Technischer Bericht: SAP HANA Disaster Recovery with Azure NetApp Files

NetApp solutions for SAP

NetApp
October 30, 2025

Inhalt

Technischer Bericht: SAP HANA Disaster Recovery with Azure NetApp Files

TR-4891: SAP HANA Disaster Recovery mit Azure NetApp Files

Studien haben gezeigt, dass Ausfallzeiten von Business-Applikationen erhebliche negative Auswirkungen auf das Geschäft von Unternehmen haben.

Autoren: Nils Bauer, NetApp Ralf Klahr, Microsoft

Neben den finanziellen Auswirkungen können Ausfallzeiten auch den Ruf des Unternehmens, die Arbeitsmoral des Personals und die Kundenbindung schädigen. Überraschenderweise haben nicht alle Unternehmen eine umfassende Disaster Recovery-Richtlinie.

Wenn SAP HANA auf Azure NetApp Files (ANF) läuft, erhalten Kunden Zugriff auf zusätzliche Funktionen, mit denen die integrierte Datensicherung und Disaster Recovery-Funktionen von SAP HANA erweitert und verbessert werden können. In der Übersicht werden die folgenden Optionen erläutert, mit denen Kunden Optionen auswählen können, die ihre geschäftlichen Anforderungen unterstützen.

Zur Entwicklung einer umfassenden Disaster Recovery-Richtlinie müssen Kunden die Anforderungen ihrer Business-Applikationen und die technischen Funktionen kennen, die sie für Datensicherung und Disaster Recovery benötigen. Die folgende Abbildung bietet einen Überblick über die Datensicherung.

[Die Abbildung zeigt den Input/Output-Dialog oder die Darstellung des schriftlichen Inhalts]

Anforderungen von Business-Applikationen

Für Geschäftsanwendungen gibt es zwei wichtige Indikatoren:

- Der Recovery-Zeitpunkt (Recovery Point Objective, RPO) oder der maximal tolerierbare Datenverlust
- Die Recovery-Zeitvorgabe (Recovery Time Objective, RTO) bzw. die maximal tolerierbare Ausfallzeit von Business-Applikationen

Diese Anforderungen werden durch die Art der verwendeten Applikation und die Art der Geschäftsdaten definiert. RPO und RTO können unterschiedlich sein, wenn Sie vor Ausfällen in einer einzelnen Azure Region schützen. Sie können auch voneinander abweichen, wenn Sie sich auf katastrophale Katastrophen wie den Verlust einer kompletten Azure-Region vorbereiten. Es ist wichtig, die geschäftlichen Anforderungen zu bewerten, die RPO und RTO definieren, da diese Anforderungen erhebliche Auswirkungen auf die verfügbaren technischen Optionen haben.

Hochverfügbarkeit

Die Infrastruktur für SAP HANA wie Virtual Machines, Netzwerk und Storage muss über redundante Komponenten verfügen, um sicherzustellen, dass es keinen Single Point of Failure gibt. MS Azure bietet Redundanz für die verschiedenen Infrastrukturkomponenten.

Um auf der Computing- und Applikationsseite Hochverfügbarkeit zu gewährleisten, können Standby-SAP HANA-Hosts mit einem SAP HANA System mit mehreren Hosts für integrierte Hochverfügbarkeit konfiguriert werden. Wenn ein Server oder ein SAP HANA-Service ausfällt, erfolgt ein Failover des SAP HANA-Service auf den Standby-Host, was zu einem Ausfall von Applikationen führt.

Wenn eine Applikationsausfallzeit im Falle eines Server- oder Applikationsausfalls nicht akzeptabel ist, kann auch die SAP HANA Systemreplizierung als Hochverfügbarkeitslösung eingesetzt werden, die Failover in einem sehr kurzen Zeitrahmen ermöglicht. SAP-Kunden nutzen HANA-Systemreplizierung, um Hochverfügbarkeit bei ungeplanten Ausfällen sicherzustellen, aber auch die Ausfallzeiten bei geplanten Vorgängen wie HANA-Software-Upgrades zu minimieren.

Logische Beschädigung

Logische Beschädigungen können durch Softwarefehler, menschliche Fehler oder Sabotage verursacht werden. Leider können logische Beschädigungen oft nicht mit standardmäßigen Hochverfügbarkeits- und Disaster Recovery-Lösungen behoben werden. Daher können in manchen Fällen RTO- und RPO-Anforderungen in Abhängigkeit von der Ebene, der Applikation, dem File-System oder dem Storage mit der logischen Beschädigung nicht erfüllt werden.

Schlimmstenfalls ist die SAP-Applikation beschädigt oder logisch. SAP Applikationen laufen oft in einer Landschaft, in der verschiedene Applikationen miteinander kommunizieren und Daten austauschen. Daher wird die Wiederherstellung eines SAP-Systems, bei dem eine logische Beschädigung aufgetreten ist, nicht empfohlen. Das Wiederherstellen des Systems zu einem Zeitpunkt vor der Beschädigung führt zu Datenverlusten, sodass die RPO größer als null ist. Außerdem würde die SAP-Landschaft nicht mehr synchron sein und eine zusätzliche Nachbearbeitung erfordern.

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

Die zum Einrichten eines Reparatursystems erforderlichen Schritte sind mit einem in diesem Dokument beschriebenen Disaster-Recovery-Testszenario identisch. Somit kann die beschriebene Disaster Recovery-Lösung problemlos auf logische Beschädigungen erweitert werden.

Backups

Backups werden erstellt, um Restores und Recovery von unterschiedlichen zeitpunktgenauen Datensätzen zu ermöglichen. In der Regel werden diese Backups einige Tage bis einige Wochen aufbewahrt.

Je nach Art der Beschädigung können Restores und Recovery mit oder ohne Datenverlust durchgeführt werden. Wenn das RPO null beträgt, selbst bei einem Verlust des Primär- und Backup-Storage, muss das Backup mit der synchronen Datenreplizierung kombiniert werden.

Die RTO für Restore und Recovery wird durch die erforderliche Wiederherstellungszeit, die Recovery-Zeit (einschließlich Datenbankstart) und das Laden der Daten in den Arbeitsspeicher definiert. Bei großen Datenbanken und herkömmlichen Backup-Ansätzen kann die RTO problemlos mehrere Stunden betragen, was unter Umständen nicht akzeptabel ist. Um eine sehr geringe RTO-Werte zu erzielen, muss ein Backup mit einer Hot-Standby-Lösung kombiniert werden, die das Vorladen von Daten in den Speicher beinhaltet.

Eine Backup-Lösung muss dagegen die logische Beschädigung beheben, da Datenreplizierungslösungen nicht alle Arten von logischen Beschädigungen abdecken können.

Synchrone oder asynchrone Datenreplizierung

Der RPO bestimmt hauptsächlich, welche Datenreplizierungsmethode Sie verwenden sollten. Bei einem RPO von null muss auch bei einem Ausfall des primären und des Backup-Storage die Daten synchron repliziert werden. Allerdings gibt es technische Einschränkungen bei der synchronen Replizierung, beispielsweise die Entfernung zwischen zwei Azure Regionen. In den meisten Fällen ist synchrone Replizierung aufgrund von Latenz bei Entfernungen von mehr als 100 km nicht geeignet. Daher ist diese Lösung keine Option für die Datenreplizierung zwischen Azure Regionen.

Wenn ein größerer RPO-Wert akzeptabel ist, kann die asynchrone Replizierung über große Entfernungen hinweg verwendet werden. Der RPO in diesem Fall wird durch die Replizierungsfrequenz definiert.

HANA System-Replizierung mit oder ohne vorab geladen

Die Startzeit einer SAP HANA-Datenbank ist wesentlich länger als die von herkömmlichen Datenbanken, da eine große Datenmenge in den Arbeitsspeicher geladen werden muss, bevor die Datenbank die erwartete Performance liefern kann. Daher ist ein großer Teil der RTO die Zeit, die zum Starten der Datenbank benötigt wird. Mit jeder Storage-basierten Replizierung sowie mit HANA System Replication ohne vorab geladen werden, muss die SAP HANA-Datenbank für den Failover zum Disaster-Recovery-Standort gestartet werden.

Die SAP HANA Systemreplizierung bietet einen Betriebsmodus, in dem die Daten vorgeladen und kontinuierlich am sekundären Host aktualisiert werden. Dieser Modus ermöglicht sehr niedrige RTO-Werte, benötigt aber auch einen dedizierten Server, der nur für den Empfang der Replizierungsdaten vom Quellsystem verwendet wird.

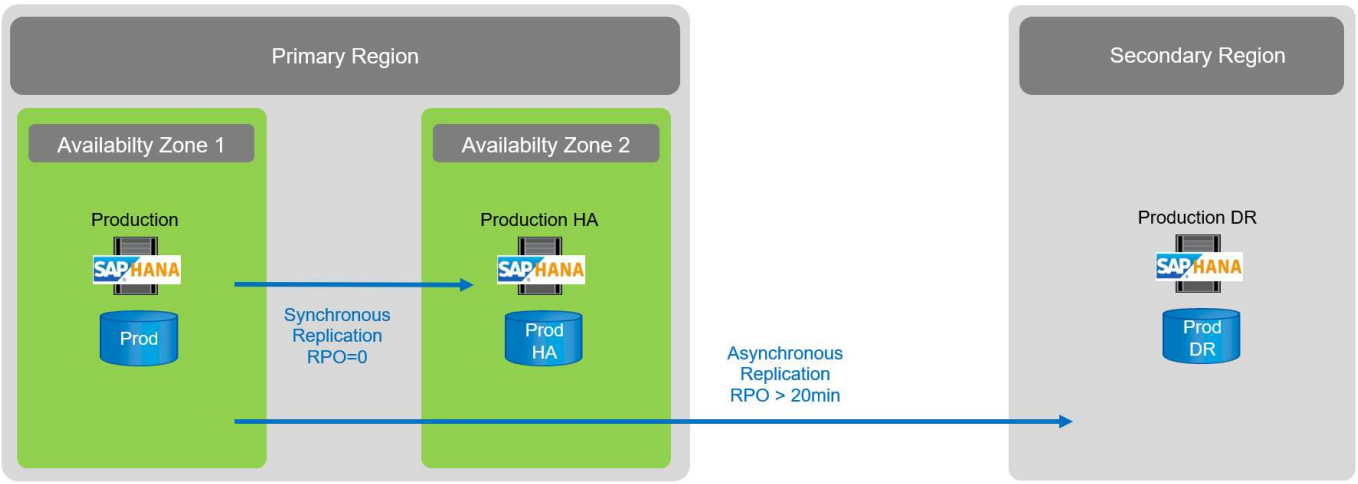
Disaster-Recovery-Lösungsvergleich

Eine umfassende Disaster Recovery-Lösung muss Kunden nach einem vollständigen Ausfall des primären Standorts die Wiederherstellung ermöglichen. Daher müssen die Daten an einen sekundären Standort übertragen werden und eine komplette Infrastruktur ist erforderlich, um bei einem Standortausfall die erforderlichen SAP HANA Produktionssysteme auszuführen. Abhängig von den Verfügbarkeitsanforderungen der Applikation und der Art des zu schützenden Disaster ist eine Disaster Recovery-Lösung mit zwei oder drei Standorten zu berücksichtigen.

Die folgende Abbildung zeigt eine typische Konfiguration, bei der die Daten innerhalb derselben Azure-Region synchron in eine zweite Verfügbarkeitszone repliziert werden. Durch die kurze Entfernung können Sie die Daten synchron replizieren und ein RPO von null (normalerweise HA-Bereitstellung) erreichen.

Darüber hinaus werden Daten asynchron in eine sekundäre Region repliziert, um sie vor Ausfällen zu schützen, wenn die primäre Region betroffen ist. Der erzielbare MindestRPO hängt von der Datenreplizierungsfrequenz ab, die durch die verfügbare Bandbreite zwischen dem primären und dem sekundären Bereich begrenzt ist. Ein typischer minimaler RPO liegt im Bereich von 20 Minuten bis mehreren Stunden.

Dieses Dokument erläutert verschiedene Implementierungsoptionen für eine Disaster Recovery-Lösung für zwei Regionen.



SAP HANA System Replication

SAP HANA System Replication arbeitet auf Datenbankebene. Die Lösung basiert auf einem zusätzlichen SAP HANA-System am Disaster-Recovery-Standort, das die Änderungen vom Primärsystem empfängt. Dieses sekundäre System muss mit dem Primärsystem identisch sein.

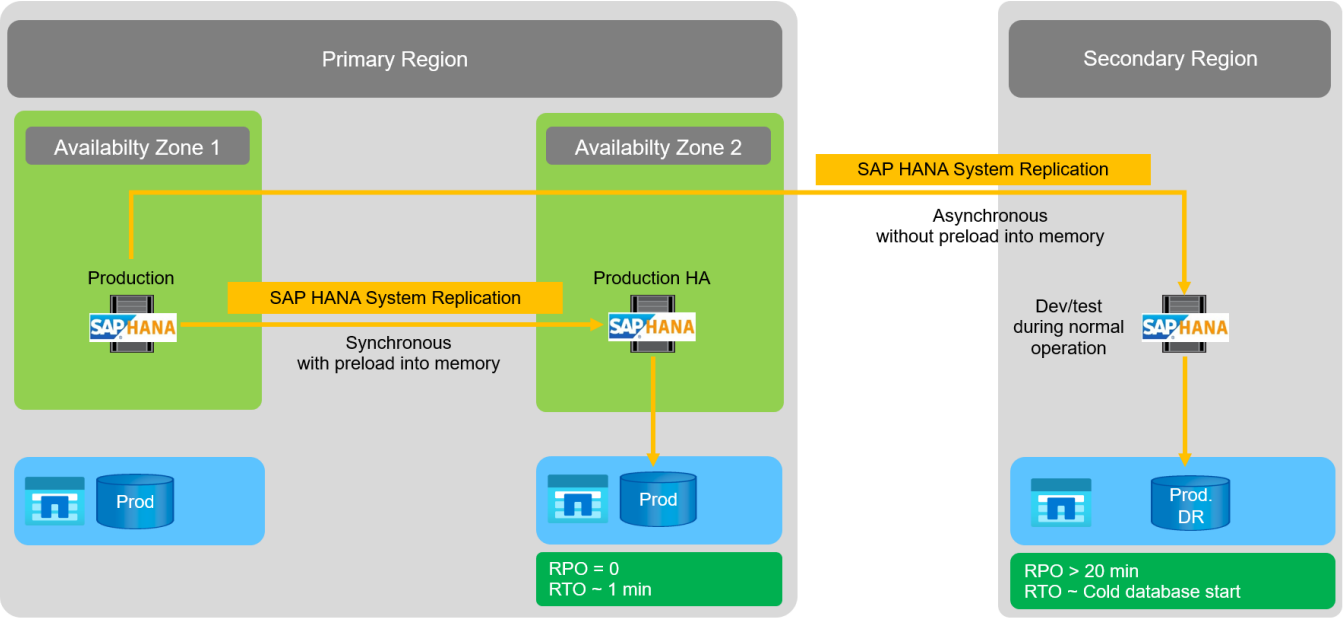
SAP HANA System Replication kann in einem von zwei Modi betrieben werden:

- Mit vorab in den Arbeitsspeicher geladenen Daten und einem dedizierten Server am Disaster-Recovery-Standort:
  - Der Server wird ausschließlich als sekundärer SAP HANA System Replication Host verwendet.
  - Sehr geringe RTO-Werte können erzielt werden, weil die Daten bereits in den Speicher geladen sind und bei einem Failover kein Datenbankstart erforderlich ist.
- Ohne Daten, die vorab in den Arbeitsspeicher geladen sind und einen gemeinsam genutzten Server am Disaster Recovery-Standort nutzen:
  - Der Server wird als sekundäres SAP HANA System Replication und als Entwicklungs-/Testsystem gemeinsam genutzt.
  - RTO hängt hauptsächlich von der Zeit ab, die zum Starten der Datenbank und Laden der Daten in den Arbeitsspeicher benötigt wird.

Eine vollständige Beschreibung aller Konfigurationsoptionen und Replikationsszenarien finden Sie im "SAP HANA Administration Guide".

Die folgende Abbildung zeigt das Setup einer Disaster-Recovery-Lösung für zwei Regionen mit SAP HANA System Replication. Die synchrone Replizierung mit vorab in den Speicher geladenen Daten wird für lokale HA in derselben Azure-Region verwendet, allerdings in verschiedenen Verfügbarkeitszonen. Die asynchrone Replizierung ohne vorab geladene Daten wird für die Remote Disaster-Recovery-Region konfiguriert.

Die folgende Abbildung zeigt die SAP HANA System Replication.



SAP HANA System Replication mit vorab in den Speicher geladenen Daten

Sehr geringe RTO-Werte mit SAP HANA können nur mit SAP HANA System Replication erreicht werden, wobei Daten vorab in den Speicher geladen sind. Der Betrieb von SAP HANA System Replication mit einem dedizierten sekundären Server am Disaster-Recovery-Standort ermöglicht einen RTO-Wert von maximal einer Minute. Die replizierten Daten werden empfangen und im sekundären System vorgeladen. Aus diesem Grund wird SAP HANA System Replication häufig auch für Wartungsvorgänge ohne Ausfallzeiten eingesetzt, beispielsweise für HANA-Software-Upgrades.

In der Regel ist SAP HANA System Replication so konfiguriert, dass sie synchron repliziert wird, wenn eine vorab-Datenlast ausgewählt wird. Die maximal unterstützte Entfernung bei synchroner Replizierung liegt im Bereich von 100 km.

SAP System Replication ohne vorab in den Speicher geladene Daten

Für weniger strenge RTO-Anforderungen kann SAP HANA System Replication ohne vorab geladene Daten verwendet werden. In diesem Betriebsmodus werden die Daten der Disaster-Recovery-Region nicht in den Arbeitsspeicher geladen. Der Server in der DR-Region wird weiterhin zur Verarbeitung von SAP HANA System Replication verwendet, auf dem alle erforderlichen SAP HANA-Prozesse ausgeführt werden. Der Großteil des Serverspeichers ist jedoch für andere Dienste verfügbar, wie zum Beispiel SAP HANA Entwicklungs-/Testsysteme.

Bei einem Notfall muss das Entwicklungs-/Testsystem heruntergefahren, der Failover initiiert und die Daten in den Arbeitsspeicher geladen werden. Das RTO dieses Cold-Standby-Ansatzes hängt von der Größe der Datenbank und dem Lesedurchsatz während der Last des Zeilen- und Spaltenspeichers ab. Mit der Annahme, dass die Daten mit einem Durchsatz von 1000 MBit/s gelesen werden, dass das Laden von 1 TB Daten ungefähr 18 Minuten dauert.

Technischer Bericht: SAP HANA Disaster Recovery with ANF Cross-Region Replication

ANF Cross-Region Replication ist in ANF als Disaster-Recovery-Lösung mit asynchroner Datenreplizierung integriert. ANF regionsübergreifende Replizierung wird über eine Datensicherungsbeziehung zwischen zwei ANF-Volumes in einer primären und einer sekundären Azure-Region konfiguriert. ANF-Cross-Region Replication aktualisiert das sekundäre Volume mithilfe effizienter Block-Delta-Replikationen. Update-Zeitpläne

können während der Replikationskonfiguration definiert werden.

