



Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter

NetApp Solutions SAP

NetApp
September 11, 2024

Inhalt

- Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter 1
 - TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter 1
 - SAP Szenarien für Systemkopie, Aktualisierung und Klonen 3
 - Anwendungsfälle für Systemaktualisierung und Klonen 3
 - Unterstützte Infrastruktur und Szenarien 7
 - Überblick über den Workflow zur SAP Systemaktualisierung mit SnapCenter 7
 - Überblick über den SAP Systemklonen-Workflow mit SnapCenter 10
 - Überlegungen zu Systemaktualisierungen für SAP HANA mit Storage-Snapshot-Backups 11
 - Beispielskripte zur Automatisierung 16
 - Systemaktualisierung für SAP HANA mit SnapCenter 19
 - SAP Systemklon mit SnapCenter 45
 - Wo finden Sie weitere Informationen und Versionsverlauf 59

Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter

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

Nils Bauer, NetApp

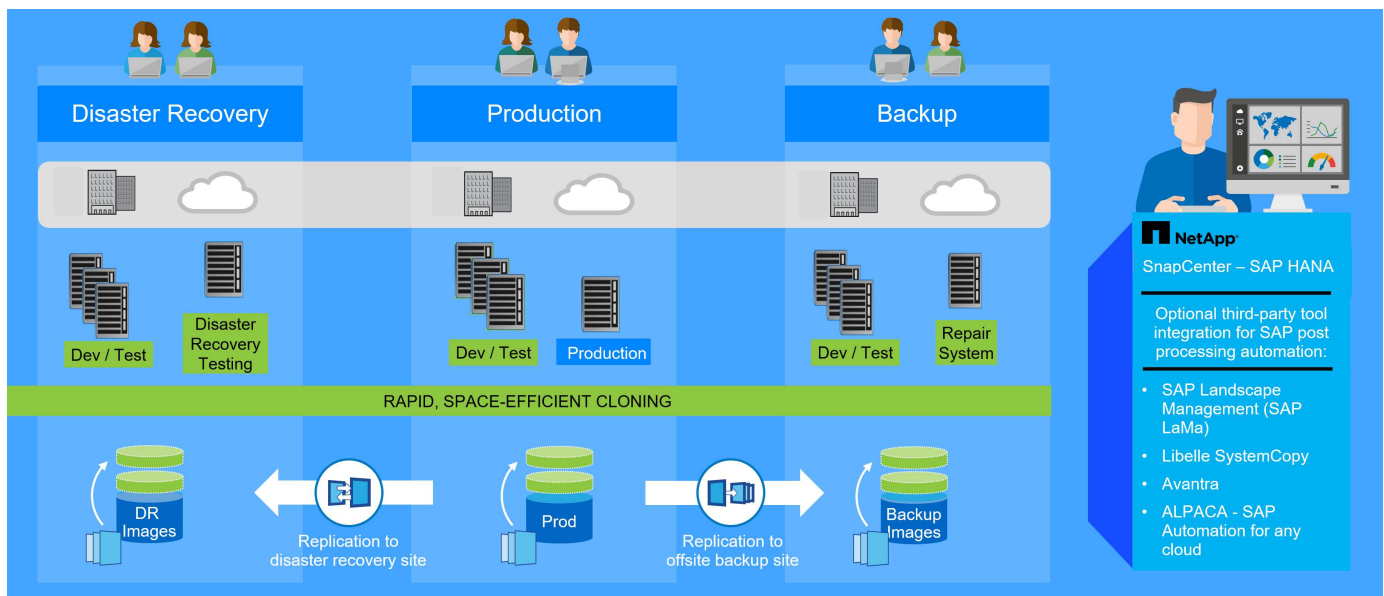
Einführung

Im dynamischen Geschäftsumfeld von heute müssen Unternehmen kontinuierlich Innovationen liefern und schnell auf sich ändernde Märkte reagieren. Unter diesen Wettbewerbsbedingungen können sich Unternehmen, die mehr Flexibilität in ihren Arbeitsprozessen implementieren, effektiver an die Marktanforderungen anpassen.

Wechselnde Marktanforderungen betreffen auch die SAP-Umgebungen eines Unternehmens, so dass sie regelmäßige Integrationen, Änderungen und Updates erfordern. DIE IT-Abteilungen müssen diese Veränderungen mit weniger Ressourcen und über kürzere Zeiträume hinweg umsetzen. Die Minimierung des Risikos bei der Implementierung dieser Änderungen erfordert gründliche Tests und Schulungen, für die zusätzliche SAP-Systeme mit tatsächlichen Daten aus der Produktion erforderlich sind.

Herkömmliche Ansätze für das SAP Lifecycle Management zur Bereitstellung dieser Systeme basieren in erster Linie auf manuellen Prozessen. Diese manuellen Prozesse sind oft fehleranfällig und zeitaufwendig, wodurch Innovationen und die Reaktion auf geschäftliche Anforderungen verzögert werden.

NetApp Lösungen zur Optimierung des SAP Lifecycle Managements sind in SAP HANA Datenbank- und Lifecycle-Management-Tools integriert und kombinieren effiziente applikationsintegrierte Datensicherung mit der flexiblen Bereitstellung von SAP Testsystemen, wie in der folgenden Abbildung dargestellt. Diese Lösungen sind für SAP HANA verfügbar, die lokal oder in der Cloud ausgeführt werden – On-Premises Azure NetApp Files (ANF) oder Amazon FSX for NetApp ONTAP (FSX for ONTAP).



Applikationsintegrierte Snapshot Backup-Vorgänge

Die Fähigkeit, applikationskonsistente Snapshot Backups auf Storage-Ebene zu erstellen, ist die Grundlage für die in diesem Dokument beschriebenen Systemkopien- und Systemklonvorgänge. Storage-basierte Snapshot Backups werden mit dem NetApp SnapCenter Plug-in für SAP HANA und Schnittstellen der SAP HANA Datenbank erstellt. SnapCenter registriert Snapshot-Backups im SAP HANA Backup-Katalog, sodass die Backups für Restore, Recovery und Klonvorgänge verwendet werden können.

Standortexterne Backup- und/oder Disaster Recovery-Datenreplikation

Applikationskonsistente Snapshot Backups können auf der Storage-Ebene zu einem externen Backup-Standort oder einem durch SnapCenter kontrollierten Disaster Recovery-Standort repliziert werden. Die Replizierung basiert auf geänderten und neuen Blöcken und ist damit Platz- und bandbreiteneffizient.

Beliebige Snapshot Sicherung für SAP Systemkopie- oder Klonvorgänge verwenden

Dank der NetApp Technologie und Software-Integration können Sie jedes Snapshot Backup eines Quellsystems für eine SAP-Systemkopie oder einen Klonvorgang verwenden. Dieses Snapshot Backup kann entweder aus demselben Storage ausgewählt werden, der für die SAP Produktionssysteme verwendet wird, aus dem für externe Backups verwendeten Storage oder aus dem Storage am Disaster Recovery-Standort. Dank dieser Flexibilität können Entwicklungs- und Testsysteme bei Bedarf von der Produktion getrennt werden. Außerdem werden weitere Szenarien abgedeckt, zum Beispiel Disaster Recovery-Tests am Disaster Recovery-Standort.



Das Klonen aus dem externen Backup- oder Disaster-Recovery-Storage wird für die lokalen NetApp Systeme und für Amazon FSX for NetApp ONTAP unterstützt. Mit Azure NetApp Files können Klone nur am Quell-Volume erstellt werden.

Automatisierung mit Integration

Es gibt verschiedene Szenarien und Anwendungsfälle für die Bereitstellung von SAP-Testsystemen. Dabei gibt es möglicherweise auch unterschiedliche Anforderungen an den Automatisierungsgrad. NetApp Softwareprodukte für SAP können in Datenbank- und Lifecycle-Management-Produkte von SAP integriert werden, um verschiedene Szenarien und Automatisierungsstufen zu unterstützen.

NetApp SnapCenter mit dem Plug-in für SAP HANA wird verwendet, um die erforderlichen Storage Volumes auf Basis eines applikationskonsistenten Snapshot Backups bereitzustellen und alle erforderlichen Host- und Datenbankvorgänge bis zu einer starteten SAP HANA Datenbank auszuführen. Je nach Anwendungsfall können SAP Systemkopien, Systemklone, Systemaktualisierung oder zusätzliche manuelle Schritte wie die SAP Nachbearbeitung erforderlich sein. Weitere Informationen werden im nächsten Abschnitt behandelt.

Eine vollautomatisierte End-to-End-Bereitstellung von SAP Testsystemen kann unter Verwendung von Tools anderer Anbieter und durch die Integration von NetApp Funktionen durchgeführt werden. Weitere Informationen finden Sie unter:

["TR-4953: NetApp SAP Landscape Management Integration Using Ansible"](#)

["TR-4929: SAP-Systemkopien automatisieren mit Libelle SystemCopy \(netapp.com\)"](#)

["Automatisierung von SAP System copy, Refresh, und Klonen von Workflows mit ALPACA und NetApp SnapCenter"](#)

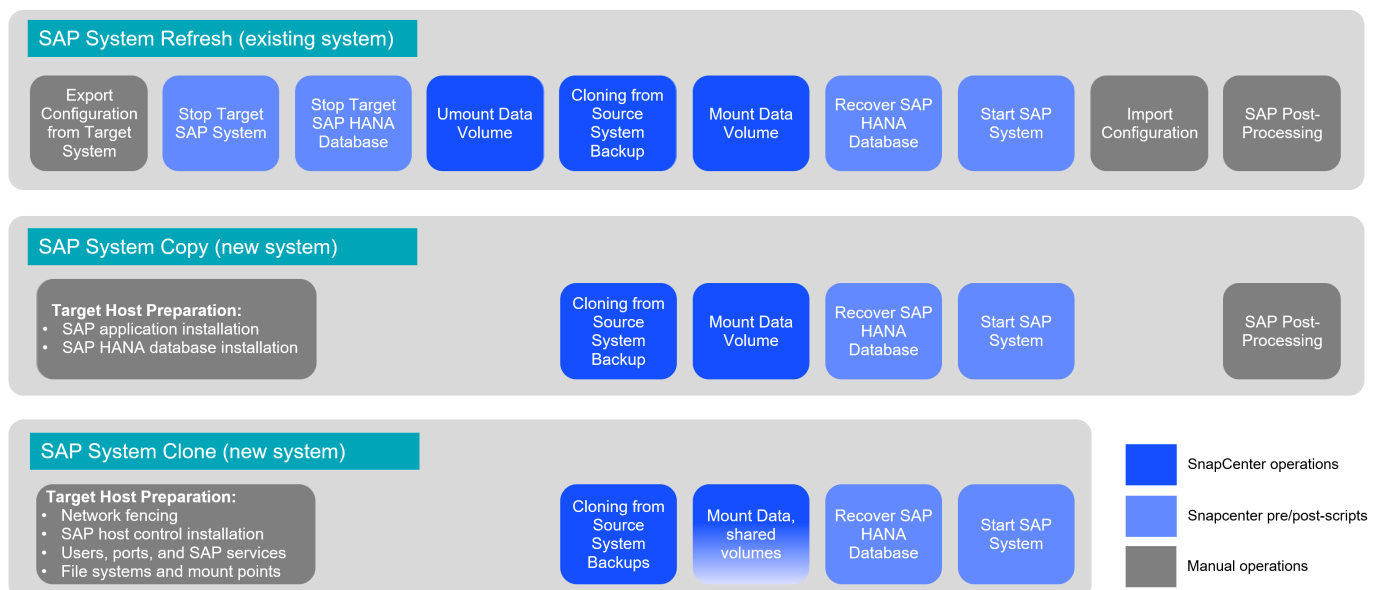
["Automatisierung von SAP Systemkopien Verstärkern;#44; Refresh, Klonen von Workflows mit Avantra und NetApp SnapCenter"](#)

SAP Szenarien für Systemkopie, Aktualisierung und Klonen

Der Begriff SAP Systemkopie wird oft als Synonym für drei verschiedene Prozesse verwendet: SAP Systemaktualisierung, SAP Systemkopie oder SAP Systemklonvorgänge. Es ist wichtig, zwischen den verschiedenen Vorgängen zu unterscheiden, da sich Workflows und Anwendungsfälle für jedes einzelne unterscheiden.

- **SAP-Systemaktualisierung.** eine SAP-Systemaktualisierung ist eine Aktualisierung eines bestehenden SAP-Zielsystems mit Daten aus einem SAP-Quellsystem. Das Zielsystem ist in der Regel Teil einer SAP-Transportlandschaft, beispielsweise ein Qualitätssicherungssystem, das mit den Daten des Produktionssystems aktualisiert wird. Hostname, Instanznummer und SID unterscheiden sich für die Quell- und Zielsysteme.
- **SAP-Systemkopie.** eine SAP-Systemkopie ist ein Setup eines neuen SAP-Zielsystems mit Daten aus einem SAP-Quellsystem. Dabei könnte das neue Zielsystem beispielsweise ein zusätzliches Testsystem mit den Daten aus dem Produktionssystem sein. Hostname, Instanznummer und SID unterscheiden sich für die Quell- und Zielsysteme.
- **SAP-Systemklon.** ein SAP-Systemklon ist ein identischer Klon eines Quell-SAP-Systems. SAP Systemklone werden typischerweise zur Beseitigung logischer Beschädigungen oder zum Testen von Disaster-Recovery-Szenarien eingesetzt. Bei einem Systemklonvorgang bleiben der Hostname, die Instanznummer und die SID unverändert. Daher ist es wichtig, für das Zielsystem ein ordnungsgemäßes Netzwerkfechten einzurichten, um sicherzustellen, dass keine Kommunikation mit der Produktionsumgebung besteht.

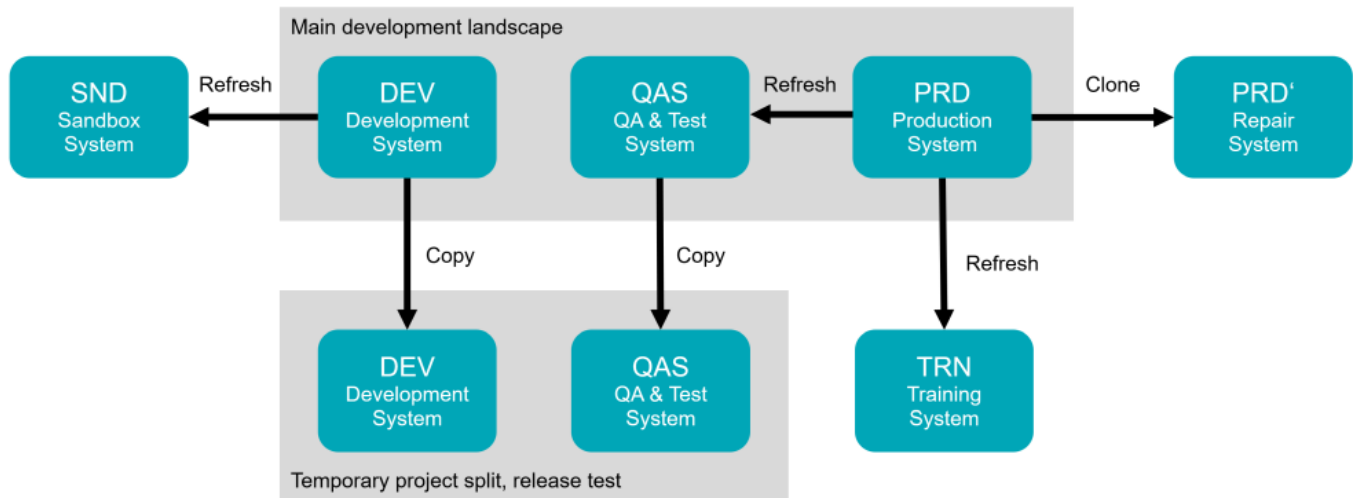
In der Abbildung unten sind die wichtigsten Schritte aufgeführt, die während einer Systemaktualisierung, Systemkopie oder Systemklonfunktion durchgeführt werden müssen. Die blauen Felder kennzeichnen Schritte, die mit SnapCenter automatisiert werden können, während die grauen Felder die Schritte kennzeichnen, die entweder manuell oder mithilfe von Tools anderer Hersteller außerhalb von SnapCenter ausgeführt werden müssen.



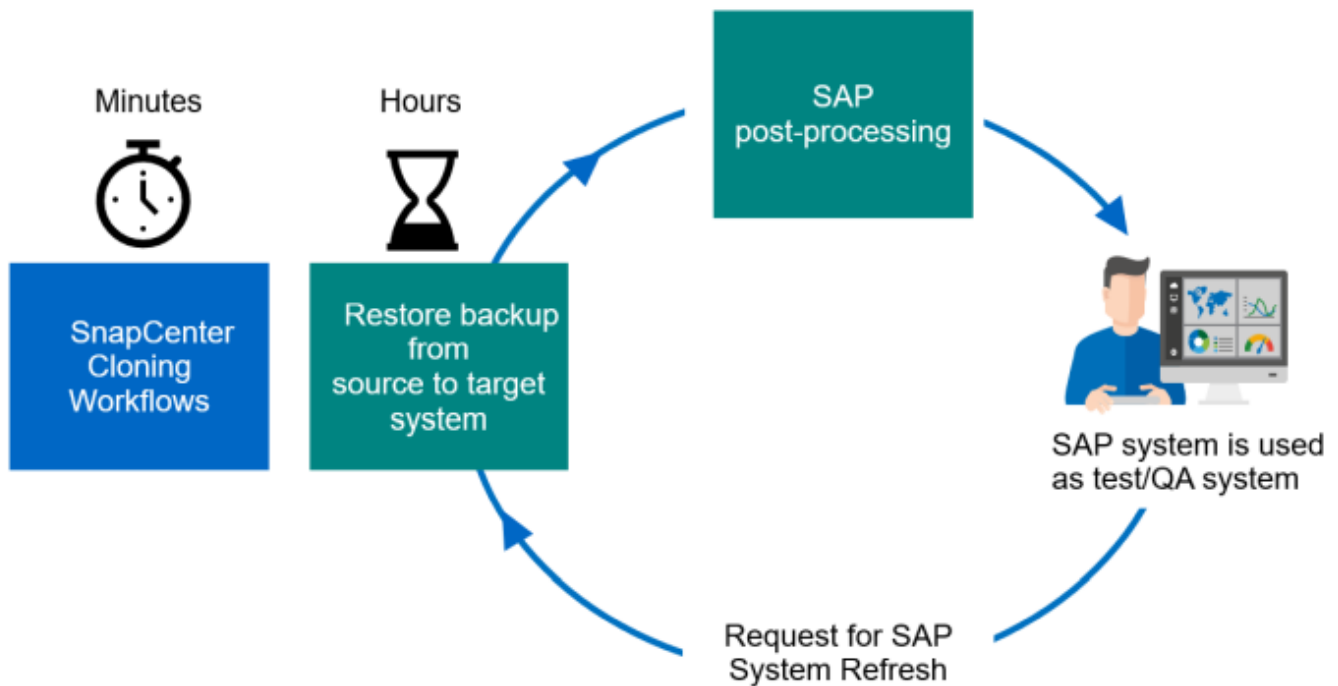
Anwendungsfälle für Systemaktualisierung und Klonen

Datenaktualisierung von QA-, Test-, Sandboxsystemen- und Trainingssystemen

Es gibt verschiedene Szenarien, in denen Daten aus einem Quellsystem zu Test- oder Schulungszwecken einem Zielsystem zur Verfügung gestellt werden müssen. Diese Test- und Trainingssysteme müssen regelmäßig mit Daten des Quellsystems aktualisiert werden, um sicherzustellen, dass die Test- und Schulungsmaßnahmen mit dem aktuellen Datensatz durchgeführt werden. Diese Systemaktualisierungen bestehen aus mehreren Aufgaben auf Infrastruktur-, Datenbank- und Applikationsebene und können je nach Automatisierungsgrad mehrere Tage dauern.



Mit SnapCenter Klon-Workflows werden die erforderlichen Aufgaben an der Infrastruktur und auf Datenbankebene beschleunigt und automatisiert. Anstatt ein Backup vom Quellsystem zum Zielsystem wiederherzustellen, verwendet SnapCenter die NetApp Snapshot Kopie und die NetApp FlexClone Technologie. So können erforderliche Aufgaben bis zu einer gestarteten SAP HANA Datenbank in Minuten anstatt Stunden durchgeführt werden. Der für das Klonen erforderliche Zeitaufwand ist unabhängig von der Größe der Datenbank, sodass selbst sehr große Systeme innerhalb weniger Minuten erstellt werden können. Die Startzeit hängt nur von der Größe der Datenbank und der Verbindung zwischen dem Datenbankserver und dem Storage-System ab.



