Disaster recovery SAP HANA con Azure NetApp Files

NetApp solutions for SAP

NetApp
October 30, 2025

Sommario

Disaster recovery SAP HANA con Azure NetApp Files

TR-4891: Disaster recovery SAP HANA con Azure NetApp Files

Gli studi hanno dimostrato che il downtime delle applicazioni di business ha un impatto negativo significativo sul business delle aziende.

Autori: Nils Bauer, NetApp Ralf Klahr, Microsoft

Oltre all'impatto finanziario, il downtime può anche danneggiare la reputazione dell'azienda, il morale dello staff e la fedeltà del cliente. Sorprendentemente, non tutte le aziende dispongono di una policy di disaster recovery completa.

L'esecuzione di SAP HANA su Azure NetApp Files (ANF) offre ai clienti l'accesso a funzionalità aggiuntive che estendono e migliorano le funzionalità integrate di protezione dei dati e disaster recovery di SAP HANA. Questa sezione panoramica illustra queste opzioni per aiutare i clienti a selezionare le opzioni che supportano le loro esigenze di business.

Per sviluppare una policy di disaster recovery completa, i clienti devono comprendere i requisiti delle applicazioni di business e le funzionalità tecniche di cui hanno bisogno per la protezione dei dati e il disaster recovery. La figura seguente fornisce una panoramica della protezione dei dati.

[Figura che mostra la finestra di dialogo input/output o rappresenta il contenuto scritto]

Requisiti delle applicazioni di business

Sono disponibili due indicatori chiave per le applicazioni aziendali:

- L'RPO (Recovery Point Objective) o la perdita massima tollerabile di dati
- L'RTO (Recovery Time Objective) o il downtime massimo tollerabile delle applicazioni aziendali

Questi requisiti sono definiti in base al tipo di applicazione utilizzata e alla natura dei dati di business. L'RPO e l'RTO potrebbero differire se si sta proteggendo dai guasti in una singola regione di Azure. Potrebbero anche differire se ti stai preparando a disastri catastrofici come la perdita di una regione Azure completa. È importante valutare i requisiti di business che definiscono l'RPO e l'RTO, perché questi requisiti hanno un impatto significativo sulle opzioni tecniche disponibili.

Alta disponibilità

L'infrastruttura per SAP HANA, come macchine virtuali, rete e storage, deve disporre di componenti ridondanti per garantire che non vi sia un singolo punto di errore. MS Azure offre ridondanza per i diversi componenti dell'infrastruttura.

Per garantire un'elevata disponibilità sul lato di elaborazione e applicazioni, gli host SAP HANA in standby possono essere configurati per l'alta disponibilità integrata con un sistema multihost SAP HANA. In caso di guasto di un server o di un servizio SAP HANA, il servizio SAP HANA esegue il failover sull'host di standby, causando il downtime dell'applicazione.

Se il downtime dell'applicazione non è accettabile in caso di guasto di server o applicazioni, è possibile

utilizzare la replica del sistema SAP HANA come soluzione ad alta disponibilità che consente il failover in tempi molto brevi. I clienti SAP utilizzano la replica del sistema HANA non solo per gestire l'alta disponibilità in caso di guasti non pianificati, ma anche per ridurre al minimo i downtime per le operazioni pianificate, come gli aggiornamenti del software HANA.

Corruzione logica

La corruzione logica può essere causata da errori software, errori umani o sabotaggio. Purtroppo, spesso la corruzione logica non può essere affrontata con soluzioni standard di alta disponibilità e disaster recovery. Di conseguenza, a seconda del livello, dell'applicazione, del file system o dello storage in cui si è verificato il danneggiamento logico, i requisiti RTO e RPO talvolta non possono essere soddisfatti.

Il caso peggiore è un danneggiamento logico in un'applicazione SAP. Le applicazioni SAP spesso operano in un ambiente in cui diverse applicazioni comunicano tra loro e scambiano dati. Pertanto, il ripristino e il ripristino di un sistema SAP in cui si è verificato un danneggiamento logico non è l'approccio consigliato. Il ripristino del sistema a un punto temporale prima che si verificasse il danneggiamento comporta la perdita di dati, quindi l'RPO diventa maggiore di zero. Inoltre, il panorama SAP non sarebbe più sincronizzato e richiederebbe un'ulteriore post-elaborazione.

Invece di ripristinare il sistema SAP, l'approccio migliore consiste nel cercare di correggere l'errore logico all'interno del sistema, analizzando il problema in un sistema di riparazione separato. L'analisi della causa principale richiede il coinvolgimento del processo di business e del proprietario dell'applicazione. Per questo scenario, si crea un sistema di riparazione (un clone del sistema di produzione) basato sui dati memorizzati prima che si verificasse il danneggiamento logico. All'interno del sistema di riparazione, i dati richiesti possono essere esportati e importati nel sistema di produzione. Con questo approccio, non è necessario arrestare il sistema produttivo e, nel migliore dei casi, non vengono persi dati o solo una piccola parte di dati.

> I passaggi necessari per configurare un sistema di riparazione sono identici a uno scenario di test di disaster recovery descritto in questo documento. La soluzione di disaster recovery descritta può quindi essere facilmente estesa per risolvere anche la corruzione logica.

Backup

I backup vengono creati per consentire il ripristino e il ripristino da diversi set di dati point-in-time. In genere, questi backup vengono conservati per un paio di giorni o poche settimane.

A seconda del tipo di danneggiamento, il ripristino e il ripristino possono essere eseguiti con o senza perdita di dati. Se l'RPO deve essere pari a zero, anche in caso di perdita dello storage primario e di backup, il backup deve essere combinato con la replica sincrona dei dati.

L'RTO per il ripristino e il ripristino è definito dal tempo di ripristino richiesto, dal tempo di ripristino (incluso l'avvio del database) e dal caricamento dei dati in memoria. Per database di grandi dimensioni e approcci di backup tradizionali, l'RTO può essere facilmente di diverse ore, il che potrebbe non essere accettabile. Per ottenere valori RTO molto bassi, è necessario combinare un backup con una soluzione hot-standby, che include il precaricamento dei dati in memoria.

Al contrario, una soluzione di backup deve affrontare la corruzione logica, perché le soluzioni di replica dei dati non possono coprire tutti i tipi di corruzione logica.

Replica sincrona o asincrona dei dati

L'RPO determina principalmente il metodo di replica dei dati da utilizzare. Se l'RPO deve essere pari a zero, anche in caso di perdita dello storage primario e di backup, i dati devono essere replicati in modo sincrono. Tuttavia, esistono limiti tecnici per la replica sincrona, ad esempio la distanza tra due aree Azure. Nella

maggior parte dei casi, la replica sincrona non è appropriata per distanze superiori a 100 km a causa della latenza, pertanto non è un'opzione per la replica dei dati tra le regioni di Azure.

Se un RPO più grande è accettabile, la replica asincrona può essere utilizzata su grandi distanze. L'RPO in questo caso è definito dalla frequenza di replica.

Replica di sistema HANA con o senza precaricamento dei dati

Il tempo di avvio di un database SAP HANA è molto più lungo di quello dei database tradizionali, perché è necessario caricare una grande quantità di dati in memoria prima che il database possa fornire le performance previste. Pertanto, una parte significativa dell'RTO è il tempo necessario per avviare il database. Con qualsiasi replica basata su storage e con la replica del sistema HANA senza precaricamento dei dati, il database SAP HANA deve essere avviato in caso di failover nel sito di disaster recovery.

La replica del sistema SAP HANA offre una modalità operativa in cui i dati vengono precaricati e continuamente aggiornati sull'host secondario. Questa modalità consente valori RTO molto bassi, ma richiede anche un server dedicato che viene utilizzato solo per ricevere i dati di replica dal sistema di origine.

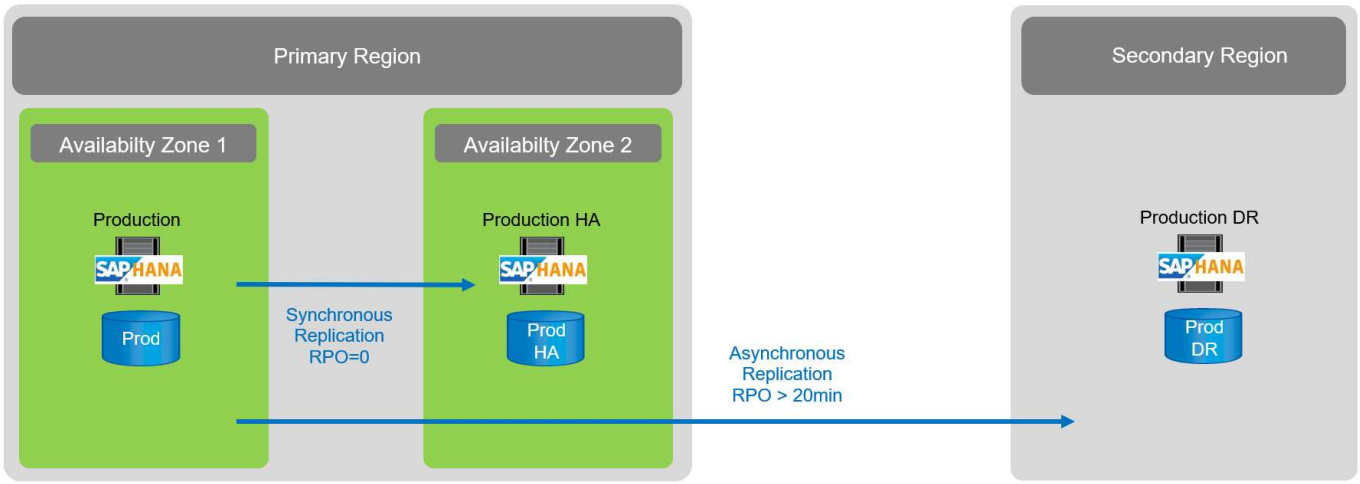
Confronto tra soluzioni di disaster recovery

Una soluzione di disaster recovery completa deve consentire ai clienti di eseguire il ripristino da un guasto completo del sito primario. Pertanto, i dati devono essere trasferiti a un sito secondario ed è necessaria un'infrastruttura completa per eseguire i sistemi SAP HANA di produzione richiesti in caso di guasto di un sito. A seconda dei requisiti di disponibilità dell'applicazione e del tipo di disastro da cui si desidera essere protetti, è necessario prendere in considerazione una soluzione di disaster recovery a due o tre siti.

La figura seguente mostra una configurazione tipica in cui i dati vengono replicati in modo sincrono all'interno della stessa regione Azure in una seconda zona di disponibilità. La breve distanza consente di replicare i dati in modo sincrono per ottenere un RPO pari a zero (generalmente utilizzato per fornire ha).

Inoltre, i dati vengono replicati in modo asincrono in una regione secondaria per essere protetti da disastri, quando la regione principale è interessata. L'RPO minimo ottenibile dipende dalla frequenza di replica dei dati, che è limitata dalla larghezza di banda disponibile tra la regione primaria e la regione secondaria. Un RPO minimo tipico è nell'intervallo da 20 minuti a più ore.

In questo documento vengono illustrate le diverse opzioni di implementazione di una soluzione di disaster recovery a due regioni.



Replica di sistema SAP HANA

La replica del sistema SAP HANA funziona a livello di database. La soluzione si basa su un sistema SAP HANA aggiuntivo nel sito di disaster recovery che riceve le modifiche dal sistema primario. Questo sistema secondario deve essere identico al sistema primario.

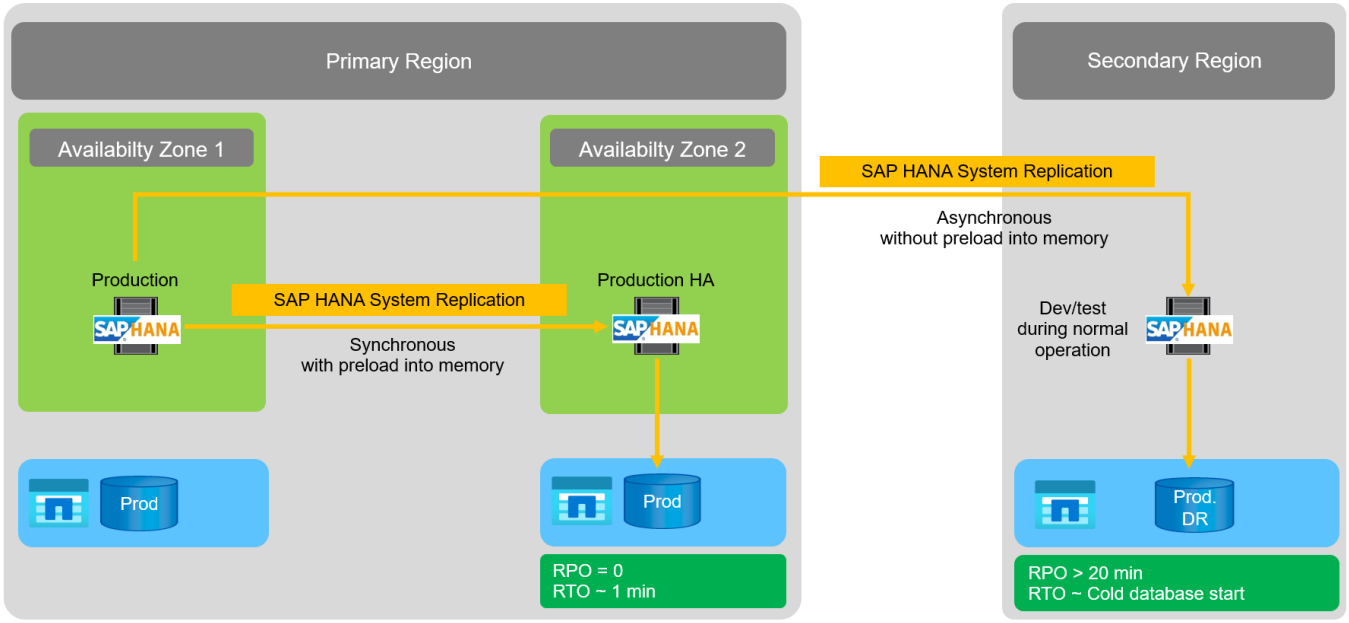
La replica del sistema SAP HANA può essere utilizzata in due modalità:

- Con i dati precaricati nella memoria e un server dedicato nel sito di disaster recovery:
  - Il server viene utilizzato esclusivamente come host secondario SAP HANA System Replication.
  - È possibile ottenere valori RTO molto bassi perché i dati sono già caricati in memoria e non è richiesto l'avvio del database in caso di failover.
- Senza i dati precaricati nella memoria e un server condiviso nel sito di disaster recovery:
  - Il server è condiviso come sistema secondario SAP HANA System Replication e come sistema di sviluppo/test.
  - L'RTO dipende principalmente dal tempo necessario per avviare il database e caricare i dati in memoria.

Per una descrizione completa di tutte le opzioni di configurazione e gli scenari di replica, vedere "Guida all'amministrazione di SAP HANA".

La figura seguente mostra la configurazione di una soluzione di disaster recovery a due regioni con SAP HANA System Replication. La replica sincrona con i dati precaricati nella memoria viene utilizzata per l'ha locale nella stessa regione Azure, ma in zone di disponibilità diverse. La replica asincrona senza dati precaricati viene configurata per l'area di disaster recovery remota.

La seguente figura illustra la replica di sistema SAP HANA.



Replica di sistema SAP HANA con dati precaricati in memoria

I valori RTO molto bassi con SAP HANA possono essere ottenuti solo con la replica di sistema SAP HANA con i dati precaricati in memoria. La replica del sistema SAP HANA con un server secondario dedicato nel sito di disaster recovery consente un valore RTO di circa 1 minuto o meno. I dati replicati vengono ricevuti e precaricati in memoria nel sistema secondario. A causa di questo basso tempo di failover, la replica del sistema SAP HANA viene spesso utilizzata anche per operazioni di manutenzione con downtime quasi pari a zero, come gli aggiornamenti del software HANA.

In genere, la replica del sistema SAP HANA è configurata per replicare in modo sincrono quando si sceglie il precarico dei dati. La distanza massima supportata per la replica sincrona è compresa nell'intervallo di 100 km.

Replica del sistema SAP senza dati precaricati in memoria

Per requisiti RTO meno rigorosi, è possibile utilizzare la replica del sistema SAP HANA senza precaricare i dati. In questa modalità operativa, i dati nell'area di disaster recovery non vengono caricati in memoria. Il server nell'area di DR viene ancora utilizzato per elaborare la replica del sistema SAP HANA eseguendo tutti i processi SAP HANA richiesti. Tuttavia, la maggior parte della memoria del server è disponibile per eseguire altri servizi, come i sistemi di sviluppo/test SAP HANA.

In caso di disastro, il sistema di sviluppo/test deve essere spento, deve essere avviato il failover e i dati devono essere caricati in memoria. L'RTO di questo approccio di standby a freddo dipende dalle dimensioni del database e dal throughput di lettura durante il caricamento dell'archivio di righe e colonne. Supponendo che i dati siano letti con un throughput di 1000 Mbps, il caricamento di 1 TB di dati dovrebbe richiedere circa 18 minuti.