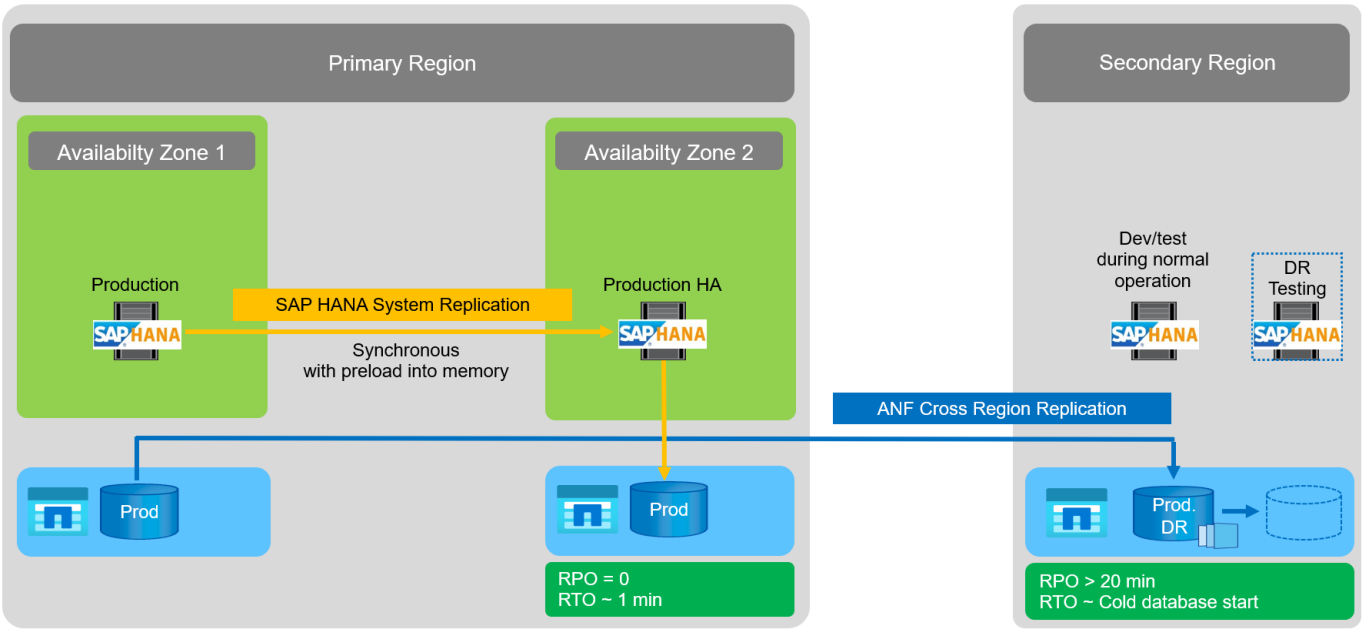
Die folgende Abbildung zeigt ein Beispiel für eine Disaster-Recovery-Lösung für zwei Regionen mithilfe von ANF-bereichsübergreifender Replizierung. In diesem Beispiel ist das HANA-System mit HANA System Replication innerhalb der primären Region geschützt, wie im vorherigen Kapitel erläutert. Die Replikation in eine sekundäre Region wird mittels ANF-bereichsübergreifender Replikation durchgeführt. Der RPO-Wert wird durch den Replizierungszeitplan und die Replizierungsoptionen definiert.

Das RTO hängt hauptsächlich von der Zeit ab, die zum Starten der HANA-Datenbank am Disaster-Recovery-Standort und zum Laden der Daten in den Arbeitsspeicher benötigt wird. Mit der Annahme, dass die Daten mit einem Durchsatz von 1000 MB/s gelesen werden, dass das Laden von 1 TB Daten ungefähr 18 Minuten dauert. Je nach Replizierungskonfiguration ist auch Recovery-Prozesse erforderlich und wird der RTO-Gesamtwert steigern.

Weitere Details zu den verschiedenen Konfigurationsoptionen finden Sie in Kapitel "Konfigurationsoptionen für regionsübergreifende Replizierung mit SAP HANA".

Die Server an den Disaster-Recovery-Standorten können als Entwicklungs-/Testsysteme im normalen Betrieb eingesetzt werden. Bei einem Notfall müssen die Entwicklungs-/Testsysteme heruntergefahren und als DR-Produktionsserver gestartet werden.

Mit der standortübergreifenden ANF Replizierung können Sie den DR-Workflow testen, ohne dass RPO und RTO beeinträchtigt werden. Dazu werden Volume-Klone erstellt und an den DR-Testserver angeschlossen.



Zusammenfassung der Disaster Recovery-Lösungen

In der folgenden Tabelle werden die in diesem Abschnitt beschriebenen Disaster-Recovery-Lösungen verglichen und die wichtigsten Kennzahlen hervorgehoben.

Die wichtigsten Ergebnisse:

- Ist ein sehr niedriges RTO erforderlich, ist SAP HANA System Replication mit vorab-Load in den Speicher die einzige Option.
  - Am DR-Standort ist ein dedizierter Server erforderlich, um die replizierten Daten zu erhalten und die Daten in den Arbeitsspeicher zu laden.

- Darüber hinaus ist eine Storage-Replizierung für die Daten erforderlich, die sich außerhalb der Datenbank befinden (z. B. gemeinsam genutzte Dateien, Schnittstellen usw.).
- Bei einer geringeren RTO/RPO-Anforderung kann auch eine regionale ANF-Replizierung verwendet werden, um:
  - Kombinieren Sie Datenreplizierung außerhalb von Datenbanken.
  - Behandeln Sie zusätzliche Anwendungsfälle wie Disaster-Recovery-Tests und Aktualisierungen von Entwicklung/Tests.
  - Bei der Storage-Replizierung kann der Server am DR-Standort im normalen Betrieb als QA- oder Testsystem verwendet werden.
- Eine Kombination aus SAP HANA System Replication als HA-Lösung mit RPO=0 mit Storage-Replizierung für große Entfernungen ist sinnvoll, um die unterschiedlichen Anforderungen zu erfüllen.

In der folgenden Tabelle werden die Disaster-Recovery-Lösungen verglichen.

	Storage-Replizierung	**SAP HANA Systemreplizierung**	
	Regionenübergreifende Replikation	* Mit Datenvorladung*	**Ohne Datenvorladung**
RTO	Gering bis mittel; abhängig von der Startzeit der Datenbank und der Vorwärtswiederherstellung	Sehr niedrig	Gering bis mittel; abhängig von der Datenbank-Startzeit
RPO	RPO > 20 Min. Asynchrone Replizierung	RPO > 20 Min. Asynchrone Replikation RPO = 0 synchrone Replizierung	RPO > 20 Min. Asynchrone Replikation RPO = 0 synchrone Replizierung
Server am DR-Standort können für Entwicklung/Test genutzt werden	Ja.	Nein	Ja.
Replizierung von nicht aus Datenbanken stammenden Daten	Ja.	Nein	Nein
DR-Daten können zur Aktualisierung von Entwicklungs-/Testsystemen genutzt werden	Ja.	Nein	Nein
DR-Tests ohne Auswirkungen auf RTO und RPO	Ja.	Nein	Nein

ANF: Regionale Replizierung mit SAP HANA

ANF: Regionale Replizierung mit SAP HANA

Anwendungsunabhängige Informationen zur regionsübergreifenden Replikation finden

Sie an folgendem Speicherort.

"Azure NetApp Files Dokumentation – Microsoft Docs" In den Abschnitten Konzepte und Anleitungen.

Konfigurationsoptionen für Regionalreplizierung mit SAP HANA

Die folgende Abbildung zeigt die Volume-Replizierungsbeziehungen für ein SAP HANA-System mit ANF-bereichsübergreifender Replizierung. Bei ANF-Cross-Region Replication müssen die HANA-Daten und das gemeinsame HANA-Volume repliziert werden. Wenn nur das HANA-Daten-Volume repliziert wird, liegen die typischen RPO-Werte im Bereich von einem Tag. Wenn niedrigere RPO-Werte erforderlich sind, müssen die HANA-Protokoll-Backups auch für die zukünftige Recovery repliziert werden.

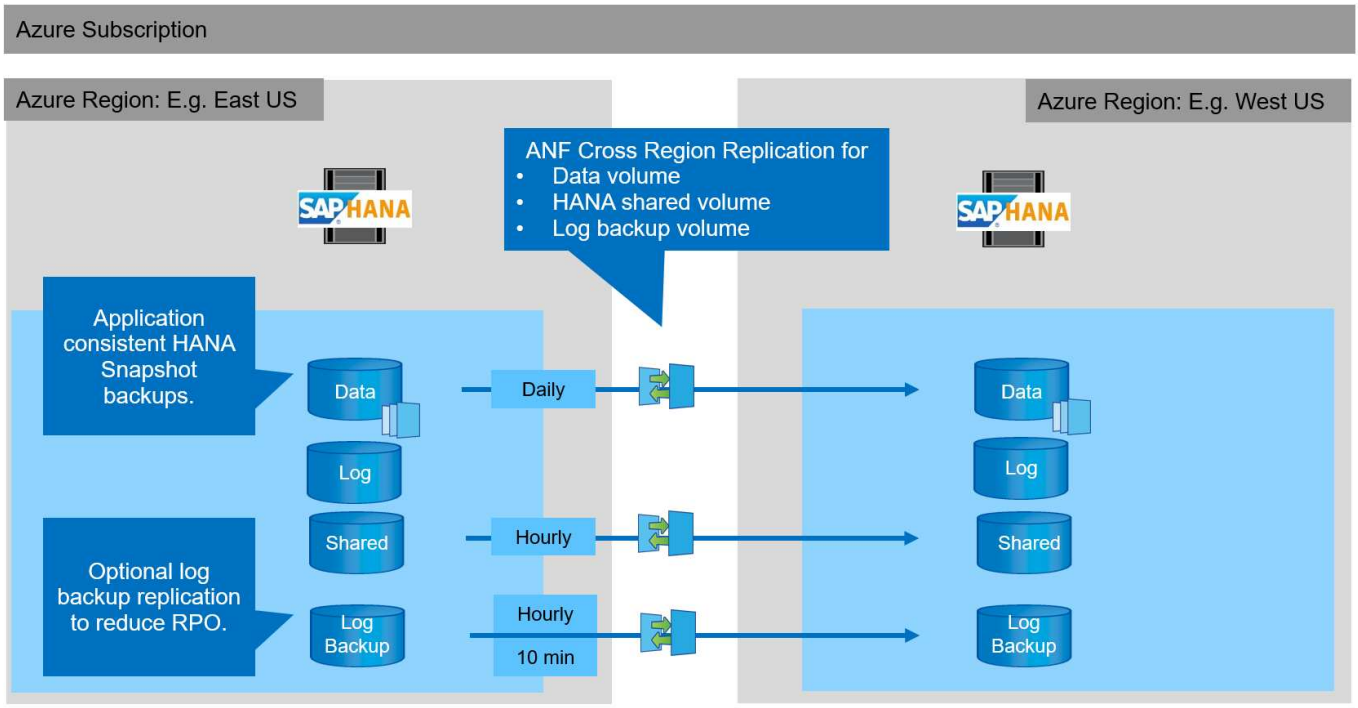
Der in diesem Dokument verwendete Begriff „Protokollsicherung“ umfasst die Protokollsicherung und die Sicherung des HANA-Backup-Katalogs. Der HANA-Backup-Katalog ist erforderlich, um Recovery-Vorgänge durchzuführen.

Die folgende Beschreibung und der Schwerpunkt der Laboreinrichtung sind auf die HANA-Datenbank. Andere gemeinsam genutzte Dateien, zum Beispiel das SAP-Transportverzeichnis, würden auf die gleiche Weise gesichert und repliziert werden wie das freigegebene HANA-Volume.

Für die HANA-Speicherpunktwiederherstellung oder Forward-Recovery mit den Backup-Protokollen müssen am primären Standort für das HANA-Daten-Volume applikationskonsistente Snapshot Backups erstellt werden. Dies kann zum Beispiel mit dem ANF-Backup-Tool AzAcSnap (siehe auch "Was ist Azure Application konsistente Snapshot Tool für Azure NetApp Files Microsoft Docs"). Die am primären Standort erstellten Snapshot Backups werden anschließend am DR-Standort repliziert.

Bei einem Disaster Failover muss die Replizierungsbeziehung beschädigt werden, die Volumes müssen auf dem DR-Produktionsserver eingebunden werden, und die HANA-Datenbank muss wiederhergestellt werden, entweder zum letzten HANA-Speicherpunkt oder bei einer Forward-Recovery mit den replizierten Log-Backups. Das Kapitel "Disaster-Recovery-Failover", beschreibt die erforderlichen Schritte.

In der folgenden Abbildung sind die HANA-Konfigurationsoptionen für die regionsübergreifende Replizierung dargestellt.



Mit der aktuellen Version der Cross-Region-Replikation können nur feste Zeitpläne ausgewählt werden, und die tatsächliche Replikationsaktualisierungszeit kann nicht vom Benutzer definiert werden. Verfügbare Termine sind täglich, stündlich und alle 10 Minuten. Bei Verwendung dieser Zeitplanoptionen sind zwei verschiedene Konfigurationen je nach RPO-Anforderungen sinnvoll: Daten-Volume-Replizierung ohne Backup-Replizierung bei Protokolldaten sowie Backup-Replizierung mit verschiedenen Zeitplänen entweder stündlich oder alle 10 Minuten. Die niedrigste mögliche RPO beträgt etwa 20 Minuten. In der folgenden Tabelle sind die Konfigurationsoptionen sowie die resultierenden RPO- und RTO-Werte zusammengefasst.

	Replizierung von Daten-Volumes	**Replizierung von Daten und Backup Volumes protokollieren**	**Replizierung von Daten und Backup Volumes protokollieren**
CRR-Volumen planen	Täglich	Täglich	Täglich
CRR-Protokoll Backup-Volumen planen	k. A.	Stündlich	10 Min
Max. RPO	24 Stunden + Snapshot Zeitplan (z. B. 6 Stunden)	1 Stunde	2 x 10 Min
Max RTO	In erster Linie durch die HANA-Startzeit definiert	+ HANA Startzeit + Wiederherstellungszeit+	+ HANA Startzeit + Wiederherstellungszeit+
Wiederherstellung vorwärts	NA	Logs der letzten 24 Stunden + Snapshot Zeitplan (z.B. 6 Stunden)	Logs der letzten 24 Stunden + Snapshot Zeitplan (z.B. 6 Stunden)

Anforderungen und Best Practices

Microsoft Azure übernimmt keine Garantie für die Verfügbarkeit eines bestimmten VM-Typs (Virtual Machine) bei der Erstellung oder beim Starten einer nicht zugewiesenen VM. Insbesondere im Falle eines regionalen Ausfalls benötigen viele Clients möglicherweise zusätzliche VMs in der Disaster Recovery-Region. Daher wird

empfohlen, eine VM mit der erforderlichen Größe für Disaster Failover aktiv als Test- oder QA-System in der Disaster Recovery-Region zu verwenden, um den erforderlichen VM-Typ zugewiesen zu haben.

Es empfiehlt sich, einen ANF-Kapazitätspool mit einer niedrigeren Performance Tier im normalen Betrieb zu verwenden, um eine Kostenoptimierung zu ermöglichen. Die Datenreplizierung erfordert keine hohe Performance und kann daher einen Kapazitäts-Pool mit einer Standard-Performance-Tier verwenden. Bei Disaster-Recovery-Tests oder bei einem Ausfall muss die Volume in einen Kapazitäts-Pool mit einer hochperformanten Tier verschoben werden.

Wenn ein zweiter Kapazitäts-Pool keine Option ist, sollten die Ziel-Volumes für die Replizierung auf Basis der Kapazitätsanforderungen konfiguriert werden und nicht auf die Performance-Anforderungen während des normalen Betriebs. Das Kontingent oder der Durchsatz (für manuelle QoS) kann dann für Disaster-Recovery-Tests angepasst werden, falls ein Notfall besteht.

Weitere Informationen finden Sie unter "Anforderungen und Überlegungen für die Verwendung von Azure NetApp Files-Volume-regionsübergreifende Replikation mit Microsoft Docs".

Laboreinrichtung

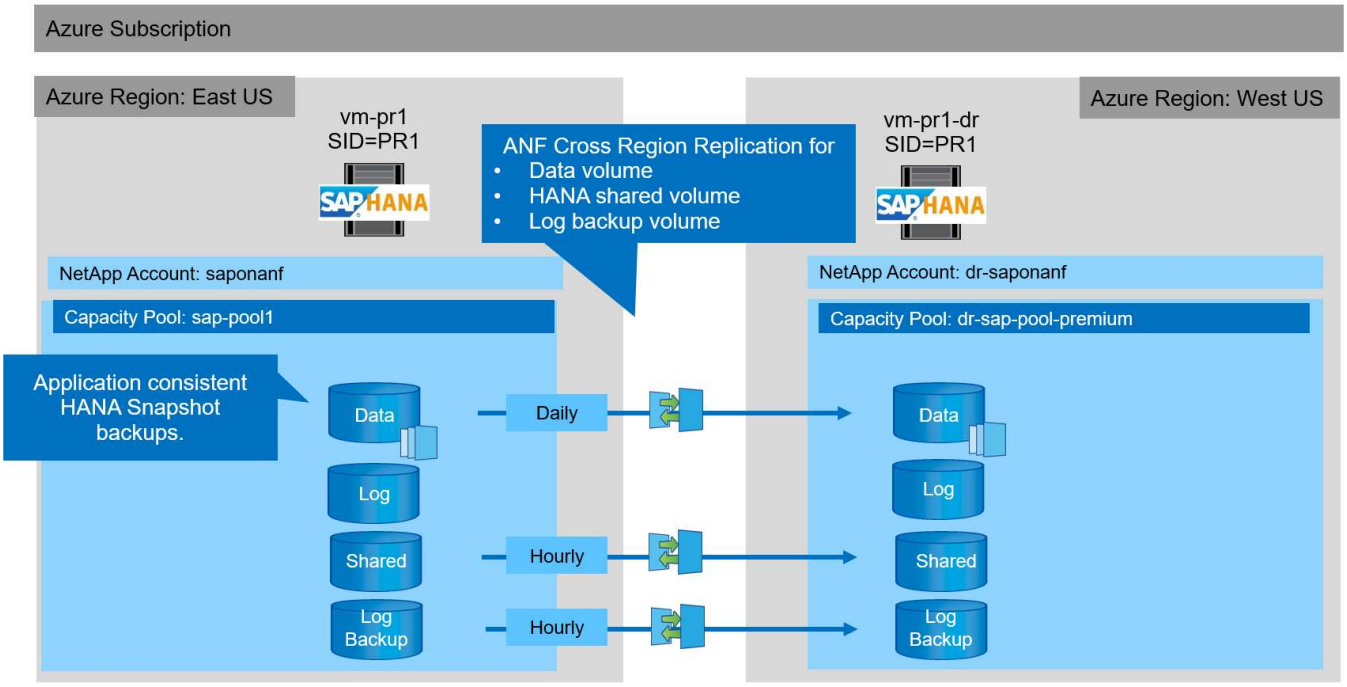
Die Lösungsvalidierung wurde mit einem Single-Host-System für SAP HANA durchgeführt. Das Microsoft AzAcSnap Snapshot Backup-Tool für ANF wurde verwendet, um applikationskonsistente HANA Snapshot Backups zu konfigurieren. Es wurden ein tägliches Datenvolumen, ein stündliches Log Backup und die gemeinsame Volume-Replizierung konfiguriert. Disaster Recovery-Tests und Failover wurden mit einem Speicherpunkt sowie bei vorwärts gerichteten Recovery-Vorgängen validiert.

