Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter

NetApp solutions for SAP

NetApp
December 16, 2025

Inhalt

Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter

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

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

Autor: Nils Bauer, NetApp

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

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

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

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

Zusätzliche plattformspezifische Dokumentationen zu Best Practices sind verfügbar unter

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

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

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

Unternehmen benötigen heutzutage eine kontinuierliche und unterbrechungsfreie Verfügbarkeit ihrer SAP-Anwendungen. Sie erwarten ein gleichbleibendes Leistungsniveau und benötigen angesichts stetig wachsender Datenmengen und des Bedarfs an routinemäßigen Wartungsarbeiten, wie z. B. Systemsicherungen, einen automatisierten täglichen Betrieb. Die Durchführung von Backups von SAP-

Datenbanken ist eine kritische Aufgabe und kann erhebliche Auswirkungen auf die Leistung des produktiven SAP-Systems haben.

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

Datensicherung und Wiederherstellung mithilfe von Snapshot-Backups

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

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

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

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

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

SnapVault und ANF-Backups bieten im Vergleich zu herkömmlichen Backups erhebliche Vorteile. Nach einer ersten Datenübertragung, bei der alle Daten von der Quelle zum Ziel übertragen werden, werden bei allen nachfolgenden Backups nur die geänderten Blöcke auf den Sekundärspeicher repliziert. Dadurch werden die

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

Laufzeit von Snapshot-Backup- und -Restore-Vorgängen

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

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

[Breite=624, Höhe=267]

Vergleich der Recovery-Zeitvorgaben

Dieser Abschnitt bietet einen Vergleich der Wiederherstellungszeitziele (RTO) von dateibasierten und speicherbasierten Snapshot-Backups. Die RTO (Recovery Time Out) ist definiert als die Summe der Zeit, die für die Wiederherstellung, die Wiederherstellung und den anschließenden Start der Datenbank benötigt wird.

Benötigte Zeit zum Wiederherstellen der Datenbank

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

Bei NetApp Snapshot-Backups ist die Wiederherstellungszeit unabhängig von der Größe der Datenbank und liegt immer im Bereich von wenigen Sekunden.

Benötigte Zeit für das Recovery von Datenbanken

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

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

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

Benötigte Zeit zum Starten der Datenbank

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

Wiederherstellungs- und Recovery-Beispielberechnung

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

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

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

[Breite=624, Höhe=326]

Anwendungsfälle und Vorteile beschleunigter Backup- und Klonvorgänge

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

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

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

[Breite=618, Höhe=279]

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

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

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

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

[Breite=627, Höhe=328]

Erfahren Sie mehr über die SnapCenter -Architektur.

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

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

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

[Breite=601, Höhe=275]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[Breite=601, Höhe=285]

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

[Breite=601, Höhe=278]

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

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

Unterstützte SAP HANA-Konfigurationen

SnapCenter unterstützt die folgenden HANA-Konfigurationen und -Funktionen:

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

Unterstützte Plattform- und Infrastrukturkonfigurationen

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

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

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

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

Unterstützte Funktionen und Vorgänge

Abkürzungserklärung

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

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

ONTAP AFF und FSx für ONTAP

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

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

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

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

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

ONTAP ASA

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

(*): Unterstützung ab SnapCenter Version 6.2

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

Azure NetApp Dateien

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

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

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

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

Bereitstellungsoptionen für das SnapCenter -Plug-in für SAP HANA

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

[Breite=601, Höhe=199]

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

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

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

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

- VMware mit FC-Datenspeichern
- SnapMirror aktive Synchronisierung

- SnapCenter Server hohe Verfügbarkeit bei Verwendung als zentraler Plug-in-Host
- Automatische Erkennung von HANA-Systemen
- Automatisierte Wiederherstellung der HANA-Datenbank
- Automatisierte SAP-Systemaktualisierung
- Wiederherstellung für Einzelmandanten

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

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

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

[Breite=601, Höhe=304]

Hochverfügbarkeit mit SnapCenter Server

SnapCenter kann in einer HA-Konfiguration mit zwei Knoten eingerichtet werden. Bei einer solchen Konfiguration wird ein Load Balancer (z. B. F5) verwendet, um auf die SnapCenter -Hosts zuzugreifen. Das SnapCenter Repository (die MySQL-Datenbank) wird von SnapCenter zwischen den beiden Hosts repliziert, sodass die SnapCenter -Daten immer synchron sind.