Disaster recovery SAP HANA con replica cross-Region ANF

ANF la replica interregionale è integrata in ANF come soluzione di disaster recovery che utilizza la replica asincrona dei dati. ANF la replica interregionale viene configurata attraverso una relazione di protezione dei dati tra due volumi ANF su una regione Azure primaria e una secondaria. ANF Cross-Region Replication aggiorna il volume secondario utilizzando repliche delta a blocchi efficienti. È possibile definire le pianificazioni degli aggiornamenti durante la configurazione della replica.

La figura seguente mostra un esempio di soluzione di disaster recovery a due regioni, utilizzando la replica

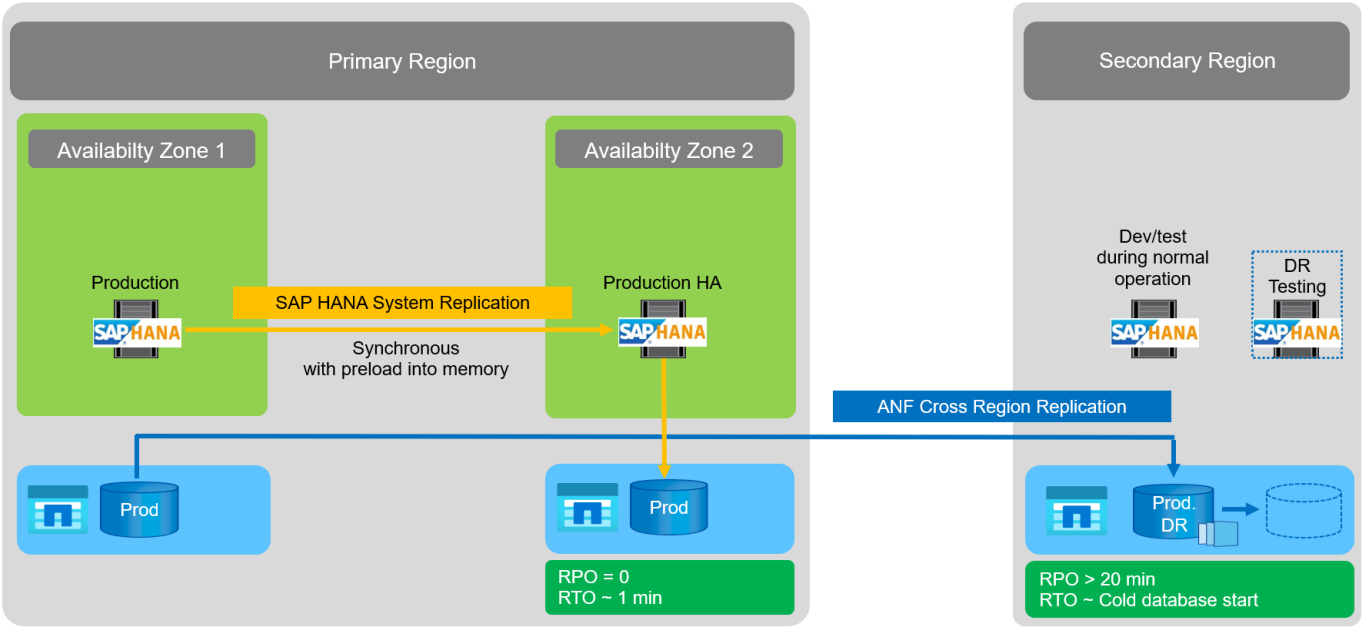
ANF Cross-Region. In questo esempio, il sistema HANA è protetto con la replica del sistema HANA all'interno della regione principale, come descritto nel capitolo precedente. La replica in una regione secondaria viene eseguita utilizzando la replica ANF cross-region. L'RPO è definito dalla pianificazione della replica e dalle opzioni di replica.

L'RTO dipende principalmente dal tempo necessario per avviare il database HANA nel sito di disaster recovery e per caricare i dati in memoria. Supponendo che i dati siano letti con un throughput di 1000 MB/s, il caricamento di 1 TB di dati richiederebbe circa 18 minuti. A seconda della configurazione della replica, è necessario eseguire anche il ripristino in avanti e aggiungerlo al valore RTO totale.

Ulteriori informazioni sulle diverse opzioni di configurazione sono fornite nel capitolo "Opzioni di configurazione per la replica tra regioni con SAP HANA".

I server dei siti di disaster recovery possono essere utilizzati come sistemi di sviluppo/test durante il normale funzionamento. In caso di disastro, i sistemi di sviluppo/test devono essere spenti e avviati come server di produzione DR.

ANF Cross-Region Replication consente di testare il flusso di lavoro DR senza influire sull'RPO e sull'RTO. Ciò si ottiene creando cloni di volume e allegandoli al server di test del DR.



Riepilogo delle soluzioni di disaster recovery

Nella tabella seguente vengono messe a confronto le soluzioni di disaster recovery discusse in questa sezione e vengono evidenziati gli indicatori più importanti.

I risultati principali sono i seguenti:

- Se è richiesto un RTO molto basso, la replica del sistema SAP HANA con precaricamento in memoria è l'unica opzione.
  - Per ricevere i dati replicati e caricare i dati in memoria, è necessario un server dedicato nel sito di DR.
- Inoltre, è necessaria la replica dello storage per i dati che risiedono all'esterno del database (ad esempio file condivisi, interfacce e così via).
- Se i requisiti RTO/RPO sono meno rigorosi, la replica ANF Cross-Region può essere utilizzata anche per:

    - Combinazione di replica dei dati di database e non di database.
    - Copertura di ulteriori casi di utilizzo come test di disaster recovery e refresh di test/sviluppo.
    - Con la replica dello storage, il server del sito di DR può essere utilizzato come sistema di QA o test durante il normale funzionamento.
- Una combinazione di SAP HANA System Replication come soluzione ha con RPO=0 con replica dello storage per lunghe distanze ha senso per soddisfare i diversi requisiti.

La seguente tabella fornisce un confronto tra le soluzioni di disaster recovery.

	Replica dello storage	**Replica di sistema SAP HANA**	
	Replica tra regioni	**Con precarico dei dati**	**Senza precaricamento dei dati**
RTO	Da basso a medio, a seconda del tempo di avvio del database e del ripristino in avanti	Molto basso	Da basso a medio, a seconda del tempo di avvio del database
RPO	RPO > 20 minuti di replica asincrona	RPO > 20 min di replica asincrona RPO=0 replica sincrona	RPO > 20 min di replica asincrona RPO=0 replica sincrona
I server del sito DR possono essere utilizzati per lo sviluppo/test	Sì	No	Sì
Replica di dati non di database	Sì	No	No
I dati DR possono essere utilizzati per il refresh dei sistemi di sviluppo/test	Sì	No	No
Test di DR senza influire su RTO e RPO	Sì	No	No

ANF Replication cross-Region con SAP HANA

ANF Replication cross-Region con SAP HANA

Le informazioni indipendenti dall'applicazione sulla replica tra più aree sono disponibili nella seguente posizione.

"Documentazione Azure NetApp Files | documenti Microsoft" nei concetti e nelle sezioni di guida.

Opzioni di configurazione per la replica interregionale con SAP HANA

La figura seguente mostra le relazioni di replica del volume per un sistema SAP HANA che utilizza la replica interregionale ANF. Con la replica interregionale ANF, i dati HANA e il volume condiviso HANA devono essere replicati. Se viene replicato solo il volume di dati HANA, i valori RPO tipici rientrano nell'intervallo di un giorno. Se sono richiesti valori RPO inferiori, è necessario replicare anche i backup del registro HANA per il forward

recovery.

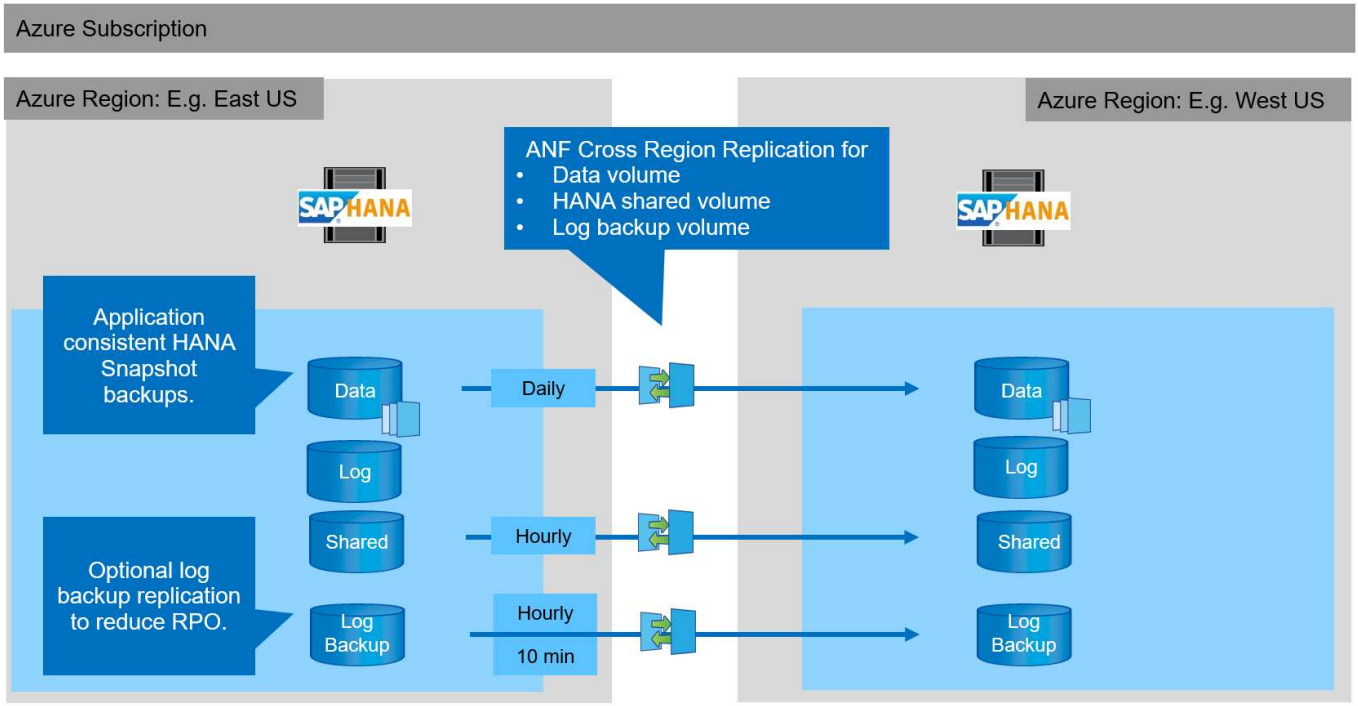
> Il termine "backup del log" utilizzato in questo documento include il backup del log e il backup del catalogo di backup HANA. Il catalogo di backup HANA è necessario per eseguire le operazioni di ripristino in avanti.

> La seguente descrizione e la configurazione di laboratorio si concentrano sul database HANA. Altri file condivisi, ad esempio la directory di trasporto SAP, vengono protetti e replicati allo stesso modo del volume condiviso HANA.

Per abilitare il ripristino del punto di salvataggio HANA o il ripristino in avanti utilizzando i backup del log, è necessario creare backup Snapshot dei dati coerenti con l'applicazione nel sito primario per il volume di dati HANA. Ciò può essere fatto ad esempio con lo strumento di backup ANF AzAcSnap (vedere anche "Che cos'è lo strumento Snapshot coerente delle applicazioni Azure per Azure NetApp Files | documenti Microsoft"). I backup Snapshot creati nel sito primario vengono quindi replicati nel sito di DR.

In caso di failover di emergenza, la relazione di replica deve essere interrotta, i volumi devono essere montati sul server di produzione DR e il database HANA deve essere ripristinato, nell'ultimo punto di salvataggio HANA o con il ripristino in avanti utilizzando i backup dei log replicati. Il capitolo "Failover del disaster recovery", descrive i passaggi necessari.

La seguente figura illustra le opzioni di configurazione HANA per la replica tra regioni.



Con la versione corrente di Cross-Region Replication, è possibile selezionare solo pianificazioni fisse e l'utente non può definire il tempo effettivo di aggiornamento della replica. I programmi disponibili sono giornalieri, orari e ogni 10 minuti. Utilizzando queste opzioni di pianificazione, due diverse configurazioni hanno senso a seconda dei requisiti RPO: Replica del volume di dati senza replica del backup del log e replica del backup del log con pianificazioni diverse, orarie o ogni 10 minuti. Il RPO più basso raggiungibile è di circa 20 minuti. La seguente tabella riassume le opzioni di configurazione e i valori RPO e RTO risultanti.

	Replica del volume di dati	Replica dei volumi di backup dei dati e dei log	Replica dei volumi di backup dei dati e dei log
Volume di dati di pianificazione CRR	Ogni giorno	Ogni giorno	Ogni giorno
Volume di backup del registro di pianificazione CRR	n/a.	Ogni ora	10 min
RPO max	24 ore + programma Snapshot (ad esempio, 6 ore)	1 ora	2 x 10 min
RTO massimo	Definito principalmente dal tempo di avvio di HANA	tempo di avvio HANA + tempo di ripristino	tempo di avvio HANA + tempo di ripristino
Recupero in avanti	NA	registri per le ultime 24 ore + programma Snapshot (ad esempio, 6 ore)	registri per le ultime 24 ore + programma Snapshot (ad esempio, 6 ore)

Requisiti e Best practice

Microsoft Azure non garantisce la disponibilità di un tipo specifico di macchina virtuale (VM) al momento della creazione o all'avvio di una macchina virtuale disallocata. In particolare, in caso di guasto di una regione, molti client potrebbero richiedere macchine virtuali aggiuntive nell'area di disaster recovery. Si consiglia pertanto di utilizzare attivamente una macchina virtuale con le dimensioni richieste per il failover di emergenza come sistema di test o di QA nell'area di disaster recovery per allocare il tipo di macchina virtuale richiesto.

Per l'ottimizzazione dei costi, è opportuno utilizzare un pool di capacità ANF con un Tier di performance inferiore durante il normale funzionamento. La replica dei dati non richiede performance elevate e potrebbe quindi utilizzare un pool di capacità con un Tier di performance standard. Per i test di disaster recovery o se è necessario un failover di emergenza, i volumi devono essere spostati in un pool di capacità con un Tier ad alte performance.

Se un secondo pool di capacità non è un'opzione, i volumi di destinazione della replica devono essere configurati in base ai requisiti di capacità e non ai requisiti di performance durante le normali operazioni. La quota o il throughput (per la QoS manuale) possono quindi essere adattati per il test di disaster recovery in caso di disaster failover.

Ulteriori informazioni sono disponibili all'indirizzo "Requisiti e considerazioni per l'utilizzo della replica cross-region dei volumi Azure NetApp Files | documenti Microsoft".

Setup di laboratorio

La convalida della soluzione è stata eseguita con un sistema host singolo SAP HANA. Lo strumento di backup Microsoft AzAcSnap Snapshot per ANF è stato utilizzato per configurare i backup Snapshot coerenti con l'applicazione HANA. Sono stati configurati un volume di dati giornaliero, un backup del registro orario e una replica del volume condiviso. Il test e il failover del disaster recovery sono stati validati con un punto di

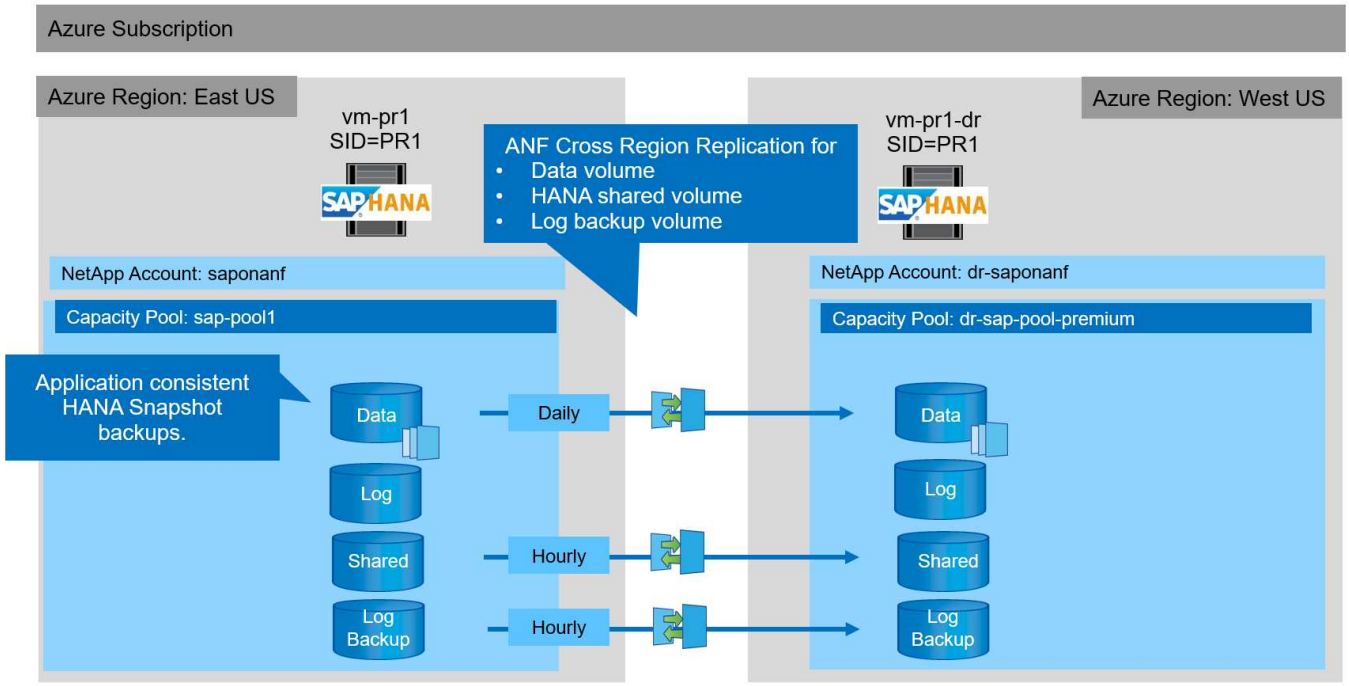
salvataggio e con operazioni di forward recovery.

