



Backup, ripristino e disaster recovery

NetApp Solutions SAP

NetApp
March 11, 2024

Sommario

- Backup, ripristino e disaster recovery 1
 - SAP HANA su Amazon FSX per NetApp ONTAP - Backup e recovery con SnapCenter 1
 - Backup e recovery SAP HANA con SnapCenter 68
 - Backup e recovery di BlueXP per SAP HANA - Cloud object storage come destinazione di backup 214
 - Backup e ripristino della replica del sistema SAP HANA con SnapCenter 237
 - Disaster recovery SAP HANA con Azure NetApp Files 270
 - TR-4646: Disaster recovery SAP HANA con replica dello storage 310
 - TR-4313: Backup e ripristino SAP HANA con Snap Creator 311
 - TR-4711: Backup e ripristino SAP HANA con sistemi di storage NetApp e software CommVault 311
 - NVA-1147-DESIGN: SAP HANA su NetApp All SAN Array - SAN moderne, protezione dei dati e disaster recovery 311

Backup, ripristino e disaster recovery

SAP HANA su Amazon FSX per NetApp ONTAP - Backup e recovery con SnapCenter

TR-4926: SAP HANA su Amazon FSX per NetApp ONTAP - Backup e recovery con SnapCenter

Nils Bauer, NetApp

Questo report tecnico fornisce le Best practice per la protezione dei dati SAP HANA su Amazon FSX per NetApp ONTAP e NetApp SnapCenter. Questo documento tratta i concetti di SnapCenter, i consigli di configurazione e i flussi di lavoro operativi, tra cui configurazione, operazioni di backup, e operazioni di ripristino e recovery.

Le aziende oggi richiedono una disponibilità continua e ininterrotta per le proprie applicazioni SAP. Si aspettano livelli di performance costanti di fronte a volumi di dati in continua crescita e alla necessità di attività di manutenzione ordinaria, come i backup di sistema. L'esecuzione di backup dei database SAP è un'attività critica e può avere un impatto significativo sulle performance del sistema SAP di produzione.

Le finestre di backup si riducono mentre la quantità di dati da sottoporre a backup aumenta. Pertanto, è difficile trovare un momento in cui è possibile eseguire backup con un effetto minimo sui processi di business. Il tempo necessario per ripristinare e ripristinare i sistemi SAP è un problema perché i downtime per i sistemi di produzione SAP e non in produzione devono essere ridotti al minimo per ridurre i costi per l'azienda.

Backup e ripristino con Amazon FSX per ONTAP

È possibile utilizzare la tecnologia NetApp Snapshot per creare backup del database in pochi minuti.

Il tempo necessario per creare una copia Snapshot è indipendente dalle dimensioni del database, in quanto una copia Snapshot non sposta alcun blocco di dati fisico sulla piattaforma di storage. Inoltre, l'utilizzo della tecnologia Snapshot non ha alcun effetto sulle performance del sistema SAP attivo. Pertanto, è possibile pianificare la creazione di copie Snapshot senza prendere in considerazione i periodi di dialogo di picco o di attività batch. I clienti SAP e NetApp pianificano in genere più backup Snapshot online durante il giorno; ad esempio, ogni sei ore è comune. Questi backup Snapshot vengono in genere conservati per tre o cinque giorni nel sistema di storage primario prima di essere rimossi o tierati per uno storage più economico per una conservazione a lungo termine.

Le copie Snapshot offrono anche vantaggi chiave per le operazioni di ripristino e ripristino. La tecnologia NetApp SnapRestore consente di ripristinare un intero database o, in alternativa, solo una parte di un database in qualsiasi momento, in base alle copie Snapshot attualmente disponibili. Tali processi di ripristino vengono completati in pochi secondi, indipendentemente dalle dimensioni del database. Poiché è possibile creare diversi backup Snapshot online durante la giornata, il tempo necessario per il processo di recovery è notevolmente ridotto rispetto a un tradizionale approccio di backup una volta al giorno. Poiché è possibile eseguire un ripristino con una copia Snapshot che ha al massimo solo poche ore di vita (anziché fino a 24 ore), durante il forward recovery è necessario applicare un numero inferiore di registri delle transazioni. Pertanto, l'RTO viene ridotto a diversi minuti piuttosto che alle diverse ore richieste per i backup di streaming convenzionali.

I backup delle copie Snapshot vengono memorizzati sullo stesso sistema di dischi dei dati online attivi. Pertanto, NetApp consiglia di utilizzare i backup di copia Snapshot come supplemento piuttosto che come

sostituito per i backup in una posizione secondaria. La maggior parte delle azioni di ripristino e ripristino viene gestita utilizzando SnapRestore sul sistema di storage primario. I ripristini da una posizione secondaria sono necessari solo se il sistema di storage primario contenente le copie Snapshot viene danneggiato. È inoltre possibile utilizzare la posizione secondaria se è necessario ripristinare un backup non più disponibile nella posizione principale.

Un backup in una posizione secondaria si basa sulle copie Snapshot create sullo storage primario. Pertanto, i dati vengono letti direttamente dal sistema di storage primario senza generare carico sul server di database SAP. Lo storage primario comunica direttamente con lo storage secondario e replica i dati di backup verso la destinazione utilizzando la funzione NetApp SnapVault.

SnapVault offre vantaggi significativi rispetto ai backup tradizionali. Dopo un trasferimento iniziale dei dati, in cui tutti i dati sono stati trasferiti dall'origine alla destinazione, tutti i backup successivi vengono copiati solo per spostare i blocchi modificati nello storage secondario. Pertanto, il carico sul sistema di storage primario e il tempo necessario per un backup completo sono notevolmente ridotti. Poiché SnapVault memorizza solo i blocchi modificati nella destinazione, eventuali backup completi del database aggiuntivi consumano molto meno spazio su disco.

Esecuzione delle operazioni di backup e ripristino Snapshot

La figura seguente mostra HANA Studio di un cliente che utilizza le operazioni di backup Snapshot. L'immagine mostra che il backup del database HANA (di circa 4 TB) viene eseguito in 1 minuto e 20 secondi utilizzando la tecnologia di backup Snapshot e più di 4 ore con un'operazione di backup basata su file.

La maggior parte del runtime complessivo del workflow di backup è il tempo necessario per eseguire l'operazione di salvataggio del backup HANA, che dipende dal carico sul database HANA. Il backup Snapshot dello storage viene sempre completato in un paio di secondi.

Backup Catalog					
<input type="checkbox"/> Show Log Backups <input type="checkbox"/> Show Delta Backups					
Stat...	Started	Duration	Size	Backup Ty...	Destinati...
■	Jan 11, 2022 10:26:59 AM	00h 01m 17s	4.51 TB	Data Back...	Snapshot
■	Jan 11, 2022 8:40:02 AM	00h 27m 11s	4.51 TB	Data Back...	Snapshot
■	Jan 11, 2022 1:00:58 AM	04h 05m 39s	3.82 TB	Data Back...	File
■	Jan 9, 2022 4:40:03 PM	00h 01m 23s	4.51 TB	Data Back...	Snapshot
■	Jan 9, 2022 8:00:02 AM	02h 39m 04s	3.82 TB	Data Back...	File
■	Jan 9, 2022 12:40:03 AM	00h 01m 18s	4.51 TB	Data Back...	Snapshot
■	Jan 8, 2022 4:40:03 PM	00h 01m 18s	4.51 TB	Data Back...	Snapshot
■	Jan 8, 2022 8:40:03 AM	00h 01m 22s	4.51 TB	Data Back...	Snapshot
■	Jan 8, 2022 12:40:03 AM	00h 01m 19s	4.51 TB	Data Back...	Snapshot
■	Jan 7, 2022 4:40:03 PM	00h 01m 19s	4.51 TB	Data Back...	Snapshot
■	Jan 7, 2022 8:40:02 AM	00h 01m 19s	4.51 TB	Data Back...	Snapshot
■	Jan 7, 2022 12:40:02 AM	00h 01m 20s	4.51 TB	Data Back...	Snapshot
■	Jan 6, 2022 4:40:02 PM	00h 01m 18s	4.51 TB	Data Back...	Snapshot
■	Jan 6, 2022 8:40:03 AM	00h 01m 17s	4.51 TB	Data Back...	Snapshot
■	Jan 6, 2022 12:40:03 AM	00h 01m 19s	4.51 TB	Data Back...	Snapshot
■	Jan 5, 2022 4:40:03 PM	00h 01m 19s	4.51 TB	Data Back...	Snapshot

File-based backup: 4 hours 05 min
(~270 MB/s throughput)

04h 05m 39s	3.82 TB	Data Back...	File
-------------	---------	--------------	------

Snapshot backup: 1 min 20 sec

00h 01m 18s	4.51 TB	Data Back...	Snapshot
00h 01m 22s	4.51 TB	Data Back...	Snapshot
00h 01m 19s	4.51 TB	Data Back...	Snapshot

Backup runtime reduced by 99%

Confronto degli obiettivi del tempo di ripristino

Questa sezione fornisce un confronto RTO (Recovery Time Objective) dei backup Snapshot basati su file e storage. L'RTO è definito dalla somma del tempo necessario per il ripristino, il ripristino e l'avvio del database.

Tempo necessario per il ripristino del database

Con un backup basato su file, il tempo di ripristino dipende dalle dimensioni del database e dell'infrastruttura di backup, che definisce la velocità di ripristino in megabyte al secondo. Ad esempio, se l'infrastruttura supporta

un'operazione di ripristino a una velocità di 250 MBps, occorrono circa 4.5 ore per ripristinare un database di 4 TB sulla persistenza.

Con i backup delle copie Snapshot dello storage, il tempo di ripristino è indipendente dalle dimensioni del database e si trova sempre nell'intervallo di un paio di secondi.

Tempo necessario per avviare il database

L'ora di inizio del database dipende dalle dimensioni del database e dal tempo necessario per caricare i dati in memoria. Negli esempi seguenti, si presuppone che i dati possano essere caricati con 1000 Mbps. Il caricamento di 4 TB in memoria richiede circa 1 ora e 10 minuti. L'ora di inizio è la stessa per le operazioni di ripristino e ripristino basate su file e Snapshot.

Tempo necessario per il ripristino del database

Il tempo di ripristino dipende dal numero di registri che devono essere applicati dopo il ripristino. Questo numero è determinato dalla frequenza con cui vengono eseguiti i backup dei dati.

Con i backup dei dati basati su file, la pianificazione del backup è generalmente una volta al giorno. In genere, non è possibile una frequenza di backup più elevata, poiché il backup diminuisce le prestazioni di produzione. Pertanto, nel peggiore dei casi, tutti i log scritti durante la giornata devono essere applicati durante il recupero in avanti.

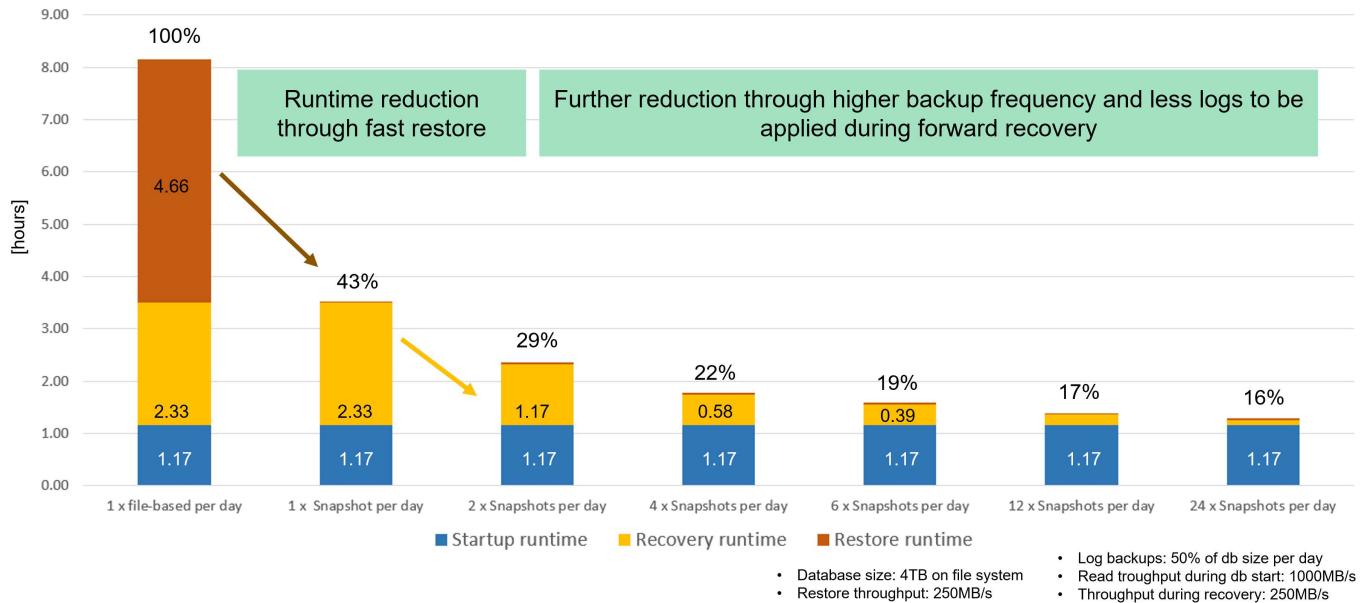
I backup di Snapshot vengono in genere pianificati con una frequenza maggiore perché non influiscono sulle prestazioni del database SAP HANA. Ad esempio, se i backup Snapshot vengono pianificati ogni sei ore, il tempo di ripristino sarebbe, nel peggiore dei casi, un quarto del tempo di ripristino per un backup basato su file (6 ore / 24 ore = .25).

La figura seguente mostra un confronto tra le operazioni di ripristino e ripristino con backup giornalieri basati su file e backup Snapshot con diverse pianificazioni.

Le prime due barre mostrano che anche con un singolo backup Snapshot al giorno, il ripristino e il ripristino vengono ridotti al 43% a causa della velocità dell'operazione di ripristino da un backup Snapshot. Se vengono creati più backup Snapshot al giorno, il runtime può essere ulteriormente ridotto perché è necessario applicare meno registri durante il forward recovery.

La figura seguente mostra anche che quattro o sei backup Snapshot al giorno sono i più sensati, perché una frequenza più elevata non influisce più in modo significativo sul runtime complessivo.

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



Casi di utilizzo e valori delle operazioni di backup e cloning accelerate

L'esecuzione dei backup è una parte fondamentale di qualsiasi strategia di protezione dei dati. I backup vengono pianificati regolarmente per garantire che sia possibile eseguire il ripristino in caso di guasti del sistema. Questo è il caso di utilizzo più ovvio, ma esistono anche altre attività di gestione del ciclo di vita SAP, in cui l'accelerazione delle operazioni di backup e ripristino è fondamentale.

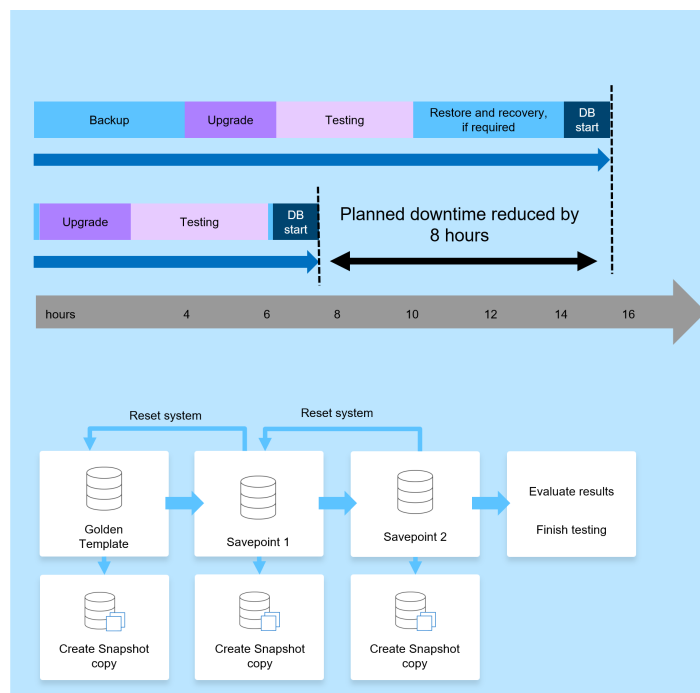
L'upgrade del sistema SAP HANA è un esempio di come un backup on-demand prima dell'upgrade e una possibile operazione di ripristino in caso di errore dell'upgrade abbiano un impatto significativo sul downtime complessivo pianificato. Con l'esempio di un database da 4 TB, è possibile ridurre il downtime pianificato di 8 ore utilizzando le operazioni di backup e ripristino basate su Snapshot.

Un altro esempio di caso d'utilizzo potrebbe essere un tipico ciclo di test, in cui il test deve essere eseguito su più iterazioni con diversi set di dati o parametri. Sfruttando le rapide operazioni di backup e ripristino, è possibile creare facilmente punti di salvataggio all'interno del ciclo di test e ripristinare il sistema a uno qualsiasi di questi punti di salvataggio precedenti se un test non riesce o deve essere ripetuto. Ciò consente di completare i test in anticipo o di eseguire più test contemporaneamente e di migliorare i risultati dei test.

Use Cases for Backup and Recovery Operations

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

- Accelerate test cycles
 - Fast creation of savepoints after a successful step
 - Fast reset of system to any savepoint
 - Repeat step until successful



Una volta implementati, i backup Snapshot possono essere utilizzati per gestire diversi altri casi di utilizzo, che richiedono copie di un database HANA. Con FSX per ONTAP, puoi creare un nuovo volume in base al contenuto di qualsiasi backup Snapshot disponibile. Il tempo di esecuzione di questa operazione è di alcuni secondi, indipendentemente dalle dimensioni del volume.

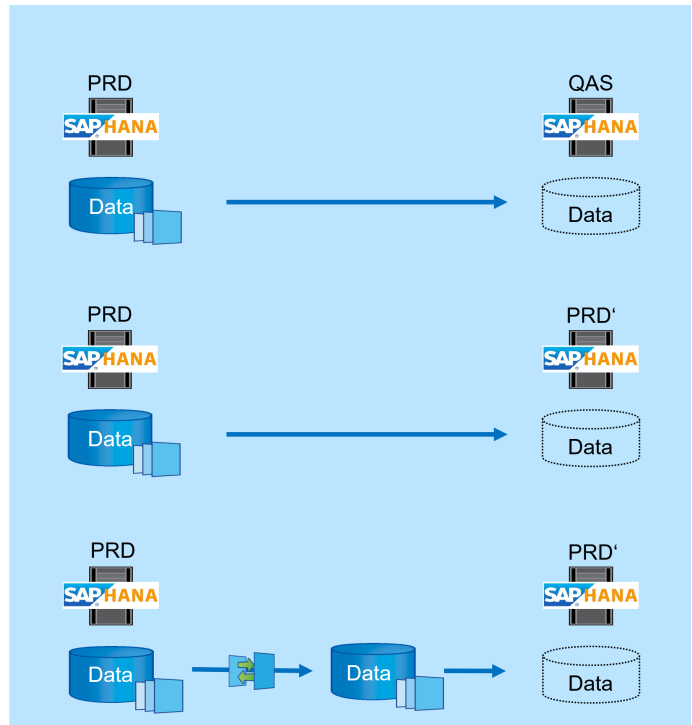
Il caso di utilizzo più diffuso è SAP System Refresh, in cui i dati del sistema di produzione devono essere copiati nel sistema di test o QA. Sfruttando la funzionalità di cloning FSX per ONTAP, è possibile eseguire il provisioning del volume per il sistema di test da qualsiasi copia Snapshot del sistema di produzione in pochi secondi. Il nuovo volume deve quindi essere collegato al sistema di test e il database HANA recuperato.

Il secondo caso di utilizzo è la creazione di un sistema di riparazione, utilizzato per risolvere un danneggiamento logico del sistema di produzione. In questo caso, viene utilizzato un backup Snapshot precedente del sistema di produzione per avviare un sistema di riparazione, che è un clone identico del sistema di produzione con i dati prima che si verificasse il danneggiamento. Il sistema di riparazione viene quindi utilizzato per analizzare il problema ed esportare i dati richiesti prima che sia danneggiato.

L'ultimo caso di utilizzo è la capacità di eseguire un test di failover per il disaster recovery senza interrompere la replica e quindi senza influenzare l'RTO e l'RPO (Recovery Point Objective) della configurazione del disaster recovery. Quando la replica di NetApp SnapMirror per FSX per ONTAP viene utilizzata per replicare i dati nel sito di disaster recovery, i backup Snapshot di produzione sono disponibili anche nel sito di disaster recovery e possono quindi essere utilizzati per creare un nuovo volume per il test di disaster recovery.

Use Cases for Cloning Operations

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



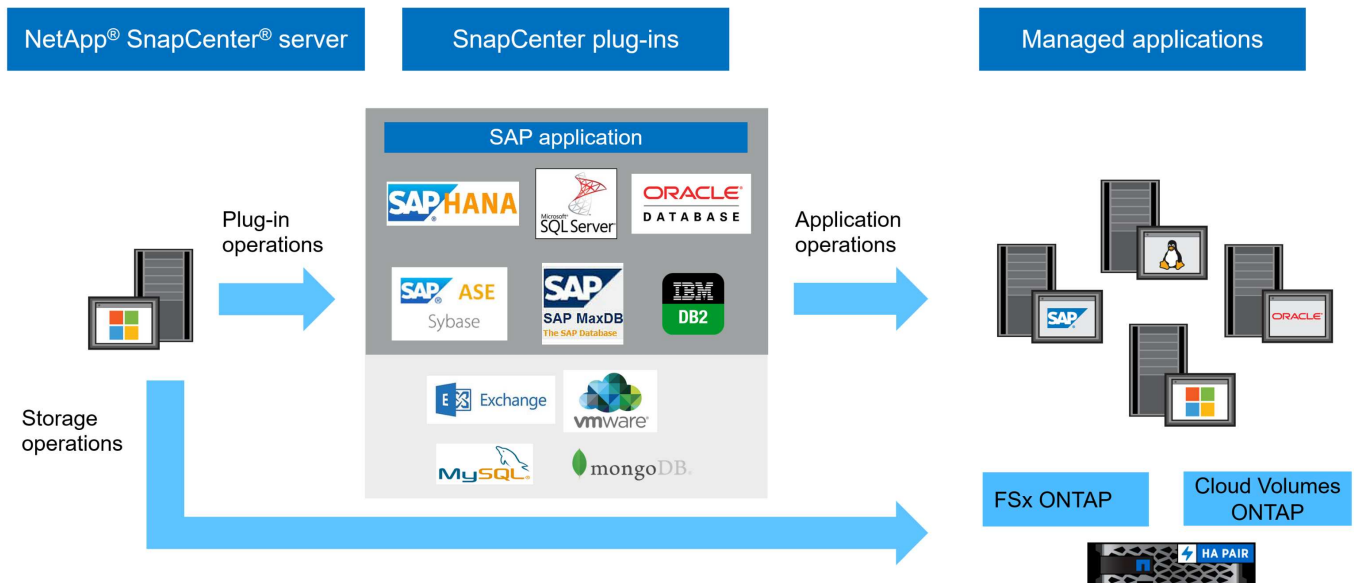
Architettura SnapCenter

SnapCenter è una piattaforma unificata e scalabile per la protezione dei dati coerente con l'applicazione. SnapCenter offre controllo e supervisione centralizzati, delegando al contempo la capacità degli utenti di gestire processi di backup, ripristino e clonazione specifici dell'applicazione. Con SnapCenter, gli amministratori di database e storage imparano a utilizzare un unico strumento per gestire le operazioni di backup, ripristino e clonazione per una vasta gamma di applicazioni e database.

SnapCenter gestisce i dati tra gli endpoint del data fabric basato su NetApp. È possibile utilizzare SnapCenter per replicare i dati tra ambienti on-premise, tra ambienti on-premise e il cloud, e tra cloud privato, ibrido e pubblico.

Componenti SnapCenter

SnapCenter include il server SnapCenter, il pacchetto plug-in SnapCenter per Windows e il pacchetto plug-in SnapCenter per Linux. Ogni pacchetto contiene plug-in per SnapCenter per varie applicazioni e componenti dell'infrastruttura.



Soluzione di backup SAP HANA di SnapCenter

La soluzione di backup SnapCenter per SAP HANA copre le seguenti aree:

- Operazioni di backup, pianificazione e gestione della conservazione
 - Backup dei dati SAP HANA con copie Snapshot basate su storage
 - Backup di volumi non dati con copie Snapshot basate su storage (ad esempio, /hana/shared)
 - Verifica dell'integrità dei blocchi di database mediante un backup basato su file
 - Replica su una posizione di backup off-site o disaster recovery
- Manutenzione del catalogo di backup SAP HANA
 - Per backup dei dati HANA (Snapshot e basato su file)
 - Per i backup dei log HANA
- Operazioni di ripristino e recovery
 - Ripristino e ripristino automatici
 - Operazioni di ripristino del tenant singolo per sistemi SAP HANA (MDC)

I backup dei file di dati del database vengono eseguiti da SnapCenter in combinazione con il plug-in per SAP HANA. Il plug-in attiva il punto di salvataggio del backup del database SAP HANA in modo che le copie Snapshot, create sul sistema di storage primario, si basino su un'immagine coerente del database SAP HANA.

SnapCenter consente la replica di immagini di database coerenti in una posizione di backup off-site o disaster recovery utilizzando SnapVault o la funzione SnapMirror. In genere, vengono definite policy di conservazione diverse per i backup nello storage di backup primario e off-site. SnapCenter gestisce la conservazione nello storage primario e ONTAP la gestisce nello storage di backup off-site.

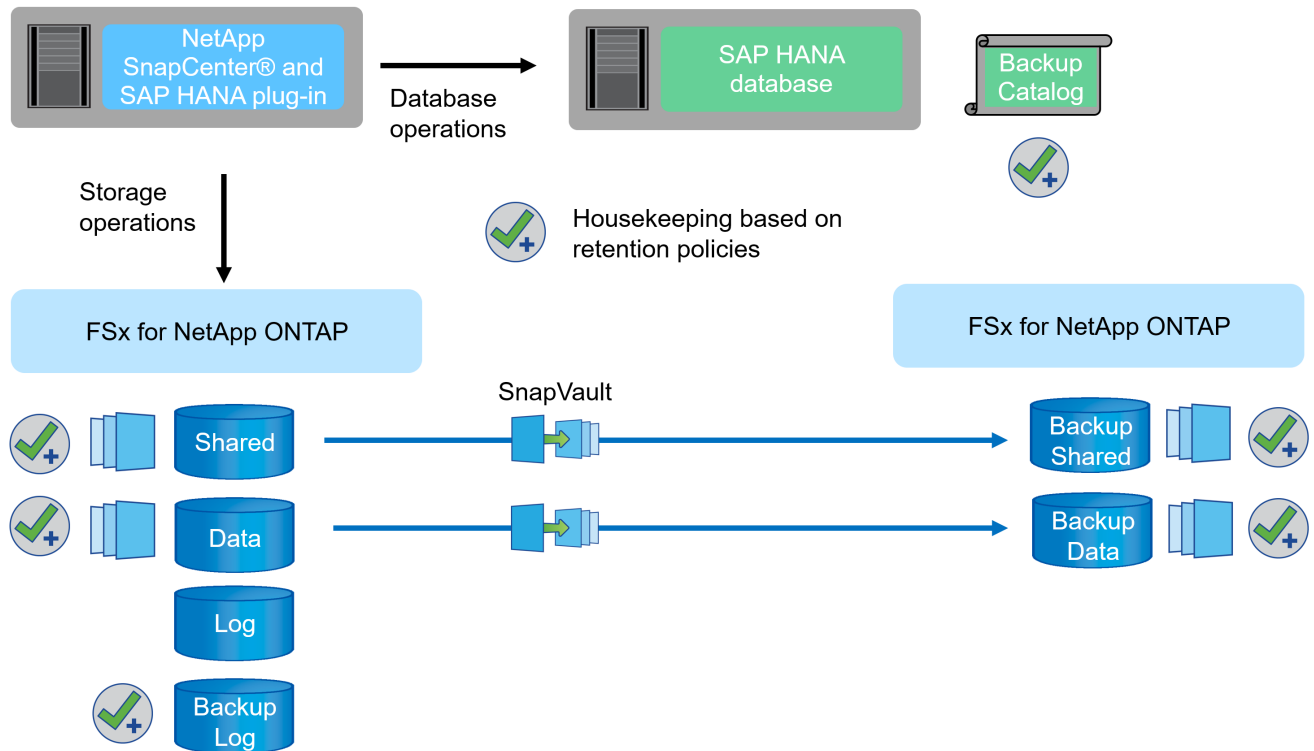
Per consentire un backup completo di tutte le risorse correlate a SAP HANA, SnapCenter consente inoltre di eseguire il backup di tutti i volumi non dati utilizzando il plug-in SAP HANA con copie Snapshot basate su storage. È possibile pianificare volumi diversi dai dati in modo indipendente dal backup dei dati del database per consentire policy di conservazione e protezione individuali.

SAP consiglia di combinare i backup Snapshot basati su storage con un backup settimanale basato su file per

eseguire un controllo dell'integrità dei blocchi. È possibile eseguire il controllo dell'integrità del blocco da SnapCenter. In base alle policy di conservazione configurate, SnapCenter gestisce la gestione dei backup dei file di dati nello storage primario, nei backup dei file di log e nel catalogo di backup SAP HANA.

SnapCenter gestisce la conservazione dello storage primario, mentre FSX per ONTAP gestisce la conservazione del backup secondario.

La figura seguente mostra una panoramica delle operazioni di backup e gestione della conservazione di SnapCenter.



Quando si esegue un backup Snapshot basato su storage del database SAP HANA, SnapCenter esegue le seguenti attività:

1. Crea un punto di salvataggio di backup SAP HANA per creare un'immagine coerente sul layer di persistenza.
2. Crea una copia Snapshot del volume di dati basata su storage.
3. Registra il backup Snapshot basato su storage nel catalogo di backup SAP HANA.
4. Rilascia il punto di salvataggio del backup SAP HANA.
5. Esegue un aggiornamento di SnapVault o SnapMirror per il volume di dati, se configurato.
6. Elimina le copie Snapshot dello storage nello storage primario in base alle policy di conservazione definite.
7. Elimina le voci del catalogo di backup SAP HANA se i backup non esistono più nello storage di backup primario o off-site.
8. Ogni volta che un backup viene cancellato in base al criterio di conservazione o manualmente, SnapCenter elimina anche tutti i backup dei log precedenti al backup dei dati meno recente. I backup dei log vengono cancellati nel file system e nel catalogo di backup SAP HANA.

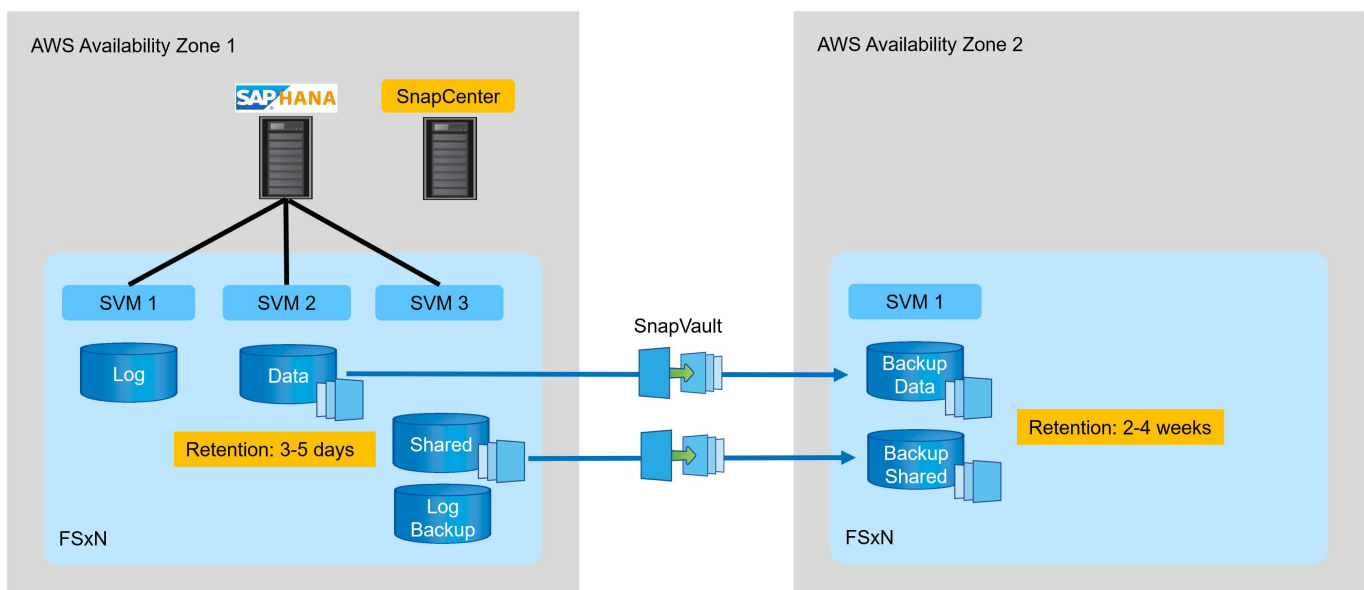
Scopo del presente documento

Questo documento descrive l'opzione di configurazione SnapCenter più comune per un sistema host singolo SAP HANA MDC con un singolo tenant su FSX per ONTAP. Sono possibili altre opzioni di configurazione e, in alcuni casi, richieste per specifici sistemi SAP HANA, ad esempio per un sistema a più host. Per una descrizione dettagliata delle altre opzioni di configurazione, vedere ["Concetti e Best practice di SnapCenter \(netapp.com\)"](https://netapp.com).

In questo documento, utilizziamo la console Amazon Web Services (AWS) e la CLI FSX per ONTAP per eseguire le procedure di configurazione richieste sul layer di storage. Puoi anche utilizzare NetApp Cloud Manager per gestire FSX per ONTAP, ma questo non rientra nell'ambito di questo documento. Per informazioni sull'utilizzo di NetApp Cloud Manager per FSX per ONTAP, vedere ["Ulteriori informazioni su Amazon FSX per ONTAP \(netapp.com\)"](https://netapp.com).

Strategia di protezione dei dati

La figura seguente mostra una tipica architettura di backup per SAP HANA su FSX per ONTAP. Il sistema HANA si trova nella zona di disponibilità AWS 1 e utilizza un file system FSX per ONTAP all'interno della stessa zona di disponibilità. Le operazioni di backup di Snapshot vengono eseguite per i dati e il volume condiviso del database HANA. Oltre ai backup Snapshot locali, conservati per 3-5 giorni, i backup vengono replicati anche in uno storage offsite per una conservazione a lungo termine. Lo storage di backup offsite è un secondo FSX per il file system ONTAP situato in una diversa zona di disponibilità AWS. I backup dei dati HANA e del volume condiviso vengono replicati con SnapVault nel secondo file system FSX per ONTAP e vengono conservati per 2-3 settimane.



Prima di configurare SnapCenter, la strategia di protezione dei dati deve essere definita in base ai requisiti RTO e RPO dei vari sistemi SAP.

Un approccio comune consiste nella definizione di tipi di sistema quali produzione, sviluppo, test o sistemi sandbox. Tutti i sistemi SAP dello stesso tipo di sistema hanno in genere gli stessi parametri di protezione dei dati.

È necessario definire i seguenti parametri:

- Con quale frequenza deve essere eseguito un backup Snapshot?
- Per quanto tempo i backup delle copie Snapshot devono essere conservati nel sistema di storage

primario?

- Con quale frequenza deve essere eseguito un controllo dell'integrità dei blocchi?
- I backup primari devono essere replicati in un sito di backup off-site?
- Per quanto tempo i backup devono essere conservati nello storage di backup off-site?

La seguente tabella mostra un esempio di parametri di protezione dei dati per i tipi di sistema: Produzione, sviluppo e test. Per il sistema di produzione, è stata definita una frequenza di backup elevata e i backup vengono replicati su un sito di backup off-site una volta al giorno. I sistemi di test hanno requisiti inferiori e nessuna replica dei backup.

Parametri	Sistemi di produzione	Sistemi di sviluppo	Sistemi di test
Frequenza di backup	Ogni 6 ore	Ogni 6 ore	Ogni 6 ore
Conservazione primaria	3 giorni	3 giorni	3 giorni
Controllo dell'integrità del blocco	Una volta alla settimana	Una volta alla settimana	No
Replica su un sito di backup off-site	Una volta al giorno	Una volta al giorno	No
Conservazione del backup off-site	2 settimane	2 settimane	Non applicabile

La tabella seguente mostra i criteri che devono essere configurati per i parametri di protezione dei dati.

Parametri	Policy LocalSnap	Policy LocalSnapAndSnapVault	Blocco policy IntegrityCheck
Tipo di backup	Basato su Snapshot	Basato su Snapshot	Basato su file
Frequenza di pianificazione	Ogni ora	Ogni giorno	Settimanale
Conservazione primaria	Conteggio = 12	Conteggio = 3	Conteggio = 1
Replica SnapVault	No	Sì	Non applicabile

La policy `LocalSnapshot` Viene utilizzato per i sistemi di produzione, sviluppo e test per coprire i backup Snapshot locali con una conservazione di due giorni.

Nella configurazione di protezione delle risorse, la pianificazione viene definita in modo diverso per i tipi di sistema:

- Produzione: Pianificazione ogni 4 ore.
- Sviluppo: Pianifica ogni 4 ore.
- Test: Pianifica ogni 4 ore.

La policy `LocalSnapAndSnapVault` viene utilizzato per i sistemi di produzione e sviluppo per coprire la replica giornaliera nello storage di backup off-site.

Nella configurazione della protezione delle risorse, viene definito il calendario per la produzione e lo sviluppo:

- Produzione: Pianifica ogni giorno.
- Sviluppo: Pianifica ogni giorno. la policy `BlockIntegrityCheck` viene utilizzato per i sistemi di produzione e sviluppo per la verifica settimanale dell'integrità dei blocchi mediante un backup basato su file.

Nella configurazione della protezione delle risorse, viene definito il calendario per la produzione e lo sviluppo:

- Produzione: Pianifica ogni settimana.
- Sviluppo: Pianifica ogni settimana.

Per ogni singolo database SAP HANA che utilizza la policy di backup off-site, è necessario configurare una relazione di protezione sul layer di storage. La relazione di protezione definisce quali volumi vengono replicati e la conservazione dei backup nello storage di backup off-site.

Nell'esempio seguente, per ciascun sistema di produzione e sviluppo, viene definita una conservazione di due settimane nello storage di backup off-site.

In questo esempio, le policy di protezione e la conservazione delle risorse di database SAP HANA e delle risorse non di volumi di dati non sono diverse.

Esempio di setup di laboratorio

Il seguente setup di laboratorio è stato utilizzato come configurazione di esempio per il resto di questo documento.

Sistema HANA PFX:

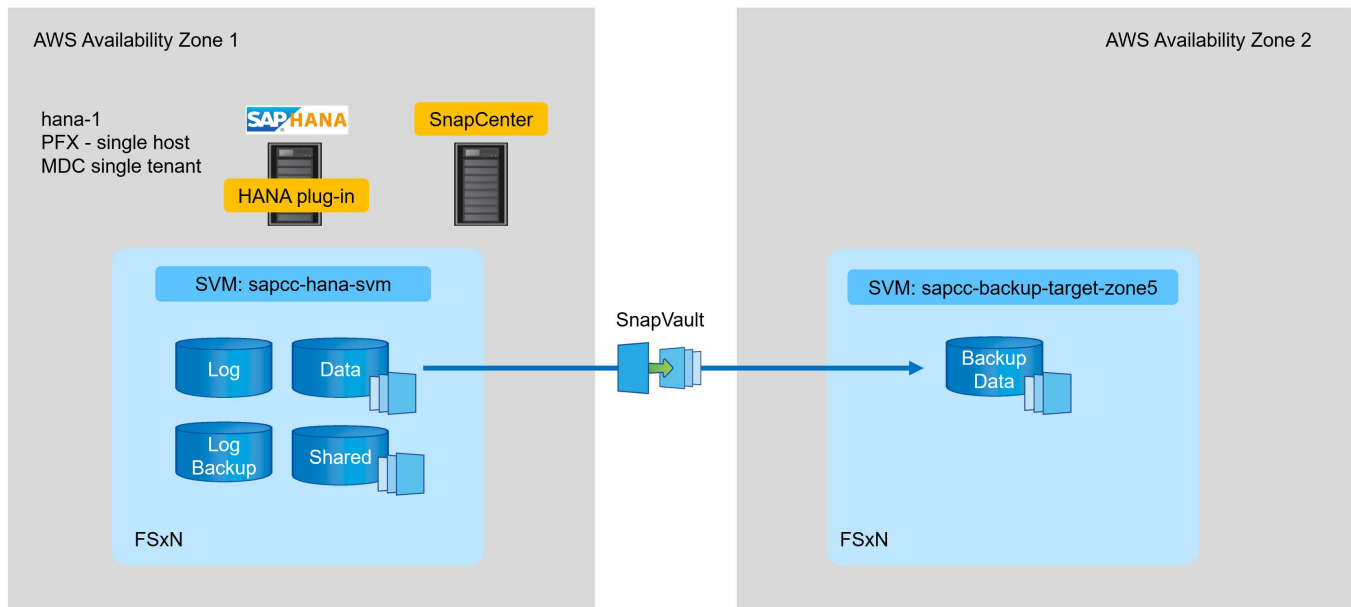
- Sistema MDC a host singolo con un singolo tenant
- HANA 2.0 SPS 6 revisione 60
- SLES PER SAP 15SP3

SnapCenter:

- Versione 4.6
- Plug-in HANA e Linux implementati su un host di database HANA

FSX per file system ONTAP:

- Due FSX per file system ONTAP con una singola SVM (Storage Virtual Machine)
- Ciascun sistema FSX per ONTAP in una zona di disponibilità AWS diversa
- Volume di dati HANA replicato nel secondo file system FSX per ONTAP



Configurazione di SnapCenter

Per la configurazione di base del SnapCenter e la protezione della risorsa HANA, è necessario eseguire le operazioni descritte in questa sezione.

Panoramica delle fasi di configurazione

Per la configurazione SnapCenter di base e la protezione della risorsa HANA, è necessario eseguire le seguenti operazioni. Ogni fase viene descritta in dettaglio nei seguenti capitoli.

1. Configurare l'utente di backup SAP HANA e la chiave hdbuserstore. Utilizzato per accedere al database HANA con il client hdbsql.
2. Configurare lo storage in SnapCenter. Credenziali per accedere a FSX per SVM ONTAP da SnapCenter
3. Configurare le credenziali per l'implementazione del plug-in. Utilizzato per implementare e installare automaticamente i plug-in SnapCenter richiesti sull'host del database HANA.
4. Aggiungere l'host HANA a SnapCenter. Implementa e installa i plug-in SnapCenter richiesti.
5. Configurare i criteri. Definisce il tipo di operazione di backup (Snapshot, file), le ritenzioni e la replica di backup Snapshot opzionale.
6. Configurare la protezione delle risorse HANA. Fornire la chiave hdbuserstore e allegare policy e pianificazioni alla risorsa HANA.

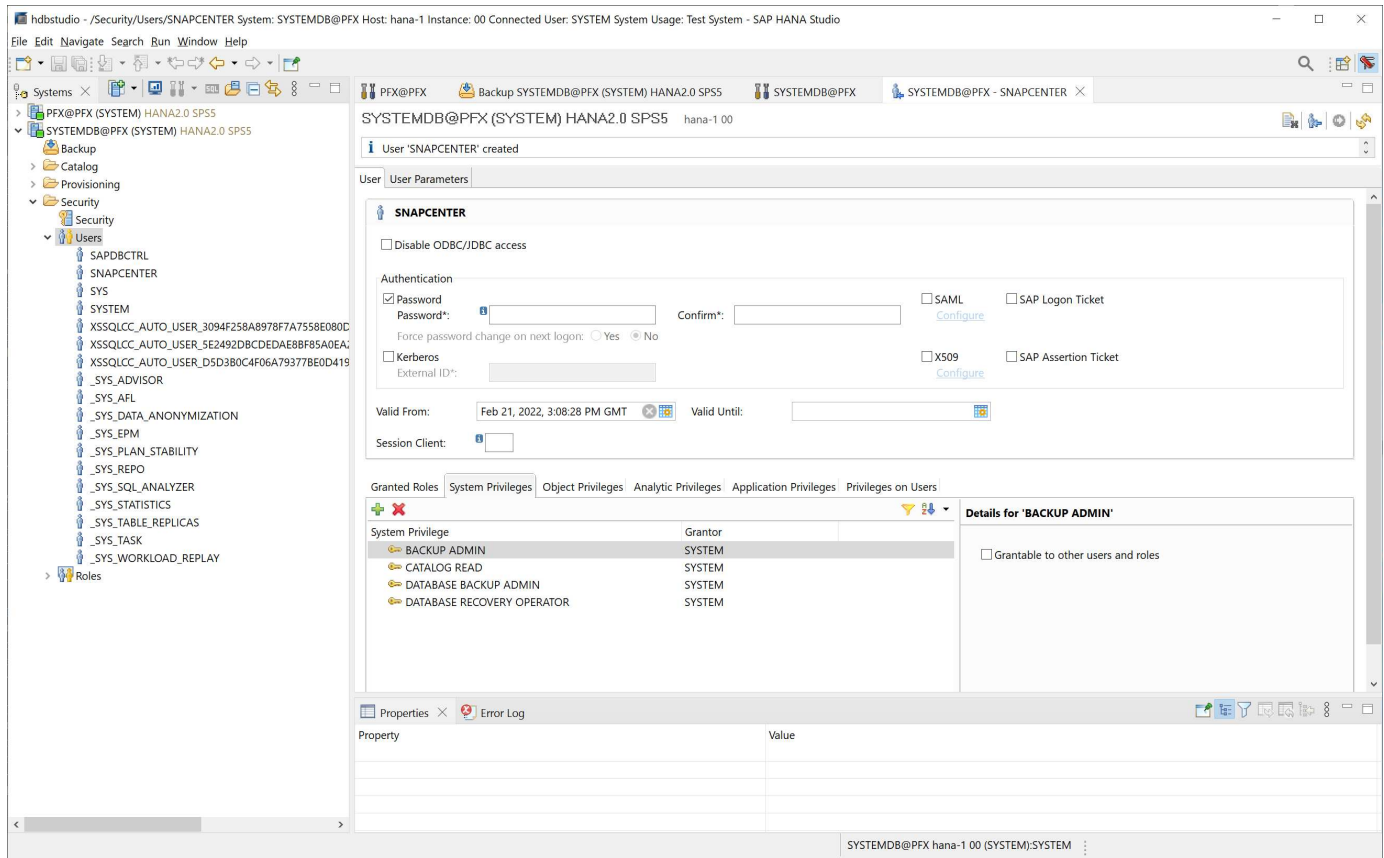
Configurazione di SAP HANA backup user e hdbuserstore

NetApp consiglia di configurare un utente di database dedicato nel database HANA per eseguire le operazioni di backup con SnapCenter. Nella seconda fase, per questo utente di backup viene configurata una chiave di archivio utente SAP HANA, che viene utilizzata nella configurazione del plug-in SAP HANA di SnapCenter.

La figura seguente mostra SAP HANA Studio attraverso il quale è possibile creare l'utente di backup

I privilegi richiesti vengono modificati con la release HANA 2.0 SPS5: Backup admin, lettura catalogo, database backup admin e database recovery operator. Per le versioni precedenti, sono sufficienti l'amministratore del backup e la lettura del catalogo.

Per un sistema SAP HANA MDC, è necessario creare l'utente nel database di sistema perché tutti i comandi di backup per il sistema e i database tenant vengono eseguiti utilizzando il database di sistema.



Il seguente comando viene utilizzato per la configurazione dell'archivio utente con <sid>adm utente:

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

SnapCenter utilizza <sid>adm Per comunicare con il database HANA. Pertanto, è necessario configurare la chiave di memorizzazione utente utilizzando l'utente <'sid>adm` sull'host del database. In genere, il software client SAP HANA hdbsql viene installato insieme all'installazione del server di database. In caso contrario, installare prima il client hdbclient.

In una configurazione di SAP HANA MDC, porta 3<instanceNo>13 È la porta standard per l'accesso SQL al database di sistema e deve essere utilizzata nella configurazione hdbuserstore.

Per una configurazione di più host SAP HANA, è necessario configurare le chiavi dell'archivio utente per tutti gli host. SnapCenter tenta di connettersi al database utilizzando ciascuna delle chiavi fornite e può quindi funzionare in modo indipendente dal failover di un servizio SAP HANA su un host diverso. Nella configurazione di laboratorio, abbiamo configurato una chiave di memorizzazione utente per l'utente pfxadm Per il nostro sistema PFX, che è un sistema HANA MDC a singolo host con un singolo tenant.

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

```

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

```

È possibile controllare l'accesso al database di sistema HANA che utilizza la chiave con `hdbsql` comando.

```

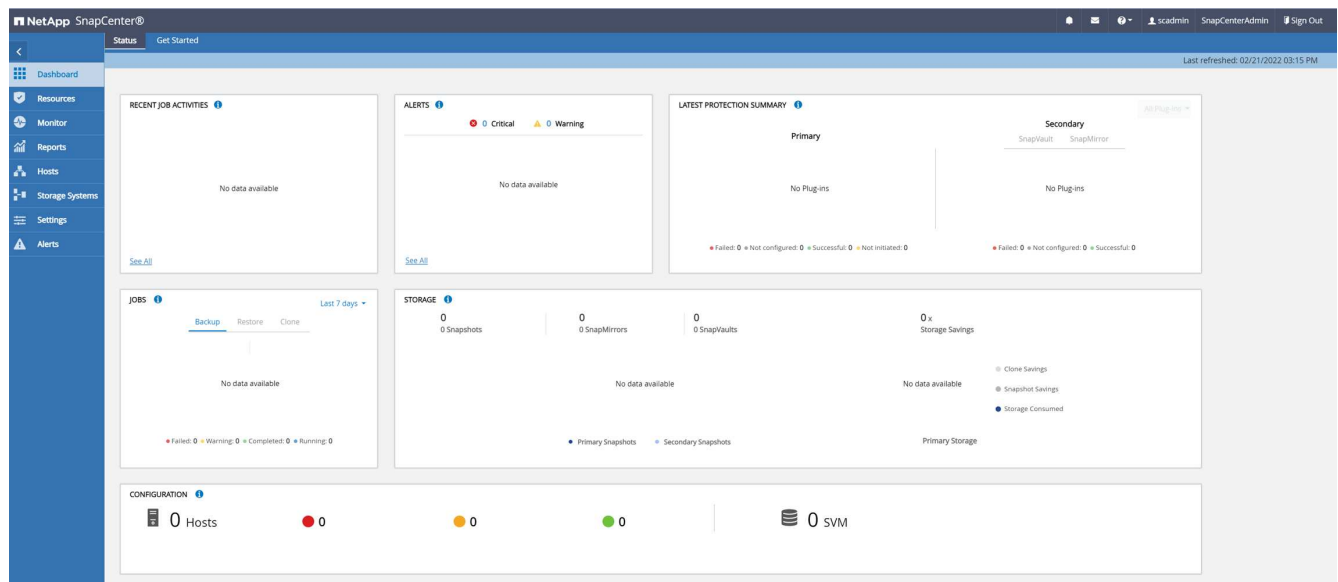
pfxadm@hana-1:/usr/sap/PFX/home> hdbsql -U PFXKEY
Welcome to the SAP HANA Database interactive terminal.
Type: \h for help with commands
      \q to quit
hdbsql SYSTEMDB=>

```

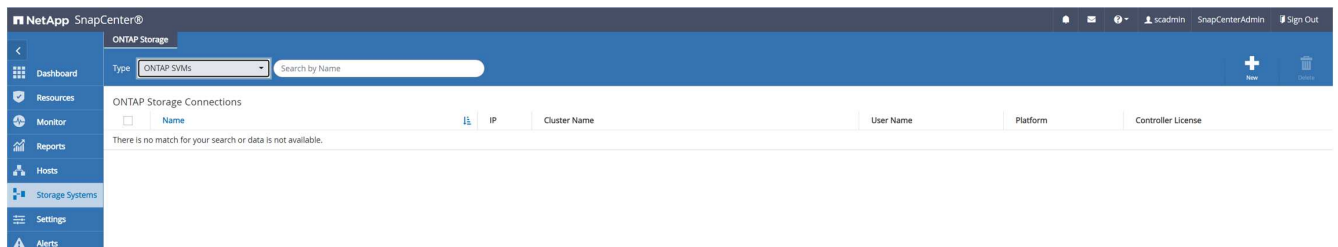
Configurare lo storage

Per configurare lo storage in SnapCenter, procedere come segue.

1. Nell'interfaccia utente di SnapCenter, selezionare sistemi storage.

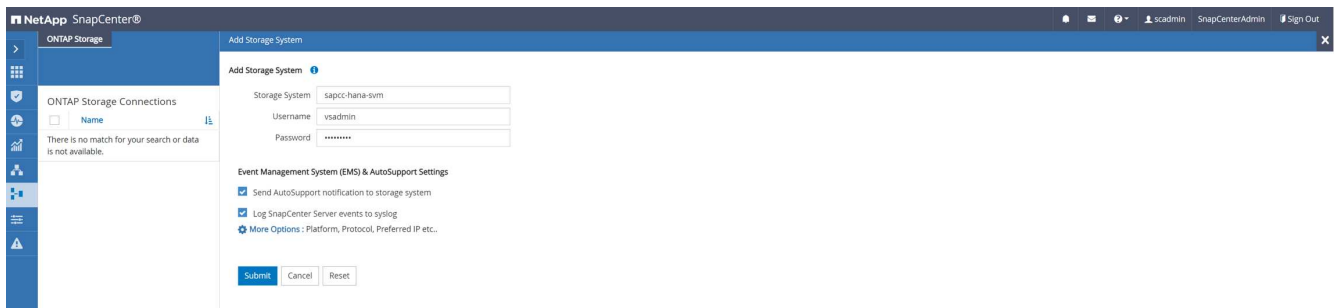


È possibile selezionare il tipo di sistema storage, che può essere SVM ONTAP o cluster ONTAP. Nell'esempio seguente, viene selezionata la gestione SVM.

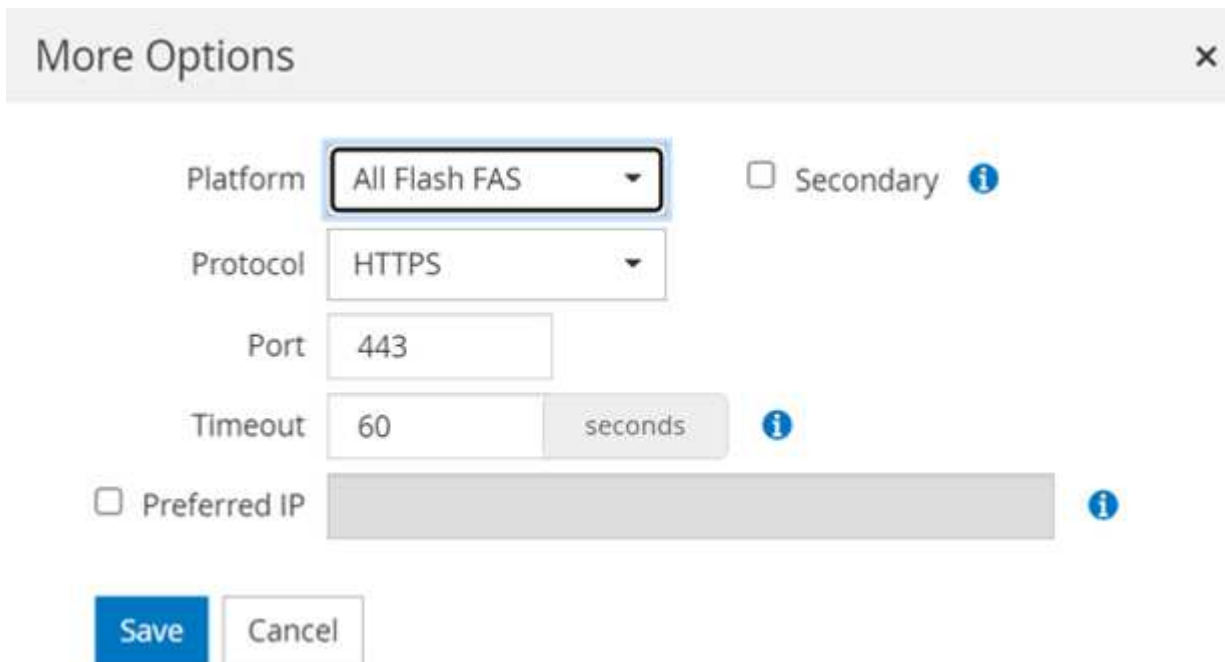


2. Per aggiungere un sistema storage e fornire il nome host e le credenziali richiesti, fare clic su New (nuovo).

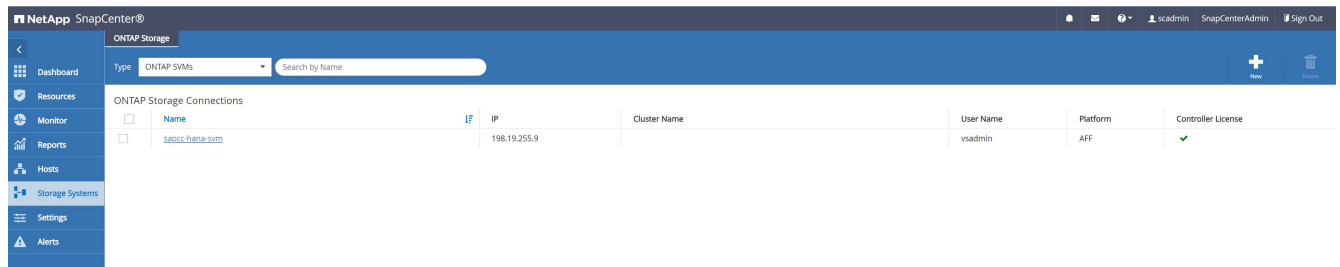
L'utente SVM non deve essere l'utente vsadmin, come mostrato nella figura seguente. In genere, un utente viene configurato sulla SVM e assegnato i permessi necessari per eseguire le operazioni di backup e ripristino. Per informazioni sui privilegi richiesti, vedere ["Guida all'installazione di SnapCenter"](#) Nella sezione intitolata "privilegi minimi ONTAP richiesti".



3. Per configurare la piattaforma di storage, fare clic su More Options (altre opzioni).
4. Selezionare All Flash FAS come sistema storage per garantire che la licenza, che fa parte di FSX per ONTAP, sia disponibile per SnapCenter.



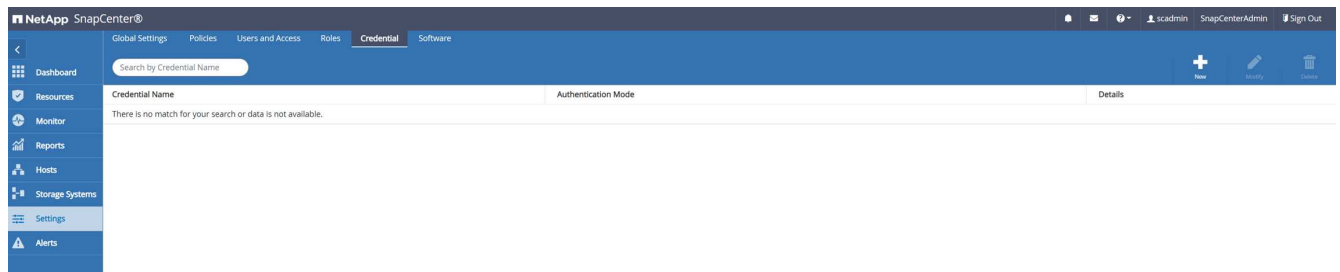
SVM sapcc-hana-svm È ora configurato in SnapCenter.



Creare le credenziali per la distribuzione del plug-in

Per consentire a SnapCenter di implementare i plug-in richiesti sugli host HANA, è necessario configurare le credenziali utente.

1. Accedere a Impostazioni, selezionare credenziali e fare clic su nuovo.



2. Nella configurazione di laboratorio, abbiamo configurato un nuovo utente, `snapcenter`, Sull'host HANA utilizzato per l'implementazione del plug-in. È necessario attivare sudo privileges, come mostrato nella figura seguente.

Credential

Credential Name

PluginOnLinux

Authentication Mode

Linux

Username

snapcenter

Password

.....

☒ Use sudo privileges

Cancel

OK

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

Aggiungere un host SAP HANA

Quando si aggiunge un host SAP HANA, SnapCenter implementa i plug-in richiesti sull'host del database ed esegue le operazioni di rilevamento automatico.

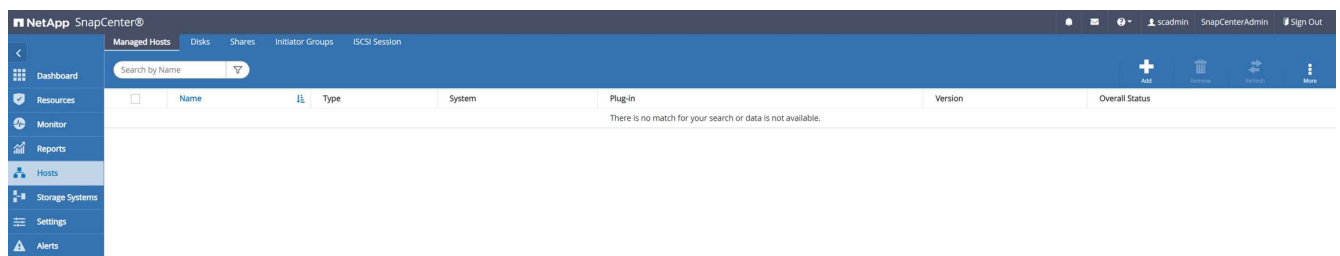
Il plug-in SAP HANA richiede Java a 64 bit versione 1.8. Java deve essere installato sull'host prima che l'host venga aggiunto a SnapCenter.

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

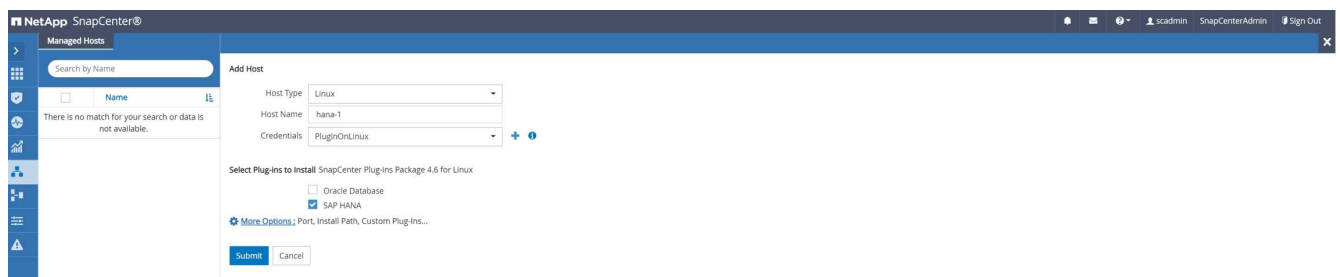
OpenJDK o Oracle Java è supportato con SnapCenter.

Per aggiungere l'host SAP HANA, attenersi alla seguente procedura:

1. Dalla scheda host, fare clic su Add (Aggiungi).



2. Fornire informazioni sull'host e selezionare il plug-in SAP HANA da installare. Fare clic su Invia.



3. Confermare l'impronta digitale.

Confirm Fingerprint

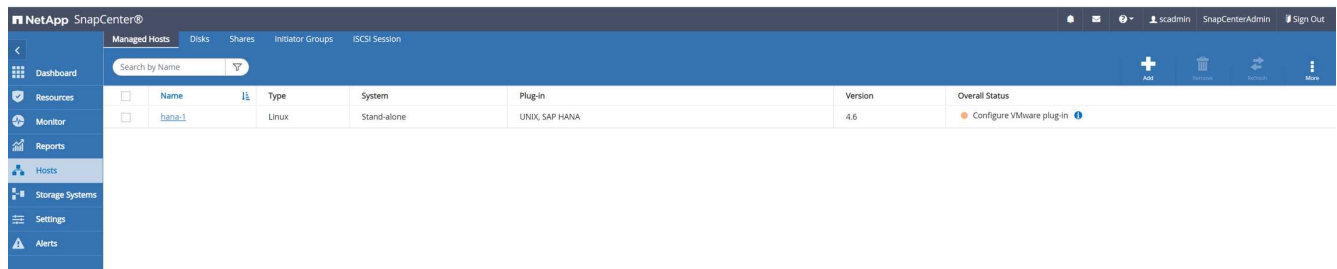
Authenticity of the host cannot be determined

Host name	Fingerprint	Valid
hana-1	ssh-rsa 3072 2A:98:DB:7E:58:A3:7E:51:06:79:83:C6:9D:BA:8E:69	

Confirm and SubmitClose

L'installazione di HANA e del plug-in Linux si avvia automaticamente. Al termine dell'installazione, la colonna di stato dell'host mostra Configure VMware Plug-in (Configura plug-in VMware). SnapCenter rileva se il plug-in SAP HANA è installato in un ambiente virtualizzato. Potrebbe trattarsi di un ambiente VMware o di un ambiente di un provider di cloud pubblico. In questo caso, SnapCenter visualizza un avviso per configurare l'hypervisor.

Per rimuovere il messaggio di avviso, procedere come segue.



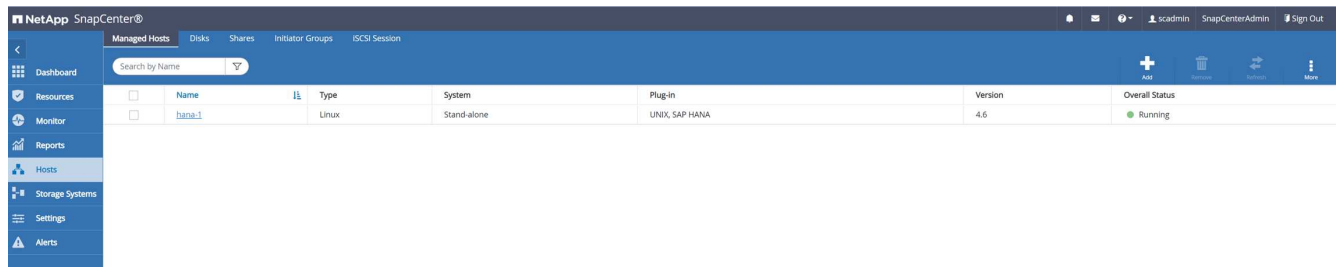
Name	Type	System	Plug-in	Version	Overall Status
hana-1	Linux	Stand-alone	UNIX, SAP HANA	4.6	Configure VMware plug-in

- Dalla scheda Settings (Impostazioni), selezionare Global Settings (Impostazioni globali).
- Per le impostazioni dell'hypervisor, selezionare VM con iSCSI Direct Attached Disk o NFS per tutti gli host e aggiornare le impostazioni.



Global Settings
Hypervisor Settings
<input checked="" type="checkbox"/> VMs have iSCSI direct attached disks or NFS for all the hosts Update
Notification Server Settings
Configuration Settings
Purge Jobs Settings
Domain Settings
CA Certificate Settings
Disaster Recovery

La schermata mostra il plug-in Linux e il plug-in HANA con lo stato in esecuzione.



Configurare i criteri

Le policy sono in genere configurate indipendentemente dalla risorsa e possono essere utilizzate da più database SAP HANA.

Una configurazione minima tipica è costituita dai seguenti criteri:

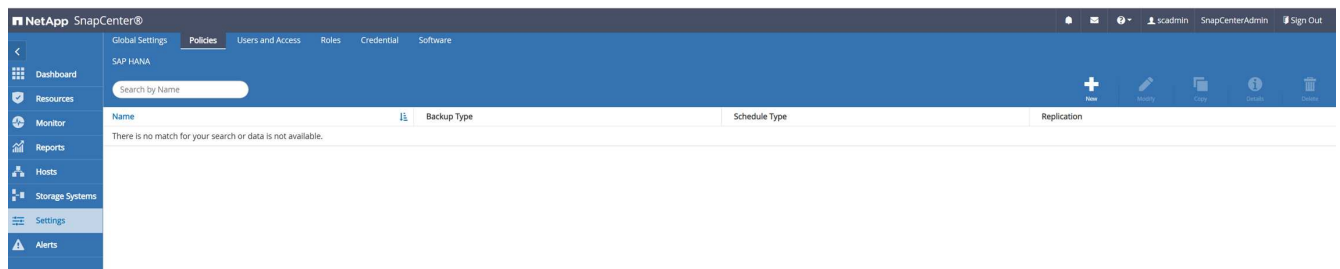
- Policy per backup orari senza replica: LocalSnap.
- Policy per il controllo settimanale dell'integrità dei blocchi utilizzando un backup basato su file: BlockIntegrityCheck.

Le sezioni seguenti descrivono la configurazione di questi criteri.

Policy per i backup Snapshot

Per configurare le policy di backup di Snapshot, procedere come segue.

1. Accedere a Impostazioni > Criteri e fare clic su nuovo.



2. Immettere il nome e la descrizione della policy. Fare clic su Avanti.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Provide a policy name

Policy name: LocalSnap

Details: Snapshot backup at primary volume

3. Selezionare il tipo di backup basato su Snapshot e selezionare orario per la frequenza di pianificazione.

La pianificazione viene configurata in seguito con la configurazione di protezione delle risorse HANA.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select backup settings

Backup Type ☒ Snapshot Based ☐ File-Based

Schedule Frequency

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

☐ On demand

☒ Hourly

☐ Daily

☐ Weekly

☐ Monthly

4. Configurare le impostazioni di conservazione per i backup on-demand.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Retention settings

Hourly retention settings

☒ Total Snapshot copies to keep 7

☐ Keep Snapshot copies for 14 days

5. Configurare le opzioni di replica. In questo caso, non è selezionato alcun aggiornamento di SnapVault o SnapMirror.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select secondary replication options

☐ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label Choose

Error retry count 3

New SAP HANA Backup Policy ✕

1 Name

2 Settings

3 Retention

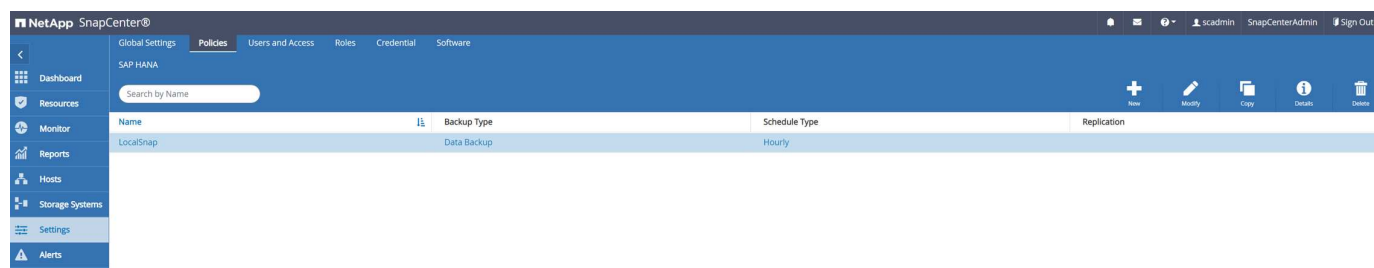
4 Replication

5 Summary

Summary

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

Il nuovo criterio è ora configurato.



Policy per il controllo dell'integrità del blocco

Per configurare il criterio di controllo dell'integrità del blocco, procedere come segue.

1. Accedere a Impostazioni > Criteri e fare clic su nuovo.
2. Immettere il nome e la descrizione della policy. Fare clic su Avanti.

New SAP HANA Backup Policy ✕

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Provide a policy name

Policy name	<input type="text" value="BlockIntegrityCheck"/>
Details	<input type="text" value="Check HANA DB blocks using file-based backup"/>

3. Impostare il tipo di backup su file-based (basato su file) e la frequenza di pianificazione su Weekly (settimanale). La pianificazione viene configurata in seguito con la configurazione di protezione delle risorse HANA.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary

Select backup settings

Backup Type

☐ Snapshot Based
☒ File-Based

Schedule Frequency

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

☐ On demand
☐ Hourly
☐ Daily
☒ Weekly
☐ Monthly

4. Configurare le impostazioni di conservazione per i backup on-demand.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary

Retention settings

Weekly retention settings

☒ Total backup copies to keep

1

☐ Keep backup copies for

14

days

5. Nella pagina Riepilogo, fare clic su fine.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary

Summary

Policy name

BlockIntegrityCheck

Details

Check HANA DB blocks using file-based backup

Backup Type

File-Based Backup

Schedule Type

Weekly

Weekly backup retention

Total backup copies to retain : 1

NetApp SnapCenter®

Global Settings

Policies

Users and Access

Roles

Credential

Software

SAP HANA

Search by Name

+

✎

📄

ℹ

🗑

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

Dashboard

Resources

Monitor

Reports

Hosts

Storage Systems

Settings

Alerts

scadmin

SnapCenterAdmin

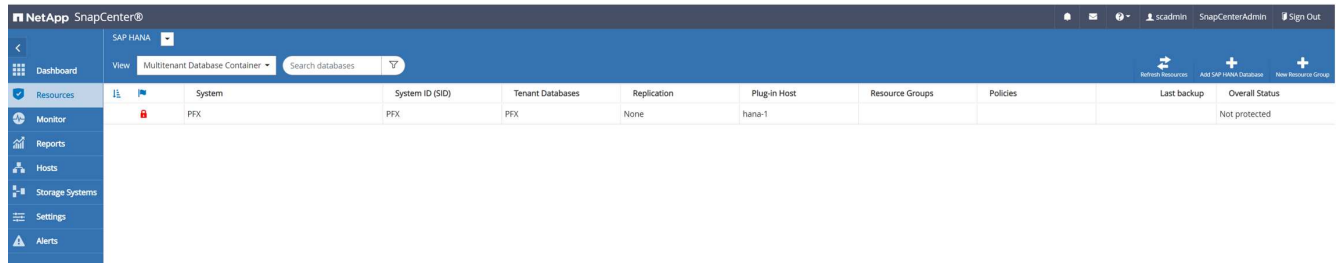
Sign Out

Configurare e proteggere una risorsa HANA

Dopo l'installazione del plug-in, il processo di rilevamento automatico della risorsa HANA viene avviato automaticamente. Nella schermata Resources (risorse) viene creata una nuova risorsa, contrassegnata come bloccata con l'icona del lucchetto rosso. Per configurare e proteggere la nuova risorsa HANA, attenersi alla seguente procedura:

1. Selezionare e fare clic sulla risorsa per continuare la configurazione.

È inoltre possibile attivare manualmente il processo di rilevamento automatico nella schermata risorse facendo clic su Aggiorna risorse.



2. Fornire la chiave dell'archivio utenti per il database HANA.

Configure Database

Plug-in host

hana-1

HDBSQL OS User

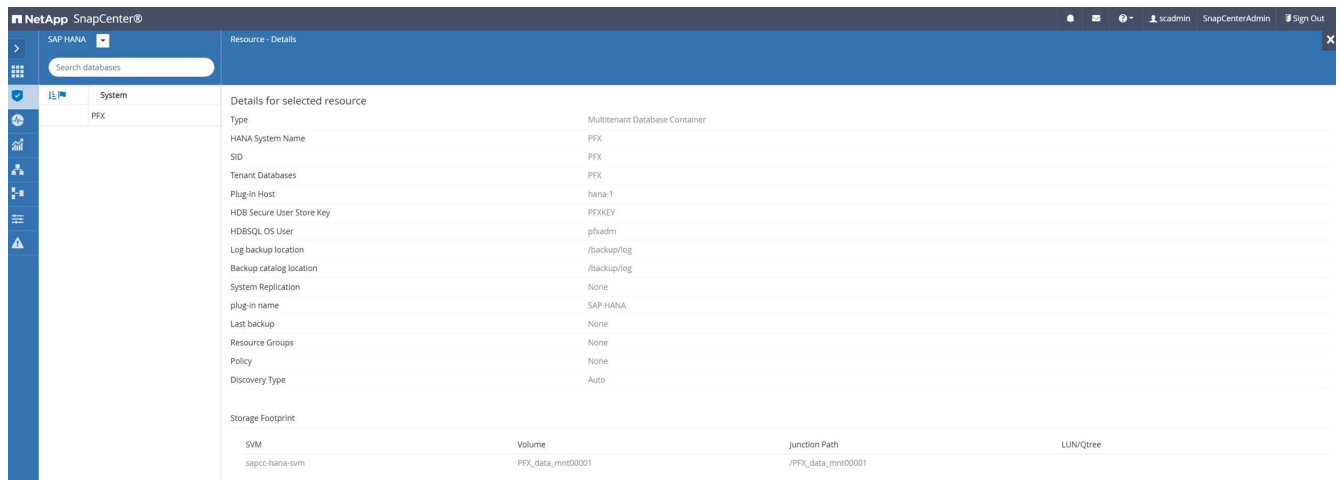
pfxadm

HDB Secure User Store Key

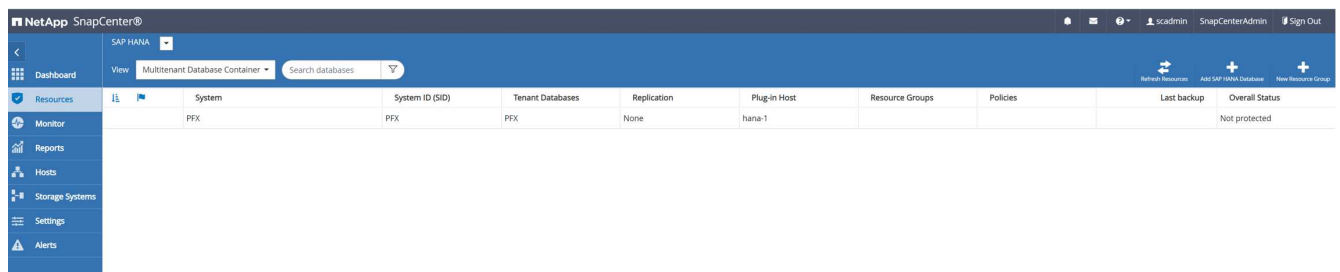
Cancel

OK

Viene avviato il processo di rilevamento automatico di secondo livello in cui vengono rilevate le informazioni relative ai dati del tenant e all'impatto dello storage.

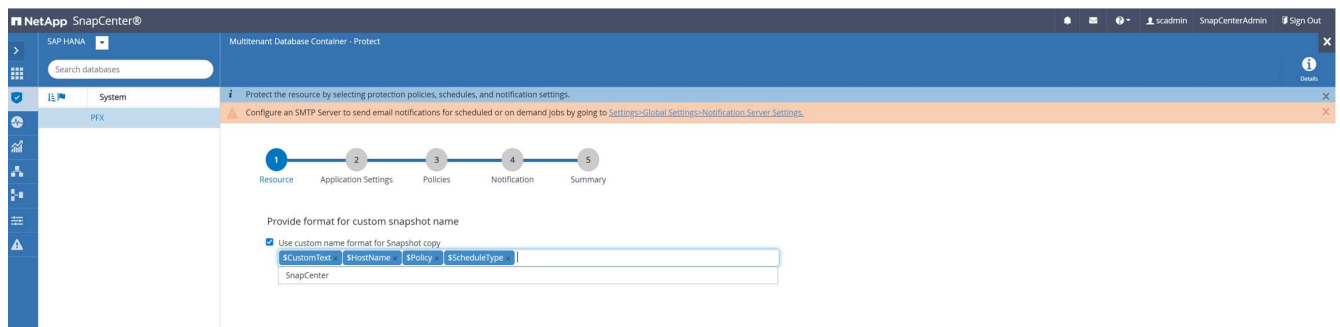


3. Dalla scheda Resources (risorse), fare doppio clic sulla risorsa per configurare la protezione delle risorse.

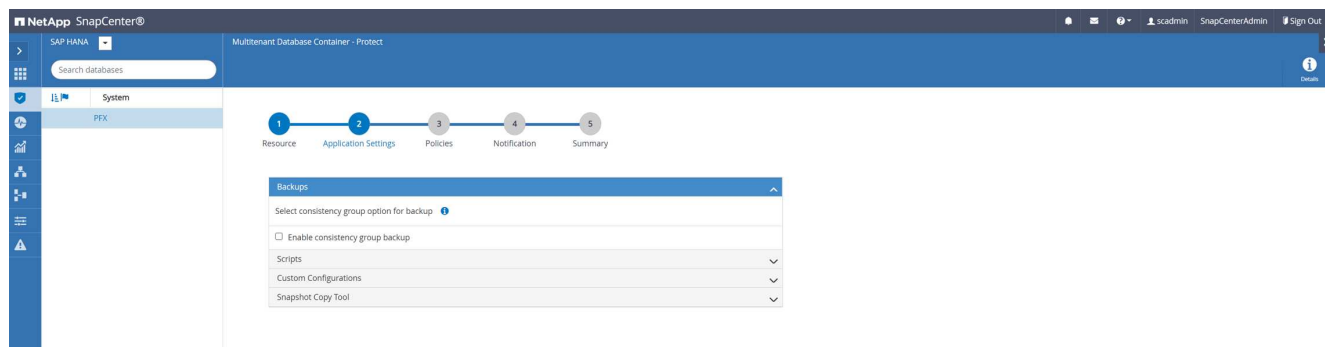


4. Configurare un formato nome personalizzato per la copia Snapshot.

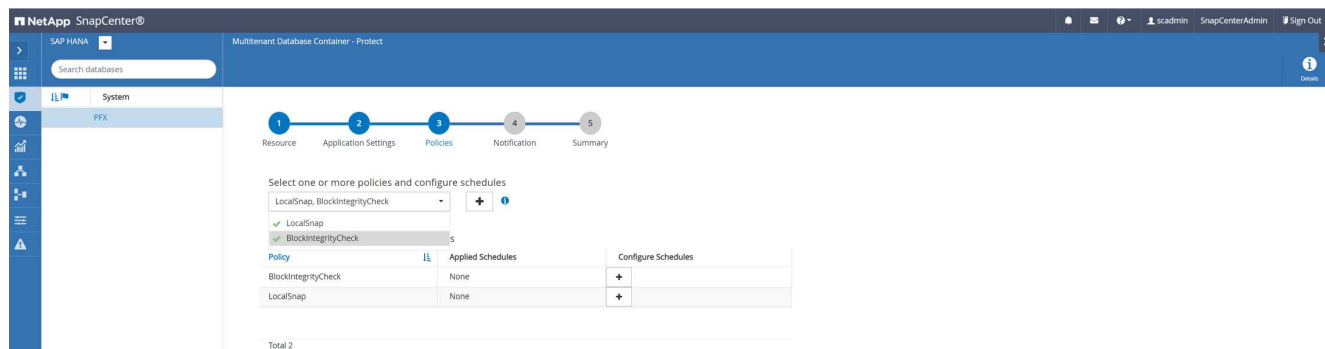
NetApp consiglia di utilizzare un nome di copia Snapshot personalizzato per identificare facilmente i backup creati con quale tipo di policy e pianificazione. Aggiungendo il tipo di pianificazione nel nome della copia Snapshot, è possibile distinguere tra backup pianificati e su richiesta. Il `schedule` name la stringa per i backup on-demand è vuota, mentre i backup pianificati includono la stringa `Hourly`, `Daily`, or `Weekly`.



5. Non è necessario impostare impostazioni specifiche nella pagina Impostazioni applicazione. Fare clic su Avanti.



6. Selezionare i criteri da aggiungere alla risorsa.



7. Definire la pianificazione per la policy di controllo dell'integrità del blocco.

In questo esempio, viene impostato per una volta alla settimana.

Add schedules for policy BlockIntegrityCheck



Weekly

Start date

02/22/2022 12:00 pm



☐ Expires on

03/22/2022 12:00 pm



Days

Sunday

✓ Sunday

Monday

Tuesday

Wednesday

Thursday

Friday



The schedules are triggered in the SnapCenter Server time zone.



Cancel

OK

8. Definire la pianificazione per la policy Snapshot locale.

In questo esempio, viene impostato ogni 6 ore.

Modify schedules for policy LocalSnap



Hourly

Start date

02/22/2022 02:00 pm



☐ Expires on

04/28/2022 11:57 am



Repeat every

6

hours

0

mins



The schedules are triggered in the SnapCenter Server time zone.



Cancel

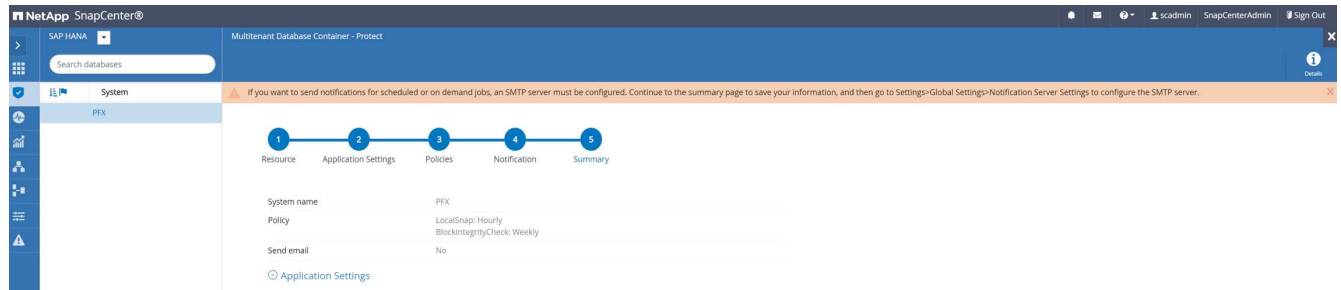
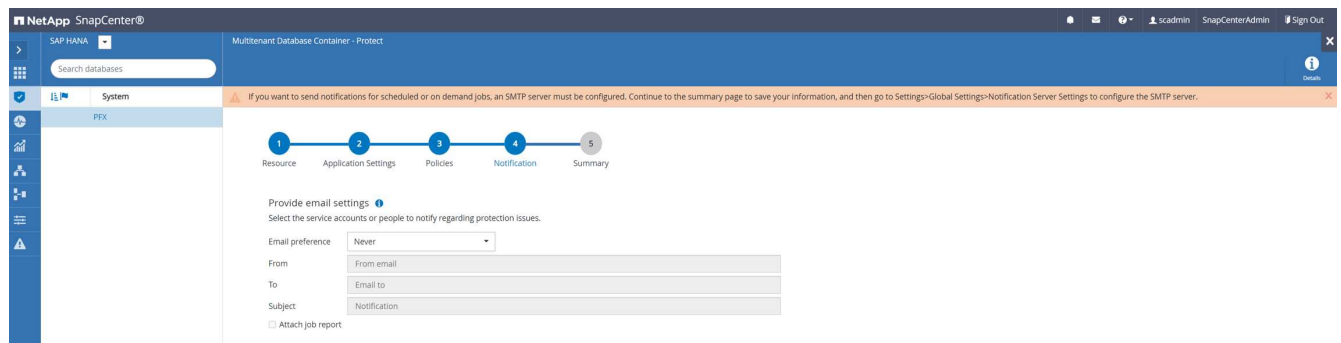
OK

The screenshot shows the NetApp SnapCenter interface. The left sidebar contains navigation icons for System, PFX, and other resources. The main area displays a progress bar with five steps: 1. Resource, 2. Application Settings, 3. Policies, 4. Notification, and 5. Summary. Below the progress bar, there is a section titled 'Select one or more policies and configure schedules' with a dropdown menu showing 'LocalSnap, BlockIntegrityCheck'. Below this, there is a table titled 'Configure schedules for selected policies'.

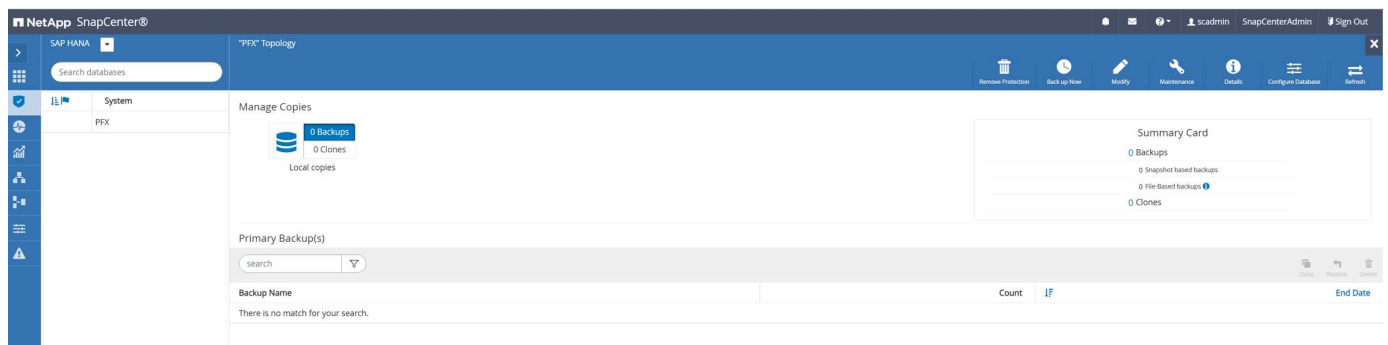
Policy	Applied Schedules	Configure Schedules
BlockIntegrityCheck	Weekly; Run on days: Sunday	
LocalSnap	Hourly; Repeat every 6 hours	

Total 2

9. Fornire informazioni sulla notifica via email.



La configurazione delle risorse HANA è stata completata ed è possibile eseguire i backup.



Operazioni di backup di SnapCenter

Puoi creare un backup Snapshot on-demand e un'operazione di controllo dell'integrità dei blocchi on-demand.

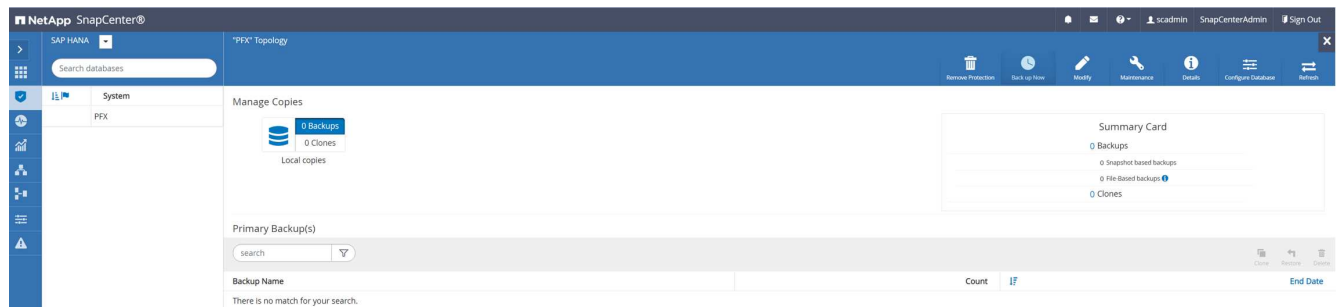
Crea un backup Snapshot on-demand

Segui questi passaggi per creare backup Snapshot on-demand.

1. Nella vista Resource (risorse), selezionare la risorsa e fare doppio clic sulla riga per passare alla vista Topology (topologia).

La vista topologia delle risorse offre una panoramica di tutti i backup disponibili creati utilizzando SnapCenter. L'area superiore di questa vista visualizza la topologia di backup che mostra i backup sullo storage primario (copie locali) e, se disponibile, sullo storage di backup off-site (copie del vault).

2. Nella riga superiore, selezionare l'icona Backup Now per avviare un backup on-demand.



3. Dall'elenco a discesa, selezionare il criterio di backup LocalSnap, Quindi fare clic su Backup per avviare il backup on-demand.

Backup

Create a backup for the selected resource

Resource Name

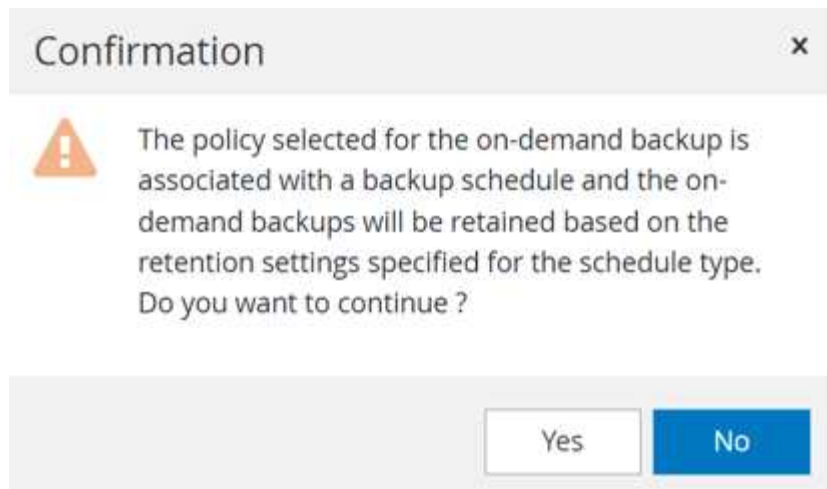
PFX

Policy

LocalSnap

Cancel

Backup



Un registro dei cinque job precedenti viene visualizzato nell'area Activity (attività) nella parte inferiore della vista Topology (topologia).

4. I dettagli della commessa vengono visualizzati facendo clic sulla riga dell'attività della commessa nell'area Activity (attività). È possibile aprire un registro dettagliato dei processi facendo clic su View Logs (Visualizza registri)

Job Details

Backup of Resource Group 'hana-1_hana_MDC_PFX' with policy 'LocalSnap'

✓ ▾ Backup of Resource Group 'hana-1_hana_MDC_PFX' with policy 'LocalSnap'

✓ ▾ hana-1

✓ Backup

✓ ▶ Validate Dataset Parameters

✓ ▶ Validate Plugin Parameters

✓ ▶ Complete Application Discovery

✓ ▶ Initialize Filesystem Plugin

✓ ▶ Discover Filesystem Resources

✓ ▶ Validate Retention Settings

✓ ▶ Quiesce Application

✓ ▶ Quiesce Filesystem

✓ ▶ Create Snapshot

✓ ▶ UnQuiesce Filesystem

✓ ▶ UnQuiesce Application

✓ ▶ Get Snapshot Details

✓ ▶ Get Filesystem Meta Data

✓ ▶ Finalize Filesystem Plugin

✓ ▶ Collect Autosupport data

✓ ▶ Register Backup and Apply Retention

✓ ▶ Register Snapshot attributes

✓ ▶ Application Clean-Up

✓ ▶ Data Collection

✓ ▶ Agent Finalize Workflow

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

View Logs

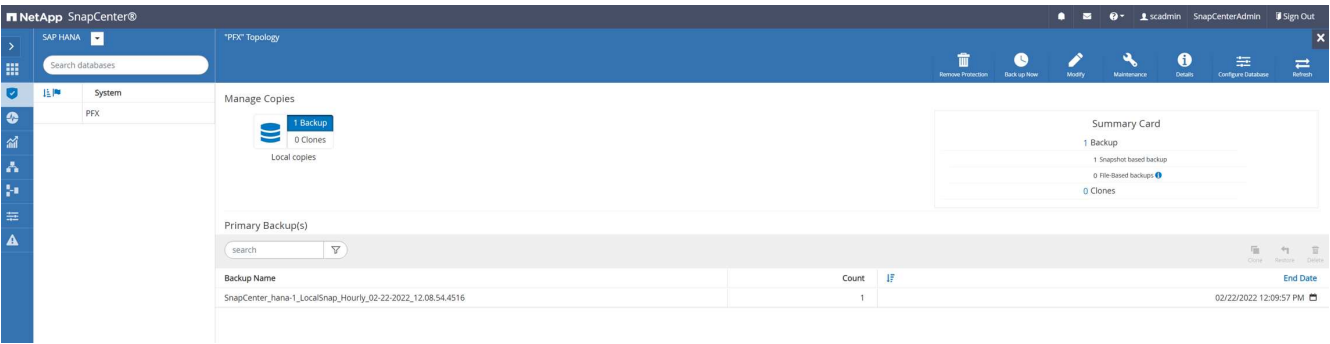
Cancel Job

Close

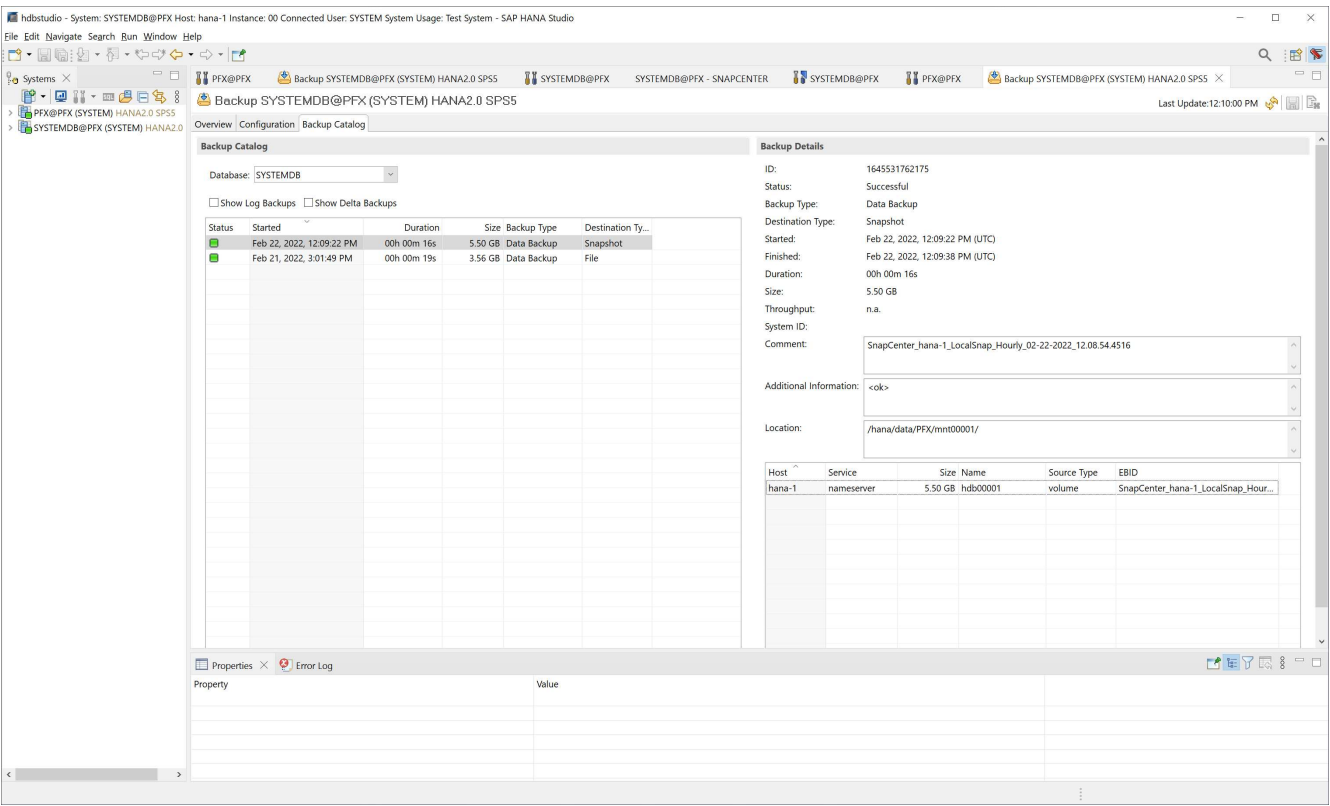
Al termine del backup, viene visualizzata una nuova voce nella vista della topologia. I nomi dei backup seguono la stessa convenzione di denominazione del nome Snapshot definito nella sezione ["Configurazione e protezione di una risorsa HANA".](#)

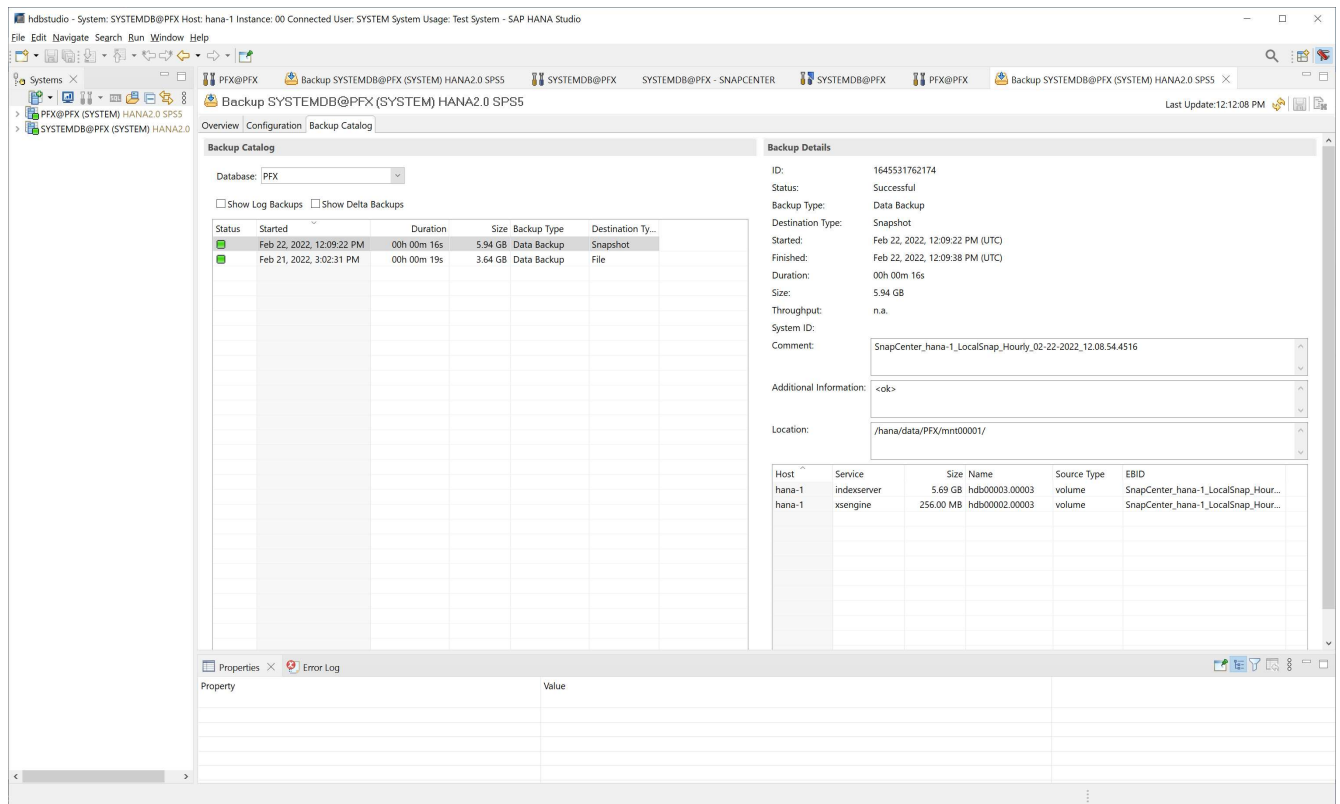
31

Per visualizzare l'elenco di backup aggiornato, è necessario chiudere e riaprire la vista della topologia.



Nel catalogo di backup SAP HANA, il nome del backup SnapCenter viene memorizzato come a. Comment oltre al campo External Backup ID (EBID). Questo è mostrato nella figura seguente per il database di sistema e nella figura successiva per il database tenant PFX.





Nel file system FSX per ONTAP, è possibile elencare i backup Snapshot collegandosi alla console di SVM.

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

Creare un'operazione di verifica dell'integrità dei blocchi on-demand

Un'operazione di verifica dell'integrità dei blocchi on-demand viene eseguita allo stesso modo di un processo di backup Snapshot, selezionando la policy BlockIntegrityCheck. Quando si pianificano i backup utilizzando questo criterio, SnapCenter crea un backup standard del file SAP HANA per i database del sistema e del tenant.

