



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

NetApp solutions for SAP

NetApp  
December 10, 2025

# Inhalt

SAP HANA auf Amazon FSX für NetApp ONTAP – Backup und Recovery mit SnapCenter .....	1
TR-4926: SAP HANA auf Amazon FSX für NetApp ONTAP – Backup und Recovery mit SnapCenter .....	1
Backup und Recovery mit Amazon FSX für ONTAP .....	1
Laufzeit von Snapshot-Backup- und -Restore-Vorgängen .....	2
Vergleich der Recovery-Zeitvorgaben .....	2
Anwendungsfälle und Vorteile beschleunigter Backup- und Klonvorgänge .....	4
Architektur von SnapCenter .....	6
Komponenten von SnapCenter .....	6
SnapCenter SAP HANA Backup-Lösung .....	7
Inhalt des vorliegenden Dokuments .....	9
Datensicherung Strategie .....	9
Beispiel für die Laboreinrichtung .....	11
SnapCenter-Konfiguration .....	12
Übersicht über die Konfigurationsschritte .....	12
SAP HANA Backup-Benutzer und hdbuserstore-Konfiguration .....	12
Speicher konfigurieren .....	14
Hinzufügen eines SAP HANA-Hosts .....	17
Richtlinien konfigurieren .....	19
Konfiguration und Sicherung einer HANA-Ressource .....	23
SnapCenter-Backup-Vorgänge .....	28
Erstellen Sie ein Snapshot Backup nach Bedarf .....	28
Erstellung einer bedarfsgerechten Blockintegritätsprüfung .....	33
Backup nicht datenmengen .....	38
Restore und Recovery .....	45
Backup-Replizierung mit SnapVault .....	53
Übersicht - Backup-Replikation mit SnapVault .....	53
Konfigurieren Sie Replikationsbeziehungen auf FSX für ONTAP-Dateisysteme .....	54
Fügen Sie eine Backup-SVM zu SnapCenter hinzu .....	59
Erstellen einer neuen SnapCenter-Richtlinie für Backup-Replizierung .....	60
Fügen Sie eine Richtlinie zum Ressourcenschutz hinzu .....	62
Erstellen Sie ein Backup mit Replikation .....	63
Wiederherstellung im Sekundär-Storage .....	66
Wo Sie weitere Informationen finden .....	67
Versionsverlauf .....	68

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

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

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

Autor: Nils Bauer, NetApp

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

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

## **Backup und Recovery mit Amazon FSX für ONTAP**

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

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

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

auf mehrere Stunden, die bei herkömmlichen Streaming Backups benötigt werden.

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

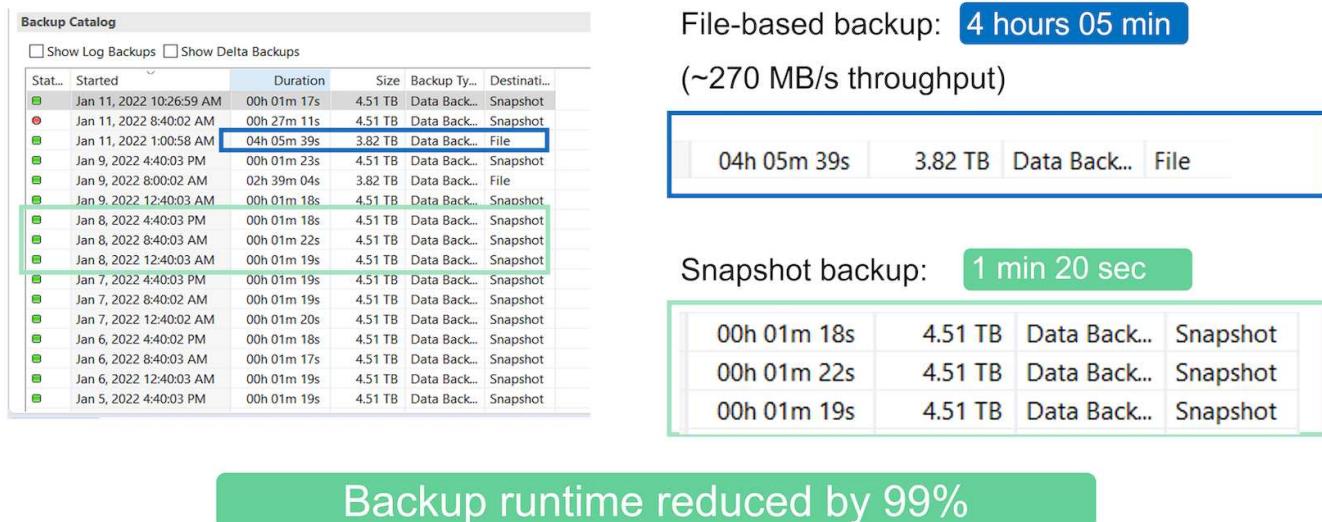
Ein Backup an einen sekundären Standort basiert auf Snapshot-Kopien, die auf dem primären Storage erstellt wurden. Somit werden die Daten direkt aus dem primären Storage-System eingelesen, ohne dass dabei der SAP Datenbankserver belastet wird. Der primäre Storage kommuniziert direkt mit dem sekundären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

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

## Laufzeit von Snapshot-Backup- und -Restore-Vorgängen

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

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



## Vergleich der Recovery-Zeitvorgaben

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

Wiederherstellen und Starten der Datenbank benötigt wird.

### **Benötigte Zeit zum Wiederherstellen der Datenbank**

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

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

### **Benötigte Zeit zum Starten der Datenbank**

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

### **Benötigte Zeit für das Recovery von Datenbanken**

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

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

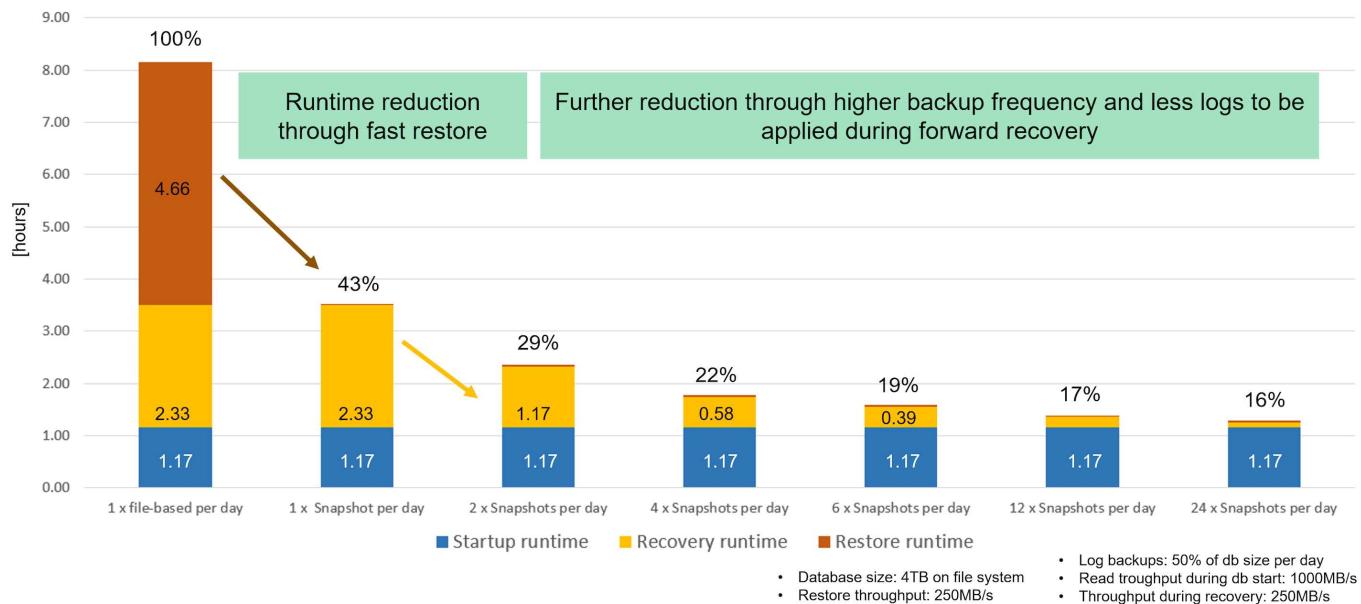
Snapshot Backups werden in der Regel mit höherer Frequenz geplant, da sie nicht die Performance der SAP HANA Datenbank beeinträchtigen. Wenn Snapshot Backups beispielsweise alle sechs Stunden geplant sind, wäre die Recovery-Zeit im schlimmsten Fall ein Viertel der Recovery-Zeit für ein dateibasiertes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

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

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

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

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



## Anwendungsfälle und Vorteile beschleunigter Backup- und Klonvorgänge

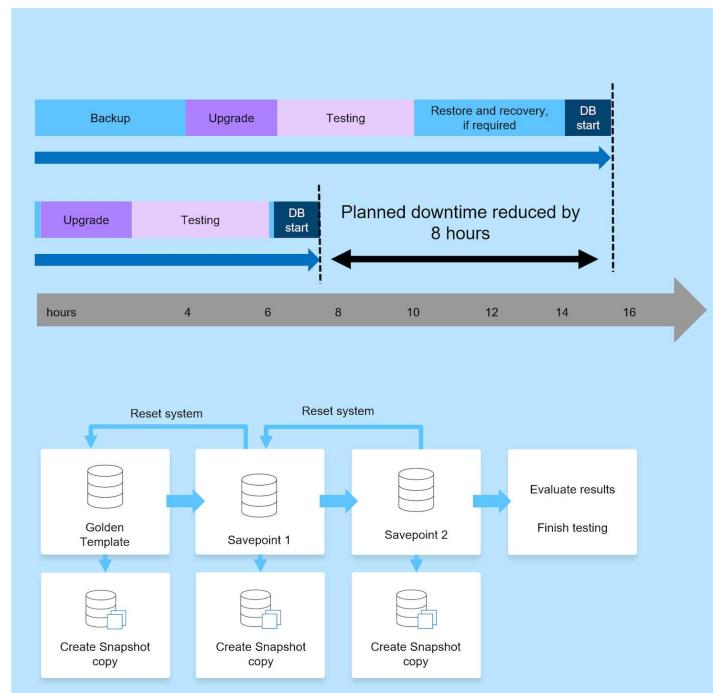
Die Ausführung von Backups ist ein wichtiger Bestandteil jeder Datensicherungsstrategie. Die Backups werden regelmäßig geplant, um sicherzustellen, dass Sie nach Systemausfällen wiederherstellen können. Dies ist der naheliegende Anwendungsfall, aber auch andere SAP Lifecycle Management-Aufgaben, von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

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

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

## Use Cases for Backup and Recovery Operations

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



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

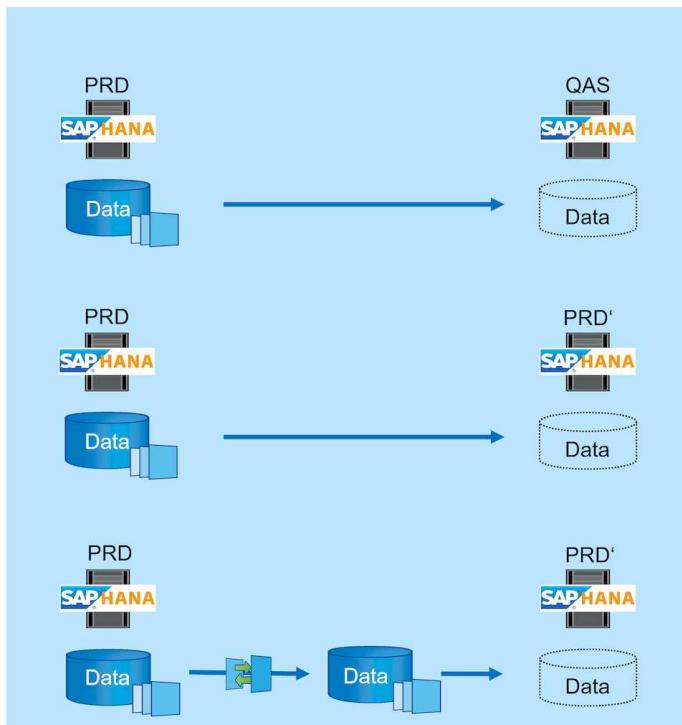
Der beliebteste Anwendungsfall ist SAP Systemaktualisierung, in dem Daten aus dem Produktionssystem in das Test- oder QA-System kopiert werden müssen. Mit der Klonfunktion von FSX für ONTAP lässt sich das Volume für das Testsystem von jeder beliebigen Snapshot Kopie des Produktionssystems in Sekundenschnelle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

