Soluzioni per applicazioni aziendali SAP e database SAP HANA

NetApp solutions for SAP

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/it-it/netapp-solutions-sap/index.html on October 03, 2025. Always check docs.netapp.com for the latest.

Sommario

Soluzioni per applicazioni aziendali SAP e database SAP HANA . . . 1
Novità nelle soluzioni di virtualizzazione NetApp . . . 2
18 agosto 2025 . . . 2
Best Practice . . . 3
Guida alla configurazione di SAP HANA su sistemi NetApp AFF con FCP . . . 3
SAP HANA su sistemi NetApp AFF con protocollo Fibre Channel . . . 3
SAP HANA con VMware vSphere . . . 4
Architettura . . . 4
Dimensionamento dello storage . . . 9
Installazione e configurazione dell'infrastruttura . . . 14
Dove trovare ulteriori informazioni . . . 51
Aggiornare la cronologia . . . 52
Guida alla configurazione di SAP HANA su sistemi NetApp AFF con NFS . . . 53
SAP HANA su sistemi NetApp AFF con NFS - Guida alla configurazione . . . 53
Architettura . . . 55
Dimensionamento dello storage . . . 60
Installazione e configurazione dell'infrastruttura . . . 65
Dove trovare ulteriori informazioni . . . 93
Aggiornare la cronologia . . . 94
Guida alla configurazione di SAP HANA su sistemi NetApp ASA con FCP . . . 95
SAP HANA su sistemi NetApp ASA con protocollo Fibre Channel . . . 95
SAP HANA con VMware vSphere . . . 96
Architettura . . . 97
Dimensionamento dello storage . . . 100
Installazione e configurazione dell'infrastruttura . . . 105
Dove trovare ulteriori informazioni . . . 140
Aggiornare la cronologia . . . 140
Guida alla configurazione di SAP HANA su sistemi NetApp FAS con NFS . . . 141
Guida alla configurazione di SAP HANA su sistemi NetApp FAS con NFS . . . 141
Architettura . . . 143
Dimensionamento dello storage . . . 148
Installazione e configurazione dell'infrastruttura . . . 154
Dove trovare ulteriori informazioni . . . 184
Aggiornare la cronologia . . . 185
Guida alla configurazione di SAP HANA su sistemi FAS con FCP . . . 186
Guida alla configurazione di SAP HANA su sistemi NetApp FAS con protocollo Fibre Channel . . . 186
Architettura . . . 188
Dimensionamento dello storage . . . 193
Installazione e configurazione dell'infrastruttura . . . 198
Dove trovare ulteriori informazioni . . . 238
Aggiornare la cronologia . . . 239
Backup, ripristino e disaster recovery . . . 240
SAP HANA su Amazon FSX per NetApp ONTAP - Backup e recovery con SnapCenter . . . 240

TR-4926: SAP HANA su Amazon FSX per NetApp ONTAP - Backup e recovery con SnapCenter 240
Backup e ripristino con Amazon FSX per ONTAP 240
Architettura SnapCenter 245
Configurazione di SnapCenter 251
Operazioni di backup di SnapCenter 267
Backup di volumi non dati 277
Ripristinare e ripristinare 284
Replica del backup con SnapVault 292
Dove trovare ulteriori informazioni 306
Backup e recovery SAP HANA con SnapCenter 307
TR-4614: Backup e recovery SAP HANA con SnapCenter 307
Architettura SnapCenter 312
Soluzione di backup SAP HANA di SnapCenter 313
Concetti e Best practice di SnapCenter 317
Setup di laboratorio utilizzato per questo report 336
Configurazione di SnapCenter 337
Configurazione iniziale di SnapCenter 339
Configurazione specifica delle risorse SnapCenter per i backup dei database SAP HANA 352
Configurazione specifica delle risorse SnapCenter per i backup di volumi diversi dai dati 371
Backup del database 376
Controllo dell'integrità del blocco 385
Ripristino e ripristino 389
Configurazione e tuning avanzati 443
Dove trovare informazioni aggiuntive e cronologia delle versioni 451
Data Protection e high Availability di SAP HANA con SnapCenter, SnapMirror Active Sync e VMware Metro Storage Cluster 453
Data Protection e high Availability di SAP HANA con SnapCenter, SnapMirror Active Sync e VMware Metro Storage Cluster 453
Panoramica sull'high Availability di SAP HANA 454
Esempio di panoramica della configurazione 457
Provisioning e installazione del sistema HANA 458
Configurazione della sincronizzazione attiva di SnapMirror 466
Configurazione di SnapCenter 472
Operazioni di backup di SnapCenter 477
Ripristino e recovery di SnapCenter 480
Operazione di refresh del sistema SAP 482
Volumi SnapCenter non dati 482
Scenari di failover 484
Informazioni aggiuntive e cronologia delle versioni 488
Protezione dei dati SAP HANA con SnapCenter con sistemi VMware VMFS e NetApp ASA 489
Protezione dei dati SAP HANA con SnapCenter con sistemi VMware VMFS e NetApp ASA 489
Configurazione di laboratorio utilizzata per questo documento 489
Provisioning e installazione del sistema HANA 490
Configurazione HANA 497
Configurazione di SnapCenter 498

Operazioni di backup . . . 505
Operazioni di ripristino e recovery . . . 508
Aggiornamento del sistema SAP . . . 512
Informazioni aggiuntive e cronologia delle versioni . . . 522
Backup e ripristino della replica del sistema SAP HANA con SnapCenter . . . 523
TR-4719: Replica del sistema SAP HANA - Backup e ripristino con SnapCenter . . . 523
Backup Snapshot dello storage e replica del sistema SAP . . . 524
Opzioni di configurazione SnapCenter per la replica del sistema SAP . . . 525
Configurazione di SnapCenter 4.6 mediante un gruppo di risorse . . . 527
Configurazione di SnapCenter con una singola risorsa . . . 538
Ripristino e ripristino da un backup creato sull'altro host . . . 551
Dove trovare ulteriori informazioni . . . 555
Cronologia delle versioni . . . 555
Disaster recovery SAP HANA con Azure NetApp Files . . . 556
TR-4891: Disaster recovery SAP HANA con Azure NetApp Files . . . 556
Confronto tra soluzioni di disaster recovery . . . 558
ANF Replication cross-Region con SAP HANA . . . 562
Test di disaster recovery . . . 574
Failover del disaster recovery . . . 587
Aggiornare la cronologia . . . 598
TR-4646: Disaster recovery SAP HANA con replica dello storage . . . 598
TR-4711: Backup e ripristino SAP HANA con sistemi di storage NetApp e software CommVault . . . 599
Integrazione SnapCenter per database SAP ASE . . . 599
Introduzione . . . 599
Informazioni aggiuntive e cronologia delle versioni . . . 611
Integrazione SnapCenter per database IBM DB2 . . . 612
Introduzione . . . 612
Esempio di panoramica della configurazione . . . 613
Ambiente demo . . . 613
Informazioni aggiuntive e cronologia delle versioni . . . 620
Integrazione SnapCenter per database SAP MaxDB . . . 621
Introduzione . . . 621
Esempio di panoramica della configurazione . . . 621
Ambiente demo . . . 622
Versioni software . . . 622
Progettazione di volumi maxdb . . . 622
Procedura per proteggere il database M02 . . . 623
Prerequisiti sull'host . . . 623
Prerequisiti per il database: Creazione di modelli di backup, attivazione del backup di accesso . . . 623
Distribuire l'agente SnapCenter per ospitare sap-lnx25 . . . 624
Creare la configurazione delle risorse SnapCenter per il database M02 . . . 625
Sequenza di ripristino del sistema M02 . . . 632
Recupera istanza M02 . . . 632
Informazioni aggiuntive e cronologia delle versioni . . . 638
Gestione del ciclo di vita . . . 639

NetApp SAP Landscape Management Integration con Ansible . . . 639
TR-4953: Integrazione della gestione del panorama SAP di NetApp con Ansible . . . 639
Scenari di cloning, copia e refresh del sistema SAP . . . 639
Casi d’utilizzo per l’aggiornamento, la copia e la clonazione del sistema . . . 640
Integrazione di NetApp SAP lama con Ansible . . . 643
Esempio di implementazione . . . 643
Workflow di provisioning SAP lama - sistema clone . . . 649
Workflow di deprovisioning SAP lama - distruzione del sistema . . . 657
Workflow di provisioning SAP lama - sistema di copia . . . 660
Workflow di provisioning SAP lama - refresh del sistema . . . 664
Configurazione dello script del provider e playbook Ansible . . . 666
Conclusione . . . 679
Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter . . . 680
TR-4667: Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter . . . 680
Scenari di copia, aggiornamento e clonazione del sistema SAP . . . 682
Casi d’utilizzo per il refresh e la clonazione del sistema . . . 683
Infrastruttura e scenari supportati . . . 686
Panoramica del workflow di refresh del sistema SAP con SnapCenter . . . 686
Panoramica del workflow dei cloni di sistema SAP con SnapCenter . . . 689
Considerazioni sulle operazioni di refresh del sistema SAP HANA utilizzando backup snapshot dello storage . . . 690
Script di esempio di automazione . . . 695
Aggiornamento del sistema SAP HANA con SnapCenter . . . 698
Clone del sistema SAP con SnapCenter . . . 723
Dove trovare informazioni aggiuntive e cronologia delle versioni . . . 736
Automazione delle operazioni di copia del sistema SAP con libelle SystemCopy . . . 736
TR-4929: Automazione delle operazioni di copia del sistema SAP con libelle SystemCopy . . . 736
Aggiornamento del sistema SAP HANA con LSC e SnapCenter . . . 739
Aggiornamento del sistema SAP HANA con LSC, AzAcSnap e Azure NetApp Files . . . 752
Dove trovare informazioni aggiuntive e cronologia delle versioni . . . 766
Solution Brief . . . 768
SB-3978: Gestione del ciclo di vita per SAP HANA . . . 768
SB-3965: Backup e ripristino per SAP HANA . . . 768
La sfida . . . 768
La soluzione . . . 768
SB-3968: Disaster Recovery per SAP HANA . . . 768
La sfida . . . 768
La soluzione . . . 768
SB-4292: Automazione SAP con Ansible . . . 769
Panoramica della soluzione . . . 769
Conclusione . . . 772
Dove trovare ulteriori informazioni . . . 772
Cronologia delle versioni . . . 773
SB-4293: Automazione dei flussi di lavoro di copia, refresh e cloning del sistema SAP con ALPACA e

NetApp SnapCenter . . . 773
Panoramica della soluzione . . . 773
Conclusione . . . 778
Dove trovare ulteriori informazioni . . . 778
Cronologia delle versioni . . . 778
SB-4294: Automazione dei flussi di lavoro di copia, refresh e cloning del sistema SAP con Avantra e NetApp SnapCenter . . . 778
Panoramica della soluzione . . . 778
Conclusione . . . 782
Dove trovare ulteriori informazioni . . . 783
Cronologia delle versioni . . . 783
Note legali . . . 784
Copyright . . . 784
Marchi . . . 784
Brevetti . . . 784
Direttiva sulla privacy . . . 784

Soluzioni per applicazioni aziendali SAP e database SAP HANA

Novità nelle soluzioni di virtualizzazione NetApp

Scopri le novità nelle soluzioni per SAP.

18 agosto 2025

Il sito NetApp Solutions è ora il"Famiglia di soluzioni NetApp" , che comprende i seguenti siti:

- "Soluzioni di intelligenza artificiale NetApp"
- "Soluzioni container NetApp"
- "Soluzioni di gestione dei dati NetApp"
- "Soluzioni di database NetApp"
- "Soluzioni cloud pubbliche e ibride NetApp"
- Soluzioni NetApp per SAP
- "Soluzioni di virtualizzazione NetApp"

Best Practice

Guida alla configurazione di SAP HANA su sistemi NetApp AFF con FCP

SAP HANA su sistemi NetApp AFF con protocollo Fibre Channel

La famiglia di prodotti NetApp AFF è certificata per l'utilizzo con SAP HANA nei progetti TDI. Questa guida fornisce le best practice per SAP HANA su questa piattaforma per FCP.

Marco Schoen, NetApp

Introduzione

La famiglia di prodotti NetApp AFF/ ASA A-Series è stata certificata per l'utilizzo con SAP HANA in progetti di integrazione di data center personalizzati (TDI).

Questa certificazione è valida per i seguenti modelli:

- AFF A20, AFF A30, AFF A50, AFF A70, AFF A90, AFF A1K

Per un elenco completo delle soluzioni di storage certificate NetApp per SAP HANA, consulta la "Directory hardware SAP HANA certificata e supportata".

Questo documento descrive le configurazioni AFF che utilizzano il protocollo Fibre Channel (FCP).

> La configurazione descritta in questo documento è necessaria per ottenere i KPI SAP HANA richiesti e le migliori performance per SAP HANA. La modifica di impostazioni o l'utilizzo di funzionalità non elencate nel presente documento potrebbe causare un peggioramento delle prestazioni o un comportamento imprevisto e dovrebbe essere eseguita solo se richiesto dal supporto NetApp.

Le guide di configurazione per i sistemi AFF che utilizzano i sistemi NFS e NetApp FAS sono disponibili tramite i seguenti collegamenti:

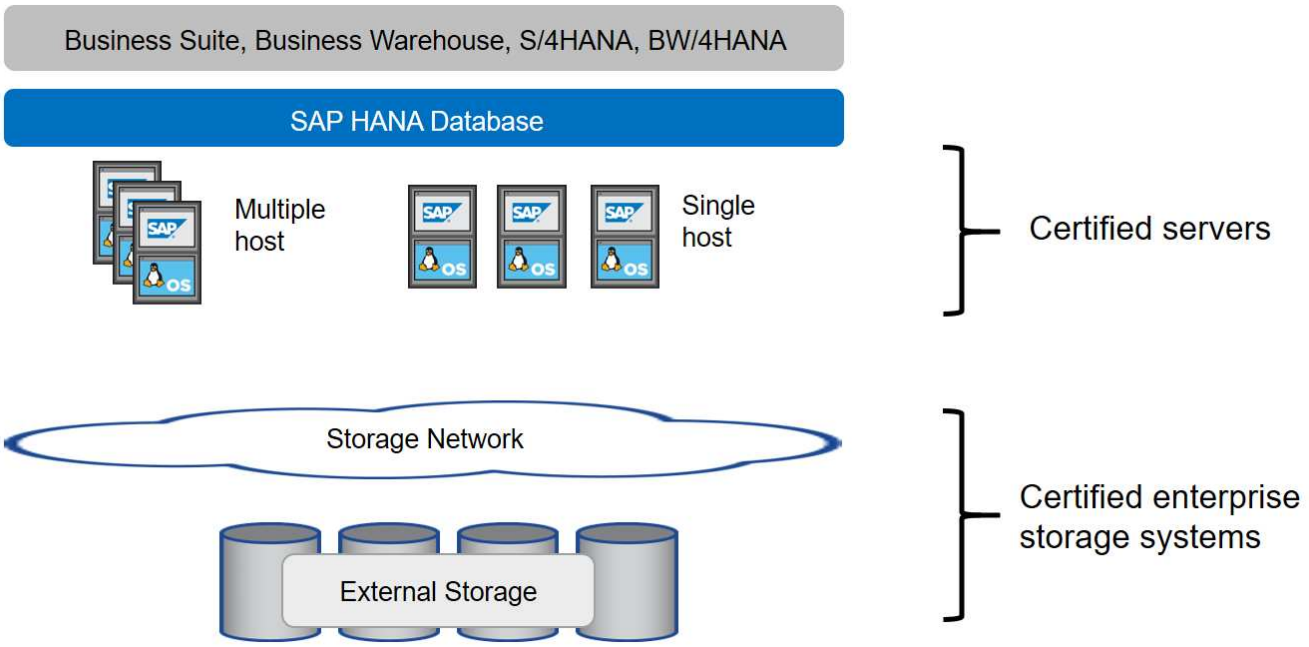
- "SAP HANA su sistemi NetApp FAS con FCP"
- "SAP HANA su sistemi NetApp ASA con FCP"
- "SAP HANA su sistemi NetApp FAS con NFS"
- "SAP HANA su sistemi NetApp AFF con NFS"

In un ambiente multi-host SAP HANA, il connettore storage standard SAP HANA viene utilizzato per fornire la scherma in caso di failover di un host SAP HANA. Fare sempre riferimento alle note SAP relative alle linee guida per la configurazione del sistema operativo e alle dipendenze specifiche del kernel Linux HANA. Per ulteriori informazioni, vedere "Nota SAP 2235581 – sistemi operativi supportati da SAP HANA".

SAP HANA: Integrazione personalizzata del data center

I sistemi storage NetApp AFF sono certificati nel programma SAP HANA TDI utilizzando sia protocolli NFS (NAS) che FC (SAN). Possono essere implementati in qualsiasi scenario SAP HANA, come SAP Business

Suite su HANA, S/4HANA, BW/4HANA o SAP Business Warehouse su HANA in configurazioni a host singolo o multiplo. Qualsiasi server certificato per l'utilizzo con SAP HANA può essere combinato con soluzioni di storage certificate NetApp. La figura seguente mostra una panoramica dell'architettura.



Per ulteriori informazioni sui prerequisiti e sui consigli per i sistemi SAP HANA produttivi, consulta la seguente risorsa:

- "SAP HANA - Domande frequenti sull'integrazione personalizzata del data center"

SAP HANA con VMware vSphere

Esistono diverse opzioni per connettere lo storage alle macchine virtuali (VM). Il metodo preferito consiste nel collegare i volumi di storage con NFS direttamente dal sistema operativo guest. Questa opzione è descritta in "SAP HANA su sistemi NetApp AFF con NFS".

Sono supportati anche RDM (Raw Device Mapping), datastore FCP o datastore VVOL con FCP. Per entrambe le opzioni del datastore, è necessario memorizzare un solo volume di log o dati SAP HANA all'interno del datastore per casi di utilizzo produttivi.

Per ulteriori informazioni sull'utilizzo di vSphere con SAP HANA, consultare i seguenti collegamenti:

- "SAP HANA su VMware vSphere - virtualizzazione - Wiki della community"
- "Guida alle Best practice di SAP HANA su VMware vSphere"
- "2161991 - linee guida per la configurazione di VMware vSphere - Launchpad di supporto SAP ONE (accesso richiesto)"

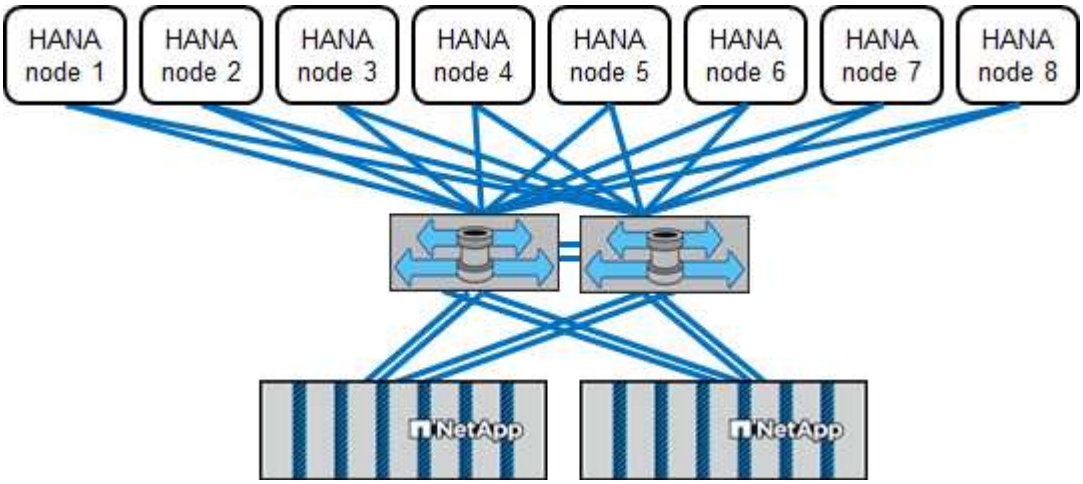
Architettura

Gli host SAP HANA sono connessi ai controller di storage utilizzando un'infrastruttura FCP ridondante e un software multipath. È necessaria un'infrastruttura di switch FCP ridondante per fornire connettività host-to-storage SAP HANA fault-tolerant in caso di guasto dello switch o dell'HBA (host bus adapter). È necessario configurare lo zoning

appropriato sullo switch per consentire a tutti gli host HANA di raggiungere i LUN richiesti sui controller di storage.

Diversi modelli della famiglia di sistemi AFF possono essere combinati e abbinati a livello di storage per consentire la crescita e le diverse esigenze di performance e capacità. Il numero massimo di host SAP HANA che possono essere collegati al sistema storage è definito dai requisiti di performance SAP HANA e dal modello di controller NetApp utilizzato. Il numero di shelf di dischi richiesti è determinato solo dai requisiti di capacità e performance dei sistemi SAP HANA.

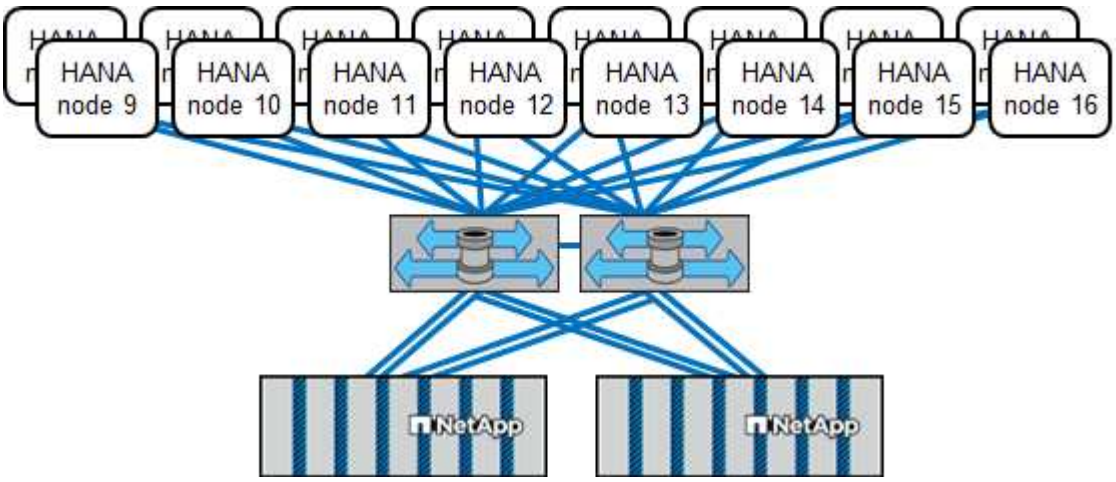
La figura seguente mostra una configurazione di esempio con otto host SAP HANA collegati a una coppia ha di storage.



Questa architettura può essere scalata in due dimensioni:

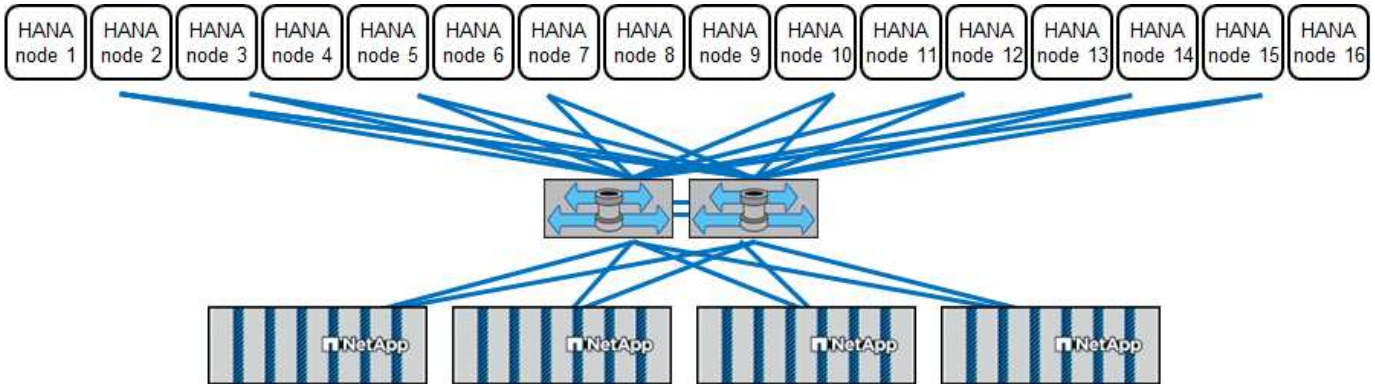
- Collegando ulteriori host SAP HANA e capacità di storage allo storage esistente, se i controller di storage forniscono performance sufficienti per soddisfare gli attuali KPI SAP HANA
- Aggiungendo altri sistemi storage con capacità di storage aggiuntiva per gli host SAP HANA aggiuntivi

La figura seguente mostra un esempio di configurazione in cui più host SAP HANA sono collegati ai controller di storage. In questo esempio, sono necessari più shelf di dischi per soddisfare i requisiti di capacità e performance dei 16 host SAP HANA. A seconda dei requisiti di throughput totale, è necessario aggiungere ulteriori connessioni FC ai controller di storage.



Indipendentemente dal sistema AFF implementato, il panorama SAP HANA può anche essere scalato

aggiungendo qualsiasi storage controller certificato per soddisfare la densità di nodo desiderata, come mostrato nella figura seguente.



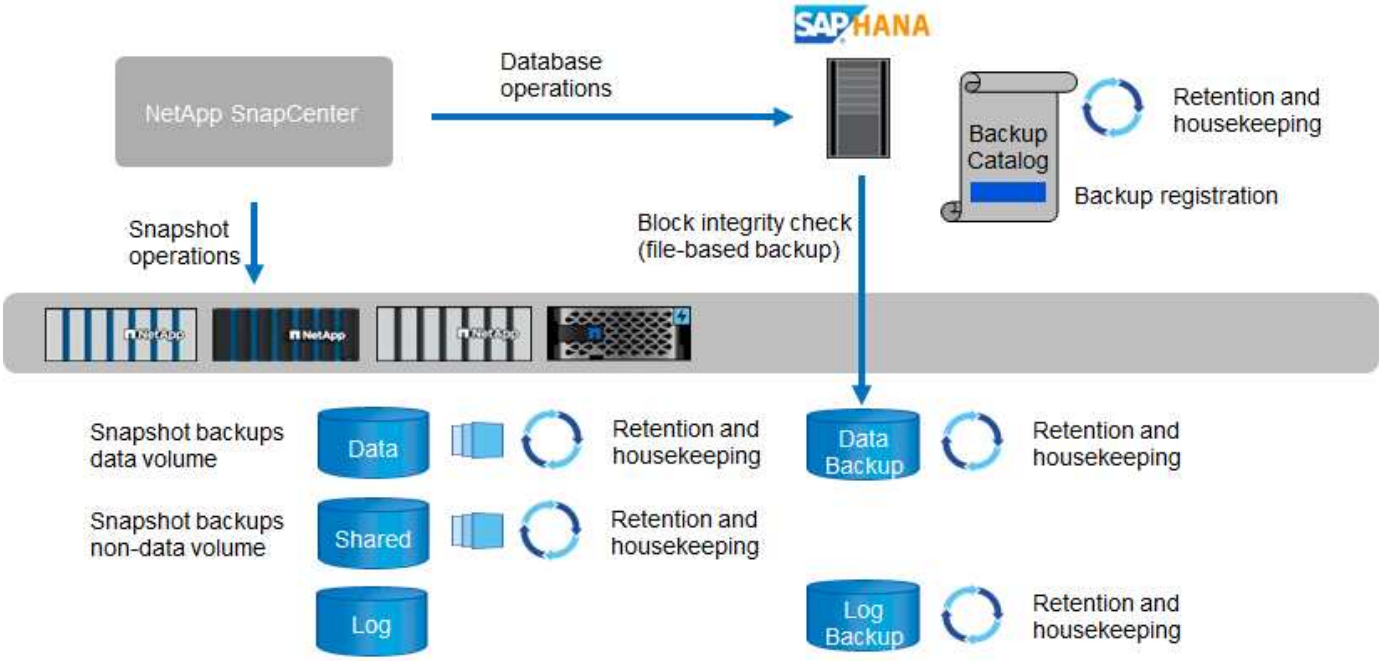
Backup SAP HANA

Il software ONTAP presente su tutti i controller di storage NetApp offre un meccanismo integrato per eseguire il backup dei database SAP HANA durante il funzionamento senza alcun effetto sulle performance. I backup NetApp Snapshot basati su storage sono una soluzione di backup completamente supportata e integrata disponibile per i singoli container SAP HANA e per i sistemi SAP HANA MDC con un singolo tenant o più tenant.

I backup Snapshot basati su storage vengono implementati utilizzando il plug-in NetApp SnapCenter per SAP HANA. Ciò consente agli utenti di creare backup Snapshot coerenti basati sullo storage utilizzando le interfacce fornite in modo nativo dai database SAP HANA. SnapCenter registra tutti i backup Snapshot nel catalogo di backup SAP HANA. Pertanto, i backup eseguiti da SnapCenter sono visibili all'interno di SAP HANA Studio o Cockpit, dove possono essere selezionati direttamente per le operazioni di ripristino e recovery.

La tecnologia NetApp SnapMirror consente di replicare le copie Snapshot create su un sistema storage su un sistema storage di backup secondario controllato da SnapCenter. È quindi possibile definire diversi criteri di conservazione dei backup per ciascuno dei set di backup sullo storage primario e anche per i set di backup sui sistemi di storage secondari. Il plug-in SnapCenter per SAP HANA gestisce automaticamente la conservazione dei backup dei dati basati su copia Snapshot e dei backup dei log, inclusa la manutenzione del catalogo di backup. Il plug-in SnapCenter per SAP HANA consente inoltre di eseguire un controllo dell'integrità del blocco del database SAP HANA eseguendo un backup basato su file.

È possibile eseguire il backup dei log del database direttamente sullo storage secondario utilizzando un montaggio NFS, come illustrato nella figura seguente.



I backup Snapshot basati su storage offrono vantaggi significativi rispetto ai backup convenzionali basati su file. Questi vantaggi includono, a titolo esemplificativo e non esaustivo, i seguenti:

- Backup più rapido (pochi minuti)
- RTO ridotto grazie a tempi di ripristino molto più rapidi sul layer di storage (pochi minuti) e a backup più frequenti
- Nessuna riduzione delle performance dell'host, della rete o dello storage del database SAP HANA durante le operazioni di backup e recovery
- Replica efficiente in termini di spazio e larghezza di banda sullo storage secondario in base alle modifiche dei blocchi

Per informazioni dettagliate sulla soluzione di backup e ripristino SAP HANA, consultare "TR-4614: Backup e ripristino SAP HANA con SnapCenter".

Disaster recovery SAP HANA

Il disaster recovery SAP HANA può essere eseguito a livello di database utilizzando la replica di sistema SAP HANA o a livello di storage utilizzando le tecnologie di replica dello storage. La sezione seguente fornisce una panoramica delle soluzioni di disaster recovery basate sulla replica dello storage.

Per informazioni dettagliate sulle soluzioni di disaster recovery SAP HANA, vedere "TR-4646: Disaster recovery SAP HANA con replica dello storage".

Replica dello storage basata su SnapMirror

La figura seguente mostra una soluzione di disaster recovery a tre siti che utilizza la sincronizzazione attiva sincrona di SnapMirror con il data center di disaster recovery locale e la sincronizzazione asincrona di SnapMirror per replicare i dati sul data center di disaster recovery remoto. La sincronizzazione attiva di SnapMirror consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover trasparente delle applicazioni utilizzando una copia secondaria (RPO=0 e RTO=0). Non sono richiesti interventi manuali o script personalizzati per attivare un failover con la sincronizzazione attiva di SnapMirror. A partire da ONTAP 9.15.1, la sincronizzazione attiva SnapMirror supporta una funzionalità Active/Active simmetrica. Active/Active simmetrico consente operazioni di i/o in lettura e scrittura da entrambe

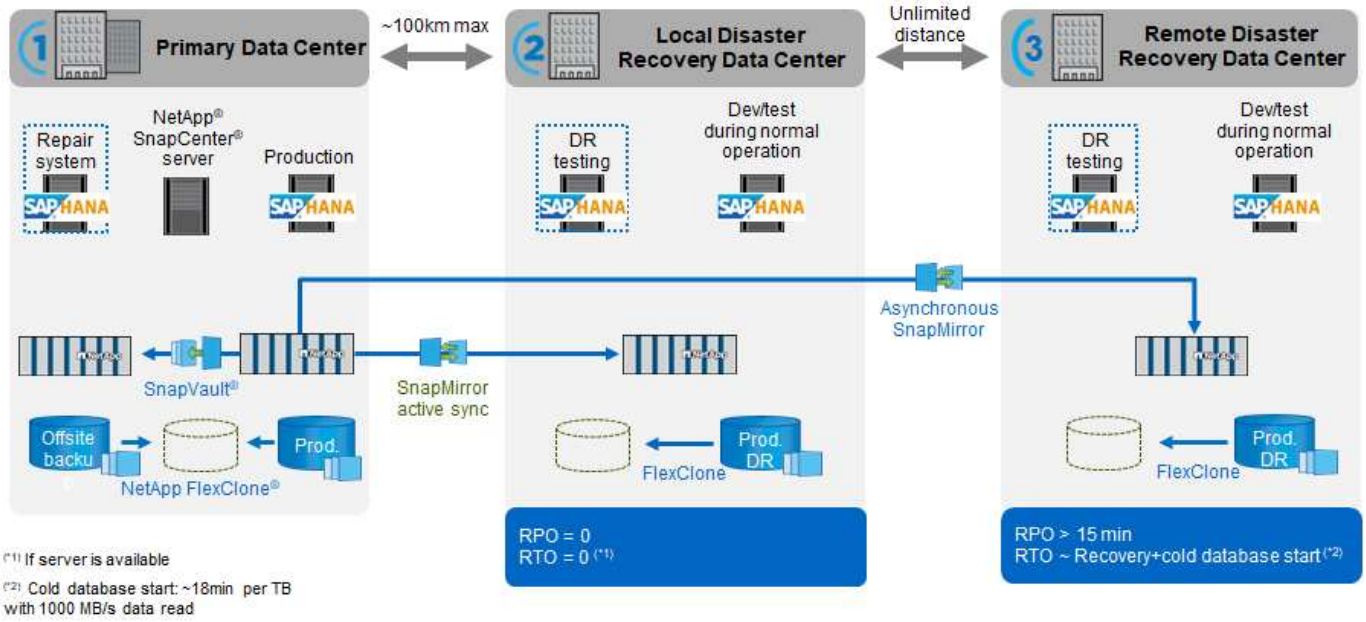
le copie di una LUN protetta con replica sincrona bidirezionale, in modo che entrambe le copie LUN possano servire le operazioni di i/o a livello locale.

Ulteriori informazioni sono disponibili all'indirizzo "Panoramica della sincronizzazione attiva di SnapMirror in ONTAP".

L'RTO per la replica asincrona di SnapMirror dipende principalmente dal tempo necessario per avviare il database HANA nel sito DR e caricare i dati nella memoria. Supponendo che i dati siano letti con un throughput di 1000 Mbps, il caricamento di 1 TB di dati richiederebbe circa 18 minuti.

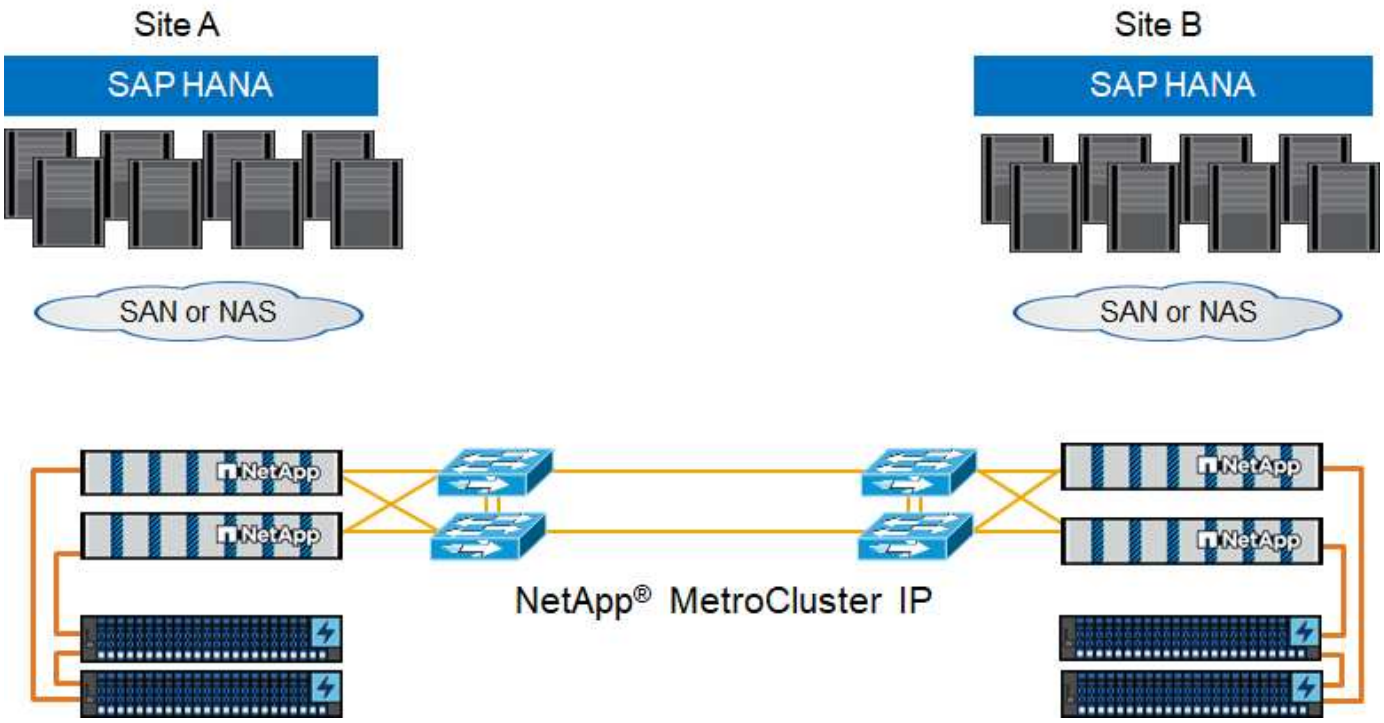
I server dei siti DR possono essere utilizzati come sistemi di sviluppo/test durante il normale funzionamento. In caso di disastro, i sistemi di sviluppo/test devono essere spenti e avviati come server di produzione DR.

Entrambi i metodi di replica consentono di eseguire test del workflow di DR senza influenzare l'RPO e l'RTO. I volumi FlexClone vengono creati sullo storage e collegati ai server di test del DR.



Replica dello storage basata su NetApp MetroCluster

La figura seguente mostra una panoramica di alto livello della soluzione. Il cluster di storage di ogni sito fornisce alta disponibilità locale e viene utilizzato per il carico di lavoro di produzione. I dati di ciascun sito vengono replicati in modo sincrono nell'altra posizione e sono disponibili in caso di failover di emergenza.



Dimensionamento dello storage

La sezione seguente fornisce una panoramica delle considerazioni relative a performance e capacità necessarie per il dimensionamento di un sistema storage per SAP HANA.

Contatta il tuo commerciale NetApp o il tuo partner NetApp per supportare il processo di dimensionamento dello storage e per aiutarti a creare un ambiente di storage di dimensioni adeguate.

Considerazioni sulle performance

SAP ha definito un set statico di indicatori di performance chiave dello storage (KPI). Questi KPI sono validi per tutti gli ambienti SAP HANA in produzione, indipendentemente dalle dimensioni della memoria degli host di database e delle applicazioni che utilizzano il database SAP HANA. Questi KPI sono validi per ambienti a host singolo, host multiplo, Business Suite su HANA, Business Warehouse su HANA, S/4HANA e BW/4HANA. Pertanto, l'attuale approccio al dimensionamento delle performance dipende solo dal numero di host SAP HANA attivi collegati al sistema storage.

I KPI relativi alle performance dello storage sono richiesti solo per i sistemi SAP HANA in produzione, ma è possibile implementarli in tutti i sistemi HANA.

SAP offre uno strumento di test delle performance che deve essere utilizzato per convalidare le performance dei sistemi storage per gli host SAP HANA attivi collegati allo storage.

NetApp ha testato e predefinito il numero massimo di host SAP HANA che possono essere collegati a un modello di storage specifico, pur continuando a soddisfare i KPI di storage richiesti da SAP per i sistemi SAP HANA basati sulla produzione.

Il numero massimo di host SAP HANA che possono essere eseguiti su uno shelf di dischi e il numero minimo

di SSD richiesti per host SAP HANA sono stati determinati eseguendo il tool di test delle performance SAP. Questo test non prende in considerazione i requisiti effettivi di capacità dello storage degli host. È inoltre necessario calcolare i requisiti di capacità per determinare l'effettiva configurazione dello storage necessaria.

Shelf di dischi SAS

Con lo shelf di dischi SAS da 12 GB (DS224C), il dimensionamento delle performance viene eseguito utilizzando configurazioni di shelf di dischi fissi:

- Shelf di dischi a metà carico con 12 SSD
- Shelf di dischi completamente caricati con 24 SSD

Entrambe le configurazioni utilizzano la partizione avanzata dei dischi (ADPv2). Uno shelf di dischi a metà carico supporta fino a 9 host SAP HANA; uno shelf a pieno carico supporta fino a 14 host in un singolo shelf di dischi. Gli host SAP HANA devono essere equamente distribuiti tra entrambi i controller di storage.

Lo shelf di dischi DS224C deve essere connesso utilizzando un SAS da 12 GB per supportare il numero di host SAP HANA.

Lo shelf di dischi SAS da 6 GB (DS2246) supporta un massimo di 4 host SAP HANA. Gli SSD e gli host SAP HANA devono essere equamente distribuiti tra entrambi i controller di storage. La figura seguente riassume il numero supportato di host SAP HANA per shelf di dischi.

	Shelf SAS da 6 GB (DS2246) con 24 SSD completamente caricati	**Shelf SAS da 12 GB (DS224C) a metà carico con 12 SSD e ADPv2**	**Shelf SAS da 12 GB (DS224C) completamente caricati con 24 SSD e ADPv2**
Numero massimo di host SAP HANA per shelf di dischi	4	9	14

Questo calcolo è indipendente dal controller di storage utilizzato. L'aggiunta di più shelf di dischi non aumenta il numero massimo di host SAP HANA supportati da uno storage controller.

Shelf NS224 NVMe

Un SSD NVMe (dati) supporta fino a 2/5 host SAP HANA a seconda del disco NVMe specifico utilizzato. Gli SSD e gli host SAP HANA devono essere equamente distribuiti tra entrambi i controller di storage. Lo stesso vale per i dischi NVMe interni dei sistemi AFF e ASA.

L'aggiunta di più shelf di dischi non aumenta il numero massimo di host SAP HANA supportati da uno storage controller.

Carichi di lavoro misti

Sono supportati SAP HANA e altri carichi di lavoro applicativi eseguiti sullo stesso storage controller o nello stesso aggregato di storage. Tuttavia, è una Best practice di NetApp separare i workload SAP HANA da tutti gli altri workload delle applicazioni.

Potresti decidere di implementare workload SAP HANA e altri workload applicativi sullo stesso storage controller o sullo stesso aggregato. In tal caso, è necessario assicurarsi che le performance di SAP HANA siano adeguate all'interno dell'ambiente di workload misto. NetApp consiglia inoltre di utilizzare i parametri

della qualità del servizio (QoS) per regolare l'effetto che queste altre applicazioni potrebbero avere sulle applicazioni SAP HANA e per garantire il throughput per le applicazioni SAP HANA.

Il tool di test SAP HCMT deve essere utilizzato per verificare se è possibile eseguire altri host SAP HANA su uno storage controller esistente già in uso per altri carichi di lavoro. I server applicativi SAP possono essere posizionati in modo sicuro sullo stesso storage controller e/o aggregato dei database SAP HANA.

Considerazioni sulla capacità

Una descrizione dettagliata dei requisiti di capacità per SAP HANA è disponibile nella "Nota SAP 1900823" white paper.

> Il dimensionamento della capacità del panorama SAP complessivo con più sistemi SAP HANA deve essere determinato utilizzando gli strumenti di dimensionamento dello storage SAP HANA di NetApp. Contatta NetApp o il tuo partner commerciale NetApp per convalidare il processo di dimensionamento dello storage per un ambiente di storage di dimensioni adeguate.

Configurazione dello strumento di test delle performance

A partire da SAP HANA 1.0 SPS10, SAP ha introdotto i parametri per regolare il comportamento di i/o e ottimizzare il database per il file e il sistema storage utilizzati. Questi parametri devono essere impostati anche per lo strumento di test delle performance di SAP quando le performance dello storage vengono testate con lo strumento di test SAP.

NetApp ha condotto test delle performance per definire i valori ottimali. La seguente tabella elenca i parametri che devono essere impostati nel file di configurazione dello strumento di test SAP.

Parametro	Valore
max_parallel_io_requests	128
async_read_submit	acceso
async_write_submit_active	acceso
async_write_submit_blocks	tutto

Per ulteriori informazioni sulla configurazione dello strumento di test SAP, vedere "Nota SAP 1943937" Per HWCCT (SAP HANA 1.0) e. "Nota SAP 2493172" PER HCMT/HCOT (SAP HANA 2.0).

Nell'esempio seguente viene illustrato come impostare le variabili per il piano di esecuzione HCMT/HCOT.

```
…
{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
```

```
         "Name": "DataAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
```

```
         "Request": "false"
      }, …
```

Queste variabili devono essere utilizzate per la configurazione del test. Questo è solitamente il caso dei piani di esecuzione predefiniti che SAP offre con lo strumento HCMT/HCOT. Il seguente esempio per un test di scrittura del log 4k è da un piano di esecuzione.

```
…
      {
         "ID": "D664D001-933D-41DE-A904F304AEB67906",
         "Note": "File System Write Test",
         "ExecutionVariants": [
            {
               "ScaleOut": {
                  "Port": "${RemotePort}",
                  "Hosts": "${Hosts}",
                  "ConcurrentExecution": "${FSConcurrentExecution}"
               },
               "RepeatCount": "${TestRepeatCount}",
               "Description": "4K Block, Log Volume 5GB, Overwrite",
               "Hint": "Log",
               "InputVector": {
                  "BlockSize": 4096,
                  "DirectoryName": "${LogVolume}",
                  "FileOverwrite": true,
                  "FileSize": 5368709120,
                  "RandomAccess": false,
                  "RandomData": true,
                  "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                  "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                  "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                  "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                  "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                  "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                  "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                  "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                  "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
               }
            },
…
```

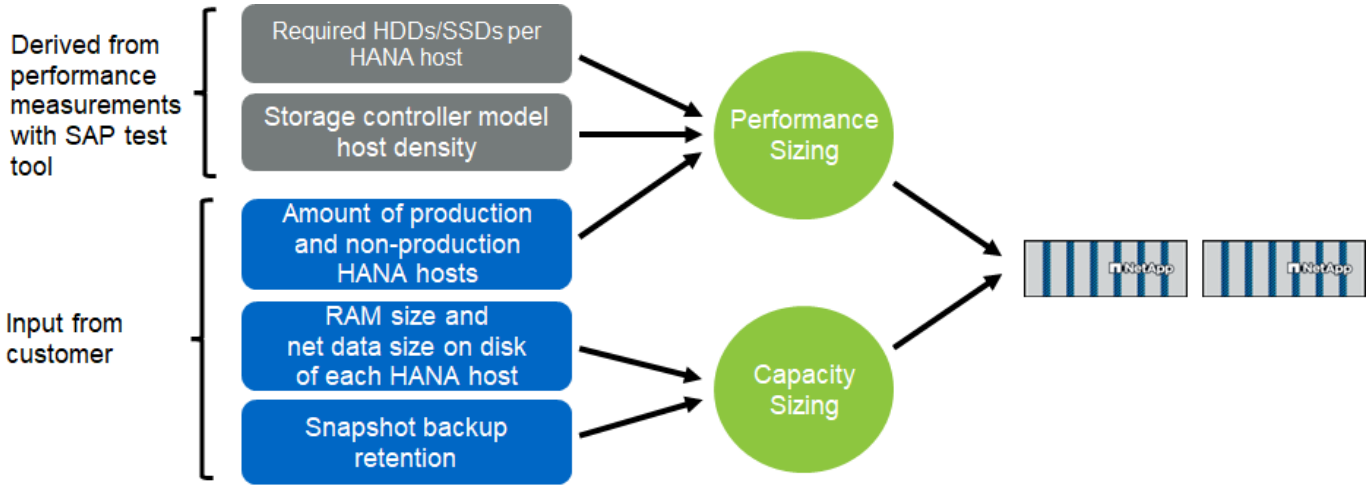
Panoramica del processo di dimensionamento dello storage

Il numero di dischi per host HANA e la densità host SAP HANA per ciascun modello di storage sono stati determinati utilizzando il tool di test SAP HANA.

Il processo di dimensionamento richiede dettagli come il numero di host SAP HANA in produzione e non in produzione, la dimensione della RAM di ciascun host e la conservazione del backup delle copie Snapshot basate sullo storage. Il numero di host SAP HANA determina il controller dello storage e il numero di dischi necessari.

La dimensione della RAM, la dimensione dei dati netti sul disco di ciascun host SAP HANA e il periodo di conservazione del backup della copia Snapshot vengono utilizzati come input durante il dimensionamento della capacità.

La figura seguente riassume il processo di dimensionamento.



Installazione e configurazione dell'infrastruttura

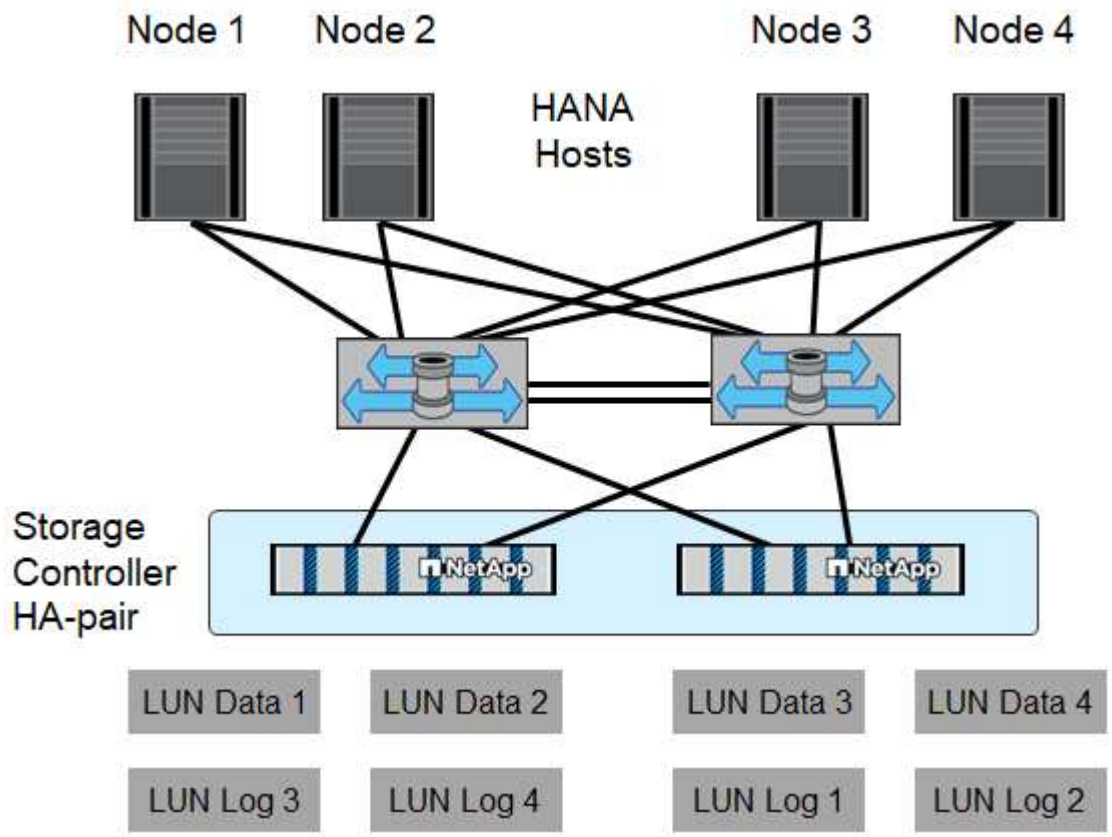
Le seguenti sezioni forniscono le linee guida per la configurazione e la configurazione dell'infrastruttura SAP HANA e descrivono tutti i passaggi necessari per configurare un sistema SAP HANA. All'interno di queste sezioni, vengono utilizzate le seguenti configurazioni di esempio:

- Sistema HANA con SID=FC5
  - Host singolo e multiplo SAP HANA che utilizza il gestore dei volumi logici Linux (LVM)
  - Host singolo SAP HANA con partizioni multiple SAP HANA

Configurazione del fabric SAN

Ogni server SAP HANA deve disporre di una connessione SAN FCP ridondante con una larghezza di banda minima di 8 Gbps. Per ogni host SAP HANA collegato a un controller di storage, è necessario configurare una larghezza di banda di almeno 8 Gbps nel controller di storage.

La figura seguente mostra un esempio con quattro host SAP HANA collegati a due storage controller. Ciascun host SAP HANA dispone di due porte FCP collegate al fabric ridondante. A livello di storage, quattro porte FCP sono configurate per fornire il throughput richiesto per ciascun host SAP HANA.



Oltre alla suddivisione in zone sul layer dello switch, è necessario mappare ogni LUN del sistema di storage agli host che si connettono a questo LUN. Mantenere lo zoning sullo switch semplice, ovvero definire un set di zone in cui tutti gli HBA host possano vedere tutti gli HBA dei controller.

Sincronizzazione dell'ora

È necessario sincronizzare l'ora tra i controller di storage e gli host del database SAP HANA. A tale scopo, impostare lo stesso server di riferimento orario per tutti i controller di storage e tutti gli host SAP HANA.

Configurazione dello storage controller

Questa sezione descrive la configurazione del sistema storage NetApp. È necessario completare l'installazione e la configurazione primaria in base alle corrispondenti guide di configurazione e configurazione di Data ONTAP.

Efficienza dello storage

La deduplica inline, la deduplica inline di più volumi, la compressione inline e la compaction inline sono supportate con SAP HANA in una configurazione SSD.

Volumi NetApp FlexGroup

L'utilizzo dei volumi NetApp FlexGroup non è supportato per SAP HANA. Grazie all'architettura di SAP HANA l'utilizzo di FlexGroup Volumes non fornisce alcun beneficio e potrebbe causare problemi di performance.

Crittografia dei volumi e degli aggregati NetApp

L'utilizzo di NetApp Volume Encryption (NVE) e NetApp aggregate Encryption (NAE) sono supportati con SAP HANA.

Qualità del servizio

La qualità del servizio può essere utilizzata per limitare il throughput dello storage per sistemi SAP HANA o applicazioni non SAP specifici su un controller condiviso.

Produzione e sviluppo/test

Un caso d'utilizzo sarebbe quello di limitare il throughput dei sistemi di sviluppo e test in modo che non possano influenzare i sistemi di produzione in una configurazione mista. Durante il processo di dimensionamento, è necessario determinare i requisiti di performance di un sistema non in produzione. I sistemi di sviluppo e test possono essere dimensionati con valori di performance inferiori, in genere nell'intervallo compreso tra il 20% e il 50% di un KPI del sistema di produzione come definito da SAP. L'i/o di scrittura di grandi dimensioni ha il maggiore effetto sulle performance del sistema storage. Pertanto, il limite di throughput QoS deve essere impostato su una percentuale dei corrispondenti valori KPI di scrittura delle performance dello storage SAP HANA nei volumi di dati e di log.

Ambienti condivisi

Un altro caso d'utilizzo consiste nel limitare il throughput dei carichi di lavoro intensivi in scrittura, soprattutto per evitare che questi carichi di lavoro abbiano un impatto su altri carichi di lavoro in scrittura sensibili alla latenza. In tali ambienti è consigliabile applicare una policy di gruppo QoS con un livello di throughput massimo non condiviso a ogni LUN all'interno di ciascuna Storage Virtual Machine (SVM) per limitare il throughput massimo di ciascun oggetto storage singolo a un valore dato. Questo riduce la possibilità che un singolo carico di lavoro possa influenzare negativamente altri carichi di lavoro.

Per fare questo, è necessario creare una policy di gruppo utilizzando l'interfaccia a riga di comando del cluster ONTAP per ogni SVM:

```
qos policy-group create -policy-group <policy-name> -vserver <vserver
name> -max-throughput 1000MB/s -is-shared false
```

E applicata a ogni LUN all'interno della SVM. Segue un esempio di applicazione del gruppo di policy a tutte le LUN esistenti all'interno di una SVM:

```
lun modify -vserver <vserver name>  -path * -qos-policy-group  <policy-
name>
```

Tutto questo è necessario per ogni SVM. Il nome del gruppo di polizia della QoS per ciascuna SVM deve essere diverso. Per i nuovi LUN, la policy può essere applicata direttamente:

```
lun create -vserver <vserver_name> -path  /vol/<volume_name>/<lun_name>
-size <size> -ostype <e.g. linux>  -qos-policy-group <policy-name>
```

Si consiglia di utilizzare 1000MB GB/s come throughput massimo per un dato LUN. Se un'applicazione

richiede maggiore throughput, verranno utilizzati più LUN con striping LUN per fornire la larghezza di banda necessaria. Questa guida fornisce un esempio per SAP HANA basato su Linux LVM nella sezione "Host Setup (impostazione host)".

> Il limite si applica anche alle letture. Pertanto, utilizza un numero sufficiente di LUN per soddisfare gli SLA richiesti per l'avvio del database SAP HANA e per i backup.

NetApp FabricPool

La tecnologia NetApp FabricPool non deve essere utilizzata per i file system primari attivi nei sistemi SAP HANA. Sono inclusi i file system per l'area dei dati e dei log, oltre a `/hana/shared` file system. In questo modo si ottengono performance imprevedibili, in particolare durante l'avvio di un sistema SAP HANA.

È possibile utilizzare il criterio di tiering Snapshot-Only insieme a FabricPool in una destinazione di backup come SnapVault o SnapMirror.

> L'utilizzo di FabricPool per tiering delle copie Snapshot nello storage primario o l'utilizzo di FabricPool in una destinazione di backup modifica il tempo necessario per il ripristino e il ripristino di un database o di altre attività, come la creazione di cloni di sistema o la riparazione di sistemi. Prenditi in considerazione questo aspetto per pianificare la tua strategia generale di gestione del ciclo di vita e verifica che gli SLA vengano ancora rispettati durante l'utilizzo di questa funzione.

FabricPool è un'ottima opzione per spostare i backup dei log in un altro Tier di storage. Lo spostamento dei backup influisce sul tempo necessario per ripristinare un database SAP HANA. Pertanto, l'opzione `tiering-minimum-cooling-days` deve essere impostato su un valore che colloca i backup dei log, normalmente necessari per il ripristino, nel tier di storage locale fast.

Configurare lo storage

La seguente panoramica riassume i passaggi necessari per la configurazione dello storage. Ogni fase viene descritta in maggiore dettaglio nelle sezioni successive. In questa sezione, si presuppone che l'hardware di storage sia configurato e che il software ONTAP sia già installato. Inoltre, la connessione delle porte FCP dello storage al fabric SAN deve essere già attiva.

1. Controllare la corretta configurazione dello scaffale del disco, come descritto inCollegamenti del ripiano del disco .
2. Creare e configurare gli aggregati richiesti, come descritto in Configurazione dell'aggregato.
3. Creare una Storage Virtual Machine (SVM), come descritto in Configurazione della macchina virtuale per lo storage.
4. Creare interfacce logiche (LIF), come descritto in Configurazione dell'interfaccia logica.
5. Creare gruppi di iniziatori (igroup) con nomi mondiali (WWN) dei server HANA come descritto nella sezione Gruppi di iniziatori .
6. Creare e configurare volumi e LUN all'interno degli aggregati come descritto nella sezione "Configurazione host singolo" per singoli host o in sezione "Configurazione host multipli"

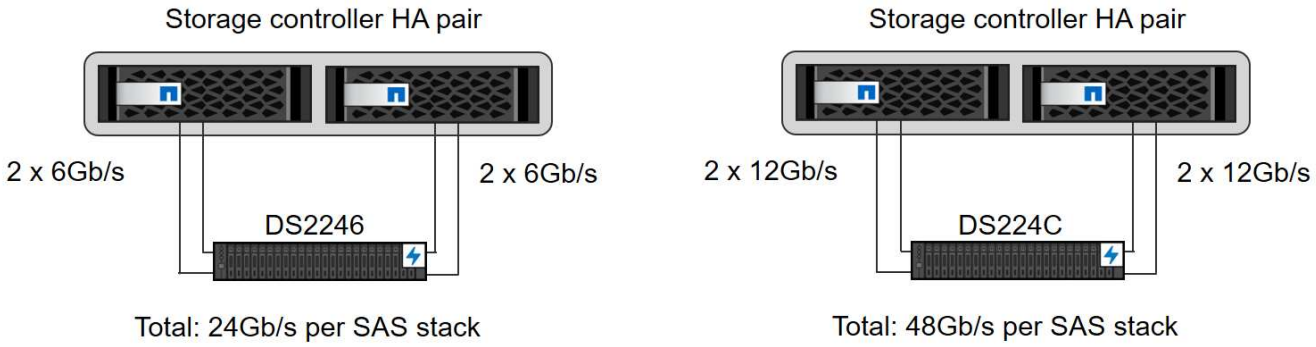
Collegamenti del ripiano del disco

Shelf di dischi basati su SAS

È possibile collegare un massimo di uno shelf di dischi a uno stack SAS per fornire le prestazioni richieste per

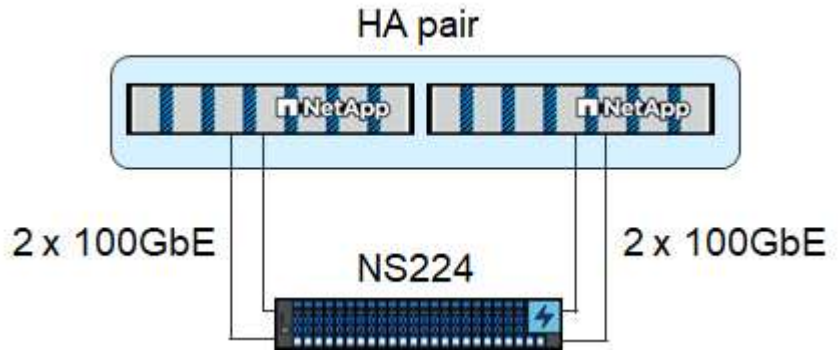
gli host SAP HANA, come mostrato nella figura seguente. I dischi all'interno di ogni shelf devono essere distribuiti in modo uguale tra entrambi i controller della coppia ha. ADPv2 viene utilizzato con ONTAP 9 e gli shelf di dischi DS224C.

Con lo shelf di dischi DS224C, è possibile utilizzare anche il cablaggio SAS quad-path, ma non è necessario.



Shelf dei dischi basati su NVMe

Ogni shelf di dischi NS224 NVMe è collegato a due porte 100GbE per controller, come illustrato nella figura seguente. I dischi all'interno di ogni shelf devono essere distribuiti in modo uguale a entrambi i controller della coppia ha. ADPv2 viene utilizzato anche per lo shelf di dischi NS224.

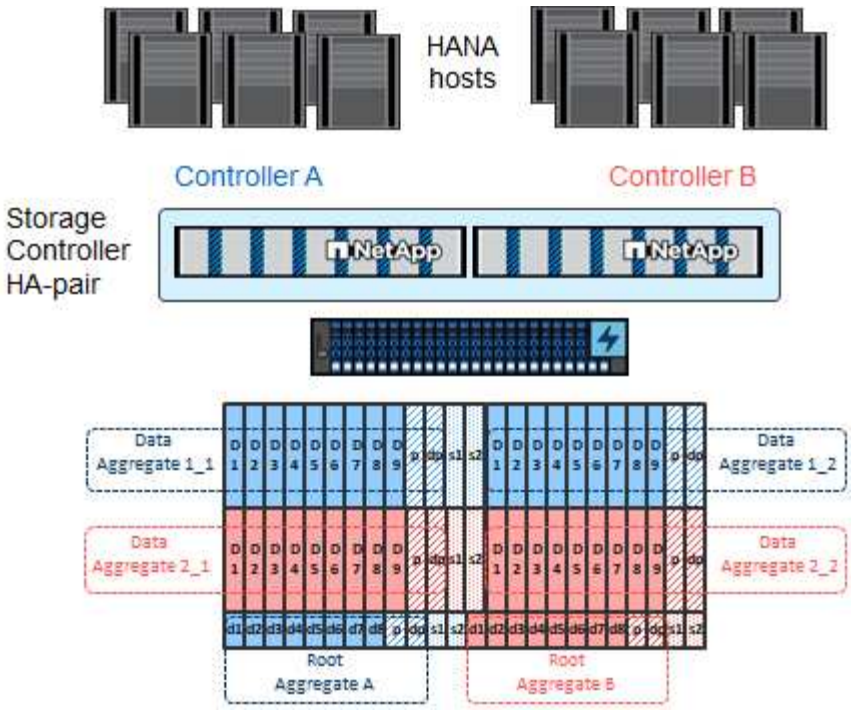


Configurazione dell'aggregato

In generale, è necessario configurare due aggregati per controller, indipendentemente da quale shelf di dischi o tecnologia di dischi (SSD o HDD) viene utilizzata. Questo passaggio è necessario per poter utilizzare tutte le risorse del controller disponibili.

I sistemi ASA lanciati dopo agosto 2024 non richiedono questo passaggio, come avviene automaticamente

La figura seguente mostra una configurazione di 12 host SAP HANA in esecuzione su uno shelf SAS da 12 GB configurato con ADPv2. Sei host SAP HANA sono collegati a ciascun controller di storage. Sono configurati quattro aggregati separati, due per ogni controller di storage. Ogni aggregato è configurato con 11 dischi con nove partizioni di dati e due di dischi di parità. Per ciascun controller sono disponibili due partizioni di riserva.



Configurazione della macchina virtuale per lo storage

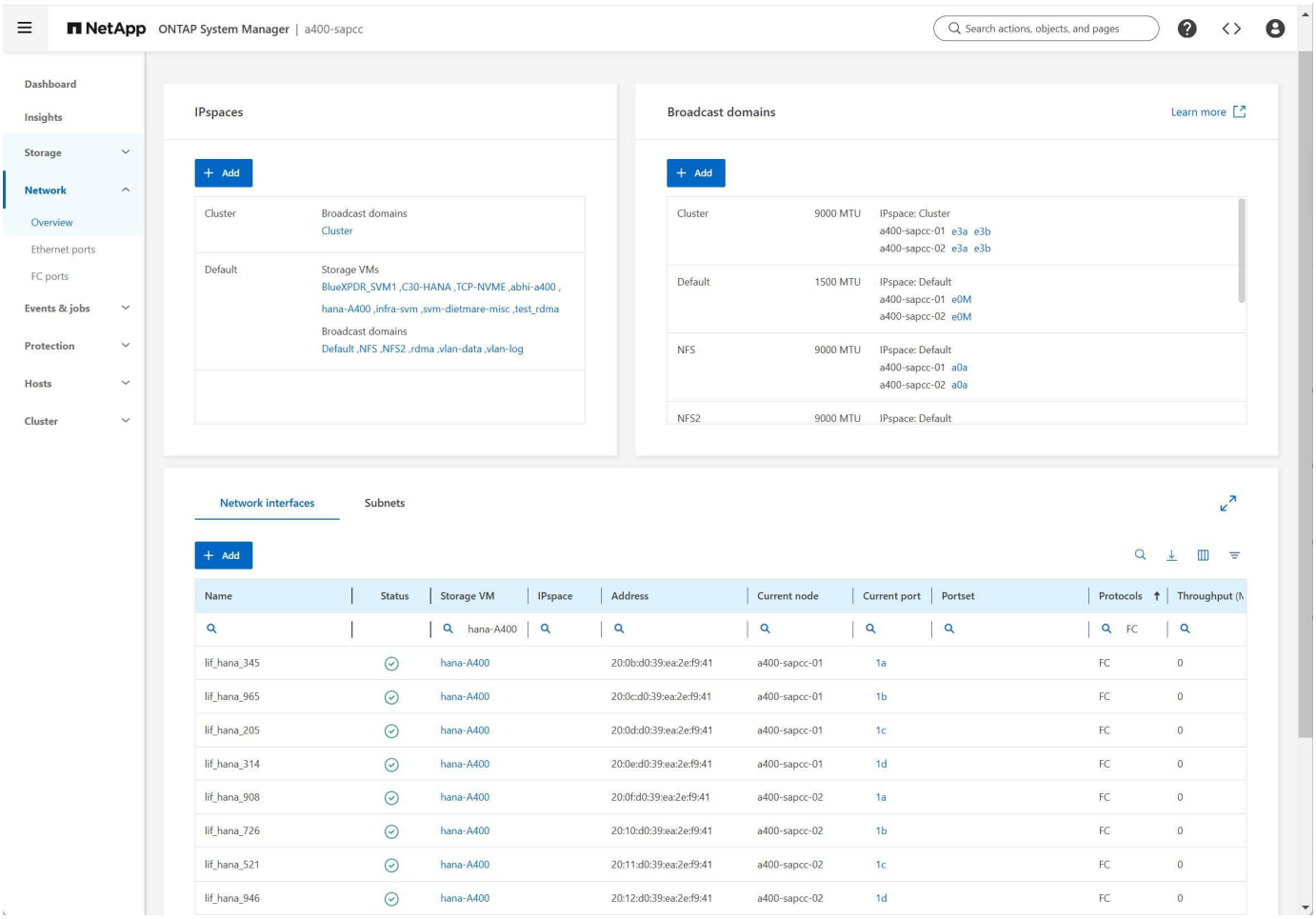
Diversi ambienti SAP con database SAP HANA possono utilizzare una singola SVM. È possibile assegnare una SVM a ciascun ambiente SAP, se necessario, nel caso in cui sia gestita da diversi team all'interno di un'azienda.

Se viene creato e assegnato automaticamente un profilo QoS durante la creazione di una nuova SVM, rimuovere questo profilo creato automaticamente dalla SVM per garantire le prestazioni richieste per SAP HANA:

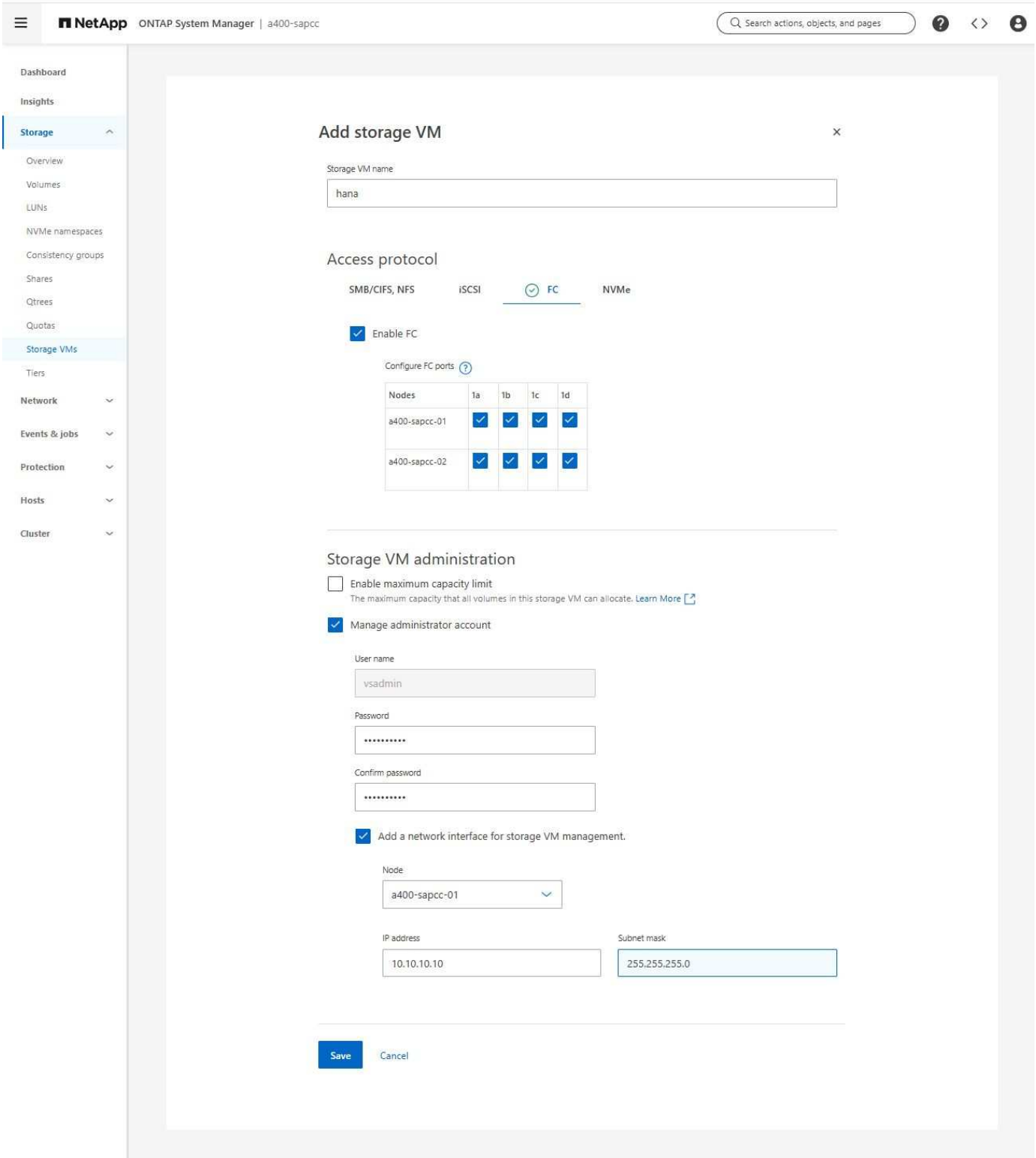
```
vserver modify -vserver <svm-name> -qos-policy-group none
```

Configurazione dell'interfaccia logica

All'interno della configurazione del cluster di storage, è necessario creare un'interfaccia di rete (LIF) e assegnarla a una porta FCP dedicata. Se, ad esempio, sono necessarie quattro porte FCP per motivi di performance, è necessario creare quattro LIF. La figura seguente mostra uno screenshot degli otto LIF configurati nella SVM.



Durante la creazione delle SVM con ONTAP System Manager, è possibile selezionare tutte le porte FCP fisiche richieste e creare automaticamente una LIF per porta fisica.



Gruppi di iniziatori

È possibile configurare un igroup per ciascun server o per un gruppo di server che richiedono l'accesso a un LUN. La configurazione di igroup richiede i nomi delle porte mondiali (WWPN) dei server.

Utilizzando il `sanlun` Eseguire il seguente comando per ottenere le WWPN di ciascun host SAP HANA:

```
stlrx300s8-6:~ # sanlun fcp show adapter
/sbin/udevadm
/sbin/udevadm

host0 ..... WWPN:2100000e1e163700
host1 ..... WWPN:2100000e1e163701
```

`sanlun`Lo strumento fa parte delle utilità host NetApp e deve essere installato su ogni host SAP HANA. Ulteriori dettagli sono disponibili nella sezione "Configurazione dell'host."

I gruppi iniziatori possono essere creati utilizzando l'interfaccia CLI del cluster ONTAP.

```
lun igroup create -igroup <igroup name> -protocol fcp -ostype linux
-initiator <list of initiators> -vserver <SVM name>
```

Host singolo

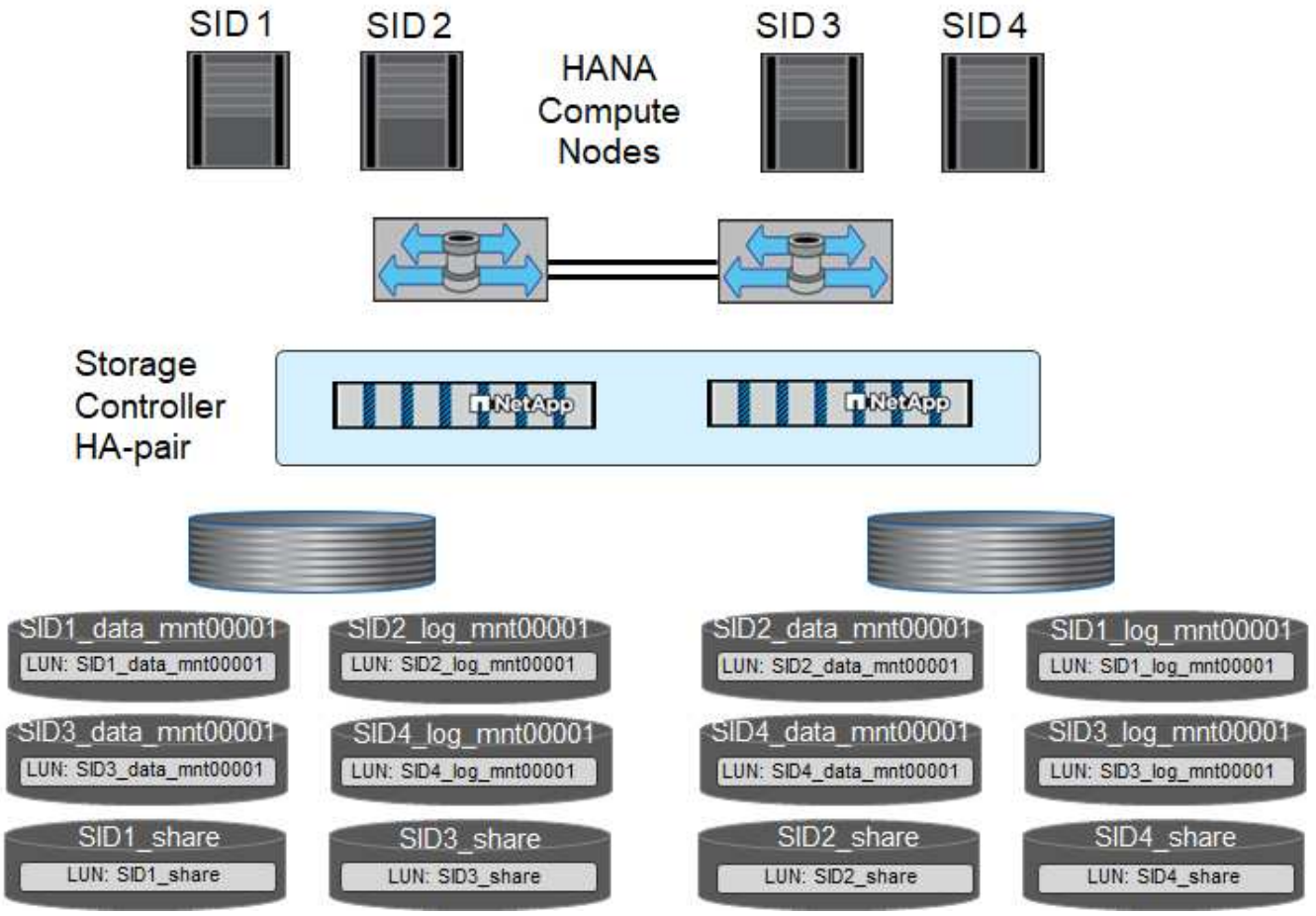
Host singolo

Questa sezione descrive la configurazione del sistema di archiviazione NetApp specifico per i sistemi SAP HANA a host singolo

Configurazione di volumi e LUN per sistemi SAP HANA a host singolo

La figura seguente mostra la configurazione dei volumi di quattro sistemi SAP HANA a host singolo. I volumi di dati e log di ciascun sistema SAP HANA vengono distribuiti a diversi storage controller. Ad esempio, volume `SID1_data_mnt00001` È configurato sul controller A e sul volume `SID1_log_mnt00001` È configurato sul controller B. All'interno di ciascun volume viene configurato un singolo LUN.

Se per i sistemi SAP HANA viene utilizzato un solo storage controller di una coppia ha, i volumi di dati e i volumi di log possono anche essere memorizzati nello stesso storage controller.



Per ogni host SAP HANA, un volume di dati, un volume di log e un volume per `/hana/shared` sono configurati. La seguente tabella mostra una configurazione di esempio con quattro sistemi SAP HANA a host singolo.

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Dati, log e volumi condivisi per il sistema SID1	Volume di dati: SID1_data_mnt00001	Volume condiviso: SID1_shared	–	Volume di log: SID1_log_mnt00001
Dati, log e volumi condivisi per il sistema SID2	–	Volume di log: SID2_log_mnt00001	Volume di dati: SID2_data_mnt00001	Volume condiviso: SID2_shared
Dati, log e volumi condivisi per il sistema SID3	Volume condiviso: SID3_shared	Volume di dati: SID3_data_mnt00001	Volume di log: SID3_log_mnt00001	–
Dati, log e volumi condivisi per il sistema SID4	Volume di log: SID4_log_mnt00001	–	Volume condiviso: SID4_shared	Volume di dati: SID4_data_mnt00001

La seguente tabella mostra un esempio di configurazione del punto di montaggio per un sistema a host singolo.

LUN	Punto di montaggio sull'host SAP HANA	Nota
SID1_data_mnt00001	/hana/data/SID1/mnt00001	Montato usando /etc/fstab entry
SID1_log_mnt00001	/hana/log/SID1/mnt00001	Montato usando /etc/fstab entry
SID1_shared	/hana/shared/SID1	Montato usando /etc/fstab entry

Con la configurazione descritta, il `/usr/sap/SID1` La directory in cui è memorizzata la home directory predefinita dell'utente SID1adm si trova sul disco locale. In una configurazione di disaster recovery con replica basata su disco, NetApp consiglia di creare un LUN aggiuntivo all'interno di `SID1_shared` volume per `/usr/sap/SID1` directory in modo che tutti i file system si trovino nello storage centrale.

Configurazione di volumi e LUN per sistemi SAP HANA a host singolo che utilizzano Linux LVM

Linux LVM può essere utilizzato per aumentare le performance e risolvere i limiti delle dimensioni del LUN. Le diverse LUN di un gruppo di volumi LVM devono essere memorizzate in un aggregato diverso e in un controller diverso. La seguente tabella mostra un esempio di due LUN per gruppo di volumi.

Non è necessario utilizzare LVM con più LUN per soddisfare i KPI di SAP HANA, ma è consigliato.

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Dati, log e volumi condivisi per sistemi basati su LVM	Volume di dati: SID1_data_mnt00001	Volume condiviso: Volume SID1_shared log2: SID1_log2_mnt00001	Volume Data2: SID1_data2_mnt00001	Volume di log: SID1_log_mnt00001

Opzioni del volume

Le opzioni del volume elencate nella tabella seguente devono essere verificate e impostate su tutti i volumi utilizzati per SAP HANA.

Azione	ONTAP 9
Disattivare le copie Snapshot automatiche	vol modify –vserver <vserver-name> -volume <volname> -snapshot-policy none
Disattiva la visibilità della directory Snapshot	vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false

Creazione di LUN e mappatura delle LUN ai gruppi di iniziatori tramite la CLI

Questa sezione mostra un esempio di configurazione mediante la riga di comando con ONTAP 9 per un sistema host singolo SAP HANA con SID FC5 mediante LVM e due LUN per gruppo di volumi LVM:

1. Creare tutti i volumi necessari.

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. Creare tutte le LUN.

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. Creare il gruppo iniziatore per tutte le porte appartenenti agli host sythe di FC5.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb -vserver hana
```

4. Mappare tutti i LUN al gruppo iniziatore creato.

```
lun map -path /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
```


Più host

Questa sezione descrive la configurazione del sistema di archiviazione NetApp specifico per i sistemi multi-host SAP HANA

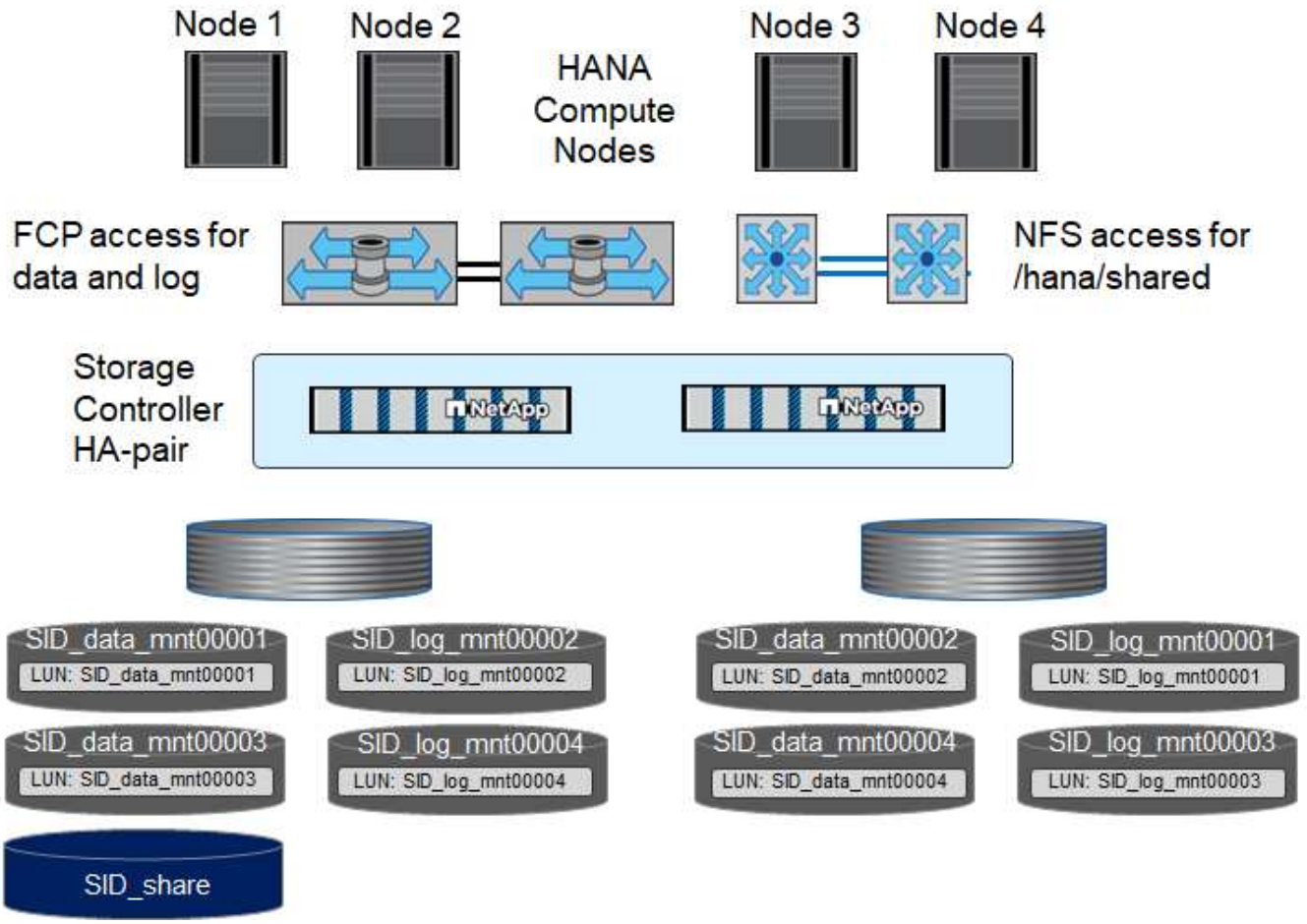
Configurazione di volumi e LUN per sistemi SAP HANA con host multipli

La figura seguente mostra la configurazione di un volume di un sistema SAP HANA 4+1 multihost. I volumi di dati e i volumi di log di ciascun host SAP HANA vengono distribuiti a diversi storage controller. Ad esempio, il volume `SID_data_mnt00001` È configurato sul controller A e sul volume `SID_log_mnt00001` È configurato sul controller B. Viene configurato un LUN per ciascun volume.

Il `/hana/shared` Il volume deve essere accessibile da tutti gli host HANA e viene quindi esportato utilizzando NFS. Anche se non sono disponibili KPI specifici per le performance per `/hana/shared` File system, NetApp consiglia di utilizzare una connessione Ethernet a 10 GB.

Se per il sistema SAP HANA viene utilizzato un solo storage controller di una coppia ha, i volumi di dati e log possono essere memorizzati anche sullo stesso storage controller.

I sistemi NetApp ASA non supportano NFS come protocollo. NetApp consiglia di utilizzare un sistema AFF o FAS aggiuntivo per `/hana/shared` sistema di file.



Per ogni host SAP HANA, vengono creati un volume di dati e un volume di log. Il `/hana/shared` Il volume viene utilizzato da tutti gli host del sistema SAP HANA. La seguente tabella mostra una configurazione di esempio per un sistema SAP HANA 4+1 a host multiplo.

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Volumi di dati e log per il nodo 1	Volume di dati: SID_data_mnt00001	–	Volume di log: SID_log_mnt00001	–
Volumi di dati e log per il nodo 2	Volume di log: SID_log_mnt00002	–	Volume di dati: SID_data_mnt00002	–
Volumi di dati e log per il nodo 3	–	Volume di dati: SID_data_mnt00003	–	Volume di log: SID_log_mnt00003
Volumi di dati e log per il nodo 4	–	Volume di log: SID_log_mnt00004	–	Volume di dati: SID_data_mnt00004
Volume condiviso per tutti gli host	Volume condiviso: SID_shared	–	–	–

La seguente tabella mostra la configurazione e i punti di montaggio di un sistema a più host con quattro host SAP HANA attivi.

LUN o volume	Punto di montaggio sull'host SAP HANA	Nota
LUN: SID_data_mnt00001	/hana/data/SID/mnt00001	Montato utilizzando un connettore storage
LUN: SID_log_mnt00001	/hana/log/SID/mnt00001	Montato utilizzando un connettore storage
LUN: SID_data_mnt00002	/hana/data/SID/mnt00002	Montato utilizzando un connettore storage
LUN: SID_log_mnt00002	/hana/log/SID/mnt00002	Montato utilizzando un connettore storage
LUN: SID_data_mnt00003	/hana/data/SID/mnt00003	Montato utilizzando un connettore storage
LUN: SID_log_mnt00003	/hana/log/SID/mnt00003	Montato utilizzando un connettore storage
LUN: SID_data_mnt00004	/hana/data/SID/mnt00004	Montato utilizzando un connettore storage
LUN: SID_log_mnt00004	/hana/log/SID/mnt00004	Montato utilizzando un connettore storage
Volume: SID_shared	/hana/shared	Montato su tutti gli host usando NFS e /etc/fstab entry

Con la configurazione descritta, il `/usr/sap/SID` La directory in cui è memorizzata la home directory predefinita di user sidadm si trova sul disco locale di ciascun host HANA. In una configurazione di disaster recovery con replica basata su disco, NetApp consiglia di creare altre quattro sottodirectory in `SID_shared` volume per `/usr/sap/SID` file system in modo che ogni host di database disponga di tutti i file system sullo storage centrale.

Configurazione di volumi e LUN per sistemi SAP HANA con host multipli che utilizzano Linux LVM

Linux LVM può essere utilizzato per aumentare le performance e risolvere i limiti delle dimensioni del LUN. Le diverse LUN di un gruppo di volumi LVM devono essere memorizzate in un aggregato diverso e in un controller diverso.

Non è necessario utilizzare LVM per combinare più LUN per soddisfare i KPI di SAP HANA, ma è consigliato

La seguente tabella mostra un esempio di due LUN per gruppo di volumi per un sistema host multiplo SAP HANA 2+1.

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Volumi di dati e log per il nodo 1	Volume di dati: SID_data_mnt00001	Volume log2: SID_log2_mnt00001	Volume di log: SID_log_mnt00001	Volume Data2: SID_data2_mnt00001

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Volumi di dati e log per il nodo 2	Volume log2: SID_log2_mnt00002	Volume di dati: SID_data_mnt00002	Volume Data2: SID_data2_mnt00002	Volume di log: SID_log_mnt00002
Volume condiviso per tutti gli host	Volume condiviso: SID_shared	–	–	–

Opzioni del volume

Le opzioni dei volumi elencate nella tabella seguente devono essere verificate e impostate su tutte le SVM.

Azione	
Disattivare le copie Snapshot automatiche	vol modify –vserver <vserver-name> -volume <volname> -snapshot-policy none
Disattiva la visibilità della directory Snapshot	vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false

Creazione di LUN, volumi e mappatura delle LUN ai gruppi di iniziatori

Puoi utilizzare NetApp ONTAP System Manager per creare volumi di storage e LUN e associarli agli igroup dei server e all'interfaccia a riga di comando di ONTAP. In questa guida viene descritto l'utilizzo della CLI.

Creazione di LUN, volumi e mappatura delle LUN ai gruppi di iniziatori mediante la CLI

Questa sezione mostra un esempio di configurazione utilizzando la riga di comando con ONTAP 9 per un sistema host 2+1 SAP HANA con SID FC5 utilizzando LVM e due LUN per gruppo di volumi LVM:

1. Creare tutti i volumi necessari.

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00002  -aggregate aggr2_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data_mnt00002  -aggregate aggr2_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00002  -aggregate aggr2_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_data2_mnt00002  -aggregate aggr2_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. Creare tutte le LUN.

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data_mnt00002/FC5_data_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00002/FC5_log_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. Creare il gruppo iniziatore per tutti i server appartenenti al sistema FC5.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator
10000090fadcc5fa,10000090fadcc5fb,10000090fadcc5c1,10000090fadcc5c2,1000
0090fadcc5c3,10000090fadcc5c4 -vserver hana
```

4. Mappare tutti i LUN al gruppo iniziatore creato.

```
lun map -path /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_data_mnt00002/FC5_data_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log_mnt00002/FC5_log_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002  -igroup HANA-FC5
```

API di SAP HANA storage Connector

Un connettore di storage è richiesto solo in ambienti con più host dotati di funzionalità di failover. In configurazioni con più host, SAP HANA offre funzionalità ad alta disponibilità in modo che un host di database SAP HANA possa eseguire il failover su un host in standby.

In questo caso, l'host di standby accede e utilizza i LUN dell'host guasto. Il connettore di storage viene utilizzato per garantire l'accesso attivo a una partizione di storage da parte di un solo host di database alla volta.

Nelle configurazioni di host multipli SAP HANA con storage NetApp, viene utilizzato il connettore di storage standard fornito da SAP. La "SAP HANA Fibre Channel Storage Connector Admin Guide" è disponibile come allegato a. "Nota SAP 1900823".

Configurazione dell'host

Prima di configurare l'host, è necessario scaricare le utility host NETAPP SAN da "Supporto NetApp" E installato sui server HANA. La documentazione dell'utility host include informazioni sul software aggiuntivo che deve essere installato in base all'HBA FCP utilizzato.

La documentazione contiene anche informazioni sulle configurazioni multipath specifiche per la versione di Linux utilizzata. Questo documento illustra le procedure di configurazione richieste per SLES 12 SP1 o versione successiva e RHEL 7. 2 o successiva, come descritto nella "Guida all'installazione e all'installazione di Linux host Utilities 7.1".

Configurare il multipathing

> ⓘ I passaggi da 1 a 6 devono essere eseguiti su tutti gli host worker e standby in una configurazione multi-host SAP HANA.

Per configurare il multipathing, attenersi alla seguente procedura:

1. Eseguire Linux `rescan-scsi-bus.sh -a` Su ciascun server per rilevare nuove LUN.

2. Esegui il `sanlun lun show` comando e verificare che tutti i LUN richiesti siano visibili. L'esempio seguente mostra il `sanlun lun show` Output del comando per un sistema HANA multi-host 2+1 con due LUN di dati e due LUN di log. L'output mostra le LUN e i file di dispositivo corrispondenti, come LUN `FC5_data_mnt00001` e il file del dispositivo `/dev/sdag` Ogni LUN ha otto percorsi FC dall'host ai controller di archiviazione.

```
sapcc-hana-tst:~ # sanlun lun show
controller(7mode/E-Series)/                                    device
host                  lun
vserver(cDOT/FlashRay)        lun-pathname                     filename
adapter    protocol   size    product
------------------------------------------------------------------------
---------------------------------------
svm1                          FC5_log2_mnt00002                /dev/sdbb
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdba
host21     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001                /dev/sdaz
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001                 /dev/sday
host21     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002               /dev/sdax
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002                /dev/sdaw
host21     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001               /dev/sdav
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001                /dev/sdau
host21     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002                /dev/sdat
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdas
host21     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001                /dev/sdar
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001                 /dev/sdaq
host21     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002               /dev/sdap
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002                /dev/sdao
host21     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001               /dev/sdan
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001                /dev/sdam
host21     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002                /dev/sdal
```

```
host20     FCP        500g    cDOT
svm1                          FC5_log_mnt00002              /dev/sdak
host20     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001             /dev/sdaj
host20     FCP        500g    cDOT
svm1                          FC5_log_mnt00001              /dev/sdai
host20     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002            /dev/sdah
host20     FCP        1t      cDOT
svm1                          FC5_data_mnt00002             /dev/sdag
host20     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001            /dev/sdaf
host20     FCP        1t      cDOT
svm1                          FC5_data_mnt00001             /dev/sdae
host20     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002             /dev/sdad
host20     FCP        500g    cDOT
svm1                          FC5_log_mnt00002              /dev/sdac
host20     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001             /dev/sdab
host20     FCP        500g    cDOT
svm1                          FC5_log_mnt00001              /dev/sdaa
host20     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002            /dev/sdz
host20     FCP        1t      cDOT
svm1                          FC5_data_mnt00002             /dev/sdy
host20     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001            /dev/sdx
host20     FCP        1t      cDOT
svm1                          FC5_data_mnt00001             /dev/sdw
host20     FCP        1t      cDOT
```

3. Esegui il `multipath -r` E `multipath -ll` comando per ottenere gli identificatori mondiali (WWID) per i nomi dei file del dispositivo.

   In questo esempio ci sono otto LUN.

```
sapcc-hana-tst:~ # multipath -r
sapcc-hana-tst:~ # multipath -ll
3600a098038314e63492b59326b4b786d dm-7 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
```

```
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
3600a098038314e63492b59326b4b786e dm-9 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
3600a098038314e63492b59326b4b786f dm-11 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
3600a098038314e63492b59326b4b7870 dm-13 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
3600a098038314e63532459326d495a64 dm-6 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
3600a098038314e63532459326d495a65 dm-8 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
3600a098038314e63532459326d495a66 dm-10 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
```

```
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
3600a098038314e63532459326d495a67 dm-12 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

4. Modificare il `/etc/multipath.conf` File e aggiungere i WWID e i nomi degli alias.

> L'output di esempio mostra il contenuto di `/etc/multipath.conf` File, che include nomi alias per le quattro LUN di un sistema a più host 2+1. Se non è disponibile alcun file multipath.conf, è possibile crearne uno eseguendo il seguente comando: `multipath -T > /etc/multipath.conf`.

```
sapcc-hana-tst:/ # cat /etc/multipath.conf
multipaths {
                multipath {
                wwid    3600a098038314e63492b59326b4b786d
                alias   svm1-FC5_data2_mnt00001
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786e
                alias   svm1-FC5_data2_mnt00002
        }
        multipath {
                wwid    3600a098038314e63532459326d495a64
                alias   svm1-FC5_data_mnt00001
        }
        multipath {
                wwid    3600a098038314e63532459326d495a65
                alias   svm1-FC5_data_mnt00002
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786f
                alias   svm1-FC5_log2_mnt00001
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b7870
                alias   svm1-FC5_log2_mnt00002
        }
        multipath {
                wwid    3600a098038314e63532459326d495a66
                alias   svm1-FC5_log_mnt00001
        }
        multipath {
                wwid    3600a098038314e63532459326d495a67
                alias   svm1-FC5_log_mnt00002
        }


}
```

5. Eseguire `multipath -r` comando per ricaricare la mappa del dispositivo.
6. Verificare la configurazione eseguendo `multipath -ll` Per elencare tutti i LUN, i nomi degli alias e i percorsi attivi e di standby.

> Il seguente esempio di output mostra l'output di un sistema HANA 2+1 multihost con due LUN di dati e due di log.

```
sapcc-hana-tst:~ # multipath -ll
hsvm1-FC5_data2_mnt00001 (3600a098038314e63492b59326b4b786d) dm-7
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
svm1-FC5_data2_mnt00002 (3600a098038314e63492b59326b4b786e) dm-9
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
svm1-FC5_data_mnt00001 (3600a098038314e63532459326d495a64) dm-6
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
svm1-FC5_data_mnt00002 (3600a098038314e63532459326d495a65) dm-8
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
svm1-FC5_log2_mnt00001 (3600a098038314e63492b59326b4b786f) dm-11
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
```

```
svm1-FC5_log2_mnt00002 (3600a098038314e63492b59326b4b7870) dm-13
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
svm1-FC5_log_mnt00001 (3600a098038314e63532459326d495a66) dm-10
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
svm1-FC5_log_mnt00002 (3600a098038314e63532459326d495a67) dm-12
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

Configurazione host singolo

Configurazione host singolo

In questo capitolo viene descritta la configurazione di un singolo host SAP HANA utilizzando LINUX LVM.

Configurazione LUN per sistemi SAP HANA a host singolo

Nell'host SAP HANA, è necessario creare e montare gruppi di volumi e volumi logici, come indicato nella tabella seguente.

Volume logico/LUN	Punto di montaggio sull'host SAP HANA	Nota
LV: FC5_data_mnt0000-vol	/hana/data/FC51/mnt00001	Montato usando /etc/fstab entry
LV: FC5_log_mnt00001-vol	/hana/log/FC5/mnt00001	Montato usando /etc/fstab entry
LUN: FC5_shared	/hana/shared/FC5	Montato usando /etc/fstab entry

Con la configurazione descritta, il `/usr/sap/FC5` la directory in cui è memorizzata la directory home predefinita dell'utente FC5adm si trova sul disco locale. In una configurazione di disaster recovery con replica basata su disco, NetApp consiglia di creare un LUN aggiuntivo all'interno di `FC5_shared` volume per il `/usr/sap/FC5` directory in modo che tutti i file system siano nella memoria centrale.

Creare gruppi di volumi LVM e volumi logici

1. Inizializzare tutti i LUN come volume fisico.

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001
```

2. Creare i gruppi di volumi per ciascuna partizione di dati e log.

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
```

3. Creare un volume logico per ciascuna partizione di dati e log. Utilizzare una dimensione dello stripe uguale al numero di LUN utilizzati per gruppo di volumi (in questo esempio, due) e una dimensione dello stripe di 256k per i dati e 64k per il registro. SAP supporta un solo volume logico per gruppo di volumi.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Eseguire la scansione dei volumi fisici, dei gruppi di volumi e dei gruppi di volumi di tutti gli altri host.

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

Se questi comandi non trovano i volumi, è necessario riavviare il sistema.

Per montare i volumi logici, è necessario attivare i volumi logici. Per attivare i volumi, eseguire il seguente comando:

```
vgchange -a y
```

Creare file system

Creare il file system XFS su tutti i volumi logici di dati e log e sulla LUN condivisa hana.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs /dev/mapper/svm1-FC5_shared
```

Creare punti di montaggio

Creare le directory dei punti di montaggio richiesti e impostare le autorizzazioni sull'host del database:

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod –R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod –R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

Montare i file system

Per montare i file system durante l'avvio del sistema utilizzando `/etc/fstab` file di configurazione, aggiungere i file system richiesti al `/etc/fstab` file di configurazione:

```
# cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/FC5_log_mnt00001-vol /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/FC5_data_mnt00001-vol /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
```

I file system XFS per i LUN di dati e log devono essere montati con `relatime` e. `inode64` opzioni di montaggio.

Per montare i file system, eseguire il comando `mount –a` comando sull'host.

Configurazione di più host

Configurazione di più host

In questo capitolo viene descritta a titolo di esempio la configurazione di un sistema multihost SAP HANA 2+1.

Configurazione LUN per sistemi multi-host SAP HANA

Nell'host SAP HANA, è necessario creare e montare gruppi di volumi e volumi logici, come indicato nella tabella seguente.

Volume logico (LV) o volume	Punto di montaggio sull'host SAP HANA	Nota
LV: FC5_data_mnt00001-vol	/hana/data/FC5/mnt00001	Montato utilizzando un connettore storage
LV: FC5_log_mnt00001-vol	/hana/log/FC5/mnt00001	Montato utilizzando un connettore storage
LV: FC5_data_mnt00002-vol	/hana/data/FC5/mnt00002	Montato utilizzando un connettore storage
LV: FC5_log_mnt00002-vol	/hana/log/FC5/mnt00002	Montato utilizzando un connettore storage
Volume: FC5_shared	/hana/shared	Montato su tutti gli host usando NFS e /etc/fstab entry

Con la configurazione descritta, il `/usr/sap/FC5` La directory in cui è memorizzata la directory home predefinita dell'utente FC5adm si trova sul disco locale di ciascun host HANA. In una configurazione di disaster recovery con replica basata su disco, NetApp consiglia di creare quattro sottodirectory aggiuntive in `FC5_shared` volume per il `/usr/sap/FC5` file system in modo che ogni host del database abbia tutti i suoi file system sullo storage centrale.

Creare gruppi di volumi LVM e volumi logici

1. Inizializzare tutti i LUN come volume fisico.

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001
pvcreate /dev/mapper/hana-FC5_data_mnt00002
pvcreate /dev/mapper/hana-FC5_data2_mnt00002
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001
pvcreate /dev/mapper/hana-FC5_log_mnt00002
pvcreate /dev/mapper/hana-FC5_log2_mnt00002
```

2. Creare i gruppi di volumi per ciascuna partizione di dati e log.

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_data_mnt00002 /dev/mapper/hana-FC5_data_mnt00002
/dev/mapper/hana-FC5_data2_mnt00002
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
vgcreate FC5_log_mnt00002 /dev/mapper/hana-FC5_log_mnt00002
/dev/mapper/hana-FC5_log2_mnt00002
```

3. Creare un volume logico per ciascuna partizione di dati e log. Utilizzare una dimensione dello stripe uguale al numero di LUN utilizzati per gruppo di volumi (in questo esempio, due) e una dimensione dello stripe di 256k per i dati e 64k per il registro. SAP supporta un solo volume logico per gruppo di volumi.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Eseguire la scansione dei volumi fisici, dei gruppi di volumi e dei gruppi di volumi di tutti gli altri host.

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

Se questi comandi non trovano i volumi, è necessario riavviare il sistema.

Per montare i volumi logici, è necessario attivare i volumi logici. Per attivare i volumi, eseguire il seguente comando:

```
vgchange -a y
```

Creare file system

Creare il file system XFS su tutti i volumi logici di dati e log.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_data_mnt00002-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs FC5_log_mnt00002-vol
```

Creare punti di montaggio

Crea le directory dei punti di montaggio richiesti e imposta le autorizzazioni su tutti gli host worker e standby:

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod -R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod -R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

Montare i file system

Per montare il `/hana/shared` file system durante l'avvio del sistema utilizzando `/etc/fstab` file di configurazione, aggiungere il `/hana/shared` file system al `/etc/fstab` file di configurazione di ciascun host.

```
sapcc-hana-tst:/ # cat /etc/fstab
<storage-ip>:/hana_shared /hana/shared nfs rw,vers=3,hard,timeo=600,
intr,noatime,nolock 0 0
```

Tutti i file system di log e dati vengono montati tramite il connettore storage SAP HANA.

Per montare i file system, eseguire `mount -a` su ciascun host.

Configurazione dello stack di i/o per SAP HANA

A partire da SAP HANA 1.0 SPS10, SAP ha introdotto i parametri per regolare il comportamento di i/o e ottimizzare il database per il file e il sistema storage utilizzati.

NetApp ha condotto test delle performance per definire i valori ideali. La seguente tabella elenca i valori ottimali dedotti dai test delle prestazioni.

Parametro	Valore
max_parallel_io_requests	128
async_read_submit	acceso
async_write_submit_active	acceso
async_write_submit_blocks	tutto

Per i sistemi da SAP HANA 1.0 a SPS12, questi parametri possono essere impostati durante l'installazione del database SAP HANA, come descritto nella nota SAP "2267798 – Configurazione del database SAP HANA durante l'installazione con hdbparam".

In alternativa, è possibile impostare i parametri dopo l'installazione del database SAP HANA utilizzando `hdbparam` framework.

```
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_read_submit=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

A partire da SAP HANA 2.0, `hdbparam` è obsoleto e i parametri vengono spostati su `global.ini` file. I parametri possono essere impostati utilizzando i comandi SQL o SAP HANA Studio. Per ulteriori informazioni, fare riferimento alla nota SAP "2399079: Eliminazione di hdbparam in HANA 2". I parametri possono essere impostati anche all'interno di `global.ini` file.

```
SS3adm@stlrx300s8-6: /usr/sap/SS3/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

Per SAP HANA 2.0 SPS5 e versioni successive, utilizzare `setParameter.py` script per impostare i parametri corretti.

```
fc5adm@sapcc-hana-tst-03:/usr/sap/FC5/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

Installazione del software SAP HANA

Questa sezione descrive la preparazione necessaria per installare SAP HANA su sistemi a host singolo e su sistemi a più host.

Installazione su sistema a host singolo

L'installazione del software SAP HANA non richiede alcuna preparazione aggiuntiva per un sistema a singolo host.

Installazione su sistemi a più host

Prima di iniziare l'installazione, creare un `global.ini` File per abilitare l'utilizzo di SAP Storage Connector durante il processo di installazione. Il connettore di storage SAP monta i file system richiesti sugli host di lavoro durante il processo di installazione. Il `global.ini` il file deve essere disponibile in un file system accessibile da tutti gli host, ad esempio `/hana/shared` file system.

Prima di installare il software SAP HANA su un sistema a più host, è necessario completare la seguente procedura:

1. Aggiungere le seguenti opzioni di montaggio per i LUN dei dati e i LUN del registro a `global.ini` file:
   - `relatime` e. `inode64` per il file system di dati e log
2. Aggiungere i WWID delle partizioni dei dati e dei log. Gli ID WWID devono corrispondere ai nomi alias configurati in `/etc/multipath.conf` file.

   L'output seguente mostra un esempio di una configurazione multi-host 2+1 utilizzando LVM con SID=FC5.

```
sapcc-hana-tst-03:/hana/shared # cat global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/FC5
basepath_logvolumes = /hana/log/FC5
[storage]
ha_provider = hdb_ha.fcClientLVM
partition_*_*__prtype = 5
partition_*_data__mountOptions = -o relatime,inode64
partition_*_log__mountOptions = -o relatime,inode64
partition_1_data__lvmname = FC5_data_mnt00001-vol
partition_1_log__lvmname = FC5_log_mnt00001-vol
partition_2_data__lvmname = FC5_data_mnt00002-vol
partition_2_log__lvmname = FC5_log_mnt00002-vol
sapcc-hana-tst-03:/hana/shared #
```

   Utilizzando lo strumento di installazione SAP hdblcm, avviare l'installazione eseguendo il seguente comando su uno degli host worker. Utilizzare l' `addhosts`opzione per aggiungere il secondo lavoratore (sapcc-hana-tst-06) e l'host di standby (sapcc-hana-tst-07).

> La directory in cui è memorizzato il file preparato `global.ini` è inclusa con l' `storage_cfg`opzione CLI (--storage_cfg=/hana/shared`).

> A seconda della versione del sistema operativo in uso, potrebbe essere necessario installare Python 2.7 prima di installare il database SAP HANA.

```
./hdblcm --action=install --addhosts=sapcc-hana-tst
-06:role=worker:storage_partition=2,sapcc-hana-tst-07:role=standby
--storage_cfg=/hana/shared/

AP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1
(1.015.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
```

```
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip


SAP HANA Database version '2.00.073.00.1695288802' will be installed.

Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------
---------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version
2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
  9     | epmmds          | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
```

```
4.203.2321.0.0

Enter comma-separated list of the selected indices [3,4]: 2,3
```

3. Verificare che lo strumento di installazione abbia installato tutti i componenti selezionati su tutti gli host di lavoro e di standby.

Aggiunta di partizioni di volumi di dati aggiuntive per sistemi SAP HANA a host singolo

A partire da SAP HANA 2.0 SPS4, è possibile configurare ulteriori partizioni del volume di dati. Questa funzione consente di configurare due o più LUN per il volume di dati di un database tenant SAP HANA e di scalare oltre i limiti di dimensioni e performance di una singola LUN.

> Non è necessario utilizzare più partizioni per soddisfare i KPI SAP HANA. Un singolo LUN con una singola partizione soddisfa i KPI richiesti.

> L'utilizzo di due o più LUN singoli per il volume di dati è disponibile solo per i sistemi SAP HANA a host singolo. Il connettore di storage SAP richiesto per i sistemi host multipli SAP HANA supporta un solo dispositivo per il volume di dati.

L'aggiunta di partizioni di volumi di dati aggiuntive può essere eseguita in qualsiasi momento, ma potrebbe richiedere il riavvio del database SAP HANA.

Attivazione di partizioni di volumi di dati aggiuntive

Per attivare ulteriori partizioni del volume di dati, attenersi alla seguente procedura:

1. Aggiungere la seguente voce all'interno di `global.ini` file.

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

2. Riavviare il database per attivare la funzione. Aggiunta del parametro tramite SAP HANA Studio a `global.ini` Utilizzando la configurazione Systemdb si impedisce il riavvio del database.

Configurazione del volume e del LUN

Il layout dei volumi e delle LUN è simile al layout di un singolo host con una partizione del volume di dati, ma con un volume di dati e un LUN aggiuntivi memorizzati su un aggregato diverso come il volume di log e l'altro volume di dati. La seguente tabella mostra un esempio di configurazione di sistemi SAP HANA a host singolo con due partizioni di volumi di dati.

Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Volume di dati: SID_data_mnt00001	Volume condiviso: SID_shared	Volume di dati: SID_data2_mnt00001	Volume di log: SID_log_mnt00001

La seguente tabella mostra un esempio di configurazione del punto di montaggio per un sistema a host singolo con due partizioni del volume di dati.

LUN	Punto di montaggio sull'host HANA	Nota
SID_data_mnt00001	/hana/data/SID/mnt00001	Montato usando /etc/fstab entry
SID_data2_mnt00001	/hana/data2/SID/mnt00001	Montato usando /etc/fstab entry
SID_log_mnt00001	/hana/log/SID/mnt00001	Montato usando /etc/fstab entry
SID_shared	/hana/shared/SID	Montato usando /etc/fstab entry

Creare le nuove LUN dei dati utilizzando Gestore di sistema di ONTAP o l'interfaccia utente di ONTAP.

Configurazione dell'host

Per configurare un host, attenersi alla seguente procedura:

1. Configurare il multipathing per i LUN aggiuntivi, come descritto nel capitolo "Host Setup (impostazione host)" .
2. Creare il file system XFS su ogni LUN aggiuntivo appartenente al sistema HANA:

```
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana-FC5_data2_mnt00001
```

3. Aggiungere i file system aggiuntivi a `/etc/fstab` file di configurazione.

> I file system XFS per il LUN di dati e log devono essere montati con `relatime` e. `inode64` opzioni di montaggio.