Backup



Create a backup for the selected resource

Resource Name

PFX

Policy

BlockIntegrityCheck



Cancel

Backup

Job Details

Backup of Resource Group 'hana-1_hana_MDC_PFX' with policy 'BlockIntegrityCheck'

✓ ▾ Backup of Resource Group 'hana-1_hana_MDC_PFX' with policy 'BlockIntegrityCheck'

✓ ▾ hana-1

✓ ▾ File-Based Backup

✓ ▶ Validate Plugin Parameters

✓ ▶ Start File-Based Backup

✓ ▶ Check File-Based Backup

✓ ▶ Register Backup and Apply Retention

✓ ▶ Data Collection

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

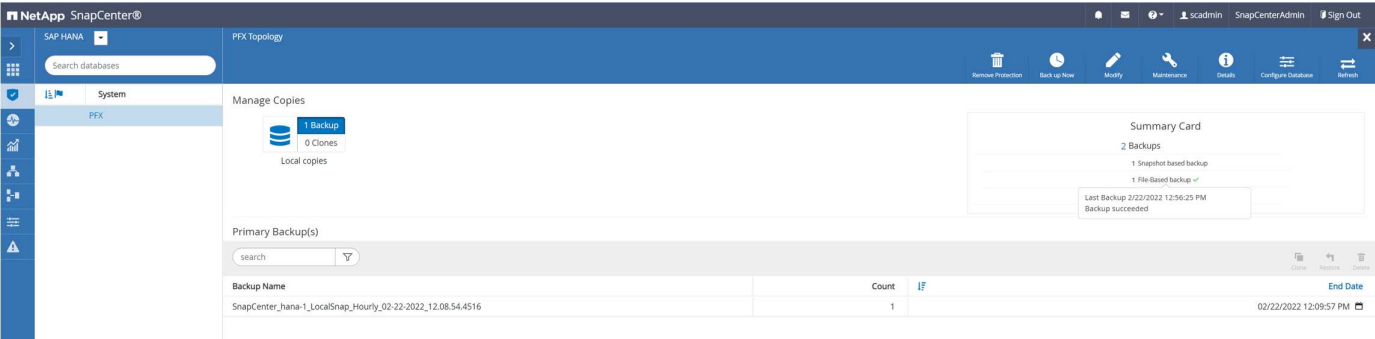
View Logs

Cancel Job

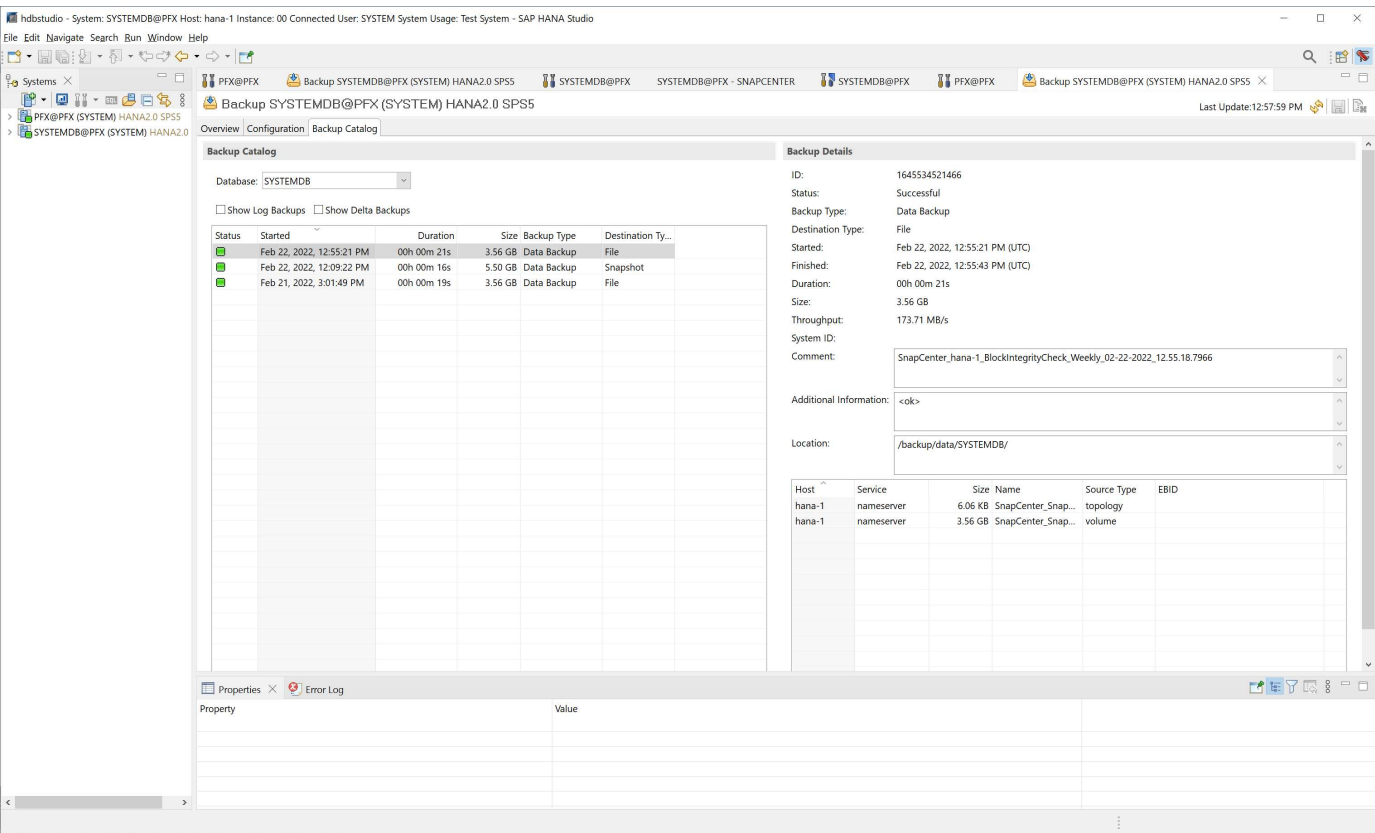
Close

SnapCenter non visualizza il controllo dell'integrità del blocco allo stesso modo dei backup basati su copia

Snapshot. La scheda di riepilogo mostra invece il numero di backup basati su file e lo stato del backup precedente.



Il catalogo di backup SAP HANA mostra le voci per i database di sistema e tenant. Le seguenti figure mostrano il controllo dell'integrità del blocco SnapCenter nel catalogo di backup del sistema e nel database tenant.



hdbstudio - System: SYSTEMDB@PFX Host: hana-1 Instance: 00 Connected User: SYSTEM System Usage: Test System - SAP HANA Studio

File Edit Navigate Search Run Window Help

Systems

Backup SYSTEMDB@PFX (SYSTEM) HANA2.0 SPS5

Last Update: 12:58:19 PM

Overview Configuration Backup Catalog

Database: PFX

☐ Show Log Backups ☐ Show Delta Backups

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

Backup Details

ID: 1645534534230

Status: Successful

Backup Type: Data Backup

Destination Type: File

Started: Feb 22, 2022, 12:55:34 PM (UTC)

Finished: Feb 22, 2022, 12:56:01 PM (UTC)

Duration: 00h 00m 27s

Size: 3.64 GB

Throughput: 138.07 MB/s

System ID:

Comment: SnapCenter_hana-1_BlockIntegrityCheck_Weekly_02-22-2022_12:55:18.7966

Additional Information: <ok>

Location: /backup/data/DB_PFX/

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

Properties Error Log

Property Value

Un controllo dell'integrità dei blocchi consente di creare file di backup dei dati SAP HANA standard. SnapCenter utilizza il percorso di backup configurato con il database HANA per le operazioni di backup dei dati basate su file.

```

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

```

Backup di volumi non dati

Il backup dei volumi non dati è parte integrante di SnapCenter e del plug-in SAP HANA.

La protezione del volume di dati del database è sufficiente per ripristinare e ripristinare il database SAP HANA in un dato momento, a condizione che le risorse di installazione del database e i registri richiesti siano ancora disponibili.

Per eseguire il ripristino da situazioni in cui devono essere ripristinati altri file non di dati, NetApp consiglia di sviluppare una strategia di backup aggiuntiva per i volumi non di dati per aumentare il backup del database

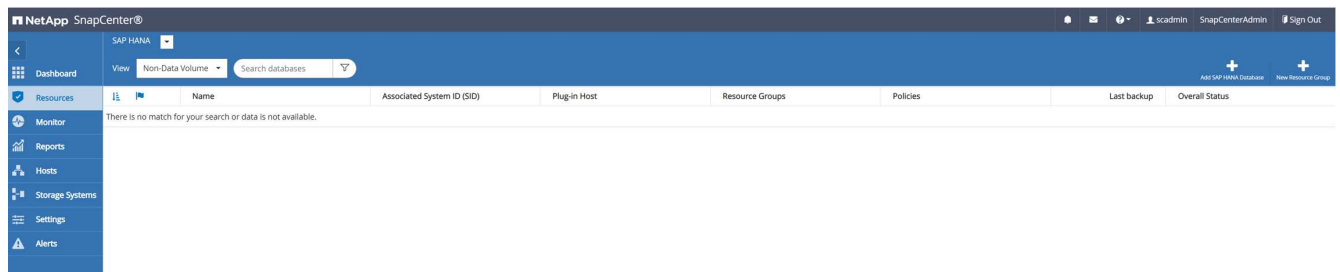
SAP HANA. A seconda dei requisiti specifici, il backup dei volumi non dati potrebbe differire in termini di frequenza di pianificazione e impostazioni di conservazione e si dovrebbe considerare la frequenza con cui i file non dati vengono modificati. Ad esempio, il volume HANA /hana/shared Contiene file eseguibili ma anche file di traccia SAP HANA. Mentre gli eseguibili cambiano solo quando il database SAP HANA viene aggiornato, i file di traccia SAP HANA potrebbero richiedere una frequenza di backup più elevata per supportare l'analisi delle situazioni problematiche con SAP HANA.

Il backup dei volumi non dati di SnapCenter consente di creare copie Snapshot di tutti i volumi rilevanti in pochi secondi con la stessa efficienza dello spazio dei backup dei database SAP HANA. La differenza è che non è richiesta alcuna comunicazione SQL con il database SAP HANA.

Configurare le risorse di volumi diversi dai dati

Per configurare le risorse non relative ai volumi di dati, attenersi alla seguente procedura:

1. Dalla scheda Resources (risorse), selezionare non-Data-Volume e fare clic su Add SAP HANA Database (Aggiungi database SAP HANA).



2. Nella fase uno della finestra di dialogo Add SAP HANA Database (Aggiungi database SAP HANA), nell'elenco Resource Type (tipo di risorsa), selezionare non-data Volumes (volumi non dati). Specificare un nome per la risorsa, il SID associato e l'host del plug-in SAP HANA che si desidera utilizzare per la risorsa, quindi fare clic su Avanti.

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Resource Details

Resource Type

Non-data Volume

Resource Name

PFX-Shared-Volume

Associated SID

PFX

Plug-In Host

hana-1

Previous

Next

3. Aggiungere la SVM e il volume di storage come footprint dello storage, quindi fare clic su Next (Avanti).

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Storage Footprint Details

Storage Type

☒ ONTAP

Add Storage Footprint

Storage System

sapcc-hana-svm

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

Volume name

PFX_shared

LUNs or Qtrees

Default is 'None' or type to find

Save

Previous

Next

4. Per salvare le impostazioni, nella fase di riepilogo, fare clic su fine.

Add SAP HANA Database

1 Name
2 Storage Footprint
3 Summary

Summary

Resource Type	Non-data Volume
Resource Name	PFX-Shared-Volume
Associated SID	PFX
Plug-in Host	hana-1

Storage Footprint

Storage System	Volume	LUN/Qtree
sapcc-hana-svm	PFX_shared	

Previous
Finish

Il nuovo volume non di dati viene ora aggiunto a SnapCenter. Fare doppio clic sulla nuova risorsa per eseguire la protezione delle risorse.

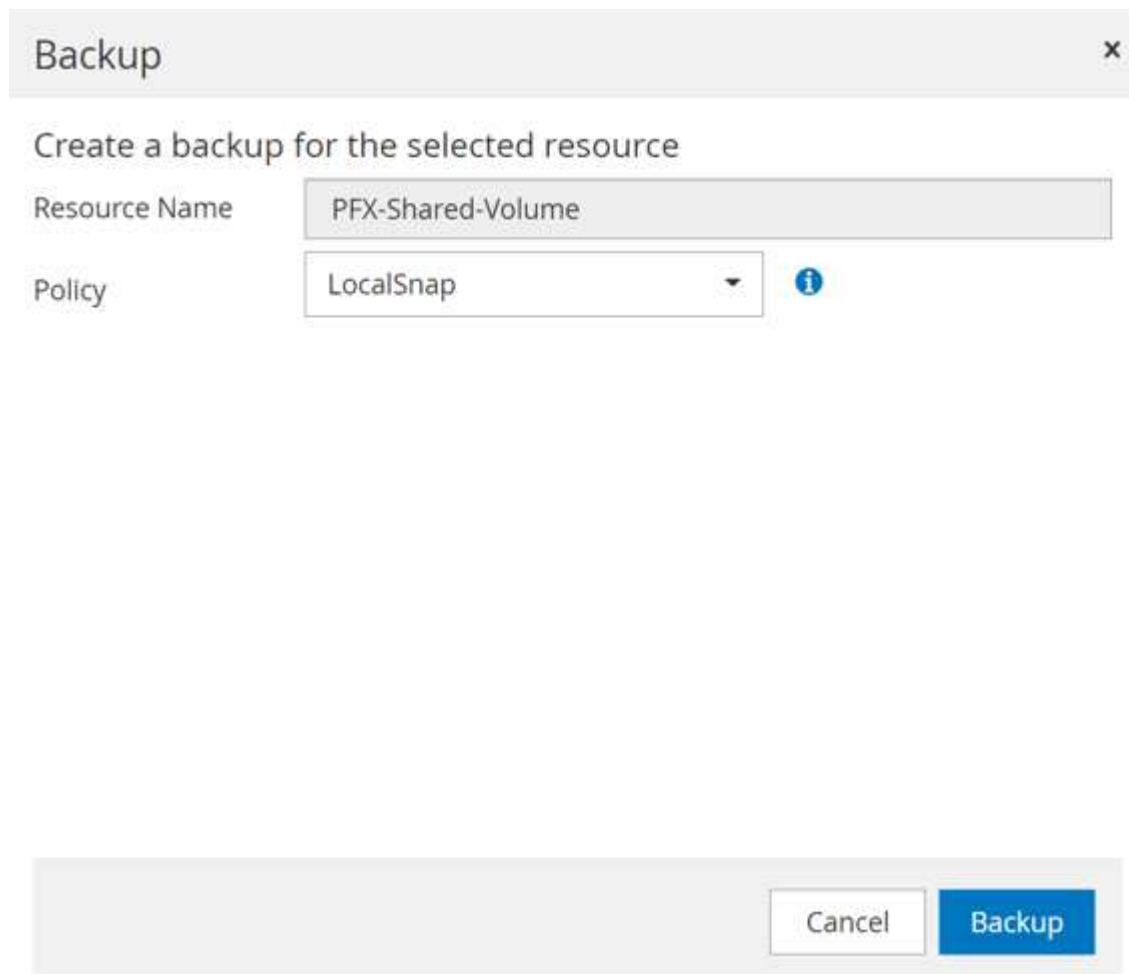
NetApp SnapCenter®								
SAP HANA								
View: Non-Data Volume Search databases								
Resources		Name	Associated System ID (SID)	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
		PFX-Shared-Volume	PFX	hana-1				Not protected

La protezione delle risorse viene eseguita nello stesso modo descritto in precedenza con una risorsa di database HANA.

5. È ora possibile eseguire un backup facendo clic su Backup Now (Esegui backup ora).



6. Selezionare il criterio e avviare l'operazione di backup.



Il log dei lavori di SnapCenter mostra le singole fasi del flusso di lavoro.

Job Details



Backup of Resource Group 'hana-1_hana_NonDataVolume_PFX_PFX-Shared-Volume' with policy 'LocalSnap'

✓ ▾ Backup of Resource Group 'hana-1_hana_NonDataVolume_PFX_PFX-Shared-Volume' with policy 'LocalSnap'

✓ ▾ hana-1

✓ ▾ Backup

- ✓ ▶ Validate Dataset Parameters
- ✓ ▶ Validate Plugin Parameters
- ✓ ▶ Validate Retention Settings
- ✓ ▶ Create Snapshot
- ✓ ▶ Get Snapshot Details
- ✓ ▶ Collect Autosupport data
- ✓ ▶ Register Backup and Apply Retention
- ✓ ▶ Register Snapshot attributes
- ✓ ▶ Data Collection
- ✓ ▶ Agent Finalize Workflow

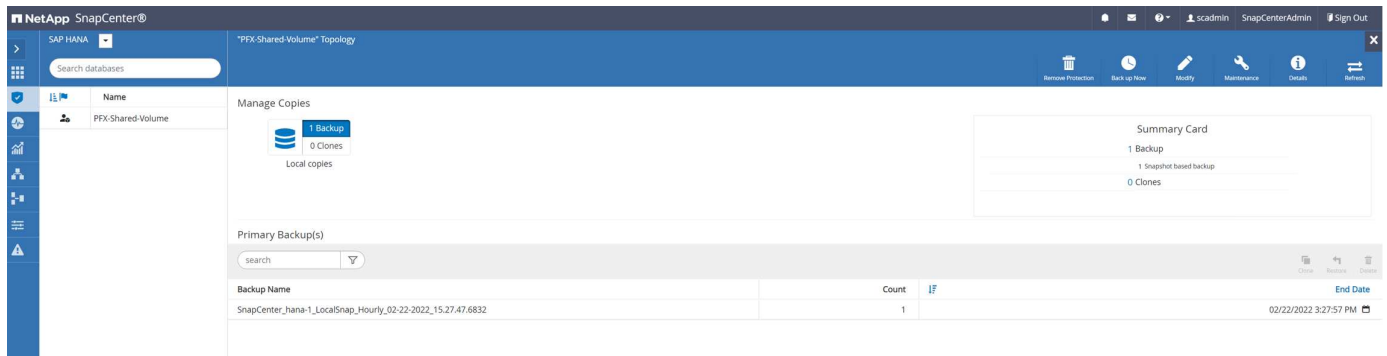
i Task Name: Backup Start Time: 02/22/2022 3:27:48 PM End Time:

View Logs

Cancel Job

Close

Il nuovo backup è ora visibile nella vista delle risorse della risorsa non del volume di dati.



Ripristinare e ripristinare

Con SnapCenter, sono supportate operazioni di ripristino e ripristino automatico per i sistemi MDC HANA a host singolo con un singolo tenant. Per sistemi con più host o sistemi MDC con più tenant, SnapCenter esegue solo l'operazione di ripristino ed è necessario eseguire il ripristino manualmente.

È possibile eseguire un'operazione di ripristino e ripristino automatico con i seguenti passaggi:

1. Selezionare il backup da utilizzare per l'operazione di ripristino.
2. Selezionare il tipo di ripristino. Selezionare Ripristino completo con ripristino del volume o senza ripristino del volume.
3. Selezionare il tipo di ripristino tra le seguenti opzioni:
 - Allo stato più recente
 - Point-in-time
 - A backup di dati specifici
 - Nessun ripristino

Il tipo di ripristino selezionato viene utilizzato per il ripristino del sistema e del database tenant.

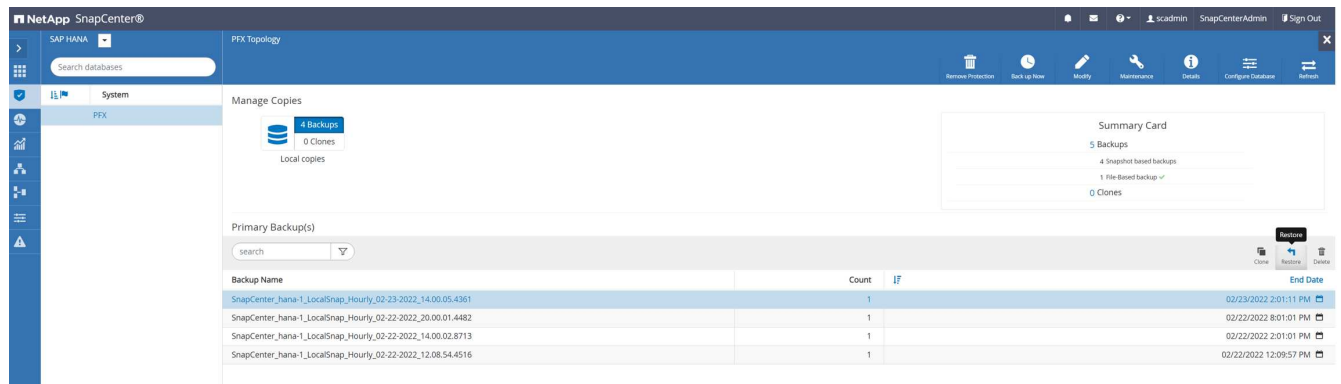
Successivamente, SnapCenter esegue le seguenti operazioni:

1. Interrompe il database HANA.
2. Ripristina il database. A seconda del tipo di ripristino selezionato, vengono eseguite diverse operazioni.
 - Se si seleziona l'opzione di ripristino del volume, SnapCenter disinstalla il volume, ripristina il volume utilizzando SnapRestore basato sul volume sul layer di storage e monta il volume.
 - Se l'opzione di ripristino del volume non è selezionata, SnapCenter ripristina tutti i file utilizzando le operazioni SnapRestore del singolo file sul layer di storage.
3. Recupera il database:
 - a. Ripristinando il database di sistema
 - b. ripristino del database tenant
 - c. Avvio del database HANA

Se si seleziona No Recovery (Nessun ripristino), SnapCenter viene chiuso ed è necessario eseguire manualmente l'operazione di ripristino per il sistema e il database tenant.

Per eseguire un'operazione di ripristino manuale, attenersi alla seguente procedura:

1. Selezionare un backup in SnapCenter da utilizzare per l'operazione di ripristino.



2. Selezionare l'ambito e il tipo di ripristino.

Lo scenario standard per i sistemi a singolo tenant HANA MDC consiste nell'utilizzare una risorsa completa con revert di volume. Per un sistema HANA MDC con più tenant, potrebbe essere necessario ripristinare solo un tenant singolo. Per ulteriori informazioni sul ripristino del tenant singolo, vedere "[Ripristino e ripristino \(netapp.com\)](https://netapp.com)".

Restore from SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361 ×

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☒ Complete Resource ?

☒ Volume Revert

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

☐ Tenant Database

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

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

Previous

Next

3. Selezionare Recovery Scope (ambito ripristino) e specificare la posizione per il backup del registro e del catalogo.

SnapCenter utilizza il percorso predefinito o i percorsi modificati nel file HANA global.ini per prepopolare le posizioni di backup del registro e del catalogo.

Restore from SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Recover database files using

☒ Recover to most recent state

☐ Recover to point in time

☐ Recover to specified data backup

☐ No recovery

Specify log backup locations

Add

/backup/log

Specify backup catalog location

/backup/log

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

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

Previous

Next

4. Immettere i comandi opzionali di pre-ripristino.

Restore from SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run before performing a restore operation

Pre restore command

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

PreviousNext

5. Immettere i comandi post-ripristino opzionali.

Restore from SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361 ×

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run after performing a restore operation ⓘ

Post restore command

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

Previous

Next

6. Per avviare l'operazione di ripristino, fare clic su fine.

Restore from SnapCenter_hana-1_LocalSnap_Hourly_02-23-2022_14.00.05.4361

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Summary

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

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

Previous

Finish

SnapCenter esegue l'operazione di ripristino e ripristino. Questo esempio mostra i dettagli del processo di ripristino e ripristino.

Job Details



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

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

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

View Logs

Cancel Job

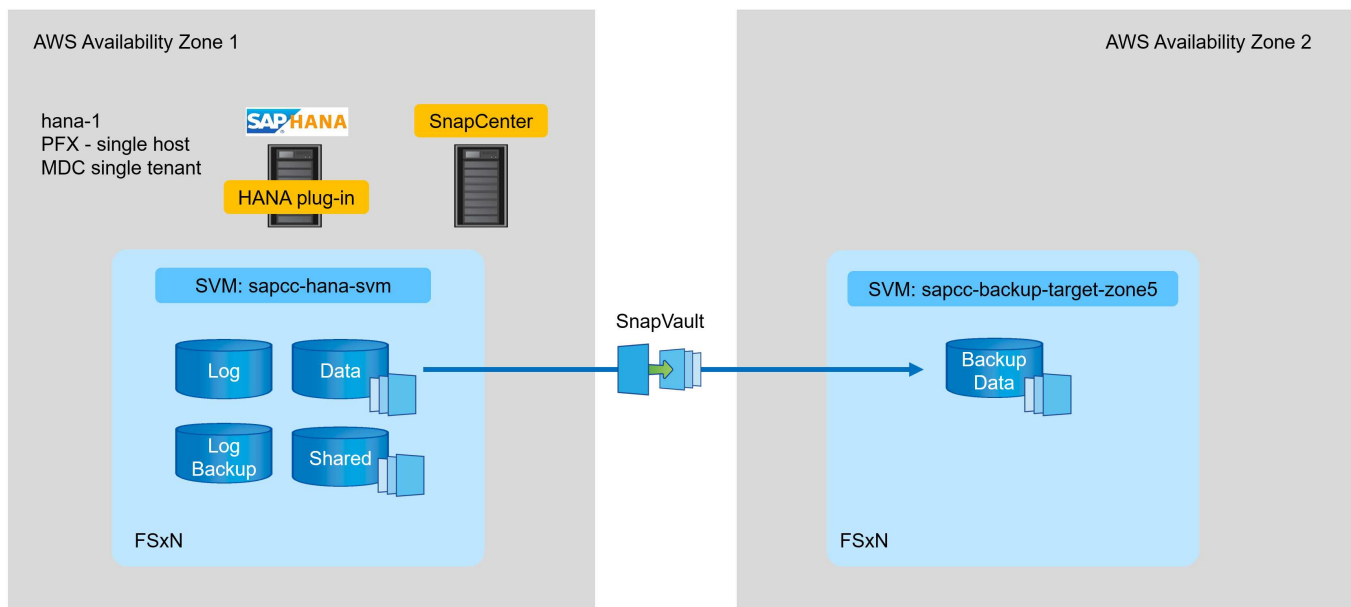
Close

Replica del backup con SnapVault

Panoramica - replica di backup con SnapVault

Nella nostra configurazione di laboratorio, utilizziamo un secondo file system FSX per ONTAP in una seconda zona di disponibilità AWS per mostrare la replica di backup per il volume di dati HANA.

Come discusso nel capitolo ["Strategia di protezione dei dati"](#), La destinazione della replica deve essere un secondo FSX per il file system ONTAP in un'altra zona di disponibilità per essere protetto da un errore del file system FSX primario per ONTAP. Inoltre, il volume condiviso HANA deve essere replicato nel file system FSX secondario per ONTAP.



Panoramica delle fasi di configurazione

È necessario eseguire un paio di passaggi di configurazione sul layer FSX per ONTAP. Puoi farlo con NetApp Cloud Manager o con la riga di comando FSX per ONTAP.

1. Peer FSX per file system ONTAP. I file system FSX per ONTAP devono essere dotati di peering per consentire la replica reciproca.
2. SVM peer. Le SVM devono essere peering per consentire la replica tra loro.
3. Creare un volume di destinazione. Creare un volume nella SVM di destinazione con il tipo di volume `DP`. Tipo `DP` deve essere utilizzato come volume di destinazione della replica.
4. Creare un criterio SnapMirror. Viene utilizzato per creare un criterio per la replica con il tipo `vault`.
 - a. Aggiungere una regola al criterio. La regola contiene l'etichetta SnapMirror e la conservazione dei backup nel sito secondario. È necessario configurare la stessa etichetta SnapMirror in un secondo momento nel criterio SnapCenter in modo che SnapCenter crei backup Snapshot nel volume di origine contenente questa etichetta.
5. Creare una relazione SnapMirror. Definisce la relazione di replica tra il volume di origine e quello di destinazione e allega un criterio.
6. Inizializzare SnapMirror. In questo modo viene avviata la replica iniziale in cui i dati di origine completi

vengono trasferiti al volume di destinazione.

Una volta completata la configurazione della replica del volume, è necessario configurare la replica di backup in SnapCenter come segue:

1. Aggiungere la SVM di destinazione a SnapCenter.
2. Creare una nuova policy SnapCenter per il backup Snapshot e la replica SnapVault.
3. Aggiungere il criterio alla protezione delle risorse HANA.
4. È ora possibile eseguire i backup con la nuova policy.

I seguenti capitoli descrivono i singoli passaggi in modo più dettagliato.

Configurare le relazioni di replica su FSX per i file system ONTAP

Per ulteriori informazioni sulle opzioni di configurazione di SnapMirror, consultare la documentazione di ONTAP all'indirizzo ["Workflow di replica di SnapMirror \(netapp.com\)"](https://netapp.com/workflow-di-replica-di-snapmirror).

- FSX di origine per il file system ONTAP: FsxId00fa9e3c784b6abbb
- SVM di origine: sapcc-hana-svm
- FSX di destinazione per il file system ONTAP: FsxId05f7f00af49dc7a3e
- SVM di destinazione: sapcc-backup-target-zone5

Peer FSX per file system ONTAP

```
FsxId00fa9e3c784b6abbb::> network interface show -role intercluster
```

Logical	Status	Network	Current	Current	
Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----

FsxId00fa9e3c784b6abbb					
inter_1	up/up	10.1.1.57/24			
FsxId00fa9e3c784b6abbb-01					e0e
true					
inter_2	up/up	10.1.2.7/24			
FsxId00fa9e3c784b6abbb-02					e0e
true					

2 entries were displayed.

```
FsxId05f7f00af49dc7a3e::> network interface show -role intercluster
```

	Logical	Status	Network	Current	Current
Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----

FsxId05f7f00af49dc7a3e	inter_1	up/up	10.1.2.144/24		
FsxId05f7f00af49dc7a3e-01					e0e
true					
	inter_2	up/up	10.1.2.69/24		
FsxId05f7f00af49dc7a3e-02					e0e
true					

2 entries were displayed.

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

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

Enter the passphrase:

Confirm the passphrase:

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



peer-addr Sono gli IP del cluster di destinazione.

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

SVM peer

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

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

```
FsxId05f7f00af49dc7a3e::> vservers peer show
```

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

Creare un volume di destinazione

È necessario creare il volume di destinazione con il tipo DP per contrassegnarlo come destinazione di replica.

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

Creare un criterio SnapMirror

Il criterio SnapMirror e la regola aggiunta definiscono la conservazione e l'etichetta SnapMirror per identificare le istantanee da replicare. Quando si crea il criterio SnapCenter in un secondo momento, è necessario utilizzare la stessa etichetta.

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

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

```
FsxId00fa9e3c784b6abbb::> snapmirror policy showVserver Policy
```

Policy Number	Transfer						
Name	Name	Type	Of Rules	Tries	Priority	Comment	

FsxId00fa9e3c784b6abbb							
	snapcenter-policy	vault	1	8	normal	-	
	SnapMirror Label: snapcenter					Keep:	14
						Total Keep:	14

Creare una relazione SnapMirror

Ora viene definita la relazione tra il volume di origine e quello di destinazione, oltre al tipo XDP e alla policy creata in precedenza.

```
FsxId05f7f00af49dc7a3e::> snapmirror create -source-path sapcc-hana-
svm:PFX_data_mnt00001 -destination-path sapcc-backup-target-
zone5:PFX_data_mnt00001 -vserver sapcc-backup-target-zone5 -throttle
unlimited -identity-preserve false -type XDP -policy snapcenter-policy
Operation succeeded: snapmirror create for the relationship with
destination "sapcc-backup-target-zone5:PFX_data_mnt00001".
```

Inizializzare SnapMirror

Con questo comando, viene avviata la replica iniziale. Si tratta di un trasferimento completo di tutti i dati dal volume di origine al volume di destinazione.

```
FsxId05f7f00af49dc7a3e::> snapmirror initialize -destination-path sapcc-backup-target-zone5:PFX_data_mnt00001 -source-path sapcc-hana-svm:PFX_data_mnt00001
Operation is queued: snapmirror initialize of destination "sapcc-backup-target-zone5:PFX_data_mnt00001".
```

È possibile controllare lo stato della replica con `snapmirror show` comando.

```
FsxId05f7f00af49dc7a3e::> snapmirror show
```

```
Progress
Source          Destination Mirror Relationship Total
Last
Path            Type  Path            State  Status          Progress Healthy
Updated
-----
-----
sapcc-hana-svm:PFX_data_mnt00001
                XDP  sapcc-backup-target-zone5:PFX_data_mnt00001
                                Uninitialized
                                Transferring  1009MB    true
02/24 12:34:28
```

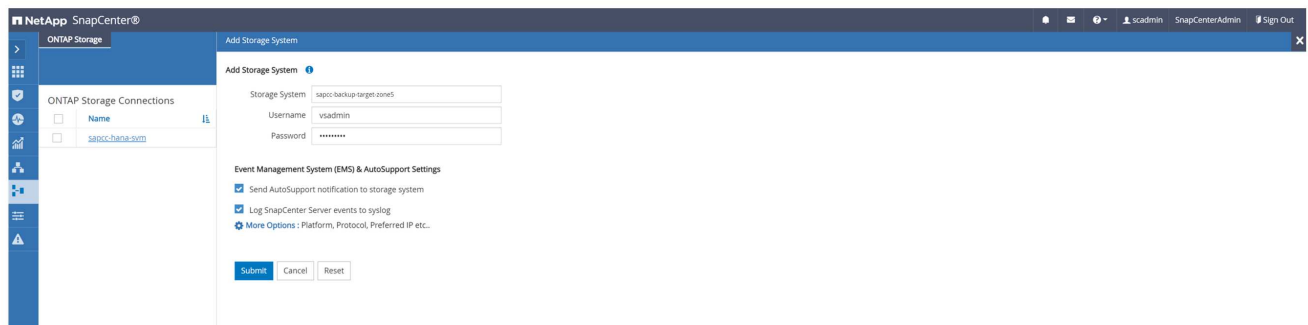
```
FsxId05f7f00af49dc7a3e::> snapmirror show
```

```
Progress
Source          Destination Mirror Relationship Total
Last
Path            Type  Path            State  Status          Progress Healthy
Updated
-----
-----
sapcc-hana-svm:PFX_data_mnt00001
                XDP  sapcc-backup-target-zone5:PFX_data_mnt00001
                                Snapmirrored
                                Idle          -        true  -
```

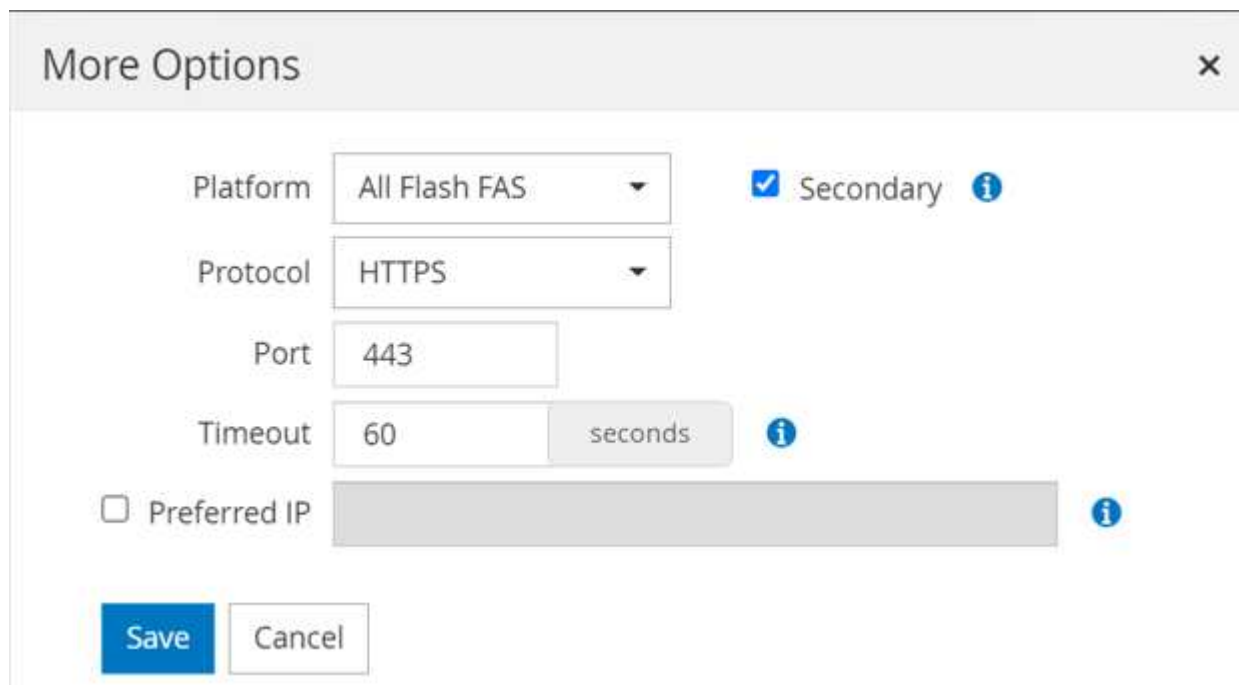

Aggiungere una SVM di backup a SnapCenter

Per aggiungere una SVM di backup a SnapCenter, attenersi alla seguente procedura:

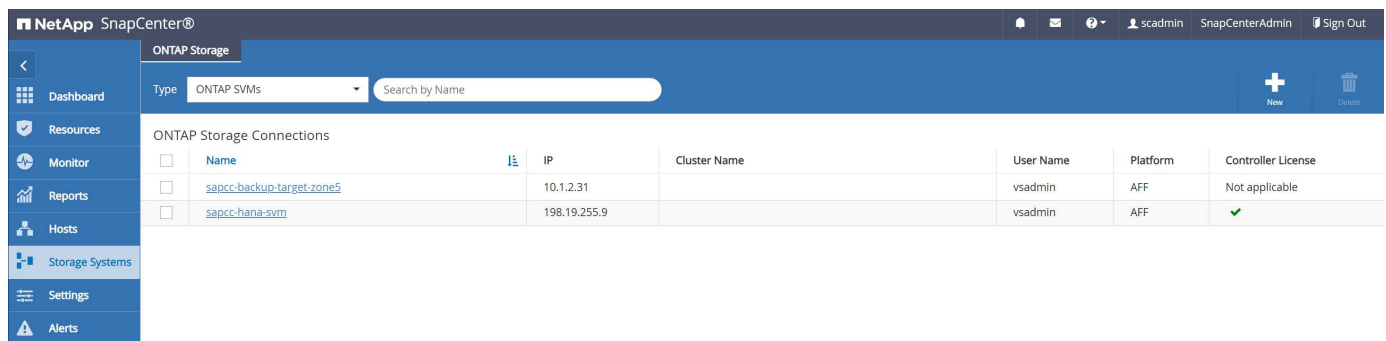
1. Configurare la SVM in cui si trova il volume di destinazione SnapVault in SnapCenter.



2. Nella finestra altre opzioni, selezionare All Flash FAS come piattaforma e selezionare secondario.



La SVM è ora disponibile in SnapCenter.

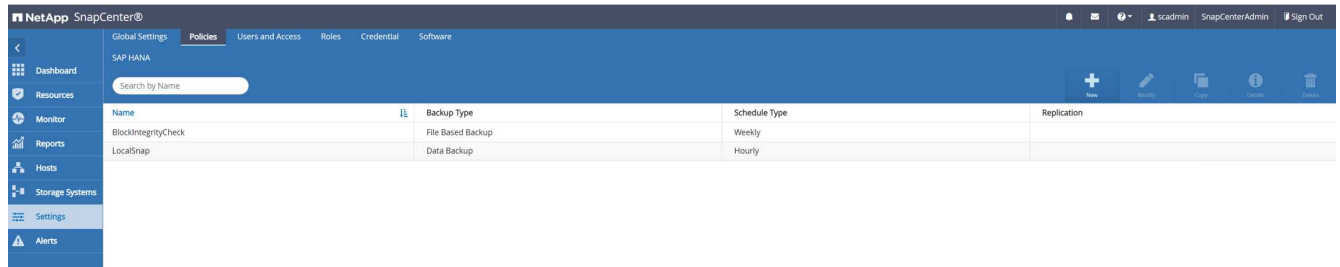


	Name	IP	Cluster Name	User Name	Platform	Controller License
<input type="checkbox"/>	sapcc-backup-target-zone5	10.1.2.31		vsadmin	AFF	Not applicable
<input type="checkbox"/>	sapcc-hana-svm	198.19.255.9		vsadmin	AFF	✓

Creare un nuovo criterio SnapCenter per la replica del backup

È necessario configurare un criterio per la replica di backup come segue:

1. Specificare un nome per il criterio.



2. Selezionare Snapshot backup (Backup Snapshot) e una frequenza di pianificazione. Daily viene generalmente utilizzato per la replica del backup.

New SAP HANA Backup Policy

1 Name

Provide a policy name

Policy name: LocalSnapAndSnapVault

Details: Replication to backup volume

2 Settings

3 Retention

4 Replication

5 Summary

3. Selezionare la conservazione per i backup Snapshot.

New SAP HANA Backup Policy

1 Name

2 Settings

Select backup settings

Backup Type: ☒ Snapshot Based ☐ File-Based

Schedule Frequency

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

☐ On demand

☐ Hourly

☒ Daily

☐ Weekly

☐ Monthly

3 Retention

4 Replication

5 Summary

Questa è la conservazione dei backup Snapshot giornalieri eseguiti sullo storage primario. La conservazione per i backup secondari nella destinazione SnapVault è già stata configurata in precedenza utilizzando il comando add rule a livello di ONTAP. Vedere "Configurazione delle relazioni di replica su FSX per file system ONTAP" (xref).

New SAP HANA Backup Policy ✕

1 Name
2 Settings
3 Retention
4 Replication
5 Summary

Retention settings

Daily retention settings

☒ Total Snapshot copies to keep ?

☐ Keep Snapshot copies for days

- Selezionare il campo Update SnapVault (Aggiorna etichetta) e fornire un'etichetta personalizzata.

Questa etichetta deve corrispondere all'etichetta SnapMirror fornita in `add rule` Comando a livello di ONTAP.

New SAP HANA Backup Policy ✕

1 Name
2 Settings
3 Retention
4 Replication
5 Summary

Select secondary replication options ?

☐ Update SnapMirror after creating a local Snapshot copy.

☒ Update SnapVault after creating a local Snapshot copy.

Secondary policy label ?

Error retry count ?

New SAP HANA Backup Policy ✕

1 Name
2 Settings
3 Retention
4 Replication
5 Summary

Summary

Policy name	LocalSnapAndSnapVault
Details	Replication to backup volume
Backup Type	Snapshot Based Backup
Schedule Type	Daily
Daily backup retention	Total backup copies to retain : 3
Replication	SnapVault enabled , Secondary policy label: Custom Label : snapcenter , Error retry count: 3

Il nuovo criterio SnapCenter è ora configurato.

NetApp SnapCenter®

Global Settings Policies Users and Access Roles Credential Software

SAP HANA

Search by Name

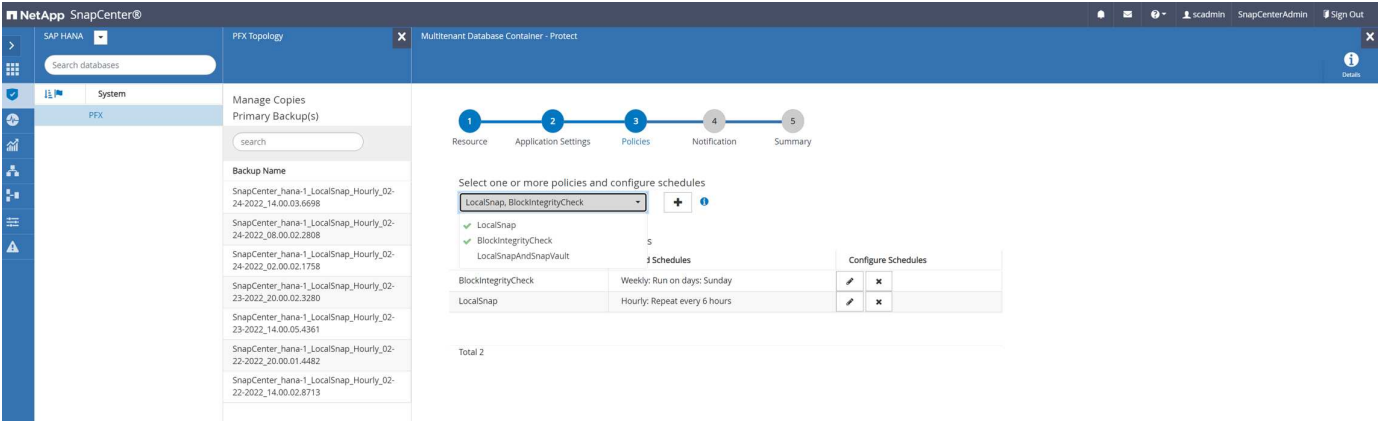
Name	Backup Type	Schedule Type	Replication
BlockIntegrityCheck	File Based Backup	Weekly	
LocalSnap	Data Backup	Hourly	
LocalSnapAndSnapVault	Data Backup	Daily	SnapVault

+ New
✎ Modify
📄 Copy
ℹ Details
🗑 Delete

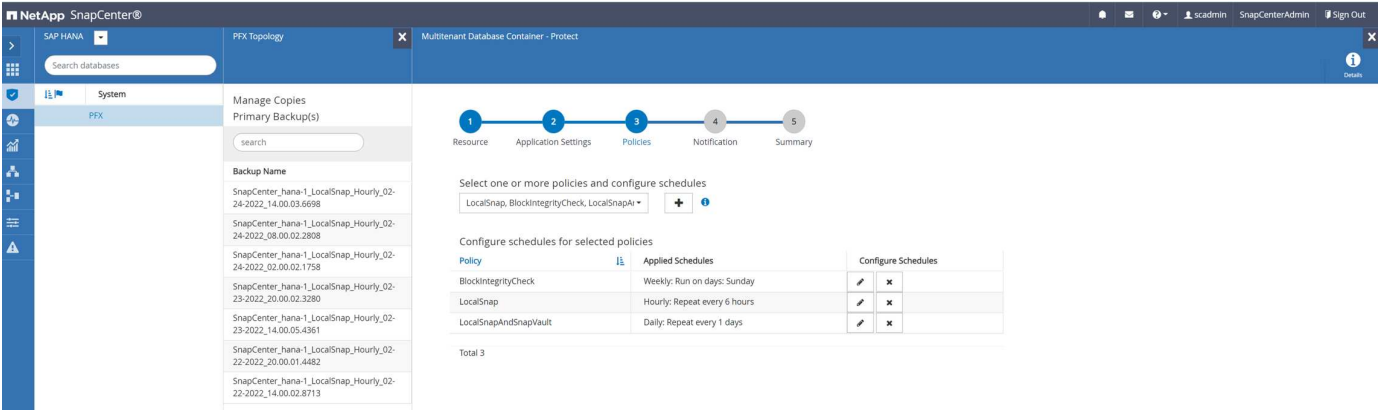
Dashboard
Resources
Monitor
Reports
Hosts
Storage Systems
Settings
Alerts

Aggiungere un criterio alla protezione delle risorse

È necessario aggiungere il nuovo criterio alla configurazione di protezione delle risorse HANA, come mostrato nella figura seguente.



Nella nostra configurazione viene definito un programma giornaliero.



Creare un backup con replica

Un backup viene creato allo stesso modo di una copia Snapshot locale.

Per creare un backup con replica, selezionare il criterio che include la replica di backup e fare clic su Backup.

Backup

x

Create a backup for the selected resource

Resource Name

PFX

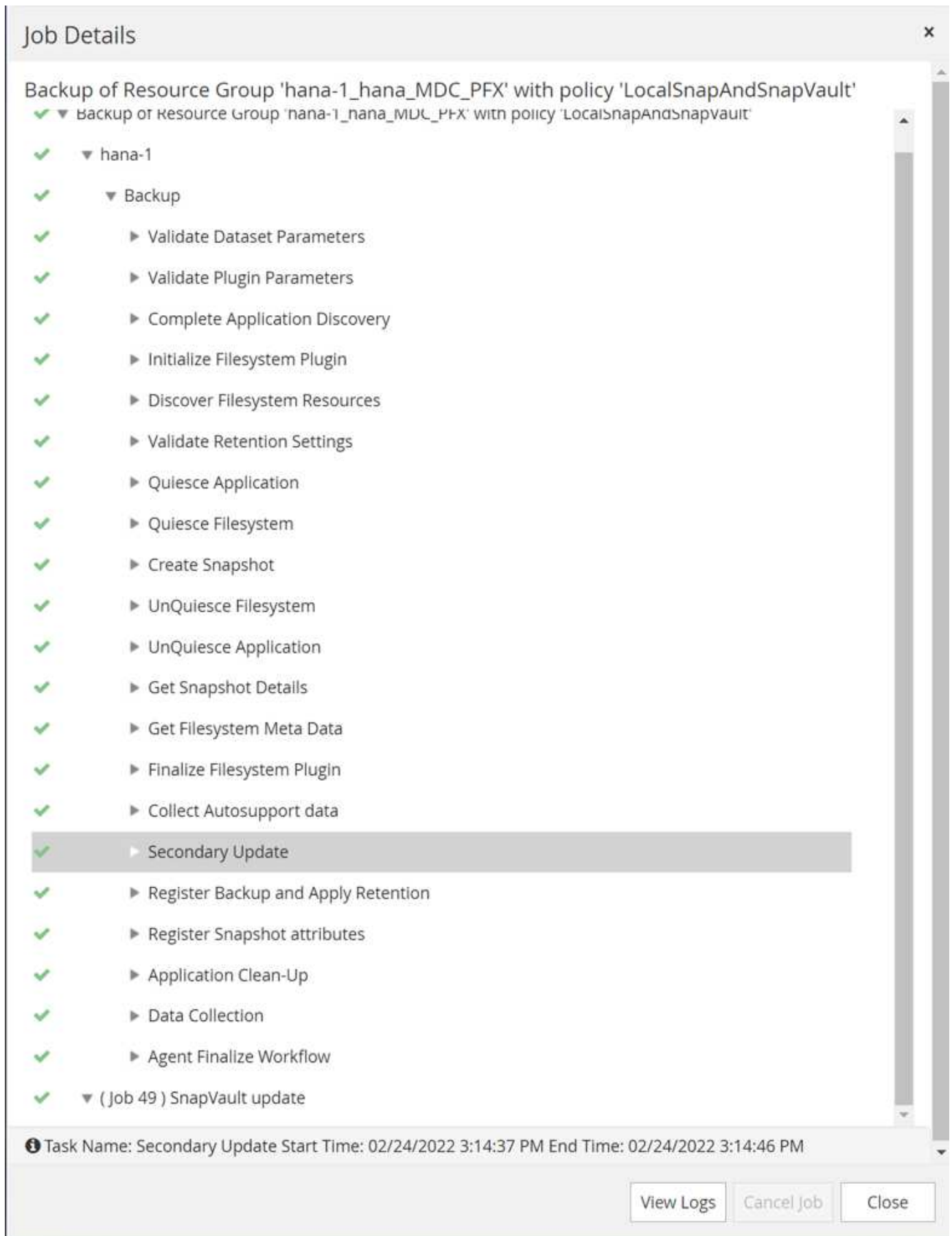
Policy

LocalSnapAndSnapVault

Cancel

Backup

All'interno del log dei lavori di SnapCenter, viene visualizzata la fase di aggiornamento secondario, che avvia un'operazione di aggiornamento del SnapVault. La replica ha modificato i blocchi dal volume di origine al volume di destinazione.



Sul file system FSX per ONTAP, viene creata un'istantanea sul volume di origine utilizzando l'etichetta

SnapMirror, snapcenter, Come configurato nel criterio SnapCenter.