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

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

## Use Cases for Cloning Operations

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



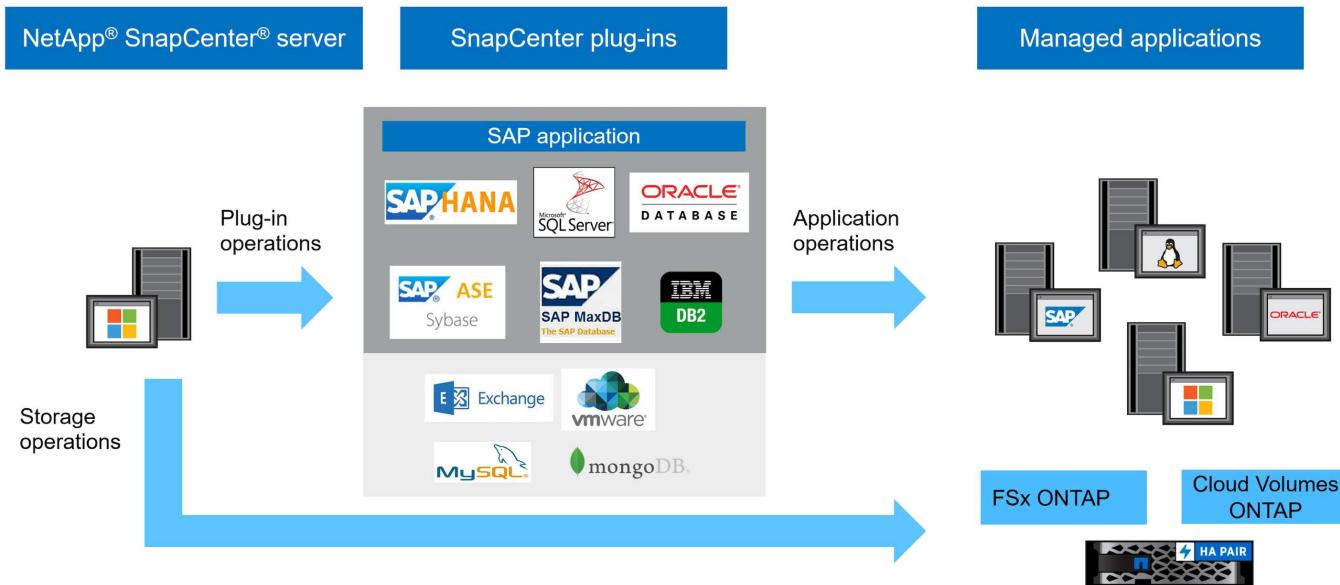
## Architektur von SnapCenter

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

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

## Komponenten von SnapCenter

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



## SnapCenter SAP HANA Backup-Lösung

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

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

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

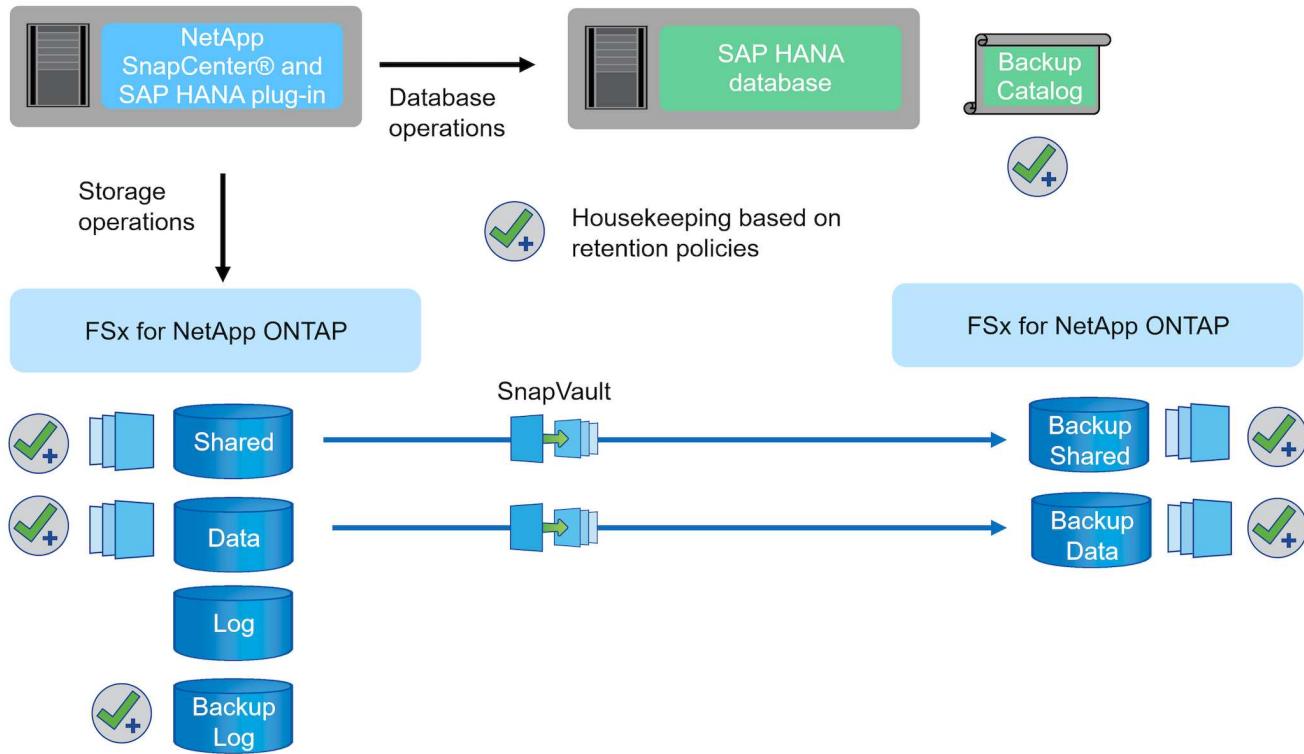
SnapCenter ermöglicht die Replizierung konsistenter Datenbank-Images auf einen externen Backup- oder Disaster-Recovery-Standort mithilfe von SnapVault oder der SnapMirror Funktion. In der Regel werden verschiedene Aufbewahrungsrichtlinien für Backups auf dem primären und externen Backup-Storage definiert.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

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

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

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

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



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

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

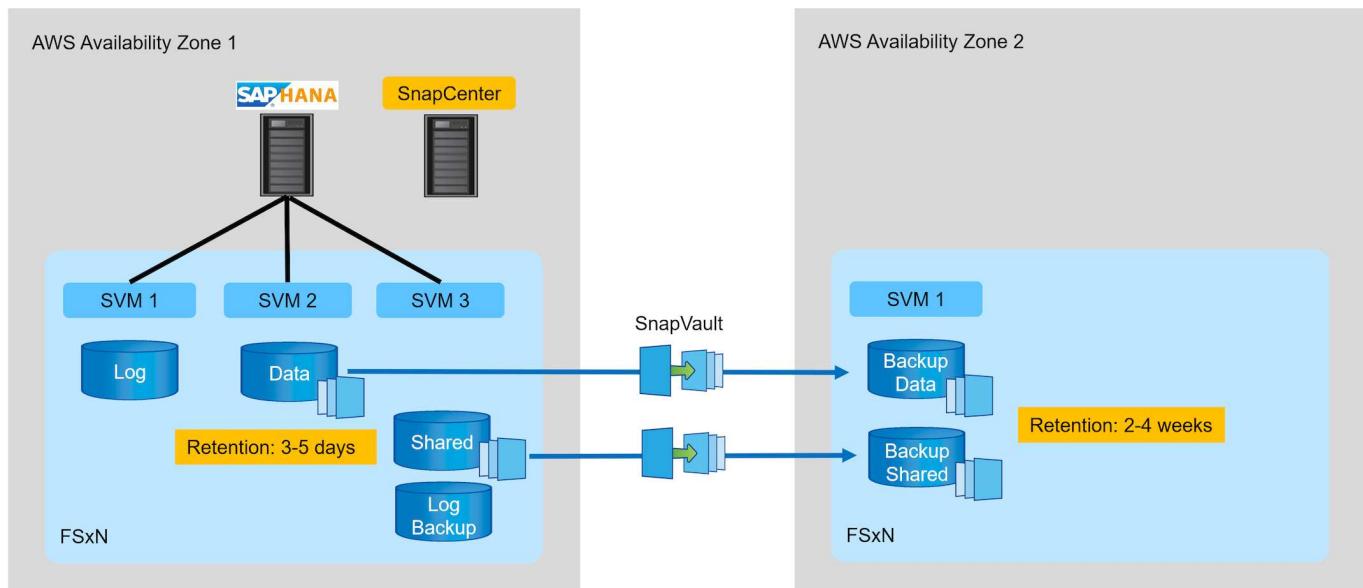
## Inhalt des vorliegenden Dokuments

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

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

## Datensicherung Strategie

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



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

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

Folgende Parameter müssen definiert werden:

- Wie oft sollte ein Snapshot Backup ausgeführt werden?

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

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

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

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

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

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

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

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

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

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

- Produktion: Zeitplan jeden Tag.

- Entwicklung: Zeitplan jeden Tag.  
die Politik BlockIntegrityCheck Wird für die Produktions- und Entwicklungssysteme eingesetzt, um die wöchentliche Blockintegritätsprüfung mithilfe eines dateibasierten Backups abzudecken.

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

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

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

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

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

## **Beispiel für die Laboreinrichtung**

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

HANA-System-PFX:

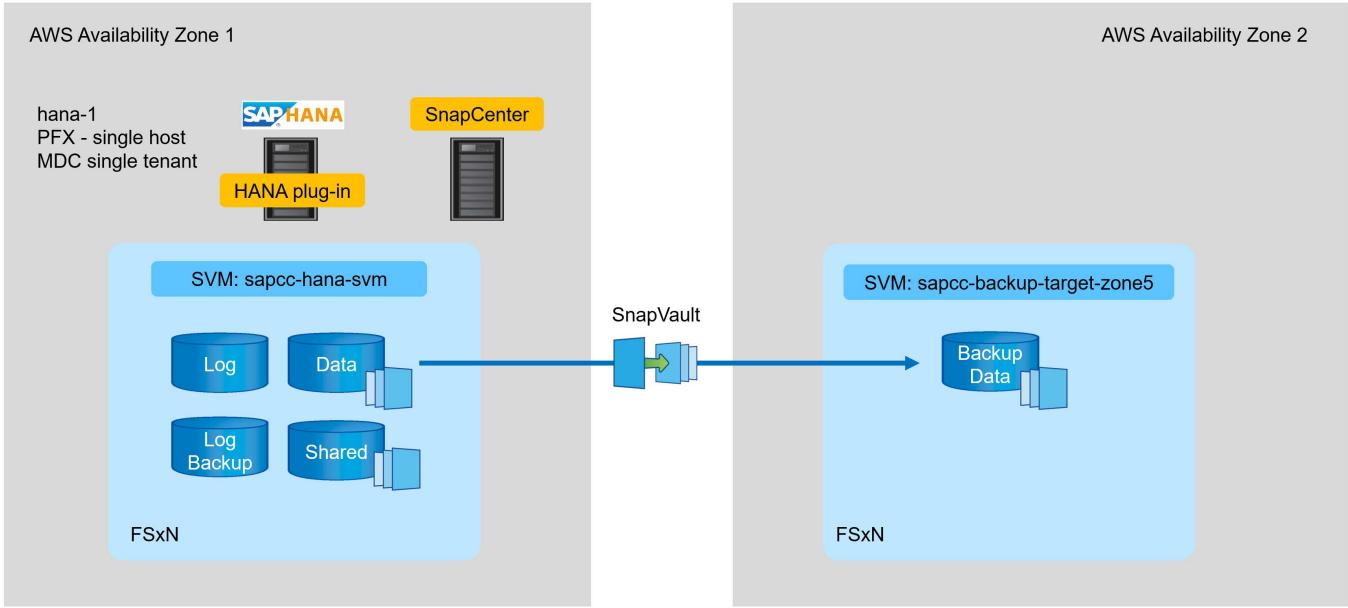
- Ein Host-MDC-System mit einem einzelnen Mandanten
- HANA 2.0 SPS 6, Version 60
- SLES FÜR SAP 15SP3