```
stlrx300s8-6:/ # cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/hana-FC5_log_mnt00001 /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/hana-FC5_data_mnt00001 /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/hana-FC5_data2_mnt00001 /hana/data2/FC5/mnt00001 xfs
relatime,inode64 0 0
```

4. Creare punti di montaggio e impostare le autorizzazioni sull'host del database.

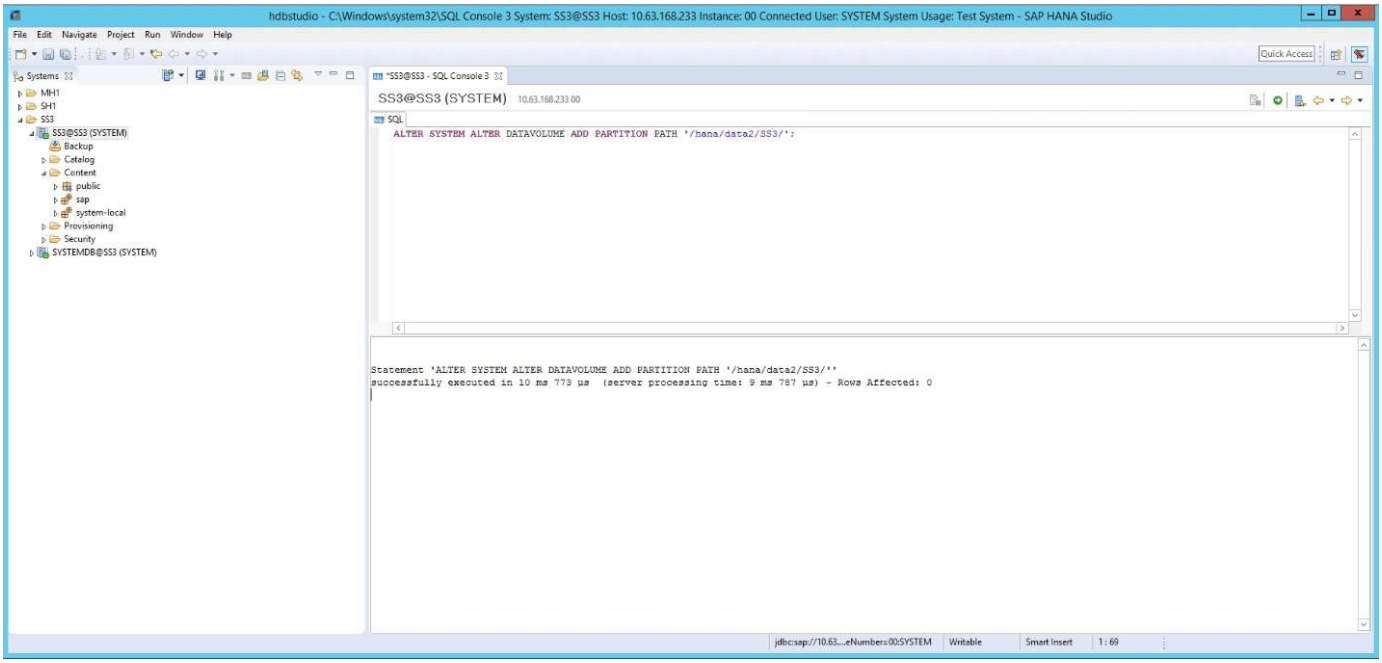
```
stlrx300s8-6:/ # mkdir -p /hana/data2/FC5/mnt00001
stlrx300s8-6:/ # chmod -R 777 /hana/data2/FC5
```

5. Montare i file system ed eseguire `mount -a` comando.

Aggiunta di una partizione datavolume aggiuntiva

Per aggiungere un'ulteriore partizione di datavolume al database del tenant, eseguire la seguente istruzione SQL sul database del tenant. Ogni LUN aggiuntivo può avere un percorso diverso:

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```



Dove trovare ulteriori informazioni

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

- "Soluzioni software SAP HANA"
- "TR-4646: Disaster recovery SAP HANA con replica dello storage"
- "TR-4614: Backup e ripristino SAP HANA con SnapCenter"
- "TR-4667: Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter"
- Centri di documentazione NetApp

  "https://www.netapp.com/support-and-training/documentation/"
- Hardware per lo storage aziendale certificato SAP per SAP HANA

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"
- Requisiti di storage SAP HANA

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"
- SAP HANA - Domande frequenti sull'integrazione personalizzata del data center

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"

- SAP HANA su VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"

- Guida alle Best practice di SAP HANA su VMware vSphere

  "https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

Aggiornare la cronologia

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

Data	Riepilogo degli aggiornamenti
Ottobre 2015	Versione iniziale
Marzo 2016	Dimensionamento della capacità aggiornato
Febbraio 2017	Nuovi sistemi storage e shelf di dischi NetApp nuove funzionalità di ONTAP 9 nuove release di sistemi operativi (SLES12 SP1 e RHEL 7.2) Nuova release di SAP HANA
Luglio 2017	Aggiornamenti minori
Settembre 2018	Nuovi sistemi storage NetApp nuove release dei sistemi operativi (SLES12 SP3 e RHEL 7.4) aggiornamenti minori aggiuntivi SAP HANA 2.0 SPS3
Novembre 2019	Nuovi sistemi storage NetApp e shelf NVMe nuove release dei sistemi operativi (SLES12 SP4, SLES 15 e RHEL 7.6) aggiornamenti minori aggiuntivi
Aprile 2020	I nuovi sistemi storage della serie AFF ASA hanno introdotto una funzione di partizione di dati multipla disponibile da SAP HANA 2.0 SPS4
Giugno 2020	Ulteriori informazioni sulle funzionalità opzionali aggiornamenti minori
Febbraio 2021	Supporto LVM Linux nuovi sistemi storage NetApp nuove release dei sistemi operativi (SLES15SP2, RHEL 8)
Aprile 2021	Aggiunta di informazioni specifiche su VMware vSphere
Settembre 2022	Nuove versioni del sistema operativo
Agosto 2023	Nuovi sistemi di storage (AFF serie C)
Maggio 2024	Nuovi sistemi di storage (AFF serie A)
Settembre 2024	Nuovi sistemi di storage (ASA serie A)
Novembre 2024	Nuovi sistemi di storage
Febbraio 2025	Nuovi sistemi di storage
Luglio 2025	Aggiornamenti minori

Guida alla configurazione di SAP HANA su sistemi NetApp AFF con NFS

SAP HANA su sistemi NetApp AFF con NFS - Guida alla configurazione

La famiglia di prodotti NetApp AFF A-Series è stata certificata per l'utilizzo con SAP HANA in progetti di integrazione di data center personalizzati (TDI). Questa guida fornisce le best practice per SAP HANA su questa piattaforma per NFS.

Marco Schoen, NetApp

Questa certificazione è valida per i seguenti modelli:

- AFF A20, AFF A30, AFF A50, AFF A70, AFF A90, AFF A1K

Un elenco completo delle soluzioni di storage certificate NetApp per SAP HANA è disponibile all'indirizzo "Directory hardware SAP HANA certificata e supportata".

Questo documento descrive i requisiti di configurazione di ONTAP per il protocollo NFS versione 3 (NFSv3) o per il protocollo NFS versione 4 (NFSv4.1).

Sono supportate solo le versioni NFS 3 o 4,1. Le versioni NFS 1, 2, 4,0 e 4,2 non sono supportate.

La configurazione descritta in questo documento è necessaria per ottenere i KPI SAP HANA richiesti e le migliori performance per SAP HANA. La modifica di impostazioni o l'utilizzo di funzionalità non elencate nel presente documento potrebbe causare un peggioramento delle prestazioni o un comportamento imprevisto e dovrebbe essere eseguita solo se richiesto dal supporto NetApp.

Le guide di configurazione per i sistemi NetApp AFF che utilizzano FCP e per i sistemi FAS che utilizzano NFS o FCP sono disponibili ai seguenti "SAP HANA su sistemi NetApp FAS con FCP"
* "SAP HANA su sistemi NetApp FAS con NFS"
* "SAP HANA su sistemi NetApp AFF con FCP"
* "SAP HANA su sistemi NetApp ASA con FCP"

La seguente tabella mostra le combinazioni supportate per le versioni di NFS, il blocco NFS e le implementazioni di isolamento richieste, a seconda della configurazione del database SAP HANA.

Per i sistemi SAP HANA a host singolo o per host multipli che non utilizzano il failover automatico dell'host, sono supportati NFSv3 e NFSv4.

Per i sistemi host SAP HANA multipli con host Auto-failover, NetApp supporta solo NFSv4, utilizzando il blocco NFSv4 come alternativa all'implementazione di STONITH (SAP HANA ha/DR provider) specifica del server.

SAP HANA	Versione di NFS	Blocco NFS	PROVIDER SAP HANA HA/DR
SAP HANA host singolo, host multipli senza failover automatico dell'host	NFSv3	Spento	n/a.

SAP HANA	Versione di NFS	Blocco NFS	PROVIDER SAP HANA HA/DR
	NFSv4	Acceso	n/a.
SAP HANA host multipli che utilizzano il failover automatico dell'host	NFSv3	Spento	Implementazione STONITH specifica del server obbligatoria
	NFSv4	Acceso	Non richiesto

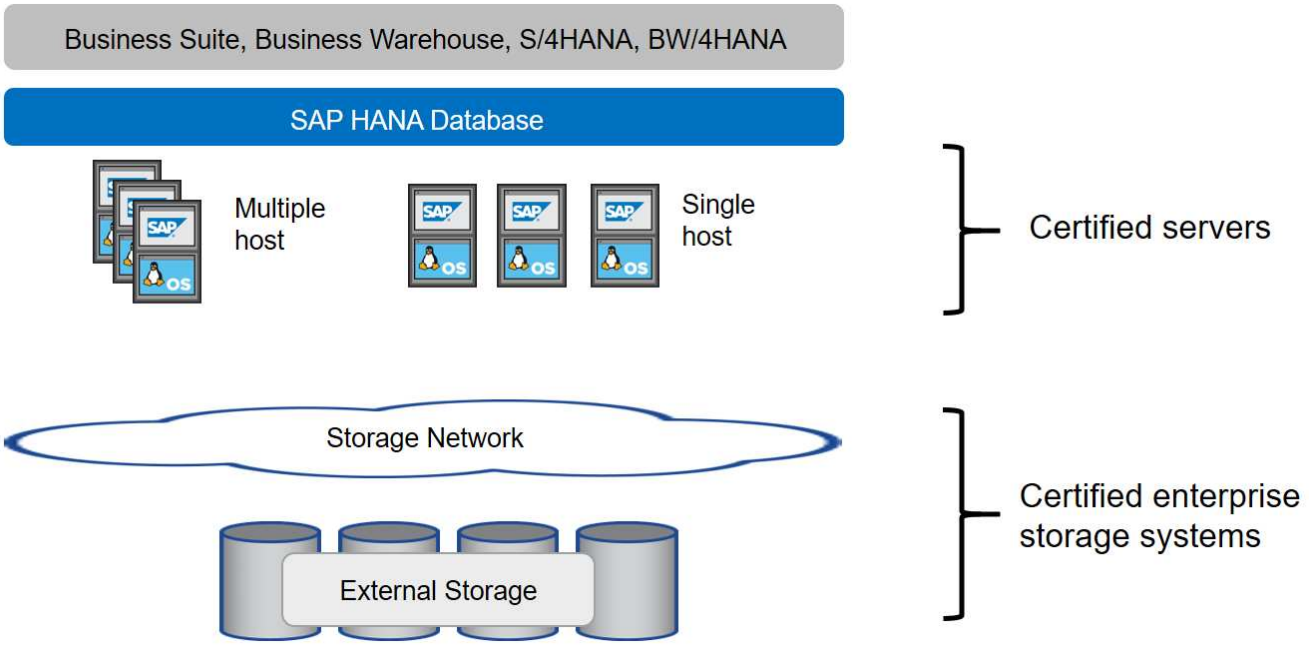
Un'implementazione STONITH specifica per il server non fa parte di questa guida. Contattare il fornitore del server per un'implementazione di questo tipo.

Questo documento illustra i consigli di configurazione per SAP HANA in esecuzione su server fisici e su server virtuali che utilizzano VMware vSphere.

Consultare le note SAP relative alle linee guida per la configurazione del sistema operativo e alle dipendenze del kernel Linux specifico di HANA. Per ulteriori informazioni, consultare la nota SAP 2235581: Sistemi operativi supportati da SAP HANA.

SAP HANA: Integrazione personalizzata del data center

I controller di storage NetApp AFF sono certificati nel programma SAP HANA TDI utilizzando protocolli NFS (NAS) e FC (SAN). Possono essere implementati in qualsiasi scenario SAP HANA, come SAP Business Suite su HANA, S/4HANA, BW/4HANA o SAP Business Warehouse su HANA in configurazioni a host singolo o multiplo. Qualsiasi server certificato per l'utilizzo con SAP HANA può essere combinato con soluzioni di storage certificate NetApp. Vedere la figura seguente per una panoramica dell'architettura di SAP HANA TDI.



Per ulteriori informazioni sui prerequisiti e sui consigli per i sistemi SAP HANA prodotti, consulta la seguente risorsa:

- "SAP HANA - Domande frequenti sull'integrazione personalizzata del data center"

SAP HANA con VMware vSphere

Sono disponibili diverse opzioni per la connessione dello storage alle macchine virtuali (VM). L'opzione preferita consiste nel connettere i volumi di storage con NFS direttamente dal sistema operativo guest. Utilizzando questa opzione, la configurazione degli host e dello storage non differisce tra host fisici e macchine virtuali.

Sono supportati anche datastore NFS e datastore VVOL con NFS. Per entrambe le opzioni, è necessario memorizzare un solo volume di log o dati SAP HANA all'interno del datastore per i casi di utilizzo in produzione.

Questo documento descrive la configurazione consigliata con i montaggi NFS diretti dal sistema operativo guest.

Per ulteriori informazioni sull'utilizzo di vSphere con SAP HANA, consultare i seguenti collegamenti:

- "SAP HANA su VMware vSphere - virtualizzazione - Wiki della community"
- "Guida alle Best practice di SAP HANA su VMware vSphere"
- "2161991 - linee guida per la configurazione di VMware vSphere - Launchpad di supporto SAP ONE (accesso richiesto)"

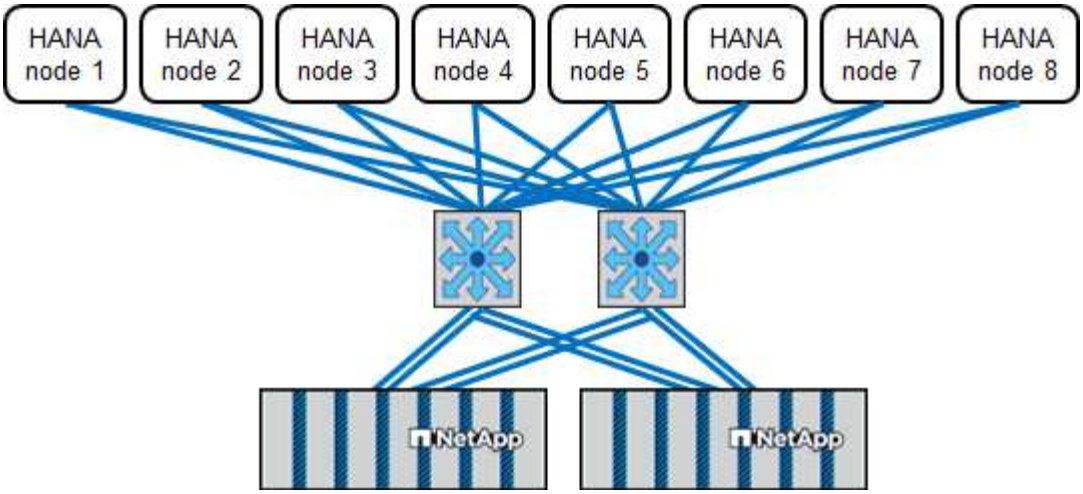
Architettura

Gli host SAP HANA sono connessi ai controller di storage utilizzando un'infrastruttura di rete ridondante da 10 GbE o più veloce. La comunicazione dei dati tra gli host SAP HANA e i controller di storage si basa sul protocollo NFS. È necessaria un'infrastruttura di switching ridondante per fornire connettività host-storage SAP HANA fault-tolerant in caso di guasto dello switch o della scheda di interfaccia di rete (NIC).

Gli switch potrebbero aggregare le performance delle singole porte con i canali delle porte in modo da apparire come una singola entità logica a livello di host.

Diversi modelli della famiglia di sistemi AFF possono essere combinati e abbinati a livello di storage per consentire la crescita e le diverse esigenze di performance e capacità. Il numero massimo di host SAP HANA che possono essere collegati al sistema storage è definito dai requisiti di performance SAP HANA e dal modello di controller NetApp utilizzato. Il numero di shelf di dischi richiesti è determinato solo dai requisiti di capacità e performance dei sistemi SAP HANA.

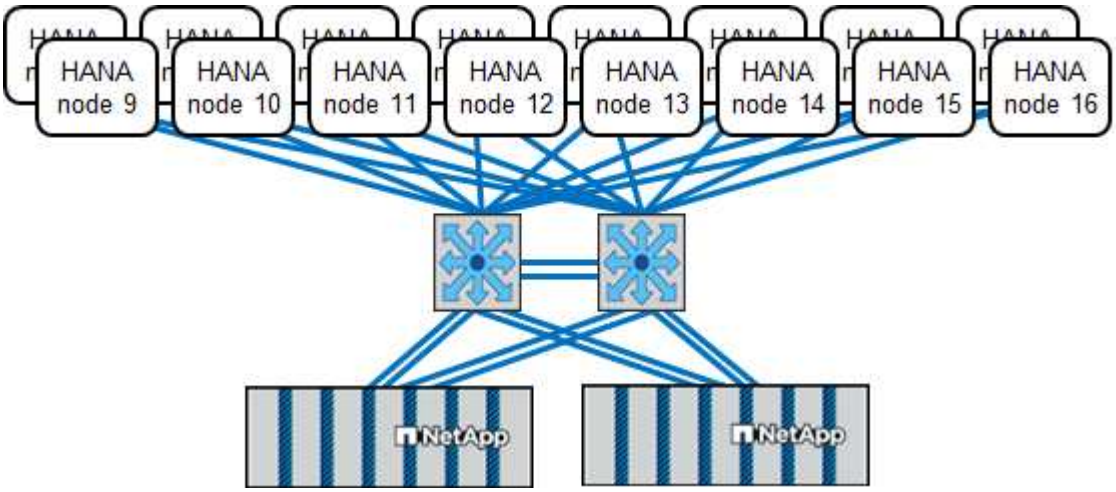
La figura seguente mostra una configurazione di esempio con otto host SAP HANA collegati a una coppia di storage ad alta disponibilità (ha).



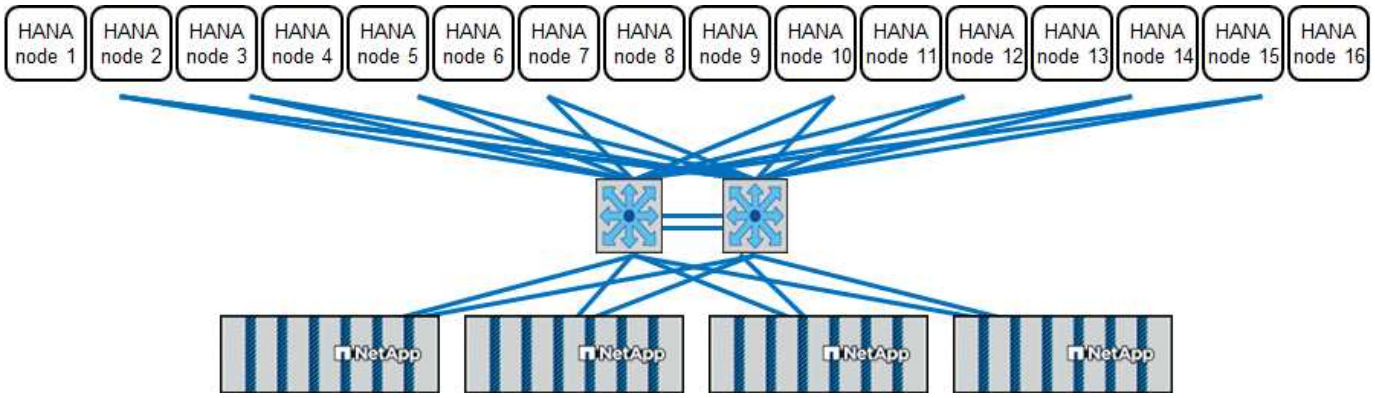
L'architettura può essere scalata in due dimensioni:

- Collegando ulteriori host SAP HANA e capacità di storage allo storage esistente, se i controller di storage forniscono performance sufficienti per soddisfare gli attuali indicatori chiave di performance SAP HANA (KPI).
- Aggiungendo altri sistemi storage con capacità di storage aggiuntiva per gli host SAP HANA aggiuntivi

La figura seguente mostra una configurazione di esempio in cui più host SAP HANA sono collegati ai controller di storage. In questo esempio, sono necessari più shelf di dischi per soddisfare i requisiti di capacità e performance dei 16 host SAP HANA. A seconda dei requisiti di throughput totale, è necessario aggiungere connessioni aggiuntive da 10 GbE o più veloci ai controller di storage.



Indipendentemente dal sistema AFF implementato, il panorama SAP HANA può essere scalato aggiungendo uno qualsiasi dei controller di storage certificati per soddisfare la densità di nodo desiderata, come mostrato nella figura seguente.



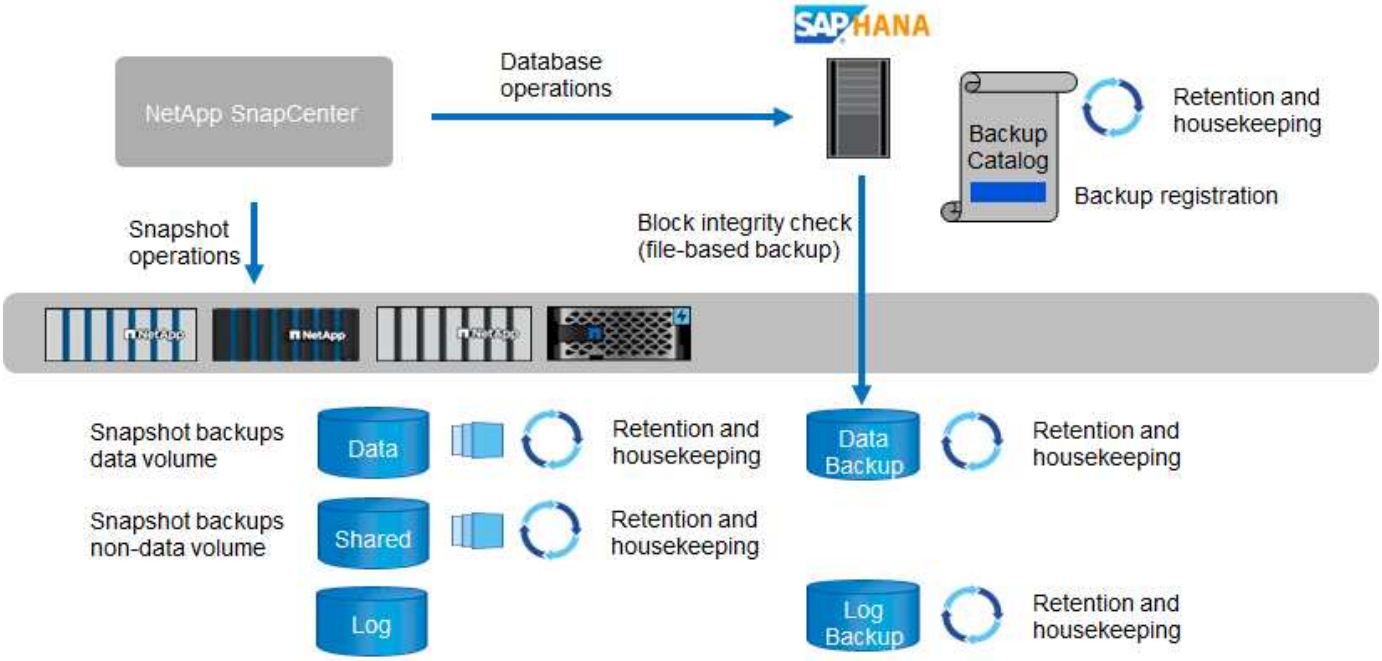
Backup SAP HANA

Il software ONTAP presente su tutti i controller di storage NetApp offre un meccanismo integrato per eseguire il backup dei database SAP HANA durante il funzionamento senza alcun effetto sulle performance. I backup NetApp Snapshot basati sullo storage sono una soluzione di backup completamente supportata e integrata disponibile per i singoli container SAP HANA e per i sistemi SAP HANA Multitenant Database Containers (MDC) con un singolo tenant o più tenant.

I backup Snapshot basati su storage vengono implementati utilizzando il plug-in NetApp SnapCenter per SAP HANA. Ciò consente agli utenti di creare backup Snapshot coerenti basati sullo storage utilizzando le interfacce fornite in modo nativo dai database SAP HANA. SnapCenter registra tutti i backup Snapshot nel catalogo di backup SAP HANA. Pertanto, i backup eseguiti da SnapCenter sono visibili all'interno di SAP HANA Studio e Cockpit, dove possono essere selezionati direttamente per le operazioni di ripristino e recovery.

La tecnologia NetApp SnapMirror consente di replicare le copie Snapshot create su un sistema storage su un sistema storage di backup secondario controllato da SnapCenter. È quindi possibile definire diversi criteri di conservazione dei backup per ciascuno dei set di backup sullo storage primario e per i set di backup sui sistemi di storage secondari. Il plug-in SnapCenter per SAP HANA gestisce automaticamente la conservazione dei backup dei dati basati su copia Snapshot e dei backup dei log, inclusa la manutenzione del catalogo di backup. Il plug-in SnapCenter per SAP HANA consente inoltre di eseguire un controllo dell'integrità del blocco del database SAP HANA eseguendo un backup basato su file.

È possibile eseguire il backup dei log del database direttamente sullo storage secondario utilizzando un montaggio NFS, come illustrato nella figura seguente.



I backup Snapshot basati su storage offrono vantaggi significativi rispetto ai backup convenzionali basati su file. Questi vantaggi includono, a titolo esemplificativo e non esaustivo, i seguenti:

- Backup più rapido (pochi minuti)
- RTO (Recovery Time Objective) ridotto grazie a un tempo di ripristino molto più rapido sul layer di storage (pochi minuti) e a backup più frequenti
- Nessuna riduzione delle performance dell'host, della rete o dello storage del database SAP HANA durante le operazioni di backup e recovery
- Replica efficiente in termini di spazio e larghezza di banda sullo storage secondario in base alle modifiche dei blocchi

Per informazioni dettagliate sulla soluzione di backup e ripristino SAP HANA, vedere "TR-4614: Backup e ripristino SAP HANA con SnapCenter".

Disaster recovery SAP HANA

Il disaster recovery SAP HANA (DR) può essere eseguito a livello di database utilizzando la replica di sistema SAP HANA o a livello di storage utilizzando le tecnologie di replica dello storage. La sezione seguente fornisce una panoramica delle soluzioni di disaster recovery basate sulla replica dello storage.

Per informazioni dettagliate sulle soluzioni di disaster recovery SAP HANA, vedere "TR-4646: Disaster recovery SAP HANA con replica dello storage".

Replica dello storage basata su SnapMirror

La figura seguente mostra una soluzione di disaster recovery a tre siti che utilizza la replica sincrona di SnapMirror nel data center di DR locale e SnapMirror asincrono per replicare i dati nel data center di DR remoto.

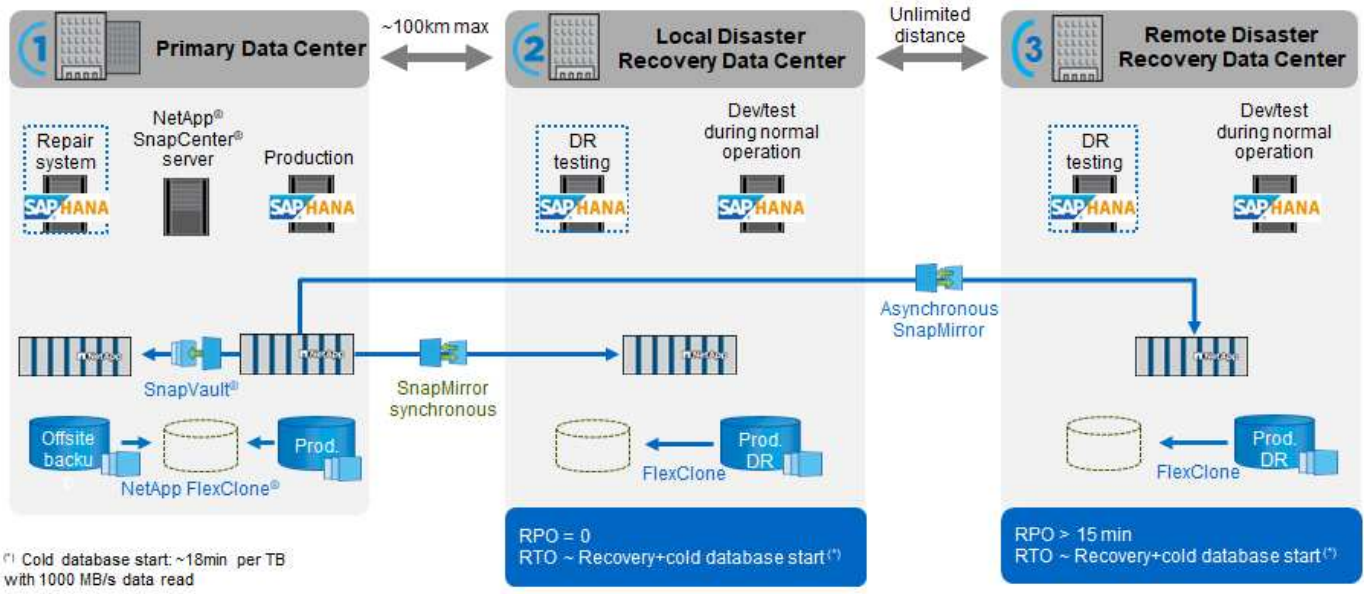
La replica dei dati con SnapMirror sincrono fornisce un RPO pari a zero. La distanza tra il data center DR principale e quello locale è limitata a circa 100 km.

La protezione dai guasti del sito di DR primario e locale viene eseguita replicando i dati in un terzo data center di DR remoto utilizzando SnapMirror asincrono. L'RPO dipende dalla frequenza degli aggiornamenti di replica e dalla velocità di trasferimento. In teoria, la distanza è illimitata, ma il limite dipende dalla quantità di dati da trasferire e dalla connessione disponibile tra i data center. I valori RPO tipici sono compresi nell'intervallo da 30 minuti a più ore.

L'RTO per entrambi i metodi di replica dipende principalmente dal tempo necessario per avviare il database HANA nel sito di DR e caricare i dati in memoria. Supponendo che i dati siano letti con un throughput di 1000 Mbps, il caricamento di 1 TB di dati richiederebbe circa 18 minuti.

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

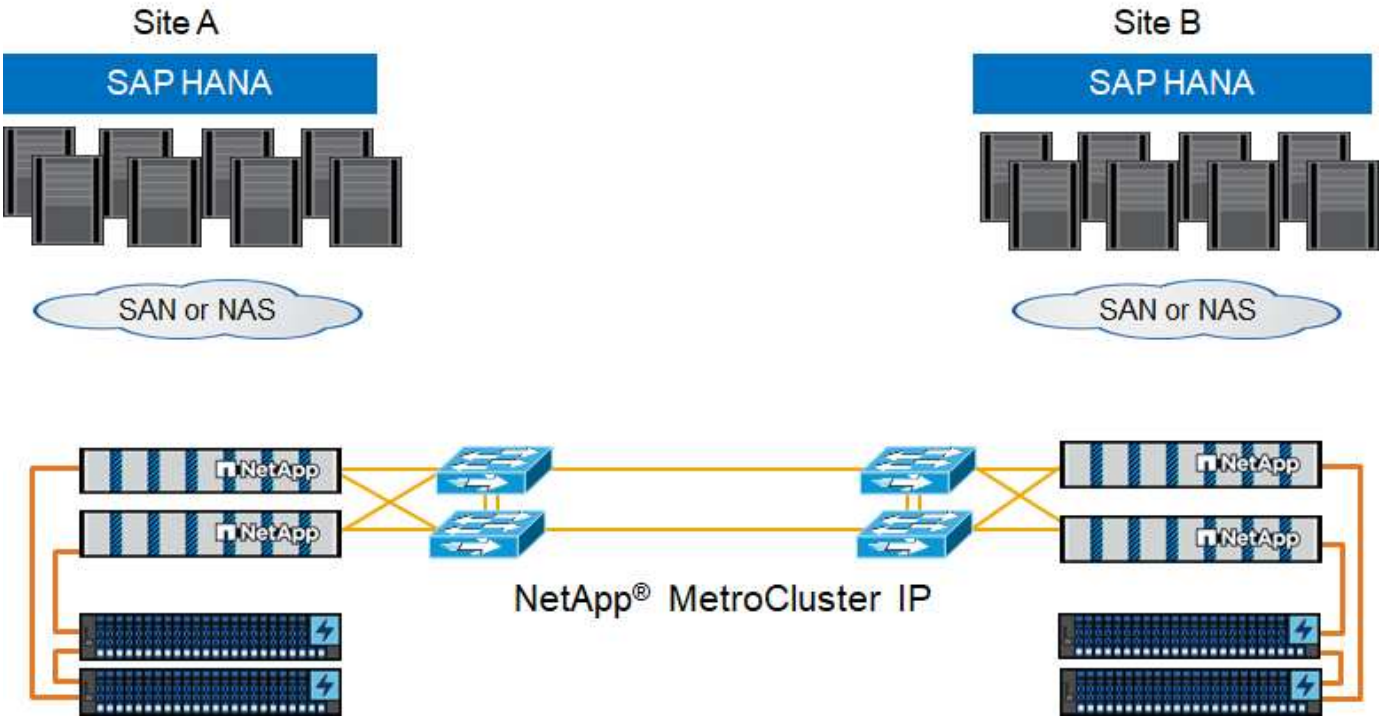
Entrambi i metodi di replica consentono di eseguire test del workflow di DR senza influenzare l'RPO e l'RTO. I volumi FlexClone vengono creati sullo storage e collegati ai server di test del DR.



La replica sincrona offre la modalità StrictSync. Se la scrittura sullo storage secondario non viene completata per qualsiasi motivo, l'i/o dell'applicazione non riesce, garantendo così che i sistemi di storage primario e secondario siano identici. L'i/o dell'applicazione al primario riprende solo dopo che la relazione SnapMirror ritorna allo stato InSync. In caso di guasto dello storage primario, l'i/o dell'applicazione può essere ripristinato sullo storage secondario dopo il failover senza perdita di dati. In modalità StrictSync, l'RPO è sempre zero.

Replica dello storage basata su MetroCluster

La figura seguente mostra una panoramica di alto livello della soluzione. Il cluster di storage di ogni sito fornisce alta disponibilità locale e viene utilizzato per il carico di lavoro di produzione. I dati di ciascun sito vengono replicati in modo sincrono nell'altra posizione e sono disponibili in caso di failover di emergenza.



Dimensionamento dello storage

La sezione seguente fornisce una panoramica delle considerazioni su performance e capacità richieste per il dimensionamento di un sistema storage per SAP HANA.

Contatta NetApp o il tuo partner commerciale NetApp per aiutarti a creare un ambiente di storage di dimensioni adeguate.

Considerazioni sulle performance

SAP ha definito un set statico di KPI relativi allo storage. Questi KPI sono validi per tutti gli ambienti SAP HANA in produzione, indipendentemente dalle dimensioni della memoria degli host di database e delle applicazioni che utilizzano il database SAP HANA. Questi KPI sono validi per ambienti a host singolo, host multiplo, Business Suite su HANA, Business Warehouse su HANA, S/4HANA e BW/4HANA. Pertanto, l'attuale approccio al dimensionamento delle performance dipende solo dal numero di host SAP HANA attivi collegati al sistema storage.

I KPI relativi alle performance dello storage sono richiesti solo per i sistemi SAP HANA in produzione, ma è possibile implementarli in tutti i sistemi HANA.

SAP offre uno strumento di test delle performance che deve essere utilizzato per convalidare le performance del sistema storage per gli host SAP HANA attivi collegati allo storage.

NetApp ha testato e predefinito il numero massimo di host SAP HANA che possono essere collegati a un modello di storage specifico, pur continuando a soddisfare i KPI di storage richiesti da SAP per i sistemi SAP HANA basati sulla produzione.

Il numero massimo di host SAP HANA che possono essere eseguiti su uno shelf di dischi e il numero minimo di SSD richiesti per host SAP HANA sono stati determinati eseguendo il tool di test delle performance SAP. Questo test non prende in considerazione i requisiti effettivi di capacità dello storage degli host. È inoltre necessario calcolare i requisiti di capacità per determinare l'effettiva configurazione dello storage necessaria.

Shelf di dischi SAS

Con lo shelf di dischi SAS (Serial-Attached SCSI) da 12 GB (DS224C), il dimensionamento delle performance viene eseguito utilizzando le seguenti configurazioni di shelf di dischi fissi:

- Shelf di dischi a metà carico con 12 SSD
- Shelf di dischi completamente caricati con 24 SSD

> Entrambe le configurazioni utilizzano la partizione avanzata dei dischi (ADPv2). Uno shelf di dischi a metà carico supporta fino a nove host SAP HANA, mentre uno shelf a pieno carico supporta fino a 14 host in un singolo shelf di dischi. Gli host SAP HANA devono essere equamente distribuiti tra entrambi i controller di storage. Lo stesso vale per i dischi interni di un sistema AFF A700s. Lo shelf di dischi DS224C deve essere connesso utilizzando SAS da 12 GB per supportare il numero di host SAP HANA.

Lo shelf di dischi SAS da 6 GB (DS2246) supporta un massimo di quattro host SAP HANA. Gli SSD e gli host SAP HANA devono essere equamente distribuiti tra entrambi i controller di storage.

La seguente tabella riassume il numero di host SAP HANA supportati per shelf di dischi.

	Shelf SAS da 6 GB (DS2246) con 24 SSD completamente caricati	**Shelf SAS da 12 GB (DS224C) a metà carico con 12 SSD e ADPv2**	**Shelf SAS da 12 GB (DS224C) completamente caricati con 24 SSD e ADPv2**
Numero massimo di host SAP HANA per shelf di dischi	4	9	14

> Questo calcolo è indipendente dal controller di storage utilizzato. L'aggiunta di più shelf di dischi non aumenta la quantità massima di host SAP HANA supportati da uno storage controller.

Shelf NS224 NVMe

Un SSD NVMe (dati) supporta fino a 2/5 host SAP HANA a seconda dei dischi NVMe utilizzati. Gli SSD e gli host SAP HANA devono essere equamente distribuiti tra entrambi i controller di storage. Lo stesso vale per i dischi NVMe interni dei sistemi AFF.

> L'aggiunta di più shelf di dischi non aumenta la quantità massima di host SAP HANA supportata da uno storage controller.

Carichi di lavoro misti

Sono supportati SAP HANA e altri carichi di lavoro applicativi eseguiti sullo stesso storage controller o nello stesso aggregato di storage. Tuttavia, è una Best practice di NetApp separare i workload SAP HANA da tutti gli altri workload delle applicazioni.

Potresti decidere di implementare workload SAP HANA e altri workload applicativi sullo stesso storage controller o sullo stesso aggregato. In tal caso, è necessario assicurarsi che le performance di SAP HANA siano adeguate all'interno dell'ambiente di workload misto. NetApp consiglia inoltre di utilizzare i parametri della qualità del servizio (QoS) per regolare l'effetto che queste altre applicazioni potrebbero avere sulle applicazioni SAP HANA e per garantire il throughput per le applicazioni SAP HANA.

Il tool di test delle performance SAP deve essere utilizzato per verificare se è possibile eseguire altri host SAP HANA su uno storage controller esistente già in uso per altri carichi di lavoro. I server applicativi SAP possono essere posizionati in modo sicuro sullo stesso storage controller e/o aggregato dei database SAP HANA.

Considerazioni sulla capacità

Una descrizione dettagliata dei requisiti di capacità per SAP HANA è disponibile nella "Nota SAP 1900823" white paper.

> Il dimensionamento della capacità del panorama SAP complessivo con più sistemi SAP HANA deve essere determinato utilizzando gli strumenti di dimensionamento dello storage SAP HANA di NetApp. Contatta NetApp o il tuo partner commerciale NetApp per convalidare il processo di dimensionamento dello storage per un ambiente di storage di dimensioni adeguate.

Configurazione dello strumento di test delle performance

A partire da SAP HANA 1.0 SPS10, SAP ha introdotto i parametri per regolare il comportamento di i/o e ottimizzare il database per il file e il sistema storage utilizzati. Questi parametri devono essere impostati anche per lo strumento di test delle performance di SAP quando le performance dello storage vengono testate con lo strumento di test delle performance di SAP.

NetApp ha condotto test delle performance per definire i valori ottimali. La seguente tabella elenca i parametri che devono essere impostati nel file di configurazione dello strumento di test delle prestazioni SAP.

Parametro	Valore
max_parallel_io_requests	128
async_read_submit	acceso
async_write_submit_active	acceso
async_write_submit_blocks	tutto

Per ulteriori informazioni sulla configurazione dei diversi strumenti di test SAP, vedere "Nota SAP 1943937" Per HWCCT (SAP HANA 1.0) e. "Nota SAP 2493172" PER HCMT/HCOT (SAP HANA 2.0).

Nell'esempio seguente viene illustrato come impostare le variabili per il piano di esecuzione HCMT/HCOT.

```
…{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "DataAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
```

```
      },
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

Queste variabili devono essere utilizzate per la configurazione del test. Questo è solitamente il caso dei piani di esecuzione predefiniti che SAP offre con lo strumento HCMT/HCOT. Il seguente esempio per un test di scrittura del log 4k è da un piano di esecuzione.

```
…
       {
          "ID": "D664D001-933D-41DE-A904F304AEB67906",
          "Note": "File System Write Test",
          "ExecutionVariants": [
             {
                "ScaleOut": {
                   "Port": "${RemotePort}",
                   "Hosts": "${Hosts}",
                   "ConcurrentExecution": "${FSConcurrentExecution}"
                },
                "RepeatCount": "${TestRepeatCount}",
                "Description": "4K Block, Log Volume 5GB, Overwrite",
                "Hint": "Log",
                "InputVector": {
                   "BlockSize": 4096,
                   "DirectoryName": "${LogVolume}",
                   "FileOverwrite": true,
                   "FileSize": 5368709120,
                   "RandomAccess": false,
                   "RandomData": true,
                   "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                   "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                   "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                   "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                   "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                   "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                   "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                   "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                   "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
                }
             }, …
```

Panoramica del processo di dimensionamento dello storage

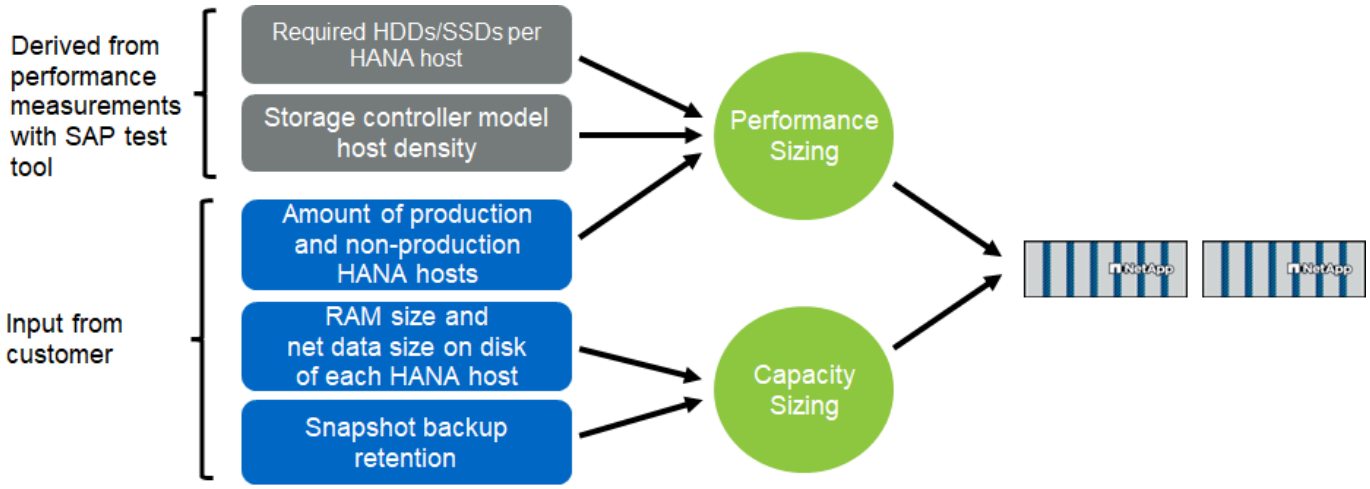
Il numero di dischi per host HANA e la densità host SAP HANA per ciascun modello di storage sono stati determinati con lo strumento di test delle performance.

Il processo di dimensionamento richiede dettagli come il numero di host SAP HANA in produzione e non in

produzione, la dimensione della RAM di ciascun host e la conservazione del backup delle copie Snapshot basate sullo storage. Il numero di host SAP HANA determina il controller dello storage e il numero di dischi necessari.

La dimensione della RAM, la dimensione dei dati netti sul disco di ciascun host SAP HANA e il periodo di conservazione del backup della copia Snapshot vengono utilizzati come input durante il dimensionamento della capacità.

La figura seguente riassume il processo di dimensionamento.



Installazione e configurazione dell'infrastruttura

Configurazione di rete

In questa sezione viene descritta la configurazione della rete di storage dedicata per gli host SAP HANA.

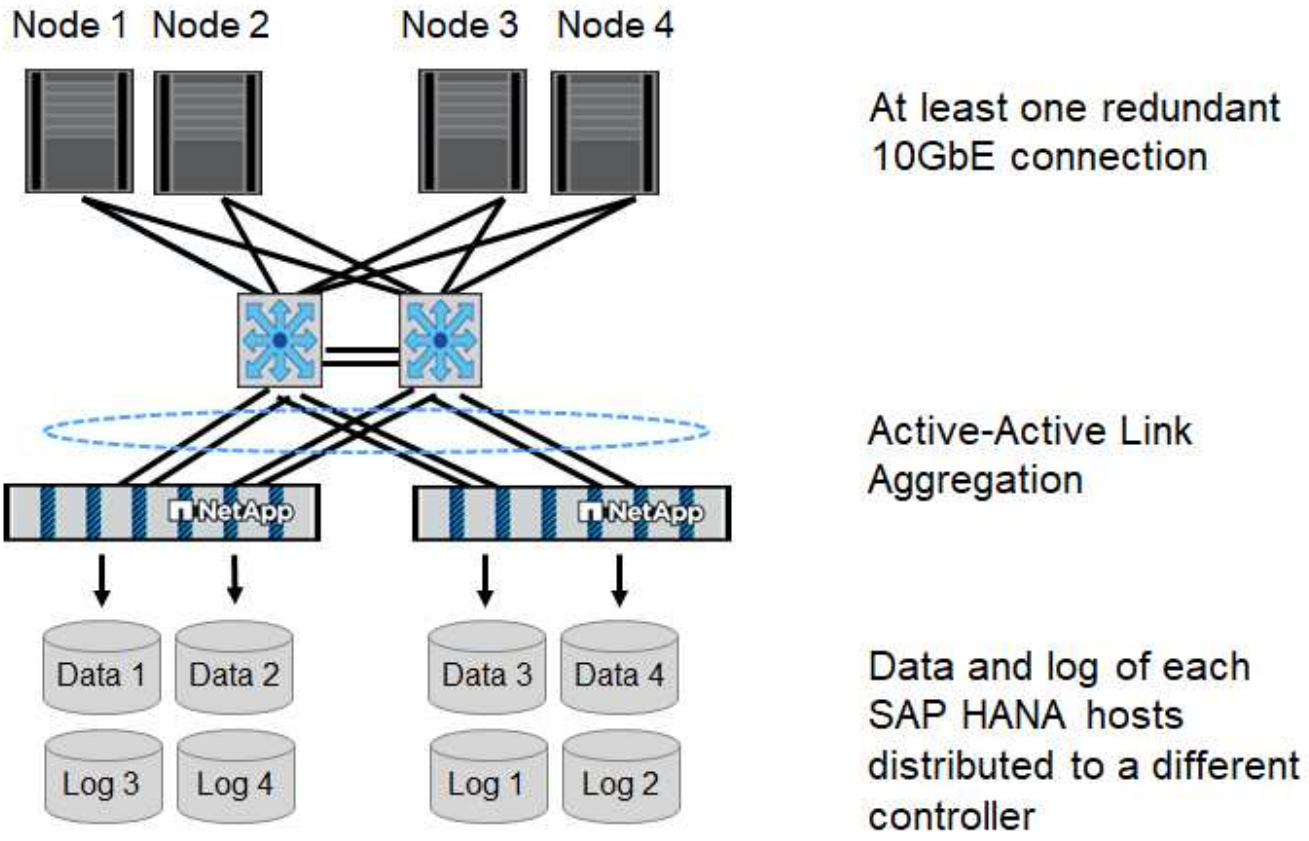
Per configurare la rete, attenersi alle seguenti indicazioni:

- Per collegare gli host SAP HANA ai controller di storage con una rete 10 GbE o superiore, è necessario utilizzare una rete storage dedicata.
- Utilizza la stessa velocità di connessione per i controller di storage e gli host SAP HANA. Se ciò non fosse possibile, assicurarsi che i componenti di rete tra i controller di storage e gli host SAP HANA siano in grado di gestire velocità diverse. Ad esempio, è necessario fornire spazio buffer sufficiente per consentire la negoziazione rapida a livello NFS tra storage e host. I componenti di rete sono in genere switch, ma devono essere presi in considerazione anche altri componenti all'interno dello chassis blade, ad esempio il backplane.
- Disattivare il controllo di flusso su tutte le porte fisiche utilizzate per il traffico dello storage sullo switch della rete di storage e sul layer host.
- Ogni host SAP HANA deve disporre di una connessione di rete ridondante con un minimo di 10 GB di larghezza di banda.
- I frame jumbo con una dimensione massima di unità di trasmissione (MTU) di 9,000 devono essere abilitati su tutti i componenti di rete tra gli host SAP HANA e i controller di storage.
- In una configurazione VMware, è necessario assegnare adattatori di rete VMXNET3 dedicati a ciascuna macchina virtuale in esecuzione. Per ulteriori requisiti, consultare i documenti pertinenti menzionati in "Introduzione".

- Per evitare interferenze reciproche, utilizzare percorsi di rete/io separati per l'area di log e dati.

La figura seguente mostra un esempio con quattro host SAP HANA collegati a una coppia di ha controller storage che utilizza una rete 10 GbE. Ogni host SAP HANA dispone di una connessione Active-Active al fabric ridondante.

A livello di storage, quattro connessioni attive sono configurate per fornire un throughput di 10 GB per ciascun host SAP HANA. A livello di storage, viene configurato un dominio di broadcast con una dimensione MTU di 9000 e tutte le interfacce fisiche richieste vengono aggiunte a questo dominio di broadcast. Questo approccio assegna automaticamente queste interfacce fisiche allo stesso gruppo di failover. Tutte le interfacce logiche (LIF) assegnate a queste interfacce fisiche vengono aggiunte a questo gruppo di failover.



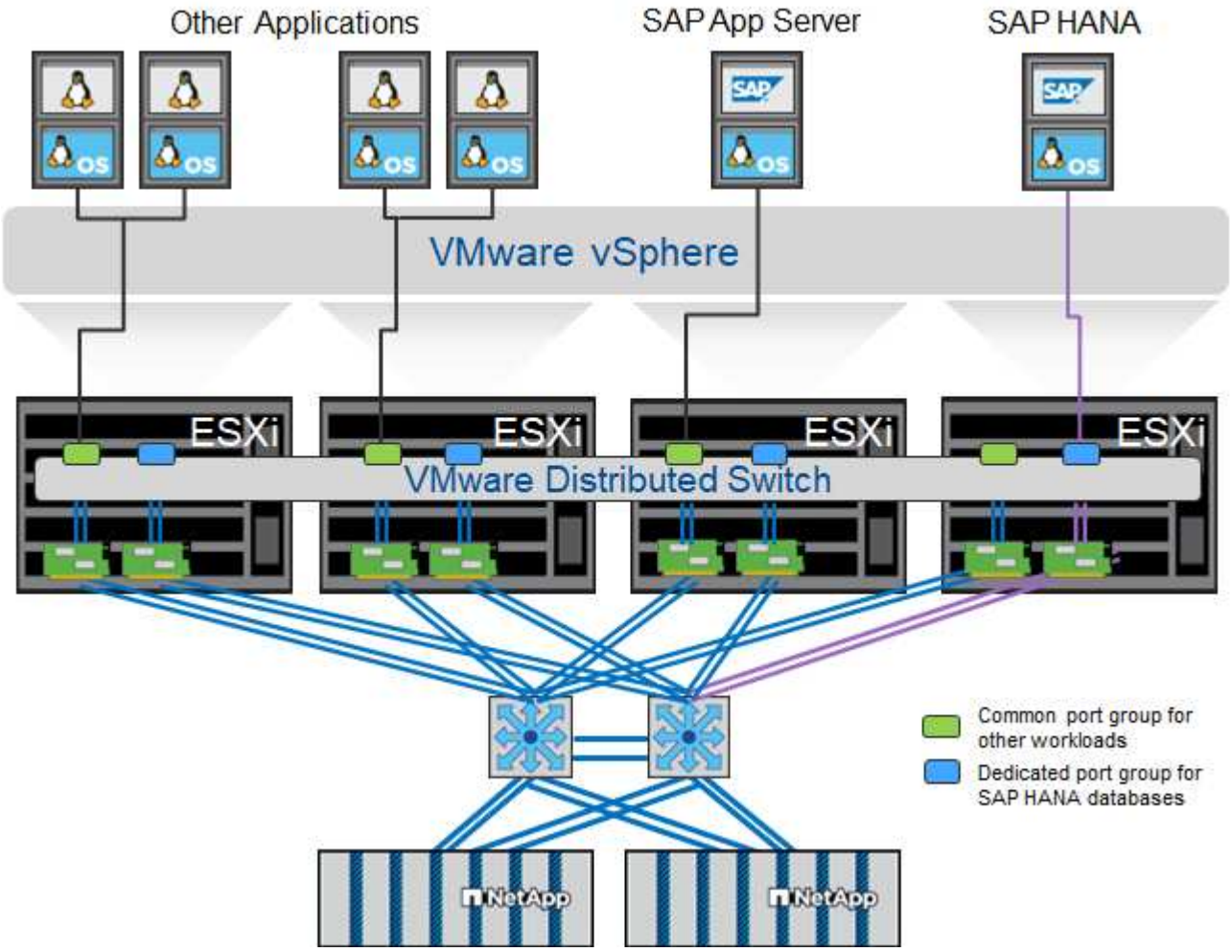
In generale, si consiglia di utilizzare i gruppi di interfacce ha sui server (Bonds) e sui sistemi di storage (ad esempio, link Aggregation Control Protocol [LACP] e ifgroup). Con i gruppi di interfacce ha, verificare che il carico sia equamente distribuito tra tutte le interfacce all'interno del gruppo. La distribuzione del carico dipende dalla funzionalità dell'infrastruttura dello switch di rete.

A seconda del numero di host SAP HANA e della velocità di connessione utilizzata, sono necessari diversi numeri di porte fisiche attive. Per ulteriori informazioni, vedere la sezione "Configurazione LIF".

Configurazione di rete specifica di VMware

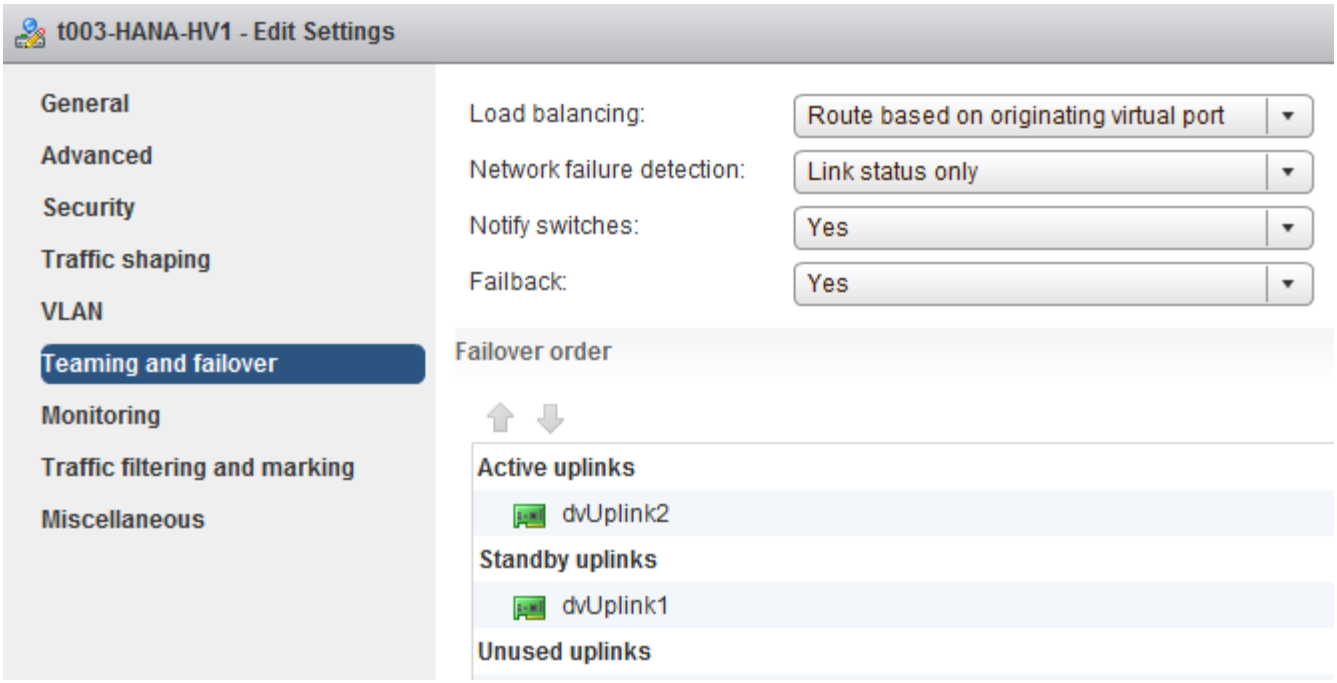
La corretta progettazione e configurazione della rete sono fondamentali perché tutti i dati per le istanze SAP HANA, inclusi i dati critici per le performance e i volumi di log per il database, vengono forniti tramite NFS in questa soluzione. Una rete storage dedicata viene utilizzata per separare il traffico NFS dal traffico di comunicazione e accesso utente tra i nodi SAP HANA. Ogni nodo SAP HANA richiede una connessione di rete dedicata ridondante con un minimo di 10 GB di larghezza di banda. È supportata anche una maggiore

larghezza di banda. Questa rete deve estendersi end-to-end dal livello di storage attraverso lo switching e il calcolo della rete fino al sistema operativo guest ospitato su VMware vSphere. Oltre all'infrastruttura di switching fisica, viene utilizzato uno switch distribuito VMware (VDS) per fornire performance e gestibilità adeguate del traffico di rete a livello di hypervisor.



Come illustrato nella figura precedente, ciascun nodo SAP HANA utilizza un gruppo di porte dedicato sullo switch distribuito VMware. Questo gruppo di porte consente di migliorare la qualità del servizio (QoS) e l'assegnazione dedicata delle schede di interfaccia di rete fisiche (NIC) sugli host ESX. Per utilizzare NIC fisiche dedicate preservando le funzionalità ha in caso di guasto alla NIC, la NIC fisica dedicata viene configurata come uplink attivo. Le schede di rete aggiuntive sono configurate come uplink in standby nelle impostazioni di teaming e failover del gruppo di porte SAP HANA. Inoltre, i jumbo frame (MTU 9,000) devono essere abilitati end-to-end sugli switch fisici e virtuali. Inoltre, disattivare il controllo di flusso su tutte le porte ethernet utilizzate per il traffico dello storage su server, switch e sistemi storage. La figura seguente mostra un esempio di tale configurazione.

LRO (Large receive offload) deve essere disattivato per le interfacce utilizzate per il traffico NFS. Per tutte le altre linee guida sulla configurazione di rete, consultare le rispettive guide alle Best practice VMware per SAP HANA.



Sincronizzazione dell'ora

È necessario sincronizzare l'ora tra i controller di storage e gli host del database SAP HANA. A tale scopo, impostare lo stesso server di riferimento orario per tutti i controller di storage e tutti gli host SAP HANA.

Configurazione dello storage controller

Questa sezione descrive la configurazione del sistema storage NetApp. È necessario completare l'installazione e la configurazione primaria in base alle corrispondenti guide di configurazione e configurazione di ONTAP.

Efficienza dello storage

La deduplica inline, la deduplica inline di più volumi, la compressione inline e la compaction inline sono supportate con SAP HANA in una configurazione SSD.

Volumi NetApp FlexGroup

L'utilizzo dei volumi NetApp FlexGroup non è supportato per SAP HANA. Grazie all'architettura di SAP HANA l'utilizzo di FlexGroup Volumes non fornisce alcun beneficio e potrebbe causare problemi di performance.

Crittografia dei volumi e degli aggregati NetApp

L'utilizzo di NetApp Volume Encryption (NVE) e NetApp aggregate Encryption (NAE) sono supportati con SAP HANA.

Qualità del servizio

La QoS può essere utilizzata per limitare il throughput dello storage per specifici sistemi SAP HANA o altre applicazioni su un controller condiviso. Un caso d'utilizzo sarebbe quello di limitare il throughput dei sistemi di sviluppo e test in modo che non possano influenzare i sistemi di produzione in una configurazione mista.

Durante il processo di dimensionamento, è necessario determinare i requisiti di performance di un sistema non in produzione. I sistemi di sviluppo e test possono essere dimensionati con valori di performance inferiori, in genere nell'intervallo compreso tra il 20% e il 50% di un KPI del sistema di produzione come definito da SAP.

A partire da ONTAP 9, la qualità del servizio viene configurata a livello di volume di storage e utilizza i valori massimi per il throughput (Mbps) e la quantità di i/o (IOPS).

L'i/o di scrittura di grandi dimensioni ha il maggiore effetto sulle performance del sistema storage. Pertanto, il limite di throughput QoS deve essere impostato su una percentuale dei corrispondenti valori KPI di scrittura delle performance dello storage SAP HANA nei volumi di dati e di log.

NetApp FabricPool

La tecnologia NetApp FabricPool non deve essere utilizzata per i file system primari attivi nei sistemi SAP HANA. Sono inclusi i file system per l'area dei dati e dei log, oltre a `/hana/shared` file system. In questo modo si ottengono performance imprevedibili, in particolare durante l'avvio di un sistema SAP HANA.

È possibile utilizzare la policy di tiering "snapshot-only" e FabricPool in generale in una destinazione di backup come NetApp SnapVault o SnapMirror.

> ⓘ L'utilizzo di FabricPool per tiering delle copie Snapshot nello storage primario o l'utilizzo di FabricPool in una destinazione di backup modifica il tempo necessario per il ripristino e il ripristino di un database o di altre attività, come la creazione di cloni di sistema o la riparazione di sistemi. Prendetevi in considerazione questo aspetto per pianificare la vostra strategia generale di gestione del ciclo di vita e verificate che i vostri SLA vengano ancora rispettati durante l'utilizzo di questa funzione.

FabricPool è un'ottima opzione per spostare i backup dei log in un altro Tier di storage. Lo spostamento dei backup influisce sul tempo necessario per ripristinare un database SAP HANA. Pertanto, l'opzione "tiering-minimum-cooling-days" deve essere impostata su un valore che colloca i backup dei log, normalmente necessari per il recovery, sul Tier di storage veloce locale.

Configurazione dello storage

La seguente panoramica riassume i passaggi necessari per la configurazione dello storage. Ogni fase viene descritta in dettaglio nelle sezioni successive. In questa sezione, si presuppone che l'hardware di storage sia configurato e che il software ONTAP sia già installato. Inoltre, le connessioni tra le porte di storage (10 GbE o superiori) e la rete devono essere già in uso.

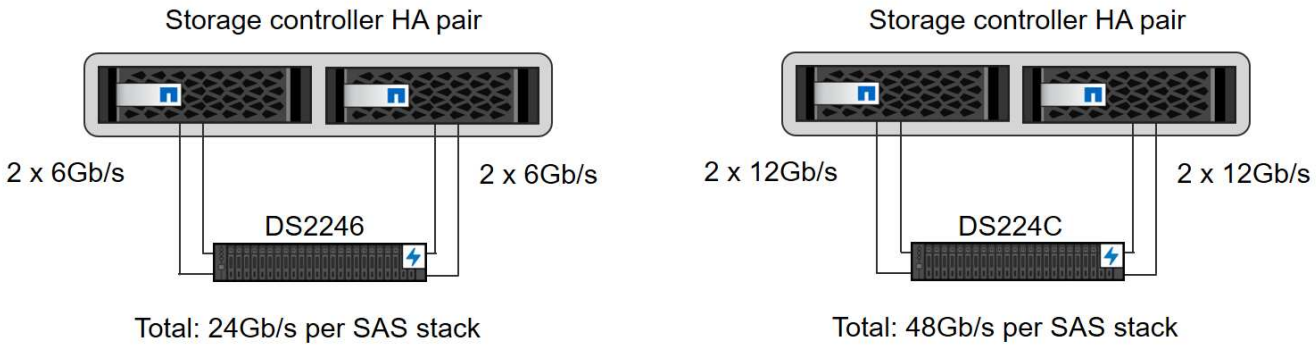
1. Verificare la corretta configurazione dello shelf di dischi come descritto in "Connessione a shelf di dischi."
2. Creare e configurare gli aggregati richiesti come descritto in "Configurazione dell'aggregato."
3. Creare una macchina virtuale per lo storage (SVM) come descritto in "Configurazione SVM."
4. Creare i LIF come descritto in "Configurazione LIF."
5. Creare volumi all'interno degli aggregati come descritto in " "Configurazione dei volumi per sistemi SAP HANA a host singolo e "Configurazione dei volumi per sistemi SAP HANA con host multipli."
6. Impostare le opzioni di volume richieste come descritto in "Opzioni del volume."
7. Impostare le opzioni richieste per NFSv3 come descritto in "Configurazione NFS per NFSv3" O per NFSv4 come descritto in "Configurazione NFS per NFSv4."
8. Montare i volumi nello spazio dei nomi e impostare i criteri di esportazione come descritto in "Montare i volumi nello spazio dei nomi e impostare i criteri di esportazione."

Connessione a shelf di dischi

Shelf di dischi SAS

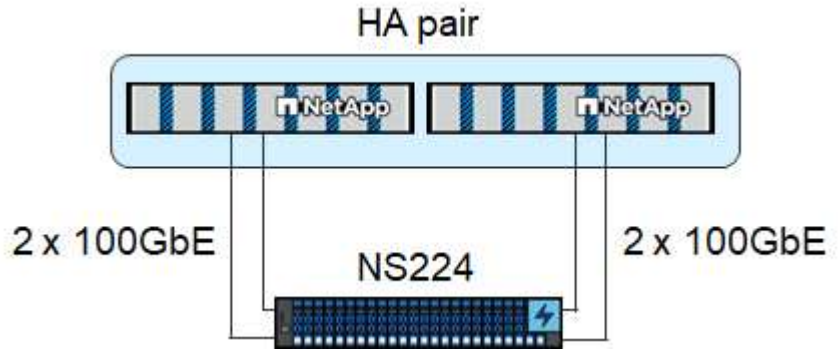
È possibile collegare un massimo di uno shelf di dischi a uno stack SAS per fornire le prestazioni richieste per gli host SAP HANA, come mostrato nella figura seguente. I dischi all'interno di ogni shelf devono essere distribuiti in modo uguale a entrambi i controller della coppia ha. ADPv2 viene utilizzato con ONTAP 9 e gli shelf di dischi DS224C.

Con lo shelf di dischi DS224C, è possibile utilizzare anche il cablaggio SAS quad-path, ma non è necessario.



Shelf di dischi NVMe (100 GbE)

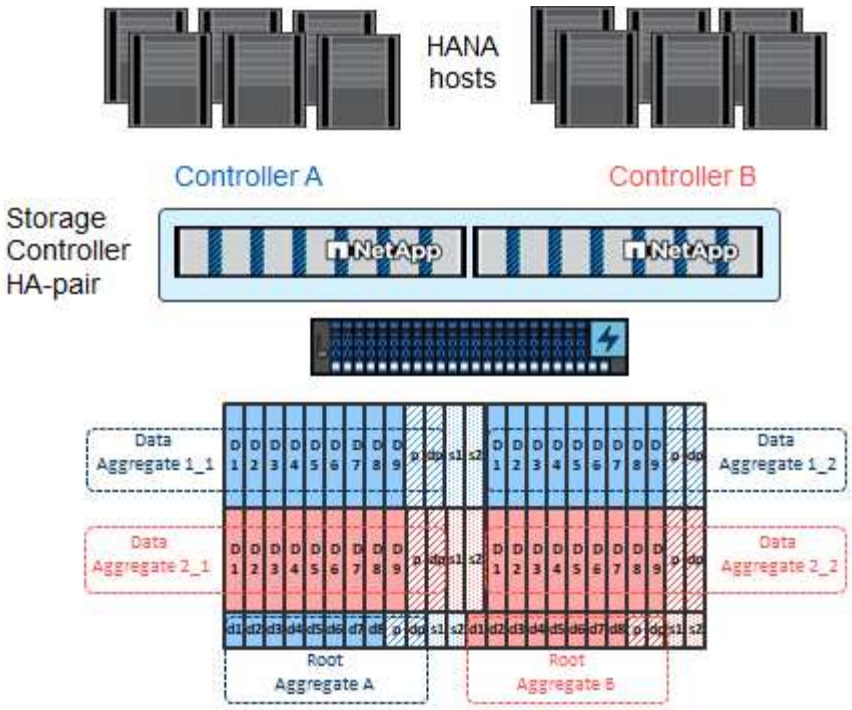
Ogni shelf di dischi NS224 NVMe è collegato a due porte 100GbE per controller, come illustrato nella figura seguente. I dischi all'interno di ogni shelf devono essere distribuiti in modo uguale a entrambi i controller della coppia ha. ADPv2, come descritto nel capitolo sulla configurazione degli aggregati, viene utilizzato anche per lo shelf di dischi NS224.



Configurazione dell'aggregato

In generale, è necessario configurare due aggregati per controller, indipendentemente dallo shelf di dischi o dalla tecnologia dei dischi (SSD SAS o SSD NVMe) utilizzata.

L'immagine seguente mostra una configurazione di 12 host SAP HANA in esecuzione su uno shelf SAS da 12 GB configurato con ADPv2. Sei host SAP HANA sono collegati a ciascun controller di storage. Sono configurati quattro aggregati separati, due per ogni controller di storage. Ogni aggregato è configurato con 11 dischi con nove partizioni di dati e due di dischi di parità. Per ciascun controller sono disponibili due partizioni di riserva.



Configurazione SVM

Diversi ambienti SAP con database SAP HANA possono utilizzare una singola SVM. È possibile assegnare una SVM a ciascun ambiente SAP, se necessario, nel caso in cui sia gestita da diversi team all'interno di un'azienda.

Se viene creato e assegnato automaticamente un profilo QoS durante la creazione di una nuova SVM, rimuovere questo profilo creato automaticamente dalla SVM per abilitare le prestazioni richieste per SAP HANA:

```
vserver modify -vserver <svm-name> -qos-policy-group none
```

Configurazione LIF

Per i sistemi di produzione SAP HANA, è necessario utilizzare diversi LIF per montare il volume di dati e il volume di log dall'host SAP HANA. Pertanto, sono necessari almeno due LIF.

I montaggi di volumi di dati e log di diversi host SAP HANA possono condividere una porta di rete dello storage fisico utilizzando gli stessi LIF o utilizzando singoli LIF per ogni montaggio.

La quantità massima di dati e volumi di log per interfaccia fisica è illustrata nella tabella seguente.

Velocità della porta Ethernet	10 GbE	25 GbE	40 GbE	100GeE
Numero massimo di montaggi di volumi di log o dati per porta fisica	3	8	12	30

La condivisione di una LIF tra diversi host SAP HANA potrebbe richiedere un remount di volumi di dati o log in un LIF diverso. Questa modifica consente di evitare penalizzazioni delle performance se un volume viene spostato in un controller di storage diverso.

I sistemi di sviluppo e test possono utilizzare più dati e volumi o LIF su un'interfaccia di rete fisica.

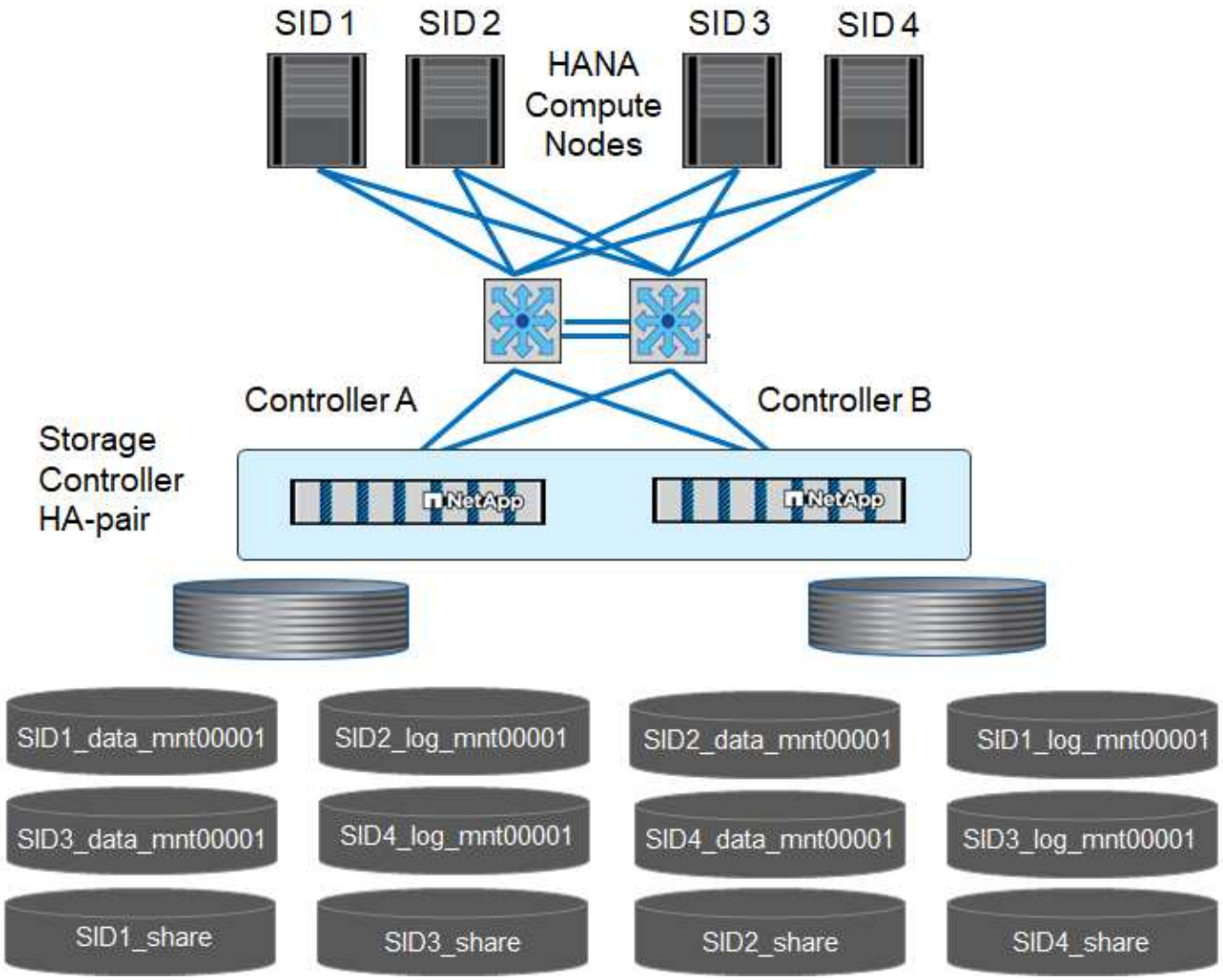
Per i sistemi di produzione, sviluppo e test, il `/hana/shared` Il file system può utilizzare la stessa LIF del volume di dati o di log.

Configurazione dei volumi per sistemi SAP HANA a host singolo

La figura seguente mostra la configurazione dei volumi di quattro sistemi SAP HANA a host singolo. I volumi di dati e log di ciascun sistema SAP HANA vengono distribuiti a diversi storage controller. Ad esempio, volume `SID1_data_mnt00001` È configurato sul controller A e sul volume `SID1_log_mnt00001` È configurato sul controller B.

Se per i sistemi SAP HANA viene utilizzato un solo storage controller di una coppia ha, è possibile memorizzare dati e volumi di log nello stesso storage controller.

Se i dati e i volumi di log sono memorizzati sullo stesso controller, l'accesso dal server allo storage deve essere eseguito con due LIF differenti: Una LIF per accedere al volume di dati e l'altra per accedere al volume di log.



Per ogni host SAP HANA, un volume di dati, un volume di log e un volume per `/hana/shared` sono configurati. La seguente tabella mostra un esempio di configurazione per i sistemi SAP HANA a host singolo.

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller b
Dati, log e volumi condivisi per il sistema SID1	Volume di dati: SID1_data_mnt00001	Volume condiviso: SID1_shared	–	Volume di log: SID1_log_mnt00001
Dati, log e volumi condivisi per il sistema SID2	–	Volume di log: SID2_log_mnt00001	Volume di dati: SID2_data_mnt00001	Volume condiviso: SID2_shared
Dati, log e volumi condivisi per il sistema SID3	Volume condiviso: SID3_shared	Volume di dati: SID3_data_mnt00001	Volume di log: SID3_log_mnt00001	–
Dati, log e volumi condivisi per il sistema SID4	Volume di log: SID4_log_mnt00001	–	Volume condiviso: SID4_shared	Volume di dati: SID4_data_mnt00001

La seguente tabella mostra un esempio di configurazione del punto di montaggio per un sistema a host singolo. Per inserire la home directory di `sidadm` sullo storage centrale, il `/usr/sap/SID` il file system deve

essere montato da `SID_shared` volume.

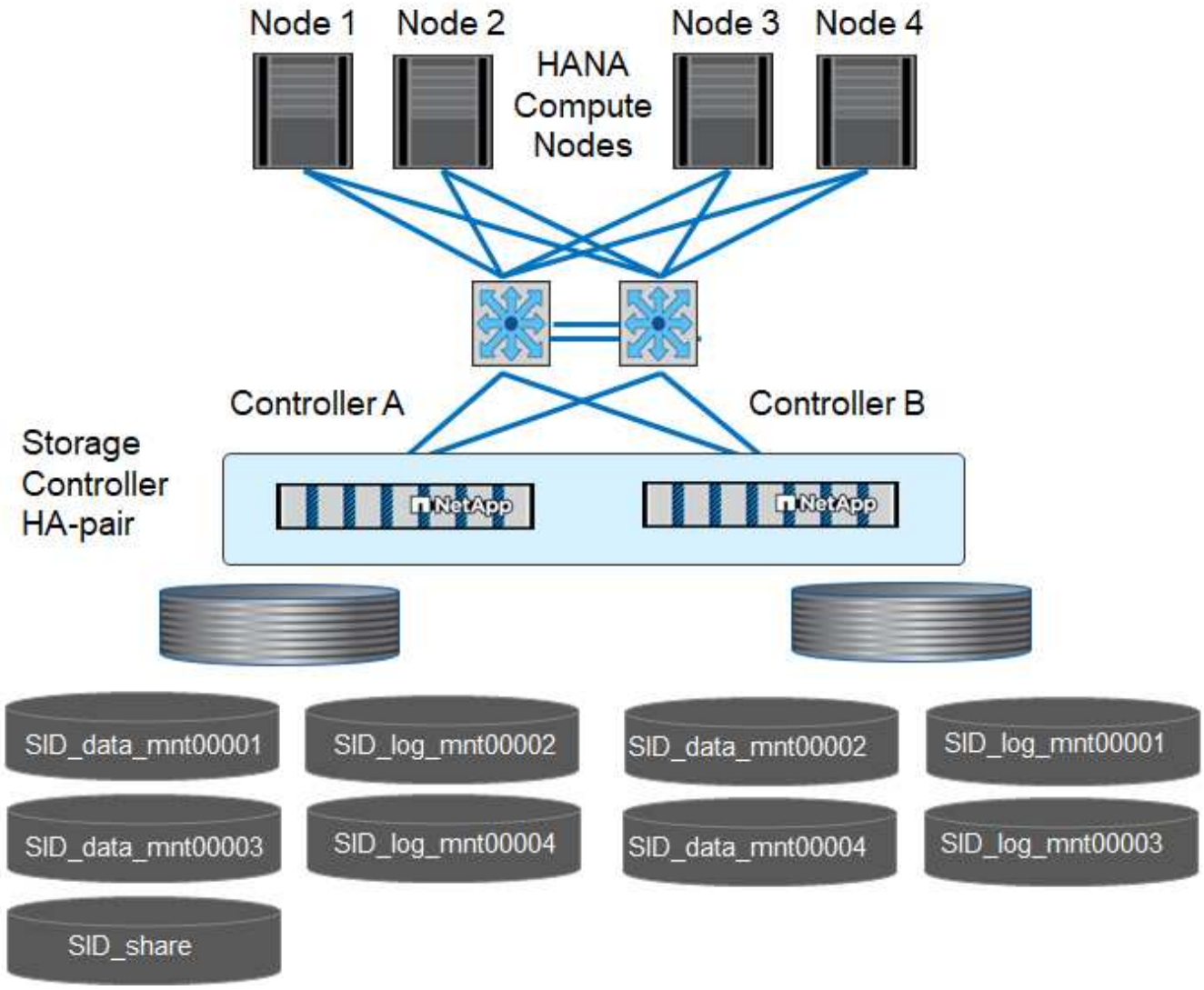
Percorso di giunzione	Directory	Punto di montaggio sull'host HANA
SID_data_mnt00001		/hana/data/SID/mnt00001
SID_log_mnt00001		/hana/log/SID/mnt00001
SID_shared	usr-sap condiviso	/Usr/sap/SID /hana/shared/

Configurazione dei volumi per sistemi SAP HANA con host multipli

La figura seguente mostra la configurazione del volume di un sistema SAP HANA 4+1. I volumi di dati e log di ciascun host SAP HANA vengono distribuiti a diversi storage controller. Ad esempio, volume `SID1_data1_mnt00001` È configurato sul controller A e sul volume `SID1_log1_mnt00001` È configurato sul controller B.

Se per il sistema SAP HANA viene utilizzato un solo storage controller di una coppia ha, i volumi di dati e log possono essere memorizzati anche sullo stesso storage controller.

Se i dati e i volumi di log sono memorizzati sullo stesso controller, l'accesso dal server allo storage deve essere eseguito con due LIF differenti: Una LIF per accedere al volume di dati e una per accedere al volume di log.



Per ogni host SAP HANA, vengono creati un volume di dati e un volume di log. Il `/hana/shared` Il volume viene utilizzato da tutti gli host del sistema SAP HANA. La seguente tabella mostra un esempio di configurazione per un sistema SAP HANA con host multipli con quattro host attivi.

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 nel controller B.	Aggregato 2 nel controller B.
Volumi di dati e log per il nodo 1	Volume di dati: SID_data_mnt00001	–	Volume di log: SID_log_mnt00001	–
Volumi di dati e log per il nodo 2	Volume di log: SID_log_mnt00002	–	Volume di dati: SID_data_mnt00002	–
Volumi di dati e log per il nodo 3	–	Volume di dati: SID_data_mnt00003	–	Volume di log: SID_log_mnt00003
Volumi di dati e log per il nodo 4	–	Volume di log: SID_log_mnt00004	–	Volume di dati: SID_data_mnt00004
Volume condiviso per tutti gli host	Volume condiviso: SID_shared			

La seguente tabella mostra la configurazione e i punti di montaggio di un sistema a più host con quattro host

SAP HANA attivi. Per inserire le home directory di `sidadm` utente di ciascun host sullo storage centrale, il `/usr/sap/SID` i file system vengono montati da `SID_shared` volume.

Percorso di giunzione	Directory	Punto di montaggio sull'host SAP HANA	Nota
SID_data_mnt00001	–	/hana/data/SID/mnt00001	Montato su tutti gli host
SID_log_mnt00001	–	/hana/log/SID/mnt00001	Montato su tutti gli host
SID_data_mnt00002	–	/hana/data/SID/mnt00002	Montato su tutti gli host
SID_log_mnt00002	–	/hana/log/SID/mnt00002	Montato su tutti gli host
SID_data_mnt00003	–	/hana/data/SID/mnt00003	Montato su tutti gli host
SID_log_mnt00003	–	/hana/log/SID/mnt00003	Montato su tutti gli host
SID_data_mnt00004	–	/hana/data/SID/mnt00004	Montato su tutti gli host
SID_log_mnt00004	–	/hana/log/SID/mnt00004	Montato su tutti gli host
SID_shared	condiviso	/hana/shared/SID	Montato su tutti gli host
SID_shared	usr-sap-host1	/Usr/sap/SID	Montato sull'host 1
SID_shared	usr-sap-host2	/Usr/sap/SID	Montato sull'host 2
SID_shared	usr-sap-host3	/Usr/sap/SID	Montato sull'host 3
SID_shared	usr-sap-host4	/Usr/sap/SID	Montato sull'host 4
SID_shared	usr-sap-host5	/Usr/sap/SID	Montato sull'host 5

Opzioni del volume

È necessario verificare e impostare le opzioni del volume elencate nella tabella seguente su tutte le SVM. Per alcuni comandi, è necessario passare alla modalità avanzata dei privilegi in ONTAP.

Azione	Comando
Disattiva la visibilità della directory Snapshot	vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false
Disattivare le copie Snapshot automatiche	vol modify –vserver <vserver-name> -volume <volname> -snapshot-policy none
Disattiva l'aggiornamento del tempo di accesso, ad eccezione del volume SID_shared	set advanced vol modify -vserver <vserver-name> -volume <volname> -atime-update false set admin

Configurazione NFS per NFSv3

Le opzioni NFS elencate nella seguente tabella devono essere verificate e impostate su tutti i controller di storage. Per alcuni dei comandi mostrati in questa tabella, è necessario passare alla modalità avanzata dei privilegi.

Azione	Comando
Abilitare NFSv3	nfs modify -vserver <vserver-name> v3.0 abilitato

Azione	Comando
Impostare la dimensione massima di trasferimento TCP NFS su 1MB	set advanced nfs modify -vserver <vserver_name> -tcp-max-xfer-size 1048576 set admin

In ambienti condivisi con carichi di lavoro diversi, impostare le dimensioni massime di trasferimento TCP NFS su 262144

Configurazione NFS per NFSv4

Le opzioni NFS elencate nella seguente tabella devono essere verificate e impostate su tutte le SVM.

Per alcuni comandi di questa tabella, è necessario passare alla modalità avanzata dei privilegi.

Azione	Comando
Abilitare NFSv4	nfs modify -vserver <vserver-name> -v4.1 abilitato
Impostare la dimensione massima di trasferimento TCP NFS su 1MB	set advanced nfs modify -vserver <vserver_name> -tcp-max-xfer-size 1048576 set admin
Disattiva gli elenchi di controllo di accesso (ACL) NFSv4	nfs modify -vserver <vserver_name> -v4.1-acl disabled
Impostare l'ID di dominio NFSv4	nfs modify -vserver <vserver_name> -v4-id-domain <domain-name>
Disattiva la delega di lettura NFSv4	nfs modify -vserver <vserver_name> -v4.1-read -delegation disabled
Disattiva la delega di scrittura NFSv4	nfs modify -vserver <vserver_name> -v4.1-write -delegation disabled
Disattiva id numerici NFSv4	nfs modify -vserver <vserver_name> -v4-numeric-ids disabled
Modificare il numero di slot di sessione NFSv4.x opzionale	imposta avanzate nfs modify -vserver hana -v4.x-session-num-slot <value> impostare admin

In ambienti condivisi con carichi di lavoro diversi, impostare le dimensioni massime di trasferimento TCP NFS su 262144

La disattivazione degli id numerici richiede la gestione degli utenti, come descritto nella sezione ""Preparazione dell'installazione di SAP HANA per NFSv4.""

L'ID del dominio NFSv4 deve essere impostato sullo stesso valore su tutti i server Linux (`/etc/idmapd.conf`) e sulle SVM, come descritto nella sezione ""Preparazione dell'installazione di SAP HANA per NFSv4.""

PNFS può essere attivato ed utilizzato.

Se si utilizzano sistemi SAP HANA a host multipli con failover automatico dell'host, è necessario regolare i

parametri di failover all'interno di `nameserver.ini` come mostrato nella tabella seguente. Mantenere l'intervallo di ripetizione predefinito di 10 secondi all'interno di queste sezioni.

Sezione all'interno di nameserver.ini	Parametro	Valore
failover	normal_rettry	9
distributed_watchdog	dischase_retretres	11
distributed_watchdog	takeover_retries	9

Montare i volumi nello spazio dei nomi e impostare i criteri di esportazione

Quando viene creato un volume, il volume deve essere montato nello spazio dei nomi. In questo documento, si presuppone che il nome del percorso di giunzione sia lo stesso del nome del volume. Per impostazione predefinita, il volume viene esportato con il criterio predefinito. Se necessario, è possibile adattare la policy di esportazione.

Configurazione dell'host

Tutte le fasi di configurazione degli host descritte in questa sezione sono valide per gli ambienti SAP HANA su server fisici e per SAP HANA in esecuzione su VMware vSphere.

Parametro di configurazione per SUSE Linux Enterprise Server

I parametri aggiuntivi di kernel e configurazione di ciascun host SAP HANA devono essere regolati in base al carico di lavoro generato da SAP HANA.

SUSE Linux Enterprise Server 12 e 15

A partire da SUSE Linux Enterprise Server 12 SP1, il parametro kernel deve essere impostato in un file di configurazione in `/etc/sysctl.d` directory. Ad esempio, è necessario creare un file di configurazione con il nome `91-NetApp-HANA.conf`.

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384  16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle=0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_max_slot_table_entries = 128
```

Saptune, incluso in SLES per le versioni di SAP OS, può essere utilizzato per impostare questi valori. Per ulteriori informazioni, vedere "Nota SAP 3024346" (Richiede l'accesso SAP).

Parametri di configurazione per Red Hat Enterprise Linux 7.2 o versioni successive

È necessario regolare altri parametri di kernel e configurazione in ogni host SAP HANA per il carico di lavoro generato da SAP HANA.

A partire da Red Hat Enterprise Linux 7.2, è necessario impostare i parametri del kernel in un file di configurazione in `/etc/sysctl.d` directory. Ad esempio, è necessario creare un file di configurazione con il nome `91-NetApp-HANA.conf`.

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384  16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle = 0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_max_slot_table_entries = 128
```

A partire dalla versione 8.6 di RedHat Enterprise Linux, le impostazioni possono essere applicate anche utilizzando i ruoli di sistema RHEL per SAP (Ansible). Vedere "Nota SAP 3024346" (Richiede l'accesso SAP).

Creare sottodirectory in /hana/volume condiviso

Gli esempi seguenti mostrano un database SAP HANA con SID=NF2.

Per creare le sottodirectory richieste, eseguire una delle seguenti operazioni:

- Per un sistema a host singolo, montare `/hana/shared` e creare il `shared` e. `usr-sap` sottodirectory.

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap
sapcc-hana-tst-06:/mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

- Per un sistema a più host, montare `/hana/shared` e creare il `shared` e a. `usr-sap` sottodirectory per ciascun host.

I comandi di esempio mostrano un sistema HANA 2+1 multi-host.

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host1
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host2
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host3
sapcc-hana-tst-06:/mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

Creare punti di montaggio

Gli esempi seguenti mostrano un database SAP HANA con SID=NF2.

Per creare le directory dei punti di montaggio richieste, eseguire una delle seguenti operazioni:

- Per un sistema a host singolo, creare punti di montaggio e impostare le autorizzazioni sull'host del database.

```
sapcc-hana-tst-06:/ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/shared
sapcc-hana-tst-06:/ # mkdir -p /usr/sap/NF2

sapcc-hana-tst-06:/ # chmod –R 777 /hana/log/NF2
sapcc-hana-tst-06:/ # chmod –R 777 /hana/data/NF2
sapcc-hana-tst-06:/ # chmod –R 777 /hana/shared
sapcc-hana-tst-06:/ # chmod –R 777 /usr/sap/NF2
```

- Per un sistema a più host, creare punti di montaggio e impostare le autorizzazioni su tutti gli host worker e standby. I seguenti comandi di esempio si riferiscono a un sistema HANA con host multiplo 2+1.
  - Primo host di lavoro:

```
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/shared
sapcc-hana-tst-06:~ # mkdir -p /usr/sap/NF2

sapcc-hana-tst-06:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:~ # chmod -R 777 /usr/sap/NF2
```

- Secondo host di lavoro:

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/shared
sapcc-hana-tst-07:~ # mkdir -p /usr/sap/NF2

sapcc-hana-tst-07:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-07:~ # chmod -R 777 /usr/sap/NF2
```

- Host in standby:

```
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/shared
sapcc-hana-tst-08:~ # mkdir -p /usr/sap/NF2

sapcc-hana-tst-08:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-08:~ # chmod -R 777 /usr/sap/NF2
```

Montare i file system

A seconda della versione di NFS e della release di ONTAP, è necessario utilizzare diverse opzioni di montaggio. I seguenti file system devono essere montati sugli host:

- `/hana/data/SID/mnt0000*`
- `/hana/log/SID/mnt0000*`
- `/hana/shared`
- `/usr/sap/SID`

La seguente tabella mostra le versioni di NFS da utilizzare per i diversi file system per i database SAP HANA a host singolo e multiplo.

File system	Host singolo SAP HANA	SAP HANA host multipli
/hana/data/SID/mnt0000*	NFSv3 o NFSv4	NFSv4
/hana/log/SID/mnt0000*	NFSv3 o NFSv4	NFSv4
/hana/shared	NFSv3 o NFSv4	NFSv3 o NFSv4
/Usr/sap/SID	NFSv3 o NFSv4	NFSv3 o NFSv4

La seguente tabella mostra le opzioni di montaggio per le varie versioni di NFS e le release di ONTAP. I parametri comuni sono indipendenti dalle versioni di NFS e ONTAP.

SAP lama richiede che la directory /usr/sap/SID sia locale. Pertanto, non montare un volume NFS per /usr/sap/SID se si utilizza SAP lama.

Per NFSv3, è necessario disattivare il blocco NFS per evitare le operazioni di pulitura del blocco NFS in caso di guasto del software o del server.

Con ONTAP 9, le dimensioni di trasferimento NFS possono essere configurate fino a 1 MB. In particolare, con connessioni a 40 GbE o più veloci al sistema storage, è necessario impostare le dimensioni di trasferimento su 1 MB per ottenere i valori di throughput previsti.

Parametro comune	NFSv3	NFSv4	Dimensione del trasferimento NFS con ONTAP 9	Dimensione del trasferimento NFS con ONTAP 8
rw, bg, hard, time=600, noatime	nfsvers=3,nolock	nfsvers=4.1,lock	rsize=1048576,wsize=262144	rsize=65536,wsize=65536

Per migliorare le prestazioni di lettura con NFSv3, NetApp consiglia di utilizzare `nconnect=n` Opzione di montaggio, disponibile con SUSE Linux Enterprise Server 12 SP4 o versione successiva e RedHat Enterprise Linux (RHEL) 8.3 o versione successiva.

I test delle performance lo hanno dimostrato `nconnect=4` fornisce buoni risultati di lettura per i volumi di dati. Le scritture dei log potrebbero trarre vantaggio da un numero inferiore di sessioni, ad esempio `nconnect=2`. Anche i volumi condivisi possono trarre vantaggio dall'utilizzo dell'opzione 'nconnect'. Tenere presente che il primo mount da un server NFS (indirizzo IP) definisce il numero di sessioni utilizzate. Ulteriori montaggi sullo stesso indirizzo IP non modificano questo valore anche se per nconnect viene utilizzato un valore diverso.

A partire da ONTAP 9.8 e SUSE SLES15SP2 o RedHat RHEL 8.4 o superiore, NetApp supporta l'opzione nconnect anche per NFSv4.1. Per ulteriori informazioni, consultare la documentazione del vendor Linux.

Se nconnect viene utilizzato con NFSv4.x, la quantità di slot di sessione NFSv4.x deve essere regolata in base alla regola seguente: Numero di slot di sessione uguale a <nconnect value> x 64. All'host questo sarà adjusted da seguito da `echo options nfs max_session_slots=<calculated value> > /etc/modprobe.d/nfsclient.conf` un riavvio. Anche il valore lato server deve essere regolato, impostare il numero di slot di sessione come descritto in "Configurazione NFS per NFSv4."

L'esempio seguente mostra un database SAP HANA host singolo con SID=NF2 utilizzando NFSv3 e una dimensione di trasferimento NFS di 1 MB per le letture e 256k per le scritture. Per montare i file system durante l'avvio del sistema con `/etc/fstab` file di configurazione, attenersi alla seguente procedura:

1. Aggiungere i file system richiesti a `/etc/fstab` file di configurazione.

```
sapcc-hana-tst-06:/ # cat /etc/fstab
<storage-vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data01>:/NF2_shared/usr-sap /usr/sap/NF2 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data01>:/NF2_shared/shared /hana/shared nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
```

2. Eseguire `mount -a` per montare i file system su tutti gli host.

Nell'esempio successivo viene illustrato un database SAP HANA multihost con SID=NF2 utilizzando NFSv4.1 per i file system di dati e log e NFSv3 per `/hana/shared` e. `/usr/sap/NF2` file system. Viene utilizzata una dimensione di trasferimento NFS di 1 MB per le letture e 256k per le scritture.

1. Aggiungere i file system richiesti a `/etc/fstab` file di configurazione su tutti gli host.

Il `/usr/sap/NF2` il file system è diverso per ciascun host di database. Viene mostrato l'esempio seguente `/NF2_shared/usr-sap-host1`.

```
stlrx300s8-5:/ # cat /etc/fstab
<storage-vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-data02>:/NF2_data_mnt00002 /hana/data/NF2/mnt00002 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-log02>:/NF2_log_mnt00002 /hana/log/NF2/mnt00002 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-data02>:/NF2_shared/usr-sap-host1 /usr/sap/NF2 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data02>:/NF2_shared/shared /hana/shared nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
```

2. Eseguire `mount -a` per montare i file system su tutti gli host.

Preparazione dell'installazione di SAP HANA per NFSv4

NFS versione 4 e successive richiede l'autenticazione dell'utente. Questa autenticazione può essere eseguita utilizzando uno strumento di gestione utente centrale, ad esempio un server LDAP (Lightweight Directory Access Protocol) o con account utente locali. Le sezioni seguenti descrivono come configurare gli account utente locali.

Gli utenti amministrativi `<sid>adm`,`<sid>crypt` e il `sapsys` gruppo devono essere creati manualmente sugli host SAP HANA e sugli storage controller prima che venga avviata l'installazione del software SAP HANA.

Host SAP HANA

Se non esiste, il `sapsys` Il gruppo deve essere creato sull'host SAP HANA. È necessario scegliere un ID di gruppo univoco che non sia in conflitto con gli ID di gruppo esistenti sui controller di storage.

Gli utenti `<sid>adm` e `<sid>crypt` vengono creati sull'host SAP HANA. È necessario scegliere ID univoci che non siano in conflitto con gli ID utente esistenti sui controller di archiviazione.

Per un sistema SAP HANA con host multipli, gli ID utente e gruppo devono essere gli stessi su tutti gli host SAP HANA. Il gruppo e l'utente vengono creati sugli altri host SAP HANA copiando le linee interessate da e `/etc/passwd` nel `/etc/group` sistema di origine a tutti gli altri host SAP HANA.

Per un sistema SAP HANA con host multipli, l'ID utente e il ID gruppo devono essere identici su tutti gli host SAP HANA. Il gruppo e l'utente vengono creati sugli altri host SAP HANA copiando le linee interessate in `/etc/group` e. `/etc/passwd` Dal sistema di origine a tutti gli altri host SAP HANA.

Il dominio NFSv4 deve essere impostato sullo stesso valore su tutti i server Linux e le SVM. Impostare il parametro di dominio "`Domain = <domain_name>`" nel file `/etc/idmapd.conf` Per gli host Linux.

Abilitare e avviare il servizio NFS idmapd:

```
systemctl enable nfs-idmapd.service
systemctl start nfs-idmapd.service
```

I kernel Linux più recenti non richiedono questo passaggio. È possibile ignorare i messaggi di avviso in tutta sicurezza.

Controller di storage

L'ID utente e l'ID gruppo devono essere identici negli host SAP HANA e nei controller di storage. Il gruppo e l'utente vengono creati immettendo i seguenti comandi sul cluster di storage:

```
vserver services unix-group create -vserver <vserver> -name <group name>
-id <group id>
vserver services unix-user create -vserver <vserver> -user <user name> -id
<user-id> -primary-gid <group id>
```

Inoltre, impostare l'ID del gruppo della root utente UNIX della SVM su 0.

```
vserver services unix-user modify -vserver <vserver> -user root -primary
-gid 0
```

Configurazione dello stack di i/o per SAP HANA

A partire da SAP HANA 1.0 SPS10, SAP ha introdotto i parametri per regolare il comportamento di i/o e ottimizzare il database per i file e i sistemi storage utilizzati.

NetApp ha condotto test delle performance per definire i valori ideali. La seguente tabella elenca i valori ottimali dedotti dai test delle prestazioni.

Parametro	Valore
max_parallel_io_requests	128
async_read_submit	acceso
async_write_submit_active	acceso
async_write_submit_blocks	tutto

Per le versioni SAP HANA 1.0 fino a SPS12, questi parametri possono essere impostati durante l'installazione del database SAP HANA, come descritto nella nota SAP "2267798: Configurazione del database SAP HANA durante l'installazione con hdbparam".

In alternativa, è possibile impostare i parametri dopo l'installazione del database SAP HANA utilizzando `hdbparam` framework.

```
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_read_submit=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

A partire da SAP HANA 2.0, `hdbparam` è stato obsoleto e i parametri sono stati spostati in `global.ini`. I parametri possono essere impostati utilizzando i comandi SQL o SAP HANA Studio. Per ulteriori informazioni, consulta la nota SAP "2399079: Eliminazione di hdbparam in HANA 2". I parametri possono essere impostati anche all'interno del global.ini, come mostrato di seguito:

```
nf2adm@stlrx300s8-6: /usr/sap/NF2/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

A partire da SAP HANA 2.0 SPS5, è possibile utilizzare `setParameter.py` script per impostare i parametri corretti:

```
nf2adm@sapcc-hana-tst-03:/usr/sap/NF2/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

Dimensioni del volume di dati SAP HANA

Per impostazione predefinita, SAP HANA utilizza un solo volume di dati per ogni servizio SAP HANA. A causa della limitazione delle dimensioni massime del file system, NetApp consiglia di limitare le dimensioni massime del volume di dati.

Per eseguire questa operazione automaticamente, impostare il seguente parametro in `global.ini` nella sezione `[persistence]`:

```
datavolume_striping = true
datavolume_striping_size_gb = 8000
```

Questo crea un nuovo volume di dati dopo il raggiungimento del limite di 8.000 GB. "Nota SAP 240005 domanda 15" fornisce ulteriori informazioni.

Installazione del software SAP HANA

In questa sezione viene descritto come configurare un sistema per l'installazione del software SAP HANA su sistemi a host singolo e multiplo.

Installazione su un sistema a host singolo

L'installazione del software SAP HANA non richiede alcuna preparazione aggiuntiva per un sistema a singolo host.

Installazione su un sistema a più host

Per installare SAP HANA su un sistema a più host, attenersi alla seguente procedura:

1. Utilizzando lo strumento di installazione SAP `hdbclm`, avviare l'installazione eseguendo il comando seguente su uno degli host di lavoro. Utilizzare l' `addhosts`opzione per aggiungere il secondo worker (`sapcc-hana-tst-03`) e l'host di standby)(`sapcc-hana-tst-04`.

```
apcc-hana-tst-02:/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_LCM_LINUX_X86_64 #
./hdblcm --action=install --addhosts=sapcc-hana-tst-03:role=worker,sapcc
-hana-tst-04:role=standby

SAP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
```

```
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1
(1.015.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip
```

```
SAP HANA Database version '2.00.073.00.1695288802' will be installed.

Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------
-------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version
2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
  9     | epmmds          | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
4.203.2321.0.0

Enter comma-separated list of the selected indices [3,4]: 2,3
```

2. Verificare che lo strumento di installazione abbia installato tutti i componenti selezionati su tutti gli host di lavoro e di standby.

Aggiunta di partizioni di volumi di dati aggiuntive

A partire da SAP HANA 2.0 SPS4, è possibile configurare ulteriori partizioni del volume di dati. Ciò consente di configurare due o più volumi per il volume di dati di un database tenant SAP HANA e di scalare oltre i limiti di dimensioni e performance di un singolo volume.

> L'utilizzo di due o più volumi singoli per il volume di dati è disponibile per i sistemi SAP HANA single-host e SAP HANA multi-host. È possibile aggiungere ulteriori partizioni del volume di dati in qualsiasi momento.

Attivazione di partizioni di volumi di dati aggiuntive

Per abilitare ulteriori partizioni del volume di dati, aggiungere la seguente voce all'interno di `global.ini` Utilizzando SAP HANA Studio o Cockpit nella configurazione SYSTEMDB.

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

Aggiunta manuale del parametro a `global.ini` il file richiede il riavvio del database.

Configurazione dei volumi per sistemi SAP HANA a host singolo

Il layout dei volumi per un sistema SAP HANA a host singolo con più partizioni è simile al layout per un sistema con una partizione del volume di dati ma con un volume di dati aggiuntivo memorizzato su un aggregato diverso come il volume di log e l'altro volume di dati. La seguente tabella mostra un esempio di configurazione di un sistema SAP HANA a host singolo con due partizioni del volume di dati.

Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 nel controller B.	Aggregato 2 nel controller b
Volume di dati: SID_data_mnt00001	Volume condiviso: SID_shared	Volume di dati: SID_data2_mnt00001	Volume di log: SID_log_mnt00001

La seguente tabella mostra un esempio di configurazione del punto di montaggio per un sistema a host singolo con due partizioni del volume di dati.

Percorso di giunzione	Directory	Punto di montaggio sull'host HANA
SID_data_mnt00001	–	/hana/data/SID/mnt00001
SID_data2_mnt00001	–	/hana/data2/SID/mnt00001
SID_log_mnt00001	–	/hana/log/SID/mnt00001
SID_shared	usr-sap condiviso	/Usr/sap/SID /hana/shared

È possibile creare il nuovo volume di dati e montarlo nello spazio dei nomi utilizzando Gestore di sistema NetApp ONTAP o l'interfaccia utente di ONTAP.

Configurazione dei volumi per sistemi SAP HANA multihost

Il layout dei volumi è simile al layout di un sistema SAP HANA con host multipli con una partizione del volume di dati ma con un volume di dati aggiuntivo memorizzato su un aggregato diverso come volume di log e l'altro volume di dati. La seguente tabella mostra un esempio di configurazione di un sistema SAP HANA con host multipli con due partizioni di volumi di dati.

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 nel controller B.	Aggregato 2 nel controller B.
Volumi di dati e log per il nodo 1	Volume di dati: SID_data_mnt00001	–	Volume di log: SID_log_mnt00001	Volume Data2: SID_data2_mnt00001

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 nel controller B.	Aggregato 2 nel controller B.
Volumi di dati e log per il nodo 2	Volume di log: SID_log_mnt00002	Volume Data2: SID_data2_mnt00002	Volume di dati: SID_data_mnt00002	–
Volumi di dati e log per il nodo 3	–	Volume di dati: SID_data_mnt00003	Volume Data2: SID_data2_mnt00003	Volume di log: SID_log_mnt00003
Volumi di dati e log per il nodo 4	Volume Data2: SID_data2_mnt00004	Volume di log: SID_log_mnt00004	–	Volume di dati: SID_data_mnt00004
Volume condiviso per tutti gli host	Volume condiviso: SID_shared	–	–	–

La seguente tabella mostra un esempio di configurazione del punto di montaggio per un sistema a host singolo con due partizioni del volume di dati.

Percorso di giunzione	Directory	Punto di montaggio sull'host SAP HANA	Nota
SID_data_mnt00001	–	/hana/data/SID/mnt00001	Montato su tutti gli host
SID_data2_mnt00001	–	/hana/data2/SID/mnt00001	Montato su tutti gli host
SID_log_mnt00001	–	/hana/log/SID/mnt00001	Montato su tutti gli host
SID_data_mnt00002	–	/hana/data/SID/mnt00002	Montato su tutti gli host
SID_data2_mnt00002	–	/hana/data2/SID/mnt00002	Montato su tutti gli host
SID_log_mnt00002	–	/hana/log/SID/mnt00002	Montato su tutti gli host
SID_data_mnt00003	–	/hana/data/SID/mnt00003	Montato su tutti gli host
SID_data2_mnt00003		/hana/data2/SID/mnt00003	Montato su tutti gli host
SID_log_mnt00003		/hana/log/SID/mnt00003	Montato su tutti gli host
SID_data_mnt00004		/hana/data/SID/mnt00004	Montato su tutti gli host
SID_data2_mnt00004	–	/hana/data2/SID/mnt00004	Montato su tutti gli host
SID_log_mnt00004	–	/hana/log/SID/mnt00004	Montato su tutti gli host
SID_shared	condiviso	/hana/shared/SID	Montato su tutti gli host
SID_shared	usr-sap-host1	/Usr/sap/SID	Montato sull'host 1
SID_shared	usr-sap-host2	/Usr/sap/SID	Montato sull'host 2
SID_shared	usr-sap-host3	/Usr/sap/SID	Montato sull'host 3
SID_shared	usr-sap-host4	/Usr/sap/SID	Montato sull'host 4

Percorso di giunzione	Directory	Punto di montaggio sull'host SAP HANA	Nota
SID_shared	usr-sap-host5	/Usr/sap/SID	Montato sull'host 5

È possibile creare il nuovo volume di dati e montarlo nello spazio dei nomi utilizzando Gestore di sistema di ONTAP o l'interfaccia utente di ONTAP.

Configurazione dell'host

Oltre alle attività descritte nella sezione, "Configurazione dell'host,"è necessario creare ulteriori punti di montaggio e `fstab` voci per i nuovi volumi di dati aggiuntivi e montare i nuovi volumi.

1. Creare punti di montaggio aggiuntivi.
   - Per un sistema a host singolo, creare punti di montaggio e impostare le autorizzazioni sull'host del database:

     ```
     sapcc-hana-tst-06:/ # mkdir -p /hana/data2/SID/mnt00001
     sapcc-hana-tst-06:/ # chmod –R 777 /hana/data2/SID
     ```

   - Per un sistema a più host, creare punti di montaggio e impostare le autorizzazioni su tutti gli host worker e standby.

     I seguenti comandi di esempio si riferiscono a un sistema HANA multihost 2-Plus-1.

     - Primo host di lavoro:

       ```
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-06:~ # chmod -R 777 /hana/data2/SID
       ```

     - Secondo host di lavoro:

       ```
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
       ```

     - Host in standby:

       ```
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
       ```

2. Aggiungere i file system aggiuntivi a `/etc/fstab` file di configurazione su tutti gli host.

   Vedere l'esempio seguente per un sistema a host singolo che utilizza NFSv4.1:

```
<storage-vif-data02>:/SID_data2_mnt00001 /hana/data2/SID/mnt00001 nfs
rw, vers=4
minorversion=1,hard,timeo=600,rsize=1048576,wsize=262144,bg,noatime,lock
0 0
```

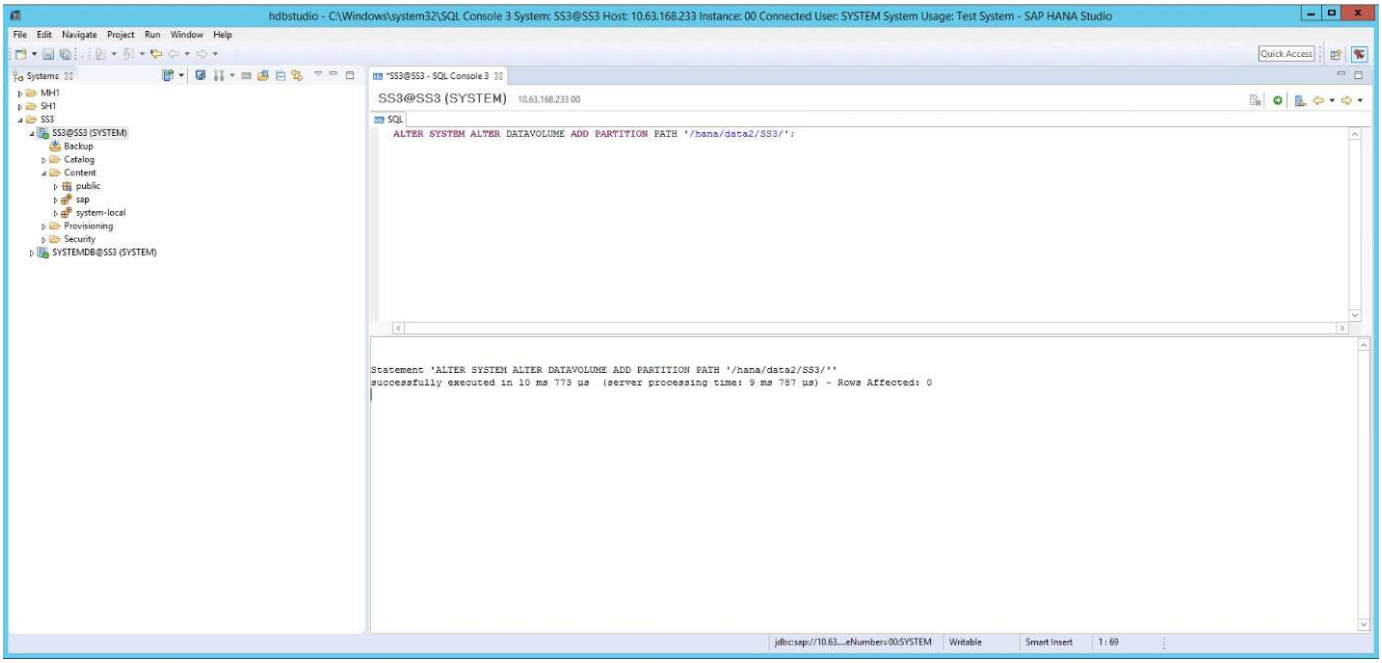
Utilizzare un'interfaccia virtuale di storage diversa per collegare ciascun volume di dati per assicurarsi di utilizzare sessioni TCP diverse per ciascun volume o l'opzione di montaggio nconnect, se disponibile per il sistema operativo in uso.