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

snapcenter
8 entries were displayed.
```

Nel volume di destinazione, viene creata una copia Snapshot con lo stesso nome.

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

Il nuovo backup Snapshot è anche elencato nel catalogo di backup HANA.

Backup Catalog						Backup Details					
Database: SYSTEMDB						ID:	1651162926424				
<input type="checkbox"/> Show Log Backups <input type="checkbox"/> Show Delta Backups						Status:	Successful				
Status	Started	Duration	Size	Backup Type	Destination Ty...	Backup Type:	Data Backup				
	Apr 28, 2022, 4:22:06 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Destination Type:	Snapshot				
	Apr 28, 2022, 2:00:26 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Started:	Apr 28, 2022, 4:22:06 PM (UTC)				
	Apr 28, 2022, 8:00:35 AM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Finished:	Apr 28, 2022, 4:22:21 PM (UTC)				
	Apr 15, 2022, 5:00:44 PM	00h 06m 59s	5.50 GB	Data Backup	Snapshot	Duration:	00h 00m 15s				
	Apr 14, 2022, 8:00:32 PM	00h 00m 16s	5.50 GB	Data Backup	Snapshot	Size:	5.50 GB				
	Apr 5, 2022, 2:00:29 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Throughput:	n.a.				
	Apr 5, 2022, 8:00:39 AM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	System ID:					
	Mar 31, 2022, 2:00:29 PM	00h 00m 15s	5.50 GB	Data Backup	Snapshot	Comment:	SnapCenter_hana-1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853				
	Mar 31, 2022, 1:10:57 PM	00h 00m 16s	5.50 GB	Data Backup	Snapshot	Additional Information:	<ok>				
	Feb 22, 2022, 12:55:21 PM	00h 00m 21s	3.56 GB	Data Backup	File	Location:	/hana/data/PFX/mnt00001/				
						Host	Service	Size	Name	Source Type	EBID
						hana-1	nameserver	5.50 GB	hdb00001	volume	SnapCent...

In SnapCenter, è possibile elencare i backup replicati facendo clic su copie del vault nella vista della topologia.

Backup Name	Count	End Date
SnapCenter_hana-1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853	1	04/28/2022 4:22:40 PM

Ripristino e ripristino dallo storage secondario

Per ripristinare e ripristinare dallo storage secondario, attenersi alla seguente procedura:

Per recuperare l'elenco di tutti i backup sullo storage secondario, nella vista topologia SnapCenter, fare clic su copie del vault, quindi selezionare un backup e fare clic su Ripristina.

Backup Name	Count	End Date
SnapCenter_hana-1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853	1	04/28/2022 4:22:40 PM

La finestra di dialogo di ripristino mostra le posizioni secondarie.

Restore from SnapCenter_hana-1_LocalSnapAndSnapVault_Daily_04-28-2022_16.21.41.5853 ×

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☒ Complete Resource ?

☐ Tenant Database

Choose archive location

sapcc-hana-svm:PFX_data_mnt00001

sapcc-backup-target-zone5:PFX_data_mnt00 ▼

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

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

Previous

Next

Ulteriori fasi di ripristino e ripristino sono identiche a quelle precedentemente descritte per un backup Snapshot nello storage primario.

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- Guida utente di FSX per NetApp ONTAP - che cos'è Amazon FSX per NetApp ONTAP?

<https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html>

- Pagina delle risorse SnapCenter

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

- Documentazione del software SnapCenter

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

- TR-4667: Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter

<https://www.netapp.com/pdf.html?item=/media/17111-tr4667.pdf>

- TR-4719: Replica del sistema SAP HANA: Backup e ripristino con SnapCenter

["https://docs.netapp.com/us-en/netapp-solutions-sap/backup/saphana-sr-scs-sap-hana-system-replication-overview.html"](https://docs.netapp.com/us-en/netapp-solutions-sap/backup/saphana-sr-scs-sap-hana-system-replication-overview.html)

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Maggio 2022	Release iniziale.

Backup e recovery SAP HANA con SnapCenter

TR-4614: Backup e recovery SAP HANA con SnapCenter

Nils Bauer, NetApp

Le aziende oggi richiedono una disponibilità continua e ininterrotta per le proprie applicazioni SAP. Si aspettano livelli di performance costanti di fronte a volumi di dati in continua crescita e alla necessità di attività di manutenzione ordinaria come i backup di sistema. L'esecuzione di backup dei database SAP è un'attività critica e può avere un impatto significativo sulle performance del sistema SAP di produzione.

Le finestre di backup si stanno riducendo, mentre la quantità di dati da sottoporre a backup aumenta. Pertanto, è difficile trovare un momento in cui i backup possono essere eseguiti con un effetto minimo sui processi di business. Il tempo necessario per ripristinare e ripristinare i sistemi SAP è un problema, perché i downtime per i sistemi di produzione SAP e non in produzione devono essere ridotti al minimo per ridurre la perdita di dati e i costi per l'azienda.

I seguenti punti riassumono le sfide che devono affrontare il backup e il recovery SAP:

- **Effetti delle performance sui sistemi SAP di produzione.** in genere, i backup tradizionali basati su copia creano un significativo scolo delle performance sui sistemi SAP di produzione a causa dei carichi pesanti posti sul server di database, sul sistema storage e sulla rete storage.
- **Riduzione delle finestre di backup.** i backup convenzionali possono essere eseguiti solo quando sono in corso poche attività di dialogo o batch sul sistema SAP. La pianificazione dei backup diventa più difficile quando i sistemi SAP vengono utilizzati 24 ore su 24.
- **Rapida crescita dei dati.** la rapida crescita dei dati e la riduzione delle finestre di backup richiedono investimenti continui nell'infrastruttura di backup. In altre parole, è necessario procurarsi più unità nastro, ulteriore spazio su disco per il backup e reti di backup più veloci. È inoltre necessario coprire le spese di storage e gestione di tali risorse su nastro. I backup incrementali o differenziali possono risolvere questi problemi, ma questa disposizione comporta un processo di ripristino molto lento, complicato e complesso, più difficile da verificare. Tali sistemi di solito aumentano i tempi di obiettivi del tempo di ripristino (RTO) e di

obiettivi del punto di ripristino (RPO) in modi che non sono accettabili per l'azienda.

- **Aumento del costo del downtime.** il downtime non pianificato di un sistema SAP influisce in genere sulle finanze aziendali. Una parte significativa di qualsiasi downtime non pianificato viene consumata dal requisito di ripristino e ripristino del sistema SAP. Pertanto, l'RTO desiderato determina la progettazione dell'architettura di backup e ripristino.
- **Tempi di backup e recovery per i progetti di upgrade SAP.** il piano di progetto per un upgrade SAP include almeno tre backup del database SAP. Questi backup riducono significativamente il tempo disponibile per il processo di aggiornamento. La decisione di procedere si basa generalmente sul tempo necessario per ripristinare e ripristinare il database dal backup creato in precedenza. Invece di ripristinare semplicemente un sistema allo stato precedente, un ripristino rapido offre più tempo per risolvere i problemi che potrebbero verificarsi durante un aggiornamento.

La soluzione NetApp

La tecnologia NetApp Snapshot può essere utilizzata per creare backup di database in pochi minuti. Il tempo necessario per creare una copia Snapshot è indipendente dalle dimensioni del database, in quanto una copia Snapshot non sposta alcun blocco di dati fisico sulla piattaforma di storage. Inoltre, l'utilizzo della tecnologia Snapshot non ha alcun effetto sulle performance del sistema SAP live, in quanto la tecnologia Snapshot di NetApp non sposta o copia i blocchi di dati quando viene creata la copia Snapshot o quando vengono modificati i dati nel file system attivo. Pertanto, la creazione di copie Snapshot può essere pianificata senza considerare i periodi di dialogo di picco o di attività batch. I clienti SAP e NetApp pianificano in genere più backup Snapshot online durante il giorno; ad esempio, ogni quattro ore è comune. Questi backup Snapshot vengono in genere conservati per tre o cinque giorni nel sistema di storage primario prima di essere rimossi.

Le copie Snapshot offrono anche vantaggi chiave per le operazioni di ripristino e ripristino. Il software di ripristino dei dati NetApp SnapRestore consente di ripristinare un intero database o, in alternativa, una parte di un database in qualsiasi momento, in base alle copie Snapshot disponibili. Tali processi di ripristino vengono completati in pochi minuti, indipendentemente dalle dimensioni del database. Poiché durante la giornata vengono creati diversi backup Snapshot online, il tempo necessario per il processo di ripristino viene ridotto in modo significativo rispetto a un approccio di backup tradizionale. Poiché un ripristino può essere eseguito con una copia Snapshot che ha poche ore di vita (anziché fino a 24 ore), è necessario applicare un numero inferiore di registri delle transazioni. Pertanto, l'RTO viene ridotto a diversi minuti piuttosto che alle diverse ore richieste per i backup su nastro convenzionali a ciclo singolo.

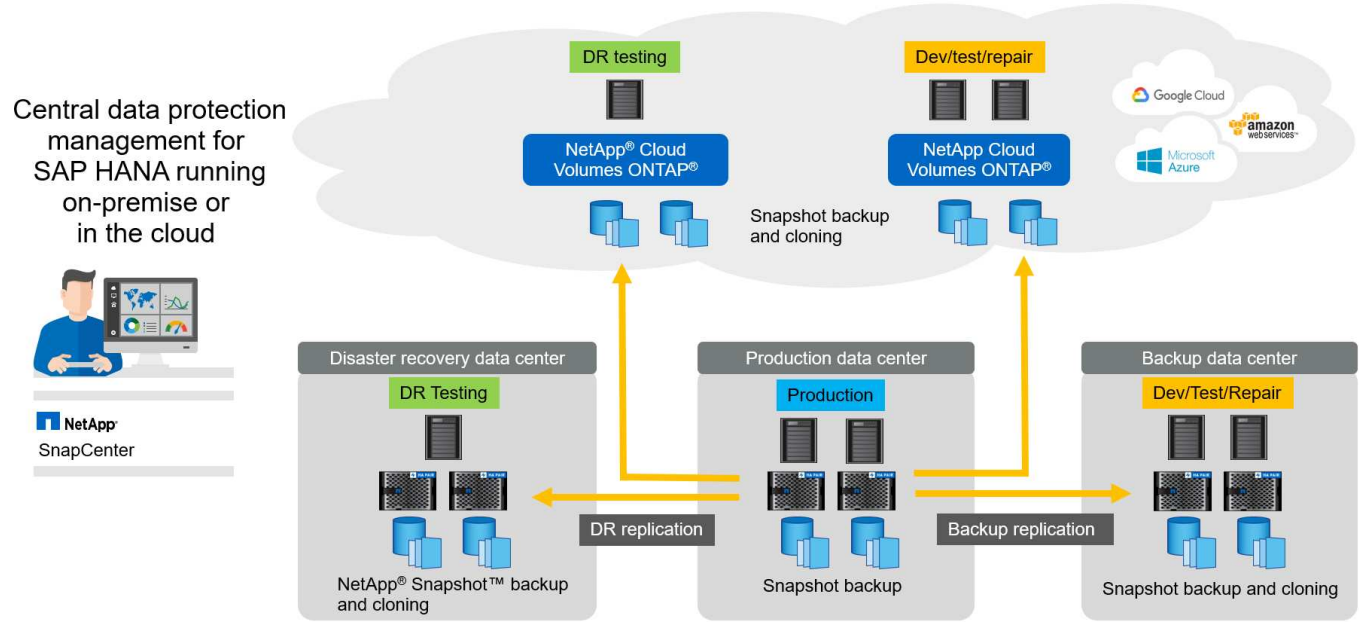
I backup delle copie Snapshot vengono memorizzati sullo stesso sistema di dischi dei dati online attivi. Pertanto, NetApp consiglia di utilizzare i backup di copia Snapshot come supplemento piuttosto che come sostituto per i backup in una posizione secondaria. La maggior parte delle azioni di ripristino e ripristino viene gestita utilizzando SnapRestore sul sistema di storage primario. I ripristini da una posizione secondaria sono necessari solo se il sistema di storage primario contenente le copie Snapshot viene danneggiato. La posizione secondaria può essere utilizzata anche se è necessario ripristinare un backup non più disponibile da una copia Snapshot, ad esempio un backup di fine mese.

Un backup in una posizione secondaria si basa sulle copie Snapshot create sullo storage primario. Pertanto, i dati vengono letti direttamente dal sistema di storage primario senza generare carico sul server di database SAP. Lo storage primario comunica direttamente con lo storage secondario e invia i dati di backup alla destinazione utilizzando un backup disk-to-disk di NetApp SnapVault.

SnapVault offre vantaggi significativi rispetto ai backup tradizionali. Dopo un trasferimento iniziale dei dati, in cui tutti i dati sono stati trasferiti dall'origine alla destinazione, tutti i backup successivi copiano solo i blocchi modificati nello storage secondario. Pertanto, il carico sul sistema di storage primario e il tempo necessario per un backup completo sono notevolmente ridotti. Poiché SnapVault memorizza solo i blocchi modificati nella destinazione, un backup completo del database richiede meno spazio su disco.

La soluzione può anche essere facilmente estesa a un modello operativo di cloud ibrido. La replica dei dati per

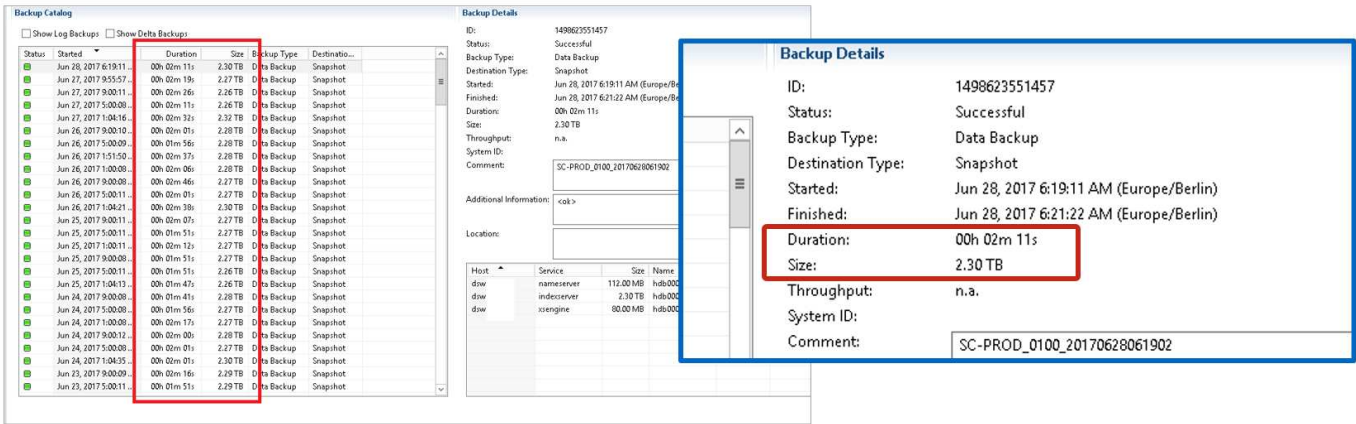
il disaster recovery o il backup fuori sede può essere eseguita dai sistemi NetApp ONTAP on-premise alle istanze di Cloud Volumes ONTAP in esecuzione nel cloud. È possibile utilizzare SnapCenter come strumento centrale per gestire la protezione dei dati e la replica dei dati, indipendentemente dal fatto che il sistema SAP HANA venga eseguito on-premise o nel cloud. La figura seguente mostra una panoramica della soluzione di backup.



Esecuzione dei backup Snapshot

La schermata successiva mostra HANA Studio di un cliente che esegue SAP HANA su storage NetApp. Il cliente utilizza le copie Snapshot per eseguire il backup del database HANA. L'immagine mostra che il backup del database HANA (di circa 2,3 TB) viene eseguito in 2 minuti e 11 secondi utilizzando la tecnologia di backup Snapshot.

La parte più importante del runtime complessivo del workflow di backup è il tempo necessario per eseguire l'operazione di salvataggio del backup HANA, che dipende dal carico sul database HANA. Il backup Snapshot dello storage viene sempre completato in un paio di secondi.



Confronto degli obiettivi del tempo di ripristino

Questa sezione fornisce un confronto RTO tra i backup Snapshot basati su file e su storage. L'RTO è definito

dalla somma del tempo necessario per ripristinare il database e del tempo necessario per avviare e ripristinare il database.

Tempo necessario per il ripristino del database

Con un backup basato su file, il tempo di ripristino dipende dalle dimensioni del database e dell'infrastruttura di backup, che definisce la velocità di ripristino in megabyte al secondo. Ad esempio, se l'infrastruttura supporta un'operazione di ripristino a una velocità di 250 MBps, il ripristino di un database di 1 TB richiede circa 1 ora e 10 minuti.

Con i backup delle copie Snapshot dello storage, il tempo di ripristino è indipendente dalle dimensioni del database e si trova nell'intervallo di un paio di secondi in cui il ripristino può essere eseguito dallo storage primario. Il ripristino dallo storage secondario è necessario solo in caso di disastro quando lo storage primario non è più disponibile.

Tempo necessario per avviare il database

L'ora di inizio del database dipende dalle dimensioni dell'archivio di righe e colonne. Per l'archivio di colonne, l'ora di inizio dipende anche dalla quantità di dati precaricati durante l'avvio del database. Negli esempi seguenti, si presuppone che l'ora di inizio sia di 30 minuti. L'ora di inizio è la stessa per un ripristino e un ripristino basati su file e per un ripristino e un ripristino basati su Snapshot.

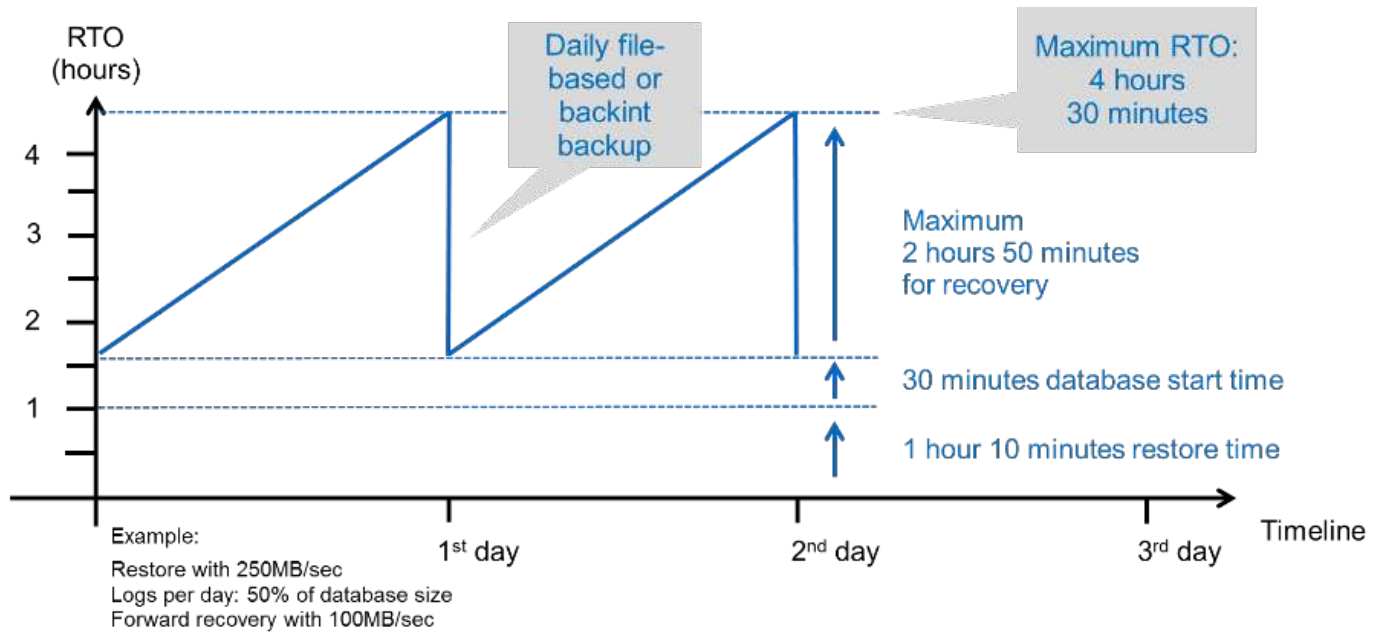
Tempo necessario per il ripristino del database

Il tempo di ripristino dipende dal numero di registri che devono essere applicati dopo il ripristino. Questo numero è determinato dalla frequenza con cui vengono eseguiti i backup dei dati.

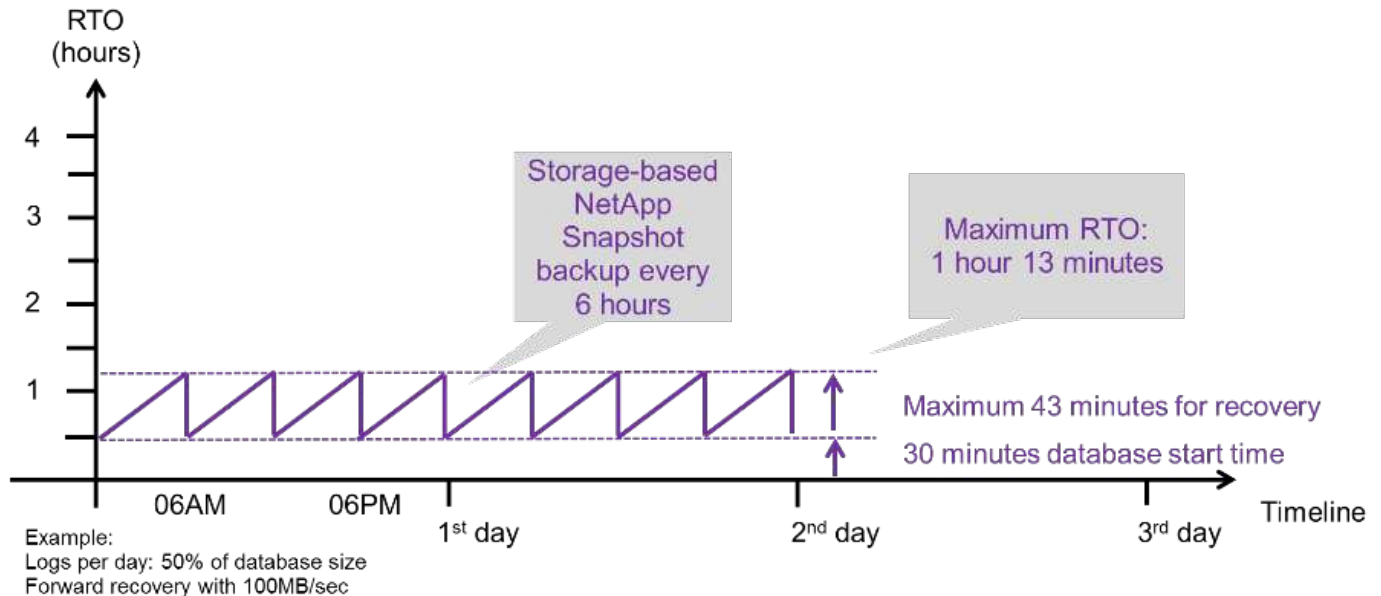
Con i backup dei dati basati su file, la pianificazione del backup è generalmente una volta al giorno. In genere, non è possibile una frequenza di backup più elevata, poiché il backup diminuisce le prestazioni di produzione. Pertanto, nel peggiore dei casi, tutti i log scritti durante la giornata devono essere applicati durante il recupero in avanti.

I backup dei dati di copia Snapshot dello storage vengono in genere pianificati con una frequenza maggiore perché non influiscono sulle prestazioni del database SAP HANA. Ad esempio, se i backup delle copie Snapshot vengono pianificati ogni sei ore, il tempo di ripristino sarebbe, nel peggiore dei casi, un quarto del tempo di ripristino per un backup basato su file (6 ore / 24 ore = $\frac{1}{4}$).

La figura seguente mostra un esempio RTO per un database da 1 TB quando vengono utilizzati backup dei dati basati su file. In questo esempio, un backup viene eseguito una volta al giorno. L'RTO varia in base al momento in cui sono stati eseguiti il ripristino e il ripristino. Se il ripristino e il ripristino sono stati eseguiti immediatamente dopo l'esecuzione di un backup, l'RTO si basa principalmente sul tempo di ripristino, che nell'esempio è di 1 ora e 10 minuti. Il tempo di ripristino è aumentato a 2 ore e 50 minuti quando il ripristino e il ripristino sono stati eseguiti immediatamente prima del backup successivo e l'RTO massimo è stato di 4 ore e 30 minuti.



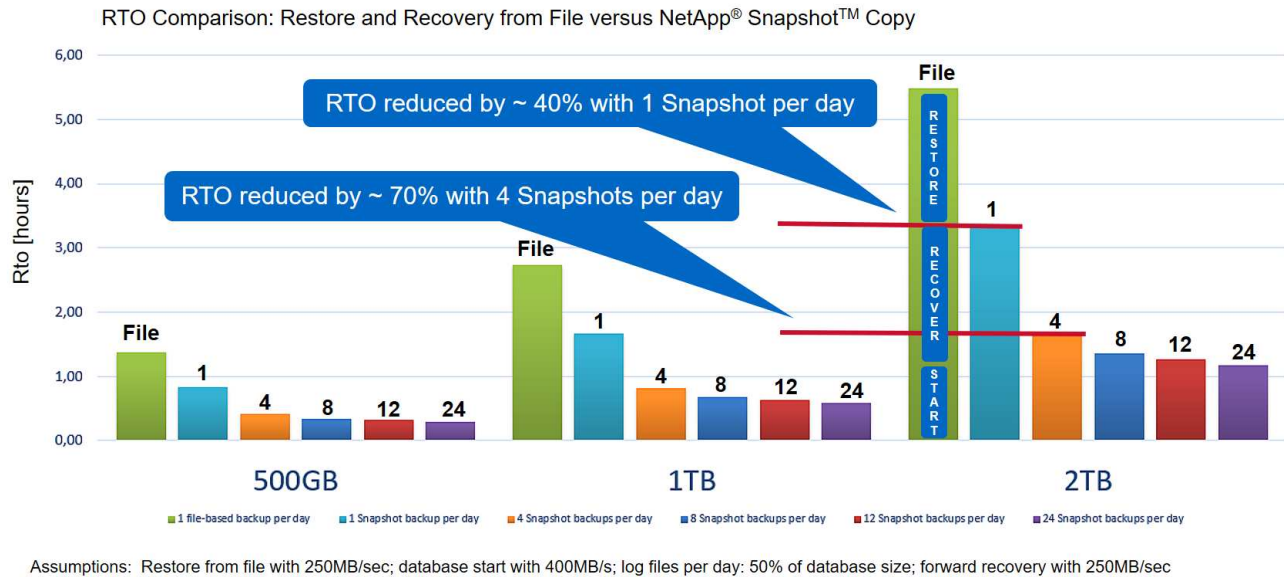
La figura seguente mostra un esempio RTO per un database da 1 TB quando vengono utilizzati backup Snapshot. Con i backup Snapshot basati sullo storage, l'RTO dipende solo dall'ora di avvio del database e dal tempo di ripristino in avanti, in quanto il ripristino viene completato in pochi secondi, indipendentemente dalle dimensioni del database. Il tempo di recupero in avanti aumenta anche a seconda del momento in cui vengono eseguiti il ripristino e il ripristino, ma a causa della maggiore frequenza dei backup (ogni sei ore in questo esempio), il tempo di recupero in avanti è di 43 minuti al massimo. In questo esempio, l'RTO massimo è di 1 ora e 13 minuti.



La figura seguente mostra un confronto RTO tra backup Snapshot basati su file e storage per database di dimensioni diverse e frequenze diverse dei backup Snapshot. La barra verde mostra il backup basato su file. Le altre barre mostrano i backup delle copie Snapshot con frequenze di backup diverse.

Con un singolo backup dei dati di copia Snapshot al giorno, l'RTO è già ridotto del 40% rispetto a un backup dei dati basato su file. La riduzione aumenta fino al 70% quando vengono eseguiti quattro backup Snapshot al giorno. La figura mostra inoltre che la curva si appiattisce se si aumenta la frequenza di backup Snapshot a più

di quattro o sei backup Snapshot al giorno. I nostri clienti configurano quindi da quattro a sei backup Snapshot al giorno.



Il grafico mostra le dimensioni della RAM del server HANA. La dimensione del database in memoria è calcolata in modo da essere la metà della dimensione della RAM del server.



I tempi di ripristino e ripristino vengono calcolati in base ai seguenti presupposti. Il database può essere ripristinato a 250 MBps. Il numero di file di log al giorno corrisponde al 50% delle dimensioni del database. Ad esempio, un database da 1 TB crea 500 MB di file di log al giorno. È possibile eseguire un ripristino a 100 Mbps.

Architettura SnapCenter

SnapCenter è una piattaforma unificata e scalabile per la protezione dei dati coerente con l'applicazione. SnapCenter offre controllo e supervisione centralizzati, delegando al contempo la capacità degli utenti di gestire processi di backup, ripristino e clonazione specifici dell'applicazione. Con SnapCenter, gli amministratori di database e storage imparano a utilizzare un unico strumento per gestire le operazioni di backup, ripristino e clonazione per una vasta gamma di applicazioni e database.

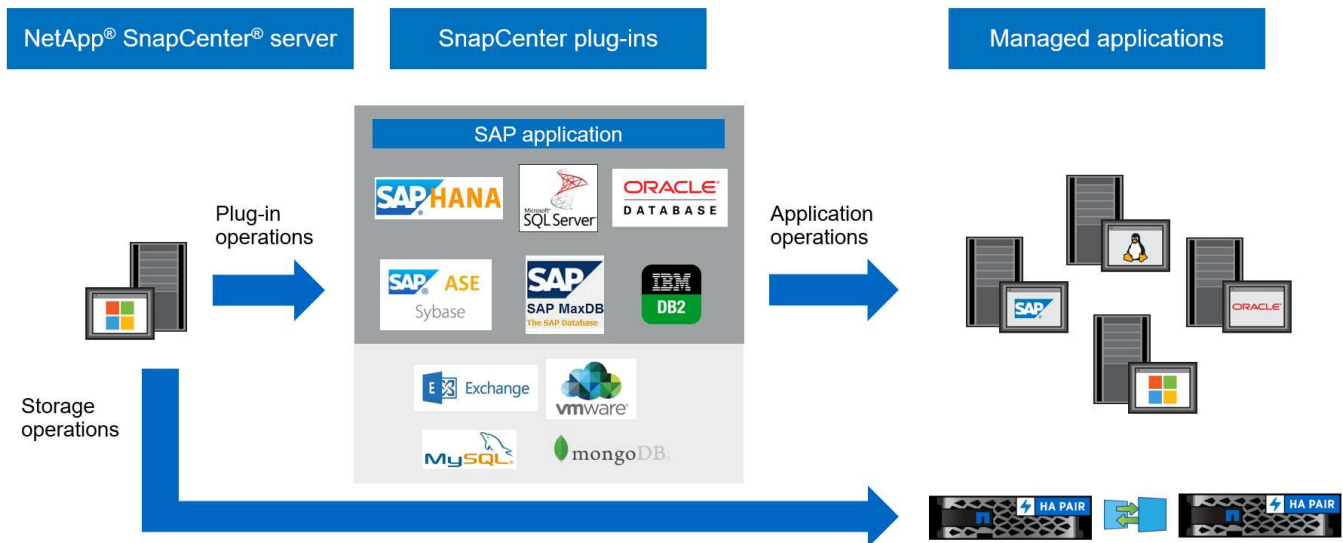
SnapCenter gestisce i dati tra gli endpoint del data fabric basato su NetApp. Puoi utilizzare SnapCenter per replicare i dati tra ambienti on-premise, tra ambienti on-premise e cloud e tra cloud privati, ibridi o pubblici.

Componenti SnapCenter

SnapCenter include il server SnapCenter, il pacchetto plug-in SnapCenter per Windows e il pacchetto plug-in SnapCenter per Linux. Ogni pacchetto contiene plug-in per SnapCenter per varie applicazioni e componenti dell'infrastruttura.

I plug-in personalizzati di SnapCenter consentono di creare plug-in personalizzati e proteggere l'applicazione utilizzando la stessa interfaccia SnapCenter.

La figura seguente illustra i componenti di SnapCenter.



Soluzione di backup SAP HANA di SnapCenter

Questa sezione elenca i componenti, le versioni e le configurazioni SAP HANA supportate e i miglioramenti di SnapCenter 4.6 utilizzati in questa soluzione.

Componenti della soluzione

La soluzione di backup SnapCenter per SAP HANA copre le seguenti aree:

- Backup dei dati SAP HANA con copie Snapshot basate su storage:
 - Pianificazione del backup
 - Gestione della conservazione
 - Manutenzione del catalogo di backup SAP HANA
- Volume non di dati (ad esempio, /hana/shared) Backup con copie Snapshot basate su storage:
 - Pianificazione del backup
 - Gestione della conservazione
- Replica su una posizione di backup off-site o disaster recovery:
 - Backup Snapshot dei dati SAP HANA
 - Volumi non dati
 - Gestione della conservazione configurata sullo storage di backup off-site
 - Manutenzione del catalogo di backup SAP HANA
- Controlli dell'integrità dei blocchi di database utilizzando un backup basato su file:
 - Pianificazione del backup
 - Gestione della conservazione
 - Manutenzione del catalogo di backup SAP HANA
- Gestione della conservazione del backup del log del database HANA:
 - Gestione della conservazione basata sulla conservazione dei dati

- Manutenzione del catalogo di backup SAP HANA
- Rilevamento automatico dei database HANA
- Ripristino e ripristino automatici
- Operazioni di ripristino single-tenant con sistemi SAP HANA multi-tenant database container (MDC)

I backup dei file di dati del database vengono eseguiti da SnapCenter in combinazione con il plug-in per SAP HANA. Il plug-in attiva un punto di salvataggio del backup del database SAP HANA in modo che le copie Snapshot, create sul sistema di storage primario, si basino su un'immagine coerente del database SAP HANA.

SnapCenter consente la replica di immagini di database coerenti in una posizione di backup off-site o disaster recovery utilizzando SnapVault o NetApp SnapMirror. funzione. In genere, vengono definite policy di conservazione diverse per i backup nello storage di backup primario e off-site. SnapCenter gestisce la conservazione nello storage primario e ONTAP la gestisce nello storage di backup off-site.

Per consentire un backup completo di tutte le risorse correlate a SAP HANA, SnapCenter consente inoltre di eseguire il backup di tutti i volumi non dati utilizzando il plug-in SAP HANA con copie Snapshot basate su storage. I volumi non dati possono essere pianificati indipendentemente dal backup dei dati del database per consentire policy di conservazione e protezione individuali.

Il database SAP HANA esegue automaticamente i backup dei log. A seconda degli obiettivi del punto di ripristino, sono disponibili diverse opzioni per la posizione di storage dei backup del log:

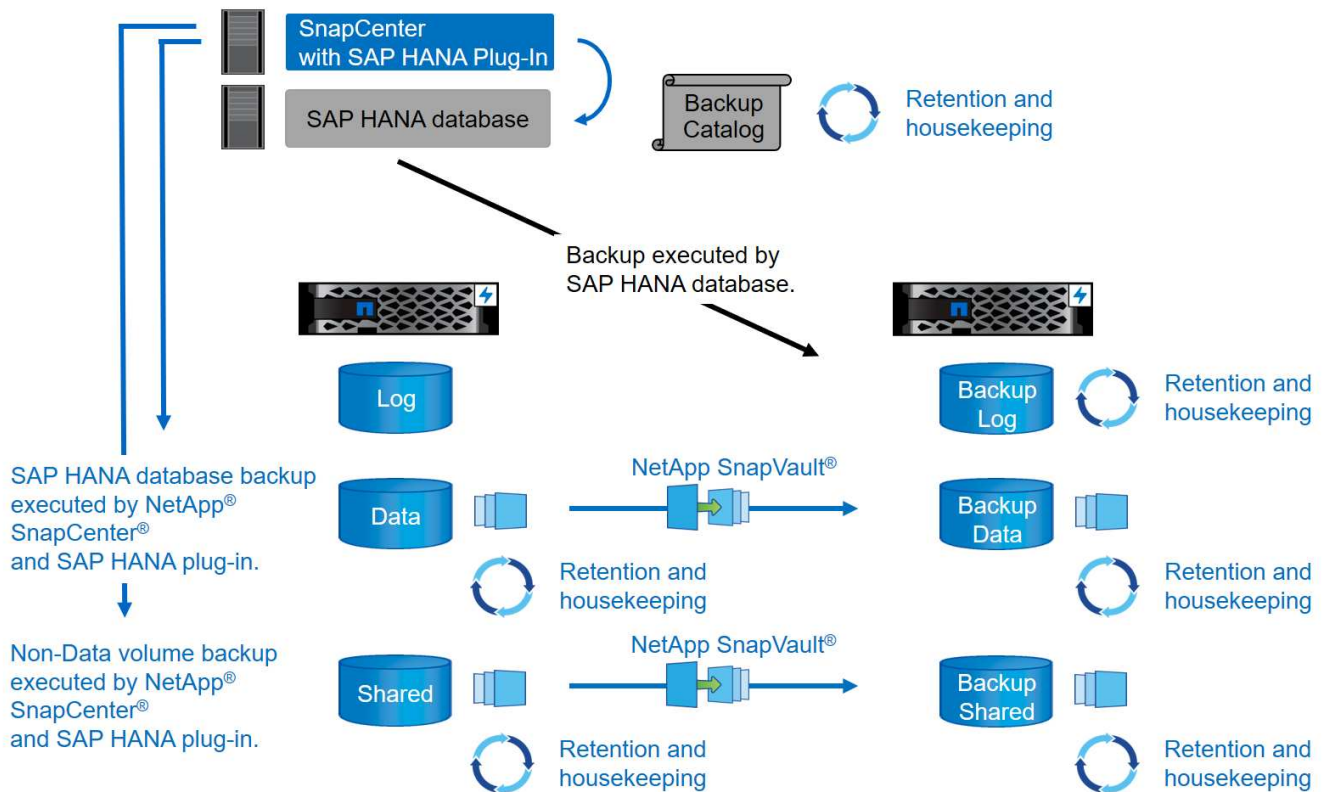
- Il backup del log viene scritto su un sistema storage che esegue il mirroring sincrono dei dati in una seconda posizione con il software di storage ad alta disponibilità (ha) e disaster recovery NetApp MetroCluster.
- La destinazione di backup del registro può essere configurata sullo stesso sistema di storage primario e quindi replicata in modo sincrono o asincrono su uno storage secondario con SnapMirror.
- La destinazione del backup del registro può essere configurata sullo stesso storage di backup off-site in cui i backup del database vengono replicati con SnapVault. Con questa configurazione, lo storage di backup off-site presenta requisiti di disponibilità come quelli dello storage primario, in modo che i backup dei log possano essere scritti nello storage di backup off-site.

SAP consiglia di combinare i backup Snapshot basati su storage con un backup settimanale basato su file per eseguire un controllo dell'integrità dei blocchi. Il controllo dell'integrità del blocco può essere eseguito da SnapCenter. In base alle policy di conservazione configurabili, SnapCenter gestisce la gestione dei backup dei file di dati nello storage primario, nei backup dei file di log e nel catalogo di backup SAP HANA.



SnapCenter gestisce la conservazione dello storage primario, mentre ONTAP gestisce la conservazione del backup secondario.

La figura seguente mostra una panoramica della configurazione del backup del database e del log, in cui i backup del log vengono scritti su un montaggio NFS dello storage di backup off-site.



Quando si esegue un backup Snapshot basato su storage di volumi non dati, SnapCenter esegue le seguenti attività:

1. Creazione di una copia Snapshot dello storage del volume non di dati.
2. Esecuzione di un aggiornamento di SnapVault o SnapMirror per il volume di dati, se configurato.
3. Eliminazione delle copie Snapshot dello storage nello storage primario in base alla policy di conservazione definita.

Quando si esegue un backup Snapshot basato su storage del database SAP HANA, SnapCenter esegue le seguenti attività:

1. Creazione di un punto di salvataggio di backup SAP HANA per creare un'immagine coerente sul layer di persistenza.
2. Creazione di una copia Snapshot dello storage del volume di dati.
3. Registrazione del backup Snapshot dello storage nel catalogo di backup SAP HANA.
4. Rilascio del punto di salvataggio del backup SAP HANA.
5. Esecuzione di un aggiornamento di SnapVault o SnapMirror per il volume di dati, se configurato.
6. Eliminazione delle copie Snapshot dello storage nello storage primario in base alla policy di conservazione definita.
7. Eliminazione delle voci del catalogo di backup SAP HANA se i backup non esistono più nello storage di backup primario o off-site.
8. Ogni volta che un backup viene cancellato in base al criterio di conservazione o manualmente, SnapCenter elimina tutti i backup del registro precedenti al backup dei dati meno recente. I backup dei log vengono cancellati nel file system e nel catalogo di backup SAP HANA.

Versioni e configurazioni SAP HANA supportate

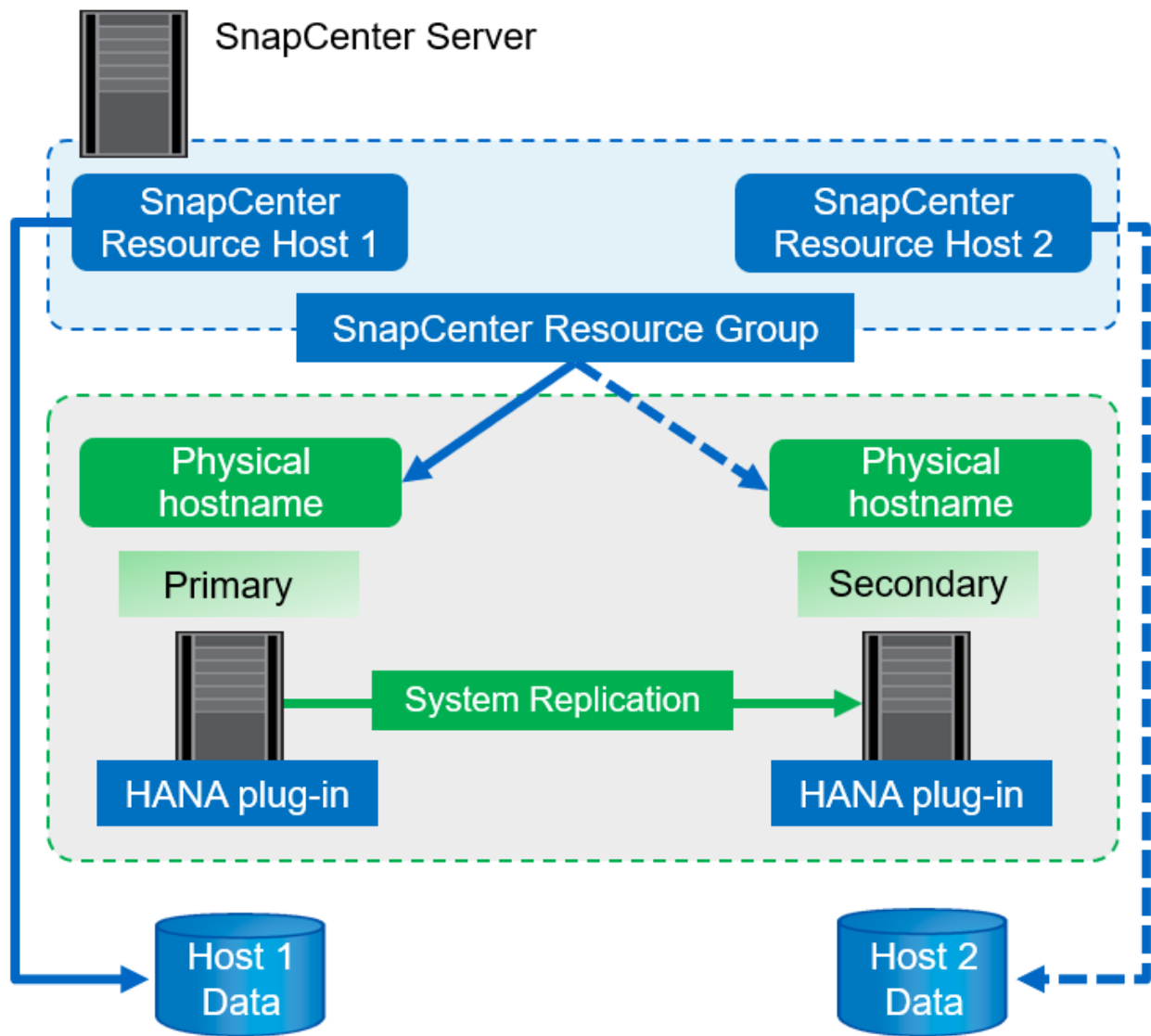
SnapCenter supporta configurazioni SAP HANA a host singolo e multiplo utilizzando sistemi storage NetApp collegati a NFS o FC (AFF e FAS), oltre a sistemi SAP HANA eseguiti su Cloud Volumes ONTAP presso AWS, Azure, la piattaforma cloud di Google e AWS FSX ONTAP utilizzando NFS.

SnapCenter supporta le seguenti architetture e release SAP HANA:

- Container singolo SAP HANA: SAP HANA 1.0 SPS12
- Tenant singolo SAP HANA multi-tenant-database container (MDC): SAP HANA 2.0 SPS3 e versioni successive
- SAP HANA multi-tenant-database container (MDC) più tenant: SAP HANA 2.0 SPS4 e versioni successive

Miglioramenti di SnapCenter 4.6

A partire dalla versione 4.6, SnapCenter supporta il rilevamento automatico dei sistemi HANA configurati in una relazione di replica del sistema HANA. Ciascun host viene configurato utilizzando il proprio indirizzo IP fisico (nome host) e il proprio volume di dati sul layer di storage. Le due risorse SnapCenter sono combinate in un gruppo di risorse, SnapCenter identifica automaticamente l'host primario o secondario e quindi esegue le operazioni di backup richieste di conseguenza. La gestione della conservazione per Snapshot e backup basati su file creati con SnapCenter viene eseguita su entrambi gli host per garantire che i vecchi backup vengano cancellati anche sull'host secondario corrente. La figura seguente mostra una panoramica di alto livello. Per una descrizione dettagliata della configurazione e del funzionamento dei sistemi HANA abilitati alla replica del sistema in SnapCenter, consultare la sezione ["TR-4719 replica, backup e ripristino del sistema SAP HANA con SnapCenter"](#).



Concetti e Best practice di SnapCenter

In questa sezione vengono descritti i concetti e le Best practice di SnapCenter relativi alla configurazione e all'implementazione delle risorse SAP HANA.

Opzioni e concetti di configurazione delle risorse SAP HANA

Con SnapCenter, la configurazione delle risorse del database SAP HANA può essere eseguita con due approcci diversi.

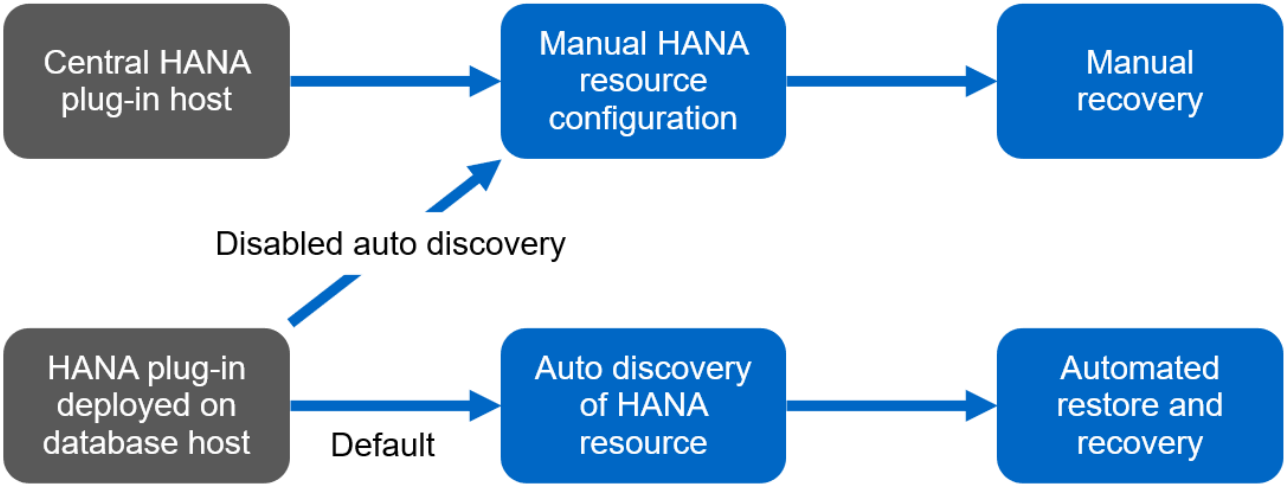
- **Configurazione manuale delle risorse.** le informazioni relative alle risorse HANA e all'impatto dello storage devono essere fornite manualmente.
- **Rilevamento automatico delle risorse HANA.** il rilevamento automatico semplifica la configurazione dei database HANA in SnapCenter e consente il ripristino e il ripristino automatici.

È importante comprendere che solo le risorse di database HANA rilevate automaticamente in SnapCenter sono abilitate per il ripristino e il ripristino automatici. Le risorse di database HANA configurate manualmente in SnapCenter devono essere ripristinate manualmente dopo un'operazione di ripristino in SnapCenter.

D’altro canto, il rilevamento automatico con SnapCenter non è supportato per tutte le architetture HANA e le configurazioni dell’infrastruttura. Pertanto, gli ambienti HANA potrebbero richiedere un approccio misto in cui alcuni sistemi HANA (sistemi host multipli HANA) richiedono la configurazione manuale delle risorse e tutti gli altri possono essere configurati utilizzando il rilevamento automatico.

Il rilevamento automatico, il ripristino e il ripristino automatici dipendono dalla capacità di eseguire comandi del sistema operativo sull’host del database. Ad esempio, le operazioni di rilevamento del footprint del file system e dello storage e di disinstallazione, montaggio o LUN. Queste operazioni vengono eseguite con il plug-in Linux di SnapCenter, che viene implementato automaticamente insieme al plug-in HANA. Pertanto, è necessario implementare il plug-in HANA sull’host del database per abilitare il rilevamento automatico e il ripristino e ripristino automatici. È inoltre possibile disattivare la funzione di rilevamento automatico dopo l’implementazione del plug-in HANA sull’host del database. In questo caso, la risorsa sarà configurata manualmente.

La figura seguente riepiloga le dipendenze. Per ulteriori informazioni sulle opzioni di implementazione di HANA, consultare la sezione "Opzioni di implementazione per il plug-in SAP HANA".



i I plug-in HANA e Linux sono attualmente disponibili solo per i sistemi basati su Intel. Se i database HANA sono in esecuzione su IBM Power Systems, è necessario utilizzare un host plug-in HANA centrale.

Architetture HANA supportate per il rilevamento automatico e il ripristino automatizzato

Con SnapCenter, il rilevamento automatico e il ripristino e ripristino automatici sono supportati per la maggior parte delle configurazioni HANA, con l’eccezione che i sistemi host multipli HANA richiedono una configurazione manuale.

La seguente tabella mostra le configurazioni HANA supportate per il rilevamento automatico.

Plug-in HANA installato su:	Architettura HANA	Configurazione del sistema HANA	Infrastruttura
Host del database HANA	Host singolo	<ul style="list-style-type: none"> • Container singolo HANA • Contenitori di database multi-tenant SAP HANA (MDC) con uno o più tenant • Replica di sistema HANA 	<ul style="list-style-type: none"> • Bare metal con NFS • Bare metal con XFS e FC con o senza Linux Logical Volume Manager (LVM) • VMware con montaggi NFS diretti per il sistema operativo



I sistemi HANA MDC con più tenant sono supportati per il rilevamento automatico, ma non per il ripristino e il ripristino automatici con la release corrente di SnapCenter.

Architetture HANA supportate per la configurazione manuale delle risorse HANA

La configurazione manuale delle risorse HANA è supportata per tutte le architetture HANA; tuttavia, richiede un host plug-in HANA centrale. L'host del plug-in centrale può essere il server SnapCenter stesso o un host Linux o Windows separato.



Quando il plug-in HANA viene distribuito sull'host del database HANA, per impostazione predefinita, la risorsa viene rilevata automaticamente. La funzione di rilevamento automatico può essere disattivata per i singoli host, in modo che il plug-in possa essere implementato, ad esempio su un host di database con replica di sistema HANA attivata e una release di SnapCenter < 4.6, in cui la funzione di rilevamento automatico non è supportata. Per ulteriori informazioni, vedere la sezione ["Disattiva il rilevamento automatico sull'host plug-in HANA."](#)

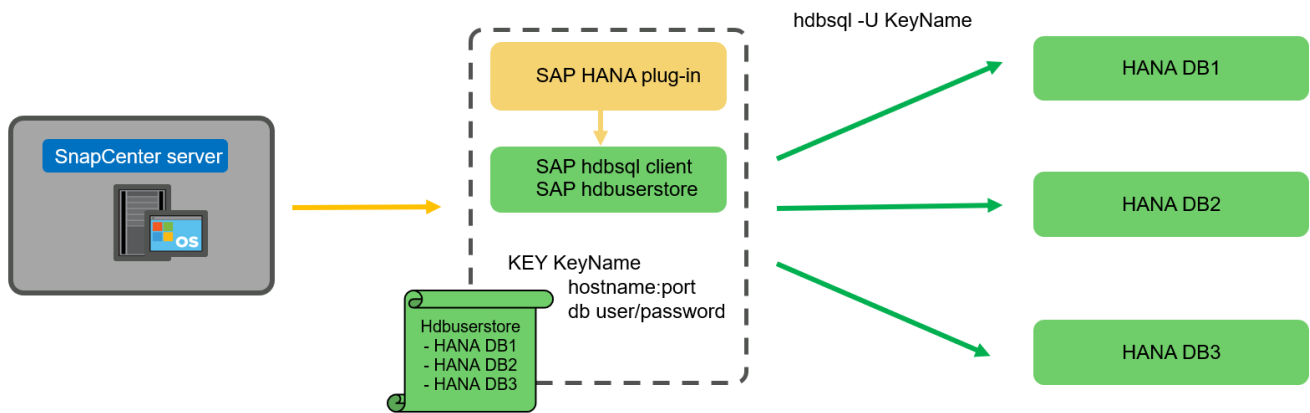
La tabella seguente mostra le configurazioni HANA supportate per la configurazione manuale delle risorse HANA.

Plug-in HANA installato su:	Architettura HANA	Configurazione del sistema HANA	Infrastruttura
Host plug-in centrale (server SnapCenter o host Linux separato)	Host singolo o multiplo	<ul style="list-style-type: none"> • Container singolo HANA • HANA MDC con uno o più tenant • Replica di sistema HANA 	<ul style="list-style-type: none"> • Bare metal con NFS • Bare metal con XFS e FC con o senza Linux LVM • VMware con montaggi NFS diretti per il sistema operativo

Opzioni di implementazione per il plug-in SAP HANA

La figura seguente mostra la vista logica e la comunicazione tra il server SnapCenter e i database SAP HANA.

Il server SnapCenter comunica tramite il plug-in SAP HANA con i database SAP HANA. Il plug-in SAP HANA utilizza il software client SAP HANA hdbsql per eseguire comandi SQL nei database SAP HANA. SAP HANA hdbuserstore viene utilizzato per fornire le credenziali dell'utente, il nome host e le informazioni sulla porta per accedere ai database SAP HANA.



Il plug-in SAP HANA e il software client SAP hdbsql, che includono il tool di configurazione hdbuserstore, devono essere installati insieme sullo stesso host.

L'host può essere il server SnapCenter stesso, un host plug-in centrale separato o i singoli host di database SAP HANA.

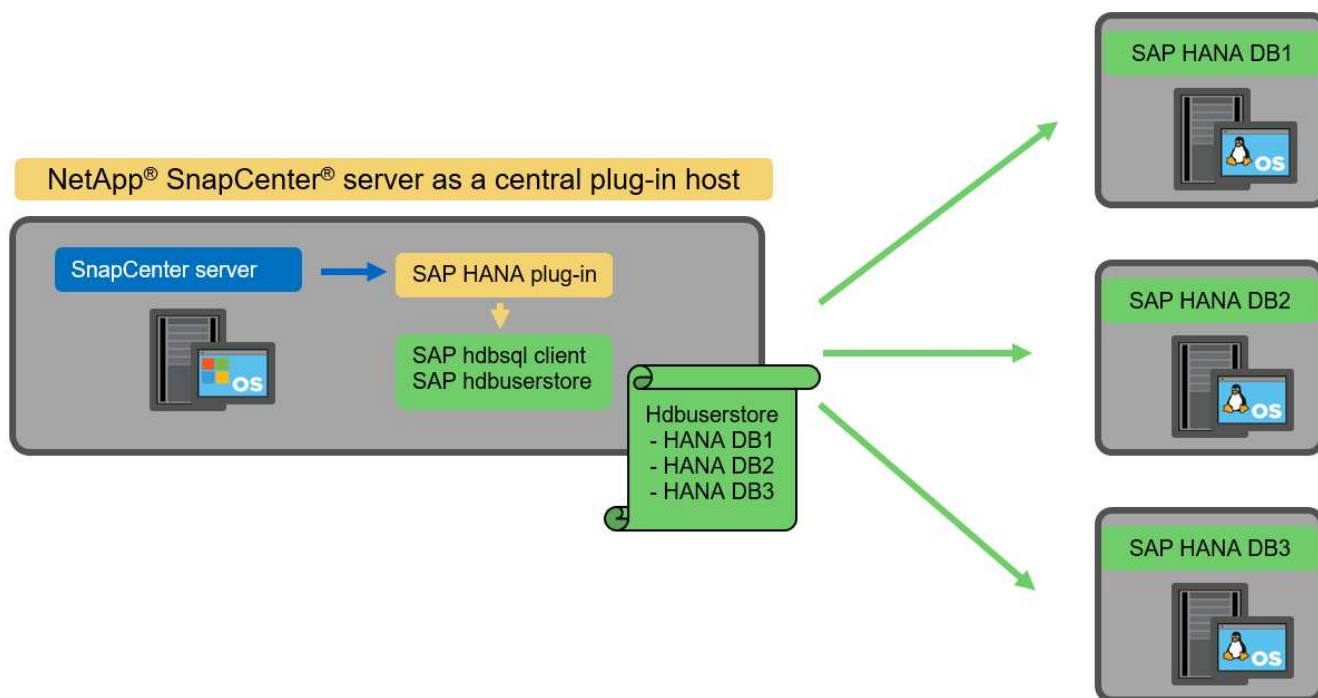
Server SnapCenter ad alta disponibilità

SnapCenter può essere configurato in una configurazione ha a due nodi. In una tale configurazione, un bilanciamento del carico (ad esempio F5) viene utilizzato in una modalità attiva/passiva utilizzando un indirizzo IP virtuale che punta all'host SnapCenter attivo. Il repository SnapCenter (il database MySQL) viene replicato da SnapCenter tra i due host in modo che i dati SnapCenter siano sempre sincronizzati.

Il server SnapCenter ha non è supportato se il plug-in HANA è installato sul server SnapCenter. Se si intende configurare SnapCenter in una configurazione ha, non installare il plug-in HANA sul server SnapCenter. Ulteriori informazioni su SnapCenter ha sono disponibili al seguente indirizzo ["Pagina della Knowledge base di NetApp"](#).

Server SnapCenter come host plug-in HANA centrale

La figura seguente mostra una configurazione in cui il server SnapCenter viene utilizzato come host plug-in centrale. Il plug-in SAP HANA e il software client SAP hdbsql sono installati sul server SnapCenter.



Poiché il plug-in HANA può comunicare con i database HANA gestiti utilizzando il client hdb attraverso la rete, non è necessario installare alcun componente SnapCenter sui singoli host di database HANA. SnapCenter può proteggere i database HANA utilizzando un plug-in host centrale HANA su cui sono configurate tutte le chiavi dell'archivio utenti per i database gestiti.

D'altro canto, l'automazione avanzata del workflow per il rilevamento automatico, l'automazione del ripristino e del ripristino, nonché le operazioni di refresh del sistema SAP, richiedono l'installazione dei componenti SnapCenter sull'host del database. Quando si utilizza un host plug-in HANA centrale, queste funzioni non sono disponibili.

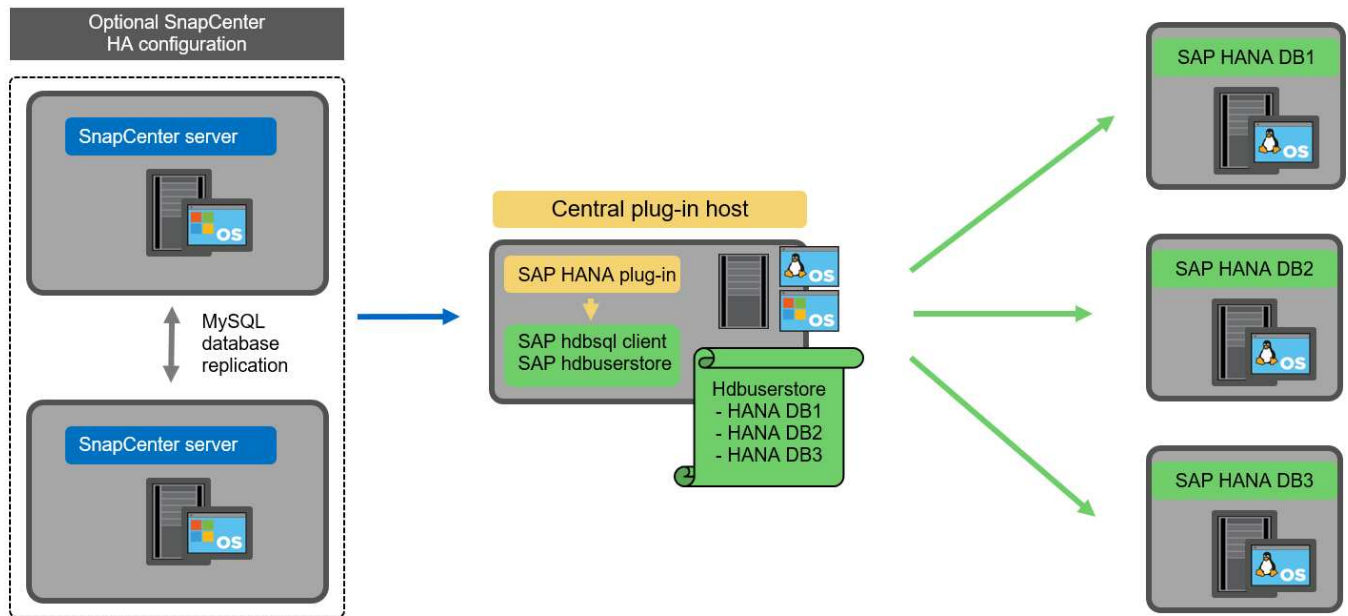
Inoltre, l'elevata disponibilità del server SnapCenter che utilizza la funzionalità ha integrata non può essere utilizzata quando il plug-in HANA è installato sul server SnapCenter. È possibile ottenere un'elevata disponibilità utilizzando VMware se il server SnapCenter viene eseguito in una macchina virtuale all'interno di un cluster VMware.

Separare l'host come host plug-in HANA centrale

La figura seguente mostra una configurazione in cui un host Linux separato viene utilizzato come host plug-in centrale. In questo caso, il plug-in SAP HANA e il software client SAP hdbsql vengono installati sull'host Linux.



Il plug-in host centrale separato può anche essere un host Windows.

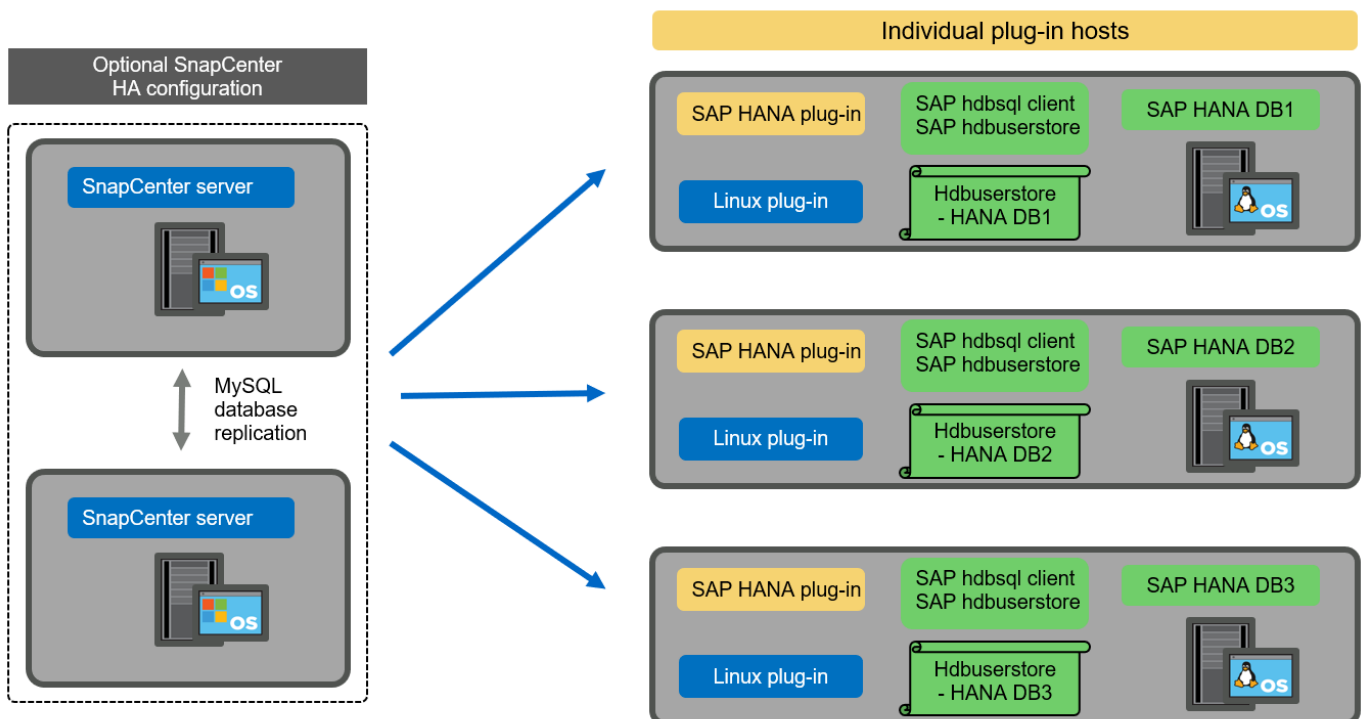


La stessa restrizione relativa alla disponibilità delle funzionalità descritta nella sezione precedente si applica anche a un host plug-in centrale separato.

Tuttavia, con questa opzione di implementazione, il server SnapCenter può essere configurato con la funzionalità ha integrata. Anche l'host del plug-in centrale deve essere ha, ad esempio, utilizzando una soluzione cluster Linux.

Plug-in HANA implementato su singoli host di database HANA

La figura seguente mostra una configurazione in cui il plug-in SAP HANA è installato su ciascun host di database SAP HANA.



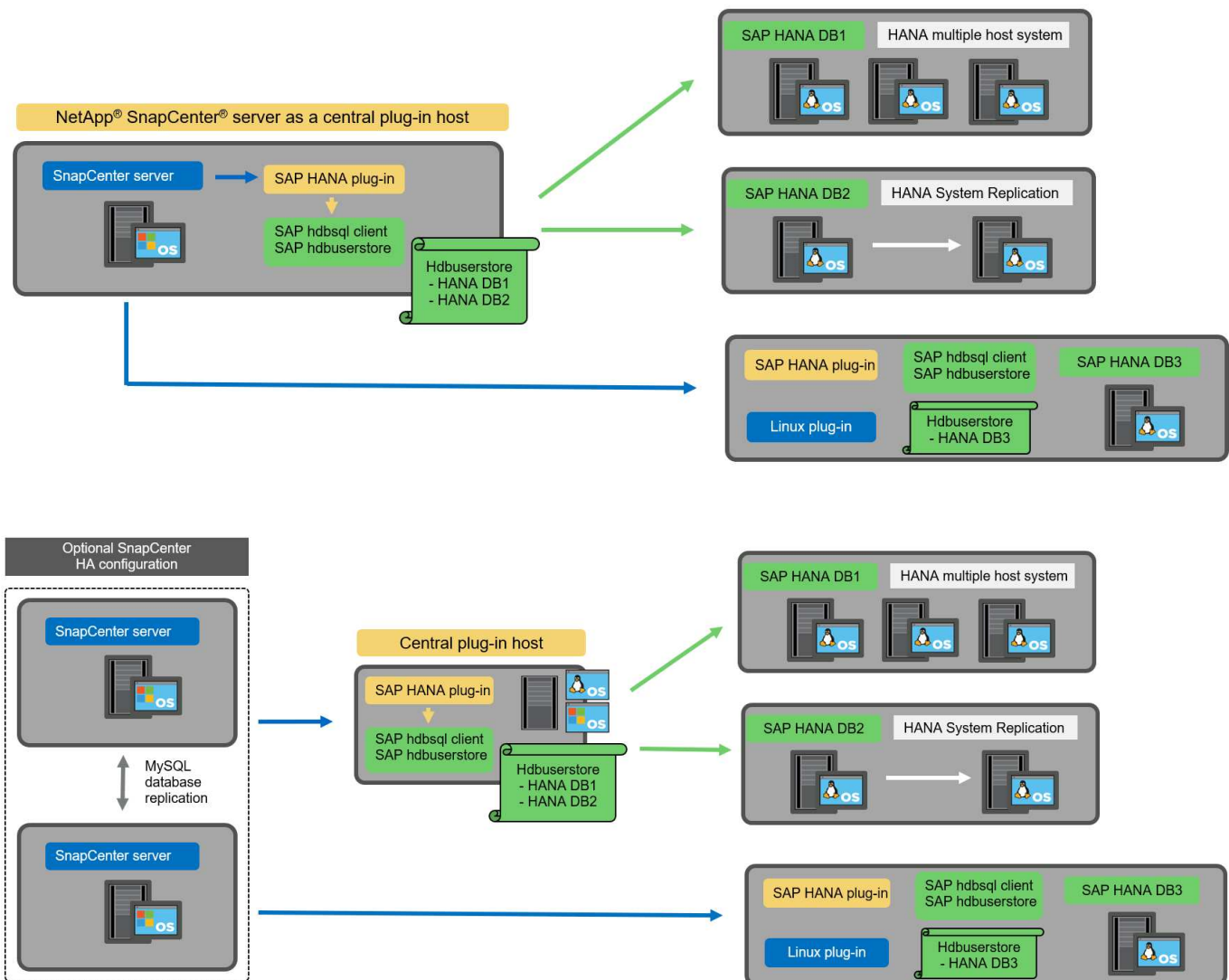
Quando il plug-in HANA viene installato su ogni singolo host di database HANA, sono disponibili tutte le funzionalità, come il rilevamento automatico e il ripristino e ripristino automatici. Inoltre, il server SnapCenter può essere configurato in una configurazione ha.

Implementazione di plug-in HANA misti

Come discusso all'inizio di questa sezione, alcune configurazioni di sistema HANA, come i sistemi a più host, richiedono un host plug-in centrale. Pertanto, la maggior parte delle configurazioni SnapCenter richiede un'implementazione mista del plug-in HANA.

NetApp consiglia di implementare il plug-in HANA sull'host del database HANA per tutte le configurazioni di sistema HANA supportate per il rilevamento automatico. Gli altri sistemi HANA, come le configurazioni di più host, devono essere gestiti con un host plug-in HANA centrale.

Le due figure seguenti mostrano le implementazioni di plug-in misti con il server SnapCenter o un host Linux separato come host plug-in centrale. L'unica differenza tra queste due implementazioni è la configurazione ha opzionale.



Riepilogo e consigli

In generale, NetApp consiglia di implementare il plug-in HANA su ciascun host SAP HANA per abilitare tutte le

funzionalità HANA SnapCenter disponibili e migliorare l'automazione del workflow.



I plug-in HANA e Linux sono attualmente disponibili solo per i sistemi basati su Intel. Se i database HANA sono in esecuzione su IBM Power Systems, è necessario utilizzare un host plug-in HANA centrale.

Per le configurazioni HANA in cui non è supportato il rilevamento automatico, come ad esempio le configurazioni di più host HANA, è necessario configurare un host plug-in HANA centrale aggiuntivo. L'host del plug-in centrale può essere il server SnapCenter se VMware ha può essere utilizzato per SnapCenter ha. Se si intende utilizzare la funzionalità ha integrata di SnapCenter, utilizzare un host plug-in Linux separato.

Nella tabella seguente sono riepilogate le diverse opzioni di implementazione.

Opzione di implementazione	Dipendenze
Plug-in host HANA centrale installato sul server SnapCenter	Pro: * Plug-in HANA singolo, configurazione centrale dello store utente HDB * Nessun componente software SnapCenter richiesto su singoli host di database HANA * supporto di tutte le architetture HANA Cons: * Configurazione manuale delle risorse * Ripristino manuale * Nessun supporto per il ripristino di un singolo tenant * qualsiasi istruzione pre e post-script viene eseguita sull'host del plug-in centrale * disponibilità elevata SnapCenter integrata non supportata * la combinazione di SID e nome del tenant deve essere univoca in tutti i database HANA gestiti * Registro Gestione della conservazione dei backup abilitata/disabilitata per tutti i database HANA gestiti
Plug-in host HANA centrale installato su server Linux o Windows separati	Pro: * Plug-in HANA singolo, configurazione centrale dello store utente HDB * Nessun componente software SnapCenter richiesto su singoli host di database HANA * supporto di tutte le architetture HANA * SnapCenter integrato ad alta disponibilità supportato Cons: * Configurazione manuale delle risorse * Ripristino manuale * Nessun supporto per il ripristino di un singolo tenant * qualsiasi istruzione pre e post-script viene eseguita sull'host del plug-in centrale * la combinazione di SID e nome del tenant deve essere unica in tutti i database HANA gestiti * Gestione della conservazione del backup del log attivata/disattivata per tutti i database gestiti Database HANA

Opzione di implementazione	Dipendenze
Plug-in host singolo HANA installato sul server di database HANA	Pro: * Rilevamento automatico delle risorse HANA * Ripristino e ripristino automatizzati * Ripristino singolo tenant * automazione pre e post-script per il refresh del sistema SAP * disponibilità elevata SnapCenter integrata supportata * Gestione della conservazione del backup dei log attivabile/disattivabile per ogni singolo database HANA Cons: * Non supportato per tutte le architetture HANA. È richiesto un host plug-in centrale aggiuntivo per sistemi host multipli HANA. * Il plug-in HANA deve essere implementato su ogni host di database HANA

Strategia di protezione dei dati

Prima di configurare SnapCenter e il plug-in SAP HANA, la strategia di protezione dei dati deve essere definita in base ai requisiti RTO e RPO dei vari sistemi SAP.

Un approccio comune consiste nella definizione di tipi di sistema quali produzione, sviluppo, test o sistemi sandbox. Tutti i sistemi SAP dello stesso tipo di sistema hanno in genere gli stessi parametri di protezione dei dati.

I parametri da definire sono:

- Con quale frequenza deve essere eseguito un backup Snapshot?
- Per quanto tempo i backup delle copie Snapshot devono essere conservati nel sistema di storage primario?
- Con quale frequenza deve essere eseguito un controllo dell'integrità dei blocchi?
- I backup primari devono essere replicati in un sito di backup off-site?
- Per quanto tempo i backup devono essere conservati nello storage di backup off-site?

La seguente tabella mostra un esempio di parametri di protezione dei dati per la produzione, lo sviluppo e il test del tipo di sistema. Per il sistema di produzione, è stata definita una frequenza di backup elevata e i backup vengono replicati su un sito di backup off-site una volta al giorno. I sistemi di test hanno requisiti inferiori e nessuna replica dei backup.

Parametri	Sistemi di produzione	Sistemi di sviluppo	Sistemi di test
Frequenza di backup	Ogni 4 ore	Ogni 4 ore	Ogni 4 ore
Conservazione primaria	2 giorni	2 giorni	2 giorni
Controllo dell'integrità del blocco	Una volta alla settimana	Una volta alla settimana	No
Replica su un sito di backup off-site	Una volta al giorno	Una volta al giorno	No
Conservazione del backup off-site	2 settimane	2 settimane	Non applicabile

La tabella seguente mostra i criteri che devono essere configurati per i parametri di protezione dei dati.

Parametri	PolicyLocalSnap	PolicyLocalSnapAndSnapVault	PolicyBlockIntegrityCheck
Tipo di backup	Basato su Snapshot	Basato su Snapshot	Basato su file
Frequenza di pianificazione	Ogni ora	Ogni giorno	Settimanale
Conservazione primaria	Conteggio = 12	Conteggio = 3	Conteggio = 1
Replica SnapVault	No	Sì	Non applicabile

La policy `LocalSnapshot` Viene utilizzato per i sistemi di produzione, sviluppo e test per coprire i backup Snapshot locali con una conservazione di due giorni.

Nella configurazione di protezione delle risorse, la pianificazione viene definita in modo diverso per i tipi di sistema:

- **Produzione.** programma ogni 4 ore.
- **Sviluppo.** programma ogni 4 ore.
- **Test.** programma ogni 4 ore.

La policy `LocalSnapAndSnapVault` viene utilizzato per i sistemi di produzione e sviluppo per coprire la replica giornaliera nello storage di backup off-site.

Nella configurazione della protezione delle risorse, viene definito il calendario per la produzione e lo sviluppo:

- **Produzione.** programma ogni giorno.
- **Sviluppo.** programma ogni giorno.

La policy `BlockIntegrityCheck` viene utilizzato per i sistemi di produzione e sviluppo per la verifica settimanale dell'integrità dei blocchi mediante un backup basato su file.

Nella configurazione della protezione delle risorse, viene definito il calendario per la produzione e lo sviluppo:

- **Produzione.** programma ogni settimana.
- *** Sviluppo.*** programma ogni settimana.

Per ogni singolo database SAP HANA che utilizza la policy di backup off-site, è necessario configurare una relazione di protezione sul layer di storage. La relazione di protezione definisce quali volumi vengono replicati e la conservazione dei backup nello storage di backup off-site.

Con il nostro esempio, per ogni sistema di produzione e sviluppo, viene definita una conservazione di due settimane nello storage di backup off-site.



Nel nostro esempio, le policy di protezione e la conservazione per le risorse di database SAP HANA e per le risorse non di volumi di dati non sono diverse.

Operazioni di backup

SAP ha introdotto il supporto dei backup Snapshot per i sistemi multi-tenant MDC con HANA 2.0 SPS4. SnapCenter supporta le operazioni di backup Snapshot dei sistemi HANA MDC con tenant multipli. SnapCenter supporta inoltre due diverse operazioni di ripristino di un sistema HANA MDC. È possibile ripristinare l'intero sistema, il database di sistema e tutti i tenant oppure un solo tenant. Esistono alcuni

prerequisiti per consentire a SnapCenter di eseguire queste operazioni.

In un sistema MDC, la configurazione del tenant non è necessariamente statica. È possibile aggiungere tenant o eliminarli. SnapCenter non può fare affidamento sulla configurazione rilevata quando il database HANA viene aggiunto a SnapCenter. SnapCenter deve sapere quali tenant sono disponibili nel momento in cui viene eseguita l'operazione di backup.

Per abilitare una singola operazione di ripristino del tenant, SnapCenter deve sapere quali tenant sono inclusi in ogni backup Snapshot. Inoltre, deve sapere quali file e directory appartengono a ciascun tenant incluso nel backup Snapshot.

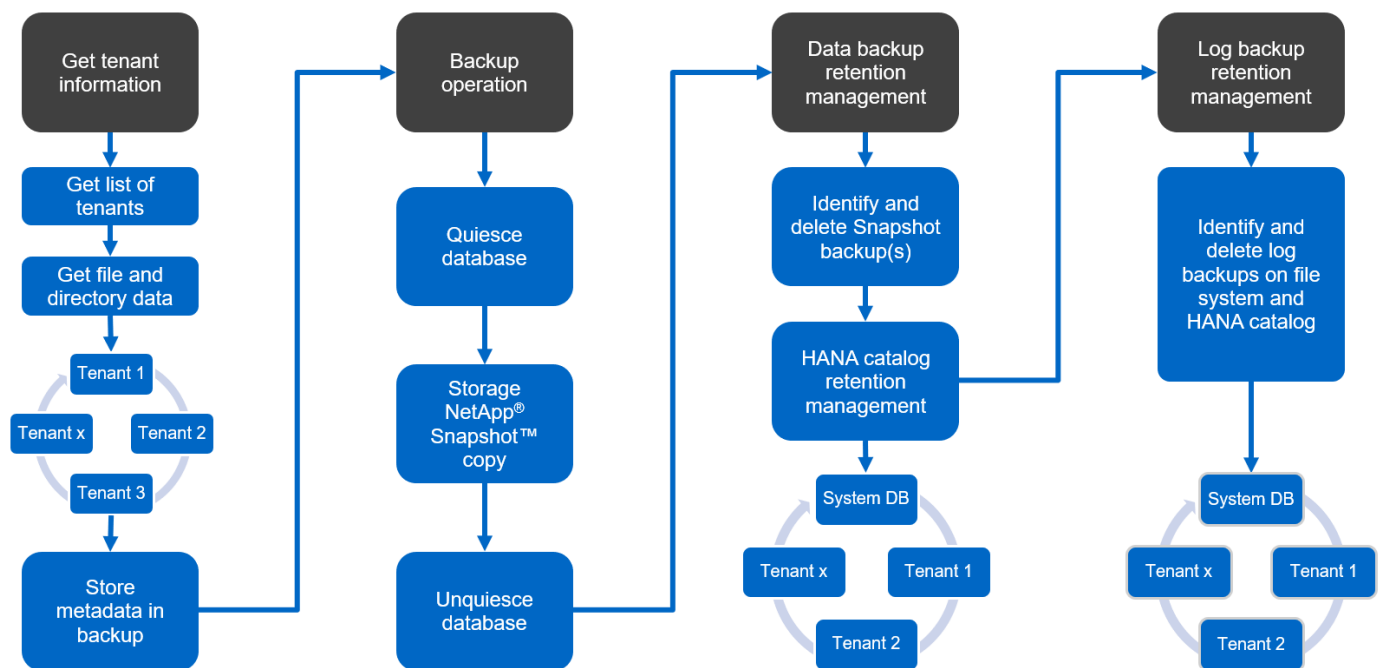
Pertanto, con ogni operazione di backup, il primo passo nel flusso di lavoro è ottenere le informazioni sul tenant. Sono inclusi i nomi dei tenant e le informazioni relative a file e directory corrispondenti. Questi dati devono essere memorizzati nei metadati di backup Snapshot per poter supportare una singola operazione di ripristino del tenant. Il passo successivo è l'operazione di backup Snapshot. Questo passaggio include il comando SQL per attivare il punto di salvataggio del backup HANA, il backup Snapshot dello storage e il comando SQL per chiudere l'operazione Snapshot. Utilizzando il comando close, il database HANA aggiorna il catalogo di backup del database di sistema e di ciascun tenant.



SAP non supporta le operazioni di backup Snapshot per i sistemi MDC quando uno o più tenant vengono arrestati.

Per la gestione della conservazione dei backup dei dati e della gestione del catalogo di backup HANA, SnapCenter deve eseguire le operazioni di eliminazione del catalogo per il database di sistema e per tutti i database tenant identificati nella prima fase. Allo stesso modo per i backup dei log, il flusso di lavoro di SnapCenter deve operare su ogni tenant che faceva parte dell'operazione di backup.

La figura seguente mostra una panoramica del flusso di lavoro di backup.



Workflow di backup per i backup Snapshot del database HANA

SnapCenter esegue il backup del database SAP HANA nella seguente sequenza:

1. SnapCenter legge l'elenco dei tenant dal database HANA.
2. SnapCenter legge i file e le directory di ciascun tenant dal database HANA.
3. Le informazioni del tenant vengono memorizzate nei metadati SnapCenter per questa operazione di backup.
4. SnapCenter attiva un punto di salvataggio di backup sincronizzato globale SAP HANA per creare un'immagine di database coerente sul layer di persistenza.



Per un sistema di tenant singolo o multiplo SAP HANA MDC, viene creato un punto di salvataggio di backup globale sincronizzato per il database di sistema e per ogni database tenant.

5. SnapCenter crea copie Snapshot dello storage per tutti i volumi di dati configurati per la risorsa. Nel nostro esempio di database HANA a host singolo, esiste un solo volume di dati. Con un database multi-host SAP HANA, esistono più volumi di dati.
6. SnapCenter registra il backup Snapshot dello storage nel catalogo di backup SAP HANA.
7. SnapCenter elimina il punto di salvataggio del backup SAP HANA.
8. SnapCenter avvia un aggiornamento di SnapVault o SnapMirror per tutti i volumi di dati configurati nella risorsa.



Questo passaggio viene eseguito solo se il criterio selezionato include una replica di SnapVault o SnapMirror.

9. SnapCenter elimina le copie Snapshot dello storage e le voci di backup nel database e nel catalogo di backup SAP HANA in base alla policy di conservazione definita per i backup nello storage primario. Le operazioni del catalogo di backup HANA vengono eseguite per il database di sistema e per tutti i tenant.



Se il backup è ancora disponibile nello storage secondario, la voce del catalogo SAP HANA non viene eliminata.

10. SnapCenter elimina tutti i backup dei log nel file system e nel catalogo di backup SAP HANA precedenti al backup dei dati meno recente identificato nel catalogo di backup SAP HANA. Queste operazioni vengono eseguite per il database di sistema e per tutti i tenant.



Questo passaggio viene eseguito solo se la gestione del backup dei log non è disattivata.

Workflow di backup per operazioni di controllo dell'integrità dei blocchi

SnapCenter esegue il controllo dell'integrità del blocco nella seguente sequenza:

1. SnapCenter legge l'elenco dei tenant dal database HANA.
2. SnapCenter attiva un'operazione di backup basata su file per il database di sistema e per ciascun tenant.
3. SnapCenter elimina i backup basati su file nel proprio database, nel file system e nel catalogo di backup SAP HANA in base alla policy di conservazione definita per le operazioni di controllo dell'integrità dei blocchi. Le operazioni di eliminazione del backup nel file system e nel catalogo di backup HANA vengono eseguite per il database di sistema e per tutti i tenant.
4. SnapCenter elimina tutti i backup dei log nel file system e nel catalogo di backup SAP HANA precedenti al backup dei dati meno recente identificato nel catalogo di backup SAP HANA. Queste operazioni vengono eseguite per il database di sistema e per tutti i tenant.



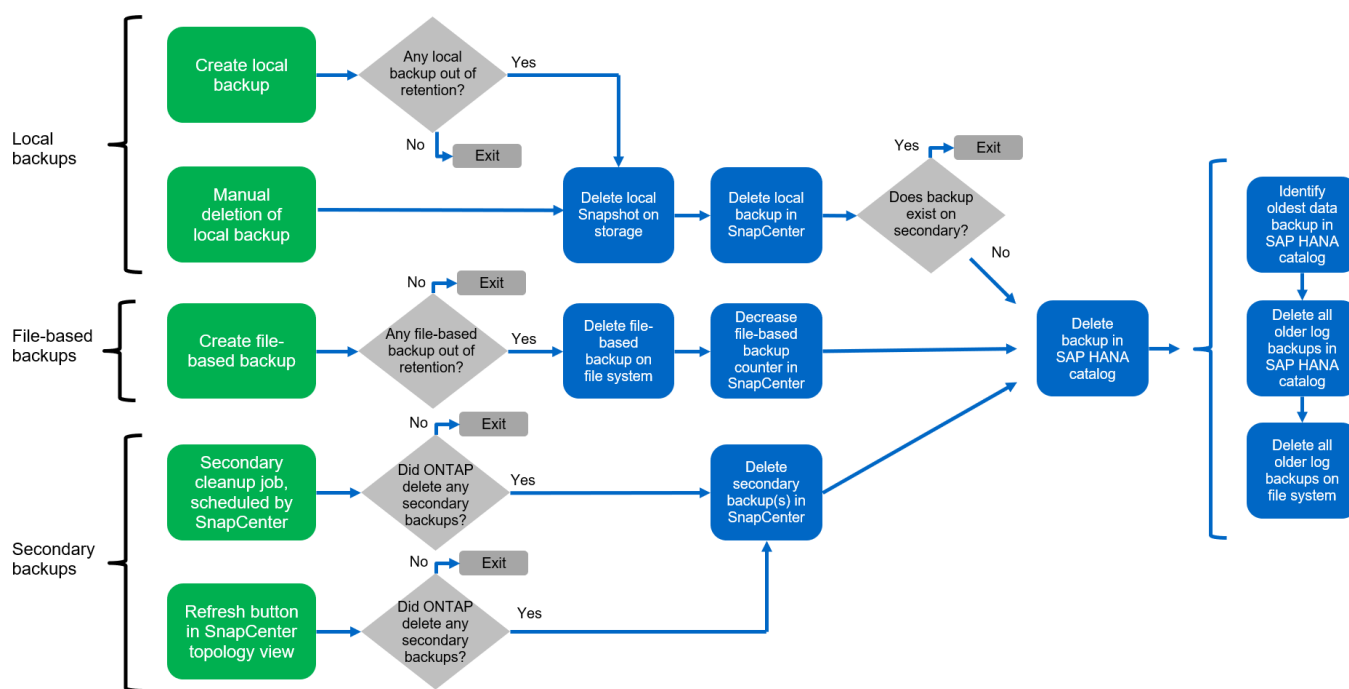
Questo passaggio viene eseguito solo se la gestione del backup dei log non è disattivata.

Gestione della conservazione dei backup e gestione dei backup di dati e log

La gestione della conservazione dei backup dei dati e la gestione del backup dei log possono essere suddivise in cinque aree principali, tra cui la gestione della conservazione di:

- Backup locali nello storage primario
- Backup basati su file
- Backup nello storage secondario
- Backup dei dati nel catalogo di backup SAP HANA
- Registrare i backup nel catalogo di backup SAP HANA e nel file system

La figura seguente fornisce una panoramica dei diversi flussi di lavoro e delle dipendenze di ciascuna operazione. Le sezioni seguenti descrivono in dettaglio le diverse operazioni.



Gestione della conservazione dei backup locali nello storage primario

SnapCenter gestisce la gestione dei backup dei database SAP HANA e dei backup dei volumi non dati eliminando le copie Snapshot sullo storage primario e nel repository SnapCenter in base a una conservazione definita nella policy di backup di SnapCenter.

La logica di gestione della conservazione viene eseguita con ogni flusso di lavoro di backup in SnapCenter.



Tenere presente che SnapCenter gestisce la gestione della conservazione individualmente per i backup pianificati e on-demand.

I backup locali nello storage primario possono anche essere cancellati manualmente in SnapCenter.

Gestione della conservazione dei backup basati su file

SnapCenter gestisce la gestione dei backup basati su file eliminando i backup sul file system in base a una conservazione definita nella policy di backup di SnapCenter.

La logica di gestione della conservazione viene eseguita con ogni flusso di lavoro di backup in SnapCenter.



Tenere presente che SnapCenter gestisce la gestione della conservazione individualmente per i backup pianificati o on-demand.

Gestione della conservazione dei backup nello storage secondario

La gestione della conservazione dei backup nello storage secondario viene gestita da ONTAP in base alla conservazione definita nella relazione di protezione ONTAP.

Per sincronizzare queste modifiche sullo storage secondario nel repository SnapCenter, SnapCenter utilizza un lavoro di pulizia pianificato. Questo processo di pulizia sincronizza tutti i backup dello storage secondario con il repository SnapCenter per tutti i plug-in SnapCenter e tutte le risorse.

Per impostazione predefinita, il lavoro di pulizia viene pianificato una volta alla settimana. Questa pianificazione settimanale comporta un ritardo nell'eliminazione dei backup in SnapCenter e SAP HANA Studio rispetto ai backup già cancellati nello storage secondario. Per evitare questa incoerenza, i clienti possono modificare la pianificazione con una frequenza più elevata, ad esempio una volta al giorno.



Il processo di pulitura può essere attivato anche manualmente per una singola risorsa facendo clic sul pulsante Refresh (Aggiorna) nella vista della topologia della risorsa.

Per informazioni dettagliate su come adattare la pianificazione del lavoro di pulizia o come attivare un aggiornamento manuale, fare riferimento alla sezione ["Modificare la frequenza di pianificazione della sincronizzazione del backup con lo storage di backup off-site."](#)

Gestione della conservazione dei backup dei dati all'interno del catalogo di backup SAP HANA

Quando SnapCenter ha eliminato qualsiasi backup, snapshot locale o basato su file o ha identificato l'eliminazione del backup nello storage secondario, questo backup dei dati viene eliminato anche nel catalogo di backup SAP HANA.

Prima di eliminare la voce del catalogo SAP HANA per un backup Snapshot locale nello storage primario, SnapCenter verifica se il backup esiste ancora nello storage secondario.

Gestione della conservazione dei backup dei log

Il database SAP HANA crea automaticamente i backup dei log. Queste operazioni di backup dei log creano file di backup per ogni singolo servizio SAP HANA in una directory di backup configurata in SAP HANA.

I backup dei log precedenti all'ultimo backup dei dati non sono più necessari per il ripristino in avanti e possono quindi essere cancellati.

SnapCenter gestisce la gestione dei backup dei file di log a livello di file system e nel catalogo di backup SAP HANA eseguendo i seguenti passaggi:

1. SnapCenter legge il catalogo di backup SAP HANA per ottenere l'ID di backup del backup più vecchio basato su file o Snapshot.
2. SnapCenter elimina tutti i backup dei log nel catalogo SAP HANA e il file system che sono più vecchi di

questo ID di backup.



SnapCenter gestisce l'housekeeping solo per i backup creati da SnapCenter. Se vengono creati backup aggiuntivi basati su file al di fuori di SnapCenter, è necessario assicurarsi che i backup basati su file vengano eliminati dal catalogo di backup. Se tale backup dei dati non viene eliminato manualmente dal catalogo di backup, può diventare il backup dei dati meno recente e i backup dei log meno recenti non vengono cancellati fino a quando questo backup basato su file non viene eliminato.



Anche se viene definita una conservazione per i backup on-demand nella configurazione dei criteri, la pulizia viene eseguita solo quando viene eseguito un altro backup on-demand. Di conseguenza, i backup on-demand devono essere cancellati manualmente in SnapCenter per assicurarsi che questi backup vengano eliminati anche nel catalogo di backup SAP HANA e che la manutenzione del backup dei log non sia basata su un vecchio backup on-demand.

La gestione della conservazione dei backup dei log è attivata per impostazione predefinita. Se necessario, può essere disattivato come descritto nella sezione [""Disattiva il rilevamento automatico sull'host plug-in HANA.""](#)

Requisiti di capacità per i backup Snapshot

È necessario considerare il tasso di cambiamento di blocco più elevato sul livello di storage rispetto al tasso di cambiamento con i database tradizionali. A causa del processo di Unione delle tabelle HANA dell'archivio di colonne, la tabella completa viene scritta su disco, non solo sui blocchi modificati.

I dati della nostra base clienti mostrano un tasso di cambiamento giornaliero compreso tra il 20% e il 50% se vengono eseguiti più backup Snapshot durante il giorno. Nella destinazione SnapVault, se la replica viene eseguita solo una volta al giorno, il tasso di cambiamento giornaliero è generalmente inferiore.

Operazioni di ripristino e recovery

Ripristinare le operazioni con SnapCenter

Dal punto di vista del database HANA, SnapCenter supporta due diverse operazioni di ripristino.

- **Ripristino della risorsa completa.** tutti i dati del sistema HANA vengono ripristinati. Se il sistema HANA contiene uno o più tenant, vengono ripristinati i dati del database di sistema e quelli di tutti i tenant.
- **Ripristino di un singolo tenant.** vengono ripristinati solo i dati del tenant selezionato.

Dal punto di vista dello storage, le suddette operazioni di ripristino devono essere eseguite in modo diverso a seconda del protocollo di storage utilizzato (NFS o SAN Fibre Channel), della protezione dei dati configurata (storage primario con o senza storage di backup fuori sede), e il backup selezionato da utilizzare per l'operazione di ripristino (ripristino dallo storage di backup primario o fuori sede).

Ripristino di una risorsa completa dallo storage primario

Quando si ripristina l'intera risorsa dallo storage primario, SnapCenter supporta due diverse funzionalità di ONTAP per eseguire l'operazione di ripristino. È possibile scegliere tra le seguenti due funzioni:

- **Volume-Based SnapRestore.** Un SnapRestore basato su volume riporta il contenuto del volume di storage allo stato del backup Snapshot selezionato.
 - Casella di controllo Volume Revert (Ripristina volume) disponibile per le risorse rilevate automaticamente utilizzando NFS.

- Pulsante di opzione complete Resource (completa risorsa) per le risorse configurate manualmente.
- **File-based SnapRestore.** Una SnapRestore basata su file, nota anche come Single file SnapRestore, ripristina tutti i singoli file (NFS) o tutte le LUN (SAN).
 - Metodo di ripristino predefinito per le risorse rilevate automaticamente. Può essere modificato utilizzando la casella di controllo Volume revert (Ripristina volume) per NFS.
 - Pulsante di opzione a livello di file per le risorse configurate manualmente.

Nella tabella seguente viene fornito un confronto tra i diversi metodi di ripristino.

	SnapRestore basato su volume	SnapRestore basato su file
Velocità delle operazioni di ripristino	Molto veloce, indipendente dalle dimensioni del volume	Operazione di ripristino molto rapida, ma utilizza un lavoro di copia in background sul sistema storage, che blocca la creazione di nuovi backup Snapshot
Cronologia del backup di Snapshot	Il ripristino a un backup Snapshot precedente rimuove tutti i backup Snapshot più recenti.	Nessuna influenza
Ripristino della struttura della directory	Viene ripristinata anche la struttura della directory	NFS: Ripristina solo i singoli file, non la struttura di directory. Se anche la struttura di directory viene persa, deve essere creata manualmente prima di eseguire l'operazione di ripristino VIENE ripristinata anche LA struttura di directory SAN:
Risorsa configurata con replica su storage di backup fuori sede	Non è possibile eseguire un ripristino basato su volume su un backup della copia Snapshot precedente alla copia Snapshot utilizzata per la sincronizzazione SnapVault	È possibile selezionare qualsiasi backup Snapshot

Ripristino di una risorsa completa dallo storage di backup fuori sede

Un ripristino dallo storage di backup offsite viene sempre eseguito utilizzando un'operazione di ripristino SnapVault in cui tutti i file o tutte le LUN del volume di storage vengono sovrascritti con il contenuto del backup Snapshot.

Ripristino di un singolo tenant

Il ripristino di un singolo tenant richiede un'operazione di ripristino basata su file. A seconda del protocollo di storage utilizzato, SnapCenter esegue diversi flussi di lavoro di ripristino.

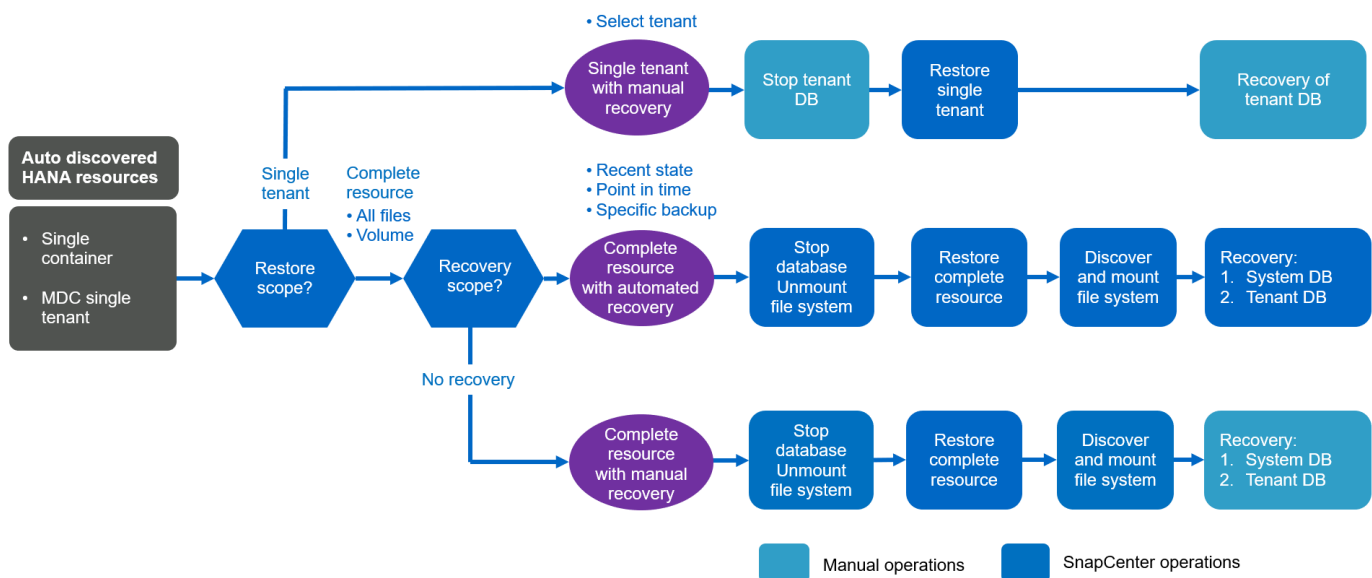
- NFS:
 - Storage primario. Le operazioni SnapRestore basate su file vengono eseguite per tutti i file del database tenant.
 - Storage di backup fuori sede: Le operazioni di ripristino SnapVault vengono eseguite per tutti i file del database tenant.

- SAN:
 - Storage primario. Clonare e connettere il LUN all'host del database e copiare tutti i file del database del tenant.
 - Storage di backup fuori sede. Clonare e connettere il LUN all'host del database e copiare tutti i file del database del tenant.

Ripristino e ripristino di sistemi HANA single container e MDC single tenant rilevati automaticamente

I sistemi HANA single container e HANA MDC single tenant rilevati automaticamente sono abilitati per il ripristino e il ripristino automatici con SnapCenter. Per questi sistemi HANA, SnapCenter supporta tre diversi flussi di lavoro di ripristino e ripristino, come mostrato nella figura seguente:

- **Tenant singolo con ripristino manuale.** se si seleziona una singola operazione di ripristino del tenant, SnapCenter elenca tutti i tenant inclusi nel backup Snapshot selezionato. È necessario arrestare e ripristinare manualmente il database del tenant. L'operazione di ripristino con SnapCenter viene eseguita con operazioni SnapRestore a file singolo per NFS o operazioni di cloning, montaggio e copia per ambienti SAN.
- **Completa la risorsa con il recovery automatizzato.** se si seleziona un'operazione completa di ripristino delle risorse e il recovery automatizzato, l'intero workflow viene automatizzato con SnapCenter. SnapCenter supporta fino a recenti stati, point-in-time o specifiche operazioni di ripristino del backup. L'operazione di ripristino selezionata viene utilizzata per il sistema e il database tenant.
- **Completare la risorsa con il ripristino manuale.** se si seleziona No Recovery, SnapCenter arresta il database HANA ed esegue le operazioni di file system (disinstallazione, montaggio) e ripristino richieste. È necessario ripristinare manualmente il sistema e il database del tenant.

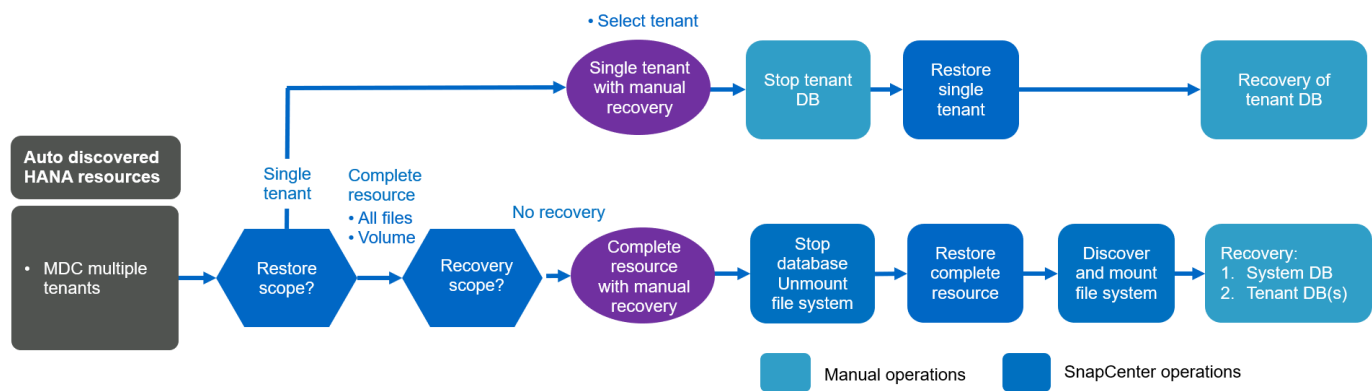


Ripristino e ripristino di più sistemi tenant HANA MDC rilevati automaticamente

Anche se i sistemi HANA MDC con più tenant possono essere rilevati automaticamente, il ripristino e il ripristino automatici non sono supportati con l'attuale release di SnapCenter. Per i sistemi MDC con tenant multipli, SnapCenter supporta due diversi flussi di lavoro di ripristino e ripristino, come illustrato nella seguente figura:

- Tenant singolo con ripristino manuale
- Risorsa completa con ripristino manuale

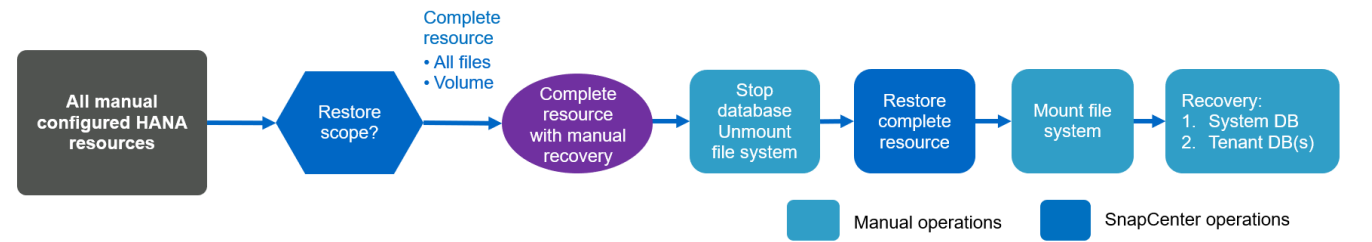
I flussi di lavoro sono gli stessi descritti nella sezione precedente.



Ripristino e ripristino di risorse HANA configurate manualmente

Le risorse HANA configurate manualmente non sono abilitate per il ripristino e il ripristino automatici. Inoltre, per i sistemi MDC con uno o più tenant, non è supportata un'operazione di ripristino del tenant singolo.

Per le risorse HANA configurate manualmente, SnapCenter supporta solo il ripristino manuale, come illustrato nella figura seguente. Il flusso di lavoro per il ripristino manuale è lo stesso descritto nelle sezioni precedenti.



Operazioni di ripristino e ripristino riepilogative

La seguente tabella riassume le operazioni di ripristino e ripristino in base alla configurazione delle risorse HANA in SnapCenter.

Configurazione delle risorse SnapCenter	Opzioni di ripristino	Arrestare il database HANA	Smontare prima, montare dopo l'operazione di ripristino	Operazione di recovery
Rilevato automaticamente singolo tenant MDC container singolo	<ul style="list-style-type: none"> • Completa la risorsa con uno dei due • Predefinito (tutti i file) • Revert del volume (NFS solo dallo storage primario) • Recovery automatica selezionata 	Automatizzato con SnapCenter	Automatizzato con SnapCenter	Automatizzato con SnapCenter
	<ul style="list-style-type: none"> • Completa la risorsa con uno dei due • Predefinito (tutti i file) • Revert del volume (NFS solo dallo storage primario) • Nessun ripristino selezionato 	Automatizzato con SnapCenter	Automatizzato con SnapCenter	Manuale
	<ul style="list-style-type: none"> • Ripristino del tenant 	Manuale	Non richiesto	Manuale
Rilevamento automatico di più tenant MDC	<ul style="list-style-type: none"> • Completa la risorsa con uno dei due • Predefinito (tutti i file) • Revert del volume (NFS solo dallo storage primario) • Recovery automatica non supportata 	Automatizzato con SnapCenter	Automatizzato con SnapCenter	Manuale

Configurazione delle risorse SnapCenter	Opzioni di ripristino	Arrestare il database HANA	Smontare prima, montare dopo l'operazione di ripristino	Operazione di recovery
	<ul style="list-style-type: none"> • Ripristino del tenant 	Manuale	Non richiesto	Manuale
Tutte le risorse configurate manualmente	<ul style="list-style-type: none"> • Risorsa completa (= Volume revert, disponibile solo per NFS e SAN dallo storage primario) • Livello file (tutti i file) • Recovery automatica non supportata 	Manuale	Manuale	Manuale

Setup di laboratorio utilizzato per questo report

La configurazione di laboratorio utilizzata per questo report tecnico include cinque diverse configurazioni SAP HANA:

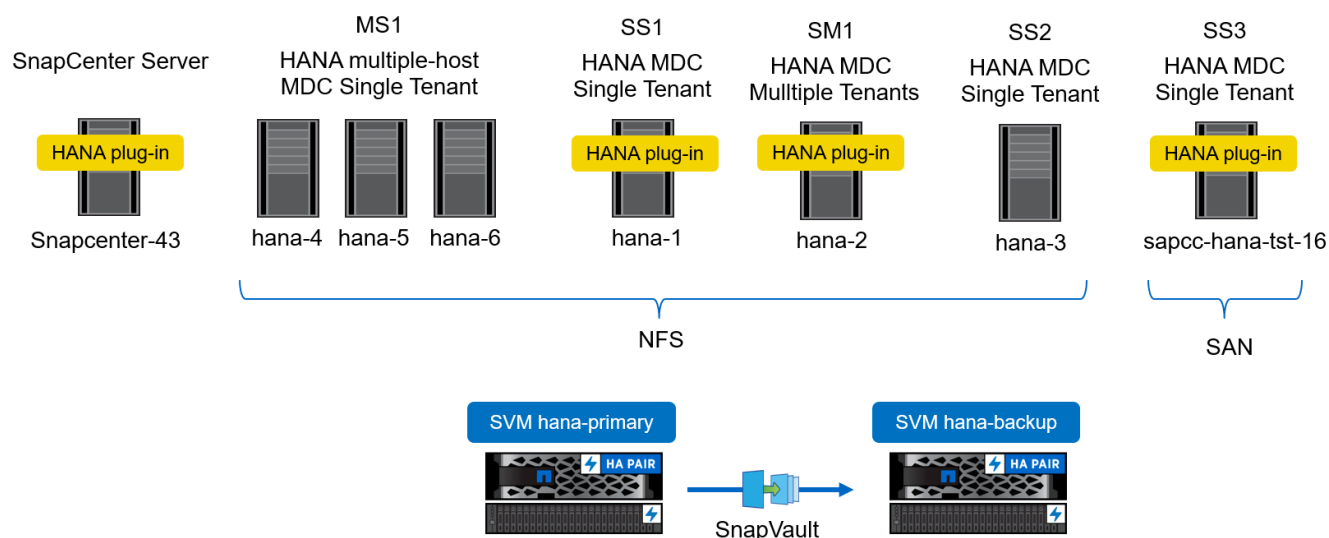
- **MS1.**
 - Sistema multi-host MDC single tenant SAP HANA
 - Gestito con un host plug-in centrale (server SnapCenter)
 - Utilizza NFS come protocollo storage
- **SS1.**
 - Sistema single-tenant SAP HANA MDC a host singolo
 - Rilevato automaticamente con il plug-in HANA installato sull'host del database HANA
 - Utilizza NFS come protocollo storage
- **SM1.**
 - Sistema multi-tenant MDC a host singolo SAP HANA
 - Rilevato automaticamente con il plug-in HANA installato sull'host del database HANA
 - Utilizza NFS come protocollo storage
- **SS2.**
 - Sistema single-tenant SAP HANA MDC a host singolo
 - Gestito con un host plug-in centrale (server SnapCenter)
 - Utilizza NFS come protocollo storage
- **SS3.**

- Sistema single-tenant SAP HANA MDC a host singolo
- Rilevato automaticamente con il plug-in HANA installato sull'host del database HANA
- Utilizza SAN Fibre Channel come protocollo storage

Le sezioni seguenti descrivono la configurazione completa e i flussi di lavoro di backup, ripristino e ripristino. La descrizione copre i backup Snapshot locali e la replica nello storage di backup utilizzando SnapVault. Le SVM (Storage Virtual Machine) lo sono `hana-primary` per lo storage primario e `hana-backup` per lo storage di backup off-site.

Il server SnapCenter viene utilizzato come host plug-in HANA centrale per i sistemi HANA MS1 e SS2.

La figura seguente mostra la configurazione del laboratorio.

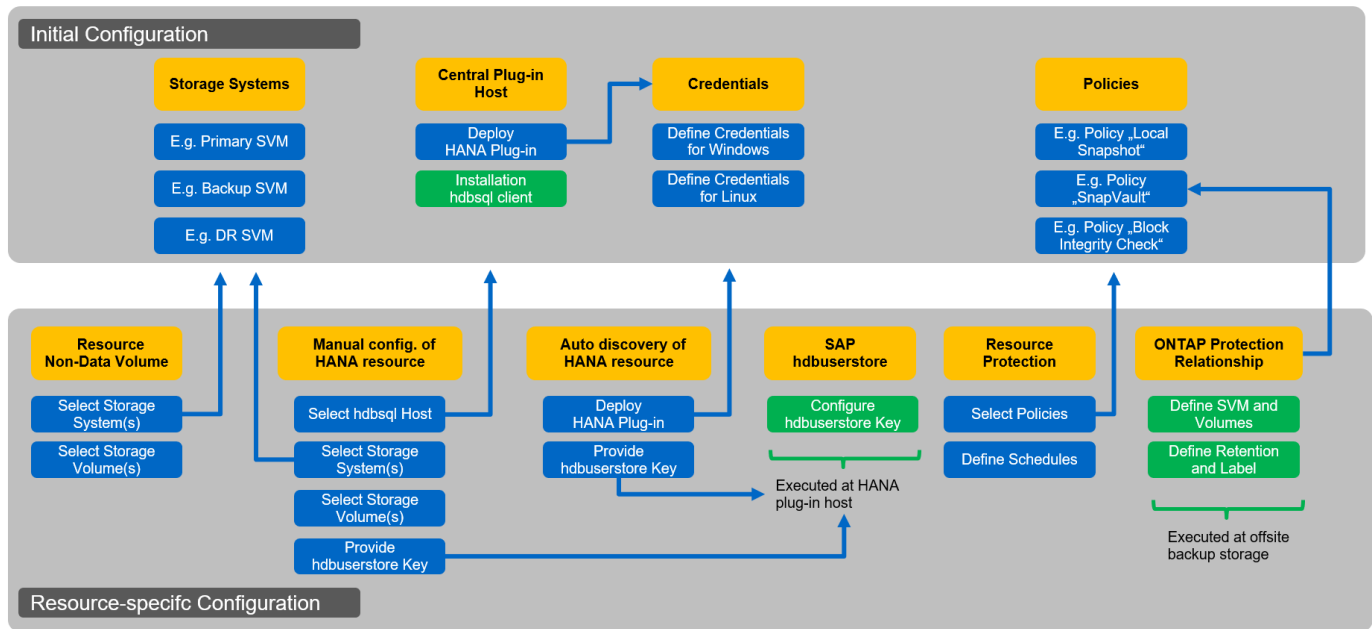


Configurazione di SnapCenter

La configurazione SnapCenter può essere divisa in due aree principali:

- **Configurazione iniziale.** copre configurazioni generiche, indipendenti da un singolo database SAP HANA. Configurazioni come sistemi storage, host plug-in HANA centrali e policy, selezionate durante l'esecuzione delle configurazioni specifiche delle risorse.
- **La configurazione specifica delle risorse.** copre le configurazioni specifiche del sistema SAP HANA e deve essere eseguita per ogni database SAP HANA.

La figura seguente fornisce una panoramica dei componenti di configurazione e delle relative dipendenze. Le caselle verdi mostrano i passaggi di configurazione che devono essere eseguiti al di fuori di SnapCenter; le caselle blu mostrano i passaggi che vengono eseguiti utilizzando l'interfaccia grafica di SnapCenter.



Con la configurazione iniziale, vengono installati e configurati i seguenti componenti:

- **Sistema di storage.** Configurazione delle credenziali per tutte le SVM utilizzate dai sistemi SAP HANA: In genere, backup primario, off-site e storage di disaster recovery.



È possibile configurare anche le credenziali del cluster di storage invece delle singole credenziali SVM.

- **Credenziali.** Configurazione delle credenziali utilizzate per implementare il plug-in SAP HANA sugli host.
- **Host (per host plug-in HANA centrali).** implementazione del plug-in SAP HANA. Installazione del software SAP HANA hdbclient sull'host. Il software SAP hdbclient deve essere installato manualmente.
- **Criteri.** Configurazione del tipo di backup, conservazione e replica. In genere, sono richiesti almeno un criterio per le copie Snapshot locali, uno per la replica SnapVault e uno per il backup basato su file.

La configurazione specifica delle risorse deve essere eseguita per ogni database SAP HANA e include le seguenti configurazioni:

- Configurazione delle risorse di volumi non dati SAP HANA:
 - Sistemi e volumi di storage
- Configurazione delle chiavi SAP hdbuserstore:
 - La configurazione della chiave hdbuserstore SAP per lo specifico database SAP HANA deve essere eseguita sull'host del plug-in centrale o sull'host del database HANA, a seconda di dove viene implementato il plug-in HANA.
- Risorse di database SAP HANA rilevate automaticamente:
 - Implementazione del plug-in SAP HANA sull'host del database
 - Fornire la chiave hdbuserstore
- Configurazione manuale delle risorse del database SAP HANA:
 - SID del database SAP HANA, host plug-in, chiave hdbuserstore, sistemi storage e volumi
- Configurazione della protezione delle risorse:

- Selezione delle policy richieste
- Definizione delle pianificazioni per ogni policy
- Configurazione della protezione dei dati ONTAP:
 - Necessario solo se i backup devono essere replicati in uno storage di backup off-site.
 - Definizione di relazione e conservazione.

Configurazione iniziale di SnapCenter

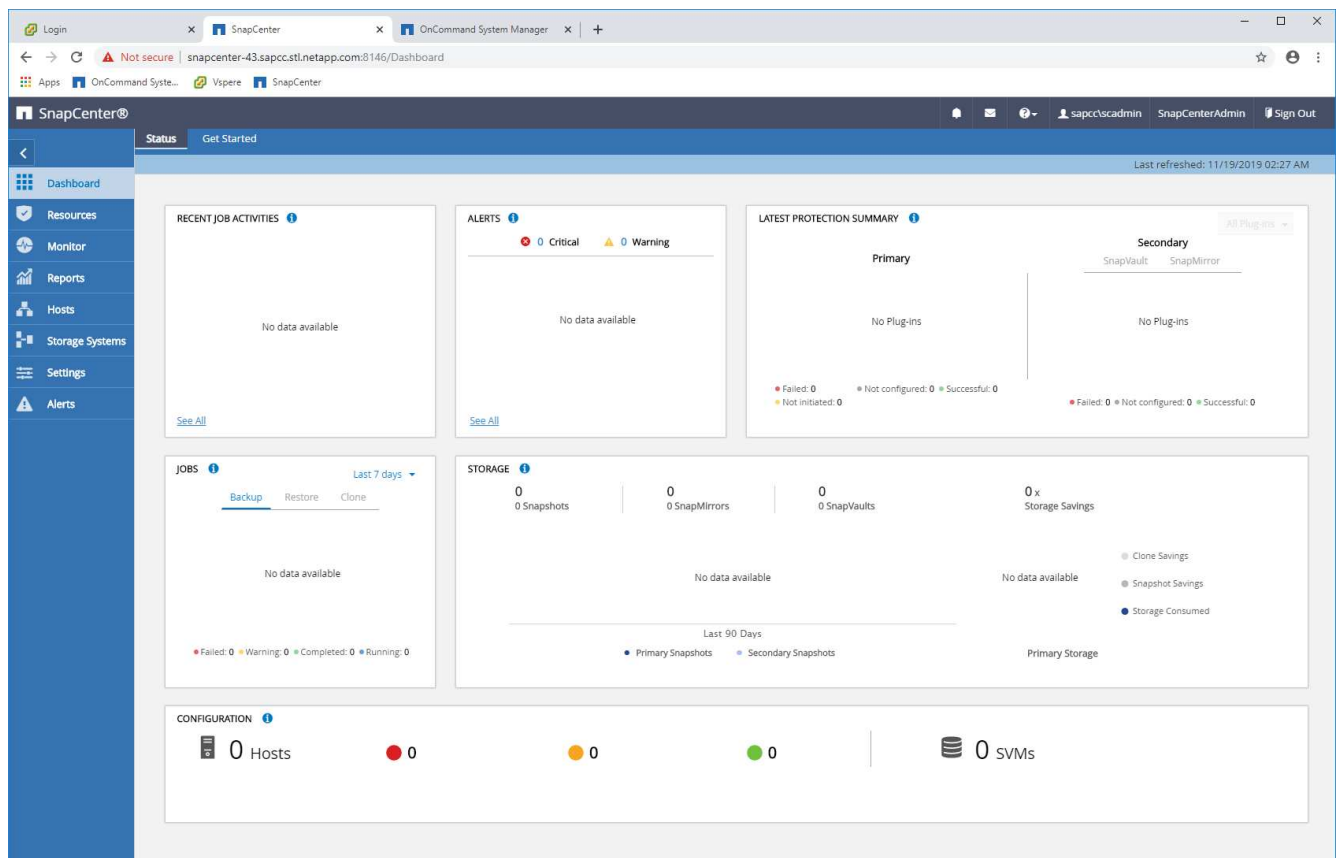
La configurazione iniziale include i seguenti passaggi:

1. Configurazione del sistema storage
2. Configurazione delle credenziali per l'installazione del plug-in
3. Per un host plug-in HANA centrale:
 - a. Configurazione dell'host e implementazione del plug-in SAP HANA
 - b. Installazione e configurazione del software client SAP HANA hdbsql
4. Configurazione dei criteri

Le sezioni seguenti descrivono le fasi iniziali della configurazione.

Configurazione del sistema storage

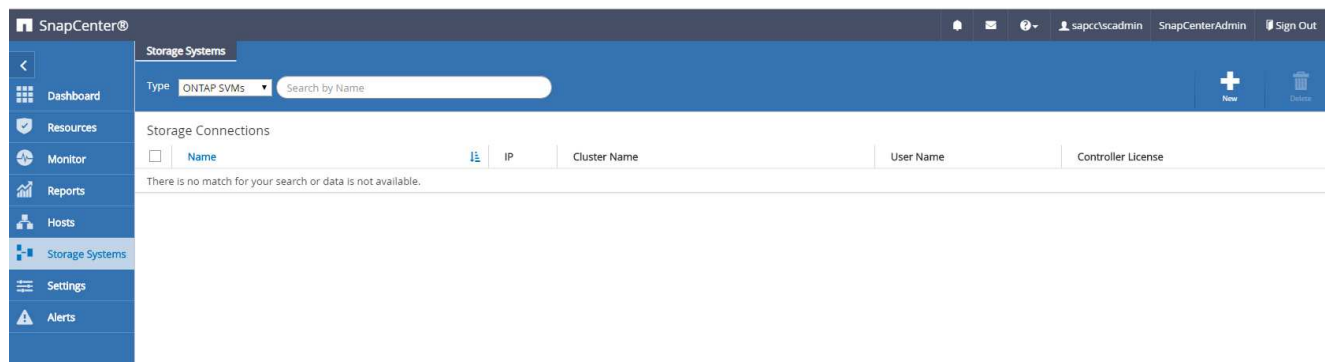
1. Accedere alla GUI del server SnapCenter.



2. Selezionare Storage Systems (sistemi storage).



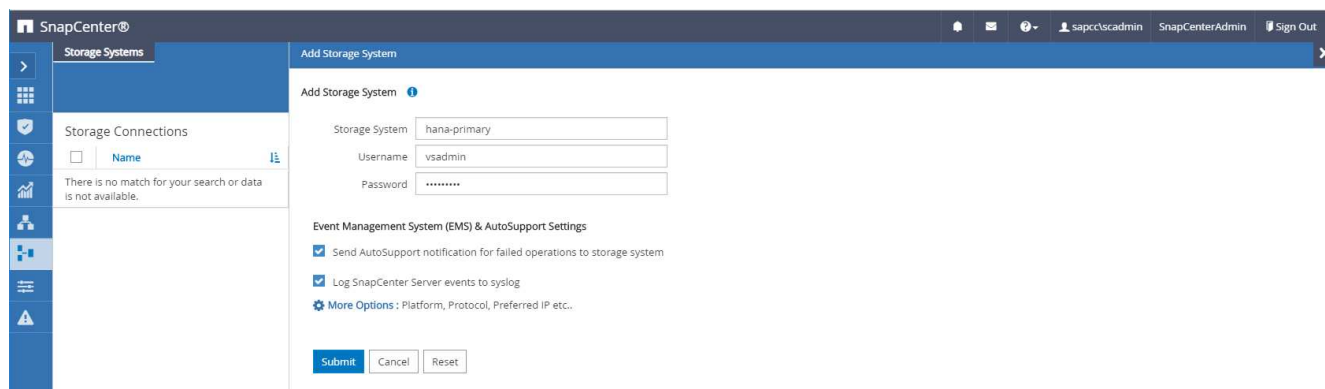
Nella schermata, è possibile selezionare il tipo di sistema storage, che può essere SVM ONTAP o cluster ONTAP. Se si configurano i sistemi storage a livello di SVM, è necessario configurare una LIF di gestione per ogni SVM. In alternativa, è possibile utilizzare un accesso di gestione SnapCenter a livello di cluster. La gestione SVM viene utilizzata nell'esempio seguente.



3. Fare clic su New (nuovo) per aggiungere un sistema storage e fornire il nome host e le credenziali richiesti.



L'utente SVM non deve essere l'utente vsadmin, come mostrato nella schermata. In genere, un utente viene configurato sulla SVM e assegnato i permessi necessari per eseguire le operazioni di backup e ripristino. I dettagli sui privilegi richiesti sono disponibili nella ["Guida all'installazione di SnapCenter"](#) Nella sezione intitolata "privilegi minimi ONTAP richiesti".

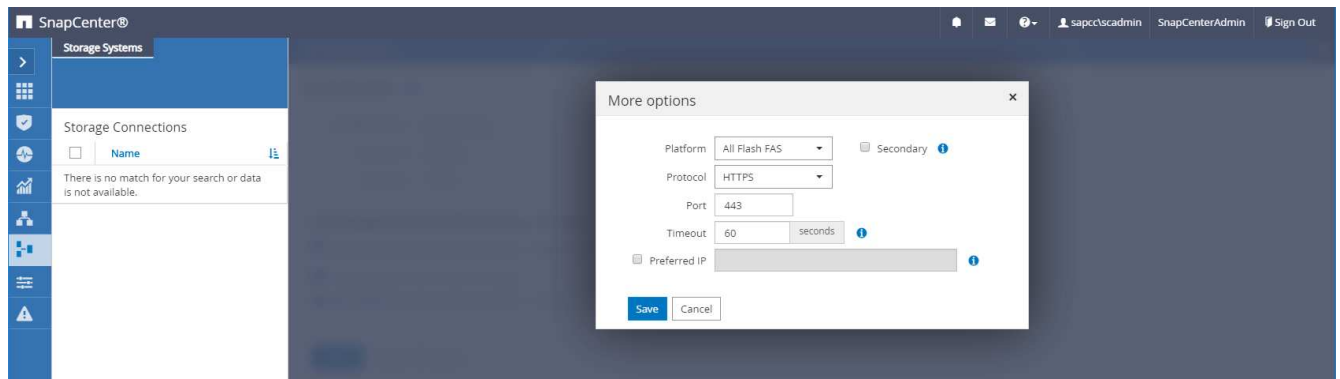


4. Fare clic su More Options (altre opzioni) per configurare la piattaforma di storage.

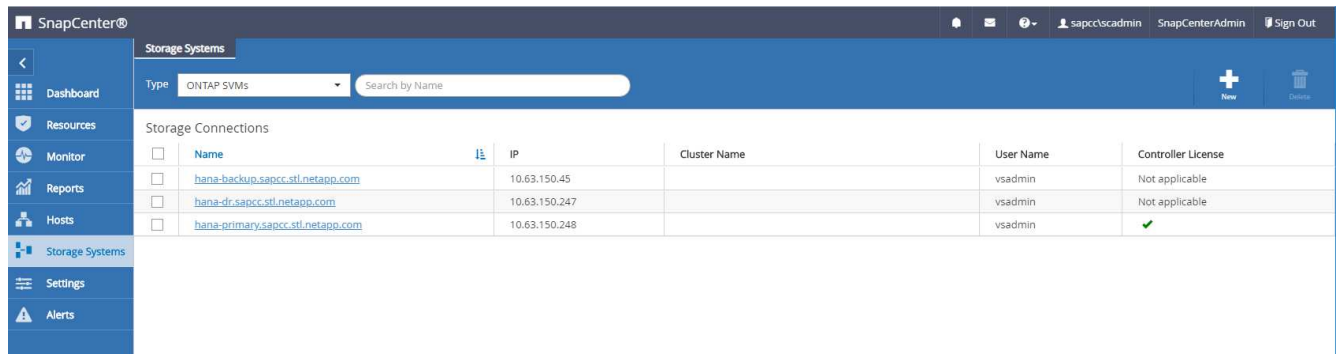
La piattaforma di storage può essere FAS, AFF, ONTAP Select o Cloud Volumes ONTAP.



Per un sistema utilizzato come destinazione SnapVault o SnapMirror, selezionare l'icona secondario.

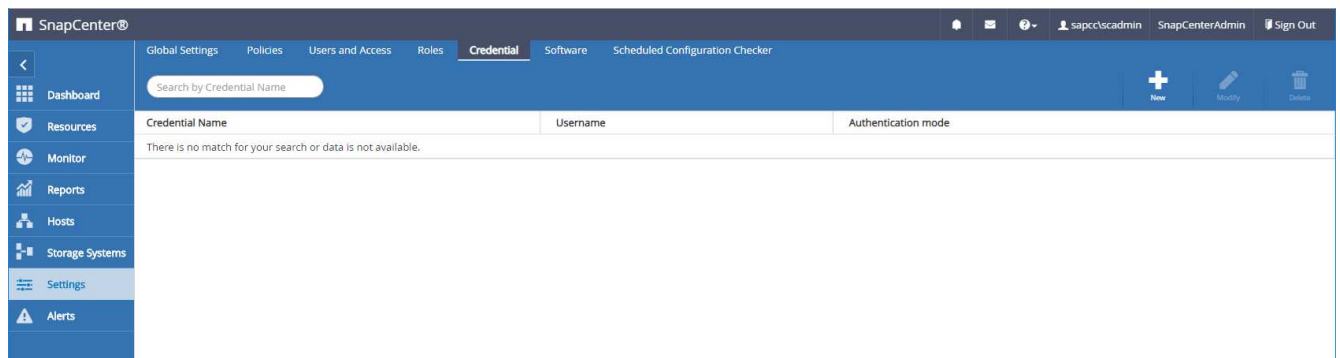


5. Aggiungere altri sistemi storage secondo necessità. Nel nostro esempio, sono stati aggiunti uno storage aggiuntivo per il backup fuori sede e uno per il disaster recovery.



Configurazione delle credenziali

1. Accedere a Impostazioni, selezionare credenziali e fare clic su nuovo.



2. Fornire le credenziali per l'utente utilizzato per le installazioni plug-in sui sistemi Linux.

Credential

×

Provide information for the Credential you want to add

Credential Name

InstallPluginOnLinux

Username

root

i

Password

.....

Authentication

Linux

▼

☐ Use sudo privileges

i

Cancel

OK

3. Fornire le credenziali per l'utente che vengono utilizzate per le installazioni dei plug-in sui sistemi Windows.

Credential

×

Provide information for the Credential you want to add

Credential Name

InstallPluginOnWindows

Username

sapcc\scadmin

Password

.....

Authentication

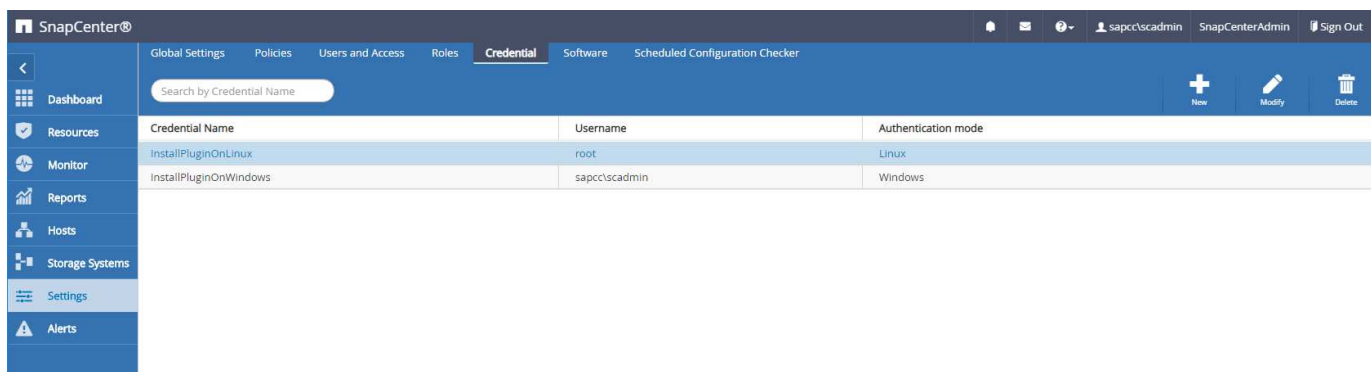
Windows

▼

Cancel

OK

La figura seguente mostra le credenziali configurate.



Credential Name	Username	Authentication mode
InstallPluginOnLinux	root	Linux
InstallPluginOnWindows	sapcc/scadmin	Windows

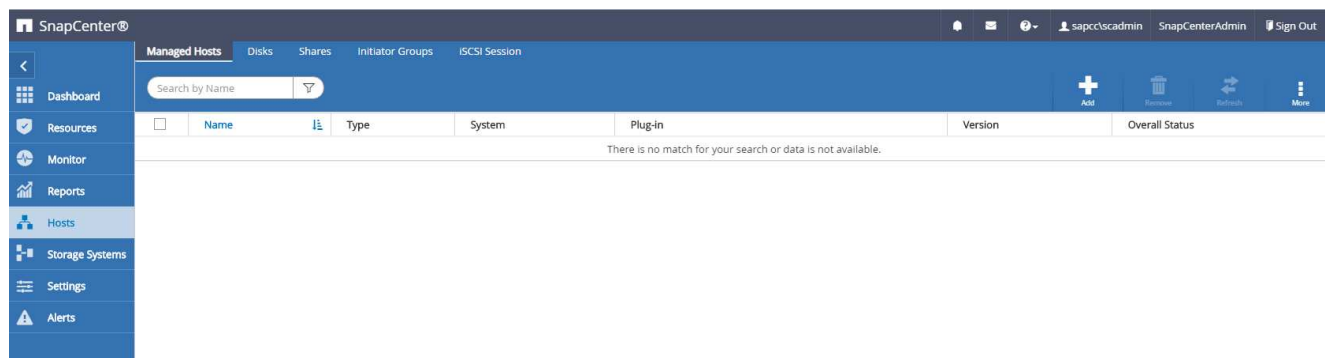
Installazione del plug-in SAP HANA su un host plug-in centrale

Nella configurazione di laboratorio, il server SnapCenter viene utilizzato anche come host plug-in HANA centrale. L'host Windows su cui viene eseguito il server SnapCenter viene aggiunto come host e il plug-in SAP HANA viene installato sull'host Windows.

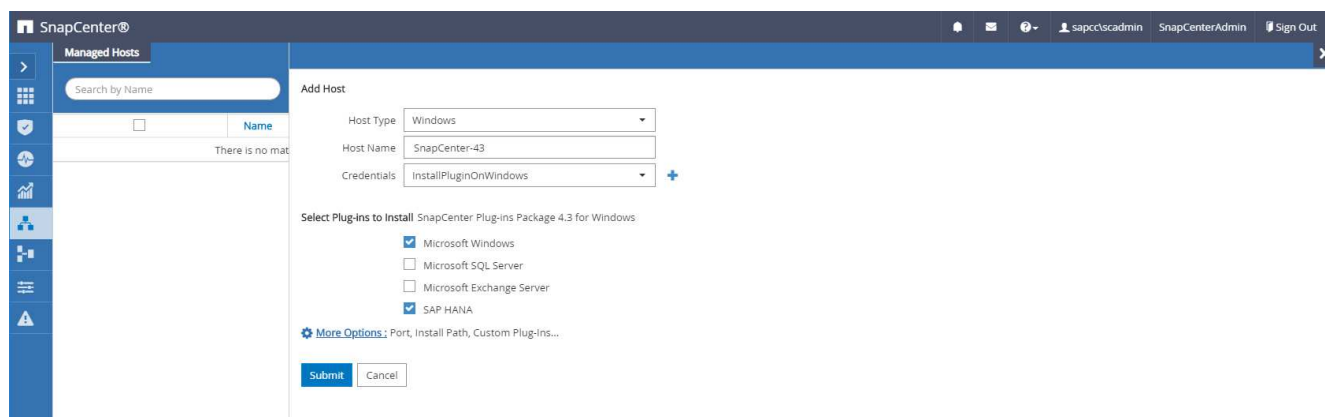


Il plug-in SAP HANA richiede Java a 64 bit versione 1.8. Java deve essere installato sull'host prima di implementare il plug-in SAP HANA.

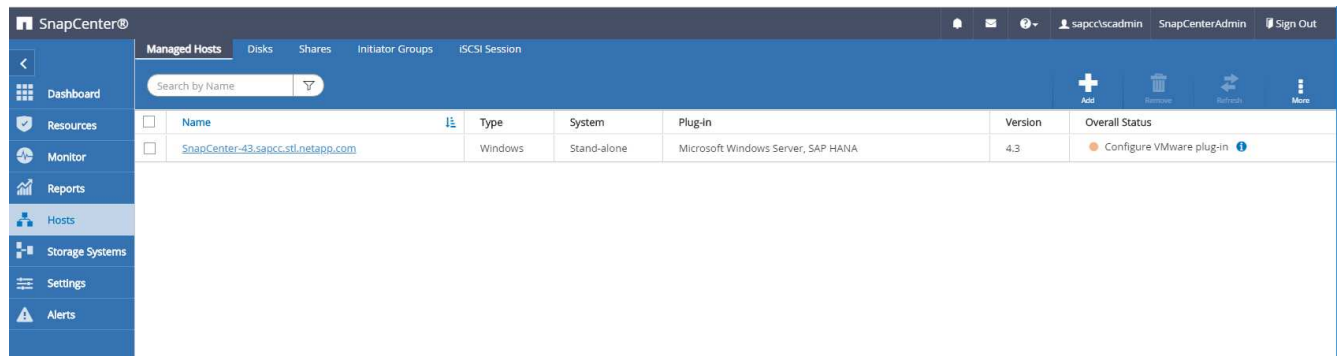
1. Accedere a hosts e fare clic su Add (Aggiungi).



2. Fornire le informazioni sull'host richieste. Fare clic su Invia.



La seguente figura mostra tutti gli host configurati dopo l'implementazione del plug-in HANA.



Installazione e configurazione del software client SAP HANA hdbsql

Il software client SAP HANA hdbsql deve essere installato sullo stesso host su cui è installato il plug-in SAP HANA. Il software può essere scaricato da ["Portale di supporto SAP"](#).

L'utente del sistema operativo HDBSQL configurato durante la configurazione delle risorse deve essere in grado di eseguire l'eseguibile hdbsql. Il percorso dell'eseguibile hdbsql deve essere configurato in `hana.properties` file.

- Finestre:

```
C:\More C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in
Creator\etc\hana.properties
HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql.exe
```

- Linux:

```
cat /opt/NetApp/snapcenter/scc/etc/hana.properties
HANA_HDBSQL_CMD=/usr/sap/hdbclient/hdbsql
```

Configurazione dei criteri

Come discusso nella sezione ["Strategia di protezione dei dati"](#), Le policy sono in genere configurate indipendentemente dalla risorsa e possono essere utilizzate da più database SAP HANA.

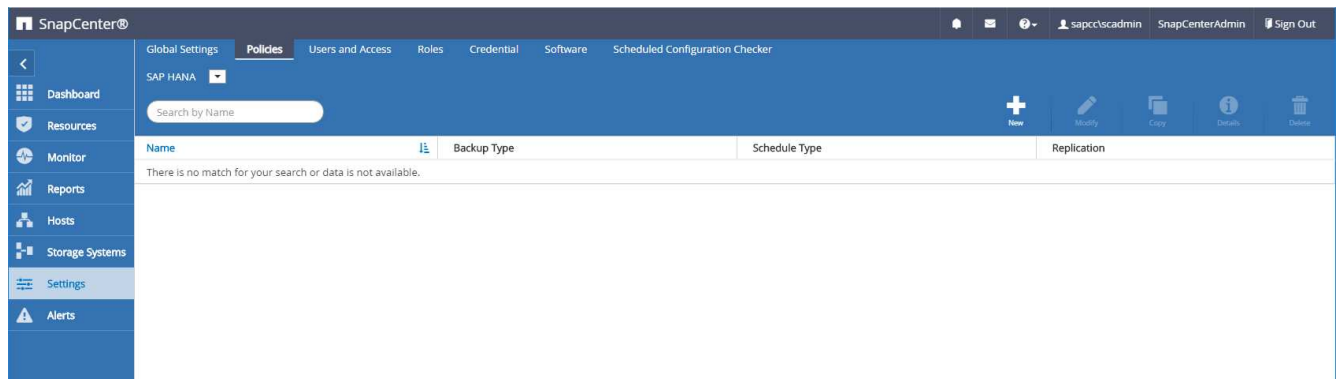
Una configurazione minima tipica è costituita dai seguenti criteri:

- Policy per backup orari senza replica: `LocalSnap`
- Policy per backup giornalieri con replica SnapVault: `LocalSnapAndSnapVault`
- Policy per il controllo settimanale dell'integrità dei blocchi utilizzando un backup basato su file: `BlockIntegrityCheck`

Le sezioni seguenti descrivono la configurazione di questi tre criteri.

Policy per backup Snapshot orari

1. Accedere a Impostazioni > Criteri e fare clic su nuovo.



2. Immettere il nome e la descrizione della policy. Fare clic su Avanti.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Provide a policy name

Policy name

LocalSnap

Description

Snapshot backup at primary storage

3. Selezionare il tipo di backup basato su Snapshot e selezionare orario per la frequenza di pianificazione.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select backup settings

Backup Type

☒ Snapshot Based
 ☐ File-Based

Schedule Frequency

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

☐ None
 ☒ Hourly
 ☐ Daily
 ☐ Weekly
 ☐ Monthly

4. Configurare le impostazioni di conservazione per i backup on-demand.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Retention settings

On demand backup retention settings

Backup retention settings

Total Snapshot copies to keep

2

Keep Snapshot copies for

14

days

Hourly retention settings

5. Configurare le impostazioni di conservazione per i backup pianificati.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Retention settings

On demand backup retention settings

Hourly retention settings

Total Snapshot copies to keep

12

Keep Snapshot copies for

14

days

6. Configurare le opzioni di replica. In questo caso, non è selezionato alcun aggiornamento di SnapVault o SnapMirror.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select secondary replication options

☐ Update SnapMirror after creating a local Snapshot copy.
 ☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

One Time

Error retry count

3

7. Nella pagina Riepilogo, fare clic su fine.

New SAP HANA Backup Policy ×

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Summary

Policy name	LocalSnap
Description	Snapshot backup at primary storage
Backup Type	Snapshot Based Backup
Schedule Type	Hourly
On demand backup retention	Total backup copies to retain : 2
Hourly backup retention	Total backup copies to retain : 12
Replication	none

Policy per backup Snapshot giornalieri con replica SnapVault

1. Accedere a Impostazioni > Criteri e fare clic su nuovo.
2. Immettere il nome e la descrizione della policy. Fare clic su Avanti.

New SAP HANA Backup Policy ×

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Provide a policy name

Policy name	<input type="text" value="LocalSnapAndSnapVault"/>	i
Description	<input type="text" value="Local Snapshot backup replicated to backup storage"/>	

3. Impostare il tipo di backup su Snapshot Based (basato su snapshot) e la frequenza di pianificazione su Daily (giornaliero).

New SAP HANA Backup Policy ×

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select backup settings

Backup Type
☒ Snapshot Based
☐ File-Based
i

Schedule Frequency

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

☐ None
☐ Hourly
☒ Daily
☐ Weekly
☐ Monthly

4. Configurare le impostazioni di conservazione per i backup on-demand.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Retention settings

On demand backup retention settings

Backup retention settings ⓘ

☒ Total Snapshot copies to keep

3

☐ Keep Snapshot copies for

14

days

Daily retention settings

5. Configurare le impostazioni di conservazione per i backup pianificati.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Retention settings

On demand backup retention settings

Daily retention settings

☒ Total Snapshot copies to keep

3 ⓘ

☐ Keep Snapshot copies for

14

days

6. Selezionare Aggiorna SnapVault dopo aver creato una copia Snapshot locale.

L'etichetta del criterio secondario deve essere la stessa dell'etichetta SnapMirror nella configurazione di protezione dei dati sul layer di storage. Vedere la sezione ["Configurazione della protezione dei dati per lo storage di backup off-site".](#)

109

Modify SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Select secondary replication options ⓘ

☐ Update SnapMirror after creating a local Snapshot copy.

☒ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Daily ⓘ

Error retry count

3 ⓘ

Previous

Next

7. Nella pagina Riepilogo, fare clic su fine.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Summary

Policy name	LocalSnapAndSnapVault
Description	Local Snapshot backup replicated to backup storage
Backup Type	Snapshot Based Backup
Schedule Type	Daily
On demand backup retention	Total backup copies to retain : 3
Daily backup retention	Total backup copies to retain : 3
Replication	SnapVault enabled , Secondary policy label: Daily , Error retry count: 3

Previous

Finish

Policy per il controllo settimanale dell'integrità del blocco

1. Accedere a Impostazioni > Criteri e fare clic su nuovo.
2. Immettere il nome e la descrizione della policy. Fare clic su Avanti.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Replication

5 Summary

Provide a policy name

Policy name	BlockIntegrityCheck
Description	Block integrity check using file based backup

3. Impostare il tipo di backup su file-based (basato su file) e la frequenza di pianificazione su Weekly (settimanale).

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary

Select backup settings

Backup Type

☐ Snapshot Based
☒ File-Based

Schedule Frequency

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

☐ None
☐ Hourly
☐ Daily
☒ Weekly
☐ Monthly

4. Configurare le impostazioni di conservazione per i backup on-demand.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary

Retention settings

On demand backup retention settings

Backup retention settings

☒ Total backup copies to keep
☐ Keep backup copies for

1

14 days

Weekly retention settings

5. Configurare le impostazioni di conservazione per i backup pianificati.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary

Retention settings

On demand backup retention settings

Backup retention settings

☒ Total backup copies to keep
☐ Keep backup copies for

1

14 days

Weekly retention settings

6. Nella pagina Riepilogo, fare clic su fine.

New SAP HANA Backup Policy

1 Name

2 Settings

3 Retention

4 Summary

Summary

Policy name	BlockIntegrityCheck
Description	Block integrity check using file based backup
Backup Type	File-Based Backup
Schedule Type	Weekly
On demand backup retention	Total backup copies to retain : 1
Weekly backup retention	Total backup copies to retain : 1

Previous

Finish

La figura seguente mostra un riepilogo dei criteri configurati.

SnapCenter®				
<div> <div> <div>Global Settings</div> <div>Policies</div> <div>Users and Access</div> <div>Roles</div> <div>Credential</div> <div>Software</div> <div>Scheduled Configuration Checker</div> </div> <div> <div>SAP HANA</div> <div>Search by Name</div> <div> <div>+</div> <div>✎</div> <div>📄</div> <div>ℹ</div> <div>🗑</div> </div> </div> </div>				
Name	Backup Type	Schedule Type	Replication	
BlockIntegrityCheck	File Based Backup	Weekly		
LocalSnap	Data Backup	Hourly		
LocalSnapAndSnapVault	Data Backup	Daily	SnapVault	

Configurazione specifica delle risorse SnapCenter per i backup dei database SAP HANA

In questa sezione vengono descritte le fasi di configurazione per due configurazioni di esempio.

- **SS2.**

- Sistema single-tenant SAP HANA MDC a host singolo che utilizza NFS per l'accesso allo storage
- La risorsa viene configurata manualmente in SnapCenter.
- La risorsa è configurata per creare backup Snapshot locali ed eseguire controlli di integrità dei blocchi per il database SAP HANA utilizzando un backup settimanale basato su file.

- **SS1.**

- Sistema single-tenant SAP HANA MDC a host singolo che utilizza NFS per l'accesso allo storage
- La risorsa viene rilevata automaticamente con SnapCenter.
- La risorsa è configurata per creare backup Snapshot locali, replicare su uno storage di backup off-site utilizzando SnapVault ed eseguire controlli di integrità dei blocchi per il database SAP HANA utilizzando un backup settimanale basato su file.

Le differenze per un sistema collegato A SAN, a singolo container o a più host si riflettono nelle corrispondenti fasi di configurazione o flusso di lavoro.

Configurazione di SAP HANA backup user e hdbuserstore

NetApp consiglia di configurare un utente di database dedicato nel database HANA per eseguire le operazioni di backup con SnapCenter. Nella seconda fase, per questo utente di backup viene configurata una chiave di archivio utente SAP HANA, che viene utilizzata nella configurazione del plug-in SAP HANA di SnapCenter.

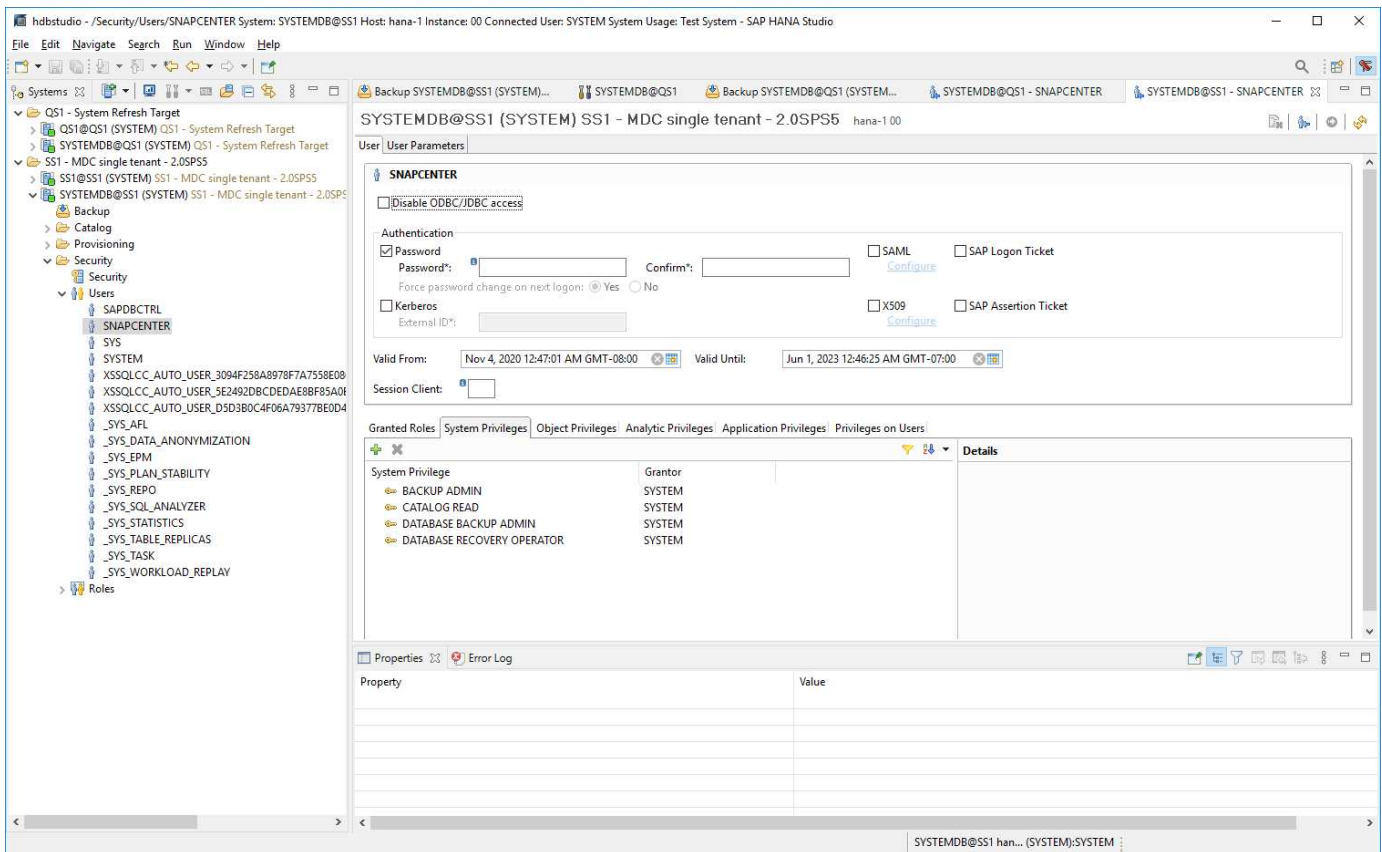
La figura seguente mostra SAP HANA Studio attraverso il quale è possibile creare l'utente di backup.



I privilegi richiesti sono stati modificati con la release HANA 2.0 SPS5: Backup admin, lettura catalogo, database backup admin e database recovery operator. Per le versioni precedenti, sono sufficienti l'amministratore del backup e la lettura del catalogo.



Per un sistema SAP HANA MDC, l'utente deve essere creato nel database di sistema perché tutti i comandi di backup per il sistema e i database tenant vengono eseguiti utilizzando il database di sistema.



Nell'host del plug-in HANA, su cui sono installati il plug-in SAP HANA e il client SAP hdbsql, è necessario configurare una chiave userstore.

Configurazione dell'archivio utenti sul server SnapCenter utilizzato come host plug-in HANA centrale

Se il plug-in SAP HANA e il client SAP hdbsql sono installati su Windows, l'utente del sistema locale esegue i comandi hdbsql e viene configurato per impostazione predefinita nella configurazione delle risorse. Poiché l'utente di sistema non è un utente di accesso, la configurazione dell'archivio utente deve essere eseguita con un altro utente e con `-u <User>` opzione.

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



Il software SAP HANA hdbclient deve essere prima installato sull'host Windows.

La configurazione dell'utente viene memorizzata su un host Linux separato utilizzato come host plug-in HANA centrale

Se il plug-in SAP HANA e il client SAP hdbsql sono installati su un host Linux separato, viene utilizzato il seguente comando per la configurazione dell'archivio utente con l'utente definito nella configurazione delle risorse:

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



Il software SAP HANA hdbclient deve essere prima installato sull'host Linux.

Configurazione dell'archivio utenti sull'host del database HANA

Se il plug-in SAP HANA viene implementato sull'host del database HANA, viene utilizzato il seguente comando per la configurazione dell'archivio utente con <sid>adm utente:

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



SnapCenter utilizza <sid>adm Per comunicare con il database HANA. Pertanto, la chiave di memorizzazione utente deve essere configurata utilizzando l'utente <'sid>adm` sull'host del database.



In genere, il software client SAP HANA hdbsql viene installato insieme all'installazione del server di database. In caso contrario, installare prima hdbclient.

Configurazione dell'archivio utenti in base all'architettura del sistema HANA

In una configurazione single-tenant SAP HANA MDC, porta 3<instanceNo>13 È la porta standard per l'accesso SQL al database di sistema e deve essere utilizzata nella configurazione hdbuserstore.

Per una configurazione di container singolo SAP HANA, porta 3<instanceNo>15 È la porta standard per l'accesso SQL all'index server e deve essere utilizzata nella configurazione hdbuserstore.

Per una configurazione di più host SAP HANA, è necessario configurare le chiavi di memorizzazione utente per tutti gli host. SnapCenter tenta di connettersi al database utilizzando ciascuna delle chiavi fornite e può quindi funzionare in modo indipendente dal failover di un servizio SAP HANA su un host diverso.

Esempi di configurazione dell'archivio utenti

Nella configurazione di laboratorio, viene utilizzata un'implementazione mista del plug-in SAP HANA. Il plug-in HANA viene installato sul server SnapCenter per alcuni sistemi HANA e distribuito sui singoli server di database HANA per altri sistemi.

Sistema SAP HANA SS1, tenant singolo MDC, istanza 00

Il plug-in HANA è stato implementato sull'host del database. Pertanto, la chiave deve essere configurata sull'host del database con l'utente ss1adm.

