



# **SAP HANA Plug-in Operations**

## **Snap Creator Framework**

NetApp

October 04, 2023

This PDF was generated from [https://docs.netapp.com/de-de/snap-creator-framework/sap-hana-ops/concept\\_considerations\\_for\\_backing\\_up\\_sap\\_hana\\_systems.html](https://docs.netapp.com/de-de/snap-creator-framework/sap-hana-ops/concept_considerations_for_backing_up_sap_hana_systems.html) on October 04, 2023. Always check docs.netapp.com for the latest.

# Inhalt

- SAP HANA Plug-in Operations Guide . . . . . 1
  - Überblick über die Backup- und Restore-Lösung für SAP HANA . . . . . 1
  - Installation und Konfiguration der erforderlichen Softwarekomponenten . . . . . 6
  - Konfigurieren von Daten-Backups . . . . . 9
  - Konfiguration von SAP HANA für SAN-Umgebungen . . . . . 31
  - Protokollsicherungen werden konfiguriert . . . . . 31
  - Datenbank-Backups werden ausgeführt . . . . . 33
  - SAP HANA dateibasiertes Backup und Integritätsprüfung der Datenbank . . . . . 38
  - Wiederherstellung von SAP HANA Datenbanken . . . . . 42
  - Plug-in-Parameter für SAP HANA . . . . . 71
  - Fehlerbehebung . . . . . 73
  - Weitere Schritte . . . . . 76

# SAP HANA Plug-in Operations Guide

Das SAP HANA Plug-in für Snap Creator 4.3.3 kann konfiguriert und für das Backup und die Wiederherstellung von SAP HANA Datenbanken verwendet werden.

## Überblick über die Backup- und Restore-Lösung für SAP HANA

SAP-Anwendungen von Unternehmen müssen heute sieben Tage die Woche 24 Stunden am Tag zur Verfügung stehen. Unabhängig vom wachsenden Datenvolumen und routinemäßigen Wartungsaufgaben, wie System-Backups, wird eine konsistente Performance erwartet.

Das Ausführen von SAP Datenbank-Backups kann einen deutlichen Performance-Effekt auf ein SAP-Produktionssystem haben. Da Backup-Fenster immer kleiner werden und die Menge der zu sichernden Daten zunimmt, lässt sich der Zeitpunkt für die Durchführung von Backups mit minimalen Auswirkungen auf Geschäftsprozesse nur schwer definieren. Von besonderer Bedeutung ist die Zeit für die Wiederherstellung von SAP-Systemen, da die Ausfallzeiten minimiert werden müssen.

### Überlegungen für das Backup von SAP HANA Systemen

SAP HANA-Administratoren müssen ein zuverlässiges Service-Level erfüllen und so die Ausfallzeiten oder Performance-Verschlechterung aufgrund von Backups minimieren.

Um ein solches Service-Level zu bieten, kämpfen SAP HANA-Administratoren mit Herausforderungen in den folgenden Bereichen:

- Performance-Effekt auf SAP-Produktionssysteme

Backups haben in der Regel erhebliche Auswirkungen auf die Performance des produktiven SAP-Systems, da der Datenbankserver, das Storage-System und das Storage-Netzwerk während der Backups sehr belastet werden.

- Kleiner werdende Backup-Fenster

Backups können nur zu Zeiten erstellt werden, in denen I/O- oder Batch-Aktivitäten auf dem SAP-System stattfinden. Es ist sehr schwierig, ein Backup-Fenster zu definieren, wenn das SAP-System die ganze Zeit aktiv ist.

- Rasantes Datenwachstum

Das rasante Datenwachstum und die immer kleiner werdenden Backup-Fenster führen zu laufenden Investitionen in die Backup-Infrastruktur: Mehr Bandlaufwerke, neue Bandlauftechnologie und schnellere Speichernetzwerke. Wachsende Datenbanken führen zu mehr Bandmedien oder Speicherplatz für Backups. Inkrementelle Backups können diese Probleme beheben, aber sie führen zu einem sehr langsamen Restore-Prozess, der normalerweise nicht akzeptabel ist.

- Steigende Kosten durch Ausfallzeiten

Ungeplante Ausfallzeiten eines SAP-Systems haben immer finanzielle Auswirkungen auf das Geschäft. Ein wesentlicher Teil der ungeplanten Ausfallzeit ist die Zeit, die für die Wiederherstellung des SAP-Systems bei einem Ausfall erforderlich ist. Die Architektur für Backup und Recovery muss auf der Grundlage einer

akzeptablen Recovery-Zeitvorgabe (Recovery Time Objective, RTO) entwickelt werden.

- Backup und Recovery-Zeit

Backup- und Recovery-Zeit sind auch in SAP Upgrade-Projekten enthalten. Der Projektplan für ein SAP-Upgrade umfasst immer mindestens drei Backups der SAP-Datenbank. Die zur Durchführung dieser Backups benötigte Zeit verringert die für den Upgrade-Prozess verfügbare Gesamtdauer. Die Entscheidung, ob Backup und Recovery durchgeführt werden sollen, hängt in der Regel von der Zeit ab, die zum Wiederherstellen der Datenbank aus dem zuvor erstellten Backup benötigt wird. Durch die Möglichkeit zur sehr schnellen Wiederherstellung wird mehr Zeit zur Lösung von Problemen bereitgestellt, die während des Upgrades auftreten können, anstatt das System wieder in seinen vorherigen Zustand wiederherzustellen.

## Die Lösung von NetApp

Ein Datenbank-Backup kann mit NetApp Snapshot Technologie 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 Datenblöcke verschoben werden.

Der Einsatz von Snapshot-Technologie hat auch keine Auswirkungen auf die Performance des SAP-Produktionssystems. Daher kann die Erstellung von Snapshot Kopien ohne Berücksichtigung von Spitzenzeiten geplant werden. SAP- und NetApp-Kunden planen in der Regel mehrere Online-Snapshot-Backups während des Tages. So können beispielsweise alle vier Stunden Backups durchgeführt werden. Diese Snapshot Backups werden in der Regel drei bis fünf Tage auf dem primären Storage-System gespeichert.

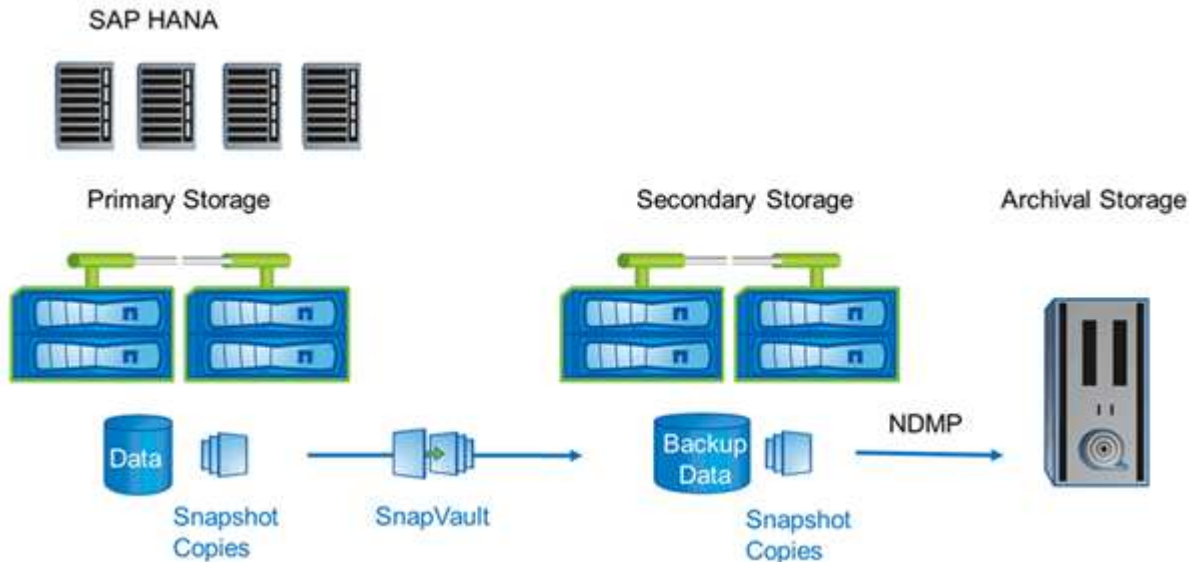
Snapshot Kopien bieten auch wichtige Vorteile für den Restore- und Recovery-Vorgang. Die Funktion von NetApp SnapRestore ermöglicht die Wiederherstellung der gesamten Datenbank oder von Teilen der Datenbank bis zu dem Zeitpunkt, zu dem eine verfügbare Snapshot-Kopie erstellt wurde. Dieser Restore-Prozess dauert nur wenige Minuten, unabhängig von der Größe der Datenbank. Der Recovery-Prozess verkürzt sich ebenfalls drastisch, da tagsüber mehrere Snapshot Kopien erstellt wurden und weniger Protokolle angewendet werden müssen.

Snapshot-Backups werden auf demselben Festplattensystem gespeichert, auf dem die aktiven Online-Daten gespeichert werden. NetApp empfiehlt daher die Verwendung von Snapshot-Backups als Ergänzung und kein Ersatz für Backups an einem sekundären Standort wie Festplatte oder Tape. Obwohl Backups an einen Sekundärstandort weiterhin notwendig sind, ist die Wahrscheinlichkeit, dass diese Backups für Restore und Recovery erforderlich werden, nur gering. Die meisten Restore- und Recovery-Aktionen werden mithilfe von SnapRestore im primären Storage-System durchgeführt. Restores von einem Sekundärstandort sind nur nötig, wenn das primäre Storage-System, auf dem die Snapshot-Kopien gespeichert sind, beschädigt ist oder wenn es zur Wiederherstellung eines Backups erforderlich ist, das über eine Snapshot Kopie nicht mehr verfügbar ist. Möglicherweise müssen Sie vor zwei Wochen ein Backup wiederherstellen.

Ein Backup an einen sekundären Standort basiert immer auf Snapshot-Kopien, die auf dem primären Storage erstellt wurden. Somit werden die Daten direkt aus dem primären Storage-System eingelesen, ohne dass dabei der SAP Datenbankserver belastet wird. Der primäre Storage kommuniziert direkt mit dem sekundären Storage und sendet die Backup-Daten über das SnapVault Disk-to-Disk Backup an das Ziel. Die NetApp SnapVault Funktion bietet entscheidende Vorteile im Vergleich zu herkömmlichen Backups. Nach einem anfänglichen Datentransfer, bei dem alle Daten von der Quelle an das Ziel übertragen werden müssen, werden bei allen nachfolgenden Backups nur die geänderten Blöcke in den sekundären Storage kopiert. Dies reduziert die Last des primären Storage-Systems deutlich und die Zeit für ein komplettes Backup. Ein vollständiges Datenbank-Backup benötigt weniger Festplattenspeicher, da SnapVault nur die geänderten Blöcke am Ziel

speichert.

Unter Umständen ist weiterhin eine Sicherung der Daten auf Tape erforderlich, da ein Langzeit-Backup erforderlich ist. Dabei könnte es sich beispielsweise um ein wöchentliches Backup handeln, das ein Jahr lang aufbewahrt wird. In diesem Fall kann die Tape-Infrastruktur direkt mit dem sekundären Storage verbunden werden. Die Daten können mithilfe des Network Data Management Protocol (NDMP) auf Tape geschrieben werden.



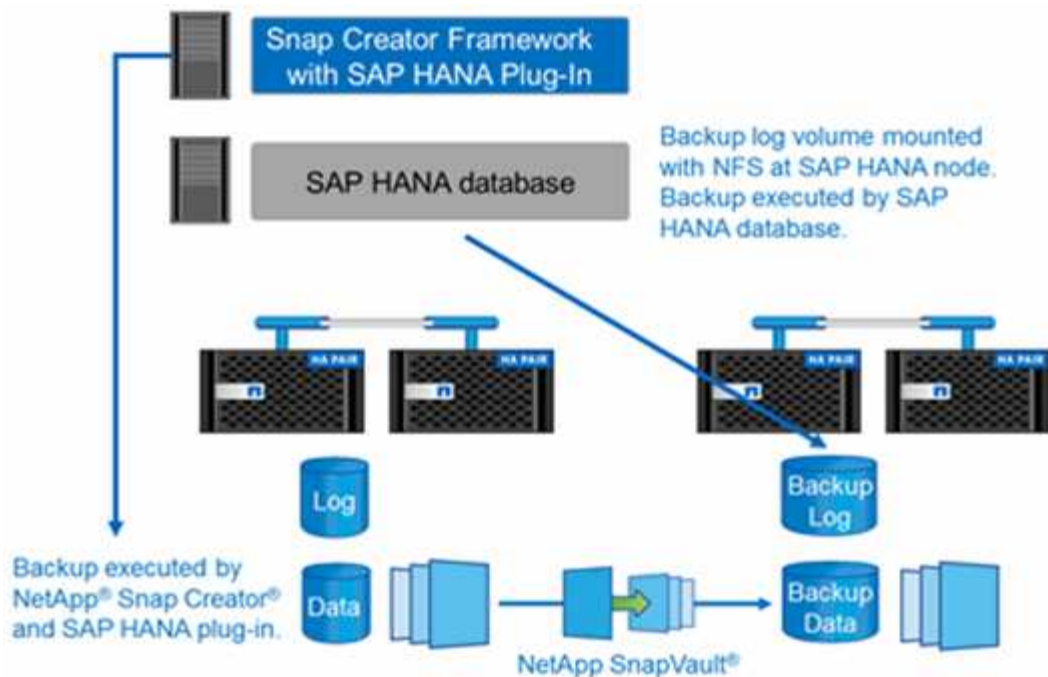
## Komponenten der Backup-Lösung

Die Snap Creator Backup-Lösung für SAP HANA besteht aus SAP HANA Datendatei-Backup mit Storage-basierten Snapshot-Kopien, der Replizierung von Datendatei-Backups auf einen sekundären externen Backup-Standort, SAP HANA-Log-Datei-Backup mit der HANA-Datenbankprotokoll-Funktion, der Integritätsprüfung der Datenbankblöcke mithilfe eines dateibasierten Backups. Und allgemeine Ordnung und Sauberkeit der Datendateien, Backup von Protokolldateien und der SAP HANA Backup-Katalog.

Datenbank-Backups werden von Snap Creator in Verbindung mit einem Plug-in für SAP HANA ausgeführt. Das Plug-in sorgt für Datenbankkonsistenz, sodass die auf dem primären Storage-System erstellten Snapshot Kopien auf einem konsistenten Image der SAP HANA Datenbank basieren.

Snap Creator ermöglicht es Ihnen, die konsistenten Datenbank-Images mithilfe von SnapVault auf einen sekundären Storage zu replizieren. In der Regel werden für die Backups auf dem primären Storage und auf dem sekundären Storage unterschiedliche Aufbewahrungsrichtlinien definiert. Snap Creator verwaltet die Aufbewahrung auf dem primären und sekundären Storage.

Das Protokoll-Backup wird automatisch durch die SAP HANA Datenbank-Tools ausgeführt. Das Backup-Ziel für das Protokoll sollte sich nicht auf demselben Speichersystem befinden, auf dem sich das Protokollvolumen der Datenbank befindet. Die Konfiguration des Backup-Ziels für das Protokoll auf demselben sekundären Storage, auf dem die Datenbank-Backups mit SnapVault repliziert werden, wird empfohlen. Mit dieser Konfiguration gelten für den sekundären Storage ähnliche Verfügbarkeitsanforderungen als den primären Storage, sodass sicher ist, dass die Log-Backups immer auf den sekundären Storage geschrieben werden können.



Die Backup-Zeitpläne und Aufbewahrungsrichtlinien müssen auf Basis der Kundenanforderungen definiert werden. Die folgende Tabelle zeigt eine Beispielkonfiguration der verschiedenen Zeitpläne und Aufbewahrungsrichtlinien.

|  | Ausgeführt von Snap Creator                     | Primärspeicher   | Sekundär-Storage                                  |
|--|---|--|---|
| Datenbank-Backups                                      | Zeitplan 1: Alle 4 Stunden                      | Aufbewahrung: 6 (=> 6 stündliche Snapshot-Kopien)            | Aufbewahrung: 6 (=> 6 stündliche Snapshot-Kopien) |
| Zeitplan 2: Einmal pro Tag                             | Aufbewahrung: 3 (=> 3 tägliche Snapshot-Kopien) | Aufbewahrung: 28 (4 Wochen) (=> 28 tägliche Snapshot Kopien) | Backup-Protokollierung                            |
| Zeitplan für SAP HANA Datenbank-Tools: Alle 15 Minuten | NA  | Aufbewahrung: 28 Tage (4 Wochen)                             | Block-Integritätsprüfung                          |

Mit diesem Beispiel werden sechs stündliche und drei tägliche Backups auf dem Primärspeicher aufbewahrt. Auf dem sekundären Storage werden die Datenbank-Backups für vier Wochen aufbewahrt. Um ein Daten-Backup wiederherstellen zu können, müssen Sie dieselbe Aufbewahrung für die Log-Backups festlegen.

## Plug-in-Übersicht über SAP HANA

Das SAP HANA Plug-in arbeitet mit Snap Creator Framework zusammen, um eine Backup-Lösung für SAP HANA Datenbanken bereitzustellen, die auf einem NetApp Storage Back-End basieren. Die von Snap Creator erstellten Snapshot Backups sind im HANA-Katalog registriert und können im HANA Studio angezeigt werden.

Snap Creator Framework unterstützt zwei Arten von SAP HANA Datenbanken: Einzelne Container und

mandantenfähige Datenbank-Container (MDC).

Snap Creator und das SAP HANA Plug-in werden von Data ONTAP 7-Mode und Clustered Data ONTAP unterstützt, wobei die SAP HANA Datenbank-Nodes über NFS oder Fibre Channel mit den Storage Controllern verbunden sind. Für Service Pack Stack (SPS) 7 und höher stehen die erforderlichen Schnittstellen zur SAP HANA-Datenbank zur Verfügung.

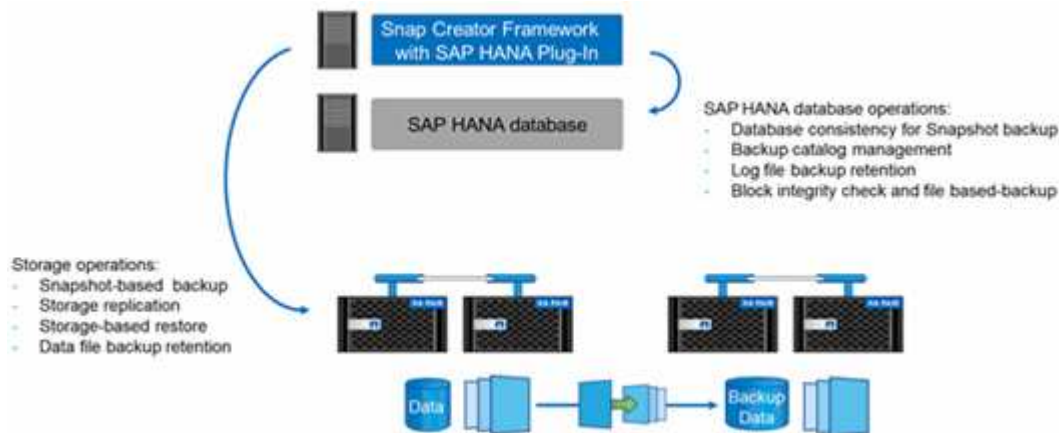
Snap Creator Framework kommuniziert mit den Storage-Systemen, um Snapshot Kopien zu erstellen und die Daten mithilfe von SnapVault auf einem sekundären Storage zu replizieren. Snap Creator wird zudem verwendet, um die Daten entweder mit SnapRestore auf dem primären Storage oder mit SnapVault Wiederherstellung vom sekundären Storage wiederherzustellen.

Das Snap Creator Plug-in für SAP HANA verwendet den SAP HANA hdbsql-Client, um SQL-Befehle auszuführen. Dies ermöglicht die Datenbankkonsistenz und das Management des SAP HANA Backup-Katalogs. Das SAP HANA Plug-in wird sowohl für SAP Certified Hardware Appliances als auch für Tailored Datacenter Integration (TDI) Programme unterstützt.

Das Snap Creator Plug-in für SAP HANA verwendet den SAP HANA hdbsql-Client, um SQL-Befehle für die folgenden Aufgaben auszuführen:

- Datenbankkonsistenz zur Vorbereitung eines Storage-basierten Snapshot-Backups
- Management der Backup-Aufbewahrung von Protokolldateien auf Filesystem-Ebene
- Management des SAP HANA Backup-Katalogs für Datei- und Log-Datei-Backups
- Führen Sie ein dateibasiertes Backup zur Überprüfung der Block-Integrität durch

Die folgende Abbildung zeigt einen Überblick über die Kommunikationswege von Snap Creator mit dem Storage und der SAP HANA Datenbank.



Snap Creator führt die folgenden Schritte zum Backup der Datenbank durch:

1. Erstellung einer SAP HANA Datenbank-Snapshot-Kopie, um ein konsistentes Image auf der Persistenzschicht zu erhalten
2. Erstellt eine Storage-Snapshot-Kopie des/der Daten-Volumes.
3. Registrieren des Storage Snapshot Backups im SAP HANA Backup-Katalog
4. Löscht die Snapshot Kopie von SAP HANA.
5. Führt ein SnapVault-Update für das Daten-Volume aus.
6. Löscht die Storage-Snapshot-Kopien im primären und/oder sekundären Storage basierend auf den definierten Aufbewahrungsrichtlinien für Backups im primären und sekundären Storage.

7. Löscht die Einträge im SAP HANA Backup-Katalog, wenn die Backups nicht mehr auf dem primären und dem sekundären Speicher vorhanden sind.
8. Löscht alle Log-Backups, die älter als die älteste Datensicherung im Filesystem und im SAP HANA Backup-Katalog sind.

## Anforderungen

Das SAP HANA Plug-in ermöglicht Ihnen das Erstellen von Backups und das Ausführen zeitpunktgenauer Recovery von HANA Datenbanken.

Die Unterstützung für das SAP HANA Plug-in erfolgt wie folgt:

- Host-Betriebssystem: SUSE Linux Enterprise Server (SLES), 32 Bit und 64 Bit
- Clustered Data ONTAP oder Data ONTAP in 7-Mode
- Mindestens ein SAP HANA Datenbank-Node, der über NFS verbunden ist
- SAP HANA mit Service Pack Stack (SPS) 7 oder höher



Aktuelle Informationen zum Support oder zum Anzeigen von Kompatibilitätsmatrizen finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool"](#).

## Erforderliche Lizenzen

Für die primären Storage Controller muss eine SnapRestore- und SnapVault-Lizenz installiert sein. Auf dem sekundären Storage muss eine SnapVault-Lizenz installiert sein.

Für Snap Creator und das Snap Creator SAP HANA Plug-in ist keine Lizenz erforderlich.

## Kapazitätsanforderungen für Snapshot-Backups

Eine höhere Blockänderungsrate auf Storage-Ebene muss mit der Änderungsrate der herkömmlichen Datenbanken verglichen werden. Aufgrund des Zusammenführungsprozesses der Tabelle des Spaltenspeichers werden viel mehr Daten als nur die Blockänderungen auf die Festplatte geschrieben. Bis mehr Kundendaten verfügbar sind, liegt die aktuelle Schätzung für die Änderungsrate bei 20% bis 50% pro Tag.

## Installation und Konfiguration der erforderlichen Softwarekomponenten

Für die SAP HANA-Backup- und Restore-Lösung mit Snap Creator Framework und dem SAP HANA-Plug-in müssen Snap Creator Softwarekomponenten und die SAP HANA hdbsql-Client-Software installiert werden.

Sie müssen das Plug-in nicht separat installieren. Es wird mit dem Agent installiert.

1. Installieren Sie den Snap Creator Server auf einem Host, der die Netzwerkverbindung mit dem Host teilt, auf dem Sie den Agent installieren.
2. Installieren Sie den Snap Creator Agent auf einem Host, der die Netzwerkverbindung mit dem Snap Creator Server-Host nutzt.
  - Installieren Sie in einer einzelnen SAP HANA-Node-Umgebung den Agent auf dem Datenbank-Host.



Alternativ können Sie den Agent auf einem anderen Host installieren, der über eine Netzwerkverbindung mit dem Datenbank-Host und dem Snap Creator Server-Host verfügt.

- In einer SAP HANA-Umgebung mit mehreren Nodes sollten Sie den Agent nicht auf dem Datenbank-Host installieren. Der Agent muss auf einem separaten Host installiert sein, der über eine Netzwerkverbindung mit dem Datenbank-Host und dem Snap Creator Server-Host verfügt.

3. Installieren Sie die SAP HANA hdbsql-Client-Software auf dem Host, auf dem Sie den Snap Creator Agent installiert haben.

Konfigurieren Sie die Benutzerspeicherschlüssel für die SAP HANA-Knoten, die Sie über diesen Host verwalten.

```
mgmtsrv01:/sapcd/HANA_SP5/DATA_UNITS/HDB_CLIENT_LINUXINTEL # ./hdbinst

SAP HANA Database Client installation kit detected.

SAP HANA Database Installation Manager - Client Installation
1.00.46.371989
*****
***

Enter Installation Path [/usr/sap/hdbclient32]:
Checking installation...
Installing and configuring required software components | 13
Preparing package "Product Manifest"...
Preparing package "SQLDBC"...
Preparing package "ODBC"...
Preparing package "JDBC"...
Preparing package "Client Installer"...
Installing SAP HANA Database Client to /usr/sap/hdbclient32...
Installing package 'Product Manifest' ...
Installing package 'SQLDBC' ...
Installing package 'ODBC' ...
Installing package 'JDBC' ...
Installing package 'Client Installer' ...
Installation done
Log file written to '/var/tmp/hdb_client_2013-07-
05_11.38.17/hdbinst_client.log'
mgmtsrv01:/sapcd/HANA_SP5/DATA_UNITS/HDB_CLIENT_LINUXINTEL #
```

## Verwandte Informationen

["Snap Creator Framework – Installationshandbuch"](#)

## Stellen Sie Annahmen in diesem Leitfaden ein

Obwohl bei einer typischen Installation von Snap Creator davon ausgegangen wird, dass

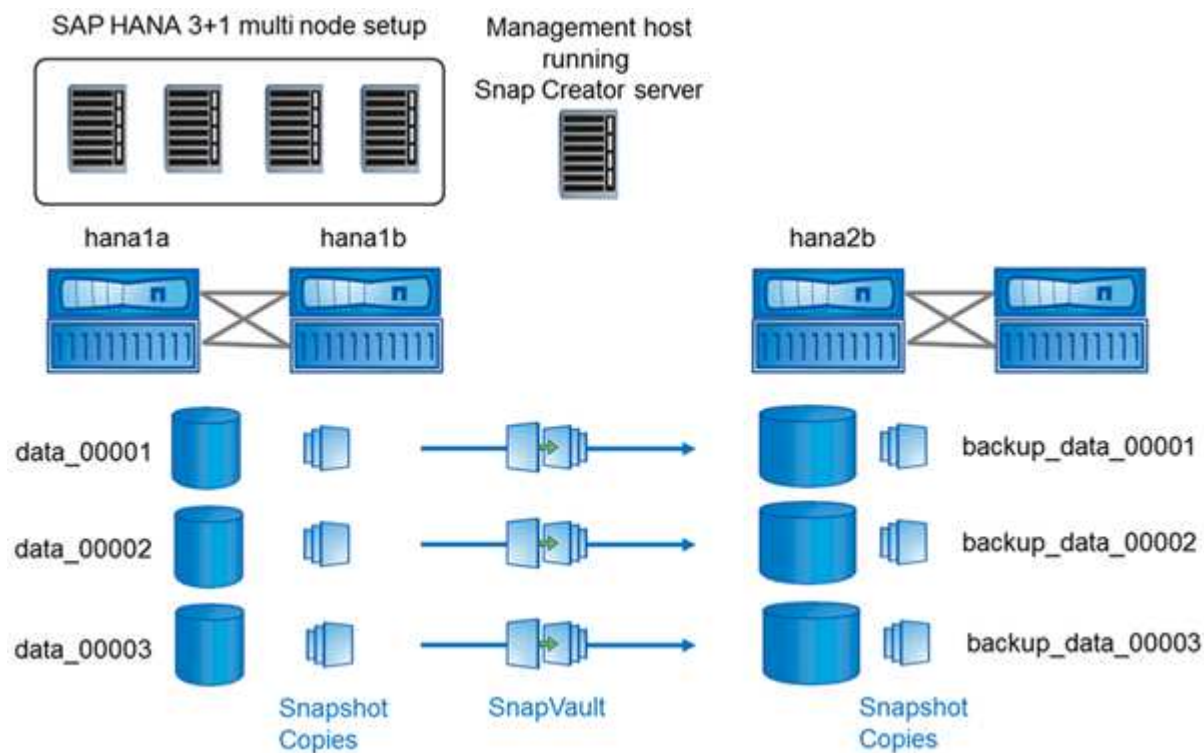
der Server auf einem Host installiert ist und der Agent auf einem anderen Host installiert ist, basiert das in diesem Handbuch verwendete Setup auf einer Multinode-Appliance von SAP HANA.

Bei dieser Konfiguration läuft die SAP HANA-Datenbank auf einer Konfiguration mit 3+1-Datenbankknoten, und alle Snap Creator-Softwarekomponenten - Server, Agent und Plug-in - werden auf demselben Host installiert.

Auf den in diesem Setup verwendeten NetApp Storage-Systemen wird Data ONTAP 7-Mode ausgeführt. Auf der Storage-Ebene wird ein HA-Controller-Paar mit Hochverfügbarkeit verwendet. Die Daten- und Protokoll-Volumes der drei SAP HANA Datenbank-Nodes werden auf beide Storage Controller verteilt. Beim Beispiel-Setup wird ein Storage Controller eines anderen HA-Controller-Paars als sekundärer Storage verwendet. Jedes Daten-Volume wird in ein dediziertes Backup-Volume im sekundären Storage repliziert. Die Größe der Backup-Volumes hängt von der Anzahl der Backups ab, die im sekundären Storage aufbewahrt werden sollen.

Die hier beschriebenen Vorgänge zu Snap Creator und SAP HANA Studio sind für Storage-Systeme mit Clustered Data ONTAP identisch. Die anfängliche SnapVault-Konfiguration auf den Storage-Systemen und alle SnapVault Befehle, die direkt auf dem Storage ausgeführt werden müssen, unterscheiden sich jedoch bei Clustered Data ONTAP. Die Unterschiede werden in diesem Leitfaden hervorgehoben und beschrieben.

In der folgenden Abbildung werden die Daten-Volumes auf dem primären Storage und der Replizierungspfad zum sekundären Storage gezeigt:



Alle Volumes, die gesichert werden müssen, müssen auf dem sekundären Storage Controller erstellt werden. In diesem Beispiel werden die Volumes Backup\_Data\_00001, Backup\_Data\_00002 und Backup\_Data\_00003 auf dem sekundären Speicher-Controller erstellt.

## Setup für Clustered Data ONTAP

Die folgende Abbildung zeigt die Einrichtung, die mit Clustered Data ONTAP verwendet wurde. Die Einrichtung basiert auf einer SAP HANA Konfiguration mit einem Node und den Storage Virtual Machines (SVMs) und Volume-Namen, die in der folgenden Abbildung dargestellt sind.

Die Vorbereitung, das Starten, die Wiederaufnahme und die Wiederherstellung von SnapVault Vorgängen unterscheiden sich in Clustered Data ONTAP und Data ONTAP 7-Mode. Diese Unterschiede sind in den entsprechenden Abschnitten dieses Leitfadens zu finden.

## Konfigurieren von Daten-Backups

Führen Sie nach der Installation der erforderlichen Softwarekomponenten die folgenden Schritte aus, um die Konfiguration abzuschließen:

1. Konfigurieren Sie einen dedizierten Datenbankbenutzer und den SAP HANA Benutzerspeicher.
2. SnapVault-Replizierung auf allen Storage Controllern vorbereiten.
3. Erstellung von Volumes auf dem sekundären Storage Controller
4. SnapVault Beziehungen für Datenbank-Volumes initialisieren.
5. Konfigurieren Sie Snap Creator.

### Konfigurieren des Backup-Benutzers und des hdbuserstore

Sie sollten einen dedizierten Datenbankbenutzer in der HANA Datenbank konfigurieren, um die Backup-Vorgänge mit Snap Creator auszuführen. In einem zweiten Schritt sollten Sie für diesen Backup-Benutzer einen SAP HANA User Store Key konfigurieren. Dieser UserStore-Schlüssel wird in der Konfiguration des Snap Creator SAP HANA Plug-ins verwendet.