SnapCenter Server HA wird nicht unterstützt, wenn das HANA-Plug-in auf dem SnapCenter Server installiert ist. Weitere Details zu SnapCenter HA finden Sie unter "Konfigurieren Sie SnapCenter -Server für hohe Verfügbarkeit"Die

[Breite=601, Höhe=307]

Zentraler Plug-in-Host

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

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

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

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

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

[Breite=601, Höhe=314]

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

[Breite=601, Höhe=338]

SAP HANA Blockkonsistenzprüfung

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

Technisch gesehen gibt es zwei Möglichkeiten, die Blockkonsistenzprüfung durchzuführen.

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

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

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

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

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

Datensicherung Strategie

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

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

Folgende Parameter müssen definiert werden:

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

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

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

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

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

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

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

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

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

[Breite=601, Höhe=192]

Sicherung der Verschlüsselungs-Root-Schlüssel

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

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

Backup-Vorgänge

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

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

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

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

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

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

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

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

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

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

[Breite=601, Höhe=237]

Backup-Aufbewahrungsverwaltung

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

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

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

[Breite=601, Höhe=309]

Aufbewahrungsmanagement von lokalen Backups auf dem Primärstorage

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

Aufbewahrungsmanagement von dateibasierten Backups

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

Aufbewahrungsverwaltung von Backups im Sekundärspeicher (SnapVault)

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

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

Aufbewahrungsverwaltung von Backups auf dem Sekundärspeicher (ANF-Backup)

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

Aufbewahrungsmanagement von Daten-Backups im SAP HANA Backup-Katalog

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

Aufbewahrungsmanagement von Protokoll-Backups

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

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

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

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

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

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

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

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

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

Die folgende Abbildung veranschaulicht die verschiedenen Konfigurationskomponenten und ihre Abhängigkeiten.

Alle Konfigurationsschritte werden in den folgenden Abschnitten detailliert beschrieben.

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

[Breite=601, Höhe=319]

Konfigurieren Sie die anfänglichen SnapCenter -Einstellungen für SAP HANA

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

Die Erstkonfiguration von SnapCenter umfasst die folgenden Schritte:

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

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

Die folgende Abbildung fasst die Konfigurationsabschnitte zusammen.

[Breite=601, Höhe=158]

Die folgenden Kapitel beschreiben die ersten Konfigurationsschritte.

Konfiguration von Anmeldeinformationen

Anmeldeinformationen für die HANA-Plug-in-Bereitstellung

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

[Breite=601, Höhe=118]

NetApp empfiehlt, auf allen HANA-Datenbankhosts einen Benutzer (z. B. scuser) zu konfigurieren und die

sudo-Berechtigungen wie beschrieben einzurichten. "Voraussetzungen für das Hinzufügen von Hosts und die Installation des SnapCenter -Plug-ins für die SAP HANA-Datenbank"Die

[Breite=287, Höhe=247]

Anmeldeinformationen für Azure NetApp Files

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

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

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

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

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

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

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

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/breakFileLocks/acti
```

```
on",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/getGroupIdListForLd
apUser/action",

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
            "Microsoft.NetApp/locations/operationresults/read",
            "Microsoft.NetApp/Operations/read",
            "Microsoft.Resources/resources/read",
            "Microsoft.Resources/subscriptions/resourceGroups/read",

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

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

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

[Breite=601, Höhe=116]