3. Montare i file system eseguendo `mount -a` comando.

Aggiunta di una partizione aggiuntiva del volume di dati

Eseguire la seguente istruzione SQL sul database tenant per aggiungere una partizione aggiuntiva del volume di dati al database tenant. Utilizza il percorso verso volumi aggiuntivi:

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```



Dove trovare ulteriori informazioni

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

- "Soluzioni software SAP HANA"
- "TR-4646: Disaster recovery SAP HANA con replica dello storage"
- "TR-4614: Backup e ripristino SAP HANA con SnapCenter"
- "TR-4667: Automatizzazione di copie di sistema SAP con il plug-in SAP HANA SnapCenter"

- Centri di documentazione NetApp

  "https://www.netapp.com/support-and-training/documentation/"

- Hardware per lo storage aziendale certificato SAP per SAP HANA

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"

- Requisiti di storage SAP HANA

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"

- SAP HANA - Domande frequenti sull'integrazione personalizzata del data center

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"

- SAP HANA su VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"

- Guida alle Best practice di SAP HANA su VMware vSphere

  "https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

Aggiornare la cronologia

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

Data	Riepilogo degli aggiornamenti
Ottobre 2015	Versione iniziale
Marzo 2016	Dimensionamento della capacità aggiornato Opzioni di montaggio per `/hana/shared`Aggiornato il parametro sysctl
Febbraio 2017	Nuovi sistemi storage e shelf di dischi NetApp nuove funzionalità di ONTAP 9 supporto per le nuove release 40 GbE del sistema operativo (SUSE Linux Enterprise Server 12 SP1 e Red Hat Enterprise Linux 7.2) Nuova release di SAP HANA
Luglio 2017	Aggiornamenti minori
Settembre 2018	Nuovi sistemi di storage NetApp supporto per le nuove release 100 GbE del sistema operativo (SUSE Linux Enterprise Server 12 SP3 e Red Hat Enterprise Linux 7.4) ulteriori modifiche minori SAP HANA 2.0 SPS3
Ottobre 2019	Nuovi sistemi storage NetApp e shelf NVMe nuove release di sistemi operativi (SUSE Linux Enterprise Server 12 SP4, SUSE Linux Enterprise Server 15 e Red Hat Enterprise Linux 7.6) dimensioni del volume MAX Data piccole modifiche
Dicembre 2019	Nuovi sistemi storage NetApp Nuova release del sistema operativo SUSE Linux Enterprise Server 15 SP1
Marzo 2020	Supporto di nconnect per NFSv3 Nuova release del sistema operativo Red Hat Enterprise Linux 8

Data	Riepilogo degli aggiornamenti
Maggio 2020	Supporto per più partizioni di volumi di dati disponibile con SAP HANA 2.0 SPS4
Giugno 2020	Ulteriori informazioni sulle funzionalità opzionali aggiornamenti minori
Dicembre 2020	Supporto di nconnect per NFSv4.1 a partire da ONTAP 9.8 nuove release del sistema operativo nuove versioni di SAP HANA
Febbraio 2021	Nuovi sistemi storage NetApp modifiche alle impostazioni della rete host modifiche minori
Aprile 2021	Aggiunta di informazioni specifiche su VMware vSphere
Settembre 2022	Nuove versioni del sistema operativo
Agosto 2023	Nuovi sistemi di storage (AFF serie C)
Dicembre 2023	Aggiornamento della configurazione dell'host impostazioni nconnect modificate aggiunta di informazioni sulle NFSv4,1 sessioni
Maggio 2024	Nuovi sistemi di storage (AFF serie A)
Settembre 2024	Aggiornamenti minori
Novembre 2024	Nuovi sistemi di storage
Luglio 2025	Aggiornamenti minori

Guida alla configurazione di SAP HANA su sistemi NetApp ASA con FCP

SAP HANA su sistemi NetApp ASA con protocollo Fibre Channel

La famiglia di prodotti NetApp ASA è certificata per l'utilizzo con SAP HANA nei progetti TDI. Questa guida fornisce le best practice per SAP HANA su questa piattaforma.

Marco Schoen, NetApp

Introduzione

Le famiglie di prodotti NetApp ASA A-Series e ASA C-Series sono state certificate per l'uso con SAP HANA nei progetti TDI (tailored data center Integration). Questa guida descrive le best practice per i seguenti modelli certificati:

- ASA A20, ASA A30, ASA A50, ASA A70, ASA A90, ASA A1K
- ASA C30

Per un elenco completo delle soluzioni di storage certificate NetApp per SAP HANA, consulta la "Directory hardware SAP HANA certificata e supportata".

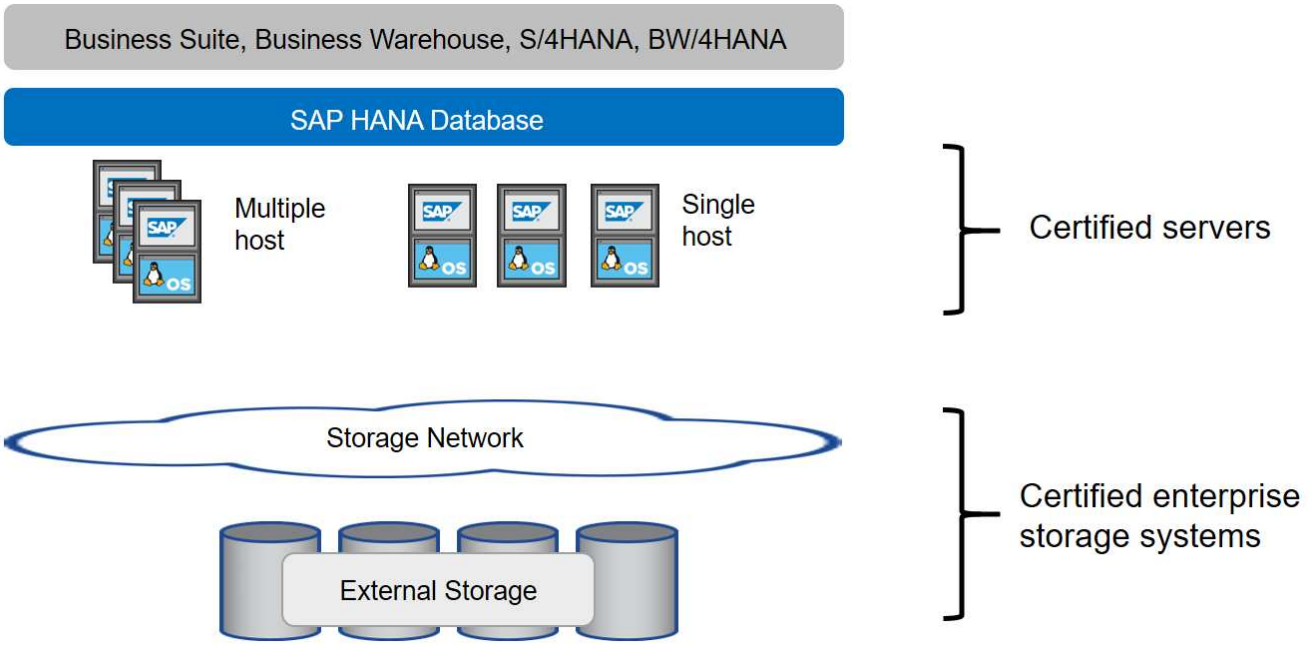
Questo documento descrive le configurazioni ASA che utilizzano il protocollo Fibre Channel (FCP).

La configurazione descritta in questo documento è necessaria per ottenere i KPI SAP HANA richiesti e le migliori performance per SAP HANA. La modifica di impostazioni o l'utilizzo di funzionalità non elencate nel presente documento potrebbe causare un peggioramento delle prestazioni o un comportamento imprevisto e dovrebbe essere eseguita solo se richiesto dal supporto NetApp.

In un ambiente multi-host SAP HANA, il connettore storage standard SAP HANA viene utilizzato per fornire la scherma in caso di failover di un host SAP HANA. Fare sempre riferimento alle note SAP relative alle linee guida per la configurazione del sistema operativo e alle dipendenze specifiche del kernel Linux HANA. Per ulteriori informazioni, vedere "Nota SAP 2235581 – sistemi operativi supportati da SAP HANA".

SAP HANA: Integrazione personalizzata del data center

I sistemi di storage NetApp ASA sono certificati nel programma SAP HANA TDI mediante protocolli FC (SAN). Possono essere implementati in qualsiasi scenario SAP HANA attuale, come SAP Business Suite su HANA, S/4HANA, BW/4HANA o SAP Business Warehouse su HANA, in configurazioni a host singolo o multi-host. Qualsiasi server certificato per l'utilizzo con SAP HANA può essere combinato con soluzioni di storage certificate NetApp. La figura seguente mostra una panoramica dell'architettura.



Per ulteriori informazioni sui prerequisiti e sui consigli per i sistemi SAP HANA produttivi, consulta la seguente risorsa:

- "SAP HANA - Domande frequenti sull'integrazione personalizzata del data center"

SAP HANA con VMware vSphere

Esistono diverse opzioni per connettere lo storage alle macchine virtuali (VM). Sono supportati i mapping dei dispositivi raw (RDM), gli archivi dati FCP o gli archivi dati VVOL con FCP. Per entrambe le opzioni del datastore, è necessario memorizzare un solo volume di log o dati SAP HANA all'interno del datastore per casi di utilizzo produttivi.

Per ulteriori informazioni sull'utilizzo di vSphere con SAP HANA, consultare i seguenti collegamenti:

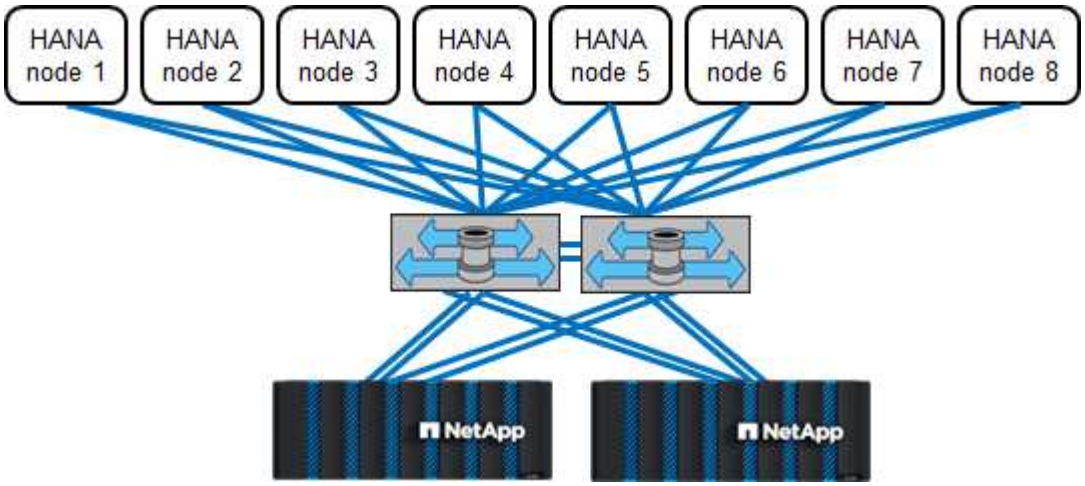
- "SAP HANA su VMware vSphere - virtualizzazione - Wiki della community"
- "Guida alle Best practice di SAP HANA su VMware vSphere"
- "2161991 - linee guida per la configurazione di VMware vSphere - Launchpad di supporto SAP ONE (accesso richiesto)"

Architettura

Gli host SAP HANA sono connessi ai controller di storage utilizzando un'infrastruttura FCP ridondante e un software multipath. È necessaria un'infrastruttura di switch FCP ridondante per fornire connettività host-to-storage SAP HANA fault-tolerant in caso di guasto dello switch o dell'HBA (host bus adapter). È necessario configurare lo zoning appropriato sullo switch per consentire a tutti gli host HANA di raggiungere i LUN richiesti sui controller di storage.

Diversi modelli della famiglia di sistemi ASA possono essere combinati e abbinati a livello di storage per consentire la crescita e le diverse esigenze di performance e capacità. Il numero massimo di host SAP HANA che possono essere collegati al sistema storage è definito dai requisiti di performance SAP HANA e dal modello di controller NetApp utilizzato. Il numero di shelf di dischi richiesti è determinato solo dai requisiti di capacità e performance dei sistemi SAP HANA.

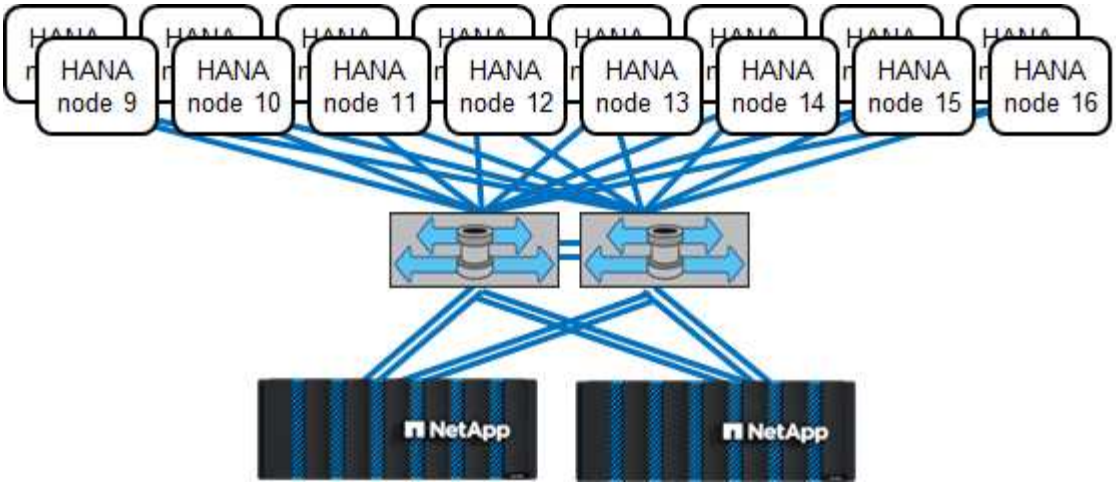
La figura seguente mostra una configurazione di esempio con otto host SAP HANA collegati a una coppia ha di storage.



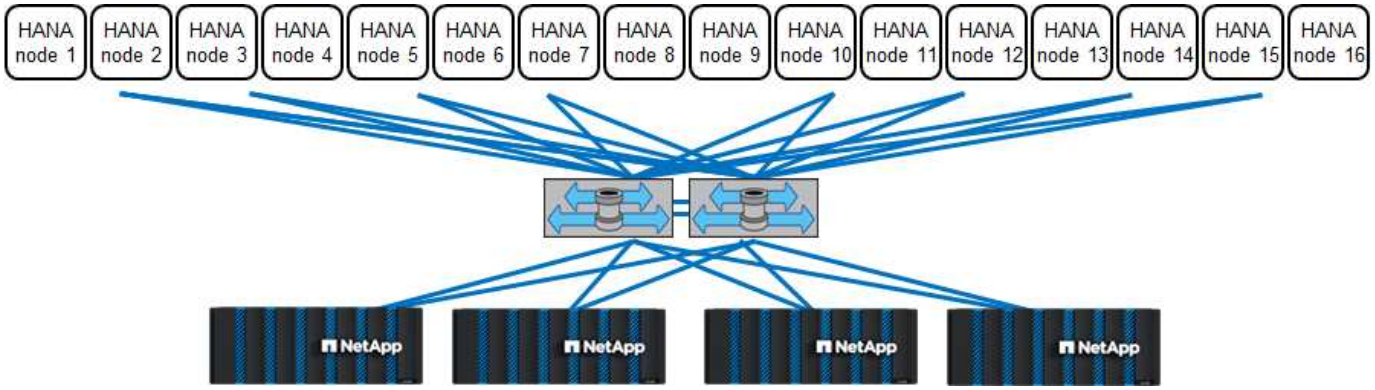
Questa architettura può essere scalata in due dimensioni:

- Collegando ulteriori host SAP HANA e capacità di storage allo storage esistente, se i controller di storage forniscono performance sufficienti per soddisfare gli attuali KPI SAP HANA
- Aggiungendo altri sistemi storage con capacità di storage aggiuntiva per gli host SAP HANA aggiuntivi

La figura seguente mostra un esempio di configurazione in cui più host SAP HANA sono collegati ai controller di storage. In questo esempio, sono necessari più shelf di dischi per soddisfare i requisiti di capacità e performance dei 16 host SAP HANA. A seconda dei requisiti di throughput totale, è necessario aggiungere ulteriori connessioni FC ai controller di storage.



Indipendentemente dal sistema ASA implementato, il panorama SAP HANA può anche essere scalato aggiungendo qualsiasi storage controller certificato per soddisfare la densità di nodo desiderata, come mostrato nella figura seguente.

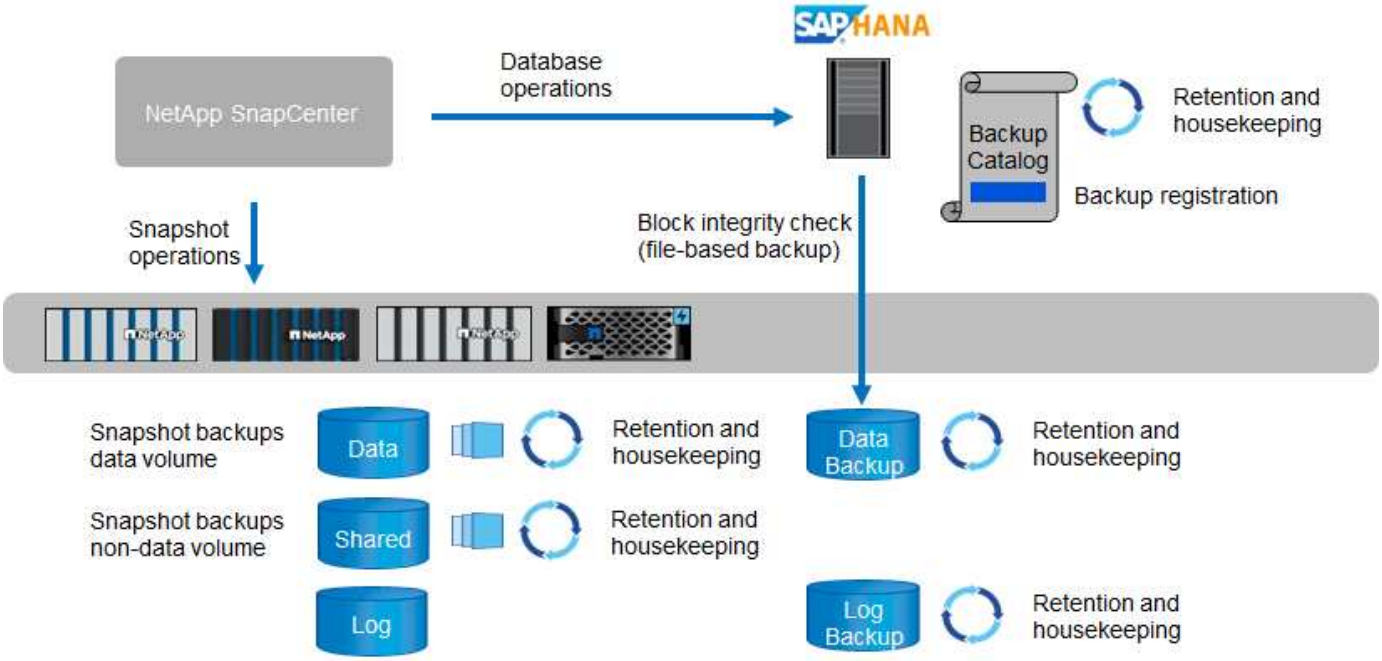


Backup SAP HANA

Il software ONTAP presente su tutti i controller di storage NetApp offre un meccanismo integrato per eseguire il backup dei database SAP HANA durante il funzionamento senza alcun effetto sulle performance. I backup NetApp Snapshot basati su storage sono una soluzione di backup completamente supportata e integrata disponibile per i singoli container SAP HANA e per i sistemi SAP HANA MDC con un singolo tenant o più tenant.

I backup Snapshot basati su storage vengono implementati utilizzando il plug-in NetApp SnapCenter per SAP HANA. Ciò consente agli utenti di creare backup Snapshot coerenti basati sullo storage utilizzando le interfacce fornite in modo nativo dai database SAP HANA. SnapCenter registra tutti i backup Snapshot nel catalogo di backup SAP HANA. Pertanto, i backup eseguiti da SnapCenter sono visibili all'interno di SAP HANA Studio o Cockpit, dove possono essere selezionati direttamente per le operazioni di ripristino e recovery.

La tecnologia NetApp SnapMirror consente di replicare le copie Snapshot create su un sistema storage su un sistema storage di backup secondario controllato da SnapCenter. È quindi possibile definire diversi criteri di conservazione dei backup per ciascuno dei set di backup sullo storage primario e anche per i set di backup sui sistemi di storage secondari. Il plug-in SnapCenter per SAP HANA gestisce automaticamente la conservazione dei backup dei dati basati su copia Snapshot e dei backup dei log, inclusa la manutenzione del catalogo di backup. Il plug-in SnapCenter per SAP HANA consente inoltre di eseguire un controllo dell'integrità del blocco del database SAP HANA eseguendo un backup basato su file.



I backup Snapshot basati su storage offrono vantaggi significativi rispetto ai backup convenzionali basati su file. Questi vantaggi includono, a titolo esemplificativo e non esaustivo, i seguenti:

- Backup più rapido (pochi minuti)
- RTO ridotto grazie a tempi di ripristino molto più rapidi sul layer di storage (pochi minuti) e a backup più frequenti
- Nessuna riduzione delle performance dell'host, della rete o dello storage del database SAP HANA durante le operazioni di backup e recovery
- Replica efficiente in termini di spazio e larghezza di banda sullo storage secondario in base alle modifiche dei blocchi

Per informazioni dettagliate sulla soluzione di backup e ripristino SAP HANA, consultare "Data Protection e high Availability di SAP HANA con SnapCenter, SnapMirror Active Sync e VMware Metro Storage Cluster".

Al momento della creazione di questo documento, SnapCenter per ASA supporta solo le VM basate su VMware che utilizzano VMDK come storage.

Disaster recovery SAP HANA

Il disaster recovery SAP HANA può essere eseguito a livello di database utilizzando la replica di sistema SAP HANA o a livello di storage utilizzando le tecnologie di replica dello storage. La sezione seguente fornisce una panoramica delle soluzioni di disaster recovery basate sulla replica dello storage.

Per informazioni dettagliate sulle soluzioni di disaster recovery SAP HANA, vedere "TR-4646: Disaster recovery SAP HANA con replica dello storage".

Replica dello storage basata su SnapMirror

La figura seguente mostra una soluzione di disaster recovery a tre siti che utilizza la sincronizzazione attiva sincrona di SnapMirror con il data center di disaster recovery locale e la sincronizzazione asincrona di SnapMirror per replicare i dati sul data center di disaster recovery remoto. La sincronizzazione attiva di SnapMirror consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito,

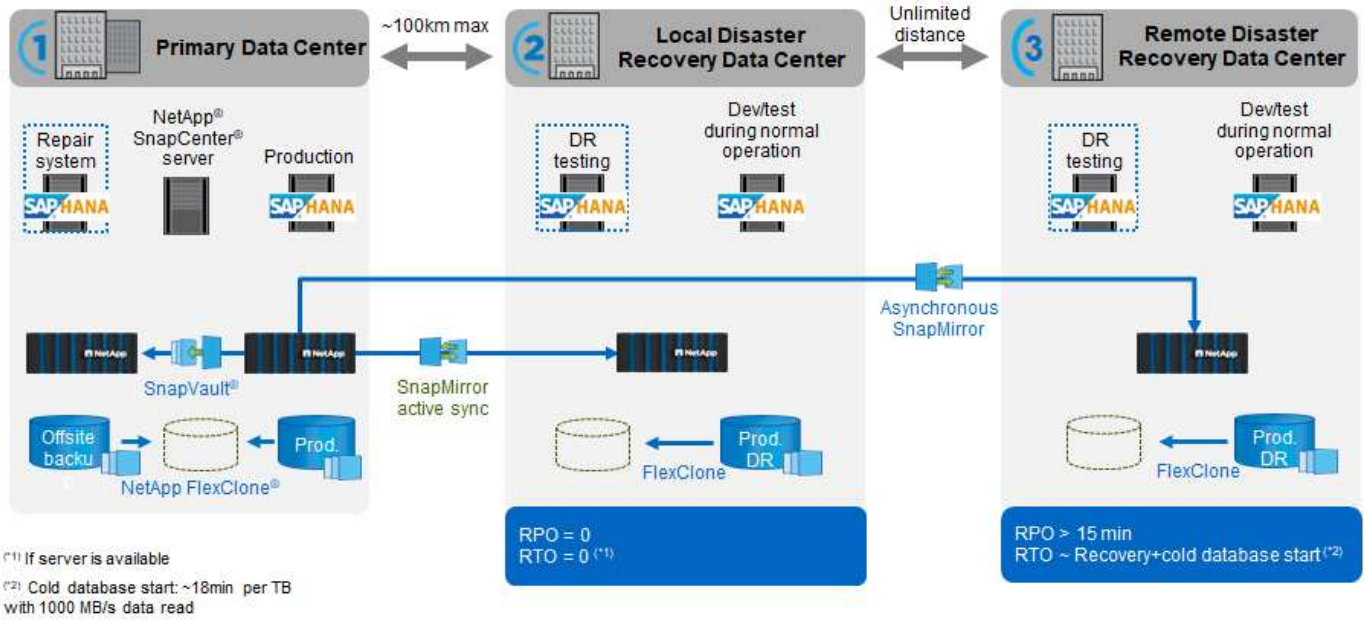
supportando il failover trasparente delle applicazioni utilizzando una copia secondaria (RPO=0 e RTO=0). Non sono richiesti interventi manuali o script personalizzati per attivare un failover con la sincronizzazione attiva di SnapMirror. A partire da ONTAP 9.15.1, la sincronizzazione attiva SnapMirror supporta una funzionalità Active/Active simmetrica. Active/Active simmetrico consente operazioni di i/o in lettura e scrittura da entrambe le copie di una LUN protetta con replica sincrona bidirezionale, in modo che entrambe le copie LUN possano servire le operazioni di i/o a livello locale.

Maggiori dettagli possono essere trovati su "Panoramica della sincronizzazione attiva di SnapMirror in ONTAP" ..

L'RTO per la replica asincrona di SnapMirror dipende principalmente dal tempo necessario per avviare il database HANA nel sito DR e caricare i dati nella memoria. Supponendo che i dati siano letti con un throughput di 1000 Mbps, il caricamento di 1 TB di dati richiederebbe circa 18 minuti.

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

Entrambi i metodi di replica consentono di eseguire test del workflow di DR senza influenzare l'RPO e l'RTO. I volumi FlexClone vengono creati sullo storage e collegati ai server di test del DR.



Dimensionamento dello storage

La sezione seguente fornisce una panoramica delle considerazioni relative a performance e capacità necessarie per il dimensionamento di un sistema storage per SAP HANA.

Contatta il tuo commerciale NetApp o il tuo partner NetApp per supportare il processo di dimensionamento dello storage e per aiutarti a creare un ambiente di storage di dimensioni adeguate.

Considerazioni sulle performance

SAP ha definito un set statico di indicatori di performance chiave dello storage (KPI). Questi KPI sono validi per tutti gli ambienti SAP HANA in produzione, indipendentemente dalle dimensioni della memoria degli host di

database e delle applicazioni che utilizzano il database SAP HANA. Questi KPI sono validi per ambienti a host singolo, host multiplo, Business Suite su HANA, Business Warehouse su HANA, S/4HANA e BW/4HANA. Pertanto, l'attuale approccio al dimensionamento delle performance dipende solo dal numero di host SAP HANA attivi collegati al sistema storage.

> I KPI relativi alle performance dello storage sono richiesti solo per i sistemi SAP HANA in produzione, ma è possibile implementarli in tutti i sistemi HANA.

SAP offre uno strumento di test delle performance che deve essere utilizzato per convalidare le performance dei sistemi storage per gli host SAP HANA attivi collegati allo storage.

NetApp ha testato e predefinito il numero massimo di host SAP HANA che possono essere collegati a un modello di storage specifico, pur continuando a soddisfare i KPI di storage richiesti da SAP per i sistemi SAP HANA basati sulla produzione.

Il numero massimo di host SAP HANA che possono essere eseguiti su uno shelf di dischi e il numero minimo di SSD richiesti per host SAP HANA sono stati determinati eseguendo il tool di test delle performance SAP. Questo test non prende in considerazione i requisiti effettivi di capacità dello storage degli host. È inoltre necessario calcolare i requisiti di capacità per determinare l'effettiva configurazione dello storage necessaria.

Shelf NS224 NVMe

Un SSD NVMe (dati) supporta fino a 2/5 host SAP HANA a seconda del disco NVMe specifico utilizzato.

> L'aggiunta di più shelf di dischi non aumenta il numero massimo di host SAP HANA supportati da uno storage controller.

Carichi di lavoro misti

Sono supportati SAP HANA e altri carichi di lavoro applicativi eseguiti sullo stesso storage controller o nello stesso aggregato di storage. Tuttavia, è una Best practice di NetApp separare i workload SAP HANA da tutti gli altri workload delle applicazioni.

Potresti decidere di implementare workload SAP HANA e altri workload applicativi sullo stesso storage controller o sullo stesso aggregato. In tal caso, è necessario assicurarsi che le performance di SAP HANA siano adeguate all'interno dell'ambiente di workload misto. NetApp consiglia inoltre di utilizzare i parametri della qualità del servizio (QoS) per regolare l'effetto che queste altre applicazioni potrebbero avere sulle applicazioni SAP HANA e per garantire il throughput per le applicazioni SAP HANA.

Il tool di test SAP HCMT deve essere utilizzato per verificare se è possibile eseguire altri host SAP HANA su uno storage controller esistente già in uso per altri carichi di lavoro. I server applicativi SAP possono essere posizionati in modo sicuro sullo stesso storage controller e/o aggregato dei database SAP HANA.

Considerazioni sulla capacità

Una descrizione dettagliata dei requisiti di capacità per SAP HANA è disponibile nella "Nota SAP 1900823" white paper.

> Il dimensionamento della capacità del panorama SAP complessivo con più sistemi SAP HANA deve essere determinato utilizzando gli strumenti di dimensionamento dello storage SAP HANA di NetApp. Contatta NetApp o il tuo partner commerciale NetApp per convalidare il processo di dimensionamento dello storage per un ambiente di storage di dimensioni adeguate.

Configurazione dello strumento di test delle performance

A partire da SAP HANA 1.0 SPS10, SAP ha introdotto i parametri per regolare il comportamento di i/o e ottimizzare il database per il file e il sistema storage utilizzati. Questi parametri devono essere impostati anche per lo strumento di test delle performance di SAP quando le performance dello storage vengono testate con lo strumento di test SAP.

NetApp ha condotto test delle performance per definire i valori ottimali. La seguente tabella elenca i parametri che devono essere impostati nel file di configurazione dello strumento di test SAP.

Parametro	Valore
max_parallel_io_requests	128
async_read_submit	acceso
async_write_submit_active	acceso
async_write_submit_blocks	tutto

Per ulteriori informazioni sulla configurazione dello strumento di test SAP, vedere "Nota SAP 1943937" Per HWCCT (SAP HANA 1.0) e. "Nota SAP 2493172" PER HCMT/HCOT (SAP HANA 2.0).

Nell'esempio seguente viene illustrato come impostare le variabili per il piano di esecuzione HCMT/HCOT.

```
…
{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "DataAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
          "Name": "LogAsyncWriteSubmitActive",
          "Value": "on",
          "Request": "false"
       },
       {
          "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
          "Name": "DataAsyncWriteSubmitActive",
```

```
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

Queste variabili devono essere utilizzate per la configurazione del test. Questo è solitamente il caso dei piani di esecuzione predefiniti che SAP offre con lo strumento HCMT/HCOT. Il seguente esempio per un test di scrittura del log 4k è da un piano di esecuzione.

```
…
      {
         "ID": "D664D001-933D-41DE-A904F304AEB67906",
         "Note": "File System Write Test",
         "ExecutionVariants": [
            {
               "ScaleOut": {
                  "Port": "${RemotePort}",
                  "Hosts": "${Hosts}",
                  "ConcurrentExecution": "${FSConcurrentExecution}"
               },
               "RepeatCount": "${TestRepeatCount}",
               "Description": "4K Block, Log Volume 5GB, Overwrite",
               "Hint": "Log",
               "InputVector": {
                  "BlockSize": 4096,
                  "DirectoryName": "${LogVolume}",
                  "FileOverwrite": true,
                  "FileSize": 5368709120,
                  "RandomAccess": false,
                  "RandomData": true,
                  "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                  "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                  "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                  "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                  "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                  "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                  "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                  "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                  "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
               }
            },
…
```

Panoramica del processo di dimensionamento dello storage

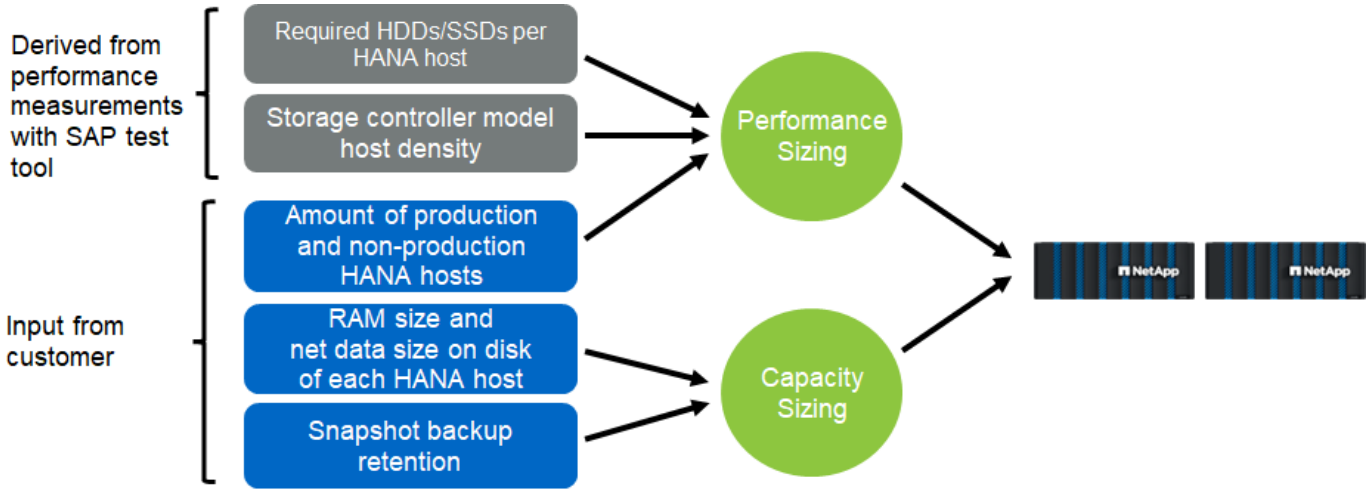
Il numero di dischi per host HANA e la densità host SAP HANA per ciascun modello di storage sono stati determinati utilizzando il tool di test SAP HANA.

Il processo di dimensionamento richiede dettagli come il numero di host SAP HANA in produzione e non in produzione, la dimensione della RAM di ciascun host e la conservazione del backup delle copie Snapshot basate sullo storage. Il numero di host SAP HANA determina il controller dello storage e il numero di dischi

necessari.

La dimensione della RAM, la dimensione dei dati netti sul disco di ciascun host SAP HANA e il periodo di conservazione del backup della copia Snapshot vengono utilizzati come input durante il dimensionamento della capacità.

La figura seguente riassume il processo di dimensionamento.



Installazione e configurazione dell'infrastruttura

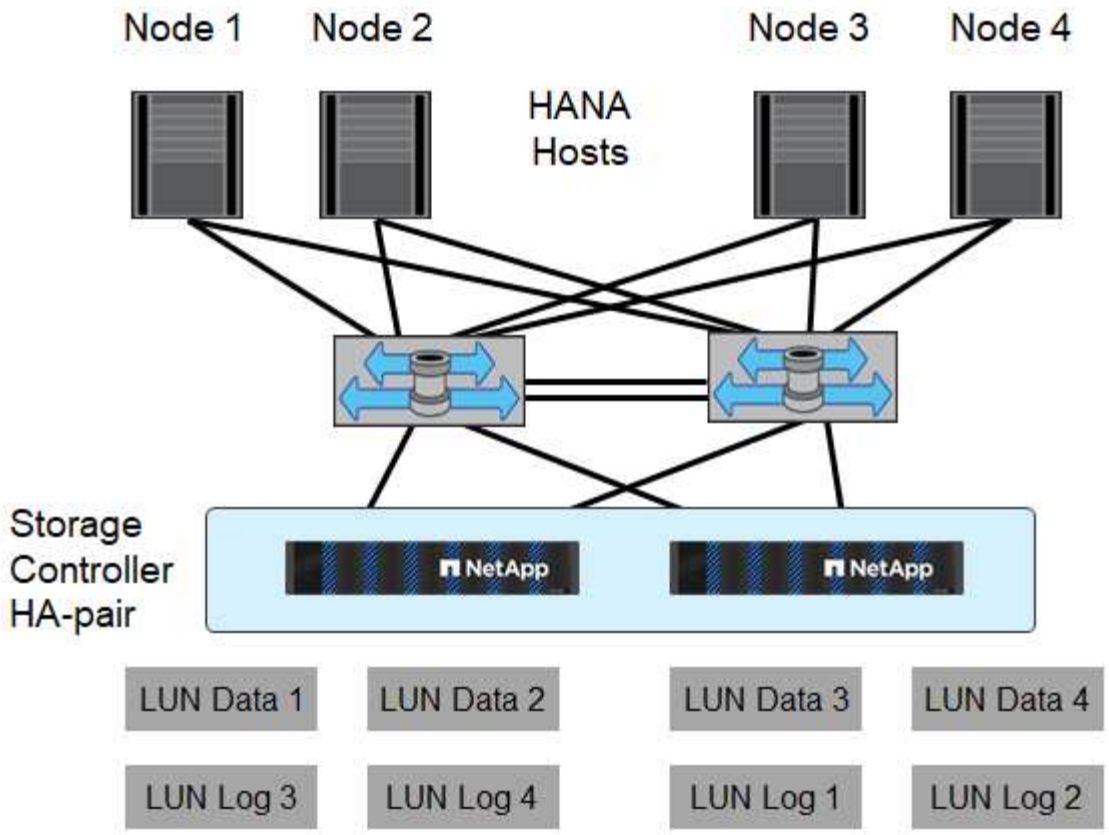
Le seguenti sezioni forniscono le linee guida per la configurazione e la configurazione dell'infrastruttura SAP HANA e descrivono tutti i passaggi necessari per configurare un sistema SAP HANA. All'interno di queste sezioni, vengono utilizzate le seguenti configurazioni di esempio:

- Sistema HANA con SID=FC5
  - SAP HANA host singolo e multiplo

Configurazione del fabric SAN

Ogni server SAP HANA deve disporre di una connessione SAN FCP ridondante con una larghezza di banda minima di 8 Gbps. Per ogni host SAP HANA collegato a un controller di storage, è necessario configurare una larghezza di banda di almeno 8 Gbps nel controller di storage.

La figura seguente mostra un esempio con quattro host SAP HANA collegati a due storage controller. Ciascun host SAP HANA dispone di due porte FCP collegate al fabric ridondante. A livello di storage, quattro porte FCP sono configurate per fornire il throughput richiesto per ciascun host SAP HANA.



Oltre alla suddivisione in zone sul layer dello switch, è necessario mappare ogni LUN del sistema di storage agli host che si connettono a questo LUN. Mantenere lo zoning sullo switch semplice, ovvero definire un set di zone in cui tutti gli HBA host possano vedere tutti gli HBA dei controller.

Sincronizzazione dell'ora

È necessario sincronizzare l'ora tra i controller di storage e gli host del database SAP HANA. A tale scopo, impostare lo stesso server di riferimento orario per tutti i controller di storage e tutti gli host SAP HANA.

Configurazione dello storage controller

Questa sezione descrive la configurazione del sistema storage NetApp. È necessario completare l'installazione e la configurazione primaria in base alle corrispondenti guide di configurazione e configurazione di Data ONTAP.

Efficienza dello storage

La deduplica inline, la deduplica inline di più volumi, la compressione inline e la compaction inline sono supportate con SAP HANA in una configurazione SSD.

Qualità del servizio

La qualità del servizio può essere utilizzata per limitare il throughput dello storage per sistemi SAP HANA o applicazioni non SAP specifici su un controller condiviso.

Produzione e sviluppo/test

Un caso d'utilizzo sarebbe quello di limitare il throughput dei sistemi di sviluppo e test in modo che non possano influenzare i sistemi di produzione in una configurazione mista. Durante il processo di dimensionamento, è necessario determinare i requisiti di performance di un sistema non in produzione. I sistemi di sviluppo e test possono essere dimensionati con valori di performance inferiori, in genere nell'intervallo compreso tra il 20% e il 50% di un KPI del sistema di produzione come definito da SAP. L'i/o di scrittura di grandi dimensioni ha il maggiore effetto sulle performance del sistema storage. Pertanto, il limite di throughput QoS deve essere impostato su una percentuale dei corrispondenti valori KPI di scrittura delle performance dello storage SAP HANA nei volumi di dati e di log.

Ambienti condivisi

Un altro caso d'utilizzo consiste nel limitare il throughput dei carichi di lavoro intensivi in scrittura, soprattutto per evitare che questi carichi di lavoro abbiano un impatto su altri carichi di lavoro in scrittura sensibili alla latenza. In tali ambienti è consigliabile applicare una policy di gruppo QoS con un livello di throughput massimo non condiviso a ogni LUN all'interno di ciascuna Storage Virtual Machine (SVM) per limitare il throughput massimo di ciascun oggetto storage singolo a un valore dato. Questo riduce la possibilità che un singolo carico di lavoro possa influenzare negativamente altri carichi di lavoro.

Per fare questo, è necessario creare una policy di gruppo utilizzando l'interfaccia a riga di comando del cluster ONTAP per ogni SVM:

```
qos policy-group create -policy-group <policy-name> -vserver <vserver
name> -max-throughput 1000MB/s -is-shared false
```

E applicata a ogni LUN all'interno della SVM. Segue un esempio di applicazione del gruppo di policy a tutte le LUN esistenti all'interno di una SVM:

```
lun modify -vserver <vserver name>  -path * -qos-policy-group  <policy-
name>
```

Tutto questo è necessario per ogni SVM. Il nome del gruppo di polizia della QoS per ciascuna SVM deve essere diverso. Per i nuovi LUN, la policy può essere applicata direttamente:

```
lun create -vserver <vserver_name> -path  /vol/<volume_name>/<lun_name>
-size <size> -ostype <e.g. linux>  -qos-policy-group <policy-name>
```

Si consiglia di utilizzare 1000 MB/s come velocità massima per una determinata LUN. Se un'applicazione richiede una maggiore capacità di elaborazione, è necessario utilizzare più LUN con striping LUN per fornire la larghezza di banda necessaria. Questa guida fornisce un esempio per SAP HANA basato su Linux LVM nella sezione"Host Setup (impostazione host)" .

> Il limite si applica anche alle letture. Pertanto, utilizza un numero sufficiente di LUN per soddisfare gli SLA richiesti per l'avvio del database SAP HANA e per i backup.

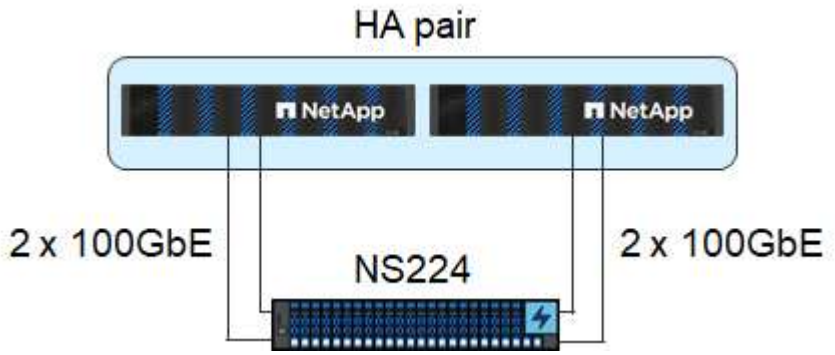
Configurare lo storage

La seguente panoramica riassume i passaggi necessari per la configurazione dello storage. Ogni fase viene descritta in maggiore dettaglio nelle sezioni successive. In questa sezione, si presuppone che l'hardware di storage sia configurato e che il software ONTAP sia già installato. Inoltre, la connessione delle porte FCP dello storage al fabric SAN deve essere già attiva.

1. Verificare la corretta configurazione degli shelf di dischi, come descritto in Shelf dei dischi basati su NVMe.
2. Creare gruppi di iniziatori (igroup) con nomi mondiali (WWN) dei server HANA come descritto nella sezione xref:./bp/saphana-asa-fc-storage-controller-setup.html#initiator-groups Gruppi di iniziatori .
3. Crea LUN e mappali sui server descritti nella sezione "Configurazione LUN per sistemi SAP HANA a host singolo" E "Configurazione LUN per sistemi multi-host SAP HANA"

Shelf dei dischi basati su NVMe

Ogni shelf di dischi NS224 NVMe è collegato a due porte 100GbE per controller, come illustrato nella figura seguente. I dischi vengono distribuiti automaticamente a entrambi i controller della coppia HA.



Gruppi di iniziatori

È possibile configurare un igroup per ciascun server o per un gruppo di server che richiedono l'accesso a un LUN. La configurazione di igroup richiede i nomi delle porte mondiali (WWPN) dei server.

Utilizzando il `sanlun` Eseguire il seguente comando per ottenere le WWPN di ciascun host SAP HANA:

```
sapcc-hana-tst:~ # sanlun fcp show adapter
/sbin/udevadm
/sbin/udevadm

host0 ..... WWPN:2100000e1e163700
host1 ..... WWPN:2100000e1e163701
```

`sanlun`Lo strumento fa parte delle utilità host NetApp e deve essere installato su ogni host SAP HANA. Ulteriori dettagli sono disponibili nella sezione "Configurazione dell'host."

Host singolo

Host singolo

Questa sezione descrive la configurazione del sistema di archiviazione NetApp specifico per i sistemi SAP HANA a host singolo

Creazione di LUN e mappatura delle LUN ai gruppi di iniziatori

È possibile utilizzare NetApp ONTAP System Manager per creare volumi di storage e LUN e mapparli agli igroup dei server e alla CLI ONTAP .

Creazione di LUN e mappatura delle LUN ai gruppi di iniziatori tramite la CLI

Questa sezione mostra un esempio di configurazione mediante la riga di comando con ONTAP 9 per un sistema host singolo SAP HANA con SID FC5 mediante LVM e due LUN per gruppo di volumi LVM:

1. Creare tutte le LUN.

```
lun create -path  FC5_data_mnt00001_1 -size 1t -ostype linux  -class
regular
lun create -path FC5_data_mnt00001_2 -size 1t -ostype linux  -class
regular
lun create -path FC5_log_mnt00001_1 -size 260g -ostype linux  -class
regular
lun create -path FC5_log_mnt00001_2 -size 260g -ostype linux  -class
regular
lun create -path FC5_shared -size 260g -ostype linux  -class regular
```

2. Creare il gruppo iniziatore per tutti i server appartenenti al sistema FC5.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb -vserver svm1
```

3. Mappare tutti i LUN al gruppo iniziatore creato.

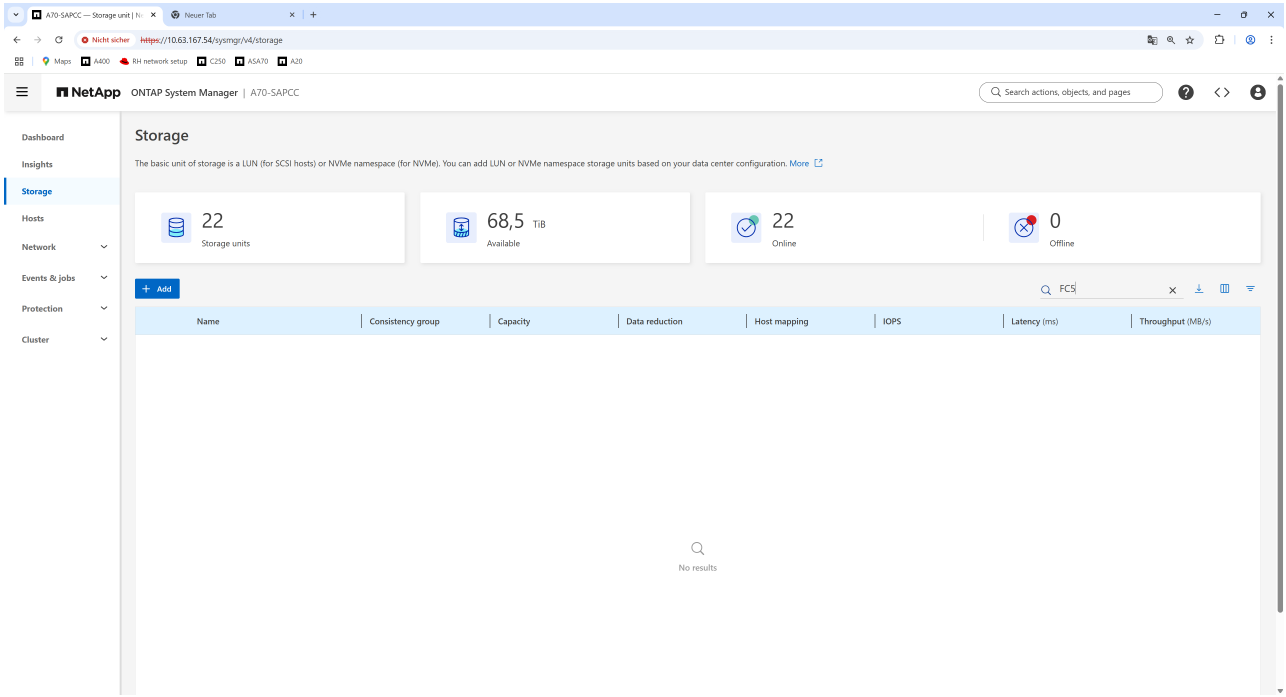
```
lun map -path FC5_data_mnt00001_1 -igroup HANA-FC5
lun map -path FC5_data_mnt00001_2 -igroup HANA-FC5
lun map -path FC5_log_mnt00001_1 -igroup HANA-FC5
lun map -path FC5_log_mnt00001_2 -igroup HANA-FC5
lun map -path FC5_shared -igroup HANA-FC5
```

Creazione di LUN e mappatura di LUN su gruppi di iniziatori tramite GUI

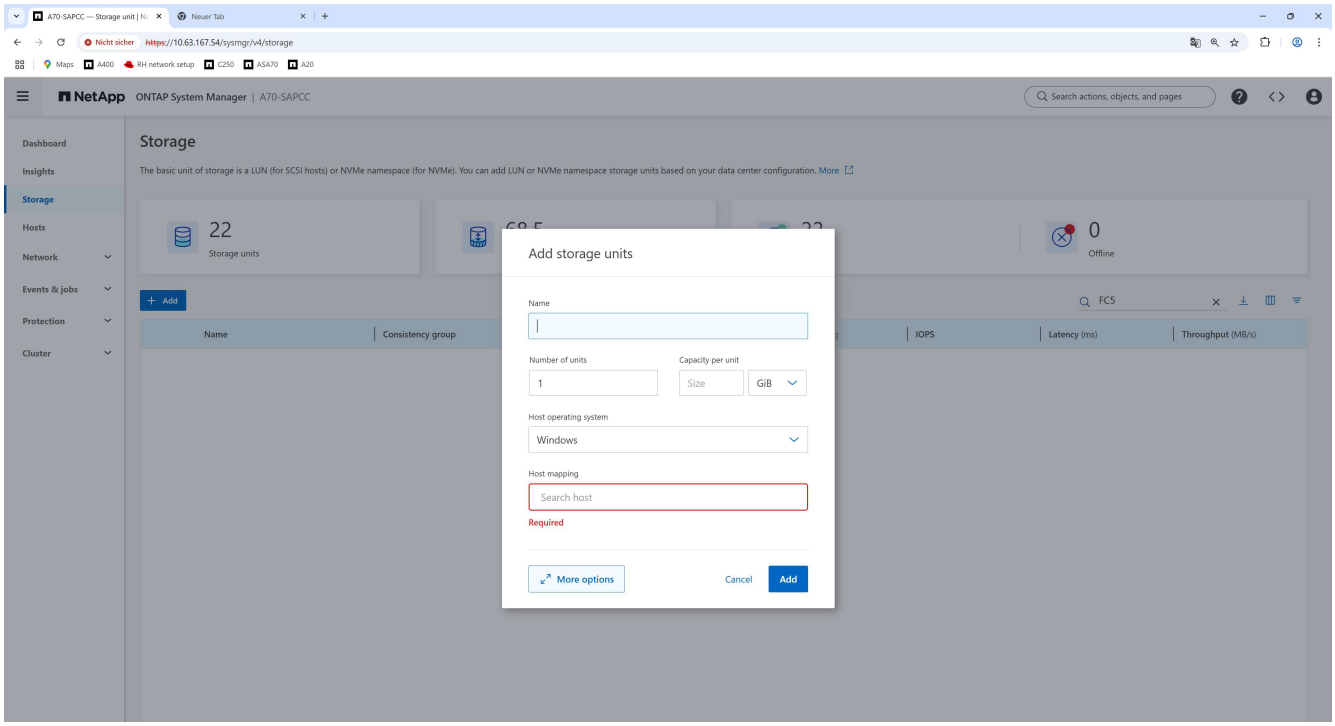
Questa sezione mostra un esempio di configurazione utilizzando `ONTAP System Manager` per un sistema host singolo SAP HANA con SID FC5 che utilizza LVM e due LUN per gruppo di volumi LVM:

1. Accedi al `ONTAP System Manager` del tuo cluster ONTAP e scegli `Storage` dal menu a sinistra.

a. Premere `Add`



2. Scegliere `More options`



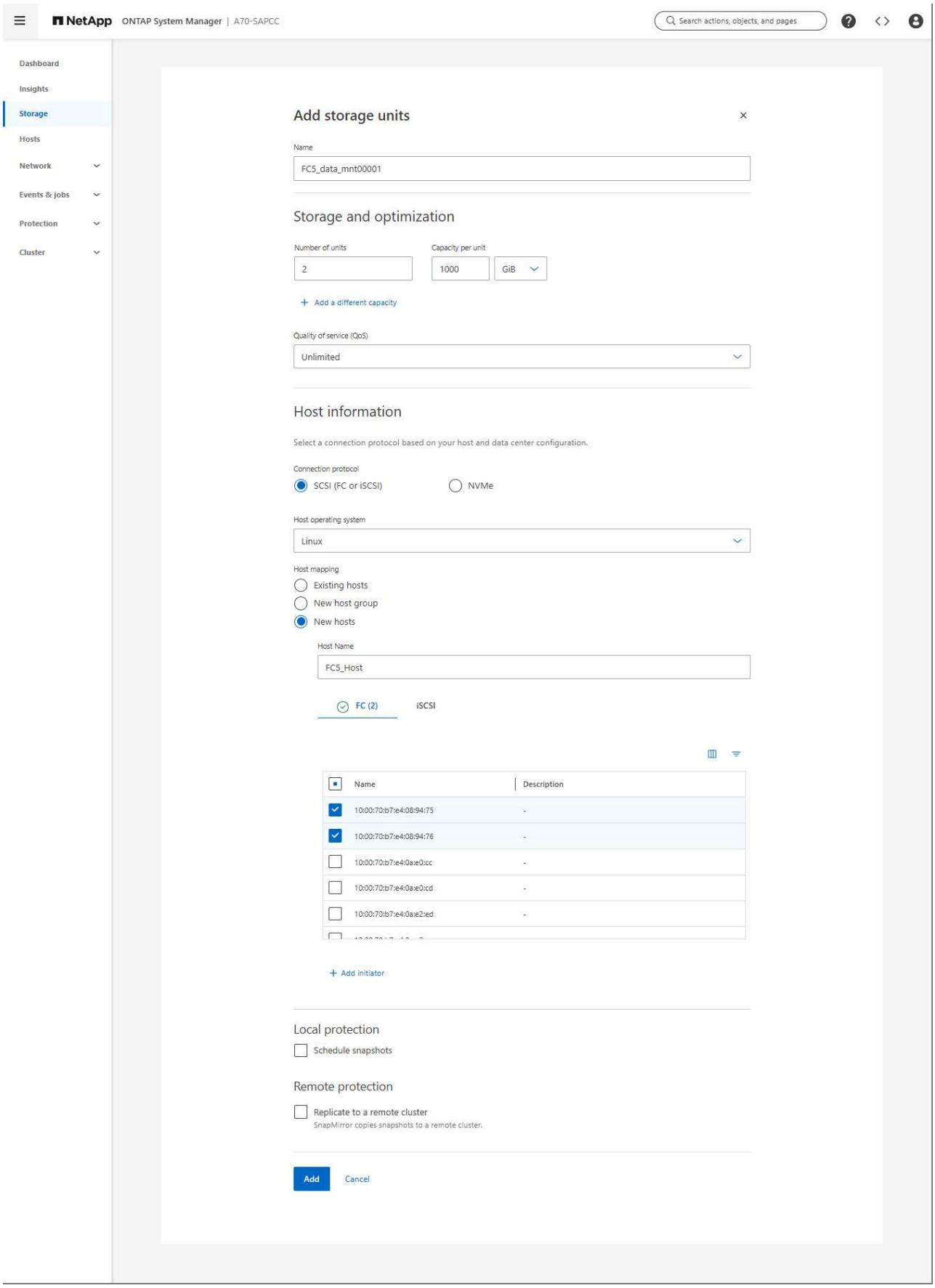
3. Fornire le informazioni richieste:
   a. il nome dei LUN dei dati, ad esempio.`FC5_data_mnt00001`
   b. la quantità di LUN da combinare con LVM, ad esempio 2
   c. la dimensione di ogni LUN, ad esempio 1000 GB
   d. scegliere `SCSI (FC or iSCSI)`

e. scegliere `Linux` COME `Host Operating system`

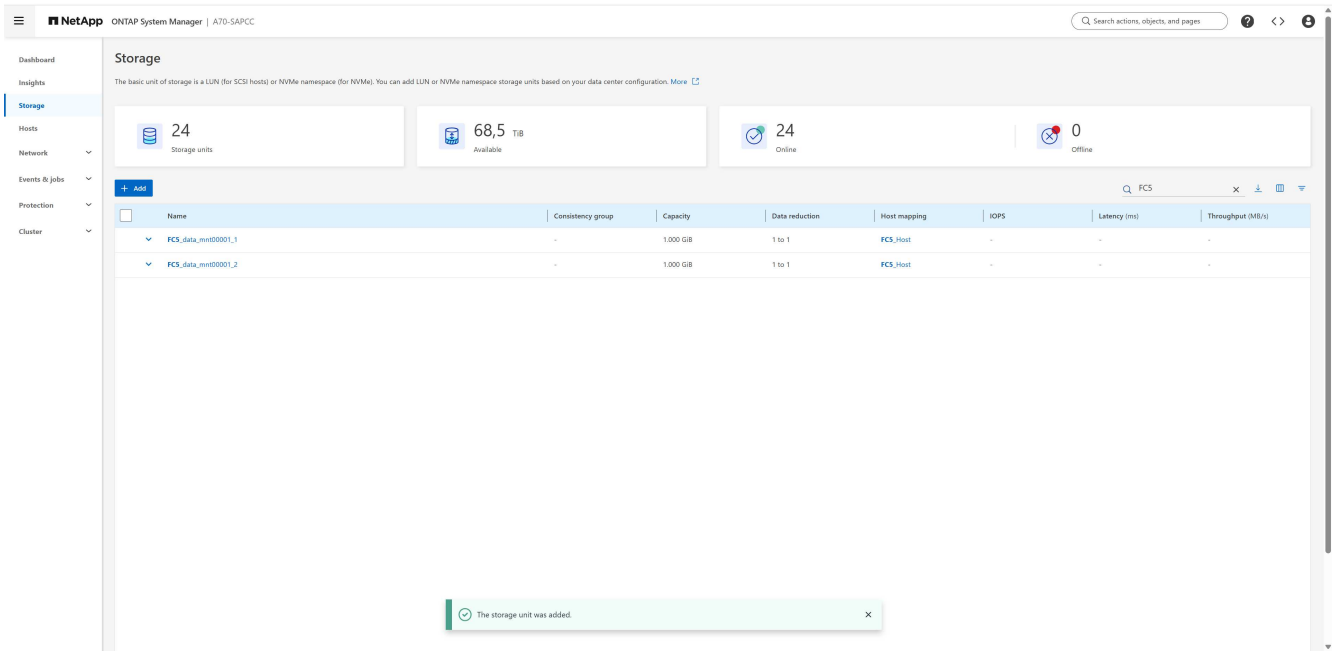
f. scegliere `New host` per il `Host mapping` opzione, fornire un nome, ad esempio `FC5_host` , seleziona o aggiungi gli iniziatori desiderati

g. Mantenere `Schedule snapshots` non selezionato

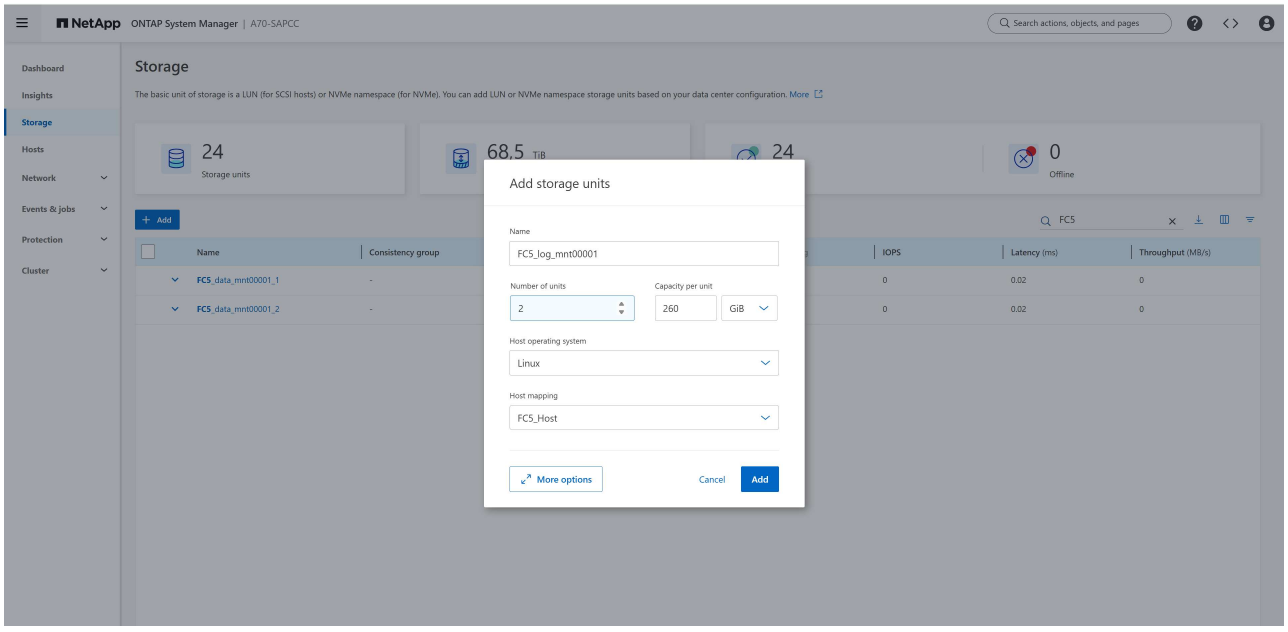
h. premere `Add`



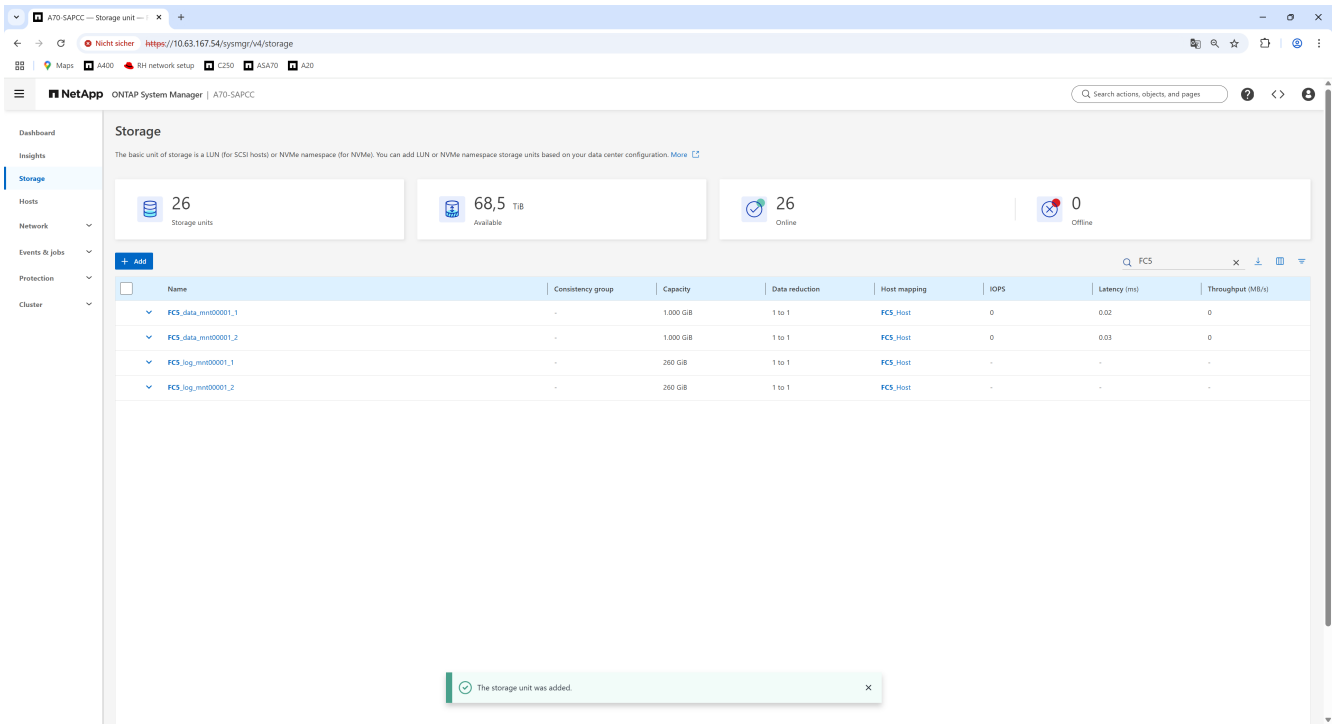
4. Dopo aver creato correttamente i LUN dei dati, creare i LUN del registro premendo `Add`



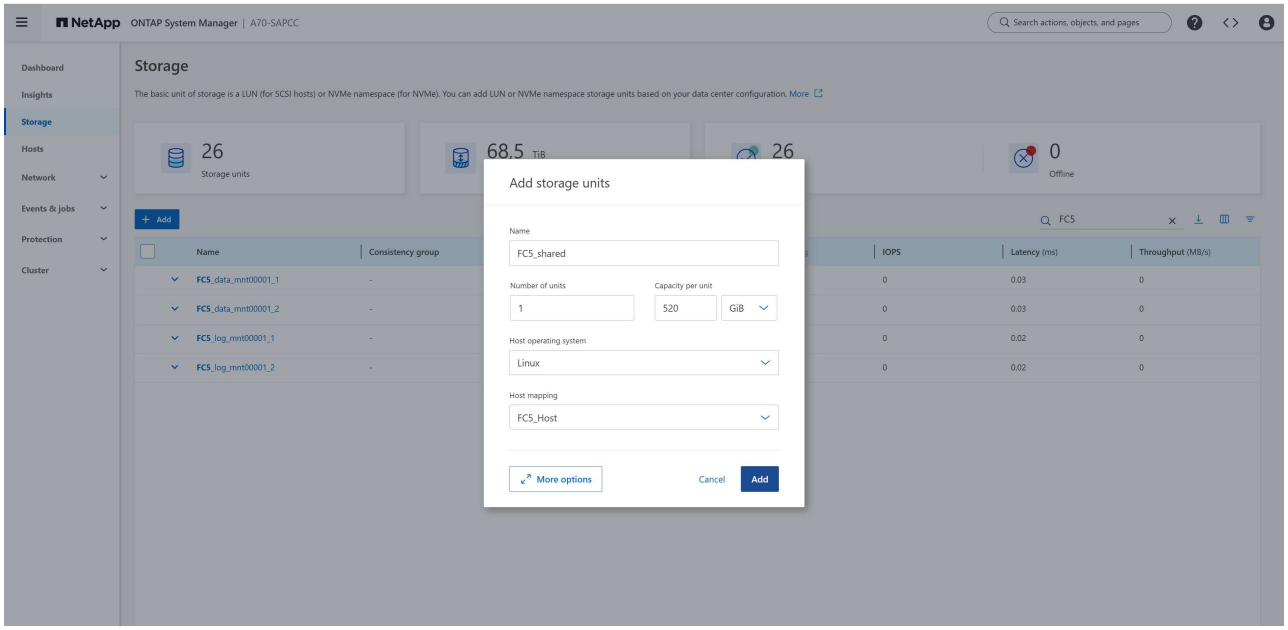
5. Fornire le informazioni richieste:
   a. il nome dei LUN di registro, ad esempio `FC5_log_mnt00001`
   b. la quantità di LUN da combinare con LVM, ad esempio 2
   c. la dimensione di ogni LUN, ad esempio 260 GB
   d. scegliere `Linux` COME `Host Operating system`
   e. scegli la mappatura creata in precedenza `FC5_host` per il `Host mapping` opzione
   f. premere `Add`



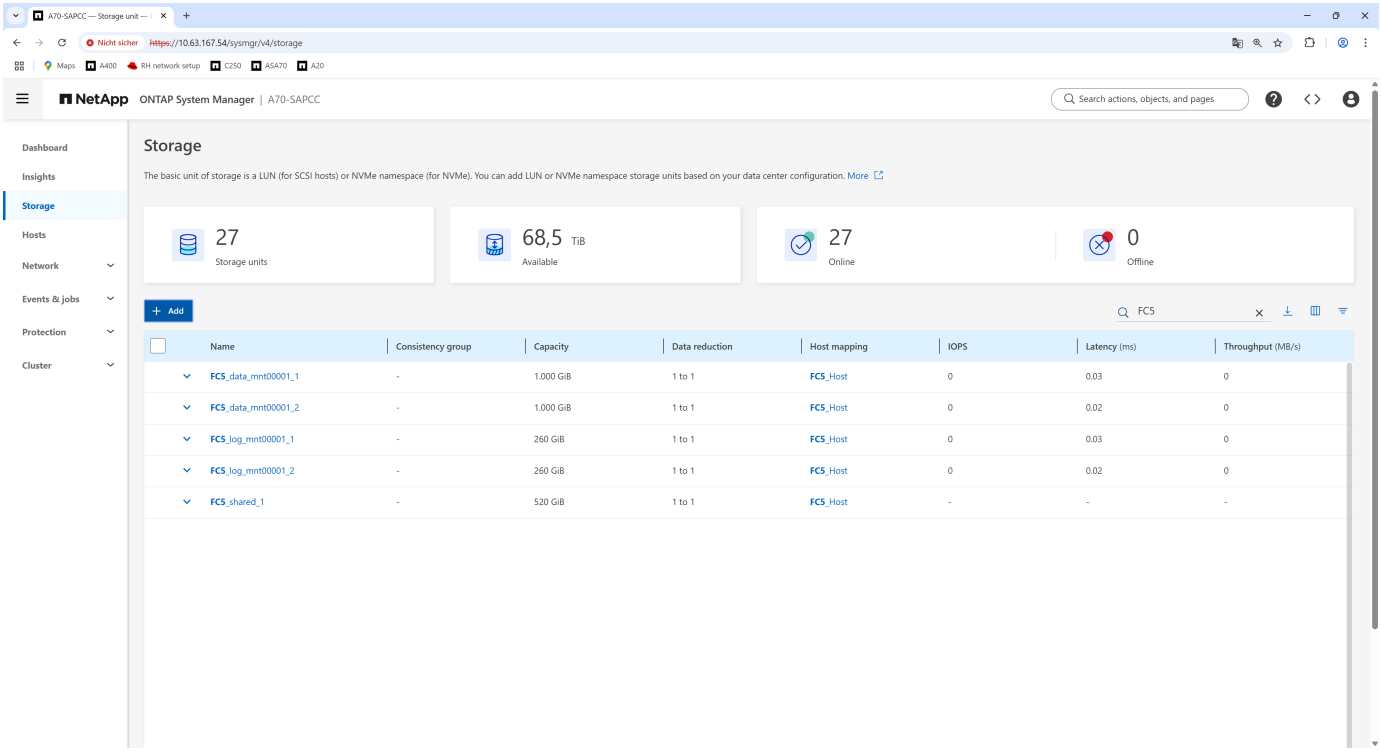
6. Dopo aver creato correttamente i LUN di registro, creare il LUN condiviso premendo `Add`



7. Fornire le informazioni richieste:
   a. il nome del LUN condiviso, ad esempio.`FC5_shared`
   b. la quantità di LUN, ad esempio 1
   c. la dimensione del LUN, ad esempio 520 GB
   d. scegliere `Linux` COME `Host Operating system`
   e. scegli la mappatura creata in precedenza `FC5_host` per il `Host mapping` opzione
   f. premere `Add`



Sono stati creati tutti i LUN necessari per un sistema SAP HANA a host singolo.



Più host

Più host

Questa sezione descrive la configurazione del sistema di archiviazione NetApp specifico per i sistemi multi-host SAP HANA

Creazione di LUN e mappatura delle LUN ai gruppi di iniziatori

È possibile utilizzare NetApp ONTAP System Manager per creare volumi di storage e LUN e mapparli agli igroup dei server e alla CLI ONTAP .

Creazione di LUN e mappatura delle LUN ai gruppi di iniziatori tramite la CLI

Questa sezione mostra un esempio di configurazione utilizzando la riga di comando con ONTAP 9 per un sistema host 2+1 SAP HANA con SID FC5 utilizzando LVM e due LUN per gruppo di volumi LVM:

1. Creare tutte le LUN.

```
lun create -path FC5_data_mnt00001_1 -size 1t -ostype linux  -class
regular
lun create -path FC5_data_mnt00001_2 -size 1t -ostype linux  -class
regular
lun create -path FC5_data_mnt00002_1 -size 1t -ostype linux  -class
regular
lun create -path FC5_data_mnt00002_2 -size 1t -ostype linux  -class
regular
lun create -path FC5_log_mnt00001_1 -size 260g -ostype linux  -class
regular
lun create -path FC5_log_mnt00001_2 -size 260g -ostype linux  -class
regular
lun create -path FC5_log_mnt00002_1 -size 260g -ostype linux  -class
regular
lun create -path FC5_log_mnt00002_2 -size 260g -ostype linux  -class
regular
```

2. Creare il gruppo iniziatore per tutti i server appartenenti al sistema FC5.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator
10000090fadcc5fa,10000090fadcc5fb,10000090fadcc5c1,10000090fadcc5c2,1000
0090fadcc5c3,10000090fadcc5c4 -vserver svm1
```

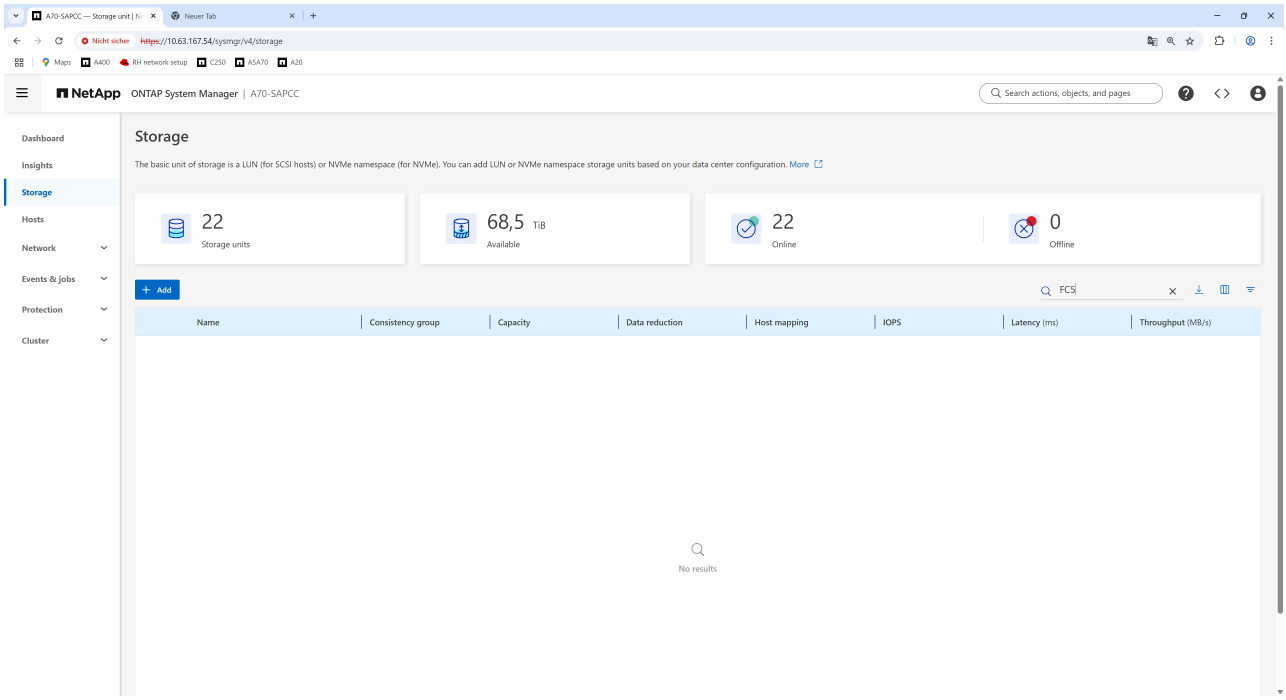
3. Mappare tutti i LUN al gruppo iniziatore creato.

```
lun map -path FC5_data_mnt00001_1 -igroup HANA-FC5
lun map -path FC5_data_mnt00001_2 -igroup HANA-FC5
lun map -path FC5_data_mnt00002_1 -igroup HANA-FC5
lun map -path FC5_data_mnt00002_2 -igroup HANA-FC5
lun map -path FC5_log_mnt00001_1 -igroup HANA-FC5
lun map -path FC5_log_mnt00001_2 -igroup HANA-FC5
lun map -path FC5_log_mnt00002_1 -igroup HANA-FC5
lun map -path FC5_log_mnt00002_2 -igroup HANA-FC5
```

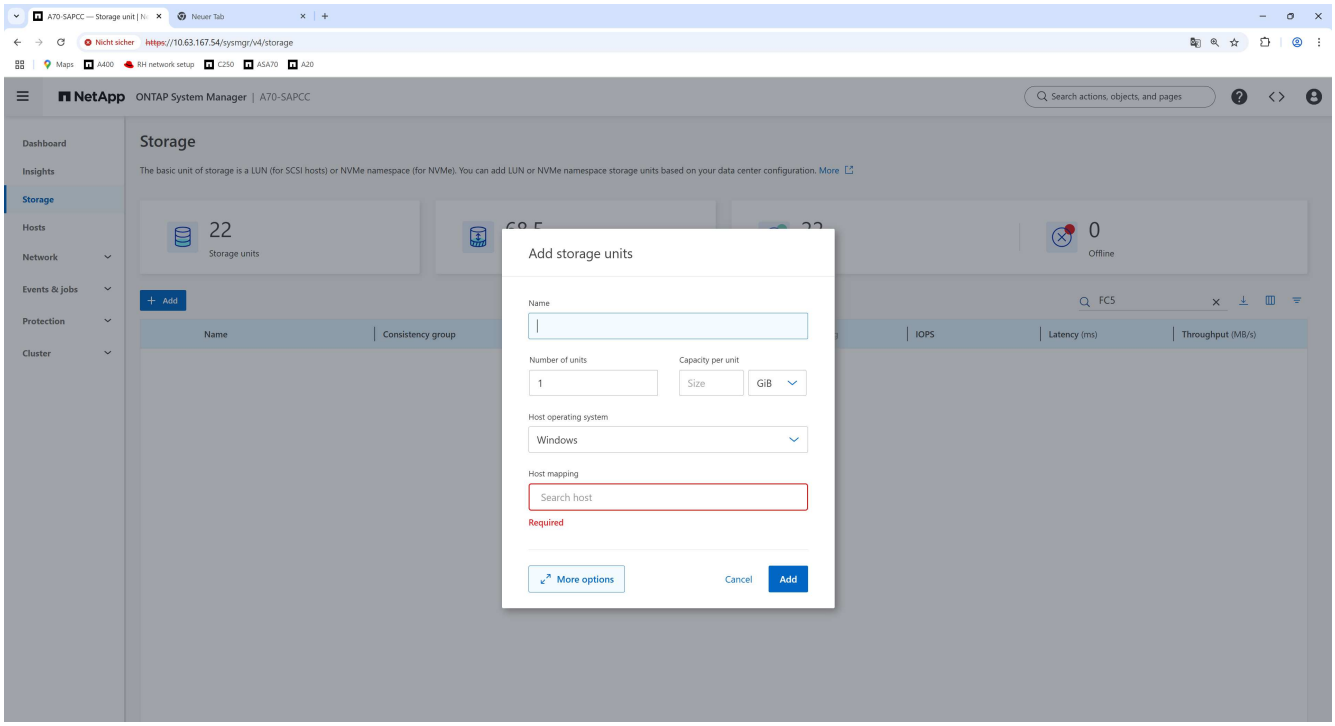
Creazione di LUN e mappatura di LUN su gruppi di iniziatori tramite GUI

Questa sezione mostra un esempio di configurazione utilizzando `ONTAP System Manager` per un sistema host multiplo SAP HANA 2+1 con SID FC5 che utilizza LVM e due LUN per gruppo di volumi LVM:

1. Accedi al `ONTAP System Manager` del tuo cluster ONTAP e scegli `Storage` dal menu a sinistra.
   a. Premere `Add`



2. Scegliere `More options`

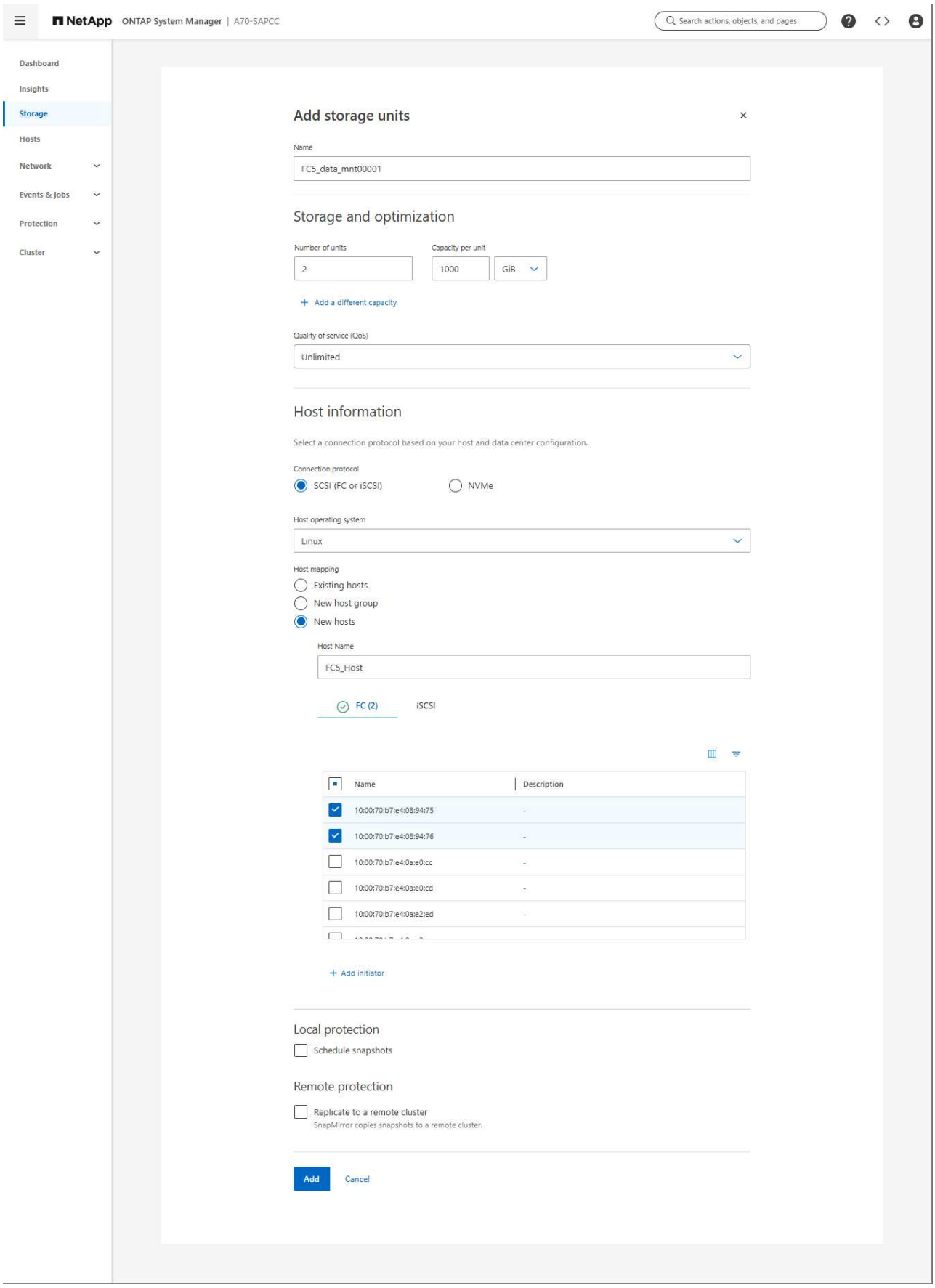


3. Fornire le informazioni richieste:
   a. nome dei LUN dei dati, ad esempio.`FC5_data_mnt00001`
   b. la quantità di LUN da combinare con LVM, ad esempio 2
   c. la dimensione di ogni LUN, ad esempio 1000 GB
   d. scegliere `SCSI (FC or iSCSI)`
   e. scegliere `Linux` COME `Host Operating system`

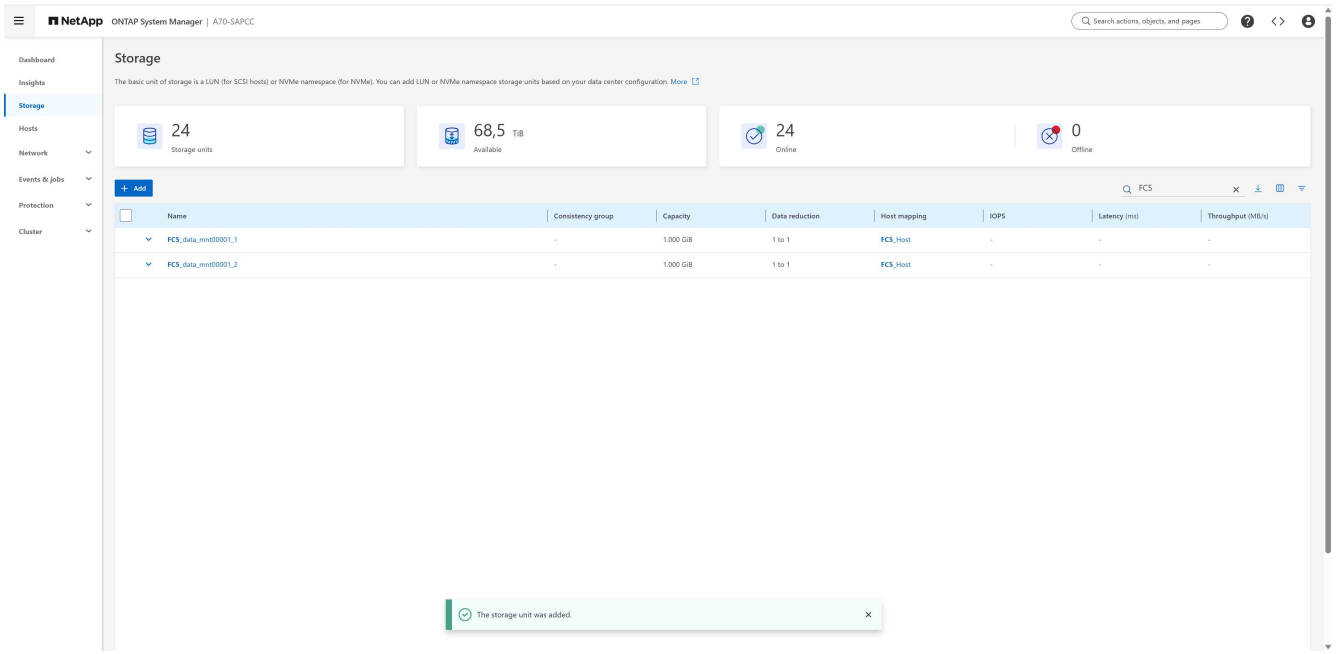
f. scegliere `New host` per il `Host mapping` opzione, fornire un nome, ad esempio `FC5_host` , seleziona o aggiungi gli iniziatori desiderati

g. Mantenere `Schedule snapshots` non selezionato

h. premere `Add`



4. Creare i LUN dati per il prossimo host worker premendo `Add`



5. Fornire le informazioni richieste:

   a. il nome dei LUN di dati aggiuntivi, ad esempio `FC5_data_mnt00002`

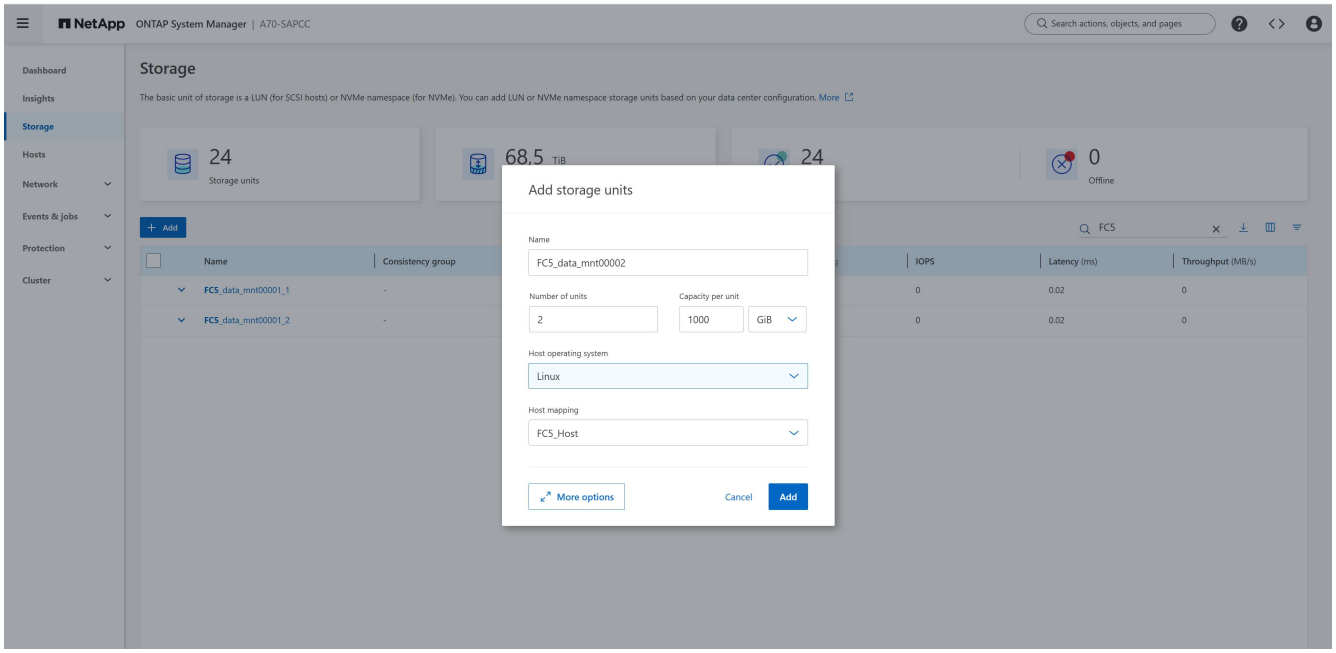
   b. la quantità di LUN da combinare con LVM, ad esempio 2

   c. la dimensione di ogni LUN, ad esempio 1000 GB

   d. scegliere `Linux` COME `Host Operating system`

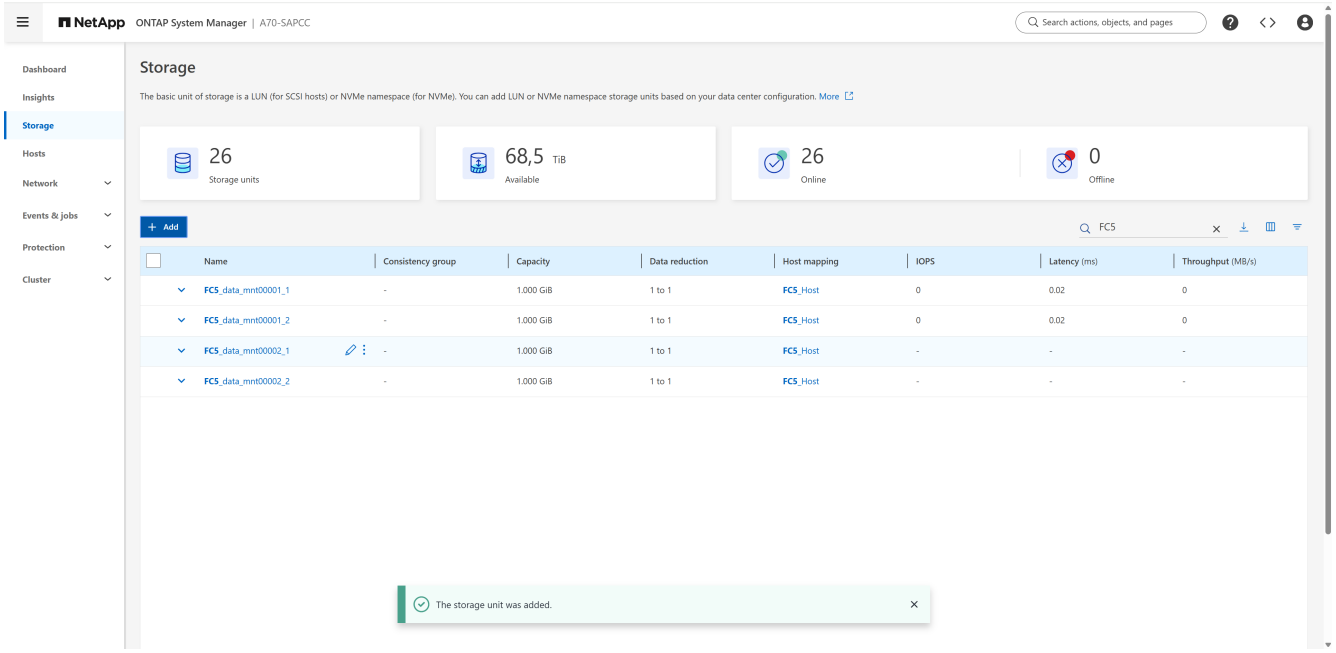
   e. scegli la mappatura creata in precedenza `FC5_host` per il `Host mapping` opzione

   f. premere `Add`

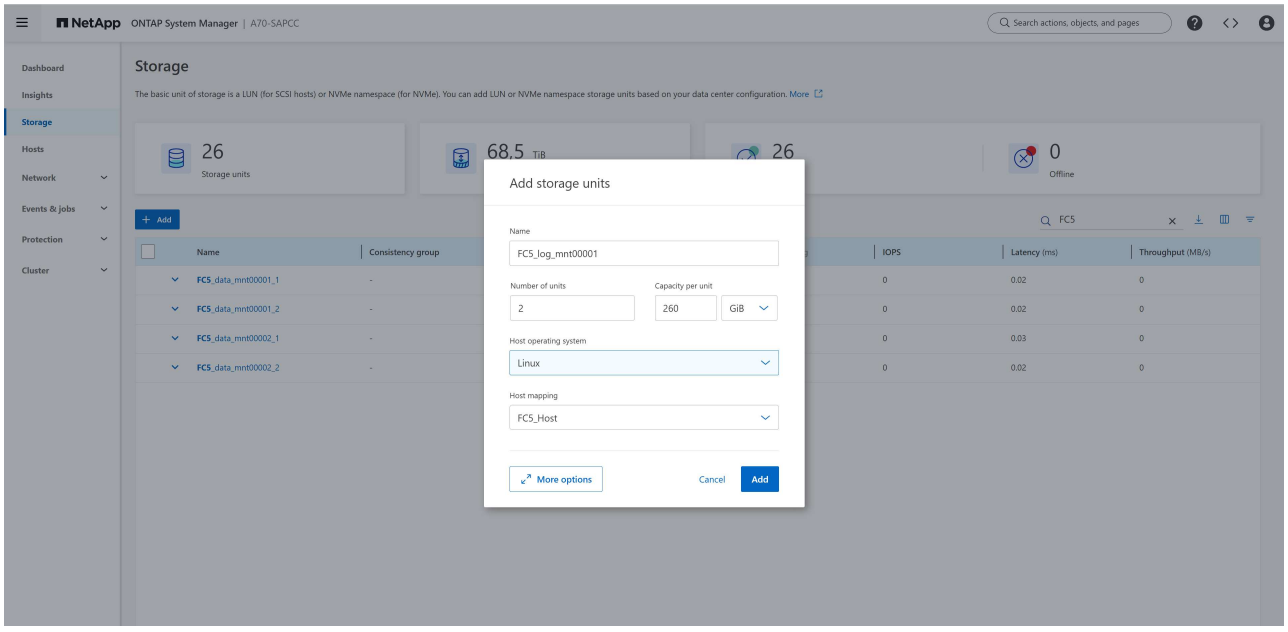


6. Ripetere i passaggi 4 e 5 per ogni host worker aggiuntivo

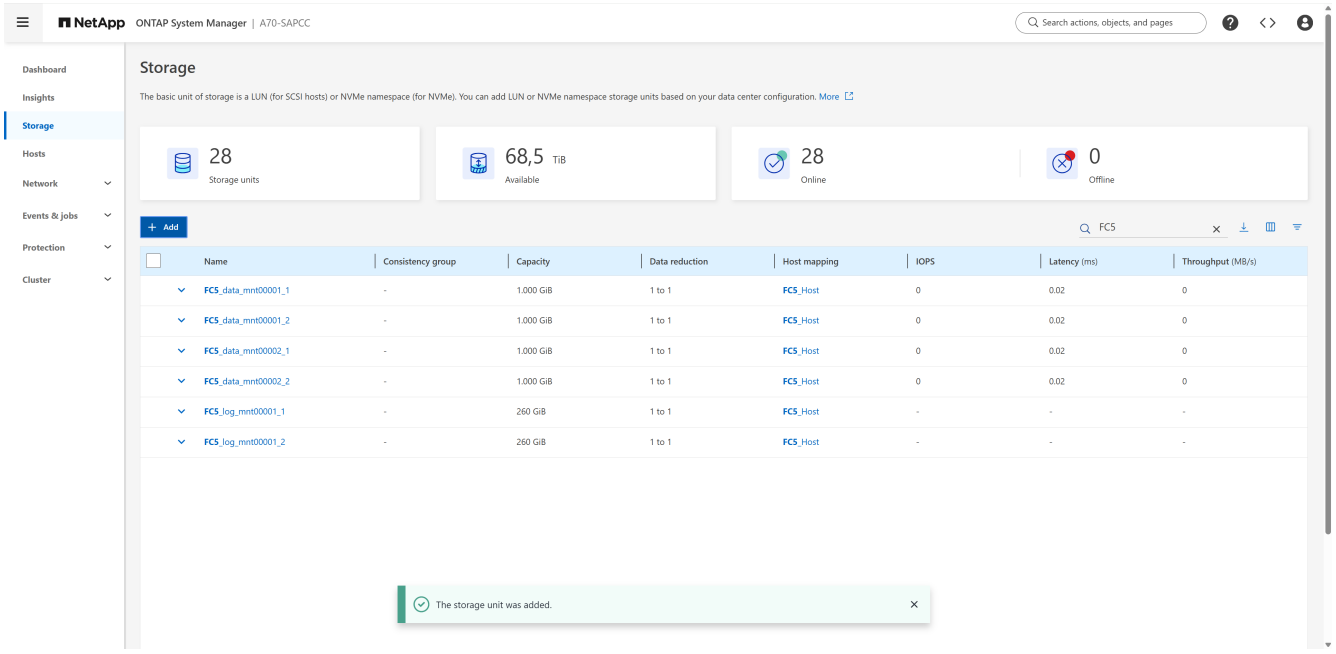
7. Dopo aver creato correttamente i LUN dei dati, creare i LUN del registro premendo `Add`



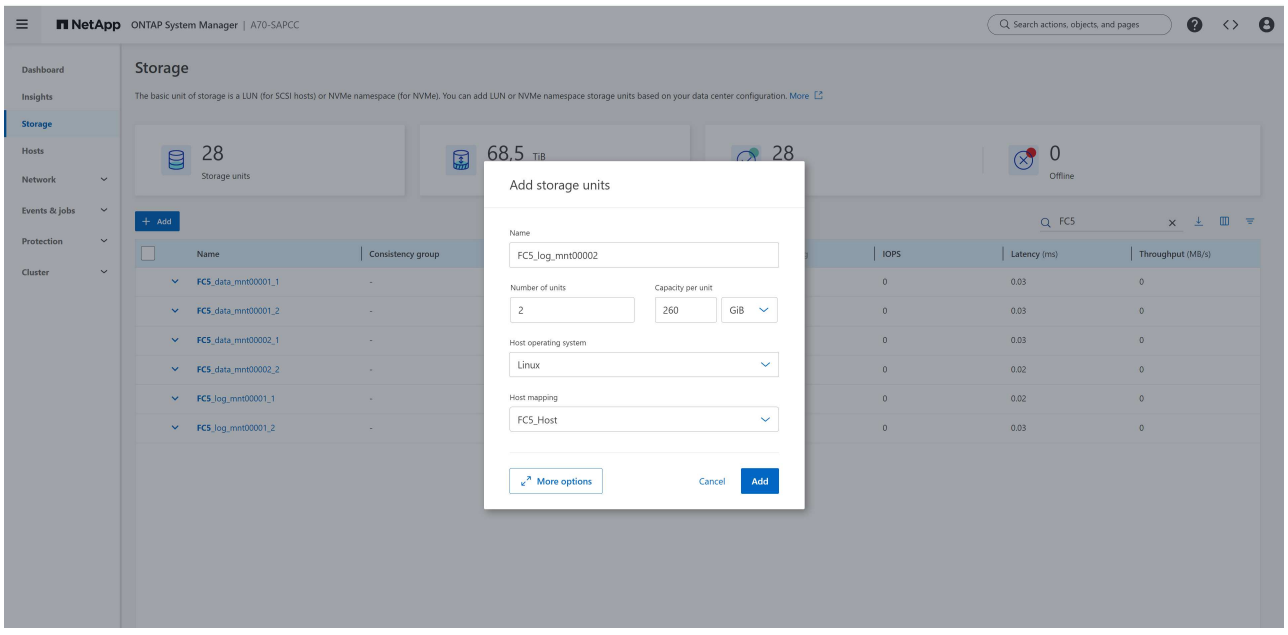
8. Fornire le informazioni richieste:
   a. il nome del registro LUN da combinare con LVM, ad esempio `FC5_log_mnt00001`
   b. la quantità di LUN da combinare con LVM, ad esempio 2
   c. la dimensione di ogni LUN, ad esempio 260 GB
   d. scegliere `Linux` COME `Host Operating system`
   e. scegli la mappatura creata in precedenza `FC5_host` per il `Host mapping` opzione
   f. premere `Add`



9. Creare i LUN di registro per il prossimo host worker premendo `Add`

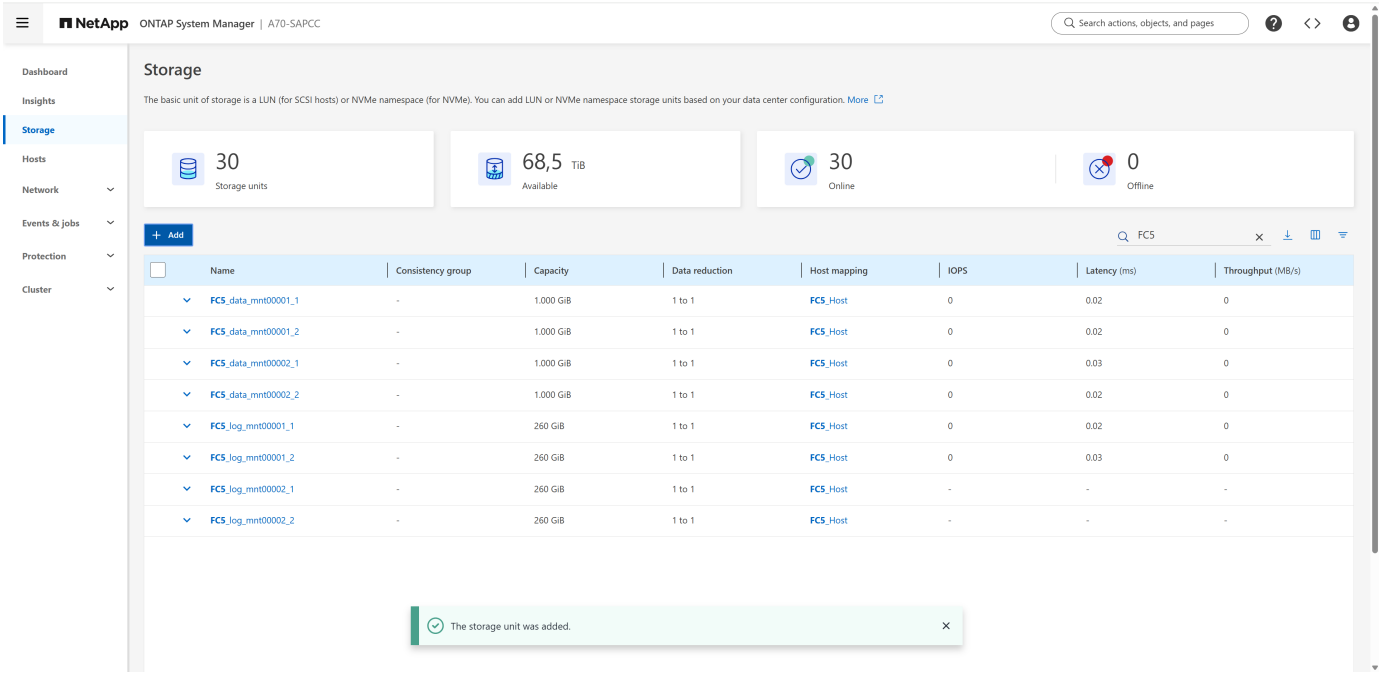


10. Fornire le informazioni richieste:
    a. il nome dei LUN di registro aggiuntivi, ad esempio `FC5_log_mnt00002`
    b. la quantità di LUN da combinare con LVM, ad esempio 2
    c. la dimensione di ogni LUN, ad esempio 260 GB
    d. scegliere `Linux` COME `Host Operating system`
    e. scegli la mappatura creata in precedenza `FC5_host` per il `Host mapping` opzione
    f. premere `Add`



11. Ripetere i passaggi 9 e 10 per ogni host worker aggiuntivo

Sono stati creati tutti i LUN necessari per un sistema SAP HANA multi-host.



API di SAP HANA storage Connector

Un connettore di storage è richiesto solo in ambienti con più host dotati di funzionalità di failover. In configurazioni con più host, SAP HANA offre funzionalità ad alta disponibilità in modo che un host di database SAP HANA possa eseguire il failover su un host in standby.

In questo caso, l'host di standby accede e utilizza i LUN dell'host guasto. Il connettore di storage viene utilizzato per garantire l'accesso attivo a una partizione di storage da parte di un solo host di database alla volta.

Nelle configurazioni di host multipli SAP HANA con storage NetApp, viene utilizzato il connettore di storage standard fornito da SAP. La "SAP HANA Fibre Channel Storage Connector Admin Guide" è disponibile come allegato a. "Nota SAP 1900823".

Configurazione dell'host

Prima di configurare l'host, è necessario scaricare le utility host NETAPP SAN da "Supporto NetApp" E installato sui server HANA. La documentazione dell'utility host include informazioni sul software aggiuntivo che deve essere installato in base all'HBA FCP utilizzato.

La documentazione contiene anche informazioni sulle configurazioni multipath specifiche per la versione di Linux utilizzata. Questo documento illustra le procedure di configurazione richieste per SLES 12 SP1 o versione successiva e RHEL 7. 2 o successiva, come descritto nella "Guida all'installazione e all'installazione di Linux host Utilities 7.1".

Configurare il multipathing

> I passaggi da 1 a 6 devono essere eseguiti su tutti gli host worker e standby in una configurazione multi-host SAP HANA.

Per configurare il multipathing, attenersi alla seguente procedura:

1. Eseguire Linux `rescan-scsi-bus.sh -a` Su ciascun server per rilevare nuove LUN.
2. Esegui il `sanlun lun show` comando e verificare che tutti i LUN richiesti siano visibili. L'esempio seguente mostra il `sanlun lun show` Output del comando per un sistema HANA multi-host 2+1 con due LUN di dati e due LUN di log. L'output mostra le LUN e i file di dispositivo corrispondenti, come LUN `FC5_data_mnt00001` e il file del dispositivo `/dev/sdag` Ogni LUN ha otto percorsi FC dall'host ai controller di archiviazione.

```
sapcc-hana-tst:~ # sanlun lun show
controller(7mode/E-Series)/                                    device
host                  lun
vserver(cDOT/FlashRay)        lun-pathname                     filename
adapter    protocol   size    product
------------------------------------------------------------------------
---------------------------------------
svm1                          FC5_log_mnt00002_2               /dev/sdbb
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002_1               /dev/sdba
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001_2               /dev/sdaz
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001_1               /dev/sday
host21     FCP        500g    cDOT
svm1                          FC5_data_mnt00002_2              /dev/sdax
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002_1              /dev/sdaw
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001_2              /dev/sdav
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001_1              /dev/sdau
host21     FCP        1t      cDOT
svm1                          FC5_log_mnt00002_2               /dev/sdat
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002_1               /dev/sdas
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001_2               /dev/sdar
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001_1               /dev/sdaq
host21     FCP        500g    cDOT
svm1                          FC5_data_mnt00002_2              /dev/sdap
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002_1              /dev/sdao
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001_2              /dev/sdan
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001_1              /dev/sdam
host21     FCP        1t      cDOT
```

```
svm1                            FC5_log_mnt00002_2            /dev/sdal
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00002_1            /dev/sdak
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001_2            /dev/sdaj
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001_1            /dev/sdai
host20     FCP         500g     cDOT
svm1                            FC5_data_mnt00002_2           /dev/sdah
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00002_1           /dev/sdag
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001_2           /dev/sdaf
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001_1           /dev/sdae
host20     FCP         1t       cDOT
svm1                            FC5_log_mnt00002_2            /dev/sdad
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00002_1            /dev/sdac
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001_2            /dev/sdab
host20     FCP         500g     cDOT
svm1                            FC5_log_mnt00001_1            /dev/sdaa
host20     FCP         500g     cDOT
svm1                            FC5_data_mnt00002_2           /dev/sdz
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00002_1           /dev/sdy
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001_2           /dev/sdx
host20     FCP         1t       cDOT
svm1                            FC5_data_mnt00001_1           /dev/sdw
host20     FCP         1t       cDOT
```

3. Esegui il `multipath -r` E `multipath -ll` comando per ottenere gli identificatori mondiali (WWID) per i nomi dei file del dispositivo.

In questo esempio ci sono otto LUN.

```
sapcc-hana-tst:~ # multipath -r
sapcc-hana-tst:~ # multipath -ll
3600a098038314e63492b59326b4b786d dm-7 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
```

```
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
3600a098038314e63492b59326b4b786e dm-9 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
3600a098038314e63492b59326b4b786f dm-11 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
3600a098038314e63492b59326b4b7870 dm-13 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
3600a098038314e63532459326d495a64 dm-6 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
3600a098038314e63532459326d495a65 dm-8 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
3600a098038314e63532459326d495a66 dm-10 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
```

```
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
3600a098038314e63532459326d495a67 dm-12 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

4. Modificare il `/etc/multipath.conf` File e aggiungere i WWID e i nomi degli alias.

> L'output di esempio mostra il contenuto di `/etc/multipath.conf` File, che include nomi alias per le quattro LUN di un sistema a più host 2+1. Se non è disponibile alcun file multipath.conf, è possibile crearne uno eseguendo il seguente comando: `multipath -T > /etc/multipath.conf`.

```
sapcc-hana-tst:/ # cat /etc/multipath.conf
multipaths {
                multipath {
                wwid    3600a098038314e63492b59326b4b786d
                alias   svm1-FC5_data_mnt00001_2
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786e
                alias   svm1-FC5_data_mnt00002_2
        }
        multipath {
                wwid    3600a098038314e63532459326d495a64
                alias   svm1-FC5_data_mnt00001_1
        }
        multipath {
                wwid    3600a098038314e63532459326d495a65
                alias   svm1-FC5_data_mnt00002_1
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786f
                alias   svm1-FC5_log_mnt00001_2
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b7870
                alias   svm1-FC5_log_mnt00002_2
        }
        multipath {
                wwid    3600a098038314e63532459326d495a66
                alias   svm1-FC5_log_mnt00001_1
        }
        multipath {
                wwid    3600a098038314e63532459326d495a67
                alias   svm1-FC5_log_mnt00002_1
        }


}
```

5. Eseguire `multipath -r` comando per ricaricare la mappa del dispositivo.
6. Verificare la configurazione eseguendo `multipath -ll` Per elencare tutti i LUN, i nomi degli alias e i percorsi attivi e di standby.