Der Backup-Benutzer muss über die folgenden Berechtigungen verfügen:

- BACKUP-ADMIN
  - KATALOG GELESEN
1. Auf dem Administrationshost, dem Host, auf dem Snap Creator installiert wurde, ist ein Benutzerspeicherschlüssel für alle Datenbank-Hosts konfiguriert, die zur SAP HANA-Datenbank gehören. Der Userstore-Schlüssel wird mit dem OS-Root-Benutzer konfiguriert: `Hdbuserstore Set keyhost 3[instance]15 userpassword`
  2. Konfigurieren Sie einen Schlüssel für alle vier Datenbank-Nodes.

```

mgmtsrv01:/usr/sap/hdbclient32 # ./hdbuserstore set SCADMIN08
cishanar08:34215 SCADMIN Password
mgmtsrv01:/usr/sap/hdbclient32 # ./hdbuserstore set SCADMIN09
cishanar09:34215 SCADMIN Password
mgmtsrv01:/usr/sap/hdbclient32 # ./hdbuserstore set SCADMIN10
cishanar10:34215 SCADMIN password
mgmtsrv01:/usr/sap/hdbclient32 # ./hdbuserstore set SCADMIN11
cishanar11:34215 SCADMIN Password
mgmtsrv01:/usr/sap/hdbclient32 # ./hdbuserstore LIST
DATA FILE          : /root/.hdb/mgmtsrv01/SSFS_HDB.DAT

KEY SCADMIN08
  ENV : cishanar08:34215
  USER: SCADMIN
KEY SCADMIN09
  ENV : cishanar09:34215
  USER: SCADMIN
KEY SCADMIN10
  ENV : cishanar10:34215
  USER: SCADMIN
KEY SCADMIN11
  ENV : cishanar11:34215
  USER: SCADMIN
mgmtsrv01:/usr/sap/hdbclient32

```

## SnapVault Beziehungen werden konfiguriert

Wenn Sie SnapVault-Beziehungen konfigurieren, müssen für die primären Storage Controller eine gültige SnapRestore- und SnapVault-Lizenz installiert sein. Auf dem sekundären Storage muss eine gültige SnapVault-Lizenz installiert sein.

1. Aktivieren Sie SnapVault und NDMP auf den primären und sekundären Storage Controllern.

```

hana1a> options snapvault.enable on
hana1a> ndmp on
hana1a>
hana1b> options snapvault.enable on
hana1b> ndmpd on
hana1b>
hana2b> options snapvault.enable on
hana2b> ndmpd on
hana2b>

```

2. Konfigurieren Sie auf allen primären Storage Controllern den Zugriff auf den sekundären Storage

Controller.

```
hana1a> options snapvault.access host=hana2b
hana1a>
hana1b> options snapvault.access host=hana2b
hana1b>
```



Die Verwendung eines dedizierten Netzwerks für den Replikationsverkehr wird empfohlen. In diesen Fällen muss der Host-Name dieser Schnittstelle am sekundären Storage Controller konfiguriert werden. Anstelle von hana2b könnte der Host Name hana2b-Rep sein.

3. Konfigurieren Sie auf dem sekundären Storage Controller den Zugriff für alle primären Storage Controller.

```
hana2b> options snapvault.access host=hana1a,hana1b
hana2b>
```



Die Verwendung eines dedizierten Netzwerks für den Replikationsverkehr wird empfohlen. In diesen Fällen muss der Host-Name dieser Schnittstelle auf den primären Storage Controllern konfiguriert werden. Anstelle von hana1b und hana1a könnte der Hostname hana1a-Rep und hana1b-rep sein.

## Starten der SnapVault Beziehungen

Sie müssen die SnapVault Partnerschaft mit Data ONTAP im 7-Mode und Clustered Data ONTAP starten.

### Starten der SnapVault Beziehungen mit Data ONTAP im 7-Mode

Sie können eine SnapVault Beziehung mit Befehlen starten, die auf dem sekundären Storage-System ausgeführt werden.

1. Für Storage-Systeme mit Data ONTAP 7-Mode starten Sie die SnapVault Beziehungen, indem Sie den folgenden Befehl ausführen:

```

hana2b> snapvault start -S hana1a:/vol/data_00001/mnt00001
/vol/backup_data_00001/mnt00001
Snapvault configuration for the qtree has been set.
Transfer started.
Monitor progress with 'snapvault status' or the snapmirror log.
hana2b>
hana2b> snapvault start -S hana1a:/vol/data_00003/mnt00003
/vol/backup_data_00003/mnt00003
Snapvault configuration for the qtree has been set.
Transfer started.
Monitor progress with 'snapvault status' or the snapmirror log.
hana2b>
hana2b> snapvault start -S hana1b:/vol/data_00002/mnt00002
/vol/backup_data_00002/mnt00002
Snapvault configuration for the qtree has been set.
Transfer started.
Monitor progress with 'snapvault status' or the snapmirror log.
hana2b>

```



Es wird empfohlen, für den Replikationsverkehr ein dediziertes Netzwerk zu verwenden. In diesem Fall konfigurieren Sie den Host-Namen dieser Schnittstelle an den primären Storage Controllern. Anstelle von hana1b und hana1a könnte der Hostname hana1a-Vertreter und hana1b-rep sein.

## Beginnen der Beziehungen zu SnapVault mit Clustered Data ONTAP

Sie müssen eine SnapMirror-Richtlinie definieren, bevor Sie eine SnapVault-Beziehung starten.

1. Bei Storage-Systemen mit Clustered Data ONTAP starten Sie die SnapVault-Beziehungen, indem Sie den folgenden Befehl ausführen.

```
hana::> snapmirror policy create -vserver hana2b -policy SV_HANA
hana::> snapmirror policy add-rule -vserver hana2b -policy SV_HANA
-snapmirror-label daily -keep 20
hana::> snapmirror policy add-rule -vserver hana2b -policy SV_HANA
-snapmirror-label hourly -keep 10
```

```
hana::> snapmirror policy show -vserver hana2b -policy SV_HANA

          Vserver: hana2b
SnapMirror Policy Name: SV_HANA
      Policy Owner: vserver-admin
        Tries Limit: 8
      Transfer Priority: normal
Ignore accesstime Enabled: false
  Transfer Restartability: always
          Comment: -
    Total Number of Rules: 2
          Total Keep: 8
          Rules: Snapmirror-label  Keep  Preserve  Warn
                  -----
                  daily            20   false      0
                  hourly           10   false      0
```

Die Richtlinie muss Regeln für alle Aufbewahrungsklassen (Labels) enthalten, die in der Snap Creator-Konfiguration verwendet werden. Die oben genannten Befehle zeigen, wie eine dedizierte SnapMirror-Richtlinie SV\_HANA erstellt wird

2. Führen Sie folgende Befehle aus, um die SnapVault-Beziehung auf der Cluster-Konsole des Backup-Clusters zu erstellen und zu starten.

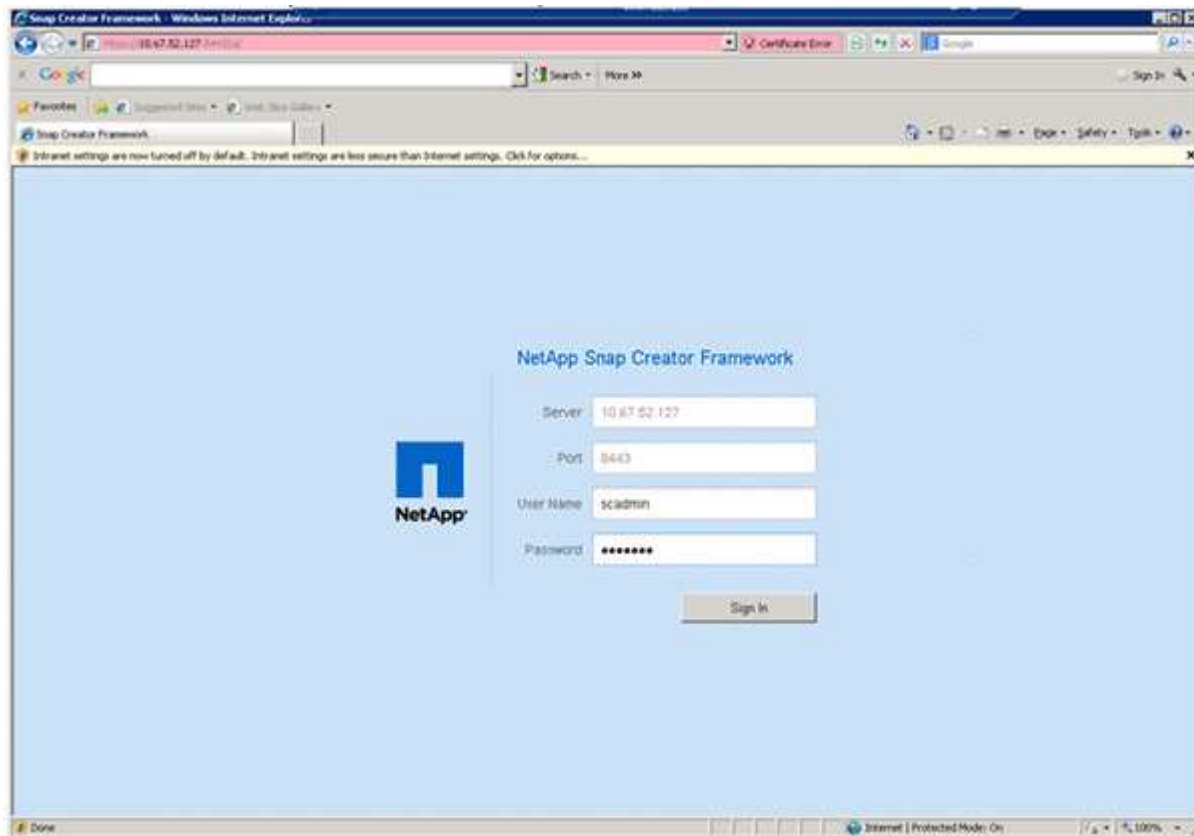
```
hana::> snapmirror create -source-path hanala:hana_data -destination
-path
hana2b:backup_hana_data -type XDP -policy SV_HANA
Operation succeeded: snapmirror create the relationship with destination
hana2b:backup_hana_data.

hana::> snapmirror initialize -destination-path hana2b:backup_hana_data
-type XDP
```

## Konfiguration des Snap Creator Framework und des Datenbank-Backups von SAP HANA

Sie müssen Snap Creator Framework und das SAP HANA Datenbank-Backup konfigurieren.

1. Verbinden Sie sich mit der grafischen Benutzeroberfläche des Snap Creator: <https://host:8443/ui/>.
2. Melden Sie sich mit dem Benutzernamen und Passwort an, die während der Installation konfiguriert wurden. Klicken Sie auf **Anmelden**.



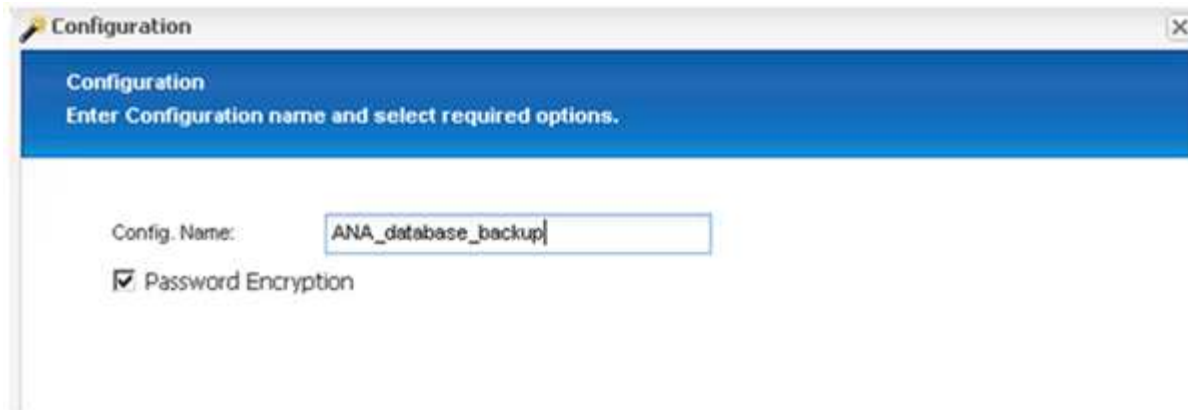
3. Geben Sie einen Profilnamen ein und klicken Sie auf **OK**.



Beispiel: „ANA“ ist die SID der Datenbank.

4. Geben Sie den Konfigurationsnamen ein, und klicken Sie auf **Weiter**.





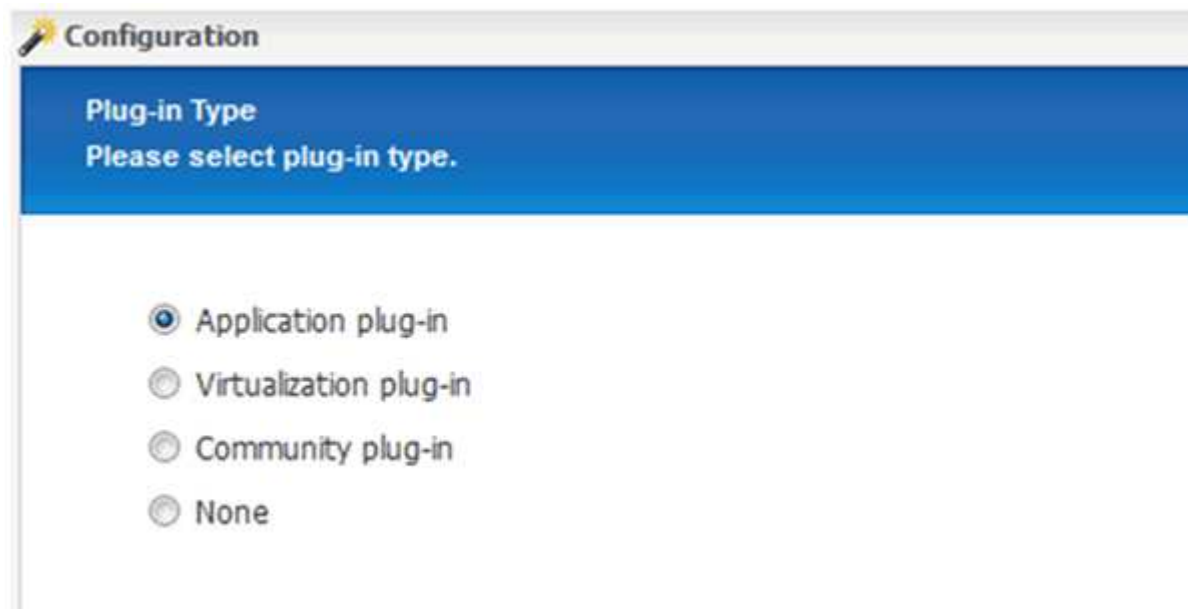
Configuration

Enter Configuration name and select required options.

Config. Name:

☒ Password Encryption

5. Wählen Sie als Plug-in-Typ \* Application Plug-in\* aus, und klicken Sie auf **Next**.



Configuration

Plug-in Type

Please select plug-in type.

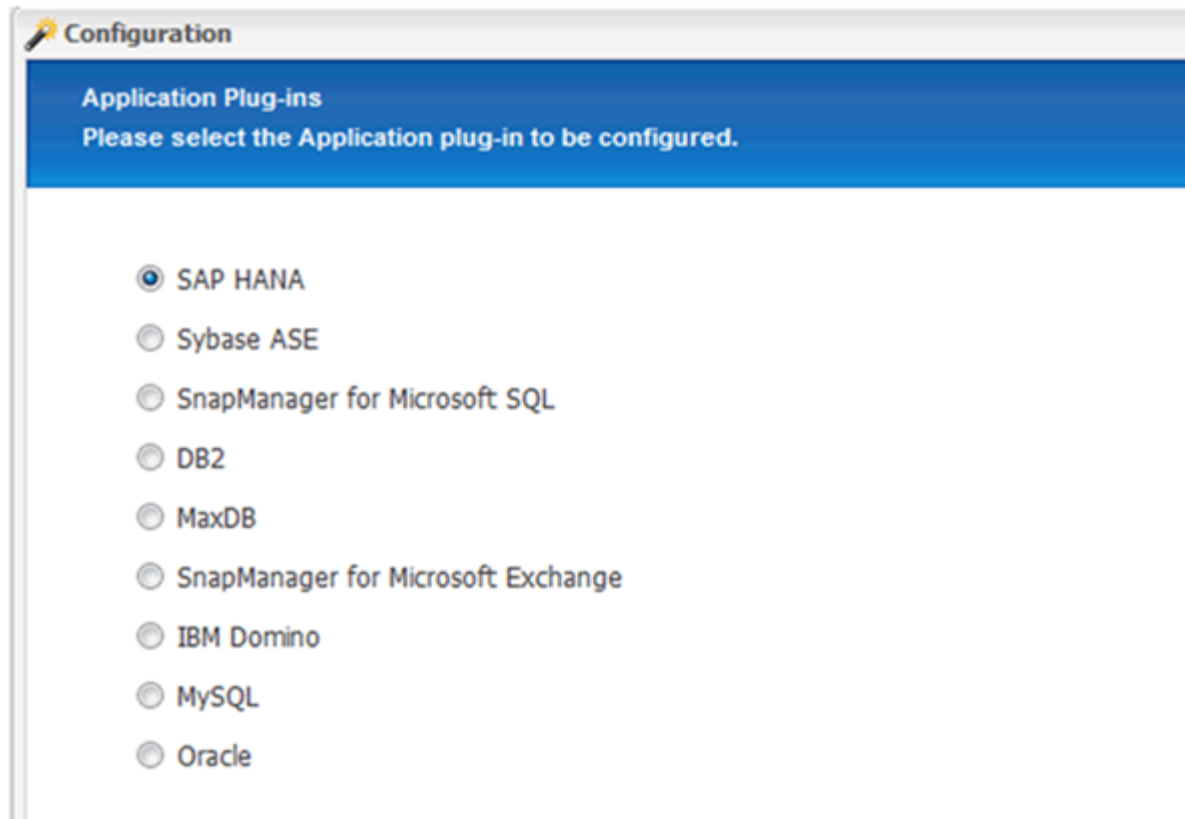
☒ Application plug-in

☐ Virtualization plug-in

☐ Community plug-in

☐ None

6. Wählen Sie als Anwendungs-Plug-in \* SAP HANA\* aus und klicken Sie auf **Weiter**.



7. Geben Sie die folgenden Konfigurationsdetails ein:

- a. Wählen Sie im Dropdown-Menü \* Ja\* aus, um die Konfiguration mit einer mandantenfähigen Datenbank zu verwenden. Wählen Sie für eine einzelne Container-Datenbank **Nein**.
- b. Wenn der Multitenant-Datenbank-Container auf **Nein** gesetzt ist, müssen Sie die Datenbank-SID angeben.
- c. Wenn der Multitenant-Datenbank-Container auf **Ja** gesetzt ist, müssen Sie für jeden SAP HANA-Knoten die hdbuserstore-Schlüssel hinzufügen.
- d. Fügen Sie den Namen der Mandanten-Datenbank hinzu.
- e. Fügen Sie die HANA-Nodes hinzu, auf denen die hdbsql-Anweisung ausgeführt werden muss.
- f. Geben Sie die HANA-Node-Instanznummer ein.
- g. Geben Sie den Pfad zur ausführbaren Datei hdbsql an.
- h. Fügen Sie den OSDB-Benutzer hinzu.
- i. Wählen Sie in der Dropdown-Liste **Ja** aus, um DIE PROTOKOLLBEREINIGUNG zu aktivieren.

HINWEIS:

- Parameter HANA\_SID Ist nur verfügbar, wenn der Wert für Parameter HANA\_MULTITENANT\_DATABASE Ist auf festgelegt N
- Für mandantenfähige Datenbank-Container (MDC) mit einem Ressourcentyp „Single Tenant“ arbeiten die SAP HANA Snapshot-Kopien mit der Key-basierten Authentifizierung von UserStore. Wenn der HANA\_MULTITENANT\_DATABASE Parameter ist auf festgelegt Y, Dann der HANA\_USERSTORE\_KEYS Parameter muss auf den entsprechenden Wert gesetzt werden.
- Ähnlich wie bei nicht-mandantenfähigen Datenbank-Containern wird die Funktion für dateibasiertes Backup und Integritätsprüfung unterstützt

j. Klicken Sie Auf **Weiter**.

|   |                               |
|---|-------------------------------|
| Multitenant Database Container (MDC) - Single Tenant: | No                            |
| SID:  | H66                           |
| hdbuserstore Keys:                                    |                               |
| Tenant Database Name:                                 |                               |
| Nodes:  | 10.235.220.66                 |
| Username:   | SYSTEM                        |
| Password:   | *****                         |
| Instance number:                                      | 66                            |
| Path to hdbsql:                                       | /usr/sap/H66/HDB66/exe/hdbsql |
| OSDB User:  |                               |
| Enable LOG Cleanup:                                   | Yes                           |

8. Aktivieren Sie den dateibasierten Backup-Vorgang:
- Legen Sie den Speicherort für die Dateisicherung fest.
  - Geben Sie das Präfix für die Dateisicherung an.
  - Aktivieren Sie das Kontrollkästchen **Datei-Backup aktivieren**.
  - Klicken Sie Auf **Weiter**.

The screenshot shows a 'Configuration' window with a blue header bar containing the text 'File-Based Backup Configuration Details' and 'Provide File-Based Backup Details'. Below the header, there are three input fields: 'File-Backup Location:', 'File-Backup prefix:', and 'Enable File-Backup:'. The 'Enable File-Backup:' field is a checkbox. At the bottom right of the window, there are three buttons: 'Back', 'Next', and 'Cancel'.

Configuration

File-Based Backup Configuration Details  
Provide File-Based Backup Details

File-Backup Location:

File-Backup prefix:

Enable File-Backup: ☐

Back Next Cancel

9. Aktivieren Sie die Datenbankintegritätsprüfung:

- Legen Sie den Speicherort für die temporäre Datei-Sicherung fest.
- Aktivieren Sie das Kontrollkästchen \* DB-Integritätsprüfung aktivieren\*.
- Klicken Sie Auf **Weiter**.

**Configuration**

**Integrity Check Configuration Details**  
Provide Integrity Check Details

Temporary File-Backup Location:

Enable DB Integrity Check: ☐

10. Geben Sie die Details für den Konfigurationsparameter des Agenten ein, und klicken Sie auf **Weiter**.

**Agent Configuration**  
Enter agent configuration details

IP/DNS:

Port:

Timeout (secs):

11. Geben Sie die Einstellungen für die Speicherverbindung ein, und klicken Sie auf **Weiter**.

**Storage Connection Settings**  
Please Provide Storage Connection Settings

Use OnCommand Proxy: ☐

Transport:

Controller/Vserver Port:

12. Geben Sie die Anmeldedaten für den Speicher ein, und klicken Sie auf **Weiter**.

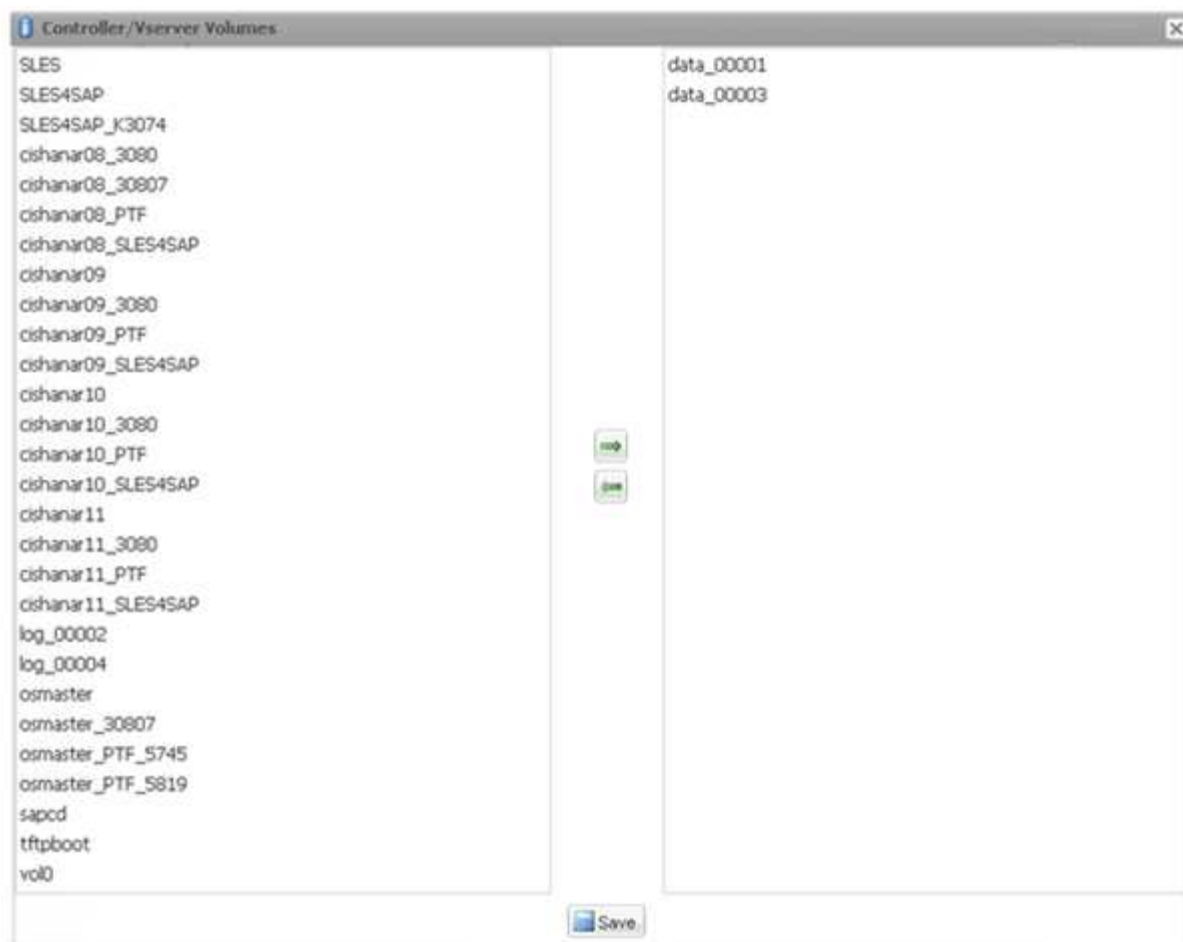
**Controller/Vserver Credentials**  
Add one or more Controller/Vserver credentials to the configuration.

**Controller/Vserver Login Credentials**

+ Add | Edit | Delete

| Controller/Vserver IP or Name   | User name/Password | Volumes |
|---|--------------------|---------|
| <p><b>New Controller/Vserver</b></p> <p>Controller/Vserver IP or Name: <input type="text" value="hana1a"/></p> <p>Controller/Vserver User: <input type="text" value="root"/></p> <p>Controller/Vserver Password: <input type="password" value="....."/></p> <p>Next</p> |                    |         |

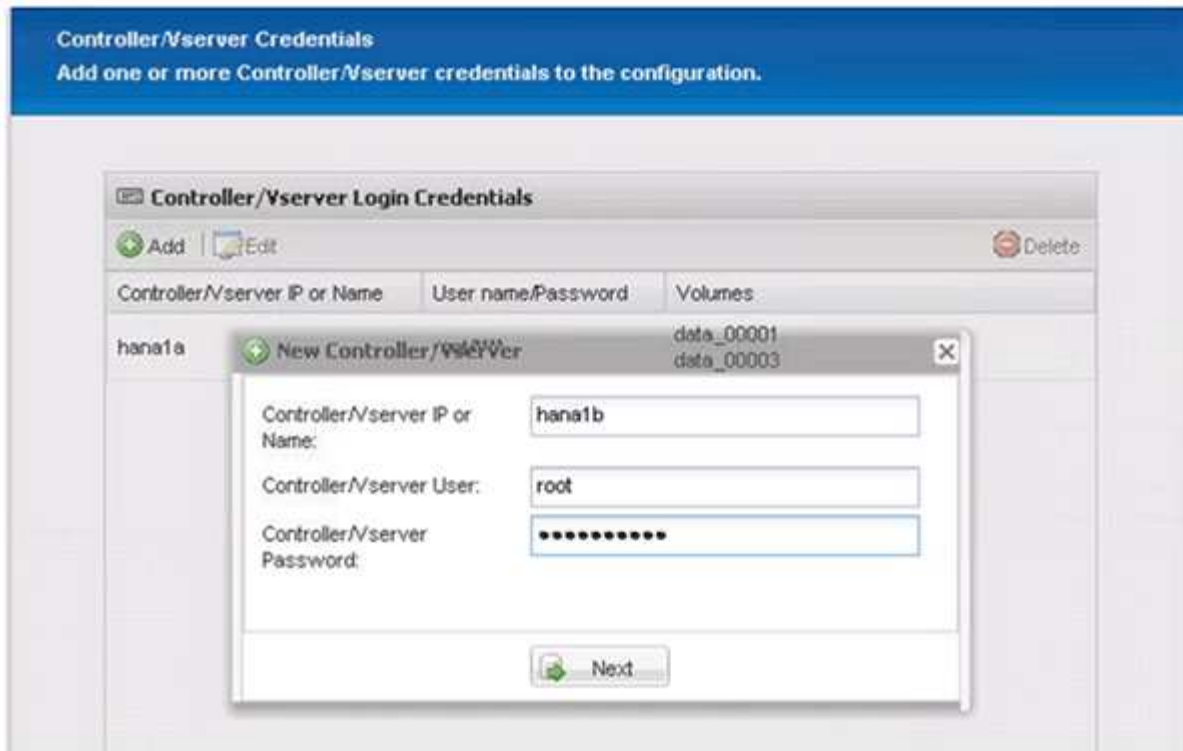
13. Wählen Sie die auf diesem Speicher-Controller gespeicherten Datenvolumen aus und klicken Sie auf **Speichern**.



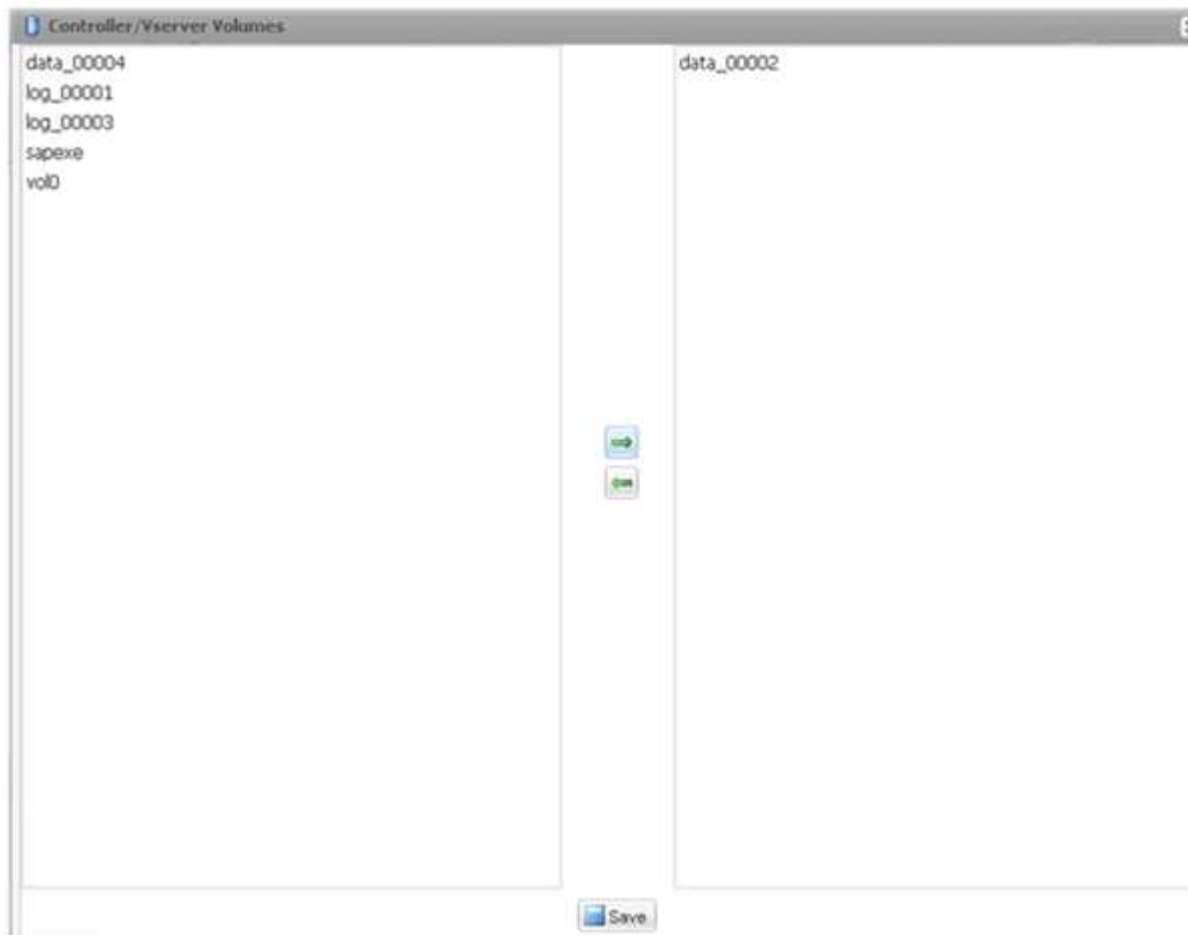
14. Klicken Sie auf **Hinzufügen**, um einen weiteren Speicher-Controller hinzuzufügen.