Der Workflow für Systemaktualisierungen wird im Abschnitt beschrieben ["SAP HANA-Systemaktualisierung mit SnapCenter."](#)

Beseitigung logischer Beschädigungen

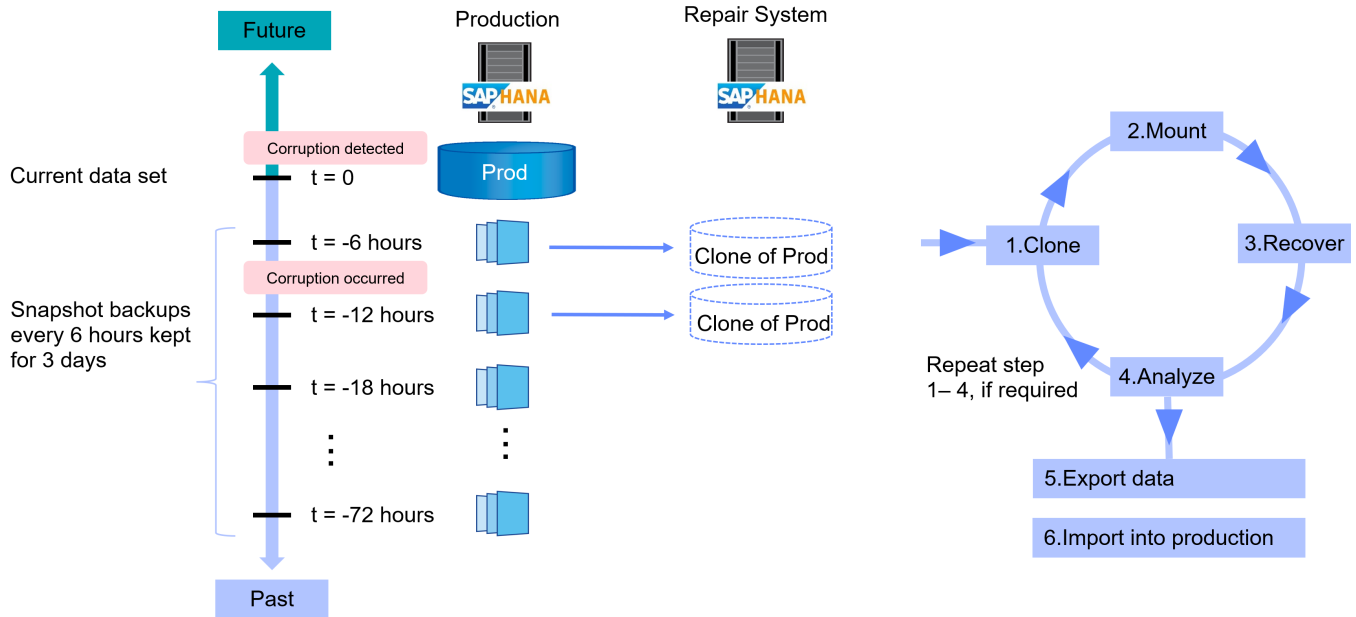
Logische Beschädigungen können durch Softwarefehler, menschliche Fehler oder Sabotage verursacht werden. Leider können logische Beschädigungen oft nicht mit standardmäßigen Hochverfügbarkeits- und Disaster Recovery-Lösungen behoben werden. Daher können abhängig von Schicht, Applikation, Filesystem oder Storage mit einer logischen Beschädigung minimale Ausfallzeiten und maximale Datenverluste nicht erfüllt werden.

Schlimmstenfalls ist die SAP-Anwendung logisch beschädigt. SAP Applikationen laufen oft in einer Landschaft, in der verschiedene Applikationen miteinander kommunizieren und Daten austauschen. Daher wird die Wiederherstellung eines SAP-Systems, bei dem eine logische Beschädigung aufgetreten ist, nicht empfohlen. Wenn Sie das System auf einen Zeitpunkt vor der Beschädigung wiederherstellen, führt dies zu Datenverlust. Außerdem würde die SAP-Landschaft nicht mehr synchron sein und eine zusätzliche Nachbearbeitung erfordern.

Anstatt das SAP-System wiederherzustellen, ist es besser, den logischen Fehler innerhalb des Systems zu beheben, indem das Problem in einem separaten Reparatursystem analysiert wird. Zur Ursachenanalyse ist die Einbindung des Geschäftsprozesses und der Applikationseigentümer erforderlich. Für dieses Szenario erstellen Sie ein Reparatursystem (ein Klon des Produktionssystems) auf Basis der Daten, die vor dem Auftreten der logischen Beschädigung gespeichert wurden. Innerhalb des Reparatursystems können die erforderlichen Daten exportiert und in das Produktionssystem importiert werden. Bei diesem Ansatz muss das Produktionssystem nicht angehalten werden. Im besten Fall gehen keine Daten oder nur ein Bruchteil der Daten verloren.

Bei der Einrichtung des Reparatursystems sind Flexibilität und Agilität entscheidend. Bei Verwendung von Storage-basierten Snapshot Backups von NetApp sind mehrere konsistente Datenbank-Images verfügbar, um mithilfe der NetApp FlexClone Technologie einen Klon des Produktionssystems zu erstellen. Die Erstellung von

FlexClone Volumes dauert nur wenige Sekunden, anstatt mehrerer Stunden, wenn zum Einrichten des Reparatursystems eine umgeleitete Wiederherstellung aus einem dateibasierten Backup verwendet wird.



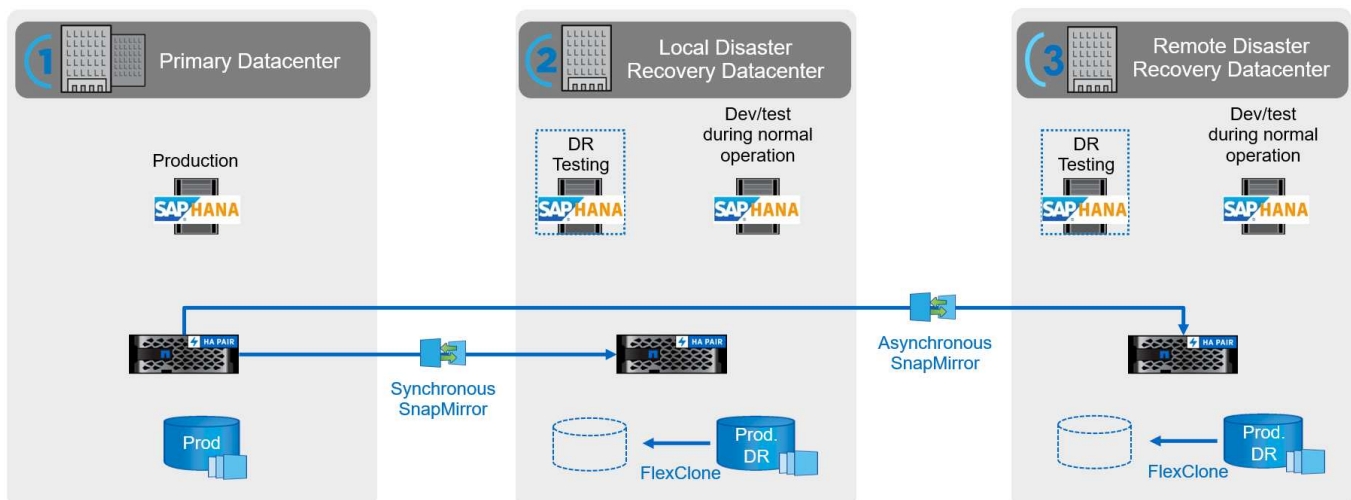
Der Arbeitsablauf der Erstellung des Reparatursystems wird im Abschnitt beschrieben „SAP Systemklon mit SnapCenter.“

Disaster Recovery-Tests

Für eine effiziente Disaster-Recovery-Strategie muss der erforderliche Workflow getestet werden. Die Tests zeigen, ob die Strategie funktioniert und ob die interne Dokumentation ausreichend ist. Darüber hinaus können Administratoren die erforderlichen Verfahren Schulern.

Die Storage-Replizierung mit SnapMirror ermöglicht die Ausführung von Disaster-Recovery-Tests ohne Risiko von RTO und RPO. Disaster-Recovery-Tests können ohne Unterbrechung der Datenreplizierung durchgeführt werden.

Disaster Recovery-Tests für asynchronen und synchronen SnapMirror verwenden Snapshot Backups und FlexClone Volumes am Disaster Recovery-Ziel.



Eine detaillierte Schritt-für-Schritt-Beschreibung finden Sie in den technischen Berichten

["TR-4646: SAP HANA Disaster Recovery with Storage Replication \(netapp.com\)"](#)

["TR-4891: SAP HANA Disaster Recovery mit Azure NetApp Files"](#)

Unterstützte Infrastruktur und Szenarien

Dieses Dokument behandelt Szenarien für SAP-Systemaktualisierung und -Klonen für SAP HANA-Systeme, die auf lokalen NetApp-Systemen, Amazon FSX für NetApp ONTAP-Systemen und Azure NetApp Files ausgeführt werden. Allerdings sind auf jeder Storage-Plattform nicht alle Features und Szenarien verfügbar. In der folgenden Tabelle sind die unterstützten Konfigurationen zusammengefasst.

Im Rahmen dieses Dokuments verwenden wir eine SAP HANA-Landschaft, die auf lokalen NetApp-Systemen mit NFS als Storage-Protokoll ausgeführt wird. Die meisten Workflow-Schritte sind auf den verschiedenen Plattformen identisch. Bei Unterschieden werden sie in diesem Dokument hervorgehoben.

	On-Premises NetApp Systeme	AWS FSX for NetApp ONTAP	Azure NetApp Files
Storage-Protokoll	NFS, Fibre Channel	NFS	NFS
Thin-Klon (FlexClone)	Ja.	Ja.	Nein, in der aktuellen ANF-Version wird das geklonte Volume immer aufgeteilt
Klonteilvorgang	Ja.	Ja.	K. A.
Klonen von Primär	Ja.	Ja.	Ja.
Klonen von Backups an externen Standorten	Ja.	Ja.	Nein
Klonen am DR-Standort	Ja.	Ja.	Ja, aber nicht in SnapCenter integriert

Überblick über den Workflow zur SAP Systemaktualisierung mit SnapCenter

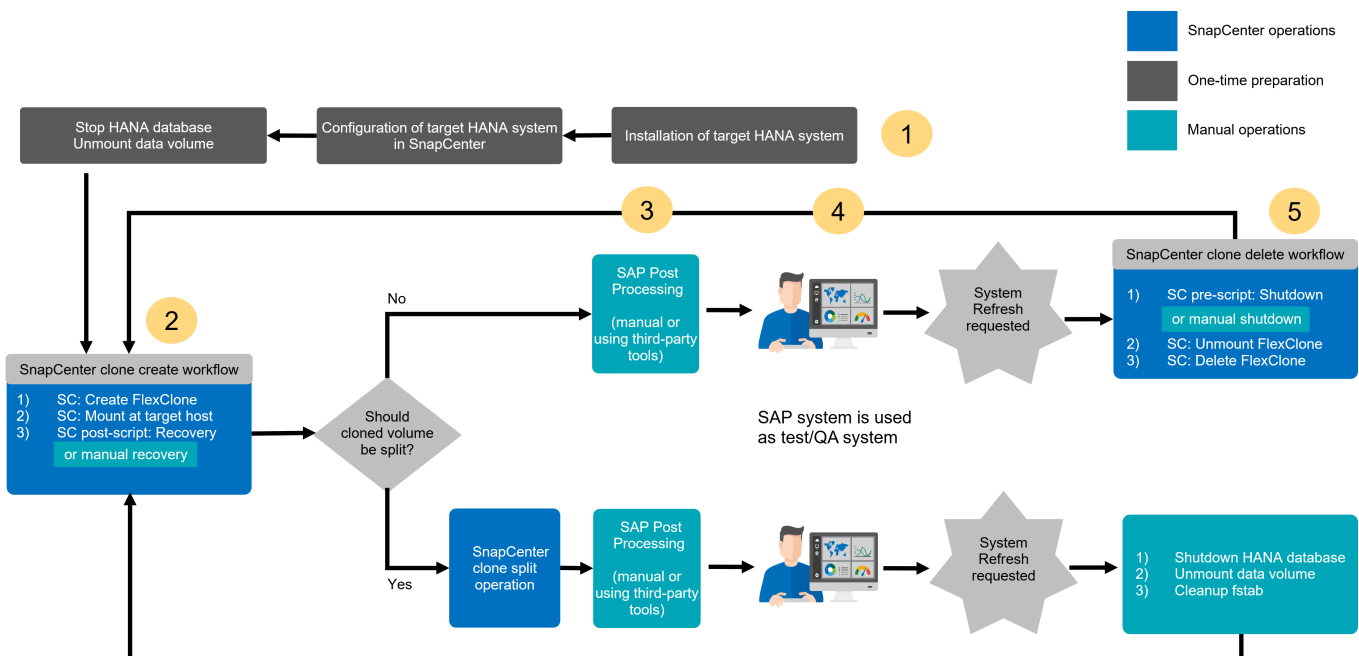
SnapCenter stellt Workflows bereit, mit denen Sie Klone von Datensätzen von bestehenden Snapshot-Backups managen können. Mit diesem geklonten Datensatz, einem FlexClone Volume, kann ein HANA Daten-Volume schnell von einem Quellsystem bereitgestellt und an ein Zielsystem angehängt werden. Die Software eignet sich daher ideal zur Ausführung von Systemaktualisierungen für QA-, Test-, Sandbox- oder Trainingssysteme.

Die Klon-Workflows von SnapCenter bearbeiten alle erforderlichen Operationen auf der Storage-Ebene und können mithilfe von Skripten erweitert werden, um hostspezifische und HANA datenbankspezifische Vorgänge auszuführen. In diesem Dokument verwenden wir ein Skript, um die Wiederherstellung der HANA-Datenbank durchzuführen und Vorgänge beim Herunterfahren auszuführen. SnapCenter-Workflows mit weiterer Automatisierung mithilfe des Skripts bearbeiten alle erforderlichen HANA-Datenbankvorgänge, decken aber keine erforderlichen SAP-Nachbearbeitungsschritte ab. Die SAP-Nachbearbeitung muss manuell oder mit Tools von Drittanbietern durchgeführt werden.

Der Workflow für die SAP-Systemaktualisierung mit SnapCenter besteht aus fünf Hauptschritten, die in der

folgenden Abbildung dargestellt sind.

1. Einmalige Erstinstallation und Vorbereitung des Zielsystems
 - a. Das SnapCenter-HANA-Plugin muss auf dem neuen Zielsystem installiert und das HANA-System in SnapCenter konfiguriert sein
 - b. Das Zielsystem muss angehalten und das HANA-Daten-Volume abgehängt werden
2. Der Workflow zur Erstellung von SnapCenter Klonen
 - a. SnapCenter erstellt ein FlexClone Volume des ausgewählten Snapshots des Quellsystems
 - b. SnapCenter bindet das FlexClone Volume im Zielsystem ein
 - c. Die Recovery der Ziel-HANA-Datenbank kann mit dem Skript als Post-Skript automatisiert `sc-system-refresh` oder manuell ausgeführt werden
3. SAP-Nachbearbeitung (manuell oder mit einem Drittanbieter-Tool)
4. Das System kann nun als Test-/QS-System eingesetzt werden.
5. Bei Anforderung einer neuen Systemaktualisierung wird das FlexClone Volume mithilfe des Workflows zum Löschen von SnapCenter Klonen entfernt
 - a. Wenn das HANA-Zielsystem in SnapCenter gesichert wurde, muss der Schutz vor dem Starten des Workflows zum Löschen von Klonen entfernt werden.
 - b. Das HANA-System muss manuell angehalten oder automatisch mit dem Skript als SnapCenter-Pre-Skript gestoppt werden `sc-system-refresh`
 - c. SnapCenter entbindet das HANA-Datenvolumen
 - d. SnapCenter löscht das FlexClone Volume
 - e. Eine Aktualisierung wird mit Schritt 2 neu gestartet.



In den meisten Fällen werden Zieltests/QA-Systeme mindestens einige Wochen lang eingesetzt. Da das FlexClone Volume den Snapshot des Quell-System-Volumen blockiert, benötigt dieser Snapshot basierend auf der Blockänderungsrate am Quell-System-Volumen zusätzliche Kapazität. Bei Produktionsquellsystemen und einer durchschnittlichen Änderungsrate von 20% pro Tag wird der blockierte Snapshot nach 5 Tagen 100%

erreichen. Daher empfiehlt NetApp, das FlexClone Volume entweder sofort oder nach ein paar Tagen aufzuteilen, wenn der Klon auf einem Produktions-Quellsystem basiert. Der Klon-Split-Vorgang blockiert nicht die Nutzung des geklonten Volume und kann daher jederzeit während des Betriebs der HANA-Datenbank durchgeführt werden.



Bei der Aufteilung des FlexClone Volume löscht SnapCenter alle Backups, die auf dem Zielsystem erstellt wurden.



Bei SnapCenter und Azure NetApp Files ist der Klonaufteilungsvorgang nicht verfügbar, da Azure NetApp Files den Klon nach der Erstellung immer teilt.

Der Aktualisierungsvorgang einschließlich der Klonaufteilung besteht aus den folgenden Schritten.

1. Einmalige Erstinstallation und Vorbereitung des Zielsystems

- a. Das SnapCenter-HANA-Plugin muss auf dem neuen Zielsystem installiert und das HANA-System in SnapCenter konfiguriert sein
- b. Das Zielsystem muss angehalten und das HANA-Daten-Volume abgehängt werden

2. Der Workflow zur Erstellung von SnapCenter Klonen

- a. SnapCenter erstellt ein FlexClone Volume des ausgewählten Snapshots des Quellsystems
- b. SnapCenter bindet das FlexClone Volume im Zielsystem ein
- c. Die Recovery der Ziel-HANA-Datenbank kann mit dem Skript als Post-Skript automatisiert `sc-system-refresh` oder manuell ausgeführt werden

3. Das FlexClone Volume wird mithilfe des SnapCenter Klon-Split-Workflows aufgeteilt.

4. SAP-Nachbearbeitung (manuell oder mit einem Drittanbieter-Tool)

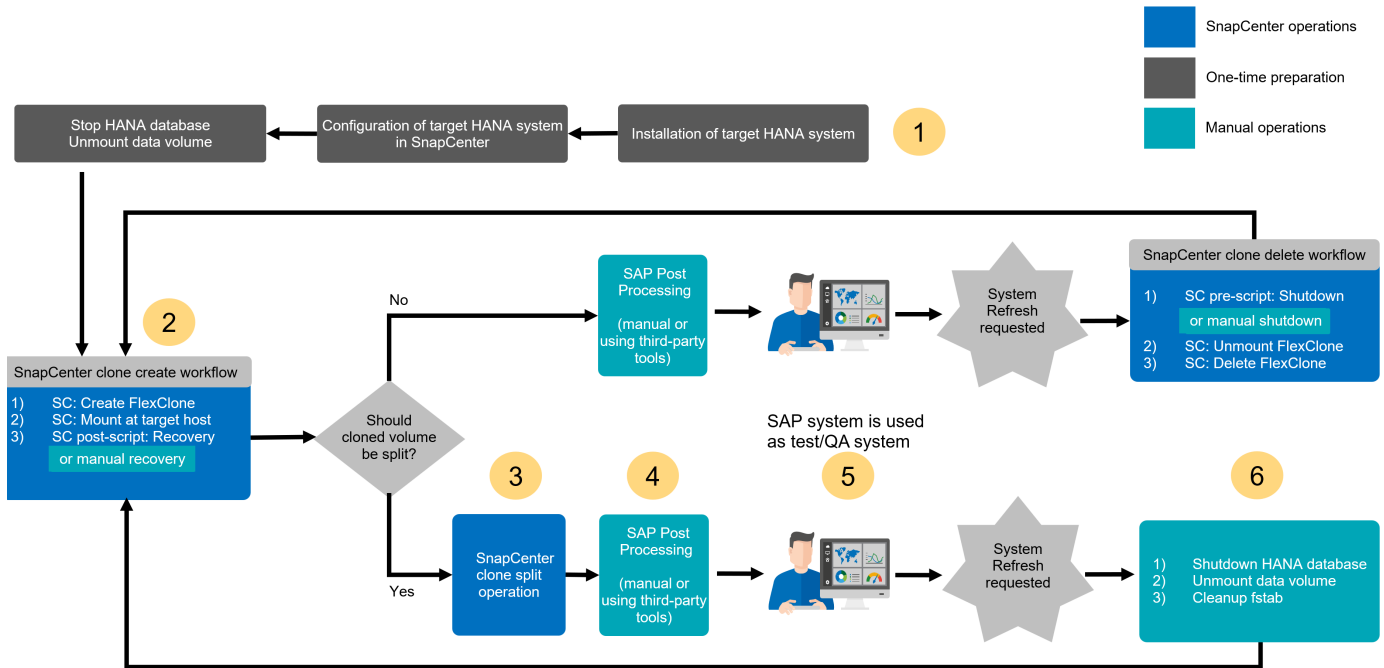
5. Das System kann nun als Test-/QS-System eingesetzt werden.

6. Wenn eine neue Systemaktualisierung angefordert wird, erfolgt die Bereinigung mit den folgenden manuellen Schritten

- a. Wenn das Ziel-HANA-System in SnapCenter geschützt wurde, muss der Schutz entfernt werden.
- b. Das HANA-System muss manuell gestoppt werden
- c. Das HANA-Datenvolumen muss abgehängt und der fstab-Eintrag aus SnapCenter entfernt werden (manuelle Aufgabe).
- d. Eine Aktualisierung wird mit Schritt 2 neu gestartet.



Das alte Daten-Volume, das zuvor gespalten wurde, muss manuell auf dem Storage-System gelöscht werden.



Den Abschnitt „SAP HANA Systemaktualisierung mit SnapCenter“ zeigt eine detaillierte Schritt-für-Schritt-Beschreibung der beiden System-Refresh-Workflows an.

Überblick über den SAP Systemklonen-Workflow mit SnapCenter

Wie im vorherigen Abschnitt beschrieben, kann SnapCenter Klone von Datensätzen von jedem vorhandenen Snapshot Backup managen und diese Datensätze schnell auf jedes beliebige Zielsystem bereitstellen. Die flexible und agile Bereitstellung von Produktionsdaten an ein Reparatursystem zur Behebung logischer Beschädigungen ist von entscheidender Bedeutung, da häufig das Reparatursystem zurückgesetzt und ein anderer Produktionsdatensatz ausgewählt werden muss. Die FlexClone Technologie ermöglicht einen schnellen Bereitstellungsprozess und sorgt für deutliche Kapazitätseinsparungen, da das Reparatursystem normalerweise nur für einen kurzen Zeitraum verwendet wird.

Die folgende Abbildung fasst die erforderlichen Schritte für einen SAP-Systemklonvorgang mit SnapCenter zusammen.

