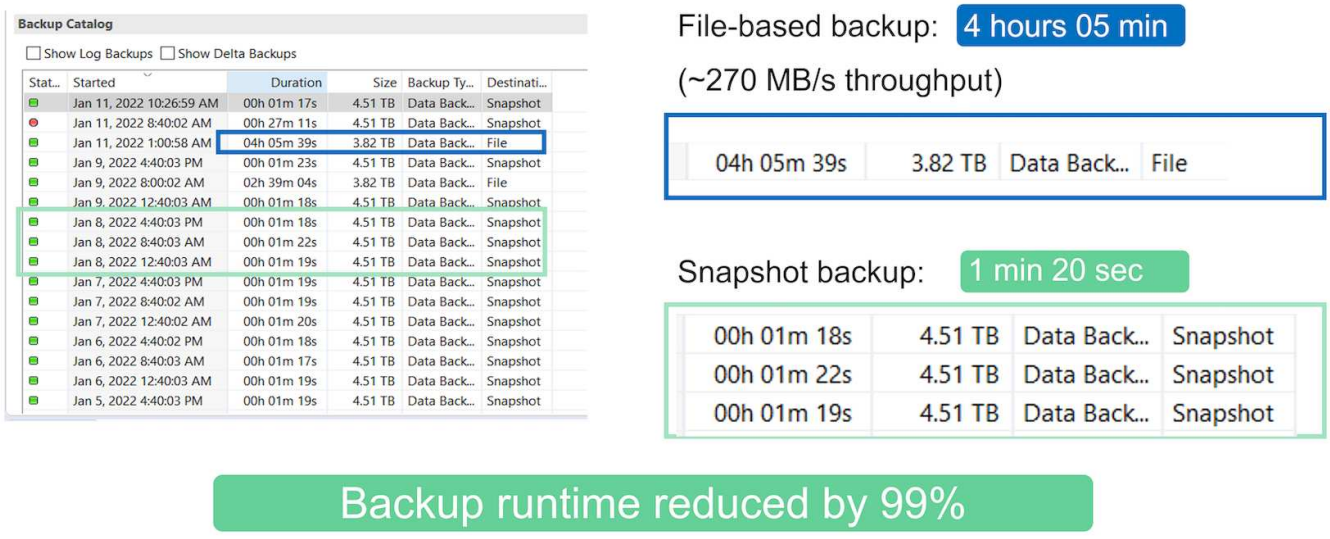
Ein Backup an einen sekundären Standort basiert auf Snapshot-Kopien, die auf dem primären Storage erstellt wurden. Somit werden die Daten direkt aus dem primären Storage-System eingelesen, ohne dass dabei der SAP Datenbankserver belastet wird. Der primäre Storage kommuniziert direkt mit dem sekundären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

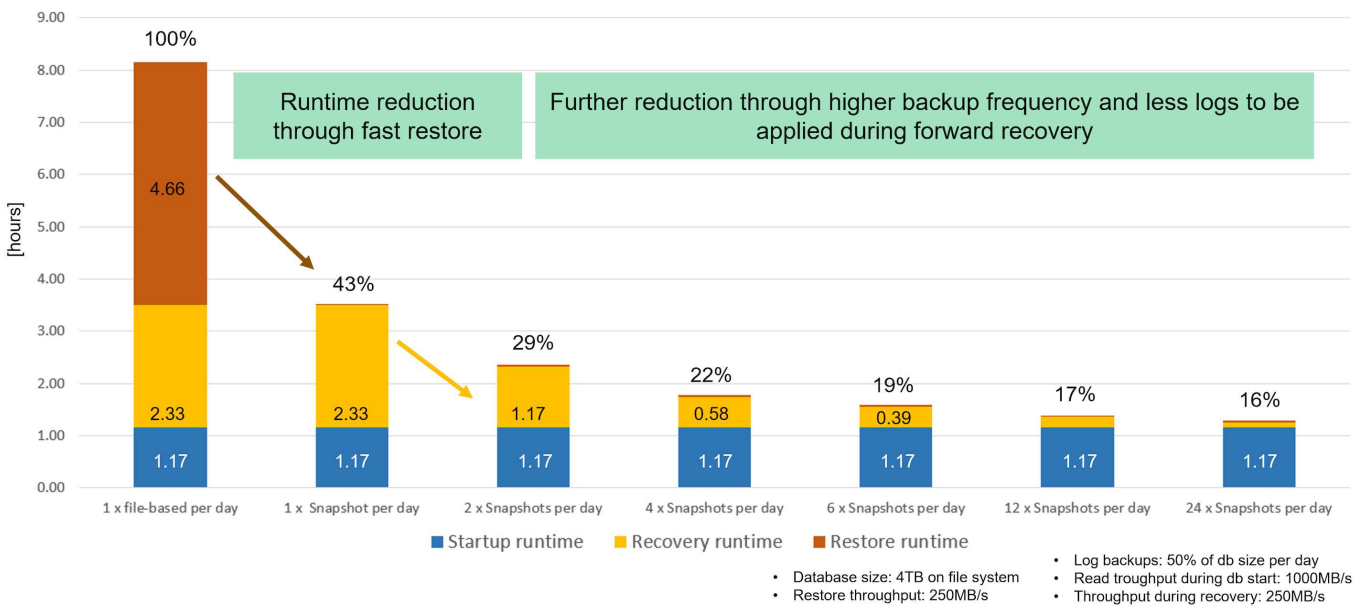
Bei dateibasierten Daten-Backups wird der Backup-Zeitplan normalerweise einmal pro Tag erstellt. Eine höhere Backup-Frequenz ist normalerweise nicht möglich, da das Backup die Produktions-Performance beeinträchtigt. Daher müssen im schlimmsten Fall alle Protokolle, die während des Tages geschrieben wurden,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



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.

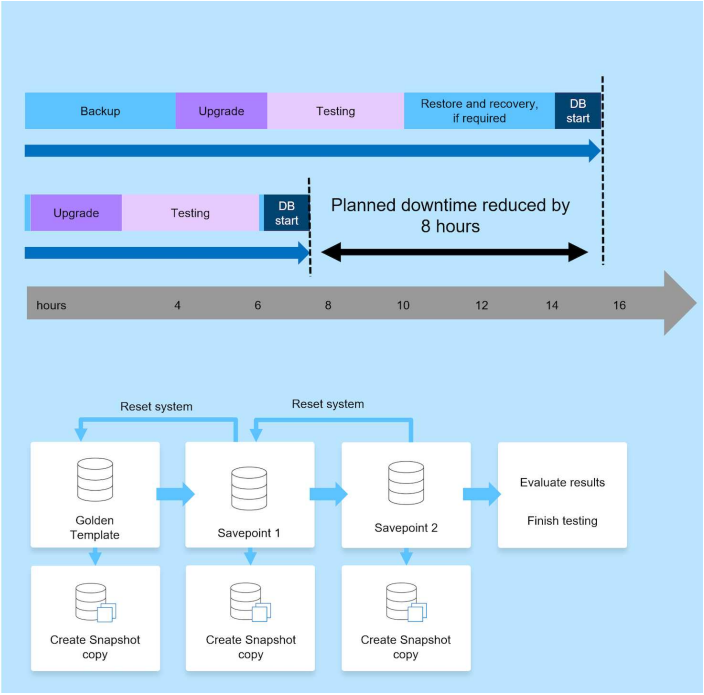
Ein SAP HANA System-Upgrade ist ein Beispiel dafür, wo ein On-Demand-Backup vor dem Upgrade und ein möglicher Restore-Vorgang, wenn das Upgrade fehlschlägt, eine erhebliche Auswirkung auf die gesamte geplante Ausfallzeit hat. Wenn Sie beispielsweise eine Datenbank mit 4 TB verwenden, können Sie die geplanten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

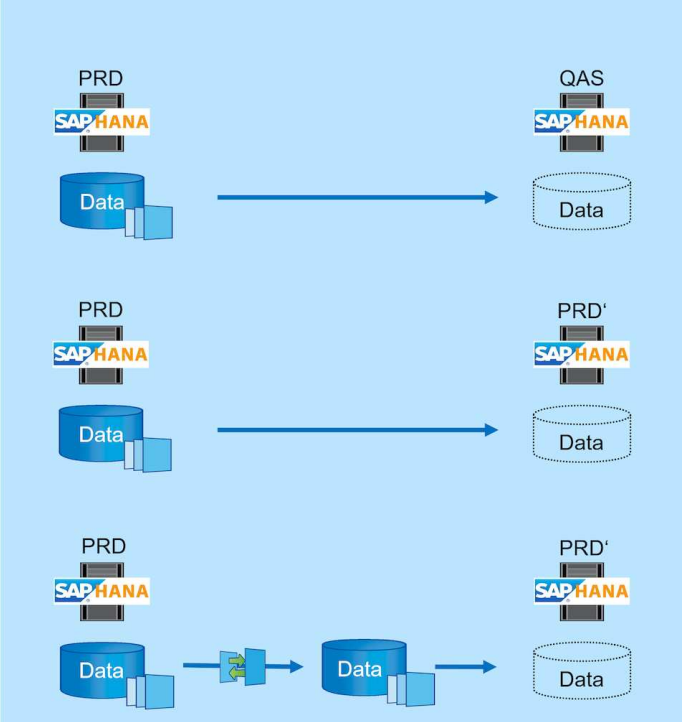
Der beliebteste Anwendungsfall ist SAP Systemaktualisierung, in dem Daten aus dem Produktionssystem in das Test- oder QA-System kopiert werden müssen. Mit der Klonfunktion von FSX für ONTAP lässt sich das Volume für das Testsystem von jeder beliebigen Snapshot Kopie des Produktionssystems in Sekundenschnelle 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



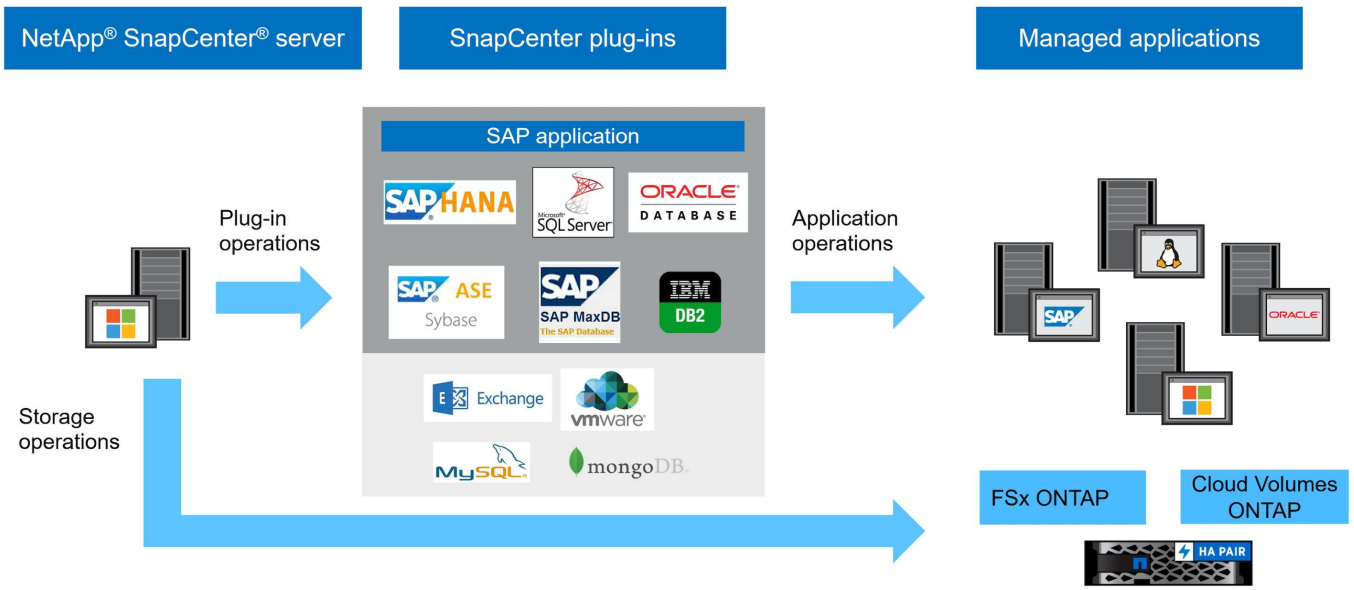
Architektur von SnapCenter

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.

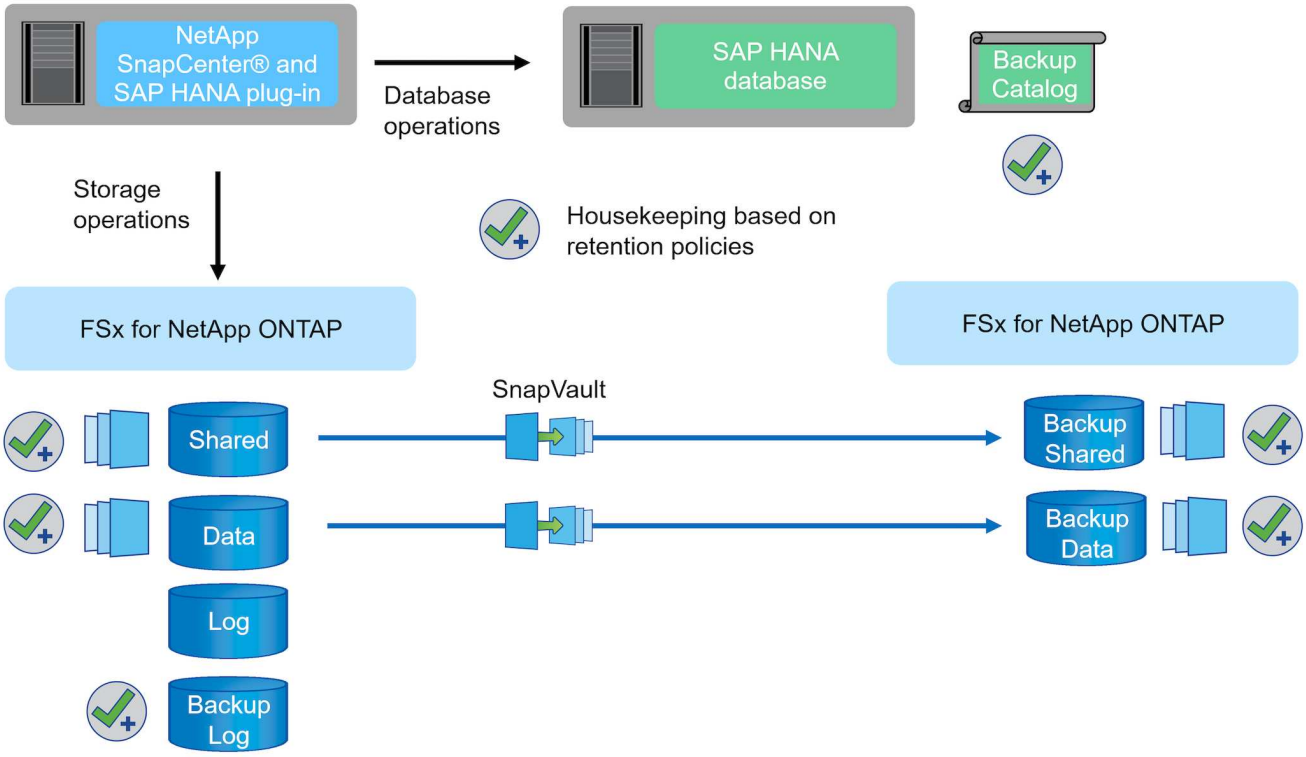
SnapCenter ermöglicht die Replizierung konsistenter Datenbank-Images auf einen externen Backup- oder Disaster-Recovery-Standort mithilfe von SnapVault oder der SnapMirror Funktion. In der Regel werden verschiedene Aufbewahrungsrichtlinien für Backups auf dem primären und externen Backup-Storage definiert.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

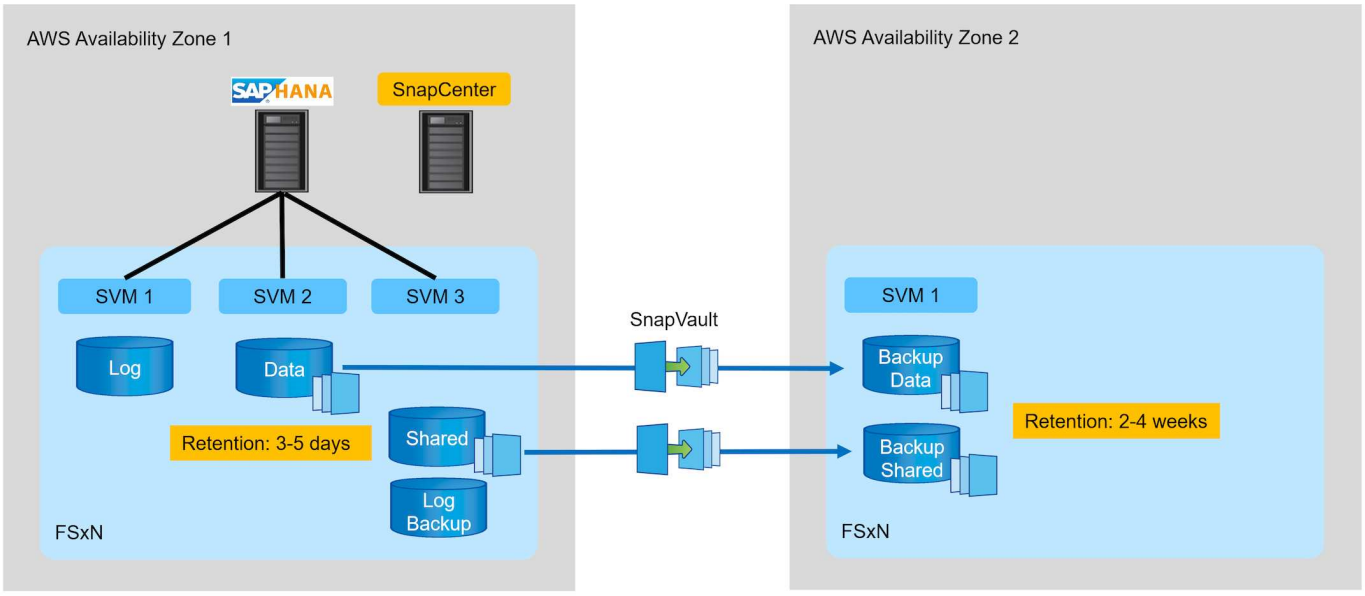
Inhalt des vorliegenden Dokuments

Dieses Dokument beschreibt die am häufigsten verwendete SnapCenter -Konfigurationsoption für ein SAP HANA MDC-Einzelhostsystem mit einem einzigen Mandanten auf FSx für ONTAP. Weitere Konfigurationsoptionen sind möglich und in einigen Fällen für bestimmte SAP HANA-Systeme erforderlich, beispielsweise für ein Multi-Host-System. Eine detaillierte Beschreibung weiterer Konfigurationsoptionen finden Sie unter "SnapCenter-Konzepte und Best Practices (netapp.com)"Die

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:

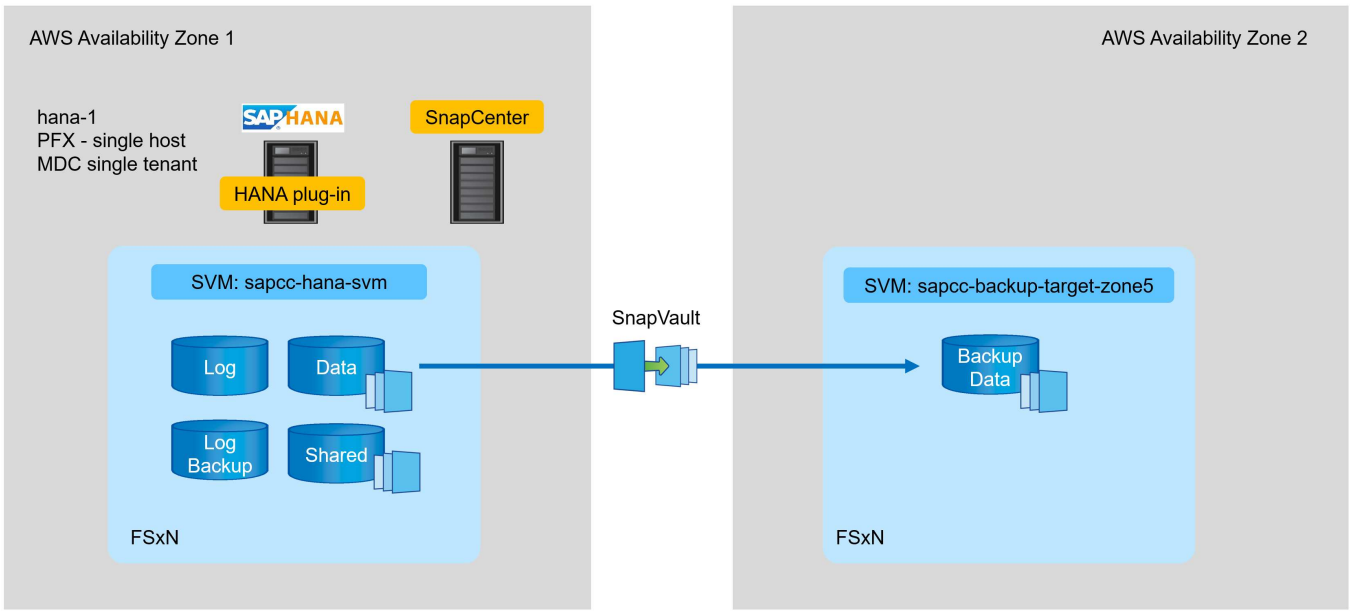
- Ein Host-MDC-System mit einem einzelnen Mandanten
- HANA 2.0 SPS 6, Version 60
- SLES FÜR SAP 15SP3

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

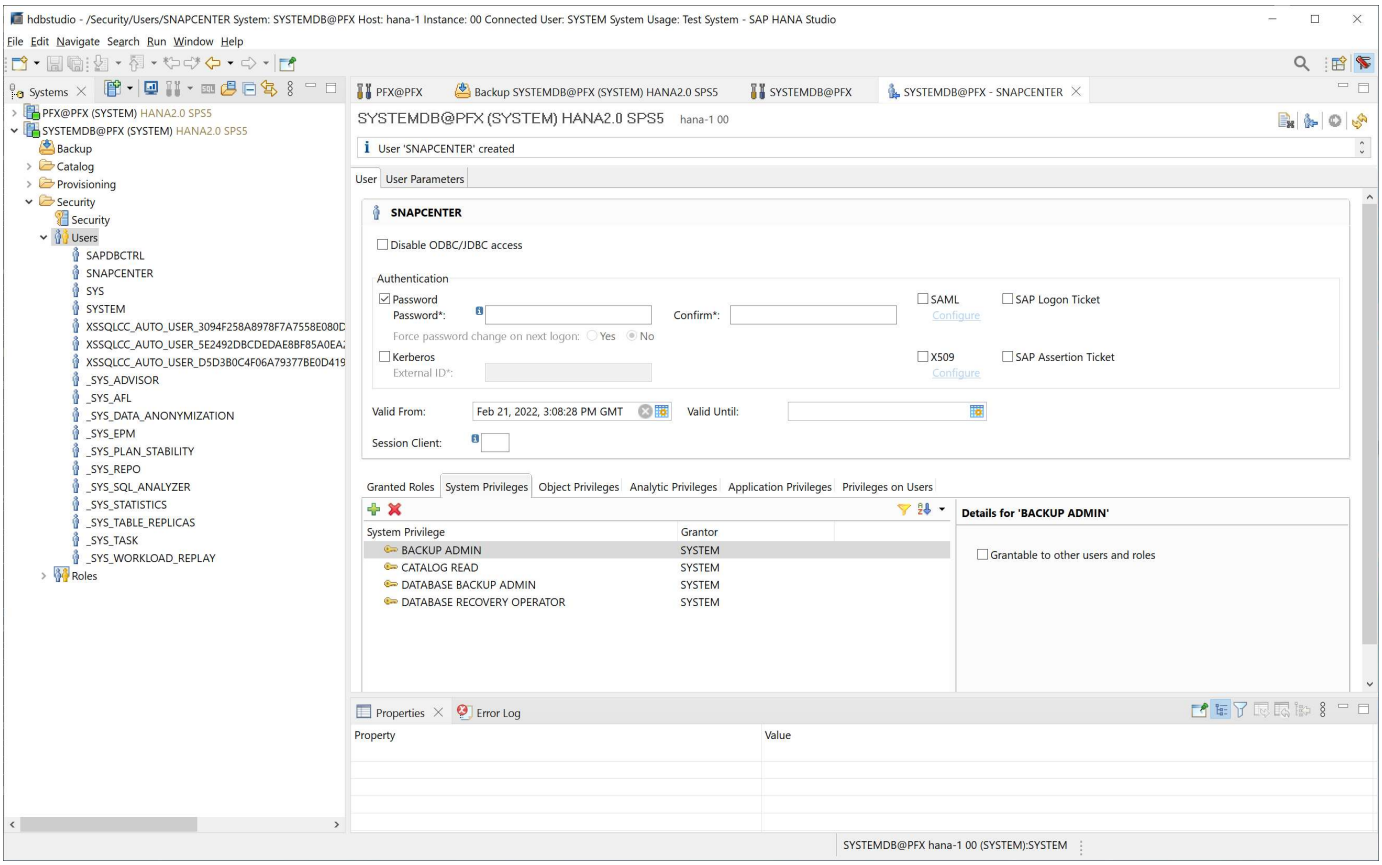
SAP HANA Backup-Benutzer und hdbuserstore-Konfiguration

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.
```

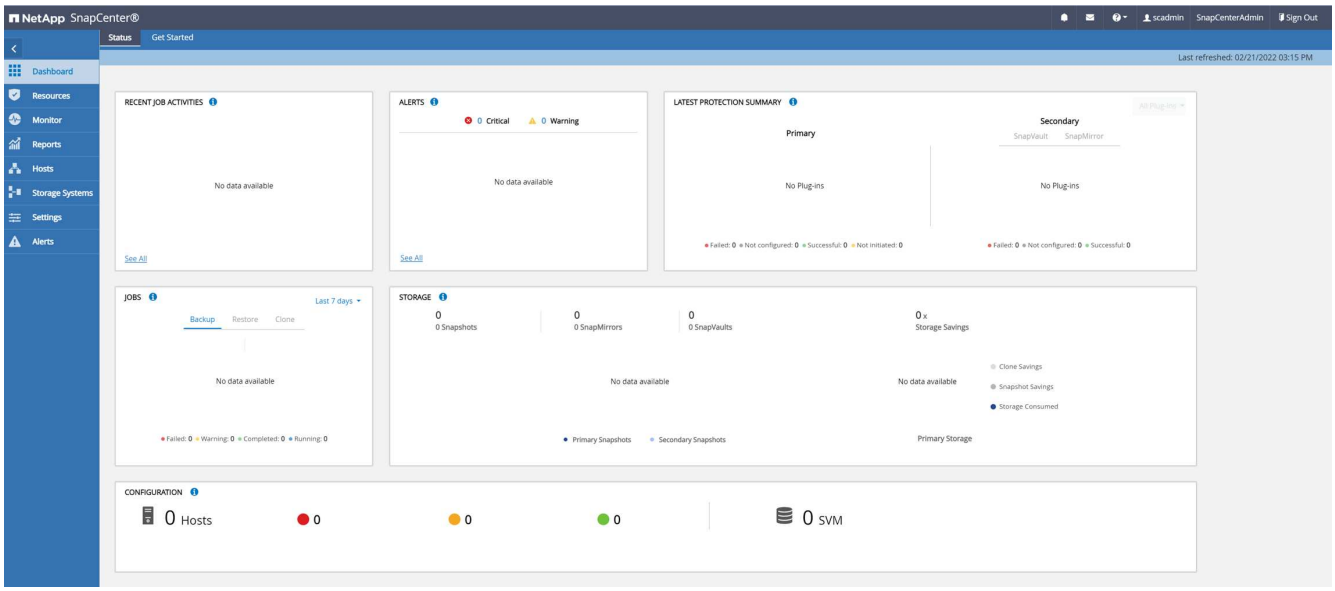
Sie können den Zugriff auf die HANA-Systemdatenbank prüfen, die den Schlüssel mit dem verwendet `hdbsql` Befehl.

```
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=>
```

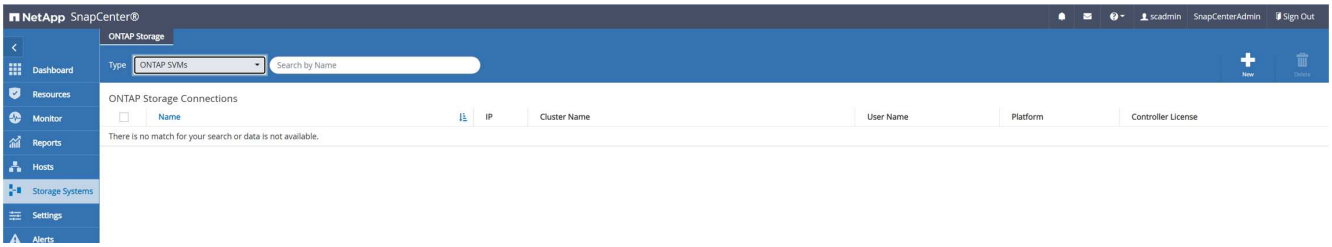
Speicher konfigurieren

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

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

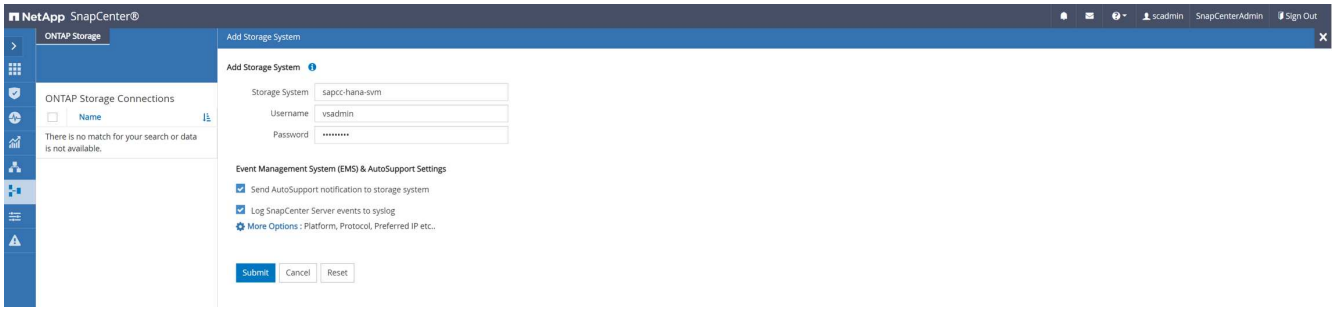


Sie können den Storage-Systemtyp auswählen, der ONTAP SVMs oder ONTAP Cluster sein kann. Im folgenden Beispiel ist das SVM-Management ausgewählt.

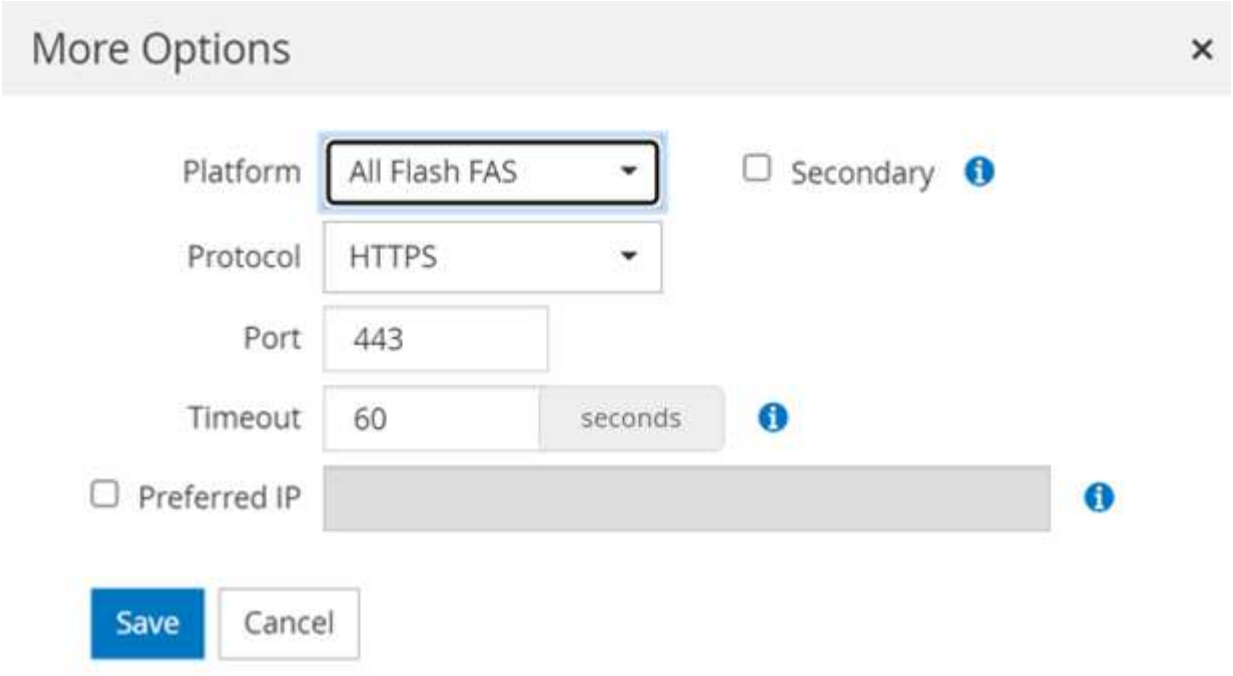


2. Klicken Sie auf Neu, um ein Speichersystem hinzuzufügen und den erforderlichen Hostnamen und die Anmeldeinformationen anzugeben.

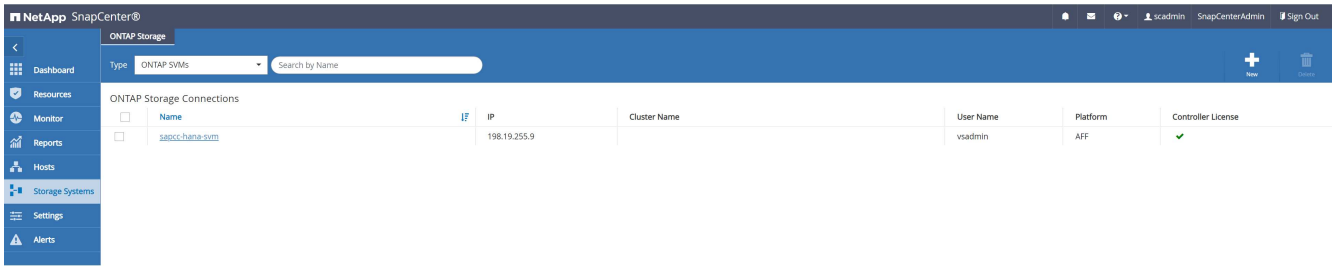
   Der SVM-Benutzer muss nicht wie in der folgenden Abbildung dargestellt vsadmin verwendet werden. In der Regel wird ein Benutzer für die SVM konfiguriert und den erforderlichen Berechtigungen zum Ausführen von Backup- und Restore-Vorgängen zugewiesen. Informationen zu erforderlichen Berechtigungen finden 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.



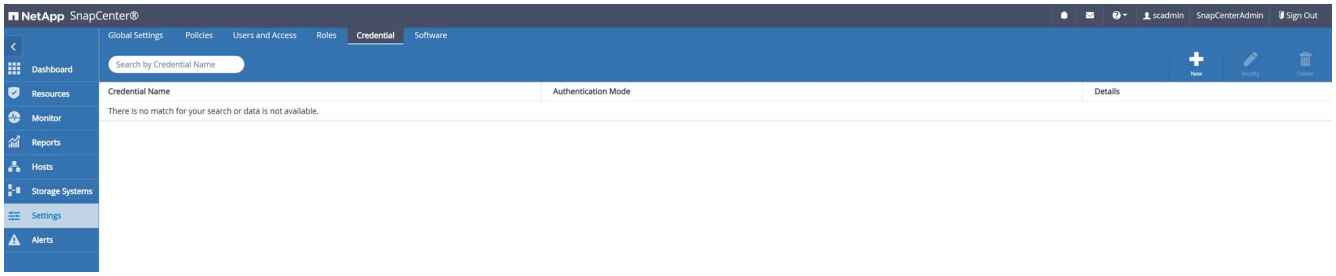
Der SVM `sapcc-hana-svm` Ist jetzt in SnapCenter konfiguriert.



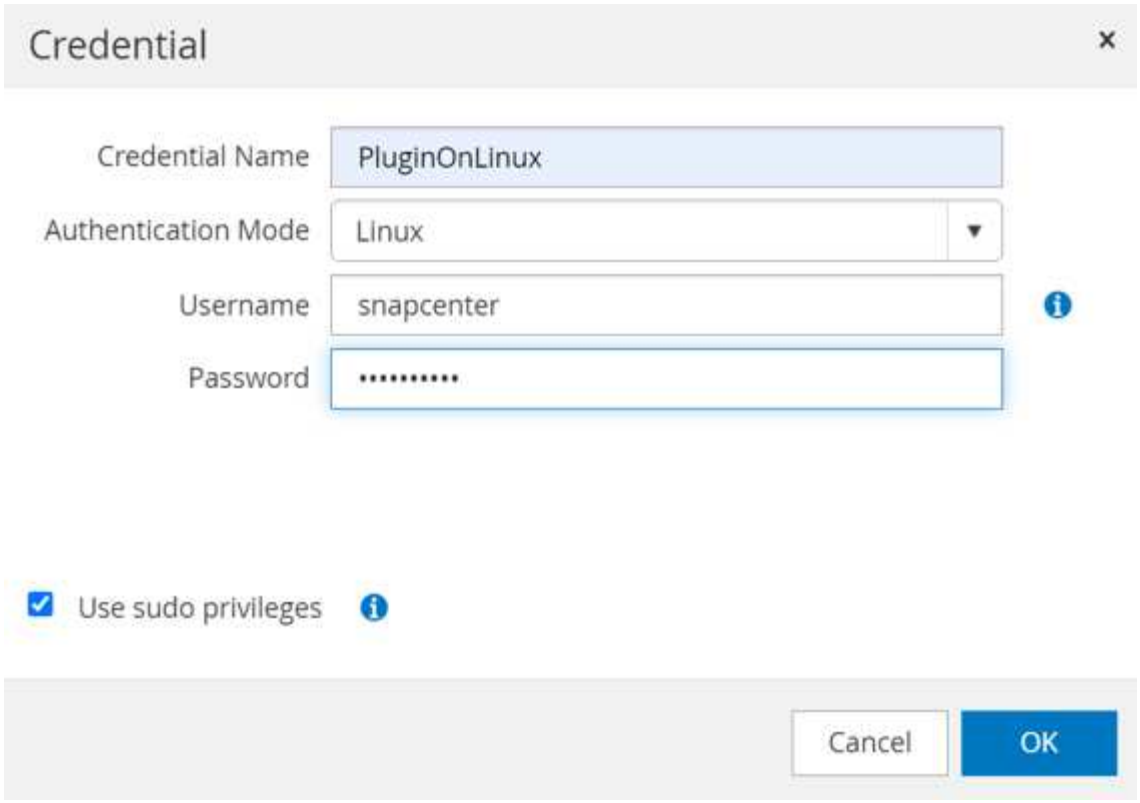
Anmeldedaten für Plug-in-Implementierung erstellen

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.

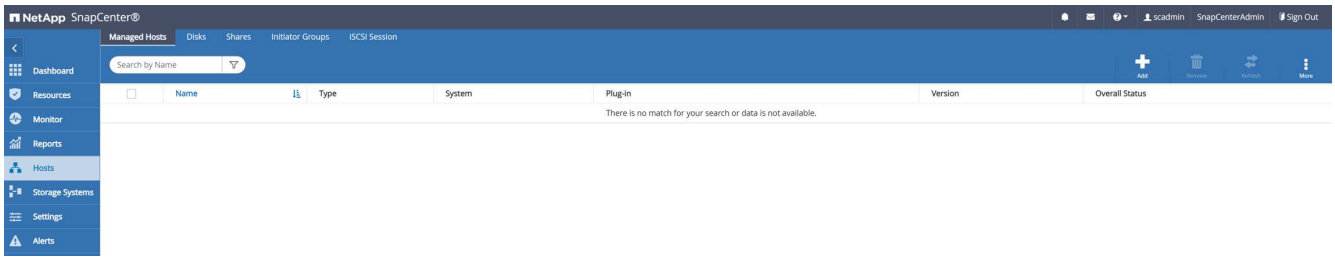
Für das SAP HANA Plug-in ist Java 64-Bit Version 1.8 erforderlich. Java muss auf dem Host installiert sein, bevor der Host zu SnapCenter hinzugefügt wird.

```
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 #
```

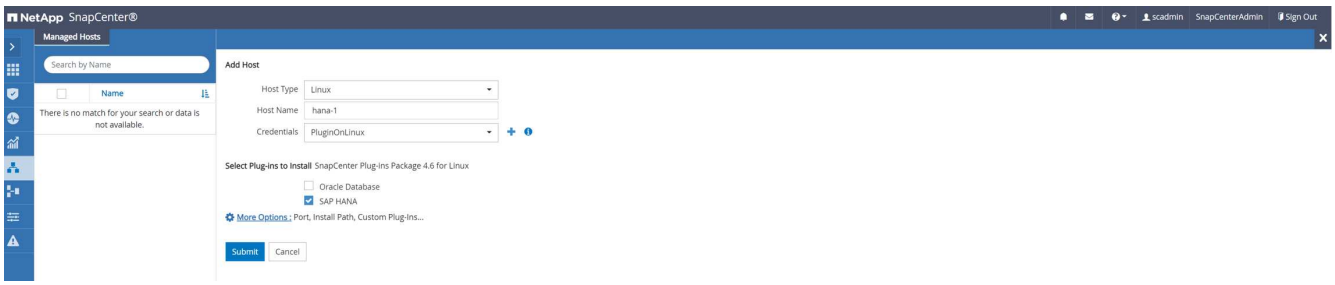
OpenJDK oder Oracle Java wird mit SnapCenter unterstützt.

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

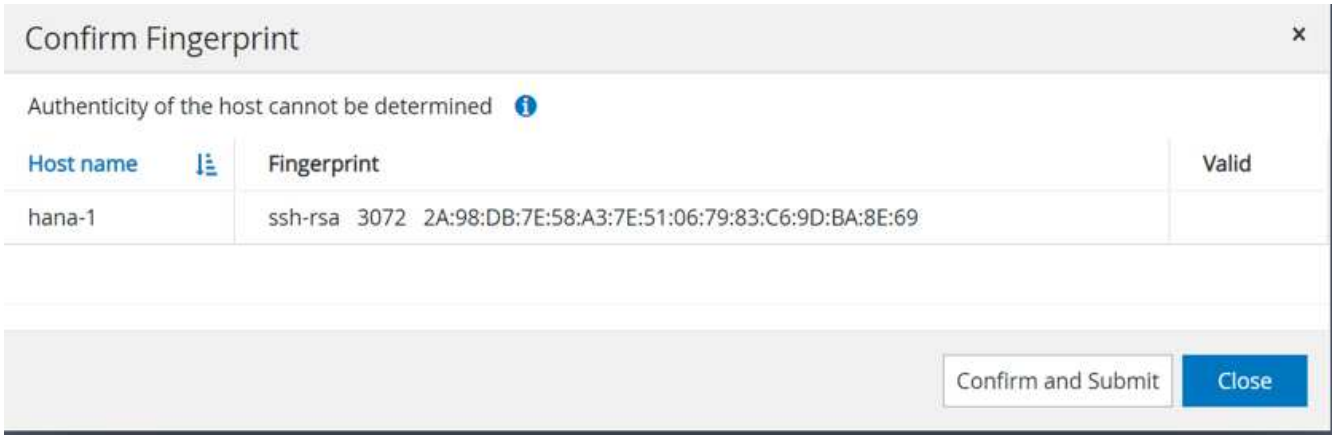
1. Klicken Sie auf der Registerkarte Host auf Hinzufügen.



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

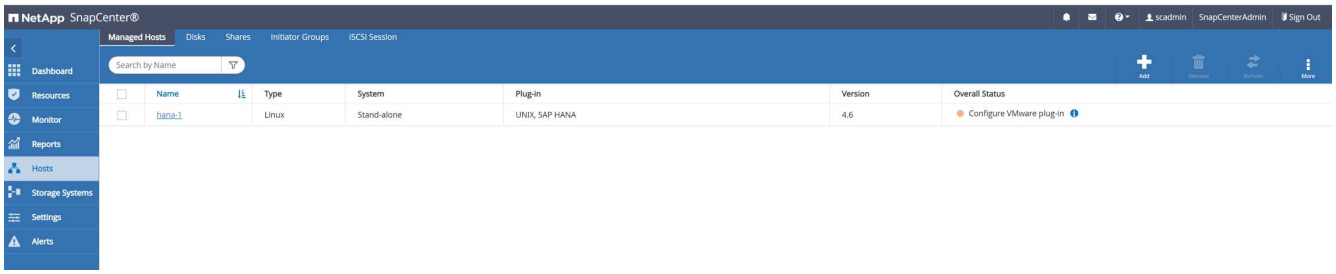


3. Bestätigen Sie den Fingerabdruck.



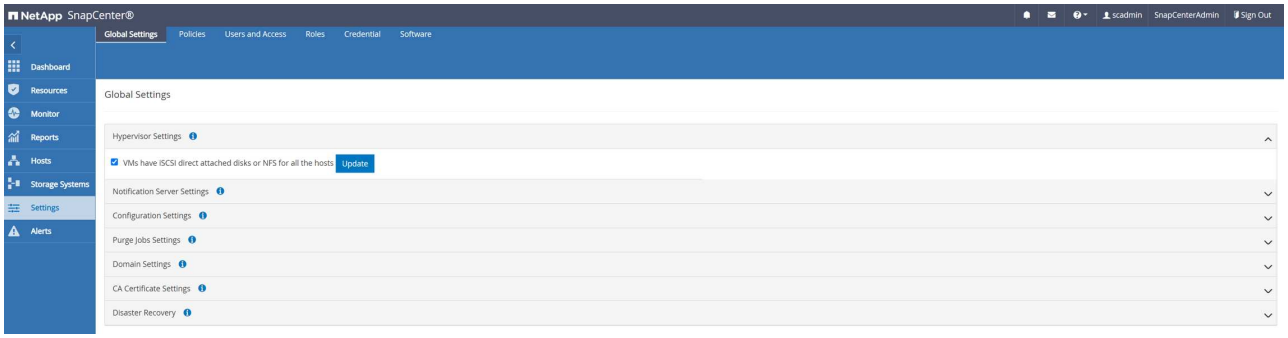
Die Installation des HANA und des Linux Plug-ins wird automatisch gestartet. Nach Abschluss der Installation wird in der Statusspalte des Hosts das VMware Plug-in konfigurieren angezeigt. SnapCenter erkennt, ob das SAP HANA Plug-in in in einer virtualisierten Umgebung installiert ist. Dabei kann es sich 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.

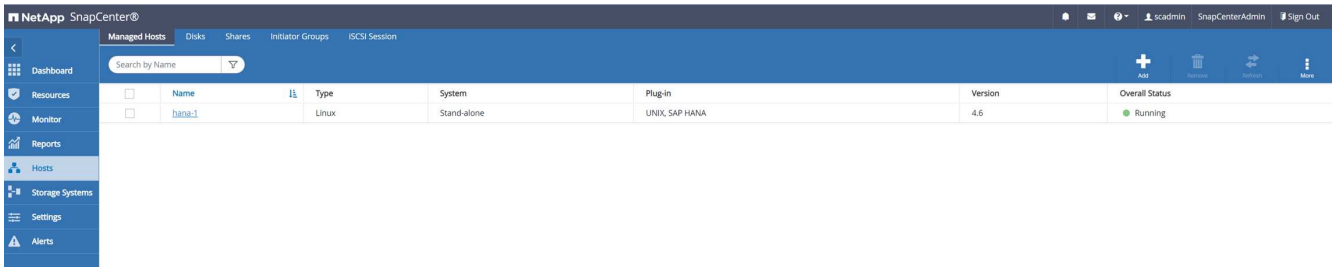


a. Wählen Sie auf der Registerkarte Einstellungen die Option Globale Einstellungen.

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:

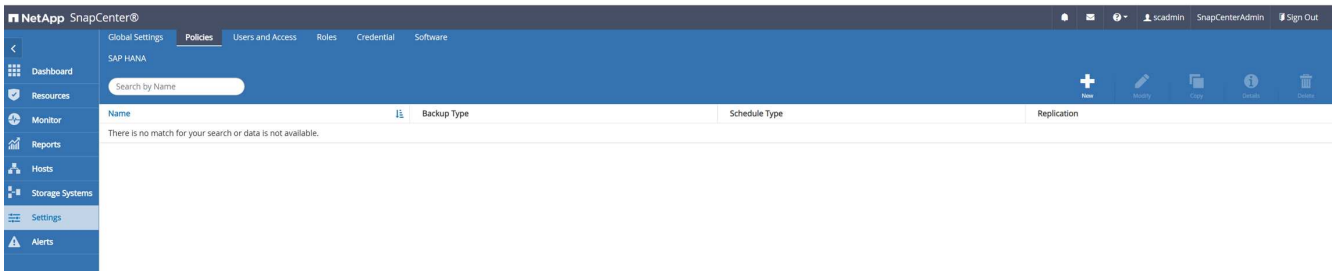
- Richtlinie für stündliche Backups ohne Replikation: `LocalSnap`.
- Richtlinie für wöchentliche Blockintegritätsprüfung über ein dateibasiertes Backup: `BlockIntegrityCheck`.

In den folgenden Abschnitten wird die Konfiguration dieser Richtlinien beschrieben.

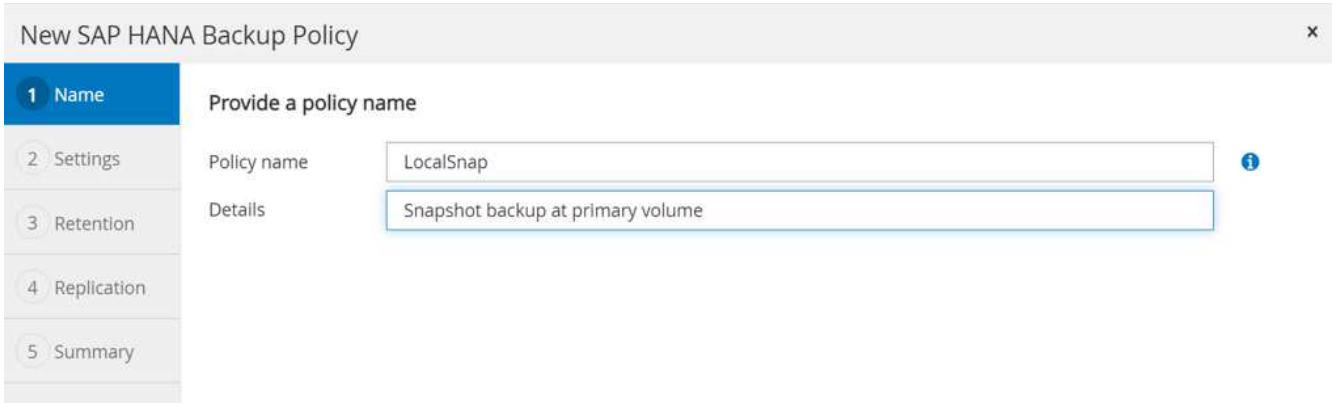
Richtlinien für Snapshot-Backups

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

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

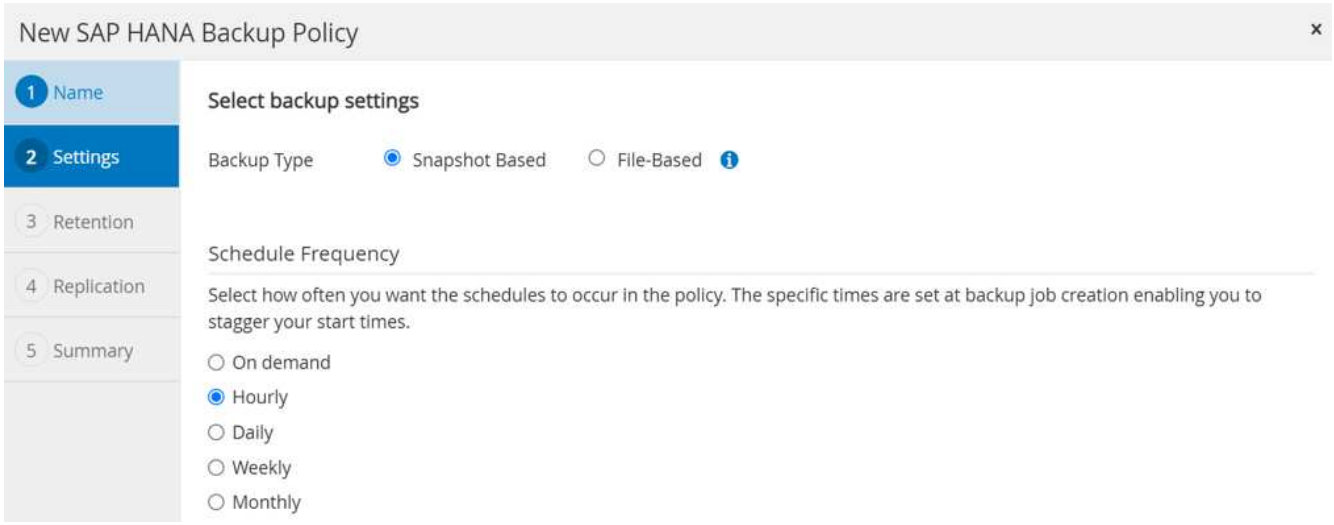


2. Geben Sie den Namen und die Beschreibung der Richtlinie ein. Klicken Sie Auf Weiter.

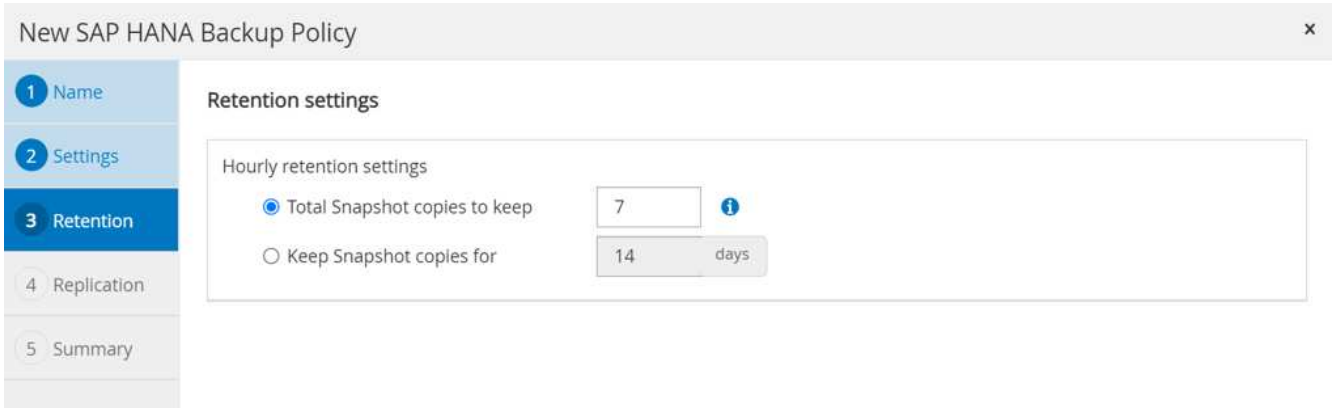


3. Wählen Sie den Backup-Typ als Snapshot-basiert aus und wählen Sie stündlich für die Zeitplanfrequenz aus.

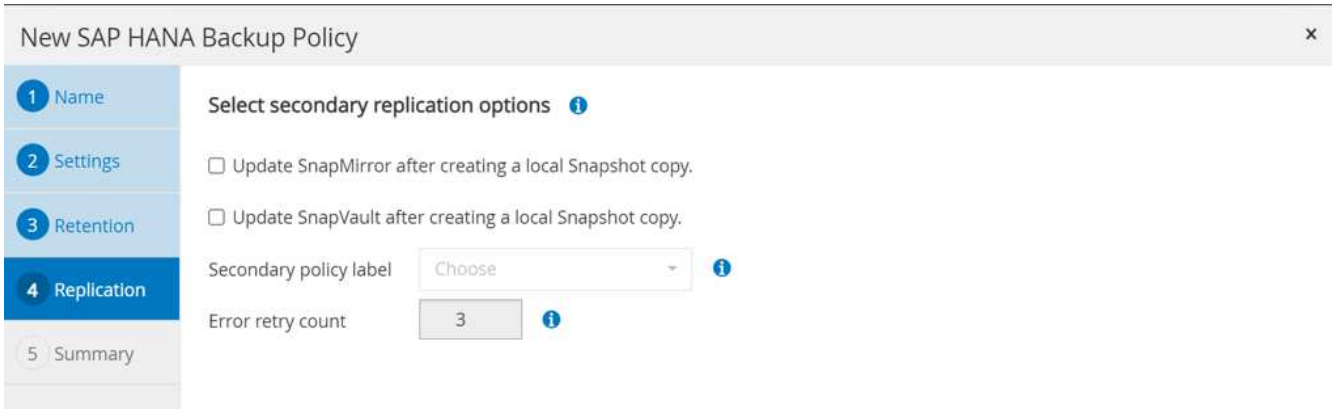
   Der Zeitplan selbst wird später mit der HANA-Ressourcenschutzkonfiguration konfiguriert.

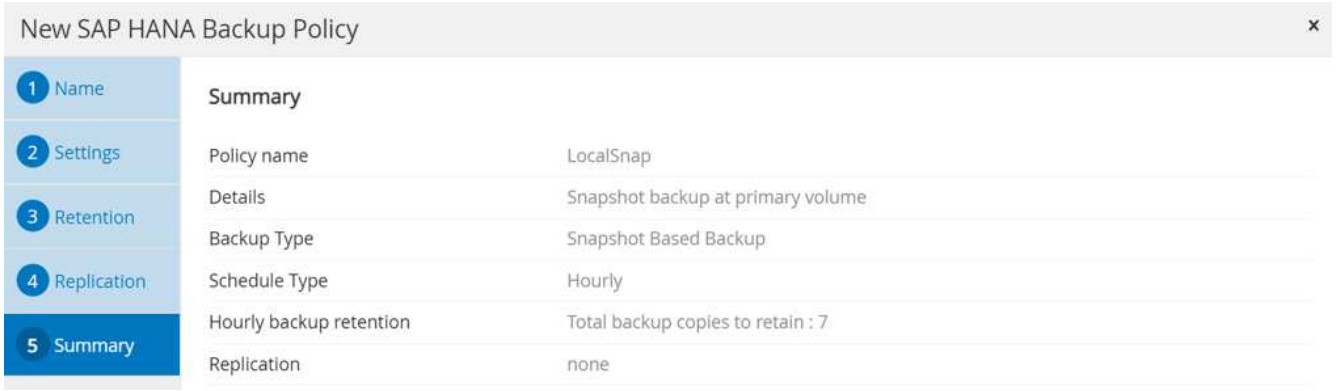


4. Konfigurieren Sie die Aufbewahrungseinstellungen für On-Demand-Backups.

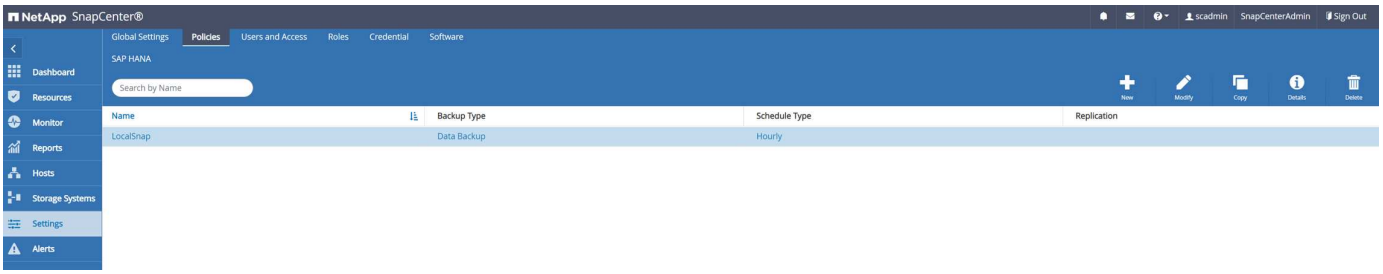


5. Konfigurieren der Replikationsoptionen. In diesem Fall ist kein SnapVault oder SnapMirror Update ausgewählt.





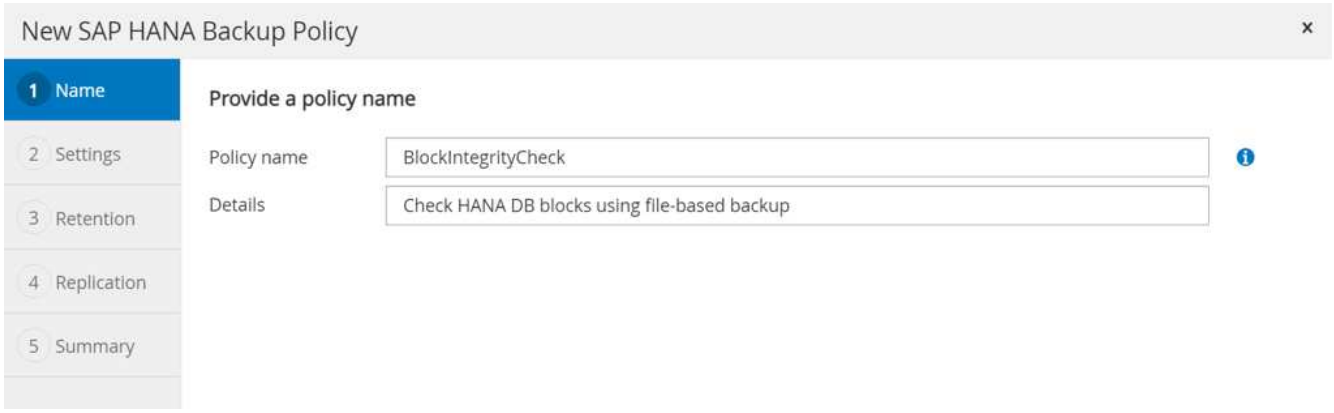
Die neue Richtlinie ist jetzt konfiguriert.



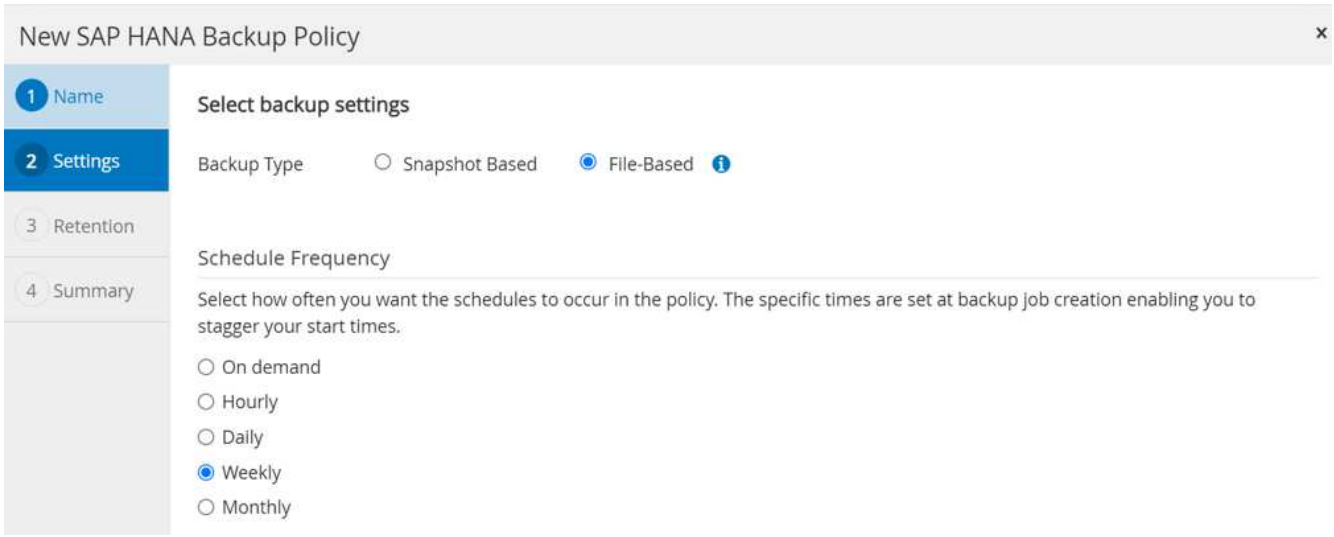
Richtlinie zur Block-Integritätsprüfung

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

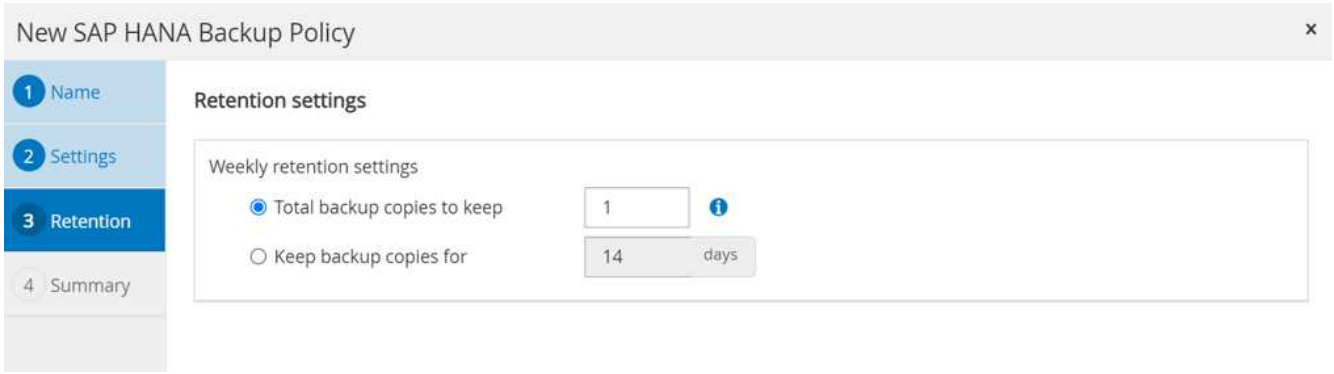
1. Gehen Sie zu Einstellungen > Richtlinien, und klicken Sie auf Neu.
2. Geben Sie den Namen und die Beschreibung der Richtlinie ein. Klicken Sie Auf Weiter.



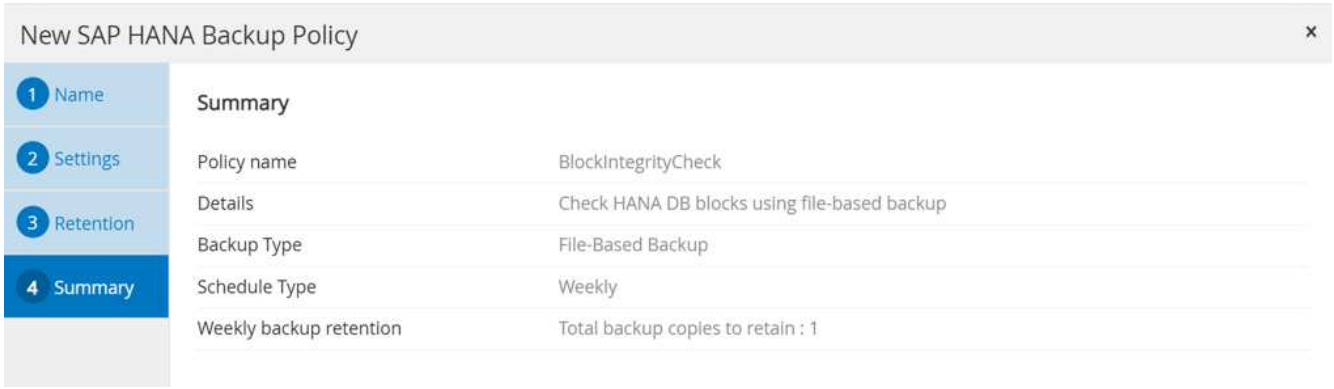
3. Legen Sie den Sicherungstyp auf „File-based“ und „Schedule Frequency“ auf „Weekly“ fest. Der Zeitplan selbst wird später mit der HANA-Ressourcenschutzkonfiguration konfiguriert.

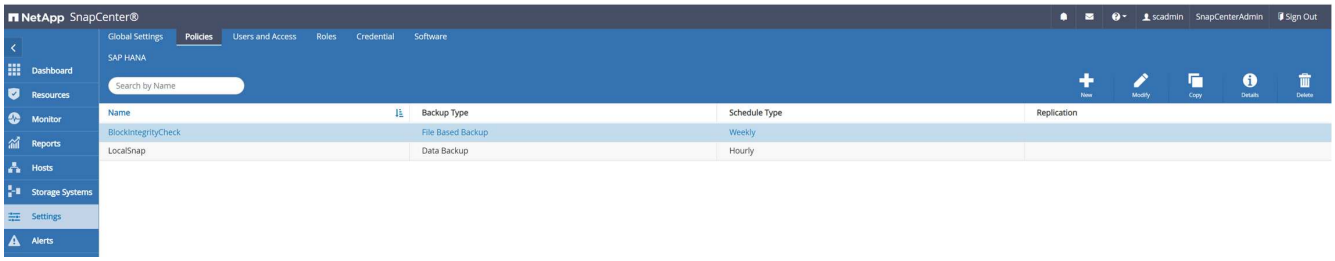


4. Konfigurieren Sie die Aufbewahrungseinstellungen für On-Demand-Backups.



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



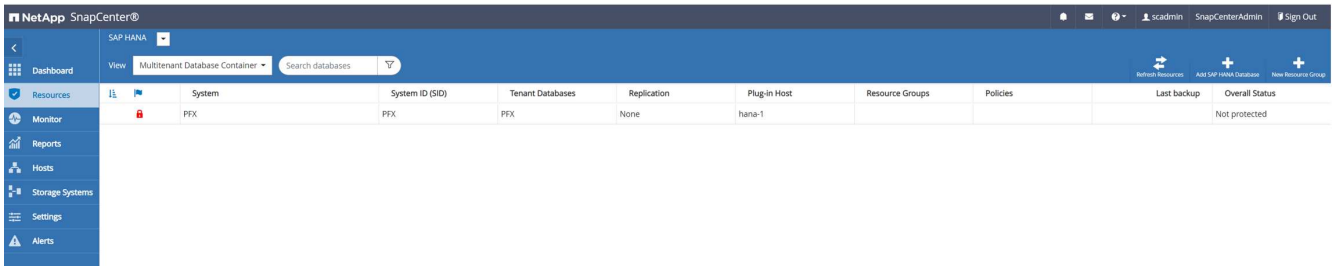


Konfiguration und Sicherung einer HANA-Ressource

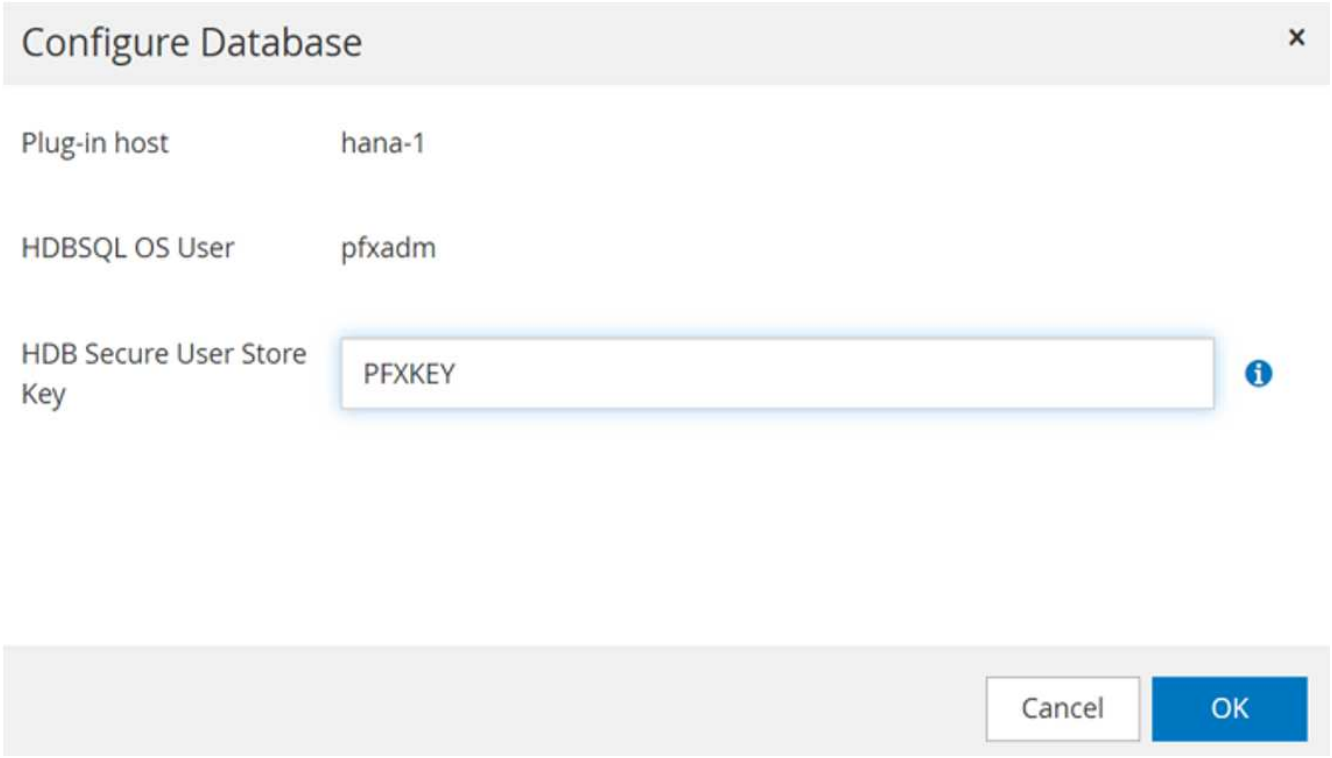
Nach der Plug-in-Installation startet der automatische Erkennungsvorgang der HANA-Ressource automatisch. Im Bildschirm Ressourcen wird eine neue Ressource erstellt, die mit dem roten Vorhängeschloss-Symbol als gesperrt markiert ist. Gehen Sie wie folgt vor, um die neue HANA-Ressource zu konfigurieren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

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

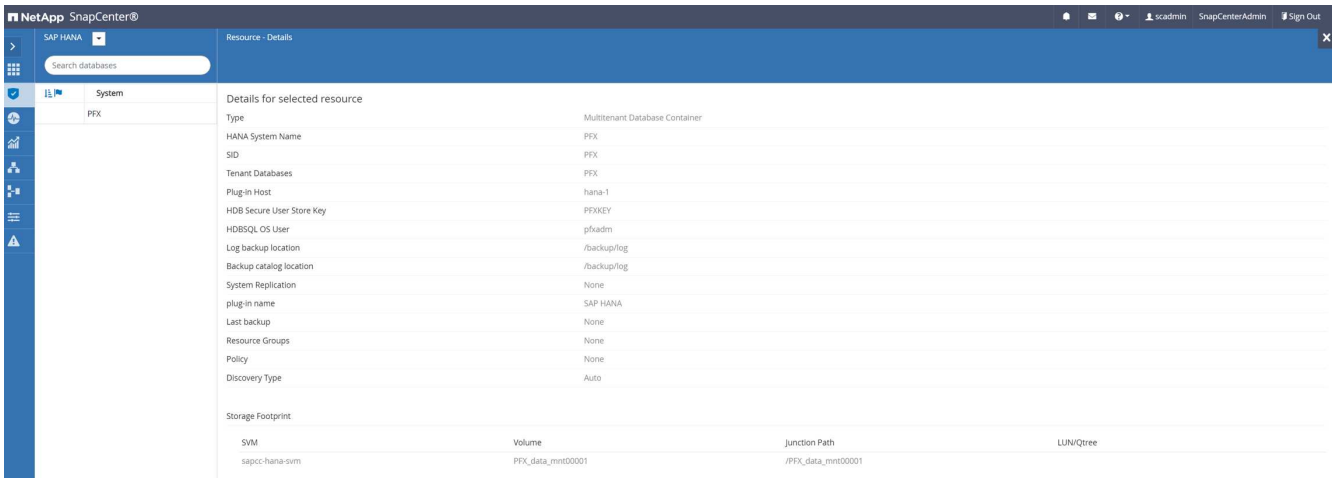
   Sie können den automatischen Erkennungsvorgang auch manuell im Bildschirm Ressourcen auslösen, indem Sie auf Ressourcen aktualisieren klicken.



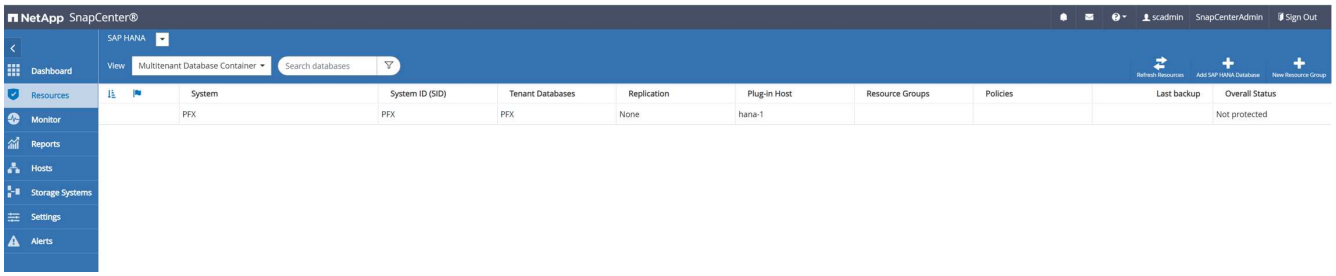
2. Geben Sie den UserStore-Schlüssel für die HANA-Datenbank an.



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

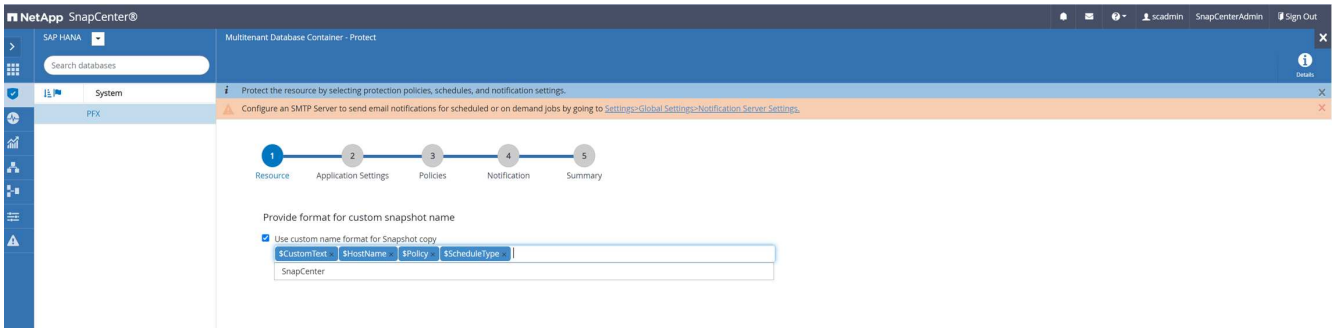


3. Doppelklicken Sie auf der Registerkarte Ressourcen auf die Ressource, um den Ressourcenschutz zu konfigurieren.

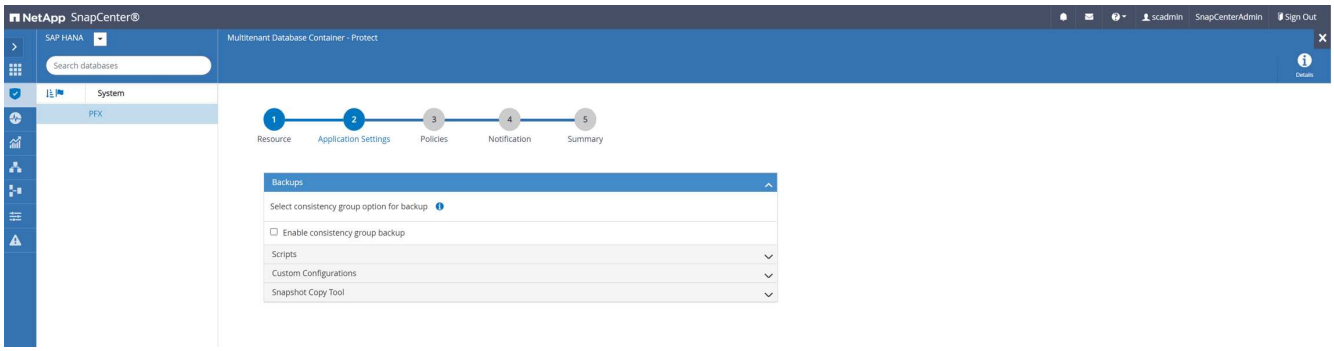


4. Konfigurieren Sie ein benutzerdefiniertes Namensformat für die Snapshot Kopie.

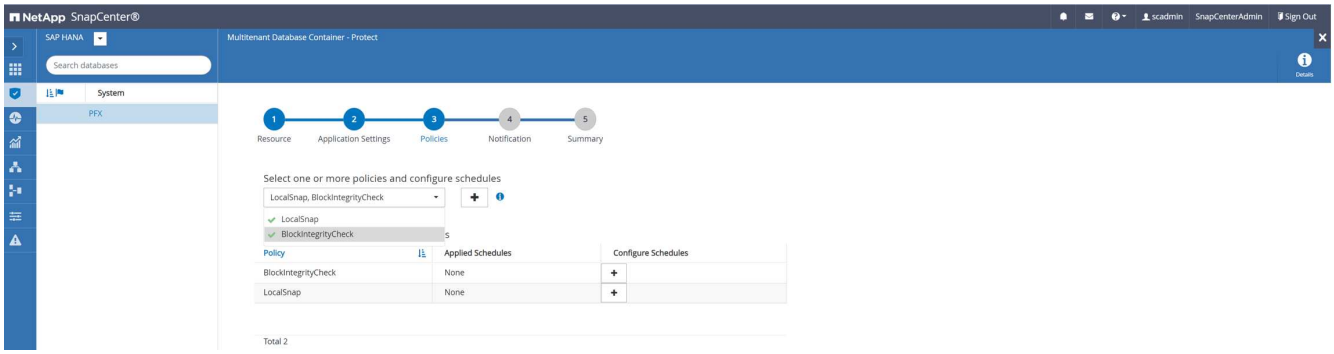
NetApp empfiehlt den Einsatz einer benutzerdefinierten Snapshot Kopie, um schnell ermitteln zu können, mit welcher Richtlinie und welche Zeitplantypen Backups erstellt wurden. Durch Hinzufügen des Zeitplantyps zum Namen der Snapshot Kopie können Sie zwischen geplanten und On-Demand-Backups unterscheiden. 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.

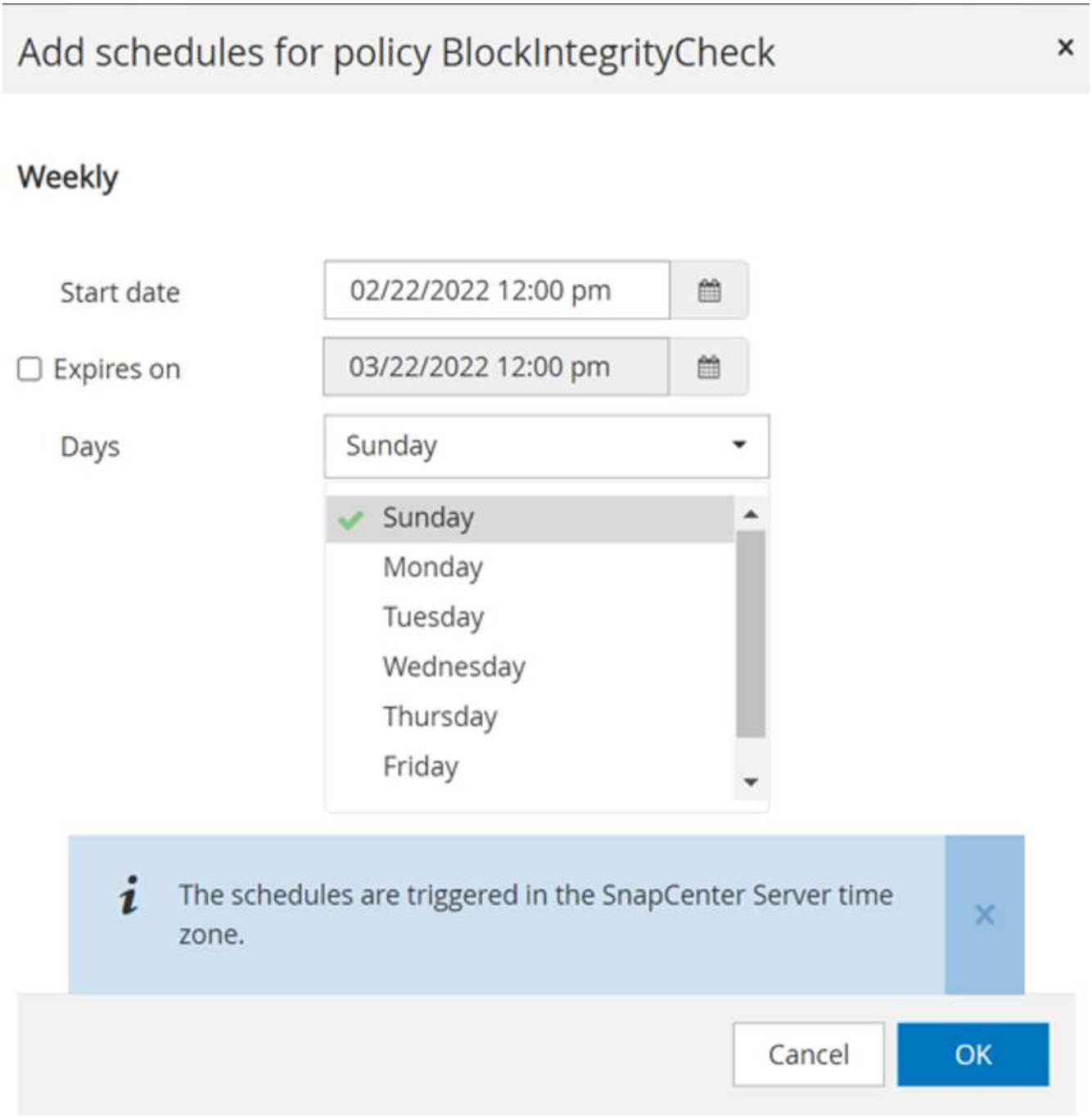


6. Wählen Sie die Richtlinien aus, die der Ressource hinzugefügt werden sollen.



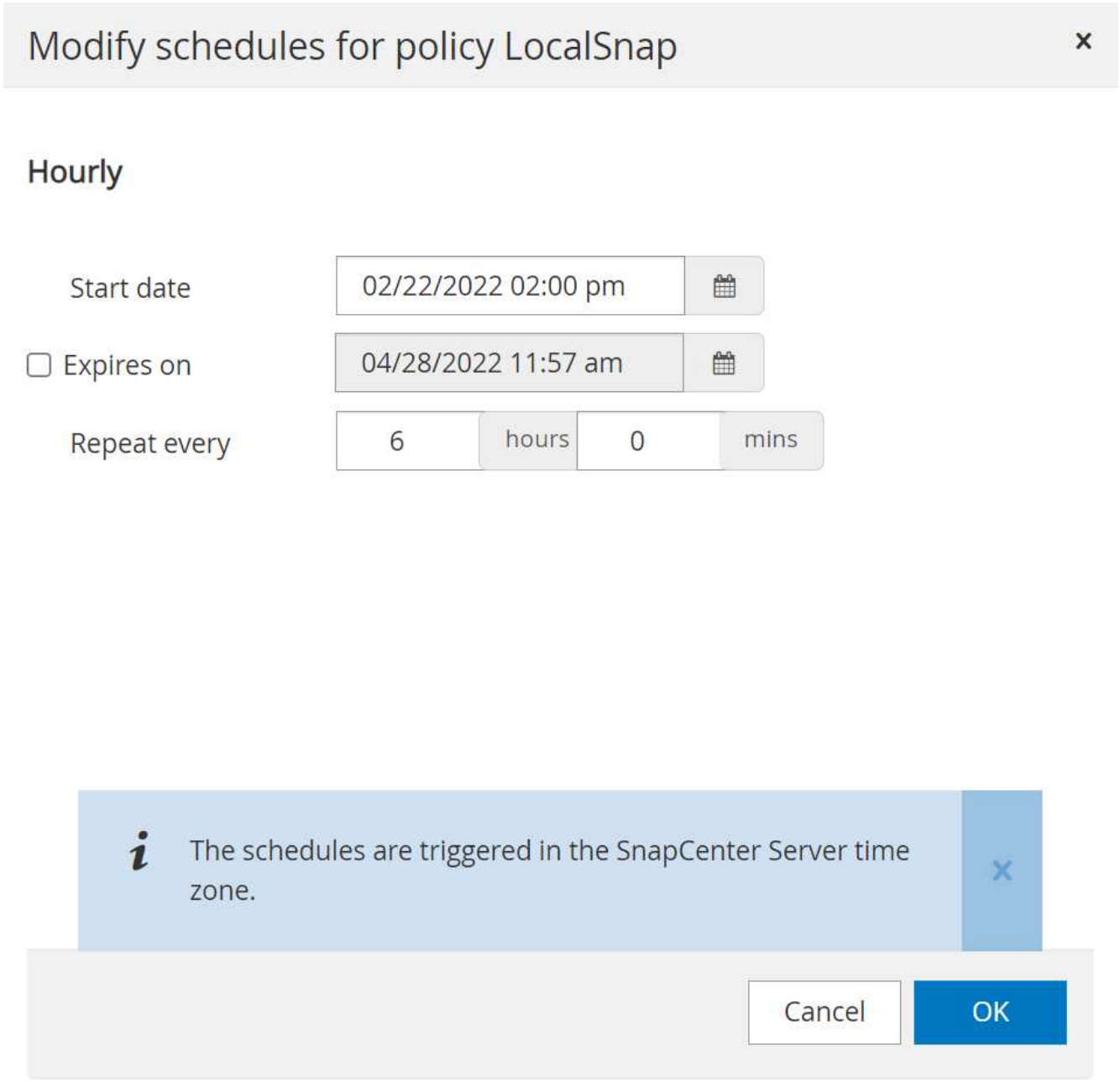
7. Legen Sie den Zeitplan für die Richtlinie zur Integritätsprüfung der Blöcke fest.

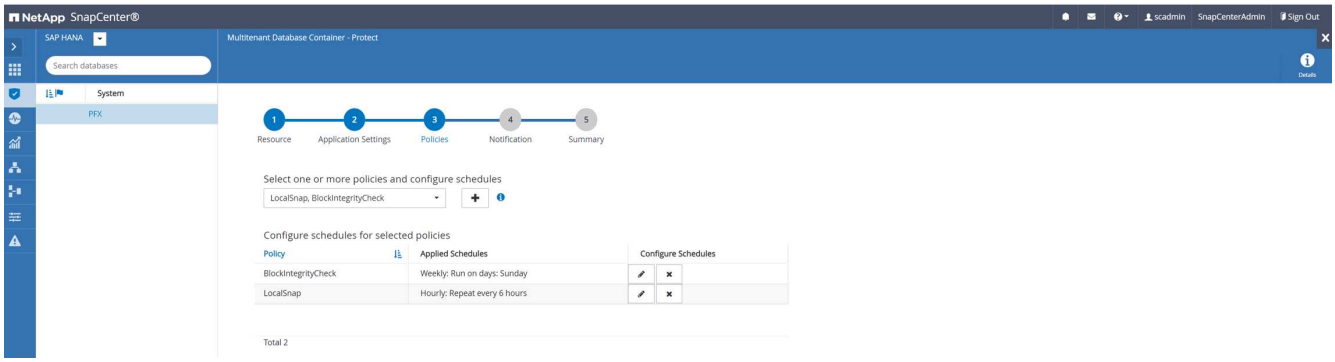
   In diesem Beispiel wird sie für einmal pro Woche festgelegt.



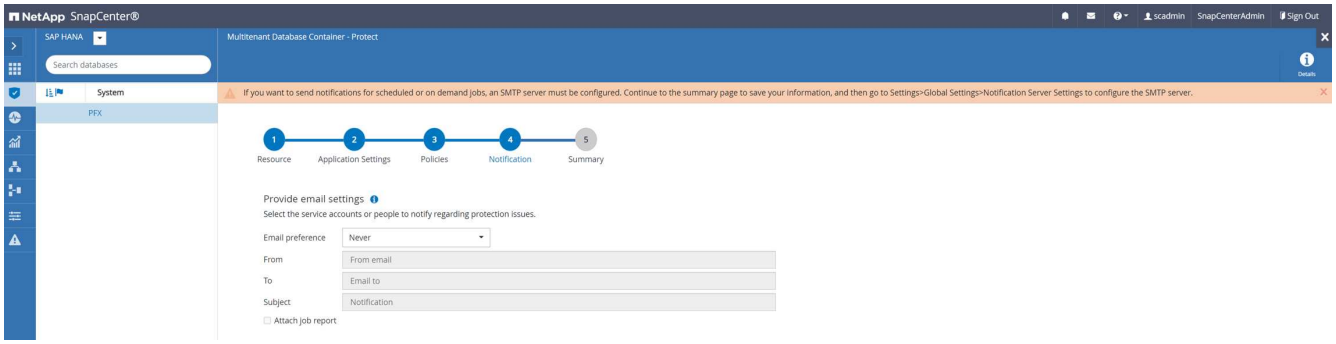
8. Legen Sie den Zeitplan für die lokale Snapshot-Richtlinie fest.

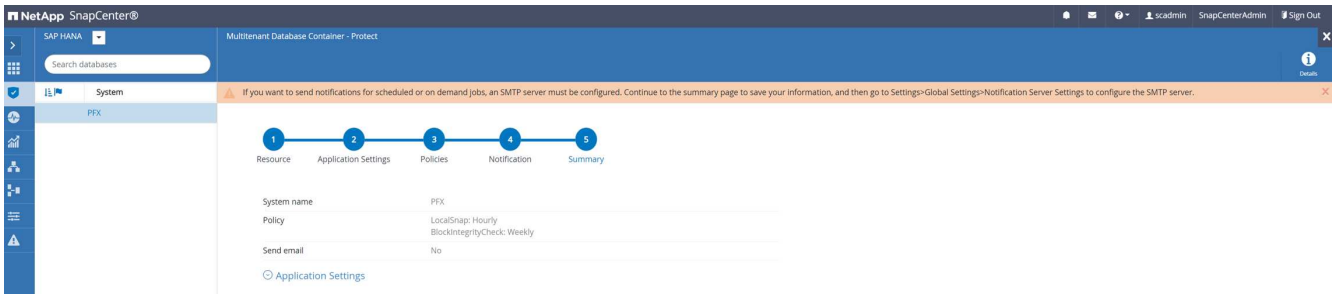
   In diesem Beispiel wird die Einstellung alle 6 Stunden durchgeführt.



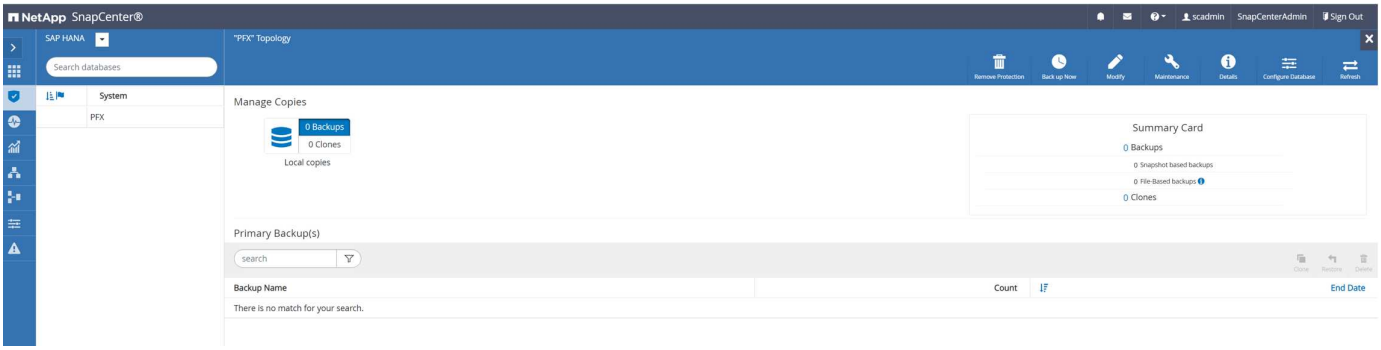


9. Geben Sie Informationen zur E-Mail-Benachrichtigung an.





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.

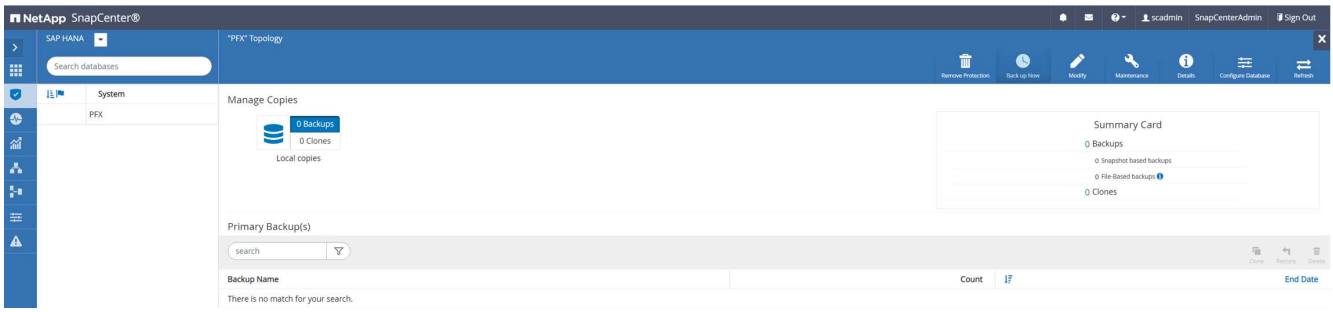
Erstellen Sie ein Snapshot Backup nach Bedarf

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

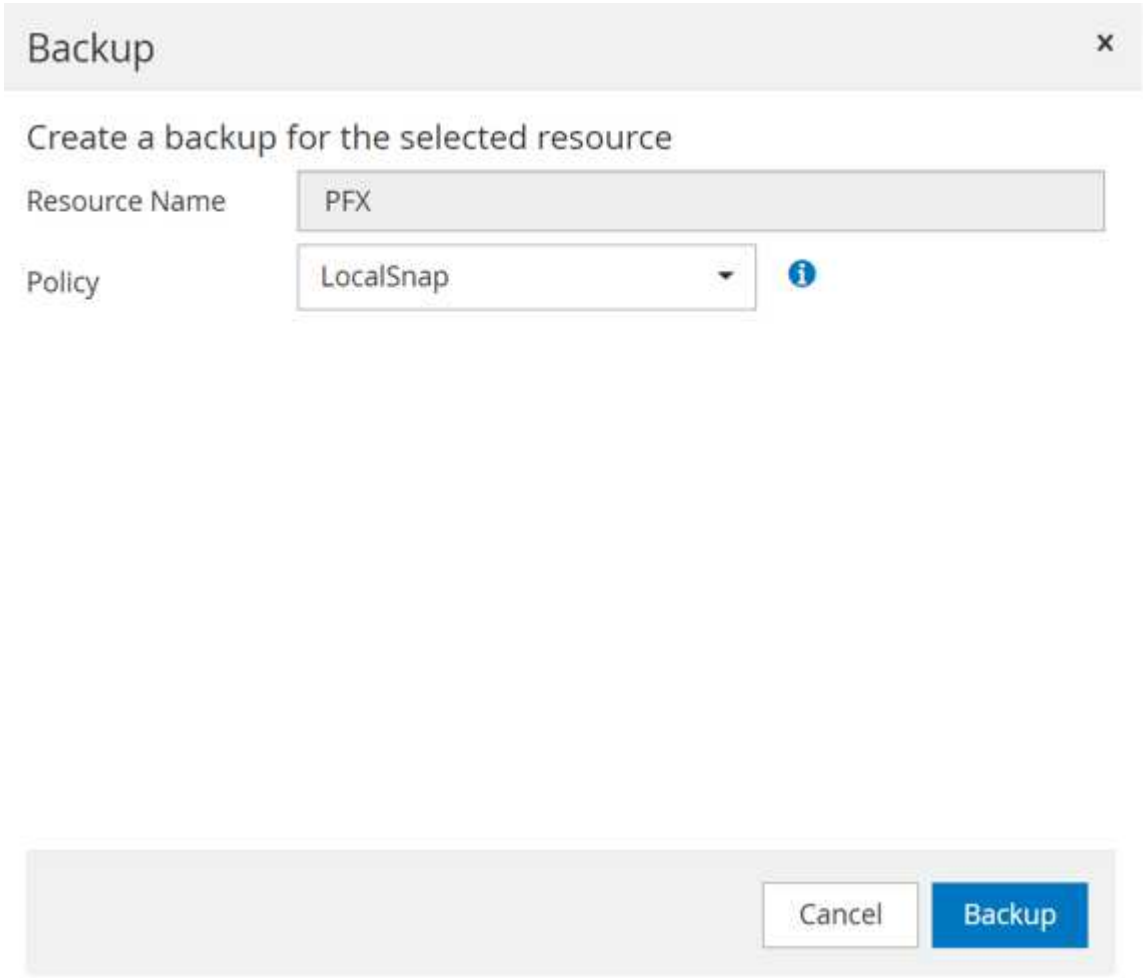
1. Wählen Sie in der Ansicht Ressource die Ressource aus und doppelklicken Sie auf die Zeile, um zur Ansicht Topologie zu wechseln.

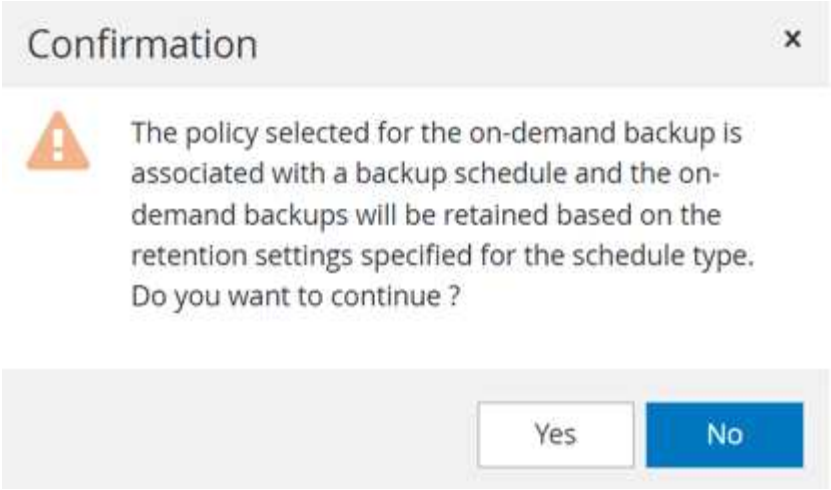
   Die Ansicht RessourcTopologie gibt einen Überblick über alle verfügbaren Backups, die mithilfe von SnapCenter erstellt wurden. Im oberen Bereich dieser Ansicht wird die Backup-Topologie angezeigt, die die Backups des primären Storage (lokale Kopien) und, falls verfügbar, auf dem externen Backup-Storage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

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



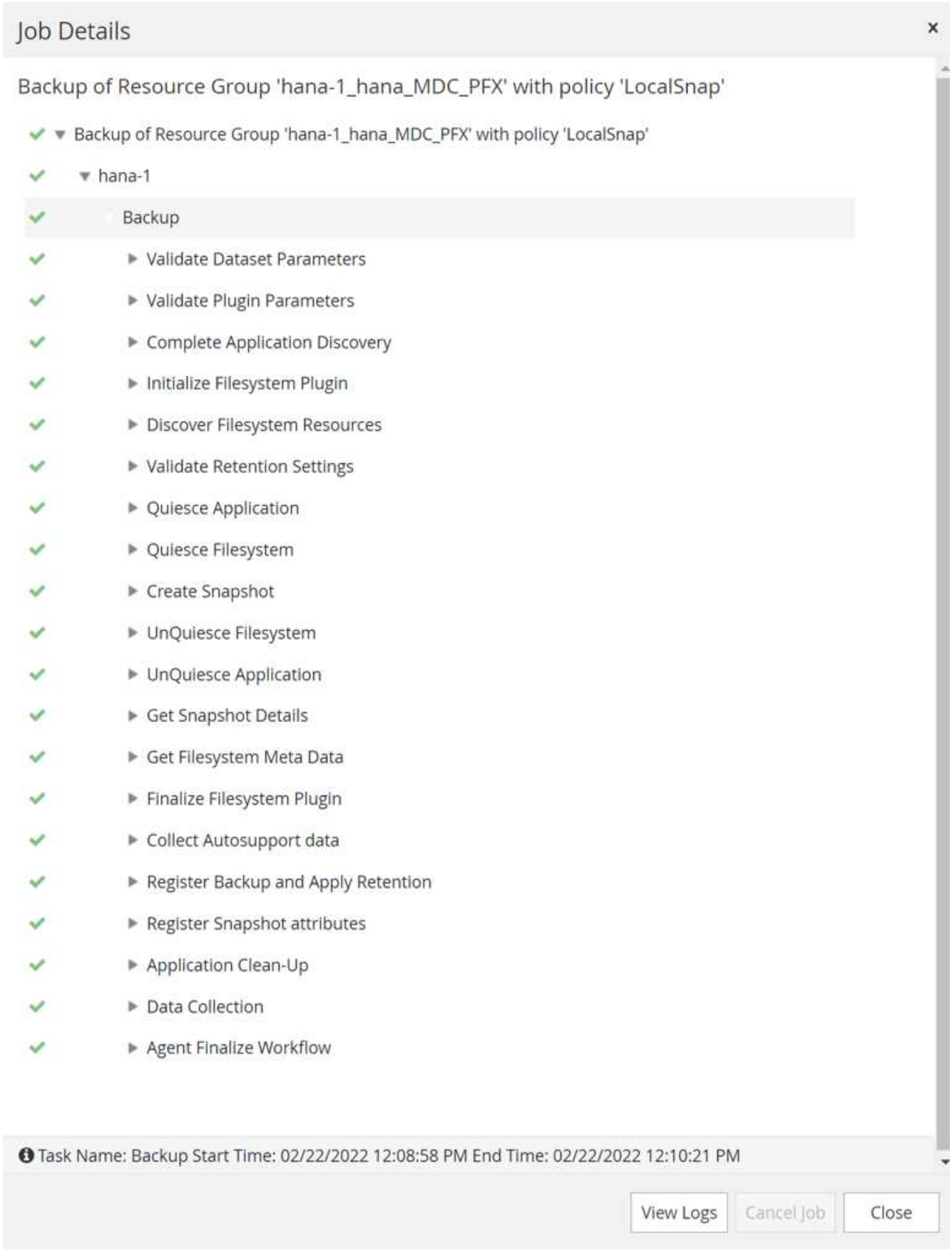
3. Wählen Sie aus der Dropdown-Liste die Backup-Richtlinie aus `LocalSnap`, Und klicken Sie dann auf Backup, um das On-Demand-Backup zu starten.





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

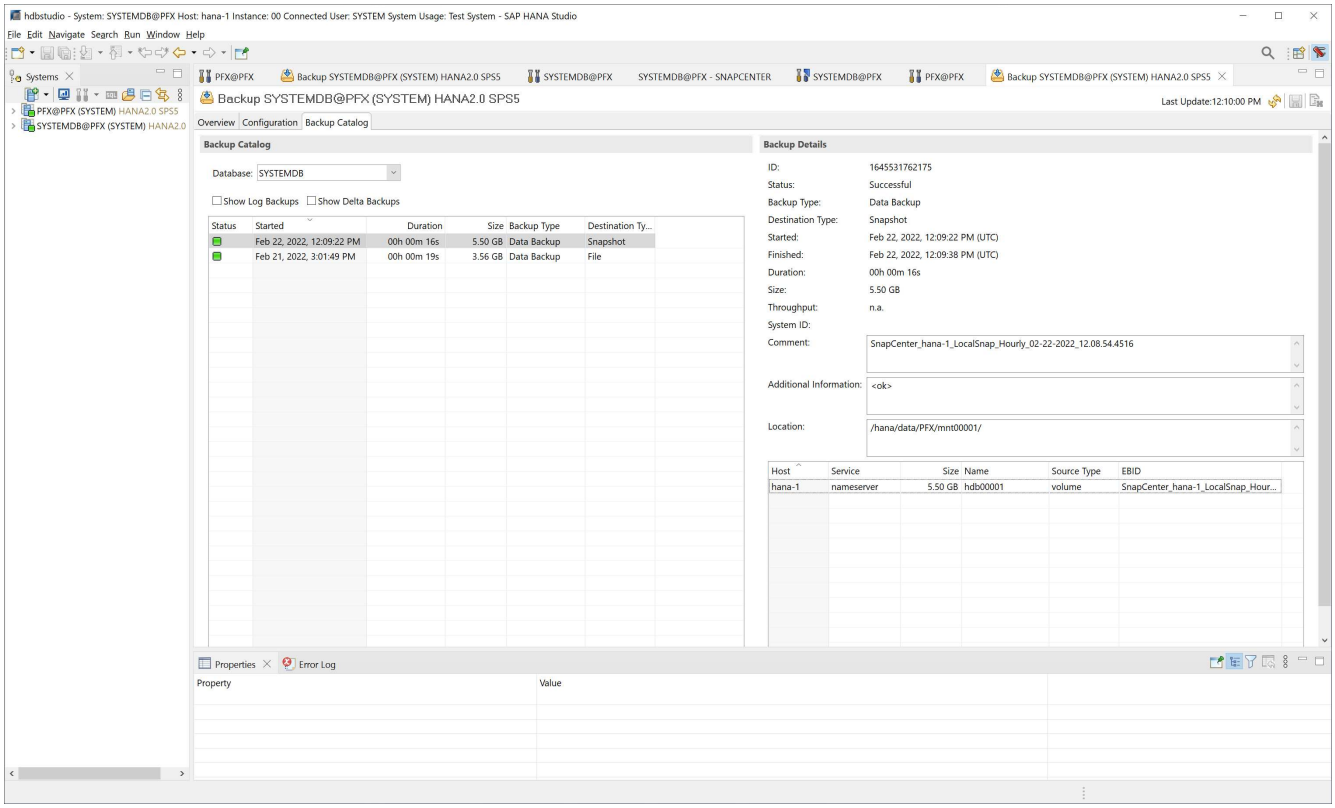
4. Die Jobdetails werden angezeigt, wenn Sie im Aktivitätsbereich auf die Vorgangszeile des Jobs klicken. Sie können ein detailliertes Jobprotokoll öffnen, indem Sie auf Protokolle anzeigen klicken

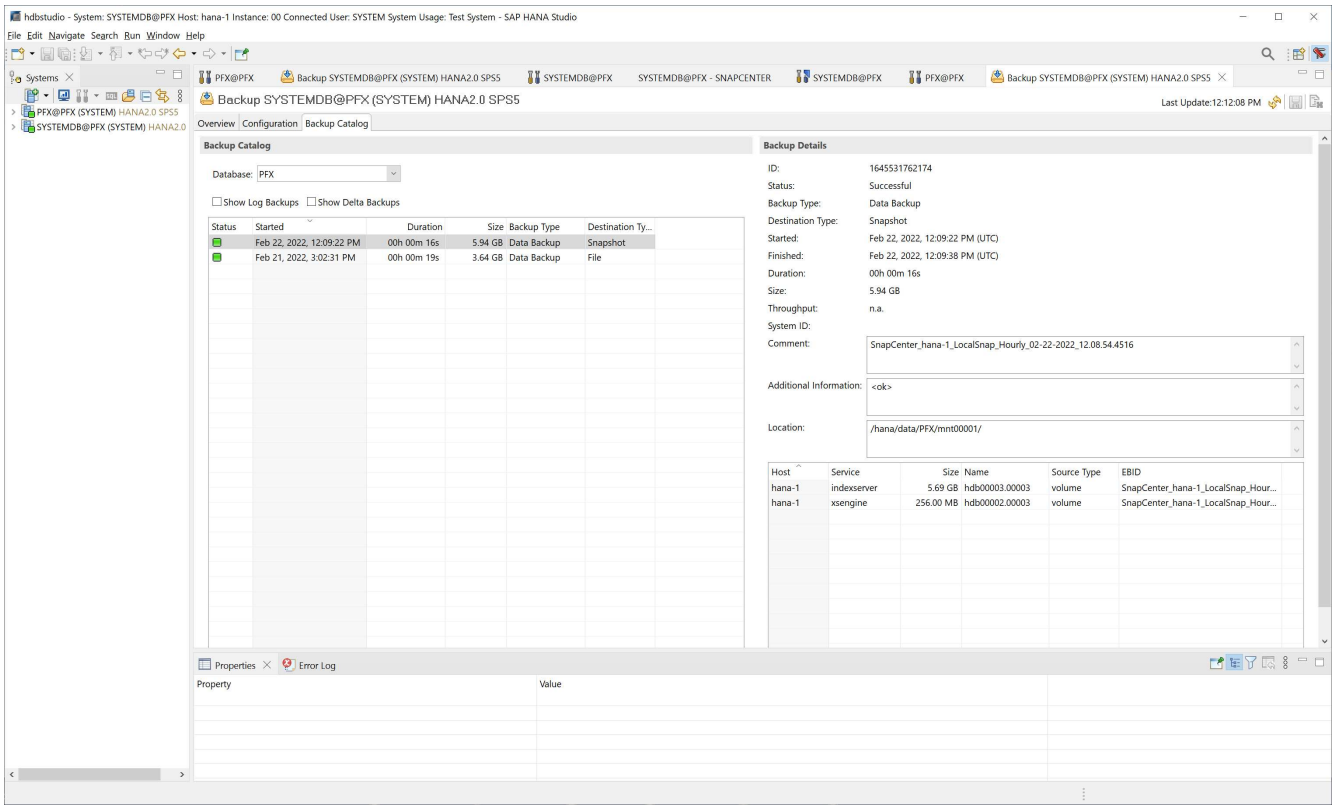


Nach Abschluss des Backups wird in der Topologieansicht ein neuer Eintrag angezeigt. Die Backup-Namen folgen derselben Namenskonvention wie der in Abschnitt definierte Snapshot Name "„Konfigurieren und Schützen einer HANA-Ressource“."

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.



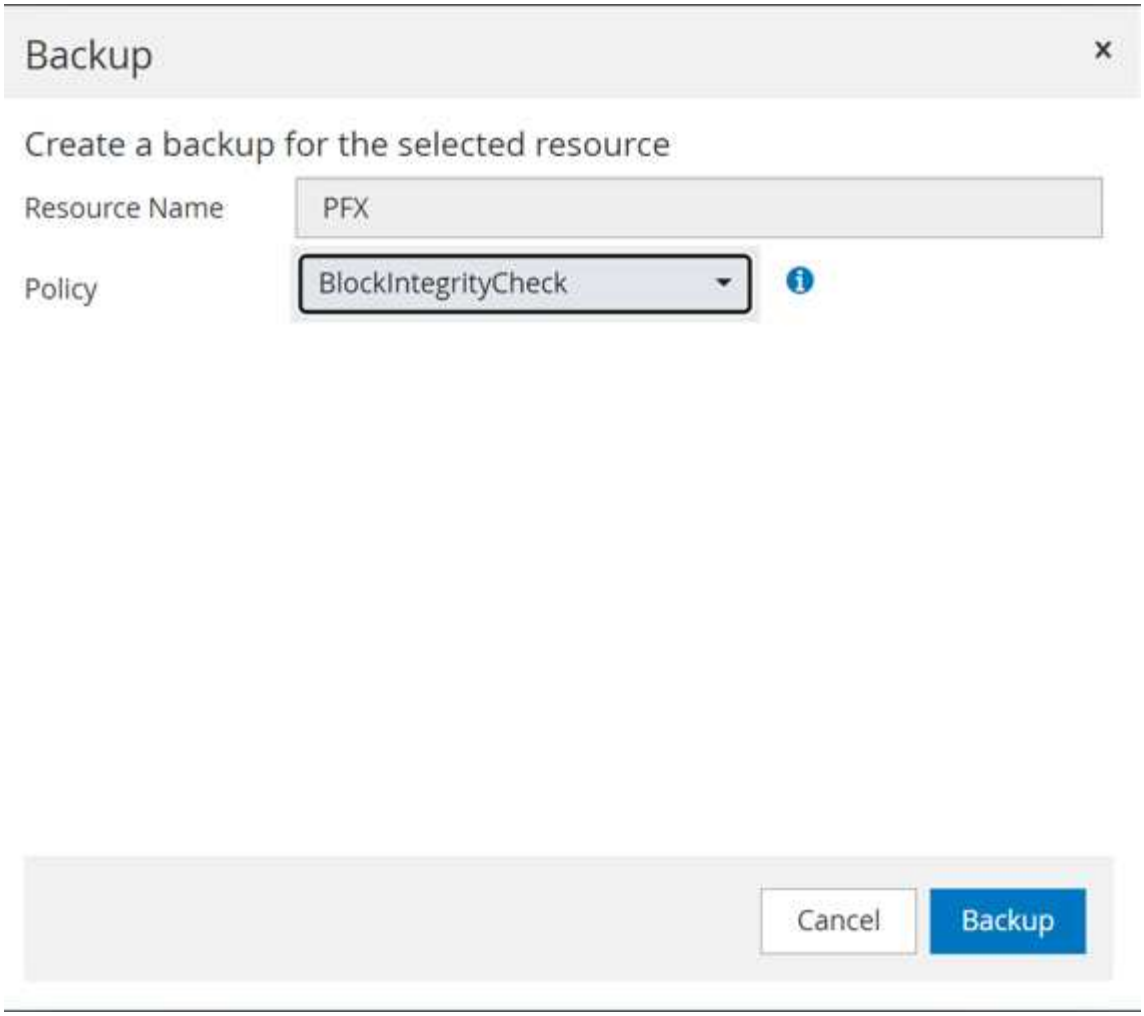


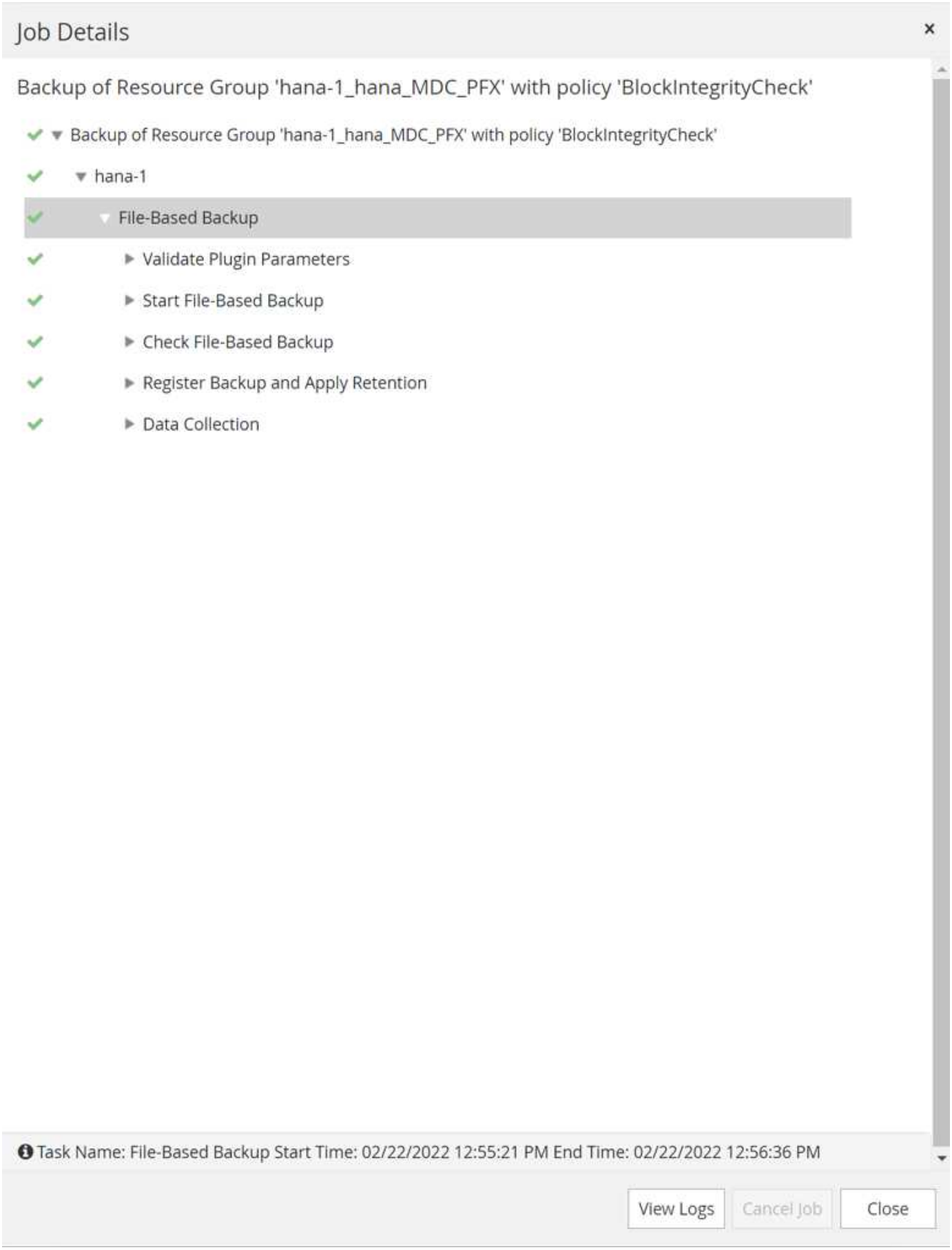
Auf dem FSX für ONTAP Filesystem können Sie die Snapshot-Backups durch eine Verbindung mit der Konsole der SVM auflisten.