15. Geben Sie die Anmeldedaten für den Speicher ein, und klicken Sie auf **Weiter**.

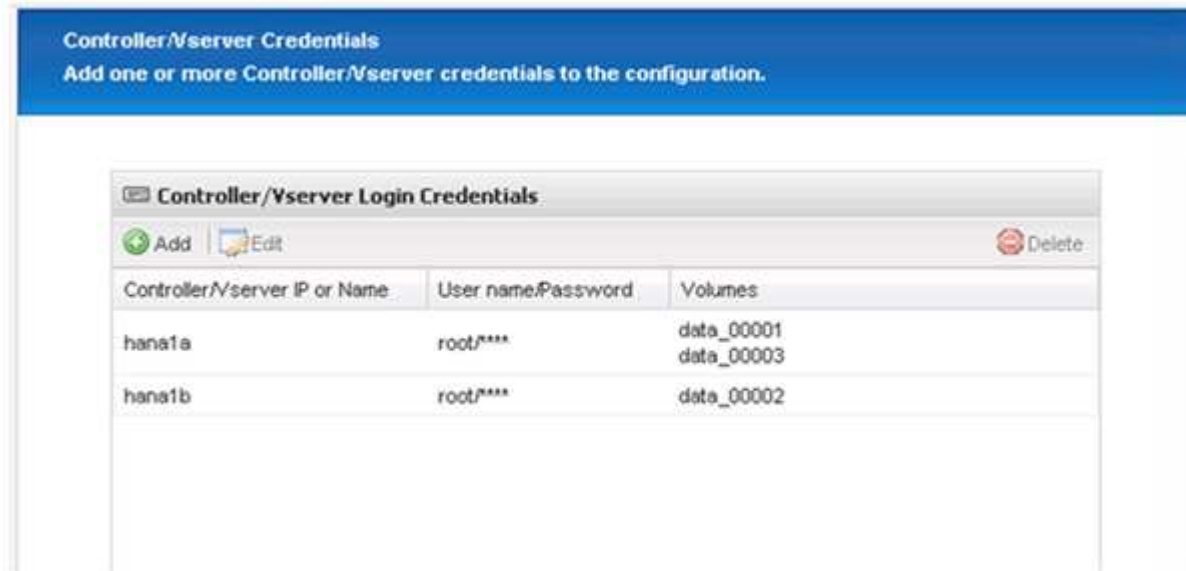


16. Wählen Sie die Datenvolumen aus, die auf dem zweiten Speicher-Controller gespeichert sind, den Sie erstellt haben, und klicken Sie auf **Speichern**.





17. Im Fenster Controller/Vserver Credentials werden die hinzugefügten Storage Controller und Volumes angezeigt. Klicken Sie Auf **Weiter**.



18. Geben Sie die Konfiguration der Snapshot-Richtlinie und -Aufbewahrung ein.

Die Aufbewahrung von drei täglichen und acht stündlichen Snapshot-Kopien ist nur ein Beispiel, das je nach Kundenanforderungen unterschiedlich konfiguriert werden könnte.



Wählen Sie als Namensgebungskonvention **Zeitstempel** aus. Die Verwendung der Namenskonvention **Recent** wird mit dem SAP HANA Plug-in nicht unterstützt, da der Zeitstempel der Snapshot Kopie auch für die SAP HANA Backup Katalog Einträge verwendet wird.

**Configuration**

**Snapshot Details**  
Provide Snapshot copy related information.

Snapshot copy Name:

Snapshot copy Label:

Policy Type: ☒ Use Policy ☐ Use Policy Object

| Snapshot copy Policies              |             |           |
|-------------------------------------|-------------|-----------|
| Enable Policy                       | Policy Name | Retention |
| <input checked="" type="checkbox"/> | hourly      | 12        |
| <input checked="" type="checkbox"/> | daily       | 3         |
| <input type="checkbox"/>            | weekly      | 0         |
| <input type="checkbox"/>            | monthly     | 0         |

Prevent Snapshot copy Deletion:

Policy Retention Age:

Naming Convention: ☐ Recent ☒ Timestamp

19. Es sind keine Änderungen erforderlich. Klicken Sie Auf **Weiter**.

**Snapshot Details Continued**  
Provide Snapshot copy related information.

Consistency Group: ☐

Consistency Timeout:

SnapDrive Discovery:

Consistency Group WAFL Sync:

Snapshot copy Delete by age only:

Snapshot copy Dependency Ignore:

Restore Auto Detect:

Ignore Application Errors:

Snapshot Copy Disable:

20. Wählen Sie **SnapVault** aus, und konfigurieren Sie die SnapVault-Aufbewahrungsrichtlinien und die SnapVault-Wartezeit.

**Configuration**

**Data Protection**  
Configure SnapMirror, SnapVault or both

Data Transfer: ☐ SnapMirror ☒ SnapVault

**SnapVault Policies**

| Enable Policy                       | Policy Name | Retention |
|-------------------------------------|-------------|-----------|
| <input checked="" type="checkbox"/> | hourly      | 10        |
| <input checked="" type="checkbox"/> | daily       | 20        |
| <input type="checkbox"/>            | weekly      | 0         |
| <input type="checkbox"/>            | monthly     | 0         |

SnapVault Retention Age:

SnapVault wait time:

21. Klicken Sie Auf **Hinzufügen**.

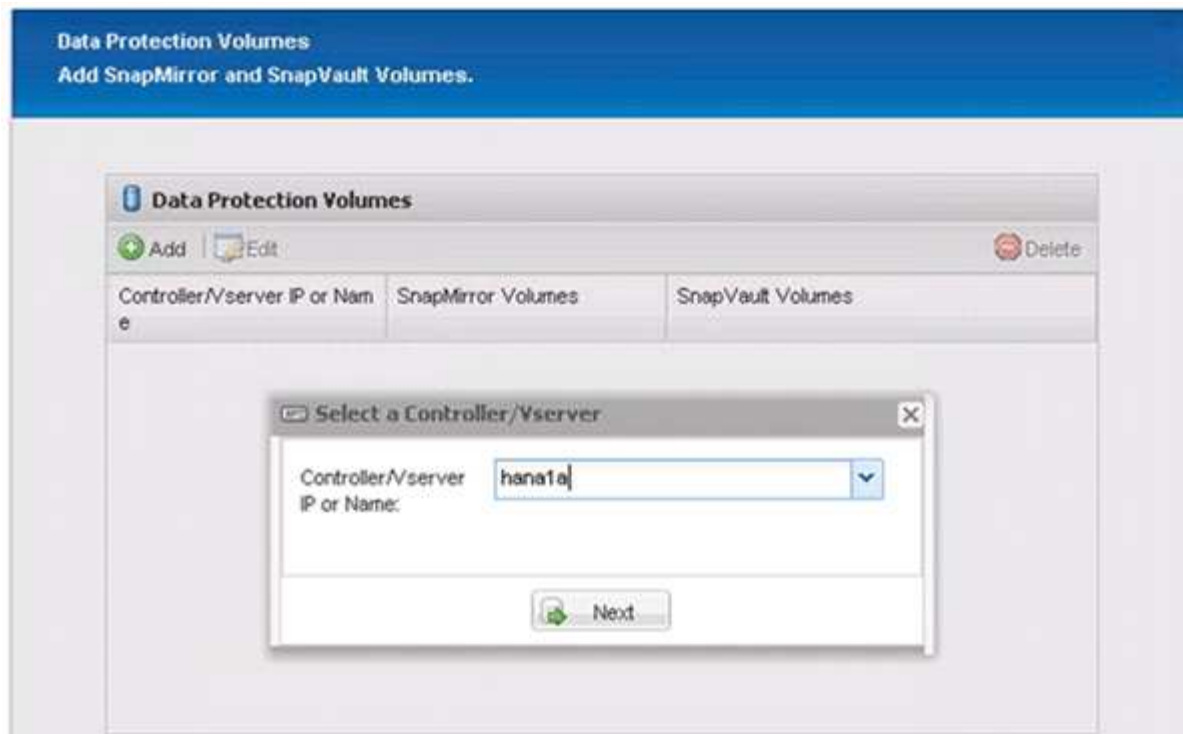
**Data Protection Volumes**  
Add SnapMirror and SnapVault Volumes.

**Data Protection Volumes**

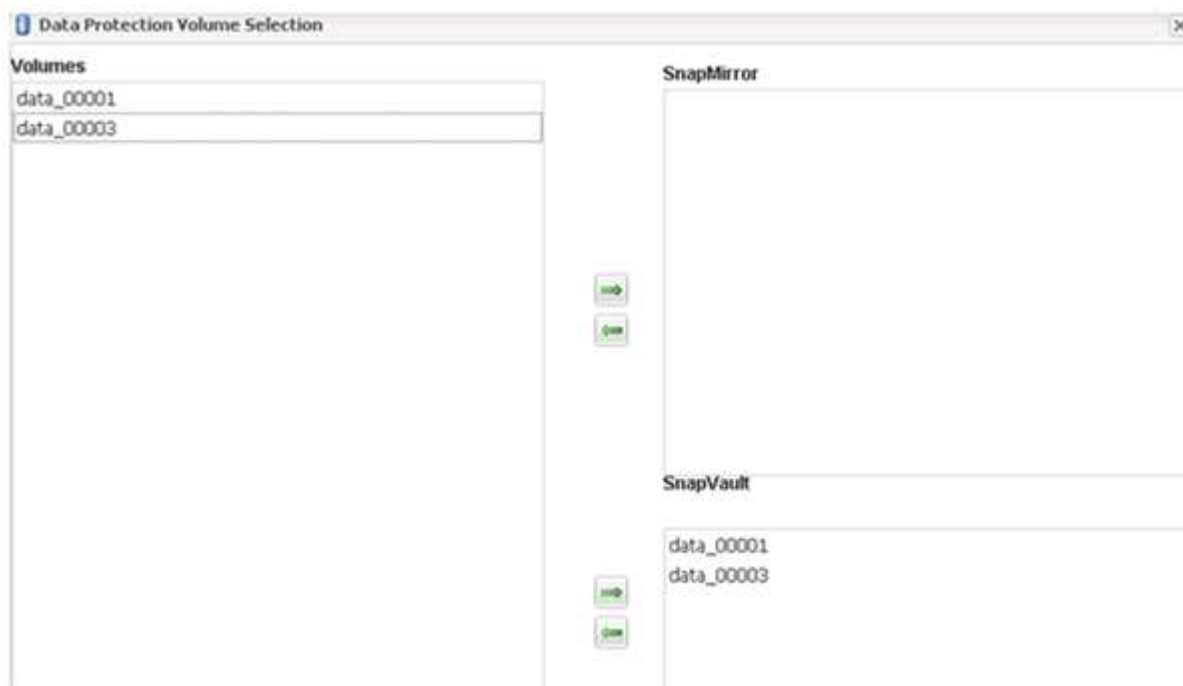
 Add  Edit  Delete

| Controller/Vserver IP or Name | SnapMirror Volumes | SnapVault Volumes |
|-------------------------------|--------------------|-------------------|
|                               |                    |                   |

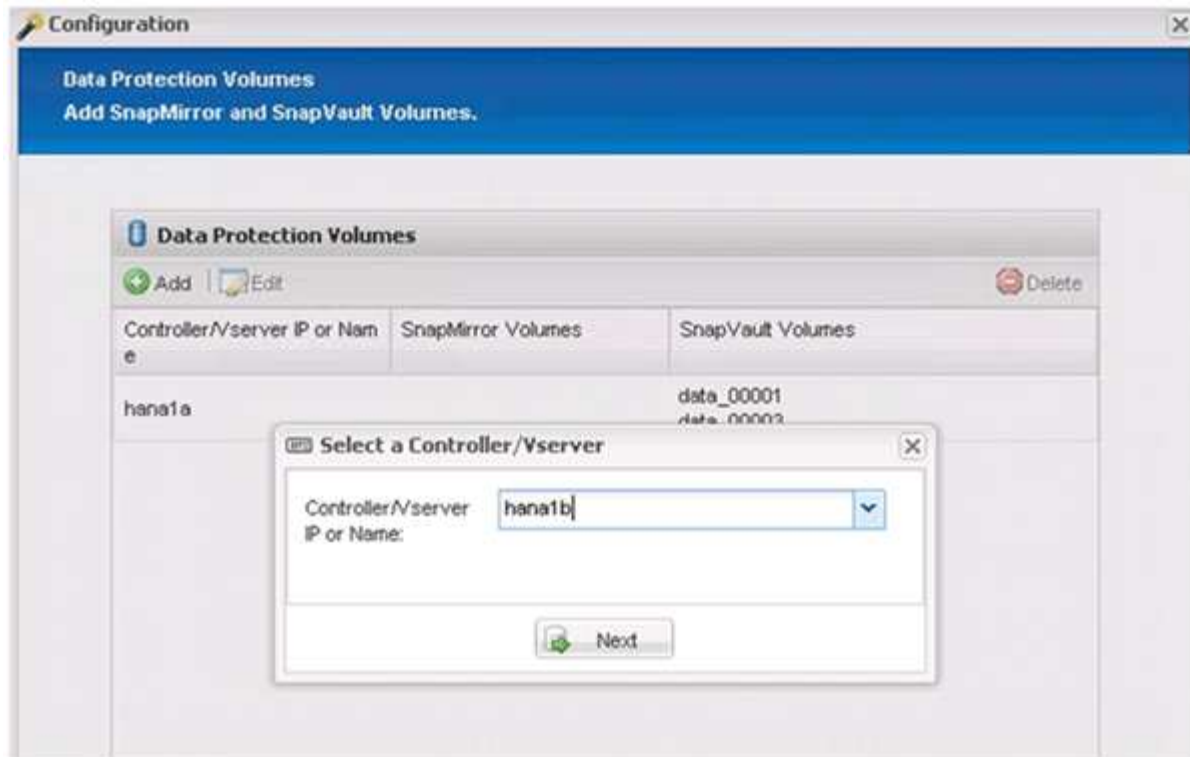
22. Wählen Sie einen Quell-Speicher-Controller aus der Liste aus, und klicken Sie auf **Weiter**.



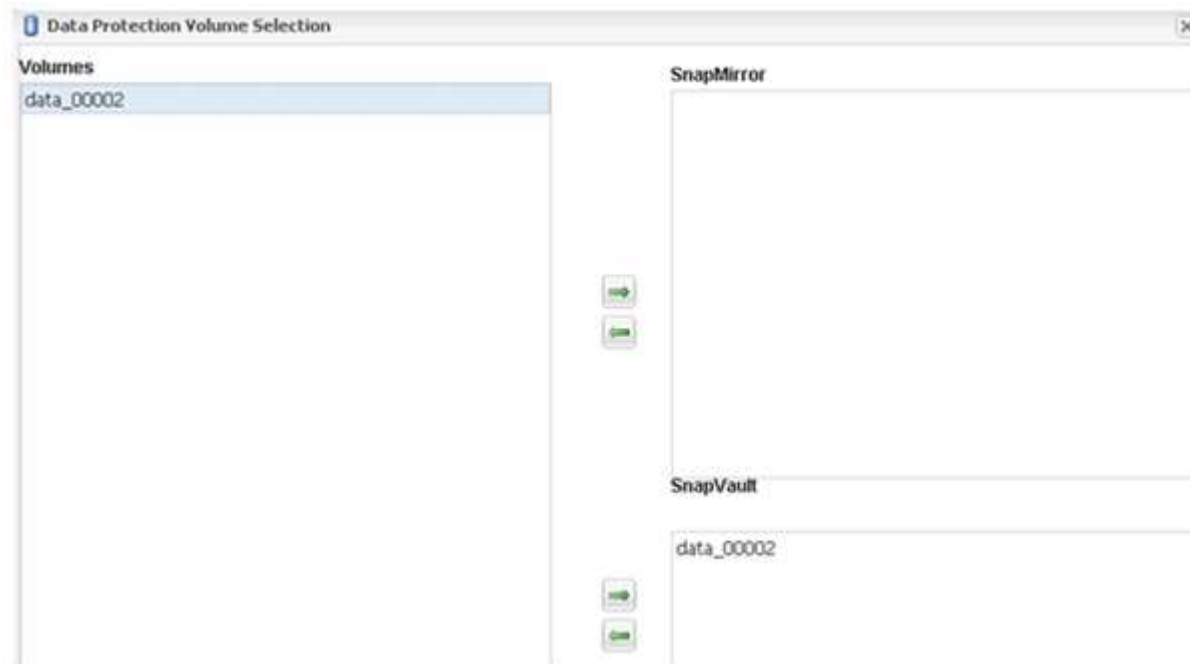
23. Wählen Sie alle Volumes aus, die auf dem Quell-Speicher-Controller gespeichert sind, und klicken Sie auf **Speichern**.



24. Klicken Sie auf **Hinzufügen**, und wählen Sie den zweiten Quell-Speicher-Controller aus der Liste aus, und klicken Sie dann auf **Weiter**.



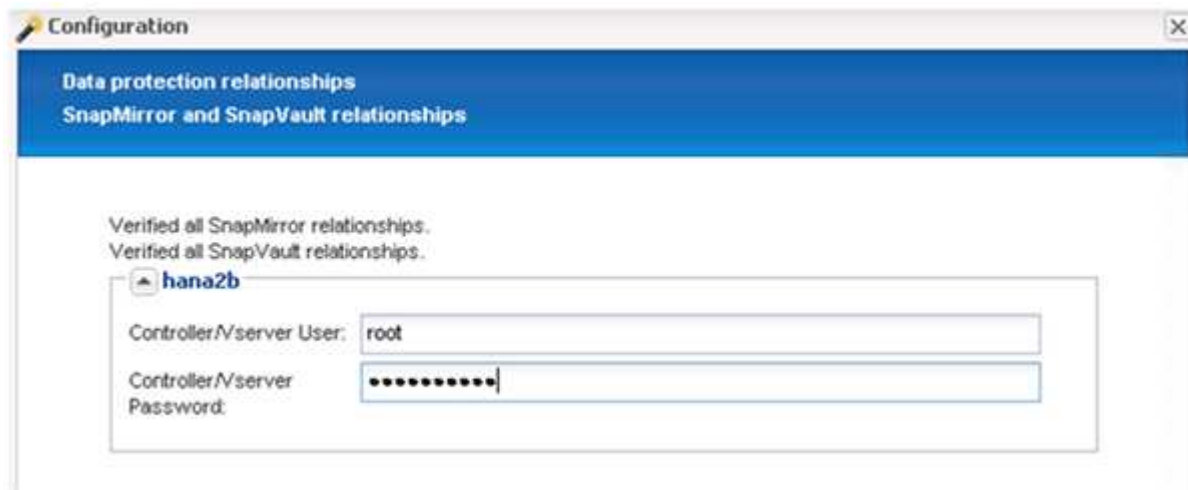
25. Wählen Sie alle Volumes aus, die auf dem zweiten Quell-Speicher-Controller gespeichert sind, und klicken Sie auf **Speichern**.



26. Im Fenster Data Protection Volumes werden alle Volumes angezeigt, die in der von Ihnen erstellten Konfiguration geschützt werden sollten. Klicken Sie Auf **Weiter**.




27. Geben Sie die Anmeldeinformationen für die Ziel-Storage-Controller ein, und klicken Sie auf **Weiter**. In diesem Beispiel werden die Benutzeranmeldeinformationen „root“ für den Zugriff auf das Speichersystem verwendet. Normalerweise wird ein dedizierter Backup-Benutzer auf dem Storage-System konfiguriert und dann mit Snap Creator verwendet.




28. Klicken Sie Auf **Weiter**.

DFM/OnCommand Settings
Enter OnCommand credentials and other details and settings.

☐ Operations Manager console Alert  
☒ NetApp Management Console data protection capability


Host:   
User:   
Password:   
Transport:    
Port:

29. Klicken Sie auf **Fertig stellen**, um die Konfiguration abzuschließen.

 Configuration

Summary

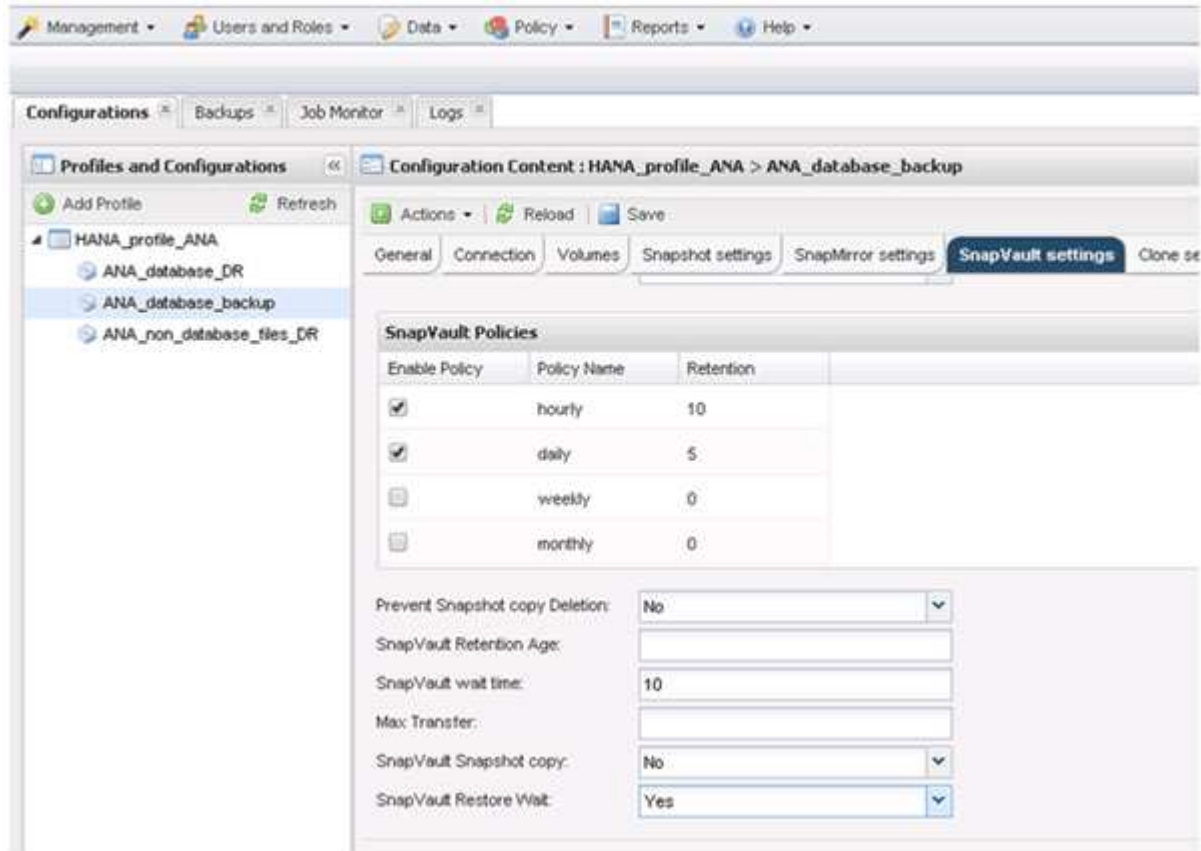
Configuration Name: ANA\_database\_backup  
Number of Controllers/Vservers added: 2  
Controller/Vserver Name: hana1a  
Controller/Vserver User: root  
Controller/Vserver Password: \*\*\*\*\*  
Controller/Vserver Name: hana1b  
Controller/Vserver User: root  
Controller/Vserver Password: \*\*\*\*\*  
Data protection Destination Controllers/Vservers added:  
Controller/Vserver Name: hana2b  
Controller/Vserver User: root  
Controller/Vserver Password: \*\*\*\*\*  
Global Controller/Vserver credentials: No  
Password Protection: Yes  
  
Volumes:  
hana1a: data\_00001, data\_00003;  
hana1b: data\_00002;  
  
Snapshot Copy Name: Backup-ANA  
Snapshot Copy Policy Name Convention: Timestamp  
  
Ignore Application Error: No  
SnapVault Update: Yes  
SnapVault Wait Time: 10  
SnapVault Volumes:  
Controller/Vserver: hana1a  
Volumes:  
data\_00001  
data\_00003  
Controller/Vserver: hana1b  
Volumes:  
data\_00002



Back Finish Cancel

30. Klicken Sie auf die Registerkarte **SnapVault-Einstellungen**.

31. Wählen Sie in der Dropdown-Liste der Option **SnapVault-Wiederherstellung warten** \* **Ja** aus, und klicken Sie auf **Speichern**.



Es wird empfohlen, für den Replikationsverkehr ein dediziertes Netzwerk zu verwenden. Wenn Sie sich dazu entscheiden, sollten Sie diese Schnittstelle in die Snap Creator-Konfigurationsdatei als sekundäre Schnittstelle aufnehmen.

Außerdem können Sie dedizierte Managementoberflächen konfigurieren, sodass Snap Creator über eine Netzwerkschnittstelle, die nicht an den Host-Namen des Storage Controllers gebunden ist, auf das Quell- oder Ziel-Storage-System zugreifen kann.

```
mgmtsrv01:/opt/NetApp/Snap_Creator_Framework_411/scServer4.1.1c/engine/c
onfigs/HANA_profile_ANA
# vi ANA_database_backup.conf

#####
#####
#      Connection Options                                #
#####
#####
PORT=443
SECONDARY_INTERFACES=hana1a:hana1a-rep/hana2b;hana1b:hana1b-rep/hana2b
MANAGEMENT_INTERFACES=hana2b:hana2b-mgmt
```



# Konfiguration von SAP HANA für SAN-Umgebungen

Nach der Konfiguration der Daten-Backups muss der Snap Creator Konfigurationsdatei in Umgebungen, in denen ein SAP HANA-System über Fibre Channel Storage Area Network (SAN) mit dem/den Storage Controller verbunden ist, ein neuer Befehl hinzugefügt werden.

Wenn ein globaler synchronisierter Backup-Speicherpunkt von Snap Creator innerhalb von SAP HANA ausgelöst wird, tritt der letzte Schritt auf, wenn SAP HANA die Datei /hana/Data/SID/mnt00001/hdb00001/Snapshot\_databackup\_0\_1 schreibt. Diese Datei ist Teil des Daten-Volumes auf dem Storage und ist daher Teil der Storage-Snapshot Kopie. Diese Datei ist bei der Durchführung einer Wiederherstellung obligatorisch, falls das Backup wiederhergestellt wird. Durch Metadaten-Caching mit dem 'X' File System (XFS) auf dem Linux-Host ist die Datei auf der Speicherebene nicht sofort sichtbar. Die standardmäßige XFS-Konfiguration für das Metadaten-Caching beträgt 30 Sekunden.

Innerhalb von Snap Creator müssen Sie einen Post-Application-Befehl quiesce hinzufügen, der wartet, bis der Metadaten-Cache der XFS auf die Festplattenebene gespeichert wird.

Sie können die Konfiguration des Metadaten-Caching mit folgendem Befehl überprüfen:

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

1. Fügen Sie in der Konfigurationsdatei (install\_PATH/scSrversion\_number/Engine/configs) den Befehl /bin/Sleep dem Abschnitt Post befiehlt, wie im folgenden Beispiel dargestellt:

```
#####
#      Post Commands      #####
POST_NTAP_DATA_TRANSFER_CMD01=
POST_APP QUIESCE_CMD01=/bin/sleep 60
POST_CLONE_CREATE_CMD01=
```



Sie sollten eine Wartezeit zulassen, die doppelt so hoch ist wie der Wert des Parameters fs.xfs.xfssyncd\_centisecs. Mit dem Standardwert 30 Sekunden sollte beispielsweise der Befehl Sleep mit 60 Sekunden konfiguriert werden.

## Protokollsicherungen werden konfiguriert

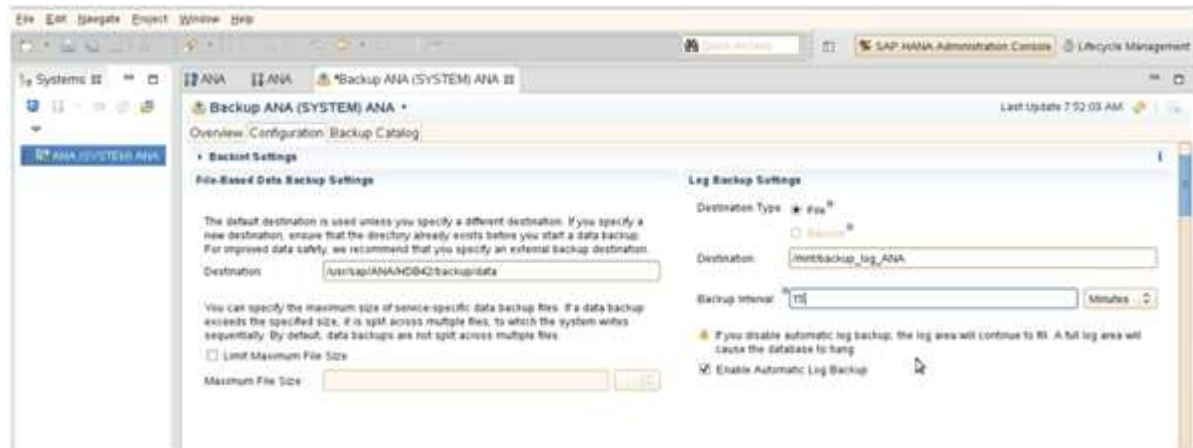
Log-Backups sollten auf einem anderen Storage-System als dem primären Storage gespeichert werden. Das Speichersystem, das für die Datensicherung verwendet wird, kann auch für das Protokoll-Backup verwendet werden.

Beim sekundären Storage muss ein Volume konfiguriert werden, um die Protokoll-Backups zu speichern. Vergewissern Sie sich, dass für dieses Volume automatische Snapshot-Kopien deaktiviert sind.

1. Mounten Sie das Volume an jedem Datenbankknoten, indem Sie entweder den Mount-Befehl ausführen oder die Dateisystemtabelle (fstab) bearbeiten.

```
hana2b:/vol/backup_log_ANA /mnt/backup_log_ANA nfs
rw,bg,vers=3,hard,timeo=600,rsz=65536,wsz=65536,actimeo=0,noatime
0 0
```

Innerhalb von SAP HANA Studio wird das Backup-Ziel für das Protokoll wie in der folgenden Abbildung dargestellt konfiguriert.



## Allgemeine Ordnung und Sauberkeit von Protokollsicherungen

Die allgemeine Ordnung und Sauberkeit von Log-Backups in SAP HANA basiert auf einer Funktion innerhalb von HANA Studio oder auf einer SQL-Anweisung, die das Löschen aller Backups ermöglicht, die älter als ein ausgewähltes Backup sind.

Snap Creator verwaltet die allgemeine Ordnung und Sauberkeit der Daten-Backups (Snapshot Kopien), indem die Snapshot Kopien auf dem primären oder sekundären Storage gelöscht und die entsprechenden Einträge im HANA-Katalog gemäß einer festgelegten Aufbewahrungsrichtlinie gelöscht werden.

Die Log-Backups, die älter als die letzte Datensicherung sind, werden gelöscht, da sie nicht benötigt werden.

Snap Creator verwaltet die allgemeine Ordnung und Sauberkeit der Backup-Erstellung von Protokolldateien auf Filesystem-Ebene und im SAP HANA Backup-Katalog. Als Teil eines jeden Snapshot Backups mit Snap Creator werden die folgenden Schritte ausgeführt:

- Lesen Sie den Backup-Katalog und erhalten Sie die Backup ID der ältesten erfolgreichen Daten oder des Snapshot Backups.
- Löschen Sie alle Backups, die älter als das älteste Backup sind.

