Backup e recovery SAP HANA con SnapCenter

NetApp Solutions SAP

NetApp
March 11, 2024

Sommario

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.

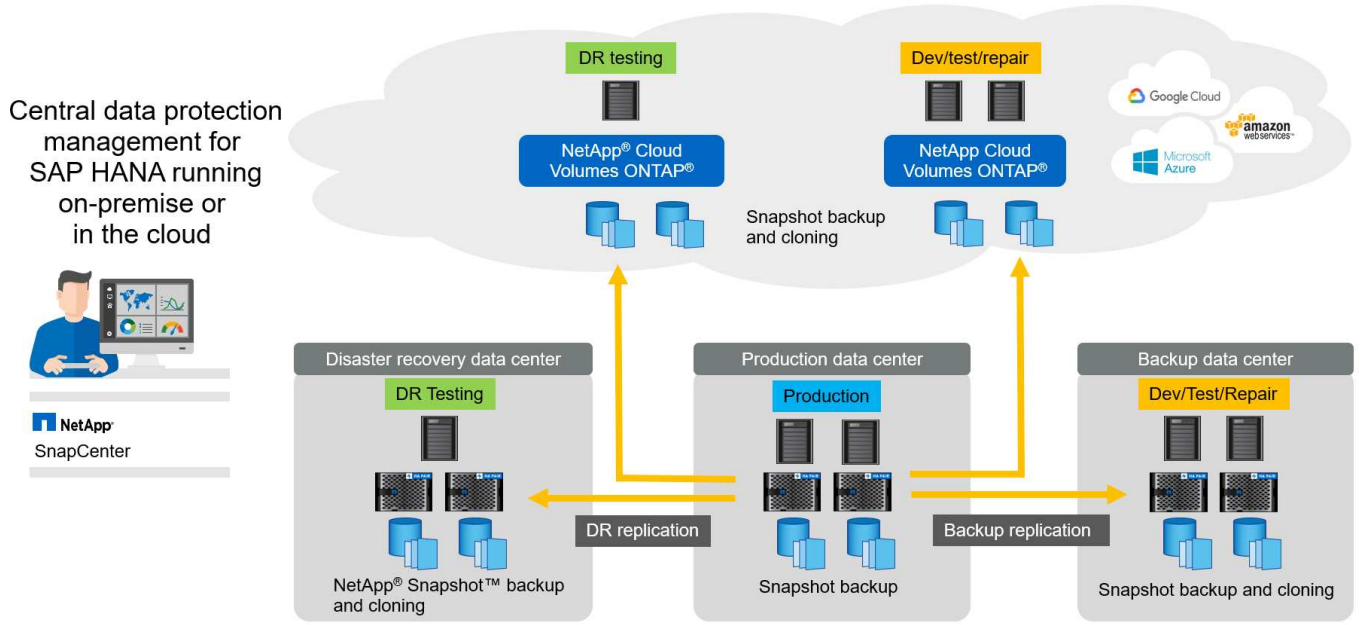
Le copie Snapshot offrono anche vantaggi chiave per le operazioni di ripristino e ripristino. Il software di ripristino dei dati NetApp SnapRestore consente di ripristinare un intero database o, in alternativa, una parte di un database in qualsiasi momento, in base alle copie Snapshot disponibili. Tali 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.

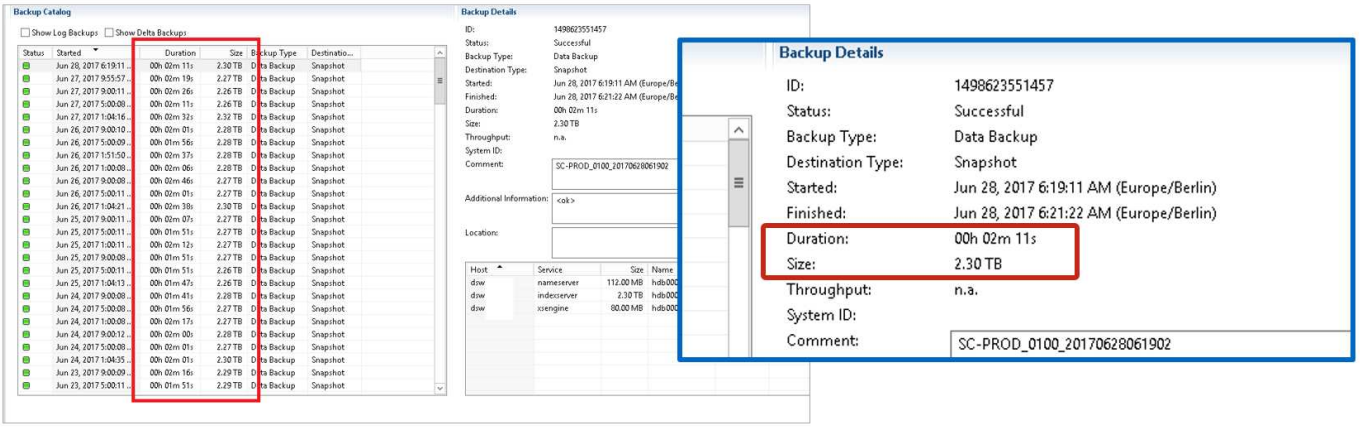
La soluzione può anche essere facilmente estesa a un modello operativo di cloud ibrido. La replica dei dati per il disaster recovery o il backup fuori sede può essere eseguita dai sistemi NetApp ONTAP on-premise alle istanze di Cloud Volumes ONTAP in esecuzione nel cloud. È possibile utilizzare SnapCenter 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.

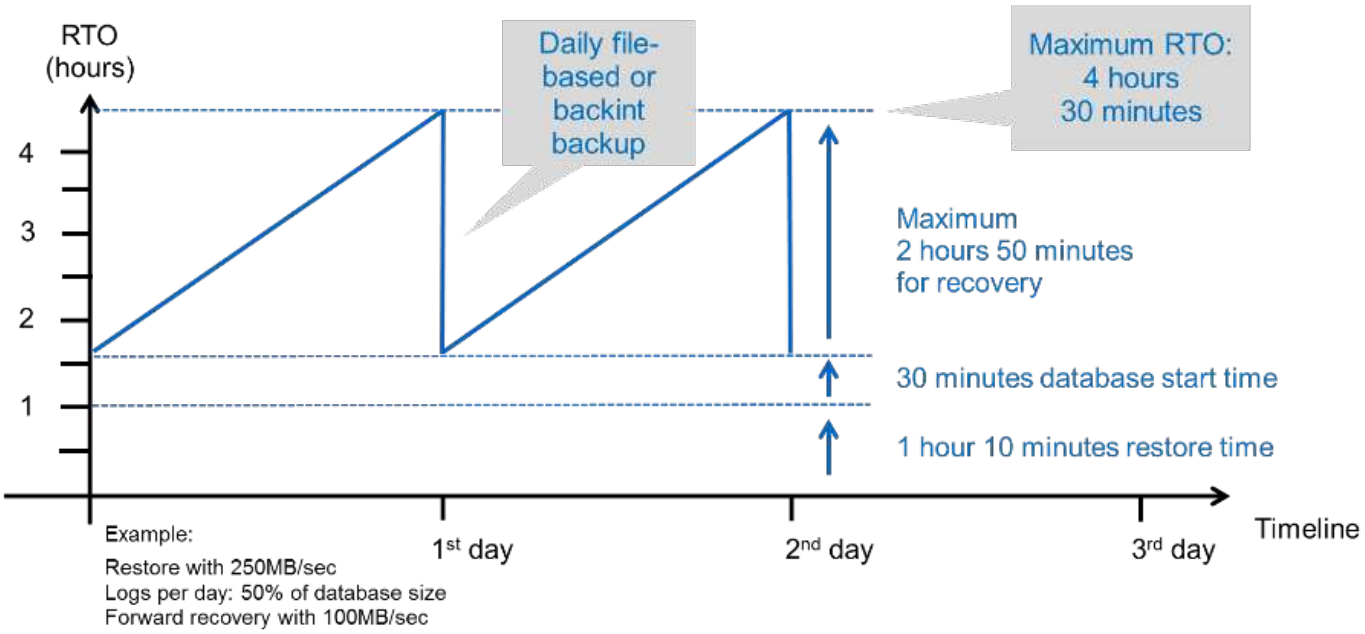
Tempo necessario per il ripristino del database

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.

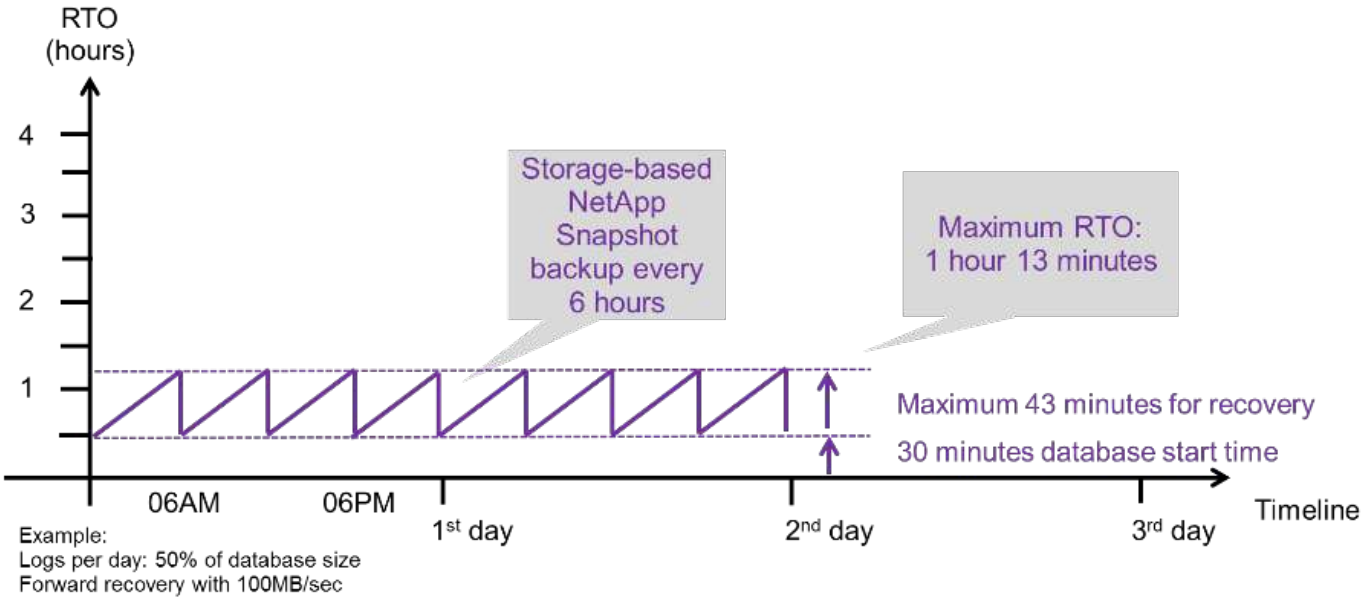
Con i backup dei dati basati su file, la pianificazione del backup è generalmente una volta al giorno. In genere, non è possibile una frequenza di backup più elevata, poiché il backup diminuisce le prestazioni di produzione. Pertanto, nel peggiore dei casi, tutti i log scritti durante la giornata devono 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 = ¼).

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.



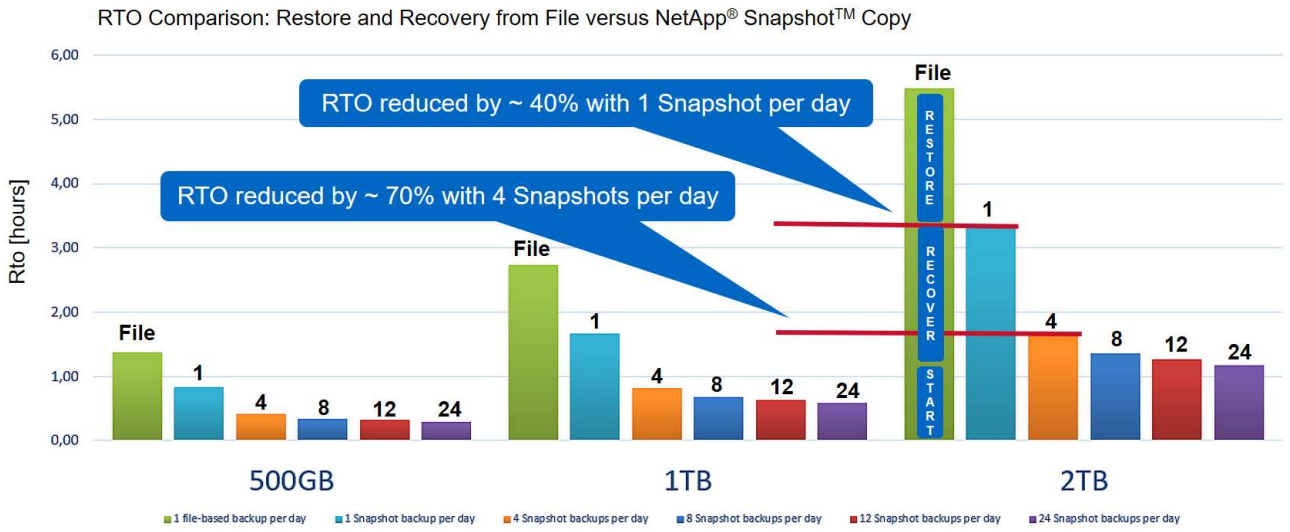
La figura seguente mostra un esempio RTO per un database da 1 TB quando vengono utilizzati backup Snapshot. Con i backup Snapshot basati sullo storage, l'RTO dipende solo dall'ora di avvio del database e dal tempo di ripristino in avanti, in quanto il ripristino viene completato in pochi secondi, indipendentemente 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 appiattire 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.



Assumptions: Restore from file with 250MB/sec; database start with 400MB/s; log files per day: 50% of database size; forward recovery with 250MB/sec

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.

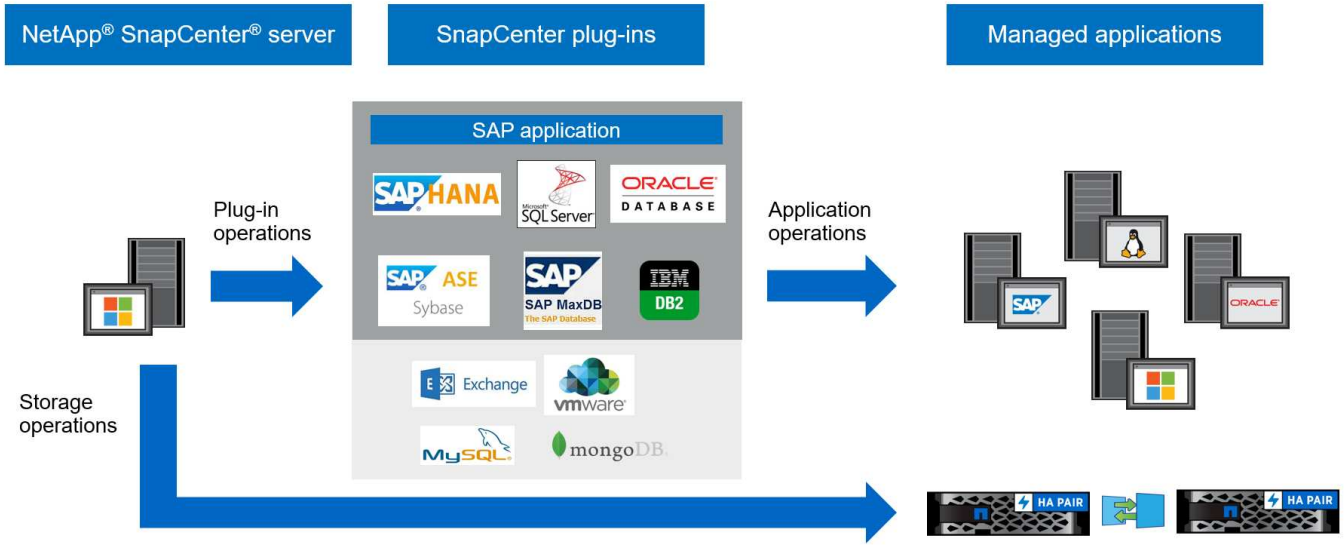
SnapCenter gestisce i dati tra gli endpoint del data fabric basato su NetApp. Puoi utilizzare SnapCenter per replicare i dati tra ambienti on-premise, tra ambienti on-premise e cloud e tra cloud privati, ibridi o pubblici.

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.

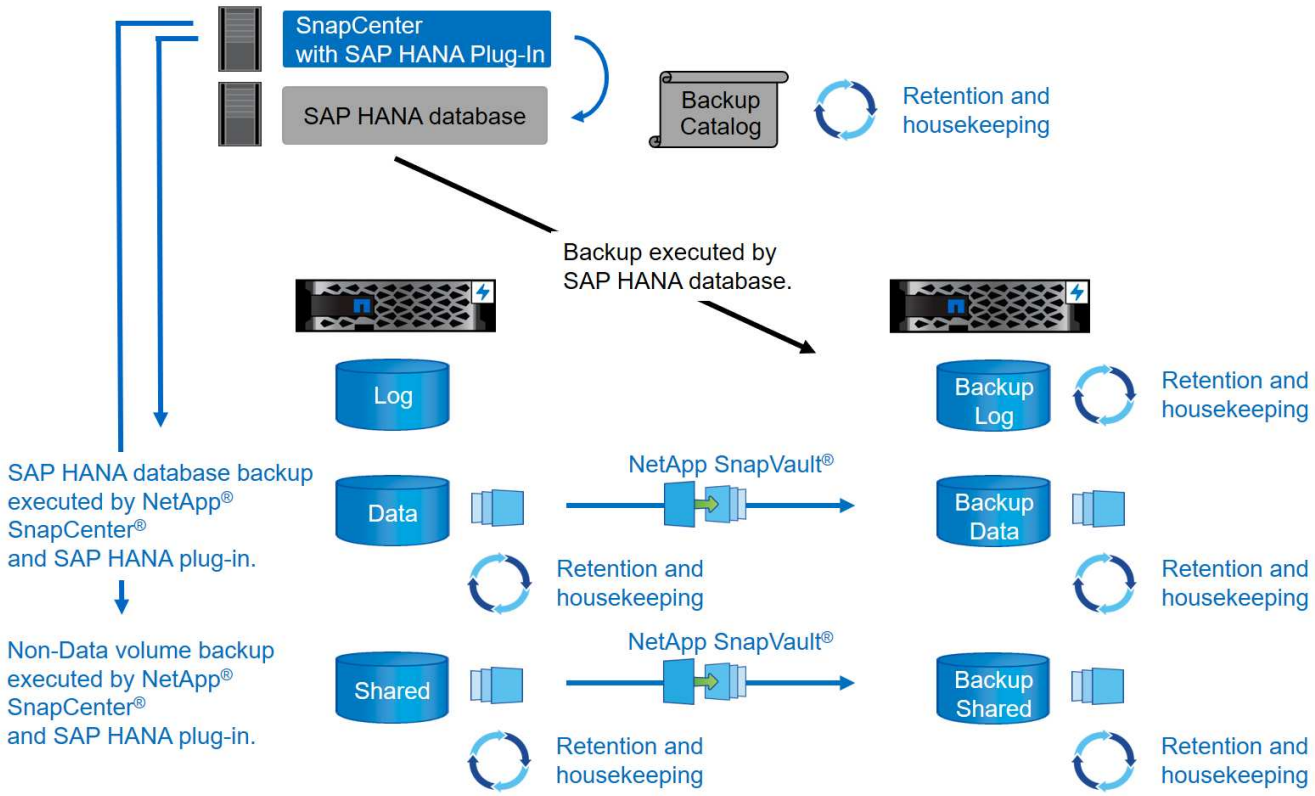
Il database SAP HANA esegue automaticamente i backup dei log. A seconda degli obiettivi del punto di ripristino, sono disponibili diverse opzioni per la posizione di storage dei backup del log:

- 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

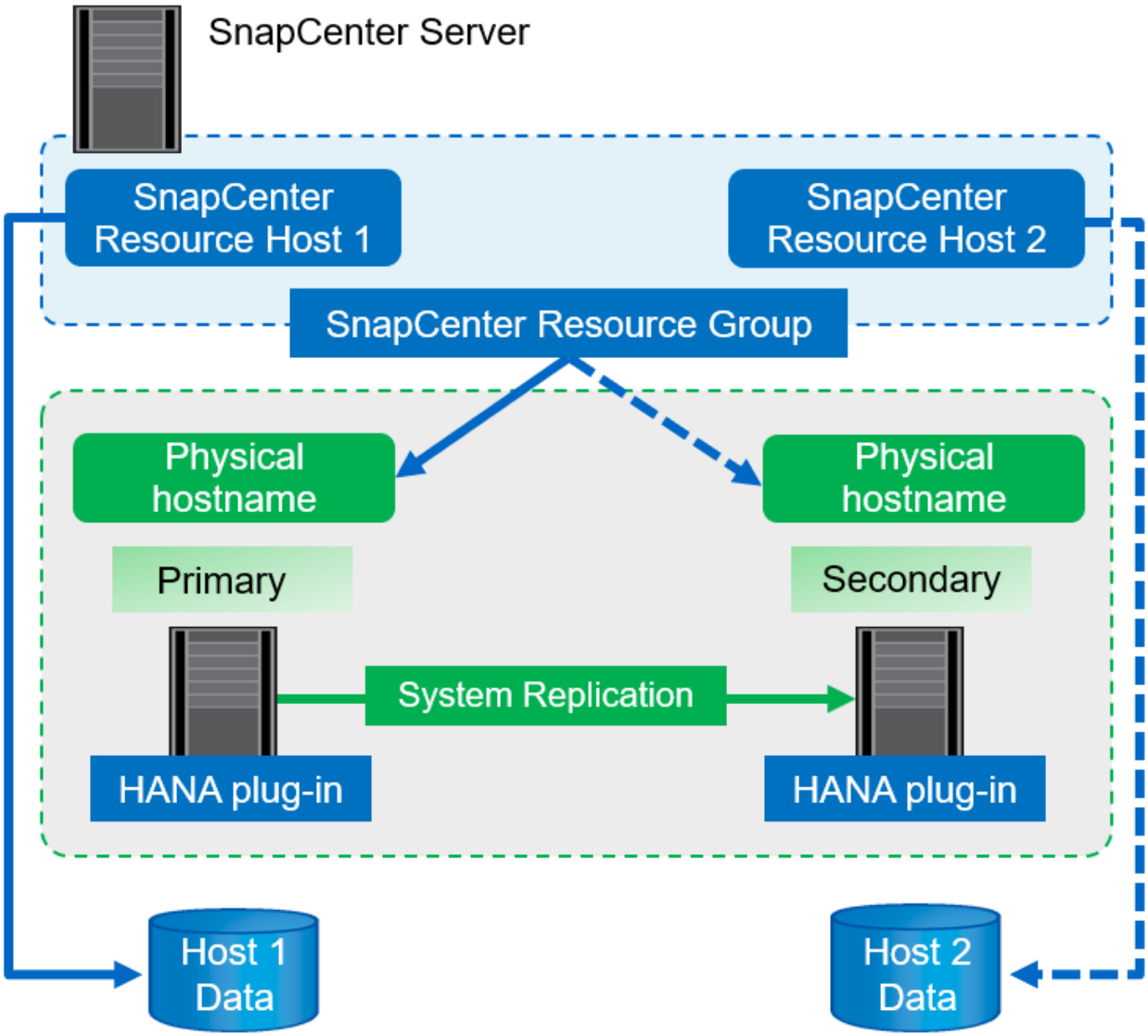
SnapCenter supporta configurazioni SAP HANA a host singolo e multiplo utilizzando sistemi storage NetApp collegati a NFS o FC (AFF e FAS), oltre a sistemi SAP HANA eseguiti su Cloud Volumes ONTAP presso AWS, Azure, la piattaforma cloud di Google e AWS FSX ONTAP utilizzando NFS.

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.

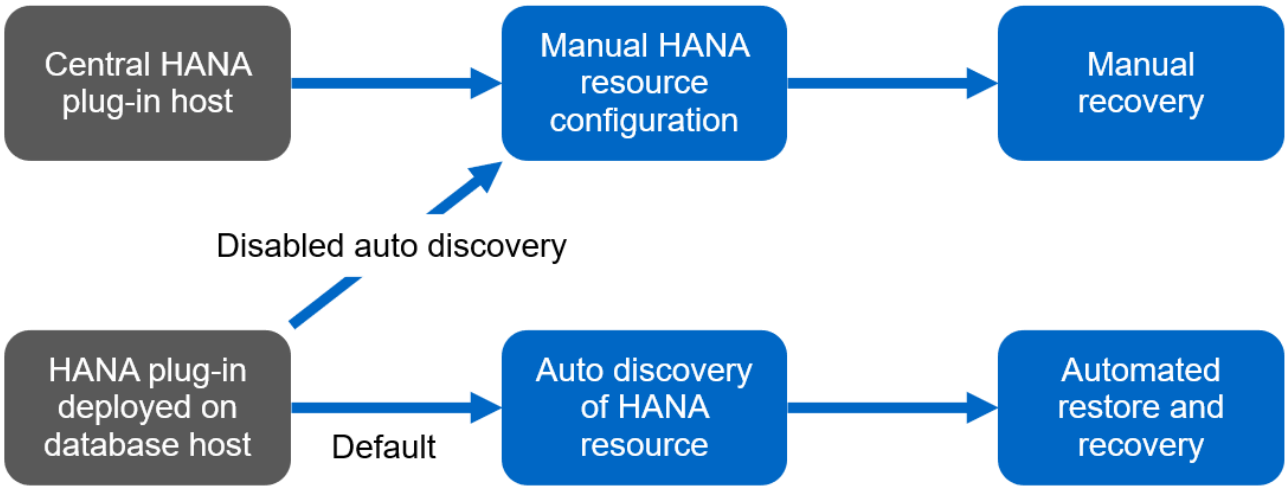
- **Configurazione manuale delle risorse.** le informazioni relative alle risorse HANA e all'impatto dello storage devono essere fornite manualmente.
- **Rilevamento automatico delle risorse HANA.** il rilevamento automatico semplifica la configurazione dei database HANA in SnapCenter e consente il ripristino 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 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	• Container singolo HANA • Contenitori di database multi-tenant SAP HANA (MDC) con uno o più tenant • Replica di sistema HANA	• 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.

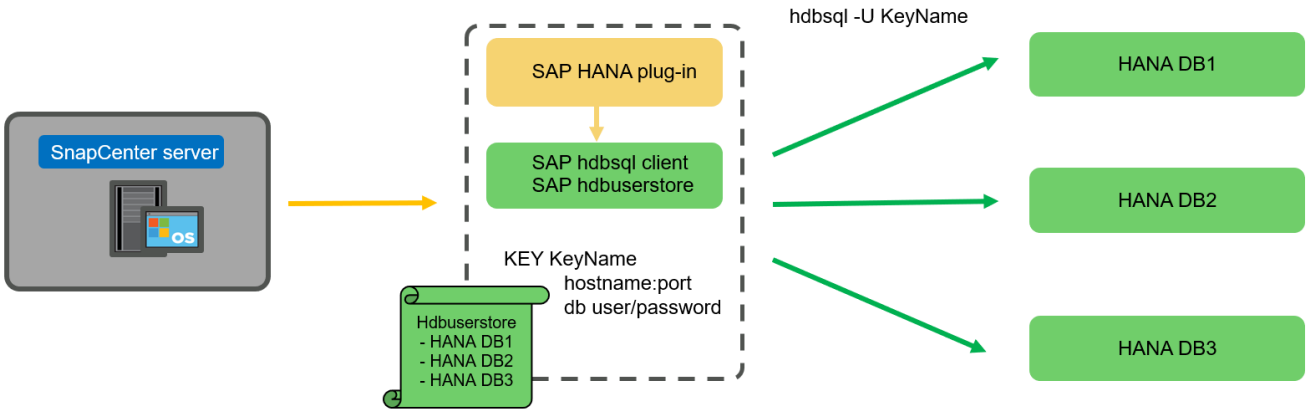
Plug-in HANA installato su:	Architettura HANA	Configurazione del sistema HANA	Infrastruttura
Host plug-in centrale (server SnapCenter o host Linux separato)	Host singolo o multiplo	• Container singolo HANA • HANA MDC con uno o più tenant • Replica di sistema HANA	• Bare metal con NFS • Bare metal con 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.

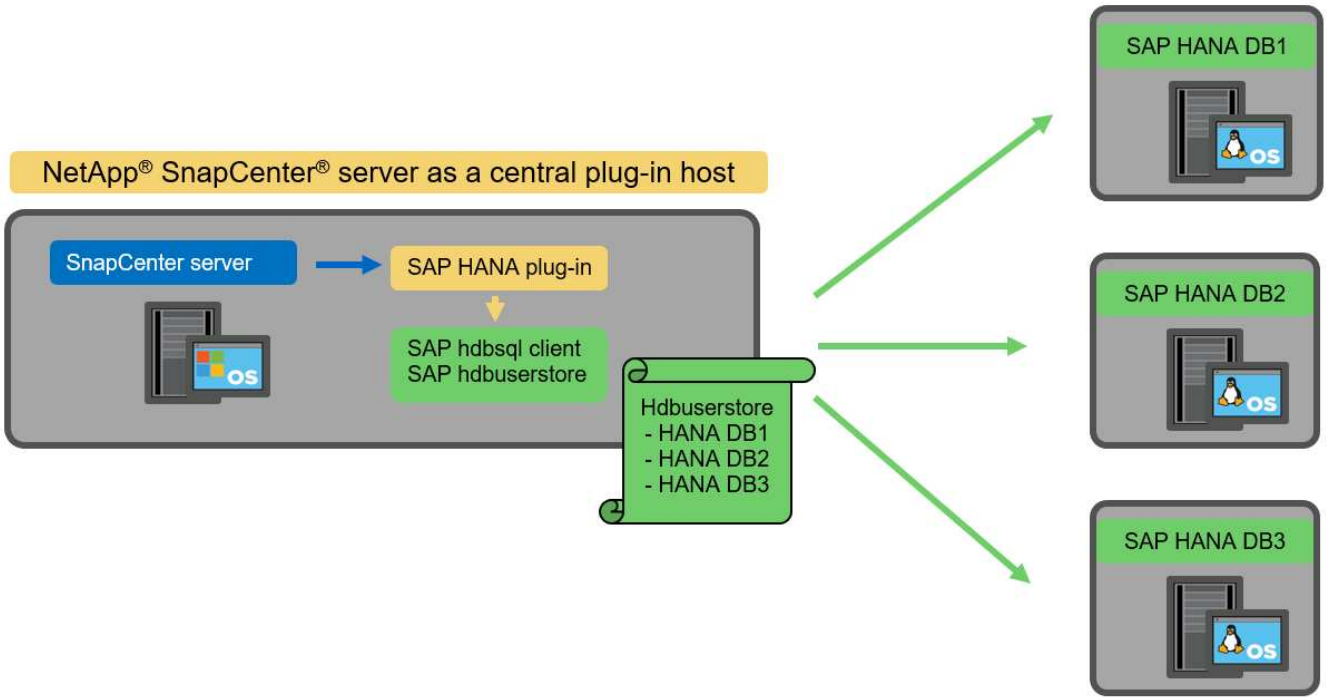
Server SnapCenter ad alta disponibilità

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 hdbattraverso 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.

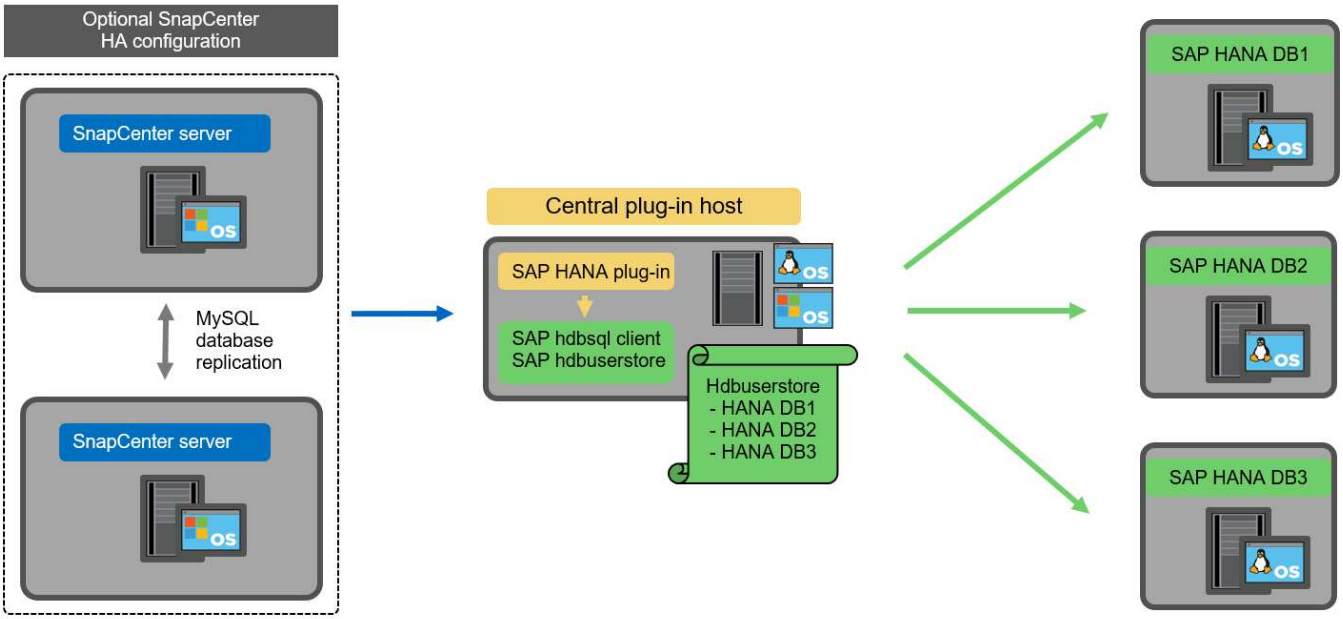
D'altro canto, l'automazione avanzata del workflow per il rilevamento automatico, l'automazione del ripristino e del ripristino, nonché le operazioni di refresh del sistema SAP, richiedono l'installazione dei componenti SnapCenter sull'host del database. Quando si utilizza un host plug-in HANA centrale,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

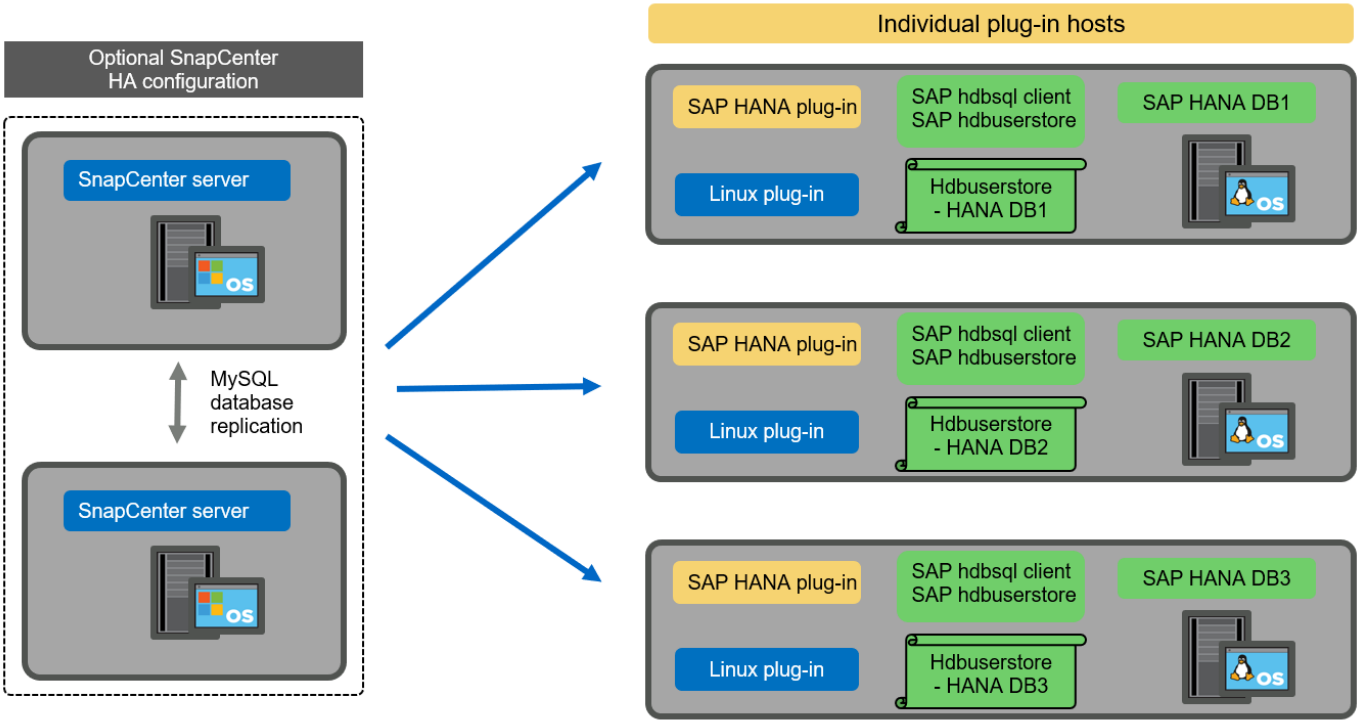


La stessa restrizione relativa alla disponibilità delle funzionalità descritta nella sezione precedente si applica anche a un host plug-in centrale separato.

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.



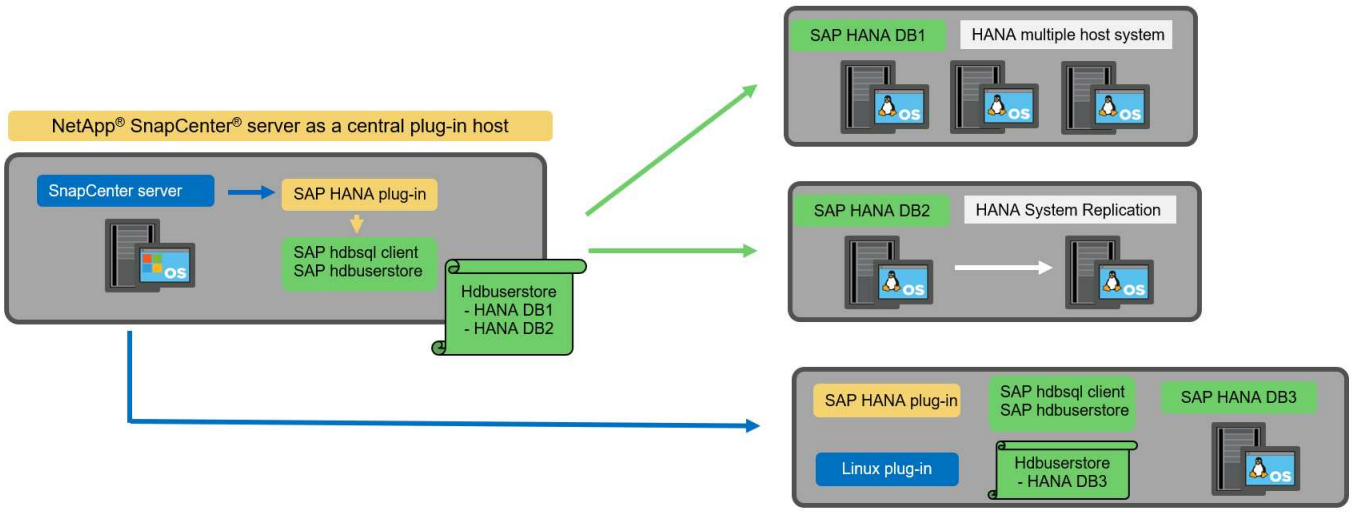
Quando il plug-in HANA viene installato su ogni singolo host di database HANA, sono disponibili tutte le funzionalità, come il rilevamento automatico e il ripristino e ripristino automatici. Inoltre, il server SnapCenter può essere configurato in una configurazione ha.

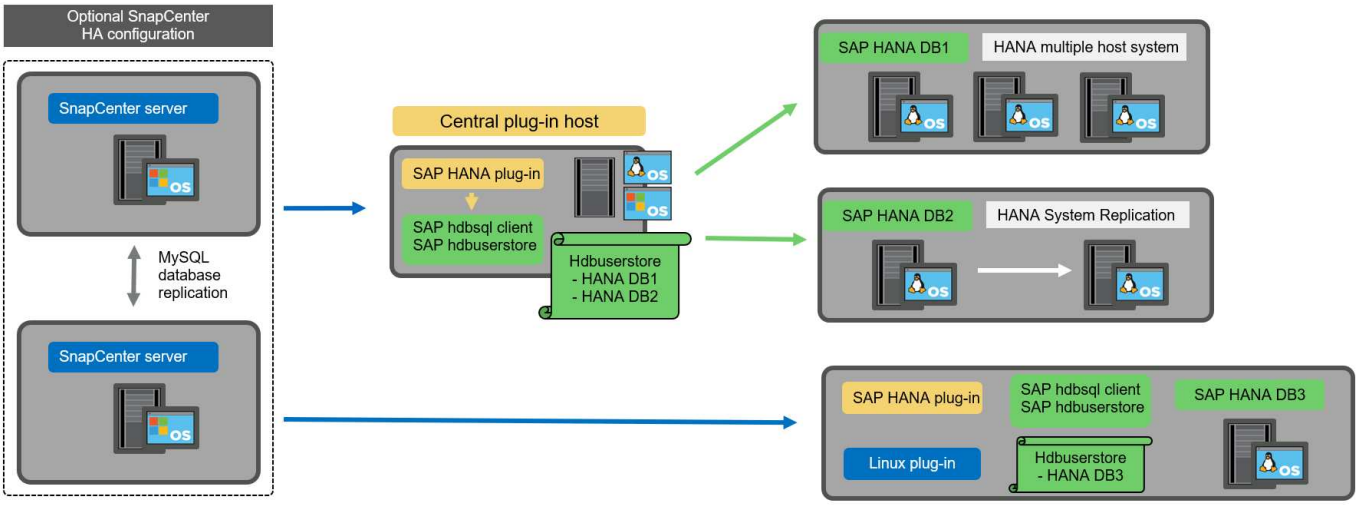
Implementazione di plug-in HANA misti

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.

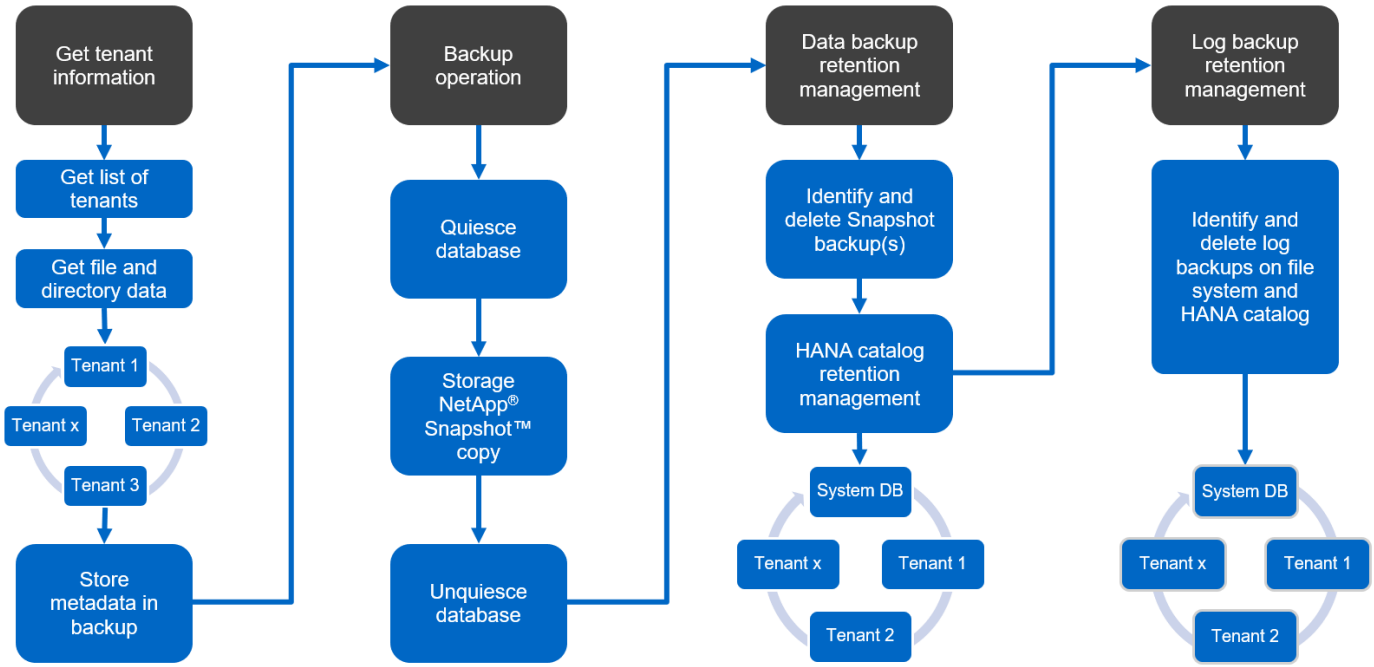
Per abilitare una singola operazione di ripristino del tenant, SnapCenter deve sapere quali tenant sono inclusi in ogni backup Snapshot. Inoltre, deve sapere quali file e directory appartengono a ciascun tenant incluso nel backup Snapshot.

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.

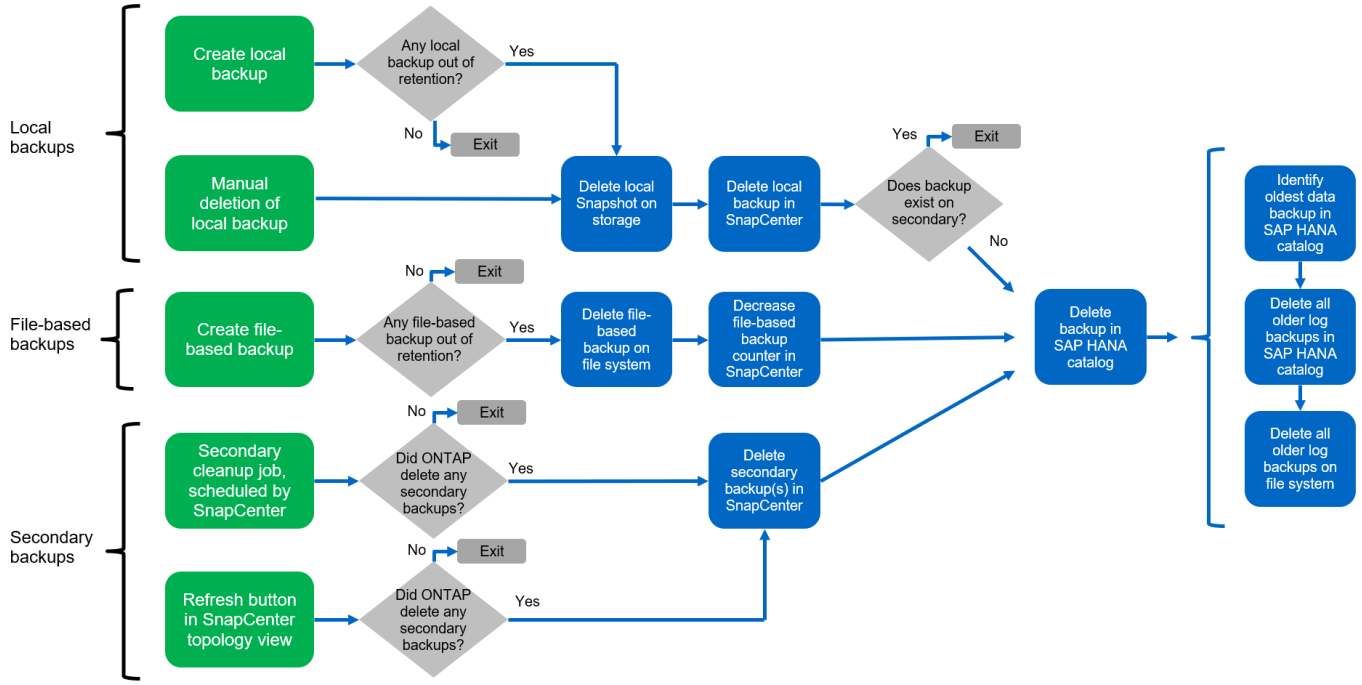
Questo passaggio viene eseguito solo se la gestione del backup dei log non è disattivata.

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

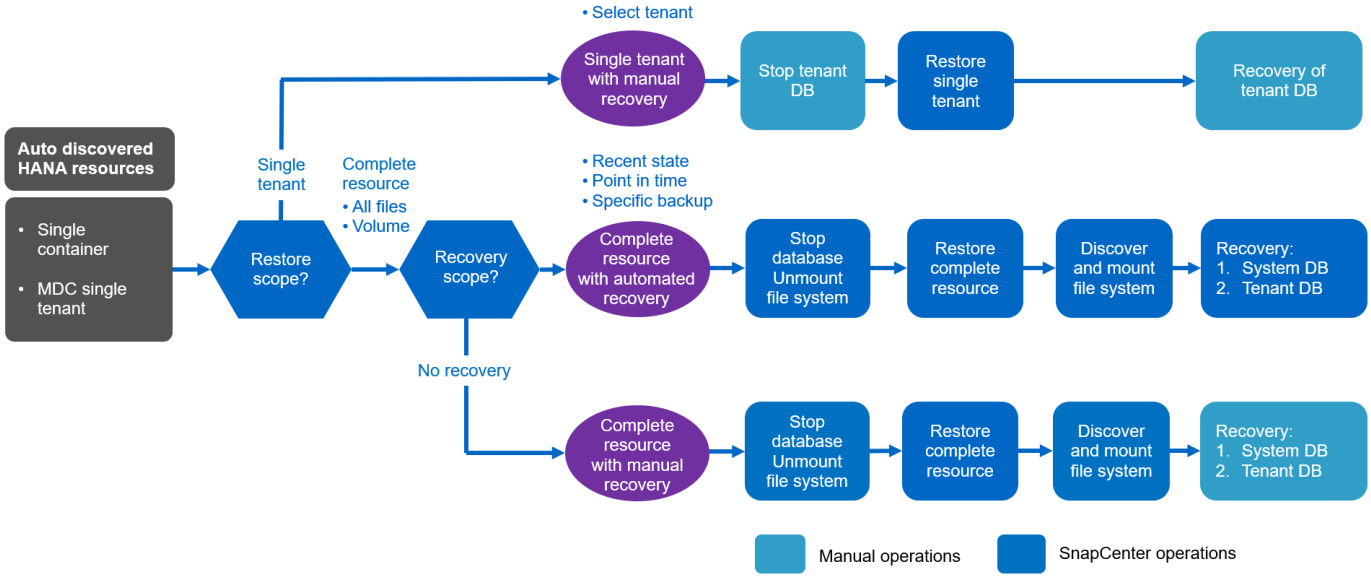
database tenant.

- 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.



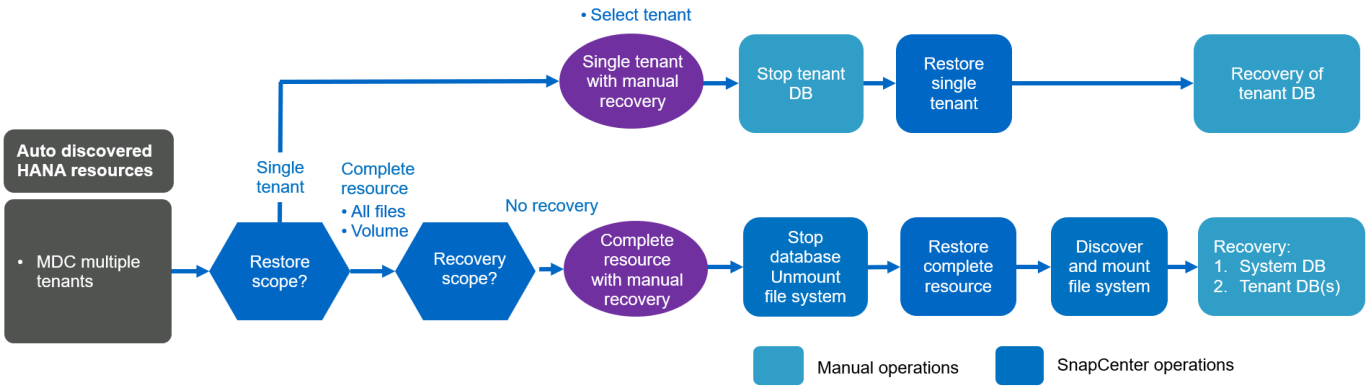
Ripristino e ripristino di più sistemi tenant HANA MDC rilevati automaticamente

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

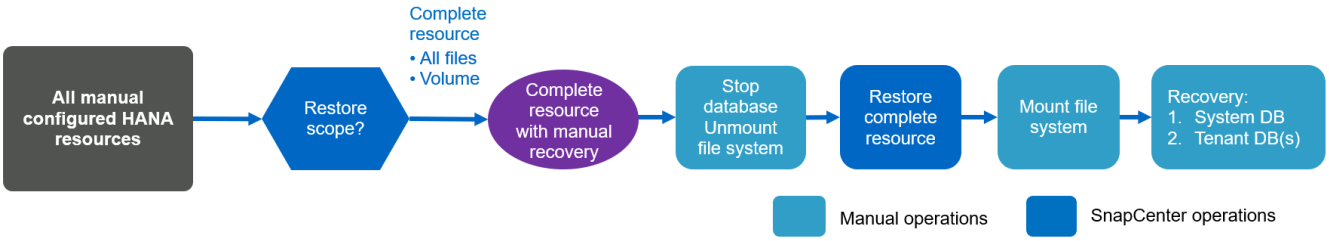
I flussi di lavoro sono gli stessi descritti nella sezione precedente.



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	• 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
	• 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
	• Ripristino del tenant	Manuale	Non richiesto	Manuale
Rilevamento automatico di più tenant MDC	• 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
	• Ripristino del tenant	Manuale	Non richiesto	Manuale
Tutte le risorse configurate manualmente	• 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:

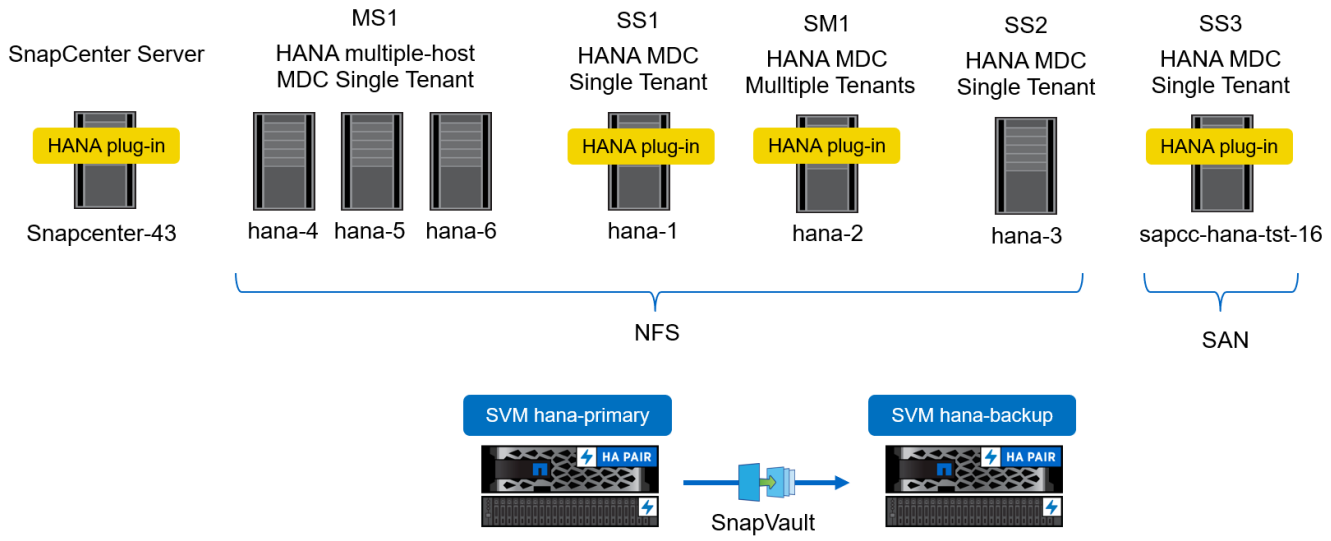
- **MS1.**
  - Sistema multi-host MDC single tenant SAP HANA
  - Gestito con un host plug-in centrale (server SnapCenter)
  - Utilizza NFS come protocollo storage
- **SS1.**
  - Sistema single-tenant SAP HANA MDC a host singolo
  - Rilevato automaticamente con il plug-in HANA installato sull'host del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

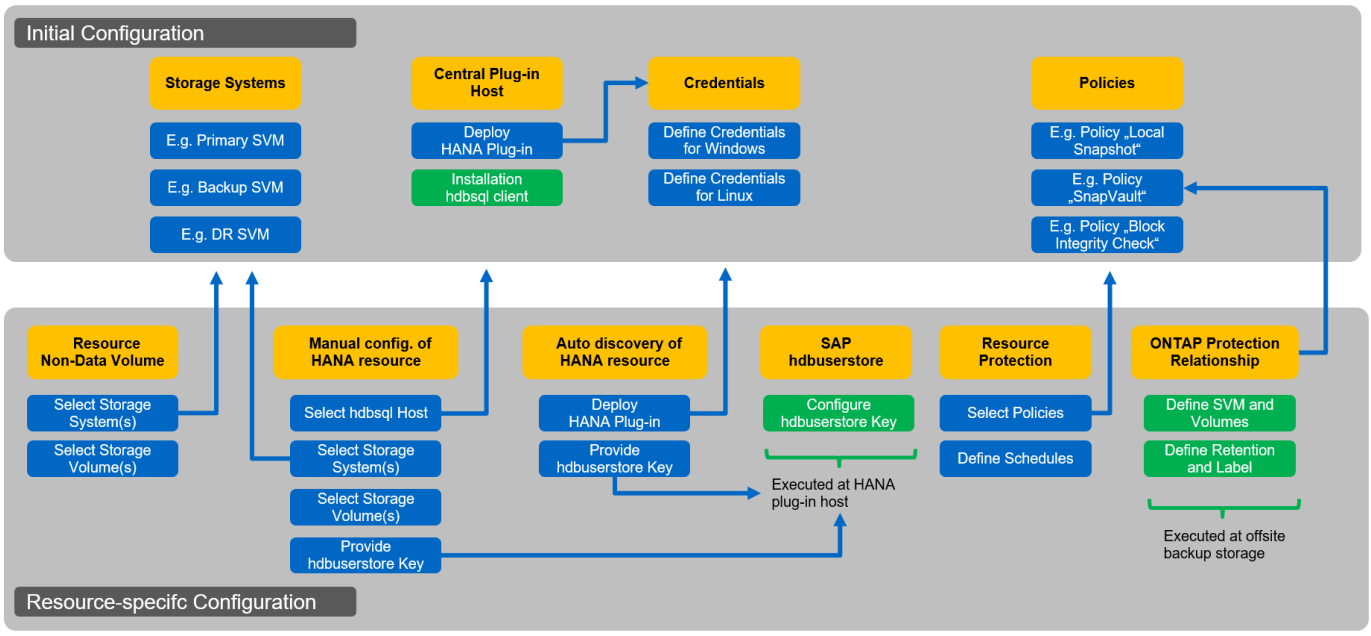


Configurazione di SnapCenter

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

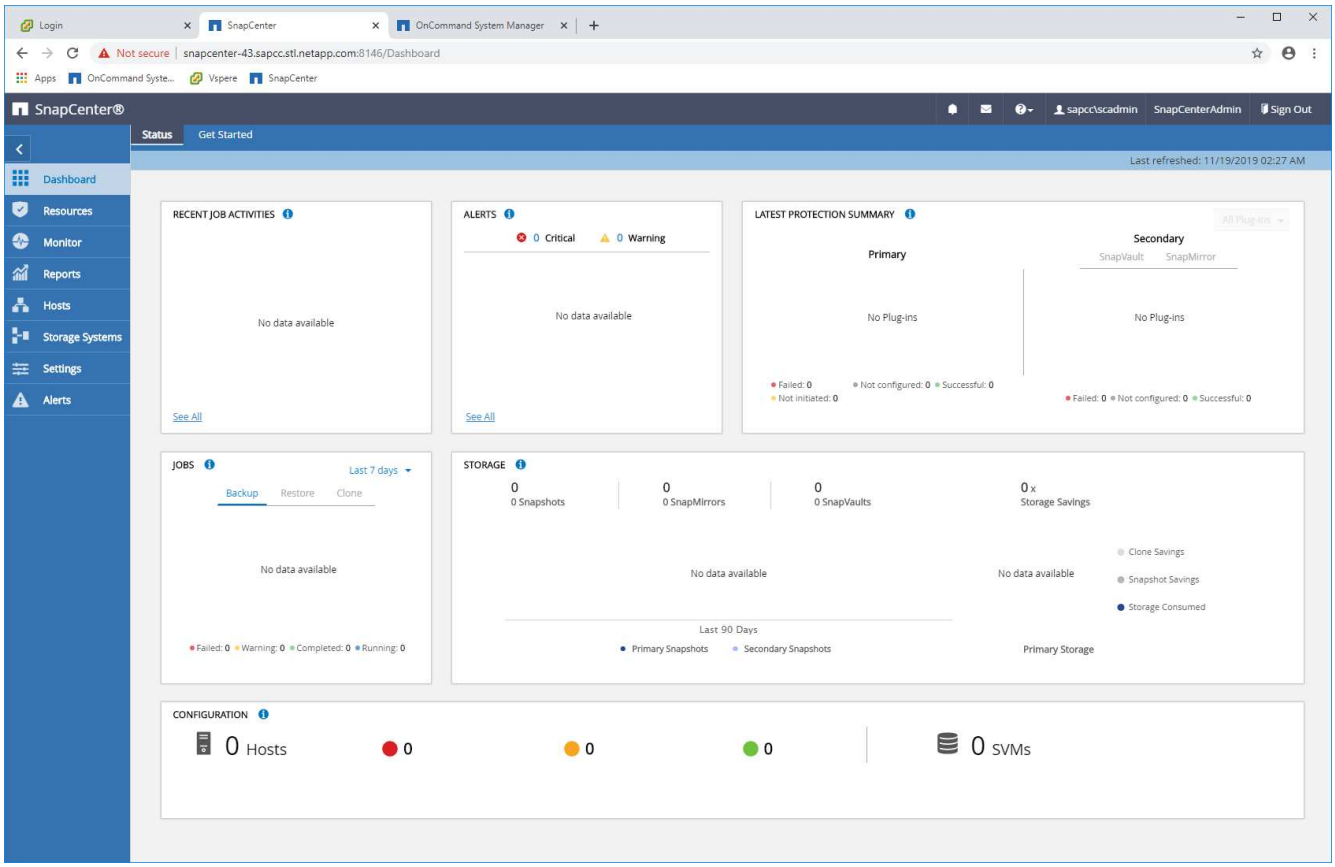
La configurazione iniziale include i seguenti passaggi:

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.