```
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

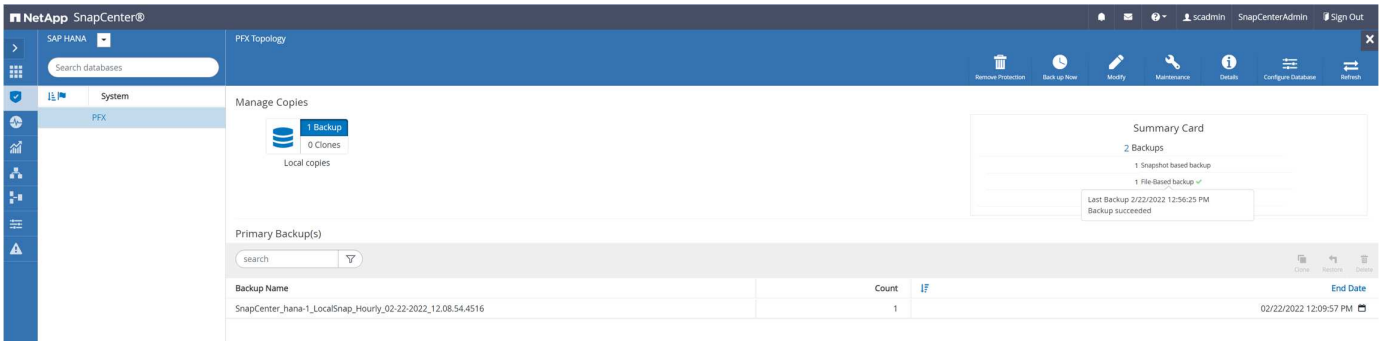
Ein on-Demand Block Integrity Check Vorgang wird auf dieselbe Weise wie ein Snapshot Backup Job ausgeführt, indem die Richtlinie BlockIntegrtyCheck ausgewählt wird. Bei der Planung von Backups mithilfe dieser Richtlinie erstellt SnapCenter eine standardmäßige SAP HANA Datei-Backup für das System und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


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

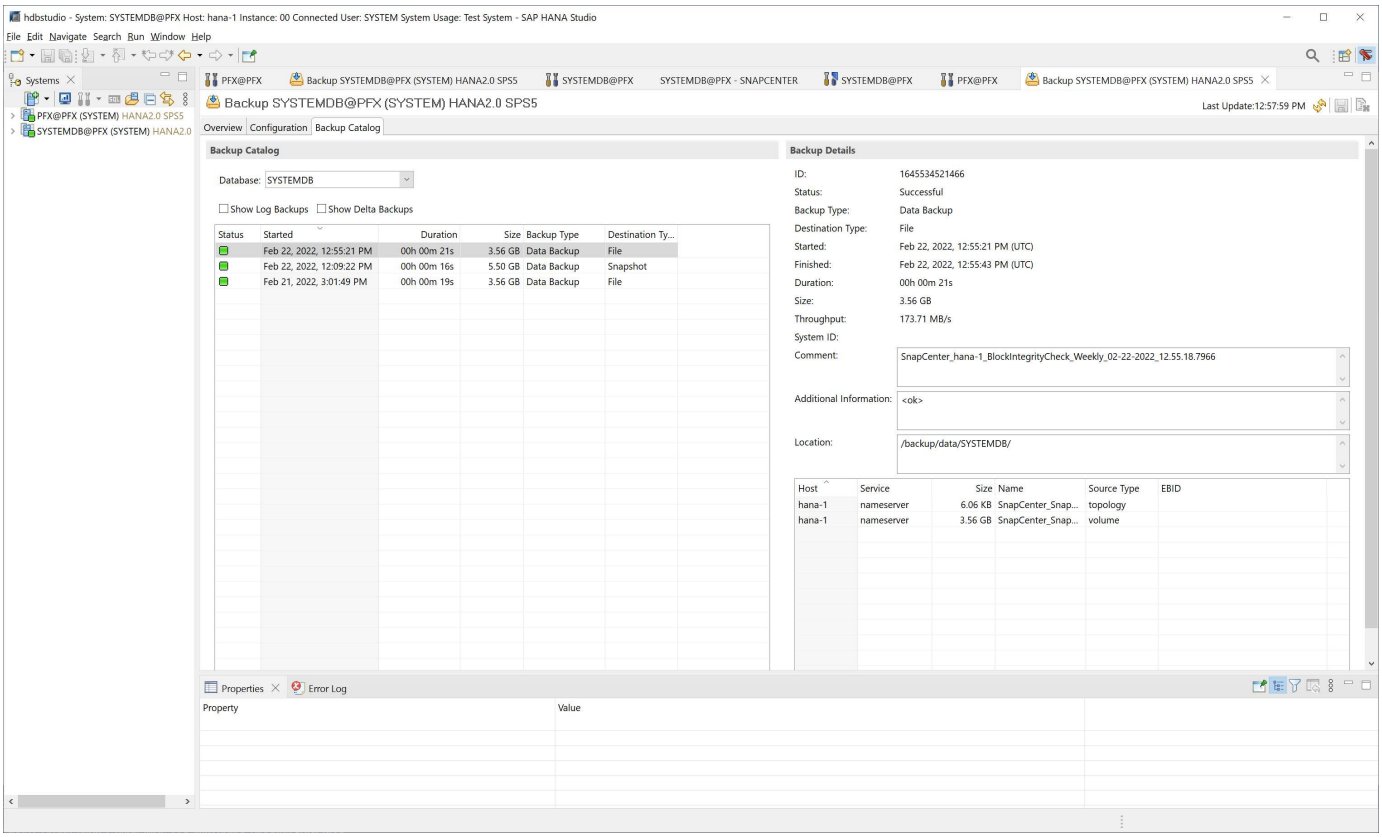


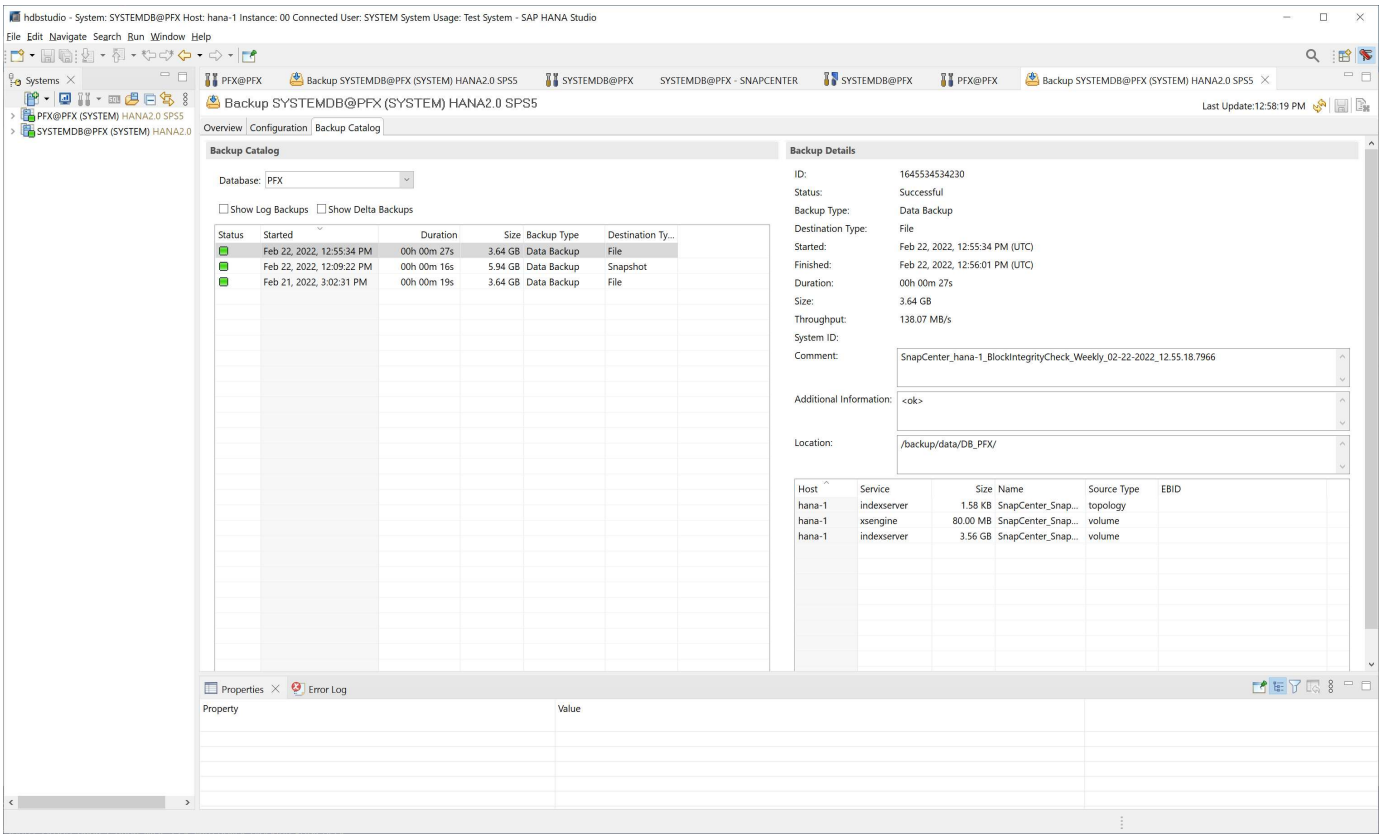
SnapCenter zeigt die Blockintegritätsprüfung nicht auf dieselbe Weise an wie Backups basierend auf

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

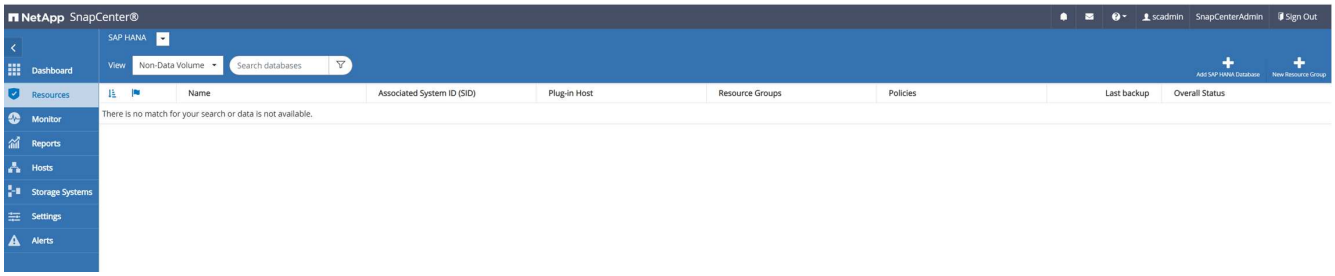
werden müssen, empfiehlt NetApp, eine zusätzliche Backup-Strategie für nicht-Daten-Volumes zu entwickeln, um das SAP HANA Datenbank-Backup zu erweitern. Je nach Ihren spezifischen Anforderungen kann sich das Backup von nicht-Daten-Volumes in den Einstellungen für die Planungsfrequenz und -Aufbewahrung 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.

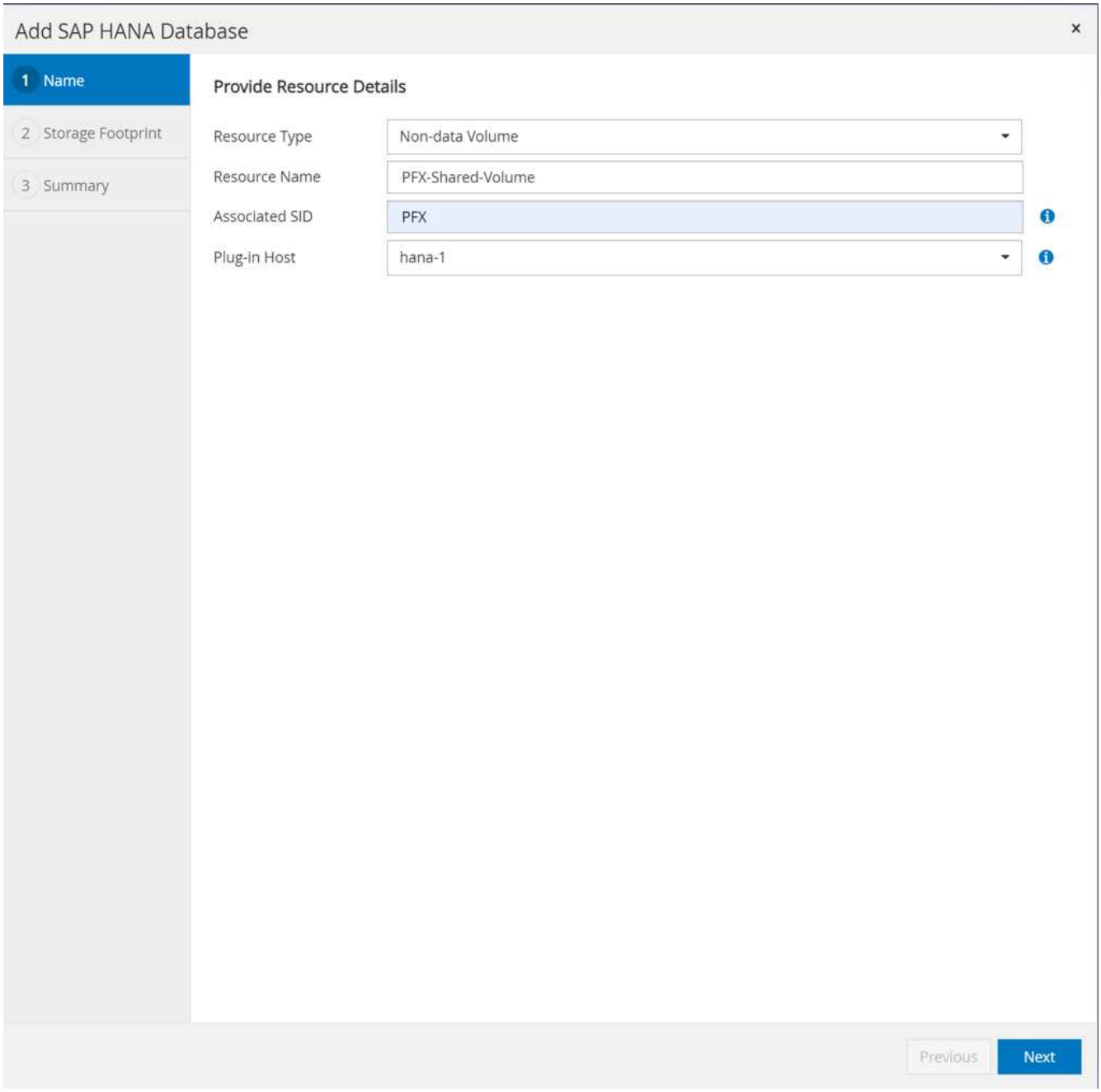
Konfiguration von Ressourcen, die nicht von Datenvolumen stammen

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

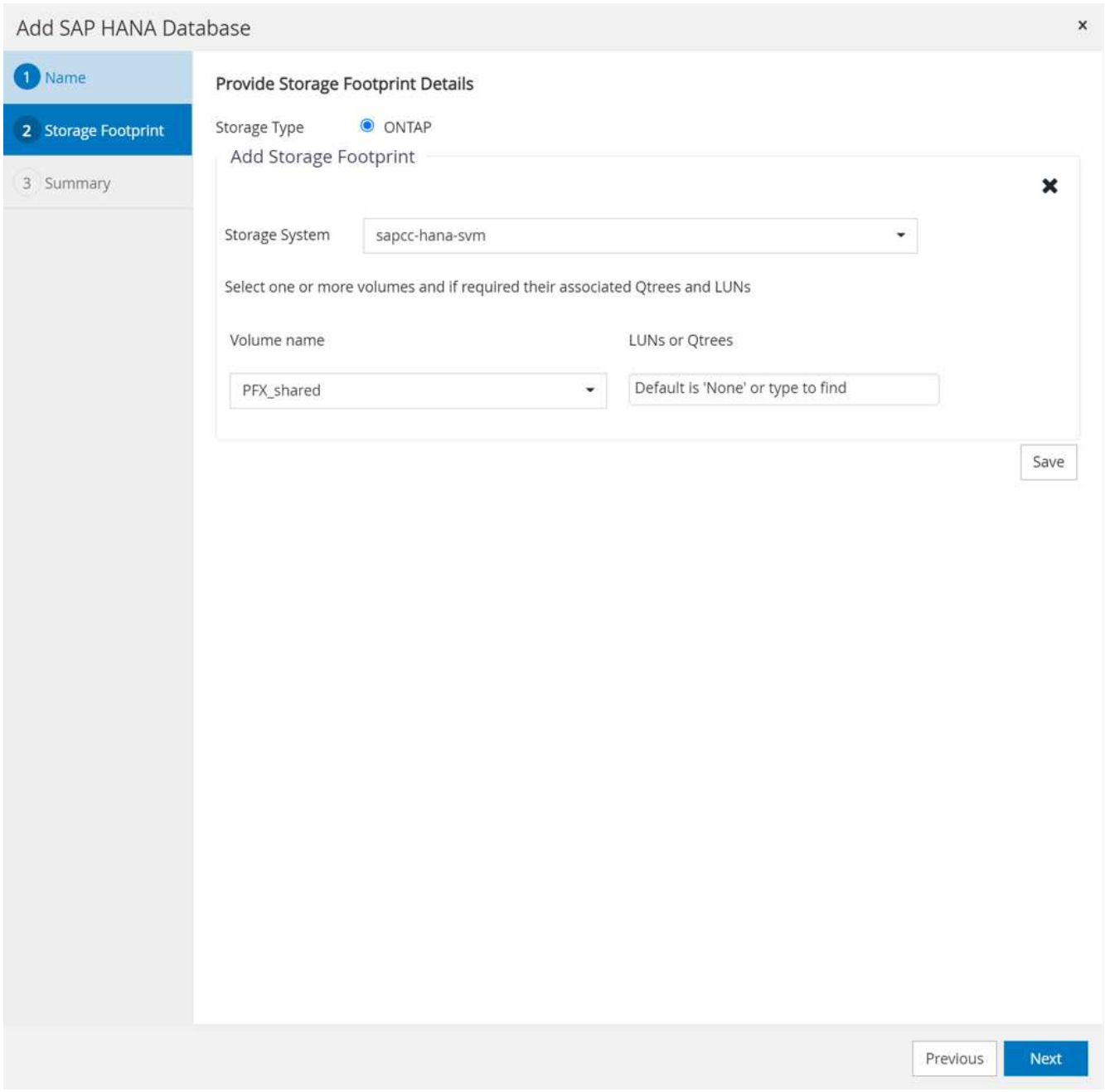
1. Wählen Sie auf der Registerkarte Ressourcen die Option Non-Data-Volume, und klicken Sie auf Add SAP HANA Database.



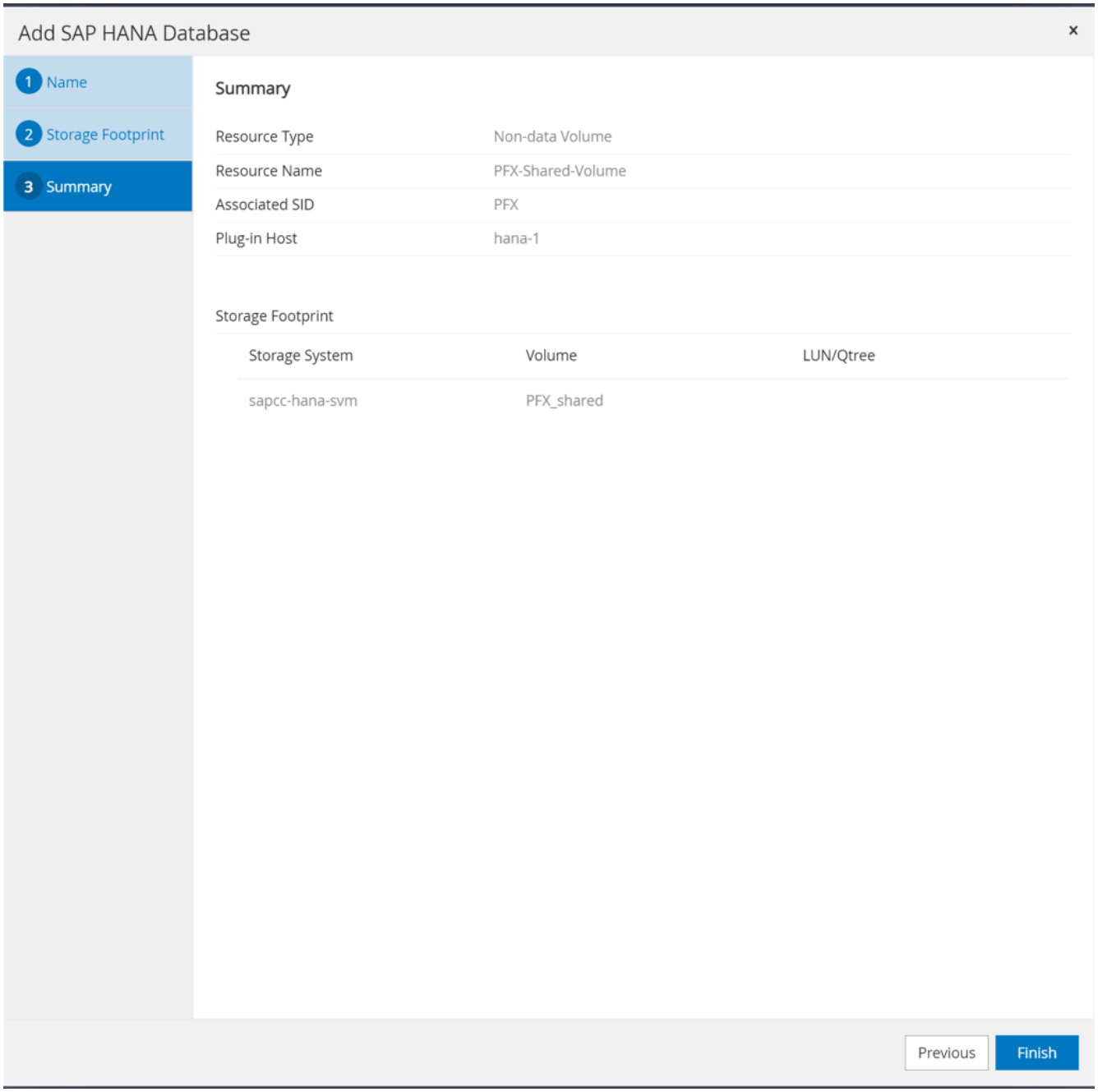
2. Wählen Sie in Schritt 1 des Dialogfelds SAP HANA-Datenbank hinzufügen in der Liste Ressourcentyp die Option nicht-Datenvolumen aus. Geben Sie einen Namen für die Ressource und den zugehörigen SID und den SAP HANA Plug-in-Host an, den Sie für die Ressource verwenden möchten, und klicken Sie dann auf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



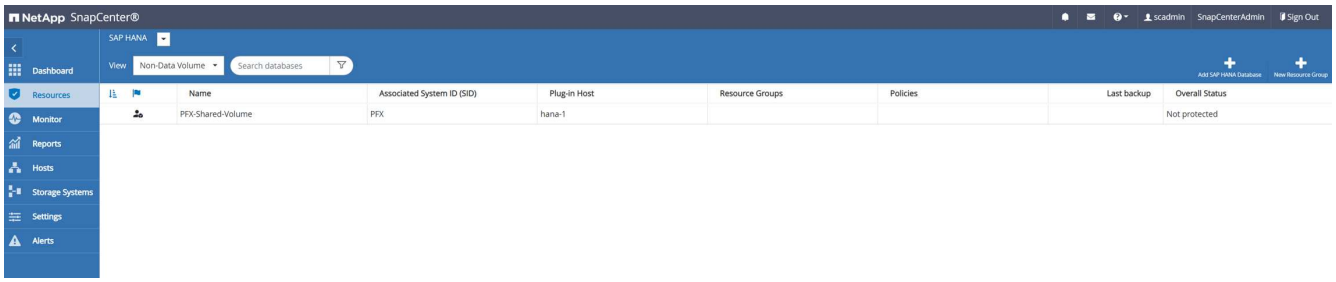
3. Fügen Sie die SVM und das Storage-Volume als Storage-Platzbedarf hinzu und klicken Sie dann auf Weiter.



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



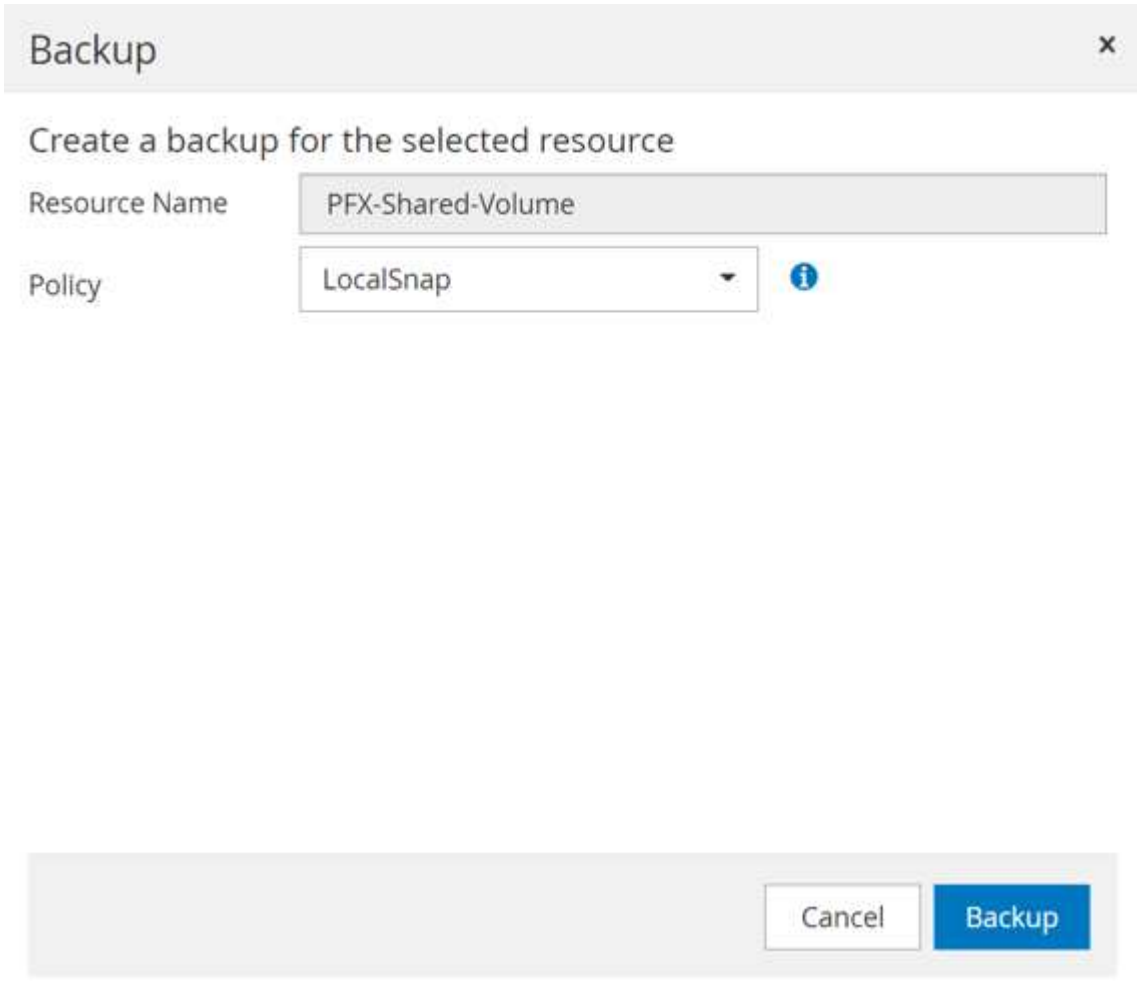
Das neue nicht-Daten-Volume wird nun SnapCenter hinzugefügt. Doppelklicken Sie auf die neue Ressource, um den Ressourcenschutz auszuführen.



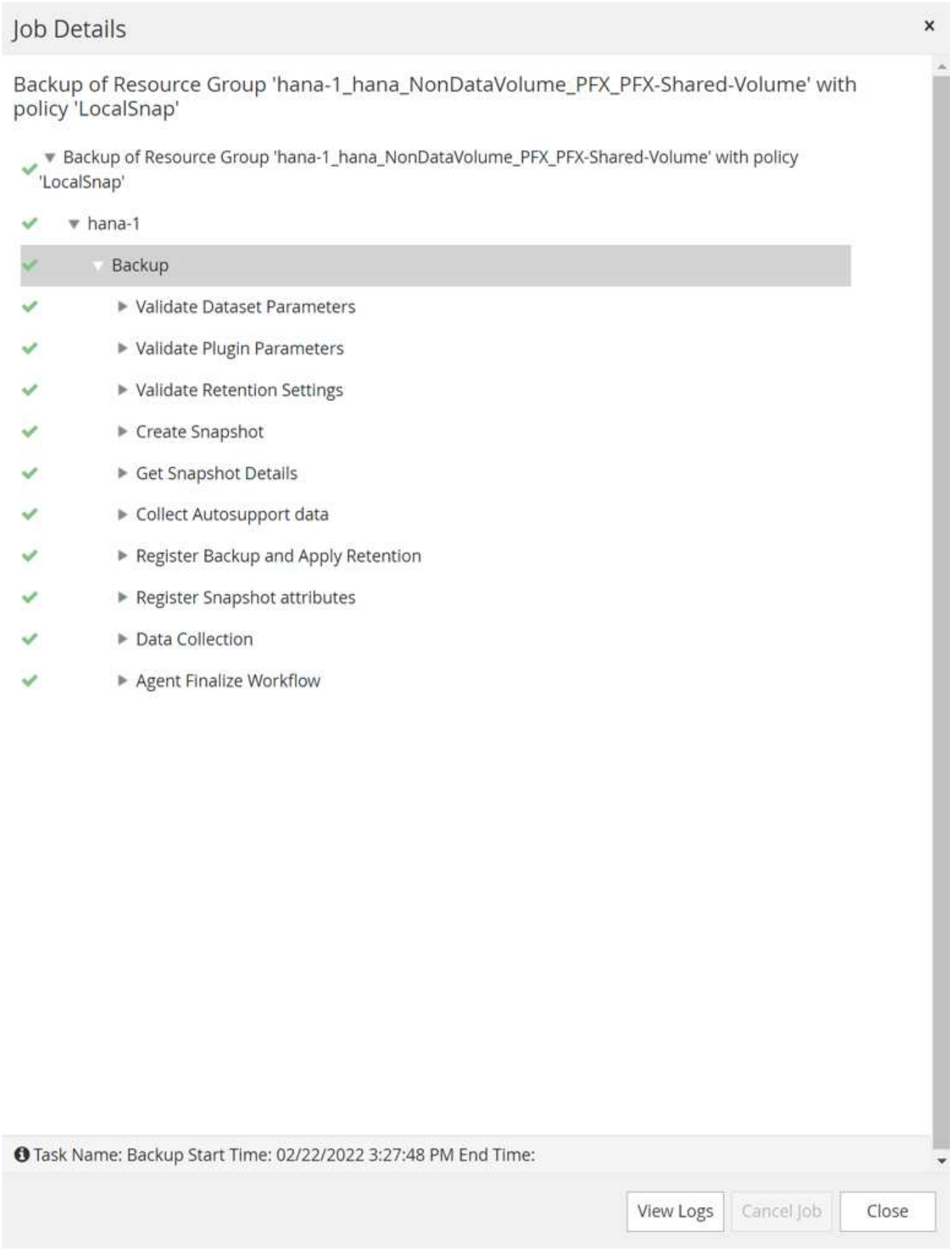
Der Ressourcenschutz erfolgt auf dieselbe Weise wie zuvor bei einer HANA-Datenbankressource.

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

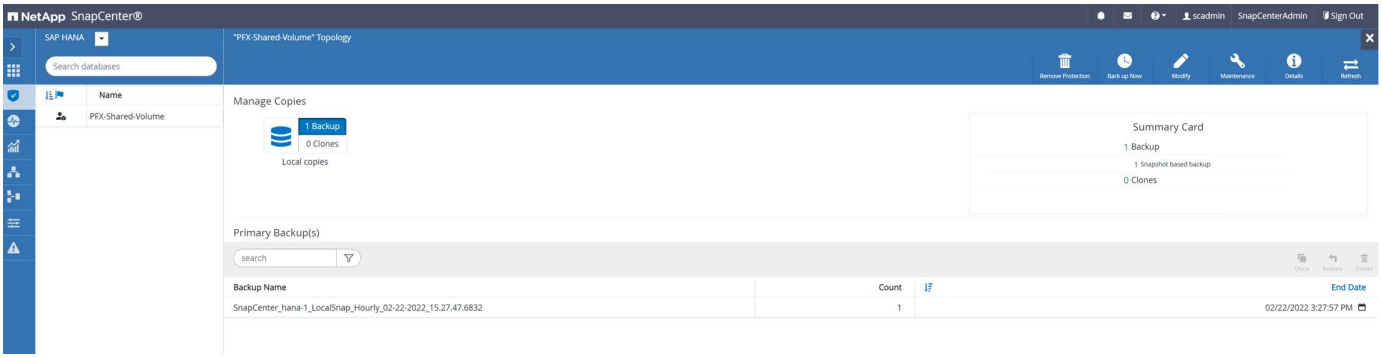
6. Wählen Sie die Richtlinie aus, und starten Sie den Backup-Vorgang.



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:

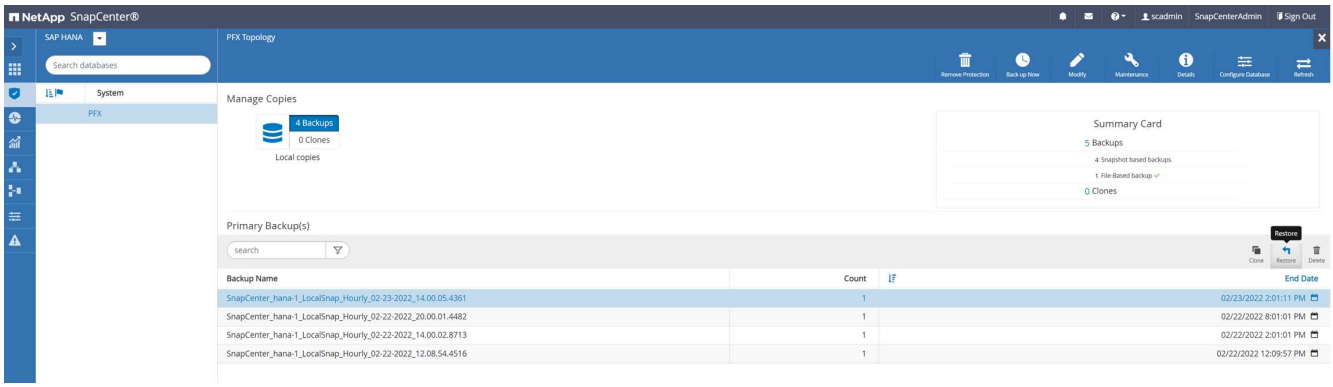
1. Die HANA-Datenbank wird gestoppt.
2. Die Datenbank wird wiederhergestellt. Je nach gewähltem Wiederherstellungstyp werden verschiedene Operationen ausgeführt.
   - Wenn das Zurücksetzen von Volumes ausgewählt wird, hängt SnapCenter das Volume ab, stellt das Volume mithilfe von Volume-basierten SnapRestore 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.

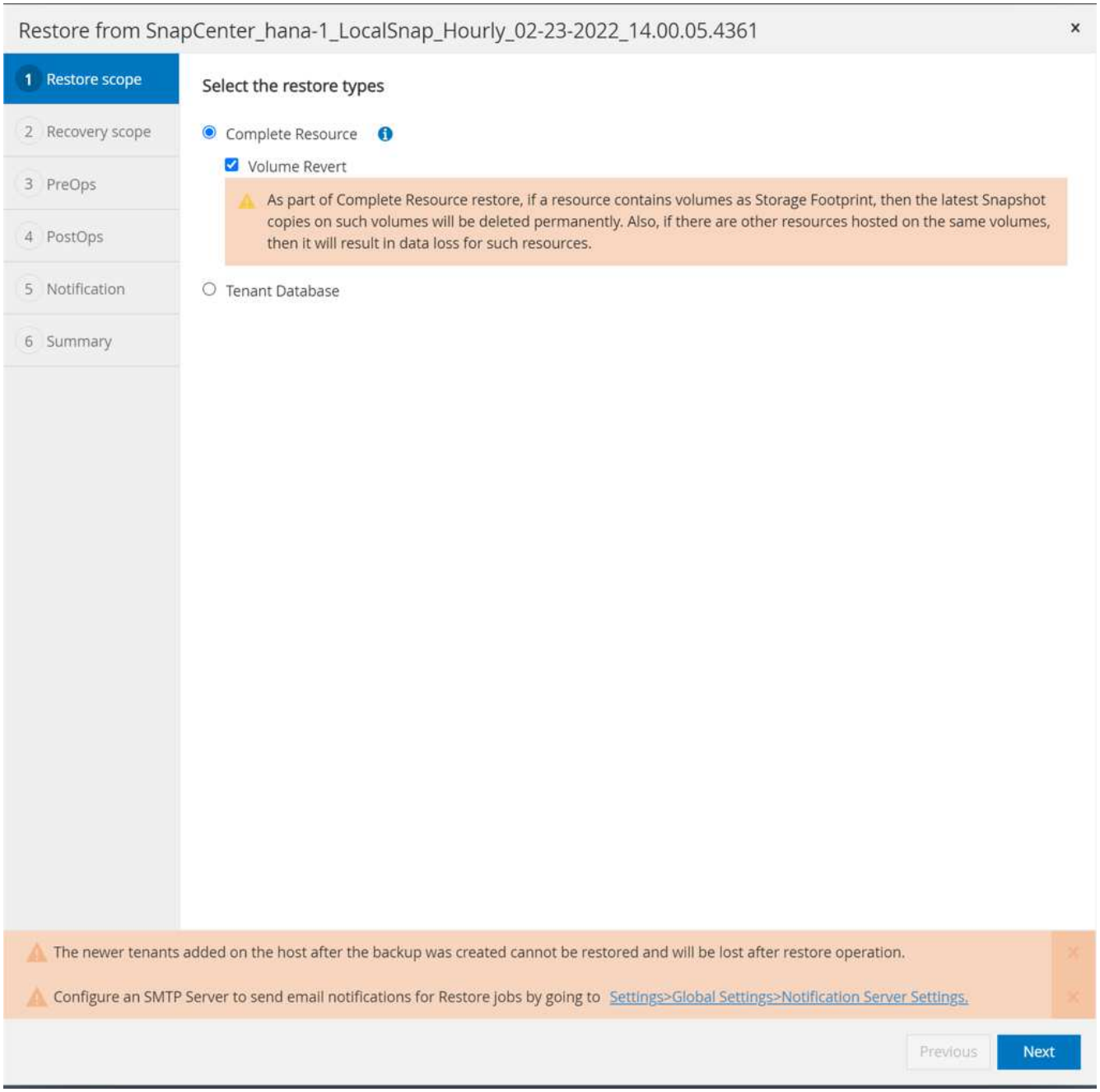
Führen Sie die folgenden Schritte aus, um einen manuellen Wiederherstellungsvorgang durchzuführen:

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



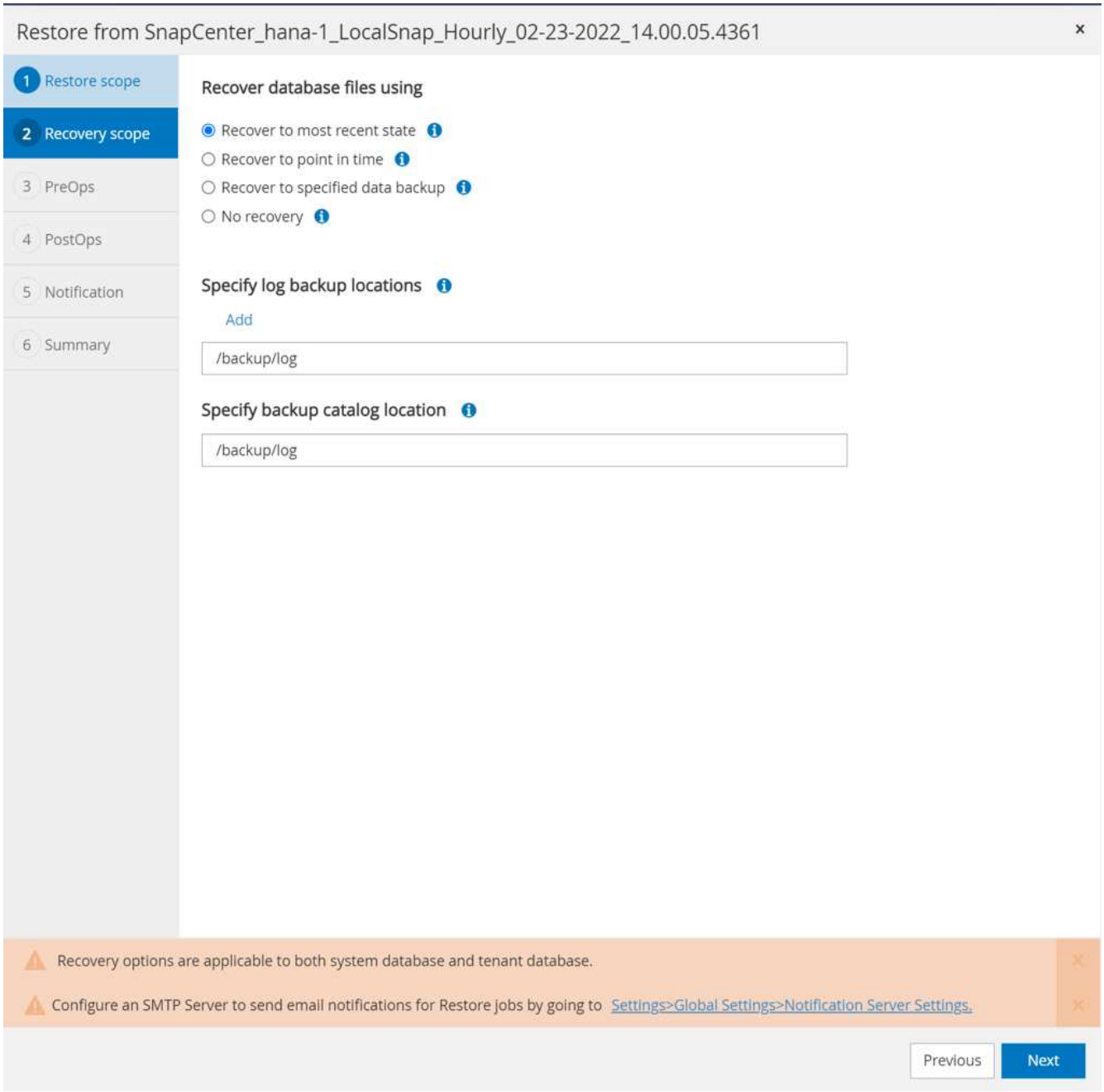
2. Wählen Sie den Umfang und den Typ der Wiederherstellung aus.

   Das Standard-Szenario für HANA MDC Single-Tenant-Systeme ist die Nutzung vollständiger Ressourcen mit Volumenrücksetzung. Bei einem HANA MDC-System mit mehreren Mandanten möchten Sie möglicherweise nur einen einzigen Mandanten wiederherstellen. Weitere Informationen zur Wiederherstellung eines einzelnen Mandanten finden Sie unter "Restore und Recovery (netapp.com)"Die

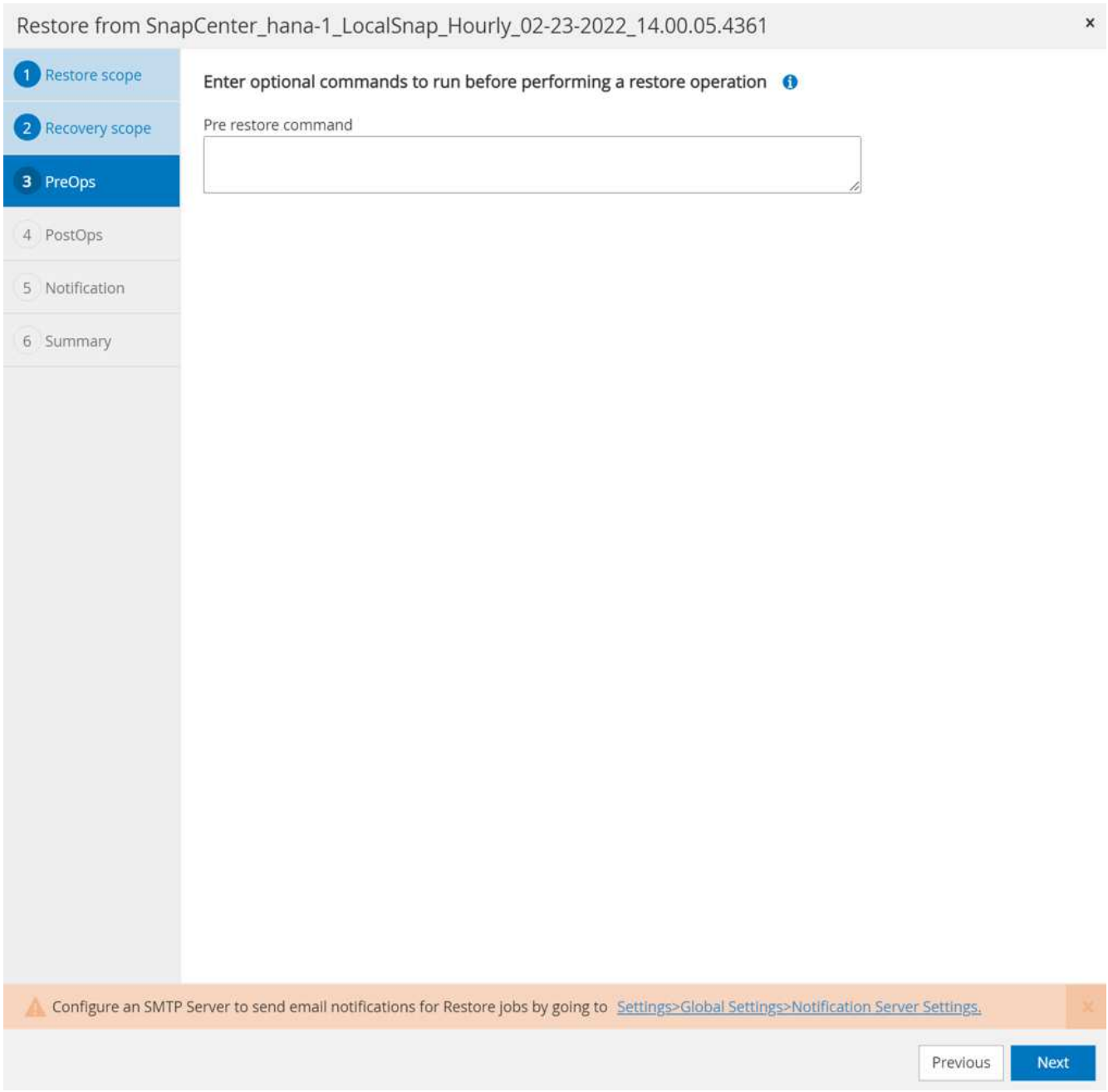


3. Wählen Sie „Recovery Scope“ aus, und stellen Sie den Speicherort für das Backup und das Katalog-Backup bereit.

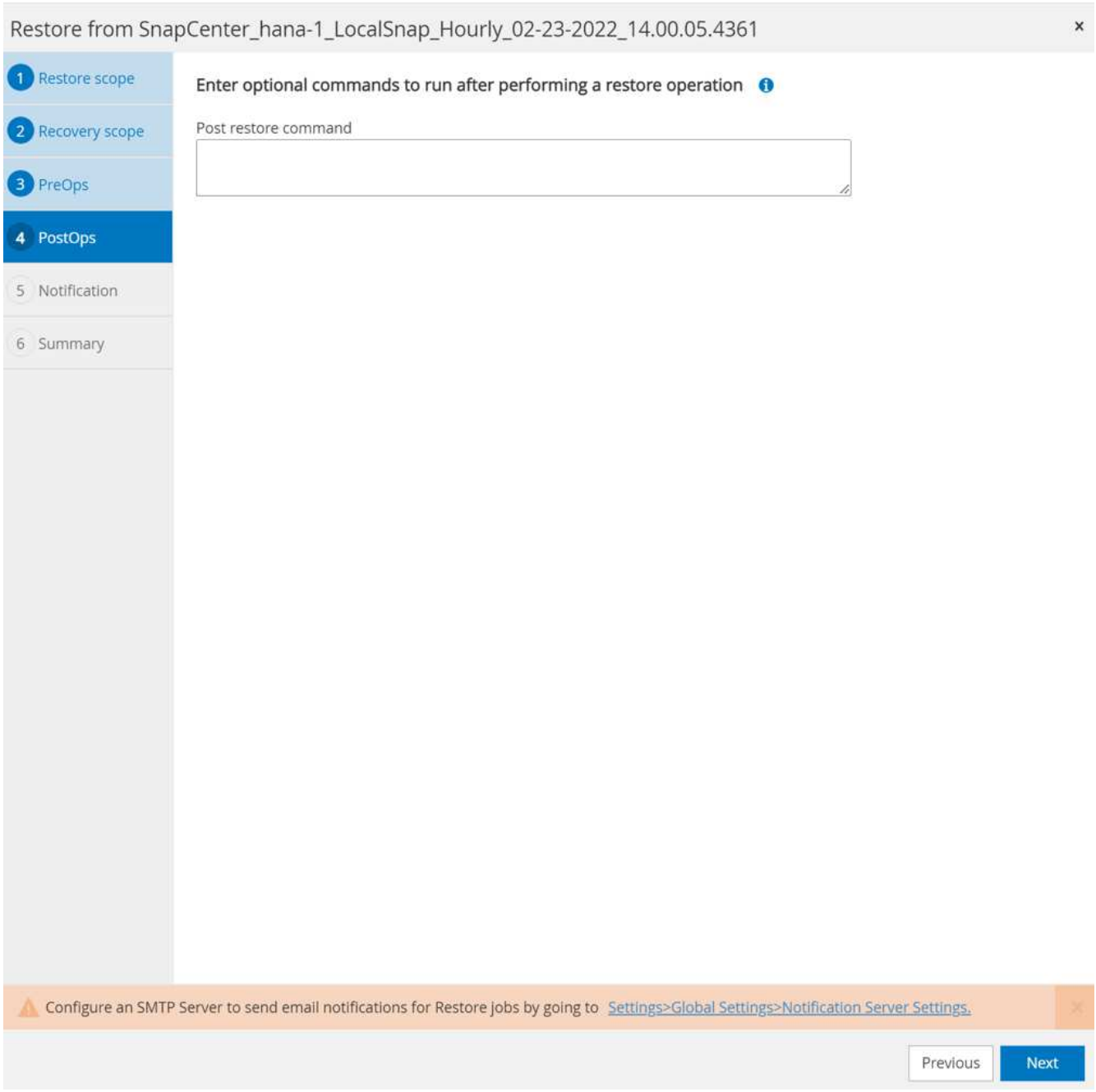
   SnapCenter verwendet den Standardpfad oder die geänderten Pfade in der HANA global.ini-Datei, um die Backup-Standorte für das Protokoll und den Katalog vorab aufzufüllen.



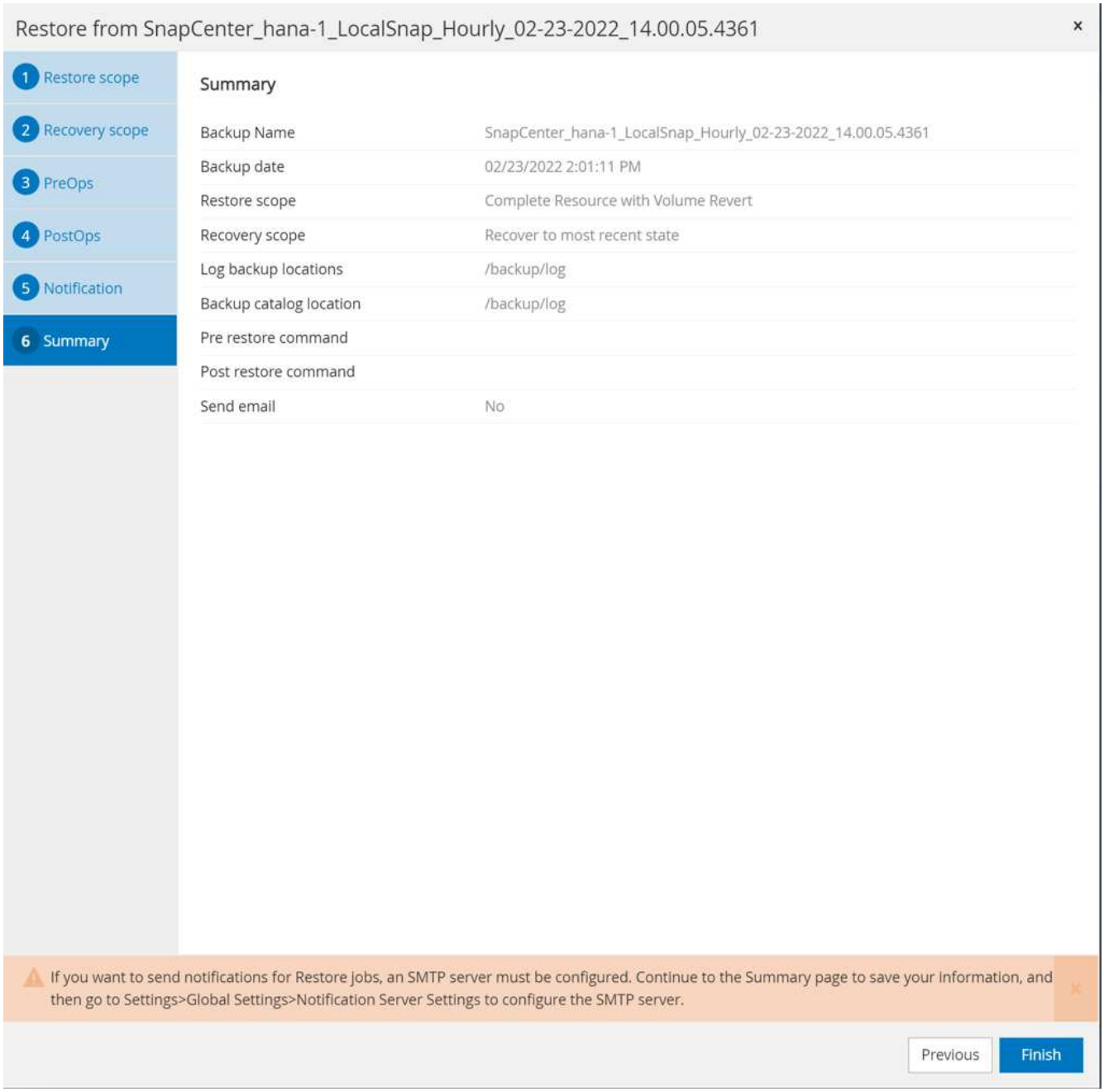
4. Geben Sie die optionalen Befehle vor der Wiederherstellung ein.



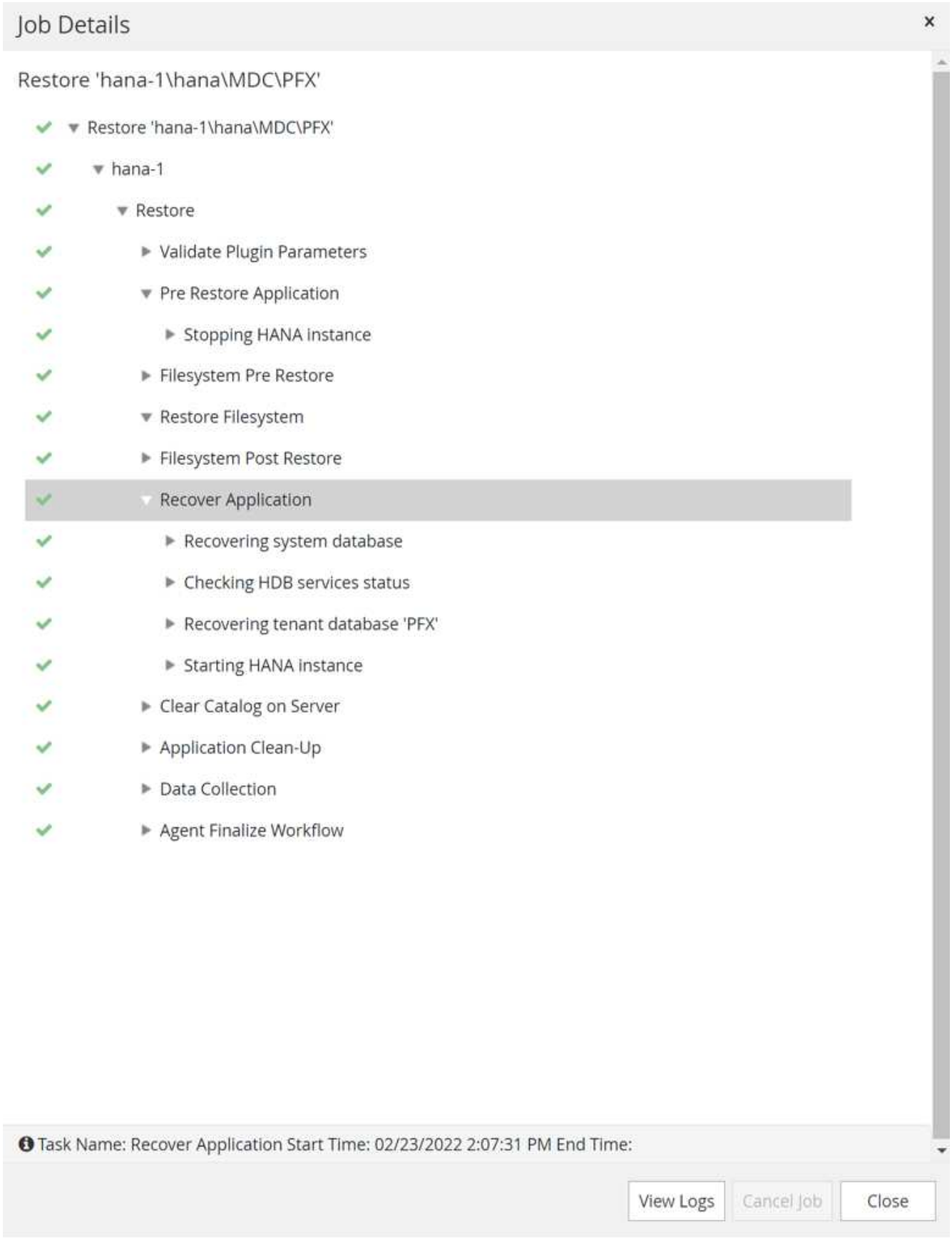
5. Geben Sie die optionalen Befehle nach der Wiederherstellung ein.



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.

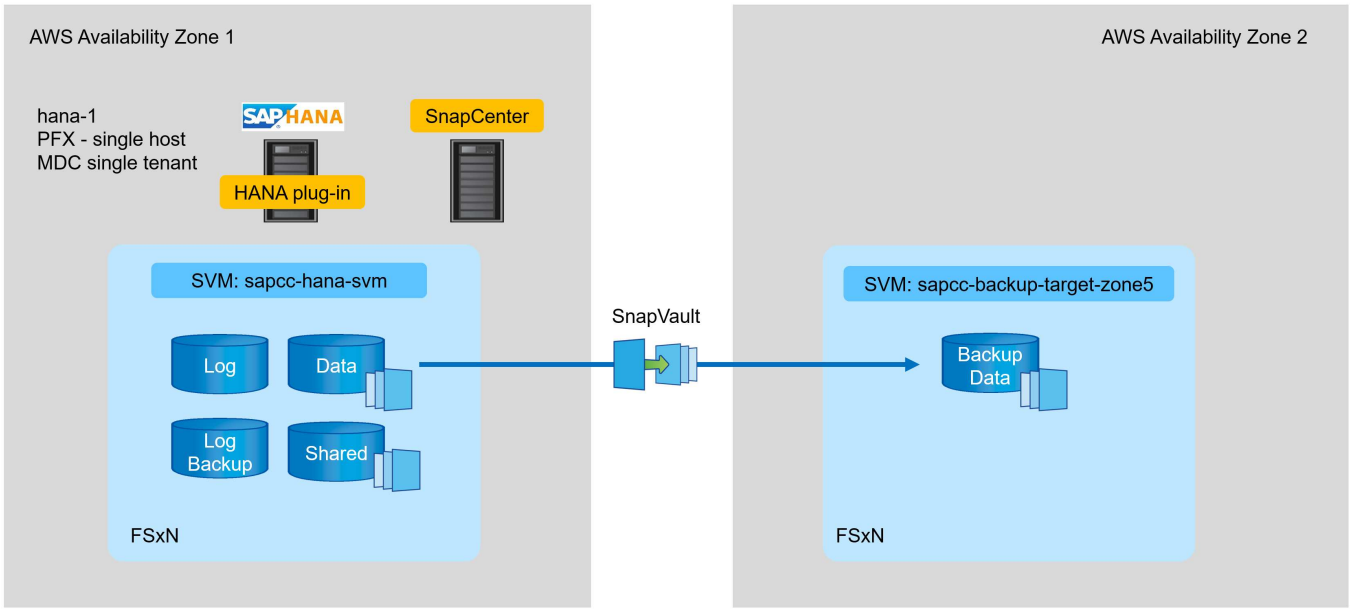

Job Details
Restore 'hana-1\hana\MDC\PFX'
Restore 'hana-1\hana\MDC\PFX'
hana-1
Restore
Validate Plugin Parameters
Pre Restore Application
Stopping HANA instance
Filesystem Pre Restore
Restore Filesystem
Filesystem Post Restore
Recover Application
Recovering system database
Checking HDB services status
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“", muss das Replikationsziel ein zweites FSX für ONTAP-Dateisystem in einer anderen Verfügbarkeitszone sein, um vor einem Ausfall des primären FSX für ONTAP-Dateisystems 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.

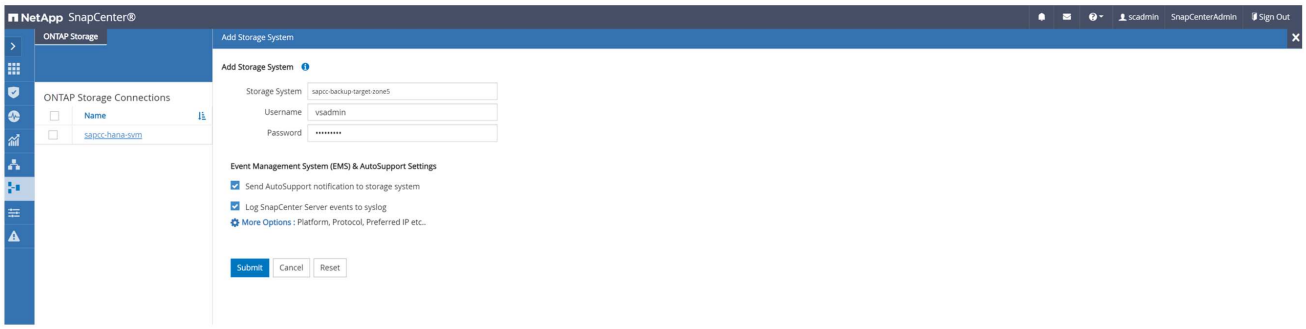
```
FsxId05f7f00af49dc7a3e::> snapmirror show

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    -
```

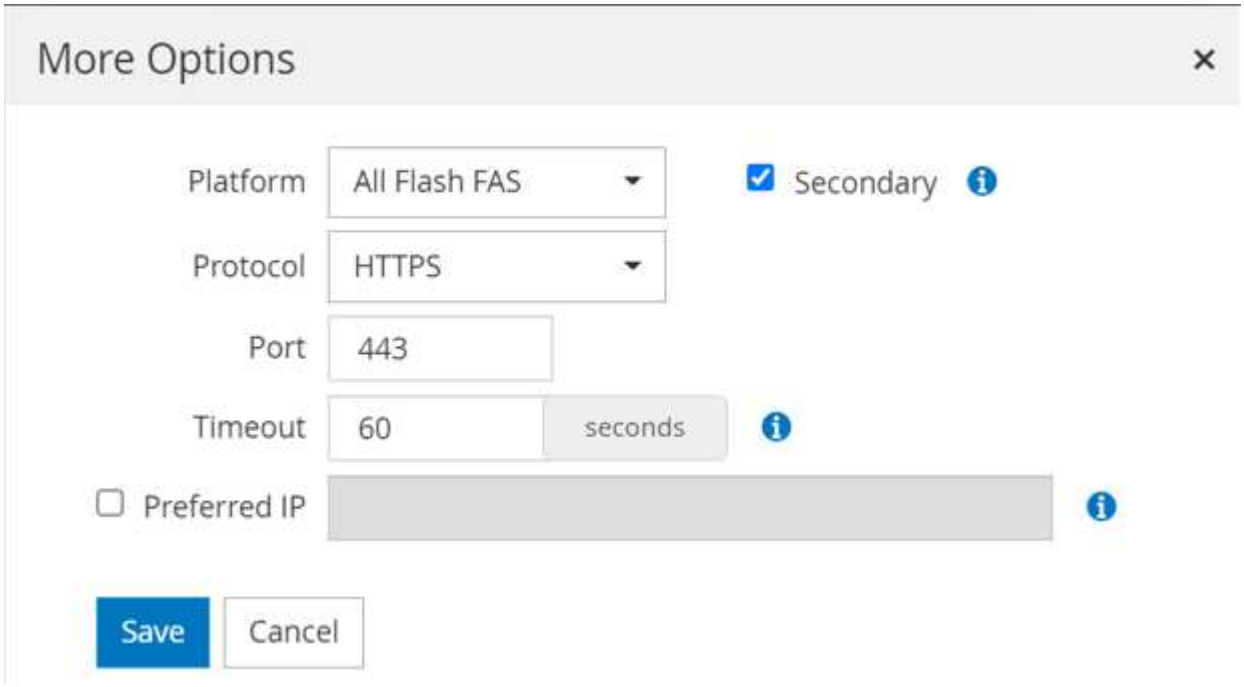
Fügen Sie eine Backup-SVM zu SnapCenter hinzu

So fügen Sie eine Backup-SVM zu SnapCenter hinzu:

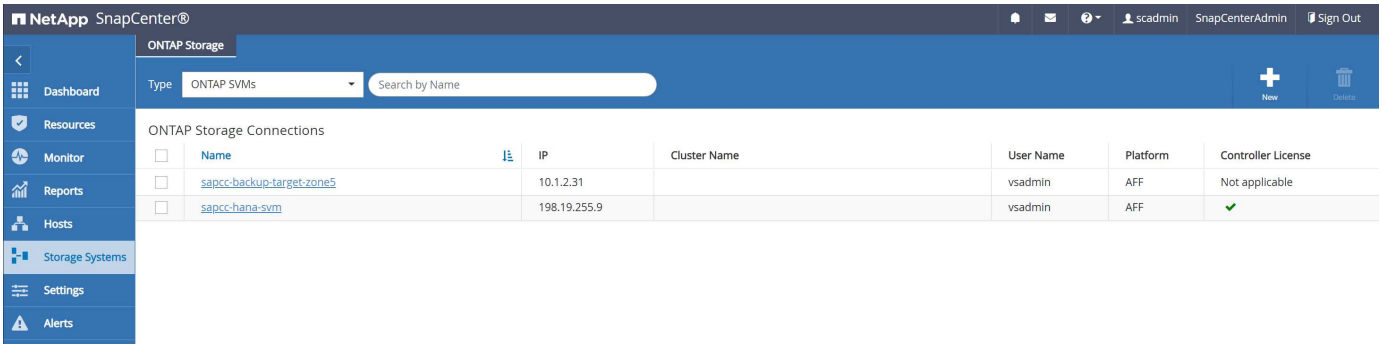
1. Konfigurieren Sie die SVM, auf der sich das SnapVault Ziel-Volume in SnapCenter befindet.



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



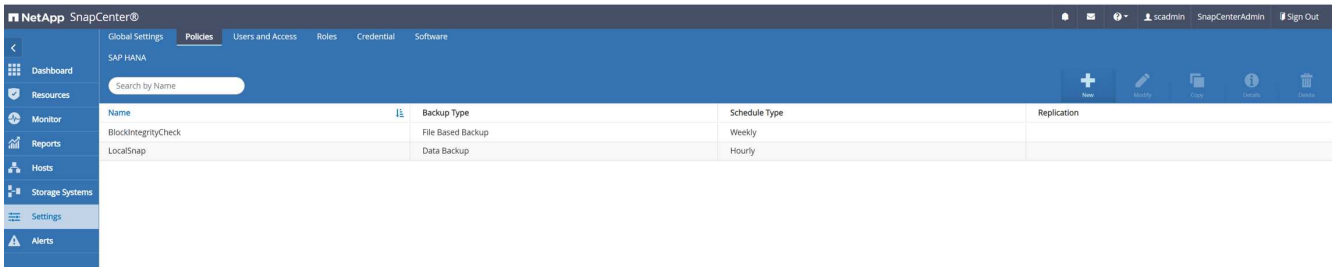
Die SVM ist jetzt in SnapCenter verfügbar.



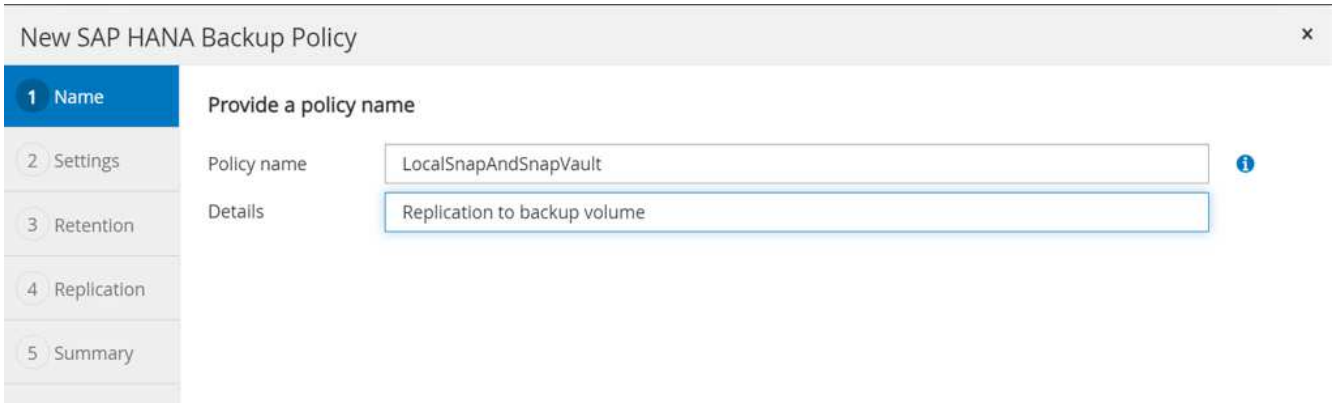
Erstellen einer neuen SnapCenter-Richtlinie für Backup-Replizierung

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

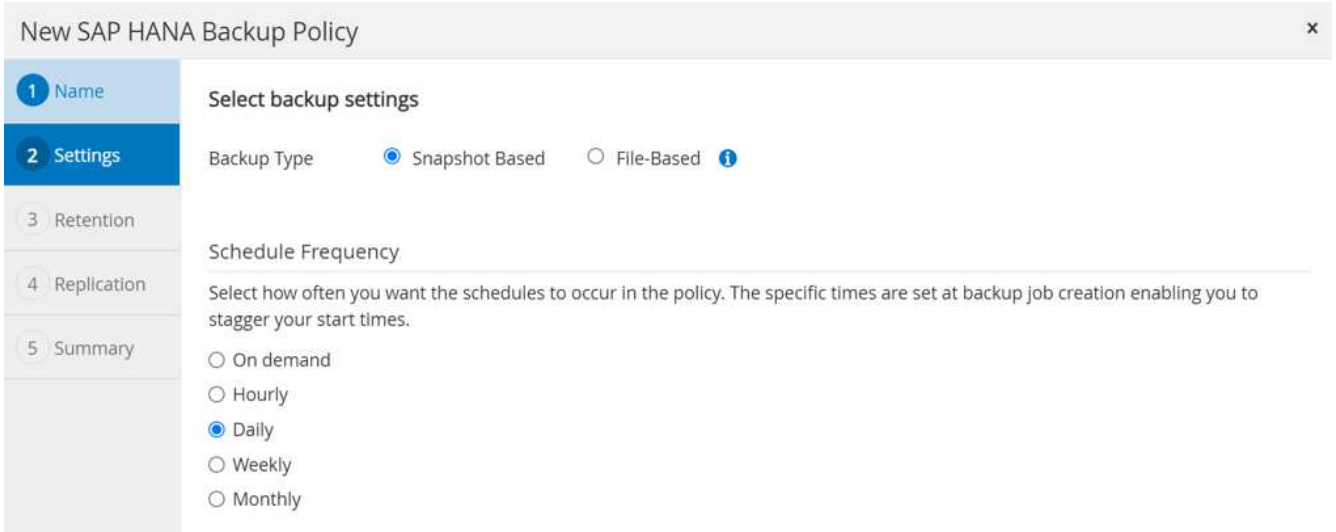
1. Geben Sie einen Namen für die Richtlinie ein.



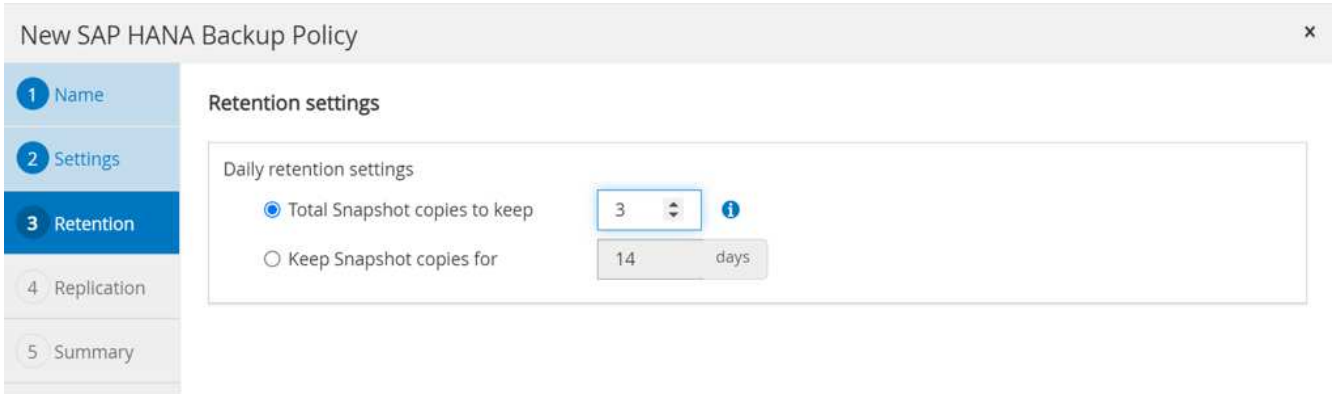
2. Wählen Sie Snapshot Backup und eine Zeitplanfrequenz aus. Für die Backup-Replizierung wird täglich verwendet.



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

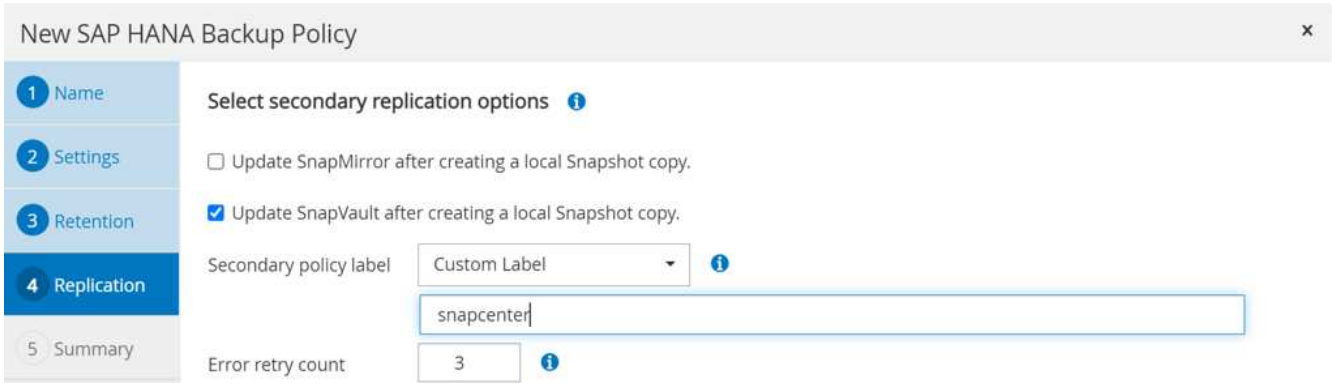


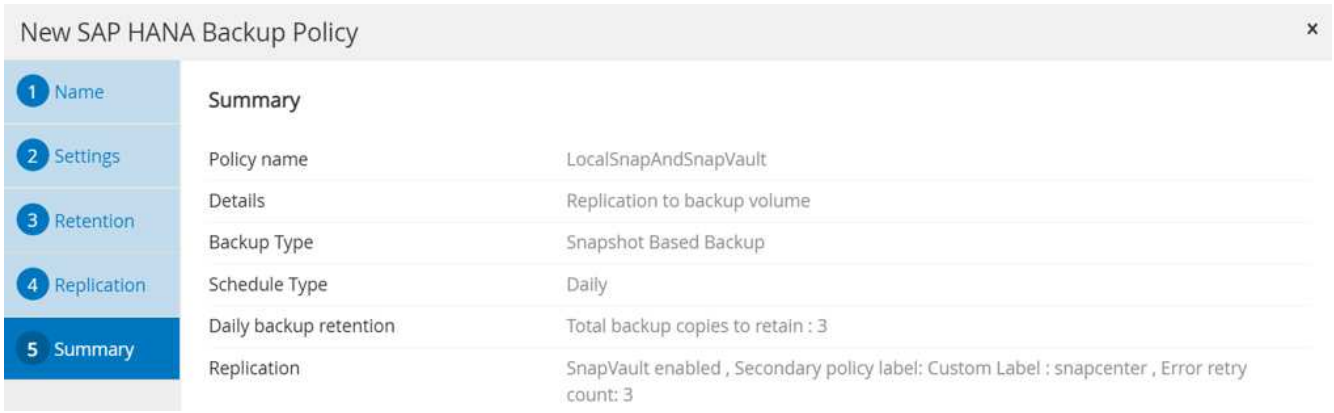
Dies ist die Aufbewahrung für die täglichen Snapshot Backups, die im primären Storage erstellt wurden. Die Aufbewahrung für sekundäre Backups auf dem SnapVault-Ziel wurde bereits mit dem Befehl „Add rule“ auf der ONTAP-Ebene konfiguriert. Siehe „Konfigurieren von Replikationsbeziehungen auf FSX für ONTAP-Dateisysteme“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



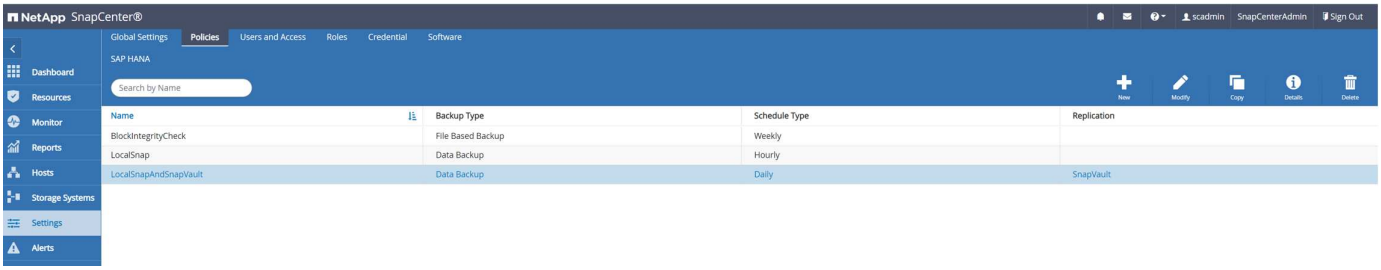
4. Wählen Sie das Feld SnapVault aktualisieren aus, und geben Sie eine benutzerdefinierte Bezeichnung an.

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



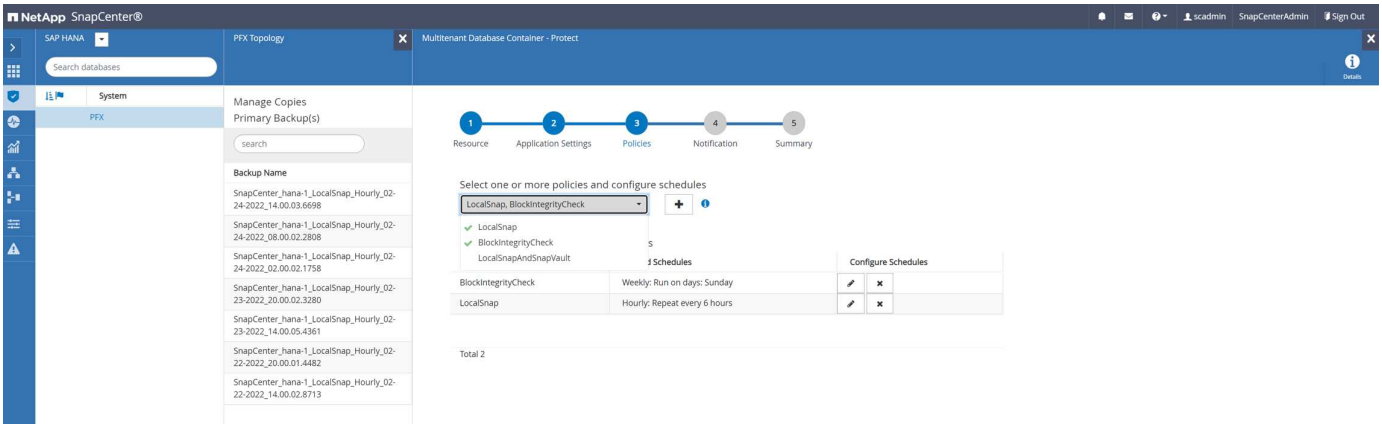


Die neue SnapCenter-Richtlinie ist jetzt konfiguriert.

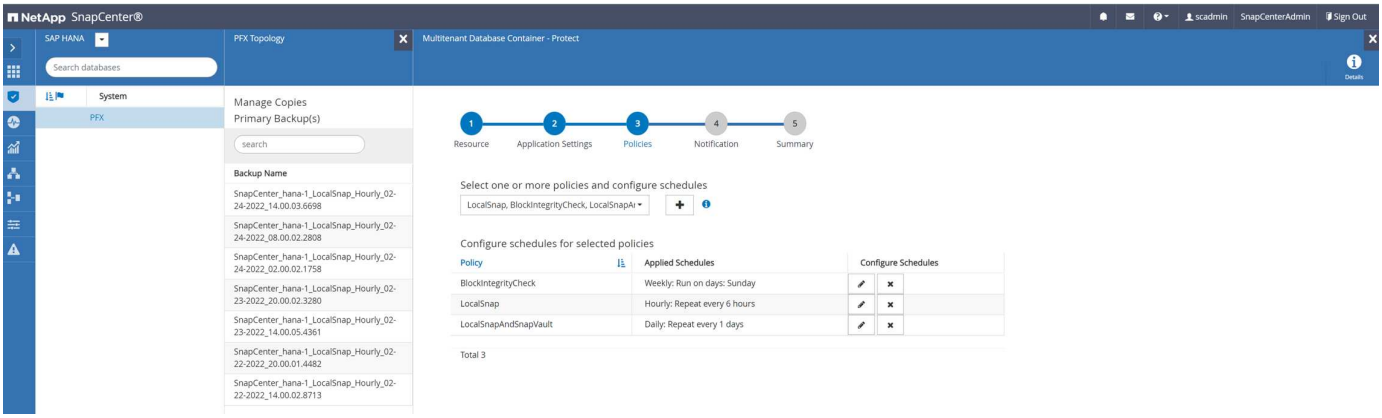


Fügen Sie eine Richtlinie zum Ressourcenschutz hinzu

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



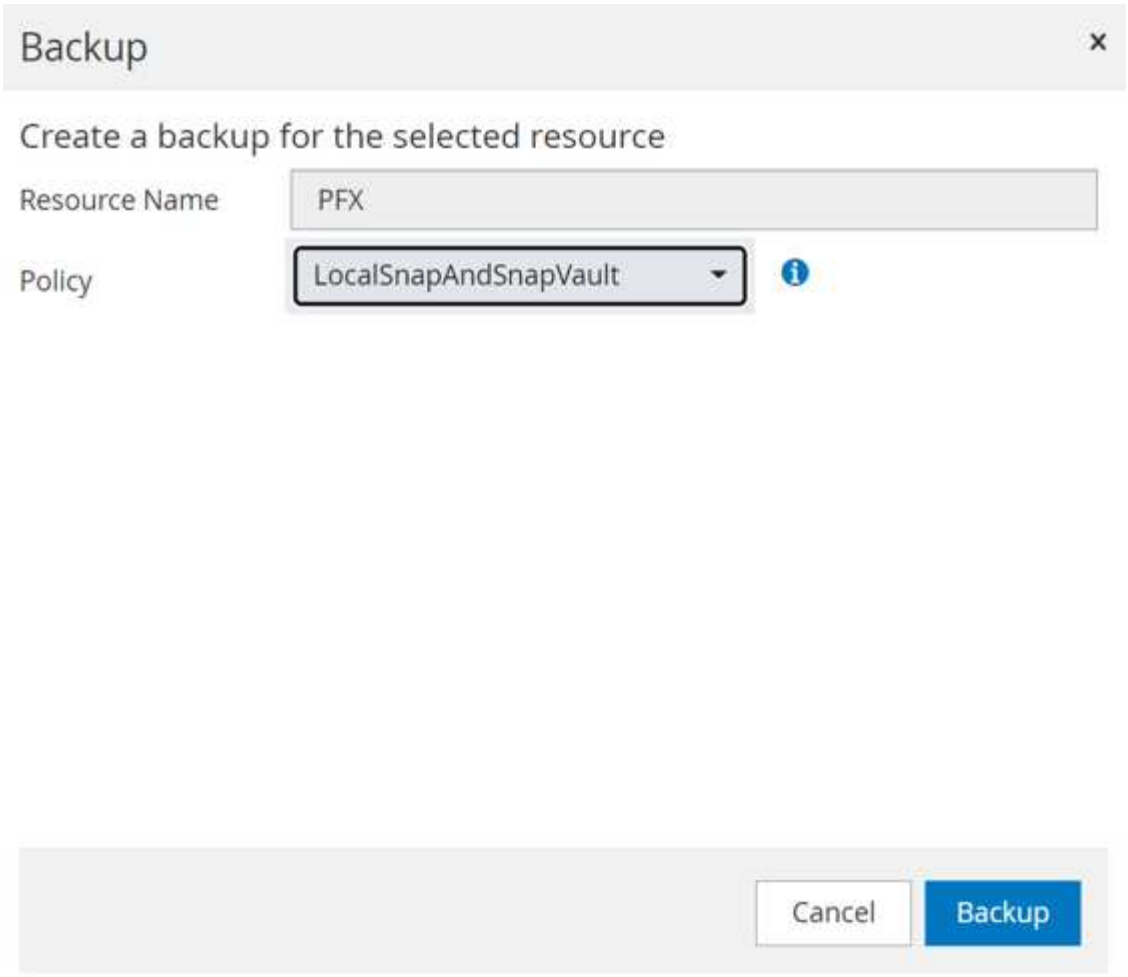
Ein täglicher Zeitplan wird in unserem Setup festgelegt.