Nella configurazione di laboratorio sono state utilizzate le seguenti versioni software:

- Sistema SAP HANA 2.0 SPS5 a host singolo con un singolo tenant
- SUSE SLES PER SAP 15 SP1
- AzAcSnap 5.0

Nel sito DR è stato configurato un singolo pool di capacità con QoS manuale.

La seguente figura illustra la configurazione di laboratorio.

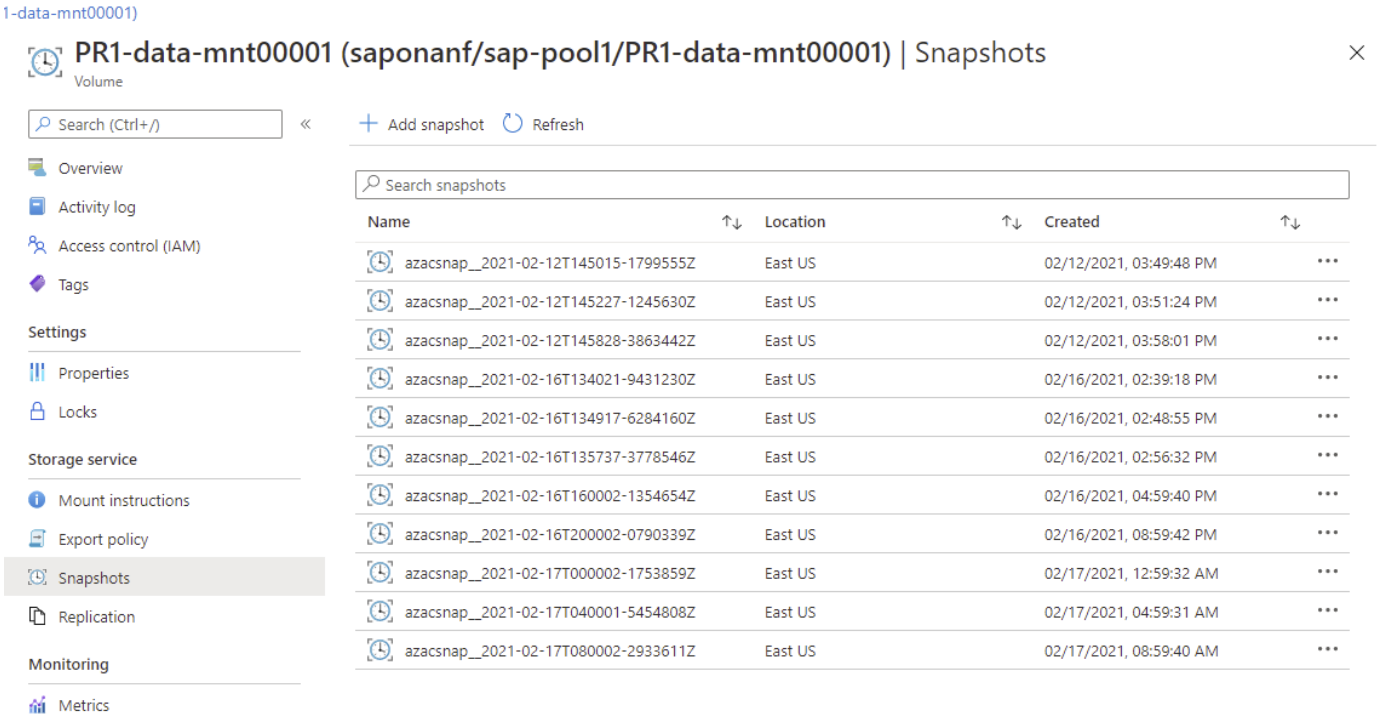


Configurazione del backup Snapshot con AzAcSnap

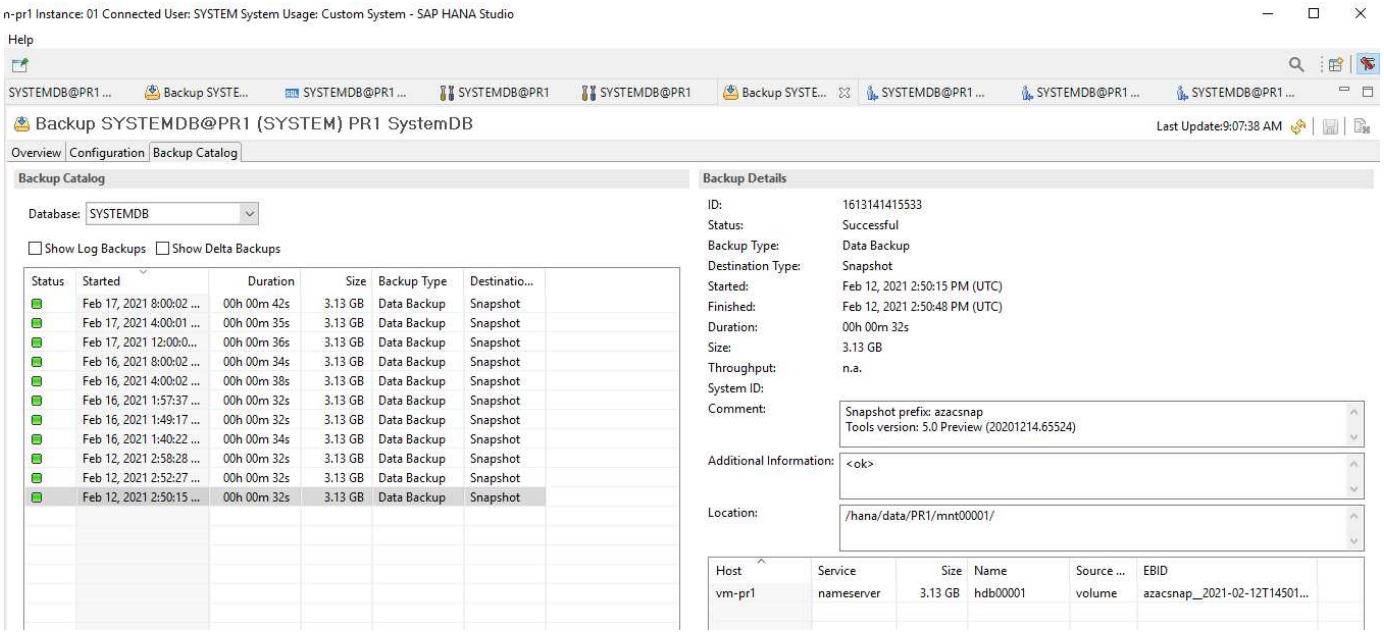
Nel sito principale, AzAcSnap è stato configurato per creare backup Snapshot coerenti con l'applicazione del sistema HANA PR1. Questi backup Snapshot sono disponibili nel volume di dati ANF del sistema PR1 HANA e sono registrati anche nel catalogo di backup SAP HANA, come mostrato nelle due figure seguenti. I backup Snapshot sono stati pianificati ogni 4 ore.

Con la replica del volume di dati utilizzando la replica ANF Cross-Region, questi backup Snapshot vengono replicati nel sito di disaster recovery e possono essere utilizzati per ripristinare il database HANA.

La figura seguente mostra i backup Snapshot del volume di dati HANA.



La figura seguente mostra il catalogo di backup SAP HANA.



Procedura di configurazione per la replica ANF Cross-Region

Prima di poter configurare la replica del volume, è necessario eseguire alcune fasi di preparazione presso il sito di disaster recovery.

- Un account NetApp deve essere disponibile e configurato con lo stesso abbonamento Azure dell'origine.
- Un pool di capacità deve essere disponibile e configurato utilizzando l'account NetApp indicato sopra.
- Una rete virtuale deve essere disponibile e configurata.
- All'interno della rete virtuale, una subnet delegata deve essere disponibile e configurata per l'utilizzo con

ANF.

È ora possibile creare volumi di protezione per i dati HANA, HANA shared e HANA log backup volume. La seguente tabella mostra i volumi di destinazione configurati nella nostra configurazione di laboratorio.

> Per ottenere la migliore latenza, i volumi devono essere posizionati vicino alle macchine virtuali che eseguono SAP HANA in caso di disaster failover. Pertanto, per i volumi DR è necessario lo stesso processo di pinning di qualsiasi altro sistema di produzione SAP HANA.

Volume HANA	Origine	Destinazione	Pianificazione della replica
Volume di dati HANA	PR1-data-mnt00001	PR1-data-mnt00001-sm-dest	Ogni giorno
Volume condiviso HANA	PR1-shared	PR1-shared-SM-dest	Ogni ora
Volume di backup di log/catalogo HANA	hanabackup	hanabackup-sm-dest	Ogni ora

Per ciascun volume, è necessario eseguire le seguenti operazioni:

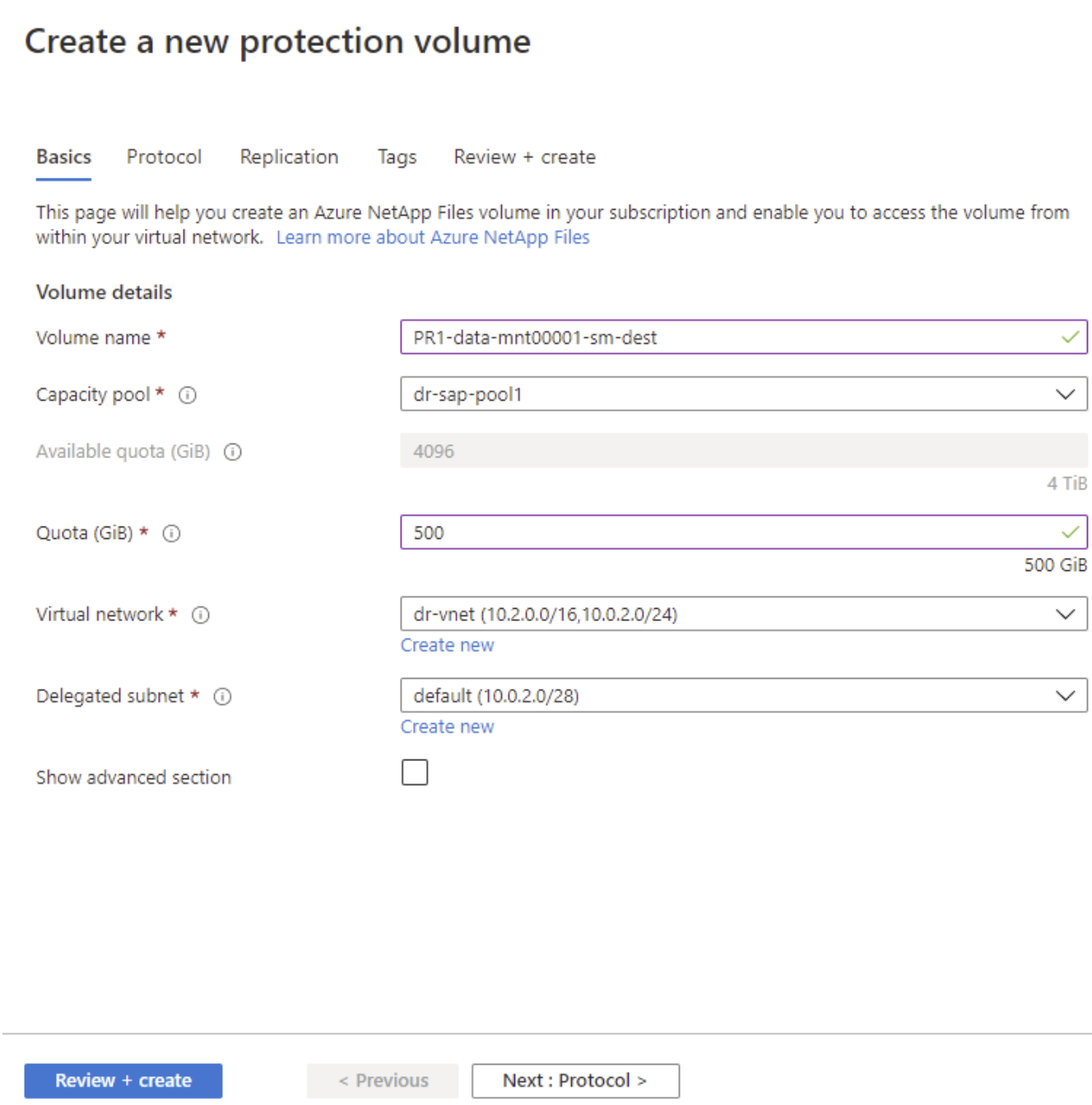
1. Creare un nuovo volume di protezione nel sito DR:
   a. Fornire il nome del volume, il pool di capacità, la quota e le informazioni di rete.
   b. Fornire le informazioni relative al protocollo e all'accesso al volume.
   c. Fornire l'ID del volume di origine e una pianificazione di replica.
   d. Creare un volume di destinazione.
2. Autorizzare la replica nel volume di origine.
   - Fornire l'ID del volume di destinazione.

Le seguenti schermate mostrano in dettaglio i passaggi di configurazione.

Nel sito di disaster recovery, viene creato un nuovo volume di protezione selezionando i volumi e facendo clic su Add Data Replication (Aggiungi replica dati). Nella scheda Nozioni di base, è necessario fornire il nome del volume, il pool di capacità e le informazioni di rete.

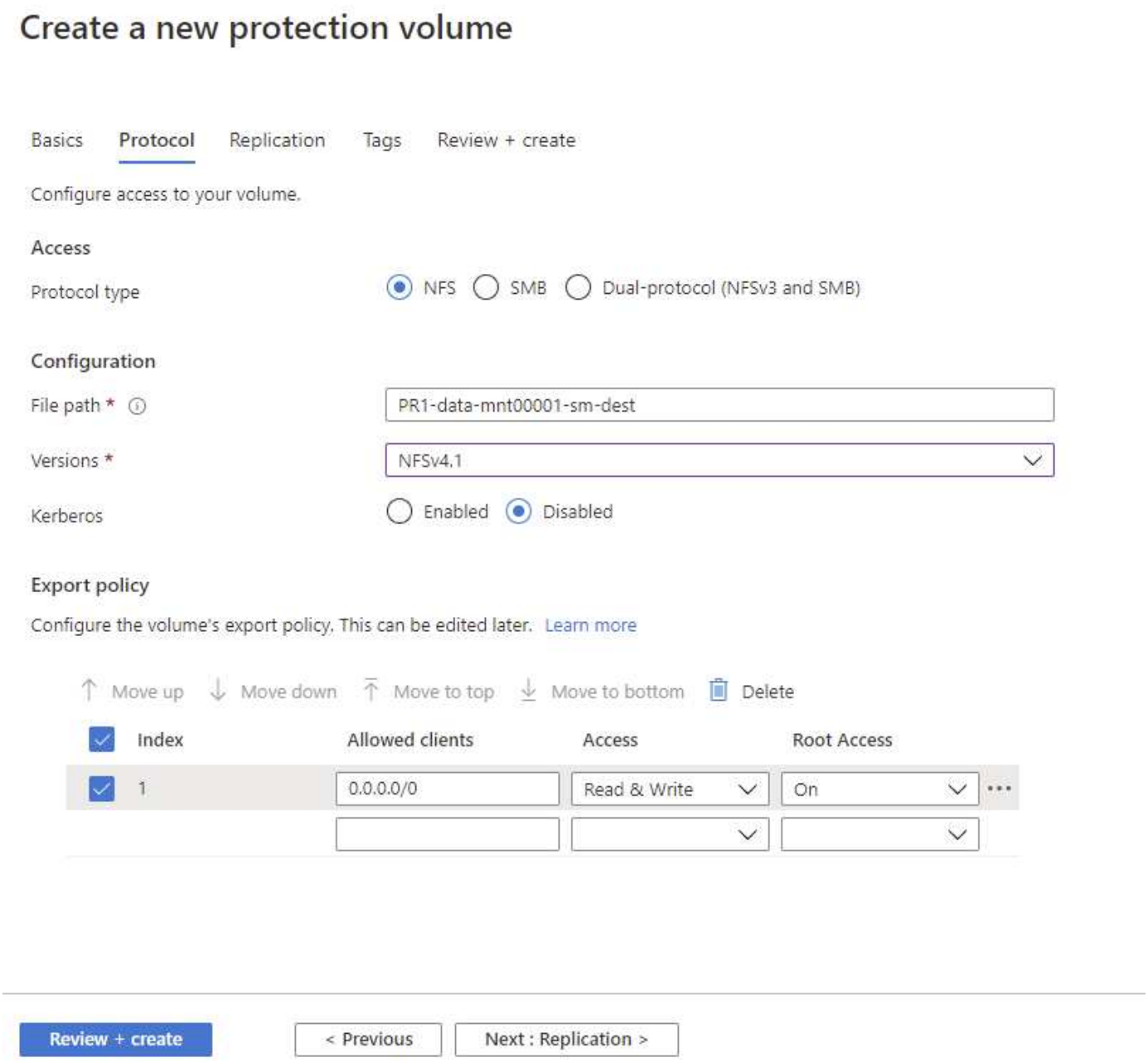
> La quota del volume può essere impostata in base ai requisiti di capacità, poiché le prestazioni del volume non influiscono sul processo di replica. In caso di failover del disaster recovery, la quota deve essere regolata per soddisfare i requisiti di performance reali.