```

hana-1:/ # su - ssladm
ssladm@hana-1:/usr/sap/SS1/HDB00>
ssladm@hana-1:/usr/sap/SS1/HDB00>
ssladm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore set SS1KEY hana-1:30013
SnapCenter password
ssladm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore list
DATA FILE          : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE           : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.KEY
KEY SS1KEY
  ENV : hana-1:30013
  USER: SnapCenter
KEY SS1SAPDBCTRLSS1
  ENV : hana-1:30015
  USER: SAPDBCTRL
ssladm@hana-1:/usr/sap/SS1/HDB00>

```

Sistema SAP HANA MS1, tenant singolo MDC multi-host, istanza 00

Per i sistemi host HANA multipli, è necessario un host plug-in centrale, nella nostra configurazione abbiamo utilizzato il server SnapCenter. Pertanto, la configurazione dell'archivio utente deve essere eseguita sul server SnapCenter.

```

hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER
password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE          : C:\ProgramData\.hdb\SNAPCENTER-43\S-1-5-18\SSFS_HDB.DAT
KEY FILE           : C:\ProgramData\.hdb\SNAPCENTER-43\S-1-5-18\SSFS_HDB.KEY
KEY MS1KEYHOST1
  ENV : hana-4:30013
  USER: SNAPCENTER
KEY MS1KEYHOST2
  ENV : hana-5:30013
  USER: SNAPCENTER
KEY MS1KEYHOST3
  ENV : hana-6:30013
  USER: SNAPCENTER
KEY SS2KEY
  ENV : hana-3:30013
  USER: SNAPCENTER
C:\Program Files\sap\hdbclient>

```

Configurazione della protezione dei dati per lo storage di backup off-site

La configurazione della relazione di protezione dei dati e il trasferimento iniziale dei dati devono essere eseguiti prima che gli aggiornamenti di replica possano essere gestiti da SnapCenter.

La figura seguente mostra la relazione di protezione configurata per il sistema SAP HANA SS1. Con il nostro esempio, il volume di origine `SS1_data_mnt00001` Alla SVM `hana-primary` Viene replicato su SVM `hana-backup` e il volume di destinazione `SS1_data_mnt00001_dest`.



La pianificazione della relazione deve essere impostata su Nessuno, perché SnapCenter attiva l'aggiornamento di SnapVault.

The screenshot shows the OnCommand System Manager interface. The left sidebar contains navigation options: Dashboard, Applications & Tiers, Storage, Network, Protection, Volume Relationships, SVM DR Relationships, Protection Policies, Schedules, Snapshot Policies, Events & Jobs, and Configuration. The main panel is titled 'Volume Relationships' and displays a table of relationships. A row is highlighted with a blue border, showing the relationship between 'hana-primary' and 'hana-backup' for source volume 'SS1_data_mnt00001' and destination volume 'SS1_data_mnt00001_dest'. Below the table, the 'Details' tab is active, showing configuration parameters for the selected relationship.

Source Storage Vi...	Source Volume	Destination Volume	Destination Stora...	Is Healthy	Object ...	Rela...	Transf...	Relationship Type	Lag Time	Policy Name	Policy Type
hana-primary	SS1_data_mnt00001	SS1_data_mnt00001_dest	hana-backup	Yes	Volume	Snapmi...	Idle	Asynchronous V...	21 hrs(s)...	SnapCenterVault	Asynchronous Vault

Source Location:	Is Healthy:	Transfer Status:
hana-primary:SS1_data_...	Yes	Idle
Destination Location:	Relationship State:	Current Transfer Type:
hana-backup:SS1_data_m...	Snapmirrored	None
Source Cluster:	Network Compression Ratio:	Current Transfer Error:
a700-marco	Not Applicable	None
Destination Cluster:	Transfer Schedule:	Current Transfer Progress:
a700-marco	None	None
Data Transfer Rate:	Latest Snapshot Timestamp:	Last Transfer Error:
Unlimited	11/26/2019 11:03:53	None
Lag Time:	Latest Snapshot Copy:	Last Transfer Type:
21 hr(s) 23 min(s)	SnapCenter_Local/SnapAndSnapVault_Daily_11-26-2019_08.17.01.8979	Update

La seguente figura mostra il criterio di protezione. Il criterio di protezione utilizzato per la relazione di protezione definisce l'etichetta SnapMirror e la conservazione dei backup nello storage secondario. Nel nostro esempio, l'etichetta utilizzata è 'Daily' e la conservazione è impostata su 5.



L'etichetta SnapMirror nel criterio creato deve corrispondere all'etichetta definita nella configurazione del criterio SnapCenter. Per ulteriori informazioni, fare riferimento a "[Policy per backup Snapshot giornalieri con replica SnapVault](#)."



La conservazione dei backup nello storage di backup off-site è definita nella policy e controllata da ONTAP.

OnCommand System Manager

Type: All Search all Objects

Volume Relationships

+ Create Edit Delete Operations Refresh

Source Storage Vi...	Source Volume	Destination Volume	Destination Stora...	Is Healthy	Object ...	Rela...	Transf...	Relationship Type	Lag Time	Policy Name	Policy Type
hana-primary	SS1_data_mnt00001	SS1_data_mnt00001_dest	hana-backup	Yes	Volume	Snapmi...	Idle	Asynchronous V...	21 hr(s)...	SnapCenterVault	Asynchronous Vault

Policy Name: SnapCenterVault

Comments:

Label	Number of Copies	Matching Snapshot copy Schedules in Source Volume
Daily	5	Source does not have any schedules with this label

Details Policy Details Snapshot Copies

Configurazione manuale delle risorse HANA

Questa sezione descrive la configurazione manuale delle risorse SAP HANA SS2 e MS1.

- SS2 è un sistema single-tenant MDC a host singolo
- MS1 è un sistema single-tenant MDC multihost.
 - a. Dalla scheda Resources (risorse), selezionare SAP HANA e fare clic su Add SAP HANA Database (Aggiungi database SAP HANA).
 - b. Inserire le informazioni per la configurazione del database SAP HANA e fare clic su Next (Avanti).

Selezionare il tipo di risorsa nel nostro esempio, Container di database multi-tenant.



Per un sistema container singolo HANA, è necessario selezionare il tipo di risorsa container singolo. Tutte le altre fasi di configurazione sono identiche.

Per il nostro sistema SAP HANA, il SID è SS2.

L'host del plug-in HANA nel nostro esempio è il server SnapCenter.

La chiave hdbuserstore deve corrispondere alla chiave configurata per il database HANA SS2. Nel nostro esempio è SS2KEY.

Add SAP HANA Database

1 Name
2 Storage Footprint
3 Summary

Provide Resource Details

Resource Type
Multitenant Database Container

HANA System Name
SS2 - HANA 20 SPS4 MDC Single Tenant

SID
SS2

Plug-in Host
SnapCenter-43.sapcc.stl.netapp.com

HDB Secure User Store Keys
SS2KEY

HDBSQL OS User
SYSTEM



Per un sistema SAP HANA con host multipli, è necessario includere le chiavi hdbuserstore per tutti gli host, come mostrato nella figura seguente. SnapCenter tenterà di connettersi con la prima chiave dell'elenco e continuerà con l'altro caso, nel caso in cui la prima chiave non funzioni. Questo è necessario per supportare il failover HANA in un sistema con più host con host di lavoro e di standby.

Modify SAP HANA Database

1 Name
2 Storage Footprint
3 Summary

Provide Resource Details

Resource Type
Multitenant Database Container

HANA System Name
MS1 - Multiple Hosts MDC Single Tenant

SID
MS1

Plug-in Host
SnapCenter-43.sapcc.stl.netapp.com

HDB Secure User Store Keys
MS1KEYHOST1,MS1KEYHOST2,MS1KEYHOST3

HDBSQL OS User
SYSTEM

c. Selezionare i dati richiesti per il sistema di storage (SVM) e il nome del volume.

Add SAP HANA Database

1 Name
2 Storage Footprint
3 Summary

Provide Storage Footprint Details

Add Storage Footprint

Storage System
hana-primary.sapcc.stl.netapp.com

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

Volume name
SS2_data_mnt00001

LUNs or Qtrees
Default is 'None' or type to find

Save



Per una configurazione SAN Fibre Channel, è necessario selezionare anche il LUN.



Per un sistema host multiplo SAP HANA, è necessario selezionare tutti i volumi di dati del sistema SAP HANA, come mostrato nella figura seguente.

Add SAP HANA Database

1 Name

2 **Storage Footprint**

3 Summary

Provide Storage Footprint Details

Add Storage Footprint

Storage System: hana-primary.sapcc.stl.netapp.com

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

Volume name	LUNs or Qtrees
MS1_data_mnt00001	Default is 'None' or type to find
MS1_data_mnt00002	Default is 'None' or type to find

Save

Viene visualizzata la schermata di riepilogo della configurazione delle risorse.

- Fare clic su Finish (fine) per aggiungere il database SAP HANA.

Add SAP HANA Database

1 Name

2 Storage Footprint

3 **Summary**

Summary

Resource Type	Multitenant Database Container
HANA System Name	SS2 - HANA 20 SP54 MDC Single Tenant
SID	SS2
Plug-in Host	SnapCenter-43.sapcc.stl.netapp.com
HDB Secure User Store Keys	SS2KEY
HDBSQL OS User	SYSTEM

Storage Footprint

Storage System	Volume	LUN/Qtree
hana-primary.sapcc.stl.netapp.com	SS2_data_mnt00001	

- Al termine della configurazione delle risorse, eseguire la configurazione della protezione delle risorse come descritto nella sezione "[Configurazione della protezione delle risorse.](#)"

Rilevamento automatico dei database HANA

Questa sezione descrive il rilevamento automatico della risorsa SAP HANA SS1 (sistema single-tenant MDC host con NFS). Tutti i passaggi descritti sono identici per un singolo container HANA, per i sistemi di tenant multipli HANA MDC e per un sistema HANA che utilizza SAN Fibre Channel.



Il plug-in SAP HANA richiede Java a 64 bit versione 1.8. Java deve essere installato sull'host prima di implementare il plug-in SAP HANA.

1. Dalla scheda host, fare clic su Add (Aggiungi).
2. Fornire informazioni sull'host e selezionare il plug-in SAP HANA da installare. Fare clic su Invia.

Managed Hosts

Search by Name

Add Host

Host Type: Linux

Host Name: hana-1

Credentials: InstallPluginOnLinux

Select Plug-ins to Install: SnapCenter Plug-ins Package 4.3 for Linux

☐ Oracle Database

☒ SAP HANA

[More Options](#): Port, Install Path, Custom Plug-Ins...

3. Confermare l'impronta digitale.

Confirm Fingerprint

Authenticity of the host cannot be determined

Host name	Fingerprint	Valid
hana-1.sapcc.stl.netapp.com	ssh-rsa 2048 6E:80:F0:B7:6E:8F:E4:9A:E5:2E:E8:6A:0C:0A:18:C7	

L'installazione del plug-in HANA e del plug-in Linux si avvia automaticamente. Al termine dell'installazione, la colonna di stato dell'host mostra in esecuzione. La schermata mostra inoltre che il plug-in Linux è installato insieme al plug-in HANA.

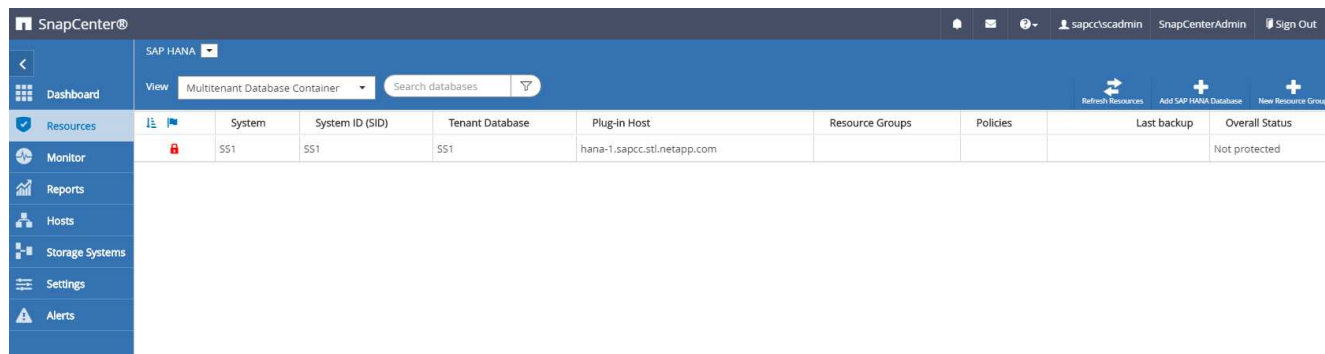
Name	Type	System	Plug-in	Version	Overall Status
hana-1.sapcc.stl.netapp.com	Linux	Stand-alone	UNIX, SAP HANA	4.3	Running
SnapCenter-43.sapcc.stl.netapp.com	Windows	Stand-alone	Microsoft Windows Server, SAP HANA	4.3	Running

Dopo l'installazione del plug-in, il processo di rilevamento automatico della risorsa HANA viene avviato automaticamente. Nella schermata Resources (risorse) viene creata una nuova risorsa, contrassegnata come bloccata con l'icona del lucchetto rosso.

4. Selezionare e fare clic sulla risorsa per continuare la configurazione.



È inoltre possibile attivare manualmente il processo di rilevamento automatico nella schermata risorse, facendo clic su **Aggiorna risorse**.



5. Fornire la chiave dell'archivio utenti per il database HANA.

Configure Database

Plug-in host: hana-1.sapcc.stl.netapp.com

HDBSQL OS User: ss1adm

HDB Secure User Store Keys:

Configuring Database... Cancel OK

Viene avviato il processo di rilevamento automatico di secondo livello in cui vengono rilevate le informazioni relative ai dati del tenant e all'impatto dello storage.

6. Fare clic su **Details** (Dettagli) per esaminare le informazioni di configurazione delle risorse HANA nella vista della topologia delle risorse.

Manage Copies

Local copies: 17 Backups, 0 Clones

Vault copies: 5 Backups, 0 Clones

Summary Card

- 24 Backups
- 22 Snapshot based backups
- 2 File-Based backups ✓
- 0 Clones

Primary Backup(s)

Backup Name	Count	End Date
SnapCenter_LocalSnap_Hourly_11-27-2019_02.30.01.1788	1	11/27/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_11-26-2019_22.30.01.0413	1	11/26/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_11-26-2019_18.30.01.0738	1	11/26/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_11-26-2019_14.30.01.0340	1	11/26/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_11-26-2019_10.30.01.0649	1	11/26/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_11-26-2019_08.17.01.8979	1	11/26/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_11-26-2019_06.30.01.0003	1	11/26/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_11-26-2019_02.30.00.9915	1	11/26/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_11-25-2019_22.30.01.0536	1	11/25/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_11-25-2019_18.30.01.0250	1	11/25/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_11-25-2019_14.30.01.0151	1	11/25/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_11-25-2019_10.30.00.9895	1	11/25/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_11-25-2019_08.17.01.8577	1	11/25/2019 8:17:55 AM
SnapCenter_LocalSnap_Hourly_11-25-2019_06.30.00.9717	1	11/25/2019 6:30:55 AM

Total 4

Activity: The 5 most recent jobs are displayed. 4 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, 0 Queued.

Resource - Details

Details for selected resource

Type: Multitenant Database Container

HANA System Name: SS1

SID: SS1

Tenant Database: SS1

Plug-in Host: hana-1.sapcc.stl.netapp.com

HDB Secure User Store Keys: SS1KEY

HDBSQL OS User: ssladm

plug-in name: SAP HANA

Last backup: 11/27/2019 2:30:55 AM (Completed)

Resource Groups: hana-1_sapcc_stl_netapp_com_hana_MDC_SS1

Policy: BlockIntegrityCheck, LocalSnap, LocalSnapAndSnapVault

Discovery Type: Auto

Storage Footprint

SVM	Volume	Junction Path	LUN/Qtire
hana-primary.sapcc.stl.netapp.com	SS1_data_mnt00001	/SS1_data_mnt00001	

Total 4

Activity: The 5 most recent jobs are displayed. 4 Completed, 0 Warnings, 0 Failed, 0 Canceled, 1 Running, 0 Queued.

Al termine della configurazione delle risorse, la configurazione di protezione delle risorse deve essere eseguita come descritto nella sezione seguente.

Configurazione della protezione delle risorse

Questa sezione descrive la configurazione della protezione delle risorse. La configurazione di protezione delle risorse è la stessa, indipendentemente dal fatto che la risorsa sia stata rilevata o configurata manualmente. È identico anche per tutte le architetture HANA, host singoli o multipli, container singolo o sistemi MDC.

1. Dalla scheda risorse, fare doppio clic sulla risorsa.
2. Configurare un formato nome personalizzato per la copia Snapshot.



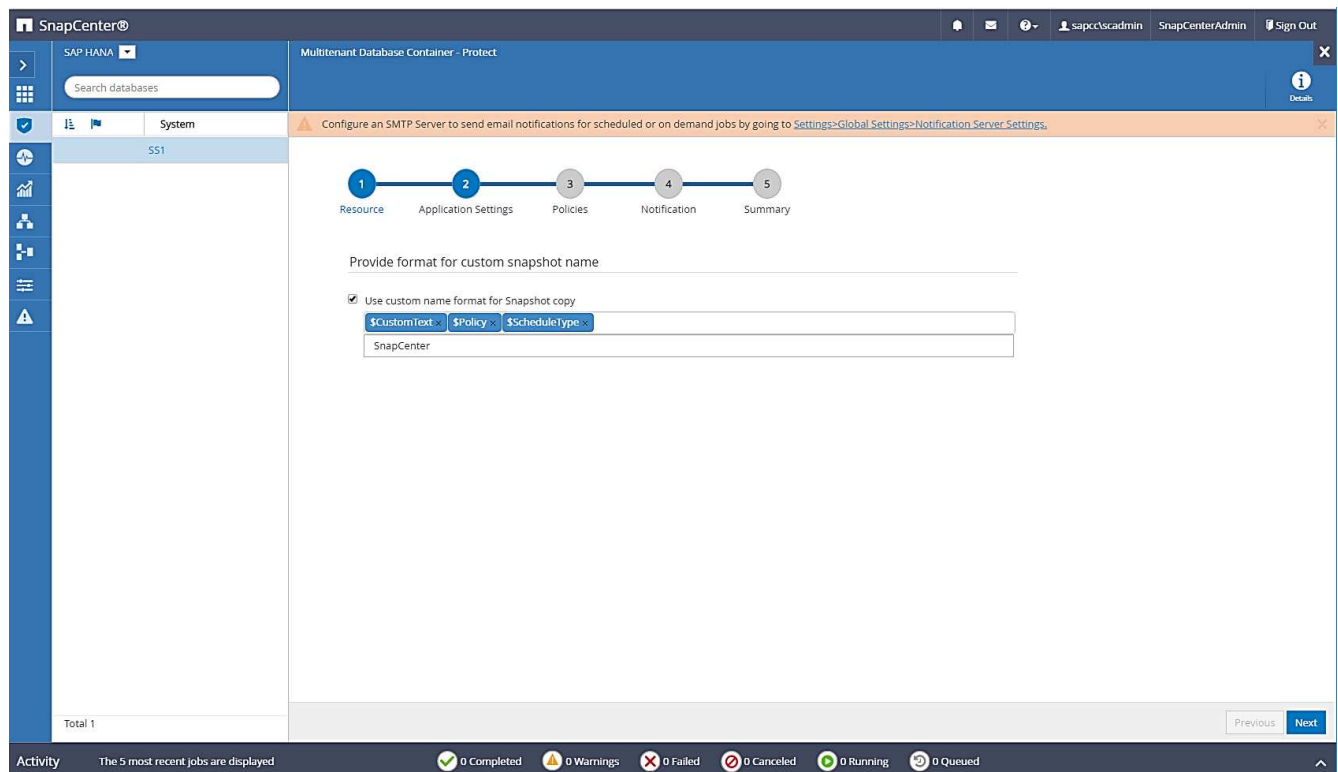
NetApp consiglia di utilizzare un nome di copia Snapshot personalizzato per identificare facilmente i backup creati con quale tipo di policy e pianificazione. Aggiungendo il tipo di pianificazione nel nome della copia Snapshot, è possibile distinguere tra backup pianificati e su richiesta. Il `schedule name` la stringa per i backup on-demand è vuota, mentre i backup pianificati includono la stringa `Hourly`, `Daily`, or `Weekly`.

Nella configurazione illustrata nella figura seguente, i nomi delle copie Snapshot e di backup hanno il seguente formato:

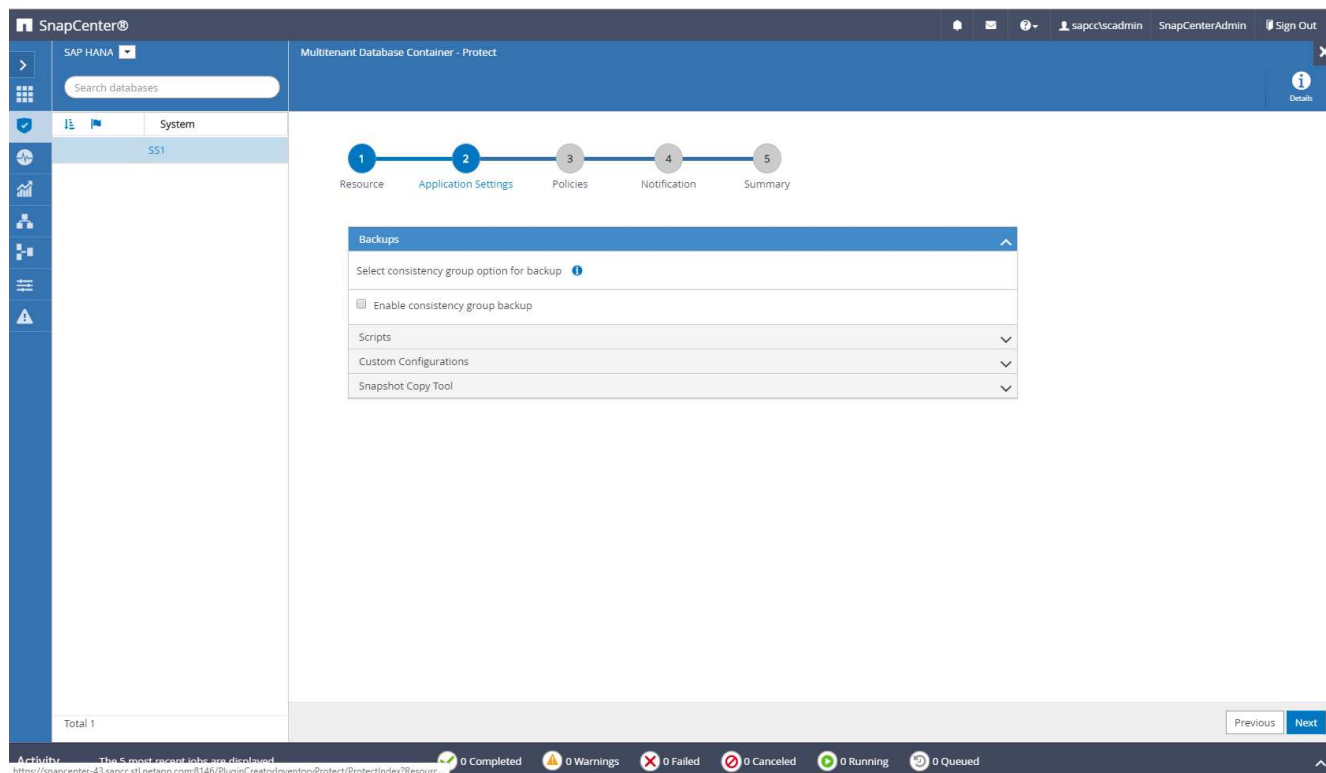
- Backup orario pianificato: `SnapCenter_LocalSnap_Hourly_<time_stamp>`
- Backup giornaliero pianificato: `SnapCenter_LocalSnapAndSnapVault_Daily_<time_stamp>`
- Backup orario on-demand: `SnapCenter_LocalSnap_<time_stamp>`
- Backup giornaliero on-demand: `SnapCenter_LocalSnapAndSnapVault_<time_stamp>`



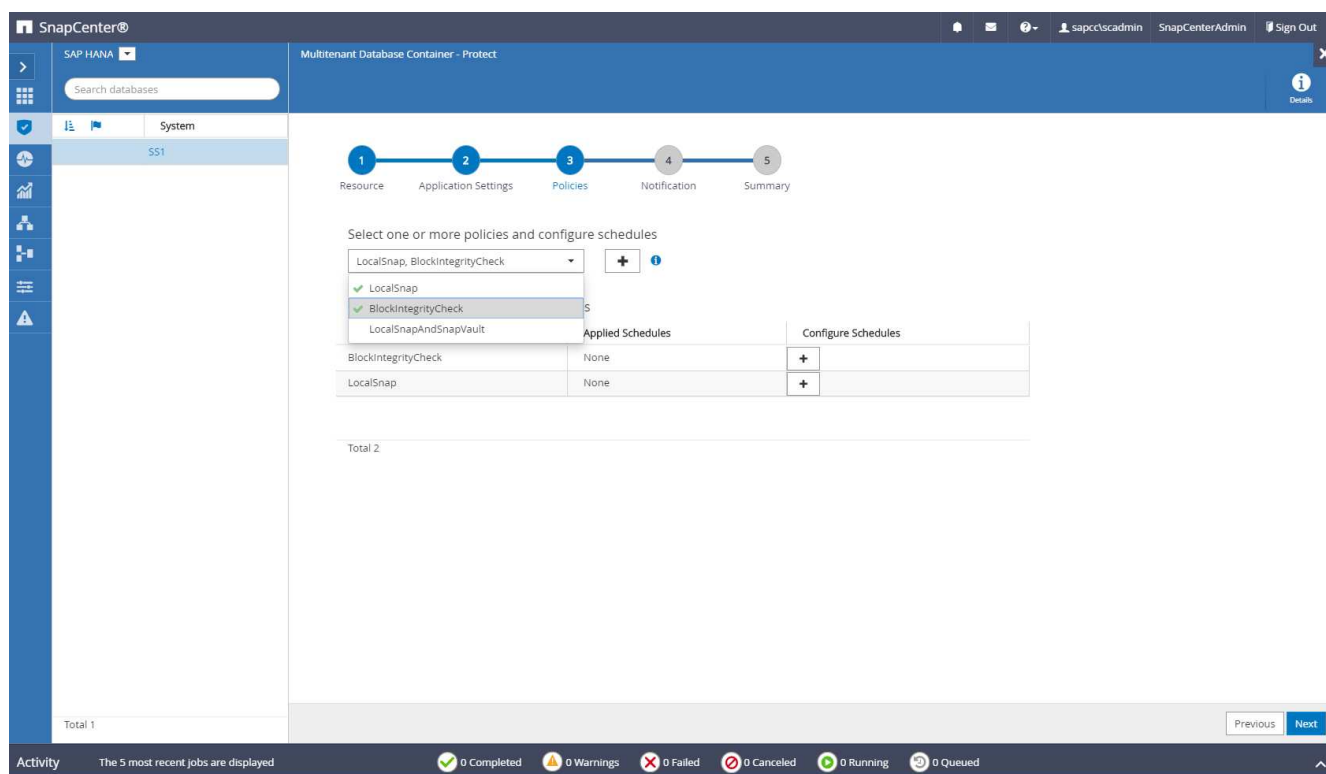
Anche se viene definita una conservazione per i backup on-demand nella configurazione dei criteri, la pulizia viene eseguita solo quando viene eseguito un altro backup on-demand. Di conseguenza, i backup on-demand devono in genere essere cancellati manualmente in SnapCenter per assicurarsi che questi backup vengano eliminati anche nel catalogo di backup SAP HANA e che la manutenzione del backup del log non sia basata su un vecchio backup on-demand.



3. Non è necessario impostare impostazioni specifiche nella pagina Impostazioni applicazione. Fare clic su Avanti.



4. Selezionare i criteri da aggiungere alla risorsa.



5. Definire la pianificazione per il criterio LocalSnap (in questo esempio, ogni quattro ore).

Add schedules for policy LocalSnap

Hourly

Start date

11/19/2019 6:30 AM

☐ Expires on

12/19/2019 5:59 AM

Repeat every

4

hours

0

mins

i

The schedules are triggered in the SnapCenter Server time zone.

Cancel

Ok

6. Definire la pianificazione per la policy LocalSnapAndSnapVault (in questo esempio, una volta al giorno).

Modify schedules for policy LocalSnapAndSnapVault

Daily

Start date

11/19/2019 8:17 AM

☐ Expires on

12/19/2019 8:17 AM

Repeat every

1

days

i

The schedules are triggered in the SnapCenter Server time zone.

Cancel

Ok

7. Definire la pianificazione per la policy di controllo dell'integrità del blocco (in questo esempio, una volta alla settimana).

Add schedules for policy BlockIntegrityCheck

Weekly

Start date

11/19/2019 5:57 AM

☐ Expires on

12/19/2019 5:57 AM

Days

Saturday

Monday

Tuesday

Wednesday

Thursday

Friday

✓ Saturday

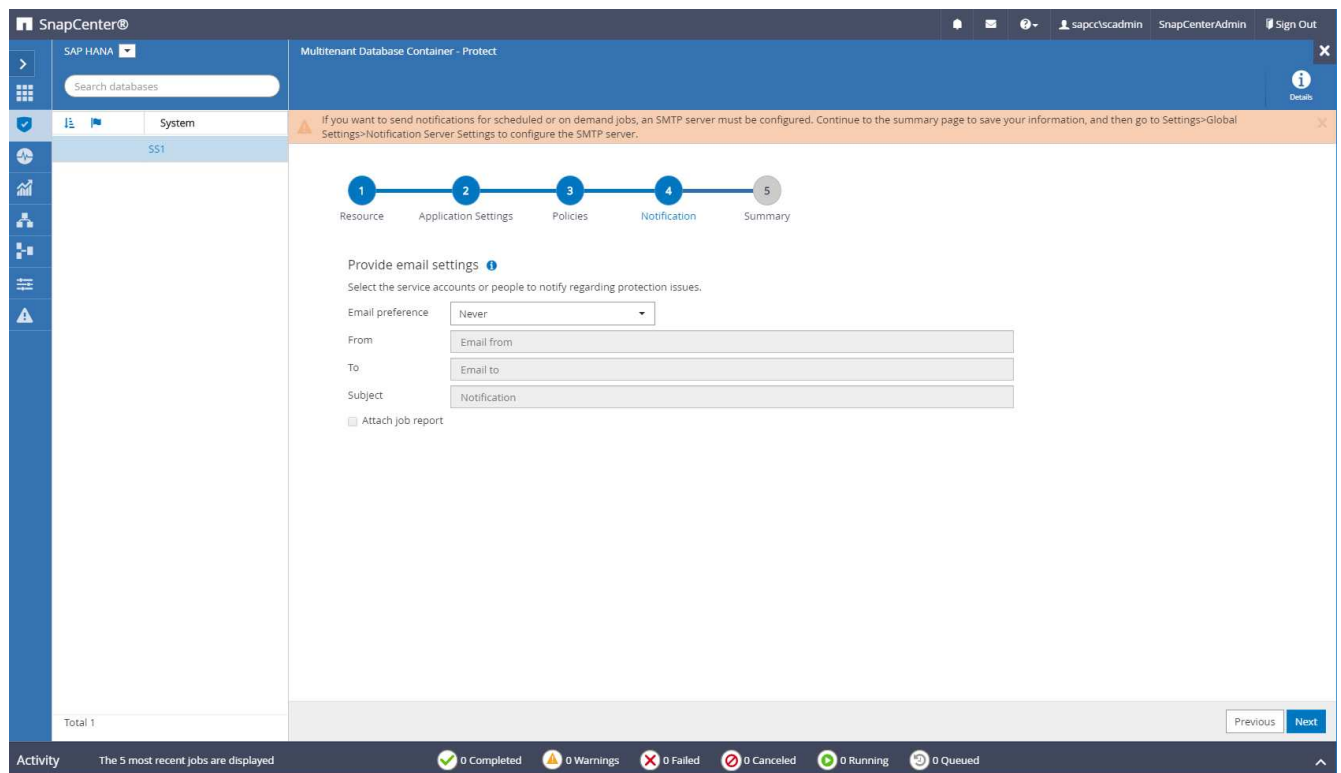
i

The schedules are triggered in the SnapCenter Server time zone.

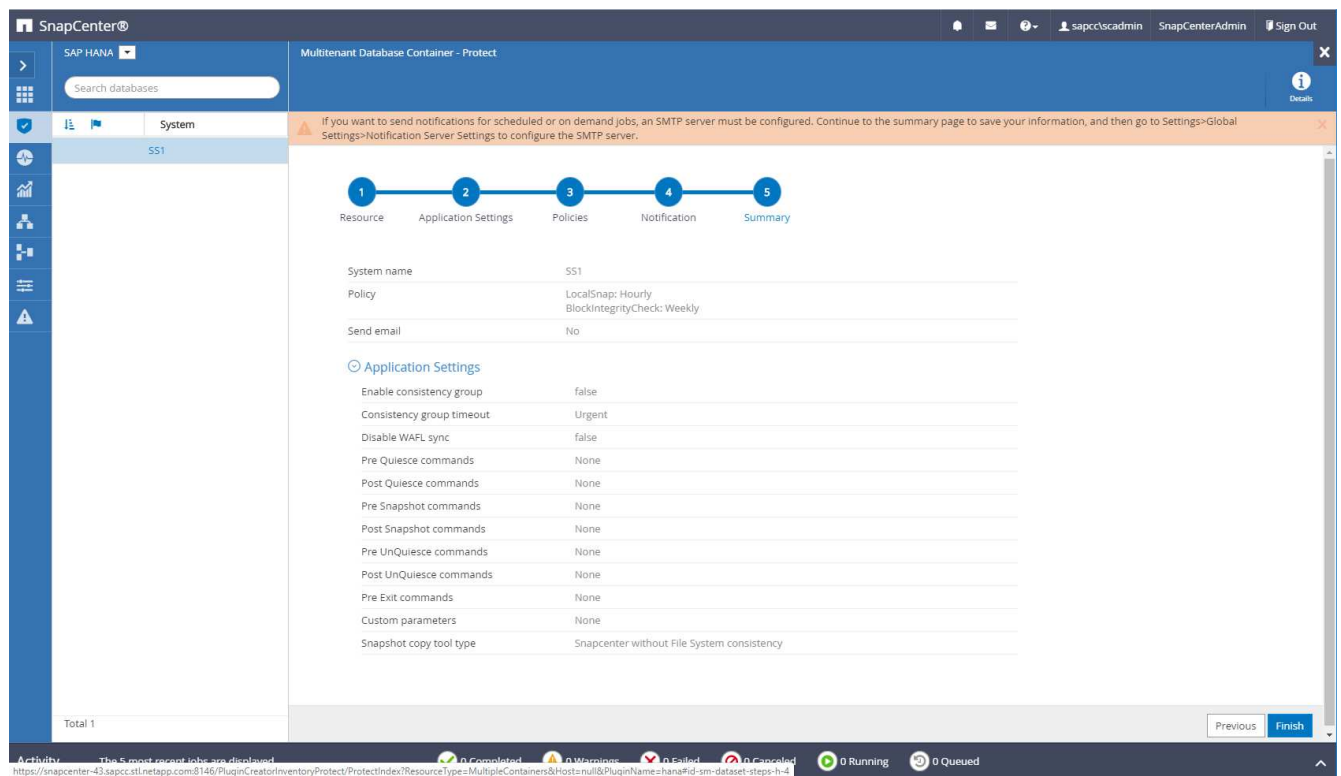
Cancel

Ok

8. Fornire informazioni sulla notifica via email.



9. Nella pagina Riepilogo, fare clic su fine.



10. È ora possibile creare backup on-demand nella pagina della topologia. I backup pianificati vengono eseguiti in base alle impostazioni di configurazione.

System	System ID (SID)	Tenant Database	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
SS1	SS1	SS1	hana-1.sapcc.sti.netapp.com		BlockIntegrityCheck LocalSnap LocalSnapAndSnapVault	11/19/2019 6:30:54 AM	Backup succeeded

Total 1

Activity: The 5 most recent jobs are displayed. 2 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, 0 Queued.

Ulteriori procedure di configurazione per ambienti SAN Fibre Channel

A seconda della versione di HANA e dell'implementazione del plug-in HANA, sono necessarie ulteriori procedure di configurazione per gli ambienti in cui i sistemi SAP HANA utilizzano Fibre Channel e il file system XFS.



Questi passaggi di configurazione aggiuntivi sono necessari solo per le risorse HANA, che sono configurate manualmente in SnapCenter. È inoltre necessario solo per le release HANA 1.0 e HANA 2.0 fino a SPS2.

Quando un punto di salvataggio di backup HANA viene attivato da SnapCenter in SAP HANA, SAP HANA scrive i file ID Snapshot per ogni tenant e servizio di database come ultima fase (ad esempio, `/hana/data/SID/mnt00001/hdb00001/snapshot_databackup_0_1`). Questi file fanno parte del volume di dati dello storage e fanno quindi parte della copia Snapshot dello storage. Questo file è obbligatorio quando si esegue un ripristino in una situazione in cui il backup viene ripristinato. A causa del caching dei metadati con il file system XFS sull'host Linux, il file non è immediatamente visibile a livello di storage. La configurazione XFS standard per il caching dei metadati è di 30 secondi.



Con HANA 2.0 SPS3, SAP ha modificato l'operazione di scrittura di questi file ID Snapshot in modo sincrono, in modo che il caching dei metadati non sia un problema.



Con SnapCenter 4.3, se il plug-in HANA viene implementato sull'host del database, il plug-in Linux esegue un'operazione di svuotamento del file system sull'host prima che venga attivata l'istantanea dello storage. In questo caso, il caching dei metadati non è un problema.

In SnapCenter, è necessario configurare un `postquiesce` Comando che attende fino a quando la cache dei metadati XFS non viene scaricata nel livello del disco.

La configurazione effettiva del caching dei metadati può essere verificata utilizzando il seguente comando:

```
stlrx300s8-2:/ # sysctl -A | grep xfssyncd_centisecs
fs.xfs.xfssyncd_centisecs = 3000
```

NetApp consiglia di utilizzare un tempo di attesa pari al doppio del valore di `fs.xfs.xfssyncd_centisecs` parametro. Poiché il valore predefinito è 30 secondi, impostare il comando di sospensione su 60 secondi.

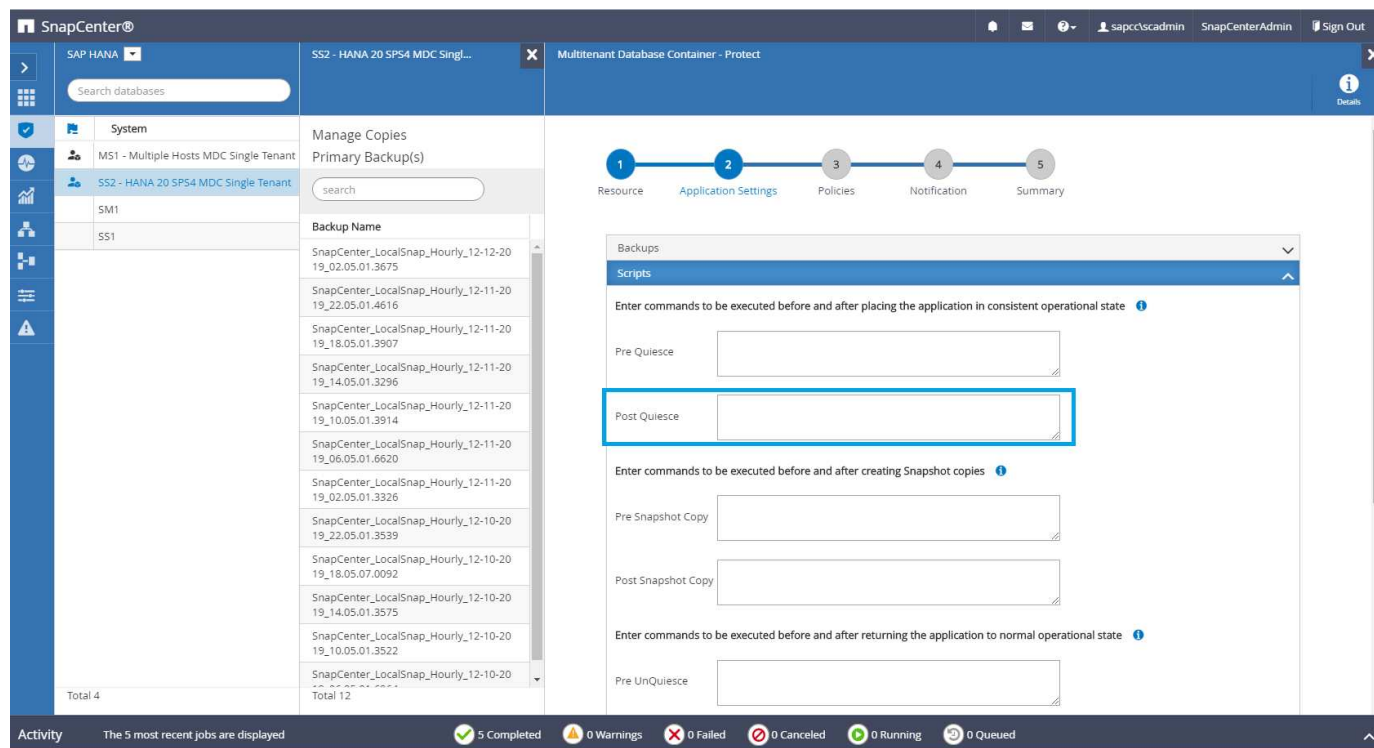
Se il server SnapCenter viene utilizzato come host plug-in HANA centrale, è possibile utilizzare un file batch. Il file batch deve avere il seguente contenuto:

```
@echo off
waitfor AnyThing /t 60 2>NUL
Exit /b 0
```

Il file batch può essere salvato, ad esempio, come `C:\Program Files\NetApp\Wait60Sec.bat`. Nella configurazione di protezione delle risorse, il file batch deve essere aggiunto come comando Post Quiesce.

Se un host Linux separato viene utilizzato come host plug-in HANA centrale, è necessario configurare il comando `/bin/sleep 60` Come il comando Post Quiesce nell'interfaccia utente di SnapCenter.

La figura seguente mostra il comando Post Quiesce nella schermata di configurazione della protezione delle risorse.



Configurazione specifica delle risorse SnapCenter per i backup di volumi diversi dai dati

Il backup dei volumi non dati è parte integrante del plug-in SAP HANA. La protezione del volume di dati del database è sufficiente per ripristinare e ripristinare il database SAP

HANA in un dato momento, a condizione che le risorse di installazione del database e i registri richiesti siano ancora disponibili.

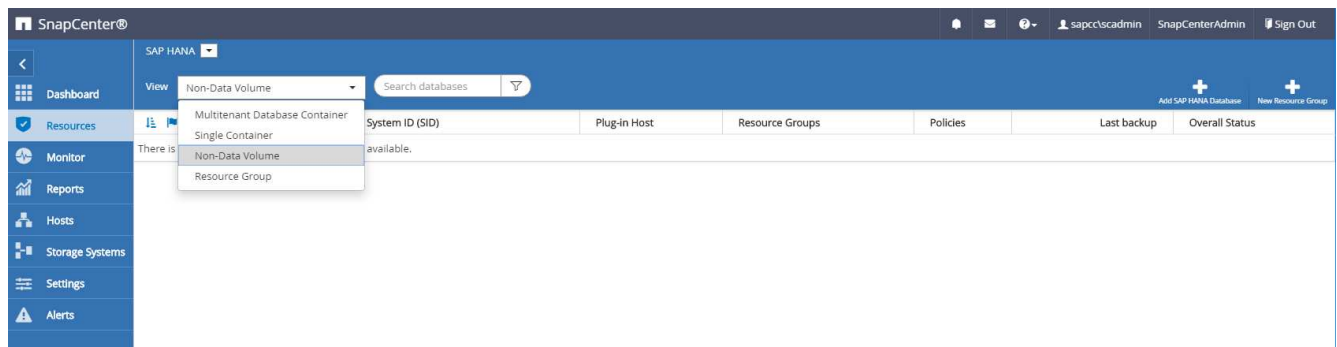
Per eseguire il ripristino da situazioni in cui devono essere ripristinati altri file non di dati, NetApp consiglia di sviluppare una strategia di backup aggiuntiva per i volumi non di dati per aumentare il backup del database SAP HANA. A seconda dei requisiti specifici, il backup dei volumi non dati potrebbe differire in termini di frequenza di pianificazione e impostazioni di conservazione e si dovrebbe considerare la frequenza con cui i file non dati vengono modificati. Ad esempio, il volume HANA /hana/shared Contiene file eseguibili ma anche file di traccia SAP HANA. Mentre gli eseguibili cambiano solo quando il database SAP HANA viene aggiornato, i file di traccia SAP HANA potrebbero richiedere una frequenza di backup più elevata per supportare l'analisi delle situazioni problematiche con SAP HANA.

Il backup dei volumi non dati di SnapCenter consente di creare copie Snapshot di tutti i volumi rilevanti in pochi secondi con la stessa efficienza dello spazio dei backup dei database SAP HANA. La differenza è che non è richiesta alcuna comunicazione SQL con il database SAP HANA.

Configurazione di risorse non di volumi di dati

In questo esempio, vogliamo proteggere i volumi non dati del database SAP HANA SS1.

1. Dalla scheda Resource, selezionare non-Data-Volume e fare clic su Add SAP HANA Database (Aggiungi database SAP HANA).



2. Nella fase uno della finestra di dialogo Add SAP HANA Database (Aggiungi database SAP HANA), nell'elenco Resource Type (tipo di risorsa), selezionare non-data Volumes (volumi non dati). Specificare un nome per la risorsa, il SID associato e l'host del plug-in SAP HANA che si desidera utilizzare per la risorsa, quindi fare clic su Avanti.

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Resource Details

Resource Type

Non-data Volumes

Resource Name

SS1-Shared-Volume

Associated SID

SS1

Plug-in Host

hana-1.sapcc.stl.netapp.com

Previous

Next

3. Aggiungere la SVM e il volume di storage come footprint dello storage, quindi fare clic su Next (Avanti).

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Storage Footprint Details

Add Storage Footprint

Storage System

hana-primary.sapcc.stl.netapp.com

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

Volume name

SS1_shared

SM1_data_mnt00001

SM1_log_mnt00001

SM1_shared

SS1_data_mnt00001

SS1_log_mnt00001

SS1_shared

SS1_data_mnt00001

LUNs or Qtrees

Default is 'None' or type to find

+

x

Save

Previous

Next

- Nella fase di riepilogo, fare clic su fine per salvare le impostazioni.
- Ripetere questi passaggi per tutti i volumi non dati richiesti.
- Continuare con la configurazione della protezione della nuova risorsa.



La protezione dei dati per risorse non di volumi di dati è identica al workflow per le risorse di database SAP HANA e può essere definita a livello di risorse individuali.

La figura seguente mostra l'elenco delle risorse di volumi non dati configurate.

SnapCenter®							
SAP HANA							
View: Non-Data Volume Search databases							
Dashboard	Add SAP HANA Database New Resource Group						
Resources							
Monitor							
Reports							
Hosts							
Storage Systems							
Settings							
Alerts							
	Name	Associated System ID (SID)	Plug-In Host	Resource Groups	Policies	Last backup	Overall Status
	SS1-Shared-Volume	SS1	hana-1.sapcc.stl.netapp.com		LocalSnap		Backup not run

Gruppi di risorse

I gruppi di risorse sono un metodo pratico per definire la protezione di più risorse che richiedono le stesse policy di protezione e la stessa pianificazione. Le singole risorse che fanno parte di un gruppo di risorse possono comunque essere protette a livello individuale.

I gruppi di risorse offrono le seguenti funzionalità:

- È possibile aggiungere una o più risorse a un gruppo di risorse. Tutte le risorse devono appartenere allo stesso plug-in SnapCenter.
- La protezione può essere definita a livello di gruppo di risorse. Tutte le risorse del gruppo di risorse utilizzano lo stesso criterio e la stessa pianificazione quando vengono protette.
- Tutti i backup nel repository SnapCenter e le copie Snapshot dello storage hanno lo stesso nome definito nella protezione delle risorse.
- Le operazioni di ripristino vengono applicate a un singolo livello di risorse, non come parte di un gruppo di risorse.
- Quando si utilizza SnapCenter per eliminare il backup di una risorsa creata a livello di gruppo di risorse, questo backup viene eliminato per tutte le risorse del gruppo di risorse. L'eliminazione del backup include l'eliminazione del backup dal repository SnapCenter e l'eliminazione delle copie Snapshot dello storage.
- Il caso d'utilizzo principale per i gruppi di risorse è quando un cliente desidera utilizzare i backup creati con SnapCenter per la clonazione del sistema con SAP Landscape Management. Questa procedura viene descritta nella sezione successiva.

Utilizzo di SnapCenter insieme alla gestione dell'ambiente SAP

Con SAP Landscape Management (SAP lama), i clienti possono gestire complessi scenari di sistema SAP nei data center on-premise e nei sistemi in esecuzione nel cloud. SAP lama, insieme a NetApp Storage Services Connector (SSC), può eseguire operazioni di storage come cloning e replica per i casi di utilizzo di cloni, copie e refresh del sistema SAP utilizzando la tecnologia Snapshot e FlexClone. Ciò consente di automatizzare completamente una copia del sistema SAP basata sulla tecnologia di cloning dello storage, includendo anche la postelaborazione SAP richiesta. Per ulteriori informazioni sulle soluzioni NetApp per SAP lama, fare riferimento a ["TR-4018: Integrazione dei sistemi NetApp ONTAP con la gestione del panorama SAP"](#).

NetApp SSC e SAP lama possono creare copie Snapshot on-demand direttamente utilizzando NetApp SSC, ma possono anche utilizzare copie Snapshot create utilizzando SnapCenter. Per utilizzare i backup SnapCenter come base per le operazioni di copia e clonazione del sistema con SAP lama, è necessario soddisfare i seguenti prerequisiti:

- SAP lama richiede che tutti i volumi siano inclusi nel backup, inclusi i dati SAP HANA, i volumi log e condivisi.
- Tutti i nomi Snapshot dello storage devono essere identici.
- I nomi Snapshot dello storage devono iniziare con VCM.



Nelle normali operazioni di backup, NetApp sconsiglia di includere il volume di log. Se si ripristina il volume di log da un backup, vengono sovrascritti gli ultimi log di ripristino attivi e viene impedito il ripristino del database all'ultimo stato recente.

I gruppi di risorse SnapCenter soddisfano tutti questi requisiti. In SnapCenter sono configurate tre risorse: Una risorsa per il volume di dati, il volume di log e il volume condiviso. Le risorse vengono inserite in un gruppo di risorse e la protezione viene quindi definita a livello di gruppo di risorse. Nella protezione del gruppo di risorse, il nome Snapshot personalizzato deve essere definito con VCM all'inizio.

Backup del database

In SnapCenter, i backup del database vengono in genere eseguiti utilizzando le pianificazioni definite all'interno della configurazione di protezione delle risorse di ciascun database HANA.

Il backup del database on-demand può essere eseguito utilizzando l'interfaccia utente grafica di SnapCenter, una riga di comando PowerShell o API REST.

Identificazione dei backup SnapCenter in SAP HANA Studio

La topologia delle risorse di SnapCenter mostra un elenco di backup creati utilizzando SnapCenter. La figura seguente mostra i backup disponibili sullo storage primario ed evidenzia il backup più recente.

The screenshot shows the SnapCenter interface with the 'SS1 Topology' view. On the left, a sidebar lists 'System' and 'SS1'. The main area displays 'Manage Copies' with a diagram showing 'Local copies' (15 Backups, 0 Clones) and 'Vault copies' (5 Backups, 0 Clones). A 'Summary Card' on the right shows '21 Backups', '20 Snapshot-based backups', '1 File-based backup', and '0 Clones'. Below this is a table of 'Primary Backup(s)' with columns for 'Backup Name', 'Count', and 'End Date'. The first row is highlighted with a blue box.

Backup Name	Count	End Date
SnapCenter_LocalSnap_Hourly_12-03-2019_02.30.01.5053	1	12/03/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_22.30.01.4925	1	12/02/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_18.30.01.3834	1	12/02/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_14.30.01.3366	1	12/02/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_10.30.01.4510	1	12/02/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08.17.01.9273	1	12/02/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_06.30.01.3164	1	12/02/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_02.30.01.3555	1	12/02/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-01-2019_22.30.01.3859	1	12/01/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-01-2019_18.30.01.3834	1	12/01/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-01-2019_14.30.01.3255	1	12/01/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-01-2019_10.30.01.2508	1	12/01/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-01-2019_08.17.01.9654	1	12/01/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-01-2019_06.30.01.2968	1	12/01/2019 6:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_11-30-2019_08.17.01.8590	1	11/30/2019 8:17:55 AM
Total 15		

Quando si esegue un backup utilizzando le copie Snapshot dello storage per un sistema SAP HANA MDC, viene creata una copia Snapshot del volume di dati. Questo volume di dati contiene i dati del database di sistema e i dati di tutti i database tenant. Per riflettere questa architettura fisica, SAP HANA esegue internamente un backup combinato del database di sistema e di tutti i database tenant ogni volta che SnapCenter attiva un backup Snapshot. Ciò comporta più voci di backup separate nel catalogo di backup SAP HANA: Una per il database di sistema e una per ogni database tenant.



Per i sistemi a container singolo SAP HANA, il volume di database contiene solo il singolo database e c'è una sola voce nel catalogo di backup di SAP HANA.

Nel catalogo di backup SAP HANA, il nome del backup SnapCenter viene memorizzato come a. Comment oltre al campo External Backup ID (EBID). Questo è mostrato nella seguente schermata per il database di sistema e nella schermata successiva per il database del tenant SS1. Entrambe le figure evidenziano il nome del backup SnapCenter memorizzato nel campo dei commenti e EBID.



La release HANA 2.0 SPS4 (revisione 40 e 41) mostra sempre una dimensione di backup pari a zero per i backup basati su Snapshot. Questo problema è stato risolto con la revisione 42. Per ulteriori informazioni, consulta la nota SAP "<https://launchpad.support.sap.com/#/notes/2795010>".

Backup SYSTEMDB@SS1 (SYSTEM) SS1 - HANA20 SPS4 MDC Single Tenant

Overview | Configuration | Backup Catalog

Database: SYSTEMDB

Show Log Backups Show Delta Backups

Status	Started	Duration	Size	Backup Type	Destination
Dec 3, 2019 2:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 10:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 6:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 2:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 10:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 8:17:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 2, 2019 6:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 2:30:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 1, 2019 10:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 1, 2019 6:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 1, 2019 2:30:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 1, 2019 10:30:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 1, 2019 8:17:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 1, 2019 6:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Nov 30, 2019 8:17:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Nov 30, 2019 6:00:04 ...	00h 00m 03s	1.48 GB	Data Backup	File	
Nov 29, 2019 8:17:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Nov 28, 2019 8:17:25 ...	00h 00m 13s	0 B	Data Backup	Snapshot	

Backup Details

ID: 1575369024442

Status: Successful

Backup Type: Data Backup

Destination Type: Snapshot

Started: Dec 3, 2019 2:30:24 AM (America/Los_Angeles)

Finished: Dec 3, 2019 2:30:38 AM (America/Los_Angeles)

Duration: 00h 00m 14s

Size: 0 B

Throughput: n.a.

System ID: SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053

Additional Information: <ok>

Location: /hana/data/SS1/mnt00001/

Host	Service	Name	EBID
hana-1	nameserver	hdb00001	SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053

Backup SYSTEMDB@SS1 (SYSTEM) SS1 - HANA20 SPS4 MDC Single Tenant

Overview | Configuration | Backup Catalog

Database: SS1

Show Log Backups Show Delta Backups

Status	Started	Duration	Size	Backup Type	Destination
Dec 3, 2019 2:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 10:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 6:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 2:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 10:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 8:17:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 2, 2019 6:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 2, 2019 2:30:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 1, 2019 10:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 1, 2019 6:30:23 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 1, 2019 2:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 1, 2019 10:30:24 ...	00h 00m 13s	0 B	Data Backup	Snapshot	
Dec 1, 2019 8:17:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 1, 2019 6:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Dec 1, 2019 2:30:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Nov 30, 2019 8:17:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Nov 30, 2019 6:00:10 ...	00h 00m 03s	1.67 GB	Data Backup	File	
Nov 29, 2019 8:17:24 ...	00h 00m 14s	0 B	Data Backup	Snapshot	
Nov 28, 2019 8:17:25 ...	00h 00m 13s	0 B	Data Backup	Snapshot	

Backup Details

ID: 1575369024443

Status: Successful

Backup Type: Data Backup

Destination Type: Snapshot

Started: Dec 3, 2019 2:30:24 AM (America/Los_Angeles)

Finished: Dec 3, 2019 2:30:38 AM (America/Los_Angeles)

Duration: 00h 00m 14s

Size: 0 B

Throughput: n.a.

System ID: SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053

Additional Information: <ok>

Location: /hana/data/SS1/mnt00001/

Host	Service	Name	EBID
hana-1	indexserver	hdb00003...	SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053
hana-1	xsengine	hdb00002...	SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053



SnapCenter è consapevole solo dei propri backup. I backup aggiuntivi creati, ad esempio, con SAP HANA Studio, sono visibili nel catalogo SAP HANA, ma non in SnapCenter.

Identificazione dei backup SnapCenter sui sistemi storage

Per visualizzare i backup sul layer di storage, utilizzare Gestione di sistema di NetApp OnCommand e selezionare il volume del database nella vista SVM - Volume. La scheda copie Snapshot inferiori visualizza le copie Snapshot del volume. La seguente schermata mostra i backup disponibili per il volume di database SS1_data_mnt00001 allo storage primario. Il backup evidenziato è il backup mostrato in SnapCenter e SAP HANA Studio nelle immagini precedenti e ha la stessa convenzione di denominazione.

The screenshot shows the OnCommand System Manager interface. The left sidebar contains navigation options: Dashboard, Applications & Tiers, Storage, Nodes, Aggregates & Disks, SVMs, Volumes, LUNs, Qtrees, Quotas, Junction Paths, Network, Protection, Events & Jobs, and Configuration. The main panel displays the 'Volumes' section for 'Volume: SS1_data_mnt00001'. The 'Snapshots Copies' tab is selected, showing a table of snapshots. The table has columns: Status, State, Snapshot Name, Date Time, Total Size, and Application Dependency. One snapshot is highlighted with a blue border.

Status	State	Snapshot Name	Date Time	Total Size	Application Dependency
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-01-2019_08.17.01.9654	Dec/01/2019 11:03:44	106.27 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_06.30.01.3164	Dec/02/2019 09:16:42	74.76 MB	None
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08.17.01.9273	Dec/02/2019 11:03:43	17.21 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_10.30.01.4510	Dec/02/2019 13:16:42	39.11 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_14.30.01.3366	Dec/02/2019 17:16:42	87.53 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_18.30.01.3834	Dec/02/2019 21:16:41	95.67 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-02-2019_22.30.01.4925	Dec/03/2019 01:16:41	29.86 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-03-2019_02.30.01.5053	Dec/03/2019 05:16:41	43.81 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-03-2019_06.30.01.4088	Dec/03/2019 09:16:40	49.46 MB	None
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-03-2019_08.17.01.9180	Dec/03/2019 11:03:41	77.14 MB	snapmirror
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-03-2019_10.30.01.4554	Dec/03/2019 13:16:40	42.12 MB	None
Normal	-NA-	SnapCenter_LocalSnap_Hourly_12-03-2019_14.30.01.3902	Dec/03/2019 17:16:40	57.42 MB	None

La seguente schermata mostra i backup disponibili per il volume di destinazione della replica hana_SA1_data_mnt00001_dest nel sistema di storage secondario.

The screenshot shows the OnCommand System Manager interface. The left sidebar contains navigation options: Dashboard, Applications & Tiers, Storage, Nodes, Aggregates & Disks, SVMs, Volumes, LUNs, Qtrees, Quotas, Junction Paths, Network, Protection, Events & Jobs, and Configuration. The main panel displays the 'Volumes' section for 'Volume: SS1_data_mnt00001_dest'. The 'Snapshots Copies' tab is selected, showing a table of snapshots. The table has columns: Status, State, Snapshot Name, Date Time, Total Size, and Application Dependency. One snapshot is highlighted with a blue border.

Status	State	Snapshot Name	Date Time	Total Size	Application Dependency
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_11-29-2019_08.17.01.8567	Nov/29/2019 11:03:48	113.34 MB	None
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_11-30-2019_08.17.01.8590	Nov/30/2019 11:03:46	87.69 MB	None
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-01-2019_08.17.01.9654	Dec/01/2019 11:03:44	108.67 MB	None
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08.17.01.9273	Dec/02/2019 11:03:43	102 MB	None
Busy	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_12-03-2019_08.17.01.9180	Dec/03/2019 11:03:41	176 KB	busy

Backup del database on-demand sullo storage primario

1. Nella vista delle risorse, selezionare la risorsa e fare doppio clic sulla riga per passare alla vista della topologia.

La vista della topologia delle risorse offre una panoramica di tutti i backup disponibili creati utilizzando SnapCenter. L'area superiore di questa vista visualizza la topologia di backup, mostrando i backup sullo storage primario (copie locali) e, se disponibile, sullo storage di backup off-site (copie del vault).

The screenshot displays the SnapCenter interface for the SS1 Topology. The top navigation bar includes icons for 'Remove Protection', 'Backup Now' (highlighted with a red box), 'Modify', 'Maintenance', 'Details', 'Configure Database', and 'Refresh'. The main content area is divided into several sections:

- Manage Copies:** Shows a hierarchy of backup copies. 'Local copies' are listed as '15 Backups' and '0 Clones'. 'Vault copies' are listed as '5 Backups' and '0 Clones'.
- Summary Card:** Provides a high-level overview of backup statistics: 21 Backups, 20 Snapshot based backups, 1 File-based backup, and 0 Clones.
- Primary Backup(s):** A table listing individual backup jobs with columns for Backup Name, Count, and End Date.

Backup Name	Count	End Date
SnapCenter_LocalSnap_Hourly_12-03-2019_02.30.01.5053	1	12/03/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_22.30.01.4925	1	12/02/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_18.30.01.3834	1	12/02/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_14.30.01.3366	1	12/02/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_10.30.01.4510	1	12/02/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08.17.01.9273	1	12/02/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_06.30.01.3164	1	12/02/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_02.30.01.3555	1	12/02/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-01-2019_22.30.01.3859	1	12/01/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-01-2019_18.30.01.3834	1	12/01/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-01-2019_14.30.01.3255	1	12/01/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-01-2019_10.30.01.2508	1	12/01/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-01-2019_08.17.01.9654	1	12/01/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-01-2019_06.30.01.2968	1	12/01/2019 6:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_11-30-2019_08.17.01.8590	1	11/30/2019 8:17:55 AM

The bottom status bar shows activity metrics: 5 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, and 0 Queued.

2. Nella riga superiore, selezionare l'icona Backup Now per avviare un backup on-demand. Dall'elenco a discesa, selezionare il criterio di backup LocalSnap. Quindi fare clic su Backup per avviare il backup on-demand.

Backup

×

Create a backup for the selected resource

Resource Name

SS1

Policy

LocalSnap

▼

i

Cancel

Backup

Viene avviato il processo di backup. Un registro dei cinque job precedenti viene visualizzato nell'area Activity (attività) sotto la vista della topologia. Al termine del backup, viene visualizzata una nuova voce nella vista della topologia. I nomi dei backup seguono la stessa convenzione di denominazione del nome Snapshot definito nella sezione ["Configurazione della protezione delle risorse"](#).



Per visualizzare l'elenco di backup aggiornato, è necessario chiudere e riaprire la vista della topologia.

Manage Copies

Local copies: 16 Backups, 0 Clones

Vault copies: 5 Backups, 0 Clones

Summary Card

- 22 Backups
- 21 Snapshot based backups
- 1 File Based backup ✓
- 0 Clones

Primary Backup(s)

Backup Name	Count	End Date
SnapCenter_LocalSnap_12-03-2019_06:37:50.1491	1	12/03/2019 6:38:44 AM
SnapCenter_LocalSnap_Hourly_12-03-2019_06:30:01.4088	1	12/03/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-03-2019_02:30:01.5053	1	12/03/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_22:30:01.4925	1	12/02/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_18:30:01.3834	1	12/02/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_14:30:01.3366	1	12/02/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_10:30:01.4510	1	12/02/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08:17:01.9273	1	12/02/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_06:30:01.3164	1	12/02/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_02:30:01.3555	1	12/02/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-01-2019_22:30:01.3859	1	12/01/2019 10:30:55 PM

Total 4

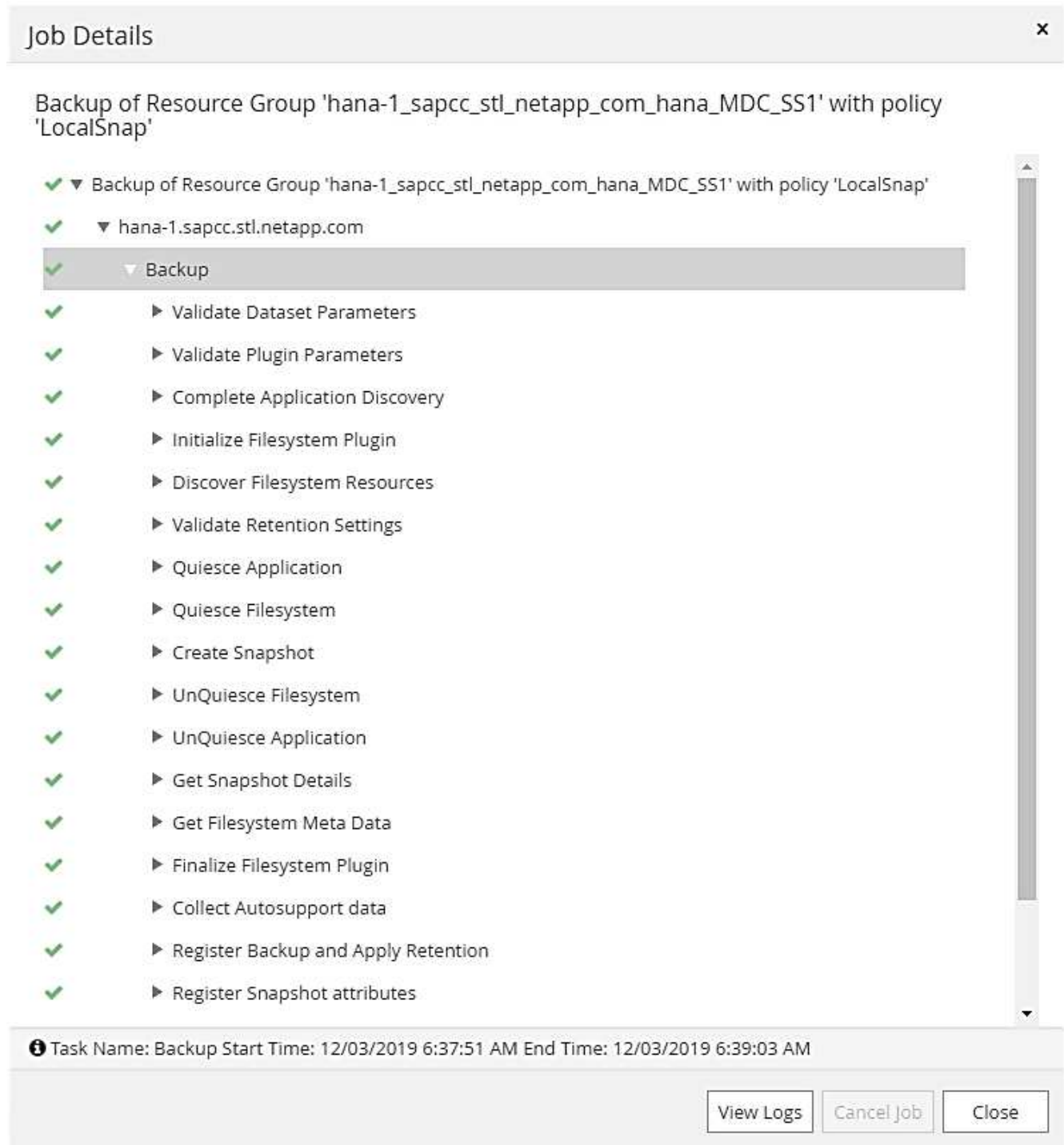
Activity

The 5 most recent jobs are displayed

- 5 Completed
- 0 Warnings
- 0 Failed
- 0 Canceled
- 0 Running
- 0 Queued

Activity	Status
Backup of Resource Group 'hana-1_sapcc_stl_netapp_com_hana_MDC_S51' with policy 'LocalSnap'	Completed ✓
Backup of Resource Group 'hana-1_sapcc_stl_netapp_com_hana_MDC_S51' with policy 'LocalSnap'	Completed ✓
Backup of Resource Group 'hana-2_sapcc_stl_netapp_com_hana_MDC_S51' with policy 'LocalSnap'	Completed ✓
Backup of Resource Group 'SnapCenter-43_sapcc_stl_netapp_com_hana_MDC_S52' with policy 'LocalSnap'	Completed ✓
Backup of Resource Group 'SnapCenter-43_sapcc_stl_netapp_com_hana_MDC_S51' with policy 'LocalSnap'	Completed ✓

- I dettagli della commessa vengono visualizzati facendo clic sulla riga dell'attività della commessa nell'area Activity (attività). È possibile aprire un registro dettagliato dei processi facendo clic su View Logs (Visualizza registri).



4. In SAP HANA Studio, il nuovo backup è visibile nel catalogo di backup. Lo stesso nome di backup in SnapCenter viene utilizzato anche nel campo comment e EBID nel catalogo di backup.

Backup di database on-demand con replica SnapVault

1. Nella vista delle risorse, selezionare la risorsa e fare doppio clic sulla riga per passare alla vista della topologia.
2. Nella riga superiore, selezionare l'icona Backup Now per avviare un backup on-demand. Dall'elenco a discesa, selezionare il criterio di backup `LocalSnapAndSnapVault`, Quindi fare clic su Backup per avviare il backup on-demand.

Backup

×

Create a backup for the selected resource

Resource Name

SS1

Policy

LocalSnapAndSnapVault

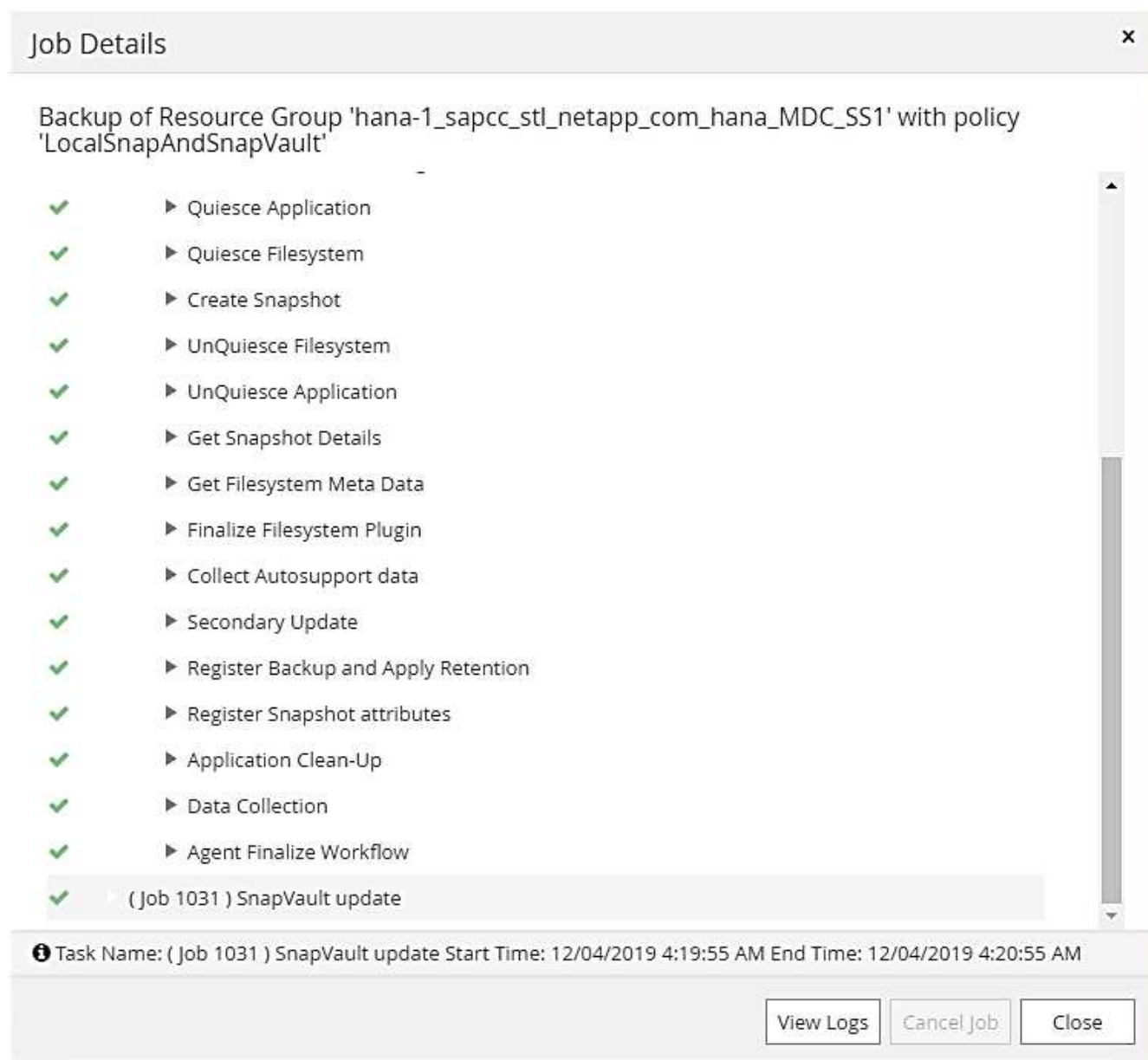
▼

i

Cancel

Backup

3. I dettagli della commessa vengono visualizzati facendo clic sulla riga dell'attività della commessa nell'area Activity (attività).



4. Al termine del backup, viene visualizzata una nuova voce nella vista della topologia. I nomi dei backup seguono la stessa convenzione di denominazione del nome Snapshot definito nella sezione ["Configurazione della protezione delle risorse"](#).



Per visualizzare l'elenco di backup aggiornato, è necessario chiudere e riaprire la vista della topologia.

Manage Copies

Local copies: 16 Backups, 0 Clones

Vault copies: 6 Backups, 0 Clones

Primary Backup(s)

Backup Name	Count	IF	End Date
SnapCenter_LocalSnapAndSnapVault_12-04-2019_04.18.57.8527	1		12/04/2019 4:19:52 AM
SnapCenter_LocalSnap_Hourly_12-04-2019_02.30.01.4636	1		12/04/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-03-2019_22.30.01.4836	1		12/03/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-03-2019_18.30.01.4818	1		12/03/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-03-2019_14.30.01.3902	1		12/03/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-03-2019_10.30.01.4554	1		12/03/2019 10:30:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-03-2019_08.17.01.9180	1		12/03/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-03-2019_06.30.01.4088	1		12/03/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-03-2019_02.30.01.5053	1		12/03/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-02-2019_22.30.01.4925	1		12/02/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-02-2019_18.30.01.3934	1		12/02/2019 6:30:55 PM
Total 16			

Activity: The 5 most recent jobs are displayed. 5 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, 0 Queued.

5. Selezionando le copie del vault, vengono visualizzati i backup nello storage secondario. Il nome del backup replicato è identico al nome del backup nello storage primario.

Manage Copies

Local copies: 16 Backups, 0 Clones

Vault copies: 6 Backups, 0 Clones

Secondary Vault Backup(s)

Backup Name	Count	IF	End Date
SnapCenter_LocalSnapAndSnapVault_12-04-2019_04.18.57.8527	1		12/04/2019 4:19:52 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-03-2019_08.17.01.9180	1		12/03/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08.17.01.9273	1		12/02/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-01-2019_08.17.01.9654	1		12/01/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_11-30-2019_08.17.01.8590	1		11/30/2019 8:17:55 AM
SnapCenter_LocalSnapAndSnapVault_Daily_11-29-2019_08.17.01.8567	1		11/29/2019 8:17:56 AM
Total 6			

Activity: The 5 most recent jobs are displayed. 5 Completed, 0 Warnings, 0 Failed, 0 Canceled, 0 Running, 0 Queued.

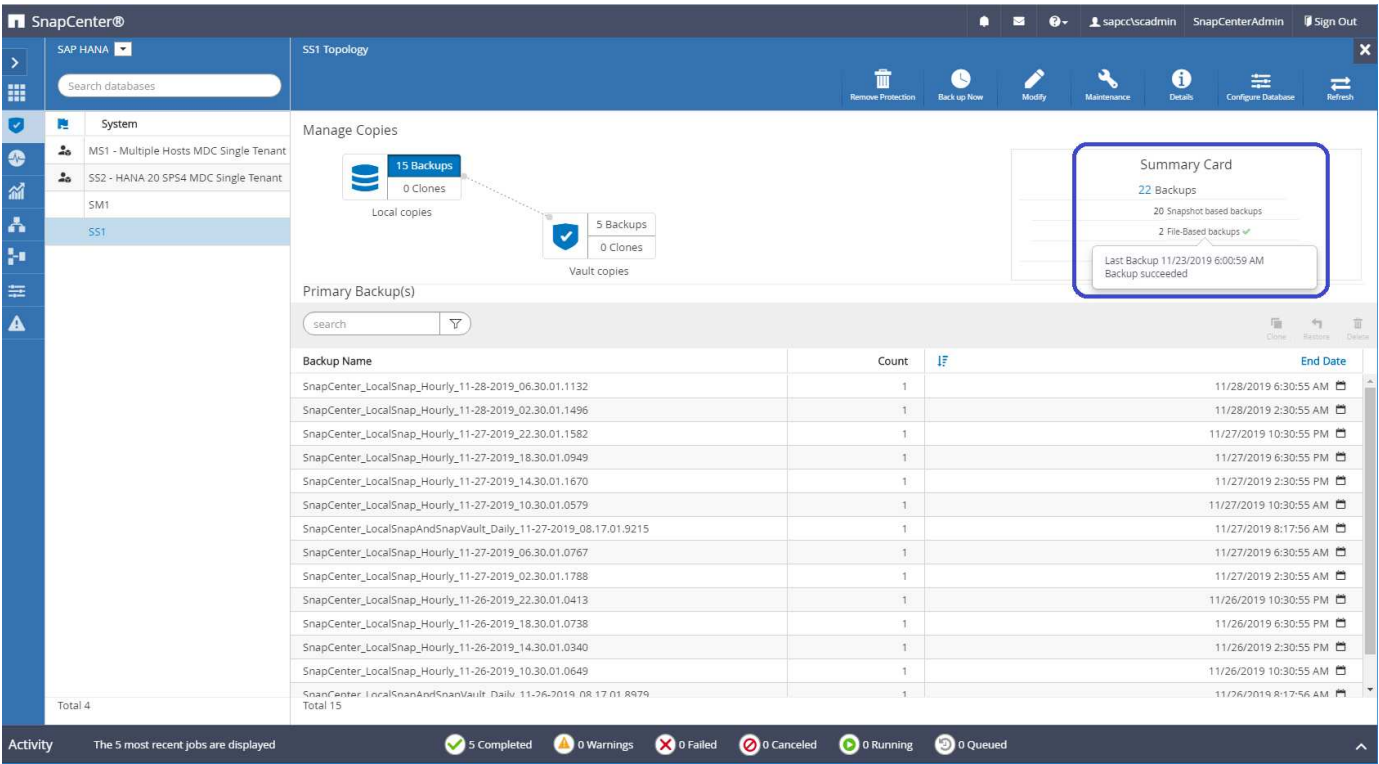
6. In SAP HANA Studio, il nuovo backup è visibile nel catalogo di backup. Lo stesso nome di backup in SnapCenter viene utilizzato anche nel campo comment e EBID nel catalogo di backup.

Controllo dell'integrità del blocco

SAP consiglia di combinare i backup Snapshot basati su storage con un backup settimanale basato su file per eseguire un controllo dell'integrità dei blocchi. SnapCenter supporta l'esecuzione di un controllo dell'integrità dei blocchi utilizzando un criterio in cui il backup basato su file viene selezionato come tipo di backup.

Quando si pianificano i backup utilizzando questo criterio, SnapCenter crea un backup standard del file SAP HANA per i database del sistema e del tenant.

SnapCenter non visualizza il controllo dell'integrità del blocco allo stesso modo dei backup basati su copia Snapshot. La scheda di riepilogo mostra invece il numero di backup basati su file e lo stato del backup precedente.



Non è possibile eliminare un backup del controllo dell'integrità dei blocchi utilizzando l'interfaccia utente di SnapCenter, ma è possibile eliminarlo utilizzando i comandi di PowerShell.

```

PS C:\Users\scadmin> Get-SmBackupReport -Resource SS1
SmBackupId           : 9
SmJobId              : 42
StartDateTime        : 11/19/2019 8:26:32 AM
EndDateTime          : 11/19/2019 8:27:33 AM
Duration             : 00:01:00.7652030
CreatedDateTime       : 11/19/2019 8:27:24 AM
Status               : Completed
ProtectionGroupName  : hana-1_sapcc_stl_netapp_com_hana_MDC_SS1
SmProtectionGroupId   : 1
PolicyName           : BlockIntegrityCheck
SmPolicyId           : 5
BackupName           : SnapCenter_BlockIntegrityCheck_11-19-
2019_08.26.33.2913
VerificationStatus   : NotApplicable
VerificationStatuses :
SmJobError            :
BackupType           : SCC_BACKUP
CatalogingStatus     : NotApplicable
CatalogingStatuses   :
ReportDataCreatedDateTime :
PluginCode           : SCC
PluginName           : hana
JobTypeId            : 0
JobHost              :

PS C:\Users\scadmin> Remove-SmBackup -BackupIds 9

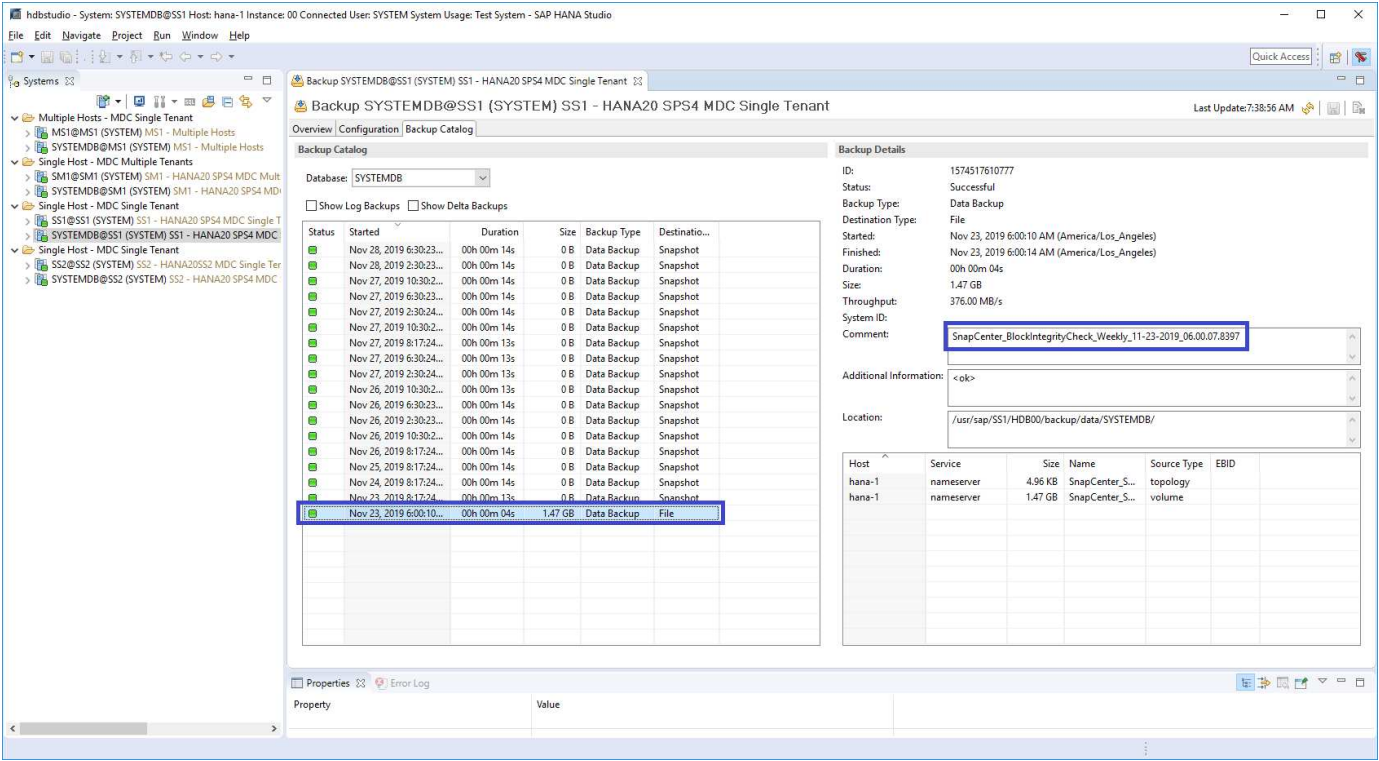
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"): y

BackupResult : {}
Result       : SMCoreContracts.SMResult
TotalCount   : 0
DisplayCount : 0
Context      :
Job          : SMCoreContracts.SmJob

PS C:\Users\scadmin>

```

Il catalogo di backup SAP HANA mostra le voci per i database di sistema e tenant. La figura seguente mostra un controllo dell'integrità del blocco SnapCenter nel catalogo di backup del database di sistema.



Un controllo dell'integrità dei blocchi consente di creare file di backup dei dati SAP HANA standard. SnapCenter utilizza il percorso di backup configurato nel database HANA per le operazioni di backup dei dati basate su file.

```

hana-1:/usr/sap/SS1/HDB00/backup/data # ls -al *
DB_SS1:
total 1710840
drwxr-xr-- 2 ssladm sapsys      4096 Nov 28 10:25 .
drwxr-xr-- 4 ssladm sapsys      4096 Nov 19 05:11 ..
-rw-r----- 1 ssladm sapsys    155648 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ssladm sapsys    83894272 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_2_1
-rw-r----- 1 ssladm sapsys 1660952576 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_3_1
SYSTEMDB:
total 1546340
drwxr-xr-- 2 ssladm sapsys      4096 Nov 28 10:24 .
drwxr-xr-- 4 ssladm sapsys      4096 Nov 19 05:11 ..
-rw-r----- 1 ssladm sapsys    159744 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ssladm sapsys 1577066496 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_1_1

```

Ripristino e ripristino

Le sezioni seguenti descrivono i flussi di lavoro di ripristino e ripristino di tre scenari diversi e configurazioni di esempio.

- Ripristino e ripristino automatici:
 - Sistema HANA rilevato automaticamente SS1
 - Sistema single-tenant SAP HANA host, MDC con NFS
- Ripristino e ripristino single-tenant:
 - Sistema HANA rilevato automaticamente SM1
 - Sistema multi-tenant SAP HANA singolo host, MDC con NFS
- Ripristino con ripristino manuale:
 - Sistema HANA configurato manualmente SS2
 - Sistema multi-tenant SAP HANA singolo host, MDC con NFS

Nelle sezioni seguenti vengono evidenziate le differenze tra host singolo e host multipli SAP HANA e sistemi HANA collegati FIBRE Channel SAN.

Gli esempi mostrano SAP HANA Studio come uno strumento per eseguire il ripristino manuale. È inoltre

possibile utilizzare istruzioni SAP HANA Cockpit o HANA SQL.

Ripristino e ripristino automatici

Con SnapCenter 4.3, le operazioni di ripristino e ripristino automatizzate sono supportate per i sistemi HANA single container o MDC single tenant che sono stati rilevati automaticamente da SnapCenter.

È possibile eseguire un'operazione di ripristino e ripristino automatica con i seguenti passaggi:

1. Selezionare il backup da utilizzare per l'operazione di ripristino. Il backup può essere selezionato tra le seguenti opzioni di storage:
 - Storage primario
 - Storage di backup offsite (destinazione SnapVault)
2. Selezionare il tipo di ripristino. Selezionare Ripristino completo con ripristino del volume o senza ripristino del volume.



L'opzione di ripristino del volume è disponibile solo per le operazioni di ripristino dallo storage primario e se il database HANA utilizza NFS come protocollo di storage.

3. Selezionare il tipo di ripristino tra le seguenti opzioni:
 - Allo stato più recente
 - Point-in-time
 - A backup di dati specifici
 - Nessun ripristino



Il tipo di ripristino selezionato viene utilizzato per il ripristino del sistema e del database tenant.

Successivamente, SnapCenter esegue le seguenti operazioni:

1. Interrompe il database HANA.
2. Ripristina il database.

A seconda del tipo di ripristino selezionato e del protocollo di storage utilizzato, vengono eseguite diverse operazioni.

- Se sono selezionati NFS e revert volume, SnapCenter smonta il volume, ripristina il volume utilizzando SnapRestore basato sul volume sul layer di storage e monta il volume.
 - Se si seleziona NFS e l'opzione di ripristino del volume non è selezionata, SnapCenter ripristina tutti i file utilizzando operazioni SnapRestore a file singolo sul layer di storage.
 - Se si seleziona SAN Fibre Channel, SnapCenter dismonta i LUN, ripristina i LUN utilizzando operazioni SnapRestore a file singolo sul layer di storage e rileva e monta i LUN.
3. Recupera il database:
 - a. Recupera il database di sistema.
 - b. Recupera il database del tenant.

In alternativa, per i sistemi container singoli HANA, il ripristino viene eseguito in un'unica fase:

c. Avvia il database HANA.



Se si seleziona No Recovery (Nessun ripristino), SnapCenter viene chiuso e l'operazione di ripristino del sistema e del database tenant deve essere eseguita manualmente.

In questa sezione vengono fornite le procedure per il ripristino e il ripristino automatici del sistema HANA rilevato automaticamente SS1 (host singolo SAP HANA, sistema tenant singolo MDC che utilizza NFS).

1. Selezionare un backup in SnapCenter da utilizzare per l'operazione di ripristino.



È possibile selezionare il ripristino dallo storage di backup primario o esterno al sito.

The screenshot shows the SnapCenter interface for the SS1 topology. The 'Manage Copies' section displays 16 Backups (0 Clones) for Local copies and 6 Backups (0 Clones) for Vault copies. The 'Primary Backup(s)' table lists the following backups:

Backup Name	Count	End Date
SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385	1	12/05/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-05-2019_18.30.01.5244	1	12/05/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-05-2019_14.30.01.6022	1	12/05/2019 2:30:55 PM
SnapCenter_LocalSnap_Hourly_12-05-2019_10.30.01.5450	1	12/05/2019 10:30:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-05-2019_08.17.02.0191	1	12/05/2019 8:17:56 AM
SnapCenter_LocalSnap_Hourly_12-05-2019_06.30.01.5487	1	12/05/2019 6:30:55 AM
SnapCenter_LocalSnap_Hourly_12-05-2019_02.30.01.5470	1	12/05/2019 2:30:55 AM
SnapCenter_LocalSnap_Hourly_12-04-2019_22.30.01.5182	1	12/04/2019 10:30:55 PM
SnapCenter_LocalSnap_Hourly_12-04-2019_18.30.01.5249	1	12/04/2019 6:30:55 PM
SnapCenter_LocalSnap_Hourly_12-04-2019_14.30.01.5069	1	12/04/2019 2:30:55 PM

Total 4 for Local copies, Total 16 for Vault copies.

The screenshot shows the SnapCenter interface for the SS1 topology, focusing on the 'Secondary Vault Backup(s)' section. The 'Manage Copies' section displays 16 Backups (0 Clones) for Local copies and 5 Backups (0 Clones) for Vault copies. The 'Secondary Vault Backup(s)' table lists the following backups:

Backup Name	Count	End Date
SnapCenter_LocalSnapAndSnapVault_Daily_12-05-2019_08.17.02.0191	1	12/05/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-04-2019_08.17.01.9976	1	12/04/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_12-04-2019_04.18.57.8527	1	12/04/2019 4:19:52 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-03-2019_08.17.01.9180	1	12/03/2019 8:17:56 AM
SnapCenter_LocalSnapAndSnapVault_Daily_12-02-2019_08.17.01.9273	1	12/02/2019 8:17:56 AM

Total 4 for Local copies, Total 5 for Vault copies.

2. Selezionare l'ambito e il tipo di ripristino.

Le tre schermate seguenti mostrano le opzioni di ripristino per il ripristino da primario con NFS, il ripristino da secondario con NFS e il ripristino da primario con SAN Fibre Channel.

Opzioni del tipo di ripristino per il ripristino dallo storage primario.



L'opzione di ripristino del volume è disponibile solo per le operazioni di ripristino da primarie con NFS.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Select the restore types

☐ Complete Resource

☒ Volume Revert

☐ Tenant Database

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

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

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

Previous

Next

Opzioni del tipo di ripristino per il ripristino dallo storage di backup fuori sede.

Restore from SnapCenter_LocalSnapAndSnapVault_Daily_12-05-2019_08.17.02.0191

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

Select the restore types

☒ Complete Resource ⓘ

☐ Tenant Database

Choose archive location

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

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

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

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

Previous Next

Opzioni del tipo di ripristino per il ripristino dallo storage primario con SAN Fibre Channel.

Restore from SnapCenter_LocalSnap_Hourly_12-16-2019_22.35.01.3065

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

Select the restore types

☒ Complete Resource ⓘ

☐ Tenant Database

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

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

Previous Next

3. Selezionare Recovery Scope (ambito ripristino) e specificare la posizione per il backup del registro e del catalogo.



SnapCenter utilizza il percorso predefinito o i percorsi modificati nel file HANA global.ini per prepopolare le posizioni di backup del registro e del catalogo.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Recover database files using

☒ Recover to most recent state

☐ Recover to point in time

☐ Recover to specified data backup

☐ No recovery

Specify log backup locations

Add

/mnt/log-backup

Specify backup catalog location

/mnt/log-backup

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

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

Previous

Next

4. Immettere i comandi opzionali di prerestore.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run before performing a restore operation

Pre restore command

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

Previous

Next

5. Immettere i comandi post-ripristino opzionali.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run after performing a restore operation

Post restore command

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

Previous

Next

6. Immettere le impostazioni e-mail opzionali.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Provide email settings ⓘ

Email preference

Never

From

Email from

To

Email to

Subject

Notification

☐ Attach Job Report

⚠

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

✕

Previous

Next

7. Per avviare l'operazione di ripristino, fare clic su fine.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385 ✕

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Summary

Backup Name	SnapCenter_LocalSnap_Hourly_12-05-2019_22.30.01.5385
Backup date	12/05/2019 10:30:55 PM
Restore scope	Complete Resource with Volume Revert
Recovery scope	Recover to most recent state
Log backup locations	/mnt/log-backup
Backup catalog location	/mnt/log-backup
Pre restore command	
Post restore command	
Send email	No

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

Previous

Finish

8. SnapCenter esegue l'operazione di ripristino e ripristino. Questo esempio mostra i dettagli del processo di ripristino e ripristino.

Restore 'hana-1.sapcc.stl.netapp.com\hana\MDC\SS1'

- ✓ ▼ Restore 'hana-1.sapcc.stl.netapp.com\hana\MDC\SS1'
- ✓ ▼ hana-1.sapcc.stl.netapp.com
- ✓ ▼ Restore
- ✓ ▼ Validate Plugin Parameters
- ✓ ▼ Pre Restore Application
 - ▶ Stopping HANA instance
- ✓ ▼ Filesystem Pre Restore
 - ▶ Determining the restore mechanism
 - ▶ Deporting file systems and associated entities
- ✓ ▶ Restore Filesystem
- ✓ ▼ Filesystem Post Restore
 - ▶ Building file systems and associated entities
- ✓ ▼ Recover Application
- ✓ ▶ Recovering system database
- ✓ ▶ Checking HDB services status
- ✓ ▶ Recovering tenant database 'SS1'
- ✓ ▶ Starting HANA instance
- ✓ ▶ Clear Catalog on Server
- ✓ ▶ Application Clean-Up
- ✓ ▶ Data Collection
- ✓ ▶ Agent Finalize Workflow

i Task Name: Recover Application Start Time: 12/06/2019 7:26:11 AM End Time: 12/06/2019 7:28:46 AM

[View Logs](#)[Cancel Job](#)[Close](#)

Operazioni di ripristino e ripristino single-tenant

Con SnapCenter 4.3, le operazioni di ripristino single-tenant sono supportate per i sistemi HANA MDC con un singolo tenant o con più tenant rilevati automaticamente da SnapCenter.

È possibile eseguire un'operazione di ripristino e ripristino con un singolo tenant seguendo la procedura riportata di seguito:

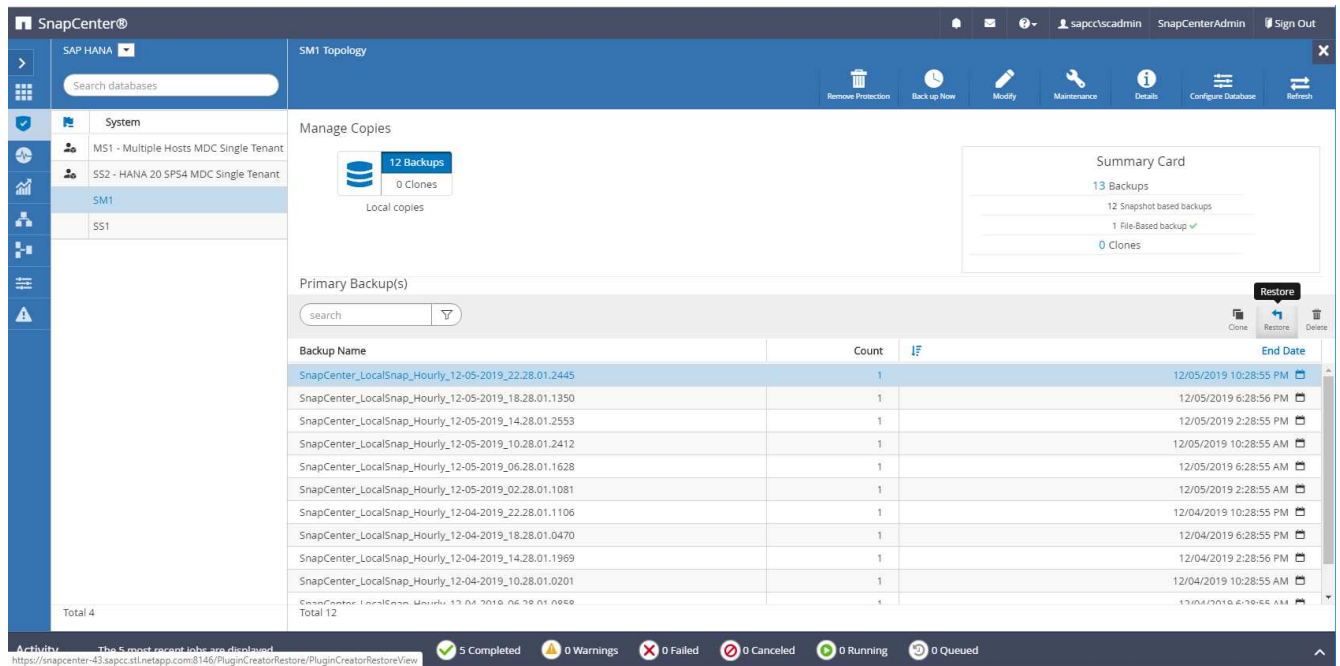
1. Arrestare il tenant da ripristinare e ripristinare.
2. Ripristinare il tenant con SnapCenter.
 - Per un ripristino dallo storage primario, SnapCenter esegue le seguenti operazioni:
 - **NFS.** Storage operazioni Single file SnapRestore per tutti i file del database tenant.
 - **SAN.** Clona e connetti il LUN all'host del database, quindi copia tutti i file del database tenant.
 - Per un ripristino dallo storage secondario, SnapCenter esegue le seguenti operazioni:
 - **NFS.** Storage SnapVault Ripristina le operazioni per tutti i file del database tenant
 - **SAN.** Clona e connetti il LUN all'host del database, quindi copia tutti i file del database tenant
3. Ripristinare il tenant con l'istruzione HANA Studio, Cockpit o SQL.

In questa sezione vengono fornite le procedure per l'operazione di ripristino dallo storage primario del sistema HANA SMI (sistema single-host SAP HANA, multi-tenant MDC con NFS) rilevato automaticamente. Dal punto di vista dell'input dell'utente, i flussi di lavoro sono identici per un ripristino da un ripristino secondario o da un ripristino in un'installazione SAN Fibre Channel.

1. Arrestare il database tenant.