SnapCenter

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

FSX für ONTAP-Dateisysteme:

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



## SnapCenter-Konfiguration

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

### Übersicht über die Konfigurationsschritte

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

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

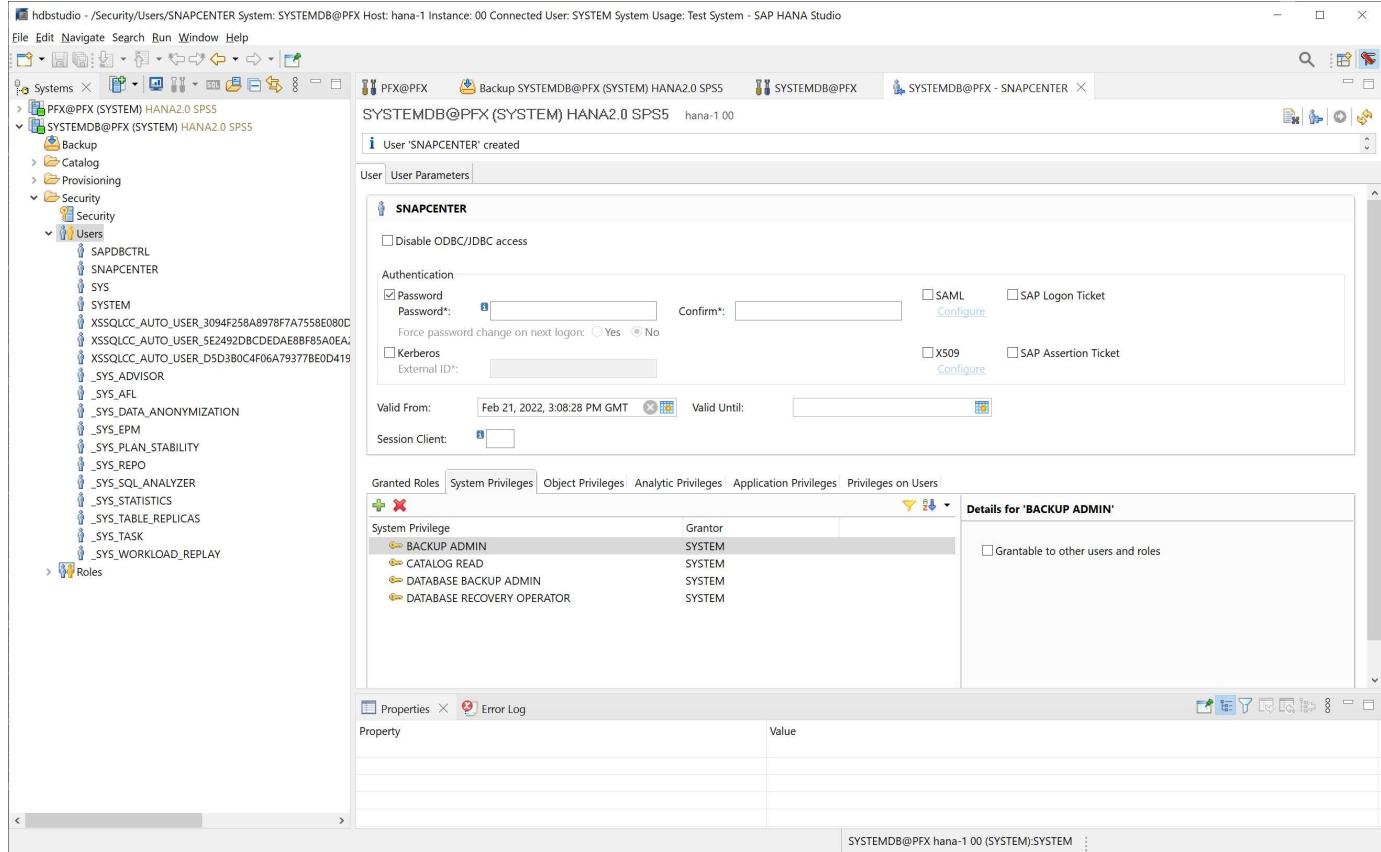
### SAP HANA Backup-Benutzer und hdbuserstore-Konfiguration

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

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

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

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



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

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

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

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

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

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

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

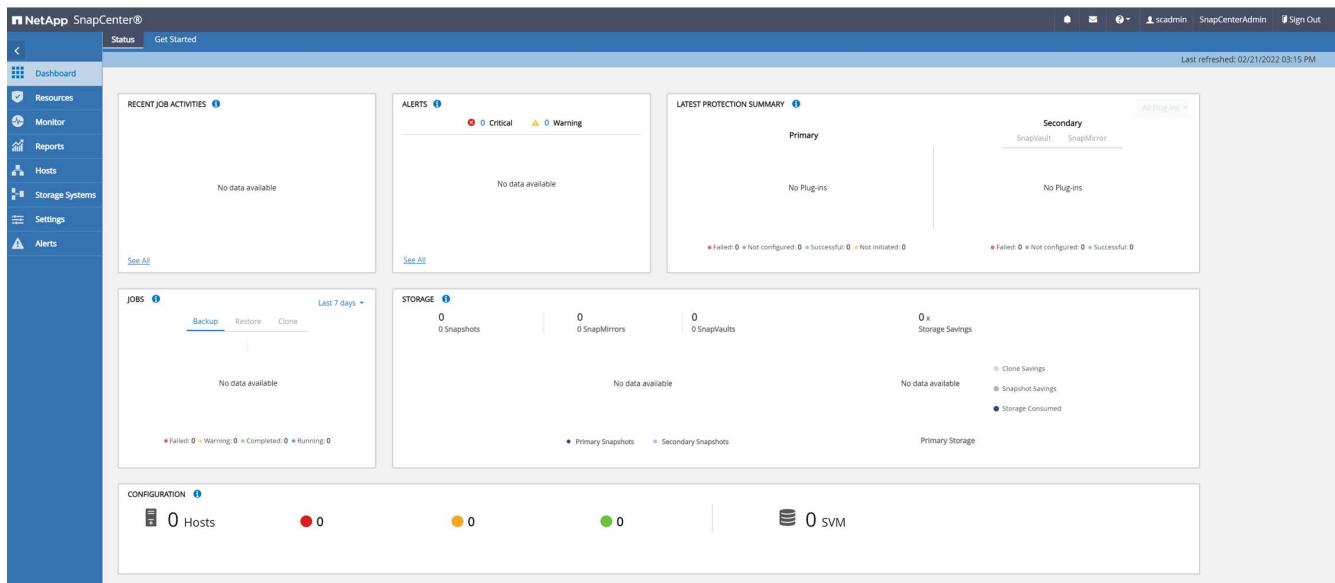
Sie können den Zugriff auf die HANA-Systemdatenbank prüfen, die den Schlüssel mit dem verwendet `hdbsql` Befehl.

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

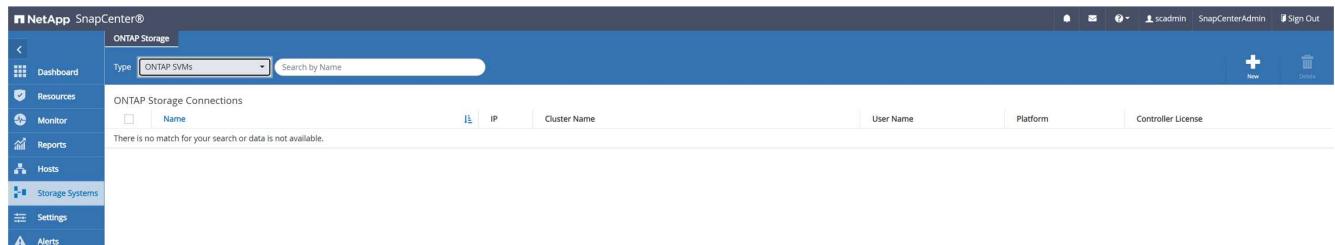
## Speicher konfigurieren

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

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

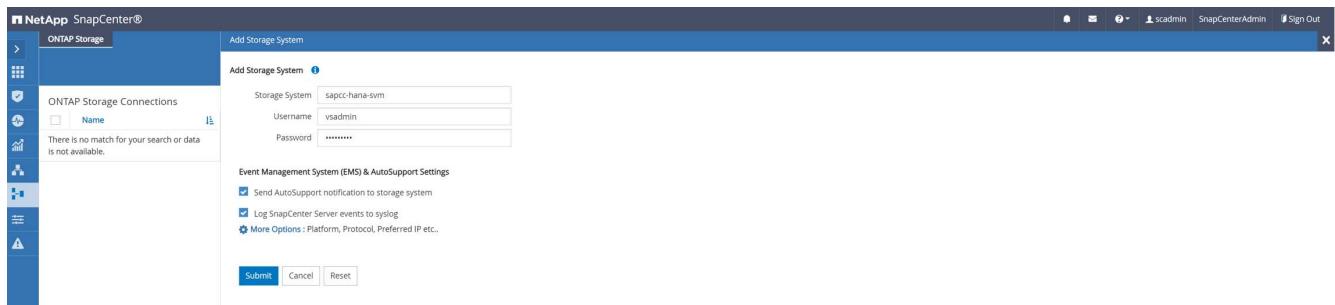


Sie können den Storage-Systemtyp auswählen, der ONTAP SVMs oder ONTAP Cluster sein kann. Im folgenden Beispiel ist das SVM-Management ausgewählt.



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

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



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

## More Options

Platform: All Flash FAS

Protocol: HTTPS

Port: 443

Timeout: 60 seconds

Preferred IP:

Der SVM sapcc-hana-svm ist jetzt in SnapCenter konfiguriert.

The screenshot shows the 'ONTAP Storage' section of the NetApp SnapCenter interface. A table lists storage connections, with one entry for 'sapcc-hana-svm'. The table columns include Name, IP, Cluster Name, User Name, Platform, and Controller License. The 'sapcc-hana-svm' row has '198.19.255.9' in the IP column, 'vsadmin' in the User Name column, 'AFF' in the Platform column, and a checked 'Controller License' checkbox.

### Anmelddaten für Plug-in-Implementierung erstellen

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

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

The screenshot shows the 'Credential' tab of the NetApp SnapCenter interface. A search bar at the top contains 'Search by Credential Name'. Below it, a table lists credentials, with a single row for 'snapcenter'. The table includes columns for Credential Name, Authentication Mode, and Details. A 'New' button is visible in the top right corner.

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

## Credential

Credential Name	PluginOnLinux
Authentication Mode	Linux
Username	snapcenter
Password	*****

Use sudo privileges i

Cancel OK

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

## Hinzufügen eines SAP HANA-Hosts

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

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

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

OpenJDK oder Oracle Java wird mit SnapCenter unterstützt.