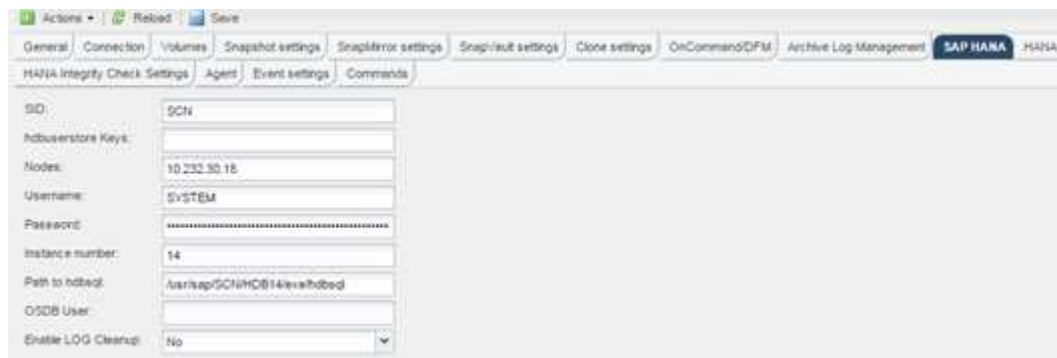


Snap Creator verwaltet nur die allgemeine Ordnung und Sauberkeit für Backups auf der Basis von Snapshot-Kopien. Wenn zusätzliche dateibasierte Backups erstellt werden, müssen Sie sicherstellen, dass die dateibasierten Backups aus dem Backup-Katalog und dem Dateisystem gelöscht werden. Wird eine solche Datensicherung nicht manuell aus dem Backup-Katalog gelöscht, kann sie zur ältesten Datensicherung werden, und die allgemeine Ordnung und Sauberkeit der Protokolle schlägt fehl.

## Änderung der allgemeinen Ordnung der Protokollsicherungen

Sie können die Parameter ändern, die für die allgemeine Ordnung der Protokollsicherungen konfiguriert sind, wenn Sie die Protokollbereinigung deaktivieren möchten.

1. Wählen Sie das SAP HANA-Profil aus, das Sie ändern möchten.
2. Wählen Sie die zu ändernde Konfiguration aus, und klicken Sie auf **SAP HANA-Einstellungen**.
3. Bearbeiten Sie den Parameter Protokollbereinigung aktivieren, und klicken Sie auf **Speichern**.



## Datenbank-Backups werden ausgeführt

Sie können ein Backup Ihrer SAP HANA Datenbank über die Snap Creator GUI oder die Befehlszeile erstellen. Zum Planen von Backups können Sie den Scheduler innerhalb der GUI verwenden oder die Befehlszeile in Kombination mit einem externen Scheduler wie cron verwenden.

### Überblick über Datenbank-Backups

Wenn Snap Creator die Datenbank sichert, werden die folgenden Schritte ausgeführt.

1. Erstellen eines globalen, synchronisierten Speicherpunktes für Backups (SAP HANA Snapshot Kopie), um ein konsistentes Image auf der Persistenzschicht zu erhalten
2. Erstellung von Storage-Snapshot Kopien für alle Daten-Volumes

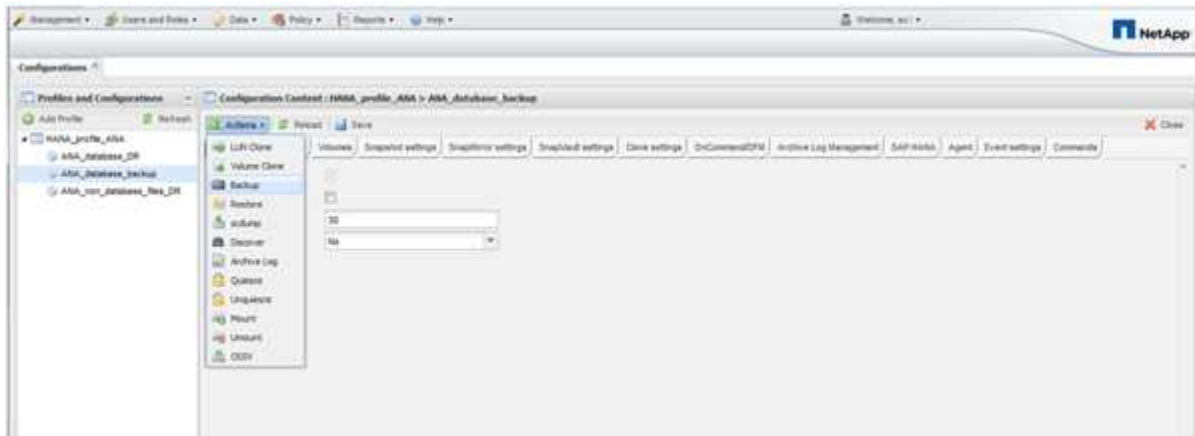
In diesem Beispiel gibt es drei Daten-Volumes, die auf beide Storage Controller verteilt sind: Hana1a und hana1b.

3. Das Storage-Snapshot-Backup im SAP HANA Backup-Katalog registrieren
4. Löschen Sie die SAP HANA Snapshot Kopie.
5. Starten Sie das SnapVault Update für alle Daten-Volumes.
6. Überprüfen Sie den SnapVault-Status und warten Sie, bis die Zeitüberschreitung beendet oder konfigurierbar ist.
7. Löschen der Storage-Snapshot-Kopien und Löschen der Backups im SAP HANA Backup-Katalog basierend auf der festgelegten Aufbewahrungsrichtlinie für Backups im primären und sekundären Storage
8. Löschen Sie alle Log-Backups, die älter als die älteste Datensicherung des Filesystems und im SAP HANA Backup-Katalog sind.

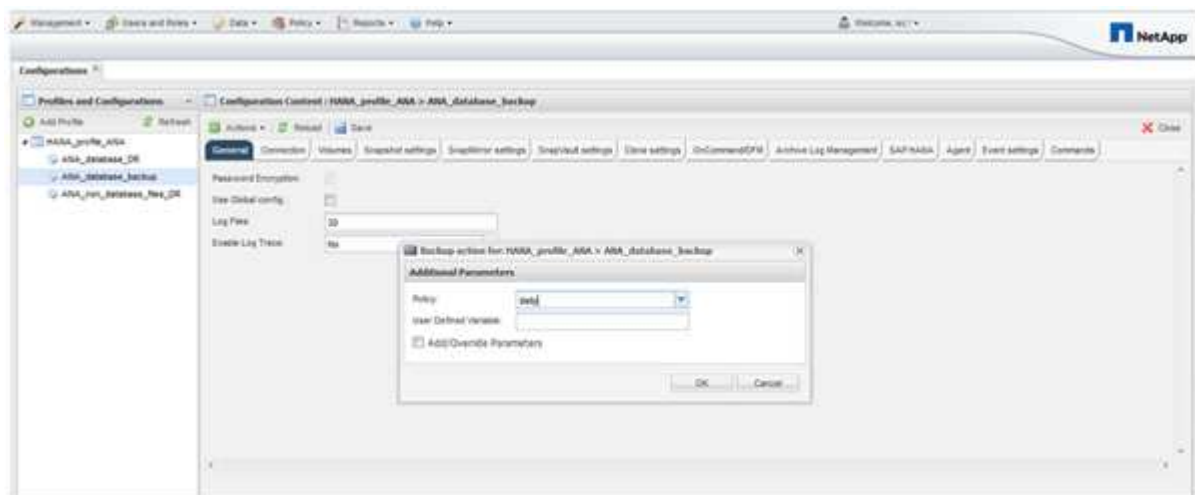
## Sichern der Datenbank mit der Snap Creator GUI

Sie können eine Datenbank über die Snap Creator GUI sichern.

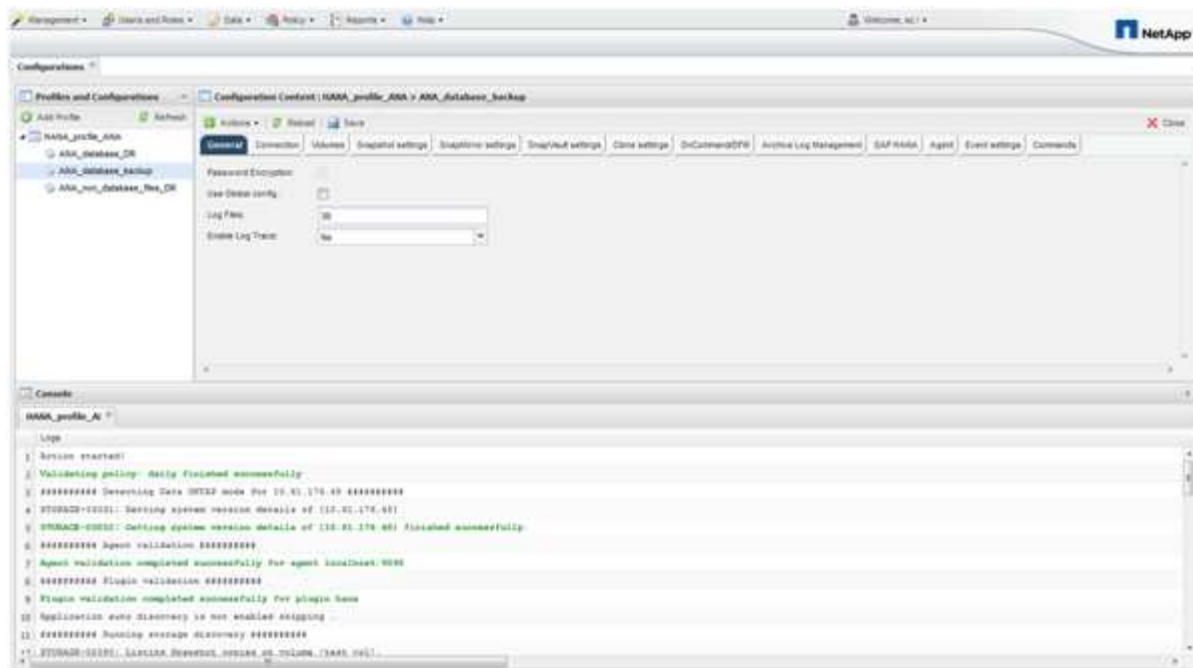
1. Wählen Sie die Konfiguration **HANA\_Database\_Backup** und dann **Aktionen > Backup** aus.



2. Wählen Sie die Backup Policy aus und klicken Sie auf **OK**.



Das Backup wird gestartet. Snap Creator löst das „SnapVault Update“ aus, und Snap Creator wartet, bis die Daten auf den sekundären Storage repliziert werden. Die Wartezeit wurde während der Konfiguration konfiguriert und kann auf der Registerkarte SnapVault-Einstellungen angepasst werden. Snap Creator löst die SnapVault Updates parallel für jedes Volume auf demselben Storage Controller aus, allerdings in Sequenz für jeden Storage Controller.



## Sichern der Datenbank mit der Snap Creator Kommandozeile

Sie können ein Backup der Datenbank auch über die Snap Creator Befehlszeile erstellen.

1. Um die Datenbank zu sichern, führen Sie den folgenden Befehl aus.

```

mgmtsrv01:~ #
/opt/NetApp/Snap_Creator_Framework_411/scServer4.1.1/snapcreator
--server
localhost --port 8443 --user scadmin --passwd scadmin --profile
HANA_profile_ANA --config
ANA_database_backup --action backup --policy daily --verbose
[Wed Mar 5 14:17:08 2014] INFO: Validating policy: daily finished
successfully

##### Detecting Data ONTAP mode for hanala #####

##### Detecting Data ONTAP mode for hanalb #####
[Wed Mar 5 14:17:13 2014] INFO: STORAGE-03031: Getting system version
details of [hana2b]
[Wed Mar 5 14:17:13 2014] INFO: STORAGE-03032: Getting system version
details of [hana2b] finished successfully.
[Wed Mar 5 14:17:13 2014] INFO: STORAGE-03031: Getting system version
details of [hanala]
[Wed Mar 5 14:17:13 2014] INFO: STORAGE-03032: Getting system version
details of [hanala] finished successfully.
[Wed Mar 5 14:17:13 2014] INFO: STORAGE-03031: Getting system version
details of [hanalb]
[Wed Mar 5 14:17:13 2014] INFO: STORAGE-03032: Getting system version
details of [hanalb] finished successfully.

...
Truncated
...

```

## Überprüfung verfügbarer Backups im SAP HANA Studio

Die Liste der Storage Snapshot Backups finden Sie im SAP HANA Studio.

Der hervorgehobene Backup in der folgenden Abbildung zeigt eine Snapshot Kopie mit dem Namen „Backup-ANA\_hourly\_20140320103943.“ Dieses Backup umfasst Snapshot Kopien für alle drei Daten-Volumes des SAP HANA Systems. Das Backup ist auch auf dem sekundären Speicher verfügbar.





# SAP HANA dateibasiertes Backup und Integritätsprüfung der Datenbank

SAP empfiehlt, Storage-basierte Snapshot-Backups mit einem wöchentlichen dateibasierten Backup zu kombinieren, um eine Integritätsprüfung für Blöcke durchzuführen. Die Block-Integritätsprüfung kann über die grafische Benutzeroberfläche (GUI) oder die Befehlszeilenschnittstelle (CLI) von Snap Creator ausgeführt werden.

Die dateibasierte Datensicherung wird verwendet, wenn die Backup-Kopien von Dateien aufbewahrt werden sollen. Die Datenbankintegritätsprüfungen werden verwendet, wenn Backup-Kopien verworfen werden müssen.

Sie können einen oder beide Vorgänge konfigurieren. Während eines On-Demand-Backups können Sie eine der Operationen auswählen.

## Ändern der Konfiguration für das dateibasierte Backup

Sie können die Parameter ändern, die für File-Based Backup konfiguriert sind. Der nachfolgende geplante oder dateibasierte Backup-Vorgang auf Abruf gibt die aktualisierten Informationen wieder.

1. Klicken Sie auf das SAP HANA-Profil.
2. Wählen Sie die Konfiguration aus, die Sie ändern möchten, und klicken Sie auf **HANA File Based Backup Settings**.



3. Bearbeiten Sie die Informationen und klicken Sie auf **Speichern**.

## Ändern der Konfiguration für Datenbankintegritätsprüfungen

Sie können die Parameter ändern, die für Datenbankintegritätsprüfungen konfiguriert sind. Der nachfolgende geplante oder On-Demand Integrity Check gibt die aktualisierten Informationen wieder.

1. Klicken Sie auf das SAP HANA-Profil.
2. Wählen Sie die Konfiguration aus, die Sie ändern möchten, und klicken Sie auf **HANA Integrity Check Settings**.





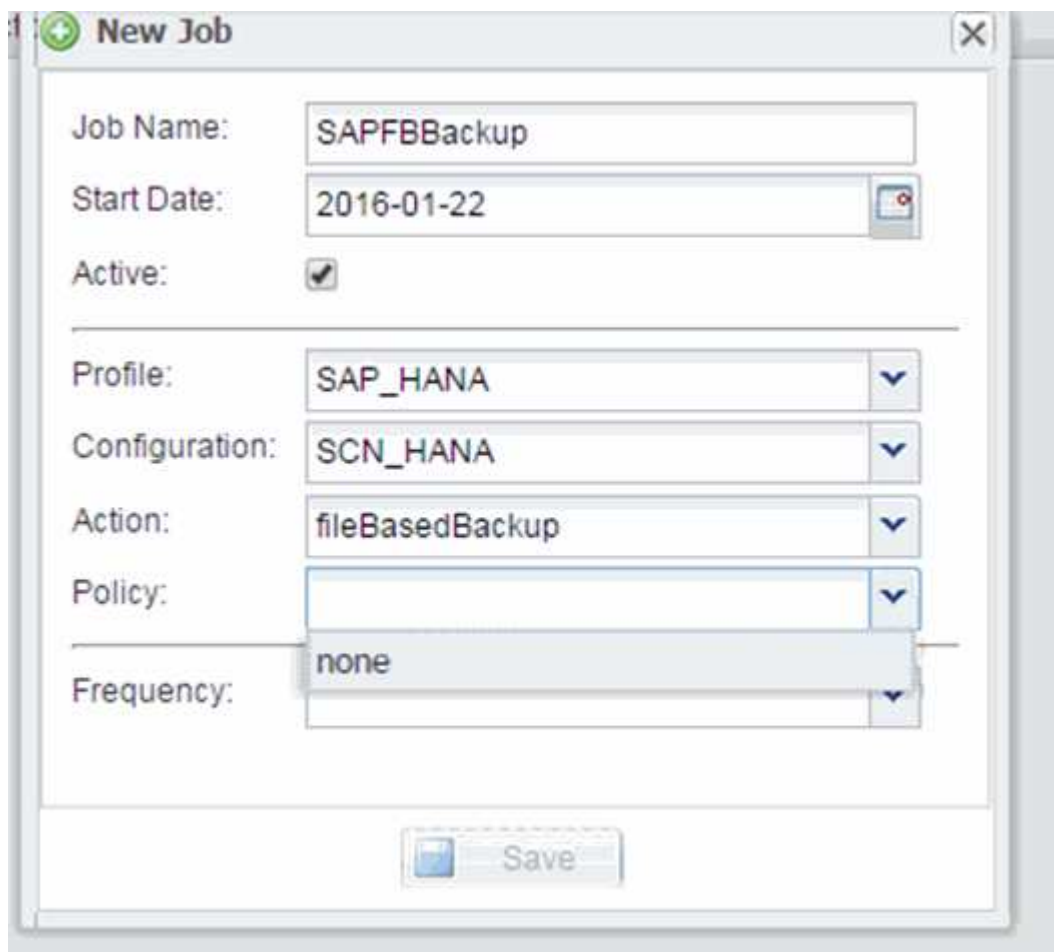
3. Bearbeiten Sie die Informationen und klicken Sie auf **Speichern**.

## Planung des dateibasierten Backups

Für SAP HANA Konfigurationen können zusätzliche Vorgänge, wie z. B. dateibasierte Backups und Integritätsprüfungen für Datenbanken, geplant werden. Sie können den dateibasierten Backup-Vorgang in bestimmten Intervallen planen.

1. Wählen Sie im Hauptmenü der Snap Creator GUI die Option **Verwaltung > Zeitpläne** und klicken Sie auf **Erstellen**.
2. Geben Sie im Fenster Neuer Job die Details für den Job ein.

Die Datei-basierte Backup-Richtlinie ist standardmäßig auf „none“ eingestellt.

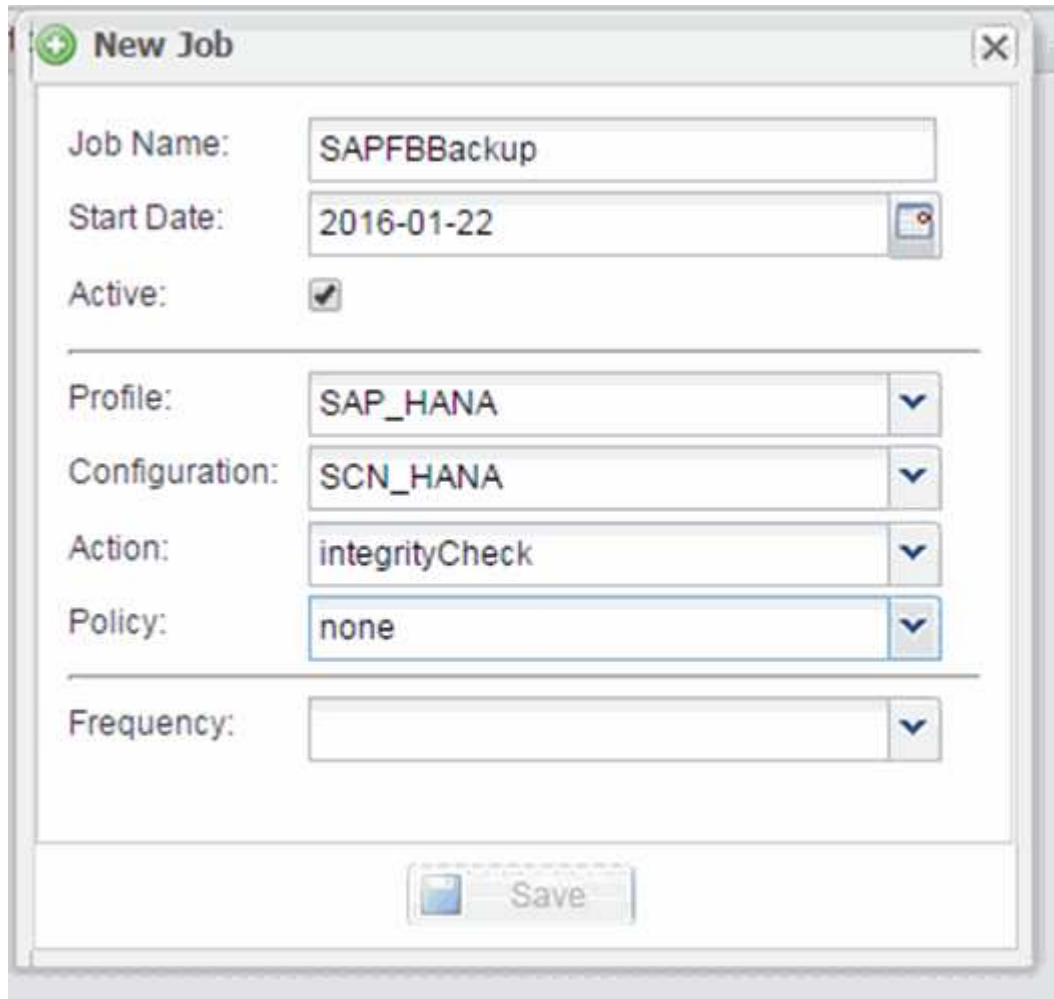


## Planen der Datenbankintegritätsprüfungen

Für SAP HANA Konfigurationen können zusätzliche Vorgänge, wie z. B. dateibasierte Backups und Integritätsprüfungen für Datenbanken, geplant werden. Sie können den Betrieb der Datenbankintegritätsprüfungen in bestimmten Intervallen planen.

1. Wählen Sie im Hauptmenü der Snap Creator GUI die Option **Verwaltung > Zeitpläne** und klicken Sie auf **Erstellen**.
2. Geben Sie im Fenster Neuer Job die Details für den Job ein.

Die Integritätsprüfung ist standardmäßig auf „none“ eingestellt.



The screenshot shows the 'New Job' dialog box with the following settings:

- Job Name: SAPFBBBackup
- Start Date: 2016-01-22
- Active: ☒
- Profile: SAP\_HANA
- Configuration: SCN\_HANA
- Action: integrityCheck
- Policy: none
- Frequency: (empty)

A 'Save' button is located at the bottom of the dialog.

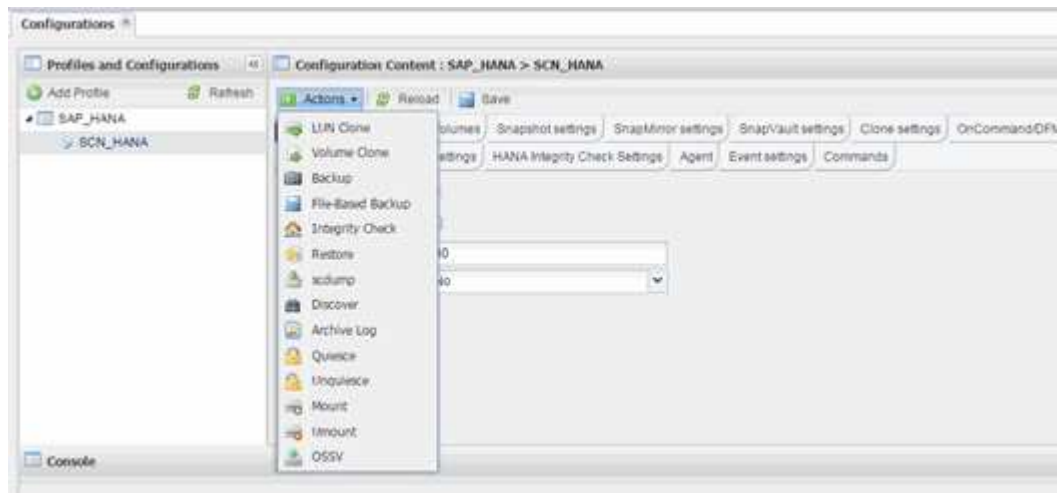
## Durchführen dateibasierter Backups über die Snap Creator GUI

Sie können File-basierte Backups über die grafische Benutzeroberfläche von Snap Creator durchführen (GUI).

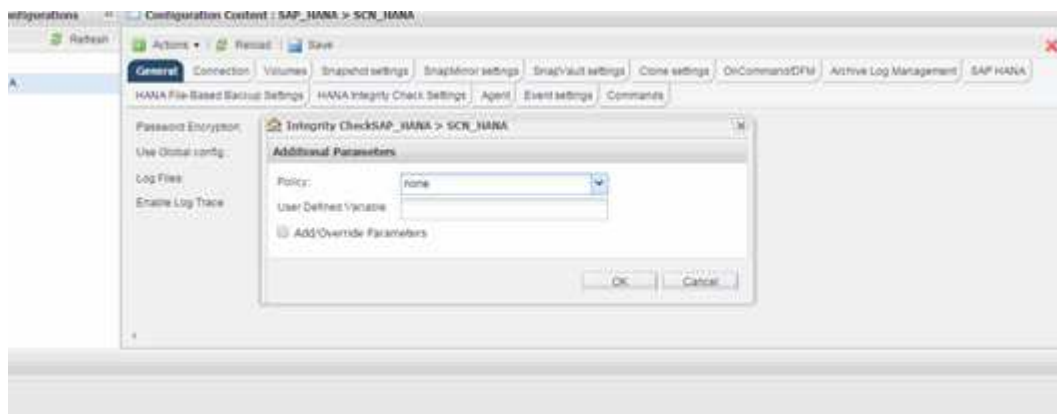
Sie müssen den Parameter File-Based Backup auf der Registerkarte HANA File-Based Backup Settings aktiviert haben.

1. Wählen Sie die HANA\_Database\_Backup-Konfiguration aus.

2. Wählen Sie **Actions > File-Based Backup** Aus.



3. Legen Sie die Policy-Option auf **Keine** fest, und klicken Sie auf **OK**.



## Durchführen der dateibasierten Datensicherung über die Befehlszeile von Snap Creator

Sie können File-basierte Backups über die Snap Creator Befehlszeile durchführen.

1. Führen Sie den folgenden Befehl aus, um eine dateibasierte Sicherung durchzuführen:

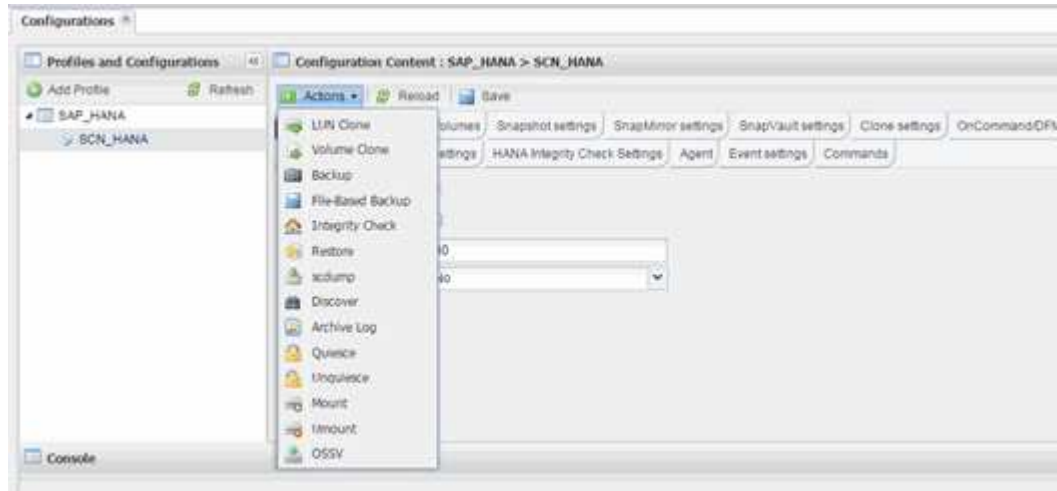
```
./snapcreator --server localhost --port 8443 --user sc --passwd sc  
--profile hana_testing --config HANA_Test --action fileBasedBackup  
--policy none --verbose
```

## Durchführen von Datenbankintegritätsprüfungen über die Snap Creator GUI

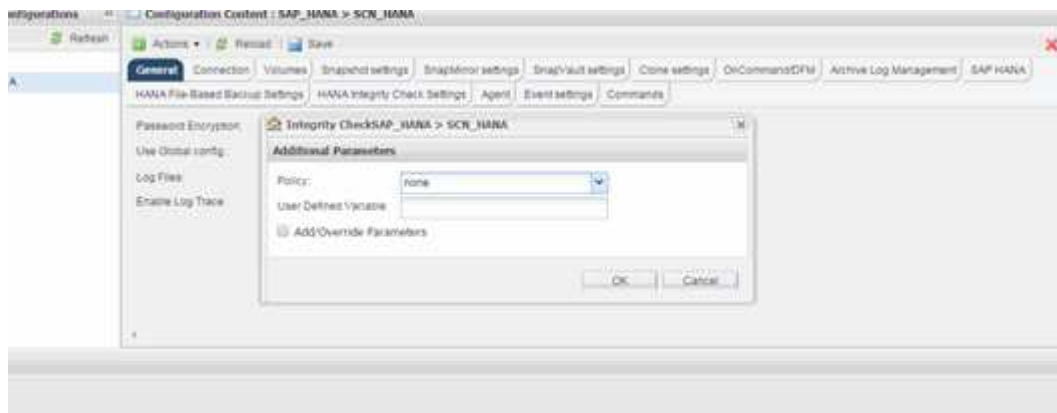
Sie können Datenbankintegritätsprüfungen über die grafische Benutzeroberfläche von Snap Creator durchführen.

Sie müssen den Parameter DB Integrity Check auf der Registerkarte „HANA Integrity Check Settings“ aktiviert haben.

1. Wählen Sie die Konfiguration HANA\_Database\_Integrity\_Check aus.
2. Wählen Sie **Aktionen > Integritätsprüfung**.



3. Legen Sie die Policy-Option auf **Keine** fest, und klicken Sie auf **OK**.



## Durchführen von Datenbankintegritätsprüfungen über die Befehlszeile von Snap Creator

Sie können eine Datenbankintegritätsprüfung über die Snap Creator-Befehlszeile durchführen.

1. Führen Sie den folgenden Befehl aus, um Datenbankintegritätsprüfungen durchzuführen:

```
./snapcreator --server localhost --port 8443 --user sc --passwd sc
--profile hana_testing --config HANA_Test --action integrityCheck
--policy none --verbose
```

## Wiederherstellung von SAP HANA Datenbanken

Mit SAP HANA Studio und Snap Creator lassen sich SAP HANA Datenbanken wiederherstellen und wiederherstellen.

1. In SAP HANA Studio:
  - a. Wählen Sie Recover für das SAP HANA-System aus.
  - b. Das SAP HANA-System wird heruntergefahren.
  - c. Wählen Sie den Wiederherstellungstyp aus.
  - d. Bereitstellung von Backup-Speicherorten für Protokolle
  - e. Es wird eine Liste von Daten-Backups angezeigt
  - f. Wählen Sie Sicherung, um die externe Backup-ID anzuzeigen.
2. Nur bei einem Storage-System mit Clustered Data ONTAP:
  - a. Nur erforderlich, wenn für die Wiederherstellung ein anderes Backup als das neueste verwendet wurde.
  - b. Nur erforderlich für „Volume SnapRestore“ aus dem Primärspeicher.
  - c. SnapVault-Beziehungen deaktivieren
3. In Snap Creator:
  - a. Wählen Sie „Restore“ für das SAP HANA-System aus.
  - b. Wählen Sie je nach Verfügbarkeit des Backups im primären oder sekundären Storage das Restore aus.
  - c. Wählen Sie Storage-Controller, Volume-Namen und den Namen der Snapshot Kopie aus. Der Name der Snapshot Kopie entspricht der vorherigen Backup-ID.
  - d. Bei SAP HANA Systemen mit mehreren Nodes müssen mehrere Volumes wiederhergestellt werden:
    - i. Wählen Sie **Weitere wiederherstellende Elemente hinzufügen**.
    - ii. Wählen Sie Storage-Controller, Volume-Namen und den Namen der Snapshot Kopie aus.
    - iii. Wiederholen Sie diesen Vorgang für alle erforderlichen Volumes.
  - e. Bei mandantenfähigen Datenbankcontainern (MDC) Einzelmandanten-Datenbanksystemen werden sowohl DIE SYSTEM- als auch DIE MANDANTENDATENBANKEN wiederhergestellt.
  - f. Der Wiederherstellungsprozess wird gestartet
  - g. Wiederherstellung für alle Volumes abgeschlossen.
4. Heben Sie an den Datenbank-Knoten alle Datenvolumen ab und mounten Sie sie mit den „veralteten NFS-Handles“.
5. In SAP HANA Studio:
  - a. Wählen Sie in der Sicherungsliste die Option **Aktualisieren** aus.
  - b. Wählen Sie verfügbares Backup für die Recovery (grünes Element).
  - c. Starten Sie den Recovery-Prozess.
  - d. Starten Sie bei einzelnen mandantenfähigen Datenbanksystemen den Recovery-Prozess zunächst für die SYSTEMDATENBANK und schließlich für die MANDANTEN-Datenbank.
  - e. Das SAP HANA System wird gestartet.
6. (Optional) Fortsetzen der SnapVault-Beziehungen für alle wiederhergestellten Volumes.