Die folgenden Softwareversionen wurden für die Laboreinrichtung verwendet:

- Ein einziges Host-System SAP HANA 2.0 SPS5 mit einem einzelnen Mandanten
- SUSE SLES FÜR SAP 15 SP1
- AzAcSnap 5.0

Am DR-Standort wurde ein einzelner Kapazitäts-Pool mit manueller QoS konfiguriert.

Die folgende Abbildung zeigt die Laboreinrichtung.

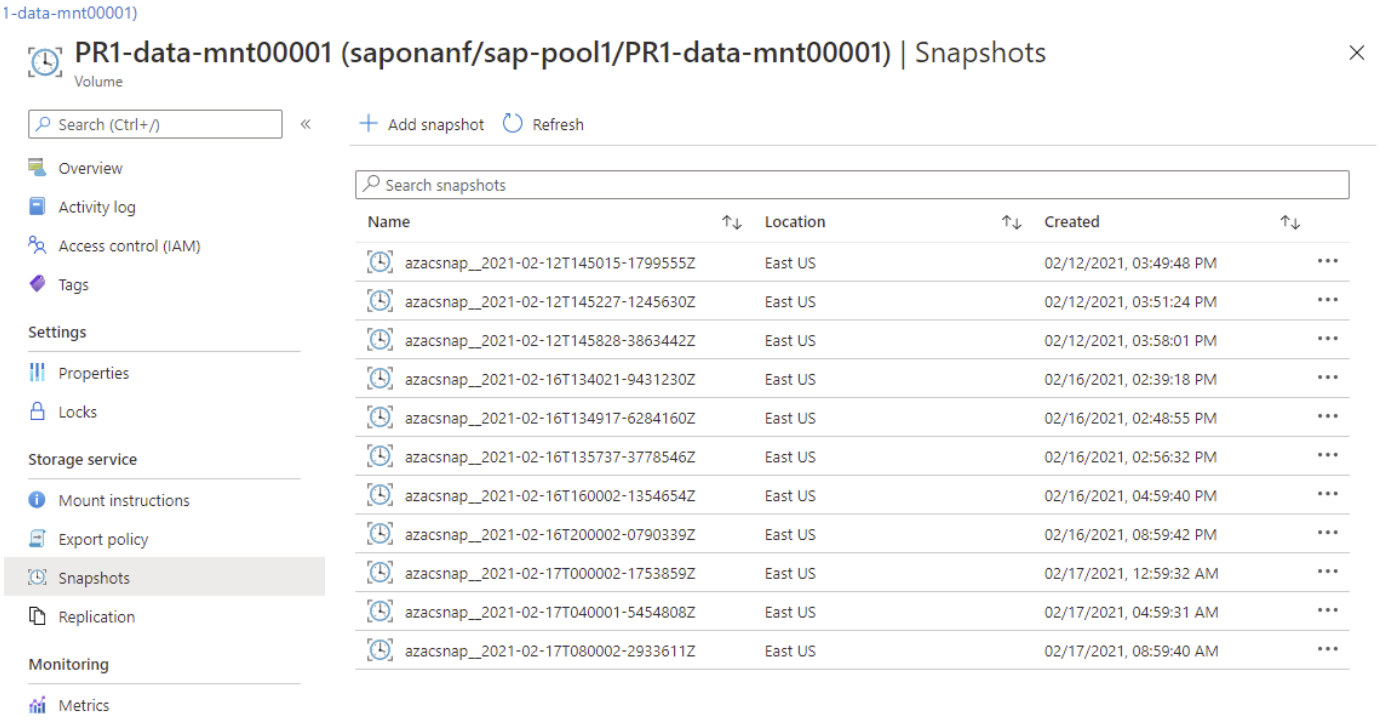


Snapshot Backup-Konfiguration mit AzAcSnap

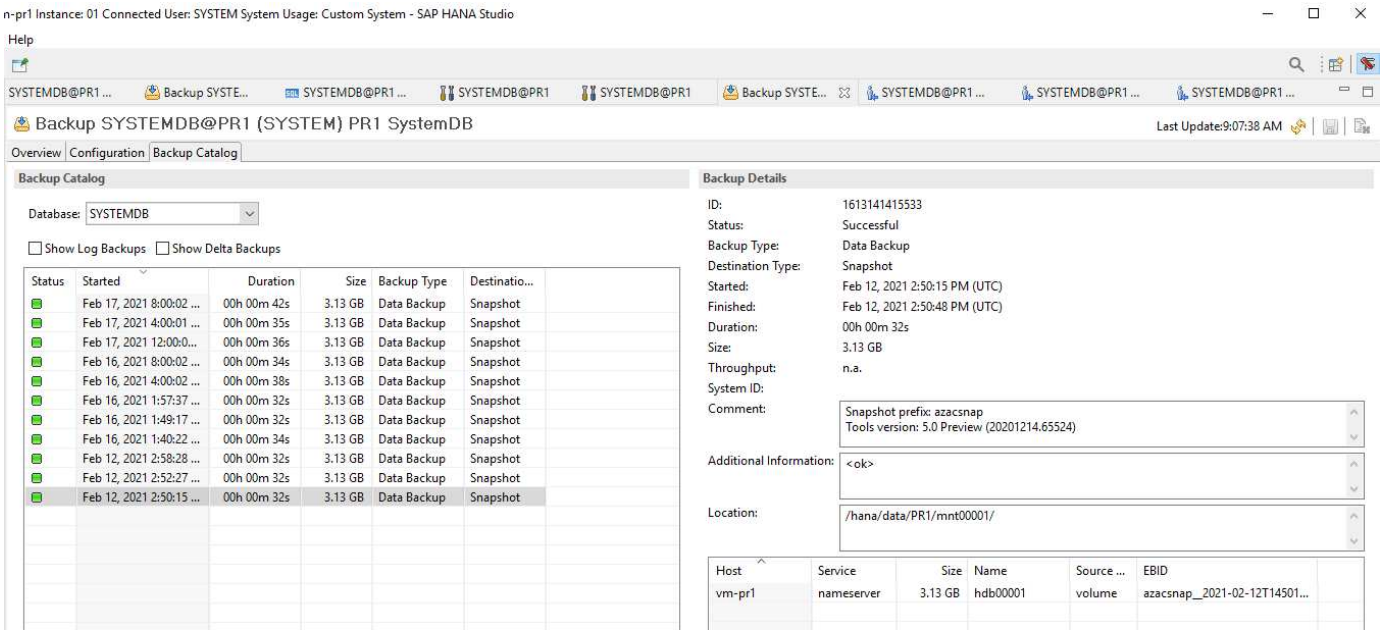
Am primären Standort wurde AzAcSnap für die Erstellung applikationskonsistenter Snapshot-Backups des HANA-Systems PR1 konfiguriert. Diese Snapshot-Backups sind im ANF-Datenvolumen des PR1 HANA Systems verfügbar und sind auch im SAP HANA Backup-Katalog registriert, wie in den beiden folgenden Abbildungen dargestellt. Snapshot Backups wurden alle 4 Stunden geplant.

Bei der Replizierung des Daten-Volumes mithilfe von ANF Cross-Region Replication werden diese Snapshot-Backups am Disaster Recovery-Standort repliziert und können zur Wiederherstellung der HANA-Datenbank verwendet werden.

Die folgende Abbildung zeigt die Snapshot Backups des HANA Daten-Volumes.



Die folgende Abbildung zeigt den SAP HANA-Backup-Katalog.



Konfigurationsschritte für ANF-bereichsübergreifende Replikation

Am Disaster Recovery-Standort sind einige Vorbereitungsschritte durchzuführen, bevor die Volume-Replizierung konfiguriert werden kann.

- Ein NetApp Konto muss verfügbar und mit demselben Azure Abonnement wie die Quelle konfiguriert sein.
- Ein Kapazitäts-Pool muss über das oben genannte NetApp Konto verfügbar und konfiguriert sein.
- Ein virtuelles Netzwerk muss verfügbar und konfiguriert sein.
- Innerhalb des virtuellen Netzwerks muss ein delegiertes Subnetz zur Verwendung mit ANF verfügbar und

konfiguriert sein.

Protection Volumes können nun für HANA-Daten, HANA Shared IT und das HANA-Log-Backup-Volume erstellt werden. Die folgende Tabelle zeigt die konfigurierten Ziel-Volumes in unserer Laboreinrichtung.

> Um eine optimale Latenz zu erzielen, müssen die Volumes in der Nähe der VMs platziert werden, die im Falle eines Disaster-Failover den SAP HANA ausführen. Daher ist für die DR-Volumes derselbe Pinning-Prozess wie für jedes andere SAP HANA-Produktionssystem erforderlich.

HANA Volume	Quelle	Ziel	Replizierungsplan
HANA-Datenvolumen	PR1-Data-mnt00001	PR1-Data-mnt00001-SM-dest	Täglich
HANA Shared Volume	PR1 freigegeben	PR1-shared-SM-dest	Stündlich
HANA-Protokoll-/Katalogbackup-Volume	Hanabackup	Hanabackup-SM-dest	Stündlich

Für jedes Volume müssen folgende Schritte durchgeführt werden:

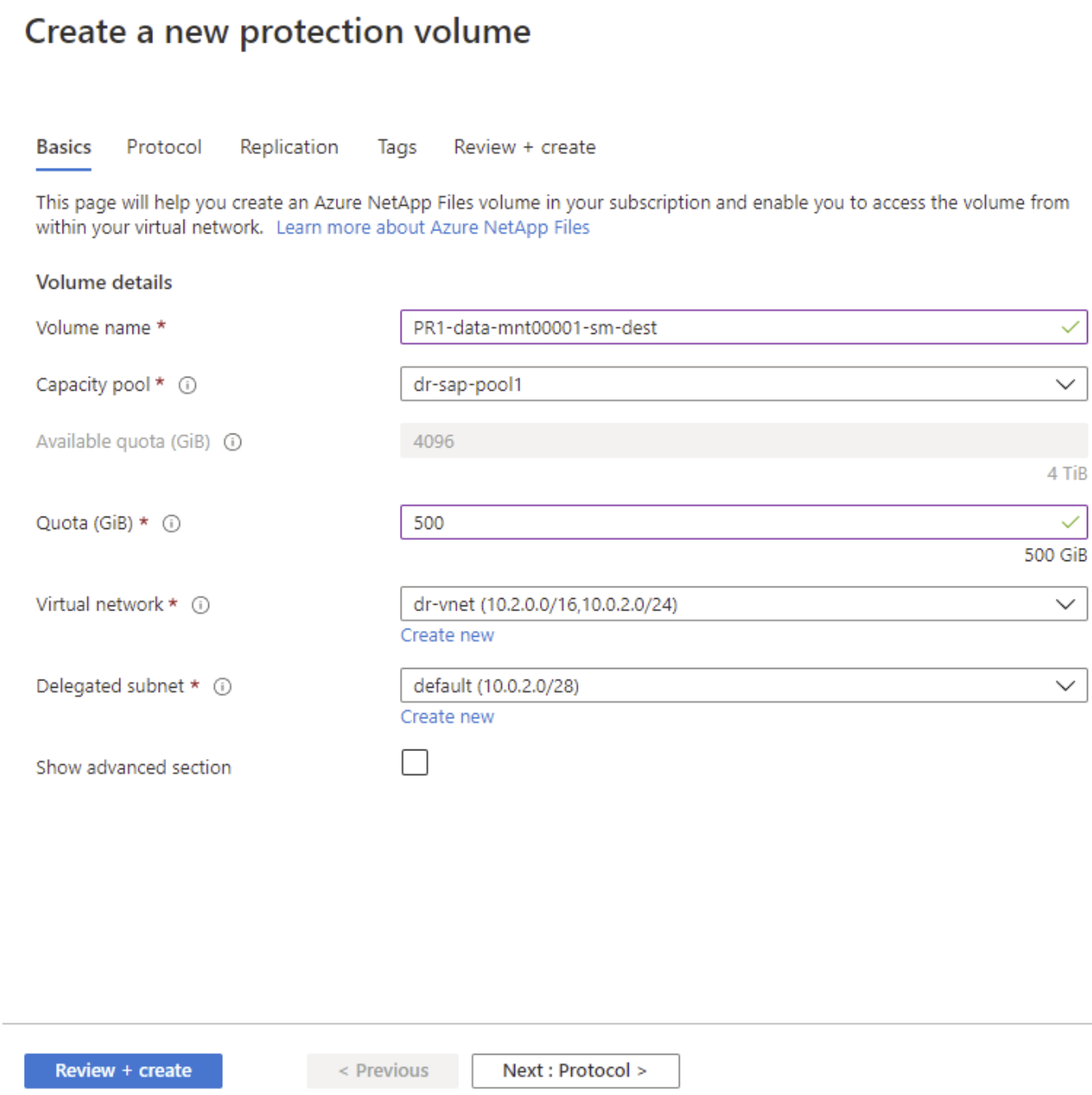
1. Erstellen eines neuen Sicherungs-Volumes am DR-Standort:
   a. Stellen Sie Volume-Namen, den Kapazitäts-Pool, die Quota- und Netzwerkinformationen bereit.
   b. Bereitstellen der Zugriffsinformationen für Protokolle und Volumes
   c. Geben Sie die Quell-Volume-ID und einen Replizierungsplan an.
   d. Erstellen eines Ziel-Volumes
2. Autorisieren Sie die Replikation auf dem Quell-Volume.
   - Geben Sie die ID des Zielvolumens an.

Die folgenden Screenshots zeigen die Konfigurationsschritte im Detail.

Am Disaster Recovery-Standort wird ein neues Datensicherungs-Volume erstellt, indem Sie Volumes auswählen und auf Datenreplizierung hinzufügen klicken. Auf der Registerkarte „Grundlagen“ müssen Sie den Namen des Volumes, den Kapazitäts-Pool und die Netzwerkinformationen angeben.

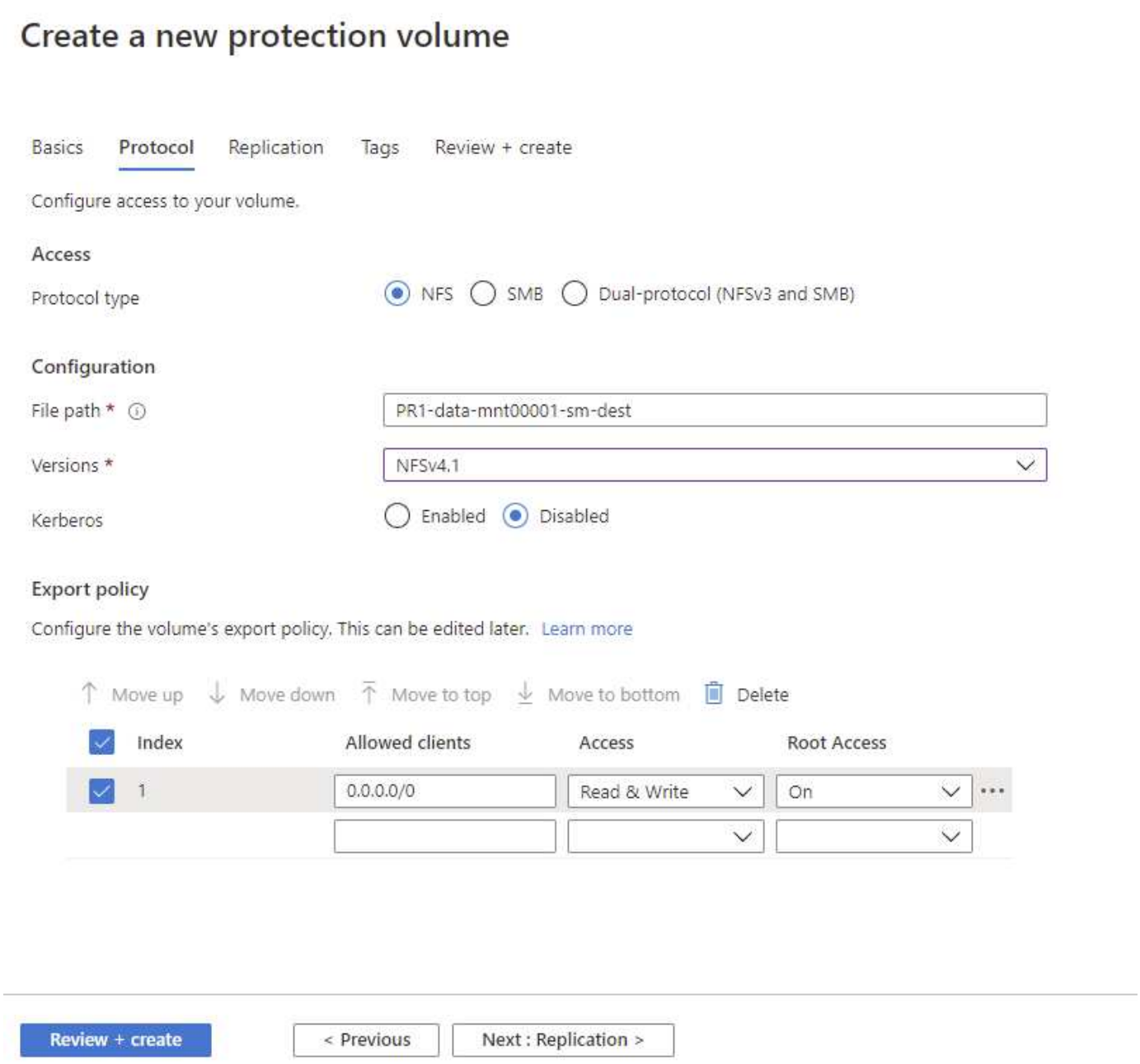
> Das Kontingent kann auf Basis der Kapazitätsanforderungen festgelegt werden, da die Volume-Performance sich nicht auf den Replizierungsprozess auswirkt. Bei einem Disaster Recovery-Failover muss die Quote an die tatsächlichen Performance-Anforderungen angepasst werden.

> Wenn der Kapazitäts-Pool mit manueller QoS konfiguriert wurde, können Sie den Durchsatz zusätzlich zu den Kapazitätsanforderungen konfigurieren. Wie oben angegeben können Sie den Durchsatz auch im normalen Betrieb mit niedrigem Wert konfigurieren und im Falle eines Disaster Recovery Failover diesen erhöhen.