```
smladm@hana-2:/usr/sap/SM1/HDB00> hdbsql -U SYSKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql=>
hdbsql SYSTEMDB=> alter system stop database tenant2;
0 rows affected (overall time 14.215281 sec; server time 14.212629 sec)
hdbsql SYSTEMDB=>
```

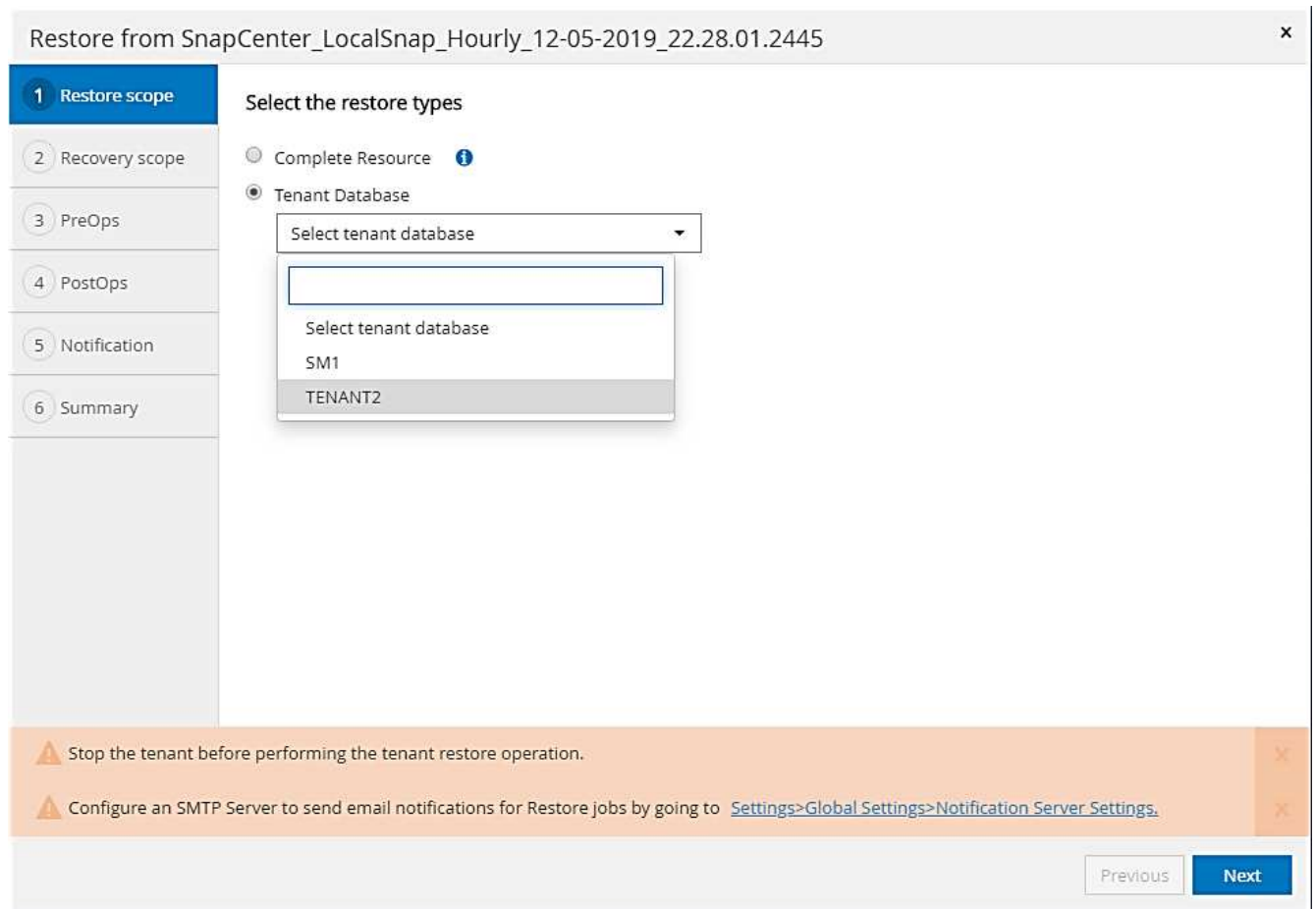
2. Selezionare un backup in SnapCenter da utilizzare per l'operazione di ripristino.



3. Selezionare il tenant da ripristinare.



SnapCenter mostra un elenco di tutti i tenant inclusi nel backup selezionato.



Il ripristino single-tenant non è supportato con SnapCenter 4.3. Nessun ripristino preselezionato e non modificabile.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Recover database files using

☐ Recover to most recent state

☐ Recover to point in time

☐ Recover to specified data backup

☒ No recovery

Recovery of an multitenant database container with multiple tenants is not supported

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

Previous

Next

4. Immettere i comandi opzionali di prerestore.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445 ✕

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run before performing a restore operation ⓘ

Pre restore command

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

Previous

Next

5. Immettere comandi post-ripristino opzionali.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Enter optional commands to run after performing a restore operation

Post restore command

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

Previous

Next

6. Immettere le impostazioni e-mail opzionali.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Provide email settings ⓘ

Email preference

Never

From

Email from

To

Email to

Subject

Notification

☐ Attach Job Report

⚠

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

✕

Previous

Next

7. Per avviare l'operazione di ripristino, fare clic su fine.

Restore from SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

1 Restore scope

2 Recovery scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Summary

Backup Name	SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445
Backup date	12/05/2019 10:28:55 PM
Restore scope	Restore tenant database 'TENANT2'
Recovery scope	No recovery
Pre restore command	
Post restore command	
Send email	No

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

Previous

Finish

L'operazione di ripristino viene eseguita da SnapCenter. Questo esempio mostra i dettagli del lavoro di ripristino.

Restore 'hana-2.sapcc.stl.netapp.com\hana\MDC\SM1'

✓ ▼ Restore 'hana-2.sapcc.stl.netapp.com\hana\MDC\SM1'

✓ ▼ hana-2.sapcc.stl.netapp.com

✓ ▼ Restore

✓ ▶ Validate Plugin Parameters

✓ ▶ Pre Restore Application

✓ ▶ Filesystem Pre Restore

✓ ▶ Restore Filesystem

✓ ▶ Filesystem Post Restore

✓ ▶ Recover Application

✓ ▶ Application Clean-Up

✓ ▶ Data Collection

✓ ▶ Agent Finalize Workflow

i Task Name: Restore Start Time: 12/06/2019 1:10:40 AM End Time: 12/06/2019 1:12:04 AM

View Logs

Cancel Job

Close



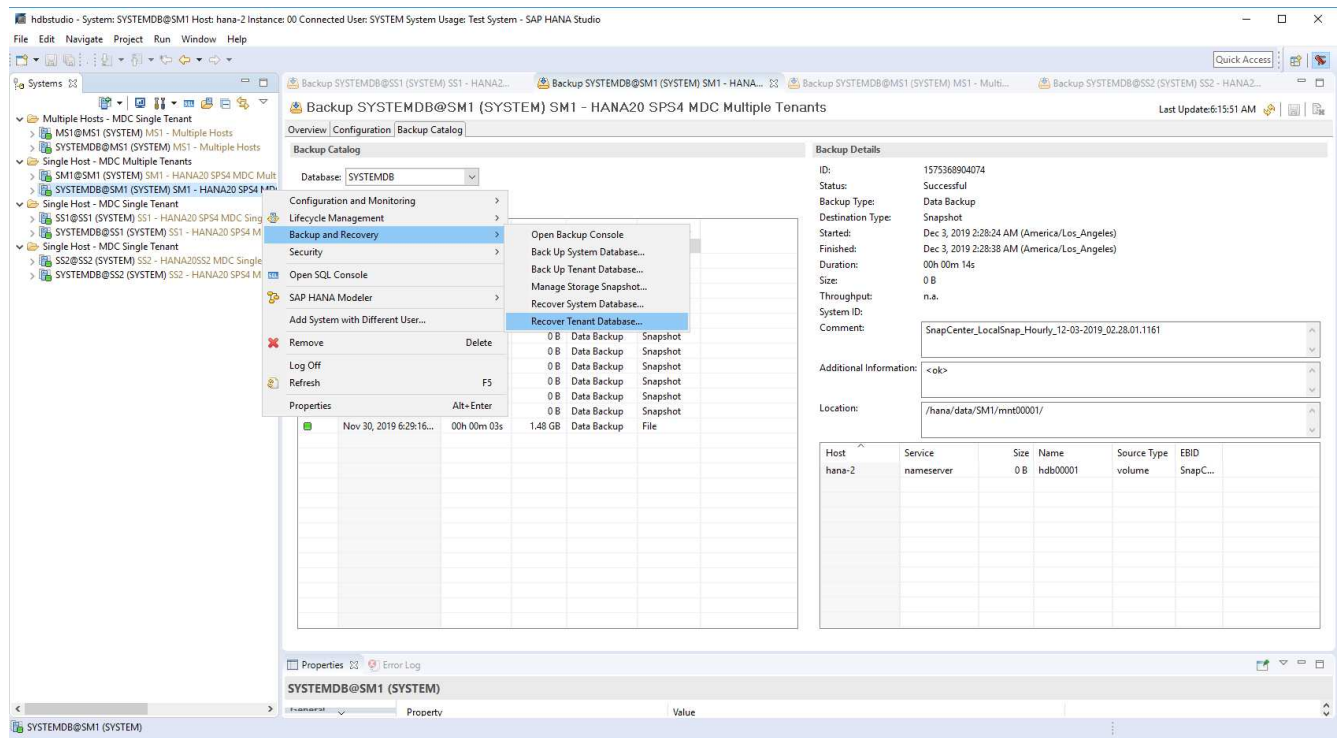
Al termine dell'operazione di ripristino del tenant, vengono ripristinati solo i dati rilevanti del tenant. Sul file system dell'host del database HANA, sono disponibili il file di dati ripristinato e il file ID di backup Snapshot del tenant.

```

smladm@hana-2:/usr/sap/SM1/HDB00> ls -al /hana/data/SM1/mnt00001/*
-rw-r--r-- 1 smladm sapsys 17 Dec 6 04:01
/hana/data/SM1/mnt00001/nameserver.lck
/hana/data/SM1/mnt00001/hdb00001:
total 3417776
drwxr-x--- 2 smladm sapsys 4096 Dec 6 01:14 .
drwxr-x--- 6 smladm sapsys 4096 Nov 20 09:35 ..
-rw-r----- 1 smladm sapsys 3758096384 Dec 6 03:59 datavolume_0000.dat
-rw-r----- 1 smladm sapsys 0 Nov 20 08:36
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 smladm sapsys 36 Nov 20 08:37 landscape.id
/hana/data/SM1/mnt00001/hdb00002.00003:
total 67772
drwxr-xr-- 2 smladm sapsys 4096 Nov 20 08:37 .
drwxr-x--- 6 smladm sapsys 4096 Nov 20 09:35 ..
-rw-r--r-- 1 smladm sapsys 201441280 Dec 6 03:59 datavolume_0000.dat
-rw-r--r-- 1 smladm sapsys 0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
/hana/data/SM1/mnt00001/hdb00002.00004:
total 3411836
drwxr-xr-- 2 smladm sapsys 4096 Dec 6 03:57 .
drwxr-x--- 6 smladm sapsys 4096 Nov 20 09:35 ..
-rw-r--r-- 1 smladm sapsys 3758096384 Dec 6 01:14 datavolume_0000.dat
-rw-r--r-- 1 smladm sapsys 0 Nov 20 09:35
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 smladm sapsys 155648 Dec 6 01:14
snapshot_databackup_0_1
/hana/data/SM1/mnt00001/hdb00003.00003:
total 3364216
drwxr-xr-- 2 smladm sapsys 4096 Dec 6 01:14 .
drwxr-x--- 6 smladm sapsys 4096 Nov 20 09:35 ..
-rw-r--r-- 1 smladm sapsys 3758096384 Dec 6 03:59 datavolume_0000.dat
-rw-r--r-- 1 smladm sapsys 0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
smladm@hana-2:/usr/sap/SM1/HDB00>

```

8. Avviare il ripristino con HANA Studio.



9. Selezionare il tenant.

Recovery of Tenant Database in SM1

Specify tenant database

ipe filter text

☐ SM1

☒ TENANT2

? < Back Next > Finish Cancel

10. Selezionare il tipo di ripristino.


Recovery of Tenant Database in SM1


Specify Recovery Type

Select a recovery type.

☒ Recover the database to its most recent state ⁱ

☐ Recover the database to the following point in time ⁱ


Date: 2019-12-06  Time: 01:18:31

Select Time Zone: (GMT-08:00) Pacific Standard Time 

ⁱ System Time Used (GMT): 2019-12-06 09:18:31

☐ Recover the database to a specific data backup ⁱ

Advanced >>

 < Back Next > Finish Cancel

11. Fornire la posizione del catalogo di backup.

Recovery of Tenant Database in SM1

Locate Backup Catalog

Specify location of the backup catalog.

☒ Recover using the backup catalog

☒ Search for the backup catalog in the file system only


Backup Catalog Location:

☐ Recover without the backup catalog


Backint System Copy

☐ Backint System Copy

Source System:



Stop Database TENANT2@SM1

 The database must be offline before recovery can start; the database will be stopped now

All'interno del catalogo di backup, il backup ripristinato viene evidenziato con un'icona verde. L'ID del backup esterno mostra il nome del backup precedentemente selezionato in SnapCenter.

12. Selezionare la voce con l'icona verde e fare clic su Next (Avanti).

Recovery of Tenant Database in SM1

Select a Backup

Select a backup to recover the SAP HANA database

Selected Point in Time

Database will be recovered to its most recent state.

Backups

The overview shows backups that were recorded in the backup catalog as successful. The backup at the top is estimated to have the shortest recovery time.

Start Time	Location	Backup Prefix	A...
2019-12-05 22:28:24	/hana/data/SM1	SNAPSHOT	●
2019-12-05 18:28:24	/hana/data/SM1	SNAPSHOT	✖
2019-12-05 14:28:23	/hana/data/SM1	SNAPSHOT	✖
2019-12-05 10:28:24	/hana/data/SM1	SNAPSHOT	✖
2019-12-05 06:28:23	/hana/data/SM1	SNAPSHOT	✖
2019-12-05 02:28:23	/hana/data/SM1	SNAPSHOT	✖
2019-12-04 22:28:24	/hana/data/SM1	SNAPSHOT	✖
2019-12-04 18:28:23	/hana/data/SM1	SNAPSHOT	✖
2019-12-04 14:28:25	/hana/data/SM1	SNAPSHOT	✖
2019-12-04 10:28:24	/hana/data/SM1	SNAPSHOT	✖

Refresh
Show More

Details of Selected Item

Start Time:
2019-12-05 22:28:24

Destination Type:
SNAPSHOT

Source System:
TENANT2@SM1

Size:
0 B

Backup ID:
1575613704345

External Backup ID:
SnapCenter_LocalSnap_Hourly_12-05-2019_22.28.01.2445

Backup Name:
/hana/data/SM1

Alternative Location:

Check Availability

?

< Back
Next >
Finish
Cancel

13. Fornire la posizione di backup del registro.

Recovery of Tenant Database in SM1

Locate Log Backups

Specify location(s) of log backup files to be used to recover the database.

i Even if no log backups were created, a location is still needed to read data that will be used for recovery.

If the log backups were written to the file system and subsequently moved, you need to specify their current location. If you do not specify an alternative location for the log backups, the system uses the location where the log backups were first saved. The directory specified will be searched recursively.

Locations:

14. Selezionare le altre impostazioni desiderate.

Recovery of Tenant Database in SM1

Other Settings

Check Availability of Delta and Log Backups
You can have the system check whether all required delta and log backups are available at the beginning of the recovery process. If delta or log backups are missing, they will be listed and the recovery process will stop before any data is changed. If you choose not to perform this check now, it will still be performed but later. This may result in a significant loss of time if the complete recovery must be repeated.
Check the availability of delta and log backups:

☒ File System [?]
☐ Third-Party Backup Tool (Backint)

Initialize Log Area
If you do not want to recover log segments residing in the log area, select this option. After the recovery, the log entries will be deleted from the log area.


☐ Initialize Log Area [?]

Use Delta Backups
Select this option if you want to perform a recovery using delta backups. If you choose to perform a recovery without delta backups, only log backups will be used.

☒ Use Delta Backups (Recommended)

Install New License Key
If you recover the database from a different system, the old license key will no longer be valid
You can:
- Select a new license key to install now
- Install a new license key manually after the database has been recovered

☐ Install New License Key



15. Avviare l'operazione di ripristino del tenant.

Recovery of Tenant Database in SM1

Review Recovery Settings

Review the recovery settings and choose 'Finish' to start the recovery. You can modify the recovery settings by choosing 'Back'.

Database Information

Database:

TENANT2@SM1

Host:

hana-2

Version:

2.00.040.00.1553674765

Recovery Definition

Recovery Type:

Snapshot (Point-in-Time Recovery (Until Now))

Configuration File Handling

⚠ Caution

To recover customer-specific configuration changes, you may need to make the changes manually in the target system.
More Information: SAP HANA Administration Guide

Show SQL Statement

?

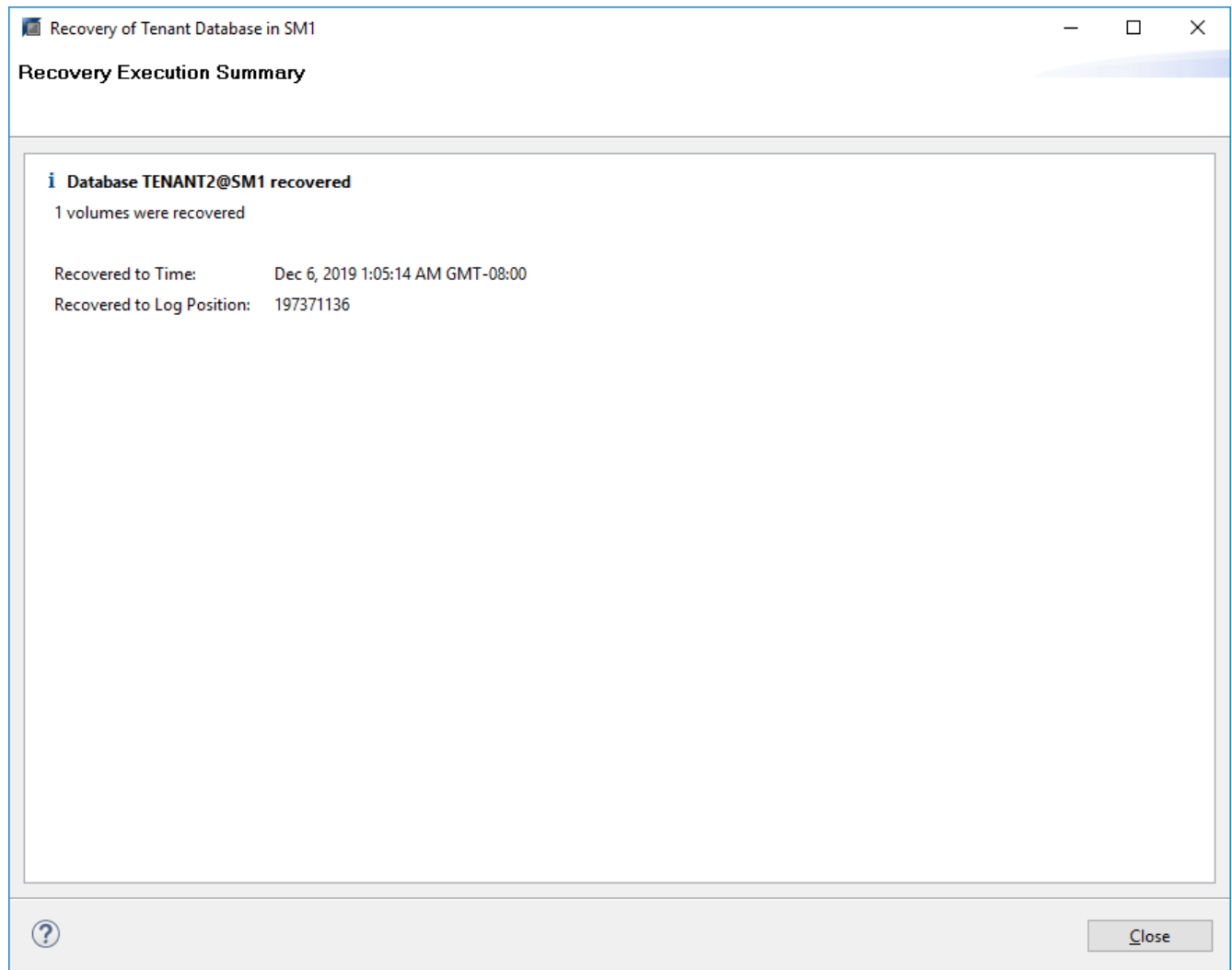
< Back

Next >

Finish

Cancel

177



Ripristino con ripristino manuale

Per ripristinare e ripristinare un sistema single-tenant SAP HANA MDC utilizzando SAP HANA Studio e SnapCenter, attenersi alla seguente procedura:

1. Preparare il processo di ripristino con SAP HANA Studio:
 - a. Selezionare Recover System Database (Ripristina database di sistema) e confermare l'arresto del sistema SAP HANA.
 - b. Selezionare il tipo di ripristino e la posizione di backup del registro.
 - c. Viene visualizzato l'elenco dei backup dei dati. Selezionare Backup per visualizzare l'ID del backup esterno.
2. Eseguire il processo di ripristino con SnapCenter:
 - a. Nella vista della topologia della risorsa, selezionare copie locali da ripristinare dallo storage primario o dalle copie del vault se si desidera eseguire il ripristino da uno storage di backup off-site.
 - b. Selezionare il backup SnapCenter che corrisponde all'ID di backup esterno o al campo del commento di SAP HANA Studio.
 - c. Avviare il processo di ripristino.



Se si sceglie un ripristino basato su volume dallo storage primario, i volumi di dati devono essere smontati da tutti gli host di database SAP HANA prima del ripristino e rimontati al termine del processo di ripristino.



In una configurazione di host multipli SAP HANA con FC, le operazioni di dismount e mount vengono eseguite dal name server SAP HANA come parte del processo di shutdown e startup del database.

3. Eseguire il processo di ripristino del database di sistema con SAP HANA Studio:

- Fare clic su Refresh (Aggiorna) dall'elenco dei backup e selezionare il backup disponibile per il ripristino (indicato da un'icona verde).
- Avviare il processo di ripristino. Al termine del processo di ripristino, viene avviato il database di sistema.

4. Eseguire il processo di ripristino del database tenant con SAP HANA Studio:

- Selezionare Recover tenant Database (Ripristina database tenant) e selezionare il tenant da ripristinare.
- Selezionare il tipo di ripristino e la posizione di backup del registro.

Viene visualizzato un elenco di backup dei dati. Poiché il volume di dati è già stato ripristinato, il backup del tenant viene indicato come disponibile (in verde).

- Selezionare questo backup e avviare il processo di ripristino. Al termine del processo di ripristino, il database del tenant viene avviato automaticamente.

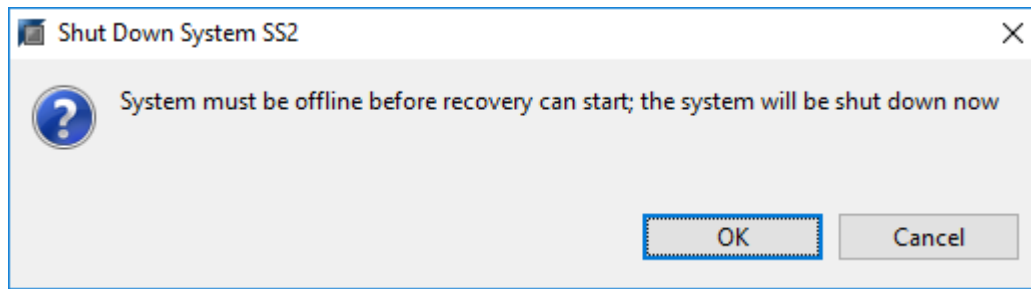
La sezione seguente descrive i passaggi delle operazioni di ripristino e ripristino del sistema HANA SS2 configurato manualmente (host singolo SAP HANA, sistema tenant multiplo MDC che utilizza NFS).

1. In SAP HANA Studio, selezionare l'opzione Recover System Database (Ripristina database di sistema) per avviare il ripristino del database di sistema.

The screenshot shows the SAP HANA Studio interface. The left pane displays a tree view of systems, including 'SYSTEMDB@SS1 (SYSTEM) SM1 - HANA20 SP54 MDC Multiple Tenants' and 'SYSTEMDB@SS2 (SYSTEM) SM1 - HANA20 SP54 MDC Single Tenant'. The right pane shows the 'Backup SYSTEMDB@SS1 (SYSTEM) SM1 - HANA20 SP54 MDC Multiple Tenants' window. The 'Processes' tab is active, displaying a table of running processes. The 'Configuration and Monitoring' menu is open, and the 'Backup and Recovery' option is selected, showing a sub-menu with 'Recover System Database...' and 'Recover Tenant Database...'.

Active	Host	Process	Description	Process ID	Status	Start Time	Elapsed Time
	hana-1	hdbcompilerver	HDB Compilerver	384	Running	Dec 10, 2019 6:34:00 AM	0:07:32
	hana-1	hdbdaemon	HDB Daemon	32375	Running	Dec 10, 2019 6:33:52 AM	0:07:40
	hana-1	hdbindexserver	HDB Indexserver-SS1	505	Running	Dec 10, 2019 6:34:01 AM	0:07:31
	hana-1	hdbnameserver	HDB Nameserver	32393	Running	Dec 10, 2019 6:33:53 AM	0:07:39
	hana-1	hdbpreprocessor	HDB Preprocessor	387	Running	Dec 10, 2019 6:34:00 AM	0:07:32
		jwebdispatcher	HDB Web Dispatcher	828	Running	Dec 10, 2019 6:34:16 AM	0:07:16
		xsengine	HDB XSEngine-SS1	510	Running	Dec 10, 2019 6:34:01 AM	0:07:31

2. Fare clic su OK per chiudere il database SAP HANA.



Il sistema SAP HANA si spegne e viene avviata la procedura guidata di ripristino.

3. Selezionare il tipo di ripristino e fare clic su Next (Avanti).


Recovery of SYSTEMDB@SS2


Specify Recovery Type

Select a recovery type.

☒ Recover the database to its most recent state ⁱ

☐ Recover the database to the following point in time ⁱ


Date: 2019-12-10  Time: 03:43:03

Select Time Zone: (GMT-08:00) Pacific Standard Time 

ⁱ System Time Used (GMT): 2019-12-10 11:43:03

☐ Recover the database to a specific data backup ⁱ

Advanced >>

 < Back Next > Finish Cancel

4. Fornire la posizione del catalogo di backup e fare clic su Next (Avanti).

Recovery of SYSTEMDB@SS2

Locate Backup Catalog

Specify location of the backup catalog.

☒ Recover using the backup catalog

☒ Search for the backup catalog in the file system only


Backup Catalog Location:

☐ Recover without the backup catalog

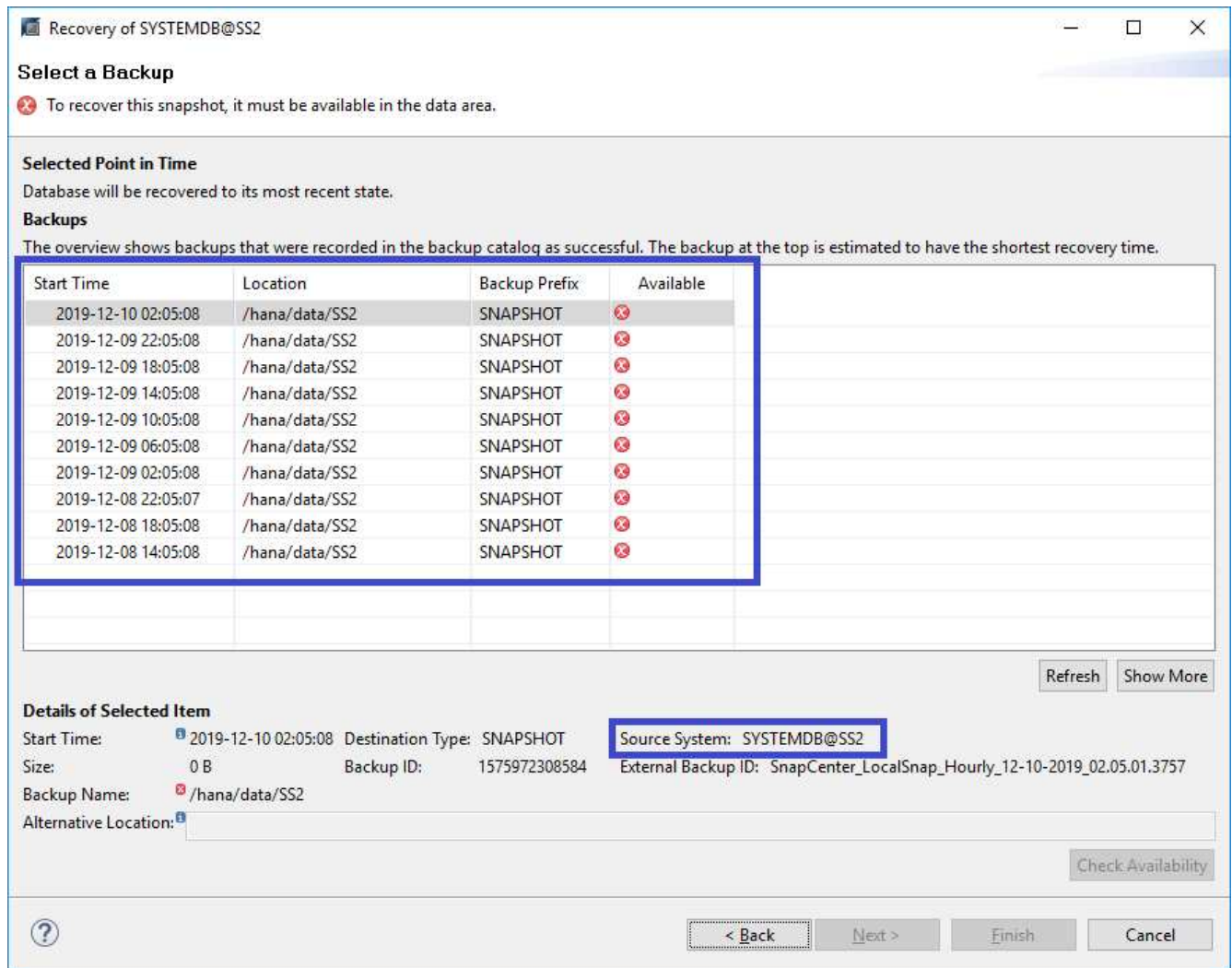
Backint System Copy

☐ Backint System Copy

Source System:



- Viene visualizzato un elenco dei backup disponibili in base al contenuto del catalogo di backup. Scegliere il backup richiesto e annotare l'ID del backup esterno: Nel nostro esempio, il backup più recente.



6. Smontare tutti i volumi di dati.

```
umount /hana/data/SS2/mnt00001
```



Per un sistema host SAP HANA multiplo con NFS, tutti i volumi di dati su ciascun host devono essere smontati.



In una configurazione di host multipli SAP HANA con FC, l'operazione di disinstallazione viene eseguita dal name server SAP HANA come parte del processo di arresto.

7. Dalla GUI di SnapCenter, selezionare la vista della topologia delle risorse e selezionare il backup da ripristinare; nel nostro esempio, il backup primario più recente. Fare clic sull'icona Restore (Ripristina) per avviare il ripristino.

SnapCenter®

SAP HANA

SS2 - HANA 20 SPS4 MDC Single Tenant Topology

Search databases

System

MS1 - Multiple Hosts MDC Single Tenant

SS2 - HANA 20 SPS4 MDC Single Tenant

SM1

SS1

Manage Copies

12 Backups

0 Clones

Local copies

Summary Card

14 Backups

12 Snapshot based backups

2 File-Based backups ✓

0 Clones

Primary Backup(s)

search

Backup Name	Count	if	End Date
SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757	1		12/10/2019 2:05:23 AM
SnapCenter_LocalSnap_Hourly_12-09-2019_22.05.01.3848	1		12/09/2019 10:05:23 PM
SnapCenter_LocalSnap_Hourly_12-09-2019_18.05.01.2909	1		12/09/2019 6:05:23 PM
SnapCenter_LocalSnap_Hourly_12-09-2019_14.05.01.3300	1		12/09/2019 2:05:23 PM
SnapCenter_LocalSnap_Hourly_12-09-2019_10.05.01.3143	1		12/09/2019 10:05:23 AM
SnapCenter_LocalSnap_Hourly_12-09-2019_06.05.01.6648	1		12/09/2019 6:05:23 AM
SnapCenter_LocalSnap_Hourly_12-09-2019_02.05.01.2792	1		12/09/2019 2:05:22 AM
SnapCenter_LocalSnap_Hourly_12-08-2019_22.05.01.1815	1		12/08/2019 10:05:22 PM
SnapCenter_LocalSnap_Hourly_12-08-2019_18.05.01.2784	1		12/08/2019 6:05:23 PM
SnapCenter_LocalSnap_Hourly_12-08-2019_14.05.01.2938	1		12/08/2019 2:05:23 PM
Total 4			
Total 12			

Activities

5 Completed 0 Warnings 0 Failed 0 Canceled 0 Running 0 Queued

Viene avviata la procedura guidata di ripristino di SnapCenter.

8. Selezionare il tipo di ripristino complete Resource (risorsa completa) o file Level (livello file).

Selezionare completa risorsa per utilizzare un ripristino basato su volume.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Select the restore types

☒ Complete Resource

☐ File Level

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

Previous Next

9. Selezionare livello file e tutto per utilizzare un'operazione SnapRestore a file singolo per tutti i file.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Select the restore types

☐ Complete Resource

☒ File Level

Select files to restore

Volume/Qtree	All	File Path
<input checked="" type="checkbox"/> hana-primary.sapcc.stl.netapp.com:/vol/SS...	<input checked="" type="checkbox"/>	<div>Provide one or more file paths separated by comma</div>

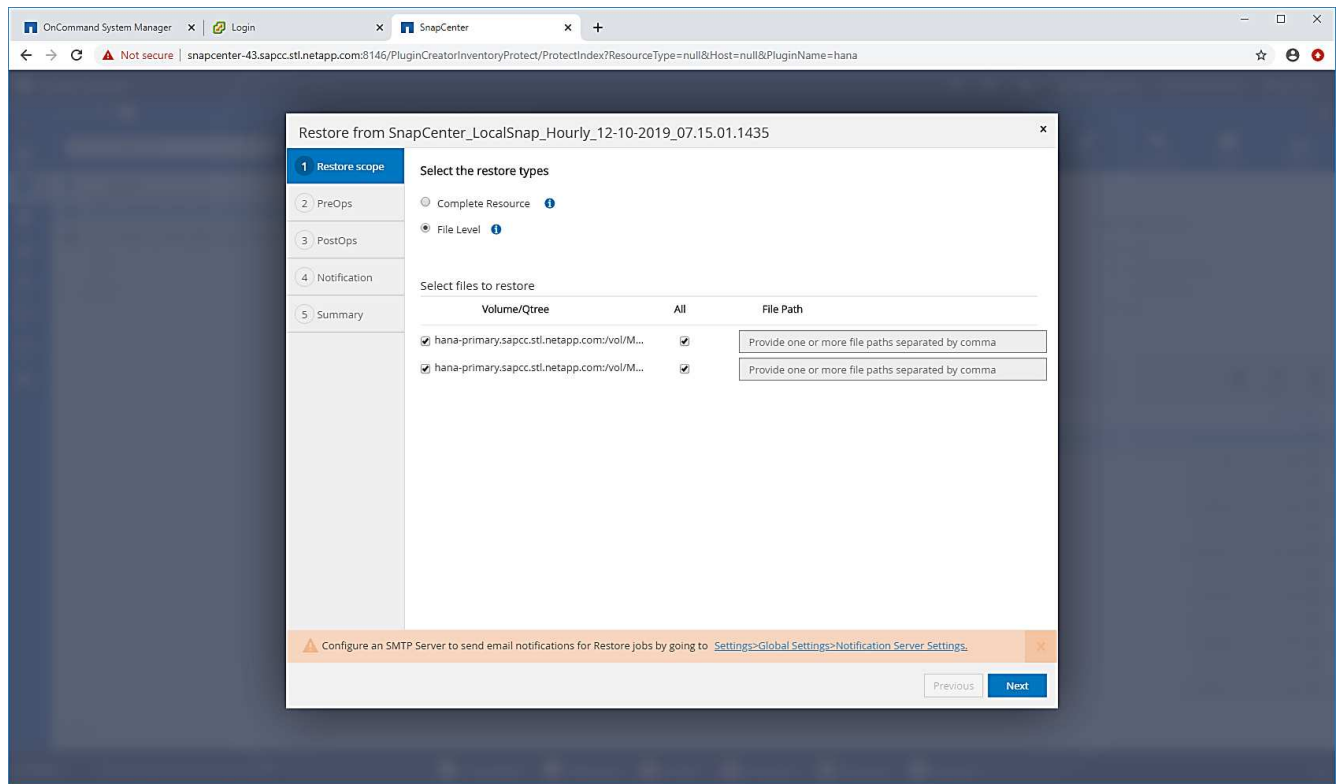
Configure an SMTP Server to send email notifications for Restore jobs by going to [Settings>Global Settings>Notification Server Settings.](#)

Previous

Next



Per un ripristino a livello di file di un sistema host multiplo SAP HANA, selezionare tutti i volumi.



10. (Facoltativo) specificare i comandi da eseguire dal plug-in SAP HANA in esecuzione sull'host del plug-in HANA centrale. Fare clic su Avanti.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Enter optional commands to run before performing a restore operation

Pre restore command

Unmount command

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

Previous Next

11. Specificare i comandi opzionali e fare clic su Next (Avanti).

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Enter optional commands to run after performing a restore operation

Mount command

Post restore command

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

Previous

Next

12. Specificare le impostazioni di notifica in modo che SnapCenter possa inviare un'e-mail di stato e un registro dei processi. Fare clic su Avanti.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Provide email settings ⓘ

Email preference

Never

From

Email from

To

Email to

Subject

Notification

☐ Attach Job Report

⚠

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

✕

Previous

Next

13. Esaminare il riepilogo e fare clic su Finish (fine) per avviare il ripristino.

Restore from SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757 ✕

1 Restore scope

2 PreOps

3 PostOps

4 Notification

5 Summary

Summary

Backup Name	SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757
Backup date	12/10/2019 2:05:23 AM
Restore scope	Complete Resource
Pre restore command	
Unmount command	
Mount command	
Post restore command	
Send email	No

⚠

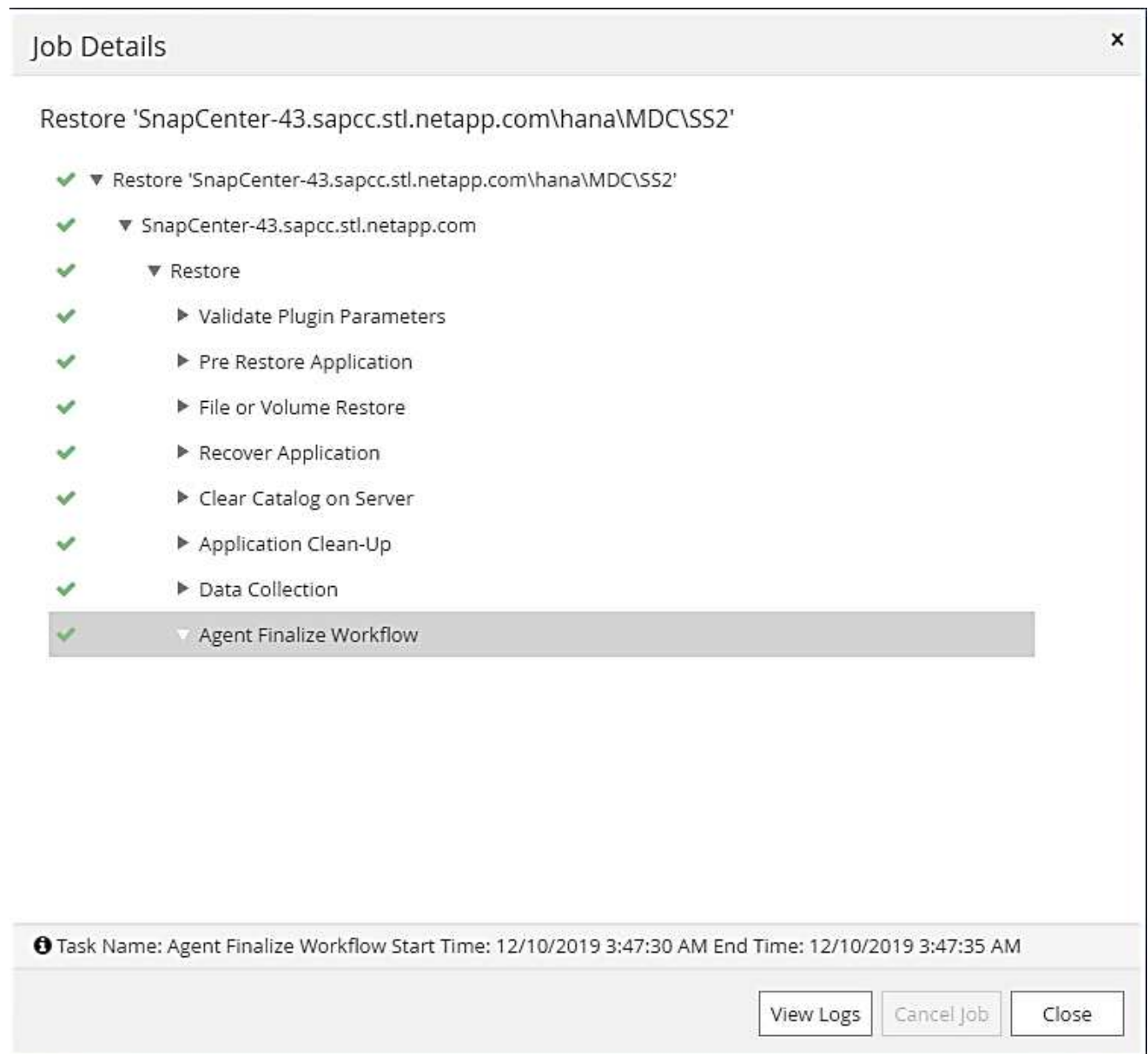
If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

✕

Previous

Finish

14. Il lavoro di ripristino viene avviato e il log dei lavori può essere visualizzato facendo doppio clic sulla riga del log nel riquadro delle attività.



15. Attendere il completamento del processo di ripristino. Su ciascun host di database, montare tutti i volumi di dati. Nel nostro esempio, è necessario rimontare un solo volume sull'host del database.

```
mount /hana/data/SP1/mnt00001
```

16. Accedere a SAP HANA Studio e fare clic su Refresh (Aggiorna) per aggiornare l'elenco dei backup disponibili. Il backup ripristinato con SnapCenter viene visualizzato con un'icona verde nell'elenco dei backup. Selezionare il backup e fare clic su Next (Avanti).

Recovery of SYSTEMDB@SS2

Select a Backup

Select a backup to recover the SAP HANA database

Selected Point in Time

Database will be recovered to its most recent state.

Backups

The overview shows backups that were recorded in the backup catalog as successful. The backup at the top is estimated to have the shortest recovery time.

Start Time	Location	Backup Prefix	Available
2019-12-10 02:05:08	/hana/data/SS2	SNAPSHOT	●
2019-12-09 22:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 18:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 14:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 10:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 06:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-09 02:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-08 22:05:07	/hana/data/SS2	SNAPSHOT	✗
2019-12-08 18:05:08	/hana/data/SS2	SNAPSHOT	✗
2019-12-08 14:05:08	/hana/data/SS2	SNAPSHOT	✗

Refresh
Show More

Details of Selected Item

Start Time:

2019-12-10 02:05:08

Destination Type:

SNAPSHOT

Source System:

SYSTEMDB@SS2

Size:

0 B

Backup ID:

1575972308584

External Backup ID:

SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

Backup Name:

/hana/data/SS2

Alternative Location:

Check Availability

?

< Back

Next >

Finish

Cancel

17. Fornire la posizione dei backup del registro. Fare clic su Avanti.

Recovery of SYSTEMDB@SS2

Locate Log Backups

Specify location(s) of log backup files to be used to recover the database.

i Even if no log backups were created, a location is still needed to read data that will be used for recovery.

If the log backups were written to the file system and subsequently moved, you need to specify their current location. If you do not specify an alternative location for the log backups, the system uses the location where the log backups were first saved. The directory specified will be searched recursively.

Locations:

18. Selezionare le altre impostazioni desiderate. Assicurarsi che l'opzione Usa backup delta non sia selezionata. Fare clic su Avanti.

Recovery of SYSTEMDB@SS2

Other Settings


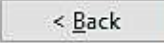
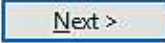

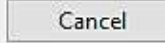
Check Availability of Delta and Log Backups
You can have the system check whether all required delta and log backups are available at the beginning of the recovery process. If delta or log backups are missing, they will be listed and the recovery process will stop before any data is changed. If you choose not to perform this check now, it will still be performed but later. This may result in a significant loss of time if the complete recovery must be repeated.
Check the availability of delta and log backups:
☒ File System [?]
☐ Third-Party Backup Tool (Backint)

Initialize Log Area
If you do not want to recover log segments residing in the log area, select this option. After the recovery, the log entries will be deleted from the log area.
☐ Initialize Log Area [?]

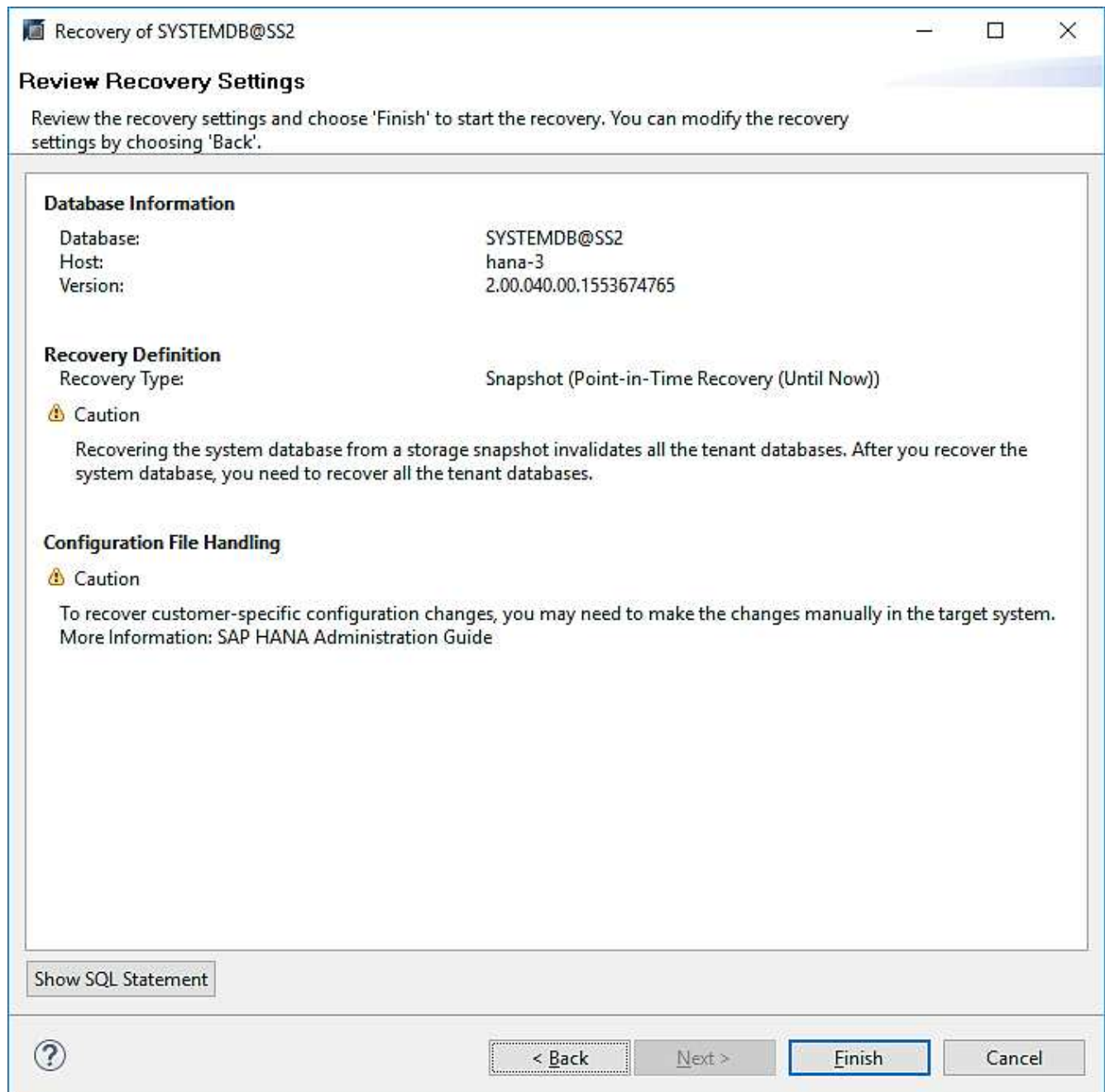
Use Delta Backups
Select this option if you want to perform a recovery using delta backups. If you choose to perform a recovery without delta backups, only log backups will be used.
☐ Use Delta Backups (Recommended)

Install New License Key
If you recover the database from a different system, the old license key will no longer be valid
You can:
- Select a new license key to install now
- Install a new license key manually after the database has been recovered
☐ Install New License Key

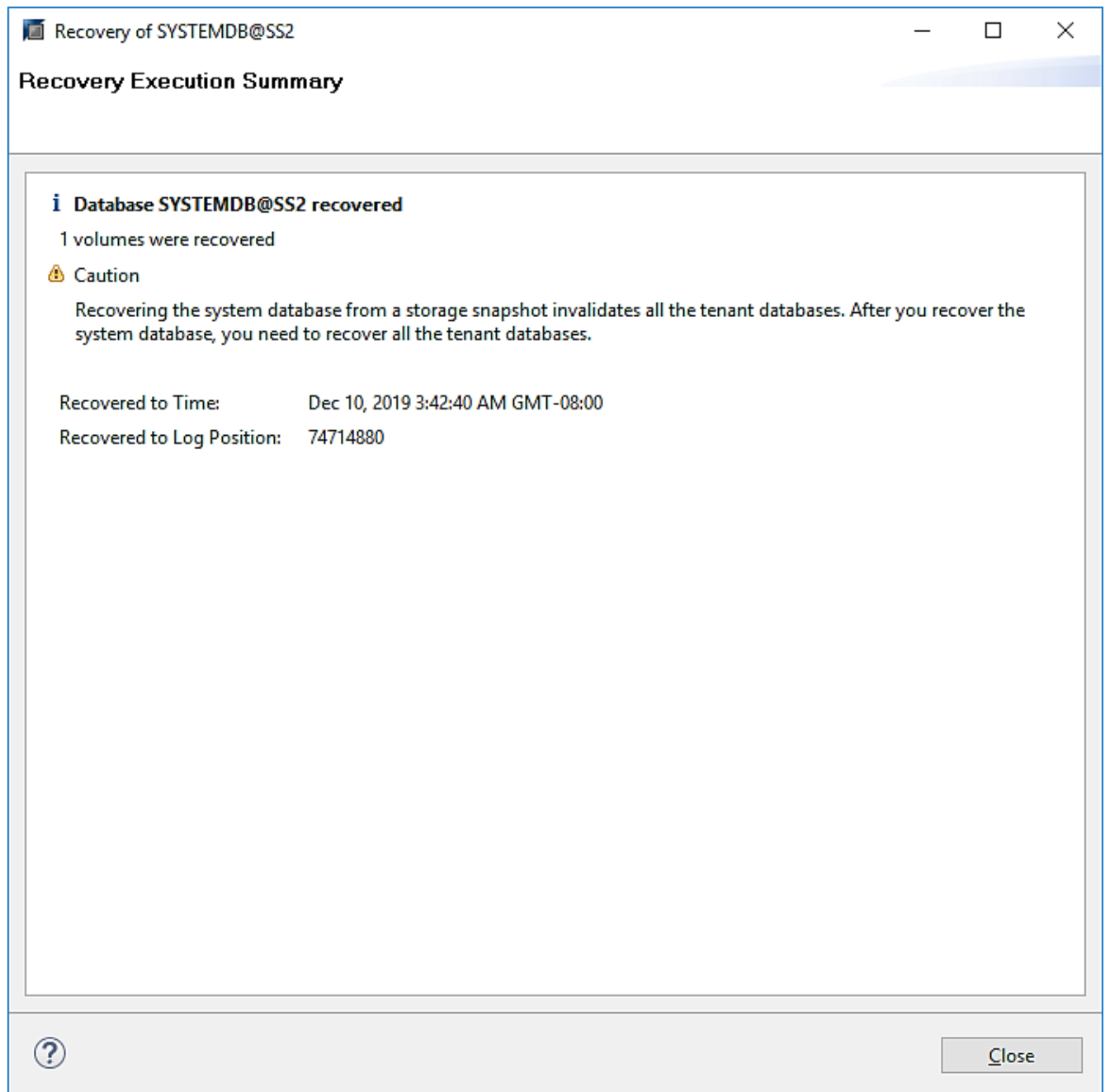
Browse

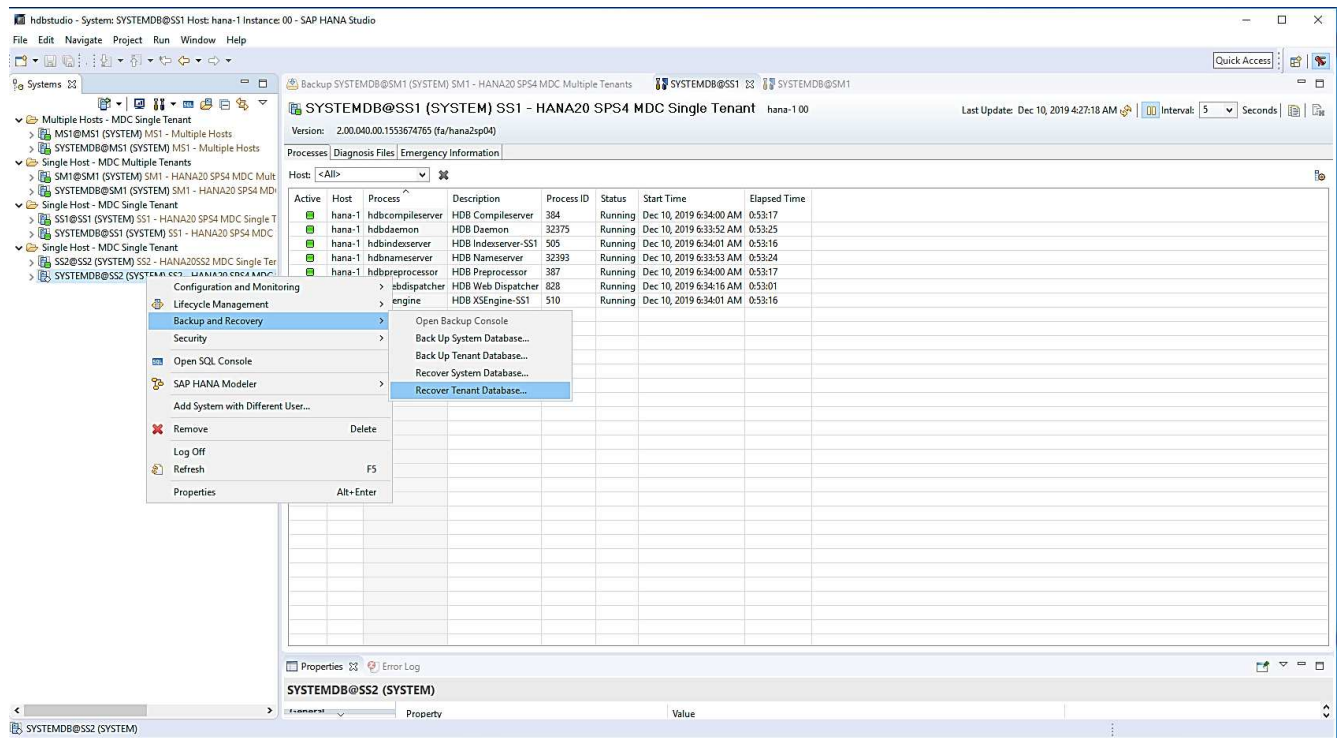
19. Rivedere le impostazioni di ripristino e fare clic su fine.



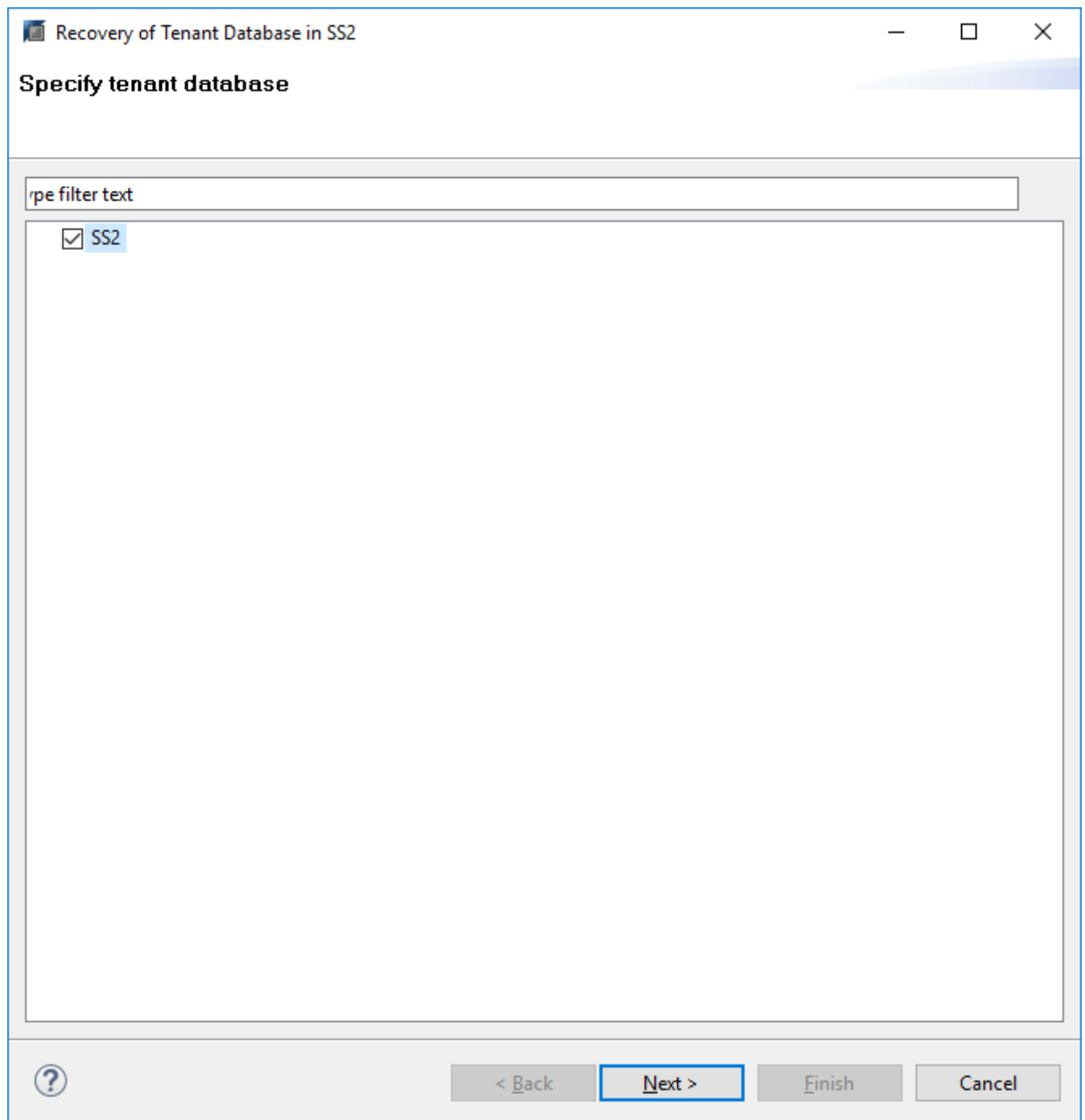
20. Viene avviato il processo di ripristino. Attendere il completamento del ripristino del database di sistema.



21. In SAP HANA Studio, selezionare la voce per il database di sistema e avviare Backup Recovery - Recover Tenant Database.



22. Selezionare il tenant da ripristinare e fare clic su Next (Avanti).



23. Specificare il tipo di ripristino e fare clic su Next (Avanti).


Recovery of Tenant Database in SS2


Specify Recovery Type

Select a recovery type.

☒ Recover the database to its most recent state ⁱ

☐ Recover the database to the following point in time ⁱ


Date:  Time:

Select Time Zone: 

ⁱ System Time Used (GMT): 2019-12-10 12:27:22

☐ Recover the database to a specific data backup ⁱ

[Advanced >>](#)

 [< Back](#) [Next >](#) [Finish](#) [Cancel](#)

24. Confermare la posizione del catalogo di backup e fare clic su Next (Avanti).

Recovery of Tenant Database in SS2

Locate Backup Catalog

Specify location of the backup catalog.

☒ Recover using the backup catalog

☒ Search for the backup catalog in the file system only


Backup Catalog Location:

☐ Recover without the backup catalog

Backint System Copy


☐ Backint System Copy

Source System:



25. Verificare che il database del tenant sia offline. Fare clic su OK per continuare.

Stop Database SS2@SS2

 The database must be offline before recovery can start; the database will be stopped now

26. Poiché il ripristino del volume di dati si è verificato prima del ripristino del database di sistema, il backup del tenant è immediatamente disponibile. Selezionare il backup evidenziato in verde e fare clic su Next

(Avanti).

Recovery of Tenant Database in SS2

Select a Backup

Select a backup to recover the SAP HANA database

Selected Point in Time

Database will be recovered to its most recent state.

Backups

The overview shows backups that were recorded in the backup catalog as successful. The backup at the top is estimated to have the shortest recovery time.

Start Time	Location	Backup Prefix	Available
2019-12-10 02:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-09 22:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-09 18:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-09 14:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-09 10:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-09 06:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-09 02:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-08 22:05:07	/hana/data/SS2	SNAPSHOT	
2019-12-08 18:05:08	/hana/data/SS2	SNAPSHOT	
2019-12-08 14:05:08	/hana/data/SS2	SNAPSHOT	

Refresh

Show More

Details of Selected Item

Start Time: 2019-12-10 02:05:08

Destination Type: SNAPSHOT

Source System: SS2@SS2

Size: 0 B

Backup ID: 1575972308585

External Backup ID: SnapCenter_LocalSnap_Hourly_12-10-2019_02.05.01.3757

Backup Name: /hana/data/SS2

Alternative Location:

Check Availability

?

< Back

Next >

Finish

Cancel

27. Confermare la posizione di backup del registro e fare clic su Next (Avanti).

Recovery of Tenant Database in SS2

Locate Log Backups

Specify location(s) of log backup files to be used to recover the database.

i Even if no log backups were created, a location is still needed to read data that will be used for recovery.

If the log backups were written to the file system and subsequently moved, you need to specify their current location. If you do not specify an alternative location for the log backups, the system uses the location where the log backups were first saved. The directory specified will be searched recursively.

Locations:

28. Selezionare le altre impostazioni desiderate. Assicurarsi che l'opzione Usa backup delta non sia selezionata. Fare clic su Avanti.

Recovery of Tenant Database in SS2

Other Settings

Check Availability of Delta and Log Backups

You can have the system check whether all required delta and log backups are available at the beginning of the recovery process. If delta or log backups are missing, they will be listed and the recovery process will stop before any data is changed. If you choose not to perform this check now, it will still be performed but later. This may result in a significant loss of time if the complete recovery must be repeated.

Check the availability of delta and log backups:

☒ File System ⁱ

☐ Third-Party Backup Tool (Backint)

Initialize Log Area

If you do not want to recover log segments residing in the log area, select this option. After the recovery, the log entries will be deleted from the log area.

☐ Initialize Log Area ⁱ

Use Delta Backups

Select this option if you want to perform a recovery using delta backups. If you choose to perform a recovery without delta backups, only log backups will be used.

☐ Use Delta Backups (Recommended) ⁱ

Install New License Key

If you recover the database from a different system, the old license key will no longer be valid

You can:

- Select a new license key to install now
- Install a new license key manually after the database has been recovered

☐ Install New License Key

Browse

? < Back Next > Finish Cancel

29. Esaminare le impostazioni di ripristino e avviare il processo di ripristino del database tenant facendo clic su Finish (fine).

Recovery of Tenant Database in SS2

Review Recovery Settings

Review the recovery settings and choose 'Finish' to start the recovery. You can modify the recovery settings by choosing 'Back'.

Database Information

Database:

SS2@SS2

Host:

hana-3

Version:

2.00.040.00.1553674765

Recovery Definition

Recovery Type:

Snapshot (Point-in-Time Recovery (Until Now))

Configuration File Handling

⚠ Caution

To recover customer-specific configuration changes, you may need to make the changes manually in the target system.

More Information: SAP HANA Administration Guide

Show SQL Statement

?

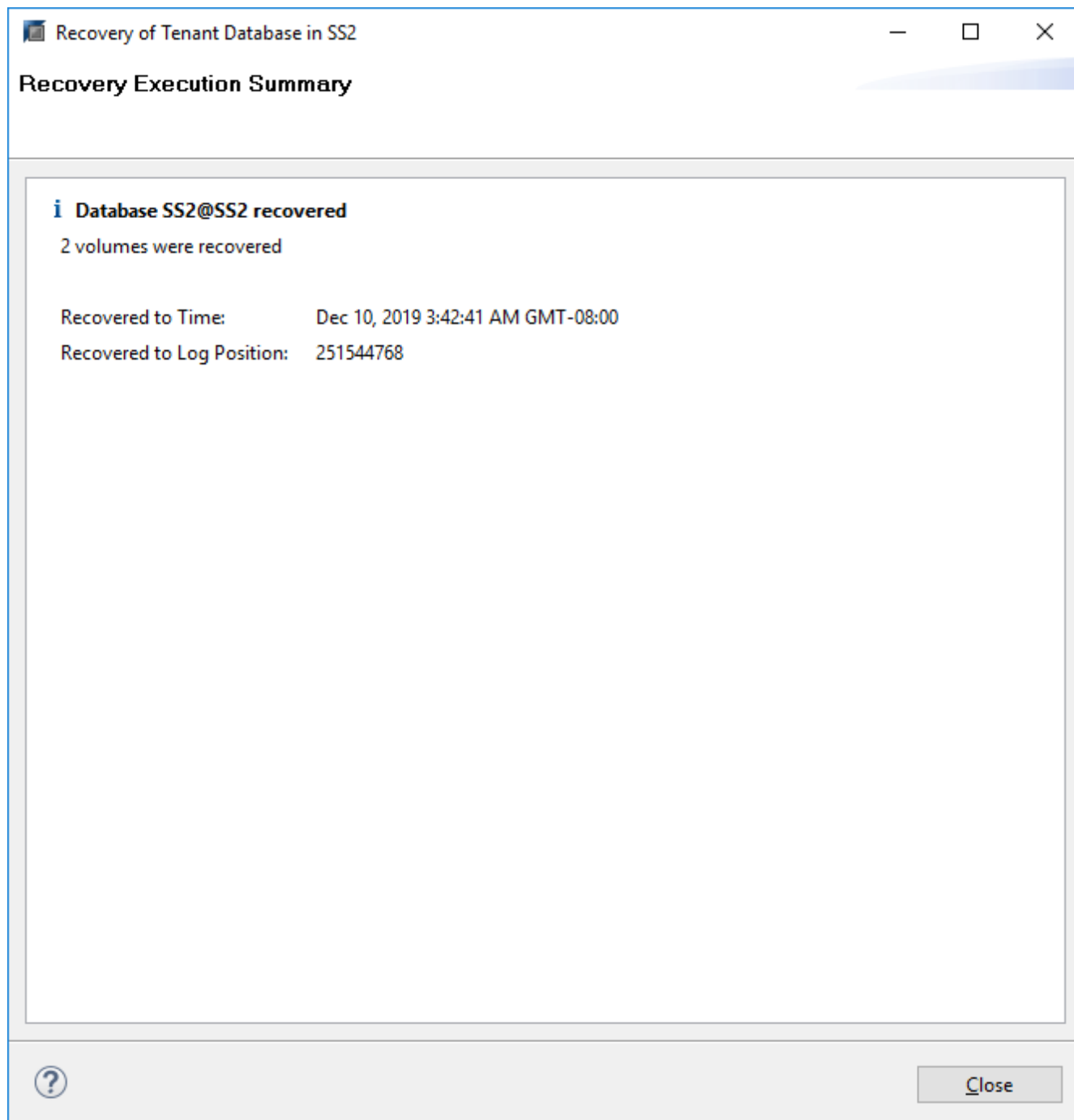
< Back

Next >

Finish

Cancel

30. Attendere il completamento del ripristino e l'avvio del database tenant.



Il sistema SAP HANA è operativo.



Per un sistema SAP HANA MDC con più tenant, è necessario ripetere i passaggi 20–29 per ciascun tenant.

Configurazione e tuning avanzati

Questa sezione descrive le opzioni di configurazione e messa a punto che i clienti possono utilizzare per adattare la configurazione di SnapCenter alle proprie esigenze specifiche. Non tutte le impostazioni possono essere valide per tutti gli scenari del cliente.

Abilitare la comunicazione sicura con il database HANA

Se i database HANA sono configurati con una comunicazione sicura, il `hdbsql` Il comando eseguito da SnapCenter deve utilizzare ulteriori opzioni della riga di comando. Ciò può essere ottenuto utilizzando uno script wrapper che richiama `hdbsql` con le opzioni richieste.



Sono disponibili varie opzioni per configurare la comunicazione SSL. Negli esempi seguenti, la configurazione del client più semplice viene descritta utilizzando l'opzione della riga di comando, in cui non viene eseguita alcuna convalida del certificato del server. Se è richiesta la convalida del certificato sul lato server e/o client, sono necessarie diverse opzioni della riga di comando `hdbsql` ed è necessario configurare l'ambiente PSE di conseguenza, come descritto nella SAP HANA Security Guide.

Invece di configurare `hdbsql` eseguibile in `hana.properties` viene aggiunto lo script wrapper.

Per un host plug-in HANA centrale sul server Windows di SnapCenter, è necessario aggiungere il seguente contenuto in `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\hana.properties`.

```
HANA_HDBSQL_CMD=C:\\Program Files\\sap\\hdbclient\\hdbsql-ssl.cmd
```

Lo script wrapper `hdbsql-ssl.cmd` chiamate `hdbsql.exe` con le opzioni della riga di comando richieste.

```
@echo off
"C:\Program Files\sap\hdbclient\hdbsql.exe" -e -ssltrustcert %*
```



Il `-e -ssltrustcert` L'opzione della riga di comando `hdbsql` funziona anche per i sistemi HANA in cui SSL non è abilitato. Questa opzione può quindi essere utilizzata anche con un host plug-in HANA centrale, in cui non tutti i sistemi HANA hanno abilitato o disabilitato SSL.

Se il plug-in HANA viene implementato su singoli host di database HANA, la configurazione deve essere eseguita su ciascun host Linux di conseguenza.

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

Lo script wrapper `hdbsqls` chiamate `hdbsql` con le opzioni della riga di comando richieste.

```
#!/bin/bash
/usr/sap/SM1/HDB12/exe/hdbsql -e -ssltrustcert $*
```

Disattivare la funzione di rilevamento automatico sull'host del plug-in HANA

Per disattivare il rilevamento automatico sull'host del plug-in HANA, attenersi alla seguente procedura:

1. Sul server SnapCenter, aprire PowerShell. Connettersi al server SnapCenter eseguendo `Open-`

SmConnection e specificare il nome utente e la password nella finestra di accesso.

2. Per disattivare il rilevamento automatico, eseguire Set- SmConfigSettings comando.

Per un host HANA hana-2, il comando è il seguente:

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

3. Verificare la configurazione eseguendo Get- SmConfigSettings comando.

```
PS C:\Users\administrator.SAPCC> Get-SmConfigSettings -Agent -Hostname
hana-2 -key all
Key: CUSTOMPLUGINS_OPERATION_TIMEOUT_IN_MSEC           Value: 3600000
Details: Plug-in API operation Timeout
Key: CUSTOMPLUGINS_HOSTAGENT_TO_SERVER_TIMEOUT_IN_SEC  Value: 1800
Details: Web Service API Timeout
Key: CUSTOMPLUGINS_ALLOWED_CMDS                       Value: *;
Details: Allowed Host OS Commands
Key: DISABLE_AUTO_DISCOVERY                           Value: true
Details:
Key: PORT                                              Value: 8145
Details: Port for server communication
PS C:\Users\administrator.SAPCC>
```

La configurazione viene scritta nel file di configurazione dell'agente sull'host ed è ancora disponibile dopo un aggiornamento del plug-in con SnapCenter.

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

Disattivare l'housekeeping automatico del backup dei log

La gestione del backup dei log è attivata per impostazione predefinita e può essere disattivata a livello di host del plug-in HANA. Sono disponibili due opzioni per modificare queste impostazioni.

Modificare il file hana.property

Incluso il parametro LOG_CLEANUP_DISABLE = Y in hana.property Il file di configurazione disattiva il

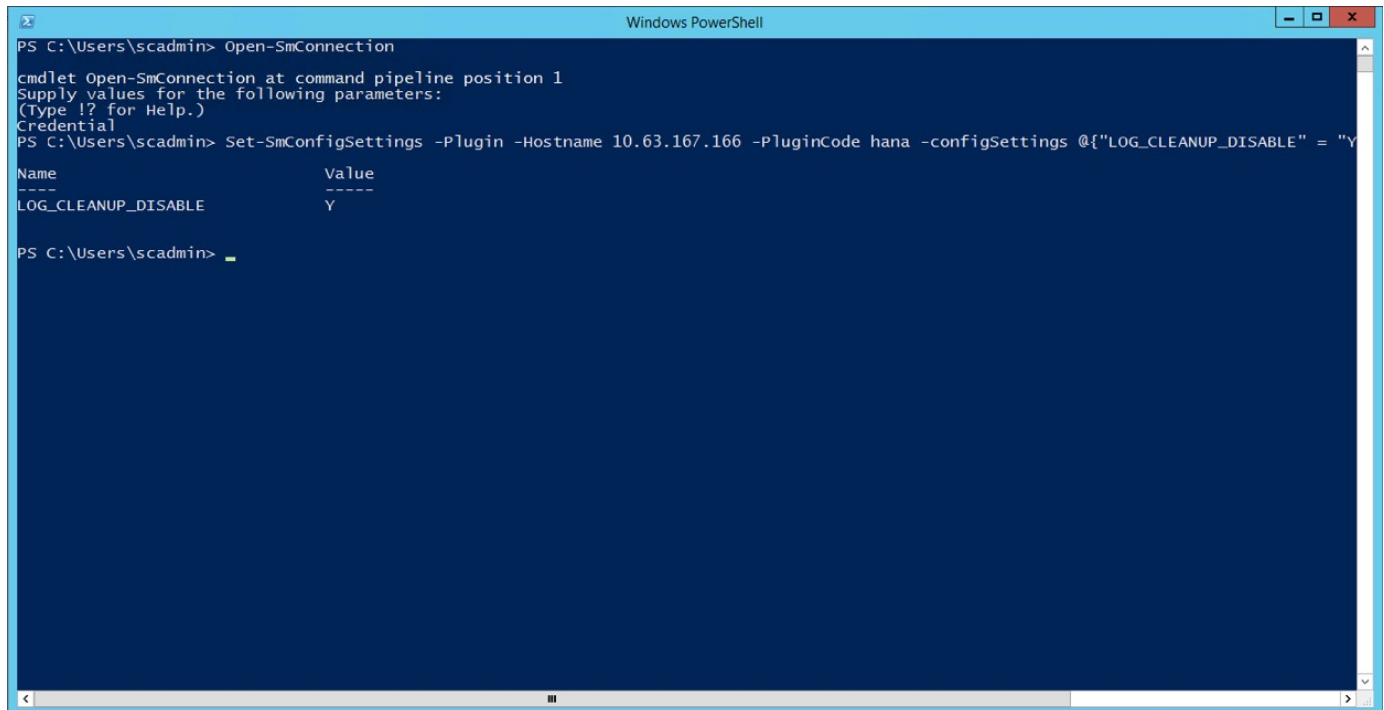
backup del log per tutte le risorse che utilizzano questo host plug-in SAP HANA come host di comunicazione:

- Per l'host di comunicazione Hdbsql su Windows, il `hana.property` il file si trova in `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc`.
- Per l'host di comunicazione Hdbsql su Linux, il `hana.property` il file si trova in `/opt/NetApp/snapcenter/scc/etc`.

Utilizzare il comando PowerShell

Una seconda opzione per configurare queste impostazioni consiste nell'utilizzare un comando PowerShell di SnapCenter.

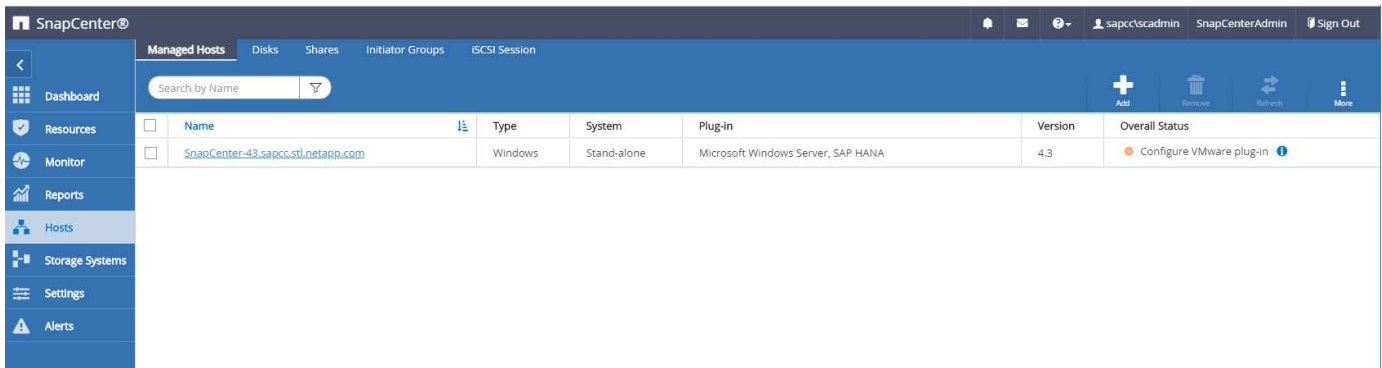
1. Sul server SnapCenter, aprire una PowerShell. Connettersi al server SnapCenter utilizzando il comando `Open-SmConnection` e specificare il nome utente e la password nella finestra di accesso aperta.
2. Con il comando `Set-SmConfigSettings -Plugin -HostName <pluginhostname> -PluginCode hana -configSettings @{"LOG_CLEANUP_DISABLE" = "Y"}`, Le modifiche vengono configurate per l'host plug-in SAP HANA <pluginhostname> Specificato dall'IP o dal nome host (vedere la figura seguente).



```
PS C:\Users\scadmin> Open-SmConnection
cmdlet Open-SmConnection at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
Credential
PS C:\Users\scadmin> Set-SmConfigSettings -Plugin -HostName 10.63.167.166 -PluginCode hana -configSettings @{"LOG_CLEANUP_DISABLE" = "Y"}
Name Value
----
LOG_CLEANUP_DISABLE Y
PS C:\Users\scadmin>
```

Disattiva l'avviso quando esegui il plug-in SAP HANA in un ambiente virtuale

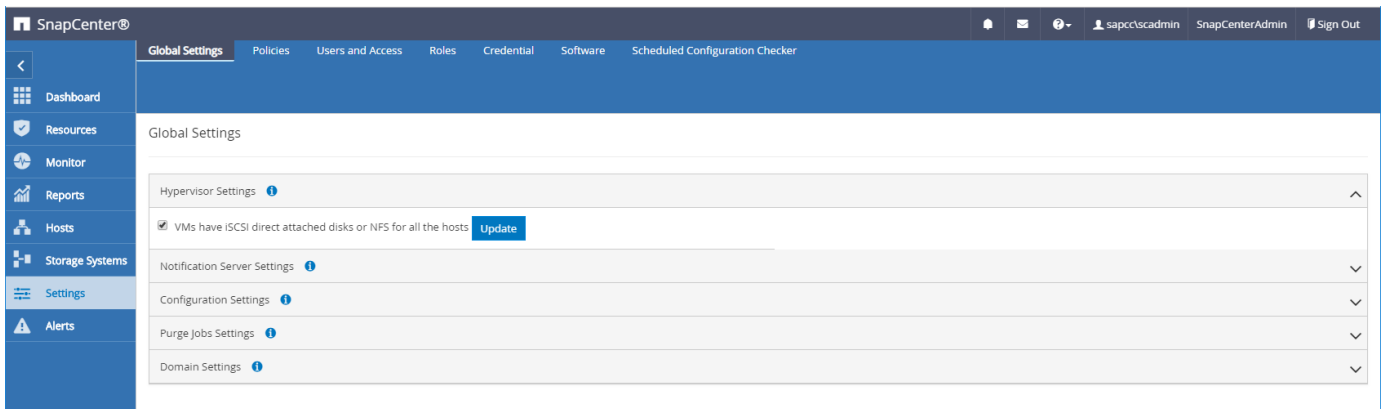
SnapCenter rileva se il plug-in SAP HANA è installato in un ambiente virtualizzato. Potrebbe trattarsi di un ambiente VMware o di un'installazione SnapCenter presso un provider di cloud pubblico. In questo caso, SnapCenter visualizza un avviso per la configurazione dell'hypervisor, come illustrato nella figura seguente.



È possibile eliminare questo avviso a livello globale. In questo caso, SnapCenter non è a conoscenza degli ambienti virtualizzati e, di conseguenza, non mostra questi avvisi.

Per configurare SnapCenter in modo da eliminare questo avviso, è necessario applicare la seguente configurazione:

1. Dalla scheda Settings (Impostazioni), selezionare Global Settings (Impostazioni globali).
2. Per le impostazioni dell'hypervisor, selezionare VM con iSCSI Direct Attached Disk o NFS per tutti gli host e aggiornare le impostazioni.



Modifica della frequenza di pianificazione della sincronizzazione del backup con lo storage di backup off-site

Come descritto nella sezione ["Gestione della conservazione dei backup nello storage secondario"](#), La gestione della conservazione dei backup dei dati in uno storage di backup off-site viene gestita da ONTAP. SnapCenter verifica periodicamente se ONTAP ha eliminato i backup nello storage di backup off-site eseguendo un processo di pulizia con una pianificazione predefinita settimanale.

Il processo di pulizia di SnapCenter elimina i backup nel repository SnapCenter e nel catalogo di backup SAP HANA se sono stati identificati backup cancellati nello storage di backup off-site.

Il processo di pulizia esegue anche la pulizia dei backup del registro SAP HANA.

Fino al termine della pulizia pianificata, SAP HANA e SnapCenter potrebbero ancora mostrare i backup che sono già stati eliminati dallo storage di backup off-site.

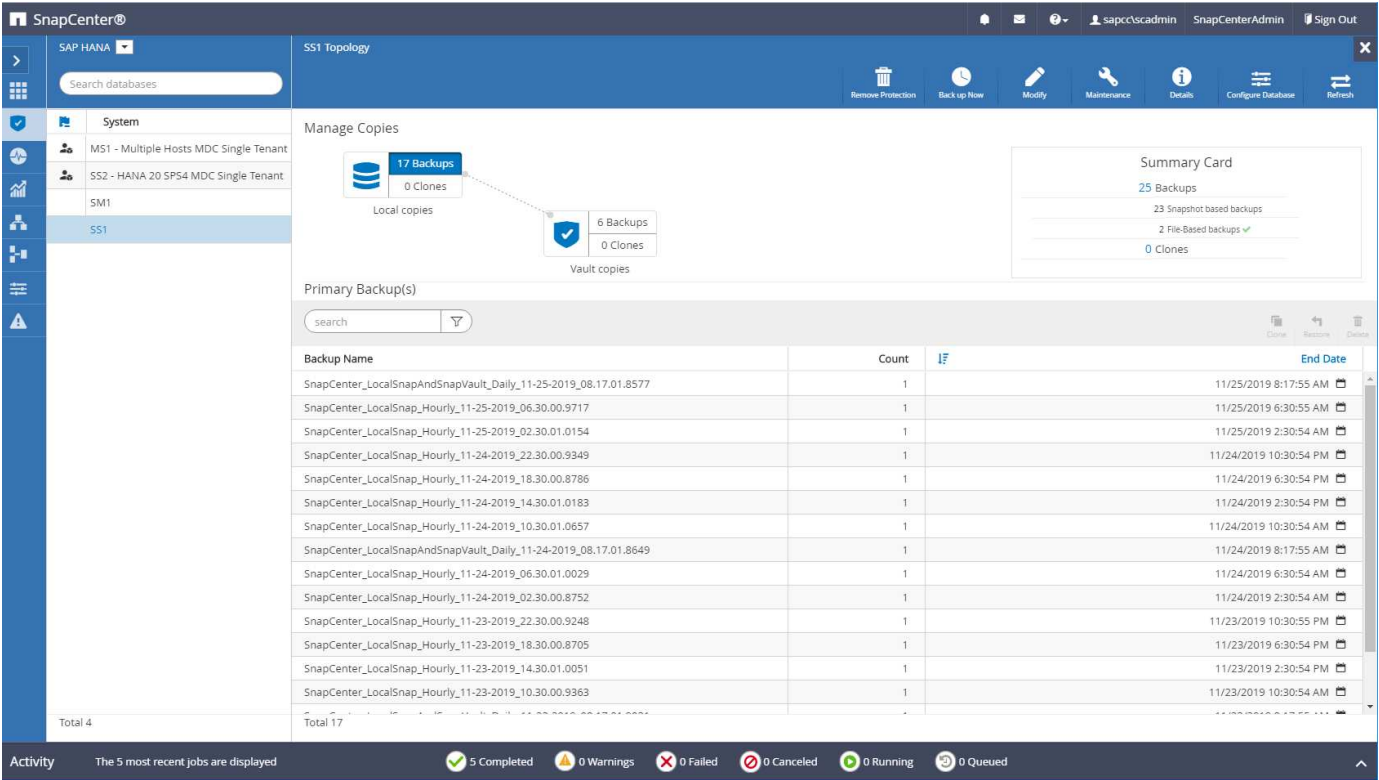


Ciò potrebbe comportare la conservazione di ulteriori backup dei log, anche se i backup Snapshot basati sullo storage corrispondenti sullo storage di backup off-site sono già stati eliminati.

Le sezioni seguenti descrivono due modi per evitare questa discrepanza temporanea.

Aggiornamento manuale a livello di risorse

Nella vista della topologia di una risorsa, SnapCenter visualizza i backup sullo storage di backup off-site quando si selezionano i backup secondari, come illustrato nella seguente schermata. SnapCenter esegue un'operazione di pulizia con l'icona Refresh (Aggiorna) per sincronizzare i backup di questa risorsa.



Modificare la frequenza del lavoro di pulizia SnapCenter

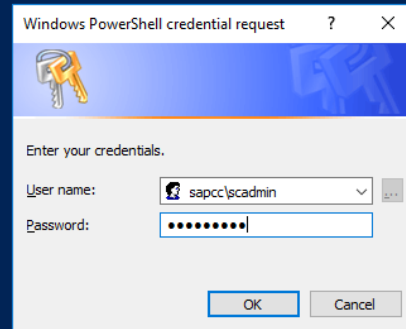
SnapCenter esegue il lavoro di pulizia SnapCenter_RemoveSecondaryBackup Per impostazione predefinita, per tutte le risorse su base settimanale utilizzando il meccanismo di pianificazione delle attività di Windows. È possibile modificarla utilizzando un cmdlet PowerShell di SnapCenter.

1. Avviare una finestra di comando PowerShell sul server SnapCenter.
2. Aprire la connessione al server SnapCenter e immettere le credenziali di amministratore SnapCenter nella finestra di accesso.

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\scadmin> Open-SmConnection

cmdlet Open-SmConnection at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
Credential
```



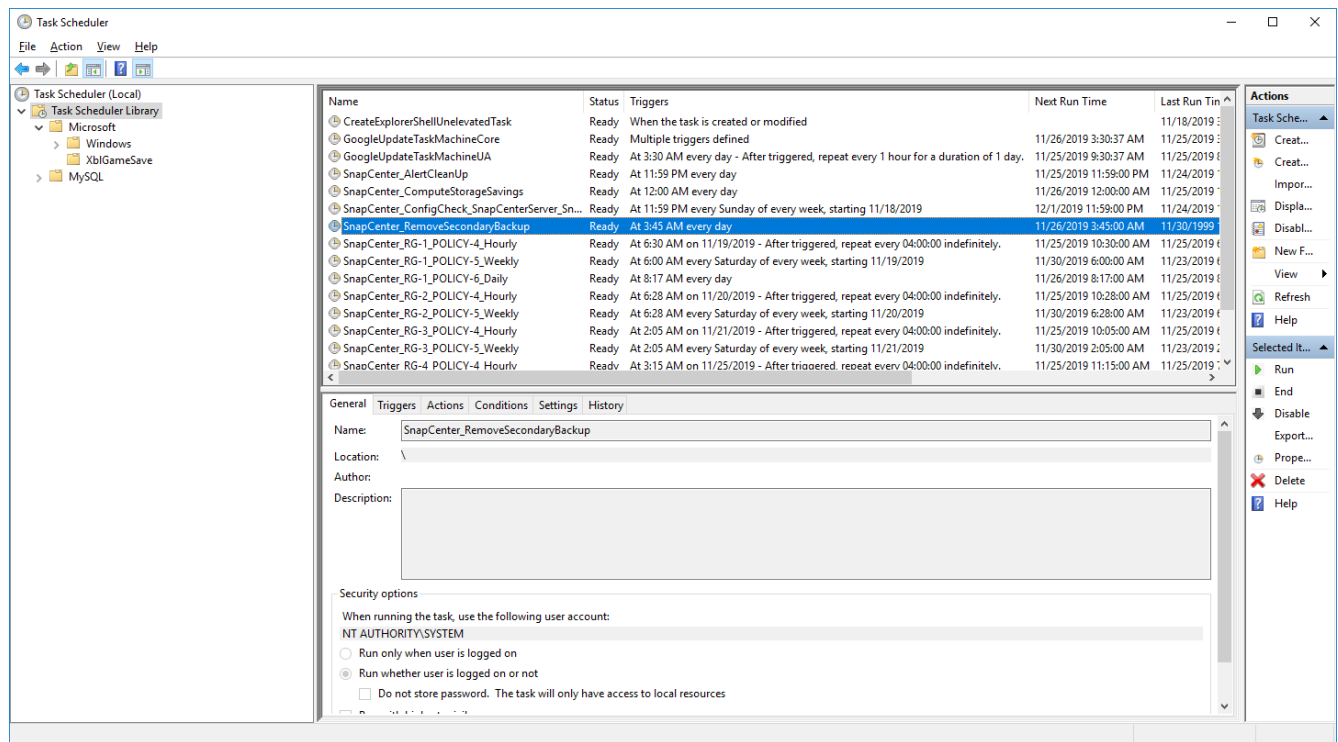
3. Per modificare la pianificazione da settimanale a giornaliera, utilizzare il cmdlet `Set-SmSchedule`.


```

PS C:\Users\scadmin> Set-SmSchedule -ScheduleInformation
@{"ScheduleType"="Daily";"StartTime"="03:45 AM";"DaysInterval"=
"1"} -TaskName SnapCenter_RemoveSecondaryBackup
TaskName                : SnapCenter_RemoveSecondaryBackup
Hosts                    : {}
StartTime                : 11/25/2019 3:45:00 AM
DaysOfTheMonth           :
MonthsOfTheYear          :
DaysInterval             : 1
DaysOfTheWeek            :
AllowDefaults            : False
ReplaceJobIfExist        : False
UserName                 :
Password                 :
SchedulerType            : Daily
RepeatTask_Every_Hour    :
IntervalDuration         :
EndTime                  :
LocalScheduler           : False
AppType                  : False
AuthMode                 :
SchedulerSQLInstance     : SMCoreContracts.SmObject
MonthlyFrequency         :
Hour                     : 0
Minute                   : 0
NodeName                 :
ScheduleID               : 0
RepeatTask_Every_Mins    :
CronExpression           :
CronOffsetInMinutes      :
StrStartTime             :
StrEndTime               :
PS C:\Users\scadmin> Check the configuration using the Windows Task
Scheduler.

```

4. È possibile controllare le proprietà del lavoro in Task Scheduler di Windows.



Dove trovare informazioni aggiuntive e cronologia delle versioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- Pagina delle risorse SnapCenter

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

- Documentazione software SnapCenter

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

- TR-4667: Automazione delle copie del sistema SAP con SnapCenter

<https://www.netapp.com/pdf.html?item=/media/17111-tr4667pdf.pdf>

- TR-4719: Replica, backup e ripristino del sistema SAP HANA con SnapCenter

<https://www.netapp.com/pdf.html?item=/media/17030-tr4719pdf.pdf>

- TR-4018: Integrazione dei sistemi NetApp ONTAP con la gestione del panorama SAP

<https://www.netapp.com/pdf.html?item=/media/17195-tr4018pdf.pdf>

- TR-4646: Disaster recovery SAP HANA con replica dello storage

<https://www.netapp.com/pdf.html?item=/media/8584-tr4646pdf.pdf>

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Luglio 2017	<ul style="list-style-type: none"> • Release iniziale.
Versione 1.1	Settembre 2017	<ul style="list-style-type: none"> • Aggiunta della sezione "Configurazione e ottimizzazione avanzate". • Correzioni minori.
Versione 2.0	Marzo 2018	<ul style="list-style-type: none"> • Aggiornamenti per SnapCenter 4,0: Nuova risorsa del volume di dati Miglioramento del funzionamento di Single file SnapRestore
Versione 3.0	Gennaio 2020	<ul style="list-style-type: none"> • Aggiunta la sezione "concetti e Best practice SnapCenter". • Aggiornamenti per SnapCenter 4,3: Rilevamento automatico Ripristino e ripristino automatici Supporto di tenant multipli HANA MDC Operazione di ripristino single-tenant
Versione 3.1	Luglio 2020	<ul style="list-style-type: none"> • Aggiornamenti e correzioni minori: Supporto NFSv4 con SnapCenter 4.3.1 Configurazione della comunicazione SSL Implementazione centralizzata dei plug-in per Linux su IBM Power
Versione 3.2	Novembre 2020	<ul style="list-style-type: none"> • Aggiunti i privilegi utente del database richiesti per HANA 2.0 SPS5.
Versione 3.3	Maggio 2021	<ul style="list-style-type: none"> • Aggiornata la sezione di configurazione di SSL hdbsql. • Supporto LVM Linux aggiunto.

Versione	Data	Cronologia delle versioni del documento
Versione 3.4	Agosto 2021	<ul style="list-style-type: none"> È stata aggiunta la descrizione della configurazione per la disattivazione del rilevamento automatico.
Versione 3.5	Febbraio 2022	<ul style="list-style-type: none"> Aggiornamenti minori per SnapCenter 4.6 e supporto del rilevamento automatico per i sistemi HANA abilitati alla replica del sistema HANA.

Backup e recovery di BlueXP per SAP HANA - Cloud object storage come destinazione di backup

Backup e recovery di BlueXP per SAP HANA - Cloud object storage come destinazione di backup

Panoramica

Questo documento descrive come configurare e configurare SAP HANA per la data Protection dagli archivi di oggetti on-premise a quelli basati sul cloud con NetApp BlueXP. Copre la parte di backup e recovery di BlueXP della soluzione. Questa soluzione è un miglioramento della soluzione di backup SAP HANA on-premise utilizzando NetApp Snap Center, che fornisce un metodo conveniente per l'archiviazione a lungo termine dei backup SAP HANA su storage a oggetti basato sul cloud e offre un tiering opzionale dello storage a oggetti verso storage di archiviazione come AWS Glacier/Deep Glacier, archiviazione BLOB di Microsoft Azure e archiviazione GCP.

Il setup e la configurazione della soluzione di backup e recovery SAP HANA on-premise sono descritti in "[TR-4614: Backup e recovery SAP HANA con SnapCenter \(netapp.com\)](#)".

Questo TR descrive solo come migliorare la soluzione di backup e recovery SAP HANA on-premise basata su SnapCenter con il backup e recovery di BlueXP per SAP HANA utilizzando ad esempio lo storage a oggetti AWS S3. Il setup e la configurazione che utilizzano lo storage a oggetti Microsoft Azure e GCP al posto di AWS S3 sono simili, ma non vengono descritti in questo documento.

Architettura di backup e recovery di BlueXP

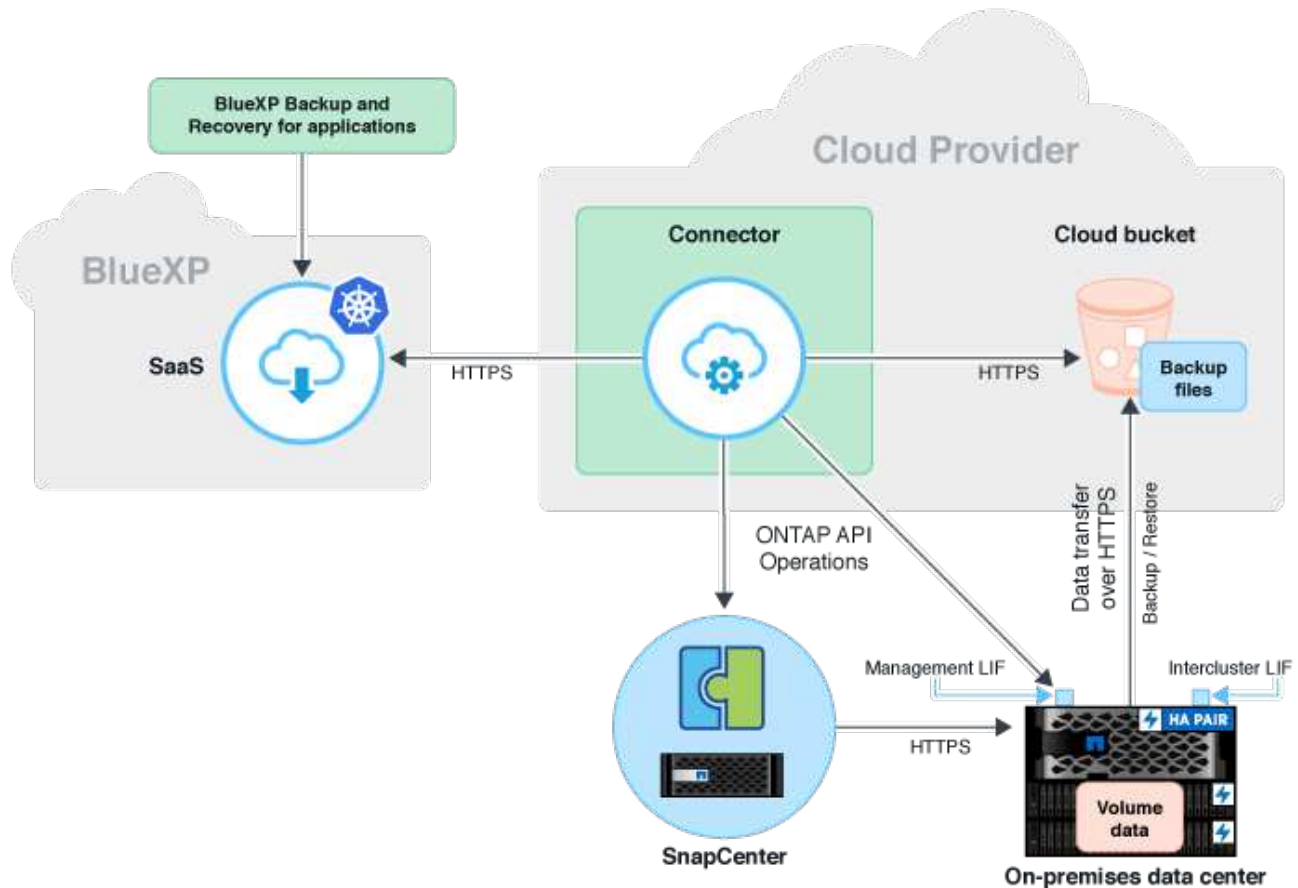
Il backup e recovery di BlueXP è una soluzione SaaS che offre funzionalità di data Protection per le applicazioni eseguite sullo storage on-premise NetApp nel cloud. Offre una protezione efficiente, coerente con l'applicazione e basata su policy di SAP HANA utilizzando lo storage NetApp. Inoltre, il backup e recovery di BlueXP offre controllo e supervisione centralizzati, delegando al contempo la possibilità per gli utenti di gestire le operazioni di backup e ripristino specifiche dell'applicazione.

Il backup e recovery di BlueXP viene eseguito come SaaS all'interno di NetApp BlueXP e sfrutta il framework e l'interfaccia utente. Il framework dell'ambiente di lavoro BlueXP viene utilizzato per configurare e gestire le credenziali per lo storage on-premise basato su NetApp ONTAP e per il server NetApp SnapCenter.

È necessario implementare un connettore BlueXP nella rete virtuale del cliente. È necessaria una connessione tra l'ambiente locale e l'ambiente cloud, ad esempio una connessione VPN da sito a sito. La comunicazione tra

i componenti SaaS di NetApp e l'ambiente del cliente avviene esclusivamente tramite il connettore. Il connettore sta eseguendo le operazioni di storage utilizzando le API di gestione di ONTAP e SnapCenter.

Il trasferimento dei dati tra lo storage on-premise e il bucket cloud è protetto end-to-end con crittografia AES a riposo a 256 bit, crittografia TLS/HTTPS in uso e supporto della chiave gestita dal cliente (CMK). I dati di backup vengono memorizzati in uno stato WORM immutabile e indelebile. L'unico modo per accedere ai dati dallo storage a oggetti è ripristinarli nello storage basato su NetApp ONTAP, incluso NetApp CVO.



Panoramica delle fasi di installazione e configurazione

Le fasi di installazione e configurazione richieste possono essere suddivise in tre aree.

Prerequisito: La configurazione del backup per SAP HANA è stata configurata in NetApp Snap Center. Per la configurazione di Snap Center per SAP HANA, il primo revisore al mondo "[Configurazione SnapCenter \(netapp.com\)](https://netapp.com)".

1. Installazione e configurazione dei componenti NetApp BlueXP.

Deve essere eseguita una volta durante la configurazione iniziale della soluzione per la protezione dei dati.

2. Fasi di preparazione in NetApp SnapCenter.

Occorre fare per ogni database SAP HANA, che deve essere protetto.

3. Passaggi di configurazione nel backup e recovery di BlueXP.

Occorre fare per ogni database SAP HANA, che deve essere protetto.

Installazione e configurazione del backup dell'applicazione ibrida NetApp BlueXP

L'installazione e la configurazione dei componenti NetApp BlueXP sono descritte nella "[Proteggi i dati delle applicazioni on-premise | documentazione NetApp](#)".