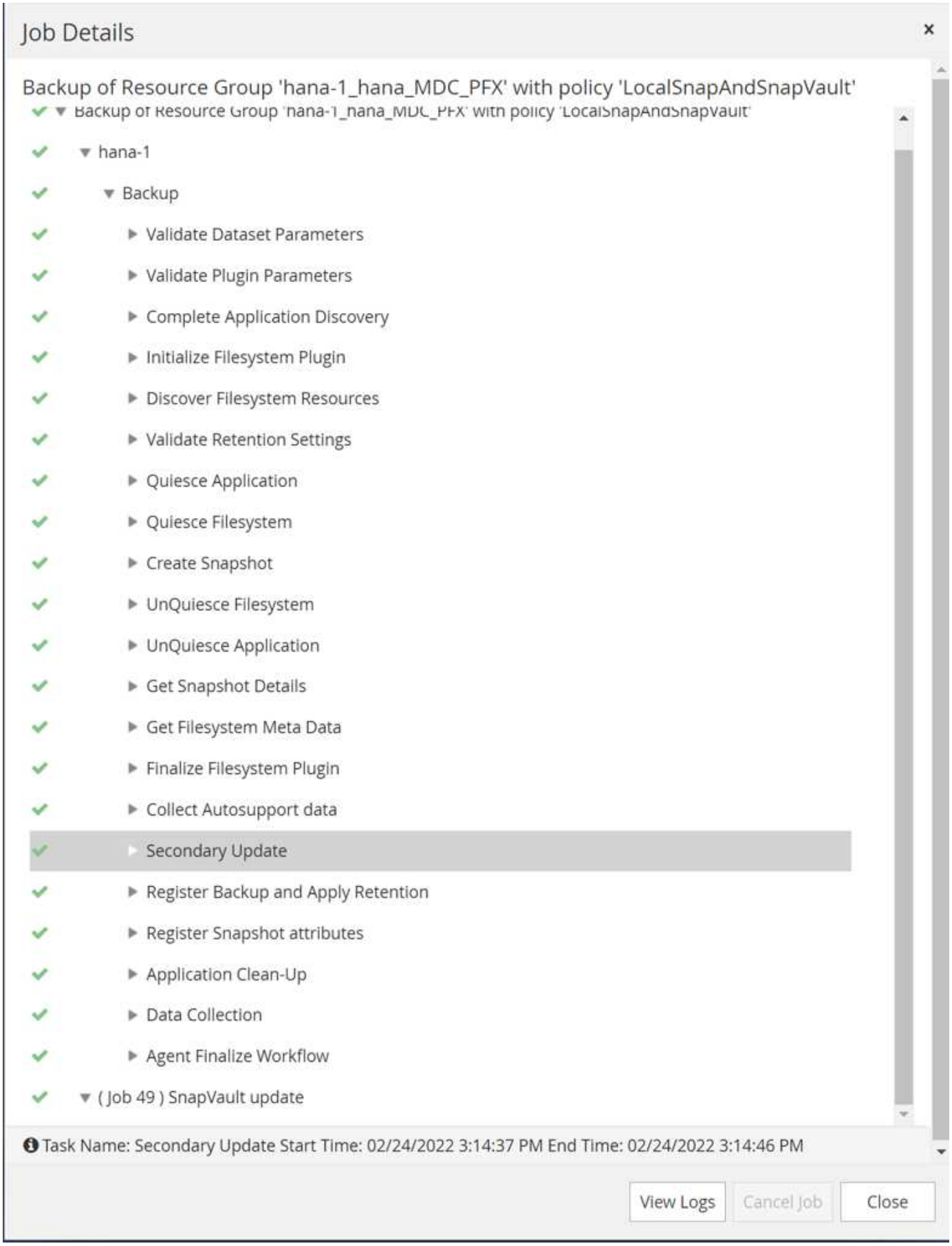
Erstellen Sie ein Backup mit Replikation

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

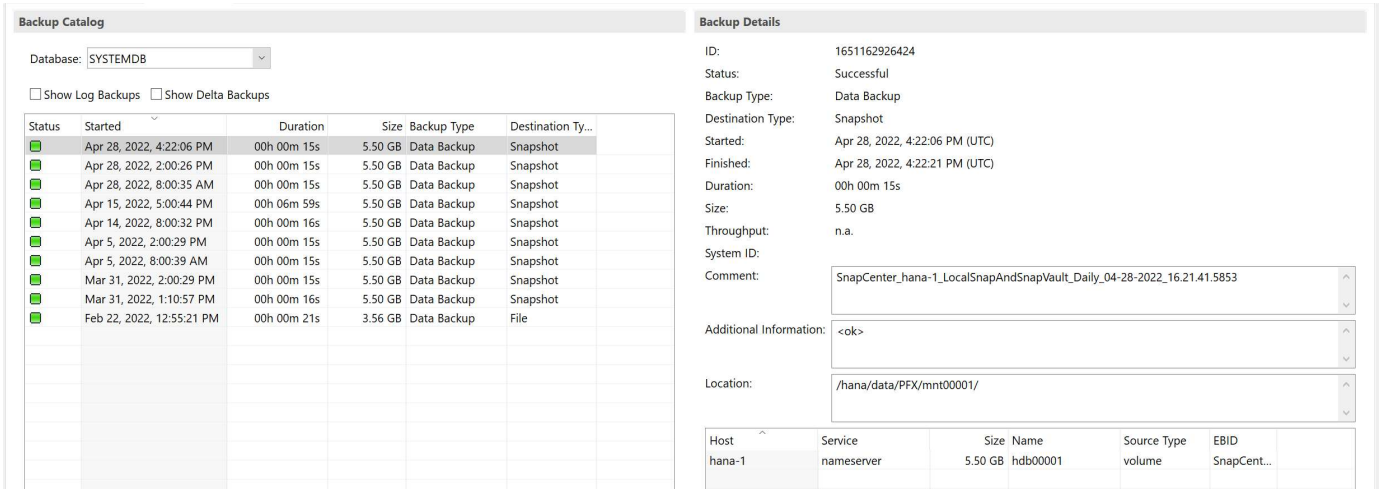
erstellt. `snapcenter`, Wie in der SnapCenter-Richtlinie konfiguriert.

```
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.
```

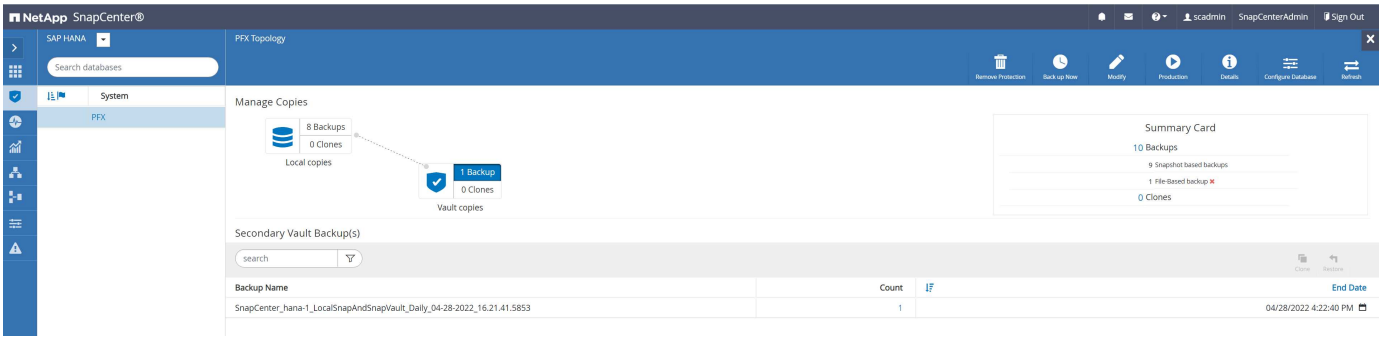
Auf dem Ziel-Volume wird eine Snapshot Kopie mit demselben Namen erstellt.

```
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.



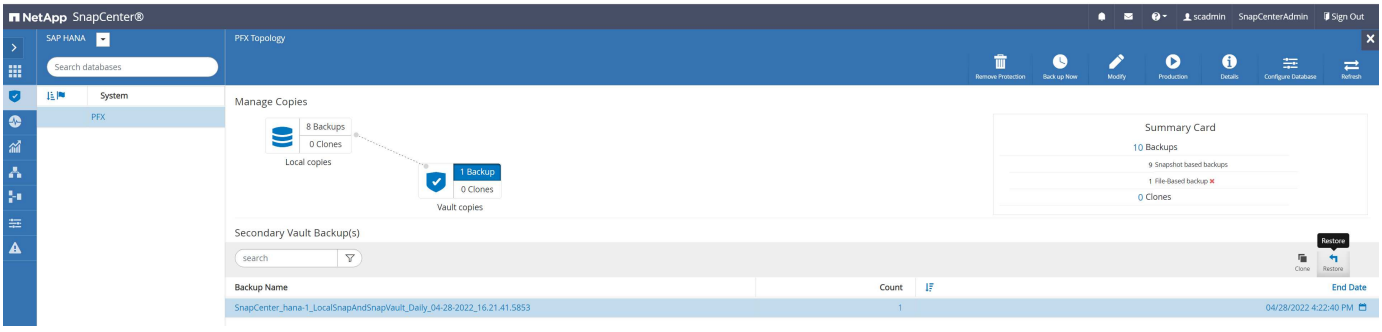
In SnapCenter können Sie die replizierten Backups auflisten, indem Sie in der Topologieansicht auf Vault Kopien klicken.



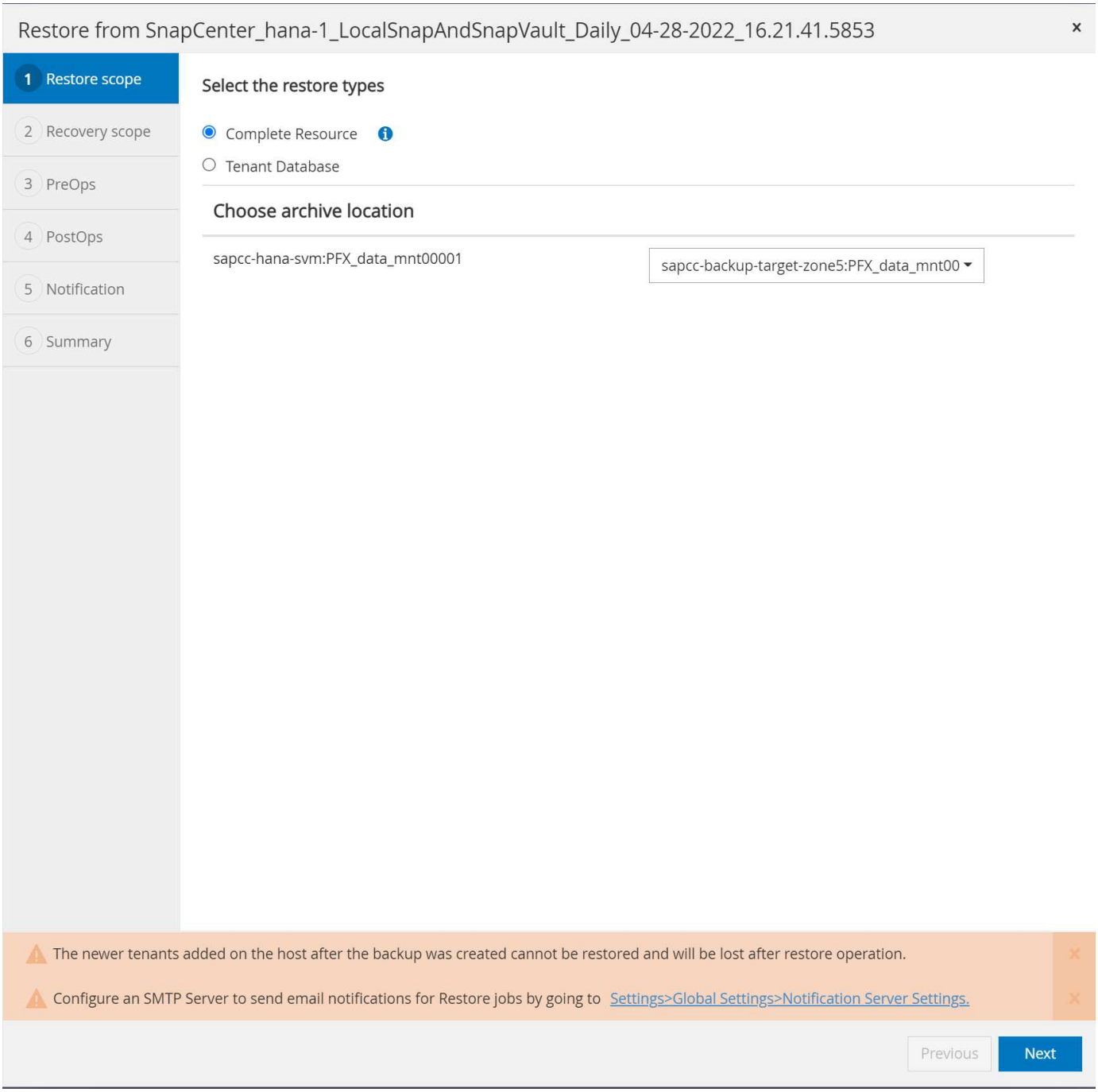
Wiederherstellung im Sekundär-Storage

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

  "Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"

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

  "Backup und Recovery mit SnapCenter"

Versionsverlauf

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

SAP HANA Datensicherung und Hochverfügbarkeit mit SnapCenter, SnapMirror Active Sync und VMware Metro Storage Cluster

SAP HANA Datensicherung und Hochverfügbarkeit mit SnapCenter, SnapMirror Active Sync und VMware Metro Storage Cluster

Dieses Dokument enthält Best Practices für die Datensicherung mit SnapCenter in einer VMware-Umgebung in Kombination mit SnapMirror Active Sync als Hochverfügbarkeitslösung für die HANA-Storage-Ressourcen.

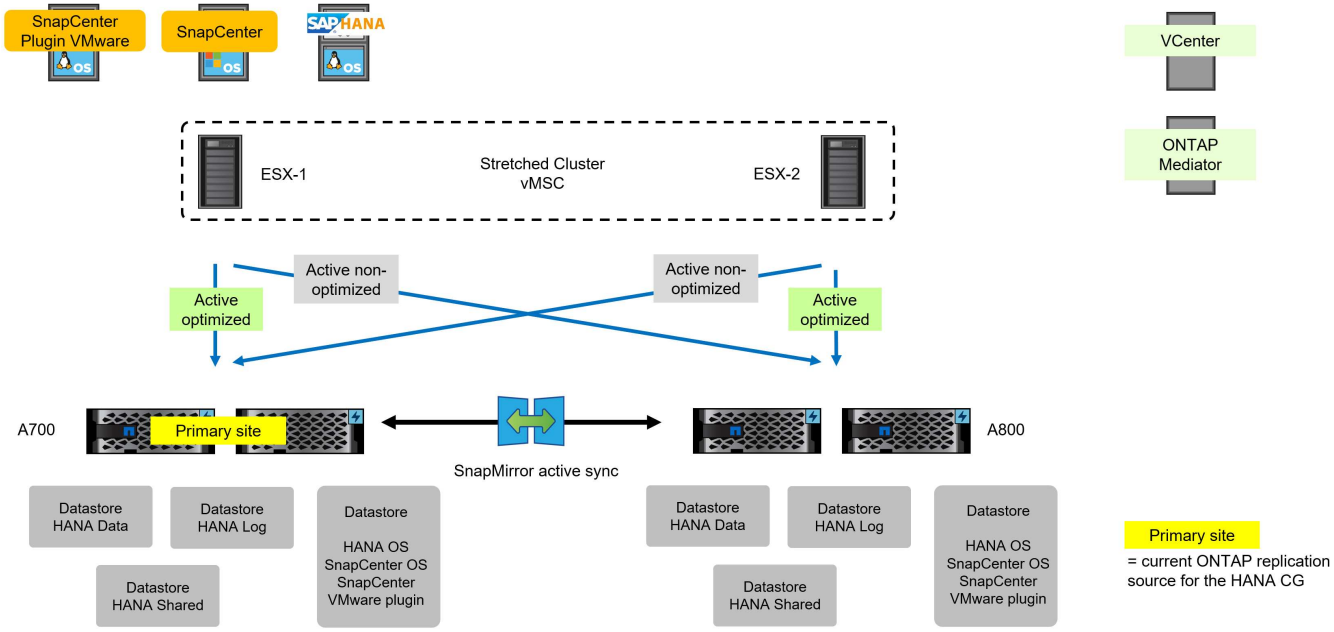
Autor: Nils Bauer, NetApp

Inhalt des vorliegenden Dokuments

Das Dokument soll keine Schritt-für-Schritt-Beschreibung der Einrichtung der gesamten Umgebung sein, sondern umfasst Konzepte und relevante Details zu:

- Setup von SAP HANA Systemen mit VMware VMFS
- SnapMirror Active Sync Konfiguration für SAP HANA
- SnapCenter-Konfiguration für HANA auf VMware mit VMFS
- SnapCenter-Konfiguration für SnapMirror Active Sync
- SnapCenter Betrieb mit HANA auf VMware und SnapMirror Active Sync

Wir werden uns auf eine VMware Metro Storage Cluster (vMSC) Konfiguration mit einem einheitlichen Zugriff Setup von SnapMirror Active Sync wie in der Abbildung unten gezeigt, aber wir werden auch kurz berühren Bare Metal sowie nicht-einheitliche Access-Konfigurationen.



Überblick über die Hochverfügbarkeit mit SAP HANA

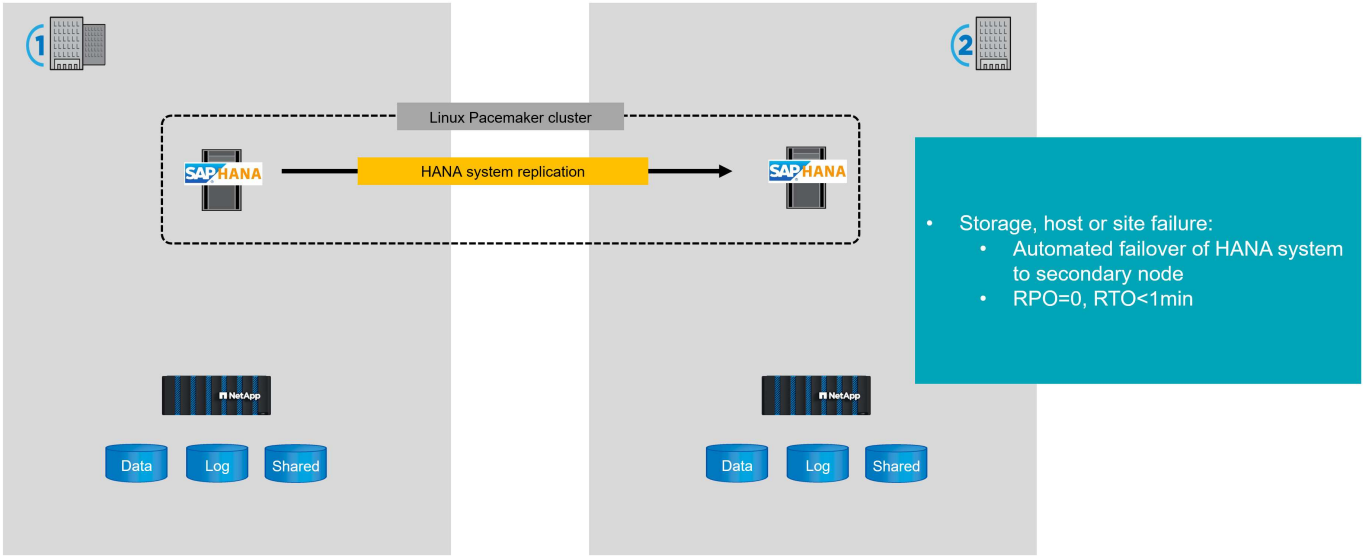
Dieses Kapitel bietet einen Überblick über Hochverfügbarkeitsoptionen für SAP HANA, bei denen die Replizierung auf Applikationsebene mit der Storage-Replizierung verglichen wird.

SAP HANA Systemreplizierung (HSR)

Die SAP HANA-Systemreplikation bietet einen Betriebsmodus, in dem die Daten synchron repliziert, in den Arbeitsspeicher vorgeladen und auf dem sekundären Host kontinuierlich aktualisiert werden. Dieser Modus ermöglicht sehr niedrige RTO-Werte, etwa eine Minute oder weniger, aber er erfordert auch einen dedizierten Server, der nur verwendet wird, um die Replikationsdaten vom Quellsystem zu empfangen. Aufgrund der geringen Failover-Zeit wird die SAP HANA Systemreplizierung auch für Wartungsarbeiten ohne Ausfallzeiten wie HANA-Software-Upgrades eingesetzt. Linux Pacemaker-Cluster-Lösungen werden in der Regel zur Automatisierung von Failover-Vorgängen eingesetzt.

Bei einem Ausfall am primären Standort, Speicher, Host oder kompletten Standort erfolgt automatisch ein Failover des HANA-Systems auf den sekundären Standort, der vom Linux Pacemaker-Cluster gesteuert wird.

Eine vollständige Beschreibung aller Konfigurationsoptionen und Replikationsszenarien finden Sie unter "SAP HANA System Replication SAP Help Portal".



Aktive NetApp SnapMirror-Synchronisierung

SnapMirror Active Sync ermöglicht Business Services auch bei einem vollständigen Standortausfall den Betrieb weiter und unterstützt Applikationen bei einem transparenten Failover mithilfe einer sekundären Kopie. Für die Auslösung eines Failover mit SnapMirror Active Sync sind keine manuellen Eingriffe oder benutzerdefinierten Skripts erforderlich. SnapMirror Active Sync wird auf AFF-Clustern, ASA-Clustern (All-Flash SAN Array) und C-Series (AFF oder ASA) unterstützt. SnapMirror Active Sync sichert Applikationen mit iSCSI- oder FCP-LUNs.

Ab ONTAP 9.15.1 unterstützt die SnapMirror Active Sync symmetrische aktiv/aktiv-Funktion. Symmetrische aktiv/aktiv-Konfiguration ermöglicht I/O-Vorgänge für Lese- und Schreibvorgänge von beiden Kopien einer geschützten LUN mit bidirektionaler synchroner Replizierung, sodass beide LUN-Kopien lokal für I/O-Vorgänge sorgen können.

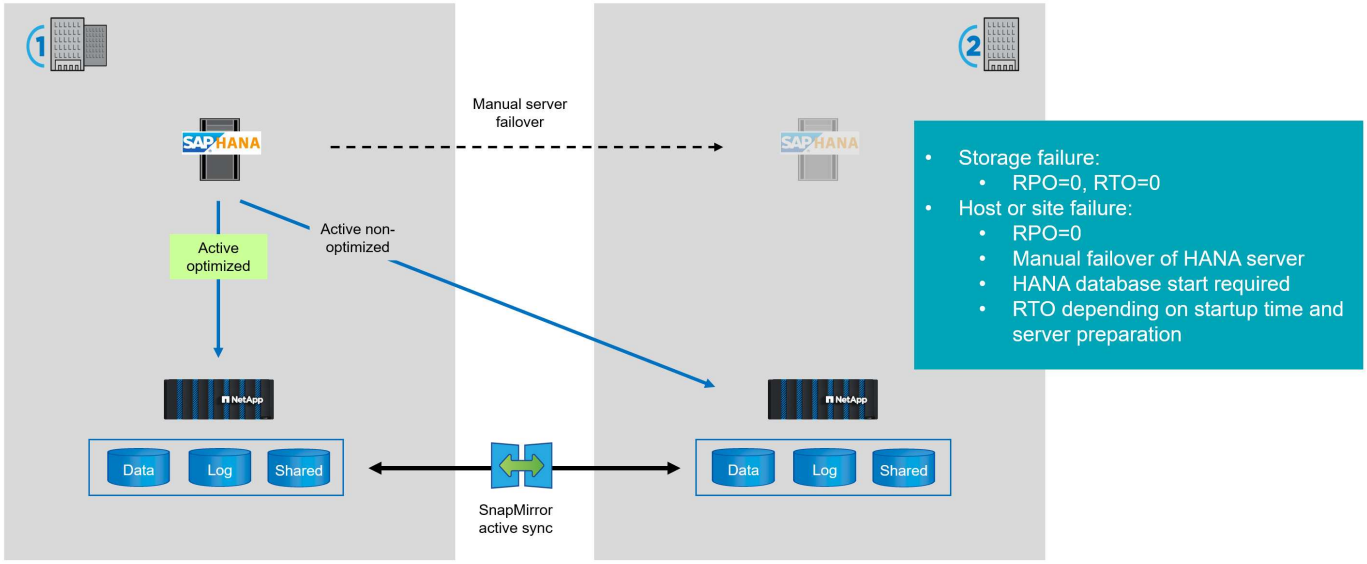
Weitere Details finden Sie unter "Übersicht über die aktive SnapMirror-Synchronisierung in ONTAP".

HANA Bare Metal

Wenn Sie SAP HANA auf einem Bare Metal-Server ausführen, können Sie SnapMirror Active Sync verwenden, um eine hochverfügbare Storage-Lösung bereitzustellen. Die Daten werden synchron repliziert und bieten daher ein RPO=0.

Bei einem Storage-Ausfall greift das HANA-System über den zweiten FCP-Pfad transparent auf die gespiegelte Kopie am sekundären Standort zu und bietet somit RTO=0.

Im Falle eines Host- oder vollständigen Standortausfalls muss ein neuer Server am sekundären Standort bereitgestellt werden, um auf die Daten vom ausgefallenen Host zugreifen zu können. Dabei handelt es sich normalerweise um ein Test- oder QA-System der gleichen Größe wie die Produktion, das nun heruntergefahren und für die Ausführung des Produktionssystems verwendet wird. Nachdem die LUNs am sekundären Standort mit dem neuen Host verbunden wurden, muss die HANA-Datenbank gestartet werden. Das gesamte RTO hängt daher von der für die Bereitstellung des Hosts benötigten Zeit und der Startzeit der HANA-Datenbank ab.

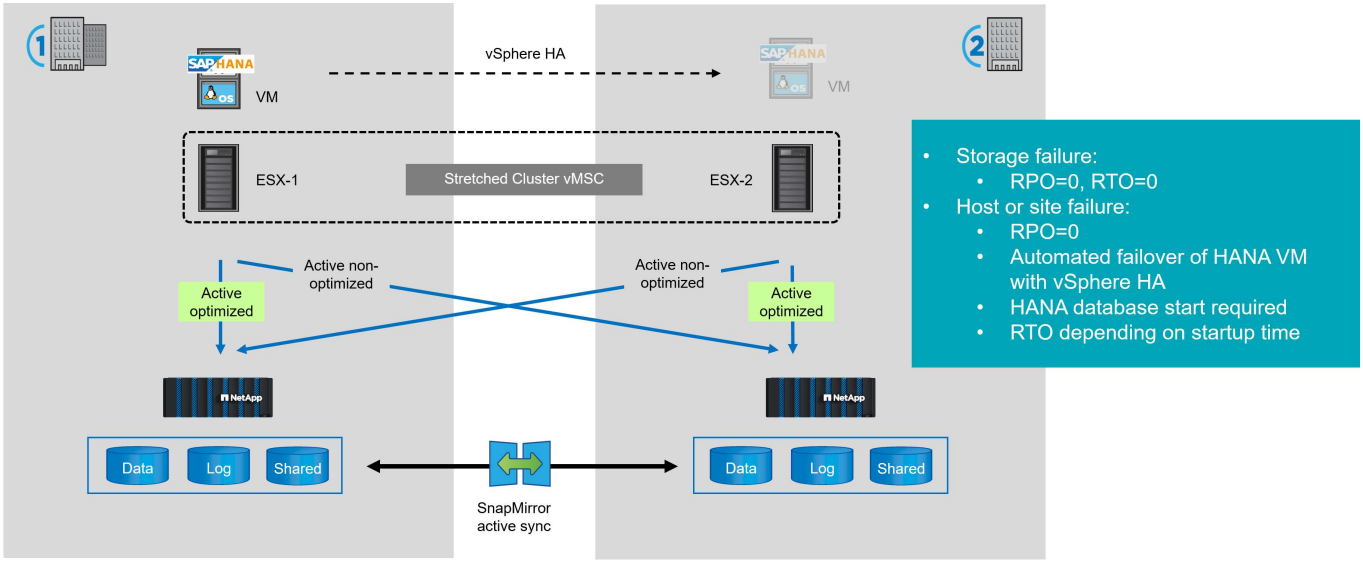


VSphere Metro Storage-Cluster (vMSC)

Wenn Sie SAP HANA in einer VMware-Umgebung mit FCP-verbundenen Datastores ausführen, können Sie SnapMirror Active Sync verwenden, um einen VMware Metro Storage-Cluster zu erstellen. In einem solchen Setup werden die vom HANA-System verwendeten Datastores synchron am sekundären Standort repliziert.

Bei einem Storage-Ausfall greift der ESX-Host automatisch auf die gespiegelte Kopie am sekundären Standort zu und liefert eine RTO=0.

Im Fall eines Host- oder vollständigen Standortausfalls wird vSphere HA verwendet, um die HANA-VM auf dem sekundären ESX-Host zu starten. Wenn die HANA VM ausgeführt wird, muss die HANA Datenbank gestartet werden. Die gesamte RTO hängt daher hauptsächlich von der Startzeit der HANA-Datenbank ab.



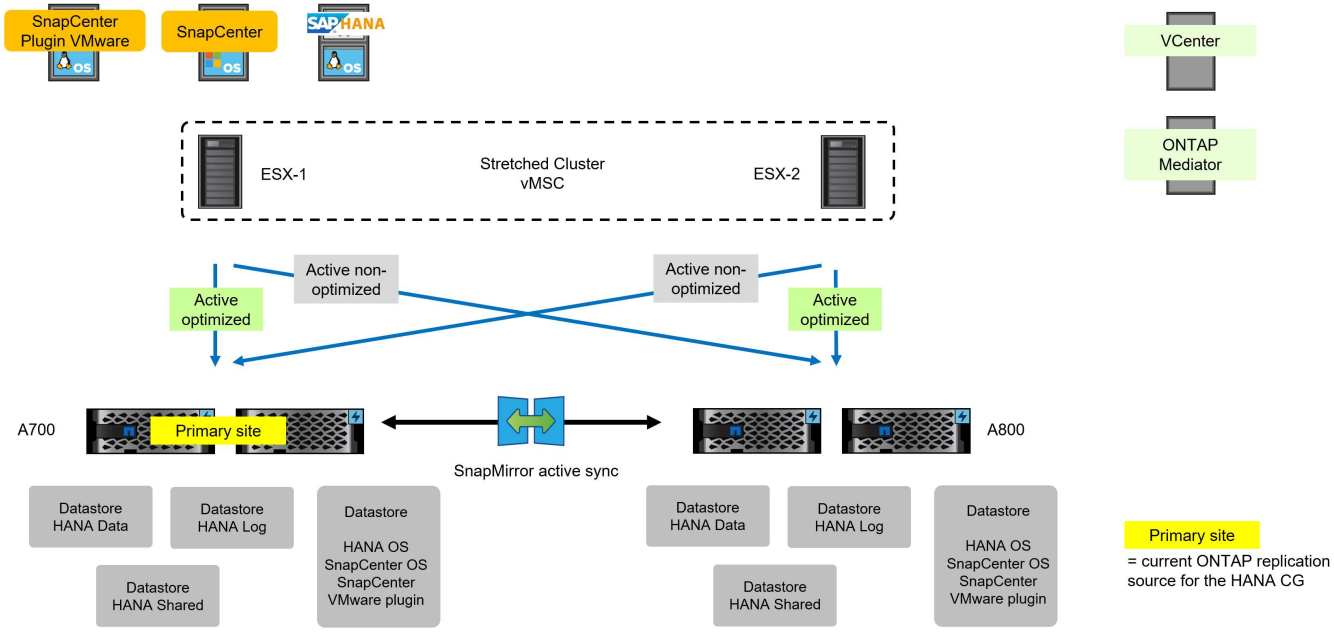
Lösungsvergleich

Die folgende Tabelle bietet eine Zusammenfassung der wichtigsten Merkmale der oben beschriebenen Lösungen.

	HANA System Replication	Aktive SnapMirror-Synchronisierung – Bare Metal	SnapMirror Active Sync – VMware vMSC
RPO bei jedem Ausfall	RPO=0 + synchrone Replikation		
RTO bei Storage-Ausfall	RTO +< 1 Min	RTO=0 + transparenter Storage-Failover	
RTO + bei Standort- oder Host-Ausfall	RTO +< 1 Min	RTO: Abhängig von der Zeit, die für die Servervorbereitung und den Start der HANA-Datenbank benötigt wird.	RTO: Abhängig von der für den Start der HANA-Datenbank erforderlichen Zeit.
Failover-Automatisierung	Ja, Automatisches Failover auf sekundären HSR-Host Gesteuert durch Schrittmachercluster.	Ja, bei Storage-Ausfällen Nein, bei Host- oder Standortausfall (Bereitstellung des Hosts, Verbinden von Storage-Ressourcen, Start der HANA-Datenbank)	Ja, bei Storage-Ausfällen Ja, bei Host- oder Standortausfall (Failover von VM zum anderen Standort automatisiert mit vSphere HA, Start der HANA-Datenbank)
Dedizierter Server am sekundären Standort erforderlich	Ja, Daten mussten vorab in den Speicher geladen und ein schnelles Failover ohne Datenbankstart ermöglicht werden.	Nein, Server ist nur bei Failover erforderlich. In der Regel wird der für die Qualitätssicherung verwendete Server dann für die Produktion genutzt.	Nein, Ressourcen auf ESX Host sind nur im Failover-Fall erforderlich. In der Regel werden QA-Ressourcen dann für die Produktion genutzt.

Beispiel für eine Konfigurationsübersicht

Im Lab Setup verwenden wir eine einheitliche Zugriffskonfiguration, auf der beide ESX Hosts Zugriff auf beide Storage Cluster haben. In den nächsten Abschnitten beschreiben wir die einheitliche Zugriffskonfiguration, heben aber auch die Unterschiede für ein nicht einheitliches Setup hervor.



Softwareversionen

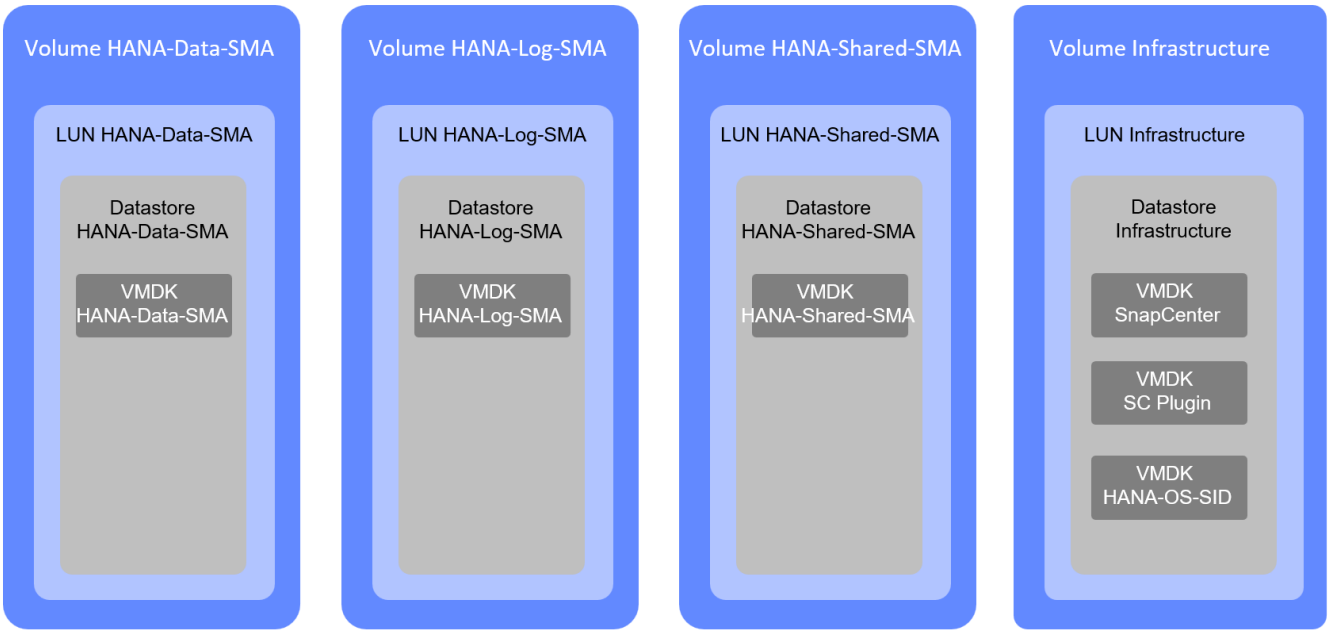
Software	Version
ONTAP	A700: 9.15.1 P7, A800: 9.16.1 RC1
VSphere Client	8.0.3
ESXi	8.0.3
SnapCenter Plug-in für vSphere	6.0.1
Linux BS	SLES FÜR SAP 15 SP5
SAP HANA	2,0 SPS8
SnapCenter	6.0.1

HANA-Systembereitstellung und -Installation

In diesem Kapitel werden die Installation und Konfiguration des für eine VMware-Einrichtung mithilfe von VMFS spezifischen SAP HANA-Systems beschrieben. Weitere allgemeine Best Practices finden Sie unter "Technischer Bericht: SAP HANA on NetApp AFF Systems with Fibre Channel Protocol".

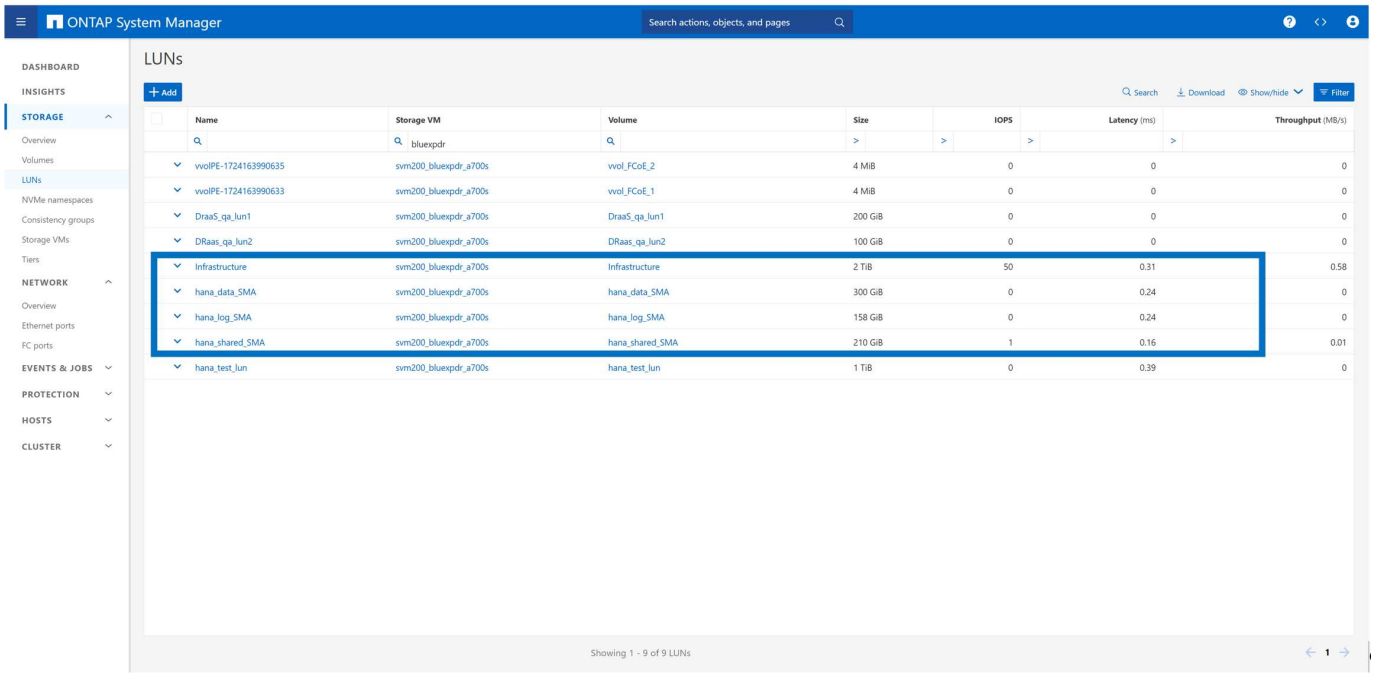
Storage-Konfiguration

Die Abbildung unten zeigt die Storage- und Datastore-Konfiguration für das HANA-System. Sie müssen für jedes Dateisystem des HANA-Systems ein dediziertes Volume, eine LUN oder einen Datastore konfigurieren. Datastores dürfen nicht über mehrere HANA-Systeme oder andere Workloads hinweg freigegeben werden.



Alle drei LUNs des HANA-Systems (hana_Data_SMA, hana_log+*SAM und hana+_shared*+++SMA) sowie die LUN für die OS-Images und SnapCenter-Komponenten wurden beim A700-Storage-Cluster bereitgestellt.

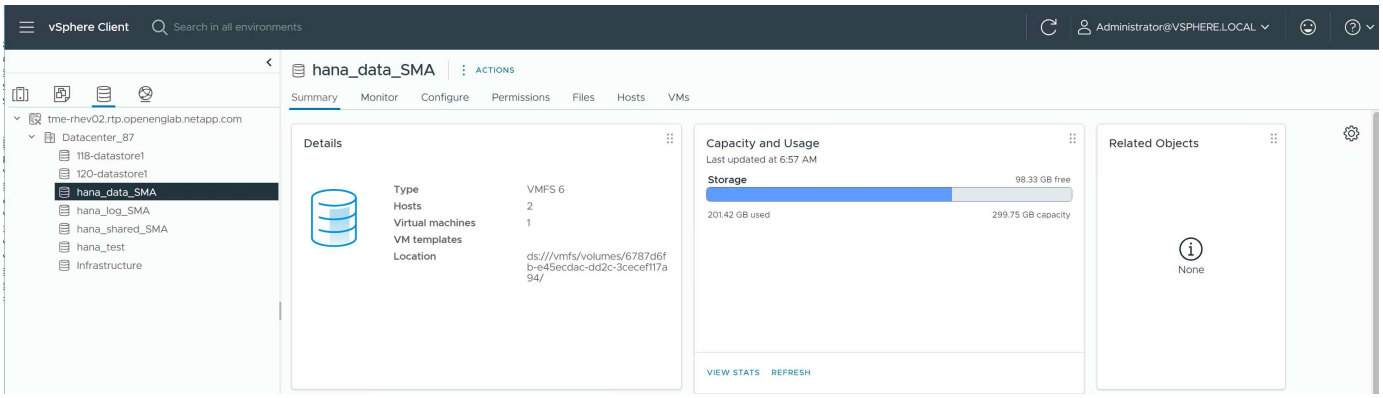
Alle Volumes des HANA-Systems müssen in derselben SVM bereitgestellt werden. In der später beschriebenen Konfiguration für aktive SnapMirror-Synchronisierung wird eine Konsistenzgruppe über alle drei HANA-Volumes erstellt, bei der sich die Volumes in derselben SVM befinden müssen. Das Infrastruktur-Volume wird sich in einer anderen Konsistenzgruppe befinden und könnte sich daher in einer anderen SVM befinden.



Eine Initiatorgruppe muss konfiguriert werden und die oben genannten LUNs müssen dem ESX-1 Host zugeordnet werden, der sich in unserem Lab-Setup in unmittelbarer Nähe des A700 Storage-Systems befindet.

Datastore-Bereitstellung

Wir haben drei Datastores für das HANA-System mit den drei LUNs erstellt, die wir zuvor bereitgestellt haben. Darüber hinaus haben wir mit der Infrastruktur-LUN einen Infrastruktur-Datastore erstellt.

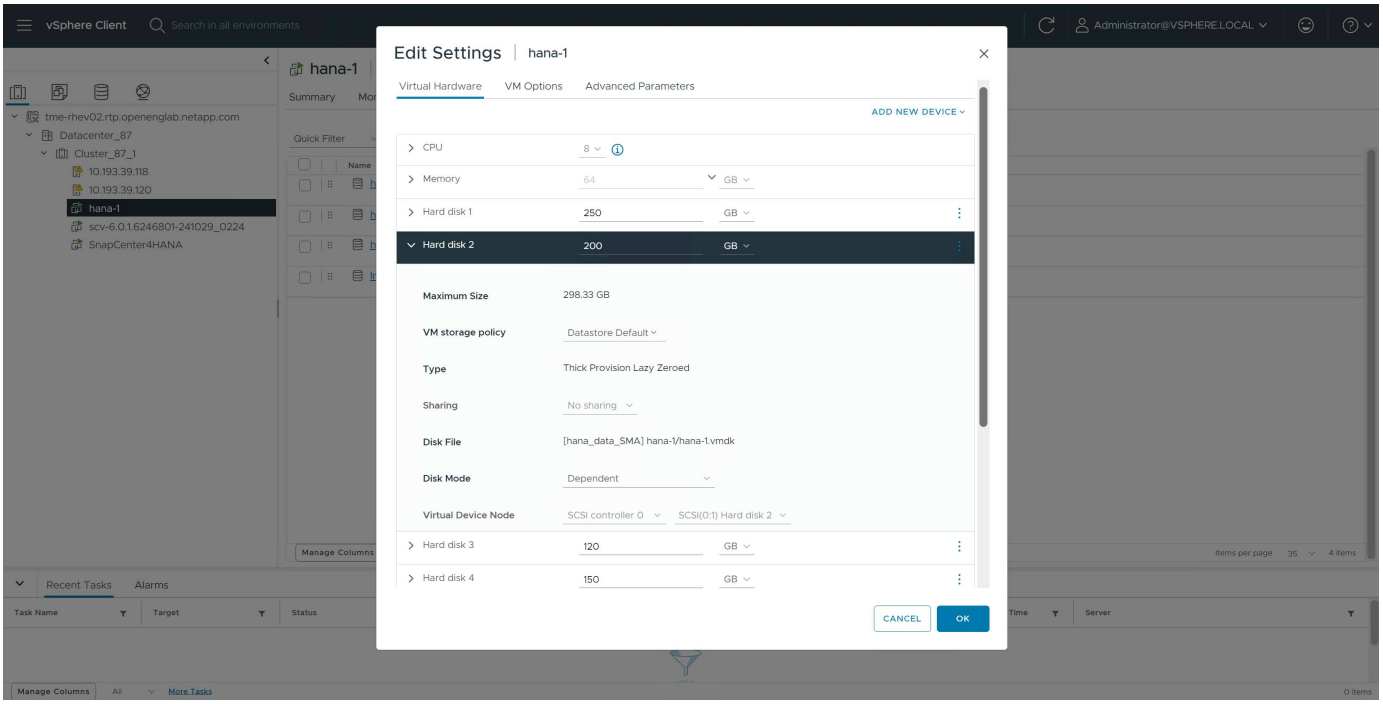


VM-Bereitstellung und Betriebssysteminstallation

In unserem Lab-Setup haben wir eine neue VM implementiert und die VMDK für das Linux Betriebssystem im Infrastruktur-Datenspeicher platziert.

Konfiguration von VM-Festplatten

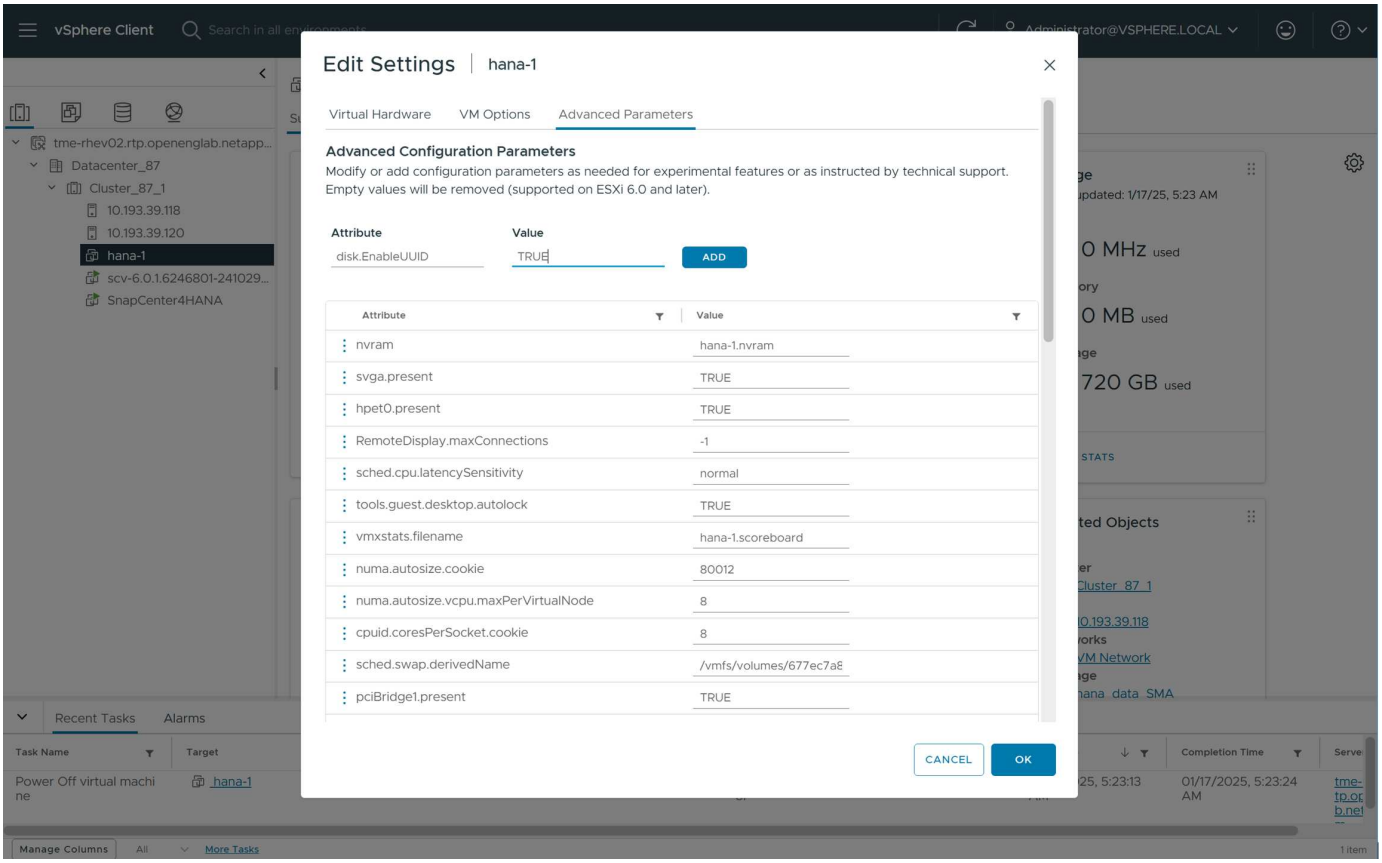
Der HANA VM wurden drei neue Festplatten hinzugefügt, jede Festplatte in einem der Datenspeicher, die für das HANA-System erstellt wurden.



VM-Parametereinstellung

Der Parameter Disk.EnableUUID muss hinzugefügt und auf TRUE gesetzt werden. Der Parameter wird von SnapCenter benötigt. Wenn nicht festgelegt, schlägt der SnapCenter-Vorgang „Ermittlung der virtuellen Ressource“ fehl.

Die VM muss angehalten werden, bevor Parameter hinzugefügt werden können.



Die Funktionalität kann mit dem folgenden Befehl überprüft werden.

```
hana-1:~ # sg_inq /dev/sdd
standard INQUIRY:
PQual=0 PDT=0 RMB=0 LU_CONG=0 hot_pluggable=0 version=0x06 [SPC-4]
[AERC=0] [TrmTsk=] NormACA=0 HiSUP=0 Resp_data_format=2
SCCS=0 ACC=0 TPGS=0 3PC=0 Protect=0 [BQue=0]
EncServ=0 MultiP=0 [MChngr=0] [ACKREQQ=0] Addr16=0
[RelAdr=0] WBus16=1 Sync=1 [Linked=0] [TranDis=0] CmdQue=1
length=36 (0x24) Peripheral device type: disk
Vendor identification: VMware
Product identification: Virtual disk
Product revision level: 2.0
Unit serial number: 6000c293fecf25ac6bc457af67fe1f54
```

Vorbereitung des Dateisystems auf Linux-Host

Erstellung des xfs-Dateisystems auf neuen Platten

Die Gerätenamen der neuen Festplatten können mit dem folgenden Befehl überprüft werden.

```
hana-1:/install # lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 250G 0 disk
├─sda1 8:1 0 256M 0 part /boot/efi
└─sda2 8:2 0 82G 0 part
├─system-root 254:0 0 60G 0 lvm /root
│ /var
│ /usr/local
│ /tmp
│ /srv
│ /opt
│ /home
│ /boot/grub2/x86++_++64-efi
│ /boot/grub2/i386-pc
│ /.snapshots
│ /
└─system-swap 254:1 0 2G 0 lvm SWAP
sdb 8:16 0 200G 0 disk
sdc 8:32 0 120G 0 disk
sdd 8:48 0 150G 0 disk
sr0 11:0 1 1024M 0 rom
hana-1:/install #
```

Auf jedem der drei neuen Festplatten wurde ein xfs-Dateisystem erstellt.

```
hana-1:/install # mkfs.xfs /dev/sdb
meta-data=/dev/sdb isize=512 agcount=4, agsize=7864320 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=31457280, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=15360, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0

hana-1:/install # mkfs.xfs /dev/sdc
meta-data=/dev/sdc isize=512 agcount=4, agsize=7864320 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=31457280, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=15360, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0

hana-1:/install # mkfs.xfs /dev/sdd
meta-data=/dev/sdd isize=512 agcount=4, agsize=9830400 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=39321600, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=19200, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
hana-1:/install #
```

Erstellung von Bereitstellungspunkten

```
hana-1:/ # mkdir -p /hana/data/SMA/mnt00001
hana-1:/ # mkdir -p /hana/log/SMA/mnt00001
hana-1:/ # mkdir -p /hana/shared
hana-1:/ # chmod -R 777 /hana/log/SMA
hana-1:/ # chmod -R 777 /hana/data/SMA
hana-1:/ # chmod -R 777 /hana/shared
```

Konfiguration von /etc/fstab

```
hana-1:/install # cat /etc/fstab
/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=/@/var 0 0
/dev/system/root /usr/local btrfs subvol=/@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=/@/tmp 0 0
/dev/system/root /srv btrfs subvol=/@/srv 0 0
/dev/system/root /root btrfs subvol=/@/root 0 0
/dev/system/root /opt btrfs subvol=/@/opt 0 0
/dev/system/root /home btrfs subvol=/@/home 0 0
/dev/system/root /boot/grub2/x86_64-efi btrfs subvol=/@/boot/grub2/x86_64-
efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=/@/.snapshots 0 0
UUID=2E8C-48E1 /boot/efi vfat utf8 0 2
/dev/sdb /hana/data/SMA/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/SMA/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
hana-1:/install #

hana-1:/install # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 4.0K 49G 1% /dev/shm
tmpfs 13G 26M 13G 1% /run
tmpfs 4.0M 0 4.0M 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 35G 25G 58% /
/dev/mapper/system-root 60G 35G 25G 58% /.snapshots
/dev/mapper/system-root 60G 35G 25G 58% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 35G 25G 58% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 35G 25G 58% /home
/dev/mapper/system-root 60G 35G 25G 58% /opt
/dev/mapper/system-root 60G 35G 25G 58% /srv
/dev/mapper/system-root 60G 35G 25G 58% /tmp
/dev/mapper/system-root 60G 35G 25G 58% /usr/local
/dev/mapper/system-root 60G 35G 25G 58% /var
/dev/mapper/system-root 60G 35G 25G 58% /root
/dev/sda1 253M 5.1M 247M 3% /boot/efi
tmpfs 6.3G 56K 6.3G 1% /run/user/0
/dev/sdb 200G 237M 200G 1% /hana/data/SMA/mnt00001
/dev/sdc 120G 155M 120G 1% /hana/log/SMA/mnt00001
/dev/sdd 150G 186M 150G 1% /hana/shared
hana-1:/install #
```

HANA-Installation

Die HANA-Installation kann nun ausgeführt werden.

> Bei der beschriebenen Konfiguration befindet sich das Verzeichnis /usr/sap/SMA auf der OS VMDK. Wenn /usr/sap/SMA in der gemeinsam genutzten VMDK gespeichert werden soll, kann der gemeinsam genutzte hana-Datenträger partitioniert werden, um ein weiteres Dateisystem für /usr/sap/SMA bereitzustellen.

Userstore-Schlüssel für SnapCenter

Es muss ein Benutzerspeicher für einen Systemdatenbankbenutzer erstellt werden, der von SnapCenter verwendet werden soll. Die HANA-Instanznummer muss für den Kommunikations-Port entsprechend festgelegt werden. In unserem Setup wird die Instanznummer „00“ verwendet.

Eine detailliertere Beschreibung finden Sie unter "Ressourcenspezifische SnapCenter Konfiguration für SAP HANA Datenbank-Backups"

```
smaadm@hana-1:/usr/sap/SMA/HDB00> hdbuserstore set SMAKEY hana-1:30013
SNAPCENTER <password>
Operation succeed.
```

Die Konnektivität kann mit dem folgenden Befehl überprüft werden.

```
smaadm@hana-1:/usr/sap/SMA/HDB00> hdbsql -U SMAKEY
Welcome to the SAP HANA Database interactive terminal.
Type: \h for help with commands
\q to quit
hdbsql SYSTEMDB=> exit
smaadm@hana-1:/usr/sap/SMA/HDB00
```

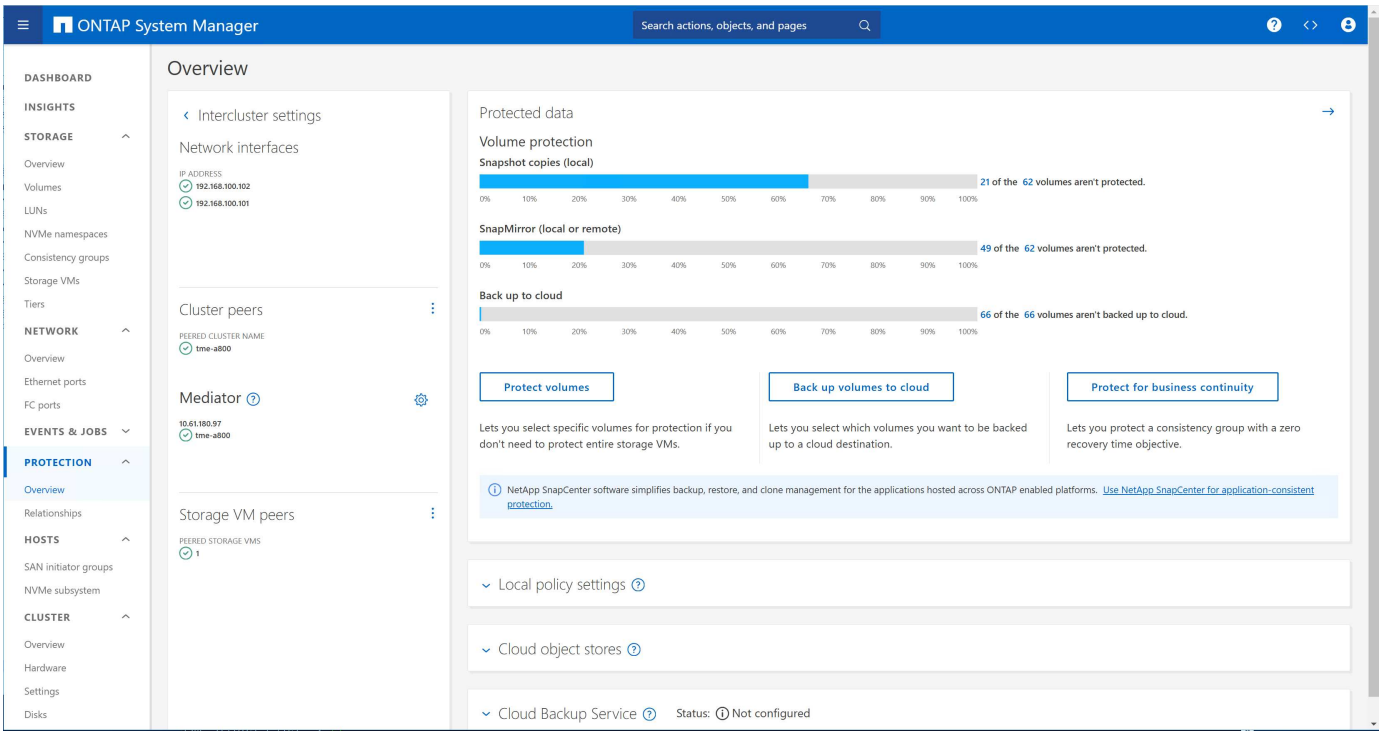
Konfiguration der aktiven SnapMirror-Synchronisierung

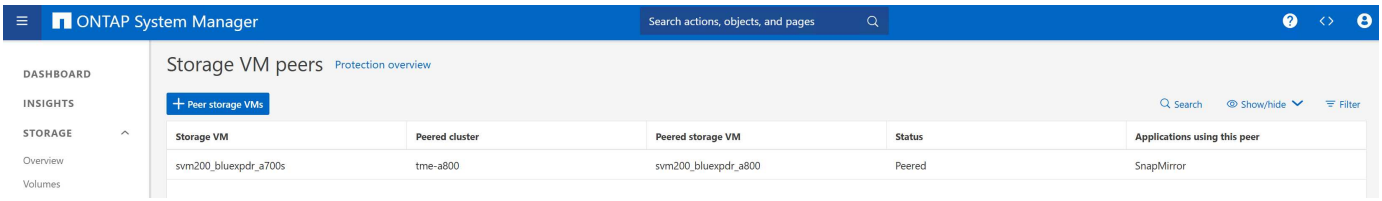
In diesem Artikel werden die für diese Lösung erforderlichen Konfigurationsschritte beschrieben.

Voraussetzungen

Storage-Cluster und relevante SVMs müssen aktiviert werden.

Der ONTAP Mediator muss auf beiden Storage-Clustern verfügbar und konfiguriert sein.





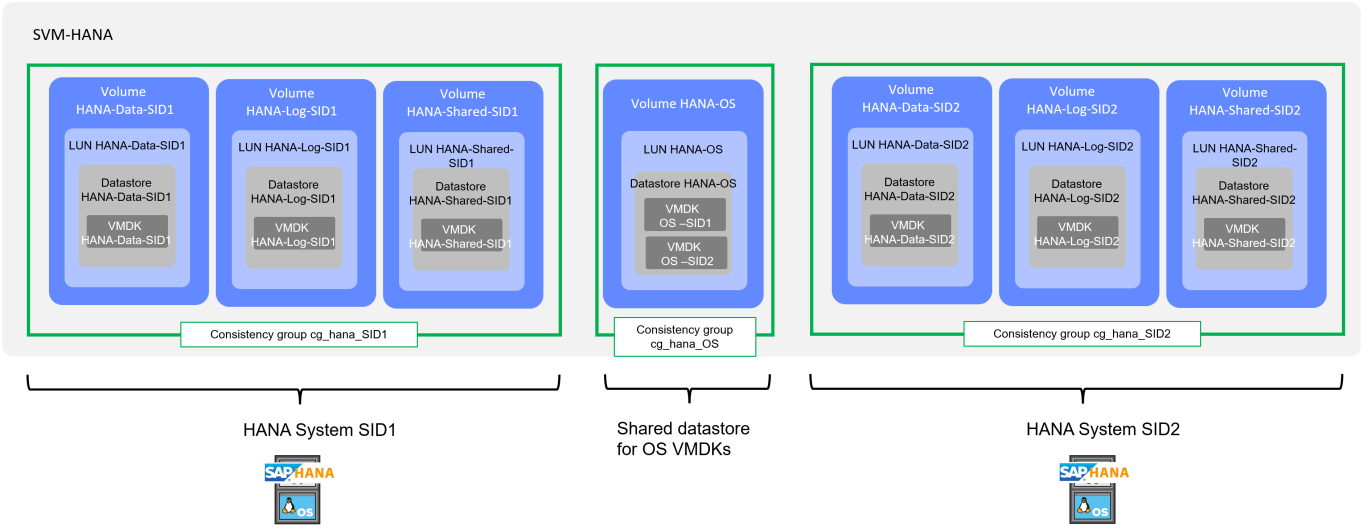
Konfiguration von Storage-Layout und Konsistenzgruppen

In der ONTAP-Dokumentation "Übersicht über die aktive SnapMirror-Synchronisierung in ONTAP" wird das Konzept der Konsistenzgruppen mit SnapMirror Active Sync wie folgt beschrieben:

Eine Konsistenzgruppe ist eine Sammlung von FlexVol Volumes, die eine Konsistenzgarantie für den Applikations-Workload bietet, der für Business Continuity geschützt werden muss.

Der Zweck einer Konsistenzgruppe besteht darin, gleichzeitige Snapshot Images mehrerer Volumes zu erstellen. Auf diese Weise wird sichergestellt, dass absturzkonsistente Kopien einer Sammlung von Volumes zu einem Zeitpunkt erstellt werden. Eine Konsistenzgruppe stellt sicher, dass alle Volumes eines Datensatzes stillgelegt und dann zu genau dem gleichen Zeitpunkt eingerastet werden. So erhalten Sie einen datenkonsistenten Restore-Zeitpunkt über Volumes hinweg, der den Datensatz unterstützt. Eine Konsistenzgruppe behält dabei die abhängige Konsistenz der Schreibreihenfolge bei. Wenn Sie Applikationen für Business Continuity schützen möchten, muss die Volume-Gruppe, die dieser Applikation entspricht, einer Konsistenzgruppe hinzugefügt werden, damit eine Datensicherungsbeziehung zwischen einer Quell- und einer Zielkonsistenzgruppe hergestellt wird. Die Quell- und Zielkonsistenz muss die gleiche Anzahl und den gleichen Typ von Volumes enthalten.

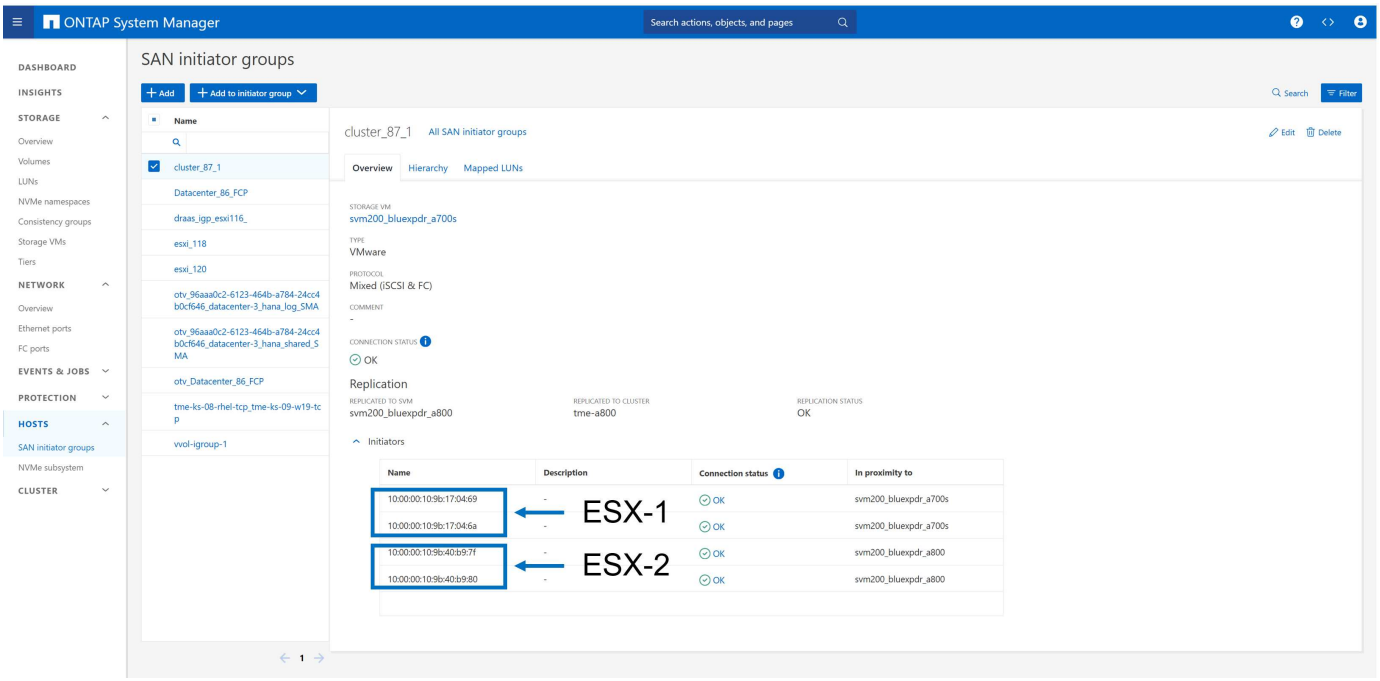
Für die Replizierung von HANA-Systemen muss die Konsistenzgruppe alle Volumes enthalten, die vom einzelnen HANA-System verwendet werden (Daten, Protokoll und Shared). Volumes, die Teil einer Konsistenzgruppe sein sollten, müssen auf derselben SVM gespeichert werden. Betriebssystem-Images können auf einem separaten Volume mit einer eigenen Konsistenzgruppe gespeichert werden. Die Abbildung unten zeigt ein Konfigurationsbeispiel mit zwei HANA-Systemen.

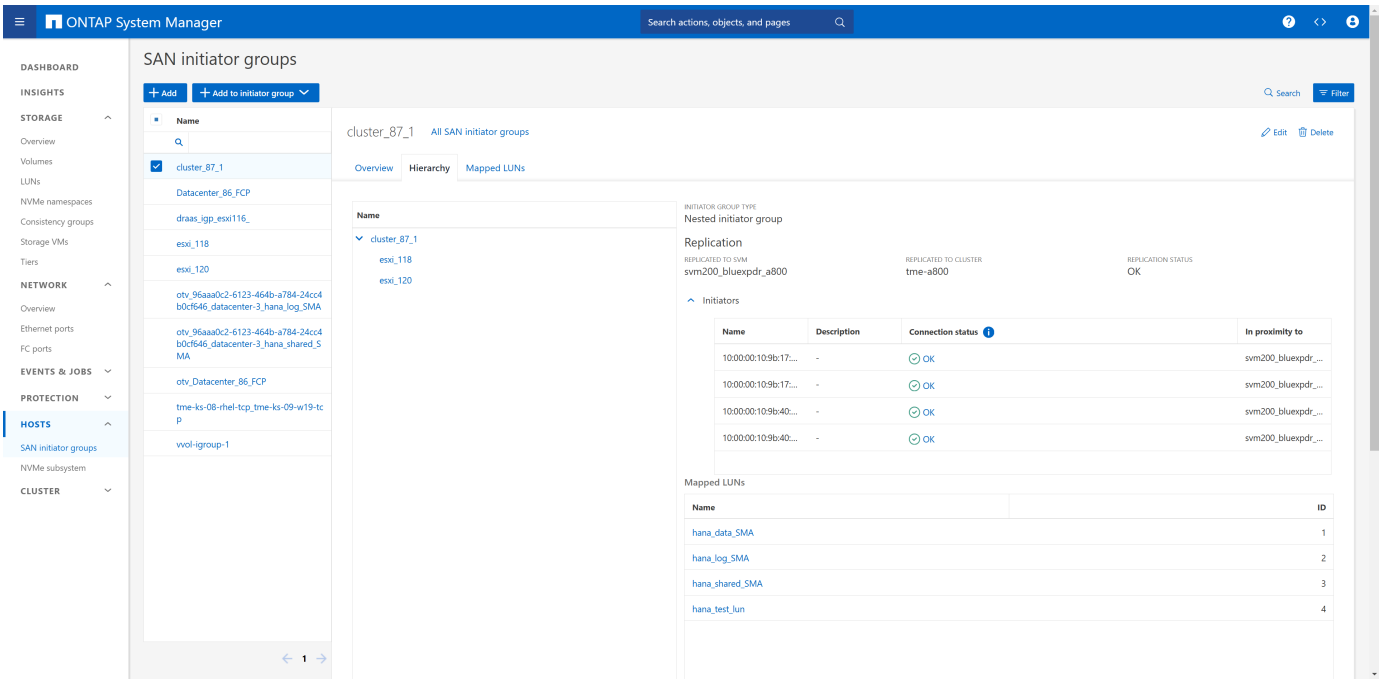


Konfiguration der Initiatorgruppe

In unserem Lab-Setup haben wir eine Initiatorgruppe erstellt, die beide Storage-SVMs für die aktive synchrone Replizierung mit SnapMirror verwendet. In der später beschriebenen Konfiguration für aktive SnapMirror-Synchronisierung wird festgelegt, dass die Initiatorgruppe Teil der Replizierung ist.

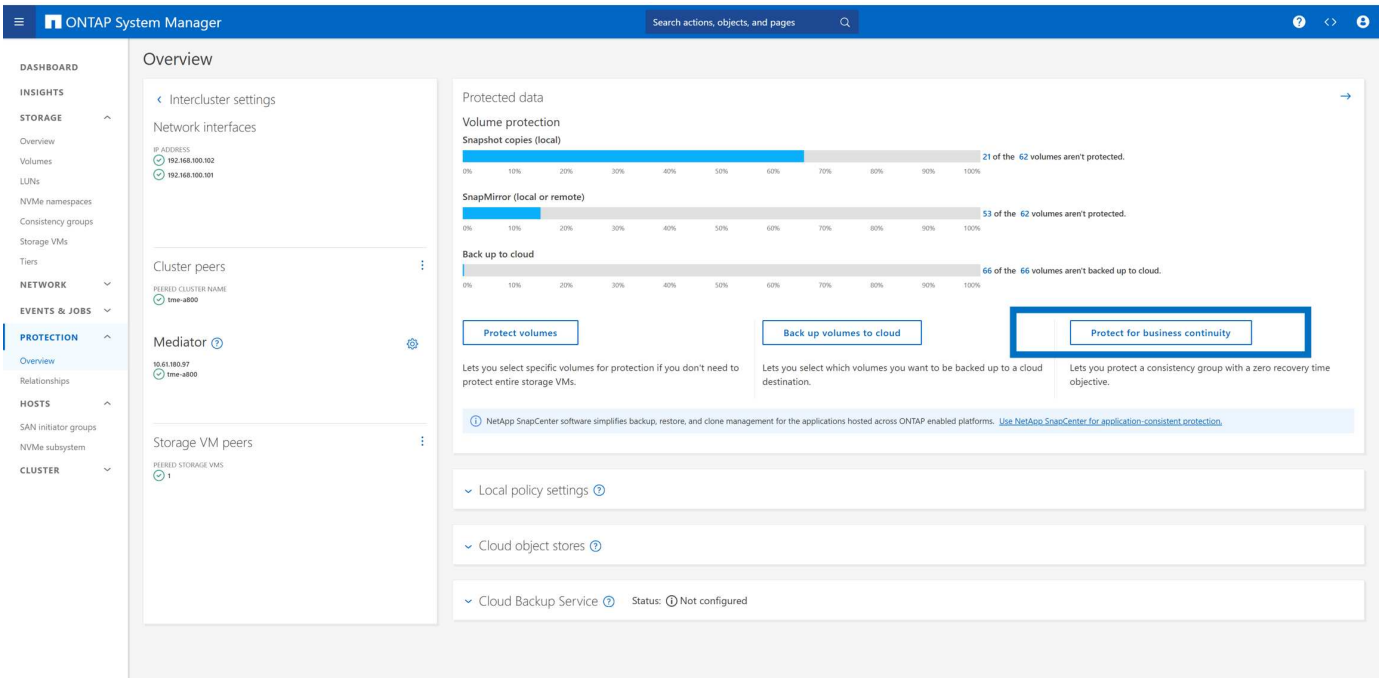
Mithilfe der Annäherungseinstellungen wurde festgelegt, welcher ESX Host sich in der Nähe des Storage-Clusters befindet. In unserem Fall liegt die A700 in der Nähe von ESX-1 und die A800 ist nah an ESX-2.





In einem nicht einheitlichen Access Setup darf die Initiatorgruppe im primären Storage-Cluster (A700) nur die Initiatoren des ESX-1-Hosts einschließen, da es keine SAN-Verbindung zu ESX-2 gibt. Darüber hinaus müssen Sie eine andere Initiatorgruppe auf dem zweiten Storage-Cluster (A800) konfigurieren, der nur die Initiatoren des ESX-2 Hosts enthalten. Die Proximity-Konfiguration und die Replizierung von Initiatorgruppen sind nicht erforderlich.

Konfigurieren Sie den Schutz mit ONTAP System Manager

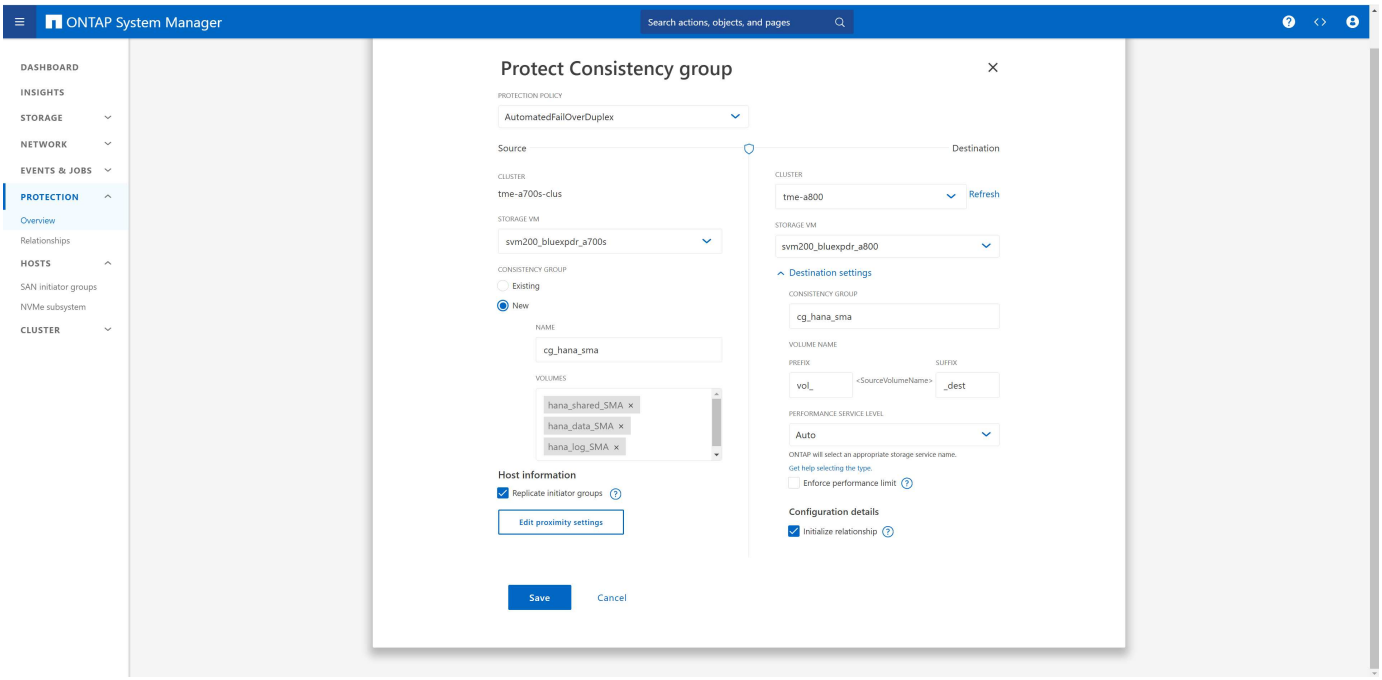


Replizierung von Konsistenzgruppen und Initiatorgruppen

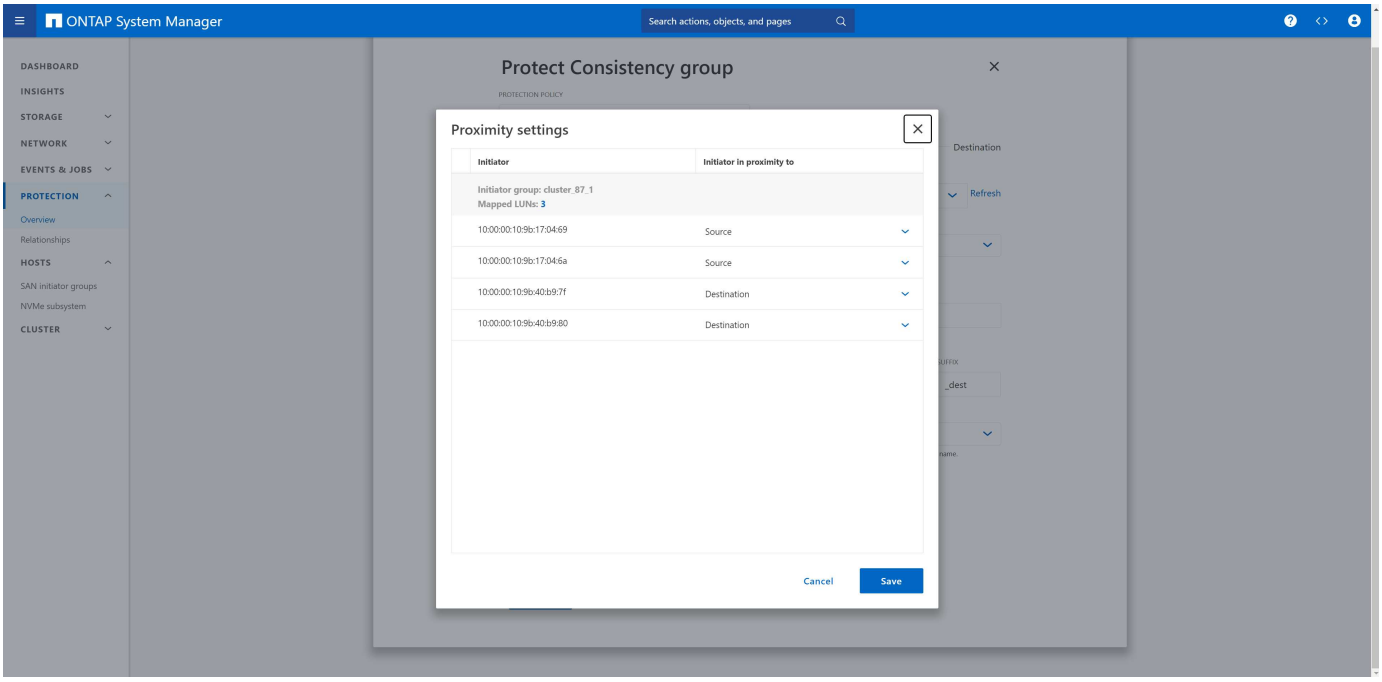
Eine neue Konsistenzgruppe muss erstellt werden, und alle drei LUNs des HANA-Systems müssen der Konsistenzgruppe hinzugefügt werden.

„Initiatorgruppe replizieren“ wurde aktiviert. Die Imitatorgruppe bleibt dann unabhängig, wo Änderungen vorgenommen werden.

In einer nicht einheitlichen Zugriffseinrichtung darf die Initiatorgruppe nicht repliziert werden, da auf dem zweiten Storage-Cluster eine separate Initiatorgruppe konfiguriert werden muss.



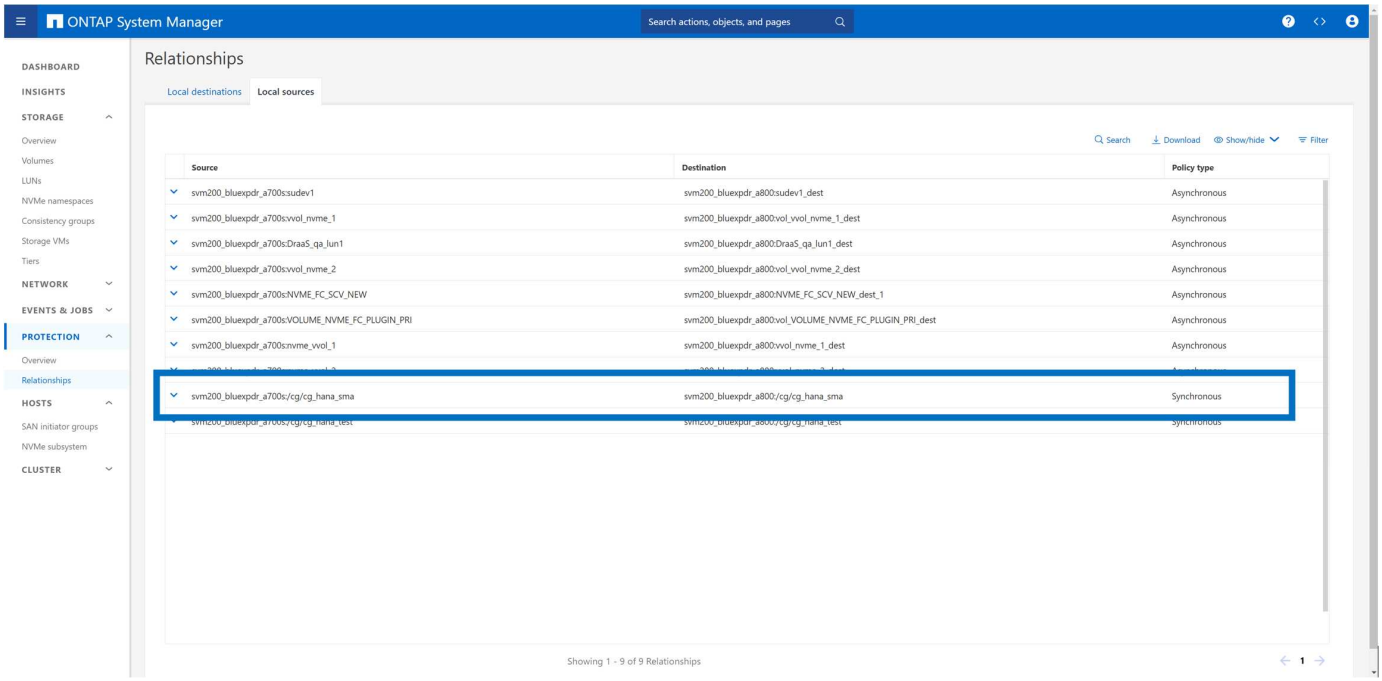
Indem Sie auf „Annäherungseinstellungen“ klicken, können Sie die zuvor im Setup der Initiatorgruppe vorgenommenen Konfigurationen überprüfen.



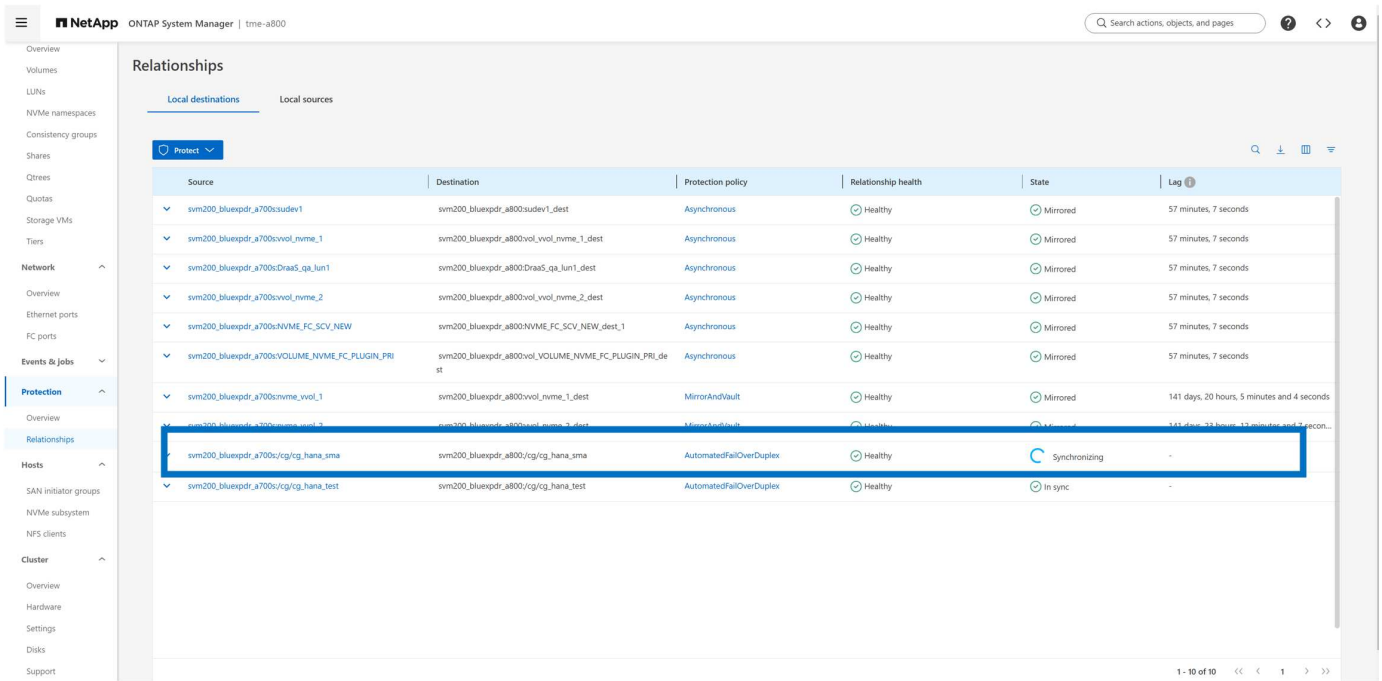
Der Ziel-Storage-Cluster muss konfiguriert und die „Initialisierungsbeziehung“ aktiviert sein.

Synchronisierung

Bei dem A700 Storage-Cluster (Quelle) ist die neue Beziehung jetzt aufgelistet.



Am A800 Storage-Cluster (Ziel) werden die neue Beziehung und der Status der Replizierung aufgeführt.



Infrastrukturdatenspeicher

Der Datastore, in dem die OS-Images des HANA-Systems, SnapCenter und das vSphere Plug-in gespeichert werden, wird in der gleichen Weise repliziert wie bei den HANA-Datenbankdatenspeichern beschrieben.

Primärer Standort

Das aktive Synchronisierungsverhalten von SnapMirror ist symmetrisch, mit einer wichtigen Ausnahme: Konfiguration des primären Standorts.

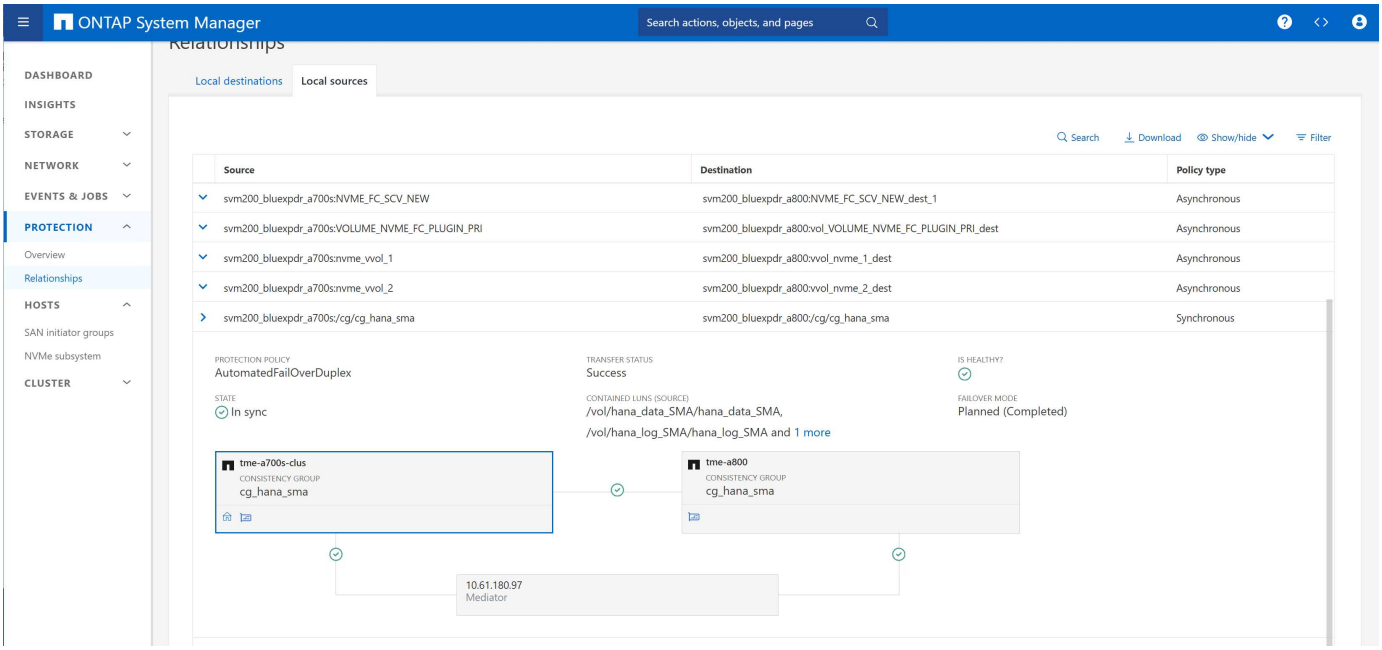
SnapMirror Active Sync betrachtet einen Standort als „Quelle“ und den anderen als „Ziel“. Dies impliziert eine One-Way-Replikationsbeziehung, aber dies gilt nicht für das IO-Verhalten. Die Replizierung ist bidirektional und symmetrisch, und die I/O-Reaktionszeiten sind auf beiden Seiten der Spiegelung identisch.

Wenn die Replikationsverbindung verloren geht, stellen die LUN-Pfade auf der Quellkopie weiterhin Daten bereit, während die LUN-Pfade auf der Zielkopie erst dann nicht mehr verfügbar sind, wenn die Replikation wiederhergestellt ist und SnapMirror wieder in den synchronen Zustand wechselt. Die Pfade setzen dann das Bereitstellen von Daten fort.

Der Effekt der Festlegung eines Clusters als Quelle steuert einfach, welches Cluster als Lese-/Schreib-Speichersystem überlebt, wenn die Replikationsverbindung verloren geht.

Der primäre Standort wird von SnapCenter erkannt und zur Durchführung von Backup-, Wiederherstellungs- und Klonvorgängen verwendet.

Beachten Sie, dass Quelle und Ziel nicht an SVM oder Storage-Cluster gebunden sind, sondern für jede Replizierungsbeziehung unterschiedlich sein können.



SnapCenter-Konfiguration

Wie bereits zu Beginn des Dokuments erwähnt, dient das Dokument dazu, Best Practices für eine HANA-Umgebung mit VMware mit VMFS und SnapMirror Active Sync bereitzustellen. Wir behandeln nur Details und wichtige Schritte, die für diese spezifische Lösung relevant sind, und erläutern die allgemeinen SnapCenter-Konzepte nicht. Diese Konzepte und weitere Informationen zu SnapCenter finden Sie unter:

"Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter"

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

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

Voraussetzungen

Im Allgemeinen sollte SnapMirror Active Sync eingerichtet werden, bevor die geschützten Ressourcen zu SnapCenter hinzugefügt werden. Wenn Backups vor der Einrichtung von SnapMirror Active Sync erstellt wurden, sind sie nur im ursprünglichen primären Speicher vorhanden und werden danach nicht repliziert.

Die SnapCenter HANA-Ressource muss automatisch erkannt werden

Ressourcen, die mit VMware VMFS oder mit SnapMirror Active Sync geschützten Ressourcen konfiguriert sind, müssen automatisch von SnapCenter erkannt werden, damit bestimmte Vorgänge für diese Konfigurationen möglich sind.

Da HANA-nicht-Daten-Volumes immer manuell konfigurierte Ressourcen in SnapCenter sind, werden sie nicht von SnapCenter out of the box unterstützt. Im weiteren Verlauf dieses Dokuments besprechen wir Optionen und Problemumgehungen für nicht-Datenvolumes.

SAP HANA mehrere Hostsysteme müssen über ein zentrales HANA-Plugin konfiguriert werden und sind daher standardmäßig manuell konfigurierte Ressourcen. Solche HANA-Systeme werden von SnapCenter nicht unterstützt, wenn VMware VMFS oder SnapMirror Active Sync verwendet wird.

SnapCenter für VMware vSphere-Plugin

Das SnapCenter für VMware vSphere Plug-in muss in der VMware Umgebung implementiert werden.

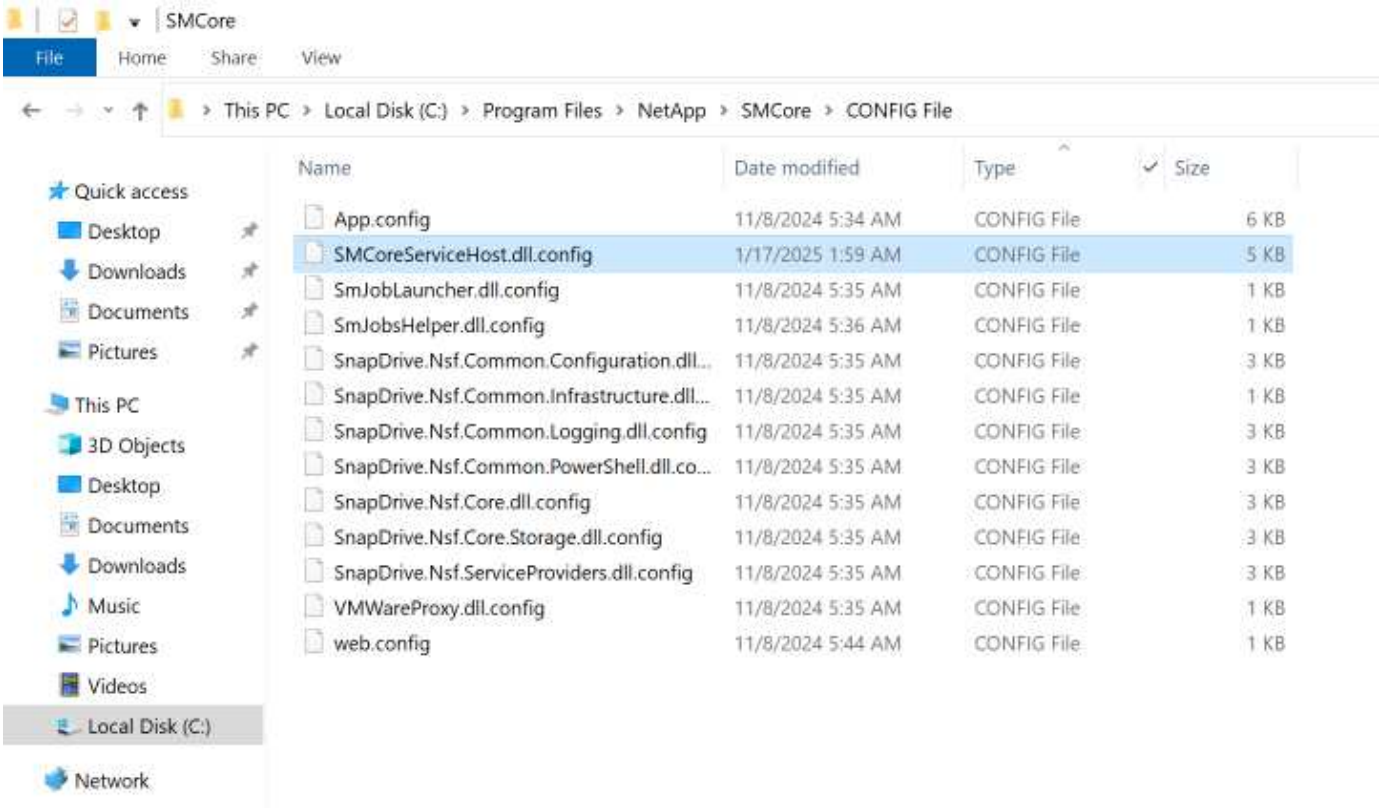
Management-IP-Adresse auf der SVM, die die Volumes hostet

Obwohl SnapCenter Cluster hinzugefügt werden, muss für die SVMs, die die Quell- und Ziel-Volumes hosten, eine Management-IP-Adresse konfiguriert sein.

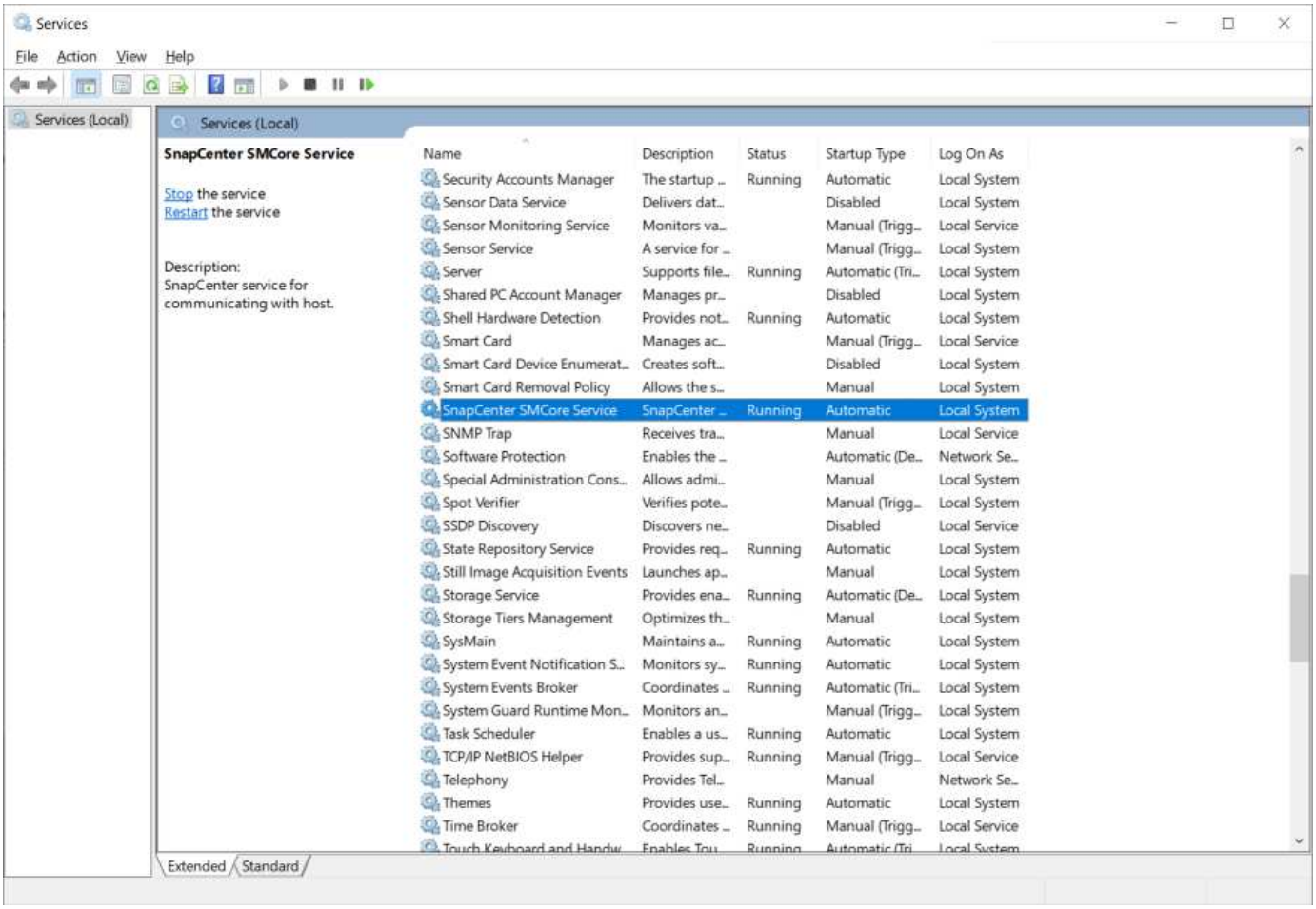
REST-APIs zur Storage-Kommunikation

Für das Management und die Überwachung der aktiven SnapMirror-Synchronisierung ist REST-API-Zugriff erforderlich. Daher muss SnapCenter so konfiguriert werden, dass es REST-APIs für Storage-Kommunikation verwendet. Der Parameter "IsRestEnabledForStorageConnection" in der Konfigurationsdatei + C:\Programme\NetApp++SMCore+\++SMCoreServiceHost.dll.config muss auf true gesetzt werden.

```
<add key="IsRestEnabledForStorageConnection" value="true">
```

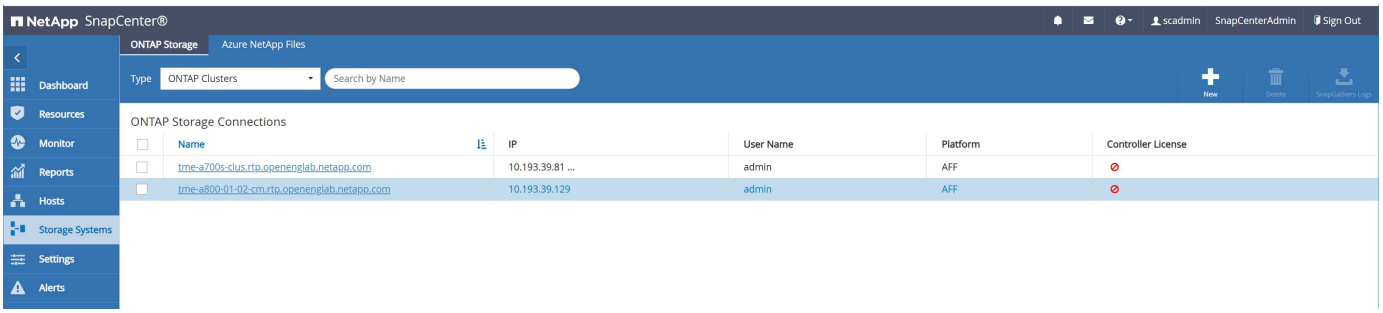


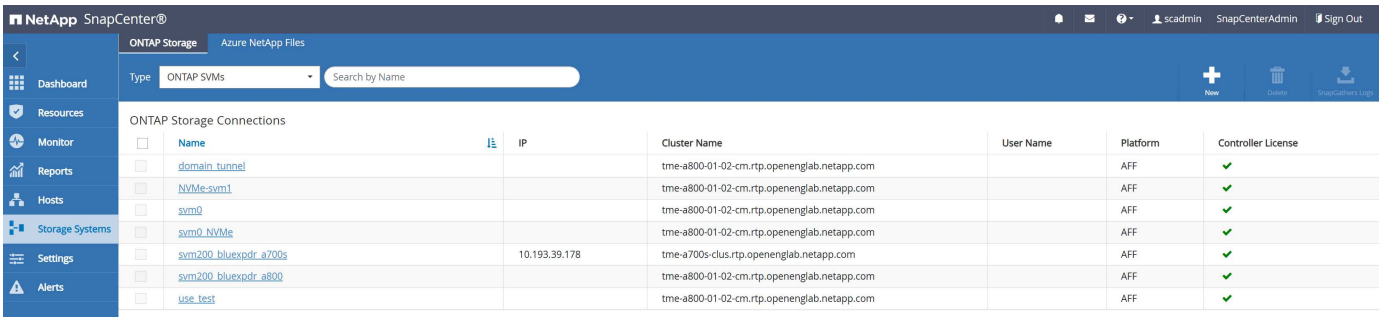
Nach der Parameteränderung muss der SnapCenter-SMCore-Dienst neu gestartet werden.



Storage-Systeme hinzufügen

Storage-Systeme können hinzugefügt werden, nachdem die REST-API für SnapCenter aktiviert ist. Es müssen nicht die einzelnen SVMs, sondern beide Storage-Cluster hinzugefügt werden.



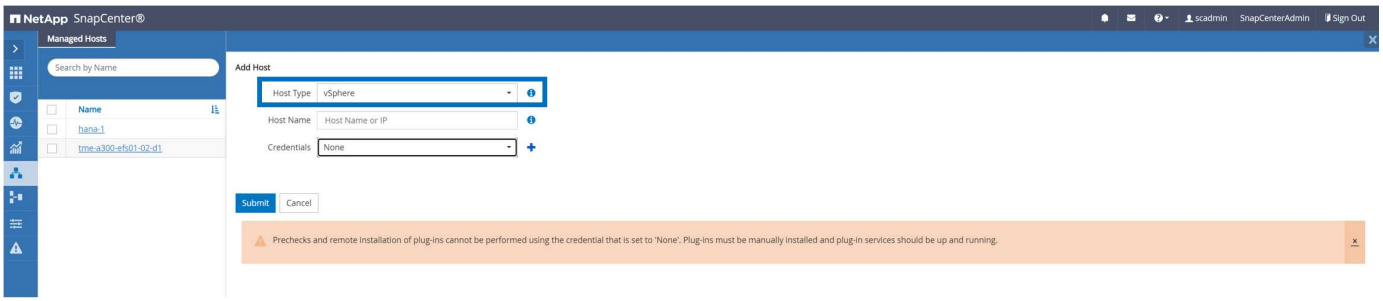


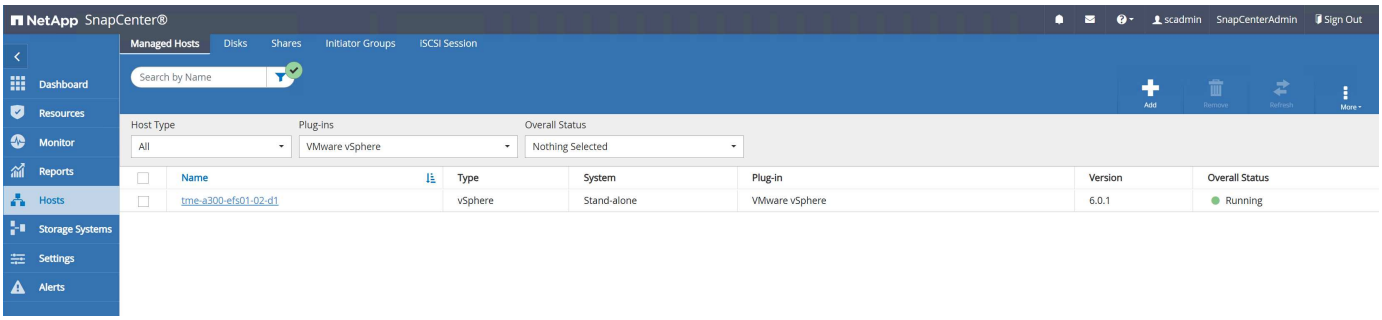
Host hinzufügen – SnapCenter für VMware vSphere Plug-in

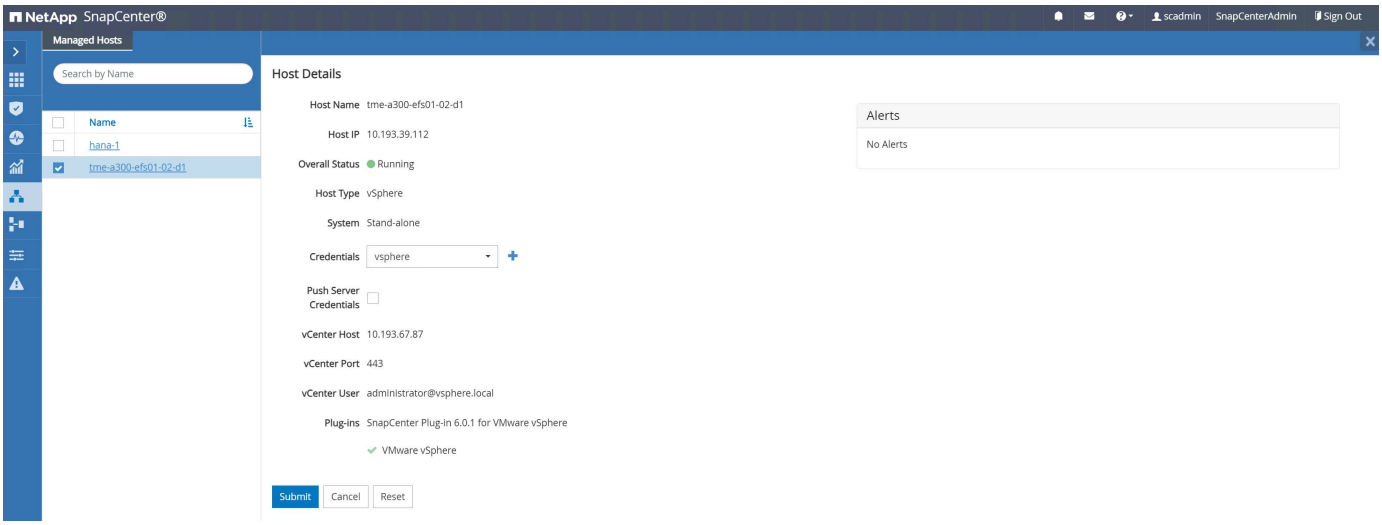
Wenn eine Ressource in SnapCenter in einer virtualisierten VMware Umgebung ausgeführt wird, nutzt SnapCenter das SnapCenter Plug-in für VMware vSphere, um die Backup-, Restore- und Klon-Workflows von SnapCenter mit den erforderlichen Schritten auf der VMware Ebene zu erweitern.

Bevor der Host in SnapCenter hinzugefügt werden kann, muss das SnapCenter Plug-in für VMware vSphere in der VMware Umgebung implementiert werden.

Die Anmeldeinformationen müssen während des Host-Add-Workflows festgelegt werden, wobei vSphere als Hosttyp ausgewählt werden kann.







Beim SnapCenter für vSphere Plugin selbst ist keine zusätzliche Konfiguration erforderlich.

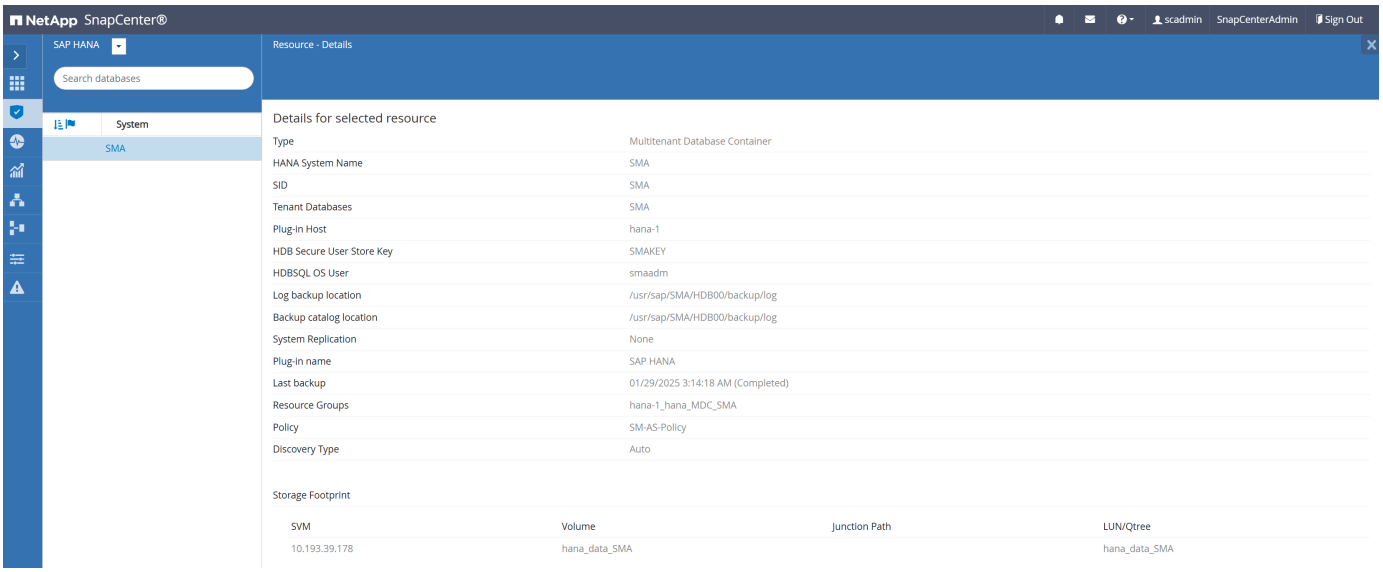
Host – HANA-System hinzufügen

Keine besonderen Anforderungen. Plugin-Bereitstellung und automatische Erkennung erfolgt wie gewohnt.

Durch den automatischen Erkennungsprozess erkennt SnapCenter, dass die HANA-Ressource virtualisiert mit VMFS/VMDKs ausgeführt wird. SnapCenter erkennt außerdem die SnapMirror Active Sync Einrichtung und identifiziert den aktuellen primären Standort.

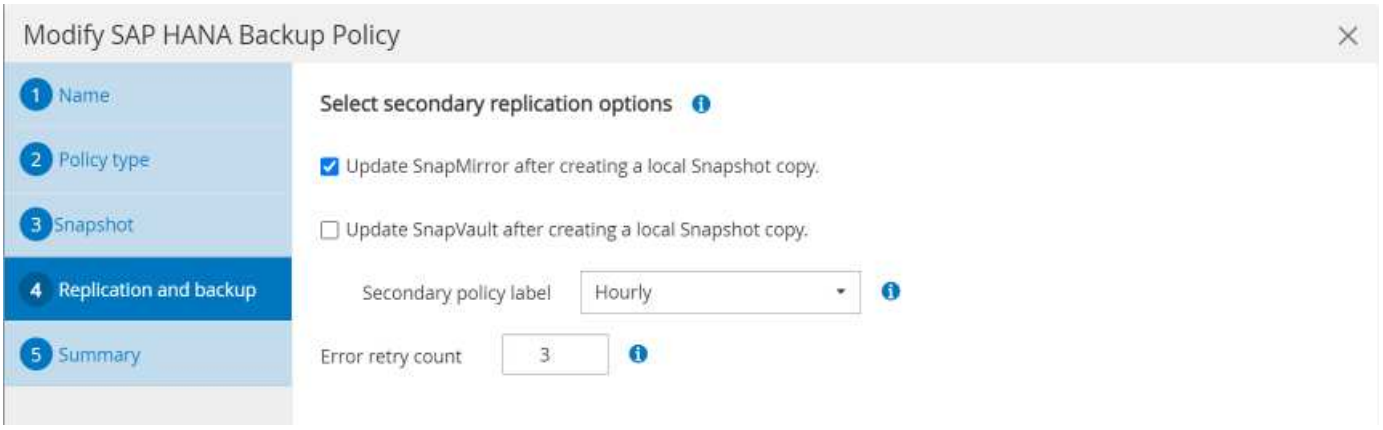
Nach der automatischen Ressourcenerkennung wird der aktuelle primäre Standort im Abschnitt Storage Footprint der Ressourcenansicht angezeigt. Die Erkennung, welches Storage-System Master ist, basiert auf der Ausgabe des Befehls ONTAP, der von SnapCenter verwendet wird.

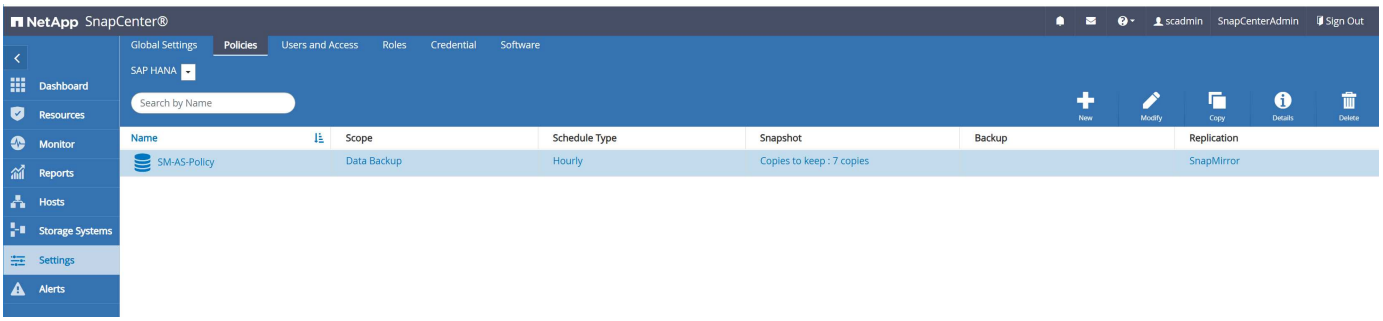
```
volume show -vserver <vs> -volume <vol> -fields smbc-consensus,is-smbc-
master
```



Konfiguration von Richtlinien

Die Richtlinie, die für die mit SnapMirror Active Sync geschützte Ressource verwendet wird, muss mithilfe der SnapMirror-Replizierung konfiguriert werden, auch wenn SnapCenter keine SnapMirror Update-Vorgänge auslöst.





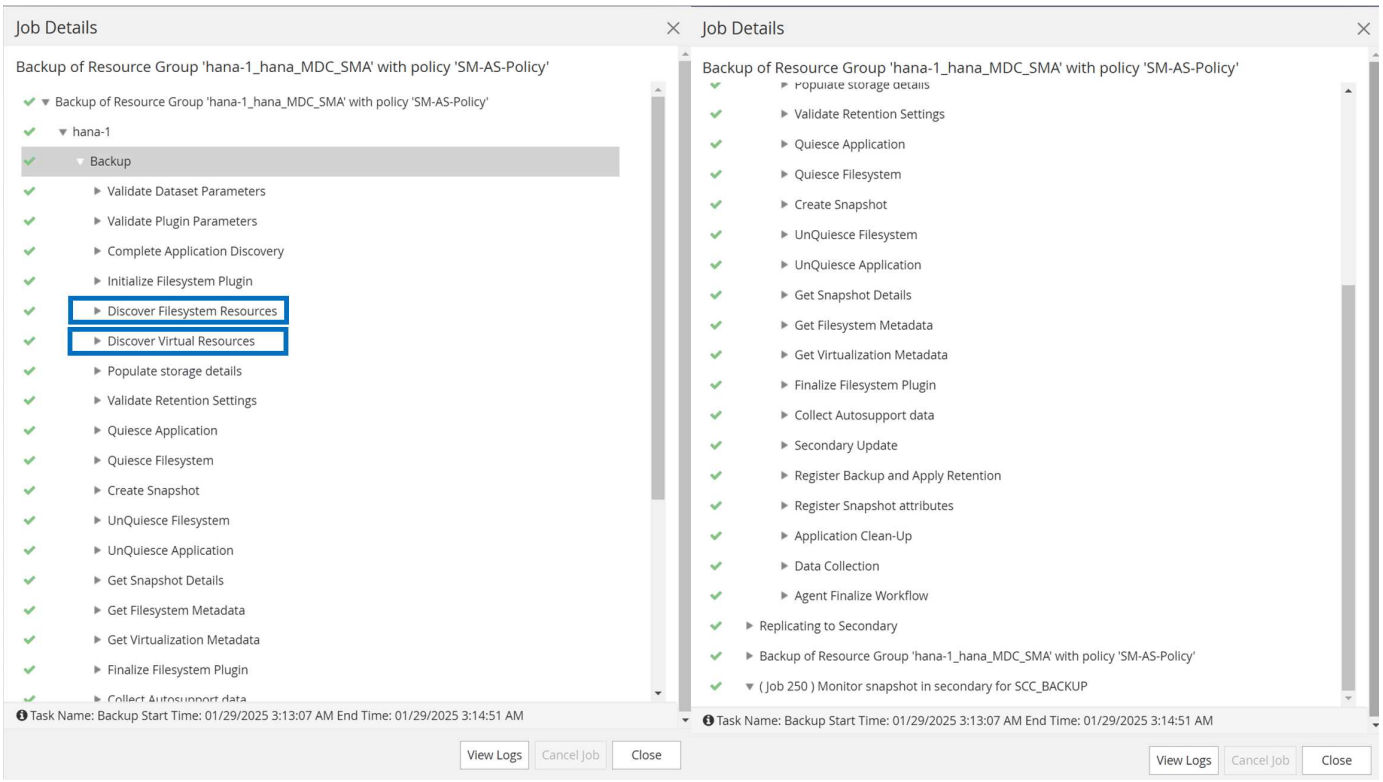
Konfiguration der HANA-Ressourcensicherung

Keine besonderen Anforderungen. Die Konfiguration des Ressourcenschutzes erfolgt wie gewohnt.

SnapCenter-Backup-Vorgänge

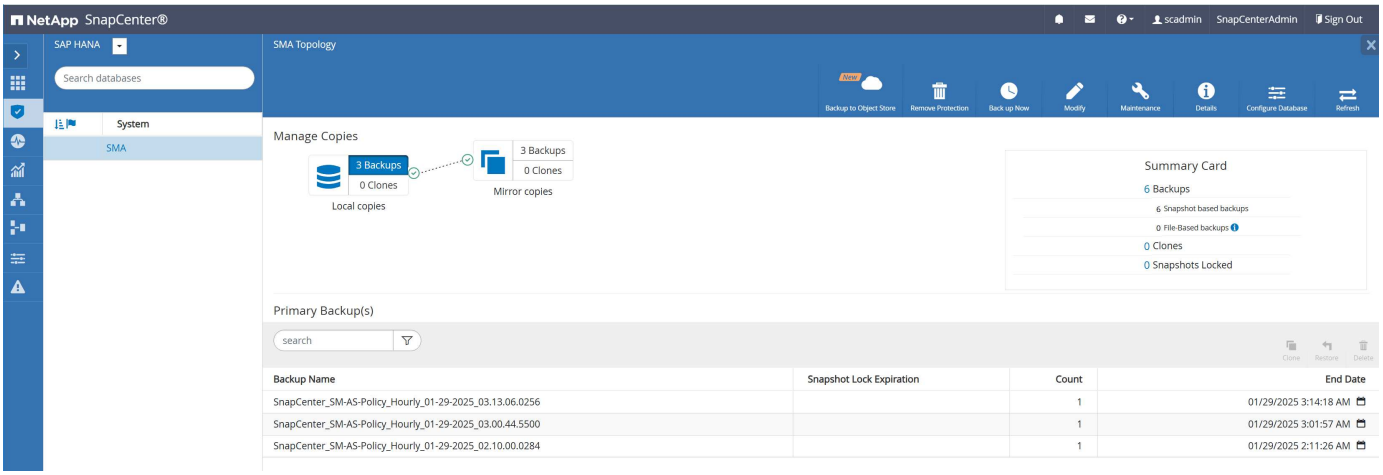
Bei jedem Backup-Vorgang führt SnapCenter die Erkennung auf VMware-Seite aus und

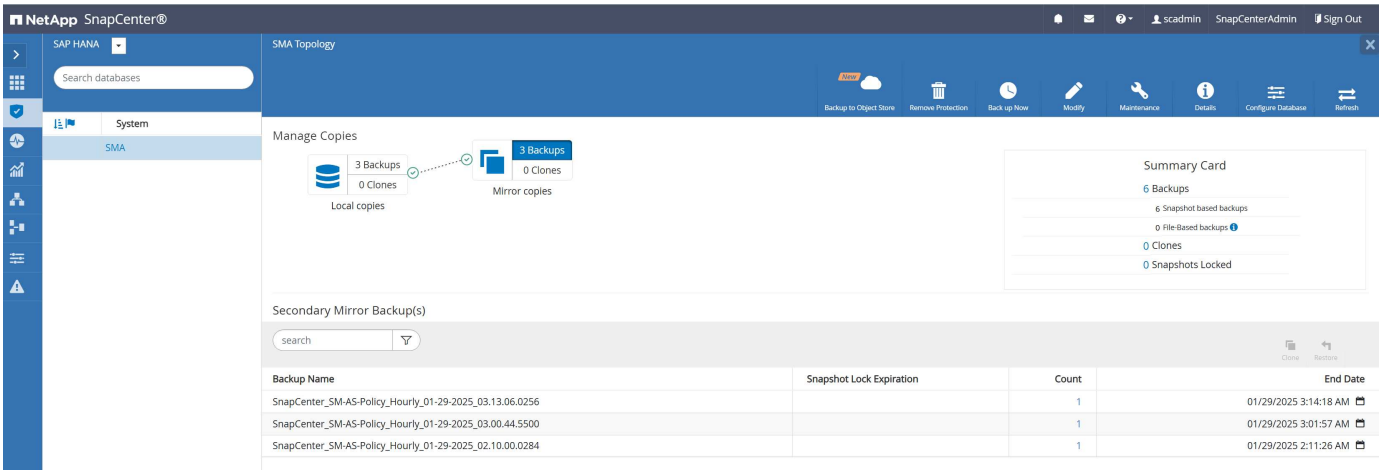
erkennt den primären Standort. Bei einem Storage-Failover erkennt SnapCenter den neuen primären Standort, sobald ein Backup für die Ressource ausgeführt wurde.



Topologieansicht

In der Topologieansicht zeigt SnapCenter die Backups sowohl des Quell- als auch des Ziel-Storage-Clusters.



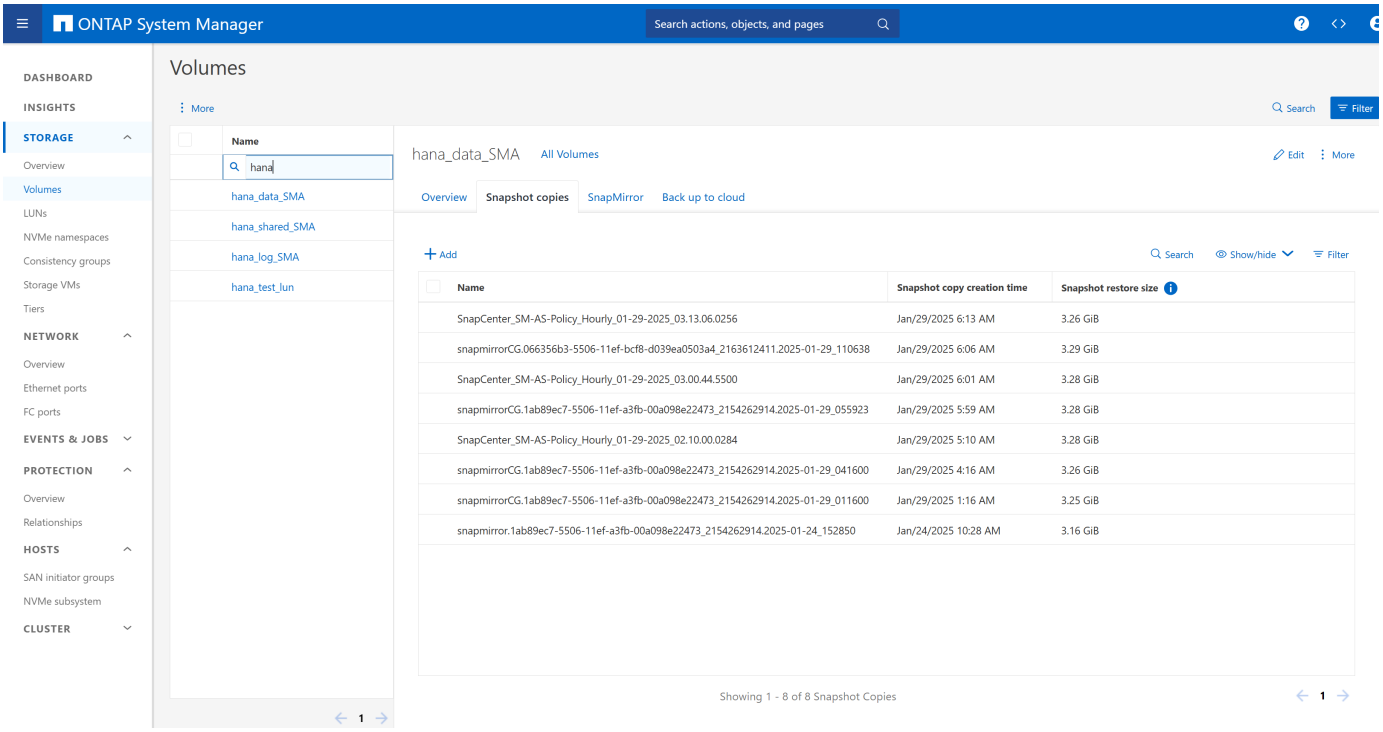


Durch Klicken auf die Zählzahl im sekundären Speicher wird die aktuelle Beziehung und Replikationsrichtung angezeigt. Die Quelle ist immer der aktuelle primäre Standort. Nach einem Speicher-Failover ändert sich der primäre Standort und die Anzeige wird entsprechend angepasst. Alle Backups verfügen immer über die gleiche Beziehung, je nach Speichersystem derzeit der primäre Standort ist.

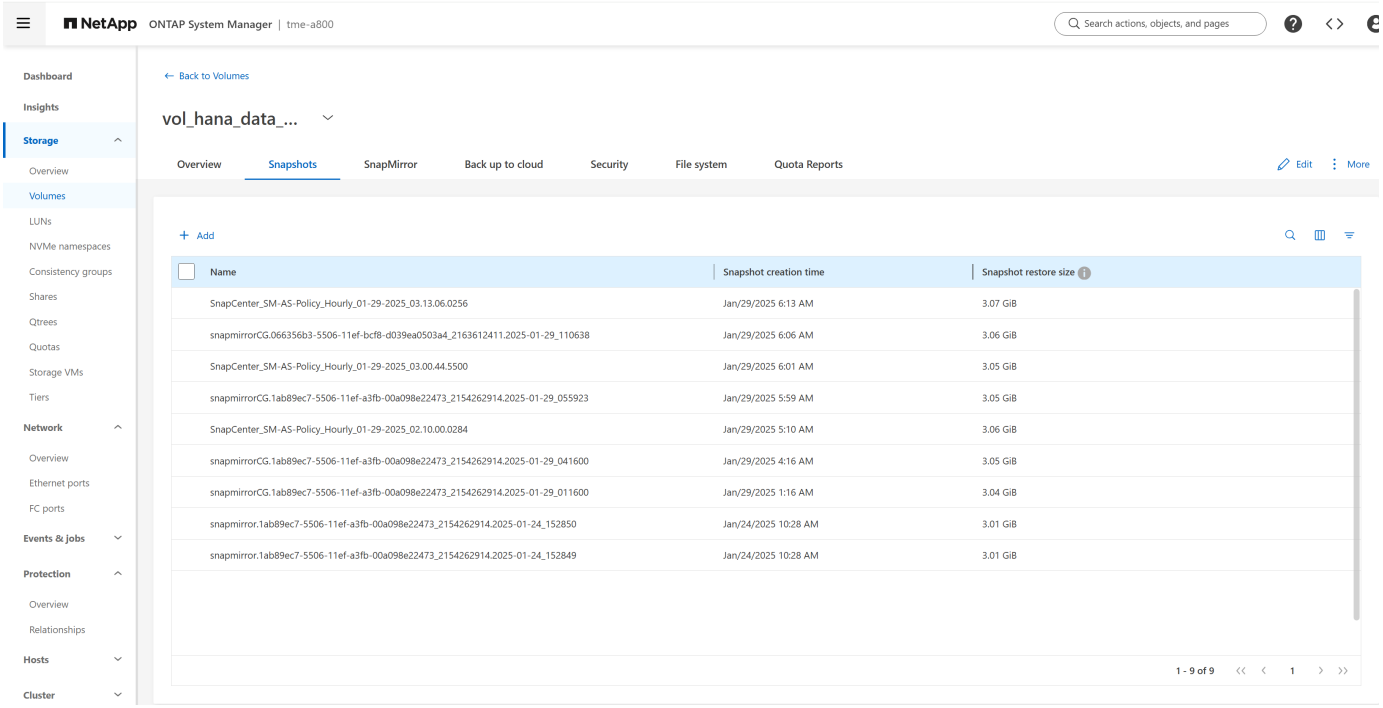
Snapshots auf Storage-Systemen

Die von SnapCenter erstellten Snapshot Backups sind bei beiden HANA Daten-Volumes auf beiden Storage-Systemen verfügbar. ONTAP erstellt zusätzliche Snapshots auf Konsistenzgruppenebene, die auch für alle anderen HANA-Volumes verfügbar sind.

Die Abbildung unten zeigt die Snapshots des HANA-Daten-Volumes beim A700-Cluster.



Die Abbildung unten zeigt die Snapshots des HANA-Daten-Volumes auf dem A800 Cluster.



SnapCenter Restore und Recovery

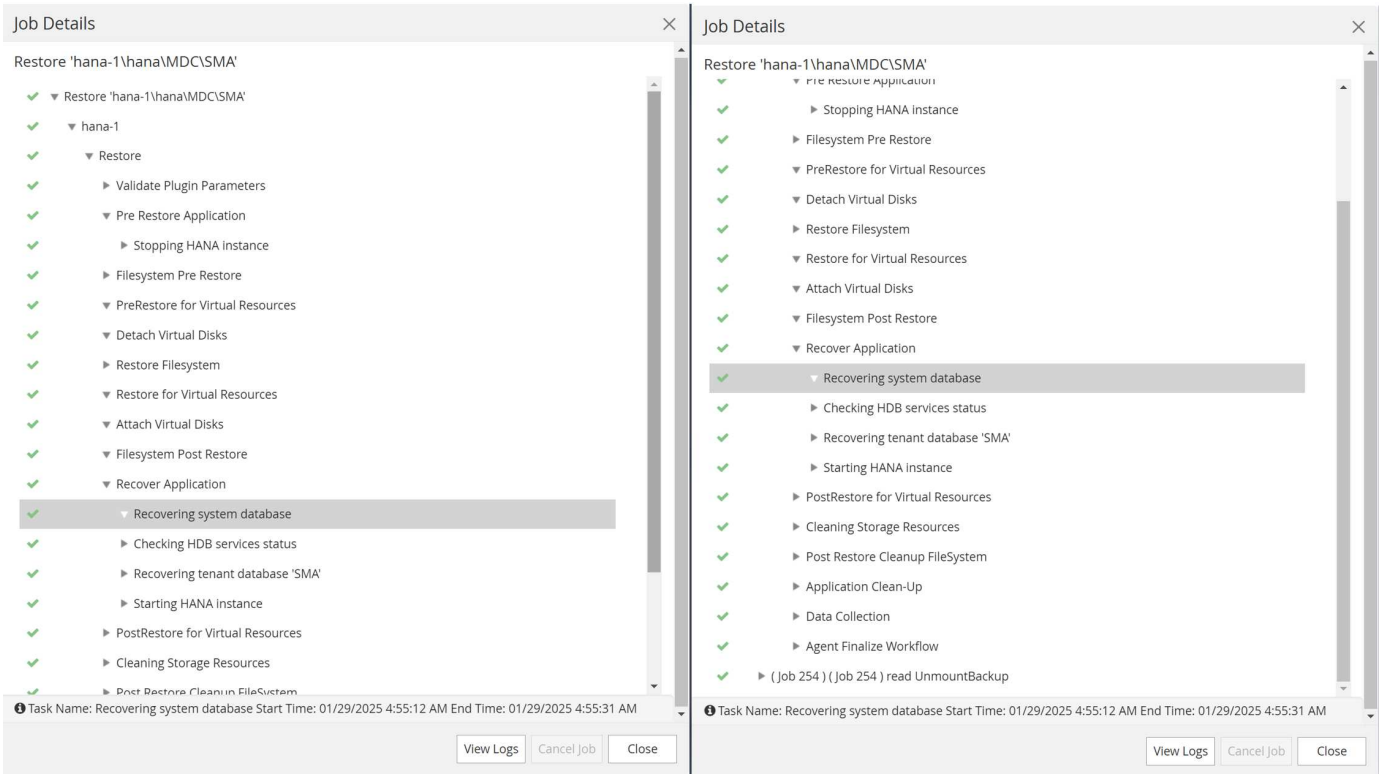
Wenn virtuelle Ressourcen auf VMFS/VMDK gespeichert sind, erfolgt eine SnapCenter-Wiederherstellung immer durch einen Klon-, Mount- und Kopiervorgang.

1. SnapCenter erstellt auf Basis des ausgewählten Snapshots einen Volume-Klon
2. SnapCenter bindet die LUN im geklonten Volume als neuen Datastore in den ESX Host ein

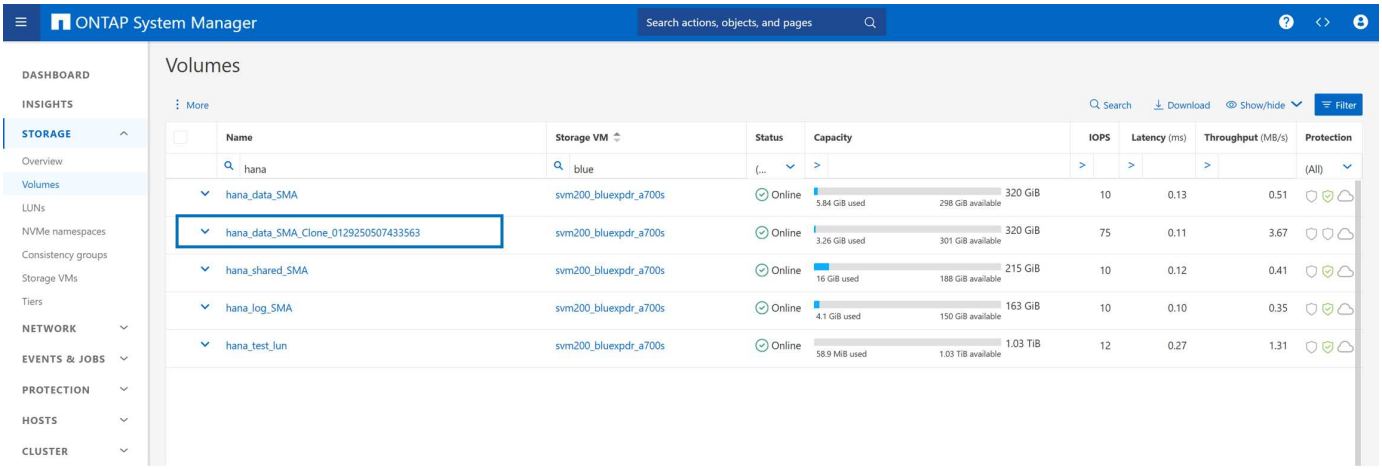
3. SnapCenter fügt die VMDK innerhalb des Datenspeichers der HANA-VM als neue Festplatte hinzu
4. SnapCenter bindet die neue Festplatte an das Linux Betriebssystem an
5. SnapCenter kopiert die Daten von der neuen Festplatte zurück in den ursprünglichen Speicherort
6. Wenn der Kopiervorgang abgeschlossen ist, werden alle oben genannten Ressourcen wieder entfernt
7. Die HANA-Wiederherstellung erfolgt wie gewohnt

Die Gesamtlaufzeit des Wiederherstellungsvorgangs ist daher abhängig von der Datenbankgröße und dem Durchsatz der FC-Verbindung zwischen den Storage-Clustern und den ESX-Hosts.

Wenn eine Ressource mit SnapMirror Active Sync konfiguriert ist, kann die SnapCenter-Wiederherstellung auch nur am aktuellen primären Standort ausgewählt werden.



Während der Restore- und Recovery-Vorgang ausgeführt wird, sehen Sie ein neues geklontes Volume, das am aktuellen Primärstandort erstellt wurde.



Auf dem HANA Linux Host sehen Sie eine neue Festplatte, die auf den Host gemountet wurde. Wenn die Wiederherstellung abgeschlossen ist, werden die Festplatte, Datenspeicher und Volumes von SnapCenter wieder entfernt.