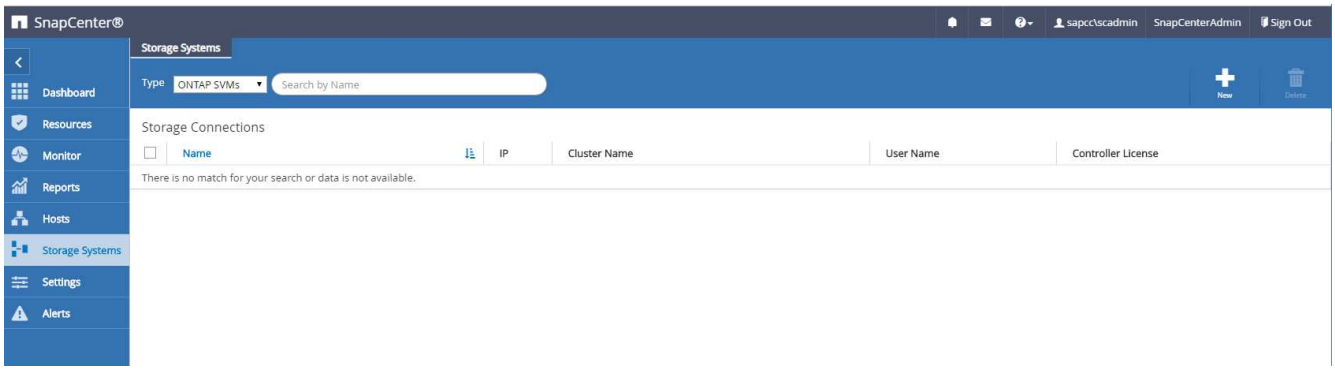
Configurazione del sistema storage

1. Accedere alla GUI del server SnapCenter.



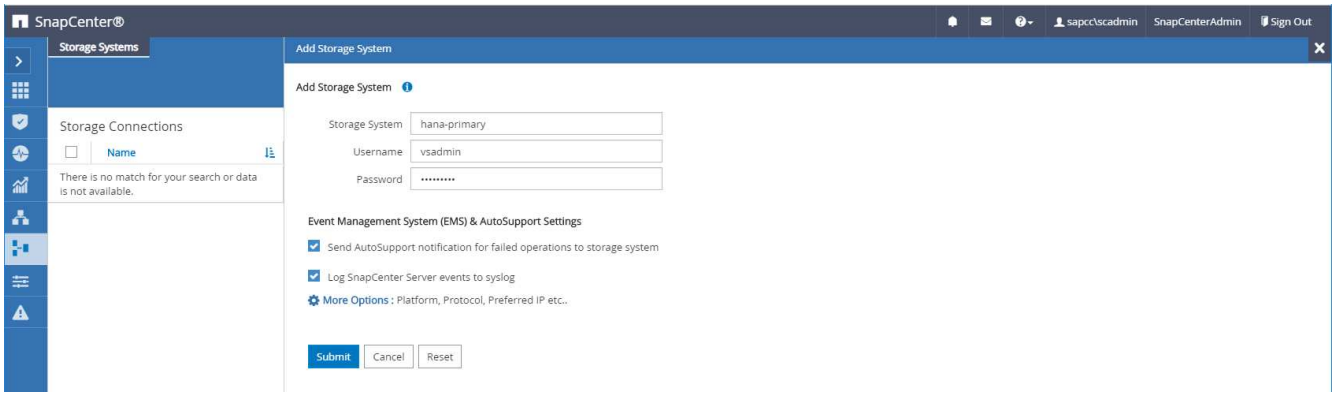
2. Selezionare Storage Systems (sistemi storage).

> 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.

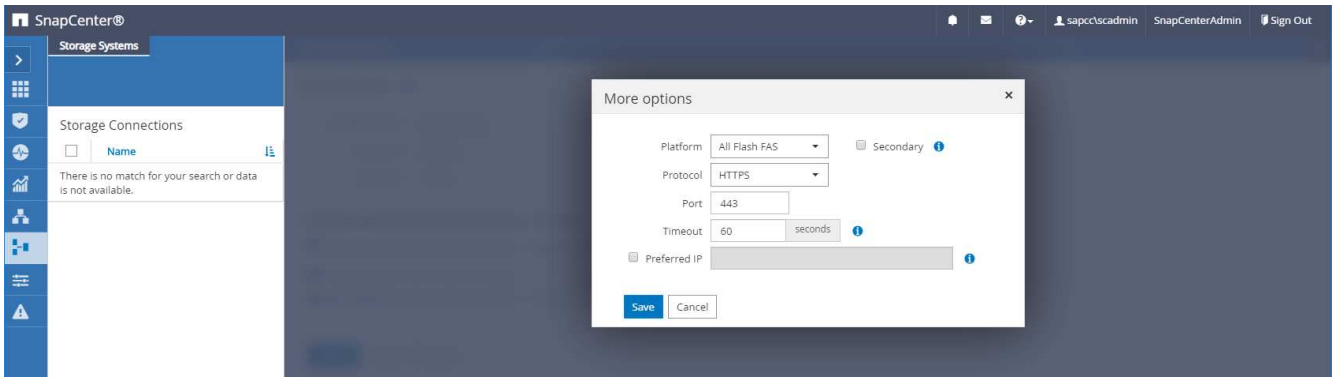
> L'utente SVM non deve essere l'utente vsadmin, come mostrato nella schermata. In genere, un utente viene configurato sulla SVM e assegnato i permessi necessari per eseguire le operazioni di backup e ripristino. I dettagli sui privilegi richiesti sono disponibili nella "Guida all'installazione di SnapCenter"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



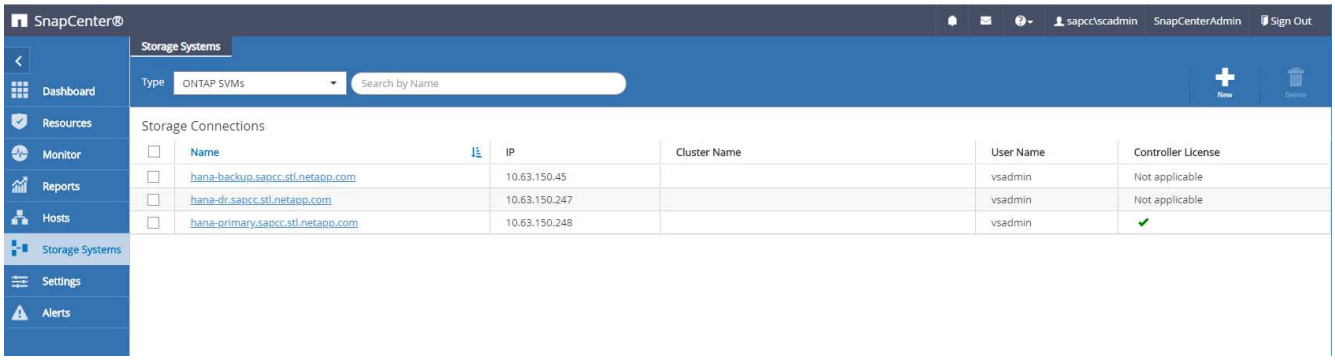
4. Fare clic su More Options (altre opzioni) per configurare la piattaforma di storage.

   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.

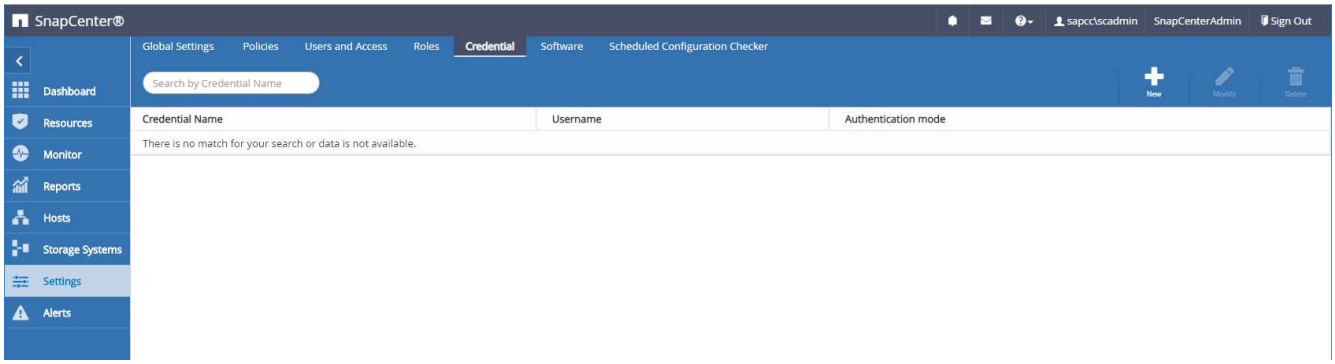


5. Aggiungere altri sistemi storage secondo necessità. Nel nostro esempio, sono stati aggiunti uno storage aggiuntivo per il backup fuori sede e uno per il disaster recovery.

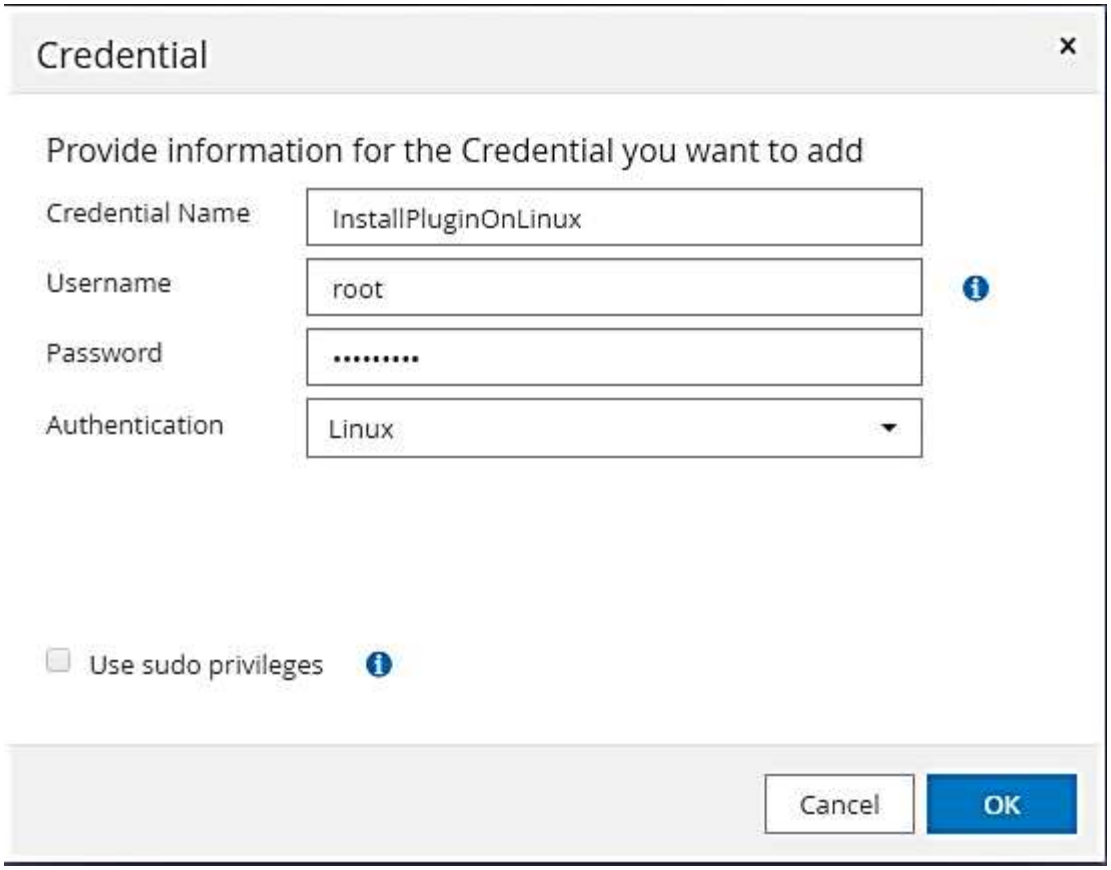


Configurazione delle credenziali

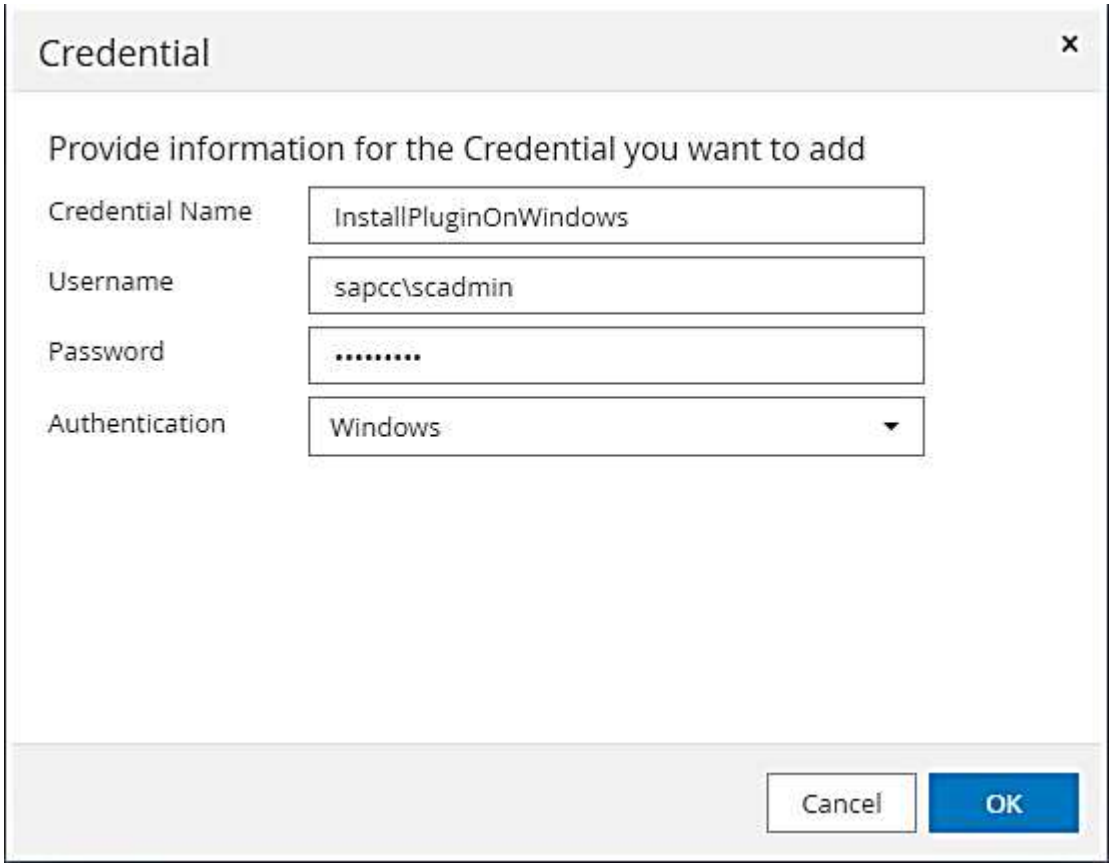
1. Accedere a Impostazioni, selezionare credenziali e fare clic su nuovo.



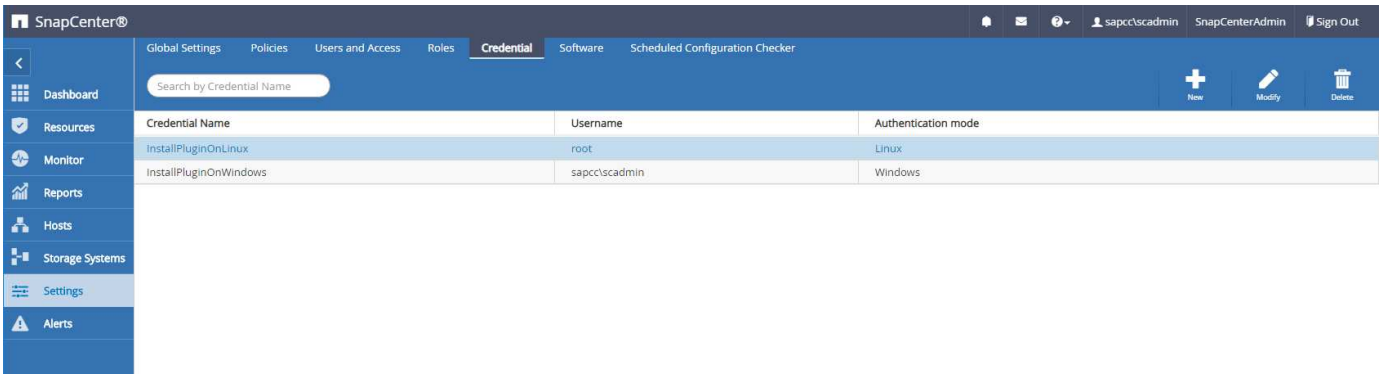
2. Fornire le credenziali per l'utente utilizzato per le installazioni plug-in sui sistemi Linux.



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



La figura seguente mostra le credenziali configurate.

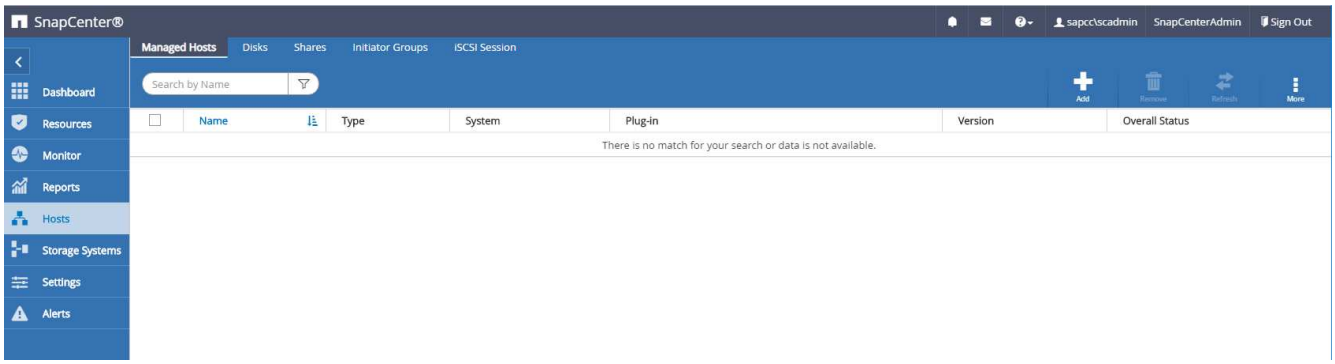


Installazione del plug-in SAP HANA su un host plug-in centrale

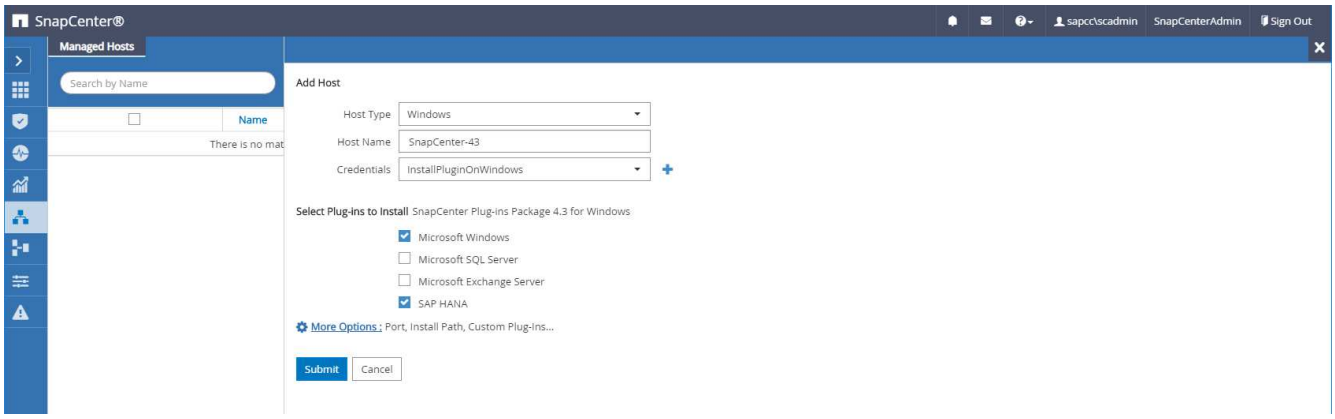
Nella configurazione di laboratorio, il server SnapCenter viene utilizzato anche come host plug-in HANA centrale. L'host Windows su cui viene eseguito il server SnapCenter viene aggiunto come host e il plug-in SAP HANA viene installato sull'host Windows.

> 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.

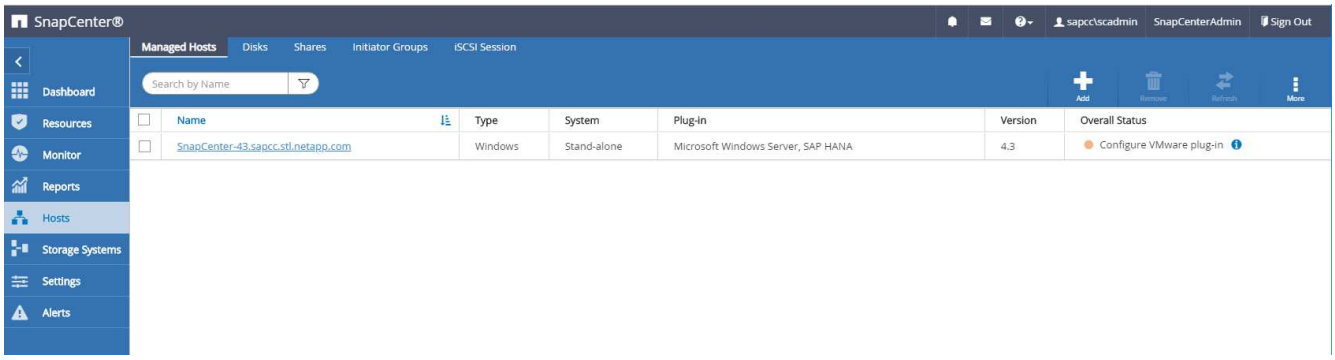
1. Accedere a hosts e fare clic su Add (Aggiungi).



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.

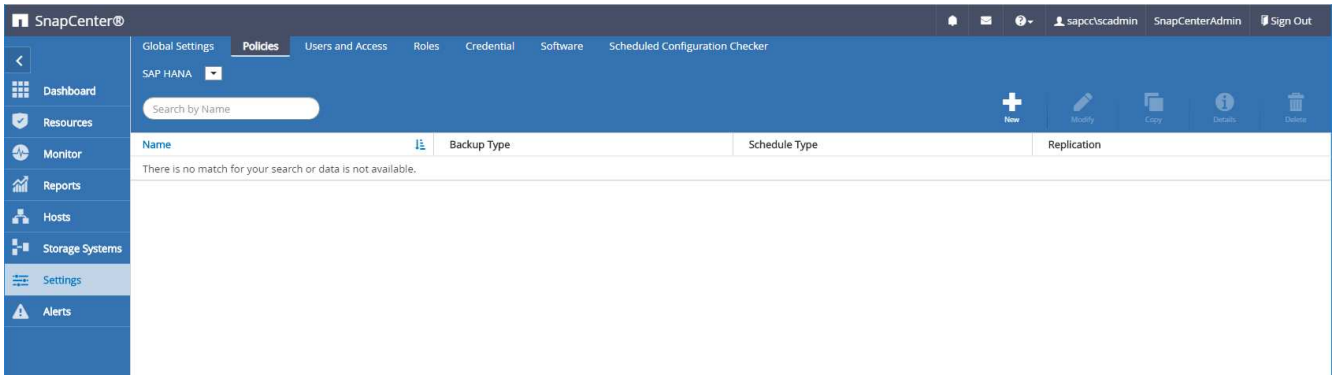
Una configurazione minima tipica è costituita dai seguenti criteri:

- 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`

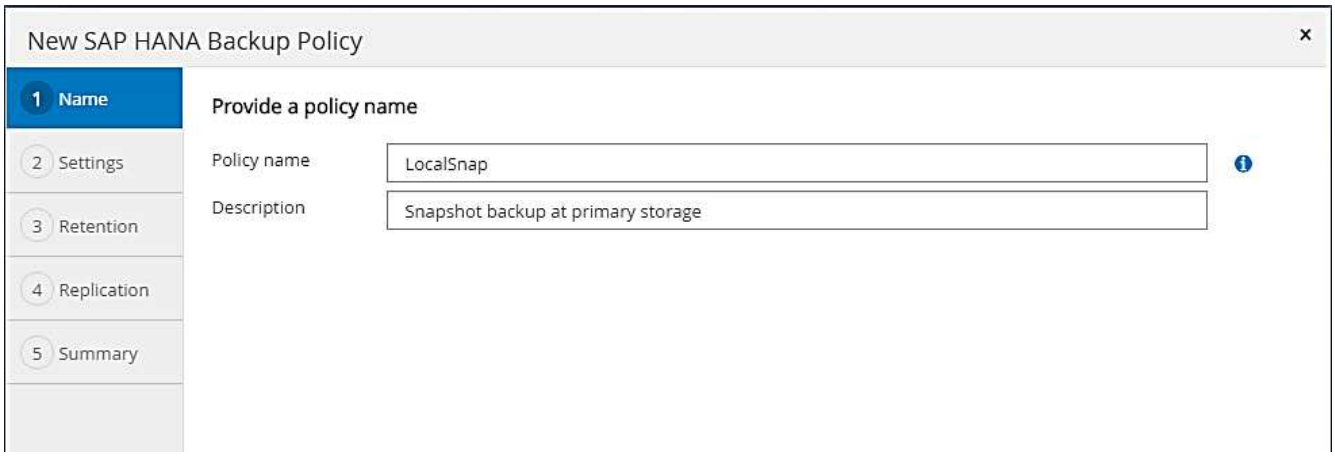
Le sezioni seguenti descrivono la configurazione di questi tre criteri.

Policy per backup Snapshot orari

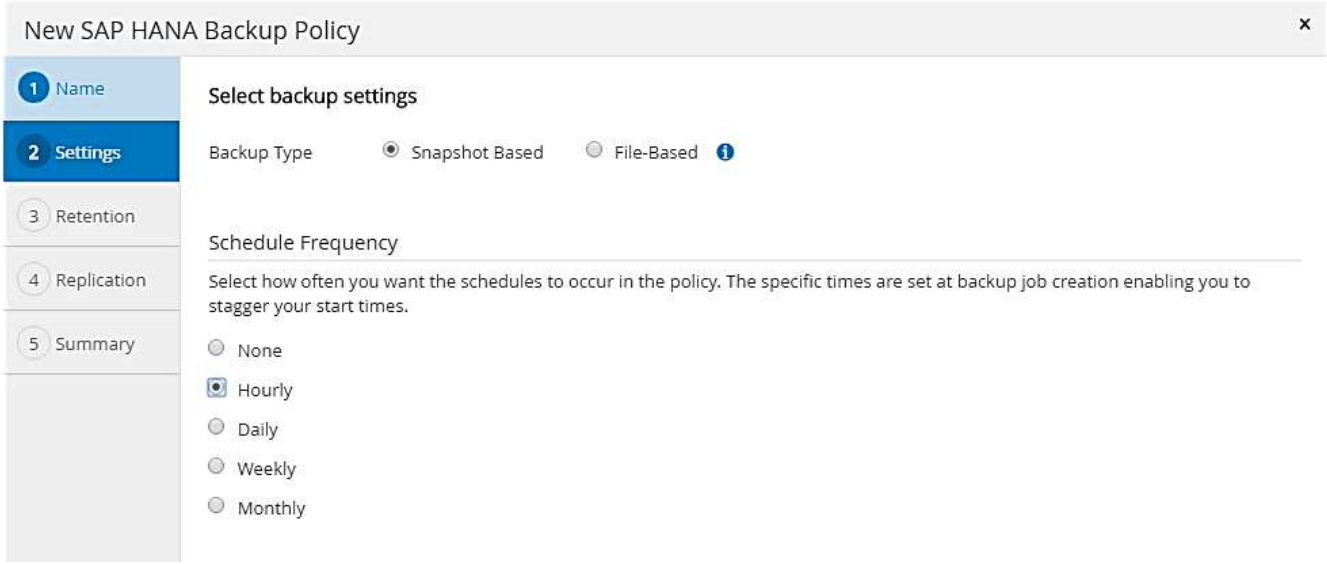
1. Accedere a Impostazioni > Criteri e fare clic su nuovo.



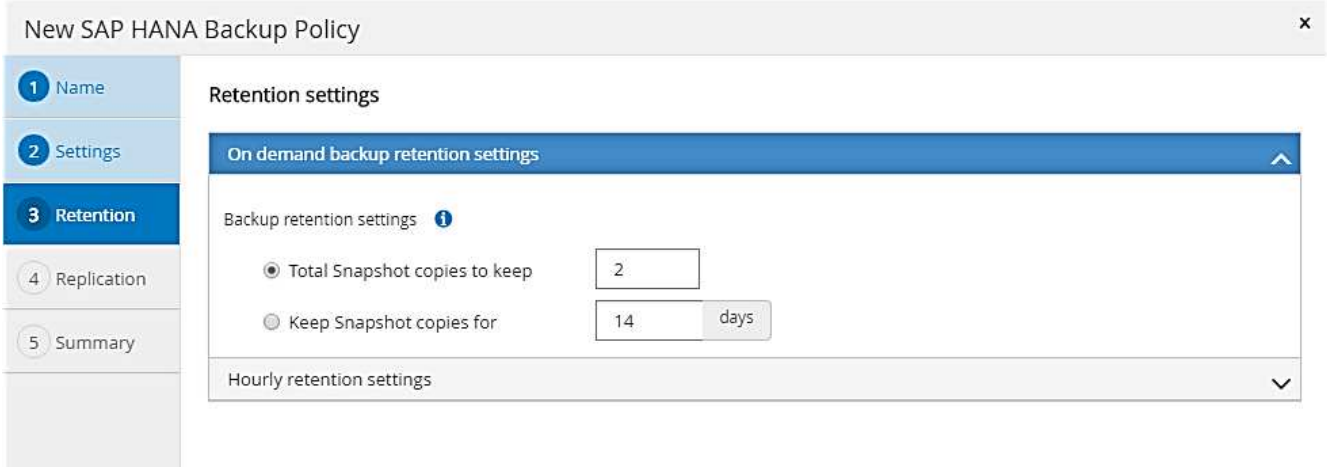
2. Immettere il nome e la descrizione della policy. Fare clic su Avanti.



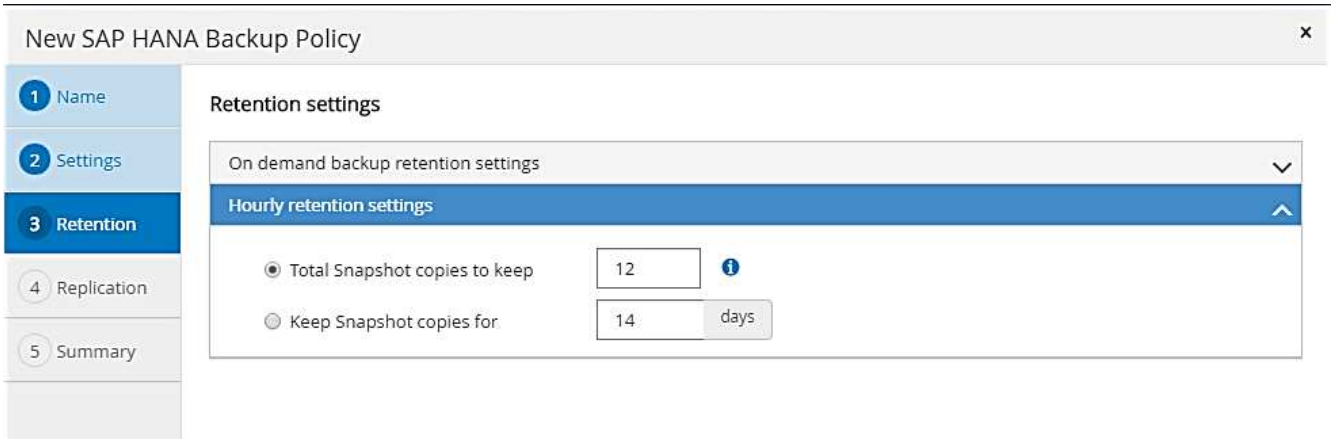
3. Selezionare il tipo di backup basato su Snapshot e selezionare orario per la frequenza di pianificazione.



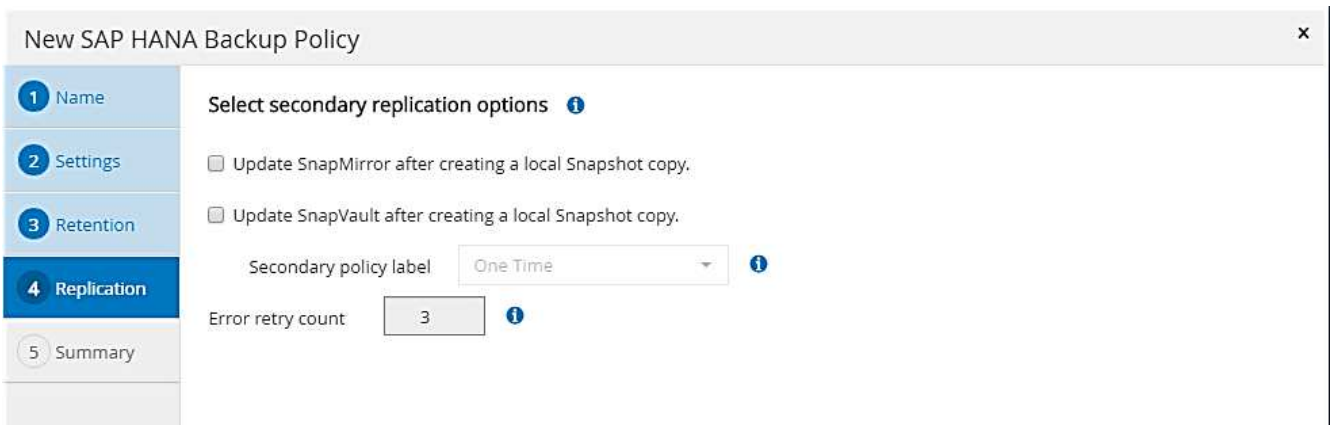
4. Configurare le impostazioni di conservazione per i backup on-demand.



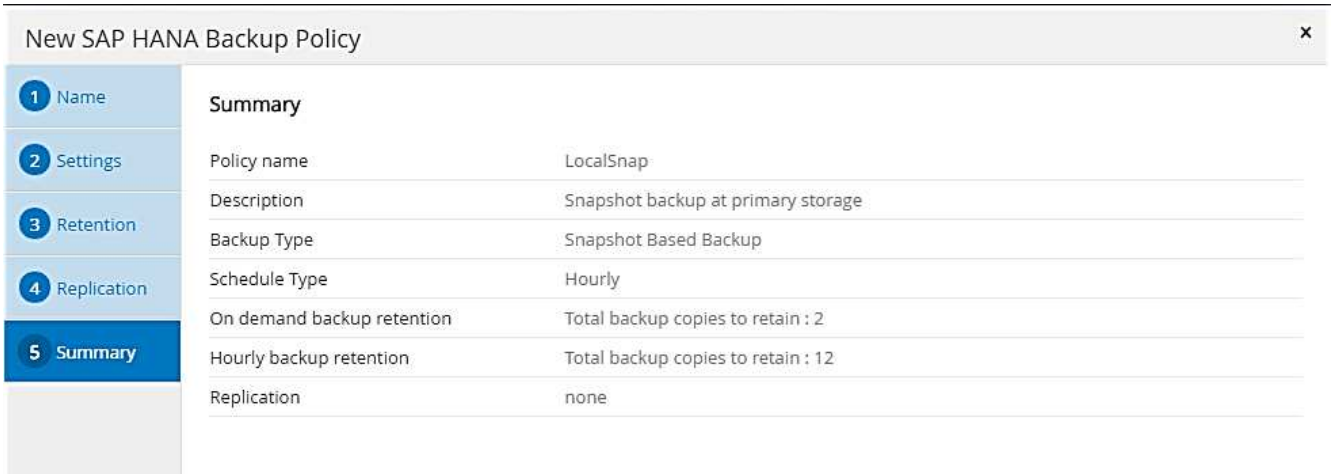
5. Configurare le impostazioni di conservazione per i backup pianificati.



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

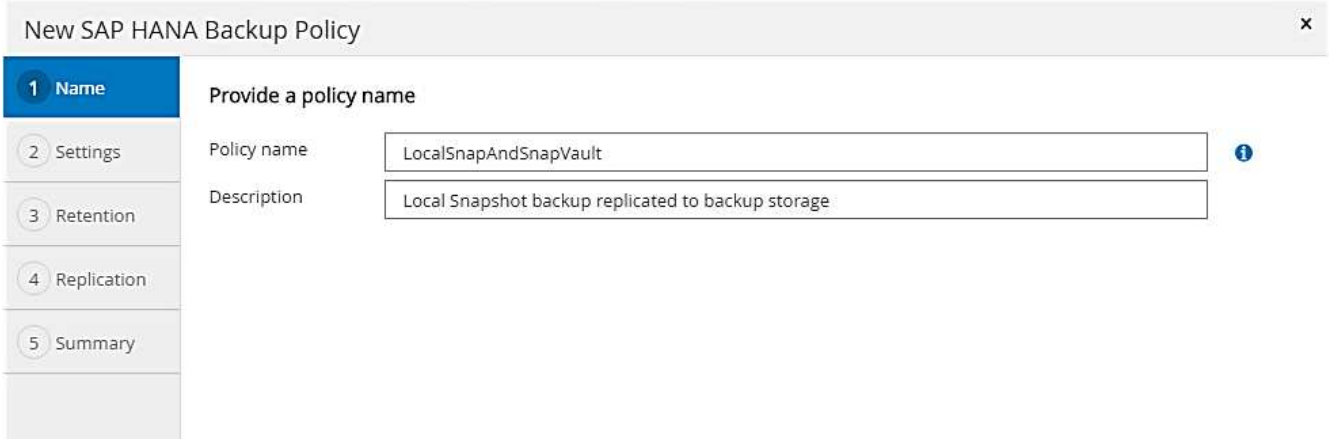


7. Nella pagina Riepilogo, fare clic su fine.

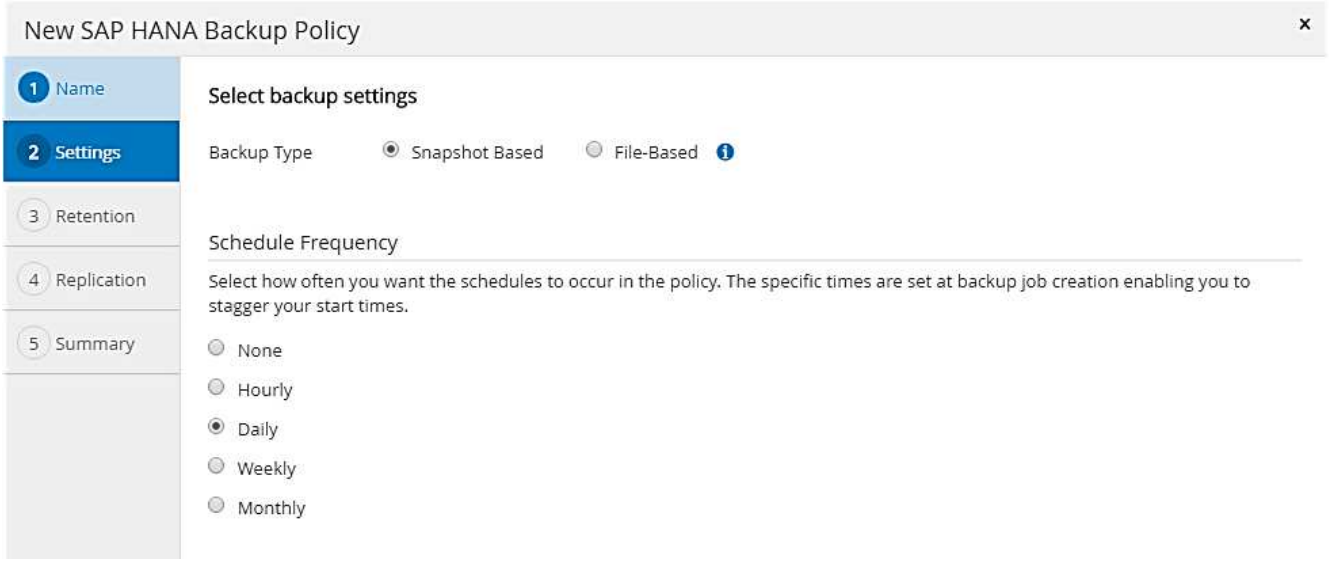


Policy per backup Snapshot giornalieri con replica SnapVault

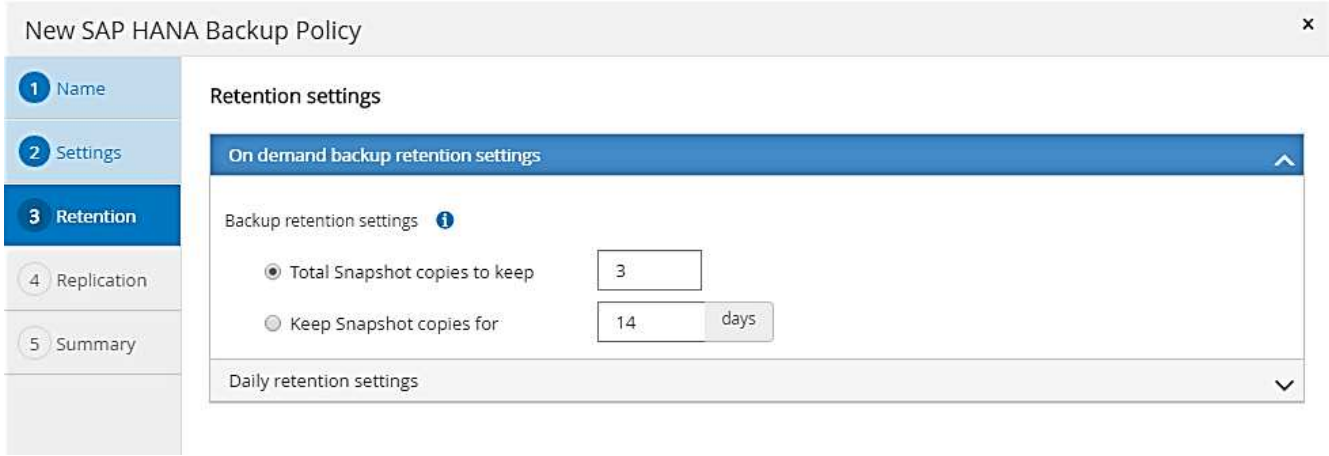
1. Accedere a Impostazioni > Criteri e fare clic su nuovo.
2. Immettere il nome e la descrizione della policy. Fare clic su Avanti.



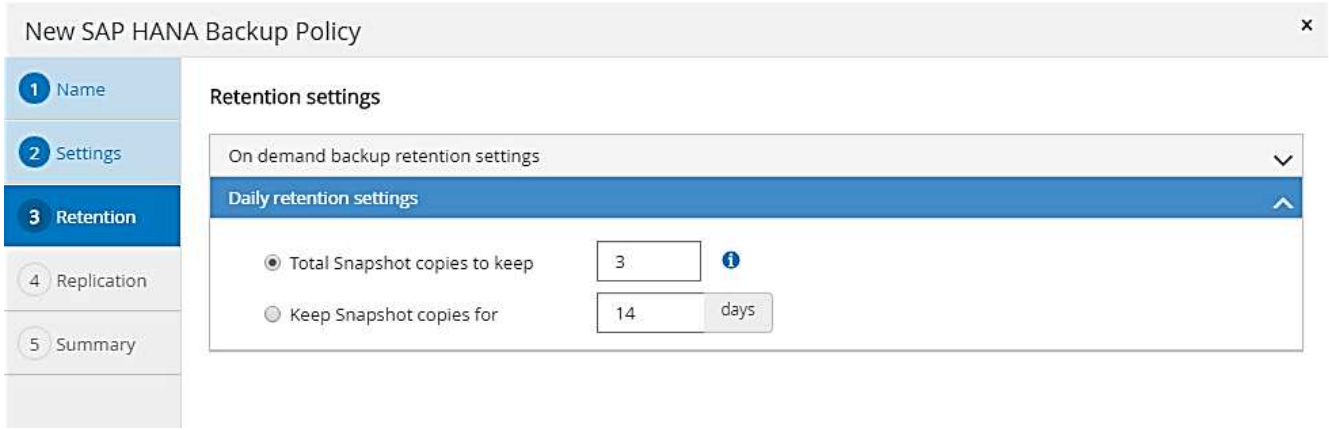
3. Impostare il tipo di backup su Snapshot Based (basato su snapshot) e la frequenza di pianificazione su Daily (giornaliero).



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

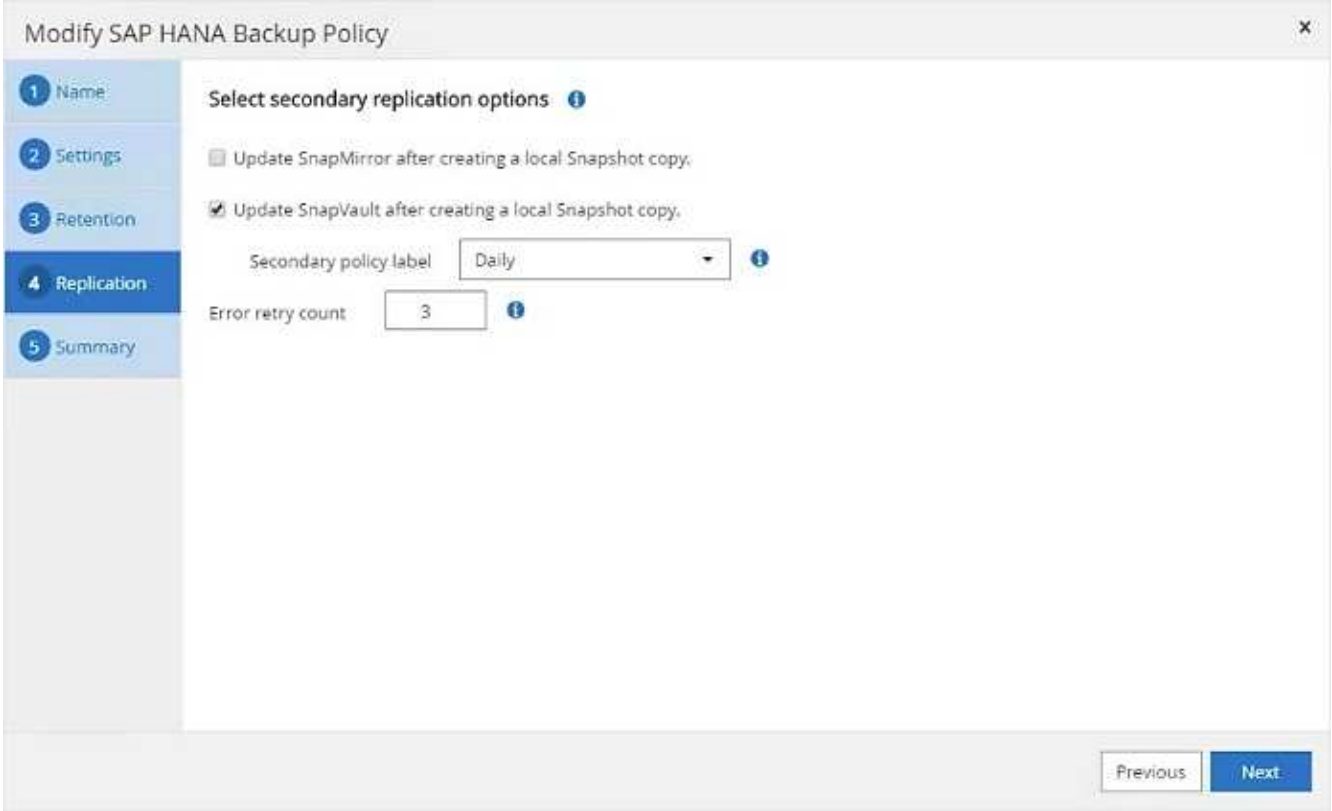


5. Configurare le impostazioni di conservazione per i backup pianificati.

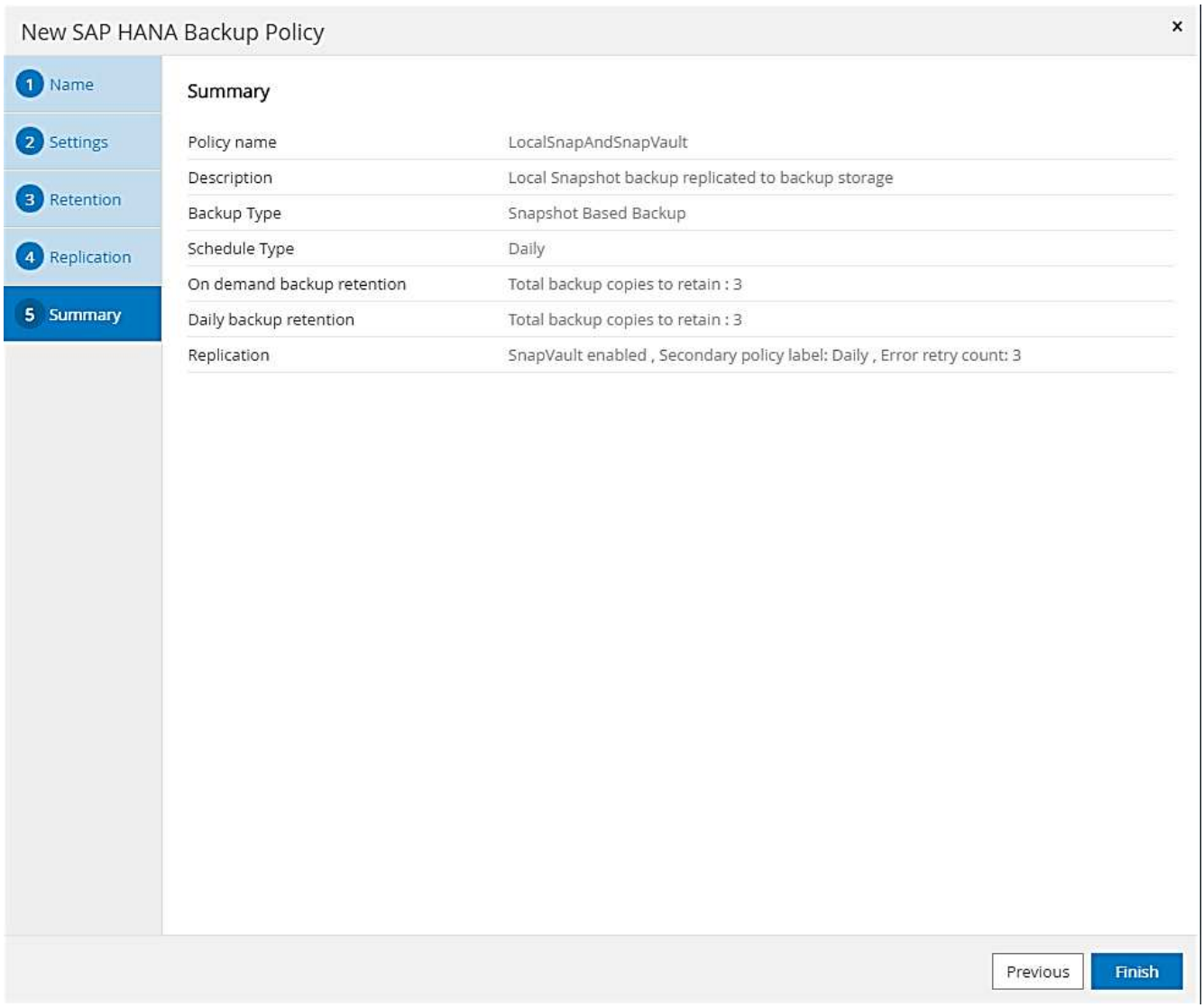


6. Selezionare Aggiorna SnapVault dopo aver creato una copia Snapshot locale.

> 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"."

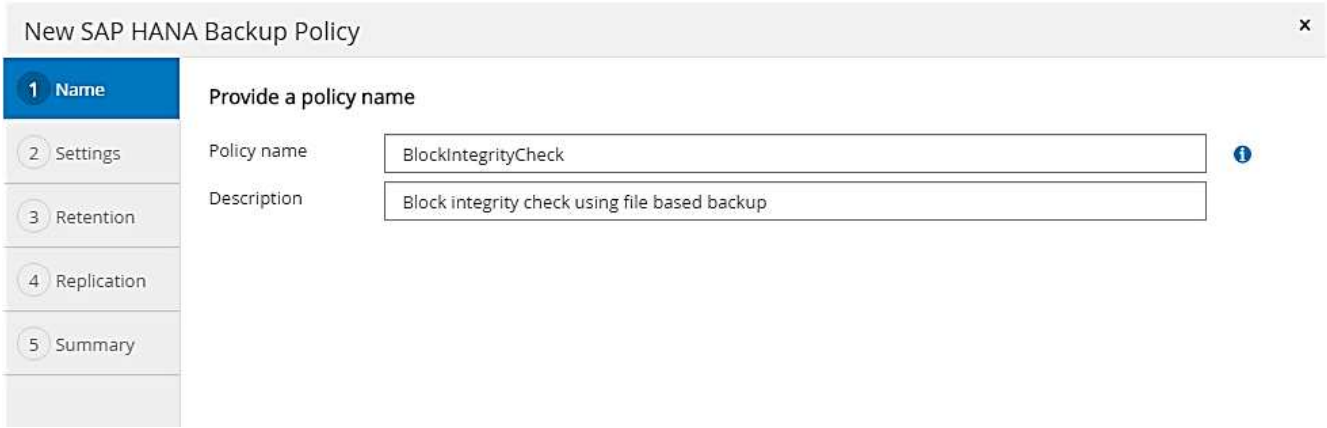


7. Nella pagina Riepilogo, fare clic su fine.

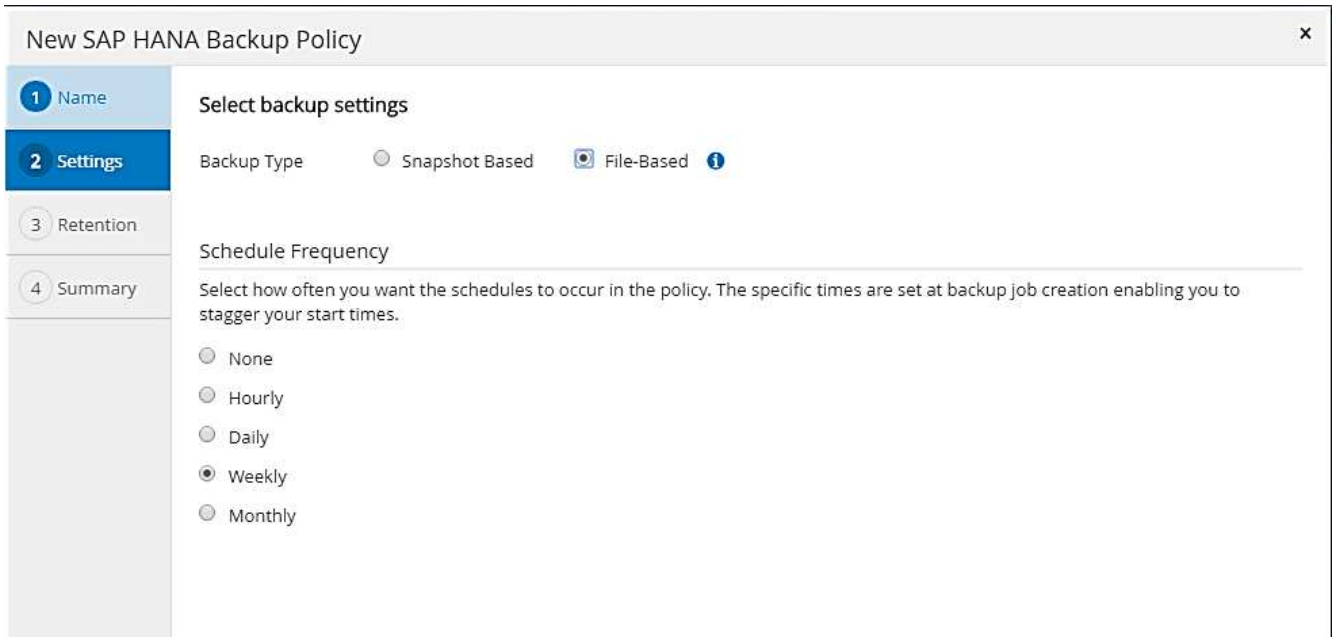


Policy per il controllo settimanale dell'integrità del blocco

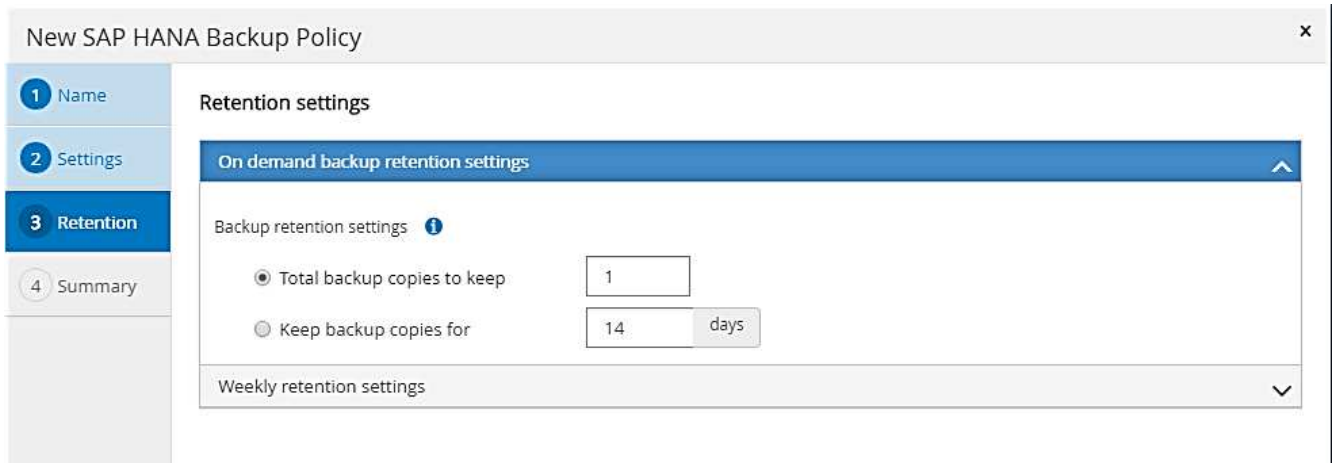
1. Accedere a Impostazioni > Criteri e fare clic su nuovo.
2. Immettere il nome e la descrizione della policy. Fare clic su Avanti.



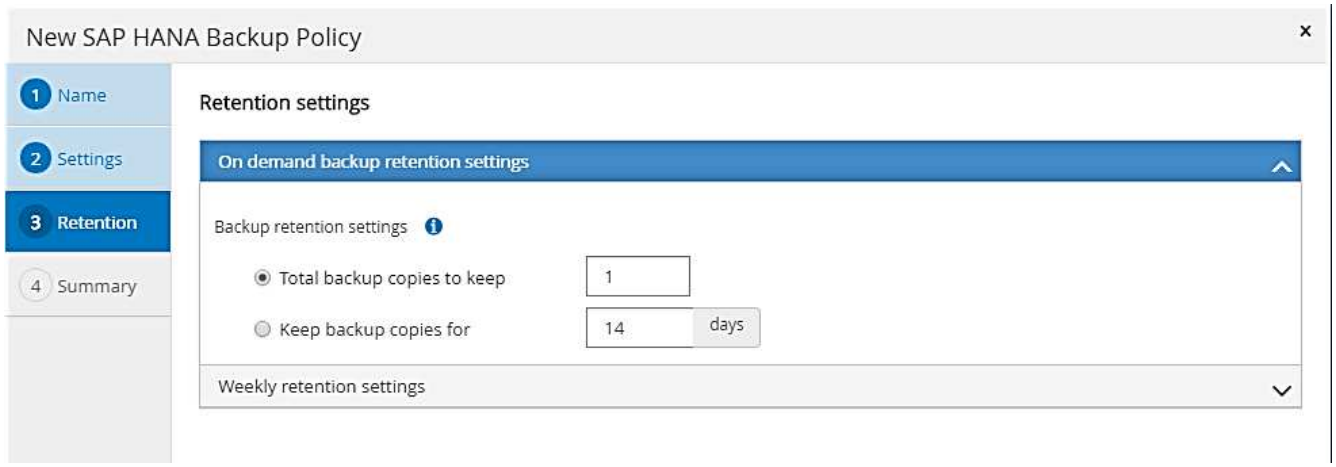
3. Impostare il tipo di backup su file-based (basato su file) e la frequenza di pianificazione su Weekly (settimanale).