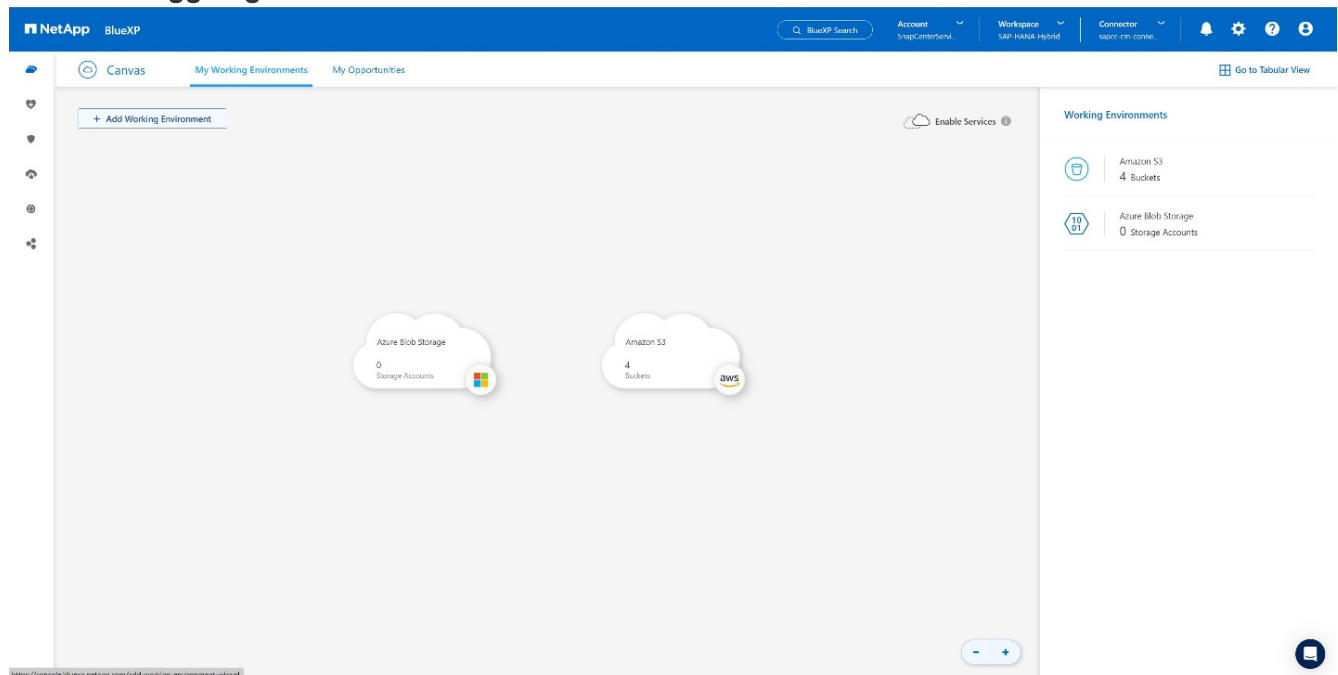
1. Registrati ad BlueXP e configura l'account NetApp all'indirizzo <https://bluexp.netapp.com/>.
2. Implementa il connettore BlueXP nel tuo ambiente. La descrizione è disponibile all'indirizzo "[Informazioni sui connettori | documentazione NetApp](#)".
3. Aggiungi/acquista una licenza Cloud Backup su BlueXP: <https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-licensing-cloud-backup.html>.
4. Crea un ambiente di lavoro per l'ambiente on-premise NetApp e la tua destinazione cloud in BlueXP aggiungendo lo storage on-premise.
5. Crea una nuova relazione di archivio di oggetti per lo storage on-premise in un bucket AWS S3.
6. Configura la risorsa di sistema SAP HANA su SnapCenter.
7. Aggiungi Snap Center al tuo ambiente di lavoro.
8. Creare una policy per il proprio ambiente.
9. Protezione del sistema SAP HANA.

Configurazione di BlueXP Backup and Recovery per SAP HANA

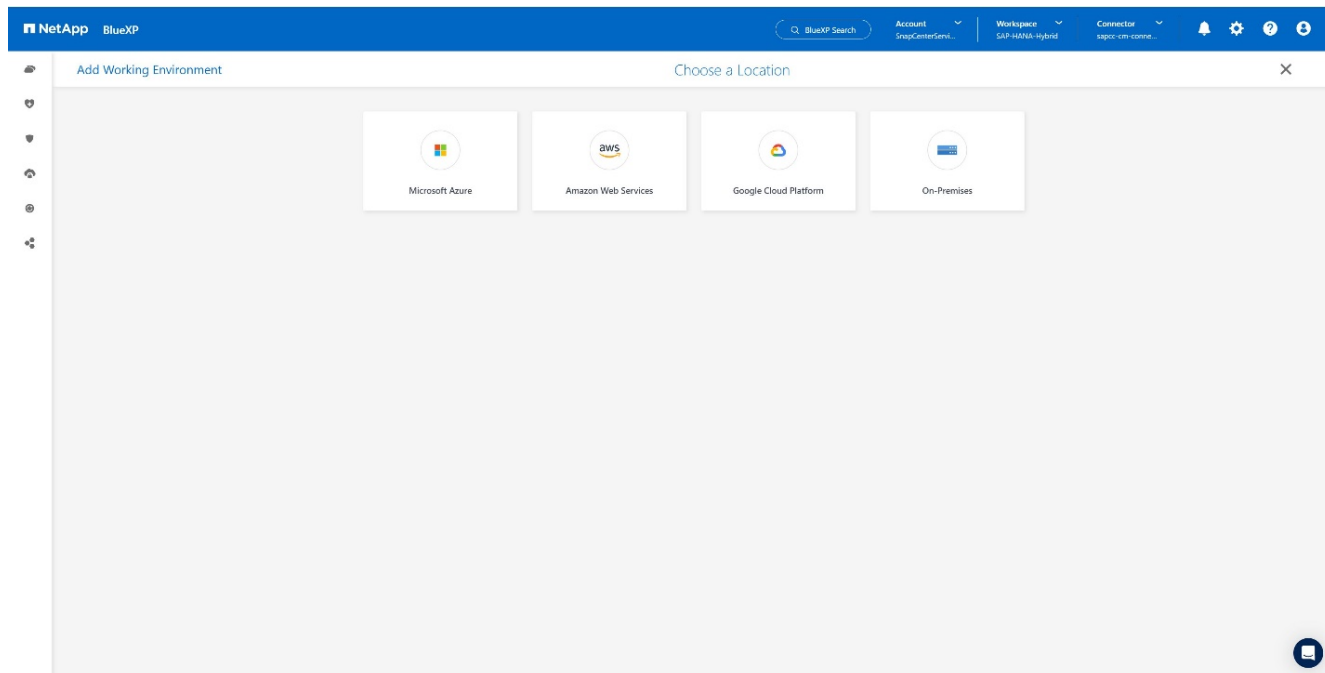
Crea un ambiente di lavoro per BlueXP

Aggiungi il sistema storage on-premise all'ambiente di lavoro.

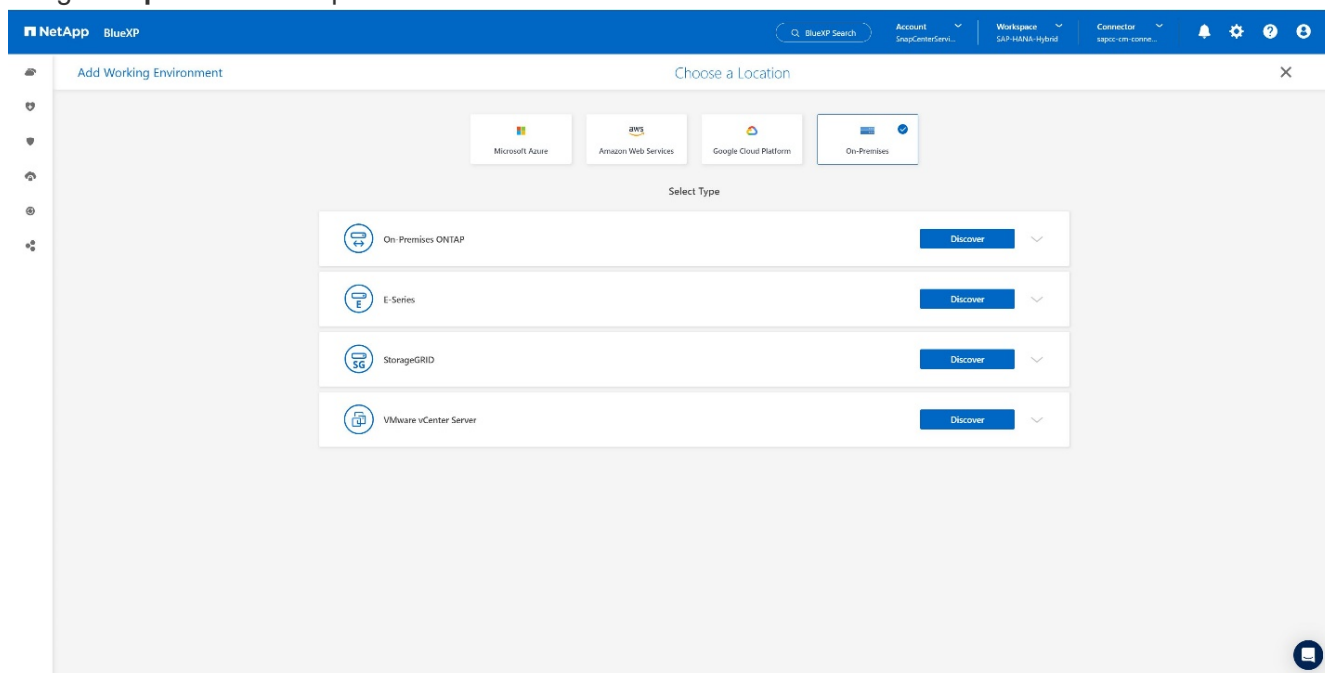
1. Nel menu a sinistra scegli **Storage** → **Canvas** → **My Working Environment**.
2. Premere **+ Aggiungi ambiente di lavoro**.



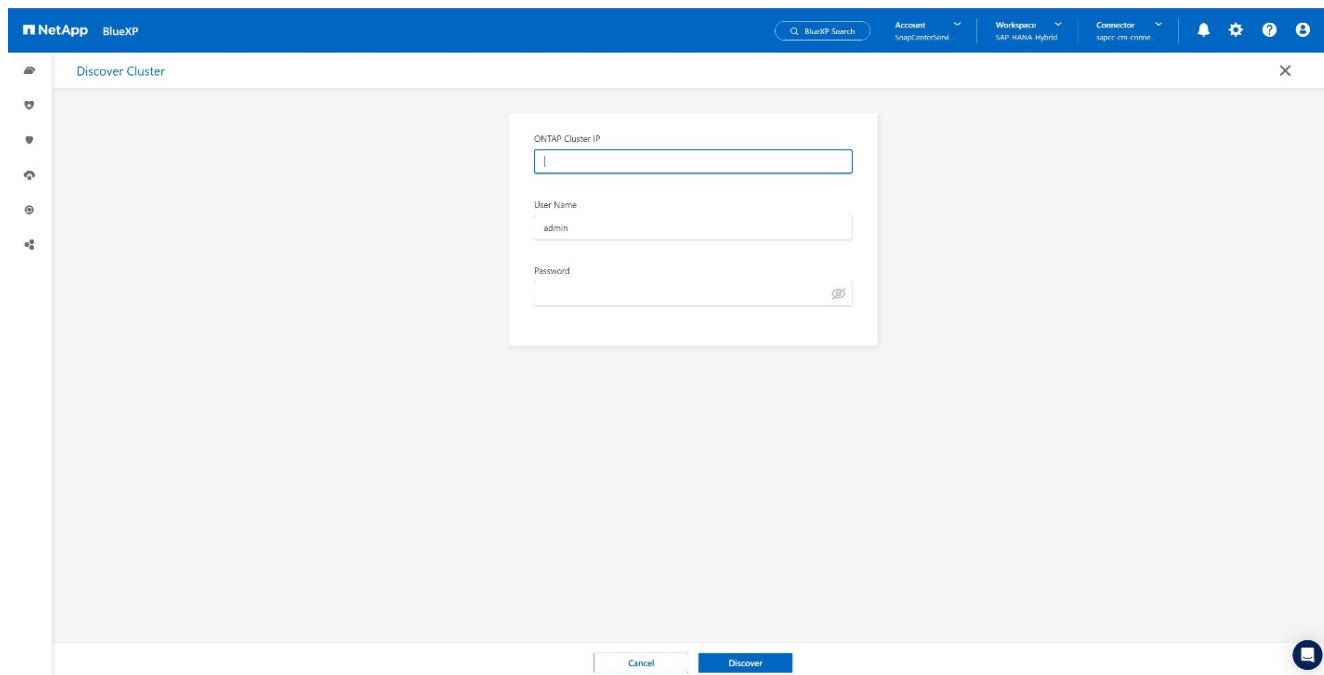
3. Scegliere **on-premise**.



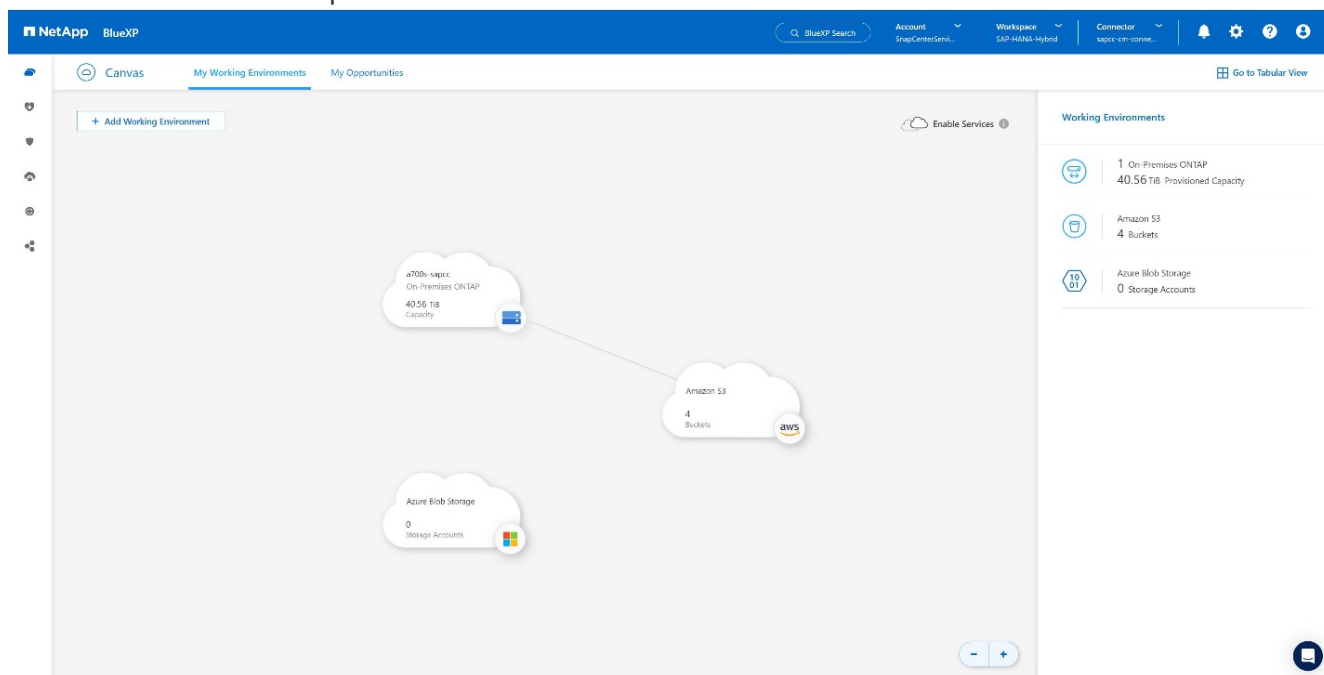
4. Scegli **Scopri ONTAP** on-premise.



5. Aggiungere l'indirizzo IP del cluster ONTAP e la password, quindi premere **Scopri**.



6. Il cluster ONTAP è ora disponibile.



Creare un rapporto tra il sistema storage on-premise e un bucket di storage a oggetti

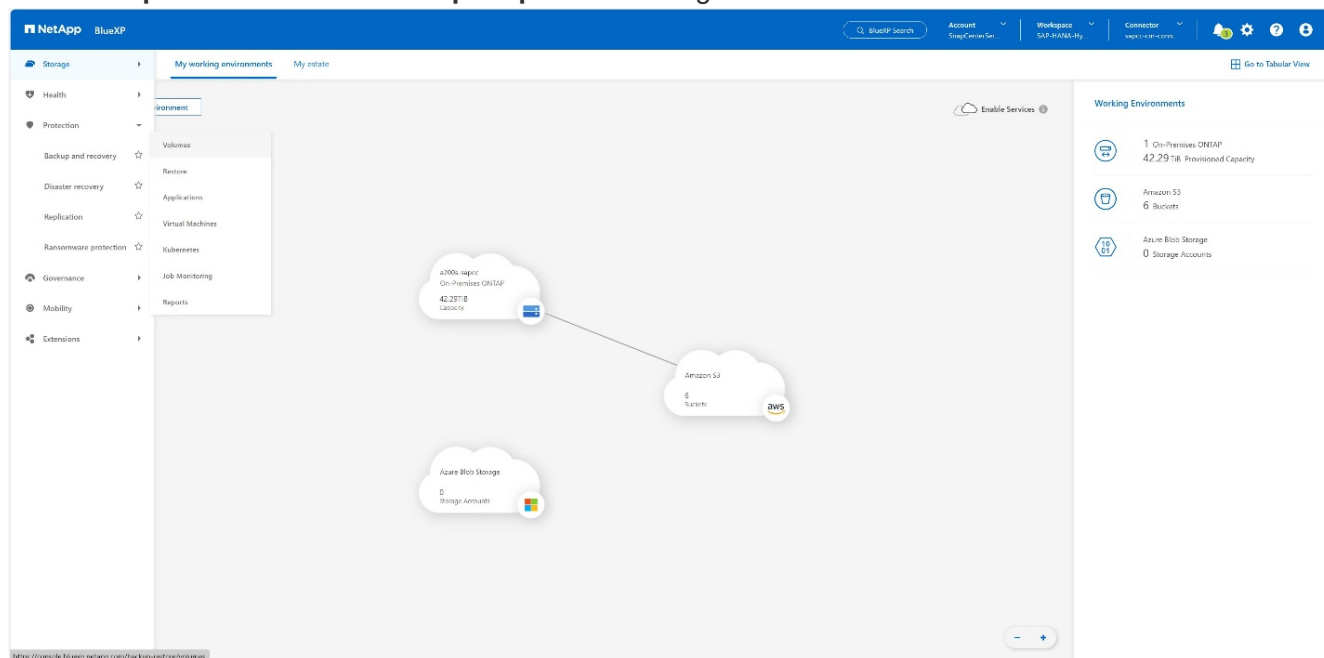
La relazione tra lo storage on-premise e il bucket S3 viene effettuata creando un backup per un volume o attivando un backup di un'applicazione. Se si deve utilizzare una VPN da sito a sito esistente per trasferire i dati da un sistema on-premise a S3, è necessario utilizzare un backup di volume per creare la relazione tra lo storage on-premise e il bucket S3 come endpoint VPC da utilizzare.

Al momento della creazione di questa documentazione, il flusso di lavoro di backup delle applicazioni non offre la possibilità di scegliere gli endpoint VPC per accedere ai bucket S3.

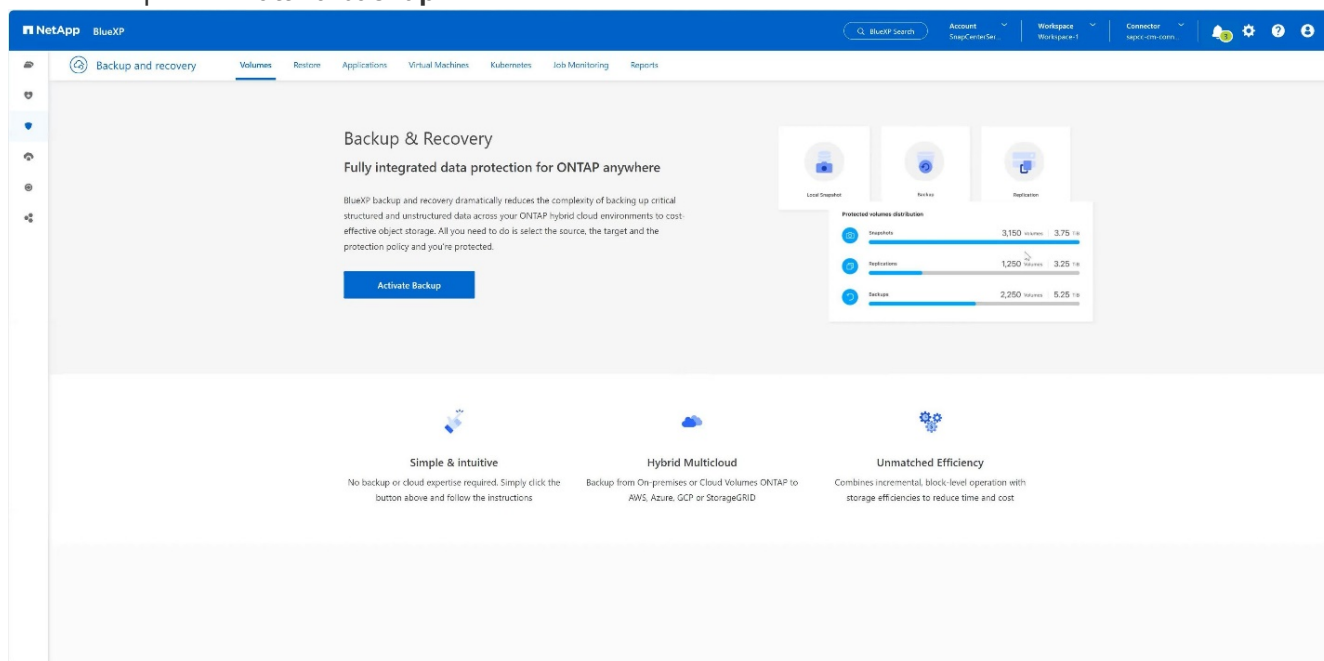
Fare riferimento a ["Endpoint del gateway per Amazon S3 - Amazon Virtual Private Cloud"](#) Come impostare gli endpoint VPC per S3 all'interno del VPC.

Per creare un backup del primo volume, attenersi alla seguente procedura:

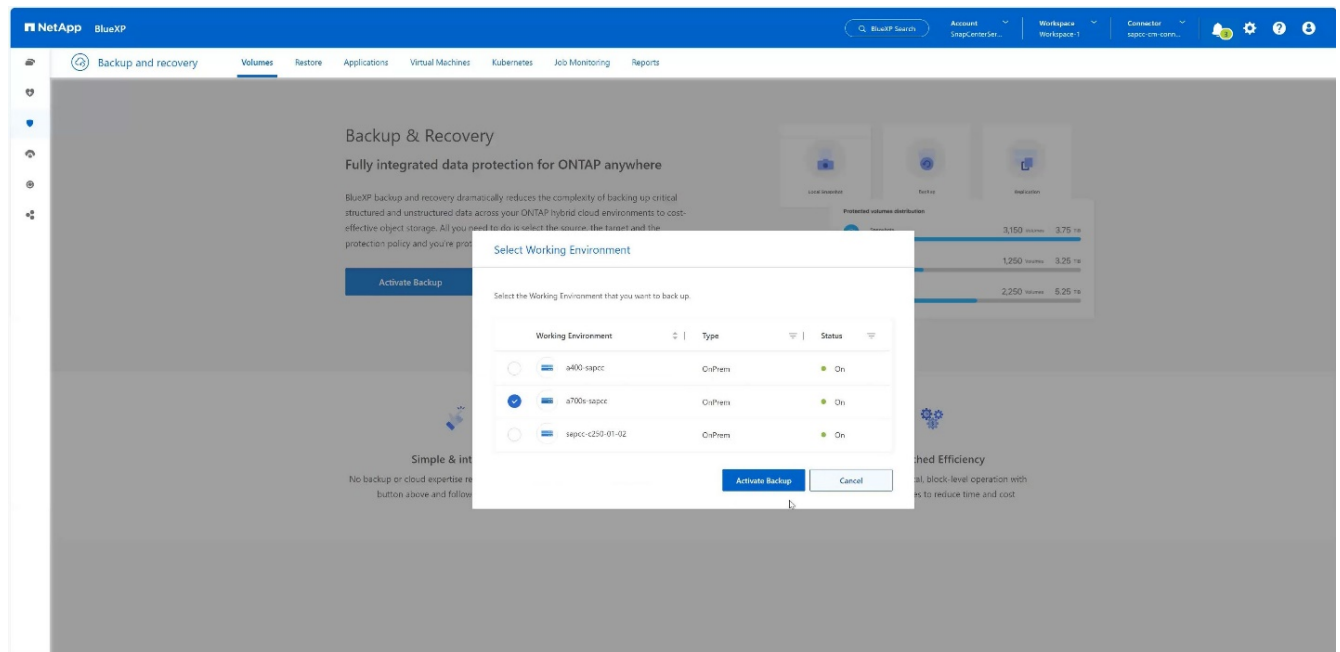
1. Passare a **protezione** fino a **Backup e ripristino** e scegliere volumi.



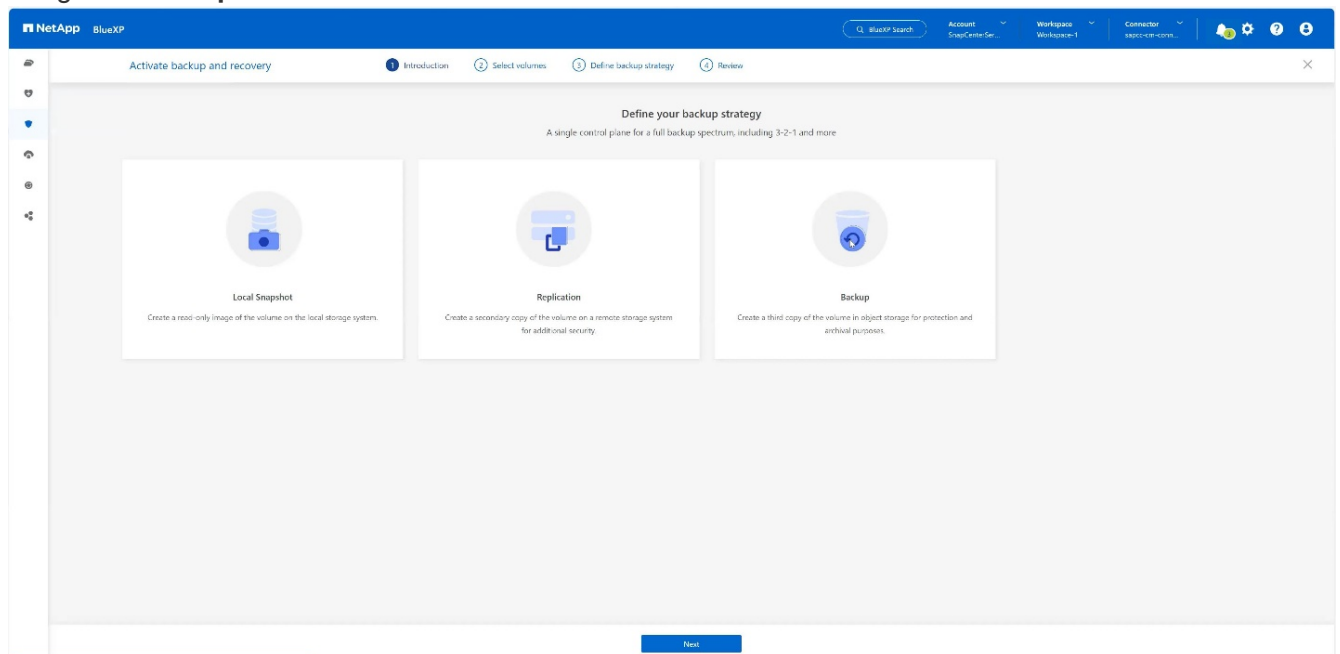
2. Premere il pulsante **attiva backup**.



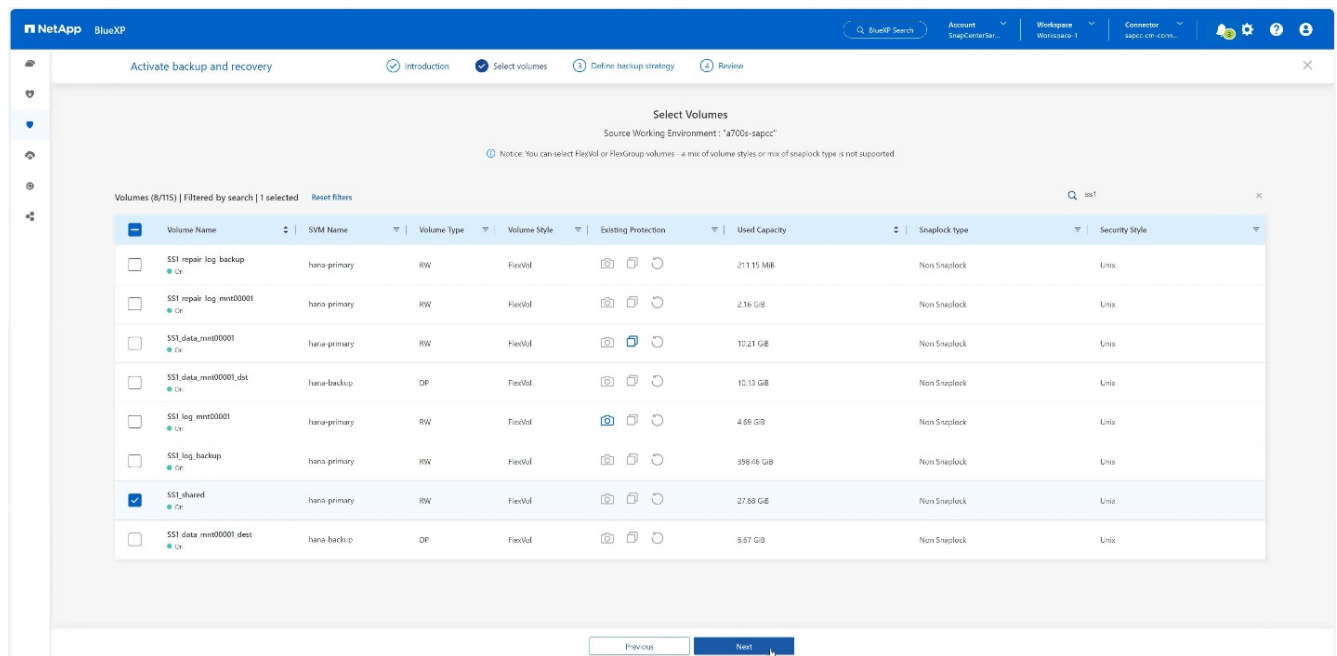
3. Scegli il sistema di storage on-premise desiderato e fai clic su **attiva backup**.



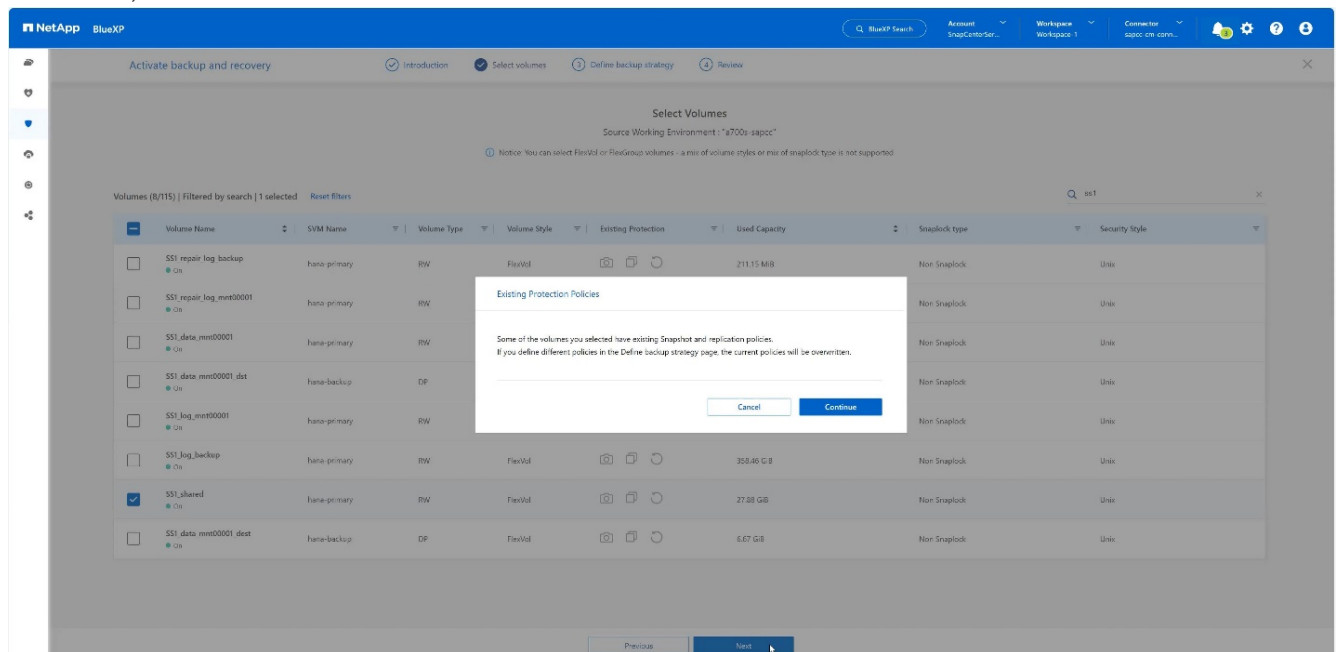
4. Scegliere **Backup**.



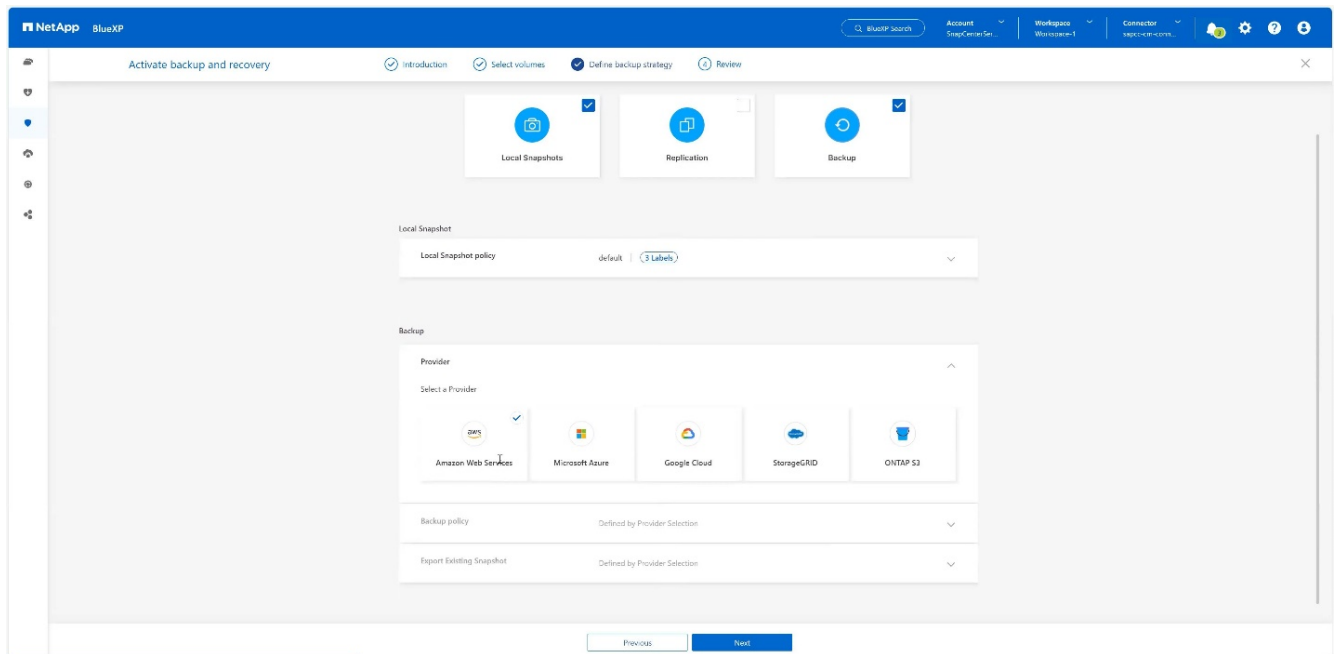
- Scegli un volume memorizzato nella stessa SVM dei tuoi file di dati SAP HANA e premi **Avanti**. In questo esempio è stato scelto il volume per /hana/shared.



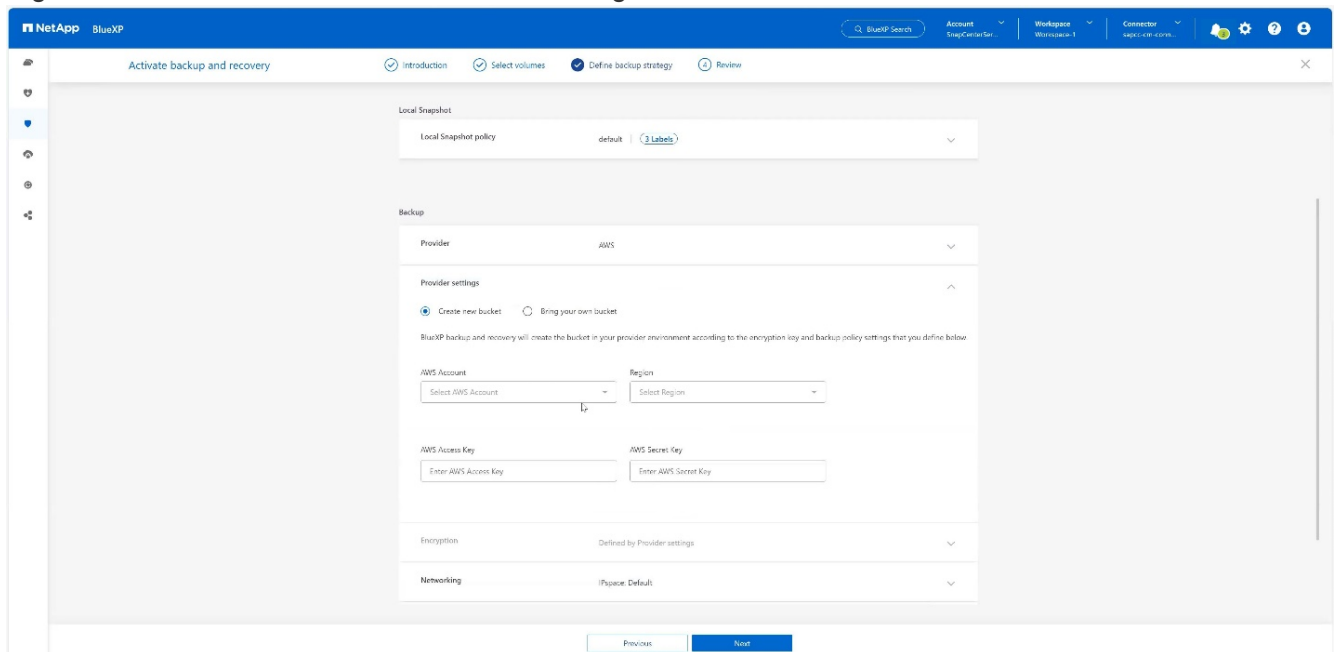
6. Continua, se esiste un criterio esistente.



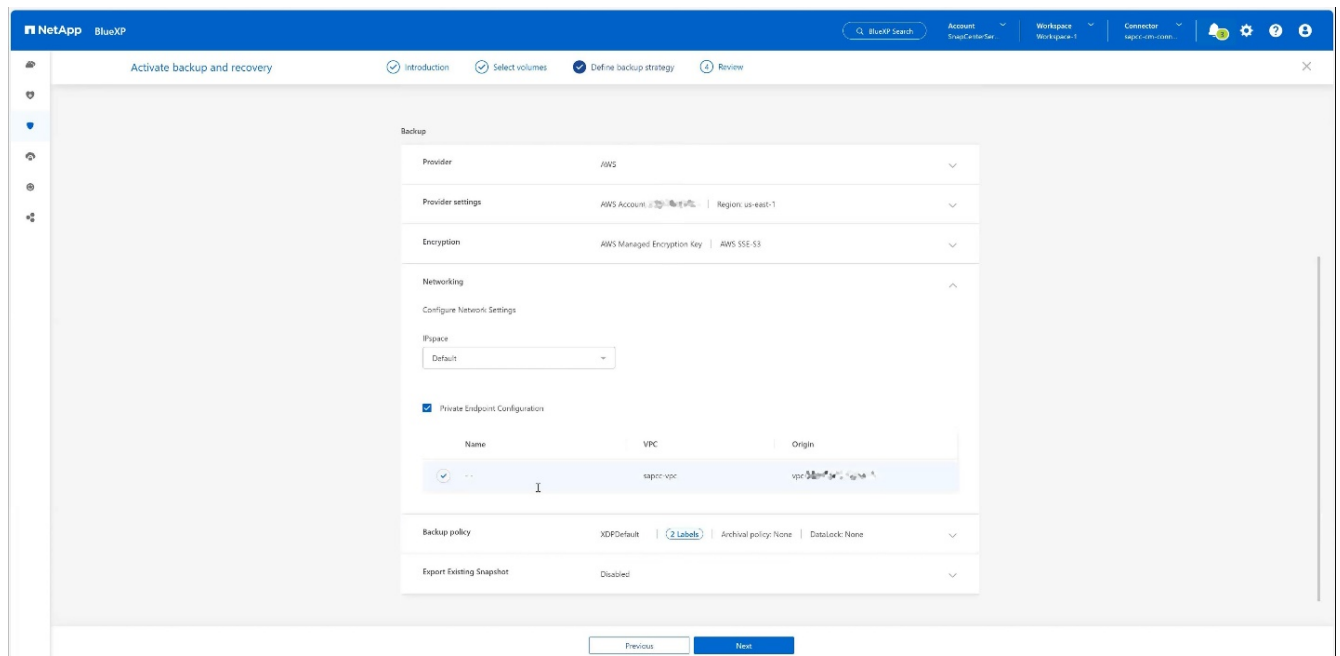
7. Selezionare l'opzione **Backup** e scegliere il provider di backup desiderato. In questo esempio AWS. Tenere selezionata l'opzione per i criteri già esistenti. Deselezionare le opzioni che non si desidera utilizzare.



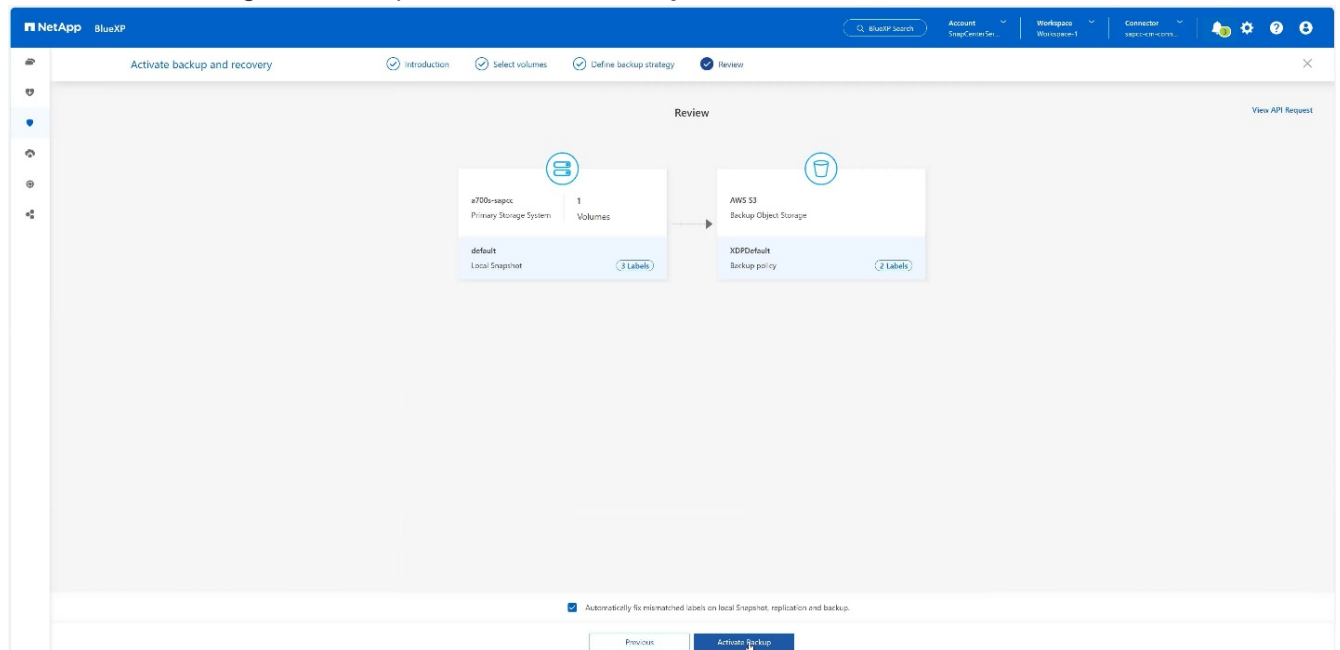
8. Creare un nuovo bucket o sceglierne uno esistente. Fornire le impostazioni dell'account AWS, la registrazione, la chiave di accesso e la chiave segreta. Premere **Avanti**.



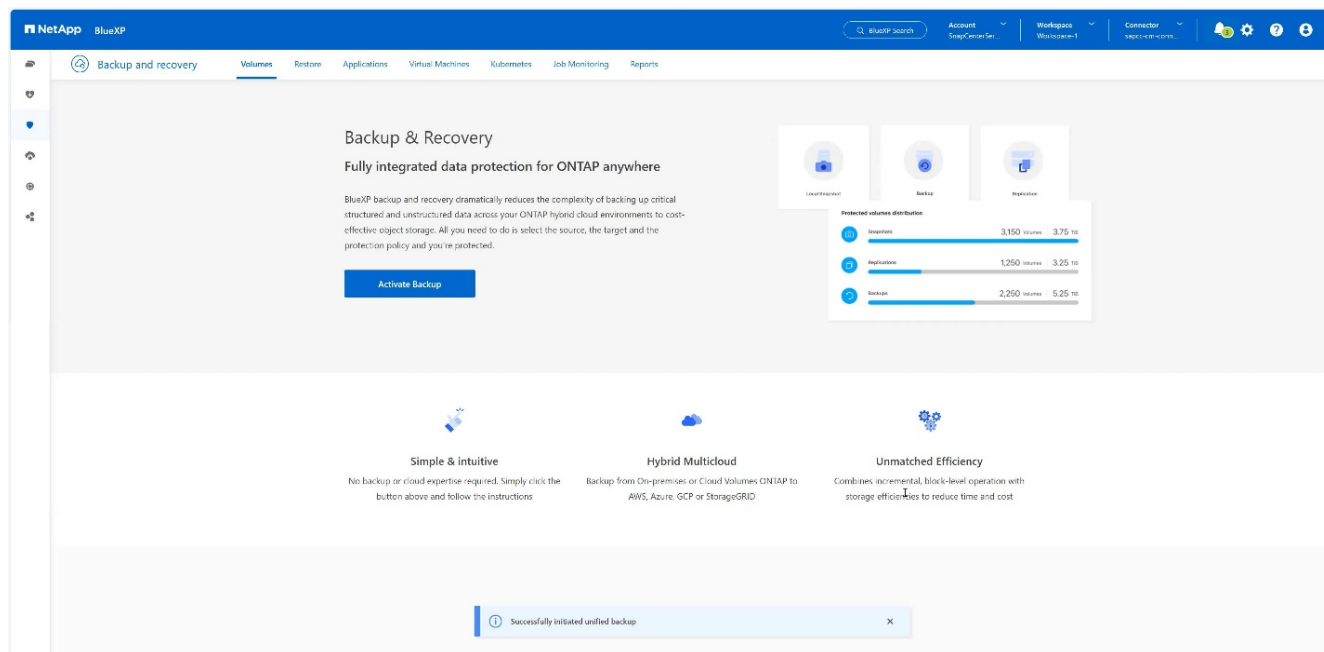
9. Scegli l'IPSpace corretto del tuo sistema di storage on-premise, seleziona **Privat Endpoint Configuration** e scegli l'endpoint VPC per S3. Premere **Avanti**.



10. Controllare la configurazione e premere **attiva backup**.



11. Il backup è stato avviato correttamente.



Configura la risorsa di sistema SAP HANA su SnapCenter

1. Controlla se la SVM (hana in questo esempio), dove è memorizzato il tuo sistema SAP HANA, è stata aggiunta tramite il cluster. In caso di aggiunta solo della SVM, aggiungere il cluster.

Name	IP	Cluster Name	User Name	Platform	Controller License
hana	10.63.150.245	10.63.150.245	vsadmin	AFF	✓
hana-backup.sapcc-stf.netapp.com	10.63.150.246		vsadmin	FAS	Not applicable
hana-dr.sapcc-stf.netapp.com	10.63.150.247		vsadmin	FAS	Not applicable
hana-primary.sapcc-stf.netapp.com	10.63.150.248		vsadmin	FAS	✓
speed		10.63.150.245		AFF	✓
srm-openstack		10.63.150.245		AFF	✓

2. Definire un criterio di pianificazione con il tipo di pianificazione giornaliera, settimanale o mensile.

Name	Backup Type	Schedule Type	Replication
BlockIntegrityCheck	File Based Backup	Weekly	
LocalSnap	Data Backup	Hourly	
LocalSnapAndMirrorAndVault	Data Backup	Daily	SnapVault, SnapMirror
LocalSnapAndSnapVault	Data Backup	Daily	SnapVault
LocalSnapKeep2	Data Backup	Hourly	
LocalSnap-OnDemand	Data Backup	On demand	
PolicyACBA	Data Backup	Daily	


×

Modify schedules for policy Policy4CBA

Daily


Start date

03/24/2023 01:00 am




☐ Expires on

03/15/2024 09:52 am




Repeat every

1



days

 The schedules are triggered in the SnapCenter Server time zone.

×

Cancel

OK

Daily

Start date

03/24/2023 01:00 am

☐ Expires on

03/15/2024 09:52 am

Repeat every

1

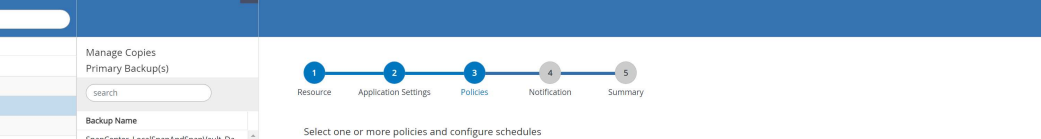
days

i The schedules are triggered in the SnapCenter Server time zone.

Cancel









OK

3. Aggiungi la nuova policy al sistema SAP HANA e assegna una pianificazione giornaliera.



The screenshot displays the NetApp SnapCenter console interface. On the left, the 'System' tree shows a hierarchy of resources, with 'SS1' selected under the 'SnapCenter' node. The main pane shows the 'Manage Copies' section for a 'Primary Backup(s)' policy. A table lists backup copies, including their names and timestamps. The right sidebar shows the 'Multitenant Database Container - Protect' section, which includes a progress bar with five steps: 1. Resource, 2. Application Settings, 3. Policies, 4. Notification, and 5. Summary. Below the progress bar, there is a section for 'Select one or more policies and configure schedules' showing a list of policies and their associated schedules.

Backup Name	Timestamp
SnapCenter_LocalSnapAndSnapVault_Daily_03-24-2023_05.00.02.8413	
SnapCenter_LocalSnap_Hourly_03-24-2023_03.00.01.5889	
SnapCenter_PolicyCBA_Daily_03-24-2023_01.00.01.0312	
SnapCenter_LocalSnap_Hourly_03-23-2023_23.00.01.5691	
SnapCenter_LocalSnap_Hourly_03-23-2023_19.00.01.5084	
SnapCenter_LocalSnap_Hourly_03-23-2023_15.00.02.4395	
SnapCenter_PolicyCBA_Daily_03-23-2023_11.57.36.5415	
SnapCenter_LocalSnapAndSnapVault_Daily_03-23-2023_11.07.43.1336	
SnapCenter_LocalSnap_Hourly_03-23-2023_11.00.01.0469	
SnapCenter_LocalSnap_Hourly_03-23-2023_10.39.26.0813	

Policy	Applied Schedules	Configure Schedules
BlockIntegrityCheck	Weekly: Run on days: Sunday	 
LocalSnap	Hourly: Repeat every 4 hours	 
LocalSnap-OnDemand	None	To schedule operations select a policy that has the appropriate schedule associated, or modify the selected policy to allow schedules.
LocalSnapAndSnapVault	Daily: Repeat every 1 days	 
PolicyCBA	Daily: Repeat every 1 days	 
Total 5		

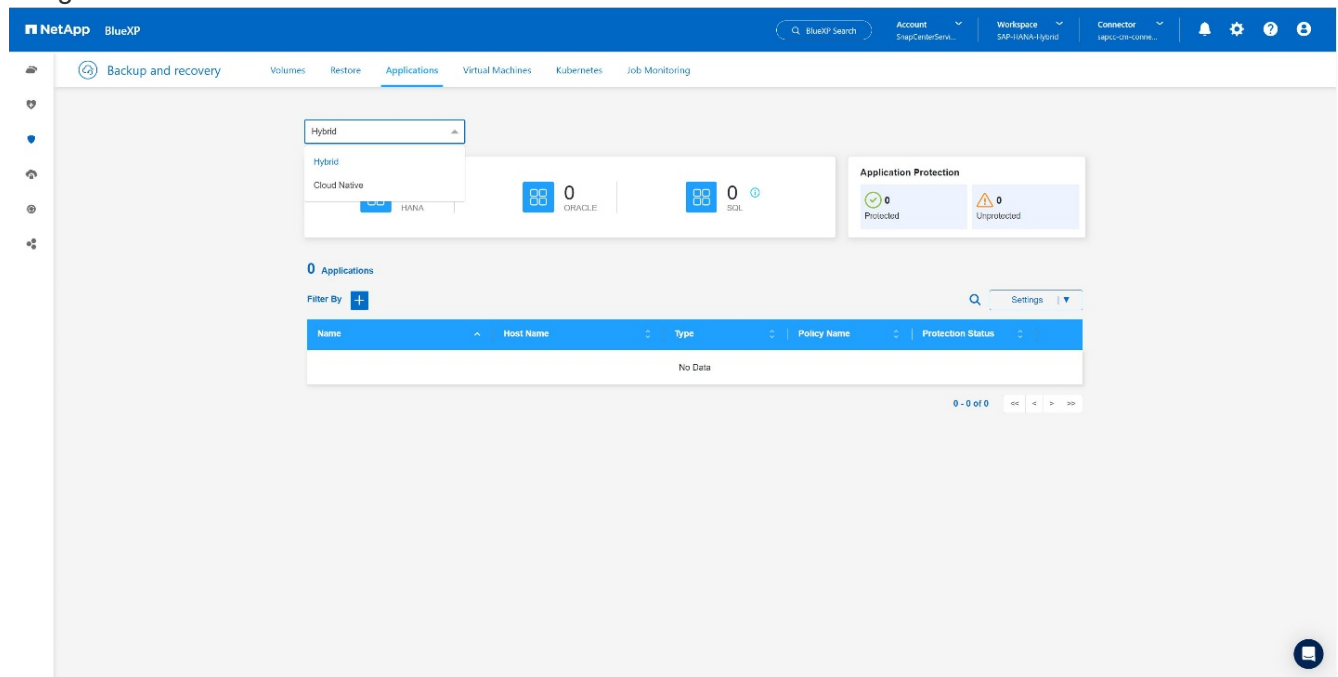
4. Una volta configurati, i nuovi backup con questo criterio saranno disponibili dopo l'esecuzione del criterio in base alla pianificazione definita.

The screenshot displays the NetApp SnapCenter web interface. The top navigation bar includes the NetApp logo, user information (sapccitadmin), and a sign-out button. A left sidebar contains icons for various functions like search, system overview, and reports. The main content area is titled "SAP HANA" and shows a "System" view with a list of databases: QS1, SM1, SS1, SS2, and SS2. Below this, there's a "Manage Copies" section with a diagram showing "Local copies" (17 Backups, 0 Clones) and "Vault copies" (12 Backups, 0 Clones). To the right, a "Summary Card" provides an overview: 31 Backups, 29 Snapshot based backups, 2 File-based backups, and 0 Clones. At the bottom, a table lists the primary backup(s) with columns for Backup Name, Count, and End Date.

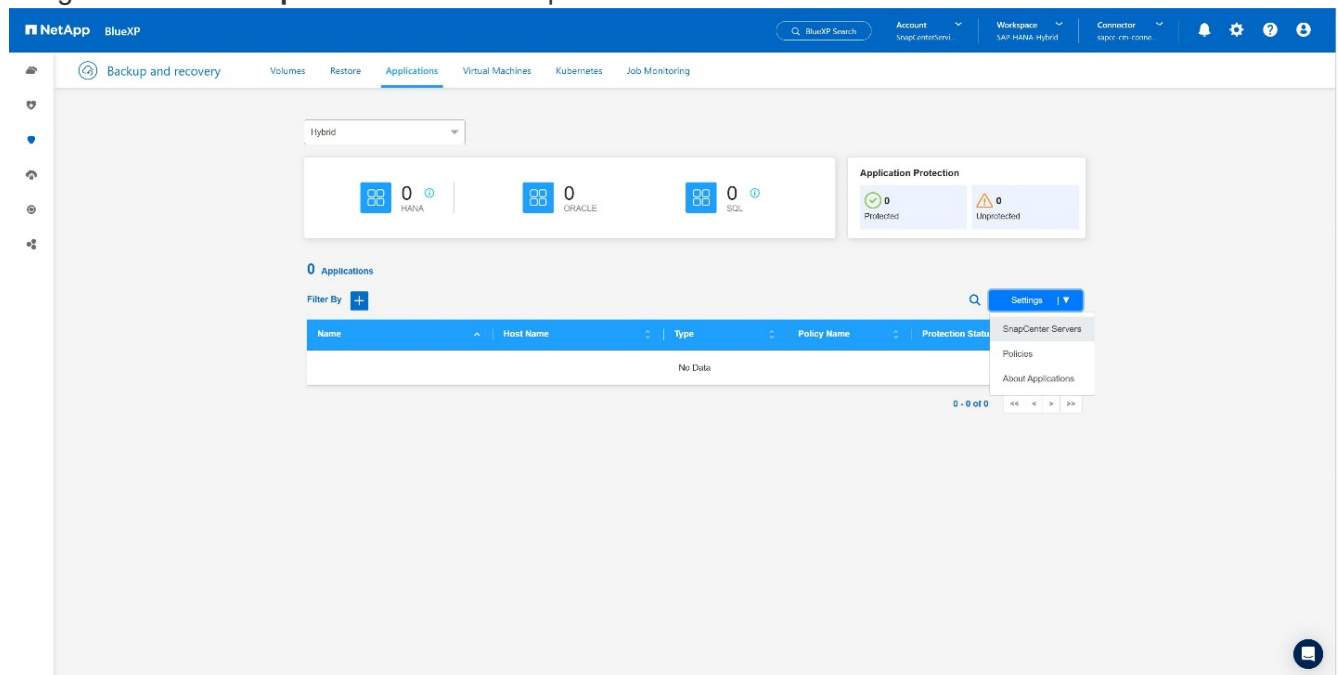
Backup Name	Count	End Date
SnapCenter_LocalSnapAndSnapVault_Daily_03-24-2023_05.00.02.8413	1	03/24/2023 5:01:01 AM
SnapCenter_LocalSnap_Hourly_03-24-2023_03.00.01.5889	1	03/24/2023 3:01:02 AM
SnapCenter_PolicyCDBA_Daily_03-24-2023_01.00.01.0312	1	03/24/2023 1:01:02 AM
SnapCenter_LocalSnap_Hourly_03-23-2023_23.00.01.5691	1	03/23/2023 11:01:01 PM
SnapCenter_LocalSnap_Hourly_03-23-2023_19.00.01.5084	1	03/23/2023 7:01:02 PM
SnapCenter_LocalSnap_Hourly_03-23-2023_15.00.02.4395	1	03/23/2023 3:01:01 PM
SnapCenter_PriviledCBA_Daily_03-23-2023_11.57.36.5415	1	03/23/2023 11:58:35 AM

Aggiunta di SnapCenter all'ambiente di lavoro BlueXP

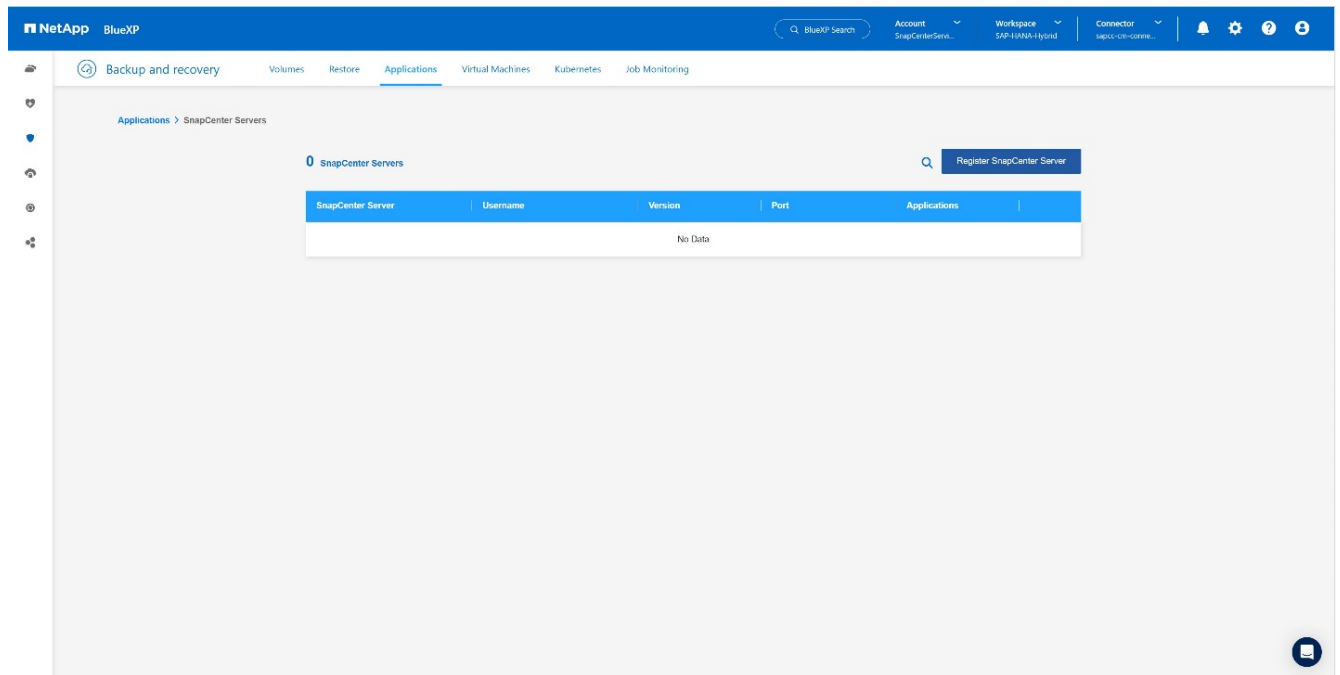
1. Nel menu a sinistra scegliere **protezione** → **Backup e ripristino** → **applicazioni**.
2. Scegliere **ibrido** dal menu a discesa.



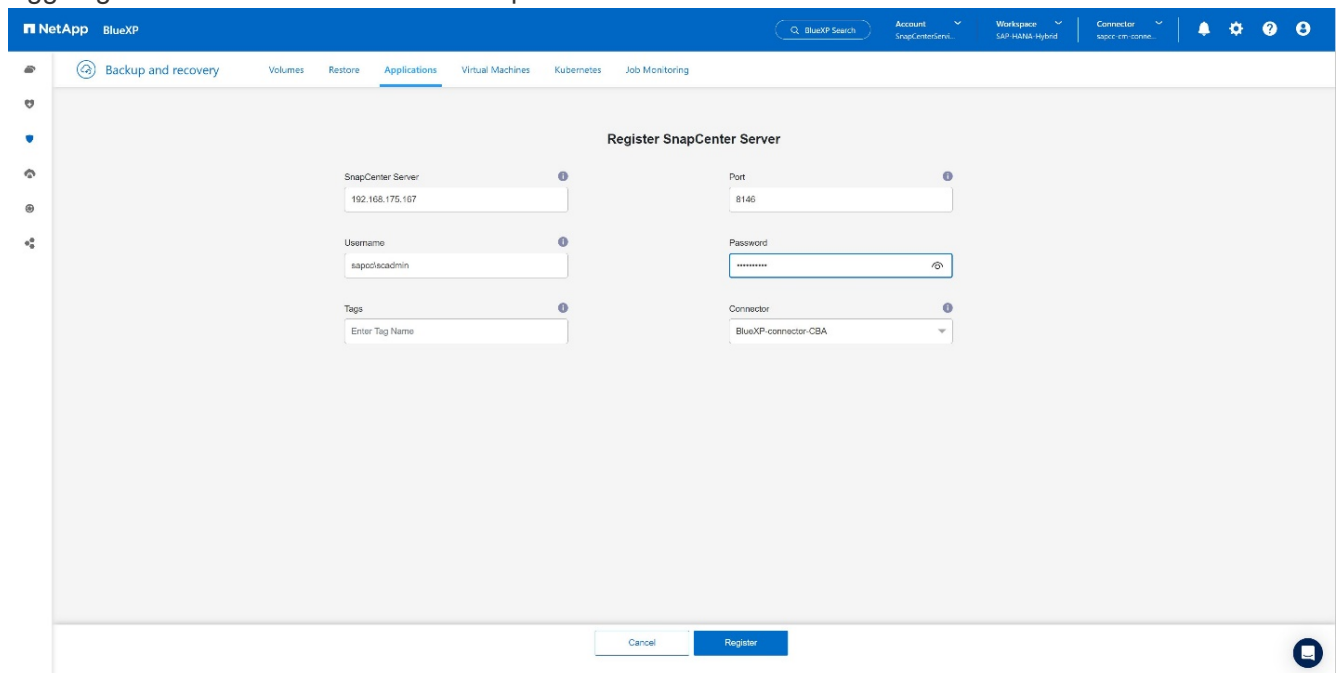
3. Scegliere **Server SnapCenter** dal menu Impostazioni.



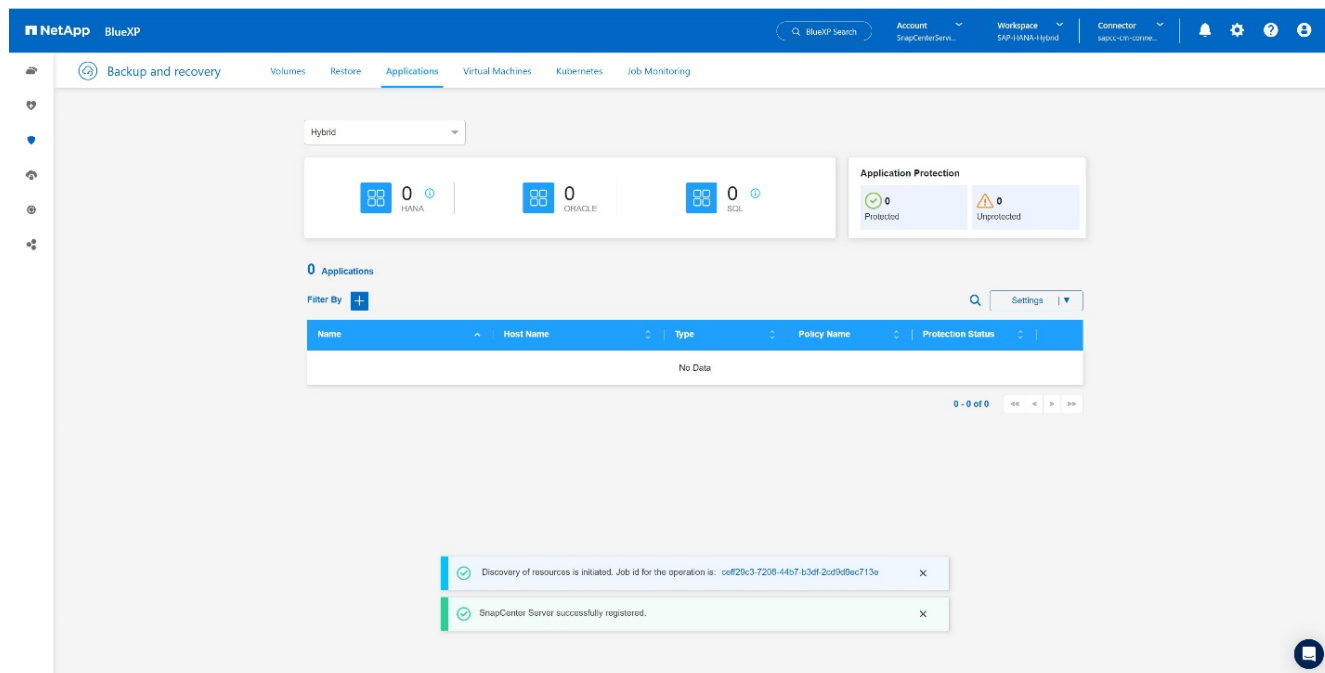
4. Registrare il server SnapCenter.



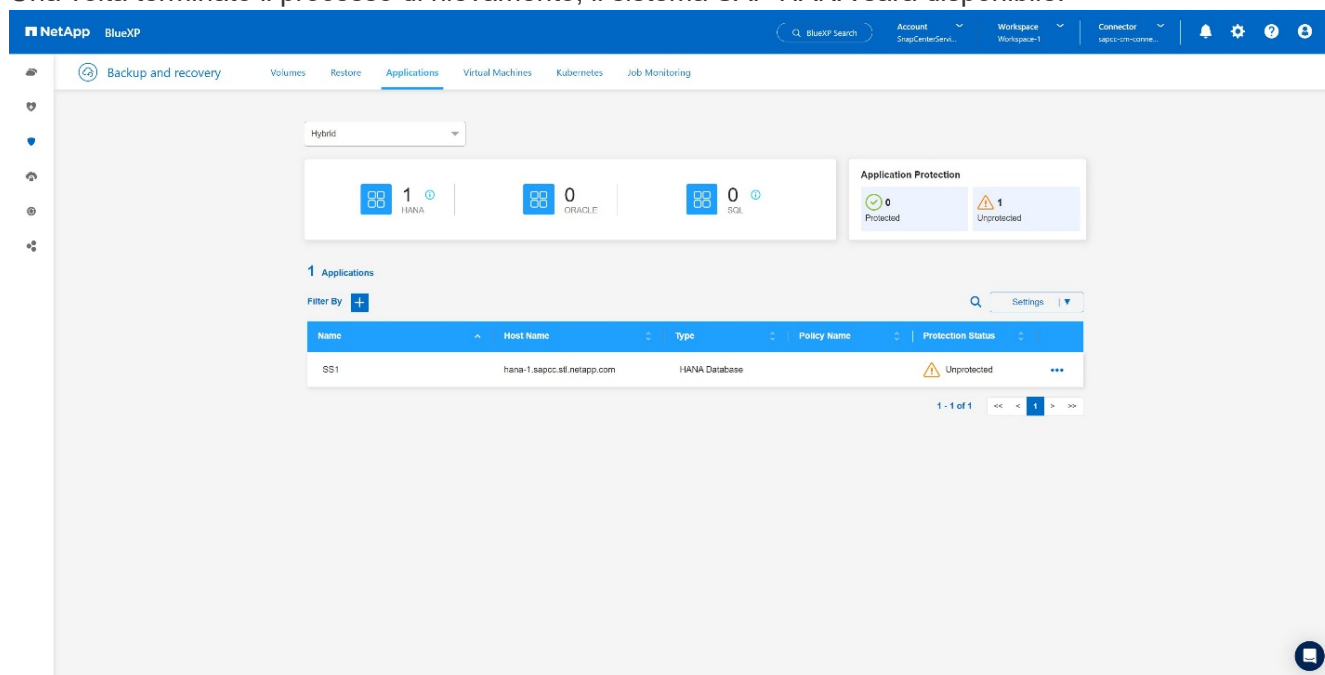
5. Aggiungere le credenziali del server SnapCenter.



6. I server SnapCenter sono stati aggiunti e i dati verranno rilevati.

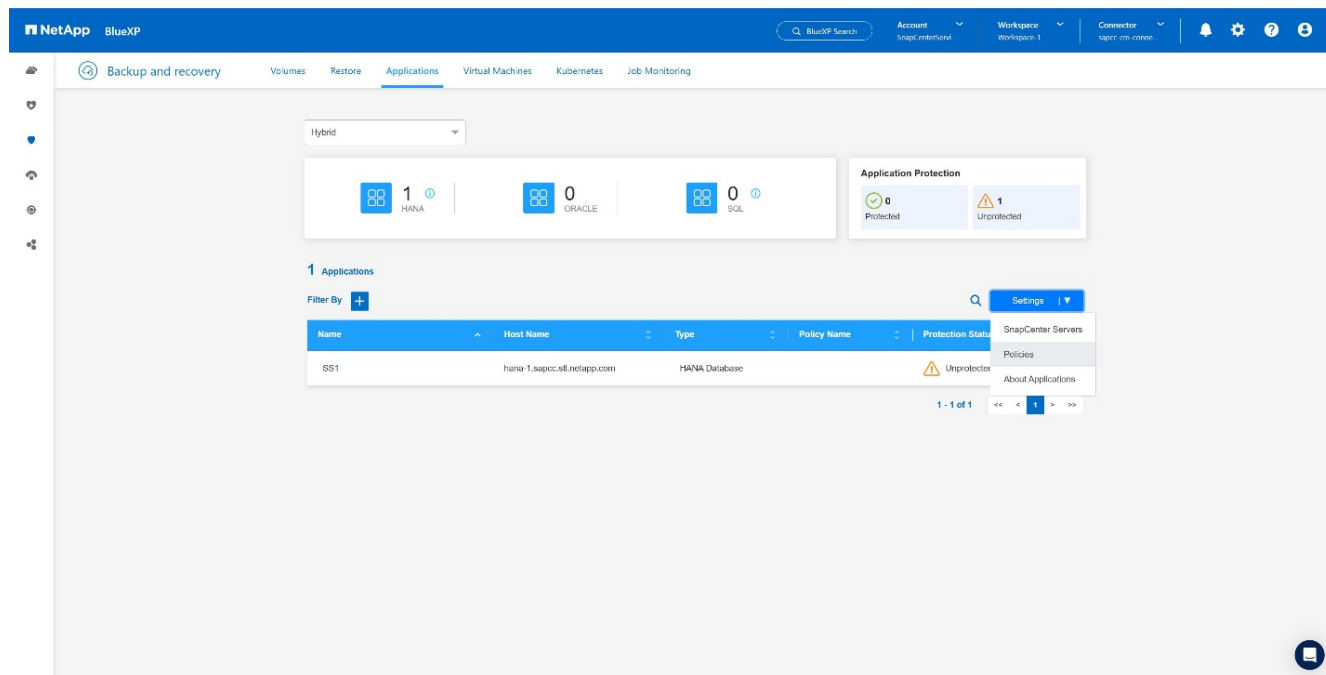


7. Una volta terminato il processo di rilevamento, il sistema SAP HANA sarà disponibile.

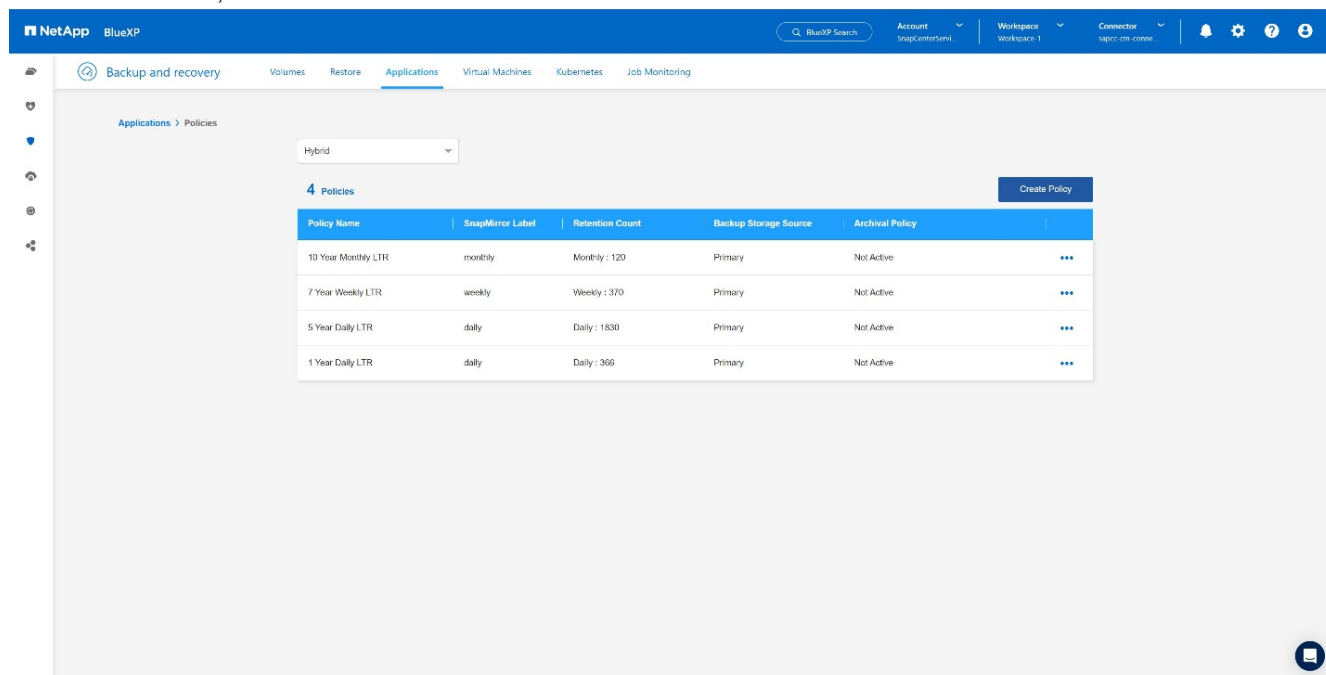


Creazione di un criterio di backup per il backup delle applicazioni

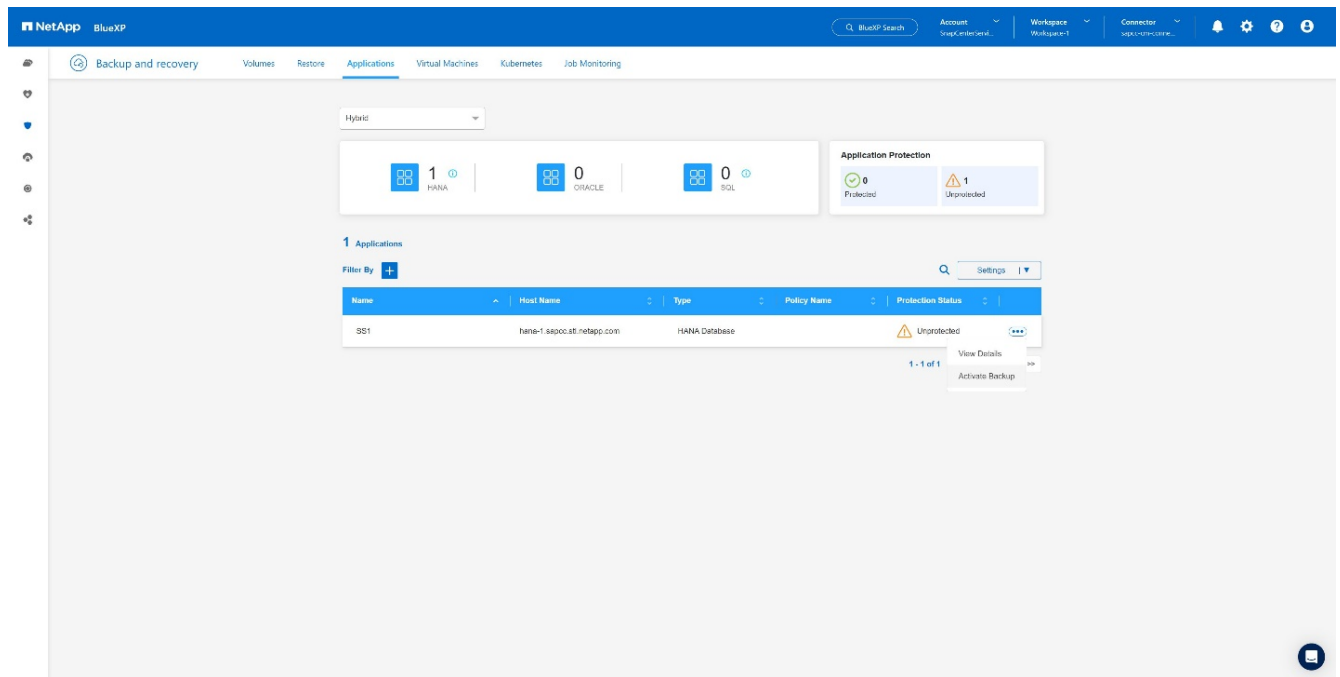
1. Scegliere **Criteri** dal menu delle impostazioni.



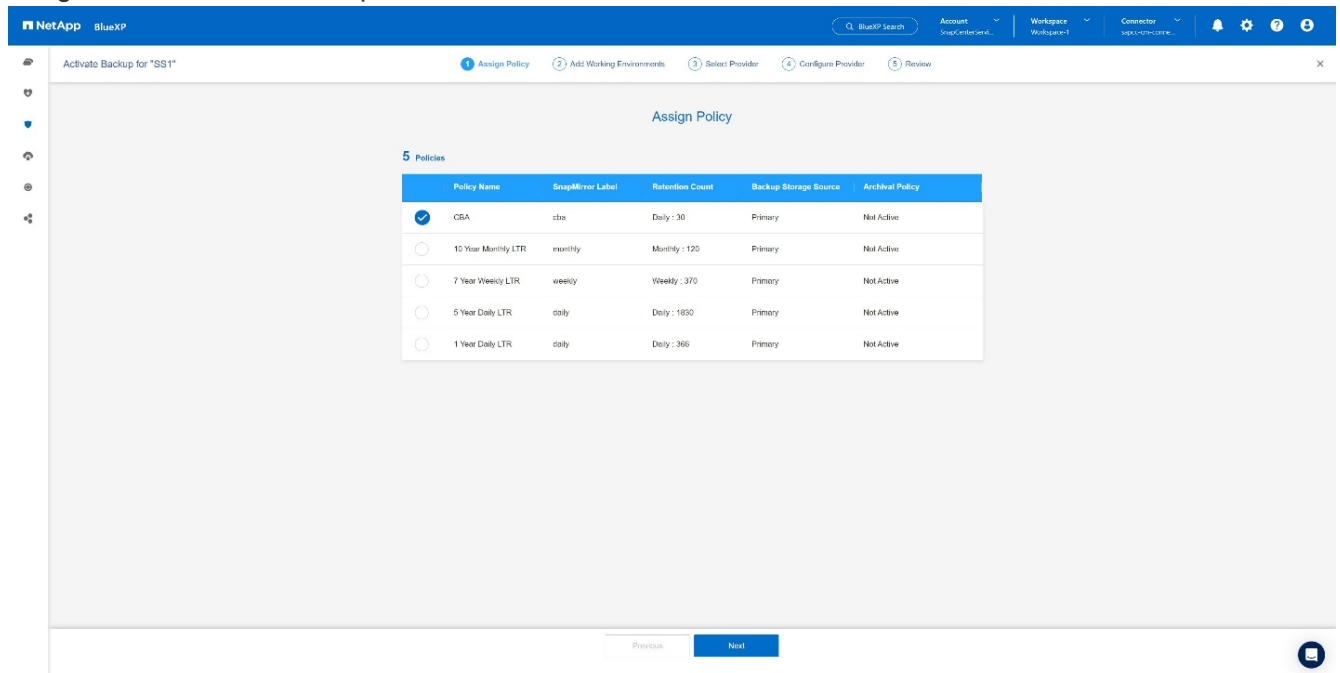
2. Se lo si desidera, creare un nuovo criterio facendo clic su **Crea criterio**.



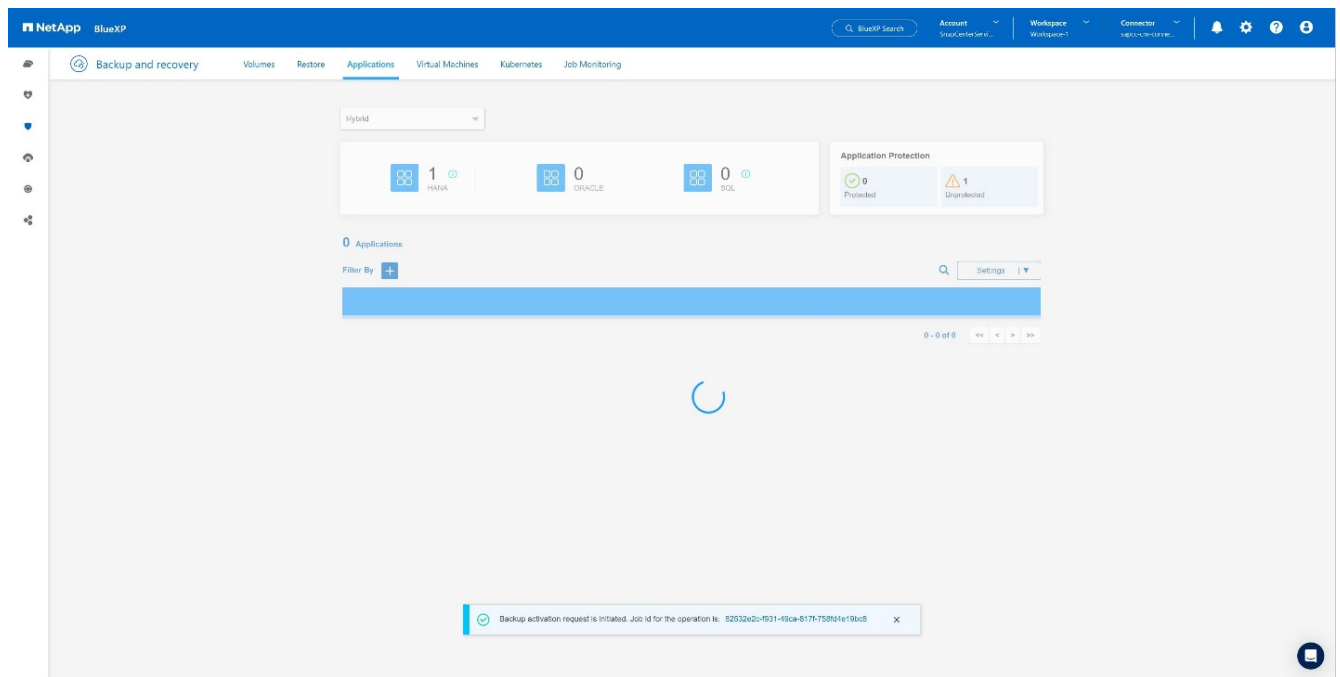
3. Fornire il nome della policy e l'etichetta SnapMirror desiderata, scegliere le opzioni desiderate e premere **Crea**.



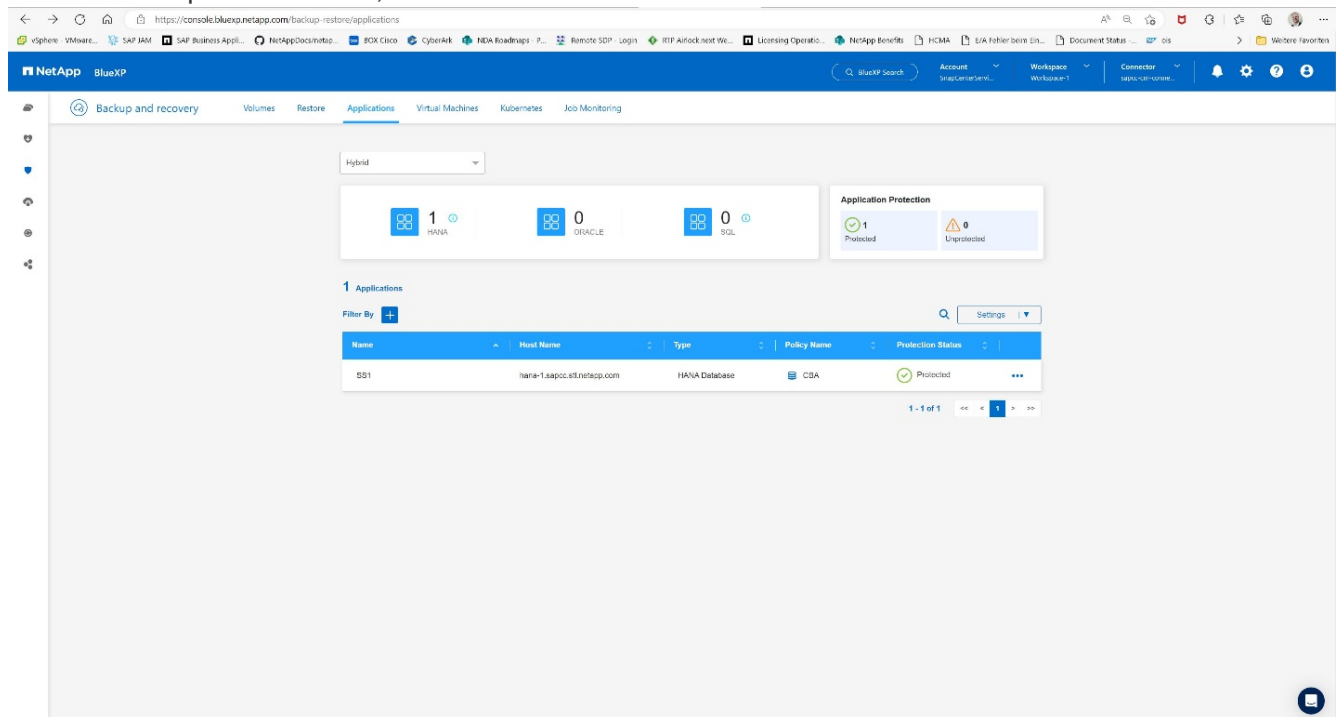
2. Scegliere il criterio creato in precedenza e fare clic su **Avanti**.



3. Quando il sistema di archiviazione e il connettore sono stati configurati in anticipo, il backup viene attivato.



4. Una volta completato il lavoro, viene visualizzato l'elenco sistema.



5. Dopo qualche tempo i backup saranno elencati nella vista dettagliata del sistema SAP HANA. Il giorno successivo verrà elencato un backup giornaliero.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The 'Applications' section is selected, showing details for a database named 'SS1'.

Database Details:

- Database Name: SS1
- Database Version: 2.0 SP906
- Database Type: Multiple Containers
- Discovery Type: Auto Discovered
- Tenant Database Names: SS1
- Application Type: HANA Database

Storage Details:

- Volume 1

Protection Details:

- Policy Name: cba-test
- Working Environment: a700e sapcc
- Provider: AWS
- Bucket: netapp-backup-1f6e2ef5a9-4cad-11eq-af05-00a096d994db
- Region: us-east-1
- Account: 811586431415

Backups:

26 Backups

Filter By: [icon]

Last Updated: Apr 17, 2023, 12:23:43 PM

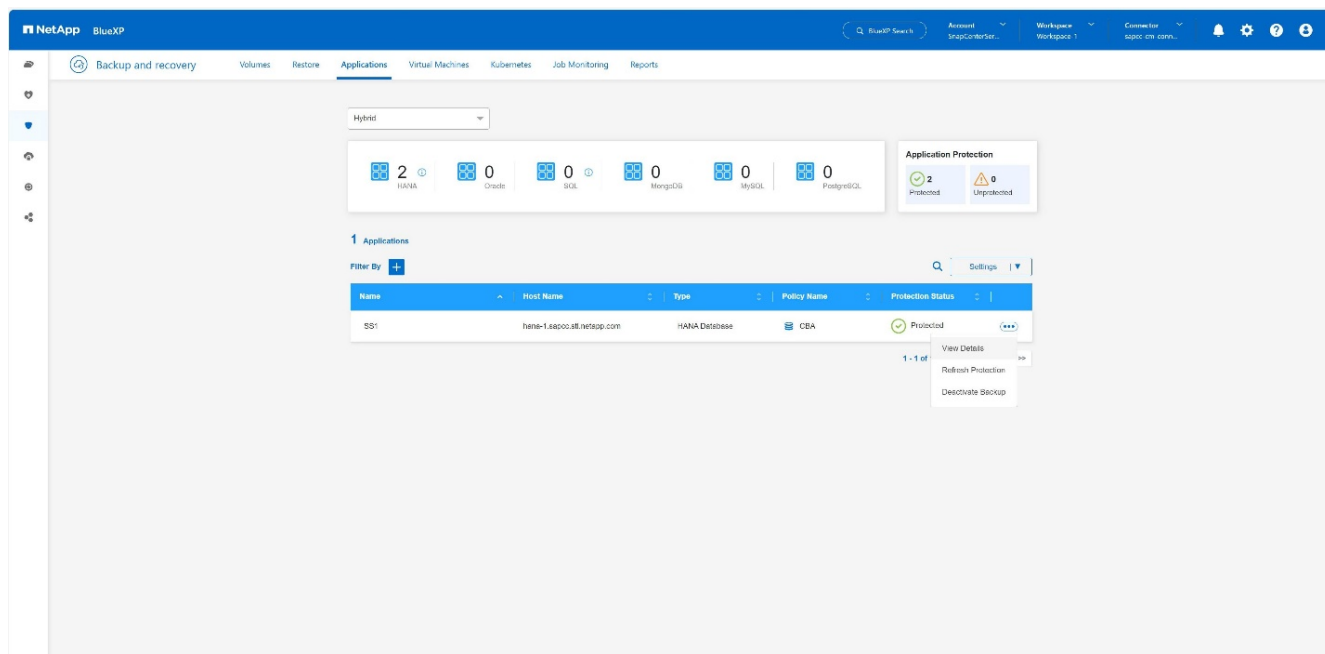
Backup Name	Backup Type	Backup Date
SnapCenter_Policy4CBA_Daily_04-17-2023_01.00.02.2237	Data	4/17/2023 1:01:03 AM
SnapCenter_Policy4CBA_Daily_04-16-2023_01.00.02.0710	Data	4/16/2023 1:01:05 AM
SnapCenter_Policy4CBA_Daily_04-15-2023_01.00.02.1403	Data	4/15/2023 1:01:03 AM

In alcuni ambienti potrebbe essere necessario rimuovere eventuali impostazioni di pianificazione esistenti dell'origine snapmirror. Per farlo, esegui il seguente comando nel sistema ONTAP di origine: *snapmirror modify -destination-path <hana-cloud-svm>:<SID_data_mnt00001>_copy -planning ""* .

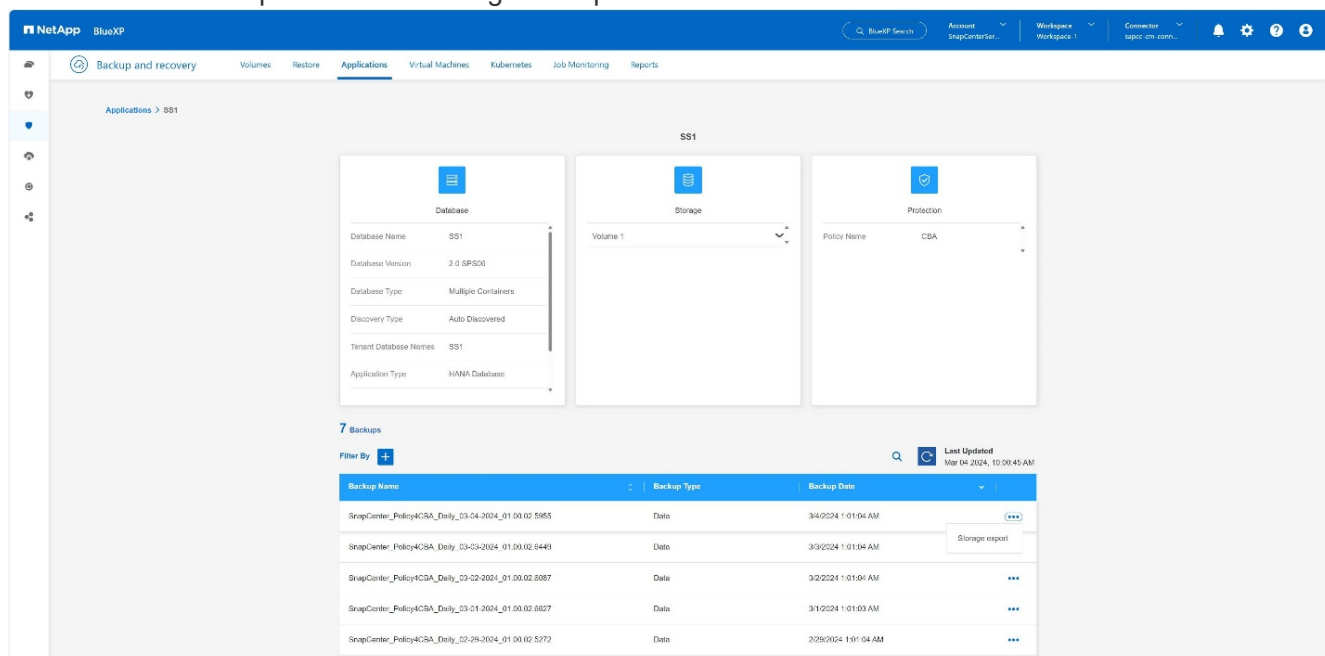
Ripristino del backup di SAP HANA BlueXP

Un ripristino dal backup può essere effettuato solo su un sistema storage basato su NetApp ONTAP on-premise o su NetApp CVO all'interno del cloud. È possibile eseguire un ripristino effettuando le seguenti operazioni:

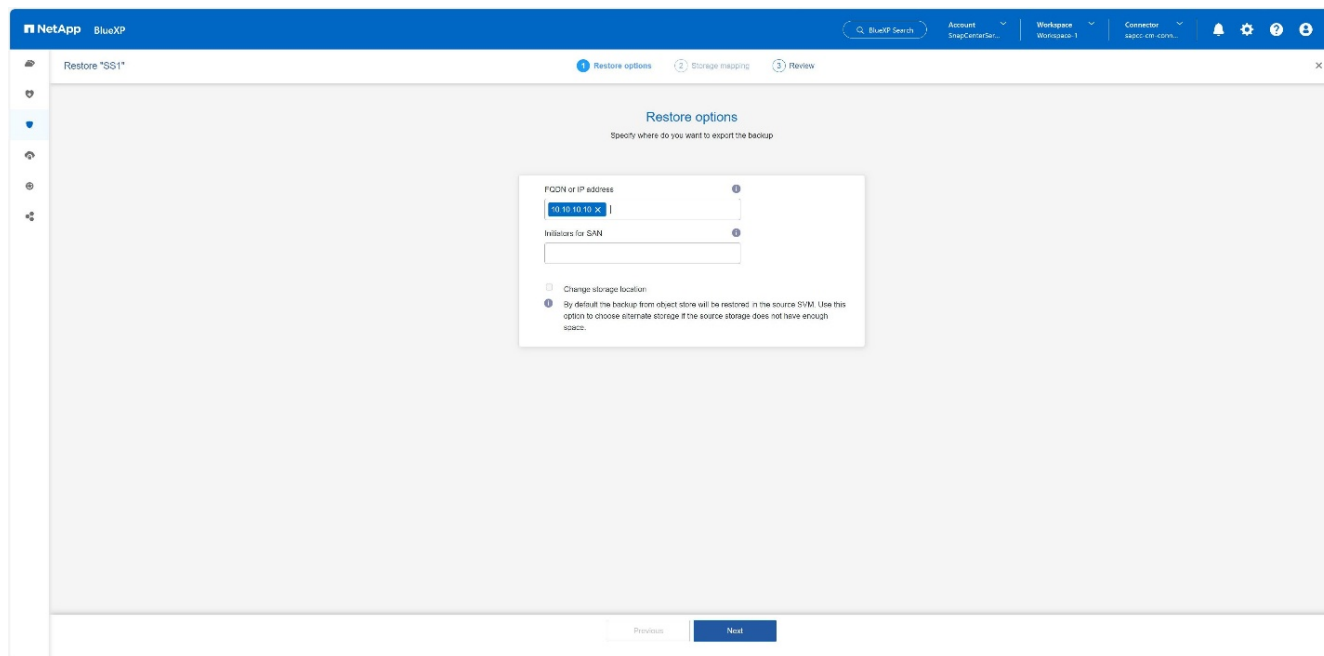
1. Nell'interfaccia utente di BlueXP, fai clic su **protezione > Backup e ripristino > applicazioni** e scegli ibrido.
2. Nel campo **Filtra per**, seleziona il filtro **tipo** e dal menu a discesa seleziona **HANA**.
3. Fare clic su **Visualizza dettagli** corrispondente al database che si desidera ripristinare.



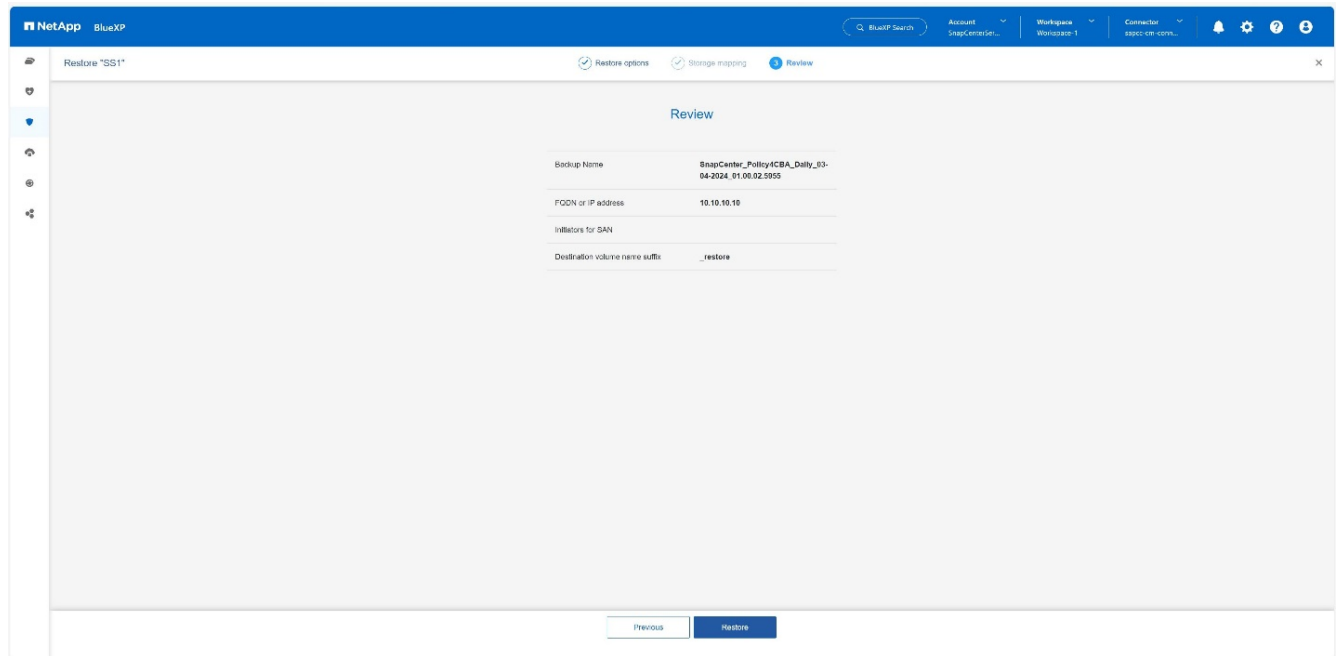
4. Selezionare il backup desiderato e scegliere esportazione archiviazione.



5. Fornire le opzioni desiderate:



- a. Per l'ambiente NAS, specificare l'FQDN o l'indirizzo IP dell'host su cui esportare i volumi ripristinati dall'archivio di oggetti.
 - b. Per l'ambiente SAN, specificare gli iniziatori dell'host a cui mappare le LUN dei volumi ripristinati dall'archivio di oggetti.
6. Se lo snapshot si trova nello storage di archiviazione, selezionare la priorità per ripristinare i dati dallo storage di archiviazione.
 7. Se lo spazio non è sufficiente nell'archivio di origine o l'archivio di origine non è disponibile, selezionare **Modifica posizione di archiviazione**.
 8. Se si seleziona **Modifica posizione di memorizzazione**, è possibile aggiungere un suffisso al volume di destinazione. Se la casella di controllo non è stata selezionata, per impostazione predefinita **_restore** viene aggiunto al volume di destinazione. Fare clic su **Avanti**.
 9. Se è stato selezionato Cambia posizione di archiviazione, specificare i dettagli della posizione di archiviazione alternativa in cui i dati ripristinati dall'archivio oggetti verranno memorizzati nella pagina mappatura archiviazione e fare clic su **Avanti**.
 10. Rivedere i dettagli e fare clic su **Ripristina**.



Questa operazione esegue solo l'esportazione di archiviazione del backup ripristinato per l'host specificato. È necessario montare manualmente il filesystem sull'host e richiamare il database. Dopo aver utilizzato il volume, l'amministratore dello storage può eliminare il volume dal cluster ONTAP.