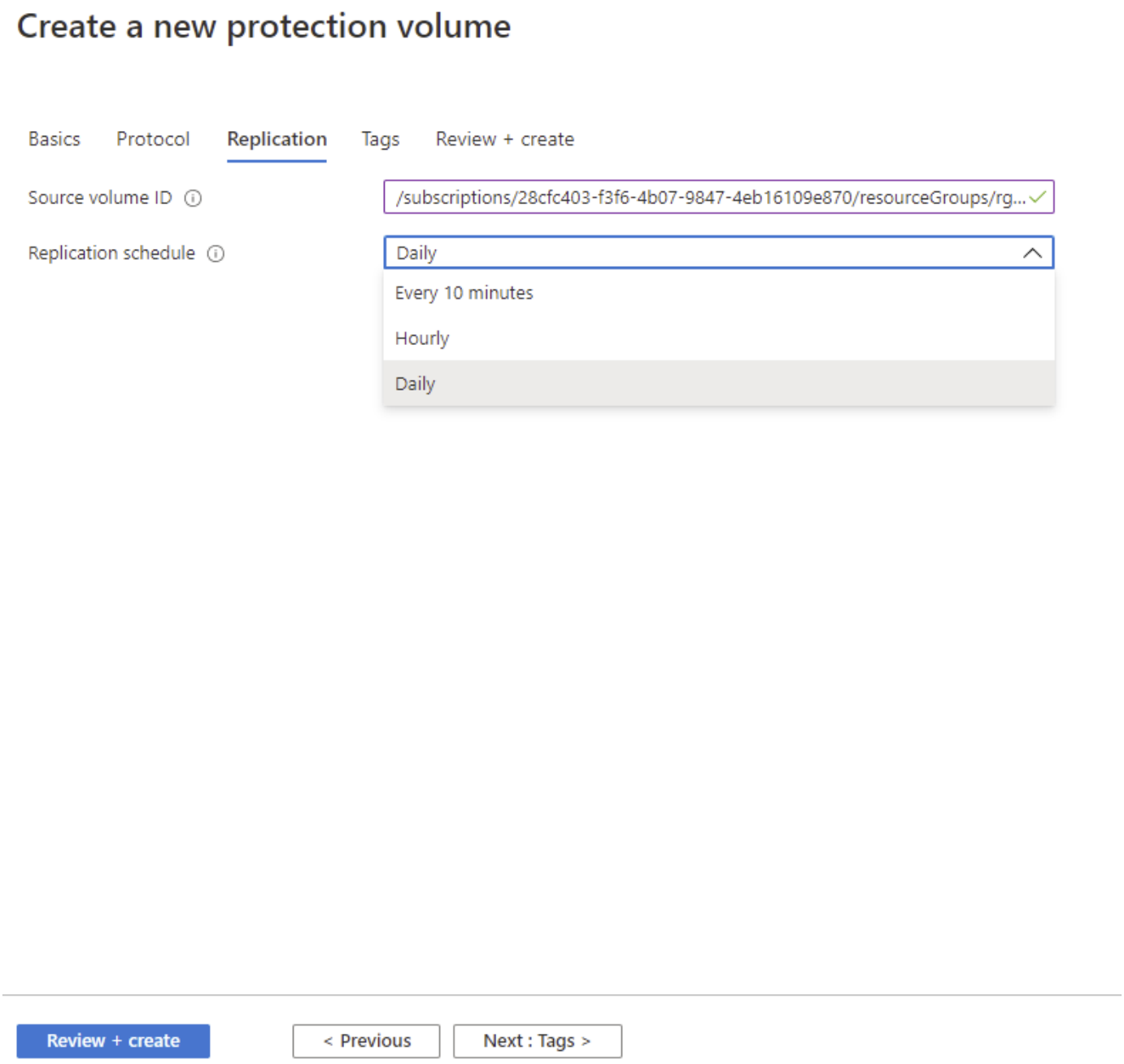
Auf der Registerkarte Protokoll müssen Sie das Netzwerkprotokoll, den Netzwerkpfad und die Exportrichtlinie angeben.

Das Protokoll muss dasselbe sein wie das für das Quell-Volume verwendete Protokoll.



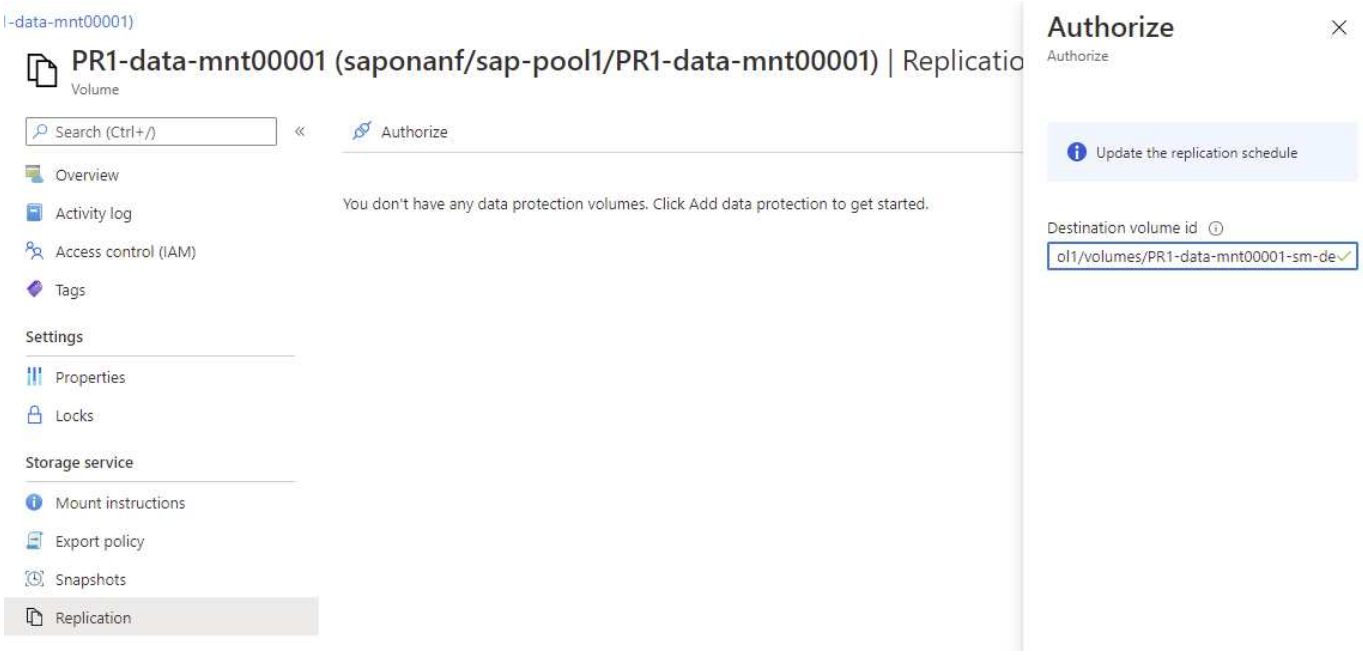
Auf der Registerkarte „Replikation“ müssen Sie die Quell-Volume-ID und den Replizierungsplan konfigurieren. Für die Datenreplizierung mit Daten-Volumes haben wir einen täglichen Replizierungszeitplan für unsere Einrichtung im Labor konfiguriert.

Die Quell-Volume-ID kann vom Bildschirm Eigenschaften des Quell-Volumes kopiert werden.



Als letzter Schritt müssen Sie die Replikation am Quell-Volume durch Angabe der ID des Ziel-Volume autorisieren.

Sie können die Ziel-Volume-ID vom Bildschirm Eigenschaften des Ziel-Volumes kopieren.



Für das freigegebene HANA und das Protokoll-Backup-Volume müssen dieselben Schritte durchgeführt werden.

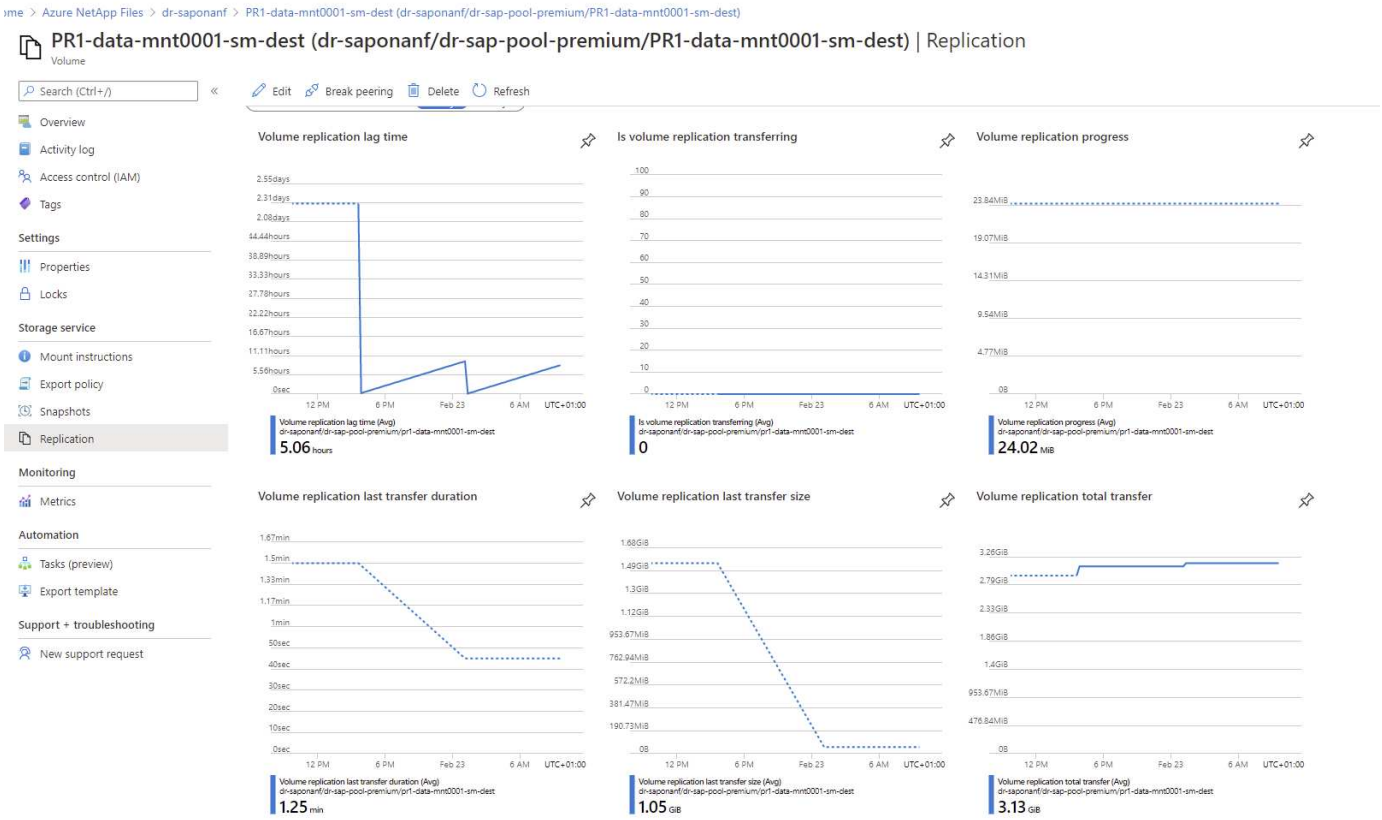
Überwachung der standortübergreifenden ANF-Replikation

Die folgenden drei Screenshots zeigen den Replikationsstatus für die Daten, Backup-Protokollierung und gemeinsam genutzte Volumes.

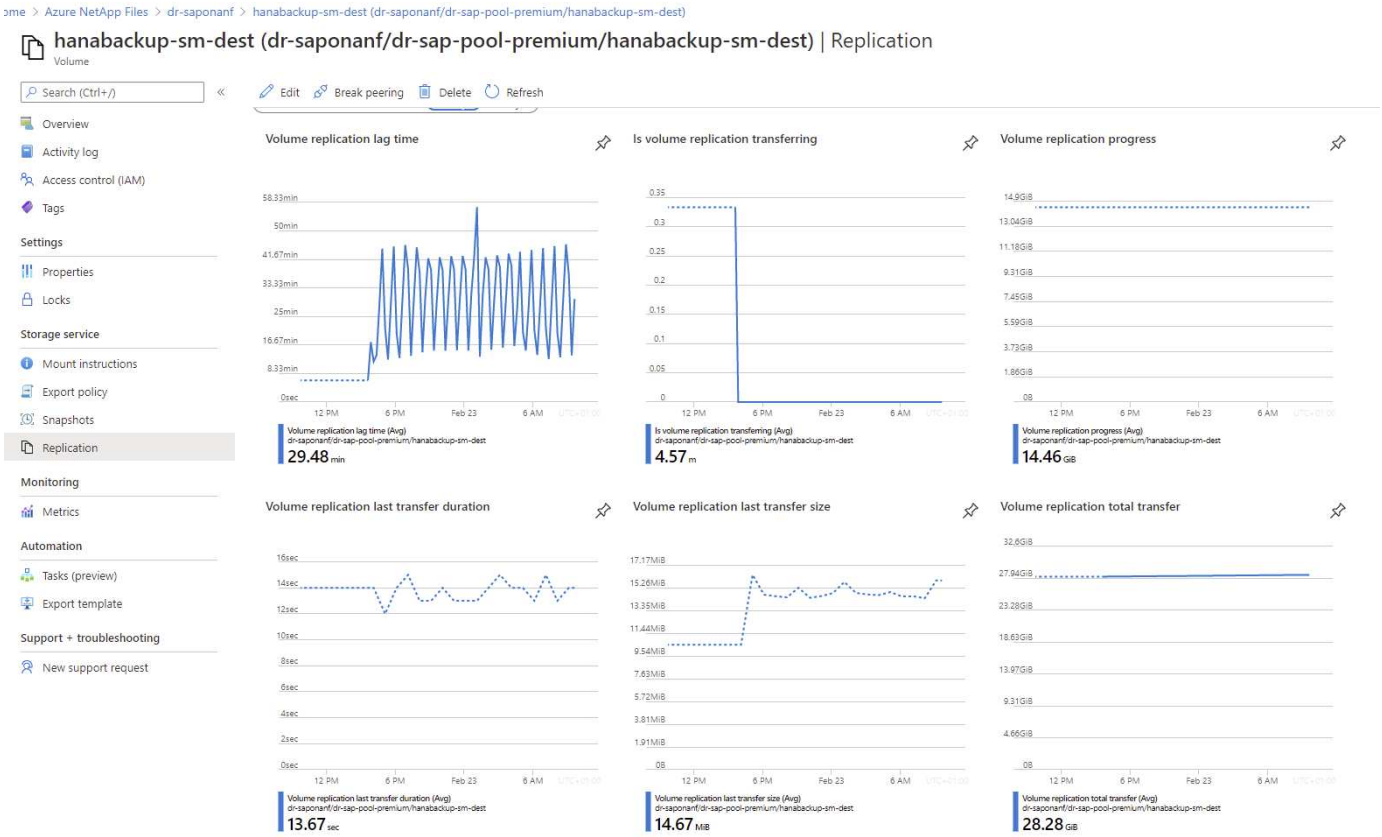
Die Verzögerung bei der Volume-Replizierung ist ein nützlicher Wert, um die RPO-Erwartungen zu verstehen. Beispielsweise zeigt die Replizierung des Backup-Volumes für das Protokoll eine maximale Verzögerungszeit von 58 Minuten, das heißt, dass der maximale RPO den gleichen Wert hat.

Die Übertragungsdauer und Übertragungsgröße bieten wertvolle Informationen zu den Bandbreitenanforderungen und ändern die Rate des replizierten Volumes.

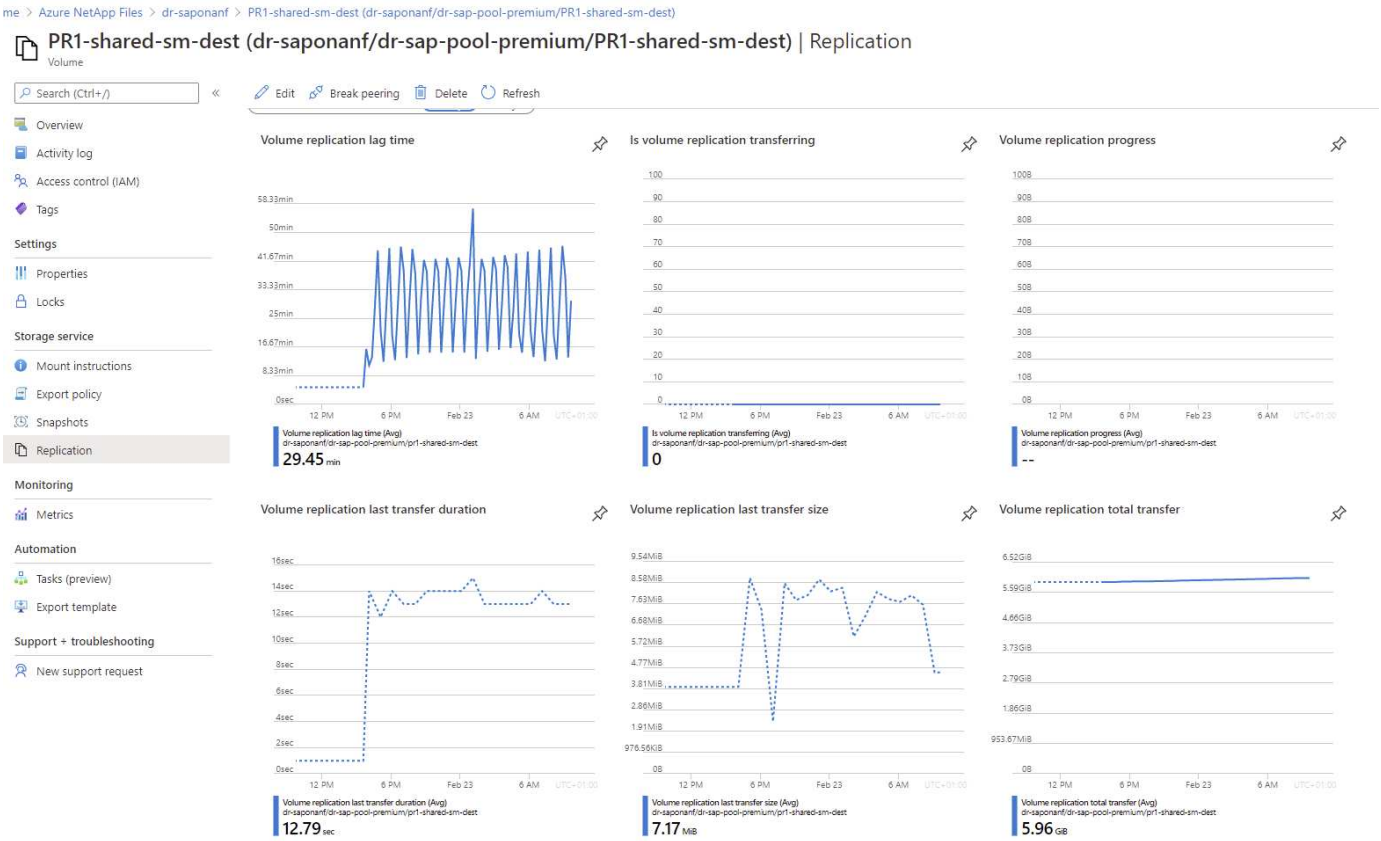
Der folgende Screenshot zeigt den Replizierungsstatus eines HANA Daten-Volumes.



Der folgende Screenshot zeigt den Replizierungsstatus eines HANA-Protokoll-Backup-Volumes.