> Se il pool di capacità è stato configurato con QoS manuale, è possibile configurare il throughput in aggiunta ai requisiti di capacità. Come sopra, è possibile configurare il throughput con un valore basso durante il normale funzionamento e aumentarlo in caso di failover del disaster recovery.



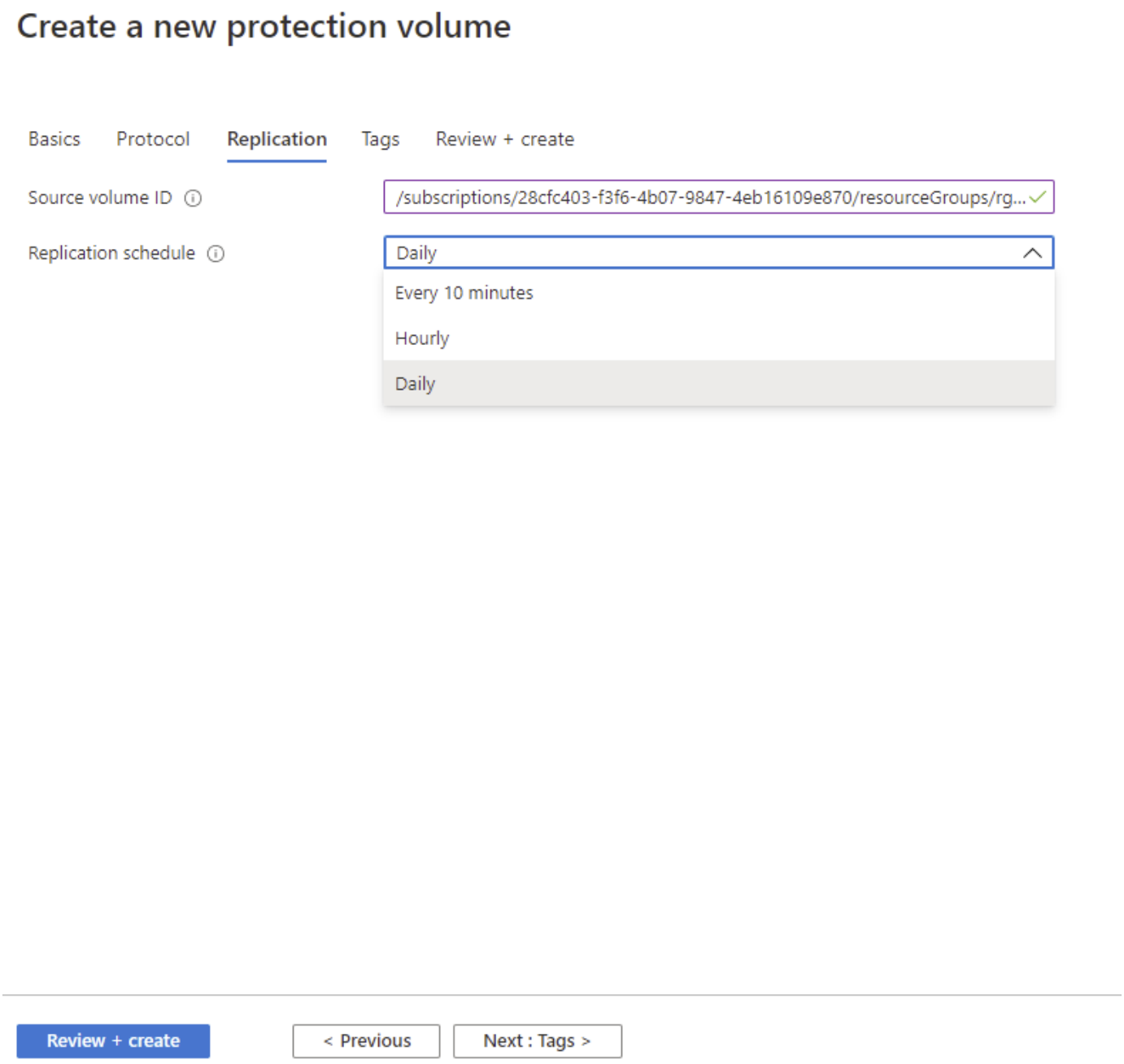
Nella scheda Protocol (protocollo), specificare il protocollo di rete, il percorso di rete e il criterio di esportazione.

Il protocollo deve essere lo stesso utilizzato per il volume di origine.



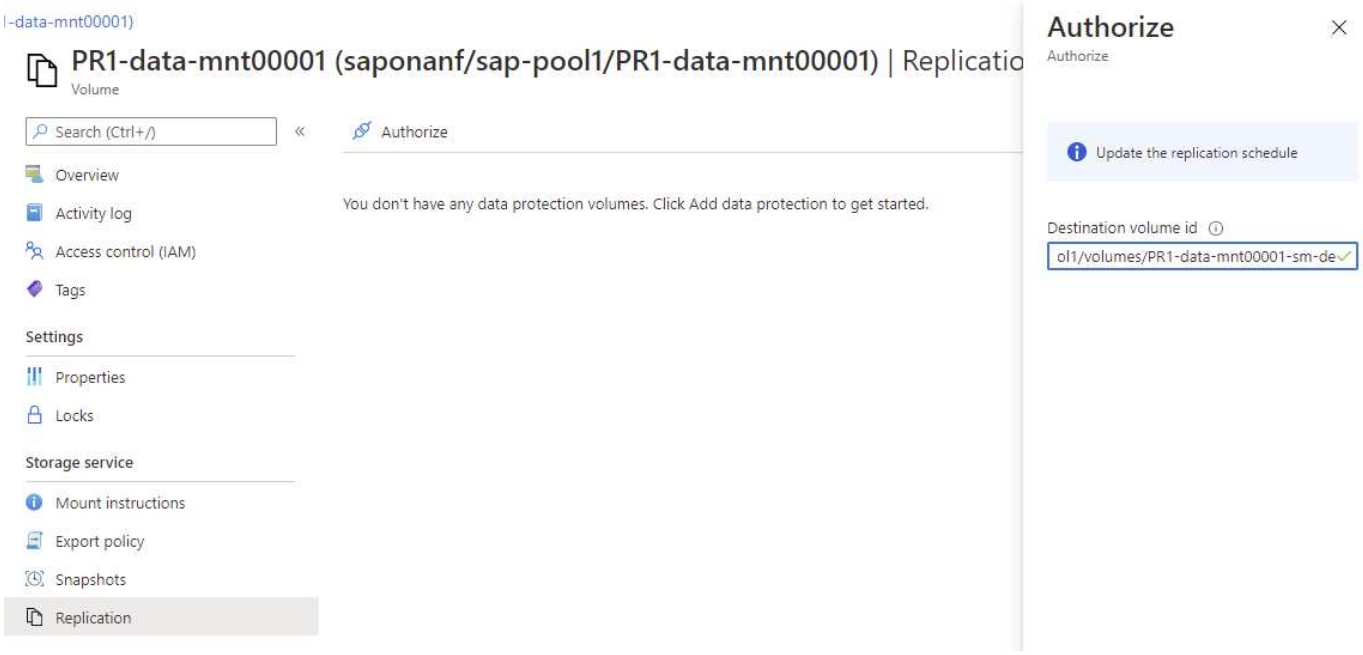
Nella scheda Replication (Replica), è necessario configurare l'ID del volume di origine e la pianificazione della replica. Per la replica dei volumi di dati, abbiamo configurato una pianificazione di replica giornaliera per la nostra configurazione di laboratorio.

L'ID del volume di origine può essere copiato dalla schermata Proprietà del volume di origine.



Come fase finale, è necessario autorizzare la replica nel volume di origine fornendo l'ID del volume di destinazione.

È possibile copiare l'ID del volume di destinazione dalla schermata Proprietà del volume di destinazione.



È necessario eseguire le stesse operazioni per il volume condiviso HANA e per il volume di backup del registro.

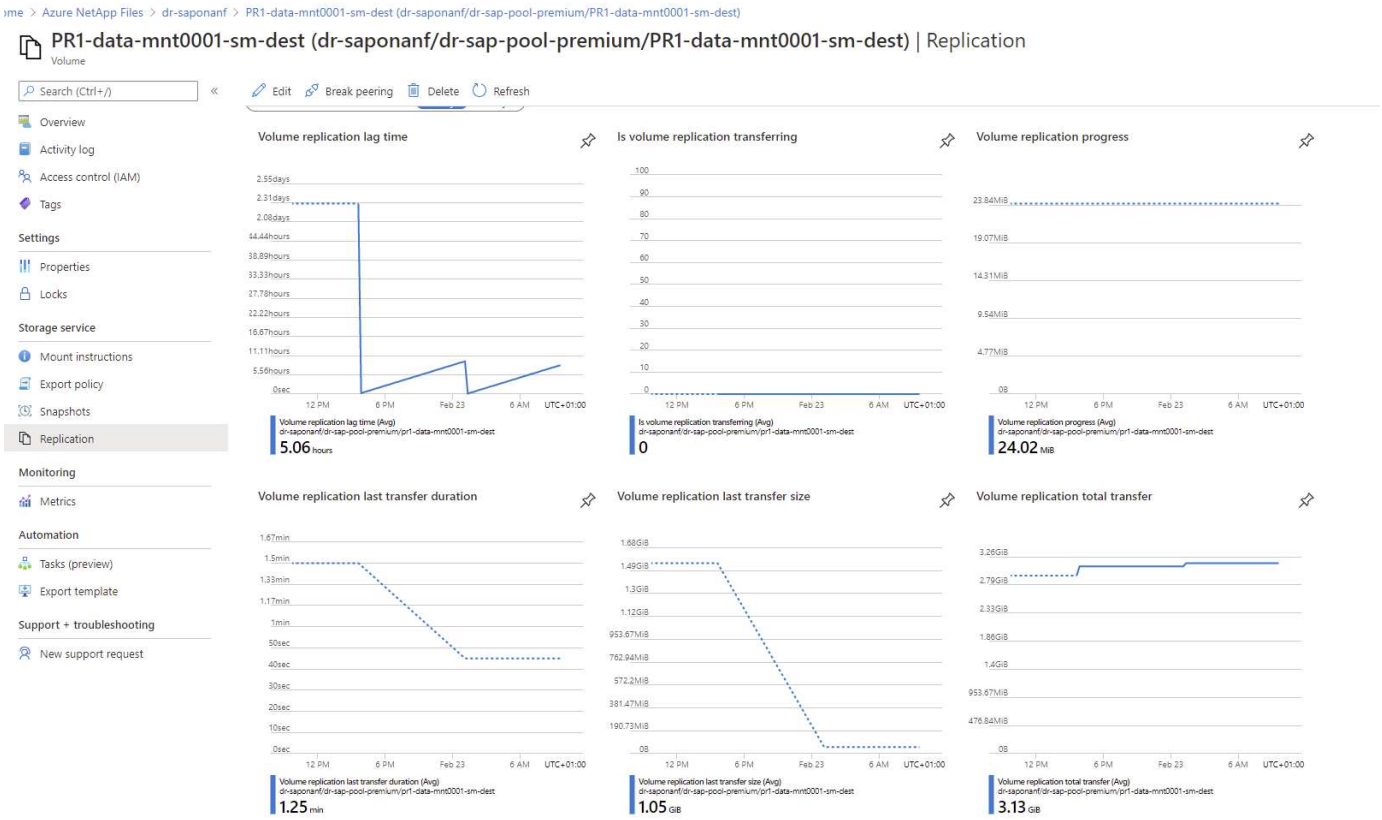
Monitoraggio della replica ANF tra regioni

Le tre schermate seguenti mostrano lo stato della replica per i dati, il backup del log e i volumi condivisi.

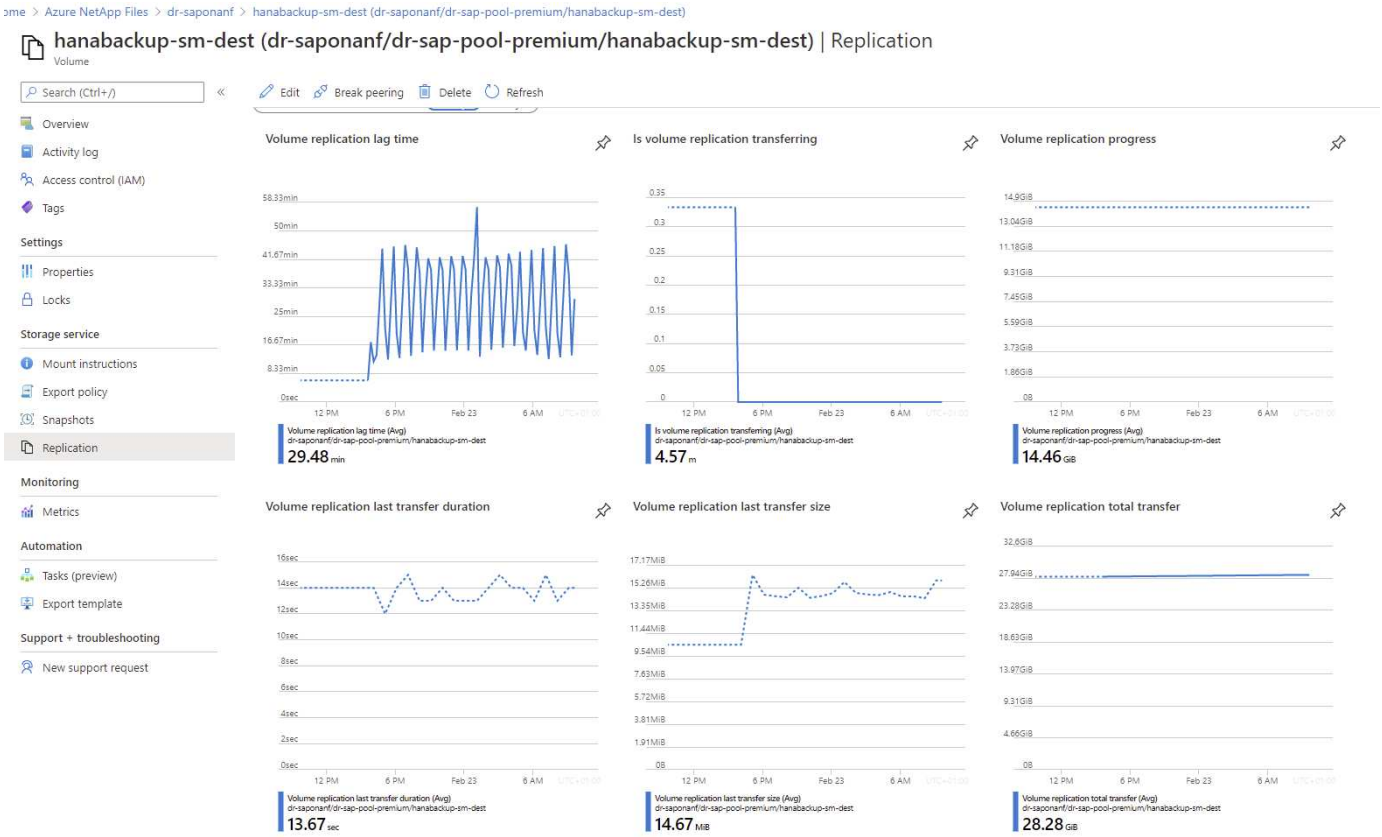
Il ritardo della replica del volume è un valore utile per comprendere le aspettative RPO. Ad esempio, la replica del volume di backup del registro mostra un ritardo massimo di 58 minuti, il che significa che l'RPO massimo ha lo stesso valore.