Informazioni aggiuntive e cronologia versioni

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- Documentazione di backup e recovery di NetApp BlueXP
["Proteggi i dati delle applicazioni on-premise | documentazione NetApp"](#)
- Backup e recovery per SAP HANA con SnapCenter
<https://docs.netapp.com/us-en/netapp-solutions-sap/backup/saphana-br-scs-overview.html#the-netapp-solution>

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Marzo 2024	Versione iniziale

Fare riferimento a ["Tool di matrice di interoperabilità \(IMT\)"](#) Sul sito del supporto NetApp per verificare che le versioni esatte dei prodotti e delle funzionalità descritte in questo documento siano supportate per il tuo ambiente specifico. NetApp IMT definisce i componenti e le versioni dei prodotti che possono essere utilizzati per costruire configurazioni supportate da NetApp. I risultati specifici dipendono dall'installazione di ciascun cliente in conformità alle specifiche pubblicate.

Backup e ripristino della replica del sistema SAP HANA con SnapCenter

TR-4719: Replica del sistema SAP HANA - Backup e ripristino con SnapCenter

Nils Bauer, NetApp

SAP HANA System Replication viene comunemente utilizzato come soluzione ad alta disponibilità o di disaster recovery per i database SAP HANA. SAP HANA System Replication offre diverse modalità operative che è possibile utilizzare in base al caso d'utilizzo o ai requisiti di disponibilità.

È possibile combinare due casi di utilizzo principali:

- Alta disponibilità con un obiettivo del punto di ripristino (RPO) pari a zero e un obiettivo RTO (Recovery Time Objective) minimo utilizzando un host SAP HANA secondario dedicato.
- Disaster recovery su larga distanza. L'host SAP HANA secondario può essere utilizzato anche per lo sviluppo o il test durante il normale funzionamento.

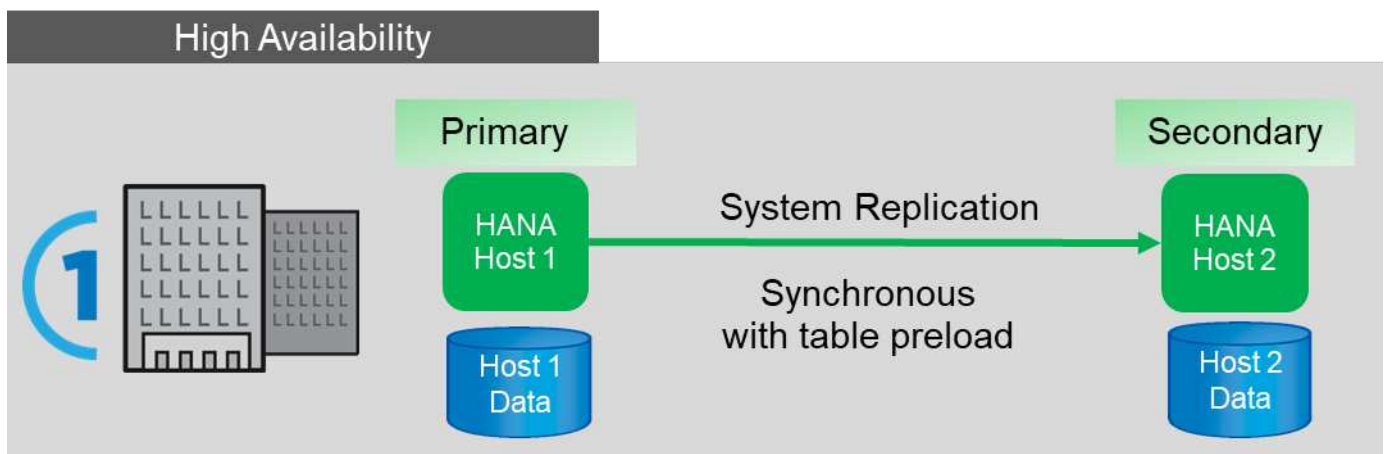
Alta disponibilità con un RPO pari a zero e un RTO minimo

La replica di sistema viene configurata con la replica sincrona utilizzando tabelle precaricate in memoria sull'host SAP HANA secondario. Questa soluzione ad alta disponibilità può essere utilizzata per risolvere i guasti hardware o software e per ridurre i downtime pianificati durante gli aggiornamenti del software SAP HANA (operazioni di downtime quasi pari a zero).

Le operazioni di failover vengono spesso automatizzate utilizzando software di cluster di terze parti o con un semplice clic del workflow con il software SAP Landscape Management.

Dal punto di vista dei requisiti di backup, devi essere in grado di creare backup indipendenti dall'host SAP HANA principale o secondario. Un'infrastruttura di backup condivisa viene utilizzata per ripristinare qualsiasi backup, indipendentemente dall'host su cui è stato creato il backup.

Il resto di questo documento si concentra sulle operazioni di backup con la replica del sistema SAP configurata come soluzione ad alta disponibilità.

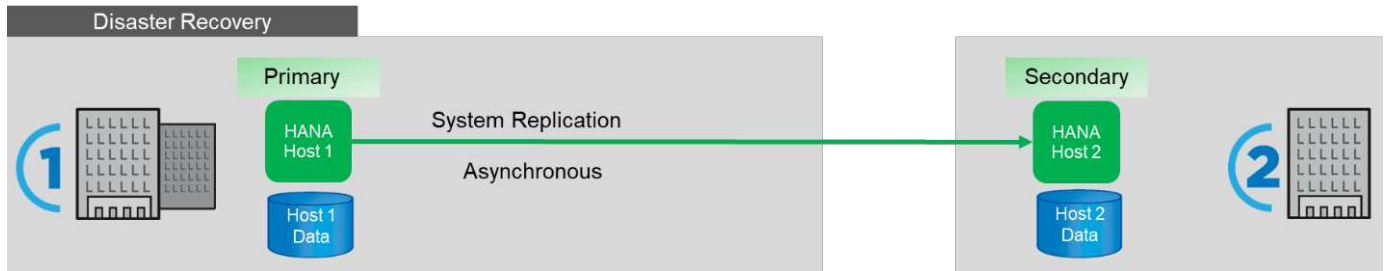


Disaster recovery su larga distanza

La replica del sistema può essere configurata con una replica asincrona senza alcuna tabella precaricata nella memoria dell'host secondario. Questa soluzione viene utilizzata per risolvere i guasti del data center e le

operazioni di failover vengono in genere eseguite manualmente.

Per quanto riguarda i requisiti di backup, è necessario essere in grado di creare backup durante il normale funzionamento nel data center 1 e durante il disaster recovery nel data center 2. Nei data center 1 e 2 è disponibile un'infrastruttura di backup separata e le operazioni di backup vengono attivate come parte del disaster failover. L'infrastruttura di backup in genere non è condivisa e non è possibile eseguire un'operazione di ripristino di un backup creato nell'altro data center.



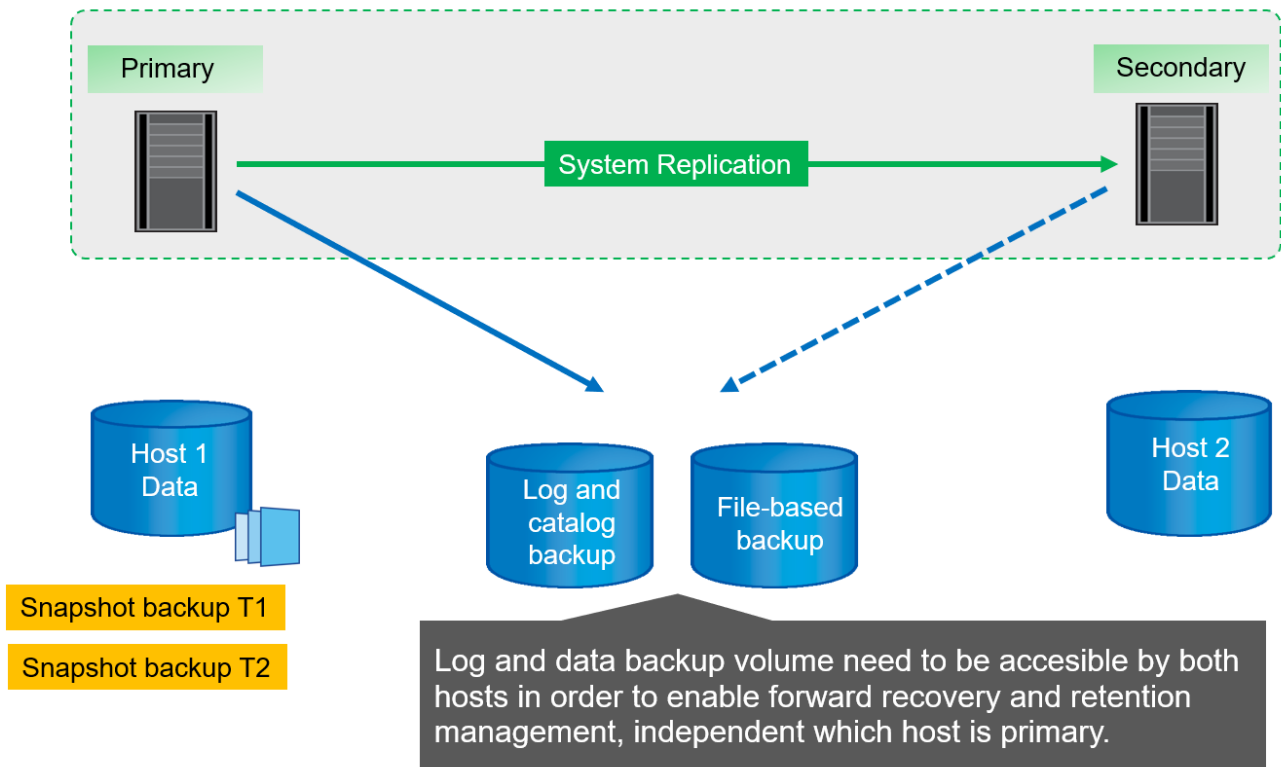
Backup Snapshot dello storage e replica del sistema SAP

Le operazioni di backup vengono sempre eseguite sull'host SAP HANA primario. I comandi SQL richiesti per l'operazione di backup non possono essere eseguiti sull'host SAP HANA secondario.

Per le operazioni di backup SAP HANA, gli host SAP HANA primari e secondari sono una singola entità. Condividono lo stesso catalogo di backup SAP HANA e utilizzano i backup per il ripristino, indipendentemente dal fatto che il backup sia stato creato nell'host SAP HANA primario o secondario.

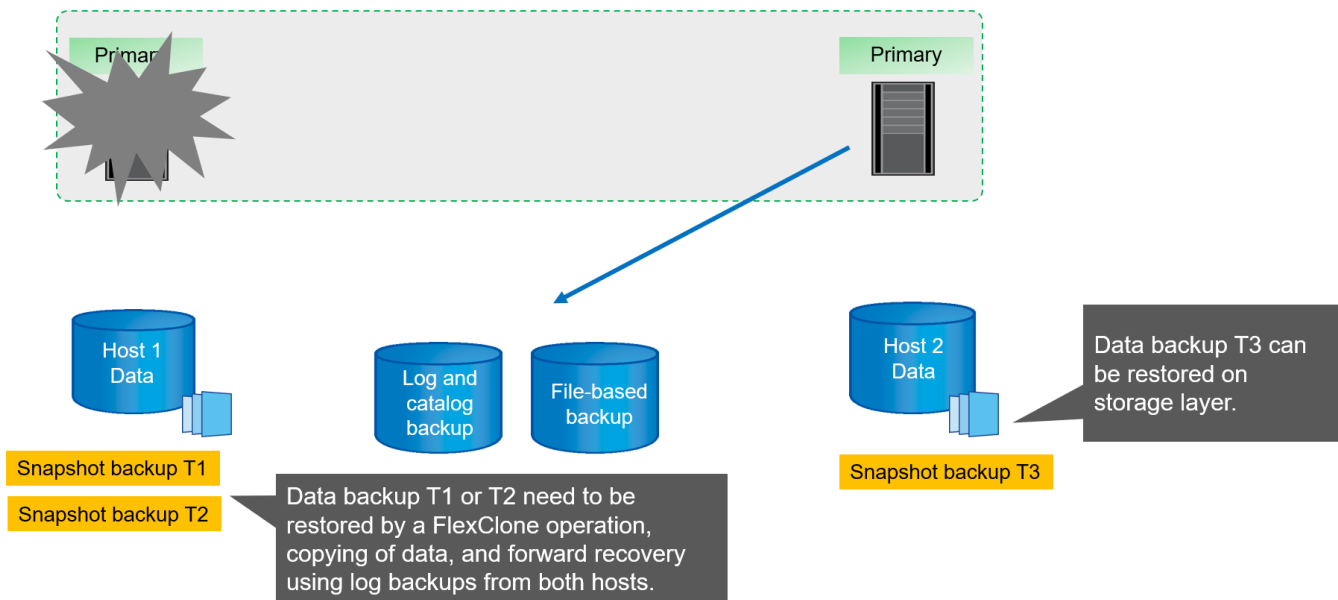
La possibilità di utilizzare qualsiasi backup per il ripristino e l'inoltro del ripristino utilizzando i backup dei log da entrambi gli host richiede una posizione di backup dei log condivisa accessibile da entrambi gli host. NetApp consiglia di utilizzare un volume di storage condiviso. Tuttavia, occorre anche separare la destinazione di backup del log in sottodirectory all'interno del volume condiviso.

Ogni host SAP HANA dispone di un proprio volume di storage. Quando si utilizza un'istantanea basata su storage per eseguire un backup, viene creata un'istantanea coerente con il database sul volume di storage dell'host SAP HANA primario.



Quando viene eseguito un failover sull'host 2, l'host 2 diventa l'host primario, i backup vengono eseguiti sull'host 2 e i backup Snapshot vengono creati sul volume di storage dell'host 2.

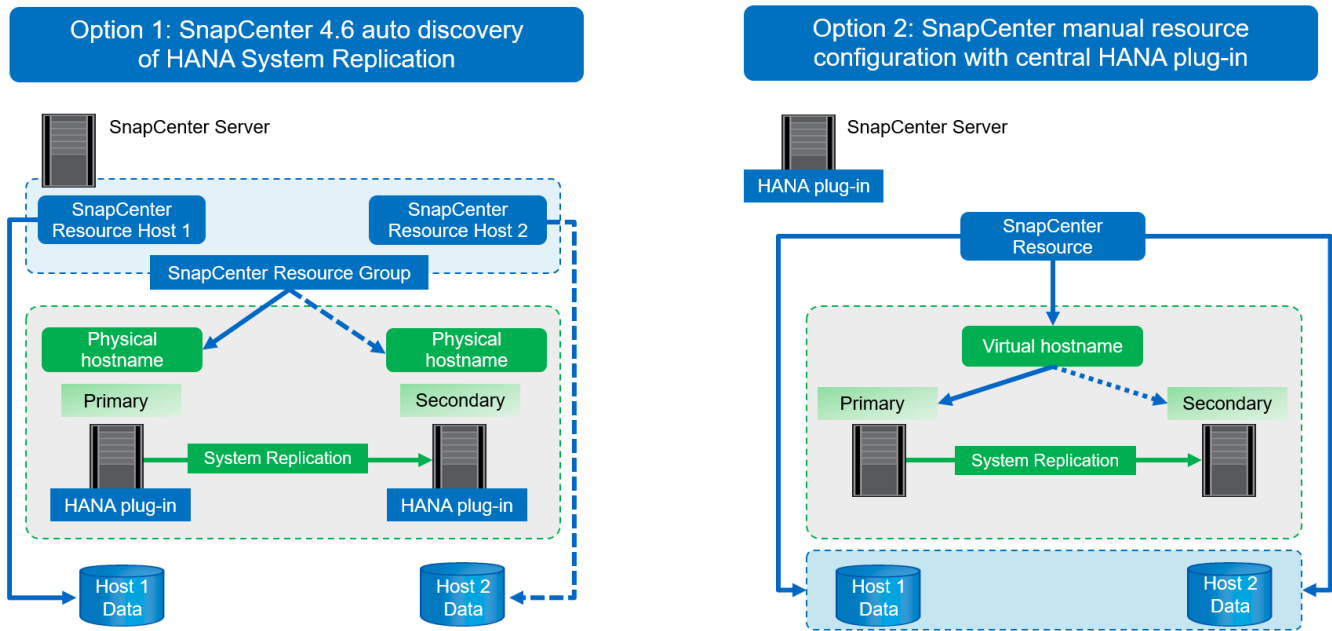
Il backup creato sull'host 2 può essere ripristinato direttamente al livello di storage. Se è necessario utilizzare un backup creato sull'host 1, il backup deve essere copiato dal volume di storage dell'host 1 al volume di storage dell'host 2. Forward Recovery utilizza i backup dei log di entrambi gli host.



Opzioni di configurazione SnapCenter per la replica del sistema SAP

Sono disponibili due opzioni per la configurazione della protezione dei dati con il software NetApp SnapCenter in un ambiente di replica del sistema SAP HANA:

- Un gruppo di risorse SnapCenter che include host SAP HANA e il rilevamento automatico con SnapCenter versione 4.6 o superiore.
- Una singola risorsa SnapCenter per entrambi gli host SAP HANA che utilizzano un indirizzo IP virtuale.



A partire da SnapCenter 4.6, SnapCenter supporta il rilevamento automatico dei sistemi HANA configurati in una relazione di replica del sistema HANA. Ciascun host viene configurato utilizzando il proprio indirizzo IP fisico (nome host) e il proprio volume di dati sul layer di storage. Le due risorse SnapCenter sono combinate in un gruppo di risorse e SnapCenter identifica automaticamente l'host primario o secondario ed esegue le operazioni di backup richieste di conseguenza. La gestione della conservazione per Snapshot e backup basati su file creati da SnapCenter viene eseguita su entrambi gli host per garantire che i vecchi backup vengano cancellati anche sull'host secondario corrente.

Con una configurazione a singola risorsa per entrambi gli host SAP HANA, la singola risorsa SnapCenter viene configurata utilizzando l'indirizzo IP virtuale degli host di replica del sistema SAP HANA. Entrambi i volumi di dati degli host SAP HANA sono inclusi nella risorsa SnapCenter. Poiché si tratta di una singola risorsa SnapCenter, la gestione della conservazione per Snapshot e i backup basati su file creati da SnapCenter funziona indipendentemente dall'host attualmente primario o secondario. Queste opzioni sono possibili con tutte le versioni di SnapCenter.

La seguente tabella riassume le differenze principali delle due opzioni di configurazione.

	Gruppo di risorse con SnapCenter 4.6	Singola risorsa SnapCenter e indirizzo IP virtuale
Operazione di backup (Snapshot e basato su file)	Identificazione automatica dell'host primario nel gruppo di risorse	Utilizza automaticamente l'indirizzo IP virtuale
Gestione della conservazione (Snapshot e basato su file)	Eseguito automaticamente su entrambi gli host	Utilizza automaticamente una singola risorsa
Requisiti di capacità per il backup	I backup vengono creati solo sul volume host primario	I backup vengono sempre creati su entrambi i volumi host. Il backup del secondo host è coerente solo con il crash e non può essere utilizzato per eseguire un rollforward.

	Gruppo di risorse con SnapCenter 4.6	Singola risorsa SnapCenter e indirizzo IP virtuale
Ripristinare l'operazione	I backup dall'host attivo corrente sono disponibili per l'operazione di ripristino	Script di pre-backup necessario per identificare i backup validi e che possono essere utilizzati per il ripristino
Operazione di recovery	Tutte le opzioni di ripristino disponibili, come per qualsiasi risorsa rilevata automaticamente	Ripristino manuale richiesto



In generale, NetApp consiglia di utilizzare l'opzione di configurazione del gruppo di risorse con SnapCenter 4.6 per proteggere i sistemi HANA con la replica del sistema HANA abilitata. L'utilizzo di una singola configurazione delle risorse SnapCenter è necessario solo se l'approccio operativo SnapCenter è basato su un host plug-in centrale e il plug-in HANA non è distribuito sugli host del database HANA.

Le due opzioni sono descritte in dettaglio nelle sezioni seguenti.

Configurazione di SnapCenter 4.6 mediante un gruppo di risorse

SnapCenter 4.6 supporta il rilevamento automatico per i sistemi HANA configurati con la replica del sistema HANA. SnapCenter 4.6 include la logica per identificare gli host HANA primari e secondari durante le operazioni di backup e gestisce anche la gestione della conservazione su entrambi gli host HANA. Inoltre, il ripristino e il ripristino automatici sono ora disponibili anche per gli ambienti di replica del sistema HANA.

Configurazione di SnapCenter 4.6 per gli ambienti di replica del sistema HANA

La figura seguente mostra la configurazione di laboratorio utilizzata per questo capitolo. Due host HANA, hana-3 e hana-4, sono stati configurati con la replica di sistema HANA.

È stato creato un utente di database "SnapCenter" per il database di sistema HANA con i privilegi necessari per eseguire le operazioni di backup e ripristino (vedere ["Backup e ripristino SAP HANA con SnapCenter"](#)). È necessario configurare una chiave di memorizzazione utente HANA su entrambi gli host utilizzando l'utente del database indicato sopra.

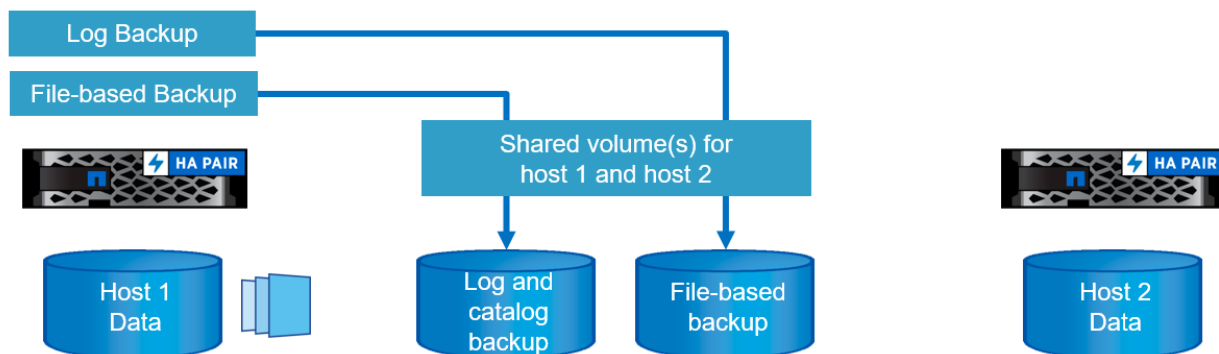
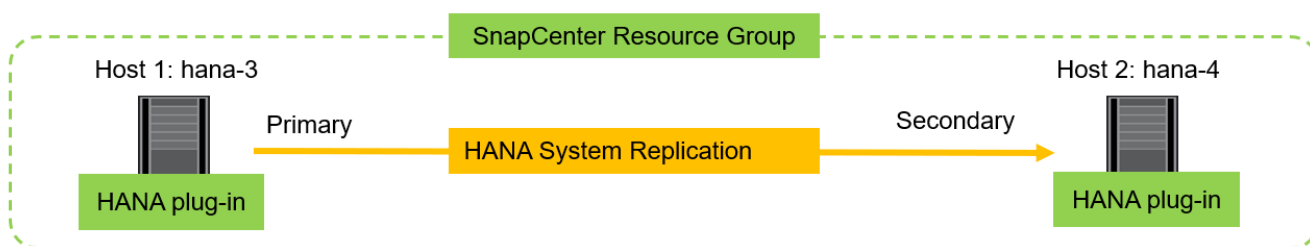
```
ss2adm@hana- 3: / > hdbuserstore set SS2KEY hana- 3:33313 SNAPCENTER
<password>
```

```
ss2adm@hana- 4:/ > hdbuserstore set SS2KEY hana-4:33313 SNAPCENTER
<password>
```

Da un punto di vista di alto livello, è necessario eseguire i seguenti passaggi per configurare la replica del sistema HANA in SnapCenter.

1. Installare il plug-in HANA sull'host primario e secondario. Viene eseguita la rilevazione automatica e viene rilevato lo stato di replica del sistema HANA per ogni host primario o secondario.

2. Eseguire SnapCenter `configure database` e fornire il `hdbuserstore` chiave. Vengono eseguite ulteriori operazioni di rilevamento automatico.
3. Creare un gruppo di risorse, inclusi entrambi gli host e configurare la protezione.



Dopo aver installato il plug-in HANA di SnapCenter su entrambi gli host HANA, i sistemi HANA vengono visualizzati nella vista delle risorse di SnapCenter allo stesso modo delle altre risorse rilevate automaticamente. A partire da SnapCenter 4.6, viene visualizzata una colonna aggiuntiva che mostra lo stato della replica del sistema HANA (attivata/disattivata, primaria/secondaria).

NetApp SnapCenter®									
SAP HANA									
View: Multitenant Database Container Search databases									
	System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
	SS2	SS2	SS2	Enabled (Primary)	hana-3.sapcc.stl.netapp.com				Not protected
	SS2	SS2	SS2	Enabled (Secondary)	hana-4.sapcc.stl.netapp.com				Not protected

Facendo clic sulla risorsa, SnapCenter richiede la chiave di archivio utente HANA per il sistema HANA.

Configure Database

✕

Plug-in host

hana-3.sapcc.stl.netapp.com

HDBSQL OS User

ss2adm

HDB Secure User Store Key

SS2KEY

?

Cancel

OK

Vengono eseguite ulteriori operazioni di rilevamento automatico e SnapCenter mostra i dettagli delle risorse. In SnapCenter 4.6, lo stato della replica del sistema e il server secondario sono elencati in questa vista.

NetApp SnapCenter

SAP HANA

Search databases

System

SS2

SS2

Total 2

Resource - Details

Details for selected resource

Type

Multitenant Database Container

HANA System Name

SS2

SID

SS2

Tenant Databases

SS2

Plug-in Host

hana-3.sapcc.stl.netapp.com

HDB Secure User Store Key

SS2KEY

HDBSQL OS User

ss2adm

Log backup location

/mnt/backup/SS2

Backup catalog location

/mnt/backup/SS2

System Replication

Enabled (Primary)

Secondary Servers

hana-4

plug-in name

SAP HANA

Last backup

None

Resource Groups

None

Policy

None

Discovery Type

Auto

Storage Footprint

SVM	Volume	Junction Path	LUN/Qtree
hana-primary.sapcc.stl.netapp.com	SS2_data_mnt00001	/SS2_data_mnt00001	

Activity

The 5 most recent jobs are displayed

0 Completed

0 Warnings

0 Failed

0 Canceled

0 Running

0 Queued

Dopo aver eseguito le stesse operazioni per la seconda risorsa HANA, il processo di individuazione automatica è completo e entrambe le risorse HANA sono configurate in SnapCenter.

NetApp SnapCenter

SAP HANA

View Multitenant Database Container

Search databases

Resources

Monitor

Reports

Hosts

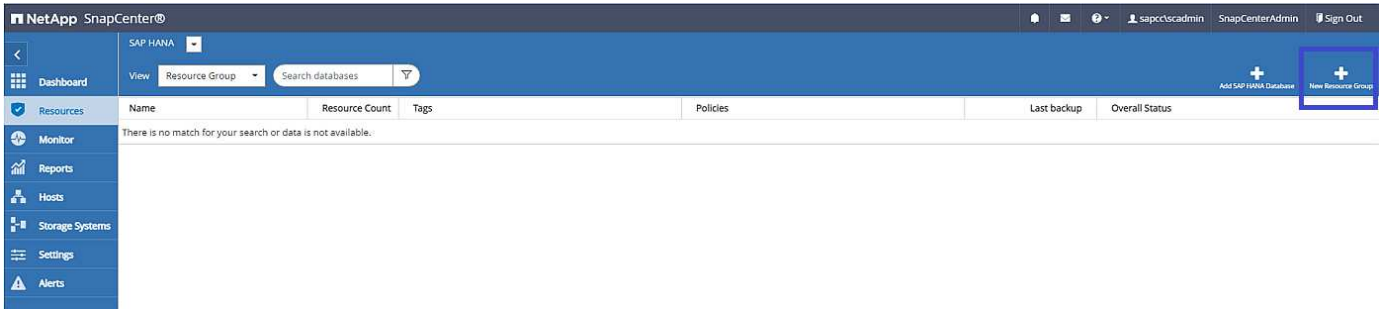
Storage Systems

Settings

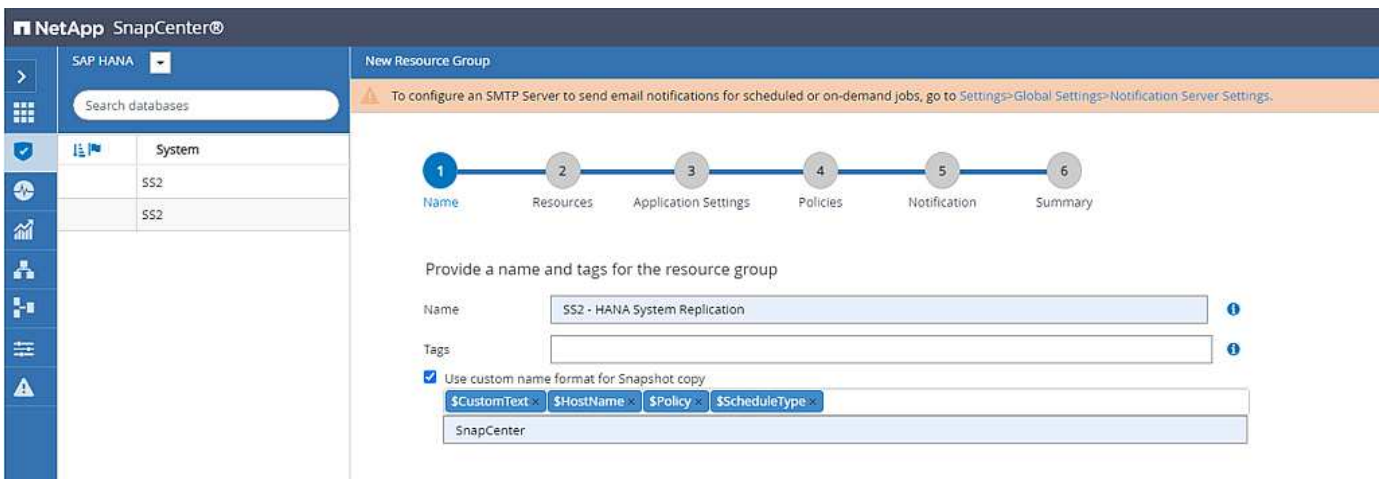
Alerts

System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
SS2	SS2	SS2	Enabled (Primary)	hana-3.sapcc.stl.netapp.com				Not protected
SS2	SS2	SS2	Enabled (Secondary)	hana-4.sapcc.stl.netapp.com				Not protected

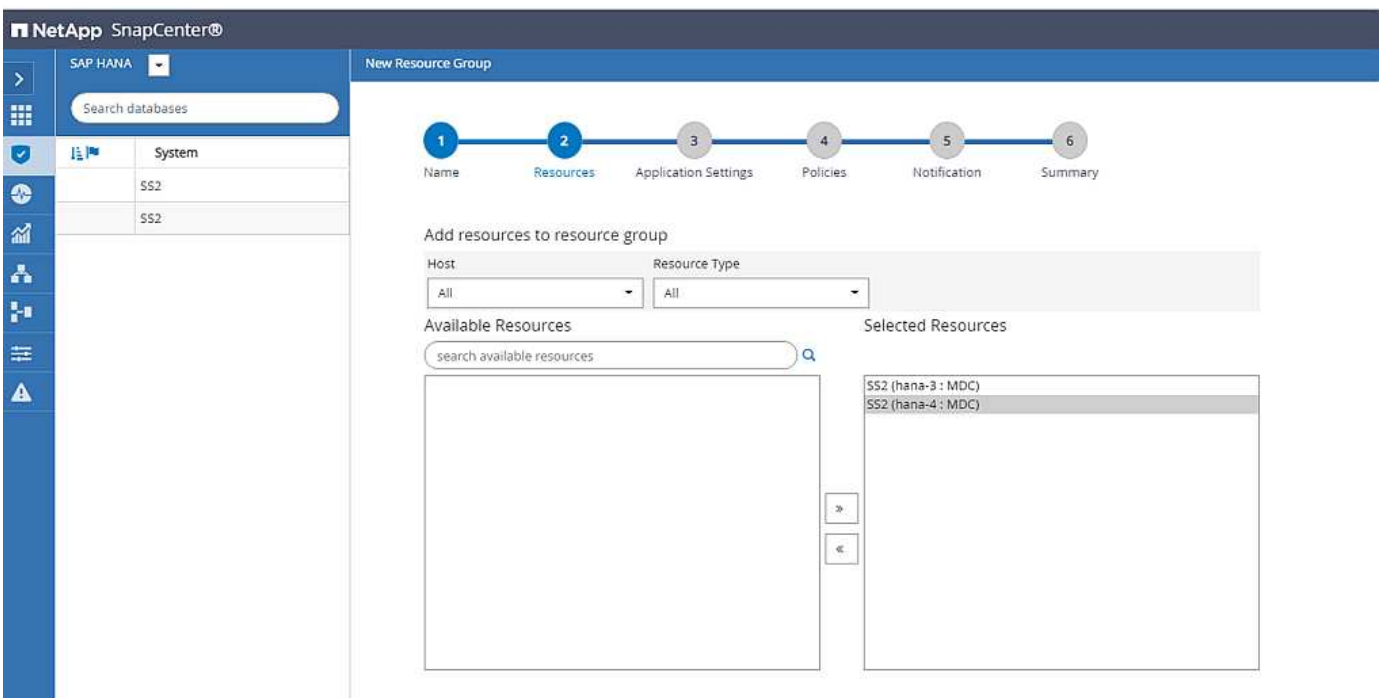
Per i sistemi abilitati alla replica del sistema HANA, è necessario configurare un gruppo di risorse SnapCenter, incluse entrambe le risorse HANA.



NetApp consiglia di utilizzare un formato nome personalizzato per il nome Snapshot, che deve includere il nome host, la policy e la pianificazione.



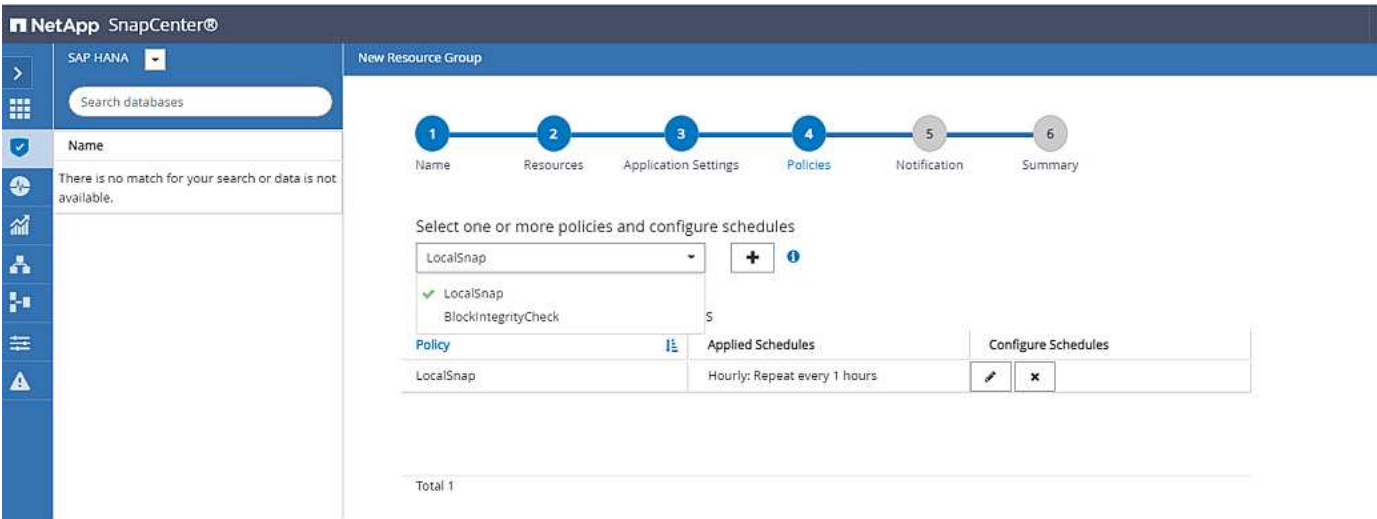
È necessario aggiungere entrambi gli host HANA al gruppo di risorse.



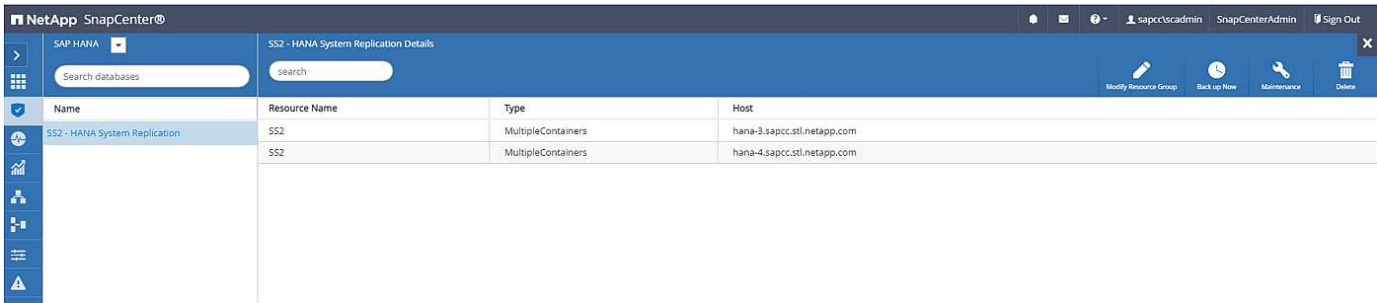
I criteri e le pianificazioni vengono configurati per il gruppo di risorse.



La conservazione definita nel criterio viene utilizzata in entrambi gli host HANA. Se, ad esempio, nel criterio viene definita una conservazione di 10, la somma dei backup di entrambi gli host viene utilizzata come criterio per l'eliminazione del backup. SnapCenter elimina il backup meno recente indipendentemente se è stato creato sull'host primario o secondario corrente.

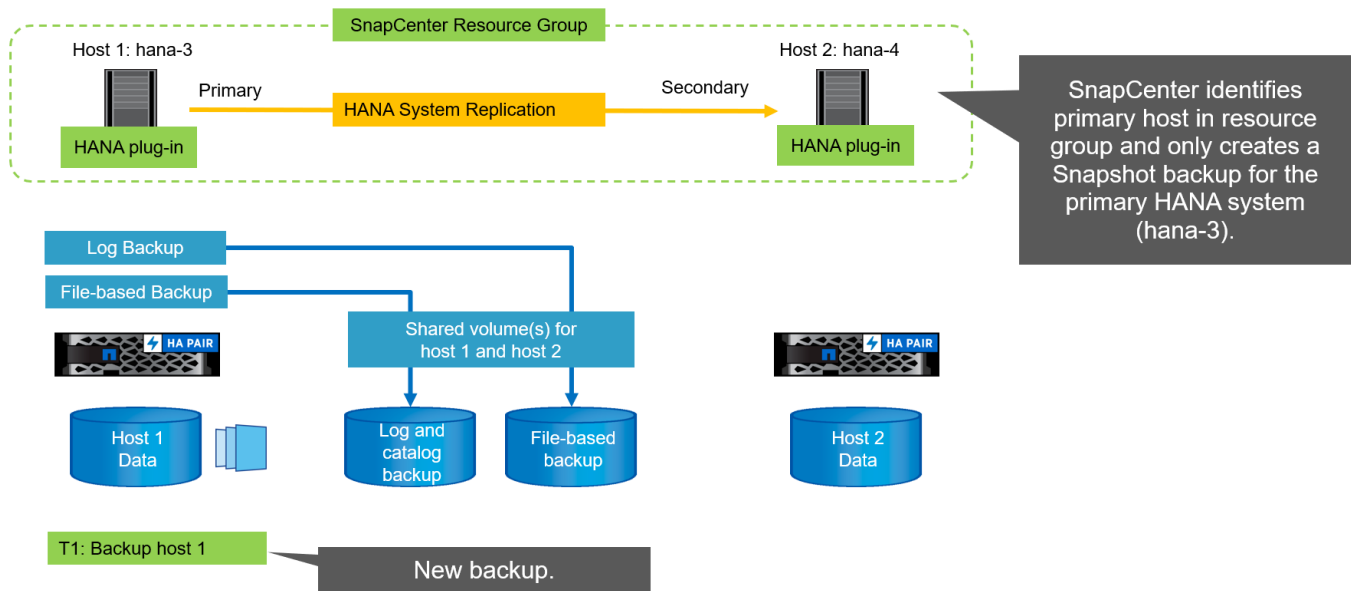


La configurazione del gruppo di risorse è terminata ed è possibile eseguire i backup.

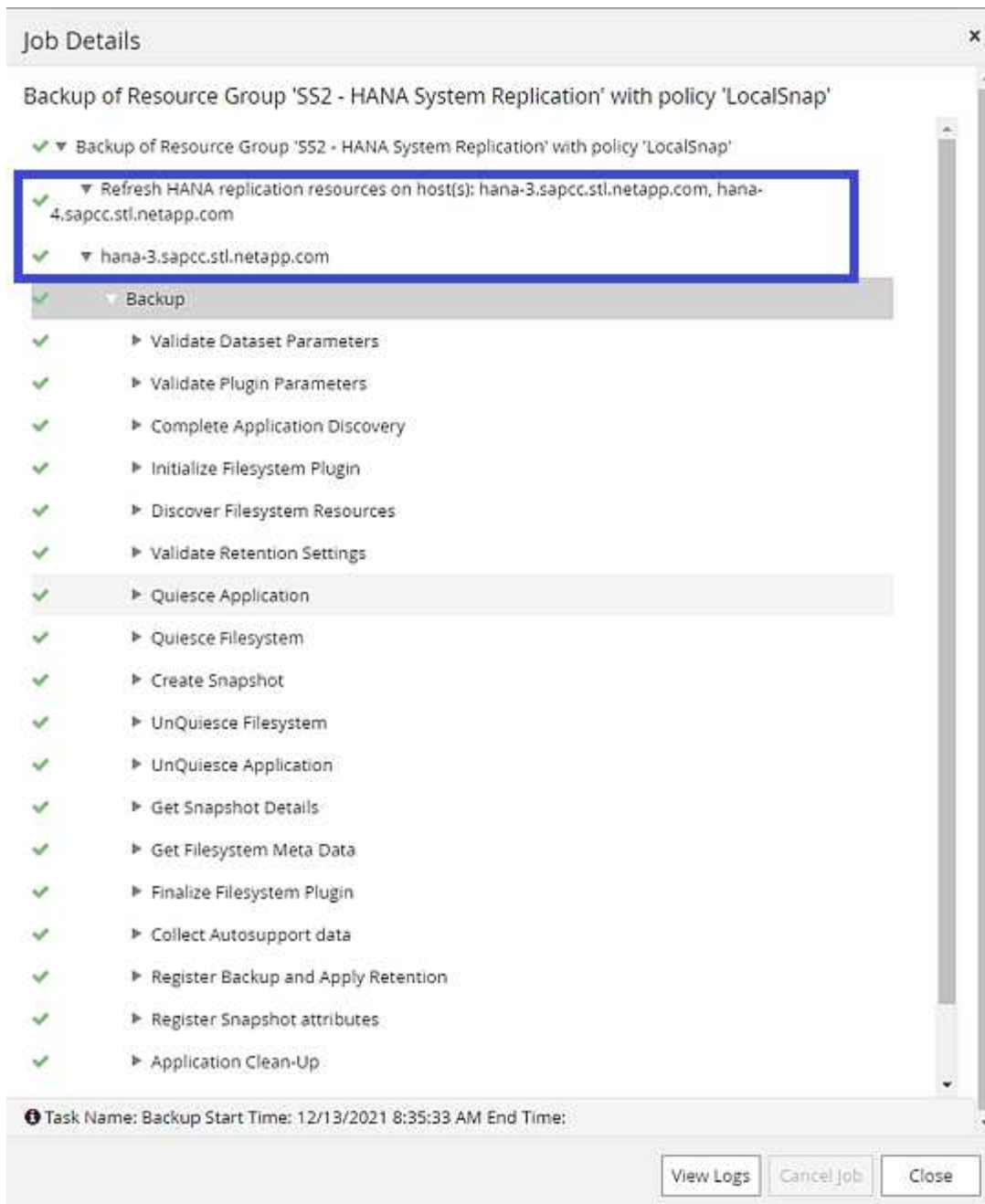


Operazioni di backup di Snapshot

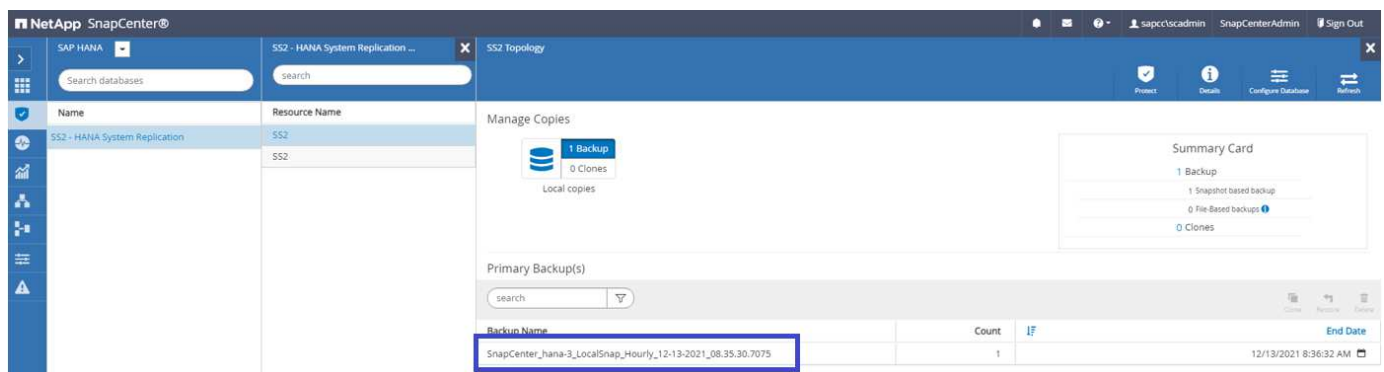
Quando viene eseguita un'operazione di backup del gruppo di risorse, SnapCenter identifica l'host primario e attiva un backup solo sull'host primario. In questo modo, verrà attivato lo snap-shoting solo del volume di dati dell'host primario. Nel nostro esempio, hana-3 è l'host primario corrente e viene eseguito un backup su questo host.



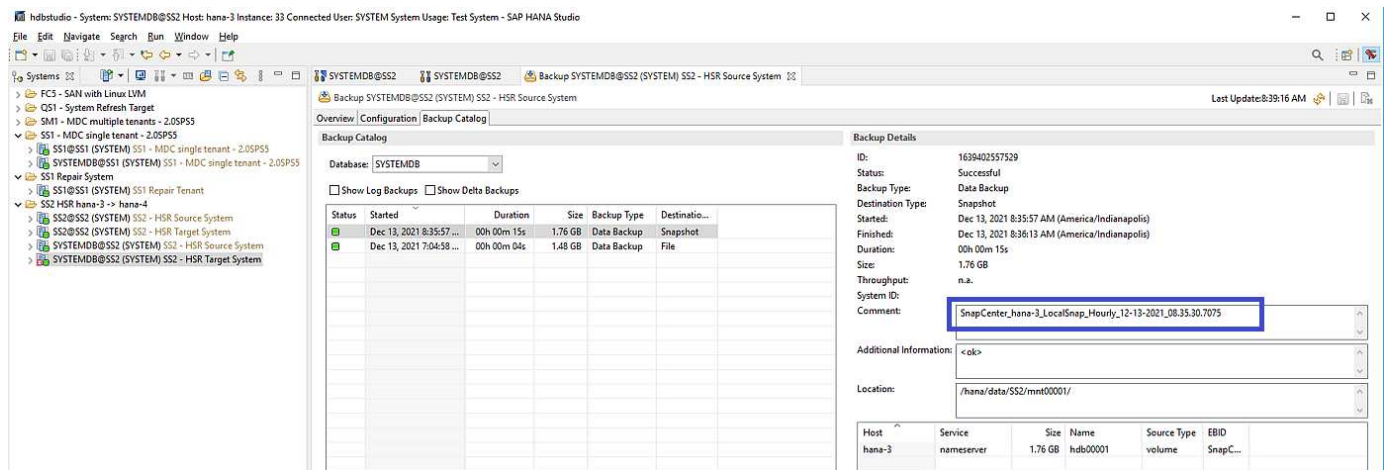
Il log dei lavori di SnapCenter mostra l'operazione di identificazione e l'esecuzione del backup sull'host primario corrente hana-3.



È stato creato un backup Snapshot nella risorsa HANA principale. Il nome host incluso nel nome del backup mostra hana-3.



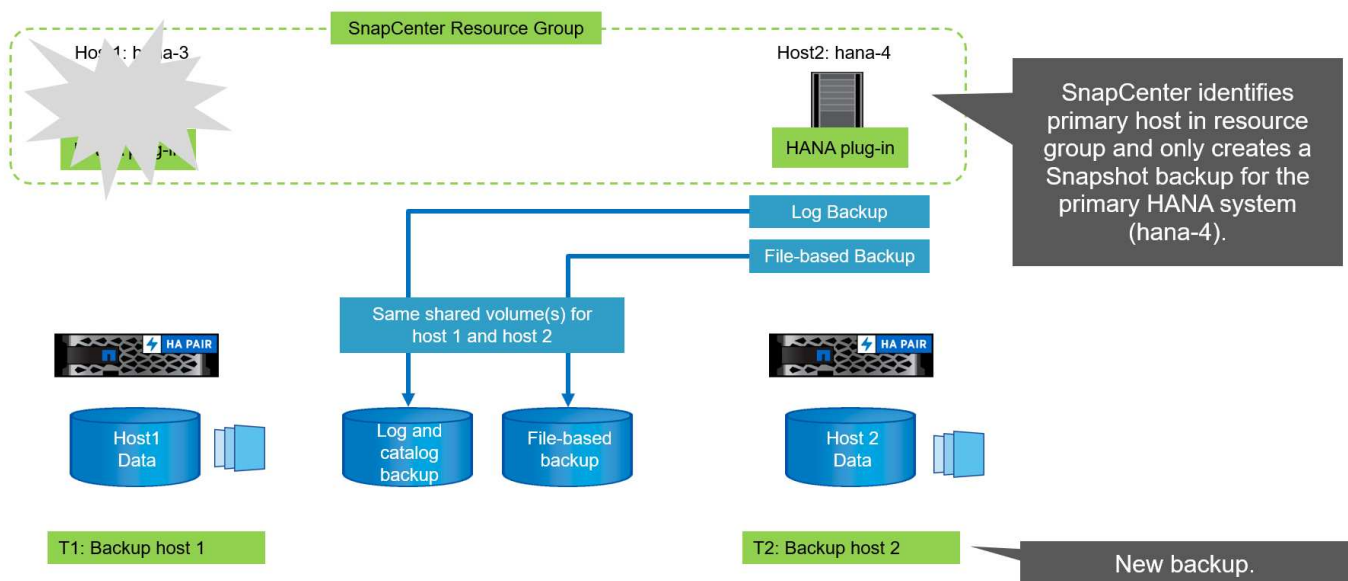
Lo stesso backup Snapshot è anche visibile nel catalogo di backup HANA.



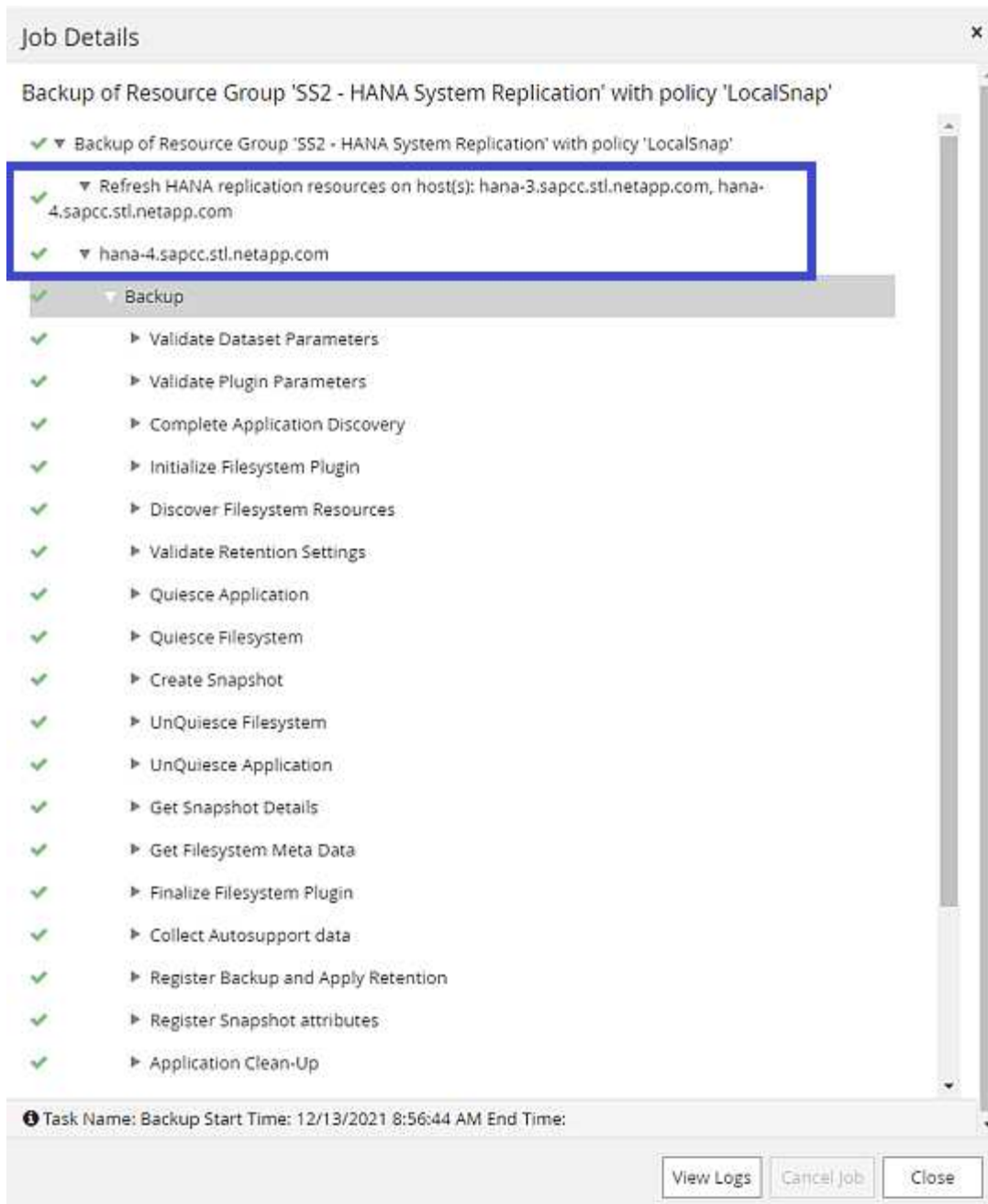
Se viene eseguita un'operazione di Takeover, ulteriori backup SnapCenter identificano ora il precedente host secondario (hana-4) come primario e l'operazione di backup viene eseguita in hana-4. Anche in questo caso, viene attivato solo il volume di dati del nuovo host primario (hana-4).



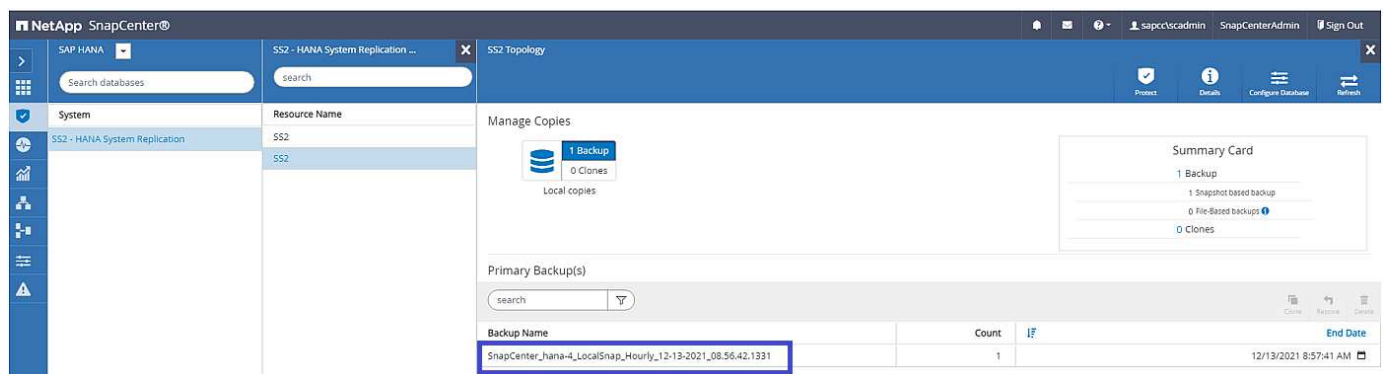
La logica di identificazione SnapCenter copre solo gli scenari in cui gli host HANA si trovano in una relazione primaria-secondaria o quando uno degli host HANA è offline.



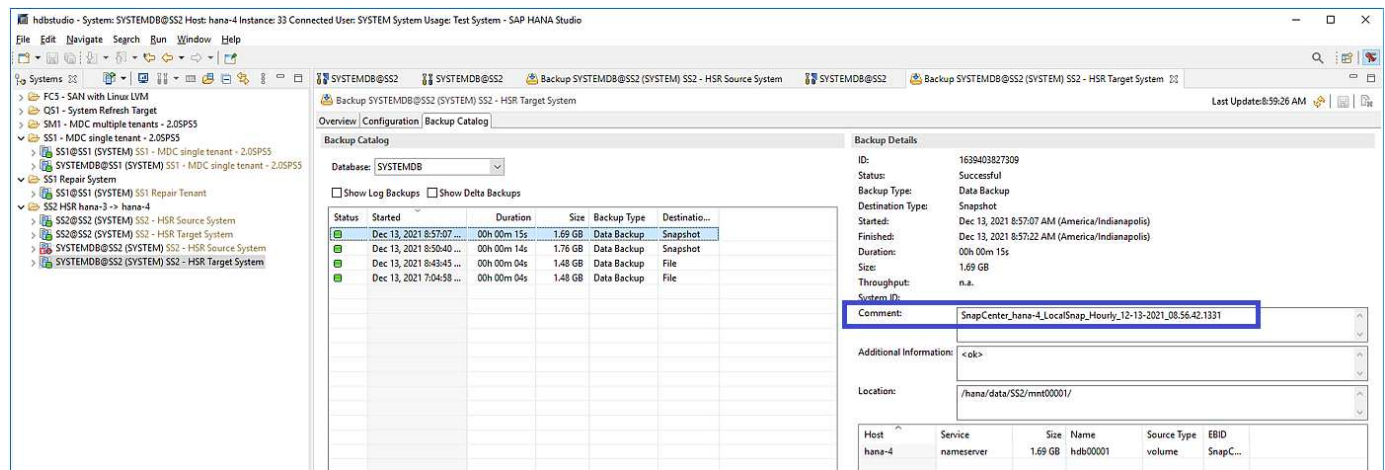
Il log dei lavori di SnapCenter mostra l'operazione di identificazione e l'esecuzione del backup sull'host primario corrente hana-4.



È stato creato un backup Snapshot nella risorsa HANA principale. Il nome host incluso nel nome del backup mostra hana-4.



Lo stesso backup Snapshot è anche visibile nel catalogo di backup HANA.



Operazioni di controllo dell'integrità dei blocchi con backup basati su file

SnapCenter 4.6 utilizza la stessa logica descritta per le operazioni di backup Snapshot per le operazioni di controllo dell'integrità dei blocchi con backup basati su file. SnapCenter identifica l'host HANA primario corrente ed esegue il backup basato su file per questo host. La gestione della conservazione viene eseguita anche su entrambi gli host, in modo che il backup più vecchio venga cancellato indipendentemente dall'host attualmente primario.

Replica SnapVault

Per consentire operazioni di backup trasparenti senza l'interazione manuale in caso di Takeover e indipendentemente da quale host HANA sia attualmente l'host primario, è necessario configurare una relazione SnapVault per i volumi di dati di entrambi gli host. SnapCenter esegue un'operazione di aggiornamento del SnapVault per l'host primario corrente ad ogni esecuzione del backup.

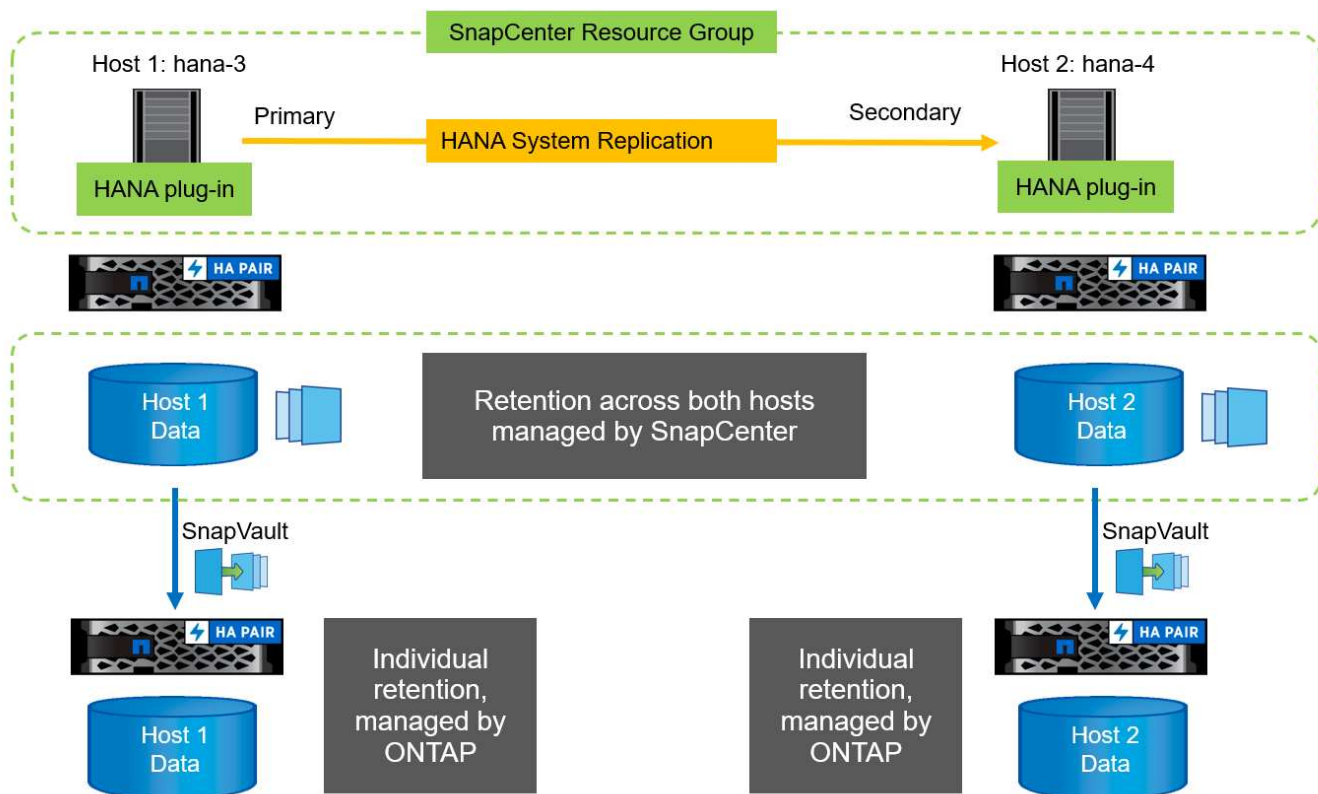


Se un takeover all'host secondario non viene eseguito per molto tempo, il numero di blocchi modificati per il primo aggiornamento SnapVault sull'host secondario sarà elevato.

Poiché la gestione della conservazione presso la destinazione SnapVault viene gestita da ONTAP al di fuori di SnapCenter, la conservazione non può essere gestita su entrambi gli host HANA. Pertanto, i backup creati prima di un Takeover non vengono cancellati con le operazioni di backup sul precedente secondario. Questi backup rimangono fino a quando il primo primario non diventa nuovamente primario. Affinché questi backup non blocchino la gestione della conservazione dei backup dei log, devono essere eliminati manualmente nella destinazione SnapVault o all'interno del catalogo di backup HANA.



Non è possibile eseguire la pulizia di tutte le copie Snapshot di SnapVault, poiché una copia Snapshot viene bloccata come punto di sincronizzazione. Se è necessario eliminare anche la copia Snapshot più recente, è necessario eliminare la relazione di replica SnapVault. In questo caso, NetApp consiglia di eliminare i backup nel catalogo di backup HANA per sbloccare la gestione della conservazione dei backup dei log.



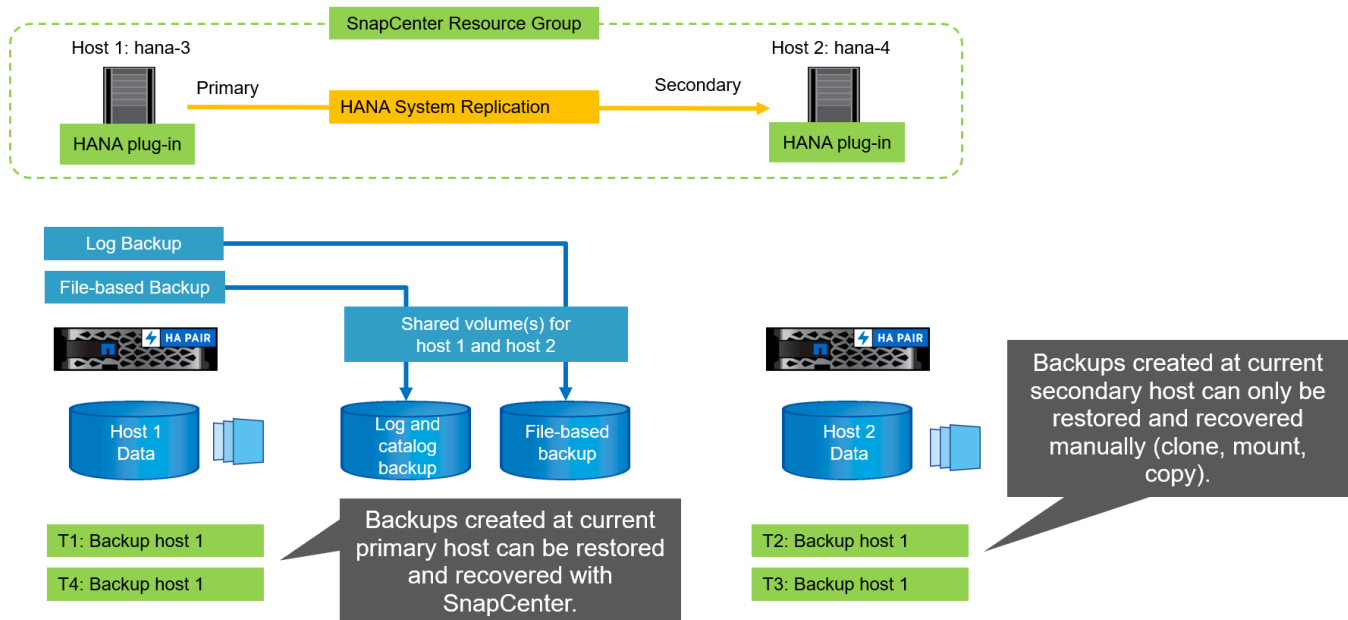
Gestione della conservazione

SnapCenter 4.6 gestisce la conservazione per i backup Snapshot, le operazioni di controllo dell'integrità dei blocchi, le voci del catalogo di backup HANA e i backup dei log (se non disattivati) su entrambi gli host HANA, quindi non importa quale host sia attualmente primario o secondario. I backup (dati e log) e le voci del catalogo HANA vengono cancellati in base alla conservazione definita, indipendentemente dal fatto che sia necessaria un'operazione di eliminazione sull'host primario o secondario corrente. In altre parole, non è richiesta alcuna interazione manuale se viene eseguita un'operazione di Takeover e/o la replica viene configurata nell'altra direzione.

Se la replica di SnapVault fa parte della strategia di protezione dei dati, è necessaria un'interazione manuale per scenari specifici, come descritto nella sezione [\[SnapVault Replication\]](#).

Ripristino e ripristino

La figura seguente mostra uno scenario in cui sono stati eseguiti più takeover e sono stati creati backup Snapshot in entrambi i siti. Con lo stato corrente, l'host hana-3 è l'host primario e l'ultimo backup è T4, creato sull'host hana-3. Se è necessario eseguire un'operazione di ripristino e ripristino, i backup T1 e T4 sono disponibili per il ripristino e il ripristino in SnapCenter. I backup creati sull'host hana-4 (T2, T3) non possono essere ripristinati utilizzando SnapCenter. Questi backup devono essere copiati manualmente nel volume di dati di hana-3 per il ripristino.



Le operazioni di ripristino e ripristino per una configurazione del gruppo di risorse di SnapCenter 4.6 sono identiche a quelle di una configurazione della replica non di sistema rilevata automaticamente. Sono disponibili tutte le opzioni per il ripristino e il ripristino automatizzato. Per ulteriori dettagli, consultare il report tecnico "[TR-4614: Backup e ripristino SAP HANA con SnapCenter](#)".

Nella sezione viene descritta un'operazione di ripristino da un backup creato sull'altro host "[Ripristino e ripristino da un backup creato sull'altro host](#)".

Configurazione di SnapCenter con una singola risorsa

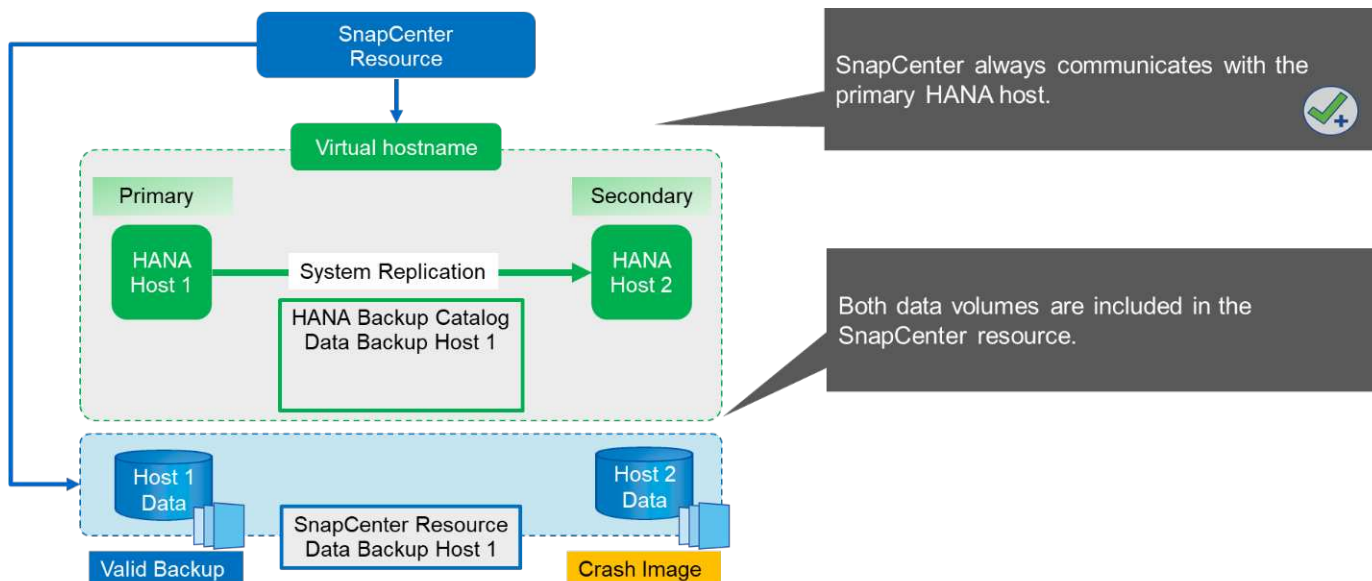
Una risorsa SnapCenter viene configurata con l'indirizzo IP virtuale (nome host) dell'ambiente di replica del sistema HANA. Con questo approccio, SnapCenter comunica sempre con l'host primario, indipendentemente dal fatto che l'host 1 o l'host 2 sia primario. I volumi di dati di entrambi gli host SAP HANA sono inclusi nella risorsa SnapCenter.



Si presuppone che l'indirizzo IP virtuale sia sempre associato all'host SAP HANA primario. Il failover dell'indirizzo IP virtuale viene eseguito all'esterno di SnapCenter come parte del workflow di failover della replica del sistema HANA.

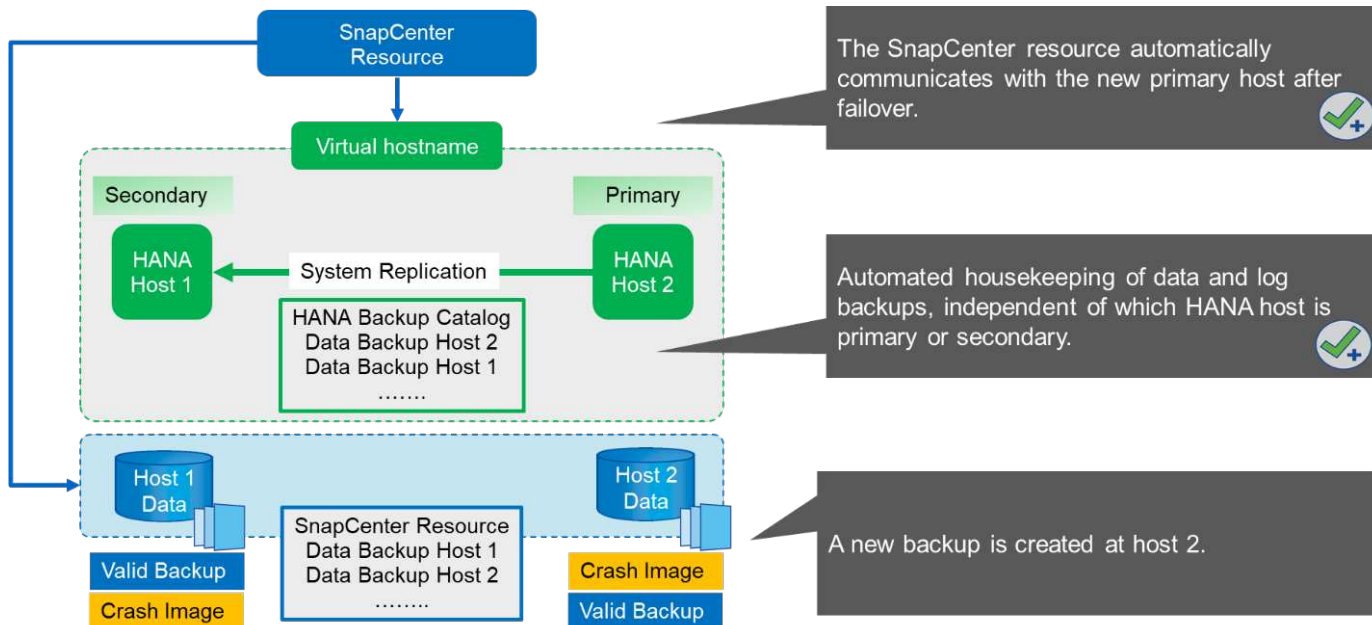
Quando viene eseguito un backup con host 1 come host primario, viene creato un backup Snapshot coerente con il database nel volume di dati dell'host 1. Poiché il volume di dati dell'host 2 fa parte della risorsa SnapCenter, viene creata un'altra copia Snapshot per questo volume. Questa copia Snapshot non è coerente con il database, ma è solo un'immagine di crash dell'host secondario.

Il catalogo di backup SAP HANA e la risorsa SnapCenter includono il backup creato sull'host 1.



La figura seguente mostra l'operazione di backup dopo il failover sull'host 2 e la replica dall'host 2 all'host 1. SnapCenter comunica automaticamente con l'host 2 utilizzando l'indirizzo IP virtuale configurato nella risorsa SnapCenter. I backup vengono ora creati sull'host 2. SnapCenter crea due copie Snapshot: Un backup coerente con il database nel volume di dati dell'host 2 e una copia Snapshot dell'immagine di crash nel volume di dati dell'host 1. Il catalogo di backup SAP HANA e la risorsa SnapCenter ora includono il backup creato sull'host 1 e il backup creato sull'host 2.

La gestione dei backup dei dati e dei log si basa sulla policy di conservazione di SnapCenter definita e i backup vengono cancellati indipendentemente dall'host primario o secondario.

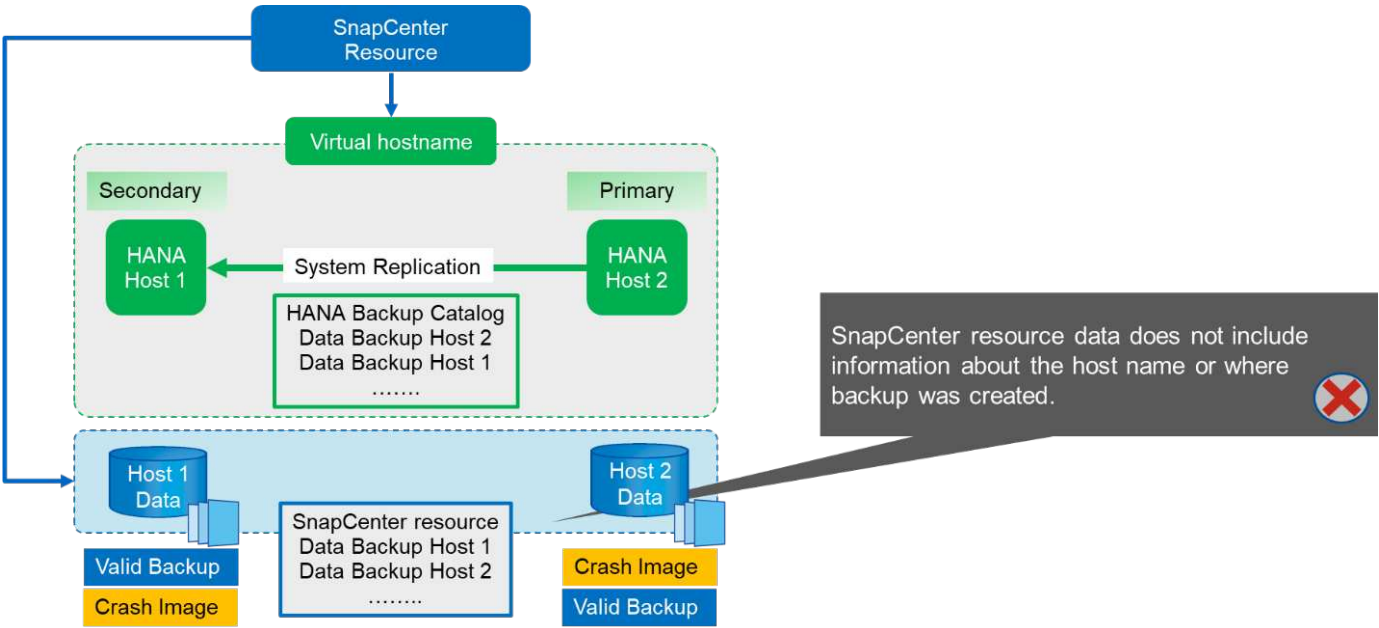


Come discusso nella sezione "[Backup Snapshot dello storage e replica del sistema SAP](#)", Un'operazione di ripristino con backup Snapshot basati sullo storage è diversa, a seconda del backup da ripristinare. È importante identificare l'host in cui è stato creato il backup per determinare se il ripristino può essere eseguito sul volume di storage locale o se il ripristino deve essere eseguito sul volume di storage dell'altro host.

Con la configurazione SnapCenter a singola risorsa, SnapCenter non è a conoscenza della posizione in cui è stato creato il backup. Pertanto, NetApp consiglia di aggiungere uno script di prebackup al workflow di backup

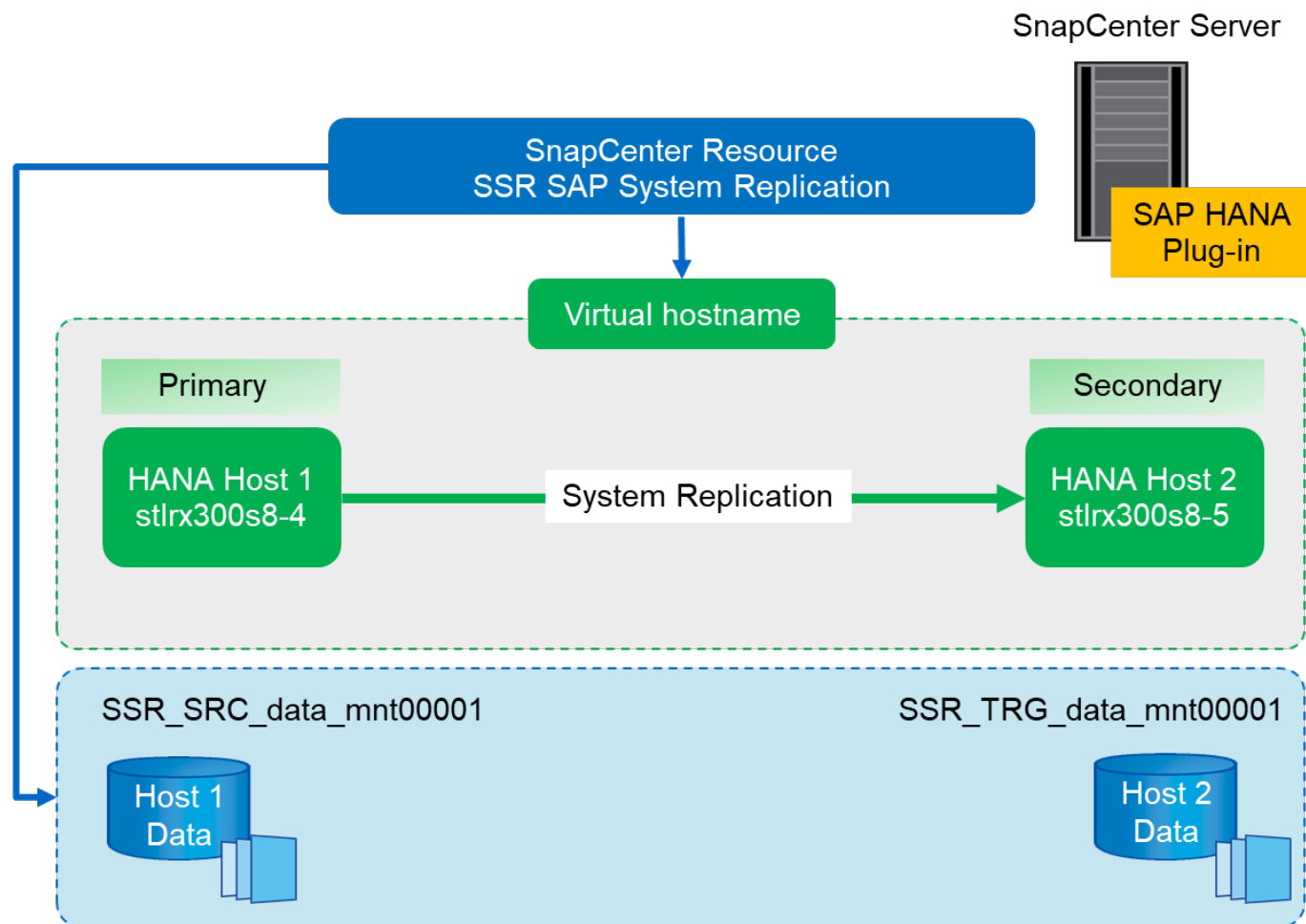
di SnapCenter per identificare quale host è attualmente l'host SAP HANA primario.

La figura seguente mostra l'identificazione dell'host di backup.



Configurazione di SnapCenter

La figura seguente mostra la configurazione di laboratorio e una panoramica della configurazione SnapCenter richiesta.



Per eseguire operazioni di backup indipendentemente dall'host SAP HANA primario e anche quando un host è inattivo, il plug-in SAP HANA di SnapCenter deve essere implementato su un host plug-in centrale. Nella nostra configurazione di laboratorio, abbiamo utilizzato il server SnapCenter come host plug-in centrale e abbiamo implementato il plug-in SAP HANA sul server SnapCenter.

Nel database HANA è stato creato un utente per eseguire operazioni di backup. Una chiave di archivio utente è stata configurata sul server SnapCenter su cui è stato installato il plug-in SAP HANA. La chiave dell'archivio utente include l'indirizzo IP virtuale degli host di replica del sistema SAP HANA (`ssr-vip`).

```
hdbuserstore.exe -u SYSTEM set SSRKEY ssr-vip:31013 SNAPCENTER <password>
```

Per ulteriori informazioni sulle opzioni di implementazione del plug-in SAP HANA e sulla configurazione dell'archivio utenti, consultare il report tecnico TR-4614: ["Backup e ripristino SAP HANA con SnapCenter"](#).

In SnapCenter, la risorsa viene configurata come mostrato nella figura seguente utilizzando la chiave di memorizzazione utente, configurata in precedenza, e il server SnapCenter come `hdbsql` host di comunicazione.

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Resource Details

☐ Single Container

☒ Multitenant Database Container (MDC) - Single Tenant

☐ Non-data Volumes

Resource Type

HANA System Name

SSR - SAP System Replication

SID

SSR

Tenant Database

SSR

HDBSQL Client Host

SC30-V2.sapcc.stl.netapp.com

HDB Secure User Store Keys

SSRKEY

HDBSQL OS User

SYSTEM

Previous

Next

I volumi di dati di entrambi gli host SAP HANA sono inclusi nella configurazione del footprint dello storage, come mostrato nella figura seguente.

256

Add SAP HANA Database

1 Name
2 **Storage Footprint**
3 Resource Settings
4 Summary

Provide Storage Footprint Details

Storage Systems for storage footprint

hana

Modify hana

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

Volume Name

SSR_TRG_data_mnt00001

SSR_SRC_data_mnt00001

LUNs or Qtrees

Default is 'None' or type to find

Default is 'None' or type to find

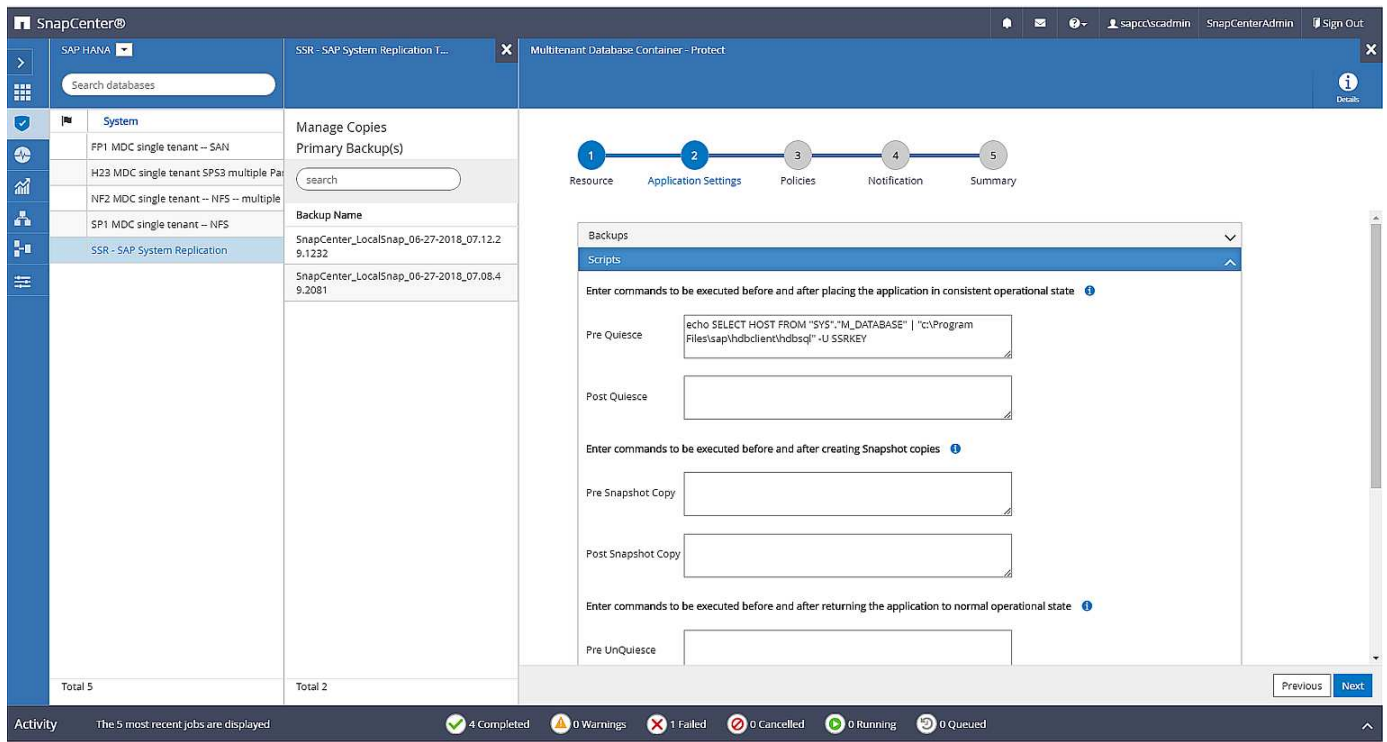
Save

Previous

Next

Come discusso in precedenza, SnapCenter non è a conoscenza della posizione in cui è stato creato il backup. NetApp consiglia pertanto di aggiungere uno script di pre-backup nel flusso di lavoro di backup di SnapCenter per identificare quale host è attualmente l'host SAP HANA primario. È possibile eseguire questa identificazione utilizzando un'istruzione SQL aggiunta al flusso di lavoro di backup, come illustrato nella figura seguente.

```
Select host from "SYS".M_DATABASE
```

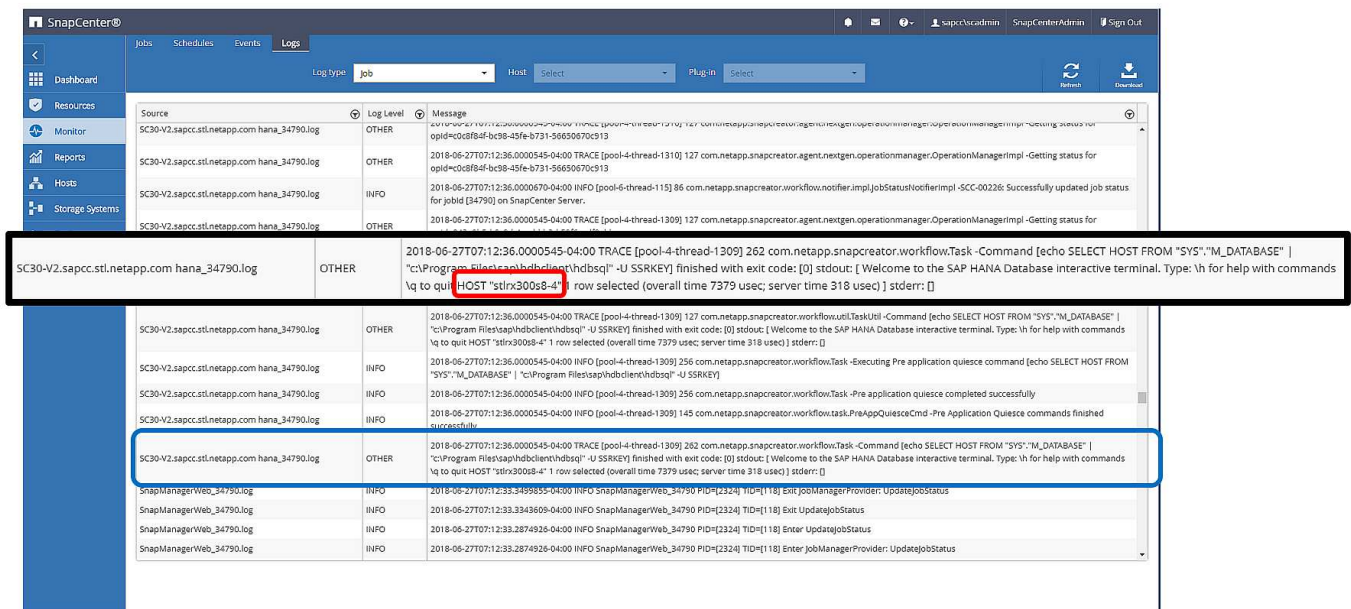



Operazione di backup di SnapCenter

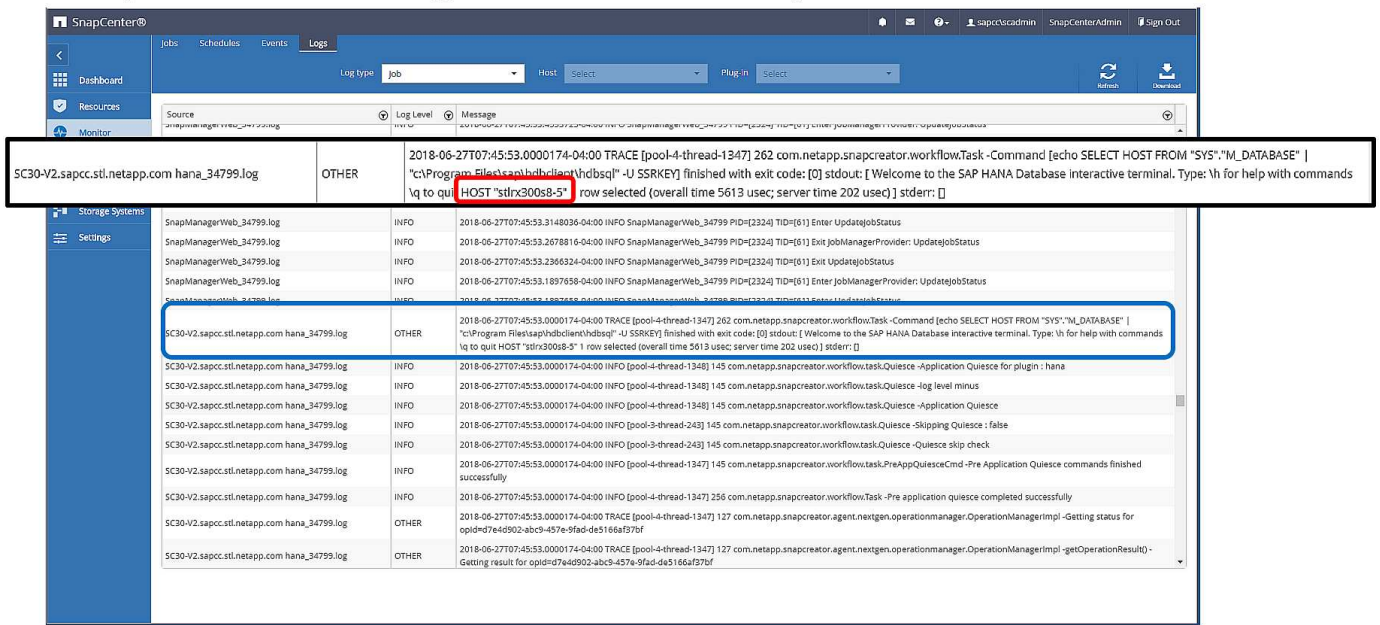
Le operazioni di backup vengono ora eseguite come di consueto. La gestione dei backup dei dati e dei log viene eseguita indipendentemente dall'host SAP HANA primario o secondario.

I log dei processi di backup includono l'output dell'istruzione SQL, che consente di identificare l'host SAP HANA in cui è stato creato il backup.

La figura seguente mostra il log del processo di backup con l'host 1 come host primario.



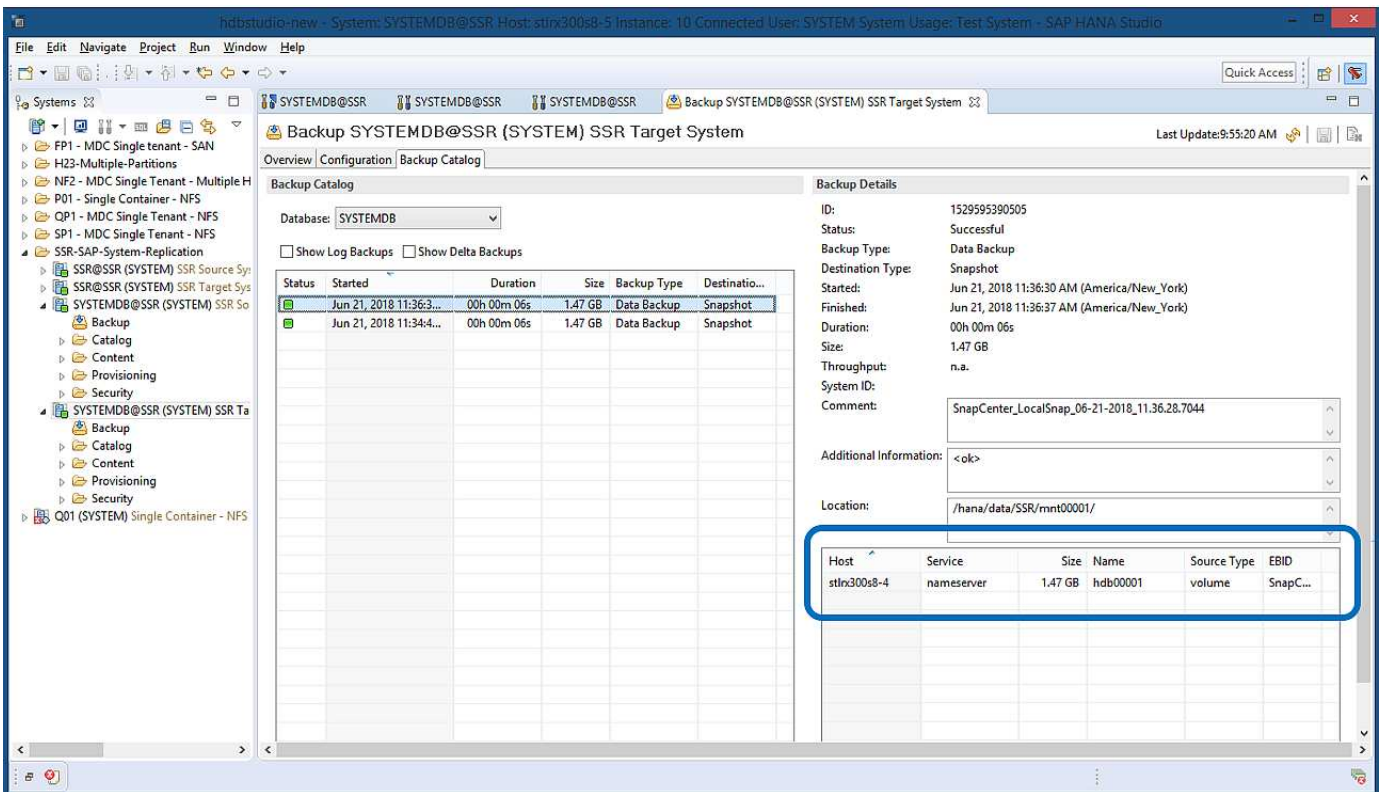
Questa figura mostra il log del processo di backup con l'host 2 come host primario.



La figura seguente mostra il catalogo di backup SAP HANA in SAP HANA Studio. Quando il database SAP HANA è online, l'host SAP HANA in cui è stato creato il backup è visibile in SAP HANA Studio.



Il catalogo di backup SAP HANA sul file system, utilizzato durante un'operazione di ripristino e ripristino, non include il nome host in cui è stato creato il backup. L'unico modo per identificare l'host quando il database è inattivo consiste nel combinare le voci del catalogo di backup con backup.log File di entrambi gli host SAP HANA.



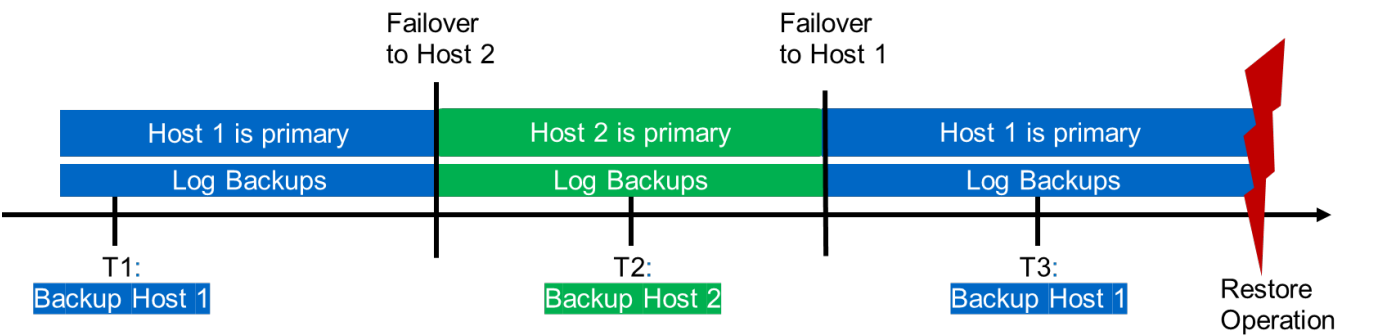
Ripristino e ripristino

Come discusso in precedenza, è necessario essere in grado di identificare la posizione in cui è stato creato il backup selezionato per definire l’operazione di ripristino richiesta. Se il database SAP HANA è ancora online, è possibile utilizzare SAP HANA Studio per identificare l’host in cui è stato creato il backup. Se il database non è in linea, le informazioni sono disponibili solo nel log del processo di backup di SnapCenter.

La figura seguente illustra le diverse operazioni di ripristino a seconda del backup selezionato.

Se è necessario eseguire un’operazione di ripristino dopo l’indicazione di data e ora T3 e l’host 1 è il principale, è possibile ripristinare il backup creato in T1 o T3 utilizzando SnapCenter. Questi backup Snapshot sono disponibili nel volume di storage collegato all’host 1.

Se è necessario eseguire il ripristino utilizzando il backup creato nell’host 2 (T2), ovvero una copia Snapshot nel volume di storage dell’host 2, il backup deve essere reso disponibile per l’host 1. È possibile rendere disponibile questo backup creando una copia di NetApp FlexClone dal backup, montando la copia di FlexClone sull’host 1 e copiando i dati nella posizione originale.



Restore Operation With	
Backup T1	SnapCenter
Backup T2	Create FlexClone from „Backup host 2“, mount and copy
Backup T3	SnapCenter

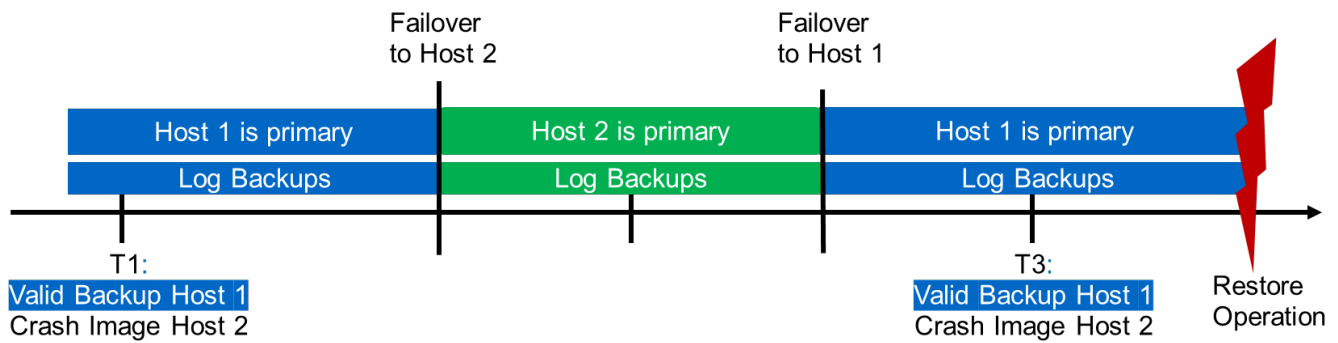
Con una singola configurazione delle risorse SnapCenter, le copie Snapshot vengono create su entrambi i volumi di storage di entrambi gli host di replica del sistema SAP HANA. Solo il backup Snapshot creato nel volume di storage dell’host SAP HANA primario è valido per il forward recovery. La copia Snapshot creata nel volume di storage dell’host SAP HANA secondario è un’immagine di crash che non può essere utilizzata per il forward recovery.