> Il seguente esempio di output mostra l'output di un sistema HANA 2+1 multihost con due LUN di dati e due di log.

```
sapcc-hana-tst:~ # multipath -ll
svm1-FC5_data_mnt00001_2 (3600a098038314e63492b59326b4b786d) dm-7
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
svm1-FC5_data_mnt00002_2 (3600a098038314e63492b59326b4b786e) dm-9
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
svm1-FC5_data_mnt00001_1 (3600a098038314e63532459326d495a64) dm-6
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
svm1-FC5_data_mnt00002_1 (3600a098038314e63532459326d495a65) dm-8
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
svm1-FC5_log_mnt00001_2 (3600a098038314e63492b59326b4b786f) dm-11
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
```

```
svm1-FC5_log_mnt00002_2 (3600a098038314e63492b59326b4b7870) dm-13
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
svm1-FC5_log_mnt00001_1 (3600a098038314e63532459326d495a66) dm-10
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
svm1-FC5_log_mnt00002_1 (3600a098038314e63532459326d495a67) dm-12
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

Configurazione host singolo

Configurazione host singolo

In questo capitolo viene descritta la configurazione di un singolo host SAP HANA.

Configurazione LUN per sistemi SAP HANA a host singolo

Linux LVM viene utilizzato per aumentare le prestazioni e risolvere i limiti delle dimensioni LUN. Nell'host SAP HANA, è necessario creare e montare gruppi di volumi e volumi logici, come indicato nella tabella seguente.

Volume logico/LUN	Punto di montaggio sull'host SAP HANA	Nota
LV: FC5_data_mnt00001-vol	/hana/data/FC5/mnt00001	Montato usando /etc/fstab entry
LV: FC5_log_mnt00001-vol	/hana/log/FC5/mnt00001	Montato usando /etc/fstab entry
LUN: FC5_shared	/hana/shared/FC5	Montato usando /etc/fstab entry

Con la configurazione descritta, il `/usr/sap/FC5` La directory in cui è memorizzata la directory home predefinita dell'utente FC5adm si trova sul disco locale. In una configurazione di disaster recovery con replica basata su disco, NetApp consiglia di creare una LUN aggiuntiva per `/usr/sap/FC5` directory in modo che tutti i file system siano nella memoria centrale.

Creare gruppi di volumi LVM e volumi logici

1. Inizializzare tutti i LUN come volume fisico.

```
pvcreate /dev/mapper/svm1-FC5_data_mnt00001_1
pvcreate /dev/mapper/svm1-FC5_data_mnt00001_2
pvcreate /dev/mapper/svm1-FC5_log_mnt00001_1
pvcreate /dev/mapper/svm1-FC5_log_mnt00001_2
```

2. Creare i gruppi di volumi per ciascuna partizione di dati e log.

```
vgcreate FC5_data_mnt00001 /dev/mapper/svm1-FC5_data_mnt00001_1
/dev/mapper/svm1-FC5_data_mnt00001_2
vgcreate FC5_log_mnt00001 /dev/mapper/svm1-FC5_log_mnt00001_1
/dev/mapper/svm1-FC5_log_mnt00001_2
```

3. Creare un volume logico per ciascuna partizione di dati e log. Utilizzare una dimensione dello stripe uguale al numero di LUN utilizzati per gruppo di volumi (in questo esempio, due) e una dimensione dello stripe di 256k per i dati e 64k per il registro. SAP supporta un solo volume logico per gruppo di volumi.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Eseguire la scansione dei volumi fisici, dei gruppi di volumi e dei gruppi di volumi di tutti gli altri host.

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

Se questi comandi non trovano i volumi, è necessario riavviare il sistema.

Per montare i volumi logici, è necessario attivare i volumi logici. Per attivare i volumi, eseguire il seguente comando:

```
vgchange -a y
```

Creare file system

Creare il file system XFS su tutti i volumi logici di dati e log e sulla LUN condivisa hana.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs /dev/mapper/svm1-FC5_shared
```

I comandi di esempio di host multipli mostrano un sistema HANA a host multipli 2+1.

Creare punti di montaggio

Creare le directory dei punti di montaggio richiesti e impostare le autorizzazioni sull'host del database:

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod –R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod –R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

Montare i file system

Per montare i file system durante l'avvio del sistema utilizzando `/etc/fstab` file di configurazione, aggiungere i file system richiesti al `/etc/fstab` file di configurazione:

```
# cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/FC5_log_mnt00001-vol /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/FC5_data_mnt00001-vol /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
```

I file system XFS per i LUN di dati e log devono essere montati con `relatime` e. `inode64` opzioni di montaggio.

Per montare i file system, eseguire il comando `mount –a` comando sull'host.

Configurazione di più host

Configurazione di più host

In questo capitolo viene descritta a titolo di esempio la configurazione di un sistema multihost SAP HANA 2+1.

Configurazione LUN per sistemi multi-host SAP HANA

Linux LVM viene utilizzato per aumentare le prestazioni e risolvere i limiti delle dimensioni LUN.

Nell'host SAP HANA, è necessario creare e montare gruppi di volumi e volumi logici, come indicato nella tabella seguente.

Volume logico (LV)	Punto di montaggio sull'host SAP HANA	Nota
LV: FC5_data_mnt00001-vol	/hana/data/FC5/mnt00001	Montato utilizzando un connettore storage
LV: FC5_log_mnt00001-vol	/hana/log/FC5/mnt00001	Montato utilizzando un connettore storage
LV: FC5_data_mnt00002-vol	/hana/data/FC5/mnt00002	Montato utilizzando un connettore storage
LV: FC5_log_mnt00002-vol	/hana/log/FC5/mnt00002	Montato utilizzando un connettore storage
Condivisione NFS esterna: FC5_shared	/hana/shared	Montato su tutti gli host usando NFS e /etc/fstab entry

I sistemi multi-host SAP HANA richiedono `/hana/shared` File system connesso a tutti gli host di un sistema. Solitamente si tratta di una condivisione NFS fornita da un server NFS. Si consiglia di utilizzare un server NFS ad alta disponibilità, ad esempio un sistema NetApp FAS o AFF. Un'altra opzione è quella di utilizzare il server NFS integrato di un host LINUX.

Con la configurazione descritta, il `/usr/sap/FC5` La directory in cui è memorizzata la directory home predefinita dell'utente FC5adm si trova sul disco locale di ciascun host HANA. In una configurazione di disaster recovery con replica basata su disco, NetApp consiglia di utilizzare quattro LUN aggiuntive per `/usr/sap/FC5` file system di ciascun host in modo che ogni host del database abbia tutti i suoi file system sullo storage centrale.

Creare gruppi di volumi LVM e volumi logici

1. Inizializzare tutti i LUN come volume fisico.

```
pvcreate /dev/mapper/svm1-FC5_data_mnt00001_1
pvcreate /dev/mapper/svm1-FC5_data_mnt00001_2
pvcreate /dev/mapper/svm1-FC5_data_mnt00002_1
pvcreate /dev/mapper/svm1-FC5_data_mnt00002_2
pvcreate /dev/mapper/svm1-FC5_log_mnt00001_1
pvcreate /dev/mapper/svm1-FC5_log_mnt00001_2
pvcreate /dev/mapper/svm1-FC5_log_mnt00002_1
pvcreate /dev/mapper/svm1-FC5_log_mnt00002_2
```

2. Creare i gruppi di volumi per ciascuna partizione di dati e log.

```
vgcreate FC5_data_mnt00001 /dev/mapper/svm1-FC5_data_mnt00001_1
/dev/mapper/svm1-FC5_data_mnt00001_2
vgcreate FC5_data_mnt00002 /dev/mapper/svm1-FC5_data_mnt00002_1
/dev/mapper/svm1-FC5_data_mnt00002_2
vgcreate FC5_log_mnt00001 /dev/mapper/svm1-FC5_log_mnt00001_1
/dev/mapper/svm1-FC5_log_mnt00001_2
vgcreate FC5_log_mnt00002 /dev/mapper/svm1-FC5_log_mnt00002_1
/dev/mapper/svm1-FC5_log_mnt00002_2
```

3. Creare un volume logico per ciascuna partizione di dati e log. Utilizzare una dimensione dello stripe uguale al numero di LUN utilizzati per gruppo di volumi (in questo esempio, due) e una dimensione dello stripe di 256k per i dati e 64k per il registro. SAP supporta un solo volume logico per gruppo di volumi.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Eseguire la scansione dei volumi fisici, dei gruppi di volumi e dei gruppi di volumi di tutti gli altri host.

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

Se questi comandi non trovano i volumi, è necessario riavviare il sistema.

Per montare i volumi logici, è necessario attivare i volumi logici. Per attivare i volumi, eseguire il seguente comando:

```
vgchange -a y
```

Creare file system

Creare il file system XFS su tutti i volumi logici di dati e log.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_data_mnt00002-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs FC5_log_mnt00002-vol
```

Creare punti di montaggio

Crea le directory dei punti di montaggio richiesti e imposta le autorizzazioni su tutti gli host worker e standby:

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod -R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod -R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

Montare i file system

Per montare il `/hana/shared` file system durante l'avvio del sistema utilizzando `/etc/fstab` file di configurazione, aggiungere il `/hana/shared` file system al `/etc/fstab` file di configurazione di ciascun host.

```
sapcc-hana-tst:/ # cat /etc/fstab
<storage-ip>:/hana_shared /hana/shared nfs rw,vers=3,hard,timeo=600,
intr,noatime,nolock 0 0
```

Tutti i file system di log e dati vengono montati tramite il connettore storage SAP HANA.

Per montare i file system, eseguire `mount -a` su ciascun host.

Configurazione dello stack di i/o per SAP HANA

Configurazione dello stack di i/o per SAP HANA

A partire da SAP HANA 1.0 SPS10, SAP ha introdotto i parametri per regolare il comportamento di i/o e ottimizzare il database per il file e il sistema storage utilizzati.

NetApp ha condotto test delle performance per definire i valori ideali. La seguente tabella elenca i valori ottimali dedotti dai test delle prestazioni.

Parametro	Valore
max_parallel_io_requests	128
async_read_submit	acceso
async_write_submit_active	acceso
async_write_submit_blocks	tutto

Per i sistemi da SAP HANA 1.0 a SPS12, questi parametri possono essere impostati durante l'installazione del database SAP HANA, come descritto nella nota SAP "2267798 – Configurazione del database SAP HANA durante l'installazione con hdbparam".

In alternativa, è possibile impostare i parametri dopo l'installazione del database SAP HANA utilizzando `hdbparam` framework.

```
FC5adm@sapcc-hana-tst:/usr/sap/FC5/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
FC5adm@sapcc-hana-tst:/usr/sap/FC5/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
FC5adm@sapcc-hana-tst:/usr/sap/FC5/HDB00> hdbparam --paramset
fileio.async_read_submit=on
FC5adm@sapcc-hana-tst:/usr/sap/FC5/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

A partire da SAP HANA 2.0, `hdbparam` è obsoleto e i parametri vengono spostati su `global.ini` file. I parametri possono essere impostati utilizzando i comandi SQL o SAP HANA Studio. Per ulteriori informazioni, fare riferimento alla nota SAP "2399079: Eliminazione di hdbparam in HANA 2". I parametri possono essere impostati anche all'interno di `global.ini` file.

```
FC5adm@sapcc-hana-tst: /usr/sap/FC5/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

Per SAP HANA 2.0 SPS5 e versioni successive, utilizzare `setParameter.py` script per impostare i parametri corretti.

```
fc5adm@sapcc-hana-tst-03:/usr/sap/FC5/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

Installazione del software SAP HANA

Questa sezione descrive la preparazione necessaria per installare SAP HANA su sistemi a host singolo e su sistemi a più host.

Installazione su sistema a host singolo

L'installazione del software SAP HANA non richiede alcuna preparazione aggiuntiva per un sistema a singolo host.

Installazione su sistemi a più host

Prima di iniziare l'installazione, creare un `global.ini` File per abilitare l'utilizzo di SAP Storage Connector durante il processo di installazione. Il connettore di storage SAP monta i file system richiesti sugli host di lavoro durante il processo di installazione. Il `global.ini` il file deve essere disponibile in un file system accessibile da tutti gli host, ad esempio `/hana/shared` file system.

Prima di installare il software SAP HANA su un sistema a più host, è necessario completare la seguente procedura:

1. Aggiungere le seguenti opzioni di montaggio per i LUN dei dati e i LUN del registro a `global.ini` file:
   - `relatime` e. `inode64` per il file system di dati e log
2. Aggiungere i WWID delle partizioni dei dati e dei log. Gli ID WWID devono corrispondere ai nomi alias configurati in `/etc/multipath.conf` file.

   L'esempio seguente mostra un setup di 2+1 host multipli con SID=FC5.

```
sapcc-hana-tst-03:/hana/shared # cat global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/FC5
basepath_logvolumes = /hana/log/FC5
[storage]
ha_provider = hdb_ha.fcClientLVM
partition_*_*__prtype = 5
partition_*_data__mountOptions = -o relatime,inode64
partition_*_log__mountOptions = -o relatime,inode64
partition_1_data__lvmname = FC5_data_mnt00001-vol
partition_1_log__lvmname = FC5_log_mnt00001-vol
partition_2_data__lvmname = FC5_data_mnt00002-vol
partition_2_log__lvmname = FC5_log_mnt00002-vol
sapcc-hana-tst-03:/hana/shared #
```

Utilizzando lo strumento di installazione SAP hdblcm, avviare l'installazione eseguendo il seguente comando su uno degli host worker. Utilizzare l' `addhosts`opzione per aggiungere il secondo lavoratore (sapcc-hana-tst-06) e l'host di standby (sapcc-hana-tst-07).

+

> La directory in cui è memorizzato il file preparato `global.ini` è inclusa con l' `storage_cfg`opzione CLI (--storage_cfg=/hana/shared`).

+

A seconda della versione del sistema operativo in uso, potrebbe essere necessario installare Python 2.7 prima di installare il database SAP HANA.

+

```
./hdblcm --action=install --addhosts=sapcc-hana-tst
-06:role=worker:storage_partition=2,sapcc-hana-tst-07:role=standby
--storage_cfg=/hana/shared/

AP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1 (1.015.0)
in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
```

```
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip


SAP HANA Database version '2.00.073.00.1695288802' will be installed.

Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------
------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version 2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
```

```
  9     | epmmds           | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
4.203.2321.0.0

Enter comma-separated list of the selected indices [3,4]: 2,3
```

1. Verificare che lo strumento di installazione abbia installato tutti i componenti selezionati su tutti gli host di lavoro e di standby.

Dove trovare ulteriori informazioni

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

- "Soluzioni software SAP HANA"
- "TR-4646: Disaster recovery SAP HANA con replica dello storage"
- "Data Protection e high Availability di SAP HANA con SnapCenter, SnapMirror Active Sync e VMware Metro Storage Cluster"
- "TR-4614: Backup e ripristino SAP HANA con SnapCenter"
- "TR-4667: Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter"
- Centri di documentazione NetApp

  "https://www.netapp.com/support-and-training/documentation/"
- Hardware per lo storage aziendale certificato SAP per SAP HANA

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"
- Requisiti di storage SAP HANA

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"
- SAP HANA - Domande frequenti sull'integrazione personalizzata del data center

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"
- SAP HANA su VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"
- Guida alle Best practice di SAP HANA su VMware vSphere

  "https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

Aggiornare la cronologia

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

Data	Riepilogo degli aggiornamenti
Luglio 2025	Versione iniziale

Guida alla configurazione di SAP HANA su sistemi NetApp FAS con NFS

Guida alla configurazione di SAP HANA su sistemi NetApp FAS con NFS

La famiglia di prodotti NetApp FAS è stata certificata per l'utilizzo con SAP HANA in progetti TDI (Tailored Data Center Integration). Questa guida fornisce le best practice per SAP HANA su questa piattaforma con NFS.

Marco Schoen, NetApp

Questa certificazione è attualmente valida solo per i seguenti modelli:

- FAS2750, FAS2820, FAS8300, FAS50, FAS8700, FAS70, FAS9500, FAS90 Un elenco completo delle soluzioni storage con certificazione NetApp per SAP HANA è disponibile all'indirizzo "Directory hardware SAP HANA certificata e supportata" .

Questo documento descrive i requisiti di configurazione di ONTAP per il protocollo NFS versione 3 (NFSv3) o per il protocollo NFS versione 4 (NFSv4.1).

Sono supportate solo le versioni NFS 3 o 4,1. Le versioni NFS 1, 2, 4,0 e 4,2 non sono supportate.

La configurazione descritta in questo documento è necessaria per ottenere i KPI SAP HANA richiesti e le migliori performance per SAP HANA. La modifica di impostazioni o l'utilizzo di funzionalità non elencate nel presente documento potrebbe causare un peggioramento delle prestazioni o un comportamento imprevisto e deve essere eseguita solo se richiesto dal supporto NetApp.

Le guide di configurazione per i sistemi NetApp FAS che utilizzano FCP e per i sistemi AFF che utilizzano NFS o FC sono disponibili ai seguenti "SAP HANA su sistemi NetApp FAS con FCP"
* "SAP HANA su sistemi NetApp AFF con NFS"
* "SAP HANA su sistemi NetApp AFF con FCP"
* "SAP HANA su sistemi NetApp ASA con FCP"

La seguente tabella mostra le combinazioni supportate per le versioni di NFS, il blocco NFS e le implementazioni di isolamento richieste, a seconda della configurazione del database SAP HANA.

Per sistemi SAP HANA a host singolo o host multipli senza failover automatico host, sono supportati NFSv3 e NFSv4.

Per i sistemi host SAP HANA multipli con host Auto-failover, NetApp supporta solo NFSv4, utilizzando il blocco NFSv4 come alternativa all'implementazione di STONITH (SAP HANA ha/DR provider) specifica del server.

SAP HANA	Versione NFS	Blocco NFS	PROVIDER SAP HANA HA/DR
SAP HANA host singolo, host multipli senza failover automatico dell'host	NFSv3	Spento	n/a.
	NFSv4	Acceso	n/a.
SAP HANA host multipli con host Auto-failover	NFSv3	Spento	Implementazione STONITH specifica del server obbligatoria
	NFSv4	Acceso	Non richiesto

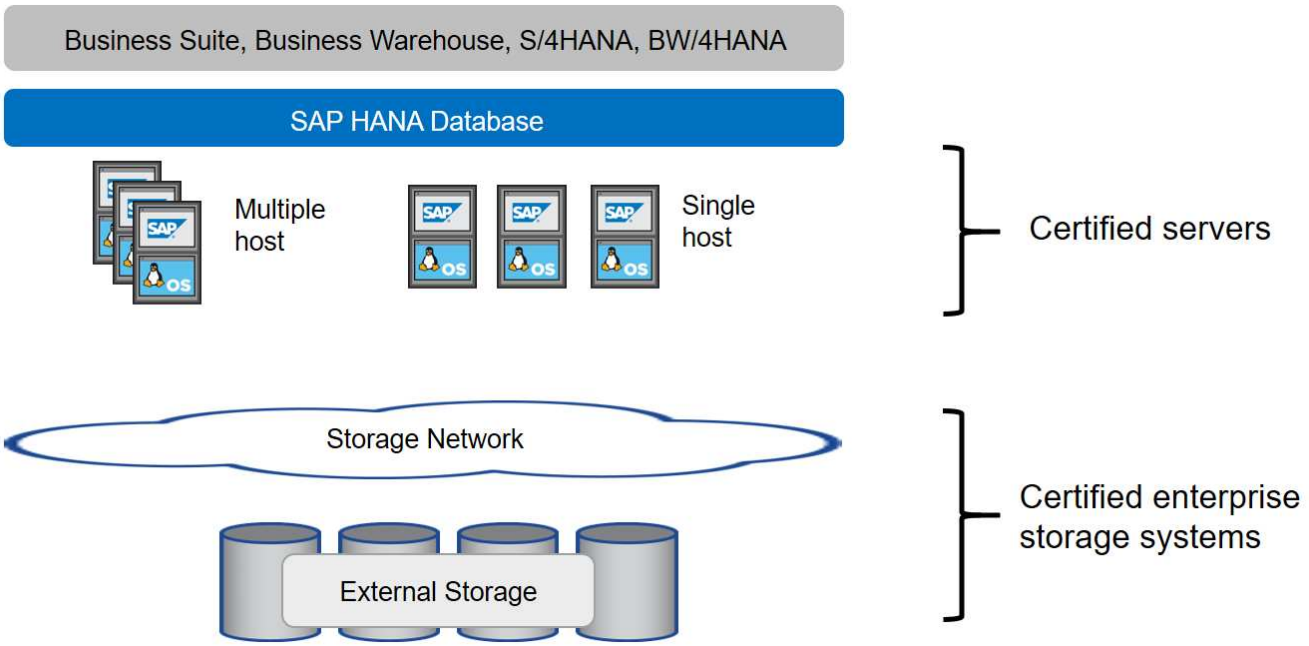
Un'implementazione STONITH specifica per il server non fa parte di questa guida. Contattare il fornitore del server per un'implementazione di questo tipo.

Questo documento illustra i consigli di configurazione per SAP HANA in esecuzione su server fisici e su server virtuali che utilizzano VMware vSphere.

Fare sempre riferimento alle note SAP relative alle linee guida per la configurazione del sistema operativo e alle dipendenze specifiche del kernel Linux HANA. Per ulteriori informazioni, vedere "Nota SAP 2235581: Sistemi operativi supportati da SAP HANA".

SAP HANA integrazione personalizzata del data center

I controller di storage NetApp FAS sono certificati nel programma SAP HANA TDI utilizzando protocolli NFS (NAS) e FC (SAN). Possono essere implementati in uno qualsiasi degli scenari SAP HANA attuali, come SAP Business Suite su HANA, S/4HANA, BW/4HANA o SAP Business Warehouse su HANA, in configurazioni a host singolo o multiplo. Qualsiasi server certificato per l'utilizzo con SAP HANA può essere combinato con soluzioni di storage certificate NetApp. Vedere la figura seguente per una panoramica dell'architettura.



Per ulteriori informazioni sui prerequisiti e sui consigli per i sistemi SAP HANA in produzione, consulta la seguente risorsa SAP:

- "SAP HANA - Domande frequenti sull'integrazione personalizzata del data center"

SAP HANA con VMware vSphere

Esistono diverse opzioni per connettere lo storage alle macchine virtuali (VM). Il metodo preferito consiste nel collegare i volumi di storage con NFS direttamente dal sistema operativo guest. Utilizzando questa opzione, la configurazione di host e storage non differisce tra host fisici e macchine virtuali.

Sono supportati anche datastore NFS o datastore VVOL con NFS. Per entrambe le opzioni, è necessario memorizzare un solo volume di log o dati SAP HANA all'interno del datastore per i casi di utilizzo in produzione.

Questo documento descrive la configurazione consigliata con i montaggi NFS diretti dal sistema operativo guest.

Per ulteriori informazioni sull'utilizzo di vSphere con SAP HANA, consultare i seguenti collegamenti:

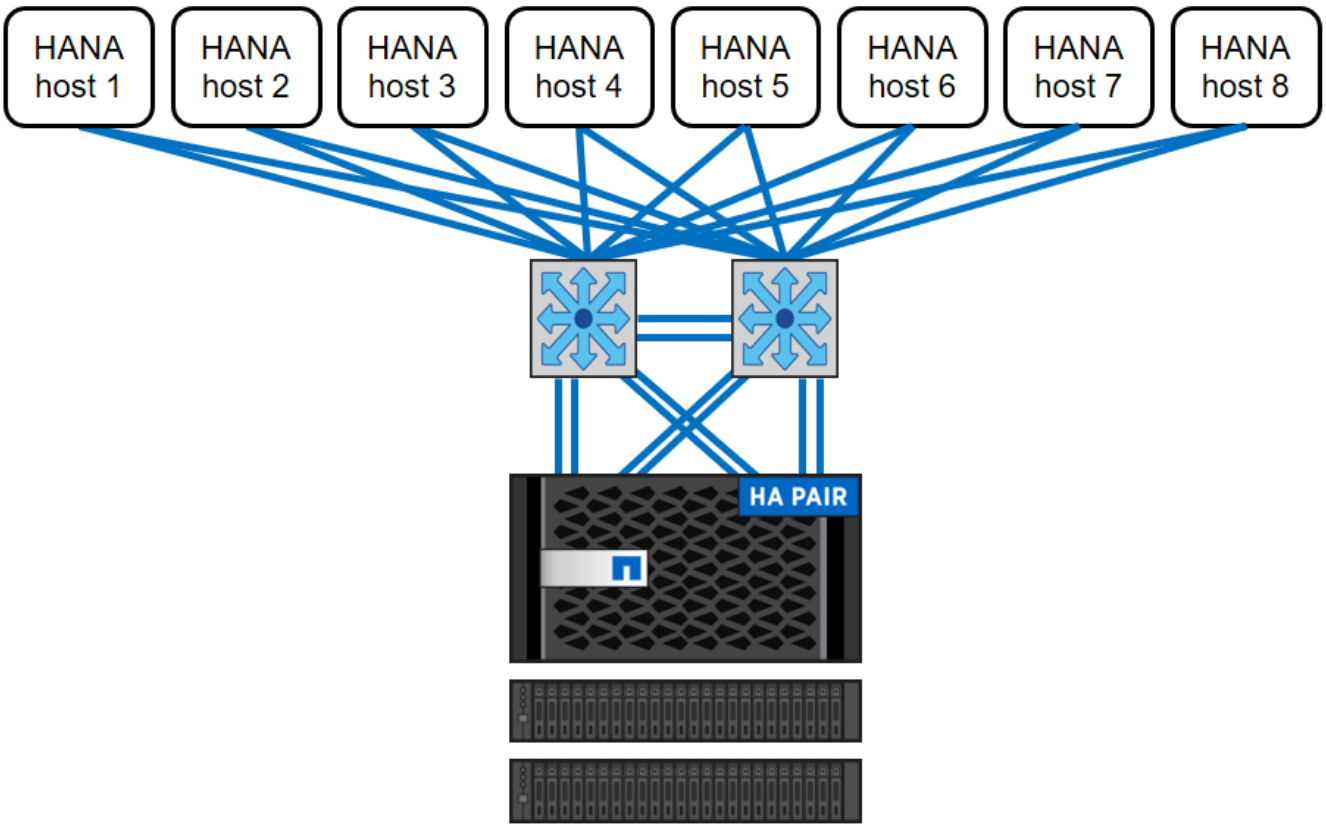
- "SAP HANA su VMware vSphere - virtualizzazione - Wiki della community"
- "Guida alle Best practice di SAP HANA su VMware vSphere"
- "2161991 - linee guida per la configurazione di VMware vSphere - Launchpad di supporto SAP ONE (accesso richiesto)"

Architettura

Gli host SAP HANA sono connessi ai controller di storage utilizzando un'infrastruttura di rete ridondante da 10 GbE o più veloce. La comunicazione dei dati tra gli host SAP HANA e i controller di storage si basa sul protocollo NFS.

Si consiglia di utilizzare un'infrastruttura di switching ridondante per fornire una connettività host-to-storage SAP HANA fault-tolerant in caso di guasto dello switch o della scheda di interfaccia di rete (NIC). Gli switch potrebbero aggregare le performance delle singole porte con i canali delle porte in modo da apparire come una singola entità logica a livello di host.

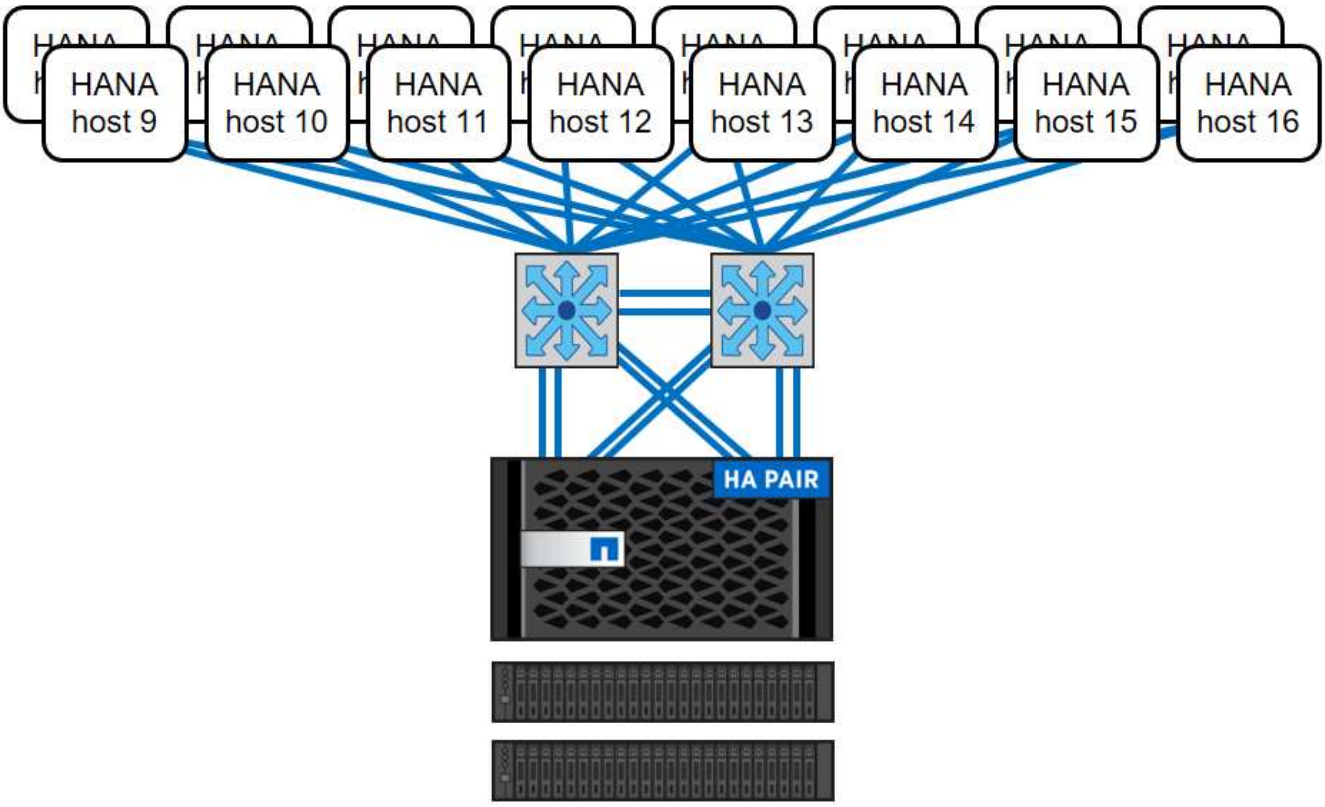
Diversi modelli della famiglia di sistemi FAS possono essere combinati e abbinati a livello di storage per consentire la crescita e le diverse esigenze di performance e capacità. Il numero massimo di host SAP HANA che possono essere collegati al sistema storage è definito dai requisiti di performance SAP HANA e dal modello di controller NetApp utilizzato. Il numero di shelf di dischi richiesti è determinato solo dai requisiti di capacità e performance dei sistemi SAP HANA. La figura seguente mostra una configurazione di esempio con otto host SAP HANA collegati a una coppia di storage ad alta disponibilità (ha).



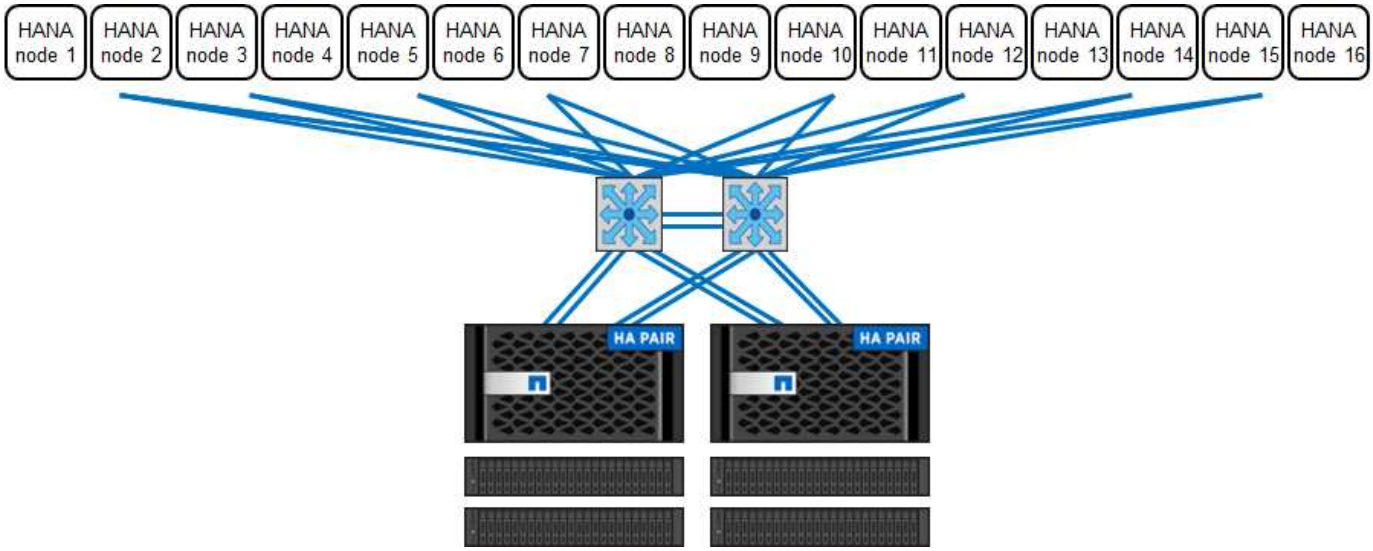
L'architettura può essere scalata in due dimensioni:

- Collegando altri host SAP HANA e/o capacità di storage allo storage esistente, se i controller di storage forniscono performance sufficienti per soddisfare gli attuali indicatori chiave di performance SAP (KPI)
- Aggiungendo altri sistemi storage con capacità di storage aggiuntiva per gli host SAP HANA aggiuntivi

La figura seguente mostra una configurazione di esempio in cui più host SAP HANA sono collegati ai controller di storage. In questo esempio, sono necessari più shelf di dischi per soddisfare i requisiti di capacità e performance di 16 host SAP HANA. A seconda dei requisiti di throughput totale, è necessario aggiungere ulteriori connessioni 10 GbE (o più veloci) ai controller di storage.



Indipendentemente dal sistema FAS implementato, il panorama SAP HANA può essere scalato aggiungendo uno qualsiasi dei controller di storage certificati per soddisfare la densità di nodo desiderata (figura seguente).



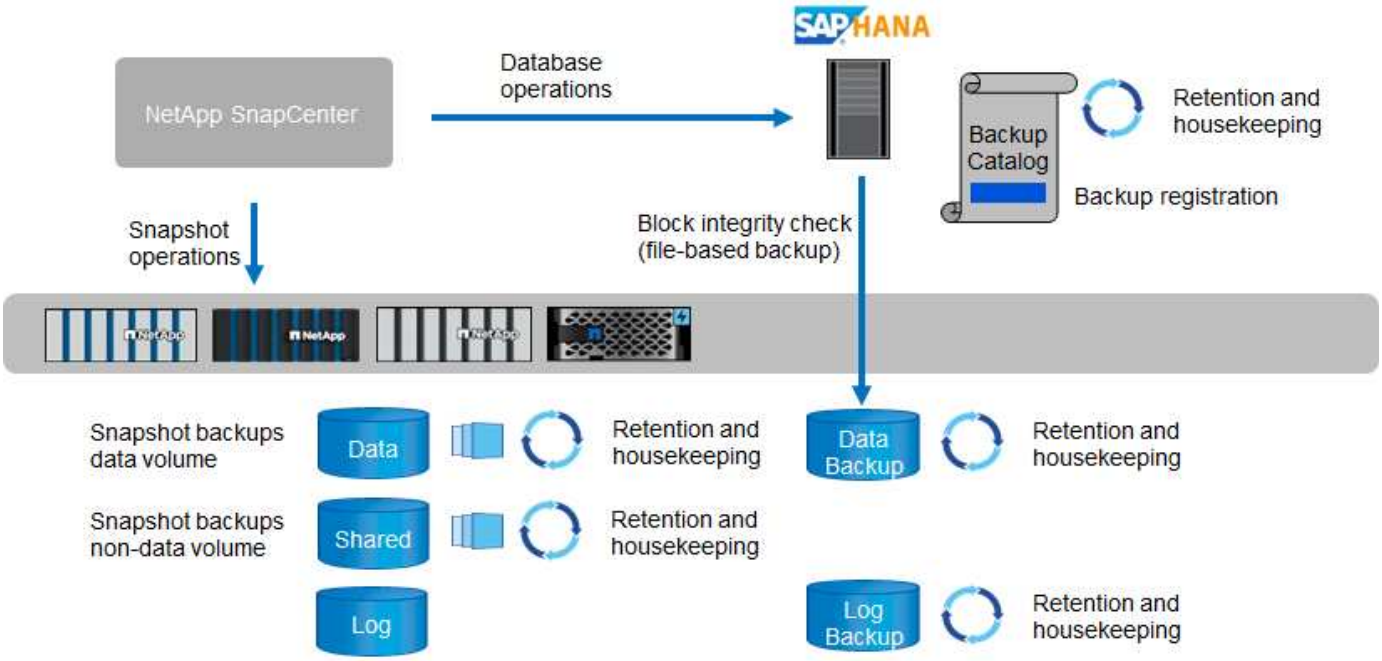
Backup SAP HANA

Il software ONTAP presente su tutti i controller di storage NetApp offre un meccanismo integrato per eseguire il backup dei database SAP HANA durante il funzionamento senza alcun effetto sulle performance. I backup NetApp Snapshot basati su storage sono una soluzione di backup completamente supportata e integrata disponibile per i singoli container SAP HANA e per i sistemi SAP HANA Multitenant Database Container (MDC) con un singolo tenant o più tenant.

I backup Snapshot basati su storage vengono implementati utilizzando il plug-in NetApp SnapCenter per SAP HANA. Ciò consente agli utenti di creare backup Snapshot coerenti basati sullo storage utilizzando le interfacce fornite in modo nativo dai database SAP HANA. SnapCenter registra tutti i backup Snapshot nel catalogo di backup SAP HANA. Pertanto, i backup eseguiti da SnapCenter sono visibili all'interno di SAP HANA Studio e Cockpit, dove possono essere selezionati direttamente per le operazioni di ripristino e recovery.

La tecnologia NetApp SnapMirror consente di replicare le copie Snapshot create su un sistema storage su un sistema storage di backup secondario controllato da SnapCenter. È quindi possibile definire diversi criteri di conservazione dei backup per ciascuno dei set di backup sullo storage primario e per i set di backup sui sistemi di storage secondari. Il plug-in SnapCenter per SAP HANA gestisce automaticamente la conservazione dei backup dei dati basati su copia Snapshot e dei backup dei log, inclusa la manutenzione del catalogo di backup. Il plug-in SnapCenter per SAP HANA consente inoltre di eseguire un controllo dell'integrità del blocco del database SAP HANA eseguendo un backup basato su file.

È possibile eseguire il backup dei log del database direttamente sullo storage secondario utilizzando un montaggio NFS, come illustrato nella figura seguente.



I backup Snapshot basati su storage offrono vantaggi significativi rispetto ai backup convenzionali basati su file. Questi vantaggi includono, a titolo esemplificativo e non esaustivo, i seguenti:

- Backup più rapido (pochi minuti)
- RTO (Recovery Time Objective) ridotto grazie a un tempo di ripristino molto più rapido sul layer di storage (pochi minuti) e a backup più frequenti
- Nessuna riduzione delle performance dell'host, della rete o dello storage del database SAP HANA durante le operazioni di backup e recovery
- Replica efficiente in termini di spazio e larghezza di banda sullo storage secondario in base alle modifiche dei blocchi

Per informazioni dettagliate sulla soluzione di backup e ripristino SAP HANA con SnapCenter, consultare "TR-4614: Backup e ripristino SAP HANA con SnapCenter".

Disaster recovery SAP HANA

Il disaster recovery SAP HANA può essere eseguito a livello di database utilizzando la replica di sistema SAP HANA o a livello di storage utilizzando le tecnologie di replica dello storage. La sezione seguente fornisce una panoramica delle soluzioni di disaster recovery basate sulla replica dello storage.

Per informazioni dettagliate sulle soluzioni di disaster recovery SAP HANA, vedere "TR-4646: Disaster recovery SAP HANA con replica dello storage".

Replica dello storage basata su SnapMirror

La figura seguente mostra una soluzione di disaster recovery a tre siti che utilizza la replica sincrona di SnapMirror nel data center di disaster recovery locale e SnapMirror asincrono per replicare i dati nel data center di disaster recovery remoto.

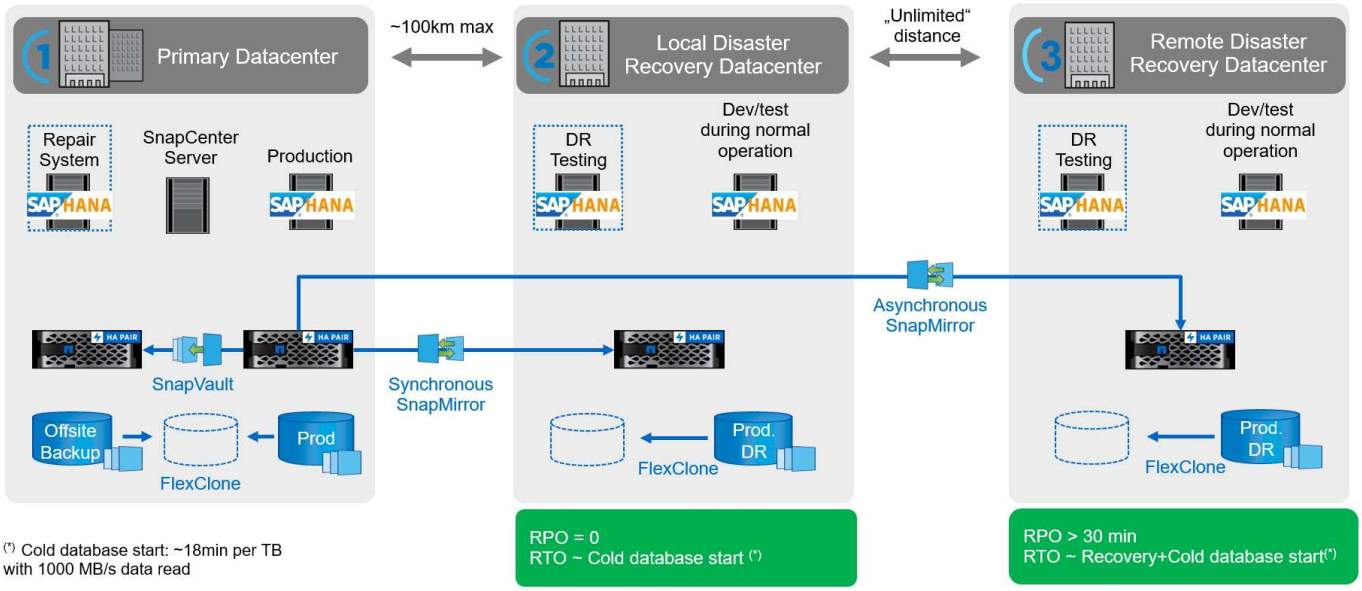
La replica dei dati con SnapMirror sincrono fornisce un RPO pari a zero. La distanza tra il data center principale e quello locale per il disaster recovery è limitata a circa 100 km.

La protezione dai guasti del sito di disaster recovery primario e locale viene eseguita replicando i dati in un terzo data center di disaster recovery remoto utilizzando SnapMirror asincrono. L'RPO dipende dalla frequenza degli aggiornamenti di replica e dalla velocità di trasferimento. In teoria, la distanza è illimitata, ma il limite dipende dalla quantità di dati da trasferire e dalla connessione disponibile tra i data center. I valori RPO tipici sono compresi nell'intervallo da 30 minuti a più ore.

L'RTO per entrambi i metodi di replica dipende principalmente dal tempo necessario per avviare il database HANA nel sito di disaster recovery e caricare i dati in memoria. Supponendo che i dati siano letti con un throughput di 1000 Mbps, il caricamento di 1 TB di dati richiederebbe circa 18 minuti.

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

Entrambi i metodi di replica consentono di eseguire test del workflow di disaster recovery senza influenzare RPO e RTO. I volumi FlexClone vengono creati sullo storage e collegati ai server di test del disaster recovery.

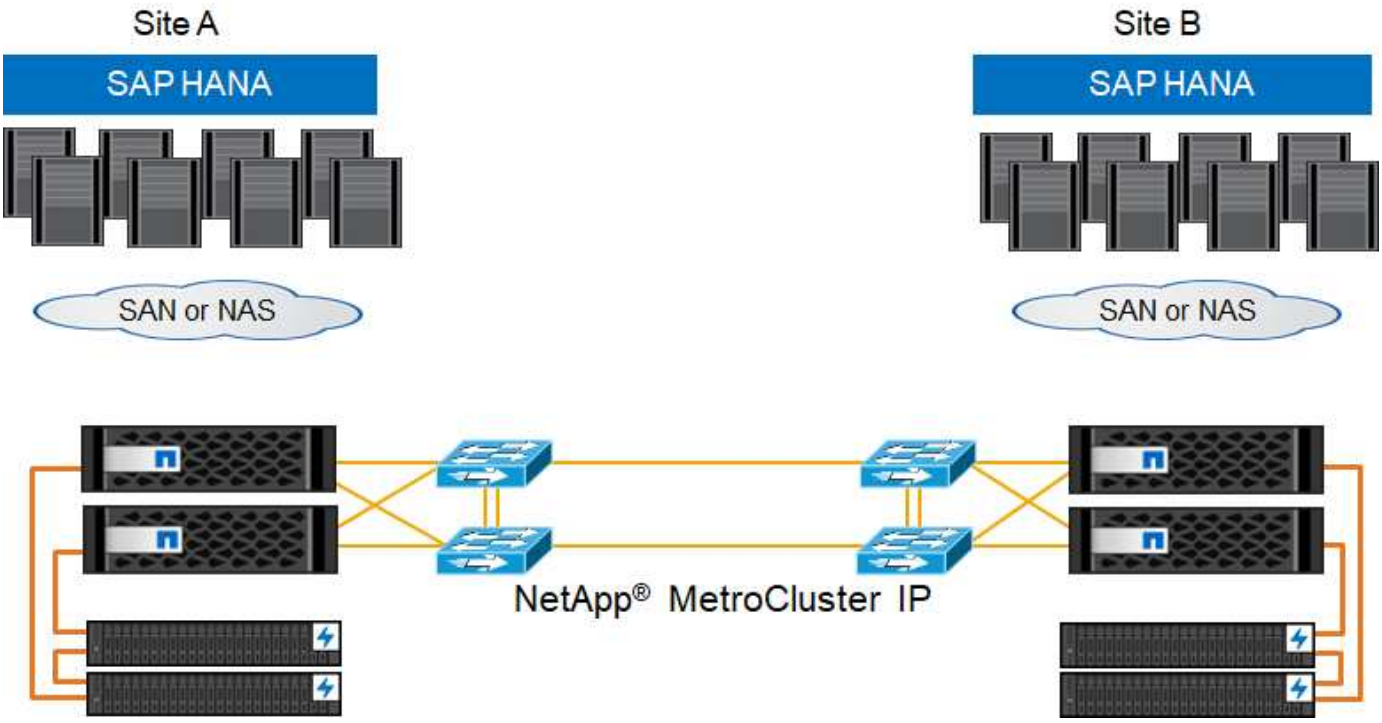


La replica sincrona offre la modalità StrictSync. Se la scrittura sullo storage secondario non viene completata per qualsiasi motivo, l'i/o dell'applicazione non riesce, garantendo così che i sistemi di storage primario e

secondario siano identici. L'i/o dell'applicazione al primario riprende solo dopo che la relazione SnapMirror ritorna allo stato InSync. In caso di guasto dello storage primario, l'i/o dell'applicazione può essere ripristinato sullo storage secondario dopo il failover, senza perdita di dati. In modalità StrictSync, l'RPO è sempre zero.

Replica dello storage basata su MetroCluster

La figura seguente mostra una panoramica di alto livello della soluzione. Il cluster di storage di ogni sito fornisce alta disponibilità locale e viene utilizzato per il carico di lavoro di produzione. I dati di ciascun sito vengono replicati in modo sincrono nell'altra posizione e sono disponibili in caso di failover di emergenza.



Dimensionamento dello storage

La sezione seguente fornisce una panoramica delle considerazioni su performance e capacità richieste per il dimensionamento di un sistema storage per SAP HANA.

Contatta NetApp o il tuo partner commerciale NetApp per aiutarti a creare un ambiente di storage di dimensioni adeguate.

Considerazioni sulle performance

SAP ha definito un set statico di KPI dello storage validi per tutti gli ambienti SAP HANA in produzione, indipendentemente dalle dimensioni della memoria degli host di database e delle applicazioni che utilizzano il database SAP HANA. Questi KPI sono validi per ambienti a host singolo, host multiplo, Business Suite su HANA, Business Warehouse su HANA, S/4HANA e BW/4HANA. Pertanto, l'attuale approccio al dimensionamento delle performance dipende solo dal numero di host SAP HANA attivi collegati al sistema storage.

I KPI relativi alle performance dello storage sono richiesti solo per i sistemi SAP HANA in produzione, ma è possibile implementarli in tutti i sistemi HANA.

SAP offre uno strumento di test delle performance utilizzato per convalidare le performance del sistema

storage per gli host SAP HANA attivi collegati allo storage.

NetApp ha testato e predefinito il numero massimo di host SAP HANA che possono essere collegati a un modello di storage specifico, pur continuando a soddisfare i KPI di storage richiesti da SAP per i sistemi SAP HANA basati sulla produzione.

> I controller di storage della famiglia di prodotti certificati FAS possono essere utilizzati anche per SAP HANA con altri tipi di dischi o soluzioni di back-end su disco. Tuttavia, devono essere supportati da NetApp e soddisfare i KPI delle performance SAP HANA TDI. Ad esempio, NetApp Storage Encryption (NSE) e la tecnologia NetApp FlexArray.

Questo documento descrive il dimensionamento dei dischi per HDD SAS e unità a stato solido (SSD).

HDD

Per soddisfare i KPI relativi alle performance di storage di SAP, è necessario un minimo di 10 dischi dati (SAS a 10.000 rpm) per nodo SAP HANA.

> Questo calcolo è indipendente dallo storage controller e dallo shelf di dischi utilizzati, nonché dai requisiti di capacità del database. L'aggiunta di più shelf di dischi non aumenta la quantità massima di host SAP HANA supportati da uno storage controller.

Dischi a stato solido

Con gli SSD, il numero di dischi dati è determinato dal throughput della connessione SAS dai controller di storage allo shelf SSD.

Il numero massimo di host SAP HANA che possono essere eseguiti su un singolo shelf di dischi e il numero minimo di SSD richiesti per host SAP HANA sono stati determinati eseguendo il tool di test delle performance SAP. Questo test non prende in considerazione i requisiti effettivi di capacità dello storage degli host. Inoltre, è necessario calcolare i requisiti di capacità per determinare l'effettiva configurazione dello storage necessaria.

- Lo shelf di dischi SAS da 12 GB (DS224C) con 24 SSD supporta fino a 14 host SAP HANA quando lo shelf di dischi è collegato a 12 GB.
- Lo shelf di dischi SAS da 6 GB (DS2246) con 24 SSD supporta fino a 4 host SAP HANA.

Gli SSD e gli host SAP HANA devono essere equamente distribuiti tra entrambi i controller di storage.

La seguente tabella riassume il numero di host SAP HANA supportati per shelf di dischi.

	Shelf SAS da 6 GB (DS2246) con 24 SSD completamente caricati	**Shelf SAS da 12 GB (DS224C) con 24 SSD completamente caricati**
Numero massimo di host SAP HANA per shelf di dischi	4	14

> Questo calcolo è indipendente dal controller di storage utilizzato. L'aggiunta di più shelf di dischi non aumenta la quantità massima di host SAP HANA supportati da uno storage controller.

Carichi di lavoro misti

Sono supportati SAP HANA e altri carichi di lavoro applicativi eseguiti sullo stesso storage controller o nello stesso aggregato di storage. Tuttavia, è una Best practice di NetApp separare i workload SAP HANA da tutti gli altri workload delle applicazioni.

Potresti decidere di implementare workload SAP HANA e altri workload applicativi sullo stesso storage controller o sullo stesso aggregato. In tal caso, è necessario assicurarsi che le performance di SAP HANA siano adeguate all'interno dell'ambiente di workload misto. NetApp consiglia inoltre di utilizzare i parametri della qualità del servizio (QoS) per regolare l'effetto che queste altre applicazioni potrebbero avere e per garantire il throughput per le applicazioni SAP HANA.

Il tool di test delle performance SAP deve essere utilizzato per verificare se è possibile eseguire altri host SAP HANA su uno storage controller esistente già in uso per altri carichi di lavoro. I server applicativi SAP possono essere posizionati in modo sicuro sullo stesso storage controller e/o aggregato dei database SAP HANA.

Considerazioni sulla capacità

Una descrizione dettagliata dei requisiti di capacità per SAP HANA è disponibile nella "Nota SAP 1900823" white paper allegato.

> Il dimensionamento della capacità del panorama SAP complessivo con più sistemi SAP HANA deve essere determinato utilizzando gli strumenti di dimensionamento dello storage SAP HANA di NetApp. Contatta NetApp o il tuo partner commerciale NetApp per convalidare il processo di dimensionamento dello storage per un ambiente di storage di dimensioni adeguate.

Configurazione dello strumento di test delle performance

A partire da SAP HANA 1.0 SPS10, SAP ha introdotto i parametri per regolare il comportamento di i/o e ottimizzare il database per il file e il sistema storage utilizzati. Questi parametri devono essere impostati anche quando si esegue il test delle performance dello storage con lo strumento di test delle performance SAP.

NetApp ha condotto test delle performance per definire i valori ottimali. La seguente tabella elenca i parametri che devono essere impostati nel file di configurazione dello strumento di test delle prestazioni SAP.

Parametro	Valore
max_parallel_io_requests	128
async_read_submit	acceso
async_write_submit_active	acceso
async_write_submit_blocks	tutto

Per ulteriori informazioni sulla configurazione dello strumento di test SAP, vedere "Nota SAP 1943937" Per HWCCT (SAP HANA 1.0) e. "Nota SAP 2493172" PER HCMT/HCOT (SAP HANA 2.0).

Nell'esempio seguente viene illustrato come impostare le variabili per il piano di esecuzione HCMT/HCOT.

```
…{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
```

```
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
         "Name": "DataAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
```

```
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

Queste variabili devono essere utilizzate per la configurazione del test. Questo è solitamente il caso dei piani di esecuzione predefiniti che SAP offre con lo strumento HCMT/HCOT. Il seguente esempio per un test di scrittura del log 4k è da un piano di esecuzione.

```
…
      {
         "ID": "D664D001-933D-41DE-A904F304AEB67906",
         "Note": "File System Write Test",
         "ExecutionVariants": [
            {
               "ScaleOut": {
                  "Port": "${RemotePort}",
                  "Hosts": "${Hosts}",
                  "ConcurrentExecution": "${FSConcurrentExecution}"
               },
               "RepeatCount": "${TestRepeatCount}",
               "Description": "4K Block, Log Volume 5GB, Overwrite",
               "Hint": "Log",
               "InputVector": {
                  "BlockSize": 4096,
                  "DirectoryName": "${LogVolume}",
                  "FileOverwrite": true,
                  "FileSize": 5368709120,
                  "RandomAccess": false,
                  "RandomData": true,
                  "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                  "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                  "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                  "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                  "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                  "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                  "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                  "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                  "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
               }
            }, …
```

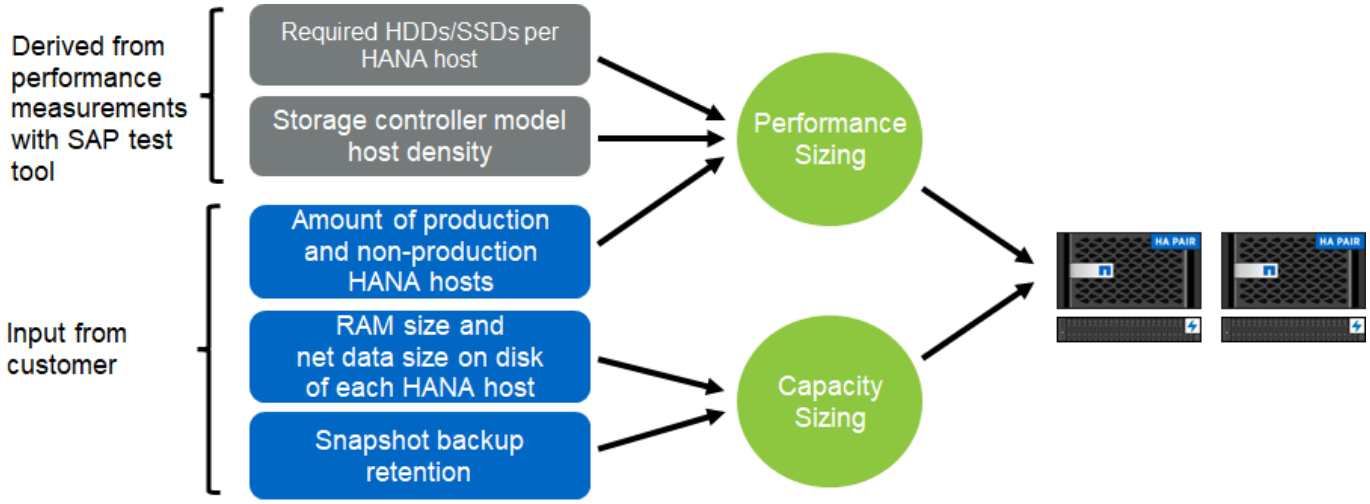
Panoramica del processo di dimensionamento dello storage

Il numero di dischi per host HANA e la densità host SAP HANA per ciascun modello di storage sono stati determinati con lo strumento di test delle performance SAP.

Il processo di dimensionamento richiede dettagli come il numero di host SAP HANA in produzione e non in produzione, la dimensione della RAM di ciascun host e la conservazione del backup delle copie Snapshot basate sullo storage. Il numero di host SAP HANA determina il controller dello storage e il numero di dischi necessari.

La dimensione della RAM, la dimensione dei dati netti sul disco di ciascun host SAP HANA e il periodo di conservazione del backup della copia Snapshot vengono utilizzati come input durante il dimensionamento della capacità.

La figura seguente riassume il processo di dimensionamento.



Installazione e configurazione dell'infrastruttura

Configurazione di rete

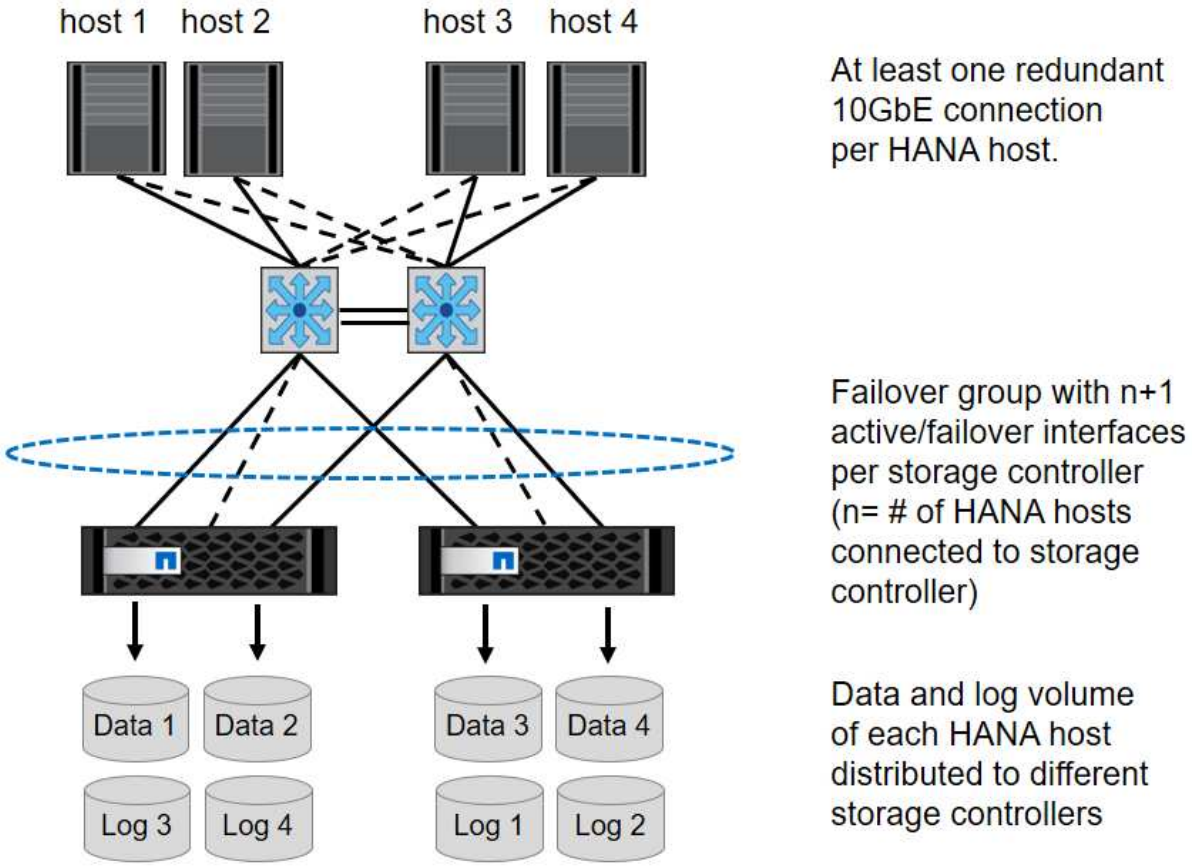
Per configurare la rete, attenersi alle seguenti indicazioni:

- Per collegare gli host SAP HANA ai controller di storage con una rete 10 GbE o superiore, è necessario utilizzare una rete storage dedicata.
- Utilizza la stessa velocità di connessione per i controller di storage e gli host SAP HANA. Se ciò non fosse possibile, assicurarsi che i componenti di rete tra i controller di storage e gli host SAP HANA siano in grado di gestire velocità diverse. Ad esempio, è necessario fornire spazio buffer sufficiente per consentire la negoziazione rapida a livello NFS tra storage e host. I componenti di rete sono in genere switch, ma devono essere presi in considerazione anche altri componenti all'interno dello chassis blade, ad esempio il backplane.
- Disattivare il controllo di flusso su tutte le porte fisiche utilizzate per il traffico dello storage sullo switch della rete di storage e sul layer host.
- Ogni host SAP HANA deve disporre di una connessione di rete ridondante con un minimo di 10 GB di larghezza di banda.
- I frame jumbo con una dimensione massima di unità di trasmissione (MTU) di 9,000 devono essere abilitati su tutti i componenti di rete tra gli host SAP HANA e i controller di storage.
- In una configurazione VMware, è necessario assegnare adattatori di rete VMXNET3 dedicati a ciascuna macchina virtuale in esecuzione. Per ulteriori requisiti, consultare i documenti indicati nella "Introduzione".
- Per evitare interferenze reciproche, utilizzare percorsi di rete/io separati per l'area di log e dati.

La figura seguente mostra un esempio con quattro host SAP HANA collegati a una coppia di ha controller storage che utilizza una rete 10 GbE. Ogni host SAP HANA dispone di una connessione Active-passive al fabric ridondante.

A livello di storage, quattro connessioni attive sono configurate per fornire un throughput di 10 GB per ciascun host SAP HANA. Inoltre, su ciascun controller di storage viene configurata un'interfaccia spare.

A livello di storage, viene configurato un dominio di broadcast con una dimensione MTU di 9000 e tutte le interfacce fisiche richieste vengono aggiunte a questo dominio di broadcast. Questo approccio assegna automaticamente queste interfacce fisiche allo stesso gruppo di failover. Tutte le interfacce logiche (LIF) assegnate a queste interfacce fisiche vengono aggiunte a questo gruppo di failover.



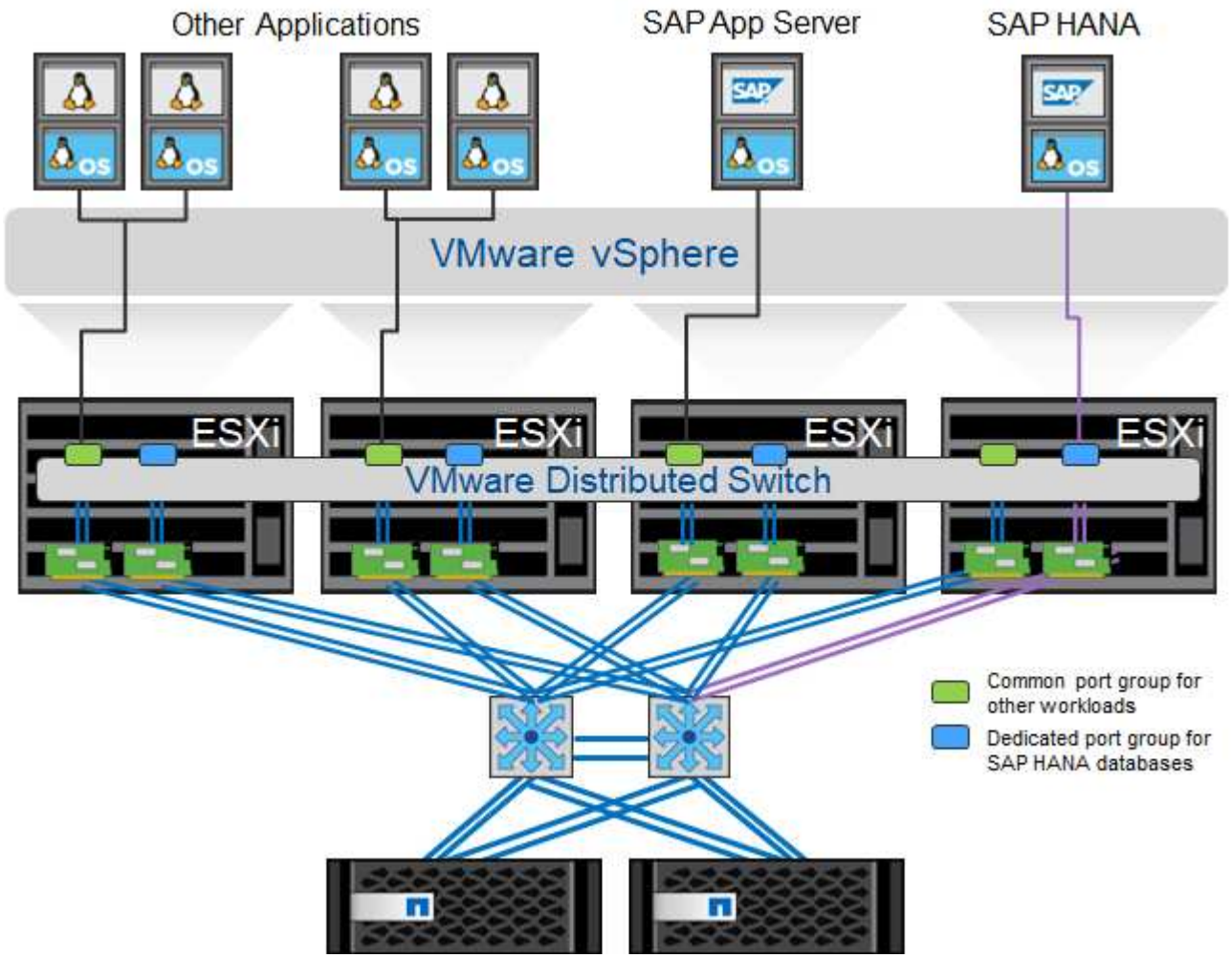
In generale, è anche possibile utilizzare gruppi di interfacce ha sui server (bonds) e sui sistemi storage (ad esempio, link Aggregation Control Protocol [LACP] e ifgroup). Con i gruppi di interfacce ha, verificare che il carico sia equamente distribuito tra tutte le interfacce all'interno del gruppo. La distribuzione del carico dipende dalla funzionalità dell'infrastruttura dello switch di rete.

A seconda del numero di host SAP HANA e della velocità di connessione utilizzata, sono necessari diversi numeri di porte fisiche attive.

Configurazione di rete specifica di VMware

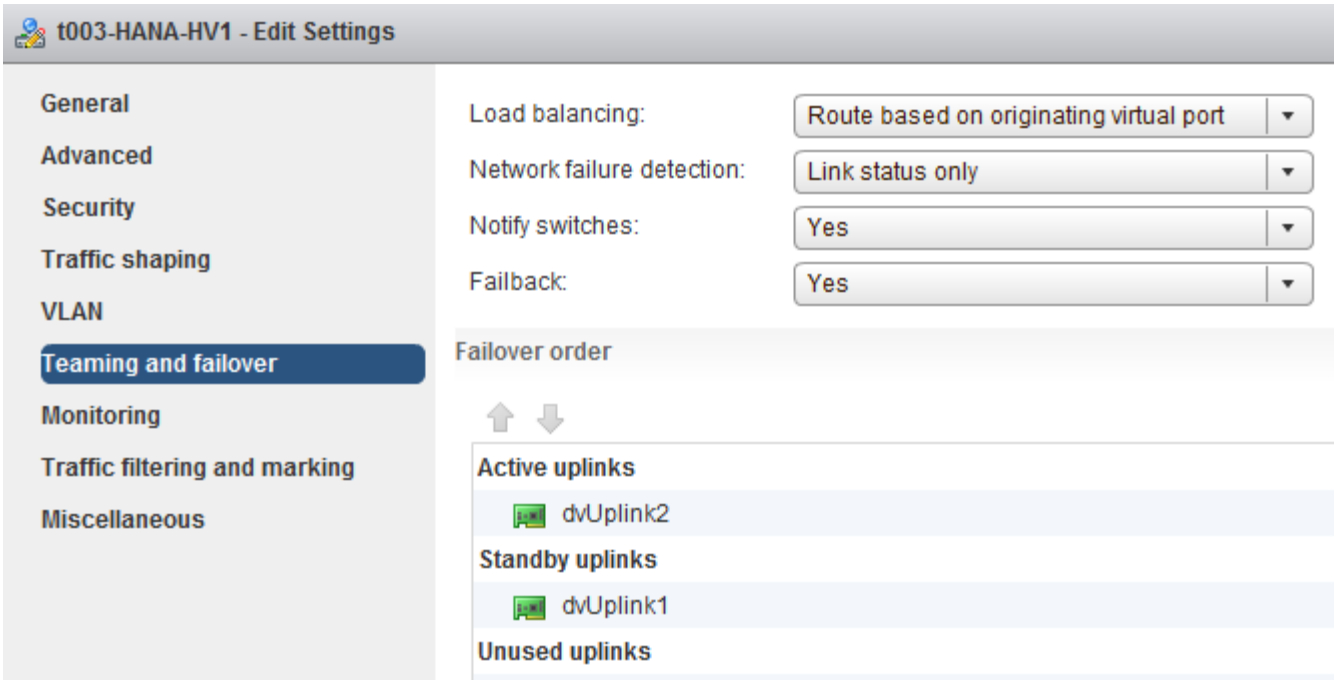
Poiché tutti i dati per le istanze SAP HANA, inclusi i dati critici per le performance e i volumi di log per il database, vengono forniti tramite NFS in questa soluzione, la progettazione e la configurazione di rete corrette sono fondamentali. Una rete storage dedicata viene utilizzata per separare il traffico NFS dal traffico di comunicazione e accesso utente tra i nodi SAP HANA. Ogni nodo SAP HANA richiede una connessione di rete dedicata ridondante con un minimo di 10 GB di larghezza di banda. È supportata anche una maggiore larghezza di banda. Questa rete deve estendersi end-to-end dal livello di storage attraverso lo switching e il calcolo della rete fino al sistema operativo guest ospitato su VMware vSphere. Oltre all'infrastruttura di switching fisica, viene utilizzato uno switch distribuito VMware (VDS) per fornire performance e gestibilità adeguate del traffico di rete a livello di hypervisor.

La figura seguente fornisce una panoramica della rete.



Ogni nodo SAP HANA utilizza un gruppo di porte dedicato sullo switch distribuito VMware. Questo gruppo di porte consente di migliorare la qualità del servizio (QoS) e l'assegnazione dedicata delle schede di interfaccia di rete fisiche (NIC) sugli host ESX. Per utilizzare NIC fisiche dedicate preservando le funzionalità ha in caso di guasto alla NIC, la NIC fisica dedicata viene configurata come uplink attivo. Le schede di rete aggiuntive sono configurate come uplink in standby nelle impostazioni di teaming e failover del gruppo di porte SAP HANA. Inoltre, i jumbo frame (MTU 9,000) devono essere abilitati end-to-end sugli switch fisici e virtuali. Inoltre, disattivare il controllo di flusso su tutte le porte ethernet utilizzate per il traffico dello storage su server, switch e sistemi storage. La figura seguente mostra un esempio di tale configurazione.

LRO (Large receive offload) deve essere disattivato per le interfacce utilizzate per il traffico NFS. Per tutte le altre linee guida sulla configurazione di rete, consultare le rispettive guide alle Best practice VMware per SAP HANA.



Sincronizzazione dell'ora

È necessario sincronizzare l'ora tra i controller di storage e gli host del database SAP HANA. A tale scopo, impostare lo stesso server di riferimento orario per tutti i controller di storage e tutti gli host SAP HANA.

Configurazione dello storage controller

Questa sezione descrive la configurazione del sistema storage NetApp. È necessario completare l'installazione e la configurazione primaria in base alle corrispondenti guide di configurazione e configurazione di ONTAP.

Efficienza dello storage

La deduplica inline, la deduplica inline di più volumi, la compressione inline e la compaction inline sono supportate con SAP HANA in una configurazione SSD.

L'abilitazione delle funzionalità di efficienza dello storage in una configurazione basata su HDD non è supportata.

Volumi NetApp FlexGroup

L'utilizzo dei volumi NetApp FlexGroup non è supportato per SAP HANA. Grazie all'architettura di SAP HANA l'utilizzo di FlexGroup Volumes non fornisce alcun beneficio e potrebbe causare problemi di performance.

Crittografia dei volumi e degli aggregati NetApp

L'utilizzo di NetApp Volume Encryption (NVE) e NetApp aggregate Encryption (NAE) sono supportati con SAP HANA.

Qualità del servizio

La QoS può essere utilizzata per limitare il throughput dello storage per specifici sistemi SAP HANA o altre applicazioni su un controller condiviso. Un caso d'utilizzo sarebbe quello di limitare il throughput dei sistemi di sviluppo e test in modo che non possano influenzare i sistemi di produzione in una configurazione mista.

Durante il processo di dimensionamento, è necessario determinare i requisiti di performance di un sistema non in produzione. I sistemi di sviluppo e test possono essere dimensionati con valori di performance inferiori, in genere nell'intervallo compreso tra il 20% e il 50% di un KPI del sistema di produzione come definito da SAP.

A partire da ONTAP 9, la qualità del servizio viene configurata a livello di volume di storage e utilizza i valori massimi per il throughput (Mbps) e la quantità di i/o (IOPS).

L'i/o di scrittura di grandi dimensioni ha il maggiore effetto sulle performance del sistema storage. Pertanto, il limite di throughput QoS deve essere impostato su una percentuale dei corrispondenti valori KPI di scrittura delle performance dello storage SAP HANA nei volumi di dati e di log.

NetApp FabricPool

La tecnologia NetApp FabricPool non deve essere utilizzata per i file system primari attivi nei sistemi SAP HANA. Sono inclusi i file system per l'area dei dati e dei log, oltre a `/hana/shared` file system. In questo modo si ottengono performance imprevedibili, in particolare durante l'avvio di un sistema SAP HANA.

È possibile utilizzare la policy di tiering "snapshot-only" e FabricPool in generale in una destinazione di backup come una destinazione SnapVault o SnapMirror.

> ⓘ L'utilizzo di FabricPool per tiering delle copie Snapshot nello storage primario o l'utilizzo di FabricPool in una destinazione di backup modifica il tempo necessario per il ripristino e il ripristino di un database o di altre attività, come la creazione di cloni di sistema o la riparazione di sistemi. Prendere in considerazione questo aspetto per pianificare la strategia di gestione del ciclo di vita generale e verificare che gli SLA vengano ancora rispettati durante l'utilizzo di questa funzione.

FabricPool è un'ottima opzione per spostare i backup dei log in un altro Tier di storage. Lo spostamento dei backup influisce sul tempo necessario per ripristinare un database SAP HANA. Pertanto, l'opzione "tiering-minimum-cooling-days" deve essere impostata su un valore che colloca i backup dei log, normalmente necessari per il recovery, sul Tier di storage veloce locale.

Configurazione dello storage

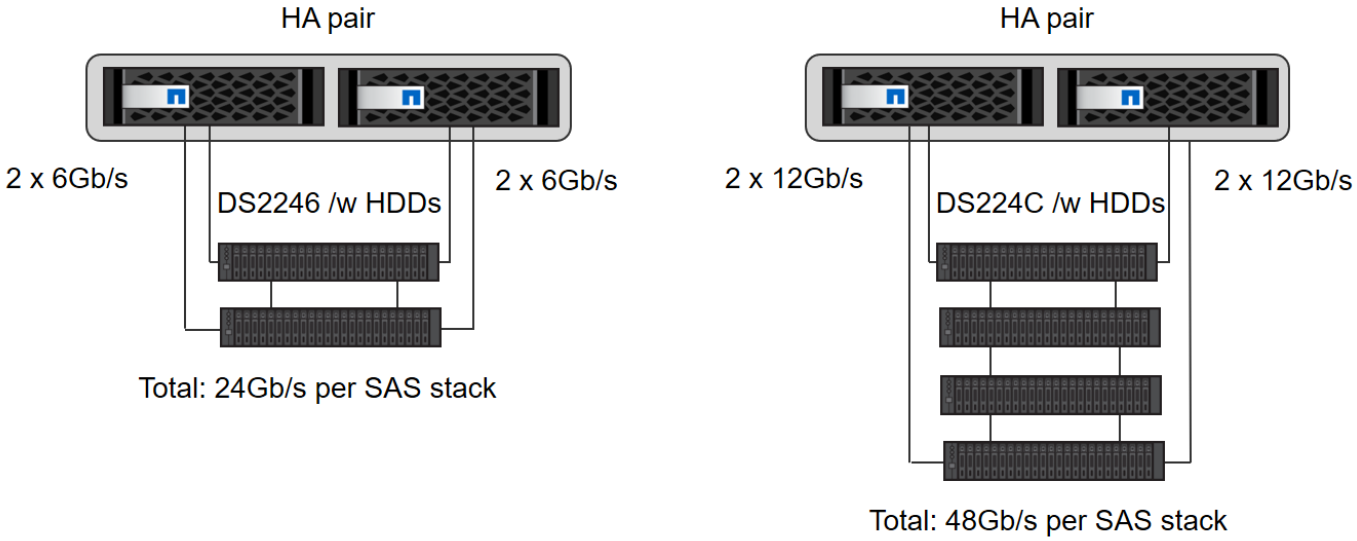
La seguente panoramica riassume i passaggi necessari per la configurazione dello storage. Ogni fase viene descritta in dettaglio nelle sezioni successive. In questa sezione, si presuppone che l'hardware di storage sia configurato e che il software ONTAP sia già installato. Inoltre, le connessioni tra le porte di storage (10 GbE o superiori) e la rete devono essere già in uso.

1. Verificare la corretta configurazione dello stack SAS come descritto in "Connessione a shelf di dischi."
2. Creare e configurare gli aggregati necessari come descritto in "Configurazione dell'aggregato."
3. Creare una Storage Virtual Machine (SVM) come descritto in "Configurazione della macchina virtuale per lo storage."
4. Creare LIF come descritto in "Configurazione dell'interfaccia logica."
5. Creare volumi all'interno degli aggregati come descritto in "Configurazione dei volumi per sistemi SAP HANA a host singolo" e. "Configurazione dei volumi per sistemi SAP HANA con host multipli."

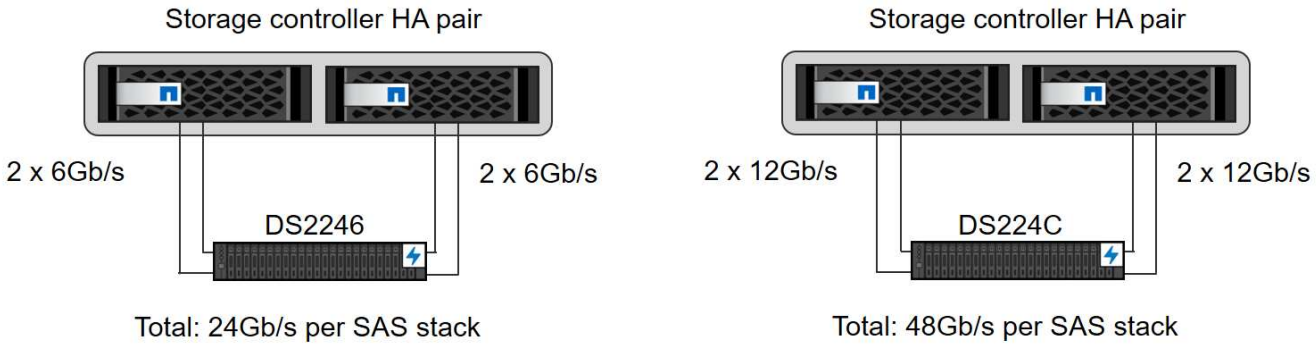
6. Impostare le opzioni di volume richieste come descritto in "Opzioni del volume."
7. Impostare le opzioni richieste per NFSv3 come descritto in "Configurazione NFS per NFSv3" o per NFSv4 come descritto in "Configurazione NFS per NFSv4."
8. Montare i volumi nello spazio dei nomi e impostare le policy di esportazione come descritto in "Montare i volumi nello spazio dei nomi e impostare i criteri di esportazione."

Connessione a shelf di dischi

Con gli HDD, è possibile collegare un massimo di due shelf di dischi DS2246 o quattro shelf di dischi DS224C a uno stack SAS per fornire le prestazioni richieste per gli host SAP HANA, come mostrato nella figura seguente. I dischi all'interno di ogni shelf devono essere distribuiti in modo uguale a entrambi i controller della coppia ha.

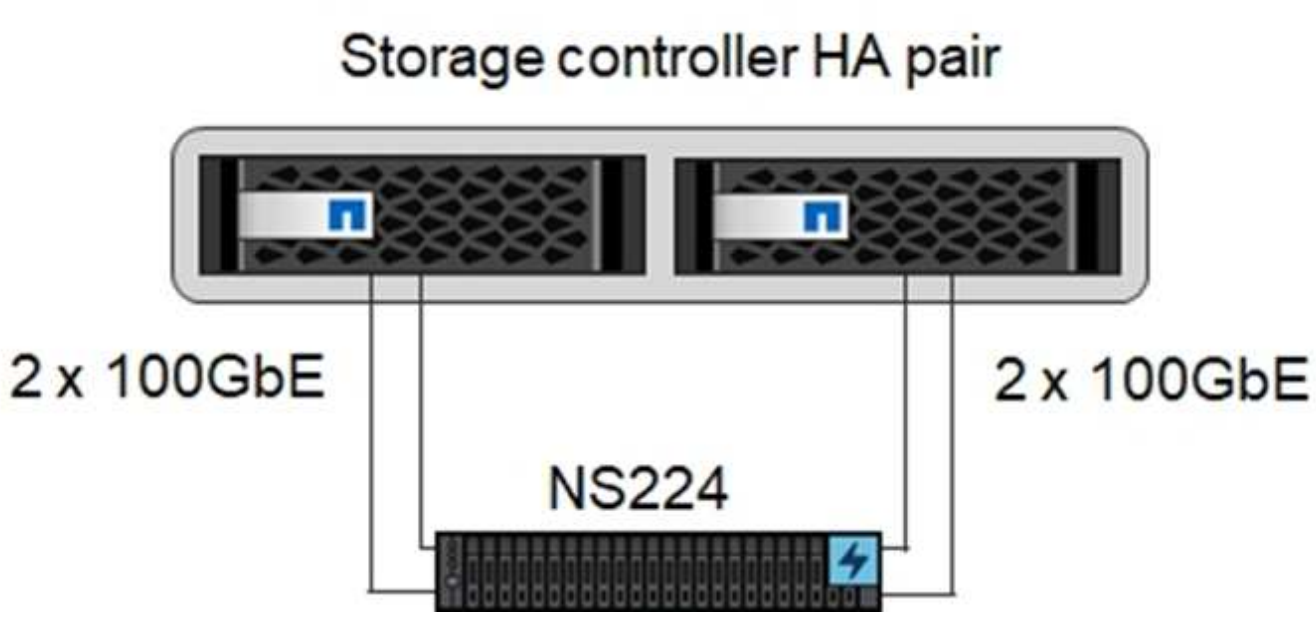


Con gli SSD, è possibile collegare un massimo di uno shelf di dischi a uno stack SAS per fornire le prestazioni richieste per gli host SAP HANA, come mostrato nella figura seguente. I dischi all'interno di ogni shelf devono essere distribuiti in modo uguale a entrambi i controller della coppia ha. Con lo shelf di dischi DS224C, è possibile utilizzare anche il cablaggio SAS quad-path, ma non è necessario.



Shelf di dischi NVMe (100 GbE)

Ogni shelf di dischi NS224 NVMe è collegato a due porte 100GbE per controller, come illustrato nella figura seguente. I dischi all'interno di ogni shelf devono essere distribuiti in modo uguale a entrambi i controller della coppia ha.

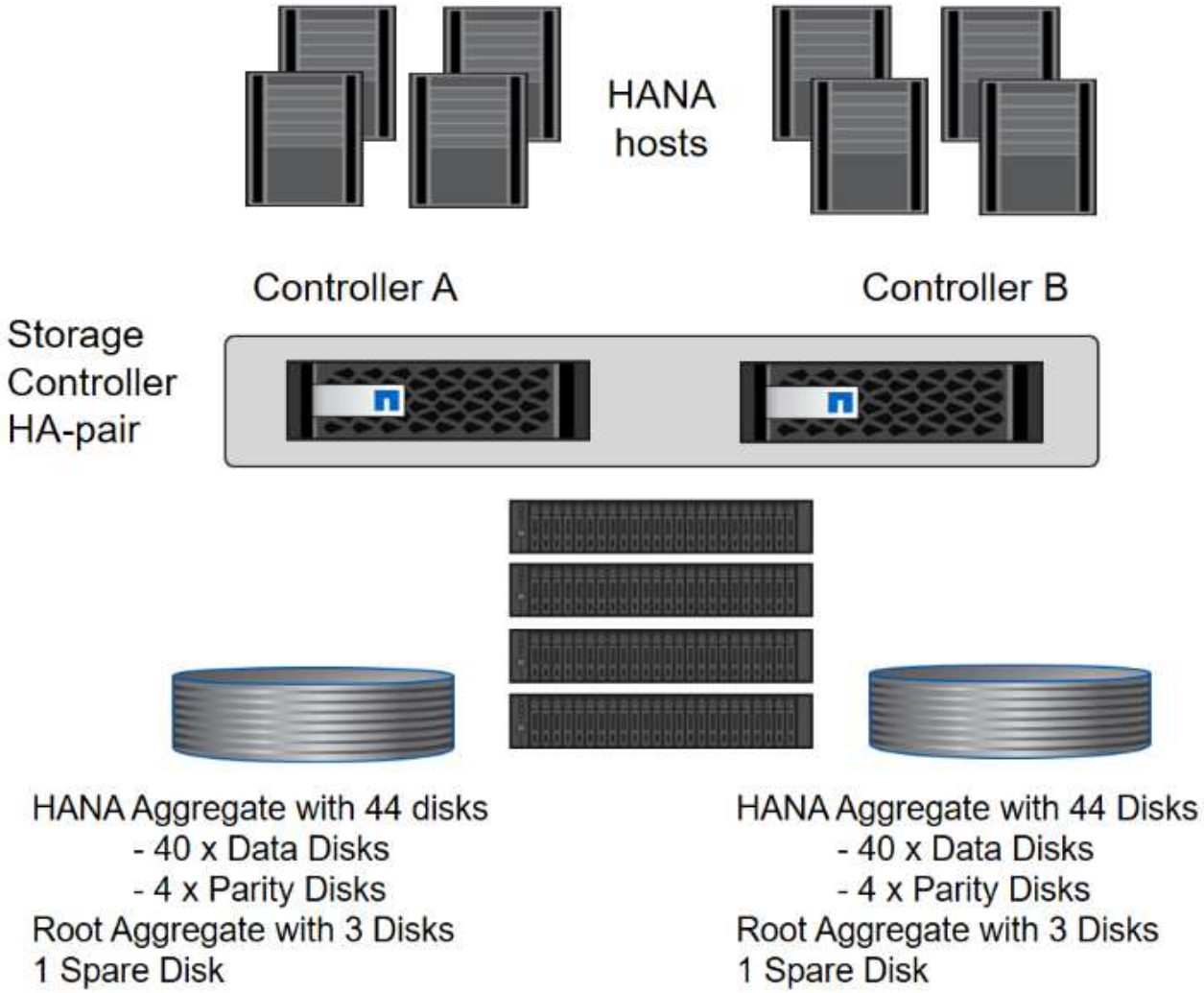


Configurazione dell'aggregato

In generale, è necessario configurare due aggregati per controller, indipendentemente dallo shelf di dischi o dalla tecnologia dei dischi (SSD o HDD) utilizzata. Per i sistemi della serie FAS2000, è sufficiente un aggregato di dati.

Configurazione aggregata con HDD

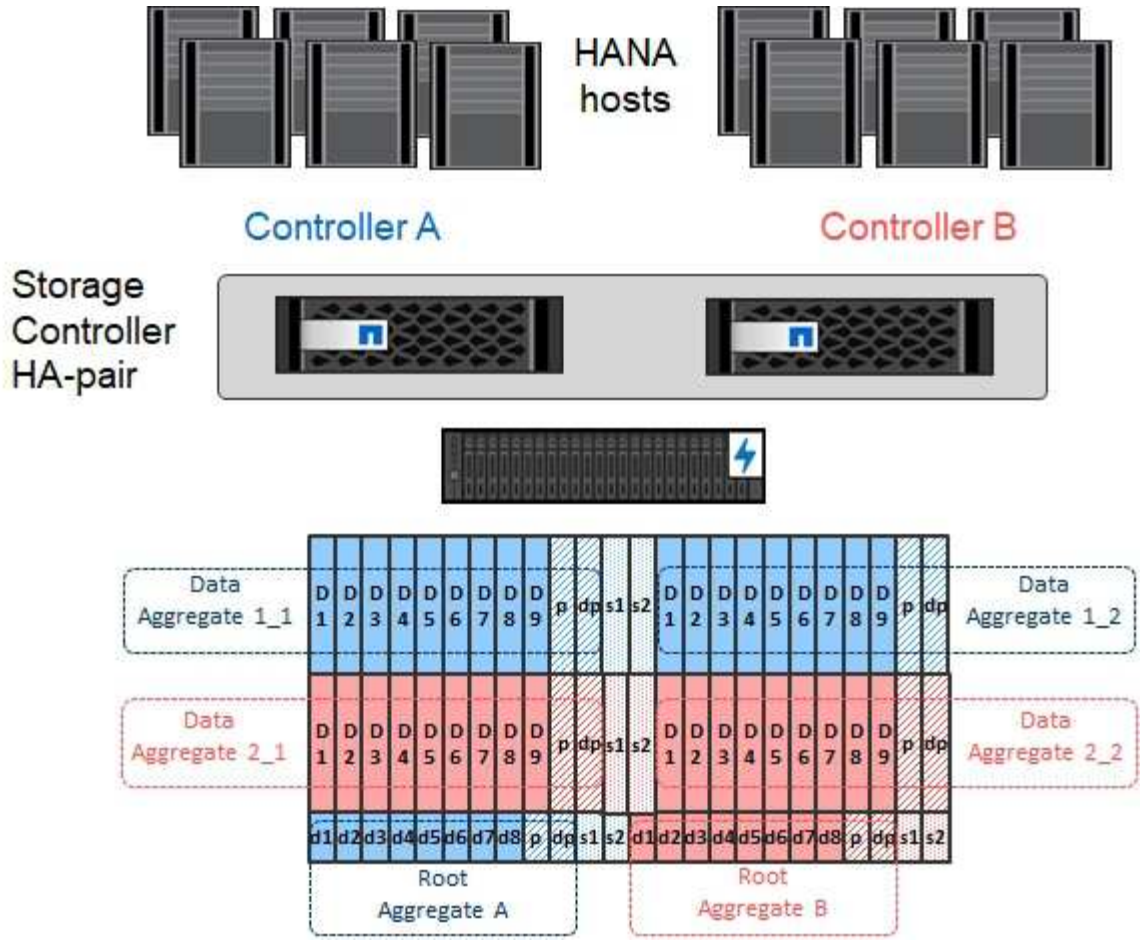
La figura seguente mostra una configurazione per otto host SAP HANA. Quattro host SAP HANA sono collegati a ciascun controller di storage. Vengono configurati due aggregati separati, uno per ciascun controller di storage. Ogni aggregato è configurato con 4 × 10 = 40 dischi dati (HDD).



Configurazione aggregata con sistemi solo SDD

In generale, è necessario configurare due aggregati per controller, indipendentemente da quale shelf di dischi o tecnologia di dischi (SSD o HDD) viene utilizzata. Per i sistemi della serie FAS2000, è sufficiente un aggregato di dati.

La figura seguente mostra una configurazione di 12 host SAP HANA in esecuzione su uno shelf SAS da 12 GB configurato con ADPv2. Sei host SAP HANA sono collegati a ciascun controller di storage. Sono configurati quattro aggregati separati, due per ogni controller di storage. Ogni aggregato è configurato con 11 dischi con nove partizioni di dati e due di dischi di parità. Per ciascun controller sono disponibili due partizioni di riserva.



Configurazione della macchina virtuale per lo storage

Diversi ambienti SAP con database SAP HANA possono utilizzare una singola SVM. È possibile assegnare una SVM a ciascun ambiente SAP, se necessario, nel caso in cui sia gestita da diversi team all'interno di un'azienda.

Se un profilo QoS è stato creato e assegnato automaticamente durante la creazione di una nuova SVM, rimuovere il profilo creato automaticamente dalla SVM per fornire le prestazioni richieste per SAP HANA:

```
vserver modify -vserver <svm-name> -qos-policy-group none
```

Configurazione dell'interfaccia logica

Per i sistemi di produzione SAP HANA, è necessario utilizzare diversi LIF per montare il volume di dati e il volume di log dall'host SAP HANA. Pertanto, sono necessari almeno due LIF.

I montaggi di volumi di dati e log di diversi host SAP HANA possono condividere una porta di rete dello storage fisico utilizzando gli stessi LIF o utilizzando singoli LIF per ogni montaggio.

Il numero massimo di montaggi di volumi di dati e log per interfaccia fisica è indicato nella seguente tabella.

Velocità della porta Ethernet	10 GbE	25 GbE	40 GbE	100GeE
Numero massimo di montaggi di volumi di log o dati per porta fisica	3	8	12	30

La condivisione di una LIF tra diversi host SAP HANA potrebbe richiedere un remount di volumi di dati o log in un LIF diverso. Questa modifica consente di evitare penalizzazioni delle performance se un volume viene spostato in un controller di storage diverso.

I sistemi di sviluppo e test possono utilizzare più dati e volumi o LIF su un'interfaccia di rete fisica.

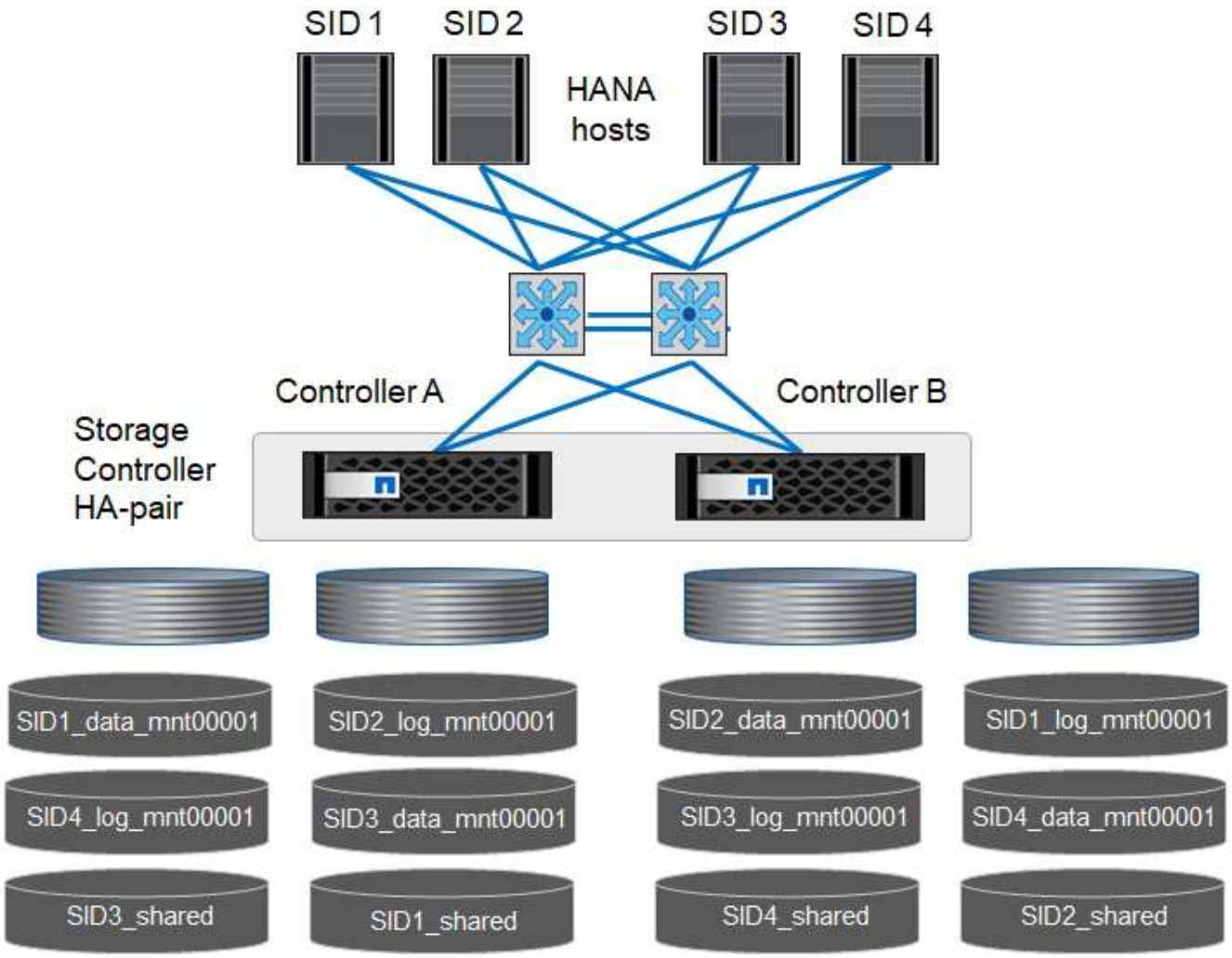
Per i sistemi di produzione, sviluppo e test, il `/hana/shared` Il file system può utilizzare la stessa LIF del volume di dati o di log.

Configurazione dei volumi per sistemi SAP HANA a host singolo

La figura seguente mostra la configurazione dei volumi di quattro sistemi SAP HANA a host singolo. I volumi di dati e log di ciascun sistema SAP HANA vengono distribuiti a diversi storage controller. Ad esempio, volume `SID1_data_mnt00001` È configurato sul controller A e sul volume `SID1_log_mnt00001` È configurato sul controller B.

Se per i sistemi SAP HANA viene utilizzato un solo storage controller di una coppia ha, è possibile memorizzare dati e volumi di log nello stesso storage controller.

Se i dati e i volumi di log sono memorizzati sullo stesso controller, l'accesso dal server allo storage deve essere eseguito con due LIF differenti: Una LIF per accedere al volume di dati e una per accedere al volume di log.



Per ogni host SAP HANA DB, un volume di dati, un volume di log e un volume per `/hana/shared` sono configurati. La seguente tabella mostra un esempio di configurazione per i sistemi SAP HANA a host singolo.

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller b
Dati, log e volumi condivisi per il sistema SID1	Volume di dati: SID1_data_mnt00001	Volume condiviso: SID1_shared	–	Volume di log: SID1_log_mnt00001
Dati, log e volumi condivisi per il sistema SID2	–	Volume di log: SID2_log_mnt00001	Volume di dati: SID2_data_mnt00001	Volume condiviso: SID2_shared
Dati, log e volumi condivisi per il sistema SID3	Volume condiviso: SID3_shared	Volume di dati: SID3_data_mnt00001	Volume di log: SID3_log_mnt00001	–
Dati, log e volumi condivisi per il sistema SID4	Volume di log: SID4_log_mnt00001	–	Volume condiviso: SID4_shared	Volume di dati: SID4_data_mnt00001

La seguente tabella mostra un esempio di configurazione del punto di montaggio per un sistema a host singolo. Per inserire la home directory di `sidadm` sullo storage centrale, il `/usr/sap/SID` il file system deve

essere montato da `SID_shared` volume.

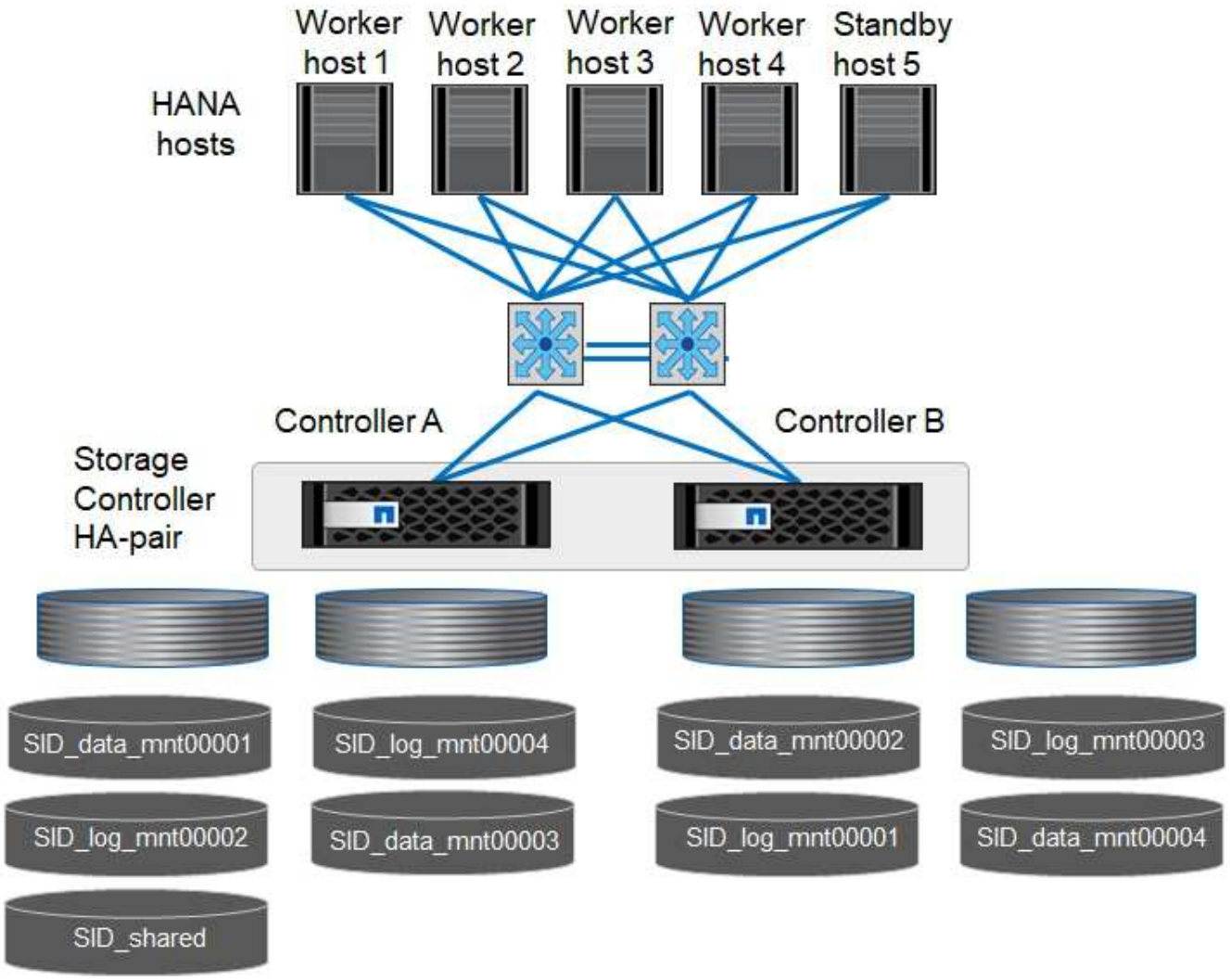
Percorso di giunzione	Directory	Punto di montaggio sull'host HANA
SID_data_mnt00001	–	/hana/data/SID/mnt00001
SID_log_mnt00001	–	/hana/log/SID/mnt00001
SID_shared	usr-sap condiviso	/Usr/sap/SID /hana/shared

Configurazione dei volumi per sistemi SAP HANA con host multipli

La figura seguente mostra la configurazione del volume di un sistema SAP HANA 4+1. I volumi di dati e log di ciascun host SAP HANA vengono distribuiti a diversi storage controller. Ad esempio, volume `SID1_data1_mnt00001` È configurato sul controller A e sul volume `SID1_log1_mnt00001` È configurato sul controller B.

Se per il sistema SAP HANA viene utilizzato un solo storage controller di una coppia ha, i volumi di dati e log possono essere memorizzati anche sullo stesso storage controller.

Se i dati e i volumi di log sono memorizzati sullo stesso controller, l'accesso dal server allo storage deve essere eseguito con due diversi LIF: Uno per accedere al volume di dati e uno per accedere al volume di log.



Per ogni host SAP HANA, vengono creati un volume di dati e un volume di log. Il `/hana/shared` Il volume viene utilizzato da tutti gli host del sistema SAP HANA. La seguente tabella mostra un esempio di configurazione per un sistema SAP HANA con host multipli con quattro host attivi.

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Volumi di dati e log per il nodo 1	Volume di dati: SID_data_mnt00001	–	Volume di log: SID_log_mnt00001	–
Volumi di dati e log per il nodo 2	Volume di log: SID_log_mnt00002	–	Volume di dati: SID_data_mnt00002	–
Volumi di dati e log per il nodo 3	–	Volume di dati: SID_data_mnt00003	–	Volume di log: SID_log_mnt00003
Volumi di dati e log per il nodo 4	–	Volume di log: SID_log_mnt00004	–	Volume di dati: SID_data_mnt00004
Volume condiviso per tutti gli host	Volume condiviso: SID_shared	–	–	–

La seguente tabella mostra la configurazione e i punti di montaggio di un sistema a più host con quattro host SAP HANA attivi. Per inserire le home directory di `sidadm` utente di ciascun host sullo storage centrale, il

`/usr/sap/SID` i file system vengono montati da `SID_shared` volume.

Percorso di giunzione	Directory	Punto di montaggio sull'host SAP HANA	Nota
SID_data_mnt00001	–	/hana/data/SID/mnt00001	Montato su tutti gli host
SID_log_mnt00001	–	/hana/log/SID/mnt00001	Montato su tutti gli host
SID_data_mnt00002	–	/hana/data/SID/mnt00002	Montato su tutti gli host
SID_log_mnt00002	–	/hana/log/SID/mnt00002	Montato su tutti gli host
SID_data_mnt00003	–	/hana/data/SID/mnt00003	Montato su tutti gli host
SID_log_mnt00003	–	/hana/log/SID/mnt00003	Montato su tutti gli host
SID_data_mnt00004	–	/hana/data/SID/mnt00004	Montato su tutti gli host
SID_log_mnt00004	–	/hana/log/SID/mnt00004	Montato su tutti gli host
SID_shared	condiviso	/hana/shared/	Montato su tutti gli host
SID_shared	usr-sap-host1	/Usr/sap/SID	Montato sull'host 1
SID_shared	usr-sap-host2	/Usr/sap/SID	Montato sull'host 2
SID_shared	usr-sap-host3	/Usr/sap/SID	Montato sull'host 3
SID_shared	usr-sap-host4	/Usr/sap/SID	Montato sull'host 4
SID_shared	usr-sap-host5	/Usr/sap/SID	Montato sull'host 5

Opzioni del volume

È necessario verificare e impostare le opzioni del volume elencate nella tabella seguente su tutte le SVM. Per alcuni comandi, è necessario passare alla modalità avanzata dei privilegi in ONTAP.

Azione	Comando
Disattiva la visibilità della directory Snapshot	vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false
Disattivare le copie Snapshot automatiche	vol modify –vserver <vserver-name> -volume <volname> -snapshot-policy none
Disattiva l'aggiornamento del tempo di accesso ad eccezione del volume SID_shared	set advanced vol modify -vserver <vserver-name> -volume <volname> -atime-update false set admin

Configurazione NFS per NFSv3

Le opzioni NFS elencate nella seguente tabella devono essere verificate e impostate su tutti i controller di storage.

Per alcuni dei comandi mostrati, è necessario passare alla modalità avanzata dei privilegi in ONTAP.

Azione	Comando
Abilitare NFSv3	nfs modify -vserver <vserver-name> v3.0 abilitato

Azione	Comando
Impostare la dimensione massima di trasferimento TCP NFS su 1MB	set advanced nfs modify -vserver <vserver_name> -tcp-max-xfer-size 1048576 set admin

In ambienti condivisi con carichi di lavoro diversi, impostare le dimensioni massime di trasferimento TCP NFS su 262144

Configurazione NFS per NFSv4

Le opzioni NFS elencate nella seguente tabella devono essere verificate e impostate su tutte le SVM.

Per alcuni comandi, è necessario passare alla modalità avanzata dei privilegi in ONTAP.

Azione	Comando
Abilitare NFSv4	nfs modify -vserver <vserver-name> -v4.1 abilitato
Impostare la dimensione massima di trasferimento TCP NFS su 1MB	set advanced nfs modify -vserver <vserver_name> -tcp-max-xfer-size 1048576 set admin
Disattiva gli elenchi di controllo di accesso (ACL) NFSv4	nfs modify -vserver <vserver_name> -v4.1-acl disabled
Impostare l'ID di dominio NFSv4	nfs modify -vserver <vserver_name> -v4-id-domain <domain-name>
Disattiva la delega di lettura NFSv4	nfs modify -vserver <vserver_name> -v4.1-read -delegation disabled
Disattiva la delega di scrittura NFSv4	nfs modify -vserver <vserver_name> -v4.1-write -delegation disabled
Disattiva id numerici NFSv4	nfs modify -vserver <vserver_name> -v4-numeric-ids disabled
Modificare la quantità di slot di sessione NFSv4.x opzionale	imposta avanzate nfs modify -vserver hana -v4.x-session-num-slot <value> impostare admin

In ambienti condivisi con carichi di lavoro diversi, impostare le dimensioni massime di trasferimento TCP NFS su 262144

La disattivazione degli id numerici richiede la gestione degli utenti come descritto in "Preparazione dell'installazione di SAP HANA per NFSv4."

L'ID del dominio NFSv4 deve essere impostato sullo stesso valore su tutti i server Linux (`/etc/idmapd.conf`) e le SVM, come descritto in "Preparazione dell'installazione di SAP HANA per NFSv4."

PNFS può essere attivato ed utilizzato.

Se si utilizzano sistemi SAP HANA a host multipli con failover automatico dell'host, è necessario regolare i

parametri di failover all'interno di `nameserver.ini` come mostrato nella tabella seguente. Mantenere l'intervallo di tentativi predefinito di 10 secondi all'interno di queste sezioni.

Sezione all'interno di nameserver.ini	Parametro	Valore
failover	normal_rettry	9
distributed_watchdog	dischase_retretres	11
distributed_watchdog	takeover_retries	9

Montare i volumi nello spazio dei nomi e impostare i criteri di esportazione

Quando viene creato un volume, il volume deve essere montato nello spazio dei nomi. In questo documento, si presuppone che il nome del percorso di giunzione sia lo stesso del nome del volume. Per impostazione predefinita, il volume viene esportato con il criterio predefinito. Se necessario, è possibile adattare la policy di esportazione.

Configurazione dell'host

Tutti i passaggi descritti in questa sezione sono validi per gli ambienti SAP HANA su server fisici e per SAP HANA in esecuzione su VMware vSphere.

Parametro di configurazione per SUSE Linux Enterprise Server

I parametri aggiuntivi di kernel e configurazione di ciascun host SAP HANA devono essere regolati in base al carico di lavoro generato da SAP HANA.

SUSE Linux Enterprise Server 12 e 15

A partire da SUSE Linux Enterprise Server (SLES) 12 SP1, il parametro kernel deve essere impostato in un file di configurazione in `/etc/sysctl.d` directory. Ad esempio, un file di configurazione con il nome `91-NetApp-HANA.conf` deve essere creato.

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384 16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle = 0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_max_slot_table_entries = 128
```

Saptune, incluso in SLES per le versioni di SAP OS, può essere utilizzato per impostare questi valori. Vedere "Nota SAP 3024346" (Richiede l'accesso SAP).

Parametro di configurazione per Red Hat Enterprise Linux 7.2 o versioni successive

È necessario regolare altri parametri di kernel e configurazione in ogni host SAP HANA per il carico di lavoro generato da SAP HANA.

A partire da Red Hat Enterprise Linux 7.2, è necessario impostare i parametri del kernel in un file di configurazione in `/etc/sysctl.d` directory. Ad esempio, un file di configurazione con il nome `91-NetApp-HANA.conf` deve essere creato.

```
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_rmem = 4096 131072 16777216
net.ipv4.tcp_wmem = 4096 16384  16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_slow_start_after_idle = 0
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_max_slot_table_entries = 128
```

A partire dalla versione 8.6 di RedHat Enterprise Linux, queste impostazioni possono essere applicate anche utilizzando RHEL System Roles for SAP (Ansible). Vedere "Nota SAP 3024346" (Richiede l'accesso SAP).

Creare sottodirectory in /hana/volume condiviso

Gli esempi mostrano un database SAP HANA con SID=NF2.

Per creare le sottodirectory richieste, eseguire una delle seguenti operazioni:

- Per un sistema a host singolo, montare `/hana/shared` e creare il `shared` e. `usr-sap` sottodirectory.

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap
sapcc-hana-tst-06:mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

- Per un sistema a più host, montare `/hana/shared` e creare il `shared` e a. `usr-sap` sottodirectory per ciascun host.

  I comandi di esempio mostrano un sistema HANA 2+1 multi-host.

```
sapcc-hana-tst-06:/mnt # mount <storage-hostname>:/NF2_shared /mnt/tmp
sapcc-hana-tst-06:/mnt # cd /mnt/tmp
sapcc-hana-tst-06:/mnt/tmp # mkdir shared
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host1
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host2
sapcc-hana-tst-06:/mnt/tmp # mkdir usr-sap-host3
sapcc-hana-tst-06:/mnt/tmp # cd ..
sapcc-hana-tst-06:/mnt # umount /mnt/tmp
```

Creare punti di montaggio

Gli esempi mostrano un database SAP HANA con SID=NF2.

Per creare le directory dei punti di montaggio richieste, eseguire una delle seguenti operazioni:

- Per un sistema a host singolo, creare punti di montaggio e impostare le autorizzazioni sull'host del database.

```
sapcc-hana-tst-06:/ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:/ # mkdir -p /hana/shared
sapcc-hana-tst-06:/ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-06:/ # chmod –R 777 /hana/log/NF2
sapcc-hana-tst-06:/ # chmod –R 777 /hana/data/NF2
sapcc-hana-tst-06:/ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:/ # chmod -R 777 /usr/sap/NF2
```

- Per un sistema a più host, creare punti di montaggio e impostare le autorizzazioni su tutti gli host worker e standby.