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

[Breite=252, Höhe=246]

Konfiguration des Storage-Systems

ONTAP Systeme und FSx für ONTAP

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

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

[Breite=601, Höhe=117]

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

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

[Breite=299, Höhe=176]

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

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

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

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

[Breite=331, Höhe=199]

Azure NetApp Dateien

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

[Breite=601, Höhe=117]

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

[Breite=401, Höhe=176]

Speicherkonfiguration bei Verwendung von SnapMirror ActiveSync

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

Konfiguration von Richtlinien

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

Eine typische Minimalkonfiguration umfasst folgende Richtlinien:

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

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

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

[Breite=601, Höhe=133]

[Breite=601, Höhe=138]

Snapshot-Backups mit ONTAP -Systemen und FSx für ONTAP

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

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

[Breite=376, Höhe=103]

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

[Breite=385, Höhe=97]

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

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

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

Replikationsbeziehung konfigurierten Bezeichnung übereinstimmen.

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

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

[Breite=378, Höhe=352]

Die Übersichtsseite zeigt die konfigurierten Parameter an.

[Breite=385, Höhe=119]

Snapshot-Backups mit Azure NetApp Files

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

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

[Breite=356, Höhe=95]

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

[Breite=360, Höhe=102]

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

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

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

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

[Breite=373, Höhe=361]

Die Übersichtsseite zeigt die konfigurierten Parameter an.

[Breite=376, Höhe=138]

Blockintegritätsprüfungsvorgänge für alle Plattformen

HANA-Tool hdbpersdiag

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

Dateibasierte Datensicherung

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

[Breite=346, Höhe=95]

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

[Breite=357, Höhe=98]

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

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

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

[Breite=351, Höhe=173]

Die Übersichtsseite zeigt die konfigurierten Parameter an.

[Breite=366, Höhe=101]

Richtlinienkonfiguration bei Verwendung von SnapMirror ActiveSync

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

SnapCenter Ressourcen für einzelne SAP HANA-Datenbanken konfigurieren

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

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

1. In der HANA-Systemdatenbank muss ein SnapCenter Backup-Benutzer konfiguriert und auf dem HANA-Datenbankhost ein SAP-HANA-Benutzerspeicherschlüssel eingerichtet werden.
2. Wenn eine Datenreplikation auf einen Sekundärspeicher erforderlich ist, muss die ONTAP -Speicherreplikation für das HANA-Datenvolume konfiguriert werden.
3. Das SnapCenter HANA-Plug-in muss auf dem HANA-Datenbankhost bereitgestellt werden.
    a. Der automatische Erkennungsprozess wird gestartet
    b. Der SAP HANA-Benutzerspeicherschlüssel muss in SnapCenter konfiguriert werden.

c. Die zweite Phase der automatischen Erkennung wird gestartet und die HANA-Ressource wird von SnapCenter automatisch hinzugefügt.

4. Der HANA-Ressourcenschutz muss für die neu hinzugefügte HANA-Ressource konfiguriert werden.

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

Die folgende Abbildung veranschaulicht die verschiedenen Konfigurationskomponenten und Abhängigkeiten.

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

SAP HANA Backup-Benutzer- und SAP HANA Benutzerspeicherkonfiguration

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

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

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

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

[Breite=601, Höhe=382]

SAP HANA-Benutzerspeicherkonfiguration auf dem HANA-Datenbankhost

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

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

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

SAP HANA Benutzerspeicherkonfigurationsbeispiele

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

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

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

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

Speicherreplikationskonfiguration

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

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

Die folgende Abbildung zeigt die konfigurierte Schutzbeziehung für das Datenvolumen des SAP HANA-Systems SS1. In diesem Beispiel wird das Quellvolume SS1_data_mnt00001 auf dem SVM hana-primary auf das SVM hana-backup und das Zielvolume SS1_data_mnt00001_dst repliziert.