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

1. Klicken Sie auf der Registerkarte Host auf Hinzufügen.

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

3. Bestätigen Sie den Fingerabdruck.

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

Sie können die Warnmeldung mithilfe der folgenden Schritte entfernen.

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

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

## Richtlinien konfigurieren

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

Eine typische Minimalkonfiguration umfasst folgende Richtlinien:

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

In den folgenden Abschnitten wird die Konfiguration dieser Richtlinien beschrieben.

### Richtlinien für Snapshot-Backups

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

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

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

### New SAP HANA Backup Policy

**1 Name**

Provide a policy name

Policy name	LocalSnap	<a href="#">i</a>
Details	Snapshot backup at primary volume	

**2 Settings**

**3 Retention**

**4 Replication**

**5 Summary**

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

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

### New SAP HANA Backup Policy

**1 Name**

Select backup settings

Backup Type  Snapshot Based  File-Based [i](#)

**2 Settings**

**3 Retention**

**4 Replication**

**5 Summary**

Schedule Frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

On demand  
 Hourly  
 Daily  
 Weekly  
 Monthly

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

New SAP HANA Backup Policy

Retention settings

Hourly retention settings

Total Snapshot copies to keep  ⓘ

Keep Snapshot copies for  days

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

New SAP HANA Backup Policy

Select secondary replication options ⓘ

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label  ⓘ

Error retry count  ⓘ

New SAP HANA Backup Policy

Summary

Policy name	LocalSnap
Details	Snapshot backup at primary volume
Backup Type	Snapshot Based Backup
Schedule Type	Hourly
Hourly backup retention	Total backup copies to retain : 7
Replication	none

Die neue Richtlinie ist jetzt konfiguriert.

Name	Backup Type	Schedule Type	Replication
LocalSnap	Data Backup	Hourly	

## Richtlinie zur Block-Integritätsprüfung

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

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

New SAP HANA Backup Policy

The dialog shows the 'Name' tab selected. It has fields for 'Policy name' (BlockIntegrityCheck) and 'Details' (Check HANA DB blocks using file-based backup). A sidebar on the left lists steps 1 through 5: Name, Settings, Retention, Replication, and Summary. Step 1 is highlighted.

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

New SAP HANA Backup Policy

The dialog shows the 'Settings' tab selected. It includes a 'Backup Type' section with 'File-Based' selected, and a 'Schedule Frequency' section where 'Weekly' is selected. A sidebar on the left lists steps 1 through 4: Name, Settings, Retention, and Summary. Step 2 is highlighted.

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

New SAP HANA Backup Policy

The dialog shows the 'Retention' tab selected. It displays 'Weekly retention settings' with 'Total backup copies to keep' set to 1. A sidebar on the left lists steps 1 through 4: Name, Settings, Retention, and Summary. Step 3 is highlighted.

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

New SAP HANA Backup Policy

<b>1 Name</b>	<b>Summary</b>
<b>2 Settings</b>	Policy name: BlockIntegrityCheck Details: Check HANA DB blocks using file-based backup
<b>3 Retention</b>	Backup Type: File-Based Backup
<b>4 Summary</b>	Schedule Type: Weekly Weekly backup retention: Total backup copies to retain : 1

Name	Backup Type	Schedule Type	Replication
BlockIntegrityCheck	File Based Backup	Weekly	
LocalSnap	Data Backup	Hourly	

## Konfiguration und Sicherung einer HANA-Ressource

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

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

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

System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
PFX	PFX	PFX	None	hana-1				Not protected

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

## Configure Database

X

Plug-in host hana-1

HDBSQL OS User pfxadm

HDB Secure User Store Key **PFXKEY**



Cancel

OK

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

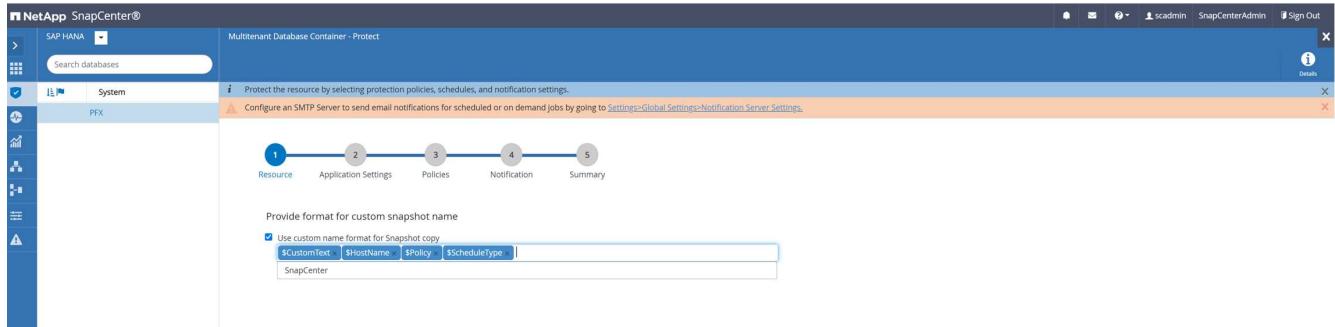
System			
Type	Multitenant Database Container		
HANA System Name	PFX		
SID	PFX		
Tenant Databases	PFX		
Plug-in Host	hana-1		
HDB Secure User Store Key	PFXKEY		
HDBSQL OS User	pfxadm		
Log backup location	/backup/log		
Backup catalog location	/backup/log		
System Replication	None		
plug-in name	SAP HANA		
Last backup	None		
Resource Groups	None		
Policy	None		
Discovery Type	Auto		
Storage Footprint			
SVM	Volume	Junction Path	LUN/Qtree
sapcc-hana-svm	PFX_data_mnt00001	/PFX_data_mnt00001	

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

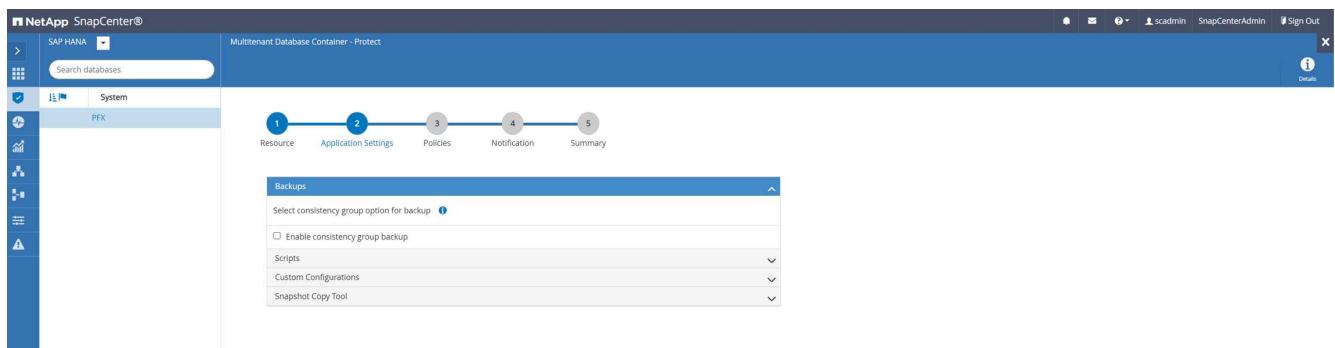
System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
PFX	PFX	PFX	None	hana-1				Not protected

- Konfigurieren Sie ein benutzerdefiniertes Namensformat für die Snapshot Kopie.

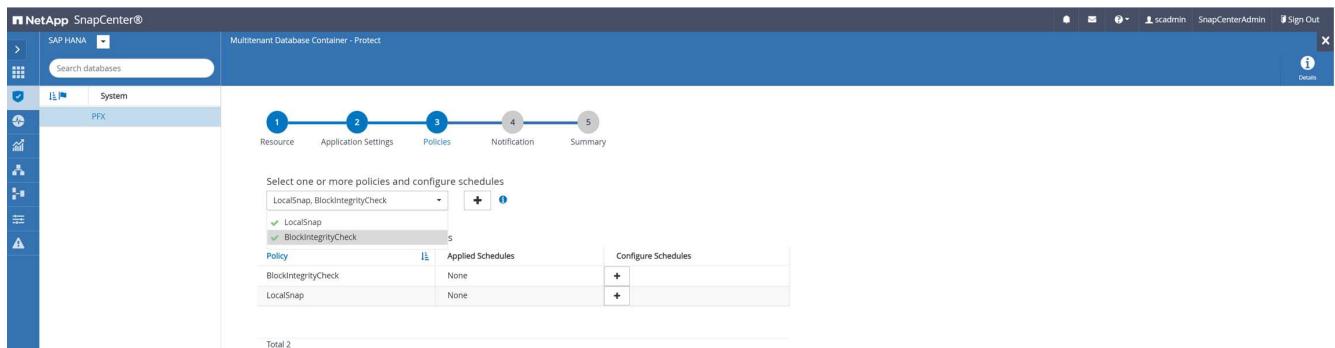
NetApp empfiehlt den Einsatz einer benutzerdefinierten Snapshot Kopie, um schnell ermitteln zu können, mit welcher Richtlinie und welche Zeitplantypen Backups erstellt wurden. Durch Hinzufügen des Zeitplantyps zum Namen der Snapshot Kopie können Sie zwischen geplanten und On-Demand-Backups unterscheiden.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



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



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



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

In diesem Beispiel wird sie für einmal pro Woche festgelegt.

## Add schedules for policy BlockIntegrityCheck

X

### Weekly

Start date	02/22/2022 12:00 pm	
<input type="checkbox"/> Expires on	03/22/2022 12:00 pm	
Days	Sunday	

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday



The schedules are triggered in the SnapCenter Server time zone.

X

Cancel

OK

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

In diesem Beispiel wird die Einstellung alle 6 Stunden durchgeführt.

## Modify schedules for policy LocalSnap

x

### Hourly

Start date	02/22/2022 02:00 pm	
<input type="checkbox"/> Expires on	04/28/2022 11:57 am	
Repeat every	6 hours	0 mins



The schedules are triggered in the SnapCenter Server time zone.