Un’operazione di ripristino con SnapCenter può essere eseguita in due modi diversi:

- Ripristinare solo il backup valido
- Ripristinare la risorsa completa, incluso il backup valido e l’immagine del crash.le sezioni seguenti illustrano in dettaglio le due diverse operazioni di ripristino.

Nella sezione viene descritta un’operazione di ripristino da un backup creato sull’altro host "[Ripristino e ripristino da un backup creato sull’altro host](#)".

La figura seguente illustra le operazioni di ripristino con una singola configurazione delle risorse SnapCenter.

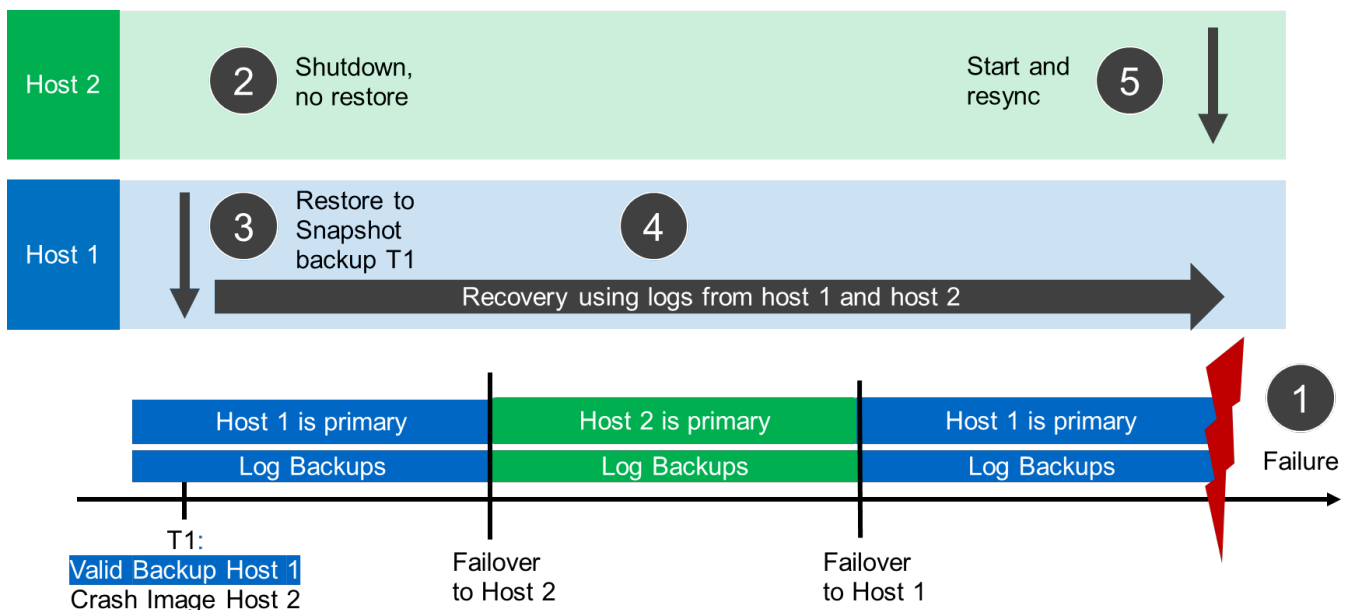


Ripristino SnapCenter solo del backup valido

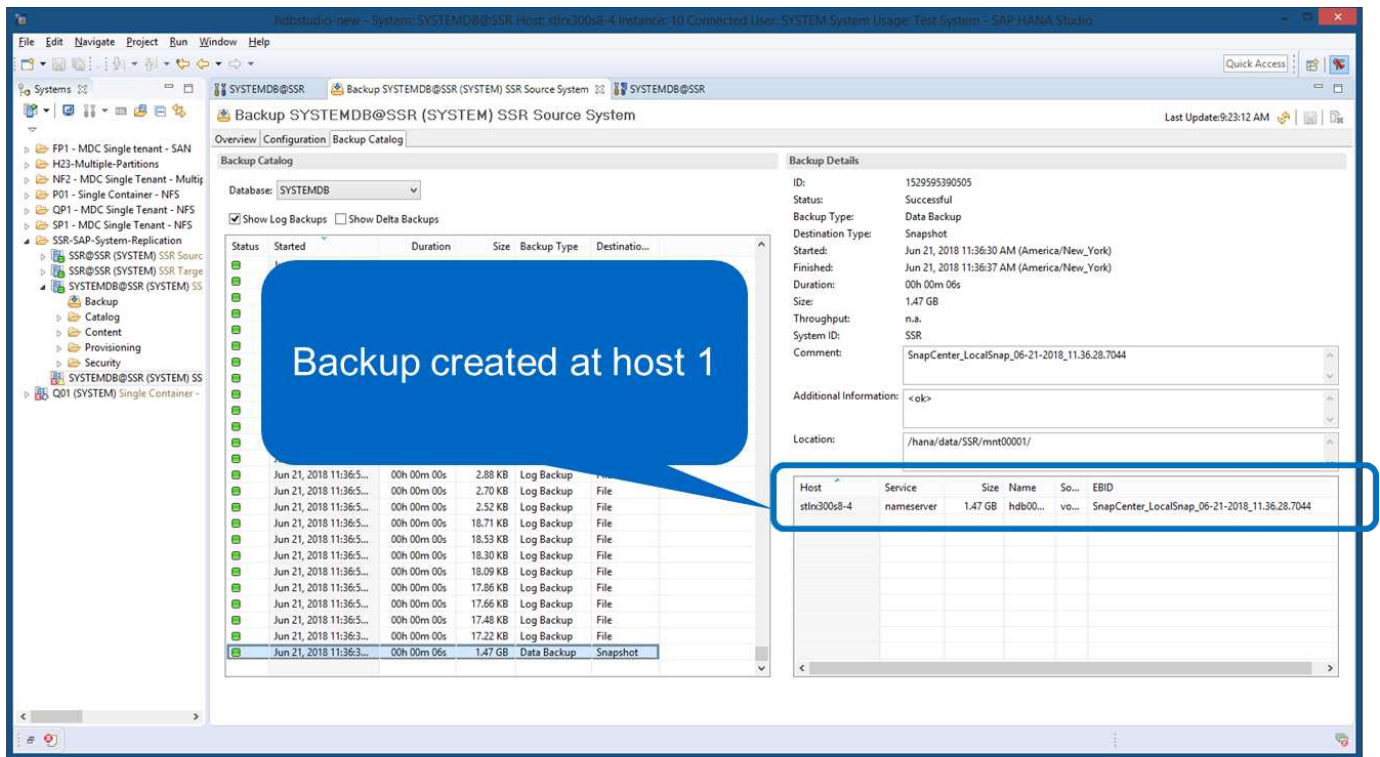
La figura seguente mostra una panoramica dello scenario di ripristino e ripristino descritto in questa sezione.

È stato creato un backup in T1 sull'host 1. È stato eseguito un failover sull'host 2. Dopo un certo punto di tempo, è stato eseguito un altro failover verso l'host 1. Al momento attuale, l'host 1 è l'host primario.

1. Si è verificato un errore ed è necessario ripristinare il backup creato in T1 sull'host 1.
2. L'host secondario (host 2) viene arrestato, ma non viene eseguita alcuna operazione di ripristino.
3. Il volume di storage dell'host 1 viene ripristinato nel backup creato in T1.
4. Viene eseguito un forward recovery con i log degli host 1 e 2.
5. Viene avviato l'host 2 e viene avviata automaticamente una risincronizzazione della replica di sistema dell'host 2.



La figura seguente mostra il catalogo di backup SAP HANA in SAP HANA Studio. Il backup evidenziato mostra il backup creato in T1 sull'host 1.

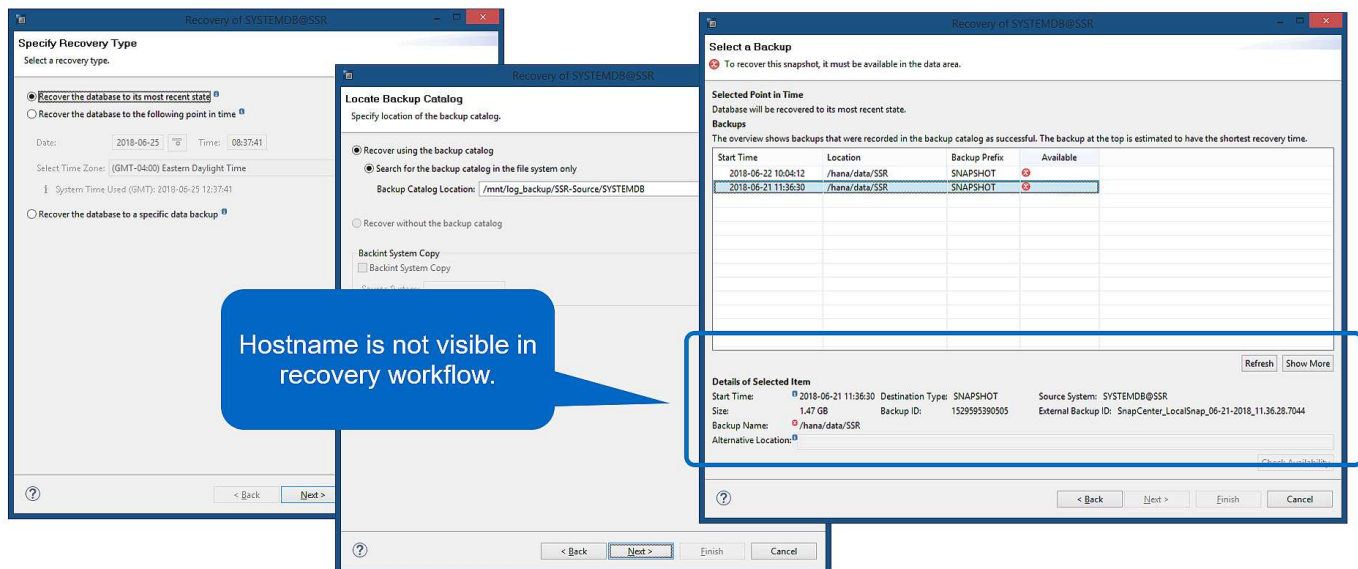


25

Viene avviata un'operazione di ripristino e ripristino in SAP HANA Studio. Come mostrato nella figura seguente, il nome dell'host in cui è stato creato il backup non è visibile nel flusso di lavoro di ripristino e ripristino.

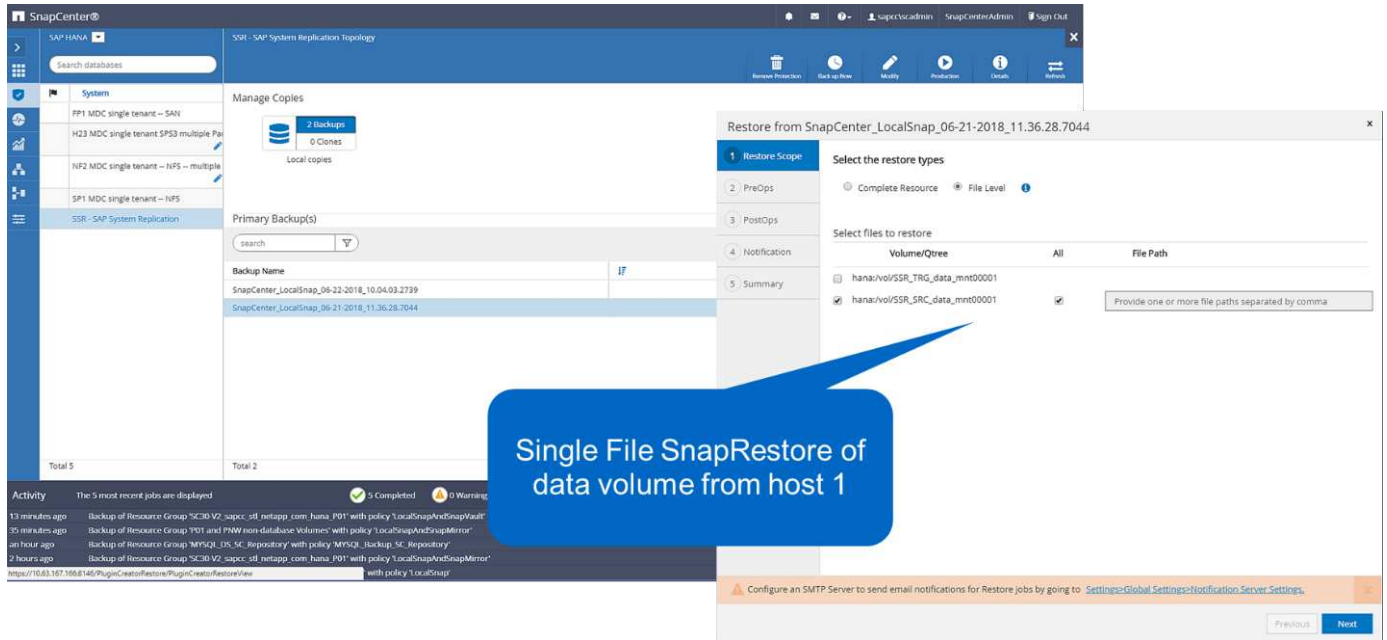


Nel nostro scenario di test, siamo stati in grado di identificare il backup corretto (il backup creato nell'host 1) in SAP HANA Studio quando il database era ancora online. Se il database non è disponibile, controllare il log del processo di backup di SnapCenter per identificare il backup corretto.

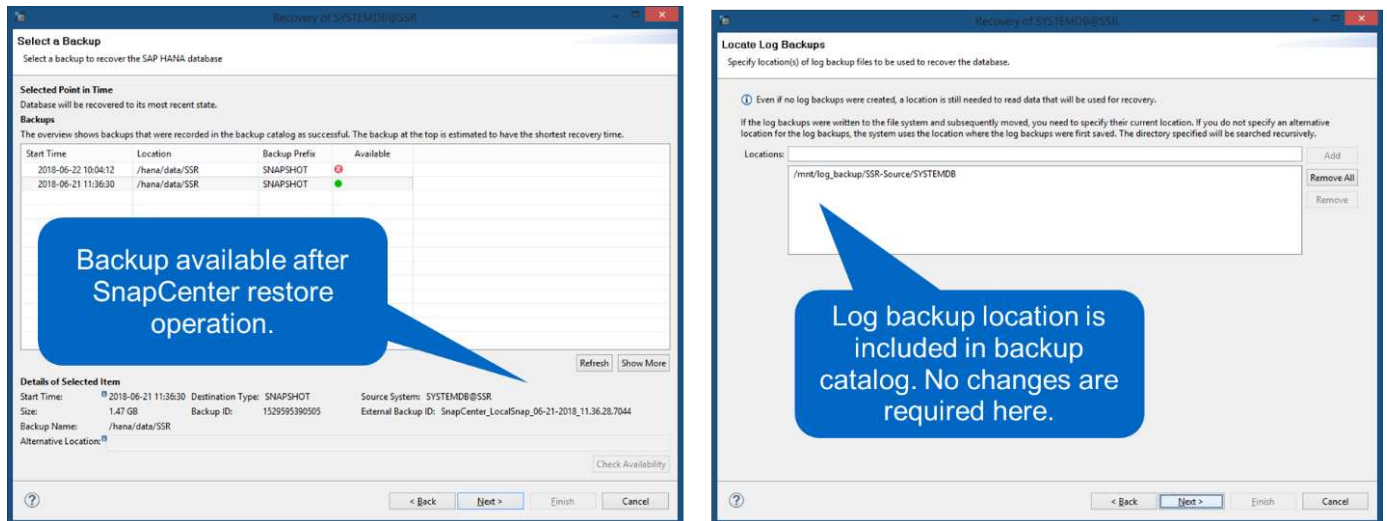


In SnapCenter, viene selezionato il backup e viene eseguita un'operazione di ripristino a livello di file. Nella

schermata di ripristino a livello di file, viene selezionato solo il volume host 1 in modo che venga ripristinato solo il backup valido.



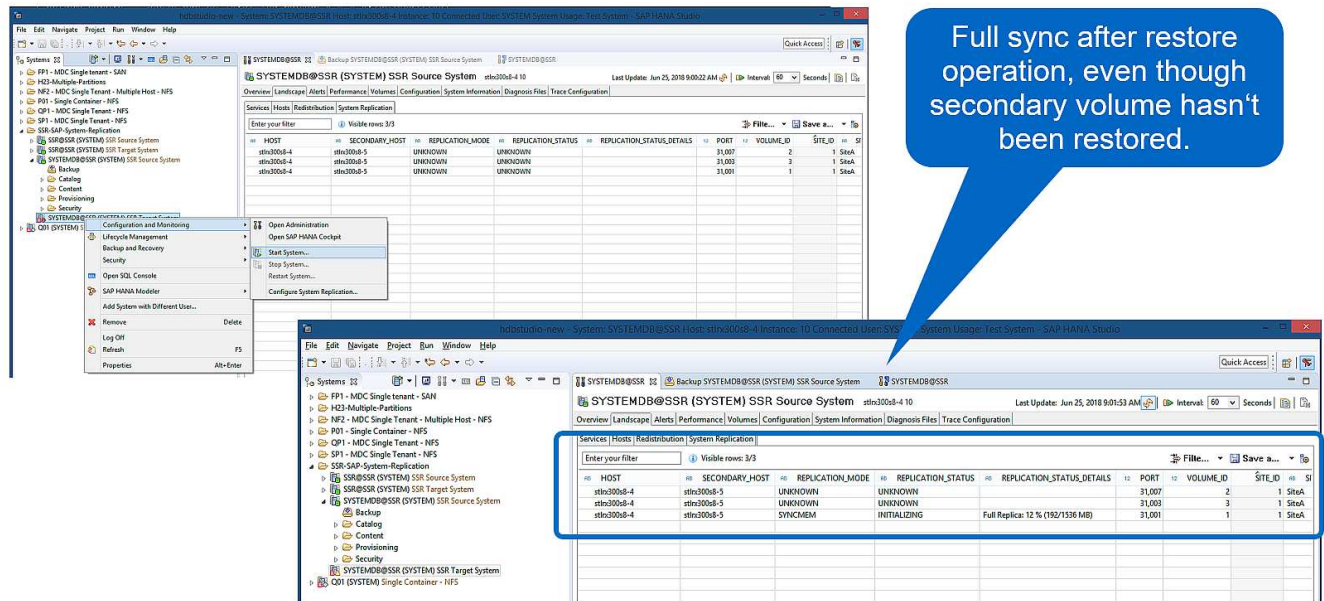
Dopo l'operazione di ripristino, il backup viene evidenziato in verde in SAP HANA Studio. Non è necessario inserire un'ulteriore posizione di backup del log, in quanto il percorso del file di backup del log degli host 1 e 2 è incluso nel catalogo di backup.



Al termine del forward recovery, viene avviato l'host secondario (host 2) e viene avviata la risincronizzazione della replica del sistema SAP HANA.



Anche se l'host secondario è aggiornato (non è stata eseguita alcuna operazione di ripristino per l'host 2), SAP HANA esegue una replica completa di tutti i dati. Questo comportamento è standard dopo un'operazione di ripristino e recovery con SAP HANA System Replication.

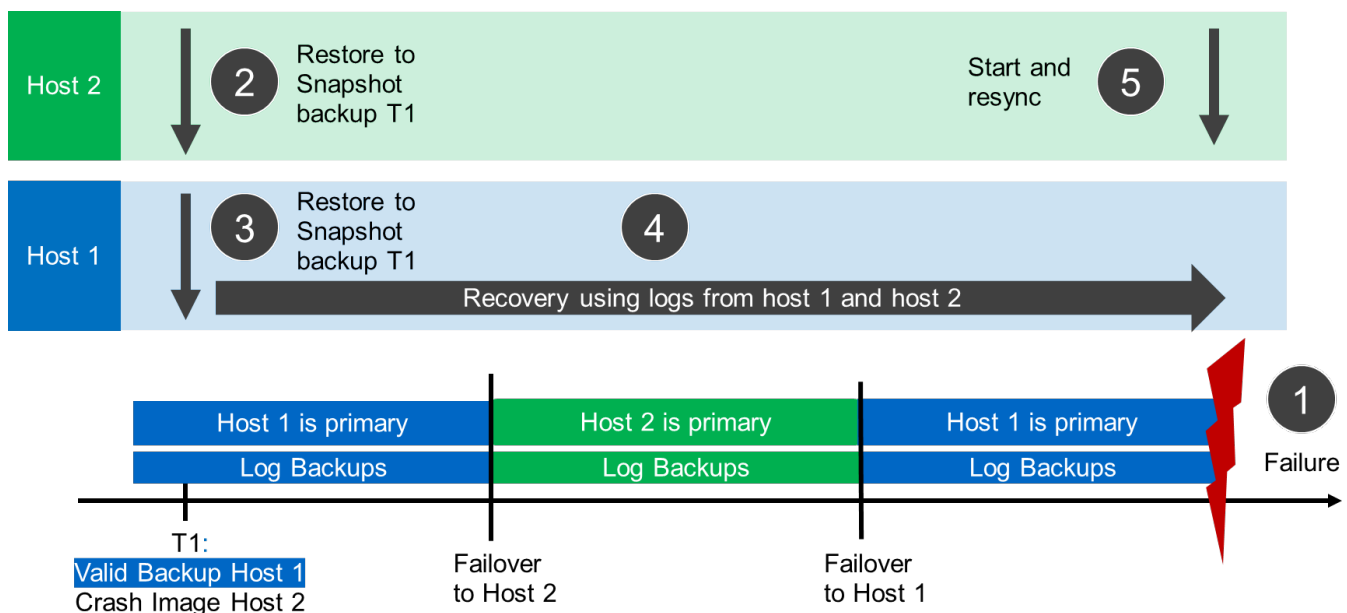


Ripristino SnapCenter di un backup valido e di un'immagine di arresto anomalo

La figura seguente mostra una panoramica dello scenario di ripristino e ripristino descritto in questa sezione.

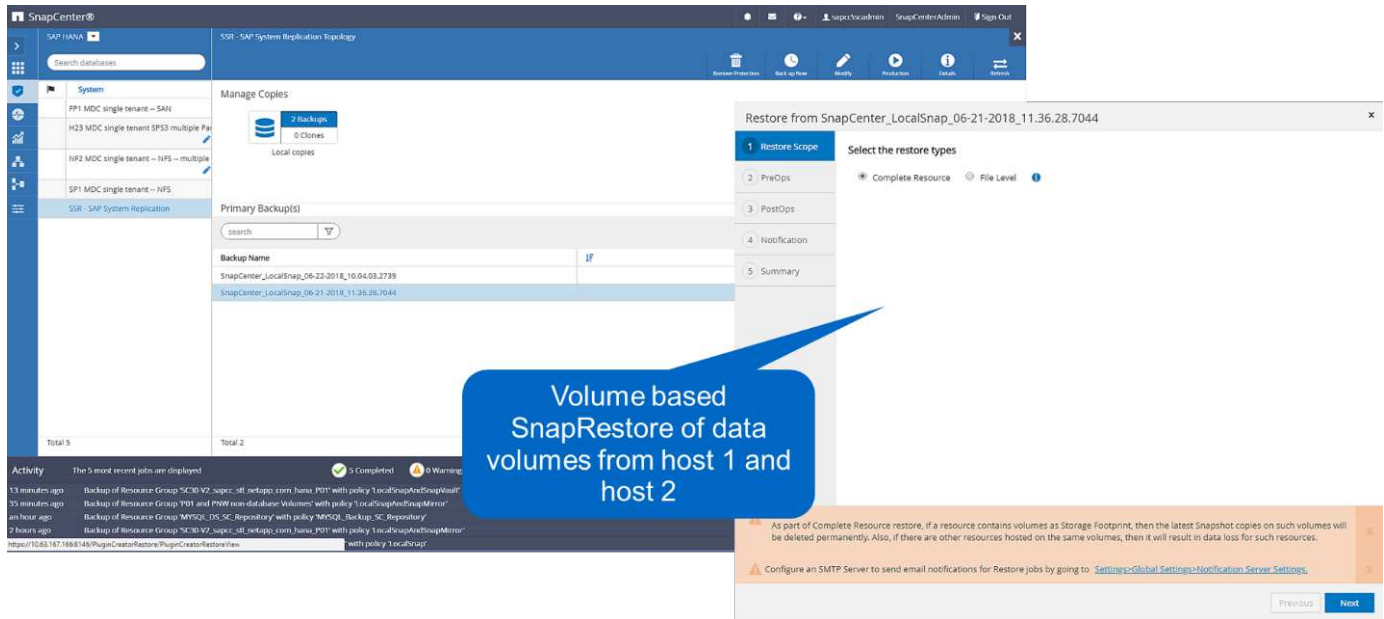
È stato creato un backup in T1 sull'host 1. È stato eseguito un failover sull'host 2. Dopo un certo punto di tempo, è stato eseguito un altro failover verso l'host 1. Al momento attuale, l'host 1 è l'host primario.

1. Si è verificato un errore ed è necessario ripristinare il backup creato in T1 sull'host 1.
2. L'host secondario (host 2) viene arrestato e l'immagine del crash T1 viene ripristinata.
3. Il volume di storage dell'host 1 viene ripristinato nel backup creato in T1.
4. Viene eseguito un forward recovery con i log degli host 1 e 2.
5. Viene avviato l'host 2 e viene avviata automaticamente una risincronizzazione della replica di sistema dell'host 2.

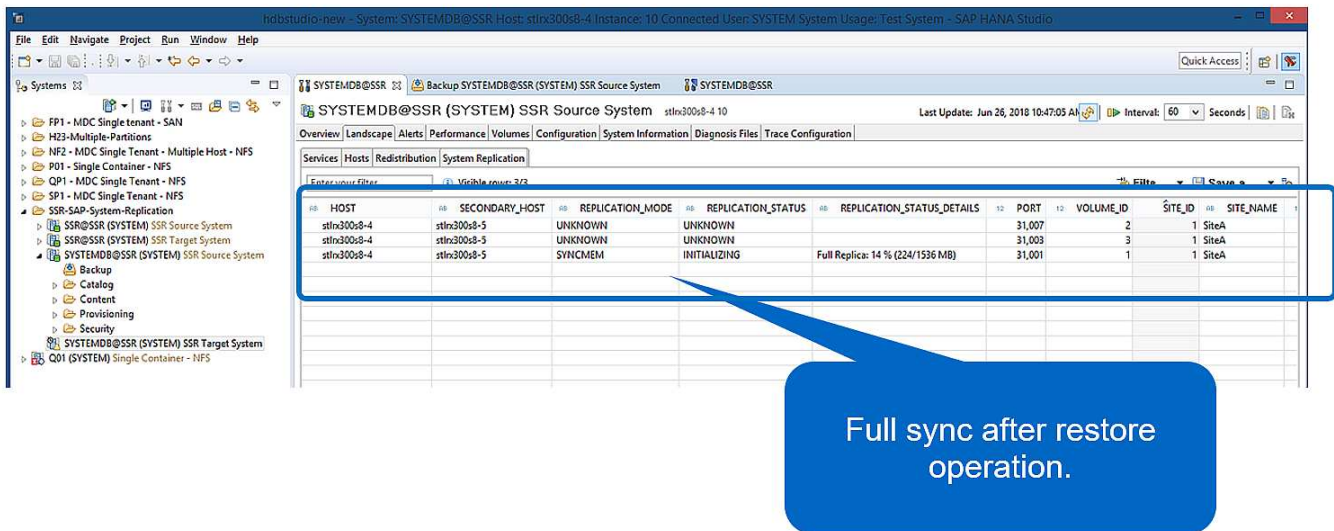


L'operazione di ripristino con SAP HANA Studio è identica a quella descritta nella sezione **"Ripristino SnapCenter solo del backup valido"**.

Per eseguire l'operazione di ripristino, selezionare completa risorsa in SnapCenter. I volumi di entrambi gli host vengono ripristinati.



Una volta completato il forward recovery, viene avviato l'host secondario (host 2) e viene avviata la risincronizzazione della replica del sistema SAP HANA. Viene eseguita la replica completa di tutti i dati.



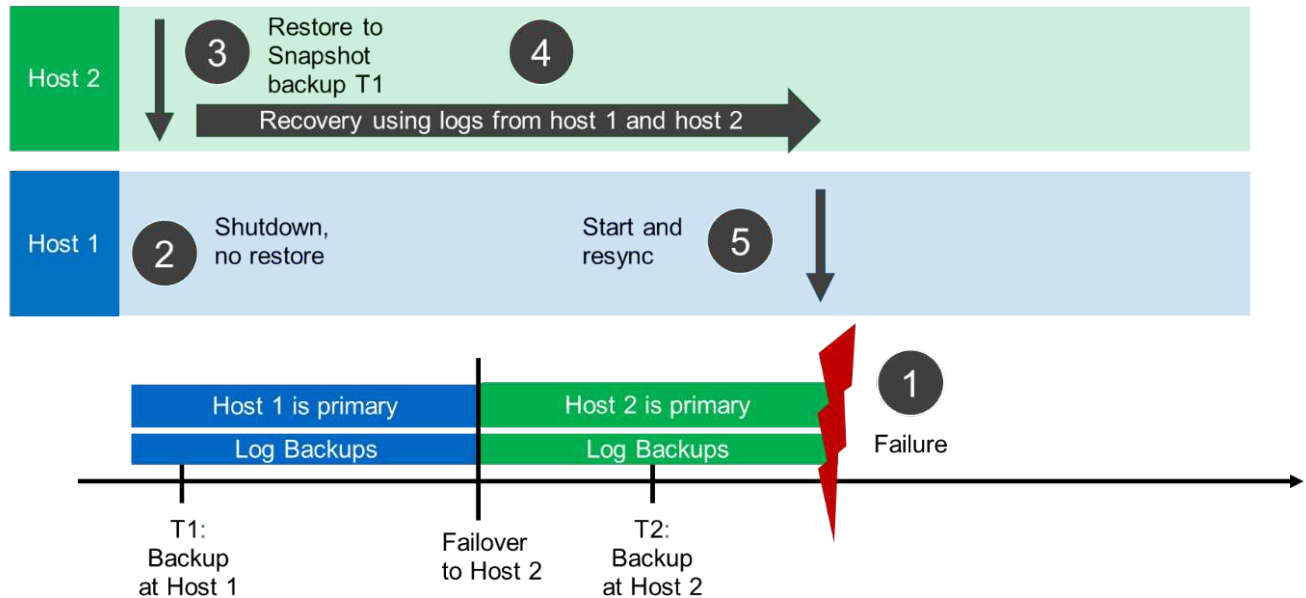
Ripristino e ripristino da un backup creato sull'altro host

Un'operazione di ripristino da un backup creato sull'altro host SAP HANA è uno scenario valido per entrambe le opzioni di configurazione di SnapCenter.

La figura seguente mostra una panoramica dello scenario di ripristino e ripristino descritto in questa sezione.

È stato creato un backup in T1 sull'host 1. È stato eseguito un failover sull'host 2. Al momento attuale, l'host 2 è l'host primario.

1. Si è verificato un errore ed è necessario ripristinare il backup creato in T1 sull'host 1.
2. L'host primario (host 1) viene arrestato.
3. I dati di backup T1 dell'host 1 vengono ripristinati nell'host 2.
4. Il ripristino in avanti viene eseguito utilizzando i registri dell'host 1 e dell'host 2.
5. Viene avviato l'host 1 e viene avviata automaticamente una risincronizzazione della replica di sistema dell'host 1.



31

La figura seguente mostra il catalogo di backup SAP HANA ed evidenzia il backup, creato sull'host 1, utilizzato per l'operazione di ripristino.

Backup SYSTEMDB@SSR (SYSTEM) SSR Target System

Overview | Configuration | Backup Catalog

Database: SYSTEMDB

☐ Show Log Backups ☐ Show Delta Backups

Status	Started	Duration	Size	Backup Type	Destination...
Success	Jun 28, 2018 9:23:46 ...	00h 00m 07s	1.53 GB	Data Backup	File
Success	Jun 27, 2018 7:45:56 ...	00h 00m 03s	1.52 GB	Data Backup	Snapshot
Success	Jun 27, 2018 7:12:37 ...	00h 00m 05s	1.55 GB	Data Backup	Snapshot

Backup Details

ID: 1530097957115

Status: Successful

Backup Type: Data Backup

Destination Type: Snapshot

Started: Jun 27, 2018 7:12:37 AM (America/New_York)

Finished: Jun 27, 2018 7:12:43 AM (America/New_York)

Duration: 00h 00m 06s

Size: 1.55 GB

Throughput: n.a.

System ID: SSR

Comment: SnapCenter_LocalSnap_06-27-2018_07.12.29.1232

Additional Information: <ok>

Location: /hana/data/SSR/mnt00001/

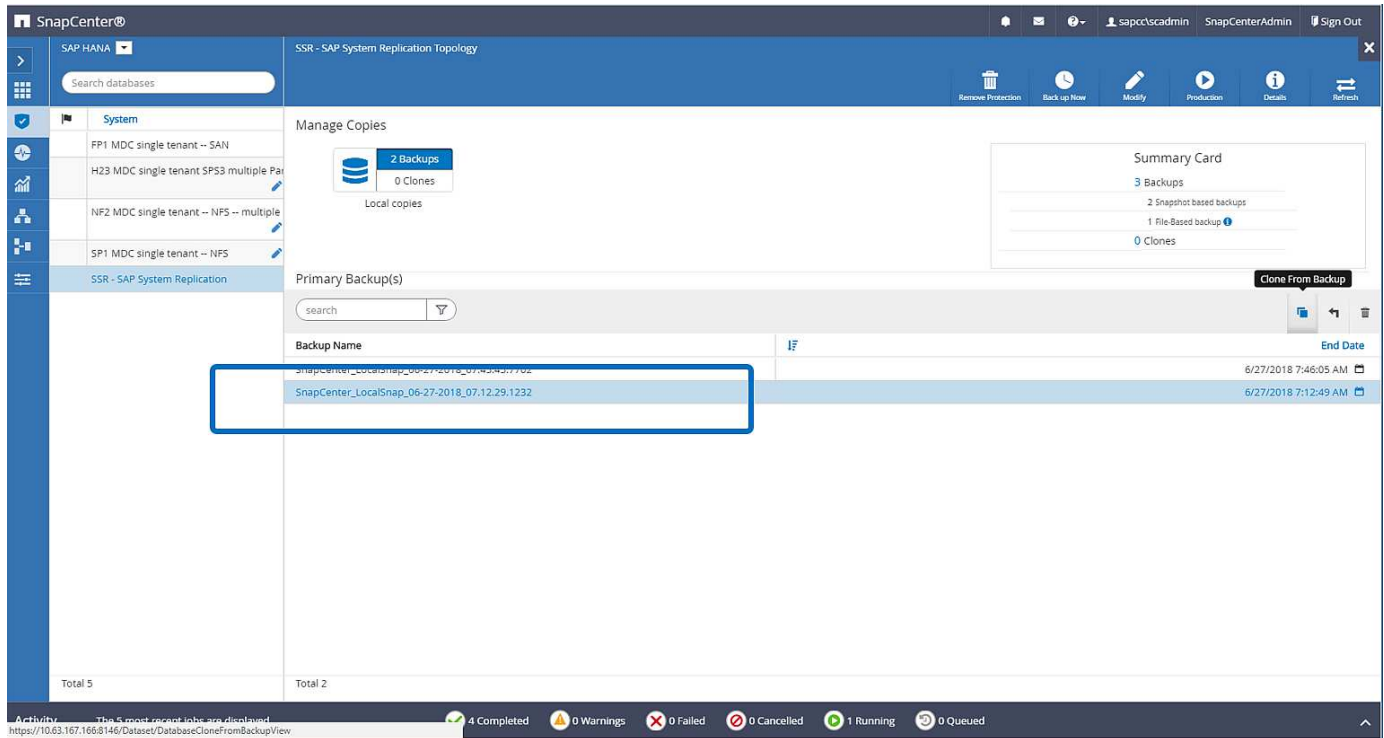
Host	Service	Size	Name	Source Type	EBID
stln300s8-4	nameserver	1.55 GB	hdb00001	volume	SnapC...

Prepare Recovery Wizard: (83%)

L'operazione di ripristino prevede i seguenti passaggi:

1. Creare un clone dal backup creato sull'host 1.
2. Montare il volume clonato sull'host 2.
3. Copiare i dati dal volume clonato nella posizione originale.

In SnapCenter, viene selezionato il backup e viene avviata l'operazione di clonazione.



È necessario fornire il server clone e l'indirizzo IP di esportazione NFS.



In una configurazione SnapCenter a risorsa singola, il plug-in SAP HANA non viene installato sull'host del database. Per eseguire il flusso di lavoro del clone di SnapCenter, è possibile utilizzare come server clone qualsiasi host con un plug-in HANA installato.

In una configurazione SnapCenter con risorse separate, l'host del database HANA viene selezionato come server clone e viene utilizzato uno script di montaggio per montare il clone sull'host di destinazione.


```
stlrx300s8-5:/mnt/tmp # mount 192.168.173.101:/Scc373da37-00ff-4694-b1e1-8153dbd46caf /mnt/tmp
```

Il volume clonato contiene i dati del database HANA.

```
stlrx300s8-5:/mnt/tmp/# ls -al
drwxr-x--x 2 ssradm sapsys 4096 Jun 27 11:12 hdb00001
drwx----- 2 ssradm sapsys 4096 Jun 21 09:38 hdb00002.00003
drwx----- 2 ssradm sapsys 4096 Jun 27 11:12 hdb00003.00003
-rw-r--r-- 1 ssradm sapsys 22 Jun 27 11:12 nameserver.lck
```

I dati vengono copiati nella posizione originale.

```
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00001 /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00002.00003/ /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00003.00003/ /hana/data/SSR/mnt00001/
```

Il ripristino con SAP HANA Studio viene eseguito come descritto nella sezione ["Ripristino SnapCenter solo del backup valido"](#).

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti:

- Backup e ripristino SAP HANA con SnapCenter
["https://www.netapp.com/us/media/tr-4614.pdf"](https://www.netapp.com/us/media/tr-4614.pdf)
- Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter
["https://docs.netapp.com/us-en/netapp-solutions-sap/lifecycle/sc-copy-clone-introduction.html"](https://docs.netapp.com/us-en/netapp-solutions-sap/lifecycle/sc-copy-clone-introduction.html)
- Disaster recovery SAP HANA con replica dello storage
["https://www.netapp.com/us/media/tr-4646.pdf"](https://www.netapp.com/us/media/tr-4646.pdf)

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Ottobre 2018	Versione iniziale
Versione 2.0	Gennaio 2022	Aggiornamento per il supporto della replica di sistema HANA di SnapCenter 4.6

Disaster recovery SAP HANA con Azure NetApp Files

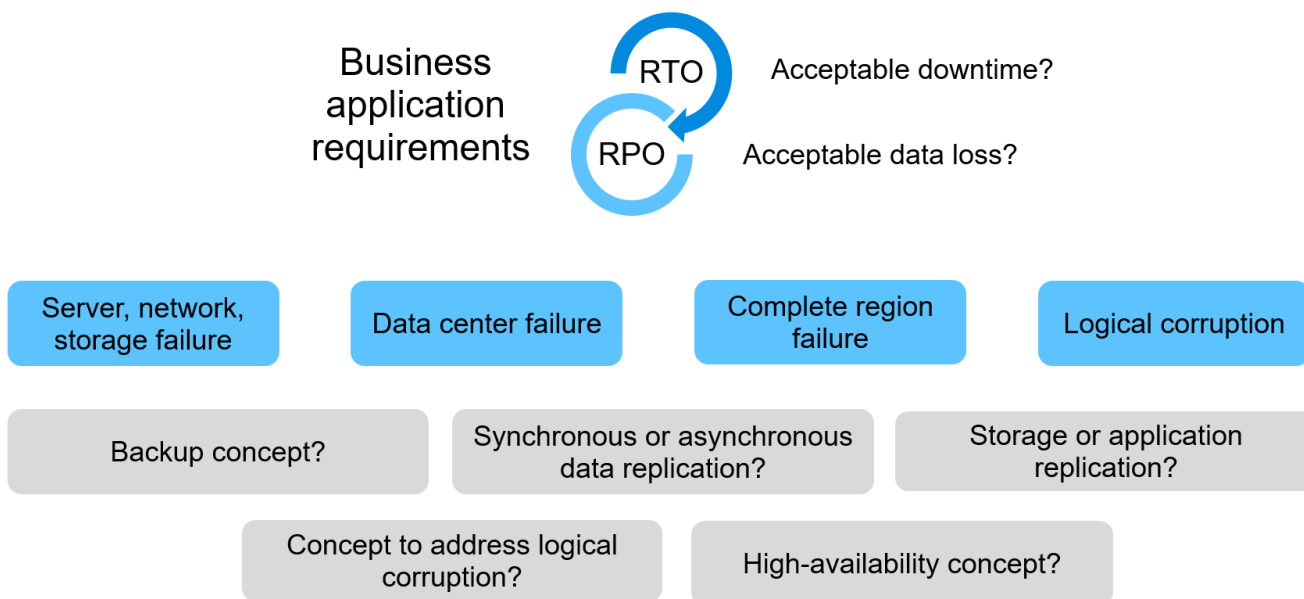
TR-4891: Disaster recovery SAP HANA con Azure NetApp Files

Nils Bauer, NetApp Ralf Klahr, Microsoft

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



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'RTTO (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'RTTO 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'RTTO, 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.

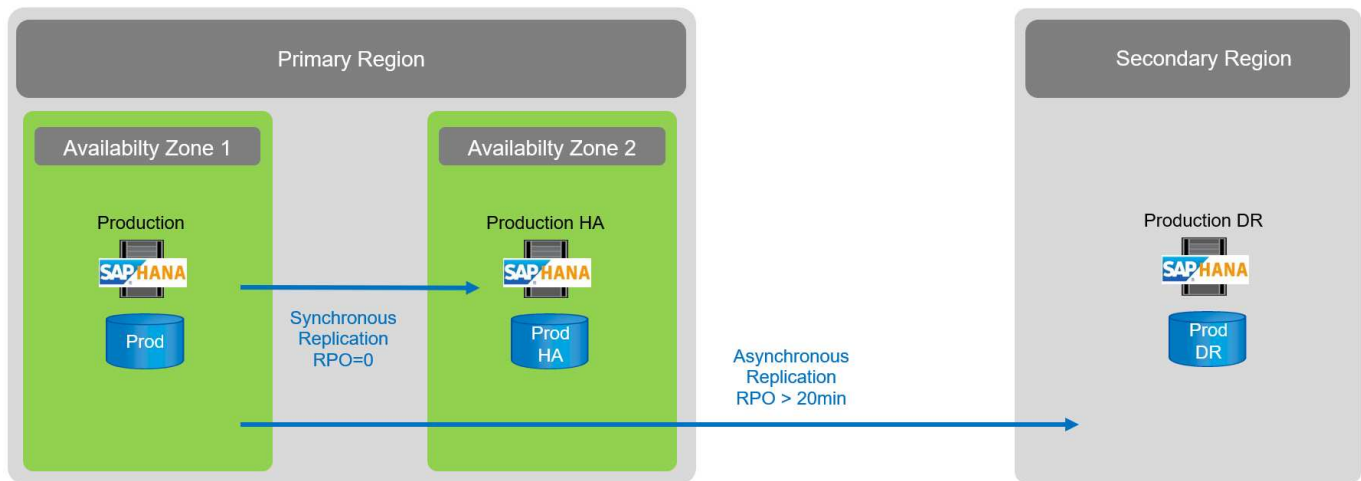
Confronto tra soluzioni di disaster recovery

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.

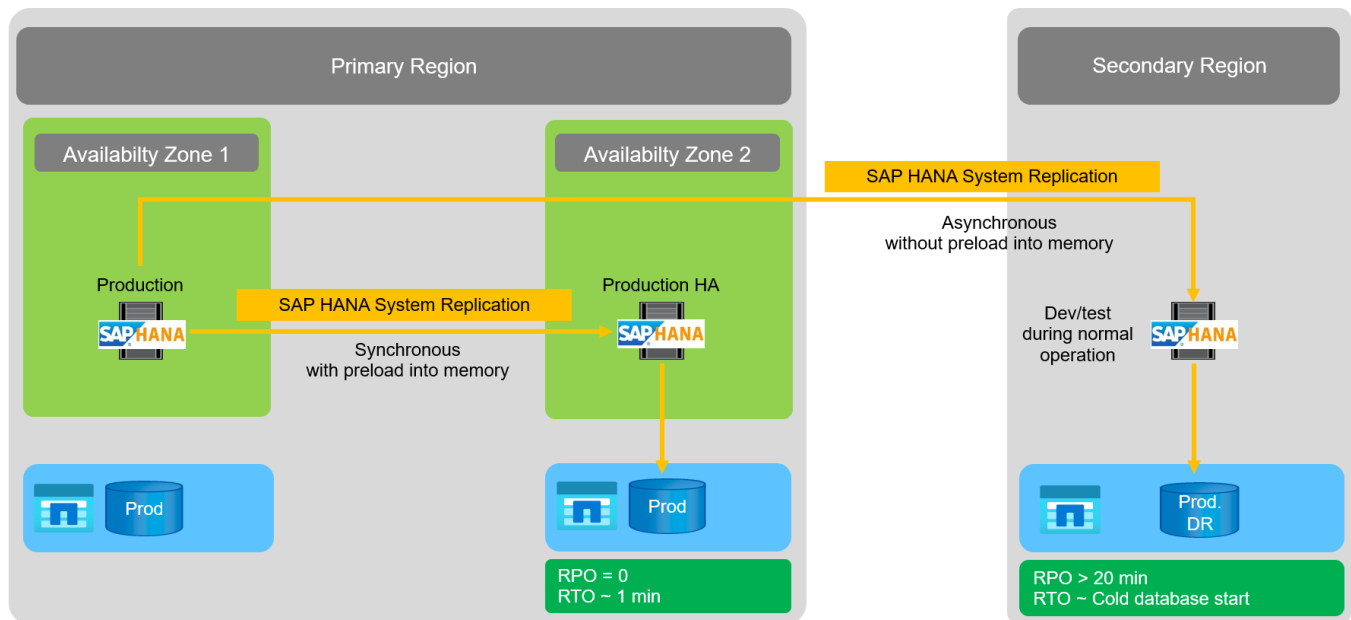
La replica del sistema SAP HANA può essere utilizzata in due modalità:

- 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

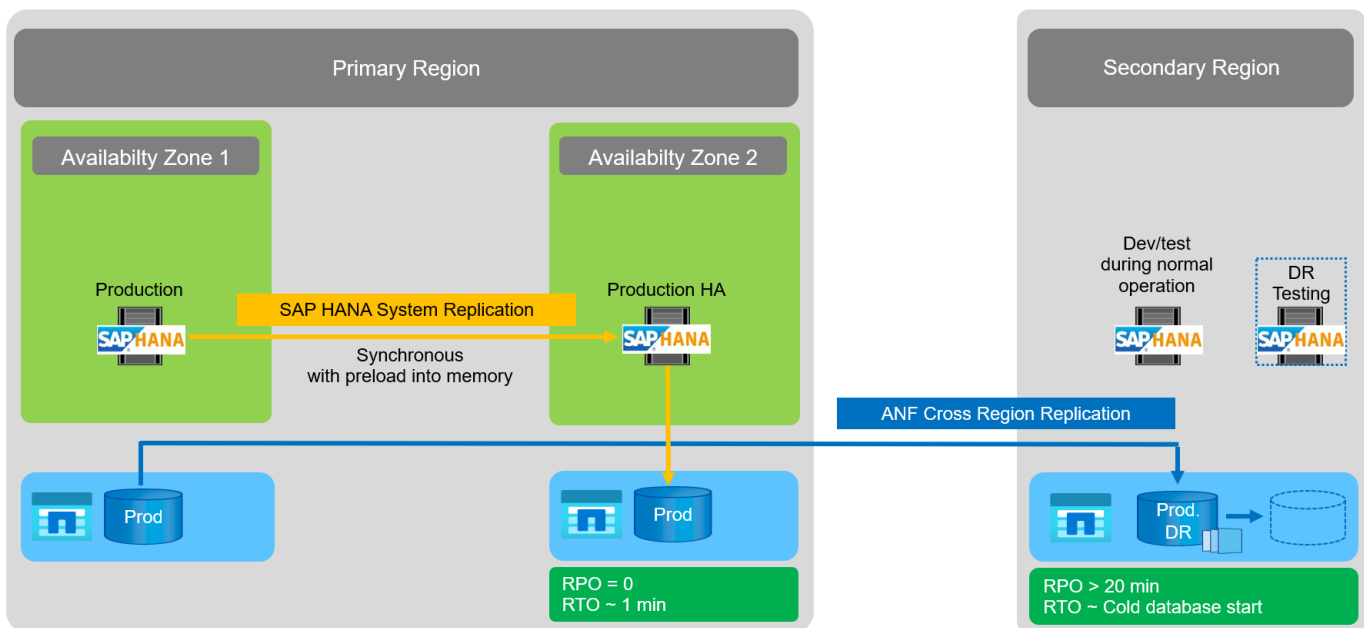
ANF Cross-Region. In questo esempio, il sistema HANA è protetto con la replica del sistema HANA all'interno della regione principale, come descritto nel capitolo precedente. La replica in una regione secondaria viene eseguita utilizzando la replica ANF cross-region. L'RPO è definito dalla pianificazione 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 dalle applicazioni sulla replica tra regioni sono disponibili all'indirizzo ["Documentazione Azure NetApp Files | documenti Microsoft"](#) nelle sezioni concetti e 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.

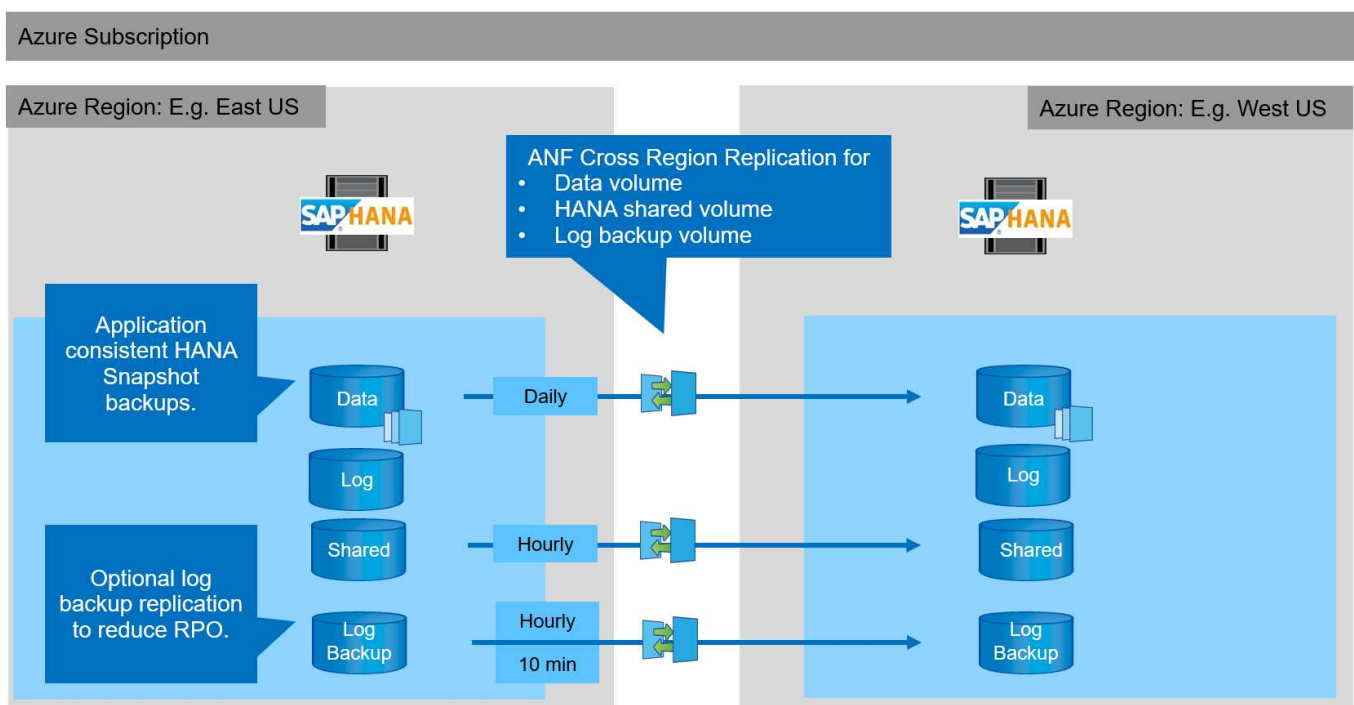


La seguente descrizione e la configurazione di laboratorio si concentrano sul database HANA. Altri file condivisi, ad esempio la directory di trasporto SAP, vengono protetti e replicati allo stesso modo del volume condiviso HANA.

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 richiesti.

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

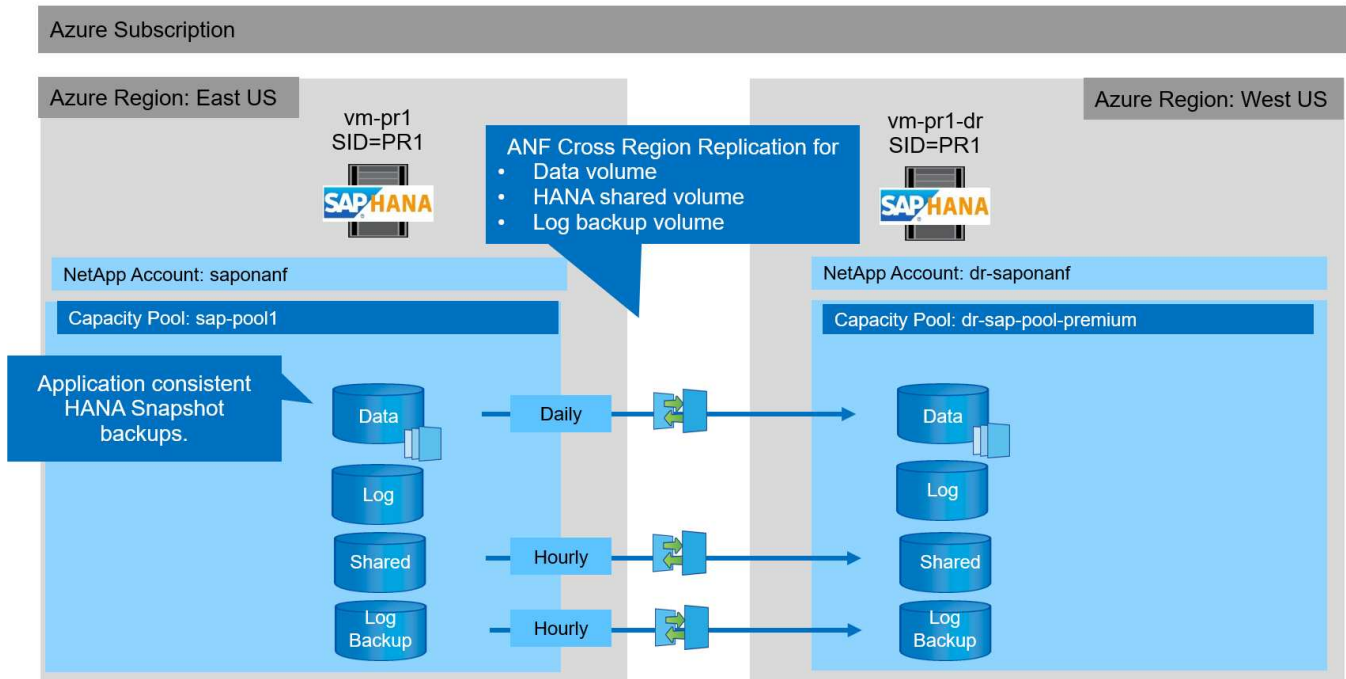
salvataggio e con operazioni di forward recovery.

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.

PR1-data-mnt00001 (saponanf/sap-pool1/PR1-data-mnt00001) | Snapshots

Volume

Search (Ctrl+/) « + Add snapshot Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Storage service

Mount instructions

Export policy

Snapshots

Replication

Monitoring

Metrics

Search snapshots

Name	Location	Created
azacsnap__2021-02-12T145015-1799555Z	East US	02/12/2021, 03:49:48 PM
azacsnap__2021-02-12T145227-1245630Z	East US	02/12/2021, 03:51:24 PM
azacsnap__2021-02-12T145828-3863442Z	East US	02/12/2021, 03:58:01 PM
azacsnap__2021-02-16T134021-9431230Z	East US	02/16/2021, 02:39:18 PM
azacsnap__2021-02-16T134917-6284160Z	East US	02/16/2021, 02:48:55 PM
azacsnap__2021-02-16T135737-3778546Z	East US	02/16/2021, 02:56:32 PM
azacsnap__2021-02-16T160002-1354654Z	East US	02/16/2021, 04:59:40 PM
azacsnap__2021-02-16T200002-0790339Z	East US	02/16/2021, 08:59:42 PM
azacsnap__2021-02-17T000002-1753859Z	East US	02/17/2021, 12:59:32 AM
azacsnap__2021-02-17T040001-5454808Z	East US	02/17/2021, 04:59:31 AM
azacsnap__2021-02-17T080002-2933611Z	East US	02/17/2021, 08:59:40 AM

La figura seguente mostra il catalogo di backup SAP HANA.

n-pr1 Instance: 01 Connected User: SYSTEM System Usage: Custom System - SAP HANA Studio

Help

SYSTEMDB@PR1 ... Backup SYSTE... SYSTEMDB@PR1 ... SYSTEMDB@PR1 ... SYSTEMDB@PR1 ... Backup SYSTE... SYSTEMDB@PR1 ... SYSTEMDB@PR1 ... SYSTEMDB@PR1 ...

Backup SYSTEMDB@PR1 (SYSTEM) PR1 SystemDB

Last Update: 9:07:38 AM

Overview Configuration Backup Catalog

Backup Catalog

Database: SYSTEMDB

☐ Show Log Backups ☐ Show Delta Backups

Status	Started	Duration	Size	Backup Type	Destination...
Success	Feb 17, 2021 8:00:02 ...	00h 00m 42s	3.13 GB	Data Backup	Snapshot
Success	Feb 17, 2021 4:00:01 ...	00h 00m 35s	3.13 GB	Data Backup	Snapshot
Success	Feb 17, 2021 12:00:00 ...	00h 00m 36s	3.13 GB	Data Backup	Snapshot
Success	Feb 16, 2021 8:00:02 ...	00h 00m 34s	3.13 GB	Data Backup	Snapshot
Success	Feb 16, 2021 4:00:02 ...	00h 00m 38s	3.13 GB	Data Backup	Snapshot
Success	Feb 16, 2021 1:57:37 ...	00h 00m 32s	3.13 GB	Data Backup	Snapshot
Success	Feb 16, 2021 1:49:17 ...	00h 00m 32s	3.13 GB	Data Backup	Snapshot
Success	Feb 16, 2021 1:40:22 ...	00h 00m 34s	3.13 GB	Data Backup	Snapshot
Success	Feb 12, 2021 2:58:28 ...	00h 00m 32s	3.13 GB	Data Backup	Snapshot
Success	Feb 12, 2021 2:52:27 ...	00h 00m 32s	3.13 GB	Data Backup	Snapshot
Success	Feb 12, 2021 2:50:15 ...	00h 00m 32s	3.13 GB	Data Backup	Snapshot

Backup Details

ID: 1613141415533

Status: Successful

Backup Type: Data Backup

Destination Type: Snapshot

Started: Feb 12, 2021 2:50:15 PM (UTC)

Finished: Feb 12, 2021 2:50:48 PM (UTC)

Duration: 00h 00m 32s

Size: 3.13 GB

Throughput: n.a.

System ID:

Comment: Snapshot prefix: azacsnap
Tools version: 5.0 Preview (20201214.65524)

Additional Information: <ok>

Location: /hana/data/PR1/mnt00001/

Host	Service	Size	Name	Source ...	EBID
vm-pr1	nameserver	3.13 GB	hdb00001	volume	azacsnap__2021-02-12T14501...

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.

Create a new protection volume

Basics Protocol Replication Tags Review + create

This page will help you create an Azure NetApp Files volume in your subscription and enable you to access the volume from within your virtual network. [Learn more about Azure NetApp Files](#)

Volume details

Volume name *	<input type="text" value="PR1-data-mnt00001-sm-dest"/>	✓
Capacity pool * ⓘ	<input type="text" value="dr-sap-pool1"/>	▼
Available quota (GiB) ⓘ	<input type="text" value="4096"/>	4 TiB
Quota (GiB) * ⓘ	<input type="text" value="500"/>	500 GiB ✓
Virtual network * ⓘ	<input type="text" value="dr-vnet (10.2.0.0/16,10.0.2.0/24)"/>	▼
	Create new	
Delegated subnet * ⓘ	<input type="text" value="default (10.0.2.0/28)"/>	▼
	Create new	
Show advanced section	<input type="checkbox"/>	

Review + create

< Previous

Next : Protocol >

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.

Create a new protection volume

Basics **Protocol** Replication Tags Review + create

Configure access to your volume.

Access

Protocol type ☒ NFS ☐ SMB ☐ Dual-protocol (NFSv3 and SMB)

Configuration

File path * ⓘ

Versions * ▼

Kerberos ☐ Enabled ☒ Disabled

Export policy

Configure the volume's export policy. This can be edited later. [Learn more](#)

↑ Move up ↓ Move down ↑ Move to top ↓ Move to bottom 🗑 Delete

<input checked="" type="checkbox"/>	Index	Allowed clients	Access	Root Access	
<input checked="" type="checkbox"/>	1	<input type="text" value="0.0.0.0/0"/>	<input type="text" value="Read & Write"/> ▼	<input type="text" value="On"/> ▼	...
		<input type="text"/>	<input type="text"/> ▼	<input type="text"/> ▼	

Review + create

< Previous

Next : Replication >

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.

Create a new protection volume

Basics Protocol **Replication** Tags Review + create

Source volume ID ⓘ

/subscriptions/28cfc403-f3f6-4b07-9847-4eb16109e870/resourceGroups/rg... ✓

Replication schedule ⓘ

Daily ^

Every 10 minutes

Hourly

Daily

Review + create

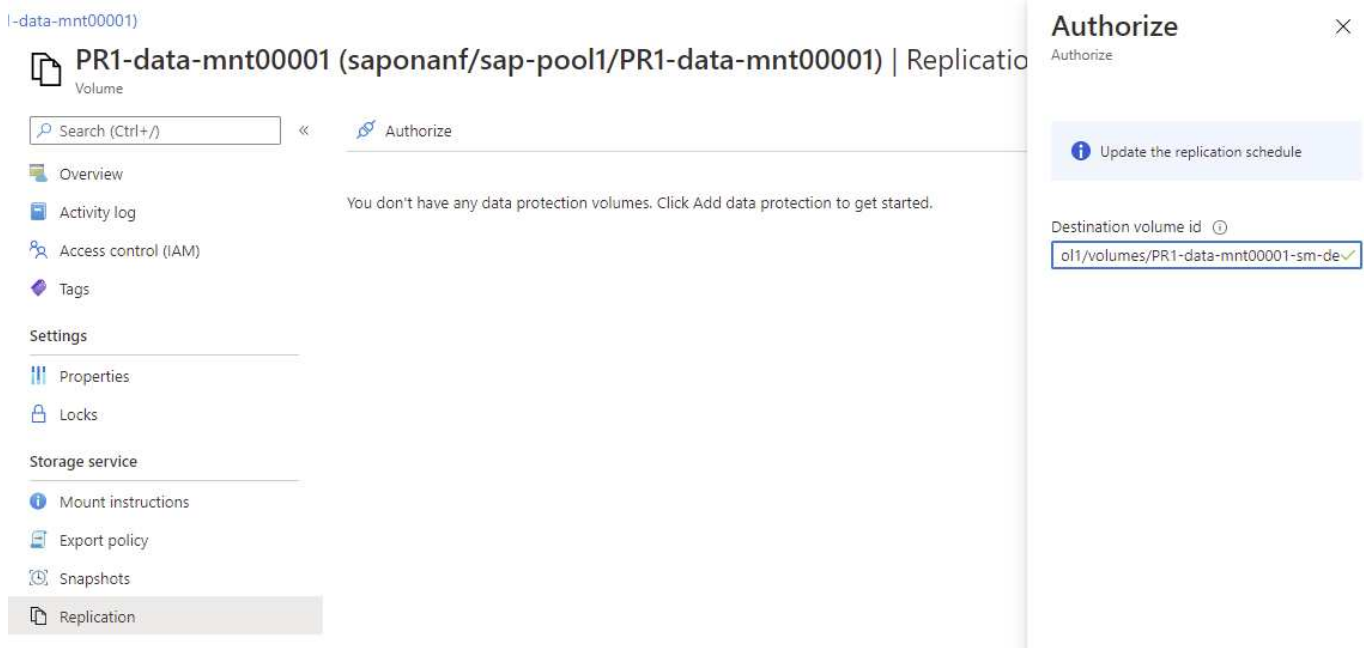
< Previous

Next : Tags >

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.

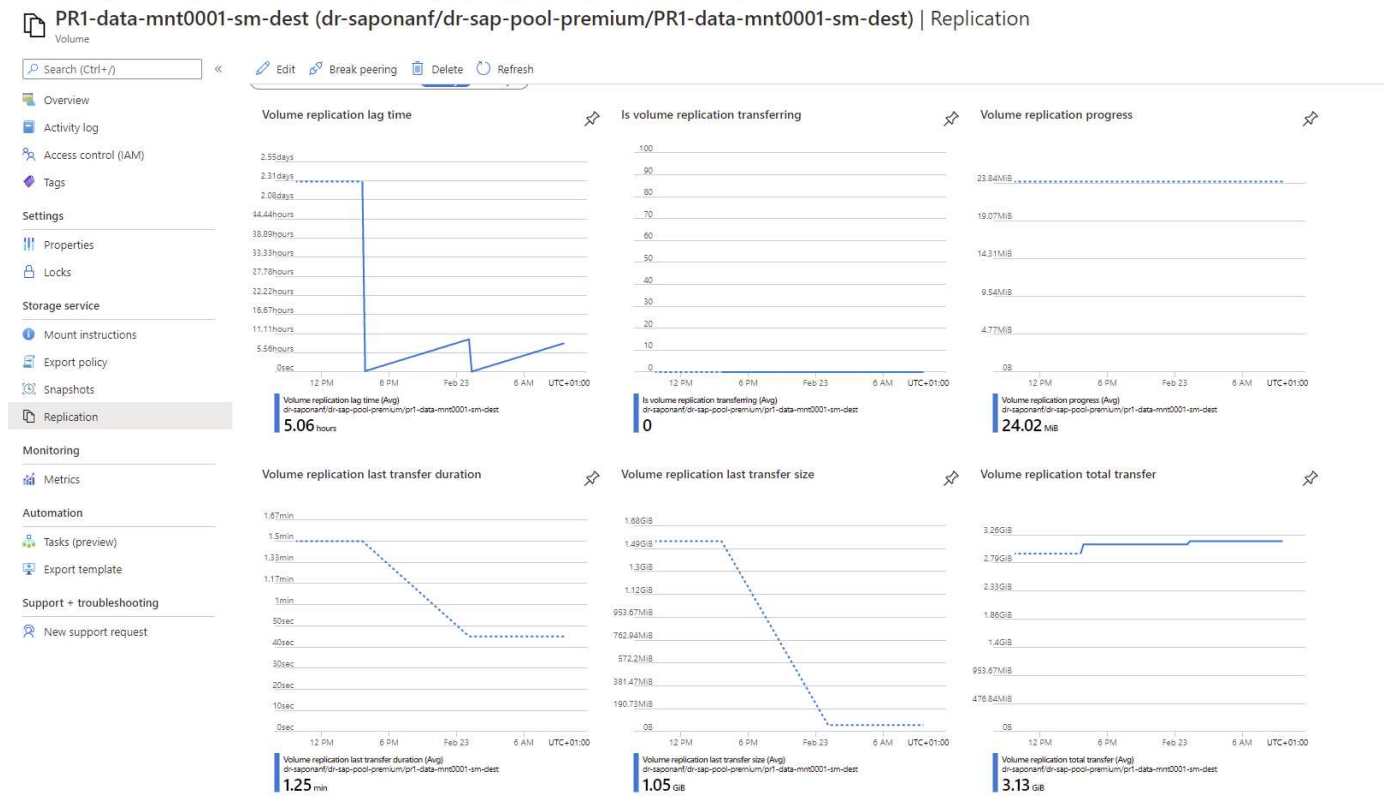
Monitoraggio della replica ANF tra regioni

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

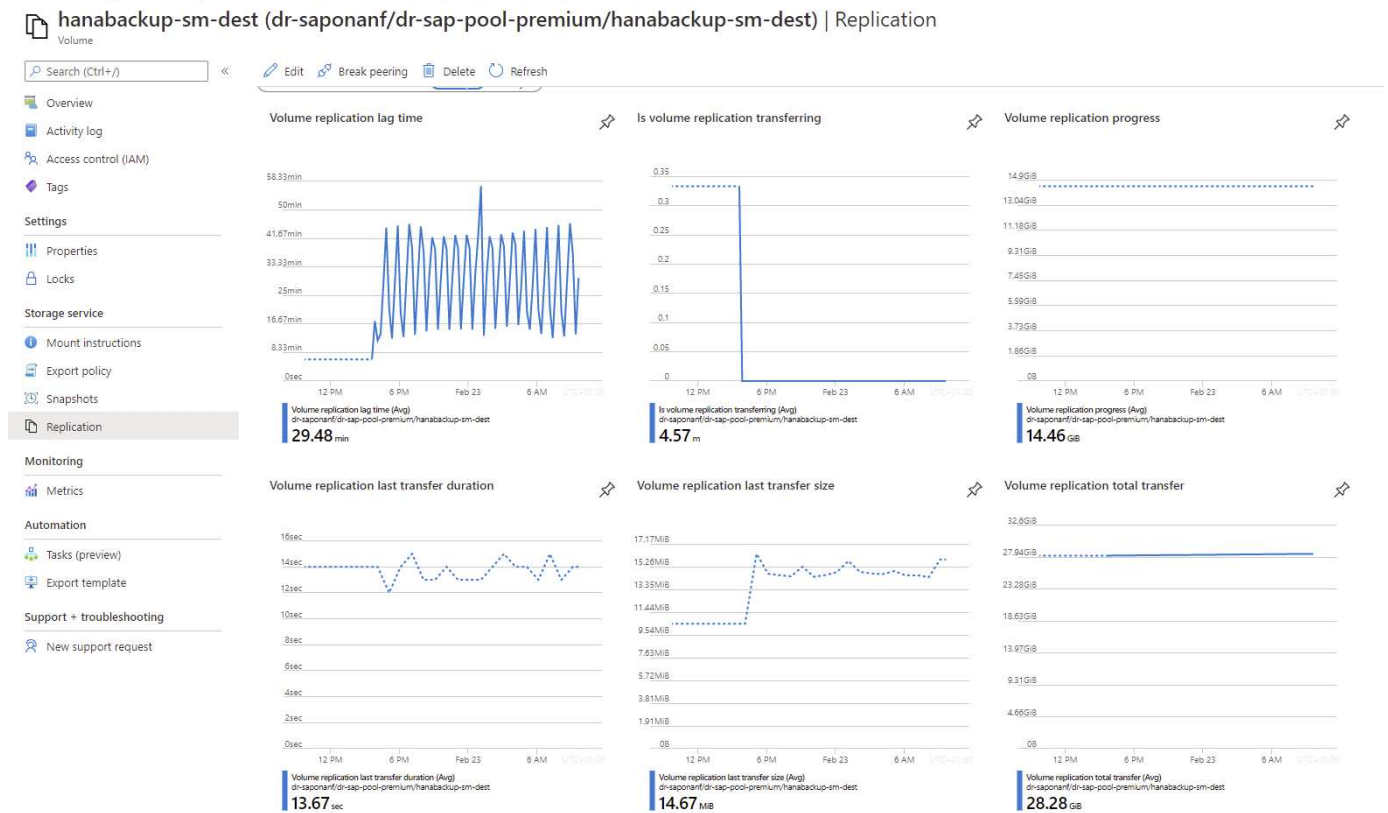
Il ritardo della replica del volume è un valore utile per comprendere le aspettative RPO. Ad esempio, la replica del volume di backup del registro mostra un ritardo massimo di 58 minuti, il che significa che l'RPO massimo ha lo stesso valore.

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.

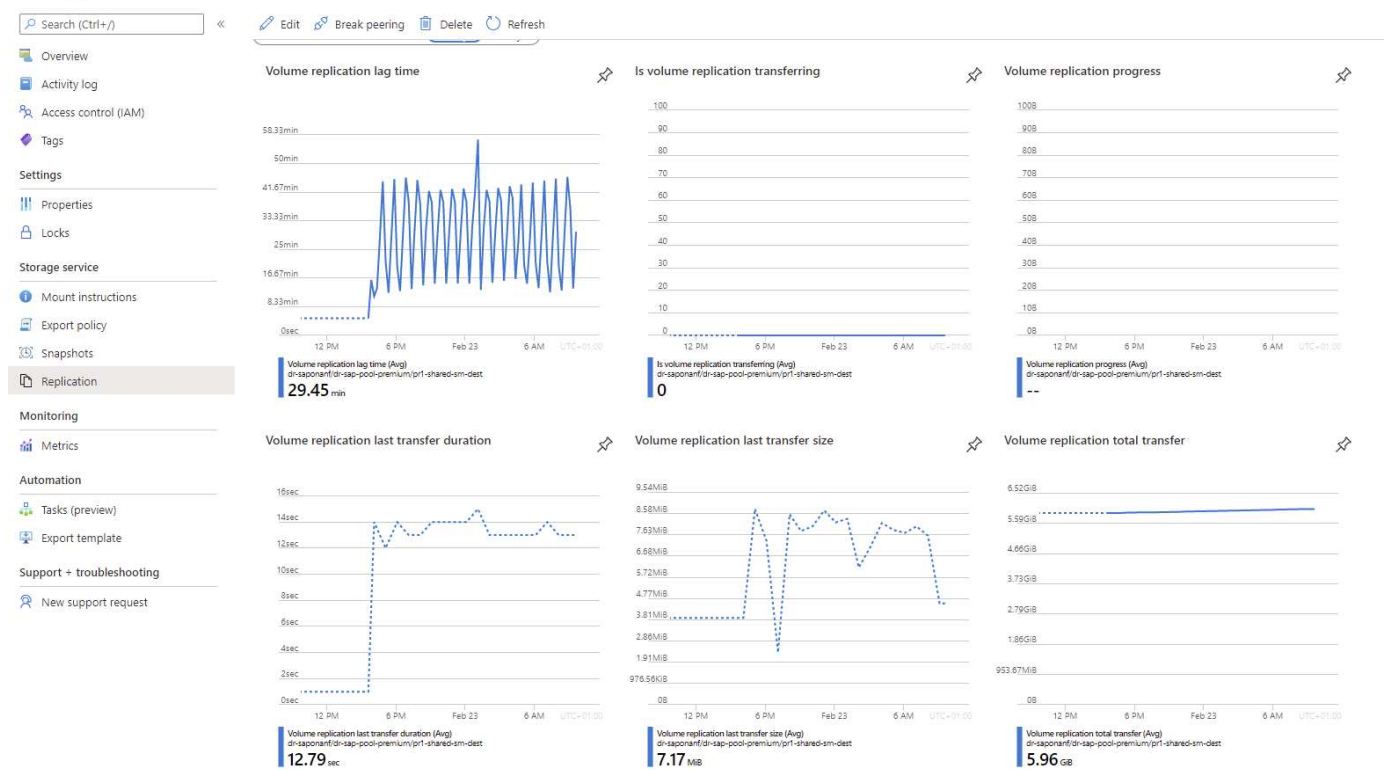


La seguente schermata mostra lo stato di replica del volume di backup del registro HANA.



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

PR1-shared-sm-dest (dr-saponanf/dr-sap-pool-premium/PR1-shared-sm-dest) | Replication



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.

me > Azure NetApp Files > dr-sapnanf > PR1-data-mnt0001-sm-dest (dr-sapnanf/dr-sap-pool-premium/PR1-data-mnt0001-sm-dest)

PR1-data-mnt0001-sm-dest (dr-sapnanf/dr-sap-pool-premium/PR1-data-mnt0001-sm-dest) | Snapshots

Volume

Search (Ctrl+/) << + Add snapshot Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Storage service

Mount instructions

Export policy

Snapshots

Replication

Monitoring

Metrics

Automation

Tasks (preview)

Export template

Support + troubleshooting

New support request

Search snapshots

Name	Location	Created
azacsnap__2021-02-18T20002-2150721Z	West US	02/18/2021, 01:00:05 PM
azacsnap__2021-02-18T160002-1442691Z	West US	02/18/2021, 05:00:49 PM
azacsnap__2021-02-18T200002-0756687Z	West US	02/18/2021, 09:00:05 PM
azacsnap__2021-02-19T000002-0039686Z	West US	02/19/2021, 01:00:05 AM
azacsnap__2021-02-19T040001-8773746Z	West US	02/19/2021, 05:00:06 AM
azacsnap__2021-02-19T080001-5198653Z	West US	02/19/2021, 09:00:05 AM
azacsnap__2021-02-19T120002-1495322Z	West US	02/19/2021, 01:00:06 PM
azacsnap__2021-02-19T160002-3698678Z	West US	02/19/2021, 05:00:05 PM
azacsnap__2021-02-22T120002-3145398Z	West US	02/22/2021, 01:00:06 PM
snapmirrorb1e8e48d-7114-11eb-b147-d039ea1e211e_2155791247.2021-02-22_143159	West US	02/22/2021, 03:32:00 PM
azacsnap__2021-02-22T160002-0144647Z	West US	02/22/2021, 05:00:05 PM
azacsnap__2021-02-22T200002-0649581Z	West US	02/22/2021, 09:00:05 PM
azacsnap__2021-02-23T000002-0311379Z	West US	02/23/2021, 01:00:05 AM
snapmirrorb1e8e48d-7114-11eb-b147-d039ea1e211e_2155791247.2021-02-23_001000	West US	02/23/2021, 01:10:00 AM

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"](#).

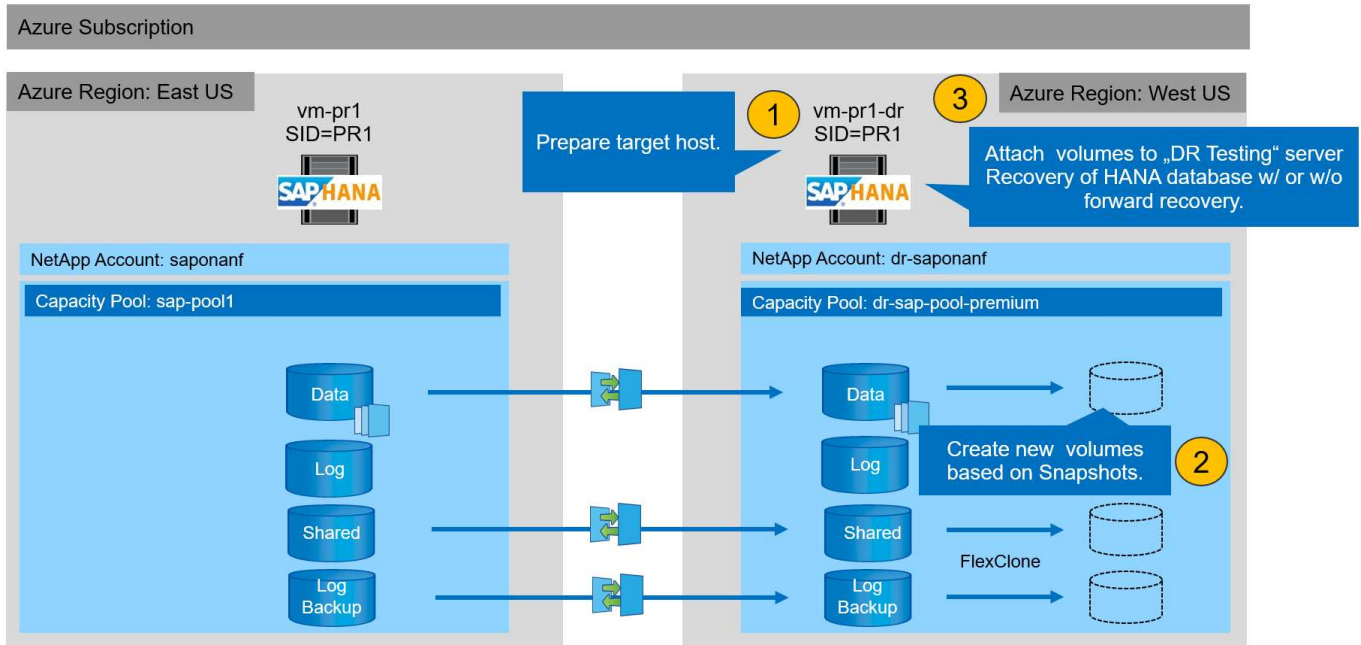
A seconda che la replica del backup dei log faccia parte o meno della configurazione del disaster recovery, le fasi del disaster recovery sono leggermente diverse. In questa sezione vengono descritti i test di disaster recovery per la replica solo backup dei dati e per la replica del volume dei dati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

288



Preparare l'host di destinazione

In questa sezione vengono descritte le fasi di preparazione necessarie per il server utilizzato per il test di 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 di questi passaggi 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 test 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 `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 schermo del server di destinazione in modo che non possa comunicare con altri sistemi. Se non è disponibile un corretto schermo, 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 ulteriori informazioni, 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 prladm
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 prladm sapsys 4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 prladm sapsys 4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 prladm 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, un nuovo volume basato su uno snapshot 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 dei nuovi volumi nel sito di disaster recovery sono inclusi in `/etc/fstab`. Questi nomi di volume vengono utilizzati nella fase di creazione del volume nella sezione successiva.

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



I punti di montaggio elencati in 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-mnt00001-sm-dest-clone /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsiz=262144,wsiz=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,rsiz=262144,wsiz=262144,intr,noa
time,lock,_netdev,sec=sys 0 0
# HANA ANF Shared Mounts
10.0.2.4:/PR1-shared-sm-dest-clone/hana-shared /hana/shared nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsiz=262144,wsiz=262144,intr,noa
time,lock,_netdev,sec=sys 0 0
10.0.2.4:/PR1-shared-sm-dest-clone/usr-sap-PR1 /usr/sap/PR1 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsiz=262144,wsiz=262144,intr,noa
time,lock,_netdev,sec=sys 0 0
# HANA file and log backup destination
10.0.2.4:/hanabackup-sm-dest-clone /hanabackup nfs
rw,vers=3,hard,timeo=600,rsiz=262144,wsiz=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.

PR1-data-mnt00001-sm-dest (dr-saponanf/dr-sap-pool1/PR1-data-mnt00001-sm-dest) | Snapshots

Volume

Search (Ctrl+/) « + Add snapshot Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Storage service

Mount instructions

Export policy

Snapshots

Replication

Monitoring

Metrics

Automation

Tasks (preview)

Export template

Support + troubleshooting

New support request

Search snapshots

Name	Location	Created	
azacsnap_2021-02-16T134021-9431230Z	West US	02/16/2021, 02:40:27 PM	...
azacsnap_2021-02-16T134917-6284160Z	West US	02/16/2021, 02:49:20 PM	...
azacsnap_2021-02-16T135737-3778546Z	West US	02/16/2021, 02:57:41 PM	...
azacsnap_2021-02-16T160002-1354654Z	West US	02/16/2021, 05:00:05 PM	...
azacsnap_2021-02-16T200002-0790339Z	West US	02/16/2021, 09:00:08 PM	...
azacsnap_2021-02-17T000002-1753859Z	West US	02/17/2021, 01:00:06 AM	...
azacsnap_2021-02-17T040001-5454808Z	West US	02/17/2021, 05:00:05 AM	...
azacsnap_2021-02-17T080002-2933611Z	West US	02/17/2021, 09:00:18 AM	...
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...	West US	02/17/2021, 12:46:22 PM	...
azacsnap_2021-02-17T120001-9196266Z	West US	02/17/2021, 01:00:08 PM	...
azacsnap_2021-02-17T160002-2801612Z	West US	02/17/2021, 05:00:06 PM	...
azacsnap_2021-02-17T200001-9149055Z	West US	02/17/2021, 09:00:05 PM	...
azacsnap_2021-02-18T000001-7955243Z	West US	02/18/2021, 01:00:07	...
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...	West US	02/18/2021, 01:10:00	...

Restore to new volume

Revert volume

Delete

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

Home > Azure NetApp Files > dr-saponanf > dr-sap-pool1 (dr-saponanf/dr-sap-pool1) > PR1-data-mnt00001-sm-dest (d

Create a volume

Basics Protocol Tags Review + create

This page will help you create an Azure NetApp Files volume in your subscription and enable you to access the volume from within your virtual network. [Learn more about Azure NetApp Files](#)

Volume details

Volume name * PR1-data-mnt00001-sm-dest-clone ✓

Restoring from snapshot ⓘ azacsnap_2021-02-18T000001-7955243Z

Available quota (GiB) ⓘ 2096 2.05 TiB

Quota (GiB) * ⓘ 500 500 GiB ✓

Virtual network ⓘ dr-vnet (10.2.0.0/16,10.0.2.0/24) ▼

Delegated subnet ⓘ default (10.0.2.0/28) ▼

Show advanced section ☐

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

[Home](#) > [Azure NetApp Files](#) > [dr-saponanf](#) > [dr-sap-pool1 \(dr-saponanf/dr-sap-pool1\)](#) > [PR1-data-mnt00001-sm-dest \(d](#)

Create a volume

Basics **Protocol** Tags Review + create

Configure access to your volume.

Access

Protocol type

☒ NFS ☐ SMB ☐ Dual-protocol (NFSv3 and SMB)

Configuration

File path * ⓘ

PR1-data-mnt00001-sm-dest-clone

Versions

NFSv4.1

Kerberos

☐ Enabled ☒ Disabled

Export policy

Configure the volume's export policy. This can be edited later. [Learn more](#)

↑ Move up ↓ Move down ↕ Move to top ⬇ Move to bottom 🗑 Delete

<input checked="" type="checkbox"/> Index	Allowed clients	Access	Root Access	
<input checked="" type="checkbox"/> 1	0.0.0.0/0	Read & Write	On	...

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

Create a volume

✓ Validation passed

Basics Protocol Tags Review + create

Basics

Subscription	Pay-As-You-Go
Resource group	dr-rg-sap
Region	West US
Volume name	PR1-data-mnt00001-sm-dest-clone
Capacity pool	dr-sap-pool1
Service level	Standard
Quota	500 GiB


Networking

Virtual network	dr-vnet (10.2.0.0/16,10.0.2.0/24)
Delegated subnet	default (10.0.2.0/28)

Protocol

Protocol	NFSv4.1
File path	PR1-data-mnt00001-sm-dest-clone

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

 dr-saponanf | Volumes

NetApp account

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Azure NetApp Files

Active Directory connections

Storage service

Capacity pools

Volumes

Data protection

Snapshot policies

Automation

Tasks (preview)

Export template

Support + troubleshooting

New support request

+ Add volume

+ Add data replication

Refresh

Search volumes

Name	↑↓	Quota	↑↓	Protocol type	↑↓	Mount path	↑↓	Service level	↑↓	Capacity pool	↑↓
hanabackup-sm-dest		1000 GiB		NFSv3		10.0.2.4/hanabackup-sm-dest		Standard		dr-sap-pool1	...
PR1-data-mnt00001-sm-dest		500 GiB		NFSv4.1		10.0.2.4/PR1-data-mnt00001-s		Standard		dr-sap-pool1	...
PR1-data-mnt00001-sm-dest-clone		500 GiB		NFSv4.1		10.0.2.4/PR1-data-mnt00001-s		Standard		dr-sap-pool1	...
PR1-log-mnt00001-dr		250 GiB		NFSv4.1		10.0.2.4/PR1-log-mnt00001-dr		Standard		dr-sap-pool1	...
PR1-shared-sm-dest		250 GiB		NFSv4.1		10.0.2.4/PR1-shared-sm-dest		Standard		dr-sap-pool1	...

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.

pool1/hanabackup-sm-dest

hanabackup-sm-dest (dr-saponanf/dr-sap-pool1/hanabackup-sm-dest) | Snapshots

Search (Ctrl+/) « + Add snapshot Refresh

Overview
Activity log
Access control (IAM)
Tags
Settings
Properties
Locks
Storage service
Mount instructions
Export policy
Snapshots
Replication

Search snapshots

Name	Location	Created	
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...	West US	02/18/2021, 02:05:00 PM	...
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...	West US	02/18/2021, 03:05:00	...

- Restore to new volume
- Revert volume
- Delete

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

pool1/PR1-shared-sm-dest

PR1-shared-sm-dest (dr-saponanf/dr-sap-pool1/PR1-shared-sm-dest) | Snapshots

Search (Ctrl+/) « + Add snapshot Refresh

Overview
Activity log
Access control (IAM)
Tags
Settings
Properties
Locks
Storage service
Mount instructions
Export policy
Snapshots
Replication

Search snapshots

Name	Location	Created	
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...	West US	02/18/2021, 02:05:00 PM	...
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...	West US	02/18/2021, 03:05:00	...

- Restore to new volume
- Revert volume
- Delete



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

```

prladm@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

```

prladm@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.

```
prladm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivercache'
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

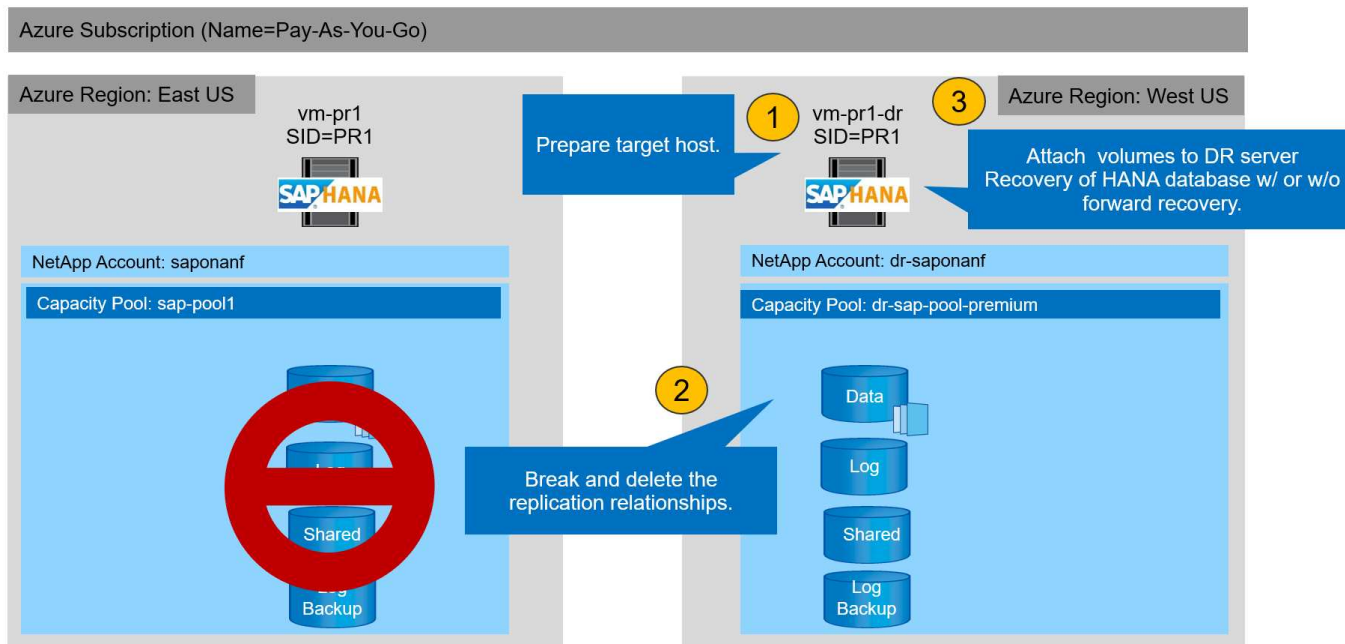
Failover del disaster recovery

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 schermo del server di destinazione in modo che non possa comunicare con altri sistemi. Se non è disponibile un corretto schermo, 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 prladm
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 prladm  sapsys  4096 Feb 22 10:25 hdb00001
drwxr-xr-- 2 prladm  sapsys  4096 Feb 22 10:25 hdb00002.00003
drwxr-xr-- 2 prladm  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-mnt00001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsiz=262144,wsiz=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,rsiz=262144,wsiz=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,rsiz=262144,wsiz=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,rsiz=262144,wsiz=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,rsiz=262144,wsiz=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.



PR1-data-mnt0001-sm-dest (dr-saponanf/dr-sap-pool-premium/PR1-data-mnt

Volume

Search (Ctrl+/)

Edit Break peering Delete Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Storage service

Mount instructions

Export policy

Snapshots

Replication

Essentials

End point type : Destination

Healthy : Healthy

Mirror state : Mirrored

Source

Relationship st

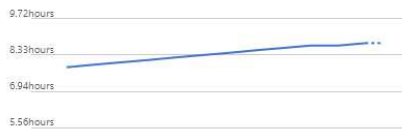
Replication sch

Total progress

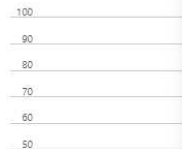
Show data for last:

1 hour 6 hours 12 hours 1 day 7 days

Volume replication lag time



Is volume replication transfer



Break replication peering

Break replication peering

Warning! This action will stop data replication between the volumes and might result in loss of data.

Type 'yes' to proceed

yes



PR1-data-mnt0001-sm-dest (dr-saponanf/dr-sap-pool-premium/PR1-data-mnt

Volume

Search (Ctrl+/)

Resync Delete Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Storage service

Mount instructions

Export policy

Snapshots

Replication

Essentials

End point type : Destination

Healthy : Healthy

Mirror state : Broken

Source

Relationship st

Replication sch

Total progress

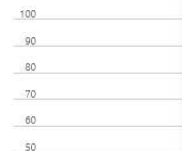
Show data for last:

1 hour 6 hours 12 hours 1 day 7 days

Volume replication lag time



Is volume replication transfer



Delete replication

Delete replication object

Warning this operation will delete the connection between PR1-data-mnt0001 and PR1-data-mnt0001-sm-dest

This will delete the replication object of PR1-data-mnt0001, type 'yes' to proceed

yes

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.



PR1-data-mnt0001-sm-dest (dr-saponanf/dr-sap-pool-premium/PR1-data-mnt0001-sm-dest) | Snapshots



Volume

Search (Ctrl+/) « + Add snapshot ↻ Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Storage service

Mount instructions

Export policy

Snapshots

Replication

Monitoring

Metrics

Automation

Tasks (preview)

Export template

Support + troubleshooting

New support request

Search snapshots

Name	↕	Location	↕	Created	↕
azacsnap__2021-02-18T120002-2150721Z		West US		02/18/2021, 01:00:05 PM	...
azacsnap__2021-02-18T160002-1442691Z		West US		02/18/2021, 05:00:49 PM	...
azacsnap__2021-02-18T200002-0758687Z		West US		02/18/2021, 09:00:05 PM	...
azacsnap__2021-02-19T000002-0039686Z		West US		02/19/2021, 01:00:05 AM	...
azacsnap__2021-02-19T040001-8773748Z		West US		02/19/2021, 05:00:06 AM	...
azacsnap__2021-02-19T080001-5198653Z		West US		02/19/2021, 09:00:05 AM	...
azacsnap__2021-02-19T120002-1495322Z		West US		02/19/2021, 01:00:06 PM	...
azacsnap__2021-02-19T160002-3698678Z		West US		02/19/2021, 05:00:05 PM	...
azacsnap__2021-02-22T120002-3145398Z		West US		02/22/2021, 01:00:06 PM	...
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...		West US		02/22/2021, 03:32:00 PM	...
azacsnap__2021-02-22T160002-0144647Z		West US		02/22/2021, 05:00:05 PM	...
azacsnap__2021-02-22T200002-0649581Z		West US		02/22/2021, 09:00:05 PM	...
azacsnap__2021-02-23T000002-0311379Z		West US		02/23/2021, 01:00:05 PM	...
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...		West US		02/23/2021, 01:10:00 PM	...

- Restore to new volume
- Revert volume
- Delete



PR1-data-mnt0001-sm-dest (dr-saponanf/dr-sap-pool-premium/PR1-data-mnt0001-sm-dest) | Snapshots

Volume

Search (Ctrl+/) « + Add snapshot ↻ Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Properties

Locks

Storage service

Mount instructions

Export policy

Snapshots

Replication

Monitoring

Metrics

Automation

Tasks (preview)

Export template

Support + troubleshooting

New support request

Search snapshots

Name	↕	Location
azacsnap__2021-02-18T120002-2150721Z		West US
azacsnap__2021-02-18T160002-1442691Z		West US
azacsnap__2021-02-18T200002-0758687Z		West US
azacsnap__2021-02-19T000002-0039686Z		West US
azacsnap__2021-02-19T040001-8773748Z		West US
azacsnap__2021-02-19T080001-5198653Z		West US
azacsnap__2021-02-19T120002-1495322Z		West US
azacsnap__2021-02-19T160002-3698678Z		West US
azacsnap__2021-02-22T120002-3145398Z		West US
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...		West US
azacsnap__2021-02-22T160002-0144647Z		West US
azacsnap__2021-02-22T200002-0649581Z		West US
azacsnap__2021-02-23T000002-0311379Z		West US
snapmirror.b1e8e48d-7114-11eb-b147-d039ea...		West US

Revert volume to snapshot



Revert volume PR1-data-mnt0001-sm-dest to snapshot azacsnap__2021-...

This action is irreversible and it will delete all the volumes snapshots that are newer than azacsnap__2021-02-23T000002-0311379Z. Please type 'PR1-data-mnt0001-sm-dest' to confirm.

Are you sure you want to revert 'PR1-data-mnt0001-sm-dest' to state of 'azacsnap__2021-02-23T000002-0311379Z'?

PR1-data-mnt0001-sm-dest ✓

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 sono riportati 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 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.

I comandi per eseguire un ripristino all'ultimo punto di salvataggio dei dati sono descritti nel capitolo ["Recovery to latest HANA Data Volume Backup savepoint"](#).

Recovery con forward recovery utilizzando i backup dei log

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 '2021-02-24 00:00:00' CLEAR LOG USING
SNAPSHOT"
[139792805873472, 0.008] >> starting recoverSys (at Tue Feb 23 12:05:16
2021)
[139792805873472, 0.008] args: ()
[139792805873472, 0.008] keys: {'command': "RECOVER DATABASE UNTIL
TIMESTAMP '2021-02-24 00:00:00' CLEAR LOG USING SNAPSHOT"}
using logfile /usr/sap/PR1/HDB01/vm-pr1/trace/backup.log
recoverSys started: =====2021-02-23 12:05:16 =====
testing master: vm-pr1
vm-pr1 is master
shutdown database, timeout is 120
stop system
stop system on: vm-pr1
stopping system: 2021-02-23 12:05:17
stopped system: 2021-02-23 12:05:18
creating file recoverInstance.sql
restart database
restart master nameserver: 2021-02-23 12:05:23
start system: vm-pr1
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2021-02-23T12:07:53+00:00 P0012969 177cec93d51 INFO RECOVERY
RECOVER DATA finished successfully, reached timestamp 2021-02-
23T09:03:11+00:00, reached log position 43123520
recoverSys finished successfully: 2021-02-23 12:07:54
[139792805873472, 157.466] 0
[139792805873472, 157.466] << ending recoverSys, rc = 0 (RC_TEST_OK),
after 157.458 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.

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

```
prladm@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 '2021-02-24
00:00:00' CLEAR LOG USING SNAPSHOT
0 rows affected (overall time 98.740038 sec; server time 98.737788 sec)
hdbsql SYSTEMDB=>
```

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.

```
prladm@hana-10: > hdbbackupcheck
/hanabackup/PR1/log/SYSTEMDB/log_backup_0_0_0_0.1589289811148
Loaded library 'libhdbcsaccessor'
Loaded library 'libhdblivercache'
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

TR-4646: Disaster recovery SAP HANA con replica dello storage

Nils Bauer, NetApp

TR-4646 è una panoramica delle opzioni per la protezione del disaster recovery per SAP HANA. Include informazioni dettagliate sull'installazione e una descrizione del caso di utilizzo di una soluzione di disaster recovery a tre siti basata sulla replica sincrona e asincrona dello storage NetApp SnapMirror. La soluzione descritta utilizza NetApp SnapCenter con il plug-in SAP HANA per gestire la coerenza del database.

<https://www.netapp.com/pdf.html?item=/media/8584-tr4646pdf.pdf>

TR-4313: Backup e ripristino SAP HANA con Snap Creator

Nils Bauer, NetApp

TR-4313 descrive l'installazione e la configurazione della soluzione di backup e ripristino NetApp per SAP HANA. La soluzione si basa sul framework NetApp Snap Creator e sul plug-in Snap Creator per SAP HANA. Questa soluzione è supportata con l'appliance multinodo certificata Cisco SAP HANA in combinazione con lo storage NetApp. Questa soluzione è supportata anche con sistemi SAP HANA a nodo singolo e multinodo in progetti TDI (Tailored Data Center Integration).

<https://www.netapp.com/pdf.html?item=/media/19779-tr-4313.pdf>

TR-4711: Backup e ripristino SAP HANA con sistemi di storage NetApp e software CommVault

Marco Schoen, NetApp

Dr. Tristan DAUDE, CommVault Systems

TR-4711 descrive la progettazione di una soluzione NetApp e CommVault per SAP HANA, che include la tecnologia di gestione delle snapshot CommVault IntelliSnap e la tecnologia NetApp Snapshot. La soluzione si basa sullo storage NetApp e sulla suite di protezione dei dati CommVault.

<https://www.netapp.com/pdf.html?item=/media/17050-tr4711pdf.pdf>

NVA-1147-DESIGN: SAP HANA su NetApp All SAN Array - SAN moderne, protezione dei dati e disaster recovery

Nils Bauer, Roland Wartenberg, Darryl Clinkscale, Daniel Hohman, Marco Schöen, Steve Botkin, Michael Peppers, Vidula Aiyer, Steve Collins, Pavan Jhamnani, Lee Dorrier, NetApp

Jim Zuccherro, Naem Saafein, pH.D., Broadcom Brocade

Questa architettura verificata di NetApp copre la modernizzazione dei sistemi e delle operazioni SAP per SAP HANA su sistemi storage All SAN Array (ASA) NetApp con Brocade FC SAN Fabric. Include backup e ripristino, disaster recovery e protezione dei dati. La soluzione sfrutta NetApp SnapCenter per automatizzare backup, ripristino e recovery SAP HANA, oltre a clonare i flussi di lavoro. Gli scenari di configurazione, test e failover del disaster recovery vengono descritti utilizzando il software di replica dei dati sincrono NetApp SnapMirror. Inoltre, viene illustrata la protezione dei dati SAP con CommVault.

<https://www.netapp.com/pdf.html?item=/media/10235-nva-1147-design.pdf>

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.