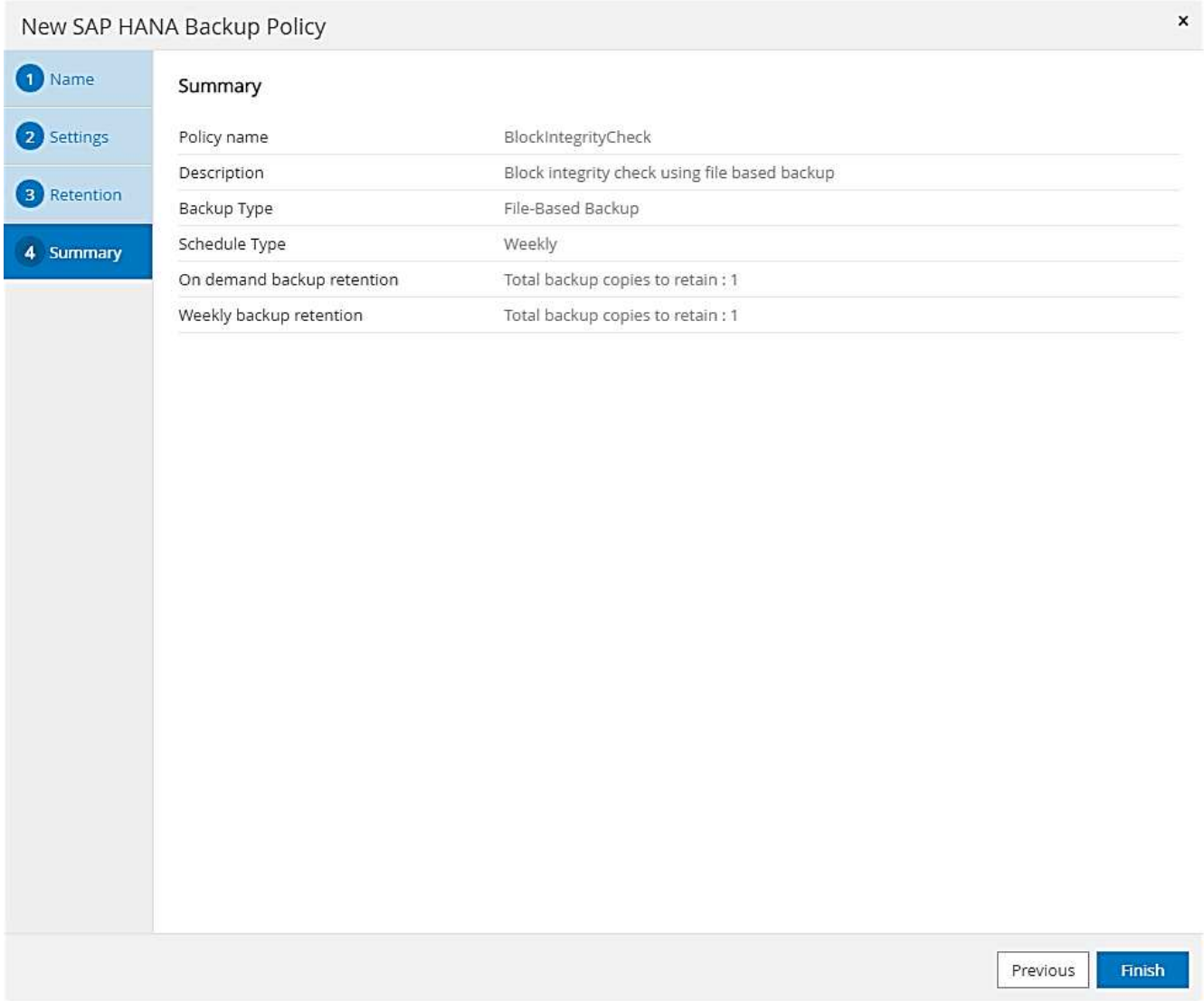
4. Configurare le impostazioni di conservazione per i backup on-demand.



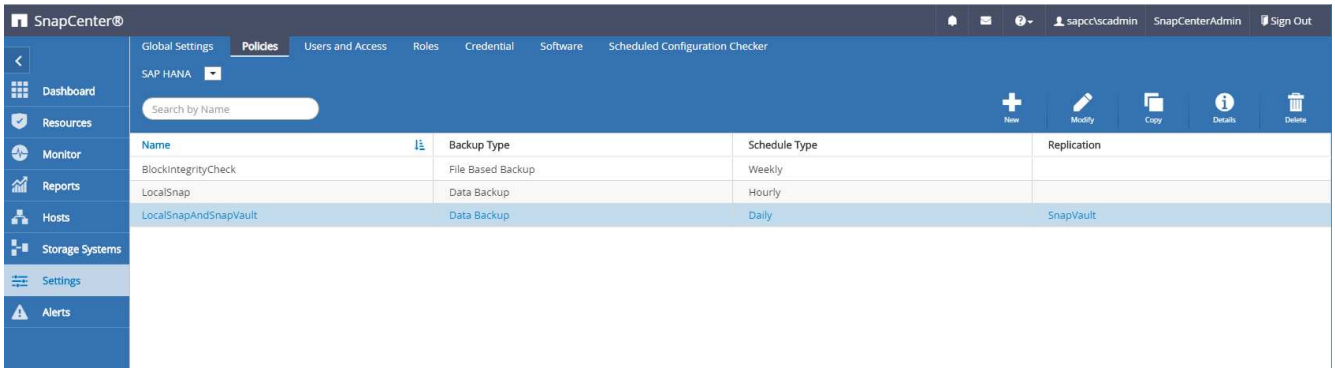
5. Configurare le impostazioni di conservazione per i backup pianificati.



6. Nella pagina Riepilogo, fare clic su fine.



La figura seguente mostra un riepilogo dei criteri configurati.



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.

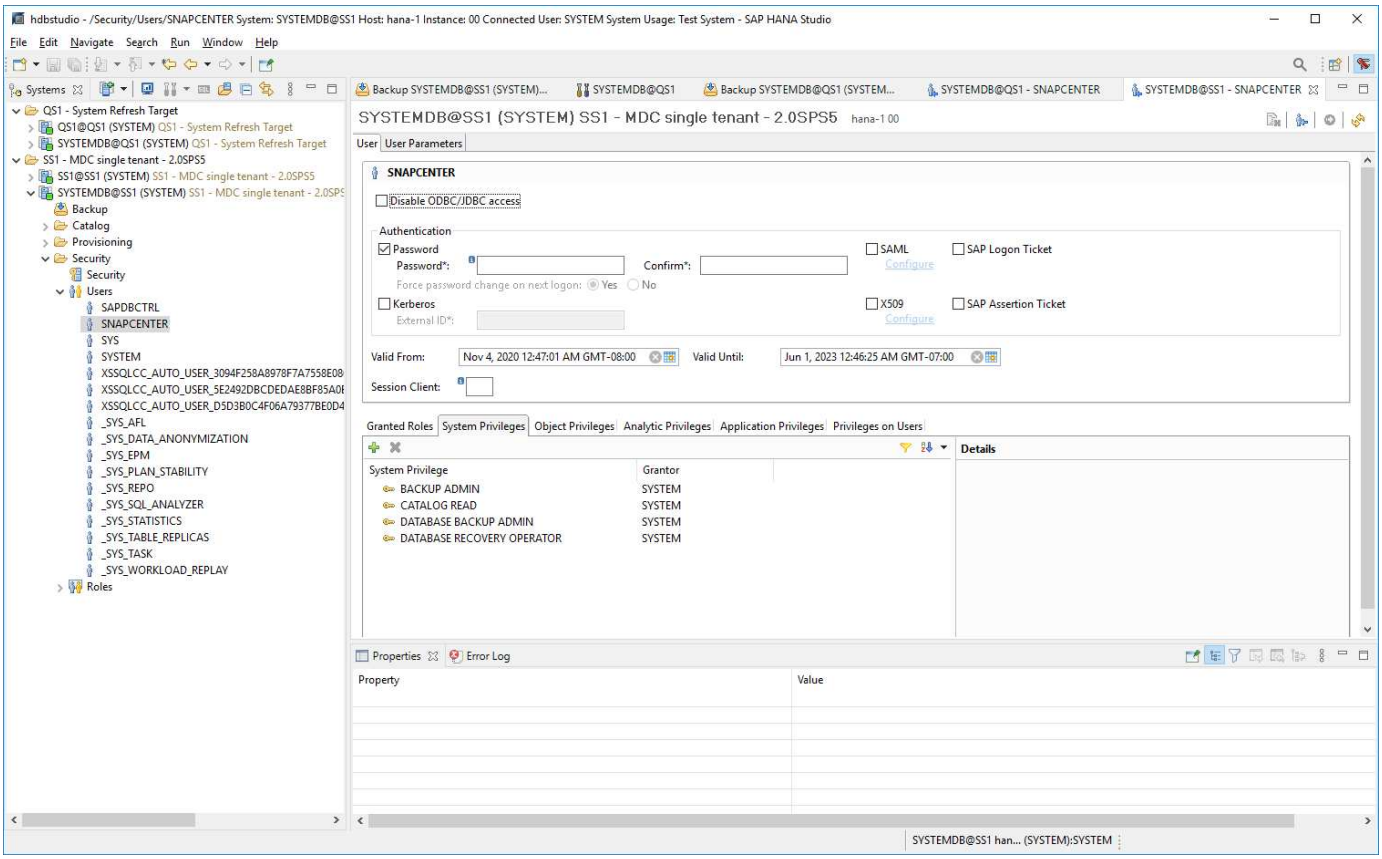
Configurazione di SAP HANA backup user e hdbuserstore

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 - ss1adm
ss1adm@hana-1:/usr/sap/SS1/HDB00>
ss1adm@hana-1:/usr/sap/SS1/HDB00>
ss1adm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore set SS1KEY hana-1:30013
SnapCenter password
ss1adm@hana-1:/usr/sap/SS1/HDB00> hdbuserstore list
DATA FILE       : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.DAT
KEY FILE        : /usr/sap/SS1/home/.hdb/hana-1/SSFS_HDB.KEY
KEY SS1KEY
  ENV : hana-1:30013
  USER: SnapCenter
KEY SS1SAPDBCTRLSS1
  ENV : hana-1:30015
  USER: SAPDBCTRL
ss1adm@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.

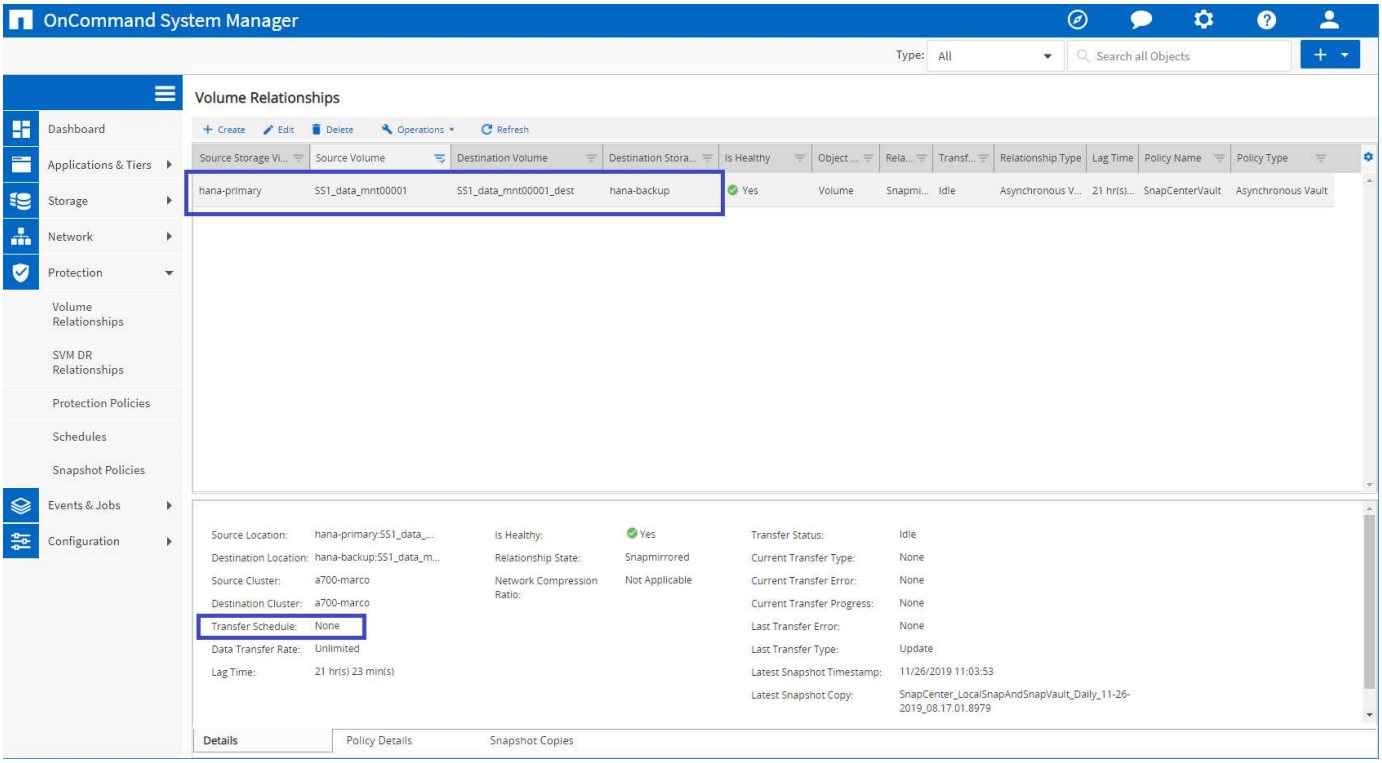
```
hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER
password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE       : 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`.

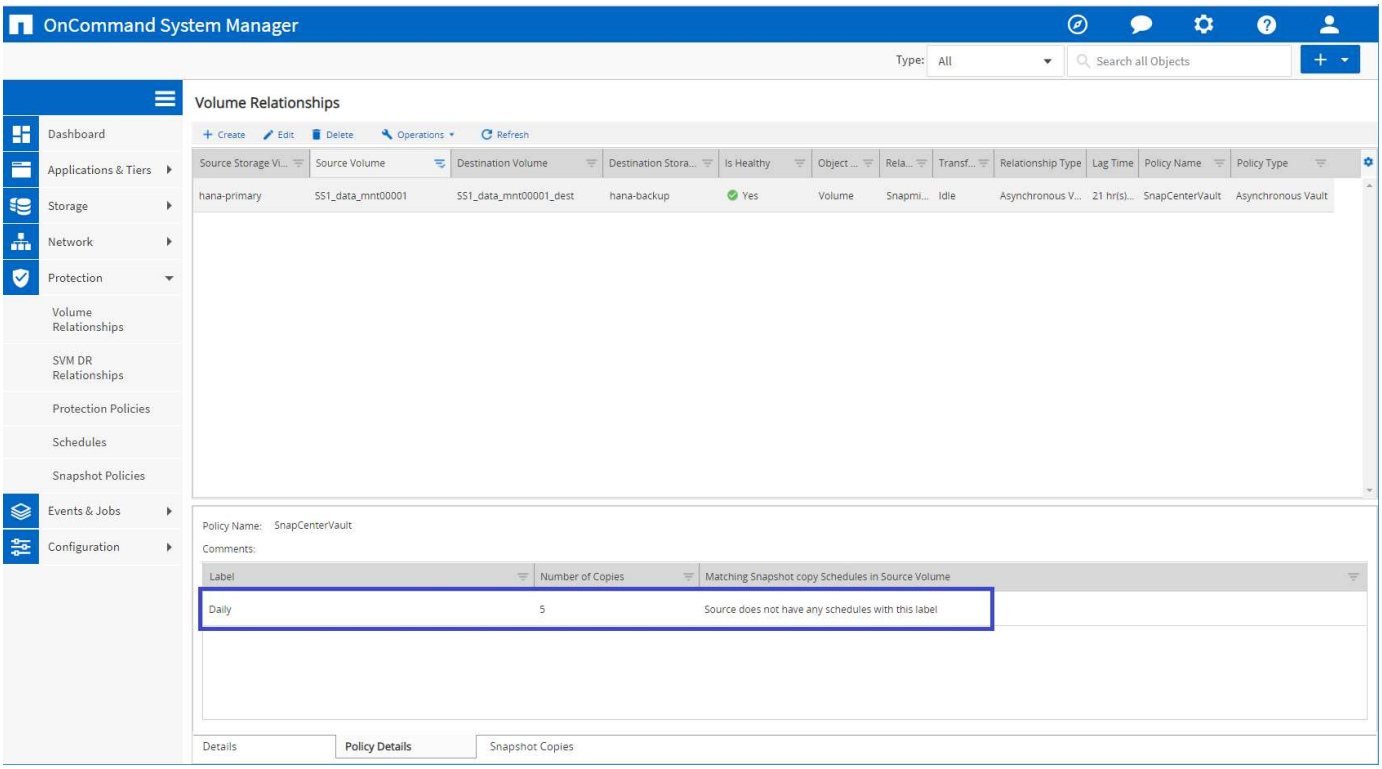
> La pianificazione della relazione deve essere impostata su Nessuno, perché SnapCenter attiva l'aggiornamento di SnapVault.



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.



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).

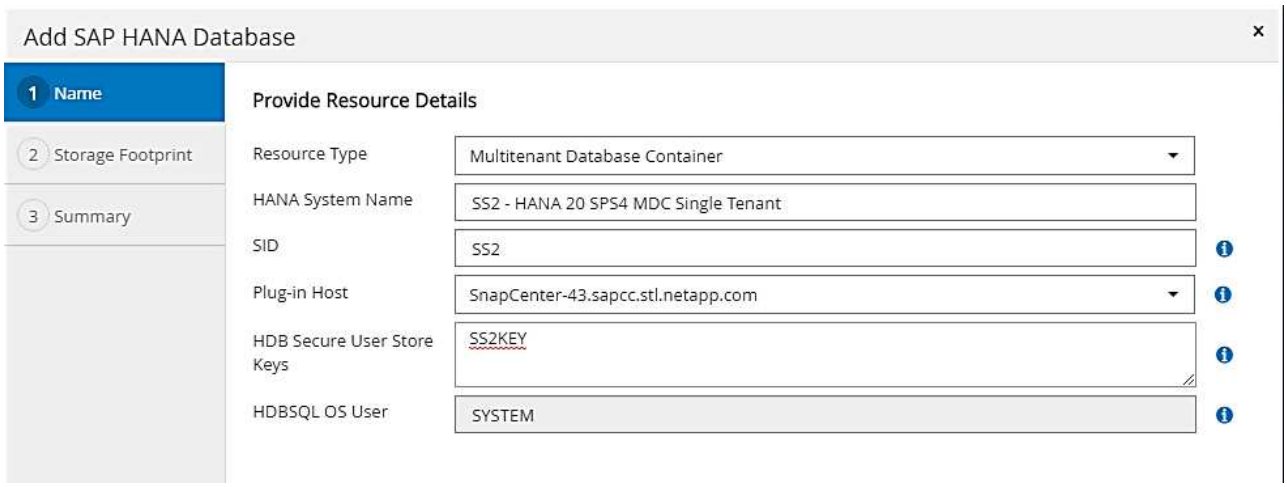
   Selezionare il tipo di risorsa nel nostro esempio, Container di database multi-tenant.

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

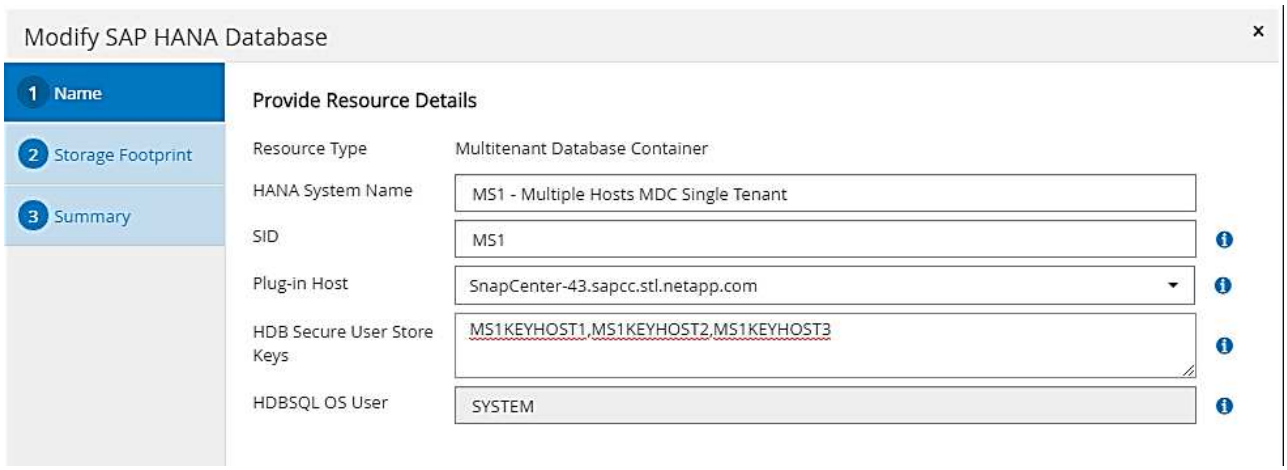
   Per il nostro sistema SAP HANA, il SID è SS2.

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

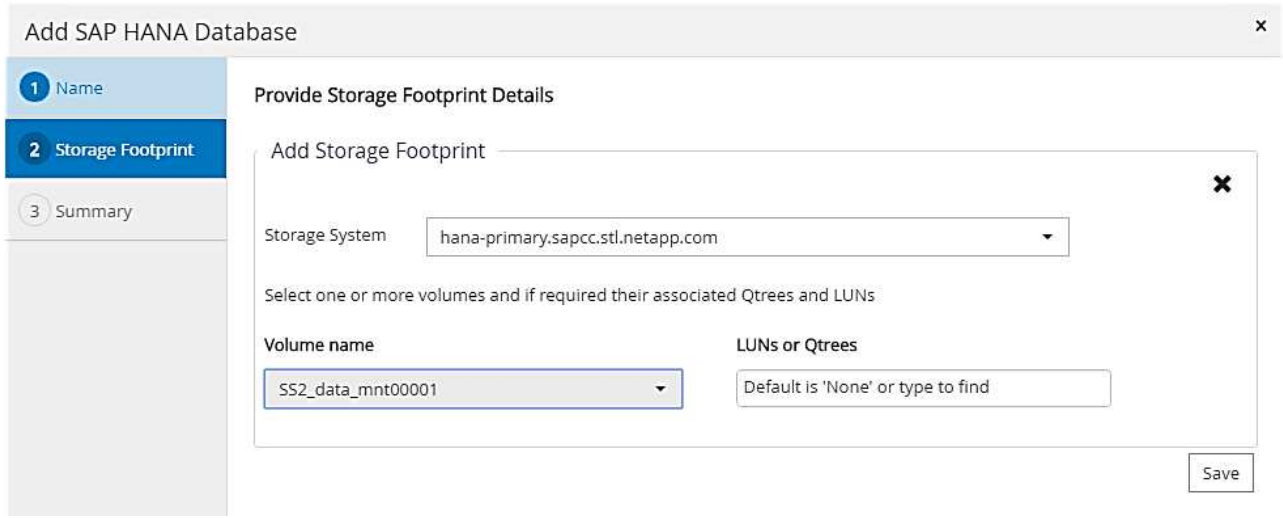
   La chiave hdbuserstore deve corrispondere alla chiave configurata per il database HANA SS2. Nel nostro esempio è SS2KEY.



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.

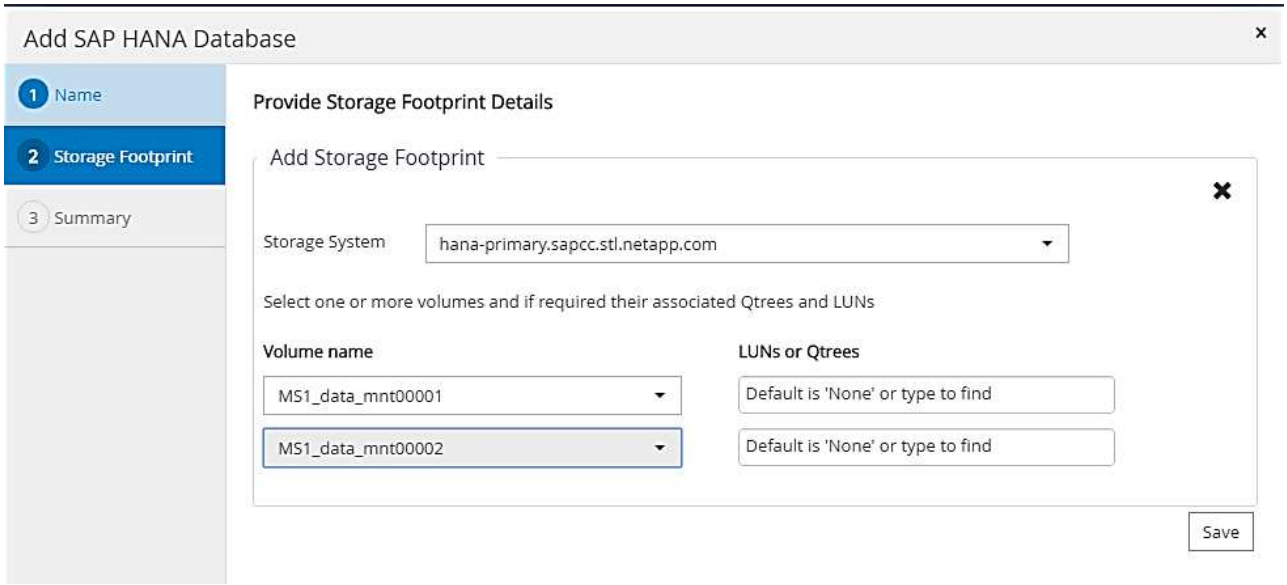


c. Selezionare i dati richiesti per il sistema di storage (SVM) e il nome del volume.



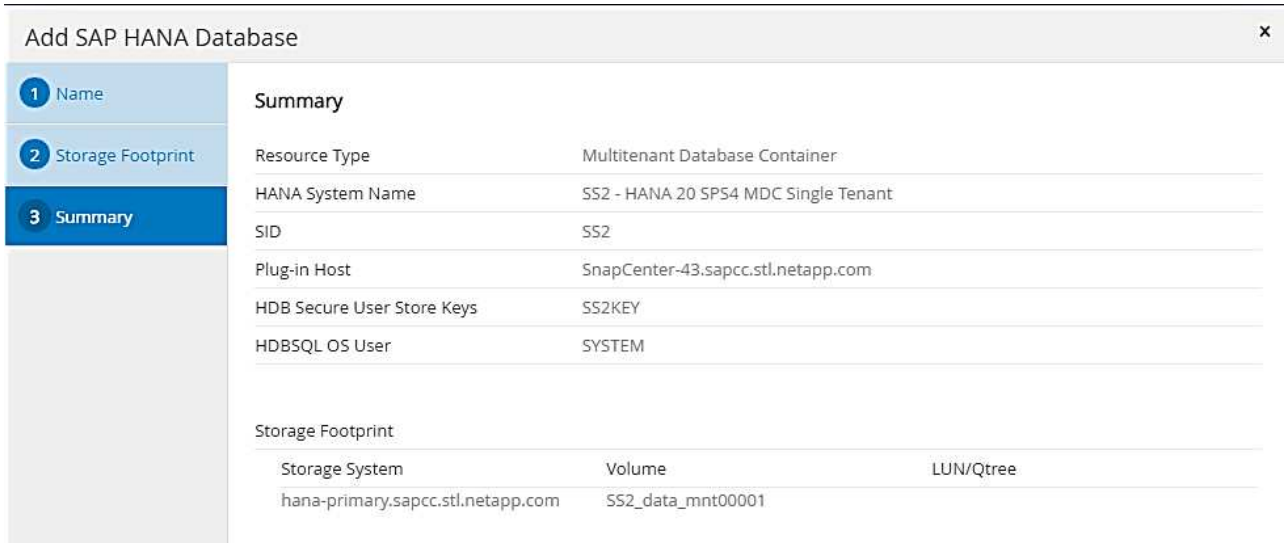
Per una configurazione SAN Fibre Channel, è necessario selezionare anche il LUN.

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



Viene visualizzata la schermata di riepilogo della configurazione delle risorse.

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



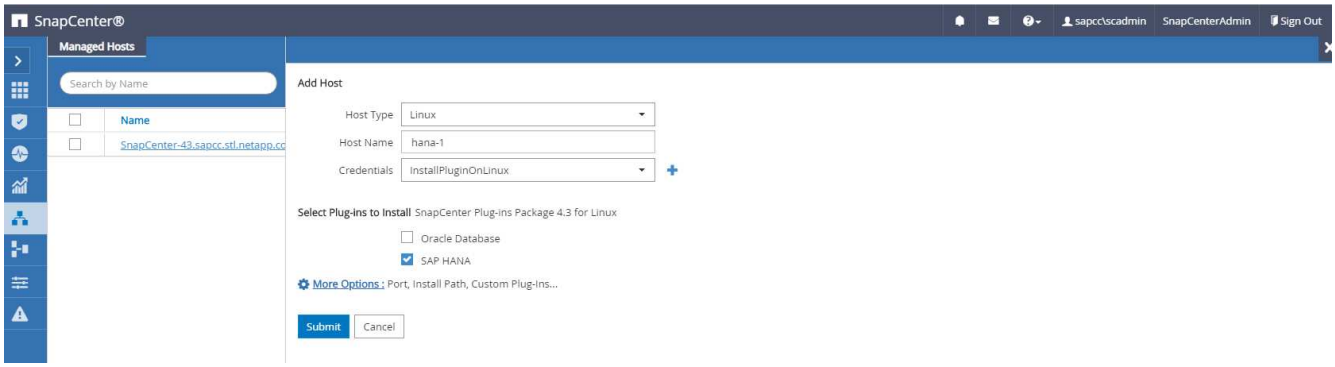
b. Al termine della configurazione delle risorse, eseguire la configurazione della protezione delle risorse come descritto nella sezione "Configurazione della protezione delle risorse."

Rilevamento automatico dei database HANA

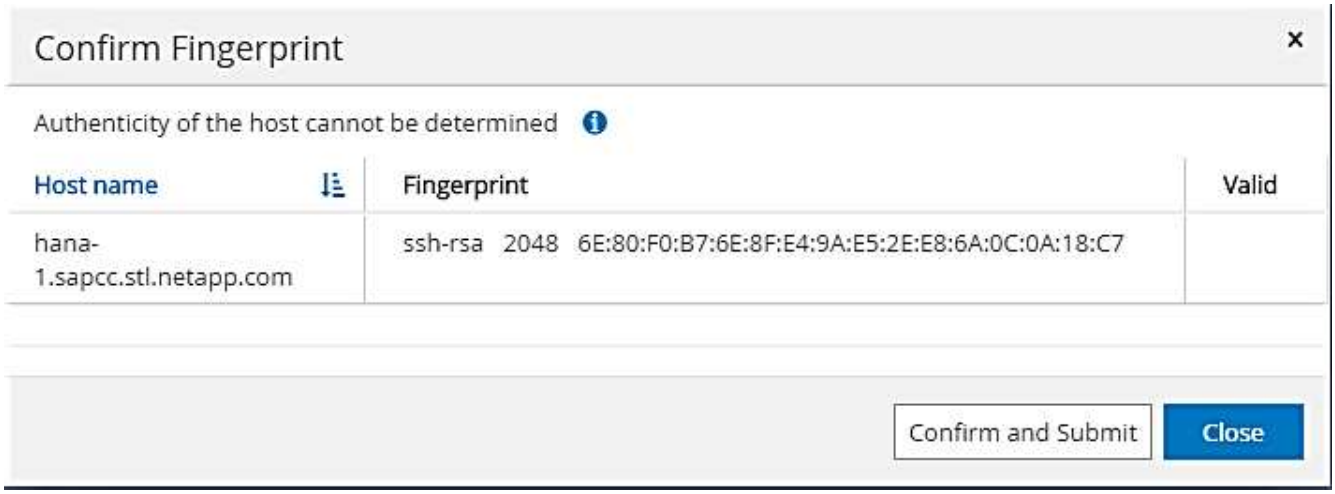
Questa sezione descrive il rilevamento automatico della risorsa SAP HANA SS1 (sistema single-tenant MDC host con NFS). Tutti i passaggi descritti sono identici per un singolo container HANA, per i sistemi di tenant multipli HANA MDC e per un sistema HANA che utilizza SAN Fibre Channel.

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.

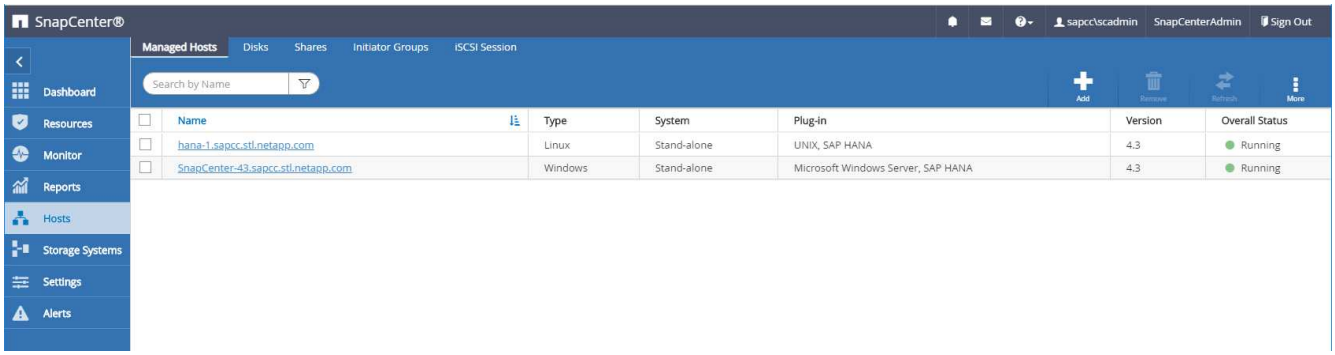
1. Dalla scheda host, fare clic su Add (Aggiungi).
2. Fornire informazioni sull'host e selezionare il plug-in SAP HANA da installare. Fare clic su Invia.



3. Confermare l'impronta digitale.



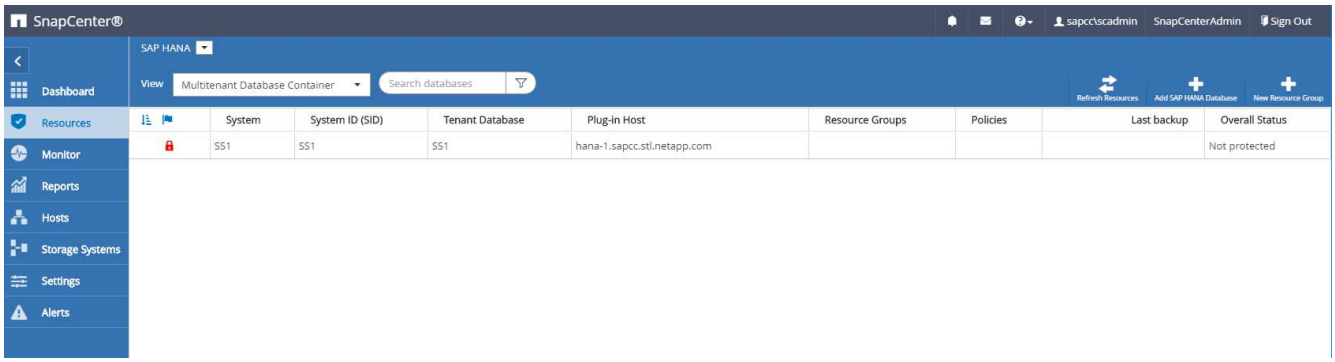
L'installazione del plug-in HANA e del plug-in Linux si avvia automaticamente. Al termine dell'installazione, la colonna di stato dell'host mostra in esecuzione. La schermata mostra inoltre che il plug-in Linux è installato insieme al plug-in HANA.



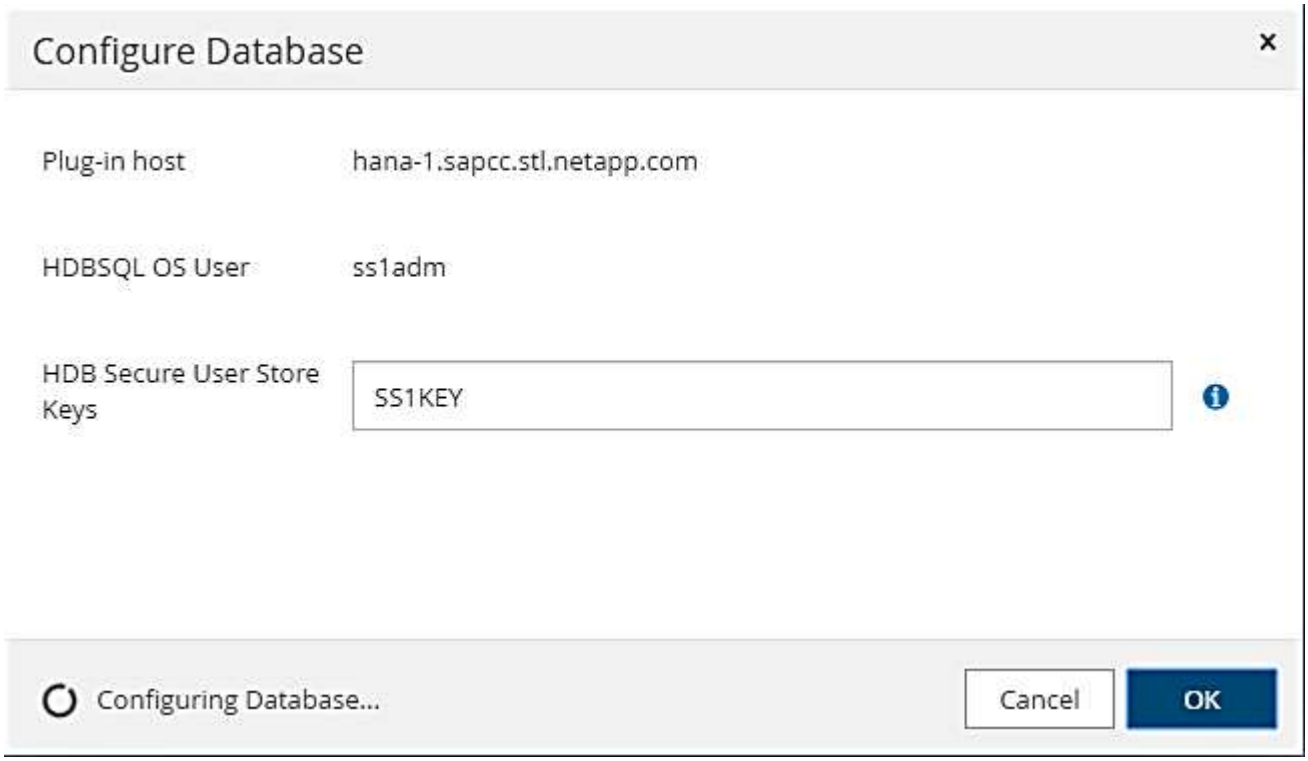
Dopo l'installazione del plug-in, il processo di rilevamento automatico della risorsa HANA viene avviato automaticamente. Nella schermata Resources (risorse) viene creata una nuova risorsa, contrassegnata come bloccata con l'icona del lucchetto rosso.

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.

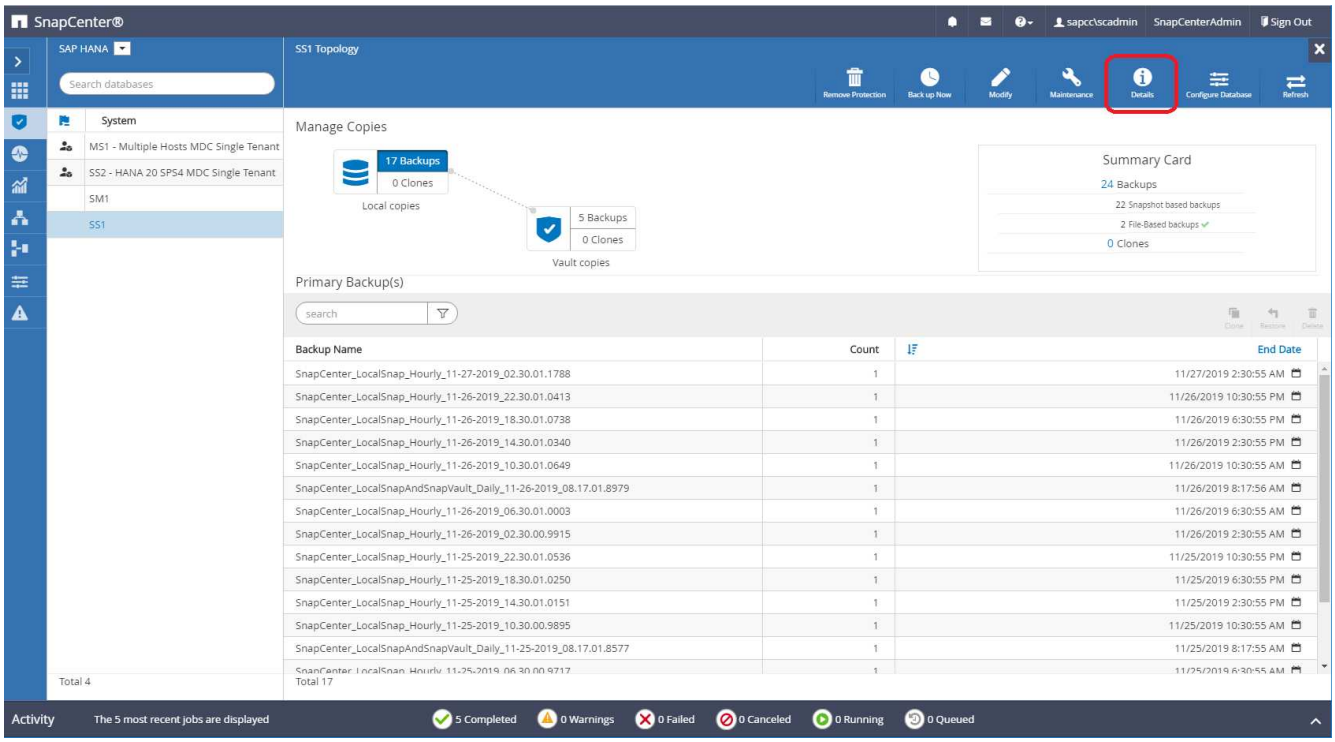


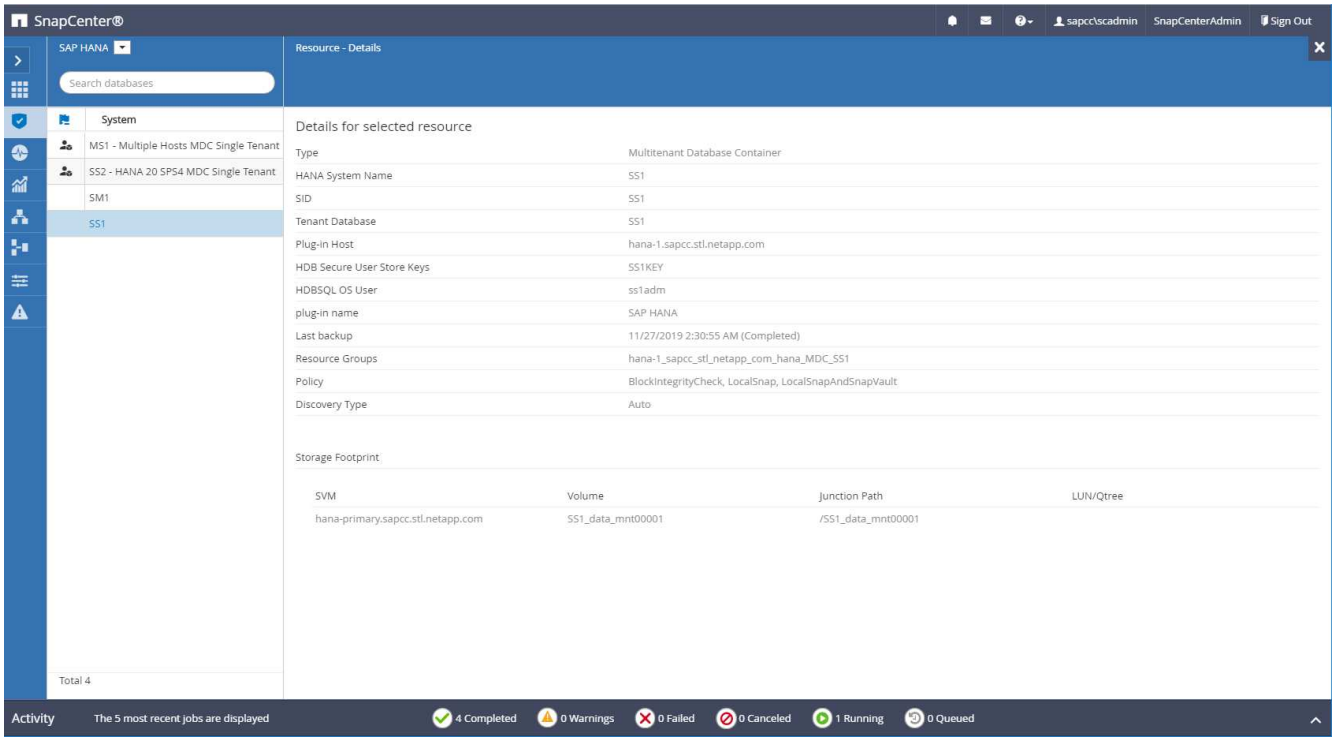
5. Fornire la chiave dell'archivio utenti per il database HANA.



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.





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.

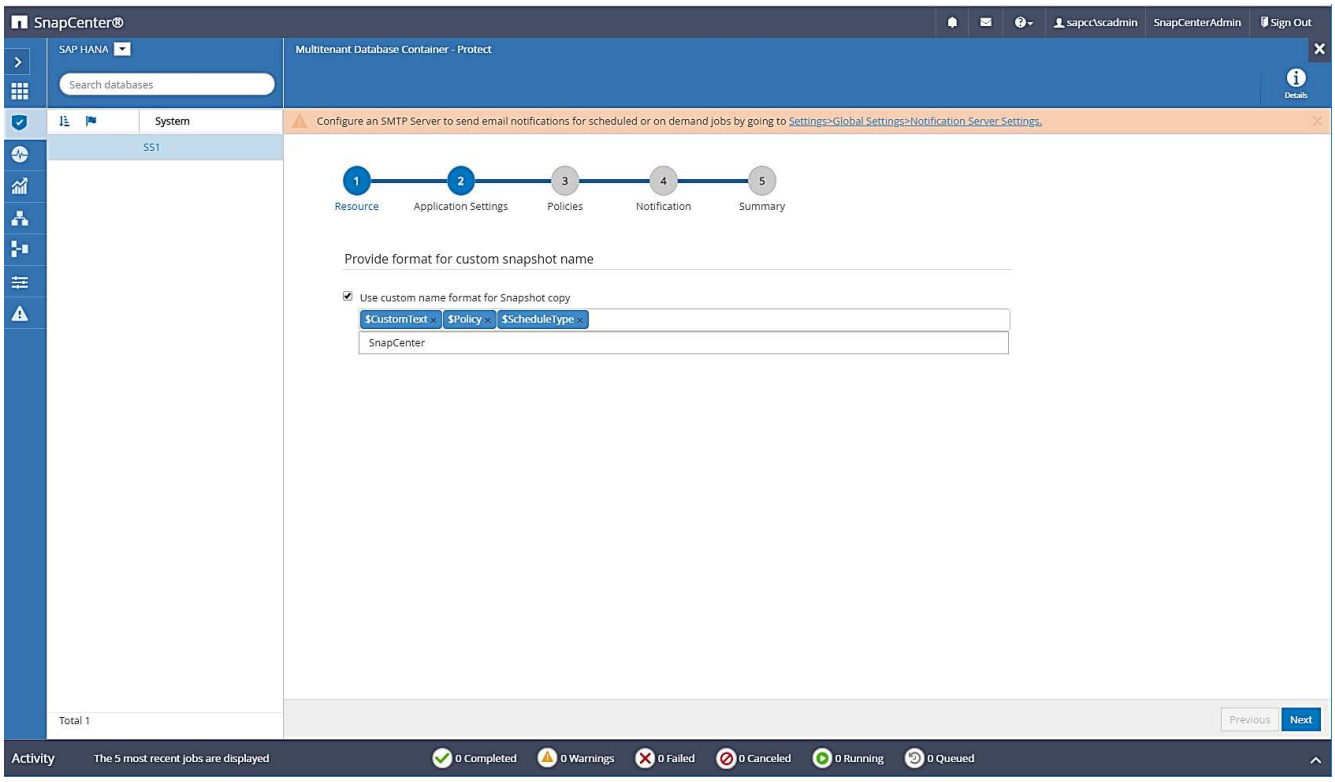
1. Dalla scheda risorse, fare doppio clic sulla risorsa.
2. Configurare un formato nome personalizzato per la copia Snapshot.

> 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`.

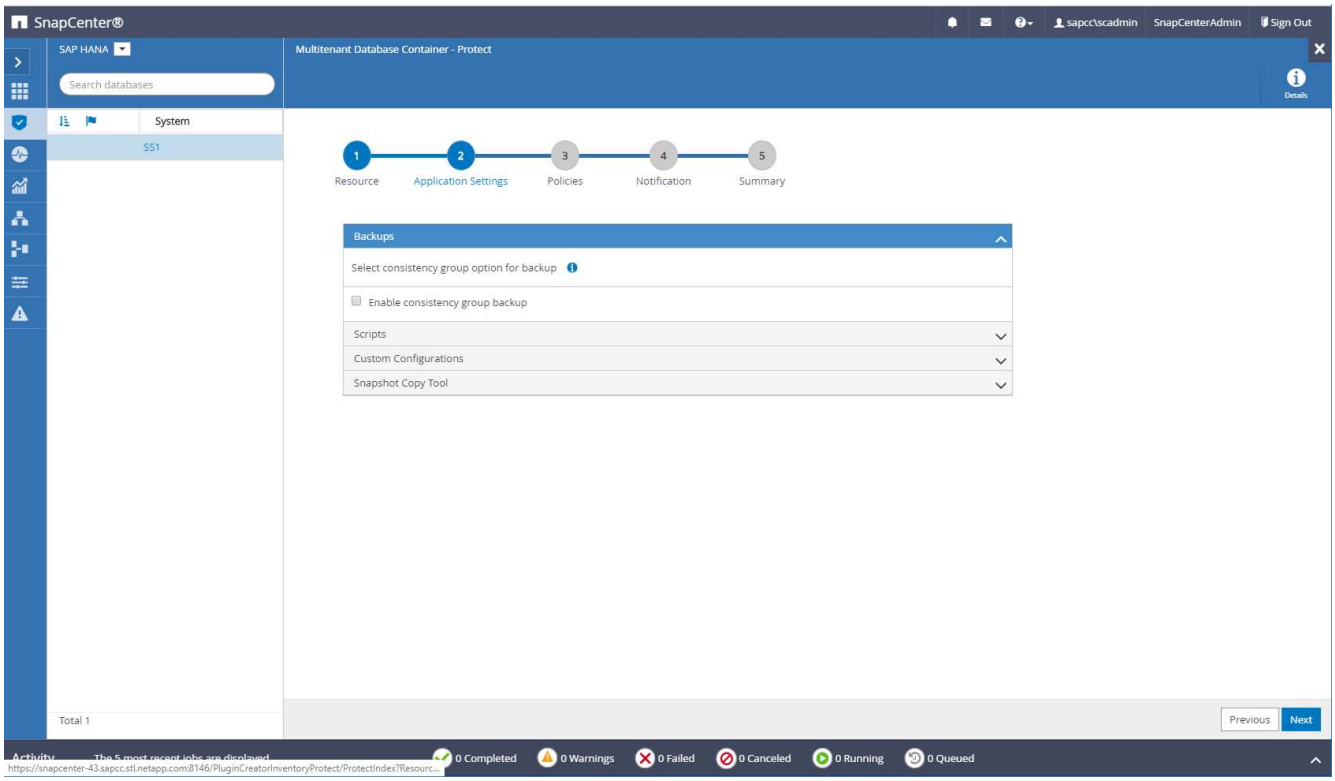
Nella configurazione illustrata nella figura seguente, i nomi delle copie Snapshot e di backup hanno il seguente formato:

- 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>`

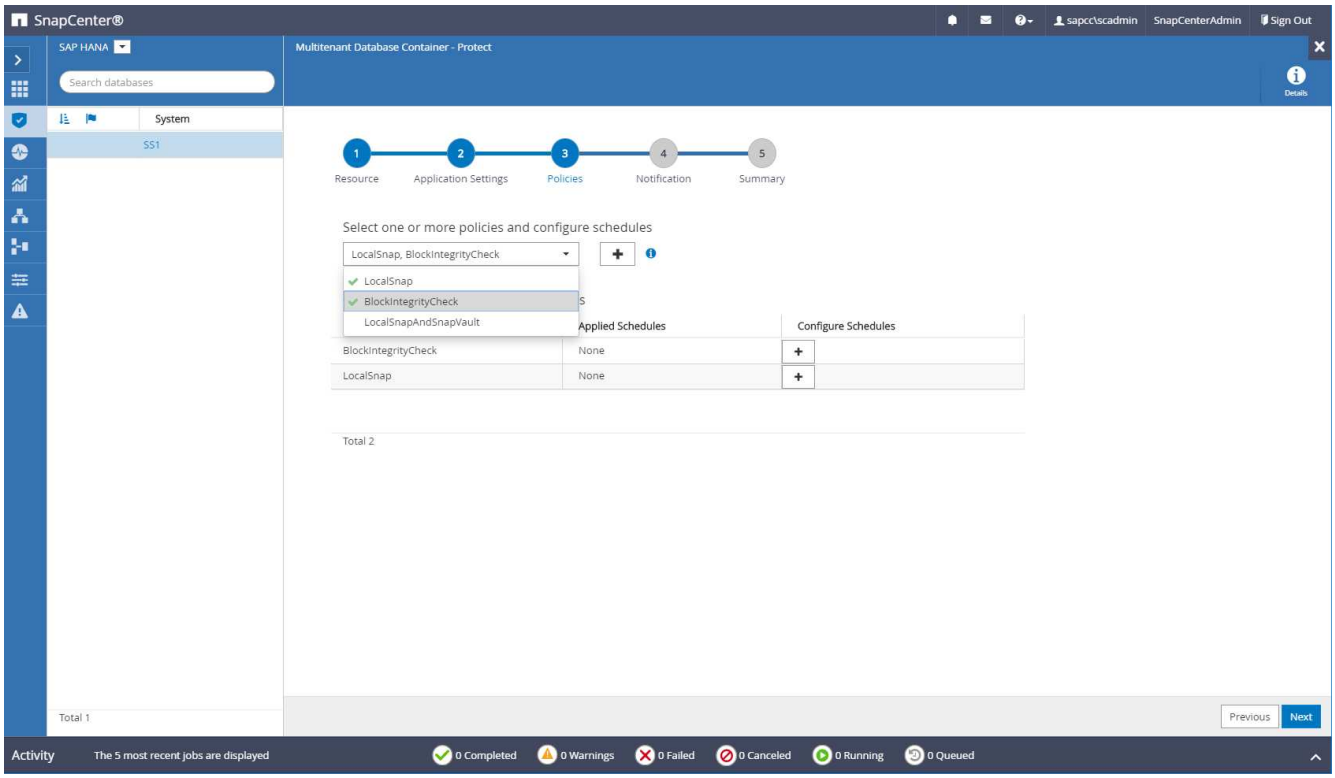
> Anche se viene definita una conservazione per i backup on-demand nella configurazione dei criteri, la pulizia viene eseguita solo quando viene eseguito un altro backup on-demand. Di conseguenza, i backup on-demand devono in genere essere cancellati manualmente in SnapCenter per assicurarsi che questi 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.



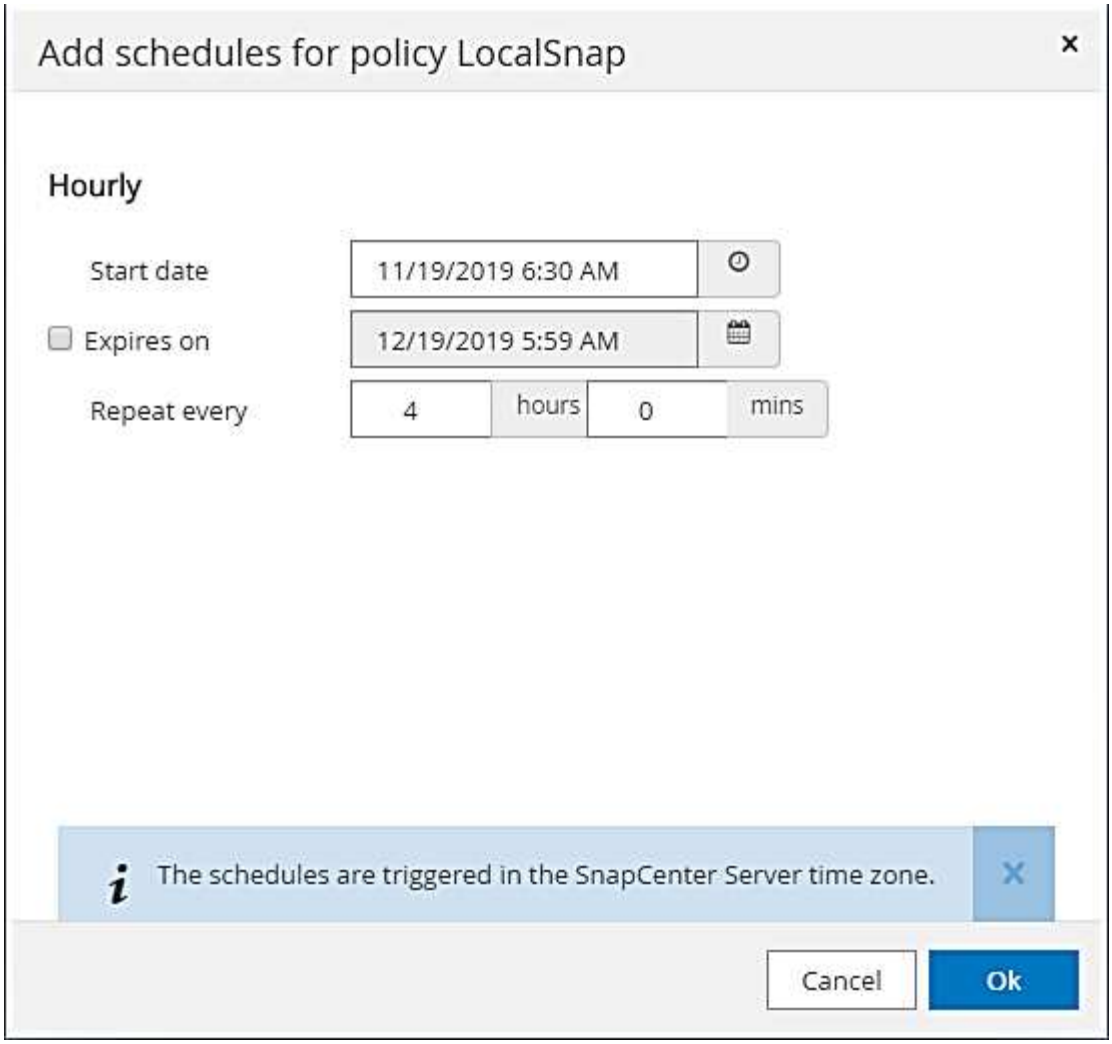
3. Non è necessario impostare impostazioni specifiche nella pagina Impostazioni applicazione. Fare clic su Avanti.



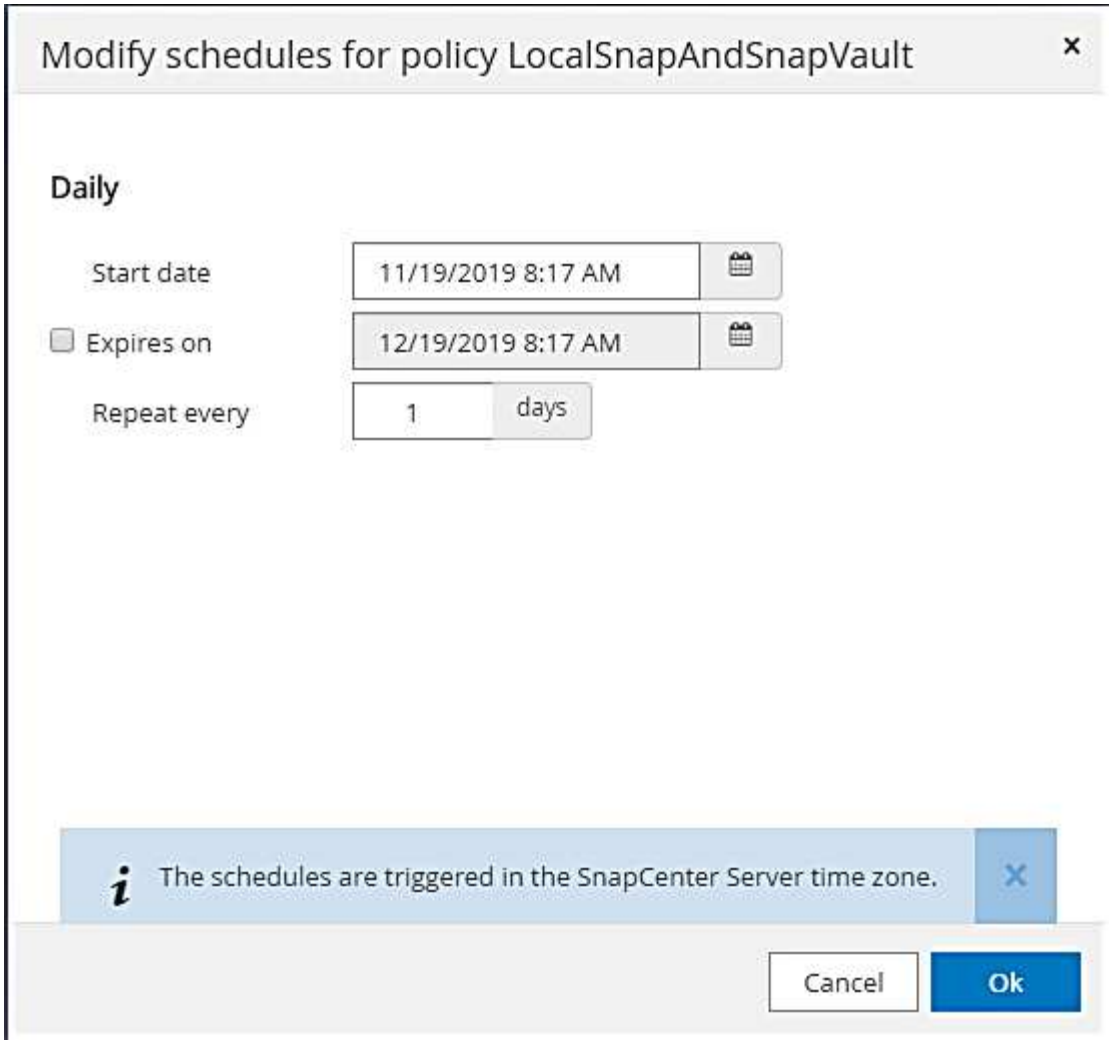
4. Selezionare i criteri da aggiungere alla risorsa.



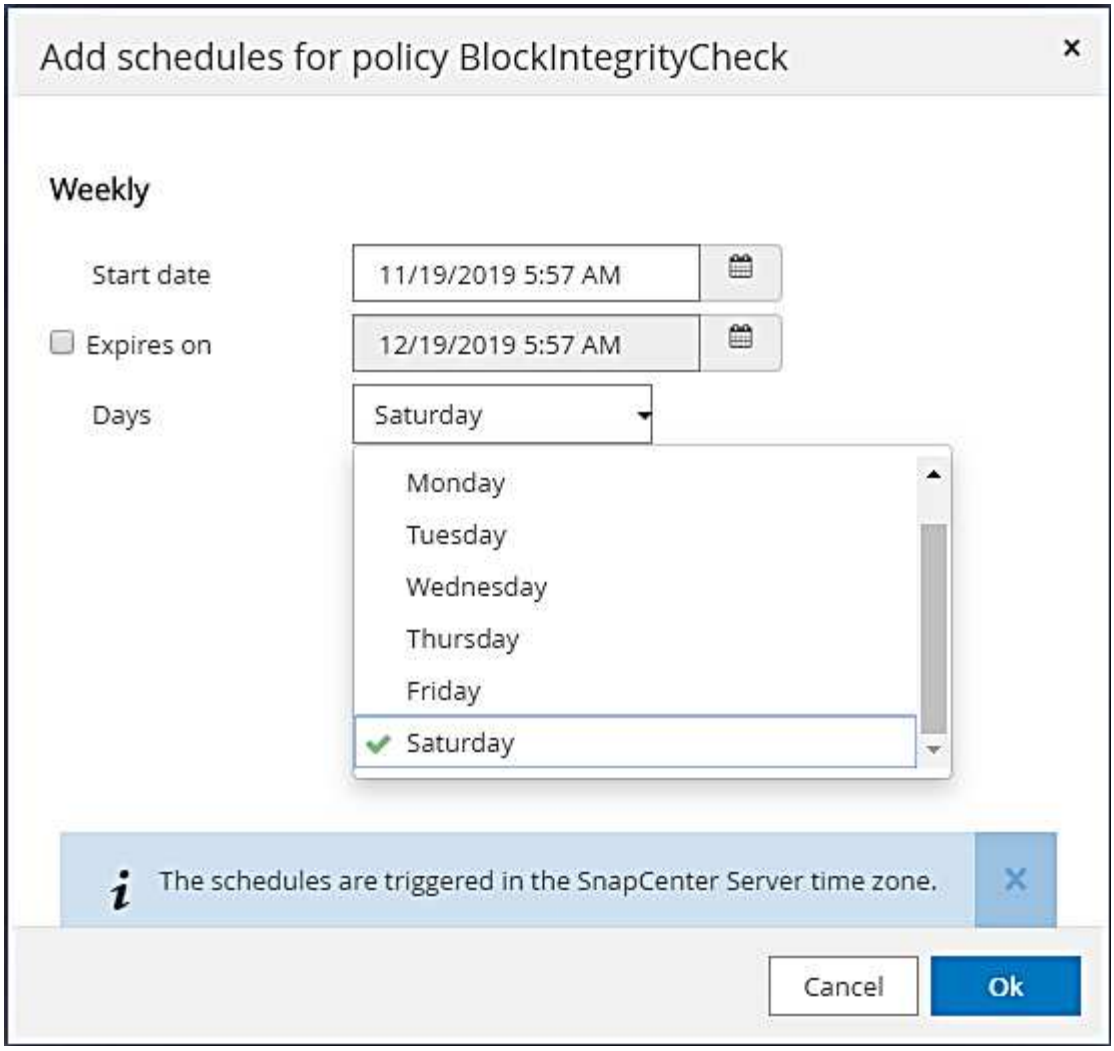
5. Definire la pianificazione per il criterio LocalSnap (in questo esempio, ogni quattro ore).



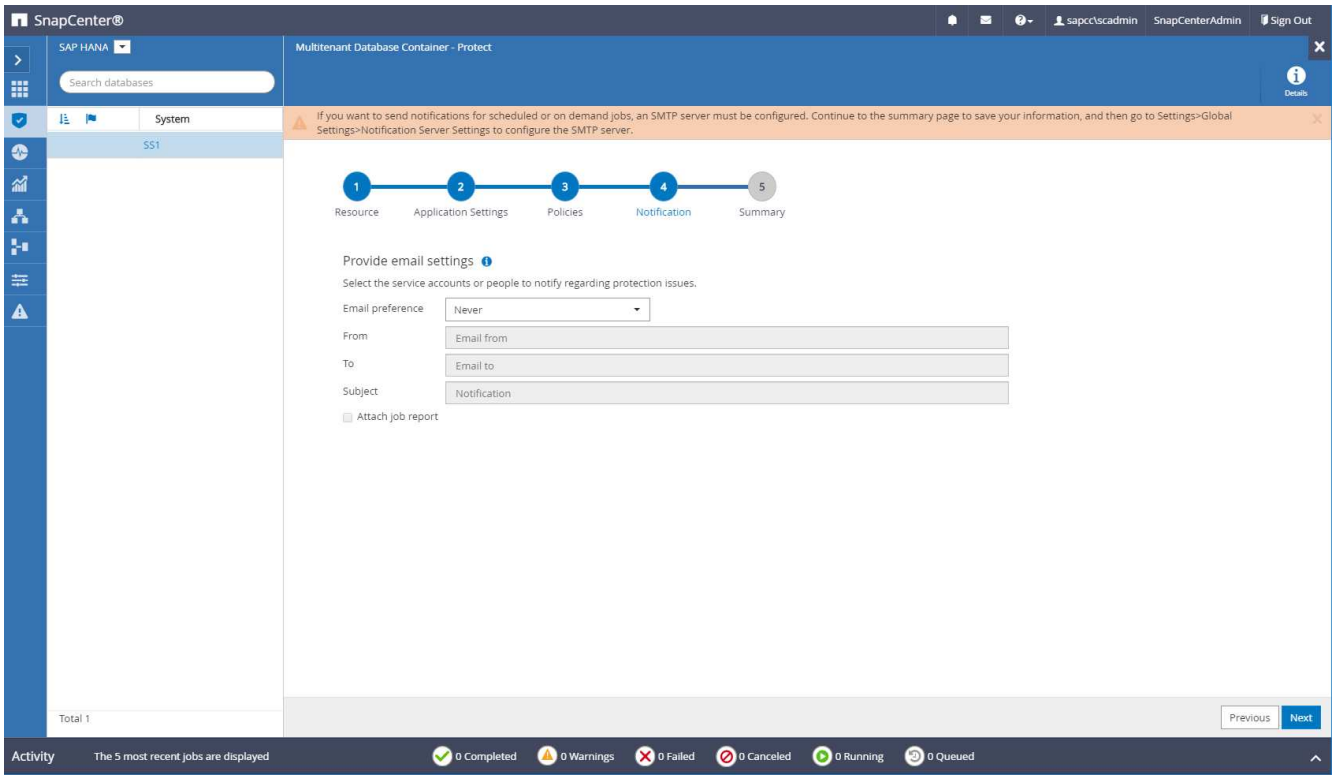
6. Definire la pianificazione per la policy LocalSnapAndSnapVault (in questo esempio, una volta al giorno).



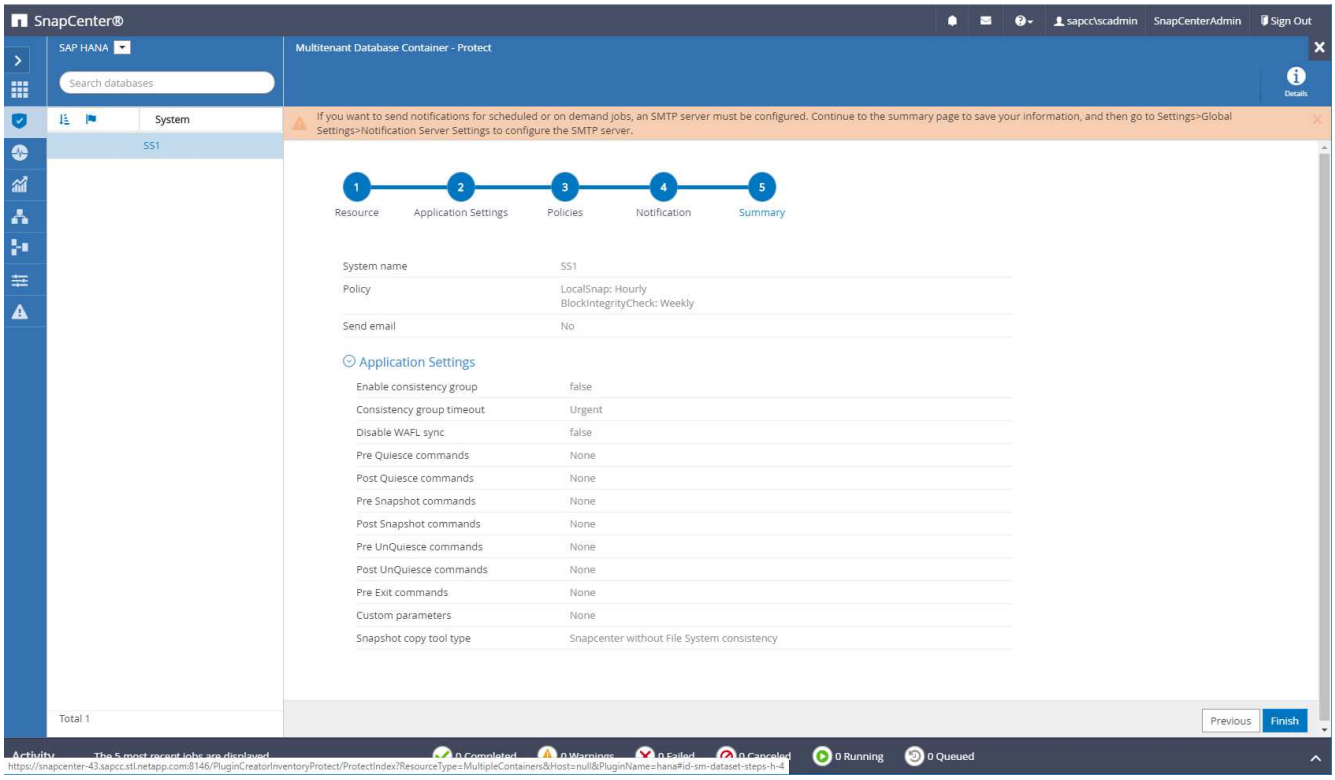
7. Definire la pianificazione per la policy di controllo dell'integrità del blocco (in questo esempio, una volta alla settimana).



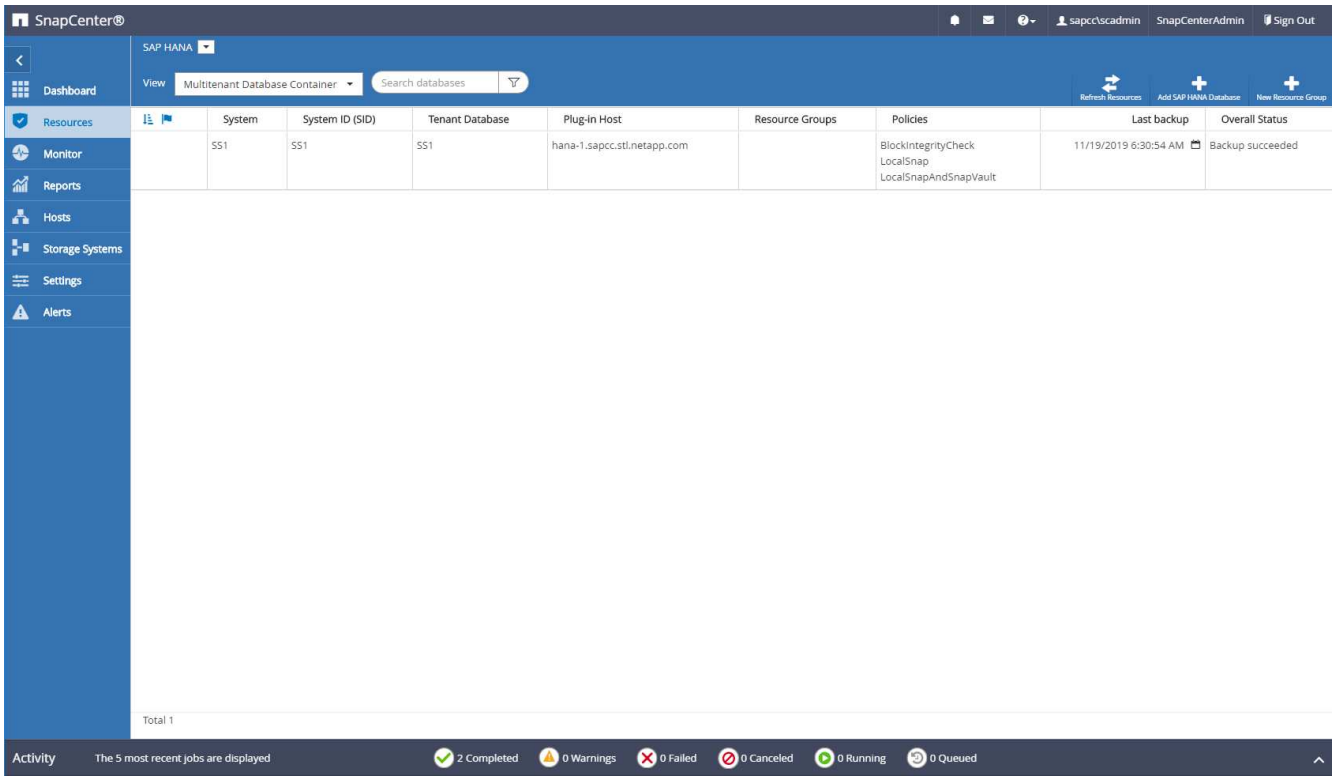
8. Fornire informazioni sulla notifica via email.



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.



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.

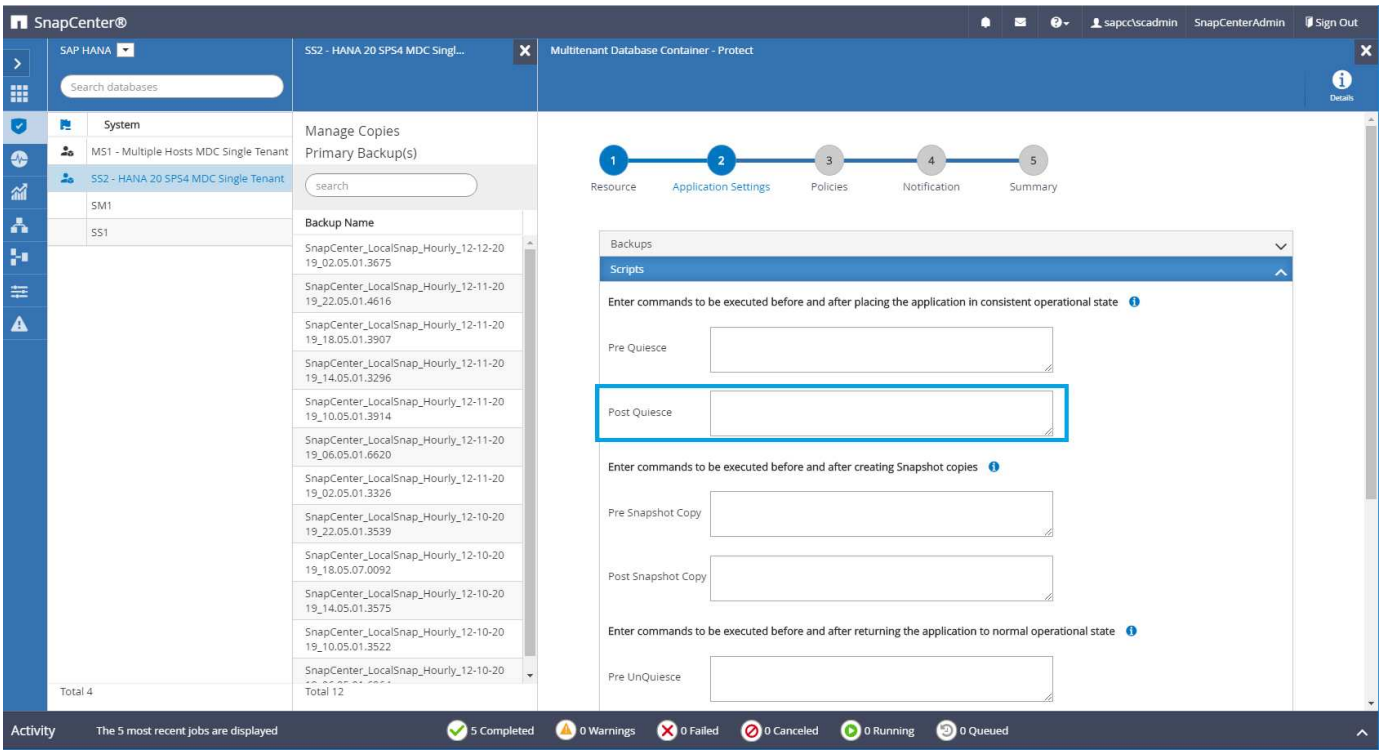
Se il server SnapCenter viene utilizzato come host plug-in HANA centrale, è possibile utilizzare un file batch. Il file batch deve avere il seguente contenuto:

```
@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.

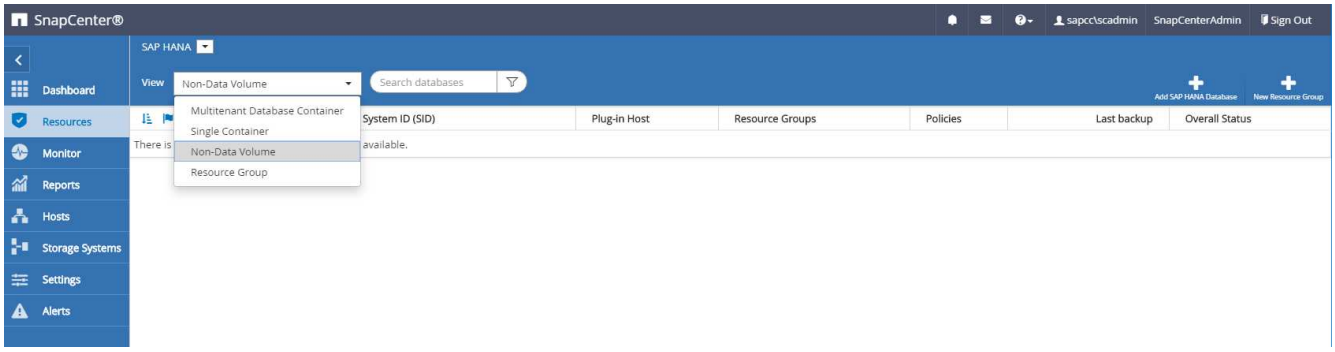
Per eseguire il ripristino da situazioni in cui devono essere ripristinati altri file non di dati, NetApp consiglia di sviluppare una strategia di backup aggiuntiva per i volumi non di dati per aumentare il backup del database SAP HANA. A seconda dei requisiti specifici, il backup dei volumi non dati 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.

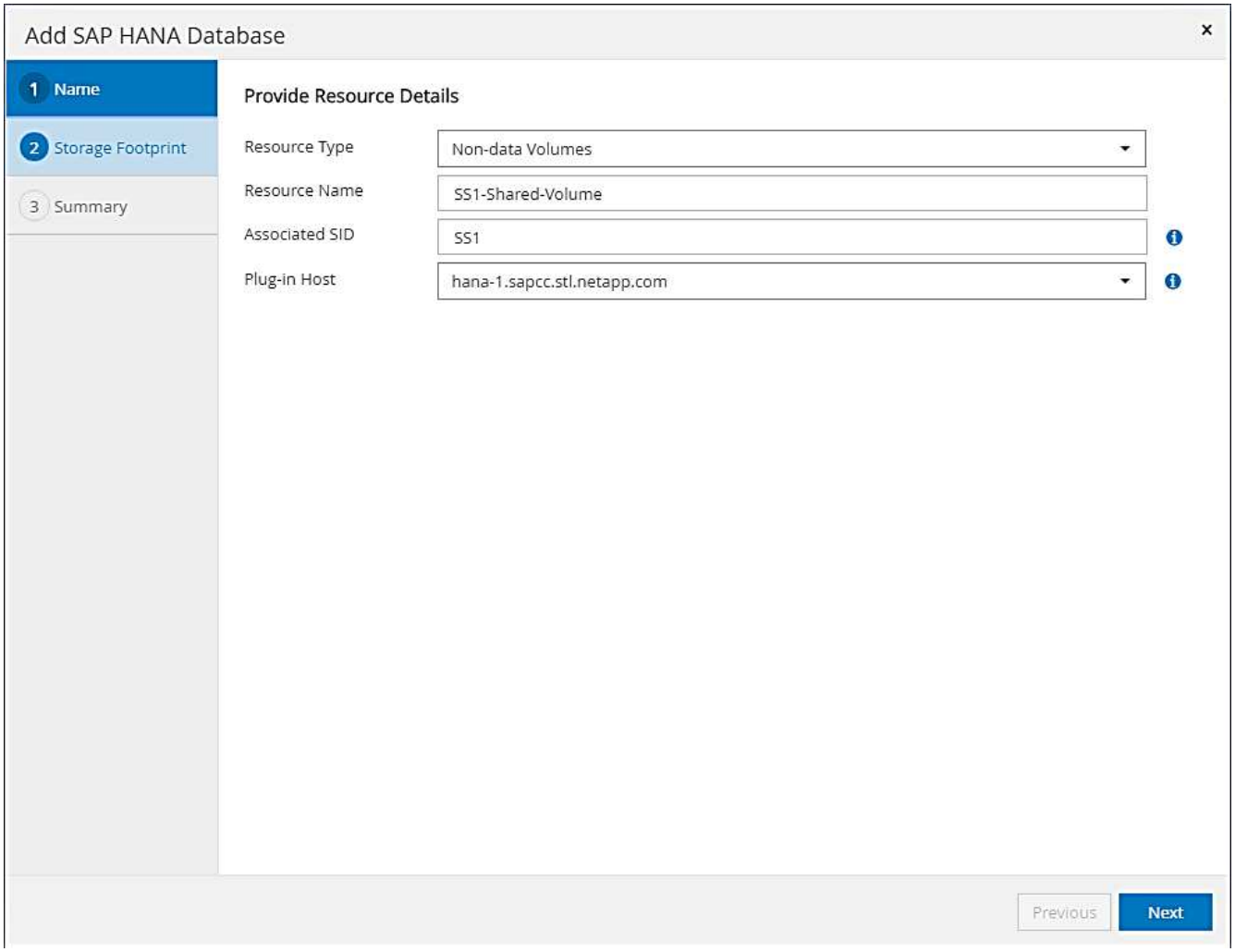
Configurazione di risorse non di volumi di dati

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

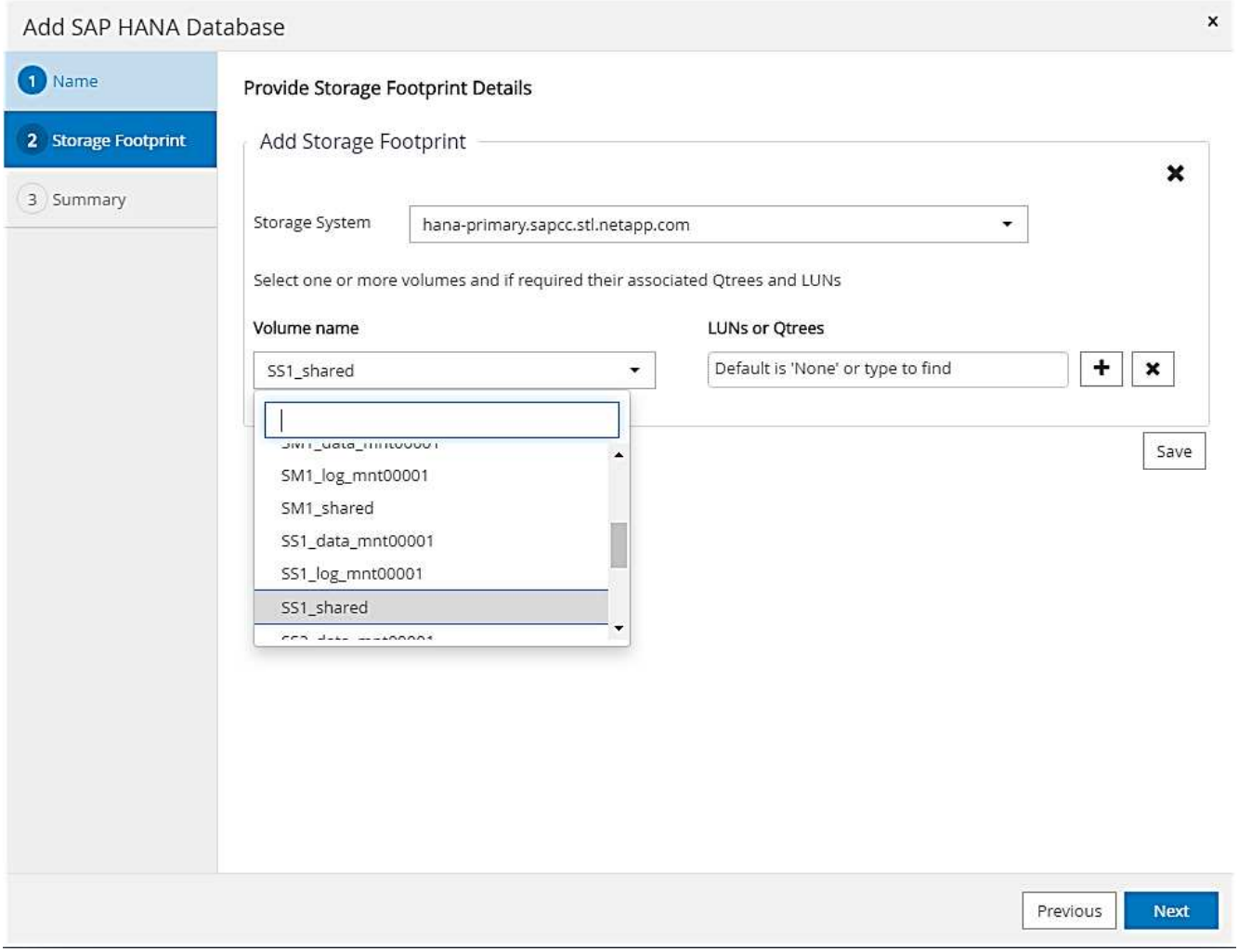
1. Dalla scheda Resource, selezionare non-Data-Volume e fare clic su Add SAP HANA Database (Aggiungi database SAP HANA).



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.



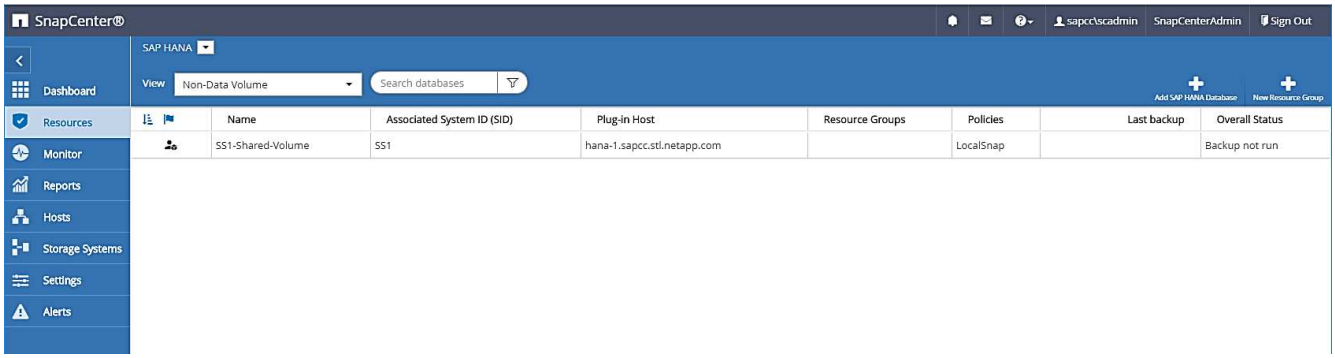
3. Aggiungere la SVM e il volume di storage come footprint dello storage, quindi fare clic su Next (Avanti).



4. Nella fase di riepilogo, fare clic su fine per salvare le impostazioni.
5. Ripetere questi passaggi per tutti i volumi non dati richiesti.
6. 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.



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.

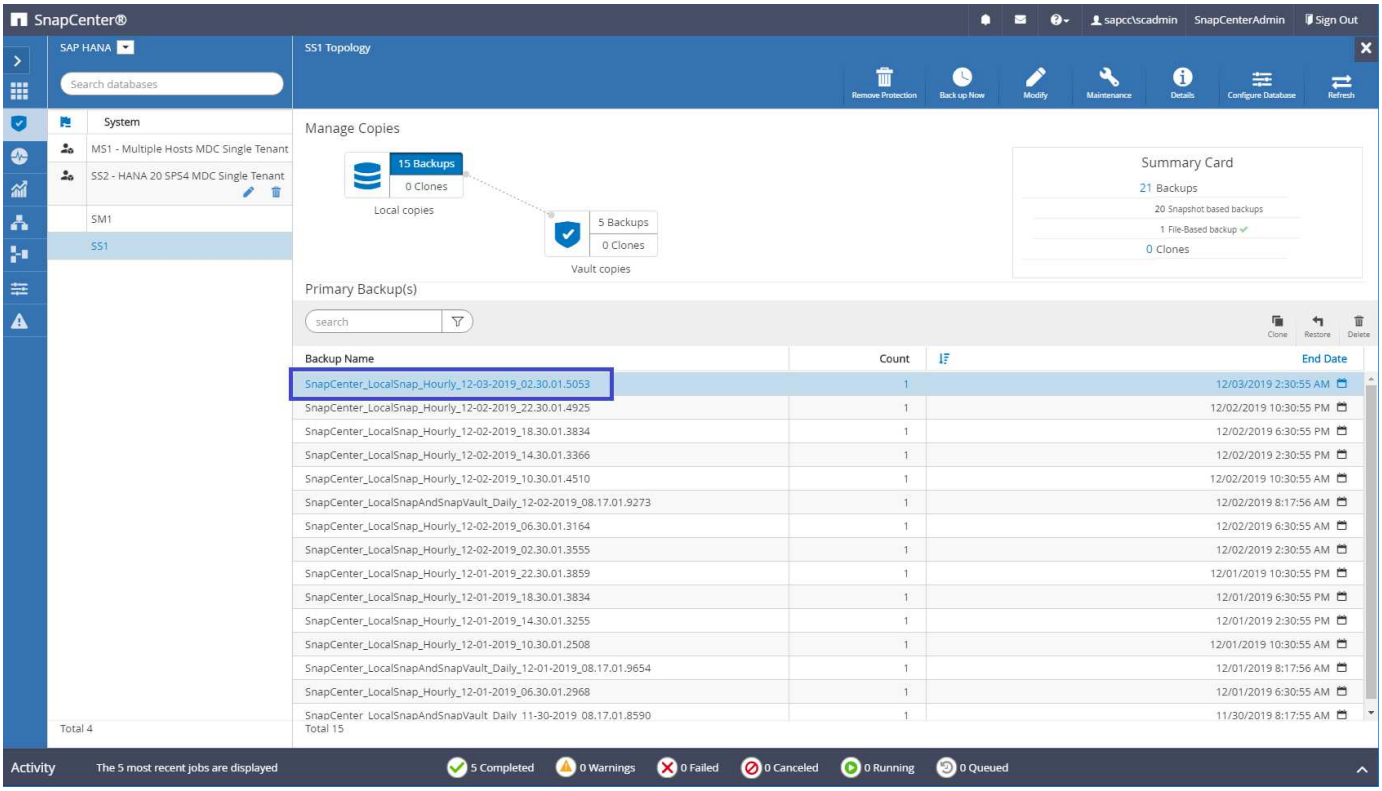
Backup del database

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.

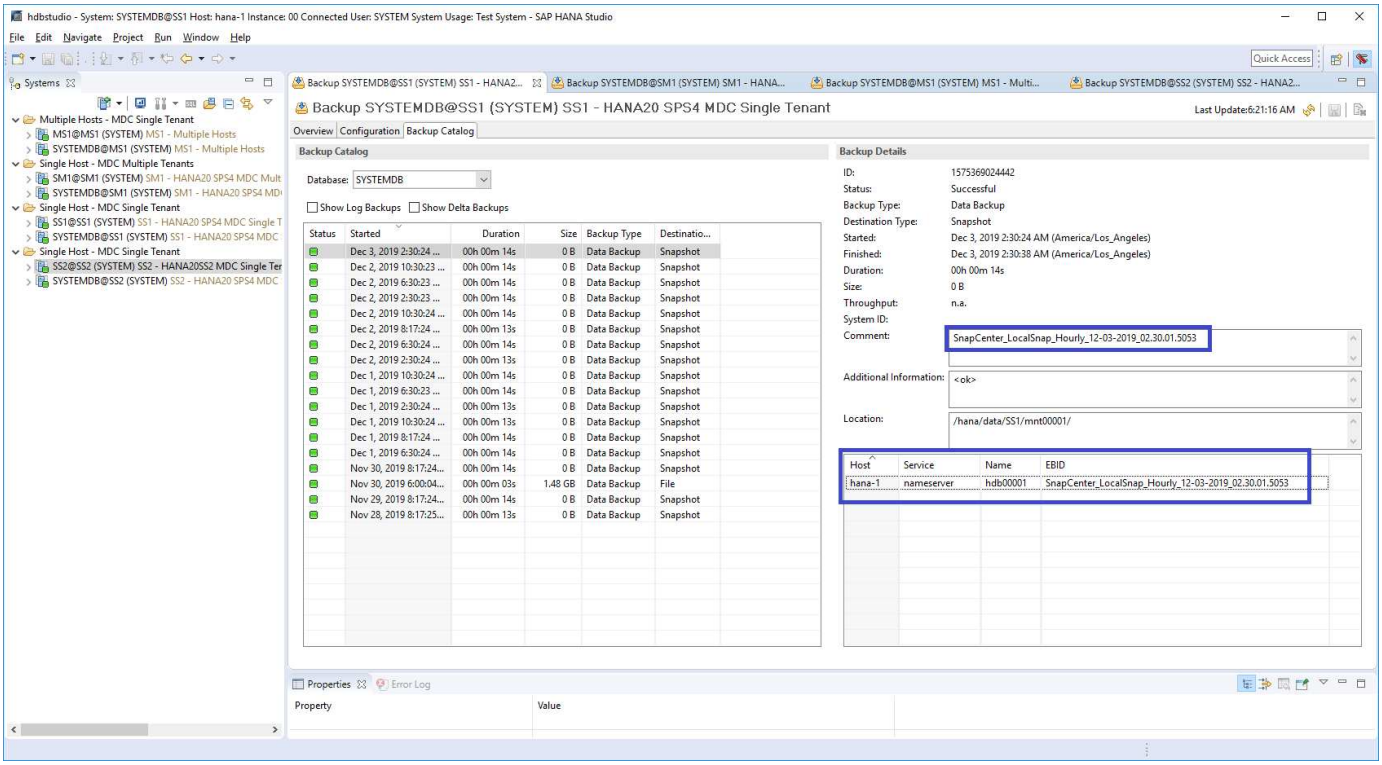


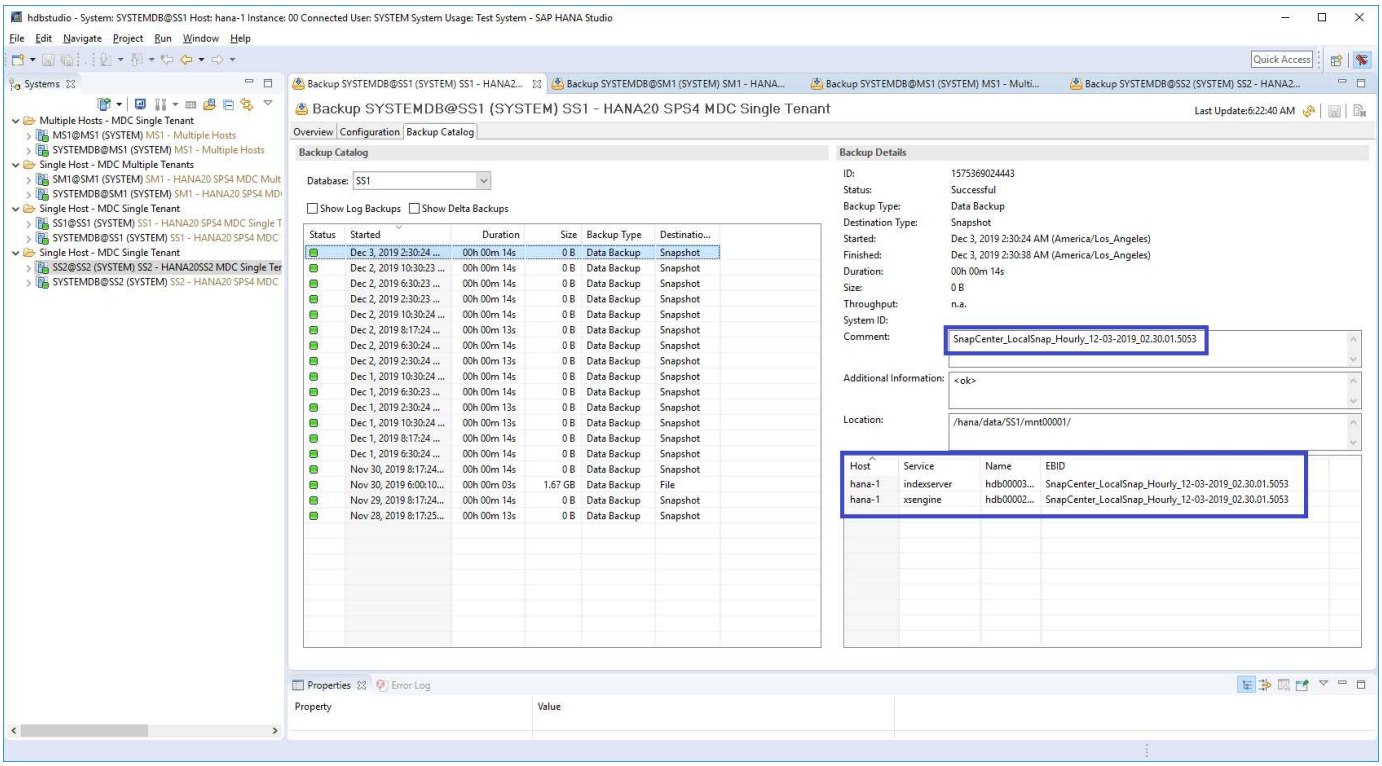
Quando si esegue un backup utilizzando le copie Snapshot dello storage per un sistema SAP HANA MDC, viene creata una copia Snapshot del volume di dati. Questo volume di dati contiene i dati del database di sistema e i dati di tutti i database tenant. Per riflettere questa architettura fisica, SAP HANA 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".

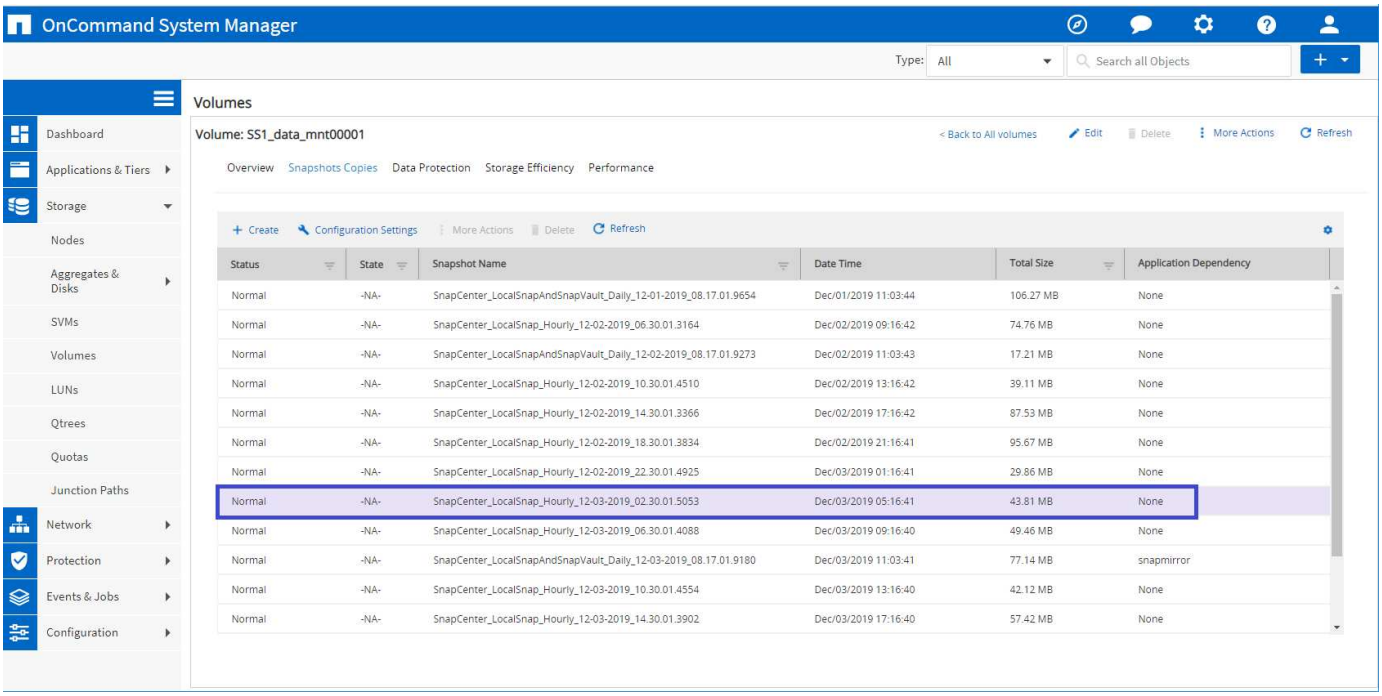




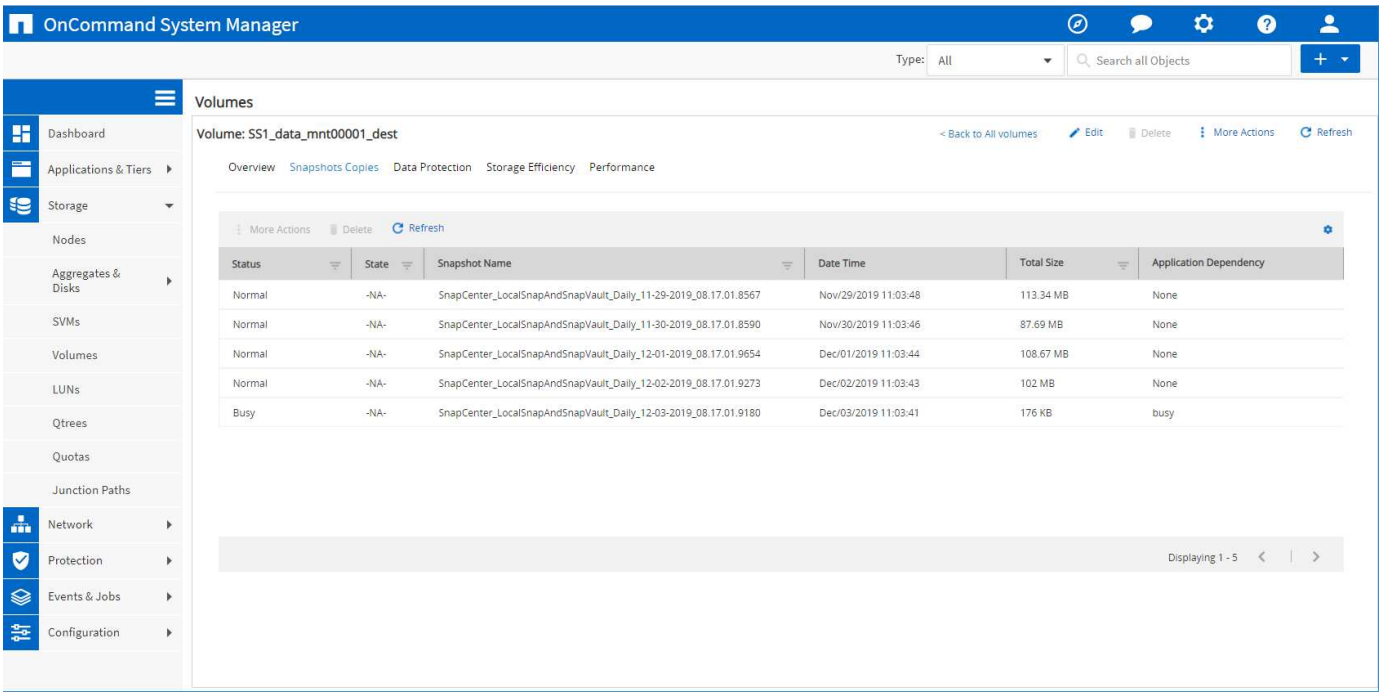
SnapCenter è consapevole solo dei propri backup. I backup aggiuntivi creati, ad esempio, con SAP HANA Studio, sono visibili nel catalogo SAP HANA, ma non in SnapCenter.

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.



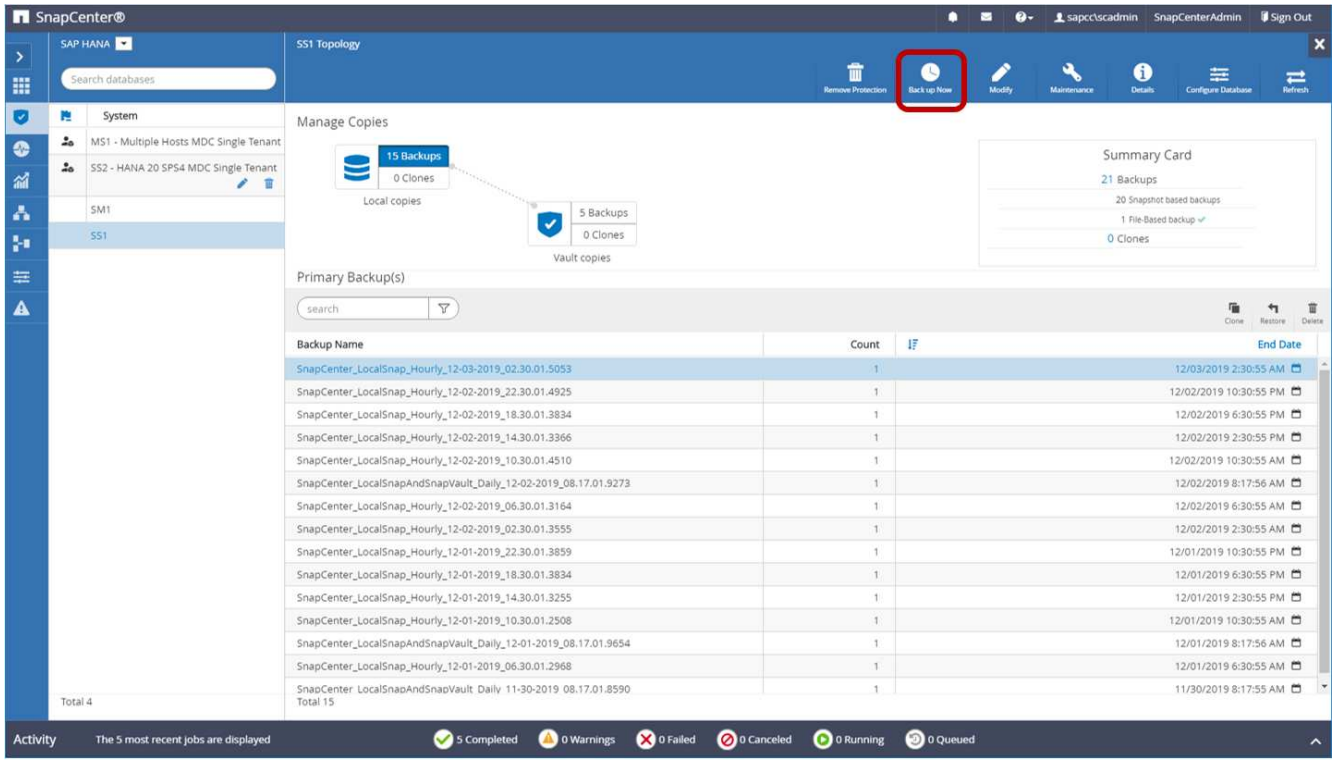
La seguente schermata mostra i backup disponibili per il volume di destinazione della replica `hana_SA1_data_mnt00001_dest` nel sistema di storage secondario.



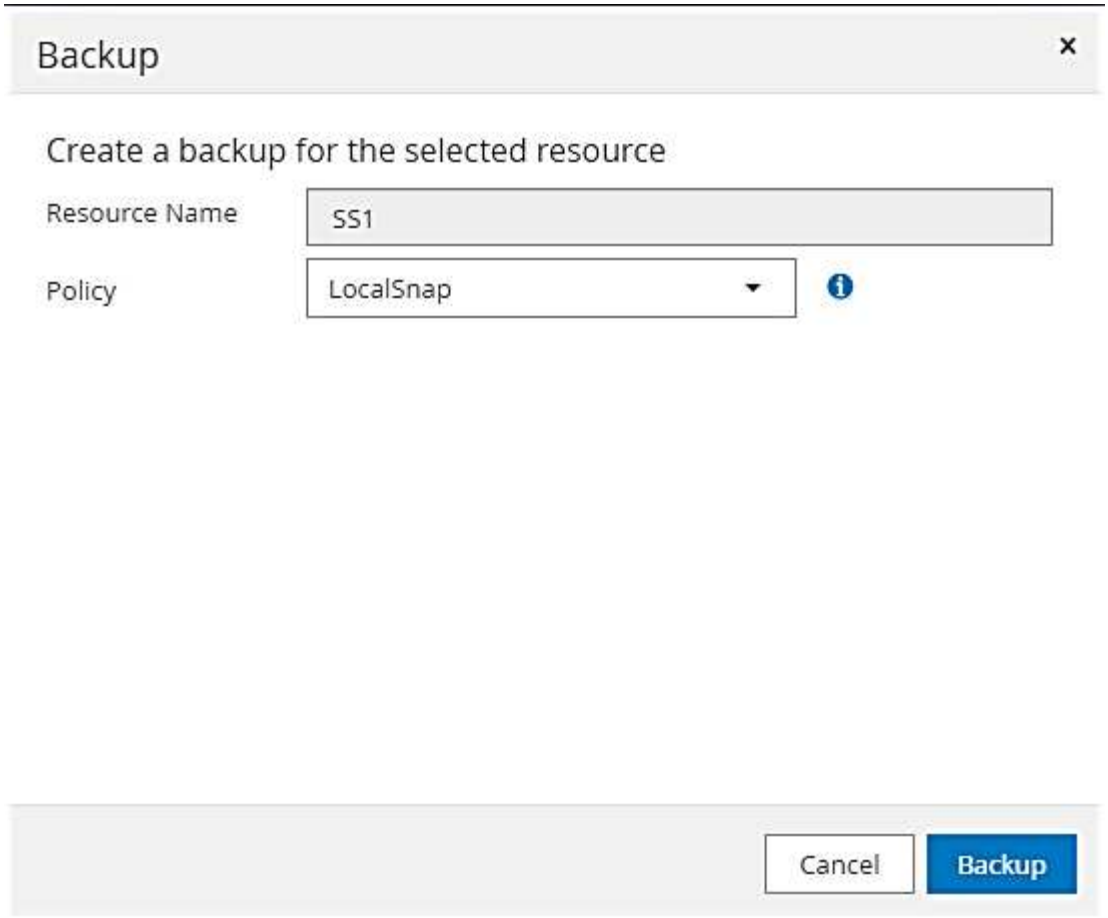
Backup del database on-demand sullo storage primario

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).

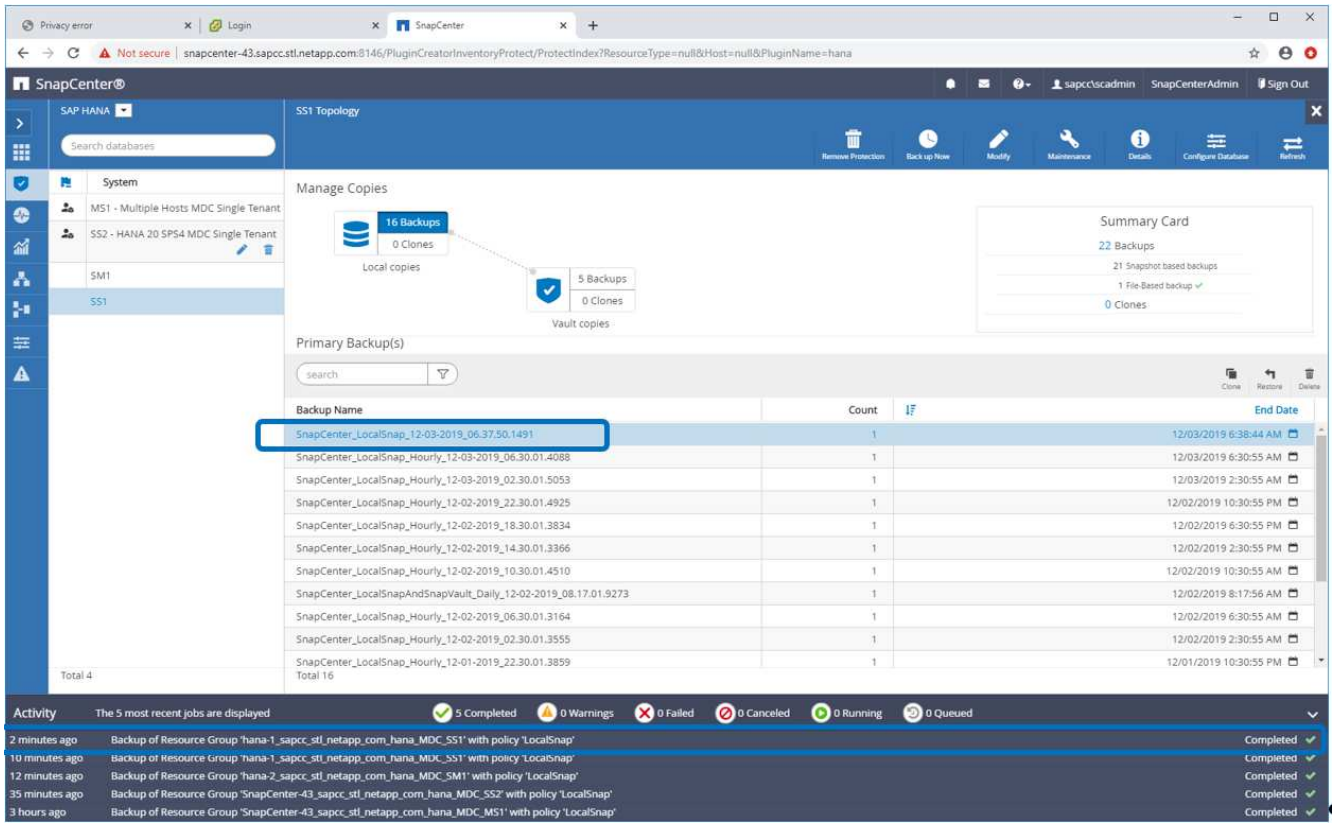


2. Nella riga superiore, selezionare l'icona Backup Now per avviare un backup on-demand. Dall'elenco a discesa, selezionare il criterio di backup `LocalSnap` Quindi fare clic su Backup per avviare il backup on-demand.

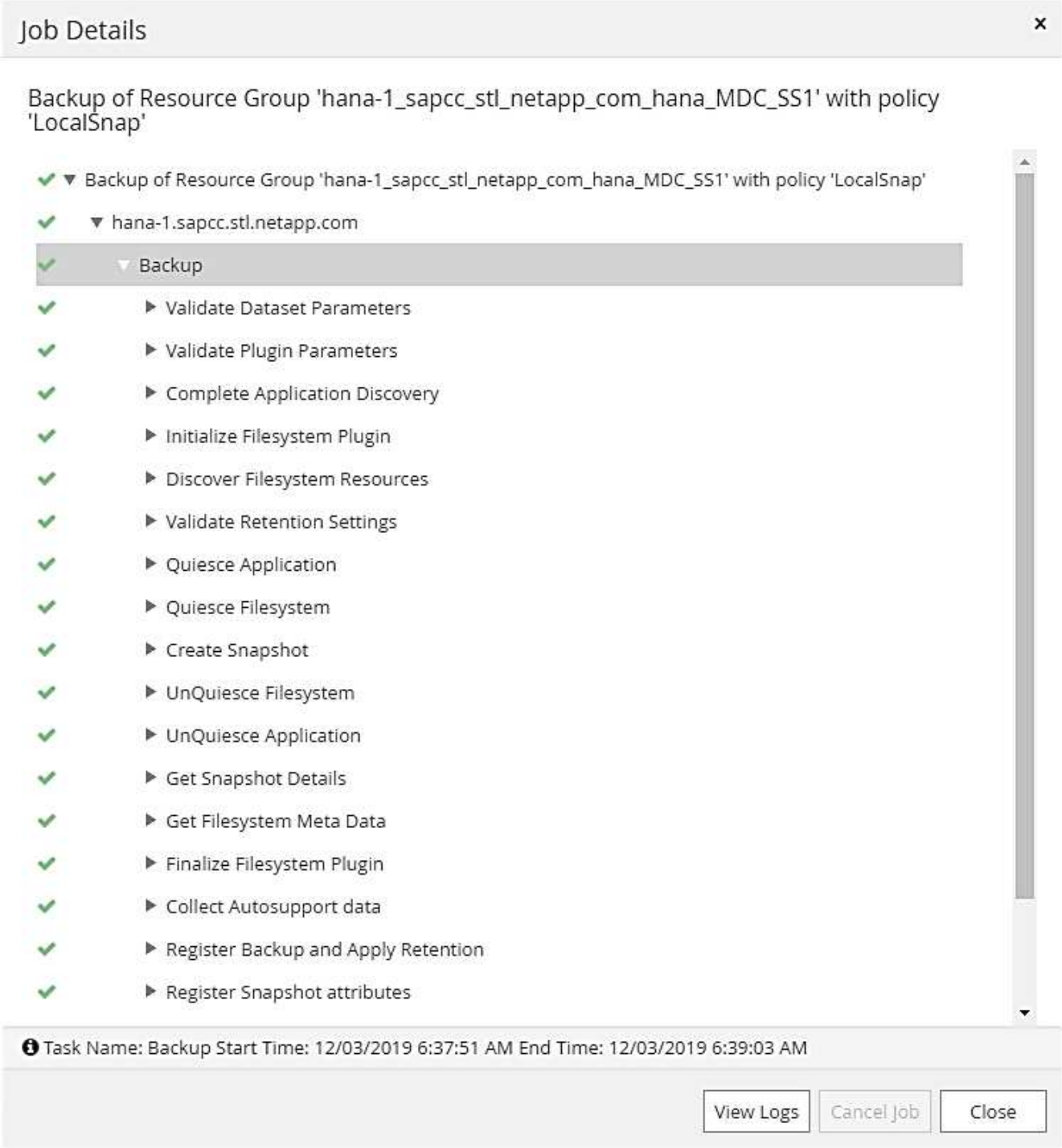


Viene avviato il processo di backup. Un registro dei cinque job precedenti viene visualizzato nell'area Activity (attività) sotto la vista della topologia. Al termine del backup, viene visualizzata una nuova voce nella vista della topologia. I nomi dei backup seguono la stessa convenzione di denominazione 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.