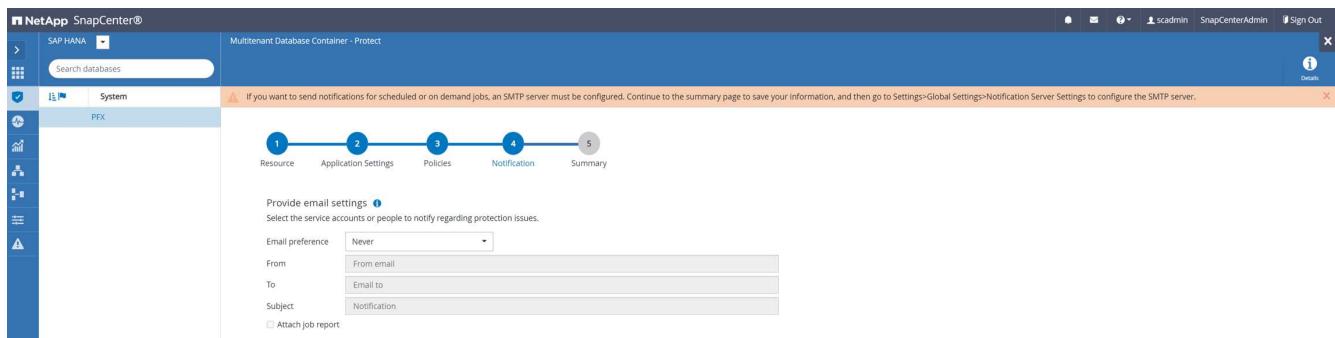


Cancel

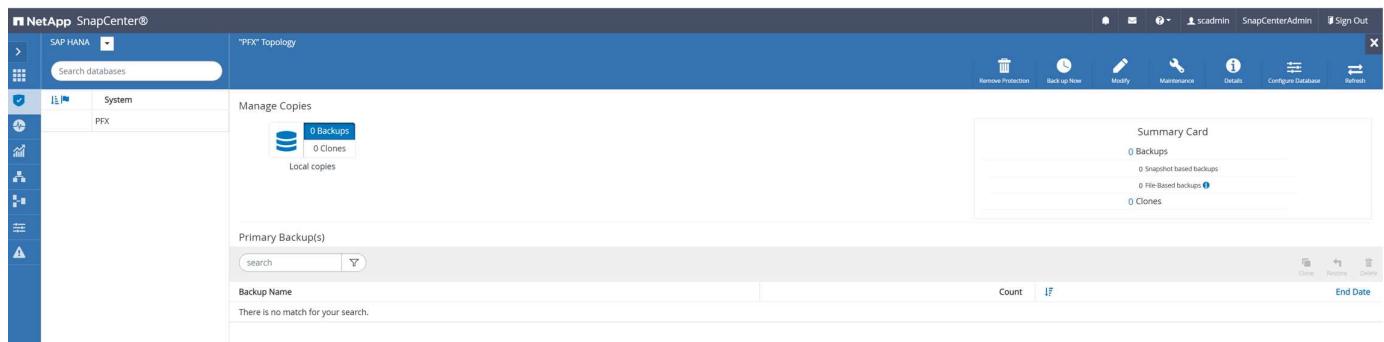
OK

The screenshot shows the 'Multitenant Database Container - Protect' screen in the NetApp SnapCenter interface. A progress bar at the top indicates steps 1 through 5. Step 2, 'Application Settings', is selected. Below it, a section titled 'Select one or more policies and configure schedules' shows 'LocalSnap, BlockIntegrityCheck' selected. Under 'Configure schedules for selected policies', there are two entries: 'BlockIntegrityCheck' with 'Applied Schedules' 'Weekly: Run on days: Sunday' and 'Configure Schedules' 'x'; and 'LocalSnap' with 'Applied Schedules' 'Hourly: Repeat every 6 hours' and 'Configure Schedules' 'x'. A note at the bottom says 'Total 2'.

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



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



## SnapCenter-Backup-Vorgänge

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

### Erstellen Sie ein Snapshot Backup nach Bedarf

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

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

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

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

NetApp SnapCenter®

SAP HANA

"PFX" Topology

Remove Protection Back up Now Monitor Maintenance Details Configure Database Sign Out

Manage Copies

0 Backups  
0 Clones

Local copies

Primary Backup(s)

search

Backup Name

There is no match for your search.

Count

End Date

Summary Card

0 Backups  
0 Snapshot-based backups  
0 File-based backups  
0 Clones

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

### Backup

Create a backup for the selected resource

Resource Name: PFX

Policy: LocalSnap

Cancel

Backup

## Confirmation

x



The policy selected for the on-demand backup is associated with a backup schedule and the on-demand backups will be retained based on the retention settings specified for the schedule type.

Do you want to continue ?

Yes

No

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

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

## Job Details

X

Backup of Resource Group 'hana-1\_hana\_MDC\_PFX' with policy 'LocalSnap'

- ✓ ▾ Backup of Resource Group 'hana-1\_hana\_MDC\_PFX' with policy 'LocalSnap'
  - ✓ ▾ hana-1
    - ✓ Backup
      - ✓ Validate Dataset Parameters
      - ✓ Validate Plugin Parameters
      - ✓ Complete Application Discovery
      - ✓ Initialize Filesystem Plugin
      - ✓ Discover Filesystem Resources
      - ✓ Validate Retention Settings
      - ✓ Quiesce Application
      - ✓ Quiesce Filesystem
      - ✓ Create Snapshot
      - ✓ UnQuiesce Filesystem
      - ✓ UnQuiesce Application
      - ✓ Get Snapshot Details
      - ✓ Get Filesystem Meta Data
      - ✓ Finalize Filesystem Plugin
      - ✓ Collect Autosupport data
      - ✓ Register Backup and Apply Retention
      - ✓ Register Snapshot attributes
      - ✓ Application Clean-Up
      - ✓ Data Collection
      - ✓ Agent Finalize Workflow

Task Name: Backup Start Time: 02/22/2022 12:08:58 PM End Time: 02/22/2022 12:10:21 PM

[View Logs](#)

[Cancel Job](#)

[Close](#)

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

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

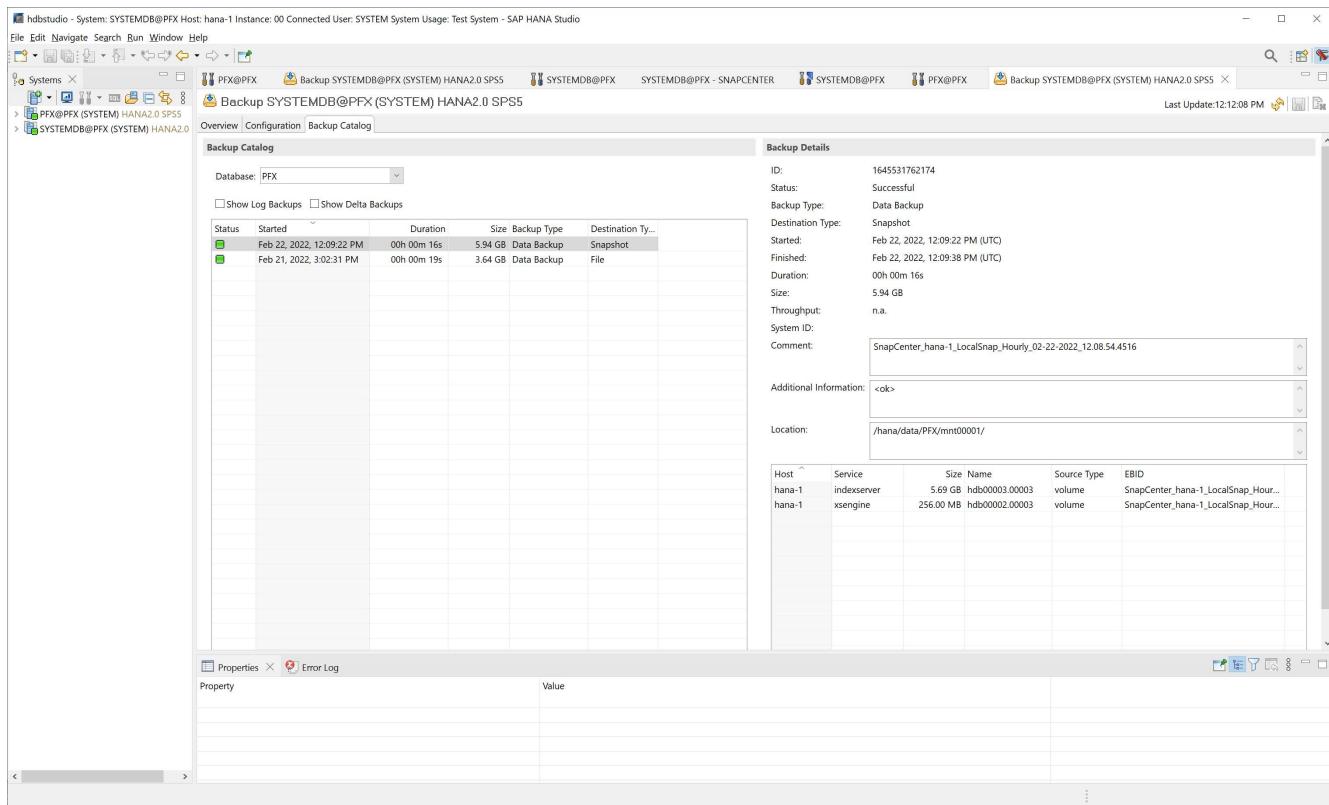
The screenshot shows the NetApp SnapCenter interface. At the top, there's a navigation bar with tabs like SAP HANA, PFX, and System. Below the navigation is a search bar labeled "Search databases". The main area is titled "PFX Topology" and contains a "Manage Copies" section with a summary card showing 1 Backup, 0 Clones, and a "Summary Card" panel. Below this is a table titled "Primary Backup(s)" with one entry: "Backup Name: SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-22-2022\_12.08.54.4516" and a "Count" of 1. The interface includes various buttons like Remove Protection, Back up Now, Modify, Maintenance, Details, Configure Database, and Refresh.

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

The screenshot shows the SAP HANA Studio interface. The title bar indicates "hdbstudio - System: SYSTEMDB@PFX Host: hana-1 Instance: 00 Connected User: SYSTEM System Usage: Test System - SAP HANA Studio". The left sidebar shows a tree view of "Systems" and "PFX@PFX (SYSTEM) HANA2.0 SPSS". The main area is titled "Backup Catalog" and shows a table of backups for the "SYSTEMDB" database. The table has columns: Status, Started, Duration, Size, Backup Type, and Destination Ty... (partially visible). There are two entries: one from Feb 22, 2022, at 12:09:22 PM, and another from Feb 21, 2022, at 3:01:49 PM. To the right of the table is a "Backup Details" panel. It displays the following information:

ID:	1645531762175
Status:	Successful
Backup Type:	Data Backup
Destination Type:	Snapshot
Started:	Feb 22, 2022, 12:09:22 PM (UTC)
Finished:	Feb 22, 2022, 12:09:38 PM (UTC)
Duration:	00h 00m 16s
Size:	5.50 GB
Throughput:	n.a.
System ID:	
Comment:	SnapCenter_hana-1_LocalSnap_Hourly_02-22-2022_12.08.54.4516
Additional Information:	<ok>
Location:	/hana/data/PFX/mnt00001/

Below the details panel is a table showing host, service, size, name, source type, and EBID for the backup. The table has one row for "hana-1" with values: nameserver, 5.50 GB, hdB00001, volume, and SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-22-2022\_12.08.54.4516. At the bottom, there are "Properties" and "Error Log" tabs.



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

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

## Erstellung einer bedarfsgerechten Blockintegritätsprüfung

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

## Backup

X

Create a backup for the selected resource

Resource Name

PFX

Policy

BlockIntegrityCheck

i

Cancel

Backup

## Job Details

Backup of Resource Group 'hana-1\_hana\_MDC\_PFX' with policy 'BlockIntegrityCheck'

✓ ▾ Backup of Resource Group 'hana-1\_hana\_MDC\_PFX' with policy 'BlockIntegrityCheck'

✓ ▾ hana-1

✓ ▾ File-Based Backup

✓ ▶ Validate Plugin Parameters

✓ ▶ Start File-Based Backup

✓ ▶ Check File-Based Backup

✓ ▶ Register Backup and Apply Retention

✓ ▶ Data Collection

Task Name: File-Based Backup Start Time: 02/22/2022 12:55:21 PM End Time: 02/22/2022 12:56:36 PM

[View Logs](#)

[Cancel Job](#)

[Close](#)

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

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

Backup Name	Count	End Date
SnapCenter_hana-1_LocalSnap_Hourly_02-22-2022_12.08.54.4516	1	02/22/2022 12:09:57 PM

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

Host	Service	Size	Name	Source Type	EBID
hana-1	nameserver	6.06 KB	SnapCenter_Snap... topology		
hana-1	nameserver	3.56 GB	SnapCenter_Snap... volume		

**Backup Catalog**

Status	Started	Duration	Size	Backup Type	Destination
Success	Feb 22, 2022, 12:55:34 PM	00h 00m 27s	3.64 GB	Data Backup	File
Success	Feb 22, 2022, 12:09:22 PM	00h 00m 16s	5.94 GB	Data Backup	Snapshot
Success	Feb 21, 2022, 3:02:31 PM	00h 00m 19s	3.64 GB	Data Backup	File

**Backup Details**

ID:	1645534534230
Status:	Successful
Backup Type:	Data Backup
Destination Type:	File
Started:	Feb 22, 2022, 12:55:34 PM (UTC)
Finished:	Feb 22, 2022, 12:56:01 PM (UTC)
Duration:	00h 00m 27s
Size:	3.64 GB
Throughput:	138.07 MB/s
System ID:	
Comment:	SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-2022_12.55.18.7966
Additional Information:	<ok>
Location:	/backup/data/DB_PFX/