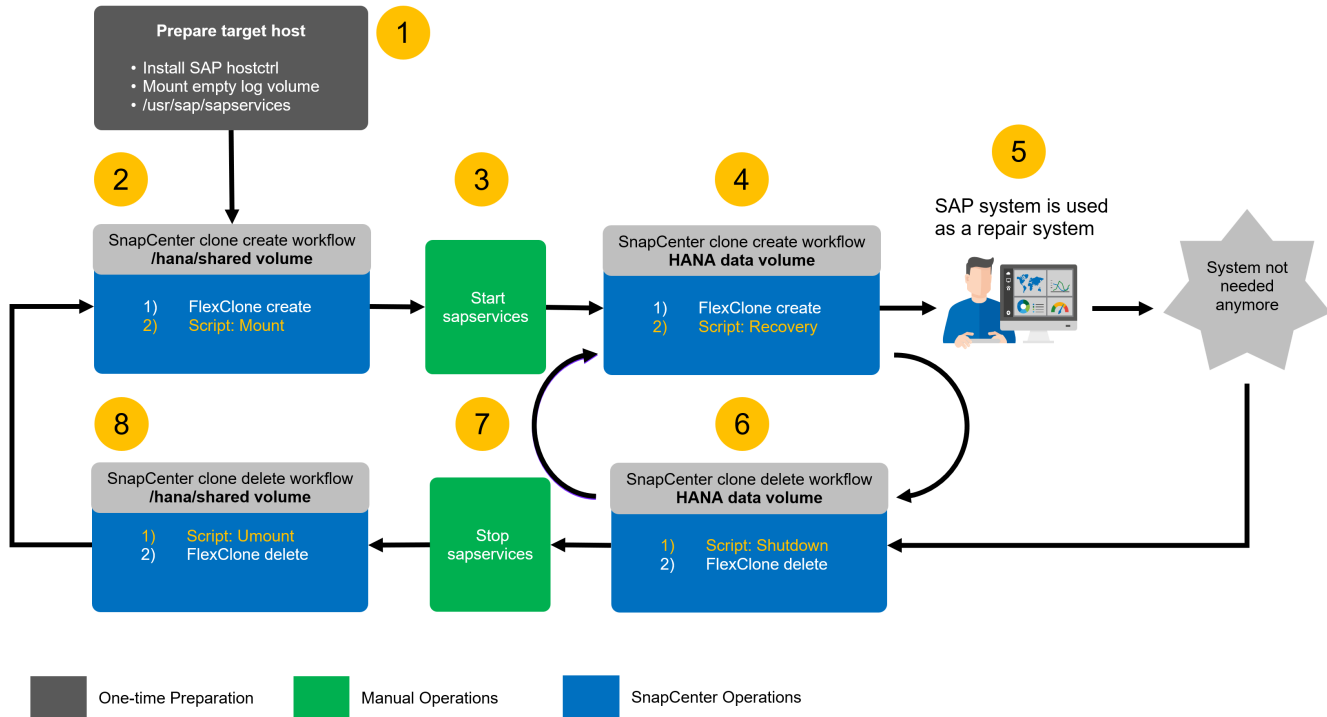
1. Bereiten Sie den Zielhost vor.
2. Workflow für die SAP HANA-Freigabe-Volumes durch SnapCenter-Klon erstellen
3. Starten Sie SAP HANA Services.
4. SnapCenter Clone erstellen Sie einen Workflow für das SAP HANA Daten-Volume einschließlich Datenbank-Recovery.
5. Das SAP HANA-System kann nun als Reparatursystem eingesetzt werden.

Wenn das System nicht mehr benötigt wird, erfolgt die Bereinigung mit den folgenden Schritten.

1. SnapCenter Clone delete Workflow für das SAP HANA Daten-Volume einschließlich Datenbank-Shutdown (unter Verwendung des Automatisierungsskripts).
2. Stoppen Sie SAP HANA Services.
3. SnapCenter Clone delete Workflow für das SAP HANA Shared Volume.



Wenn Sie das System auf ein anderes Snapshot Backup zurücksetzen müssen, reichen die Schritte 6 und Schritt 4 aus. Eine Aktualisierung des gemeinsam genutzten SAP HANA-Volumes ist nicht erforderlich.



Den Abschnitt „SAP Systemklon mit SnapCenter“ Enthält eine detaillierte Schritt-für-Schritt-Beschreibung des Systemklonworkflows.

Überlegungen zu Systemaktualisierungen für SAP HANA mit Storage-Snapshot-Backups

Mandantenname(n) im Zielsystem

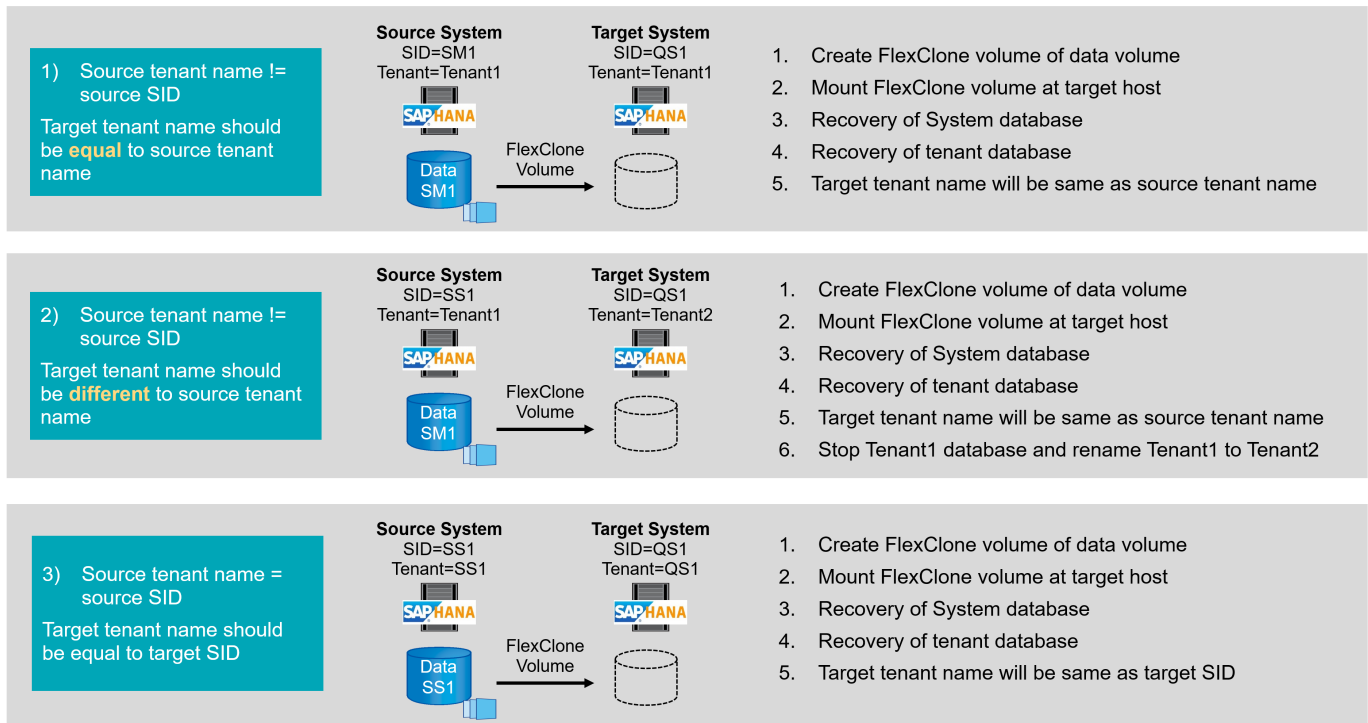
Die zur Aktualisierung des SAP HANA-Systems erforderlichen Schritte hängen von der Mandantenkonfiguration des Quellsystems und dem erforderlichen Mandantennamen auf dem Zielsystem ab, wie in der folgenden Abbildung dargestellt.

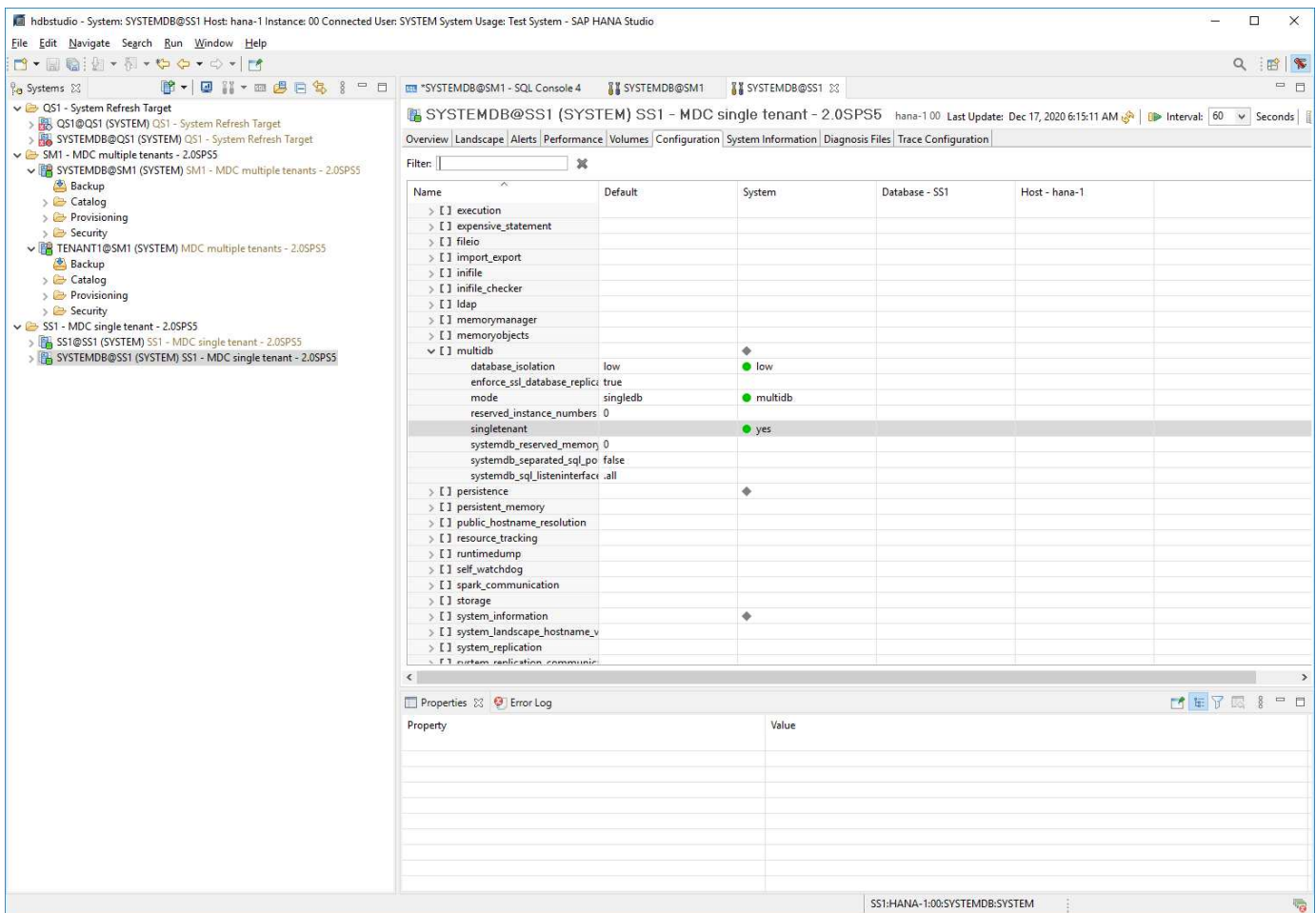
Da der Mandantenname in der Systemdatenbank konfiguriert ist, steht nach der Wiederherstellung der Systemdatenbank auch der Mandantenname des Quellsystems auf dem Zielsystem zur Verfügung. Daher kann der Mandant im Zielsystem nur mit dem gleichen Namen wie der Quellmandant wiederhergestellt werden, wie in Option 1 dargestellt. Wenn der Mandantenname im Zielsystem anders sein muss, muss er zuerst mit demselben Namen wie der Quellmandant wiederhergestellt und dann in den erforderlichen Zielmandanten-Namen umbenannt werden. Dies ist Option 2.

Eine Ausnahme von dieser Regel ist ein SAP HANA-System mit einem einzelnen Mandanten, bei dem der Mandantenname mit der System-SID identisch ist. Diese Konfiguration ist nach einer ersten SAP HANA-Installation die Standardeinstellung. Diese spezifische Konfiguration wird von der SAP HANA-Datenbank gekennzeichnet. In diesem Fall kann die Mandantenwiederherstellung am Zielsystem mit dem Mandantennamen des Zielsystems durchgeführt werden, was ebenfalls mit der System-SID des Zielsystems identisch sein muss. Dieser Workflow wird in Option 3 angezeigt.



Sobald ein Mandant im Quellsystem erstellt, umbenannt oder abgelegt wird, wird dieses Konfigurationskennzeichen von der SAP HANA-Datenbank gelöscht. Somit ist auch dann, wenn die Konfiguration an Mandant = SID zurückgebracht wurde, das Flag nicht mehr verfügbar und die Ausnahme hinsichtlich der Mandantenwiederherstellung mit Workflow 3 ist nicht mehr möglich. In diesem Fall ist Option 2 der erforderliche Workflow.





Workflow zur Systemaktualisierung mit aktivierter SAP HANA-Verschlüsselung

Wenn die Persistenz-Verschlüsselung von SAP HANA aktiviert ist, sind weitere Schritte erforderlich, bevor Sie die SAP HANA-Datenbank im Zielsystem wiederherstellen können.

Im Quellsystem müssen Sie eine Sicherung der Verschlüsselungsroot-Schlüssel für die Systemdatenbank sowie für alle Mandantendatenbanken erstellen. Die Sicherungsdateien müssen auf das Zielsystem kopiert und die Stammschlüssel müssen aus dem Backup importiert werden, bevor der Wiederherstellungsvorgang ausgeführt wird.

Siehe auch ["SAP HANA Administration Guide"](#).

Sicherung von Stammschlüsseln

Wenn Änderungen an den Stammschlüsseln vorgenommen wurden, ist immer eine Sicherung der Stammschlüssel erforderlich. Der Backup-Befehl erfordert den dbid als CLI-Parameter. Die dbid's können mit der unten stehenden SQL-Anweisung identifiziert werden.

SYSTEMDB@SS1 (SYSTEM) hana-1 00

SQL Result

```

SELECT DATABASE_NAME,
CASE WHEN (DBID = " AND
DATABASE_NAME = 'SYSTEMDB')
THEN 1
WHEN (DBID = " AND
DATABASE_NAME <> 'SYSTEMDB')
THEN 3
ELSE TO_INT(DBID)
END DATABASE_ID
FROM (SELECT DISTINCT DATABASE_NAME, SUBSTR_AFTER (SUBPATH, '.') AS DBID FROM SYS_DATABASES.M_VOLUMES)

```

	DATABASE_NAME	DATABASE_ID
1	SYSTEMDB	1
2	SS1	3

Die SQL-Anweisung und weitere Dokumentation sind im SAP HANA Admin Guide verfügbar. Die ["Sichern Sie die Stammschlüssel im SAP-Hilfeportal"](#) folgenden Schritte zeigen die erforderlichen Operationen für ein HANA-System mit einem einzelnen Mandanten SS1 und werden im Quellsystem ausgeführt.

1. Legen Sie das Sicherungspasswort für System- und Mandantendatenbanken (SS1) fest (falls noch nicht geschehen).

```

hdbsql SYSTEMDB=> ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD
Netappl23;
0 rows affected (overall time 3658.128 msec; server time 3657.967 msec)
hdbsql SYSTEMDB=>
hdbsql SS1=> ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD
Netappl23;
0 rows affected (overall time 2424.236 msec; server time 2424.010 msec)
hdbsql SS1=>

```

1. Sicherung von Stammschlüsseln für System- und Mandantendatenbanken (SS1) erstellen.

```

ssladm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-backupRootKeys root-key-backup-SS1-SYSTEMDB.rkb --dbid=1 --type='ALL'
Exporting root key backup for database SYSTEMDB (DBID: 1) to
/usr/sap/SS1/home/root-key-backup-SS1-SYSTEMDB.rkb
done.
ssladm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-backupRootKeys root-key-backup-SS1-SS1.rkb --dbid=3 --type='ALL'
Exporting root key backup for database SS1 (DBID: 3) to
/usr/sap/SS1/home/root-key-backup-SS1-SS1.rkb
done.

```

1. Validieren von Stammschlüsselsicherungen (optional)


```

ssladm@hana-1:/usr/sap/SS1/home> ls -al root*
-rw-r----- 1 ssladm sapsys 1440 Apr 24 07:00 root-key-backup-SS1-SS1.rkb
-rw-r----- 1 ssladm sapsys 1440 Apr 24 06:54 root-key-backup-SS1-
SYSTEMDB.rkb
ssladm@hana-1:/usr/sap/SS1/home>

ssladm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-validateRootKeysBackup root-key-backup-SS1-SS1.rkb
Please Enter the password:
Successfully validated SSFS backup file /usr/sap/SS1/home/root-key-backup-
SS1-SS1.rkb
done.

ssladm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-validateRootKeysBackup root-key-backup-SS1-SYSTEMDB.rkb
Please Enter the password:
Successfully validated SSFS backup file /usr/sap/SS1/home/root-key-backup-
SS1-SYSTEMDB.rkb
done.

```

Import von Root-Schlüsseln auf dem Zielsystem

Der Import der Stammschlüssel ist zunächst für die erste Systemaktualisierung erforderlich. Wenn die Stammschlüssel im Quellsystem nicht geändert werden, ist kein zusätzlicher Import erforderlich. Der Import-Befehl erfordert den dbid als CLI-Parameter. Die dbid's können in der gleichen Weise identifiziert werden wie für die Root-Key-Backup beschrieben.

1. In unserem Setup werden die Root-Schlüssel vom Quellsystem auf eine NFS-Share kopiert

```

hana-1:~ # cp /usr/sap/SS1/home/root-key-backup-SS1-SS1.rkb /mnt/sapcc-
share/SAP-System-Refresh/
hana-1:~ # cp /usr/sap/SS1/home/root-key-backup-SS1-SYSTEMDB.rkb
/mnt/sapcc-share/SAP-System-Refresh/

```

1. Die Stammschlüssel können nun mit hdbnsutil importiert werden. Das dbid für die System- und Mandantendatenbank muss mit dem Befehl bereitgestellt werden. Das Backup-Passwort ist ebenfalls erforderlich.

```

qsladm@hana-7:/usr/sap/QS1/HDB11> ./exe/hdbnsutil -recoverRootKeys
/mnt/sapcc-share/SAP-System-Refresh/root-key-backup-SS1-SYSTEMDB.rkb
--dbid=1 --type=ALL
Please Enter the password:
Importing root keys for DBID: 1 from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SYSTEMDB.rkb
Successfully imported root keys from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SYSTEMDB.rkb
done.

qsladm@hana-7:/usr/sap/QS1/HDB11> ./exe/hdbnsutil -recoverRootKeys
/mnt/sapcc-share/SAP-System-Refresh/root-key-backup-SS1-SS1.rkb --dbid=3
--type=ALL Please Enter the password:
Importing root keys for DBID: 3 from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SS1.rkb
Successfully imported root keys from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SS1.rkb
done.
qsladm@hana-7:/usr/sap/QS1/HDB11>

```

Root-Schlüssel importieren, wenn dbid nicht am Ziel vorhanden ist

Wie im vorherigen Kapitel beschrieben, ist das dbid erforderlich, um den Stammschlüssel für das System und alle Mandantendatenbanken zu importieren. Während die Systemdatenbank immer dbid=0 hat, können die Mandantendatenbanken unterschiedliche dbid's haben.



The screenshot shows a SQL query in the SAP HANA Studio interface. The query is a SELECT statement that uses a CASE WHEN clause to map database names to their respective DBIDs. The output is a table with three rows: TENANT1 (DBID 4), SYSTEMDB (DBID 1), and TENANT2 (DBID 3).

```

SELECT DATABASE_NAME,
CASE WHEN (DBID = " AND
DATABASE_NAME = 'SYSTEMDB')
THEN 1
WHEN (DBID = " AND
DATABASE_NAME <> 'SYSTEMDB')
THEN 3
ELSE TO_INT(DBID)
END DATABASE_ID
FROM (SELECT DISTINCT DATABASE_NAME, SUBSTR_AFTER (SUBPATH,':') AS DBID FROM SYS_DATABASES.M_VOLUMES)

```

	DATABASE_NAME	DATABASE_ID
1	TENANT1	4
2	SYSTEMDB	1
3	TENANT2	3

Die obige Ausgabe zeigt zwei Mandanten mit dbid=3 und dbid=4. Wenn das Zielsystem noch keinen Mandanten mit dbid=4 gehostet hat, schlägt der Import des Stammschlüssels fehl. In diesem Fall müssen Sie zuerst die Systemdatenbank wiederherstellen und dann den Schlüssel für den Mandanten mit dbid=4 importieren.

Beispielskripte zur Automatisierung

In diesem Dokument werden zwei Skripte verwendet, um die Vorgänge zur SnapCenter-Klonerstellung und -Löschung weiter zu automatisieren.

- Das Skript `sc-system-refresh.sh` wird für die Systemaktualisierung und den Systemklonworkflow verwendet, um Recovery- und Shutdown-Vorgänge der SAP HANA-Datenbank auszuführen.
- Das Skript `sc-mount-volume.sh` wird für den Systemklonworkflow verwendet, um Mount- und Unmounting-Vorgänge für das gemeinsam genutzte SAP HANA-Volume auszuführen.



Die Beispielskripte werden wie IS bereitgestellt und von NetApp nicht unterstützt. Die Skripte können Sie per E-Mail an ng-sapcc@netapp.com anfordern.