[Breite=601, Höhe=183]

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

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

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

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

[Breite=601, Höhe=180]

ANF-Backup-Konfiguration

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

[Breite=601, Höhe=227]

Bereitstellung des SnapCenter -Plug-ins für SAP HANA

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

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

[Breite=601, Höhe=145]

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

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

[Breite=601, Höhe=154]

HANA-Autoerkennung

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

[Breite=601, Höhe=169]

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

[Breite=316, Höhe=180]

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

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

[Breite=601, Höhe=219]

Konfiguration für Ressourcenschutz

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

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

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

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

[Breite=601, Höhe=294]

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

[Breite=601, Höhe=294]

Nun werden Richtlinien mit den Ressourcen verknüpft und Zeitpläne definiert.

In diesem Beispiel haben wir Folgendes konfiguriert:

- Wöchentliche Überprüfung der Blockintegrität, jeden Sonntag

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

[Breite=601, Höhe=294]

E-Mail-Benachrichtigungen können konfiguriert werden.

[Breite=601, Höhe=294]

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

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

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

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

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

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

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

[Breite=601, Höhe=173]

[Breite=601, Höhe=112]

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

[Breite=332, Höhe=310]

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

[Breite=332, Höhe=312]

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

[Breite=350, Höhe=337]

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

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

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

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

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

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

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

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

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

SnapCenter HANA-Plug-in-Bereitstellung

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

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

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

[Breite=601, Höhe=166]

Installation und Konfiguration der SAP HANA hdbsql Client-Software

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

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

Zentraler Plug-in-Host unter Windows:

```
C:\More C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in
Creator\etc\hana.properties

HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql.exe
```

Zentraler Plugin-Host unter Linux:

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

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

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

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

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

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

Bei einer SAP HANA-Umgebung mit mehreren Hosts müssen die SAP HANA-Benutzerspeicherschlüssel für alle Hosts konfiguriert werden. SnapCenter versucht, mit jedem der bereitgestellten Schlüssel eine Verbindung zur Datenbank herzustellen und kann daher unabhängig von einem Failover der Systemdatenbank (HANA-

Namensserver) auf einen anderen Host funktionieren. Für alle Worker- und Standby-Hosts ist ein SAP HANA-Benutzerspeicherschlüssel konfiguriert. Der HANA-Datenbankbenutzer, in diesem Beispiel SNAPCENTER, ist der Benutzer, der in der Systemdatenbank konfiguriert wurde.

```
hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER
password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE : C:\ProgramData\.hdb\SNAPCENTER-61\S-1-5-18\SSFS_HDB.DAT
KEY FILE : C:\ProgramData\.hdb\SNAPCENTER-61\S-1-5-18\SSFS_HDB.KEY
KEY MS1KEYHOST1
ENV : hana-4:30013
USER: SNAPCENTER
KEY MS1KEYHOST2
ENV : hana-5:30013
USER: SNAPCENTER
KEY MS1KEYHOST3
ENV : hana-6:30013
USER: SNAPCENTER
KEY SS2KEY
ENV : hana-3:30013
USER: SNAPCENTER

C:\Program Files\sap\hdbclient>
```

Manuelle HANA-Ressourcenkonfiguration

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

[Breite=601, Höhe=189]

Im nächsten Bildschirm müssen Sie einige Systemparameter angeben.

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

[Breite=384, Höhe=357]

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

[Breite=385, Höhe=359]

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

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

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

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

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

SnapCenter unterstützt die folgenden Sicherungsvorgänge.