**Properties**

Property	Value

**Error Log**

Host	Service	Size	Name	Source Type	EBID
hana-1	indexserver	1.58 KB	SnapCenter_Snap...	topology	
hana-1	xengine	80.00 MB	SnapCenter_Snap...	volume	
hana-1	indexserver	3.56 GB	SnapCenter_Snap...	volume	

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

```

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

```

## Backup nicht datenmengen

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

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

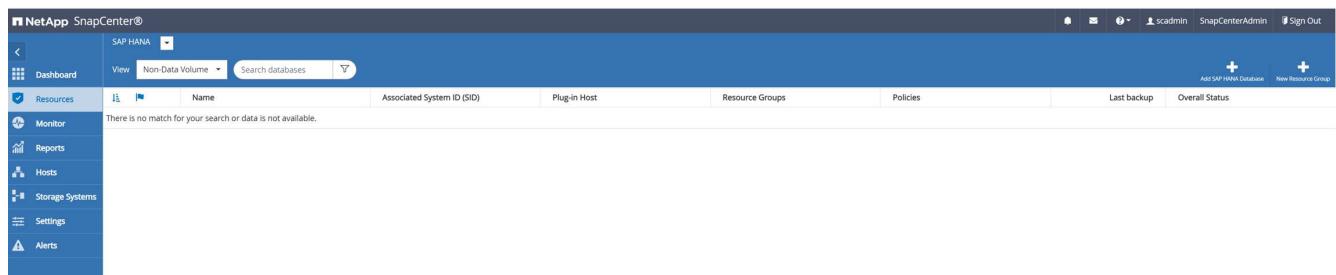
Um das Recovery von Situationen durchzuführen, in denen andere nicht-Datendateien wiederhergestellt werden müssen, empfiehlt NetApp, eine zusätzliche Backup-Strategie für nicht-Daten-Volumes zu entwickeln, um das SAP HANA Datenbank-Backup zu erweitern. Je nach Ihren spezifischen Anforderungen kann sich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

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

## Konfiguration von Ressourcen, die nicht von Datenvolumen stammen

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

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



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

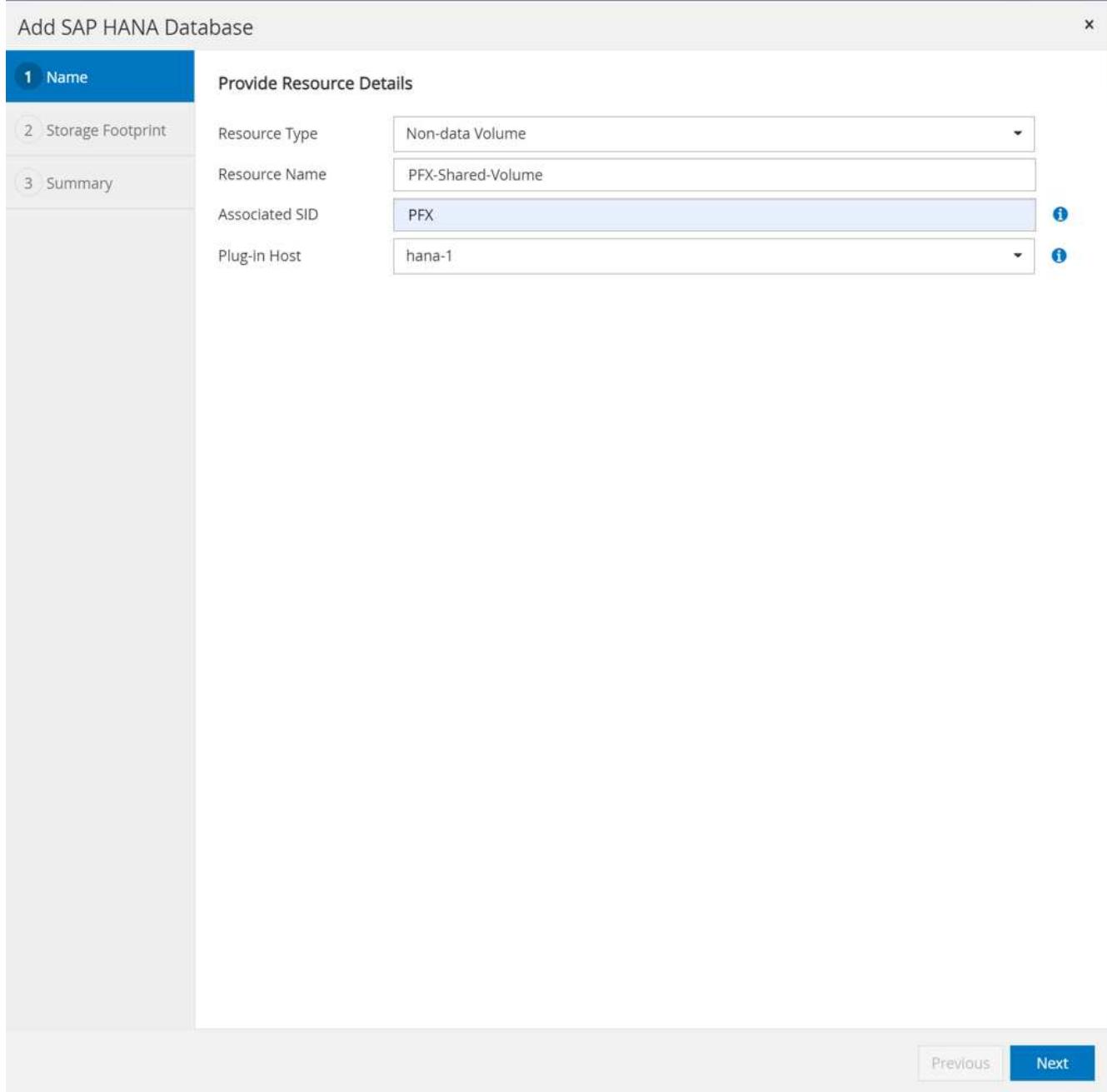
Add SAP HANA Database

**1 Name**

**Provide Resource Details**

2 Storage Footprint	Resource Type	Non-data Volume
3 Summary	Resource Name	PFX-Shared-Volume
	Associated SID	PFX
	Plug-in Host	hana-1

**Previous** **Next**



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

Add SAP HANA Database

**1 Name**

**2 Storage Footprint**

**3 Summary**

Provide Storage Footprint Details

Storage Type  ONTAP

Add Storage Footprint X

Storage System

Select one or more volumes and if required their associated Qtrees and LUNs

Volume name	LUNs or Qtrees
PFX_shared	Default is 'None' or type to find

Save

Previous Next

The screenshot shows the 'Add SAP HANA Database' wizard, specifically step 2: Storage Footprint. The left sidebar lists three steps: 1. Name (highlighted in blue), 2. Storage Footprint (selected), and 3. Summary. The main panel title is 'Provide Storage Footprint Details'. It specifies 'Storage Type' as 'ONTAP'. Below this, there's a section titled 'Add Storage Footprint' with a close button ('X'). A dropdown menu for 'Storage System' contains the entry 'sapcc-hana-svm'. A note below says 'Select one or more volumes and if required their associated Qtrees and LUNs'. A table lists a single volume 'PFX\_shared' under 'Volume name' and its corresponding 'LUNs or Qtrees' (which is 'Default is 'None'' or 'type to find'). At the bottom right of the main panel are 'Save' and 'Cancel' buttons. At the very bottom of the screen are 'Previous' and 'Next' buttons.

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

Add SAP HANA Database

<b>1 Name</b>	Summary						
<b>2 Storage Footprint</b>	Resource Type Non-data Volume Resource Name PFX-Shared-Volume Associated SID PFX Plug-in Host hana-1						
<b>3 Summary</b>	<p>Storage Footprint</p> <table border="1"> <thead> <tr> <th>Storage System</th> <th>Volume</th> <th>LUN/Qtree</th> </tr> </thead> <tbody> <tr> <td>sapcc-hana-svm</td> <td>PFX_shared</td> <td></td> </tr> </tbody> </table>	Storage System	Volume	LUN/Qtree	sapcc-hana-svm	PFX_shared	
Storage System	Volume	LUN/Qtree					
sapcc-hana-svm	PFX_shared						
	<input type="button" value="Previous"/> <input type="button" value="Finish"/>						

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

The screenshot shows the NetApp SnapCenter interface. On the left, there's a navigation sidebar with options like Dashboard, Resources (which is selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area has a blue header bar with the text "SAP HANA". Below it, there's a search bar with "Non-Data Volume" and a "Search databases" button. The main content area displays a table with the following data:

Name	Associated System ID (SID)	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
PFX-Shared-Volume	PFX	hana-1				Not protected

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

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

The screenshot shows the NetApp SnapCenter interface. The top navigation bar includes 'NetApp SnapCenter®', 'SAP HANA', 'Search databases', and user information like 'scadmin', 'SnapCenterAdmin', and 'Sign Out'. The main content area is titled 'PFX-Shared-Volume' Topology. On the left, there's a sidebar with various icons. The central part shows 'Manage Copies' with '0 Backups' and '0 Clones'. Below that is a section for 'Primary Backup(s)' with a search bar and a note: 'There is no match for your search.' To the right is a 'Summary Card' showing statistics: '0 Backups', '0 Snapshot based backups', and '0 Clones'. A toolbar at the bottom right includes 'Clone', 'Restore', 'Delete', and 'End Date'.

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

The screenshot shows a 'Backup' dialog box. The title is 'Backup'. Inside, it says 'Create a backup for the selected resource'. There are two input fields: 'Resource Name' containing 'PFX-Shared-Volume' and 'Policy' containing 'LocalSnap'. Below these is an information icon. At the bottom are two buttons: 'Cancel' and a larger 'Backup' button.

Das Jobprotokoll von SnapCenter zeigt die einzelnen Workflow-Schritte.

## Job Details

Backup of Resource Group 'hana-1\_hana\_NonDataVolume\_PFX\_PFX-Shared-Volume' with policy 'LocalSnap'

- ✓ ▾ Backup of Resource Group 'hana-1\_hana\_NonDataVolume\_PFX\_PFX-Shared-Volume' with policy 'LocalSnap'
- ✓ ▾ hana-1
  - ✓ ▾ Backup
    - ✓ ▶ Validate Dataset Parameters
    - ✓ ▶ Validate Plugin Parameters
    - ✓ ▶ Validate Retention Settings
    - ✓ ▶ Create Snapshot
    - ✓ ▶ Get Snapshot Details
    - ✓ ▶ Collect Autosupport data
    - ✓ ▶ Register Backup and Apply Retention
    - ✓ ▶ Register Snapshot attributes
    - ✓ ▶ Data Collection
    - ✓ ▶ Agent Finalize Workflow

Task Name: Backup Start Time: 02/22/2022 3:27:48 PM End Time:

[View Logs](#)

[Cancel Job](#)

[Close](#)

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

## Restore und Recovery

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

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

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

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

Als Nächstes führt SnapCenter die folgenden Operationen durch:

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

Wenn keine Wiederherstellung ausgewählt ist, wird die SnapCenter beendet, und Sie müssen den Wiederherstellungsvorgang für das System und die Mandantendatenbank manuell durchführen.

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

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

The screenshot shows the NetApp SnapCenter interface for SAP HANA. The left sidebar has a 'System' tab selected. In the center, there's a 'Manage Copies' section with '4 Backups' and '0 Clones'. Below it, a table lists 'Primary Backup(s)' with four entries. The table columns are 'Backup Name', 'Count', and 'End Date'. The data is as follows:

Backup Name	Count	End Date
SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361	1	02/23/2022 2:01:11 PM
SnapCenter_hana-1_LocalSnap_Hourly_02-22-2022_20.00.01.4482	1	02/22/2022 8:01:01 PM
SnapCenter_hana-1_LocalSnap_Hourly_02-22-2022_14.00.02.8713	1	02/22/2022 2:01:01 PM
SnapCenter_hana-1_LocalSnap_Hourly_02-22-2022_12.08.54.4516	1	02/22/2022 12:09:57 PM

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

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

Restore from SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-23-2022\_14.00.05.4361

**1 Restore scope**

Select the restore types

Complete Resource i

Volume Revert

⚠ As part of Complete Resource restore, if a resource contains volumes as Storage Footprint, then the latest Snapshot copies on such volumes will be deleted permanently. Also, if there are other resources hosted on the same volumes, then it will result in data loss for such resources.