Skript `sc-system-refresh.sh`

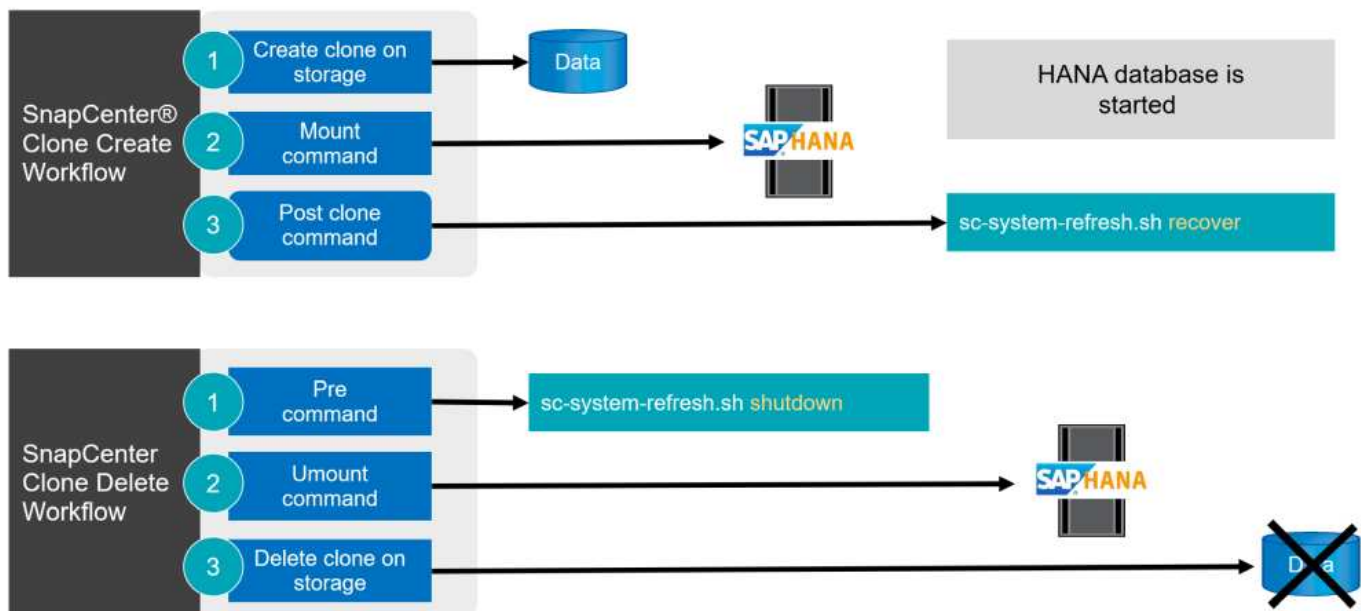
Das Beispielskript `sc-system-refresh.sh` wird verwendet, um Recovery- und Shutdown-Vorgänge auszuführen. Das Skript wird mit spezifischen Befehlszeilenoptionen innerhalb der SnapCenter-Workflows zum Erstellen und Löschen von Klonen aufgerufen, wie in der Abbildung unten dargestellt.

Das Skript ist generisch und liest alle erforderlichen Parameter, wie die SID vom Zielsystem. Das Skript muss auf dem Zielhost des Systemaktualisierungsvorgangs verfügbar sein. Ein hdb-Benutzerspeicherschlüssel muss für die Benutzer-<SID>-Konfiguration m auf dem Zielsystem konfiguriert werden. Der Schlüssel muss den Zugriff auf die SAP HANA-Systemdatenbank ermöglichen und Berechtigungen für Wiederherstellungsvorgänge bereitstellen. Der Schlüssel muss den Namen <TARGET-SID>-Ausmuster Y haben.

Das Skript schreibt eine Protokolldatei `sc-system-refresh-SID.log`, in das gleiche Verzeichnis, wo es ausgeführt wird.



Die aktuelle Version des Skripts unterstützt MDC-Konfigurationen für einzelne Hostsysteme oder MDC für mehrere Mandanten. SAP HANA wird nicht mit Systemen mit mehreren Hosts unterstützt.



Unterstützte Mandanten-Recovery-Vorgänge

Wie im Abschnitt „SAP HANA System Refresh Operation Workflows using Storage Snapshot“ beschrieben, hängen die möglichen Mandanten-Recovery-Operationen am Zielsystem von der Mandantenkonfiguration des

Quellsystems ab. Das Skript `sc-system-refresh.sh` unterstützt alle Wiederherstellungsvorgänge für Mandanten, die je nach Konfiguration des Quellsystems möglich sind, wie in der Tabelle unten gezeigt.

Wenn auf dem Zielsystem ein anderer Mandantennamen benötigt wird, muss der Mandant nach dem Recovery-Vorgang manuell umbenannt werden.

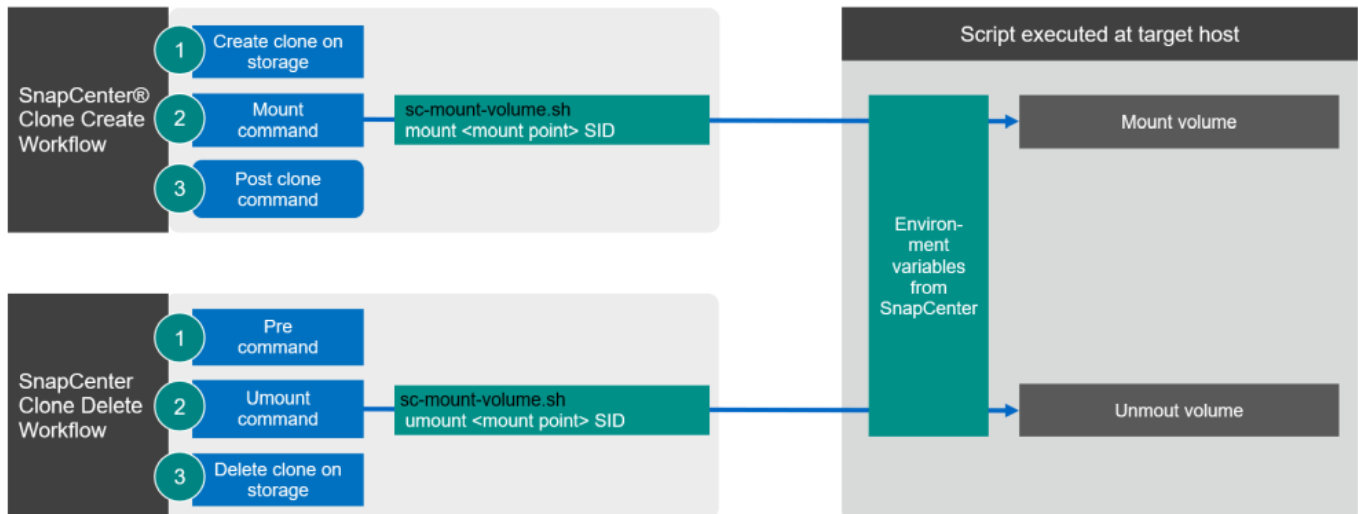
SAP HANA-System	Mandantenkonfiguration + am Quellsystem	Resultierende Mandantenkonfiguration + am Zielsystem
MDC-Einzelmandant	Quell-Mandantenname entspricht der Quell-SID	Der Zielmandant-Name entspricht der Ziel-SID
MDC-Einzelmandant	Der Name des Quell-Mandanten entspricht nicht dem Quell-SID	Der Zielmandant-Name entspricht dem Quell-Mandantennamen
MDC mehrere Mandanten	Alle Mandantennamen	Alle Mandanten werden wiederhergestellt und haben denselben Namen wie die Quell-Mandanten.

Skript `sc-mount-volume.sh`

Das Beispielskript `sc-mount-volume.sh` wird zum Ausführen von Mount und Unmounten für ein beliebiges Volume verwendet. Das Skript wird verwendet, um das gemeinsam genutzte SAP HANA-Volume bei der Klonoperation des SAP HANA-Systems zu mounten. Das Skript wird mit spezifischen Befehlszeilenoptionen innerhalb der SnapCenter-Workflows zum Erstellen und Löschen von Klonen aufgerufen, wie in der Abbildung unten dargestellt.



Das Skript unterstützt SAP HANA-Systeme mit NFS als Storage-Protokoll.



SnapCenter-Umgebungsvariablen

SnapCenter bietet einen Satz von Umgebungsvariablen, die innerhalb des Skripts verfügbar sind, die auf dem Ziel-Host ausgeführt werden. Das Skript verwendet diese Variablen, um die entsprechenden Konfigurationseinstellungen zu bestimmen.

- Die Skriptvariablen `STORAGE`, `JUNCTION_PATH` werden für den Mount-Vorgang verwendet.
- Abgeleitet von `CLONED_VOLUMES_MOUNT_PATH` Umgebungsvariable:
- `CLONED_VOLUMES_MOUNT_PATH=${STORAGE}:/${JUNCTION_PATH}`
- Beispiel:
`CLONED_VOLUMES_MOUNT_PATH=192.168.175.117:/SS1_shared_Clone_05112206115489411`

Skript zum Abrufen von SnapCenter Umgebungsvariablen

Wenn keine Automatisierungsskripts verwendet werden und die Schritte manuell ausgeführt werden sollten, müssen Sie den Verbindungspfad des FlexClone Volume zum Storage-System kennen. Der Verbindungspfad ist in SnapCenter nicht sichtbar. Sie müssen also entweder den Verbindungspfad direkt am Storage-System nachschlagen oder ein einfaches Skript verwenden, das die SnapCenter Umgebungsvariablen auf dem Ziel-Host bereitstellt. Dieses Skript muss als Mount-Operation-Skript innerhalb der SnapCenter Clone Erstellungsvorgang hinzugefügt werden.

```
ssladm@hana-1:/mnt/sapcc-share/SAP-System-Refresh> cat get-env.sh
#!/bin/bash
env > /tmp/env-from-sc.txt
ssladm@hana-1:/mnt/sapcc-share/SAP-System-Refresh>
```

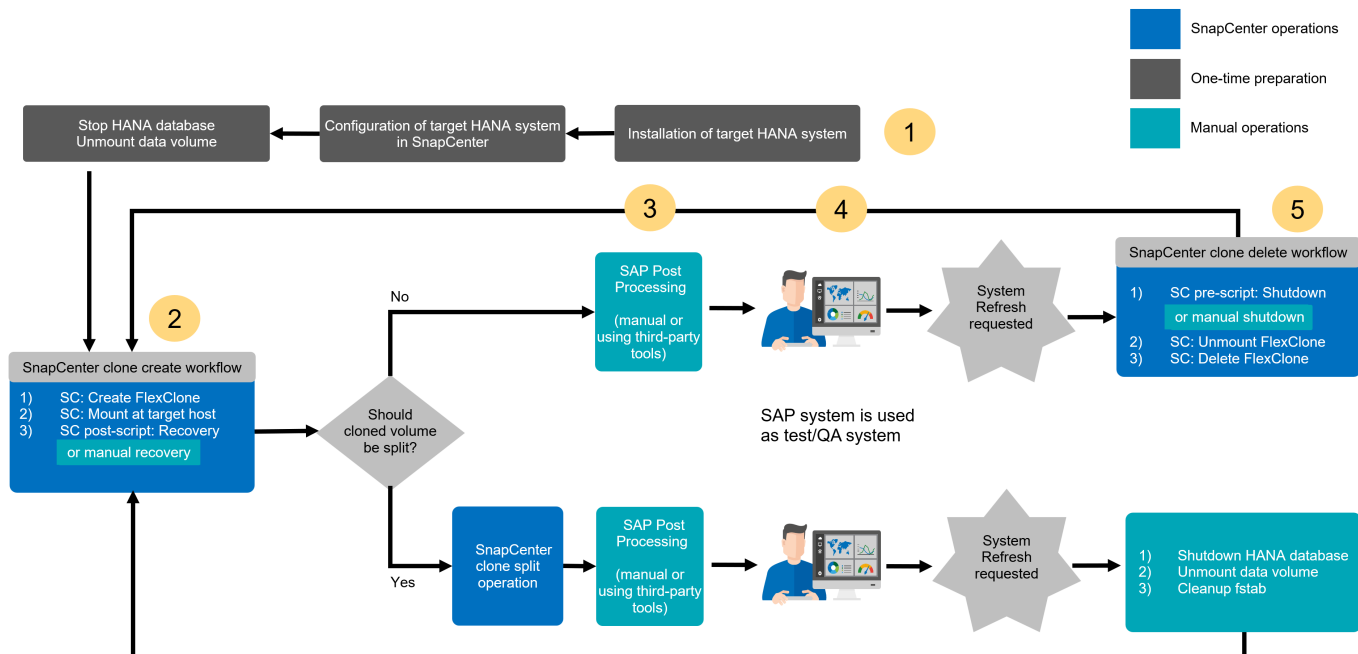
Innerhalb des `env-from-sc.txt` Datei, suchen Sie nach der Variable `CLONED_VOLUMES_MOUNT_PATH` Um die IP-Adresse des Storage-Systems und den Verbindungspfad des FlexClone Volume zu erhalten.

Beispiel:

```
CLONED_VOLUMES_MOUNT_PATH=192.168.175.117:/SS1_data_mnt00001_Clone_05112206115489411
```

Systemaktualisierung für SAP HANA mit SnapCenter

Im folgenden Abschnitt finden Sie eine Schritt-für-Schritt-Beschreibung der verschiedenen Optionen für die Systemaktualisierung einer SAP HANA-Datenbank.



Je nach Konfiguration der SAP HANA-Datenbank werden weitere Schritte ausgeführt bzw. müssen vorbereitet werden. Die folgende Tabelle bietet eine Zusammenfassung.

Quellsystem	Konfiguration des Quellsystems	SnapCenter- und SAP HANA-Betrieb
MDC Einzelmandant + SID = Mandantenname	Standardkonfiguration	SnapCenter-Klonvorgang und optionale Ausführung von Wiederherstellungsskripten.
	SAP HANA-Verschlüsselung mit Persistenz	Zunächst oder wenn die Stammschlüssel im Quellsystem geändert wurden, müssen die Stammschlüsselsicherungen auf dem Zielsystem importiert werden, bevor die Wiederherstellung ausgeführt werden kann.
	Quelle für die SAP HANA-Systemreplizierung	Weitere Schritte sind nicht erforderlich. Wenn für das Zielsystem kein HSR konfiguriert ist, bleibt es ein eigenständiges System.
	SAP HANA mehrere Partitionen	Keine zusätzlichen Schritte erforderlich, aber Mount-Punkte für SAP HANA-Volume-Partitionen müssen auf dem Zielsystem mit derselben Namenskonvention verfügbar sein (nur SID ist unterschiedlich).

Quellsystem	Konfiguration des Quellsystems	SnapCenter- und SAP HANA-Betrieb
MDC mehrere Mandanten Oder MDC Einzelmandant + mit SID <> Mandantenname	Standardkonfiguration	SnapCenter-Klonvorgang und optionale Ausführung von Wiederherstellungsskripten. Skript stellt alle Mandanten wieder her. Wenn bei den Zielsystemnamen keine Mandanten- oder Mandantennamen vorhanden sind, werden erforderliche Verzeichnisse automatisch während der SAP HANA-Wiederherstellung erstellt. Die Mandantennamen entsprechen der Quelle und müssen bei Bedarf nach der Wiederherstellung umbenannt werden.
	SAP HANA-Verschlüsselung mit Persistenz	Wenn zuvor auf dem Zielsystem keine DBID des Quellsystems vorhanden ist, muss die Systemdatenbank zuerst wiederhergestellt werden, bevor die Stammschlüsselsicherung dieses Mandanten importiert werden kann.
	Quelle für HANA-Systemreplizierung	Weitere Schritte sind nicht erforderlich. Wenn für das Zielsystem kein HSR konfiguriert ist, bleibt es ein eigenständiges System.
	HANA mit mehreren Partitionen	Keine zusätzlichen Schritte erforderlich, aber Mount-Punkte für SAP HANA-Volume-Partitionen müssen auf dem Zielsystem mit derselben Namenskonvention verfügbar sein (nur SID ist unterschiedlich).

In diesem Abschnitt werden die folgenden Szenarien behandelt.

- SAP HANA Systemaktualisierung ohne Trennung von Klonen
- Wird aus dem primären Storage geklont, wobei der Mandantenname der SID entspricht
- Klonen aus standortexternen Backup-Storage
- Klonen aus dem Primärspeicher mit mehreren Mandanten
- Klonvorgang
- SAP HANA Systemaktualisierung mit einem Klonabteilvergang
- Wird aus dem primären Storage geklont, wobei der Mandantenname der SID entspricht
- Klonteilvergang

Voraussetzungen und Einschränkungen

Die in den folgenden Abschnitten beschriebenen Workflows weisen einige Voraussetzungen und Einschränkungen hinsichtlich der SAP HANA-Systemarchitektur und der SnapCenter-Konfiguration auf.

- Die beschriebenen Workflows gelten nur für die SnapCenter Version 5.0 oder höher.
- Die beschriebenen Workflows gelten für SAP HANA MDC-Systeme mit einzelnen Hosts und mehreren Mandanten. SAP HANA Multiple Host-Systeme sind nicht abgedeckt.
- Das SnapCenter SAP HANA Plug-in muss auf dem Ziel-Host implementiert werden, um die automatische

Erkennung von SnapCenter und die Ausführung von Automatisierungsskripten zu ermöglichen.

- Die Workflows gelten für SAP HANA-Systeme mit NFS oder FCP auf physischen Hosts oder für virtuelle Hosts, die in-Guest-NFS-Mounts verwenden.

Laboreinrichtung

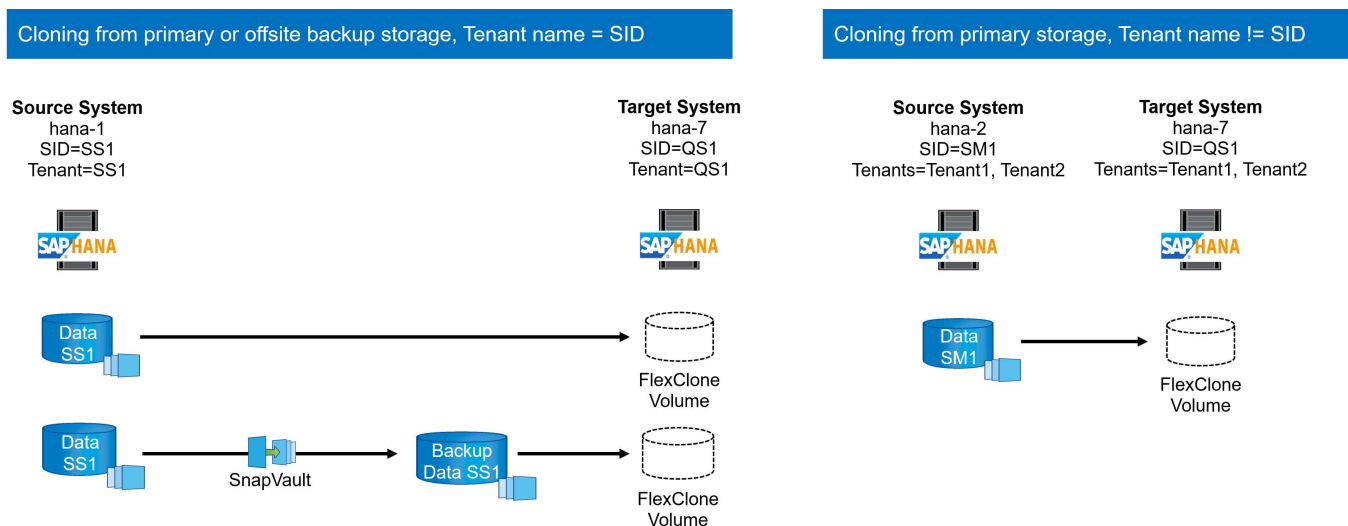
Die Abbildung unten zeigt das Lab-Setup, das für die verschiedenen Optionen zur Systemaktualisierung verwendet wurde.

- Klonen aus dem primären Storage oder externen Backup-Storage. Der Mandantenname entspricht der SID.
 - Quelle SAP HANA System: SS1 mit Mandant SS1
 - Ziel SAP HANA-System: QS1 mit Mandant QS1
- Klonen aus dem primären Storage, mehrere Mandanten.
 - Quell-SAP HANA-System: SM1 mit Tenant1 und Tenant2
 - SAP HANA-Zielsystem: QS1 mit Tenant1 und Tenant2

Es wurden folgende Softwareversionen verwendet:

- SnapCenter 5.0
- SAP HANA Systeme: HANA 2.0 SPS7 Rev. 73
- SLES 15
- ONTAP 9.14P1

Alle SAP HANA-Systeme müssen auf Basis des Konfigurationsleitfadens konfiguriert werden "[SAP HANA auf NetApp AFF Systemen mit NFS](#)". SnapCenter und die SAP HANA-Ressourcen wurden basierend auf dem Best Practice Guide konfiguriert "[Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter](#)".



Erste, einmalige Vorbereitungsschritte

In einem ersten Schritt muss das SAP HANA Zielsystem innerhalb von SnapCenter konfiguriert sein.