La durata del trasferimento e le dimensioni del trasferimento forniscono informazioni preziose sui requisiti di larghezza di banda e modificano la velocità del volume replicato.

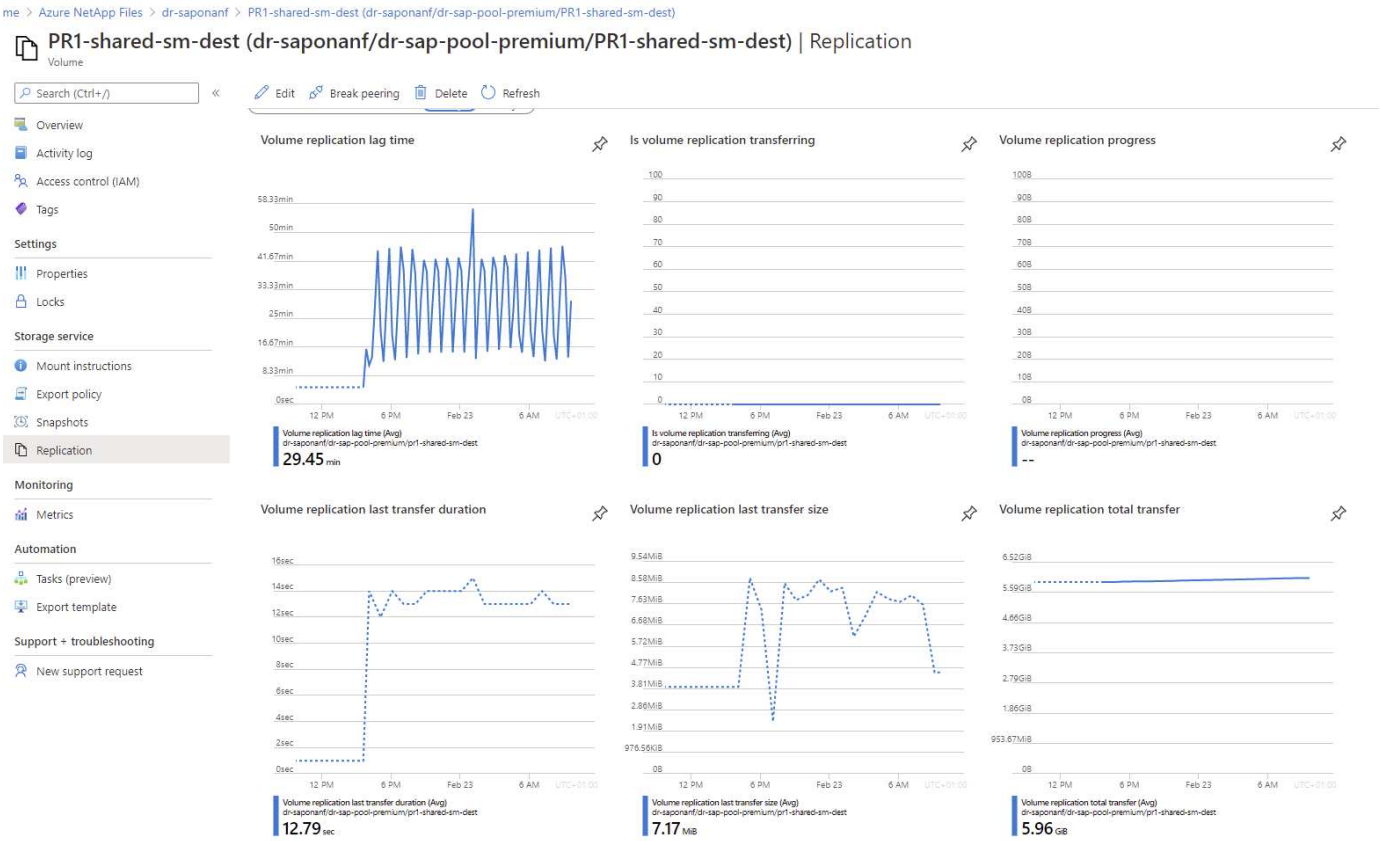
La seguente schermata mostra lo stato di replica del volume di dati HANA.



La seguente schermata mostra lo stato di replica del volume di backup del registro HANA.



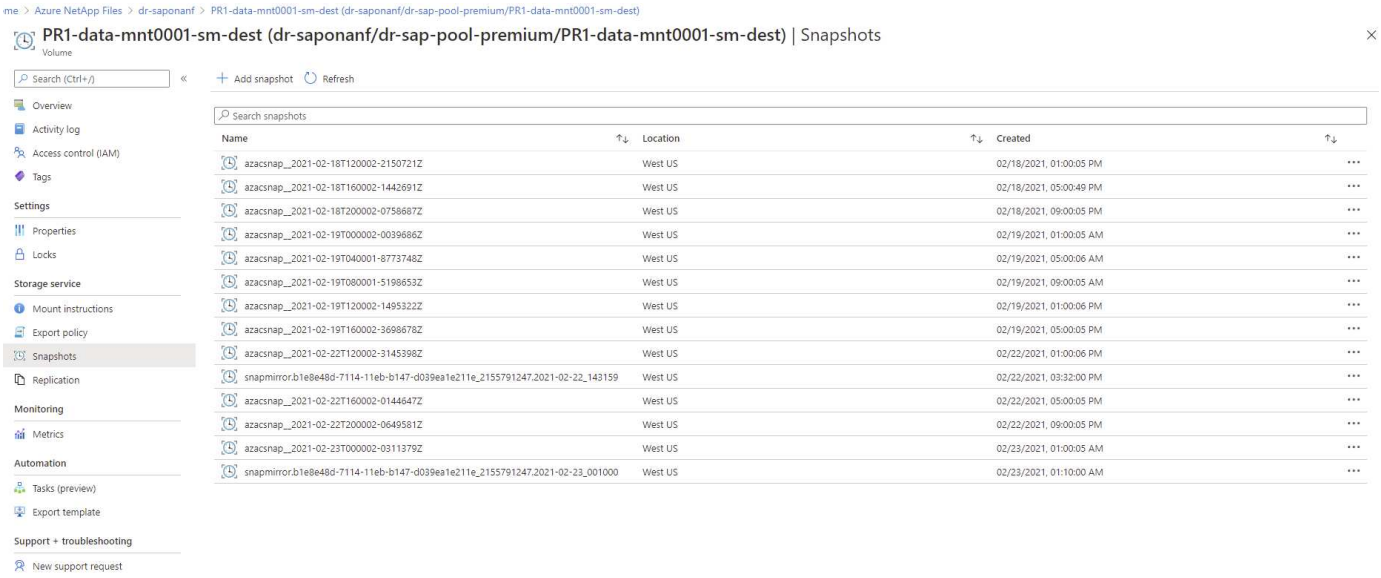
La seguente schermata mostra lo stato di replica del volume condiviso HANA.



Backup snapshot replicati

Ogni volta che si aggiorna la replica dal volume di origine al volume di destinazione, tutte le modifiche apportate al blocco tra l'ultimo e l'aggiornamento corrente vengono replicate nel volume di destinazione. Sono incluse anche le snapshot create nel volume di origine. La seguente schermata mostra le snapshot disponibili nel volume di destinazione. Come già discusso, ciascuna snapshot creata dallo strumento AzAcSnap è un'immagine coerente con l'applicazione del database HANA che può essere utilizzata per eseguire un Savepoint o un forward recovery.

All'interno del volume di origine e di destinazione, vengono create anche le copie Snapshot di SnapMirror, utilizzate per le operazioni di risincronizzazione e aggiornamento della replica. Queste copie Snapshot non sono coerenti con l'applicazione dal punto di vista del database HANA; solo le snapshot coerenti con l'applicazione create tramite AzaCSnap possono essere utilizzate per le operazioni di ripristino HANA.



Test di disaster recovery

Test di disaster recovery

Per implementare una strategia di disaster recovery efficace, è necessario testare il flusso di lavoro richiesto. I test dimostrano se la strategia funziona e se la documentazione interna è sufficiente e consentono agli amministratori di seguire le procedure richieste.

ANF la replica interregionale consente di eseguire test di disaster recovery senza mettere a rischio RTO e RPO. I test di disaster recovery possono essere eseguiti senza interrompere la replica dei dati.

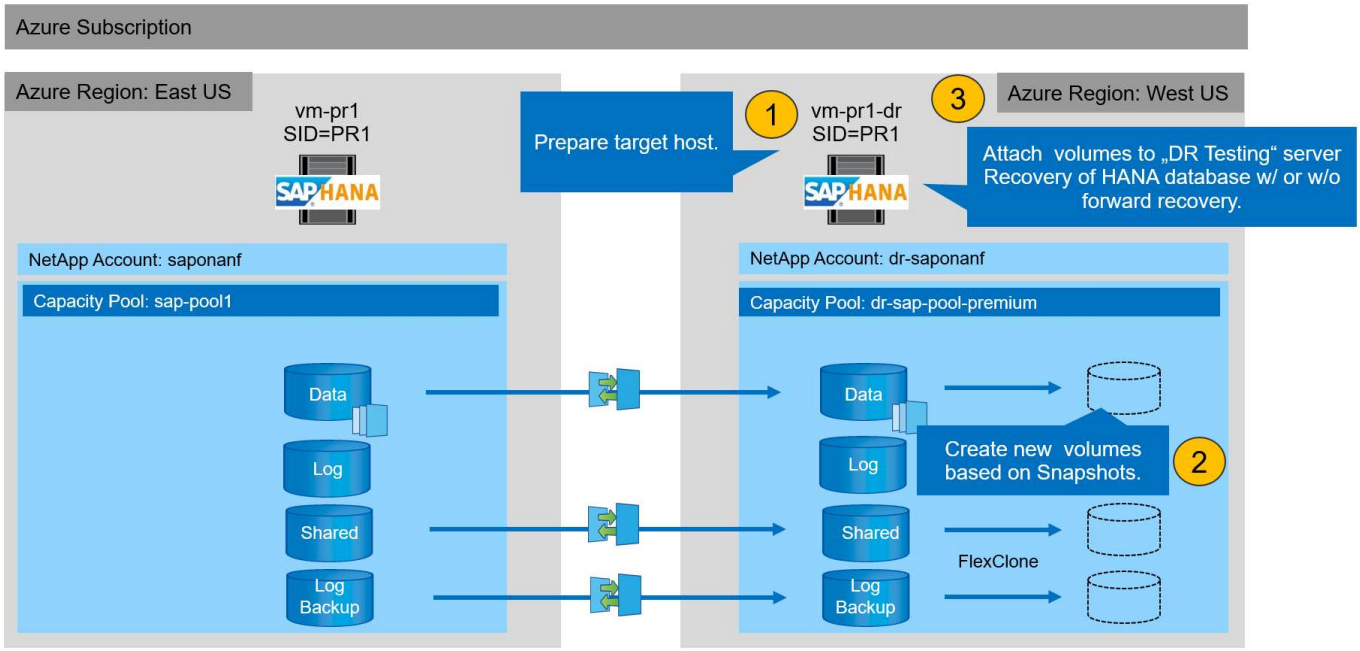
Il workflow di test del disaster recovery sfrutta il set di funzionalità ANF per creare nuovi volumi in base ai backup Snapshot esistenti nella destinazione del disaster recovery. Vedere "Funzionamento delle istantanee di Azure NetApp Files | documenti Microsoft".

A seconda che la replica del backup dei log faccia parte o meno della configurazione del disaster recovery, le fasi del disaster recovery sono leggermente diverse. In questa sezione vengono descritti i test di disaster recovery per la replica solo backup dei dati e per la replica del volume dei dati combinata con la replica del volume di backup del registro.

Per eseguire il test di disaster recovery, attenersi alla seguente procedura:

1. Preparare l'host di destinazione.
2. Creare nuovi volumi in base ai backup Snapshot nel sito di disaster recovery.
3. Montare i nuovi volumi sull'host di destinazione.
4. Ripristinare il database HANA.
    - Solo ripristino del volume di dati.
    - Eseguire il ripristino in avanti utilizzando backup di log replicati.

Le seguenti sottosezioni descrivono in dettaglio questi passaggi.



Preparare l’host di destinazione

In questa sezione vengono descritte le fasi di preparazione necessarie per il server utilizzato per il failover del disaster recovery.

Durante il normale funzionamento, l’host di destinazione viene generalmente utilizzato per altri scopi, ad esempio come sistema di test o QA HANA. Pertanto, la maggior parte dei passaggi descritti deve essere eseguita quando viene eseguito il test di failover di emergenza. D’altra parte, i file di configurazione pertinenti, come `/etc/fstab` e. `/usr/sap/sapservices`, può essere preparato e quindi messo in produzione semplicemente copiando il file di configurazione. La procedura di failover del disaster recovery garantisce che i file di configurazione preparati siano configurati correttamente.

La preparazione dell’host di destinazione include anche lo spegnimento del sistema di test o QA HANA e l’interruzione di tutti i servizi utilizzati `systemctl stop sapinit`.

Nome host e indirizzo IP del server di destinazione

Il nome host del server di destinazione deve essere identico al nome host del sistema di origine. L’indirizzo IP può essere diverso.

È necessario stabilire un corretto scherma del server di destinazione in modo che non possa comunicare con altri sistemi. Se non è disponibile un corretto scherma, il sistema di produzione clonato potrebbe scambiare dati con altri sistemi di produzione, causando la corruzione logica dei dati.

Installare il software richiesto

Il software dell’agente host SAP deve essere installato sul server di destinazione. Per informazioni complete, consultare "Agente host SAP" Nel portale di assistenza SAP.

Se l’host viene utilizzato come sistema di test o QA HANA, il software dell’agente host SAP è già installato.

Configurare utenti, porte e servizi SAP

Gli utenti e i gruppi richiesti per il database SAP HANA devono essere disponibili sul server di destinazione. In genere, viene utilizzata la gestione centrale degli utenti, pertanto non sono necessarie operazioni di configurazione sul server di destinazione. Le porte richieste per il database HANA devono essere configurate sugli host di destinazione. È possibile copiare la configurazione dal sistema di origine copiando `/etc/services` sul server di destinazione.

Le voci dei servizi SAP richieste devono essere disponibili sull'host di destinazione. È possibile copiare la configurazione dal sistema di origine copiando `/usr/sap/sapservices` sul server di destinazione. Il seguente output mostra le voci richieste per il database SAP HANA utilizzato nella configurazione di laboratorio.

```
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
```

Preparare il volume di log HANA

Poiché il volume di log HANA non fa parte della replica, è necessario che nell'host di destinazione esista un volume di log vuoto. Il volume di log deve includere le stesse sottodirectory del sistema HANA di origine.

```
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:~ #
```

Preparare il volume di backup del log

Poiché il sistema di origine è configurato con un volume separato per i backup del registro HANA, un volume di backup del registro deve essere disponibile anche sull'host di destinazione. Un volume per i backup del log deve essere configurato e montato sull'host di destinazione.

Se la replica del volume di backup del registro fa parte della configurazione del disaster recovery, il volume di backup del registro replicato viene montato sull'host di destinazione e non è necessario preparare un volume di backup del registro aggiuntivo.

Preparare i montaggi del file system

La seguente tabella mostra le convenzioni di denominazione utilizzate nella configurazione di laboratorio. I nomi dei volumi nel sito di disaster recovery sono inclusi in `/etc/fstab`.

Volumi HANA PR1	Volume e sottodirectory nel sito di disaster recovery	Punto di montaggio sull'host di destinazione
Volume di dati	PR1-data-mnt00001-sm-dest	/hana/data/PR1/mnt00001
Volume condiviso	PR1-shared-sm-dest/shared PR1-shared-sm-dest/usr-sap-PR1	/hana/shared /usr/sap/PR1
Volume di backup del registro	hanabackup-sm-dest	/hanabackup

I punti di montaggio di questa tabella devono essere creati sull'host di destinazione.

Ecco i requisiti `/etc/fstab` voci.