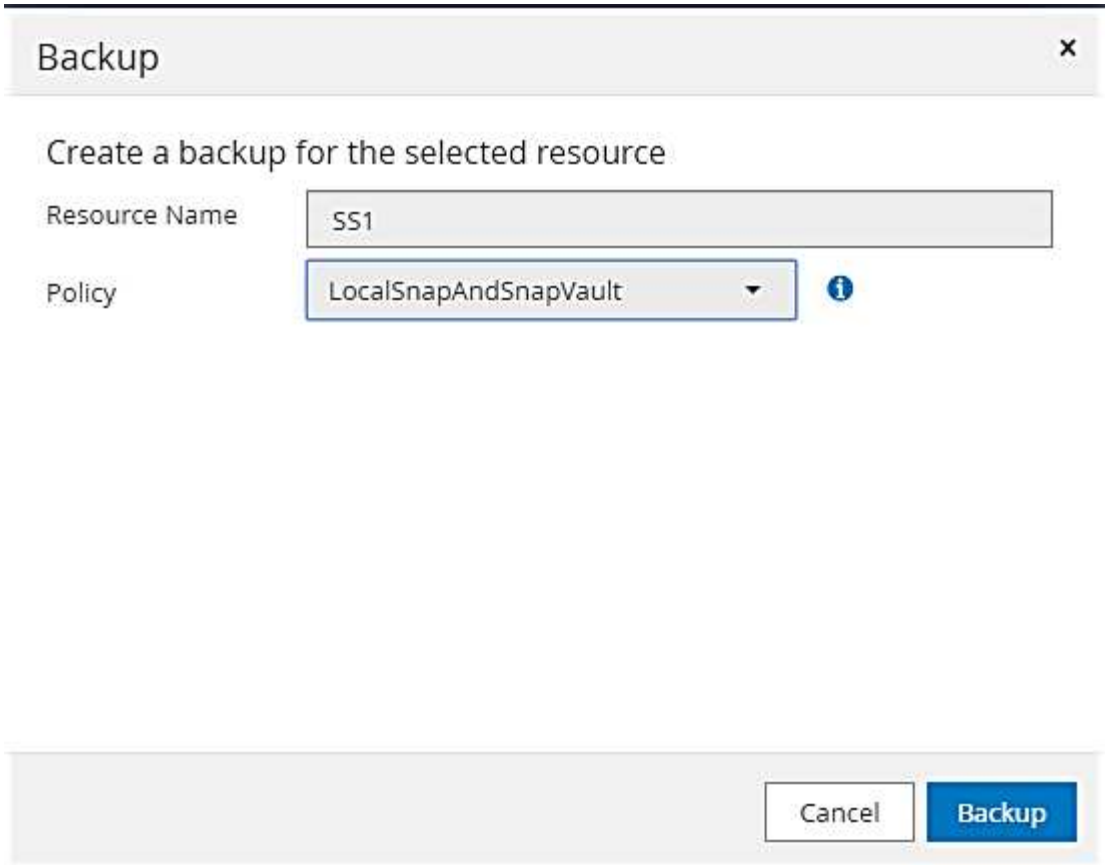
3. I dettagli della commessa vengono visualizzati facendo clic sulla riga dell'attività della commessa nell'area Activity (attività). È possibile aprire un registro dettagliato dei processi facendo clic su View Logs (Visualizza registri).



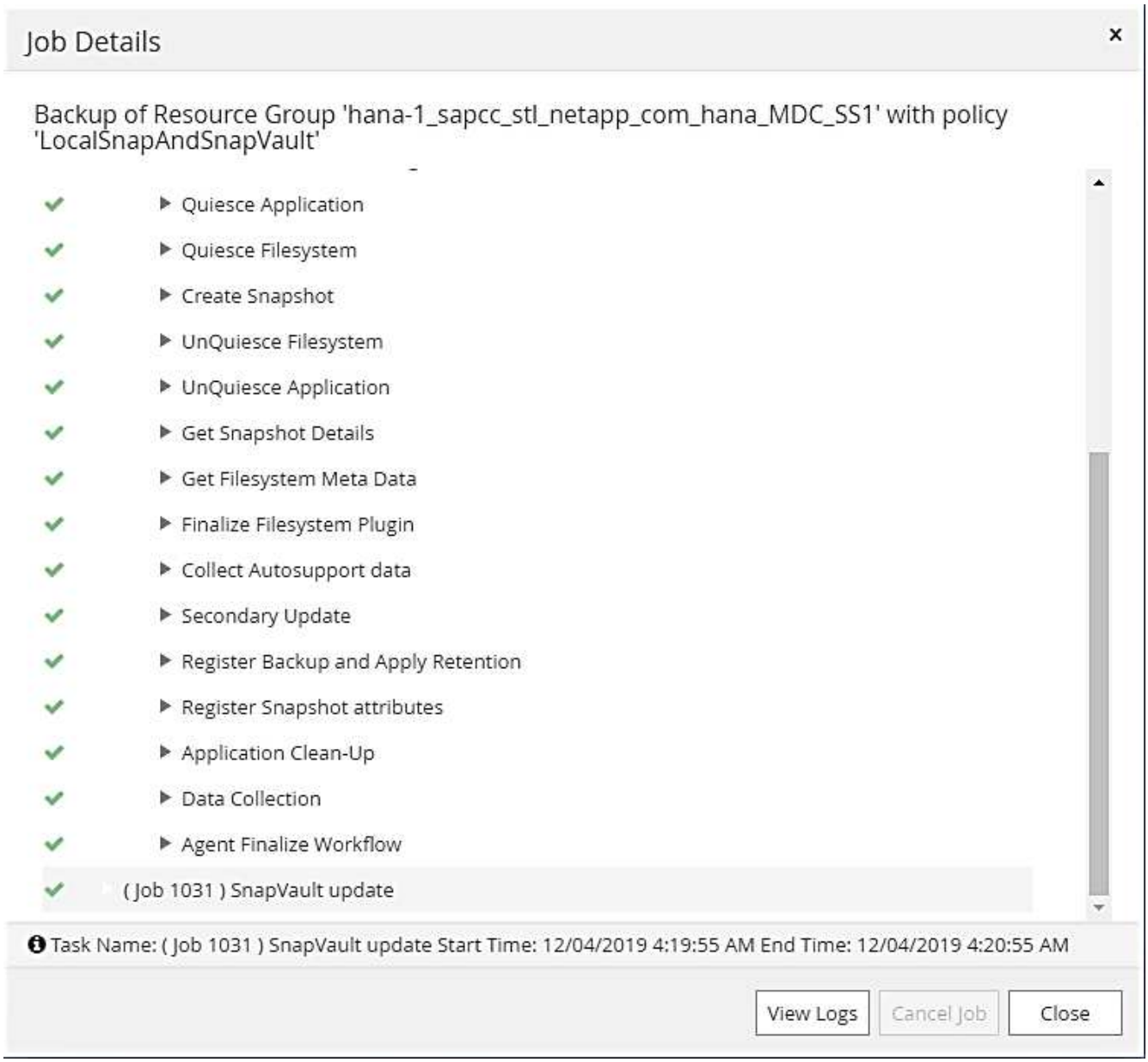
4. In SAP HANA Studio, il nuovo backup è visibile nel catalogo di backup. Lo stesso nome di backup in SnapCenter viene utilizzato anche nel campo comment e EBID nel catalogo di backup.

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.

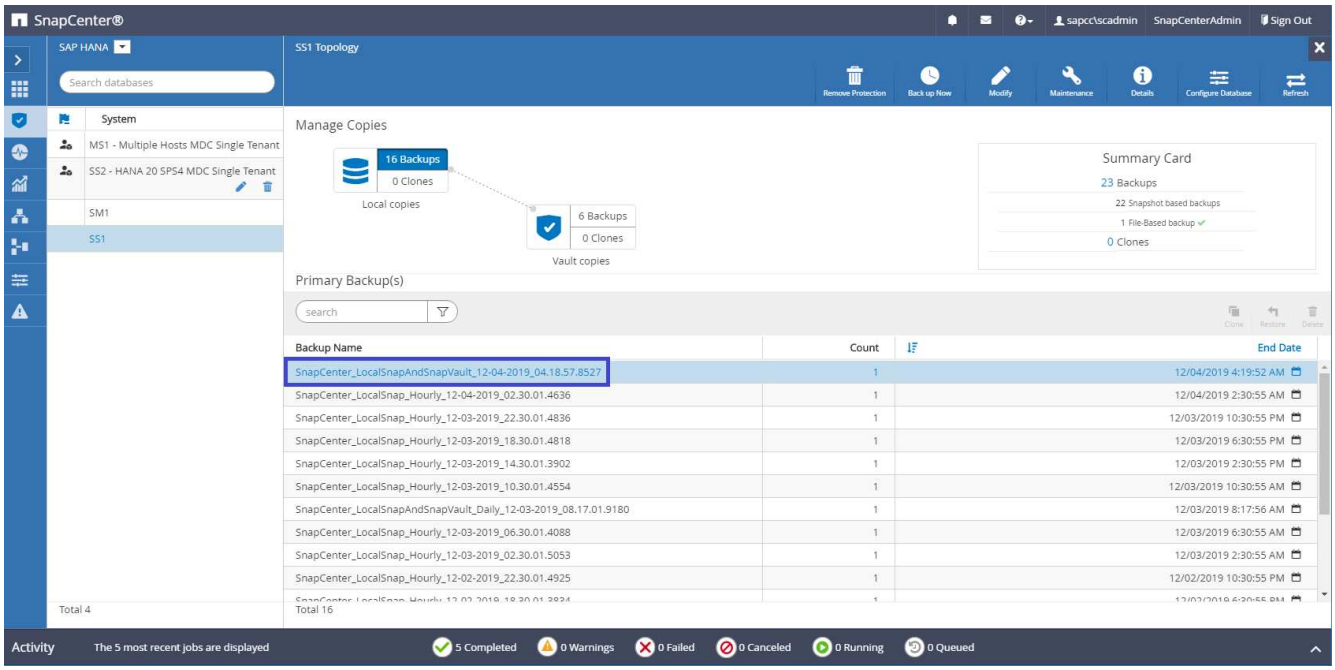


3. I dettagli della commessa vengono visualizzati facendo clic sulla riga dell'attività della commessa nell'area Activity (attività).

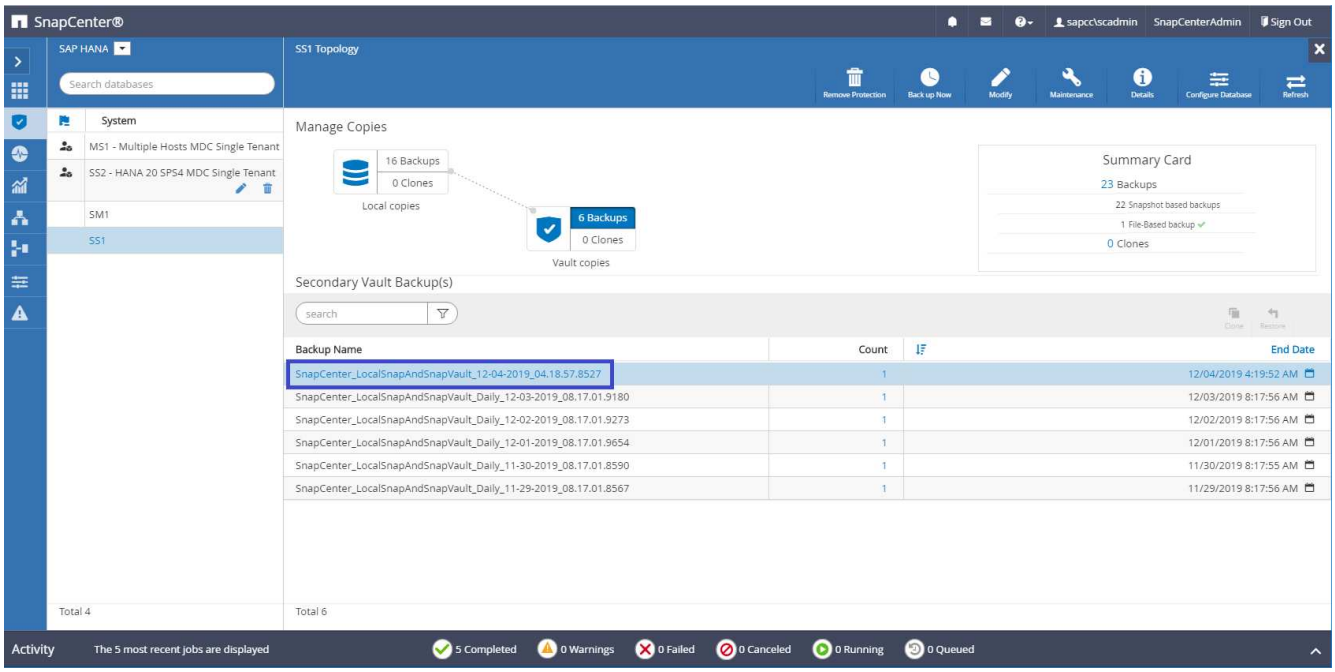


4. Al termine del backup, viene visualizzata una nuova voce nella vista della topologia. I nomi dei backup seguono la stessa convenzione di denominazione del nome Snapshot definito nella sezione ""Configurazione della protezione delle risorse"."

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



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.



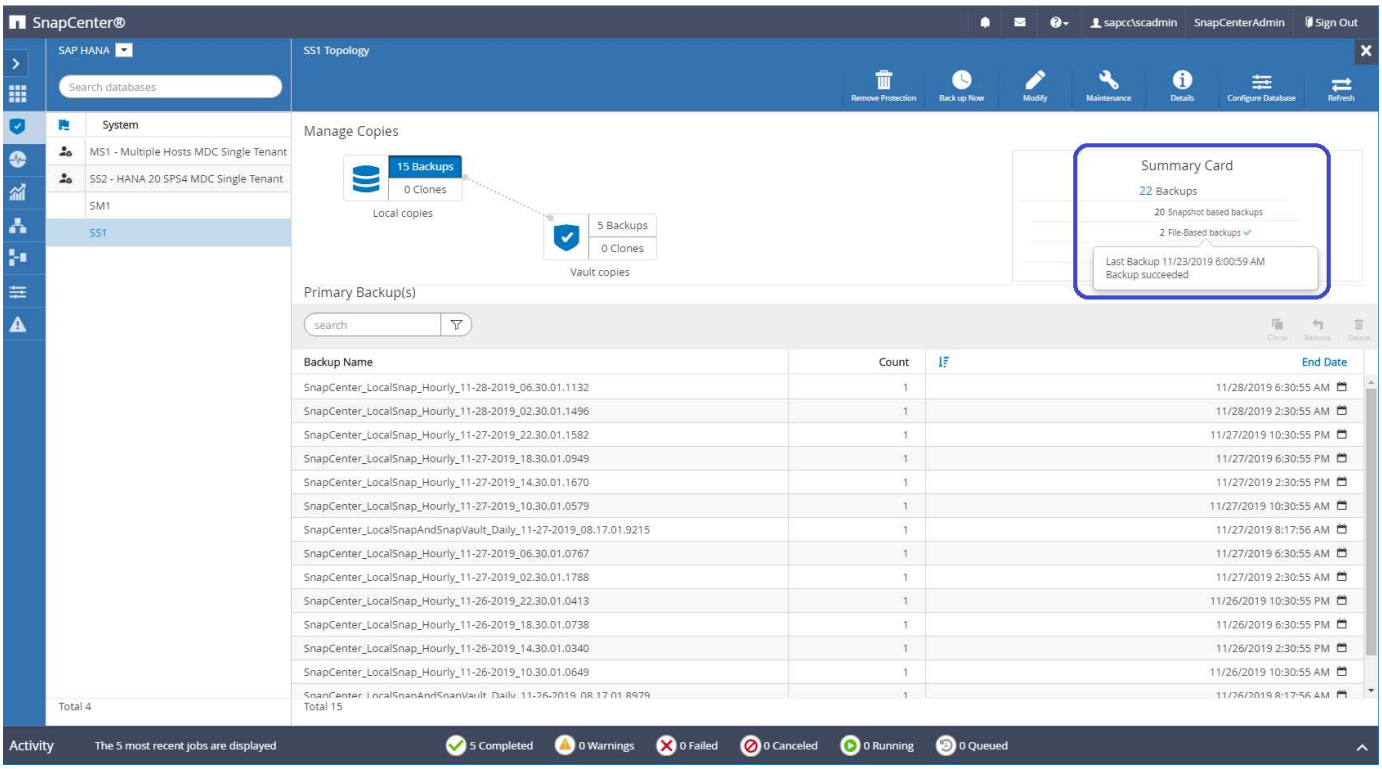
6. In SAP HANA Studio, il nuovo backup è visibile nel catalogo di backup. Lo stesso nome di backup in SnapCenter viene utilizzato anche nel campo comment e EBID nel catalogo di backup.

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.

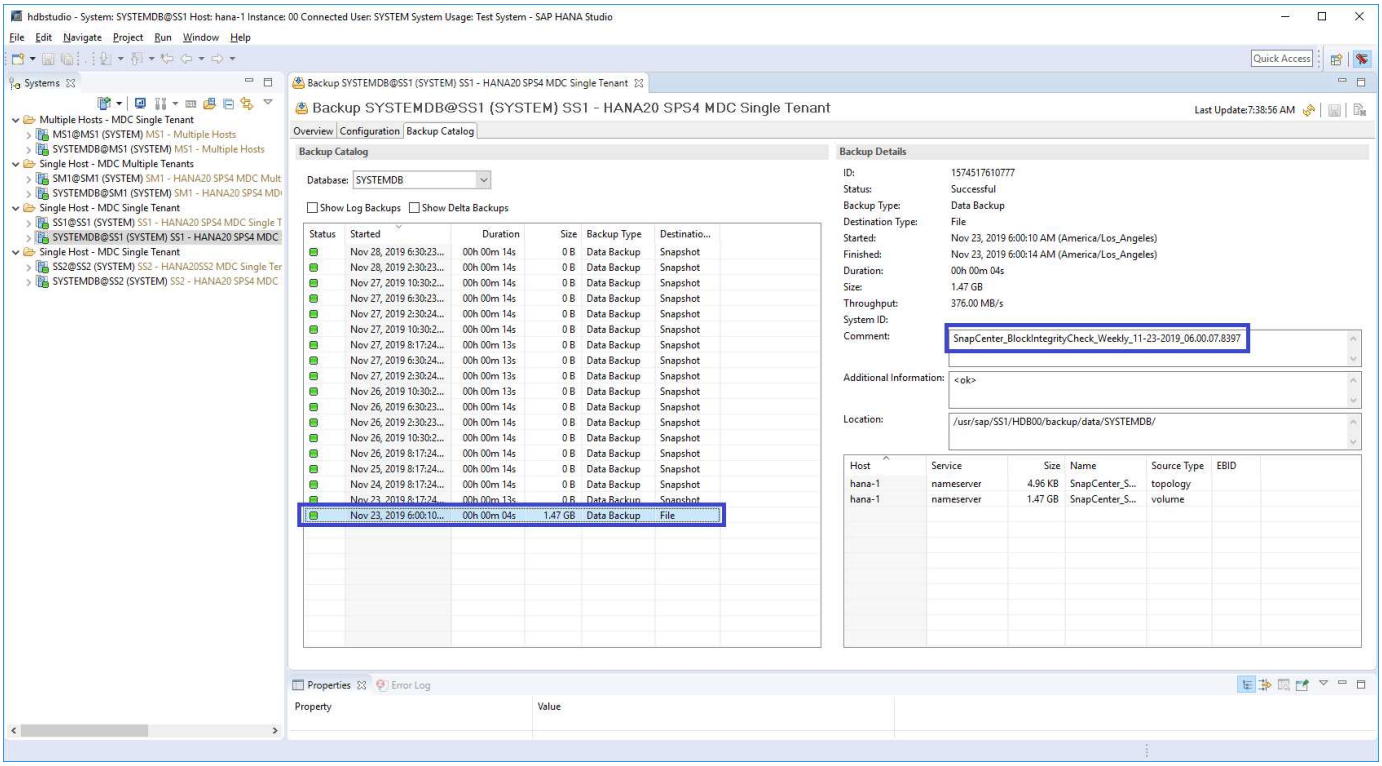
SnapCenter non visualizza il controllo dell'integrità del blocco allo stesso modo dei backup basati su copia Snapshot. La scheda di riepilogo mostra invece il numero di backup basati su file e lo stato del backup precedente.



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 ss1adm sapsys       4096 Nov 28 10:25 .
drwxr-xr-- 4 ss1adm sapsys       4096 Nov 19 05:11 ..
-rw-r----- 1 ss1adm sapsys     155648 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ss1adm sapsys   83894272 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_2_1
-rw-r----- 1 ss1adm 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 ss1adm sapsys       4096 Nov 28 10:24 .
drwxr-xr-- 4 ss1adm sapsys       4096 Nov 19 05:11 ..
-rw-r----- 1 ss1adm sapsys     159744 Nov 23 08:46
SnapCenter_SnapCenter_BlockIntegrityCheck_Weekly_11-23-
2019_06.00.07.8397_databackup_0_1
-rw-r----- 1 ss1adm 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:

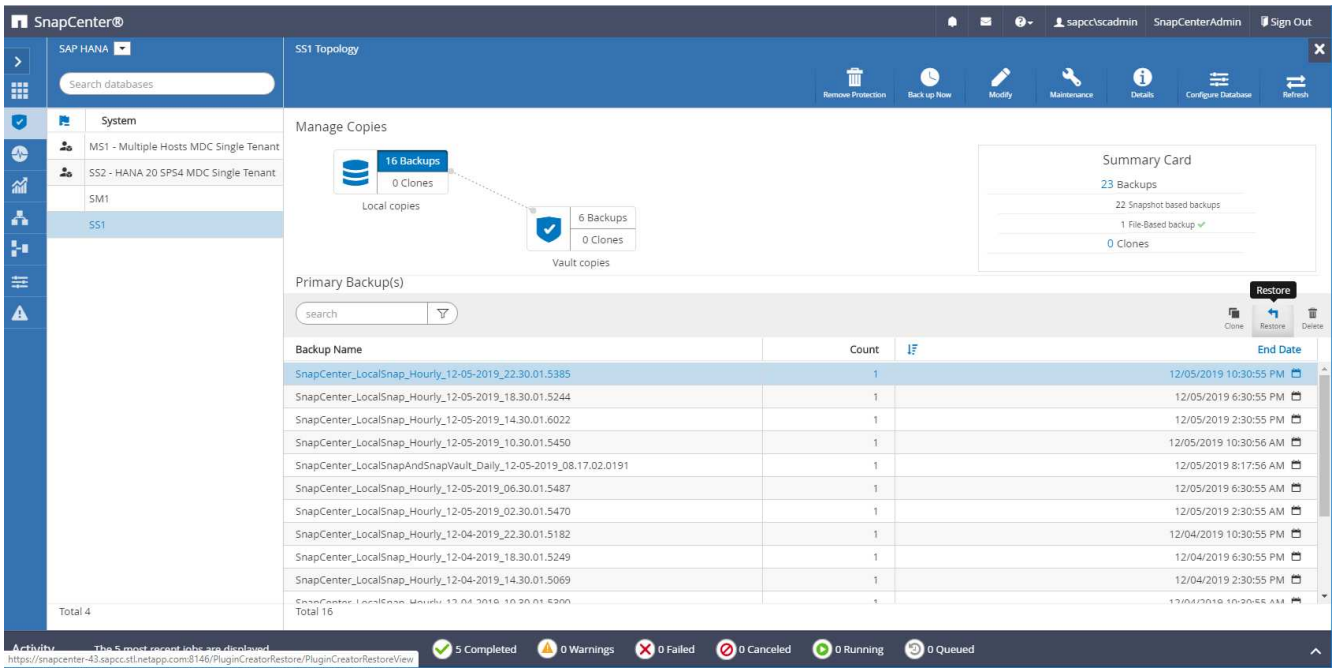
c. Avvia il database HANA.

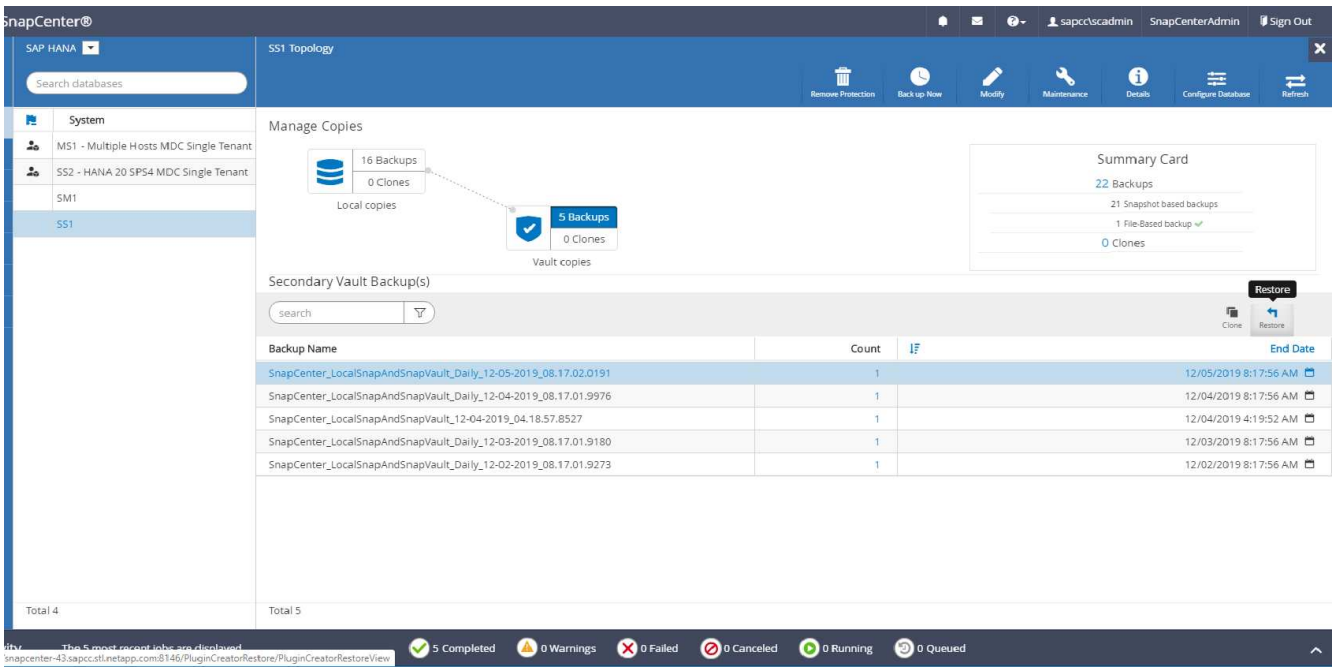
> Se si seleziona No Recovery (Nessun ripristino), SnapCenter viene chiuso e l'operazione di ripristino del sistema e del database tenant deve essere eseguita manualmente.

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.



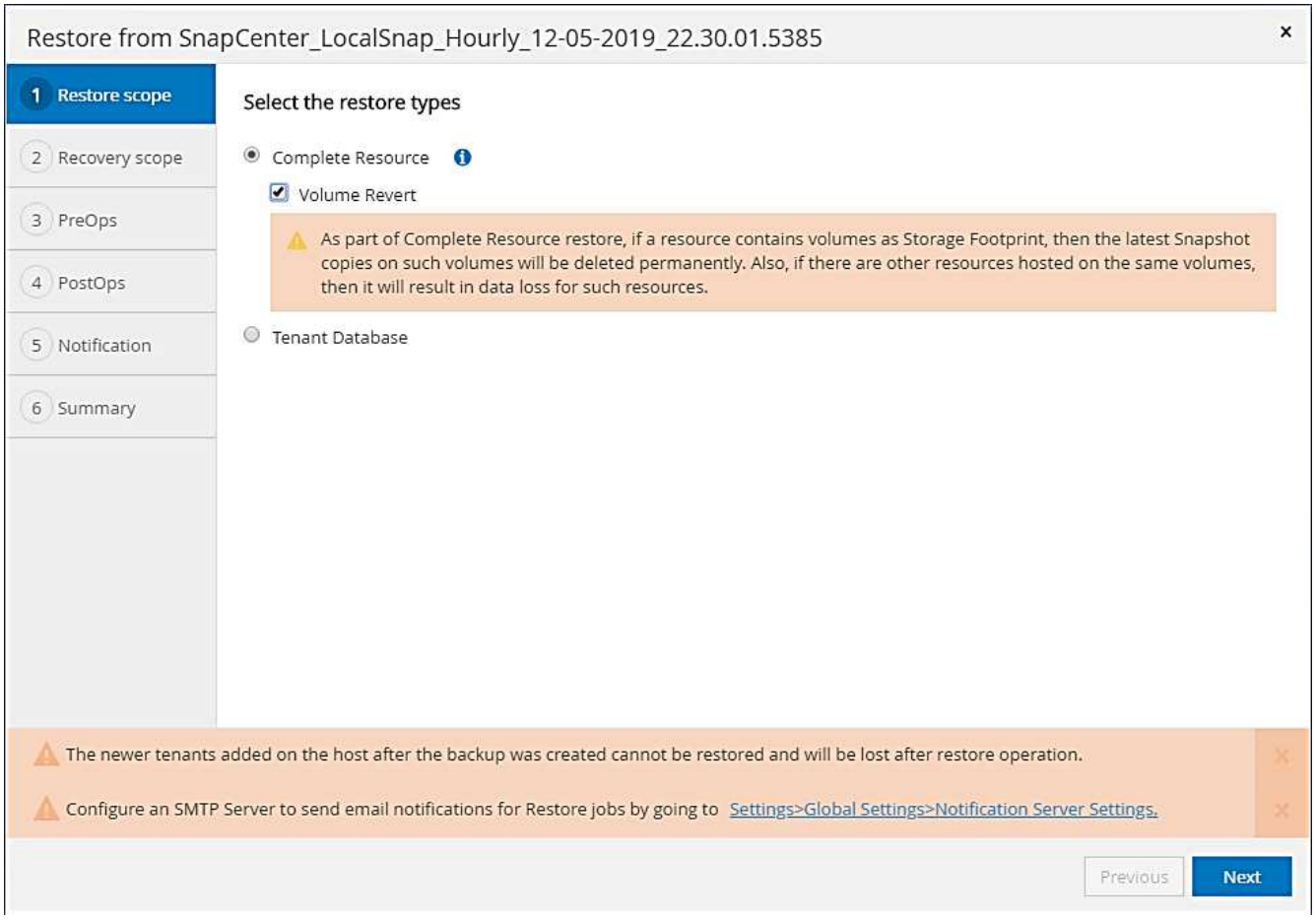


2. Selezionare l'ambito e il tipo di ripristino.

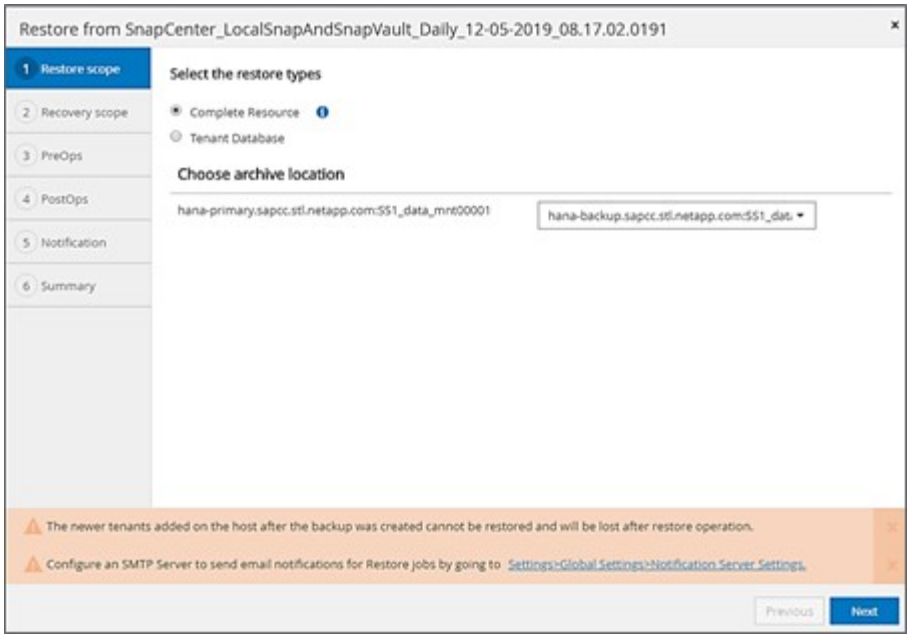
   Le tre schermate seguenti mostrano le opzioni di ripristino per il ripristino da primario con NFS, il ripristino da secondario con NFS e il ripristino da primario con SAN Fibre Channel.

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

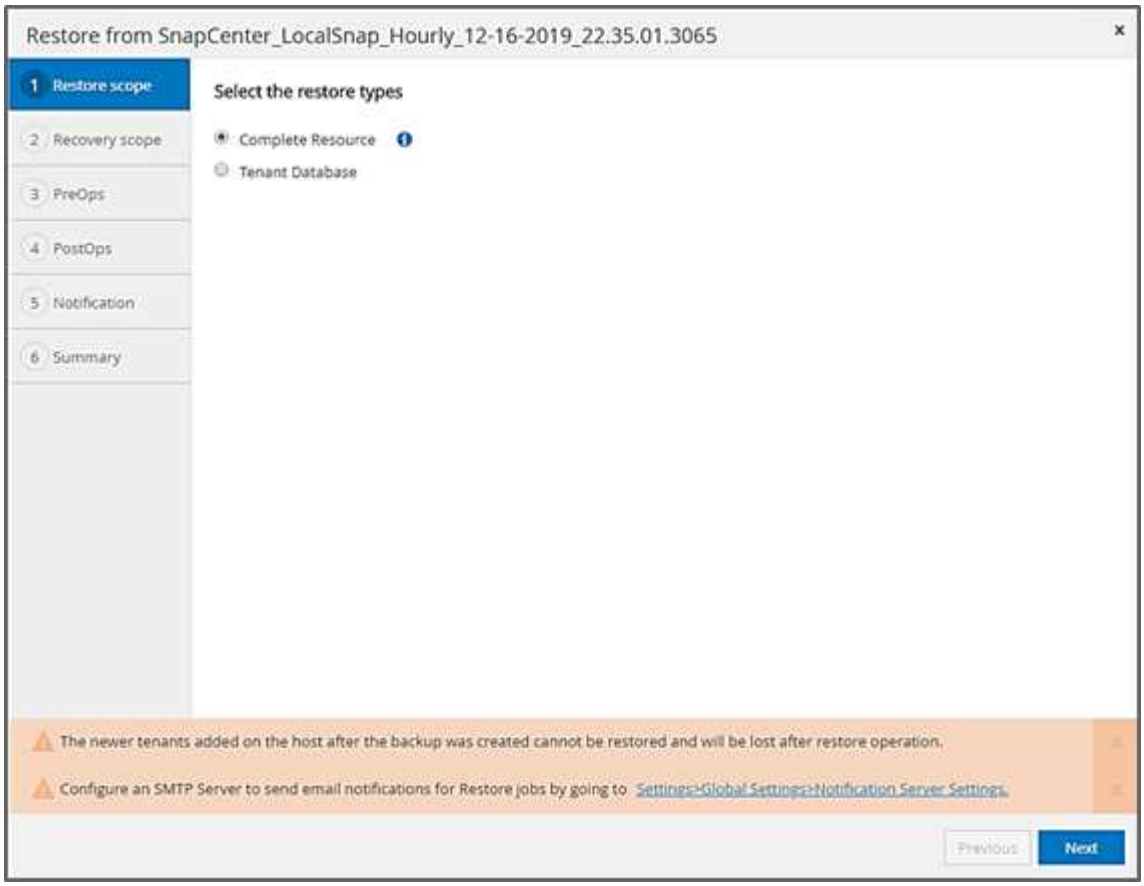
   > L'opzione di ripristino del volume è disponibile solo per le operazioni di ripristino da primarie con NFS.



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

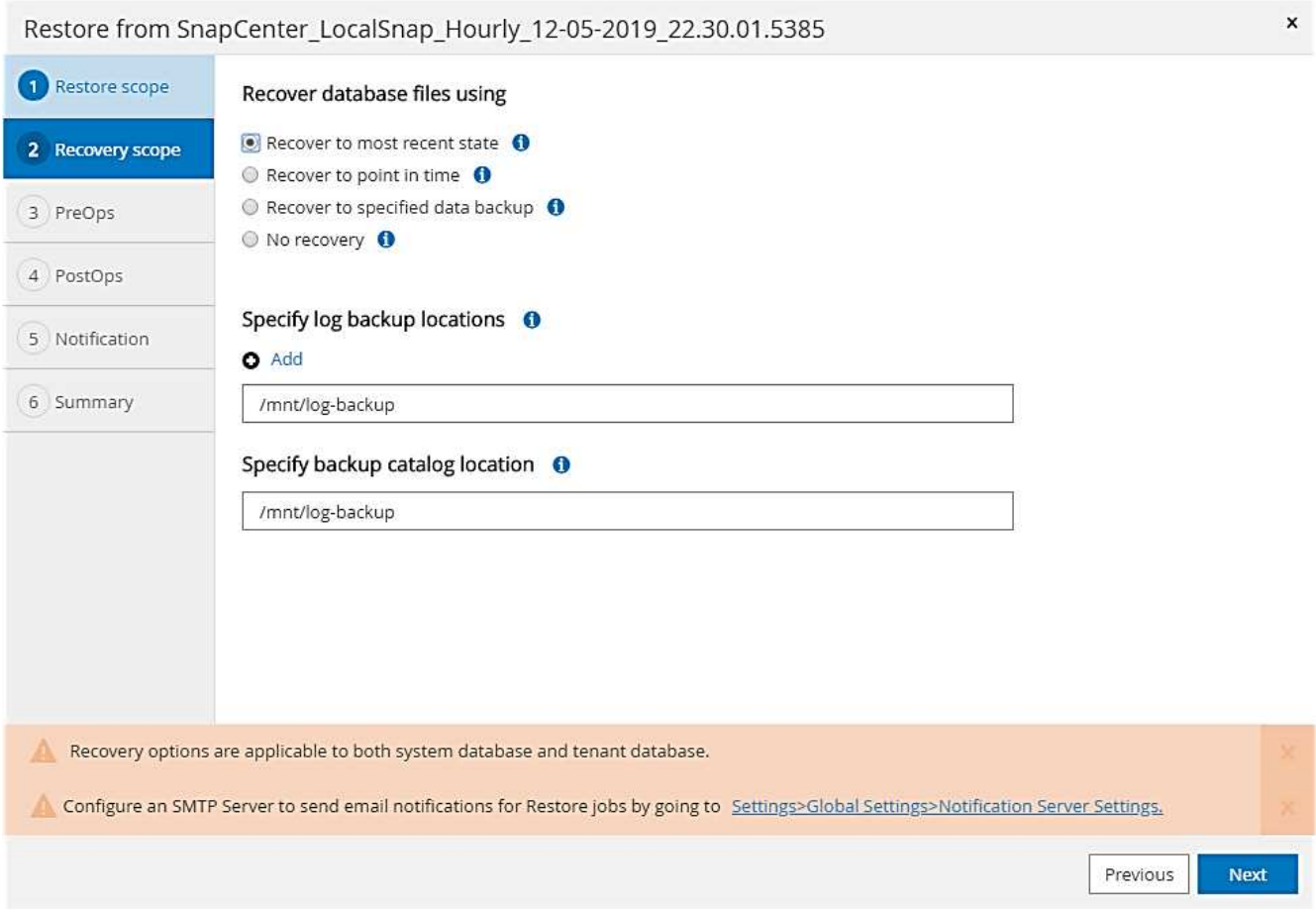


Opzioni del tipo di ripristino per il ripristino dallo storage primario con SAN Fibre Channel.

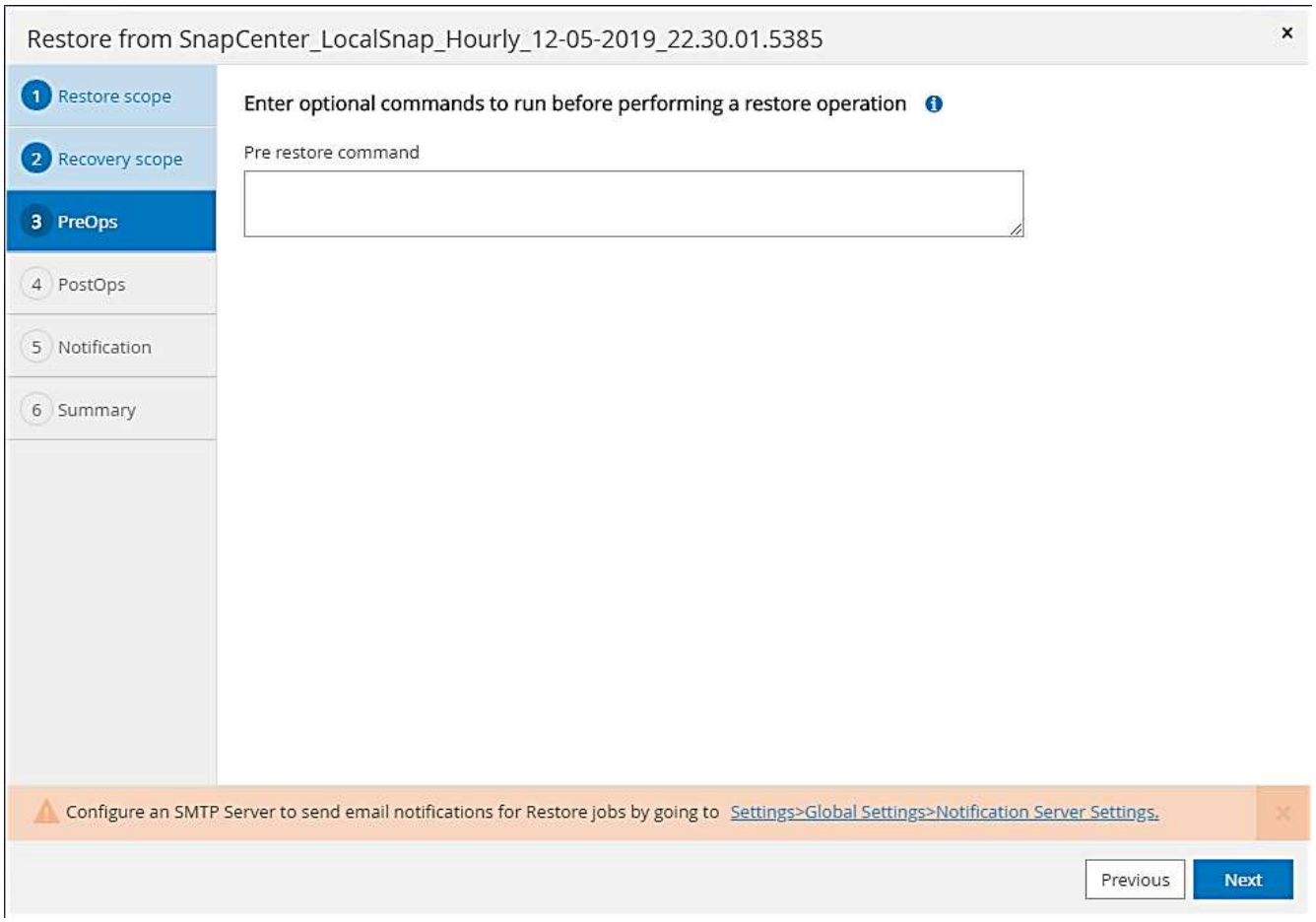


3. Selezionare Recovery Scope (ambito ripristino) e specificare la posizione per il backup del registro e del catalogo.

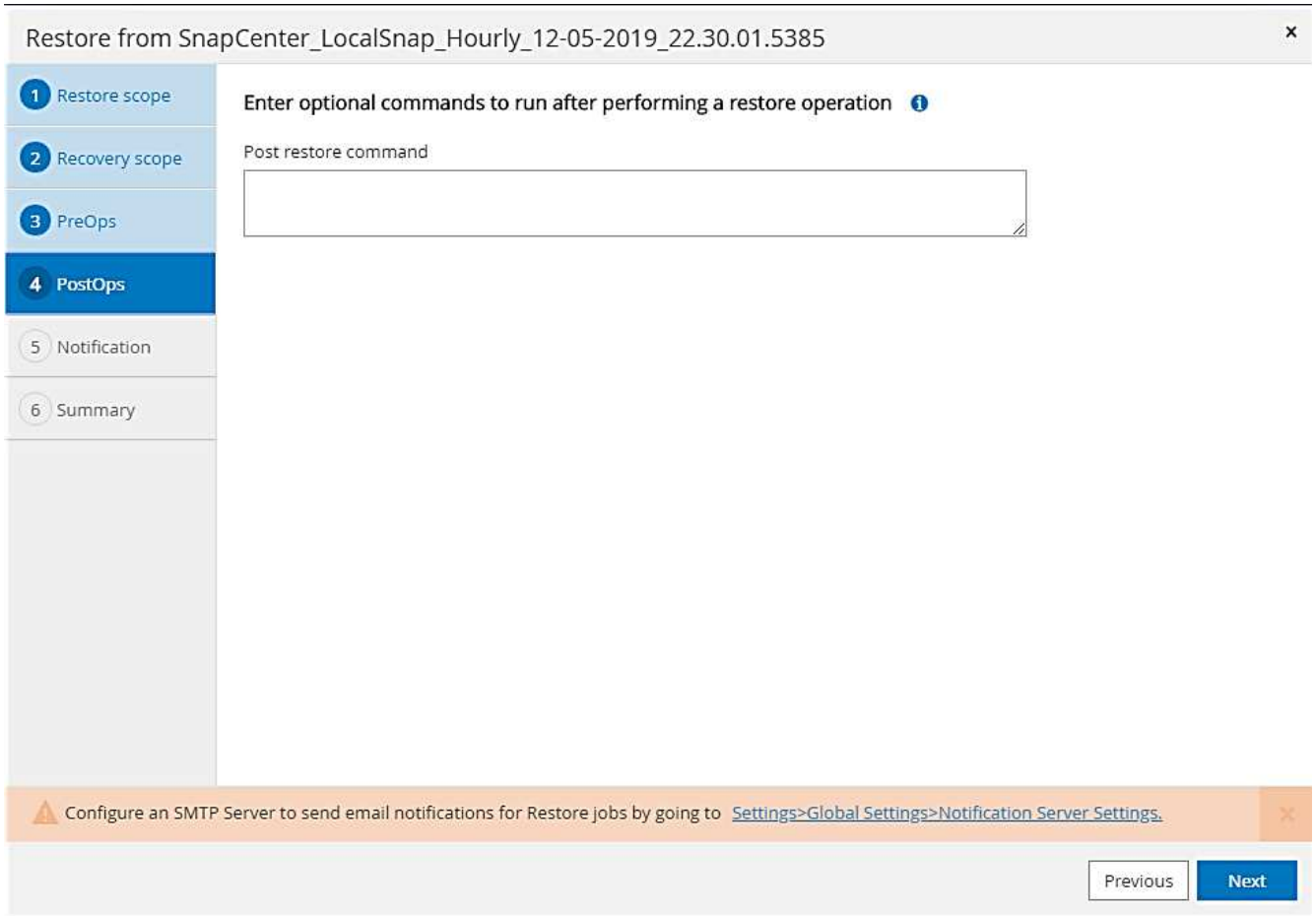
> SnapCenter utilizza il percorso predefinito o i percorsi modificati nel file HANA global.ini per prepopolare le posizioni di backup del registro e del catalogo.



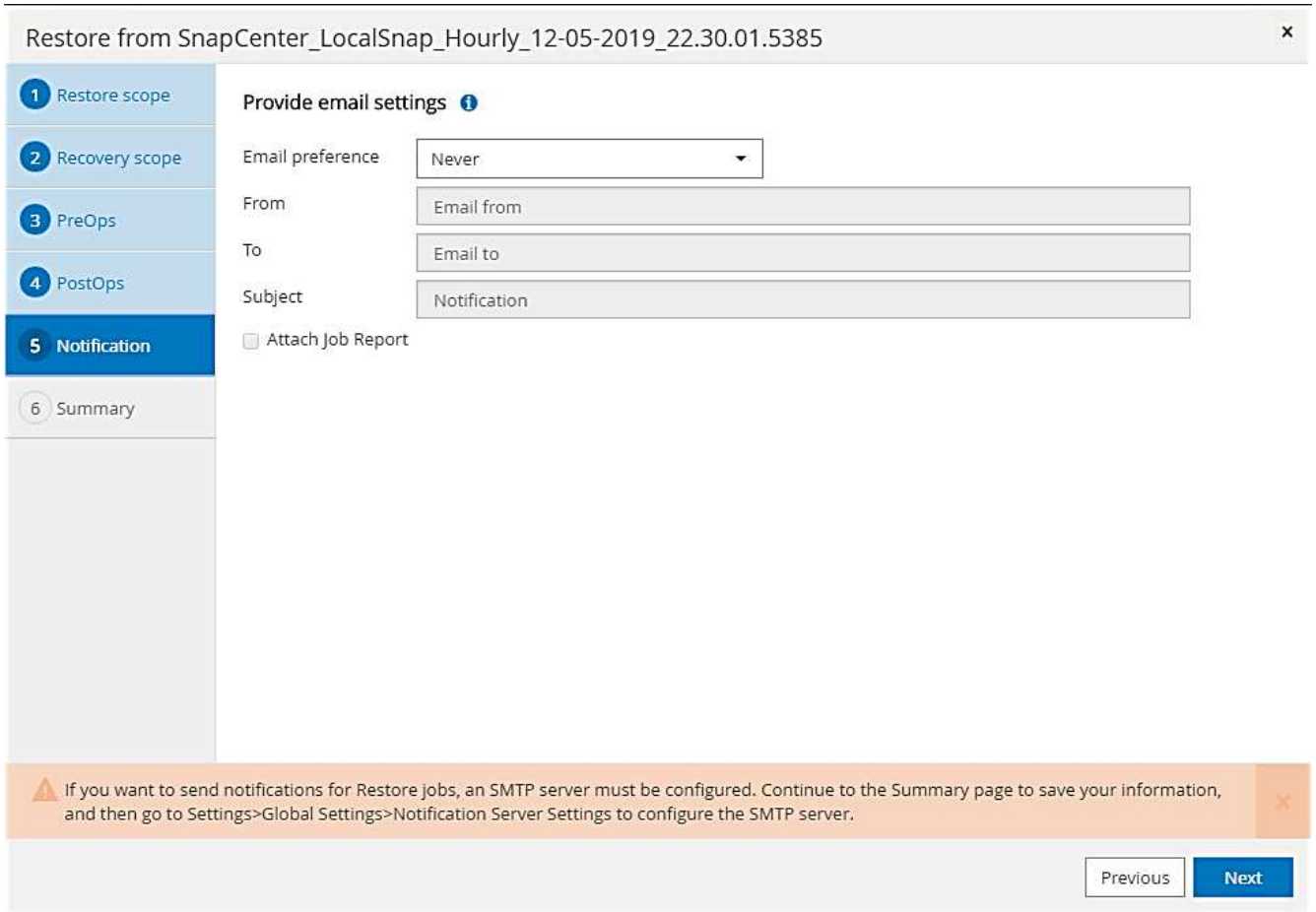
4. Immettere i comandi opzionali di prerestore.



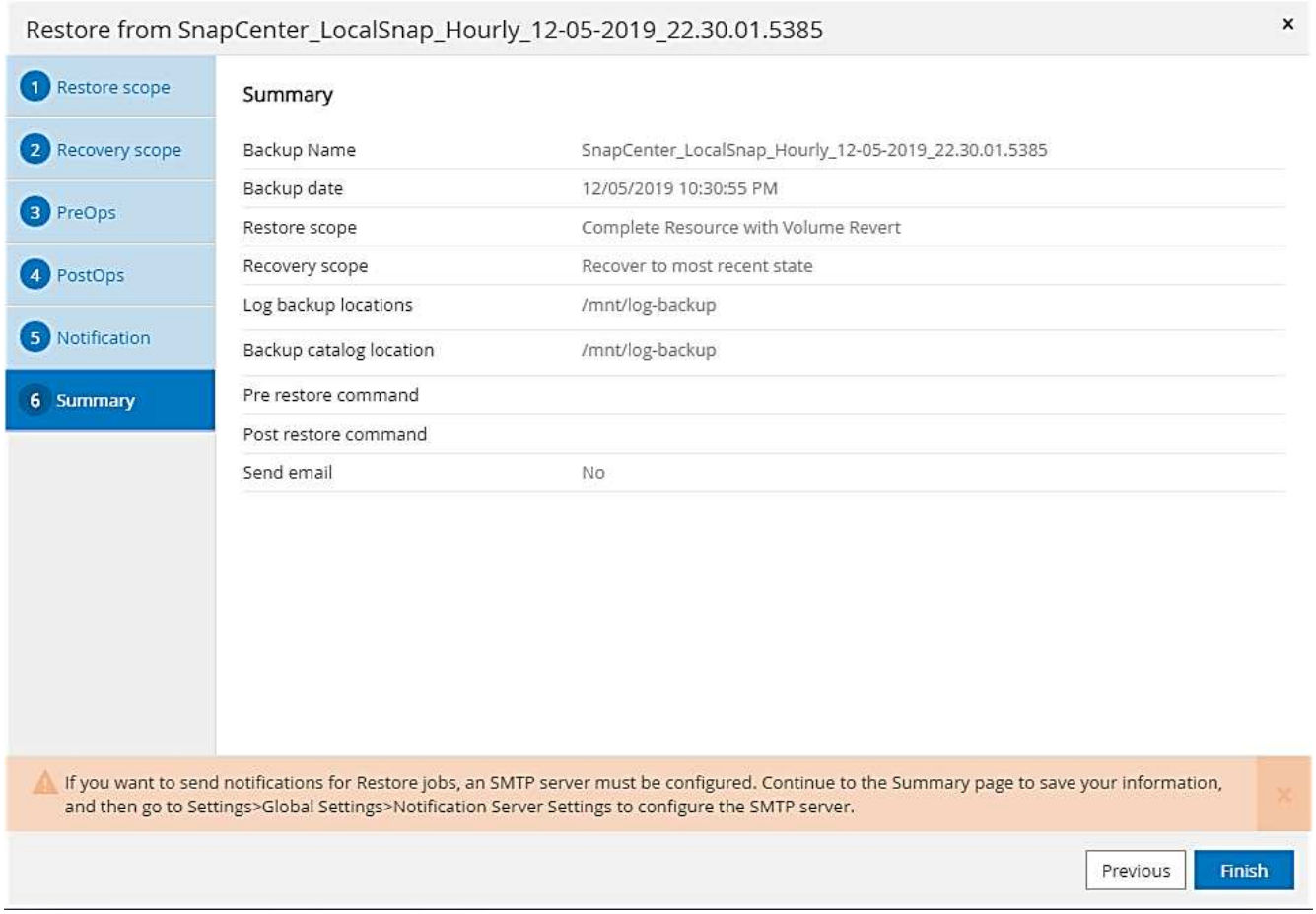
5. Immettere i comandi post-ripristino opzionali.



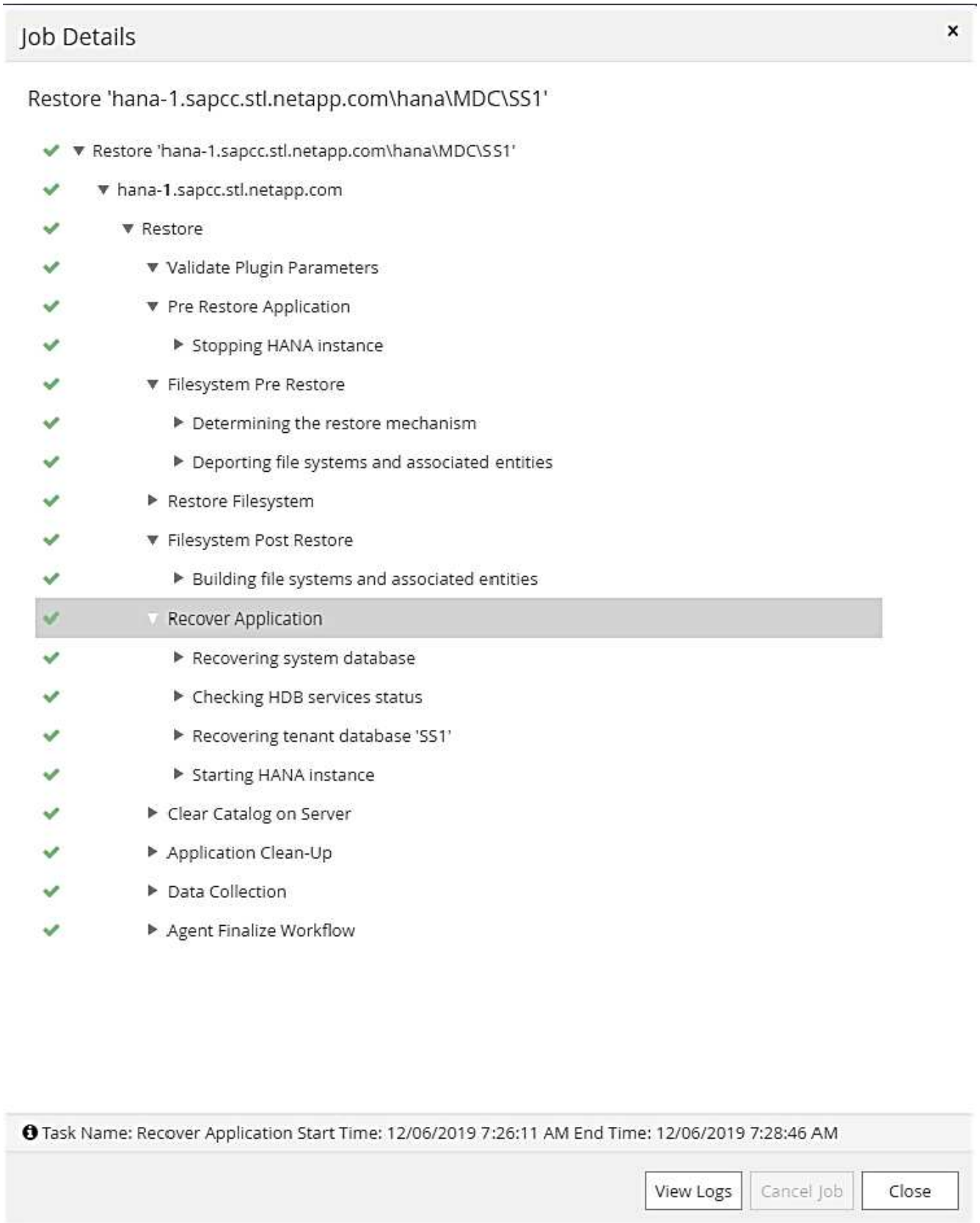
6. Immettere le impostazioni e-mail opzionali.



7. Per avviare l’operazione di ripristino, fare clic su fine.



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



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:

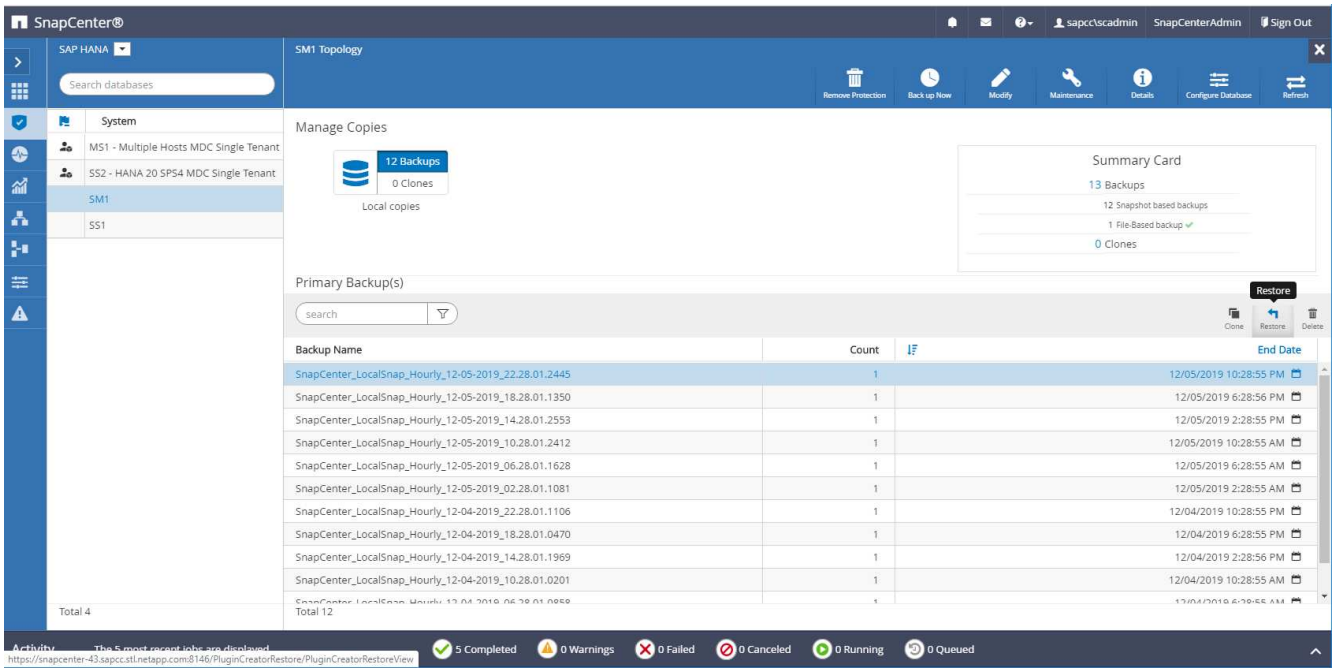
1. Arrestare il tenant da ripristinare e ripristinare.
2. Ripristinare il tenant con SnapCenter.
   - Per un ripristino dallo storage primario, SnapCenter esegue le seguenti operazioni:
     - **NFS.** Storage operazioni Single file SnapRestore per tutti i file del database tenant.
     - **SAN.** Clona 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.