1. Installation des SAP HANA-Zielsystems

2. Konfiguration des SAP HANA-Systems in SnapCenter wie in beschrieben ["TR-4614: SAP HANA Backup and Recovery with SnapCenter"](#)
 - a. Konfiguration des SAP HANA Datenbankbenutzers für SnapCenter-Backup-Vorgänge dieser Benutzer muss am Quell- und Zielsystem identisch sein.
 - b. Konfiguration des Schlüssels hdbuserstore für die <sid>-Lösung m mit obigem Backup-Benutzer. Wenn das Automatisierungsskript für die Wiederherstellung verwendet wird, muss der Schlüsselname <SID>-Ausschreiben Y sein
 - c. Implementierung des SnapCenter SAP HANA Plug-ins auf dem Ziel-Host. Das SAP HANA-System wird von SnapCenter automatisch erkannt.
 - d. Konfiguration des SAP HANA-Ressourcenschutzes (optional)

Der erste SAP-Systemaktualisierungsvorgang nach der Erstinstallation wird mit den folgenden Schritten vorbereitet:

1. Herunterfahren des Ziel-SAP HANA-Systems
2. SAP HANA-Datenvolumen unmounten.

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

```
hana-7:/opt/NetApp/snapcenter/scc/etc # cat
/opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh
hana-7:/opt/NetApp/snapcenter/scc/etc #
```

Klonen vom primären Storage mit dem Mandantennamen SID

In diesem Abschnitt wird der Workflow zur Systemaktualisierung von SAP HANA beschrieben, bei dem der Mandantennamen am Quell- und Zielsystem mit der SID identisch ist. Das Klonen des Storage wird im Primärspeicher durchgeführt und die Recovery wird mit dem Skript automatisiert `sc-system-refresh.sh`.

Source System

hana-1
SID=SS1
Tenant=SS1



Target System

hana-7
SID=QS1
Tenant=QS1



FlexClone
Volume

Der Workflow besteht aus den folgenden Schritten:

1. Wenn die SAP HANA-Persistenz-Verschlüsselung im Quellsystem aktiviert ist, müssen die Verschlüsselungsroot-Schlüssel einmal importiert werden. Ein Import ist auch erforderlich, wenn die Schlüssel im Quellsystem geändert wurden. Siehe Kapitel [„Considerations for SAP HANA System Refresh Operations using Storage Snapshot Backups“](#)
2. Wurde das SAP HANA-Zielsystem in SnapCenter geschützt, so muss zunächst der Schutz entfernt werden.
3. Workflow zur Erstellung von SnapCenter Klonen
 - a. Wählen Sie Snapshot Backup aus dem SAP HANA-Quellsystem SS1 aus.
 - b. Wählen Sie den Zielhost aus, und stellen Sie die Speichernetzwerk-Schnittstelle des Zielhosts bereit.
 - c. Geben Sie SID des Zielsystems, in unserem Beispiel QS1
 - d. Stellen Sie optional ein Skript für die Wiederherstellung als Post-Clone-Vorgang bereit.
4. Klonvorgang für SnapCenter:
 - a. Erstellt ein FlexClone Volume basierend auf ausgewähltem Snapshot Backup des SAP HANA Quellsystems.
 - b. Exportiert das FlexClone Volume zur Ziel-Host-Storage-Netzwerkschnittstelle oder Initiatorgruppe.
 - c. Mount-Vorgang wird von FlexClone Volume auf dem Ziel-Host gemountet.
 - d. Führt ein Wiederherstellungsskript für Vorgänge nach dem Klonen aus, falls zuvor konfiguriert. Andernfalls muss das Recovery manuell durchgeführt werden, wenn der SnapCenter Workflow abgeschlossen ist.
 - Recovery der Systemdatenbank
 - Wiederherstellung der Mandantendatenbank mit Mandantenname = QS1.
5. Optional können Sie die SAP HANA-Zielressource in SnapCenter schützen.

Die folgenden Screenshots zeigen die erforderlichen Schritte.

1. Wählen Sie eine Snapshot-Sicherung aus dem Quellsystem SS1 aus, und klicken Sie auf Klonen.

The screenshot shows the NetApp SnapCenter interface. On the left, there's a sidebar with a search bar and a list of systems: DT1, QS1, SM1, SS1, SS2, and SS2. The main area displays the 'SS1 Topology' with a 'Manage Copies' section showing '14 Backups' and '0 Clones' for local copies, and '5 Backups' and '0 Clones' for vault copies. A 'Summary Card' on the right shows '21 Backups', '19 Snapshot based backups', '2 File-based backups', '0 Clones', and '0 Snapshots Locked'. Below this is a table of 'Primary Backup(s)' with columns: Backup Name, Snapshot Lock Expiration, Count, and End Date. The table lists several backups, including 'SnapCenter_hana-1_LocalSnap_Hourly_04-24-2024_07.00.01.4581' and 'SnapCenter_LocalSnap_Hourly_04-23-2024_03.00.01.2297'. At the bottom, an 'Activity' bar shows '5 Completed', '0 Warnings', '0 Failed', '0 Canceled', '0 Running', and '0 Queued'.

1. Wählen Sie den Host aus, auf dem das Zielsystem QS1 installiert ist. QS1 als Ziel-SID eingeben. Die NFS-Export-IP-Adresse muss die Speichernetzwerk-Schnittstelle des Ziel-Hosts sein.



Die eingegebene Ziel-SID steuert, wie SnapCenter die geklonte Ressource verwaltet. Wenn eine Ressource mit der Ziel-SID bereits in SnapCenter konfiguriert ist und mit dem Plug-in-Host übereinstimmt, weist SnapCenter dieser Ressource einfach den Klon zu. Wenn die SID nicht auf dem Ziel-Host konfiguriert ist, erstellt SnapCenter eine neue Ressource.



Es ist wichtig, dass die Zielsystemressource und der Host vor dem Starten des Klon-Workflows in SnapCenter konfiguriert wurden. Andernfalls unterstützt die neue von SnapCenter erstellte Ressource keine automatische Erkennung, und die beschriebenen Workflows funktionieren nicht.

The screenshot shows the 'Clone From Backup' dialog box. It has a sidebar with four steps: 1 Location, 2 Scripts, 3 Notification, and 4 Summary. The '1 Location' step is active, showing a form to 'Select the host to create the clone'. The form has three fields: 'Plug-in host' with the value 'hana-7.sapcc.stl.netapp.com', 'Target Clone SID' with the value 'QS1', and 'NFS Export IP Address' with the value '192.168.175.75'. Each field has an information icon to its right.

Bei einer Fibre-Channel-SAN-Einrichtung ist keine Export-IP-Adresse erforderlich, Sie müssen jedoch im nächsten Bildschirm das verwendete Protokoll angeben.



Die Screenshots zeigen ein anderes Lab-Setup mit einer FibreChannel-Konnektivität.

Clone From Backup

1 Location

2 Settings

3 Scripts

4 Notification

5 Summary

Select the host to create the clone

Plug-in host

cbc-demosrv02.muccbc.hq.netapp.com

Target Clone SID

H12

NFS Export IP Address

Clone From Backup

1 Location

2 Settings

3 Scripts

4 Notification

5 Summary

LUN Map Settings

Igroup protocol

FCP

Mit Azure NetApp Files und einem manuellen QoS-Kapazitäts-Pool müssen Sie den maximalen Durchsatz für das neue Volume erzielen. Stellen Sie sicher, dass der Kapazitäts-Pool über genügend Reserven verfügt, sonst schlägt der Klon-Workflow fehl.



Die Screenshots zeigen ein anderes Lab Setup, das in Microsoft Azure mit Azure NetApp Files läuft.

Clone From Backup

1 Location

2 Scripts

3 Notification

4 Summary

Select the host to create the clone

Plug-in host

vm-s01.1h05kdpkcgaujd4qsseqldygg.bx.i

Target Clone SID

S01

NFS Export IP Address

10.1.8.101

Capacity Pool Max. Throughput (MiB/s)

25

1. Geben Sie die optionalen Post-Clone-Skripte mit den erforderlichen Befehlszeilenoptionen ein. In unserem Beispiel verwenden wir ein Post-Clone-Skript, um die SAP HANA Datenbank-Recovery auszuführen.

Clone From Backup ✕

1

Location

2

Scripts

3

Notification

4

Summary

The following commands will run on the Plug-in Host: **hana-7.sapcc.stl.netapp.com**

Enter optional commands to run before performing a clone operation ⓘ

Pre clone command

Enter optional commands to run after performing a clone operation ⓘ

Post clone command

/mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh
recover

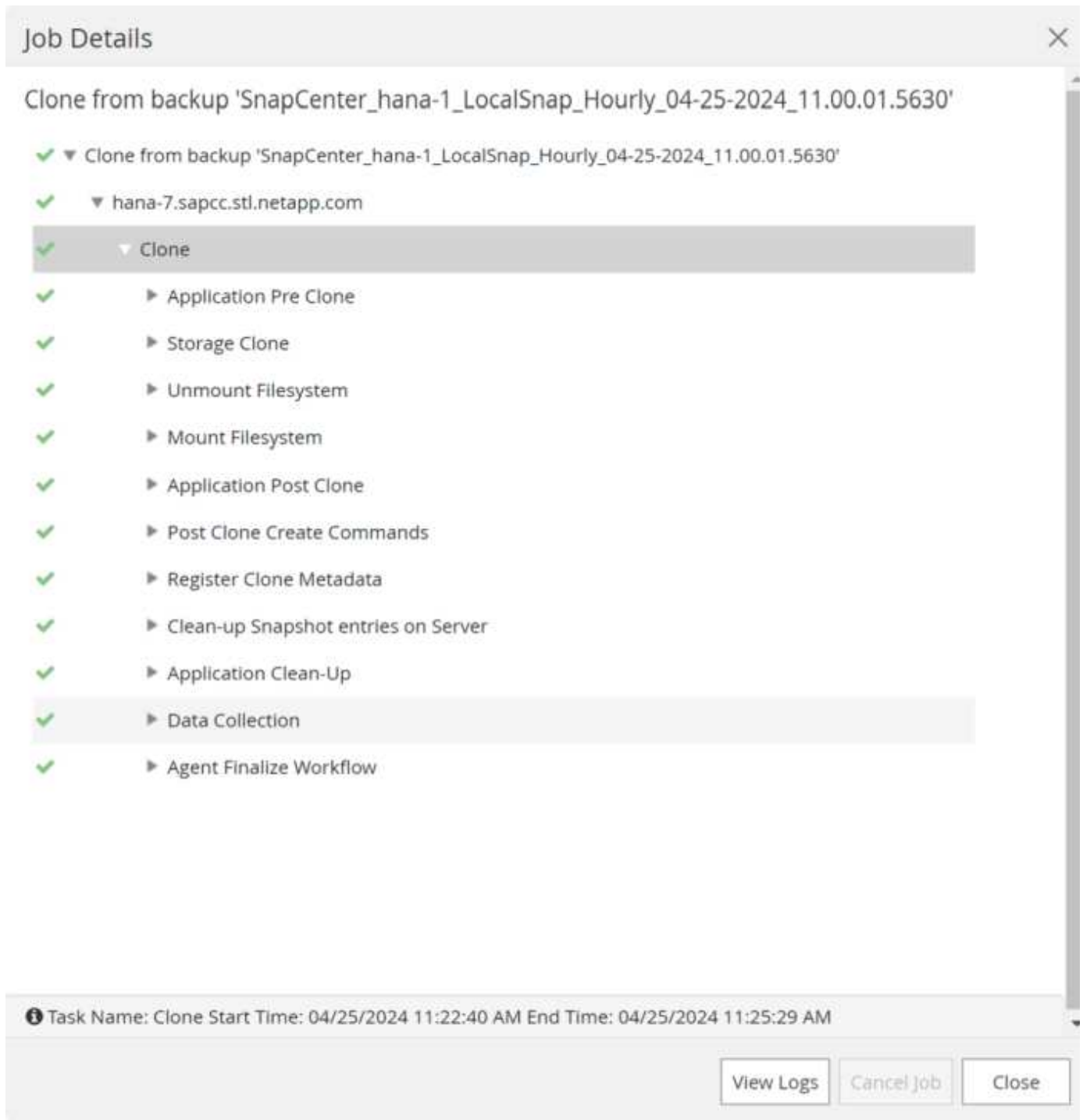


Wie bereits besprochen, ist die Verwendung des Wiederherstellungsskripts optional. Die Wiederherstellung kann auch manuell durchgeführt werden, nachdem der SnapCenter Klon-Workflow abgeschlossen ist.



Das Skript für den Wiederherstellungsvorgang stellt die SAP HANA-Datenbank mithilfe des Vorgangs „Clear Logs“ auf den Zeitpunkt des Snapshots wieder her und führt keine Forward Recovery aus. Wenn eine Rückführung auf einen bestimmten Zeitpunkt erforderlich ist, muss die Wiederherstellung manuell durchgeführt werden. Eine manuelle vorwärts-Wiederherstellung erfordert außerdem, dass die Protokoll-Backups aus dem Quellsystem auf dem Ziel-Host verfügbar sind.

1. Im Bildschirm Jobdetails in SnapCenter wird der Fortschritt des Vorgangs angezeigt. Die Job-Details zeigen außerdem, dass die Gesamtlaufzeit einschließlich Datenbank-Recovery weniger als 3 Minuten beträgt.



1. Die Protokolldatei des `sc-system-refresh` Skripts zeigt die verschiedenen Schritte an, die für den Wiederherstellungsvorgang ausgeführt wurden. Das Skript liest die Liste der Mandanten aus der Systemdatenbank und führt eine Wiederherstellung aller vorhandenen Mandanten durch.

```
20240425112328###hana-7###sc-system-refresh.sh: Script version: 3.0
hana-7:/mnt/sapcc-share/SAP-System-Refresh # cat sap-system-refresh-
QS1.log
20240425112328###hana-7###sc-system-refresh.sh: *****
Starting script: recovery operation *****
20240425112328###hana-7###sc-system-refresh.sh: Recover system database.
```

```

20240425112328###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/HDB11/exe/Python/bin/python
/usr/sap/QS1/HDB11/exe/python_support/recoverSys.py --command "RECOVER
DATA USING SNAPSHOT CLEAR LOG"
20240425112346###hana-7###sc-system-refresh.sh: Wait until SAP HANA
database is started ....
20240425112347###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112357###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112407###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112417###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112428###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112438###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425112448###hana-7###sc-system-refresh.sh: Status: GREEN
20240425112448###hana-7###sc-system-refresh.sh: HANA system database
started.
20240425112448###hana-7###sc-system-refresh.sh: Checking connection to
system database.
20240425112448###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY 'select * from sys.m_databases;'
DATABASE_NAME,DESCRIPTION,ACTIVE_STATUS,ACTIVE_STATUS_DETAILS,OS_USER,OS_G
ROUP,RESTART_MODE,FALLBACK_SNAPSHOT_CREATE_TIME
"SYSTEMDB","SystemDB-QS1-11","YES","","","","DEFAULT",?
"QS1","QS1-11","NO","ACTIVE","","","DEFAULT",?
2 rows selected (overall time 16.225 msec; server time 860 usec)
20240425112448###hana-7###sc-system-refresh.sh: Successfully connected to
system database.
20240425112449###hana-7###sc-system-refresh.sh: Tenant databases to
recover: QS1
20240425112449###hana-7###sc-system-refresh.sh: Found inactive
tenants(QS1) and starting recovery
20240425112449###hana-7###sc-system-refresh.sh: Recover tenant database
QS1.
20240425112449###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY RECOVER DATA FOR QS1 USING
SNAPSHOT CLEAR LOG
0 rows affected (overall time 22.138599 sec; server time 22.136268 sec)
20240425112511###hana-7###sc-system-refresh.sh: Checking availability of
Indexserver for tenant QS1.
20240425112511###hana-7###sc-system-refresh.sh: Recovery of tenant
database QS1 succesfully finished.
20240425112511###hana-7###sc-system-refresh.sh: Status: GREEN
20240425112511###hana-7###sc-system-refresh.sh: *****
Finished script: recovery operation *****
hana-7:/mnt/sapcc-share/SAP-System-Refresh

```

1. Nach Abschluss des SnapCenter-Jobs ist der Klon in der Topologieweise des Quellsystems sichtbar.

The screenshot shows the NetApp SnapCenter interface. On the left, a sidebar lists systems: DT1, QS1, SM1, SS1 (selected), SS2, and SS2. The main area displays the 'SS1 Topology' with a 'Manage Copies' section showing 14 Backups, 1 Clone, and 5 Backups in the Vault. A 'Summary Card' on the right shows 21 Backups, 19 Snapshot based backups, 2 File Based backups, 1 Clone, and 0 Snapshots Locked. Below this is a table for 'Primary Clone(s)' with columns: Clone SID, Clone Host, Clone Name, Start Date, and End date. The table contains one entry for QS1. At the bottom, an 'Activity' bar shows job status: 1 Completed, 2 Warnings, 1 Failed, 0 Canceled, 2 Running, and 0 Queued.

Clone SID	Clone Host	Clone Name	Start Date	End date
QS1	hana-7.sapcc.stl.netapp.com	hana-1_sapcc_stl_netapp_com_hana_MDC_SS1_clone__102162_MDC_SS1_04-22-2024_09:54:34	04/24/2024 9:47:10 AM	04/24/2024 9:48:00 AM

1. Die SAP HANA Datenbank läuft nun.
2. Wenn Sie das Ziel-SAP HANA-System schützen möchten, müssen Sie die automatische Erkennung ausführen, indem Sie auf die Zielsystemressource klicken.

The 'Configure Database' dialog box is shown with the following fields:

- Plug-in host: hana-7.sapcc.stl.netapp.com
- HDBSQL OS User: qs1adm
- HDB Secure User Store Key: QS1KEY

At the bottom right, there are 'Cancel' and 'OK' buttons.

Wenn der automatische Erkennungsprozess abgeschlossen ist, wird das neue geklonte Volume im Abschnitt „Storage-Platzbedarf“ aufgeführt.

NetApp SnapCenter®

SAP HANA

Search databases

System

DT1

Q51

SM1

SS1

SS2

SS2

Total 6

Resource - Details

Details for selected resource

Type	Multitenant Database Container
HANA System Name	Q51
SID	Q51
Tenant Databases	Q51
Plug-in Host	hana-7.sapcc.stl.netapp.com
HDB Secure User Store Key	Q51KEY
HDBSQL OS User	qs1adm
Log backup location	/usr/sap/Q51/HDB11/backup/log
Backup catalog location	/usr/sap/Q51/HDB11/backup/log
System Replication	None
plug-in name	SAP HANA
Last backup	None
Resource Groups	None
Policy	None
Discovery Type	Auto
Backup Name	SnapCenter_hana-1_LocalSnap_Hourly_06-25-2024_03.00.01.8458
Backup Name of Clone	SnapCenter_hana-1_LocalSnap_Hourly_06-25-2024_03.00.01.8458

Storage Footprint

SVM	Volume	Junction Path	LUN/Qtree
hana-primary	SS1_data_mnt00001_Clone_06252405324571927	/SS1_data_mnt00001_Clone_06252405324571927	

Activity The 5 most recent jobs are displayed

4 Completed 0 Warnings 1 Failed 0 Canceled 0 Running 0 Queued

Durch erneutes Klicken auf die Ressource kann der Datenschutz für das aktualisierte Q51-System konfiguriert werden.

NetApp SnapCenter®

SAP HANA

Search databases

System

DT1

Q51

SM1

SS1

SS2

SS2

Multitenant Database Container - Protect

Protect the resource by selecting protection policies, schedules, and notification settings.

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

1 Resource 2 Application Settings 3 Policies 4 Notification 5 Summary

Provide format for custom snapshot name

☐ Use custom name format for Snapshot copy

Klonen aus standortexternen Backup-Storage

In diesem Abschnitt wird der Workflow zur Systemaktualisierung von SAP HANA beschrieben, bei dem der Mandantennamen am Quell- und Zielsystem mit der SID identisch ist. Das Klonen von Speichern wird im externen Backup-Speicher ausgeführt und wird mithilfe des Skripts `sc-System-refresh.sh` weiter automatisiert.

Source System

hana-1
SID=SS1
Tenant=SS1



SnapVault



Target System

hana-7
SID=QS1
Tenant=QS1



FlexClone
Volume

Der einzige Unterschied im Workflow der SAP HANA Systemaktualisierung zwischen dem Klonen des primären und externen Backup-Storage ist die Auswahl des Snapshot Backups in SnapCenter. Für das Klonen von Backup-Storage außerhalb des Standorts müssen zunächst die sekundären Backups und anschließend die Auswahl des Snapshot-Backups ausgewählt werden.

NetApp SnapCenter®

SAP HANA

SS1 Topology

Search databases

System

QS1

SM1

SS1

SS2

SS2

Manage Copies

14 Backups
0 Clones
Local copies

9 Backups
0 Clones
Vault copies

Summary Card

25 Backups

23 Snapshot based backups

2 File-based backups

0 Clones

Secondary Vault Backup(s)

search

Backup Name	Count	IF	End Date
SnapCenter_LocalSnapAndSnapVault_Daily_05-11-2022_05.00.02.9288	1		05/11/2022 5:01:01 AM
SnapCenter_LocalSnapAndSnapVault_Daily_05-10-2022_05.00.02.9444	1		05/10/2022 5:01:01 AM
SnapCenter_LocalSnapAndSnapVault_Daily_05-09-2022_05.00.02.9432	1		05/09/2022 5:01:01 AM
SnapCenter_LocalSnapAndSnapVault_Daily_05-08-2022_05.00.02.9894	1		05/08/2022 5:01:01 AM
SnapCenter_LocalSnapAndSnapVault_Daily_05-07-2022_05.00.02.9253	1		05/07/2022 5:01:01 AM
SnapCenter_LocalSnapAndSnapVault_Daily_05-06-2022_05.00.02.9333	1		05/06/2022 5:01:01 AM
SnapCenter_LocalSnapAndSnapVault_Daily_05-05-2022_05.00.03.8844	1		05/05/2022 5:01:02 AM
SnapCenter_LocalSnapAndSnapVault_Daily_05-04-2022_05.00.03.0342	1		05/04/2022 5:01:01 AM
SnapCenter_LocalSnapAndSnapVault_Daily_05-03-2022_05.00.02.9761	1		05/03/2022 5:01:01 AM

Clone From Backup

Clone Restore

Wenn mehrere sekundäre Speicherorte für das ausgewählte Backup vorhanden sind, müssen Sie das erforderliche Zielvolume auswählen.