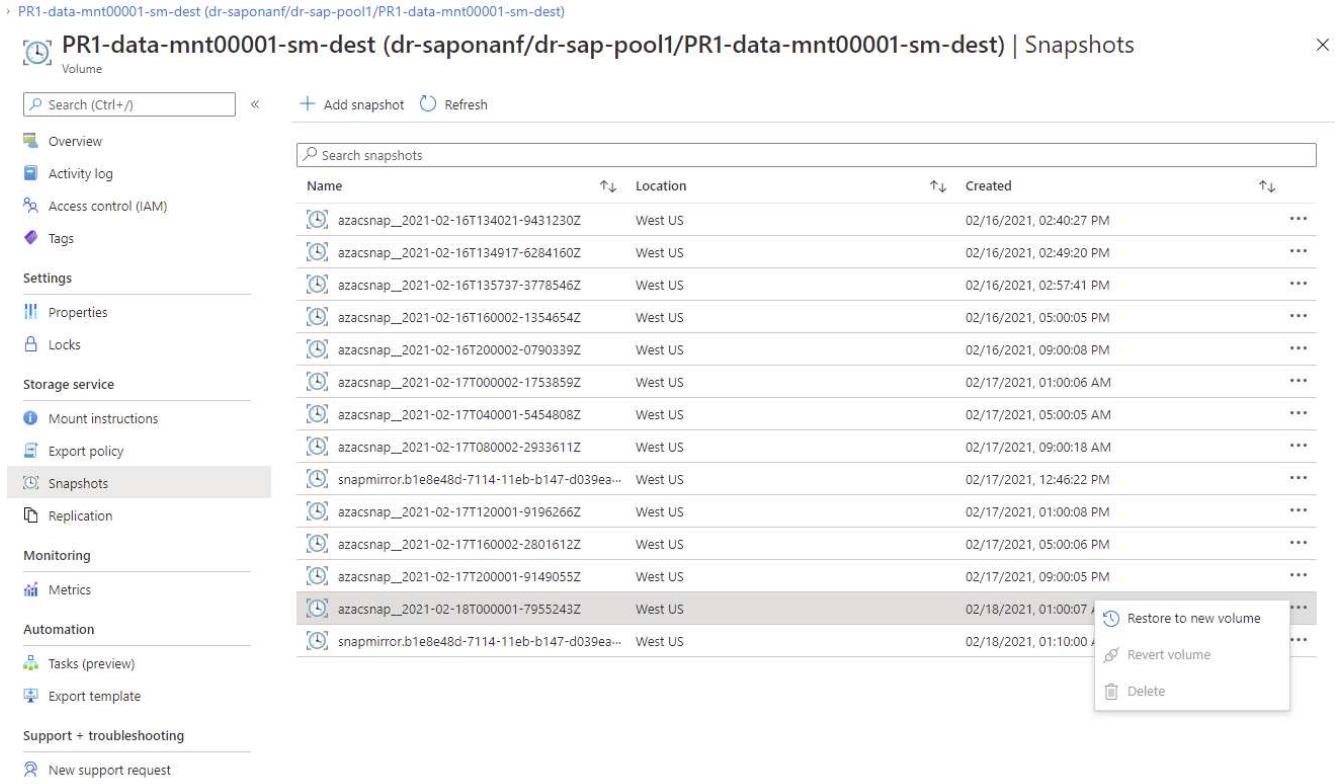
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
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
```

Creare nuovi volumi in base ai backup snapshot nel sito di disaster recovery

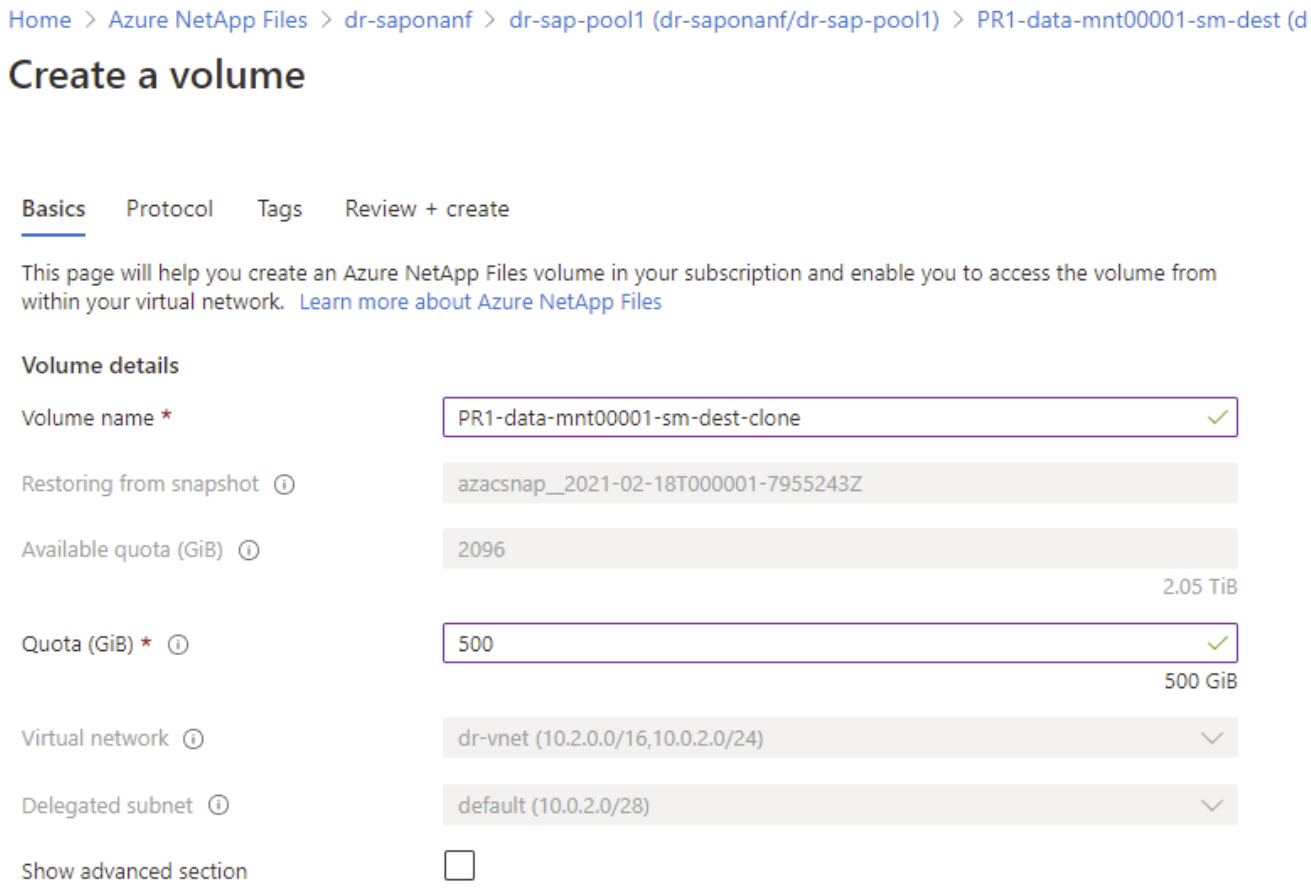
A seconda della configurazione del disaster recovery (con o senza replica del backup del log), è necessario creare due o tre nuovi volumi basati sui backup snapshot. In entrambi i casi, è necessario creare un nuovo volume dei dati e il volume condiviso HANA.

Se vengono replicati anche i dati di backup del registro, è necessario creare un nuovo volume del volume di backup del registro. Nel nostro esempio, i dati e il volume di backup del log sono stati replicati nel sito di disaster recovery. La procedura seguente utilizza Azure Portal.

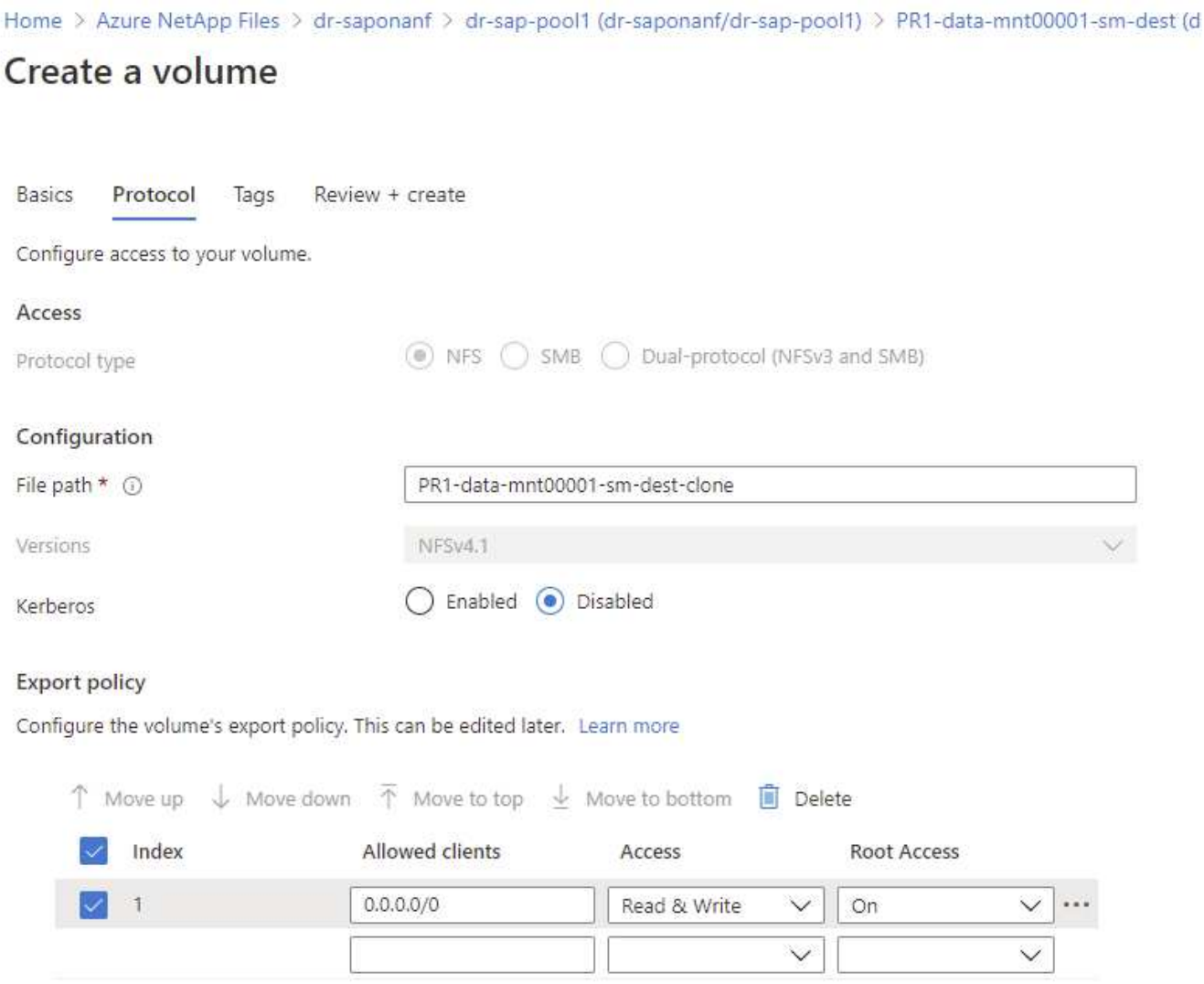
1. Uno dei backup snapshot coerenti con l'applicazione viene selezionato come origine per il nuovo volume del volume di dati HANA. L'opzione Restore to New Volume (Ripristina su nuovo volume) è selezionata per creare un nuovo volume in base al backup dello snapshot.



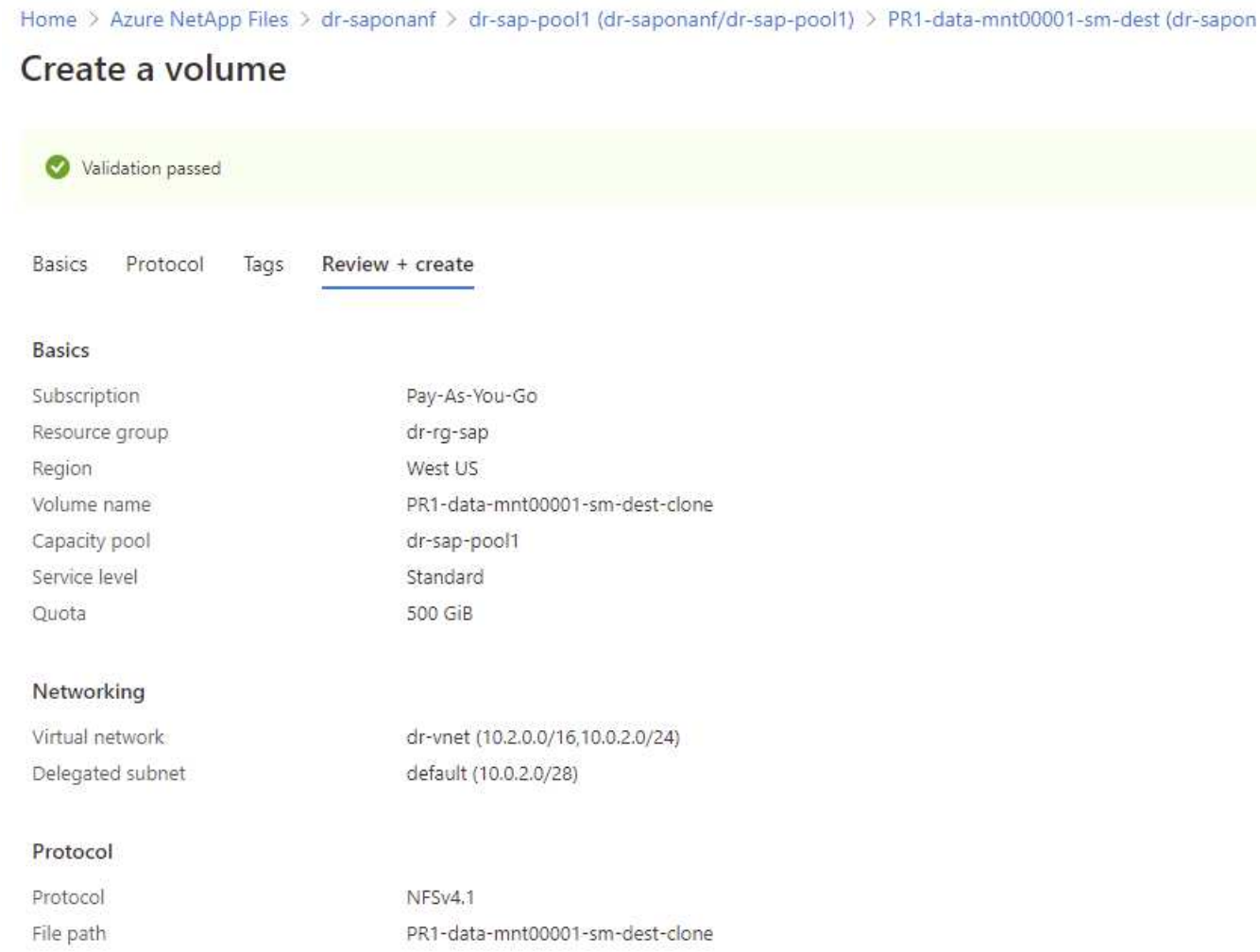
2. Il nuovo nome del volume e la nuova quota devono essere forniti nell'interfaccia utente.



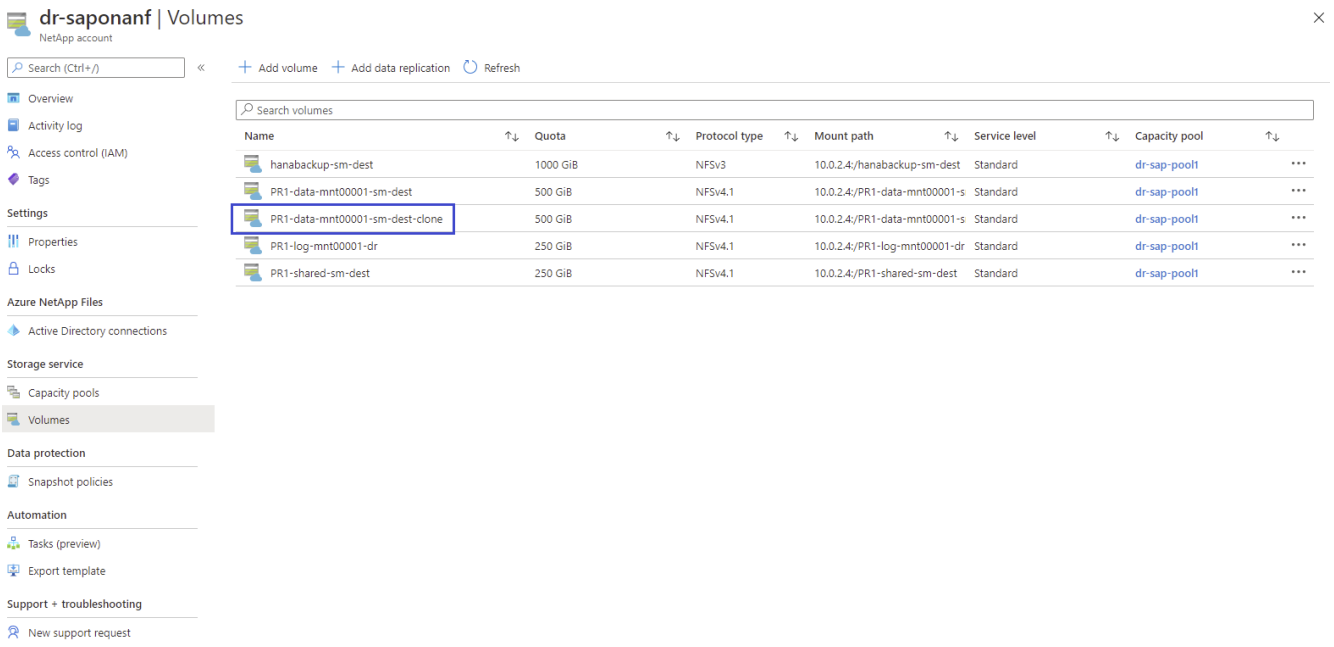
3. Nella scheda Protocol (protocollo), vengono configurati il percorso del file e la policy di esportazione.



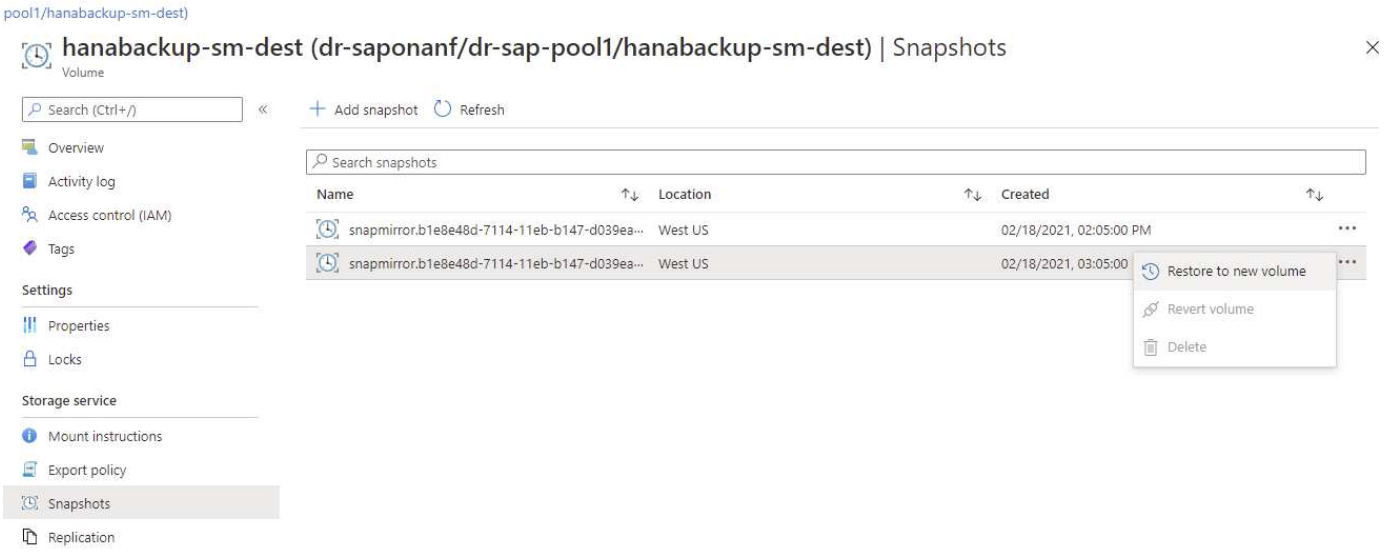
4. La schermata Create and Review (Crea e rivedi) riassume la configurazione.



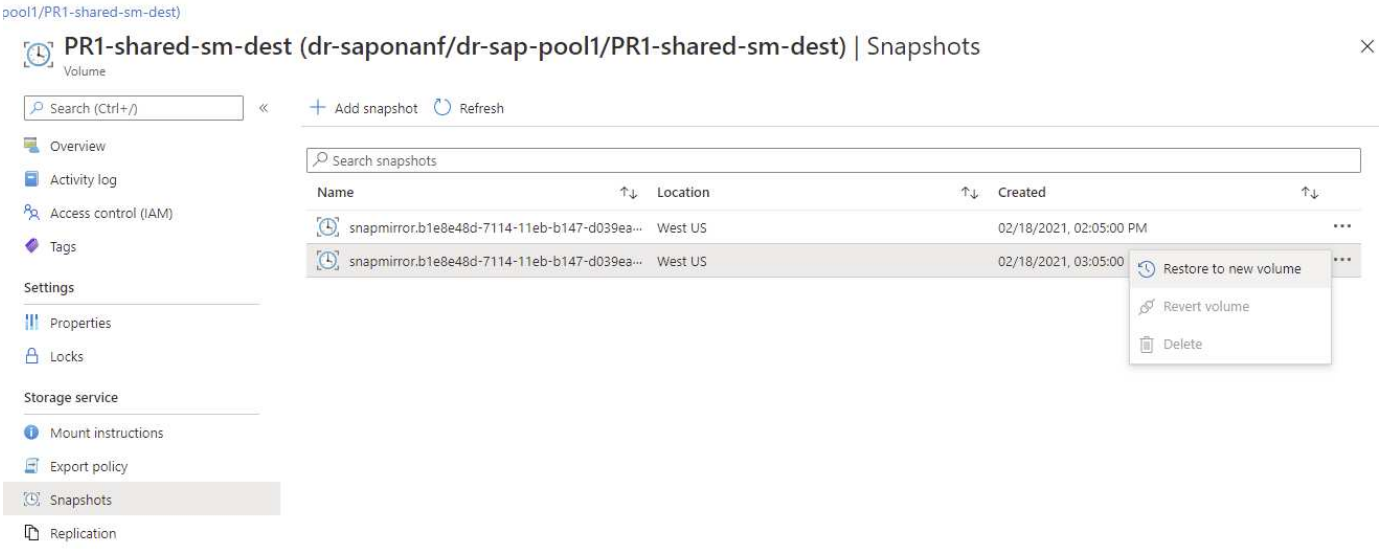
5. È stato creato un nuovo volume in base al backup di snapshot HANA.



A questo punto, è necessario eseguire le stesse operazioni per il volume condiviso HANA e per il volume di backup del registro, come illustrato nelle due schermate seguenti. Poiché non sono stati creati snapshot aggiuntivi per il volume di backup del registro e condiviso HANA, la copia Snapshot SnapMirror più recente deve essere selezionata come origine per il nuovo volume. Si tratta di dati non strutturati e per questo caso di utilizzo è possibile utilizzare la copia Snapshot di SnapMirror.



La seguente schermata mostra il volume condiviso HANA ripristinato nel nuovo volume.



Se è stato utilizzato un pool di capacità con un livello di performance basso, i volumi devono ora essere spostati in un pool di capacità che fornisca le performance richieste.

Tutti e tre i nuovi volumi sono ora disponibili e possono essere montati sull'host di destinazione.

Montare i nuovi volumi sull'host di destinazione

I nuovi volumi possono ora essere montati sull'host di destinazione, in base a. `/etc/fstab` file creato in precedenza.

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

Il seguente output mostra i file system richiesti.