Bei den Speichersystemen ist dieser Schritt nur erforderlich, wenn ein anderes Backup als das neueste für die Wiederherstellung verwendet wurde.

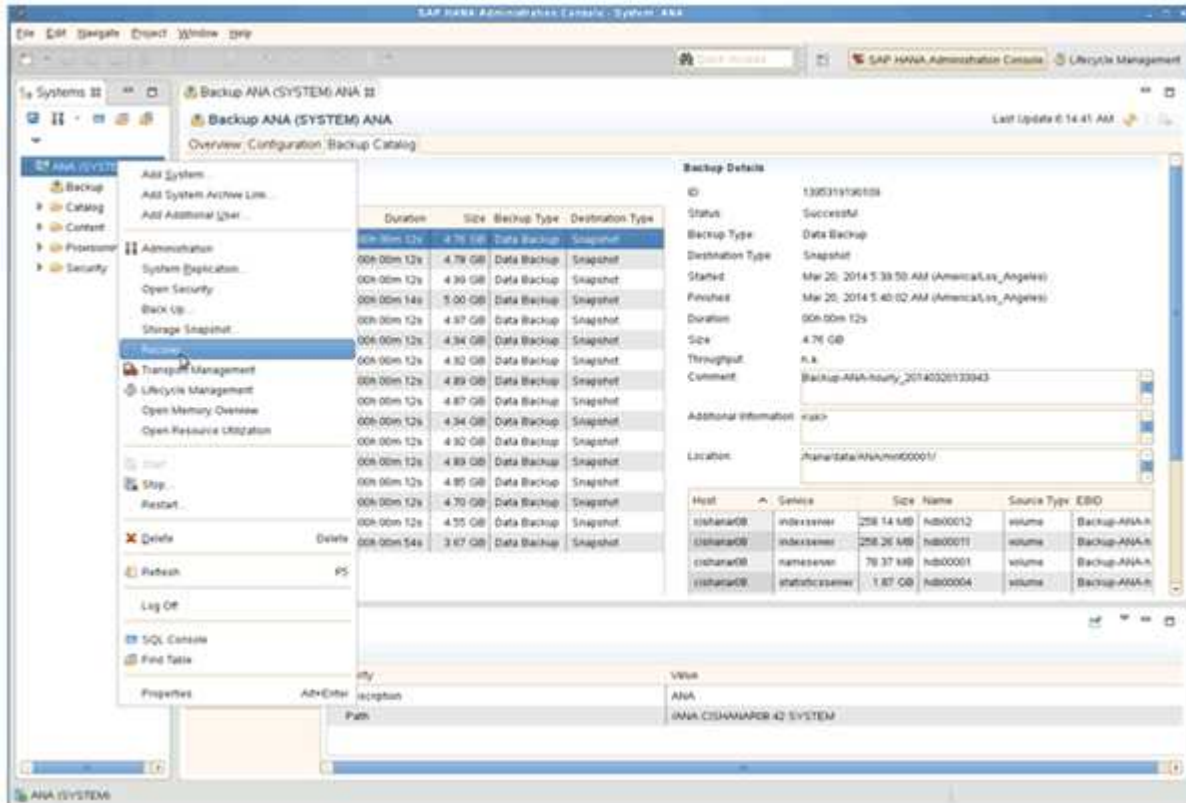
## Wiederherstellung von Datenbanken aus dem Primärspeicher

Sie können die Datenbank aus dem primären Storage wiederherstellen.



Sie können keine dateibasierten Backup Kopien von Snap Creator wiederherstellen.

1. Wählen Sie in SAP HANA Studio **Recover** für das SAP HANA-System aus.



Das SAP HANA-System wird heruntergefahren.

2. Wählen Sie den Wiederherstellungstyp aus und klicken Sie auf **Weiter**.

Recovery of System ANA (on nshahar08)

### Specify Recovery Type

Select a recovery type.

☒ Recover the database to its most recent state<sup>?</sup>

☐ Recover the database to the following point in time<sup>?</sup>

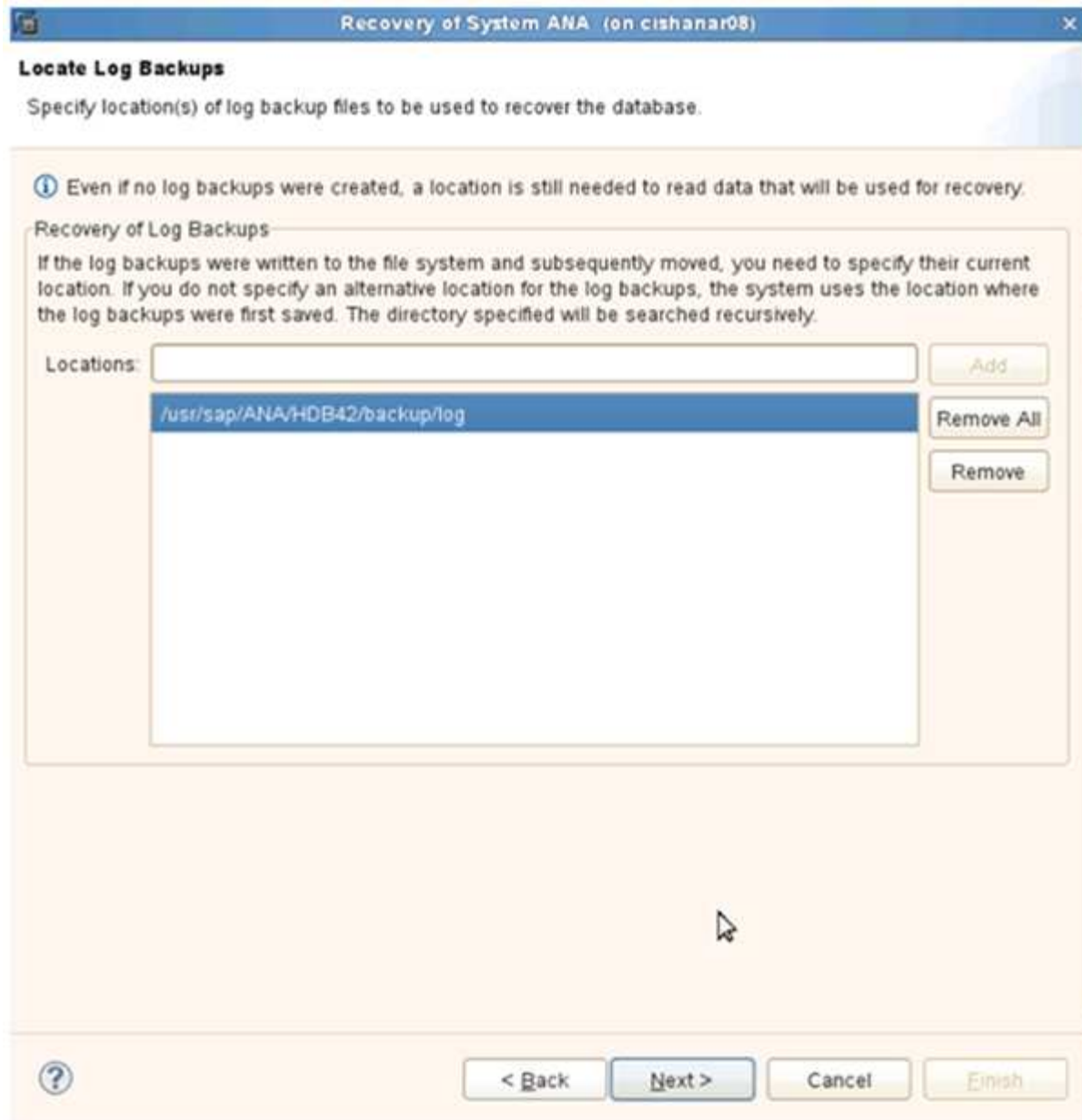
Date:   Time:

Select Time Zone:

System time used (GMT): 2014-03-20 10:28:17

☐ Recover Database to a Specific Data Backup<sup>?</sup>

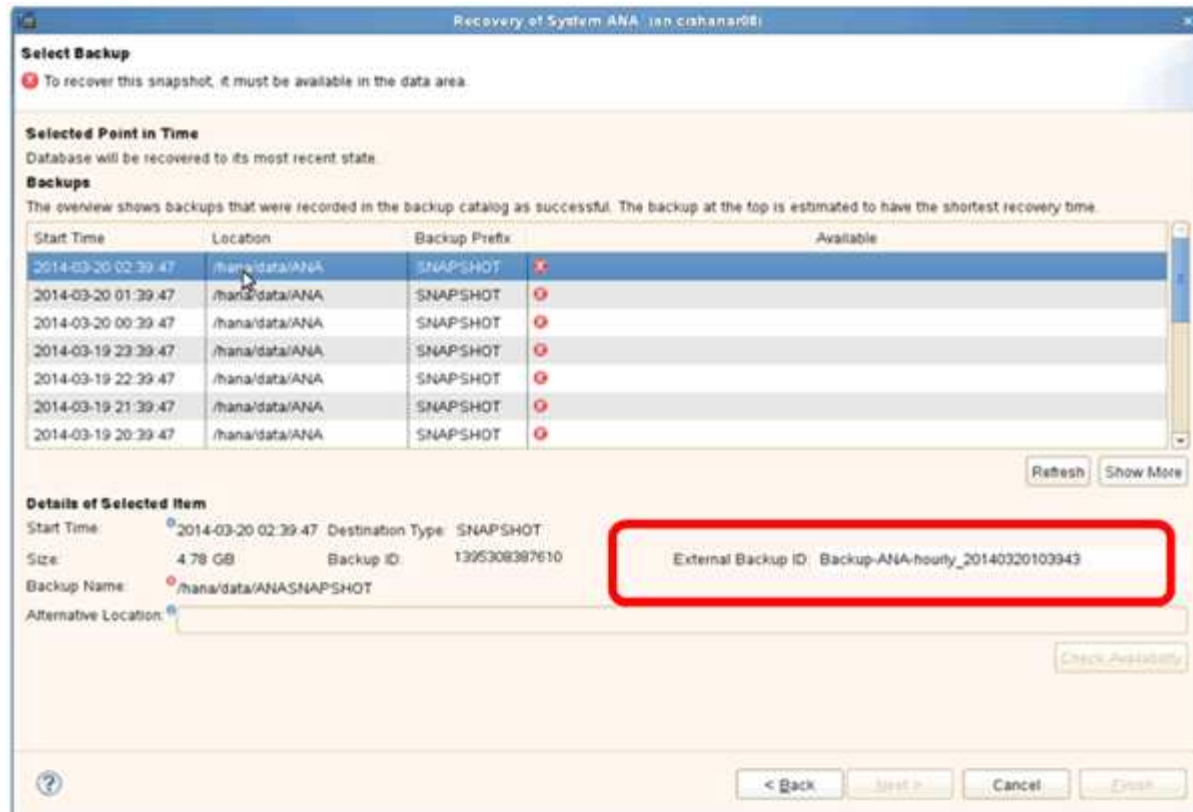
3. Geben Sie die Log-Backup-Speicherorte an und klicken Sie auf **Next**.



Die Liste der verfügbaren Backups, die Sie sehen, basiert auf dem Inhalt des Backup-Katalogs.

4. Wählen Sie die gewünschte Sicherung aus und notieren Sie die externe Backup-ID.





##### 5. Deaktivieren der SnapVault-Beziehung.



Dieser Schritt ist nur bei Clustered Data ONTAP erforderlich.

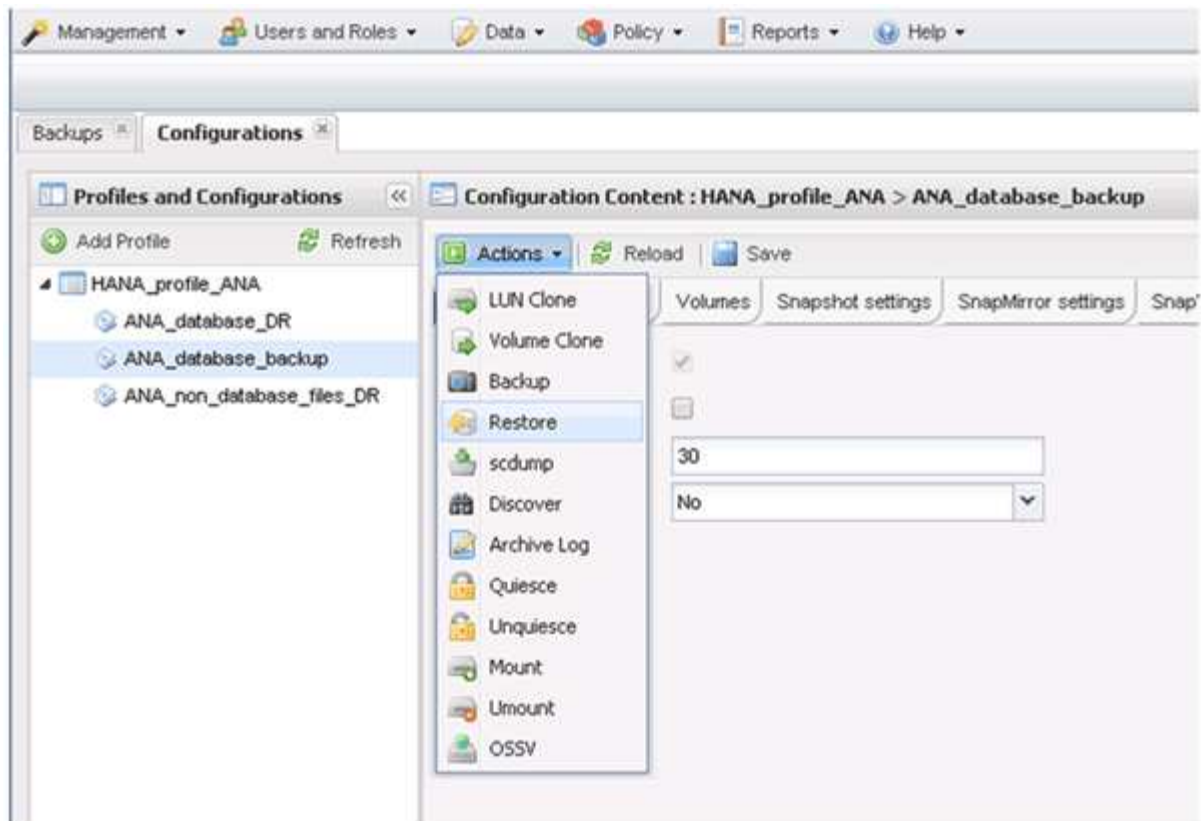
Wenn Sie eine Snapshot Kopie wiederherstellen müssen, die älter als die Snapshot Kopie ist, die derzeit als Basis-Snapshot Kopie für SnapVault verwendet wird, müssen Sie zuerst die SnapVault-Beziehung in Clustered Data ONTAP deaktivieren. Führen Sie dazu folgende Befehle an der Backup-Cluster-Konsole aus:

```
hana::> snapmirror quiesce -destination-path hana2b:backup_hana_data
Operation succeeded: snapmirror quiesce for destination
hana2b:backup_hana_data.
```

```
hana::> snapmirror delete -destination-path hana2b:backup_hana_data
Operation succeeded: snapmirror delete the relationship with destination
hana2b:backup_hana_data.
```

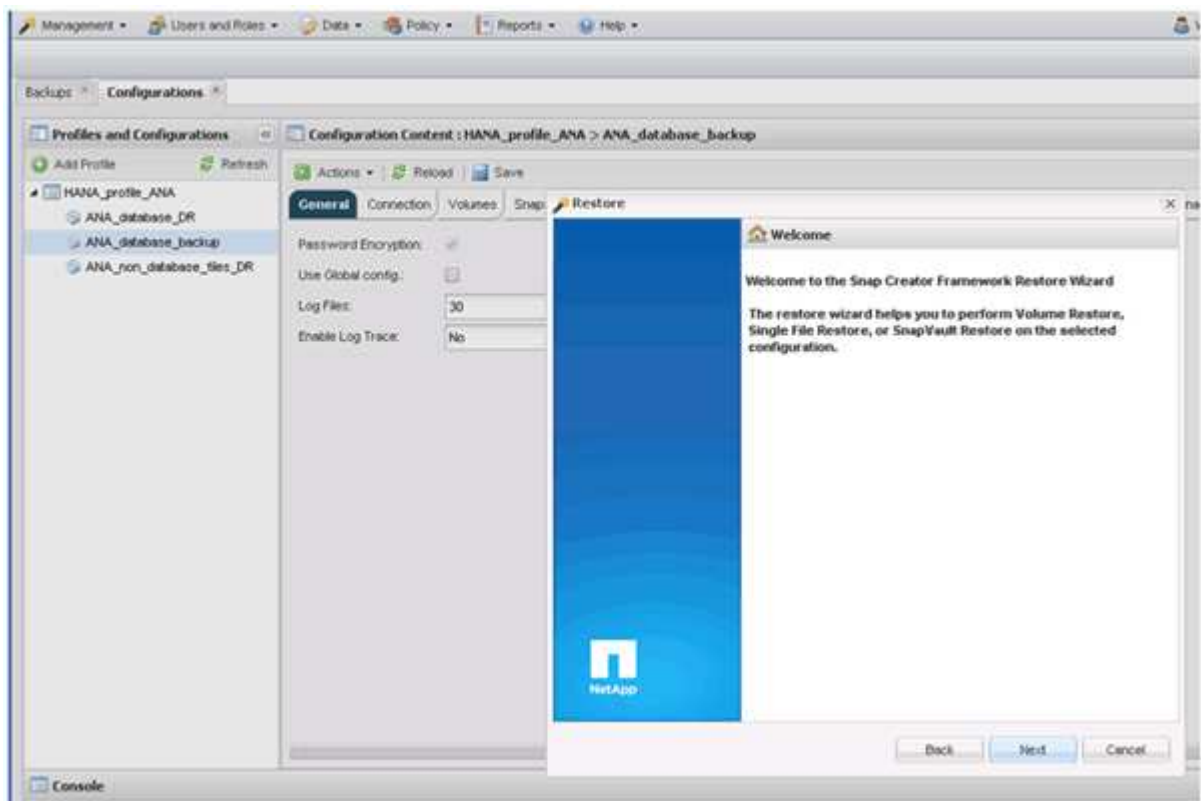
```
hana::> snapmirror release -destination-path hana2b:backup_hana_data
[Job 6551] Job succeeded: SnapMirror Release Succeeded
```

##### 6. Wählen Sie in der Snap Creator GUI das SAP HANA-System aus und wählen Sie dann **Aktionen > Wiederherstellen** aus.

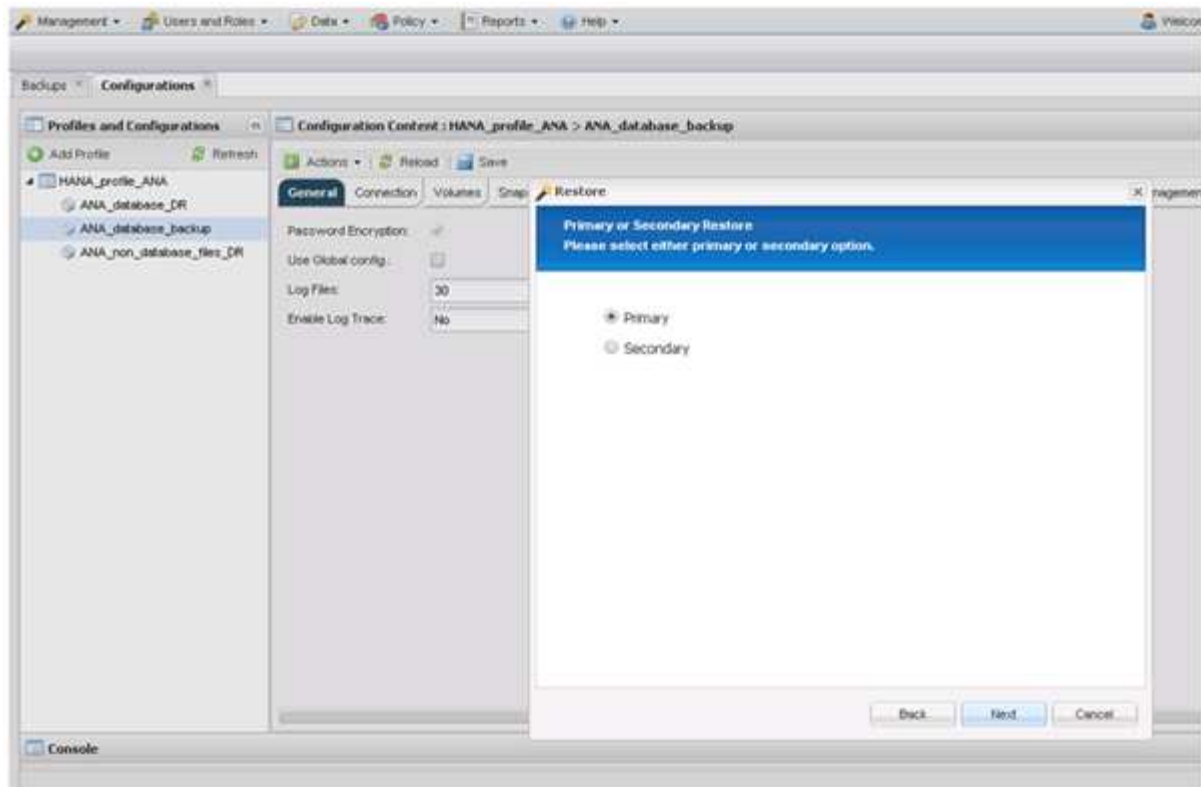


Der Bildschirm Willkommen im Snap Creator Framework Restore Wizard wird angezeigt.

7. Klicken Sie Auf **Weiter**.



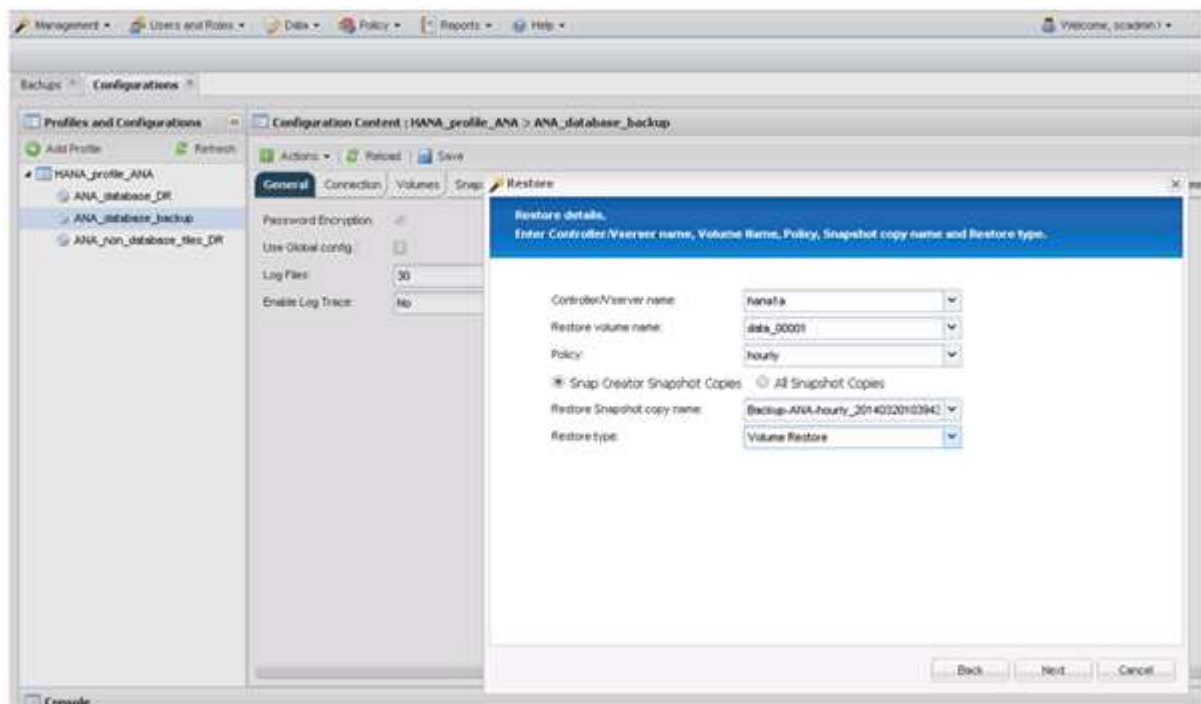
8. Wählen Sie **Primär** und klicken Sie auf **Weiter**.



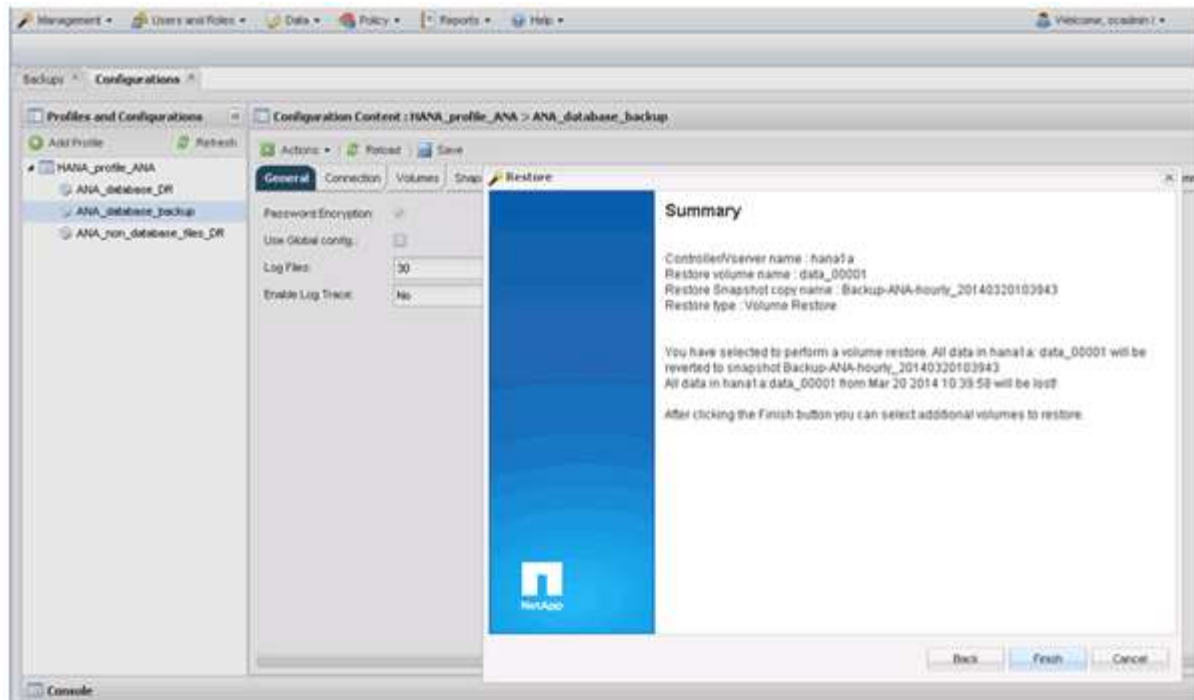
9. Wählen Sie Restore aus dem primären Storage aus.

10. Wählen Sie den Storage-Controller, den Volume-Namen und den Snapshot-Namen aus.

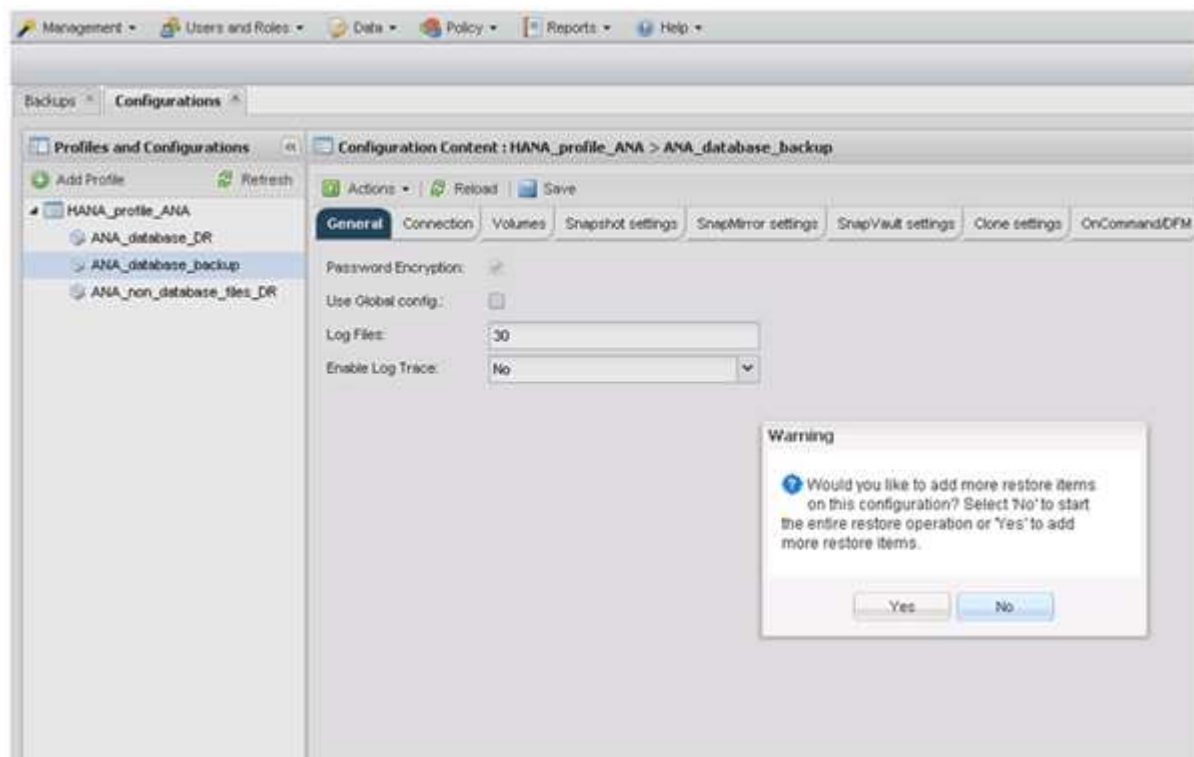
Der Snapshot-Name steht im Zusammenhang mit der Backup-ID, die im SAP HANA Studio ausgewählt wurde.