```
hana-1:~ # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 4.0K 49G 1% /dev/shm
tmpfs 13G 58M 13G 1% /run
tmpfs 4.0M 0 4.0M 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 36G 24G 60% /
/dev/mapper/system-root 60G 36G 24G 60% /.snapshots
/dev/mapper/system-root 60G 36G 24G 60% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 36G 24G 60% /home
/dev/mapper/system-root 60G 36G 24G 60% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 36G 24G 60% /opt
/dev/mapper/system-root 60G 36G 24G 60% /srv
/dev/mapper/system-root 60G 36G 24G 60% /usr/local
/dev/mapper/system-root 60G 36G 24G 60% /tmp
/dev/mapper/system-root 60G 36G 24G 60% /root
/dev/mapper/system-root 60G 36G 24G 60% /var
/dev/sdb 200G 8.0G 192G 4% /hana/data/SMA/mnt00001
/dev/sdc 120G 7.0G 113G 6% /hana/log/SMA/mnt00001
/dev/sda1 253M 5.1M 247M 3% /boot/efi
/dev/sdd 150G 28G 123G 19% /hana/shared
tmpfs 6.3G 48K 6.3G 1% /run/user/467
tmpfs 6.3G 28K 6.3G 1% /run/user/0
/dev/sde 200G 8.0G 192G 4%
/var/opt/snapcenter/scu/clones/hana_data_SMAmnt00001_255_scu_clone_1
hana-1:~ #
```

Aktualisierung des SAP-Systems

Klonvorgänge können am primären Standort oder im sekundären Storage ausgeführt werden.

Das geklonte Volume ist nicht Teil der HANA-Konsistenzgruppe und wird nicht mit der aktiven SnapMirror-Synchronisierung repliziert.

Detaillierte Informationen zu den Workflows für die Systemaktualisierung sind verfügbar unter: "TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"

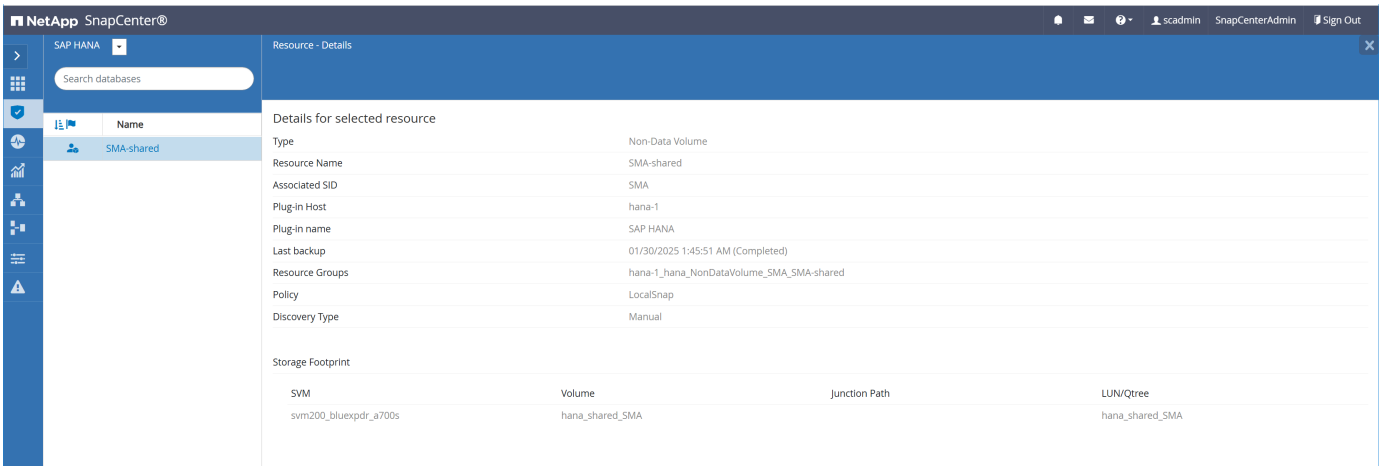
Nicht datenbasierte SnapCenter-Volumes

Wenn Ressourcen in SnapCenter manuell konfiguriert und nicht automatisch erkannt werden, erkennt SnapCenter die aktive Synchronisierung von VMware und SnapMirror nicht. Daher werden sie von SnapCenter nicht nativ unterstützt.

Bei nicht-Daten-Volumes wie HANA Shared könnten Backup- und Restore-Vorgänge unter Berücksichtigung zusätzlicher manueller Schritte weiterhin mit SnapCenter ausgeführt werden.

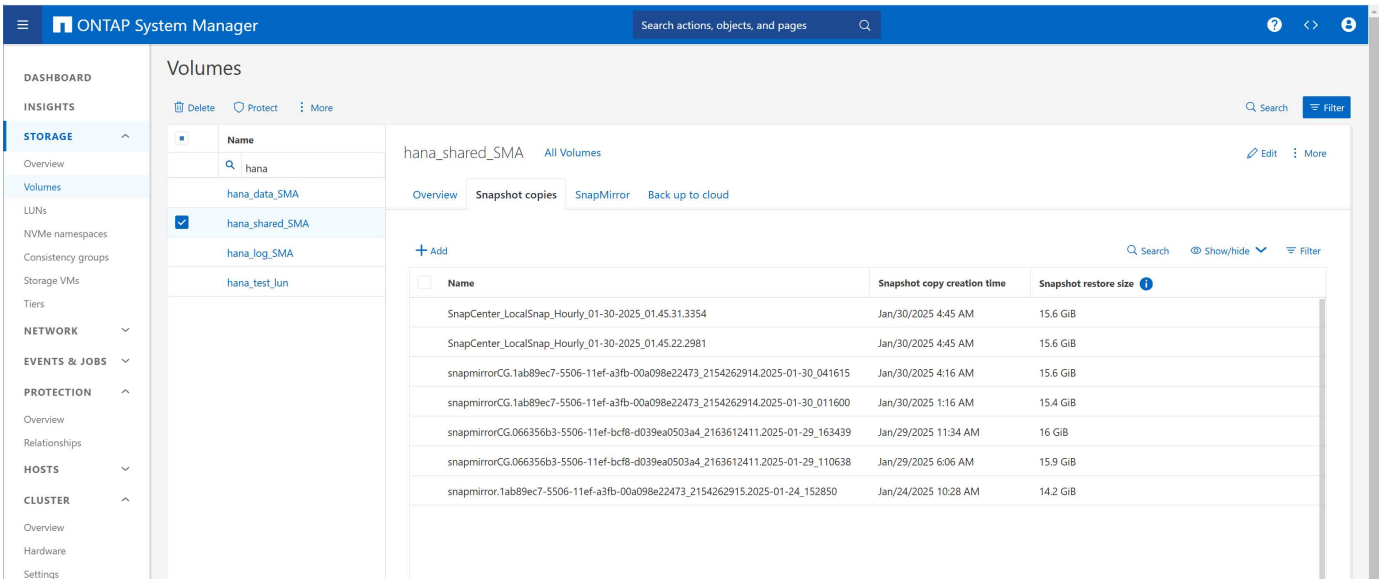
Ausfall des in SnapCenter konfigurierten Storage-Systems

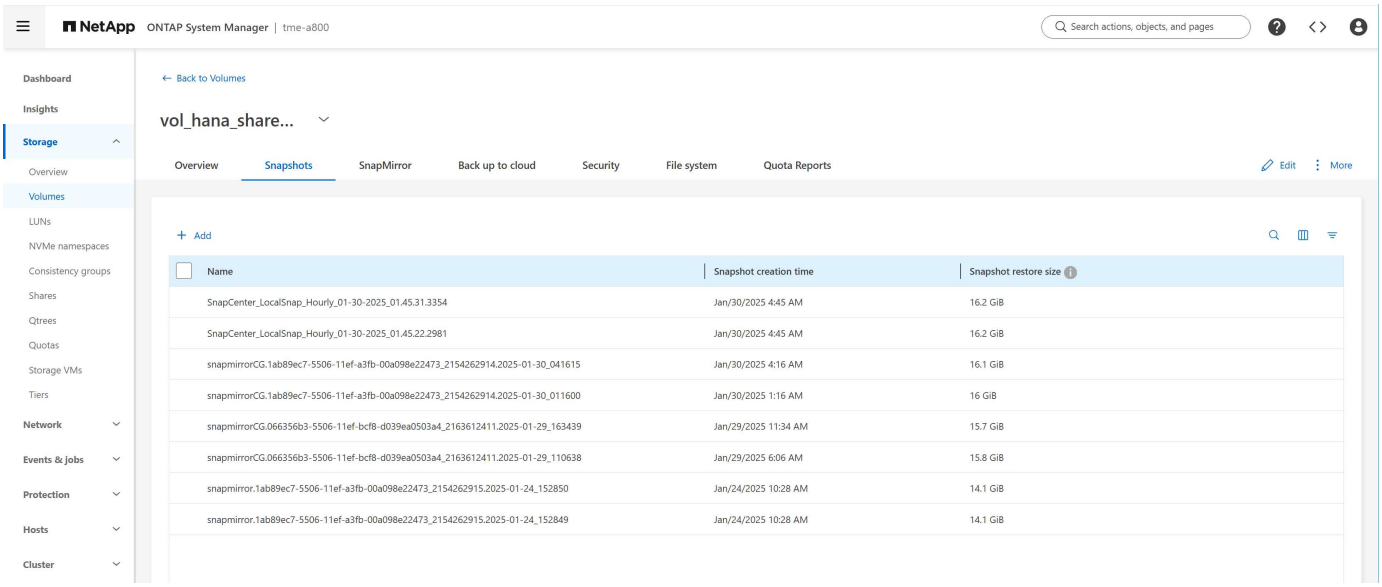
Bei einem Ausfall des in SnapCenter konfigurierten Storage-Systems wechselt SnapCenter nicht automatisch zu dem anderen Storage-System. Die nicht datenbezogene Volume-Ressource muss manuell angepasst werden, damit die gespiegelte Kopie des Volumes für Backup- und Restore-Vorgänge verwendet wird.



Backup-Vorgänge

Obwohl SnapCenter die SnapMirror Active Sync Konfiguration für das HANA Shared Volume nicht kennt, werden Snapshots an beiden Standorten repliziert.





Wiederherstellungsvorgang

Im Falle einer Wiederherstellung würde SnapCenter einfach eine Volume-Wiederherstellung ohne irgendwelche VMware spezifischen Schritte durchführen. Normalerweise müssten Sie das HANA Shared Volume auf dem Linux Host abmounten, den Datastore trennen und dann die Volume-Wiederherstellung durchführen, den Datastore erneut verbinden und dann das Filesystem auf dem Linux Host mounten. Als manuelle Operation könnten Sie die HANA VM stoppen, das HANA Shared Volume mit SnapCenter wiederherstellen und dann die VM erneut starten.

Failover-Szenarien

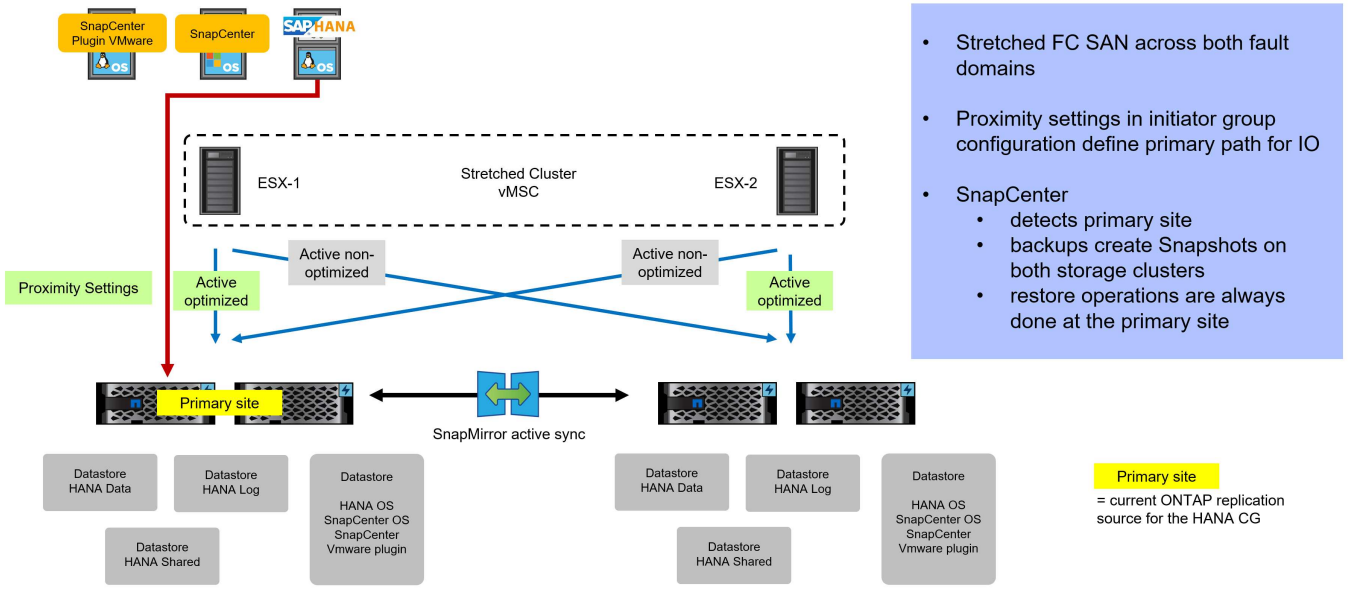
In diesem Artikel werden die Failover-Szenarien für diese Lösung hervorgehoben.

Einheitliche Zugriffseinrichtung

In einer einheitlichen Zugriffskonfiguration ist das Fibre-Channel-SAN auf beide Standorte verteilt. Die ESX Hosts an beiden Standorten könnten auf beide Kopien der Datensätze zugreifen. Während des normalen Betriebs greift der ESX Host, auf dem das HANA-System ausgeführt wird, basierend auf den Annäherungseinstellungen in der Konfiguration der Initiatorgruppe auf die lokale Kopie der Daten zu. Jeder ESX Host verfügt über einen aktiv optimierten Pfad zur lokalen Kopie und einen aktiven, nicht optimierten Pfad zur gespiegelten Kopie.

Normaler Betrieb

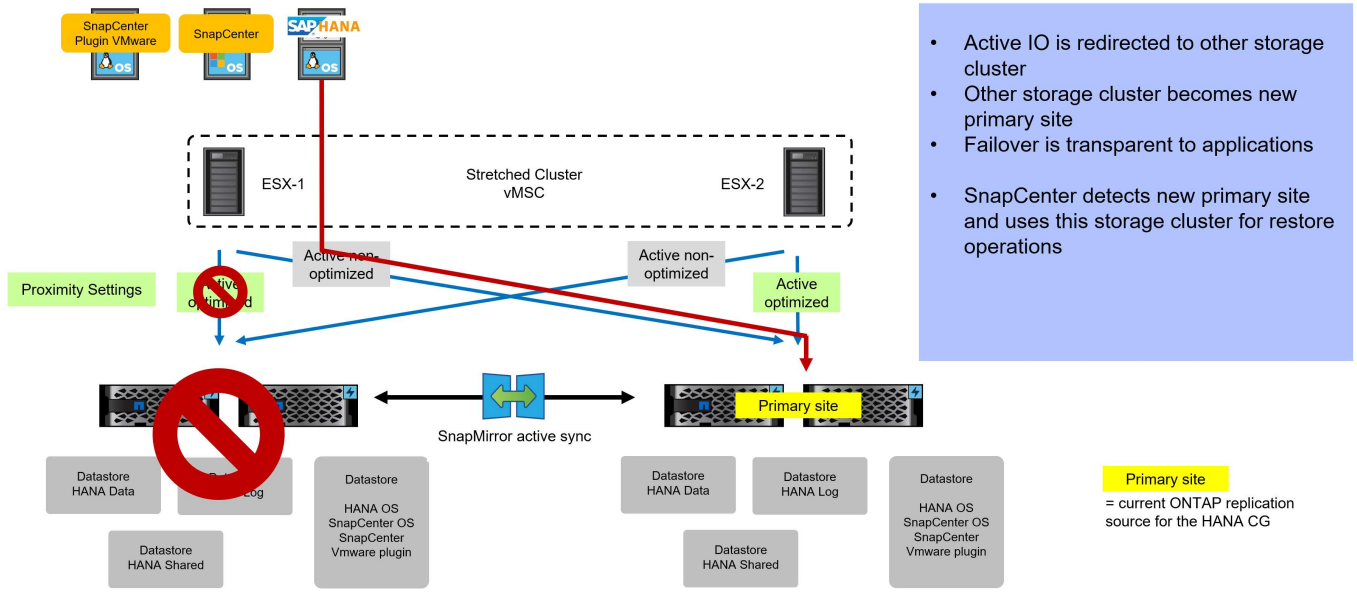
Im normalen Betrieb liest und schreibt das HANA-System basierend auf dem aktiv optimierten Pfad von ESX-Host ESX-1 von/auf die lokale Kopie. Bei jedem Backup-Vorgang erkennt SnapCenter den aktuellen primären Standort der Replizierungsbeziehung und führt die Backup-Vorgänge am primären Standort aus. Die Snapshots werden auf die gespiegelte Kopie repliziert und sind an beiden Standorten verfügbar. Am primären Standort würde eine SnapCenter-Wiederherstellung ausgeführt werden.



- Stretched FC SAN across both fault domains
- Proximity settings in initiator group configuration define primary path for IO
- SnapCenter
  - detects primary site
  - backups create Snapshots on both storage clusters
  - restore operations are always done at the primary site

Storage-Ausfall

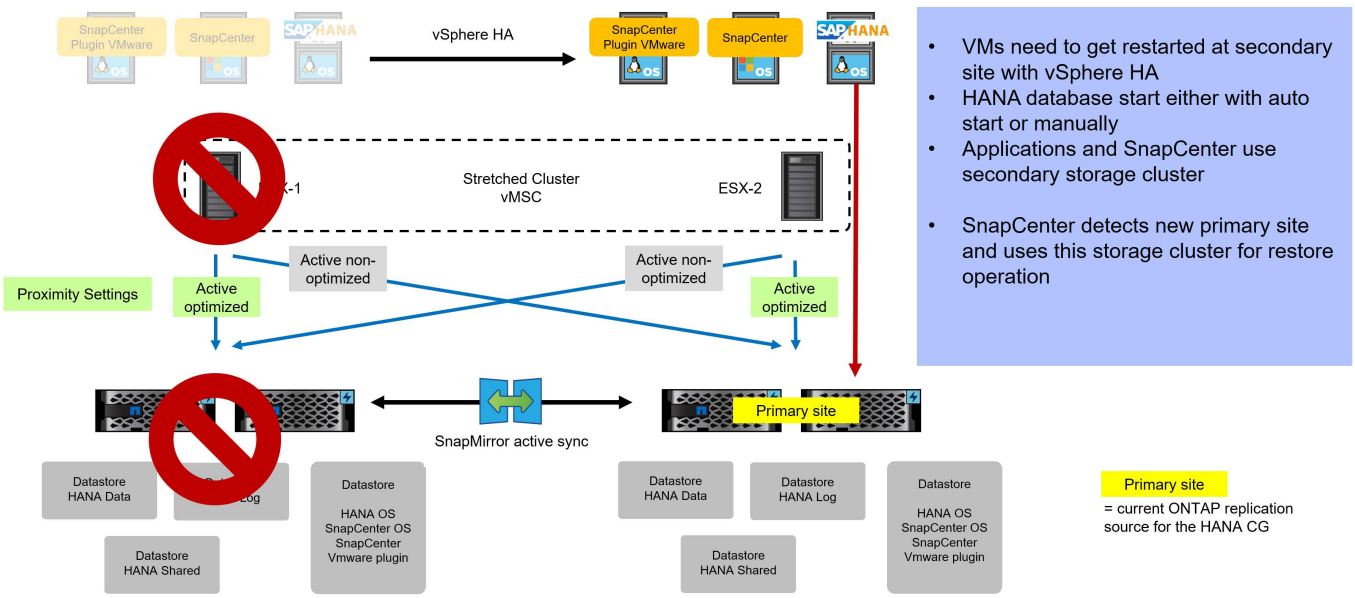
Fällt das Storage-System an Standort 1 aus, greifen die HANA-Systeme auf die gespiegelte Kopie an Standort 2 zu und setzen den Betrieb fort. Der primäre Standort schaltet auf den sekundären Standort um und SnapCenter führt nun Backup- und Restore-Vorgänge am neuen primären Standort aus.



- Active IO is redirected to other storage cluster
- Other storage cluster becomes new primary site
- Failover is transparent to applications
- SnapCenter detects new primary site and uses this storage cluster for restore operations

Standortausfall

Im Falle eines Standortausfalls werden sowohl die HANA VM als auch SnapCenter und das SnapCenter für VMware Plugin VM über vSphere HA auf den ESX-Host am sekundären Standort umschlagen. Die HANA-Datenbank muss gestartet werden und greift dann auf die gespiegelte Kopie am zweiten Standort zu. Der primäre Standort schaltet auf den sekundären Standort um und SnapCenter führt nun Backup- und Restore-Vorgänge am neuen primären Standort aus.



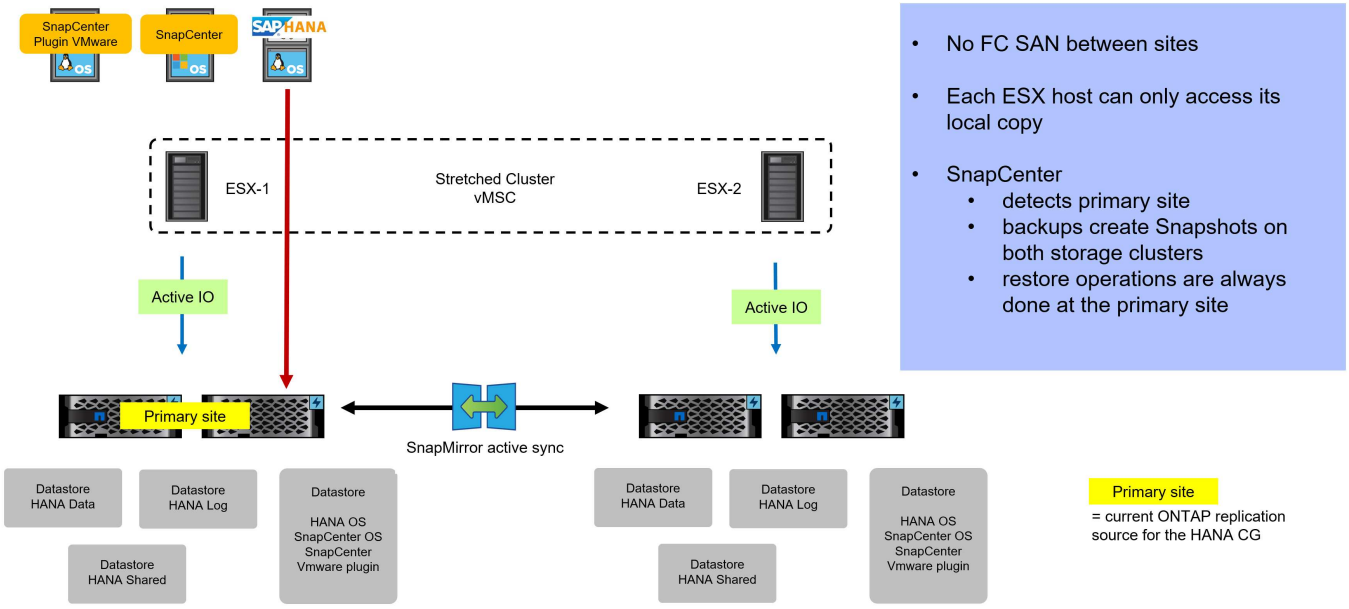
- VMs need to get restarted at secondary site with vSphere HA
- HANA database start either with auto start or manually
- Applications and SnapCenter use secondary storage cluster
- SnapCenter detects new primary site and uses this storage cluster for restore operation

Uneinheitliche Zugriffseinrichtung

In einer nicht einheitlichen Zugriffskonfiguration wird das Fibre-Channel-SAN nicht auf beide Standorte ausgedehnt. Jeder ESX Host an jedem Standort kann nur auf die lokale Kopie der Datensätze zugreifen.

Normaler Betrieb

Im normalen Betrieb liest und schreibt das HANA-System von/auf die lokale Kopie. Bei jedem Backup-Vorgang erkennt SnapCenter den aktuellen primären Standort der Replizierungsbeziehung und führt die Backup-Vorgänge am primären Standort aus. Die Snapshots werden auf die gespiegelte Kopie repliziert und sind an beiden Standorten verfügbar. Am primären Standort würde eine SnapCenter-Wiederherstellung ausgeführt werden.

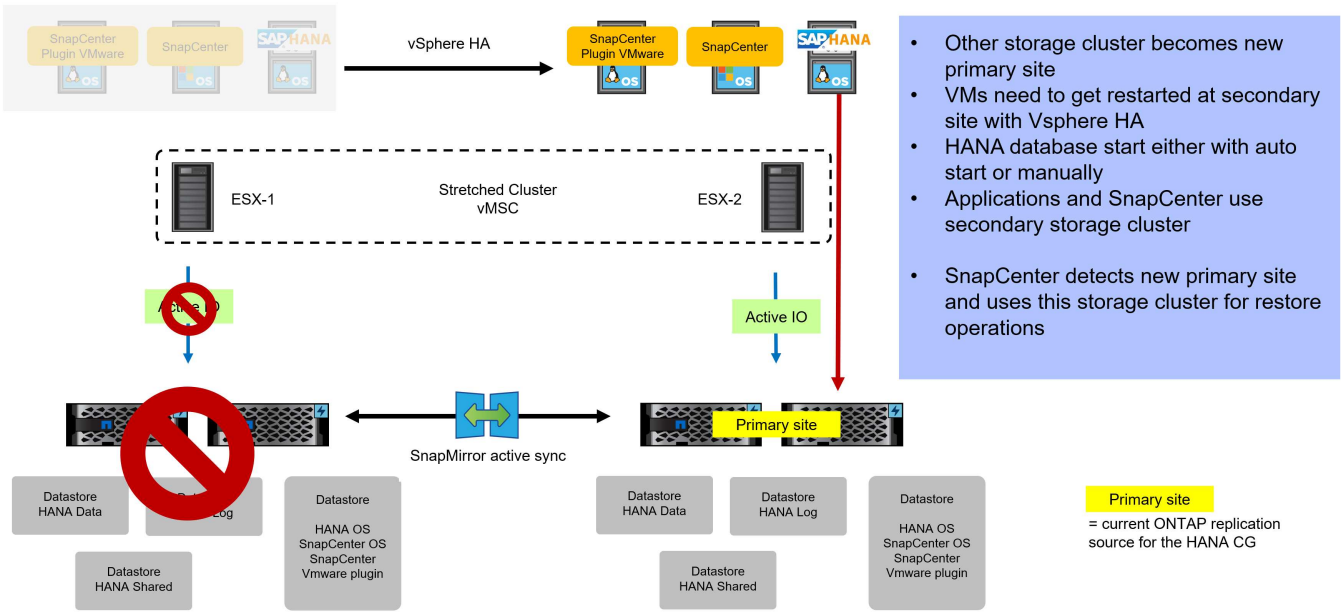


- No FC SAN between sites
- Each ESX host can only access its local copy
- SnapCenter
  - detects primary site
  - backups create Snapshots on both storage clusters
  - restore operations are always done at the primary site

Storage-Ausfall

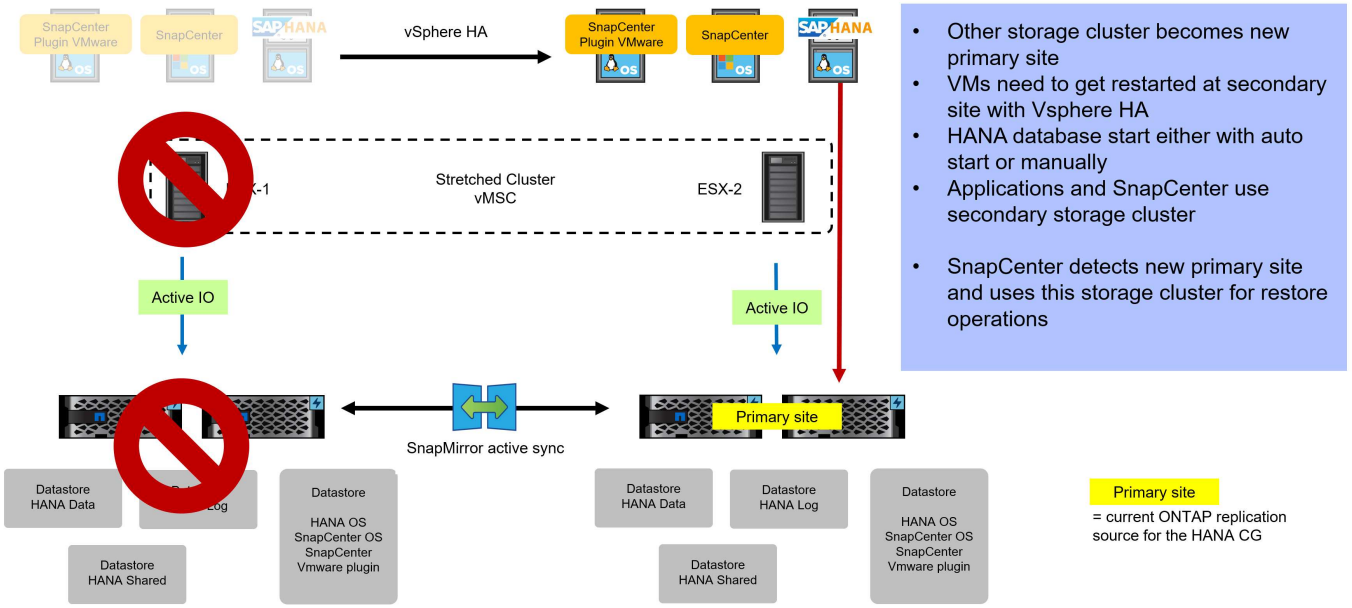
Im Falle eines Storage-Ausfalls werden sowohl die HANA VM als auch SnapCenter und das SnapCenter für VMware Plugin VM mithilfe von vSphere HA auf den ESX-Host am sekundären Standort umschlagen. Die

HANA-Datenbank muss gestartet werden und greift dann auf die gespiegelte Kopie am zweiten Standort zu. Der primäre Standort schaltet auf den sekundären Standort um und SnapCenter führt nun Backup- und Restore-Vorgänge am neuen primären Standort aus.



Standortausfall

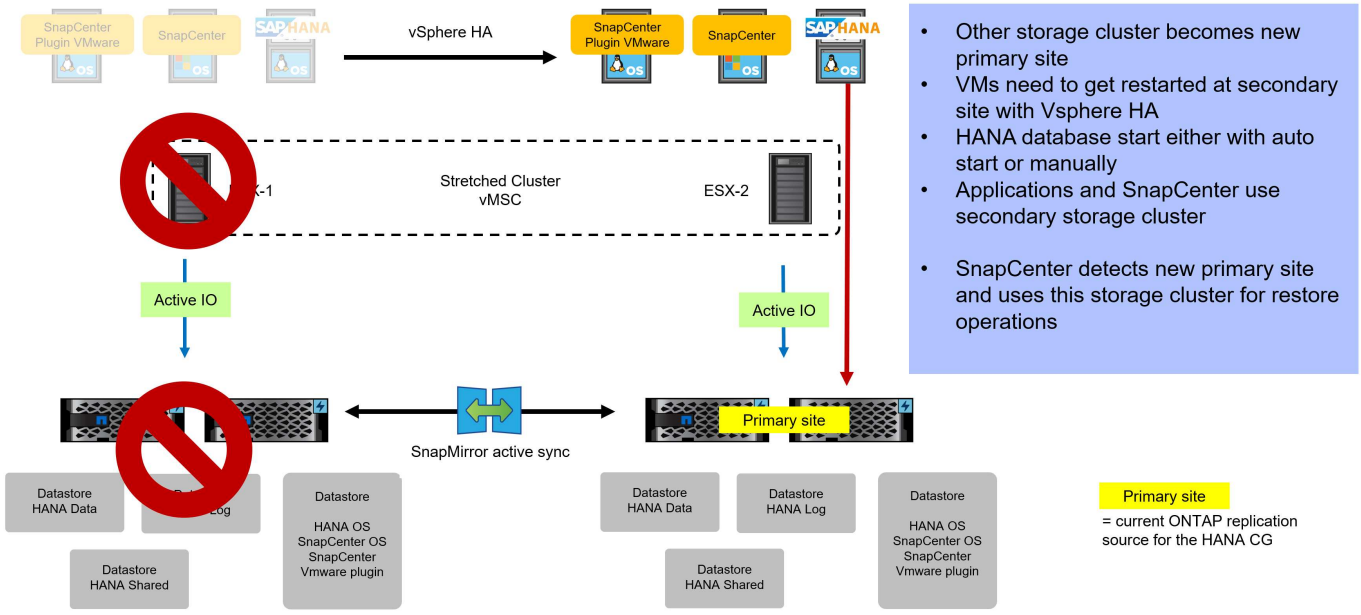
Das gleiche gilt für Storage-Ausfälle.



Verlagerung der HANA-VM oder des primären Standorts

Wenn die HANA VM auf den anderen ESX Host umgezogen wird und der primäre Standort des Storage unverändert bleibt, schlägt ein Wiederherstellungsvorgang mit SnapCenter fehl. Da SnapCenter zur Durchführung der Wiederherstellung den primären Standort nutzt, wird der Klon auf der linken Seite erstellt, während die HANA VM auf der rechten Seite ausgeführt wird. Da es keinen Datenpfad zwischen den Standorten gibt, wird SnapCenter die Daten nicht kopieren.

Als Behelfslösung müssen Sie sicherstellen, dass die Verschiebung der VM und der primären Seite gemeinsam durchgeführt wird oder Sie vor der Wiederherstellung mit SnapCenter einen Failover des primären Standorts durchführen müssen.



Zusätzliche Informationen und Versionsverlauf

Dieser Artikel enthält Links zu weiteren Ressourcen für diese Lösung.

SnapCenter

"Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter"

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

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

"SnapCenter-Softwaredokumentation"

Aktive SnapMirror-Synchronisierung:

"Übersicht über die aktive SnapMirror-Synchronisierung in ONTAP"

"NetApp ONTAP mit NetApp SnapMirror Active Sync mit VMware vSphere Metro Storage Cluster (vMSC)."

"VMware vSphere Metro Storage-Cluster mit SnapMirror Active Sync"

"VMware vSphere Metro Storage-Cluster (vMSC)"

Versionsverlauf:

Version	Datum	Kommentar
Version 1.0	März 2025	Ausgangsversion

SAP HANA-Datenschutz mit SnapCenter mit VMware VMFS und NetApp ASA -Systemen

SAP HANA-Datenschutz mit SnapCenter mit VMware VMFS und NetApp ASA -Systemen

In diesem Dokument werden die Best Practices für den Datenschutz mit SnapCenter für HANA-Systeme beschrieben, die auf VMware mit Datenspeichern ausgeführt werden, die VMFS und LUNs verwenden, die auf NetApp ASA -Systemen gespeichert sind.

Autor: Nils Bauer, NetApp

Inhalt des vorliegenden Dokuments

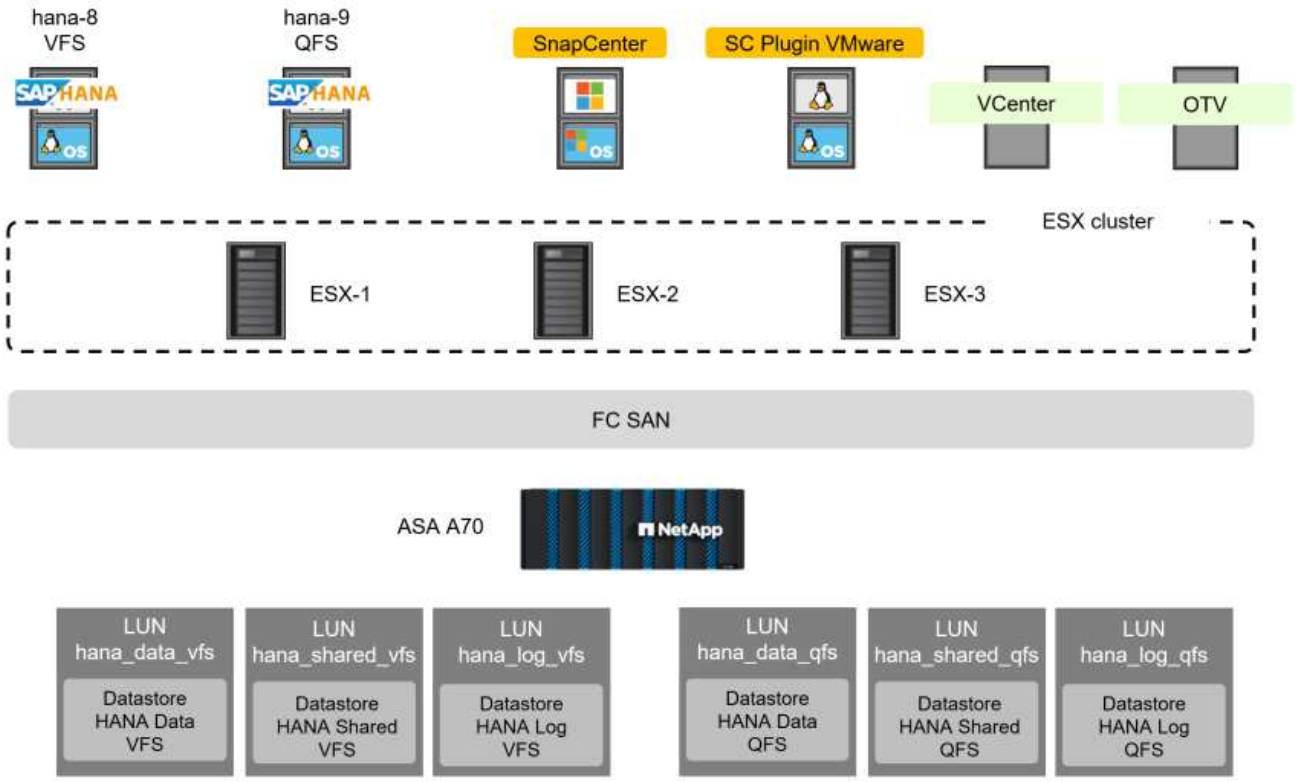
Es dient nicht als Schritt-für-Schritt-Anleitung zur Konfiguration der gesamten Umgebung, sondern konzentriert sich auf Details, die spezifisch für SnapCenter und HANA auf VMFS sind, darunter:

- Einrichten von SAP HANA-Systemen mit VMware VMFS
- Spezifische SnapCenter -Konfigurationen für HANA auf VMware mit VMFS
- SnapCenter -Sicherungs-, Wiederherstellungs- und Recovery-Vorgänge für HANA auf VMware mit VMFS
- SnapCenter SAP System Refresh-Vorgänge für HANA auf VMware mit VMFS

Weitere Informationen und detaillierte Konfigurationsanweisungen finden Sie in den Dokumenten im ""Weitere Informationen"" Kapitel.

Für dieses Dokument verwendeter Laboraufbau

Die folgende Abbildung bietet einen Überblick über das verwendete Labor-Setup. Zwei Single-Host-HANA-MDC-Systeme dienen zur Demonstration der verschiedenen Vorgänge. Das HANA-System VFS ist für die Ausführung von Sicherungs-, Wiederherstellungs- und Recovery-Vorgängen vorgesehen, während das HANA-System QFS als Zielsystem für SAP-Systemaktualisierungen dient. Das SnapCenter Plug-in für VMware ist unerlässlich, damit SnapCenter die mit VMware VMFS konfigurierten HANA-Ressourcen verwalten kann. Obwohl ONTAP Tools für VMware zur Bereitstellung der Speichereinheiten für die HANA-Systeme verwendet wurden, sind diese keine zwingende Komponente.



Softwareversionen

Software	Version
ONTAP	ASA A70 ONTAP 9.16.1
VSphere Client	8.0.3
ESXi	8.0.3
SnapCenter Plug-in für vSphere	6.1.0
ONTAP Tools für VMware vSphere	10,4
Linux BS	SLES FÜR SAP 15 SP6
SAP HANA	2,0 SPS8
SnapCenter	6.1P1

HANA-Systembereitstellung und -Installation

In diesem Kapitel werden die Installation und Konfiguration des für eine VMware-Einrichtung mithilfe von VMFS spezifischen SAP HANA-Systems beschrieben. Weitere allgemeine Best Practices finden Sie unter "Technischer Bericht: SAP HANA on NetApp ASA Systems with Fibre Channel Protocol".

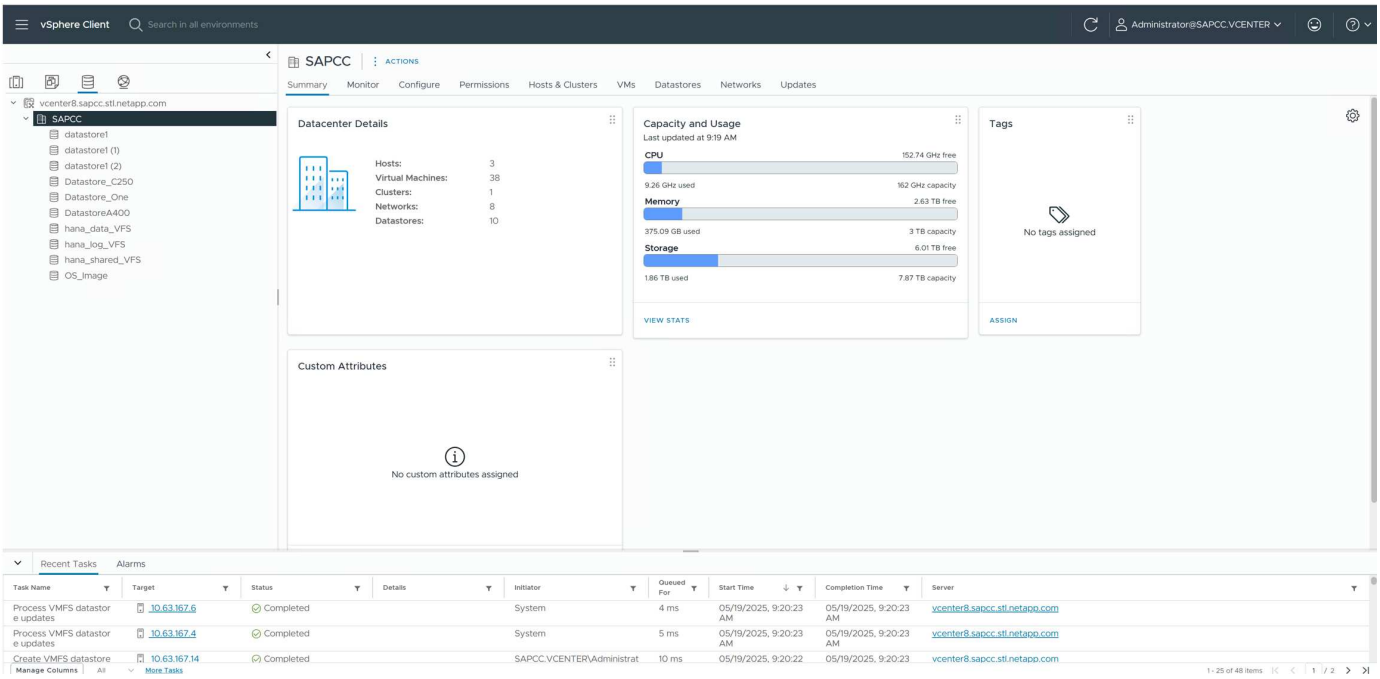
Storage-Konfiguration

Um die von SAP definierten Speicherleistungs-KPIs für HANA-Produktionssysteme zu erfüllen, müssen dedizierte LUNs und Datenspeicher für die Daten- und Protokolldateisysteme des HANA-Systems konfiguriert werden. Datenspeicher dürfen nicht von mehreren HANA-Systemen oder anderen Workloads gemeinsam genutzt werden.

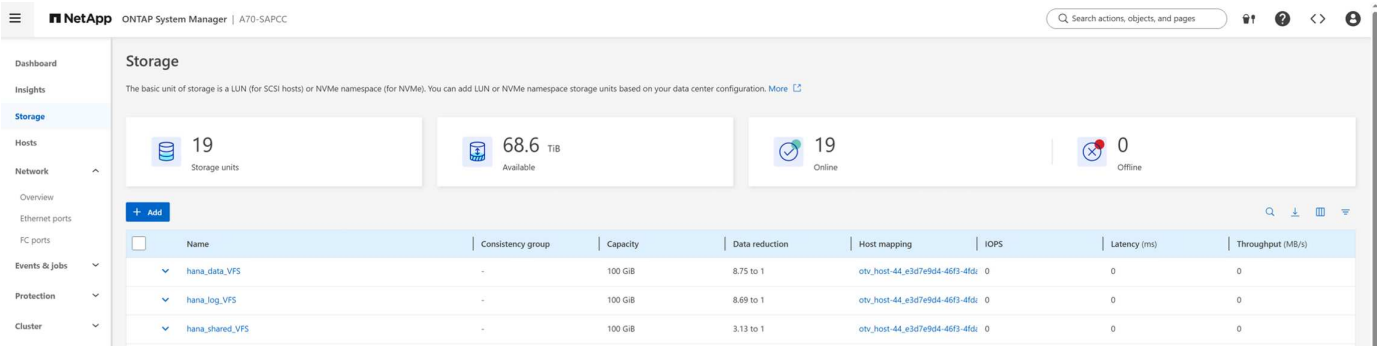
ONTAP Tools für VMware (OTV) wurden verwendet, um die drei Datenspeicher für das HANA-System VFS bereitzustellen.

- hana_data_VFS
- hana_log_VFS
- hana_shared_VFS

Der Datenspeicher für das gemeinsam genutzte HANA-Dateisystem kann auch von mehreren HANA-Systemen gemeinsam genutzt werden.

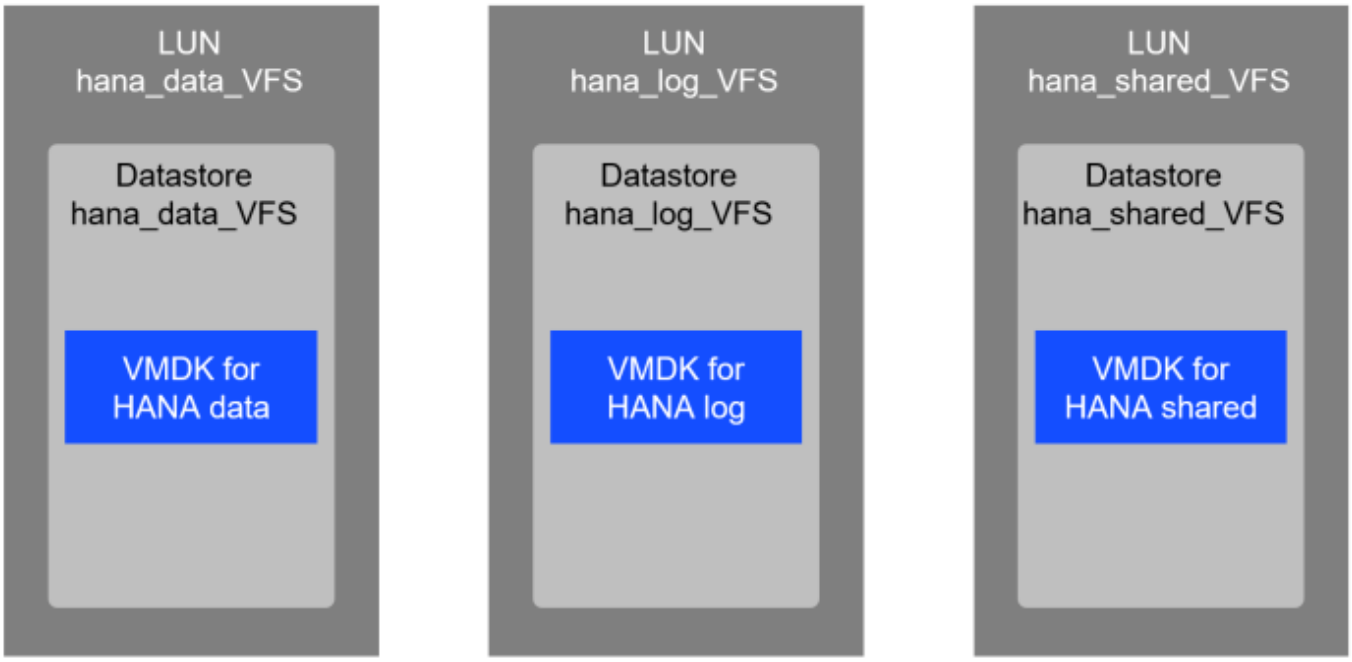


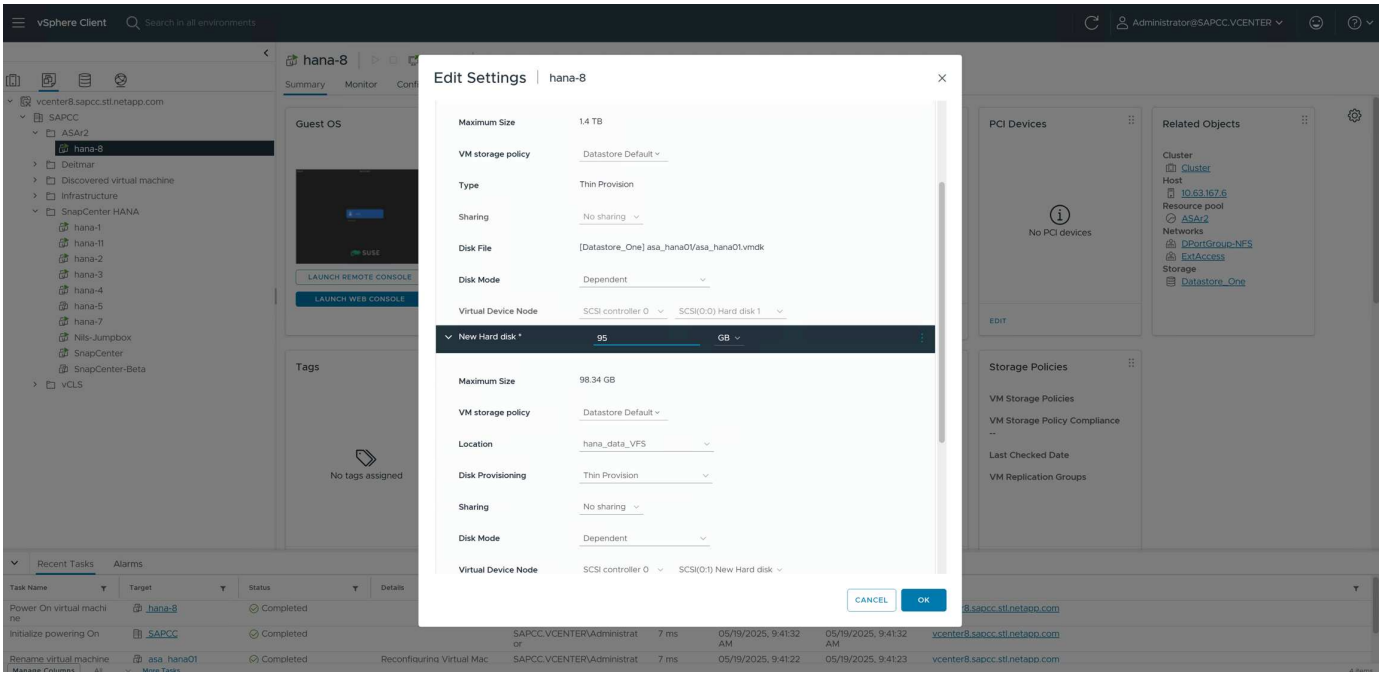
Auf dem Speichersystem wurden von OTV drei LUNs erstellt.

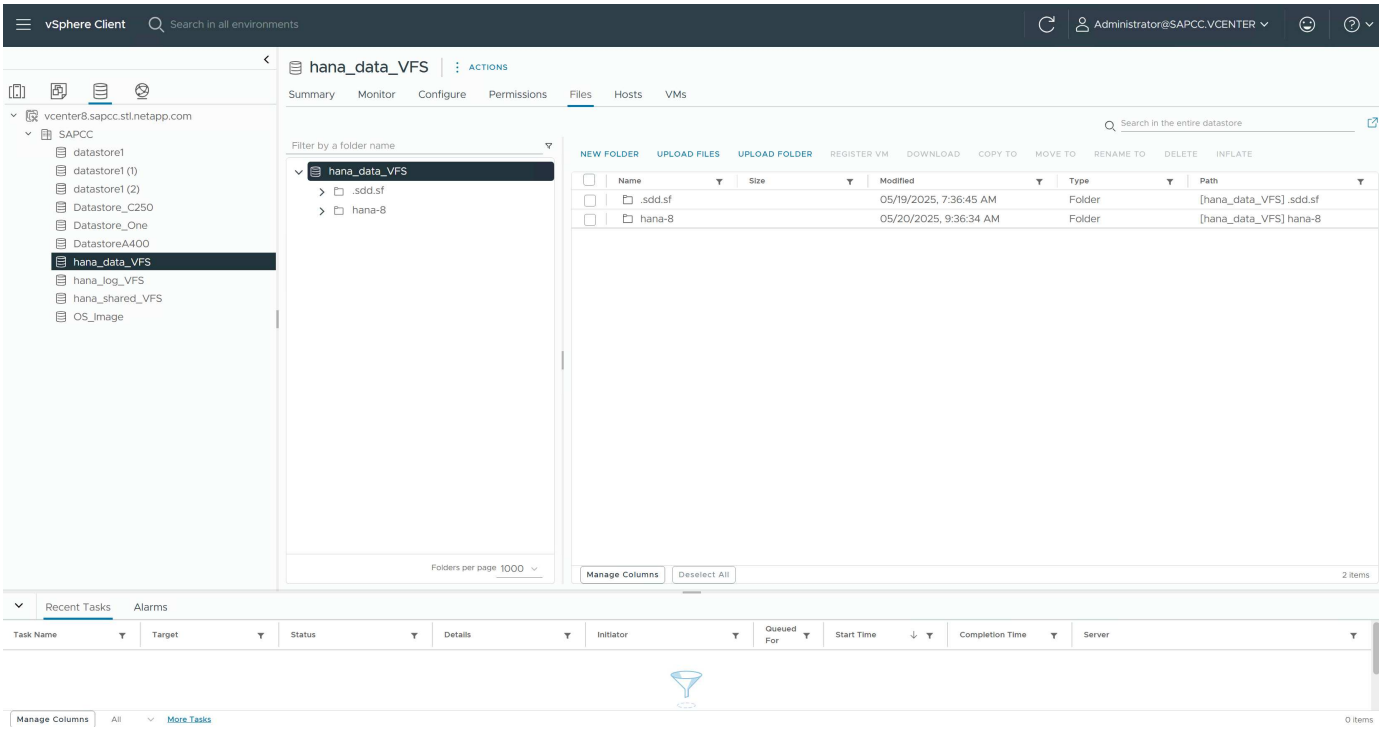


Konfiguration von VM-Festplatten

Der HANA-VM müssen drei neue Datenträger (VMDK) hinzugefügt werden. Jeder Datenträger befindet sich in einem der zuvor erstellten Datenspeicher, wie in der Abbildung unten dargestellt.


LUN
hana_data_VFS
Datastore
hana_data_VFS
VMDK for
HANA data
LUN
hana_log_VFS
Datastore
hana_log_VFS
VMDK for
HANA log
LUN
hana_shared_VFS
Datastore
hana_shared_VFS
VMDK for
HANA shared


vSphere Client
Edit Settings
hana-8
Maximum Size
1.4 TB
VM storage policy
Datastore Default
Type
Thin Provision
Sharing
No sharing
Disk File
[Datastore_One] asa_hana01/asa_hana01.vmdk
Disk Mode
Dependent
Virtual Device Node
SCSI controller 0
SCSI(0:0) Hard disk 1
New Hard disk *
95
GB
Maximum Size
98.34 GB
VM storage policy
Datastore Default
Location
hana_data_VFS
Disk Provisioning
Thin Provision
Sharing
No sharing
Disk Mode
Dependent
Virtual Device Node
SCSI controller 0
SCSI(0:1) New Hard disk
CANCEL
OK



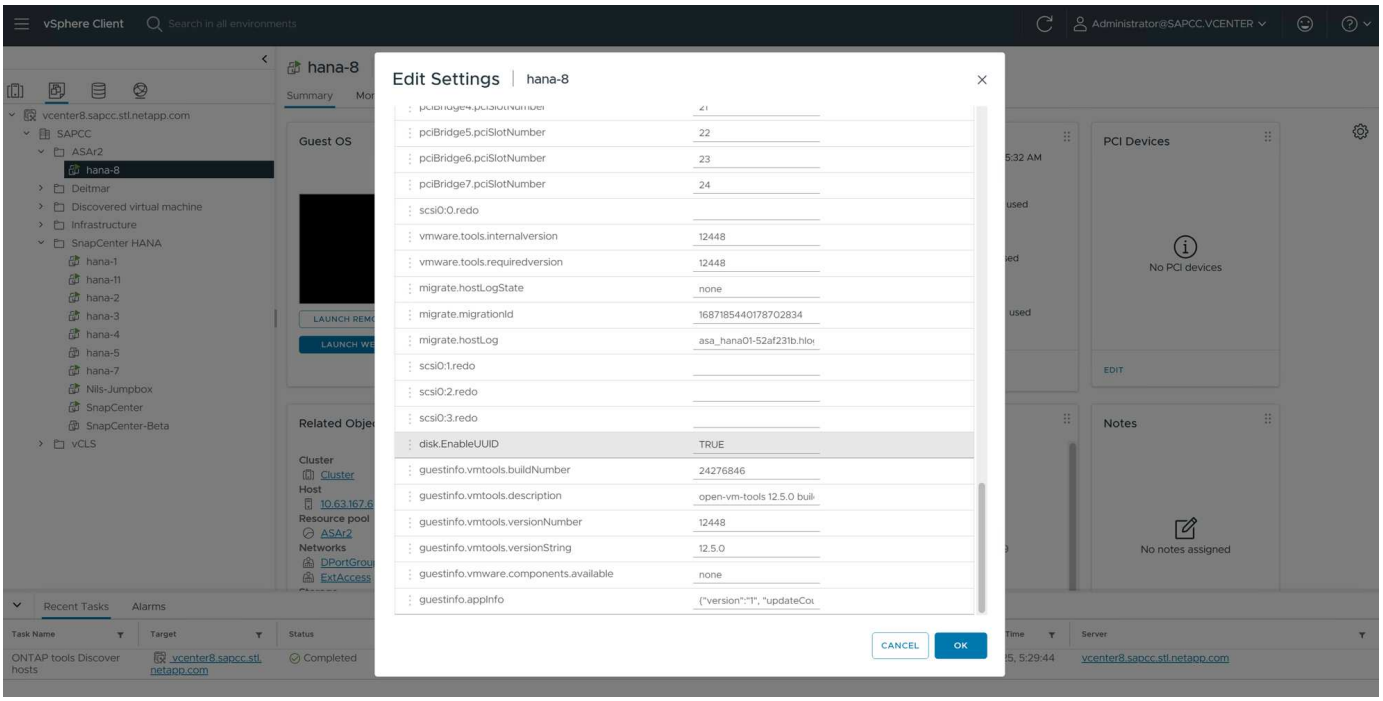
Wenn die drei Festplatten zur VM hinzugefügt wurden, können sie auf Betriebssystemebene aufgelistet werden.

```
hana-8:~ # lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 100G 0 disk
├─sda1 8:1 0 256M 0 part /boot/efi
└─sda2 8:2 0 82G 0 part
├─system-root 254:0 0 60G 0 lvm /root
│ /var
│ /usr/local
│ /tmp
│ /srv
│ /opt
│ /home
│ /boot/grub2/x86++_++64-efi
│ /boot/grub2/i386-pc
│ /.snapshots
│ /
└─system-swap 254:1 0 2G 0 lvm [SWAP]
sdb 8:16 0 95G 0 disk
sdc 8:32 0 95G 0 disk
sdd 8:48 0 95G 0 disk
sr0 11:0 1 17.1G 0 rom
```

VM-Parameter disk.EnableUUID

Dieser Parameter muss entsprechend eingestellt werden, sonst schlägt die automatische Erkennung der SnapCenter Datenbank fehl.

1. VM herunterfahren
2. Neuen Parameter „disk.EnableUUID“ hinzufügen und auf „TRUE“ setzen
3. VM starten



Vorbereitung des Dateisystems auf Linux-Host

Erstellung des xfs-Dateisystems auf neuen Platten

Auf jedem der drei neuen Festplatten wurde ein xfs-Dateisystem erstellt.

```
hana-8:~ # mkfs.xfs /dev/sdb
meta-data=/dev/sdb isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nrext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.

hana-8:~ # mkfs.xfs /dev/sdc
meta-data=/dev/sdc isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nrext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.

hana-8:~ # mkfs.xfs /dev/sdd
meta-data=/dev/sdd isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nrext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.

hana-8:~ #
```

Erstellung von Bereitstellungspunkten

```
hana-8:/ # mkdir -p /hana/data/VFS/mnt00001
hana-8:/ # mkdir -p /hana/log/VFS/mnt00001
hana-8:/ # mkdir -p /hana/shared
hana-8:/ # chmod –R 777 /hana/log/SMA
hana-8:/ # chmod –R 777 /hana/data/SMA
hana-8:/ # chmod -R 777 /hana/shared
```

Konfiguration von /etc/fstab

```
hana-8:/ # cat /etc/fstab

/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=/@/var 0 0
/dev/system/root /usr/local btrfs subvol=/@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=/@/tmp 0 0
/dev/system/root /srv btrfs subvol=/@/srv 0 0
/dev/system/root /root btrfs subvol=/@/root 0 0
/dev/system/root /opt btrfs subvol=/@/opt 0 0
/dev/system/root /home btrfs subvol=/@/home 0 0
/dev/system/root /boot/grub2/x86++_++64-efi btrfs
subvol=/@/boot/grub2/x86++_++64-efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=/@/.snapshots 0 0
UUID=FB79-24DC /boot/efi vfat utf8 0 2
### SAPCC_share
192.168.175.86:/sapcc_share /mnt/sapcc-share nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
/dev/sdb /hana/data/VFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/VFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
hana-8:/ #

hana-8:/ # df -h
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 4.4G 54G 8% /
devtmpfs 4.0M 0 4.0M 0% /dev
tmpfs 49G 0 49G 0% /dev/shm
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 18M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
```

```
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/mapper/system-root 60G 4.4G 54G 8% /.snapshots
/dev/mapper/system-root 60G 4.4G 54G 8% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 4.4G 54G 8% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 4.4G 54G 8% /home
/dev/mapper/system-root 60G 4.4G 54G 8% /opt
/dev/mapper/system-root 60G 4.4G 54G 8% /srv
/dev/mapper/system-root 60G 4.4G 54G 8% /tmp
/dev/mapper/system-root 60G 4.4G 54G 8% /usr/local
/dev/mapper/system-root 60G 4.4G 54G 8% /var
/dev/sda1 253M 5.9M 247M 3% /boot/efi
/dev/mapper/system-root 60G 4.4G 54G 8% /root
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
192.168.175.86:/sapcc_share 1.4T 840G 586G 59% /mnt/sapcc-share
/dev/sdb 95G 1.9G 94G 2% /hana/data/VFS/mnt00001
/dev/sdc 95G 1.9G 94G 2% /hana/log/VFS/mnt00001
/dev/sdd 95G 1.9G 94G 2% /hana/shared

hana-8:/ #
```

HANA-Installation

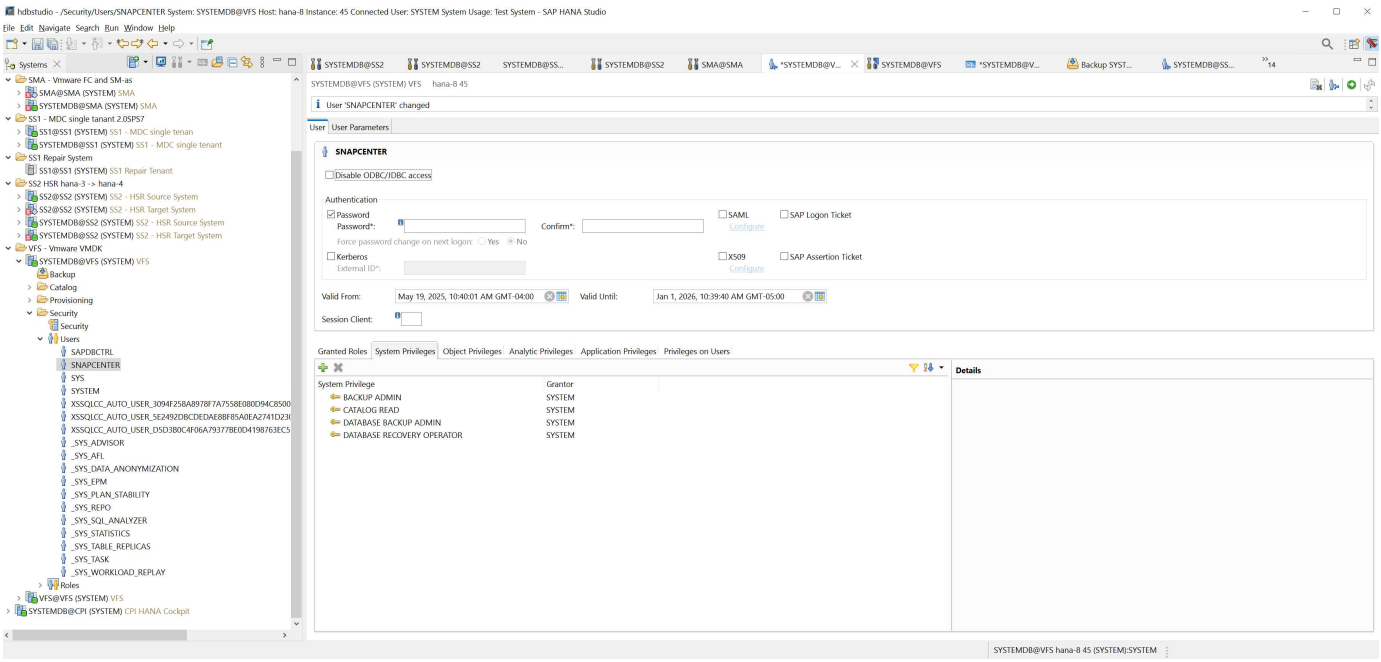
Die HANA-Installation kann nun ausgeführt werden.

> Bei der beschriebenen Konfiguration befindet sich das Verzeichnis /usr/sap/VFS auf der OS VMDK. Wenn /usr/sap/VFS in der gemeinsam genutzten VMDK gespeichert werden soll, kann der gemeinsam genutzte hana-Datenträger partitioniert werden, um ein weiteres Dateisystem für /usr/sap/VFS bereitzustellen.

HANA-Konfiguration

Konfigurieren des SnapCenter -Datenbankbenutzers

Es muss ein Benutzerspeicher für einen Systemdatenbankbenutzer erstellt werden, der von SnapCenter verwendet werden soll.



Konfigurieren des HDB-Benutzerspeicherschlüssels

Für den Benutzer vfsadm muss ein User Store Key angelegt werden. Für die Kommunikation mit dem Port muss die HANA-Instanznummer entsprechend gesetzt werden. In unserem Setup wird die Instanznummer „45“ verwendet.

```
vfsadm@hana-8:/usr/sap/VFS/HDB45> hdbuserstore SET VFSKEY hana-8:34513
SNAPCENTER <password>

Retroactive report: Operation succeed.
```

Zugriff prüfen mit:

```
vfsadm@hana-8:/usr/sap/VFS/HDB45> hdbsql -U VFSKEY

Welcome to the SAP HANA Database interactive terminal.
Type: \h for help with commands
\q to quit
hdbsql SYSTEMDB=> exit

vfsadm@hana-8:/usr/sap/VFS/HDB45>
```

SnapCenter-Konfiguration

Voraussetzungen

Die SnapCenter HANA-Ressource muss automatisch erkannt werden

Mit VMware VMFS konfigurierte Ressourcen müssen von SnapCenter automatisch erkannt werden, um bestimmte für diese Konfigurationen erforderliche Vorgänge zu ermöglichen.

Da es sich bei HANA-Nicht-Datenvolumes in SnapCenter immer um manuell konfigurierte Ressourcen handelt, werden sie von SnapCenter mit VMFS nicht unterstützt.

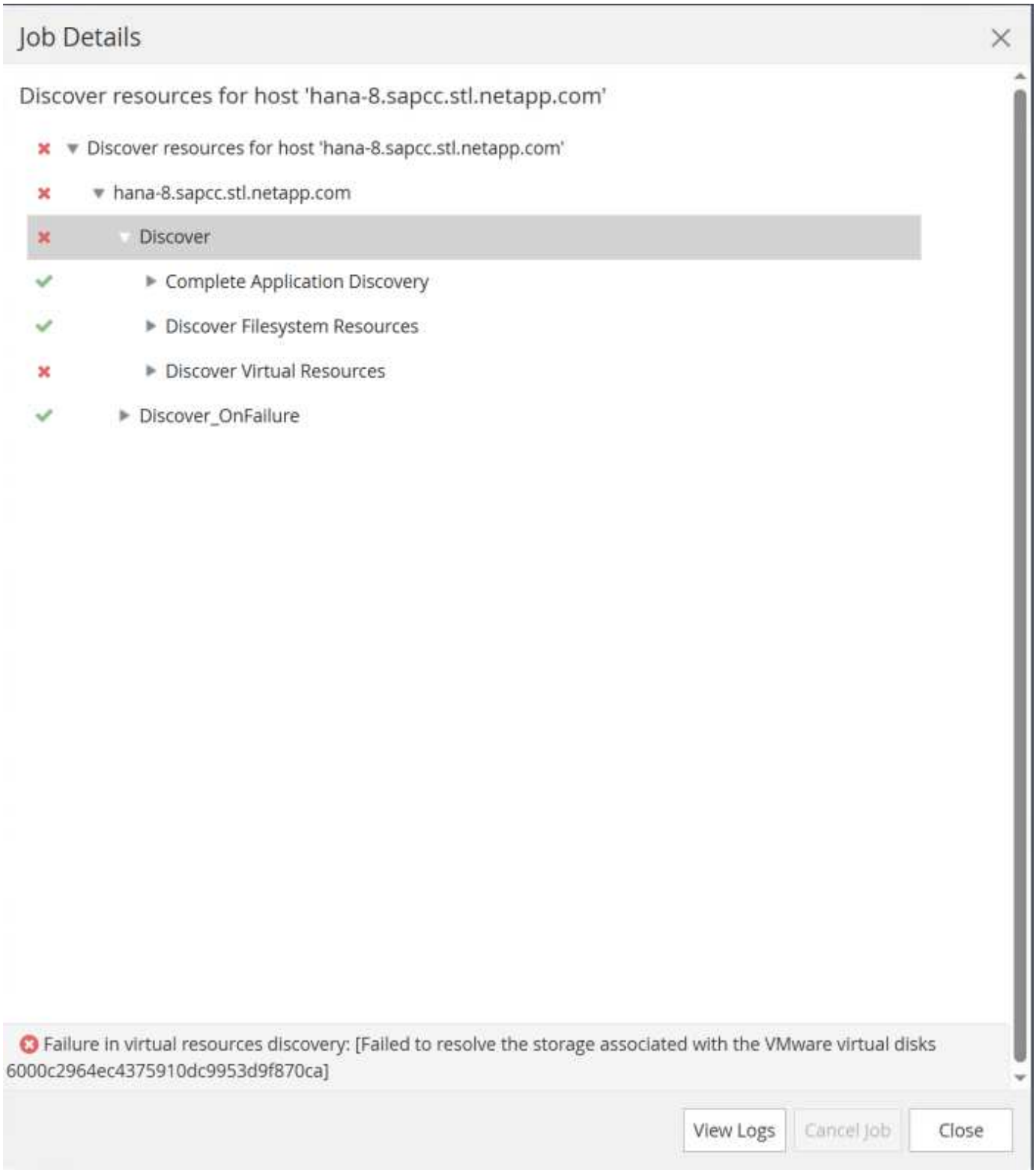
SAP HANA-Mehrfachhostsysteme müssen über ein zentrales HANA-Plugin konfiguriert werden und werden daher standardmäßig manuell konfiguriert. Solche Systeme werden von SnapCenter bei Verwendung von VMware VMFS auch nicht unterstützt.

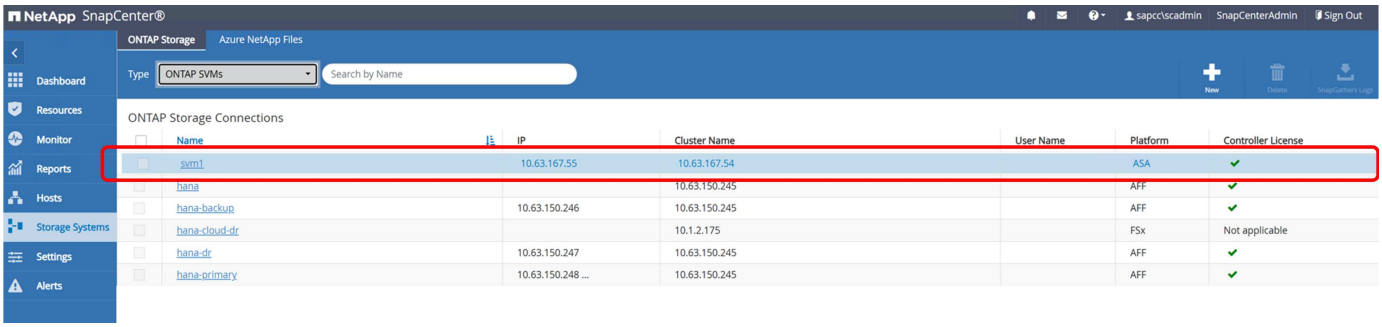
SnapCenter für VMware vSphere Plug-in

Das SnapCenter für VMware vSphere Plug-in muss in der VMware Umgebung implementiert werden.

Storage-SVM-Management-IP

Für Speicher-SVMs, die die LUNs hosten, muss eine Verwaltungsschnittstelle konfiguriert sein. Andernfalls werden die SVMs beim Hinzufügen von Speicher mit der Option „Cluster hinzufügen“ nicht in SnapCenter aufgeführt und der automatische Erkennungsvorgang schlägt fehl.


Job Details
Discover resources for host 'hana-8.sapcc.stl.netapp.com'
Discover resources for host 'hana-8.sapcc.stl.netapp.com'
hana-8.sapcc.stl.netapp.com
Discover
Complete Application Discovery
Discover Filesystem Resources
Discover Virtual Resources
Discover_OnFailure
Failure in virtual resources discovery: [Failed to resolve the storage associated with the VMware virtual disks 6000c2964ec4375910dc9953d9f870ca]
View Logs
Cancel Job
Close



VM-Festplattenparameter

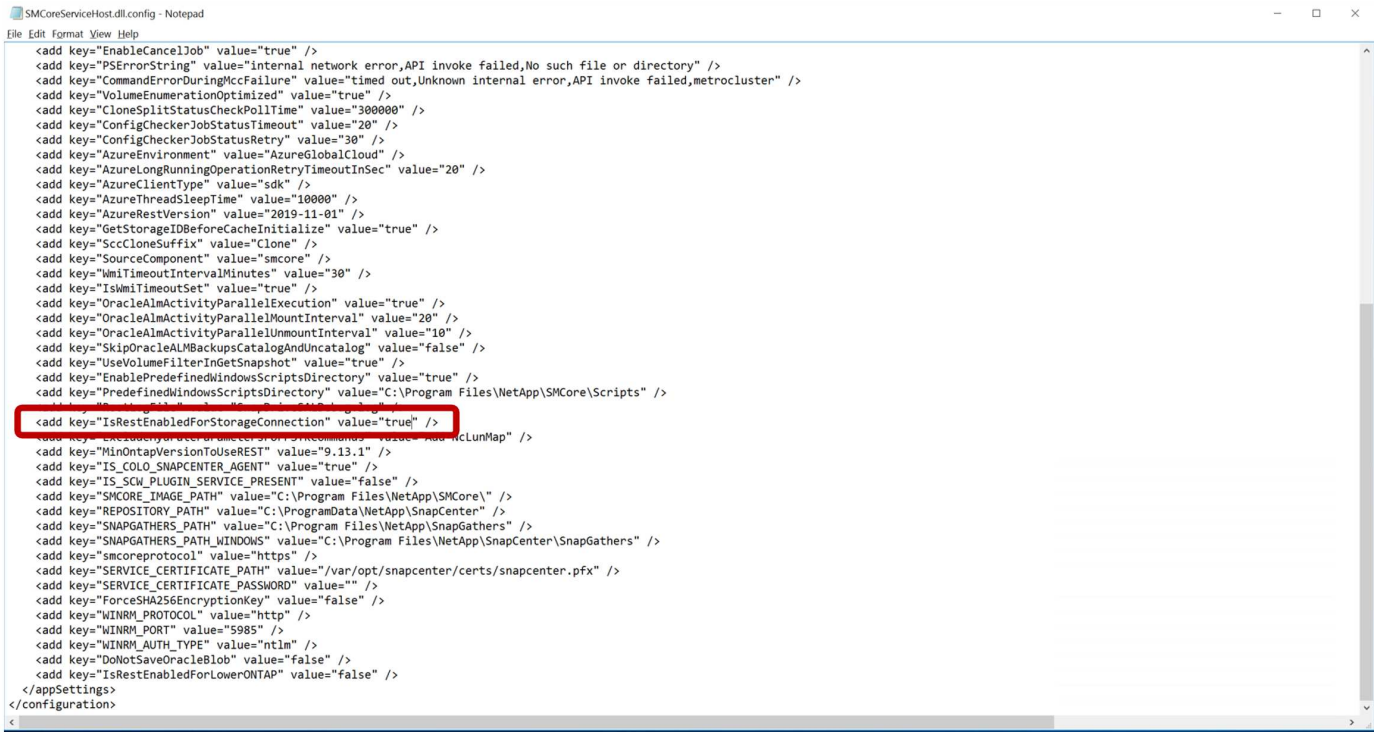
Der Parameter muss wie im Kapitel beschrieben eingestellt werden "„VM-Parameter disk.EnableUUID“" , andernfalls schlägt die automatische Erkennung der SnapCenter -Datenbank fehl.

Konfigurieren Sie SnapCenter für die Verwendung von REST-APIs für die Speicherkommunikation

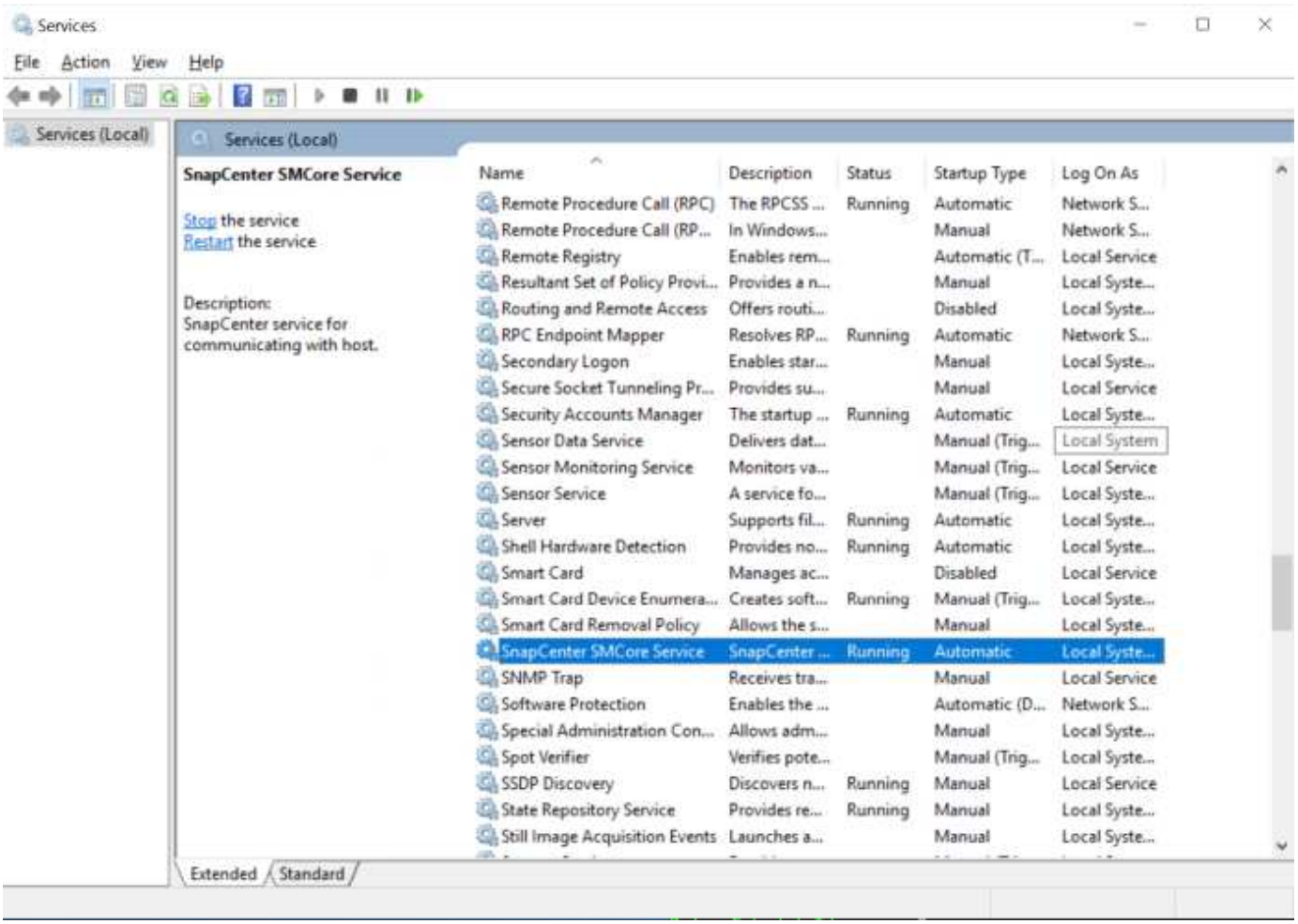
SnapCenter muss für die Speicherkommunikation REST-APIs verwenden. Andernfalls schlägt die Snapshot-Erstellung mit der unten gezeigten Fehlermeldung fehl.

Der Parameter „IsRestEnabledForStorageConnection“ in der Konfigurationsdatei + C:\Program Files\NetApp\SMCore\SMCoreServiceHost.dll.config muss auf „true“ gesetzt werden.

<add key="IsRestEnabledForStorageConnection" value="true" />



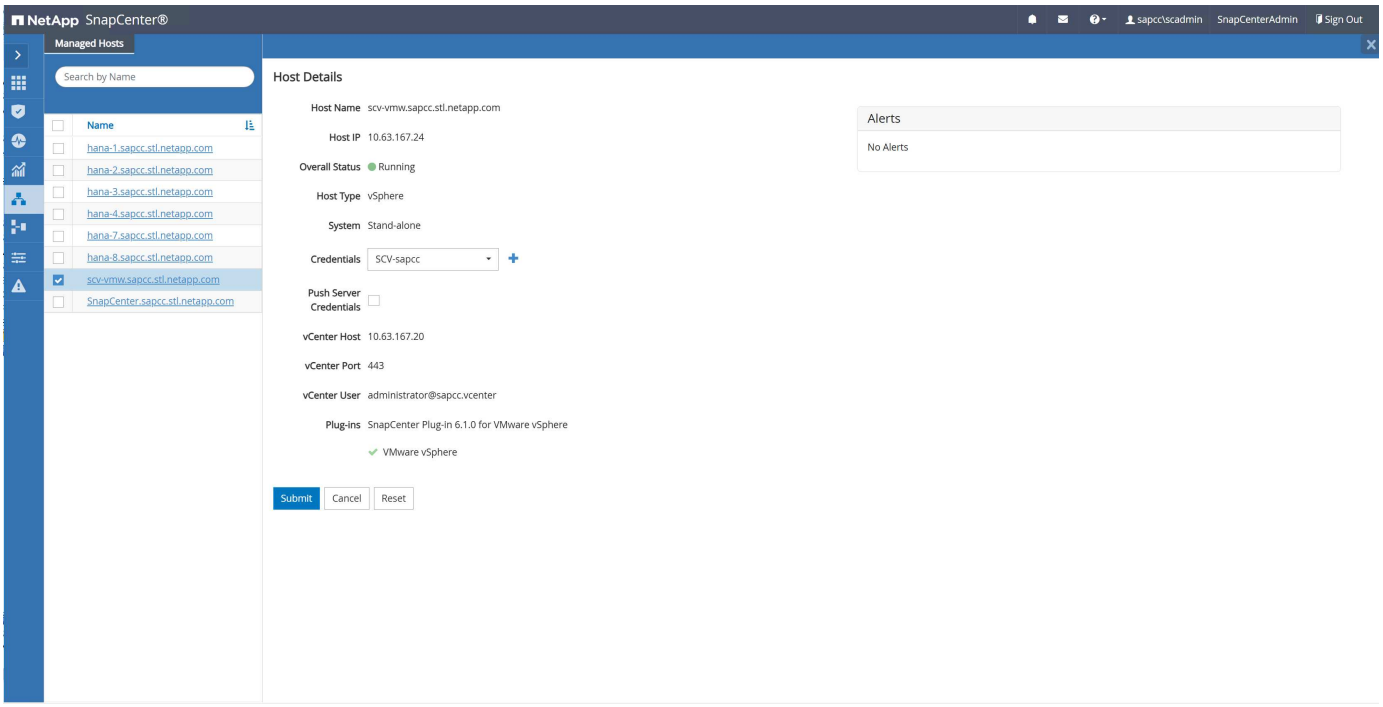
Nachdem die Änderung vorgenommen wurde, muss der SnapCenter SMCore-Dienst gestoppt und gestartet werden.



VMware-Plugin zu SnapCenter hinzufügen

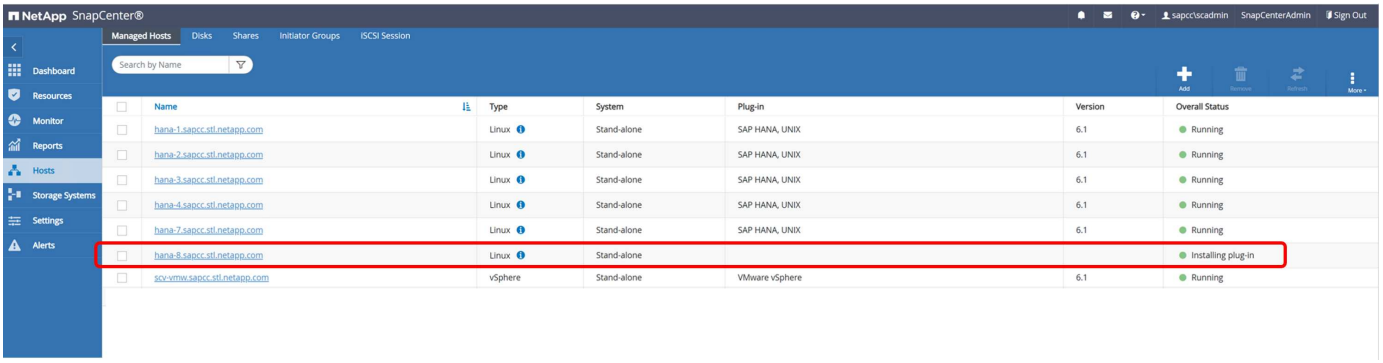
Bevor der Host in SnapCenter hinzugefügt werden kann, muss das SnapCenter Plug-in für VMware vSphere in der VMware Umgebung implementiert werden. Siehe auch "Implementieren Sie das SnapCenter Plug-in für VMware vSphere".

Die Anmeldeinformationen müssen während des Host-Add-Workflows festgelegt werden, wobei vSphere als Hosttyp ausgewählt werden kann.

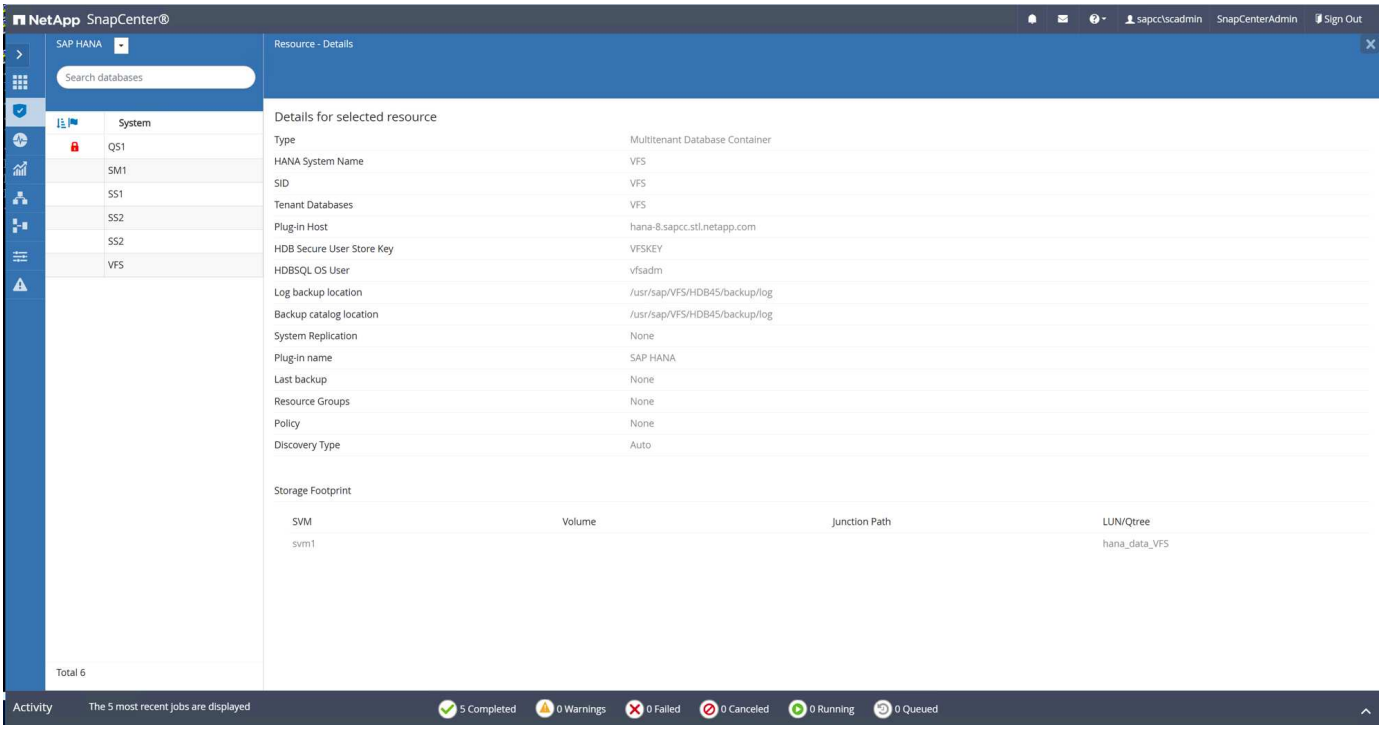


HANA-Host hinzufügen

Keine besonderen Anforderungen. Plugin-Bereitstellung und automatische Erkennung erfolgt wie gewohnt.



Mit dem automatischen Erkennungsprozess erkennt SnapCenter , dass die HANA-Ressource virtualisiert mit VMFS ausgeführt wird.

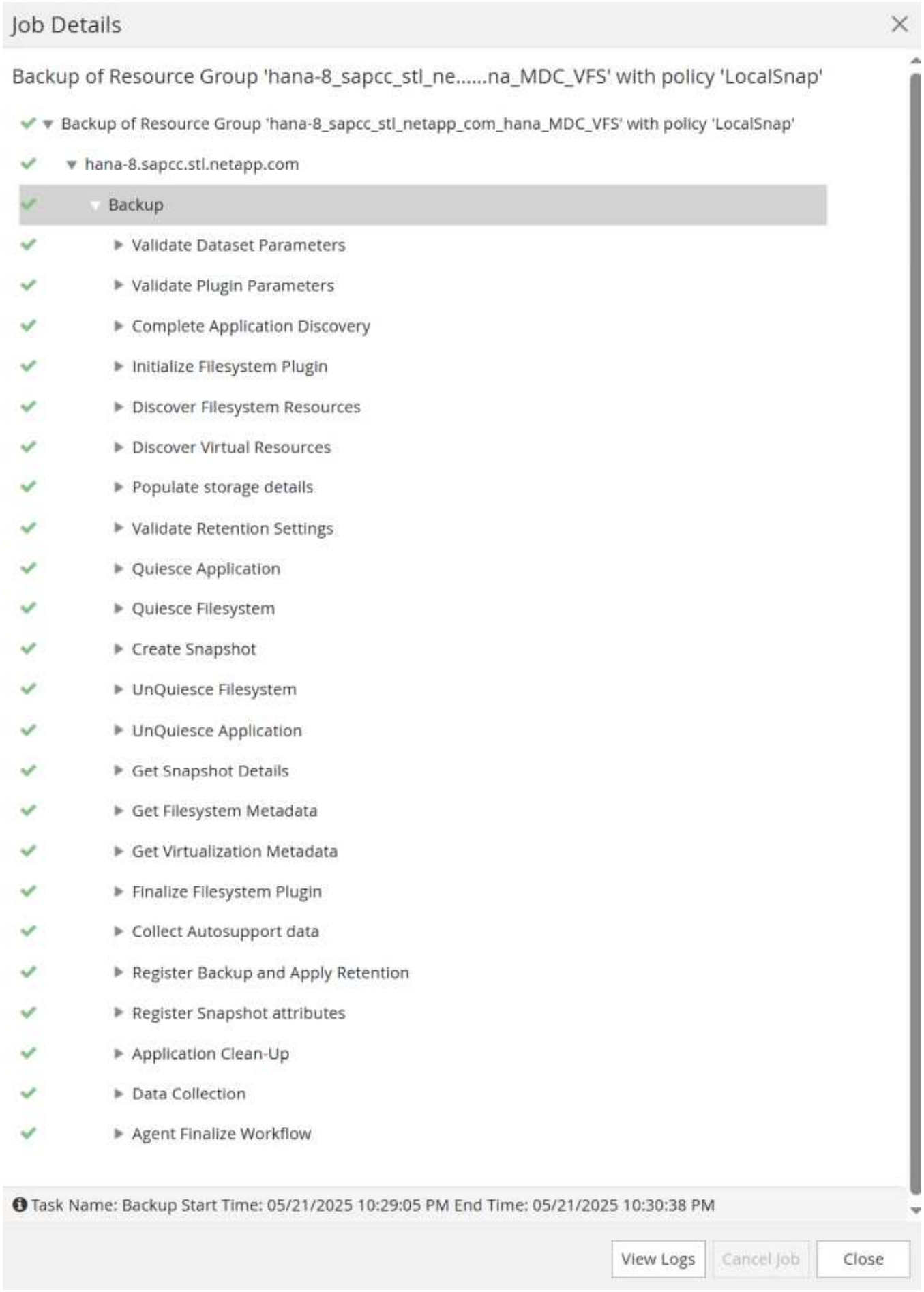


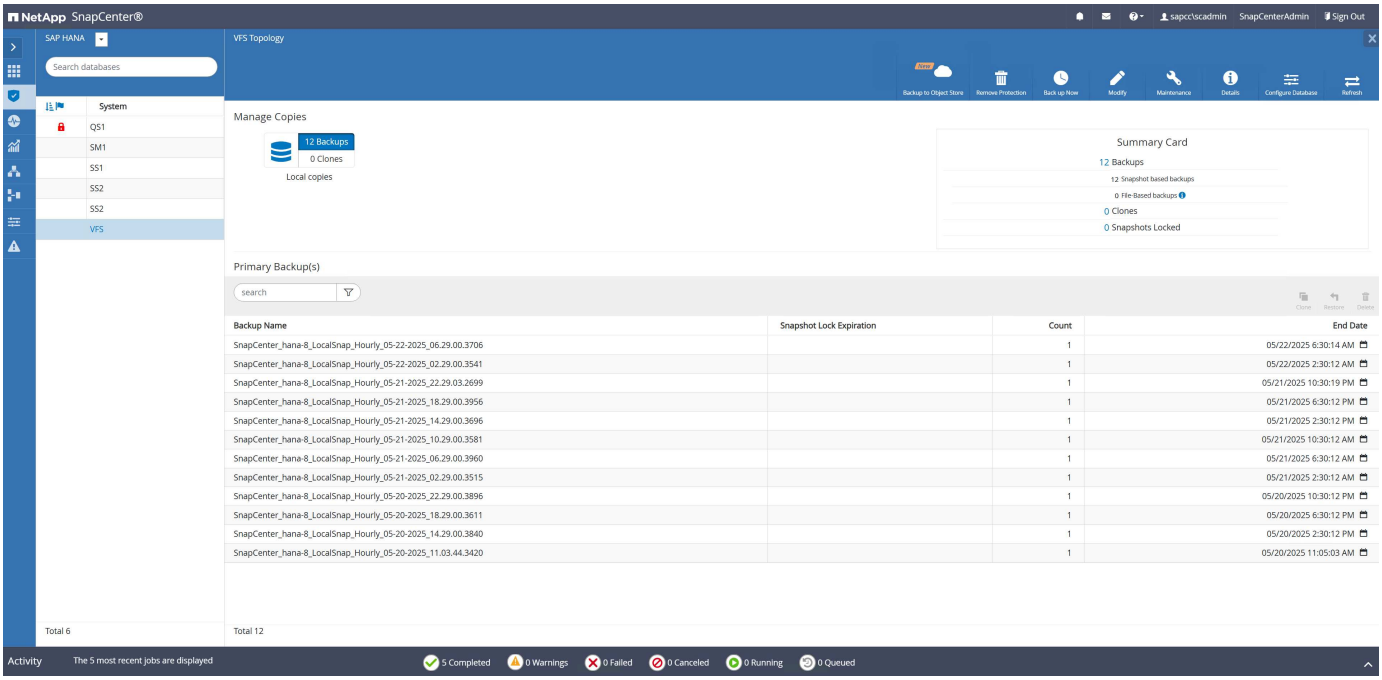
Konfiguration von Richtlinien und Ressourcenschutz

Nichts Spezifisches für VMware mit VMFS.

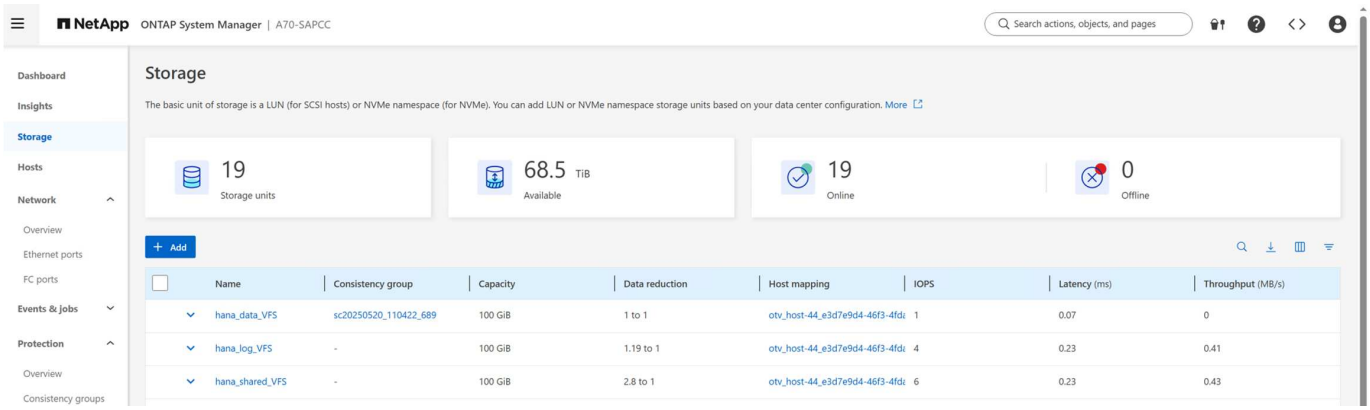
Backup-Vorgänge

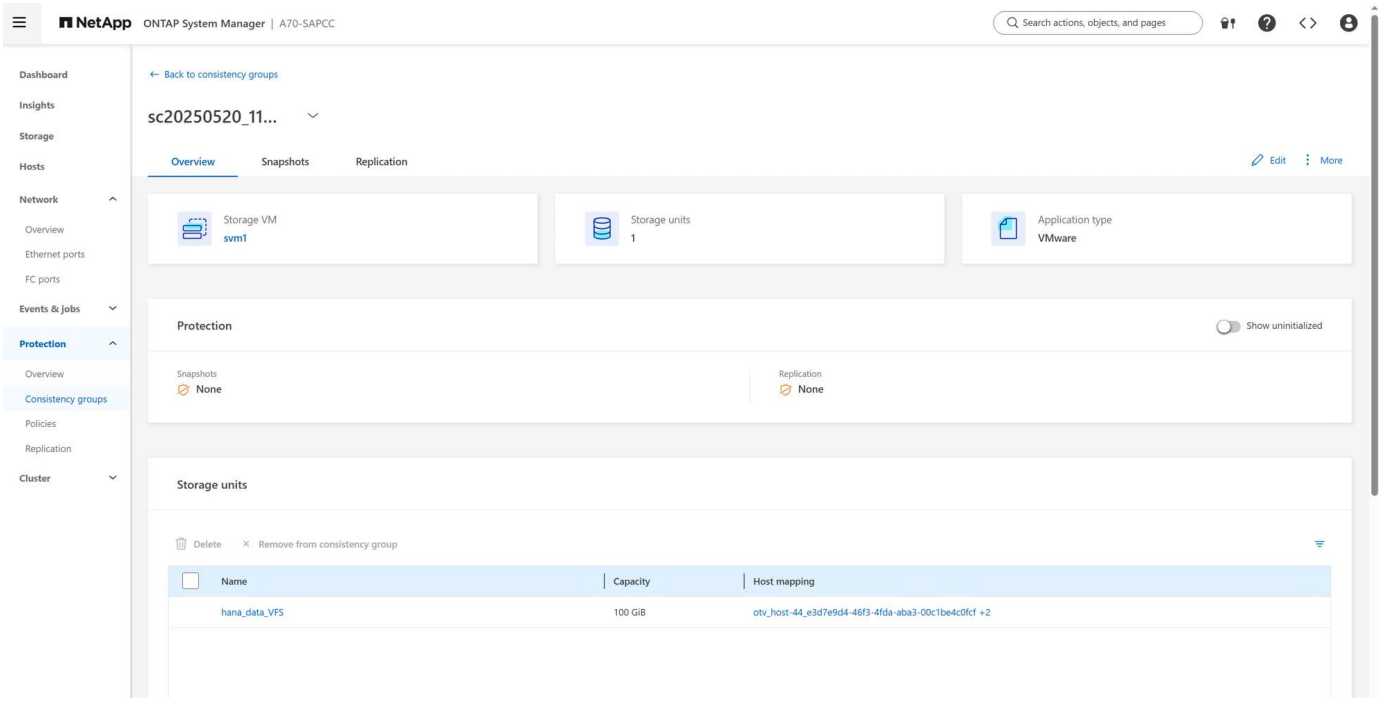
Nichts Spezifisches für VMware mit VMFS.

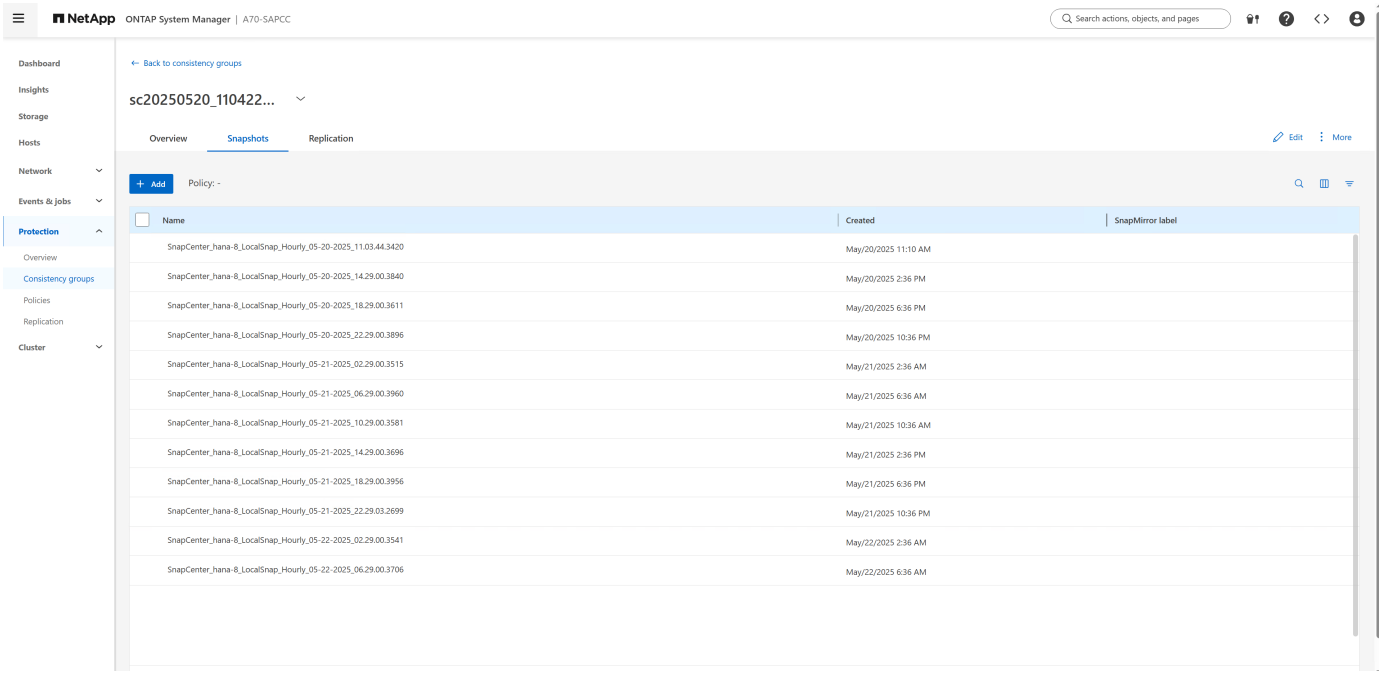

Job Details
Backup of Resource Group 'hana-8_sapcc_stl_ne.....na_MDC_VFS' with policy 'LocalSnap'
Backup of Resource Group 'hana-8_sapcc_stl_netapp_com_hana_MDC_VFS' with policy 'LocalSnap'
hana-8.sapcc.stl.netapp.com
Backup
Validate Dataset Parameters
Validate Plugin Parameters
Complete Application Discovery
Initialize Filesystem Plugin
Discover Filesystem Resources
Discover Virtual Resources
Populate storage details
Validate Retention Settings
Quiesce Application
Quiesce Filesystem
Create Snapshot
UnQuiesce Filesystem
UnQuiesce Application
Get Snapshot Details
Get Filesystem Metadata
Get Virtualization Metadata
Finalize Filesystem Plugin
Collect Autosupport data
Register Backup and Apply Retention
Register Snapshot attributes
Application Clean-Up
Data Collection
Agent Finalize Workflow
Task Name: Backup Start Time: 05/21/2025 10:29:05 PM End Time: 05/21/2025 10:30:38 PM
View Logs
Cancel Job
Close



SnapCenter erstellt eine Konsistenzgruppe (CG) und fügt der CG die Speichereinheit hana_data_VFS hinzu. Snapshots werden auf CG-Ebene erstellt.







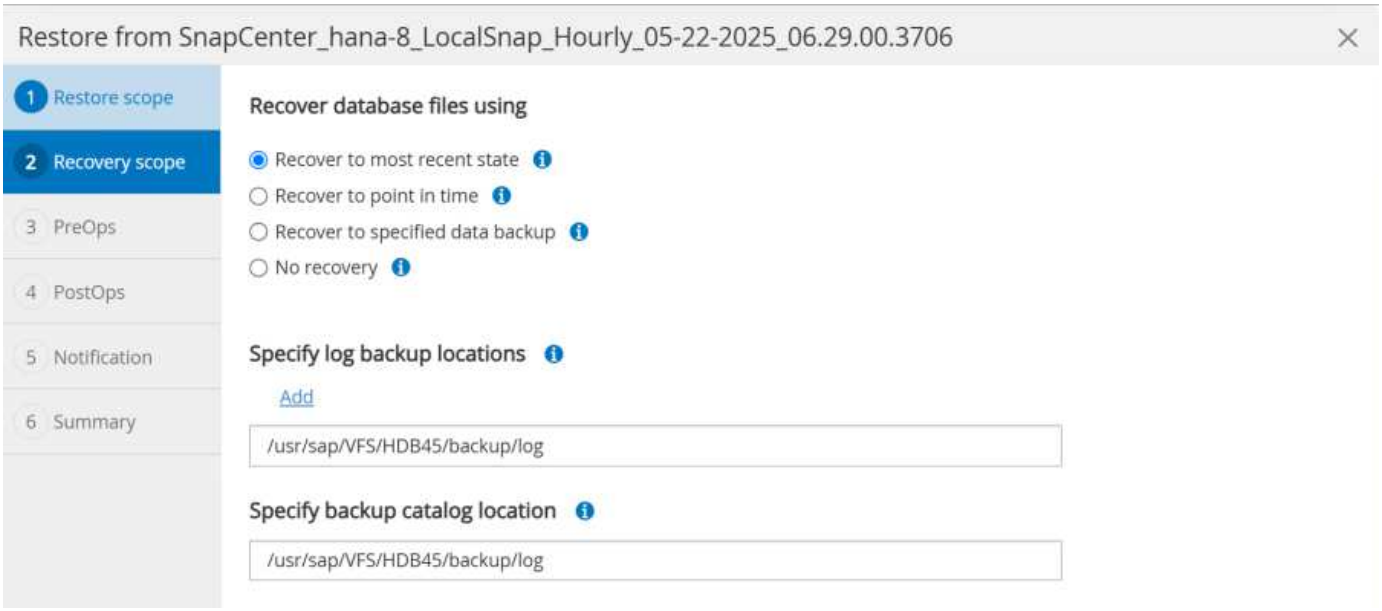
Restore- und Recovery-Vorgänge

Bei virtuellen Ressourcen, die auf dem SnapCenter von VMFS/VMDK gespeichert sind, werden Wiederherstellungsvorgänge immer durch einen Klon-, Mount- und Kopiervorgang durchgeführt.

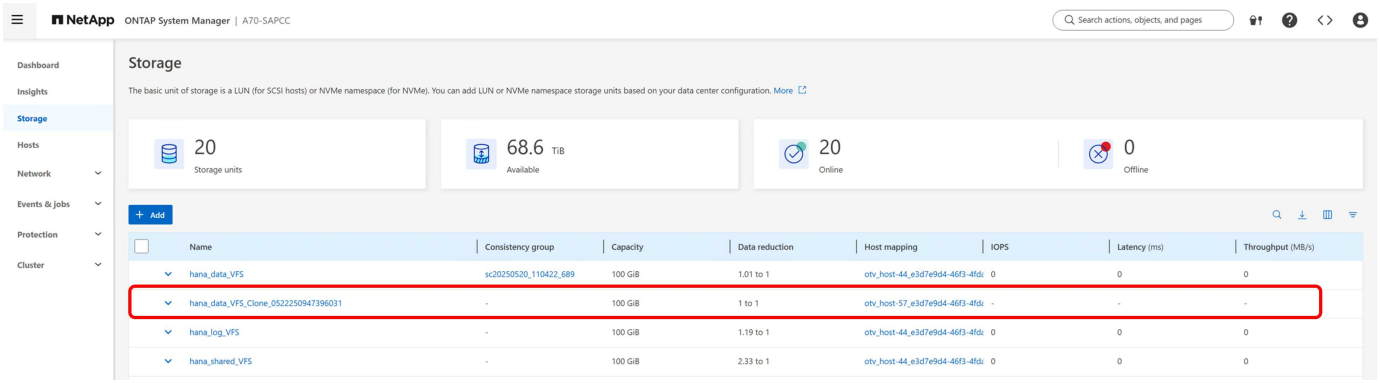
1. SnapCenter erstellt einen Speicherklon basierend auf dem ausgewählten Snapshot
2. SnapCenter mountet die LUN als neuen Datenspeicher auf dem ESX-Host
3. SnapCenter fügt die VMDK innerhalb des Datenspeichers der HANA-VM als neue Festplatte hinzu
4. SnapCenter bindet die neue Festplatte an das Linux Betriebssystem an
5. SnapCenter kopiert die Daten von der neuen Festplatte zurück in den ursprünglichen Speicherort

6. Wenn der Kopiervorgang abgeschlossen ist, werden alle oben genannten Ressourcen wieder entfernt
7. SnapCenter führt die Wiederherstellung der HANA-Systemdatenbank durch
8. SnapCenter führt die Wiederherstellung der HANA-Tenant-Datenbank durch

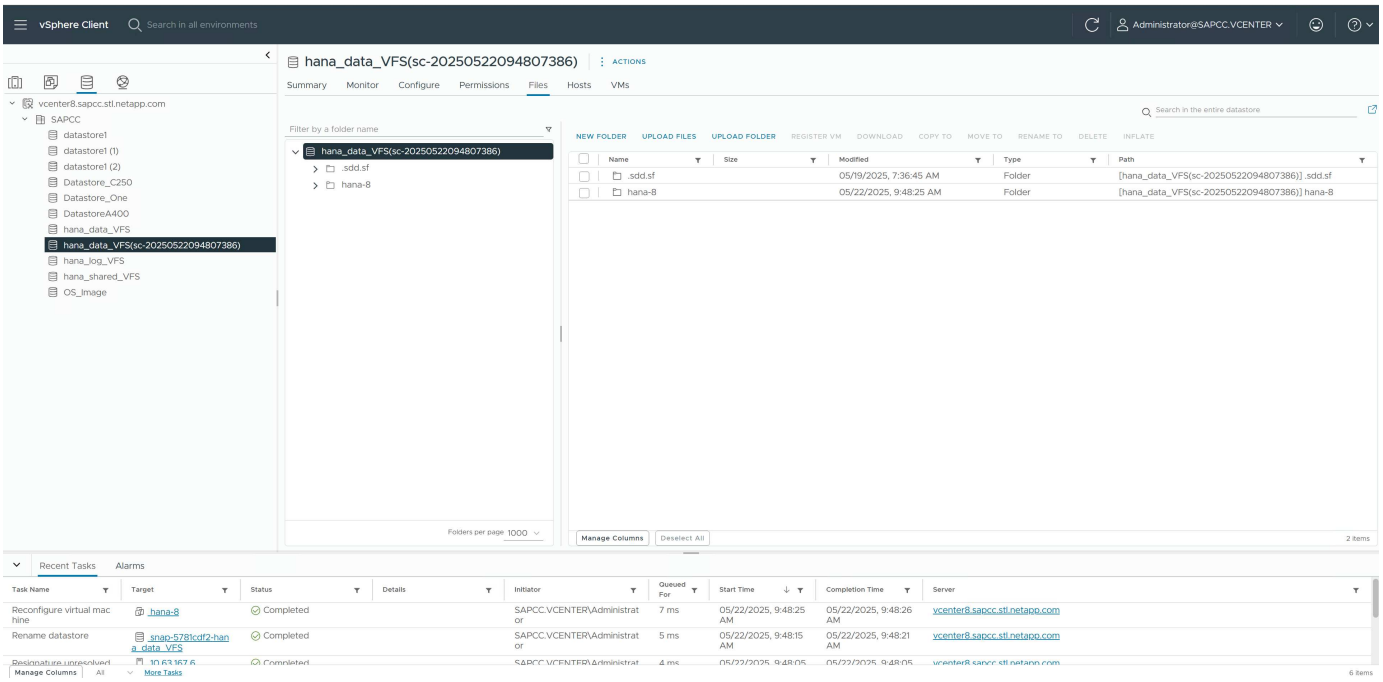
Die Gesamtlaufzeit des Wiederherstellungsvorgangs hängt von der Datenbankgröße und dem Durchsatz der FC-Verbindung zwischen den Storage-Clustern und den ESX-Hosts ab. In unserem Laboraufbau mit einer initialen HANA-Installation betrug die Laufzeit etwa 12 Minuten.



Während der Wiederherstellungsvorgang ausgeführt wird, können Sie eine neue geklonte Speichereinheit sehen.

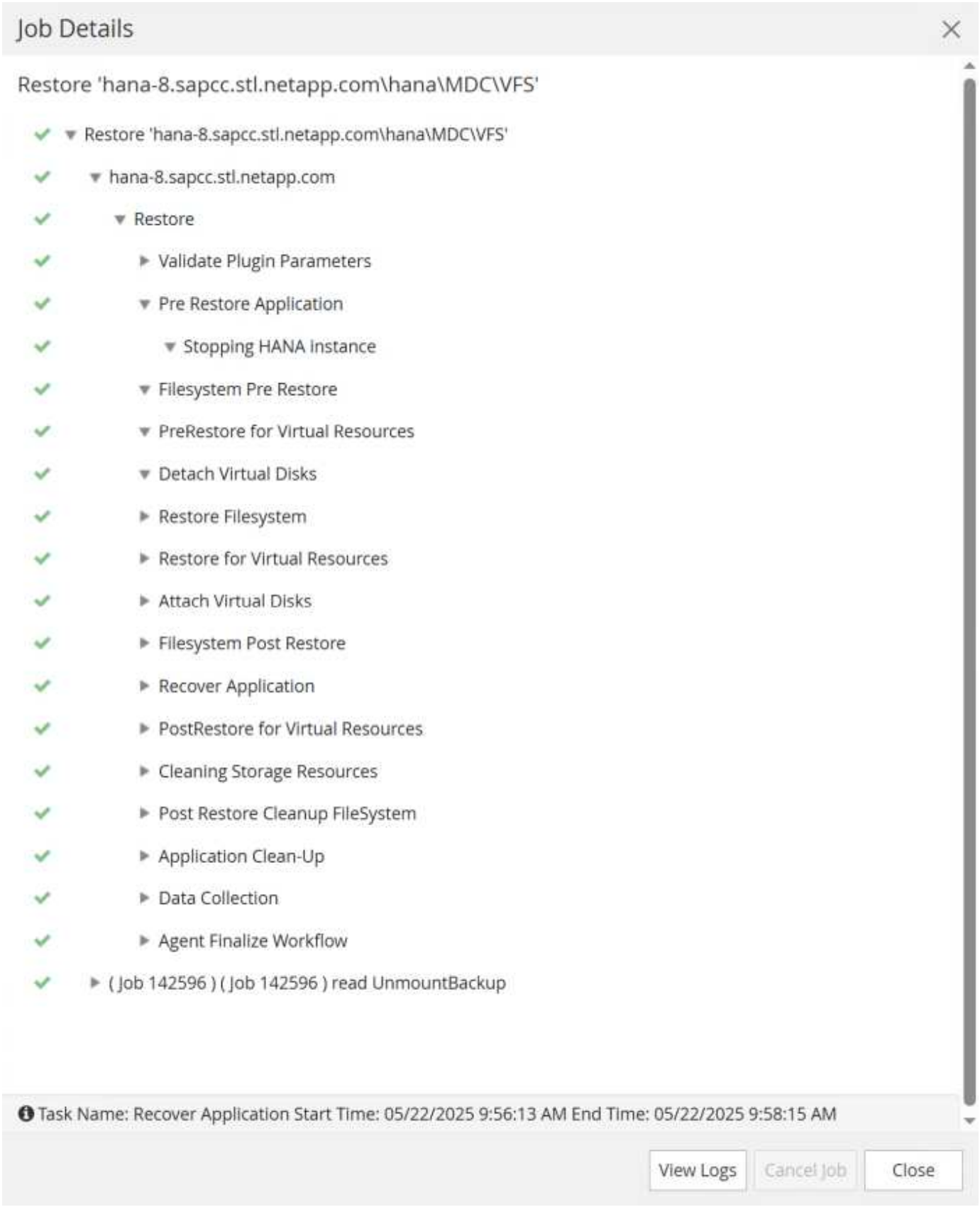


Die neue LUN (Datenspeicher) basierend auf der geklonten Speichereinheit wird an den ESX-Cluster angeschlossen.



Die VMDK im Datenspeicher wird der Ziel-HANA-VM zugeordnet und im HANA-System bereitgestellt.