  I seguenti comandi di esempio si riferiscono a un sistema HANA con host multiplo 2+1.

  - Primo host di lavoro:

```
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-06:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-06:~ # mkdir -p /hana/shared
sapcc-hana-tst-06:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-06:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-06:~ # chmod -R 777 /usr/sap/NF2
```

- Secondo host di lavoro:

```
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-07:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-07:~ # mkdir -p /hana/shared
sapcc-hana-tst-07:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-07:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-07:~ # chmod -R 777 /usr/sap/NF2
```

- Host in standby:

```
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/data/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00001
sapcc-hana-tst-08:~ # mkdir -p /hana/log/NF2/mnt00002
sapcc-hana-tst-08:~ # mkdir -p /hana/shared
sapcc-hana-tst-08:~ # mkdir -p /usr/sap/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/log/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/data/NF2
sapcc-hana-tst-08:~ # chmod -R 777 /hana/shared
sapcc-hana-tst-08:~ # chmod -R 777 /usr/sap/NF2
```

Montare i file system

A seconda della versione di NFS e della release di ONTAP, vengono utilizzate diverse opzioni di montaggio. I seguenti file system devono essere montati sugli host:

- `/hana/data/SID/mnt0000*`
- `/hana/log/SID/mnt0000*`
- `/hana/shared`
- `/usr/sap/SID`

La seguente tabella mostra le versioni di NFS che devono essere utilizzate per i diversi file system per i database SAP HANA a host singolo e multiplo.

File system	Host singolo SAP HANA	SAP HANA host multipli
/hana/data/SID/mnt0000*	NFSv3 o NFSv4	NFSv4
/hana/log/SID/mnt0000*	NFSv3 o NFSv4	NFSv4
/hana/shared	NFSv3 o NFSv4	NFSv3 o NFSv4

File system	Host singolo SAP HANA	SAP HANA host multipli
/Usr/sap/SID	NFSv3 o NFSv4	NFSv3 o NFSv4

La seguente tabella mostra le opzioni di montaggio per le varie versioni di NFS e le release di ONTAP. I parametri comuni sono indipendenti dalle versioni di NFS e ONTAP.

SAP lama richiede che la directory /usr/sap/SID sia locale. Pertanto, non montare un volume NFS per /usr/sap/SID se si utilizza SAP lama.

Per NFSv3, è necessario disattivare il blocco NFS per evitare le operazioni di pulitura del blocco NFS in caso di guasto al software o al server.

Con ONTAP 9, le dimensioni di trasferimento NFS possono essere configurate fino a 1 MB. In particolare, con connessioni a 40 GbE o più veloci al sistema storage, è necessario impostare le dimensioni di trasferimento su 1 MB per ottenere i valori di throughput previsti.

Parametro comune	NFSv3	NFSv4	Dimensione del trasferimento NFS con ONTAP 9	Dimensione del trasferimento NFS con ONTAP 8
rw, bg, hard, time=600, noatime,	nfsvers=3,nolock,	nfsvers=4.1,lock	rsize=1048576,wsize=262144,	rsize=65536,wsize=65536,

Per migliorare le prestazioni di lettura con NFSv3, NetApp consiglia di utilizzare `nconnect=n` Opzione di montaggio, disponibile con SUSE Linux Enterprise Server 12 SP4 o versione successiva e RedHat Enterprise Linux (RHEL) 8.3 o versione successiva.

I test delle performance lo dimostrano `nconnect=4` fornisce buoni risultati di lettura, in particolare per i volumi di dati. Le scritture dei log potrebbero trarre vantaggio da un numero inferiore di sessioni, ad esempio `nconnect=2`. Anche i volumi condivisi potrebbero trarre vantaggio dall'utilizzo dell'opzione 'nconnect'. Tenere presente che il primo mount da un server NFS (indirizzo IP) definisce il numero di sessioni utilizzate. Ulteriori montaggi sullo stesso indirizzo IP non modificano questo valore anche se per nconnect viene utilizzato un valore diverso.

A partire da ONTAP 9.8 e SUSE SLES15SP2 o RedHat RHEL 8.4 o superiore, NetApp supporta l'opzione nconnect anche per NFSv4.1.

Se nconnect viene utilizzato con NFSv4.x, la quantità di slot di sessione NFSv4.x deve essere regolata in base alla regola seguente: Numero di slot di sessione uguale a <nconnect value> x 64. All'host questo sarà adjusted da seguito da `echo options nfs max_session_slots=<calculated value> > /etc/modprobe.d/nfsclient.conf` un riavvio. Anche il valore lato server deve essere regolato, impostare il numero di slot di sessione come descritto in "Configurazione NFS per NFSv4."

Per montare i file system durante l'avvio del sistema con `/etc/fstab` file di configurazione, attenersi alla seguente procedura:

L'esempio seguente mostra un database SAP HANA host singolo con SID=NF2 utilizzando NFSv3 e una

dimensione di trasferimento NFS di 1 MB per le letture e 256k per le scritture.

1. Aggiungere i file system richiesti a `/etc/fstab` file di configurazione.

```
sapcc-hana-tst-06:/ # cat /etc/fstab
<storage-vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data01>:/NF2_shared/usr-sap /usr/sap/NF2 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data01>:/NF2_shared/shared /hana/shared nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
```

2. Eseguire `mount -a` per montare i file system su tutti gli host.

Nell'esempio successivo viene illustrato un database SAP HANA multihost con SID=NF2 utilizzando NFSv4.1 per i file system di dati e log e NFSv3 per `/hana/shared` e. `/usr/sap/NF2` file system. Viene utilizzata una dimensione di trasferimento NFS di 1 MB per le letture e 256k per le scritture.

1. Aggiungere i file system richiesti a `/etc/fstab` file di configurazione su tutti gli host.



Il `/usr/sap/NF2` il file system è diverso per ciascun host di database. Viene mostrato l'esempio seguente `/NF2_shared/usr-sap-host1`.

```
sapcc-hana-tst-06:/ # cat /etc/fstab
<storage-vif-data01>:/NF2_data_mnt00001 /hana/data/NF2/mnt00001 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-data02>:/NF2_data_mnt00002 /hana/data/NF2/mnt00002 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-log01>:/NF2_log_mnt00001 /hana/log/NF2/mnt00001 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-log02>:/NF2_log_mnt00002 /hana/log/NF2/mnt00002 nfs
rw,nfsvers=4.1,hard,timeo=600,nconnect=2,rsize=1048576,wsize=262144,bg,n
oatime,lock 0 0
<storage-vif-data02>:/NF2_shared/usr-sap-host1 /usr/sap/NF2 nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
<storage-vif-data02>:/NF2_shared/shared /hana/shared nfs
rw,nfsvers=3,hard,timeo=600,nconnect=4,rsize=1048576,wsize=262144,bg,noa
time,nolock 0 0
```

2. Eseguire `mount -a` per montare i file system su tutti gli host.

Preparazione dell'installazione di SAP HANA per NFSv4

NFS versione 4 e successive richiede l'autenticazione dell'utente. Questa autenticazione può essere eseguita utilizzando uno strumento di gestione utente centrale, ad esempio un server LDAP (Lightweight Directory Access Protocol) o con account utente locali. Le sezioni seguenti descrivono come configurare gli account utente locali.

Gli utenti amministrativi `<sid>adm`,`<sid>crypt` e il `sapsys` gruppo devono essere creati manualmente sugli host SAP HANA e sugli storage controller prima che venga avviata l'installazione del software SAP HANA.

Host SAP HANA

Se non esiste, il `sapsys` Il gruppo deve essere creato sull'host SAP HANA. È necessario scegliere un ID di gruppo univoco che non sia in conflitto con gli ID di gruppo esistenti sui controller di storage.

Gli utenti `<sid>adm` e `<sid>crypt` vengono creati sull'host SAP HANA. È necessario scegliere ID univoci che non siano in conflitto con gli ID utente esistenti sui controller di archiviazione.

Per un sistema SAP HANA con host multipli, gli ID utente e gruppo devono essere gli stessi su tutti gli host SAP HANA. Il gruppo e l'utente vengono creati sugli altri host SAP HANA copiando le linee interessate da e `/etc/passwd` nel `/etc/group` sistema di origine a tutti gli altri host SAP HANA.

Il dominio NFSv4 deve essere impostato sullo stesso valore su tutti i server Linux `/etc/idmapd.conf`) E SVM. Impostare il parametro di dominio "dominio = <domain-name>" nel file `/etc/idmapd.conf` Per gli host Linux.

Attivare e avviare il servizio NFS IDMAPD.

```
systemctl enable nfs-idmapd.service
systemctl start nfs-idmapd.service
```

I kernel Linux più recenti non richiedono questo passaggio. I messaggi di avviso possono essere ignorati in modo sicuro.

Controller di storage

Gli ID utente e l'ID del gruppo devono essere gli stessi sugli host SAP HANA e sugli storage controller. Il gruppo e l'utente vengono creati immettendo i seguenti comandi sul cluster di storage:

```
vserver services unix-group create -vserver <vserver> -name <group name>
-id <group id>
vserver services unix-user create -vserver <vserver> -user <user name> -id
<user-id> -primary-gid <group id>
```

Inoltre, impostare l'ID del gruppo della root utente UNIX della SVM su 0.

```
vserver services unix-user modify -vserver <vserver> -user root -primary
-gid 0
```

Configurazione dello stack di i/o per SAP HANA

A partire da SAP HANA 1.0 SPS10, SAP ha introdotto i parametri per regolare il comportamento di i/o e ottimizzare il database per i file e i sistemi storage utilizzati.

NetApp ha condotto test delle performance per definire i valori ideali. La seguente tabella elenca i valori ottimali dedotti dai test delle prestazioni.

Parametro	Valore
max_parallel_io_requests	128
async_read_submit	acceso
async_write_submit_active	acceso
async_write_submit_blocks	tutto

Per le versioni SAP HANA 1.0 fino a SPS12, questi parametri possono essere impostati durante l'installazione del database SAP HANA, come descritto nella nota SAP "2267798: Configurazione del database SAP HANA durante l'installazione con hdbparam".

In alternativa, è possibile impostare i parametri dopo l'installazione del database SAP HANA utilizzando `hdbparam` framework.

```
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_read_submit=on
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

A partire da SAP HANA 2.0, `hdbparam` è stato obsoleto e i parametri sono stati spostati in `global.ini`. I parametri possono essere impostati utilizzando i comandi SQL o SAP HANA Studio. Per ulteriori informazioni, consulta la nota SAP "2399079: Eliminazione di hdbparam in HANA 2". È inoltre possibile impostare i parametri all'interno di global.ini, come illustrato nel seguente testo:

```
nf2adm@stlrx300s8-6: /usr/sap/NF2/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

A partire da SAP HANA 2.0 SPS5, la `setParameter.py` è possibile utilizzare lo script per impostare i parametri corretti:

```
nf2adm@sapcc-hana-tst-06:/usr/sap/NF2/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

Dimensioni del volume di dati SAP HANA

Per impostazione predefinita, SAP HANA utilizza un solo volume di dati per ogni servizio SAP HANA. A causa della limitazione delle dimensioni massime del file system, si consiglia di limitare le dimensioni massime del volume di dati.

Per eseguire questa operazione automaticamente, impostare il seguente parametro in `global.ini` nella sezione `[persistence]`:

```
datavolume_striping = true
datavolume_striping_size_gb = 8000
```

In questo modo, viene creato un nuovo volume di dati dopo il raggiungimento del limite di 800 GB. "Nota SAP 240005 domanda 15" fornisce ulteriori informazioni.

Installazione del software SAP HANA

Di seguito sono riportati i requisiti per l'installazione del software per SAP HANA.

Installazione su un sistema a host singolo

L'installazione del software SAP HANA non richiede alcuna preparazione aggiuntiva per un sistema a singolo host.

Installazione su sistemi con più host

Per installare SAP HANA su un sistema a più host, attenersi alla seguente procedura:

1. Utilizzando lo strumento di installazione SAP `hdbclm`, avviare l'installazione eseguendo il comando seguente su uno degli host di lavoro. Utilizzare l' `addhosts`opzione per aggiungere il secondo worker (`sapcc-hana-tst-03`) e l'host di standby)(`sapcc-hana-tst-04`.

```
apcc-hana-tst-02:/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_LCM_LINUX_X86_64 #
./hdblcm --action=install --addhosts=sapcc-hana-tst-03:role=worker,sapcc
-hana-tst-04:role=standby

SAP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
```

```
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1
(1.015.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip


SAP HANA Database version '2.00.073.00.1695288802' will be installed.
```

```
Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------
-------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version
2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
  9     | epmmds          | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
4.203.2321.0.0

Enter comma-separated list of the selected indices [3,4]: 2,3
```

2. Verificare che lo strumento di installazione abbia installato tutti i componenti selezionati su tutti gli host di lavoro e di standby.

Aggiunta di partizioni di volumi di dati aggiuntive

A partire da SAP HANA 2.0 SPS4, è possibile configurare ulteriori partizioni del volume di dati, che consentono di configurare due o più volumi per il volume di dati di un database tenant SAP HANA. Puoi anche scalare oltre i limiti di dimensioni e performance di un singolo volume.

> L'utilizzo di due o più volumi singoli per il volume di dati è disponibile per i sistemi SAP HANA a host singolo e multiplo. È possibile aggiungere ulteriori partizioni del volume di dati in qualsiasi momento, ma in questo modo potrebbe essere necessario riavviare il database SAP HANA.

Attivazione di partizioni di volumi di dati aggiuntive

1. Per abilitare ulteriori partizioni del volume di dati, aggiungere la seguente voce all'interno di `global.ini` Utilizzo di SAP HANA Studio o Cockpit nella configurazione di SYSTEMDB.

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

Aggiunta manuale del parametro a `global.ini` il file richiede il riavvio del database.

Configurazione del volume per un sistema SAP HANA a host singolo

Il layout dei volumi per un sistema SAP HANA a host singolo con più partizioni è simile al layout per un sistema con una partizione del volume di dati, ma con un volume di dati aggiuntivo memorizzato su un aggregato diverso come il volume di log e l'altro volume di dati. La seguente tabella mostra un esempio di configurazione di un sistema SAP HANA a host singolo con due partizioni del volume di dati.

Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller b
Volume di dati: SID_data_mnt00001	Volume condiviso: SID_shared	Volume di dati: SID_data2_mnt00001	Volume di log: SID_log_mnt00001

La seguente tabella mostra un esempio di configurazione del punto di montaggio per un sistema a host singolo con due partizioni del volume di dati.

Percorso di giunzione	Directory	Punto di montaggio sull'host HANA
SID_data_mnt00001	–	/hana/data/SID/mnt00001
SID_data2_mnt00001	–	/hana/data2/SID/mnt00001
SID_log_mnt00001	–	/hana/log/SID/mnt00001
SID_shared	usr-sap condiviso	/Usr/sap/SID /hana/shared

Creare il nuovo volume di dati e montarlo nello spazio dei nomi utilizzando Gestore di sistema di ONTAP o l'interfaccia della riga di comando del cluster di ONTAP.

Configurazione dei volumi per sistemi SAP HANA con host multipli

Il layout dei volumi per un sistema SAP HANA con più host e più partizioni è simile al layout di un sistema con una partizione del volume di dati, ma con un volume di dati aggiuntivo memorizzato su un aggregato diverso come il volume di log e l'altro volume di dati. La seguente tabella mostra un esempio di configurazione di un sistema SAP HANA con host multipli con due partizioni di volumi di dati.

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Volumi di dati e log per il nodo 1	Volume di dati: SID_data_mnt00001	–	Volume di log: SID_log_mnt00001	Volume Data2: SID_data2_mnt00001
Volumi di dati e log per il nodo 2	Volume di log: SID_log_mnt00002	Volume Data2: SID_data2_mnt00002	Volume di dati: SID_data_mnt00002	–

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Volumi di dati e log per il nodo 3	–	Volume di dati: SID_data_mnt00003	Volume Data2: SID_data2_mnt00003	Volume di log: SID_log_mnt00003
Volumi di dati e log per il nodo 4	Volume Data2: SID_data2_mnt00004	Volume di log: SID_log_mnt00004	–	Volume di dati: SID_data_mnt00004
Volume condiviso per tutti gli host	Volume condiviso: SID_shared	–	–	–

La seguente tabella mostra un esempio di configurazione del punto di montaggio per un sistema a host singolo con due partizioni del volume di dati.

Percorso di giunzione	Directory	Punto di montaggio sull'host SAP HANA	Nota
SID_data_mnt00001	–	/hana/data/SID/mnt00001	Montato su tutti gli host
SID_data2_mnt00001	–	/hana/data2/SID/mnt00001	Montato su tutti gli host
SID_log_mnt00001	–	/hana/log/SID/mnt00001	Montato su tutti gli host
SID_data_mnt00002	–	/hana/data/SID/mnt00002	Montato su tutti gli host
SID_data2_mnt00002	–	/hana/data2/SID/mnt00002	Montato su tutti gli host
SID_log_mnt00002	–	/hana/log/SID/mnt00002	Montato su tutti gli host
SID_data_mnt00003	–	/hana/data/SID/mnt00003	Montato su tutti gli host
SID_data2_mnt00003	–	/hana/data2/SID/mnt00003	Montato su tutti gli host
SID_log_mnt00003	–	/hana/log/SID/mnt00003	Montato su tutti gli host
SID_data_mnt00004	–	/hana/data/SID/mnt00004	Montato su tutti gli host
SID_data2_mnt00004	–	/hana/data2/SID/mnt00004	Montato su tutti gli host
SID_log_mnt00004	–	/hana/log/SID/mnt00004	Montato su tutti gli host
SID_shared	condiviso	/hana/shared/SID	Montato su tutti gli host
SID_shared	usr-sap-host1	/Usr/sap/SID	Montato sull'host 1
SID_shared	usr-sap-host2	/Usr/sap/SID	Montato sull'host 2
SID_shared	usr-sap-host3	/Usr/sap/SID	Montato sull'host 3
SID_shared	usr-sap-host4	/Usr/sap/SID	Montato sull'host 4
SID_shared	usr-sap-host5	/Usr/sap/SID	Montato sull'host 5

Creare il nuovo volume di dati e montarlo nello spazio dei nomi utilizzando Gestore di sistema di ONTAP o l'interfaccia della riga di comando del cluster di ONTAP.

Configurazione dell'host

Oltre alle attività descritte nella sezione, ""Host setup" (Configurazione host),"è necessario creare punti di montaggio aggiuntivi e voci fstab per i nuovi volumi di dati aggiuntivi e montare i nuovi volumi.

1. Creare punti di montaggio aggiuntivi:
   - Per un sistema a host singolo, creare punti di montaggio e impostare le autorizzazioni sull'host del database.

     ```
     sapcc-hana-tst-06:/ # mkdir -p /hana/data2/SID/mnt00001
     sapcc-hana-tst-06:/ # chmod –R 777 /hana/data2/SID
     ```

   - Per un sistema a più host, creare punti di montaggio e impostare le autorizzazioni su tutti gli host worker e standby. I seguenti comandi di esempio si riferiscono a un sistema HANA con host multiplo 2+1.
     - Primo host di lavoro:

       ```
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-06:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-06:~ # chmod -R 777 /hana/data2/SID
       ```

     - Secondo host di lavoro:

       ```
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
       ```

     - Host in standby:

       ```
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00001
       sapcc-hana-tst-07:~ # mkdir -p /hana/data2/SID/mnt00002
       sapcc-hana-tst-07:~ # chmod -R 777 /hana/data2/SID
       ```

2. Aggiungere i file system aggiuntivi a `/etc/fstab` file di configurazione su tutti gli host. Un esempio per un sistema a host singolo che utilizza NFSv4.1 è il seguente:

   ```
   <storage-vif-data02>:/SID_data2_mnt00001 /hana/data2/SID/mnt00001 nfs
   rw,vers=4,
   minorversion=1,hard,timeo=600,rsize=1048576,wsize=262144,bg,noatime,lock
   0 0
   ```

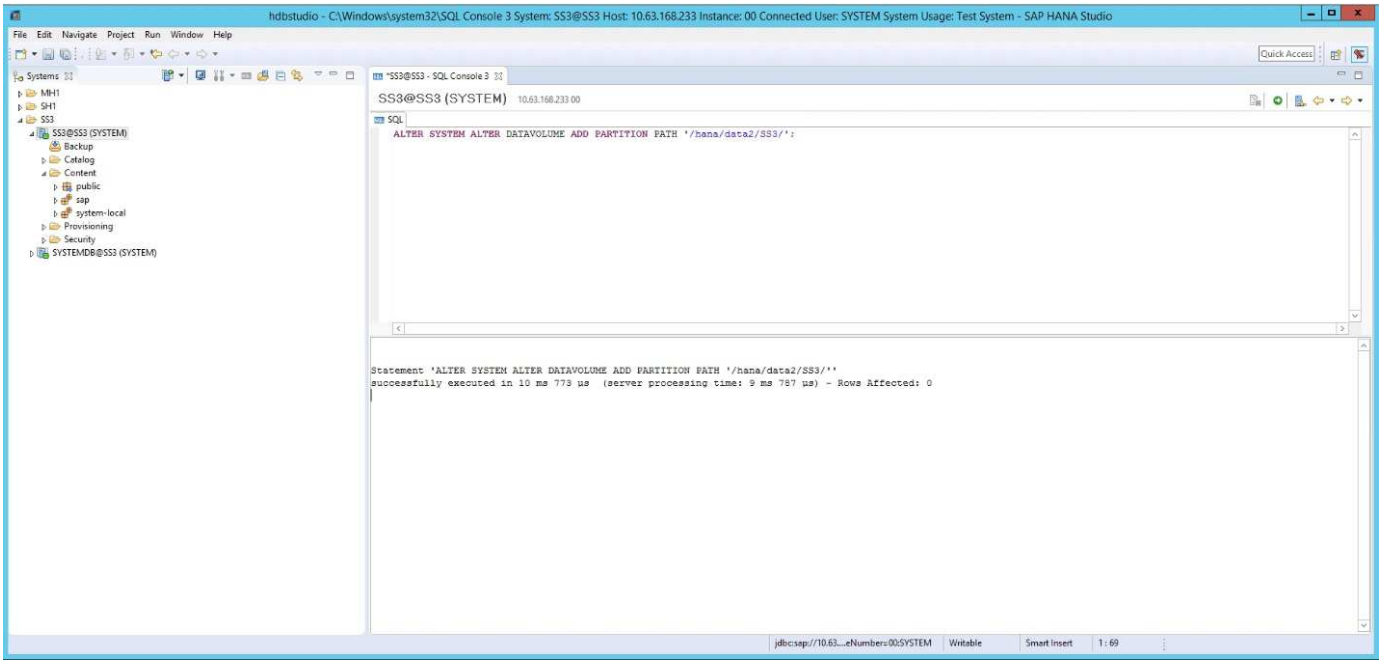
Utilizzare un'interfaccia virtuale di storage diversa per la connessione a ciascun volume di dati per assicurarsi che vengano utilizzate sessioni TCP diverse per ciascun volume. È inoltre possibile utilizzare l'opzione di montaggio di nconnect, se disponibile per il sistema operativo in uso.

3. Per montare i file system, eseguire `mount -a` comando.

Aggiunta di una partizione aggiuntiva del volume di dati

Eseguire la seguente istruzione SQL sul database tenant per aggiungere una partizione aggiuntiva del volume di dati al database tenant. Utilizzare il percorso verso volumi aggiuntivi:

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```



Dove trovare ulteriori informazioni

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

- "Soluzioni software SAP HANA"
- "TR-4646: Disaster recovery SAP HANA con replica dello storage"
- "TR-4614: Backup e ripristino SAP HANA con SnapCenter"
- "TR-4667: Automatizzazione di copie di sistema SAP con il plug-in SAP HANA SnapCenter"
- Centri di documentazione NetApp

  "https://www.netapp.com/support-and-training/documentation/"

- Hardware per lo storage aziendale certificato SAP per SAP HANA

"https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"

- Requisiti di storage SAP HANA

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"

- SAP HANA - Domande frequenti sull'integrazione personalizzata del data center

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"

- SAP HANA su VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"

- Guida alle Best practice di SAP HANA su VMware vSphere

  "https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

Aggiornare la cronologia

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

Data	Riepilogo degli aggiornamenti
Aprile 2014	Versione iniziale
Agosto 2014	Selezione aggiornata del dimensionamento dei dischi e aggiunta della configurazione SSD aggiunta della configurazione del sistema operativo Red Hat Enterprise Linux aggiunta delle informazioni sul connettore di storage SAP HANA aggiunta delle informazioni sulla configurazione di VMware
Novembre 2014	Sezione aggiornata sul dimensionamento dello storage
Gennaio 2015	Aggiornata la sezione delle API di Storage Connector aggiornata la configurazione di aggregati e volumi
Marzo 2015	Aggiunta della nuova implementazione STONITH per SAP HANA SPS9 aggiunta della sezione relativa all'installazione di HANA e alla configurazione del nodo di calcolo
Ottobre 2015	Aggiunto supporto NFSv4 per cDOT il parametro sysctl aggiornato include il parametro i/o per SAP HANA e HWVAL > SPS10
Marzo 2016	Dimensionamento della capacità aggiornato Opzioni di montaggio per /hana/shared aggiornamento del parametro sysctl
Febbraio 2017	Nuovi sistemi storage e shelf di dischi NetApp nuove funzionalità di ONTAP 9 supporto per le nuove release 40 GbE del sistema operativo (SUSE Linux Enterprise Server 12 SP1 e Red Hat Enterprise Linux 7.2) Nuova release di SAP HANA
Luglio 2017	Aggiornamenti minori
Settembre 2018	Nuovi sistemi storage NetApp nuove release dei sistemi operativi (SUSE Linux Enterprise Server 12 SP3 e Red Hat Enterprise Linux 7.4) ulteriori modifiche minori SAP HANA 2.0 SPS3

Data	Riepilogo degli aggiornamenti
Settembre 2019	Nuove release del sistema operativo (SUSE Linux Enterprise Server 12 SP4, SUSE Linux Enterprise Server 15 e Red Hat Enterprise Linux 7.6) dimensioni del volume MAX Data piccole modifiche
Dicembre 2019	Nuovi sistemi storage NetApp Nuova release del sistema operativo SUSE Linux Enterprise Server 15 SP1
Marzo 2020	Supporto di nconnect per NFSv3 Nuova release del sistema operativo Red Hat Enterprise Linux 8
Maggio 2020	Sono state introdotte più funzioni di partizione dei dati disponibili da SAP HANA 2.0 SPS4
Giugno 2020	Ulteriori informazioni sulle funzionalità opzionali aggiornamenti minori
Dicembre 2020	Supporto di nconnect per NFSv4.1 a partire da ONTAP 9.8 nuove release del sistema operativo Nuova versione di SAP HANA
Febbraio 2021	Modifiche alle impostazioni della rete host e altre modifiche minori
Aprile 2021	Aggiunta di informazioni specifiche su VMware vSphere
Settembre 2022	Nuove versioni del sistema operativo
Dicembre 2023	Aggiornamento della configurazione dell'host impostazioni nconnect modificate aggiunta di informazioni sulle NFSv4,1 sessioni
Settembre 2024	Nuovi sistemi storage e aggiornamenti minori
Febbraio 2025	Nuovo sistema storage
Luglio 2025	Aggiornamenti minori

Guida alla configurazione di SAP HANA su sistemi FAS con FCP

Guida alla configurazione di SAP HANA su sistemi NetApp FAS con protocollo Fibre Channel

La famiglia di prodotti NetApp FAS è stata certificata per l'uso con SAP HANA nei progetti TDI. Questa guida fornisce le best practice per SAP HANA su questa piattaforma per FCP.

Marco Schoen, NetApp

La certificazione è valida per i seguenti modelli:

- FAS2750, FAS2820, FAS8300, FAS50, FAS8700, FAS70, FAS9500, FAS90

Per un elenco completo delle soluzioni di storage certificate NetApp per SAP HANA, consulta la "Directory hardware SAP HANA certificata e supportata".

Questo documento descrive le configurazioni FAS che utilizzano il protocollo Fibre Channel (FCP).

La configurazione descritta in questo documento è necessaria per ottenere i KPI SAP HANA richiesti e le migliori performance per SAP HANA. La modifica di impostazioni o l'utilizzo di funzionalità non elencate nel presente documento potrebbe causare un peggioramento delle prestazioni o un comportamento imprevisto e dovrebbe essere eseguita solo se richiesto dal supporto NetApp.

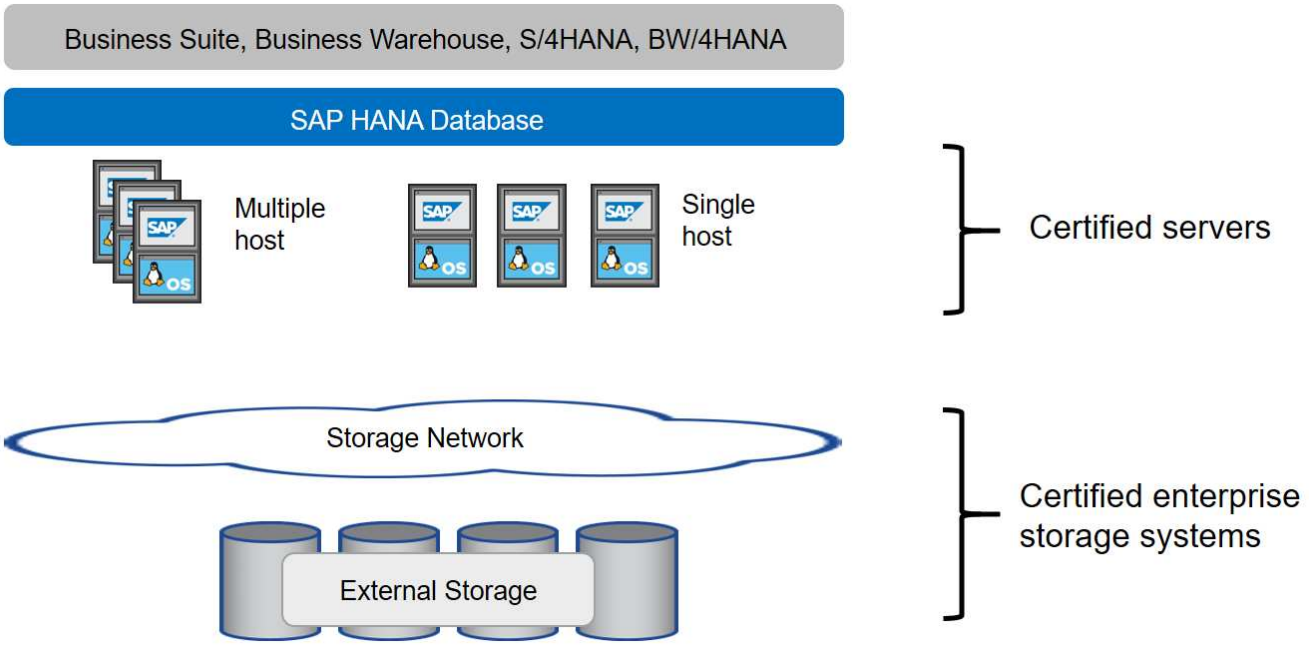
Le guide di configurazione per i sistemi FAS che utilizzano i sistemi NFS e NetApp AFF sono disponibili tramite i seguenti collegamenti:

- "SAP HANA su sistemi NetApp AFF con FCP"
- "SAP HANA su sistemi NetApp ASA con FCP"
- "SAP HANA su sistemi NetApp FAS con NFS"
- "SAP HANA su sistemi NetApp AFF con NFS"

In un ambiente multi-host SAP HANA, il connettore storage standard SAP HANA viene utilizzato per fornire la scherma in caso di failover di un host SAP HANA. Fare riferimento alle note SAP relative alle linee guida per la configurazione del sistema operativo e alle dipendenze del kernel Linux specifico di HANA. Per ulteriori informazioni, vedere "Nota SAP 2235581 – sistemi operativi supportati da SAP HANA".

SAP HANA: Integrazione personalizzata del data center

I controller di storage NetApp FAS sono certificati nel programma TDI (Tailored Data Center Integration) di SAP HANA utilizzando i protocolli NFS (NAS) e Fibre Channel (SAN). Possono essere implementati in qualsiasi scenario SAP HANA, ad esempio SAP Business Suite su HANA, S/4HANA, BW/4HANA o SAP Business Warehouse su HANA in configurazioni a host singolo o multiplo. Qualsiasi server certificato per l'utilizzo con SAP HANA può essere combinato con la soluzione di storage certificata. Vedere la figura seguente per una panoramica dell'architettura.



Per ulteriori informazioni sui prerequisiti e sui consigli per i sistemi SAP HANA produttivi, consulta la seguente risorsa:

- "SAP HANA - Domande frequenti sull'integrazione personalizzata del data center"

SAP HANA con VMware vSphere

Sono disponibili diverse opzioni per la connessione dello storage alle macchine virtuali (VM). Il metodo preferito consiste nel collegare i volumi di storage con NFS direttamente dal sistema operativo guest. Questa opzione è descritta in "SAP HANA su sistemi NetApp AFF con NFS".

Sono supportati anche RDM (Raw Device Mapping), datastore FCP o datastore VVOL con FCP. Per entrambe le opzioni del datastore, è necessario memorizzare un solo volume di log o dati SAP HANA all'interno del datastore per casi di utilizzo produttivi.

Per ulteriori informazioni sull'utilizzo di vSphere con SAP HANA, consultare i seguenti collegamenti:

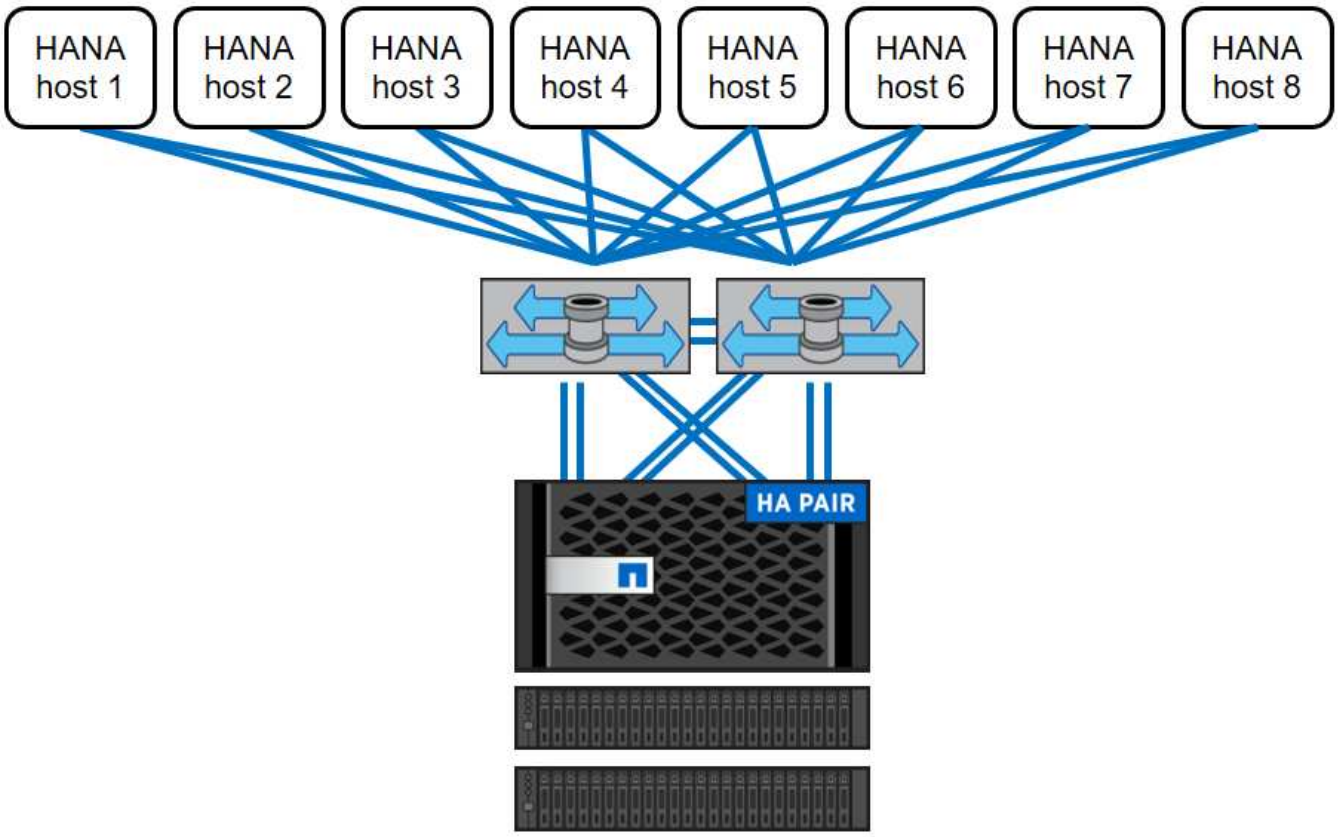
- "SAP HANA su VMware vSphere - virtualizzazione - Wiki della community"
- "Guida alle Best practice di SAP HANA su VMware vSphere"
- "2161991 - linee guida per la configurazione di VMware vSphere - Launchpad di supporto SAP ONE (accesso richiesto)"

Architettura

Gli host SAP HANA sono connessi ai controller di storage utilizzando un'infrastruttura FCP ridondante e un software multipath. È necessaria un'infrastruttura di switch FCP ridondante per fornire connettività host-to-storage SAP HANA fault-tolerant in caso di guasto dello switch o dell'HBA (host bus adapter). È necessario configurare lo zoning appropriato sullo switch per consentire a tutti gli host HANA di raggiungere i LUN richiesti sui controller di storage.

È possibile utilizzare diversi modelli della famiglia di prodotti FAS a livello di storage. Il numero massimo di host SAP HANA collegati allo storage è definito dai requisiti di performance SAP HANA. Il numero di shelf di dischi richiesti è determinato dai requisiti di capacità e performance dei sistemi SAP HANA.

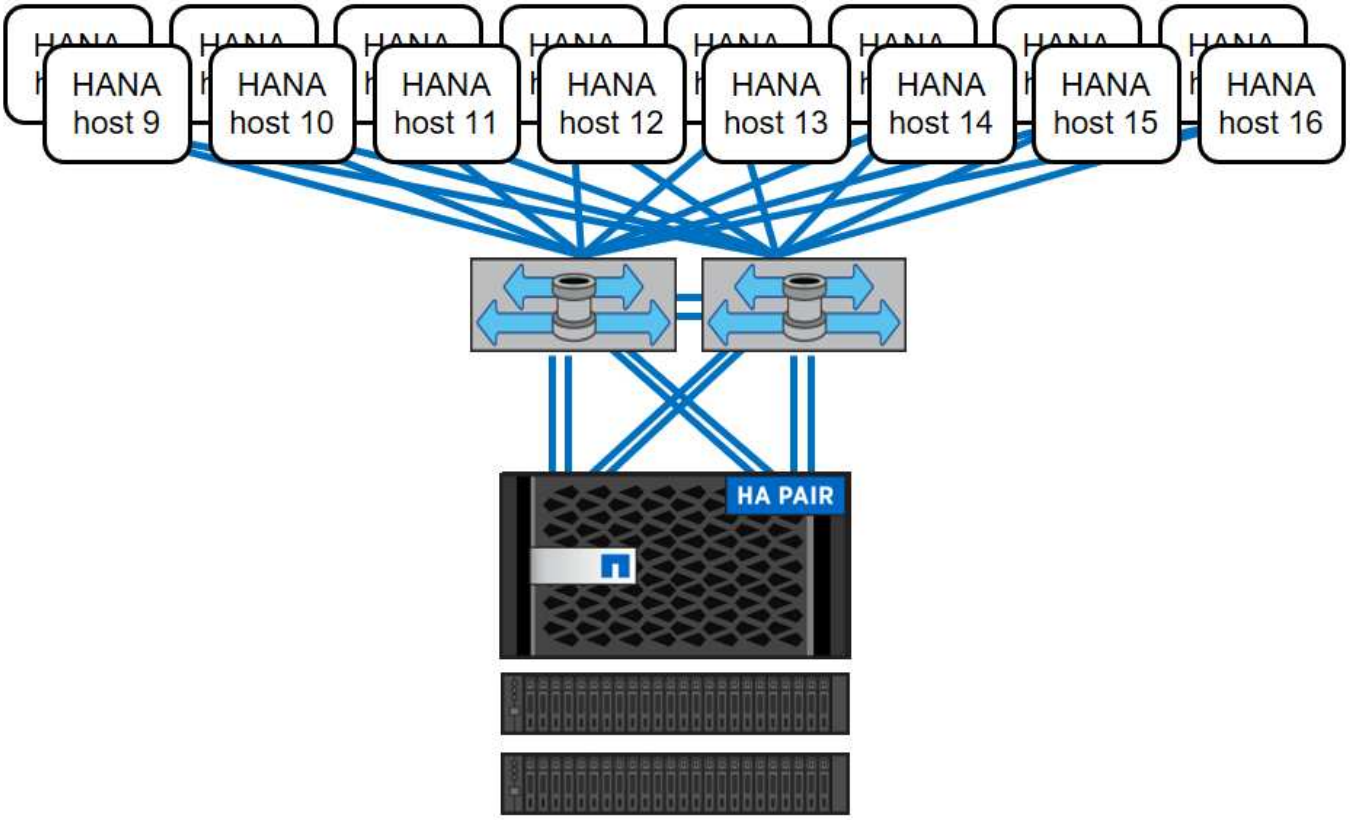
La figura seguente mostra una configurazione di esempio con otto host SAP HANA collegati a una coppia ha di storage.



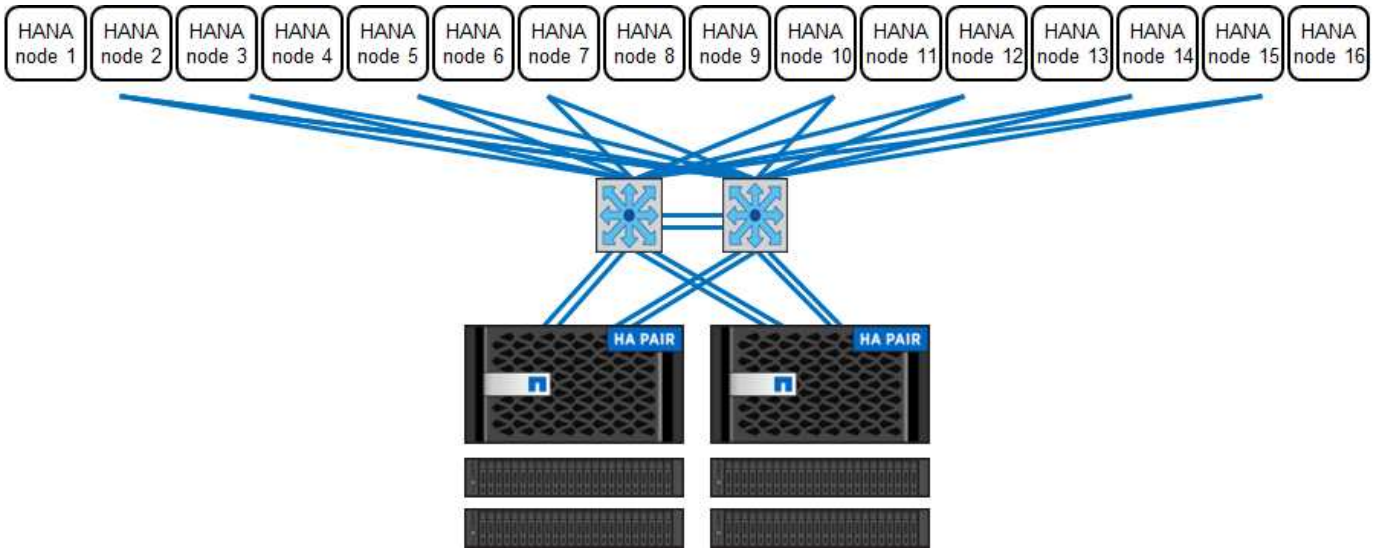
Questa architettura può essere scalata in due dimensioni:

- Collegando ulteriori host SAP HANA e capacità del disco allo storage, supponendo che i controller dello storage possano fornire performance sufficienti sotto il nuovo carico per soddisfare i principali indicatori di performance (KPI)
- Aggiungendo più sistemi storage e capacità disco per gli host SAP HANA aggiuntivi

La figura seguente mostra un esempio di configurazione in cui più host SAP HANA sono collegati ai controller di storage. In questo esempio, sono necessari più shelf di dischi per soddisfare i requisiti di capacità e performance dei 16 host SAP HANA. A seconda dei requisiti di throughput totale, è necessario aggiungere ulteriori connessioni FC ai controller di storage.



Indipendentemente dal modello di storage del sistema FAS implementato, il panorama SAP HANA può anche essere scalato aggiungendo più controller di storage, come illustrato nella figura seguente.



Backup SAP HANA

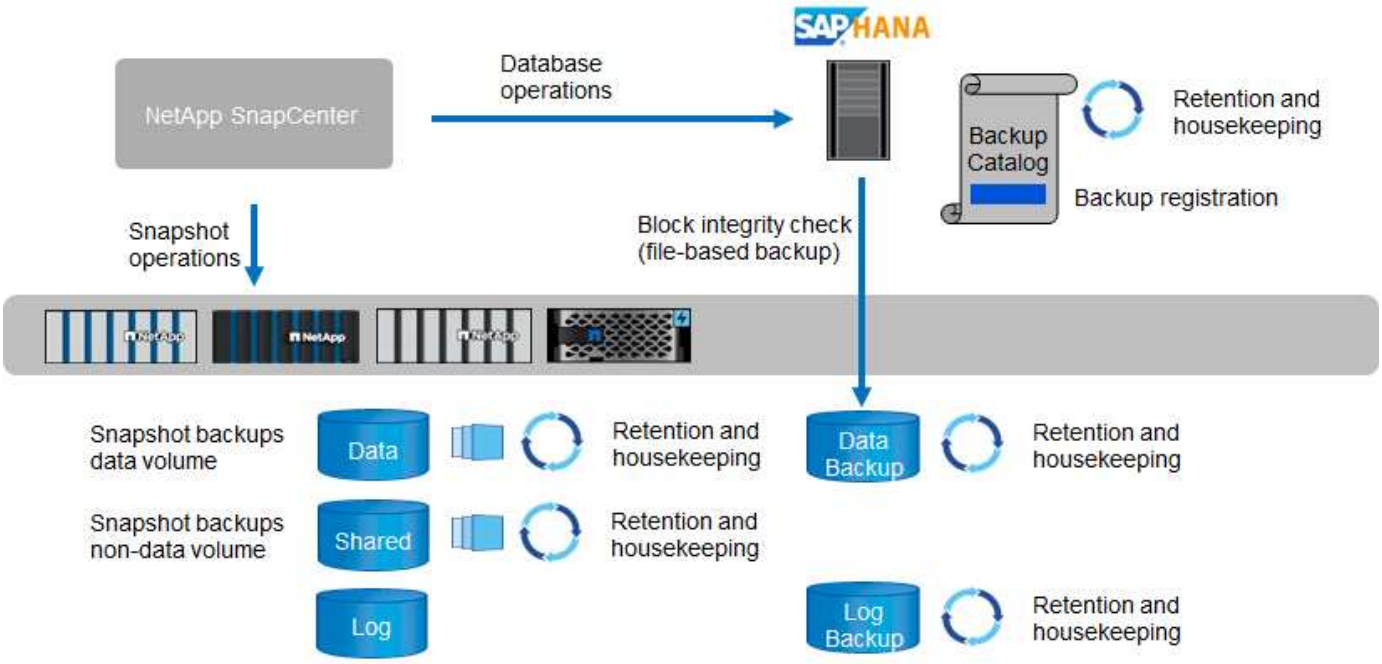
Il software NetApp ONTAP offre un meccanismo integrato per il backup dei database SAP HANA. Il backup Snapshot basato su storage è una soluzione di backup completamente supportata e integrata disponibile per i sistemi single-container SAP HANA e per i sistemi single-tenant SAP HANA MDC.

I backup Snapshot basati su storage vengono implementati utilizzando il plug-in NetApp SnapCenter per SAP HANA, che consente backup Snapshot coerenti basati su storage utilizzando le interfacce fornite dal database SAP HANA. SnapCenter registra i backup Snapshot nel catalogo di backup SAP HANA in modo che i backup

siano visibili all'interno di SAP HANA Studio e possano essere selezionati per le operazioni di ripristino e ripristino.

Utilizzando il software NetApp SnapVault, le copie Snapshot create sullo storage primario possono essere replicate nello storage di backup secondario controllato da SnapCenter. È possibile definire diverse policy di conservazione dei backup per i backup sullo storage primario e per i backup sullo storage secondario. Il plug-in SnapCenter per il database SAP HANA gestisce la conservazione dei backup dei dati basati su copia Snapshot e dei backup dei log, inclusa la manutenzione del catalogo di backup. Il plug-in SnapCenter per database SAP HANA consente inoltre di eseguire un controllo dell'integrità dei blocchi del database SAP HANA eseguendo un backup basato su file.

È possibile eseguire il backup dei log del database direttamente sullo storage secondario utilizzando un montaggio NFS, come illustrato nella figura seguente.



I backup Snapshot basati su storage offrono vantaggi significativi rispetto ai backup basati su file. Tali vantaggi includono:

- Backup più rapido (pochi minuti)
- Ripristino più rapido sul layer di storage (pochi minuti)
- Nessun effetto sulle prestazioni dell'host, della rete o dello storage del database SAP HANA durante il backup
- Replica efficiente in termini di spazio e larghezza di banda sullo storage secondario in base alle modifiche dei blocchi

Per informazioni dettagliate sulla soluzione di backup e ripristino SAP HANA con SnapCenter, consultare "TR-4614: Backup e ripristino SAP HANA con SnapCenter".

Disaster recovery SAP HANA

Il disaster recovery SAP HANA può essere eseguito a livello di database utilizzando la replica di sistema SAP o a livello di storage utilizzando le tecnologie di replica dello storage. La sezione seguente fornisce una panoramica delle soluzioni di disaster recovery basate sulla replica dello storage.

Per informazioni dettagliate sulla soluzione di disaster recovery SAP HANA con SnapCenter, vedere "TR-4646: Disaster recovery SAP HANA con replica dello storage".

Replica dello storage basata su SnapMirror

La figura seguente mostra una soluzione di disaster recovery a tre siti che utilizza la replica sincrona di SnapMirror nel data center di DR locale e SnapMirror asincrono per replicare i dati nel data center di DR remoto.

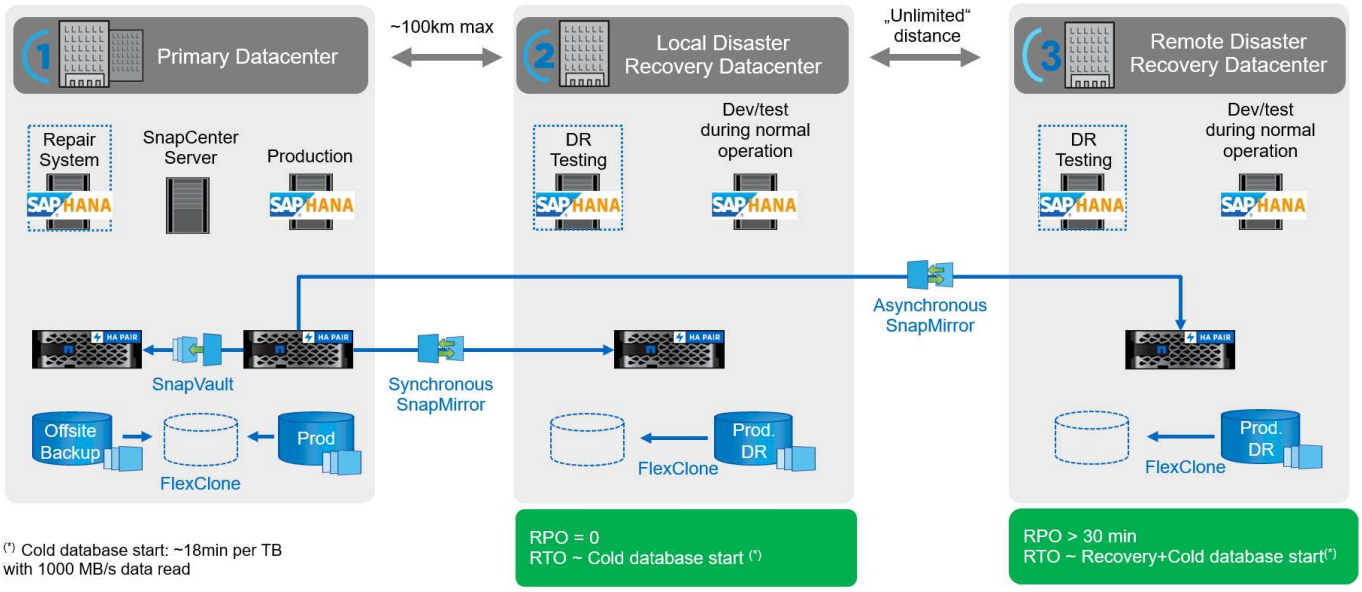
La replica dei dati con SnapMirror sincrono fornisce un RPO pari a zero. La distanza tra il data center DR principale e quello locale è limitata a circa 100 km.

La protezione dai guasti del sito di DR primario e locale viene eseguita replicando i dati in un terzo data center di DR remoto utilizzando SnapMirror asincrono. L'RPO dipende dalla frequenza degli aggiornamenti di replica e dalla velocità di trasferimento. In teoria, la distanza è illimitata, ma il limite dipende dalla quantità di dati da trasferire e dalla connessione disponibile tra i data center. I valori RPO tipici sono compresi nell'intervallo da 30 minuti a più ore.

L'RTO per entrambi i metodi di replica dipende principalmente dal tempo necessario per avviare il database HANA nel sito di DR e caricare i dati in memoria. Supponendo che i dati siano letti con un throughput di 1000 Mbps, il caricamento di 1 TB di dati richiederebbe circa 18 minuti.

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

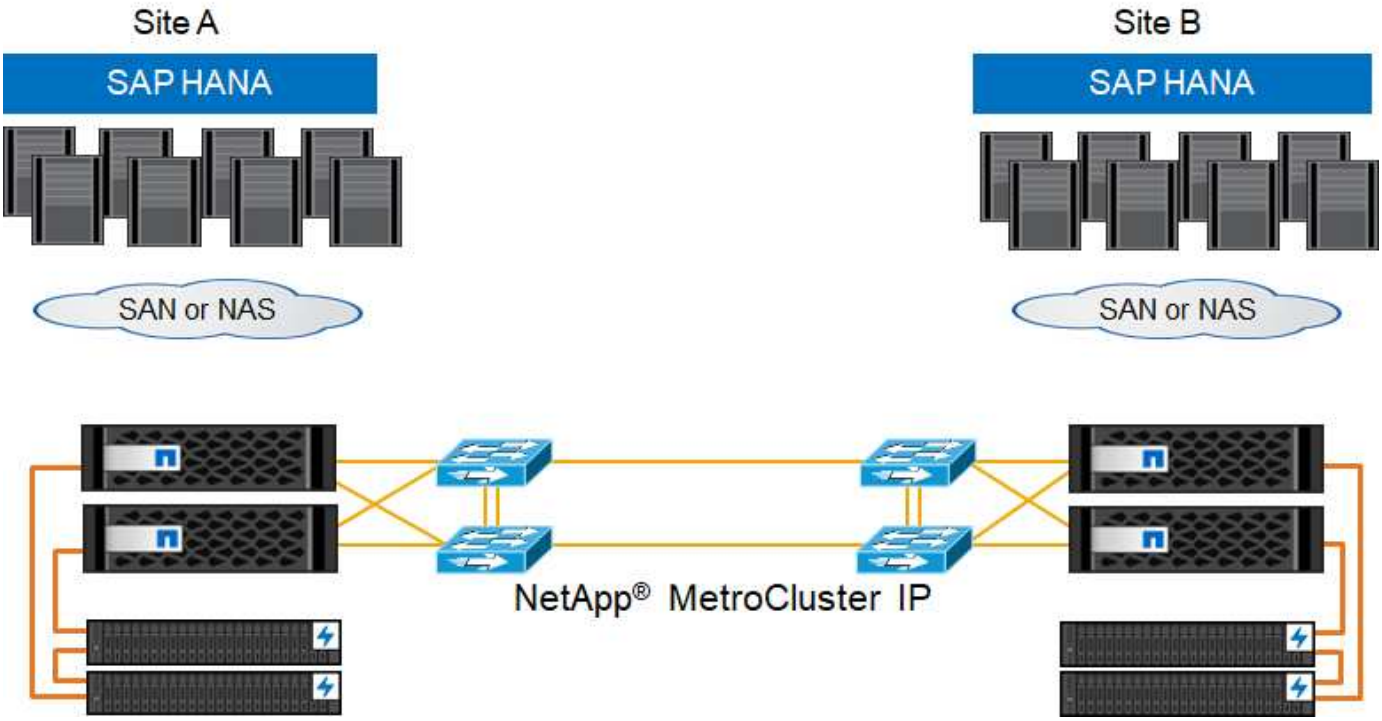
Entrambi i metodi di replica consentono di eseguire test del workflow di DR senza influenzare l'RPO e l'RTO. I volumi FlexClone vengono creati sullo storage e collegati ai server di test del DR.



La replica sincrona offre la modalità StrictSync. Se la scrittura sullo storage secondario non viene completata per qualsiasi motivo, l'i/o dell'applicazione non riesce, garantendo così che i sistemi di storage primario e secondario siano identici. L'i/o dell'applicazione al primario riprende solo dopo che la relazione SnapMirror ritorna allo stato InSync. In caso di guasto dello storage primario, l'i/o dell'applicazione può essere ripristinato sullo storage secondario dopo il failover senza perdita di dati. In modalità StrictSync, l'RPO è sempre zero.

Replica dello storage basata su NetApp MetroCluster

La figura seguente mostra una panoramica di alto livello della soluzione. Il cluster di storage di ogni sito offre alta disponibilità locale e viene utilizzato per i carichi di lavoro di produzione. I dati di ciascun sito vengono replicati in modo sincrono nell'altra posizione e sono disponibili in caso di failover di emergenza.



Dimensionamento dello storage

La sezione seguente fornisce una panoramica delle considerazioni su performance e capacità per il dimensionamento di un sistema storage per SAP HANA.

Contatta il tuo commerciale NetApp o il tuo partner NetApp per supportare il processo di dimensionamento dello storage e creare un ambiente di storage di dimensioni adeguate.

Considerazioni sulle performance

SAP ha definito un set statico di KPI relativi allo storage. Questi KPI sono validi per tutti gli ambienti SAP HANA in produzione, indipendentemente dalle dimensioni della memoria degli host di database e delle applicazioni che utilizzano il database SAP HANA. Questi KPI sono validi per ambienti a host singolo, host multiplo, Business Suite su HANA, Business Warehouse su HANA, S/4HANA e BW/4HANA. Pertanto, l'attuale approccio al dimensionamento delle performance dipende solo dal numero di host SAP HANA attivi collegati al sistema storage.

I KPI relativi alle performance dello storage sono richiesti solo per i sistemi SAP HANA in produzione.

SAP offre uno strumento di test delle performance, che deve essere utilizzato per validare le performance dello storage per gli host SAP HANA attivi collegati allo storage.

NetApp ha testato e predefinito il numero massimo di host SAP HANA che possono essere collegati a un modello di storage specifico, pur continuando a soddisfare i KPI di storage richiesti da SAP per i sistemi SAP

HANA basati sulla produzione.

> I controller di storage della famiglia di prodotti certificati FAS possono essere utilizzati anche per SAP HANA con altri tipi di dischi o soluzioni di back-end su disco, purché siano supportati da NetApp e soddisfino i KPI relativi alle performance di SAP HANA TDI. Ad esempio, NetApp Storage Encryption (NSE) e la tecnologia NetApp FlexArray.

Questo documento descrive il dimensionamento dei dischi rigidi SAS e dei dischi a stato solido.

Dischi rigidi

Per soddisfare i KPI relativi alle performance di storage di SAP, è necessario un minimo di 10 dischi dati (SAS a 10.000 rpm) per nodo SAP HANA.

> Questo calcolo è indipendente dal controller di storage e dallo shelf di dischi utilizzati.

Dischi a stato solido

Con i dischi a stato solido (SSD), il numero di dischi dati è determinato dal throughput della connessione SAS dai controller di storage allo shelf SSD.

Il numero massimo di host SAP HANA che possono essere eseguiti su uno shelf di dischi e il numero minimo di SSD richiesti per host SAP HANA sono stati determinati eseguendo il tool di test delle performance SAP.

- Lo shelf di dischi SAS da 12 GB (DS224C) con 24 SSD supporta fino a 14 host SAP HANA, quando lo shelf di dischi è collegato a 12 GB.
- Lo shelf di dischi SAS da 6 GB (DS2246) con 24 SSD supporta fino a 4 host SAP HANA.

Gli SSD e gli host SAP HANA devono essere equamente distribuiti tra entrambi i controller di storage.

La seguente tabella riassume il numero di host SAP HANA supportati per shelf di dischi.

	Shelf SAS da 6 GB (DS2246) completamente caricati con 24 SSD	**Shelf SAS da 12 GB (DS224C) completamente caricati con 24 SSD**
Numero massimo di host SAP HANA per shelf di dischi	4	14

> Questo calcolo è indipendente dal controller di storage utilizzato. L'aggiunta di più shelf di dischi non aumenta il numero massimo di host SAP HANA supportati da uno storage controller.

Shelf NS224 NVMe

Un SSD NVMe (dati) supporta fino a 2 host SAP HANA. Gli SSD e gli host SAP HANA devono essere equamente distribuiti tra entrambi i controller di storage.

Carichi di lavoro misti

Sono supportati SAP HANA e altri carichi di lavoro applicativi eseguiti sullo stesso storage controller o nello stesso aggregato di storage. Tuttavia, è una Best practice di NetApp separare i workload SAP HANA da tutti gli altri workload delle applicazioni.

Potresti decidere di implementare workload SAP HANA e altri workload applicativi sullo stesso storage controller o sullo stesso aggregato. In tal caso, è necessario assicurarsi che siano sempre disponibili performance sufficienti per SAP HANA all'interno dell'ambiente di workload misto. NetApp consiglia inoltre di utilizzare i parametri della qualità del servizio (QoS) per regolare l'impatto che queste altre applicazioni potrebbero avere sulle applicazioni SAP HANA.

Il tool di test SAP HCMT deve essere utilizzato per verificare se è possibile eseguire altri host SAP HANA su uno storage controller già utilizzato per altri carichi di lavoro. Tuttavia, i server applicativi SAP possono essere posizionati in modo sicuro sullo stesso storage controller e aggregati dei database SAP HANA.

Considerazioni sulla capacità

Una descrizione dettagliata dei requisiti di capacità per SAP HANA è disponibile nella "Nota SAP 1900823" white paper.

> Il dimensionamento della capacità del panorama SAP complessivo con più sistemi SAP HANA deve essere determinato utilizzando gli strumenti di dimensionamento dello storage SAP HANA di NetApp. Contatta NetApp o il tuo partner commerciale NetApp per convalidare il processo di dimensionamento dello storage per un ambiente di storage di dimensioni adeguate.

Configurazione dello strumento di test delle performance

A partire da SAP HANA 1.0 SPS10, SAP ha introdotto i parametri per regolare il comportamento di i/o e ottimizzare il database per il file e il sistema storage utilizzati. Questi parametri devono essere impostati anche per lo strumento di test delle performance di SAP (fsperf) quando le performance dello storage vengono testate utilizzando lo strumento di test SAP.

I test delle performance sono stati condotti da NetApp per definire i valori ottimali. La seguente tabella elenca i parametri che devono essere impostati nel file di configurazione dello strumento di test SAP.

Parametro	Valore
max_parallel_io_requests	128
async_read_submit	acceso
async_write_submit_active	acceso
async_write_submit_blocks	tutto

Per ulteriori informazioni sulla configurazione dello strumento di test SAP, vedere "Nota SAP 1943937" Per HWCCT (SAP HANA 1.0) e. "Nota SAP 2493172" PER HCMT/HCOT (SAP HANA 2.0).

Nell'esempio seguente viene illustrato come impostare le variabili per il piano di esecuzione HCMT/HCOT.

```
…{
          "Comment": "Log Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
          "Name": "LogAsyncReadSubmit",
          "Value": "on",
          "Request": "false"
      },
      {
```

```
         "Comment": "Data Volume: Controls whether read requests are
submitted asynchronously, default is 'on'",
         "Name": "DataAsyncReadSubmit",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "LogAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls whether write requests can be
submitted asynchronously",
         "Name": "DataAsyncWriteSubmitActive",
         "Value": "on",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "LogAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Controls which blocks are written
asynchronously. Only relevant if AsyncWriteSubmitActive is 'on' or 'auto'
and file system is flagged as requiring asynchronous write submits",
         "Name": "DataAsyncWriteSubmitBlocks",
         "Value": "all",
         "Request": "false"
      },
      {
         "Comment": "Log Volume: Maximum number of parallel I/O requests
per completion queue",
         "Name": "LogExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      },
      {
         "Comment": "Data Volume: Maximum number of parallel I/O requests
per completion queue",
```

```
         "Name": "DataExtMaxParallelIoRequests",
         "Value": "128",
         "Request": "false"
      }, …
```

Queste variabili devono essere utilizzate per la configurazione del test. Questo è solitamente il caso dei piani di esecuzione predefiniti che SAP offre con lo strumento HCMT/HCOT. Il seguente esempio per un test di scrittura del log 4k è da un piano di esecuzione.

```
…
      {
         "ID": "D664D001-933D-41DE-A904F304AEB67906",
         "Note": "File System Write Test",
         "ExecutionVariants": [
            {
               "ScaleOut": {
                  "Port": "${RemotePort}",
                  "Hosts": "${Hosts}",
                  "ConcurrentExecution": "${FSConcurrentExecution}"
               },
               "RepeatCount": "${TestRepeatCount}",
               "Description": "4K Block, Log Volume 5GB, Overwrite",
               "Hint": "Log",
               "InputVector": {
                  "BlockSize": 4096,
                  "DirectoryName": "${LogVolume}",
                  "FileOverwrite": true,
                  "FileSize": 5368709120,
                  "RandomAccess": false,
                  "RandomData": true,
                  "AsyncReadSubmit": "${LogAsyncReadSubmit}",
                  "AsyncWriteSubmitActive":
"${LogAsyncWriteSubmitActive}",
                  "AsyncWriteSubmitBlocks":
"${LogAsyncWriteSubmitBlocks}",
                  "ExtMaxParallelIoRequests":
"${LogExtMaxParallelIoRequests}",
                  "ExtMaxSubmitBatchSize": "${LogExtMaxSubmitBatchSize}",
                  "ExtMinSubmitBatchSize": "${LogExtMinSubmitBatchSize}",
                  "ExtNumCompletionQueues":
"${LogExtNumCompletionQueues}",
                  "ExtNumSubmitQueues": "${LogExtNumSubmitQueues}",
                  "ExtSizeKernelIoQueue": "${ExtSizeKernelIoQueue}"
               }
            }, …
```

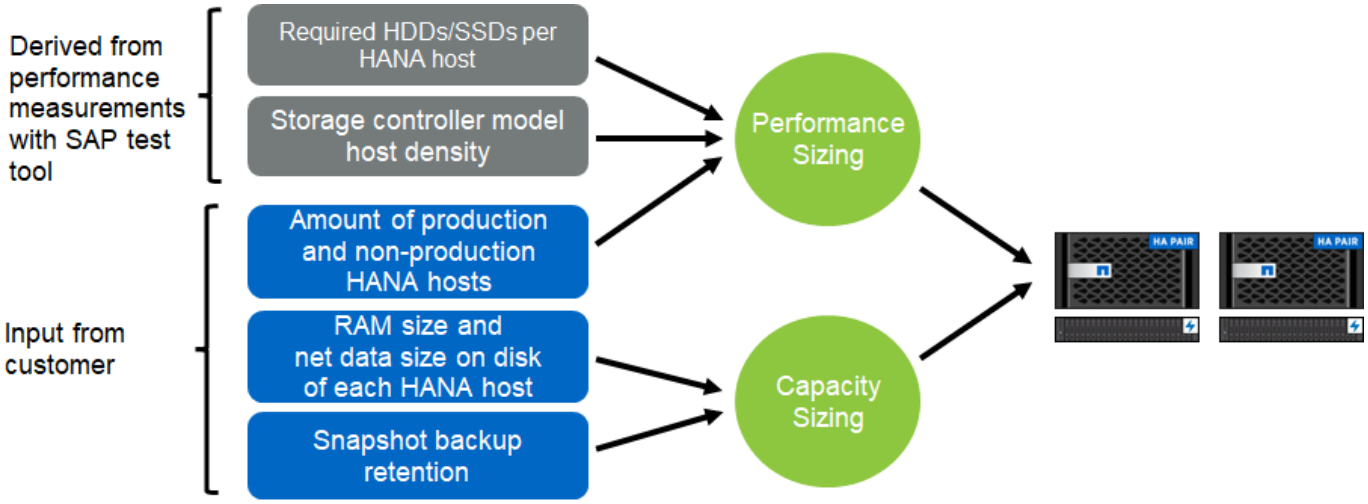
Panoramica del processo di dimensionamento dello storage

Il numero di dischi per host HANA e la densità host SAP HANA per ciascun modello di storage sono stati determinati con il tool di test SAP HANA.

Il processo di dimensionamento richiede dettagli come il numero di host SAP HANA in produzione e non in produzione, la dimensione della RAM di ciascun host e il periodo di conservazione del backup delle copie Snapshot basate sullo storage. Il numero di host SAP HANA determina il controller dello storage e il numero di dischi necessari.

Le dimensioni della RAM, le dimensioni nette dei dati sul disco di ciascun host SAP HANA e il periodo di conservazione del backup delle copie Snapshot vengono utilizzati come input durante il dimensionamento della capacità.

La figura seguente riassume il processo di dimensionamento.



Installazione e configurazione dell'infrastruttura

Le seguenti sezioni forniscono le linee guida per la configurazione e la configurazione dell'infrastruttura SAP HANA e descrivono tutti i passaggi necessari per configurare un sistema SAP HANA. All'interno di queste sezioni, vengono utilizzate le seguenti configurazioni di esempio:

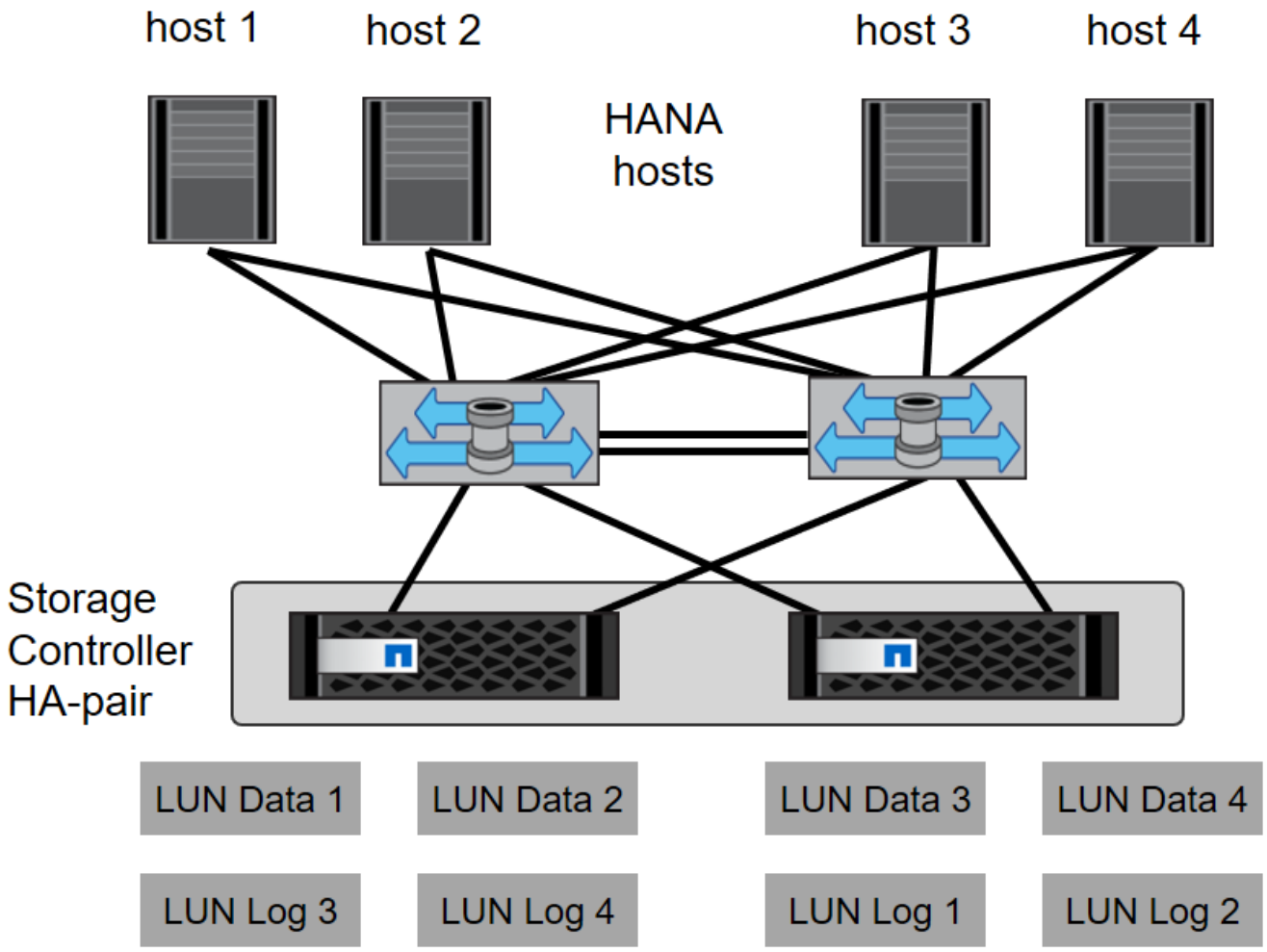
- Sistema HANA con SID=FC5
  - Host singolo e multiplo SAP HANA che utilizza il gestore dei volumi logici Linux (LVM)
  - Host singolo SAP HANA con partizioni multiple SAP HANA

Configurazione del fabric SAN

Ogni server SAP HANA deve disporre di una connessione SAN FCP ridondante con una larghezza di banda minima di 8 Gbps. Per ogni host SAP HANA collegato a un controller di storage, è necessario configurare almeno 8 Gbps di larghezza di banda nel controller di storage.

La figura seguente mostra un esempio con quattro host SAP HANA collegati a due storage controller. Ciascun host SAP HANA dispone di due porte FCP collegate al fabric ridondante. A livello di storage, quattro porte FCP

sono configurate per fornire il throughput richiesto per ciascun host SAP HANA.



Oltre alla suddivisione in zone sul layer dello switch, è necessario mappare ogni LUN del sistema di storage agli host che si connettono a questo LUN. Mantenere lo zoning sullo switch semplice, ovvero definire un set di zone in cui tutti gli HBA host possano vedere tutti gli HBA dei controller.

Sincronizzazione dell'ora

È necessario sincronizzare l'ora tra i controller di storage e gli host del database SAP HANA. È necessario impostare lo stesso server di riferimento orario per tutti i controller di storage e per tutti gli host SAP HANA.

Configurazione dello storage controller

Questa sezione descrive la configurazione del sistema storage NetApp. È necessario completare l'installazione e la configurazione primaria in base alle corrispondenti guide di configurazione e configurazione di ONTAP.

Efficienza dello storage

La deduplica inline, la deduplica inline di più volumi, la compressione inline e la compaction inline sono supportate con SAP HANA in una configurazione SSD.

L'abilitazione delle funzioni di efficienza dello storage in una configurazione HDD non è supportata.

Volumi NetApp FlexGroup

L'utilizzo dei volumi NetApp FlexGroup non è supportato per SAP HANA. Grazie all'architettura di SAP HANA l'utilizzo di FlexGroup Volumes non fornisce alcun beneficio e potrebbe causare problemi di performance.

Crittografia dei volumi e degli aggregati NetApp

L'utilizzo di NetApp Volume Encryption (NVE) e NetApp aggregate Encryption (NAE) sono supportati con SAP HANA.

Qualità del servizio

La qualità del servizio può essere utilizzata per limitare il throughput dello storage per sistemi SAP HANA o applicazioni non SAP specifici su un controller condiviso.

Produzione e sviluppo/test

Un caso d'utilizzo sarebbe quello di limitare il throughput dei sistemi di sviluppo e test in modo che non possano influenzare i sistemi di produzione in una configurazione mista. Durante il processo di dimensionamento, è necessario determinare i requisiti di performance di un sistema non in produzione. I sistemi di sviluppo e test possono essere dimensionati con valori di performance inferiori, in genere nell'intervallo compreso tra il 20% e il 50% di un KPI del sistema di produzione come definito da SAP. L'i/o di scrittura di grandi dimensioni ha il maggiore effetto sulle performance del sistema storage. Pertanto, il limite di throughput QoS deve essere impostato su una percentuale dei corrispondenti valori KPI di scrittura delle performance dello storage SAP HANA nei volumi di dati e di log.

Ambienti condivisi

Un altro caso d'utilizzo consiste nel limitare il throughput dei carichi di lavoro intensivi in scrittura, soprattutto per evitare che questi carichi di lavoro abbiano un impatto su altri carichi di lavoro in scrittura sensibili alla latenza. In tali ambienti è consigliabile applicare una policy di gruppo QoS con un livello di throughput massimo non condiviso a ogni LUN all'interno di ciascuna Storage Virtual Machine (SVM) per limitare il throughput massimo di ciascun oggetto storage singolo a un valore dato. Questo riduce la possibilità che un singolo carico di lavoro possa influenzare negativamente altri carichi di lavoro.

Per fare questo, è necessario creare una policy di gruppo utilizzando l'interfaccia a riga di comando del cluster ONTAP per ogni SVM:

```
qos policy-group create -policy-group <policy-name> -vserver <vserver
name> -max-throughput 1000MB/s -is-shared false
```

E applicata a ogni LUN all'interno della SVM. Segue un esempio di applicazione del gruppo di policy a tutte le LUN esistenti all'interno di una SVM:

```
lun modify -vserver <vserver name>  -path * -qos-policy-group  <policy-
name>
```

Tutto questo è necessario per ogni SVM. Il nome del gruppo di polizia della QoS per ciascuna SVM deve essere diverso. Per i nuovi LUN, la policy può essere applicata direttamente:

```
lun create -vserver <vserver_name> -path  /vol/<volume_name>/<lun_name>
-size <size> -ostype <e.g. linux>  -qos-policy-group <policy-name>
```

Si consiglia di utilizzare 1000 MB/s come velocità massima per una determinata LUN. Se un'applicazione richiede una maggiore capacità di elaborazione, è necessario utilizzare più LUN con striping LUN per fornire la larghezza di banda necessaria. Questa guida fornisce un esempio per SAP HANA basato su Linux LVM nella sezione"Host Setup (impostazione host)" .

> Il limite si applica anche alle letture. Pertanto, utilizza un numero sufficiente di LUN per soddisfare gli SLA richiesti per l'avvio del database SAP HANA e per i backup.

NetApp FabricPool

La tecnologia NetApp FabricPool non deve essere utilizzata per i file system primari attivi nei sistemi SAP HANA. Sono inclusi i file system per l'area dei dati e dei log, oltre a `/hana/shared` file system. In questo modo si ottengono performance imprevedibili, in particolare durante l'avvio di un sistema SAP HANA.

È possibile utilizzare la policy di tiering "snapshot-only" e FabricPool in generale in una destinazione di backup come SnapVault o SnapMirror.

> L'utilizzo di FabricPool per tiering delle copie Snapshot nello storage primario o l'utilizzo di FabricPool in una destinazione di backup modifica il tempo necessario per il ripristino e il ripristino di un database o di altre attività, come la creazione di cloni di sistema o la riparazione di sistemi. Prendetevi in considerazione questo aspetto per pianificare la strategia di gestione del ciclo di vita generale e verificate che gli SLA vengano ancora rispettati durante l'utilizzo di questa funzione.

FabricPool è un'ottima opzione per spostare i backup dei log in un altro Tier di storage. Lo spostamento dei backup influisce sul tempo necessario per ripristinare un database SAP HANA. Pertanto, l'opzione "tiering-minimum-cooling-days" deve essere impostata su un valore che colloca i backup dei log, normalmente necessari per il recovery, sul Tier di storage veloce locale.

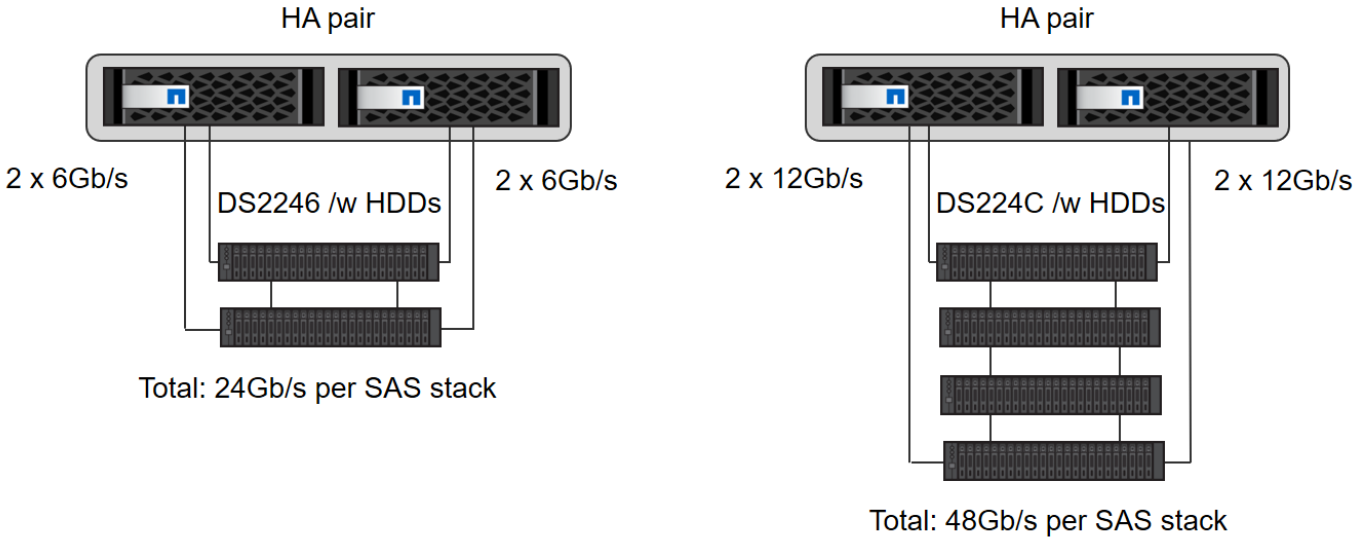
Configurare lo storage

La seguente panoramica riassume i passaggi necessari per la configurazione dello storage. Ogni fase viene descritta in maggiore dettaglio nelle sezioni successive. Prima di iniziare questa procedura, completare la configurazione dell'hardware dello storage, l'installazione del software ONTAP e la connessione delle porte FCP dello storage al fabric SAN.

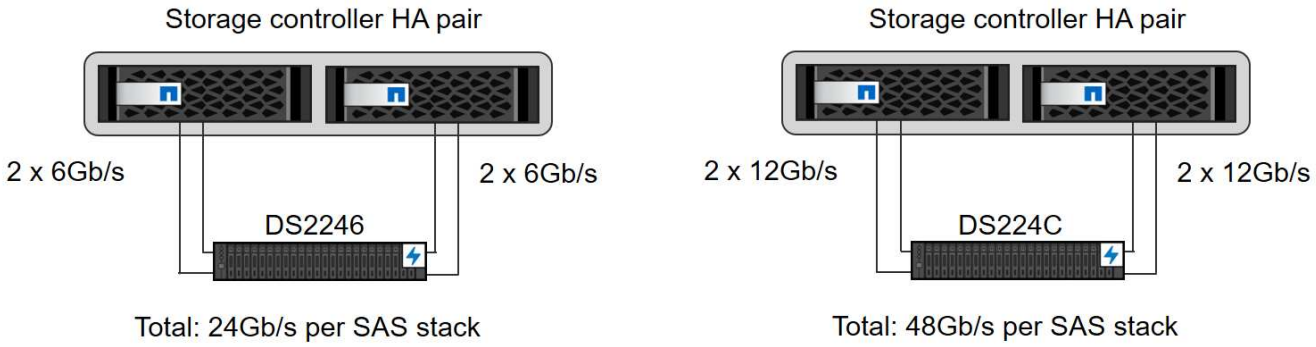
1. Controllare la corretta configurazione dello scaffale del disco, come descritto inCollegamenti del ripiano del disco .
2. Creare e configurare gli aggregati richiesti, come descritto in Configurazione dell'aggregato.
3. Creare una Storage Virtual Machine (SVM), come descritto in Configurazione della macchina virtuale per lo storage.
4. Creare interfacce logiche (LIF), come descritto in Configurazione dell'interfaccia logica.
5. Creare gruppi iniziatori (igroup) con nomi globali (WWN) dei server HANA come descritto nella sezione xref:./bp/hana-fas-fc-storage-controller-setup.html#Initiator-groups Gruppi di iniziatori.
6. Creare e configurare volumi e LUN all'interno degli aggregati come descritto nella sezione "Configurazione host singolo" per singoli host o in sezione "Configurazione host multipli" per più host

Collegamenti del ripiano del disco

Con gli HDD, è possibile collegare un massimo di due shelf di dischi DS2246 o quattro shelf di dischi DS224C a uno stack SAS per fornire le prestazioni richieste per gli host SAP HANA, come mostrato nella figura seguente. I dischi all'interno di ogni shelf devono essere distribuiti in modo uguale a entrambi i controller della coppia ha.

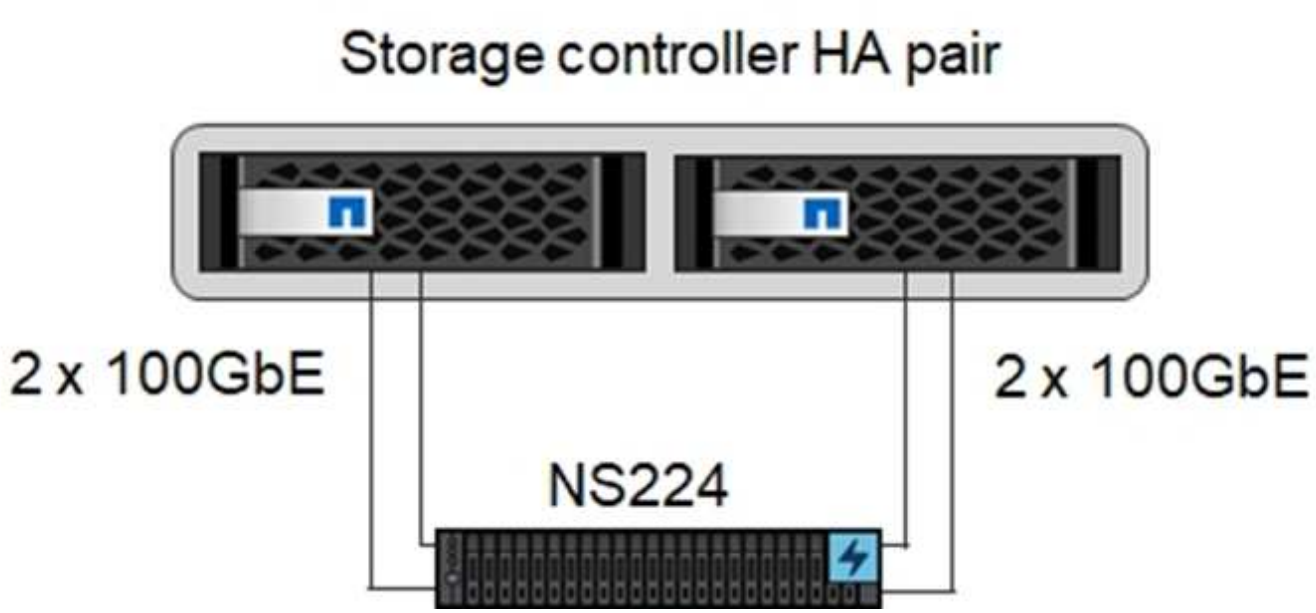


Con gli SSD, è possibile collegare un massimo di uno shelf di dischi a uno stack SAS per fornire le prestazioni richieste per gli host SAP HANA, come mostrato nella figura seguente. I dischi all'interno di ogni shelf devono essere distribuiti in modo uguale a entrambi i controller della coppia ha. Con lo shelf di dischi DS224C, è possibile utilizzare anche il cablaggio SAS quad-path, ma non è necessario.



Scaffali per dischi NVMe

Ogni shelf di dischi NS224 NVMe è collegato a due porte 100GbE per controller, come illustrato nella figura seguente. I dischi all'interno di ogni shelf devono essere distribuiti in modo uguale a entrambi i controller della coppia ha.

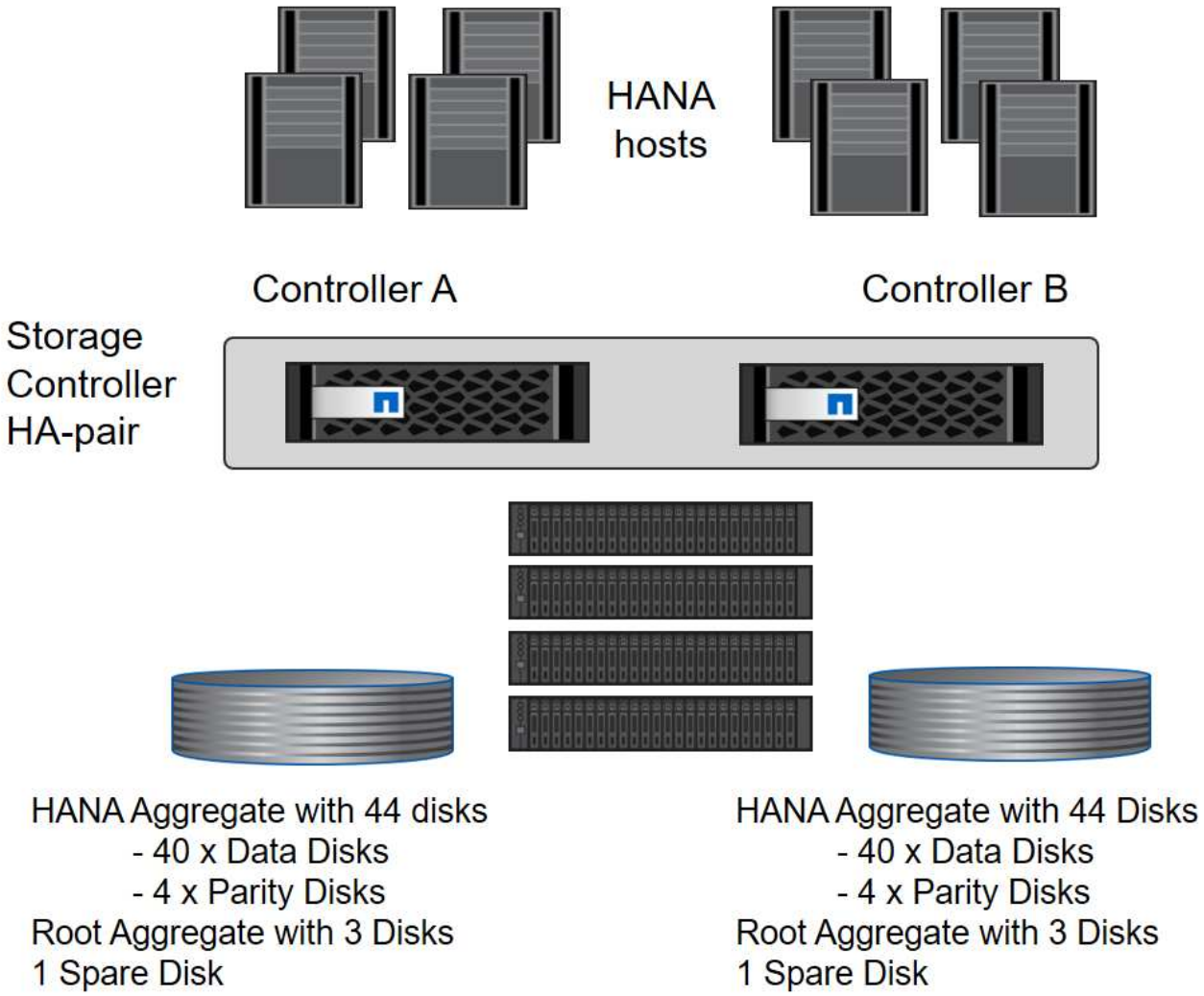


Configurazione dell'aggregato

In generale, è necessario configurare due aggregati per controller, indipendentemente da quale shelf di dischi o tecnologia di dischi (SSD o HDD) viene utilizzata. Questo passaggio è necessario per poter utilizzare tutte le risorse del controller disponibili. Per i sistemi FAS serie 2000, è sufficiente un aggregato di dati.

Configurazione aggregata con HDD

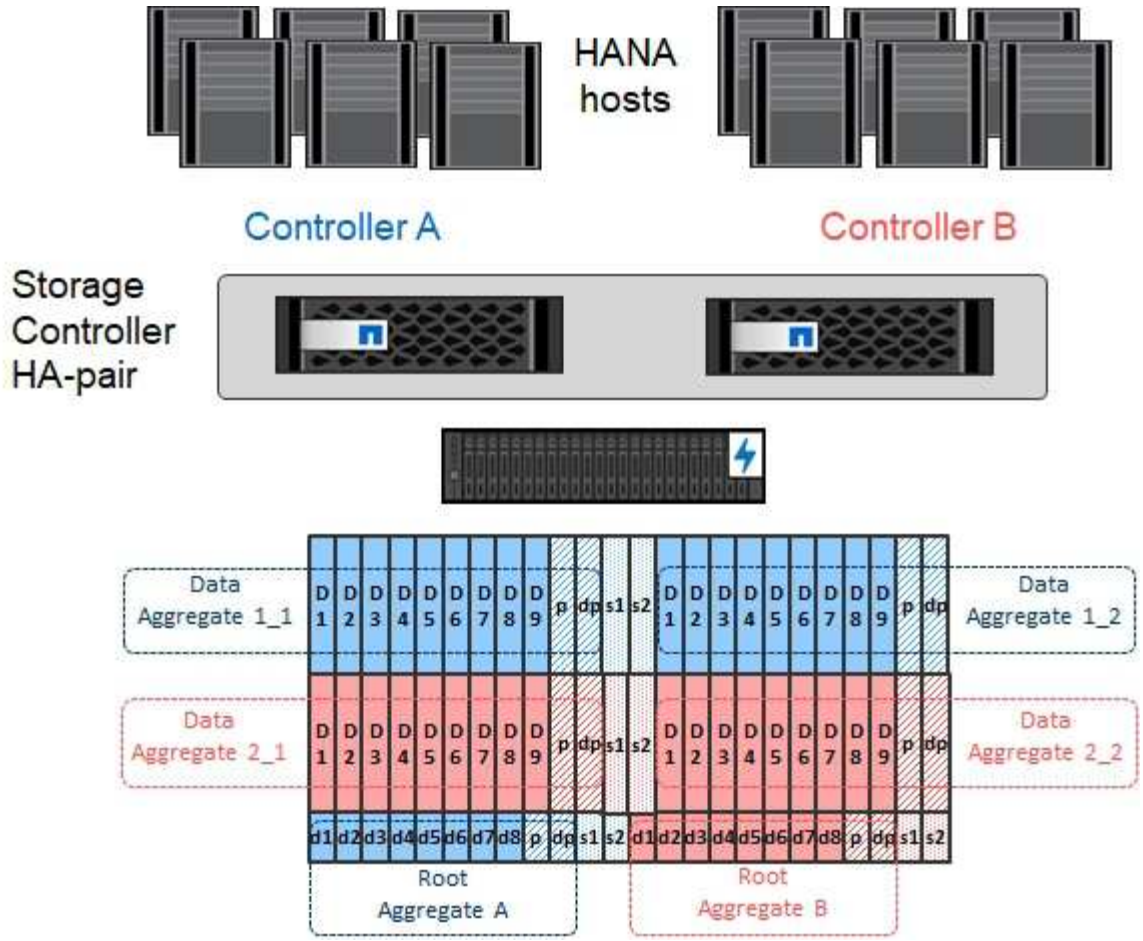
La figura seguente mostra una configurazione per otto host SAP HANA. Quattro host SAP HANA sono collegati a ciascun controller di storage. Vengono configurati due aggregati separati, uno per ciascun controller di storage. Ogni aggregato è configurato con 4 × 10 = 40 dischi dati (HDD).



Configurazione aggregata con sistemi solo SDD

In generale, è necessario configurare due aggregati per controller, indipendentemente da quale shelf di dischi o tecnologia di dischi (SSD o HDD) viene utilizzata.

La figura seguente mostra una configurazione di 12 host SAP HANA in esecuzione su uno shelf SAS da 12 GB configurato con ADPv2. Sei host SAP HANA sono collegati a ciascun controller di storage. Sono configurati quattro aggregati separati, due per ogni controller di storage. Ogni aggregato è configurato con 11 dischi con nove partizioni di dati e due di dischi di parità. Per ciascun controller sono disponibili due partizioni di riserva.

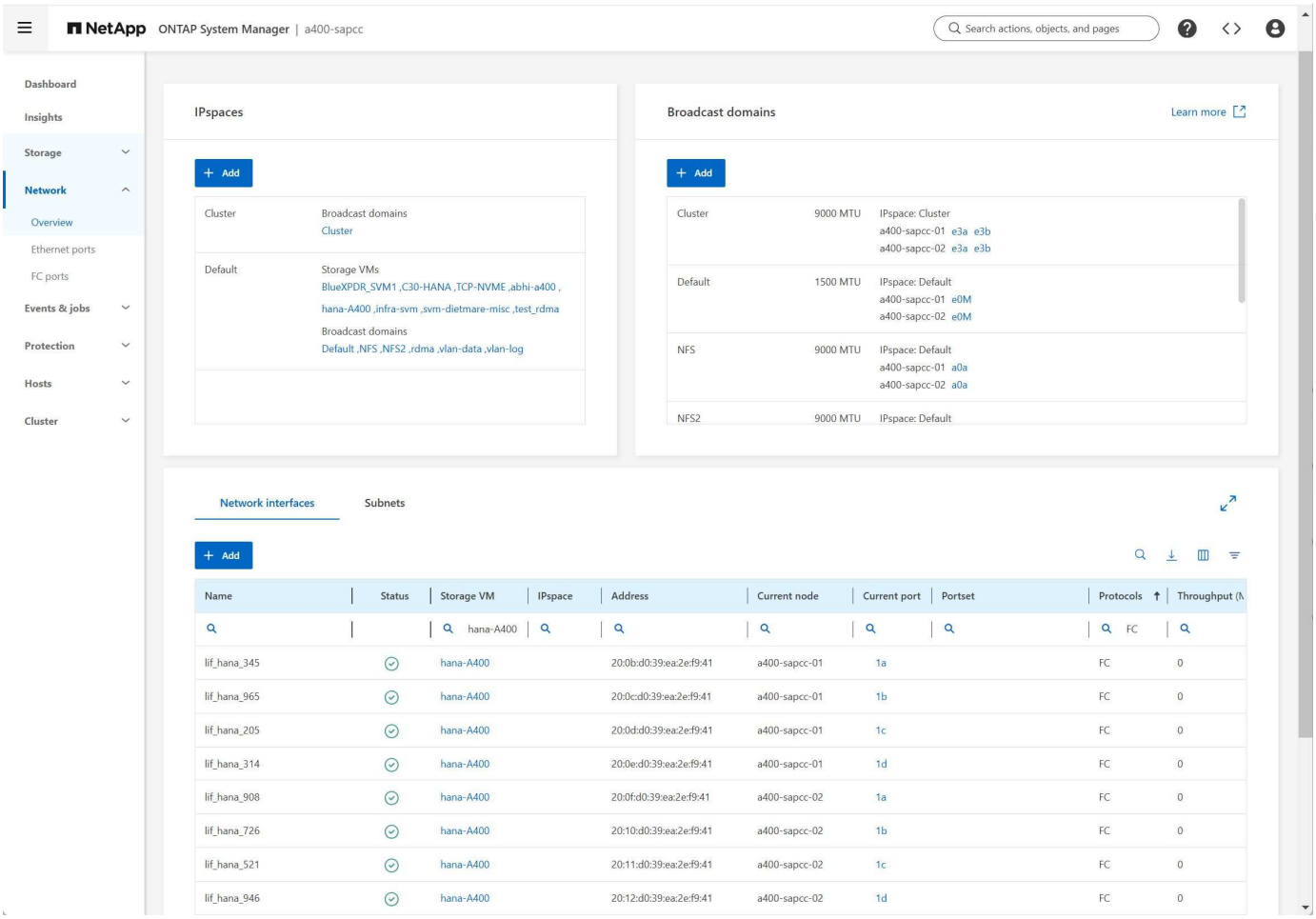


Configurazione della macchina virtuale per lo storage

Gli ambienti SAP multihost con database SAP HANA possono utilizzare una singola SVM. Se necessario, è possibile assegnare una SVM a ciascun ambiente SAP nel caso in cui sia gestita da diversi team all'interno di un'azienda. Le schermate e gli output dei comandi in questo documento utilizzano una SVM denominata `hana`.

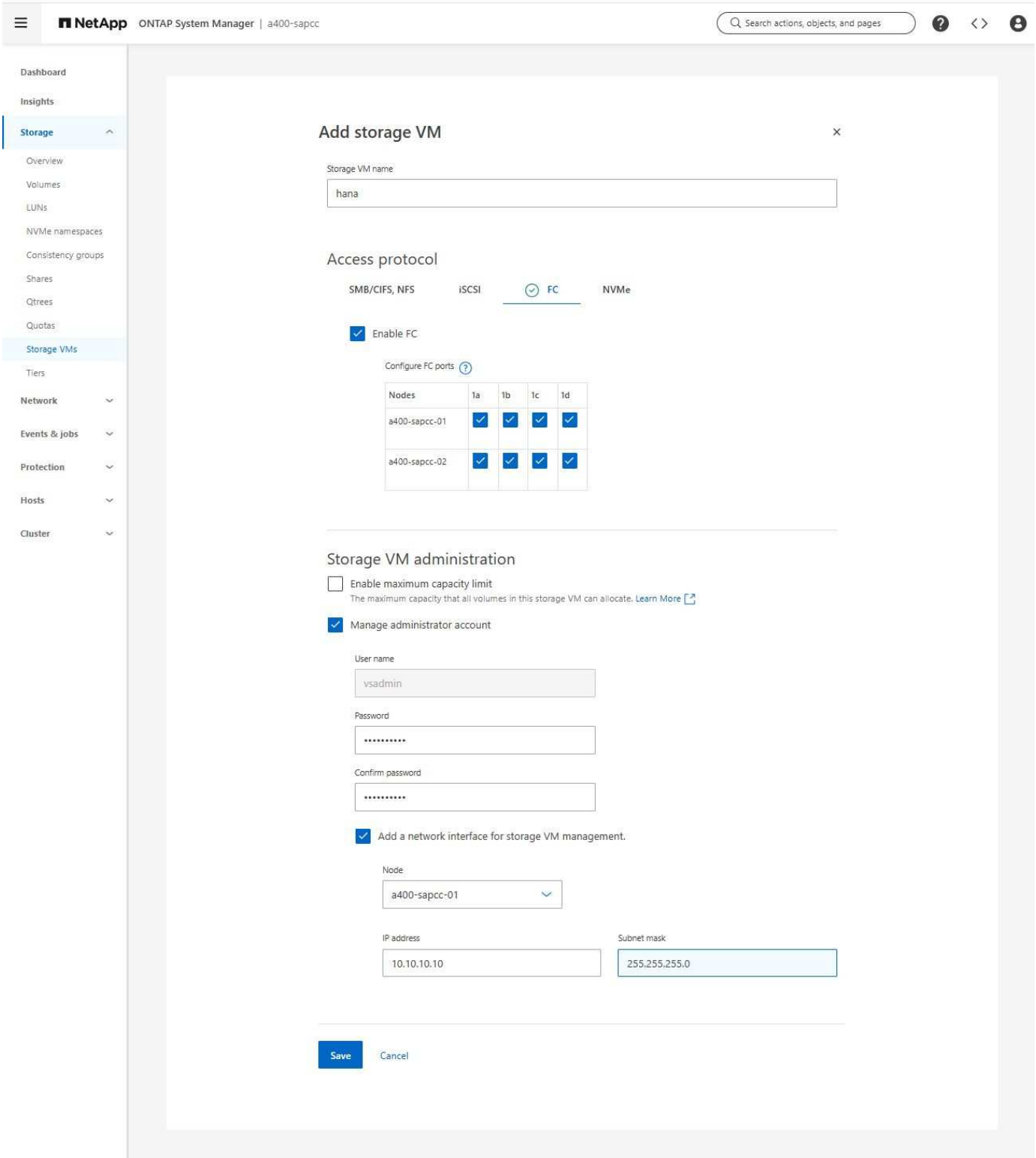
Configurazione dell'interfaccia logica

All'interno della configurazione del cluster di storage, è necessario creare un'interfaccia di rete (LIF) e assegnarla a una porta FCP dedicata. Se, ad esempio, sono necessarie quattro porte FCP per motivi di performance, è necessario creare quattro LIF. La figura seguente mostra uno screenshot degli otto LIF configurati nella SVM.



Durante la creazione di SVM con Gestore di sistema di ONTAP 9, è possibile selezionare tutte le porte FCP fisiche richieste e creare automaticamente una LIF per porta fisica.

La figura seguente illustra la creazione di SVM e LIF con ONTAP System Manager.



Gruppi di iniziatori

È possibile configurare un igroup per ciascun server o per un gruppo di server che richiedono l'accesso a un LUN. La configurazione di igroup richiede i nomi delle porte mondiali (WWPN) dei server.

Utilizzando il `sanlun` Eseguire il seguente comando per ottenere le WWPN di ciascun host SAP HANA:

```
stlrx300s8-6:~ # sanlun fcp show adapter
/sbin/udevadm
/sbin/udevadm

host0 ..... WWPN:2100000e1e163700
host1 ..... WWPN:2100000e1e163701
```

`sanlun`Lo strumento fa parte delle utilità host NetApp e deve essere installato su ogni host SAP HANA. Ulteriori dettagli sono disponibili nella sezione "Configurazione dell'host."

I gruppi iniziatori possono essere creati utilizzando l'interfaccia CLI del cluster ONTAP.

```
lun igroup create -igroup <igroup name> -protocol fcp -ostype linux
-initiator <list of initiators> -vserver <SVM name>
```

Host singolo

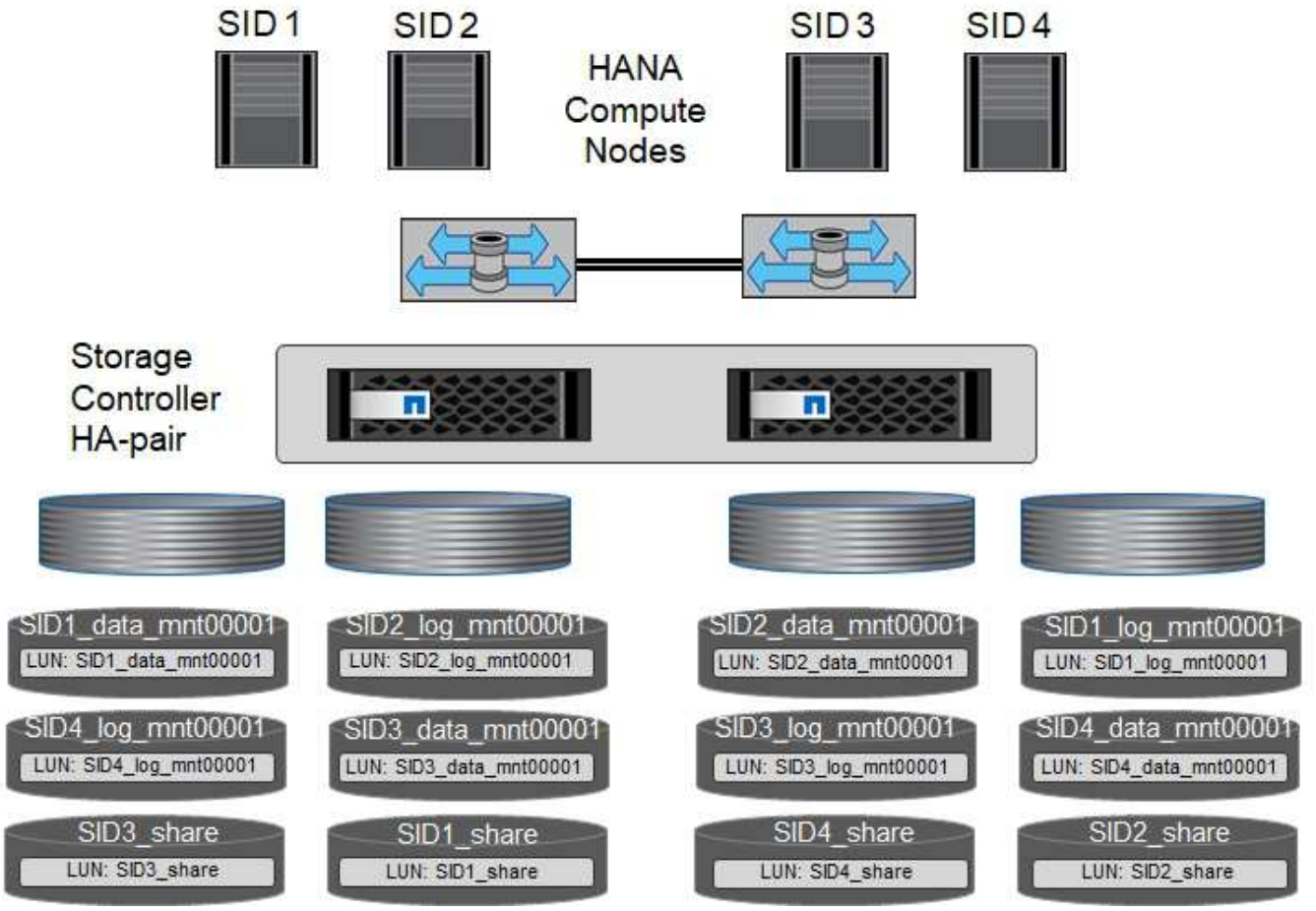
Host singolo

Questa sezione descrive la configurazione del sistema di archiviazione NetApp specifico per i sistemi SAP HANA a host singolo

Configurazione di volumi e LUN per sistemi SAP HANA a host singolo

La figura seguente mostra la configurazione dei volumi di quattro sistemi SAP HANA a host singolo. I volumi di dati e log di ciascun sistema SAP HANA vengono distribuiti a diversi storage controller. Ad esempio, il volume `SID1_data_mnt00001` è configurato sul controller A e il volume `SID1_log_mnt00001` sul controller B. all'interno di ciascun volume, viene configurato un singolo LUN.

Se per i sistemi SAP HANA viene utilizzato un solo storage controller di una coppia ad alta disponibilità (ha), è possibile memorizzare volumi di dati e volumi di log nello stesso storage controller.



Per ogni host SAP HANA, un volume di dati, un volume di log e un volume per `/hana/shared` sono configurati. La seguente tabella mostra una configurazione di esempio con quattro sistemi SAP HANA a host singolo.

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Dati, log e volumi condivisi per il sistema SID1	Volume di dati: SID1_data_mnt00001	Volume condiviso: SID1_shared	–	Volume di log: SID1_log_mnt00001
Dati, log e volumi condivisi per il sistema SID2	–	Volume di log: SID2_log_mnt00001	Volume di dati: SID2_data_mnt00001	Volume condiviso: SID2_shared
Dati, log e volumi condivisi per il sistema SID3	Volume condiviso: SID3_shared	Volume di dati: SID3_data_mnt00001	Volume di log: SID3_log_mnt00001	–
Dati, log e volumi condivisi per il sistema SID4	Volume di log: SID4_log_mnt00001	–	Volume condiviso: SID4_shared	Volume di dati: SID4_data_mnt00001

La tabella seguente mostra un esempio di configurazione del punto di montaggio per un sistema a host singolo.

LUN	Punto di montaggio sull'host HANA	Nota
SID1_data_mnt00001	/hana/data/SID1/mnt00001	Montato usando /etc/fstab entry
SID1_log_mnt00001	/hana/log/SID1/mnt00001	Montato usando /etc/fstab entry
SID1_shared	/hana/shared/SID1	Montato usando /etc/fstab entry

Con la configurazione descritta, il `/usr/sap/SID1` La directory in cui è memorizzata la home directory predefinita dell'utente SID1adm si trova sul disco locale. In una configurazione di disaster recovery con replica basata su disco, NetApp consiglia di creare un LUN aggiuntivo all'interno di `SID1_shared` volume per `/usr/sap/SID1` directory in modo che tutti i file system si trovino nello storage centrale.

Configurazione di volumi e LUN per sistemi SAP HANA a host singolo che utilizzano Linux LVM

Linux LVM può essere utilizzato per aumentare le performance e risolvere i limiti delle dimensioni del LUN. Le diverse LUN di un gruppo di volumi LVM devono essere memorizzate in un aggregato diverso e in un controller diverso. La seguente tabella mostra un esempio di due LUN per gruppo di volumi.

Non è necessario utilizzare LVM con più LUN per soddisfare i KPI SAP HANA, ma è consigliato

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Dati, log e volumi condivisi per sistemi basati su LVM	Volume di dati: SID1_data_mnt00001	Volume condiviso: Volume SID1_shared log2: SID1_log2_mnt00001	Volume Data2: SID1_data2_mnt00001	Volume di log: SID1_log_mnt00001

Con la configurazione descritta, il `/usr/sap/SID1` La directory in cui è memorizzata la home directory predefinita dell'utente SID1adm si trova sul disco locale. In una configurazione di disaster recovery con replica basata su disco, NetApp consiglia di creare un LUN aggiuntivo all'interno di `SID1_shared` volume per `/usr/sap/SID1` directory in modo che tutti i file system si trovino nello storage centrale.

Opzioni del volume

Le opzioni del volume elencate nella tabella seguente devono essere verificate e impostate su tutti i volumi utilizzati per SAP HANA.

Azione	ONTAP 9
Disattivare le copie Snapshot automatiche	vol modify –vserver <vserver-name> -volume <volname> -snapshot-policy none
Disattiva la visibilità della directory Snapshot	vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false

Creazione di LUN, volumi e mappatura delle LUN ai gruppi di iniziatori

Puoi utilizzare NetApp ONTAP System Manager per creare volumi di storage e LUN e associarli agli igroup dei server e all'interfaccia a riga di comando di ONTAP. In questa guida viene descritto l'utilizzo della CLI.

Creazione di LUN, volumi e mappatura di LUN in igroups utilizzando la CLI

Questa sezione mostra un esempio di configurazione mediante la riga di comando con ONTAP 9 per un sistema host singolo SAP HANA con SID FC5 mediante LVM e due LUN per gruppo di volumi LVM:

1. Creare tutti i volumi necessari.

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. Creare tutte le LUN.

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. Creare il gruppo iniziatore per tutte le porte appartenenti agli host sythe di FC5.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb -vserver hana
```

4. Mappare tutti i LUN al gruppo iniziatore creato.

```
lun map -path /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
```

Più host

Più host

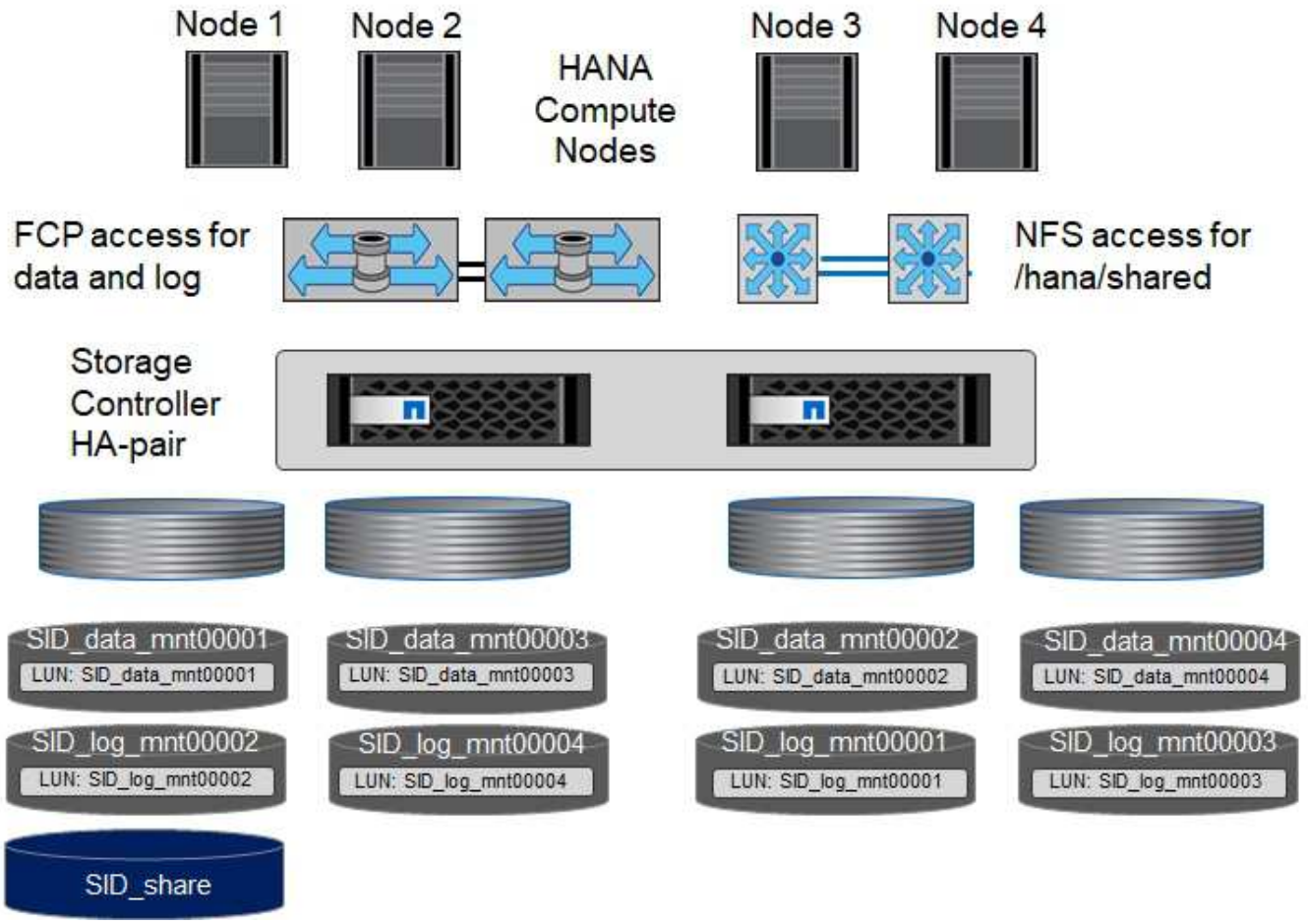
Questa sezione descrive la configurazione del sistema di archiviazione NetApp specifico per i sistemi multi-host SAP HANA

Configurazione di volumi e LUN per sistemi SAP HANA con host multipli

La figura seguente mostra la configurazione di un volume di un sistema SAP HANA 4+1 multihost. I volumi di dati e i volumi di log di ciascun host SAP HANA vengono distribuiti a diversi storage controller. Ad esempio, il volume `SID_data_mnt00001` È configurato sul controller A e sul volume `SID_log_mnt00001` È configurato sul controller B. Viene configurato un LUN per ciascun volume.