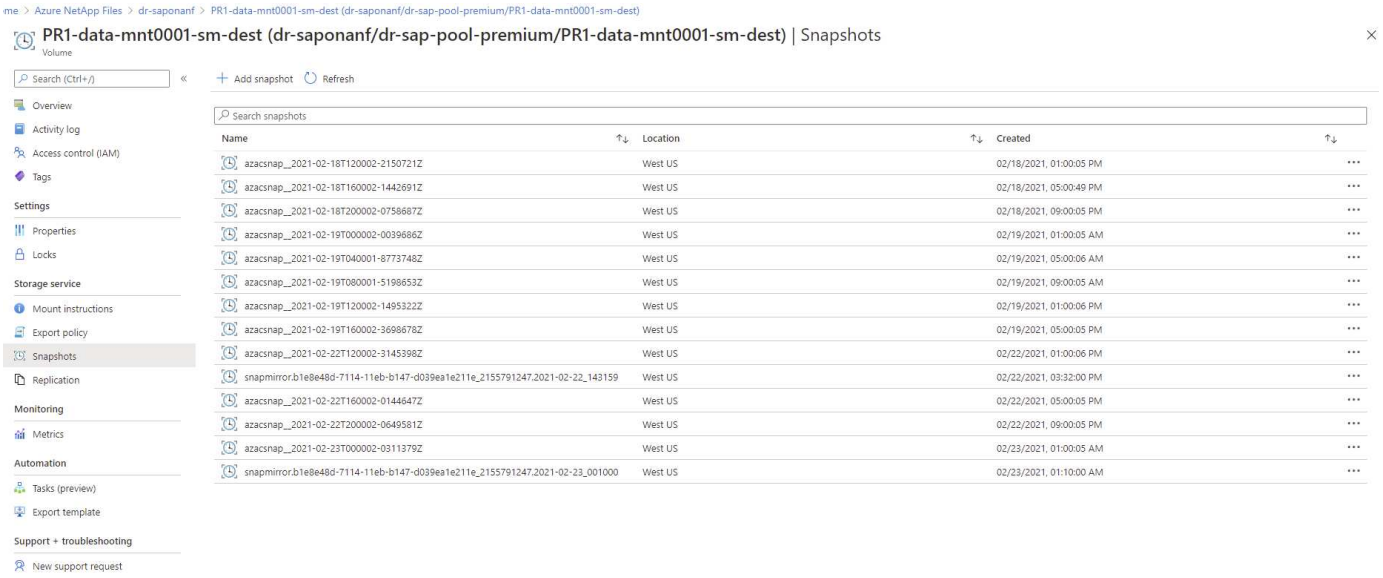
Der folgende Screenshot zeigt den Replizierungsstatus von einem Shared HANA Volume.



Replizierte Snapshot Backups

Bei jedem Replizierungs-Update vom Quell- zum Ziel-Volume werden alle Blockänderungen, die zwischen dem letzten und dem aktuellen Update stattgefunden haben, auf das Ziel-Volume repliziert. Dies umfasst auch die Snapshots, die auf dem Quell-Volume erstellt wurden. Der folgende Screenshot zeigt die Snapshots, die auf dem Zielvolume verfügbar sind. Wie bereits erwähnt, sind alle Snapshots, die vom Tool AzAcSnap erstellt wurden, applikationskonsistente Images der HANA Datenbank, die zur Ausführung eines Speicherpunktes oder einer vorwärts gerichteten Recovery verwendet werden können.

Innerhalb des Quell- und Ziel-Volume werden auch SnapMirror Snapshot Kopien erstellt, die für Resynchronisierung und Replizierungs-Updates verwendet werden. Diese Snapshot-Kopien sind aus Sicht der HANA-Datenbank nicht applikationskonsistent. Bei HANA-Recovery-Vorgängen können nur die über AzaCSnap erstellten applikationskonsistenten Snapshots verwendet werden.



Disaster Recovery-Tests

Disaster Recovery-Tests

Um eine effiziente Disaster Recovery-Strategie zu implementieren, müssen Sie den erforderlichen Workflow testen. Der Test zeigt, ob die Strategie funktioniert und ob die interne Dokumentation ausreichend ist, und ermöglicht es Administratoren auch, die erforderlichen Verfahren zu trainieren.

Die regionale ANF Replizierung ermöglicht Disaster-Recovery-Tests ohne Risiko für RTO und RPO. Disaster-Recovery-Tests können ohne Unterbrechung der Datenreplizierung durchgeführt werden.

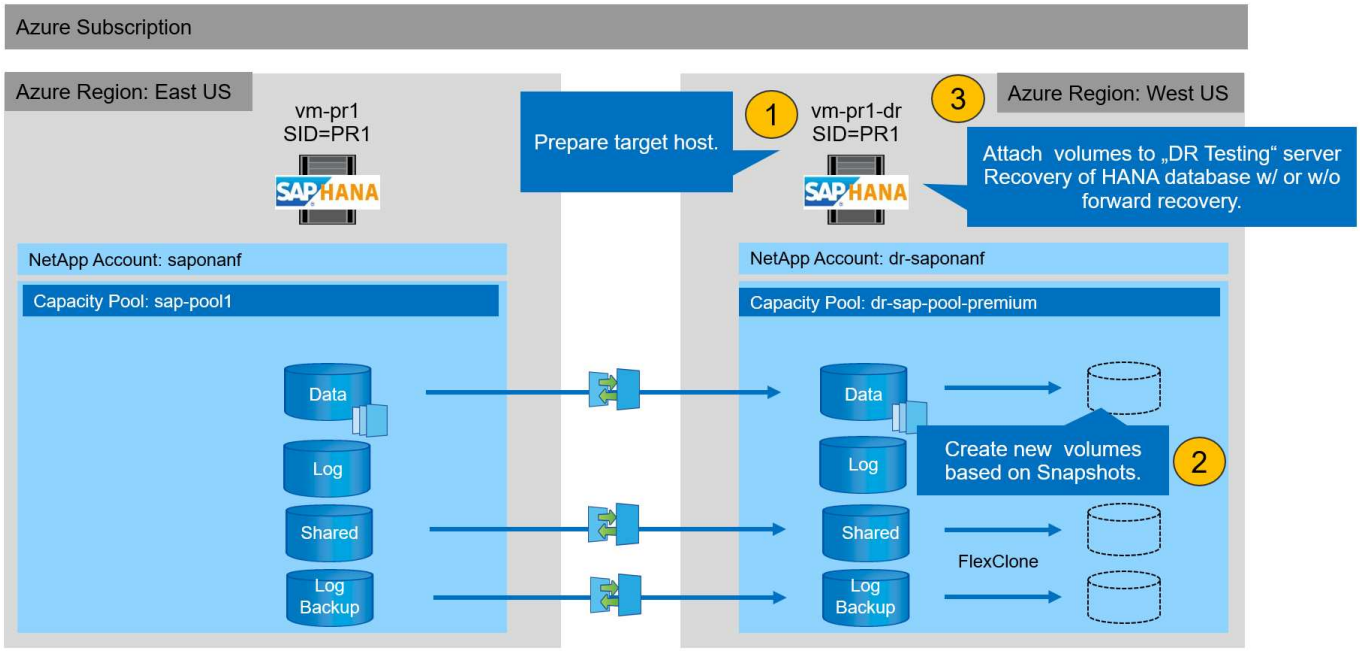
Der Workflow für Disaster Recovery-Tests nutzt die ANF-Funktionen, um auf Basis vorhandener Snapshot-Backups am Disaster-Recovery-Ziel neue Volumes zu erstellen. Siehe "Wie Azure NetApp Files Snapshots funktionieren - Microsoft Docs".

Je nachdem, ob die Backup-Replizierung des Protokolls Bestandteil der Disaster Recovery-Einrichtung ist oder nicht, unterscheiden sich die Schritte für die Disaster Recovery leicht. In diesem Abschnitt werden die Disaster Recovery-Tests für die reine Daten-Backup-Replizierung sowie für die Replizierung von Daten-Volumes in Kombination mit der Replizierung des Backup-Volumes für das Protokoll beschrieben.

Gehen Sie wie folgt vor, um Disaster-Recovery-Tests durchzuführen:

1. Bereiten Sie den Zielhost vor.
2. Erstellen neuer Volumes auf Basis von Snapshot Backups am Disaster-Recovery-Standort
3. Mounten Sie die neuen Volumes am Ziel-Host.
4. Stellen Sie die HANA Datenbank wieder her.
    - Nur Daten-Volume-Recovery.
    - Recovery mit replizierten Protokoll-Backups vorführen.

In den folgenden Abschnitten werden diese Schritte detailliert beschrieben.



Bereiten Sie den Zielhost vor

In diesem Abschnitt werden die Vorbereitungsschritte beschrieben, die auf dem Server für das Disaster-Recovery-Failover erforderlich sind.

Im normalen Betrieb wird der Zielhost normalerweise für andere Zwecke verwendet, beispielsweise als HANA QA- oder Testsystem. Daher müssen die meisten der beschriebenen Schritte bei der Ausführung von Disaster Failover-Tests ausgeführt werden. Zum anderen die relevanten Konfigurationsdateien, wie `/etc/fstab` Und `/usr/sap/sapservices`, Kann vorbereitet werden und dann in die Produktion durch einfaches Kopieren der Konfigurationsdatei. Das Disaster Recovery-Failover-Verfahren stellt sicher, dass die relevanten vorbereiteten Konfigurationsdateien korrekt konfiguriert sind.

Die Vorbereitung des Ziel-Hosts umfasst auch das Herunterfahren des HANA QA- oder Testsystems sowie das Anhalten aller Services mit `systemctl stop sapinit`.

Hostname und IP-Adresse des Zielservers

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

Ein ordnungsgemäßes Fechten des Zielservers muss eingerichtet werden, damit er nicht mit anderen Systemen kommunizieren kann. Wenn keine ordnungsgemäße Fechten vorhanden sind, kann das geklonte Produktionssystem Daten mit anderen Produktionssystemen austauschen, was zu logisch beschädigten Daten führt.

Installieren Sie die erforderliche Software

Die SAP-Hostagent-Software muss auf dem Zielserver installiert sein. Ausführliche Informationen finden Sie im "SAP Host Agent" Im SAP-Hilfeportal.

Wenn der Host als HANA QA- oder Testsystem verwendet wird, ist die SAP-Hostagent-Software bereits installiert.

Konfiguration von Benutzern, Ports und SAP-Diensten

Die erforderlichen Anwender und Gruppen für die SAP HANA-Datenbank müssen auf dem Zielserver verfügbar sein. In der Regel wird die zentrale Benutzerverwaltung verwendet. Daher sind keine Konfigurationsschritte auf dem Zielserver erforderlich. Die erforderlichen Ports für die HANA-Datenbank müssen auf den Ziel-Hosts konfiguriert sein. Die Konfiguration kann durch Kopieren des aus dem Quellsystem kopiert werden `/etc/services` Datei auf dem Zielserver.

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

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
limit.descriptors=1048576
```

HANA-Protokollvolumen vorbereiten

Da das HANA-Protokoll-Volume nicht Teil der Replikation ist, muss auf dem Ziel-Host ein leeres Protokoll-Volume vorhanden sein. Das Protokoll-Volume muss dieselben Unterverzeichnisse enthalten wie das Quell-HANA-System.

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root   root   4096 Feb 19 16:20 .
drwxr-xr-x 3 root   root     22 Feb 18 13:38 ..
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

Erstellen des Backup-Volumes für das Protokoll

Da das Quellsystem für die HANA-Protokoll-Backups mit einem separaten Volume konfiguriert ist, muss auch ein Protokoll-Backup-Volume auf dem Zielhost verfügbar sein. Ein Volume für die Protokoll-Backups muss konfiguriert und auf dem Ziel-Host gemountet werden.

Wenn die Protokollsicherung Teil der Disaster Recovery-Einrichtung ist, wird das replizierte Backup-Volume für das Protokoll auf dem Zielhost gemountet und es ist nicht erforderlich, ein zusätzliches Protokoll-Backup-Volume vorzubereiten.

Bereiten Sie Dateisystemeinhängungen vor

In der folgenden Tabelle sind die Namenskonventionen aufgeführt, die für das Lab-Setup verwendet werden. Die Volume-Namen am Disaster-Recovery-Standort sind in enthalten `/etc/fstab`.

HANA PR1-Volumes	Volumes und Unterverzeichnisse am Disaster Recovery-Standort	Bereitstellungspunkt am Zielhost
Datenvolumen	PR1-Data-mnt00001-SM-dest	/hana/Data/PR1/mnt00001
Freigegebenes Volume	PR1-shared-sm-dest/shared PR1-shared-SM-dest/usr-sap-PR1	/hana/shared /usr/sap/PR1
Backup-Volume protokollieren	Hanabackup-SM-dest	/Hanabackup

Die Mount-Punkte aus dieser Tabelle müssen auf dem Zielhost erstellt werden.

Hier sind die erforderlichen `/etc/fstab` Einträge.