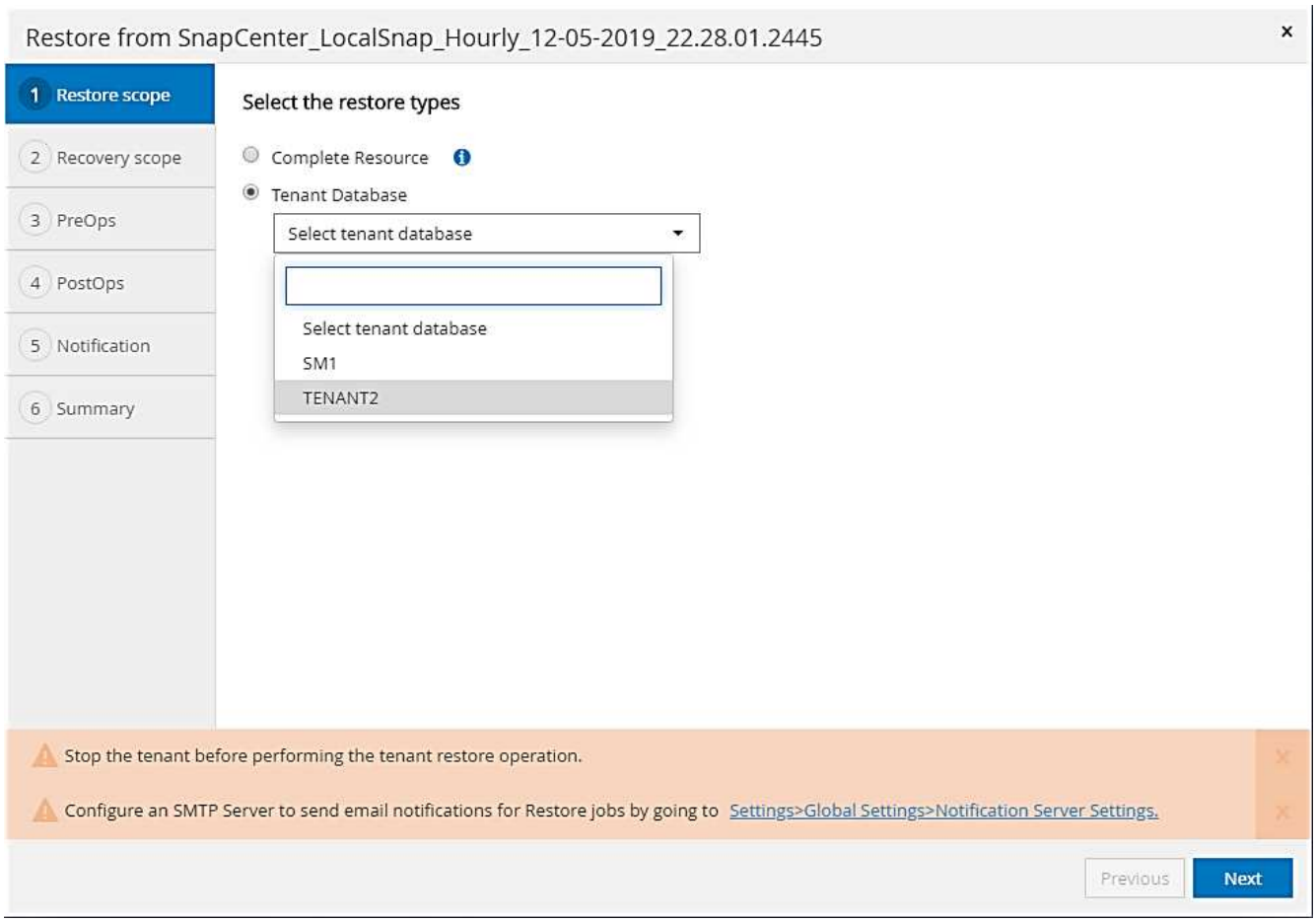
```
sm1adm@hana-2:/usr/sap/SM1/HDB00> hdbsql -U SYSKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql=>
hdbsql SYSTEMDB=> alter system stop database tenant2;
0 rows affected (overall time 14.215281 sec; server time 14.212629 sec)
hdbsql SYSTEMDB=>
```

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

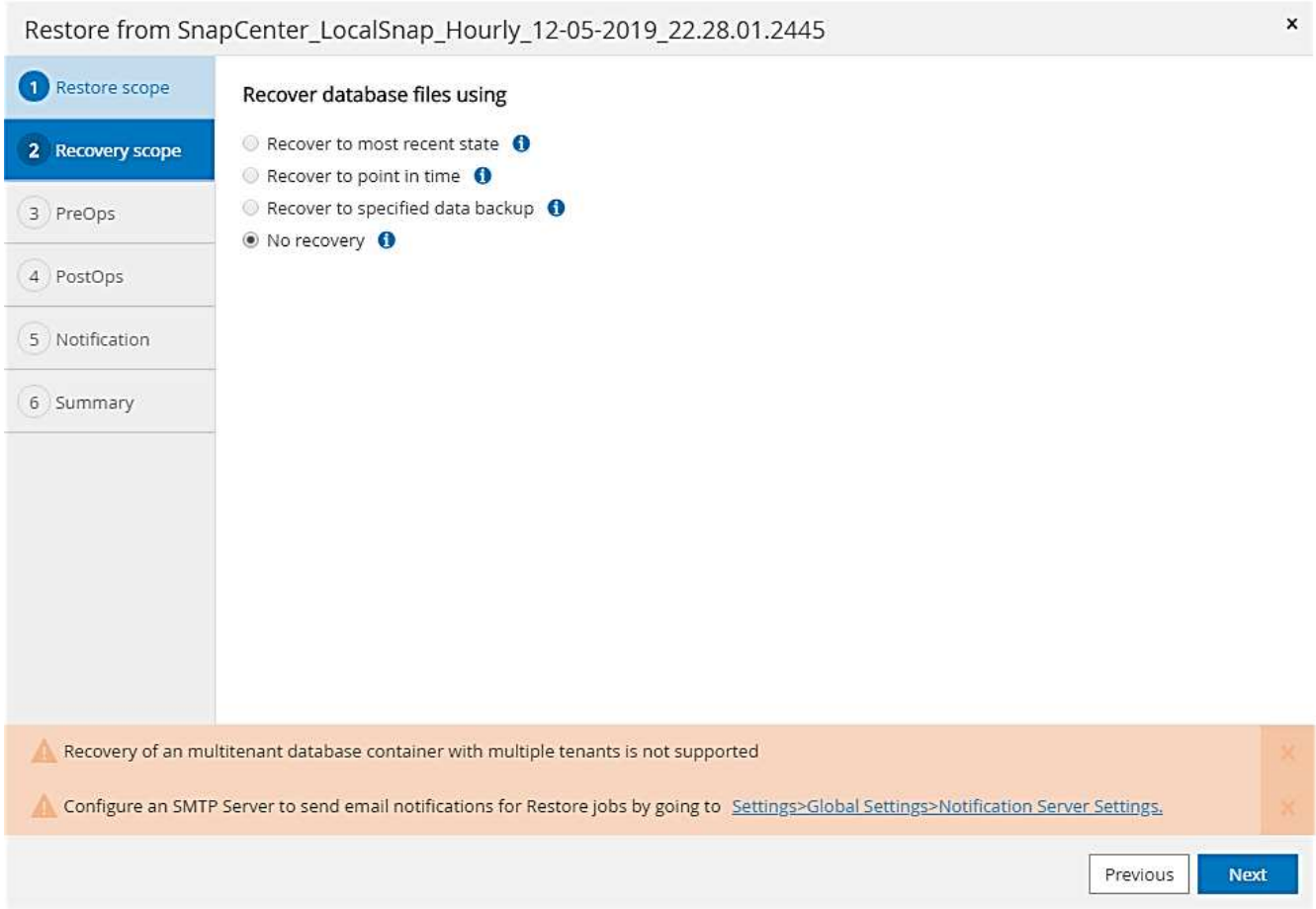


3. Selezionare il tenant da ripristinare.

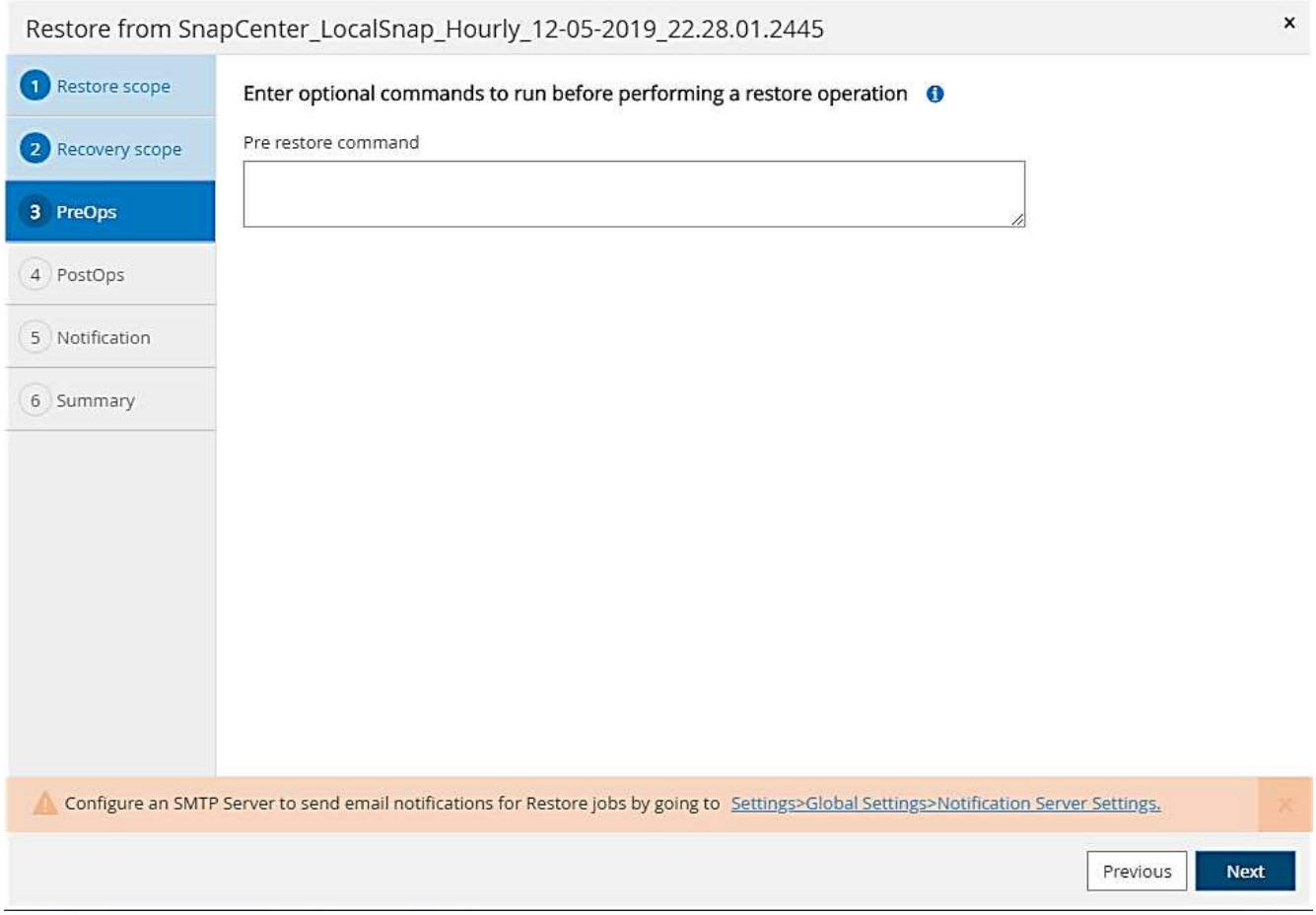
SnapCenter mostra un elenco di tutti i tenant inclusi nel backup selezionato.



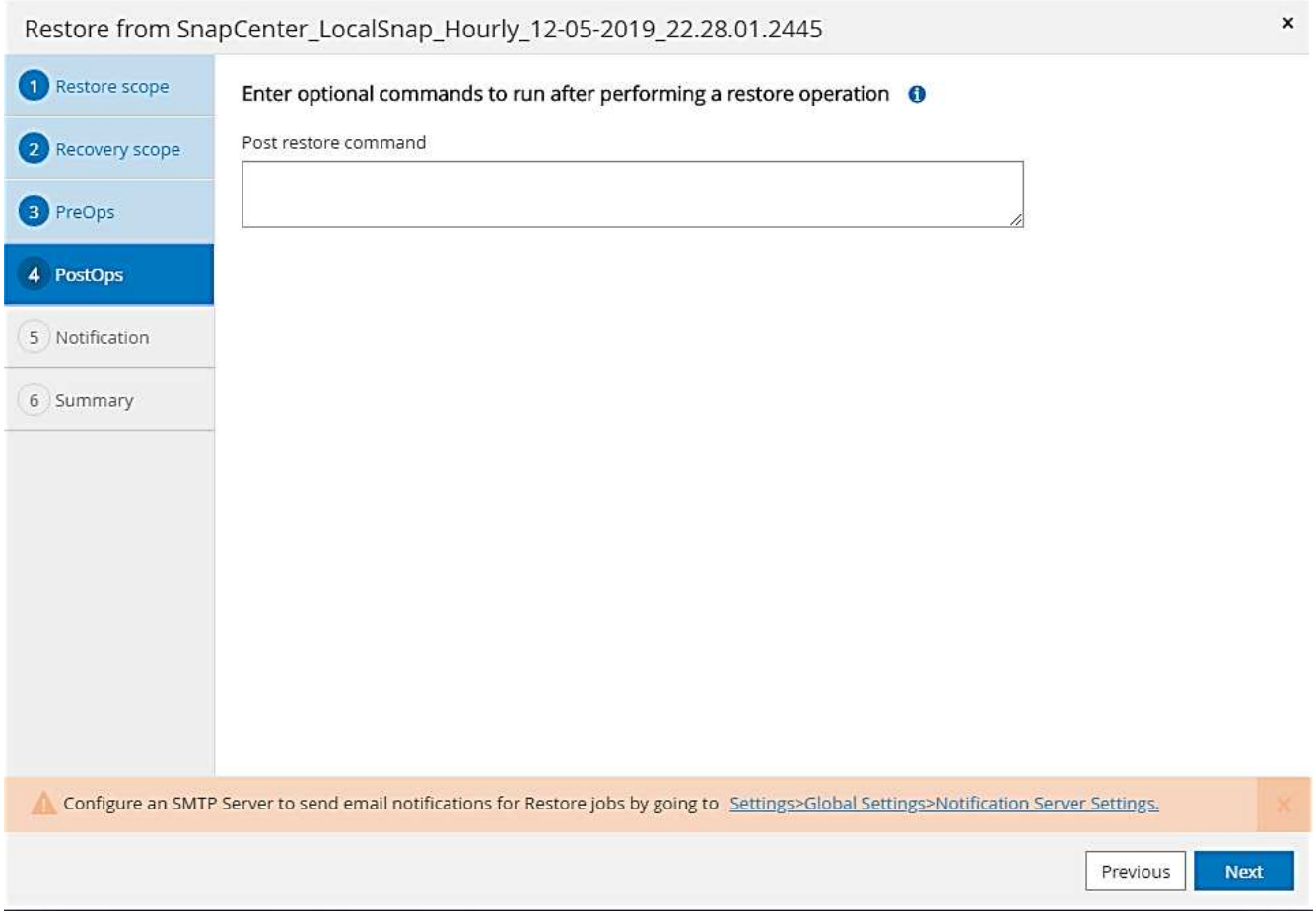
Il ripristino single-tenant non è supportato con SnapCenter 4.3. Nessun ripristino preselezionato e non modificabile.



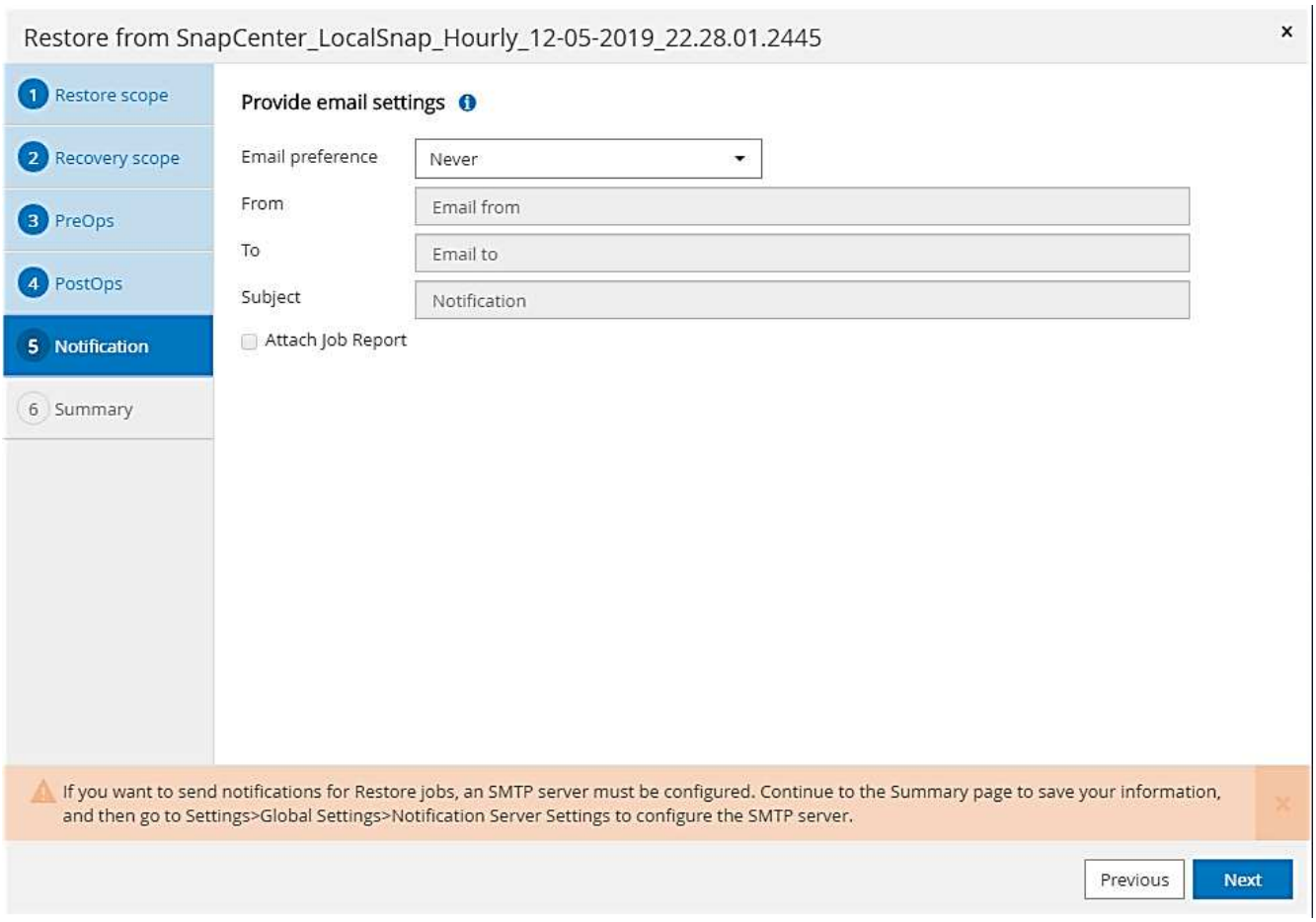
4. Immettere i comandi opzionali di prerestore.



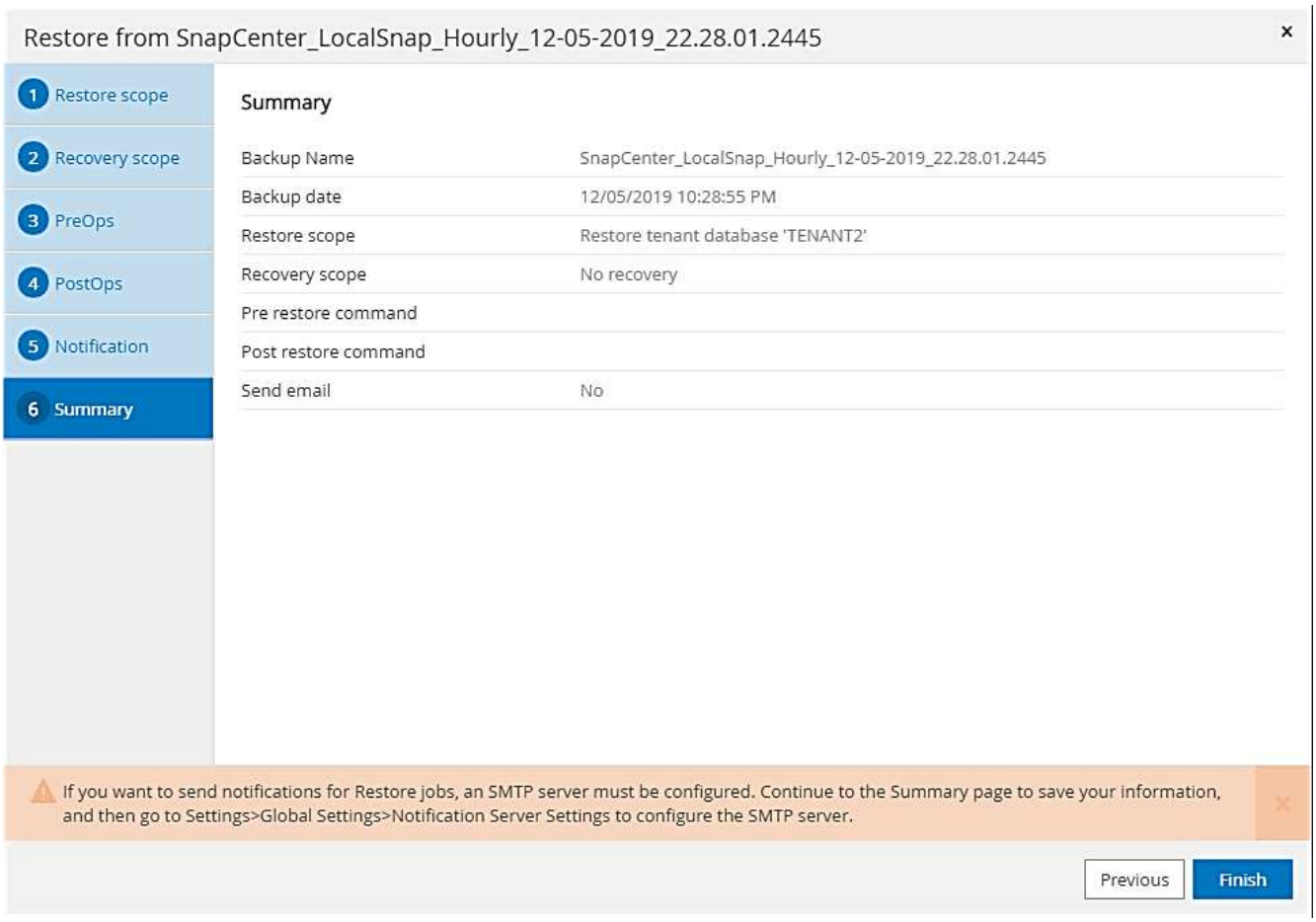
5. Immettere comandi post-ripristino opzionali.



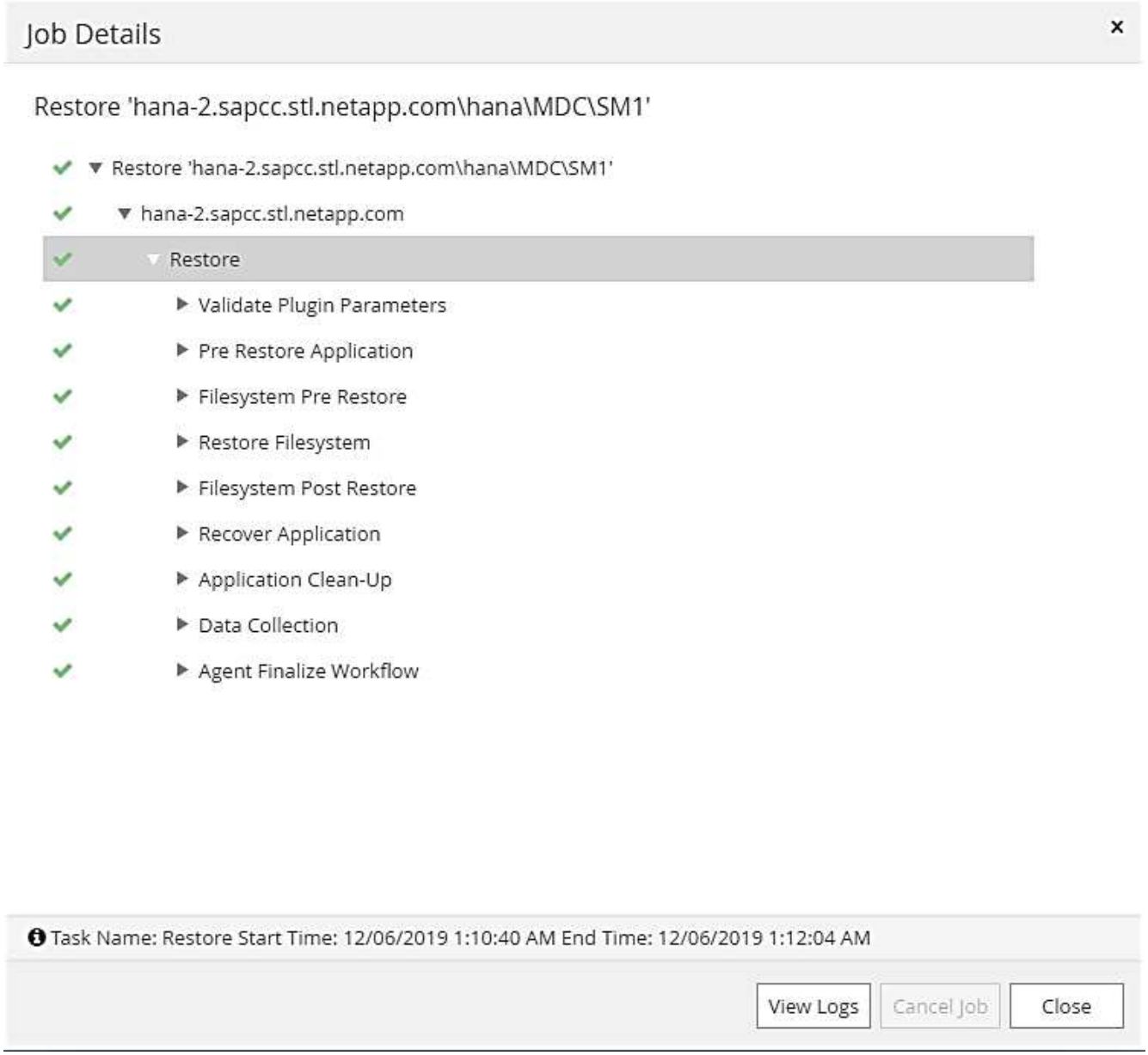
6. Immettere le impostazioni e-mail opzionali.



7. Per avviare l’operazione di ripristino, fare clic su fine.



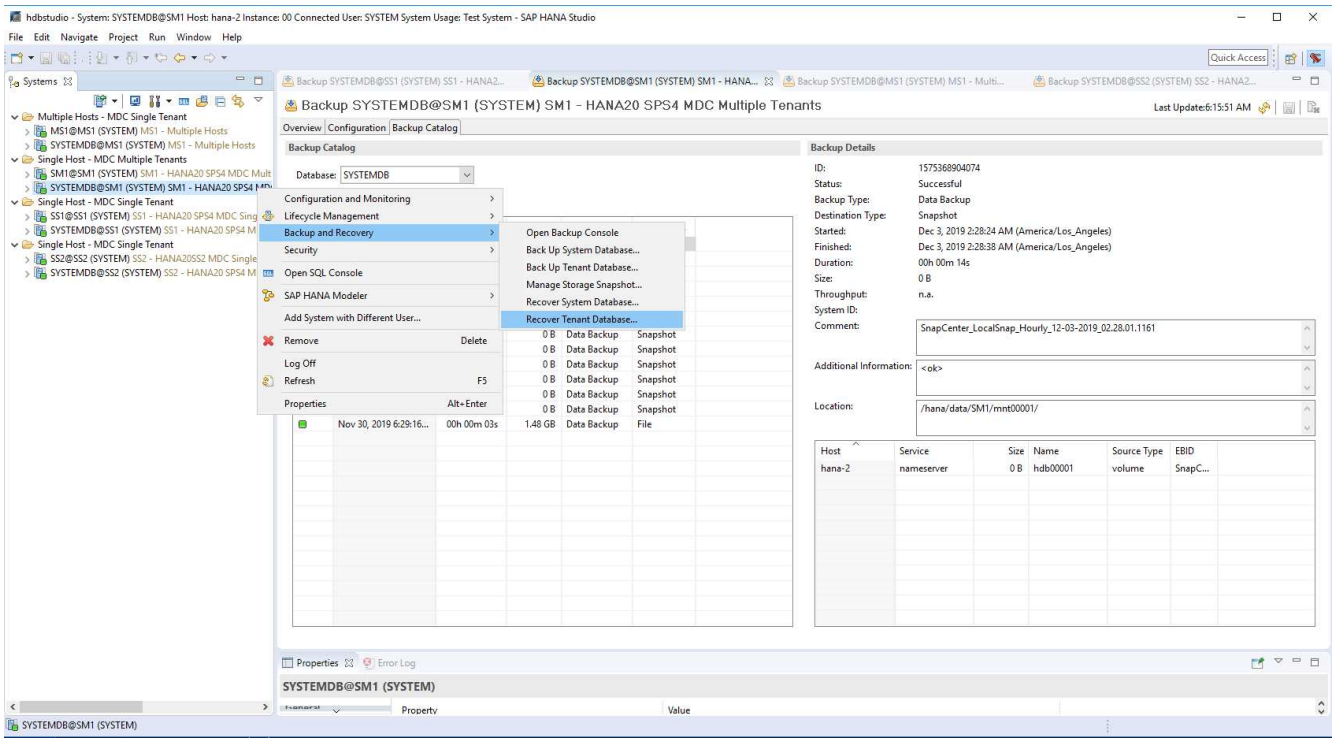
L'operazione di ripristino viene eseguita da SnapCenter. Questo esempio mostra i dettagli del lavoro di ripristino.



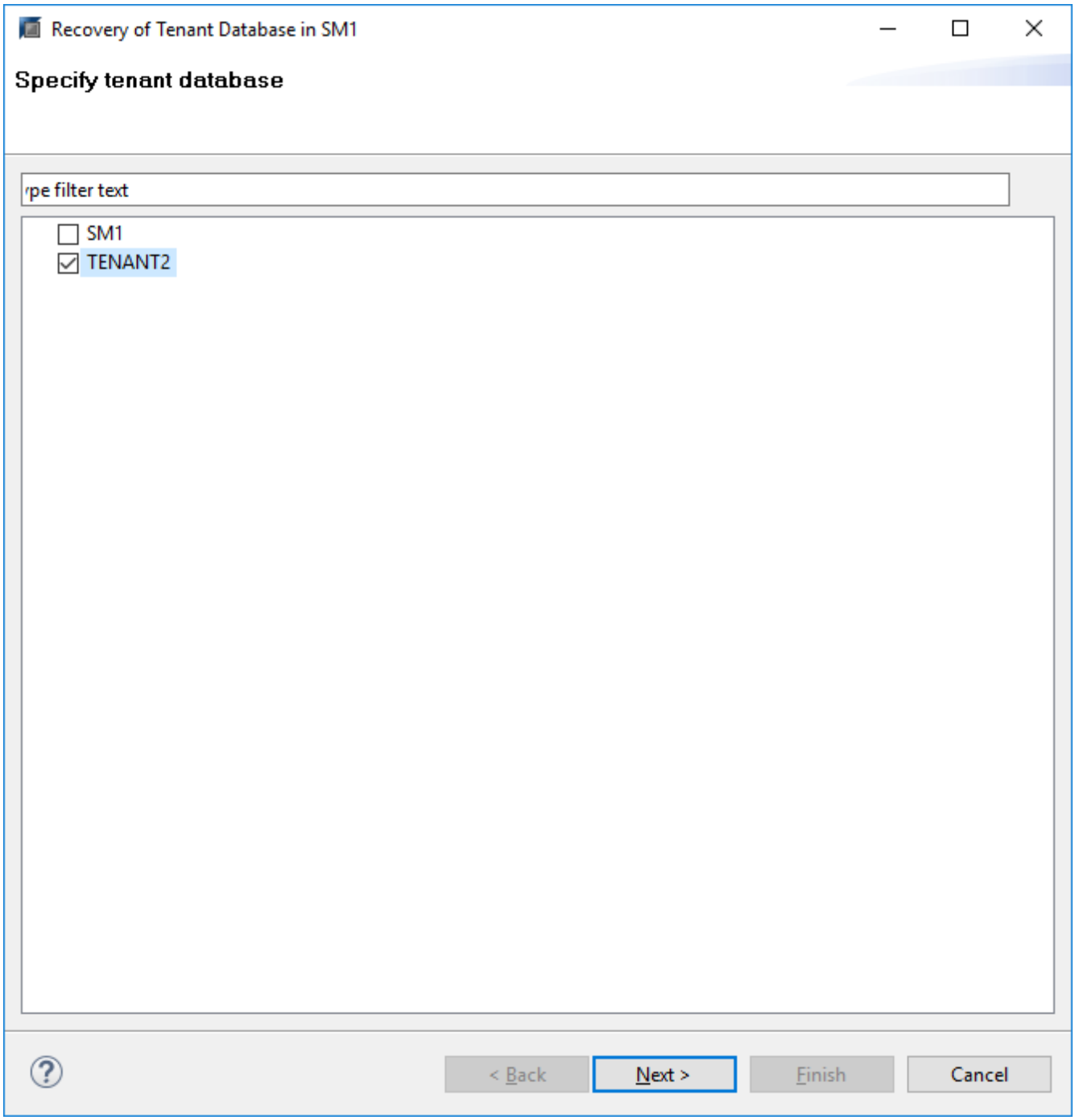
Al termine dell'operazione di ripristino del tenant, vengono ripristinati solo i dati rilevanti del tenant. Sul file system dell'host del database HANA, sono disponibili il file di dati ripristinato e il file ID di backup Snapshot del tenant.

```
sm1adm@hana-2:/usr/sap/SM1/HDB00> ls -al /hana/data/SM1/mnt00001/*
-rw-r--r-- 1 sm1adm sapsys   17 Dec  6 04:01
/hana/data/SM1/mnt00001/nameserver.lck
/hana/data/SM1/mnt00001/hdb00001:
total 3417776
drwxr-x--- 2 sm1adm sapsys       4096 Dec  6 01:14 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r----- 1 sm1adm sapsys 3758096384 Dec  6 03:59 datavolume_0000.dat
-rw-r----- 1 sm1adm sapsys          0 Nov 20 08:36
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 sm1adm sapsys         36 Nov 20 08:37 landscape.id
/hana/data/SM1/mnt00001/hdb00002.00003:
total 67772
drwxr-xr-- 2 sm1adm sapsys      4096 Nov 20 08:37 .
drwxr-x--- 6 sm1adm sapsys      4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 201441280 Dec  6 03:59 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys         0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
/hana/data/SM1/mnt00001/hdb00002.00004:
total 3411836
drwxr-xr-- 2 sm1adm sapsys       4096 Dec  6 03:57 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 3758096384 Dec  6 01:14 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys          0 Nov 20 09:35
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
-rw-r----- 1 sm1adm sapsys     155648 Dec  6 01:14
snapshot_databackup_0_1
/hana/data/SM1/mnt00001/hdb00003.00003:
total 3364216
drwxr-xr-- 2 sm1adm sapsys       4096 Dec  6 01:14 .
drwxr-x--- 6 sm1adm sapsys       4096 Nov 20 09:35 ..
-rw-r--r-- 1 sm1adm sapsys 3758096384 Dec  6 03:59 datavolume_0000.dat
-rw-r--r-- 1 sm1adm sapsys          0 Nov 20 08:37
__DO_NOT_TOUCH_FILES_IN_THIS_DIRECTORY__
sm1adm@hana-2:/usr/sap/SM1/HDB00>
```

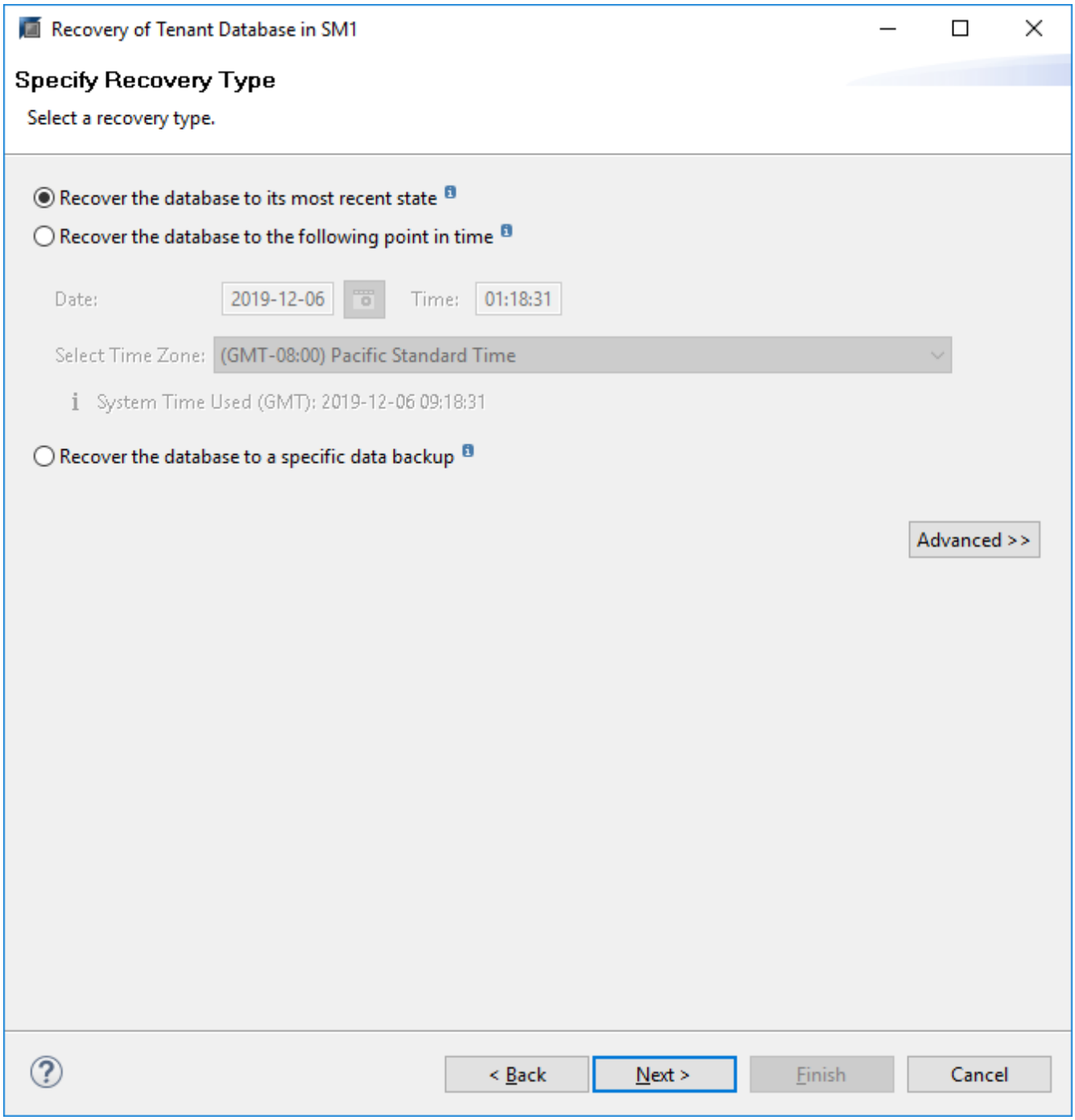
8. Avviare il ripristino con HANA Studio.



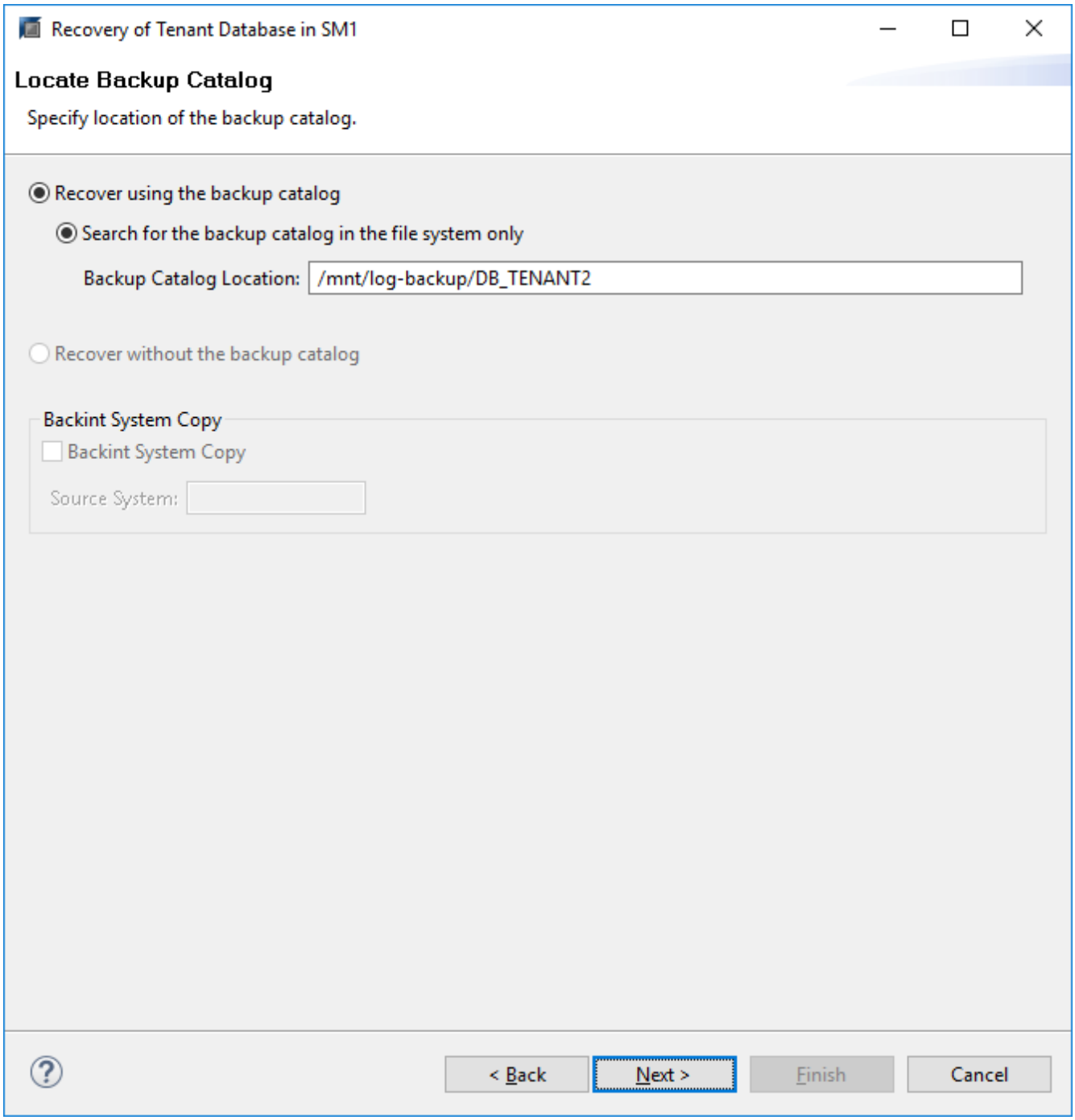
9. Selezionare il tenant.

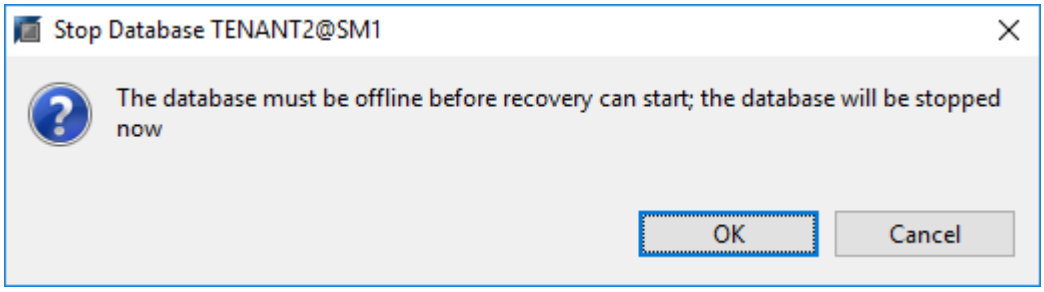


10. Selezionare il tipo di ripristino.



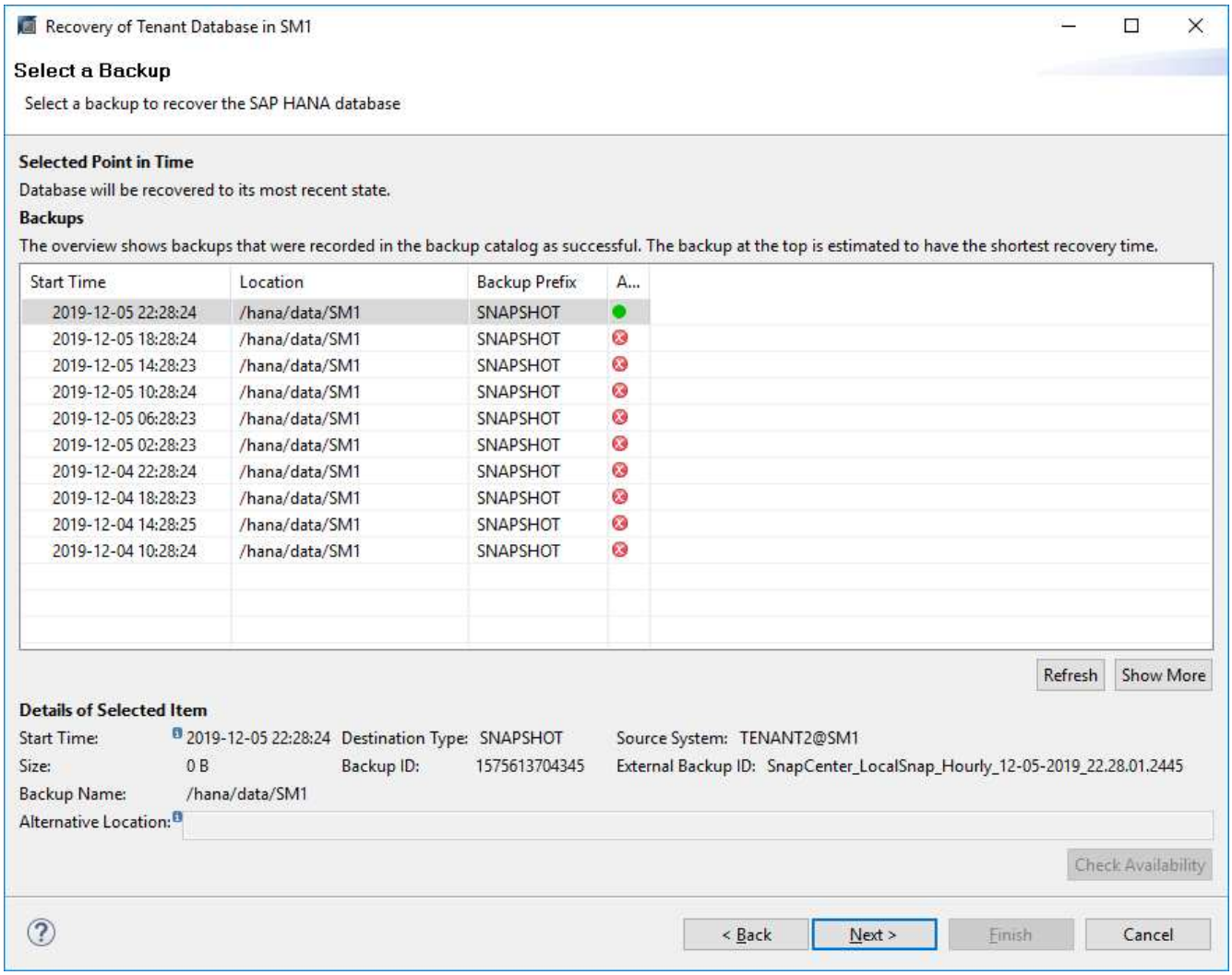
11. Fornire la posizione del catalogo di backup.



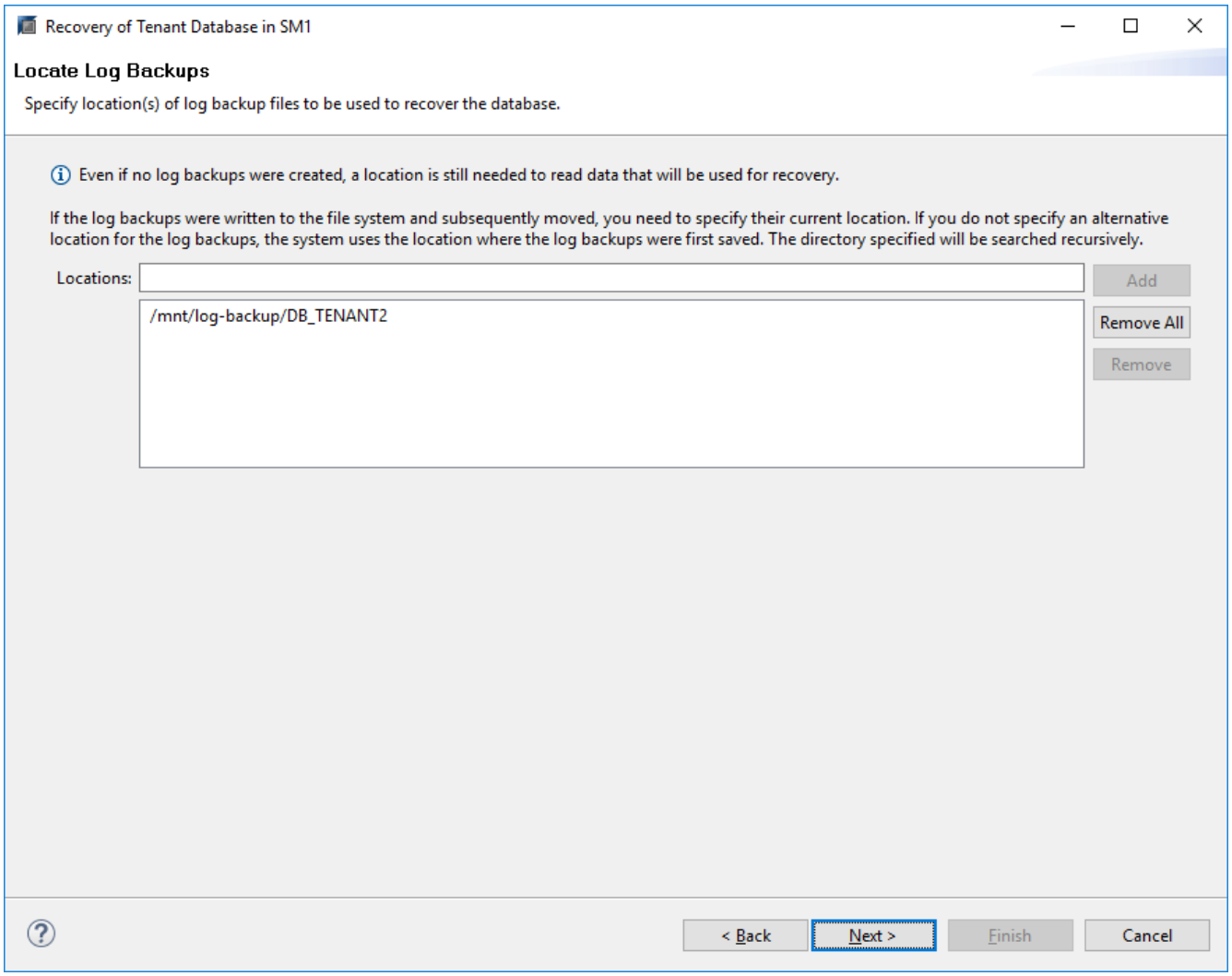


All'interno del catalogo di backup, il backup ripristinato viene evidenziato con un'icona verde. L'ID del backup esterno mostra il nome del backup precedentemente selezionato in SnapCenter.

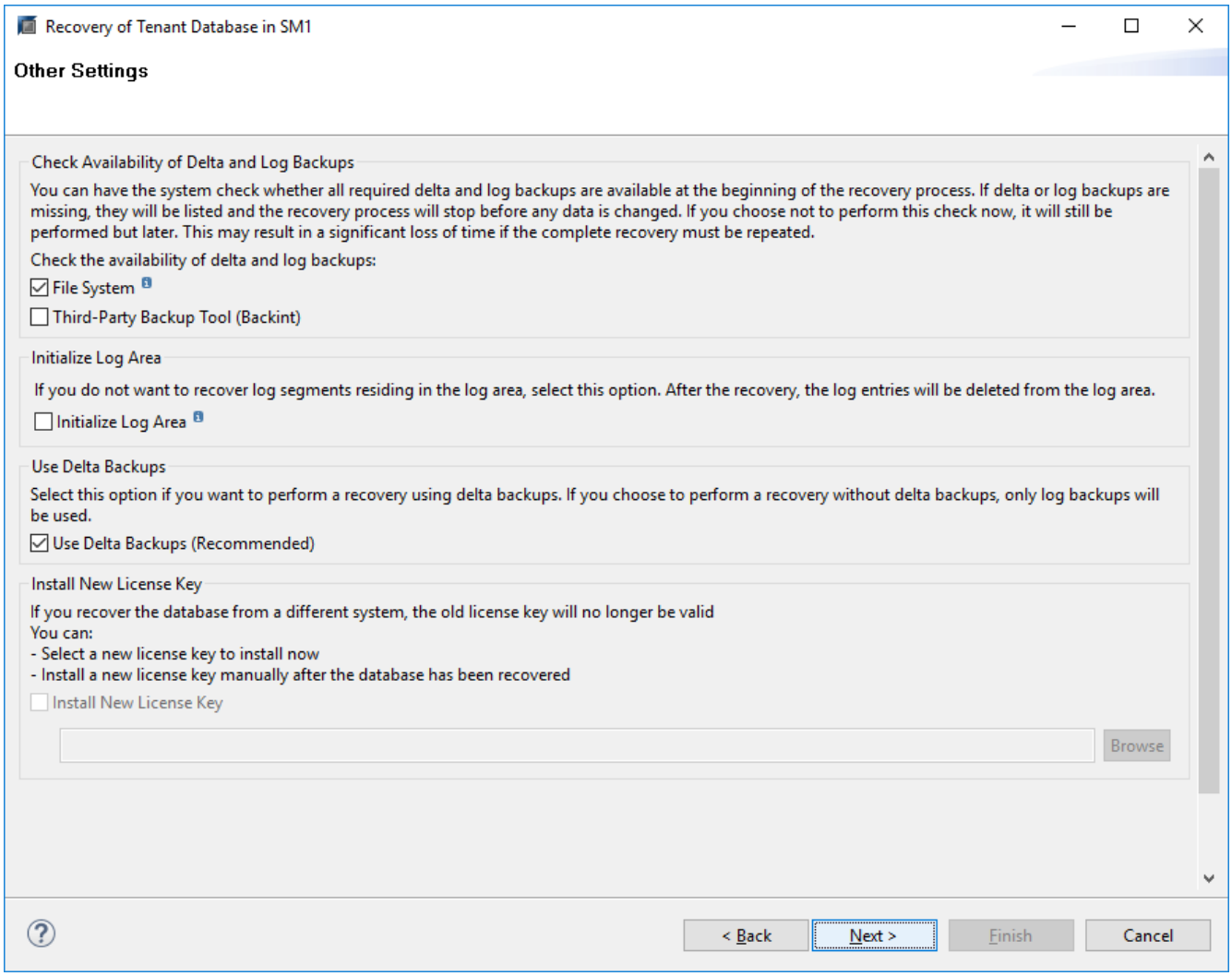
12. Selezionare la voce con l'icona verde e fare clic su Next (Avanti).



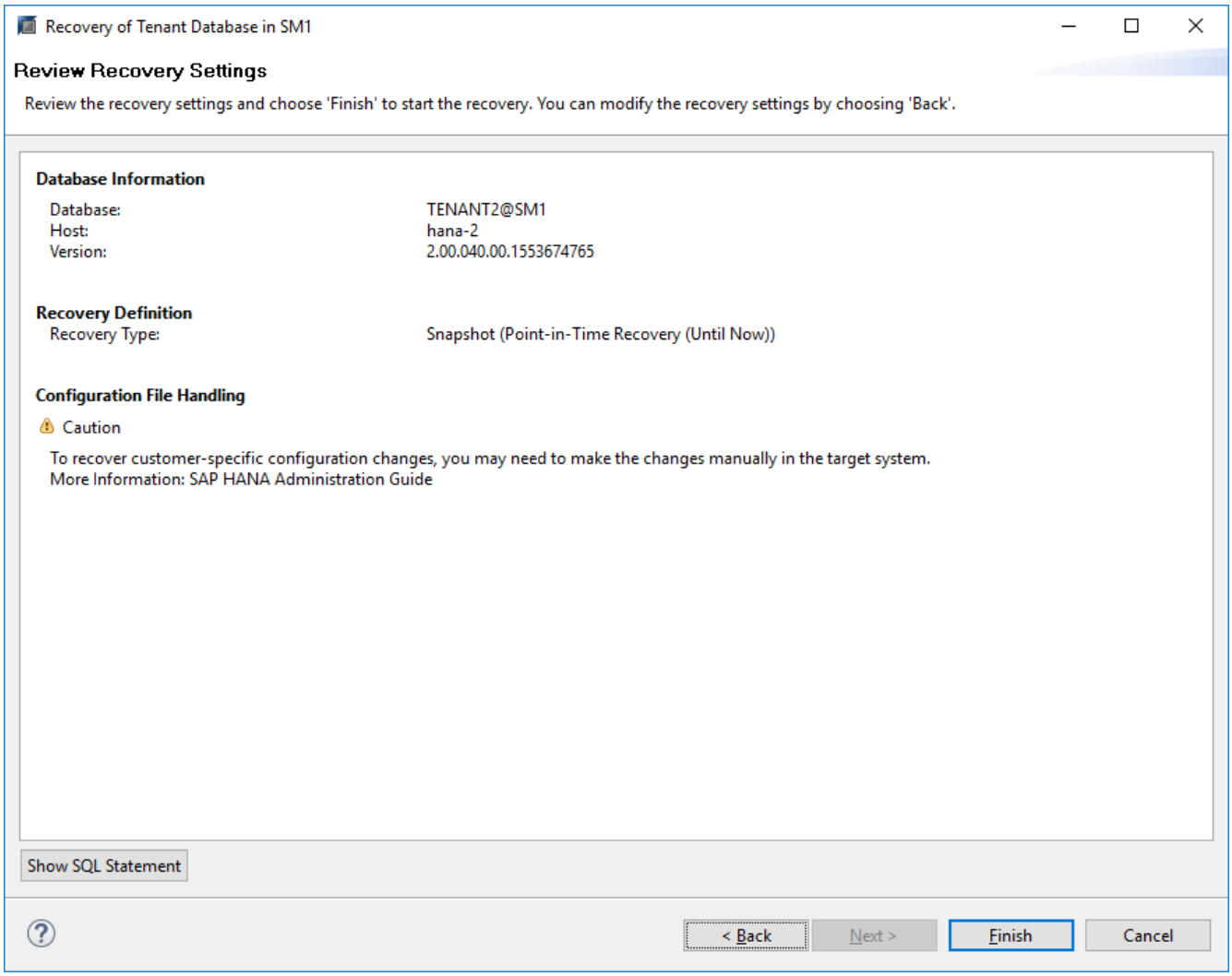
13. Fornire la posizione di backup del registro.

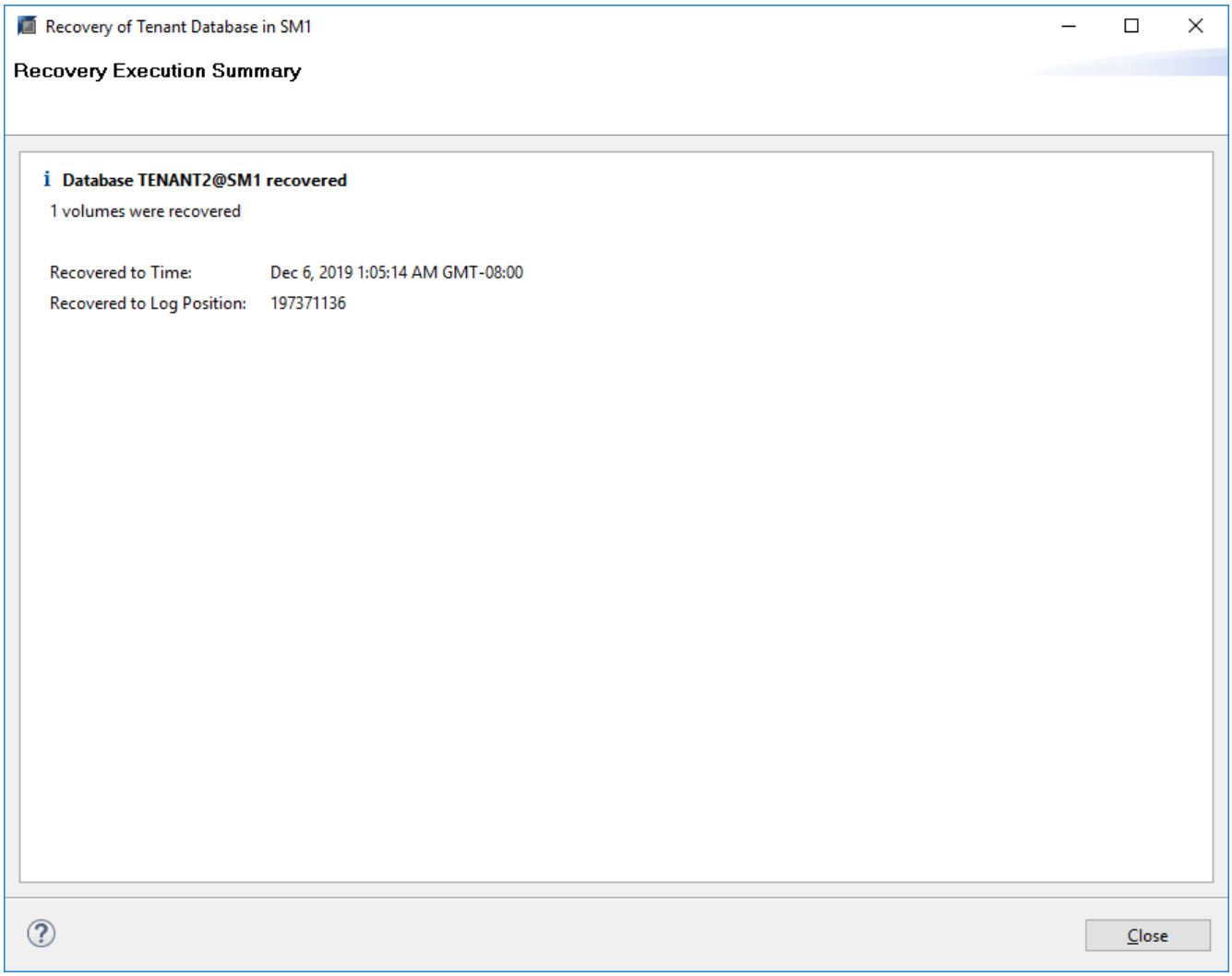


14. Selezionare le altre impostazioni desiderate.



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



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.