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

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

SAP HANA Snapshot-Backups in SnapCenter

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

[Breite=601, Höhe=293]

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

[Breite=601, Höhe=294]

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

[Breite=601, Höhe=293]

SAP HANA Snapshot-Backups in SAP HANA Studio

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

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

[Breite=601, Höhe=289]

[Breite=601, Höhe=296]

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

SAP HANA Snapshot-Backups auf der Speicherschicht

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

[Breite=601, Höhe=294]

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

[Breite=601, Höhe=294]

SAP HANA Snapshot-Backups mit ANF

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

[Breite=601, Höhe=303]

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

[Breite=601, Höhe=258]

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

[Breite=601, Höhe=304]

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

[Breite=601, Höhe=216]

Snapshot-Backups von Nicht-Datenvolumes

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

[Breite=601, Höhe=294]

Backup-Workflow für HANA-Datenbanksicherungen

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

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

[Breite=339, Höhe=475]

Backup-Workflow für Nicht-Datenvolumes

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

[Breite=329, Höhe=404]

Bereinigung sekundärer Backups

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

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

[Breite=601, Höhe=158]

[Breite=267, Höhe=330]

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

Ändern Sie die Häufigkeit des SnapCenter-Bereinigungsjobs

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

```
SnapCenterPS C:\> Open-SmConnection

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

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

TaskName : SnapCenter_RemoveSecondaryBackup
Hosts : {}
StartTime : 8/25/2025 3:45:00 AM
DaysoftheMonth :
MonthsofTheYear :
DaysInterval : 1
DaysOfTheWeek :
AllowDefaults : False
ReplaceJobIfExist : False
UserName :
Password :
SchedulerType : Daily
RepeatTask_Every_Hour : 1
```

```
IntervalDuration :
EndTime :
LocalScheduler : False
AppType : False
AuthMode :
SchedulerSQLInstance : SMCoreContracts.SmObject
MonthlyFrequency :
Hour : 0
Minute : 0
NodeName :
ScheduleID : 0
RepeatTask_Every_Mins :
CronExpression :
CronOffsetInMinutes :
StrStartTime :
StrEndTime :
ScheduleCategory :
PolicyId : 0
PolicyName :
ProtectionGroupId : 0
ProtectionGroupName :
PluginCode : NONE
PolicyType : None
ReportTriggerName :
PolicyScheduleId : 0
HoursOfTheDay :
DayStartTime :
MinuteOffset : ZeroMinutes
SnapMirrorLabel :
BackupType :
SnapCenterPS C:\>
```

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

[Breite=601, Höhe=257]

Manuelle Aktualisierung auf Ressourcenebene

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

[Breite=601, Höhe=291]

Führen Sie SAP HANA-Blockkonsistenzprüfungen mit SnapCenter durch.

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

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

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

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

Konsistenzprüfungen mit hdbpersdiag unter Verwendung des lokalen Snapshot-Verzeichnisses

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

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

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

Die folgende Abbildung zeigt das übergeordnete Konzept der Konsistenzprüfungsimplementierung.

[Breite=601, Höhe=248]

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

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

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

[Breite=414, Höhe=103]

[Breite=424, Höhe=108]

[Breite=433, Höhe=336]

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

[Breite=601, Höhe=281]

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

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

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

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

Die folgende Ausgabe zeigt die Protokolldatei des Skripts:

```
20251024055824###hana-1###call-hdbpersdiag.sh: Current policy is
SnapAndCallHdbpersdiag
20251024055824###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001
20251024055827###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001/ (4.8 GB,
5100273664 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (94276 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
```

```
UndoContainerDirectory OK
LobDirectory OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251024055827###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00001.
20251024055827###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003
20251024055828###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003/
(320.0 MB, 335544320 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (4099 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
UndoContainerDirectory OK
DRLoadedTable OK
20251024055828###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00002.00003.
20251024055828###hana-1###call-hdbpersdiag.sh: Executing hdbpersdiag in:
/hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003
20251024055833###hana-1###call-hdbpersdiag.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/SS1/HDB00/hana-1/trace
Mounted DataVolume(s)
```

```
#0 /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003/
(4.6 GB, 4898947072 bytes)
WARNING: The data volume being accessed is in use by another process, this
is most likely because a running HANA instance is operating on this data
volume
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
Static Converter Pages OK
RowStore Converter Pages OK
Logical Pages (100817 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
DRLoadedTable OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251024055833###hana-1###call-hdbpersdiag.sh: Consistency check operation
successeful for volume /hana/data/SS1/mnt00001/.snapshot/SnapCenter_hana-
1_SnapAndCallHdbpersdiag_Daily_10-24-2025_05.57.37.0274/hdb00003.00003.
20251024060048###hana-1###call-hdbpersdiag.sh: Current policy is
LocalSnapAndSnapVault, consistency check is only done with Policy
SnapAndCallHdbpersdiag
20251024080048###hana-1###call-hdbpersdiag.sh: Current policy is
LocalSnap, consistency check is only done with Policy SnapAndHdbpersdiag
```