Il `/hana/shared` Il volume deve essere accessibile da tutti gli host HANA e viene quindi esportato utilizzando NFS. Anche se non sono disponibili KPI specifici per le performance per `/hana/shared` File system, NetApp consiglia di utilizzare una connessione Ethernet a 10 GB.

> Se per il sistema SAP HANA viene utilizzato un solo storage controller di una coppia ha, i volumi di dati e log possono essere memorizzati anche sullo stesso storage controller.



Per ogni host SAP HANA, vengono creati un volume di dati e un volume di log. Il `/hana/shared` Il volume viene utilizzato da tutti gli host del sistema SAP HANA. La figura seguente mostra una configurazione di esempio per un sistema SAP HANA 4+1 a host multiplo.

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Volumi di dati e log per il nodo 1	Volume di dati: SID_data_mnt00001	–	Volume di log: SID_log_mnt00001	–
Volumi di dati e log per il nodo 2	Volume di log: SID_log_mnt00002	–	Volume di dati: SID_data_mnt00002	–
Volumi di dati e log per il nodo 3	–	Volume di dati: SID_data_mnt00003	–	Volume di log: SID_log_mnt00003
Volumi di dati e log per il nodo 4	–	Volume di log: SID_log_mnt00004	–	Volume di dati: SID_data_mnt00004
Volume condiviso per tutti gli host	Volume condiviso: SID_shared	–	–	–

La tabella seguente mostra la configurazione e i punti di montaggio di un sistema a più host con quattro host SAP HANA attivi.

LUN o volume	Punto di montaggio sull'host SAP HANA	Nota
LUN: SID_data_mnt00001	/hana/data/SID/mnt00001	Montato utilizzando un connettore storage
LUN: SID_log_mnt00001	/hana/log/SID/mnt00001	Montato utilizzando un connettore storage
LUN: SID_data_mnt00002	/hana/data/SID/mnt00002	Montato utilizzando un connettore storage
LUN: SID_log_mnt00002	/hana/log/SID/mnt00002	Montato utilizzando un connettore storage
LUN: SID_data_mnt00003	/hana/data/SID/mnt00003	Montato utilizzando un connettore storage
LUN: SID_log_mnt00003	/hana/log/SID/mnt00003	Montato utilizzando un connettore storage
LUN: SID_data_mnt00004	/hana/data/SID/mnt00004	Montato utilizzando un connettore storage
LUN: SID_log_mnt00004	/hana/log/SID/mnt00004	Montato utilizzando un connettore storage
Volume: SID_shared	/hana/shared/SID	Montato su tutti gli host usando NFS e /etc/fstab entry

Con la configurazione descritta, la `/usr/sap/SID` directory in cui è memorizzata la home directory predefinita dell'utente sidadm si trova sul disco locale per ogni host HANA. In una configurazione di disaster recovery con replica basata su disco, NetApp consiglia di creare quattro sottodirectory aggiuntive nel `SID_shared` volume per il `/usr/sap/SID` file system, in modo che ogni host del database abbia tutti i propri file system sullo storage centrale.

Configurazione di volumi e LUN per sistemi SAP HANA con host multipli che utilizzano Linux LVM

Linux LVM può essere utilizzato per aumentare le performance e risolvere i limiti delle dimensioni del LUN. Le diverse LUN di un gruppo di volumi LVM devono essere memorizzate in un aggregato diverso e in un controller diverso. La seguente tabella mostra un esempio di due LUN per gruppo di volumi per un sistema host multiplo SAP HANA 2+1.

Non è necessario utilizzare LVM per combinare più LUN per soddisfare i KPI di SAP HANA, ma è consigliato.

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Volumi di dati e log per il nodo 1	Volume di dati: SID_data_mnt00001	Volume log2: SID_log2_mnt00001	Volume di log: SID_log_mnt00001	Volume Data2: SID_data2_mnt00001
Volumi di dati e log per il nodo 2	Volume log2: SID_log2_mnt00002	Volume di dati: SID_data_mnt00002	Volume Data2: SID_data2_mnt00002	Volume di log: SID_log_mnt00002

Scopo	Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Volume condiviso per tutti gli host	Volume condiviso: SID_shared	–	–	–

Opzioni del volume

Le opzioni del volume elencate nella tabella seguente devono essere verificate e impostate su tutti i volumi utilizzati per SAP HANA.

Azione	ONTAP 9
Disattivare le copie Snapshot automatiche	vol modify –vserver <vserver-name> -volume <volname> -snapshot-policy none
Disattiva la visibilità della directory Snapshot	vol modify -vserver <vserver-name> -volume <volname> -snapdir-access false

Creazione di LUN, volumi e mappatura delle LUN ai gruppi di iniziatori

Puoi utilizzare NetApp ONTAP System Manager per creare volumi di storage e LUN e associarli agli igroup dei server e all'interfaccia a riga di comando di ONTAP. In questa guida viene descritto l'utilizzo della CLI.

Creazione di LUN, volumi e mappatura di LUN in igroups utilizzando la CLI

Questa sezione mostra una configurazione di esempio utilizzando la riga di comando con ONTAP 9 per un sistema host 2+1 SAP HANA con SID FC5 utilizzando LVM e due LUN per gruppo di volumi LVM.

1. Creare tutti i volumi necessari.

```
vol create -volume FC5_data_mnt00001 -aggregate aggr1_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00002  -aggregate aggr2_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_log_mnt00001  -aggregate aggr1_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data_mnt00002  -aggregate aggr2_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_data2_mnt00001 -aggregate aggr1_2 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00002  -aggregate aggr2_2 -size 280g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_log2_mnt00001  -aggregate aggr1_1 -size 280g
-snapshot-policy none -foreground true -encrypt false  -space-guarantee
none
vol create -volume FC5_data2_mnt00002  -aggregate aggr2_1 -size 1200g
-snapshot-policy none -foreground true -encrypt false -space-guarantee
none
vol create -volume FC5_shared -aggregate aggr1_1 -size 512g -state
online -policy default -snapshot-policy none -junction-path /FC5_shared
-encrypt false  -space-guarantee none
```

2. Creare tutte le LUN.

```
lun create -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001   -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data_mnt00002/FC5_data_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002 -size 1t
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00001/FC5_log_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log_mnt00002/FC5_log_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
lun create -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002 -size 260g
-ostype linux -space-reserve disabled -space-allocation disabled -class
regular
```

3. Creare l'igroup per tutti i server appartenenti al sistema FC5.

```
lun igroup create -igroup HANA-FC5 -protocol fcp -ostype linux
-initiator 10000090fadcc5fa,10000090fadcc5fb,
10000090fadcc5c1,10000090fadcc5c2,  10000090fadcc5c3,10000090fadcc5c4
-vserver hana
```

4. Mappare tutti i LUN all'igroup creato.

```
lun map -path  /vol/FC5_data_mnt00001/FC5_data_mnt00001    -igroup HANA-
FC5
lun map -path /vol/FC5_data2_mnt00001/FC5_data2_mnt00001  -igroup HANA-
FC5
lun map -path /vol/FC5_data_mnt00002/FC5_data_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_data2_mnt00002/FC5_data2_mnt00002  -igroup HANA-
FC5
lun map -path /vol/FC5_log_mnt00001/FC5_log_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00001/FC5_log2_mnt00001  -igroup HANA-FC5
lun map -path /vol/FC5_log_mnt00002/FC5_log_mnt00002  -igroup HANA-FC5
lun map -path /vol/FC5_log2_mnt00002/FC5_log2_mnt00002  -igroup HANA-FC5
```

API di SAP HANA storage Connector

Un connettore di storage è richiesto solo in ambienti con più host dotati di funzionalità di failover. In configurazioni con più host, SAP HANA offre funzionalità ad alta disponibilità in modo che un host di database SAP HANA possa eseguire il failover su un host in standby. In questo caso, l'host di standby accede e utilizza i LUN dell'host guasto. Il connettore di storage viene utilizzato per garantire l'accesso attivo a una partizione di storage da parte di un solo host di database alla volta.

Nelle configurazioni di host multipli SAP HANA con storage NetApp, viene utilizzato il connettore di storage standard fornito da SAP. La "SAP HANA FC Storage Connector Admin Guide" è disponibile come allegato a. "Nota SAP 1900823".

Configurazione dell'host

Prima di configurare l'host, è necessario scaricare NetApp SAN host Utilities da "Supporto NetApp" E installato sui server HANA. La documentazione dell'utility host contiene informazioni sul software aggiuntivo che deve essere installato in base all'HBA FCP utilizzato.

La documentazione contiene anche informazioni sulle configurazioni multipath specifiche per la versione di Linux utilizzata. Questo documento illustra le procedure di configurazione richieste per SLES 15 e Red Hat Enterprise Linux 7.6 o versioni successive, come descritto nella "Guida all'installazione e all'installazione di Linux host Utilities 7.1".

Configurare il multipathing

> ⓘ I passaggi da 1 a 6 devono essere eseguiti su tutti gli host worker e standby nella configurazione di più host SAP HANA.

Per configurare il multipathing, attenersi alla seguente procedura:

1. Eseguire Linux `rescan-scsi-bus.sh -a` Su ciascun server per rilevare nuove LUN.
2. Eseguire `sanlun lun show` Controllare e verificare che tutti i LUN richiesti siano visibili. Nell'esempio riportato di seguito viene illustrato il `sanlun lun show` Output di comando per un sistema HANA 2+1

multi-host con due LUN di dati e due LUN di log. L'output mostra i LUN e i file di periferica corrispondenti, ad esempio il LUN `SS3_data_mnt00001` e il file del dispositivo `/dev/sdag`. Ogni LUN dispone di otto percorsi FC dall'host ai controller dello storage.

```
sapcc-hana-tst:~ # sanlun lun show
controller(7mode/E-Series)/                                    device
host                  lun
vserver(cDOT/FlashRay)        lun-pathname                     filename
adapter    protocol   size    product
------------------------------------------------------------------------
-------------------------------------
svm1                          FC5_log2_mnt00002                /dev/sdbb
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdba
host21     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001                /dev/sdaz
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001                 /dev/sday
host21     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002               /dev/sdax
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002                /dev/sdaw
host21     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001               /dev/sdav
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001                /dev/sdau
host21     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002                /dev/sdat
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdas
host21     FCP        500g    cDOT
svm1                          FC5_log2_mnt00001                /dev/sdar
host21     FCP        500g    cDOT
svm1                          FC5_log_mnt00001                 /dev/sdaq
host21     FCP        500g    cDOT
svm1                          FC5_data2_mnt00002               /dev/sdap
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00002                /dev/sdao
host21     FCP        1t      cDOT
svm1                          FC5_data2_mnt00001               /dev/sdan
host21     FCP        1t      cDOT
svm1                          FC5_data_mnt00001                /dev/sdam
host21     FCP        1t      cDOT
svm1                          FC5_log2_mnt00002                /dev/sdal
host20     FCP        500g    cDOT
svm1                          FC5_log_mnt00002                 /dev/sdak
```

```
host20     FCP         500g    cDOT
svm1                           FC5_log2_mnt00001              /dev/sdaj
host20     FCP         500g    cDOT
svm1                           FC5_log_mnt00001               /dev/sdai
host20     FCP         500g    cDOT
svm1                           FC5_data2_mnt00002             /dev/sdah
host20     FCP         1t      cDOT
svm1                           FC5_data_mnt00002              /dev/sdag
host20     FCP         1t      cDOT
svm1                           FC5_data2_mnt00001             /dev/sdaf
host20     FCP         1t      cDOT
svm1                           FC5_data_mnt00001              /dev/sdae
host20     FCP         1t      cDOT
svm1                           FC5_log2_mnt00002              /dev/sdad
host20     FCP         500g    cDOT
svm1                           FC5_log_mnt00002               /dev/sdac
host20     FCP         500g    cDOT
svm1                           FC5_log2_mnt00001              /dev/sdab
host20     FCP         500g    cDOT
svm1                           FC5_log_mnt00001               /dev/sdaa
host20     FCP         500g    cDOT
svm1                           FC5_data2_mnt00002             /dev/sdz
host20     FCP         1t      cDOT
svm1                           FC5_data_mnt00002              /dev/sdy
host20     FCP         1t      cDOT
svm1                           FC5_data2_mnt00001             /dev/sdx
host20     FCP         1t      cDOT
svm1                           FC5_data_mnt00001              /dev/sdw
host20     FCP         1t      cDOT
```

3. Esegui il `multipath -r` E `multipath -ll` comando per ottenere gli identificatori mondiali (WWID) per i nomi dei file del dispositivo.

   In questo esempio ci sono otto LUN.

```
sapcc-hana-tst:~ # multipath -r
sapcc-hana-tst:~ # multipath -ll
3600a098038314e63492b59326b4b786d dm-7 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
```

```
3600a098038314e63492b59326b4b786e dm-9 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
3600a098038314e63492b59326b4b786f dm-11 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
3600a098038314e63492b59326b4b7870 dm-13 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
3600a098038314e63532459326d495a64 dm-6 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
3600a098038314e63532459326d495a65 dm-8 NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
3600a098038314e63532459326d495a66 dm-10 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
```

```
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
3600a098038314e63532459326d495a67 dm-12 NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

4. Modificare il `/etc/multipath.conf` File e aggiungere i WWID e i nomi degli alias.

> L'output di esempio mostra il contenuto di `/etc/multipath.conf` File, che include nomi alias per le quattro LUN di un sistema a più host 2+1. Se non è disponibile alcun file multipath.conf, è possibile crearne uno eseguendo il seguente comando: `multipath -T > /etc/multipath.conf`.

```
sapcc-hana-tst:/ # cat /etc/multipath.conf
multipaths {
                multipath {
                wwid    3600a098038314e63492b59326b4b786d
                alias   svm1-FC5_data2_mnt00001
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786e
                alias   svm1-FC5_data2_mnt00002
        }
        multipath {
                wwid    3600a098038314e63532459326d495a64
                alias   svm1-FC5_data_mnt00001
        }
        multipath {
                wwid    3600a098038314e63532459326d495a65
                alias   svm1-FC5_data_mnt00002
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b786f
                alias   svm1-FC5_log2_mnt00001
        }
        multipath {
                wwid    3600a098038314e63492b59326b4b7870
                alias   svm1-FC5_log2_mnt00002
        }
        multipath {
                wwid    3600a098038314e63532459326d495a66
                alias   svm1-FC5_log_mnt00001
        }
        multipath {
                wwid    3600a098038314e63532459326d495a67
                alias   svm1-FC5_log_mnt00002
        }


}
```

5. Eseguire `multipath -r` comando per ricaricare la mappa del dispositivo.
6. Verificare la configurazione eseguendo `multipath -ll` Per elencare tutti i LUN, i nomi degli alias e i percorsi attivi e di standby.

> Il seguente esempio di output mostra l'output di un sistema HANA 2+1 multihost con due LUN di dati e due di log.

```
sapcc-hana-tst:~ # multipath -ll
hsvm1-FC5_data2_mnt00001 (3600a098038314e63492b59326b4b786d) dm-7
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:2 sdaf 65:240 active ready running
  |- 20:0:5:2 sdx  65:112 active ready running
  |- 21:0:4:2 sdav 66:240 active ready running
  `- 21:0:6:2 sdan 66:112 active ready running
svm1-FC5_data2_mnt00002 (3600a098038314e63492b59326b4b786e) dm-9
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:4 sdah 66:16  active ready running
  |- 20:0:5:4 sdz  65:144 active ready running
  |- 21:0:4:4 sdax 67:16  active ready running
  `- 21:0:6:4 sdap 66:144 active ready running
svm1-FC5_data_mnt00001 (3600a098038314e63532459326d495a64) dm-6
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:1 sdae 65:224 active ready running
  |- 20:0:5:1 sdw  65:96  active ready running
  |- 21:0:4:1 sdau 66:224 active ready running
  `- 21:0:6:1 sdam 66:96  active ready running
svm1-FC5_data_mnt00002 (3600a098038314e63532459326d495a65) dm-8
NETAPP,LUN C-Mode
size=1.0T features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:3 sdag 66:0   active ready running
  |- 20:0:5:3 sdy  65:128 active ready running
  |- 21:0:4:3 sdaw 67:0   active ready running
  `- 21:0:6:3 sdao 66:128 active ready running
svm1-FC5_log2_mnt00001 (3600a098038314e63492b59326b4b786f) dm-11
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:6 sdaj 66:48  active ready running
  |- 20:0:5:6 sdab 65:176 active ready running
  |- 21:0:4:6 sdaz 67:48  active ready running
  `- 21:0:6:6 sdar 66:176 active ready running
```

```
svm1-FC5_log2_mnt00002 (3600a098038314e63492b59326b4b7870) dm-13
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:8 sdal 66:80  active ready running
  |- 20:0:5:8 sdad 65:208 active ready running
  |- 21:0:4:8 sdbb 67:80  active ready running
  `- 21:0:6:8 sdat 66:208 active ready running
svm1-FC5_log_mnt00001 (3600a098038314e63532459326d495a66) dm-10
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:5 sdai 66:32  active ready running
  |- 20:0:5:5 sdaa 65:160 active ready running
  |- 21:0:4:5 sday 67:32  active ready running
  `- 21:0:6:5 sdaq 66:160 active ready running
svm1-FC5_log_mnt00002 (3600a098038314e63532459326d495a67) dm-12
NETAPP,LUN C-Mode
size=500G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
  |- 20:0:4:7 sdak 66:64  active ready running
  |- 20:0:5:7 sdac 65:192 active ready running
  |- 21:0:4:7 sdba 67:64  active ready running
  `- 21:0:6:7 sdas 66:192 active ready running
```

Configurazione host singolo

Configurazione host singolo

In questo capitolo viene descritta la configurazione di un singolo host SAP HANA utilizzando Linux LVM.

Configurazione LUN per sistemi SAP HANA a host singolo

Nell'host SAP HANA, è necessario creare e montare gruppi di volumi e volumi logici, come indicato nella tabella seguente.

Volume logico/LUN	Punto di montaggio sull'host SAP HANA	Nota
LV: FC5_data_mnt0000-vol	/hana/data/FC51/mnt00001	Montato usando /etc/fstab entry
LV: FC5_log_mnt00001-vol	/hana/log/FC5/mnt00001	Montato usando /etc/fstab entry
LUN: FC5_shared	/hana/shared/FC5	Montato usando /etc/fstab entry

Con la configurazione descritta, il `/usr/sap/FC5` la directory in cui è memorizzata la directory home predefinita dell'utente FC5adm si trova sul disco locale. In una configurazione di disaster recovery con replica basata su disco, NetApp consiglia di creare un LUN aggiuntivo all'interno di `FC5_shared` volume per il `/usr/sap/FC5` directory in modo che tutti i file system siano nella memoria centrale.

Creare gruppi di volumi LVM e volumi logici

1. Inizializzare tutti i LUN come volume fisico.

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001
```

2. Creare i gruppi di volumi per ciascuna partizione di dati e log.

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
```

3. Creare un volume logico per ciascuna partizione di dati e log. Utilizzare una dimensione dello stripe uguale al numero di LUN utilizzati per gruppo di volumi (in questo esempio, due) e una dimensione dello stripe di 256k per i dati e 64k per il registro. SAP supporta un solo volume logico per gruppo di volumi.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Eseguire la scansione dei volumi fisici, dei gruppi di volumi e dei gruppi di volumi di tutti gli altri host.

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

Se questi comandi non trovano i volumi, è necessario riavviare il sistema.

Per montare i volumi logici, è necessario attivare i volumi logici. Per attivare i volumi, eseguire il seguente comando:

```
vgchange -a y
```

Creare file system

Creare il file system XFS su tutti i volumi logici di dati e log e sulla LUN condivisa hana.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs /dev/mapper/svm1-FC5_shared
```

Creare punti di montaggio

Creare le directory dei punti di montaggio richiesti e impostare le autorizzazioni sull'host del database:

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod –R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod –R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

Montare i file system

Per montare i file system durante l'avvio del sistema utilizzando `/etc/fstab` file di configurazione, aggiungere i file system richiesti al `/etc/fstab` file di configurazione:

```
# cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/FC5_log_mnt00001-vol /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/FC5_data_mnt00001-vol /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
```

I file system XFS per i LUN di dati e log devono essere montati con `relatime` e. `inode64` opzioni di montaggio.

Per montare i file system, eseguire il comando `mount –a` comando sull'host.

Configurazione di più host

Configurazione di più host

In questo capitolo viene descritta a titolo di esempio la configurazione di un sistema multihost SAP HANA 2+1.

Configurazione LUN per sistemi multi-host SAP HANA

Nell'host SAP HANA, è necessario creare e montare gruppi di volumi e volumi logici, come indicato nella tabella seguente.

Volume logico (LV) o volume	Punto di montaggio sull'host SAP HANA	Nota
LV: FC5_data_mnt00001-vol	/hana/data/FC5/mnt00001	Montato utilizzando un connettore storage
LV: FC5_log_mnt00001-vol	/hana/log/FC5/mnt00001	Montato utilizzando un connettore storage
LV: FC5_data_mnt00002-vol	/hana/data/FC5/mnt00002	Montato utilizzando un connettore storage
LV: FC5_log_mnt00002-vol	/hana/log/FC5/mnt00002	Montato utilizzando un connettore storage
Volume: FC5_shared	/hana/shared	Montato su tutti gli host usando NFS e /etc/fstab entry

Con la configurazione descritta, il `/usr/sap/FC5` La directory in cui è memorizzata la directory home predefinita dell'utente FC5adm si trova sul disco locale di ciascun host HANA. In una configurazione di disaster recovery con replica basata su disco, NetApp consiglia di creare quattro sottodirectory aggiuntive in `FC5_shared` volume per il `/usr/sap/FC5` file system in modo che ogni host del database abbia tutti i suoi file system sullo storage centrale.

Creare gruppi di volumi LVM e volumi logici

1. Inizializzare tutti i LUN come volume fisico.

```
pvcreate /dev/mapper/hana-FC5_data_mnt00001
pvcreate /dev/mapper/hana-FC5_data2_mnt00001
pvcreate /dev/mapper/hana-FC5_data_mnt00002
pvcreate /dev/mapper/hana-FC5_data2_mnt00002
pvcreate /dev/mapper/hana-FC5_log_mnt00001
pvcreate /dev/mapper/hana-FC5_log2_mnt00001
pvcreate /dev/mapper/hana-FC5_log_mnt00002
pvcreate /dev/mapper/hana-FC5_log2_mnt00002
```

2. Creare i gruppi di volumi per ciascuna partizione di dati e log.

```
vgcreate FC5_data_mnt00001 /dev/mapper/hana-FC5_data_mnt00001
/dev/mapper/hana-FC5_data2_mnt00001
vgcreate FC5_data_mnt00002 /dev/mapper/hana-FC5_data_mnt00002
/dev/mapper/hana-FC5_data2_mnt00002
vgcreate FC5_log_mnt00001 /dev/mapper/hana-FC5_log_mnt00001
/dev/mapper/hana-FC5_log2_mnt00001
vgcreate FC5_log_mnt00002 /dev/mapper/hana-FC5_log_mnt00002
/dev/mapper/hana-FC5_log2_mnt00002
```

3. Creare un volume logico per ciascuna partizione di dati e log. Utilizzare una dimensione dello stripe uguale al numero di LUN utilizzati per gruppo di volumi (in questo esempio, due) e una dimensione dello stripe di 256k per i dati e 64k per il registro. SAP supporta un solo volume logico per gruppo di volumi.

```
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00001
lvcreate --extents 100%FREE -i 2 -I 256k --name vol FC5_data_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00002
lvcreate --extents 100%FREE -i 2 -I 64k --name vol FC5_log_mnt00001
```

4. Eseguire la scansione dei volumi fisici, dei gruppi di volumi e dei gruppi di volumi di tutti gli altri host.

```
modprobe dm_mod
pvscan
vgscan
lvscan
```

Se questi comandi non trovano i volumi, è necessario riavviare il sistema.

Per montare i volumi logici, è necessario attivare i volumi logici. Per attivare i volumi, eseguire il seguente comando:

```
vgchange -a y
```

Creare file system

Creare il file system XFS su tutti i volumi logici di dati e log.

```
mkfs.xfs FC5_data_mnt00001-vol
mkfs.xfs FC5_data_mnt00002-vol
mkfs.xfs FC5_log_mnt00001-vol
mkfs.xfs FC5_log_mnt00002-vol
```

Creare punti di montaggio

Crea le directory dei punti di montaggio richiesti e imposta le autorizzazioni su tutti gli host worker e standby:

```
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00001
sapcc-hana-tst:/ # mkdir -p /hana/data/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/log/FC5/mnt00002
sapcc-hana-tst:/ # mkdir -p /hana/shared
sapcc-hana-tst:/ # chmod -R 777 /hana/log/FC5
sapcc-hana-tst:/ # chmod -R 777 /hana/data/FC5
sapcc-hana-tst:/ # chmod 777 /hana/shared
```

Montare i file system

Per montare il `/hana/shared` file system durante l'avvio del sistema utilizzando `/etc/fstab` file di configurazione, aggiungere il `/hana/shared` file system al `/etc/fstab` file di configurazione di ciascun host.

```
sapcc-hana-tst:/ # cat /etc/fstab
<storage-ip>:/hana_shared /hana/shared nfs rw,vers=3,hard,timeo=600,
intr,noatime,nolock 0 0
```

Tutti i file system di log e dati vengono montati tramite il connettore storage SAP HANA.

Per montare i file system, eseguire `mount -a` su ciascun host.

Configurazione dello stack di i/o per SAP HANA

A partire da SAP HANA 1.0 SPS10, SAP ha introdotto i parametri per regolare il comportamento di i/o e ottimizzare il database per il file e il sistema storage utilizzati.

NetApp ha condotto test delle performance per definire i valori ideali. La seguente tabella elenca i valori ottimali dedotti dai test delle prestazioni.

Parametro	Valore
max_parallel_io_requests	128
async_read_submit	acceso
async_write_submit_active	acceso
async_write_submit_blocks	tutto

Per i sistemi da SAP HANA 1.0 a SPS12, questi parametri possono essere impostati durante l'installazione del database SAP HANA come descritto nella nota SAP "2267798 – Configurazione del database SAP HANA durante l'installazione con hdbparam".

In alternativa, è possibile impostare i parametri dopo l'installazione del database SAP HANA utilizzando `hdbparam` framework.

```
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.max_parallel_io_requests=128
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_active=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_read_submit=on
SS3adm@stlrx300s8-6:/usr/sap/SS3/HDB00> hdbparam --paramset
fileio.async_write_submit_blocks=all
```

A partire da SAP HANA 2.0, `hdbparam` è obsoleto e i parametri sono stati spostati su `global.ini` file. I parametri possono essere impostati utilizzando i comandi SQL o SAP HANA Studio. Per ulteriori informazioni, consulta la nota SAP "2399079 - eliminazione di hdbparam in HANA 2". I parametri possono essere impostati anche all'interno di `global.ini` file.

```
SS3adm@stlrx300s8-6:/usr/sap/SS3/SYS/global/hdb/custom/config> cat
global.ini
…
[fileio]
async_read_submit = on
async_write_submit_active = on
max_parallel_io_requests = 128
async_write_submit_blocks = all
…
```

Con SAP HANA 2.0 SPS5 e versioni successive, è possibile utilizzare il `setParameter.py `sscript per impostare i parametri sopra indicati.

```
fc5adm@sapcc-hana-tst-03:/usr/sap/FC5/HDB00/exe/python_support>
python setParameter.py
-set=SYSTEM/global.ini/fileio/max_parallel_io_requests=128
python setParameter.py -set=SYSTEM/global.ini/fileio/async_read_submit=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_active=on
python setParameter.py
-set=SYSTEM/global.ini/fileio/async_write_submit_blocks=all
```

Installazione del software SAP HANA

Di seguito sono riportati i requisiti per l'installazione del software SAP HANA.

Installazione su un sistema a host singolo

L'installazione del software SAP HANA non richiede alcuna preparazione aggiuntiva per un sistema a singolo host.

Installazione su sistemi con più host

La seguente procedura di installazione si basa su SAP HANA 1.0 SPS12 o versione successiva.

Prima di iniziare l'installazione, creare un `global.ini` File per abilitare l'utilizzo di SAP Storage Connector durante il processo di installazione. Il connettore di storage SAP monta i file system richiesti sugli host di lavoro durante il processo di installazione. Il `global.ini` il file deve essere disponibile in un file system accessibile da tutti gli host, ad esempio `/hana/shared/SID` file system.

Prima di installare il software SAP HANA su un sistema a più host, è necessario completare la seguente procedura:

1. Aggiungere le seguenti opzioni di montaggio per i LUN dei dati e i LUN del registro a `global.ini` file:
   - `relatime` e. `inode64` per il file system di dati e log
2. Aggiungere i WWID delle partizioni dei dati e dei log. Gli ID WWID devono corrispondere ai nomi alias configurati in `/etc/multipath.conf` file.

   Il seguente output mostra un esempio di configurazione di host multipli 2+1 in cui l'identificatore di sistema (SID) è SS3.

```
stlrx300s8-6:~ # cat /hana/shared/global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/SS3
basepath_logvolumes = /hana/log/SS3
[storage]
ha_provider = hdb_ha.fcClient
partition_*_*__prtype = 5
partition_*_data__mountoptions = -o relatime,inode64
partition_*_log__mountoptions = -o relatime,inode64,nobarrier
partition_1_data__wwid = hana-SS3_data_mnt00001
partition_1_log__wwid = hana-SS3_log_mnt00001
partition_2_data__wwid = hana-SS3_data_mnt00002
partition_2_log__wwid = hana-SS3_log_mnt00002
[system_information]
usage = custom
[trace]
ha_fcclient = info
stlrx300s8-6:~ #
```

   Se si utilizza LVM, la configurazione necessaria è diversa. L'esempio riportato di seguito mostra una configurazione di 2+1 host multipli con SID=FC5.

```
sapcc-hana-tst-03:/hana/shared # cat global.ini
[communication]
listeninterface = .global
[persistence]
basepath_datavolumes = /hana/data/FC5
basepath_logvolumes = /hana/log/FC5
[storage]
ha_provider = hdb_ha.fcClientLVM
partition_*_*__prtype = 5
partition_*_data__mountOptions = -o relatime,inode64
partition_*_log__mountOptions = -o relatime,inode64
partition_1_data__lvmname = FC5_data_mnt00001-vol
partition_1_log__lvmname = FC5_log_mnt00001-vol
partition_2_data__lvmname = FC5_data_mnt00002-vol
partition_2_log__lvmname = FC5_log_mnt00002-vol
sapcc-hana-tst-03:/hana/shared #
```

Utilizzando lo strumento di installazione SAP `hdblcm`, avviare l'installazione eseguendo il comando seguente su uno degli host di lavoro. Utilizzare l' `addhosts`opzione per aggiungere il secondo lavoratore (sapcc-hana-tst-06) e l'host di standby (sapcc-hana-tst-07). La directory in cui è stato memorizzato il file preparato `global.ini` è inclusa con l' `storage_cfg`opzione CLI (--storage_cfg=/hana/shared`). A seconda della versione del sistema operativo in uso, potrebbe essere necessario installare phyton 2.7 prima di installare il database SAP HANA.

```
/hdblcm --action=install --addhosts=sapcc-hana-tst
-06:role=worker:storage_partition=2,sapcc-hana-tst-07:role=standby
--storage_cfg=/hana/shared/

AP HANA Lifecycle Management - SAP HANA Database 2.00.073.00.1695288802
************************************************************************


Scanning software locations...
Detected components:
    SAP HANA AFL (incl.PAL,BFL,OFL) (2.00.073.0000.1695321500) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_AFL_LINUX_X86_64/packages
    SAP HANA Database (2.00.073.00.1695288802) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
    SAP HANA Database Client (2.18.24.1695756995) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/SAP_HANA_CLIENT/client
    SAP HANA Studio (2.3.75.000000) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/HDB_STUDIO_LINUX_X86_64/studio
```

```
    SAP HANA Local Secure Store (2.11.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HANA_LSS_24_LINUX_X86_64/packages
    SAP HANA XS Advanced Runtime (1.1.3.230717145654) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/XSA_RT_10_LINUX_X86_64/packages
    SAP HANA EML AFL (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/HDB_EML_AFL_10_LINUX_X86_64/packages
    SAP HANA EPM-MDS (2.00.073.0000.1695321500) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/SAP_HANA_EPM-MDS_10/packages
    Automated Predictive Library (4.203.2321.0.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-73/DATA_UNITS/PAAPL4_H20_LINUX_X86_64/apl-
4.203.2321.0-hana2sp03-linux_x64/installer/packages
    GUI for HALM for XSA (including product installer) Version 1 (1.015.0)
in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACALMPIUI15_0.zip
    XSAC FILEPROCESSOR 1.0 (1.000.102) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACFILEPROC00_102.zip
    SAP HANA tools for accessing catalog content, data preview, SQL
console, etc. (2.015.230503) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_HRTT_20/XSACHRTT15_230503.zip
    Develop and run portal services for customer applications on XSA
(2.007.0) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACPORTALSERV07_0.zip
    The SAP Web IDE for HANA 2.0 (4.007.0) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSAC_SAP_WEB_IDE_20/XSACSAPWEBIDE07_0.zip
    XS JOB SCHEDULER 1.0 (1.007.22) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACSERVICES07_22.zip
    SAPUI5 FESV6 XSA 1 - SAPUI5 1.71 (1.071.52) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV671_52.zip
    SAPUI5 FESV9 XSA 1 - SAPUI5 1.108 (1.108.5) in /mnt/sapcc-
share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5FESV9108_5.zip
    SAPUI5 SERVICE BROKER XSA 1 - SAPUI5 Service Broker 1.0 (1.000.4) in
/mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACUI5SB00_4.zip
    XSA Cockpit 1 (1.001.37) in /mnt/sapcc-share/software/SAP/HANA2SPS7-
73/DATA_UNITS/XSA_CONTENT_10/XSACXSACOCKPIT01_37.zip


SAP HANA Database version '2.00.073.00.1695288802' will be installed.
```

```
Select additional components for installation:

  Index | Components      | Description

-------------------------------------------------------------------------------
------------------------
  1     | all             | All components
  2     | server          | No additional components
  3     | client          | Install SAP HANA Database Client version
2.18.24.1695756995
  4     | lss             | Install SAP HANA Local Secure Store version
2.11.0
  5     | studio          | Install SAP HANA Studio version 2.3.75.000000
  6     | xs              | Install SAP HANA XS Advanced Runtime version
1.1.3.230717145654
  7     | afl             | Install SAP HANA AFL (incl.PAL,BFL,OFL)
version 2.00.073.0000.1695321500
  8     | eml             | Install SAP HANA EML AFL version
2.00.073.0000.1695321500
  9     | epmmds          | Install SAP HANA EPM-MDS version
2.00.073.0000.1695321500
  10    | sap_afl_sdk_apl | Install Automated Predictive Library version
4.203.2321.0.0

Enter comma-separated list of the selected indices [3,4]: 2,3
```

```
Verify that the installation tool installed all selected components at all
worker and standby hosts.
```

Aggiunta di partizioni di volumi di dati aggiuntive per sistemi SAP HANA a host singolo

A partire da SAP HANA 2.0 SPS4, è possibile configurare ulteriori partizioni del volume di dati. Questa funzione consente di configurare due o più LUN per il volume di dati di un database tenant SAP HANA e di scalare oltre i limiti di dimensioni e performance di una singola LUN.

> Non è necessario utilizzare più partizioni per soddisfare i KPI SAP HANA. Un singolo LUN con una singola partizione soddisfa i KPI richiesti.

> L'utilizzo di due o più LUN singoli per il volume di dati è disponibile solo per i sistemi SAP HANA a host singolo. Il connettore di storage SAP richiesto per i sistemi host multipli SAP HANA supporta un solo dispositivo per il volume di dati.

È possibile aggiungere più partizioni di volumi di dati in qualsiasi momento, ma potrebbe essere necessario riavviare il database SAP HANA.

Attivazione di partizioni di volumi di dati aggiuntive

Per attivare ulteriori partizioni del volume di dati, attenersi alla seguente procedura:

1. Aggiungere la seguente voce all'interno di `global.ini` file:

```
[customizable_functionalities]
persistence_datavolume_partition_multipath = true
```

2. Riavviare il database per attivare la funzione. Aggiunta del parametro tramite SAP HANA Studio a `global.ini` Utilizzando la configurazione Systemdb si impedisce il riavvio del database.

Configurazione del volume e del LUN

Il layout dei volumi e delle LUN è simile al layout di un singolo host con una partizione del volume di dati, ma con un volume di dati e un LUN aggiuntivi memorizzati su un aggregato diverso come volume di log e l'altro volume di dati. La seguente tabella mostra un esempio di configurazione di sistemi SAP HANA a host singolo con due partizioni di volumi di dati.

Aggregato 1 al controller A.	Aggregato 2 al controller A.	Aggregato 1 al controller B.	Aggregato 2 al controller B.
Volume di dati: SID_data_mnt00001	Volume condiviso: SID_shared	Volume di dati: SID_data2_mnt00001	Volume di log: SID_log_mnt00001

La tabella seguente mostra un esempio di configurazione del punto di montaggio per un sistema a host singolo con due partizioni di volumi di dati.

LUN	Punto di montaggio sull'host HANA	Nota
SID_data_mnt00001	/hana/data/SID/mnt00001	Montato usando /etc/fstab entry
SID_data2_mnt00001	/hana/data2/SID/mnt00001	Montato usando /etc/fstab entry
SID_log_mnt00001	/hana/log/SID/mnt00001	Montato usando /etc/fstab entry
SID_shared	/hana/shared/SID	Montato usando /etc/fstab entry

Creare le nuove LUN dei dati utilizzando Gestore di sistema di ONTAP o l'interfaccia utente di ONTAP.

Configurazione dell'host

Per configurare un host, attenersi alla seguente procedura:

1. Configurare il multipathing per le LUN aggiuntive, come descritto nella sezione 0.
2. Creare il file system XFS su ogni LUN aggiuntivo appartenente al sistema HANA.

```
stlrx300s8-6:/ # mkfs.xfs /dev/mapper/hana-FC5_data2_mnt00001
```

3. Aggiungere i file system aggiuntivi a `/etc/fstab` file di configurazione.

I file system XFS per il LUN dei dati devono essere montati con `relatime` e. `inode64` opzioni di montaggio. I file system XFS per il LUN di log devono essere montati con `relatime`, `inode64`, e. `nobarrier` opzioni di montaggio.

```
stlrx300s8-6:/ # cat /etc/fstab
/dev/mapper/hana-FC5_shared /hana/shared xfs defaults 0 0
/dev/mapper/hana-FC5_log_mnt00001 /hana/log/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/hana-FC5_data_mnt00001 /hana/data/FC5/mnt00001 xfs
relatime,inode64 0 0
/dev/mapper/hana-FC5_data2_mnt00001 /hana/data2/FC5/mnt00001 xfs
relatime,inode64 0 0
```

4. Creare i punti di montaggio e impostare le autorizzazioni sull'host del database.

```
stlrx300s8-6:/ # mkdir -p /hana/data2/FC5/mnt00001
stlrx300s8-6:/ # chmod –R 777 /hana/data2/FC5
```

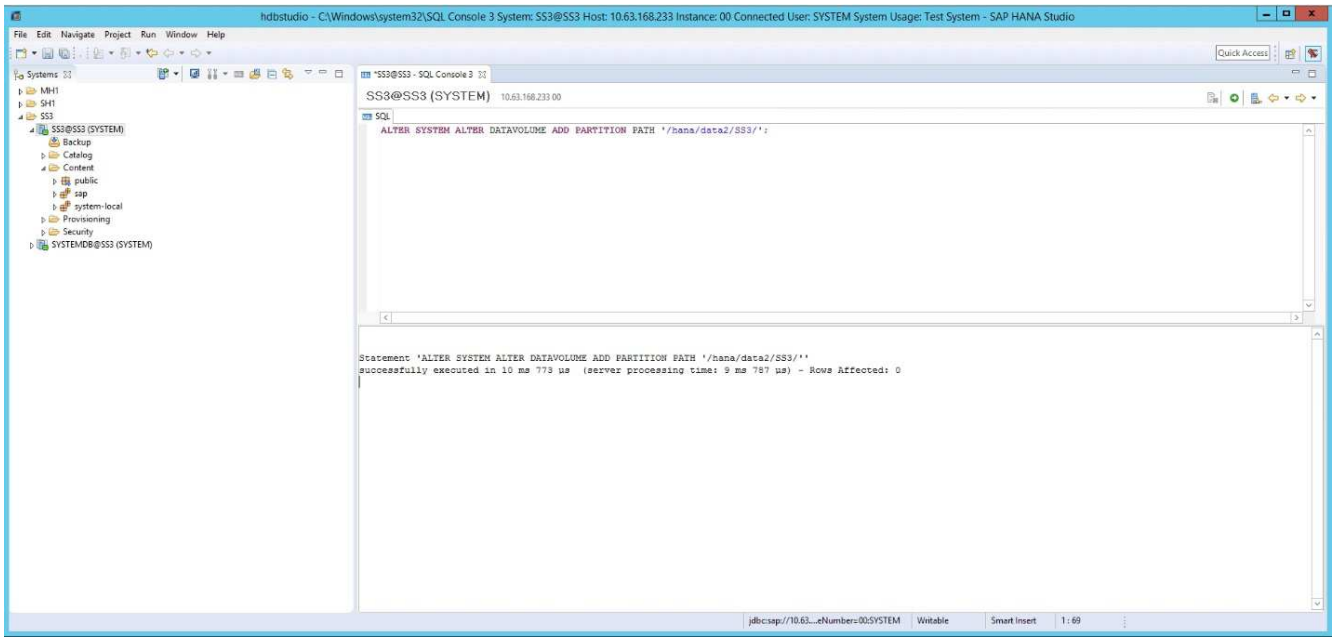
5. Per montare i file system, eseguire `mount –a` comando.

Aggiunta di una partizione datavolume aggiuntiva

Per aggiungere una partizione datavolume aggiuntiva al database tenant, completare la seguente procedura:

1. Eseguire la seguente istruzione SQL sul database tenant. Ogni LUN aggiuntivo può avere un percorso diverso.

```
ALTER SYSTEM ALTER DATAVOLUME ADD PARTITION PATH '/hana/data2/SID/';
```



Dove trovare ulteriori informazioni

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

- "Soluzioni software SAP HANA"
- "TR-4646: Disaster recovery SAP HANA con replica dello storage"
- "TR-4614: Backup e ripristino SAP HANA con SnapCenter"
- "TR-4667: Automatizzazione di copie di sistema SAP con il plug-in SAP HANA SnapCenter"
- Centri di documentazione NetApp

  "https://www.netapp.com/support-and-training/documentation/"
- Hardware per lo storage aziendale certificato SAP per SAP HANA

  "https://www.sap.com/dmc/exp/2014-09-02-hana-hardware/enEN/"
- Requisiti di storage SAP HANA

  "https://www.sap.com/documents/2024/03/146274d3-ae7e-0010-bca6-c68f7e60039b.html"
- SAP HANA - Domande frequenti sull'integrazione personalizzata del data center

  "https://www.sap.com/documents/2016/05/e8705aae-717c-0010-82c7-eda71af511fa.html"
- SAP HANA su VMware vSphere Wiki

  "https://help.sap.com/docs/SUPPORT_CONTENT/virtualization/3362185751.html"
- Guida alle Best practice di SAP HANA su VMware vSphere

  "https://www.vmware.com/docs/sap_hana_on_vmware_vsphere_best_practices_guide-white-paper"

Aggiornare la cronologia

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

Data	Riepilogo degli aggiornamenti
Febbraio 2015	Versione iniziale
Ottobre 2015	Inclusi i parametri i/o per SAP HANA e HWVAL SPS 10 e versioni successive
Febbraio 2016	Dimensionamento della capacità aggiornato
Febbraio 2017	Nuovi sistemi storage e shelf di dischi NetApp nuove funzionalità di ONTAP 9 nuove release di sistemi operativi (SLES12 SP1 e Red Hat Enterprise Linux 7.2) Nuova release di SAP HANA
Luglio 2017	Aggiornamenti minori
Settembre 2018	Nuovi sistemi storage NetApp nuove release dei sistemi operativi (SLES12 SP3 e Red Hat Enterprise Linux 7.4) aggiornamenti minori aggiuntivi SAP HANA 2.0 SPS3
Settembre 2019	Nuove release del sistema operativo aggiornamenti minori
Aprile 2020	Sono state introdotte più funzioni di partizione dei dati disponibili da SAP HANA 2.0 SPS4
Giugno 2020	Ulteriori informazioni sulle funzionalità opzionali aggiornamenti minori
Febbraio 2021	Supporto LVM Linux nuovi sistemi storage NetApp nuove release dei sistemi operativi (SLES15SP2, RHEL 8)
Aprile 2021	Aggiunta di informazioni specifiche su VMware vSphere
Settembre 2022	Nuove versioni del sistema operativo
Settembre 2024	Nuovi sistemi di storage
Febbraio 2025	Nuovo sistema storage
Luglio 2025	Aggiornamenti minori

Backup, ripristino e disaster recovery

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

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

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

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

Backup e ripristino con Amazon FSX per ONTAP

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

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

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

I backup delle copie Snapshot vengono memorizzati sullo stesso sistema di dischi dei dati online attivi.

Pertanto, NetApp consiglia di utilizzare i backup di copia Snapshot come supplemento piuttosto che come 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. È inoltre possibile utilizzare la posizione secondaria se è necessario ripristinare un backup non più disponibile nella posizione principale.

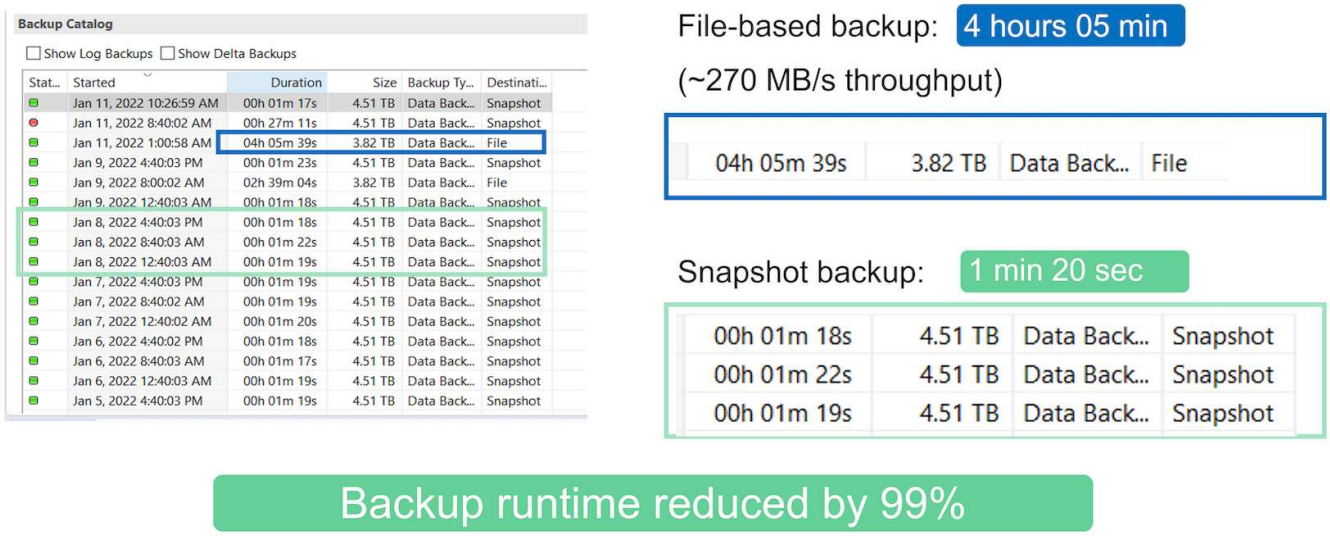
Un backup in una posizione secondaria si basa sulle copie Snapshot create sullo storage primario. Pertanto, i dati vengono letti direttamente dal sistema di storage primario senza generare carico sul server di database SAP. Lo storage primario comunica direttamente con lo storage secondario e replica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

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

Esecuzione delle operazioni di backup e ripristino Snapshot

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

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



Confronto degli obiettivi del tempo di ripristino

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

Tempo necessario per il ripristino del database

Con un backup basato su file, il tempo di ripristino dipende dalle dimensioni del database e dell'infrastruttura di backup, che definisce la velocità di ripristino in megabyte al secondo. Ad esempio, se l'infrastruttura supporta un'operazione di ripristino a una velocità di 250 MBps, occorrono circa 4.5 ore per ripristinare un database di 4 TB sulla persistenza.

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

Tempo necessario per avviare il database

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

Tempo necessario per il ripristino del database

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

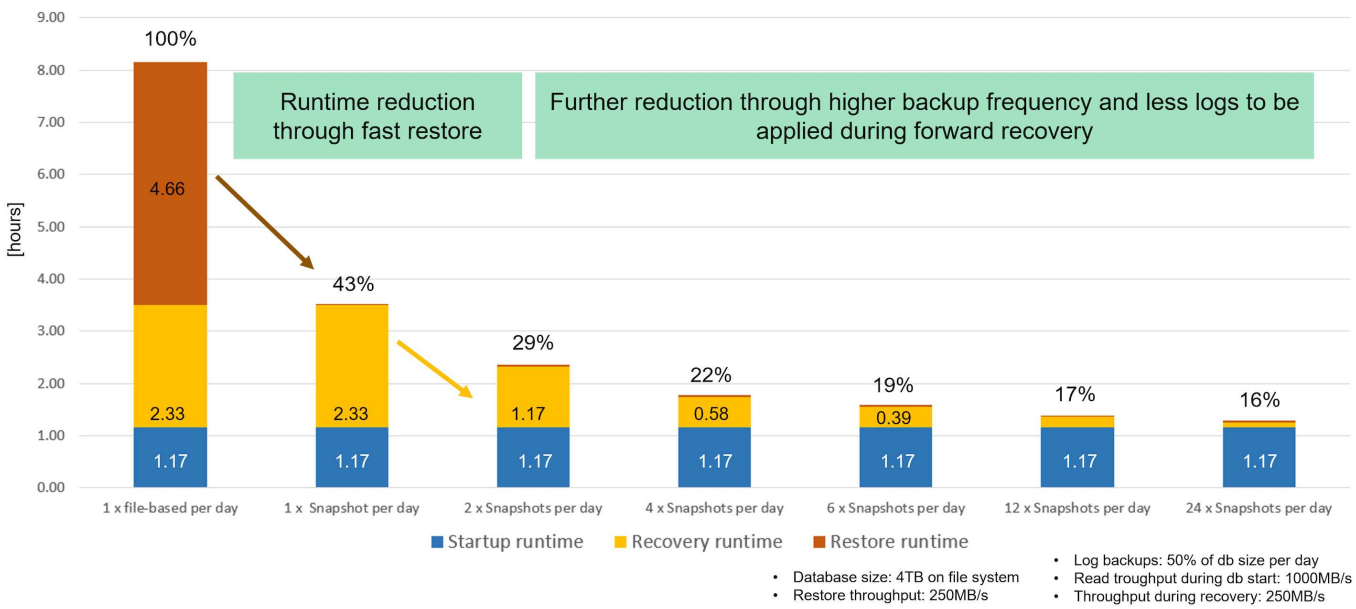
Con i backup dei dati basati su file, la pianificazione del backup è generalmente una volta al giorno. In genere, non è possibile una frequenza di backup più elevata, poiché il backup diminuisce le prestazioni di produzione. Pertanto, nel peggiore dei casi, tutti i log scritti durante la giornata devono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

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

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

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

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



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

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

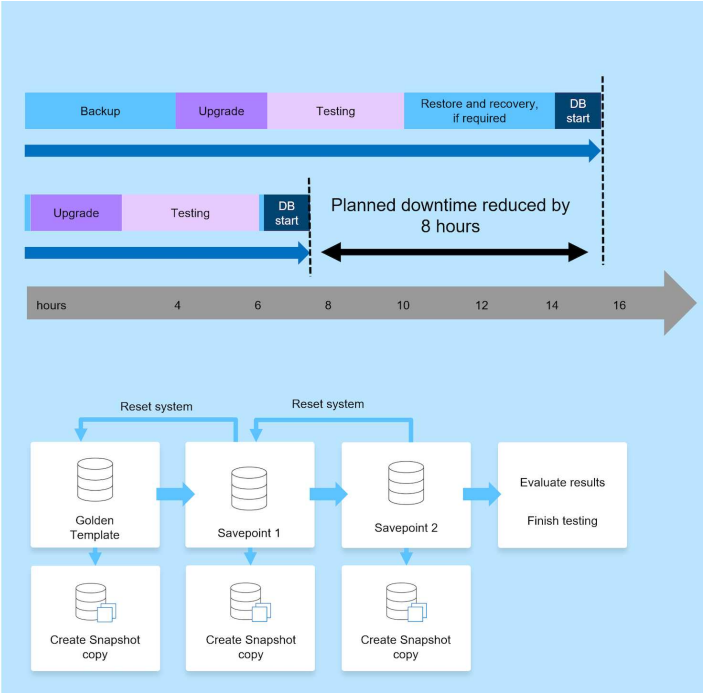
L'upgrade del sistema SAP HANA è un esempio di come un backup on-demand prima dell'upgrade e una possibile operazione di ripristino in caso di errore dell'upgrade abbiano un impatto significativo sul downtime complessivo pianificato. Con l'esempio di un database da 4 TB, è possibile ridurre il downtime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

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

Use Cases for Backup and Recovery Operations

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

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



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

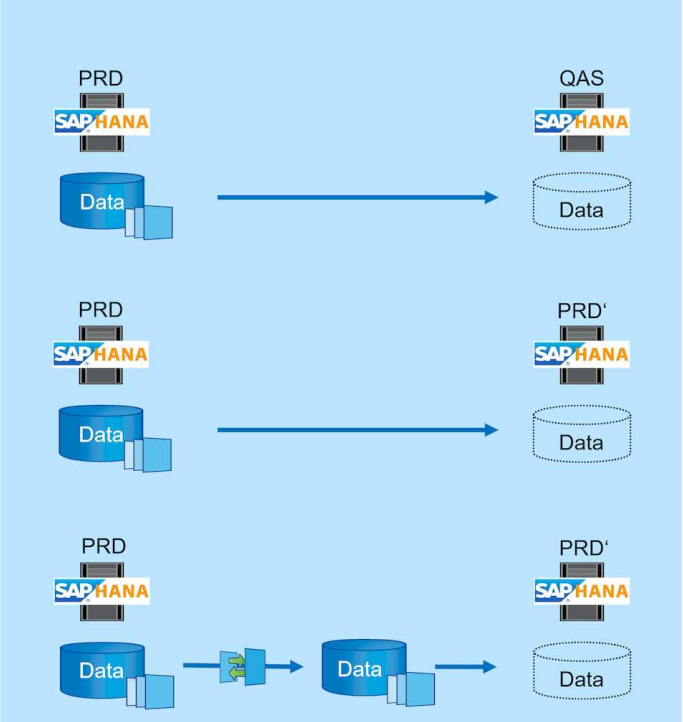
Il caso di utilizzo più diffuso è SAP System Refresh, in cui i dati del sistema di produzione devono essere copiati nel sistema di test o QA. Sfruttando la funzionalità di cloning FSX per ONTAP, è possibile eseguire il provisioning del volume per il sistema di test da qualsiasi copia Snapshot del sistema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

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

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

Use Cases for Cloning Operations

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



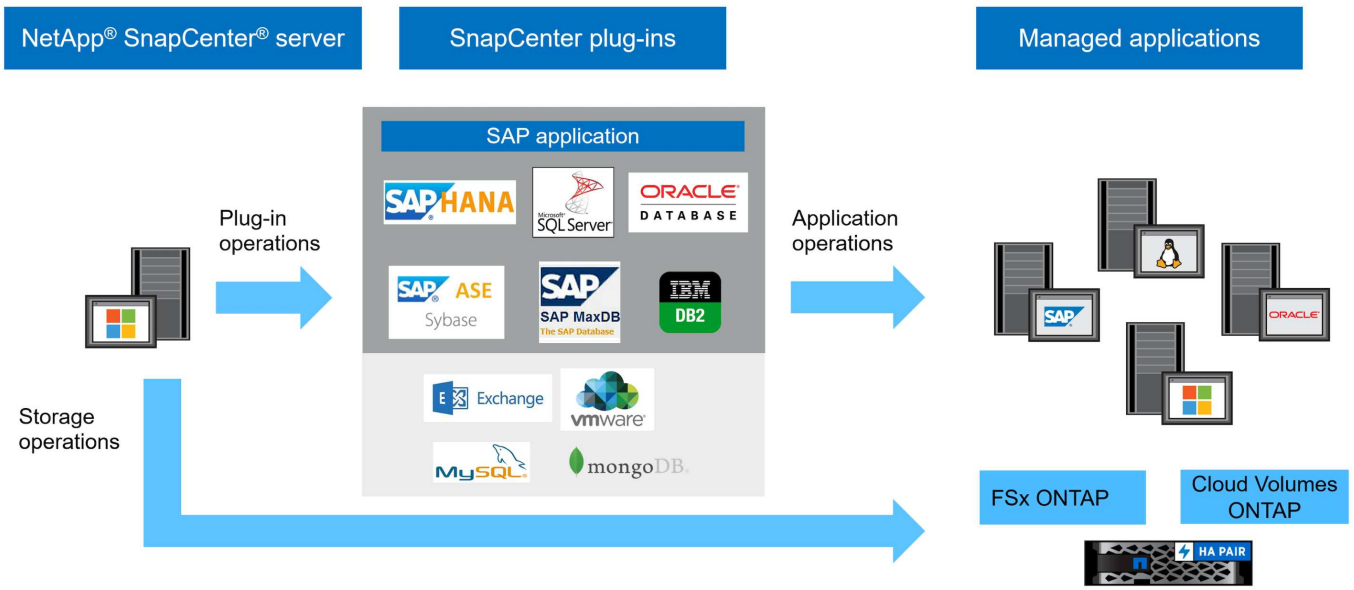
Architettura SnapCenter

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

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

Componenti SnapCenter

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



Soluzione di backup SAP HANA di SnapCenter

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

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

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

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

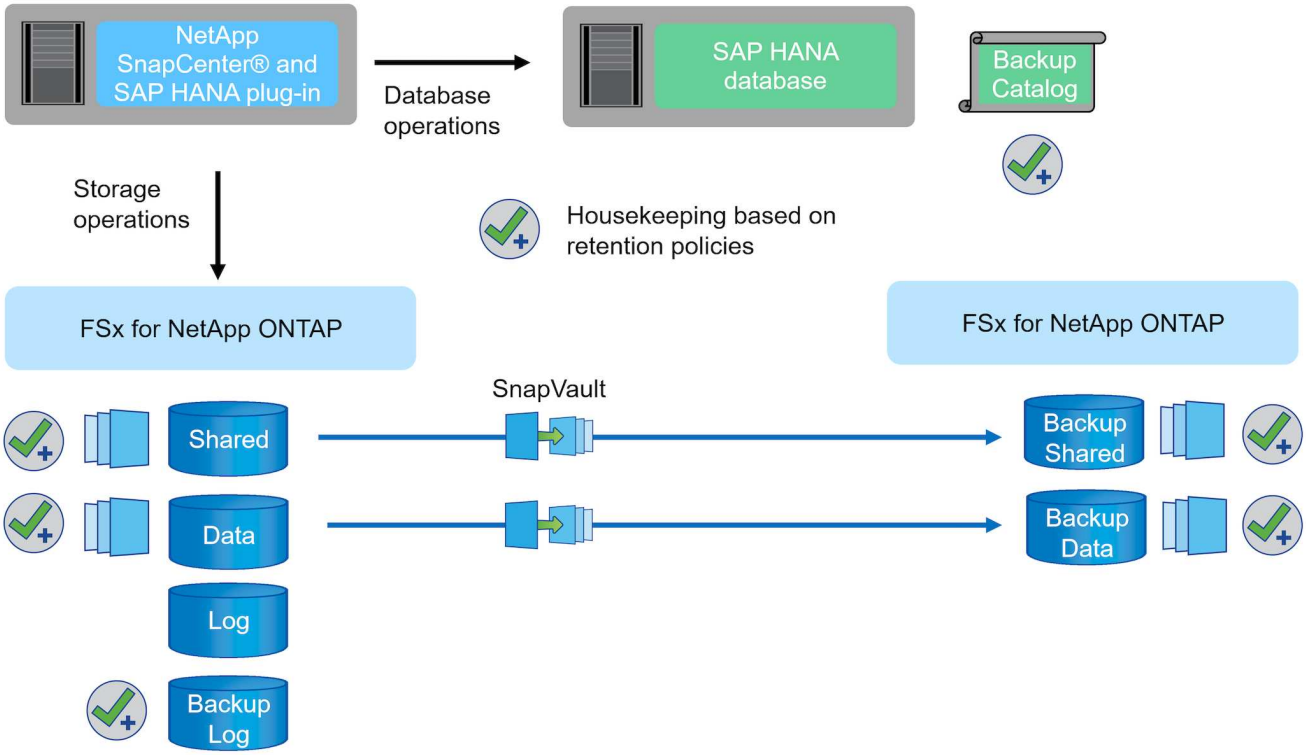
Per consentire un backup completo di tutte le risorse correlate a SAP HANA, SnapCenter consente inoltre di eseguire il backup di tutti i volumi non dati utilizzando il plug-in SAP HANA con copie Snapshot basate su storage. È possibile pianificare volumi diversi dai dati in modo indipendente dal backup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

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

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

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

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



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

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

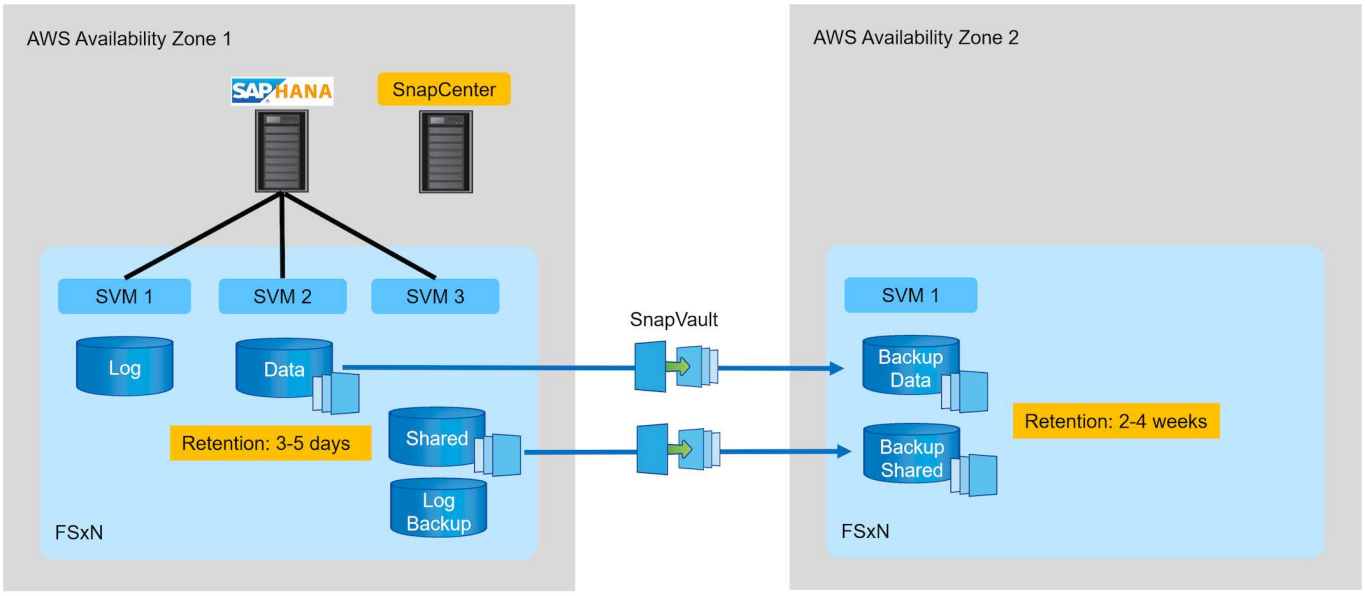
Scopo del presente documento

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

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

Strategia di protezione dei dati

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



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

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

È necessario definire i seguenti parametri:

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

primario?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Esempio di setup di laboratorio

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

Sistema HANA PFX:

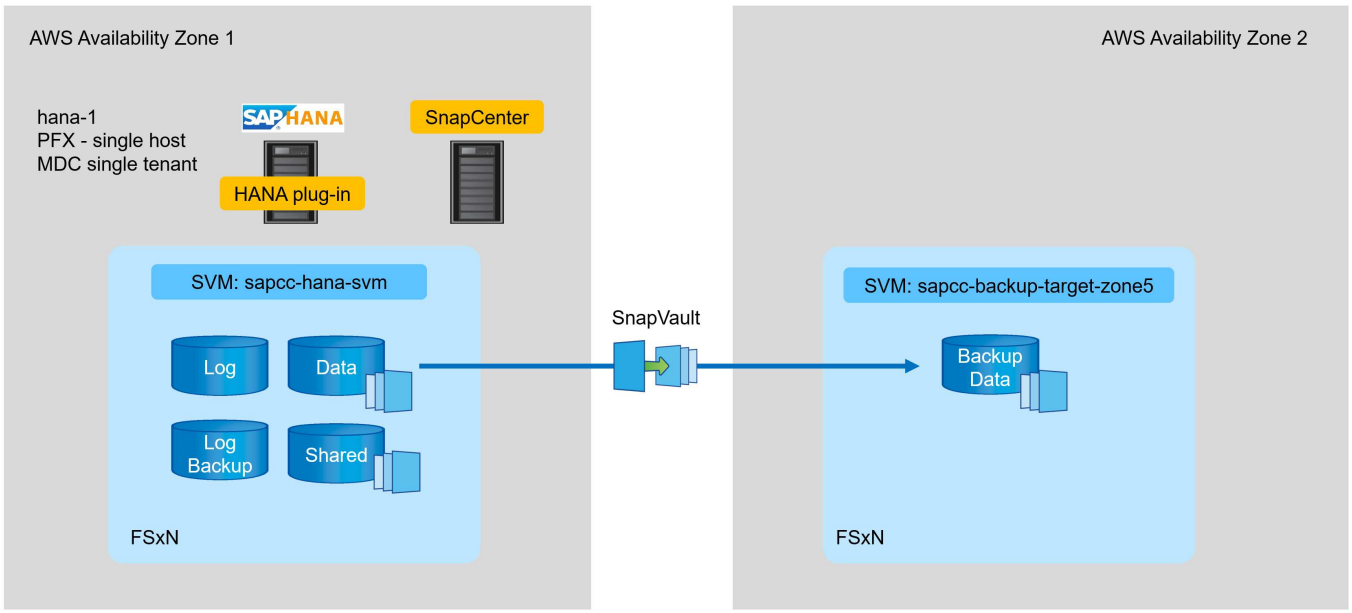
- Sistema MDC a host singolo con un singolo tenant
- HANA 2.0 SPS 6 revisione 60
- SLES PER SAP 15SP3

SnapCenter:

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

FSX per file system ONTAP:

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



Configurazione di SnapCenter

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

Panoramica delle fasi di configurazione

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

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

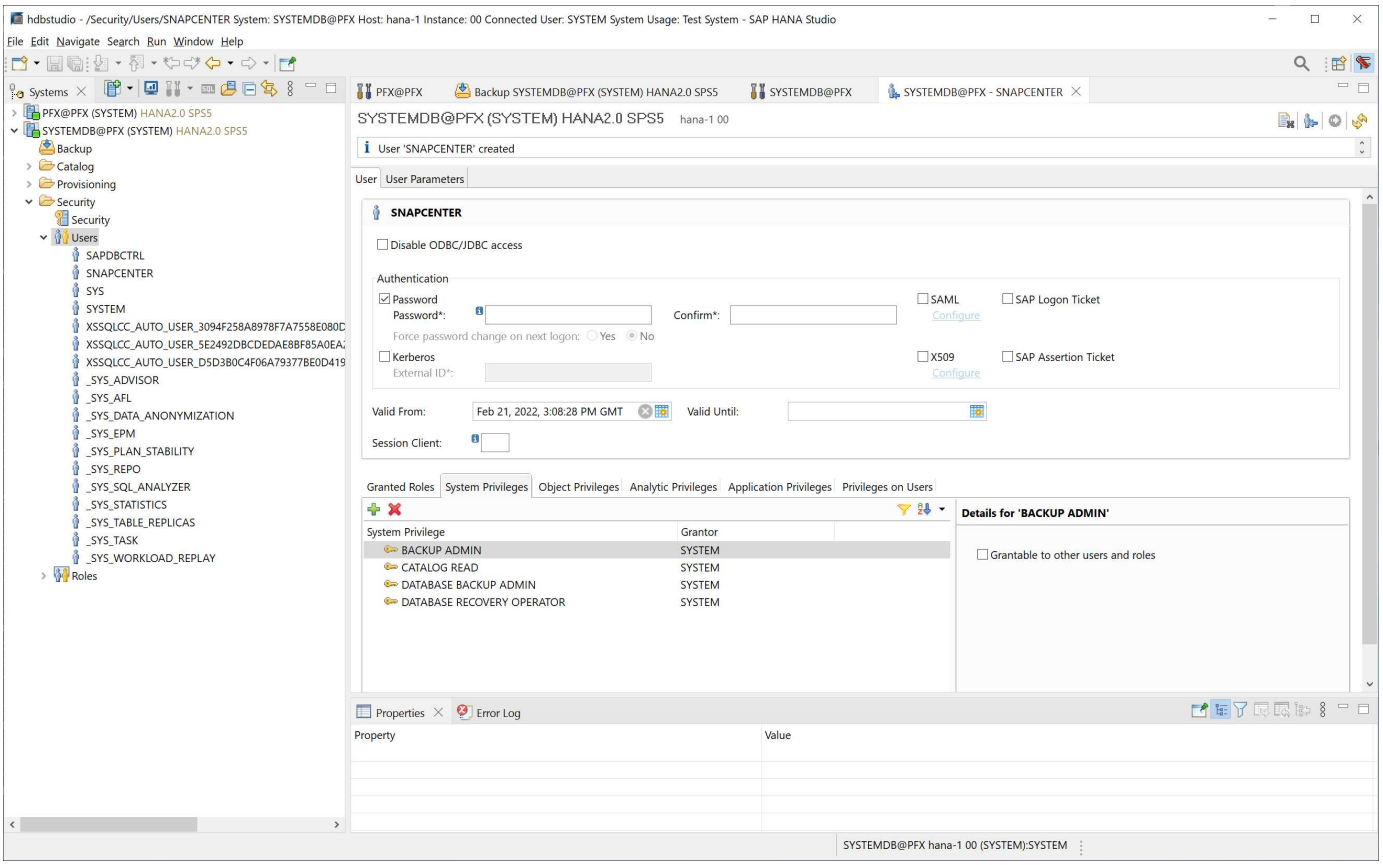
Configurazione di SAP HANA backup user e hdbuserstore

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

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

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

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



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

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

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

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

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

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

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

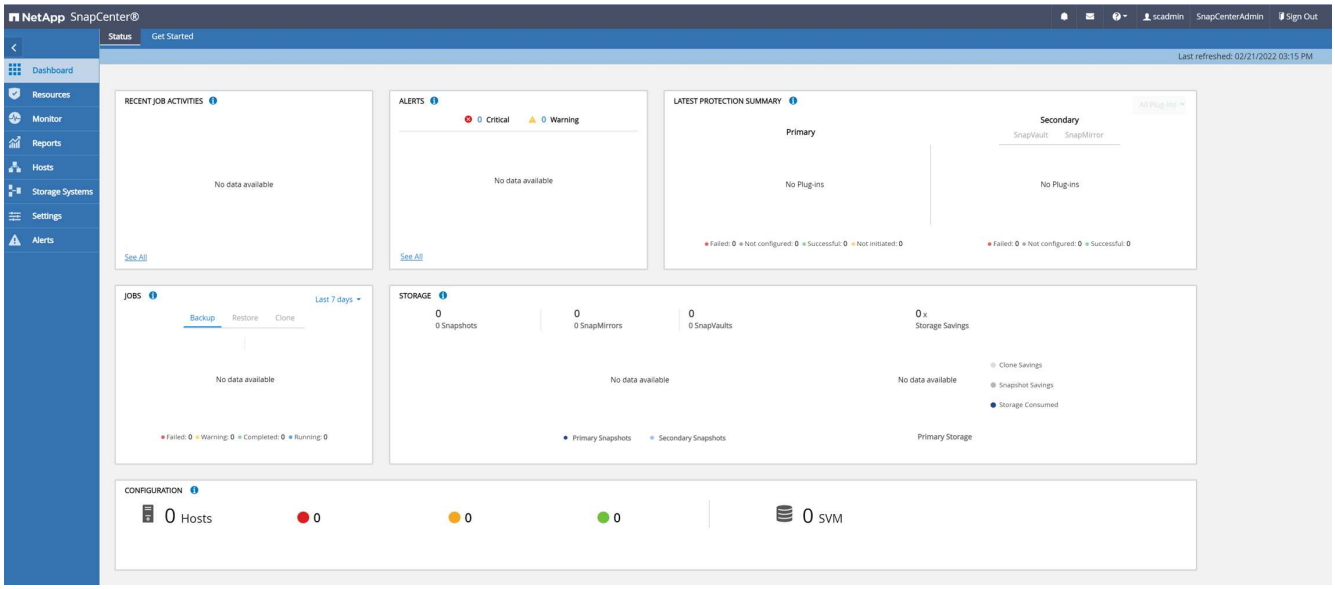
È possibile controllare l'accesso al database di sistema HANA che utilizza la chiave con `hdbsql` comando.

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

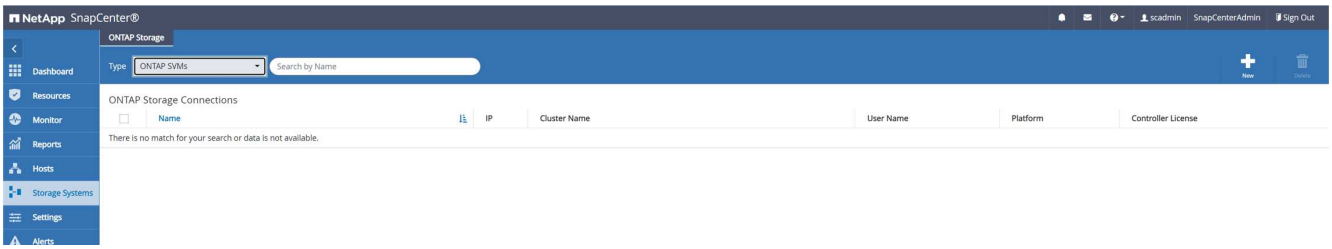
Configurare lo storage

Per configurare lo storage in SnapCenter, procedere come segue.

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

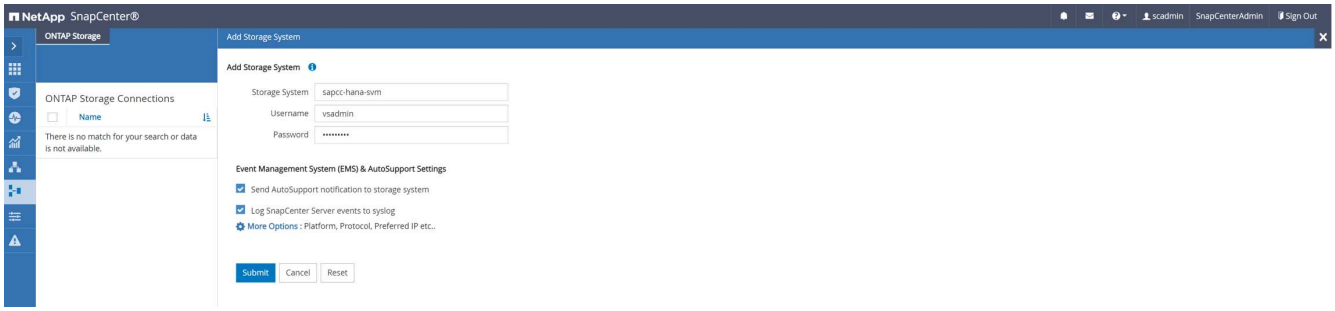


È possibile selezionare il tipo di sistema storage, che può essere SVM ONTAP o cluster ONTAP. Nell'esempio seguente, viene selezionata la gestione SVM.

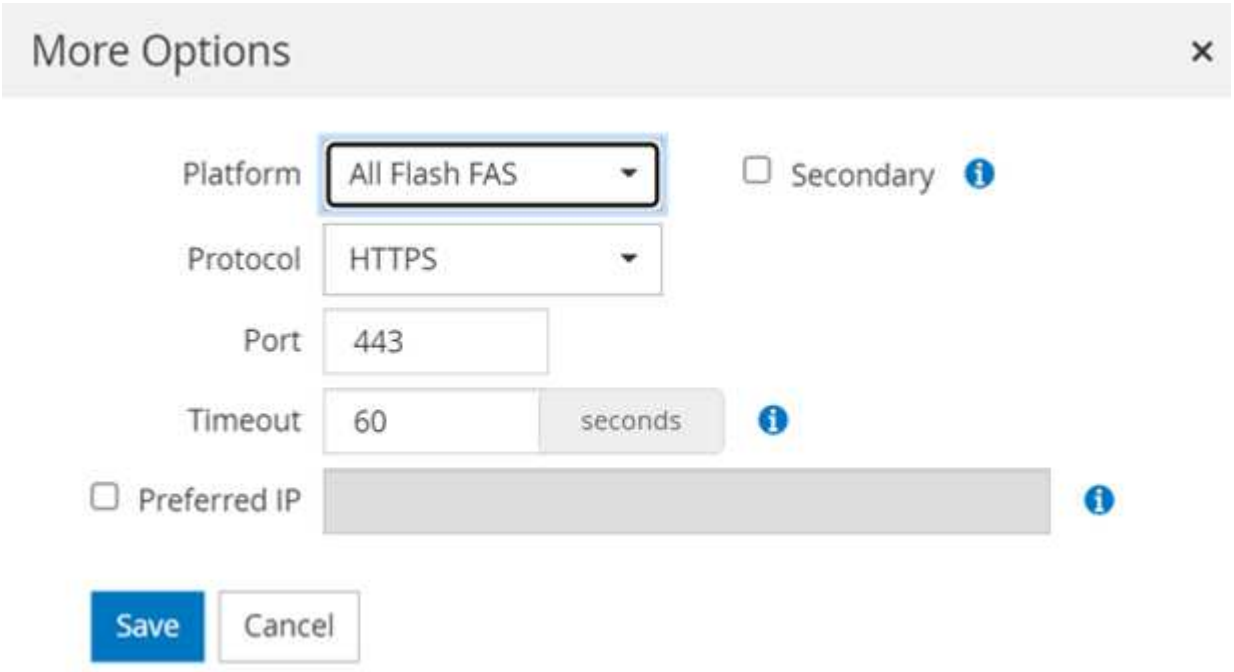


2. Per aggiungere un sistema storage e fornire il nome host e le credenziali richiesti, fare clic su New (nuovo).

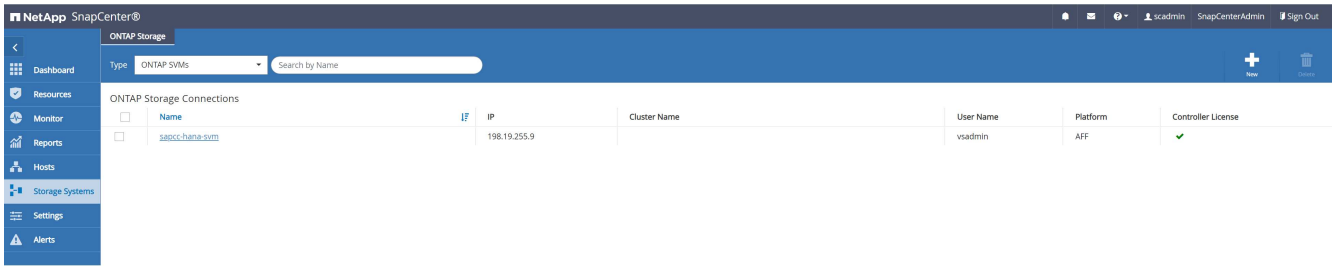
   L'utente SVM non deve essere l'utente vsadmin, come mostrato nella figura seguente. In genere, un utente viene configurato sulla SVM e assegnato i permessi necessari per eseguire le operazioni di backup e ripristino. Per informazioni sui privilegi richiesti, vedere "Guida all'installazione di SnapCenter"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



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



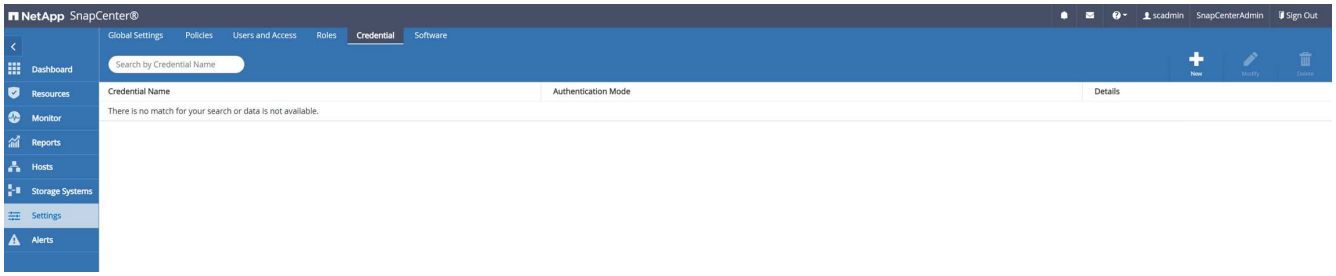
SVM `sapcc-hana-svm` È ora configurato in SnapCenter.



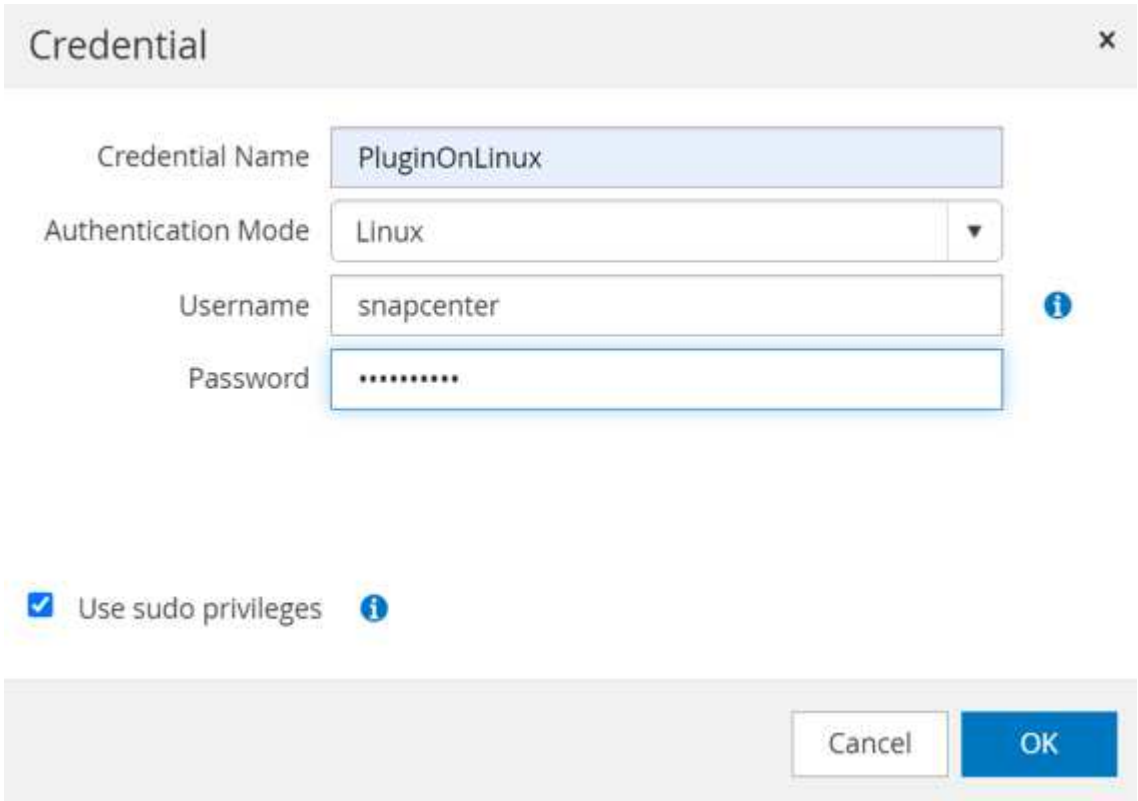
Creare le credenziali per la distribuzione del plug-in

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

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



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



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

Aggiungere un host SAP HANA

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

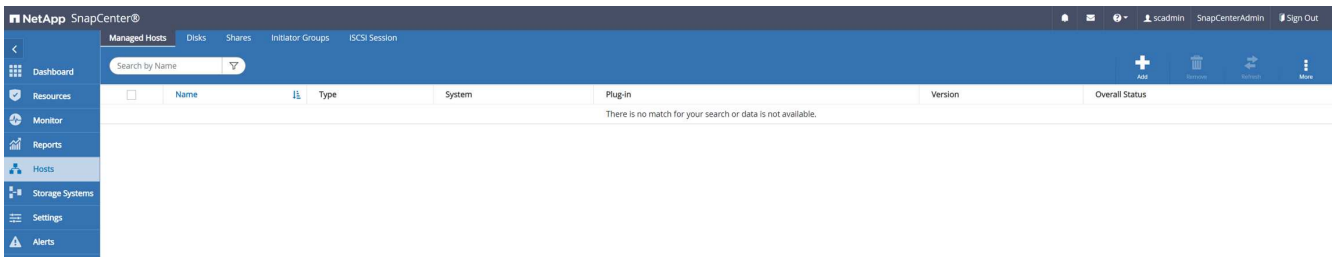
Il plug-in SAP HANA richiede Java a 64 bit versione 1.8. Java deve essere installato sull'host prima che l'host venga aggiunto a SnapCenter.

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

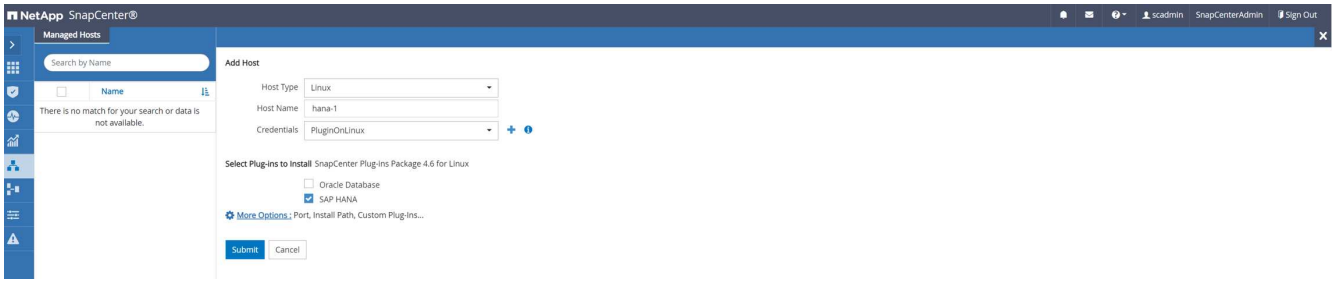
OpenJDK o Oracle Java è supportato con SnapCenter.

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

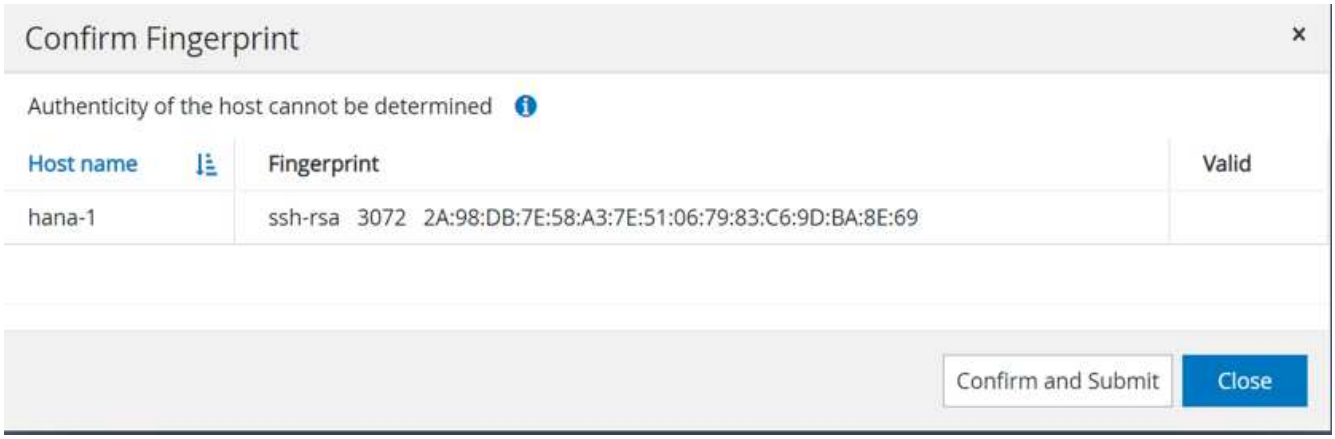
1. Dalla scheda host, fare clic su Add (Aggiungi).



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

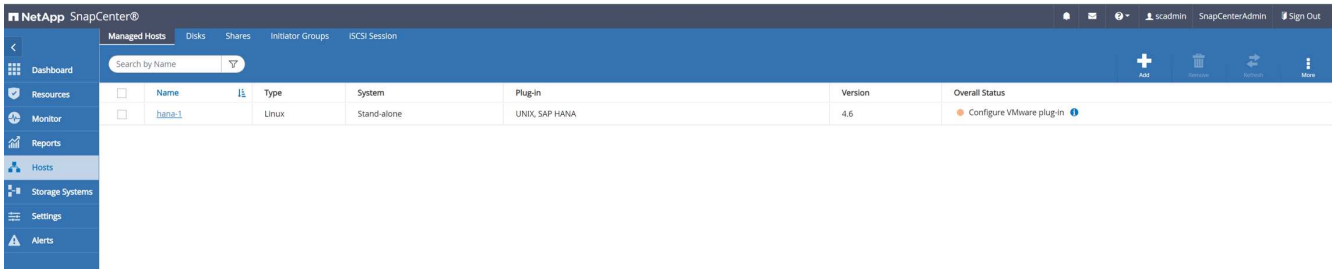


3. Confermare l'impronta digitale.



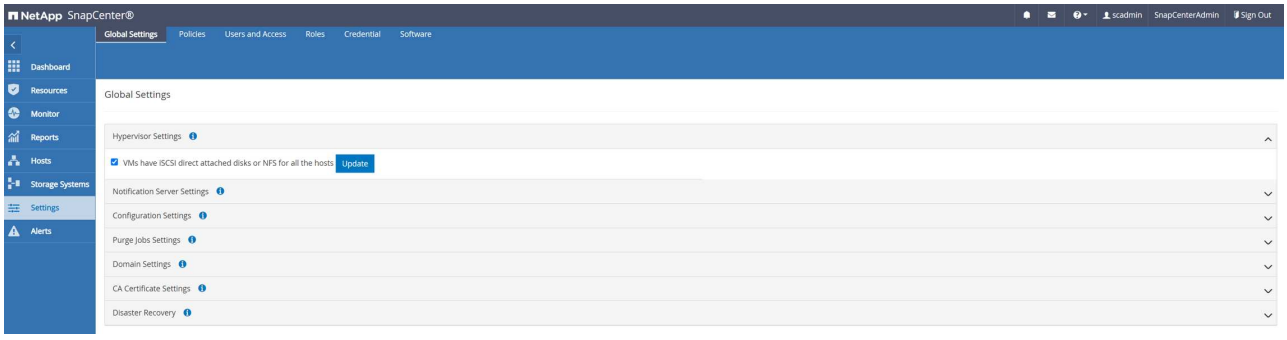
L'installazione di HANA e del plug-in Linux si avvia automaticamente. Al termine dell'installazione, la colonna di stato dell'host mostra Configure VMware Plug-in (Configura plug-in VMware). SnapCenter rileva se il plug-in SAP HANA è installato in un ambiente virtualizzato. Potrebbe trattarsi di un ambiente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

Per rimuovere il messaggio di avviso, procedere come segue.

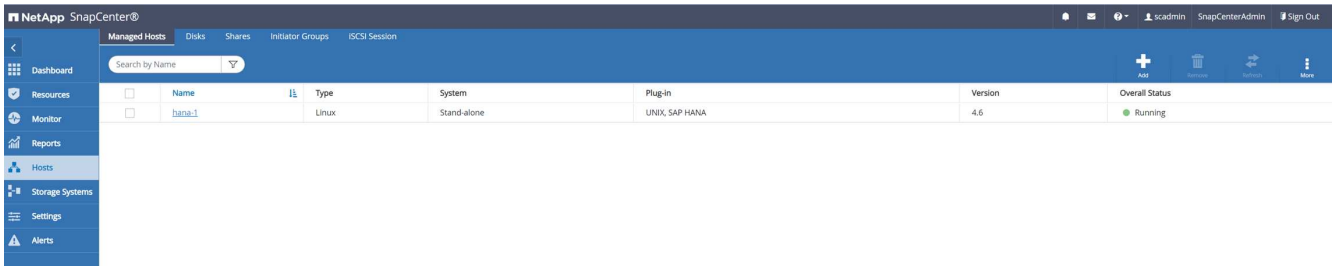


a. Dalla scheda Settings (Impostazioni), selezionare Global Settings (Impostazioni globali).

b. Per le impostazioni dell'hypervisor, selezionare VM con iSCSI Direct Attached Disk o NFS per tutti gli host e aggiornare le impostazioni.



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



Configurare i criteri

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

Una configurazione minima tipica è costituita dai seguenti criteri:

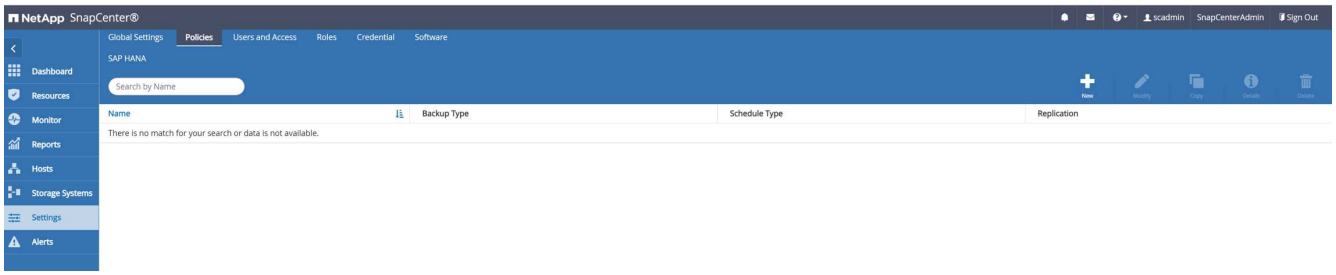
- Policy per backup orari senza replica: `LocalSnap`.
- Policy per il controllo settimanale dell'integrità dei blocchi utilizzando un backup basato su file: `BlockIntegrityCheck`.

Le sezioni seguenti descrivono la configurazione di questi criteri.

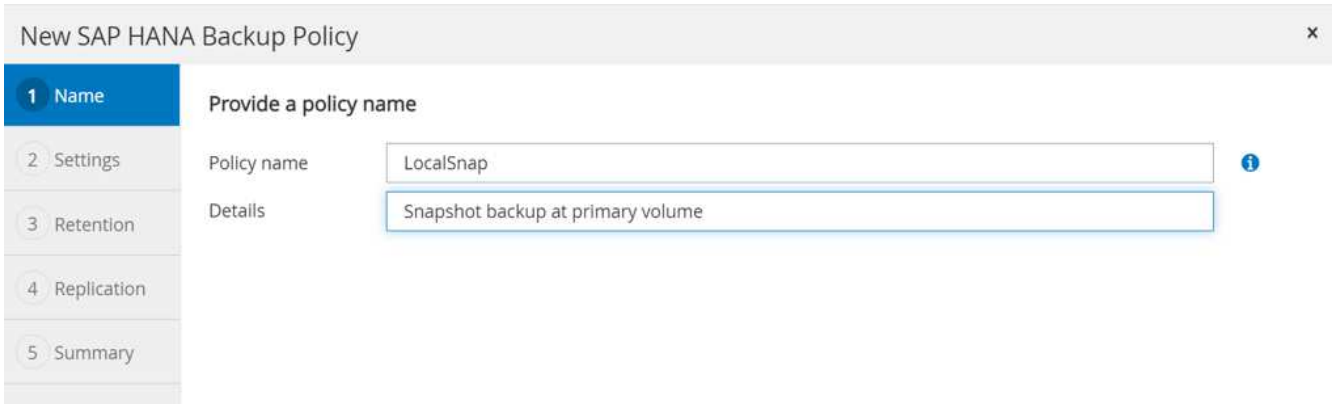
Policy per i backup Snapshot

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

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

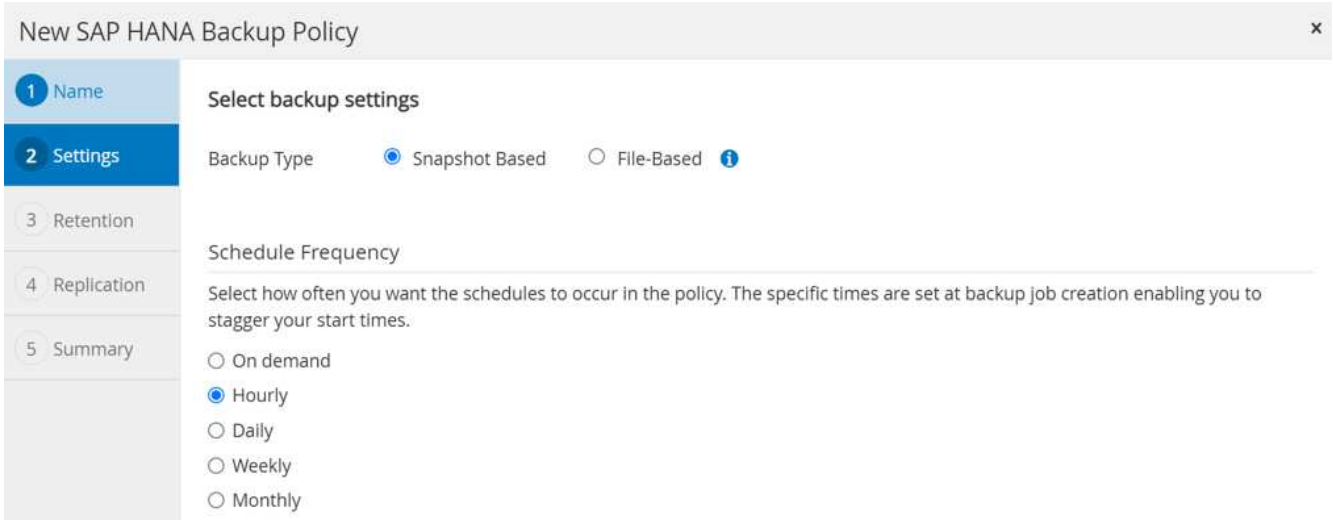


2. Immettere il nome e la descrizione della policy. Fare clic su Avanti.

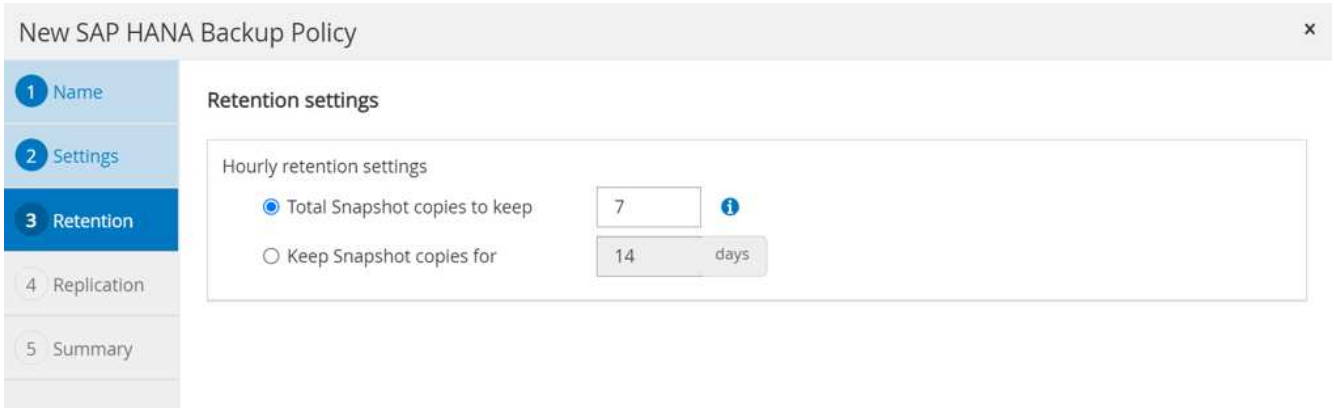


3. Selezionare il tipo di backup basato su Snapshot e selezionare orario per la frequenza di pianificazione.

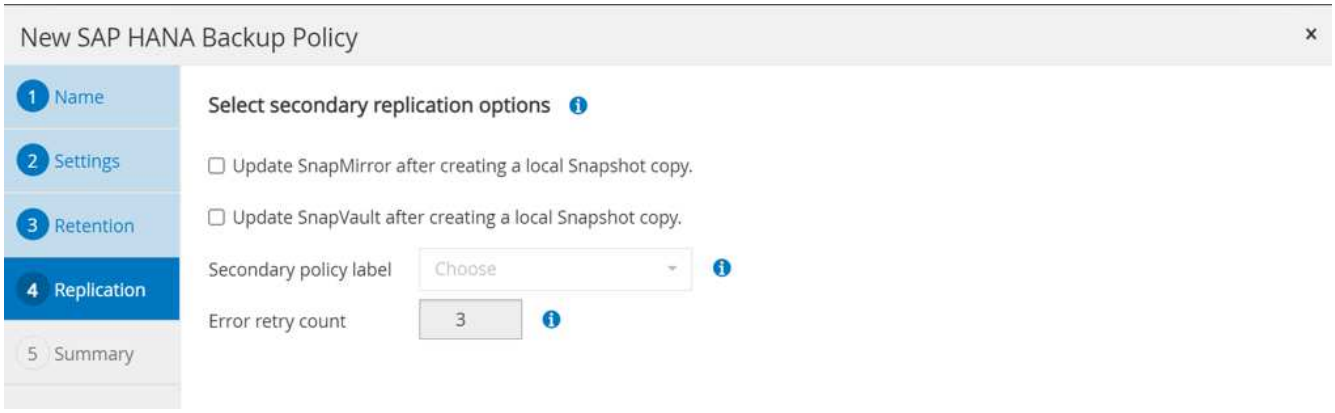
La pianificazione viene configurata in seguito con la configurazione di protezione delle risorse HANA.

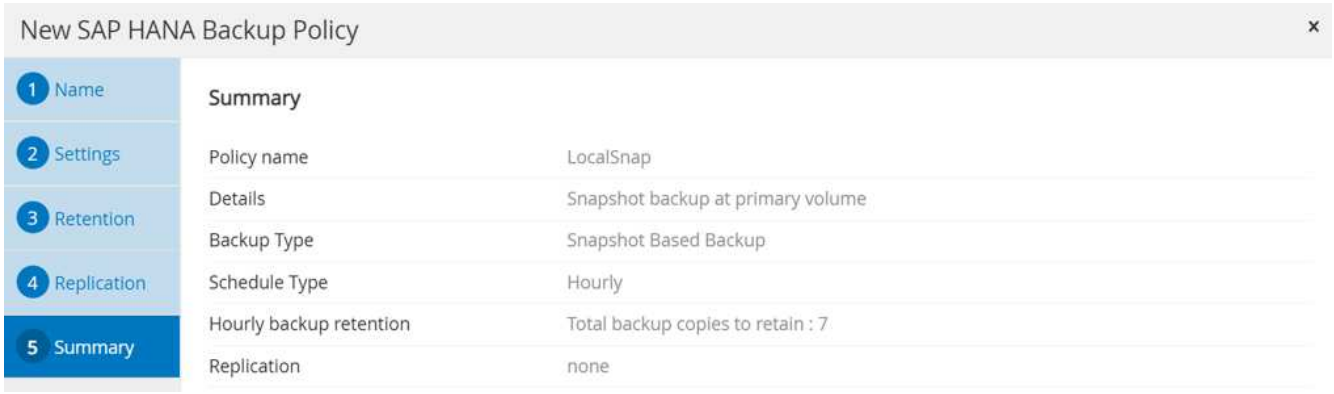


4. Configurare le impostazioni di conservazione per i backup on-demand.

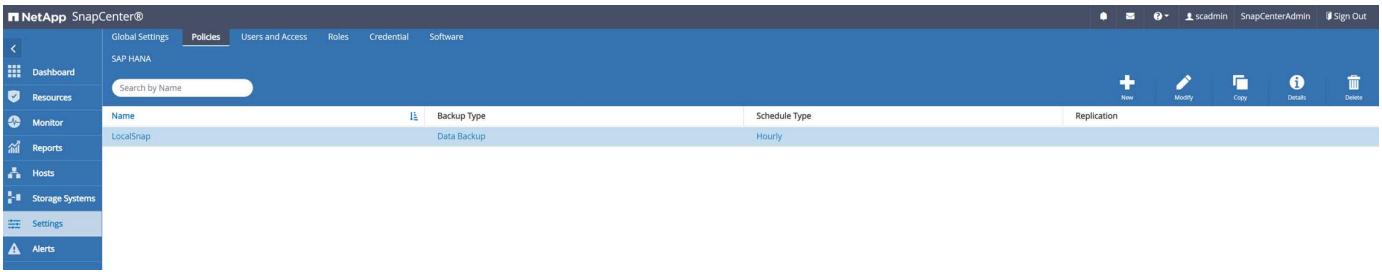


5. Configurare le opzioni di replica. In questo caso, non è selezionato alcun aggiornamento di SnapVault o SnapMirror.





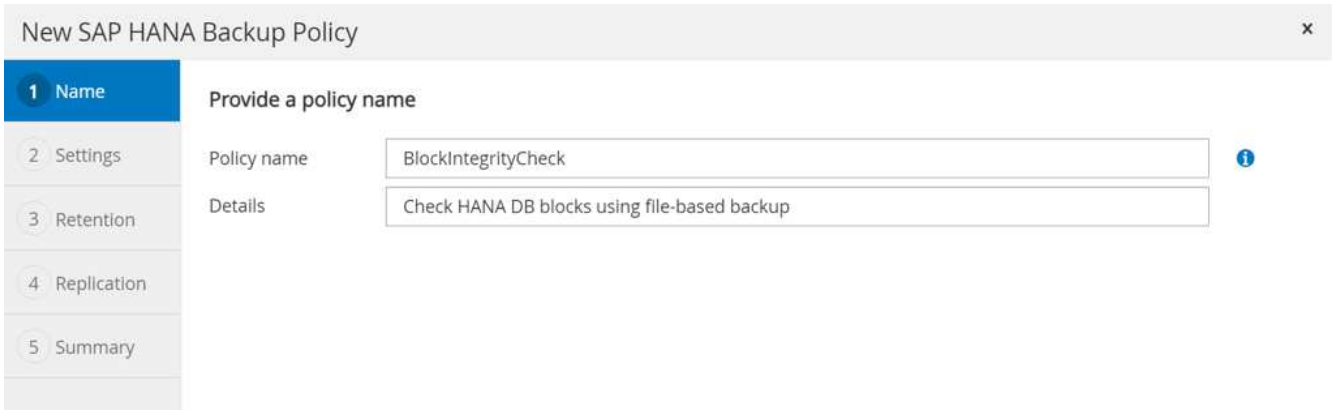
Il nuovo criterio è ora configurato.



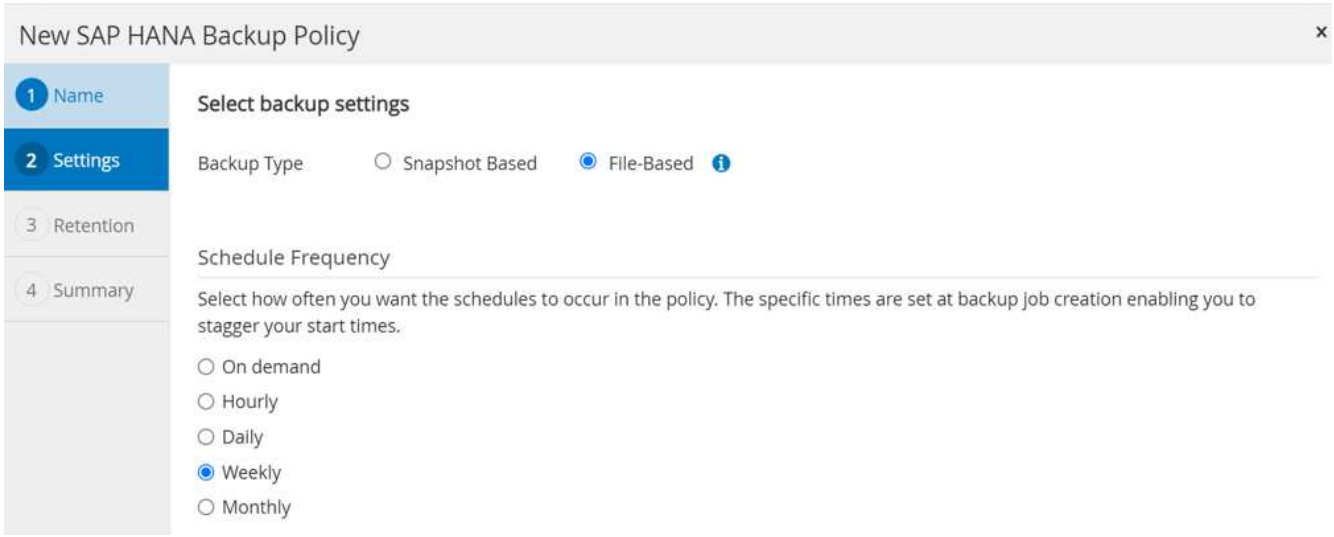
Policy per il controllo dell'integrità del blocco

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

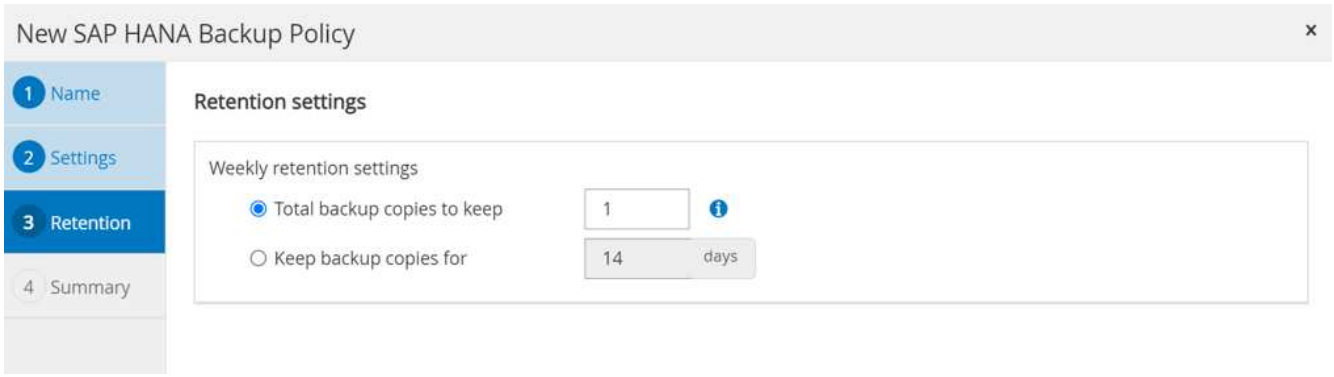
1. Accedere a Impostazioni > Criteri e fare clic su nuovo.
2. Immettere il nome e la descrizione della policy. Fare clic su Avanti.