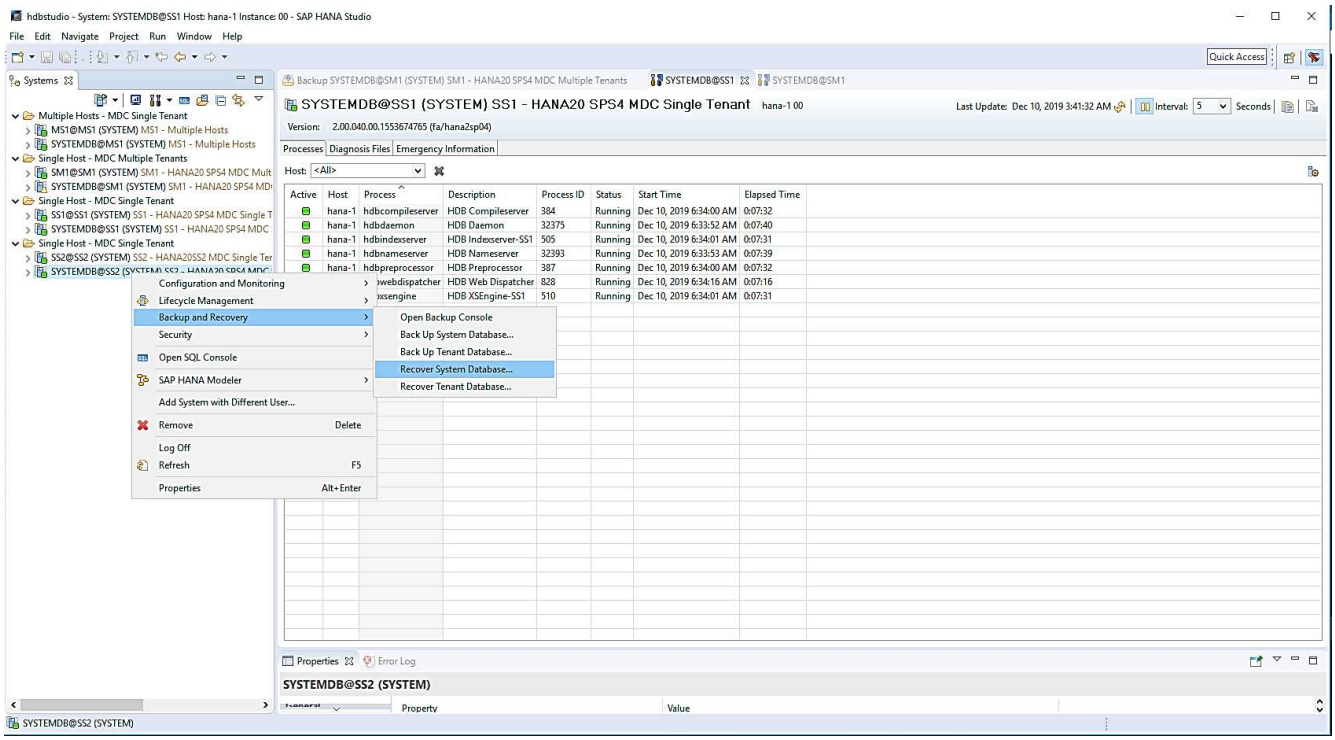
3. Eseguire il processo di ripristino del database di sistema con SAP HANA Studio:
   a. Fare clic su Refresh (Aggiorna) dall'elenco dei backup e selezionare il backup disponibile per il ripristino (indicato da un'icona verde).
   b. Avviare il processo di ripristino. Al termine del processo di ripristino, viene avviato il database di sistema.
4. Eseguire il processo di ripristino del database tenant con SAP HANA Studio:
   a. Selezionare Recover tenant Database (Ripristina database tenant) e selezionare il tenant da ripristinare.
   b. 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).

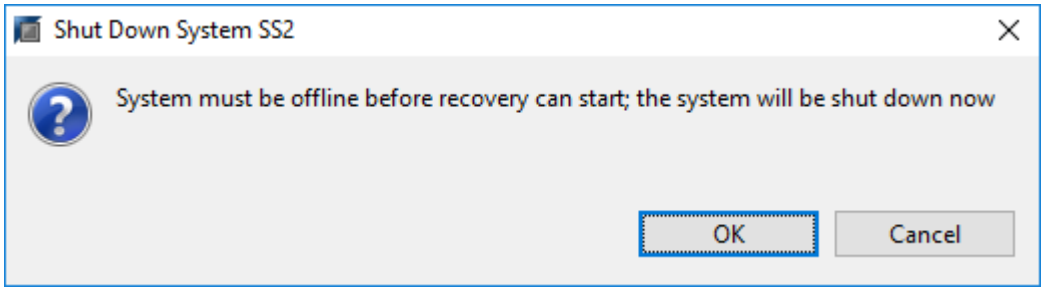
   c. Selezionare questo backup e avviare il processo di ripristino. Al termine del processo di ripristino, il database del tenant viene avviato automaticamente.

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.

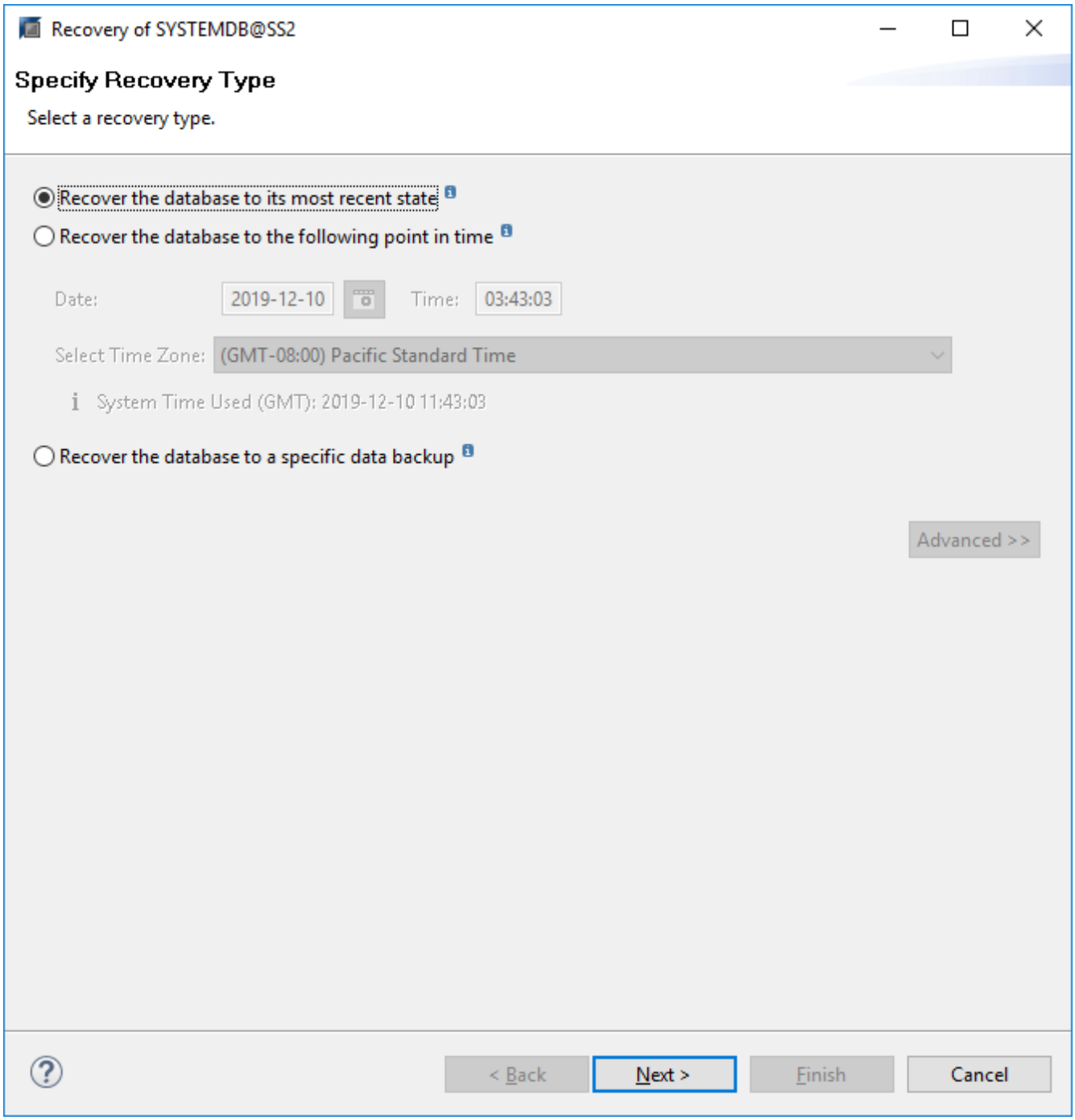


2. Fare clic su OK per chiudere il database SAP HANA.

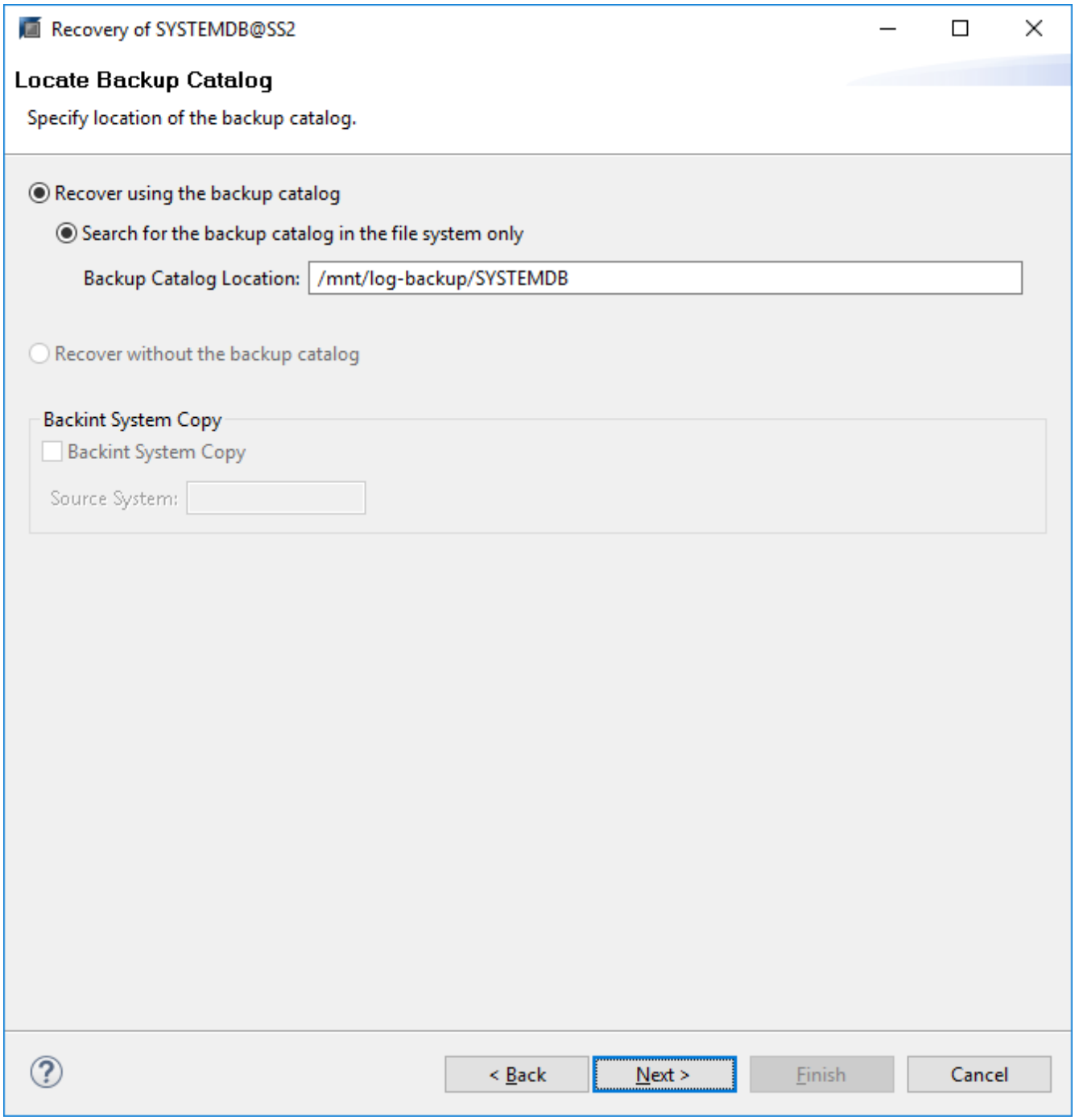


Il sistema SAP HANA si spegne e viene avviata la procedura guidata di ripristino.

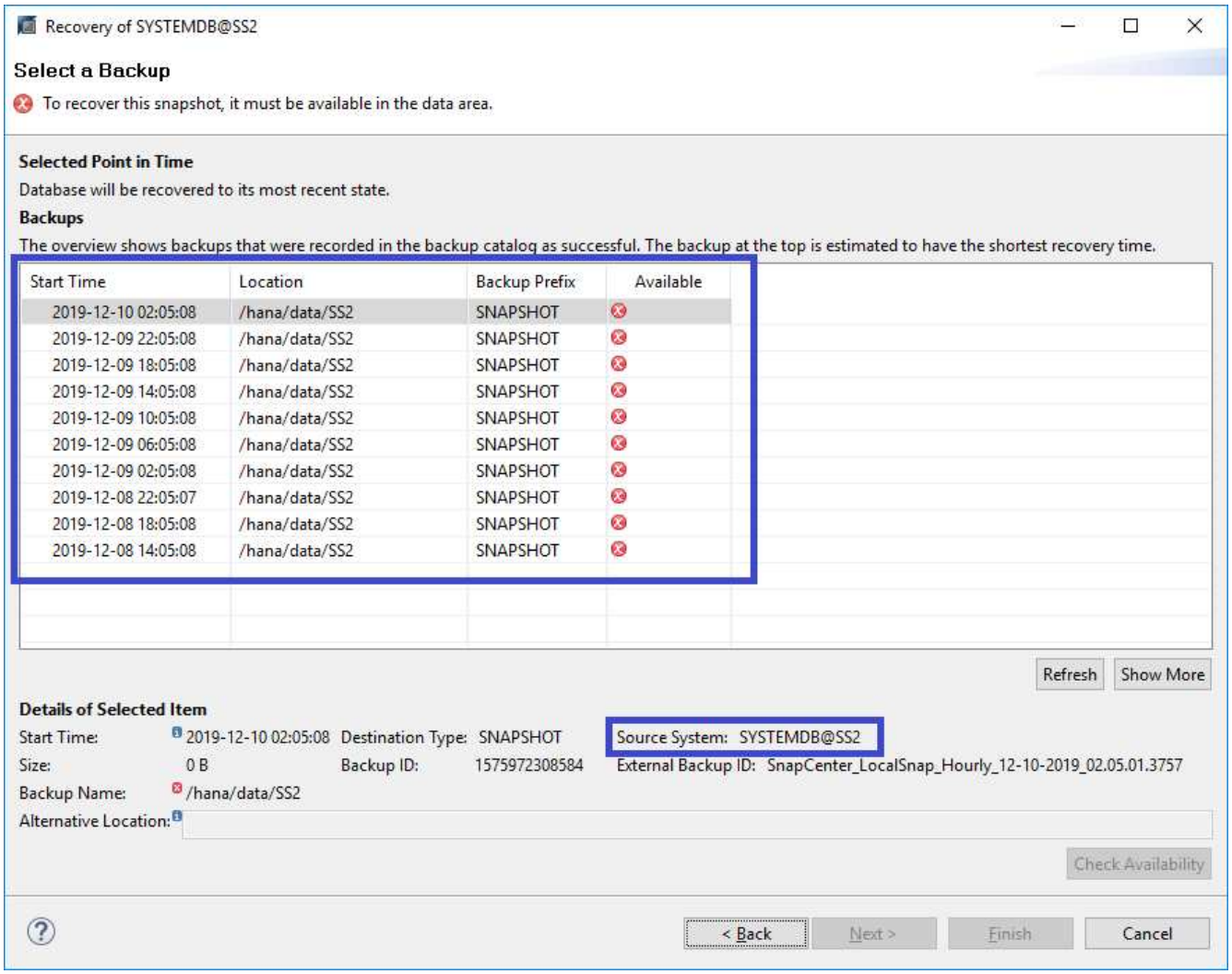
3. Selezionare il tipo di ripristino e fare clic su Next (Avanti).



4. Fornire la posizione del catalogo di backup e fare clic su Next (Avanti).



5. 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.



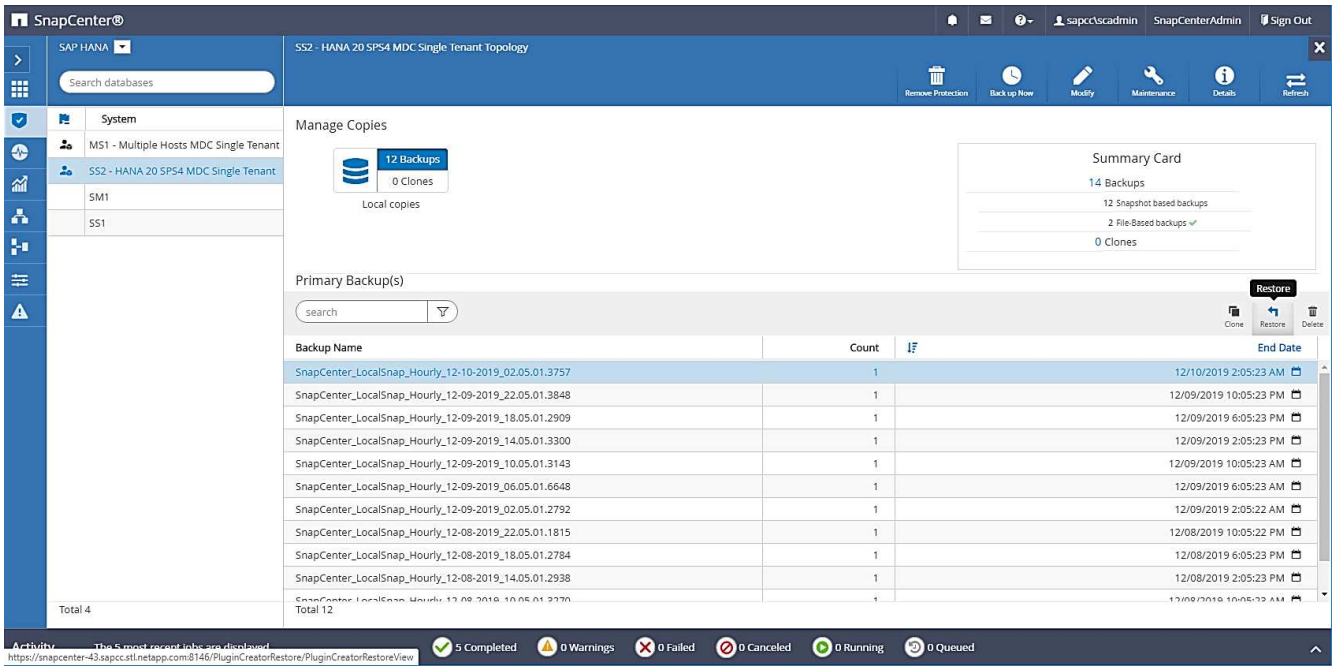
6. Smontare tutti i volumi di dati.

```
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.

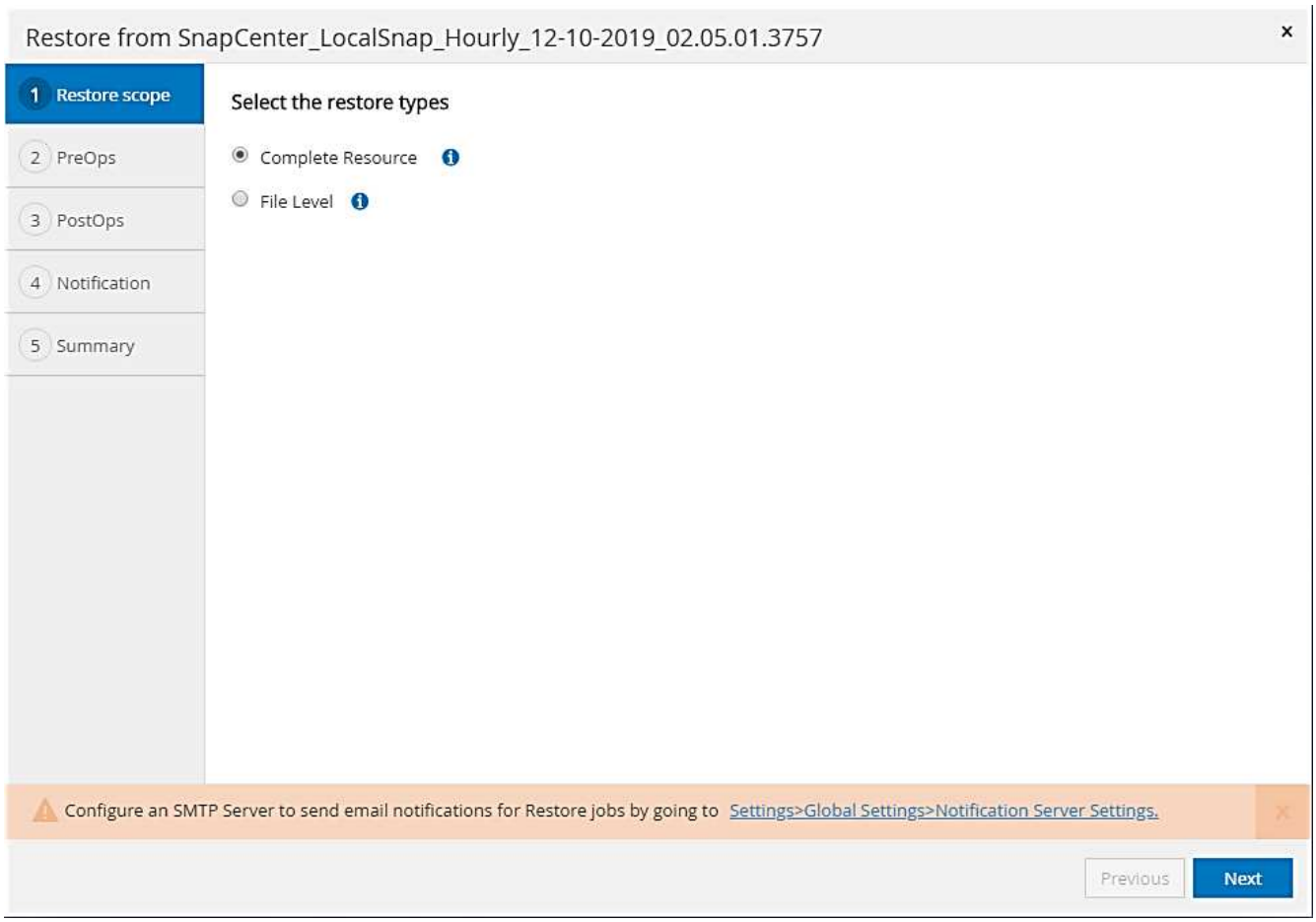
7. Dalla GUI di SnapCenter, selezionare la vista della topologia delle risorse e selezionare il backup da ripristinare; nel nostro esempio, il backup primario più recente. Fare clic sull'icona Restore (Ripristina) per avviare il ripristino.



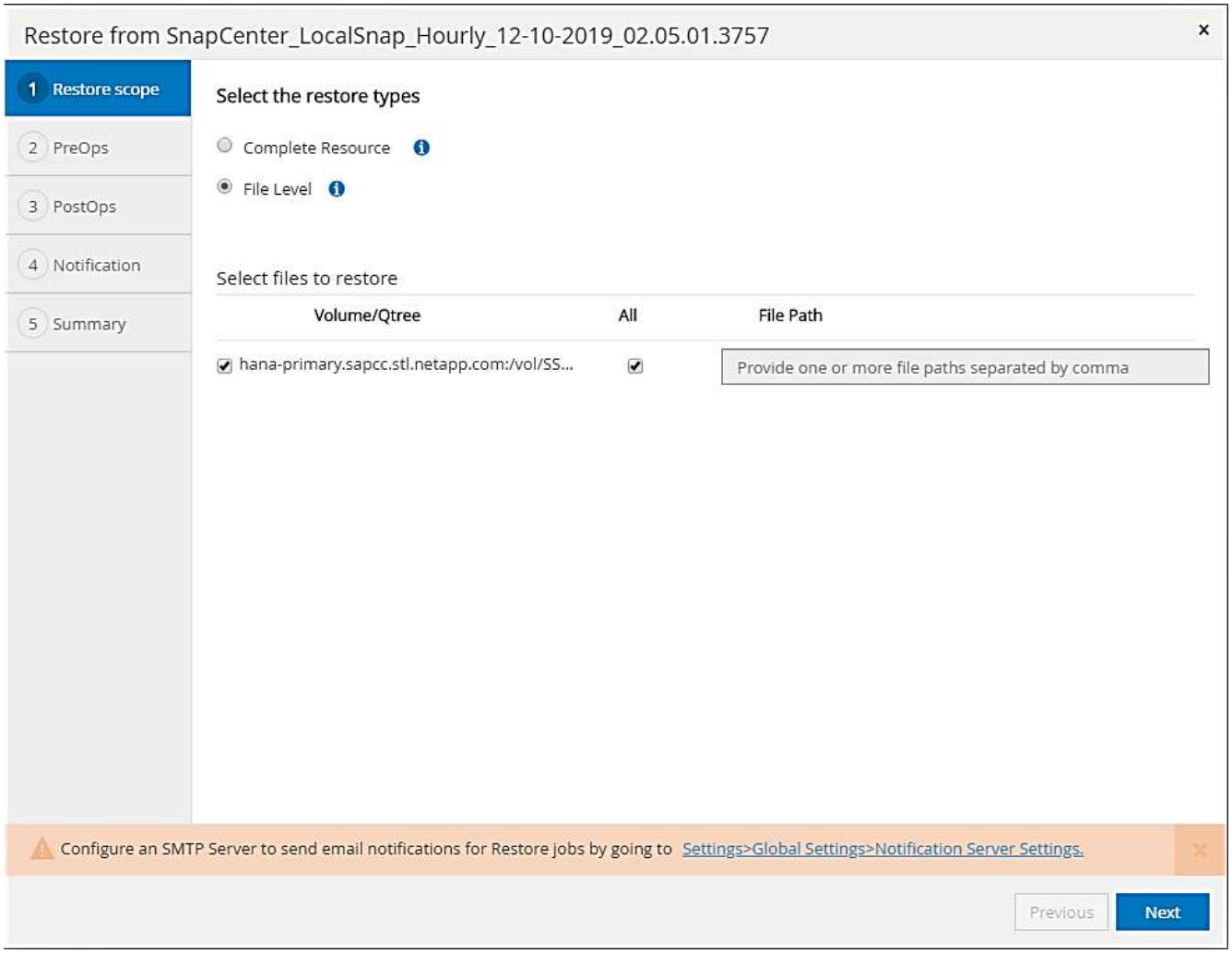
Viene avviata la procedura guidata di ripristino di SnapCenter.

8. Selezionare il tipo di ripristino complete Resource (risorsa completa) o file Level (livello file).

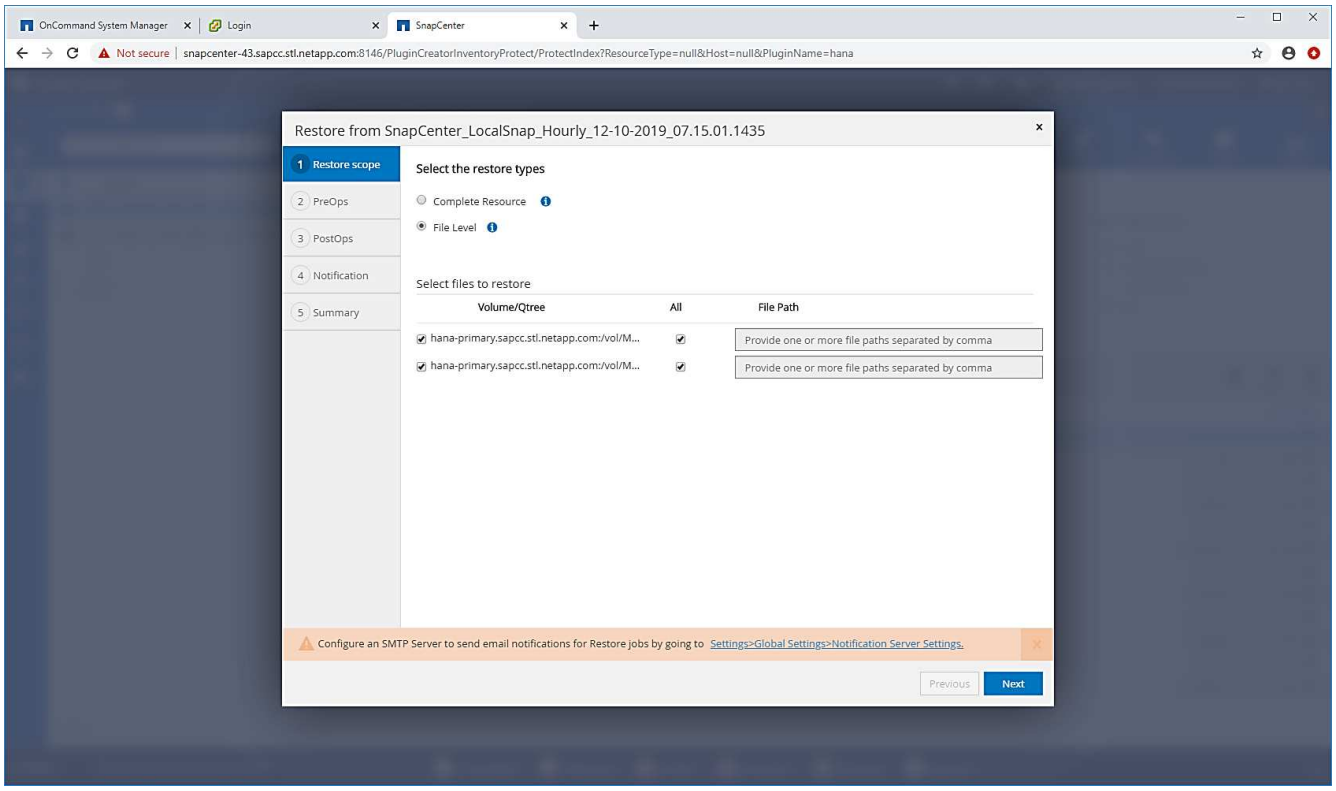
   Selezionare completa risorsa per utilizzare un ripristino basato su volume.



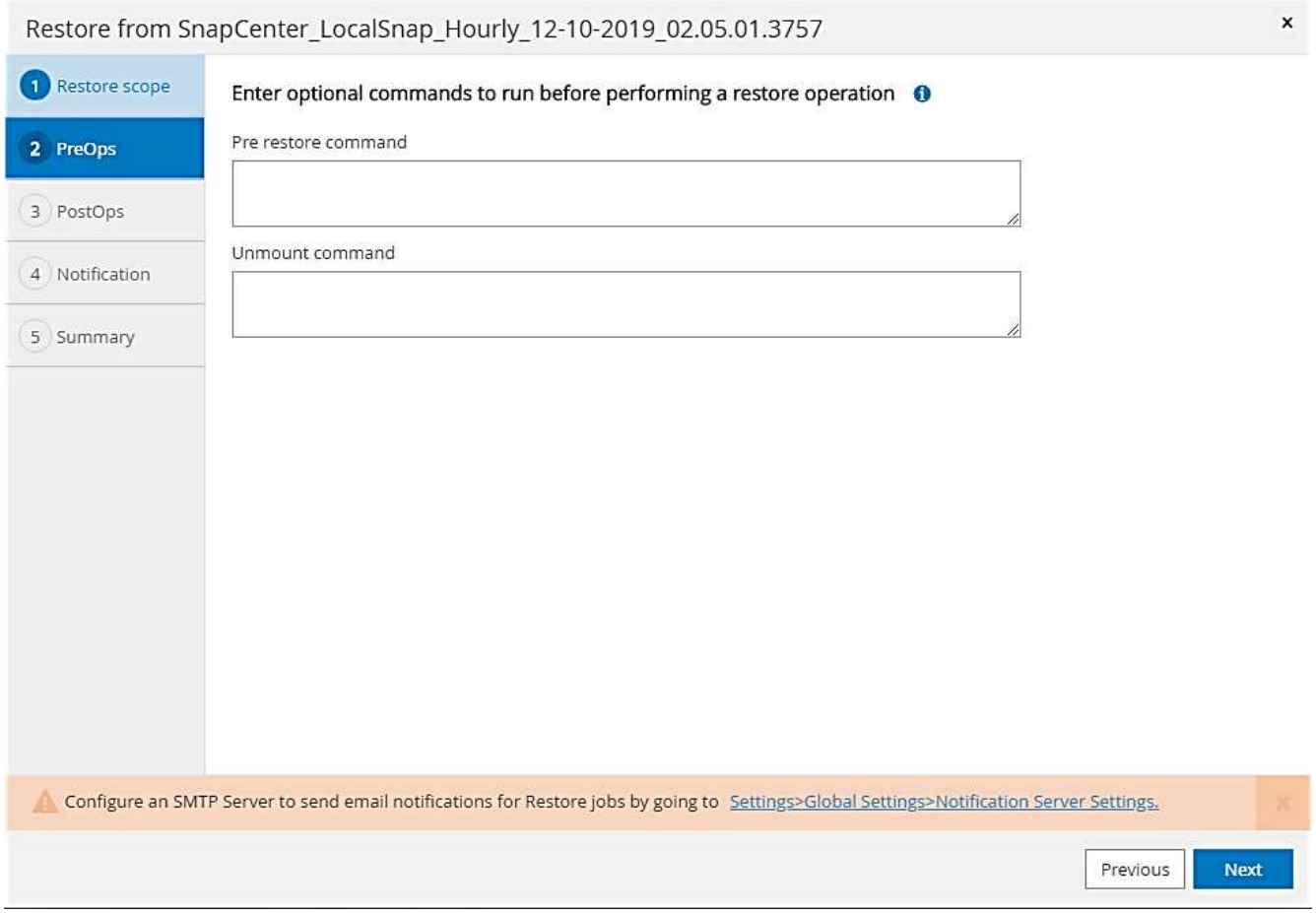
9. Selezionare livello file e tutto per utilizzare un'operazione SnapRestore a file singolo per tutti i file.



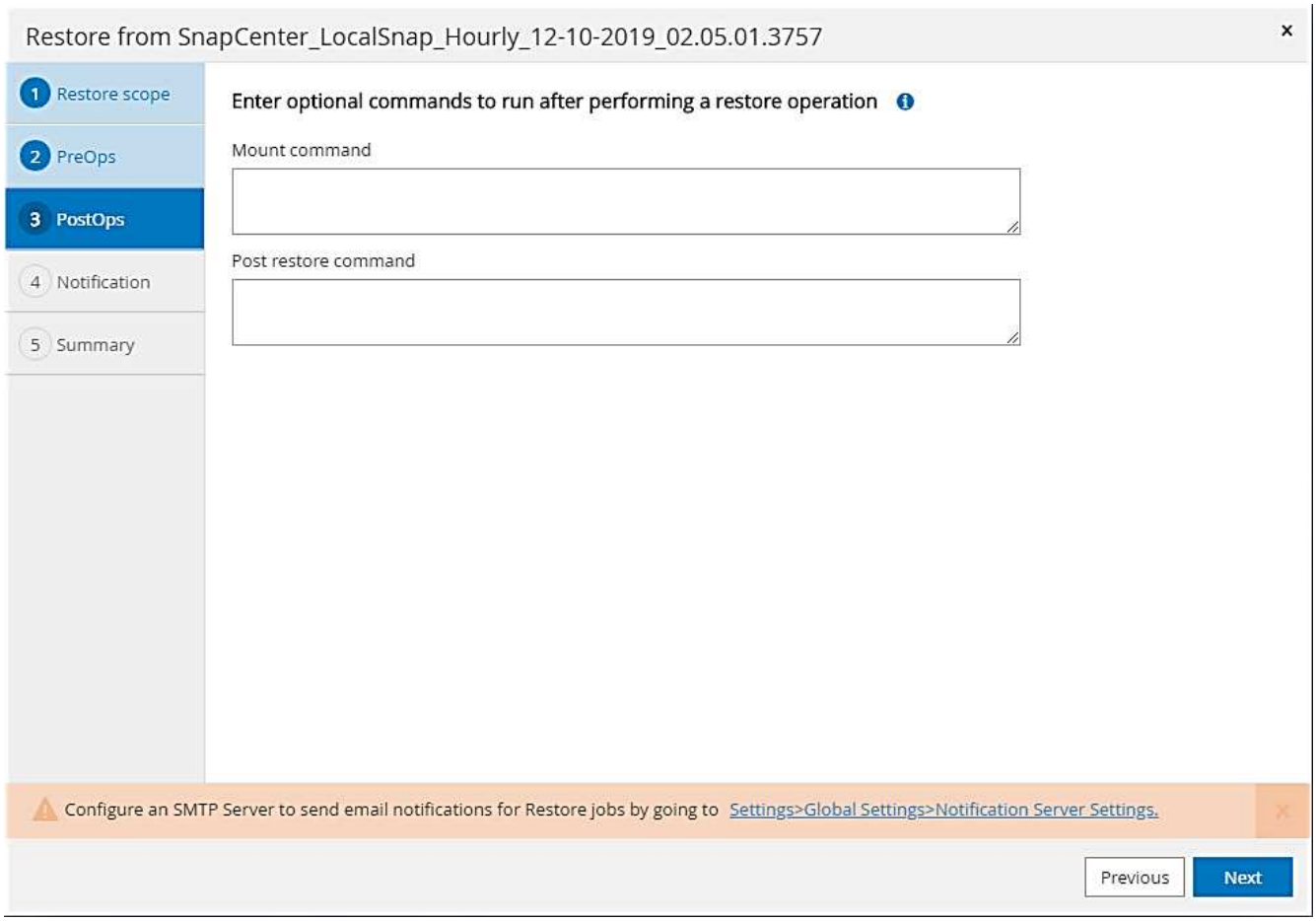
Per un ripristino a livello di file di un sistema host multiplo SAP HANA, selezionare tutti i volumi.



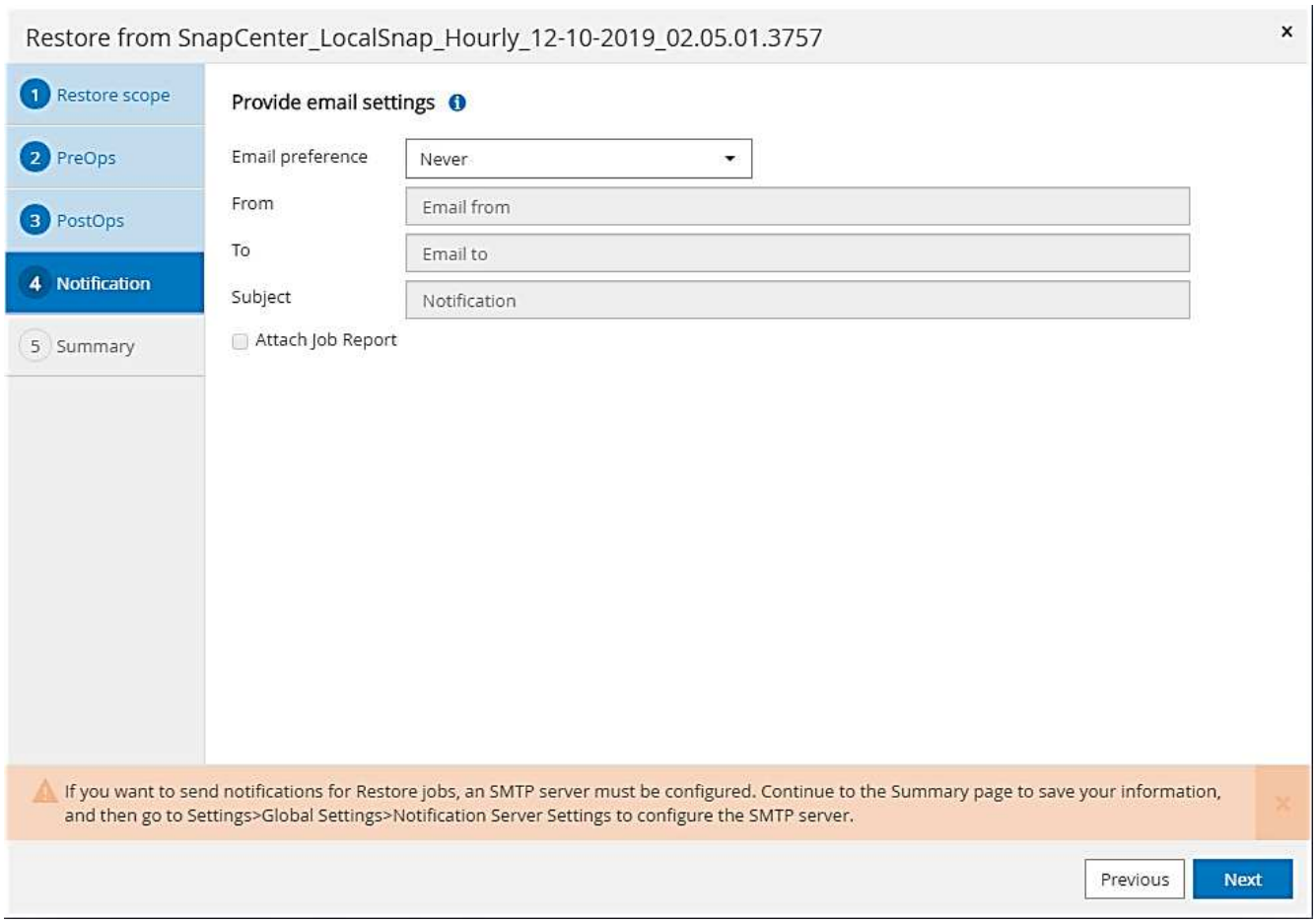
10. (Facoltativo) specificare i comandi da eseguire dal plug-in SAP HANA in esecuzione sull'host del plug-in HANA centrale. Fare clic su Avanti.



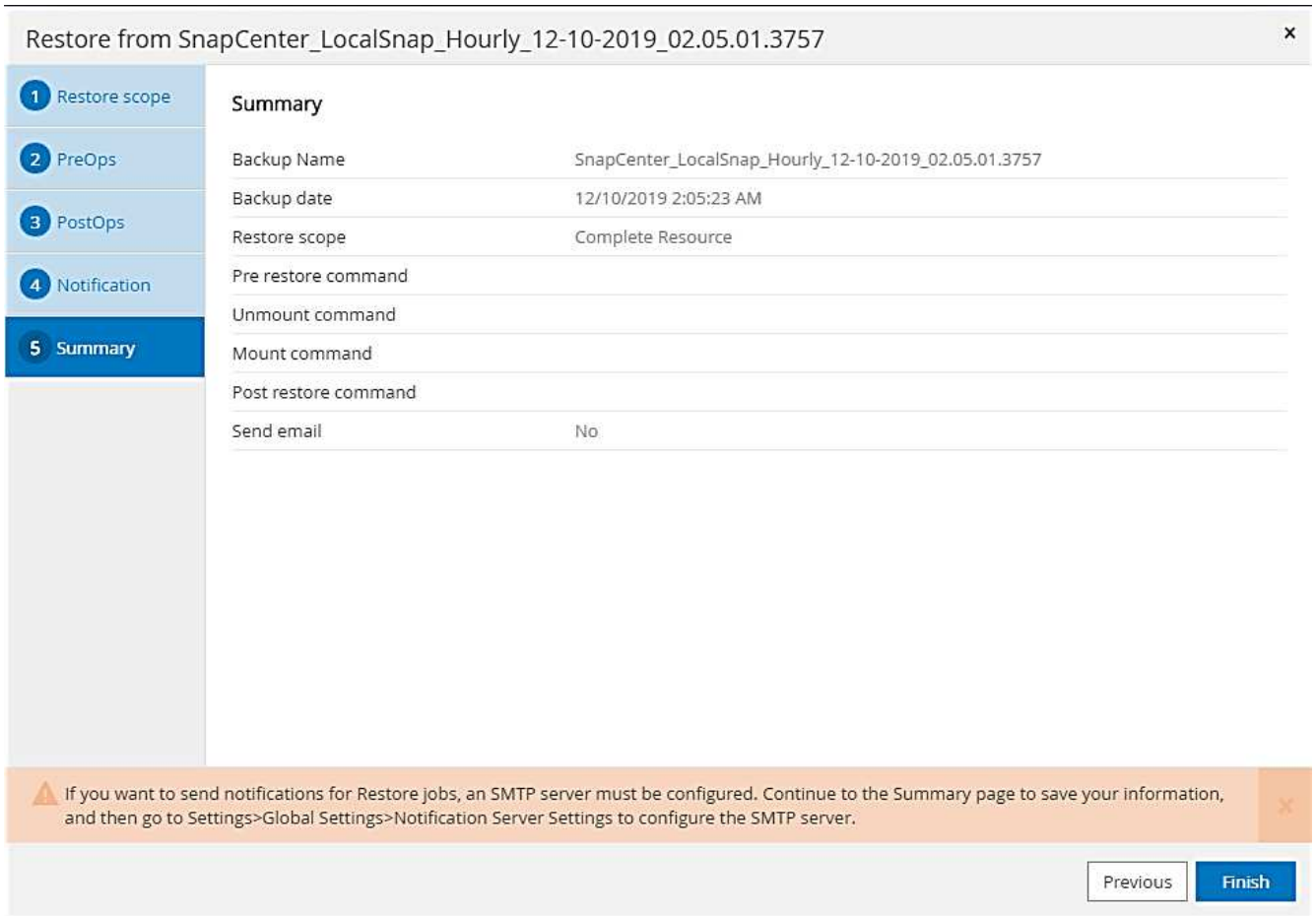
11. Specificare i comandi opzionali e fare clic su Next (Avanti).



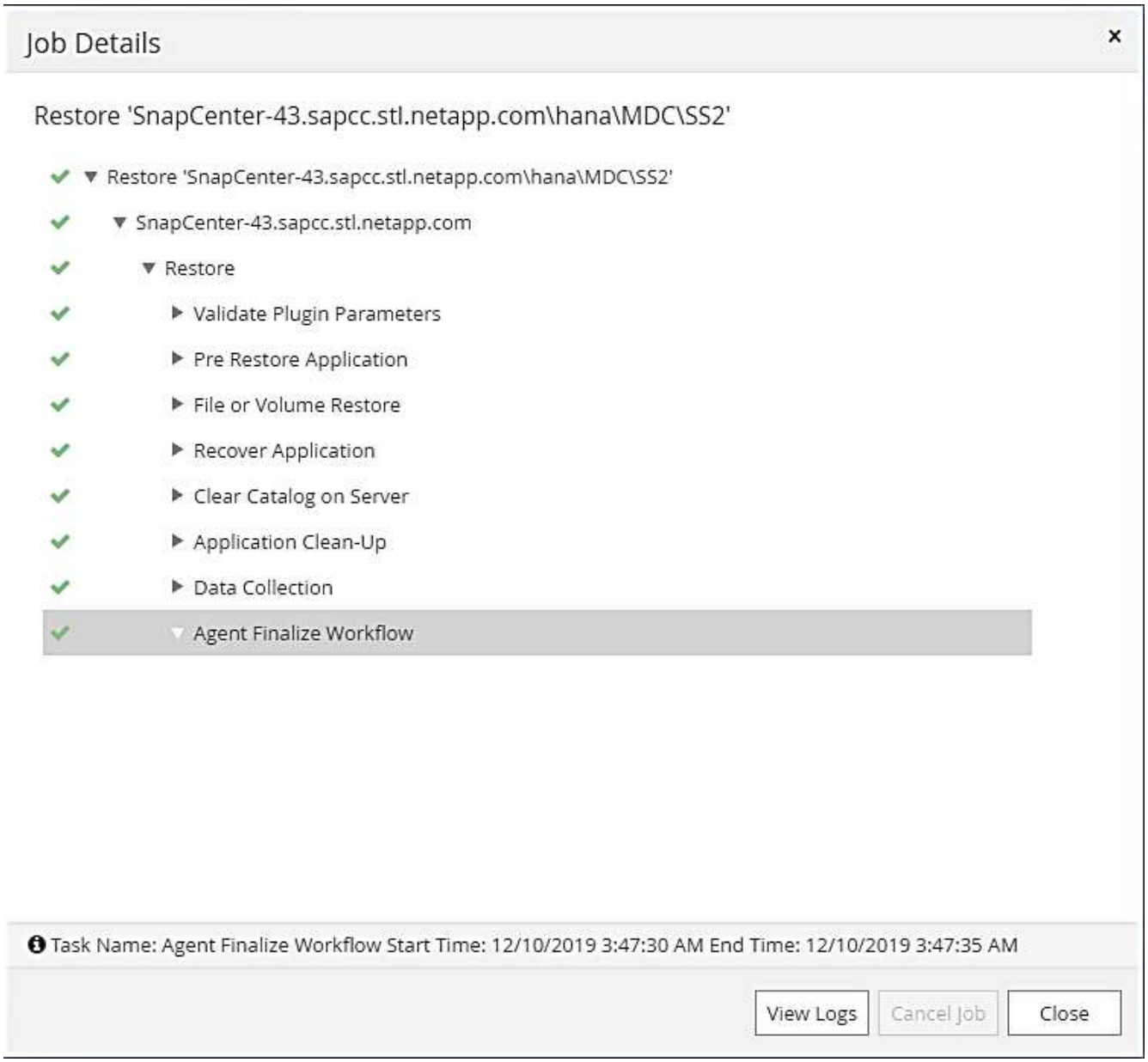
12. Specificare le impostazioni di notifica in modo che SnapCenter possa inviare un’e-mail di stato e un registro dei processi. Fare clic su Avanti.



13. Esaminare il riepilogo e fare clic su Finish (fine) per avviare il ripristino.



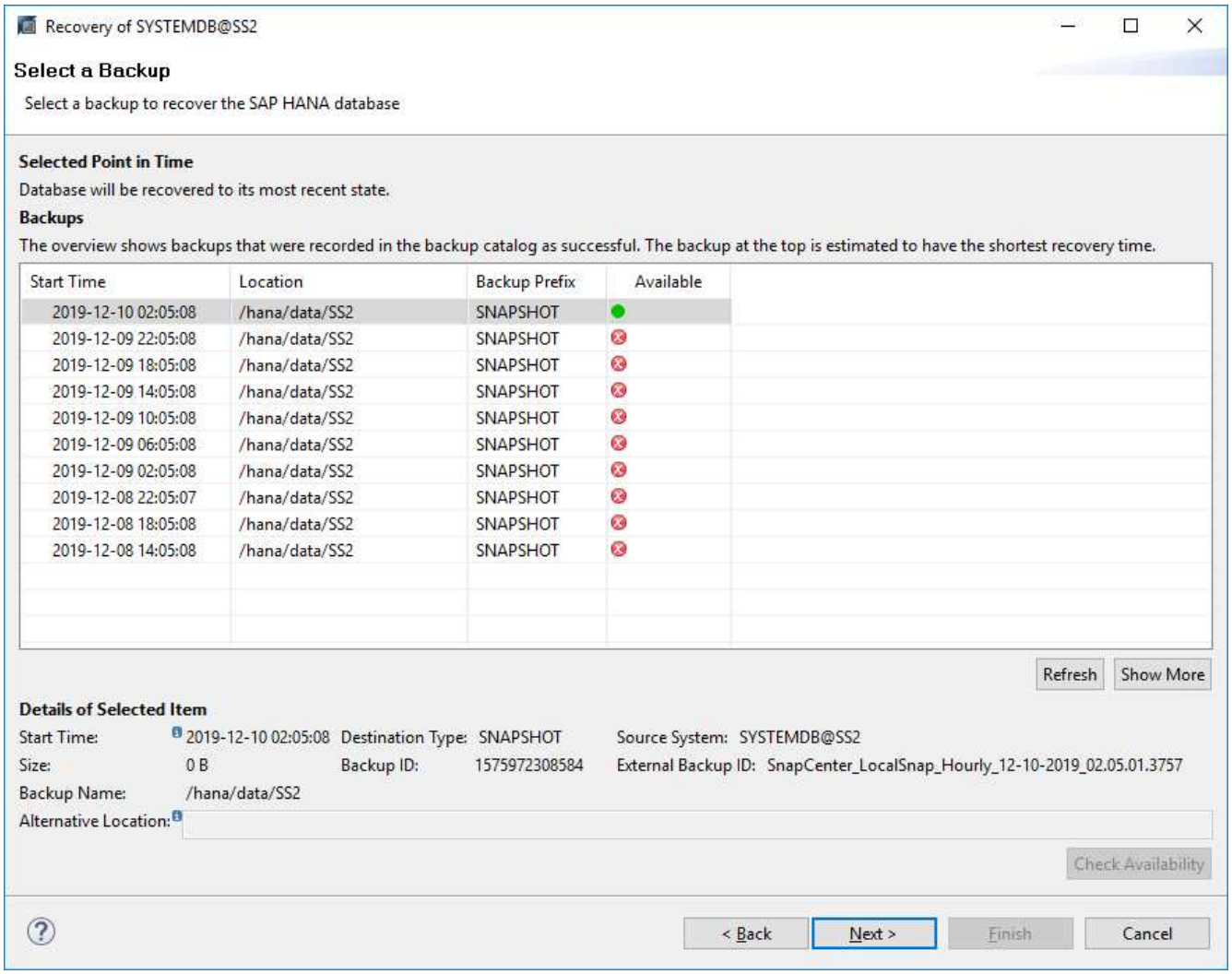
14. Il lavoro di ripristino viene avviato e il log dei lavori può essere visualizzato facendo doppio clic sulla riga del log nel riquadro delle attività.



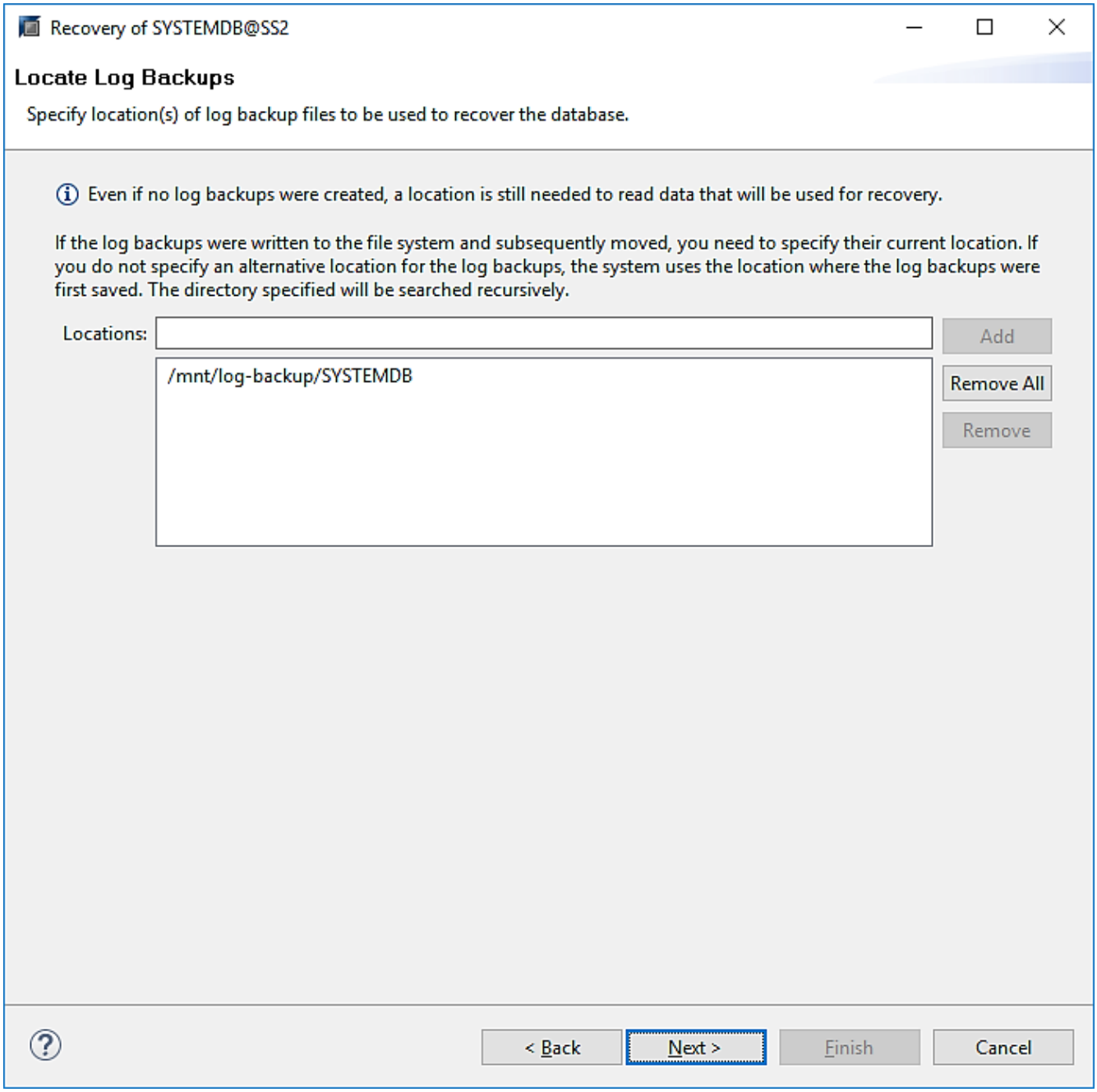
15. Attendere il completamento del processo di ripristino. Su ciascun host di database, montare tutti i volumi di dati. Nel nostro esempio, è necessario rimontare un solo volume sull'host del database.