Clone From Backup ✕

1 Location

2 Scripts

3 Notification

4 Summary

Select the host to create the clone

Plug-in host

hana-7.sapcc.stl.netapp.com

i

Target Clone SID

QS1

i

NFS Export IP Address

192.168.175.75

i

Secondary storage location : Snap Vault / Snap Mirror

Source Volume

Destination Volume

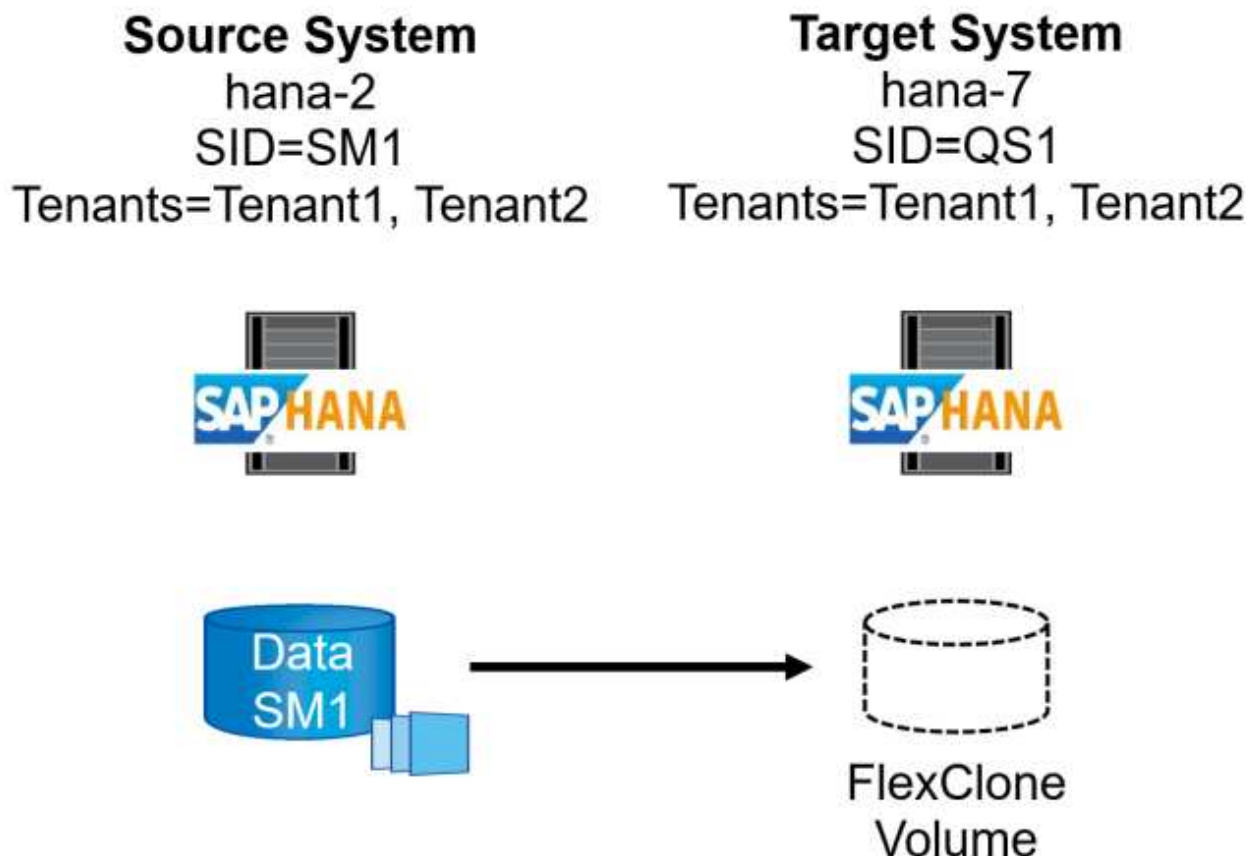
hana-primary.sapcc.stl.netapp.com:SS1_data_mnt00001

hana-backup.sapcc.stl.netapp.com:SS1_data

Alle nachfolgenden Schritte sind mit dem Workflow zum Klonen aus dem Primärspeicher identisch.

Klonen eines SAP HANA Systems mit mehreren Mandanten

In diesem Abschnitt wird der Workflow zur Aktualisierung des SAP HANA-Systems mit mehreren Mandanten beschrieben. Das Klonen von Storage wird im Primär-Storage durchgeführt und weitere automatisiert mithilfe des Skripts `sc-system-refresh.sh`.



Die erforderlichen Schritte in SnapCenter sind identisch mit den Schritten, die im Abschnitt „Klonen von primärem Storage mit Mandantenname gleich SID“ beschrieben wurden. Der einzige Unterschied besteht in der Wiederherstellung des Mandanten innerhalb des Skripts `sc-system-refresh.sh`, wo alle Mandanten wiederhergestellt werden.

```
20240430070214###hana-7###sc-system-refresh.sh:
*****
*****
20240430070214###hana-7###sc-system-refresh.sh: Script version: 3.0
20240430070214###hana-7###sc-system-refresh.sh: *****
Starting script: recovery operation *****
20240430070214###hana-7###sc-system-refresh.sh: Recover system database.
20240430070214###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/HDB11/exe/Python/bin/python
/usr/sap/QS1/HDB11/exe/python_support/recoverSys.py --command "RECOVER
DATA USING SNAPSHOT CLEAR LOG"
[140310725887808, 0.008] >> starting recoverSys (at Tue Apr 30 07:02:15
2024)
[140310725887808, 0.008] args: ()
[140310725887808, 0.008] keys: \{'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'\}
using logfile /usr/sap/QS1/HDB11/hana-7/trace/backup.log
recoverSys started: =====2024-04-30 07:02:15 =====
testing master: hana-7
hana-7 is master
shutdown database, timeout is 120
stop system
stop system on: hana-7
stopping system: 2024-04-30 07:02:15
stopped system: 2024-04-30 07:02:15
creating file recoverInstance.sql
restart database
restart master nameserver: 2024-04-30 07:02:20
start system: hana-7
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2024-04-30T07:02:32-04:00 P0023828 18f2eab9331 INFO RECOVERY RECOVER DATA
finished successfully
recoverSys finished successfully: 2024-04-30 07:02:33
[140310725887808, 17.548] 0
[140310725887808, 17.548] << ending recoverSys, rc = 0 (RC_TEST_OK), after
17.540 secs
20240430070233###hana-7###sc-system-refresh.sh: Wait until SAP HANA
database is started ....
20240430070233###hana-7###sc-system-refresh.sh: Status: GRAY
20240430070243###hana-7###sc-system-refresh.sh: Status: GRAY
```

```

20240430070253###hana-7###sc-system-refresh.sh: Status: GRAY
20240430070304###hana-7###sc-system-refresh.sh: Status: GRAY
20240430070314###hana-7###sc-system-refresh.sh: Status: GREEN
20240430070314###hana-7###sc-system-refresh.sh: HANA system database
started.
20240430070314###hana-7###sc-system-refresh.sh: Checking connection to
system database.
20240430070314###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY 'select * from sys.m_databases;'
20240430070314###hana-7###sc-system-refresh.sh: Succesfully connected to
system database.
20240430070314###hana-7###sc-system-refresh.sh: Tenant databases to
recover: TENANT2
TENANT1
20240430070314###hana-7###sc-system-refresh.sh: Found inactive
tenants(TENANT2
TENANT1) and starting recovery
20240430070314###hana-7###sc-system-refresh.sh: Recover tenant database
TENANT2.
20240430070314###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY RECOVER DATA FOR TENANT2 USING
SNAPSHOT CLEAR LOG
20240430070335###hana-7###sc-system-refresh.sh: Checking availability of
Indexserver for tenant TENANT2.
20240430070335###hana-7###sc-system-refresh.sh: Recovery of tenant
database TENANT2 succesfully finished.
20240430070335###hana-7###sc-system-refresh.sh: Status: GREEN
20240430070335###hana-7###sc-system-refresh.sh: Recover tenant database
TENANT1.
20240430070335###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/SYS/exe/hdb/hdbsql -U QS1KEY RECOVER DATA FOR TENANT1 USING
SNAPSHOT CLEAR LOG
20240430070349###hana-7###sc-system-refresh.sh: Checking availability of
Indexserver for tenant TENANT1.
20240430070350###hana-7###sc-system-refresh.sh: Recovery of tenant
database TENANT1 succesfully finished.
20240430070350###hana-7###sc-system-refresh.sh: Status: GREEN
20240430070350###hana-7###sc-system-refresh.sh: *****
Finished script: recovery operation *****

```

Klonvorgang

Ein neuer Vorgang zur Systemaktualisierung von SAP HANA wird gestartet, indem das Zielsystem mithilfe des SnapCenter-Klonlösch-Vorgangs gereinigt wird.

Wurde das SAP HANA-Zielsystem in SnapCenter geschützt, so muss zunächst der Schutz entfernt werden. Klicken Sie in der Topologieansicht des Zielsystems auf Schutz entfernen.

Der Clone delete Workflow wird nun mit den folgenden Schritten ausgeführt.

1. Wählen Sie den Klon in der Topologieansicht des Quellsystems aus, und klicken Sie auf Löschen.

NetApp SnapCenter®

SAP HANA

SS1 Topology

Manage Copies

14 Backups
1 Clone
Local copies

6 Backups
0 Clones
Vault copies

Summary Card

22 Backups

20 Snapshot based backups

2 File-based backups v1

1 Clone

0 Snapshots Locked

Primary Clone(s)

Clone SID	Clone Host	Clone Name	Start Date	End date
QS1	hana-7.sapcc.stl.netapp.com	hana-1.sapcc.stl.netapp.com_hana_MDC_SS1_clone_102336_MDC_SS1_04-22-2024_09.54.34	04/25/2024 10:41:50 AM	04/25/2024 10:42:38 AM

Total 6

Total 1

Activity

The 5 most recent jobs are displayed

4 Completed 0 Warnings 0 Failed 0 Canceled 1 Running 0 Queued

1. Geben Sie die Skripte vor dem Klonen ein und heben Sie die Bereitstellung mit den erforderlichen Befehlszeilenoptionen ab.

Delete Clone

Cloned volume will be deleted. SnapCenter backups and HANA backup catalog must be deleted manually.

Enter commands to execute before clone deletion

Pre clone delete :

```
/mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh  
shutdown
```

The selected clone(s) will be permanently deleted. If the selected clone contains other resource(s) it will also be deleted.
If the cloned databases are protected then the protection needs to be removed to delete the clone.

Do you want to proceed?

☐ Force Delete

Cancel OK

1. Der Bildschirm „Jobdetails“ in SnapCenter zeigt den Fortschritt des Vorgangs an.

Job Details

Deleting clone 'hana-1_sapcc_stl_netapp_com_ha.....S1__clone__102336_MDC_SS1_04-22-2024_09.54.34'

▼ Deleting clone 'hana-1_sapcc_stl_netapp_com_hana_MDC_SS1__clone__102336_MDC_SS1_04-22-2024_09.54.34'

▼ hana-7.sapcc.stl.netapp.com

▼ Delete Clone

▶ Validate Plugin Parameters

▼ Delete Pre Clone Commands

▶ Unmount Filesystem

▼ Delete Storage Clone

▼ Unregister Clone Metadata

▶ Filesystem Clone Metadata Cleanup

▶ Agent Finalize Workflow

Task Name: Unmount Filesystem Start Time: 04/25/2024 11:11:56 AM End Time: 04/25/2024 11:12:08 AM

View Logs

Cancel Job

Close

1. Die Protokolldatei des `sc-system-refresh` Skripts zeigt die Schritte zum Herunterfahren und Unmounten an.

```

20240425111042###hana-7###sc-system-refresh.sh:
*****
*****
20240425111042###hana-7###sc-system-refresh.sh: Script version: 3.0
20240425111042###hana-7###sc-system-refresh.sh: *****
Starting script: shutdown operation *****
20240425111042###hana-7###sc-system-refresh.sh: Stopping HANA database.
20240425111042###hana-7###sc-system-refresh.sh: sapcontrol -nr 11
-function StopSystem HDB
25.04.2024 11:10:42
StopSystem
OK
20240425111042###hana-7###sc-system-refresh.sh: Wait until SAP HANA
database is stopped ....
20240425111042###hana-7###sc-system-refresh.sh: Status: GREEN
20240425111052###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111103###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111113###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111123###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111133###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111144###hana-7###sc-system-refresh.sh: Status: YELLOW
20240425111154###hana-7###sc-system-refresh.sh: Status: GRAY
20240425111154###hana-7###sc-system-refresh.sh: SAP HANA database is
stopped.
20240425111154###hana-7###sc-system-refresh.sh: *****
Finished script: shutdown operation *****

```

1. Der SAP HANA-Aktualisierungsvorgang kann nun mithilfe des SnapCenter-Klonerstellung erneut gestartet werden.

SAP HANA Systemaktualisierung mit Klonteilvorgang

Ist die Verwendung des Zielsystems für die Systemaktualisierung über einen längeren Zeitraum geplant, ist es sinnvoll, das FlexClone Volume im Rahmen der Systemaktualisierung zu teilen.

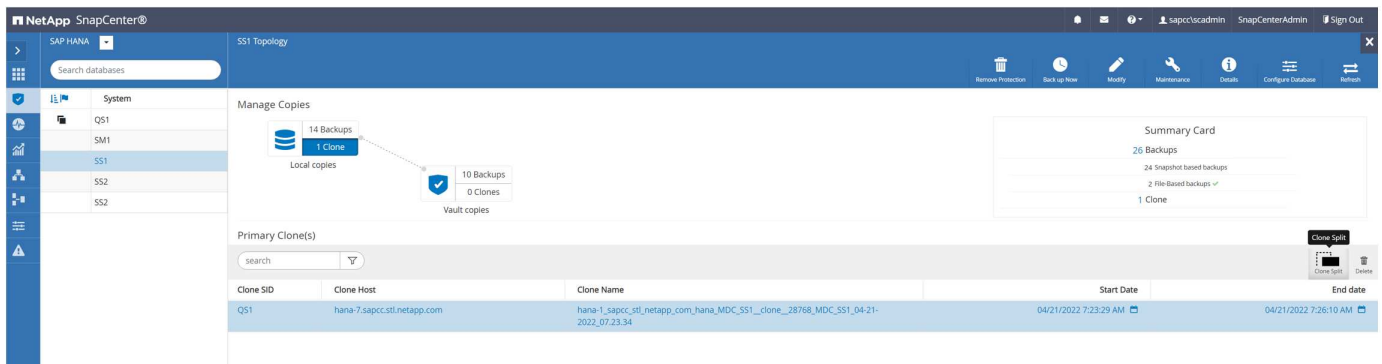


Der Aufspaltung von Klonen blockiert nicht die Verwendung des geklonten Volume und kann somit jederzeit ausgeführt werden, während die SAP HANA Datenbank verwendet wird.

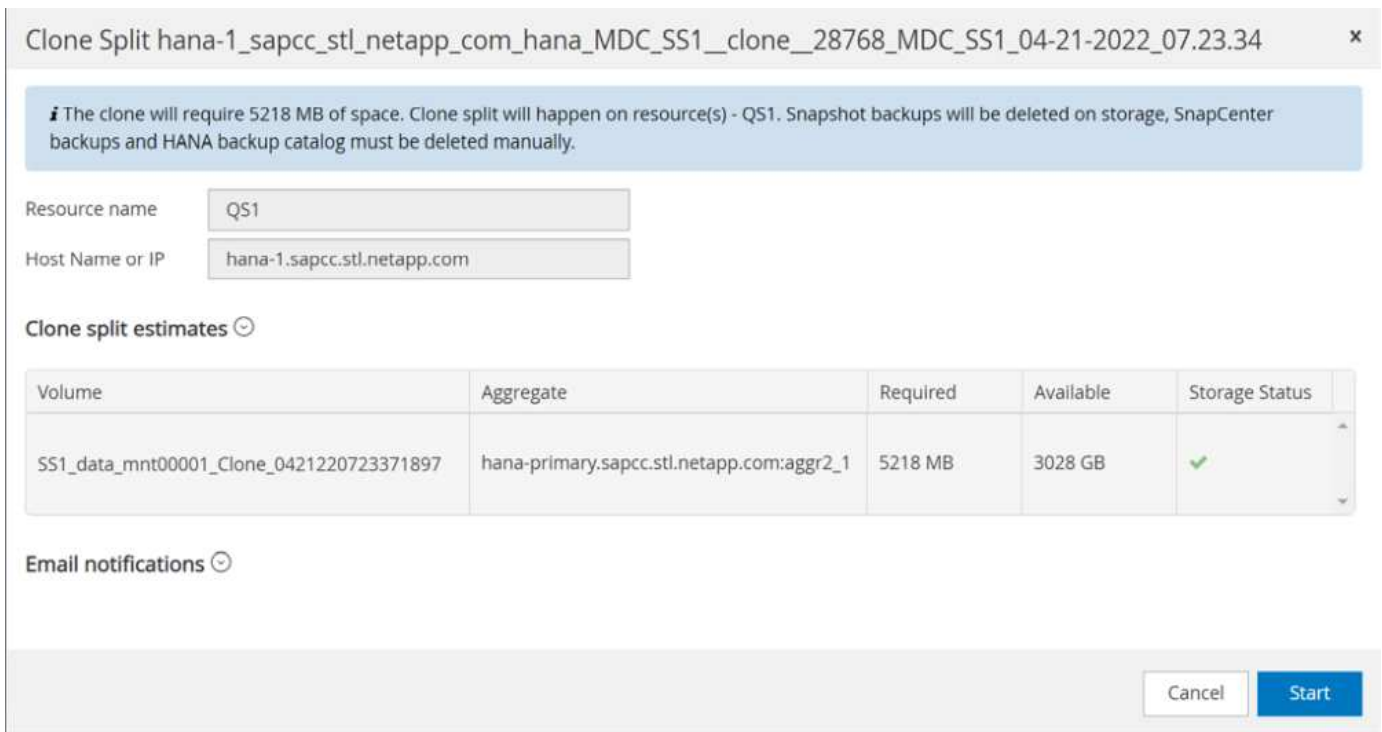


Bei Azure NetApp Files ist der Aufspaltung von Klonen nicht verfügbar, da Azure NetApp Files den Klon nach der Erstellung immer teilt.

Der Clone Split Workflow in SnapCenter wird in der Topologieansicht des Quellsystems initiiert, indem der Klon ausgewählt und auf Clone Split geklickt wird.



Im nächsten Bildschirm wird eine Vorschau angezeigt, die Informationen zur erforderlichen Kapazität für das geteilte Volumen liefert.



Das Jobprotokoll von SnapCenter zeigt den Status des Klonabteilvergangs an.

Job Details

Clone Split Start of Resource 'hana-1_sapcc_stl_ne.....MDC_SS1__clone__28768_MDC_SS1_04-21-2022_07.23.34'

▼ Clone Split Start of Resource 'hana-1_sapcc_stl_netapp_com_hana_MDC_SS1__clone__28768_MDC_SS1_04-21-2022_07.23.34'

▼ SnapCenter.sapcc.stl.netapp.com

▶ Volume Clone Estimate

▶ Volume Clone Split Start

▶ Delete Backups of Clone

▶ Volume Clone Split Status

▶ Clone Split Status for volume SS1_data_mnt00001_Clone_0421220723371897 is 'In Progress'

▶ Clone Split Status for volume SS1_data_mnt00001_Clone_0421220723371897'Completed'

▶ Register Clone Split

▶ Data Collection

▶ Send EMS Messages

Task Name: Volume Clone Split Status Start Time: 04/21/2022 7:51:16 AM End Time:

View Logs

Cancel Job

Close

In der Ressourcenansicht in SnapCenter wird das Zielsystem QS1 nun nicht mehr als geklonte Ressource markiert. Wenn der Klon zurück zur Topologieansicht des Quellsystems angezeigt wird, ist er nicht mehr sichtbar. Das Split-Volume ist jetzt unabhängig vom Snapshot Backup des Quellsystems.

40

System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
QS1	QS1	QS1	None	hana-7.sapcc.stl.netapp.com		LocalSnap	04/21/2022 7:30:50 AM	Backup succeeded
SM1	SM1	TENANT1	None	hana-2.sapcc.stl.netapp.com		LocalSnap	04/21/2022 4:01:01 AM	Backup succeeded
SS1	SS1	SS1	None	hana-1.sapcc.stl.netapp.com		BlockIntegrityCheck LocalSnap LocalSnapAndSnapVault LocalSnap-OnDemand	04/21/2022 7:01:01 AM	Backup succeeded
SS2	SS2	SS2	Enabled (Primary)	hana-3.sapcc.stl.netapp.com	SS2 - HANA System Replication	BlockIntegrityCheck LocalSnapKeep2	04/21/2022 7:57:22 AM	Backup succeeded
SS2	SS2	SS2	Enabled (Secondary)	hana-4.sapcc.stl.netapp.com	SS2 - HANA System Replication	BlockIntegrityCheck LocalSnapKeep2	04/11/2022 2:57:21 AM	Backup succeeded

SS1 Topology

Manage Copies

- Local copies: 14 Backups, 0 Clones
- Vault copies: 10 Backups, 0 Clones

Summary Card

- 26 Backups
- 24 Snapshot based backups
- 2 File Based backups w/
- 0 Clones

Primary Backup(s)

Backup Name	Count	End Date
SnapCenter_LocalSnap_Hourly_04-21-2022_07.00.02.7865	1	04/21/2022 7:01:01 AM
SnapCenter_LocalSnapAndSnapVault_Daily_04-21-2022_05.00.02.8215	1	04/21/2022 5:01:02 AM
SnapCenter_LocalSnap_Hourly_04-21-2022_03.00.01.7085	1	04/21/2022 3:01:00 AM
SnapCenter_LocalSnap_Hourly_04-20-2022_23.00.01.7142	1	04/20/2022 11:01:00 PM
SnapCenter_LocalSnap_Hourly_04-20-2022_19.00.01.9499	1	04/20/2022 7:01:00 PM

Der Aktualisierungs-Workflow nach einem Klonteilvorgang sieht etwas anders aus als der Vorgang ohne Klontrennung. Nach einer Klonaufteilung ist kein Klonvorgang erforderlich, da es sich beim Zieldatenvolume nicht mehr um ein FlexClone Volume handelt.