11. Klicken Sie Auf **Fertig Stellen**.

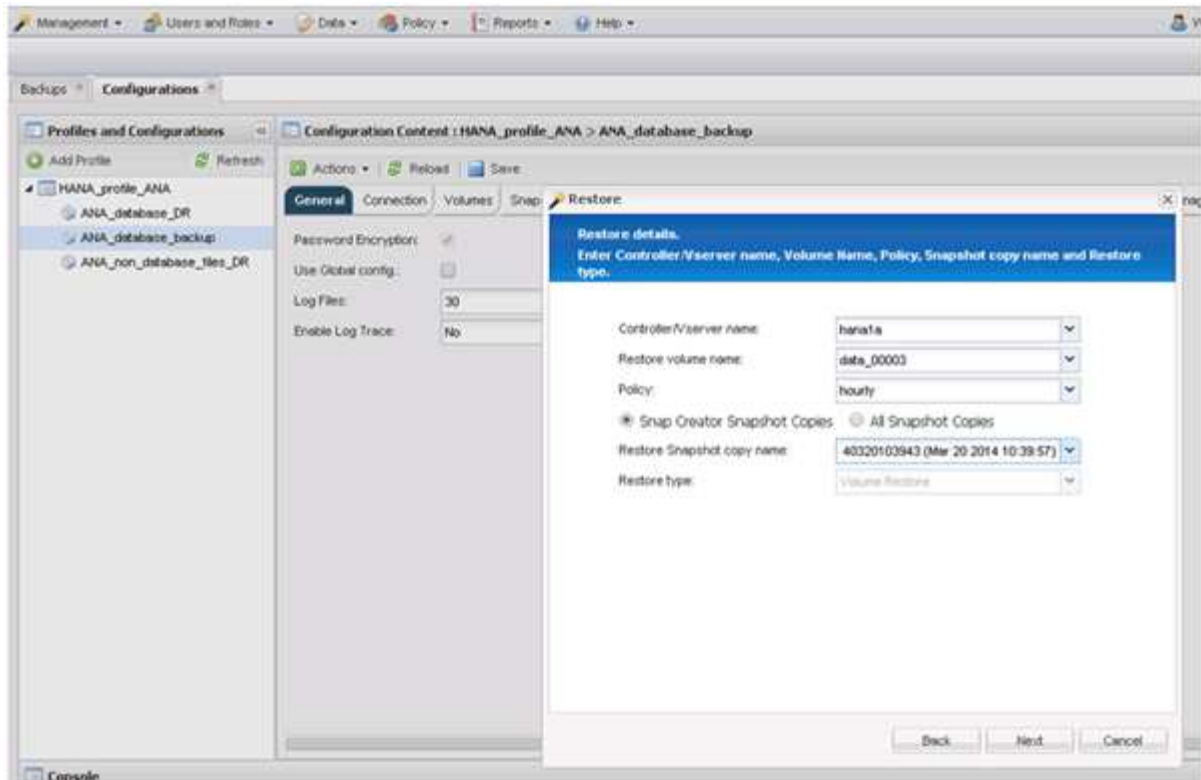


12. Klicken Sie auf **Ja**, um weitere wiederherzustellende Elemente hinzuzufügen.

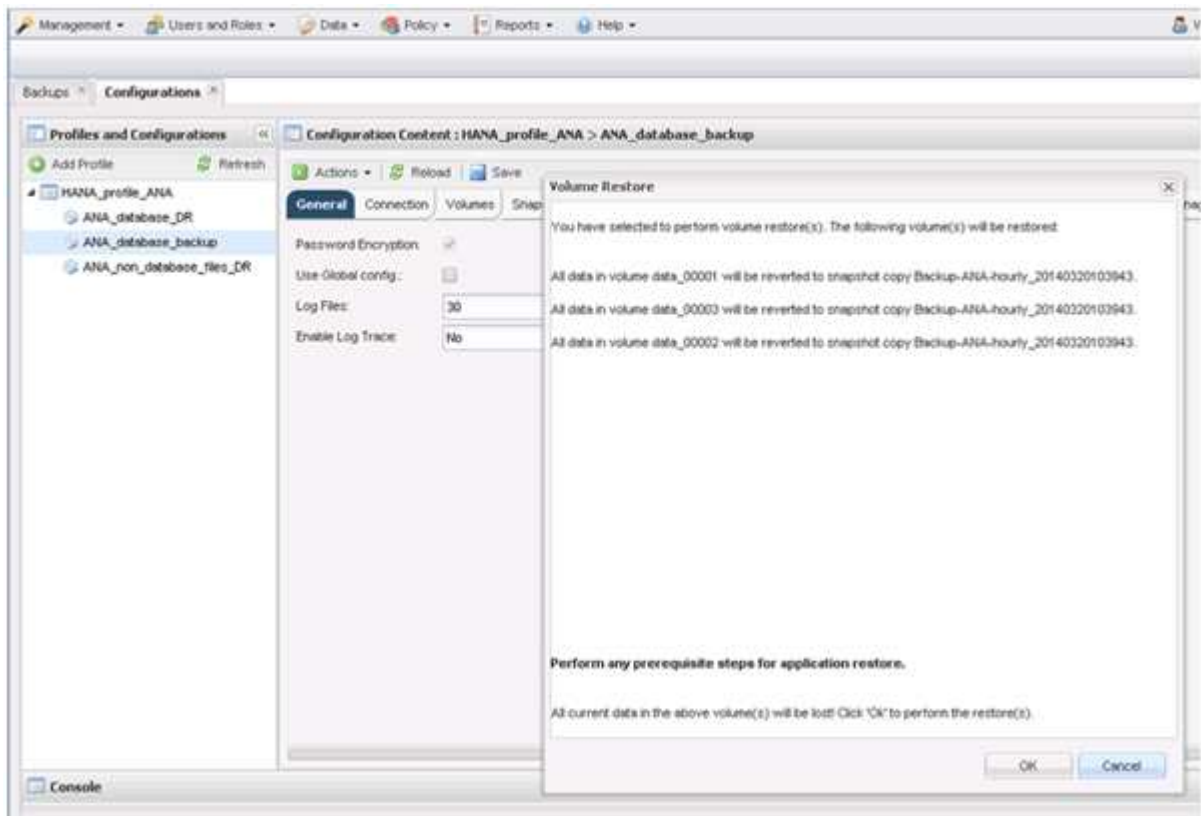


13. Wählen Sie den Storage Controller, den zusätzlichen Volume-Namen und den Namen des Snapshot aus.

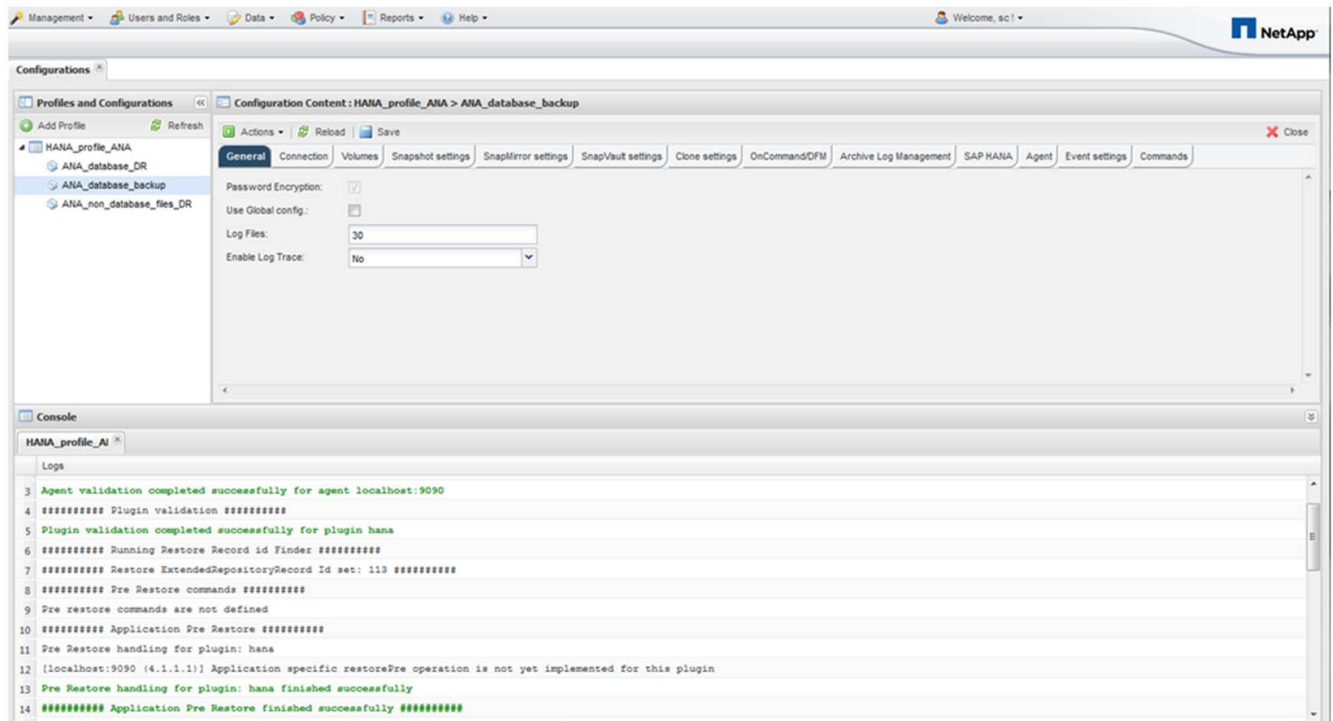
Der Snapshot-Name steht im Zusammenhang mit der Backup-ID, die im SAP HANA Studio ausgewählt wurde.



14. Wiederholen Sie die Schritte 10 bis 13, bis alle erforderlichen Volumes hinzugefügt werden; in unserem Beispiel müssen Data\_00001, Data\_00002 und Data\_00003 für den Wiederherstellungsprozess ausgewählt werden.
15. Wenn alle Volumes ausgewählt sind, klicken Sie auf **OK**, um den Wiederherstellungsprozess zu starten.



Die Wiederherstellung wird gestartet.



Warten Sie, bis der Wiederherstellungsprozess abgeschlossen ist.

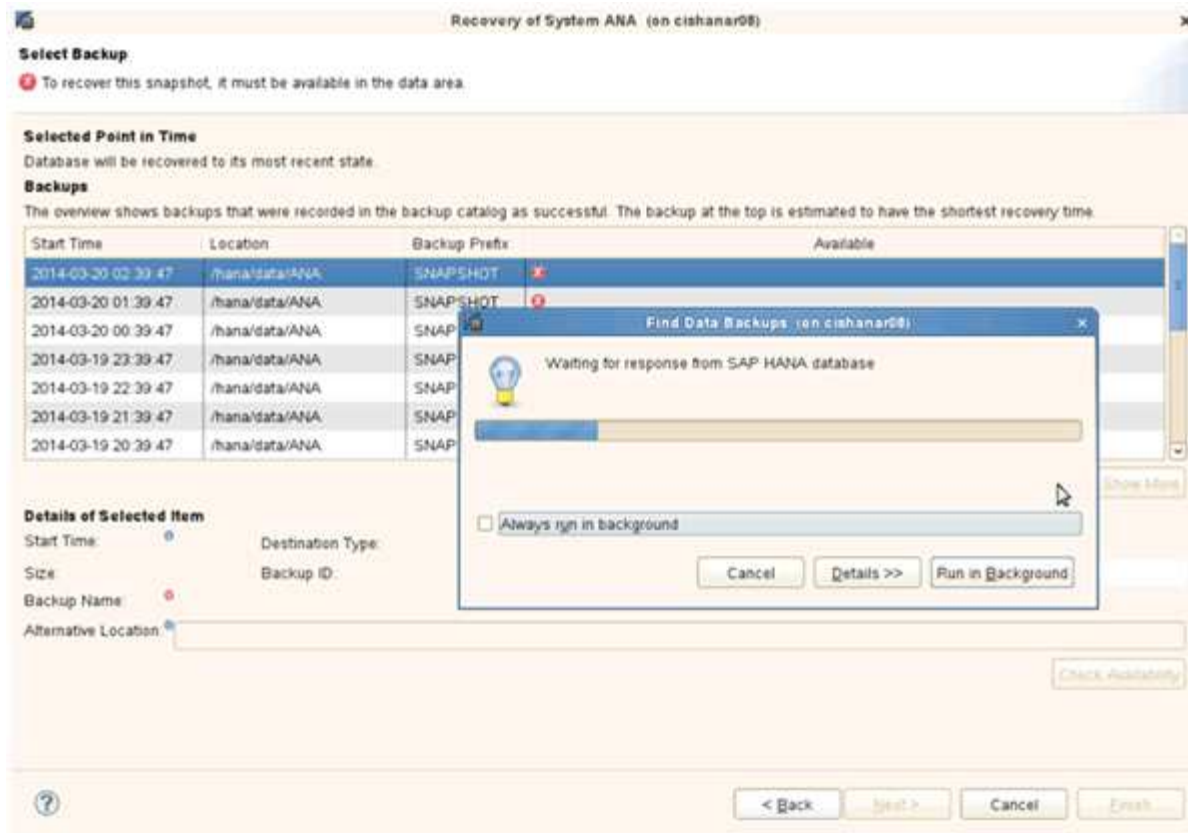
16. Mounten Sie auf jedem Datenbank-Node alle Datenvolumes neu, um veraltete NFS-Handles zu reinigen.

In dem Beispiel müssen alle drei Volumes auf jedem Datenbankknoten neu eingebunden werden.

```
mount -o remount /hana/data/ANA/mnt00001
mount -o remount /hana/data/ANA/mnt00002
mount -o remount /hana/data/ANA/mnt00003
```

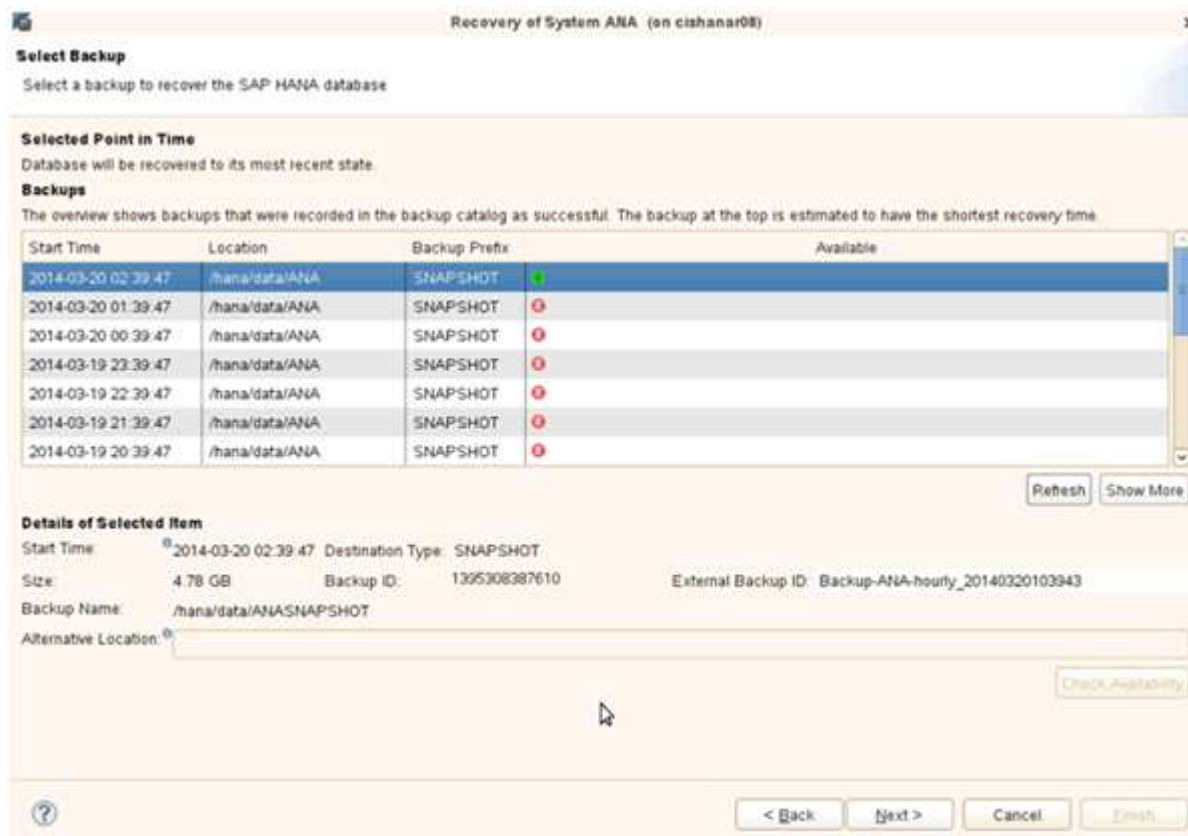
17. Gehen Sie zu SAP HANA Studio und klicken Sie auf **Aktualisieren**, um die Liste der verfügbaren Backups zu aktualisieren.





Das mit Snap Creator wiederhergestellte Backup wird durch ein grünes Symbol in der Liste der Backups angezeigt.

18. Wählen Sie das Backup aus und klicken Sie auf **Weiter**.



19. Wählen Sie weitere Einstellungen nach Bedarf aus und klicken Sie auf **Weiter**.

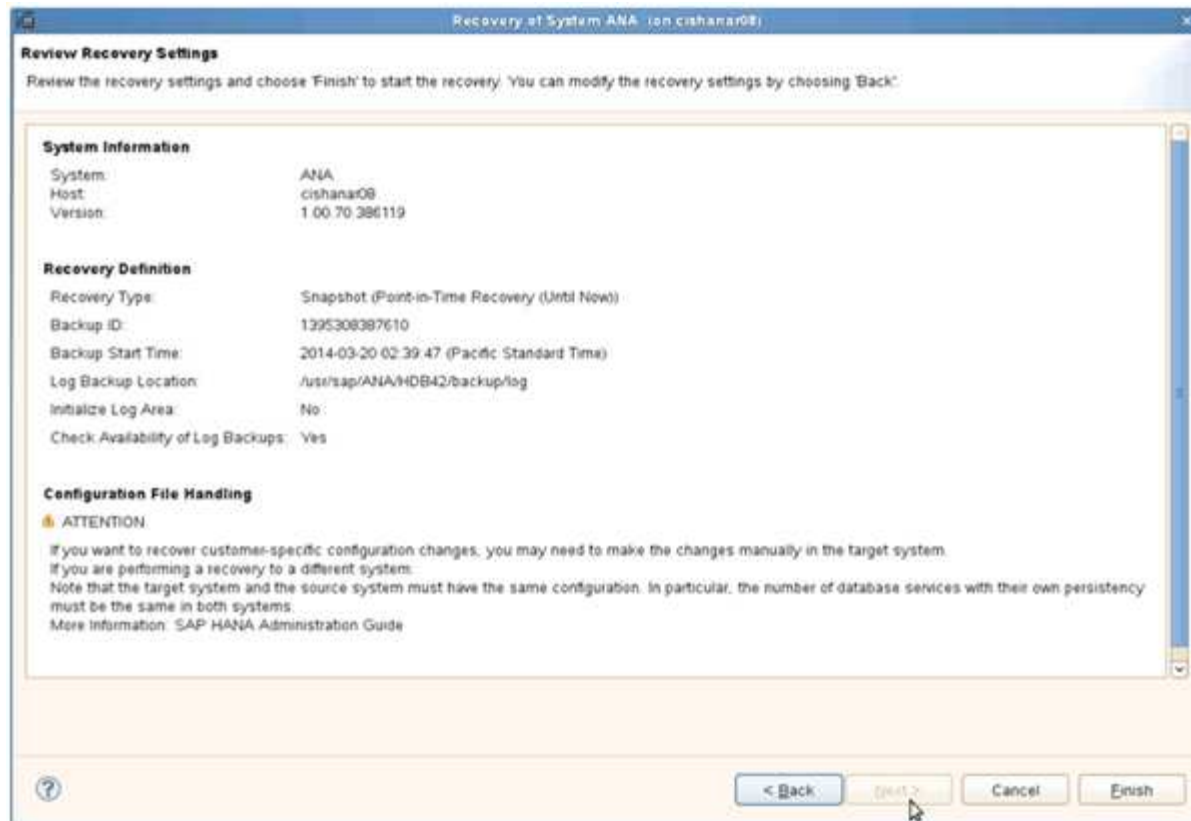
The screenshot shows a window titled "Recovery of System ANA: (sn.cishanar08)". The "Other Settings" tab is active, with the instruction "Ensure that the snapshot is available in the SAP HANA system." Below this, there are three sections:

- Check Availability of Log Backups:** A text block explaining that the system can check for log backups at the start of recovery. Below this, there are two checkboxes: ☒ "File System" and ☐ "Third-Party Backup Tool (Backupint)".
- Initialize Log Area:** A text block explaining that if log entries are not recovered, they will be deleted. Below this is a checkbox: ☐ "Initialize Log Area".
- Install New License Key:** A text block explaining that the old license key is no longer valid. Below this is a checkbox: ☐ "Install New License Key". If selected, there would be a text field and a "Browse" button.

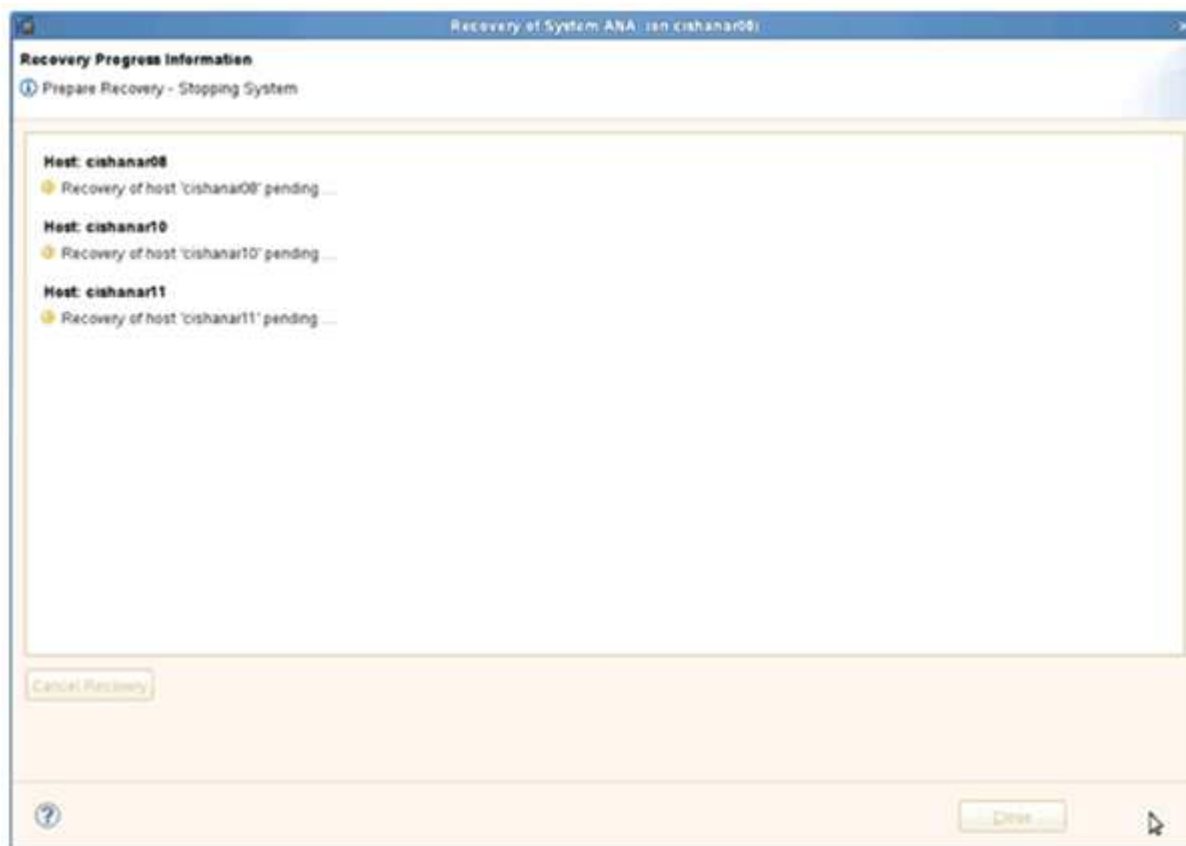
At the bottom right, there are four buttons: "< Back", "Next >", "Cancel", and "Finish". A mouse cursor is pointing at the "Next >" button.

20. Klicken Sie Auf **Fertig Stellen**.

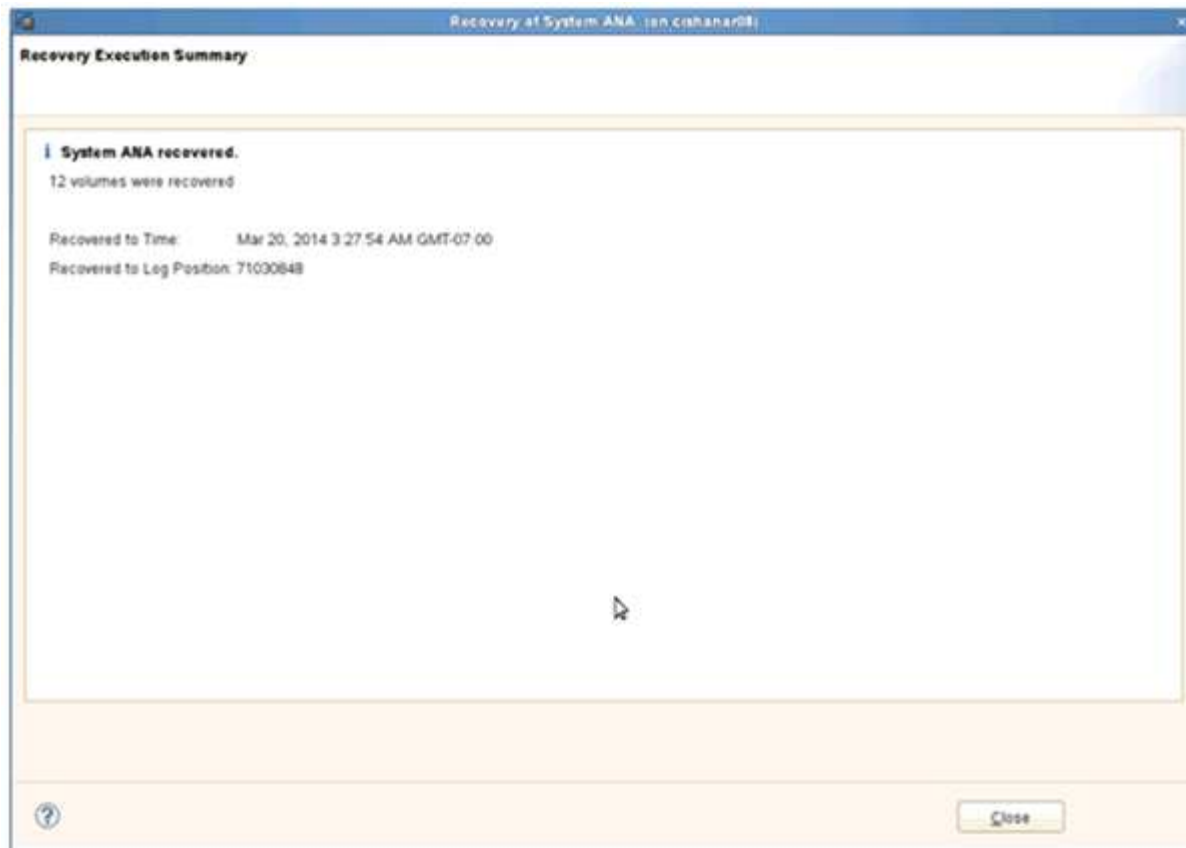




Der Wiederherstellungsprozess beginnt.



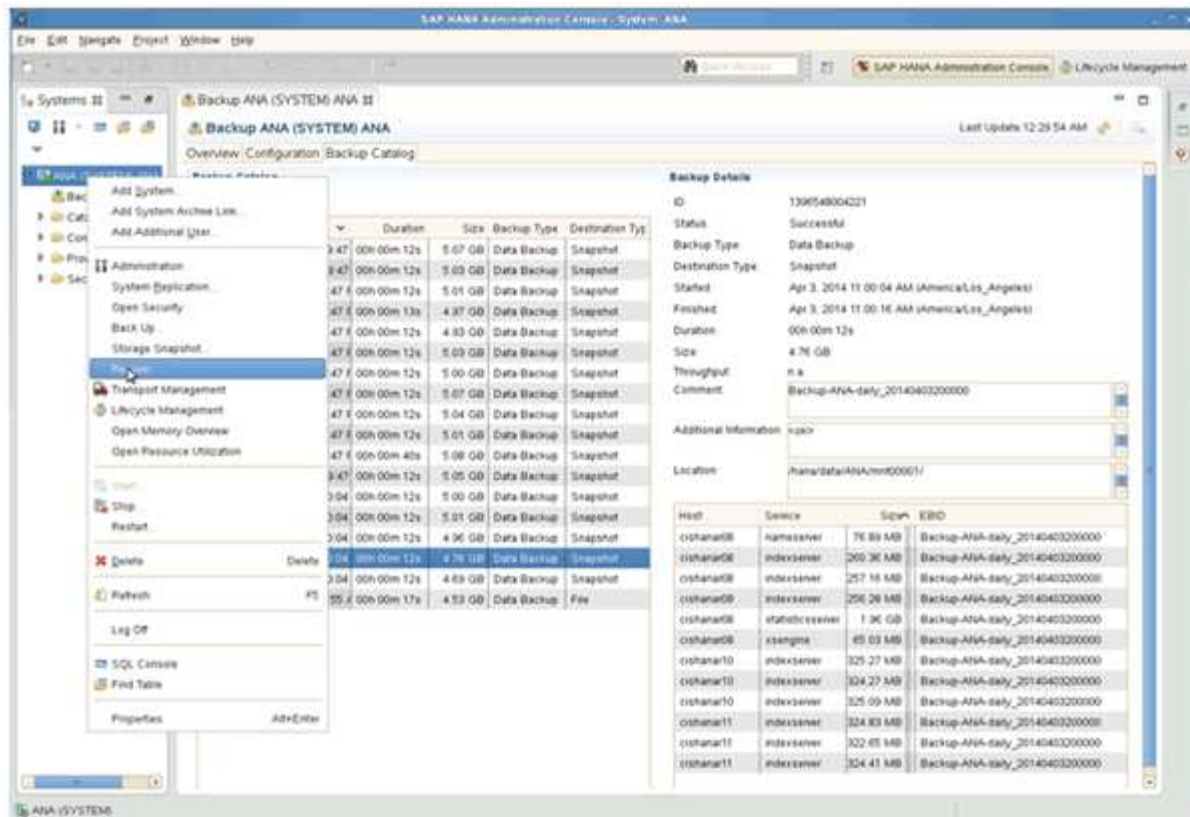
21. Setzen Sie nach Abschluss der Recovery ggf. die SnapVault Beziehungen fort.



## Wiederherstellung von Datenbanken aus sekundärem Storage

Sie können die Datenbank aus dem sekundären Storage wiederherstellen.

1. Wählen Sie in SAP HANA Studio **Recover** für das SAP HANA-System aus.



Das SAP HANA-System wird heruntergefahren.

2. Wählen Sie den Wiederherstellungstyp aus und klicken Sie auf **Weiter**.

Recovery of System ANA (on cishanar08)

### Specify Recovery Type

Select a recovery type.