```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest    /hanabackup nfs
rw,vers=3,hard,timeo=600,rsize=262144,wsize=262144,nconnect=8,bg,noatime,n
olock 0 0
```

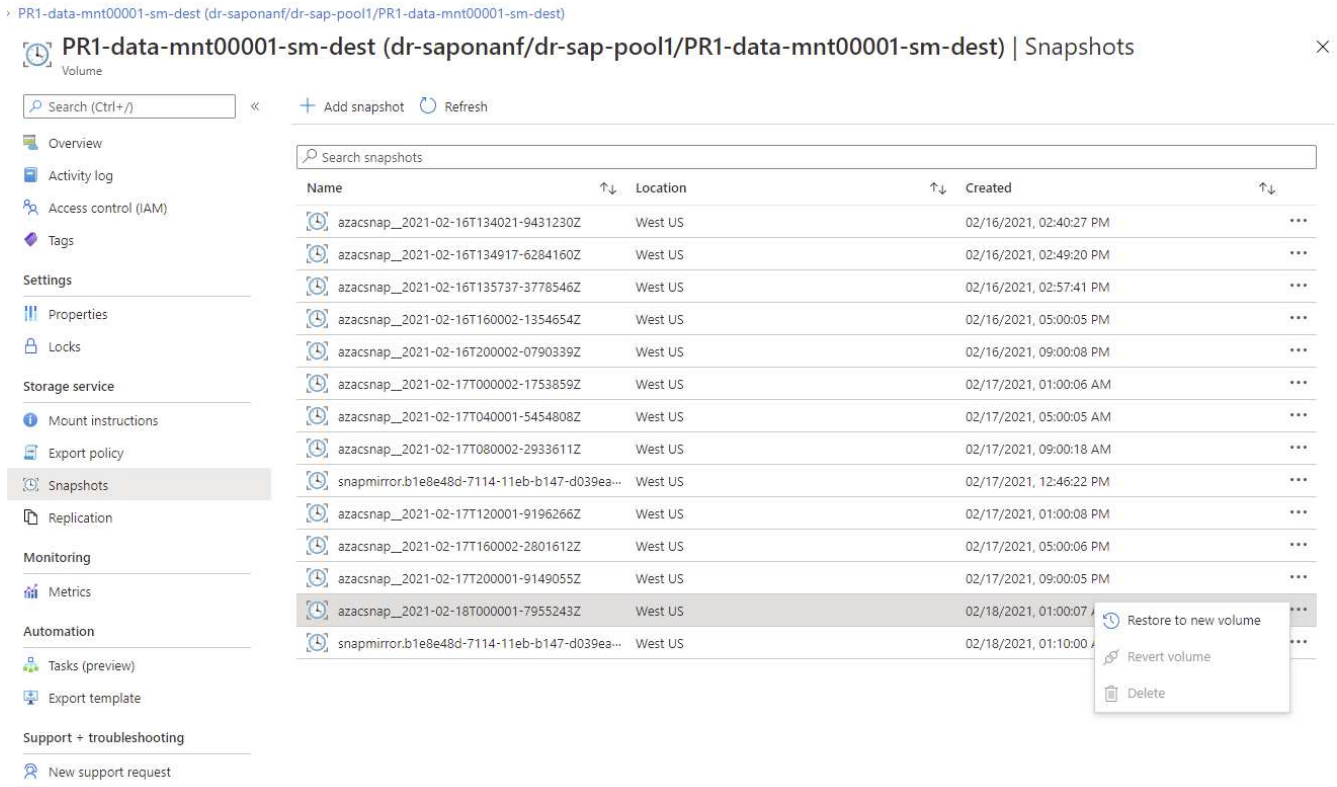
Erstellen Sie neue Volumes auf Basis von Snapshot-Backups am Disaster-Recovery-Standort

Abhängig vom Disaster Recovery Setup (mit oder ohne Log-Backup-Replikation) müssen zwei oder drei neue Volumes auf der Basis von Snapshot-Backups erstellt werden. In beiden Fällen muss ein neues Volume der Daten und das gemeinsame HANA Volume erstellt werden.

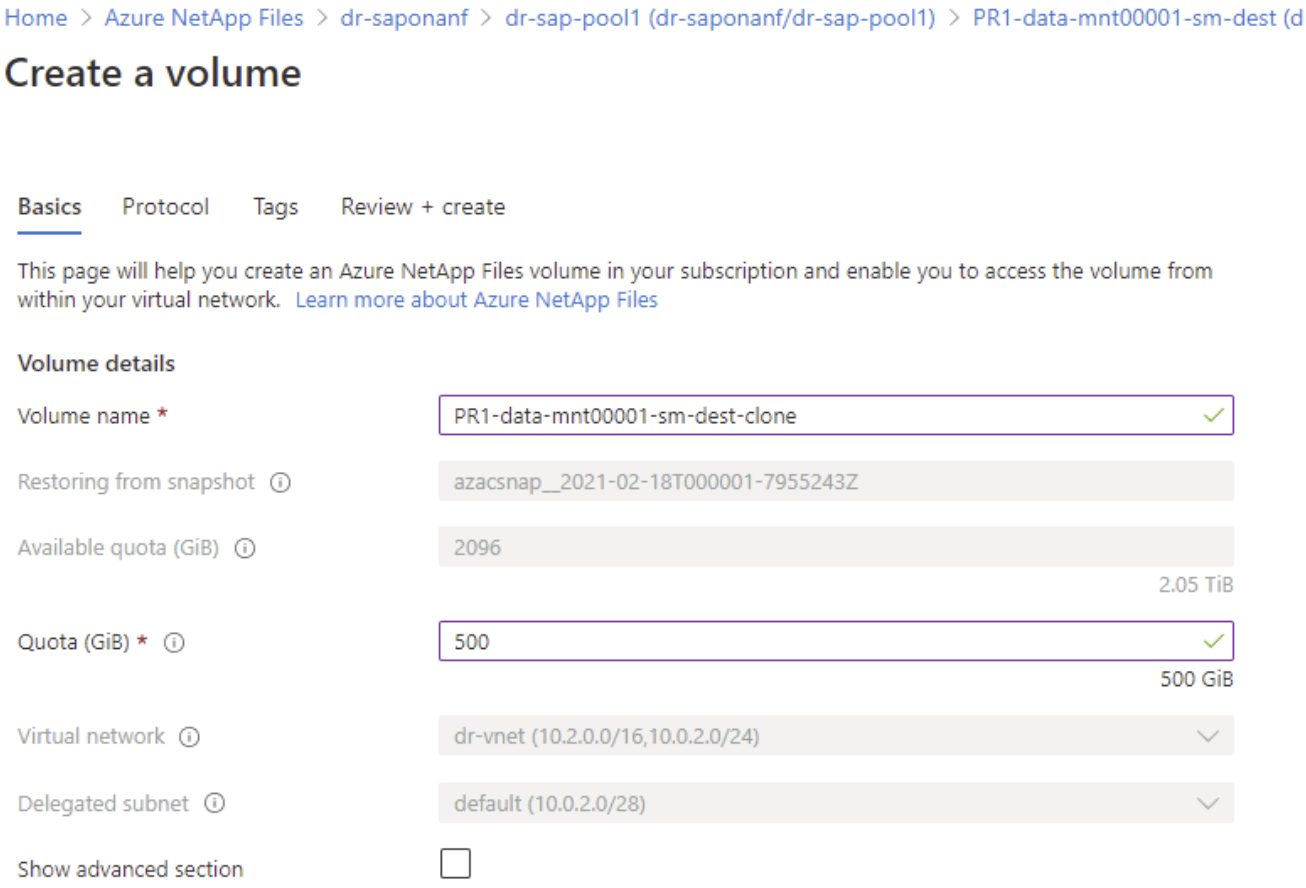
Wenn auch die Backup-Daten für das Protokoll repliziert werden, muss ein neues Volume des Backup-Volumes erstellt werden. In unserem Beispiel wurden die Daten und das Protokoll-Backup-Volume an den Disaster Recovery-Standort repliziert. In den folgenden Schritten wird das Azure-Portal verwendet.

1. Eines der applikationskonsistenten Snapshot-Backups wird als Quelle für das neue Volume des HANA-Daten-Volumes ausgewählt. Restore to New Volume ist ausgewählt, um ein neues Volume basierend auf

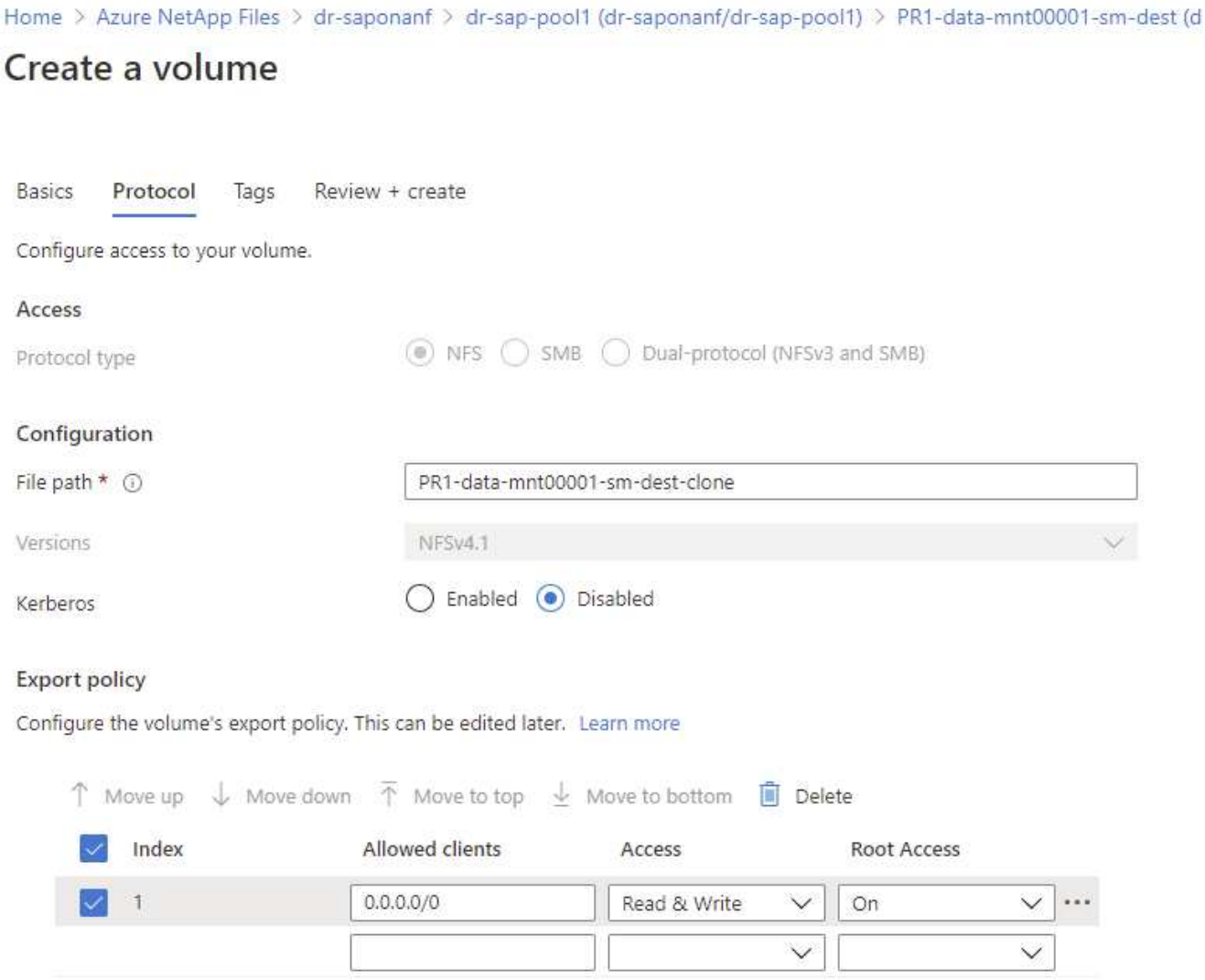
der Snapshot-Sicherung zu erstellen.



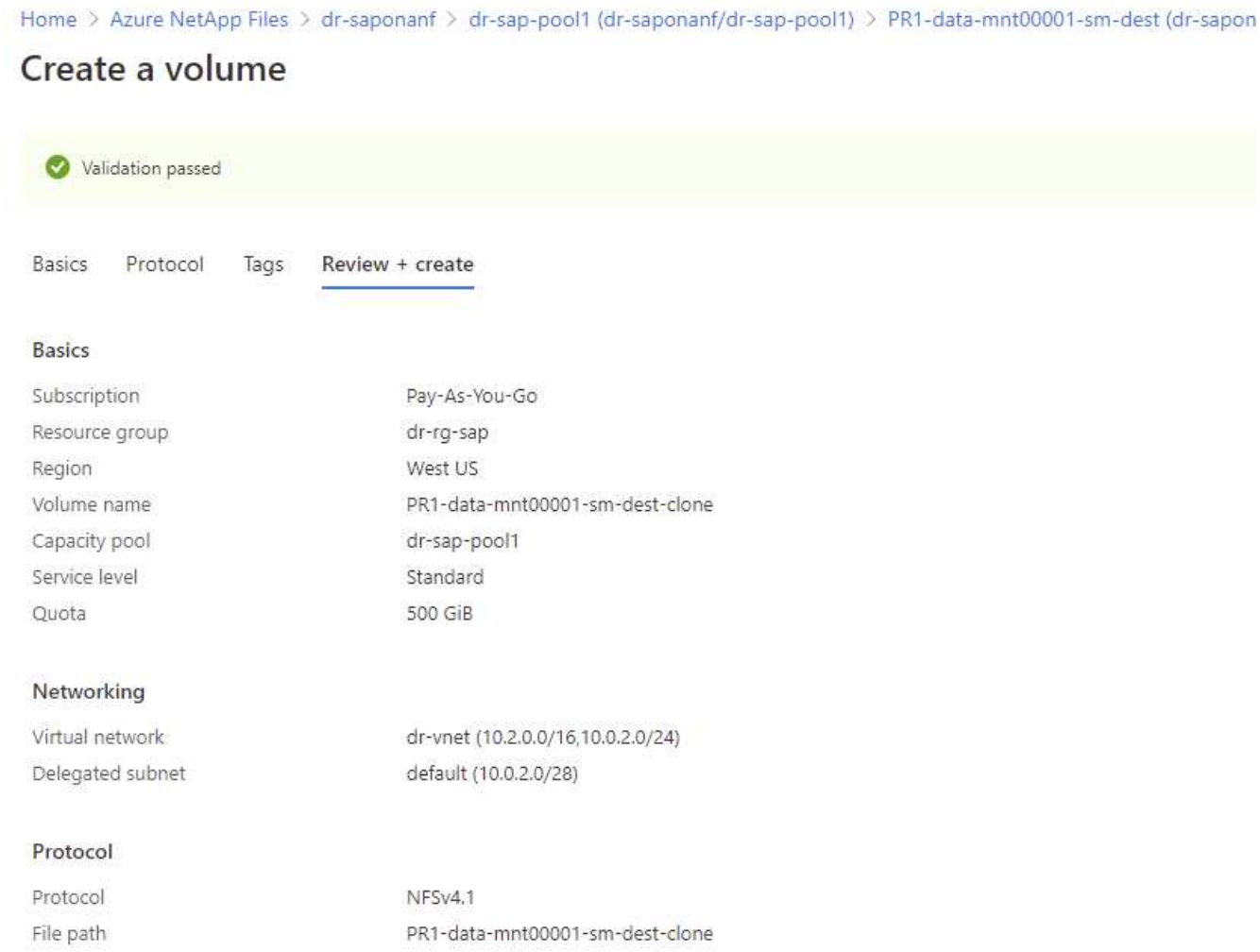
2. Der neue Volume-Name und die neue Quote müssen in der Benutzeroberfläche angegeben werden.



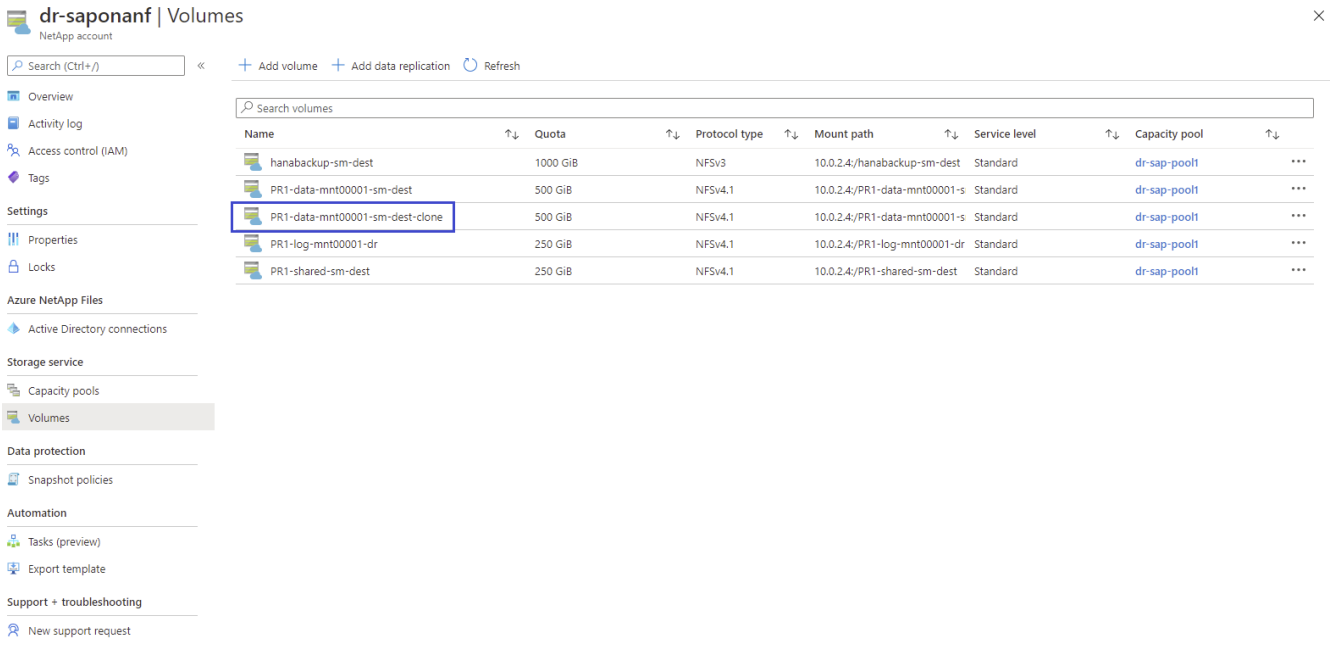
3. Auf der Registerkarte Protokoll werden der Dateipfad und die Exportrichtlinie konfiguriert.



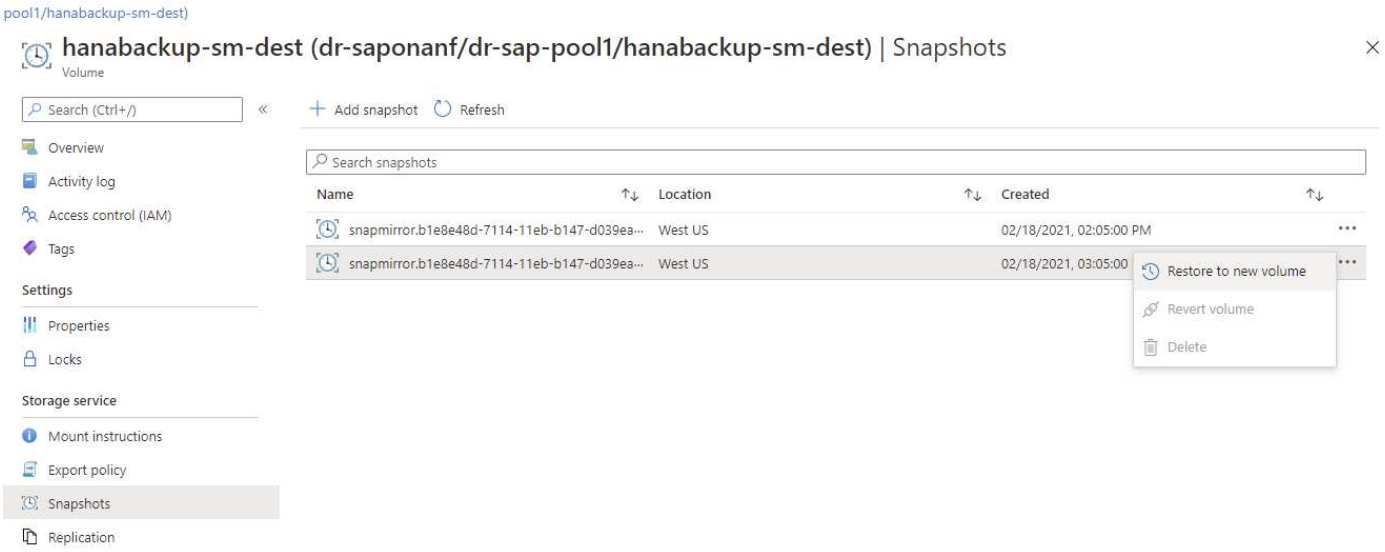
4. Der Bildschirm Erstellen und Prüfen fasst die Konfiguration zusammen.



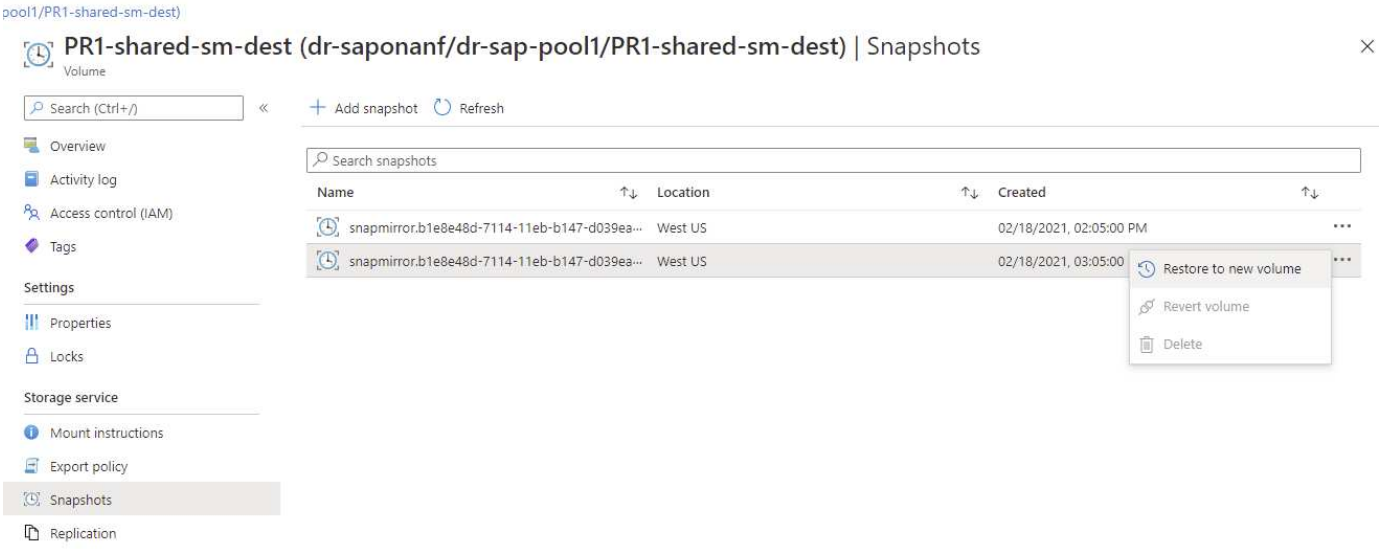
5. Auf Basis des HANA-Snapshot-Backups wurde jetzt ein neues Volume erstellt.



Die gleichen Schritte müssen nun für das freigegebene HANA und das Protokoll-Backup-Volumen, wie in den folgenden beiden Screenshots dargestellt, durchgeführt werden. Da keine zusätzlichen Snapshots für das HANA Shared-Backup-Volume und das Log-Backup-Volume erstellt wurden, muss die neueste SnapMirror Snapshot Kopie als Quelle für das neue Volume ausgewählt werden. Das sind unstrukturierte Daten, und die SnapMirror Snapshot Kopie kann für diesen Anwendungsfall genutzt werden.



Der folgende Screenshot zeigt das HANA Shared Volume, das auf dem neuen Volume wiederhergestellt ist.



Wenn ein Kapazitäts-Pool mit einer Tier mit niedriger Performance verwendet wurde, müssen die Volumes nun in einen Kapazitäts-Pool verschoben werden, der die erforderliche Performance bietet.

Alle drei neuen Volumes sind jetzt verfügbar und können auf dem Zielhost eingebunden werden.

Mounten Sie die neuen Volumes am Ziel-Host

Die neuen Volumes können jetzt auf Basis des auf dem Zielhost eingebunden werden `/etc/fstab` Datei zuvor erstellt.

```
vm-pr1:~ # mount -a
```

Die folgende Ausgabe zeigt die erforderlichen Dateisysteme.