Der Workflow besteht aus den folgenden Schritten:

1. Wurde das SAP HANA-Zielsystem in SnapCenter geschützt, so muss zunächst der Schutz entfernt werden.
2. Die SAP HANA Datenbank muss heruntergefahren, das Daten-Volume abgehängt und der von SnapCenter erstellte fstab Eintrag entfernt werden. Diese Schritte müssen manuell ausgeführt werden.
3. Der Workflow zur Erstellung von SnapCenter Klonen kann nun wie in den vorherigen Abschnitten beschrieben ausgeführt werden.
4. Nach dem Aktualisierungsvorgang ist das alte Zieldatenvolume noch vorhanden und muss manuell mit z.B. dem ONTAP-Systemmanager gelöscht werden.

SnapCenter Workflow-Automatisierung mit PowerShell Skripten

In den vorherigen Abschnitten wurden die verschiedenen Workflows über die UI von SnapCenter ausgeführt. Alle Workflows können auch mit PowerShell-Skripten oder REST-API-Aufrufen ausgeführt werden, was eine weitere Automatisierung ermöglicht. In den folgenden Abschnitten werden die grundlegenden Beispiele für PowerShell-Skripts für die folgenden Workflows beschrieben.

- Erstellen von Klonen
- Klon löschen



Die Beispielskripte werden wie IS bereitgestellt und von NetApp nicht unterstützt.

Alle Skripte müssen in einem PowerShell Befehlsfenster ausgeführt werden. Bevor die Skripte ausgeführt werden können, muss mithilfe der eine Verbindung zum SnapCenter-Server hergestellt werden `Open-SmConnection` Befehl.

Erstellen von Klonen

Das einfache Skript unten zeigt, wie eine SnapCenter Klonerstellung mithilfe von PowerShell Befehlen ausgeführt werden kann. Das SnapCenter `New-SmClone` Der Befehl wird mit der erforderlichen Befehlszeilenoption für die Lab-Umgebung und dem zuvor erläuterten Automatisierungsskript ausgeführt.

```
$BackupName='SnapCenter_hana-1_LocalSnap_Hourly_06-25-2024_03.00.01.8458'
$JobInfo=New-SmClone -AppPluginCode hana -BackupName $BackupName
-Resources @\{"Host"="hana-1.sapcc.stl.netapp.com";"UID"="MDC\SS1"}
-CloneToInstance hana-7.sapcc.stl.netapp.com -postclonecreatecommands
'/mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh recover'
-NFSEExportIPs 192.168.175.75 -CloneUid 'MDC\QS1'
# Get JobID of clone create job
$Job=Get-SmJobSummaryReport | ?\{$_.JobType -eq "Clone" } | ?\{$_.JobName
-Match $BackupName} | ?\{$_.Status -eq "Running"}
$JobId=$Job.SmJobId
Get-SmJobSummaryReport -JobId $JobId
# Wait until job is finished
do \{ $Job=Get-SmJobSummaryReport -JobId $JobId; write-host $Job.Status;
sleep 20 } while ( $Job.Status -Match "Running" )
Write-Host " "
Get-SmJobSummaryReport -JobId $JobId
Write-Host "Clone create job has been finshed."
```

Die Bildschirmausgabe zeigt die Ausführung des PowerShell-Skripts Clone erstellen.

```

PS C:\Windows\system32> C:\NetApp\clone-create.ps1
SmJobId : 110382
JobCreatedDateTime :
JobStartDateTime : 6/26/2024 9:55:34 AM
JobEndDateTime :
JobDuration :
JobName : Clone from backup 'SnapCenter_hana-1_LocalSnap_Hourly_06-25-
2024_03.00.01.8458'
JobDescription :
Status : Running
IsScheduled : False
JobError :
JobType : Clone
PolicyName :
JobResultData :
Running
Running
Running
Running
Running
Running
Running
Running
Running
Running
Running
Running
Completed
SmJobId : 110382
JobCreatedDateTime :
JobStartDateTime : 6/26/2024 9:55:34 AM
JobEndDateTime : 6/26/2024 9:58:50 AM
JobDuration : 00:03:16.6889170
JobName : Clone from backup 'SnapCenter_hana-1_LocalSnap_Hourly_06-25-
2024_03.00.01.8458'
JobDescription :
Status : Completed
IsScheduled : False
JobError :
JobType : Clone
PolicyName :
JobResultData :
Clone create job has been finshed.

```

Klon löschen

Das einfache Skript unten zeigt, wie eine SnapCenter Klonlösch-Operation mit PowerShell Befehlen

ausgeführt werden kann. Das SnapCenter `Remove-SmClone` Der Befehl wird mit der erforderlichen Befehlszeilenoption für die Lab-Umgebung und dem zuvor erläuterten Automatisierungsskript ausgeführt.

```
$CloneInfo=Get-SmClone |?{$_.CloneName -Match "hana-  
1_sapcc_stl_netapp_com_hana_MDC_SS1" }  
$JobInfo=Remove-SmClone -CloneName $CloneInfo.CloneName -PluginCode hana  
-PreCloneDeleteCommands '/mnt/sapcc-share/SAP-System-Refresh/sc-system-  
refresh.sh shutdown QS1' -UnmountCommands '/mnt/sapcc-share/SAP-System-  
Refresh/sc-system-refresh.sh umount QS1' -Confirm: $False  
Get-SmJobSummaryReport -JobId $JobInfo.Id  
# Wait until job is finished  
do \{ $Job=Get-SmJobSummaryReport -JobId $JobInfo.Id; write-host  
$Job.Status; sleep 20 } while ( $Job.Status -Match "Running" )  
Write-Host " "  
Get-SmJobSummaryReport -JobId $JobInfo.Id  
Write-Host "Clone delete job has been finshed."  
PS C:\NetApp>
```

In der Bildschirmausgabe wird die Ausführung des PowerShell-Skripts `Clone -delete.ps1` angezeigt.

```

PS C:\Windows\system32> C:\NetApp\clone-delete.ps1
SmJobId : 110386
JobCreatedDateTime :
JobStartDateTime : 6/26/2024 10:01:33 AM
JobEndDateTime :
JobDuration :
JobName : Deleting clone 'hana-
1_sapcc_stl_netapp_com_hana_MDC_SS1__clone__110382_MDC_SS1_04-22-
2024_09.54.34'
JobDescription :
Status : Running
IsScheduled : False
JobError :
JobType : DeleteClone
PolicyName :
JobResultData :
Running
Running
Running
Running
Completed
SmJobId : 110386
JobCreatedDateTime :
JobStartDateTime : 6/26/2024 10:01:33 AM
JobEndDateTime : 6/26/2024 10:02:38 AM
JobDuration : 00:01:05.5658860
JobName : Deleting clone 'hana-
1_sapcc_stl_netapp_com_hana_MDC_SS1__clone__110382_MDC_SS1_04-22-
2024_09.54.34'
JobDescription :
Status : Completed
IsScheduled : False
JobError :
JobType : DeleteClone
PolicyName :
JobResultData :
Clone delete job has been finshed.
PS C:\Windows\system32>

```

SAP Systemklon mit SnapCenter

Dieser Abschnitt enthält eine Schritt-für-Schritt-Beschreibung für den SAP-Systemklonvorgang, mit der ein Reparatursystem zur Beseitigung logischer Beschädigung eingerichtet werden kann.

Die folgende Abbildung fasst die erforderlichen Schritte für einen SAP-Systemklonvorgang mit SnapCenter

zusammen.

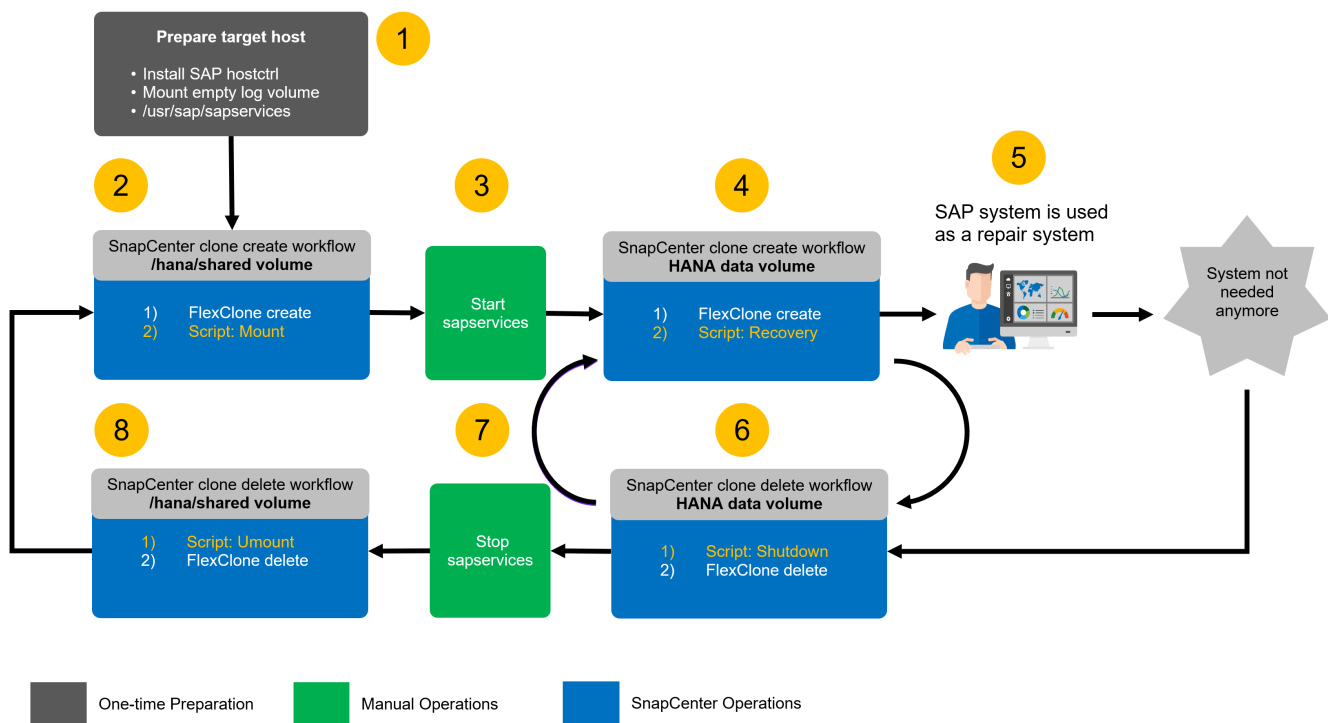
1. Bereiten Sie den Zielhost vor.
2. Workflow für die SAP HANA-Freigabe-Volumes durch SnapCenter-Klon erstellen
3. Starten Sie SAP HANA Services.
4. SnapCenter Clone erstellen Sie einen Workflow für das SAP HANA Daten-Volume einschließlich Datenbank-Recovery.
5. Das SAP HANA-System kann nun als Reparatursystem eingesetzt werden.



Wenn Sie das System auf ein anderes Snapshot Backup zurücksetzen müssen, reichen die Schritte 6 und Schritt 4 aus. Das SAP HANA Shared Volume kann weiterhin gemountet werden.

Wenn das System nicht mehr benötigt wird, erfolgt die Bereinigung mit den folgenden Schritten.

6. SnapCenter Clone delete Workflow für das SAP HANA Daten-Volume einschließlich Datenbank-Shutdown.
7. Stoppen Sie SAP HANA Services.
8. SnapCenter Clone delete Workflow für das SAP HANA Shared Volume.



Voraussetzungen und Einschränkungen

Die in den folgenden Abschnitten beschriebenen Workflows weisen einige Voraussetzungen und Einschränkungen hinsichtlich der SAP HANA-Systemarchitektur und der SnapCenter-Konfiguration auf.

- Der beschriebene Workflow gilt für SAP HANA MDC-Systeme mit einem Host. Mehrere Hostsysteme werden nicht unterstützt.
- Das SnapCenter SAP HANA-Plug-in muss auf dem Ziel-Host implementiert werden, um die Ausführung von Automatisierungsskripts zu ermöglichen.

- Der Workflow wurde für NFS validiert. Die Automatisierung `script sc-mount-volume.sh`, die verwendet wird, um das SAP HANA Shared Volume zu mounten, unterstützt nicht FCP. Dieser Schritt muss entweder manuell oder durch erweitern des Skripts durchgeführt werden.
- Der beschriebene Workflow gilt nur für die SnapCenter Version 5.0 oder höher.

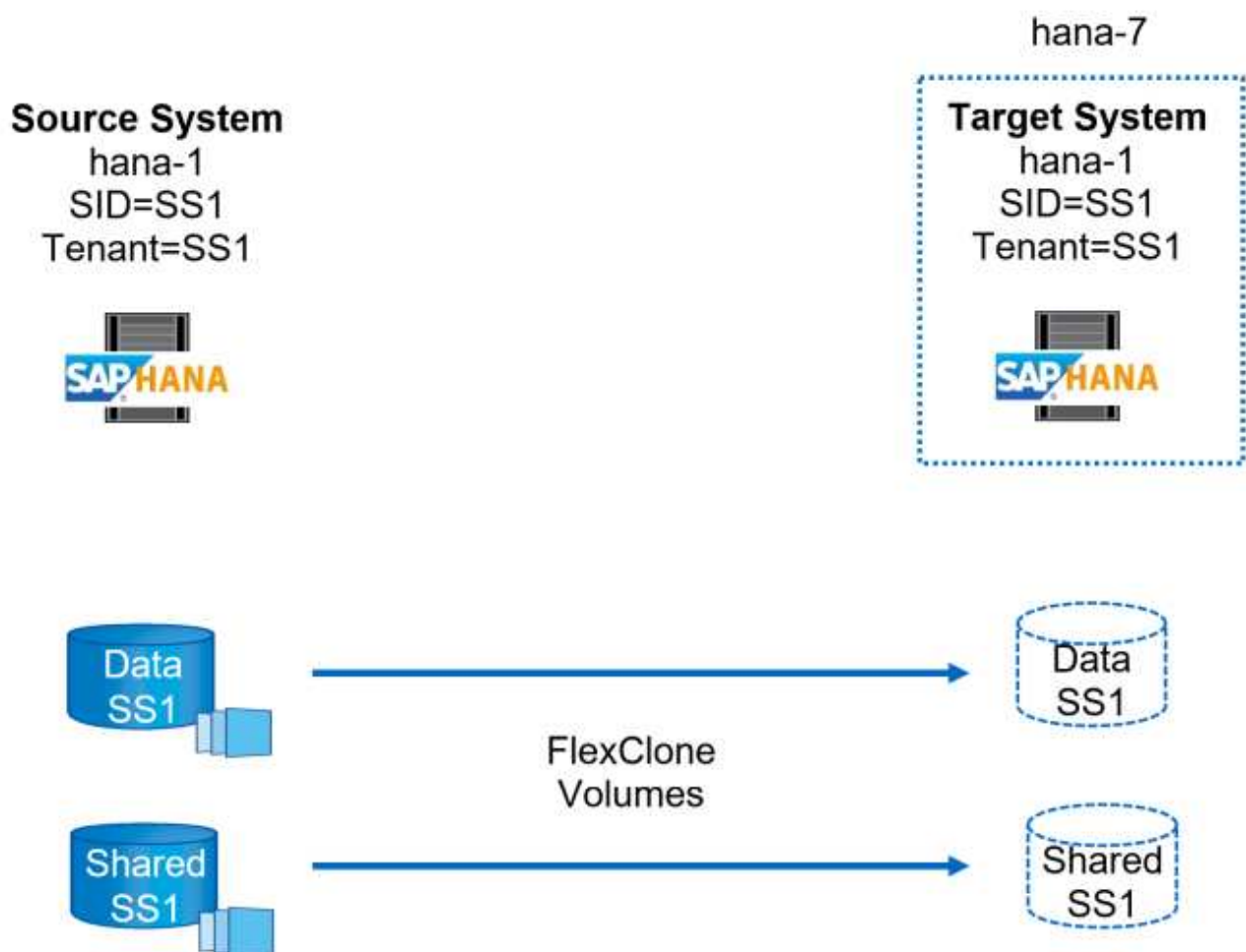
Laboreinrichtung

Die Abbildung unten zeigt das Lab-Setup, das für den Klonvorgang des Systems verwendet wird.

Es wurden folgende Softwareversionen verwendet:

- SnapCenter 5.0
- SAP HANA Systems: HANA 2.0 SPS6 Rev.61
- SLES 15
- ONTAP 9.7 P7

Alle SAP HANA-Systeme müssen auf Basis des Konfigurationsleitfadens konfiguriert werden "[SAP HANA auf NetApp AFF Systemen mit NFS](#)". SnapCenter und die SAP HANA-Ressourcen wurden basierend auf dem Best Practice Guide konfiguriert "[Technischer Bericht: SAP HANA Backup and Recovery with SnapCenter](#)".



Vorbereitung des Ziel-Hosts

In diesem Abschnitt werden die Vorbereitungsschritte beschrieben, die auf einem Server erforderlich sind, der als Systemklonziel verwendet wird.

Während des normalen Betriebs kann der Ziel-Host für andere Zwecke verwendet werden, zum Beispiel als SAP HANA QA oder Testsystem. Daher müssen die meisten der beschriebenen Schritte ausgeführt werden, wenn der Systemklonvorgang angefordert wird. Zum anderen können die relevanten Konfigurationsdateien, wie `/etc/fstab` und `/usr/sap/sapservices` dann einfach durch Kopieren der Konfigurationsdatei in die Produktion gebracht werden.

Zur Vorbereitung des Ziel-Hosts gehört auch das Herunterfahren des SAP HANA QA- oder Testsystems.

Hostname und IP-Adresse des Zielservers

Der Hostname des Zielservers muss mit dem Hostnamen des Quellsystems identisch sein. Die IP-Adresse kann unterschiedlich sein.



Ein ordnungsgemäßes Fechten des Zielservers muss eingerichtet werden, damit er nicht mit anderen Systemen kommunizieren kann. Wenn kein ordnungsgemäßes Fechten vorhanden ist, kann das geklonte Produktionssystem Daten mit anderen Produktionssystemen austauschen.



In unserem Labor-Setup haben wir den Hostnamen des Zielsystems nur intern aus der Perspektive des Zielsystems geändert. Extern war der Host immer noch mit dem Hostnamen hana-7 zugänglich. Bei der Anmeldung beim Host ist der Host selbst hana-1.

Erforderliche Software installieren

Die SAP-Hostagent-Software muss auf dem Zielsystem installiert sein. Umfassende Informationen finden Sie im ["SAP Host Agent"](#) SAP-Hilfeportal.

Das SnapCenter SAP HANA-Plug-in muss über den zusätzlichen Host-Vorgang innerhalb von SnapCenter auf dem Ziel-Host implementiert werden.

Konfigurieren von Benutzern, Ports und SAP-Diensten

Die erforderlichen Anwender und Gruppen für die SAP HANA-Datenbank müssen auf dem Zielsystem verfügbar sein. In der Regel wird die zentrale Benutzerverwaltung verwendet. Daher sind keine Konfigurationsschritte auf dem Zielsystem erforderlich. Die für die SAP HANA-Datenbank erforderlichen Ports müssen auf den Ziel-Hosts konfiguriert werden. Die Konfiguration kann vom Quellsystem kopiert werden, indem die Datei `/etc/Services` auf den Zielsystem kopiert wird.

Die erforderlichen SAP Services-Einträge müssen auf dem Zielhost verfügbar sein. Die Konfiguration kann durch Kopieren des aus dem Quellsystem kopierten `/usr/sap/sapservices` Datei auf dem Zielsystem. Die folgende Ausgabe zeigt die erforderlichen Einträge für die im Lab-Setup verwendete SAP HANA-Datenbank.

```
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/SS1/HDB00/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/SS1/HDB00/exe/sapstartsrv
pf=/usr/sap/SS1/SYS/profile/SS1_HDB00_hana-1 -D -u ssladm
limit.descriptors=1048576
```

Vorbereiten des Protokoll- und Protokollvolumes

Da Sie das Protokoll-Volume nicht aus dem Quellsystem klonen müssen und eine Wiederherstellung mit der Option Protokoll löschen durchgeführt wird, muss ein leeres Protokoll-Volume auf dem Zielhost vorbereitet sein.

Da das Quellsystem mit einem separaten Protokoll-Backup-Volume konfiguriert wurde, muss ein leeres Protokoll-Backup-Volume vorbereitet und an denselben Bereitstellungspunkt wie am Quellsystem angehängt werden.

```
hana-1:/# cat /etc/fstab
192.168.175.117:/SS1_repair_log_mnt00001 /hana/log/SS1/mnt00001 nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsiz=1048576,intr,noatime,nolock 0
0
192.168.175.117:/SS1_repair_log_backup /mnt/log-backup nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsiz=1048576,intr,noatime,nolock 0
0
```

Innerhalb des Protokollvolumens hdb* müssen Sie Unterverzeichnisse auf die gleiche Weise erstellen wie beim Quellsystem.

```
hana-1:/ # ls -al /hana/log/SS1/mnt00001/
total 16
drwxrwxrwx 5 root root 4096 Dec 1 06:15 .
drwxrwxrwx 1 root root 16 Nov 30 08:56 ..
drwxr-xr-- 2 ssladm sapsys 4096 Dec 1 06:14 hdb00001
drwxr-xr-- 2 ssladm sapsys 4096 Dec 1 06:15 hdb00002.00003
drwxr-xr-- 2 ssladm sapsys 4096 Dec 1 06:15 hdb00003.00003
```

Innerhalb des Protokoll-Backup-Volumes müssen Sie Unterverzeichnisse für das System und die Mandantendatenbank erstellen.

```
hana-1:/ # ls -al /mnt/log-backup/
total 12
drwxr-xr-- 2 ssladm sapsys 4096 Dec 1 04:48 .
drwxr-xr-- 2 ssladm sapsys 4896 Dec 1 03:42 ..
drwxr-xr-- 2 ssladm sapsys 4096 Dec 1 06:15 DB_SS1
drwxr-xr-- 2 ssladm sapsys 4096 Dec 1 06:14 SYSTEMDB
```

* Dateisystemeinschübe vorbereiten*

Die Mount-Punkte für die Daten und das freigegebene Volume müssen vorbereitet werden.