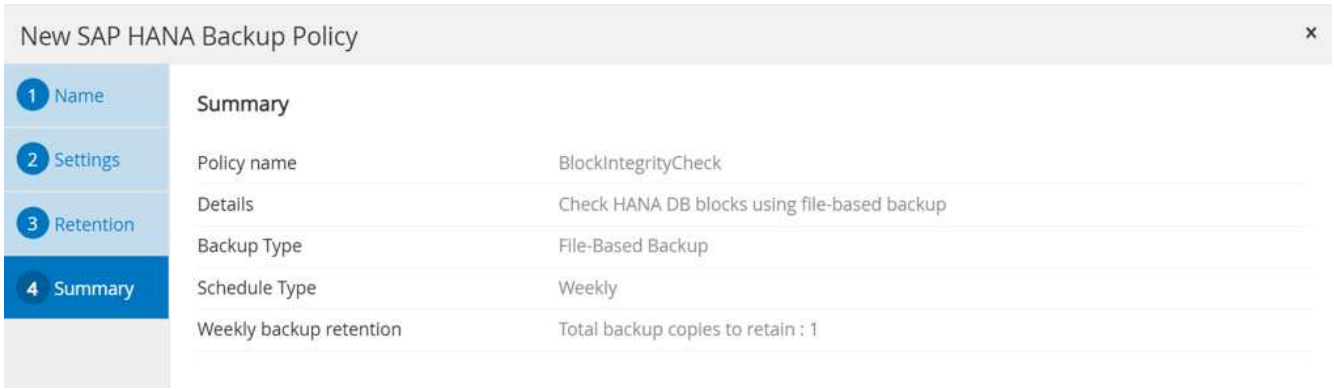
3. Impostare il tipo di backup su file-based (basato su file) e la frequenza di pianificazione su Weekly (settimanale). La pianificazione viene configurata in seguito con la configurazione di protezione delle risorse HANA.

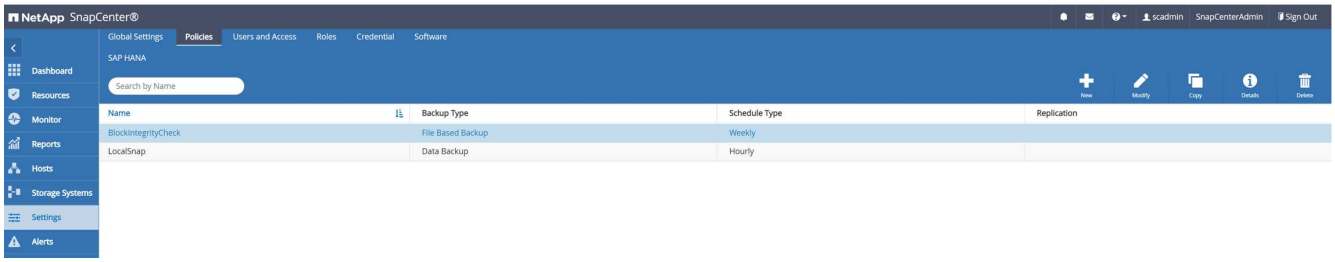


4. Configurare le impostazioni di conservazione per i backup on-demand.



5. Nella pagina Riepilogo, fare clic su fine.



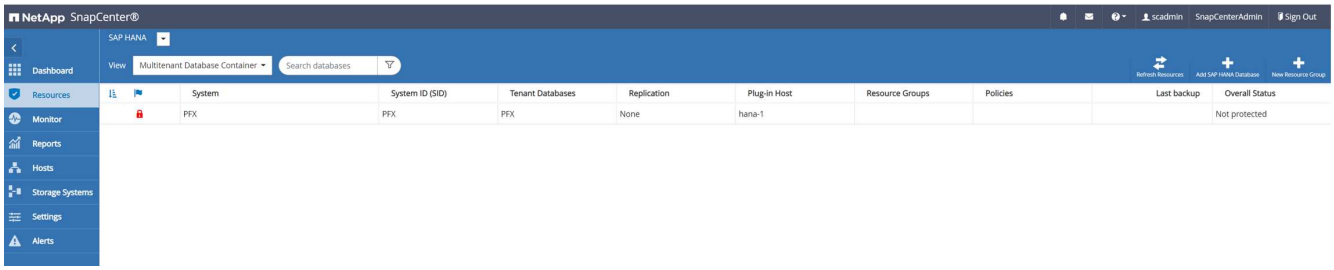


Configurare e proteggere una risorsa HANA

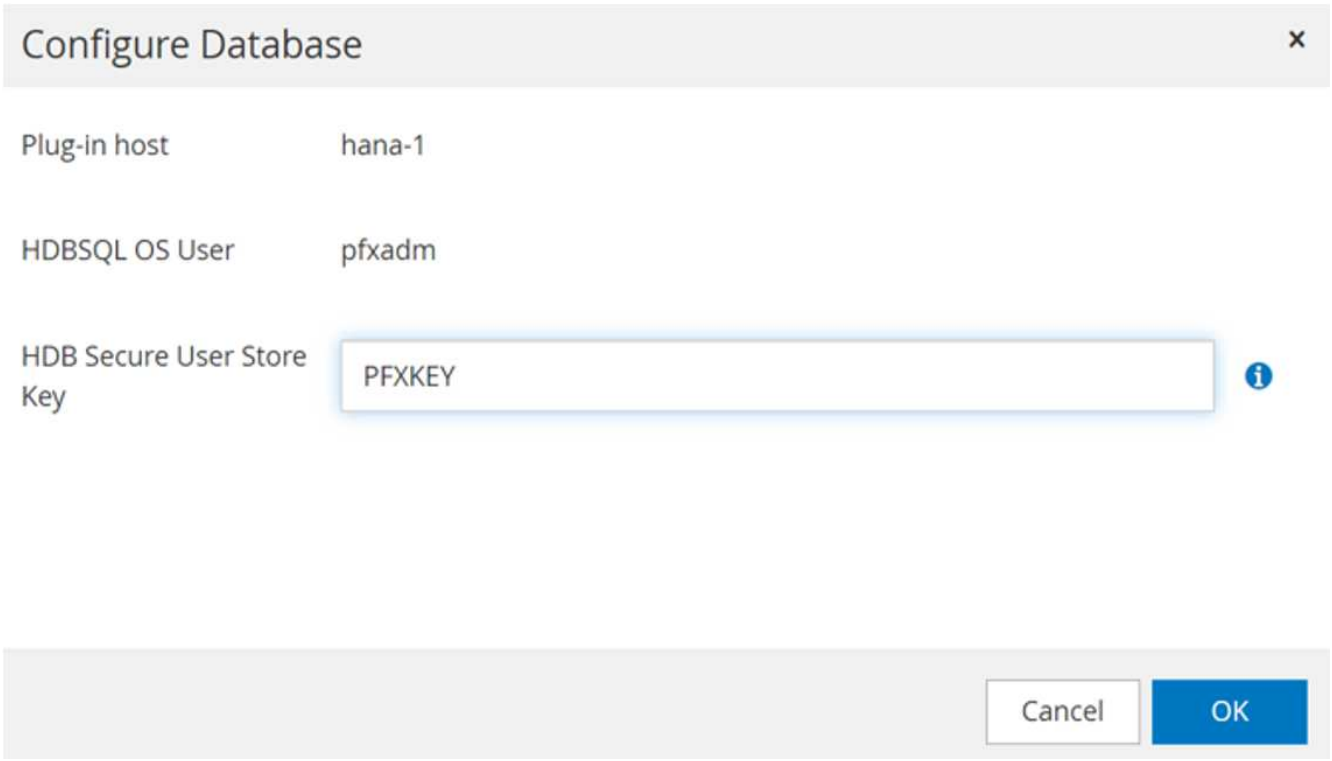
Dopo l'installazione del plug-in, il processo di rilevamento automatico della risorsa HANA viene avviato automaticamente. Nella schermata Resources (risorse) viene creata una nuova risorsa, contrassegnata come bloccata con l'icona del lucchetto rosso. Per configurare e proteggere la nuova risorsa HANA,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

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

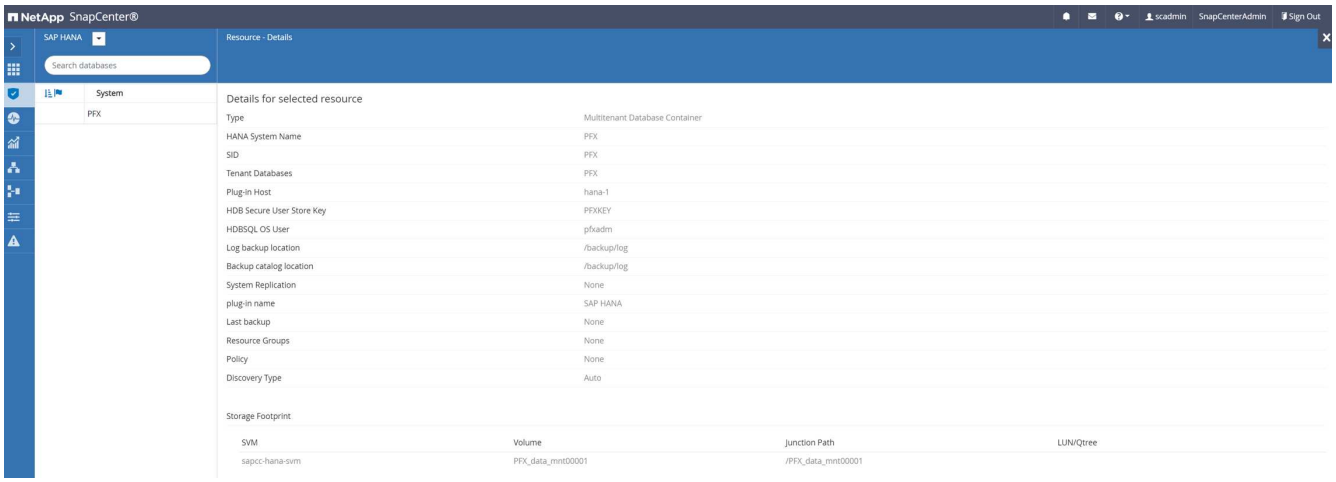
   È inoltre possibile attivare manualmente il processo di rilevamento automatico nella schermata risorse facendo clic su Aggiorna risorse.



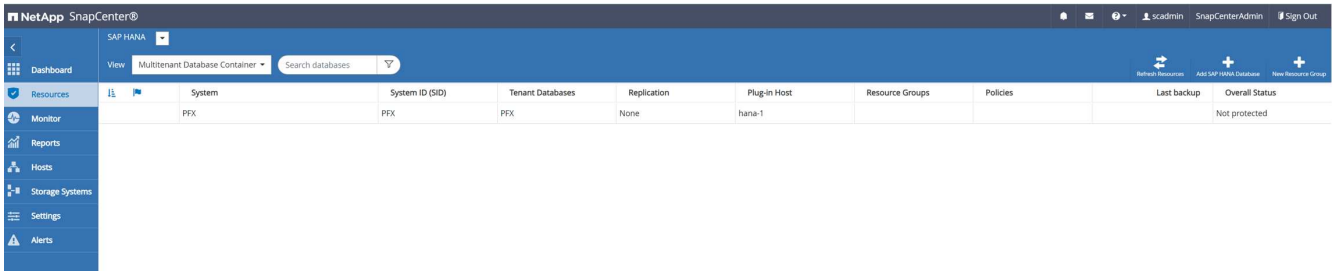
2. Fornire la chiave dell'archivio utenti per il database HANA.



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

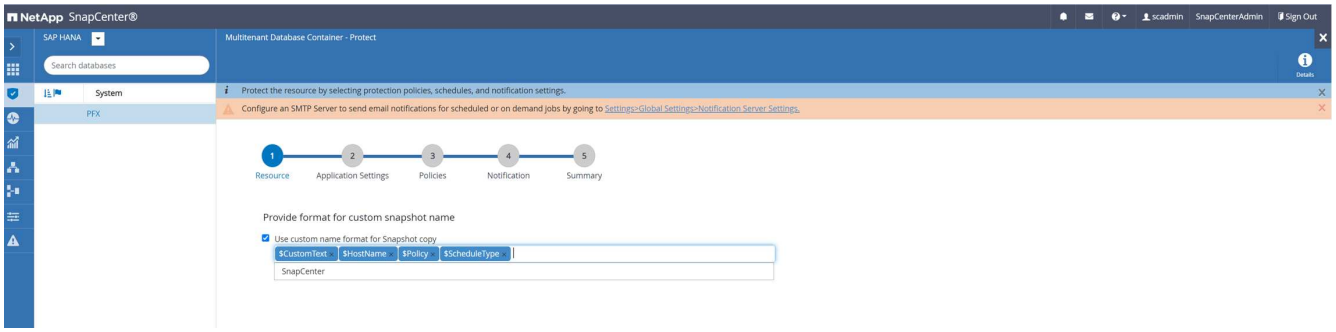


3. Dalla scheda Resources (risorse), fare doppio clic sulla risorsa per configurare la protezione delle risorse.

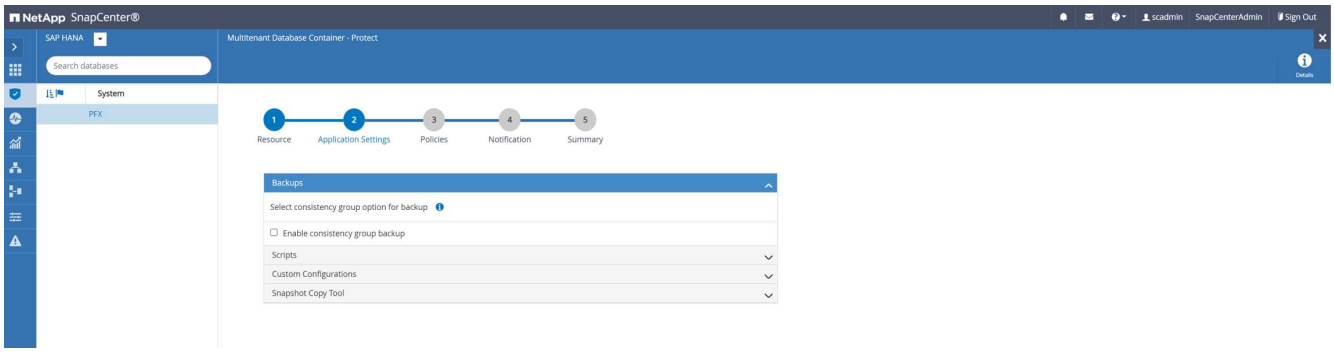


4. Configurare un formato nome personalizzato per la copia Snapshot.

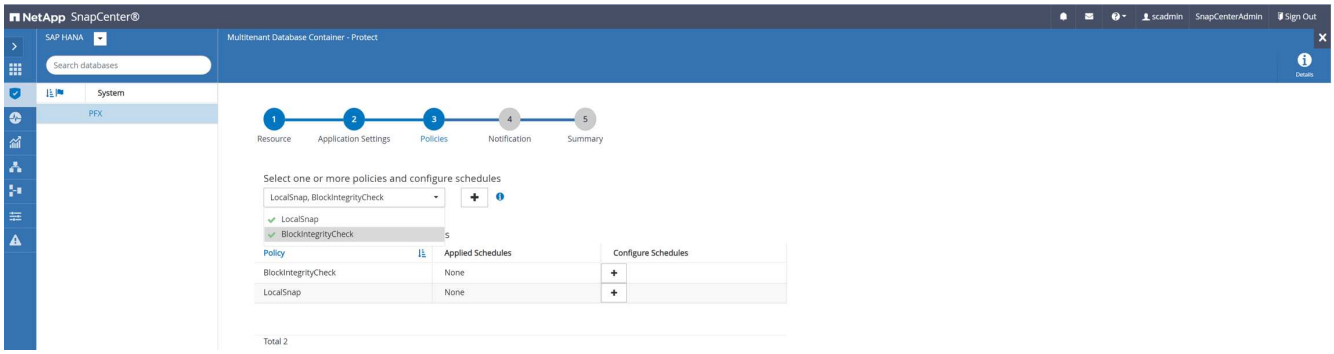
   NetApp consiglia di utilizzare un nome di copia Snapshot personalizzato per identificare facilmente i backup creati con quale tipo di policy e pianificazione. Aggiungendo il tipo di pianificazione nel nome della copia Snapshot, è possibile distinguere tra backup pianificati e su richiesta. Il `schedule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



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

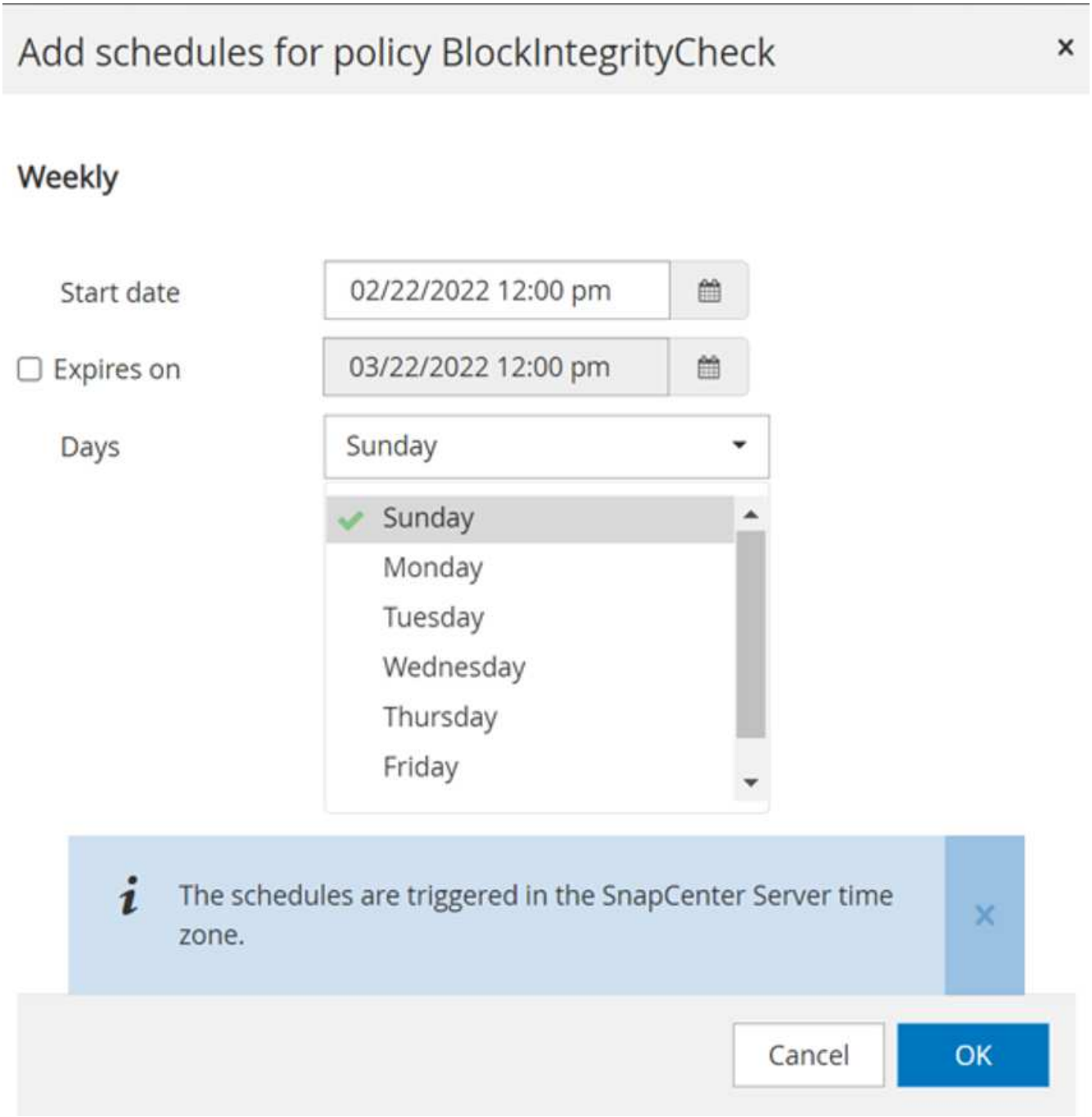


6. Selezionare i criteri da aggiungere alla risorsa.



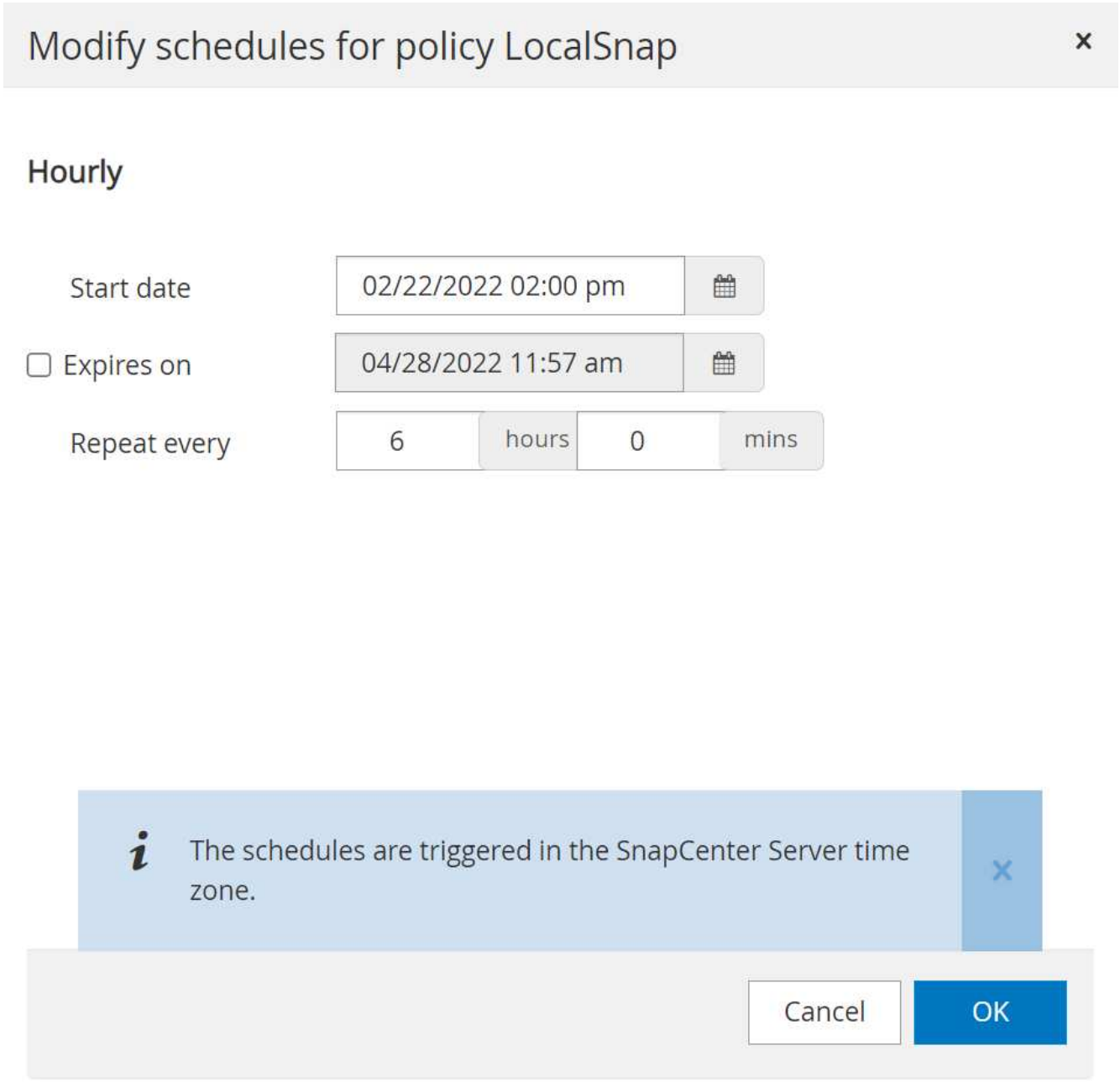
7. Definire la pianificazione per la policy di controllo dell'integrità del blocco.

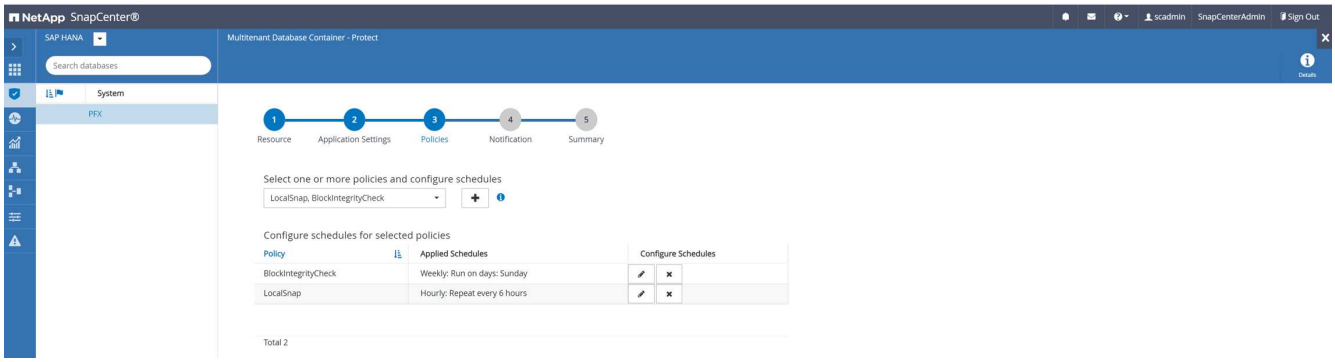
   In questo esempio, viene impostato per una volta alla settimana.



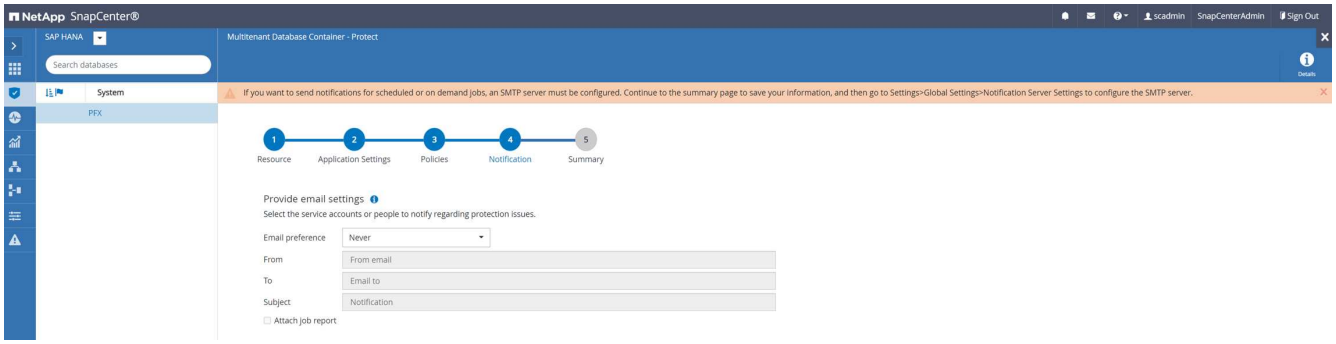
8. Definire la pianificazione per la policy Snapshot locale.

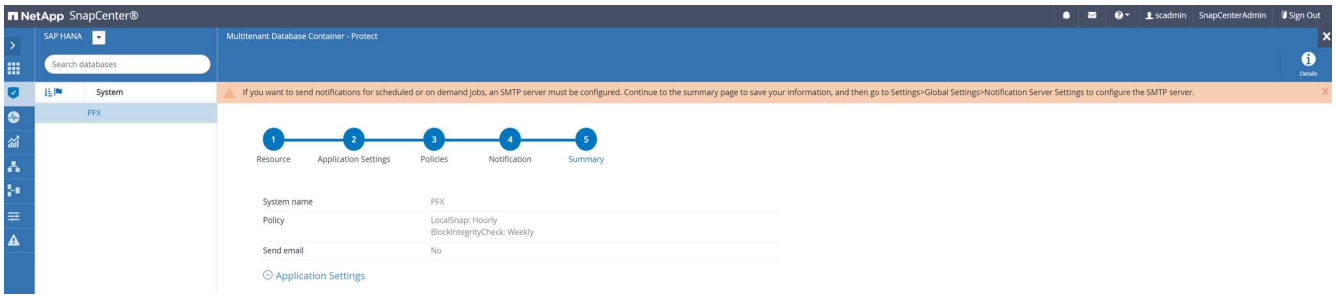
   In questo esempio, viene impostato ogni 6 ore.



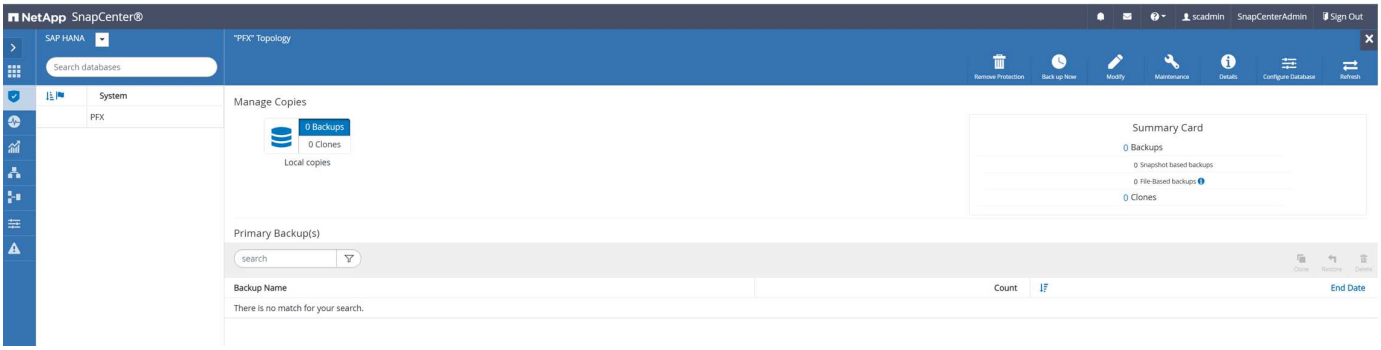


9. Fornire informazioni sulla notifica via email.





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



Operazioni di backup di SnapCenter

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

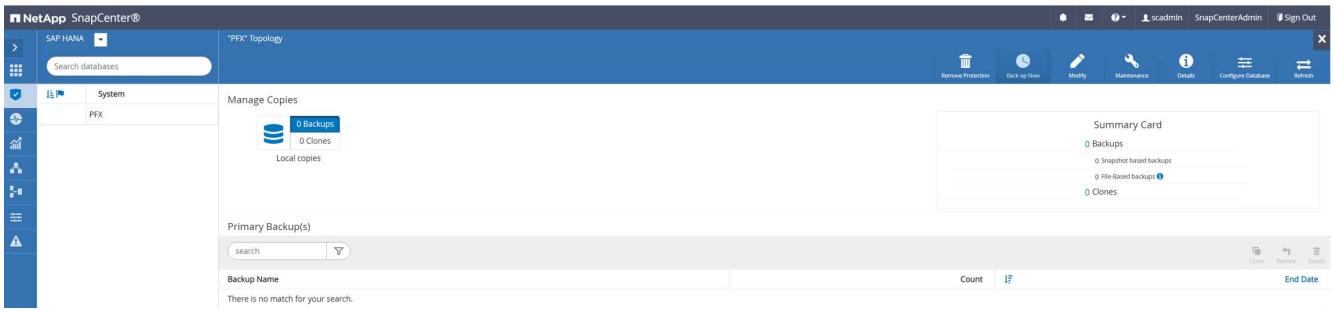
Crea un backup Snapshot on-demand

Segui questi passaggi per creare backup Snapshot on-demand.

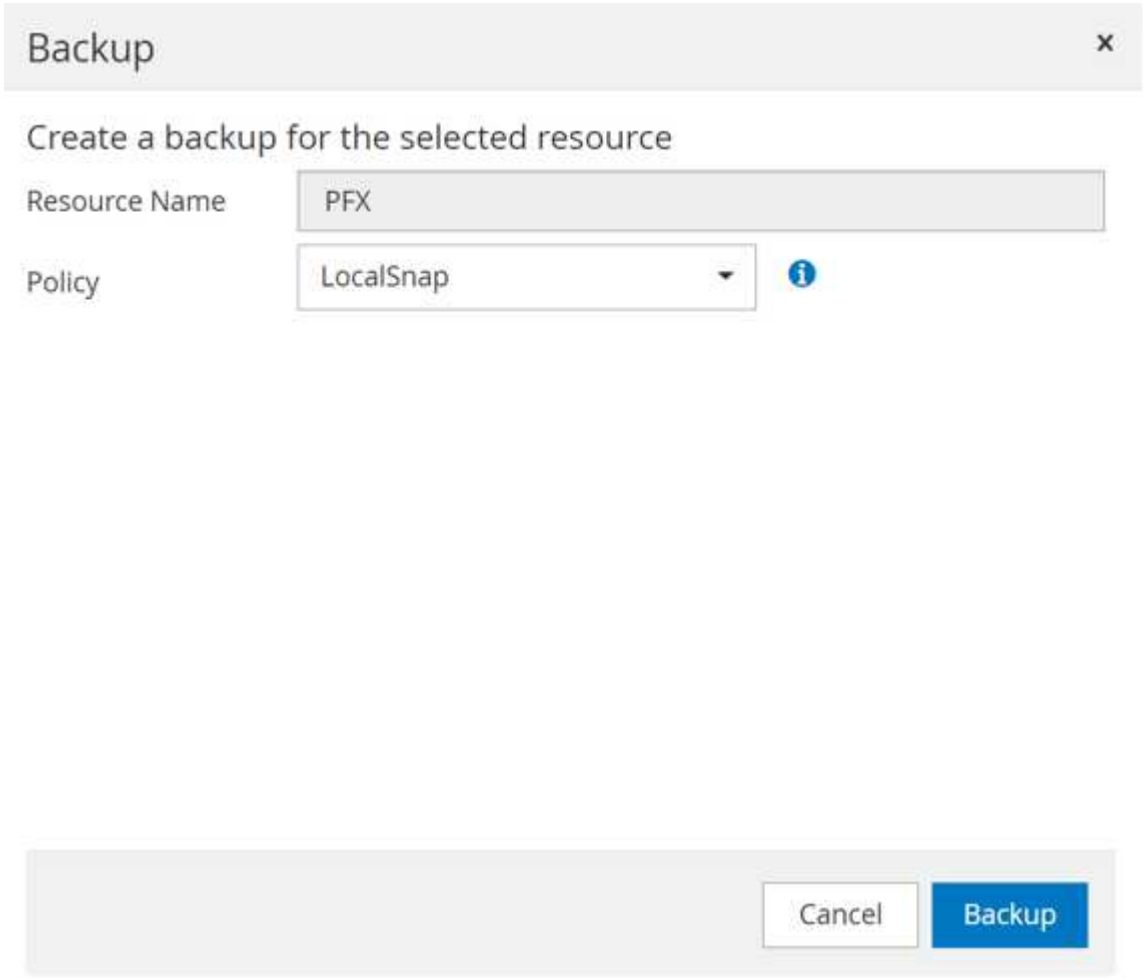
1. Nella vista Resource (risorse), selezionare la risorsa e fare doppio clic sulla riga per passare alla vista Topology (topologia).

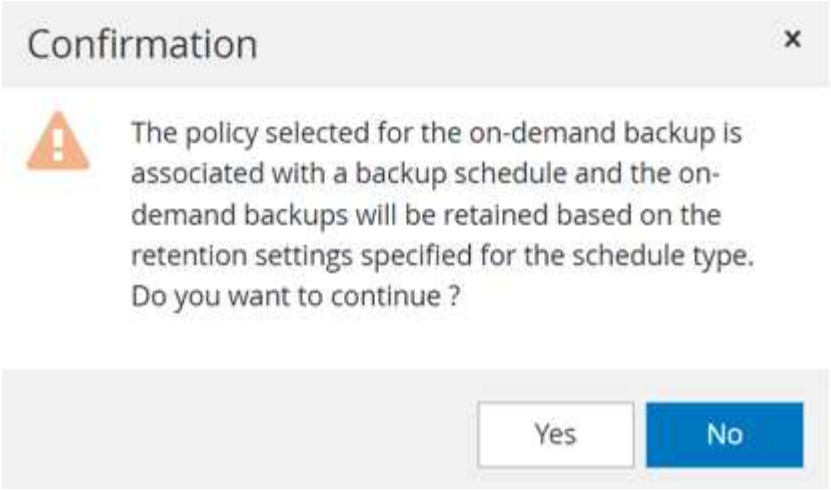
   La vista topologia delle risorse offre una panoramica di tutti i backup disponibili creati utilizzando SnapCenter. L'area superiore di questa vista visualizza la topologia di backup che mostra i backup sullo storage primario (copie locali) e, se disponibile, sullo storage di backup off-site (copie del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

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



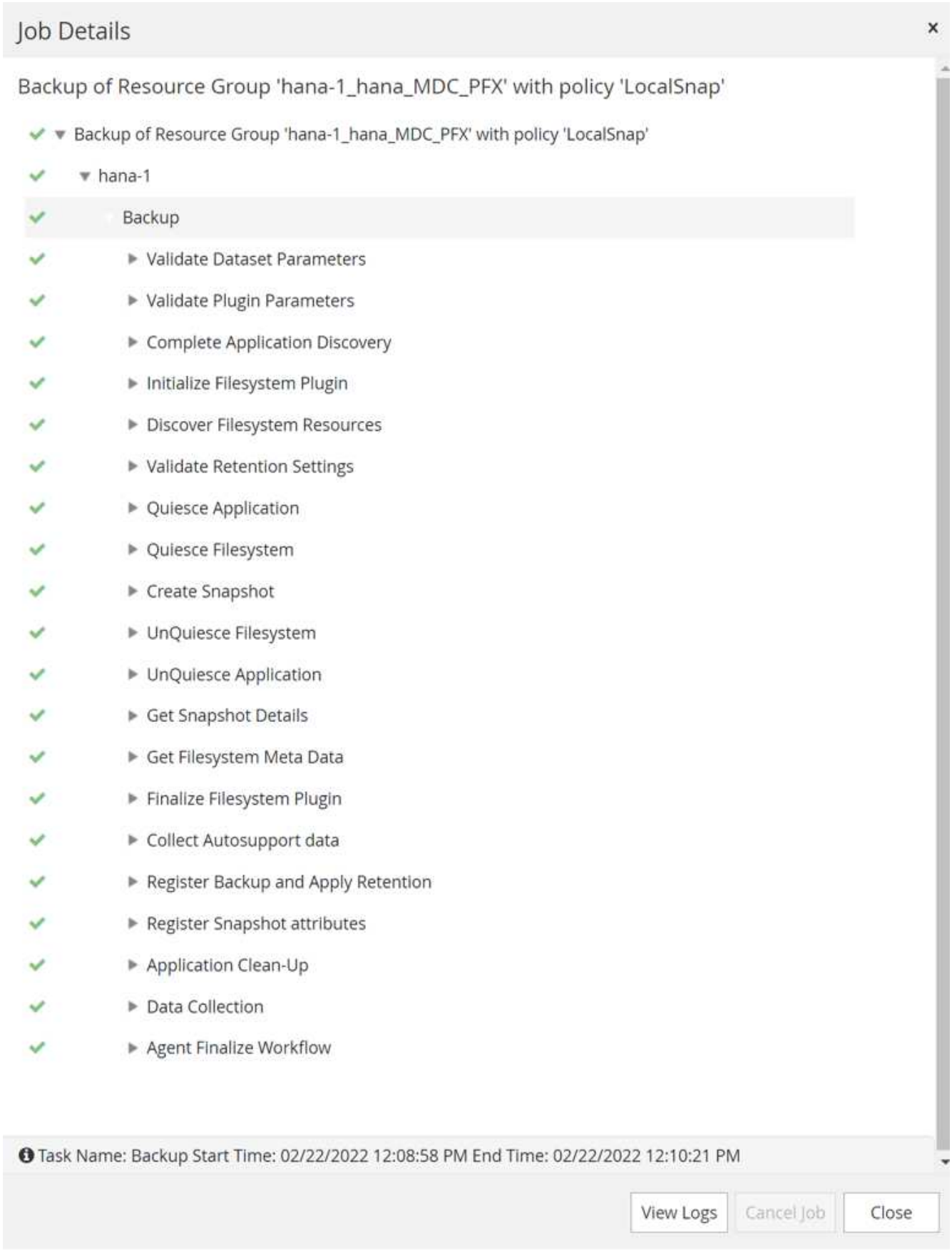
3. Dall'elenco a discesa, selezionare il criterio di backup `LocalSnap`, Quindi fare clic su Backup per avviare il backup on-demand.





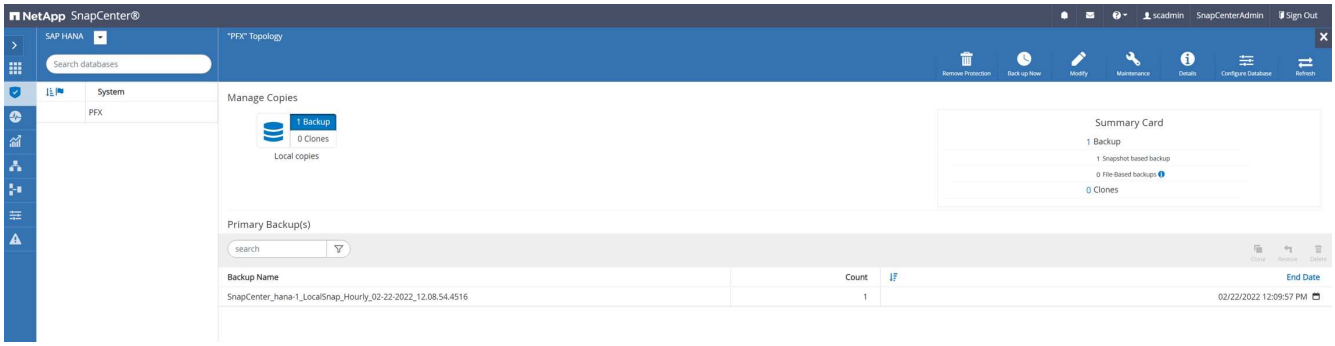
Un registro dei cinque job precedenti viene visualizzato nell'area Activity (attività) nella parte inferiore della vista Topology (topologia).

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

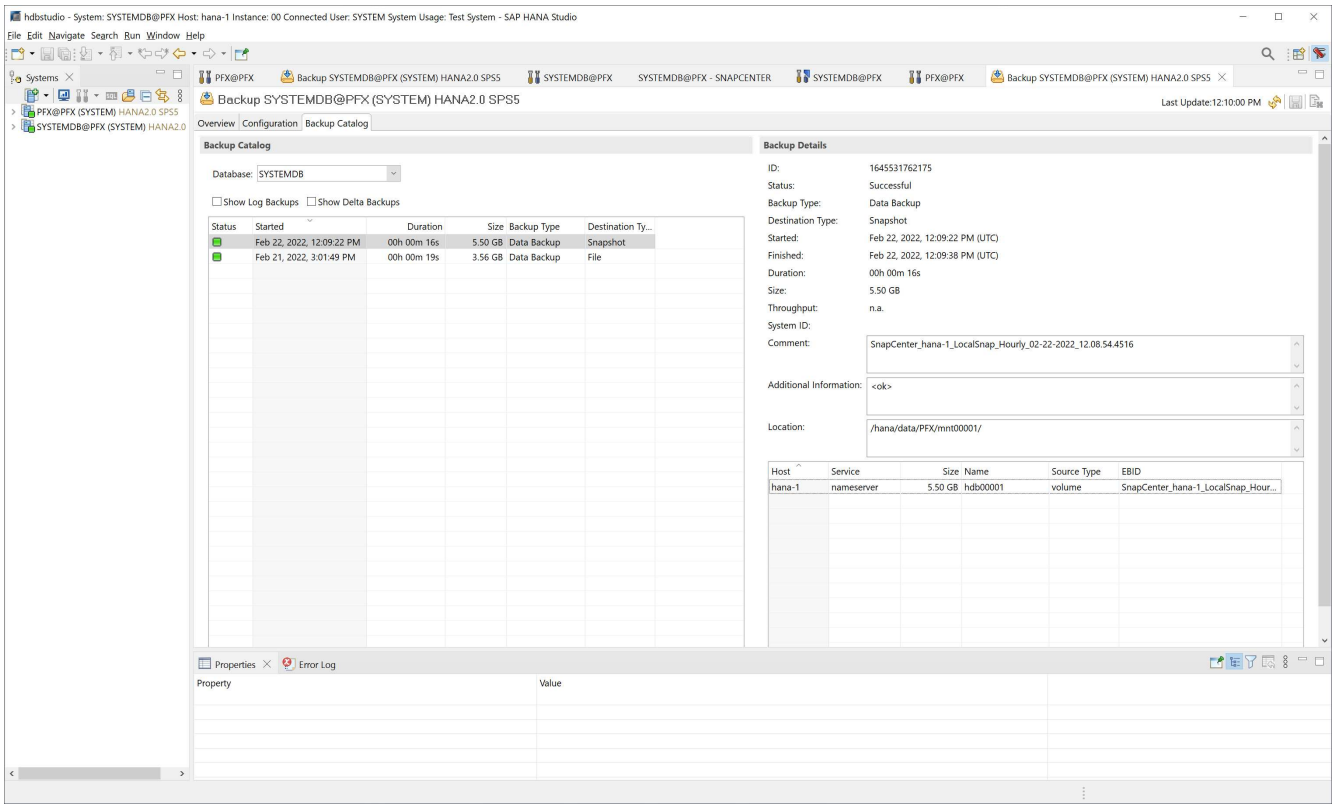


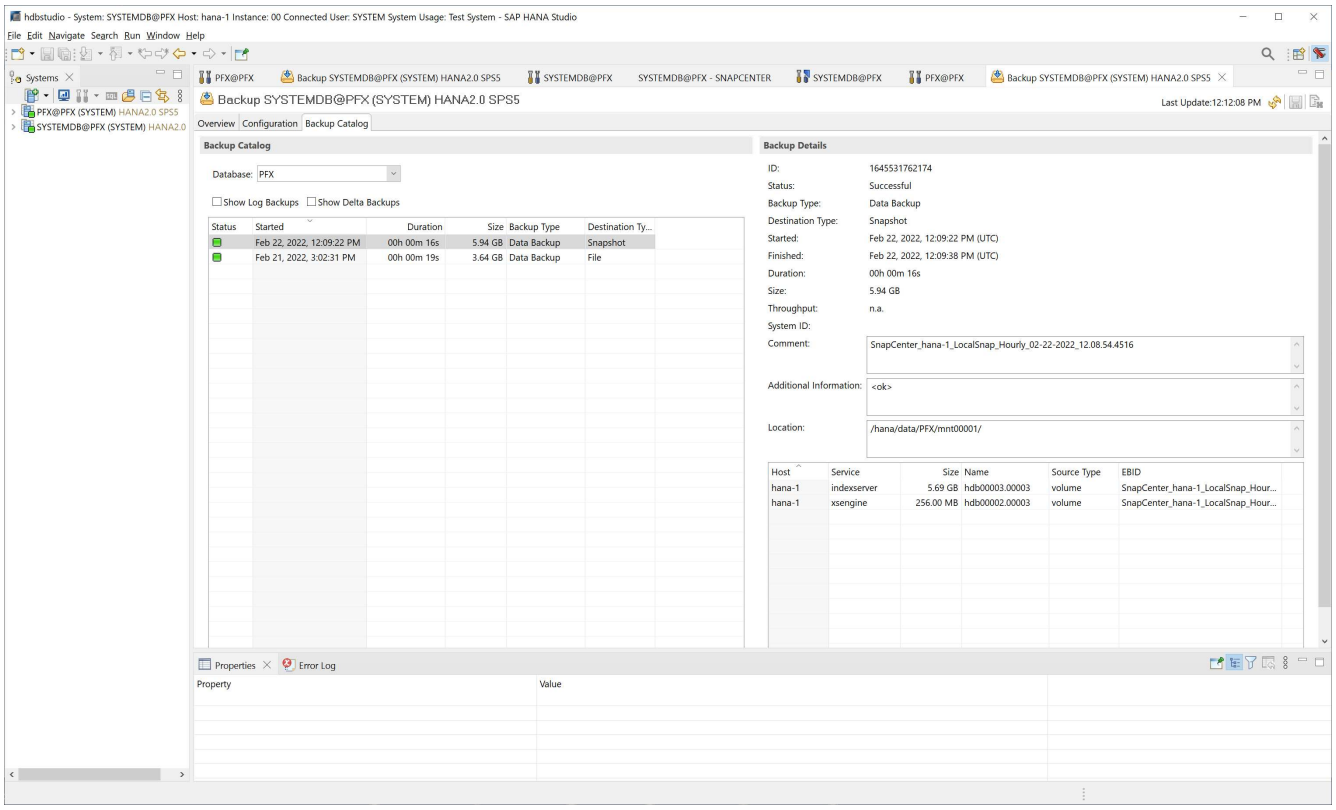
Al termine del backup, viene visualizzata una nuova voce nella vista della topologia. I nomi dei backup seguono la stessa convenzione di denominazione del nome dell'istantanea definita nella sezione ""Configurazione e protezione di una risorsa HANA"."

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



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



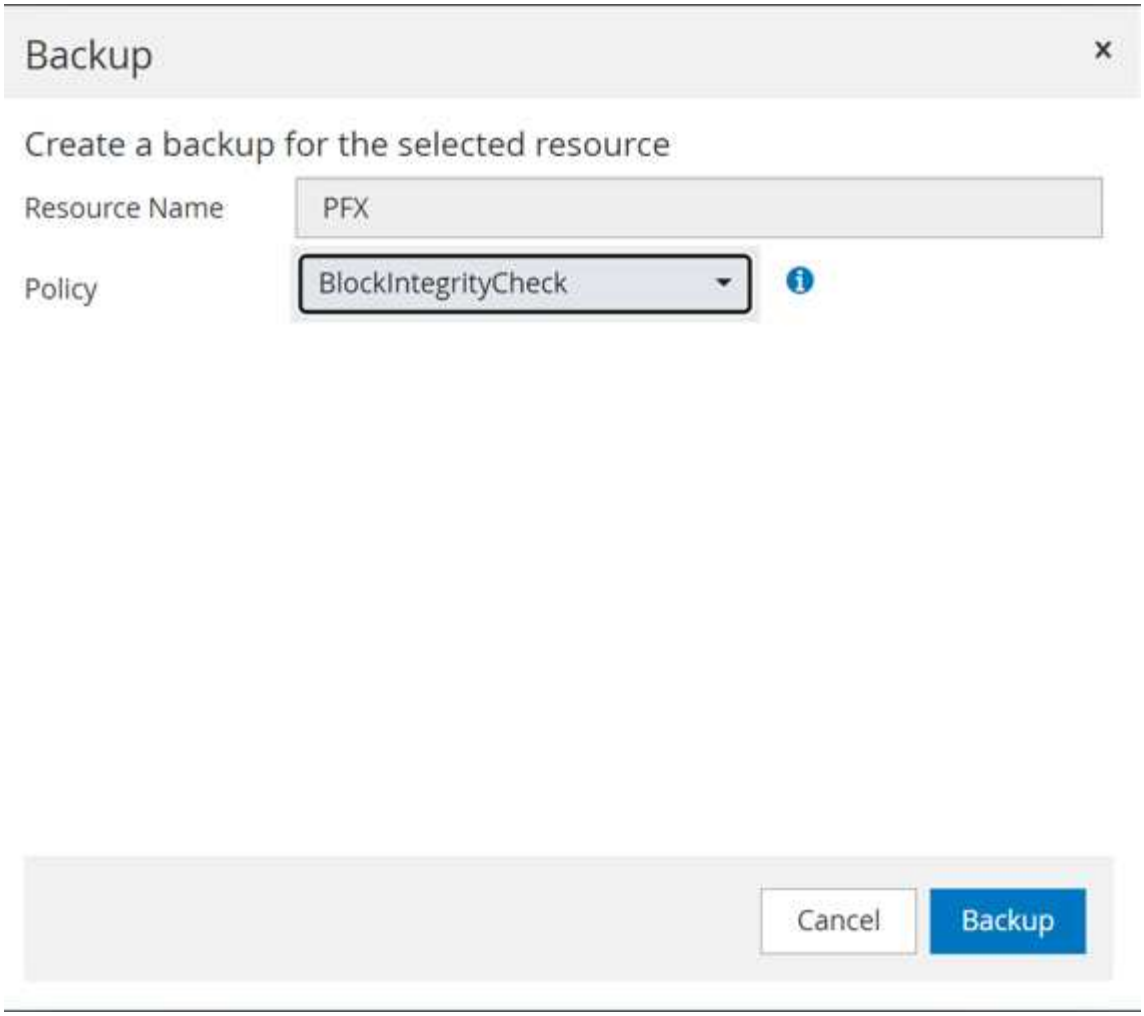


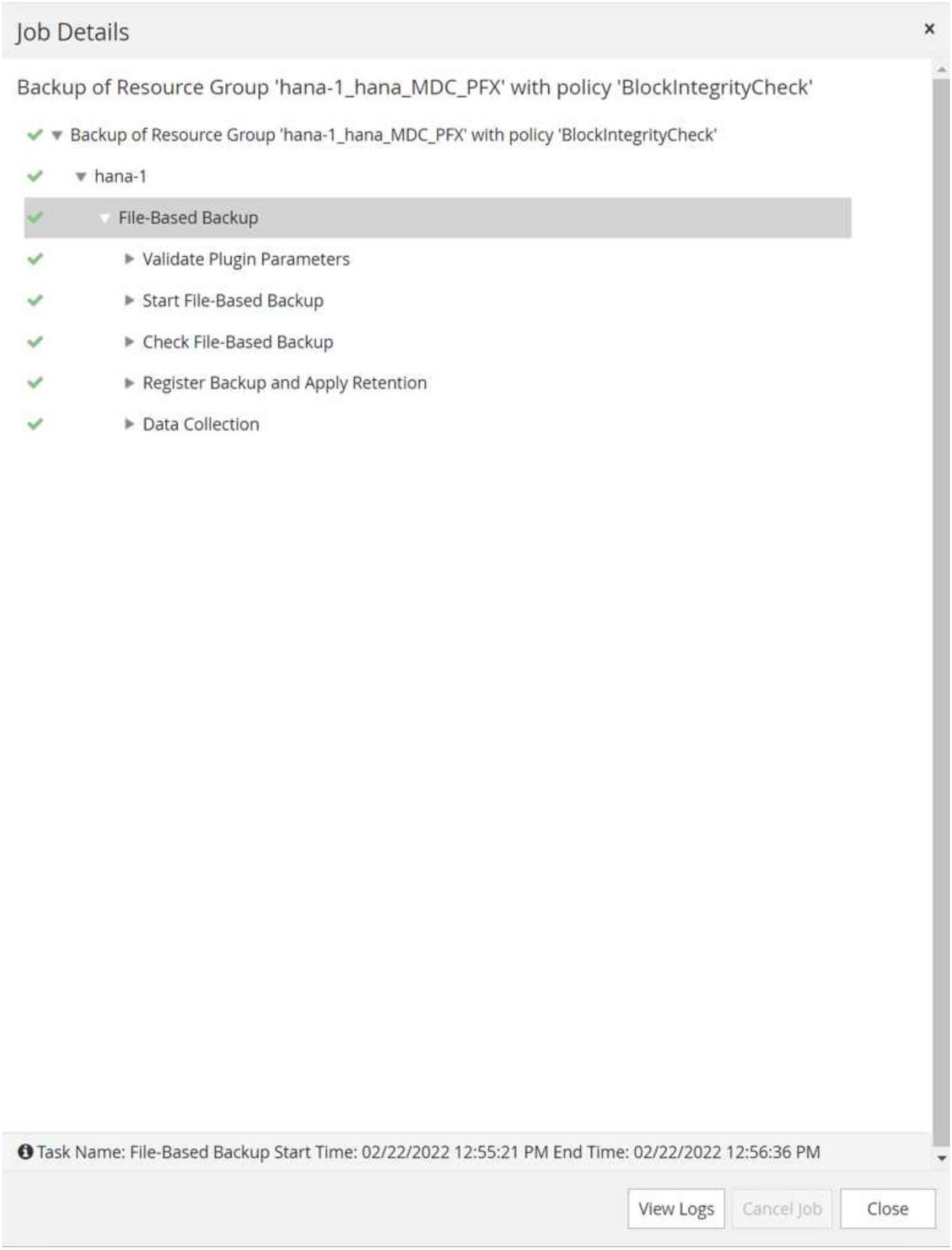
Nel file system FSX per ONTAP, è possibile elencare i backup Snapshot collegandosi alla console di SVM.

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

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

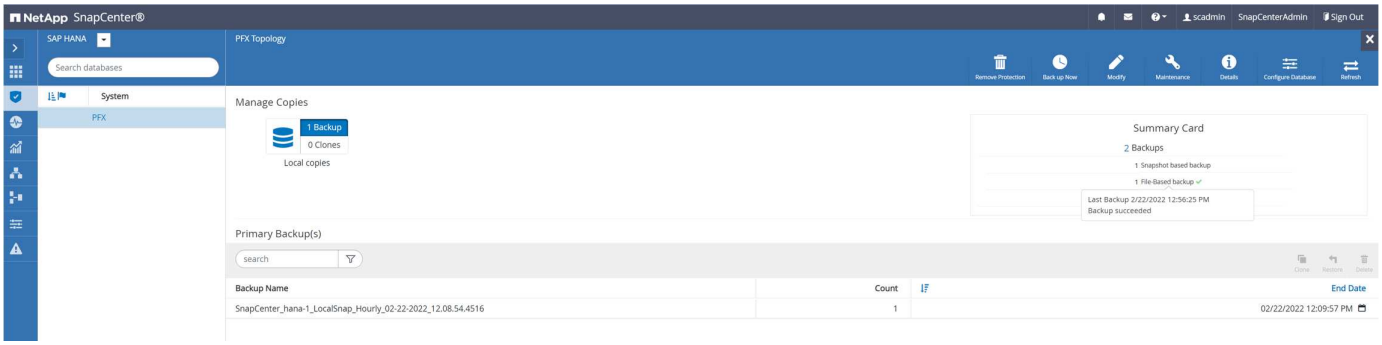
Un'operazione di verifica dell'integrità dei blocchi on-demand viene eseguita allo stesso modo di un processo di backup Snapshot, selezionando la policy BlockIntegrityCheck. Quando si pianificano i backup utilizzando questo criterio, SnapCenter crea un backup standard del file SAP HANA per i database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


Backup
Create a backup for the selected resource
Resource Name
PFX
Policy
BlockIntegrityCheck
Cancel
Backup

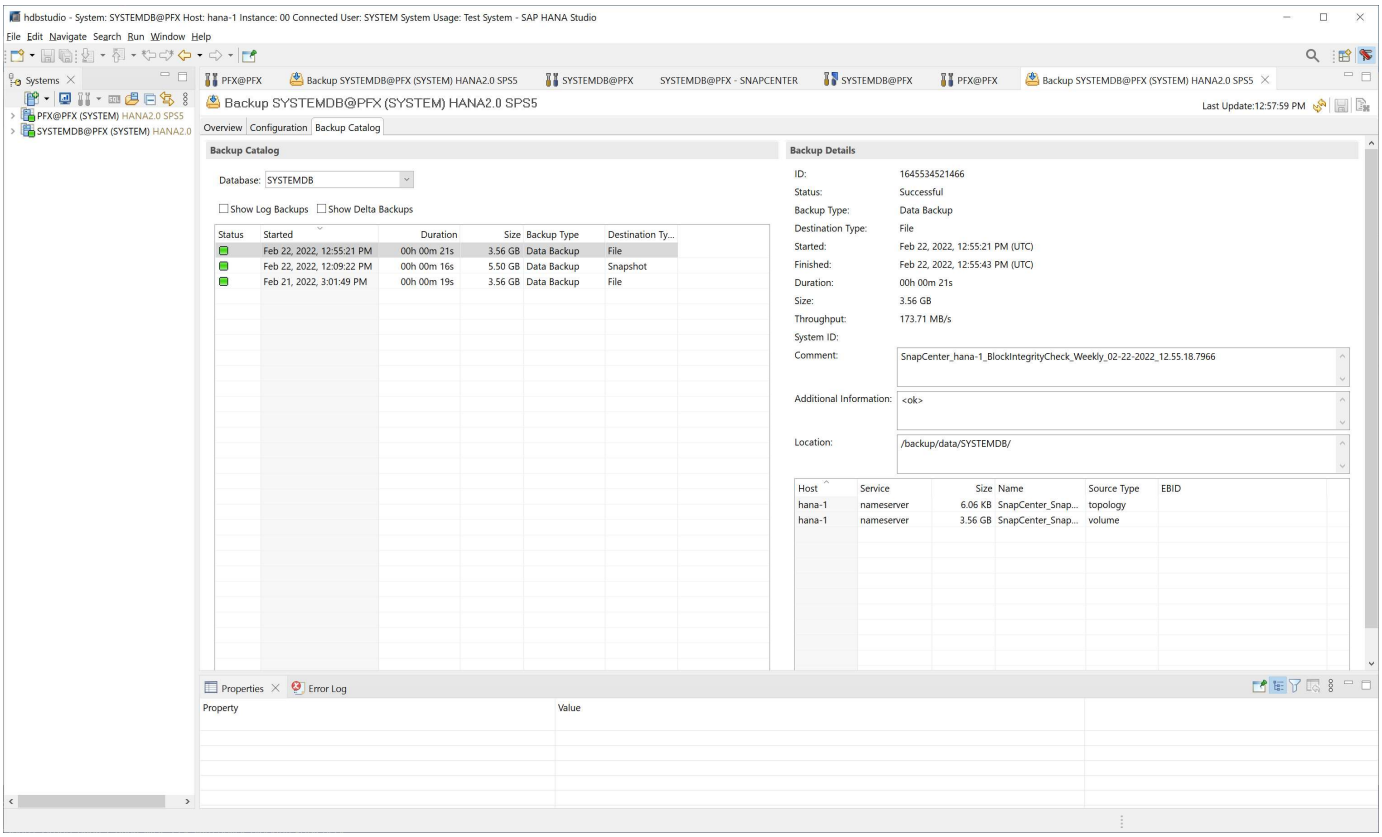


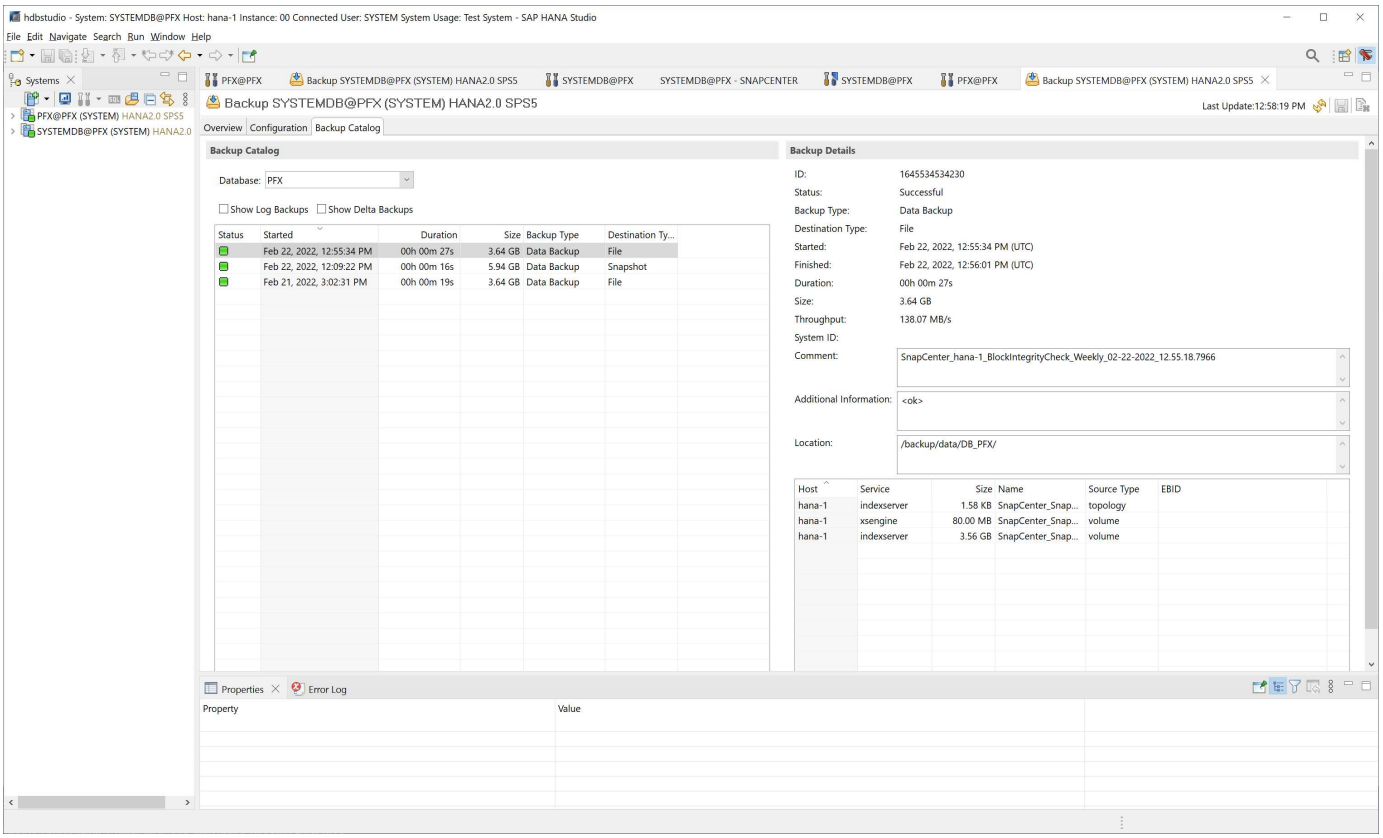
SnapCenter non visualizza il controllo dell'integrità del blocco allo stesso modo dei backup basati su copia

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



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





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

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

Backup di volumi non dati

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

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

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

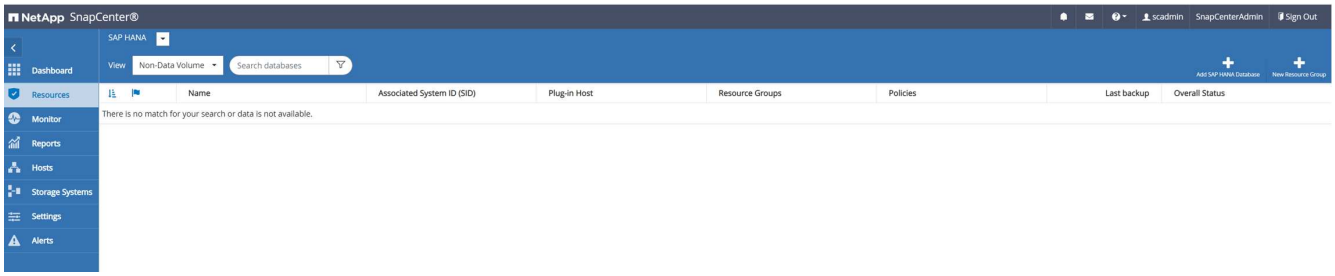
SAP HANA. A seconda dei requisiti specifici, il backup dei volumi non dati potrebbe differire in termini di frequenza di pianificazione e impostazioni di conservazione e si dovrebbe considerare la frequenza con cui i file non dati vengono modificati. Ad esempio, il volume HANA `/hana/shared` Contiene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

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

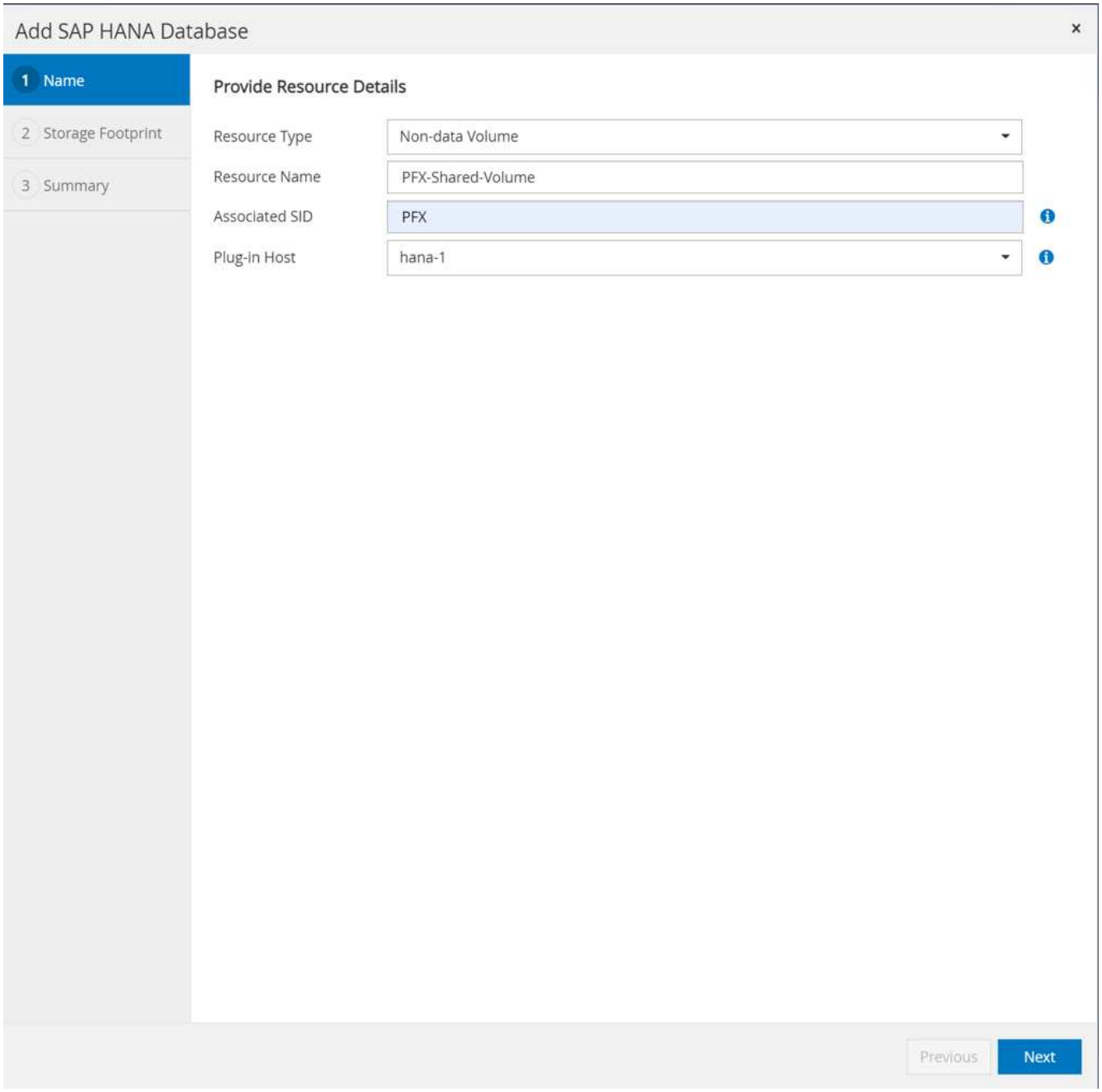
Configurare le risorse di volumi diversi dai dati

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

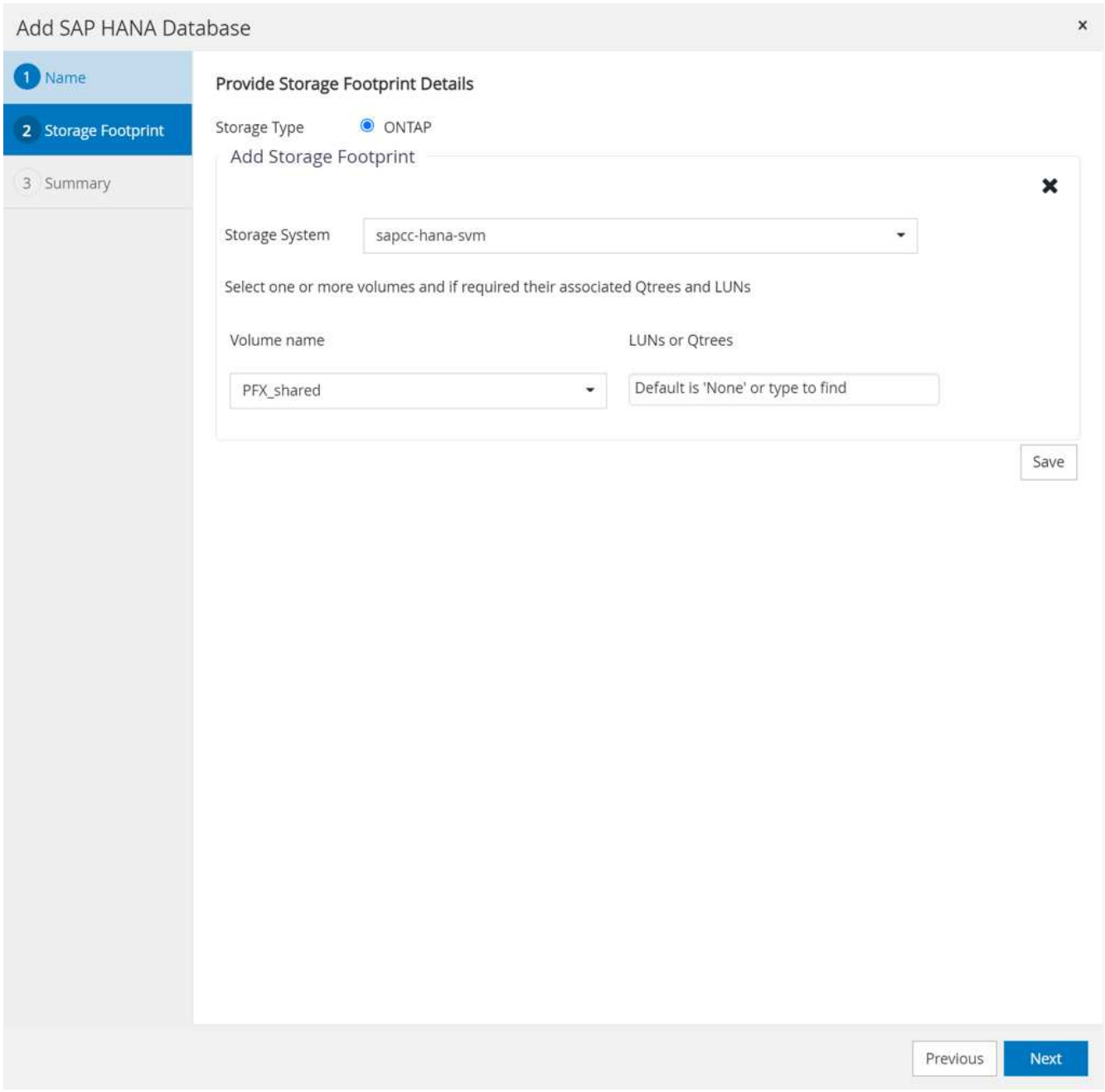
1. Dalla scheda Resources (risorse), selezionare non-Data-Volume e fare clic su Add SAP HANA Database (Aggiungi database SAP HANA).



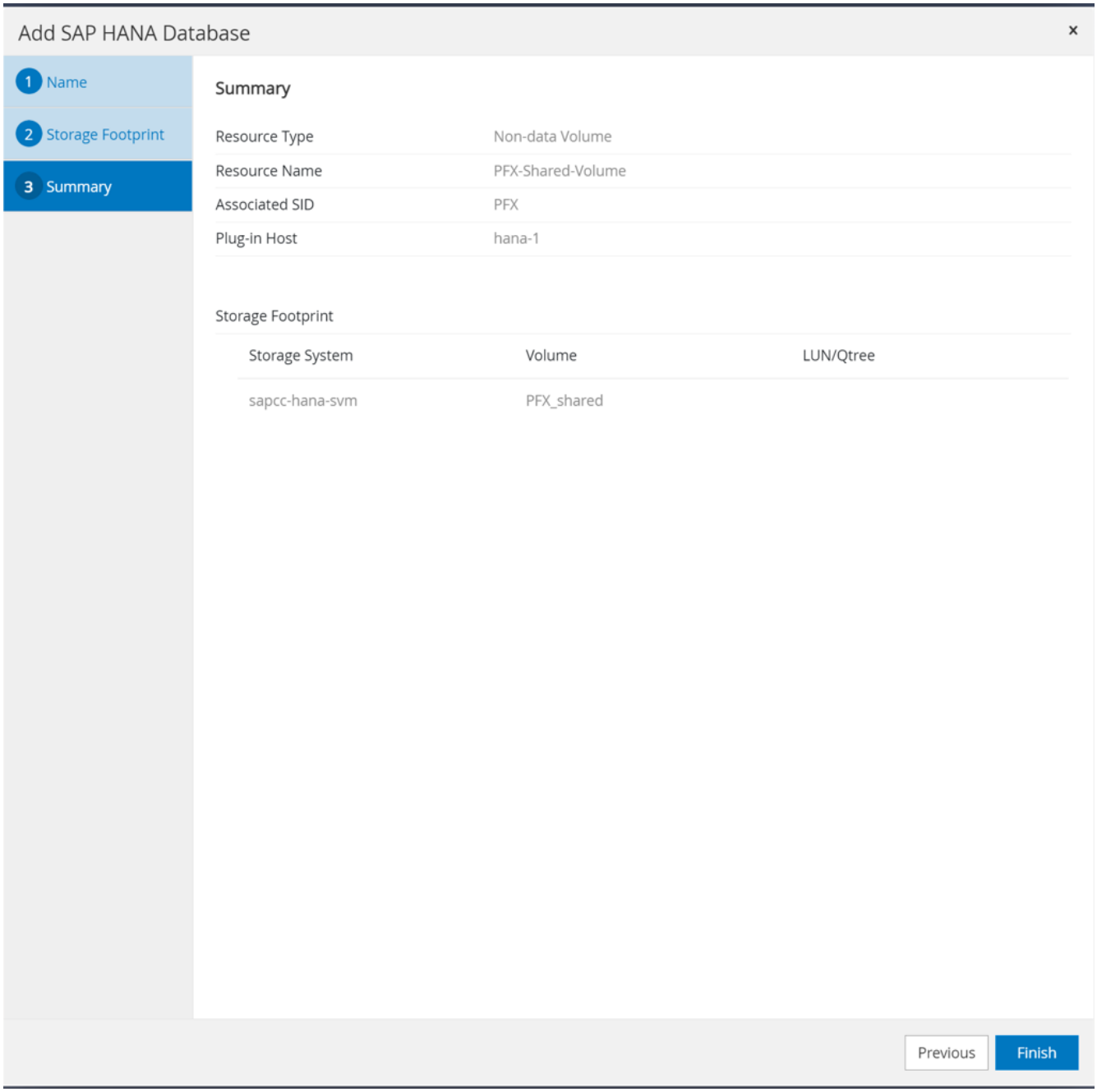
2. Nella fase uno della finestra di dialogo Add SAP HANA Database (Aggiungi database SAP HANA), nell'elenco Resource Type (tipo di risorsa), selezionare non-data Volumes (volumi non dati). Specificare un nome per la risorsa, il SID associato e l'host del plug-in SAP HANA che si desidera utilizzare per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



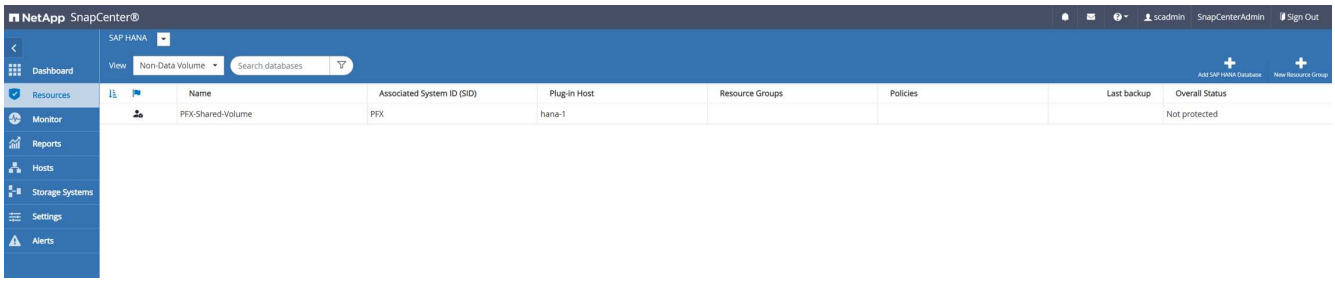
3. Aggiungere la SVM e il volume di storage come footprint dello storage, quindi fare clic su Next (Avanti).



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



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

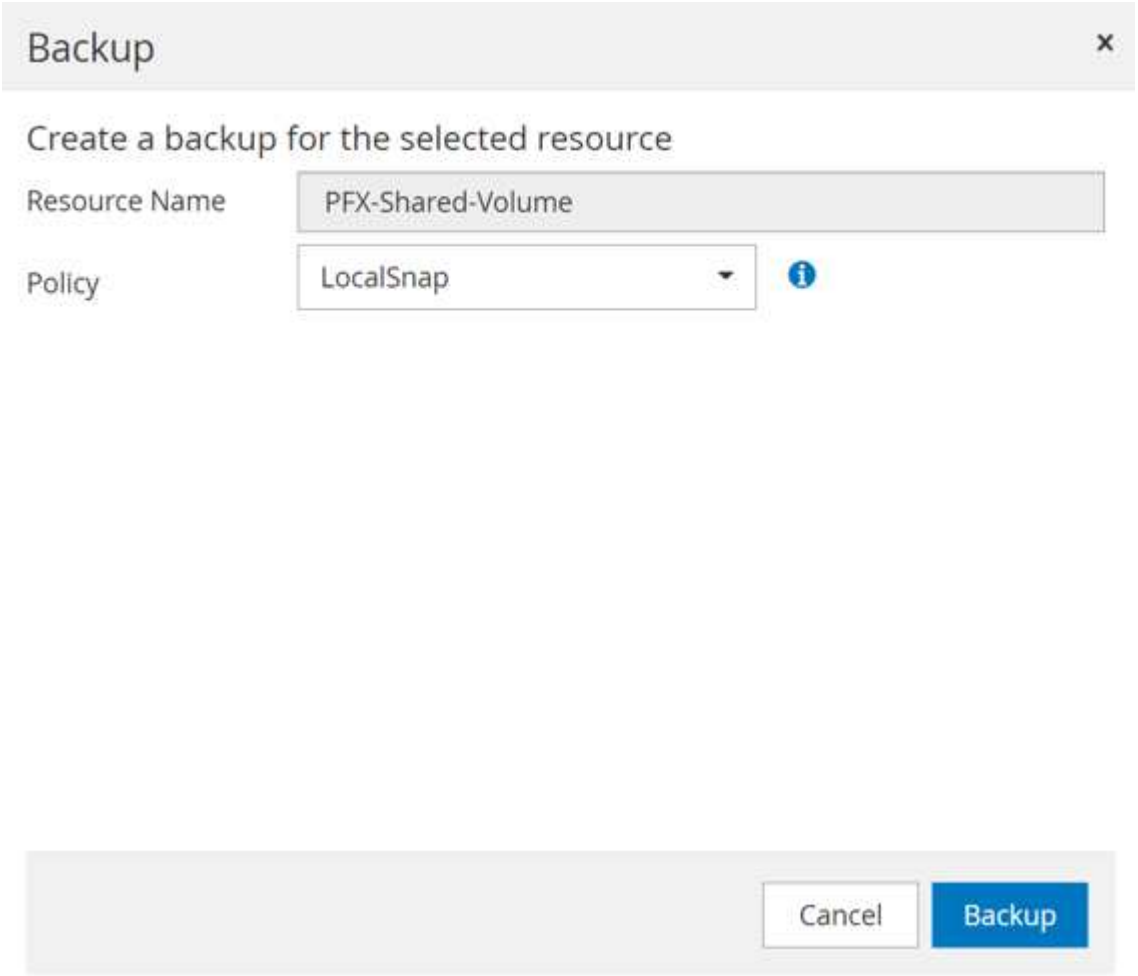


La protezione delle risorse viene eseguita nello stesso modo descritto in precedenza con una risorsa di database HANA.

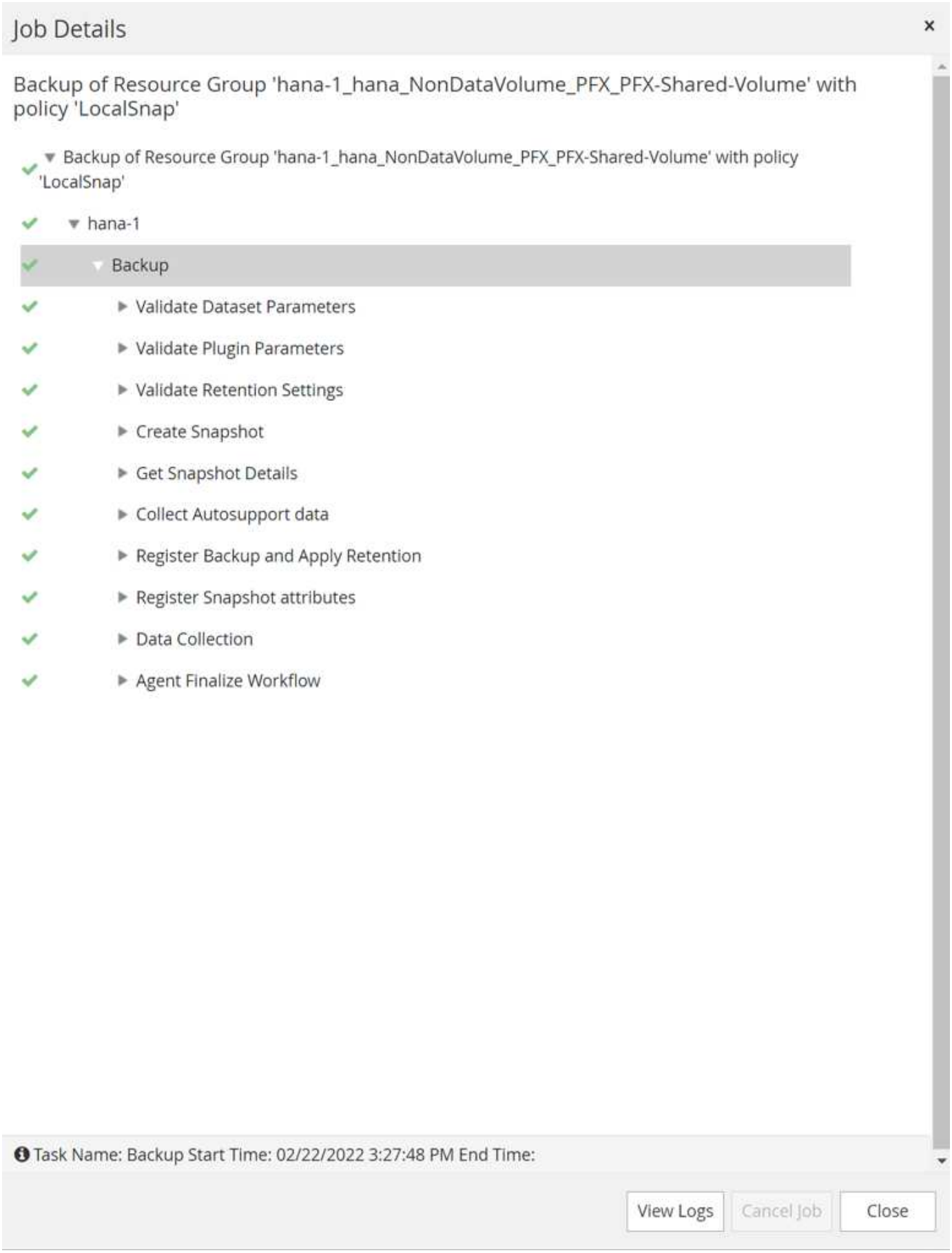
5. È ora possibile eseguire un backup facendo clic su Backup Now (Esegui backup ora).



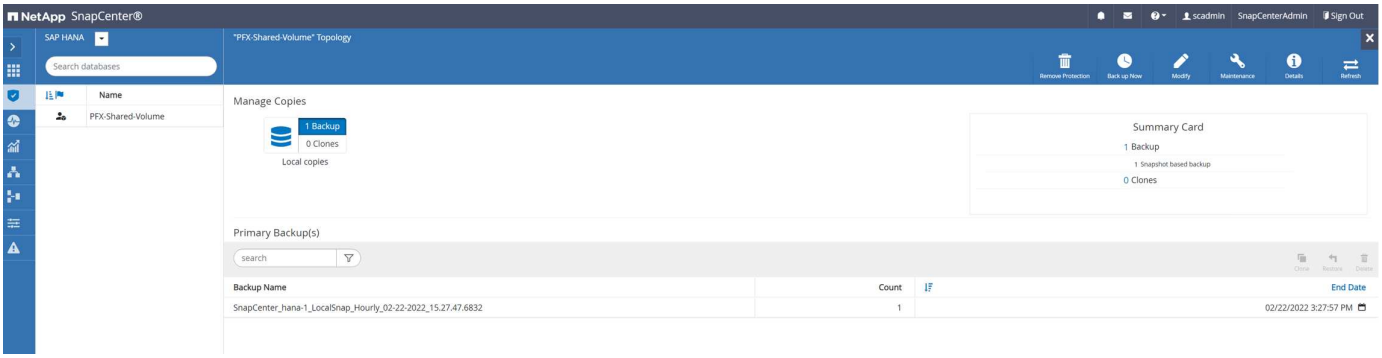
6. Selezionare il criterio e avviare l'operazione di backup.



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



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



Ripristinare e ripristinare

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

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

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

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

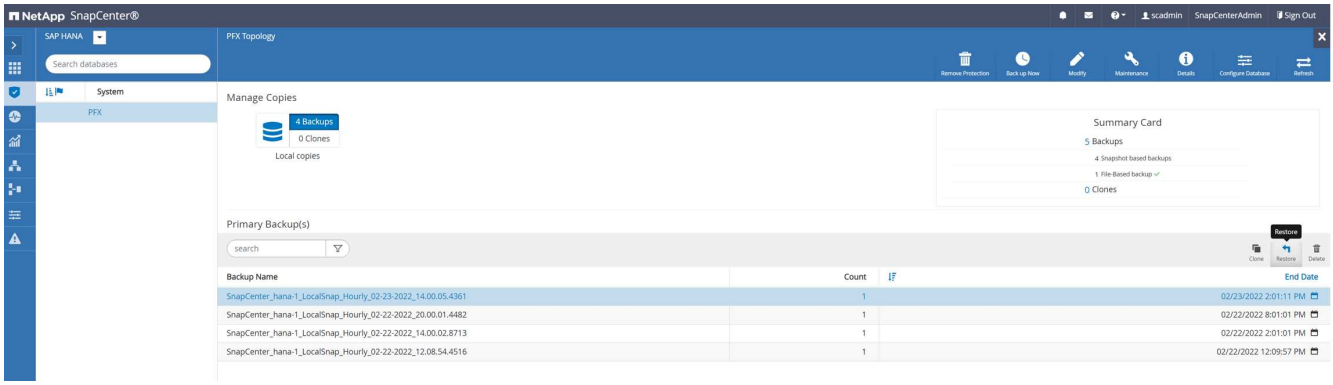
Successivamente, SnapCenter esegue le seguenti operazioni:

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

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

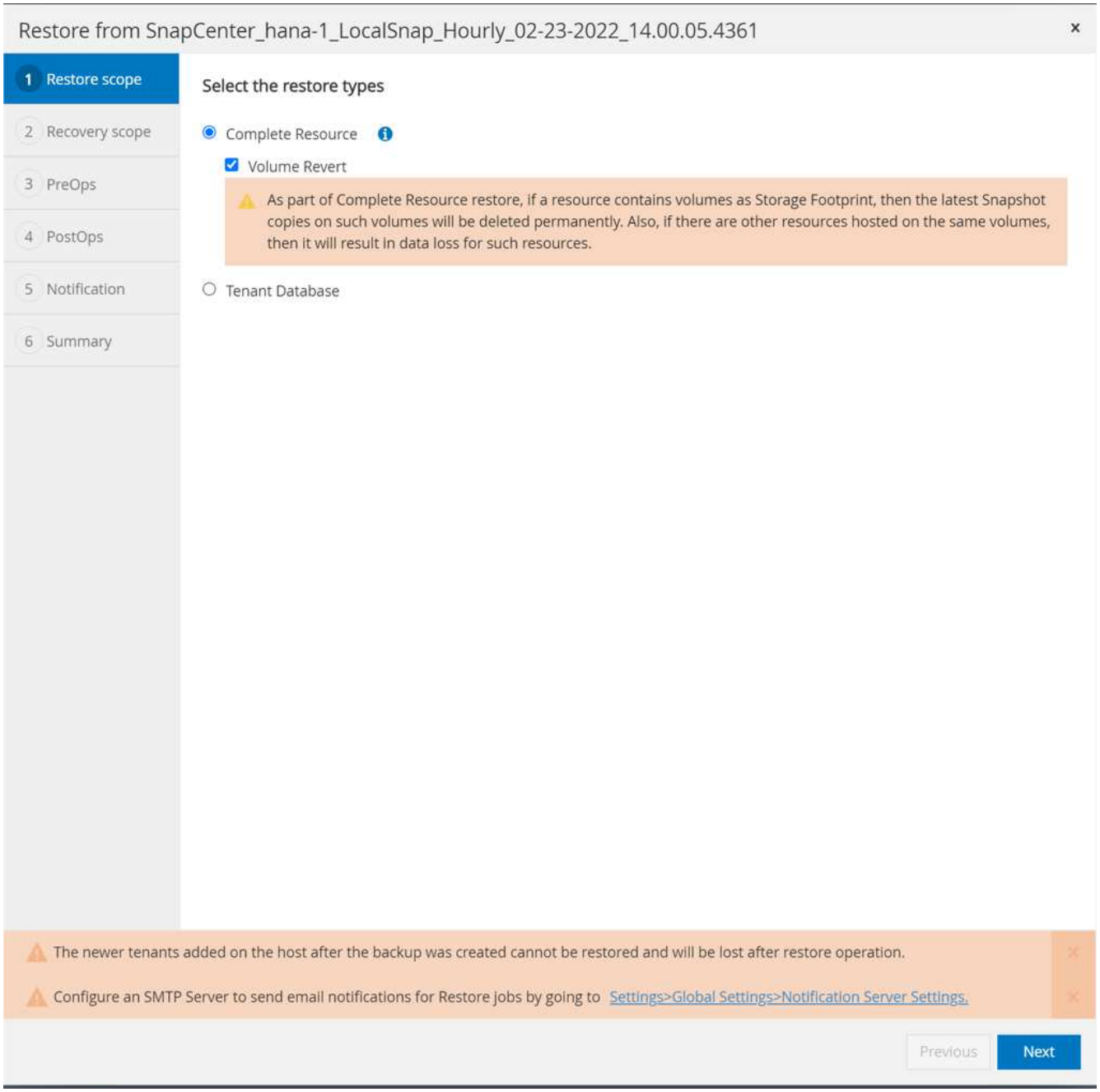
Per eseguire un'operazione di ripristino manuale, attenersi alla seguente procedura:

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



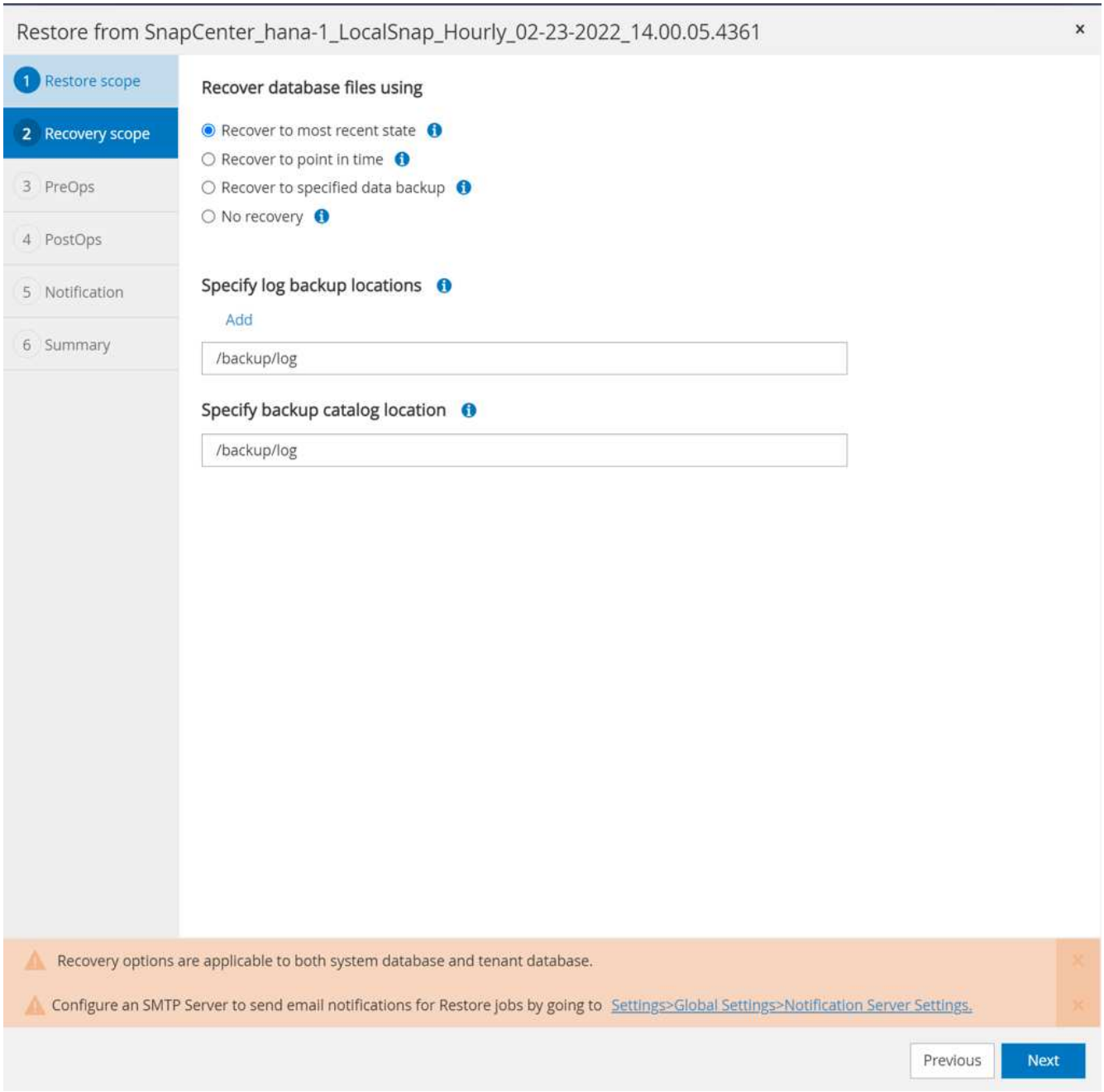
2. Selezionare l'ambito e il tipo di ripristino.

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

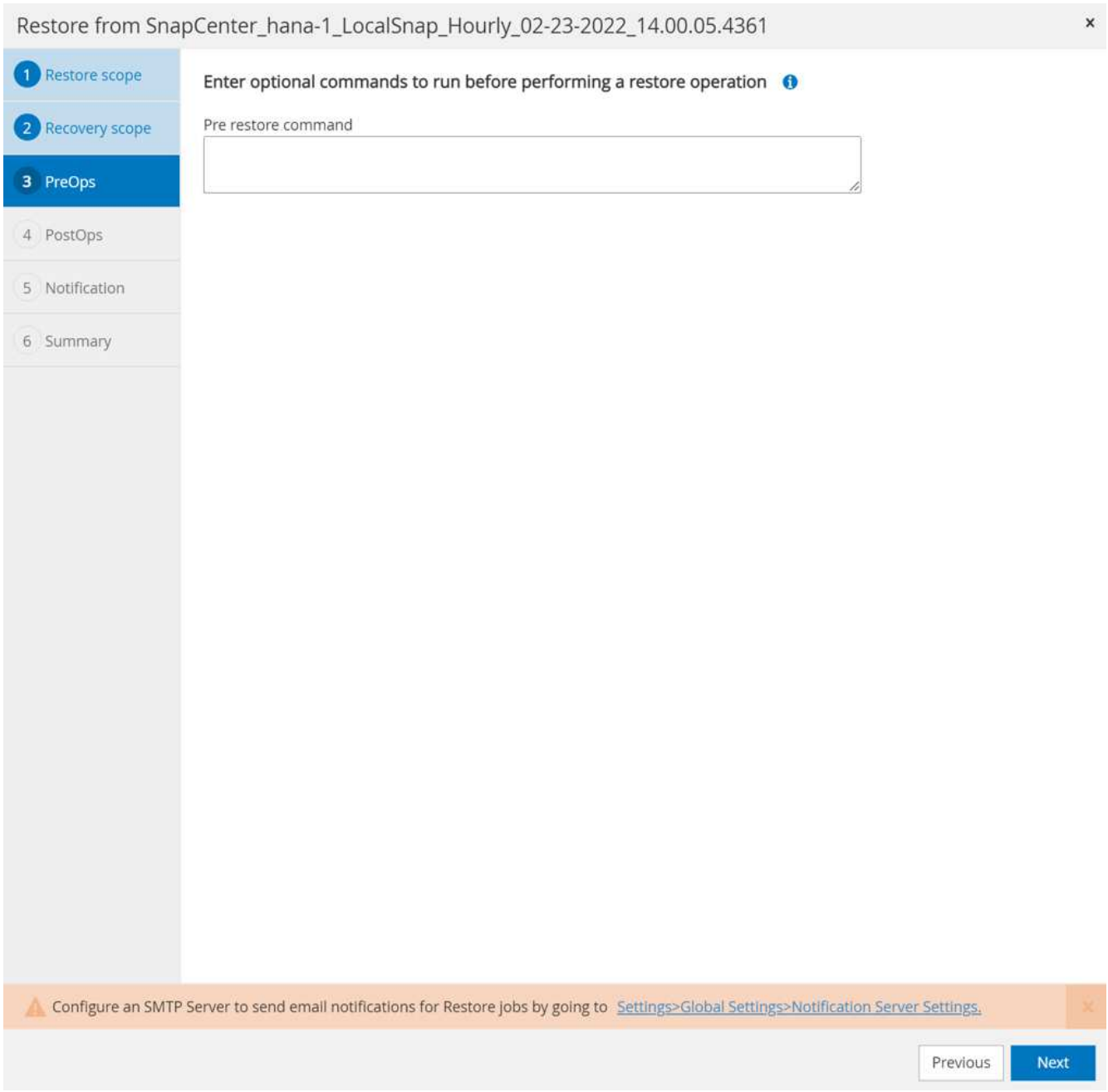


3. Selezionare Recovery Scope (ambito ripristino) e specificare la posizione per il backup del registro e del catalogo.

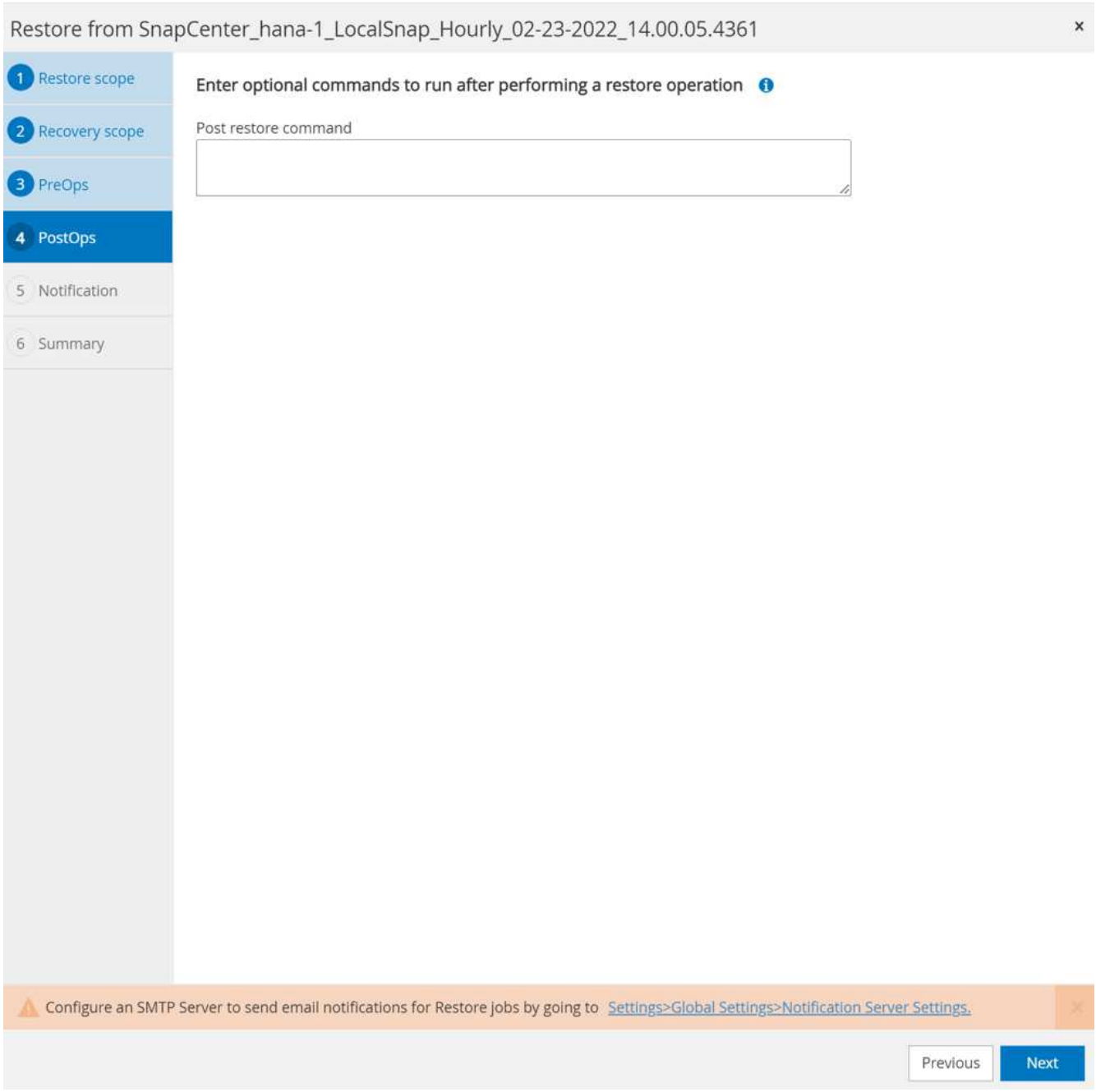
   SnapCenter utilizza il percorso predefinito o i percorsi modificati nel file HANA global.ini per prepopolare le posizioni di backup del registro e del catalogo.



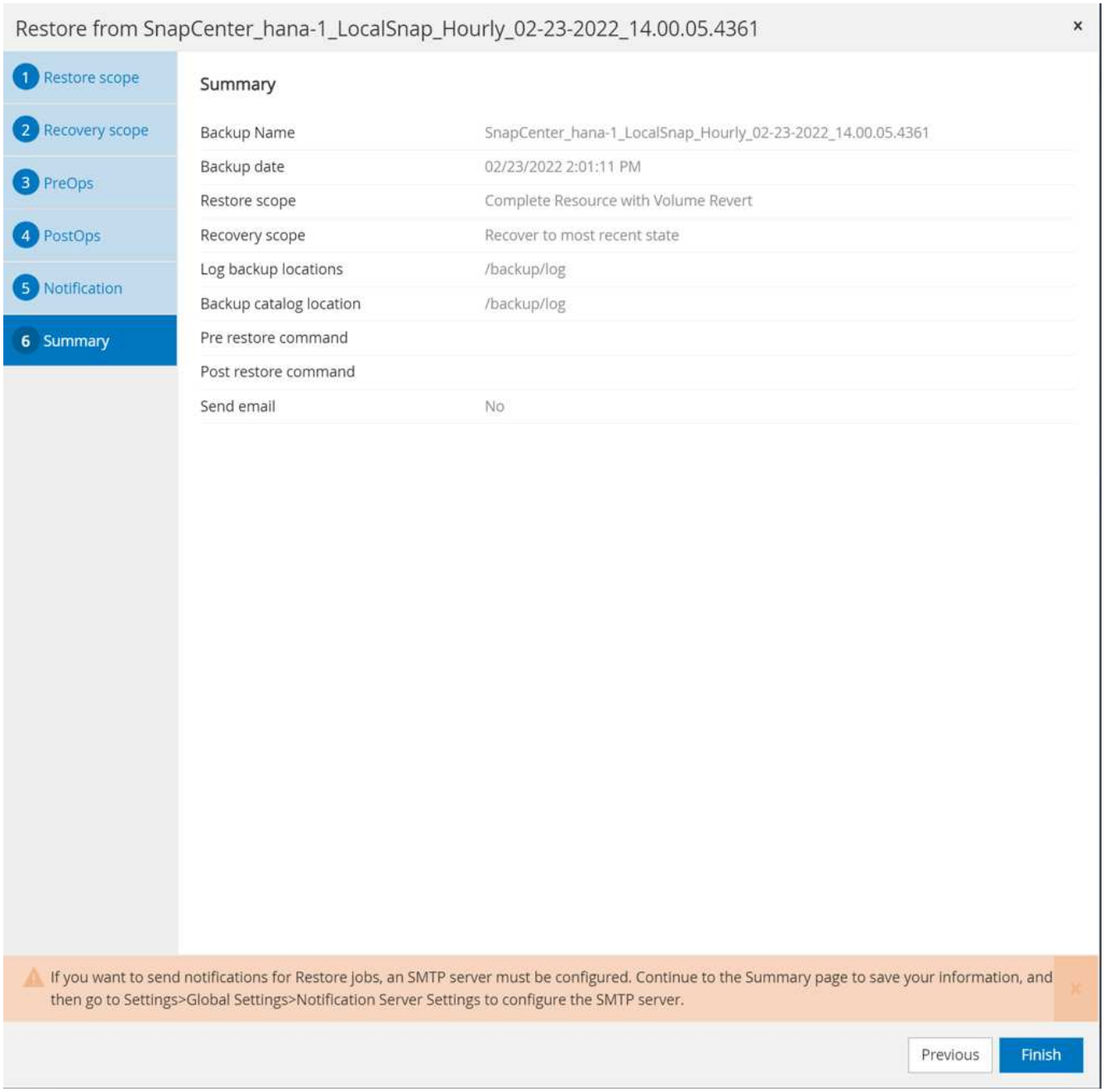
4. Immettere i comandi opzionali di pre-ripristino.



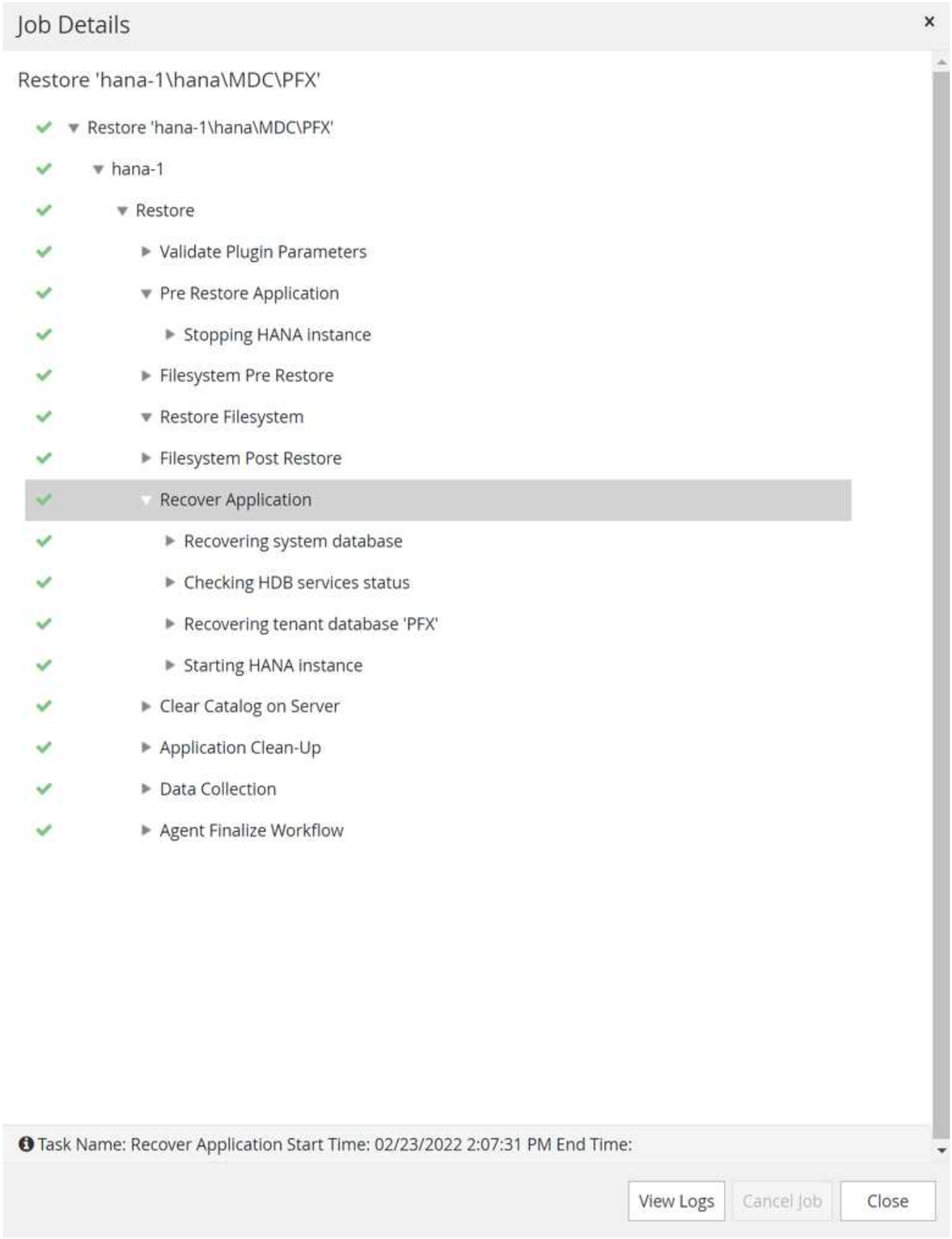
5. Immettere i comandi post-ripristino opzionali.