```
mount /hana/data/SP1/mnt00001
```

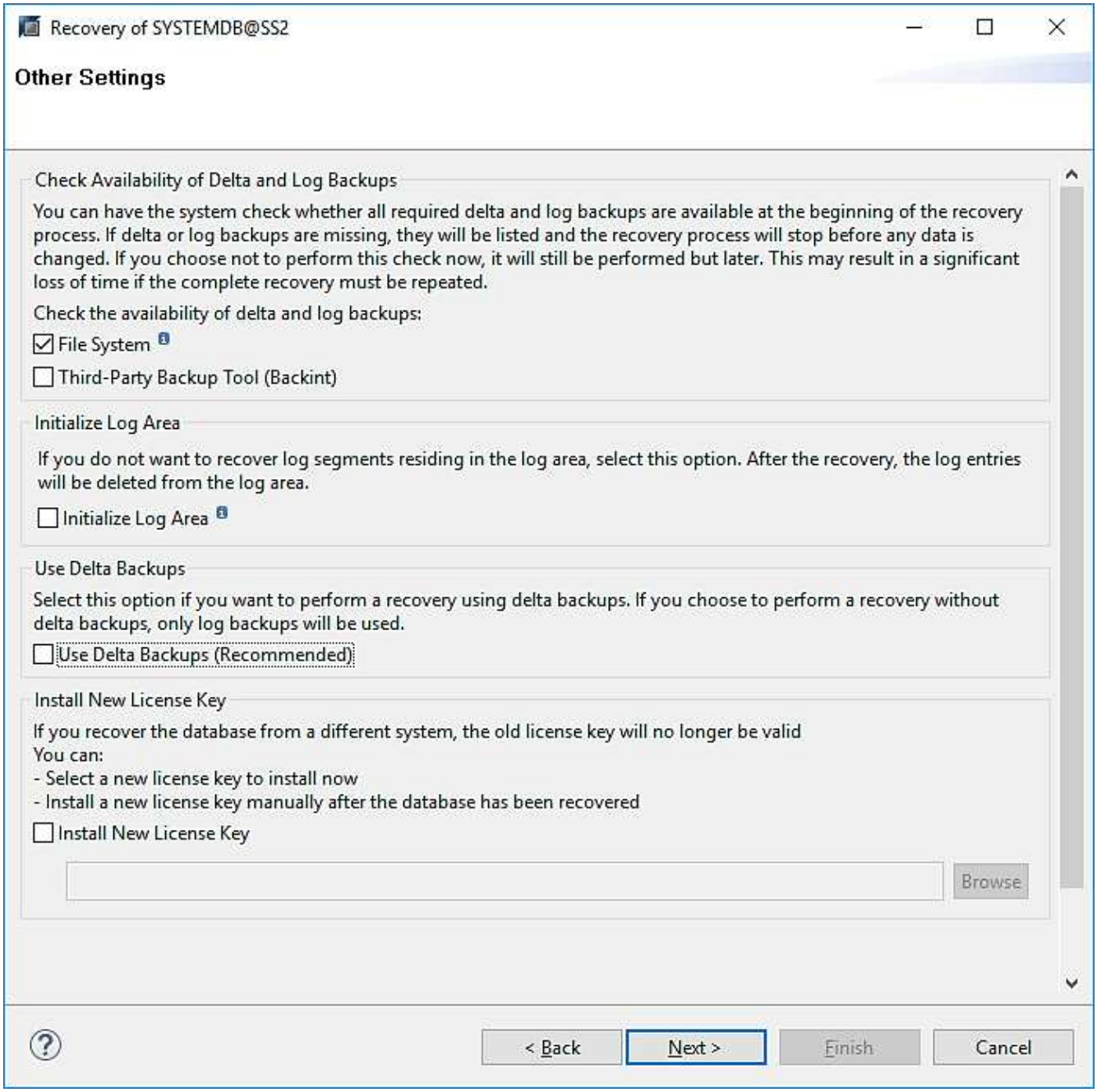
16. Accedere a SAP HANA Studio e fare clic su Refresh (Aggiorna) per aggiornare l'elenco dei backup disponibili. Il backup ripristinato con SnapCenter viene visualizzato con un'icona verde nell'elenco dei backup. Selezionare il backup e fare clic su Next (Avanti).



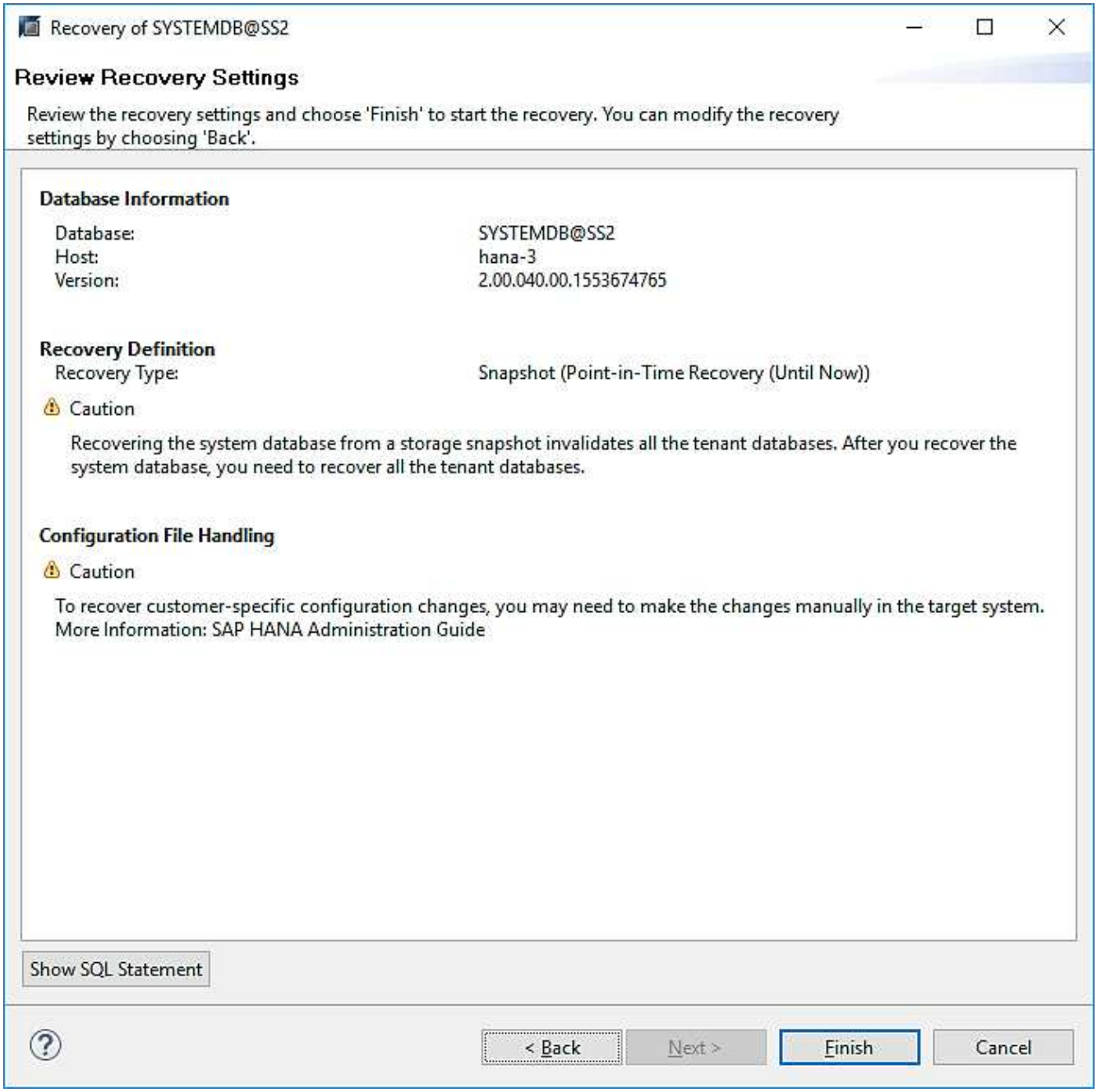
17. Fornire la posizione dei backup del registro. Fare clic su Avanti.



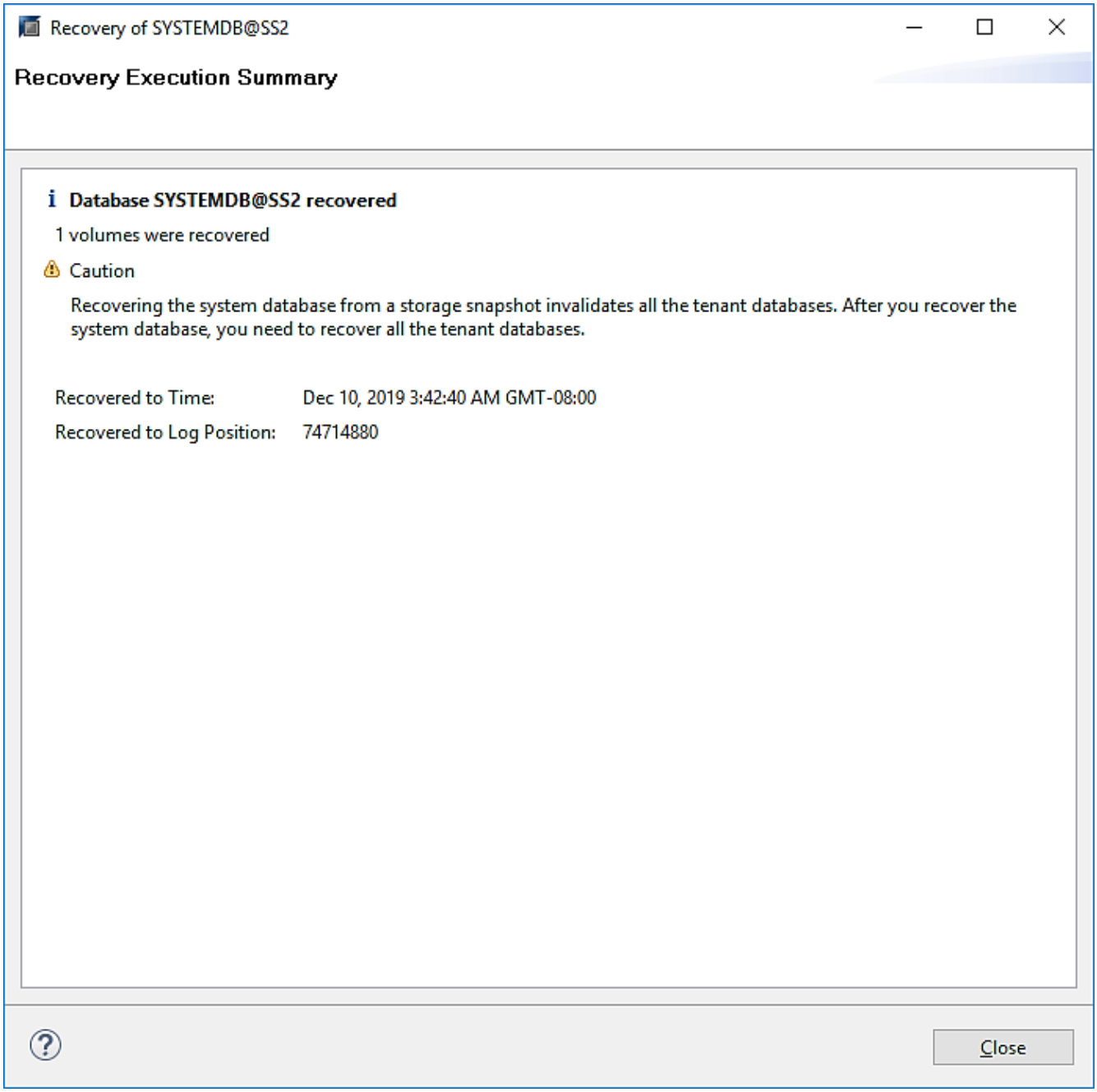
18. Selezionare le altre impostazioni desiderate. Assicurarsi che l'opzione Usa backup delta non sia selezionata. Fare clic su Avanti.



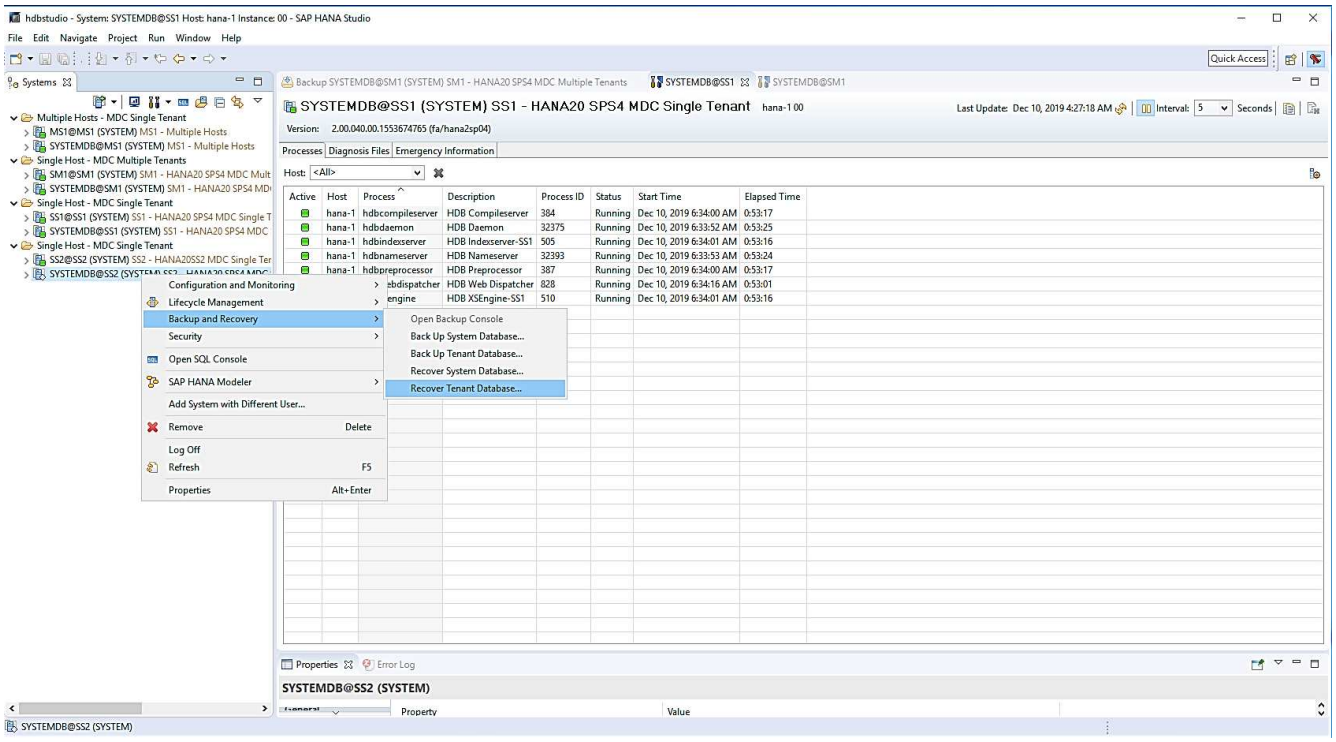
19. Rivedere le impostazioni di ripristino e fare clic su fine.



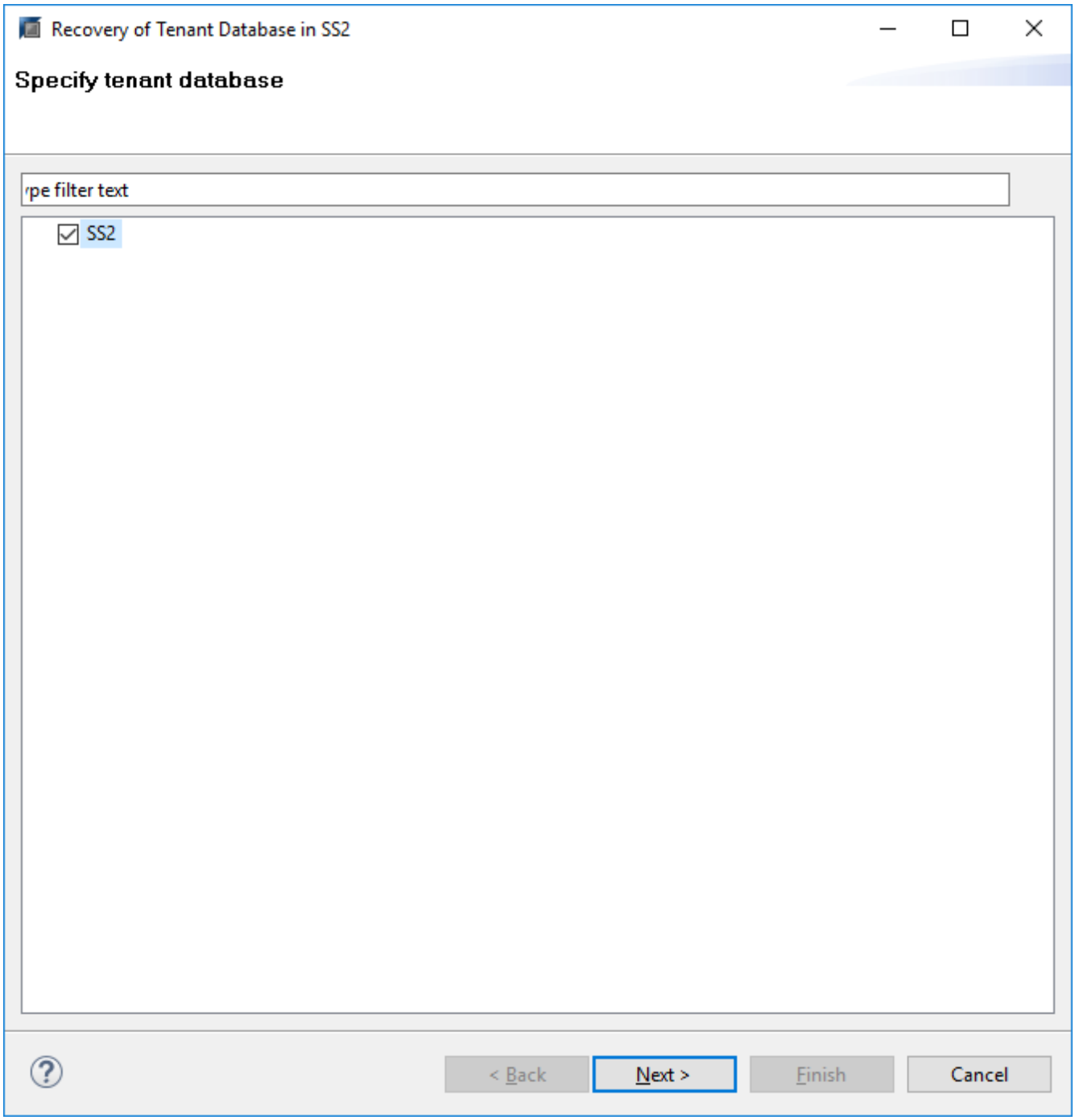
20. Viene avviato il processo di ripristino. Attendere il completamento del ripristino del database di sistema.



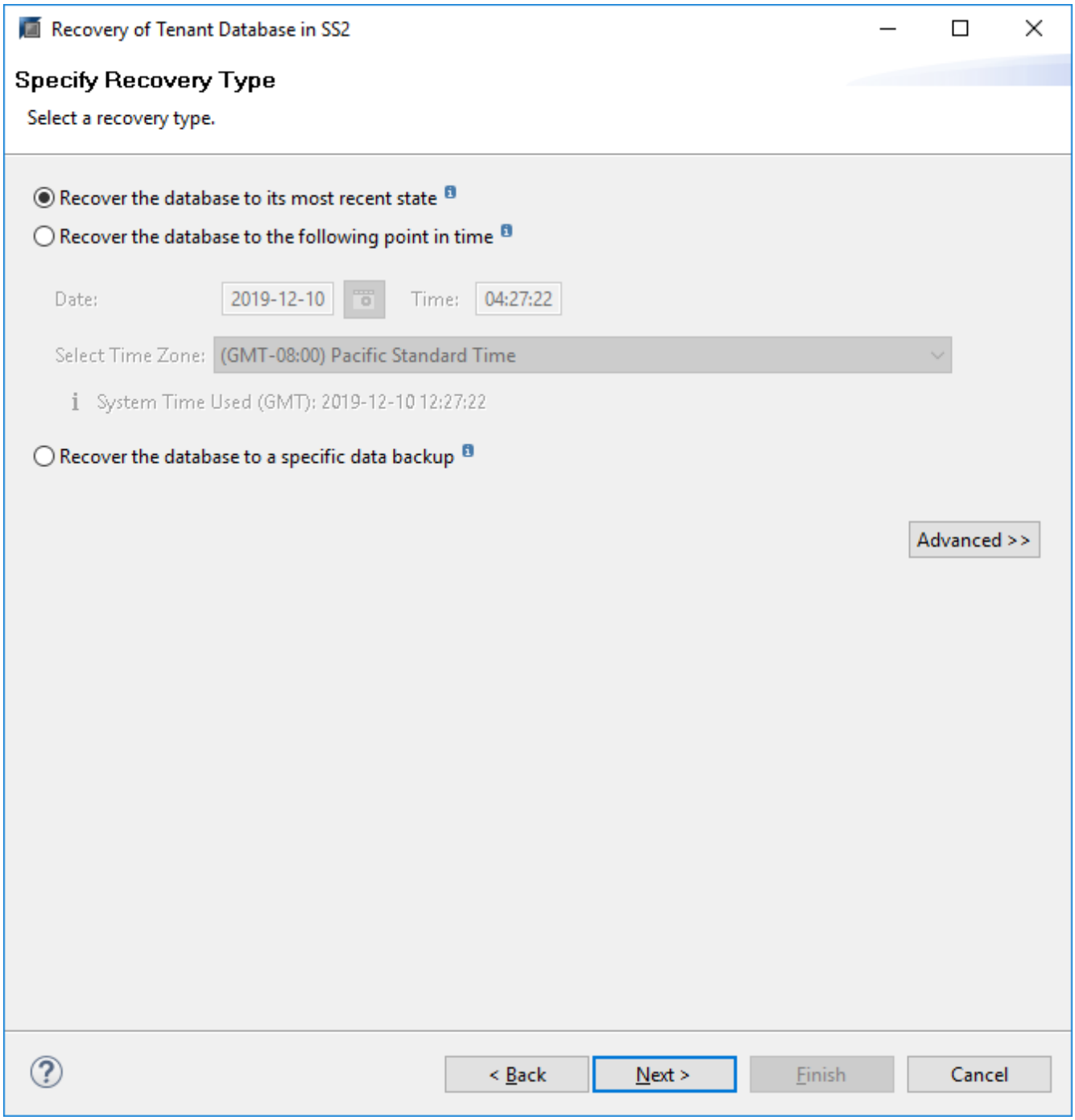
21. In SAP HANA Studio, selezionare la voce per il database di sistema e avviare Backup Recovery - Recover Tenant Database.



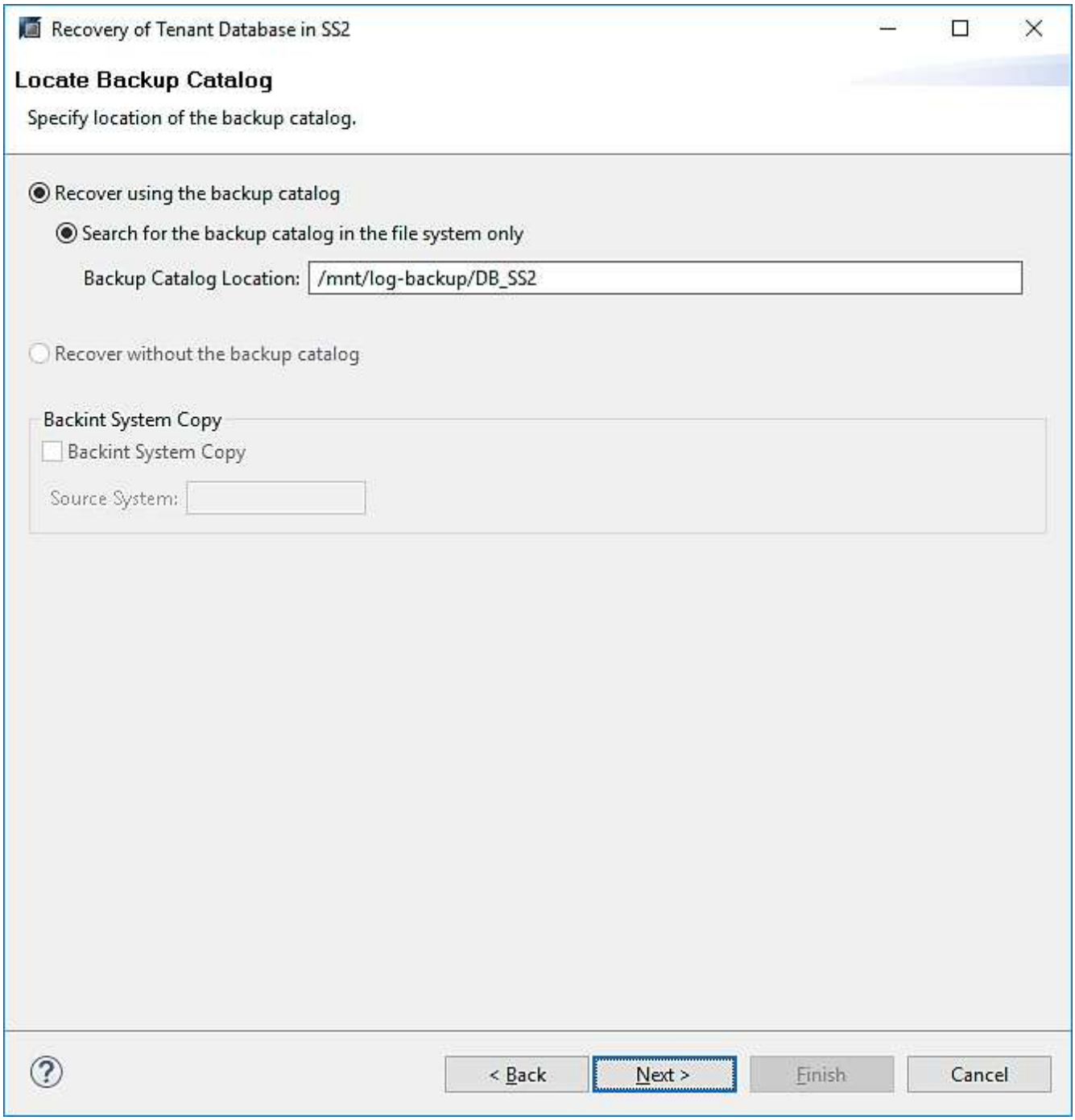
22. Selezionare il tenant da ripristinare e fare clic su Next (Avanti).



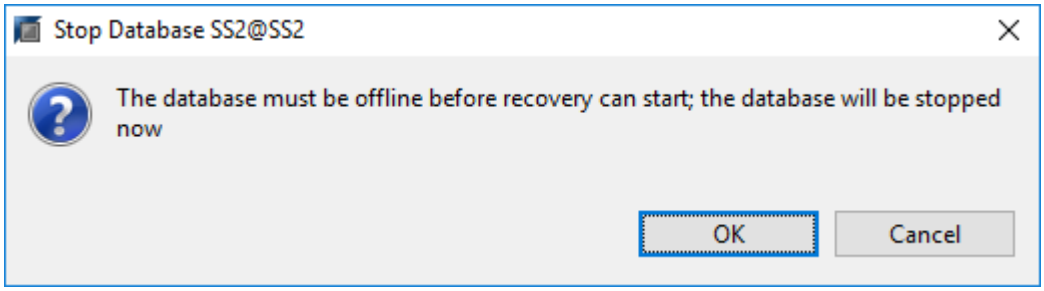
23. Specificare il tipo di ripristino e fare clic su Next (Avanti).



24. Confermare la posizione del catalogo di backup e fare clic su Next (Avanti).

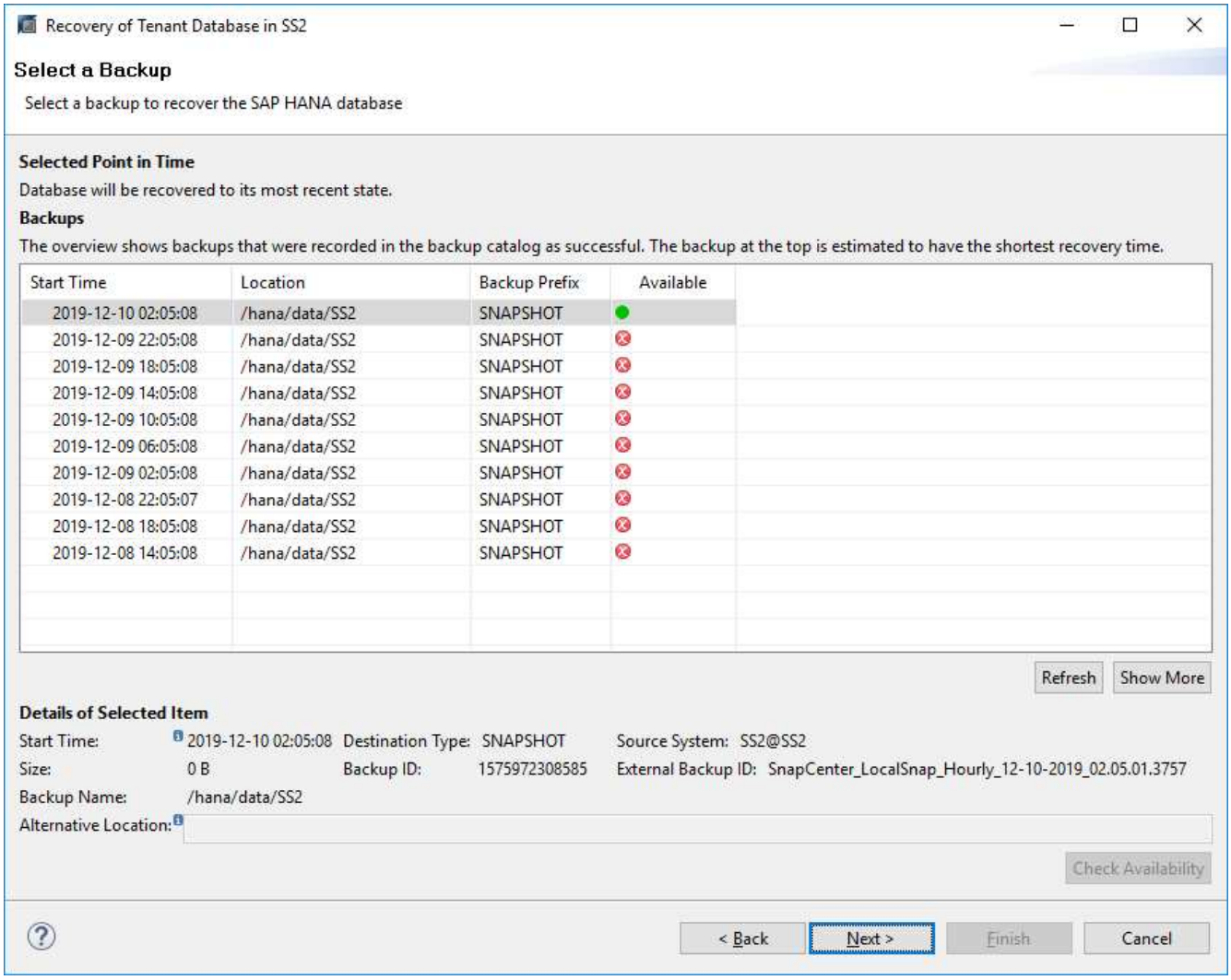


25. Verificare che il database del tenant sia offline. Fare clic su OK per continuare.

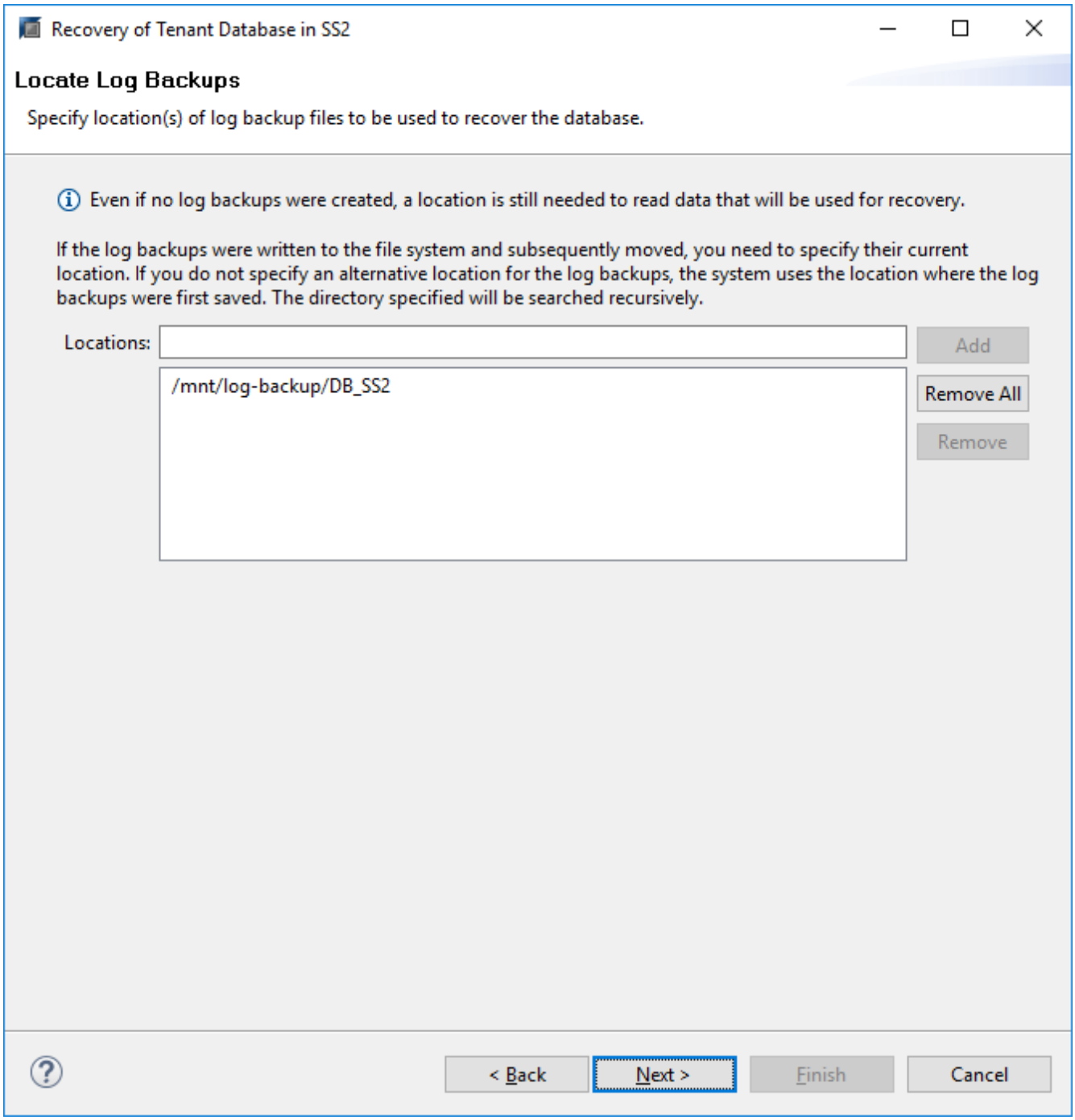


26. Poiché il ripristino del volume di dati si è verificato prima del ripristino del database di sistema, il backup del tenant è immediatamente disponibile. Selezionare il backup evidenziato in verde e fare clic su Next

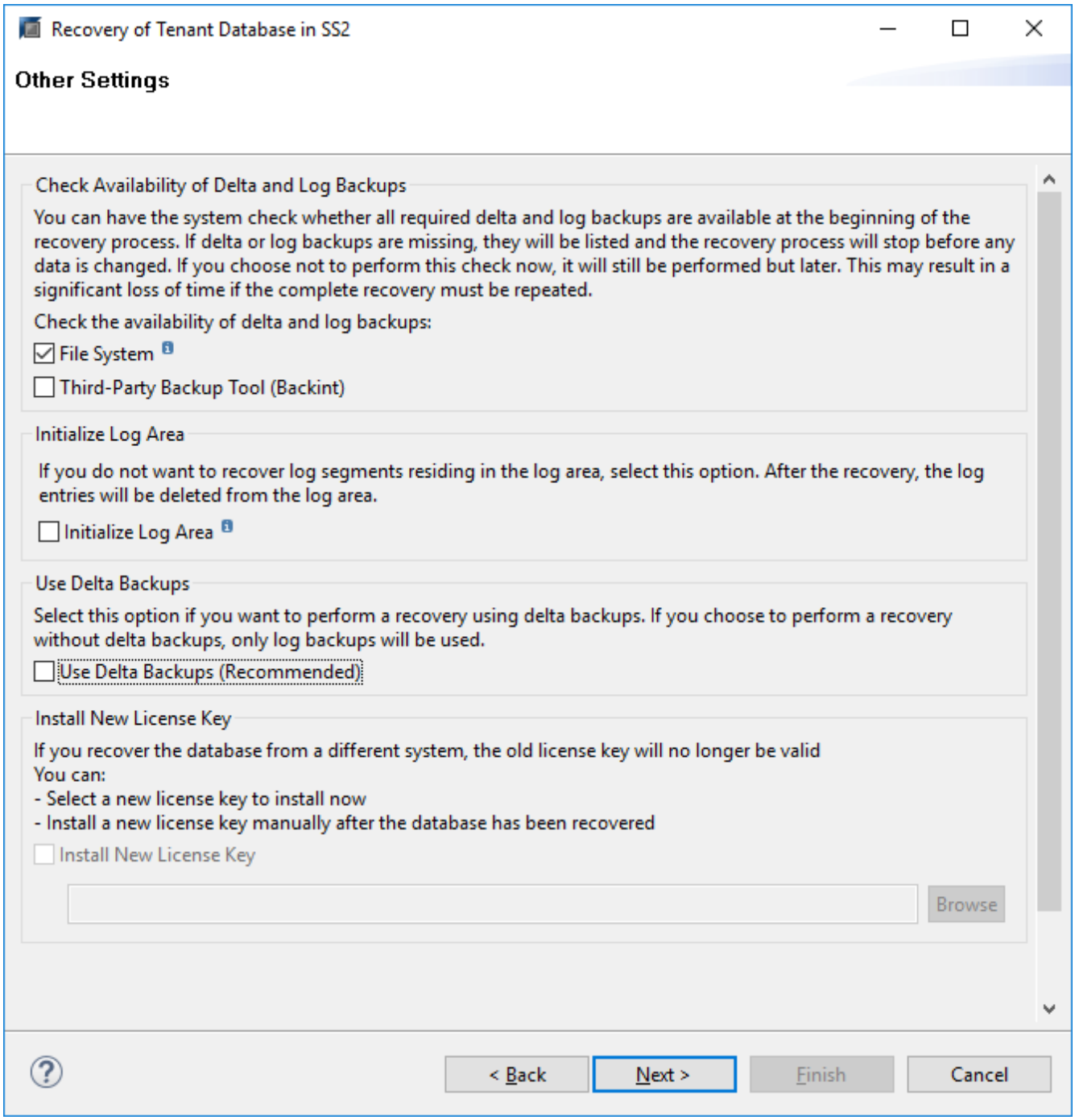
(Avanti).



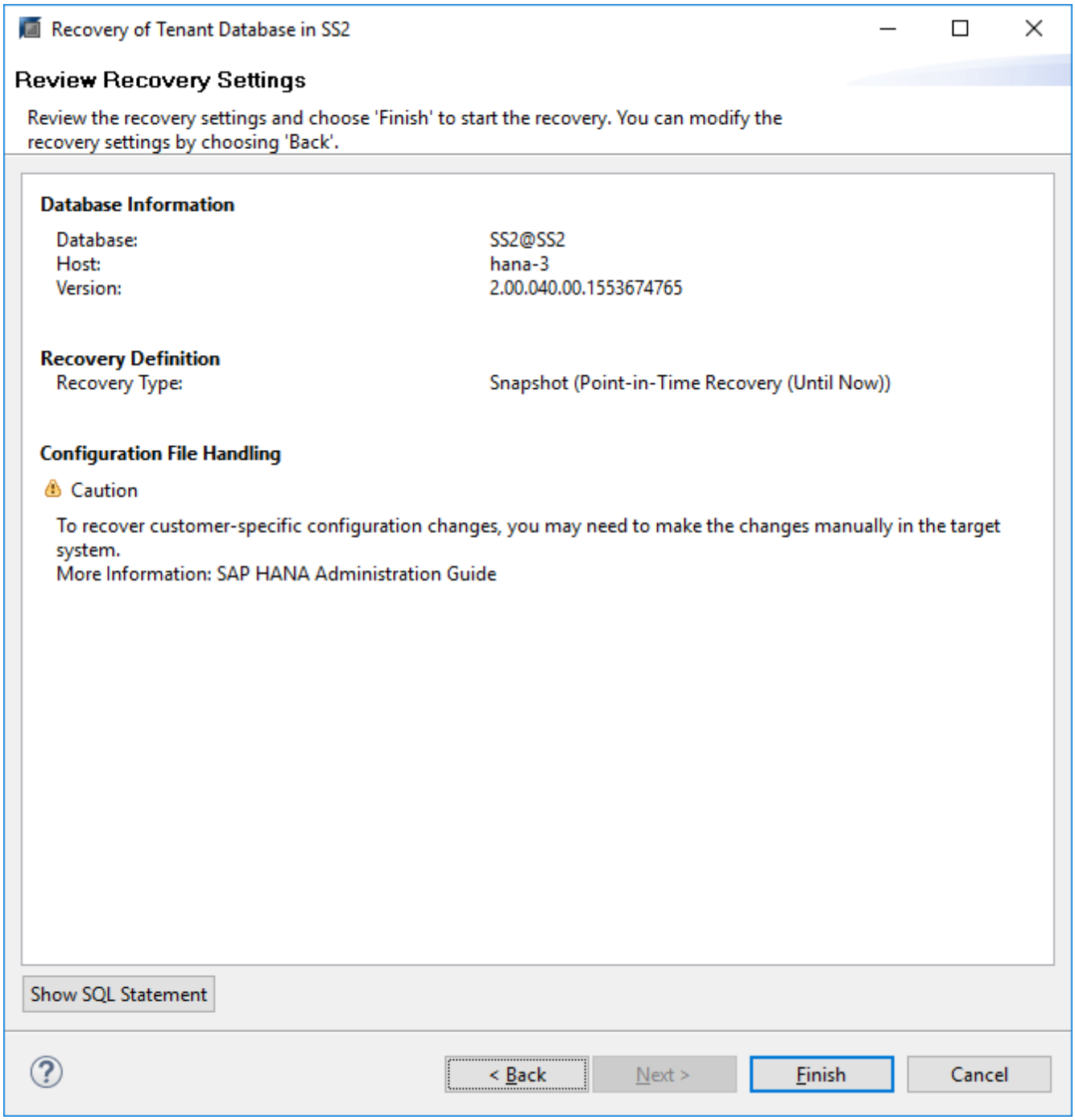
27. Confermare la posizione di backup del registro e fare clic su Next (Avanti).



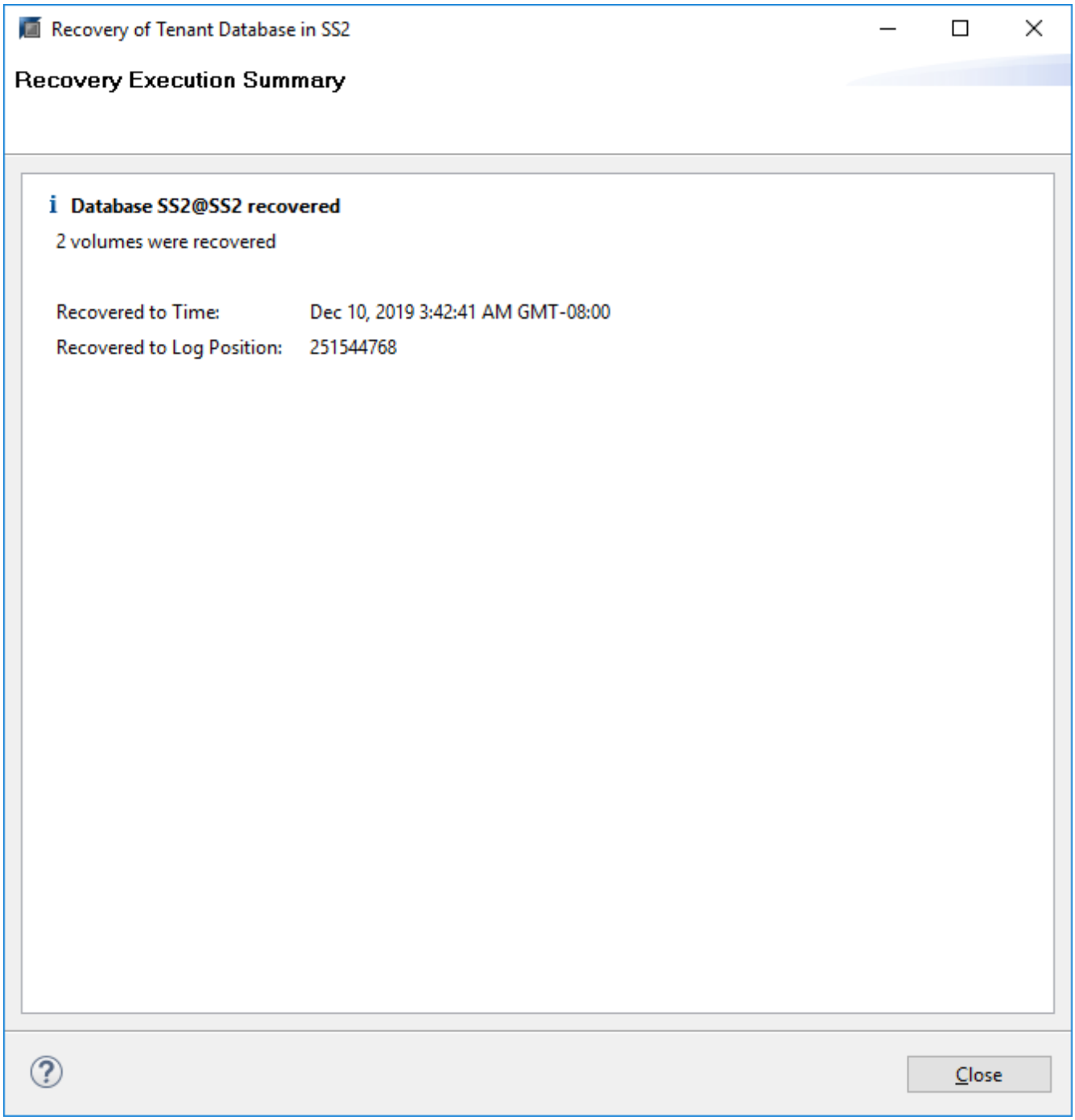
28. Selezionare le altre impostazioni desiderate. Assicurarsi che l'opzione Usa backup delta non sia selezionata. Fare clic su Avanti.



29. Esaminare le impostazioni di ripristino e avviare il processo di ripristino del database tenant facendo clic su Finish (fine).



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

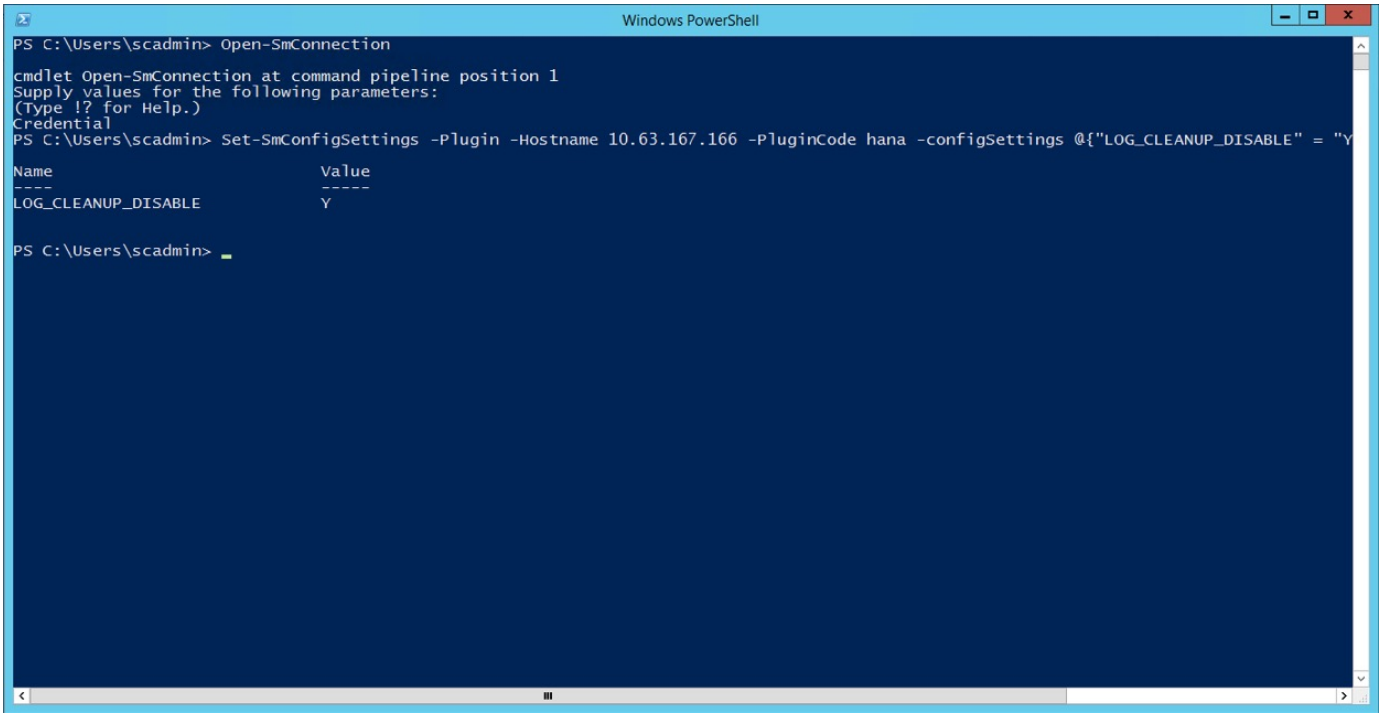
backup del log per tutte le risorse che utilizzano questo host plug-in SAP HANA come host di comunicazione:

- 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

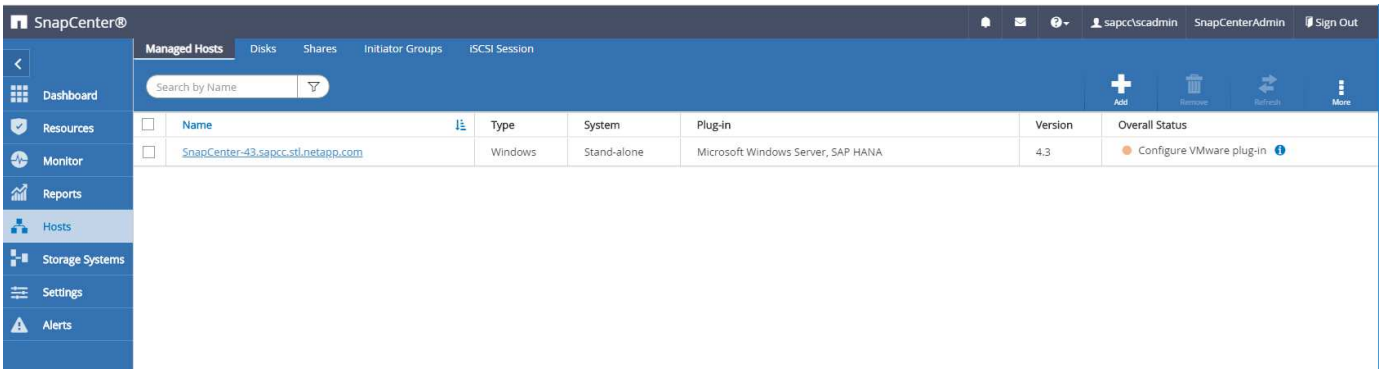
Una seconda opzione per configurare queste impostazioni consiste nell'utilizzare un comando PowerShell di SnapCenter.

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).



Disattiva l'avviso quando esegui il plug-in SAP HANA in un ambiente virtuale

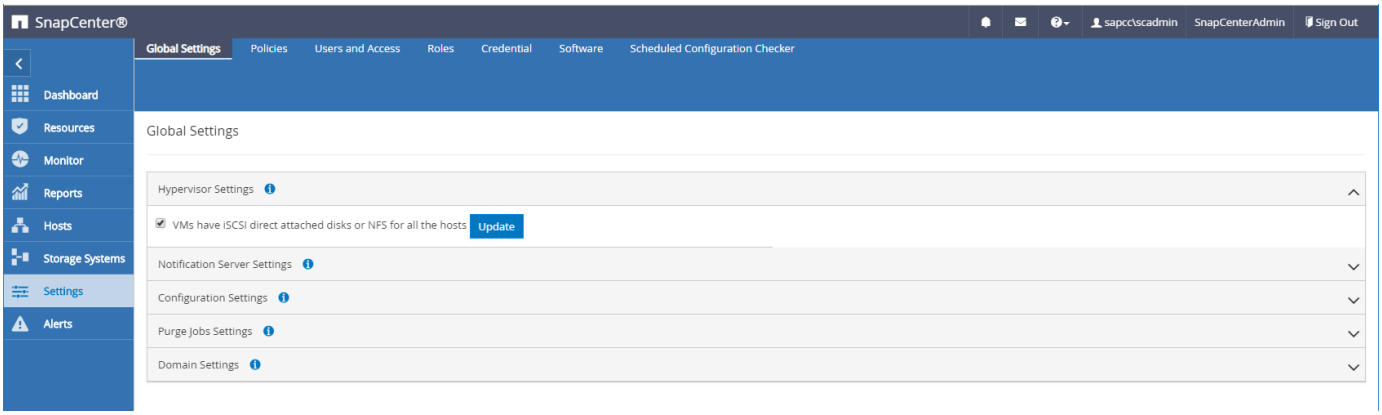
SnapCenter rileva se il plug-in SAP HANA è installato in un ambiente virtualizzato. Potrebbe trattarsi di un ambiente VMware o di un'installazione SnapCenter presso un provider di cloud pubblico. In questo caso, SnapCenter visualizza un avviso per la configurazione dell'hypervisor, come illustrato nella 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.

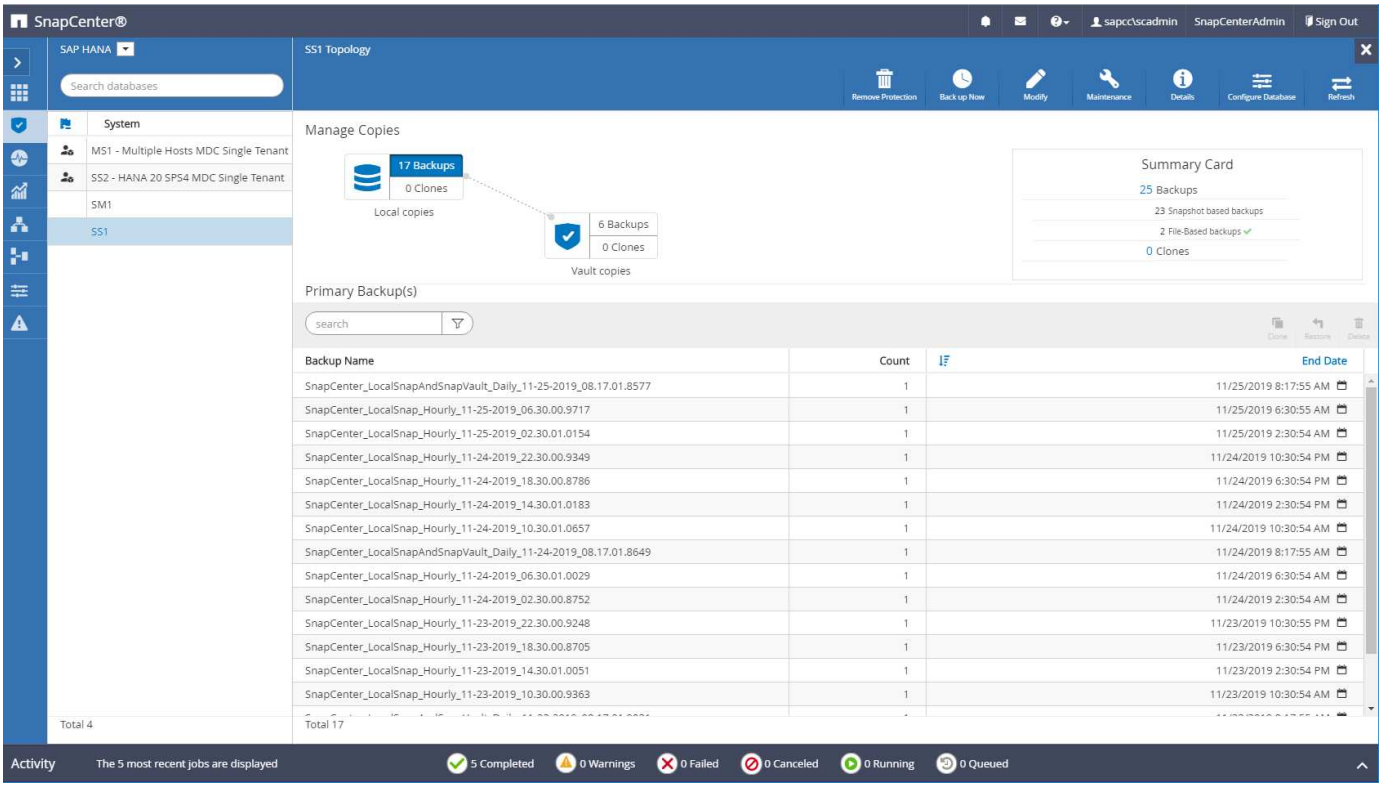
Fino al termine della pulizia pianificata, SAP HANA e SnapCenter potrebbero ancora mostrare i backup che sono già stati eliminati dallo storage di backup off-site.

> 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

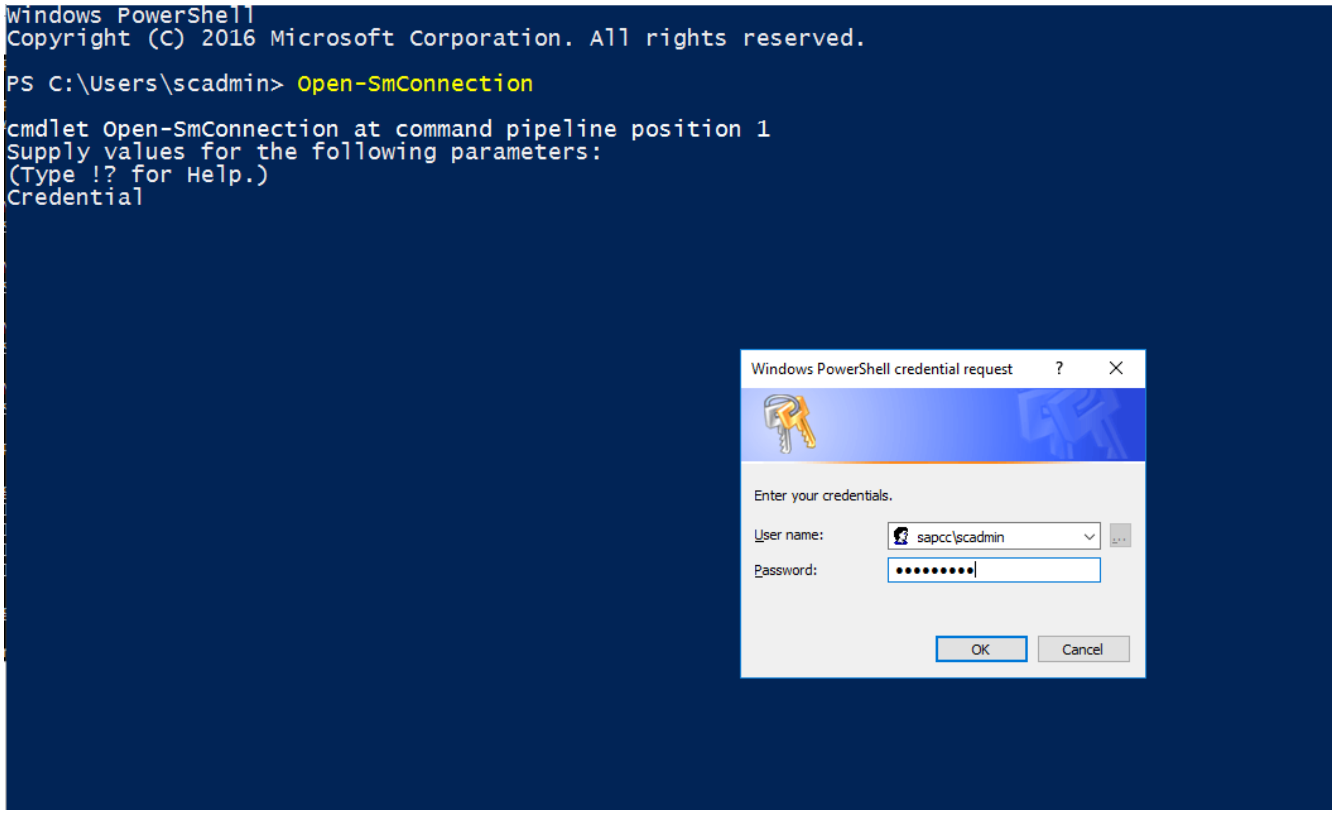
Nella vista della topologia di una risorsa, SnapCenter visualizza i backup sullo storage di backup off-site quando si selezionano i backup secondari, come illustrato nella seguente schermata. SnapCenter esegue un'operazione di pulizia con l'icona Refresh (Aggiorna) per sincronizzare i backup di questa 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.

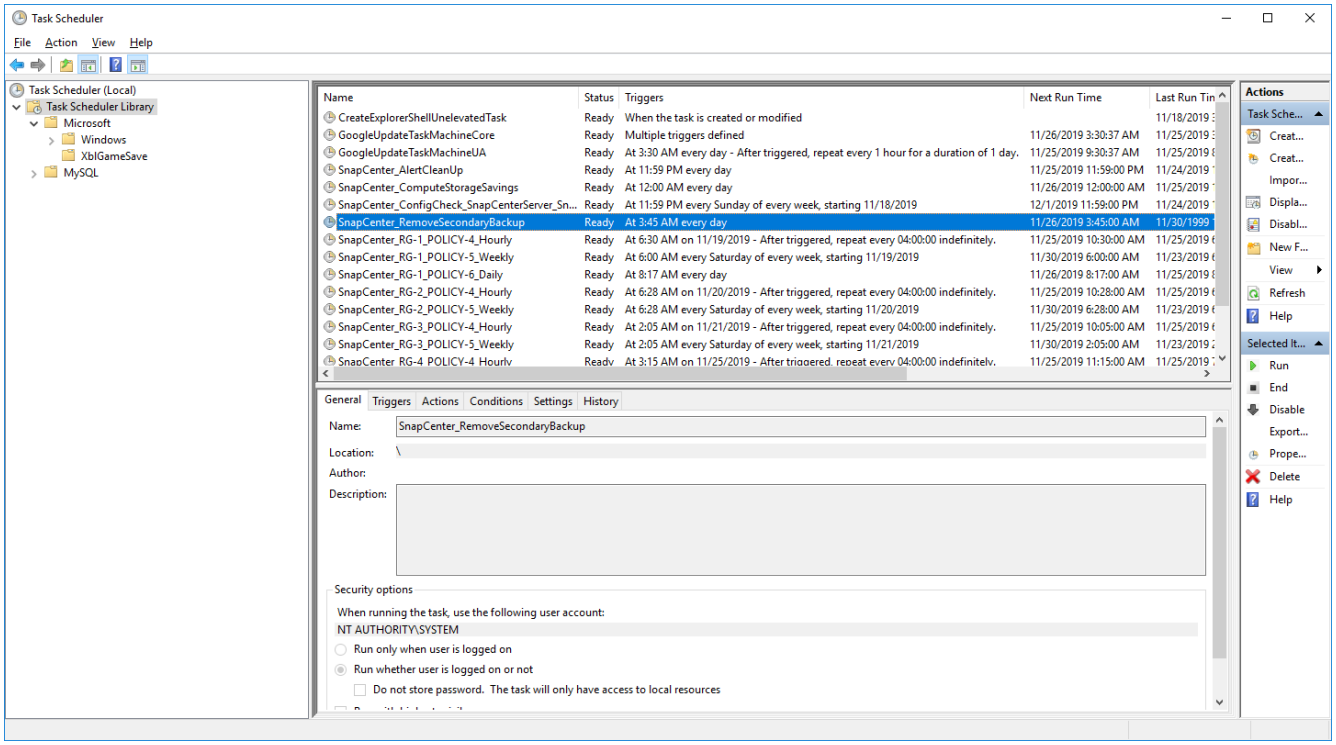
1. Avviare una finestra di comando PowerShell sul server SnapCenter.
2. Aprire la connessione al server SnapCenter e immettere le credenziali di amministratore SnapCenter nella finestra di accesso.



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"

- Documentazione software SnapCenter

  "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	• Release iniziale.
Versione 1.1	Settembre 2017	• Aggiunta della sezione "Configurazione e ottimizzazione avanzate". • Correzioni minori.
Versione 2.0	Marzo 2018	• Aggiornamenti per SnapCenter 4,0: Nuova risorsa del volume di dati Miglioramento del funzionamento di Single file SnapRestore
Versione 3.0	Gennaio 2020	• 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	• 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	• Aggiunti i privilegi utente del database richiesti per HANA 2.0 SPS5.
Versione 3.3	Maggio 2021	• Aggiornata la sezione di configurazione di SSL hdbsql. • Supporto LVM Linux aggiunto.

Versione	Data	Cronologia delle versioni del documento
Versione 3.4	Agosto 2021	• È stata aggiunta la descrizione della configurazione per la disattivazione del rilevamento automatico.
Versione 3.5	Febbraio 2022	• Aggiornamenti minori per SnapCenter 4.6 e supporto del rilevamento automatico per i sistemi HANA abilitati alla replica del sistema HANA.