Tenant Database

**2 Recovery scope**

**3 PreOps**

**4 PostOps**

**5 Notification**

**6 Summary**

⚠ The newer tenants added on the host after the backup was created cannot be restored and will be lost after restore operation.

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

Previous Next

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

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

- 1 Restore scope
- 2 Recovery scope
- 3 PreOps
- 4 PostOps
- 5 Notification
- 6 Summary

**Recover database files using**

- Recover to most recent state [i](#)
- Recover to point in time [i](#)
- Recover to specified data backup [i](#)
- No recovery [i](#)

**Specify log backup locations [i](#)**[Add](#)**Specify backup catalog location [i](#)**

 Recovery options are applicable to both system database and tenant database.

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

[Previous](#)[Next](#)

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

## Restore from SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-23-2022\_14.00.05.4361

X

- 1 Restore scope
- 2 Recovery scope
- 3 PreOps
- 4 PostOps
- 5 Notification
- 6 Summary

Enter optional commands to run before performing a restore operation i

Pre restore command



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

X

Previous

Next

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

Restore from SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-23-2022\_14.00.05.4361 x

**1 Restore scope** Enter optional commands to run after performing a restore operation i

**2 Recovery scope**

**3 PreOps**

**4 PostOps**

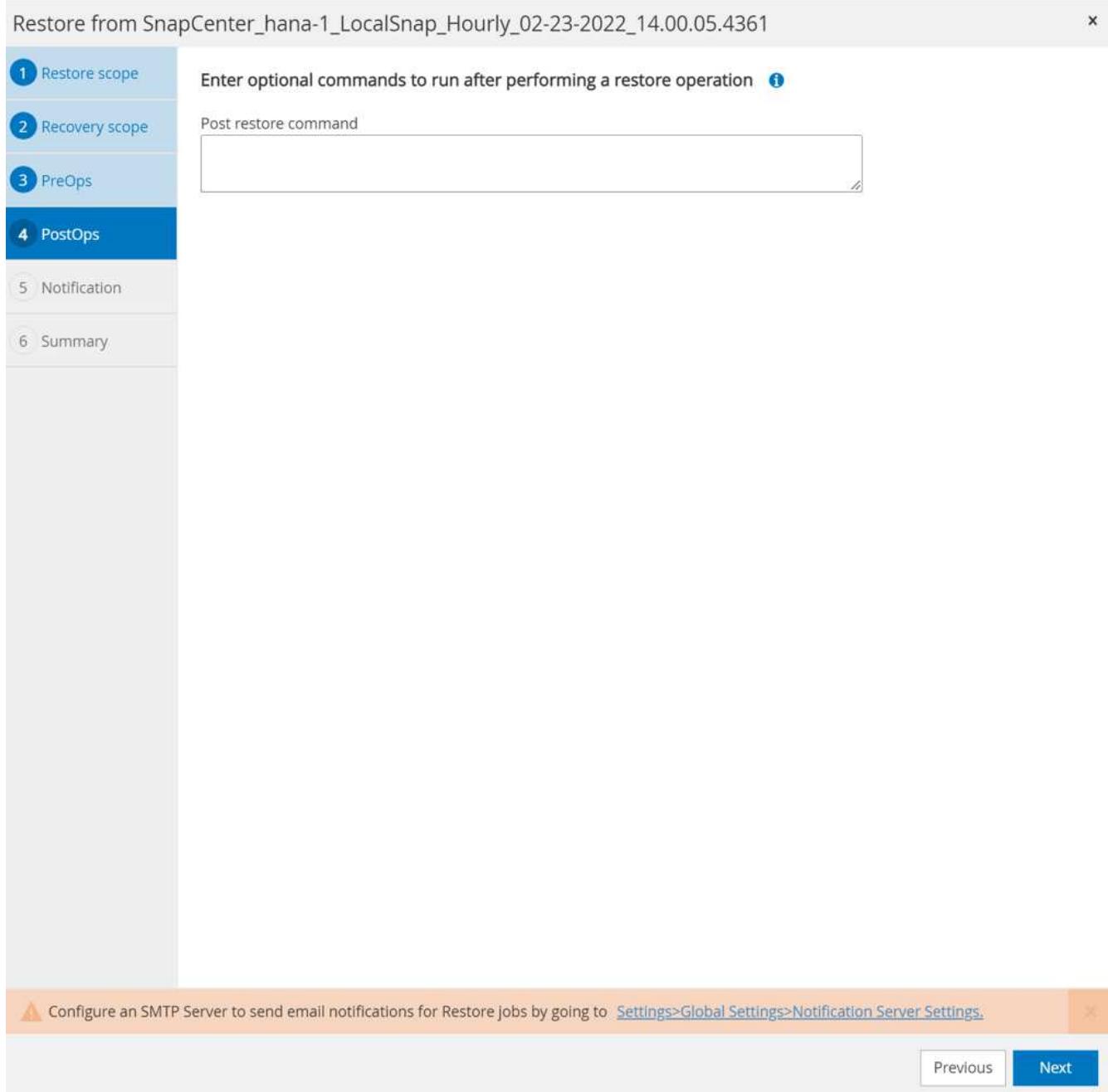
**5 Notification**

**6 Summary**

Post restore command

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

Previous Next



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

## Restore from SnapCenter\_hana-1\_LocalSnap\_Hourly\_02-23-2022\_14.00.05.4361

X

- 1 Restore scope
- 2 Recovery scope
- 3 PreOps
- 4 PostOps
- 5 Notification
- 6 Summary

### Summary

Backup Name	SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361
Backup date	02/23/2022 2:01:11 PM
Restore scope	Complete Resource with Volume Revert
Recovery scope	Recover to most recent state
Log backup locations	/backup/log
Backup catalog location	/backup/log
Pre restore command	
Post restore command	
Send email	No



If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

X

Previous

Finish

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

## Job Details

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

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

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

[View Logs](#)

[Cancel Job](#)

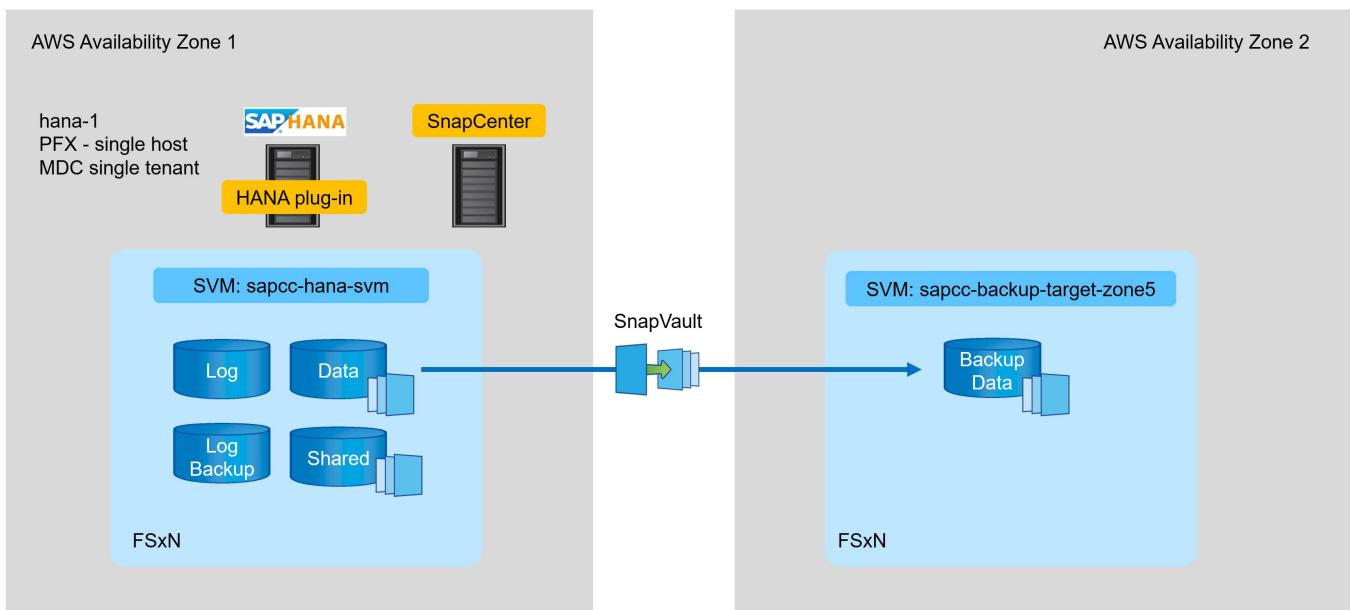
[Close](#)

# Backup-Replizierung mit SnapVault

## Übersicht - Backup-Replikation mit SnapVault

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

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



## Übersicht über die Konfigurationsschritte

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

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

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

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

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

In den folgenden Kapiteln werden die einzelnen Schritte detaillierter beschrieben.

## Konfigurieren Sie Replikationsbeziehungen auf FSX für ONTAP-Dateisysteme

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

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

## Peer-FSX für ONTAP-Filesysteme

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

```

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

```

```

FsxId05f7f00af49dc7a3e::> cluster peer create -address-family ipv4 -peer
-peer-addrs 10.1.1.57, 10.1.2.7

```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters. To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:

Confirm the passphrase:

Notice: Now use the same passphrase in the "cluster peer create" command in the other cluster.



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

```

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

```

## Peer-SVMs

```

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

```

```

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

```

```

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

```

## Erstellen eines Ziel-Volumes

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

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

## SnapMirror-Richtlinie erstellen

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

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

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

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

## SnapMirror Beziehung erstellen

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

```
FsxId05f7f00af49dc7a3e::> snapmirror create -source-path sapcc-hana-svm:PXF_data_mnt00001 -destination-path sapcc-backup-target-zone5:PXF_data_mnt00001 -vserver sapcc-backup-target-zone5 -throttle unlimited -identity-preserve false -type XDP -policy snapcenter-policy
Operation succeeded: snapmirror create for the relationship with destination "sapcc-backup-target-zone5:PXF_data_mnt00001".
```

## SnapMirror initialisieren

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

```
FsxId05f7f00af49dc7a3e::> snapmirror initialize -destination-path sapcc-backup-target-zone5:PXF_data_mnt00001 -source-path sapcc-hana-svm:PXF_data_mnt00001
Operation is queued: snapmirror initialize of destination "sapcc-backup-target-zone5:PXF_data_mnt00001".
```

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

```
FsxId05f7f00af49dc7a3e::> snapmirror show

Progress
Source          Destination Mirror Relationship Total
Last
Path           Type   Path       State    Status      Progress  Healthy
Updated
-----  -----  -----  -----  -----  -----  -----
sapcc-hana-svm:PXF_data_mnt00001
          XDP   sapcc-backup-target-zone5:PXF_data_mnt00001
                           Uninitialized
                           Transferring   1009MB   true
02/24 12:34:28
```

```
FsxId05f7f00af49dc7a3e::> snapmirror show

Progress
Source           Destination Mirror Relationship Total
Last
Path            Type    Path      State   Status       Progress  Healthy
Updated

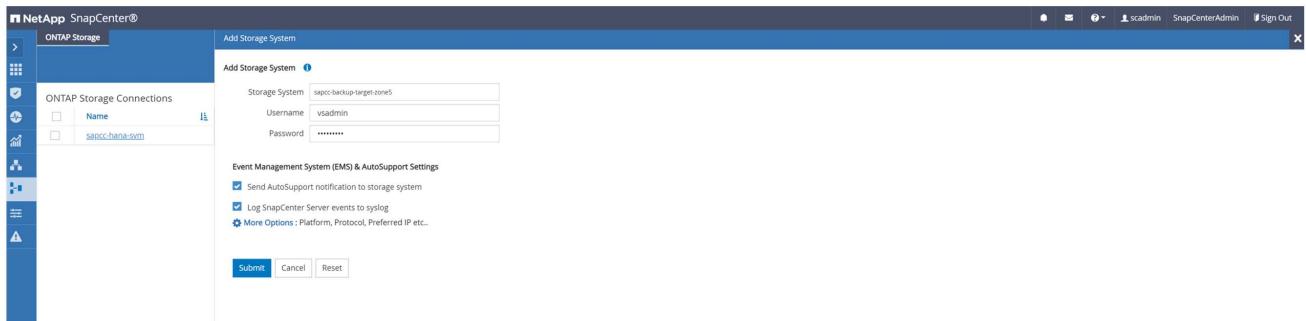
sapcc-hana-svm:PXF_data_mnt00001
XDP  sapcc-backup-target-zone5:PXF_data_mnt00001
                           Snapmirrored
                           Idle          -        true     -

```

## Fügen Sie eine Backup-SVM zu SnapCenter hinzu

So fügen Sie eine Backup-SVM zu SnapCenter hinzu:

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



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

## More Options

**Platform:** All Flash FAS

**Protocol:** HTTPS

**Port:** 443

**Timeout:** 60 seconds

Preferred IP

**Save** **Cancel**

Die SVM ist jetzt in SnapCenter verfügbar.