```
hana-8:~ # df -h

Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 5.3G 54G 9% /
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 0 49G 0% /dev/shm
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 26M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysusers.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
/dev/mapper/system-root 60G 5.3G 54G 9% /.snapshots
/dev/mapper/system-root 60G 5.3G 54G 9% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 5.3G 54G 9% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 5.3G 54G 9% /home
/dev/mapper/system-root 60G 5.3G 54G 9% /opt
/dev/mapper/system-root 60G 5.3G 54G 9% /root
/dev/mapper/system-root 60G 5.3G 54G 9% /srv
/dev/mapper/system-root 60G 5.3G 54G 9% /usr/local
/dev/mapper/system-root 60G 5.3G 54G 9% /tmp
/dev/mapper/system-root 60G 5.3G 54G 9% /var
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/sdc 95G 8.9G 87G 10% /hana/log/VFS/mnt00001
/dev/sdb 95G 7.6G 88G 8% /hana/data/VFS/mnt00001
/dev/sdd 95G 15G 81G 16% /hana/shared
/dev/sda1 253M 5.9M 247M 3% /boot/efi
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
192.168.175.86:/sapcc_share 1.4T 858G 568G 61% /mnt/sapcc-share
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
/dev/sde 95G 9.2G 86G 10%
/var/opt/snapcenter/scu/clones/hana_data_VFS_mnt00001_142592_scu_clone_1

hana-8:~ #
```



SAP-Systemaktualisierung

Detaillierte Informationen zu SAP System Refresh-Operationen mit SnapCenter finden Sie unter "TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter" .

Das zweite HANA-System QFS wurde auf die gleiche Weise provisioniert wie im Kapitel "„Bereitstellung und Installation des HANA-Systems“" .

Voraussetzungen

Die aktuelle Version von SnapCenter (6.1P1) weist einige Einschränkungen auf, die mit den nächsten Versionen behoben werden sollen.

1. Es ist erforderlich, den SPL-Prozess nach jedem „Clone Create“- und „Clone Delete“-Workflow mit dem Befehl „systemctl restart spl“ auf dem Ziel-HANA-Host neu zu starten.
2. Die als Quelle und Ziel des SAP-Systemaktualisierungsvorgangs verwendeten HANA-VMs müssen auf demselben ESX-Host ausgeführt werden.

Workflow-Zusammenfassung

Bevor der erste SAP-Systemaktualisierungsvorgang ausgeführt werden kann, muss das HANA-Zielsystem installiert und der Host zu SnapCenter hinzugefügt werden. Anschließend muss das HANA-System heruntergefahren und der HANA-Datenträger vom Host getrennt werden.

SnapCenter Klon-Erstellungsworkflow

1. Speicherklon erstellen
2. Konfigurieren der Hostzuordnung für den Speicherklon
3. Speicherklon (Datenspeicher) an ESX-Host anhängen
4. Fügen Sie der HANA-Ziel-VM eine neue Festplatte aus dem Datenspeicher hinzu
5. Datenträger in HANA VM-Betriebssystem einbinden
6. Wiederherstellen des HANA-Systems mithilfe von Postscript

Laufzeit: 12 Minuten

> ⓘ Im Vergleich zum Wiederherstellungsvorgang ist die Laufzeit des Klonvorgangs unabhängig von der Größe der HANA-Datenbank. Die Laufzeit der Schritte 1 bis 5 ist auch bei sehr großen Datenbanken ähnlich. Die Wiederherstellung dauert bei größeren HANA-Systemen natürlich länger.

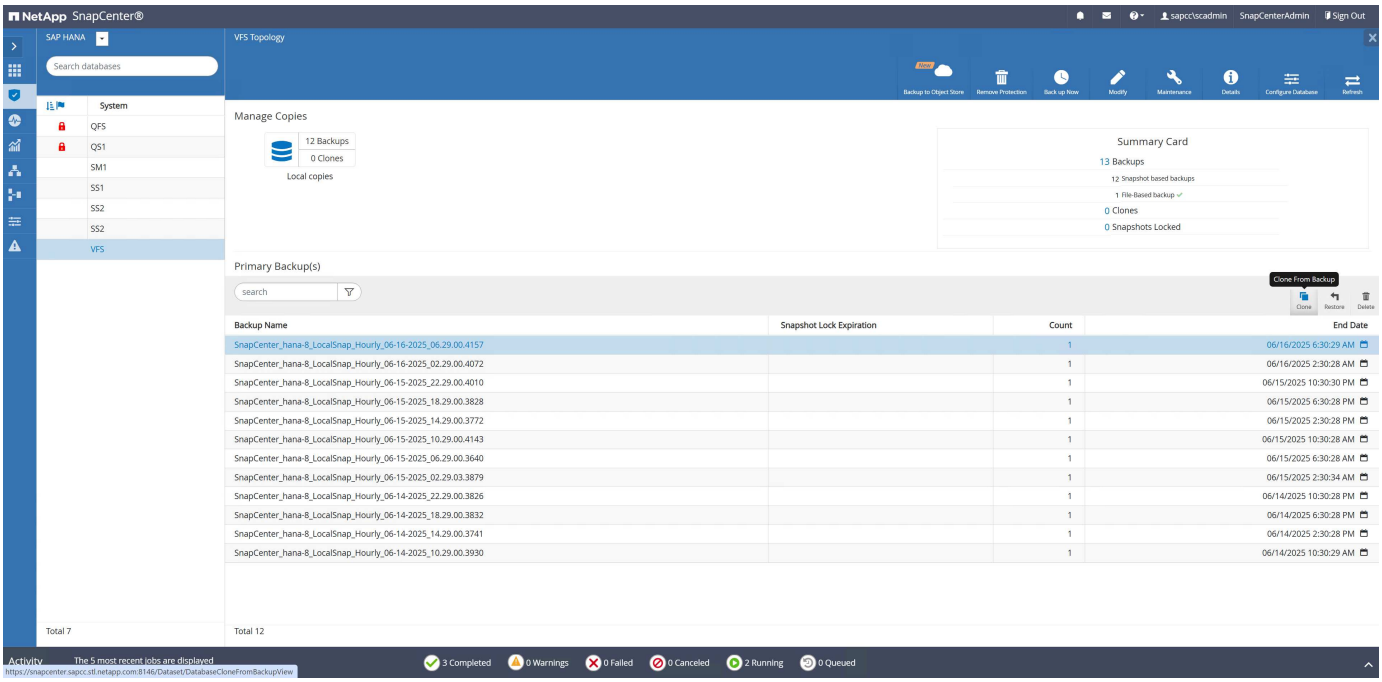
SnapCenter -Klon-Löschworkflow

1. Herunterfahren des HANA-Systems mithilfe eines vordefinierten Skripts
2. Datenträger vom HANA VM-Betriebssystem trennen
3. Datenträger aus HANA-VM entfernen
4. Entfernen des Datenspeichers vom ESX-Host
5. Storge-Klon löschen

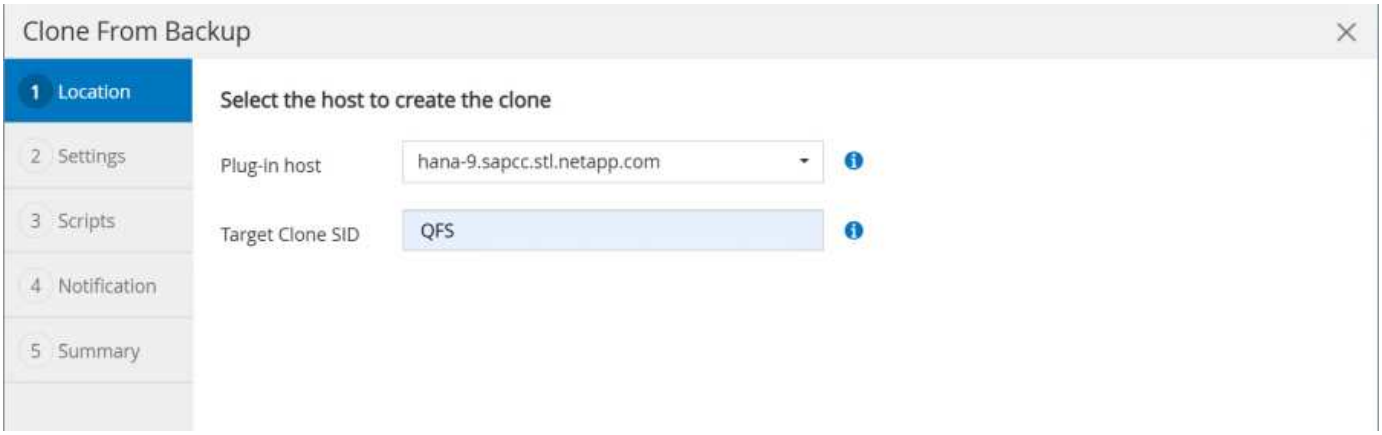
Laufzeit: 11 Minuten

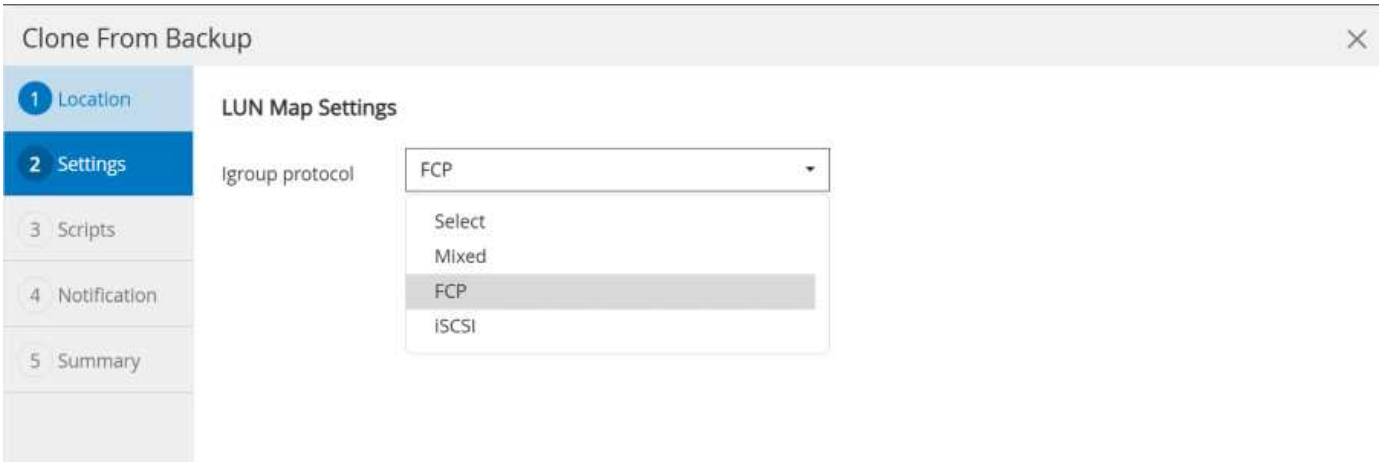
SnapCenter Klon-Erstellungsworkflow

Der Workflow zum Erstellen eines Klons wird durch Auswahl des gewünschten Snapshots und Klicken auf die Schaltfläche „Klonen“ gestartet.

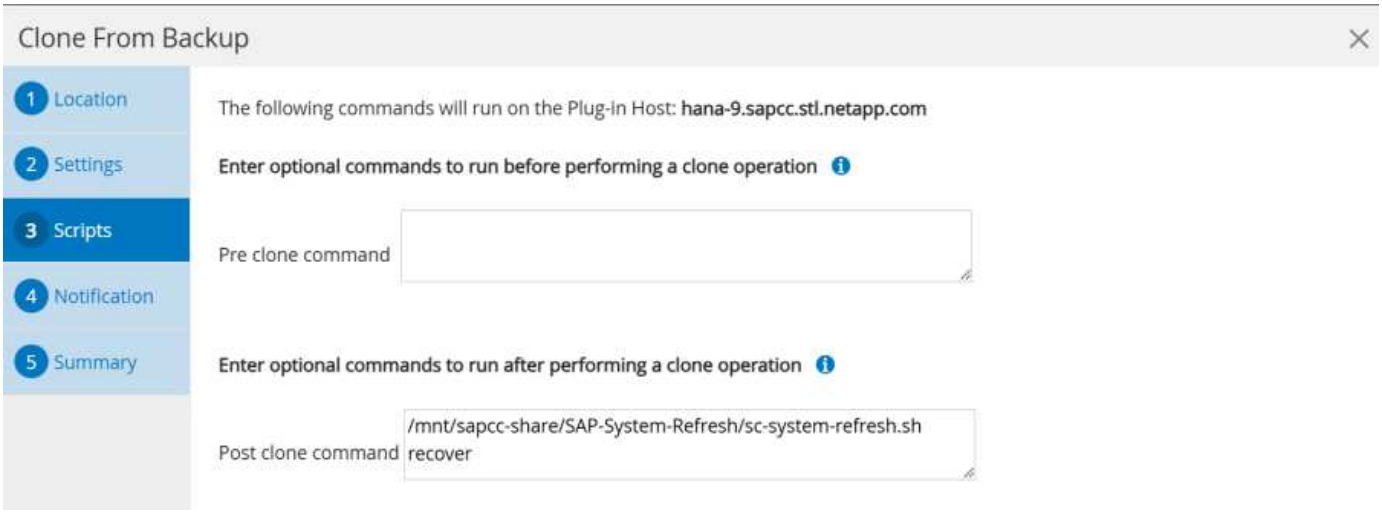


Der Zielhost und die SID müssen angegeben werden.

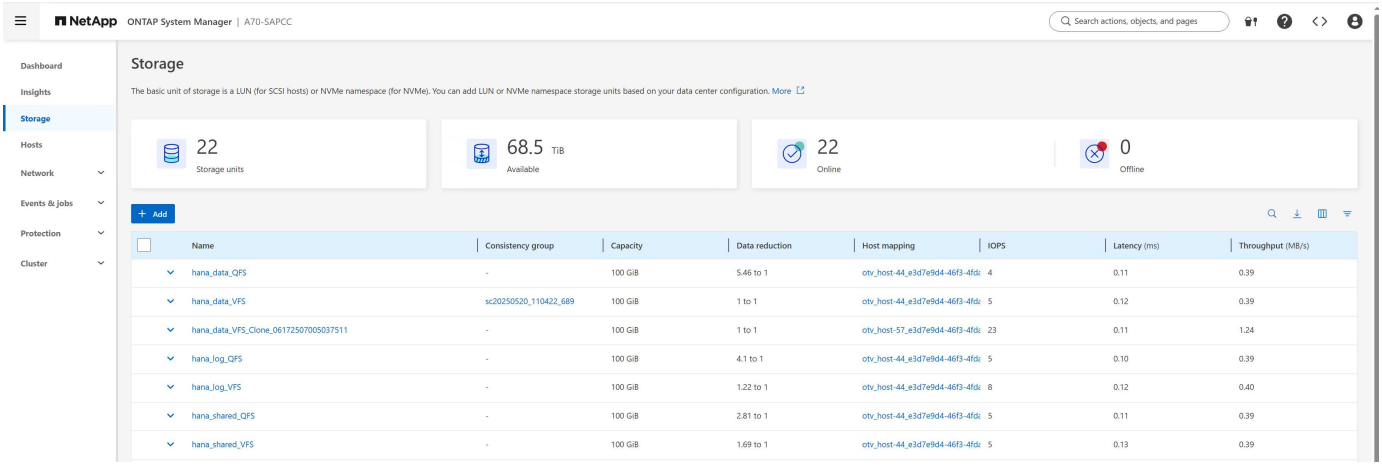




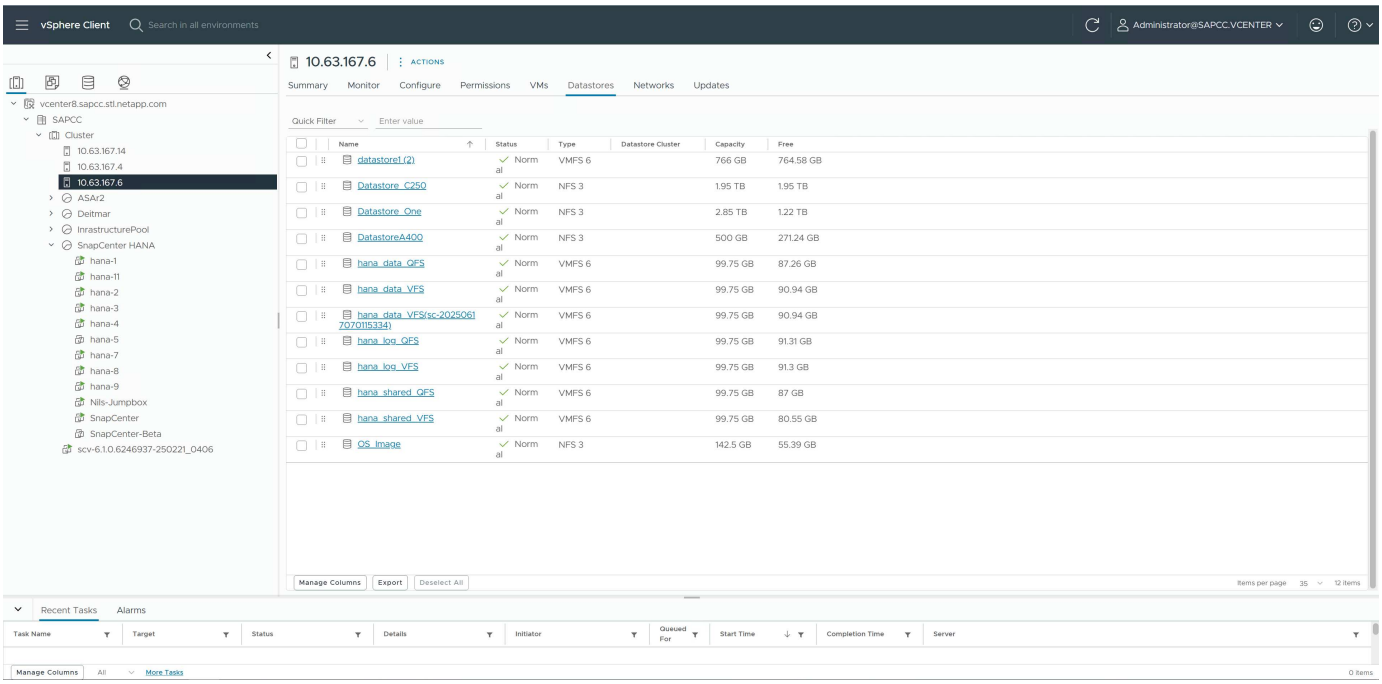
In unserem Beispiel verwenden wir ein Postskript, um die Wiederherstellung auf dem Zielhost auszuführen.



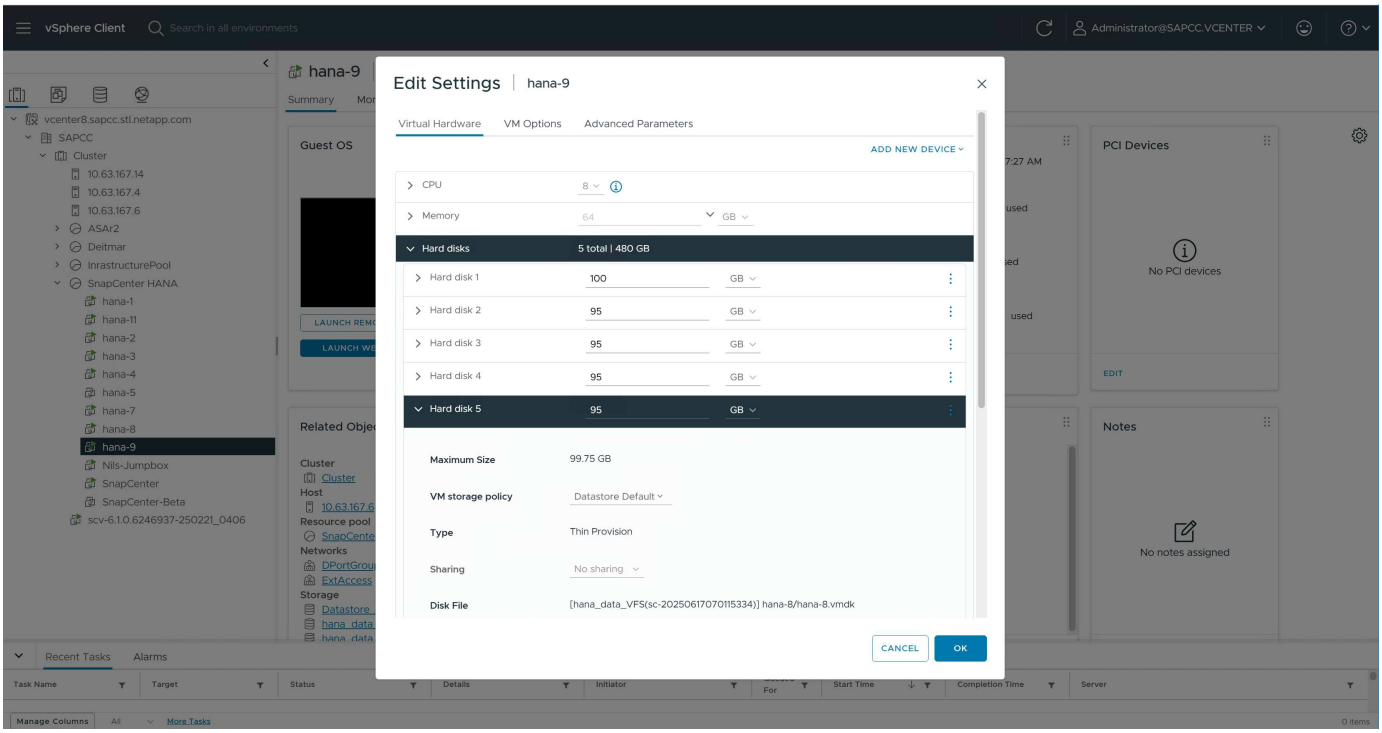
Wenn der Workflow gestartet wird, erstellt SnapCenter eine geklonte Speichereinheit basierend auf dem ausgewählten Snapshot.



SnapCenter verbindet dann die LUN (Datenspeicher) mit dem ESX-Host, auf dem die Ziel-HANA-VM ausgeführt wird.



Das VMDK im neuen Datenspeicher wird dann zur HANA-VM hinzugefügt.



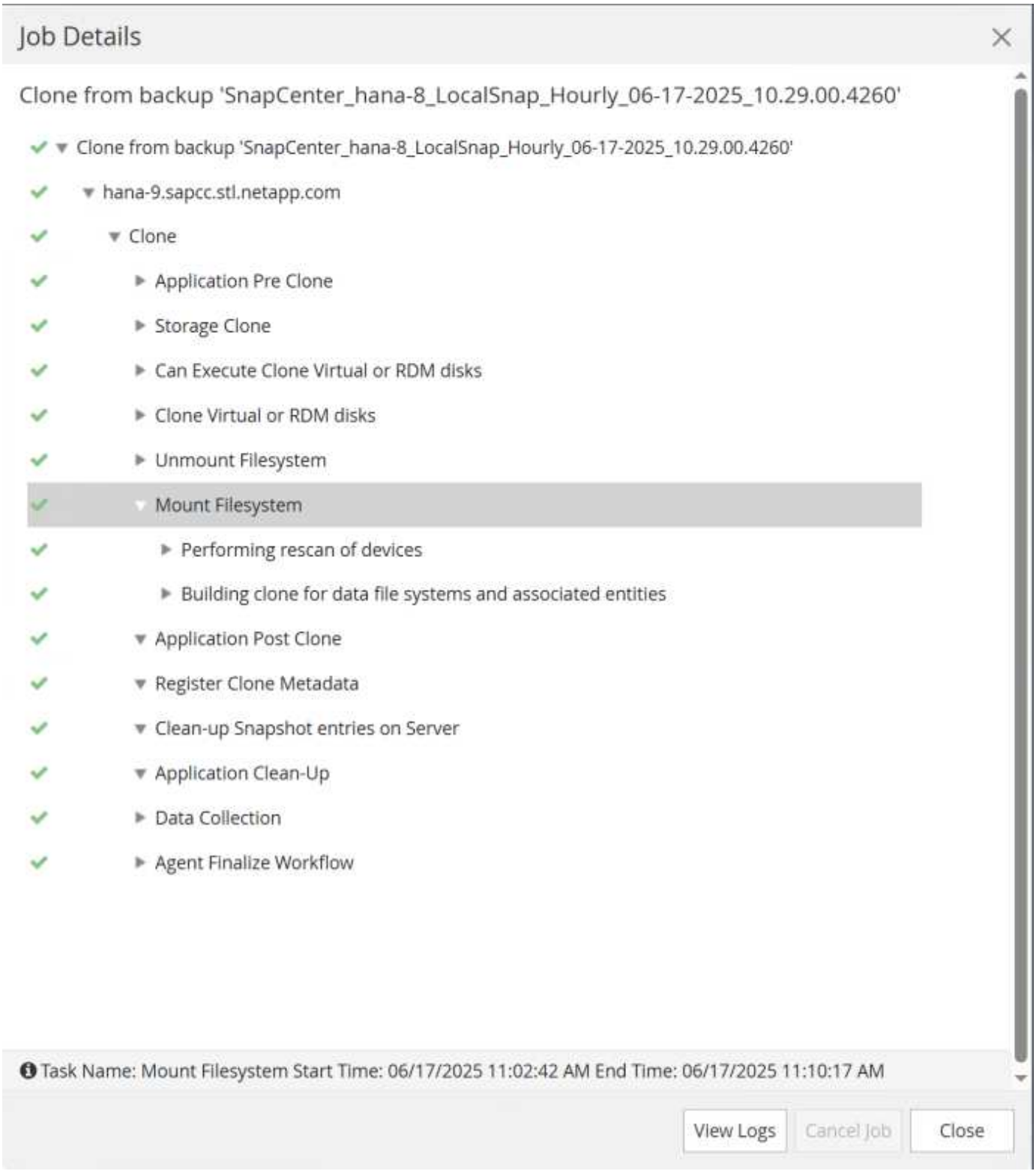
Anschließend konfiguriert und mountet SnapCenter die neue Festplatte im HANA-Linux-System.

```
hana-9:/mnt/sapcc-share/SAP-System-Refresh # df -h

Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 5.2G 52G 10% /
devtmpfs 4.0M 4.0K 4.0M 1% /dev
tmpfs 49G 0 49G 0% /dev/shm
```

```
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 26M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysusers.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
/dev/mapper/system-root 60G 5.2G 52G 10% /.snapshots
/dev/mapper/system-root 60G 5.2G 52G 10% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 5.2G 52G 10% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 5.2G 52G 10% /home
/dev/mapper/system-root 60G 5.2G 52G 10% /opt
/dev/mapper/system-root 60G 5.2G 52G 10% /srv
/dev/mapper/system-root 60G 5.2G 52G 10% /root
/dev/mapper/system-root 60G 5.2G 52G 10% /tmp
/dev/mapper/system-root 60G 5.2G 52G 10% /usr/local
/dev/mapper/system-root 60G 5.2G 52G 10% /var
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/sdc 95G 8.9G 87G 10% /hana/log/QFS/mnt00001
/dev/sdd 95G 14G 82G 14% /hana/shared
/dev/sda1 253M 5.9M 247M 3% /boot/efi
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
192.168.175.86:/sapcc++_++share 1.4T 858G 568G 61% /mnt/sapcc-share
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
/dev/sde 95G 9.2G 86G 10% /hana/data/QFS/mnt00001
tmpfs 6.3G 56K 6.3G 1% /run/user/1001
hana-9:/mnt/sapcc-share/SAP-System-Refresh #