```
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
```

Ripristino del database HANA

Di seguito vengono illustrati i passaggi per il ripristino del database HANA

Avviare i servizi SAP richiesti.

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

Il seguente output mostra i processi richiesti.

```
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
```

Le seguenti sottosezioni descrivono il processo di ripristino con e senza il ripristino in avanti utilizzando i backup del registro replicati. Il ripristino viene eseguito utilizzando lo script di ripristino HANA per il database di sistema e i comandi hdbsql per il database tenant.

Ripristino dell'ultimo Savepoint di backup del volume di dati HANA

Il ripristino all'ultimo punto di salvataggio del backup viene eseguito con i seguenti comandi come utente pr1adm:

- Database di sistema

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

- Database tenant

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

È inoltre possibile utilizzare HANA Studio o Cockpit per eseguire il ripristino del sistema e del database tenant.

L'output del seguente comando mostra l'esecuzione del ripristino.

Recovery del database di sistema

```
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 del database tenant

Se non è stata creata una chiave di memorizzazione utente per l'utente pr1adm nel sistema di origine, è necessario creare una chiave nel sistema di destinazione. L'utente del database configurato nella chiave deve disporre dei privilegi necessari per eseguire le operazioni di ripristino del tenant.

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

Il ripristino del tenant viene ora eseguito con hdbsql.

```
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=>
```

Il database HANA è ora operativo e il workflow di disaster recovery per il database HANA è stato testato.

Recovery con forward recovery utilizzando backup di log/catalogo

I backup dei log e il catalogo di backup HANA vengono replicati dal sistema di origine.

Il ripristino utilizzando tutti i backup dei log disponibili viene eseguito con i seguenti comandi come utente pr1adm:

- Database di sistema

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

- Database tenant

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

Per eseguire il ripristino utilizzando tutti i registri disponibili, è possibile utilizzare in qualsiasi momento in futuro come data e ora nell'istruzione Recovery.

È inoltre possibile utilizzare HANA Studio o Cockpit per eseguire il ripristino del sistema e del database tenant.

L'output del seguente comando mostra l'esecuzione del ripristino.

Recovery del database di sistema

```
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 del database tenant

```
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=>
```

Il database HANA è ora operativo e il workflow di disaster recovery per il database HANA è stato testato.

Verificare la coerenza dei backup dei log più recenti

Poiché la replica del volume di backup del log viene eseguita indipendentemente dal processo di backup del log eseguito dal database SAP HANA, potrebbero esserci file di backup del log aperti e incoerenti nel sito di disaster recovery. Solo i file di backup dei log più recenti potrebbero essere incoerenti e tali file devono essere controllati prima di eseguire un ripristino in avanti nel sito di disaster recovery utilizzando `hdbbackupcheck` tool.

Se il `hdbbackupcheck` lo strumento segnala un errore per i backup dei log più recenti; è necessario rimuovere o eliminare l'ultimo set di backup dei log.

```
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.
```

La verifica deve essere eseguita per i file di backup dei log più recenti del sistema e del database del tenant.

Se il `hdbbackupcheck` lo strumento segnala un errore per i backup dei log più recenti; è necessario rimuovere o eliminare l'ultimo set di backup dei log.

Failover del disaster recovery

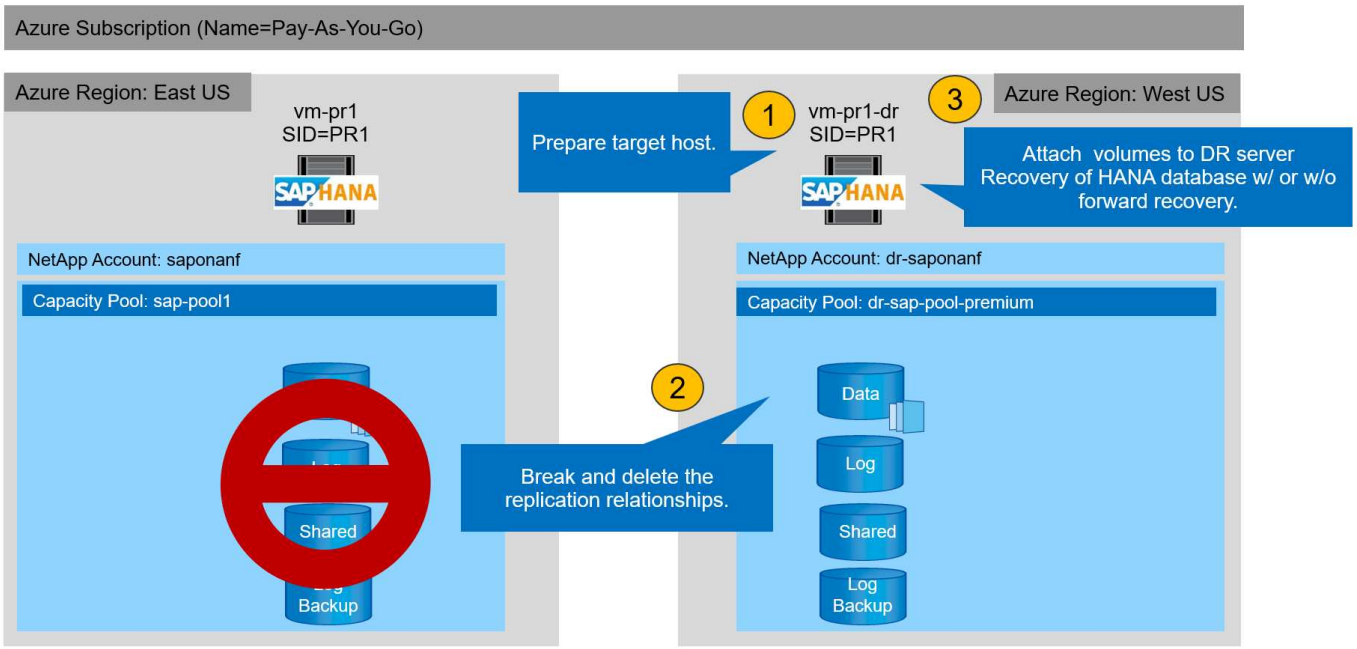
Failover del disaster recovery

A seconda che la replica del backup del registro faccia parte della configurazione del disaster recovery, le fasi del disaster recovery sono leggermente diverse. In questa sezione viene descritto il failover del disaster recovery per la replica solo backup dei dati e per la replica del volume dei dati combinata con la replica del volume di backup del registro.

Per eseguire il failover del disaster recovery, attenersi alla seguente procedura:

1. Preparare l'host di destinazione.
2. Interrompere ed eliminare le relazioni di replica.
3. Ripristinare il volume di dati al backup snapshot coerente con l'applicazione più recente.
4. Montare i volumi sull'host di destinazione.
5. Ripristinare il database HANA.
    - Solo ripristino del volume di dati.
    - Eseguire il ripristino in avanti utilizzando backup di log replicati.

Le seguenti sottosezioni descrivono in dettaglio questi passaggi e la seguente figura illustra il test di disaster failover.



Preparare l'host di destinazione

In questa sezione vengono descritte le fasi di preparazione necessarie per il server utilizzato per il failover del disaster recovery.

Durante il normale funzionamento, l'host di destinazione viene generalmente utilizzato per altri scopi, ad esempio come sistema di test o QA HANA. Pertanto, la maggior parte dei passaggi descritti deve essere eseguita quando viene eseguito il test di failover di emergenza. D'altra parte, i file di configurazione pertinenti, come `/etc/fstab` e. `/usr/sap/sapservices`, può essere preparato e quindi messo in produzione semplicemente copiando il file di configurazione. La procedura di failover del disaster recovery garantisce che i file di configurazione preparati siano configurati correttamente.

La preparazione dell'host di destinazione include anche lo spegnimento del sistema di test o QA HANA e l'interruzione di tutti i servizi utilizzati `systemctl stop sapinit`.

Nome host e indirizzo IP del server di destinazione

Il nome host del server di destinazione deve essere identico al nome host del sistema di origine. L'indirizzo IP può essere diverso.

È necessario stabilire un corretto scherma del server di destinazione in modo che non possa comunicare con altri sistemi. Se non è disponibile un corretto scherma, il sistema di produzione clonato potrebbe scambiare dati con altri sistemi di produzione, causando la corruzione logica dei dati.

Installare il software richiesto

Il software dell'agente host SAP deve essere installato sul server di destinazione. Per informazioni complete, consultare "Agente host SAP" Nel portale di assistenza SAP.

Se l'host viene utilizzato come sistema di test o QA HANA, il software dell'agente host SAP è già installato.

Configurare utenti, porte e servizi SAP

Gli utenti e i gruppi richiesti per il database SAP HANA devono essere disponibili sul server di destinazione. In genere, viene utilizzata la gestione centrale degli utenti, pertanto non sono necessarie operazioni di configurazione sul server di destinazione. Le porte richieste per il database HANA devono essere configurate sugli host di destinazione. È possibile copiare la configurazione dal sistema di origine copiando `/etc/services` sul server di destinazione.

Le voci dei servizi SAP richieste devono essere disponibili sull'host di destinazione. È possibile copiare la configurazione dal sistema di origine copiando `/usr/sap/sapservices` sul server di destinazione. Il seguente output mostra le voci richieste per il database SAP HANA utilizzato nella configurazione di laboratorio.

```
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
```

Preparare il volume di log HANA

Poiché il volume di log HANA non fa parte della replica, è necessario che nell'host di destinazione esista un volume di log vuoto. Il volume di log deve includere le stesse sottodirectory del sistema HANA di origine.