The screenshot shows the NetApp SnapCenter interface. On the left, there's a sidebar with icons for Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems (which is selected), Settings, and Alerts. The main area has a blue header bar with the title 'ONTAP Storage' and a search bar. Below the header, it says 'Type: ONTAP SVMs'. A table lists 'ONTAP Storage Connections' with columns for Name, IP, Cluster Name, User Name, Platform, and Controller License. Two entries are shown: 'sapcc-backup-target-zone5' (IP 10.1.2.31, Platform AFF, Not applicable) and 'sapcc-hana-svm' (IP 198.19.255.9, Platform AFF, checked). There are 'New' and 'Delete' buttons at the top right of the table.

## Erstellen einer neuen SnapCenter-Richtlinie für Backup-Replizierung

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

1. Geben Sie einen Namen für die Richtlinie ein.

The screenshot shows the NetApp SnapCenter interface with the 'Policies' tab selected in the top navigation bar. The sidebar remains the same. The main area shows a table of policies under the heading 'SAP HANA'. The columns are Name, Backup Type, Schedule Type, and Replication. Three policies are listed: 'BlockIntegrityCheck' (File Based Backup, Weekly), 'LocalSnap' (Data Backup, Hourly), and another unnamed row. There are 'New', 'Edit', 'Copy', 'Delete', and 'Details' buttons at the top right of the table.

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

New SAP HANA Backup Policy

**1 Name** Provide a policy name  
**2 Settings** Policy name: LocalSnapAndSnapVault  
**3 Retention** Details: Replication to backup volume  
**4 Replication**  
**5 Summary**

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

New SAP HANA Backup Policy

**1 Name**  
**2 Settings** Select backup settings  
 Backup Type:  Snapshot Based  File-Based

**3 Retention**  
**4 Replication**  
**5 Summary**

Schedule Frequency  
 Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.  
 On demand  
 Hourly  
 Daily  
 Weekly  
 Monthly

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

New SAP HANA Backup Policy

**1 Name**  
**2 Settings**  
**3 Retention** Retention settings  
 Daily retention settings  
 Total Snapshot copies to keep: 3   
 Keep Snapshot copies for: 14 days

**4 Replication**  
**5 Summary**

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

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

New SAP HANA Backup Policy

**1 Name** Select secondary replication options [i](#)

**2 Settings**  Update SnapMirror after creating a local Snapshot copy.

**3 Retention**  Update SnapVault after creating a local Snapshot copy.

**4 Replication** Secondary policy label [Custom Label](#) [i](#)  
snapcenter

**5 Summary** Error retry count 3 [i](#)

New SAP HANA Backup Policy

**1 Name** Summary

**2 Settings** Policy name LocalSnapAndSnapVault

**3 Retention** Details Replication to backup volume

**4 Replication** Backup Type Snapshot Based Backup

**5 Summary** Schedule Type Daily  
Daily backup retention Total backup copies to retain : 3  
Replication SnapVault enabled , Secondary policy label: Custom Label : snapcenter , Error retry count: 3

Die neue SnapCenter-Richtlinie ist jetzt konfiguriert.

Name	Backup Type	Schedule Type	Replication
BlockIntegrityCheck	File Based Backup	Weekly	
LocalSnap	Data Backup	Hourly	
LocalSnapAndSnapVault	Data Backup	Daily	SnapVault

## Fügen Sie eine Richtlinie zum Ressourcenschutz hinzu

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

Resource Application Settings Policies Notifications Summary

Select one or more policies and configure schedules

Policies	Schedules	Configure Schedules
LocalSnap, BlockIntegrityCheck	1	
LocalSnap	2	
BlockIntegrityCheck	3	
LocalSnapAndSnapVault	4	

Total 2

Ein täglicher Zeitplan wird in unserem Setup festgelegt.

The screenshot shows the NetApp SnapCenter interface. In the top navigation bar, 'SAP HANA' is selected under 'Search databases'. The main panel displays a 'Multitenant Database Container - Protect' topology. A horizontal navigation bar at the top of the main area shows five steps: 'Resource', 'Application Settings', 'Policies', 'Notification', and 'Summary'. Step 3, 'Policies', is highlighted. Below this, a section titled 'Select one or more policies and configure schedules' lists several policies: 'LocalSnap', 'BlockIntegrityCheck', 'LocalSnapAndVault', and others. A 'Configure Schedules' table shows the applied schedules for each policy. The table has columns for 'Policy', 'Applied Schedules', and 'Configure Schedules'. The 'Applied Schedules' column shows 'Weekly: Run on days: Sunday' for BlockIntegrityCheck and 'Hourly: Repeat every 6 hours' for LocalSnap. The 'Configure Schedules' column shows 'Daily: Repeat every 1 days' for LocalSnapAndVault. A note at the bottom indicates 'Total 3' scheduled tasks.

## Erstellen Sie ein Backup mit Replikation

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

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

A modal dialog box titled 'Backup' is shown. The title bar has a close button ('X'). The main content area is titled 'Create a backup for the selected resource'. It contains two input fields: 'Resource Name' with the value 'PFX' and 'Policy' with a dropdown menu set to 'LocalSnapAndSnapVault'. To the right of the policy dropdown is an information icon ('i'). At the bottom right of the dialog are two buttons: 'Cancel' and a blue 'Backup' button.

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

repliziert.

## Job Details

Backup of Resource Group 'hana-1\_hana\_MDC\_PFX' with policy 'LocalSnapAndSnapVault'

- ✓ ▾ Backup of Resource Group 'hana-1\_hana\_MDC\_PFX' with policy 'LocalSnapAndSnapVault'
  - ✓ ▾ hana-1
    - ✓ ▾ Backup
      - ▶ Validate Dataset Parameters
      - ▶ Validate Plugin Parameters
      - ▶ Complete Application Discovery
      - ▶ Initialize Filesystem Plugin
      - ▶ Discover Filesystem Resources
      - ▶ Validate Retention Settings
      - ▶ Quiesce Application
      - ▶ Quiesce Filesystem
      - ▶ Create Snapshot
      - ▶ UnQuiesce Filesystem
      - ▶ UnQuiesce Application
      - ▶ Get Snapshot Details
      - ▶ Get Filesystem Meta Data
      - ▶ Finalize Filesystem Plugin
      - ▶ Collect Autosupport data
      - ✓ ▶ Secondary Update
        - ▶ Register Backup and Apply Retention
        - ▶ Register Snapshot attributes
        - ▶ Application Clean-Up
        - ▶ Data Collection
        - ▶ Agent Finalize Workflow
    - ✓ ▾ ( Job 49 ) SnapVault update

Task Name: Secondary Update Start Time: 02/24/2022 3:14:37 PM End Time: 02/24/2022 3:14:46 PM

View Logs Cancel Job Close

Auf dem FSX für ONTAP Filesystem wird ein Snapshot auf dem Quell-Volume mit dem SnapMirror Label erstellt. snapcenter, Wie in der SnapCenter-Richtlinie konfiguriert.

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

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

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

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

**Backup Catalog**

Database: SYSTEMDB

Show Log Backups  Show Delta Backups

Status	Started	Duration	Size	Backup Type	Destination Ty...
Green	Apr 28, 2022, 4:22:06 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot
Green	Apr 28, 2022, 2:00:26 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot
Green	Apr 28, 2022, 8:00:35 AM	00h 00m 15s	5.50 GB	Data Backup	Snapshot
Green	Apr 15, 2022, 5:00:44 PM	00h 06m 59s	5.50 GB	Data Backup	Snapshot
Green	Apr 14, 2022, 8:00:32 PM	00h 00m 16s	5.50 GB	Data Backup	Snapshot
Green	Apr 5, 2022, 2:00:29 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot
Green	Apr 5, 2022, 8:00:39 AM	00h 00m 15s	5.50 GB	Data Backup	Snapshot
Green	Mar 31, 2022, 2:00:29 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot
Green	Mar 31, 2022, 1:10:57 PM	00h 00m 16s	5.50 GB	Data Backup	Snapshot
Green	Feb 22, 2022, 12:55:21 PM	00h 00m 21s	3.56 GB	Data Backup	File

**Backup Details**

ID: 1651162926424  
Status: Successful  
Backup Type: Data Backup  
Destination Type: Snapshot  
Started: Apr 28, 2022, 4:22:06 PM (UTC)  
Finished: Apr 28, 2022, 4:22:21 PM (UTC)  
Duration: 00h 00m 15s  
Size: 5.50 GB  
Throughput: n.a.  
System ID:  
Comment: SnapCenter\_hana-1\_LocalSnapAndSnapVault\_Daily\_04-28-2022\_16.21.41.5853  
Additional Information: <ok>  
Location: /hana/data/PFX/mnt00001/  
Host hana-1 Service nameserver Size 5.50 GB Name hdb00001 Source Type volume EBID SnapCent...  
Details Configure Database Refresh

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

## Wiederherstellung im Sekundär-Storage

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

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

Das Dialogfeld Wiederherstellen zeigt die sekundären Speicherorte an.

- 1** Restore scope
- 2** Recovery scope
- 3** PreOps
- 4** PostOps
- 5** Notification
- 6** Summary

**Select the restore types** Complete Resource i Tenant Database**Choose archive location**

sapcc-hana-svm:PFX\_data\_mnt0001

sapcc-backup-target-zone5:PFX\_data\_mnt00 ▾

⚠ The newer tenants added on the host after the backup was created cannot be restored and will be lost after restore operation.

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

[Previous](#)[Next](#)

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

## Wo Sie weitere Informationen finden

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

- FSX für NetApp ONTAP Benutzerhandbuch – Was ist Amazon FSX für NetApp ONTAP?  
<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html>
- Ressourcen-Seite zu SnapCenter

["https://www.netapp.com/us/documentation/snapcenter-software.aspx"](https://www.netapp.com/us/documentation/snapcenter-software.aspx)

- SnapCenter-Softwaredokumentation

["https://docs.netapp.com/us-en/snapcenter/index.html"](https://docs.netapp.com/us-en/snapcenter/index.html)

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

["Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter"](#)

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

["Backup und Recovery mit SnapCenter"](#)

## Versionsverlauf

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

## **Copyright-Informationen**

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

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

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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 IRGENDERINER 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.