hana-9:/mnt/sapcc-share/SAP-System-Refresh # cat /etc/fstab
/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=/@/var 0 0
/dev/system/root /usr/local btrfs subvol=/@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=/@/tmp 0 0
/dev/system/root /srv btrfs subvol=/@/srv 0 0
/dev/system/root /root btrfs subvol=/@/root 0 0
/dev/system/root /opt btrfs subvol=/@/opt 0 0
/dev/system/root /home btrfs subvol=/@/home 0 0
/dev/system/root /boot/grub2/x86++_++64-efi btrfs
subvol=/@/boot/grub2/x86++_++64-efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=/@/.snapshots 0 0
UUID=FB79-24DC /boot/efi vfat utf8 0 2
```

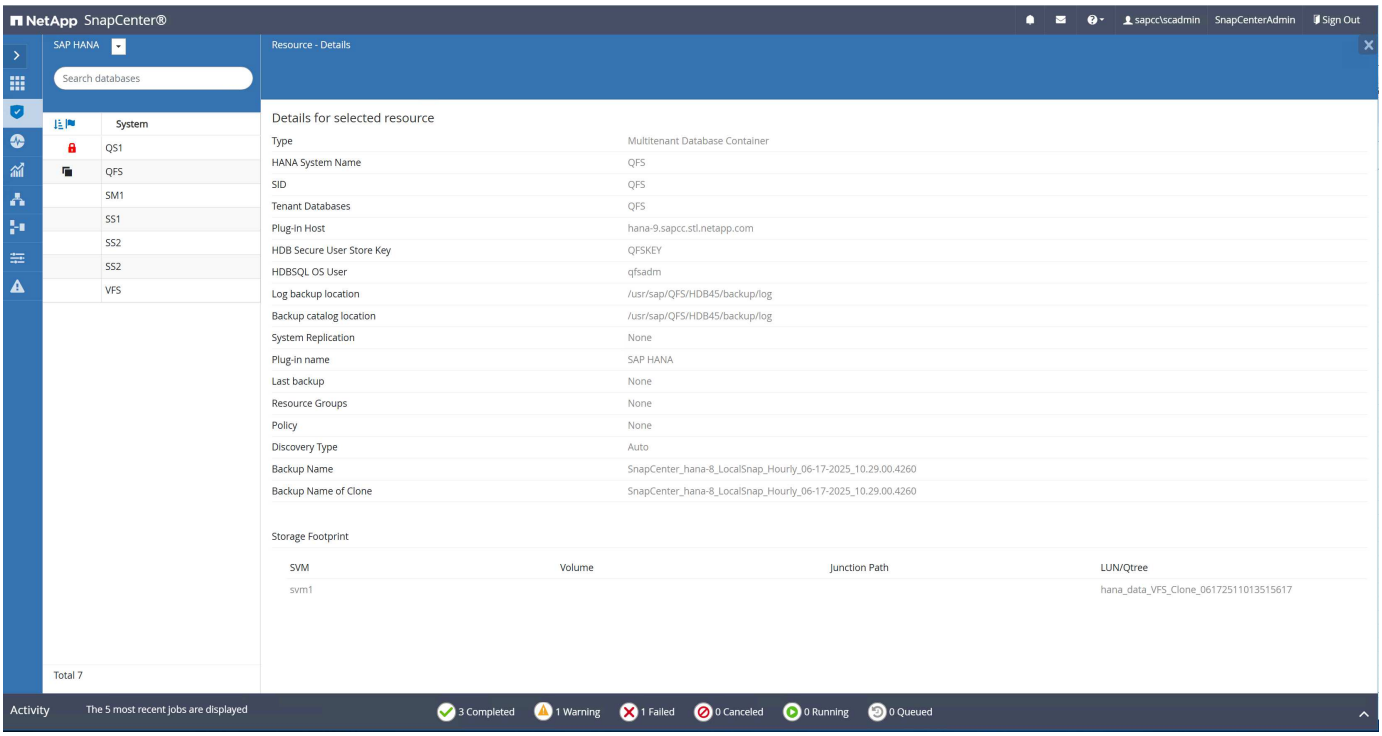
```
192.168.175.86:/sapcc++_++share /mnt/sapcc-share nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
#/dev/sdb /hana/data/QFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/QFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
# The following entry has been added by NetApp (SnapCenter Plug-in for
UNIX)
/dev/sde /hana/data/QFS/mnt00001 xfs
rw,relatime,attr2,inode64,logbufs=8,logbsize=32k,noquota 0 0
hana-9:/mnt/sapcc-share/SAP-System-Refresh #
```

Der folgende Screenshot zeigt die von SnapCenter ausgeführten Jobschritte.



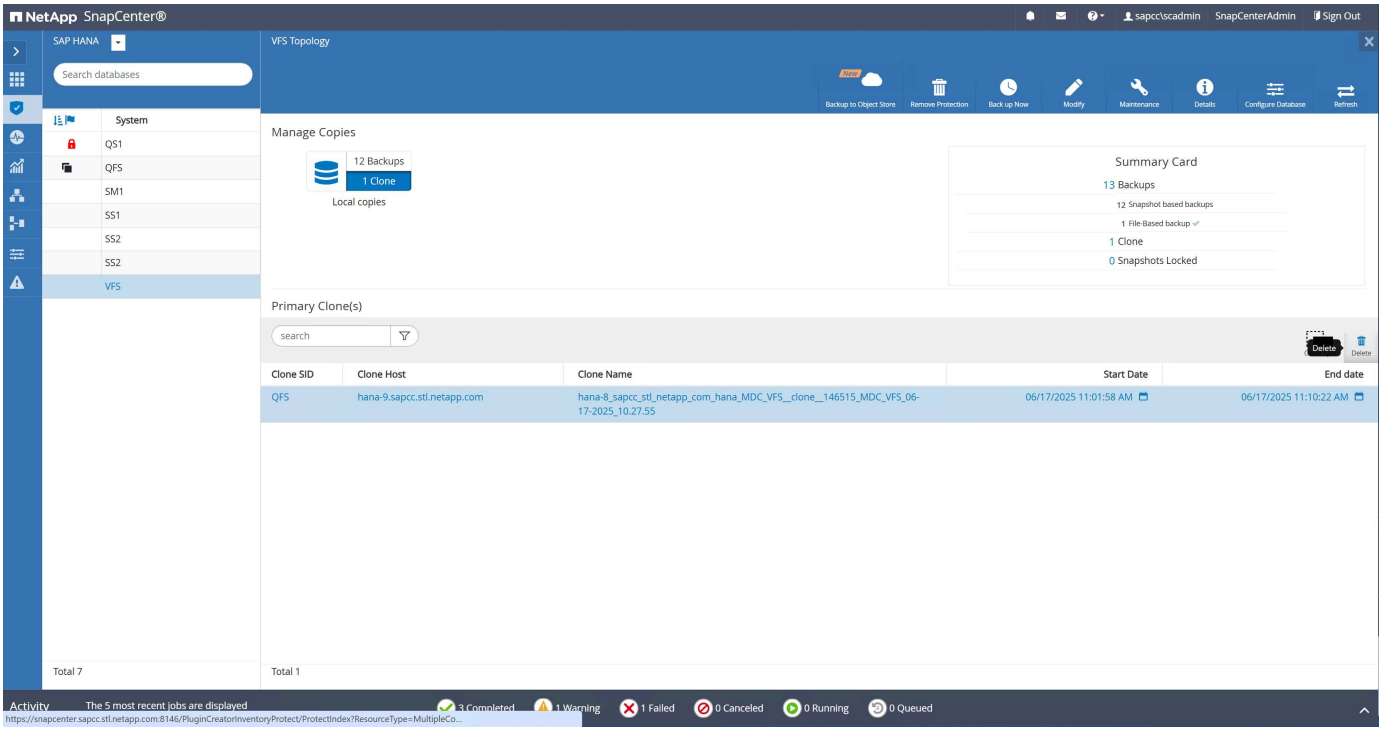
Wie im Abschnitt „Voraussetzungen“ erwähnt, muss der SnapCenter -SPL-Dienst auf dem HANA-Host mit dem Befehl „systemctl restart spl“ neu gestartet werden, um die ordnungsgemäße Bereinigung einzuleiten. Dies muss nach Abschluss des Auftrags erfolgen.

Sobald der Klon-Workflow abgeschlossen ist, kann die automatische Erkennung durch Klicken auf das Ressourcen-QFS gestartet werden. Sobald der automatische Erkennungsprozess abgeschlossen ist, wird der neue Speicherbedarf in der Detailansicht der Ressource angezeigt.

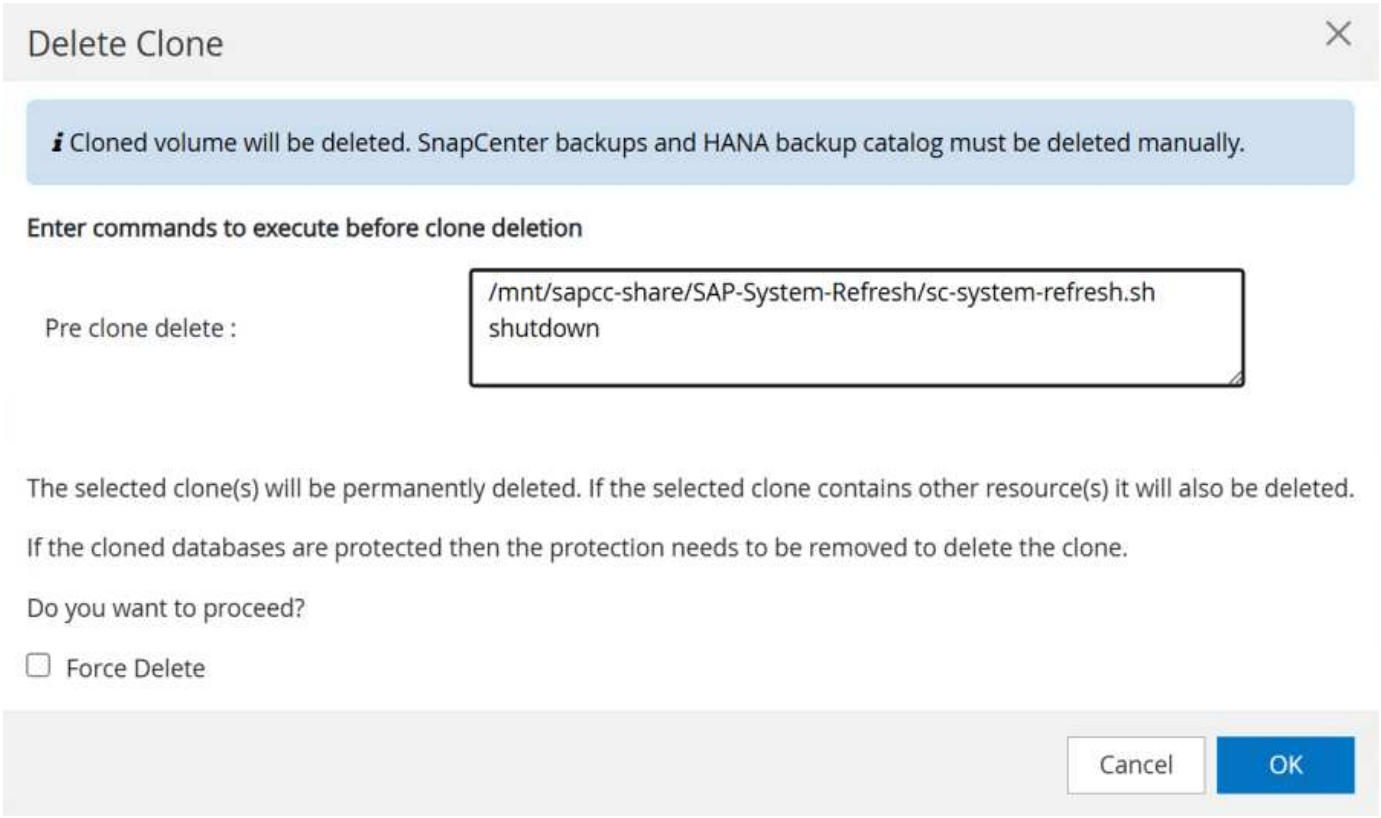


SnapCenter -Klon-Löschworkflow

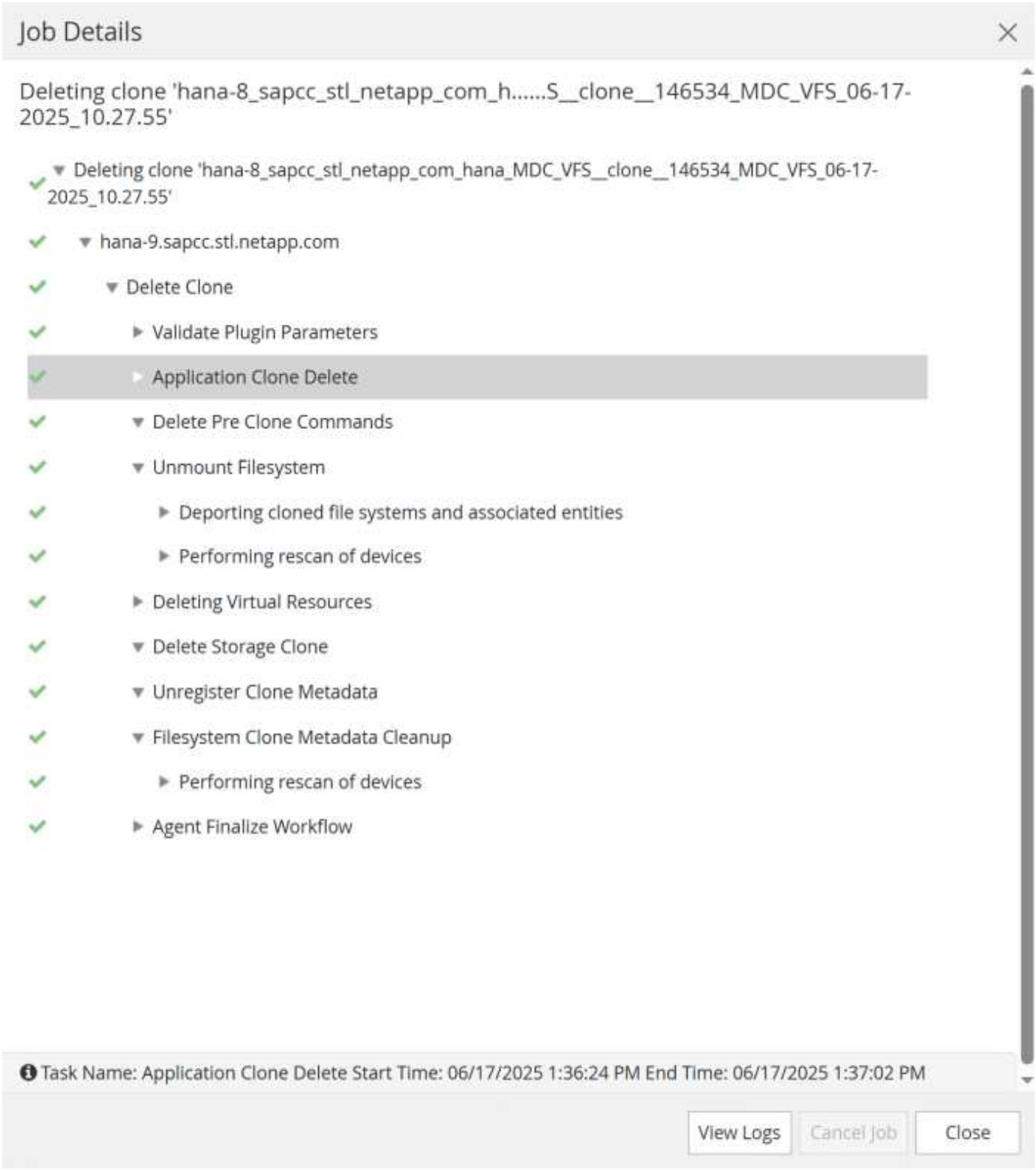
Der Klonlösch-Workflow wird gestartet, indem Sie den Klon bei der HANA-Quellressource auswählen und auf die Schaltfläche „Löschen“ klicken.



In unserem Beispiel verwenden wir ein Vorskript, um die Ziel-HANA-Datenbank herunterzufahren.



Der folgende Screenshot zeigt die von SnapCenter ausgeführten Jobschritte.



Wie im Abschnitt „Voraussetzungen“ erwähnt, muss der SnapCenter -SPL-Dienst auf dem HANA-Host mit dem Befehl „systemctl restart spl“ neu gestartet werden, um eine ordnungsgemäße Bereinigung einzuleiten.

Zusätzliche Informationen und Versionsverlauf

Bewährte Methoden für HANA:

- "Technischer Bericht: SAP HANA on NetApp ASA Systems with Fibre Channel Protocol".

SnapCenter

- "Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter"
- "TR-4719: SAP HANA System Replication – Backup und Recovery mit SnapCenter"
- "TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"
- "SAP HANA-Datenschutz und hohe Verfügbarkeit mit SnapCenter SnapMirror Active Sync und VMware Metro Storage Cluster"
- "SnapCenter-Softwaredokumentation"

Versionsverlauf:

Version	Datum	Kommentar
Version 1.0	07/2025	Ausgangsversion

SAP HANA System Replication Backup und Recovery mit SnapCenter

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

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

Autor: Nils Bauer, NetApp

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

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

Hochverfügbarkeit ohne RPO und mit minimalem RTO-Aufwand

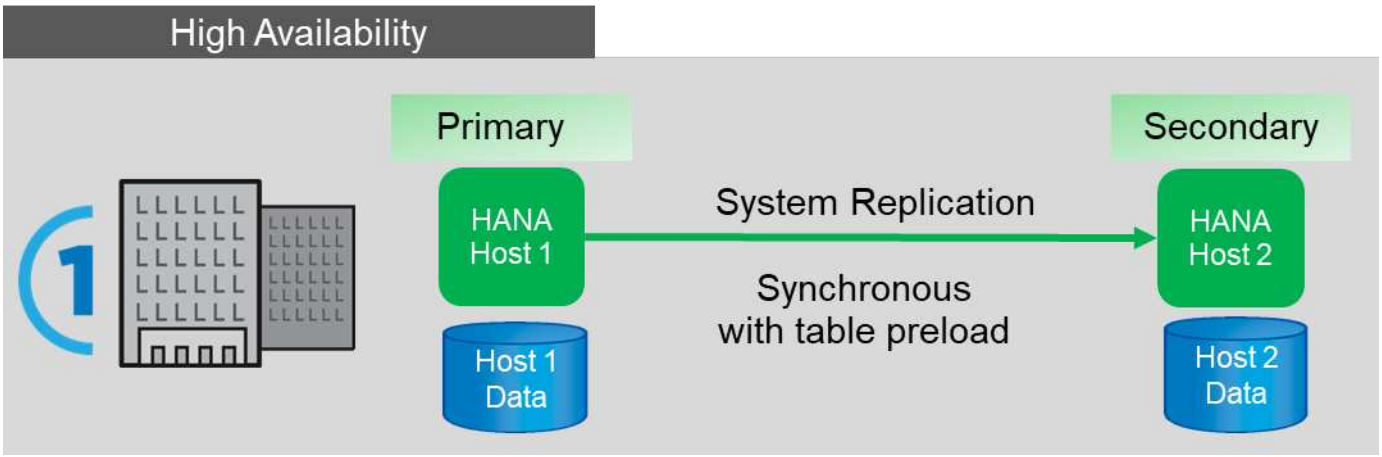
System Replication ist mit synchroner Replizierung konfiguriert und verwendet Tabellen, die auf dem sekundären SAP HANA-Host vorab in den Speicher geladen sind. Diese Hochverfügbarkeitslösung lässt sich bei Hardware- oder Softwareausfällen einsetzen und reduziert zudem geplante Ausfallzeiten während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

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

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

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

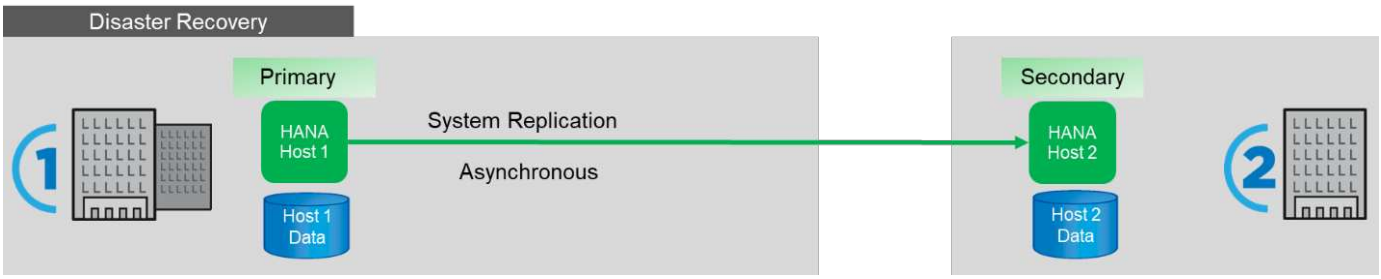
als Hochverfügbarkeitslösung.



Disaster Recovery über große Entfernungen

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

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



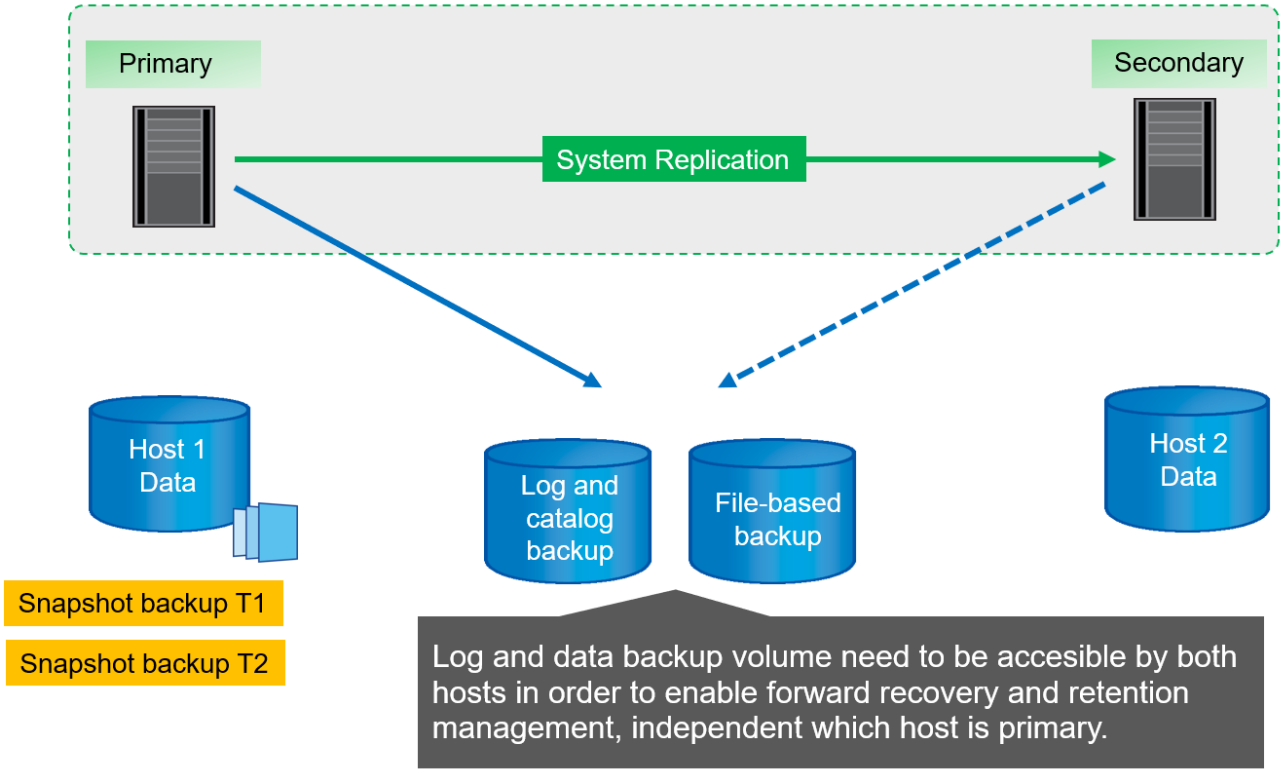
Storage Snapshot Backups und SAP System Replication

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

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

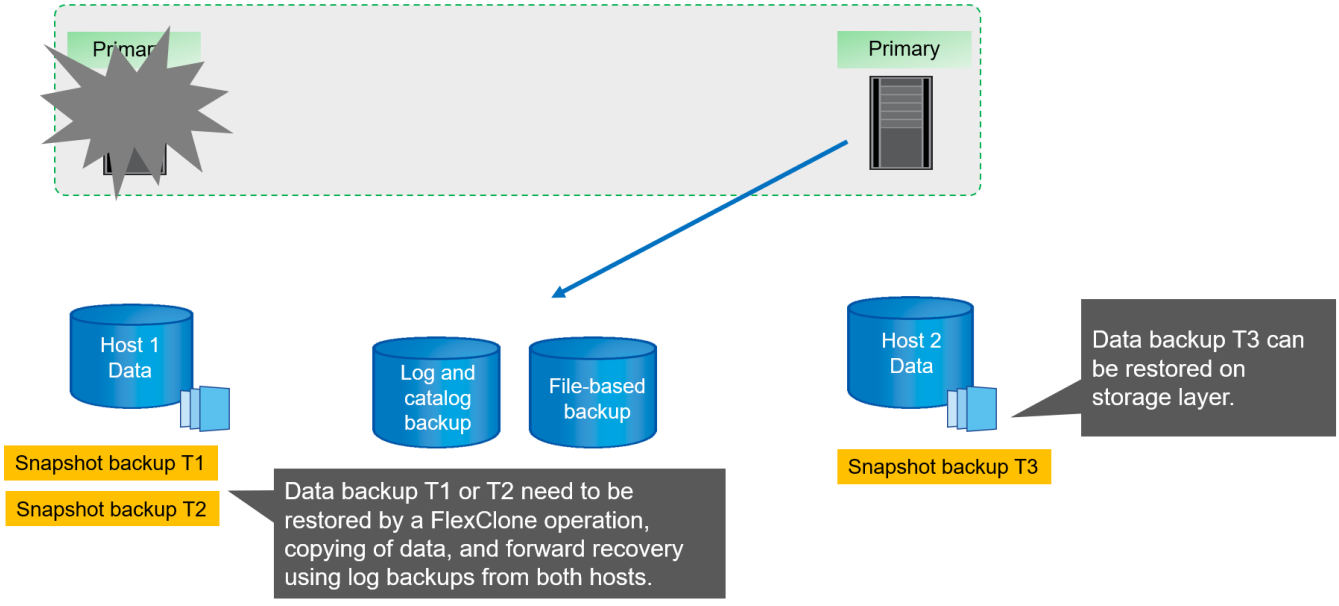
Da jedes Backup für die Wiederherstellung verwendet und mithilfe von Log-Backups von beiden Hosts durchgeführt werden kann, ist ein gemeinsamer Backup-Ort für Protokolle erforderlich, auf den von beiden Hosts zugegriffen werden kann. NetApp empfiehlt die Verwendung eines Shared Storage Volume. Sie sollten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

Jeder SAP HANA-Host verfügt über ein eigenes Storage-Volume. Wenn Sie einen Storage-basierten Snapshot für ein Backup verwenden, wird ein Datenbank-konsistenter Snapshot auf dem Speicher-Volume des primären SAP HANA-Hosts erstellt.



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

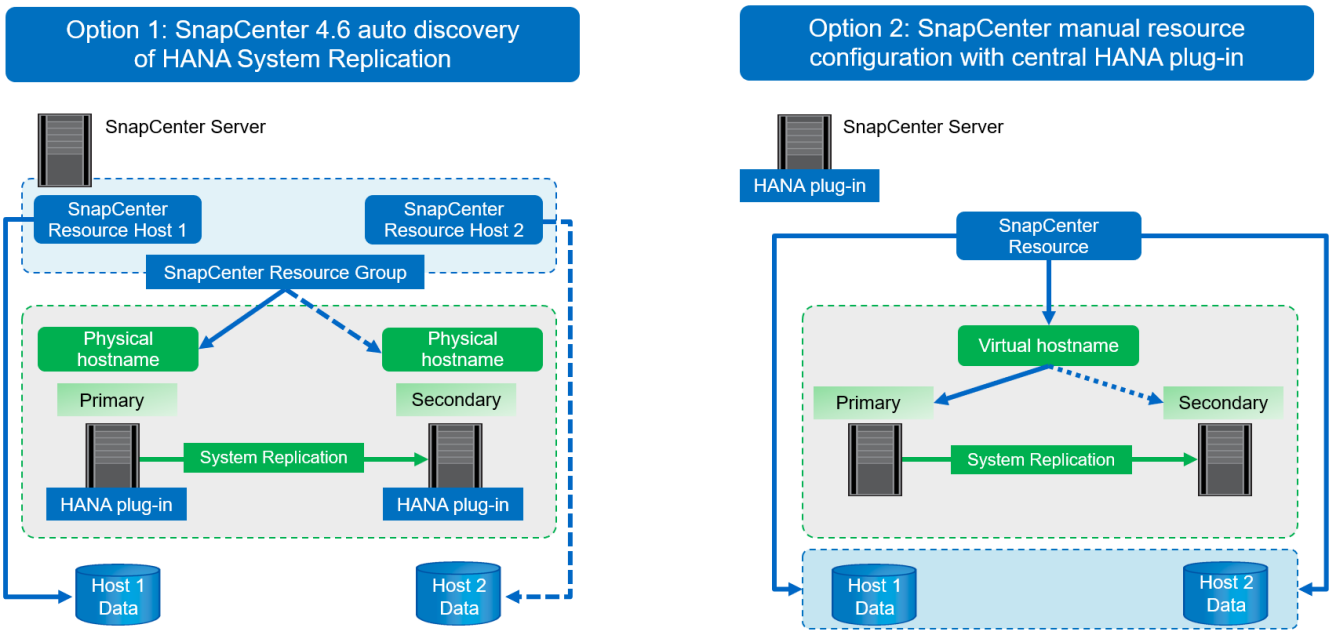
Das auf Host 2 erstellte Backup kann direkt auf der Speicherebene wiederhergestellt werden. Wenn Sie ein Backup verwenden müssen, das auf Host 1 erstellt wurde, muss das Backup vom Host-1-Speicher-Volume auf das Host-2-Speicher-Volume kopiert werden. Die vorwärts-Wiederherstellung verwendet die Protokoll-Backups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



SnapCenter Konfigurationsoptionen für SAP System Replication

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

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



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

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

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

	Ressourcengruppe mit SnapCenter 4.6	**Einzelne SnapCenter-Ressource und virtuelle IP-Adresse**
Backup-Vorgang (Snapshot und dateibasiert)	Automatische Identifizierung des primären Hosts in der Ressourcengruppe	Virtuelle IP-Adresse automatisch verwenden

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

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

Die beiden Optionen werden in den folgenden Abschnitten näher erläutert.

Konfiguration von SnapCenter 4.6 unter Verwendung einer Ressourcengruppe

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

SnapCenter 4.6-Konfiguration von HANA System Replication-Umgebungen

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

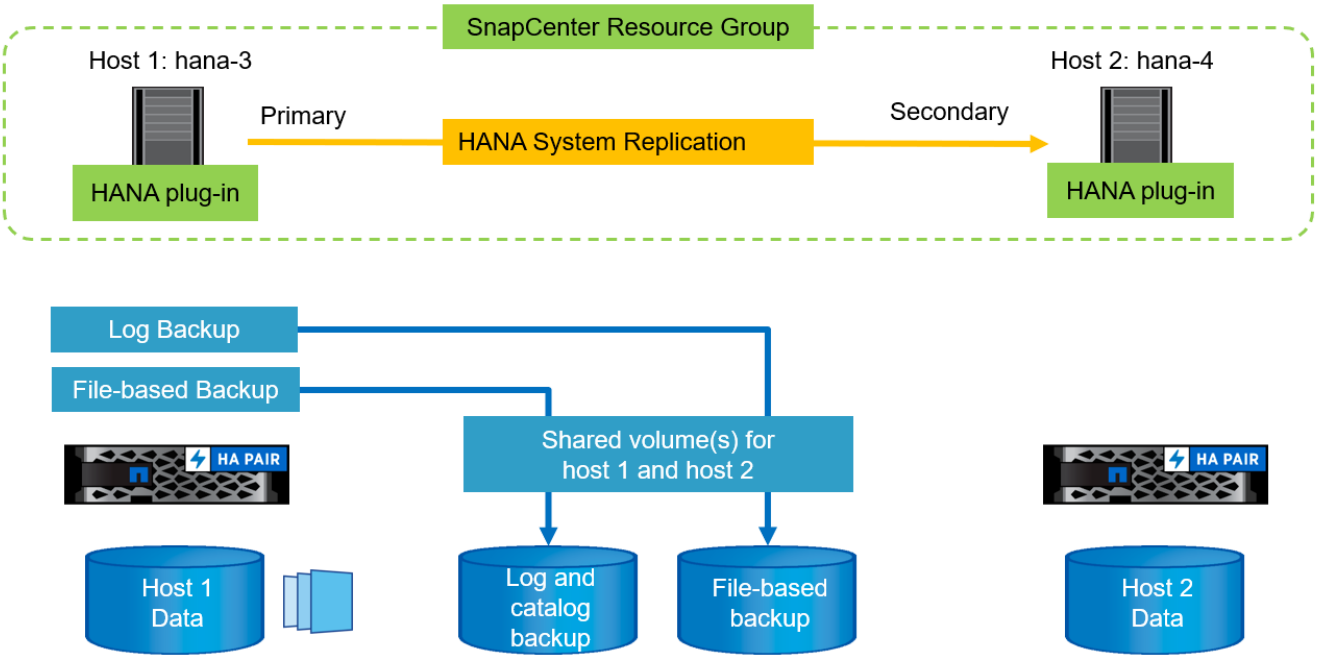
Für die HANA-Systemdatenbank wurde ein Datenbankbenutzer namens „SnapCenter“ mit den erforderlichen Berechtigungen zum Ausführen von Sicherungs- und Wiederherstellungsvorgängen erstellt (siehe "Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter"). Auf beiden Hosts muss ein HANA-Benutzerspeicherschlüssel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

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

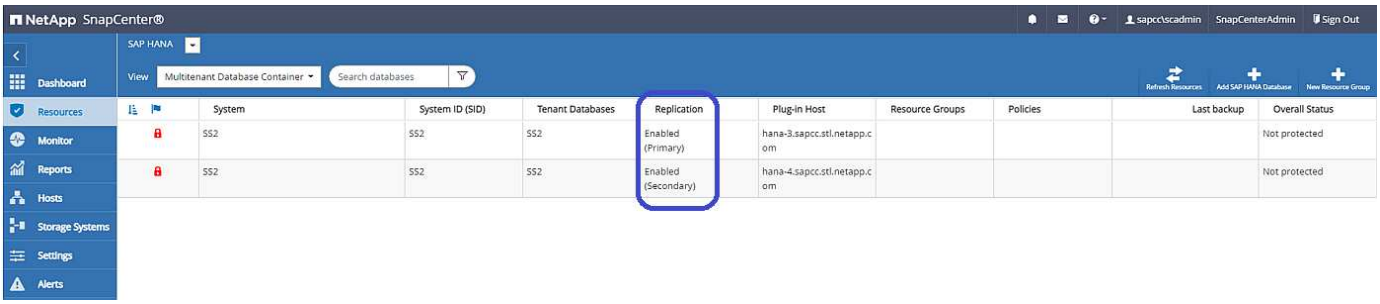
```
ss2adm@hana- 4:/ > hdbuserstore set SS2KEY hana-4:33313 SNAPCENTER
<password>
```

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

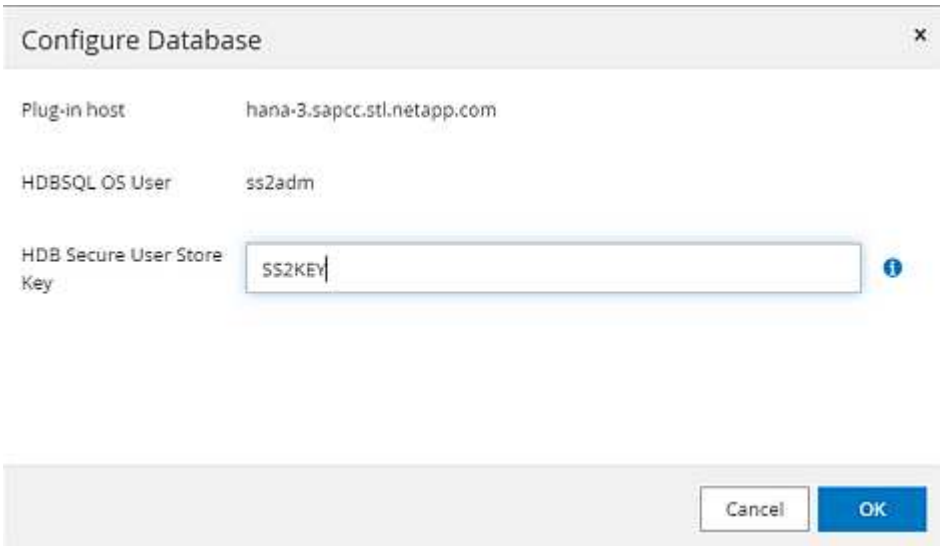
1. Das HANA-Plug-in wird auf dem primären und sekundären Host installiert. Die automatische Ermittlung wird ausgeführt und der Status der HANA-Systemreplizierung wird für jeden primären oder sekundären Host erkannt.
2. Ausführen von SnapCenter `configure database` Und stellen die bereit `hdbuserstore`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



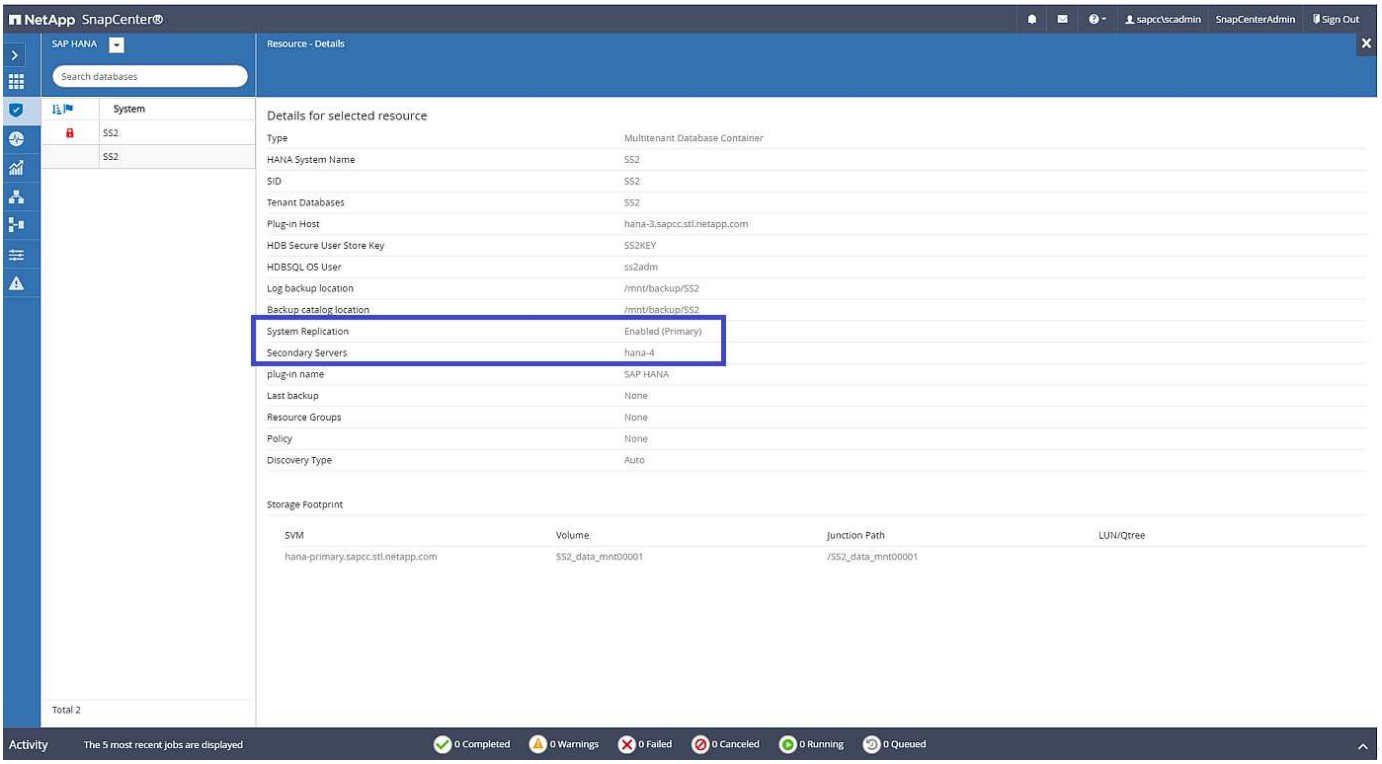
Nachdem Sie das SnapCenter HANA Plug-in auf beiden HANA-Hosts installiert haben, werden die HANA-Systeme in der Ansicht der SnapCenter-Ressourcen wie andere automatisch erkannte Ressourcen angezeigt. Ab SnapCenter 4.6 wird eine zusätzliche Spalte angezeigt, in der der Status der HANA-Systemreplizierung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



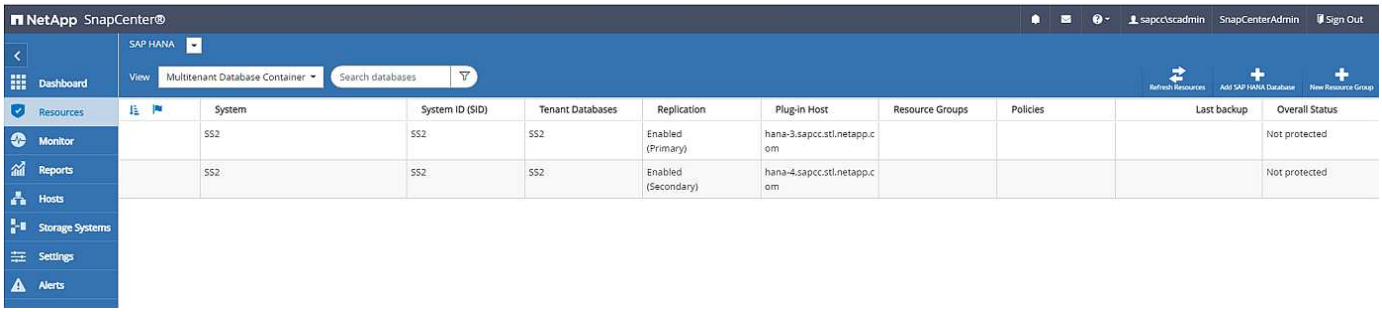
Durch Klicken auf die Ressource fordert SnapCenter den HANA-Benutzerspeicherschlüssel für das HANA-System an.



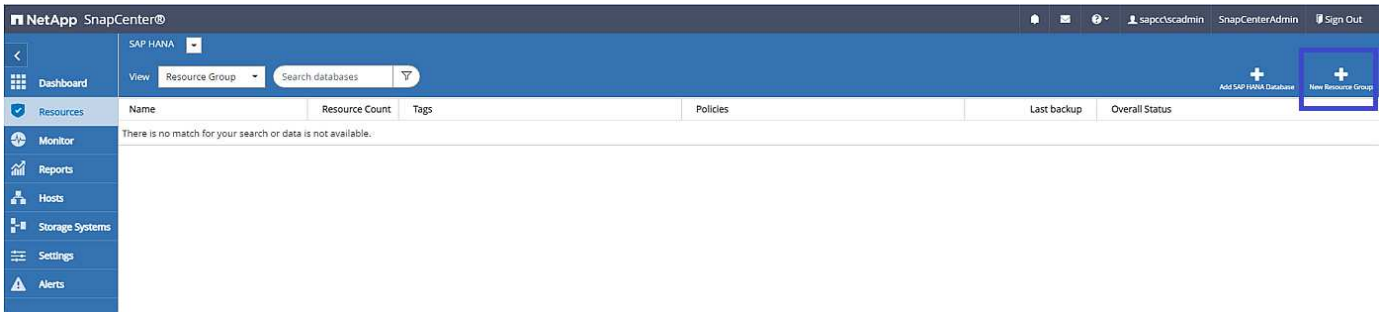
Weitere Schritte zur automatischen Ermittlung werden ausgeführt, und SnapCenter zeigen die Ressourcendetails an. In SnapCenter 4.6 werden der Replikationsstatus des Systems und der sekundäre Server in dieser Ansicht aufgelistet.



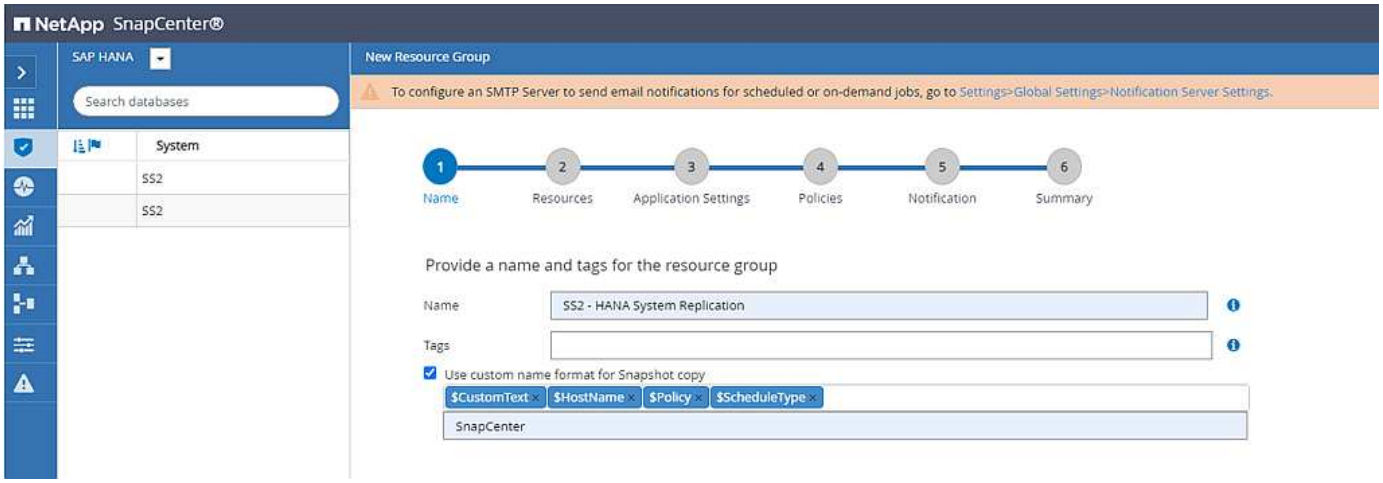
Nach Durchführung der gleichen Schritte für die zweite HANA-Ressource ist die automatische Ermittlung abgeschlossen, und beide HANA-Ressourcen werden in SnapCenter konfiguriert.



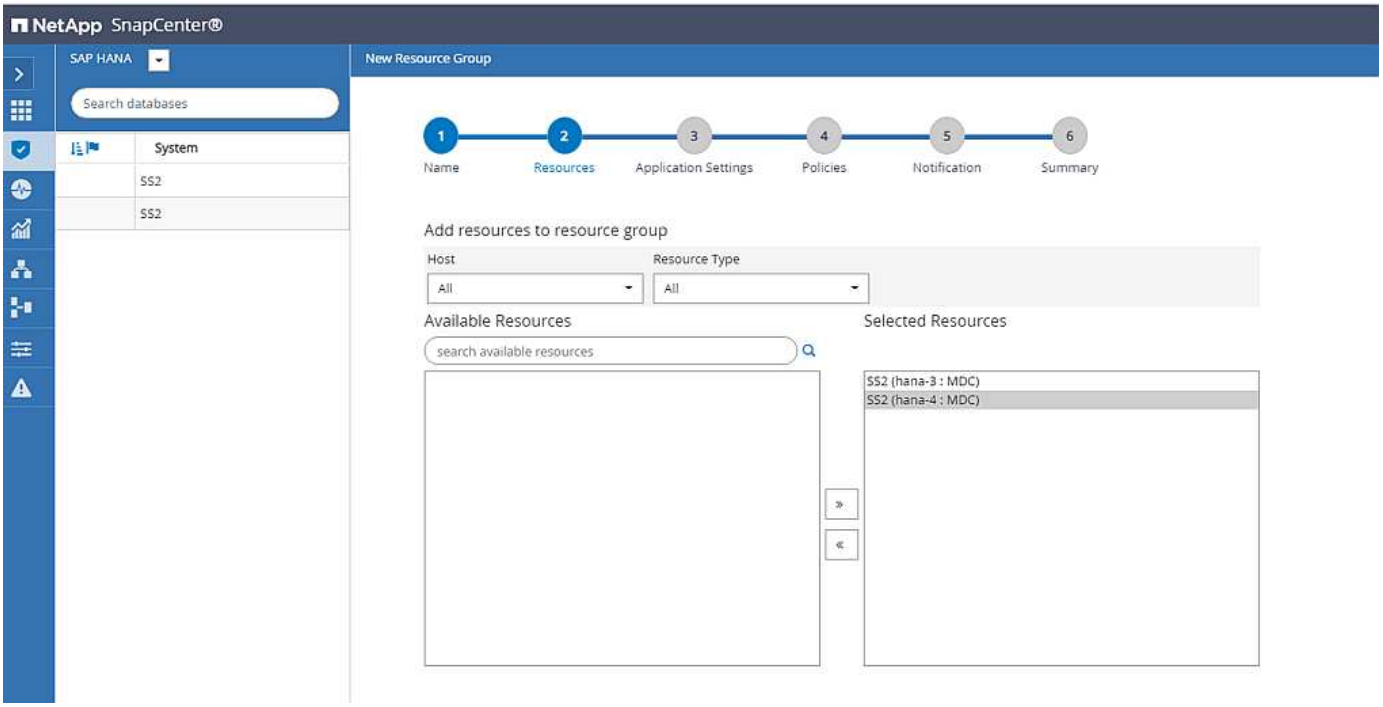
Für HANA System Replication-fähige Systeme müssen Sie eine SnapCenter-Ressourcengruppe, einschließlich beider HANA-Ressourcen, konfigurieren.



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

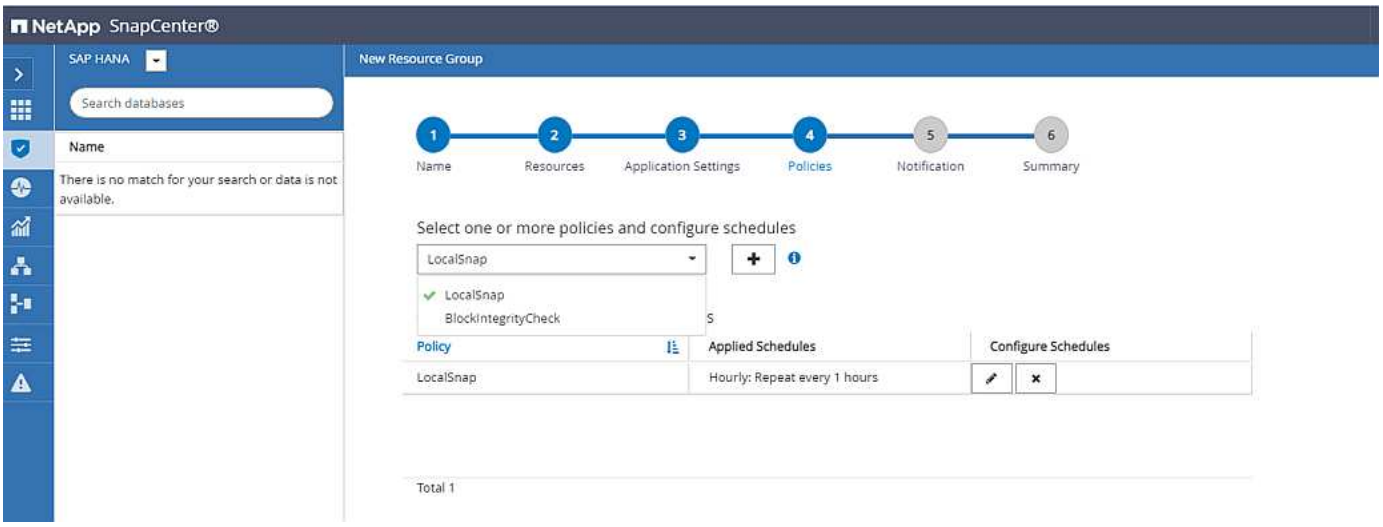


Sie müssen der Ressourcengruppe beide HANA-Hosts hinzufügen.

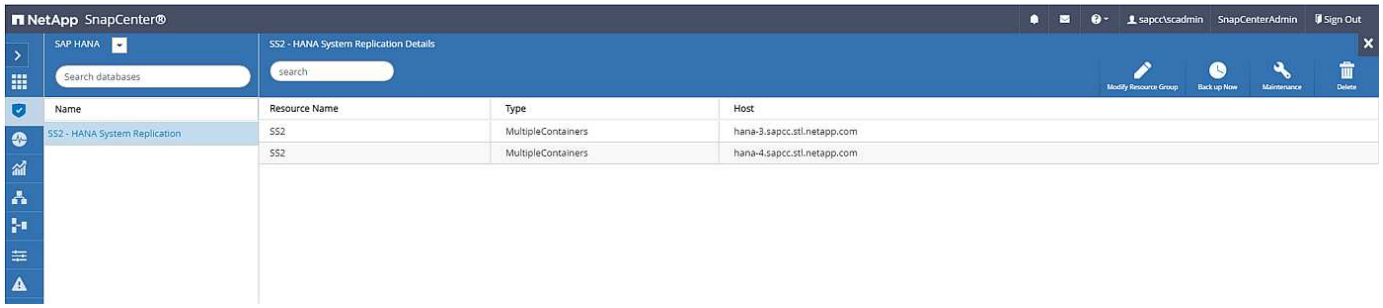


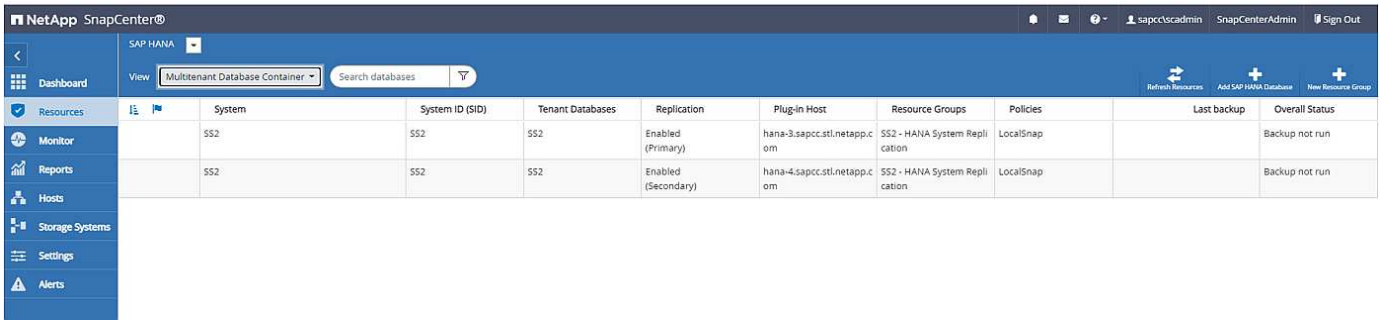
Die Richtlinien und Zeitpläne für die Ressourcengruppe werden konfiguriert.

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



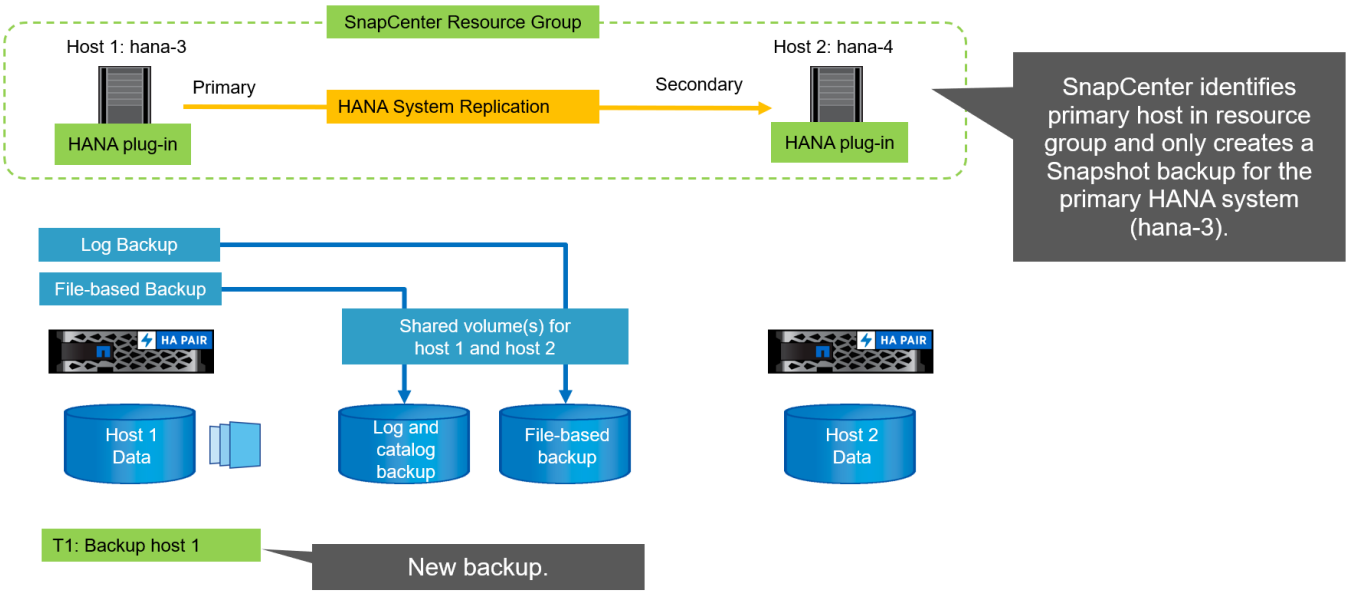
Die Konfiguration der Ressourcengruppe ist jetzt abgeschlossen und Backups können ausgeführt werden.



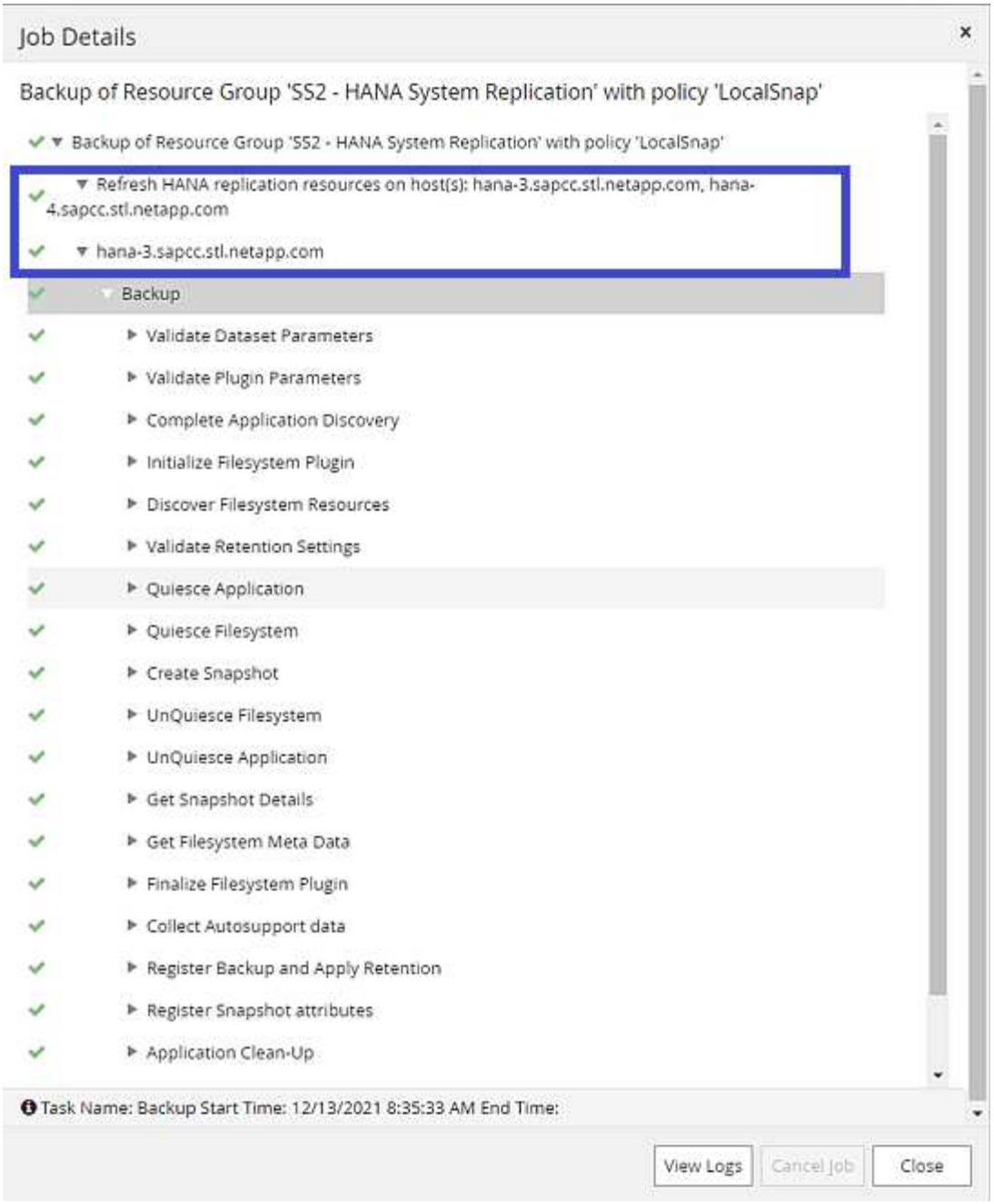


Snapshot-Backup-Vorgänge

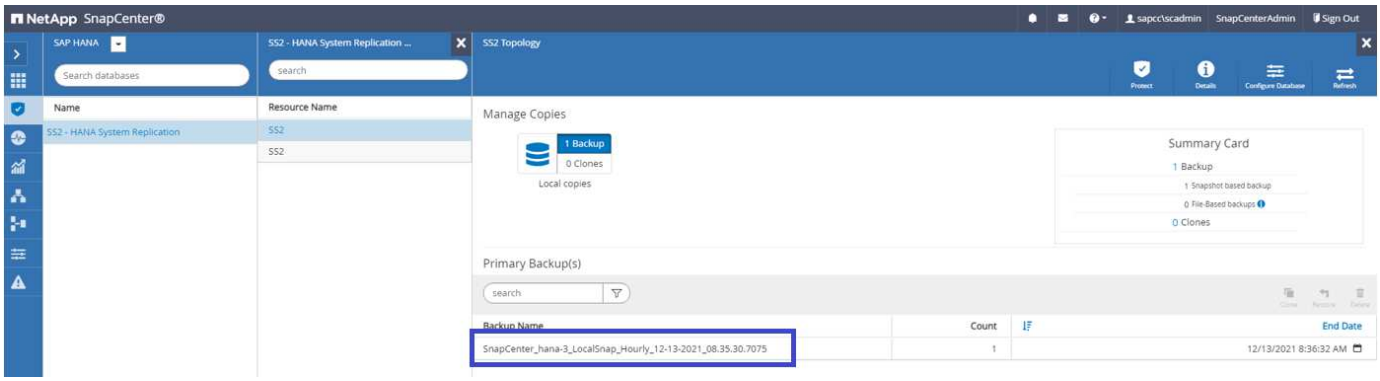
Wenn ein Backup-Vorgang der Ressourcengruppe ausgeführt wird, identifiziert SnapCenter den primären Host und löst nur ein Backup auf dem primären Host aus. Das bedeutet, dass nur das Daten-Volume des primären Hosts mit Snapshots erstellt werden wird. in unserem Beispiel ist hana-3 der aktuelle primäre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



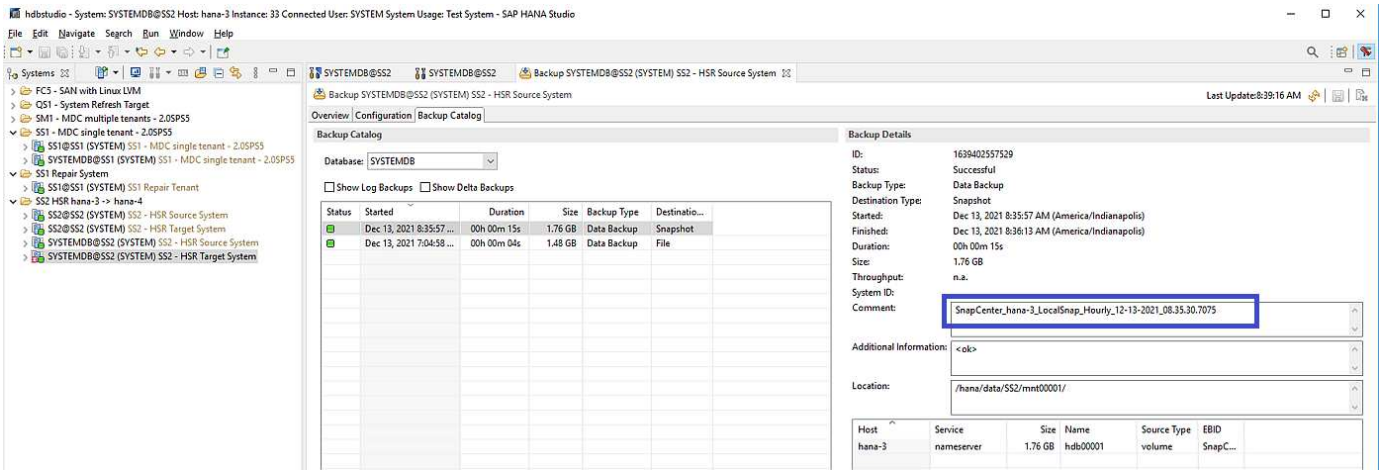
Das SnapCenter-Jobprotokoll zeigt den Identifizierungsvorgang und die Ausführung des Backups auf dem aktuellen primären Host hana-3.



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

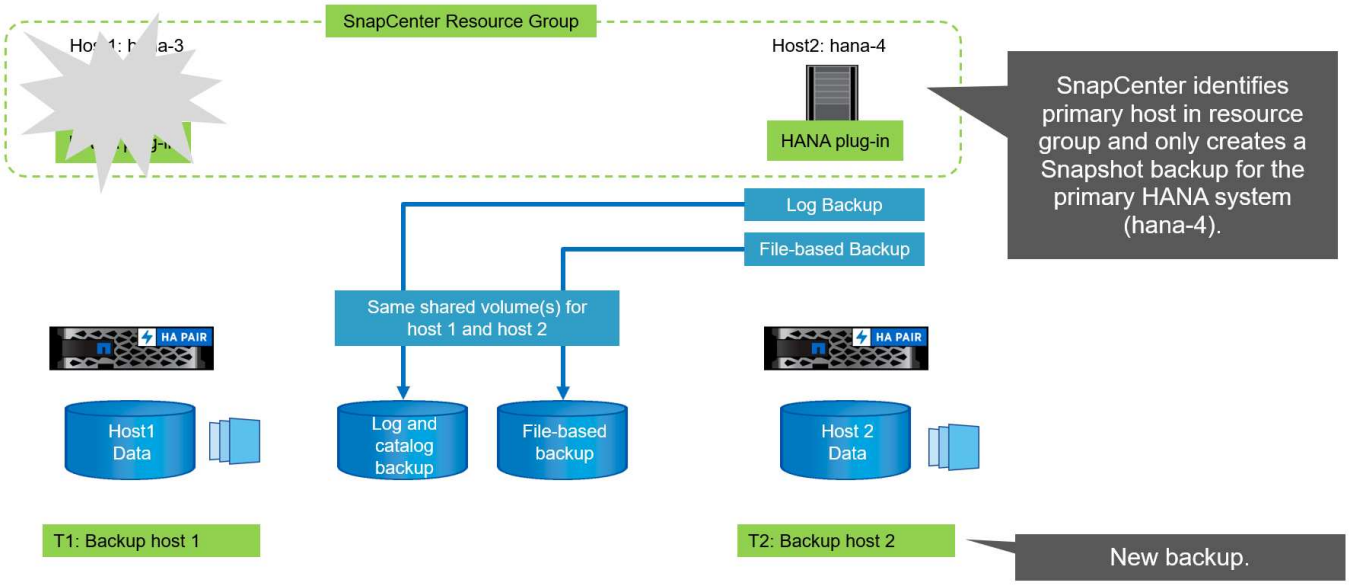


Das Snapshot-Backup ist auch im HANA-Backup-Katalog sichtbar.

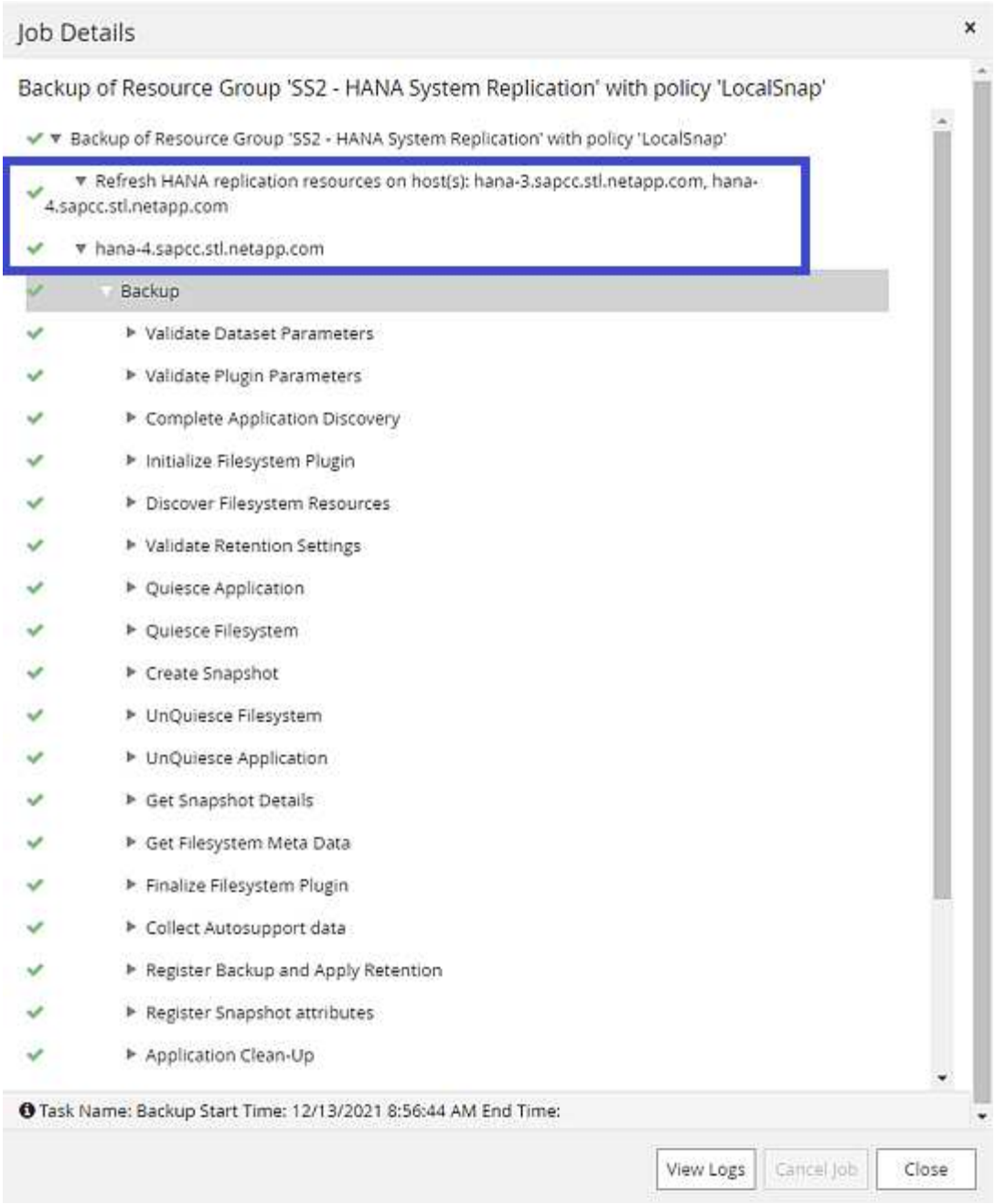


Falls ein Übernahmevorgang ausgeführt wird, identifizieren weitere SnapCenter Backups jetzt den früheren sekundären Host (hana-4) als primär und der Backup-Vorgang wird auf hana-4 ausgeführt. Erneut wird nur das Daten-Volume des neuen primären Hosts (hana-4) mit Snapshots erstellt.

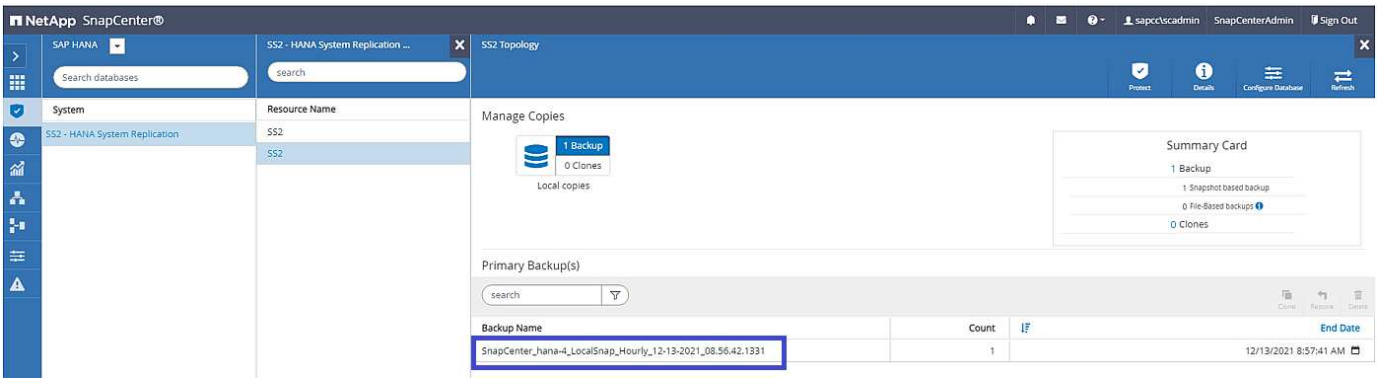
Die SnapCenter-Identifizierungslogik deckt nur Szenarien ab, in denen sich die HANA-Hosts in einer primären/sekundären Beziehung befinden oder wenn einer der HANA-Hosts offline ist.



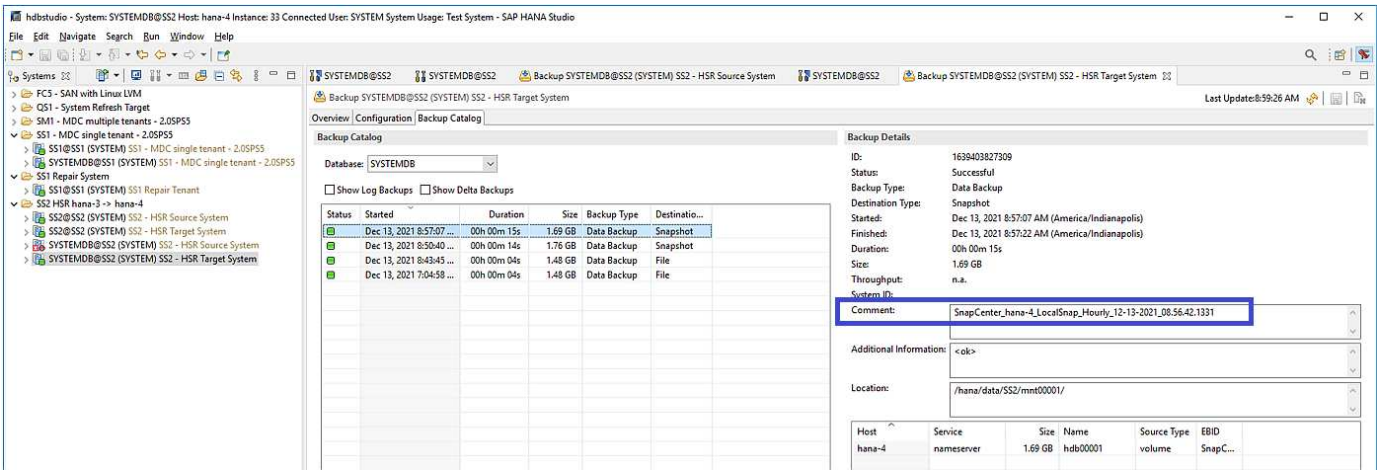
Das SnapCenter-Jobprotokoll zeigt den Identifizierungsvorgang und die Ausführung des Backups auf dem aktuellen primären Host hana-4.



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



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



Block-Integritätsprüfung mit dateibasierten Backups

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

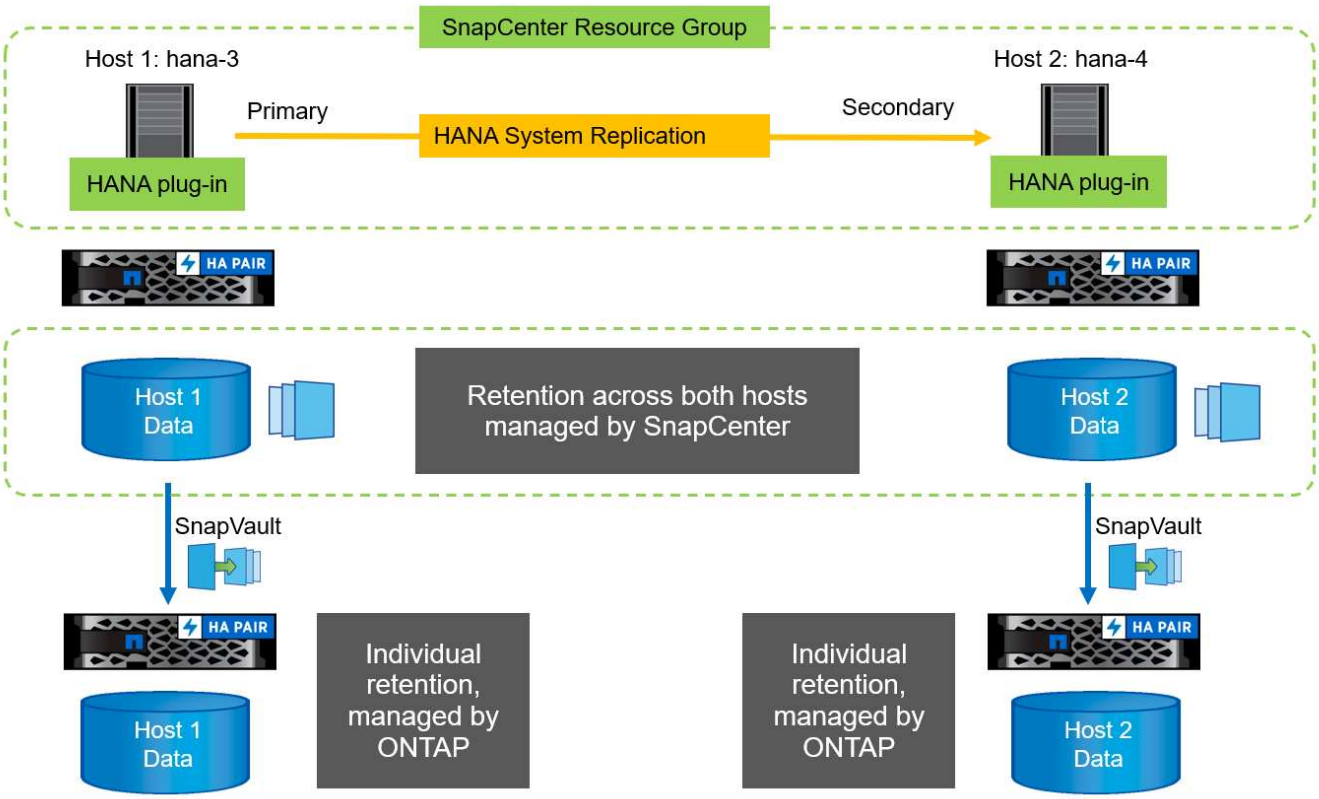
SnapVault Replizierung

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

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

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

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



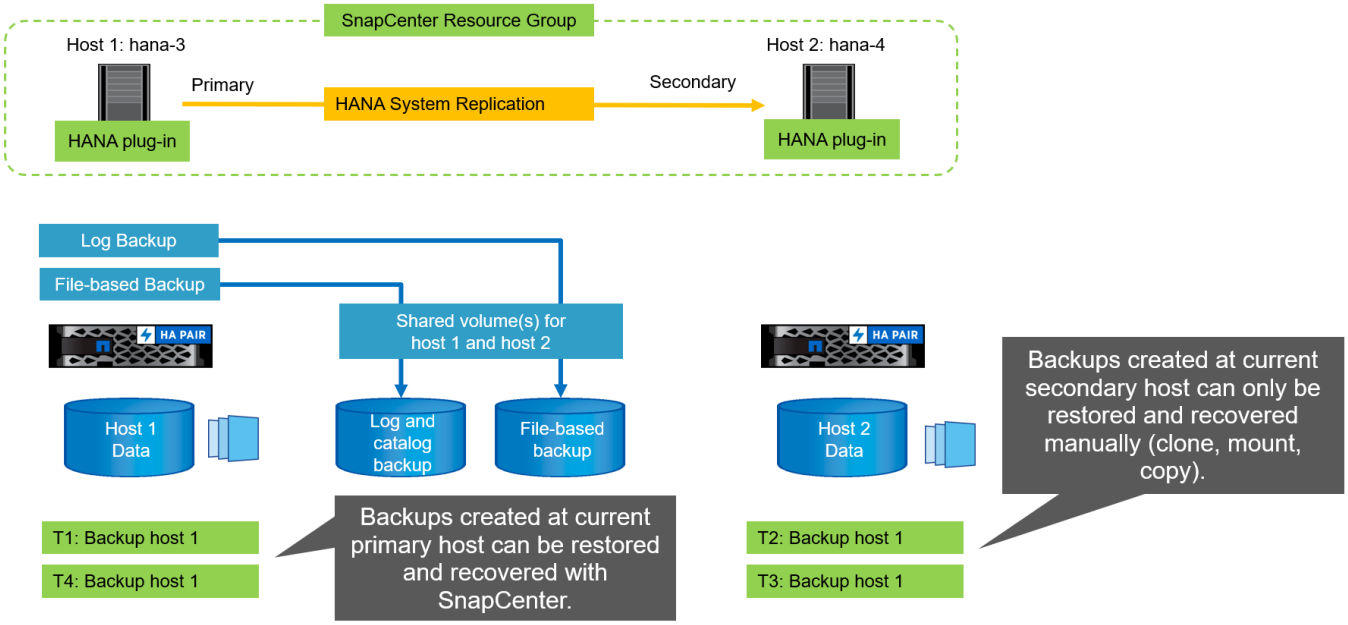
Retentionmanagement

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

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

Restore und Recovery

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



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

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

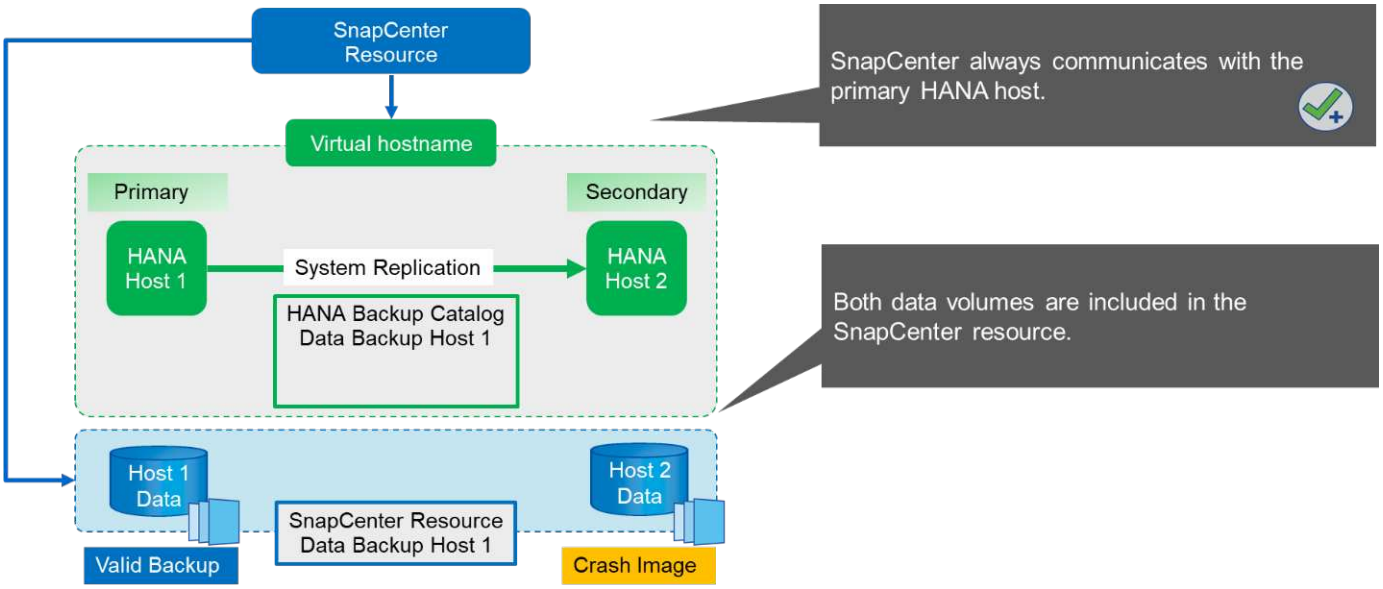
SnapCenter Konfiguration mit einer einzigen Ressource

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

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

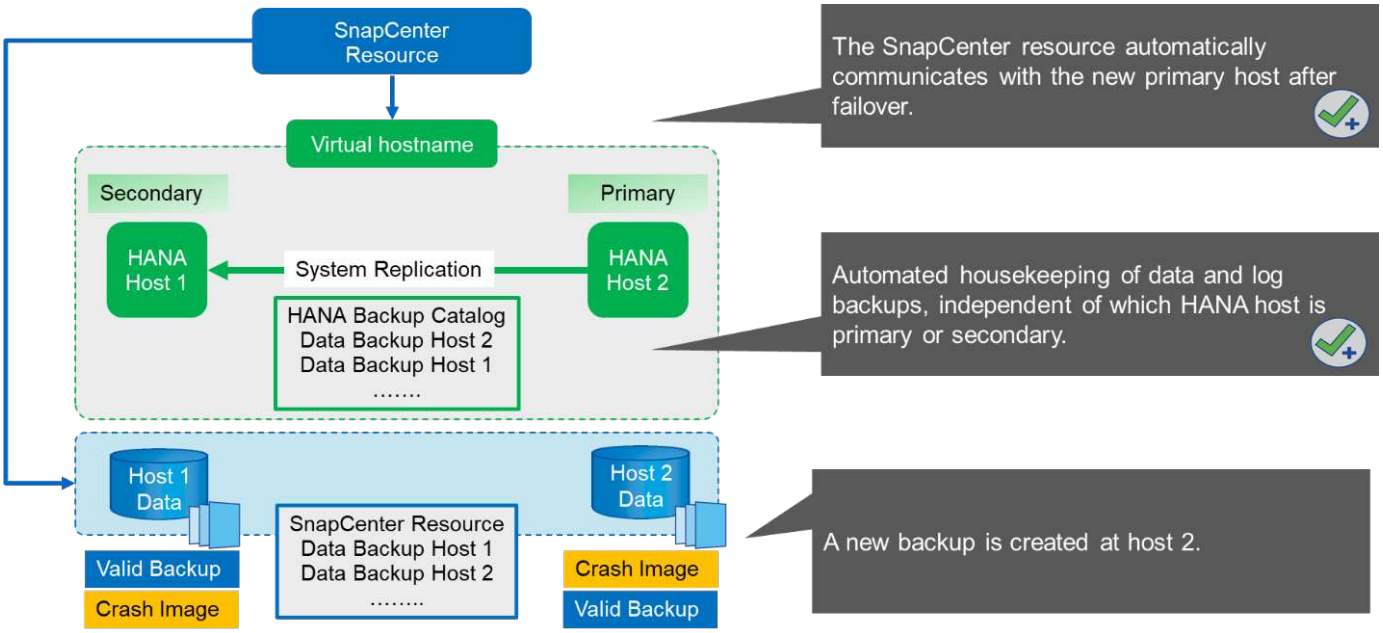
Wird ein Backup mit Host 1 als primärer Host ausgeführt, wird ein datenbankkonsistentes Snapshot-Backup auf dem Datenvolumen von Host 1 erstellt. Da das Daten-Volume des Hosts 2 Teil der SnapCenter Ressource ist, wird für dieses Volume eine weitere Snapshot Kopie erstellt. Diese Snapshot Kopie ist nicht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

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



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

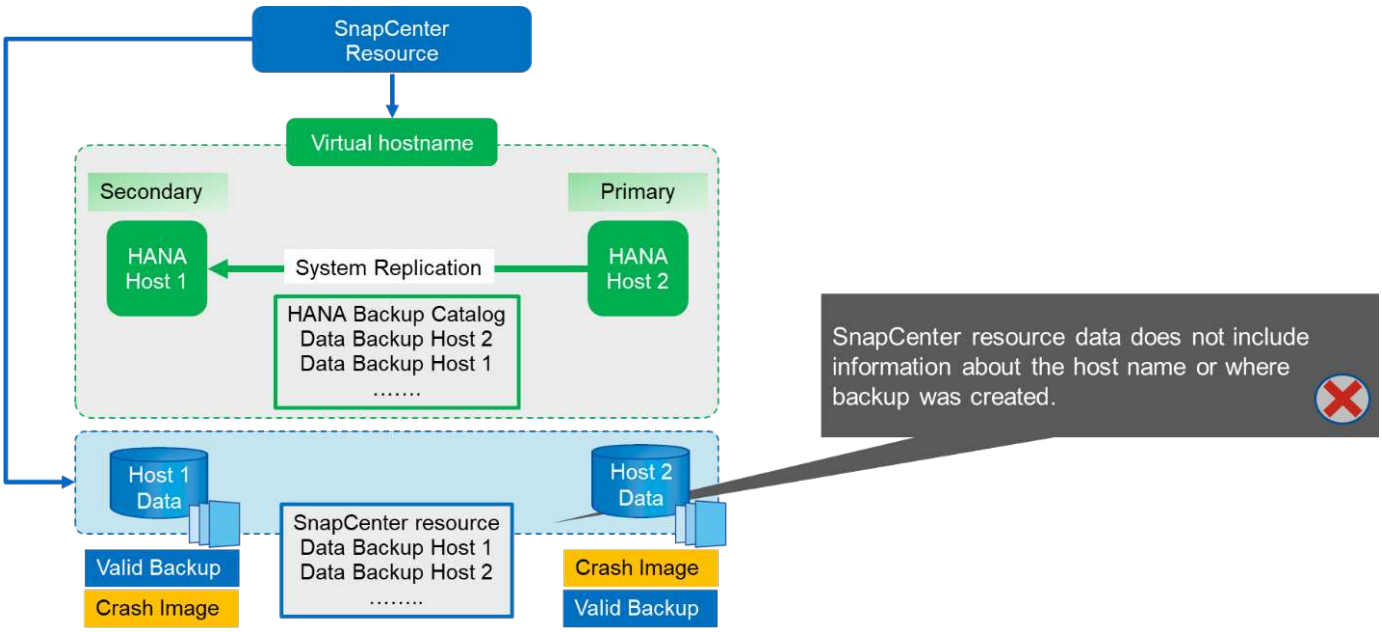
Die allgemeine Ordnung und Sauberkeit der Daten- und Log-Backups basiert auf der definierten SnapCenter-Aufbewahrungsrichtlinie und die Backups werden unabhängig vom primären oder sekundären Host gelöscht.



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

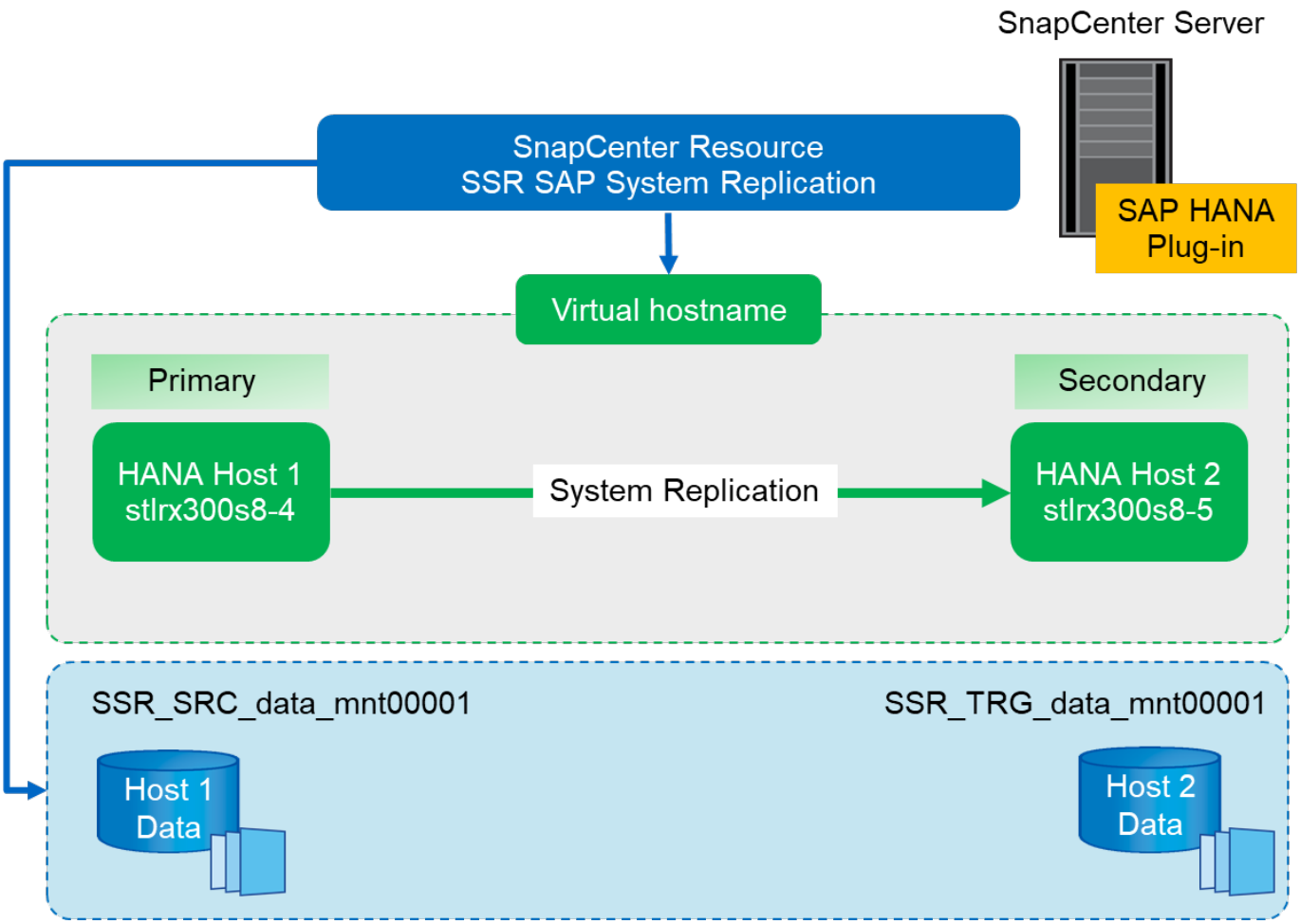
Bei einer SnapCenter-Konfiguration mit nur einem Mitarbeiter ist SnapCenter nicht bewusst, wo das Backup erstellt wurde. NetApp empfiehlt daher, dem SnapCenter Backup-Workflow ein Pre-Backup-Skript hinzuzufügen, um zu ermitteln, welcher Host derzeit der primäre SAP HANA-Host ist.

Die folgende Abbildung zeigt die Identifikation des Backup-Hosts.



SnapCenter-Konfiguration

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



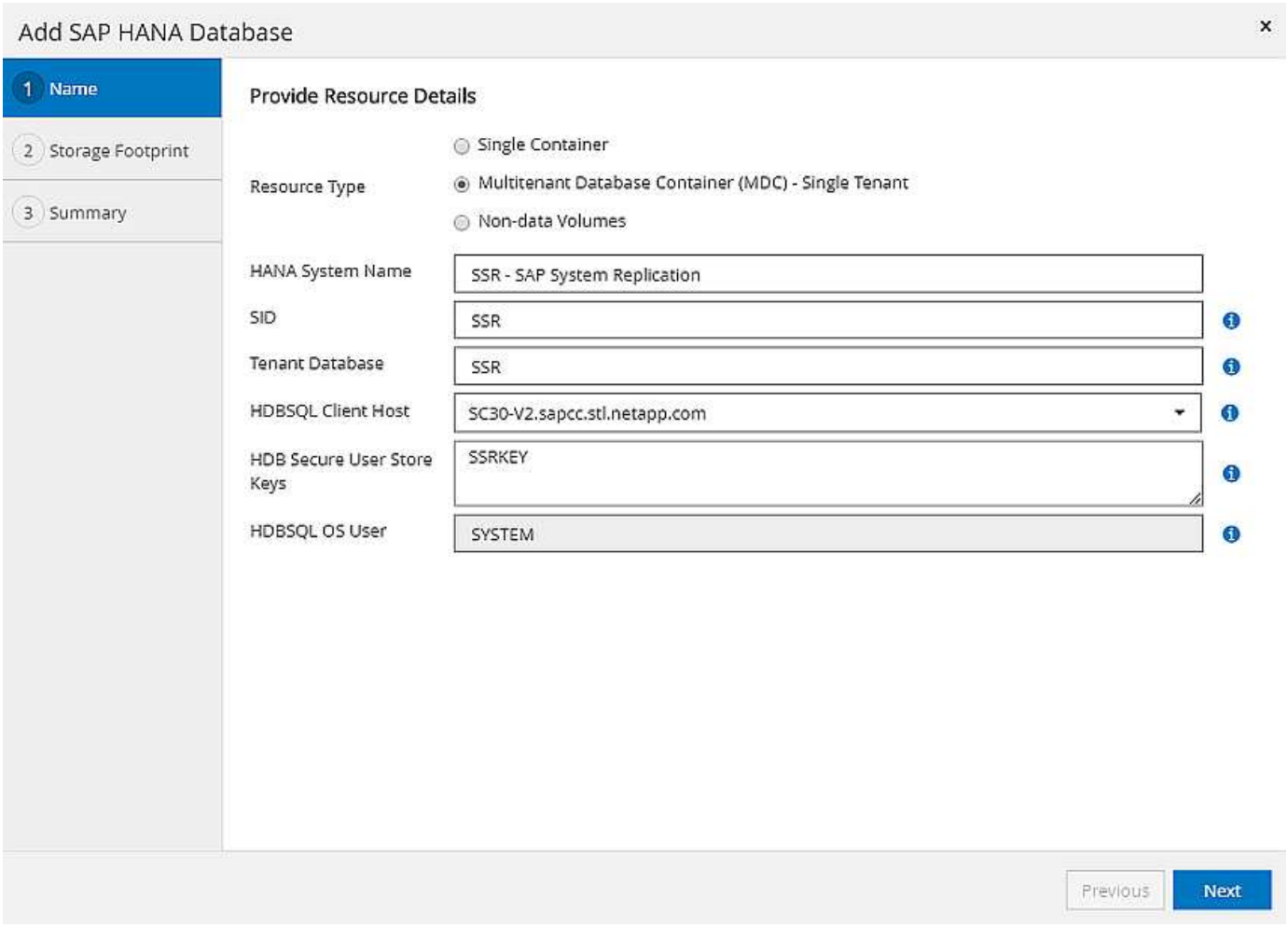
Um Backup-Vorgänge unabhängig davon durchzuführen, welcher SAP HANA Host primär ist und selbst wenn ein Host ausfällt, muss das SnapCenter SAP HANA Plug-in auf einem zentralen Plug-in-Host implementiert werden. In unserer Lab-Einrichtung wurde der SnapCenter Server als zentraler Plug-in-Host verwendet,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

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

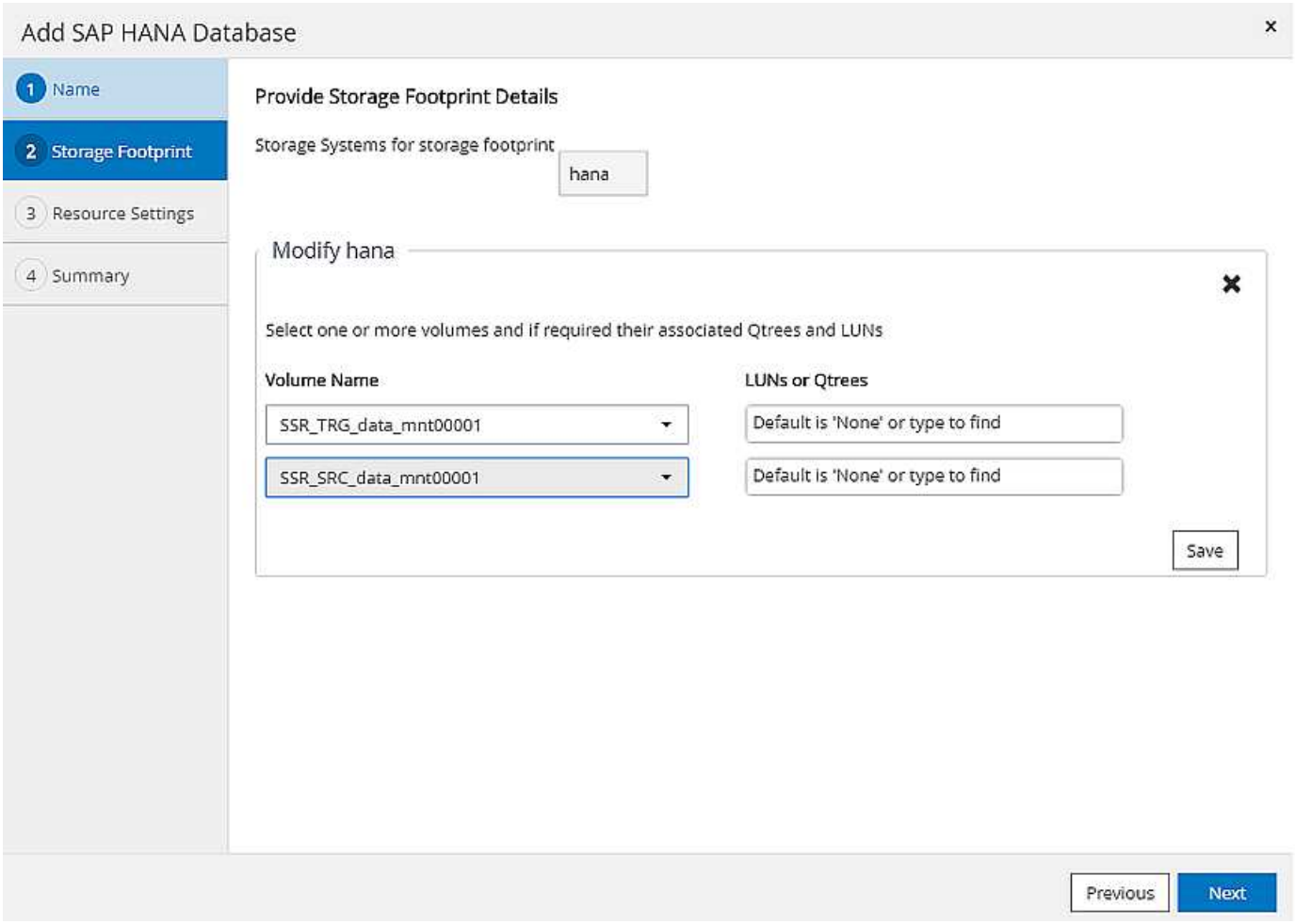
```
hdbuserstore.exe -u SYSTEM set SSRKEY ssr-vip:31013 SNAPCENTER <password>
```

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

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

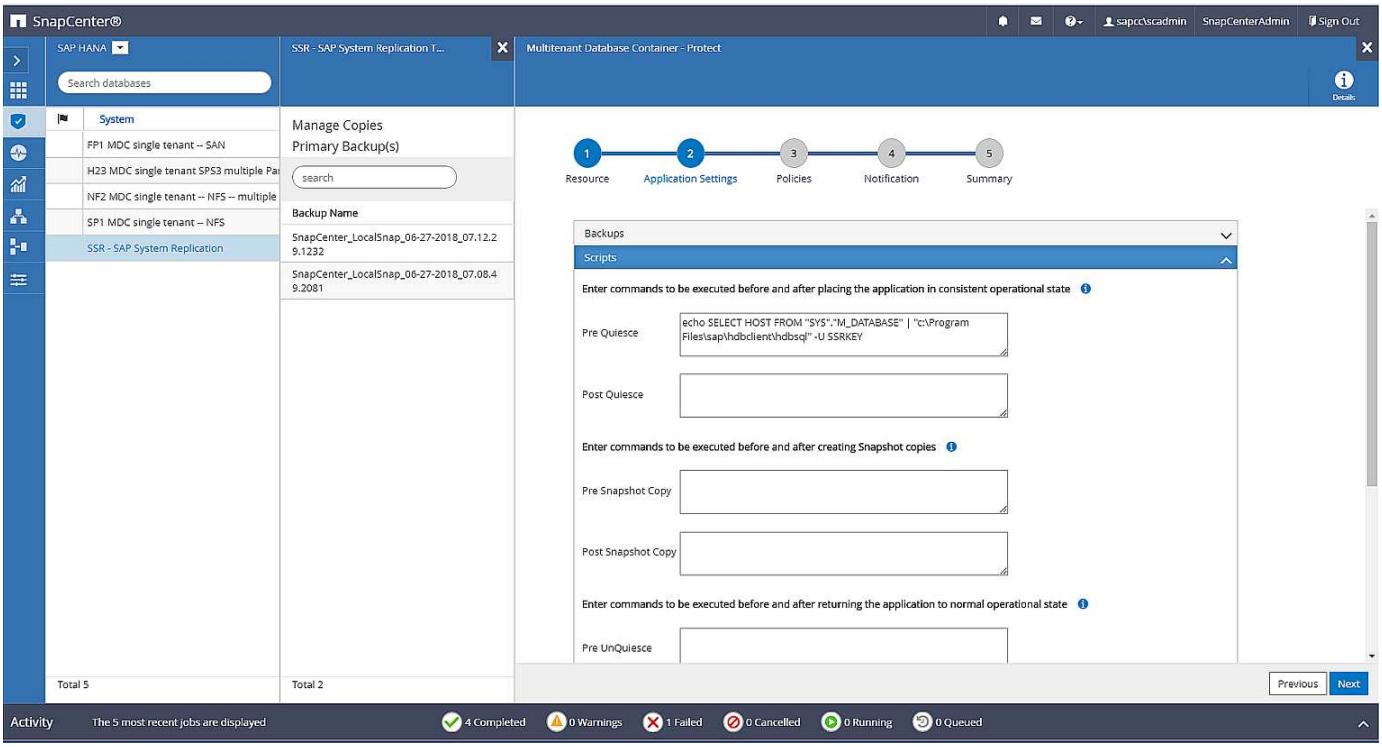


Die Datenvolumen der beiden SAP HANA-Hosts sind in der Storage-Platzbedarf-Konfiguration enthalten, wie die folgende Abbildung zeigt.



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

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

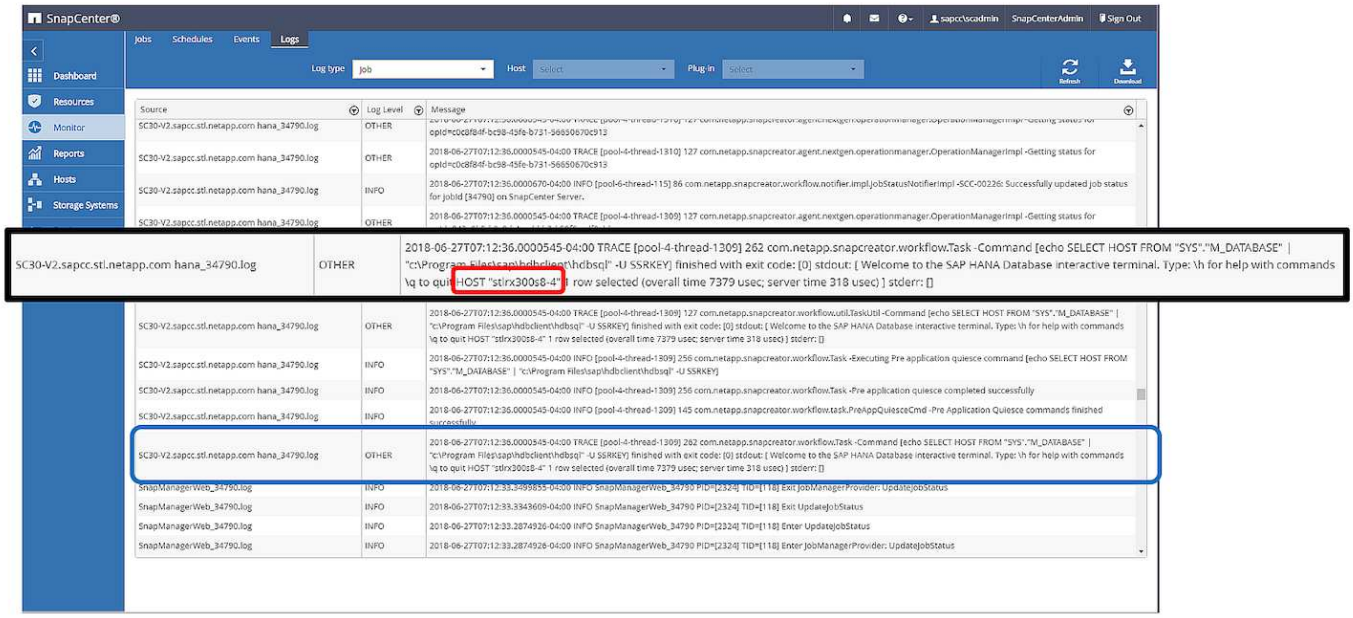


SnapCenter Backup-Vorgang

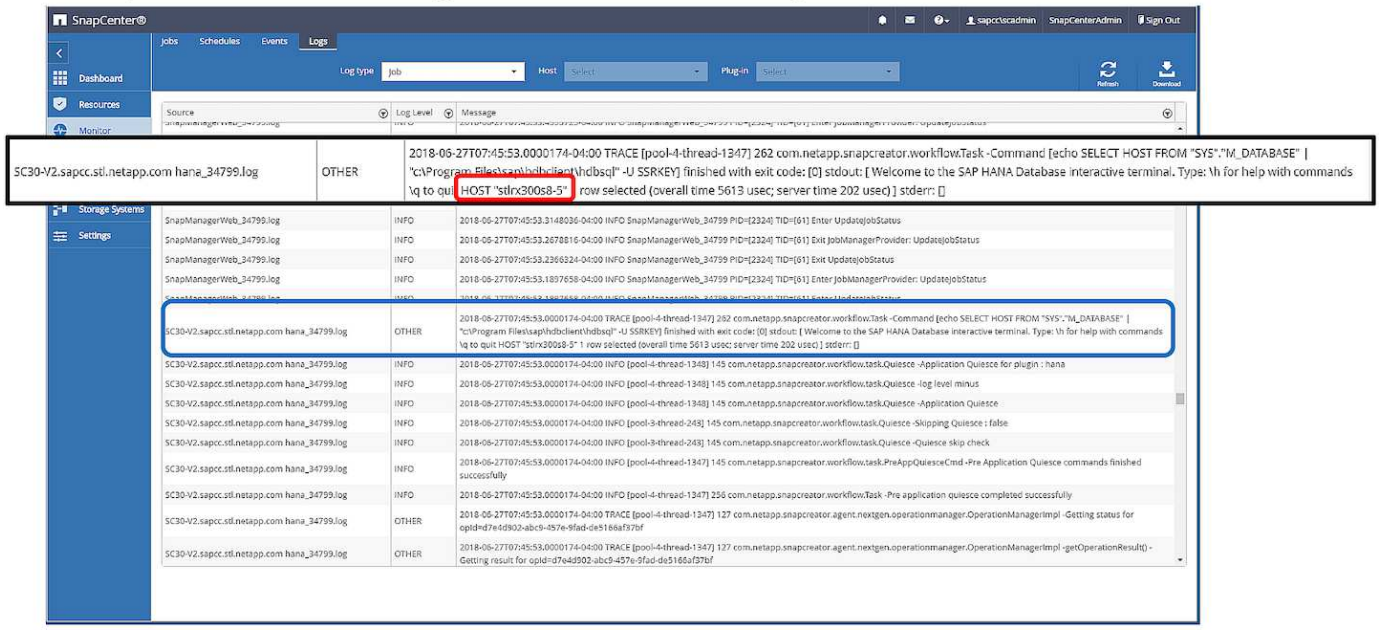
Backup-Vorgänge werden jetzt wie gewohnt ausgeführt. Die allgemeine Ordnung und Sauberkeit der Daten und Log-Backups wird unabhängig davon durchgeführt, welcher SAP HANA-Host primärer oder sekundärer ist.

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

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

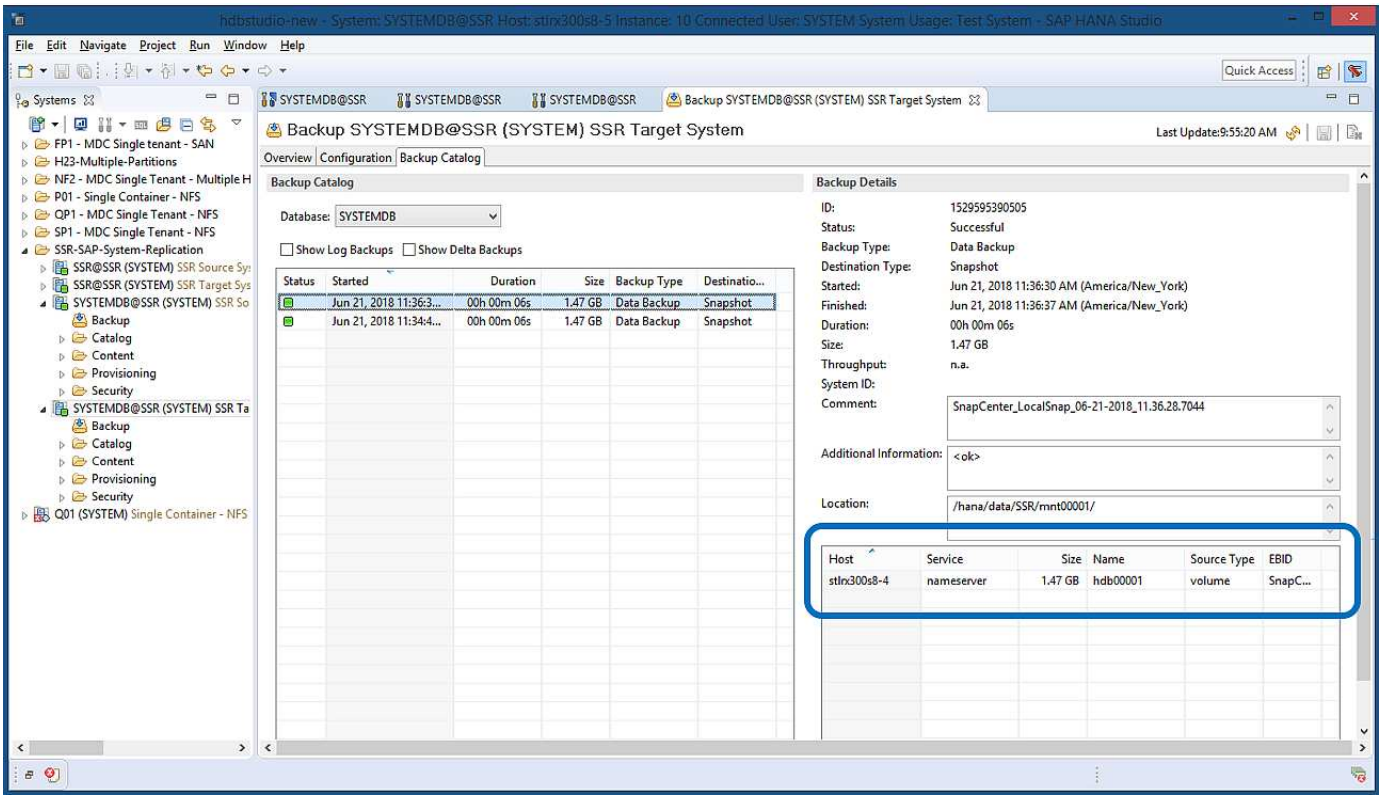


Diese Abbildung zeigt das Backup-Jobprotokoll mit Host 2 als primärer Host.



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

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



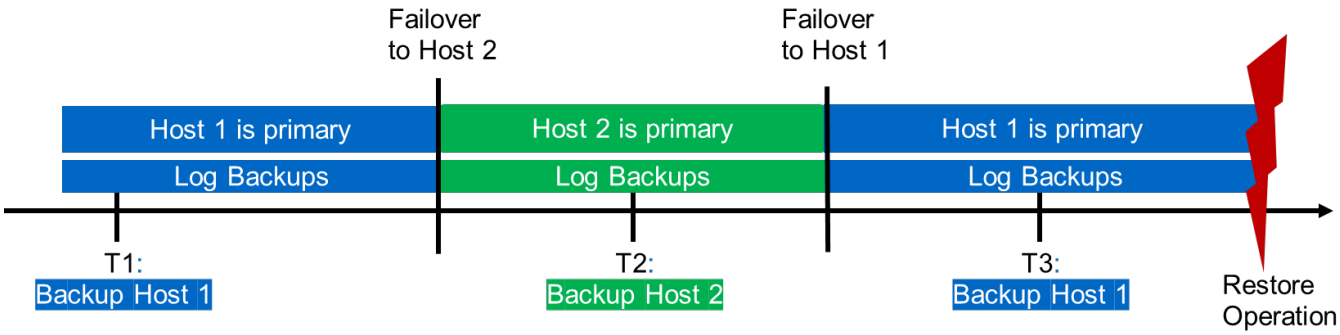
Restore und Recovery

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

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

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

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



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

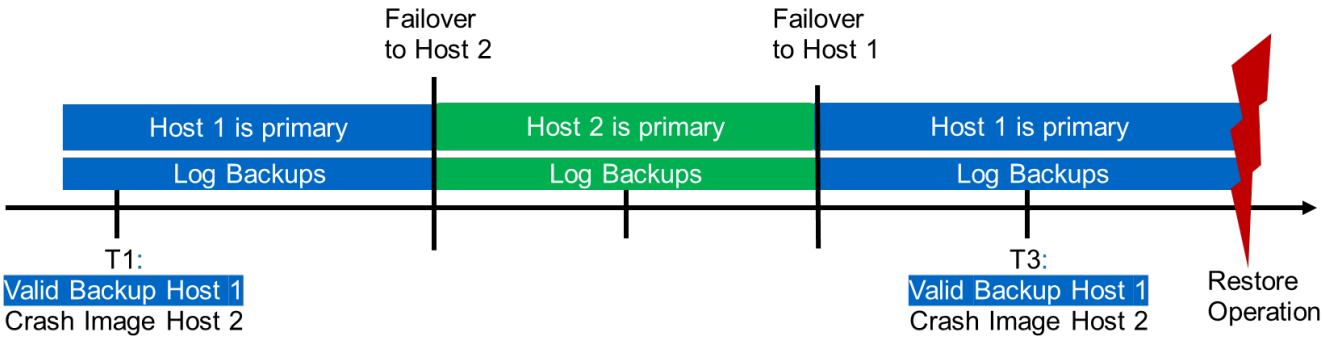
Mit einer einzelnen SnapCenter Ressourcenkonfiguration werden Snapshot Kopien auf beiden Storage-Volumes sowohl von SAP HANA System Replication Hosts erstellt. Nur das Snapshot-Backup, das auf dem Storage-Volume des primären SAP HANA-Hosts erstellt wird, ist für die zukünftige Recovery gültig. Die auf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

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

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

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

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

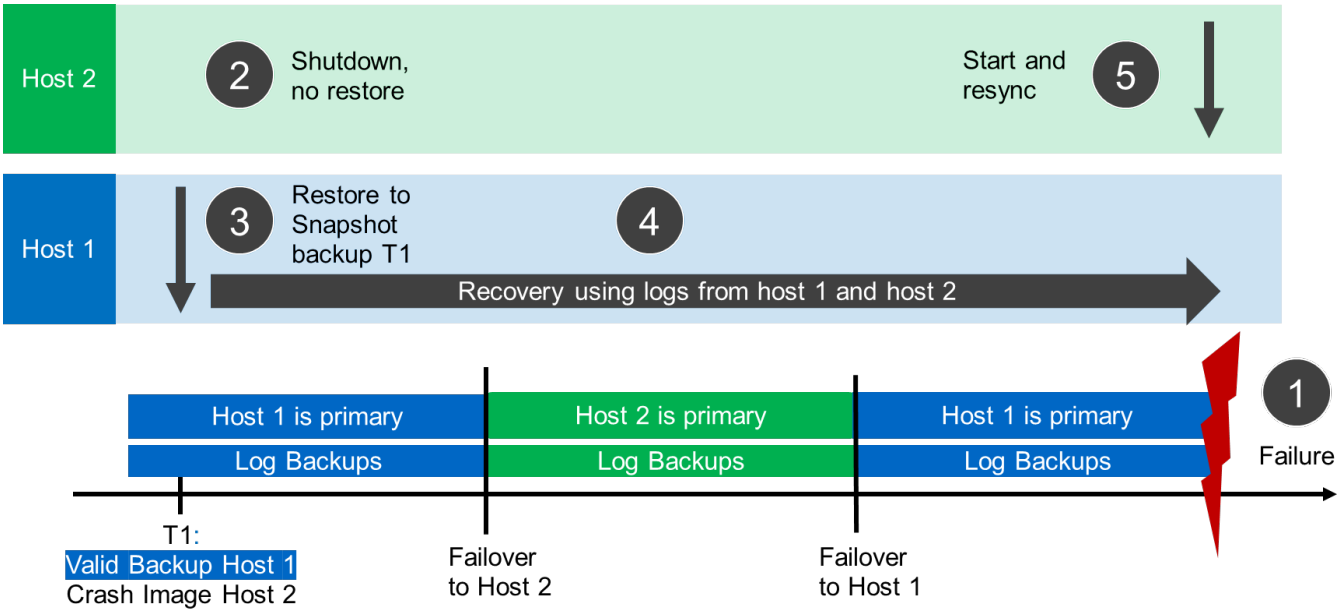


SnapCenter Restore nur für gültige Backups

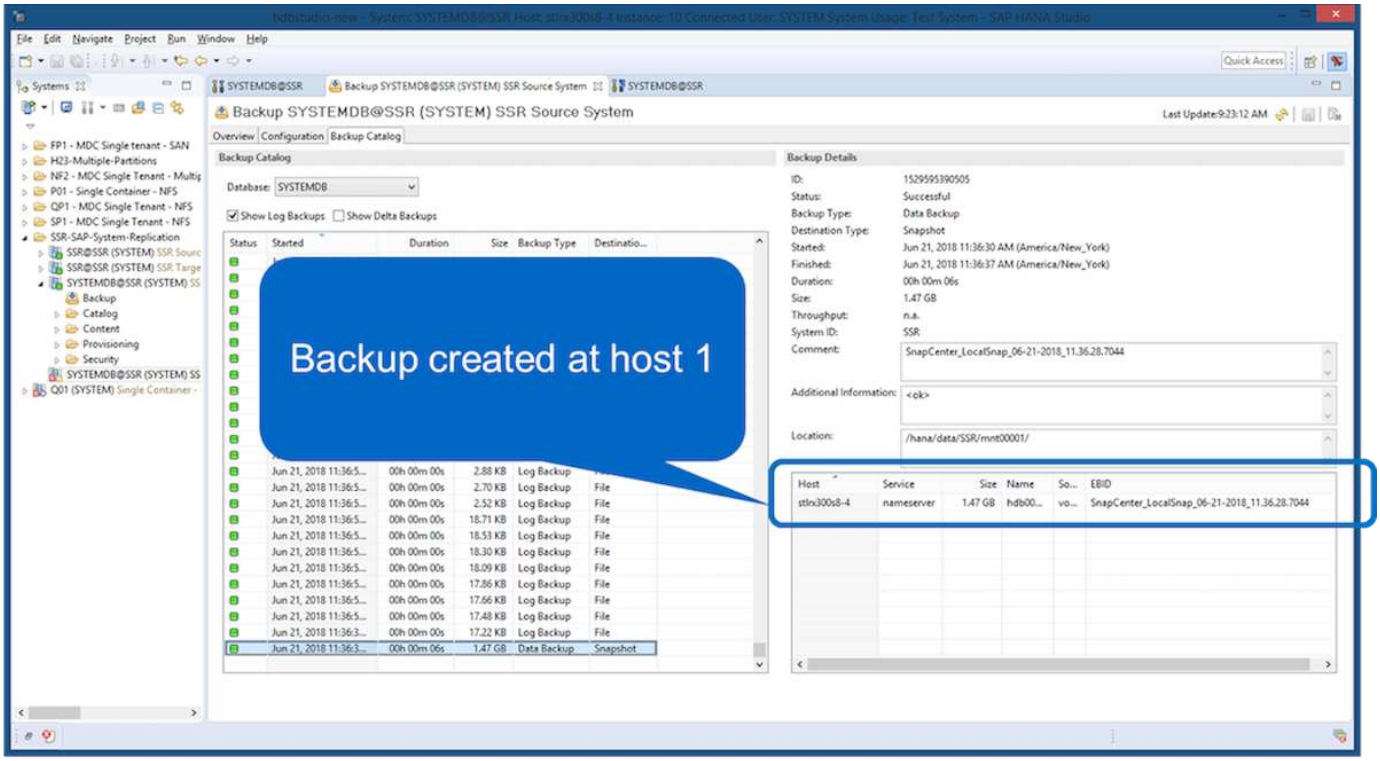
Die folgende Abbildung zeigt einen Überblick über das in diesem Abschnitt beschriebene Wiederherstellungsszenario.

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

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



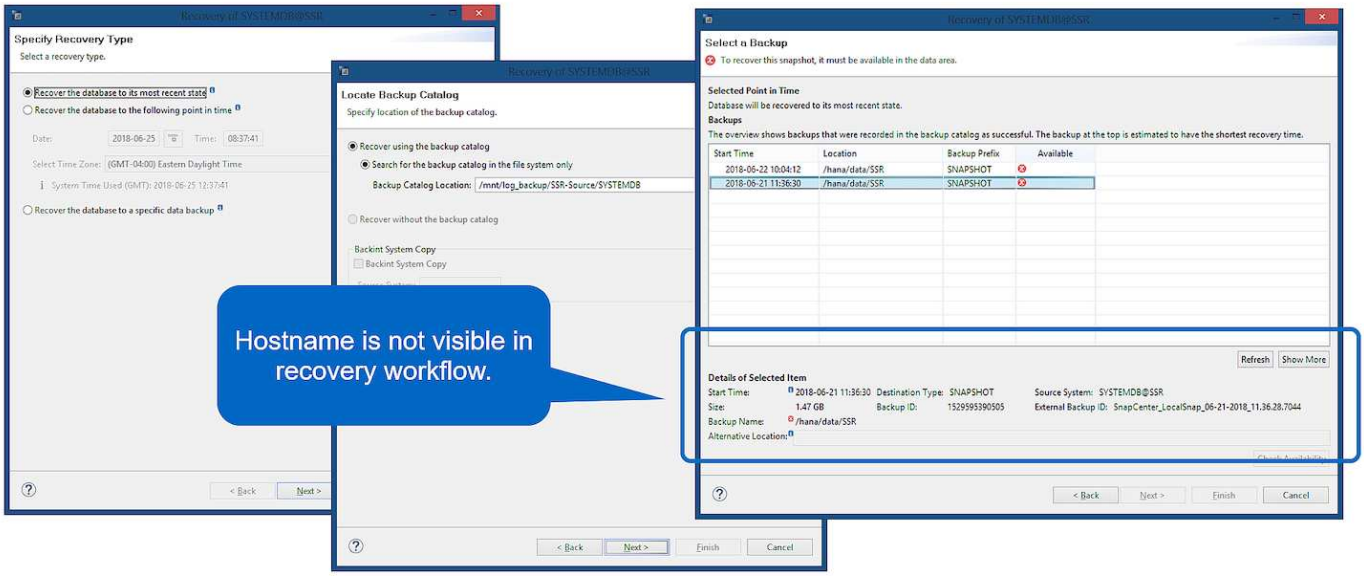
Die folgende Abbildung zeigt den SAP HANA Backup-Katalog in SAP HANA Studio. Die hervorgehobene Sicherung zeigt die Sicherung, die am T1 bei Host 1 erstellt wurde.



25

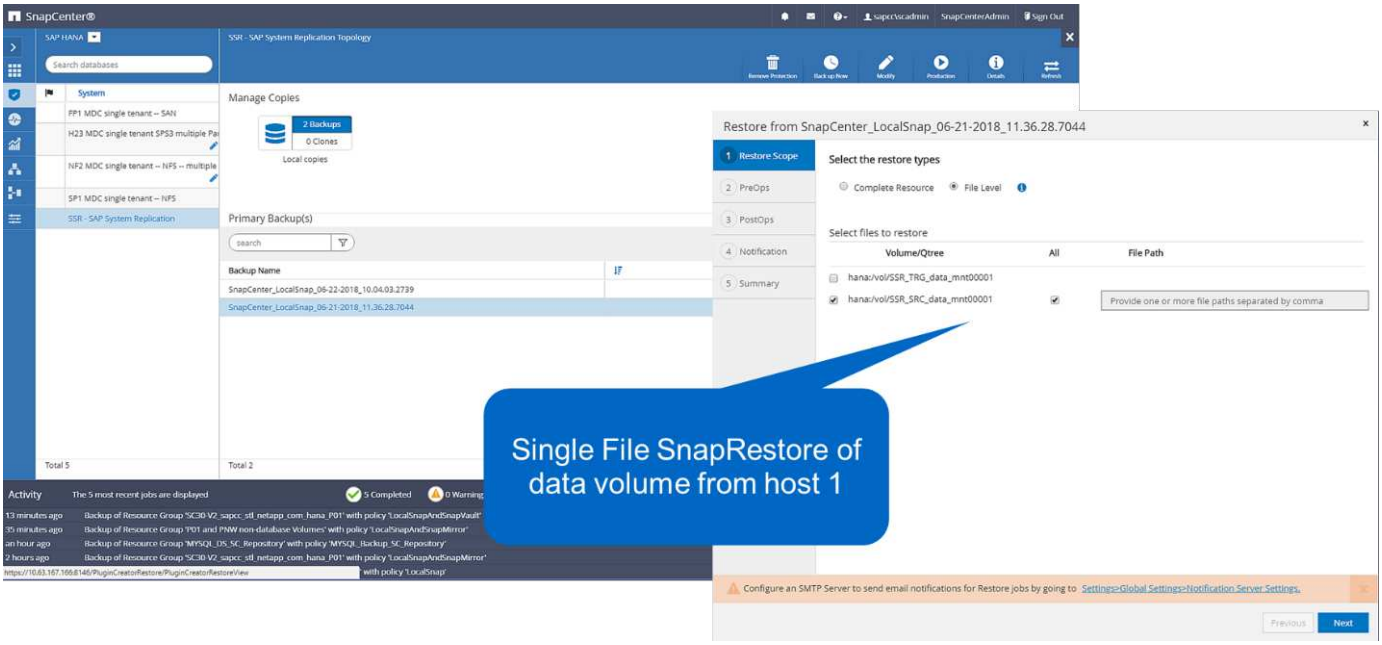
Im SAP HANA Studio wird eine Wiederherstellung gestartet. Wie die folgende Abbildung zeigt, ist der Name des Hosts, auf dem das Backup erstellt wurde, im Wiederherstellungsworkflow nicht sichtbar.

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

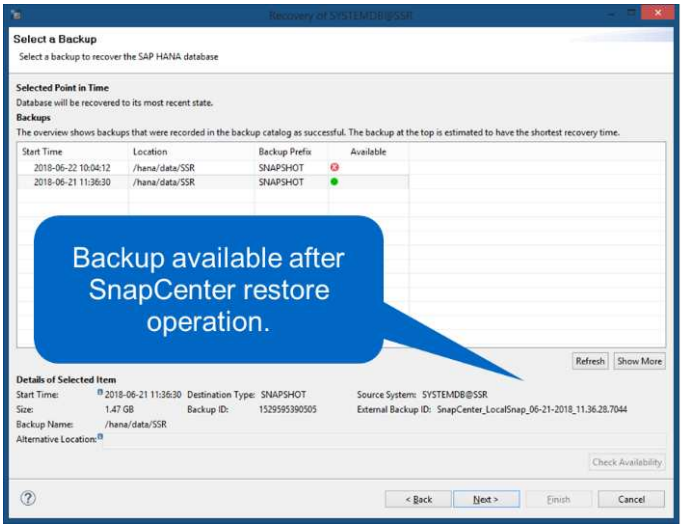


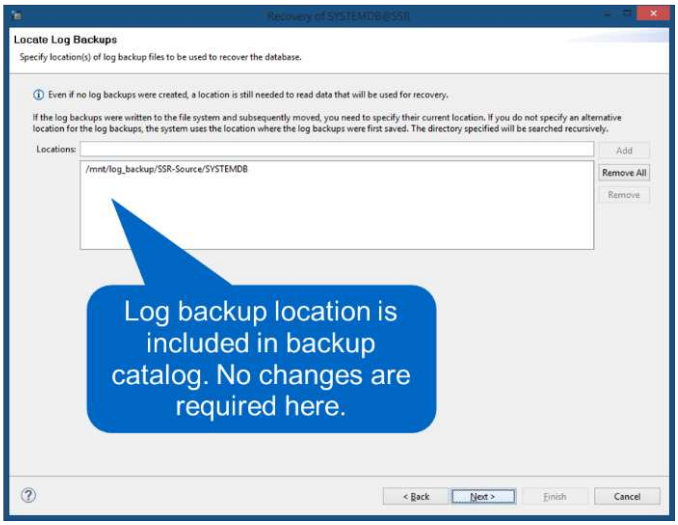
In SnapCenter wird das Backup ausgewählt und ein Restore-Vorgang auf Dateiebene durchgeführt. Auf dem Bildschirm Wiederherstellung auf Dateiebene wird nur das Host 1 Volume ausgewählt, sodass nur das gültige

Backup wiederhergestellt wird.



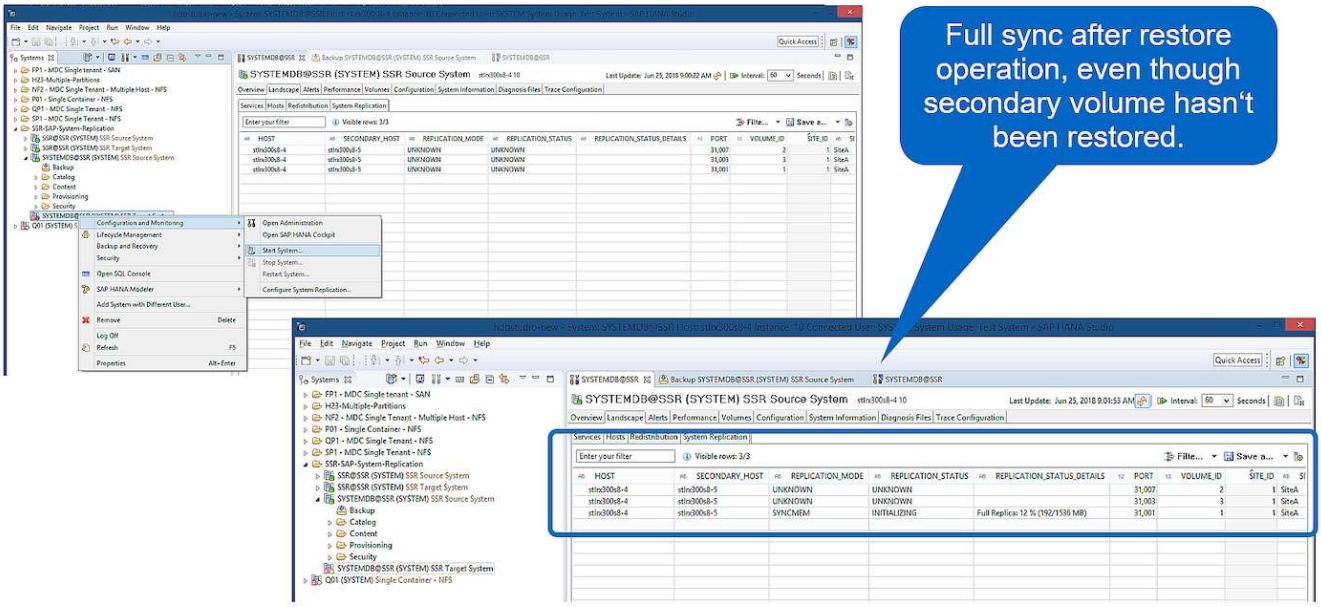
Nach der Wiederherstellung wird das Backup in SAP HANA Studio grün hervorgehoben. Sie müssen nicht einen zusätzlichen Log-Backup-Speicherort eingeben, weil der Dateipfad der Log-Backups von Host 1 und Host 2 im Backup-Katalog enthalten sind.





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

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

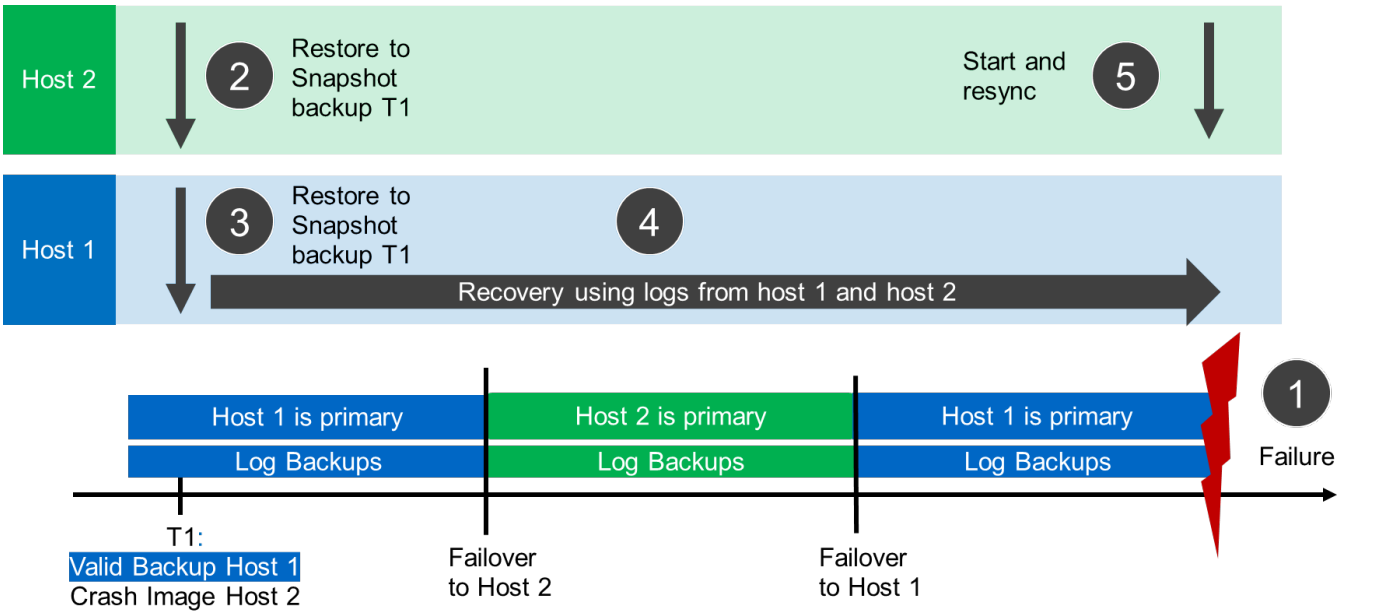


SnapCenter Restore von gültigem Backup- und Crash-Image

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

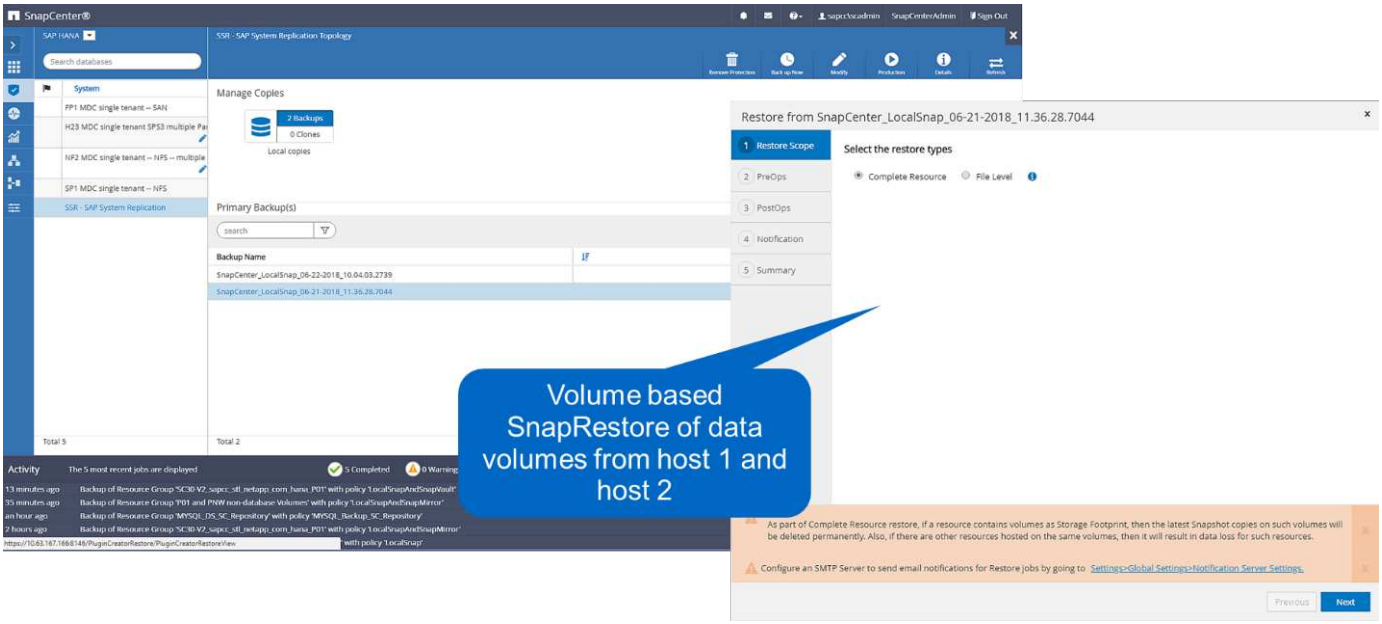
Bei T1 am Host 1 wurde ein Backup erstellt. Ein Failover wurde an Host 2 durchgeführt. Nach einem bestimmten Zeitpunkt wurde ein weiteres Failover zurück zu Host 1 durchgeführt. Zum aktuellen Zeitpunkt ist Host 1 der primäre Host.

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

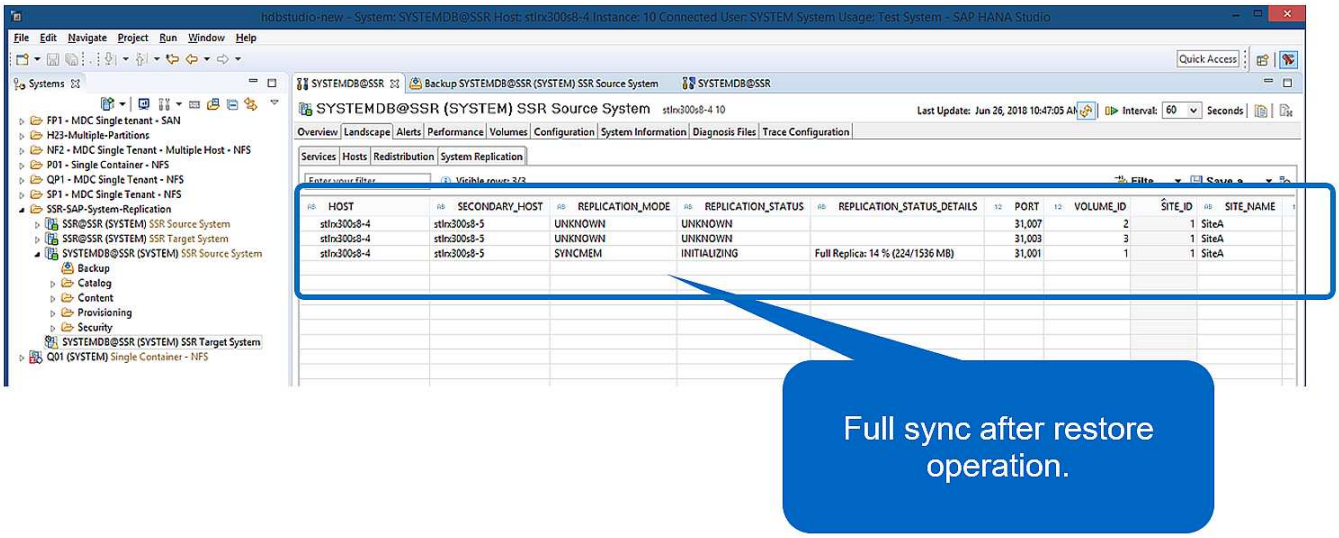


Der Wiederherstellungs- und Wiederherstellungsvorgang mit SAP HANA Studio ist identisch mit den im Abschnitt beschriebenen Schritten "SnapCenter Restore nur für gültige Backups".

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



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



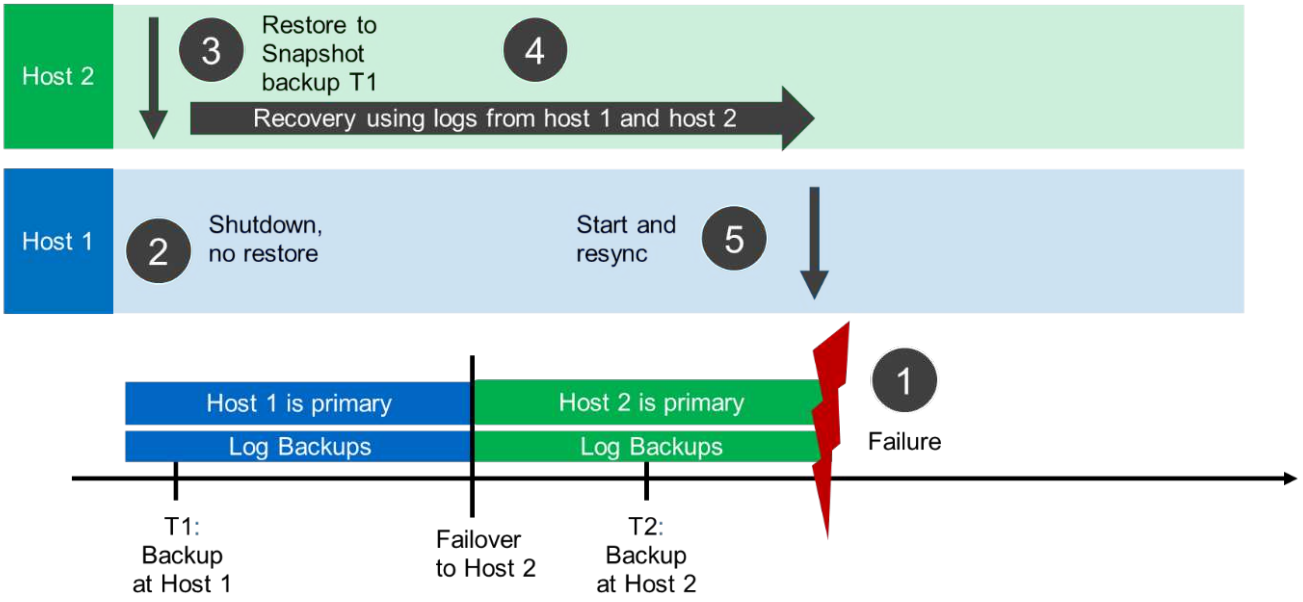
Wiederherstellung und Recovery von einem auf dem anderen Host erstellten Backup

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

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

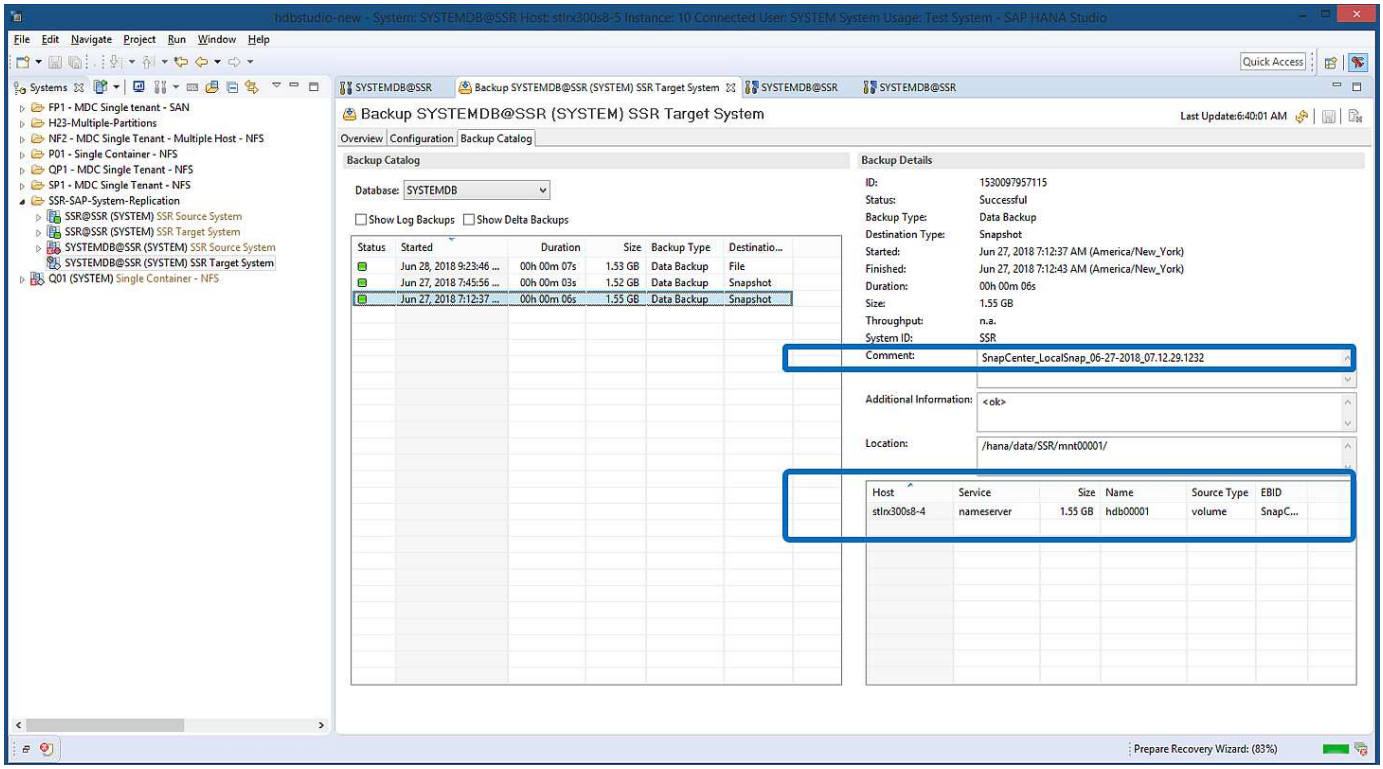
Bei T1 am Host 1 wurde ein Backup erstellt. Ein Failover wurde an Host 2 durchgeführt. Zum aktuellen Zeitpunkt ist Host 2 der primäre Host.

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



31

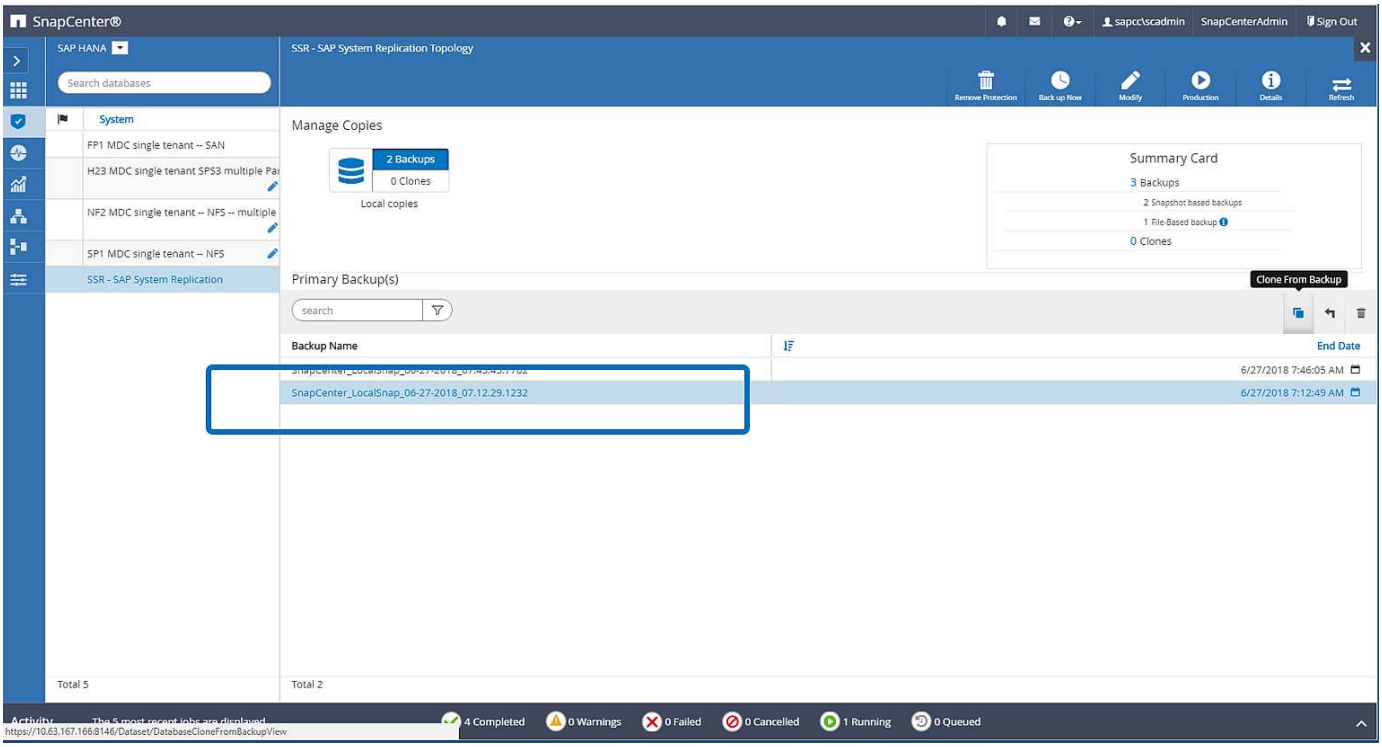
Die folgende Abbildung zeigt den SAP HANA Backup-Katalog und hebt das auf Host 1 erstellte Backup hervor, das für den Restore- und Recovery-Vorgang verwendet wurde.



Die Wiederherstellung umfasst die folgenden Schritte:

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

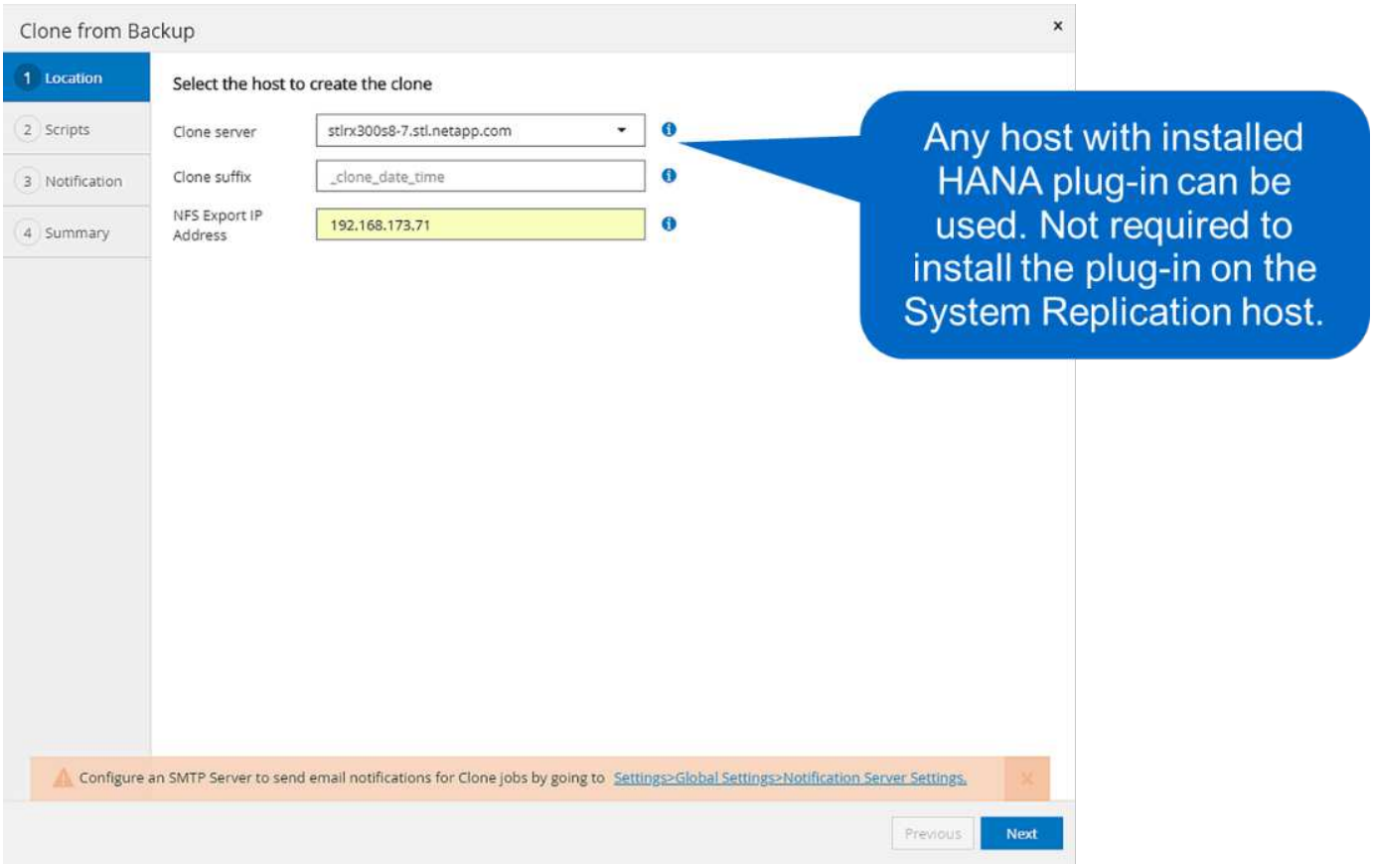
In SnapCenter wird das Backup ausgewählt und der Klonvorgang gestartet.



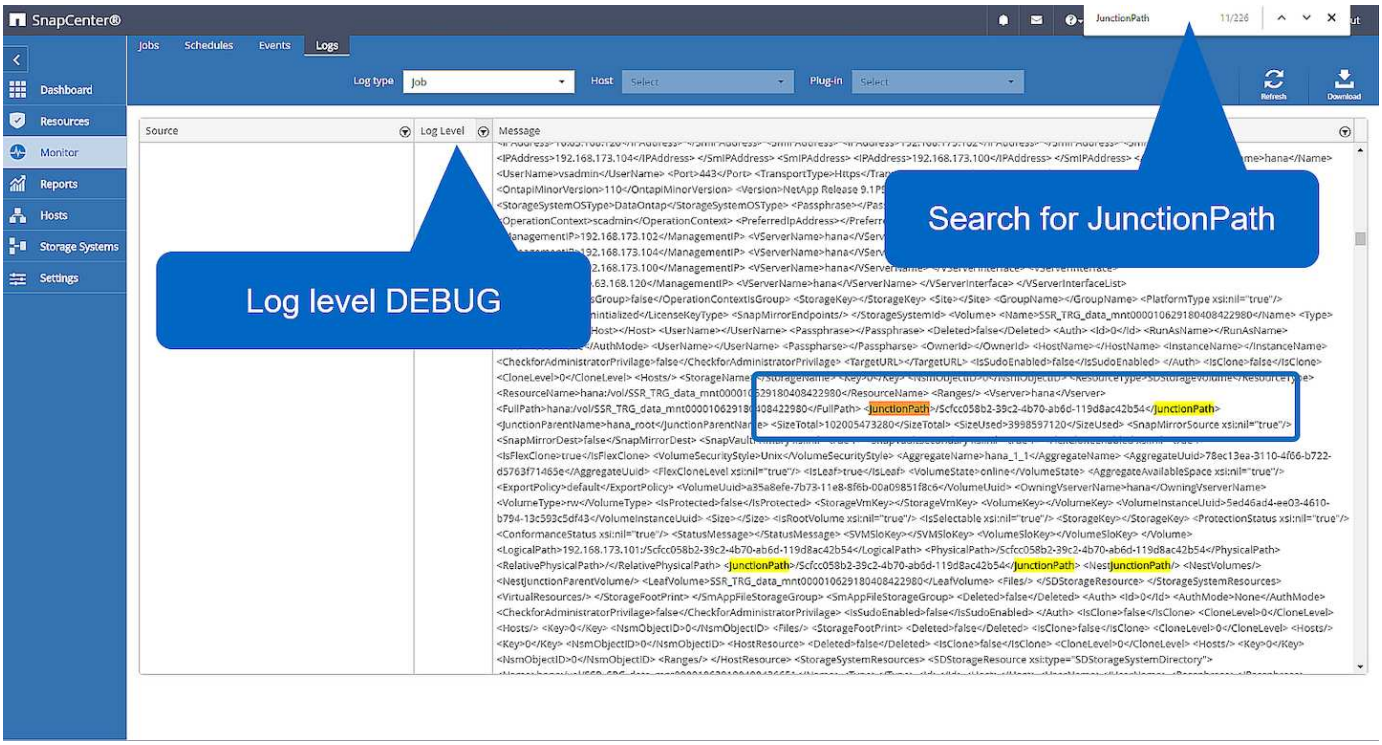
Sie müssen den Klon-Server und die NFS-Export-IP-Adresse angeben.

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

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



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



Das geklonte Volume kann jetzt angehängt werden.

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

Das geklonte Volume enthält die Daten der HANA-Datenbank.

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

Die Daten werden an den ursprünglichen Speicherort kopiert.

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

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

Wo Sie weitere Informationen finden

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

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

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

Versionsverlauf

Versionsverlauf:

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

Technischer Bericht: SAP HANA Disaster Recovery with Azure NetApp Files

TR-4891: SAP HANA Disaster Recovery mit Azure NetApp Files

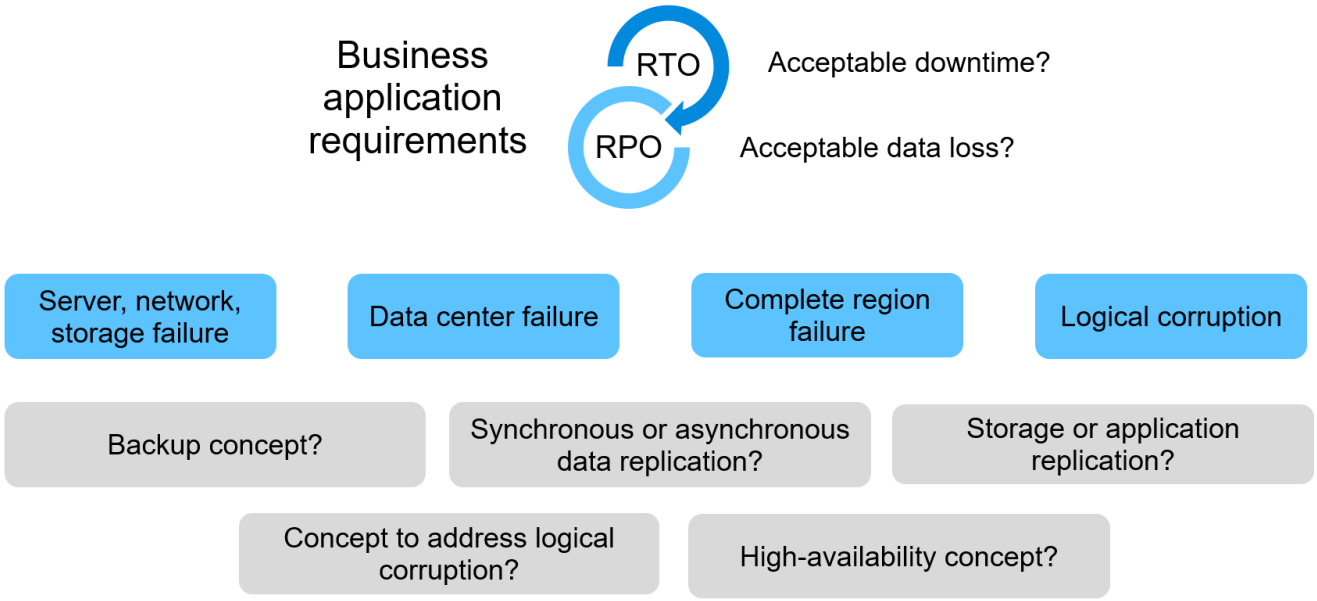
Studien haben gezeigt, dass Ausfallzeiten von Business-Applikationen erhebliche negative Auswirkungen auf das Geschäft von Unternehmen haben.

Autoren: Nils Bauer, NetApp Ralf Klahr, Microsoft

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.

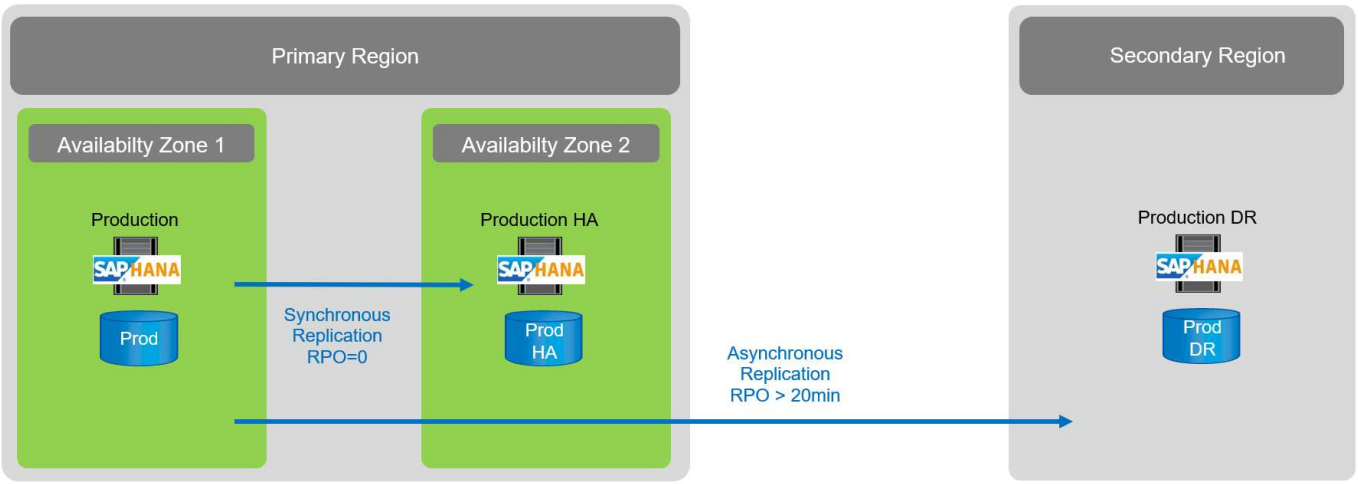
Disaster-Recovery-Lösungsvergleich

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.

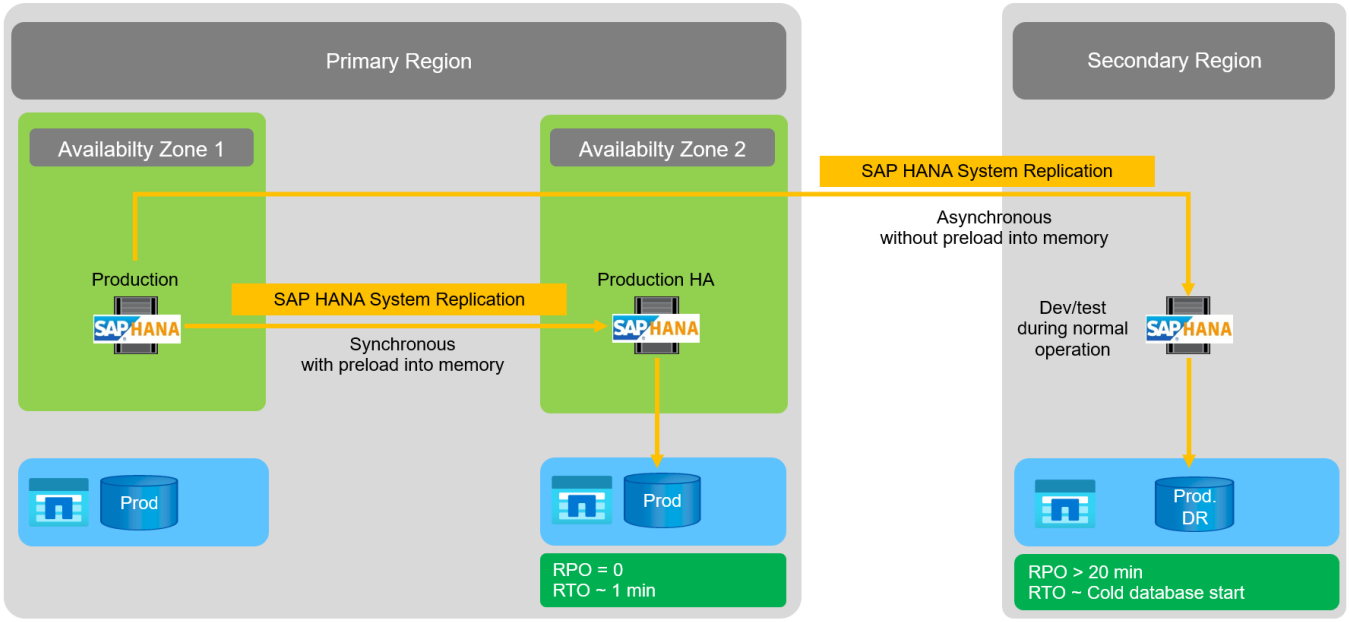
SAP HANA System Replication kann in einem von zwei Modi betrieben werden:

- 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.

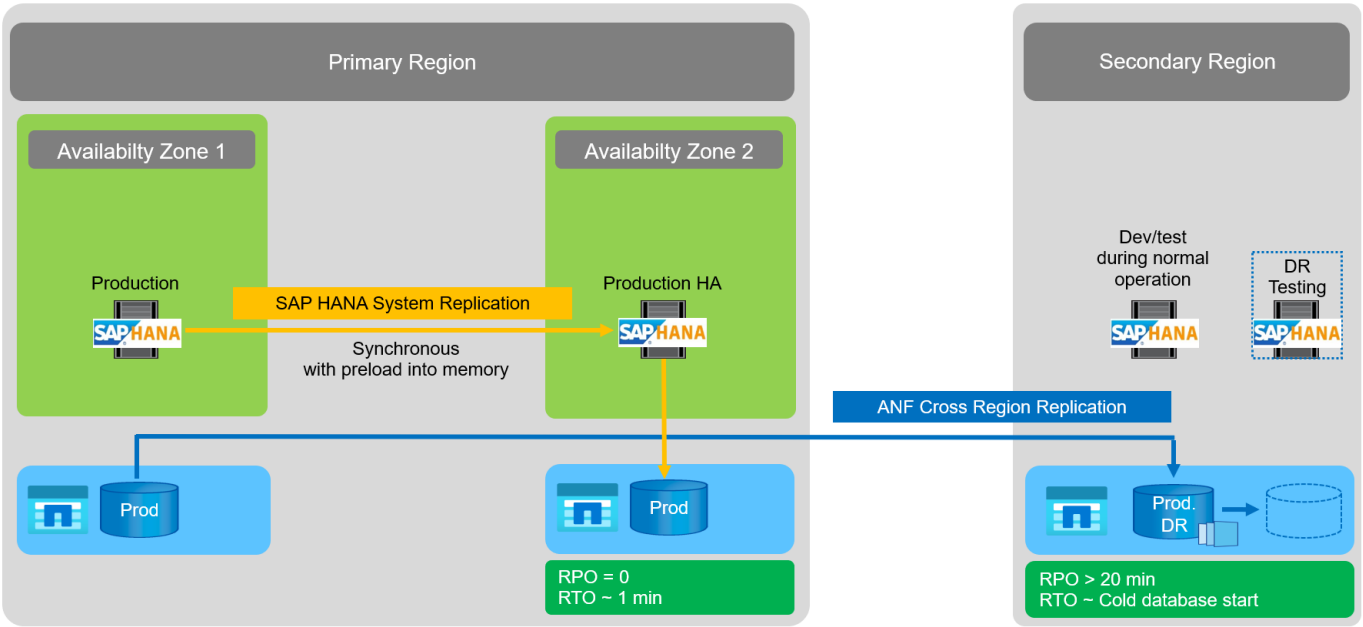
Die folgende Abbildung zeigt ein Beispiel für eine Disaster-Recovery-Lösung für zwei Regionen mithilfe von ANF-bereichsübergreifender Replizierung. In diesem Beispiel ist das HANA-System mit HANA System Replication innerhalb der primären Region geschützt, wie im vorherigen Kapitel erläutert. Die Replikation 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 regionsübergreifenden Replikation finden Sie an folgendem Speicherort.

"Azure NetApp Files Dokumentation – Microsoft Docs" In den Abschnitten Konzepte 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.

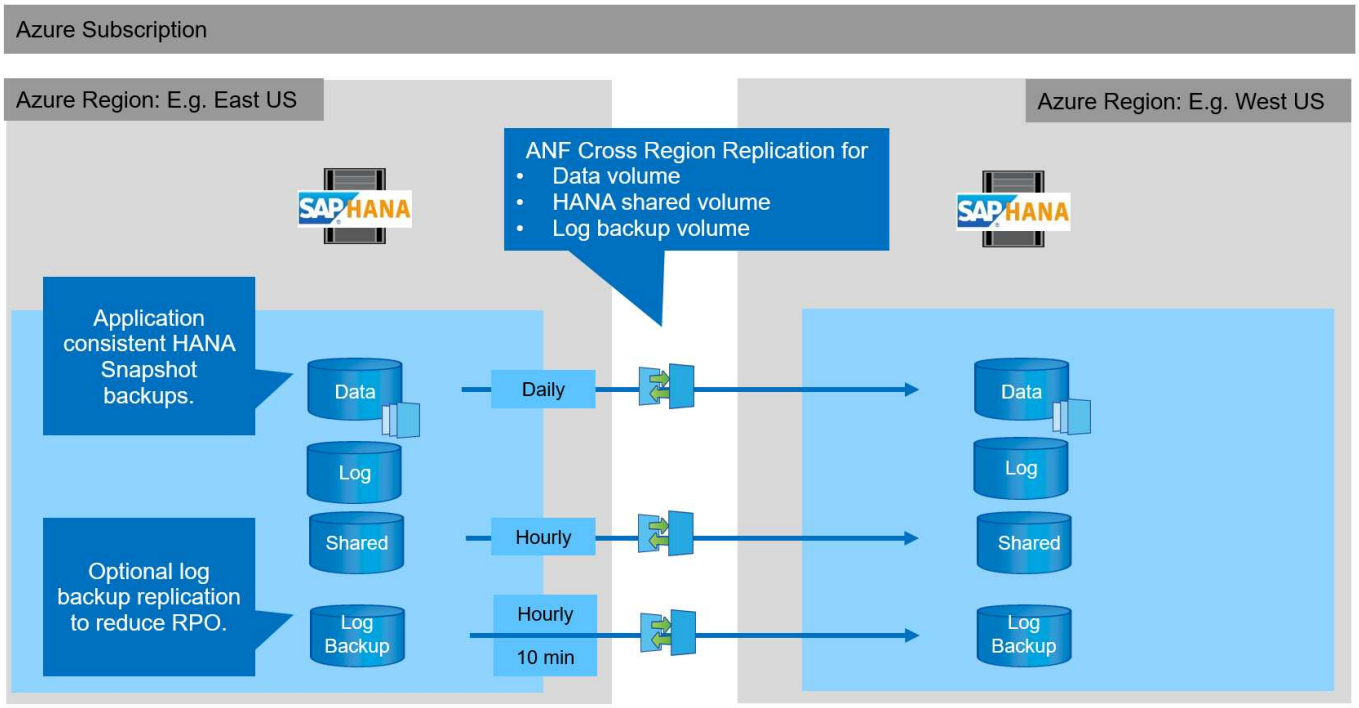
> ⓘ Der in diesem Dokument verwendete Begriff „Protokollsicherung“ umfasst die Protokollsicherung und die Sicherung des HANA-Backup-Katalogs. Der HANA-Backup-Katalog ist erforderlich, um Recovery-Vorgänge durchzuführen.

> ⓘ 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. Das 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

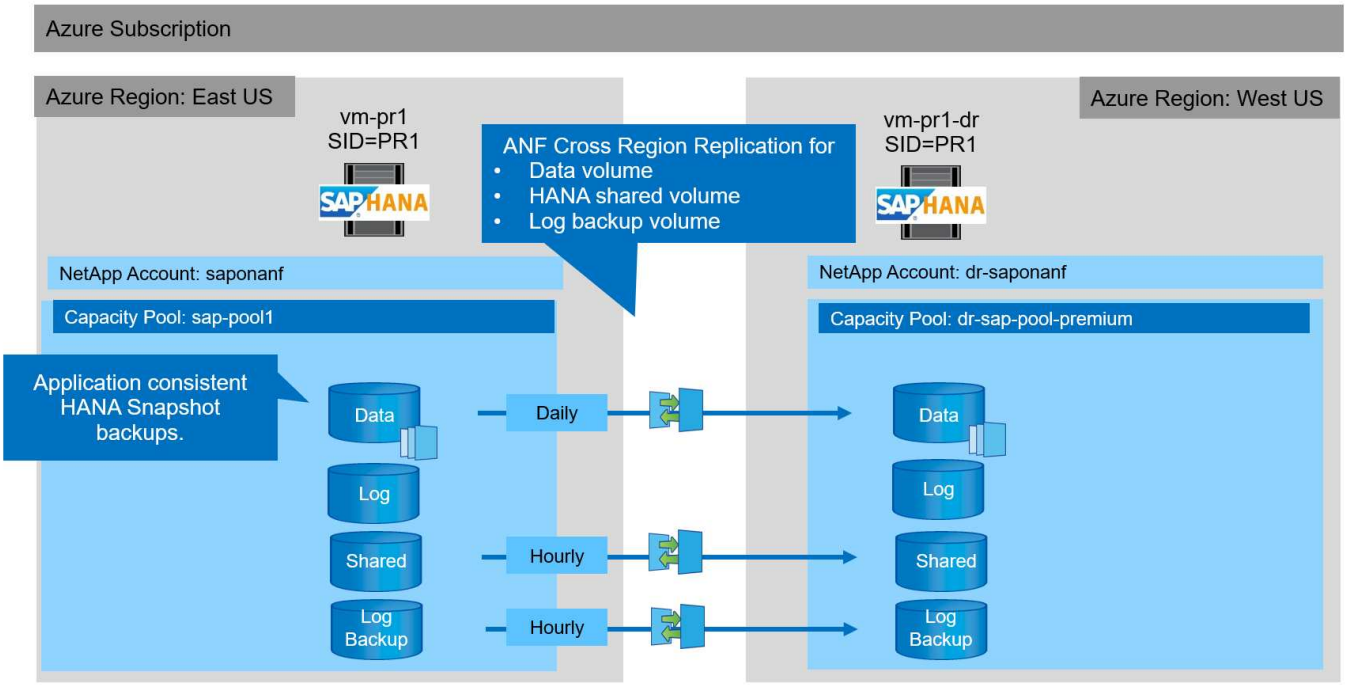
Die Lösungsvalidierung wurde mit einem Single-Host-System für SAP HANA durchgeführt. Das Microsoft AzAcSnap Snapshot Backup-Tool für ANF wurde verwendet, um applikationskonsistente HANA Snapshot Backups zu konfigurieren. Es wurden ein tägliches Datenvolumen, ein stündliches Log Backup und die gemeinsame 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.

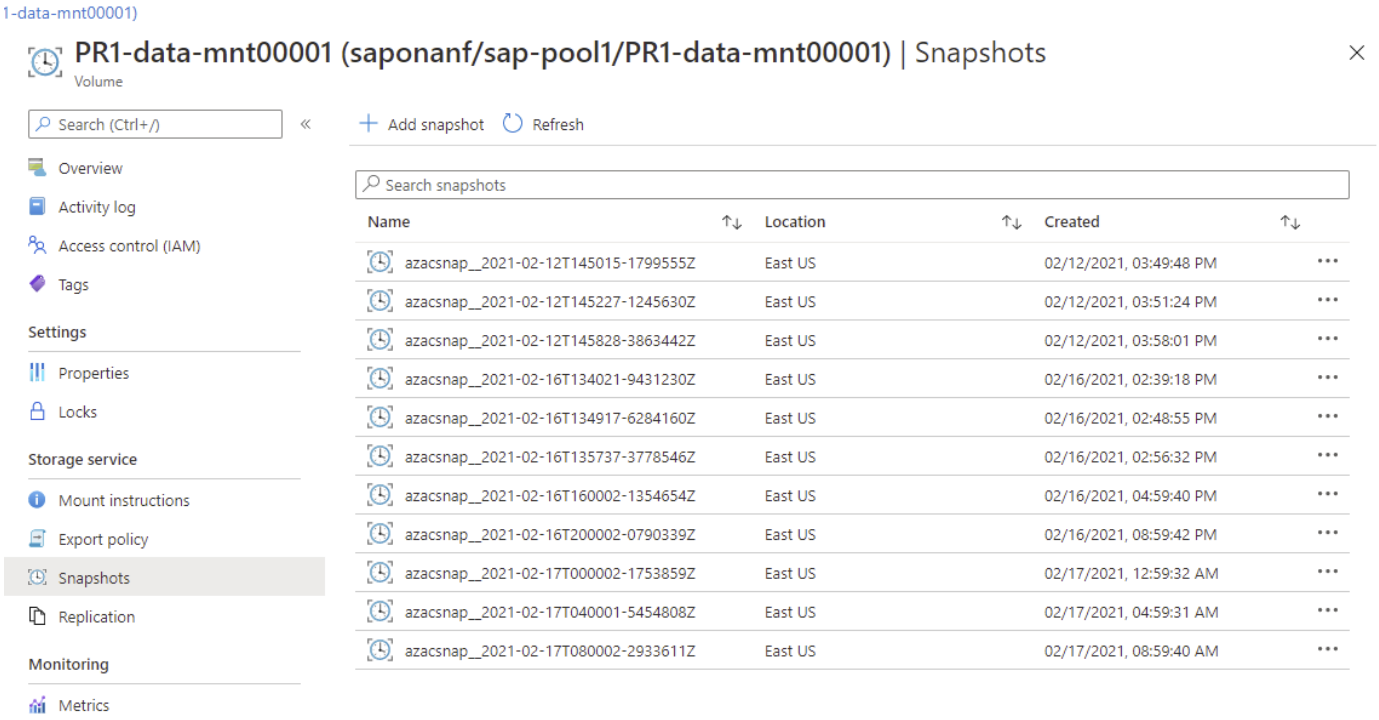


Snapshot Backup-Konfiguration mit AzAcSnap

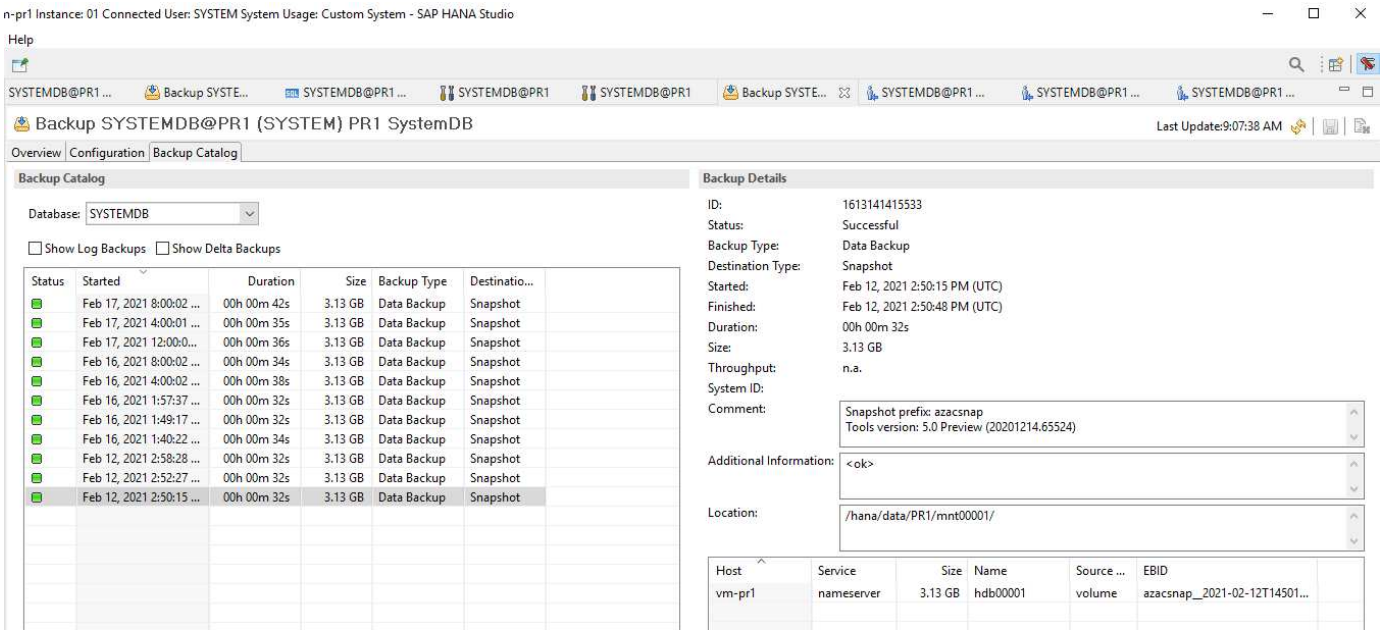
Am primären Standort wurde AzAcSnap für die Erstellung applikationskonsistenter Snapshot-Backups des HANA-Systems PR1 konfiguriert. Diese Snapshot-Backups sind im ANF-Datenvolumen des PR1 HANA Systems verfügbar und sind auch im SAP HANA Backup-Katalog registriert, wie in den beiden folgenden Abbildungen 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:

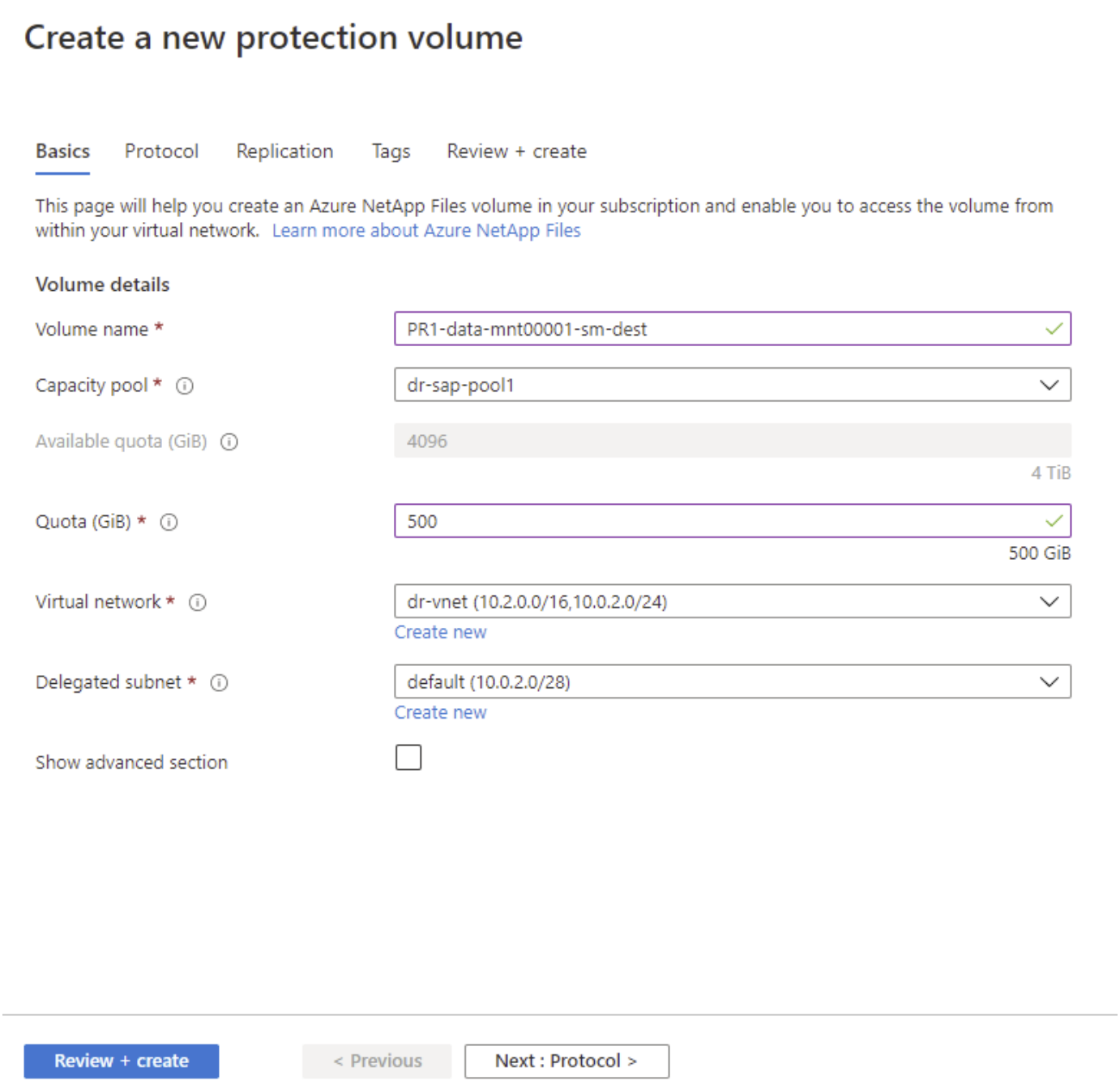
1. Erstellen eines neuen Sicherungs-Volumes am DR-Standort:
   a. Stellen Sie Volume-Namen, den Kapazitäts-Pool, die Quota- und Netzwerkinformationen bereit.
   b. Bereitstellen der Zugriffsinformationen für Protokolle und Volumes
   c. Geben Sie die Quell-Volume-ID und einen Replizierungsplan an.
   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.

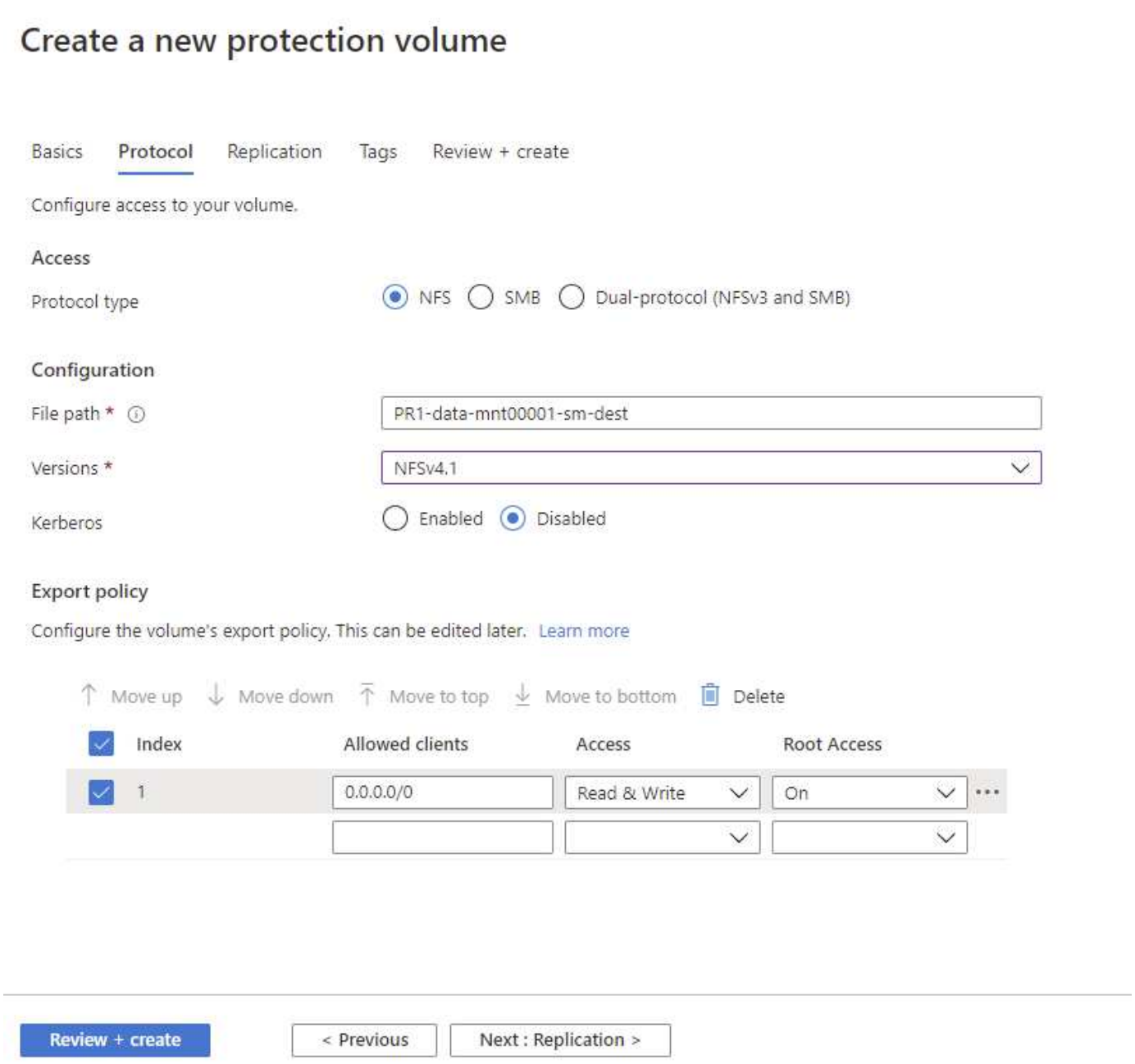
> Das Kontingent kann auf Basis der Kapazitätsanforderungen festgelegt werden, da die Volume-Performance sich nicht auf den Replizierungsprozess auswirkt. Bei einem Disaster Recovery-Failover muss die Quote an die tatsächlichen Performance-Anforderungen angepasst werden.

> 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.



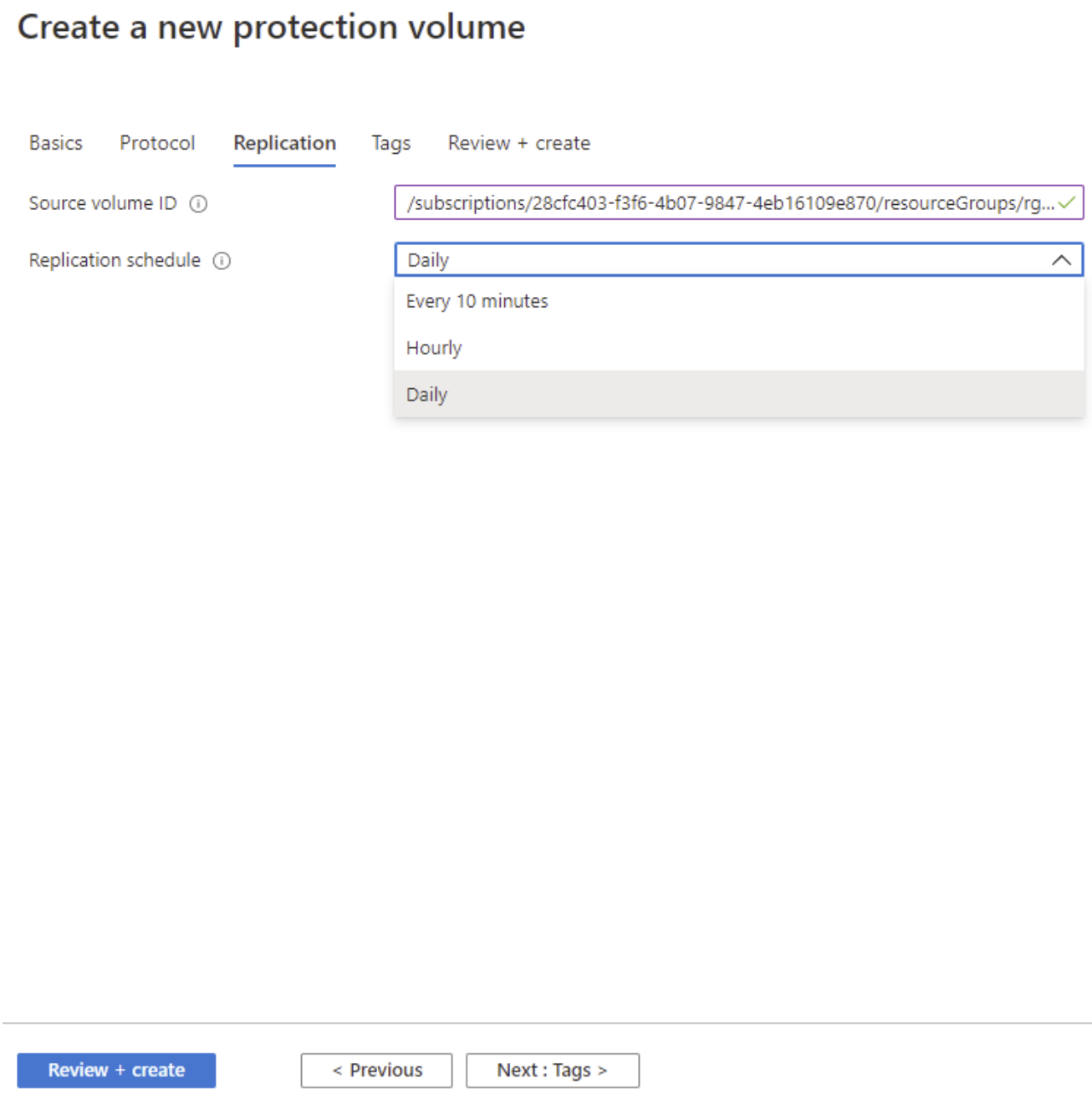
Auf der Registerkarte Protokoll müssen Sie das Netzwerkprotokoll, den Netzwerkpfad und die Exportrichtlinie angeben.

Das Protokoll muss dasselbe sein wie das für das Quell-Volume verwendete Protokoll.



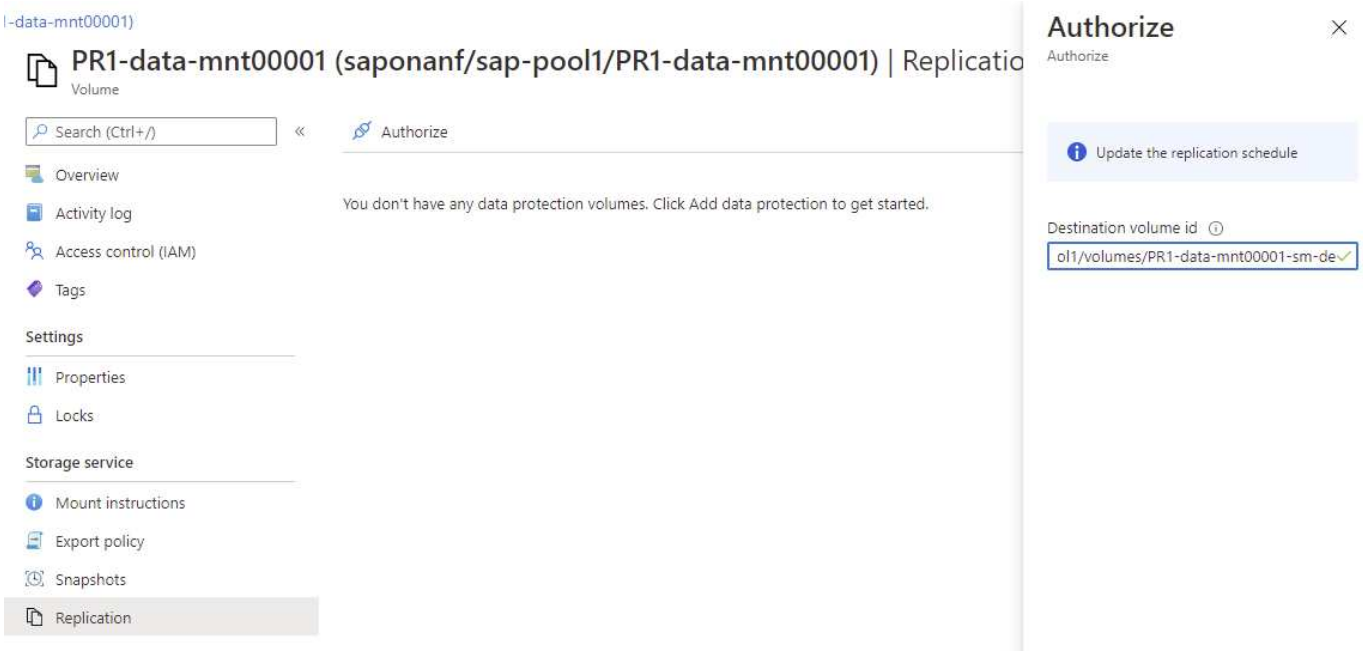
Auf der Registerkarte „Replikation“ müssen Sie die Quell-Volume-ID und den Replizierungsplan konfigurieren. Für die Datenreplizierung mit Daten-Volumes haben wir einen täglichen Replizierungszeitplan für unsere Einrichtung im Labor konfiguriert.

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.

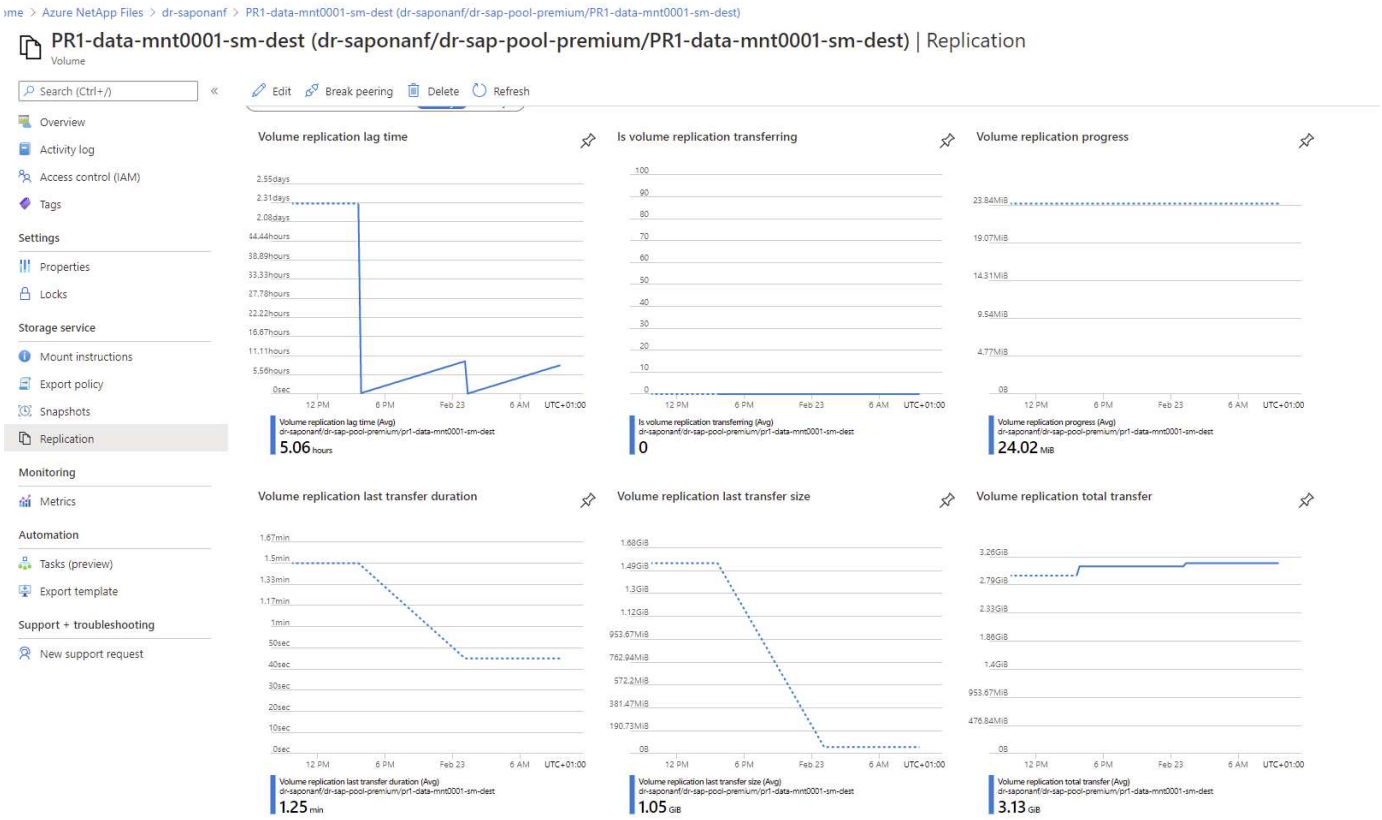
Überwachung der standortübergreifenden ANF-Replikation

Die folgenden drei Screenshots zeigen den Replikationsstatus für die Daten, Backup-Protokollierung und gemeinsam genutzte Volumes.

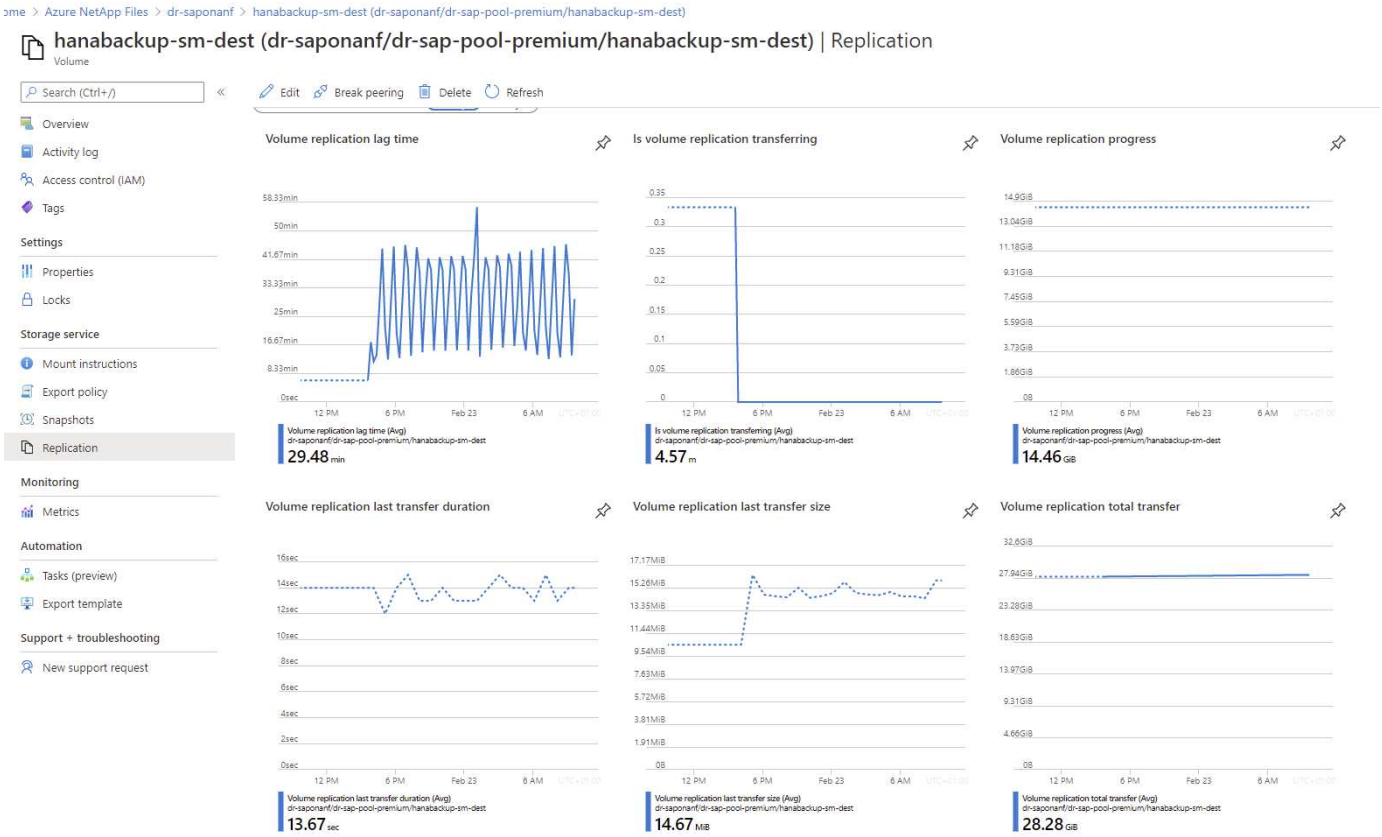
Die Verzögerung bei der Volume-Replizierung ist ein nützlicher Wert, um die RPO-Erwartungen zu verstehen. Beispielsweise zeigt die Replizierung des Backup-Volumes für das Protokoll eine maximale Verzögerungszeit von 58 Minuten, das heißt, dass der maximale RPO den gleichen Wert hat.

Die Übertragungsdauer und Übertragungsgröße bieten wertvolle Informationen zu den Bandbreitenanforderungen und ändern die Rate des replizierten Volumes.

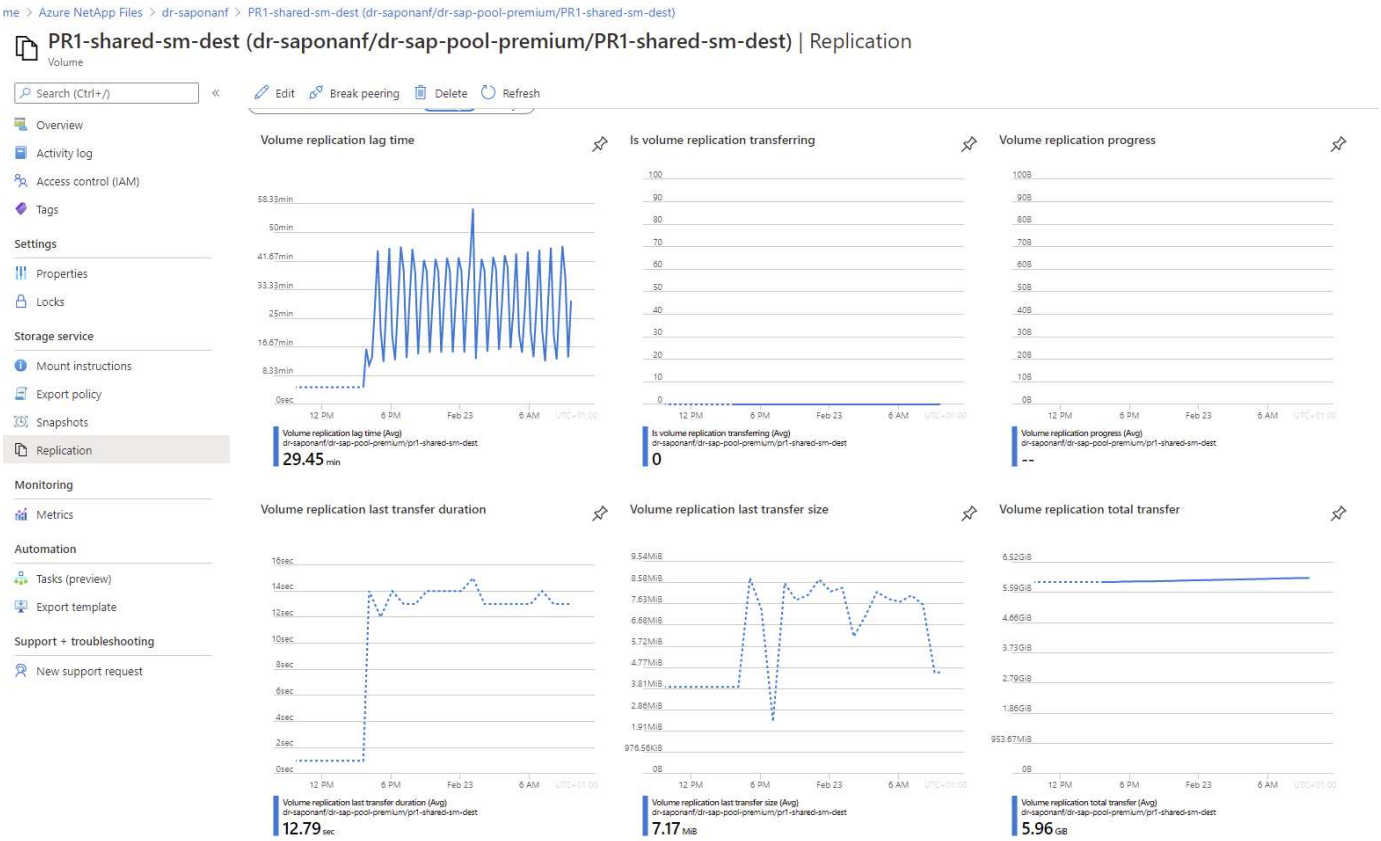
Der folgende Screenshot zeigt den Replizierungsstatus eines HANA Daten-Volumes.



Der folgende Screenshot zeigt den Replizierungsstatus eines HANA-Protokoll-Backup-Volumes.



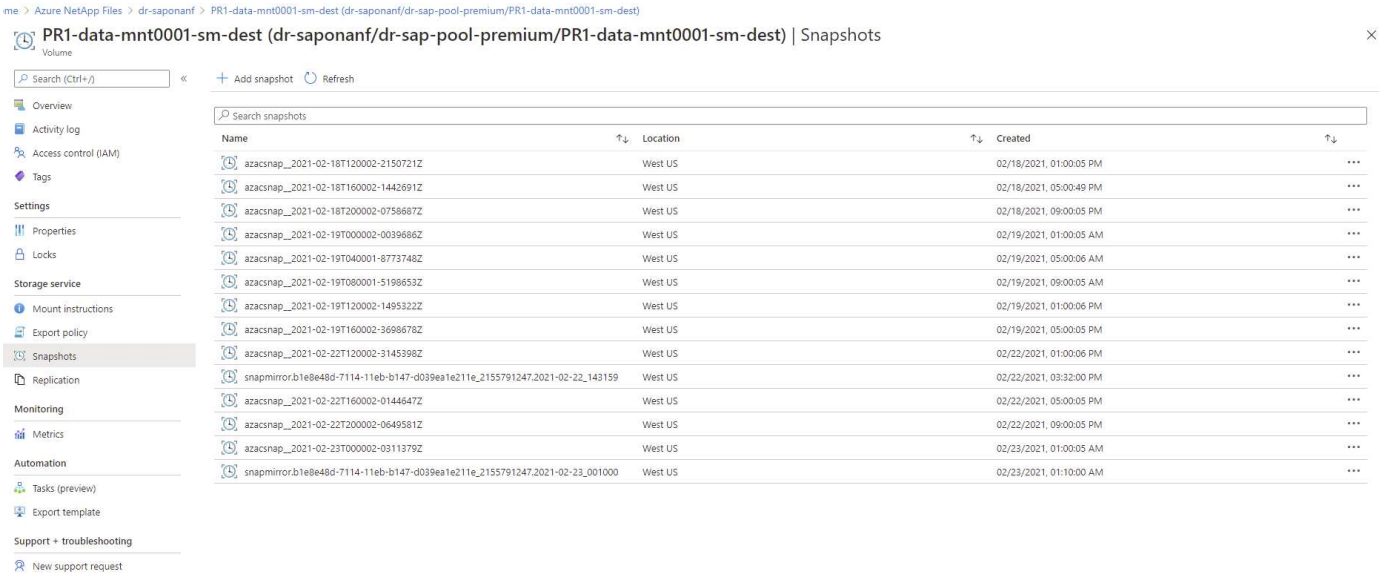
Der folgende Screenshot zeigt den Replizierungsstatus von einem Shared HANA Volume.



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.

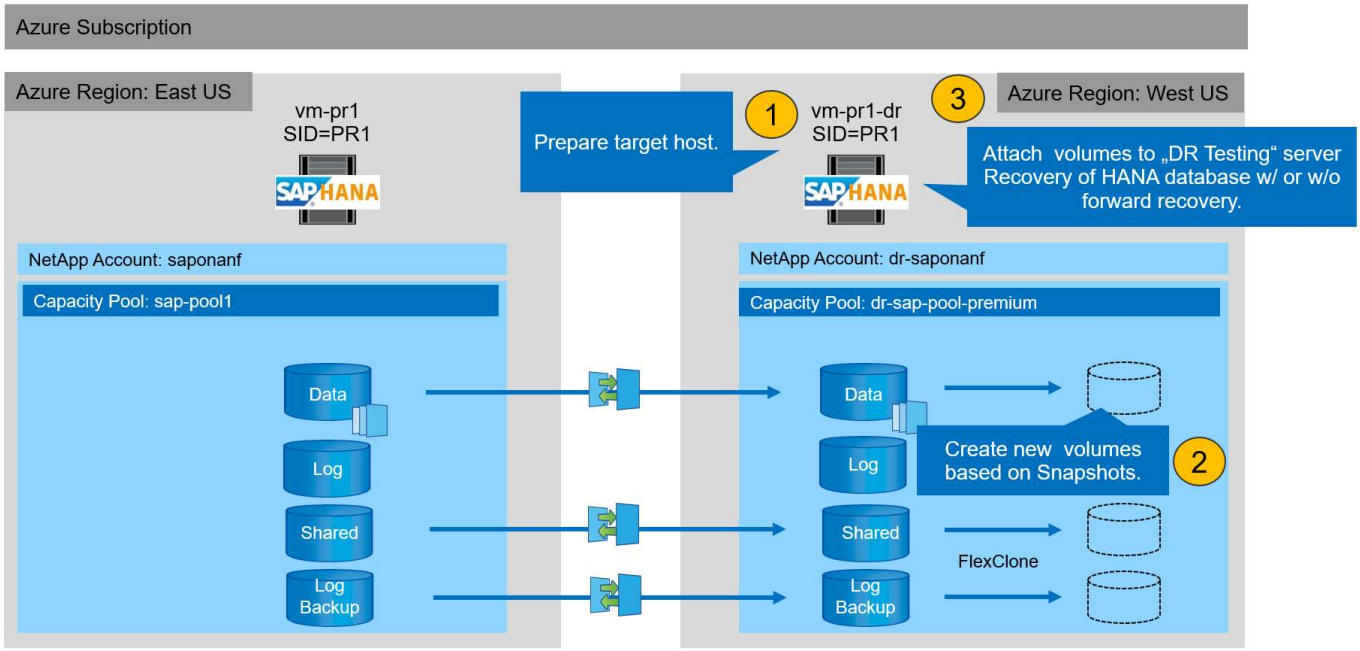
Der Workflow für Disaster Recovery-Tests nutzt die ANF-Funktionen, um auf Basis vorhandener Snapshot-Backups am Disaster-Recovery-Ziel neue Volumes zu erstellen. Siehe "Wie Azure NetApp Files Snapshots funktionieren - Microsoft Docs".

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

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.

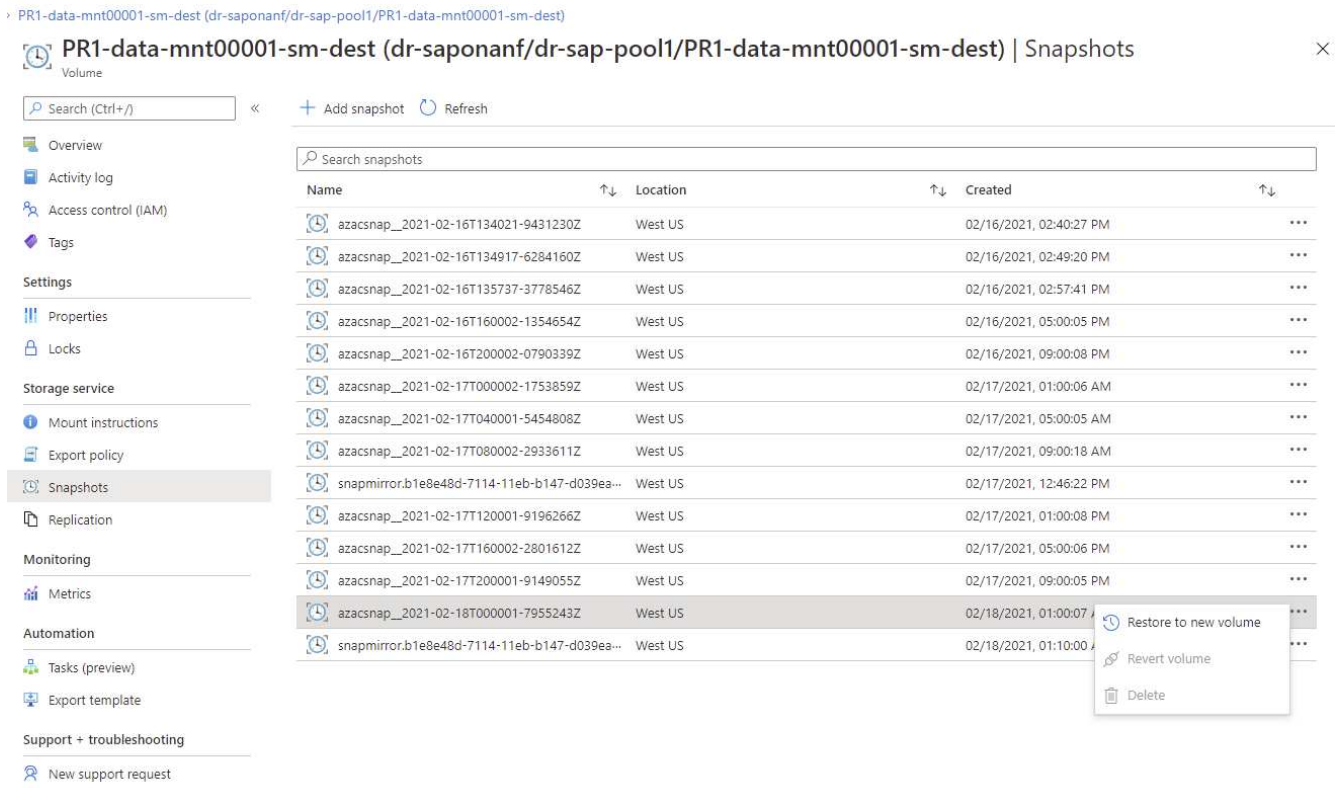
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
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
```