Konsistenzprüfungen mit hdbpersdiag unter Verwendung eines zentralen Verifizierungshosts

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

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

[Breite=601, Höhe=257]

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

Erste einmalige Vorbereitungsschritte:

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

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

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

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

Manuelle Workflow-Ausführung

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

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

[Breite=601, Höhe=247]

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

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

[Breite=431, Höhe=115]

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

[Breite=442, Höhe=169]

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

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

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

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

```
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag for source system SS2.
```

```
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Clone mounted at
/hana/data/QS1/mnt00001.
20251029112557###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00001
20251029112600###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00001/ (3.1 GB, 3361128448 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (65388 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251029112600###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00001.
20251029112601###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00002.00003
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00002.00003/ (288.0 MB, 301989888 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
```

```
Default Converter Pages OK
RowStore Converter Pages OK
Logical Pages (4099 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
UndoContainerDirectory OK
DRLoadedTable OK
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00002.00003.
20251029112602###hana-7###call-hdbpersdiag-flexclone.sh: Executing
hdbpersdiag in: /hana/data/QS1/mnt00001/hdb00003.00003
20251029112606###hana-7###call-hdbpersdiag-flexclone.sh: Loaded library
'libhdbunifiedtable'
Loaded library 'libhdblivecache'
Trace is written to: /usr/sap/QS1/HDB11/hana-7/trace
Mounted DataVolume(s)
#0 /hana/data/QS1/mnt00001/hdb00003.00003/ (3.7 GB, 3942645760 bytes)
Tips:
Type 'help' for help on the available commands
Use 'TAB' for command auto-completion
Use '|' to redirect the output to a specific command.
INFO: KeyPage loaded and decrypted with success
Default Anchor Page OK
Restart Page OK
Default Converter Pages OK
Static Converter Pages OK
RowStore Converter Pages OK
Logical Pages (79333 pages) OK
Logical Pages Linkage OK
Checking entries from restart page...
ContainerDirectory OK
ContainerNameDirectory OK
FileIDMappingContainer OK
UndoContainerDirectory OK
LobDirectory OK
DRLoadedTable OK
MidSizeLobDirectory OK
LobFileIDMap OK
20251029112606###hana-7###call-hdbpersdiag-flexclone.sh: Consistency check
operation successful for volume /hana/data/QS1/mnt00001/hdb00003.00003.
```

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

[Breite=279, Höhe=344]

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

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

[Breite=601, Höhe=165]

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

SnapCenter Workflow-Automatisierung mithilfe von PowerShell-Skripten

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

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

Das PowerShell-Beispielskript führt den folgenden Arbeitsablauf aus.