```
vm-pr1:/hana/data/PR1/mnt00001/hdb00001 # df
Filesystem                                          1K-blocks     Used
Available Use% Mounted on
devtmpfs                                              8190344        8
8190336   1% /dev
tmpfs                                                12313116        0
12313116   0% /dev/shm
tmpfs                                                 8208744    17292
8191452   1% /run
tmpfs                                                 8208744        0
8208744   0% /sys/fs/cgroup
/dev/sda4                                            29866736  2438052
27428684   9% /
/dev/sda3                                             1038336   101520
936816  10% /boot
/dev/sda2                                              524008     1072
522936   1% /boot/efi
/dev/sdb1                                            32894736    49176
31151560   1% /mnt
tmpfs                                                 1641748        0
1641748   0% /run/user/0
10.0.2.4:/PR1-log-mnt00001-dr                    107374182400      256
107374182144   1% /hana/log/PR1/mnt00001
10.0.2.4:/PR1-data-mnt00001-sm-dest-clone      107377026560  6672640
107370353920   1% /hana/data/PR1/mnt00001
10.0.2.4:/PR1-shared-sm-dest-clone/hana-shared 107377048320 11204096
107365844224   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest-clone/usr-sap-PR1 107377048320 11204096
107365844224   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest-clone             107379429120 35293440
107344135680   1% /hanabackup
```

HANA Datenbank-Recovery

Im Folgenden werden die Schritte für das HANA-Datenbank-Recovery aufgeführt

Starten Sie die erforderlichen SAP-Dienste.

```
vm-pr1:~ # systemctl start sapinit
```

Die folgende Ausgabe zeigt die erforderlichen Prozesse.

```
vm-pr1:/ # ps -ef | grep sap
root     23101     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm   23191     1  3 11:29 ?        00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm   23202     1  5 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root     23292     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root     23359  2597  0 11:29 pts/1    00:00:00 grep --color=auto sap
```

In den folgenden Abschnitten wird der Recovery-Prozess mit und ohne Forward Recovery mit den replizierten Log-Backups beschrieben. Die Recovery wird mit dem HANA-Recovery-Skript für die Systemdatenbank und hdbsql-Befehle für die Mandanten-Datenbank ausgeführt.

Recovery zum aktuellen Backup-Speicherpunkt für das HANA-Datenvolumen

Die Wiederherstellung zum neuesten Backup savepoint wird mit folgenden Befehlen als User pr1adm ausgeführt:

- Systemdatenbank

```
recoverSys.py --command "RECOVER DATA USING SNAPSHOT CLEAR LOG”
```

- Mandantendatenbank

```
Within hdbsql: RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
```

Sie können auch HANA Studio oder Cockpit verwenden, um die Wiederherstellung des Systems und der Mandanten-Datenbank auszuführen.

Die folgende Befehlsausgabe zeigt die Ausführung der Wiederherstellung.

Recovery der Systemdatenbank

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py
--command="RECOVER DATA USING SNAPSHOT CLEAR LOG"
[139702869464896, 0.008] >> starting recoverSys (at Fri Feb 19 14:32:16
2021)
[139702869464896, 0.008] args: ()
[139702869464896, 0.009] keys: {'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 14:32:16 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 14:32:16
stopped system: 2021-02-19 14:32:16
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 14:32:21
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T14:32:56+00:00  P0027646      177bab4d610 INFO    RECOVERY
RECOVER DATA finished successfully
recoverSys finished successfully: 2021-02-19 14:32:58
[139702869464896, 42.017] 0
[139702869464896, 42.017] << ending recoverSys, rc = 0 (RC_TEST_OK), after
42.009 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>
```

Recovery von Mandanten-Datenbanken

Wenn für den Benutzer pr1adm am Quellsystem kein Benutzerspeicherschlüssel erstellt wurde, muss auf dem Zielsystem ein Schlüssel erstellt werden. Der im Schlüssel konfigurierte Datenbankbenutzer muss über Berechtigungen zur Ausführung von Mandanten-Recovery-Vorgängen verfügen.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>
```

Die Mandantenwiederherstellung wird jetzt mit hdbsql ausgeführt.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
0 rows affected (overall time 66.973089 sec; server time 66.970736 sec)
hdbsql SYSTEMDB=>
```

Die HANA-Datenbank ist jetzt betriebsbereit, und der Disaster-Recovery-Workflow für die HANA-Datenbank wurde getestet.

Recovery mit vorwärtsgerichteten Recovery mithilfe von Log-/Katalog-Backups

Log-Backups und der HANA-Backup-Katalog werden aus dem Quellsystem repliziert.

Die Wiederherstellung mit allen verfügbaren Log-Backups wird mit den folgenden Befehlen als Benutzer pr1adm ausgeführt:

- Systemdatenbank

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- Mandantendatenbank

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```

Um eine Wiederherstellung mit allen verfügbaren Protokollen durchzuführen, können Sie jederzeit als Zeitstempel in der Recovery-Anweisung verwenden.

Sie können auch HANA Studio oder Cockpit verwenden, um die Wiederherstellung des Systems und der Mandanten-Datenbank auszuführen.

Die folgende Befehlsausgabe zeigt die Ausführung der Wiederherstellung.

Recovery der Systemdatenbank

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING
SNAPSHOT"
[140404915394368, 0.008] >> starting recoverSys (at Fri Feb 19 16:06:40
2021)
[140404915394368, 0.008] args: ()
[140404915394368, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 16:06:40 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 16:06:40
stopped system: 2021-02-19 16:06:41
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 16:06:46
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T16:07:19+00:00  P0009897      177bb0b4416 INFO    RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
19T15:17:33+00:00, reached log position 38272960
recoverSys finished successfully: 2021-02-19 16:07:20
[140404915394368, 39.757] 0
[140404915394368, 39.758] << ending recoverSys, rc = 0 (RC_TEST_OK), after
39.749 secs
```

Recovery von Mandanten-Datenbanken

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit

hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 63.791121 sec; server time 63.788754 sec)

hdbsql SYSTEMDB=>
```

Die HANA-Datenbank ist jetzt betriebsbereit, und der Disaster-Recovery-Workflow für die HANA-Datenbank wurde getestet.

Überprüfen Sie die Konsistenz der neuesten Protokoll-Backups

Da die Volume-Replizierung für das Protokoll unabhängig vom von dem von der SAP HANA Datenbank ausgeführten Backup-Prozess durchgeführt wird, können am Disaster Recovery-Standort inkonsistente Backup-Dateien für Protokolle vorhanden sein. Nur die letzten Backup-Dateien für Protokolle sind möglicherweise inkonsistent und diese Dateien sollten überprüft werden, bevor eine Weiterleitung der Recovery am Disaster Recovery-Standort mithilfe der erfolgt `hdbbackupcheck` Werkzeug.

Wenn der `hdbbackupcheck` Tool meldet Fehler bei den letzten Protokollsicherungen muss der neueste Satz von Protokollsicherungen entfernt oder gelöscht werden.

```
pr1adm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

Die Prüfung muss für die aktuellen Log-Backup-Dateien des Systems und der Mandanten-Datenbank ausgeführt werden.

Wenn der `hdbbackupcheck` Tool meldet Fehler bei den letzten Protokollsicherungen muss der neueste Satz von Protokollsicherungen entfernt oder gelöscht werden.

Disaster-Recovery-Failover

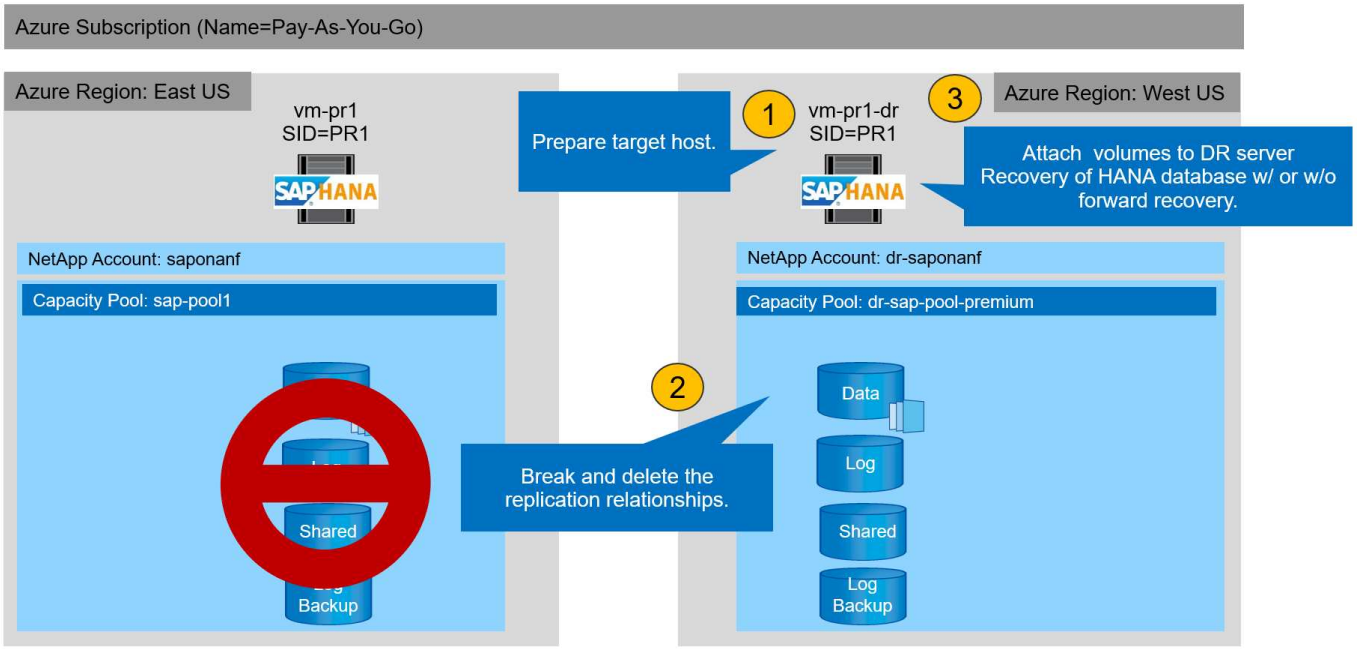
Disaster-Recovery-Failover

Je nachdem, ob die Backup-Replizierung des Protokolls Teil der Disaster Recovery-Einrichtung ist, unterscheiden sich die Schritte für Disaster Recovery leicht. In diesem Abschnitt wird das Disaster Recovery Failover für die reine Daten-Backup-Replizierung sowie für die Replizierung von Daten-Volumes in Kombination mit der Replizierung des Backup-Volumes für das Protokoll beschrieben.

Um Disaster Recovery-Failover auszuführen, gehen Sie wie folgt vor:

1. Bereiten Sie den Zielhost vor.
2. Brechen Sie die Replikationsbeziehungen auf und löschen Sie sie.
3. Wiederherstellung des Datenvolumens im letzten applikationskonsistenten Snapshot-Backup
4. Mounten Sie die Volumes am Ziel-Host.
5. Stellen Sie die HANA Datenbank wieder her.
    - Nur Daten-Volume-Recovery.
    - Recovery mit replizierten Protokoll-Backups vorführen.

In den folgenden Abschnitten werden diese Schritte detailliert beschrieben und die folgende Abbildung zeigt Disaster-Failover-Tests.



Bereiten Sie den Zielhost vor

In diesem Abschnitt werden die Vorbereitungsschritte beschrieben, die auf dem Server für das Disaster-Recovery-Failover erforderlich sind.

Im normalen Betrieb wird der Zielhost normalerweise für andere Zwecke verwendet, beispielsweise als HANA QA- oder Testsystem. Daher müssen die meisten der beschriebenen Schritte bei der Ausführung von Disaster Failover-Tests ausgeführt werden. Zum anderen die relevanten Konfigurationsdateien, wie `/etc/fstab` Und `/usr/sap/sapservices`, Kann vorbereitet werden und dann in die Produktion durch einfaches Kopieren der Konfigurationsdatei. Das Disaster Recovery-Failover-Verfahren stellt sicher, dass die relevanten vorbereiteten Konfigurationsdateien korrekt konfiguriert sind.

Die Vorbereitung des Ziel-Hosts umfasst auch das Herunterfahren des HANA QA- oder Testsystems sowie das Anhalten aller Services mit `systemctl stop sapinit`.

Hostname und IP-Adresse des Zielservers

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

> Ein ordnungsgemäßes Fechten des Zielservers muss eingerichtet werden, damit er nicht mit anderen Systemen kommunizieren kann. Wenn keine ordnungsgemäße Fechten vorhanden sind, kann das geklonte Produktionssystem Daten mit anderen Produktionssystemen austauschen, was zu logisch beschädigten Daten führt.

Installieren Sie die erforderliche Software

Die SAP-Hostagent-Software muss auf dem Zielserver installiert sein. Ausführliche Informationen finden Sie im "SAP Host Agent" Im SAP-Hilfeportal.

Wenn der Host als HANA QA- oder Testsystem verwendet wird, ist die SAP-Hostagent-Software bereits installiert.

Konfiguration von Benutzern, Ports und SAP-Diensten

Die erforderlichen Anwender und Gruppen für die SAP HANA-Datenbank müssen auf dem Zielserver verfügbar sein. In der Regel wird die zentrale Benutzerverwaltung verwendet. Daher sind keine Konfigurationsschritte auf dem Zielserver erforderlich. Die erforderlichen Ports für die HANA-Datenbank müssen auf den Ziel-Hosts konfiguriert sein. Die Konfiguration kann durch Kopieren des aus dem Quellsystem kopiert werden `/etc/services` Datei auf dem Zielserver.

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

```
vm-pr1:~ # cat /usr/sap/sapservices
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/PR1/HDB01/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
limit.descriptors=1048576
```

HANA-Protokollvolumen vorbereiten

Da das HANA-Protokoll-Volume nicht Teil der Replikation ist, muss auf dem Ziel-Host ein leeres Protokoll-Volume vorhanden sein. Das Protokoll-Volume muss dieselben Unterverzeichnisse enthalten wie das Quell-HANA-System.

```
vm-pr1:~ # ls -al /hana/log/PR1/mnt00001/
total 16
drwxrwxrwx 5 root   root   4096 Feb 19 16:20 .
drwxr-xr-x 3 root   root     22 Feb 18 13:38 ..
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 pr1adm sapsys 4096 Feb 22 10:25 hdb00003.00003
vm-pr1:~ #
```

Erstellen des Backup-Volumes für das Protokoll

Da das Quellsystem für die HANA-Protokoll-Backups mit einem separaten Volume konfiguriert ist, muss auch ein Protokoll-Backup-Volume auf dem Zielhost verfügbar sein. Ein Volume für die Protokoll-Backups muss konfiguriert und auf dem Ziel-Host gemountet werden.

Wenn die Protokollsicherung Teil der Disaster Recovery-Einrichtung ist, wird das replizierte Backup-Volume für das Protokoll auf dem Zielhost gemountet und es ist nicht erforderlich, ein zusätzliches Protokoll-Backup-Volume vorzubereiten.

Bereiten Sie Dateisystemeinhängungen vor

In der folgenden Tabelle sind die Namenskonventionen aufgeführt, die für das Lab-Setup verwendet werden. Die Volume-Namen am Disaster-Recovery-Standort sind in enthalten `/etc/fstab`.

HANA PR1-Volumes	Volumes und Unterverzeichnisse am Disaster Recovery-Standort	Bereitstellungspunkt am Zielhost
Datenvolumen	PR1-Data-mnt00001-SM-dest	/hana/Data/PR1/mnt00001
Freigegebenes Volume	PR1-shared-sm-dest/shared PR1-shared-SM-dest/usr-sap-PR1	/hana/shared /usr/sap/PR1
Backup-Volume protokollieren	Hanabackup-SM-dest	/Hanabackup

Die Mount-Punkte aus dieser Tabelle müssen auf dem Zielhost erstellt werden.

Hier sind die erforderlichen `/etc/fstab` Einträge.

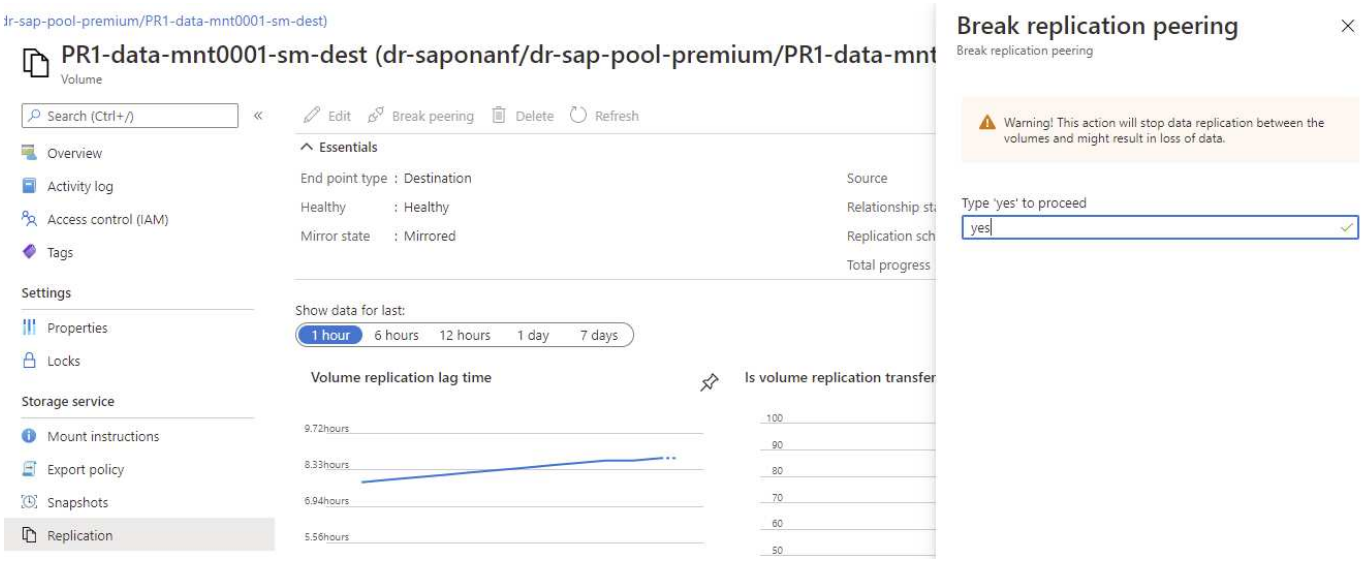
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest    /hanabackup nfs
rw,vers=3,hard,timeo=600,rsize=262144,wsize=262144,nconnect=8,bg,noatime,n
olock 0 0
```

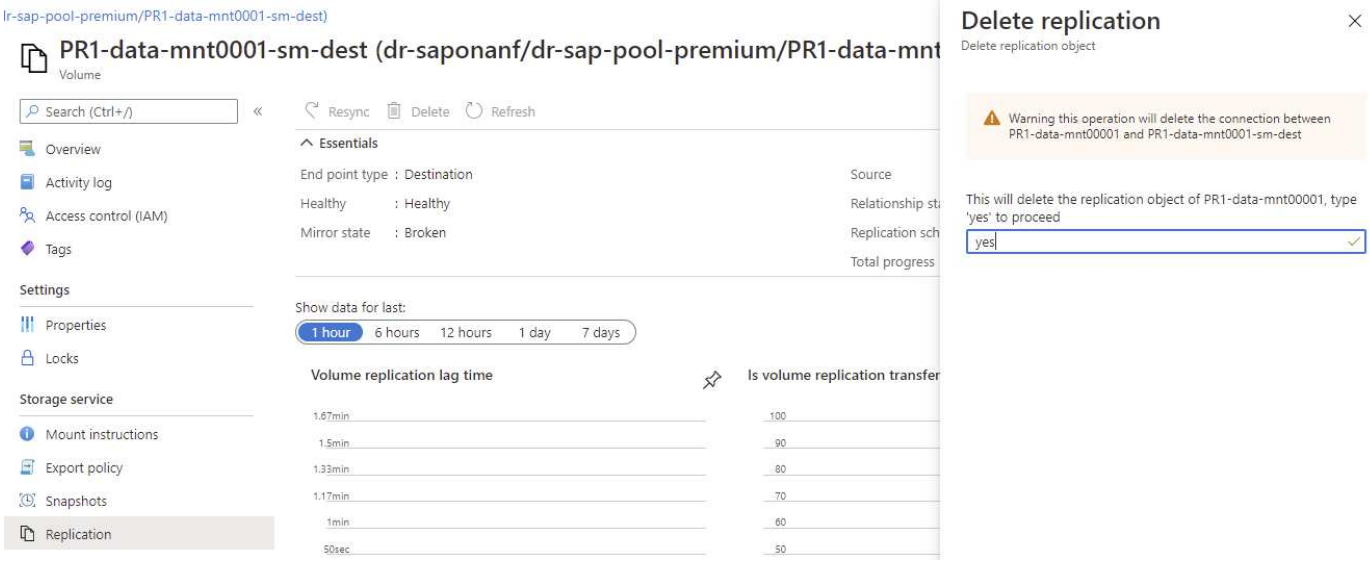
Peering der Replizierung unterbrechen und löschen

Im Falle eines Disaster-Failovers müssen die Ziel-Volumes unterbrochen werden, damit der Zielhost die Volumes für Lese- und Schreibvorgänge mounten kann.