Erstellen Sie neue Volumes auf Basis von Snapshot-Backups am Disaster-Recovery-Standort

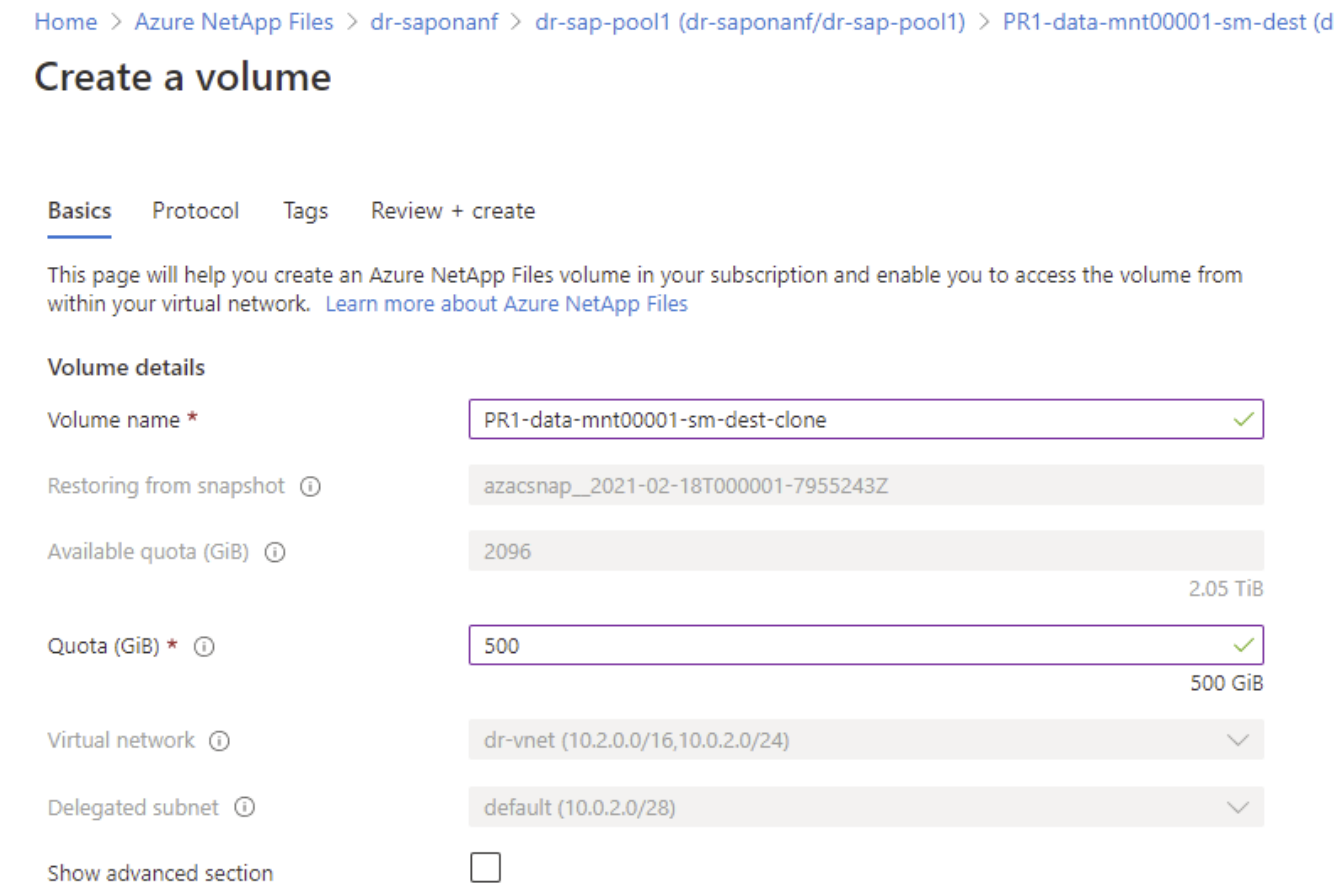
Abhängig vom Disaster Recovery Setup (mit oder ohne Log-Backup-Replikation) müssen zwei oder drei neue Volumes auf der Basis von Snapshot-Backups erstellt werden. In beiden Fällen muss ein neues Volume der Daten und das gemeinsame HANA Volume erstellt werden.

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.

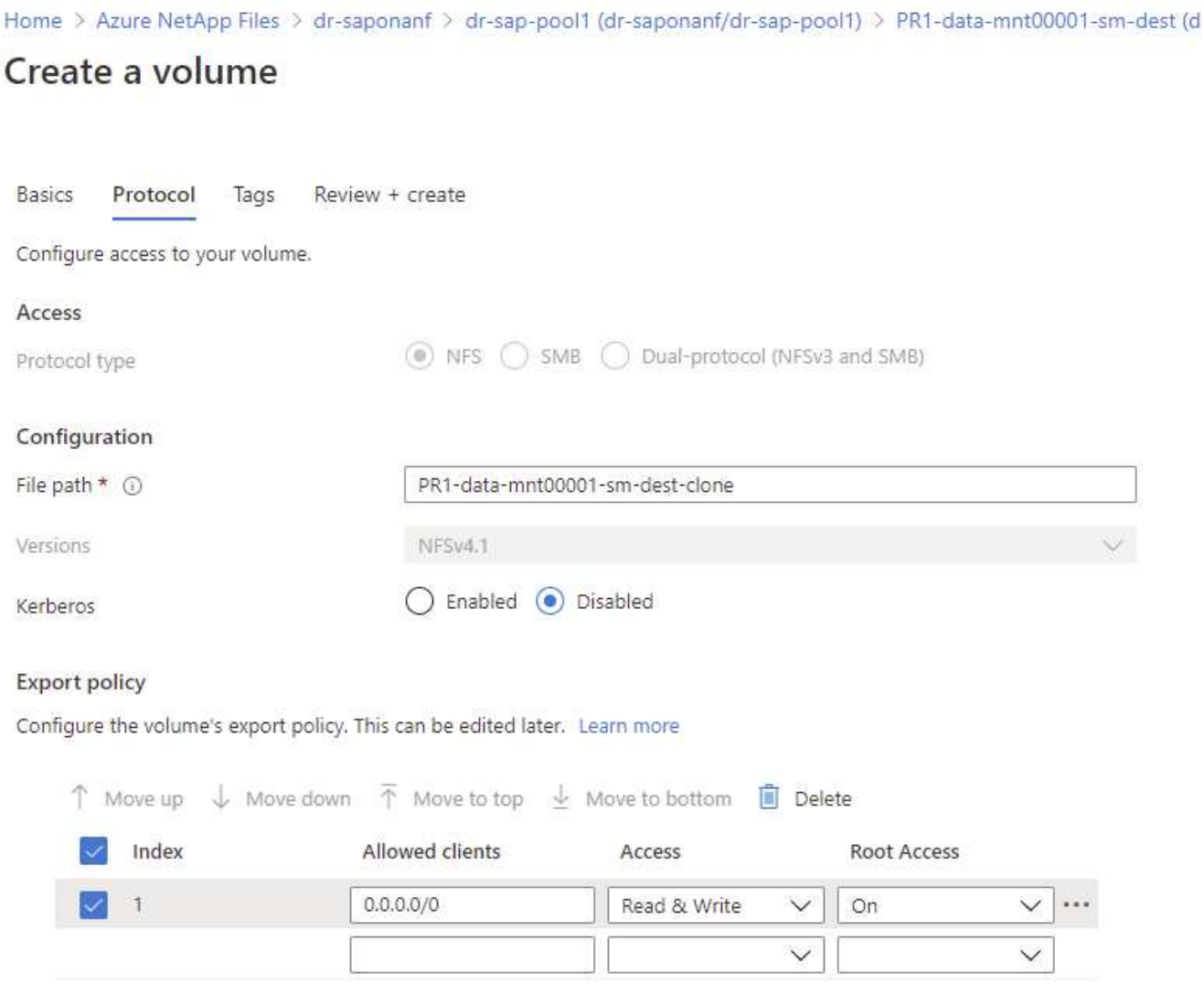
1. Eines der applikationskonsistenten Snapshot-Backups wird als Quelle für das neue Volume des HANA-Daten-Volumes ausgewählt. Restore to New Volume ist ausgewählt, um ein neues Volume basierend auf der Snapshot-Sicherung zu erstellen.



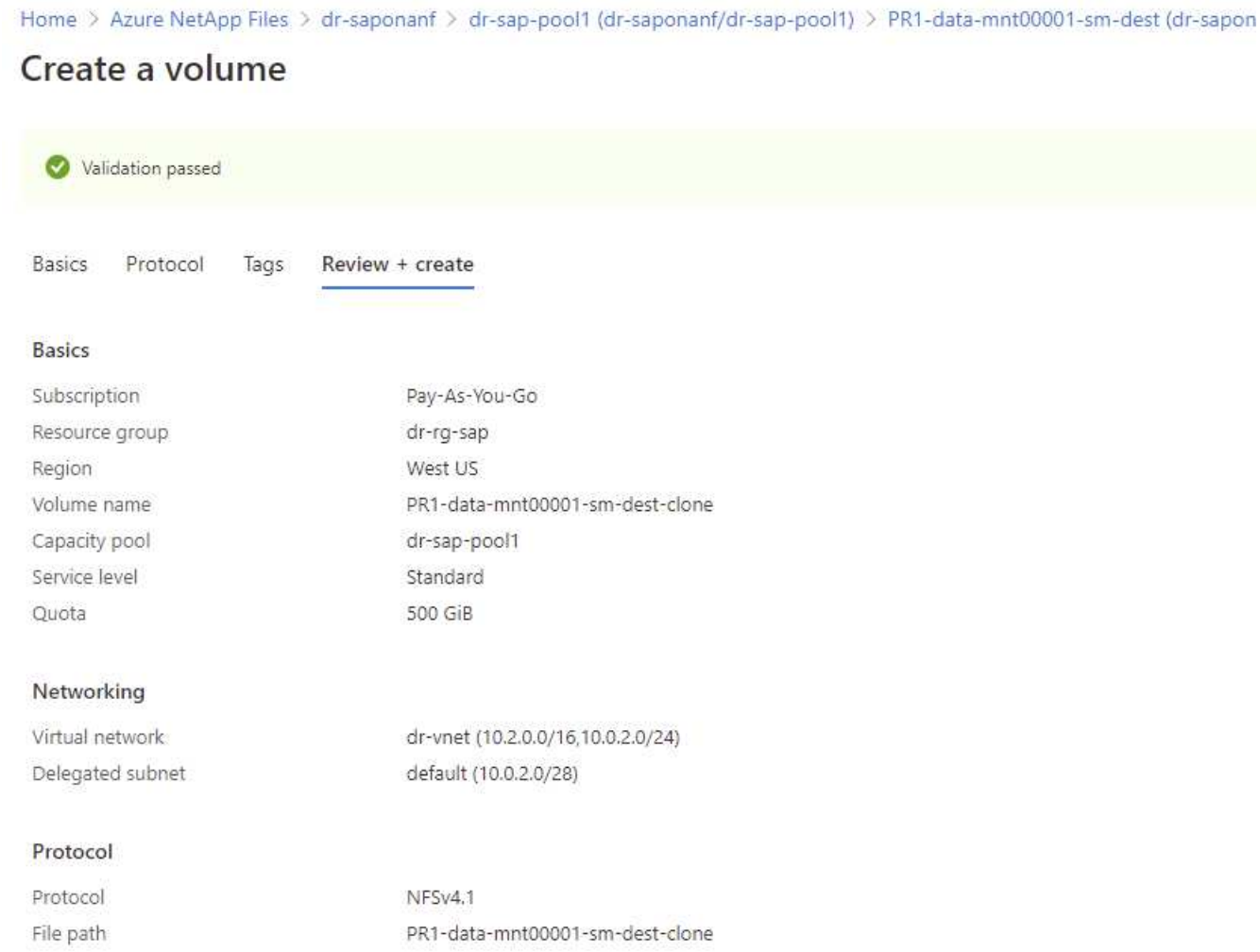
2. Der neue Volume-Name und die neue Quote müssen in der Benutzeroberfläche angegeben werden.



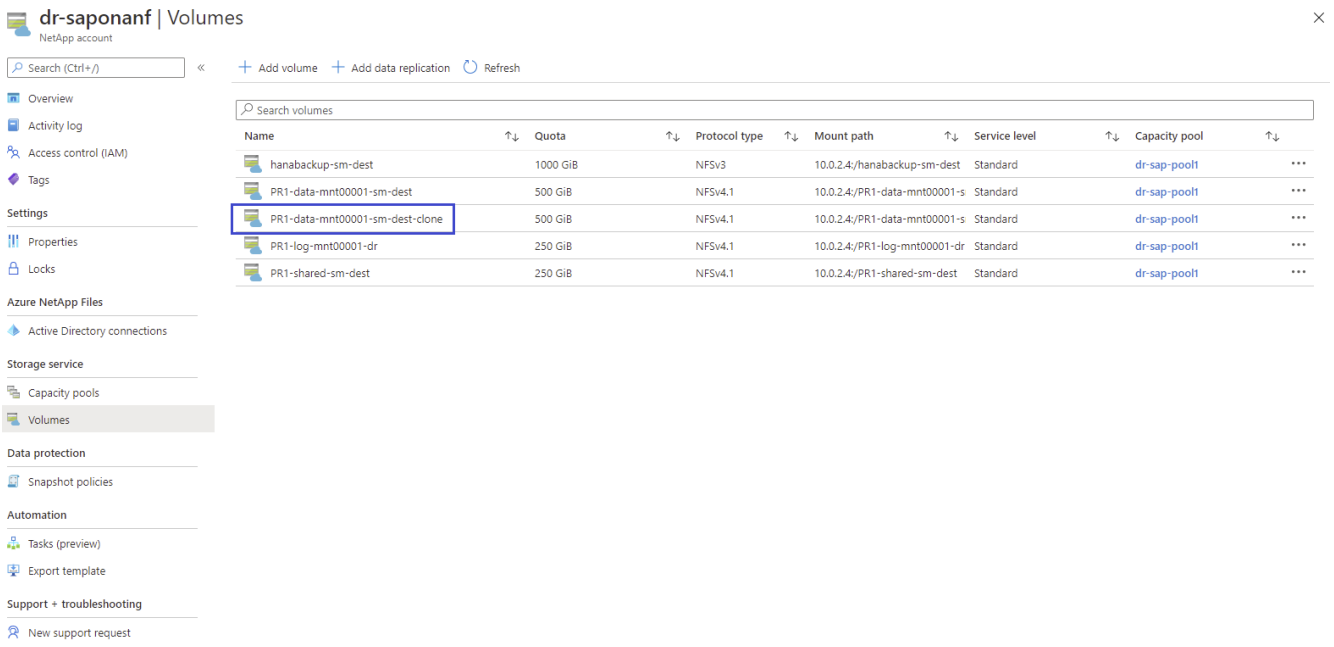
3. Auf der Registerkarte Protokoll werden der Dateipfad und die Exportrichtlinie konfiguriert.



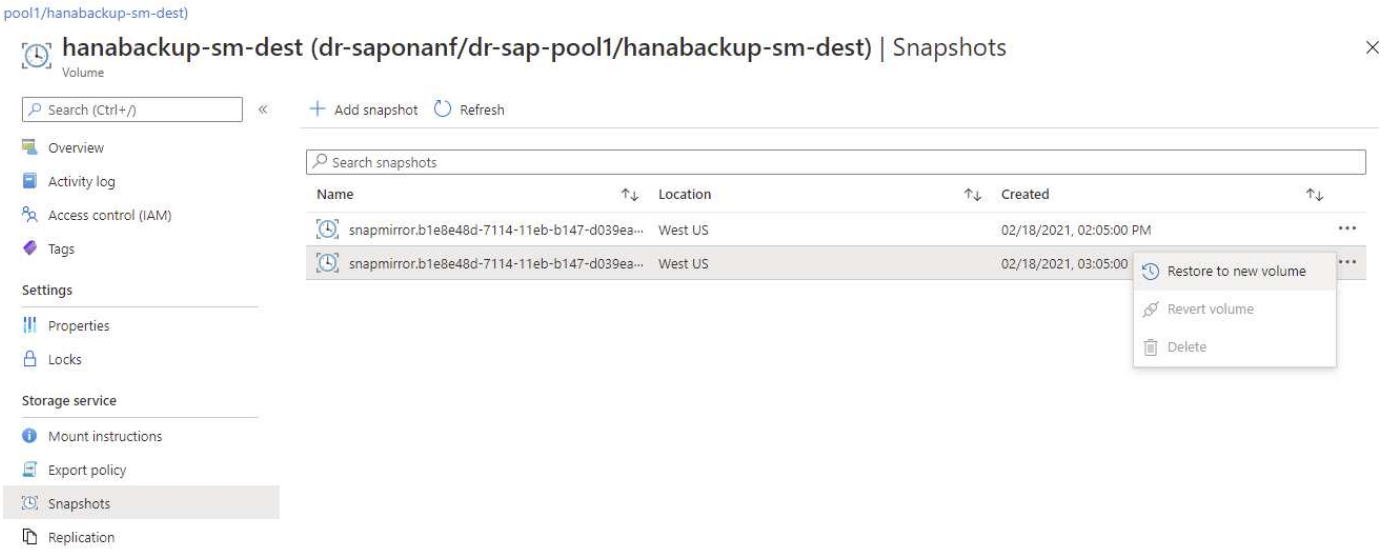
4. Der Bildschirm Erstellen und Prüfen fasst die Konfiguration zusammen.



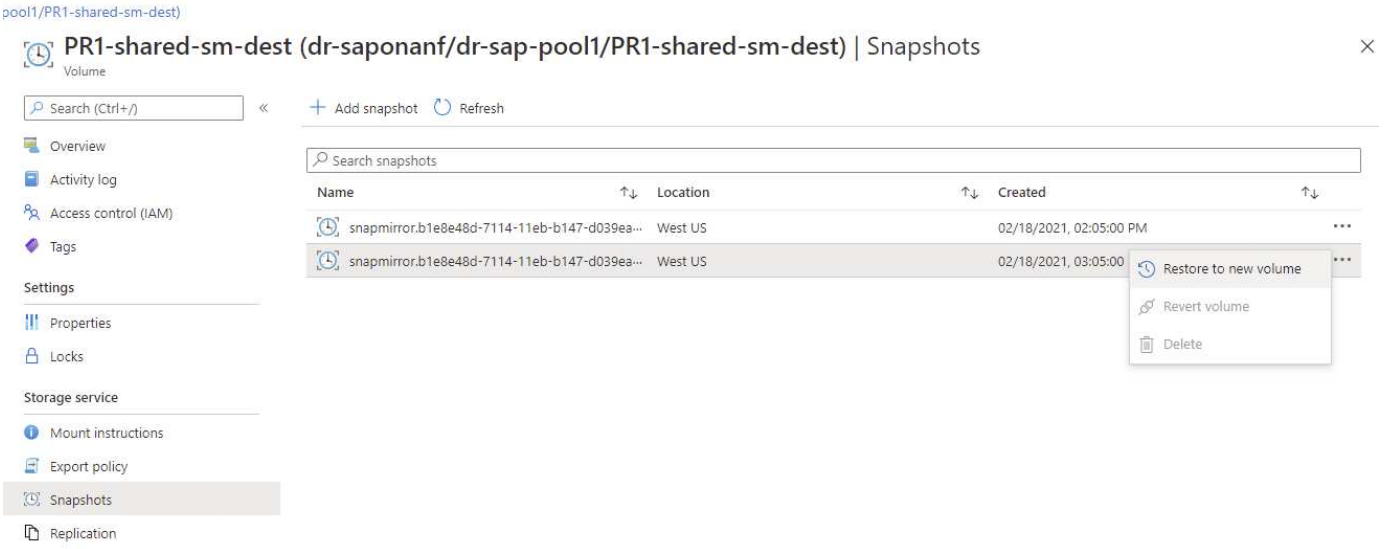
5. Auf Basis des HANA-Snapshot-Backups wurde jetzt ein neues Volume erstellt.



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

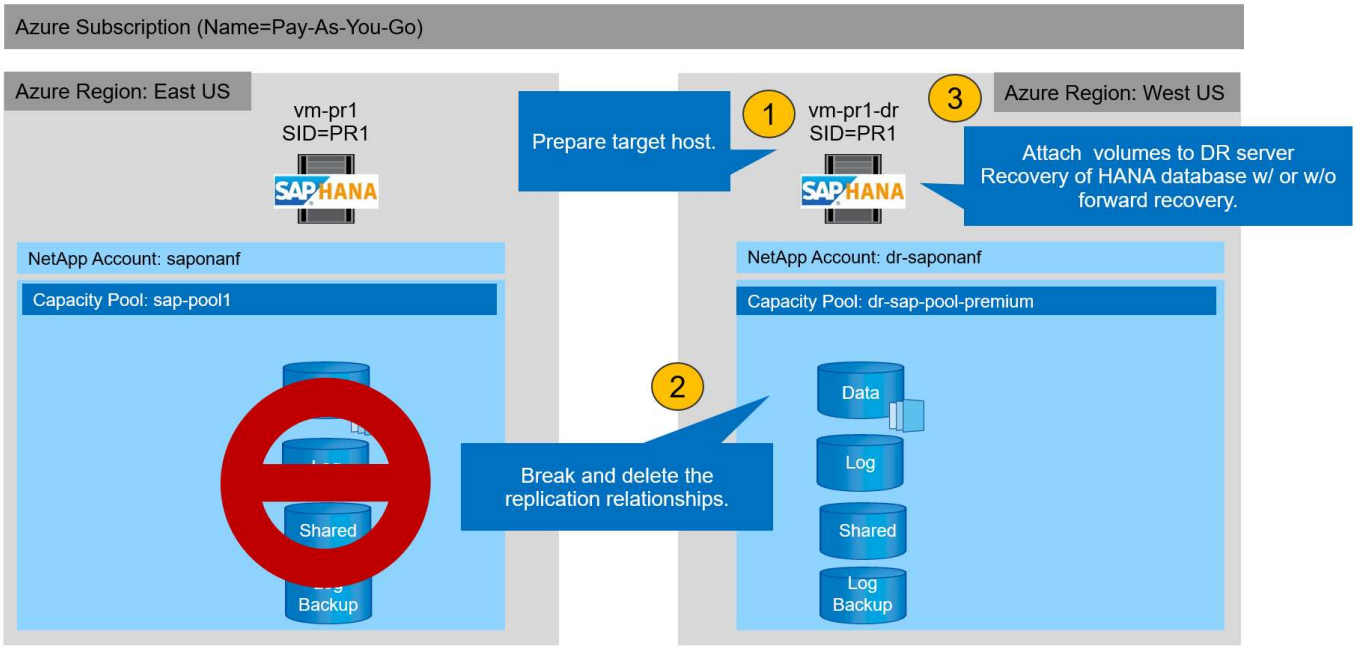
Je nachdem, ob die Backup-Replizierung des Protokolls Teil der Disaster Recovery-Einrichtung ist, unterscheiden sich die Schritte für Disaster Recovery leicht. In diesem Abschnitt wird das Disaster Recovery Failover für die reine Daten-Backup-Replizierung sowie für die Replizierung von Daten-Volumes 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.