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

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

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

C:\Users\scadmin>
```

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

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

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

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

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

Dateibasierte Datensicherung

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

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

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

[Breite=601, Höhe=293]

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

[Breite=601, Höhe=293]

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

[Breite=351, Höhe=433]

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

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

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

Wiederherstellung und Datenrettung von SAP HANA-Datenbanken mit SnapCenter

Wiederherstellung und Instandsetzung von SAP HANA-Systemen mit SnapCenter mittels automatisierter oder manueller Wiederherstellungsoptionen. Dies umfasst vollständige Systemwiederherstellungen, Wiederherstellungen einzelner Mandanten für HANA-Datenbanken auf ONTAP, Azure NetApp Files und FSx für ONTAP.

SnapCenter unterstützt die folgenden Wiederherstellungs- und Reparaturvorgänge.

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

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

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

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

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

[Breite=601, Höhe=294]

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

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

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

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

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

[Breite=300]

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

[Breite=345, Höhe=325]

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

[Breite=345, Höhe=323]

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

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

[Breite=346, Höhe=324]

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

[Breite=348, Höhe=326]

[Breite=359, Höhe=335]

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

[Breite=361, Höhe=336]

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

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

- Recovery von Mandanten-Datenbanken

[Breite=357, Höhe=439]

Manuelle Wiederherstellung mit HANA Studio

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

1. Vorbereitung des Restore- und Recovery-Prozesses mit SAP HANA Studio:
   a. Wählen Sie Recover System Database und bestätigen Sie das Herunterfahren des SAP HANA-Systems.
   b. Wählen Sie den Wiederherstellungstyp aus und geben Sie den Speicherort des Sicherungskatalogs an.
   c. Es wird eine Liste der Daten-Backups angezeigt. Wählen Sie Backup, um die externe Backup-ID anzuzeigen.
2. Führen Sie den Wiederherstellungsprozess mit SnapCenter aus:
   a. Wählen Sie in der Topologieansicht der Ressource „Lokale Kopien“ aus, um Daten vom primären Speicher wiederherzustellen, oder „Vault-Kopien“, wenn Sie Daten von einem sekundären Sicherungsspeicher wiederherstellen möchten.
   b. Wählen Sie das SnapCenter Backup aus, das mit der externen Backup-ID oder dem Kommentarfeld aus SAP HANA Studio übereinstimmt.
   c. Starten Sie den Wiederherstellungsprozess.
3. Führen Sie den Recovery-Prozess für die Systemdatenbank mit SAP HANA Studio aus:
   a. Klicken Sie in der Backup-Liste auf Aktualisieren, und wählen Sie das verfügbare Backup für die Recovery aus (wird durch ein grünes Symbol angezeigt).
   b. Starten Sie den Wiederherstellungsprozess. Nach Abschluss des Wiederherstellungsprozesses wird die Systemdatenbank gestartet.
4. Führen Sie den Recovery-Prozess für die Mandantendatenbank mit SAP HANA Studio aus:
   a. Wählen Sie die Option „Tenant Database wiederherstellen“ und wählen Sie den Mieter aus, der wiederhergestellt werden soll.
   b. Wählen Sie den Wiederherstellungstyp und den Speicherort für die Protokollsicherung aus.
   c. Es wird eine Liste der Daten-Backups angezeigt. Da das Daten-Volume bereits wiederhergestellt ist, wird das Mandanten-Backup als verfügbar angezeigt (in grün).
   d. Wählen Sie dieses Backup aus, und starten Sie den Wiederherstellungsprozess. Nach Abschluss des Recovery-Prozesses wird die Mandantendatenbank automatisch gestartet.
5. Bei einem HANA-System mit mehreren Mandanten wiederholen Sie Schritt 4 für jeden Mandanten.

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

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

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

[Breite=450, Höhe=368]

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

[Breite=349, Höhe=83]

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

[Breite=345, Höhe=359]

Geben Sie einen alternativen Speicherort für den Katalog an.

[Breite=343, Höhe=356]

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

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

[Breite=391, Höhe=283]

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

[Breite=601, Höhe=294]

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

[Breite=346, Höhe=325]

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

[Breite=358, Höhe=336]

Klicken Sie auf Fertigstellen, um den Wiederherstellungsvorgang zu starten.

[Breite=361, Höhe=339]

SnapCenter führt jetzt den Wiederherstellungsvorgang aus.

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