☒ Recover the database to its most recent state<sup>?</sup>

☐ Recover the database to the following point in time<sup>?</sup>

Date: 2014-04-07 Time: 00:44:22

Select Time Zone: (GMT-07:00) Pacific Daylight Time

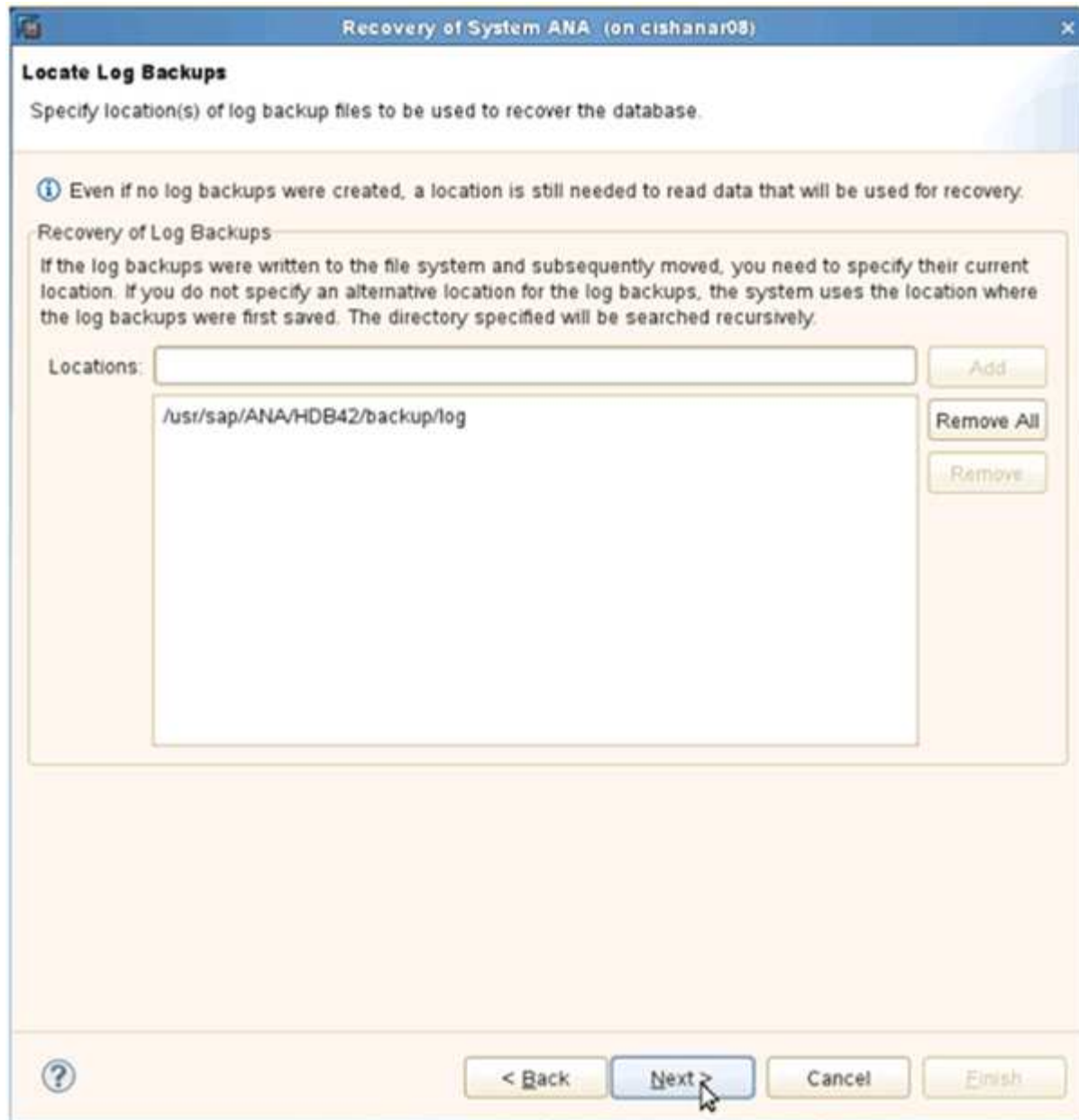
System time used (GMT): 2014-04-07 07:44:22

☐ Recover Database to a Specific Data Backup<sup>?</sup>

Advanced >>

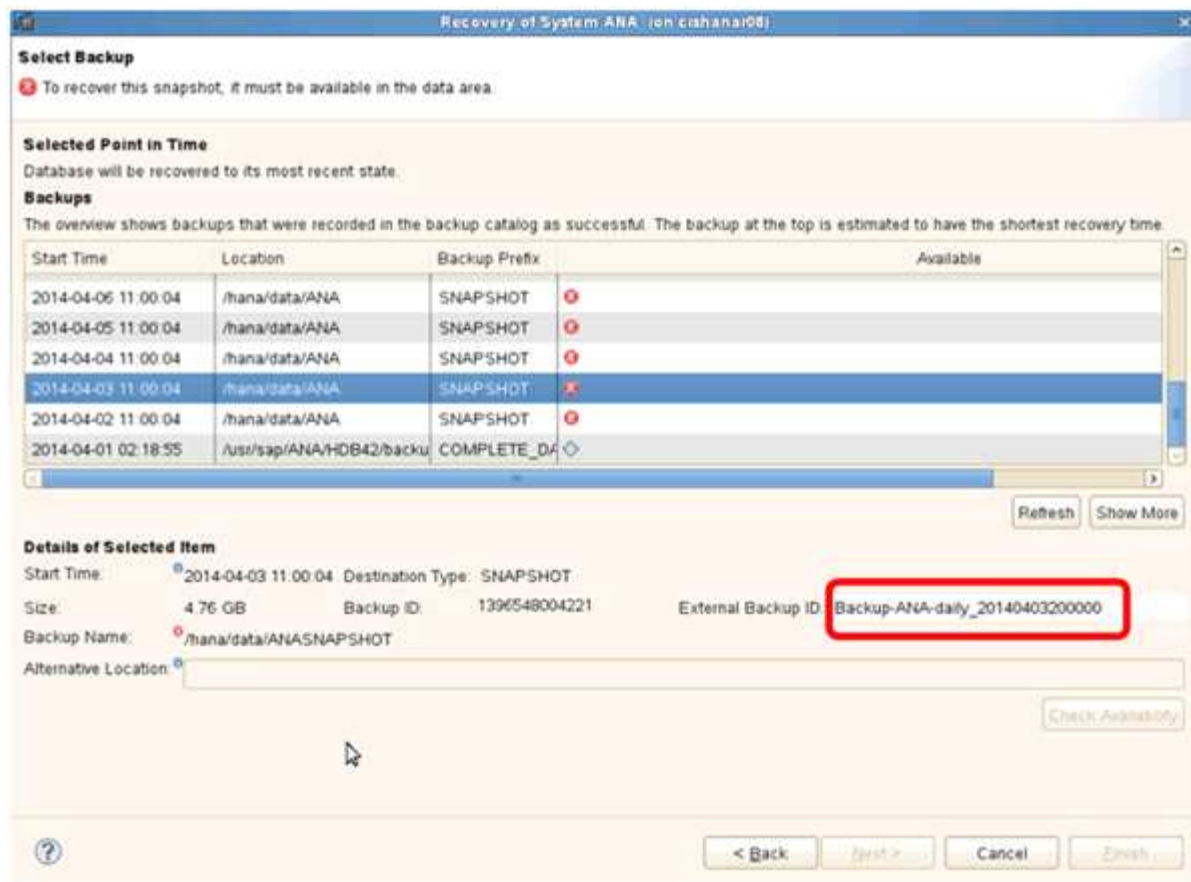
? < Back Next > Cancel Finish

3. Geben Sie Log-Backup-Speicherorte an und klicken Sie auf **Next**.



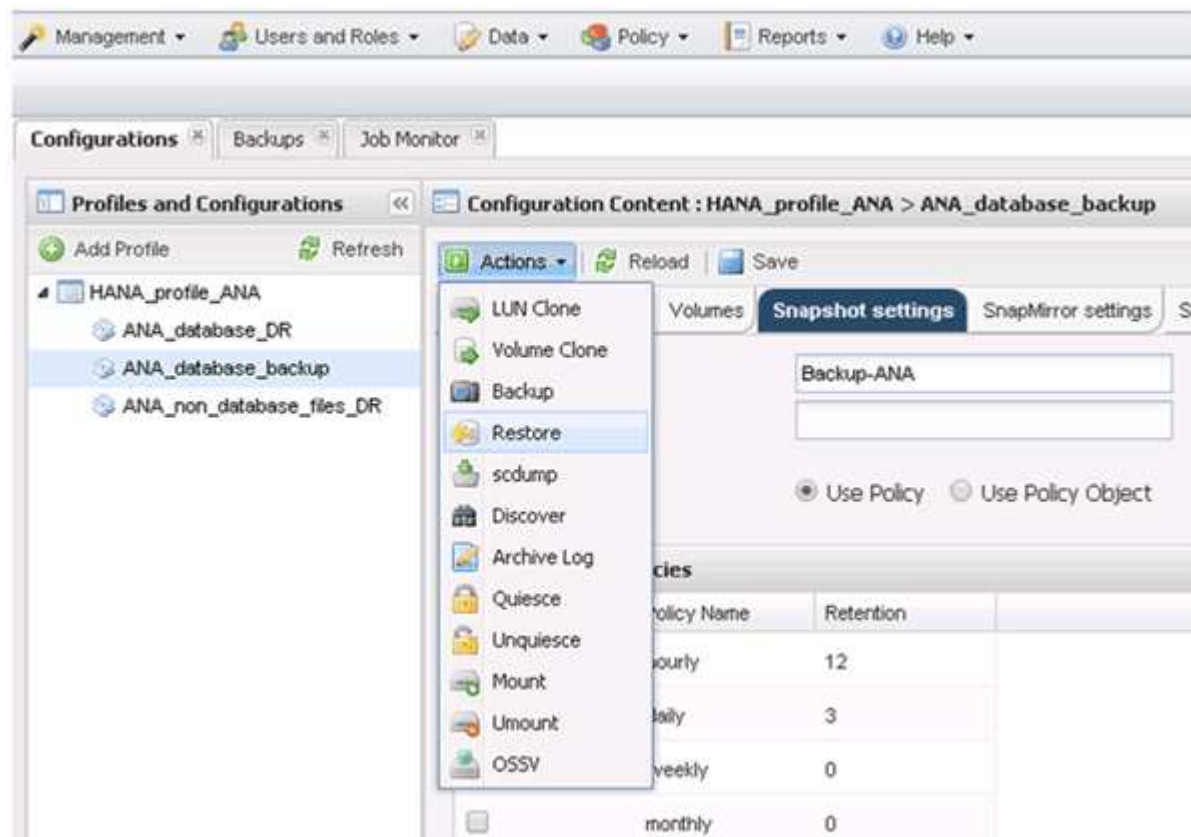
Die Liste der verfügbaren Backups wird basierend auf dem Inhalt des Backup-Katalogs angezeigt.

4. Wählen Sie die erforderliche Sicherung und notieren Sie sich die externe Backup-ID.

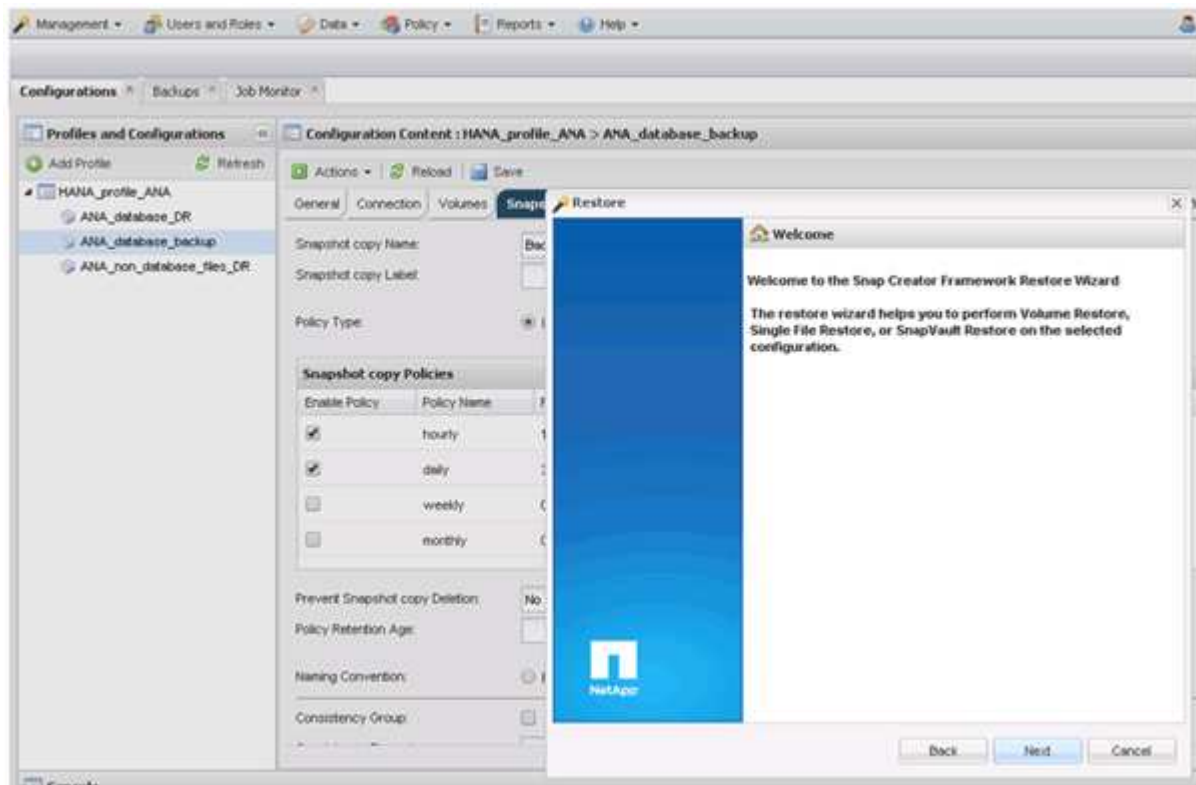


5. Wechseln Sie zur Snap Creator GUI.

6. Wählen Sie das SAP HANA-System aus und klicken Sie dann auf **Aktionen** > **Wiederherstellen**.

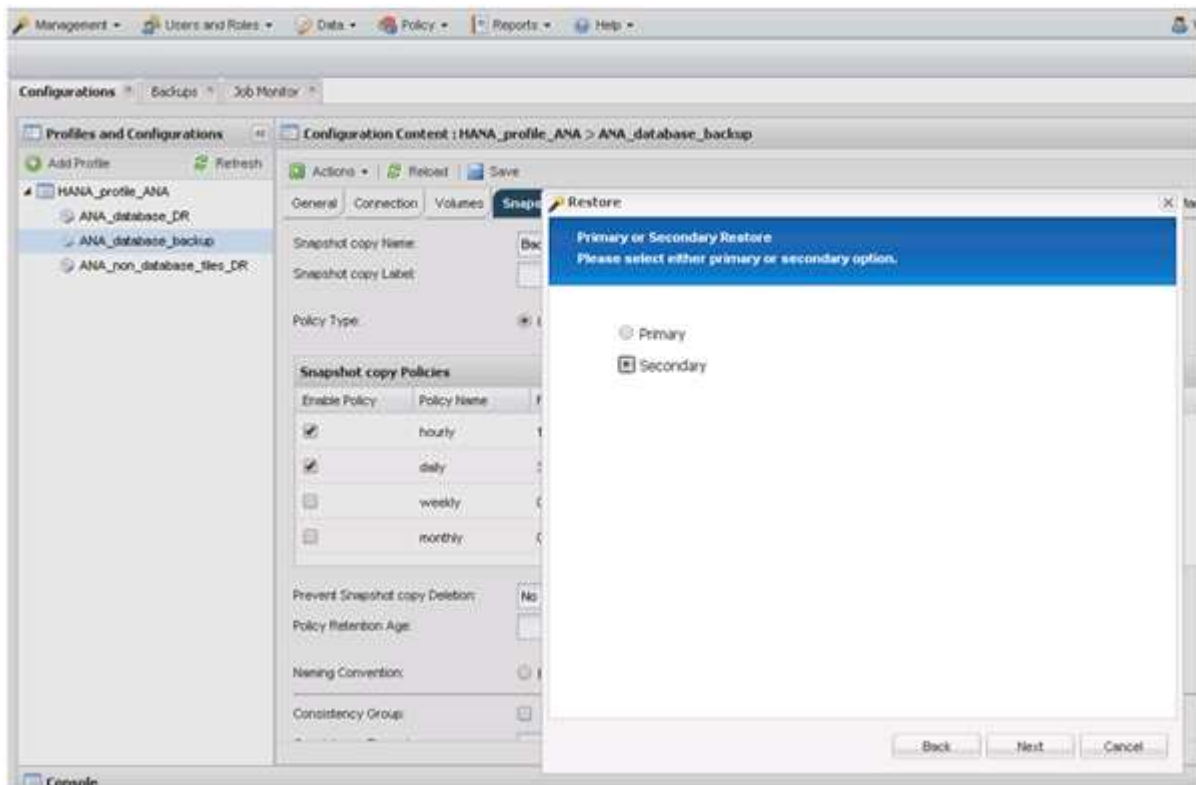


Der Begrüßungsbildschirm wird angezeigt.



7. Klicken Sie Auf **Weiter**.

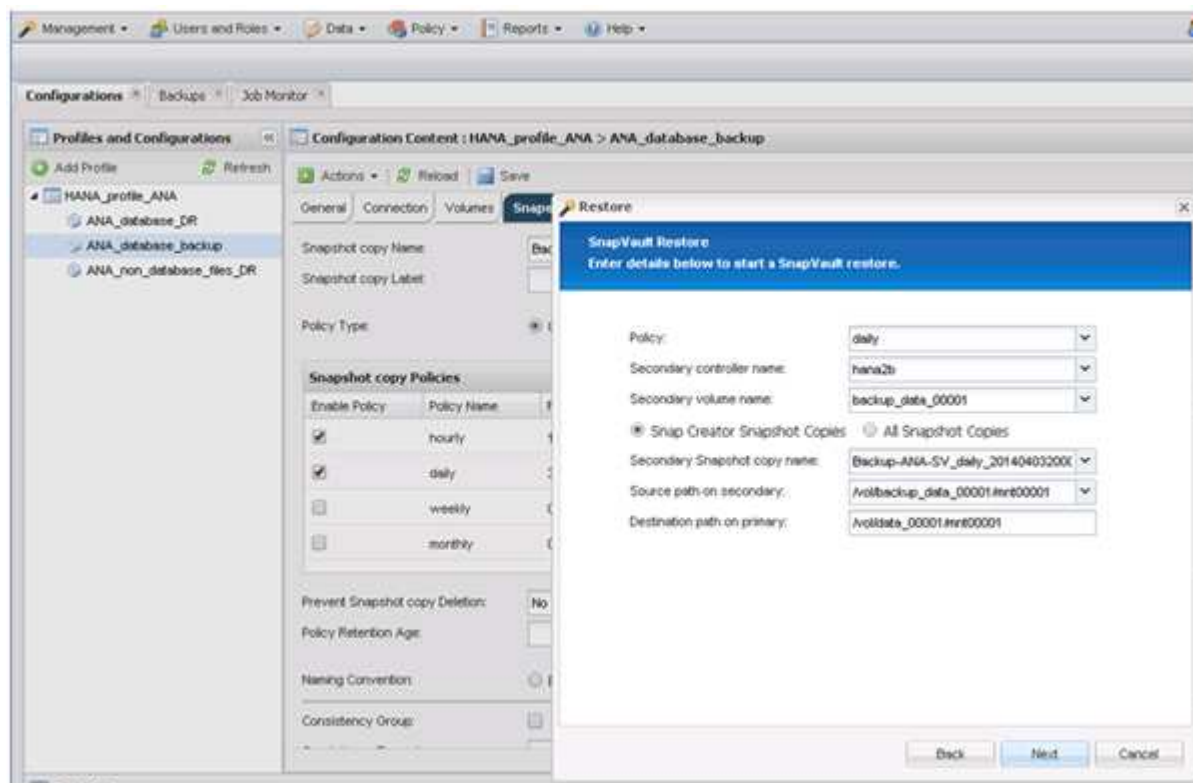
8. Wählen Sie **Sekundär** und klicken Sie auf **Weiter**.



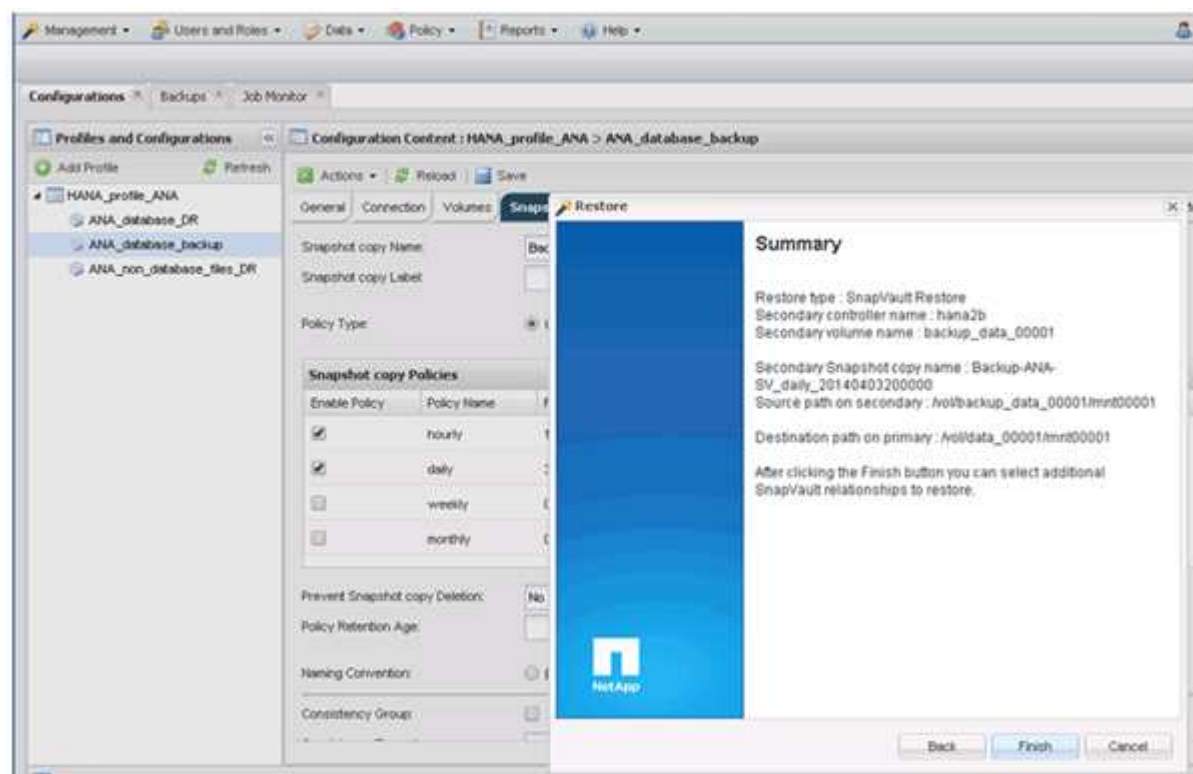
9. Geben Sie die erforderlichen Informationen ein. Der Snapshot-Name steht im Zusammenhang mit der



Backup-ID, die in SAP HANA Studio ausgewählt wurde.

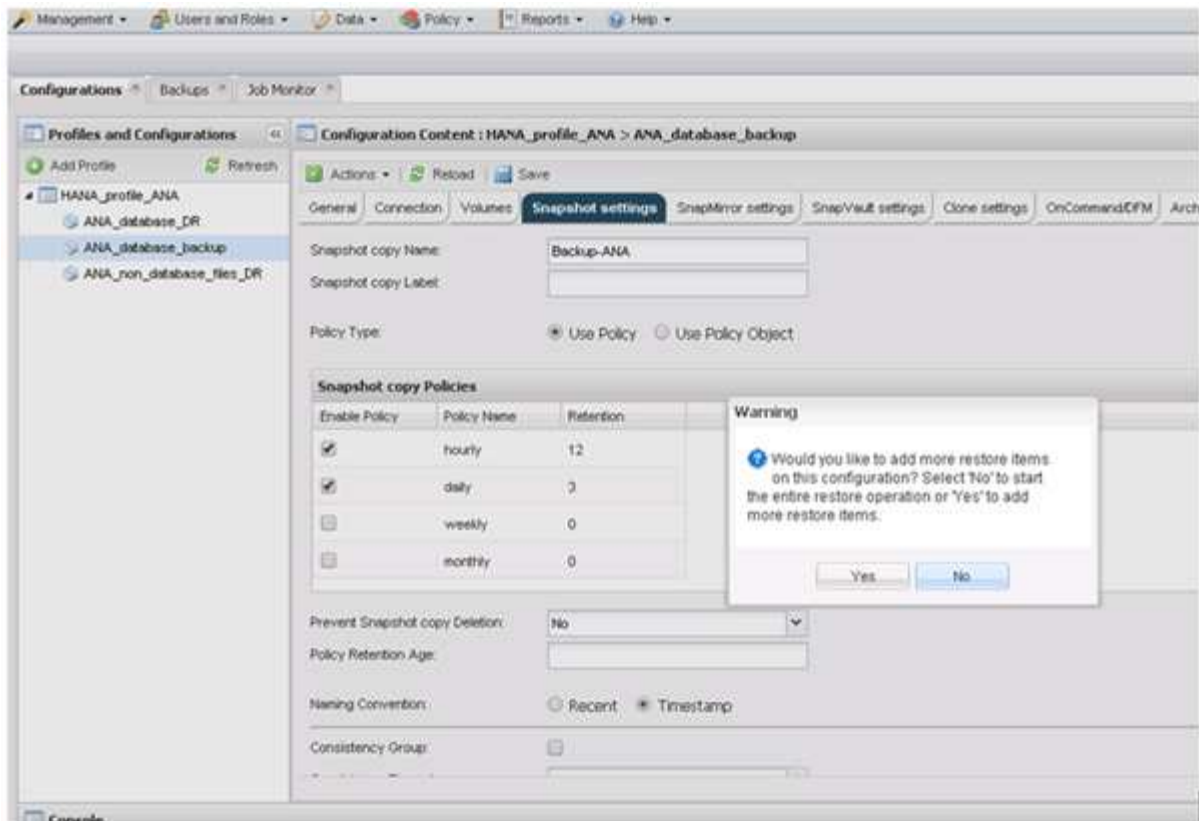


10. Wählen Sie **Fertig**.

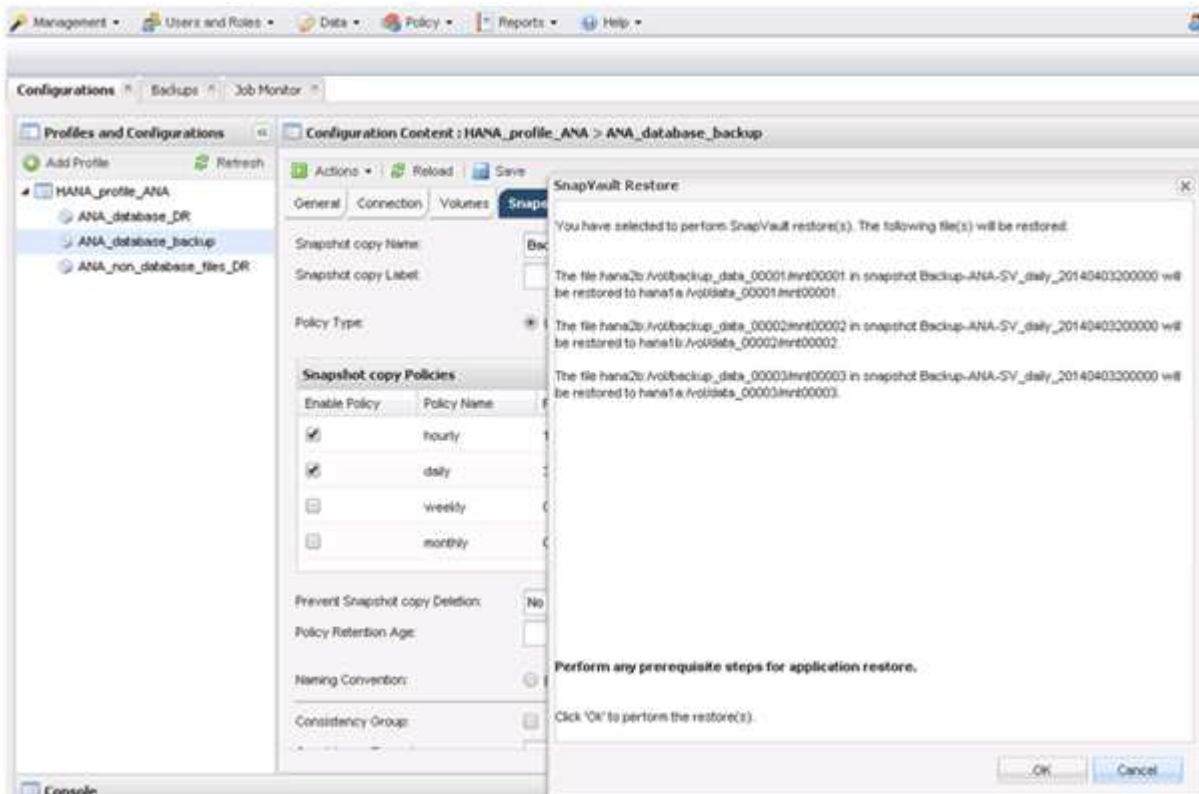


11. Klicken Sie auf **Ja**, um weitere Elemente zur Wiederherstellung hinzuzufügen.





12. Geben Sie die erforderlichen Informationen für alle Volumes an, die wiederhergestellt werden müssen. Im Setup Data\_00001 müssen Data\_00002 und Data\_00003 für den Wiederherstellungsprozess ausgewählt werden.



13. Wenn alle Volumes ausgewählt sind, wählen Sie **OK** aus, um den Wiederherstellungsprozess zu starten.

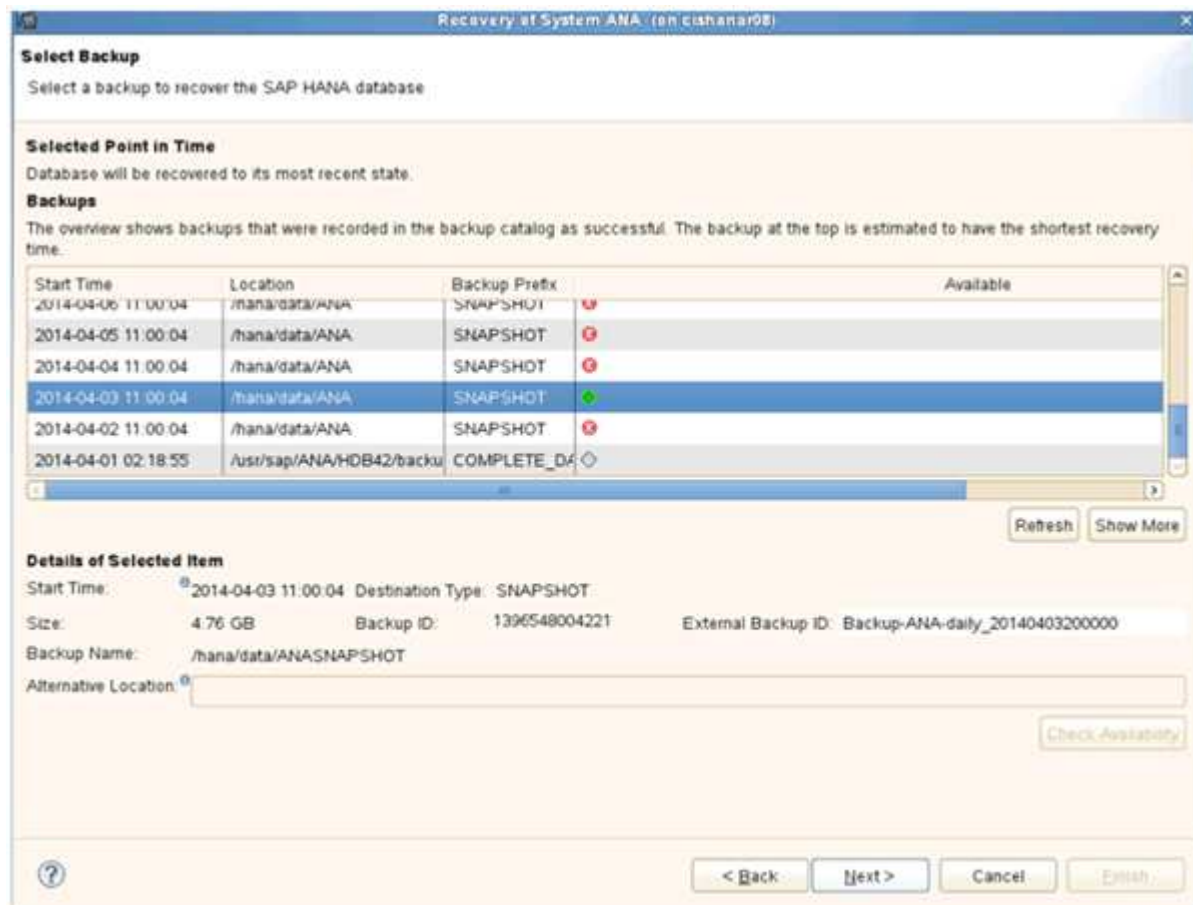
Warten Sie, bis der Wiederherstellungsprozess abgeschlossen ist.

14. Mounten Sie auf jedem Datenbank-Node alle Daten-Volumes neu und „Stale NFS Handles“.

In dem Beispiel müssen alle drei Volumes auf jedem Datenbankknoten neu eingebunden werden.