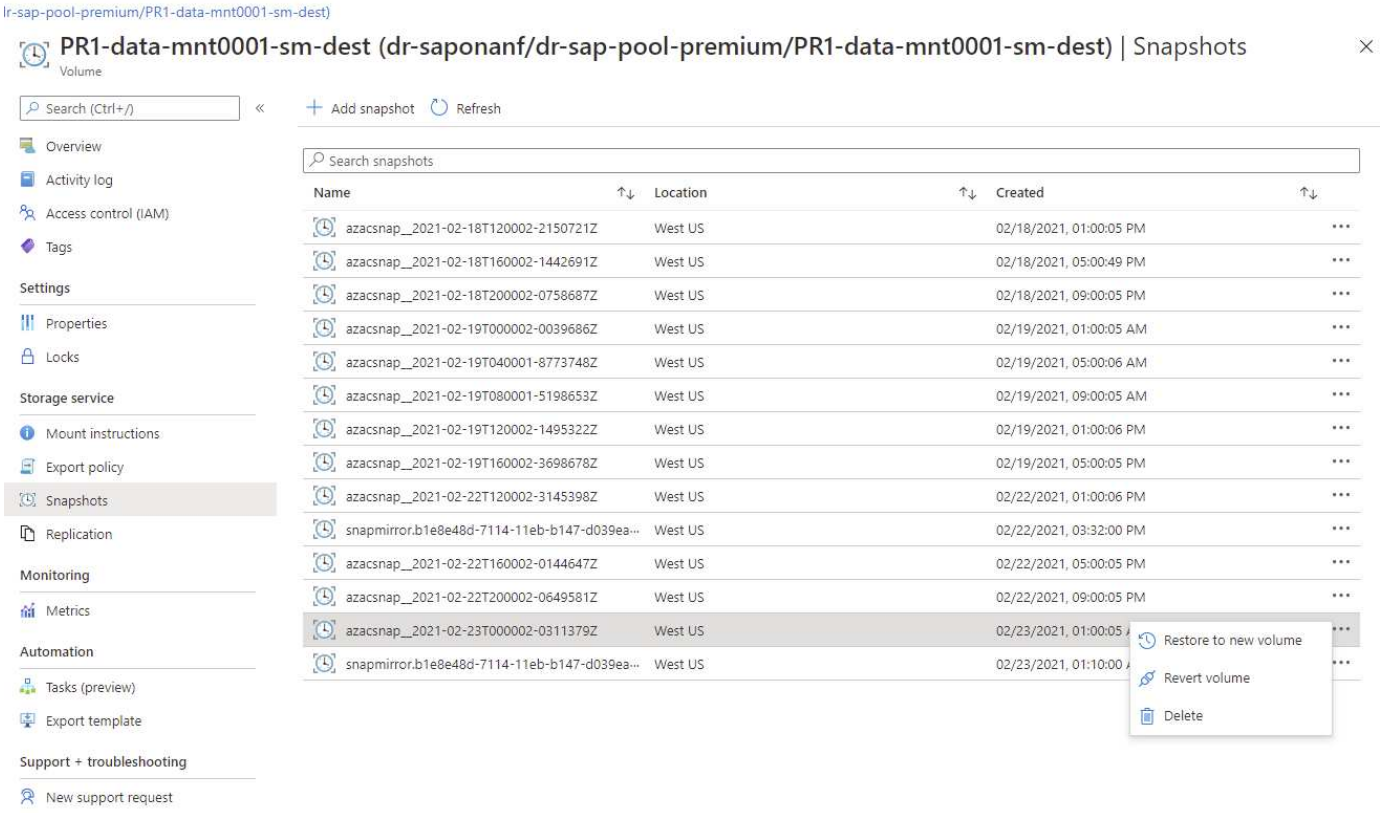
Für das HANA Daten-Volume müssen Sie das aktuelle HANA Snapshot-Backup wiederherstellen, das mit AzAcSnap erstellt wurde. Dieser Vorgang zum Zurücksetzen des Volumes ist nicht möglich, wenn der neueste ReplikationssSnapshot aufgrund des Replication Peering als belegt markiert wird. Deshalb müssen Sie auch das Replication Peering löschen.

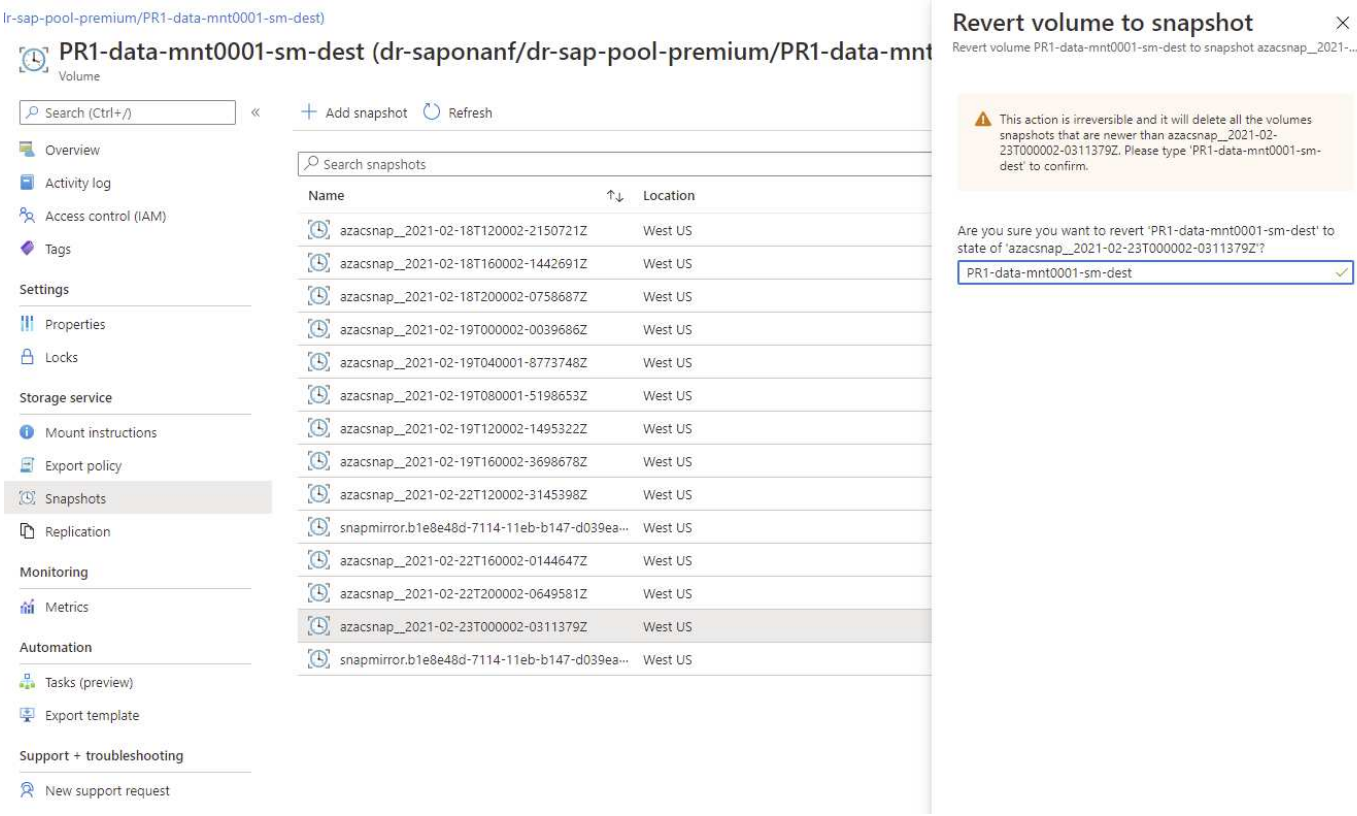
Die nächsten beiden Screenshots zeigen den Break and delete Peering-Vorgang für das HANA-Datenvolumen. Dieselben Vorgänge müssen auch für das Log-Backup und das gemeinsame HANA-Volume durchgeführt werden.





Da Replication Peering gelöscht wurde, ist es möglich, das Volume auf das neueste HANA Snapshot Backup zurückzusetzen. Wenn Peering nicht gelöscht wird, wird die Auswahl des Revert-Volumes ausgegraut und ist nicht wählbar. Die folgenden zwei Screenshots zeigen den Vorgang zur Zurücksetzen des Volumens.





Nach der Wiederherstellung des Volumes basiert das Daten-Volume auf einem konsistenten HANA-Snapshot-Backup und kann nun für Recovery-Vorgänge genutzt werden.

Wenn ein Kapazitäts-Pool mit einer Tier mit niedriger Performance verwendet wurde, müssen die Volumes nun in einen Kapazitäts-Pool verschoben werden, der die erforderliche Performance bietet.

Mounten Sie die Volumes am Ziel-Host

Die Volumes können jetzt auf der Grundlage des auf dem Zielhost eingebunden werden `/etc/fstab` Datei zuvor erstellt.

```
vm-pr1:~ # mount -a
```

Die folgende Ausgabe zeigt die erforderlichen Dateisysteme.

```
vm-pr1:~ # df
Filesystem                                      1K-blocks     Used
Available Use% Mounted on
devtmpfs                                         8201112        0
8201112   0% /dev
tmpfs                                           12313116        0
12313116   0% /dev/shm
tmpfs                                            8208744     9096
8199648   1% /run
tmpfs                                            8208744        0
8208744   0% /sys/fs/cgroup
/dev/sda4                                       29866736  2543948
27322788   9% /
/dev/sda3                                        1038336    79984
958352   8% /boot
/dev/sda2                                         524008     1072
522936   1% /boot/efi
/dev/sdb1                                       32894736    49180
31151556   1% /mnt
10.0.2.4:/PR1-log-mnt00001-dr            107374182400     6400
107374176000   1% /hana/log/PR1/mnt00001
tmpfs                                            1641748        0
1641748   0% /run/user/0
10.0.2.4:/PR1-shared-sm-dest/hana-shared 107377178368 11317248
107365861120   1% /hana/shared
10.0.2.4:/PR1-shared-sm-dest/usr-sap-PR1 107377178368 11317248
107365861120   1% /usr/sap/PR1
10.0.2.4:/hanabackup-sm-dest             107379678976 35249408
107344429568   1% /hanabackup
10.0.2.4:/PR1-data-mnt0001-sm-dest       107376511232  6696960
107369814272   1% /hana/data/PR1/mnt00001
vm-pr1:~ #
```

HANA Datenbank-Recovery

Im Folgenden werden die Schritte für das HANA-Datenbank-Recovery aufgeführt

Starten Sie die erforderlichen SAP-Dienste.

```
vm-pr1:~ # systemctl start sapinit
```

Die folgende Ausgabe zeigt die erforderlichen Prozesse.

```
vm-pr1:/ # ps -ef | grep sap
root     23101     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saphostexec pf=/usr/sap/hostctrl/exe/host_profile
pr1adm   23191     1  3 11:29 ?        00:00:00
/usr/sap/PR1/HDB01/exe/sapstartsrv
pf=/usr/sap/PR1/SYS/profile/PR1_HDB01_vm-pr1 -D -u pr1adm
sapadm   23202     1  5 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/sapstartsrv pf=/usr/sap/hostctrl/exe/host_profile -D
root     23292     1  0 11:29 ?        00:00:00
/usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root     23359  2597  0 11:29 pts/1    00:00:00 grep --color=auto sap
```

In den folgenden Abschnitten wird der Recovery-Prozess mit und ohne Forward Recovery mit den replizierten Log-Backups beschrieben. Die Recovery wird mit dem HANA-Recovery-Skript für die Systemdatenbank und hdbsql-Befehle für die Mandanten-Datenbank ausgeführt.

Recovery zum aktuellen Backup-Speicherpunkt für das HANA-Datenvolumen

Die Wiederherstellung zum neuesten Backup savepoint wird mit folgenden Befehlen als User pr1adm ausgeführt:

- Systemdatenbank

```
recoverSys.py --command "RECOVER DATA USING SNAPSHOT CLEAR LOG”
```

- Mandantendatenbank

```
Within hdbsql: RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
```

Sie können auch HANA Studio oder Cockpit verwenden, um die Wiederherstellung des Systems und der Mandanten-Datenbank auszuführen.

Die folgende Befehlsausgabe zeigt die Ausführung der Wiederherstellung.

Recovery der Systemdatenbank

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py
--command="RECOVER DATA USING SNAPSHOT CLEAR LOG"
[139702869464896, 0.008] >> starting recoverSys (at Fri Feb 19 14:32:16
2021)
[139702869464896, 0.008] args: ()
[139702869464896, 0.009] keys: {'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 14:32:16 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 14:32:16
stopped system: 2021-02-19 14:32:16
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 14:32:21
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T14:32:56+00:00  P0027646      177bab4d610 INFO    RECOVERY
RECOVER DATA finished successfully
recoverSys finished successfully: 2021-02-19 14:32:58
[139702869464896, 42.017] 0
[139702869464896, 42.017] << ending recoverSys, rc = 0 (RC_TEST_OK), after
42.009 secs
pr1adm@vm-pr1:/usr/sap/PR1/HDB01>
```

Recovery von Mandanten-Datenbanken

Wenn für den Benutzer pr1adm am Quellsystem kein Benutzerspeicherschlüssel erstellt wurde, muss auf dem Zielsystem ein Schlüssel erstellt werden. Der im Schlüssel konfigurierte Datenbankbenutzer muss über Berechtigungen zur Ausführung von Mandanten-Recovery-Vorgängen verfügen.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbuserstore set PR1KEY vm-pr1:30113
<backup-user> <password>
```

Die Mandantenwiederherstellung wird jetzt mit hdbsql ausgeführt.

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql SYSTEMDB=> RECOVER DATA FOR PR1 USING SNAPSHOT CLEAR LOG
0 rows affected (overall time 66.973089 sec; server time 66.970736 sec)
hdbsql SYSTEMDB=>
```

Die HANA-Datenbank ist jetzt betriebsbereit, und der Disaster-Recovery-Workflow für die HANA-Datenbank wurde getestet.

Recovery mit vorwärtsgerichteten Recovery mithilfe von Log-/Katalog-Backups

Log-Backups und der HANA-Backup-Katalog werden aus dem Quellsystem repliziert.

Die Wiederherstellung mit allen verfügbaren Log-Backups wird mit den folgenden Befehlen als Benutzer pr1adm ausgeführt:

- Systemdatenbank

```
recoverSys.py --command "RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT"
```

- Mandantendatenbank

```
Within hdbsql: RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
```

Um eine Wiederherstellung mit allen verfügbaren Protokollen durchzuführen, können Sie jederzeit als Zeitstempel in der Recovery-Anweisung verwenden.

Sie können auch HANA Studio oder Cockpit verwenden, um die Wiederherstellung des Systems und der Mandanten-Datenbank auszuführen.

Die folgende Befehlsausgabe zeigt die Ausführung der Wiederherstellung.

Recovery der Systemdatenbank

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> HDBSettings.sh recoverSys.py --command
"RECOVER DATABASE UNTIL TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING
SNAPSHOT"
[140404915394368, 0.008] >> starting recoverSys (at Fri Feb 19 16:06:40
2021)
[140404915394368, 0.008] args: ()
[140404915394368, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-20 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: ============2021-02-19 16:06:40 ============
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-19 16:06:40
stopped system: 2021-02-19 16:06:41
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-19 16:06:46
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-19T16:07:19+00:00  P0009897      177bb0b4416 INFO    RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
19T15:17:33+00:00, reached log position 38272960
recoverSys finished successfully: 2021-02-19 16:07:20
[140404915394368, 39.757] 0
[140404915394368, 39.758] << ending recoverSys, rc = 0 (RC_TEST_OK), after
39.749 secs
```

Recovery von Mandanten-Datenbanken

```
pr1adm@vm-pr1:/usr/sap/PR1/HDB01> hdbsql -U PR1KEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit

hdbsql SYSTEMDB=> RECOVER DATABASE FOR PR1 UNTIL TIMESTAMP '2021-02-20
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 63.791121 sec; server time 63.788754 sec)

hdbsql SYSTEMDB=>
```

Die HANA-Datenbank ist jetzt betriebsbereit, und der Disaster-Recovery-Workflow für die HANA-Datenbank wurde getestet.

Überprüfen Sie die Konsistenz der neuesten Protokoll-Backups

Da die Volume-Replizierung für das Protokoll unabhängig vom von dem von der SAP HANA Datenbank ausgeführten Backup-Prozess durchgeführt wird, können am Disaster Recovery-Standort inkonsistente Backup-Dateien für Protokolle vorhanden sein. Nur die letzten Backup-Dateien für Protokolle sind möglicherweise inkonsistent und diese Dateien sollten überprüft werden, bevor eine Weiterleitung der Recovery am Disaster Recovery-Standort mithilfe der erfolgt `hdbbackupcheck` Werkzeug.

Wenn der `hdbbackupcheck` Tool meldet Fehler bei den letzten Protokollsicherungen muss der neueste Satz von Protokollsicherungen entfernt oder gelöscht werden.

```
pr1adm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivecache'
Backup '/mnt/log-backup/SYSTEMDB/log_backup_0_0_0_0.1589289811148'
successfully checked.
```

Die Prüfung muss für die aktuellen Log-Backup-Dateien des Systems und der Mandanten-Datenbank ausgeführt werden.

Wenn der `hdbbackupcheck` Tool meldet Fehler bei den letzten Protokollsicherungen muss der neueste Satz von Protokollsicherungen entfernt oder gelöscht werden.

Aktualisierungsverlauf

An dieser Lösung wurden seit ihrer ersten Veröffentlichung folgende technische Änderungen vorgenommen:

Version	Datum	Zusammenfassung aktualisieren
Version 1.0	April 2021	Ausgangsversion