```
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:~ #
```

Preparare il volume di backup del log

Poiché il sistema di origine è configurato con un volume separato per i backup del registro HANA, un volume di backup del registro deve essere disponibile anche sull'host di destinazione. Un volume per i backup del log deve essere configurato e montato sull'host di destinazione.

Se la replica del volume di backup del registro fa parte della configurazione del disaster recovery, il volume di backup del registro replicato viene montato sull'host di destinazione e non è necessario preparare un volume di backup del registro aggiuntivo.

Preparare i montaggi del file system

La seguente tabella mostra le convenzioni di denominazione utilizzate nella configurazione di laboratorio. I nomi dei volumi nel sito di disaster recovery sono inclusi in `/etc/fstab`.

Volumi HANA PR1	Volume e sottodirectory nel sito di disaster recovery	Punto di montaggio sull'host di destinazione
Volume di dati	PR1-data-mnt00001-sm-dest	/hana/data/PR1/mnt00001
Volume condiviso	PR1-shared-sm-dest/shared PR1-shared-sm-dest/usr-sap-PR1	/hana/shared /usr/sap/PR1
Volume di backup del registro	hanabackup-sm-dest	/hanabackup

I punti di montaggio di questa tabella devono essere creati sull'host di destinazione.

Ecco i requisiti `/etc/fstab` voci.

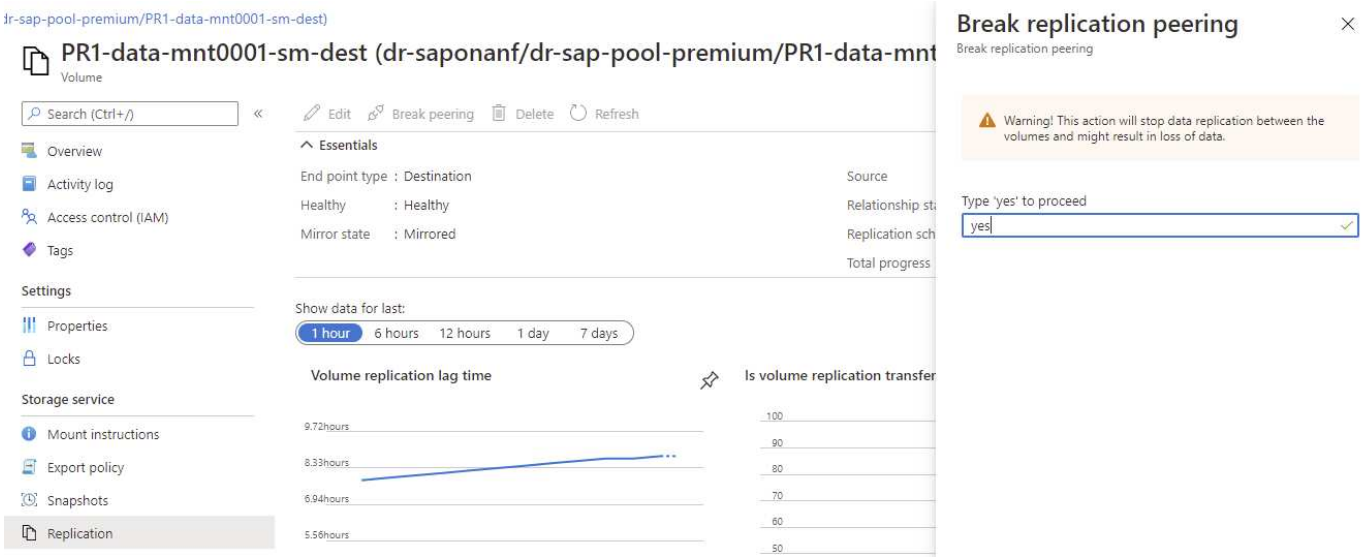
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
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
```

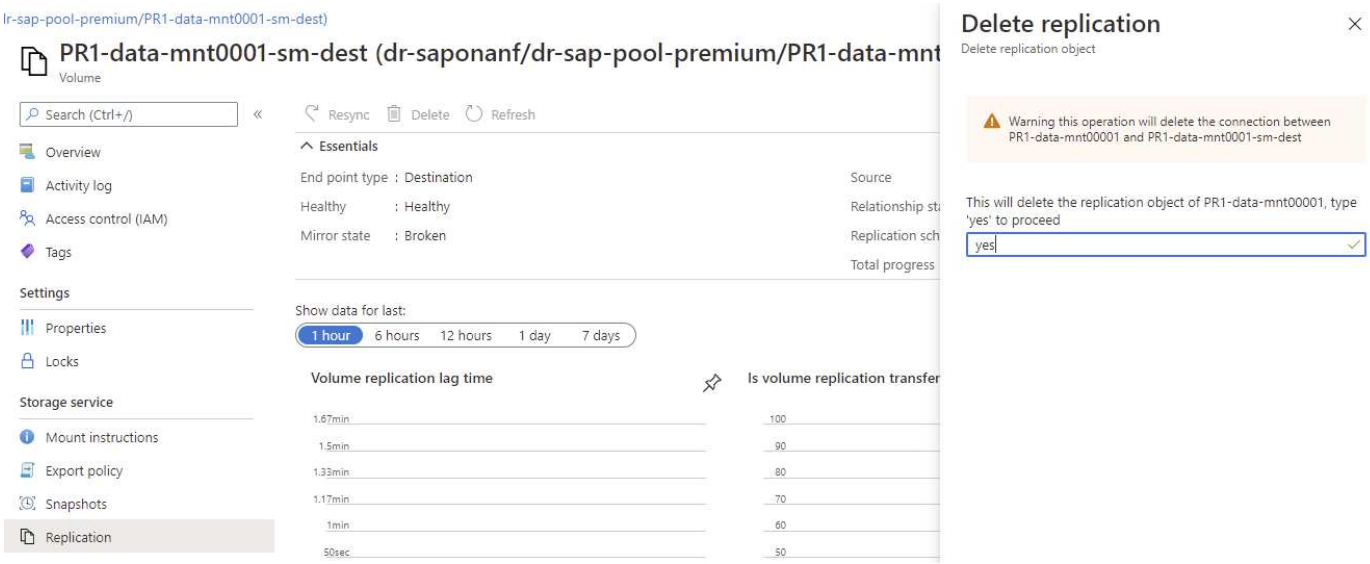
Interrompere ed eliminare il peering delle repliche

In caso di failover di emergenza, i volumi di destinazione devono essere interrotti in modo che l'host di destinazione possa montare i volumi per le operazioni di lettura e scrittura.

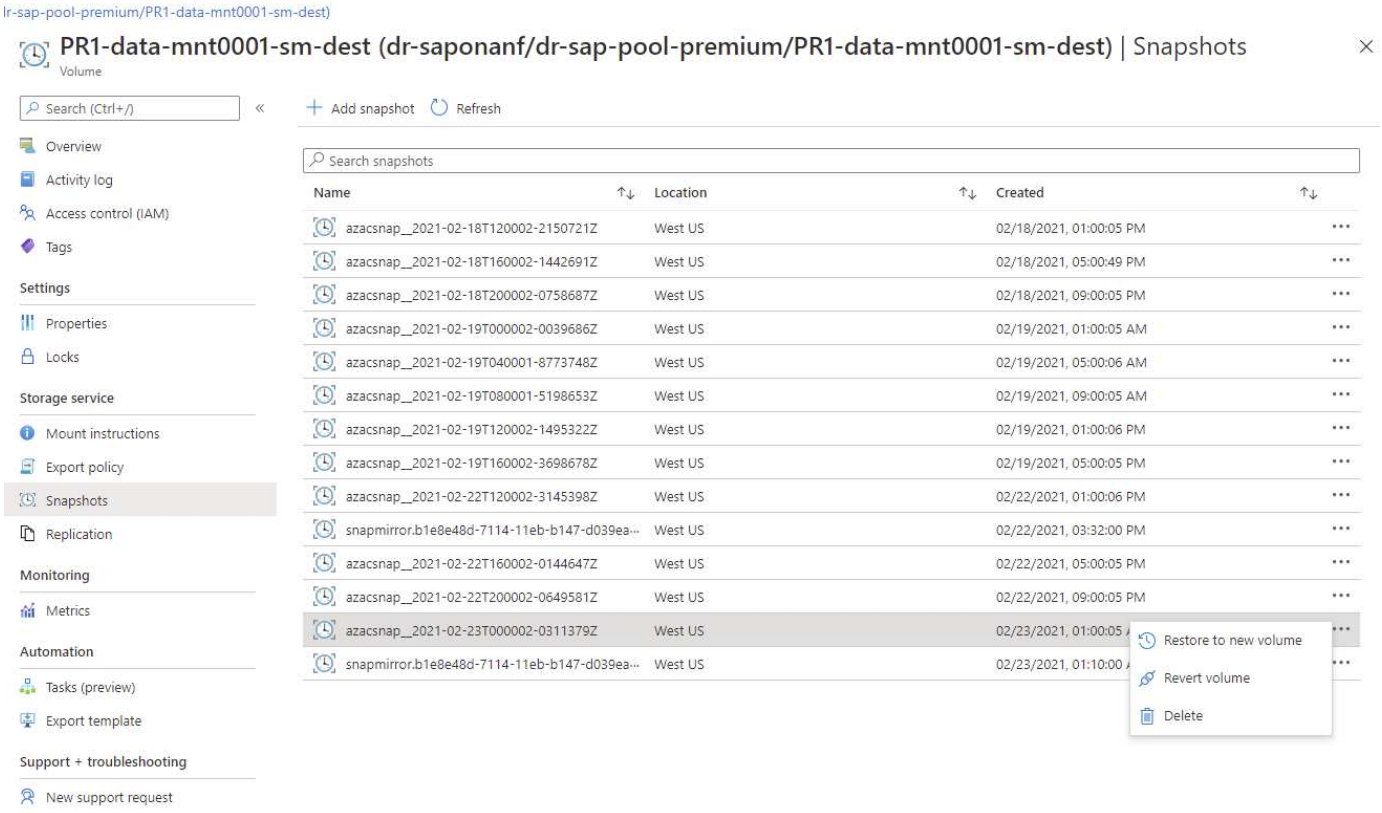
Per il volume di dati HANA, è necessario ripristinare il volume all'ultimo backup di snapshot HANA creato con AzAcSnap. Questa operazione di revert del volume non è possibile se l'ultimo snapshot di replica è contrassegnato come occupato a causa del peering della replica. Pertanto, è necessario eliminare anche il peering delle repliche.

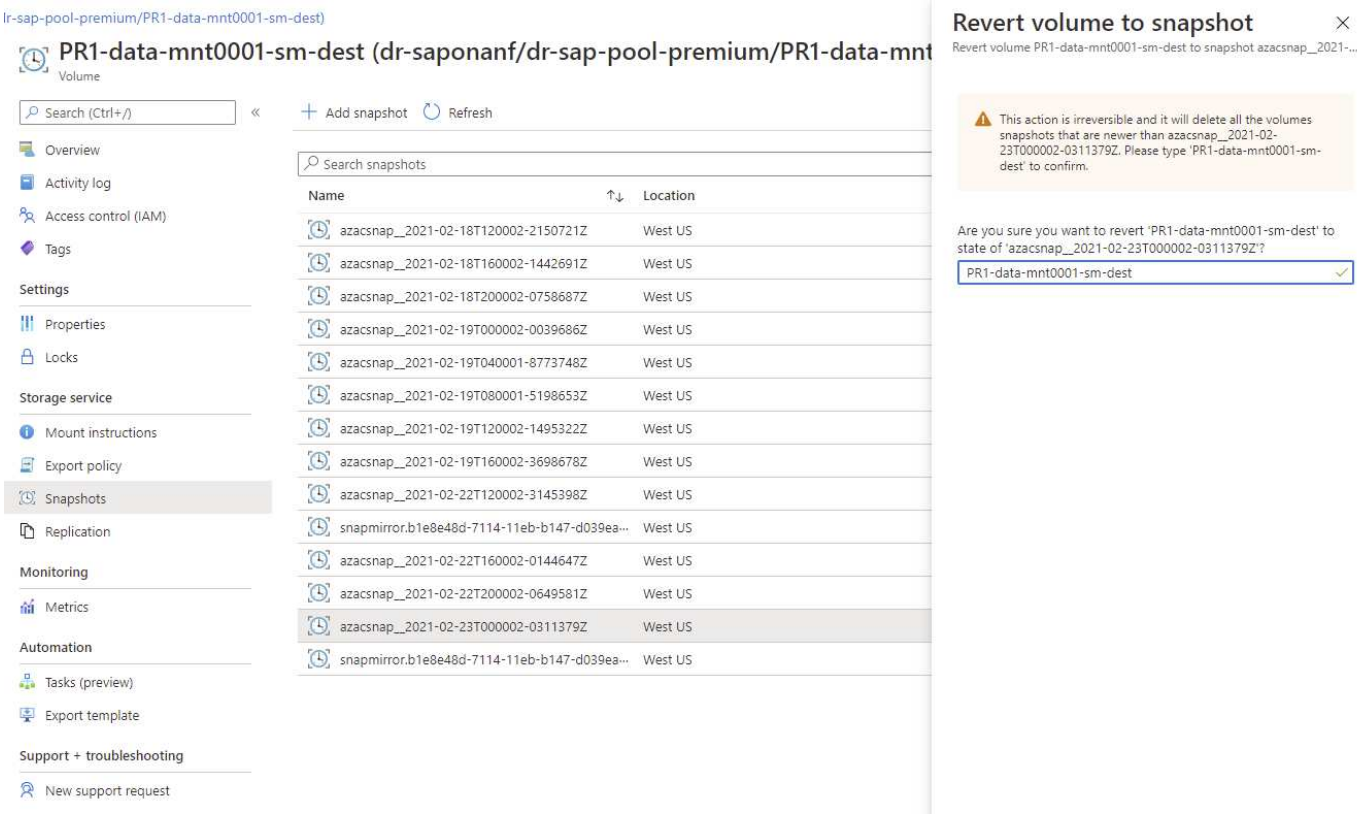
Le due schermate successive mostrano l'operazione di peering break e delete per il volume di dati HANA. Le stesse operazioni devono essere eseguite anche per il backup del log e per il volume condiviso HANA.





Poiché il peering delle repliche è stato eliminato, è possibile ripristinare il volume all'ultimo backup di snapshot HANA. Se il peering non viene cancellato, la selezione del volume di revert non è selezionabile e non è selezionabile. Le due schermate seguenti mostrano l'operazione di ripristino del volume.





Dopo l'operazione di revert del volume, il volume di dati si basa sul backup di snapshot HANA coerente e può ora essere utilizzato per eseguire operazioni di ripristino in avanti.

Se è stato utilizzato un pool di capacità con un livello di performance basso, i volumi devono ora essere spostati in un pool di capacità in grado di fornire le performance richieste.

Montare i volumi sull'host di destinazione

I volumi possono ora essere montati sull'host di destinazione, in base a. `/etc/fstab` file creato in precedenza.

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

Il seguente output mostra i file system richiesti.

```
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:~ #
```

Ripristino del database HANA

Di seguito vengono illustrati i passaggi per il ripristino del database HANA

Avviare i servizi SAP richiesti.

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

Il seguente output mostra i processi richiesti.

```
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
```

Le seguenti sottosezioni descrivono il processo di ripristino con e senza il ripristino in avanti utilizzando i backup del registro replicati. Il ripristino viene eseguito utilizzando lo script di ripristino HANA per il database di sistema e i comandi hdbsql per il database tenant.

Ripristino dell'ultimo Savepoint di backup del volume di dati HANA

Il ripristino all'ultimo punto di salvataggio del backup viene eseguito con i seguenti comandi come utente pr1adm:

- Database di sistema

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

- Database tenant

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

È inoltre possibile utilizzare HANA Studio o Cockpit per eseguire il ripristino del sistema e del database tenant.

L'output del seguente comando mostra l'esecuzione del ripristino.

Recovery del database di sistema

```
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 del database tenant

Se non è stata creata una chiave di memorizzazione utente per l'utente pr1adm nel sistema di origine, è necessario creare una chiave nel sistema di destinazione. L'utente del database configurato nella chiave deve disporre dei privilegi necessari per eseguire le operazioni di ripristino del tenant.

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

Il ripristino del tenant viene ora eseguito con hdbsql.

```
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=>
```

Il database HANA è ora operativo e il workflow di disaster recovery per il database HANA è stato testato.

Recovery con forward recovery utilizzando backup di log/catalogo

I backup dei log e il catalogo di backup HANA vengono replicati dal sistema di origine.

Il ripristino utilizzando tutti i backup dei log disponibili viene eseguito con i seguenti comandi come utente pr1adm:

- Database di sistema

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

- Database tenant

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

Per eseguire il ripristino utilizzando tutti i registri disponibili, è possibile utilizzare in qualsiasi momento in futuro come data e ora nell'istruzione Recovery.

È inoltre possibile utilizzare HANA Studio o Cockpit per eseguire il ripristino del sistema e del database tenant.

L'output del seguente comando mostra l'esecuzione del ripristino.

Recovery del database di sistema

```
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 del database tenant

```
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=>
```

Il database HANA è ora operativo e il workflow di disaster recovery per il database HANA è stato testato.

Verificare la coerenza dei backup dei log più recenti

Poiché la replica del volume di backup del log viene eseguita indipendentemente dal processo di backup del log eseguito dal database SAP HANA, potrebbero esserci file di backup del log aperti e incoerenti nel sito di disaster recovery. Solo i file di backup dei log più recenti potrebbero essere incoerenti e tali file devono essere controllati prima di eseguire un ripristino in avanti nel sito di disaster recovery utilizzando `hdbbackupcheck` tool.

Se il `hdbbackupcheck` lo strumento segnala un errore per i backup dei log più recenti; è necessario rimuovere o eliminare l'ultimo set di backup dei log.

```
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.
```

La verifica deve essere eseguita per i file di backup dei log più recenti del sistema e del database del tenant.

Se il `hdbbackupcheck` lo strumento segnala un errore per i backup dei log più recenti; è necessario rimuovere o eliminare l'ultimo set di backup dei log.

Aggiornare la cronologia

Le seguenti modifiche tecniche sono state apportate a questa soluzione dalla pubblicazione originale.

Versione	Data	Riepilogo degli aggiornamenti
Versione 1.0	Aprile 2021	Versione iniziale