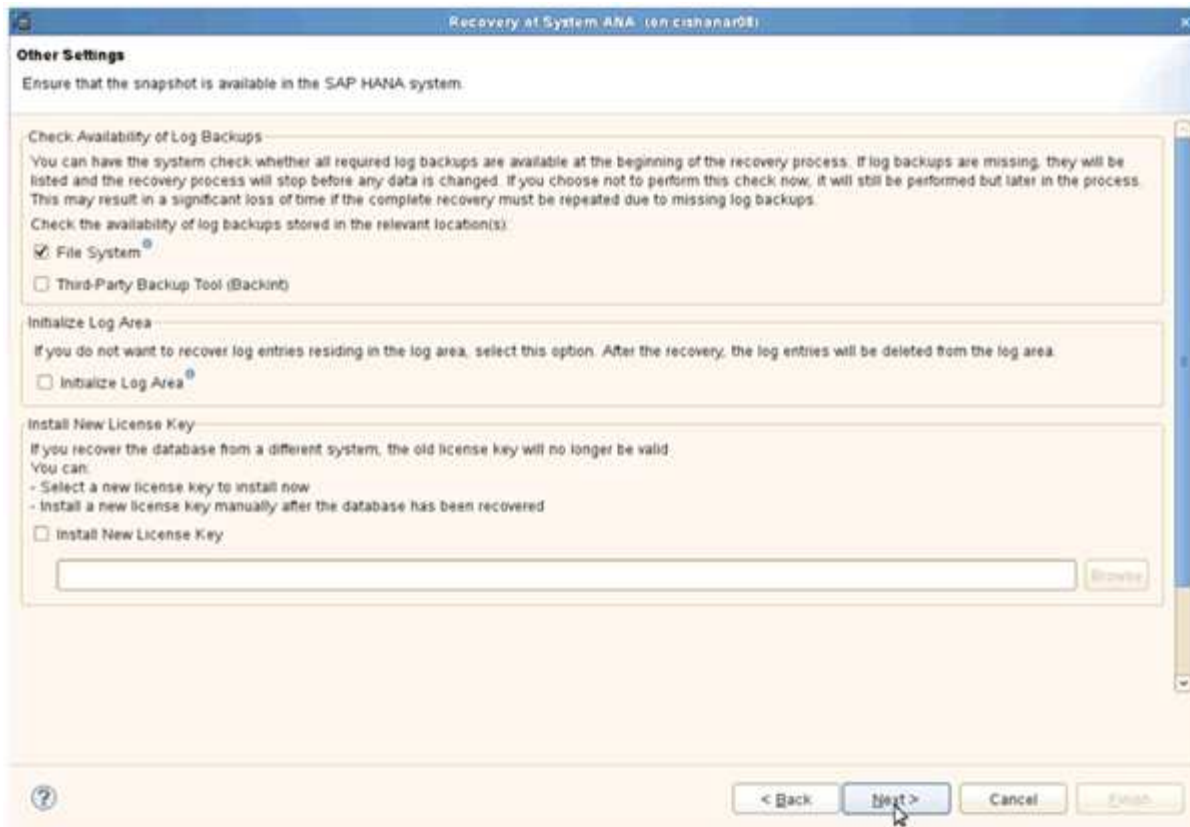
```
mount -o remount /hana/data/ANA/mnt00001
mount -o remount /hana/data/ANA/mnt00002
mount -o remount /hana/data/ANA/mnt00003
```

15. Gehen Sie zu SAP HANA Studio und klicken Sie auf **Aktualisieren**, um die Sicherungsliste zu aktualisieren.

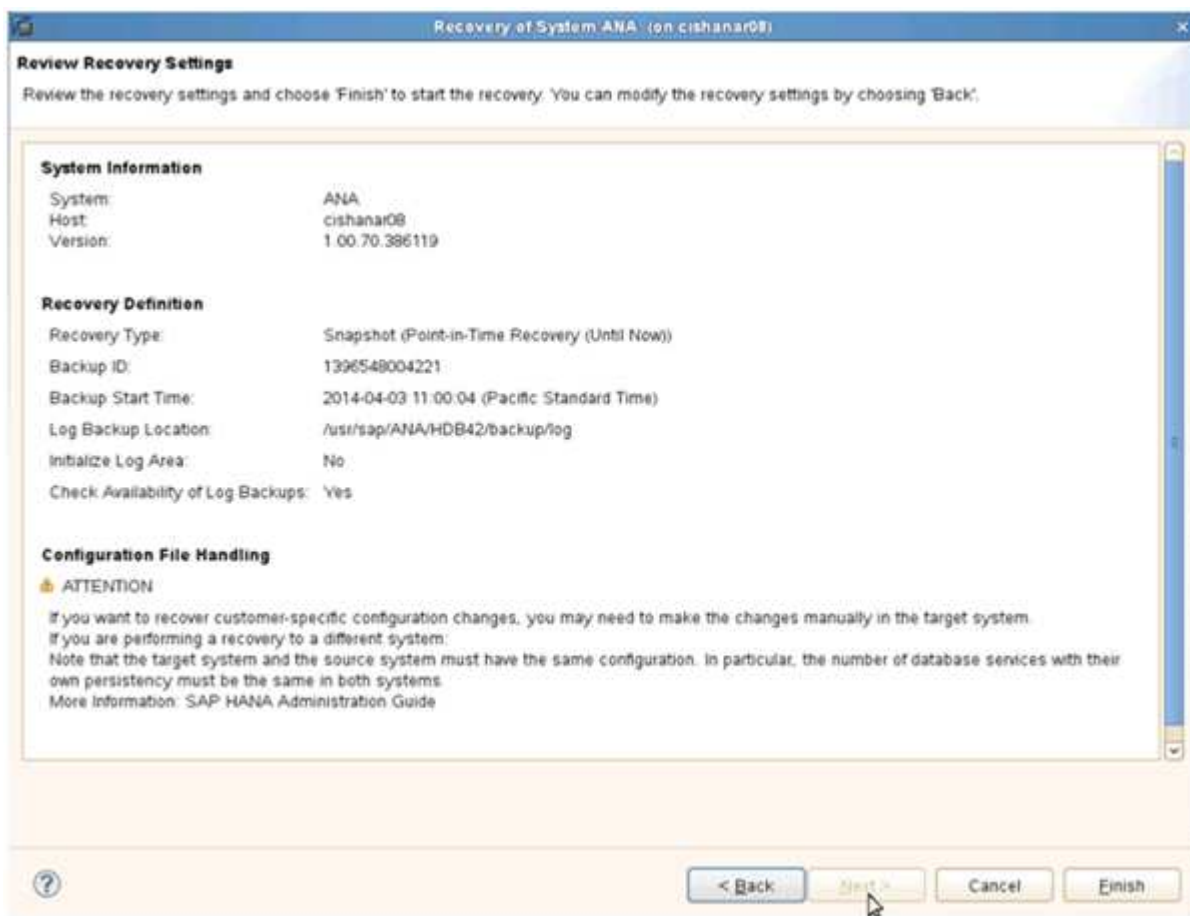


16. Das mit Snap Creator wiederhergestellte Backup wird durch ein grünes Symbol in der Liste der Backups angezeigt. Wählen Sie das Backup aus und klicken Sie auf **Weiter**.

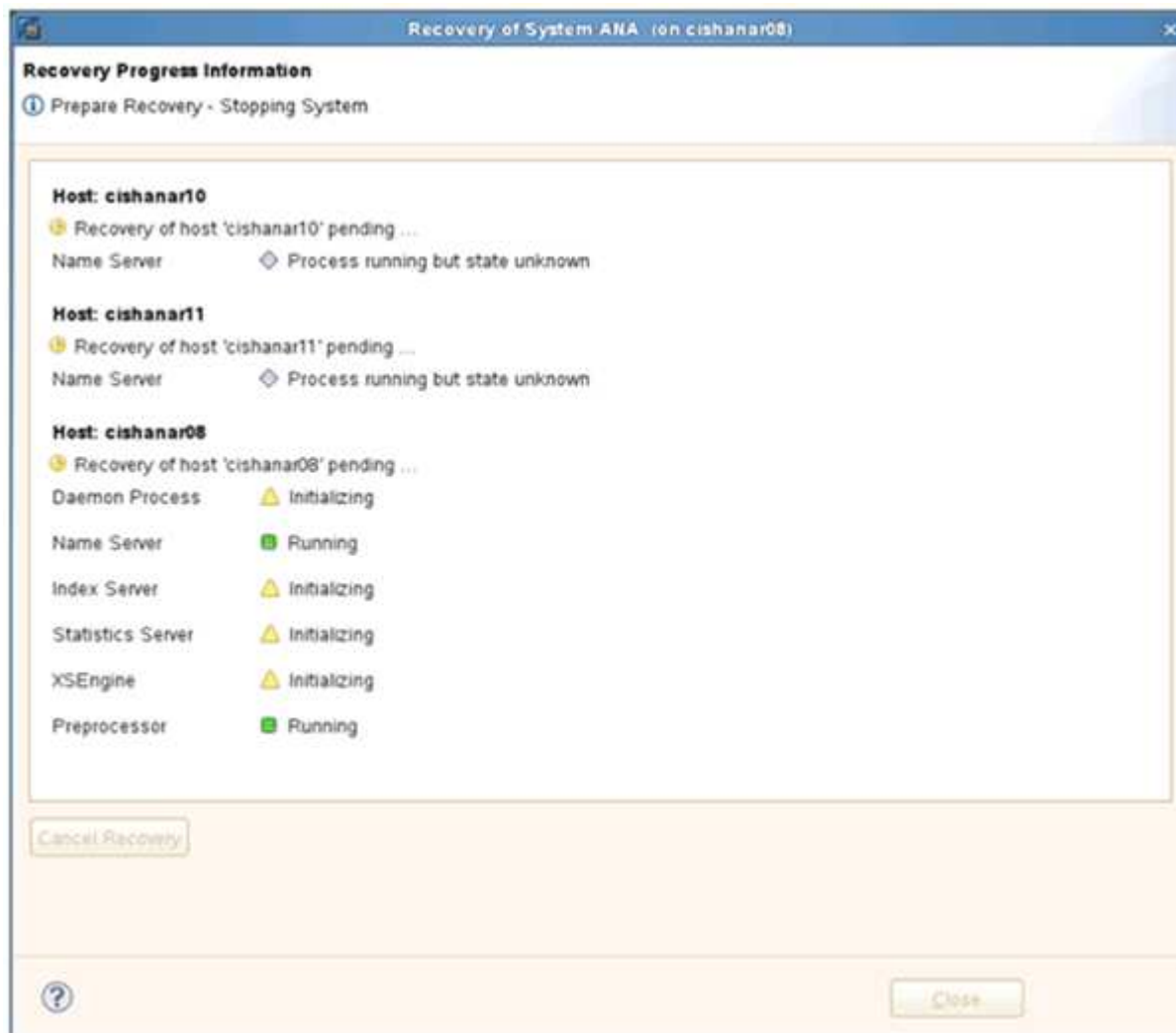
17. Wählen Sie weitere Einstellungen nach Bedarf aus und klicken Sie auf **Weiter**.



18. Klicken Sie Auf **Fertig Stellen**.



Der Wiederherstellungsprozess beginnt.



19. Setzen Sie nach Abschluss des Recovery-Prozesses ggf. die SnapVault Beziehungen fort.



## Wiederaufnahme einer SnapVault Beziehung nach einer Wiederherstellung

Jede Wiederherstellung, die nicht mit dem neuesten Snapshot Backup durchgeführt wird, löscht die SnapVault-Beziehung auf den primären Storage-Systemen.

Nach Abschluss des Restore- und Recovery-Prozesses muss die SnapVault-Beziehung wieder aufgenommen werden, damit Backups mit Snap Creator wieder ausgeführt werden können. Anderenfalls wird Snap Creator eine Fehlermeldung ausgeben, da die SnapVault-Beziehung nicht mehr auf den primären Storage-Systemen gefunden werden kann.

Der gewünschte Datentransfer basiert auf einem Delta-Transfer, falls zwischen dem Quell-Volume und dem Ziel-Volume weiterhin eine allgemeine Snapshot Kopie vorhanden ist.

### Wiederaufnahme einer SnapVault Beziehung mit Data ONTAP in 7-Mode

Wenn Sie eine Wiederherstellung mithilfe eines anderen Snapshot Backups als dem aktuellsten durchführen, müssen Sie die SnapVault Beziehung fortsetzen, damit Snap Creator weiterhin Backups ausführen kann.

1. Setzen Sie die SnapVault Beziehung mit Data ONTAP in 7-Mode fort, indem Sie den folgenden Befehl eingeben. SnapVault Start -r -S source\_Controller:Source\_Volumebackup\_Controller:Backup\_Volume

Führen Sie diesen Schritt für alle Volumes der SAP HANA Datenbank durch.

```
hana2b> snapvault start -r -S hanala:/vol/data_00001/mnt00001
hana2b:/vol/backup_data_00001/mnt00001
The resync base snapshot will be: Backup-ANA-SV_daily_20140406200000
Resync may alter the data in this qtree.
Are you sure you want to resync the qtree? y
Mon Apr 7 14:08:21 CEST [hana2b:replication.dst.resync.success:notice]:
SnapVault resync of
/vol/backup_data_00001/mnt00001 to hanala:/vol/data_00001/mnt00001 was
successful.
Transfer started.
Monitor progress with 'snapvault status' or the snapmirror log.
```

```
hana2b> snapvault start -r -S hana1b:/vol/data_00002/mnt00002
hana2b:/vol/backup_data_00002/mnt00002
The resync base snapshot will be: Backup-ANA-SV_daily_20140406200000
Resync may alter the data in this qtree.
Are you sure you want to resync the qtree? y
Mon Apr 7 14:09:49 CEST [hana2b:replication.dst.resync.success:notice]:
SnapVault resync of
/vol/backup_data_00002/mnt00002 to hana1b:/vol/data_00002/mnt00002 was
successful.
Transfer started.
Monitor progress with 'snapvault status' or the snapmirror log.
```

```

hana2b> snapvault start -r -S hana1a:/vol/data_00003/mnt00003
hana2b:/vol/backup_data_00003/mnt00003
The resync base snapshot will be: Backup-ANA-SV_daily_20140406200000
Resync may alter the data in this qtree.
Are you sure you want to resync the qtree? y
Mon Apr  7 14:10:25 CEST [hana2b:replication.dst.resync.success:notice]:
SnapVault resync of
/vol/backup_data_00003/mnt00003 to hana1a:/vol/data_00003/mnt00003 was
successful.
Transfer started.
Monitor progress with 'snapvault status' or the snapmirror log.

```

Nach Abschluss des Datentransfers können Sie die Backups mit Snap Creator erneut planen.

### Wiederaufnahme einer SnapVault Beziehung mit Clustered Data ONTAP

Wenn Sie eine Wiederherstellung mithilfe eines anderen Snapshot Backups als dem aktuellsten durchführen, müssen Sie die SnapVault Beziehung fortsetzen, damit Snap Creator weiterhin Backups ausführen kann.

1. SnapVault-Beziehung erneut erstellen und neu synchronisieren.

```

hana::> snapmirror create -source-path hana1a:hana_data -destination
-path
hana2b:backup_hana_data -type XDP
Operation succeeded: snapmirror create the relationship with destination
hana2b:backup_hana_data.

hana::> snapmirror resync -destination-path hana2b:backup_hana_data
-type XDP

Warning: All data newer than Snapshot copy sc-backup-
daily_20140430121000 on volume
hana2b:backup_hana_data will be deleted.
Do you want to continue? {y|n}: y
[Job 6554] Job is queued: initiate snapmirror resync to destination
"hana2b:backup_hana_data".
[Job 6554] Job succeeded: SnapMirror Resync Transfer Queued

```

2. Um den SnapVault Transfer neu zu starten, ist eine manuelle Snapshot Kopie erforderlich.

```
hana::> snapshot create -vserver hanala -volume hana_data -snapshot
sv_resync

hana::> snapshot modify -vserver hanala -volume hana_data -snapshot
sv_resync -snapmirror-label daily

hana::> snapmirror update -destination-path hana2b:backup_hana_data
Operation is queued: snapmirror update of destination
hana2b:backup_hana_data.
```

3. Vergewissern Sie sich, dass die SnapVault-Beziehung in der Zielliste angezeigt wird.

```
hana::> snapmirror list-destinations -source-path hanala:hana_data
Progress
Source          Destination      Transfer  Last
Relationship
Path            Type  Path            Status Progress  Updated      Id
-----
-----
hanala:hana_data
          XDP  hana2b:backup_hana_data
                        Transferring
                        38.46KB   04/30 18:15:54
                        9137fb83-
cba9-11e3-85d7-123478563412
```

## Wiederherstellung von Datenbanken nach Ausfall des primären Storage

Nach einem Ausfall des Primär-Storage oder dem Löschen aller Snapshot Kopien aus den Volumes im primären Storage ist Snap Creator nicht in der Lage, die Wiederherstellung zu verarbeiten, da es keine SnapVault-Beziehung mehr auf den primären Storage-Systemen gibt.

### Wiederherstellung von Datenbanken nach einem Ausfall des primären Storage bei Data ONTAP im 7-Mode

Nach dem Ausfall eines primären Storage-Systems mit Data ONTAP 7-Mode lassen sich SAP HANA Datenbanken wiederherstellen.

1. In diesem Fall muss die Wiederherstellung direkt auf dem sekundären Storage-System mit dem folgenden Befehl ausgeführt werden: SnapVault restore --s Snapshot\_Name -S Backup\_Controller:Backup\_volumesource\_Controller:source\_Volume

Führen Sie diesen Schritt für alle Volumes der SAP HANA Datenbank durch.

```
hanala> snapvault restore -s Backup-ANA-SV_hourly_20140410103943 -S
hana2b:/vol/backup_data_00001/mnt00001 hanala:/vol/data_00001/mnt00001
Restore will overwrite existing data in /vol/data_00001/mnt00001.
Are you sure you want to continue? y
Thu Apr 10 11:55:55 CEST [hanala:vdisk.qtreePreserveComplete:info]:
Qtree preserve is complete for /vol/data_00001/mnt00001.
Transfer started.
Monitor progress with 'snapvault status' or the snapmirror log.
```

```
hanala> snapvault restore -s Backup-ANA-SV_hourly_20140410103943 -S
hana2b:/vol/backup_data_00003/mnt00003 hanala:/vol/data_00003/mnt00003
Restore will overwrite existing data in /vol/data_00003/mnt00003.
Are you sure you want to continue? y
Thu Apr 10 11:58:18 CEST [hanala:vdisk.qtreePreserveComplete:info]:
Qtree preserve is complete for /vol/data_00003/mnt00003.
Transfer started.
Monitor progress with 'snapvault status' or the snapmirror log.
```

```
hanalb> snapvault restore -s Backup-ANA-SV_hourly_20140410103943 -S
hana2b:/vol/backup_data_00002/mnt00002 hanalb:/vol/data_00002/mnt00002
Restore will overwrite existing data in /vol/data_00002/mnt00002.
Are you sure you want to continue? y
Thu Apr 10 12:01:29 CEST [hanalb:vdisk.qtreePreserveComplete:info]:
Qtree preserve is complete for /vol/data_00002/mnt00002.
Transfer started.
Monitor progress with 'snapvault status' or the snapmirror log.
```

Nach Abschluss des Wiederherstellungsprozesses wird die Recovery mit SAP HANA durchgeführt.

## **Wiederherstellung von Datenbanken nach einem Ausfall des primären Storage mit Clustered Data ONTAP**

Nach dem Ausfall eines primären Storage-Systems mit Clustered Data ONTAP können Sie eine SAP HANA Datenbank wiederherstellen.

Wenn das primäre Volume komplett verloren geht, müssen Sie ein neues primäres Volume erstellen und dann vom Backup Volume wiederherstellen.

1. Erstellung eines primären Volumes mit type-Datensicherung



```
hana::> volume create -vserver hanala -volume hana_data -aggregate
aggr_sas_101 -size 300G -state online -type DP -policy default -autosize
-mode grow_shrink -space-guarantee none
-snapshot-policy none -foreground true
[Job 6744] Job is queued: Create hana_data.
[Job 6744] Job succeeded: Successful
```

## 2. Wiederherstellung aller Daten aus dem Backup-Volume

```
hana::> snapmirror restore -destination-path hanala:hana_data -source
-path hana2b:backup_hana_data -source-snapshot sc-backup-
daily_20140505121000
[Job 6746] Job is queued: snapmirror restore from source
"hana2b:backup_hana_data" for the
snapshot sc-backup-daily_20140505121000.

hana::> job show -id 6746
Owning
Job ID Name Vserver Node State
-----
6746 SnapMirror restore hana hana01 Running
Description: snapmirror restore from source
"hana2b:backup_hana_data" for the snapshot sc-backup-
daily_20140505121000
```

Nach Abschluss des Wiederherstellungsprozesses wird die Recovery mit SAP HANA durchgeführt.

## Plug-in-Parameter für SAP HANA

In der folgenden Tabelle sind die SAP HANA Plug-in-Parameter aufgeführt, die Parametereinstellungen angegeben und die Parameter beschrieben.

| Parameter  | Einstellung                   | Beschreibung   |
|------------|-------------------------------|--|
| HANA_SID   | Beispiel: ABC                 | HANA Datenbank-SID   |
| HANA_NODES | Beispiel: Node1, node2, node3 | Kommagetrennte Liste der HANA-Knoten, auf denen die hdbsql-Anweisungen ausgeführt werden können. |

| Parameter               | Einstellung  | Beschreibung   |
|-------------------------|--|--|
| HANA_USER_NAME          | Beispiel Backup-Benutzer   | Benutzername für HANA-Datenbank Die für diesen Benutzer erforderliche Mindestberechtigung ist DIE BACKUP-ADMINISTRATORBERECHTIGUNG.  |
| HANA_PASSWORD           | Beispiel: Hfasfh87r83r   | HANA-Datenbankpasswort.  |
| HANA_INSTANCE           | Beispiel: 42   | HANA-Node-Instanznummer  |
| HANA_HDBSQL_CMD         | Beispiel: /Usr/sap/hdbclient/hdbsql                                    | Pfad zum HANA-Befehl hdbsql. Wenn dieser Parameter nicht eingestellt ist, wird hdbsql auf dem Suchpfad verwendet. Der Standardwert ist hdbsql.   |
| HANA_OSDB_USER          | Beispiel: Benutzer1  | Der Betriebssystem-Benutzer für die Ausführung hdbsql (in der Regel sidadm) muss die hdbsql-Binärdatei im Suchpfad und die Berechtigung, sie auszuführen.  |
| HANA_USERSTORE_KEYS     | Beispiel: Node1:key1, Knoten 2:key2, node3:key3                        | Kommagetrennte Liste der HANA-Benutzerspeicherschlüssel und Knotenpaare, mit denen die hdbsql-Anweisungen ausgeführt werden können.  |
| HANA_FILE_BACKUP_ENABLE | „Y“ oder „N“   | Legt fest, ob Snap Creator ein dateibasiertes Backup für das SAP HANA Plug-in ermöglichen soll. Diese Einstellung ist nützlich, wenn Sie einen dateibasierten SAP HANA Backup-Vorgang ausführen möchten. |
| HANA_FILE_BACKUP_PATH   | Beispiel:/hana/Data/SCN/mnt00001                                       | (Optional) Pfad zum Verzeichnis, in dem die Datenbank-Dateisicherung gespeichert werden kann. Wenn dieser Parameter nicht festgelegt ist, verwenden Sie Standard.  |
| HANA_FILE_BACKUP_PREFIX | BEISPIEL:<br>SNAPCREATOR_<HANA_FILE_BACKUP_PREFIX>_<CURRENT_TIMESTAMP> | (Optional) fügt dem Namen der Sicherungsdatei ein Präfix hinzu. Standard:<br>SnapCreator_<CURRENT_TIMESTAMP>   |

| Parameter                   | Einstellung    | Beschreibung   |
|-----------------------------|----------------|--|
| HANA_INTEGRITY_CHECK_ENABLE | „Y“ oder „N“   | Legt fest, ob Snap Creator die Integritätsprüfung für das SAP HANA Plug-in aktivieren sollte. Diese Einstellung ist üblich, wenn Sie die SAP HANA Integrity Check-Operation ausführen möchten. |
| HANA_TEMP_FILE_BACKUP_PATH  | Beispiel:/Temp | (Optional) Pfad, in dem die temporäre Datenbankdatei für die Integritätsprüfung gespeichert werden kann. Wenn nicht sicher, verwenden Sie die Standardeinstellung.                             |
| HANA_LOG_CLEANUP_ENABLE     | „Y“ oder „N“   | Aktiviert die Bereinigung des Protokollkatalogs.   |

## Fehlerbehebung

Der Abschnitt Fehlerbehebung enthält Informationen zu den Fehlercodes, Fehlermeldungen und enthält die Beschreibung oder Lösung zur Behebung des Problems.

In der folgenden Tabelle sind die Fehlermeldungen des SAP HANA Plug-in aufgeführt.

| Fehlercode | Fehlermeldung   | Beschreibung/Auflösung   |
|------------|---|--|
| hdb-00001  | Es konnte kein zugänglicher HANA-Knoten gefunden werden, um hdbsql-Befehle mit den angegebenen Konfigurationsparametern auszuführen. Überprüfen und aktualisieren Sie die HANA-Einstellungen in der Konfiguration, und versuchen Sie es erneut. | Vergewissern Sie sich, dass HANA-Nodes ausgeführt und erreichbar sind, und die angegebene Instanznummer ist korrekt.   |
| hdb-00002  | Erstellen von Datenbank-Snapshot für [€sid] fehlgeschlagen.   | Überprüfen Sie, ob ein HANA Datenbank-Snapshot bereits in der Datenbank erstellt wurde. Wenn bereits erstellt, löschen Sie den HANA-Datenbank-Snapshot oder führen Sie den Vorgang unquiesce aus. Falls noch nicht erstellt, überprüfen Sie die Protokolle auf andere Fehlermeldungen und Details. |

| Fehlercode | Fehlermeldung   | Beschreibung/Auflösung   |
|------------|---|--|
| hdb-00003  | Löschen des Datenbank-Snapshot für [€dg. sid] fehlgeschlagen.   | Überprüfen, ob ein HANA Datenbank-Snapshot bereits gelöscht wurde. Wenn ja, kann dieser Fehler ignoriert werden. Falls nein, überprüfen Sie die SAP HANA-Plug-in-Parameter und stellen Sie sicher, dass Knoten erreichbar sind und die angegebene Instanznummer korrekt ist. |
| hdb-00004  | Die Verbindung zum [€dg hana_Node]-Node mit Instanz [€dexinstance] ist fehlgeschlagen, da die Verbindung abgelehnt wurde. | Der HANA-Knoten mit der in der Meldung angezeigten Instanz ist nicht erreichbar. Dies kann nur eine Warnung sein, da das Plug-in versucht, hdbsql-Befehle auf anderen Knoten auszuführen. Überprüfen Sie die Protokolle, um festzustellen, ob der Vorgang erfolgreich war.   |
| hdb-00005  | Datenbank [€sid] hat bereits einen Snapshot!  | HANA-Datenbank-Snapshot ist in der Datenbank bereits vorhanden. Löschen Sie den HANA-Datenbank-Snapshot oder führen Sie den Vorgang unquiesce aus, um dieses Problem zu beheben.   |
| hdb-00006  | Hostname [€bhana_Node] kann nicht aufgelöst werden.   | Der HANA-Node-Hostname kann nicht aufgelöst werden. Überprüfen Sie die Einträge Ihres DNS-Servers oder etc-Hosts.  |
| hdb-00007  | Ungültiger Benutzername oder ungültiges Passwort. Überprüfen Sie die Anmeldedaten, und versuchen Sie es erneut.           | Der für die HANA-Datenbank angegebene Benutzername und das für die HANA-Datenbank angegebene Passwort sind falsch. Korrigieren Sie die Einträge in der Konfigurationsdatei, und versuchen Sie es erneut.   |
| hdb-00008  | Ausführen des Befehls [€dbsql_cmd] in [€nger hana_Node] fehlgeschlagen.   | Das Plug-in konnte hdbsql-Befehl nicht auf allen HANA-Knoten ausführen, die in der Konfiguration enthalten sind. Überprüfen Sie die HANA-Nodes und die Instanzparameter und stellen Sie sicher, dass mindestens ein HANA-Node verfügbar ist.                                 |

| <b>Fehlercode</b> | <b>Fehlermeldung</b>  | <b>Beschreibung/Auflösung</b>   |
|-------------------|---|---|
| hdb-00009         | HANA konnte nicht gefunden werden [€Informationen].   | Der SAP HANA-Plug-in SCDUMP-Vorgang konnte keine bestimmten Informationen aus den HANA-Datenbanken abrufen. Überprüfen Sie die HANA-Knoten und die Instanzparameter und stellen Sie sicher, dass mindestens ein HANA-Node verfügbar ist und erreichbar ist. |
| hdb-00010         | Fehler beim Sammeln der OS-Informationen.   | Die Erfassung von Betriebssysteminformationen ist in der Windows-Umgebung fehlgeschlagen; das SAP HANA-Plug-in wird unter Windows nicht unterstützt. Verwenden Sie stattdessen ein SLES-Betriebssystem.   |
| hdb-00011         | Fehler beim Sammeln der OS-Informationen.   | Snap Creator konnte keine BS-Informationen für den SCDUMP-Vorgang sammeln. Überprüfen Sie die Agent-Konfigurationsdatei und korrigieren Sie die Einstellungen.  |
| hdb-00012         | Fehler beim Sammeln der SnapDrive-Informationen.  | Das SAP HANA Plug-in wird nur in einer NFS-Umgebung unterstützt. Ihre Konfiguration für HANA-Datenbank hat SnapDrive aktiviert; legen SIE SNAPDRIVE=Nin in der Konfigurationsdatei fest.  |
| hdb-00013         | Der Parameter HANA_NODES ist nicht festgelegt. Überprüfen Sie die HANA-Einstellungen in der Konfigurationsdatei.  | HANA-Nodes (HANA_NODES)-Parameter ist für das SAP HANA-Plug-in erforderlich. Legen Sie den Parameter fest, und versuchen Sie es erneut.   |
| hdb-00014         | Es konnte kein zugänglicher HANA-Knoten gefunden werden, um hdbsqlbedden mit den angegebenen Konfigurationsparametern auszuführen. Überprüfen und aktualisieren Sie die HANA-Einstellungen in der Konfiguration, und versuchen Sie es erneut. | Vergewissern Sie sich, dass HANA-Nodes ausgeführt und erreichbar sind, und die angegebene Instanznummer ist korrekt.  |

| Fehlercode | Fehlermeldung   | Beschreibung/Auflösung   |
|------------|---|--|
| hdb-00015  | Der Parameter HANA_INSTANCE ist nicht festgelegt. Überprüfen Sie die HANA-Einstellungen in der Konfigurationsdatei. | Für das SAP HANA-Plug-in ist HANA-Instance-Parameter (HANA_INSTANCE) erforderlich. Legen Sie den Parameter fest, und versuchen Sie es erneut.  |
| hdb-00016  | Der Parameter HANA_PASSWORD ist nicht festgelegt. Überprüfen Sie die HANA-Einstellungen in der Konfigurationsdatei. | HANA password (HANA_PASSWORD)-Parameter ist für das SAP HANA-Plug-in erforderlich. Legen Sie den Parameter fest, und versuchen Sie es erneut.  |
| hdb-00017  | Pfad zu hdbsql, Wert des Parameters HANA_HDBSQL_CMD ist ungültig!   | <p>Einer der folgenden Punkte ist aufgetreten:</p> <ul style="list-style-type: none"> <li>• Sie haben den hdbsql-Pfad nicht zur Verfügung gestellt</li> <li>• Der angegebene hdbsql-Pfad ist falsch.</li> </ul> <p>Stellen Sie sicher, dass der HANA hdbsql-Client auf dem Management-Host installiert ist, auf dem Snap Creator Agent installiert ist, und geben Sie den richtigen Pfad der hdbsql-Binärdatei in HANA-Parametern; dann versuchen Sie es erneut.</p> |

## Weitere Schritte

Weitere Informationen zu Snap Creator, einschließlich Versionsspezifischer Informationen, finden Sie auf der NetApp Support Site.

- ["Snap Creator Framework 4.3.3 – Installationshandbuch"](#)

Beschreibt die Installation von Snap Creator Server und Agent. Die Agent-Installation umfasst das SAP Hana Plug-in.

- ["Snap Creator Framework 4.3.3 – Administratorhandbuch"](#)

Hier wird die Administration von Snap Creator Framework nach Abschluss der Installation beschrieben.

- ["Snap Creator Framework 4.3.3 – Versionshinweise"](#)

Beschreibt neue Funktionen, wichtige Vorsichtsmaßnahmen, bekannte Probleme und Einschränkungen für Snap Creator Framework 4.1.1.

- ["Diskussionen Zu Snap Creator Framework"](#)

Tauschen Sie sich mit anderen aus, stellen Sie Fragen, lassen Sie sich von neuen Ideen inspirieren, finden Sie geeignete Ressourcen und erfahren Sie mehr über Snap Creator Best Practices.

- ["NetApp Video: SnapCreatorTV"](#)

In Videos werden die wichtigsten Snap Creator Technologien demonstriert.

## Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

## Markeninformationen

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