[Breite=322, Höhe=398]

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

Wiederherstellung werden die Dateien von der HANA-Datenbank gelöscht.

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

Gehen Sie zu SAP HANA Studio und klicken Sie auf Aktualisieren, um die Liste der verfügbaren Backups zu aktualisieren. Das mit SnapCenter wiederhergestellte Backup wird nun in der Backup-Liste mit einem grünen Symbol angezeigt. Wählen Sie die Sicherung aus und klicken Sie auf Weiter.

[Breite=400, Höhe=290]

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

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

[Breite=465, Höhe=296]

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

[Breite=466, Höhe=296]

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

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

[Breite=464, Höhe=295]

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

[Breite=376, Höhe=239]

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

[Breite=476, Höhe=315]

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

[Breite=342, Höhe=355]

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

[Breite=343, Höhe=356]

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

[Breite=342, Höhe=355]

Bestätigen Sie, dass die Mandantendatenbank heruntergefahren wurde.

[Breite=348, Höhe=85]

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

[Breite=433, Höhe=349]

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

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

[Breite=384, Höhe=310]

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

[Breite=384, Höhe=310]

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

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

[Breite=380, Höhe=307]

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

[Breite=378, Höhe=305]

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

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

Manuelle Wiederherstellung mit SQL-Befehlen

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

Zuerst müssen Sie die Systemdatenbank wiederherstellen.

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

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

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

Wiederherstellung und Recovery für einzelne Mandanten

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

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

1. Vorbereitung des Restore- und Recovery-Prozesses mit SAP HANA Studio:
   a. Wählen Sie „Mandantendatenbank wiederherstellen“ und bestätigen Sie das Herunterfahren der Mandantendatenbank.
   b. Wählen Sie den Wiederherstellungstyp aus und geben Sie den Speicherort des Sicherungskatalogs an.
   c. Es wird eine Liste der Daten-Backups angezeigt. Wählen Sie Backup, um die externe Backup-ID anzuzeigen.
2. Führen Sie den Wiederherstellungsprozess mit SnapCenter aus:

a. Wählen Sie in der Topologieansicht der Ressource „Lokale Kopien“ aus, um Daten vom primären Speicher wiederherzustellen, oder „Vault-Kopien“, wenn Sie Daten von einem sekundären Sicherungsspeicher wiederherstellen möchten.

b. Wählen Sie das SnapCenter Backup aus, das mit der externen Backup-ID oder dem Kommentarfeld aus SAP HANA Studio übereinstimmt.

c. Starten Sie den Wiederherstellungsprozess des Mandanten.

3. Führen Sie den Recovery-Prozess für die Mandantendatenbank mit SAP HANA Studio aus:

a. Klicken Sie in der Backup-Liste auf Aktualisieren, und wählen Sie das verfügbare Backup für die Recovery aus (wird durch ein grünes Symbol angezeigt).

b. Starten Sie den Wiederherstellungsprozess. Nach Abschluss des Wiederherstellungsprozesses wird die Mandantendatenbank gestartet.

Wiederherstellung von Nicht-Datenvolumes

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

[Breite=601, Höhe=294]

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

[Breite=369, Höhe=344]

Erweiterte SnapCenter Optionen für SAP HANA konfigurieren

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

Warnmeldung bei virtualisierten Umgebungen und Gast-Mounts

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

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

[Breite=601, Höhe=176]

Deaktivieren der automatischen Backup-Organisation für Protokolle

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

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

Sichere Kommunikation mit HANA-Datenbank ermöglichen

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

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

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

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

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

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

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

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

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

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

Für einen HANA-Host hana-2 lautet der Befehl wie folgt:

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

Name Value

---- -----

DISABLE_AUTO_DISCOVERY true

PS C:\Users\administrator.SAPCC>

Verify the configuration by running the Get- SmConfigSettings command.

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

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

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

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

Key: DISABLE_AUTO_DISCOVERY Value: true Details:

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

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

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

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