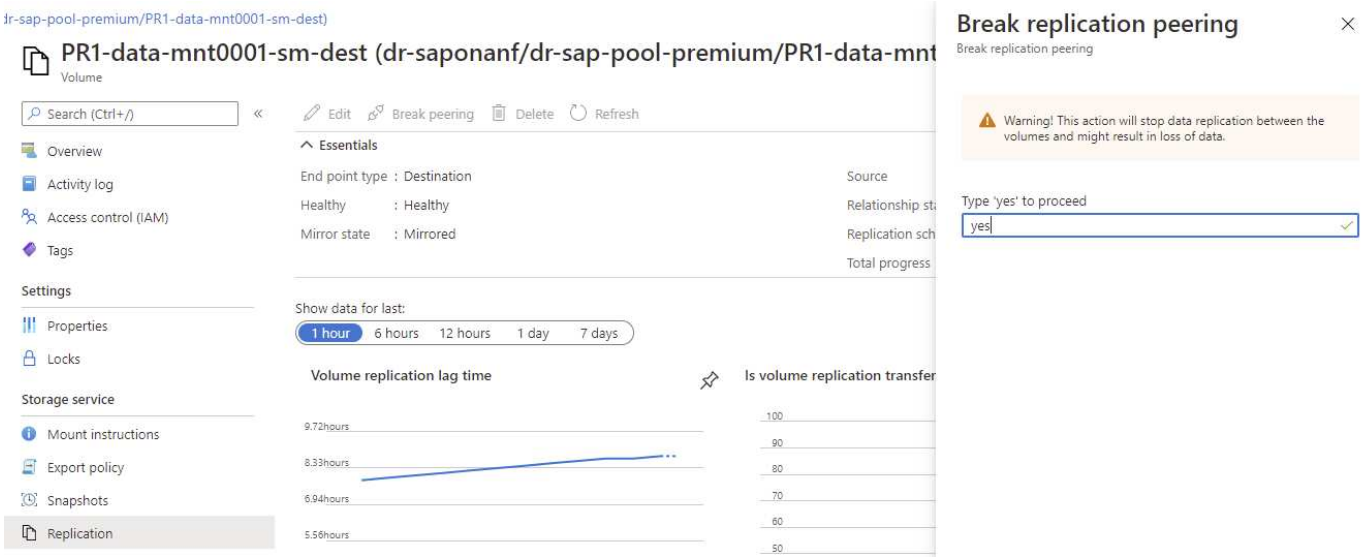
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
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
```

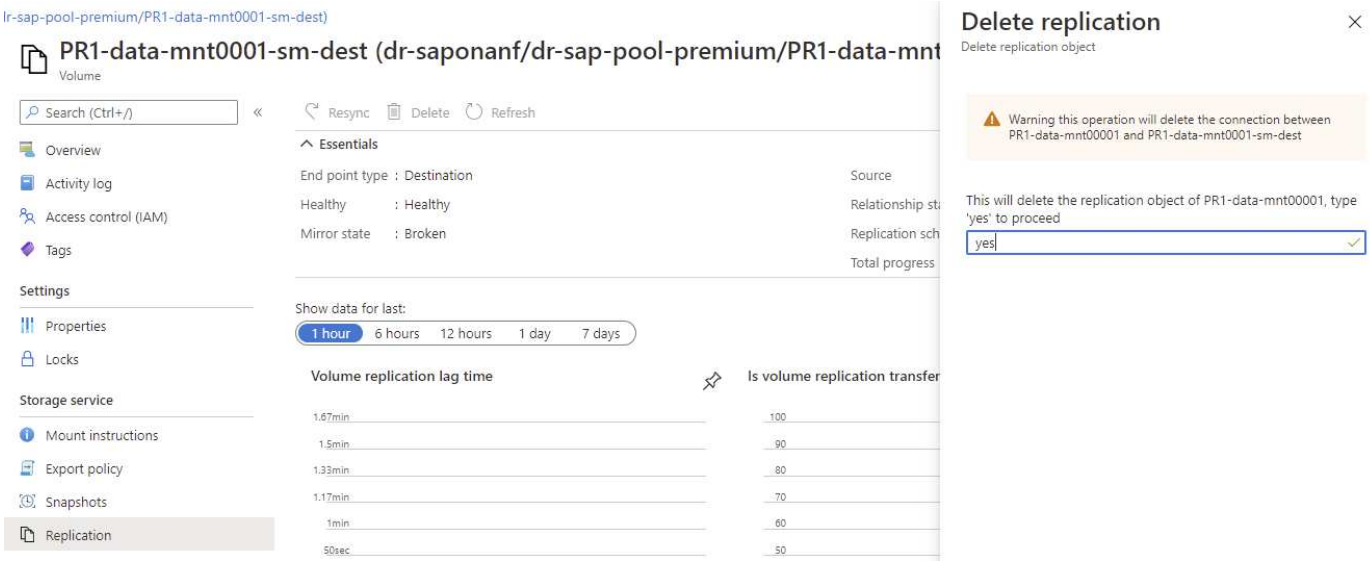
Peering der Replizierung unterbrechen und löschen

Im Falle eines Disaster-Failovers müssen die Ziel-Volumes unterbrochen werden, damit der Zielhost die Volumes für Lese- und Schreibvorgänge mounten kann.

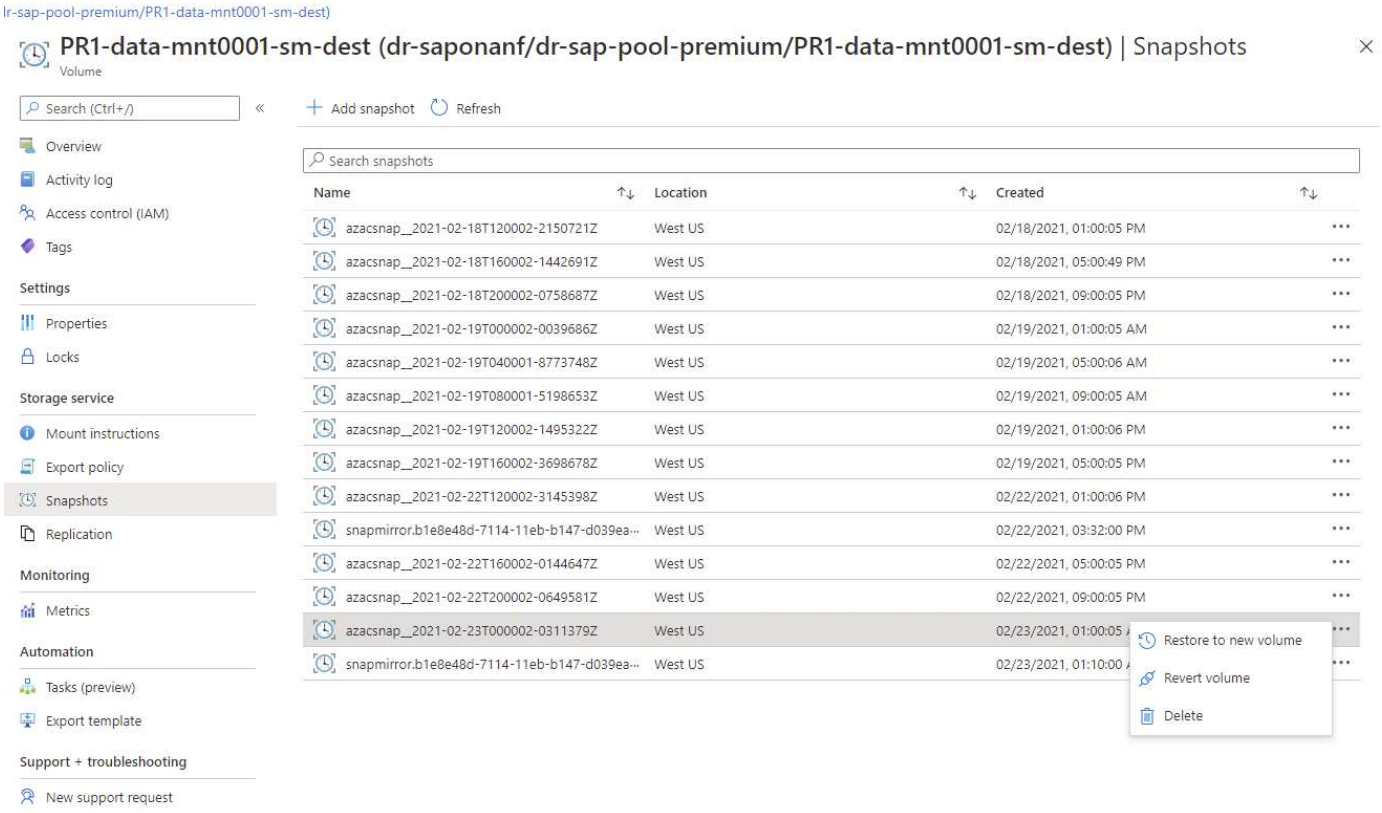
Für das HANA Daten-Volume müssen Sie das aktuelle HANA Snapshot-Backup wiederherstellen, das mit AzAcSnap erstellt wurde. Dieser Vorgang zum Zurücksetzen des Volumes ist nicht möglich, wenn der neueste ReplikationssSnapshot aufgrund des Replication Peering als belegt markiert wird. Deshalb müssen Sie auch das Replication Peering löschen.

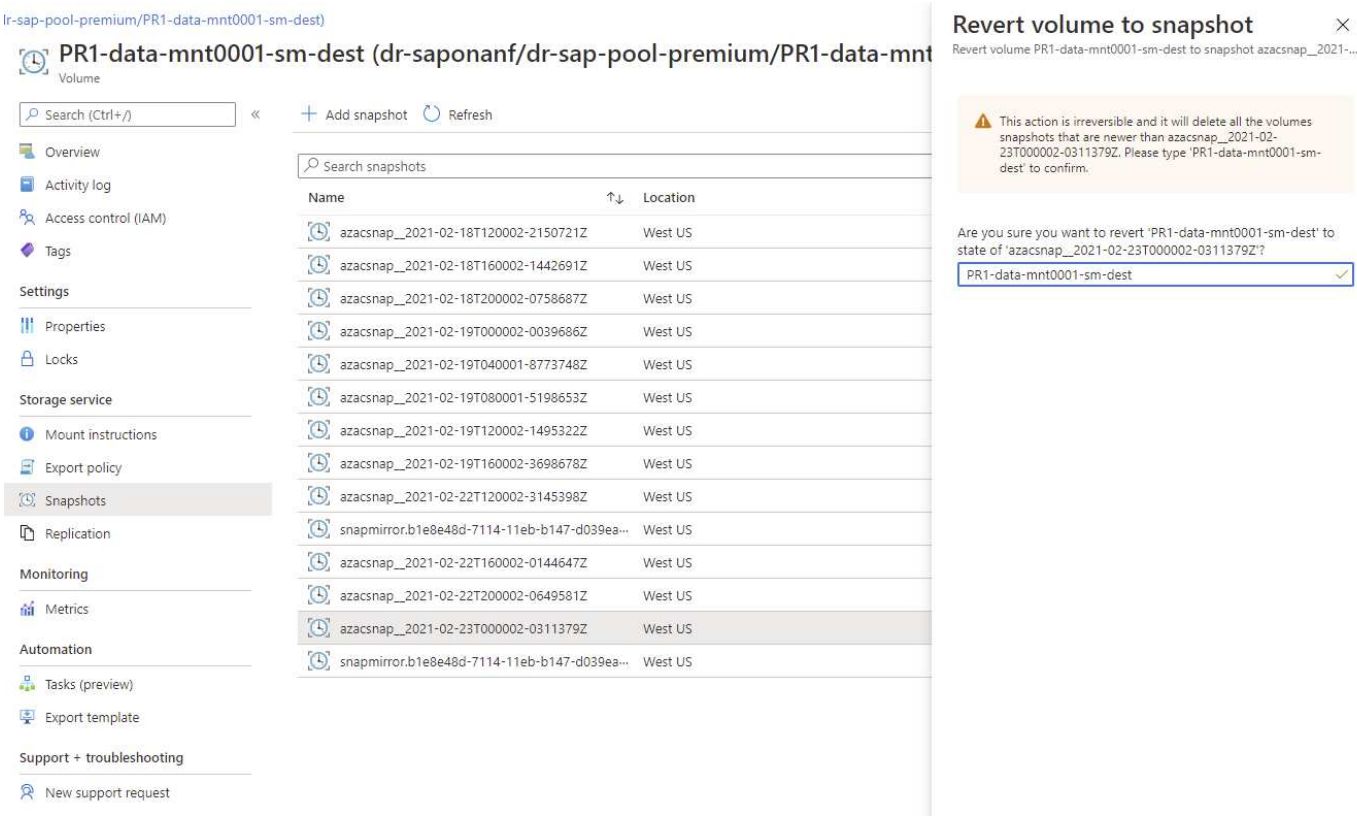
Die nächsten beiden Screenshots zeigen den Break and delete Peering-Vorgang für das HANA-Datenvolumen. Dieselben Vorgänge müssen auch für das Log-Backup und das gemeinsame HANA-Volume durchgeführt werden.





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

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.

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

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.

Autor: Nils Bauer, NetApp

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

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

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.

Autoren: Marco Schoen, NetApp; Dr. Tristan Daude, CommVault Systems

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

SnapCenter Integration für SAP ASE Database

In diesem Dokument werden die Besonderheiten der SnapCenter-Integration für die in einer SAP-Umgebung verwendete SAP ASE-Datenbank beschrieben.

Einführung

Das Dokument soll keine Schritt-für-Schritt-Beschreibung der Einrichtung der gesamten Umgebung sein, sondern umfasst Konzepte und relevante Details zu:

- Beispiel für eine Konfigurationsübersicht
- Beispiellayout
- Schutz der SAP ASE Instanz
- Wiederherstellung und Wiederherstellung von SAP ASE Instanz

Autor: Michael Schlosser, NetApp

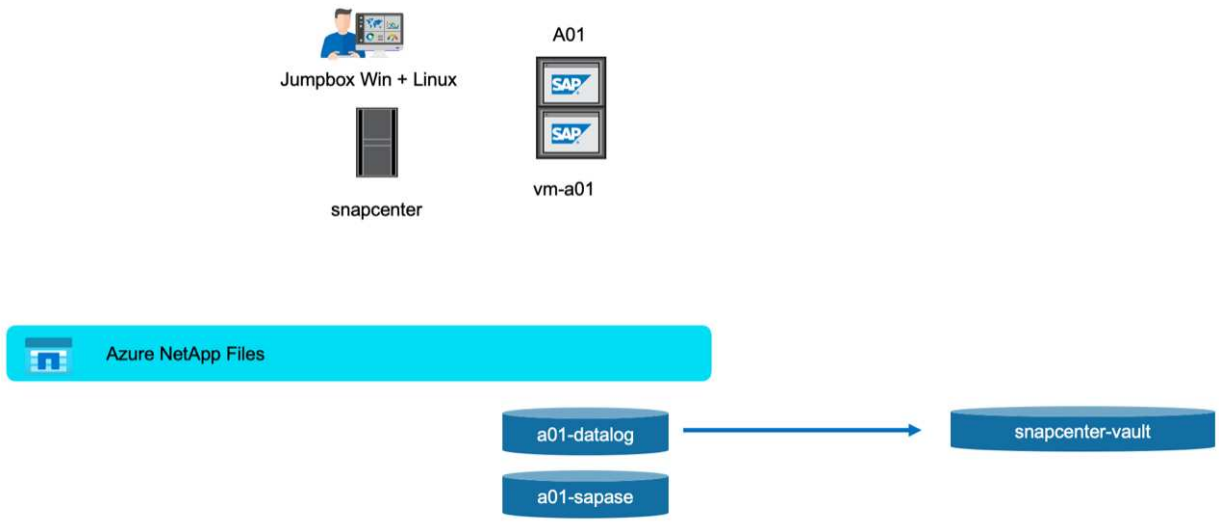
Beispiel für eine Konfigurationsübersicht

Beispiel für eine Implementierung des SnapCenter ASE Plug-ins für ein SAP-System auf der Azure Plattform.

Diese Implementierung beschreibt die minimal erforderliche Volume-Konfiguration. Data Dump Backups und Log Dump Backups werden gemäß SAP Note 1588316 konfiguriert.

Alternativ könnte die in diesem Abschnitt beschriebene Volume-Struktur "MS Technical Community Blog"verwendet werden.

Demo-Umgebung



Softwareversionen

Software	Version
Linux BS	SLES FÜR SAP 15 SP5
SAP	SAP NetWeaver 7.5 unterstützt
SAP ASE	16.0 SP04 PL06 HF1
SnapCenter	6,1

ASE Volume Design

Das nachstehende „Least Volume Layout“ muss verwendet werden, um Backup-/Recovery- und Klonfälle für die SAP ASE-Datenbank zu ermöglichen. Die Beispielkonfiguration verwendet <SID>: A01.

Volumenname	Verzeichnis (qtree) auf Volumen	Mount-Punkt auf Server	Kommentar
<SID>-sapase	sybase	/sybase	Übergeordnetes Verzeichnis für ASE-bezogene Dateien
		/sybase/<SID>/Backups	Data Dump Backups (können auf einem anderen Volume abgelegt werden)
		/sybase/<SID>/log_Archives	Log-Dump-Backups (können auf einem anderen Volume abgelegt werden)
	<sid>-Lösungen m	/Home/<sid>-Programm m	Home Verzeichnis der Benutzer <sid> Hmm
	Usrsaptrans	/Usr/sap/trans	Transportverzeichnis
	<SID>	/Usr/sap/<SID>	Usr sap
	<SID>	/Sapmnt/<SID>	SAP GlobalHost-Verzeichnis

Volumenname	Verzeichnis (qtree) auf Volumen	Mount-Punkt auf Server	Kommentar
<SID>-Datalog	sapdata_1	/sybase/<SID>/sapdata_1	DB-Daten (SID)
	saplog_1	/sybase/<SID>/saklog_1	DB-Protokoll (SID)
	Saptemp	/sybase/<SID>/saptemp	PSAPTEMP
	Systemsicherheit	/sybase/<SID>/sybsicherheit	Sybase Sicherheits-DB
	Sybsystem	/sybase/<SID>/sybsystem	Sybase System-DB
	Sybtemp	/sybase/<SID>/sybtemp	Sybase System-DB - Temp
	Sapdiag	/sybase/<SID>/sapdiag	'saptools'-Datenbank

Schritte zum Schutz von Datenbank A01

- Prüfen Sie die Dateiverteilung gemäß dem Beispiellayout
- Prüfen Sie die Voraussetzungen für den Host (vm-a01).
- Voraussetzungen für die Datenbank prüfen (A01)
- SnapCenter-Agent auf Host bereitstellen/installieren (vm-a01)
- Erstellen Sie die Ressourcenkonfiguration der SnapCenter-Instanz

Voraussetzungen auf Host

Weitere aktuelle Informationen stehen zur Verfügung"Hier".

Bevor Sie einen Host hinzufügen und das Plug-in-Paket für Linux installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie können entweder die passwortbasierte Authentifizierung für den Root- oder nicht-Root-Benutzer oder die SSH-Schlüsselauthentifizierung verwenden.
- Das SnapCenter-Plug-in für Unix-Dateisysteme kann von einem Benutzer installiert werden, der kein Root-Benutzer ist. Sie sollten jedoch die sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um den Plug-in-Prozess zu installieren und zu starten. Nach der Installation des Plug-ins werden die Prozesse als effektiver nicht-Root-Benutzer ausgeführt.
- Anmeldedaten mit Authentifizierungsmodus als Linux für den Installationsbenutzer erstellen.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.
- Stellen Sie sicher, dass Sie nur die zertifizierte Version von JAVA 11 auf dem Linux-Host installiert haben
- Informationen zum Herunterladen von JAVA finden Sie unter Java Downloads für alle Betriebssysteme
- Sie sollten bash als Standard-Shell für die Plug-in-Installation verwenden.

Voraussetzungen für die Datenbank – Aktivieren Sie Protokollierung und Backups

- Verzeichnisse für Backups und log_Archives erstellen (/sybase/A01/Backups, /sybase/A01/log_Archives)
- Verbindung zur Datenbank A01 (als OS-User syba01)
  - Isql -S A01 -U sapsa -X -w 1024

- Erstellen Sie eine Dump-Konfiguration für DATEN (A01DB) gemäß SAP Note 1588316
  - Master verwenden
  - Los
  - exec SP_config_dump @config_Name='A01DB', @Stripe_dir = '/sybase/A01/Backups' , @Komprimierung = '101' , @verify = 'header'
  - Los
- Erstellen Sie eine Dump-Konfiguration für das PROTOKOLL (A01LOG) gemäß SAP Note 1588316
  - Master verwenden
  - Los
  - SP_config_dump @config_Name='A01LOG', @Stripe_dir = '/sybase/A01/log_Archives' , @Komprimierung = '101' , @verify = 'header'
  - Los
- Aktivieren Sie die vollständige Protokollierung für Datenbank A01
  - SP_dboption A01, 'trunc log on chkpt' , false
  - Los
  - SP_dboption A01, 'vollständige Protokollierung für alle', 'true'
  - Los
  - SP_dboption A01, 'Enforce Dump tran Sequence', 'true'
  - Los
- Datenbank-DUMP-Backup zum Aktivieren von Log-DUMP-Backup
  - Dump-Datenbank A01 mit config ='A01DB'
  - Los
  - Protokollabfall
  - Dump-Transaktion A01 mit config = 'A01LOG'
  - Los
- Stellen Sie sicher, dass regelmäßige Protokollsicherungen gemäß SAP Note 1588316 konfiguriert sind

Optional – Erstellen Sie einen dedizierten Datenbankbenutzer

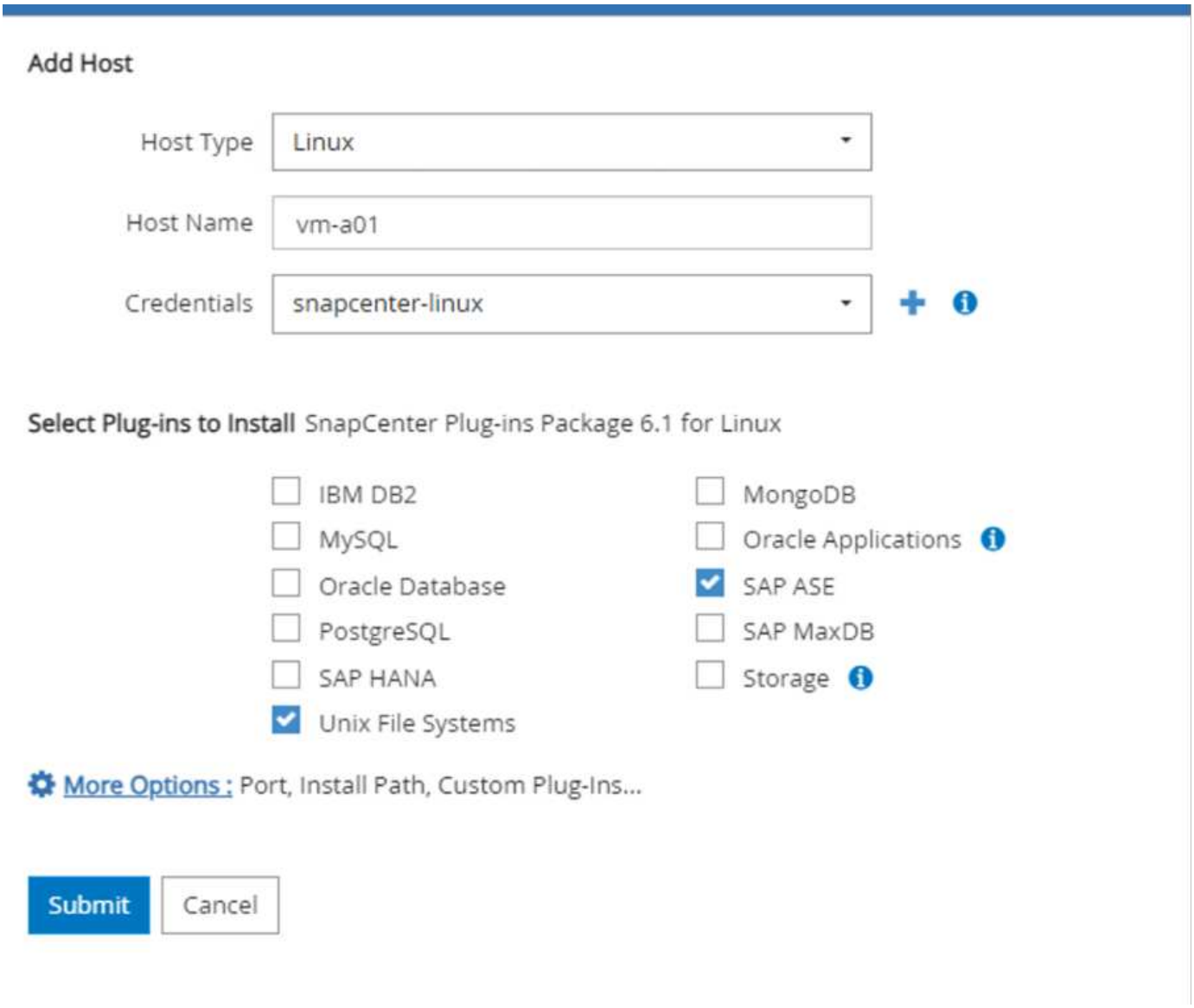
Für SAP Umgebungen könnte User sapsa genutzt werden.

- Verbindung zur Datenbank A01 (als OS-User syba01)
  - Isql -S A01 -U sapsa -X -w 1024
- Benutzer erstellen
  - Erstellen Sie ein Anmelde-Backup mit Passwort <password>
  - Los
- Weisen Sie dem Benutzer Permisssons/Rollen zu
  - Rolle sa_role,sso_role,oper_role,sybase_ts_role für Backup gewähren
  - Los

SnapCenter-Agent auf Host-vm-a01 bereitstellen

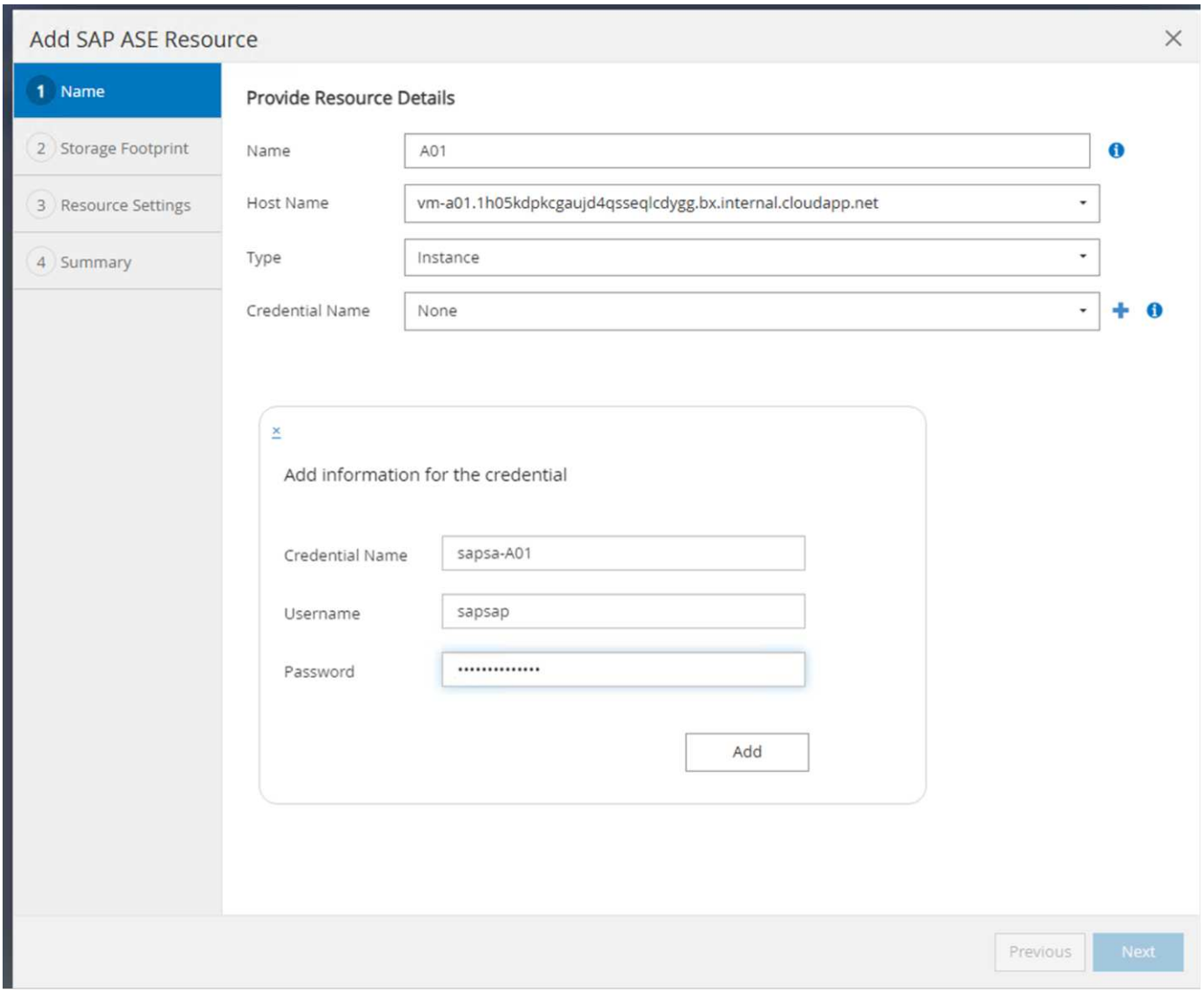
Weitere Informationen finden Sie im "SnapCenter-Dokumentation".

Wählen Sie die Plug-ins für SAP ASE und Unix File Systems aus.

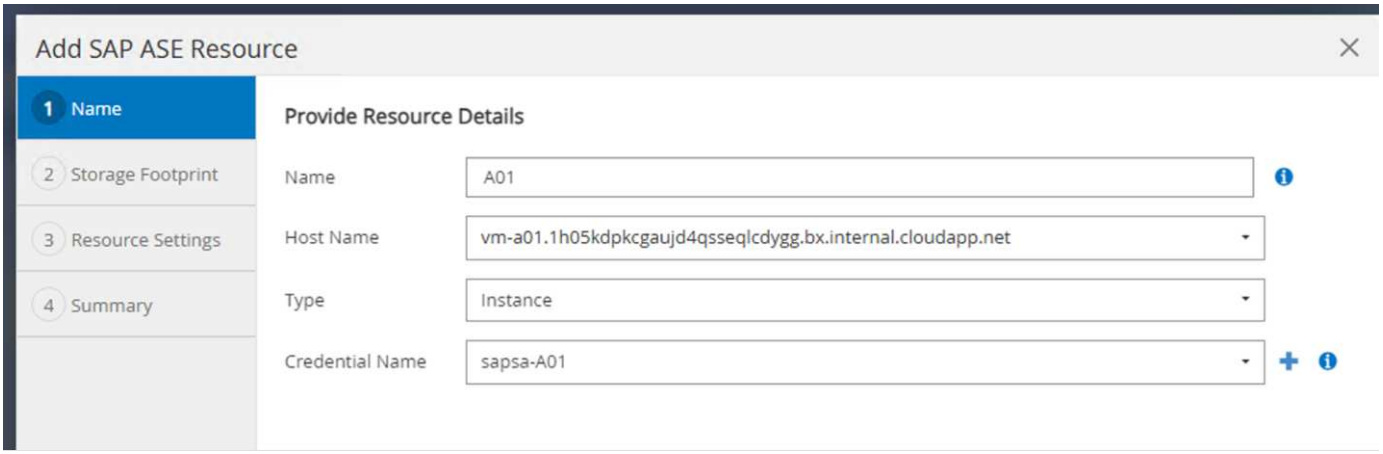


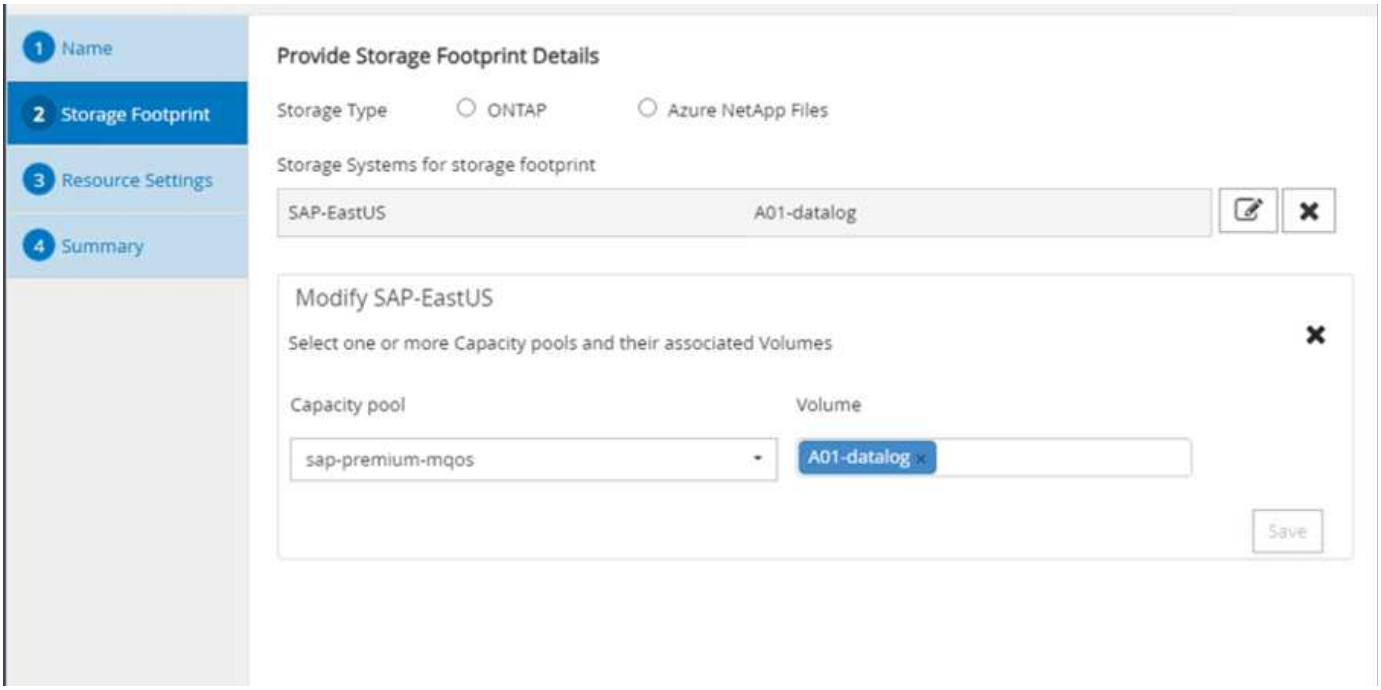
Erstellen Sie die Ressourcenkonfiguration der SnapCenter-Instanz für Datenbank A01

Ressourcen → SAP ASE → Ressourcen hinzufügen



Wenn das Passwort Sonderzeichen enthält, müssen diese mit einem umgekehrten Schrägstrich maskiert werden. Z. B. Test!123! → Test\!123\!

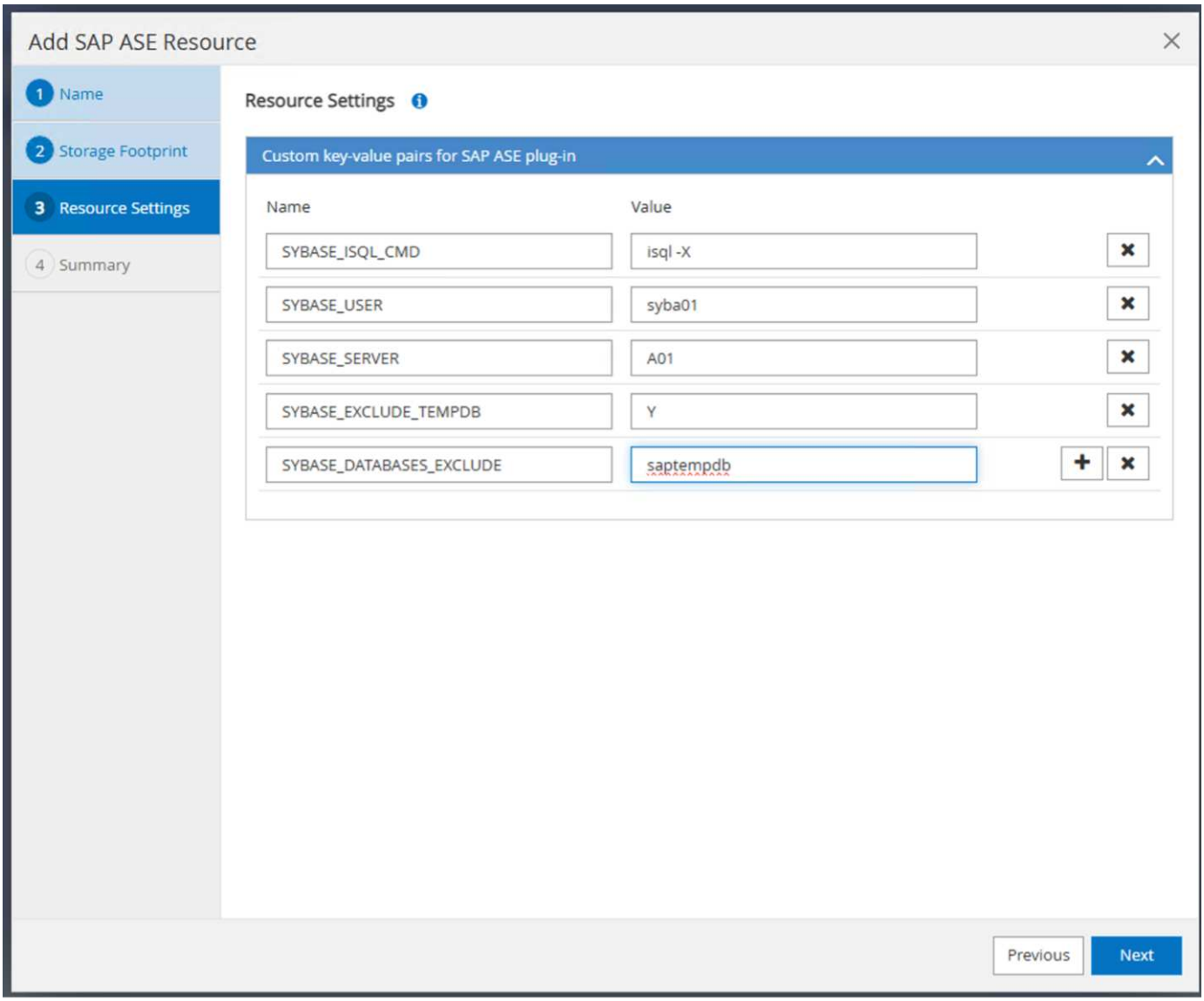




Wenn Sie das Volumendesign aus dem verwenden"MS Technical Community Blog".

Volumes /<SID> uncausage base, /uncauso <SID> uncauso, /<SID> begleichen muss als Storage Footprint konfiguriert werden

Im Anschluss an die Ressourceneinstellungen müssen (mindestens) benutzerdefinierte Schlüssel-Wert-Paare erstellt werden.



In der folgenden Tabelle sind die Sybase Plug-in-Parameter aufgeführt, ihre Einstellungen aufgeführt und beschrieben:

Parameter	Einstellung	Beschreibung
SYBASE_ISQL_CMD	Beispiel: /Opt/sybase/OCS-15__0/bin/isql -X	Definiert den Pfad zum Befehl isql. Verfügbare Optionen: https://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.dc34237.1500/html/mvsinst/CIHHFDGC.htm
SYBASE_USER	Benutzername	Gibt den Betriebssystembenutzer an, der den Befehl isql ausführen kann. Dieser Parameter ist für UNIX erforderlich. Dieser Parameter ist erforderlich, wenn der Benutzer, der die Snap Creator Agentstart- und STOP-Befehle ausführt (normalerweise der Root-Benutzer) und der Benutzer, der den isql-Befehl ausführt, unterschiedlich ist.
SYBASE_SERVER	Name_Data_Server	Gibt den Namen des Sybase-Datenservers an (-S Option auf isql Befehl).Beispiel: A01

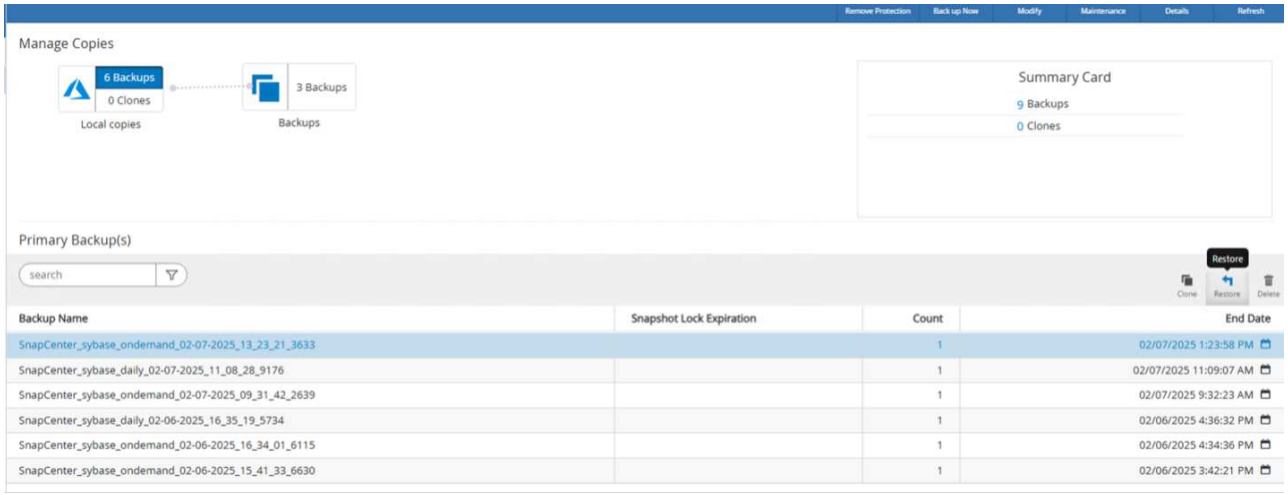
Parameter	Einstellung	Beschreibung
SYBASE_DATENBANKEN	db_Name:user_Name/password	Listet die Datenbanken innerhalb der Instanz auf, die gesichert werden sollen. Die Master-Datenbank wird hinzugefügt, zum Beispiel: DBATest2:sa/53616c7404351e.wird eine Datenbank mit dem Namen +ALL verwendet, wird die automatische Datenbankerkennung verwendet und die sybsyntax, sybsystemdb, sybsystemprocs und tempdb-Datenbanken werden ausgeschlossen. Ein Beispiel: +ALL:sa/53616c71a6351e Verschlüsselte Passwörter werden unterstützt, wenn der Parameter NTAP_PWD_PROTECTION eingestellt ist.
SYBASE_DATABASES_EXCLUDE	db_Name	Ermöglicht den Ausschluss von Datenbanken, wenn das +ALLE-Konstrukt verwendet wird. Sie können mehrere Datenbanken mit Hilfe einer durch Semikolon getrennten Liste angeben.Beispiel: Pubs2;Test_db1
SYBASE_TRAN_DUMP	db_Name:Directory_PATH	Ermöglicht Ihnen die Durchführung eines Sybase Transaktions-Dump nach dem Erstellen einer Snapshot-Kopie.Beispiel: Pubs2:/sybasedumps/pubs2 Sie müssen jede Datenbank angeben, die einen Transaktions-Dump benötigt.
SYBASE_TRAN_DUMP_FORMAT	%S_%D_%T.CMN	Ermöglicht Ihnen die Angabe der Namenskonvention für Dump. Die folgenden Schlüssel können angegeben werden: %S = Instanzname von SYBASE_SERVER %D = Datenbank von SYBASE_DATABASES %T = eindeutiger Zeitstempel Hier ist ein Beispiel: %S_%D_%T.log
SYBASE_TRAN_DUMP_COMPRESS	(J/N)	Aktiviert oder deaktiviert die native Sybase Transaktions-Dump-Komprimierung.
SYBASE	Beispiel: /Sybase	Gibt den Speicherort der Sybase-Installation an.
SYBASE_MANIFEST	Beispiel: A01:/sybase/A01/sapdiag	Gibt die Datenbanken an, für die die Manifestdatei erstellt werden soll, zusammen mit dem Speicherort, an dem die Manifestdatei platziert werden soll.
SYBASE_MANIFEST_FORMAT	%S__%D_.Manifest Beispiel: %S_%D_.Manifest	Ermöglicht Ihnen die Angabe der Namenskonvention für die Manifestdatei. Folgende Schlüssel können angegeben werden: %S = Instanzname von SYBASE_SERVER %D = Datenbank von SYBASE_DATABASES
SYBASE_MANIFEST_DELETE	(J/N)	Ermöglicht das Löschen des Manifests nach dem Erstellen der Snapshot Kopie. Die Manifest-Datei sollte in der Snapshot-Kopie erfasst werden, damit sie immer für das Backup verfügbar ist.
SYBASE_EXCLUDE_TEMPDB	(J/N)	Ermöglicht den automatischen Ausschluss von vom Benutzer erstellten temporären Datenbanken.

Sequenz zum Wiederherstellen von System A01

1. SAP System A01 stoppen (einschließlich Datenbank), sapinit stoppen
2. Umount Dateisysteme
3. Volumes A01-Datalog wiederherstellen (mit SnapCenter)
4. Mounten Sie Dateisysteme
5. Start Datenbank A01 (mit Option –q, um automatische Online zu vermeiden und Datenbank vorwärts wiederherstellbar zu halten – gemäß SAP Note 1887068)
6. Starten Sie BackupServer A01
7. Online-Datenbank saptools, sybsicherheit, sybmgmtdb
8. Datenbank A01 wiederherstellen (mit isql)
9. Online-Datenbank A01
10. Starten Sie sapinit, SAP System A01

Instanz A01 wiederherstellen

- Beenden Sie SAP System + DB A01 auf Host vm-a01
  - User a01adm: Stopsap
  - User root: /Etc/init.d/sapinit stop
  - Benutzer root: Umount -a -t nfs
- Backup Wiederherstellen
  - SnapCenter GUI: Wählen Sie erforderliche Sicherung für Wiederherstellung



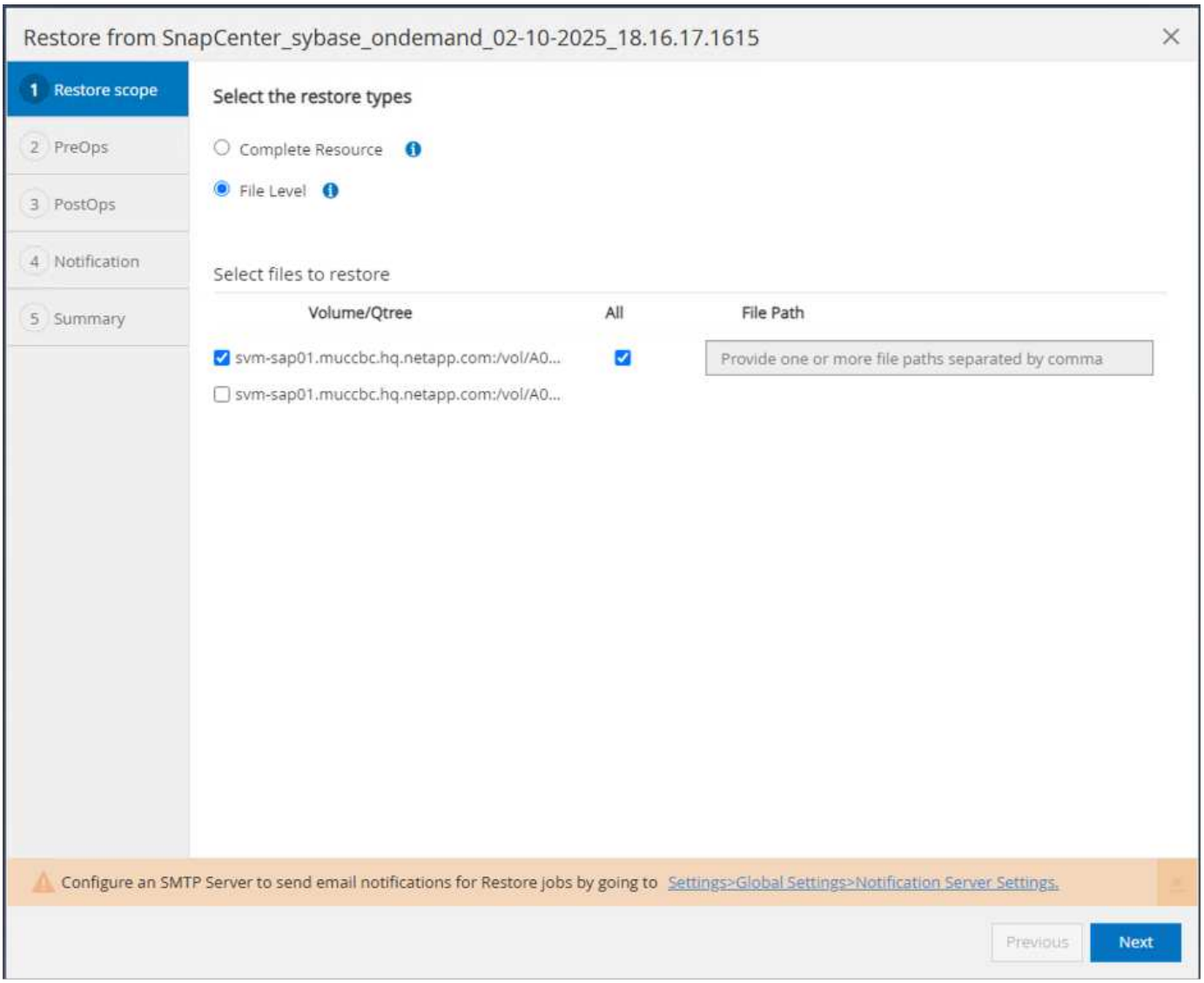
  - Für die ANF Implementierung – nur vollständige Ressource verfügbar

Wenn Sie die Option „Complete Resource“ auswählen, wird eine Volume-basierte Snap Restore (VBSR) ausgelöst. Innerhalb von Azure wird sie aufgerufen"Lautstärke zurücksetzen".

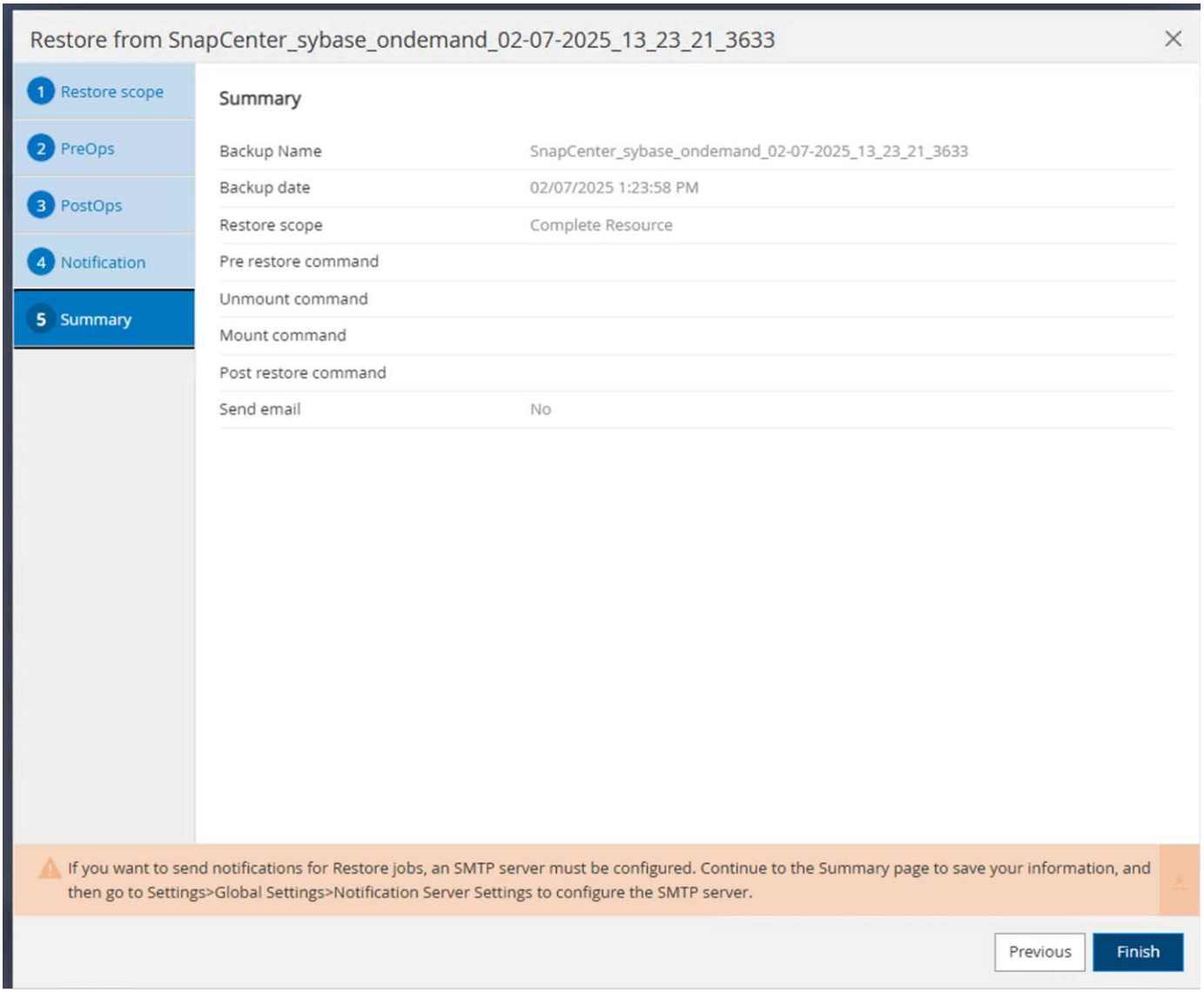
Important

Active filesystem data and snapshots that were taken after the selected snapshot will be lost. The snapshot revert operation will replace *all* the data in the targeted volume with the data in the selected snapshot. You should pay attention to the snapshot contents and creation date when you select a snapshot. You cannot undo the snapshot revert operation.

Für andere Implementierungstypen (z. B. On-Premises-ANF) könnte ein SFSR-Vorgang (Single File Snap Restore) orchestriert werden. Wählen Sie File Level und das entsprechende Volume und aktivieren Sie „All“ – siehe folgenden Screenshot.



Die Zusammenfassung wird angezeigt und mit „Fertig stellen“ wird die eigentliche Wiederherstellung gestartet.



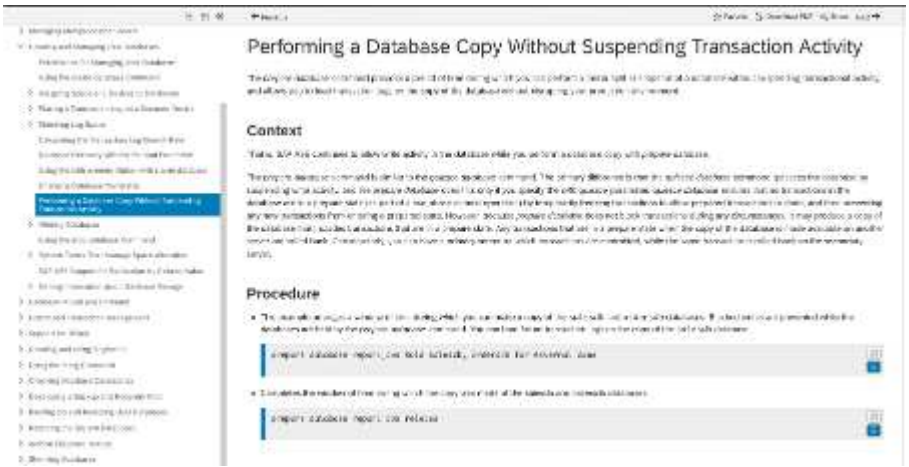
- Dateisysteme mounten (vm-a01)
  - User root: Mount -a -t nfs
- Starten Sie Datenbank A01 + BackupServer
  - RUN_A01 ändern und -q \ hinzufügen (gemäß SAP Note 1887068)
  - User syba01: RUN_A01 &
  - User syba01: RUN_A01_BS&
- Online-Datenbanken saptools, sybsicherheit, sybmgmtdb
  - User syba01: Isql -S A01 -U sapsa -X -w 1024
  - Online-Datenbank-Saptools
  - Los
  - Systemsicherheit der Online-Datenbank
  - Los
  - Online-Datenbank sybmgmtdb
  - Los

- Datenbank A01 wiederherstellen
  - SP_dump_history (Anzeige der Transaktions-Log-Dumps)
  - Los
  - Laden Sie Transaktionsprotokoll-Dumps entsprechend Ihren Anforderungen – weitere Informationen finden Sie in der Dokumentation: https://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.dc36272.1572/html/commands/X75212.htm
  - Beispiel: LADEN SIE TRAN A01 VON '/sybase/A01/log_Archives/A01.TRAN.20250207.140248.6.000'
  - Los
  - Online-Datenbank A01
  - Los
- Entfernen Sie -q aus RUN_A01
- Starten Sie das SAP-System
  - User root: /Etc/init.d/sapinit Start
  - User a01ADM: Startsap

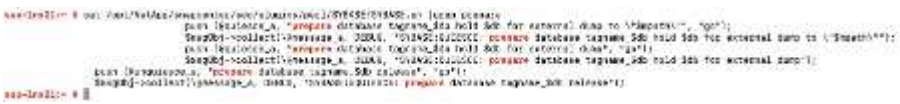
Zusätzliche Informationen und Versionsverlauf

Stilllegen vs. Vorbereiten

Siehe Dokumentation auf Link: SAP Hilfe Seite.



Das SnapCenter SAP ASE Plugin verwendet den Befehl Quiesce Database, könnte jedoch durch den Befehl Prepare ersetzt werden. Falls erforderlich, muss sie in SYBASE.pm in Zeile 473, 475, 675, 481, 673, 479 z.B. geändert werden



Aufgezeichnete Demos

Folgende neu kodierte Demos stehen zur Unterstützung der Dokumentation zur Verfügung.

Installation und Konfiguration ASE Plugin, Backup der ASE-Datenbank

Restore und Recovery von ASE-Datenbanken

Externe Dokumentation

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

- "SAP Installation Azure auf ANF"
- "SnapCenter-Voraussetzungen für Plugins"
- "SnapCenter Installations-Plugins"
- "Sybase Infocenter - Isql"
- "Sybase Infocenter - Load Transaktions-Log Dumps"
- SAP-Hinweise (Anmeldung erforderlich)
  - 1887068 - SYB: Externe Sicherung und Wiederherstellung mit SAP ASE: https://me.sap.com/notes/1887068/E
  - 1618817 - SYB: Wiederherstellen eines SAP ASE-Datenbankservers (UNIX): https://me.sap.com/notes/1618817/E
  - 1585981 – SYB: Sicherstellung der Recovery-Fähigkeit für SAP ASE: https://me.sap.com/notes/1585981/E
  - 1588316 - SYB: Automatische Datenbank- und Protokollsicherungen konfigurieren: https://me.sap.com/notes/1588316/E
  - NetApp Produktdokumentation: https://www.netapp.com/support-and-training/documentation/
  - "NetApp SAP-Lösungen – Informationen zu Anwendungsfällen, Best Practices und Vorteilen"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	April 2025	Erstversion – Backup/Recovery ASE-Datenbank

SnapCenter Integration für IBM DB2 Database

In diesem Dokument werden die Besonderheiten der SnapCenter-Integration für die in einer SAP-Umgebung verwendete IBM DB2-Datenbank beschrieben.

Einführung

Das Dokument soll keine Schritt-für-Schritt-Beschreibung der Einrichtung der gesamten Umgebung sein, sondern umfasst Konzepte und relevante Details zu:

- Beispiel für eine Konfigurationsübersicht
- Beispiellayout
- Schutz von DB2-Datenbanken
- Wiederherstellung und Wiederherstellung der DB2-Datenbank

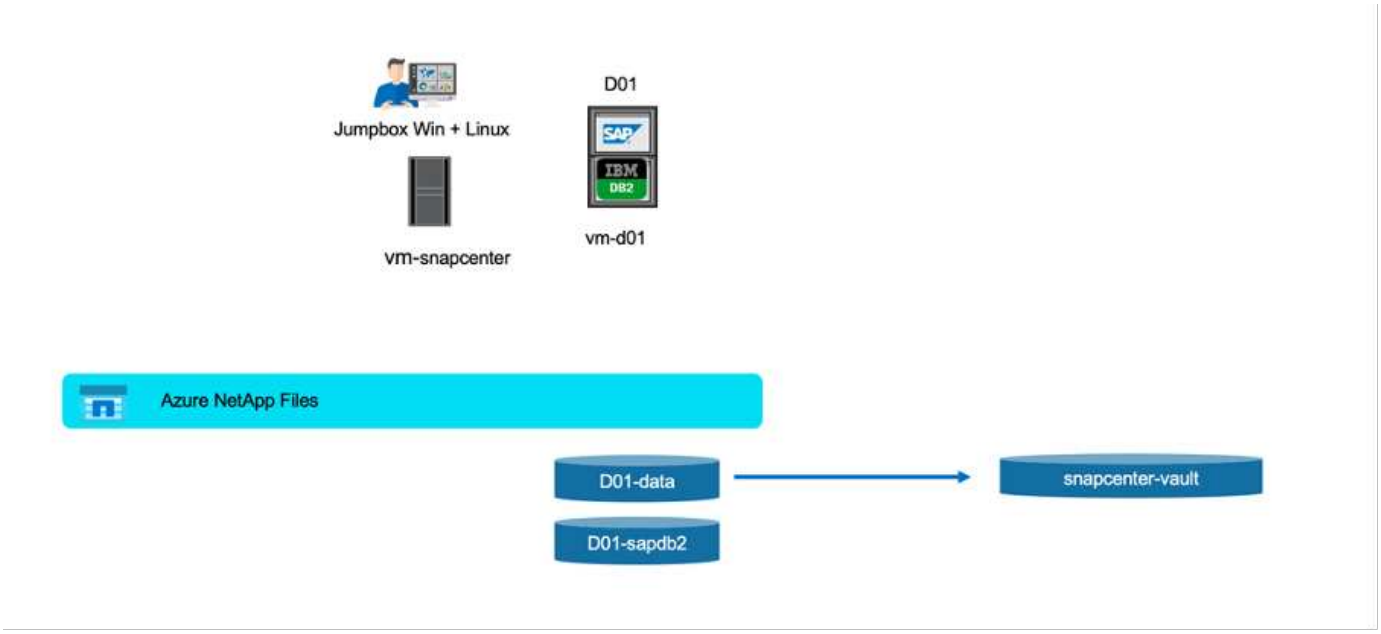
Autor: Michael Schlosser, NetApp

Beispiel für eine Konfigurationsübersicht

Beispiel für eine Implementierung für das SnapCenter DB2 Plug-in für ein SAP-System auf der Azure Plattform.

Diese Implementierung beschreibt die minimal erforderliche Volume-Konfiguration.

Alternativ könnte die in diesem Abschnitt beschriebene Volume-Struktur "MS Technical Community-Blog"verwendet werden.



Demo-Umgebung

Softwareversionen

Software	Version
Linux BS	SLES FÜR SAP 15 SP5
SAP	SAP NetWeaver 7.5 unterstützt
DB2	10.5.0.7
SnapCenter	6,1

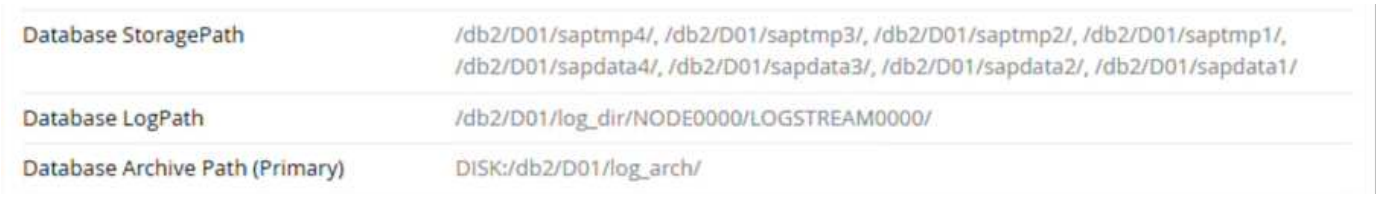
DB2-Volume-Design

Das folgende Least-Volume-Layout muss verwendet werden, um Backup-/Recovery- und Klonfälle für die DB2-Datenbank zu ermöglichen. Die Beispielkonfiguration verwendet <SID>: D01.

Volumenname	Verzeichnis (qtree) auf Volumen	Mount-Punkt auf Server	Kommentar
<SID>-sapdb2	db2	/db2	
		/db2/<SID>	Übergeordnetes Verzeichnis für DB2-bezogene Dateien

Volumenname	Verzeichnis (qtree) auf Volumen	Mount-Punkt auf Server	Kommentar
		/db2/db2<sid>	Home-Verzeichnis der Benutzer db2 <sid> und DB2 Software
		/db2/<SID>/db2dump	DB2-Diagnoseprotokoll und Dump-Dateien
		/db2/<SID>/Backup	Backup-Speicherort (kann auf einem anderen Volume platziert werden)
		/db2/<SID>/log_ARCH	Offline Redo Logs (möglicherweise auf einem anderen Volume platziert – Snapshot wird ausgelöst)
		/db2/<SID>/log_dir	Online Redo Logs (können auf einem anderen Volume platziert werden – Snapshot wird ausgelöst)
	<sid>-Lösungen m	/Home/<sid>-Programm m	Home Verzeichnis der Benutzer <sid> Hmm
	<sid> auslassen	/Home/<sid>	Home Verzeichnis des Benutzers <sid>
	Usrsaptrans	/Usr/sap/trans	Transportverzeichnis
	<SID>	/Usr/sap/<SID>	Usr sap
	<SID>	/Sapmnt/<SID>	SAP GlobalHost-Verzeichnis
<SID>-Daten	sapdata1	/db2/<SID>/sapdata1	DB-Daten
	sapdata2	/db2/<SID>/sapdata2	DB-Daten
	sapdata3	/db2/<SID>/sapdata3	DB-Daten
	sapdata4	/db2/<SID>/sapdata4	DB-Daten
	saptmp1	/db2/<SID>/saptmp1	DB Temp-Dateien
	saptmp2	/db2/<SID>/saptmp2	DB Temp-Dateien
	saptmp3	/db2/<SID>/saptmp3	DB Temp-Dateien
	saptmp4	/db2/<SID>/saptmp4	DB Temp-Dateien
	Db2 <sid>	/db2/<SID>/db2<sid>	Instanzdateien

Da die automatische Ermittlung standardmäßig für das DB2-Plug-in aktiviert ist, wird ein Snapshot für Volumes erstellt, die den folgenden Dateipfaden entsprechen.



Schritte zum Schutz von Datenbank D01

- Prüfen Sie die Dateiverteilung gemäß dem Beispiellayout
- Prüfen Sie die Voraussetzungen für den Host (vm-d01).
- Voraussetzungen für die Datenbank prüfen (D01)
- SnapCenter-Agent auf Host bereitstellen/installieren (vm-d01)
- Erstellen Sie die Ressourcenkonfiguration der SnapCenter-Instanz

Voraussetzungen auf Host

Weitere aktuelle Informationen finden Sie hier:

- https://docs.netapp.com/us-en/snapcenter/protect-scu/reference_prerequisites_for_adding_hosts_and_installing_snapcenter_plug_ins_package_for_linux.html
- https://docs.netapp.com/us-en/snapcenter/protect-db2/prerequisites-for-using-snapcenter-plug-in-for-ibm-db2.html

Bevor Sie einen Host hinzufügen und das Plug-in-Paket für Linux installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie können entweder die passwortbasierte Authentifizierung für den Root- oder nicht-Root-Benutzer oder die SSH-Schlüsselauthentifizierung verwenden.
- Das SnapCenter-Plug-in für Unix-Dateisysteme kann von einem Benutzer installiert werden, der kein Root-Benutzer ist. Sie sollten jedoch die sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um den Plug-in-Prozess zu installieren und zu starten. Nach der Installation des Plug-ins werden die Prozesse als effektiver nicht-Root-Benutzer ausgeführt.
- Anmeldedaten mit Authentifizierungsmodus als Linux für den Installationsbenutzer erstellen.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.
- Stellen Sie sicher, dass Sie nur die zertifizierte Version von JAVA 11 auf dem Linux-Host installiert haben
- Informationen zum Herunterladen von JAVA finden Sie unter Java Downloads für alle Betriebssysteme
- Sie sollten bash als Standard-Shell für die Plug-in-Installation verwenden.

Voraussetzungen für die Datenbank – Aktivieren Sie Protokollierung und Backups

Um Offline-Protokolle zu aktivieren, ist ein vollständiges Offline-Backup der Datenbank erforderlich. In der Regel ist es bereits für produktive Systeme aktiviert.

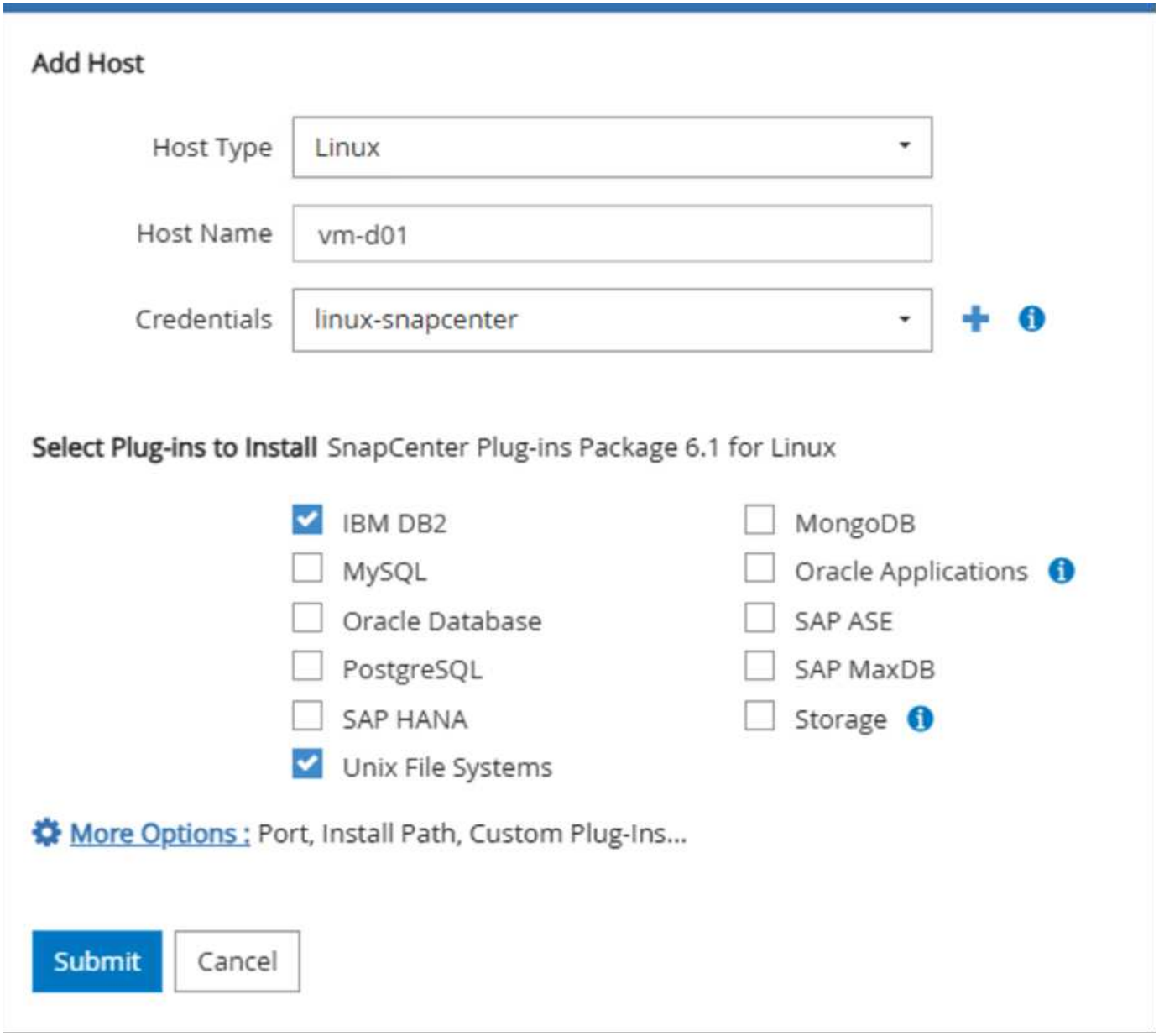
- Verzeichnisse für Backup und log_ARCH erstellen (/db2/D01/Backup, /sybase/D01/log_ARCH)
- Logarchmeth1 aktivieren (als OS-user db2d01)
  - db2-Update db cfg für D01 mit logarchmeth1-LAUFWERK:/db2/D01/log_ARCH/
- Offline-Backup erstellen (als OS-user db2d01)
  - Db2STOP-Kraft
  - Db2start Admin-Modus eingeschränkter Zugriff
  - db2 Backup db D01 auf /db2/D01/Backup

- db2 aktiviert db D01

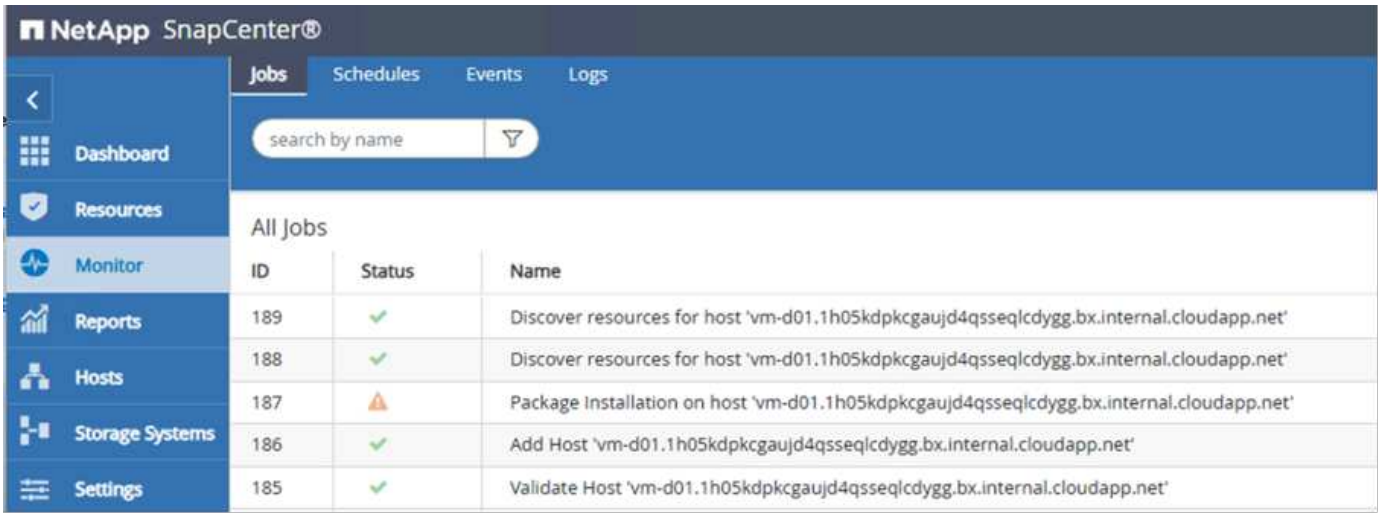
Bereitstellen des SnapCenter-Agenten auf der Host-vm-d01

Weitere Informationen finden Sie im "SnapCenter-Dokumentation".

Wählen Sie IBM DB2 und Unix File Systems Plugins aus.



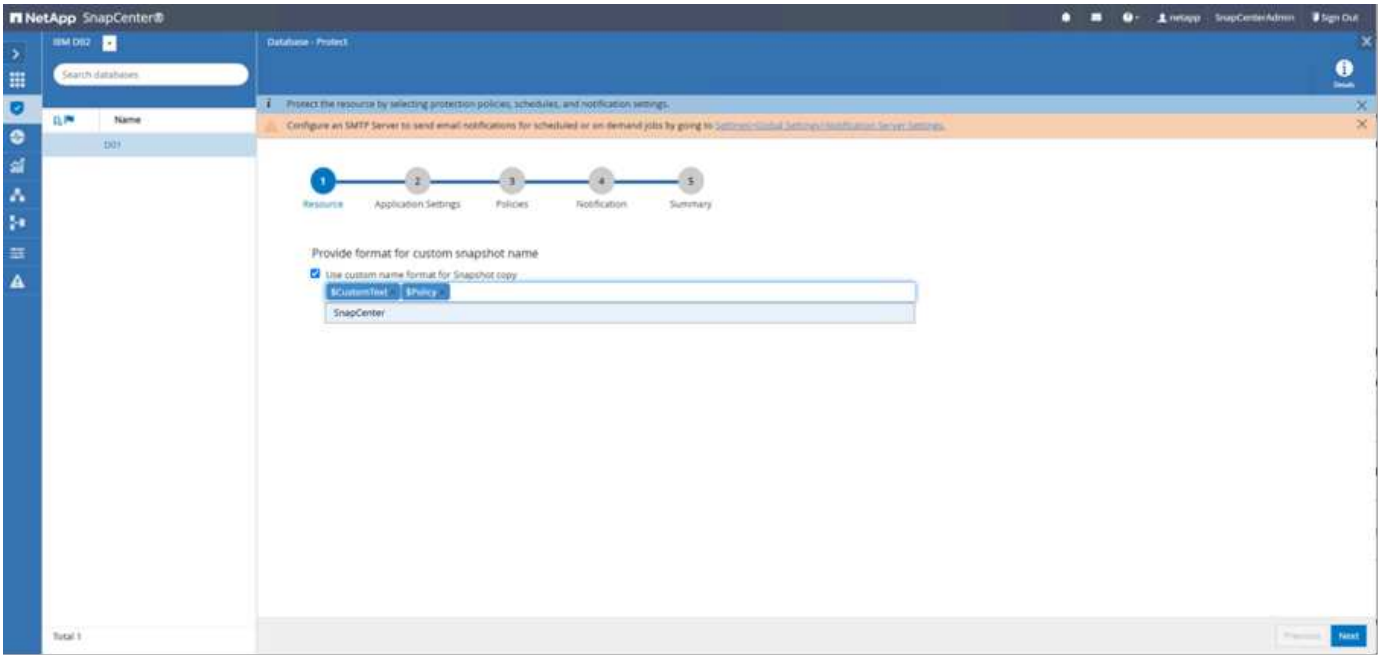
Nach der Installation wird eine Erkennung der Datenbanken auf dem Host ausgelöst.



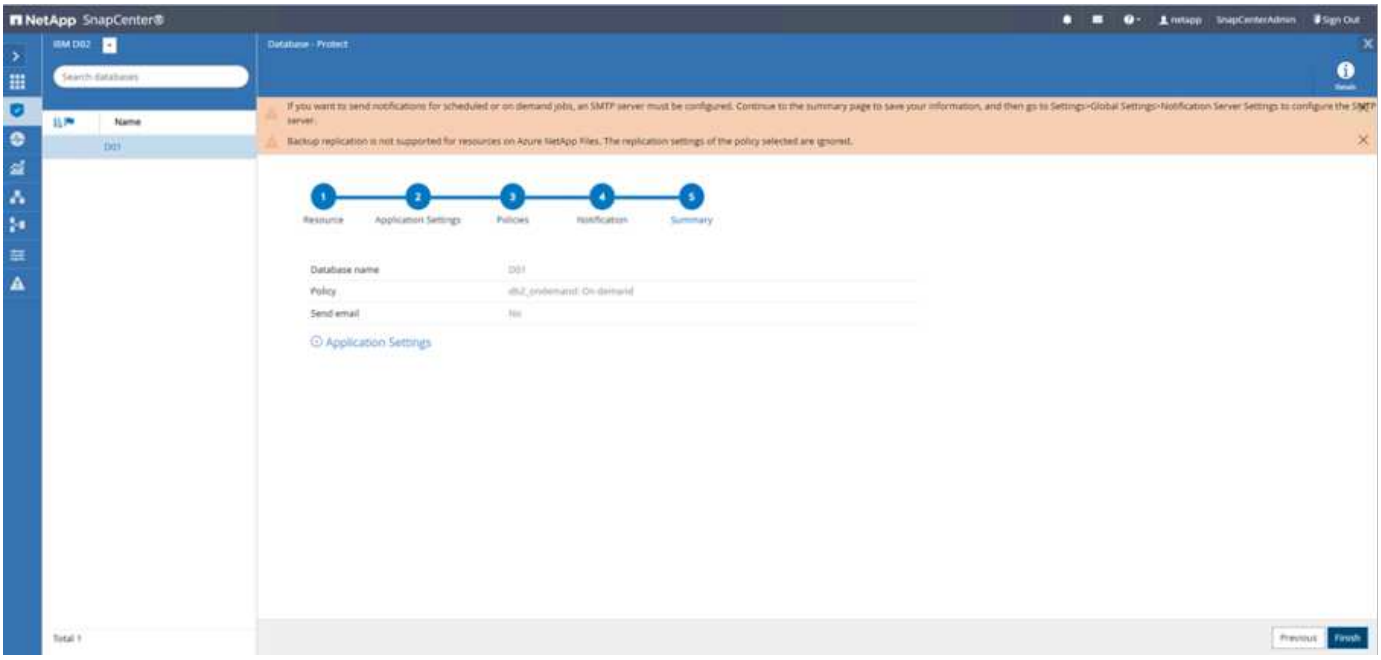
Ressourcenkonfiguration für Datenbank D01 erstellen

Wählen Sie erkannte Ressource D01

Konfigurieren Sie Den Snapshot-Namen



Es sind keine spezifischen Anwendungseinstellungen erforderlich. Konfigurieren Sie Richtlinien- und Benachrichtigungseinstellungen nach Bedarf.



Und beenden Sie die Konfiguration.

Sequenz zum Wiederherstellen von System D01

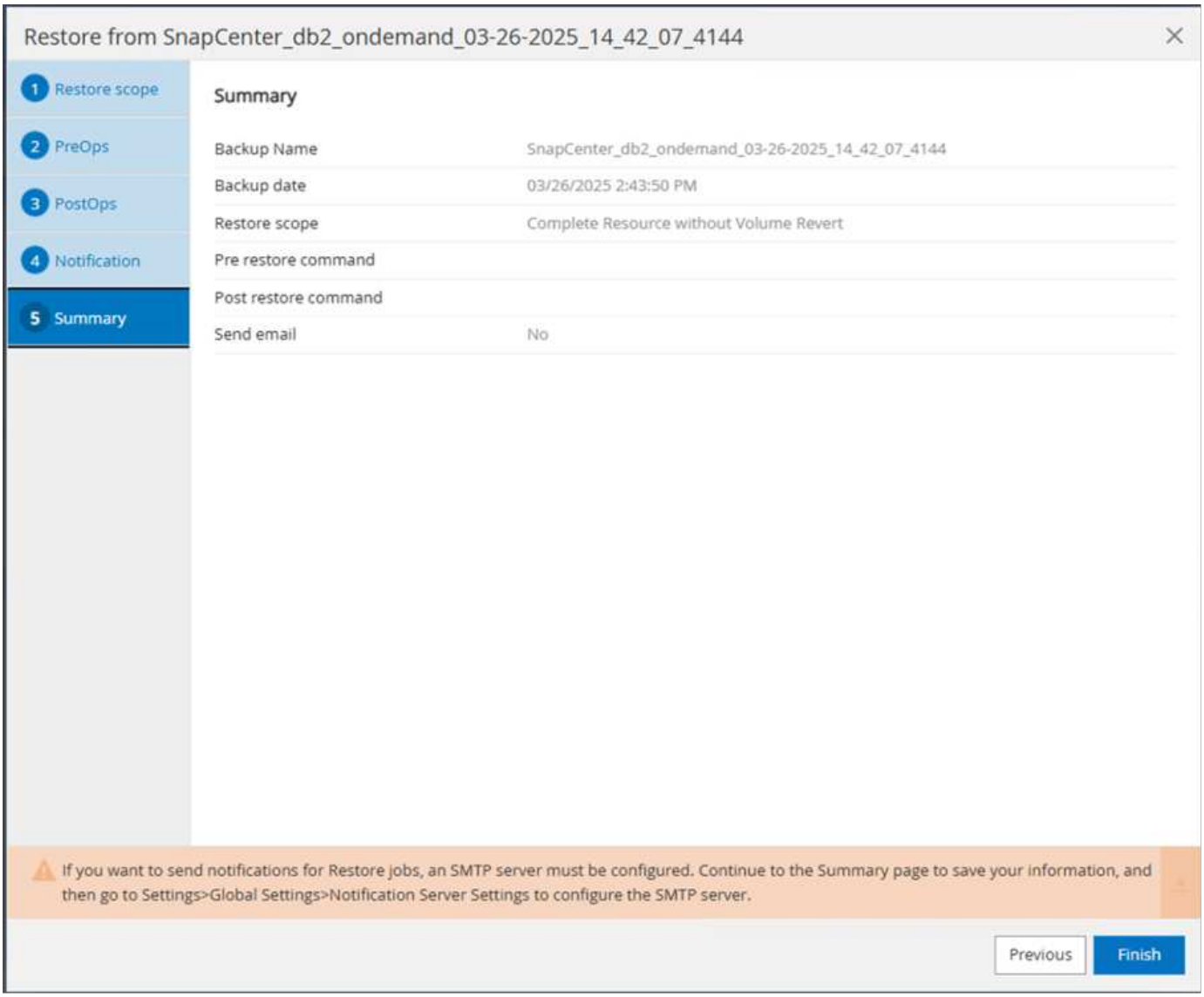
1. SAP System D01 stoppen (einschließlich Datenbank)
2. SnapCenter-Sicherung wiederherstellen (Volume D01-Daten)
    a. Unmounten Sie Dateisysteme
    b. Volume Wiederherstellen
    c. Mounten Sie Dateisysteme
    d. Initialisieren Sie die Datenbank als Spiegel db
3. Datenbank D01 wiederherstellen (mit db2 Rollforward)
4. Starten Sie SAP System D01

Datenbank D01 wiederherstellen

- Beenden Sie SAP System + DB D01 auf Host vm-d01
    - User d01adm: Stopp
- Backup Wiederherstellen
    - SnapCenter GUI: Wählen Sie erforderliche Sicherung für Wiederherstellung

- Für die ANF Implementierung – nur vollständige Ressource verfügbar

Die Zusammenfassung wird angezeigt und mit „Fertig stellen“ wird die eigentliche Wiederherstellung gestartet.



„Db2inidb D01 als Spiegel“ wird im Rahmen des SnapCenter-Wiederherstellungs-Workflows ausgeführt.

- Überprüfen Sie den Wiederherstellungsstatus Datenbank D01 (als Benutzer db2d01)
  - db2 Rollforward db D01 Abfragestatus
- Datenbank nach Bedarf wiederherstellen – hier ist eine verlustfreie Wiederherstellung angestachelt (als Benutzer db2d01)
  - db2 Rollforward db D01 zum Ende der Protokolle
- Stoppen Sie die Datenbankwiederherstellung und Online-Datenbank D01 (als Benutzer db2d01)
  - db2 Rollforward db D01 Stopp
- SAP-System starten (als Benutzer d01adm)
  - Startsap

Zusätzliche Informationen und Versionsverlauf

Folgende neu kodierte Demos stehen zur Unterstützung der Dokumentation zur Verfügung.

Installation und Konfiguration DB2 Plugin, Backup der DB2-Datenbank

Wiederherstellung und Recovery von DB2-Datenbanken

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

- "SAP auf DB2 Installation Azure auf ANF"
- "SnapCenter-Voraussetzungen für Plugins"
- "SnapCenter Installations-Plugins"
- "Dokumentation zum SnapCenter DB2 Plug-in"
- SAP-Hinweise (Anmeldung erforderlich)
  - 83000 - DB2/390: Backup- und Recovery-Optionen: https://me.sap.com/notes/83000
  - 594301 - DB6: Admin Tools und Split Mirror: https://me.sap.com/notes/594301
- NetApp Produktdokumentation: https://www.netapp.com/support-and-training/documentation/
- "NetApp SAP-Lösungen – Informationen zu Anwendungsfällen, Best Practices und Vorteilen"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	April 2025	Erste Version – Backup / Recovery DB2-Datenbank

SnapCenter Integration für SAP MaxDB Datenbank

In diesem Dokument werden die Besonderheiten der SnapCenter Integration für die in einer SAP-Umgebung verwendete SAP MaxDB Datenbank beschrieben.

Einführung

Das Dokument soll keine Schritt-für-Schritt-Beschreibung der Einrichtung der gesamten Umgebung sein, sondern umfasst Konzepte und relevante Details zu:

- Beispiel für eine Konfigurationsübersicht
- Beispiellayout
- Sicherung der SAP MaxDB Instanz
- Wiederherstellung der SAP MaxDB Instanz

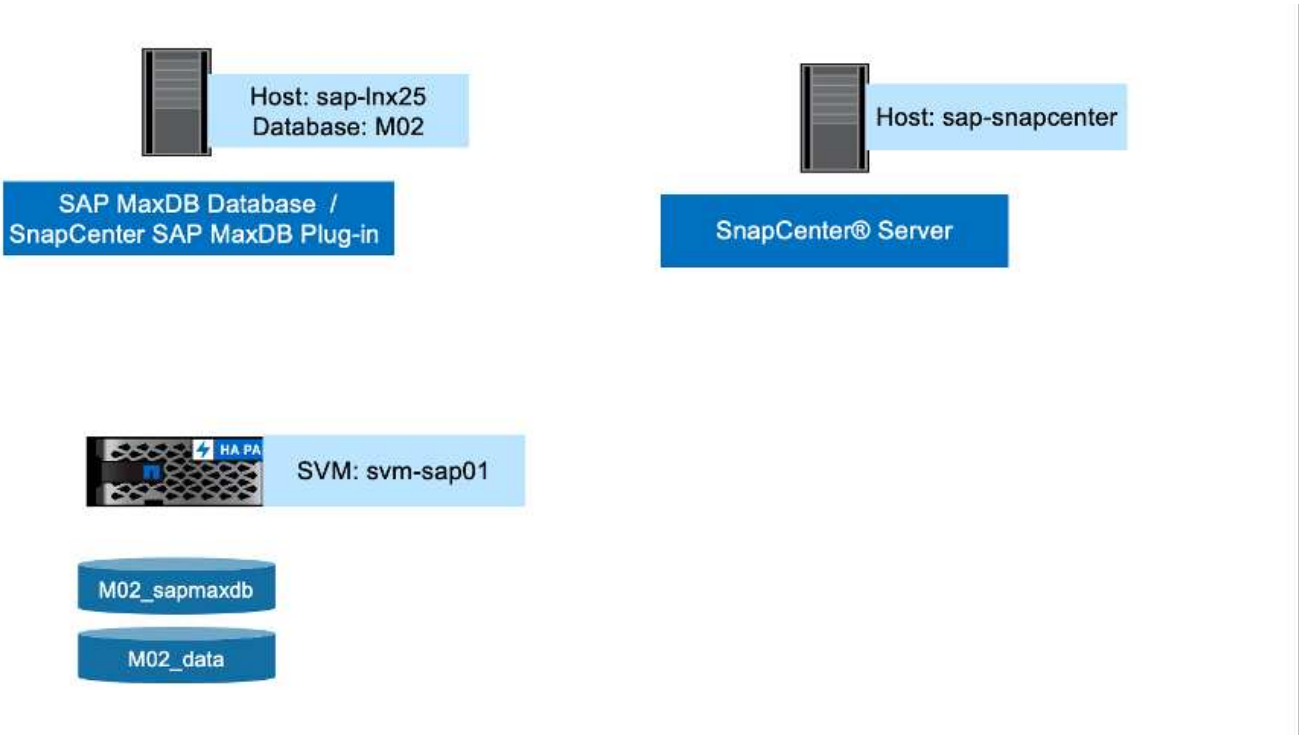
Beispiel für eine Konfigurationsübersicht

Beispiel Implementierung für das SnapCenter MaxDB Plugin für ein SAP System in unserem Demo Center.

Diese Implementierung beschreibt die minimal erforderliche Volume-Konfiguration. Data Dump Backups und Log Dump Backups, Backup Templates, etc. Werden nach SAP Note „1928060 - Datensicherung und Recovery mit Dateisystem Backup“ konfiguriert und von dort aus auf Notes verwiesen.

Alternativ kann die in beschriebene Volume-Struktur "MS TechCommunity Blog"verwendet werden.

Demo-Umgebung



Softwareversionen

Software	Version
Linux BS	SLES FÜR SAP 15 SP5
SAP	SAP NetWeaver 7.5 unterstützt
SAP MaxDB	DBMServer 7.9.10 Build 004-123-265-969
SnapCenter	6,1

MaxDB Volume-Design

Das folgende Least-Volume-Layout muss verwendet werden, um Backup / Recovery und Klonfälle für die SAP MaxDB Datenbank zu ermöglichen. Die Beispielkonfiguration verwendet <SID>: M02.

Volumenname	Verzeichnis (qtree) auf Volumen	Mount-Punkt auf Server	Kommentar
<SID>_sapmaxdb	sapdb	/Sapdb	Übergeordnetes Verzeichnis für MaxDB-bezogene Dateien
		/Sapdb/<SID>/saplog	Redo-Logs (können auf einem anderen Volume platziert werden)
		/Sapdb/<SID>/Backup	Dump Backups (Daten + Protokoll) (kann auf einem anderen Volume platziert werden)

Volumenname	Verzeichnis (qtree) auf Volumen	Mount-Punkt auf Server	Kommentar
	<sid>-Lösungen m	/Home/<sid>-Programm m	Home Verzeichnis der Benutzer <sid> Hmm
	sdb	/Home/sdb	Home-Verzeichnis von Benutzer sdb
	<sid>	/Home/<sid>	Home-Verzeichnis von Benutzer <sid>
	Usrsaptrans	/Usr/sap/trans	Transportverzeichnis
	<SID>	/Usr/sap/<SID>	Usr sap
	<SID>	/Sapmnt/<SID>	SAP GlobalHost-Verzeichnis
<SID>_Data	Sapdata	/Sapdb/<SID>/sapdata	DB-Datendateien (SID)

Schritte zum Schutz von Datenbank M02

- Prüfen Sie die Dateiverteilung gemäß dem Beispiellayout
- Voraussetzungen für den Host prüfen (sap-lnx25)
- Voraussetzungen für die Datenbank prüfen (M02)
- SnapCenter-Agent auf Host bereitstellen/installieren (sap-lnx25)
- Erstellen Sie die Ressourcenkonfiguration der SnapCenter-Instanz

Voraussetzungen auf Host

Weitere aktuelle Informationen stehen zur Verfügung"Hier".

Bevor Sie einen Host hinzufügen und das Plug-in-Paket für Linux installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie können entweder die passwortbasierte Authentifizierung für den Root- oder nicht-Root-Benutzer oder die SSH-Schlüsselauthentifizierung verwenden.
- Das SnapCenter-Plug-in für Unix-Dateisysteme kann von einem Benutzer installiert werden, der kein Root-Benutzer ist. Sie sollten jedoch die sudo-Berechtigungen für den nicht-Root-Benutzer konfigurieren, um den Plug-in-Prozess zu installieren und zu starten. Nach der Installation des Plug-ins werden die Prozesse als effektiver nicht-Root-Benutzer ausgeführt.
- Anmeldedaten mit Authentifizierungsmodus als Linux für den Installationsbenutzer erstellen.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.
- Stellen Sie sicher, dass Sie nur die zertifizierte Version von JAVA 11 auf dem Linux-Host installiert haben
- Informationen zum Herunterladen von JAVA finden Sie unter Java Downloads für alle Betriebssysteme
- Sie sollten bash als Standard-Shell für die Plug-in-Installation verwenden.

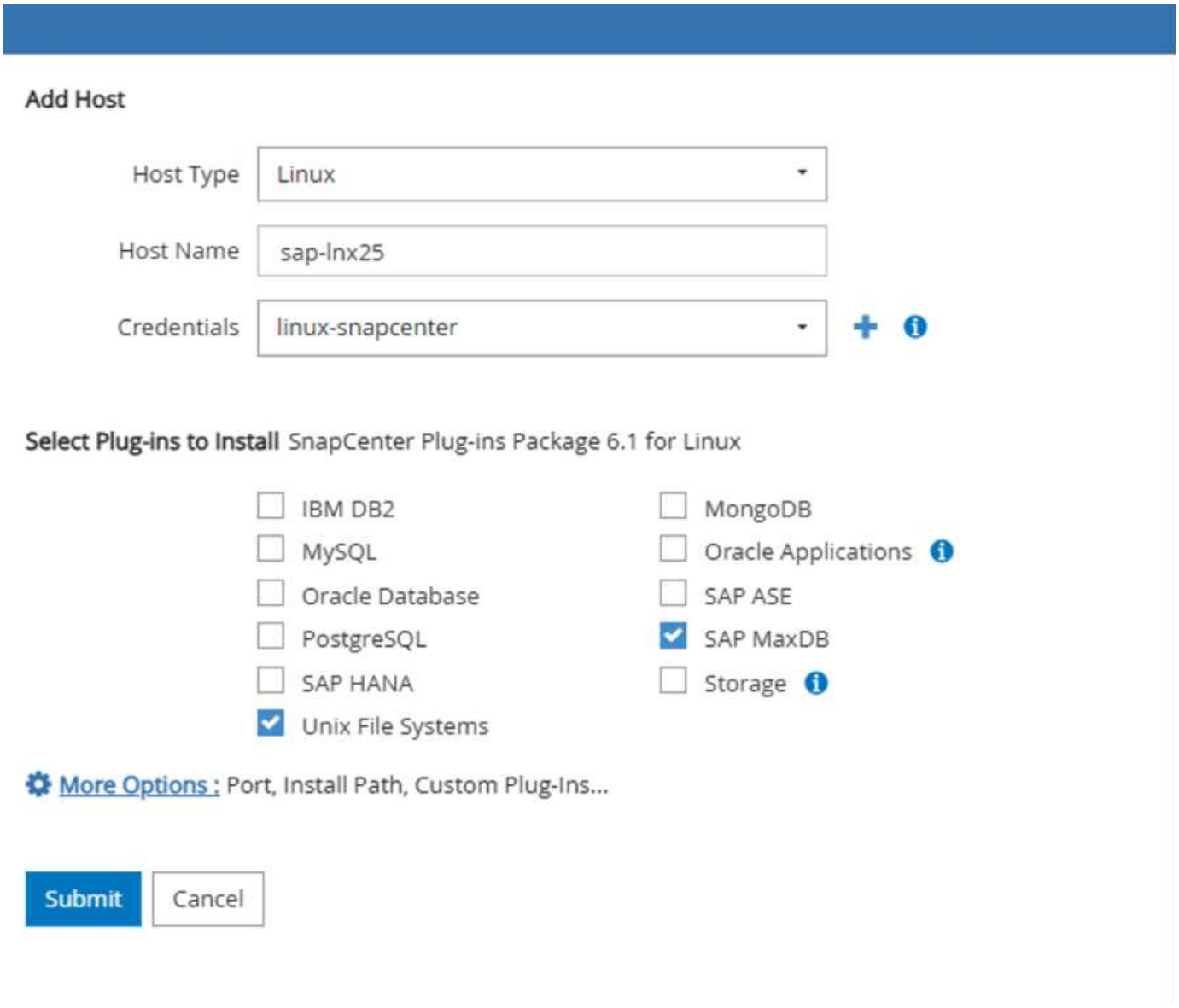
Voraussetzungen für die Datenbank – Backup-Vorlagen erstellen, Logbackup aktivieren

- Erstellen von Verzeichnissen für Daten- und Protokollsicherungen (/sapdb/M02/Backup/Data, /sapdb/M02/Backup/log – owner sdb:sdba – Permissions 755)
- Verbindung zur Datenbank M02 (als OS-User sqdm02)
  - Dbmcli -d M02 -U CONTROL,<password>
- Erstellen Sie eine Data File Backup Template (M02_DATA) gemäß SAP Note 1928060
  - Backup_template_create M02_DATA in DATEI /sapdb/M02/Backup/Data/M02_DATA INHALTSDATEN
- Erstellen Sie eine Data Backup Template (M02_LOG) gemäß SAP Note 1928060
  - Backup_template_create M02_LOG in DATEI /sapdb/M02/Backup/LOG/M02_LOG content LOG
- Erstellen Sie eine Data Snapshot Backup Template (M02_SNAP) gemäß SAP Note 1928060
  - Backup_template_create M02_SNAP auf EXTERNEN SNAPSHOT
- Erstellen Sie Fake-Backup, um die PROTOKOLLSICHERUNG zu aktivieren
  - Util_connect
  - Backup_Start M02_SNAP
  - Backup_Finish M02_SNAP ExternalBackupID First_Full_Fake_Backup
- Wechseln Sie In Den Datenbank-Protokollierungsmodus
  - autolog_off
  - autolog_ON M02_LOG INTERVALL 300
  - autolog_show

Bereitstellung von SnapCenter-Agent für das Hosting von sap-lnx25

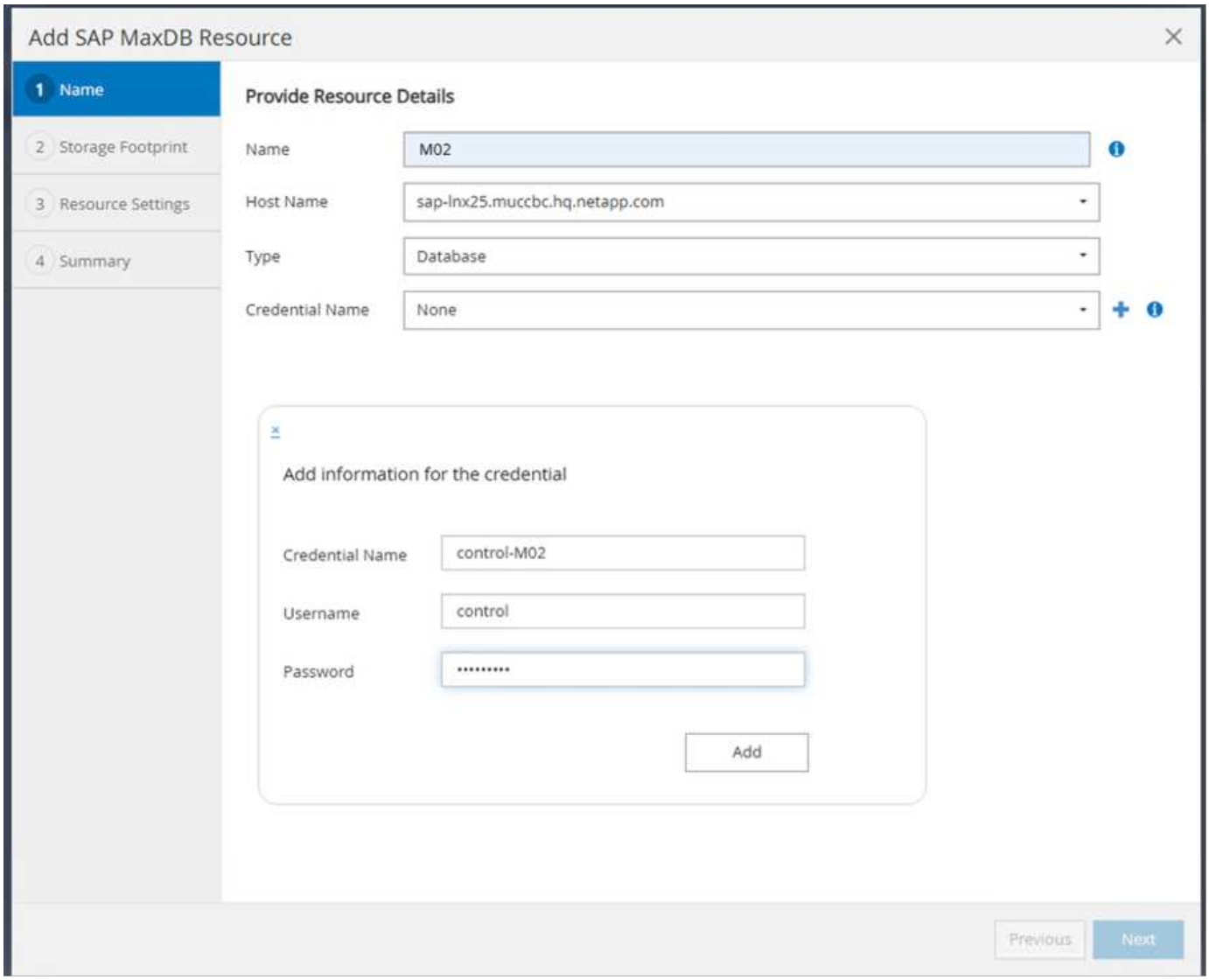
Weitere Informationen finden Sie im "SnapCenter-Dokumentation".

Wählen Sie SAP MaxDB und Unix File Systems Plugins aus.

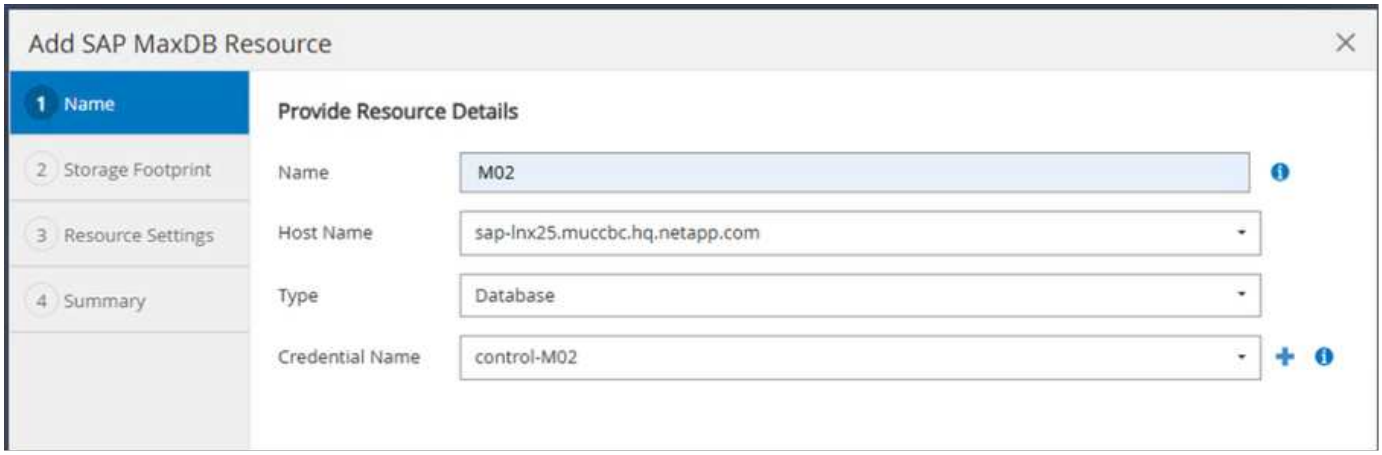


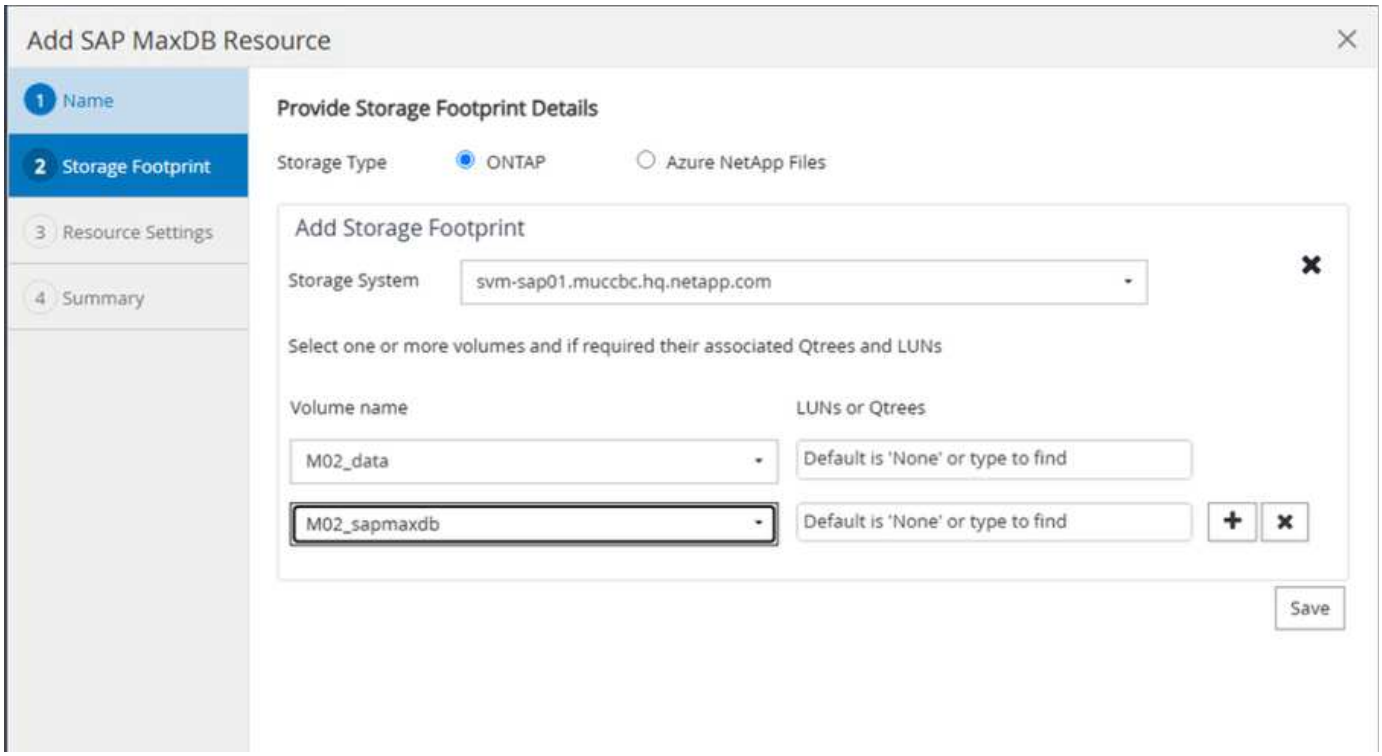
Erstellen Sie eine SnapCenter-Ressourcenkonfiguration für Datenbank M02

Ressourcen → SAP MaxDB → Ressourcen hinzufügen

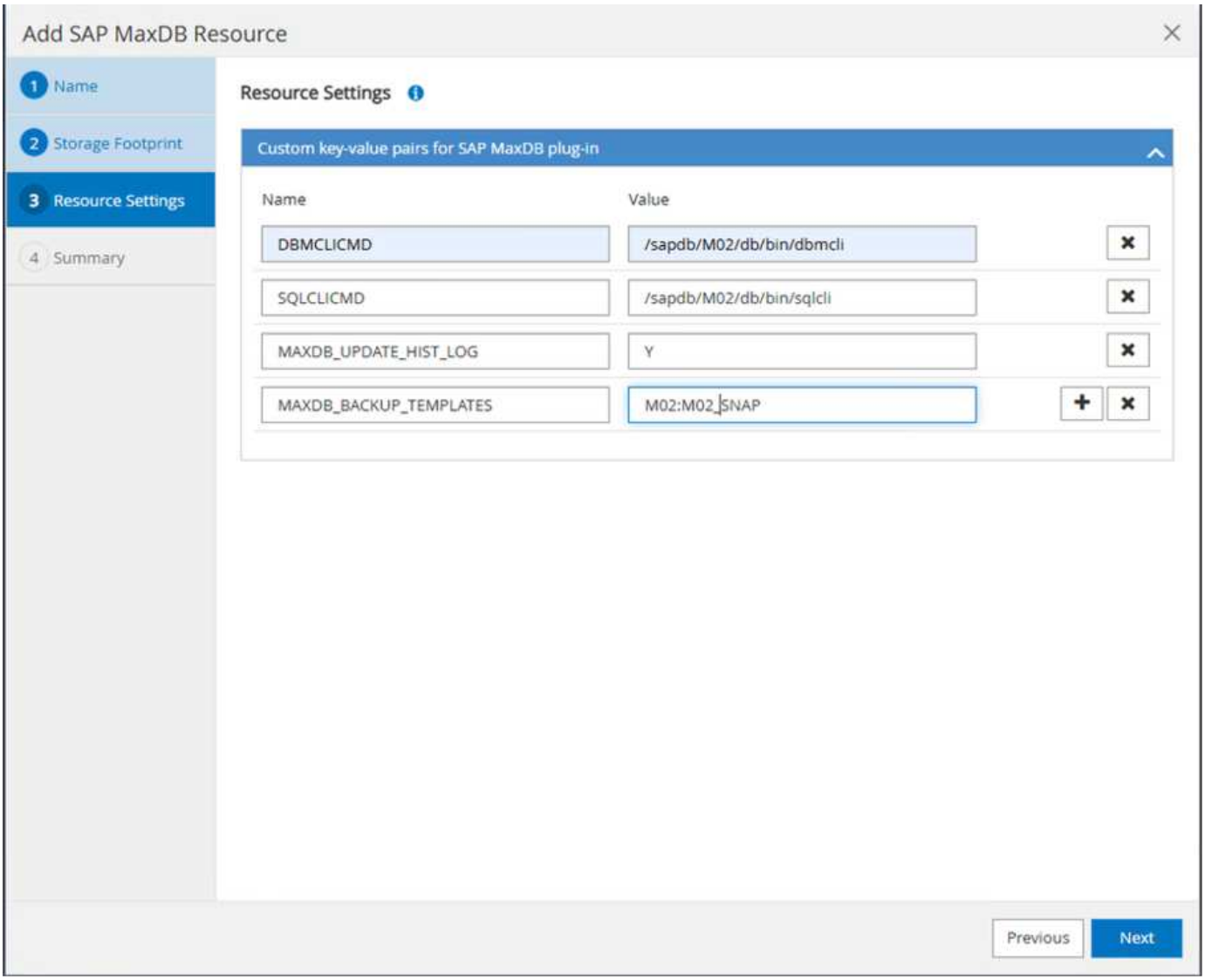


Wenn das Passwort Sonderzeichen enthält, müssen diese mit einem Backslash maskiert werden (z. B. Test!123! → Test\!123\!).





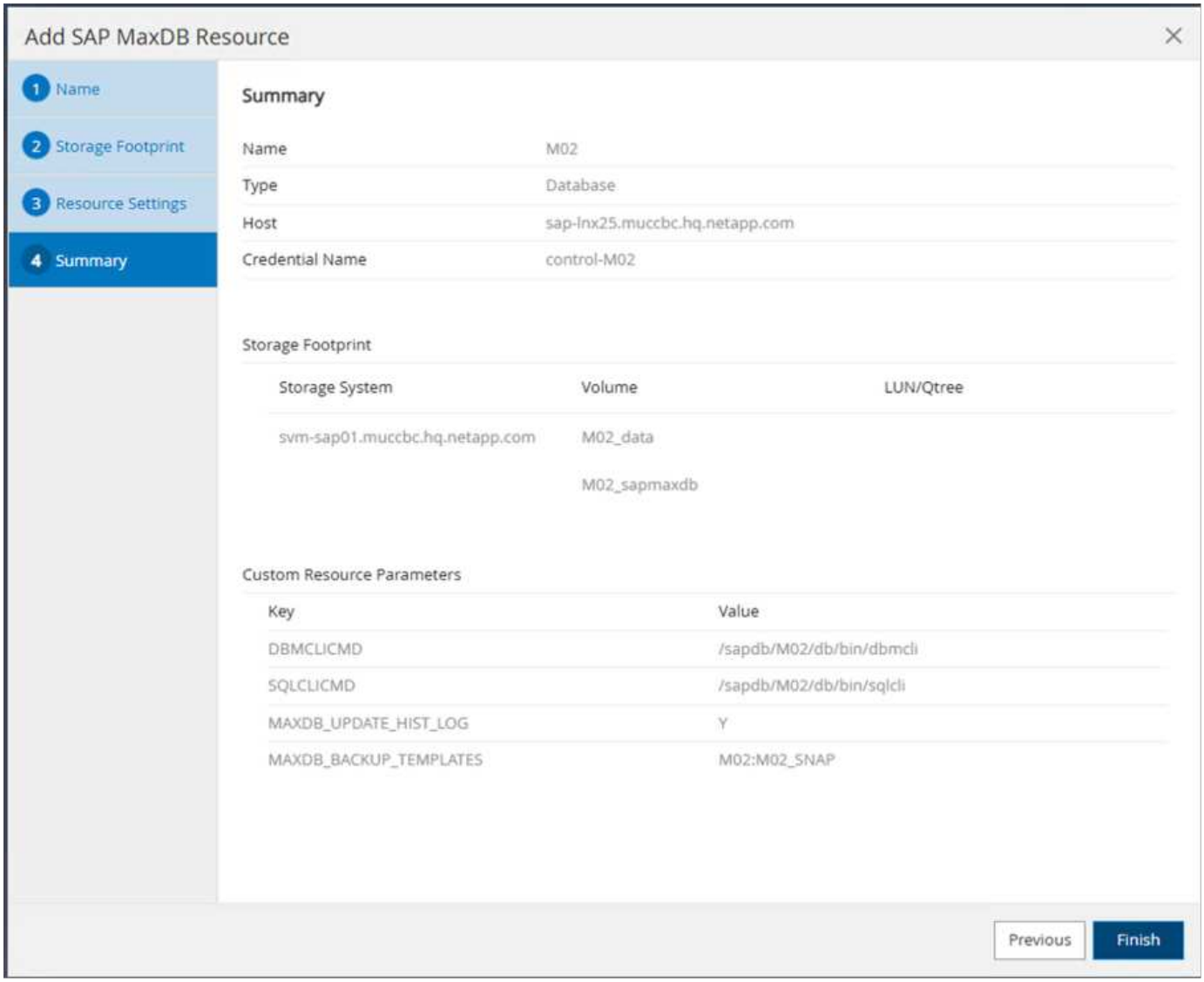
Im Anschluss an die Ressourceneinstellungen müssen (mindestens) benutzerdefinierte Schlüssel-Wert-Paare erstellt werden.



In der folgenden Tabelle sind die MaxDB Plug-in-Parameter aufgeführt, ihre Einstellungen aufgeführt und beschrieben:

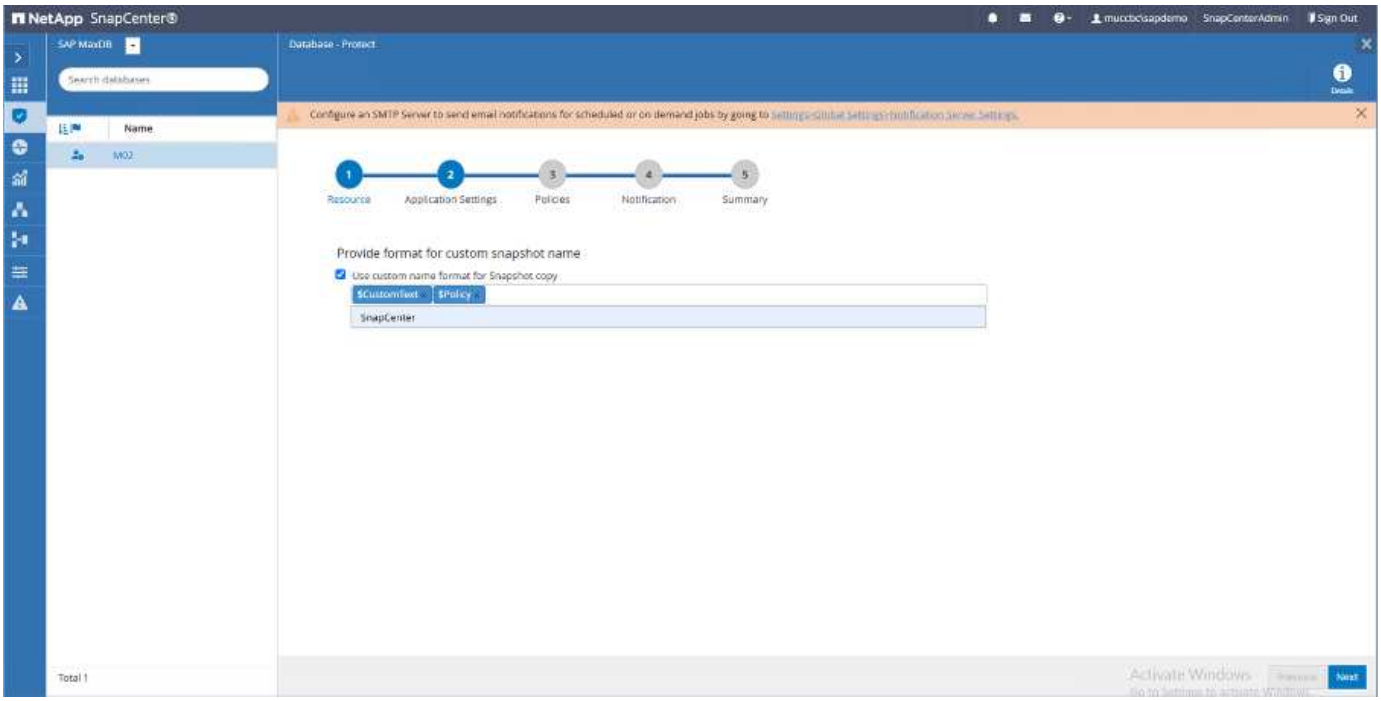
Parameter	Einstellung	Beschreibung
HANDLE_LOGWRITER	(J/N)	Führt die Vorgänge zum Anhalten des Logwriters (N) aus oder führt den Protokollwriter (Y) wieder aus.
DBMCLICMD	Pfad_zu_dbmcli_cmd	Gibt den Pfad zum Befehl MaxDB dbmcli an.Falls nicht gesetzt, wird dbmcli auf dem Suchpfad verwendet.
SQLCLICMD	Pfad_zu_sqlcli_cmd	Gibt den Pfad für den MaxDB sqlcli Befehl an.Wenn nicht festgelegt, wird sqlcli auf dem Suchpfad verwendet.
MAXDB_UPDATE_HIST_LOG	(J/N)	Weist das MaxDB Backup-Programm an, unabhängig davon, ob das MaxDB-Verlaufsprotokoll aktualisiert wird.

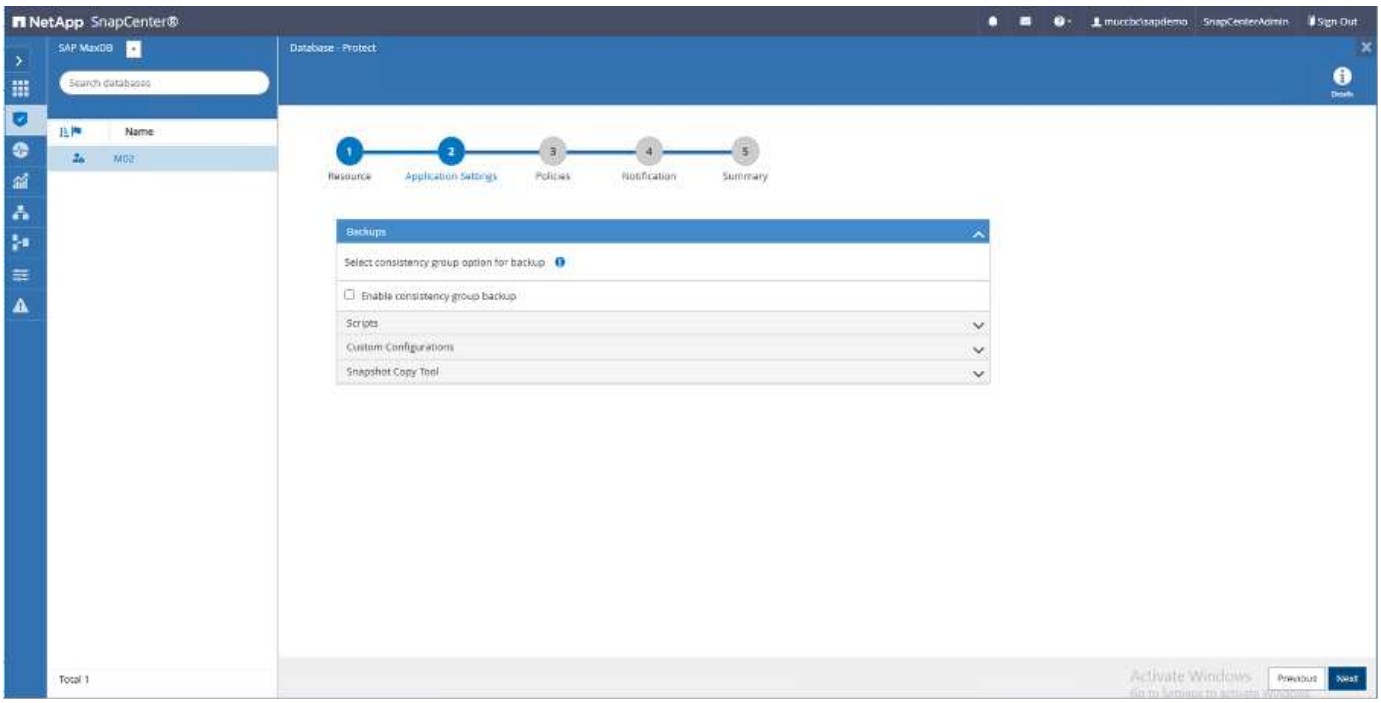
Parameter	Einstellung	Beschreibung
MAXDB_BACKUP_TEMPLATES	Template_Name (z.B. `M02_SNAP`)	Gibt eine Sicherungsvorlage für jede Datenbank an.die Vorlage muss bereits vorhanden sein und ein externer Typ von Backup-Vorlage sein. Um die Integration von Snapshot Kopien für MaxDB 7.8 und höher zu aktivieren, müssen Sie über eine Hintergrundserverfunktion von MaxDB und bereits konfigurierte MaxDB Backup-Vorlage verfügen.
MAXDB_BG_SERVER_PREFIX	bg_Server_PREFIX (z.B. `na_bg`)	Gibt das Präfix für den Namen des Hintergrundservers an. Wenn der Parameter MAXDB_BACKUP_TEMPLATES festgelegt ist, müssen Sie auch DEN PARAMETER MAXDB_BG_SERVER_PREFIX festlegen. Wenn Sie das Präfix nicht festlegen, wird der Standardwert na_bg_DATABASE verwendet.

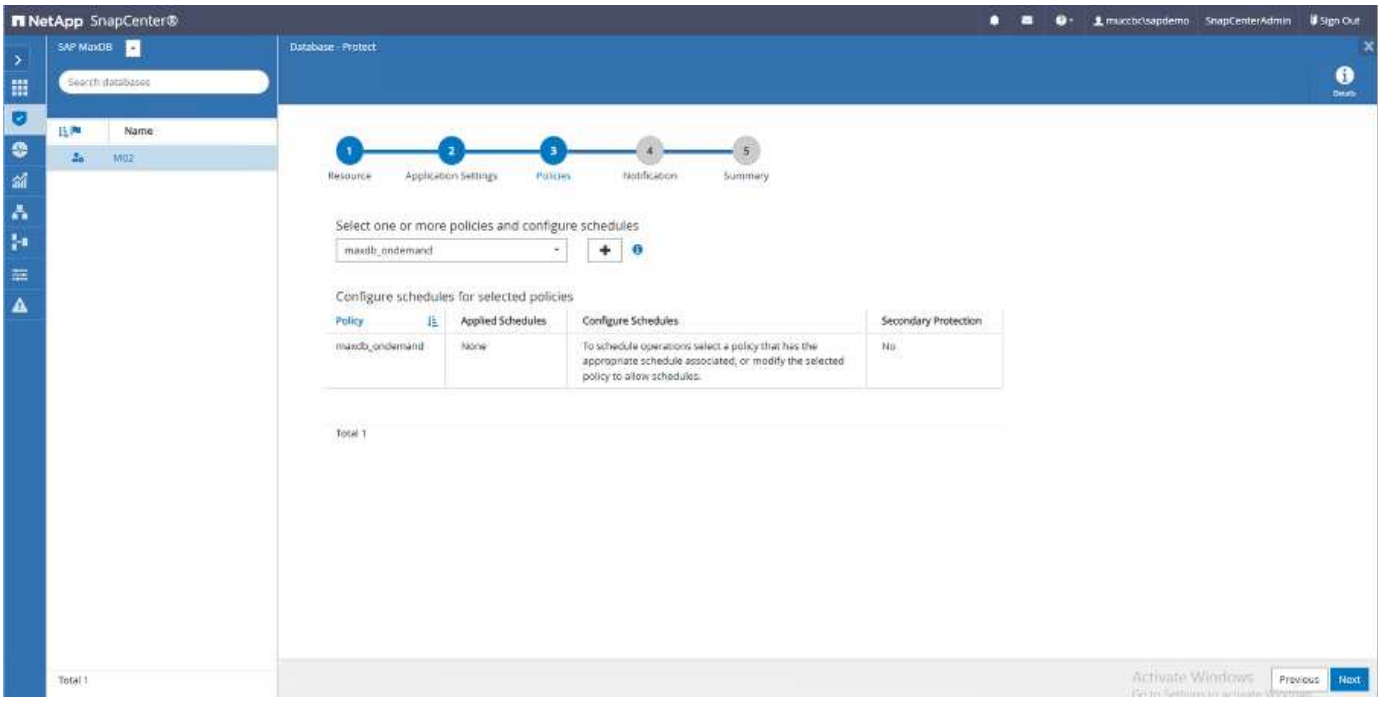


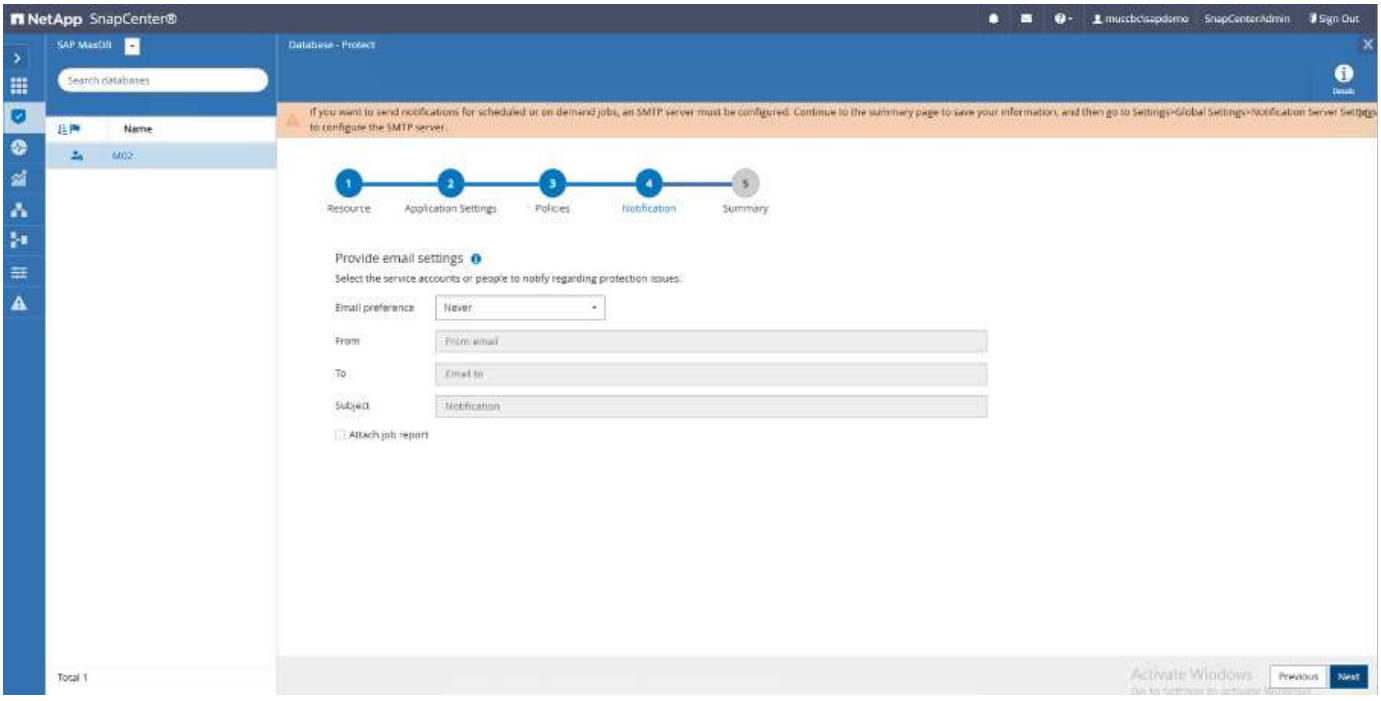
Nun könnte die Konfiguration abgeschlossen und die Sicherung nach dem Gesamtschutzkonzept geplant werden.

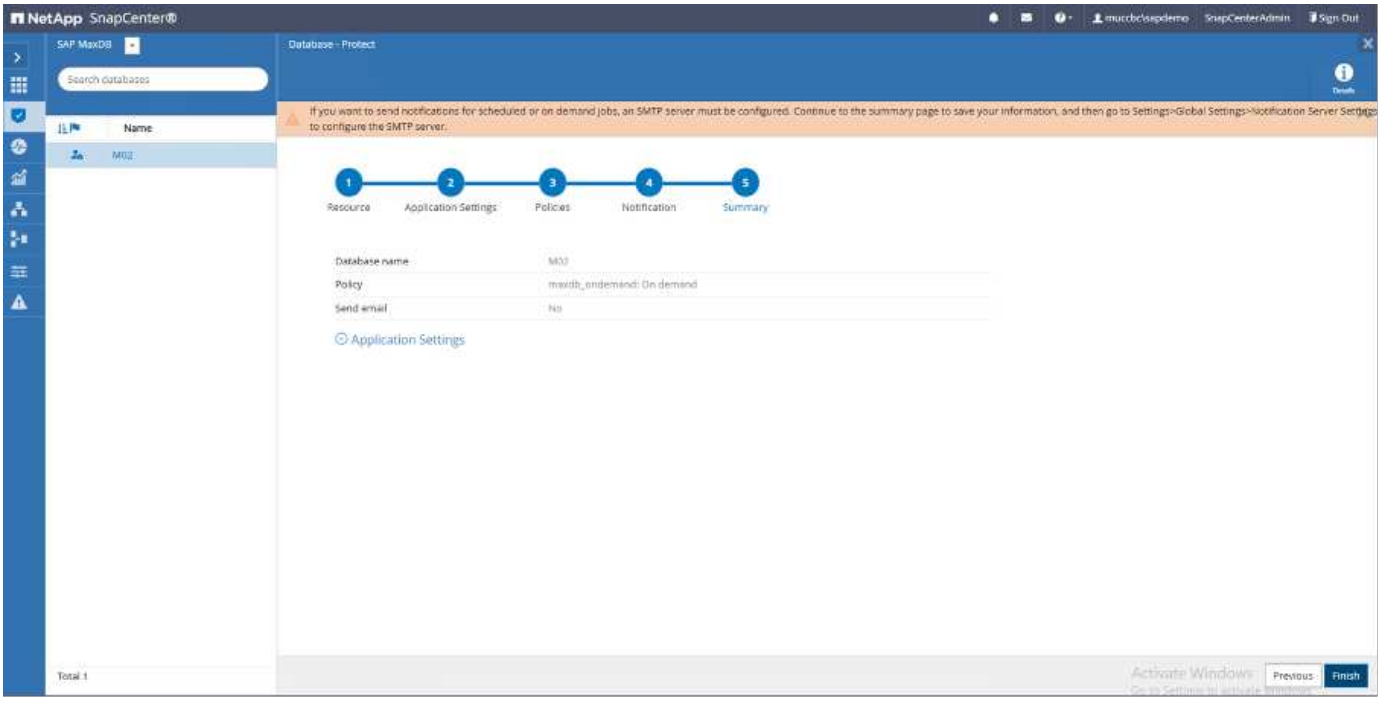

NetApp SnapCenter®
SAP MaxDB
View
Database
Search databases
Dashboard
Resources
Monitor
Reports
Hosts
Storage Systems
Settings
Alerts
Name
Type
Host
Resource Groups
Policies
Last backup
Overall Status
M02
Database
Not protected


NetApp SnapCenter®
SAP MaxDB
Search databases
Name
M02
Total 1
Database - Protect
Configure an SMTP Server to send email notifications for scheduled or on demand jobs by going to Settings>Global Settings>Notification Server Settings.
1 Resource
2 Application Settings
3 Policies
4 Notification
5 Summary
Provide format for custom snapshot name
Use custom name format for Snapshot copy
$CustomText
$Policy
SnapCenter
Activate Windows
Next


NetApp SnapCenter®
SAP MaxDB
Search databases
Name
M02
Total 1
Database - Protect
1 Resource
2 Application Settings
3 Policies
4 Notification
5 Summary
Backups
Select consistency group option for backup
Enable consistency group backup
Scripts
Custom Configurations
Snapshot Copy Tool
Activate Windows
Previous
Next


NetApp SnapCenter®
SAP MaxDB
Search databases
Name
M02
Total 1
Database - Protect
1 Resource
2 Application Settings
3 Policies
4 Notification
5 Summary
Select one or more policies and configure schedules
maxdb_ondemand
Configure schedules for selected policies
Policy
Applied Schedules
Configure Schedules
Secondary Protection
maxdb_ondemand
None
To schedule operations select a policy that has the appropriate schedule associated, or modify the selected policy to allow schedules.
No
Total 1
Activate Windows
Previous
Next


NetApp SnapCenter®
SAP MaxDB
Search databases
Name
M02
Total 1
Database - Protect
If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.
1 Resource
2 Application Settings
3 Policies
4 Notification
5 Summary
Provide email settings
Select the service accounts or people to notify regarding protection issues.
Email preference
Never
From
From email
To
Email to
Subject
Notification
Attach job report
Activate Windows
Previous
Next

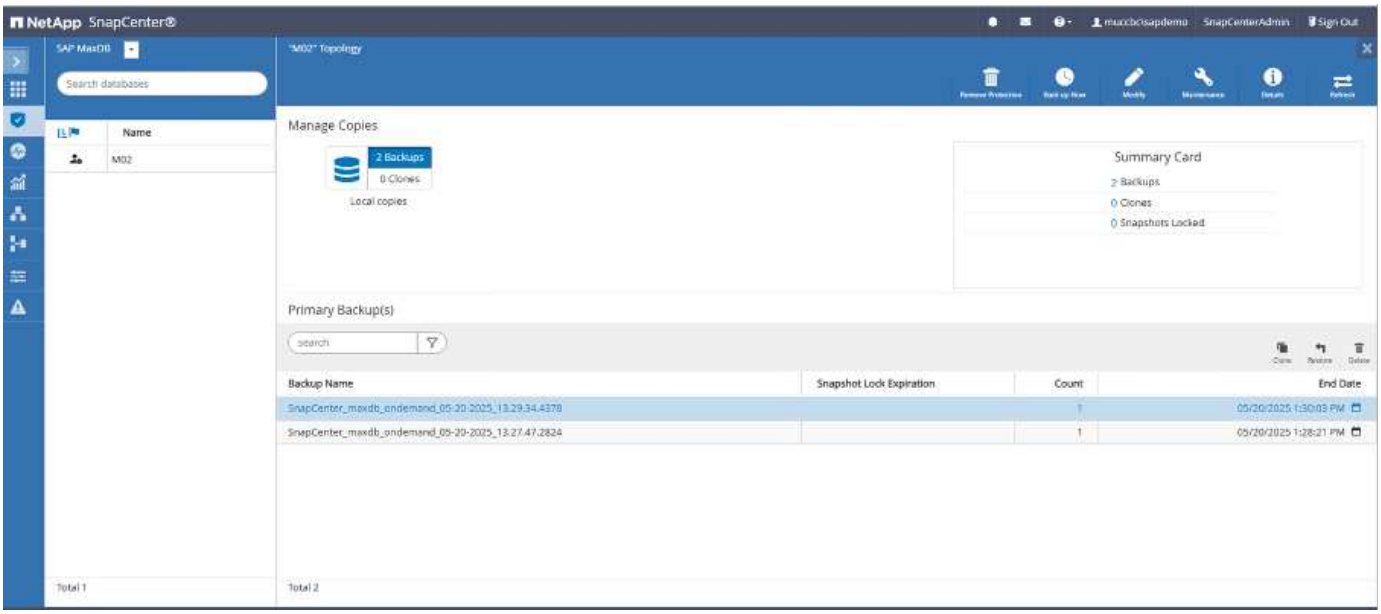


Sequenz zum Wiederherstellen von System M02

1. SAP System M02 stoppen (einschließlich Datenbank), sapinit stoppen
2. Umount Filesystem /sapdb/M02/sapdata
3. Wiederherstellen von Volumes M02_Data (mit SnapCenter)
4. Mounten Sie das Dateisystem /sapdb/M02/sapdata
5. Datenbank M02 starten und verbinden (Admin-Modus)
6. Backup-Informationen Erfassen
7. Stellen Sie das Backup von Datenbankdaten wieder her
8. Stellen Sie die Datenbank-Protokollsicherungen wieder her
9. Datenbank anhalten
10. Starten Sie sapinit, SAP System M02

Instanz M02 wiederherstellen

- Beenden Sie SAP System + DB M02 auf Host sap-lnx25
  - User m02adm: Stopsap
  - Optional – Wenn die Datenbank nicht erfolgreich angehalten wurde – Benutzer: Sqdm02
  - Dbmcli -d M02 -U CONTROL,<password>
    - db_offline
  - User root: /Etc/init.d/sapinit stop
  - User root: Umount /sapdb/M02/sapdata
- Backup Wiederherstellen
  - SnapCenter GUI: Wählen Sie erforderliche Bacukp für die Wiederherstellung

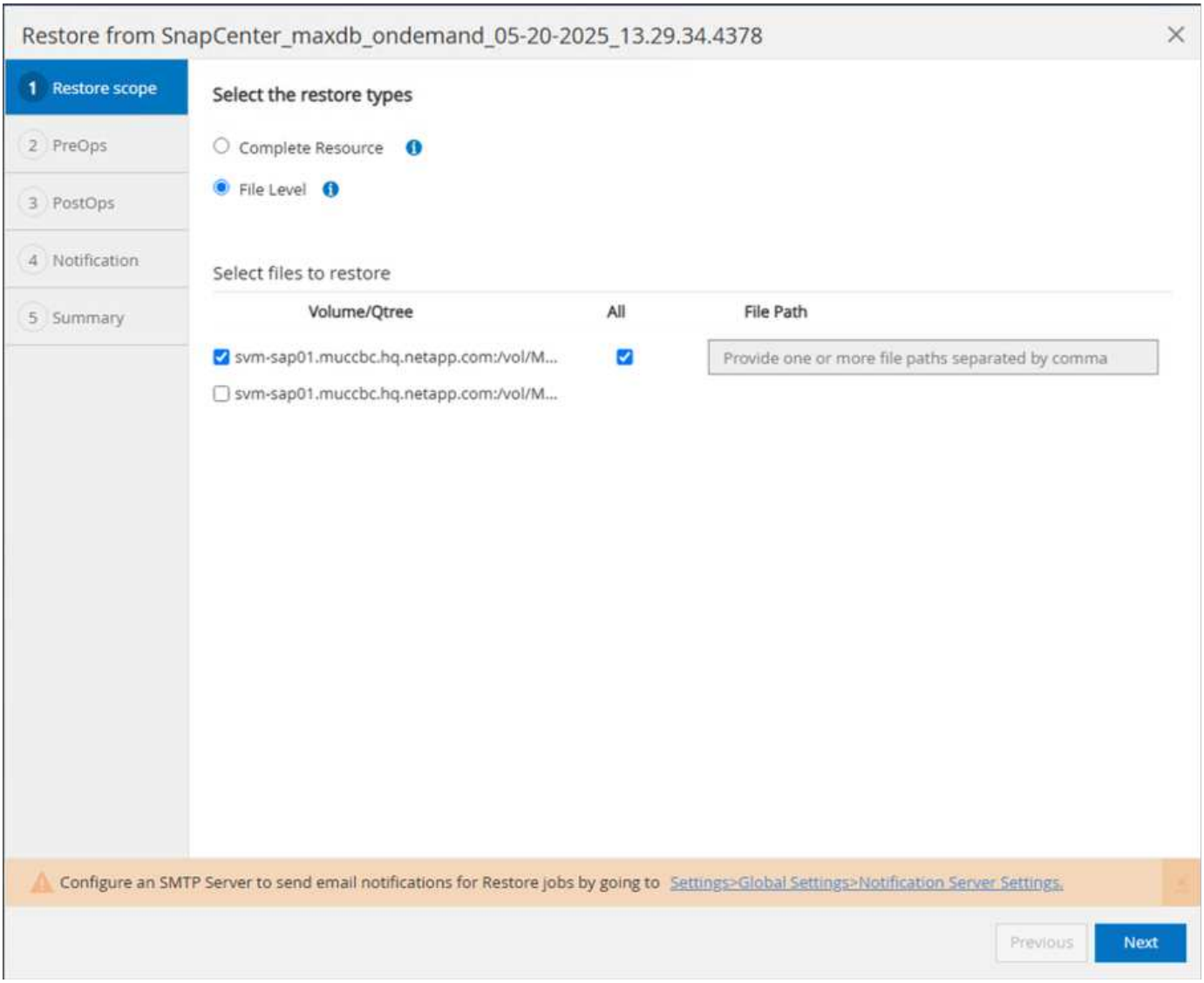


Wenn Sie die Option „Complete Resource“ auswählen, wird eine Volume-basierte Snap Restore (VBSR) ausgelöst. Innerhalb von Azure wird sie aufgerufen"Lautstärke zurücksetzen". Für die ANF-Bereitstellung * nur vollständige Ressource verfügbar*.

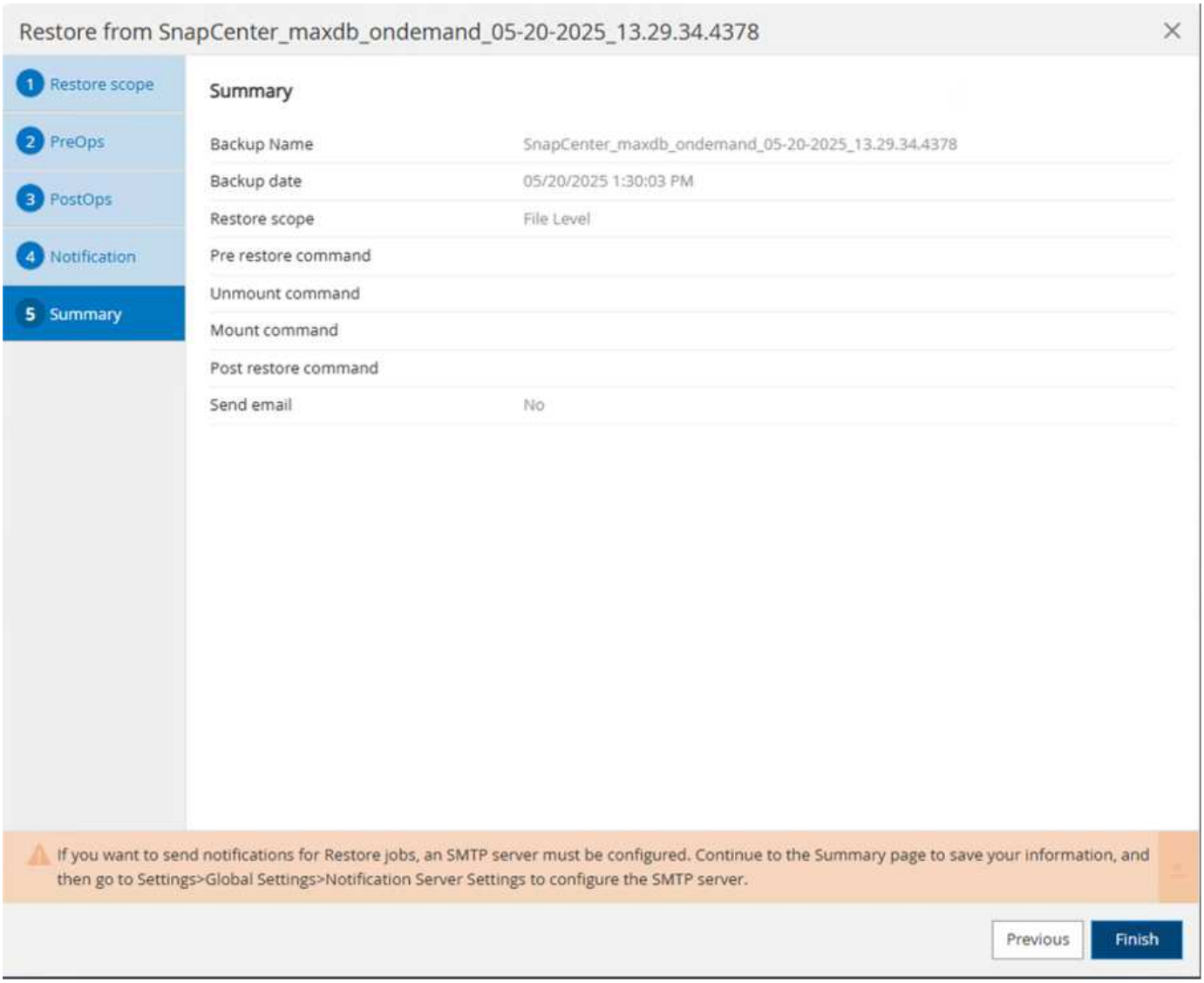
Important

Active filesystem data and snapshots that were taken after the selected snapshot will be lost. The snapshot revert operation will replace *all* the data in the targeted volume with the data in the selected snapshot. You should pay attention to the snapshot contents and creation date when you select a snapshot. You cannot undo the snapshot revert operation.

Für andere Implementierungstypen (z. B. On-Premises-ANF) könnte ein SFSR-Vorgang (Single File Snap Restore) orchestriert werden. Wählen Sie File Level und das entsprechende Volume und aktivieren Sie „All“ – siehe folgenden Screenshot.



Die Zusammenfassung wird angezeigt und mit „Fertig stellen“ wird die eigentliche Wiederherstellung gestartet.



- Dateisysteme mounten (sap-lnx25)
  - User root: Mount /sapdb/M02/sapdata
- Datenbank M02 im Admin-Modus starten und verbinden
  - Benutzer: Sqdm02: Dbmcli -d M02 -U CONTROL,<password>
    - db_admin
    - db_Connect
- Backup-Informationen Erfassen
  - Backup_history_open
  - Backup_history_list -c Label,Aktion,Seiten,stop,media -r Last

```
dbmcli on M02>backup_history_list -c label,action,pages,stop,media -r last
OK
END
DAT_000000008|SAVE WARM|         0|2025-05-20 13:29:50|M02_SNAP

---
```

- Stellen Sie Die Datenbank Wieder Her

- Wiederherstellung Von Daten-Backups
  - Recover_Start M02_SNAP Data ExternalBackupID DAT_000000008

```
dbmcli on M02>recover_start M02_SNAP data ExternalBackupID DAT_000000008
OK
Returncode              0
Date                    20250520
Time                    00151550
Server                  sap-lnx25
Database                M02
Kernel Version          Kernel    7.9.10   Build 004-123-265-969
Pages Transferred       0
Pages Left
Volumes
Medianame               M02_SNAP
Location
Errortext
Label                   DAT_000000008
Is Consistent           true
First LOG Page          512226
Last LOG Page
DB Stamp 1 Date         20250520
DB Stamp 1 Time         00132933
DB Stamp 2 Date
DB Stamp 2 Time
Page Count
Devices Used            0
Database ID             sap-lnx25:M02_20241203_104036
Max Used Data Page      3187892
Converter Page Count

---
```

- Protokollsicherung bei Bedarf wiederherstellen
  - Z. B. Recover_Start M02_LOG LOG 147

```
dbmcli on M02>recover_start M02_LOG LOG 147
OK
Returncode              0
Date                    20250521
Time                    00112001
Server                  sap-lnx25
Database                M02
Kernel Version          Kernel    7.9.10   Build 004-123-265-969
Pages Transferred       24
Pages Left              0
Volumes                 1
Medianame               M02_LOG
Location                /sapdb/M02/backup/log/M02_LOG.147
Errortext
Label                   LOG_000000147
Is Consistent
First LOG Page          514072
Last LOG Page           514075
DB Stamp 1 Date         20250520
DB Stamp 1 Time         00180238
DB Stamp 2 Date         20250520
DB Stamp 2 Time         00180539
Page Count              4
Devices Used            1
Database ID             sap-lnx25:M02_20241203_104036
Max Used Data Page
Converter Page Count
```

- Optionale Informationen – autorecover auf einen bestimmten Zeitstempel (ohne Angabe dedizierter Daten/Protokollbackp
  - Z. B. autorecover bis 20250520 200000

```
---
dbmcli on M02>autorecover until 20250520 200000
OK
Returncode              0
Date                    20250521
Time                    00131559
Server                  sap-lnx25
Database                M02
Kernel Version          Kernel    7.9.10   Build 004-123-265-969
Pages Transferred       10096
Pages Left              0
Volumes                 1
Medianame               M02_LOG
Location                /sapdb/M02/backup/log/M02_LOG.102
Errortext
Label                   LOG_000000102
Is Consistent
First LOG Page          256227
Last LOG Page           341559
DB Stamp 1 Date         20241203
DB Stamp 1 Time         00190348
DB Stamp 2 Date         20241226
DB Stamp 2 Time         00193615
Page Count              85333
Devices Used            1
Database ID             sap-lnx25:M02_20241203_104036
Max Used Data Page
Converter Page Count

---
```

- Recovery beenden und Datenbank anhalten

- db_offline

> Weitere Informationen über Recovery finden Sie im "MaxDB-Dokumentation"

- Starten Sie das SAP-System
  - User root: /Etc/init.d/sapinit Start
  - Benutzer m02adm: Startsap

Zusätzliche Informationen und Versionsverlauf

Aufgezeichnete Demos

Folgende neu kodierte Demos stehen zur Unterstützung der Dokumentation zur Verfügung.

Installation MaxDB Plugin, Konfiguration MaxDB Plugin, Sicherung der MaxDB Datenbank

Restore und Recovery der MaxDB Datenbank

Externe Dokumentation

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

- "SAP Installation Azure auf ANF"
- "SnapCenter-Voraussetzungen für Plugins"
- "SnapCenter Installations-Plugins"
- "MaxDB Recovery-Dokumentation"
- SAP-Hinweise (Anmeldung erforderlich)
  - "1928060 - Datensicherung und -Wiederherstellung mit Dateisystemsicherung"
  - "2282054 - DBM-Hintergrundserver"
  - "616814 - Protokollschreiber für Split Mirror oder Snapshot unterbrechen"
- "Howto - SAP MaxDB Backup mit Datenbank-Manager CLI"
- "Howto - SAP MaxDB Wiederherstellung mit Datenbank-Manager CLI"
- "NetApp Produktdokumentation"
- "NetApp SAP-Lösungen – Informationen zu Anwendungsfällen, Best Practices und Vorteilen"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	Mai 2025	Erste Version – Backup / Recovery MaxDB-Datenbank