Mit unserem Beispiel, die Verzeichnisse `/hana/data/SS1/mnt00001`, `/hana/shared` und `usr/sap/SS1` müssen erstellt werden.

Scriptausführung vorbereiten

Sie müssen die Skripte hinzufügen, die auf dem Zielsystem ausgeführt werden sollen, um die Konfigurationsdatei SnapCenter allowed commands hinzuzufügen.

```
hana-7:/opt/NetApp/snapcenter/scc/etc # cat
/opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh
command: /mnt/sapcc-share/SAP-System-Refresh/sc-mount-volume.sh
hana-7:/opt/NetApp/snapcenter/scc/etc #
```

Klonen des gemeinsamen HANA Volumes

1. Wählen Sie eine Snapshot-Sicherung aus dem SS1 Shared Volume des Quellsystems aus, und klicken Sie auf Klonen.

Backup Name	Count	End Date
SnapCenter_LocalSnap_Hourly_05-13-2022_05.04.01.8012	1	05/13/2022 5:04:12 AM
SnapCenter_LocalSnap_Hourly_05-13-2022_01.04.01.9799	1	05/13/2022 1:04:12 AM
SnapCenter_LocalSnap_Hourly_05-12-2022_21.04.01.8899	1	05/12/2022 9:04:12 PM

1. Wählen Sie den Host aus, auf dem das Ziel-Reparatursystem vorbereitet wurde. Die NFS-Export-IP-Adresse muss die Speichernetzwerk-Schnittstelle des Ziel-Hosts sein. Als Ziel-SID halten Sie die gleiche SID wie das Quellsystem. In unserem Beispiel SS1.

Clone From Backup
×

1 Location
2 Scripts
3 Notification
4 Summary

Select the host to create the clone

Plug-in host
hana-7.sapcc.stl.netapp.com
i

Target Clone SID
SS1
i

NFS Export IP Address
192.168.175.75
i

1. Geben Sie das Mount-Skript mit den erforderlichen Befehlszeilenoptionen ein.



Das SAP HANA-System verwendet ein einzelnes Volume sowohl für `/hana/shared` als auch für `/usr/sap/SS1`, getrennt in Unterverzeichnissen, wie im Konfigurationshandbuch empfohlen ["SAP HANA auf NetApp AFF Systemen mit NFS"](#). Das Skript `sc-mount-volume.sh` unterstützt diese Konfiguration mit einer speziellen Befehlszeilenoption für den Mount-Pfad. Wenn die Befehlszeilenoption `Mount path` dem Wert `usr-sap-and-shared` entspricht, hängt das Skript die freigegebenen Unterverzeichnisse und `usr-sap` entsprechend im Volume an.

Clone From Backup

1 Location

2 Scripts

3 Notification

4 Summary

Enter optional commands to run before performing a clone operation ⓘ

Pre clone command

Enter optional commands to mount a file system to a host ⓘ

Mount command

/mnt/sapcc-share/SAP-System-Refresh/sc-mount-volume.sh
mount usr-sap-and-shared SS1

Enter optional commands to run after performing a clone operation ⓘ

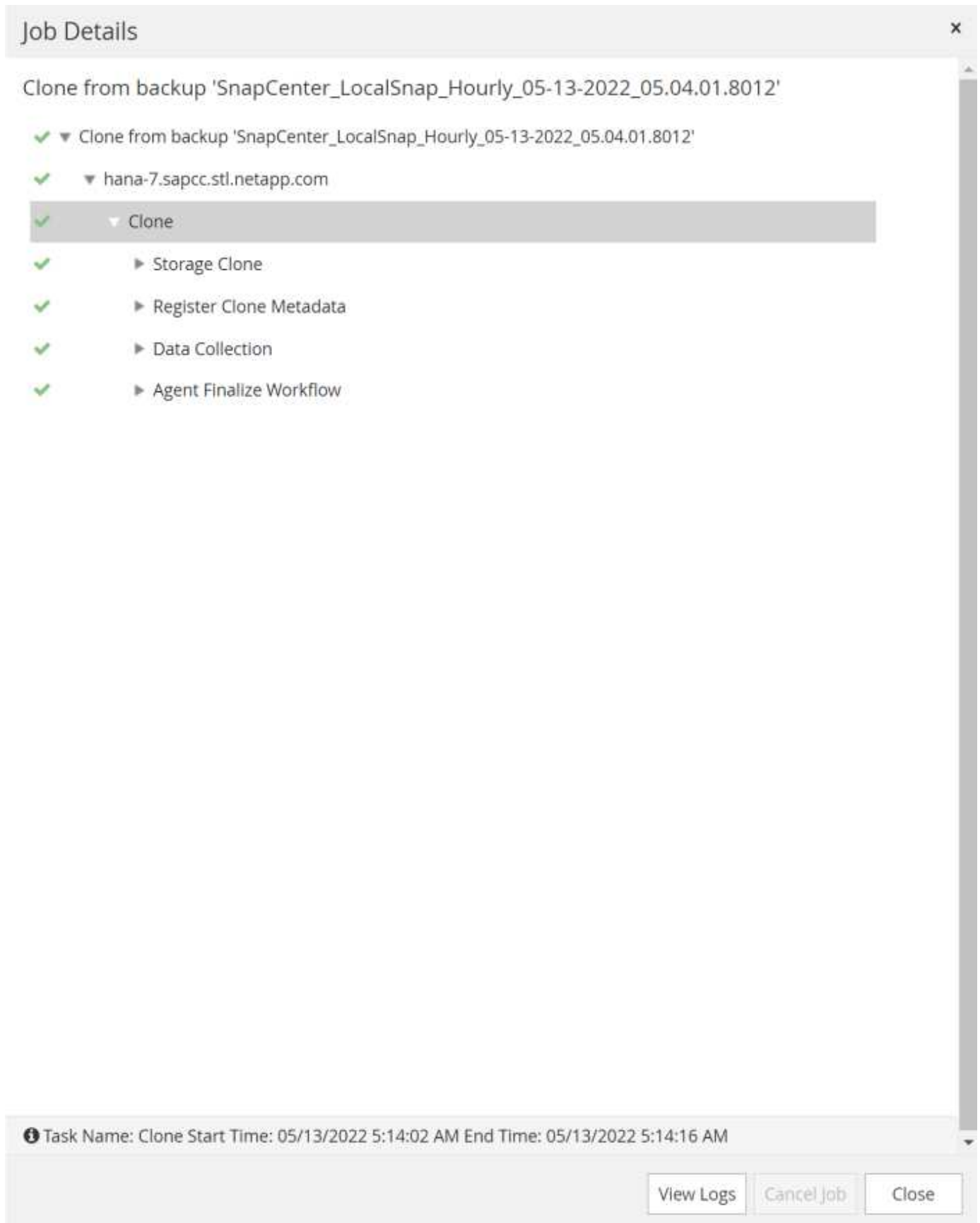
Post clone command

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

Previous

Next

1. Im Bildschirm Jobdetails in SnapCenter wird der Fortschritt des Vorgangs angezeigt.



1. Die Logdatei des Skripts `sc-mount-volume.sh` zeigt die verschiedenen Schritte, die für den Mount-Vorgang ausgeführt werden.

```

20201201041441###hana-1###sc-mount-volume.sh: Adding entry in /etc/fstab.
20201201041441###hana-1###sc-mount-volume.sh:
192.168.175.117://SS1_shared_Clone_05132205140448713/usr-sap /usr/sap/SS1
nfs
rw,vers=3,hard,timeo=600,rsz=1048576,wsz=1048576,intr,noatime,nolock 0
0
20201201041441###hana-1###sc-mount-volume.sh: Mounting volume: mount
/usr/sap/SS1.
20201201041441###hana-1###sc-mount-volume.sh:
192.168.175.117://SS1_shared_Clone_05132205140448713/shared /hana/shared
nfs
rw,vers=3,hard,timeo=600,rsz=1048576,wsz=1048576,intr,noatime,nolock 0
0
20201201041441###hana-1###sc-mount-volume.sh: Mounting volume: mount
/hana/shared.
20201201041441###hana-1###sc-mount-volume.sh: usr-sap-and-shared mounted
successfully.
20201201041441###hana-1###sc-mount-volume.sh: Change ownership to ssladm.

```

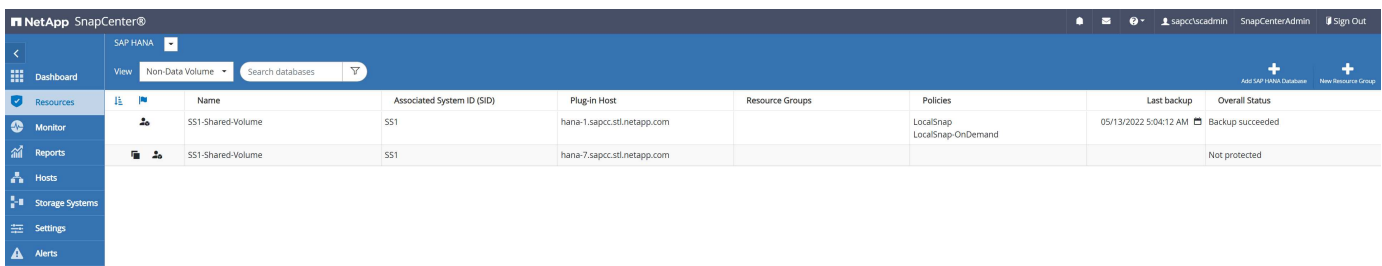
1. Nach Abschluss des SnapCenter-Workflows werden die Dateisysteme /usr/sap/SS1 und /hana/shared auf dem Ziel-Host gemountet.

```

hana-1:~ # df
Filesystem 1K-blocks Used Available Use% Mounted on
192.168.175.117://SS1_repair_log_mnt00001 262144000 320 262143680 1%
/hana/log/SS1/mnt00001
192.168.175.100:/sapcc_share 1020055552 53485568 966569984 6% /mnt/sapcc-
share
192.168.175.117://SS1_repair_log_backup 104857600 256 104857344 1%
/mnt/log-backup
192.168.175.117://SS1_shared_Clone_05132205140448713/usr-sap 262144064
10084608 252059456 4% /usr/sap/SS1
192.168.175.117://SS1_shared_Clone_05132205140448713/shared 262144064
10084608 252059456 4% /hana/shared

```

1. Innerhalb von SnapCenter ist eine neue Ressource für das geklonte Volume sichtbar.



Name	Associated System ID (SID)	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
SS1-Shared-Volume	SS1	hana-1.sapcc.stf.netapp.com		LocalSnap LocalSnap-OnDemand	05/13/2022 5:04:12 AM	Backup succeeded
SS1-Shared-Volume	SS1	hana-7.sapcc.stf.netapp.com				Not protected

1. Nachdem nun das /hana/Shared Volume verfügbar ist, können die SAP HANA-Services gestartet werden.

```
hana-1:/mnt/sapcc-share/SAP-System-Refresh # systemctl start sapinit
```

1. SAP Host Agent und sapstartsrv Prozesse werden nun gestartet.

```
hana-1:/mnt/sapcc-share/SAP-System-Refresh # ps -ef |grep sap
root 12377 1 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saphostexec
pf=/usr/sap/hostctrl/exe/host_profile
sapadm 12403 1 0 04:34 ? 00:00:00 /usr/lib/systemd/systemd --user
sapadm 12404 12403 0 04:34 ? 00:00:00 (sd-pam)
sapadm 12434 1 1 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/sapstartsrv
pf=/usr/sap/hostctrl/exe/host_profile -D
root 12485 12377 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saphostexec
pf=/usr/sap/hostctrl/exe/host_profile
root 12486 12485 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
ssladm 12504 1 0 04:34 ? 00:00:00 /usr/sap/SS1/HDB00/exe/sapstartsrv
pf=/usr/sap/SS1/SYS/profile/SS1_HDB00_hana-1 -D -u ssladm
root 12582 12486 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root 12585 7613 0 04:34 pts/0 00:00:00 grep --color=auto sap
hana-1:/mnt/sapcc-share/SAP-System-Refresh #
```

Klonen zusätzlicher SAP Applikationsservices

Weitere SAP Applikationsservices werden auf die gleiche Weise geklont wie das gemeinsam genutzte SAP HANA Volume im Abschnitt „Klonen des SAP HANA Shared Volume“ beschrieben. Natürlich müssen auch die benötigten Storage-Volumes der SAP Applikationsserver mit SnapCenter gesichert werden.

Sie müssen die erforderlichen Diensteinträge zu /usr/sap/sapservices hinzufügen, und die Ports, Benutzer und die Dateisystemeinhangepunkte (z. B. /usr/sap/SID) müssen vorbereitet werden.

Klonen des Daten-Volumes und Recovery der HANA Datenbank

1. Wählen Sie ein SAP HANA Snapshot Backup aus dem Quellsystem SS1.

The screenshot displays the NetApp SnapCenter web interface. The top navigation bar includes the NetApp logo, 'SnapCenter', and user information. The left sidebar shows a navigation menu with icons for System, Databases, Backups, Clones, and Alerts. The main content area is titled 'SS1 Topology' and shows a 'Manage Copies' section with a diagram of the backup hierarchy: 'Local copies' (15 Backups, 0 Clones) and 'Vault copies' (11 Backups, 0 Clones). A 'Summary Card' on the right provides a high-level overview: 28 Backups, 26 Snapshot based backups, 2 File based backups, and 0 Clones. Below the topology, the 'Primary Backup(s)' section contains a table with columns for Backup Name, Count, LF, and End Date. The table lists four backups, with the second one highlighted in blue.

Backup Name	Count	LF	End Date
SnapCenter_LocalSnapAndSnapVault_Daily_05-13-2022_05.00.03.0030	1		05/13/2022 5:01:01 AM
SnapCenter_LocalSnap_Hourly_05-13-2022_03.00.01.8016	1		05/13/2022 3:01:00 AM
SnapCenter_LocalSnap_Hourly_05-12-2022_23.00.01.8743	1		05/12/2022 11:01:00 PM
SnapCenter_LocalSnap_Hourly_05-12-2022_19.00.01.9803	1		05/12/2022 7:01:00 PM

1. Wählen Sie den Host aus, auf dem das Ziel-Reparatursystem vorbereitet wurde. Die NFS-Export-IP-Adresse muss die Speichernetzwerk-Schnittstelle des Ziel-Hosts sein. Als Ziel-SID halten Sie die gleiche SID wie das Quellsystem. In unserem Beispiel SS1

Clone From Backup

1 Location

2 Scripts

3 Notification

4 Summary

Select the host to create the clone

Plug-in host

hana-7.sapcc.stl.netapp.com

Target Clone SID

SS1

NFS Export IP Address

192.168.175.75

1. Geben Sie die Skripts nach dem Klonen mit den erforderlichen Befehlszeilenoptionen ein.



Das Skript für den Wiederherstellungsvorgang stellt die SAP HANA-Datenbank auf den Zeitpunkt des Snapshot-Vorgangs wieder her und führt keine Forward Recovery aus. Wenn eine Rückführung auf einen bestimmten Zeitpunkt erforderlich ist, muss die Wiederherstellung manuell durchgeführt werden. Eine manuelle vorwärts-Wiederherstellung erfordert außerdem, dass die Protokoll-Backups aus dem Quellsystem auf dem Ziel-Host verfügbar sind.

Clone From Backup

1 Location

2 Scripts

3 Notification

4 Summary

The following commands will run on the Plug-in Host: hana-7.sapcc.stl.netapp.com

Enter optional commands to run before performing a clone operation

Pre clone command

Enter optional commands to run after performing a clone operation

Post clone command

/mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh
recover

Der Bildschirm „Jobdetails“ in SnapCenter zeigt den Fortschritt des Vorgangs an.

Job Details

Clone from backup 'SnapCenter_LocalSnap_Hourly_05-13-2022_03.00.01.8016'

✓ ▼ Clone from backup 'SnapCenter_LocalSnap_Hourly_05-13-2022_03.00.01.8016'

✓ ▼ hana-7.sapcc.stl.netapp.com

✓ ▼ Clone

✓ ▶ Application Pre Clone

✓ ▶ Storage Clone

✓ ▶ Application Post Clone

✓ ▶ Register Clone Metadata

✓ ▶ Application Clean-Up

✓ ▶ Data Collection

✓ ▶ Agent Finalize Workflow

Task Name: Clone Start Time: 05/13/2022 5:24:36 AM End Time: 05/13/2022 5:25:05 AM

View Logs

Cancel Job

Close

Die Protokolldatei des `sc-system-refresh` Skripts zeigt die verschiedenen Schritte an, die für den Mount- und Wiederherstellungsvorgang ausgeführt werden.

57

```

20201201052124###hana-1###sc-system-refresh.sh: Recover system database.
20201201052124###hana-1###sc-system-refresh.sh:
/usr/sap/SS1/HDB00/exe/Python/bin/python
/usr/sap/SS1/HDB00/exe/python_support/recoverSys.py --command "RECOVER
DATA USING SNAPSHOT CLEAR LOG"
20201201052156###hana-1###sc-system-refresh.sh: Wait until SAP HANA
database is started ....
20201201052156###hana-1###sc-system-refresh.sh: Status: GRAY
20201201052206###hana-1###sc-system-refresh.sh: Status: GREEN
20201201052206###hana-1###sc-system-refresh.sh: SAP HANA database is
started.
20201201052206###hana-1###sc-system-refresh.sh: Source system has a single
tenant and tenant name is identical to source SID: SS1
20201201052206###hana-1###sc-system-refresh.sh: Target tenant will have
the same name as target SID: SS1.
20201201052206###hana-1###sc-system-refresh.sh: Recover tenant database
SS1.
20201201052206###hana-1###sc-system-refresh.sh:
/usr/sap/SS1/SYS/exe/hdb/hdbsql -U SS1KEY RECOVER DATA FOR SS1 USING
SNAPSHOT CLEAR LOG
0 rows affected (overall time 34.773885 sec; server time 34.772398 sec)
20201201052241###hana-1###sc-system-refresh.sh: Checking availability of
Indexserver for tenant SS1.
20201201052241###hana-1###sc-system-refresh.sh: Recovery of tenant
database SS1 succesfully finished.
20201201052241###hana-1###sc-system-refresh.sh: Status: GREEN
After the recovery operation, the HANA database is running and the data
volume is mounted at the target host.
hana-1:/mnt/log-backup # df
Filesystem 1K-blocks Used Available Use% Mounted on
192.168.175.117:/SS1_repair_log_mnt00001 262144000 760320 261383680 1%
/hana/log/SS1/mnt00001
192.168.175.100:/sapcc_share 1020055552 53486592 966568960 6% /mnt/sapcc-
share
192.168.175.117:/SS1_repair_log_backup 104857600 512 104857088 1%
/mnt/log-backup
192.168.175.117:/SS1_shared_Clone_05132205140448713/usr-sap 262144064
10090496 252053568 4% /usr/sap/SS1
192.168.175.117:/SS1_shared_Clone_05132205140448713/shared 262144064
10090496 252053568 4% /hana/shared
192.168.175.117:/SS1_data_mnt00001_Clone_0421220520054605 262144064
3732864 258411200 2% /hana/data/SS1/mnt00001

```

Das SAP HANA-System ist jetzt verfügbar und kann beispielsweise als Reparatursystem genutzt werden.

Wo finden Sie weitere Informationen und Versionsverlauf

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- ["SAP Business Application and SAP HANA Database Solutions \(netapp.com\)"](#)
- ["TR-4614: SAP HANA Backup and Recovery with SnapCenter"](#)
- ["TR-4436: SAP HANA on NetApp All Flash FAS Systems with Fibre Channel Protocol"](#)
- ["TR-4435: SAP HANA on NetApp All Flash FAS Systems with NFS"](#)
- ["TR-4926: SAP HANA auf Amazon FSX für NetApp ONTAP – Backup und Recovery mit SnapCenter"](#)
- ["TR-4953: NetApp SAP Landscape Management Integration Using Ansible"](#)
- ["TR-4929: SAP-Systemkopien automatisieren mit Libelle SystemCopy \(netapp.com\)"](#)
- ["Automatisierung von SAP System copy, Refresh, und Klonen von Workflows mit ALPACA und NetApp SnapCenter"](#)
- ["Automatisierung von SAP Systemkopien Verstärkern;#44; Refresh, Klonen von Workflows mit Avantra und NetApp SnapCenter"](#)

Version	Datum	Versionsverlauf Des Dokuments
Version 1.0	Februar 2018	Erste Version.
Version 2.0	Februar 2021	Vollständige Neufassung betrifft SnapCenter 4.3 und verbesserte Automatisierungsskripts. + Neue Workflow-Beschreibung für Systemaktualisierungen und Systemklonoperationen.
Version 3.0	Mai 2022	Anpassung an geänderte Arbeitsabläufe mit SnapCenter 4.6 P1
Version 4.0	Juli 2024	Dokument deckt NetApp Systeme vor Ort, FSX für ONTAP und Azure NetApp Files + Neue SnapCenter 5.0-Operationen mounten und unmounten während Clone erstellen und löschen Workflows + spezifische Schritte für Fibre Channel SAN hinzugefügt + spezifische Schritte für Azure NetApp Files hinzugefügt + angepasstes und vereinfachtes Skript + enthaltene erforderliche Schritte <code>sc-system-refresh</code> für aktiviertes SAP HANA Volume-Verschlüsselung

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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