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



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

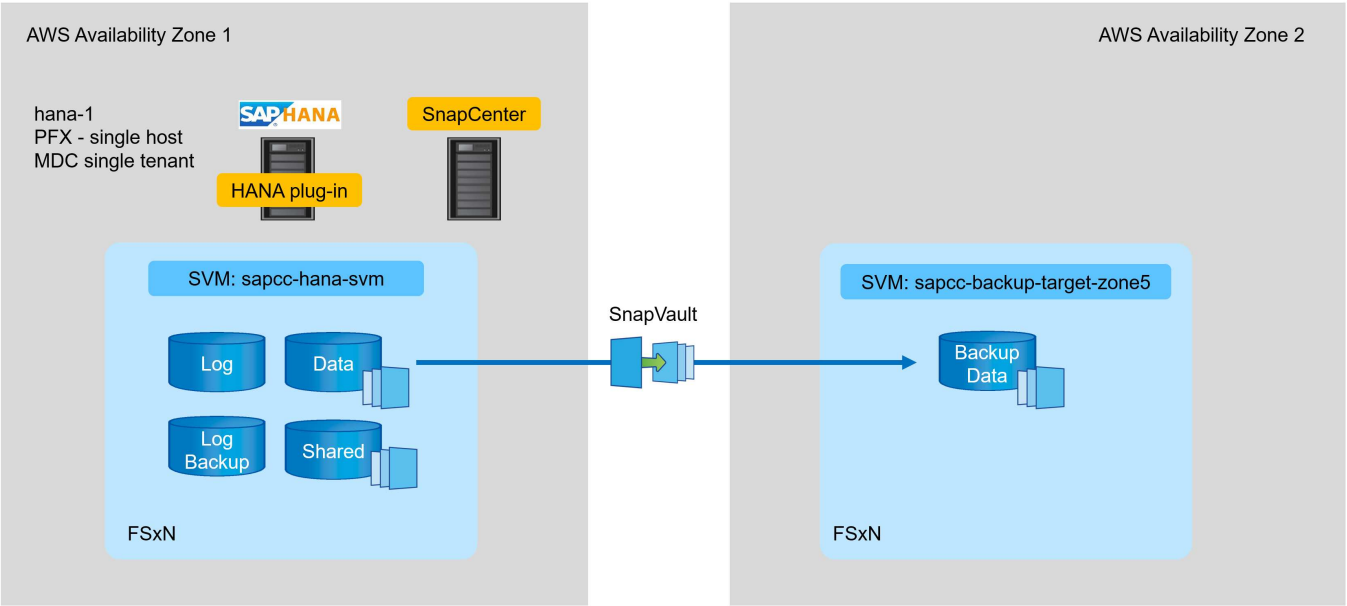

Job Details
Restore 'hana-1\hana\MDC\PFX'
Restore 'hana-1\hana\MDC\PFX'
hana-1
Restore
Validate Plugin Parameters
Pre Restore Application
Stopping HANA instance
Filesystem Pre Restore
Restore Filesystem
Filesystem Post Restore
Recover Application
Recovering system database
Checking HDB services status
Recovering tenant database 'PFX'
Starting HANA instance
Clear Catalog on Server
Application Clean-Up
Data Collection
Agent Finalize Workflow
Task Name: Recover Application Start Time: 02/23/2022 2:07:31 PM End Time:
View Logs
Cancel Job
Close

Replica del backup con SnapVault

Panoramica - replica di backup con SnapVault

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

Come illustrato nel capitolo ""Strategia di protezione dei dati"", la destinazione della replica deve essere un secondo file system FSX per ONTAP in un'altra zona di disponibilità per essere protetta da un errore del file system FSX per ONTAP primario. Inoltre, il volume condiviso HANA deve essere replicato nel file system FSX secondario per ONTAP.



Panoramica delle fasi di configurazione

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

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

vengono trasferiti al volume di destinazione.

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

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

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

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

Per ulteriori informazioni sulle opzioni di configurazione di SnapMirror, consultare la documentazione di ONTAP all'indirizzo "Workflow di replica di SnapMirror (netapp.com)".

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

Peer FSX per file system ONTAP

```
FsxId00fa9e3c784b6abbb::> network interface show -role intercluster
            Logical    Status     Network            Current       Current
Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ ------------- -------
----
FsxId00fa9e3c784b6abbb
            inter_1      up/up    10.1.1.57/24
FsxId00fa9e3c784b6abbb-01
                                                                   e0e
true
            inter_2      up/up    10.1.2.7/24
FsxId00fa9e3c784b6abbb-02
                                                                   e0e
true
2 entries were displayed.
```

```
FsxId05f7f00af49dc7a3e::> network interface show -role intercluster
            Logical    Status     Network            Current       Current
Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ ------------- -------
----
FsxId05f7f00af49dc7a3e
            inter_1      up/up    10.1.2.144/24
FsxId05f7f00af49dc7a3e-01
                                                                   e0e
true
            inter_2      up/up    10.1.2.69/24
FsxId05f7f00af49dc7a3e-02
                                                                   e0e
true
2 entries were displayed.
```

```
FsxId05f7f00af49dc7a3e::> cluster peer create -address-family ipv4 -peer
-addrs 10.1.1.57, 10.1.2.7
Notice: Use a generated passphrase or choose a passphrase of 8 or more
characters. To ensure the authenticity of the peering relationship, use a
phrase or sequence of characters that would be hard to guess.
Enter the passphrase:
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command
in the other cluster.
```

`peer-addrs` Sono gli IP del cluster di destinazione.

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

SVM peer

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

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

```
FsxId05f7f00af49dc7a3e::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
sapcc-backup-target-zone5
            peer-source-cluster
                        peered       FsxId00fa9e3c784b6abbb
                                                       snapmirror
sapcc-hana-svm
```

Creare un volume di destinazione

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

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

Creare un criterio SnapMirror

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

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

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

```
FsxId00fa9e3c784b6abbb::> snapmirror policy showVserver Policy
Policy Number         Transfer
Name    Name               Type   Of Rules Tries Priority Comment
------- ------------------ ------ -------- ----- -------- ----------
FsxId00fa9e3c784b6abbb
        snapcenter-policy  vault         1     8  normal  -
  SnapMirror Label: snapcenter                          Keep:      14
                                                  Total Keep:      14
```

Creare una relazione SnapMirror

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

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

Inizializzare SnapMirror

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

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

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

```
FsxId05f7f00af49dc7a3e::> snapmirror show

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

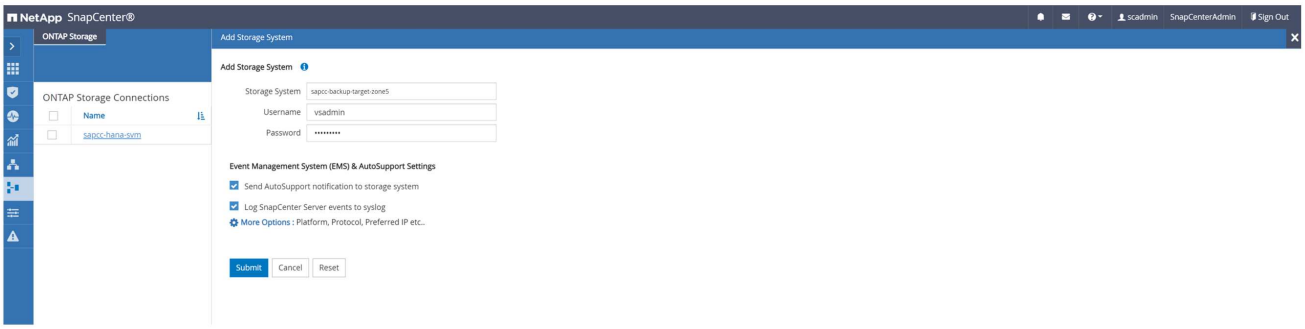
```
FsxId05f7f00af49dc7a3e::> snapmirror show

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

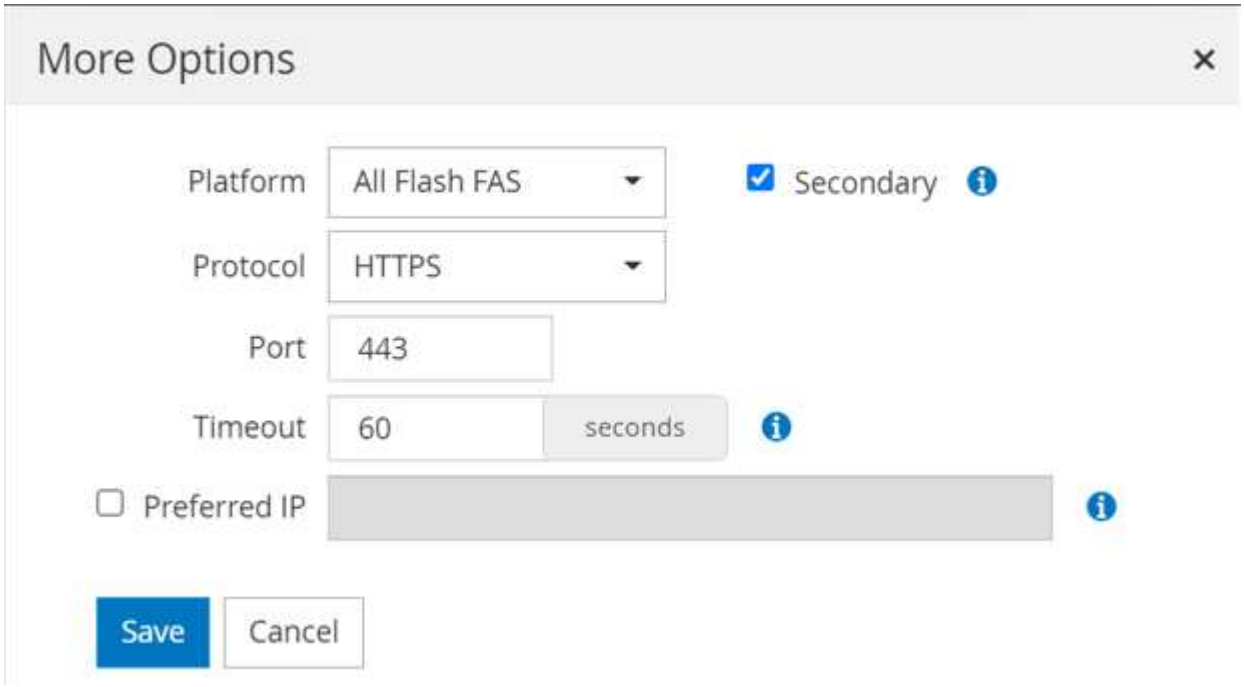
Aggiungere una SVM di backup a SnapCenter

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

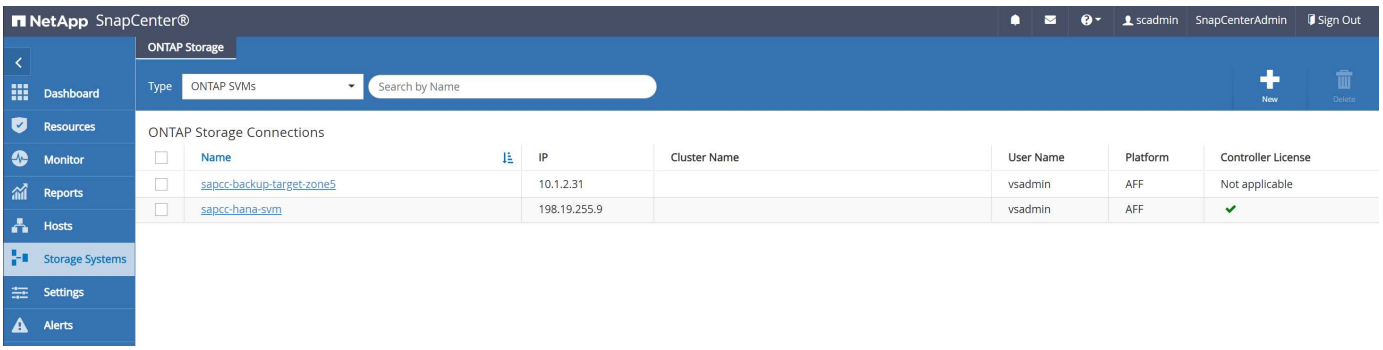
1. Configurare la SVM in cui si trova il volume di destinazione SnapVault in SnapCenter.



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



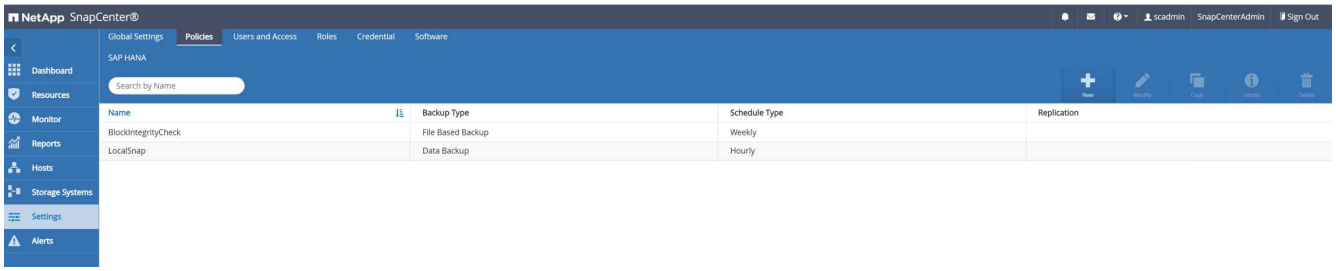
La SVM è ora disponibile in SnapCenter.



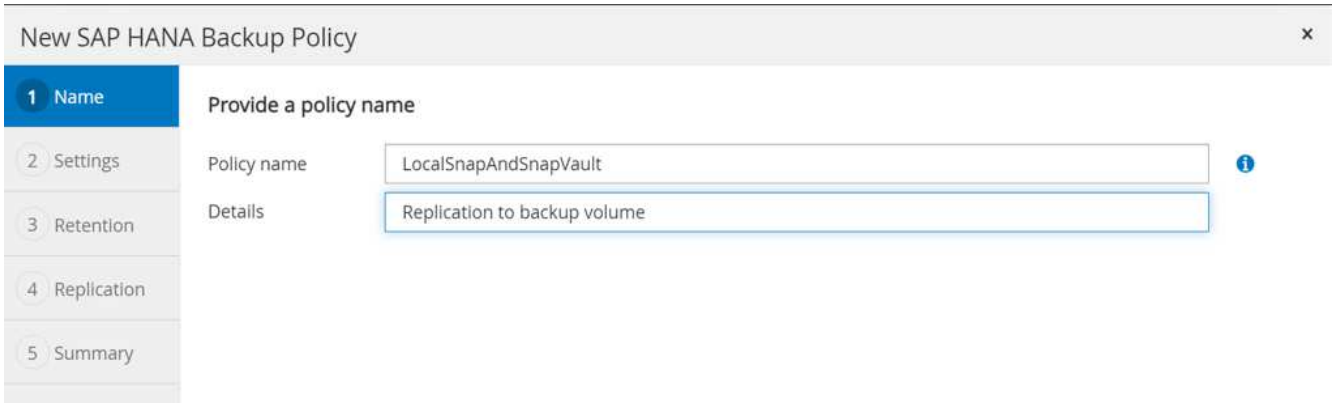
Creare un nuovo criterio SnapCenter per la replica del backup

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

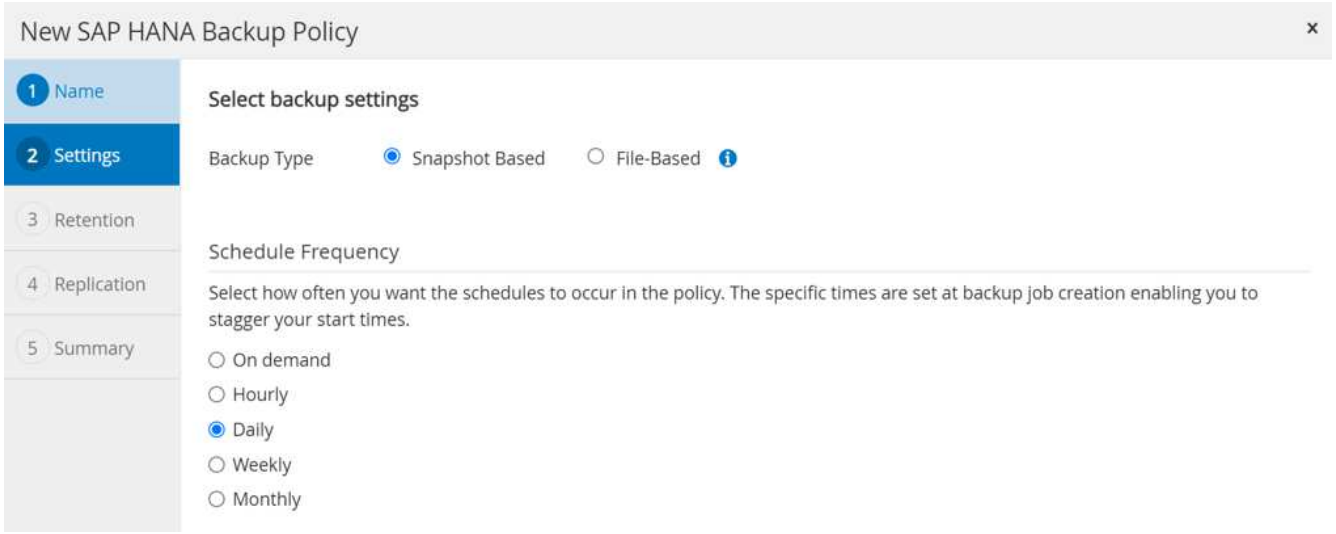
1. Specificare un nome per il criterio.



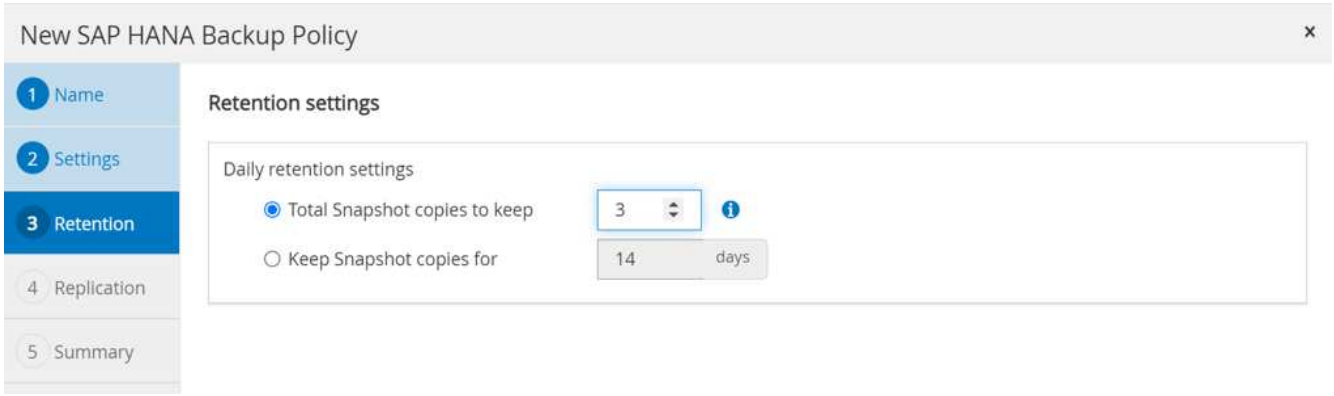
2. Selezionare Snapshot backup (Backup Snapshot) e una frequenza di pianificazione. Daily viene generalmente utilizzato per la replica del backup.



3. Selezionare la conservazione per i backup Snapshot.

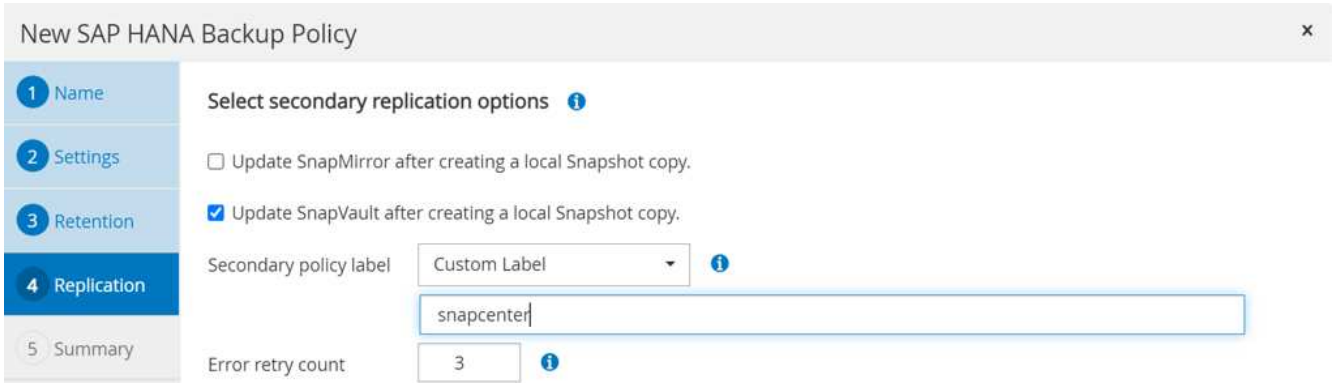


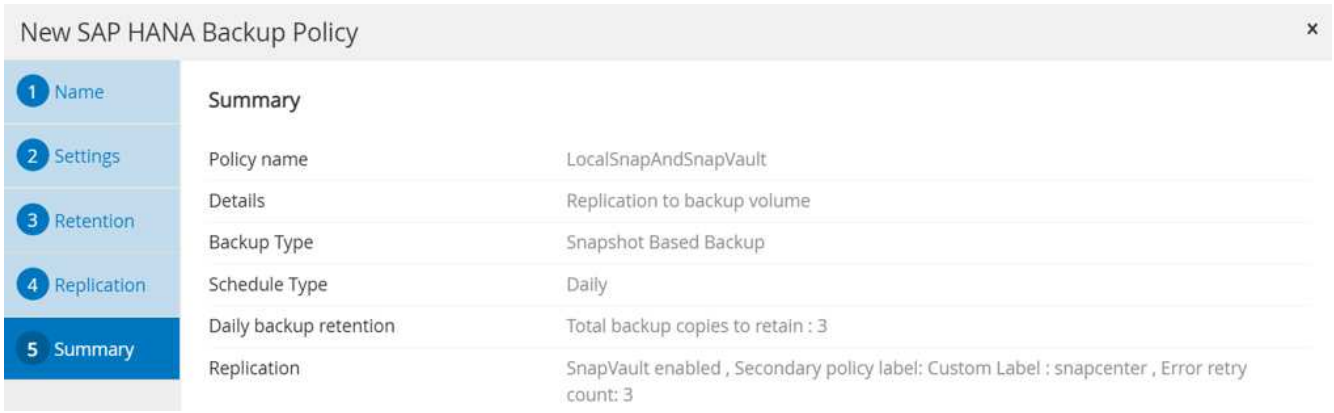
Questa è la conservazione dei backup Snapshot giornalieri eseguiti sullo storage primario. La conservazione per i backup secondari nella destinazione SnapVault è già stata configurata in precedenza utilizzando il comando add rule a livello di ONTAP. Vedere "Configurazione delle relazioni di replica su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



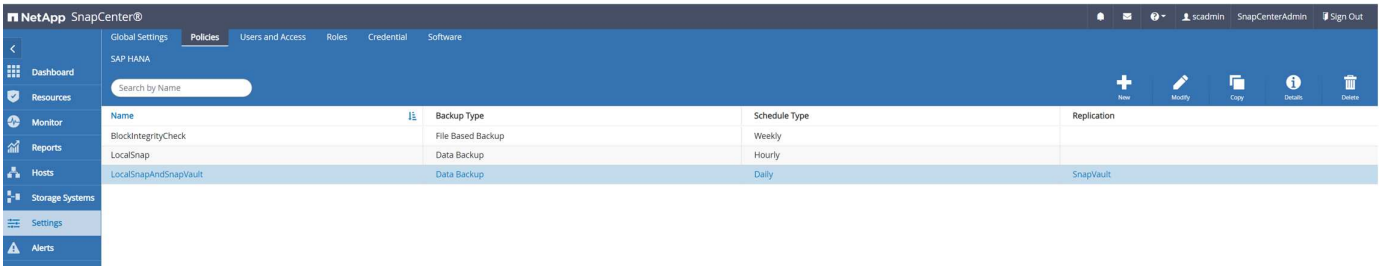
4. Selezionare il campo Update SnapVault (Aggiorna etichetta) e fornire un'etichetta personalizzata.

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



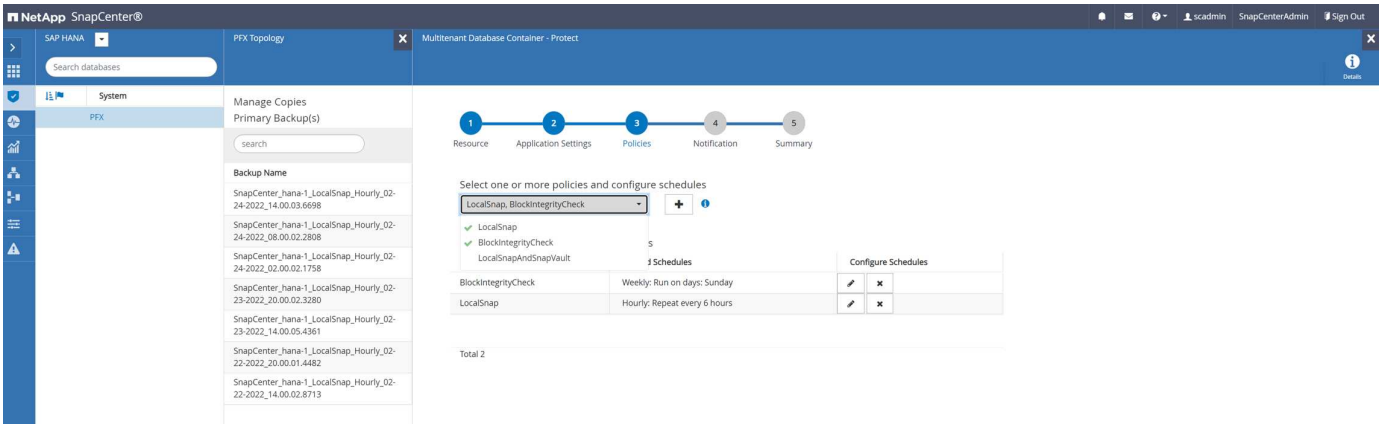


Il nuovo criterio SnapCenter è ora configurato.

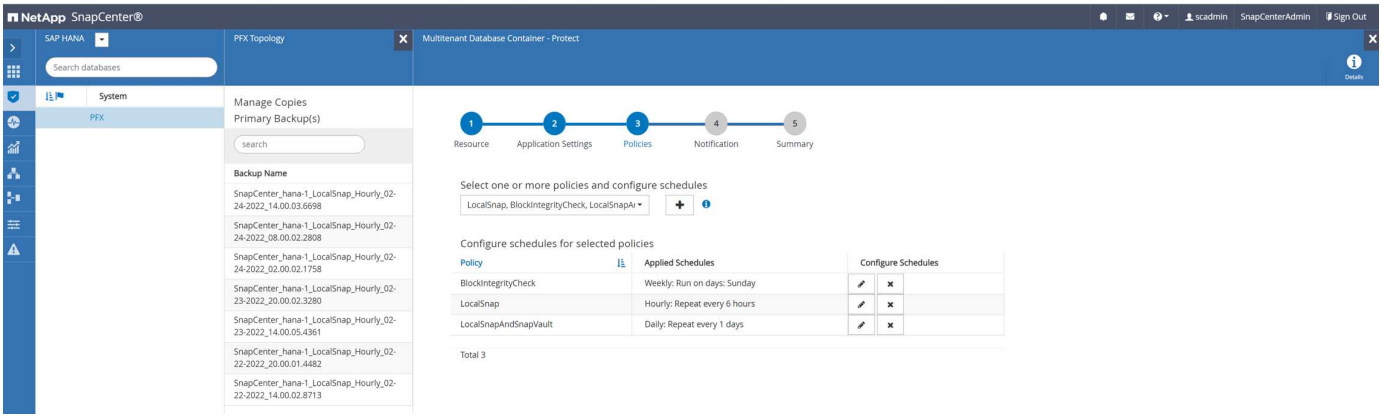


Aggiungere un criterio alla protezione delle risorse

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



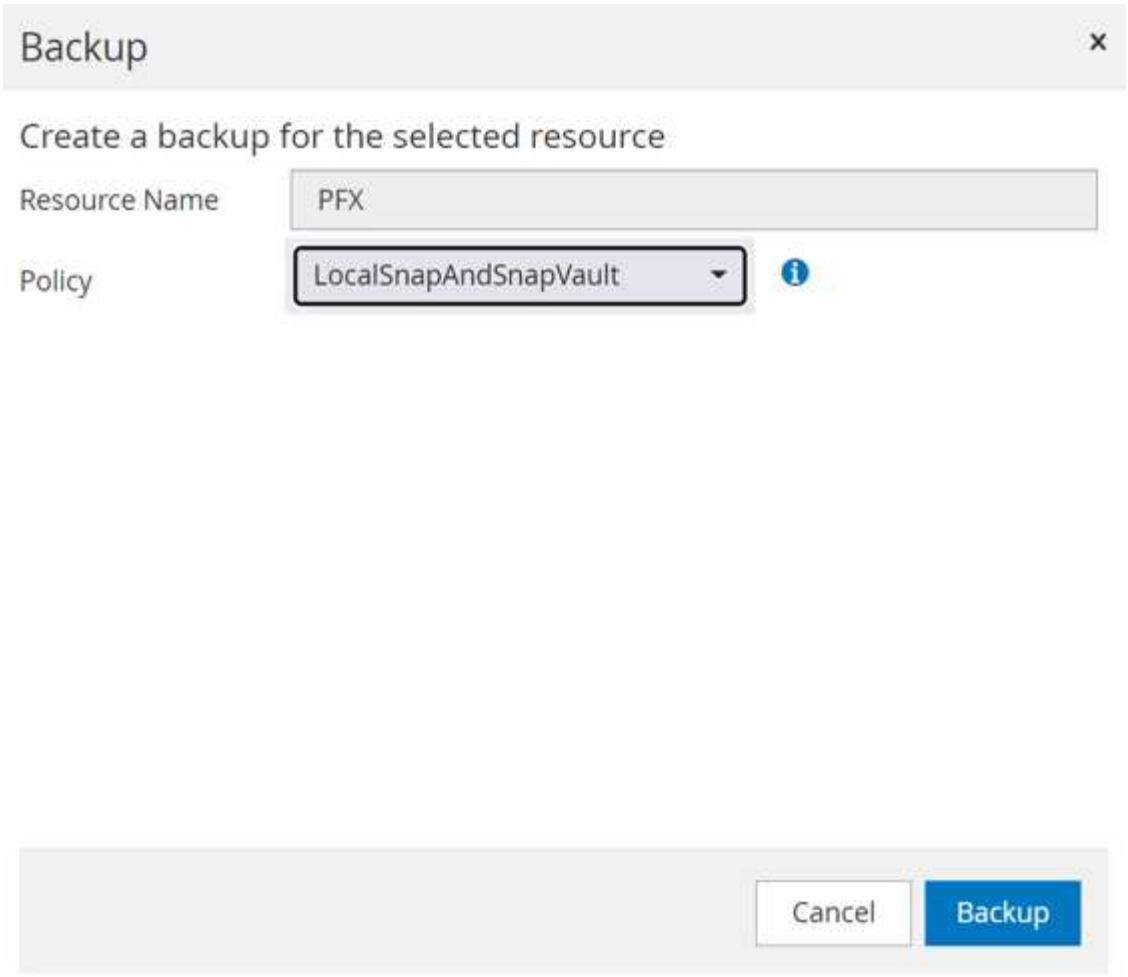
Nella nostra configurazione viene definito un programma giornaliero.



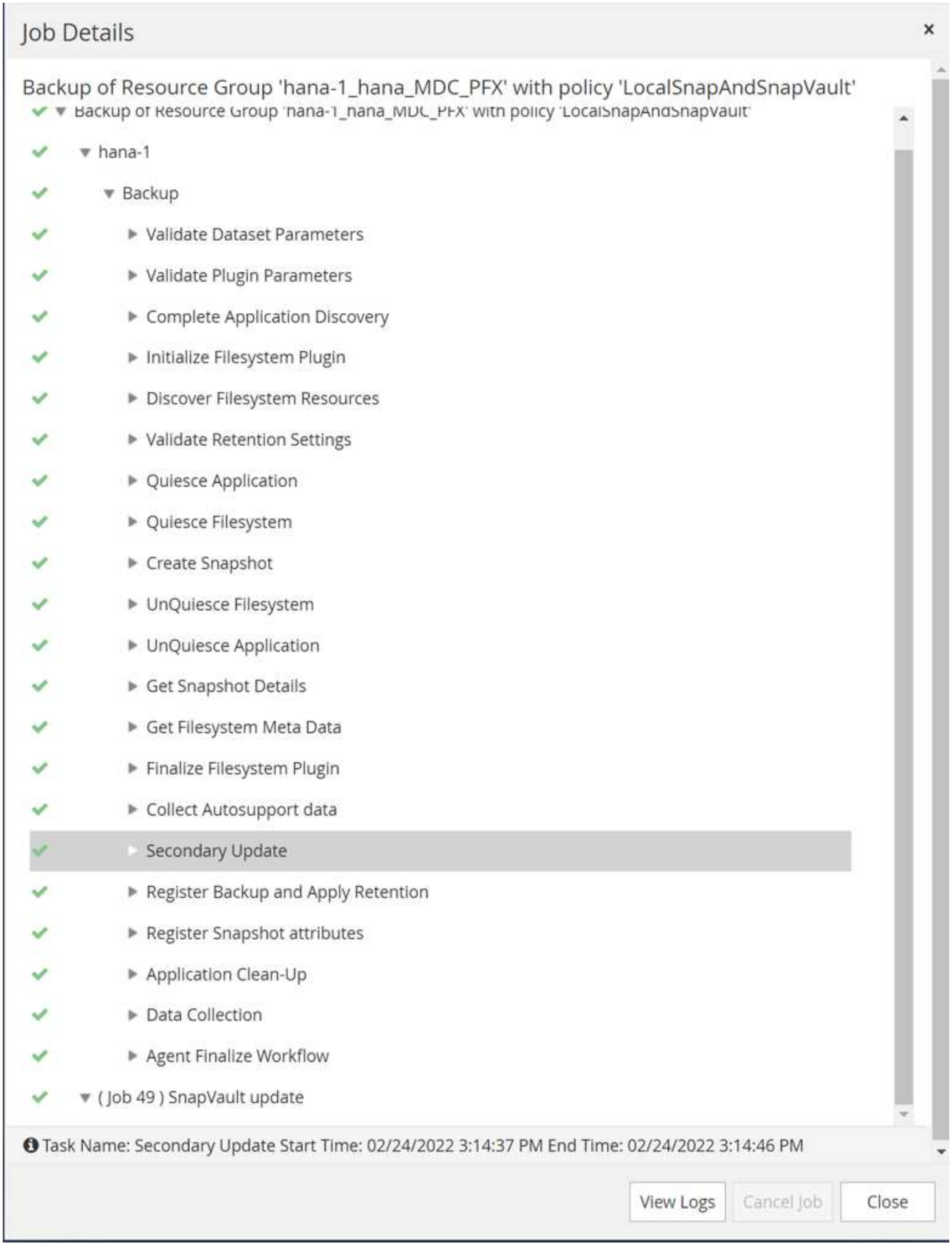
Creare un backup con replica

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

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



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



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

SnapMirror, `snapcenter`, Come configurato nel criterio SnapCenter.

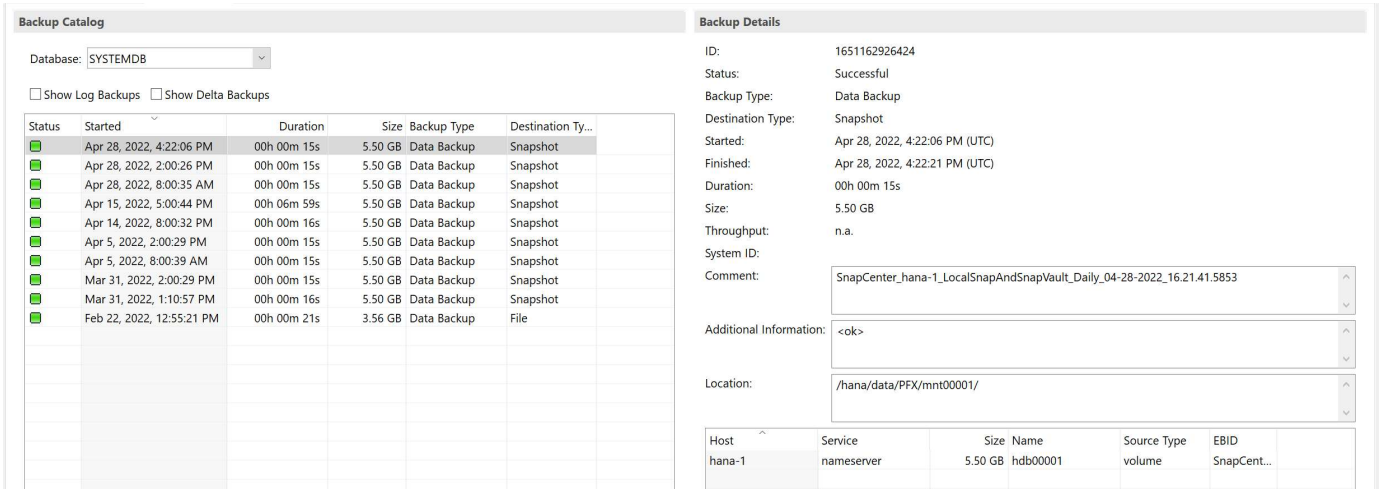
```
FsxId00fa9e3c784b6abbb::> snapshot show -vserver sapcc-hana-svm -volume
PFX_data_mnt00001 -fields snapmirror-label
vserver        volume            snapshot
snapmirror-label
-------------- -----------------
-------------------------------------------------------------
----------------
sapcc-hana-svm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

snapcenter
8 entries were displayed.
```

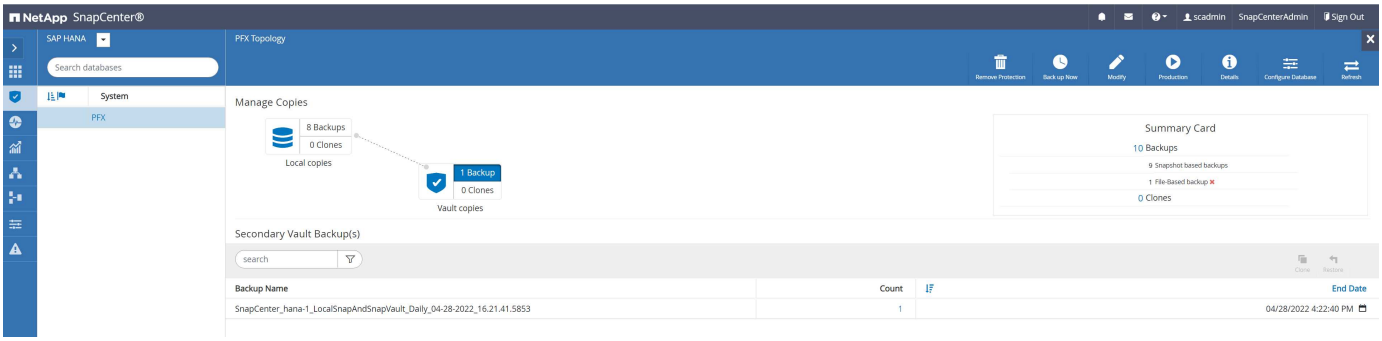
Nel volume di destinazione, viene creata una copia Snapshot con lo stesso nome.

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

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



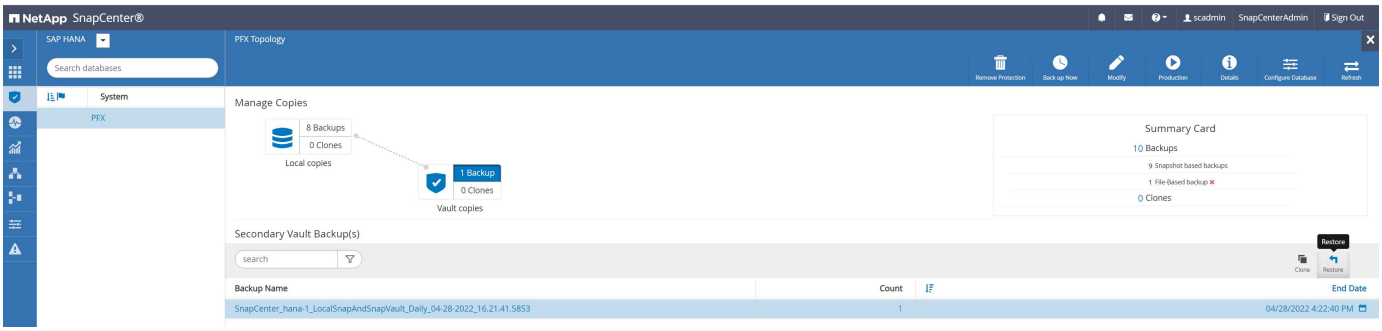
In SnapCenter, è possibile elencare i backup replicati facendo clic su copie del vault nella vista della topologia.



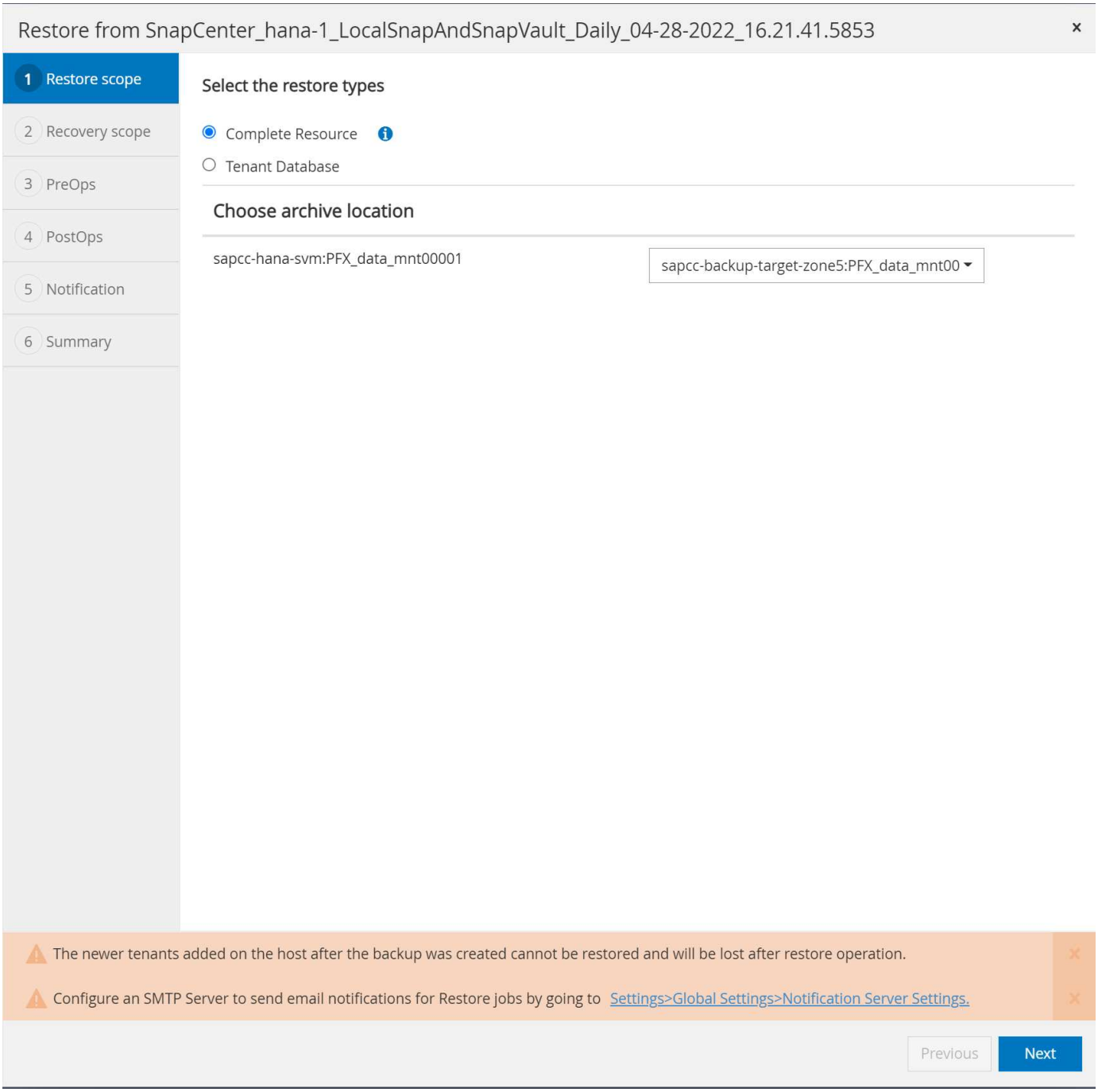
Ripristino e ripristino dallo storage secondario

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

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



La finestra di dialogo di ripristino mostra le posizioni secondarie.



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

Dove trovare ulteriori informazioni

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

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

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

- Pagina delle risorse SnapCenter

"https://www.netapp.com/us/documentation/snapcenter-software.aspx"

- Documentazione del software SnapCenter

  "https://docs.netapp.com/us-en/snapcenter/index.html"

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

  "Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter"

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

  "Backup e ripristino con SnapCenter"

Cronologia delle versioni

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

Backup e recovery SAP HANA con SnapCenter

TR-4614: Backup e recovery SAP HANA con SnapCenter

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.

Autore: Nils Bauer, NetApp

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.

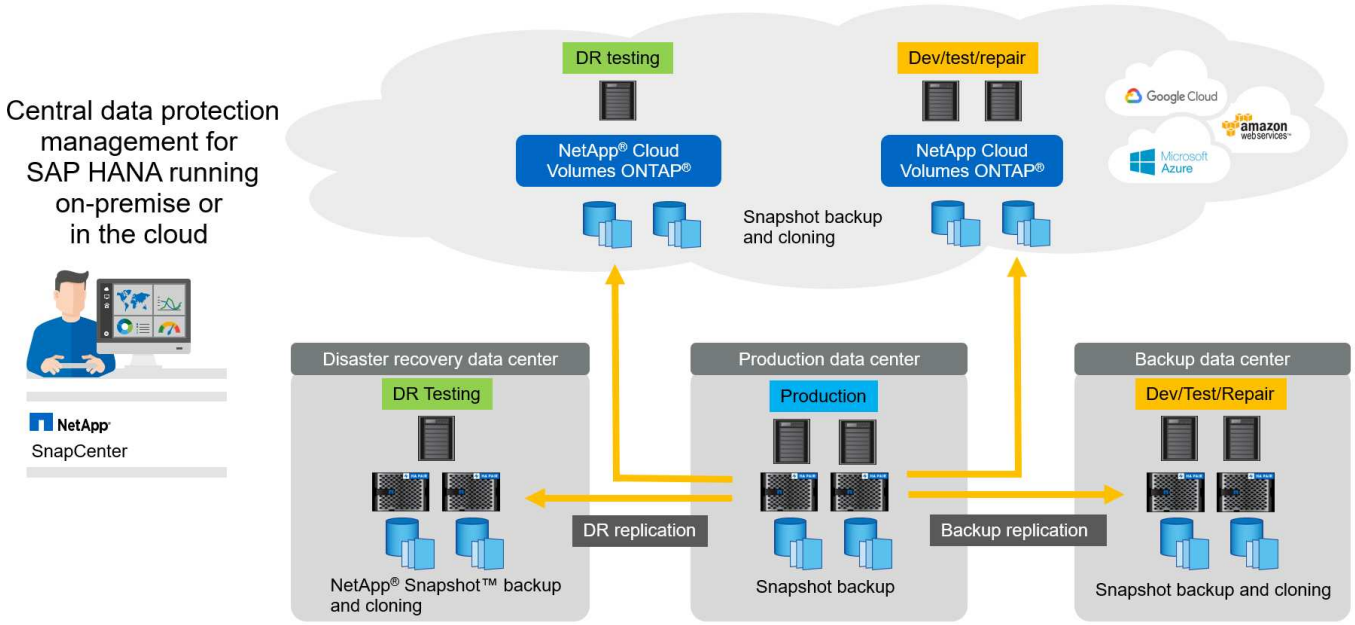
Le copie Snapshot offrono anche vantaggi chiave per le operazioni di ripristino e ripristino. Il software di ripristino dei dati NetApp SnapRestore consente di ripristinare un intero database o, in alternativa, una parte di un database in qualsiasi momento, in base alle copie Snapshot disponibili. Tali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

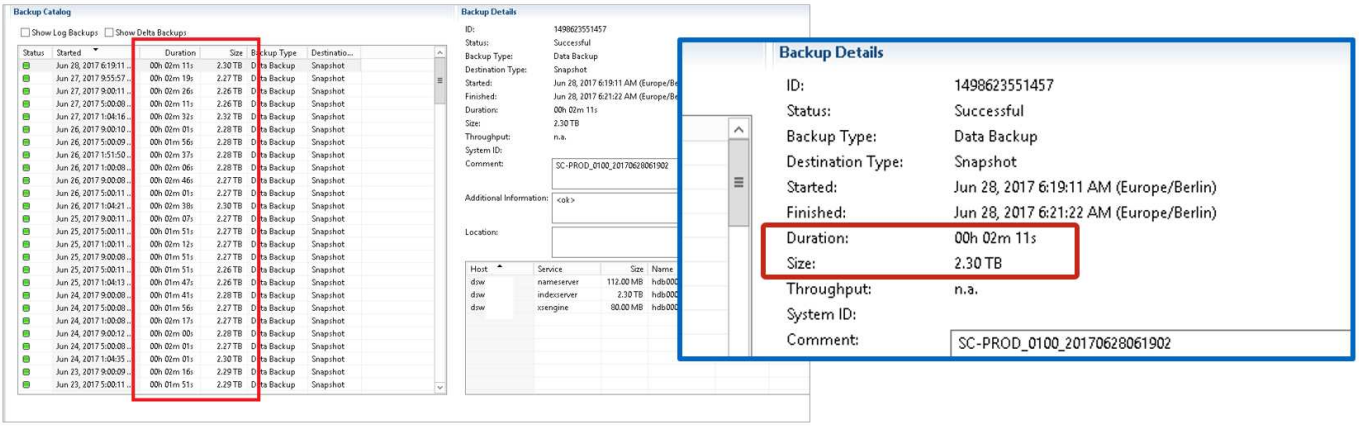
La soluzione può anche essere facilmente estesa a un modello operativo di cloud ibrido. La replica dei dati per il disaster recovery o il backup fuori sede può essere eseguita dai sistemi NetApp ONTAP on-premise alle istanze di Cloud Volumes ONTAP in esecuzione nel cloud. È possibile utilizzare SnapCenter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

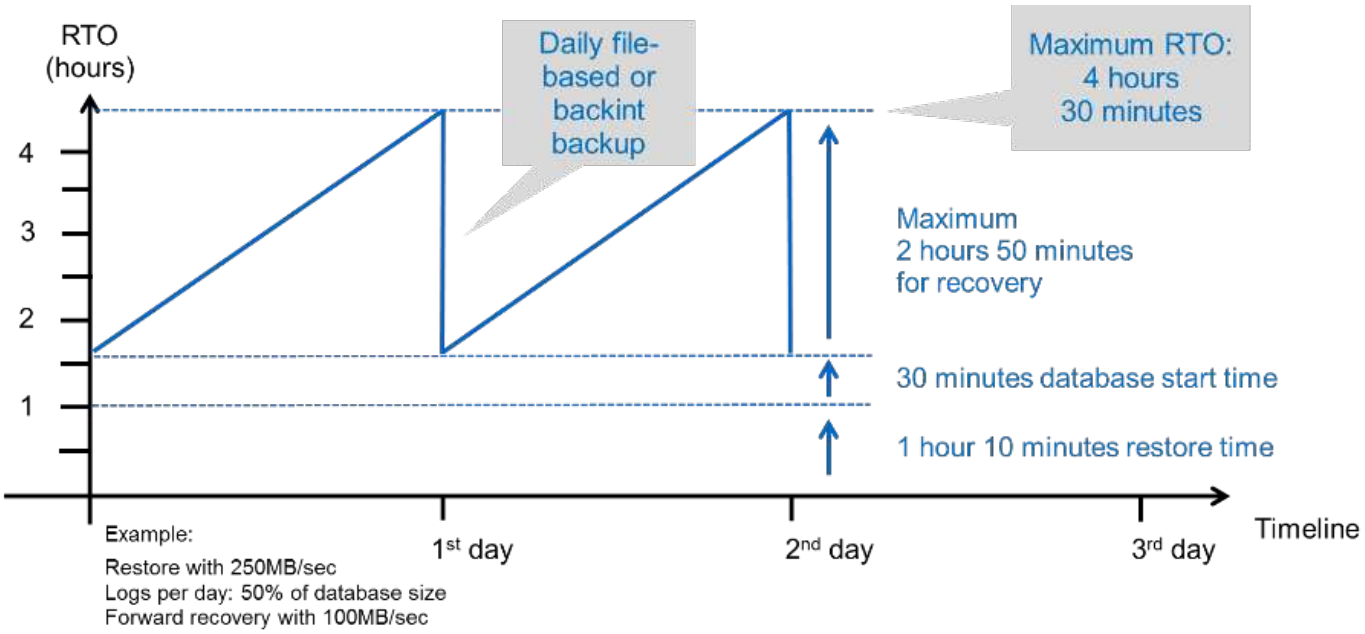
Tempo necessario per il ripristino del database

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.

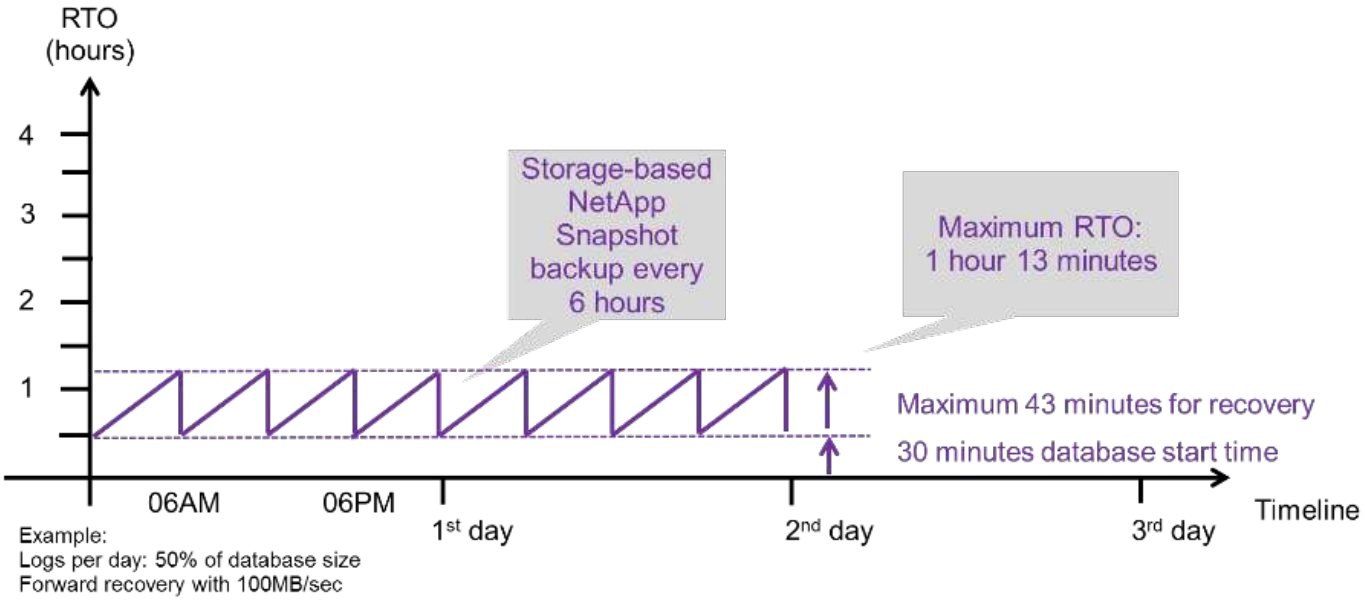
Con i backup dei dati basati su file, la pianificazione del backup è generalmente una volta al giorno. In genere, non è possibile una frequenza di backup più elevata, poiché il backup diminuisce le prestazioni di produzione. Pertanto, nel peggiore dei casi, tutti i log scritti durante la giornata devono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



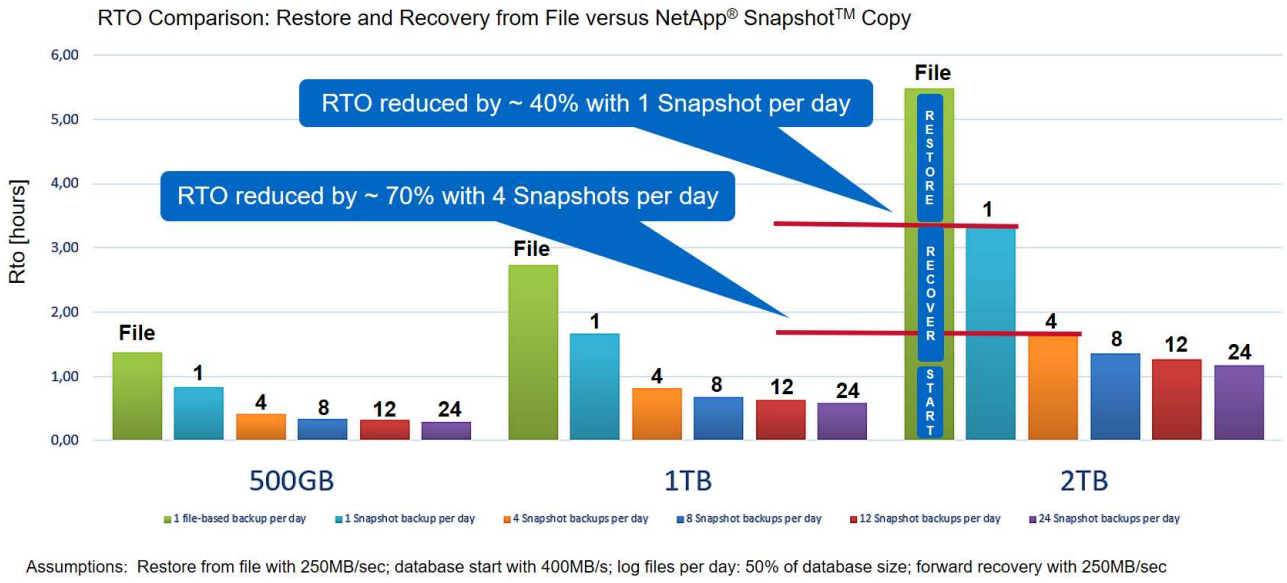
La figura seguente mostra un esempio RTO per un database da 1 TB quando vengono utilizzati backup Snapshot. Con i backup Snapshot basati sullo storage, l'RTO dipende solo dall'ora di avvio del database e dal tempo di ripristino in avanti, in quanto il ripristino viene completato in pochi secondi, indipendentemente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

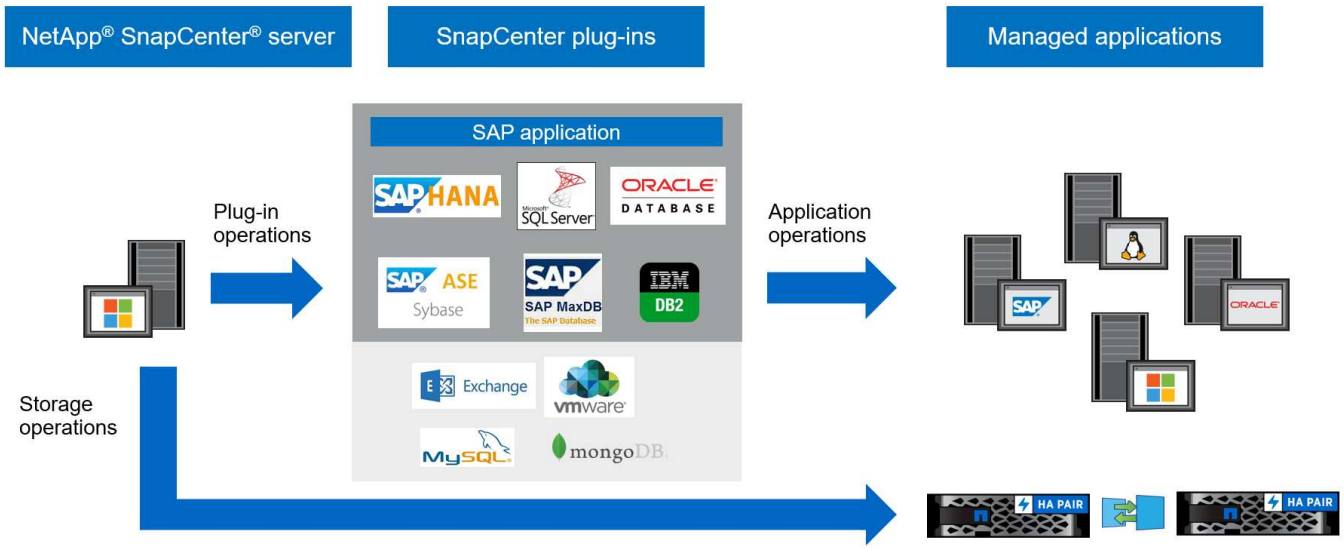
SnapCenter gestisce i dati tra gli endpoint del data fabric basato su NetApp. Puoi utilizzare SnapCenter per replicare i dati tra ambienti on-premise, tra ambienti on-premise e cloud e tra cloud privati, ibridi o pubblici.

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.

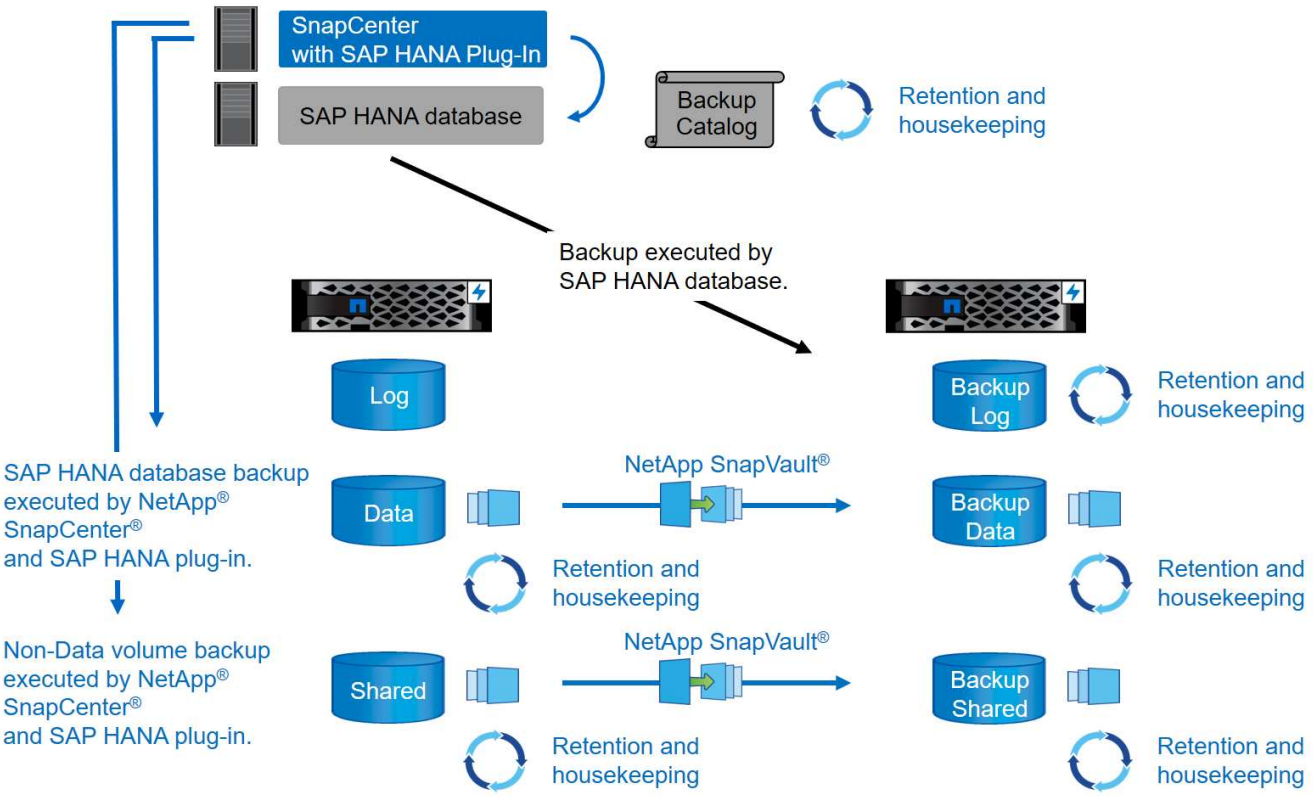
Il database SAP HANA esegue automaticamente i backup dei log. A seconda degli obiettivi del punto di ripristino, sono disponibili diverse opzioni per la posizione di storage dei backup del log:

- 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

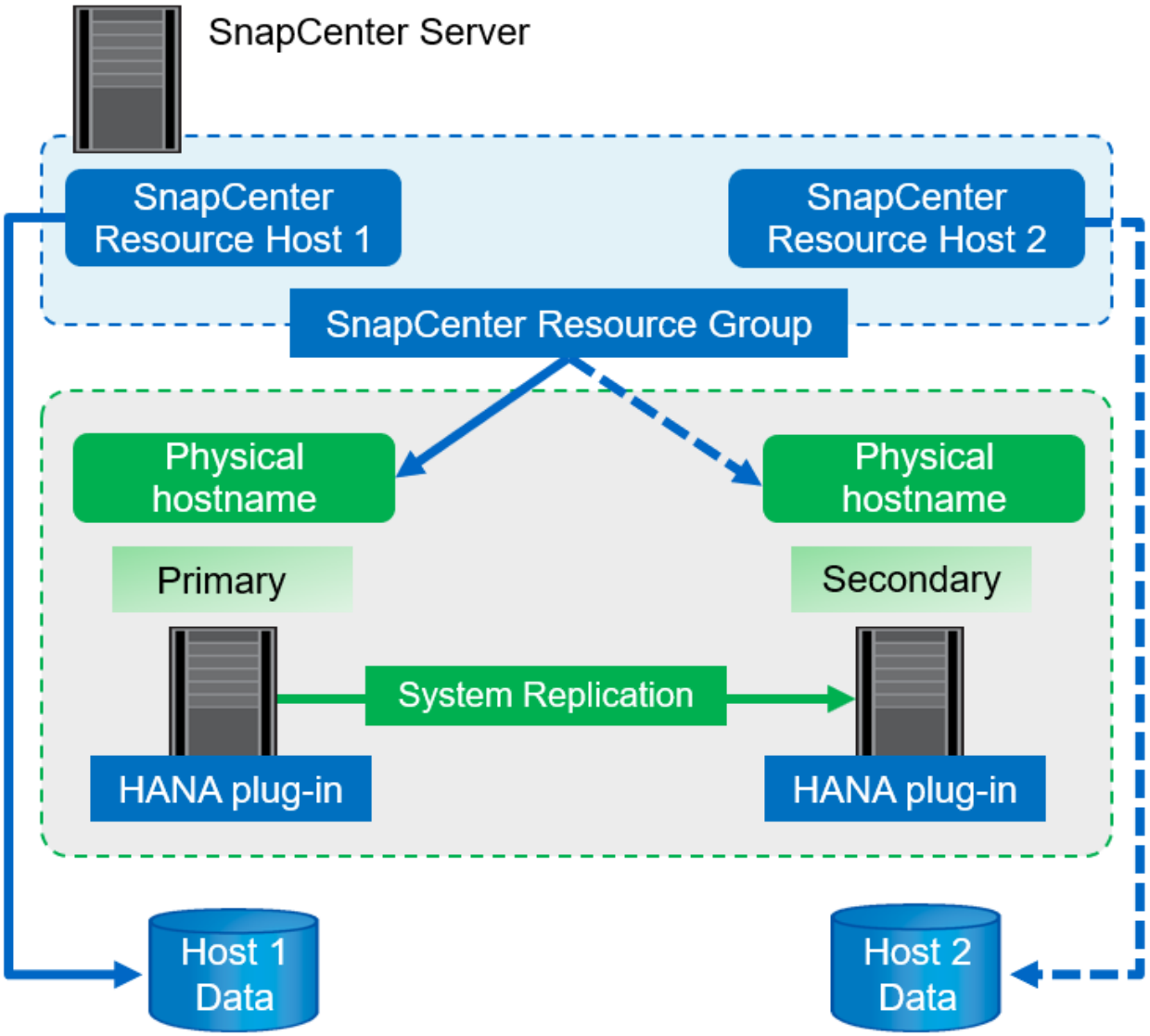
SnapCenter supporta configurazioni SAP HANA a host singolo e multiplo utilizzando sistemi storage NetApp collegati a NFS o FC (AFF e FAS), oltre a sistemi SAP HANA eseguiti su Cloud Volumes ONTAP presso AWS, Azure, la piattaforma cloud di Google e AWS FSX ONTAP utilizzando NFS.

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. Una descrizione dettagliata della configurazione e del funzionamento dei sistemi HANA abilitati per la replica di sistemi HANA in SnapCenter è disponibile in "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.

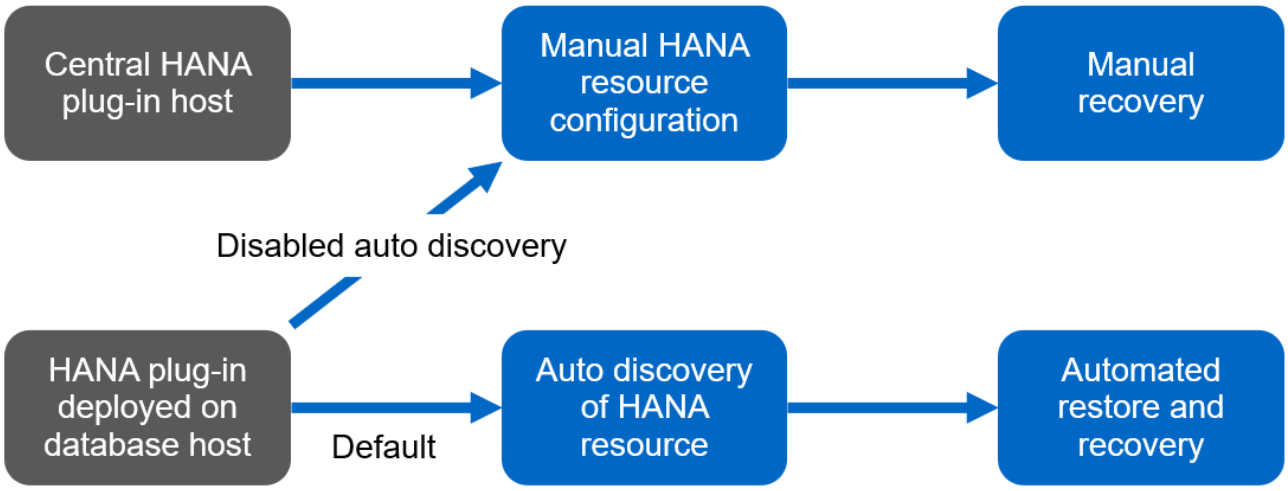
- **Configurazione manuale delle risorse.** le informazioni relative alle risorse HANA e all'impatto dello storage devono essere fornite manualmente.
- **Rilevamento automatico delle risorse HANA.** il rilevamento automatico semplifica la configurazione dei database HANA in SnapCenter e consente il ripristino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

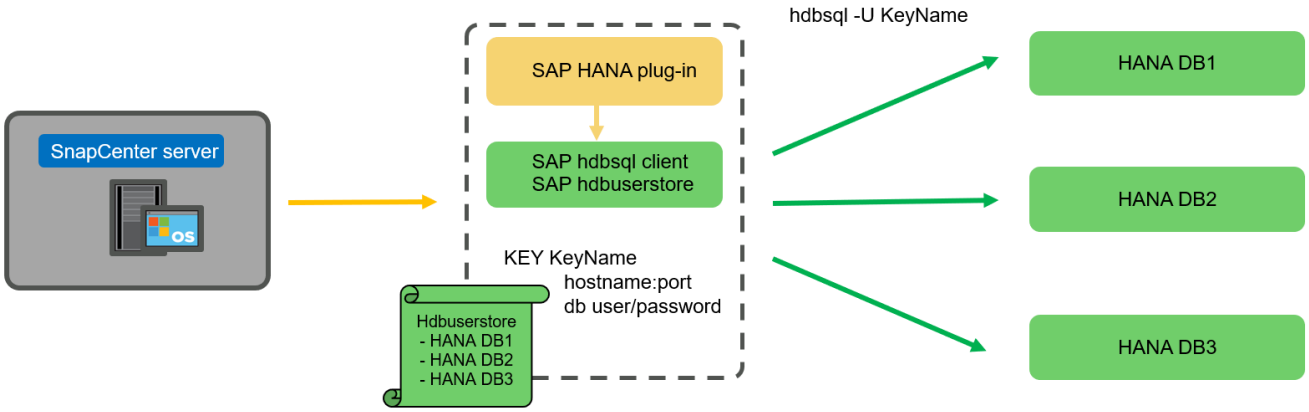
La tabella seguente mostra le configurazioni HANA supportate per la configurazione manuale delle risorse HANA.

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.

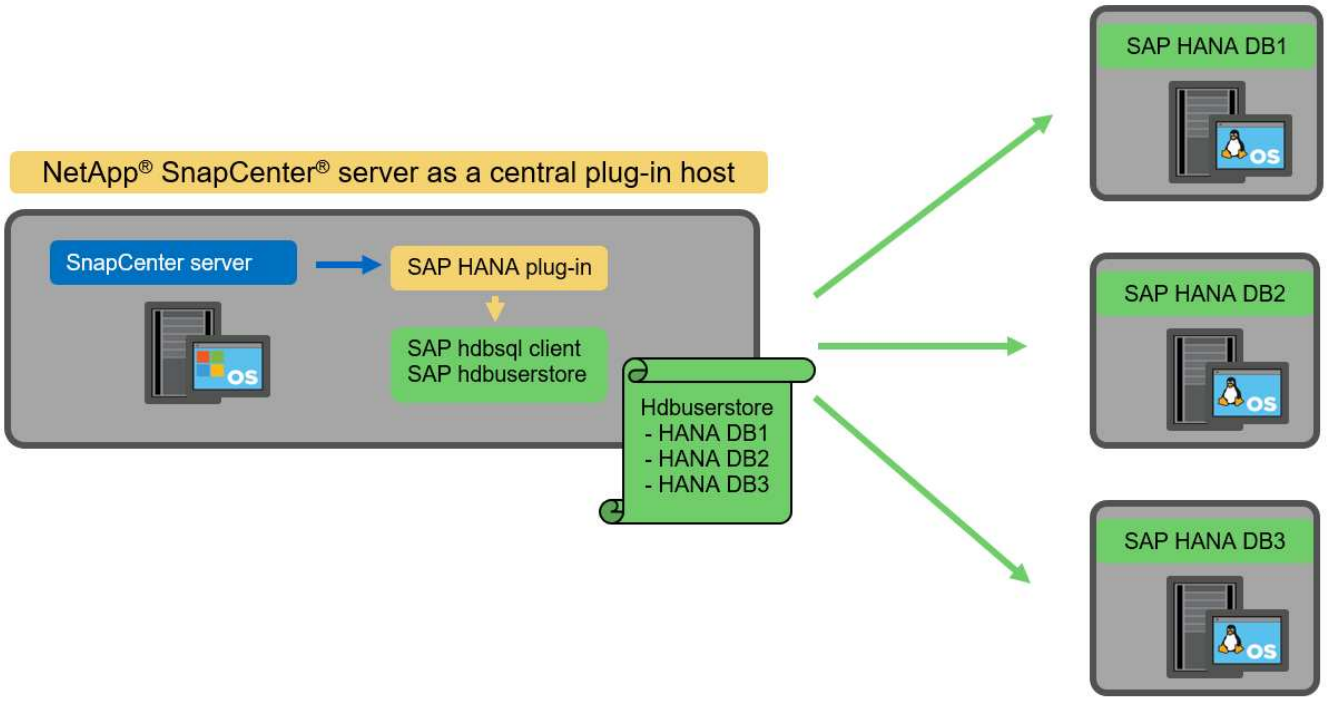
Server SnapCenter ad alta disponibilità

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.

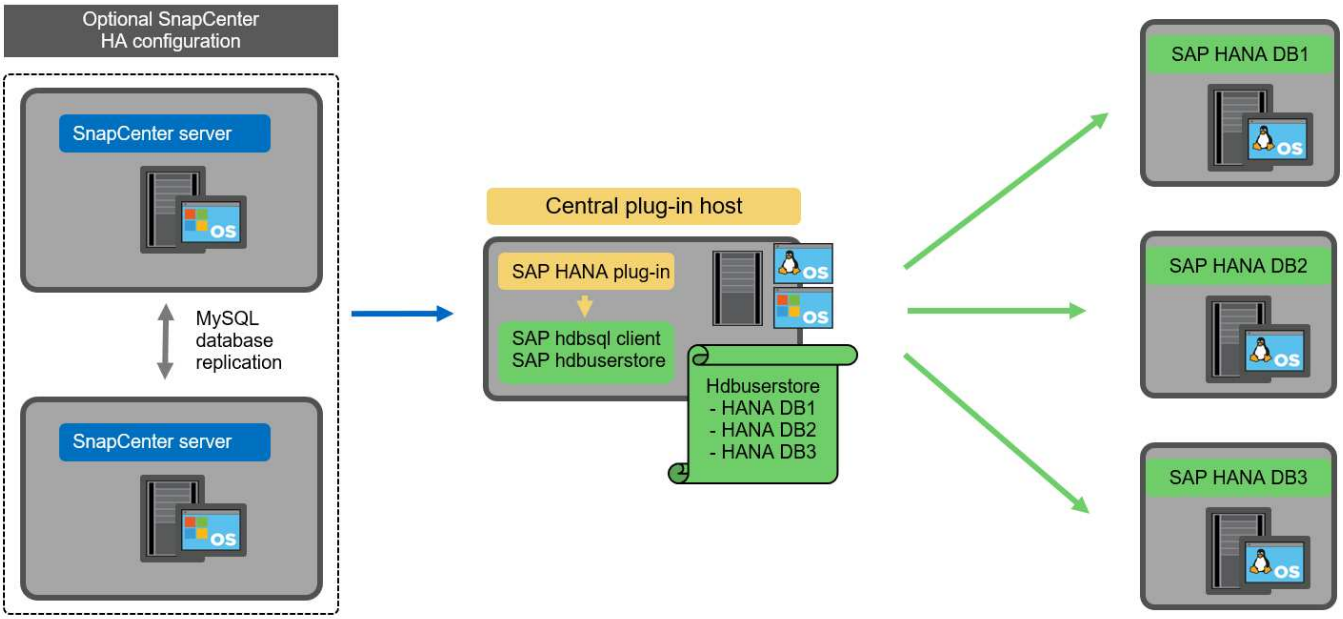
D'altro canto, l'automazione avanzata del workflow per il rilevamento automatico, l'automazione del ripristino e del ripristino, nonché le operazioni di refresh del sistema SAP, richiedono l'installazione dei componenti SnapCenter sull'host del database. Quando si utilizza un host plug-in HANA centrale,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

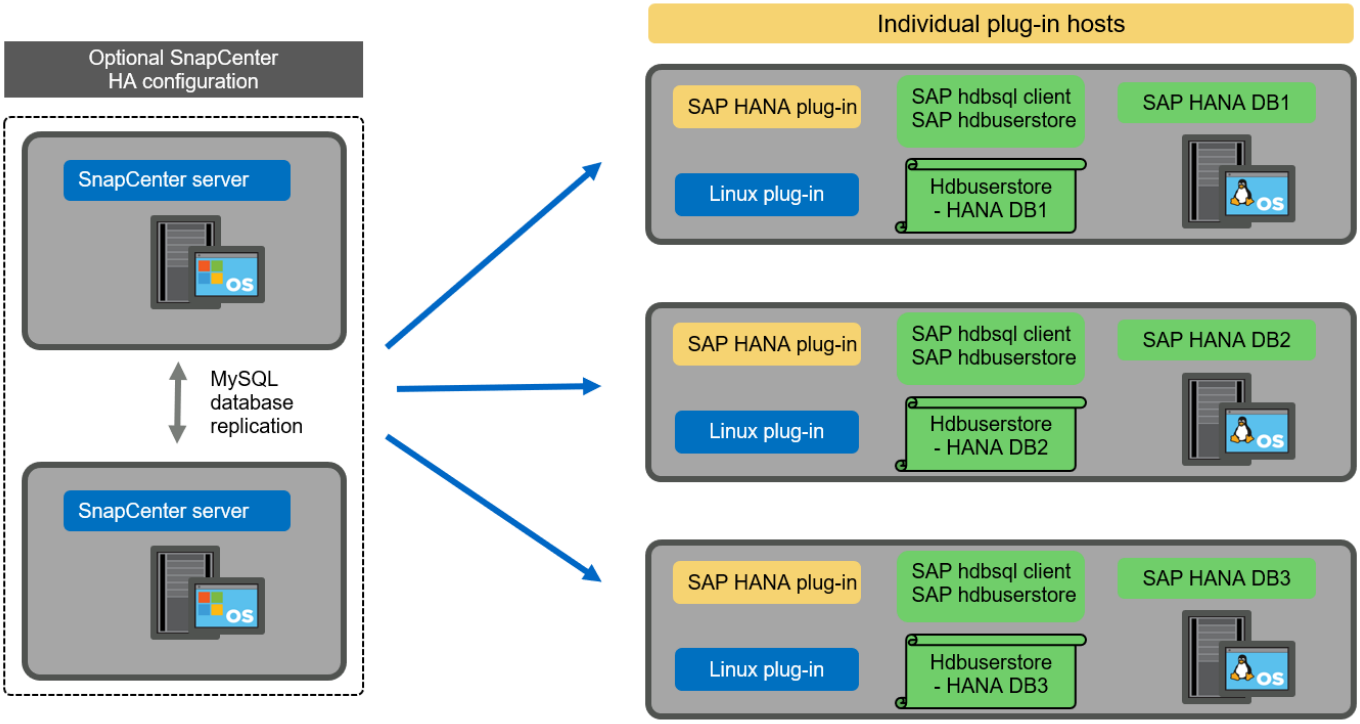


La stessa restrizione relativa alla disponibilità delle funzionalità descritta nella sezione precedente si applica anche a un host plug-in centrale separato.

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.



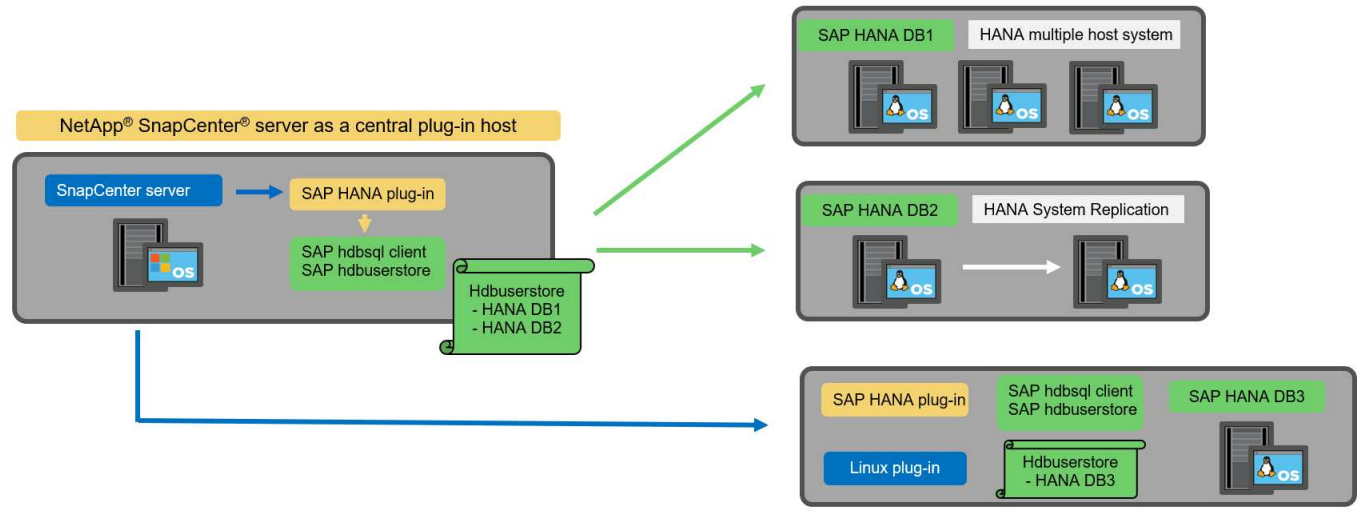
Quando il plug-in HANA viene installato su ogni singolo host di database HANA, sono disponibili tutte le funzionalità, come il rilevamento automatico e il ripristino e ripristino automatici. Inoltre, il server SnapCenter può essere configurato in una configurazione ha.

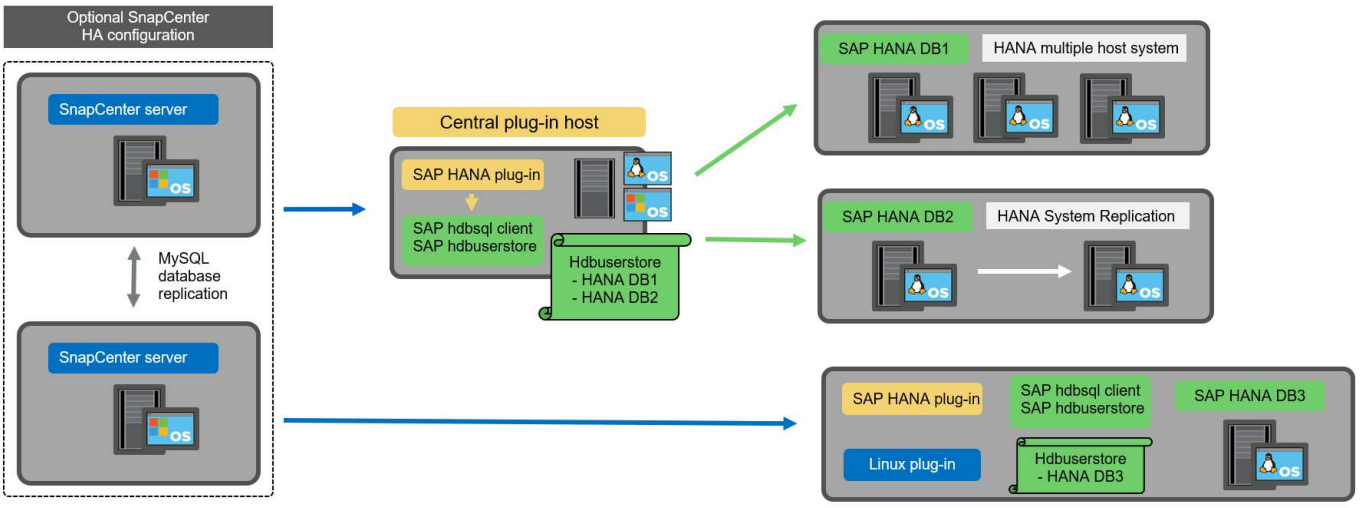
Implementazione di plug-in HANA misti

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.

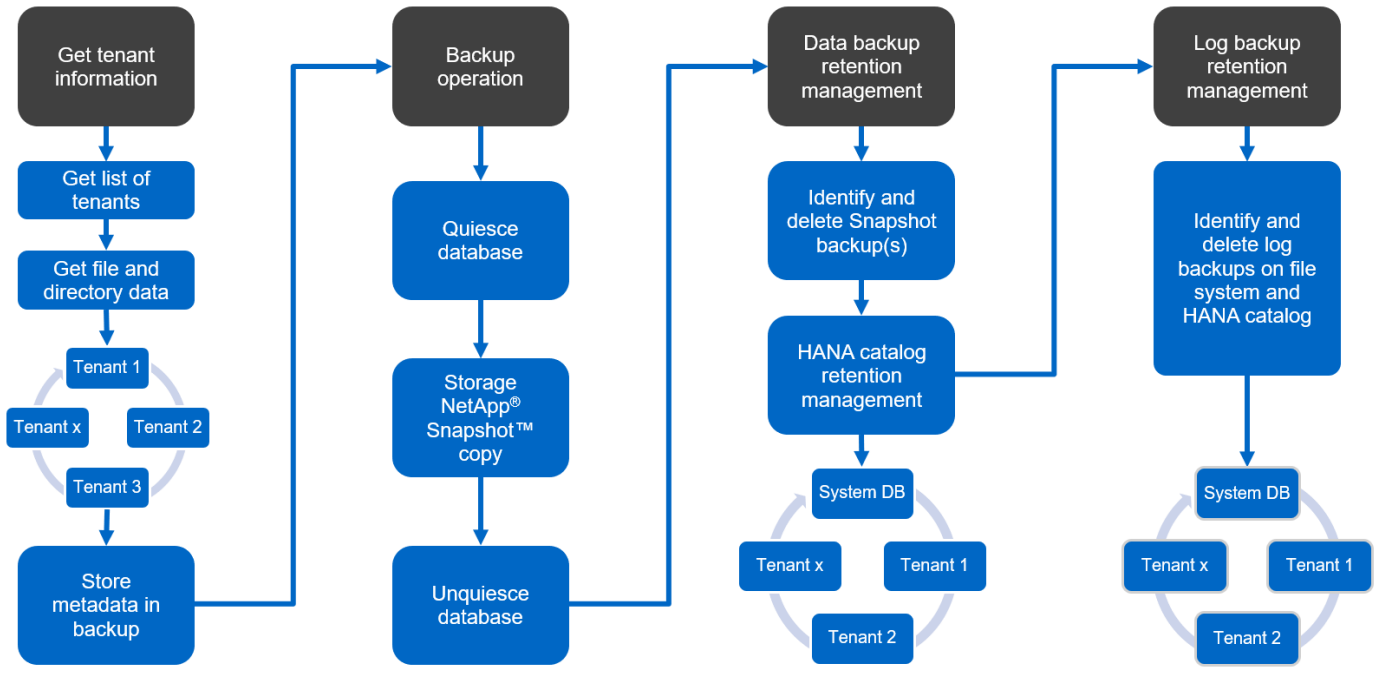
Per abilitare una singola operazione di ripristino del tenant, SnapCenter deve sapere quali tenant sono inclusi in ogni backup Snapshot. Inoltre, deve sapere quali file e directory appartengono a ciascun tenant incluso nel backup Snapshot.

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.

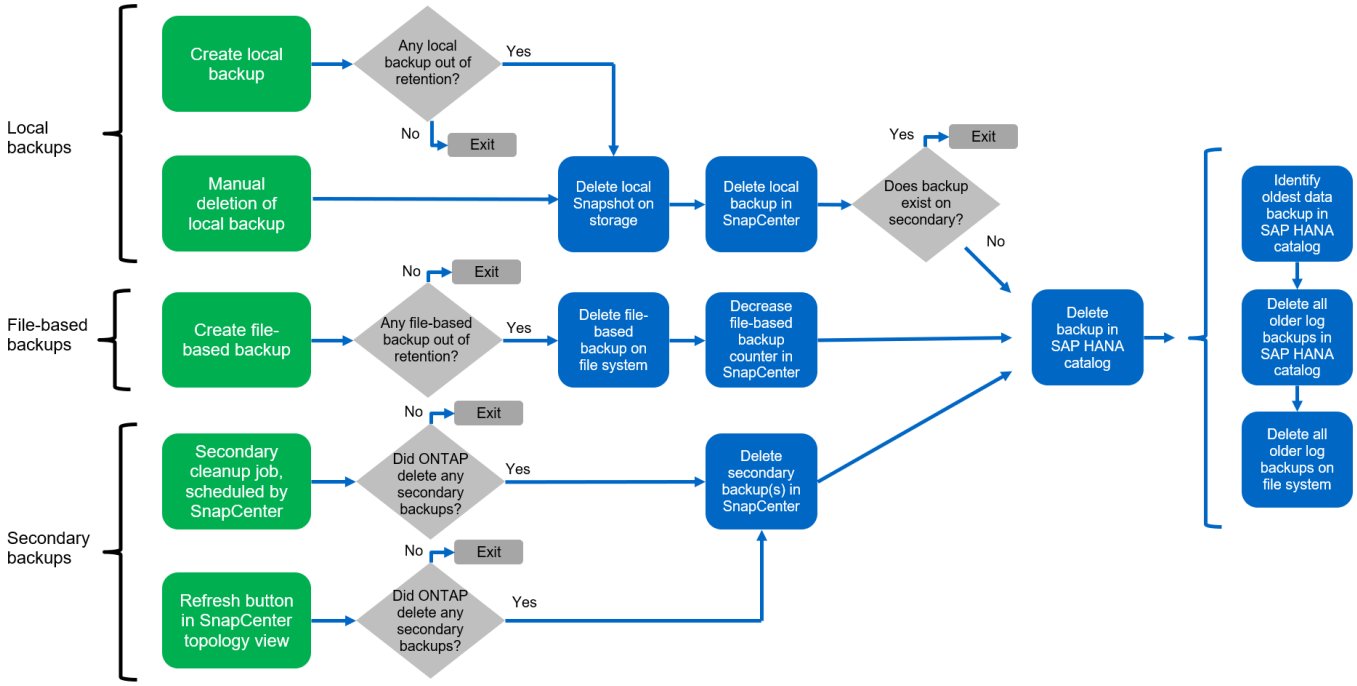
Questo passaggio viene eseguito solo se la gestione del backup dei log non è disattivata.

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 su 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.

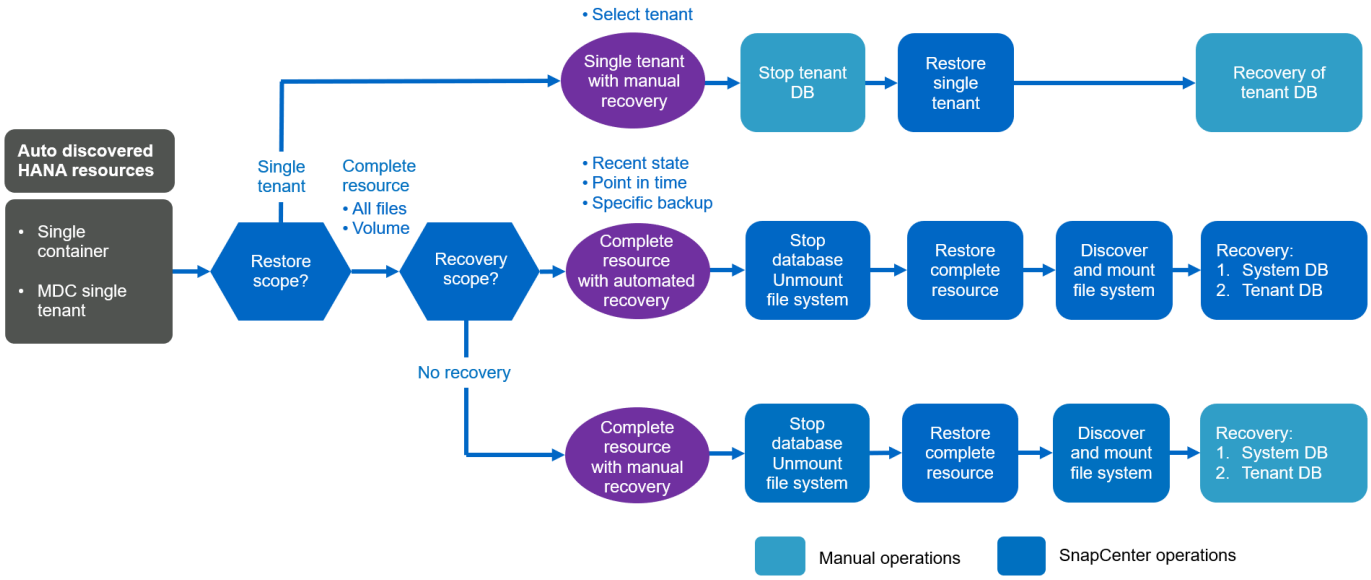
- NFS:
    - Storage primario. Le operazioni SnapRestore basate su file vengono eseguite per tutti i file del database tenant.
    - Storage di backup fuori sede: Le operazioni di ripristino SnapVault vengono eseguite per tutti i file del database tenant.

- 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.

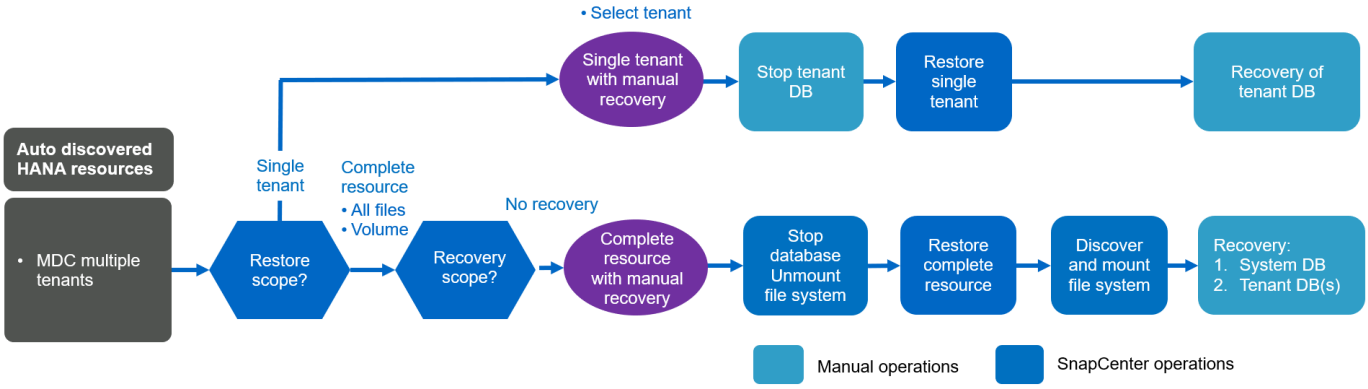


Ripristino e ripristino di più sistemi tenant HANA MDC rilevati automaticamente

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

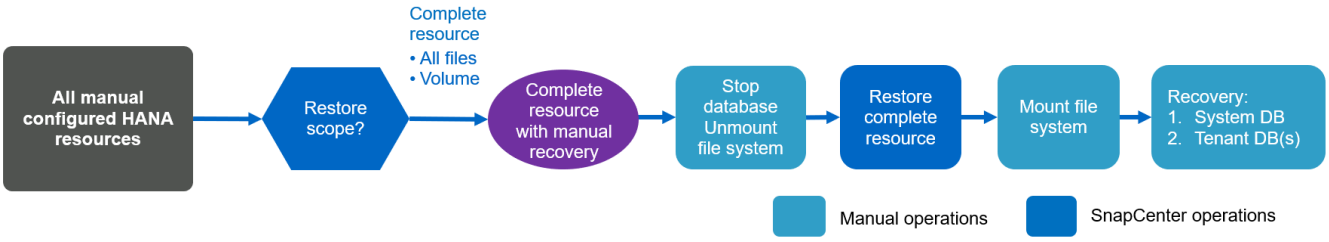
I flussi di lavoro sono gli stessi descritti nella sezione precedente.



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:

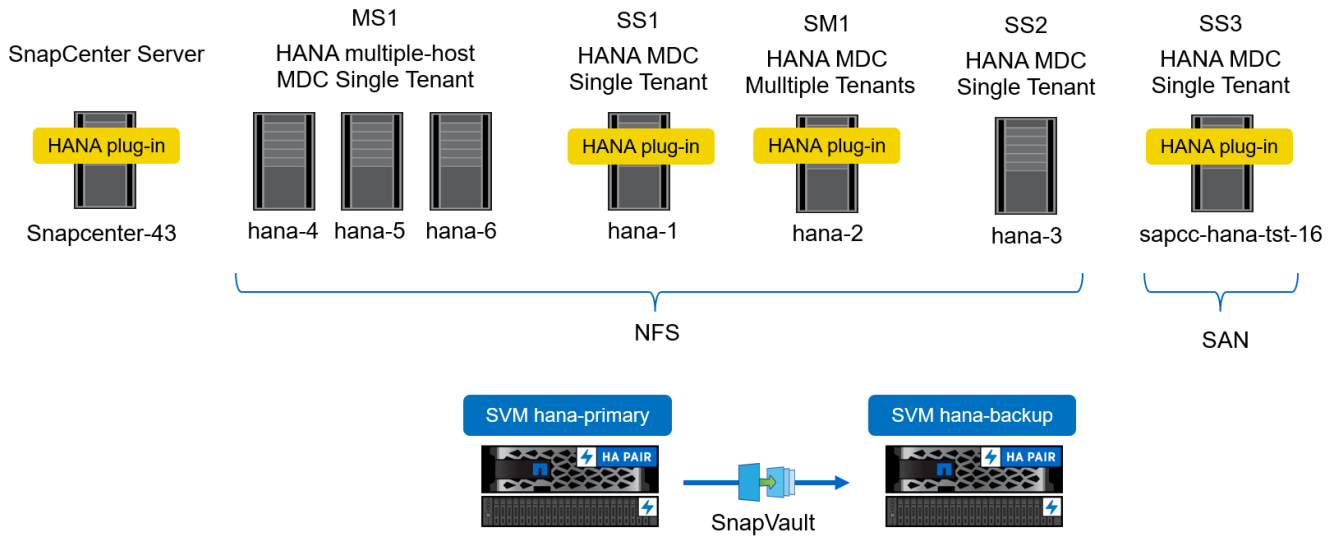
- **MS1.**
  - Sistema multi-host MDC single tenant SAP HANA
  - Gestito con un host plug-in centrale (server SnapCenter)
  - Utilizza NFS come protocollo storage
- **SS1.**
  - Sistema single-tenant SAP HANA MDC a host singolo
  - Rilevato automaticamente con il plug-in HANA installato sull'host del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

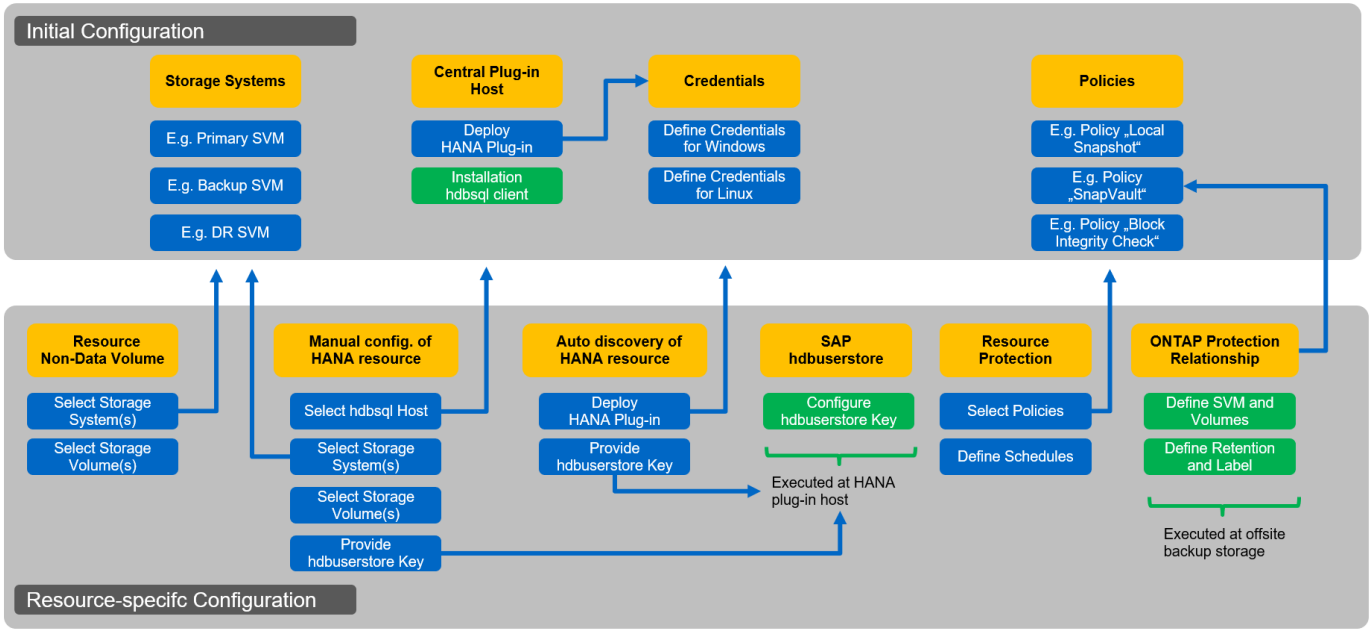


Configurazione di SnapCenter

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

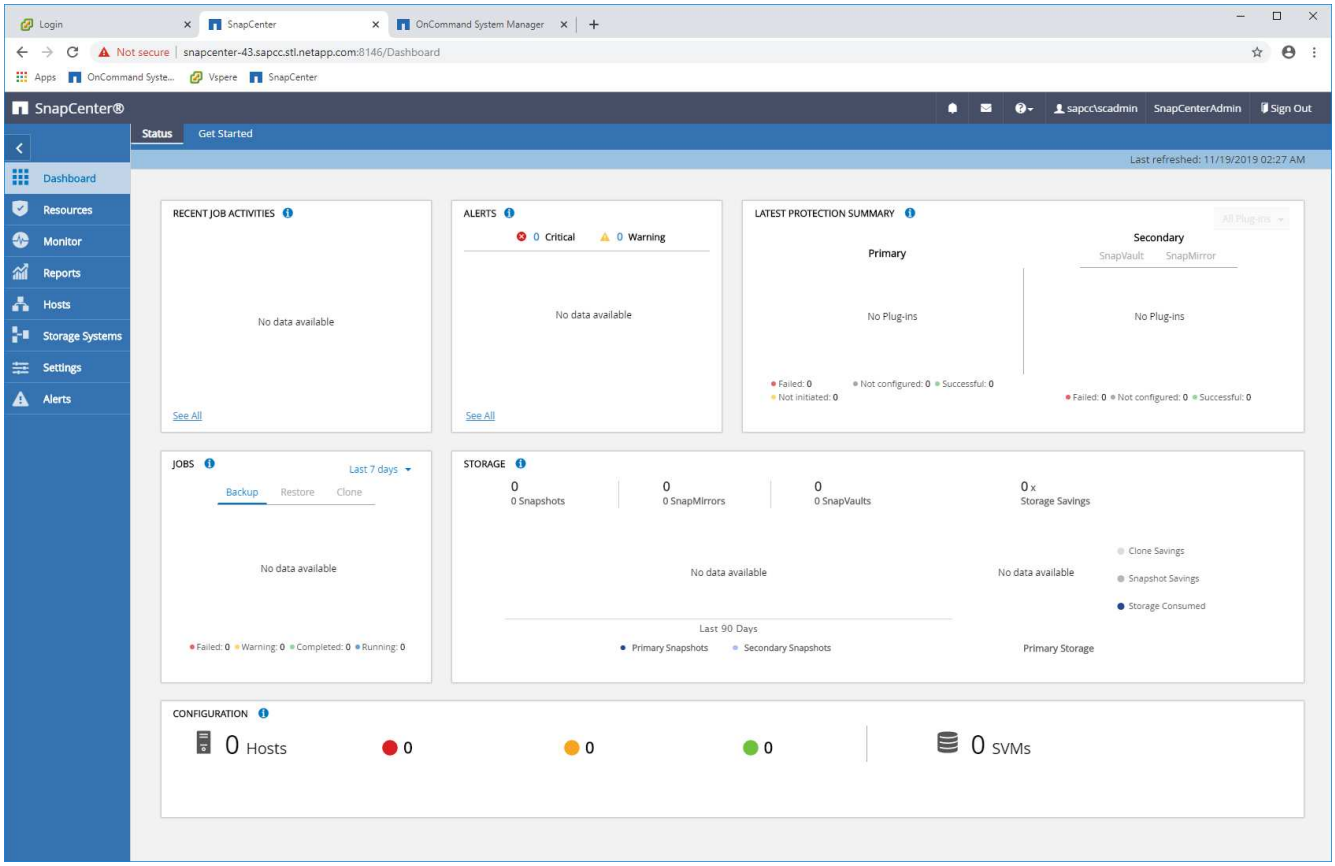
La configurazione iniziale include i seguenti passaggi:

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.

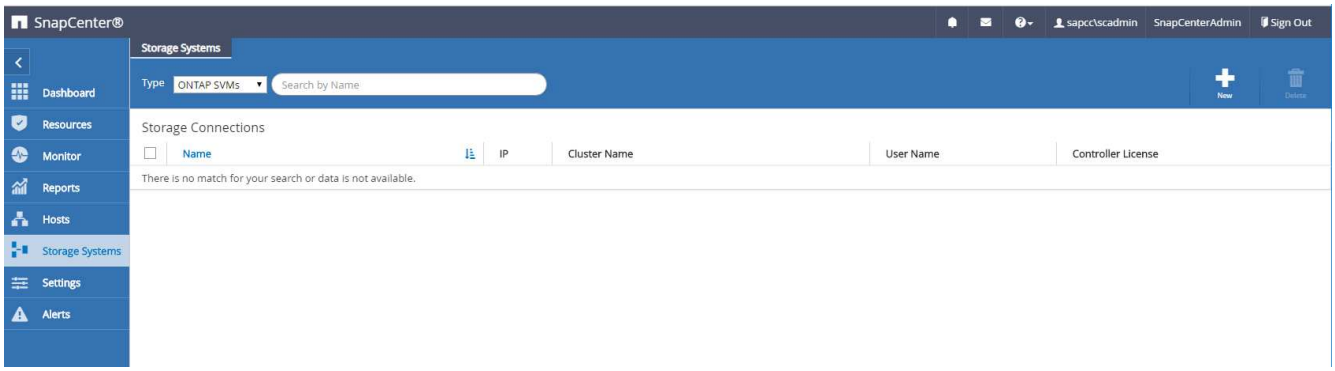
Configurazione del sistema storage

1. Accedere alla GUI del server SnapCenter.



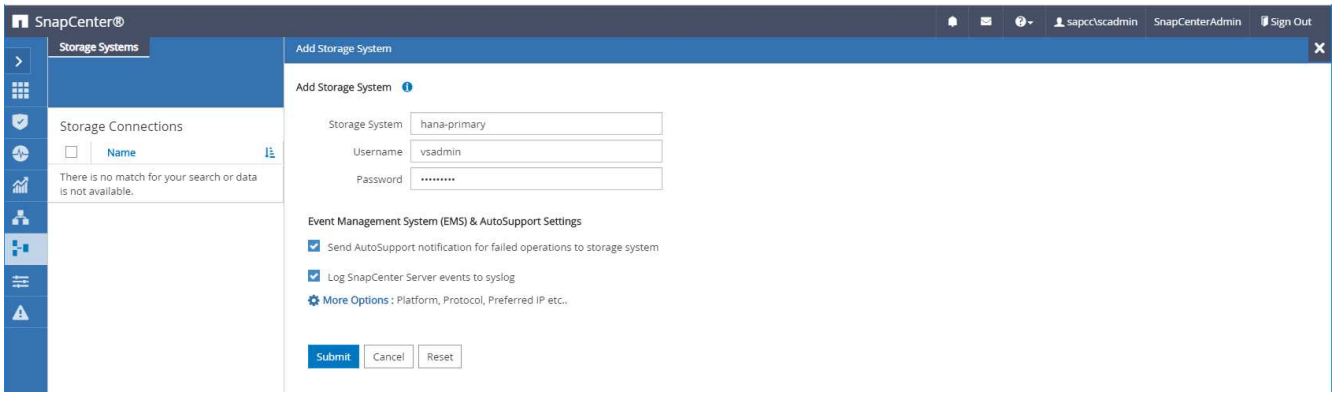
2. Selezionare Storage Systems (sistemi storage).

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.

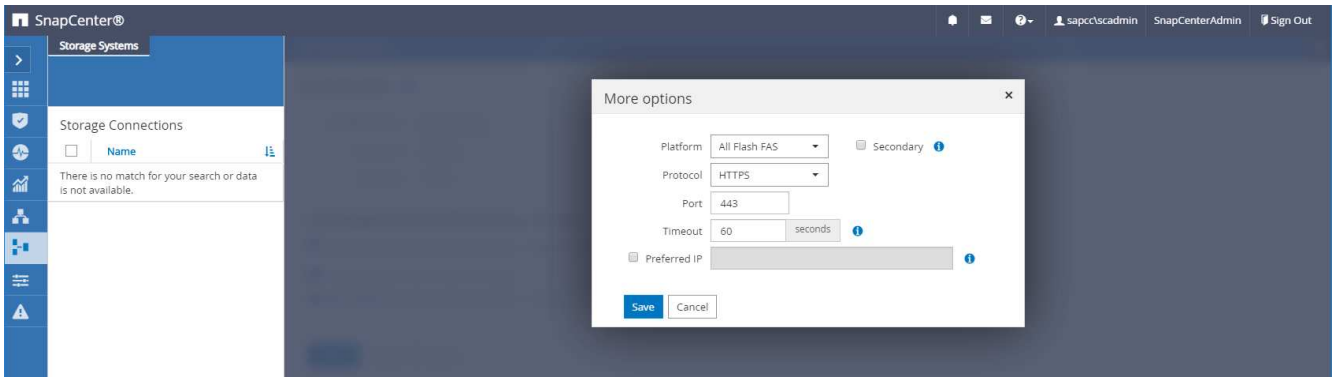
L'utente SVM non deve essere l'utente vsadmin, come mostrato nella schermata. In genere, un utente viene configurato sulla SVM e assegnato i permessi necessari per eseguire le operazioni di backup e ripristino. I dettagli sui privilegi richiesti sono disponibili nella "Guida all'installazione di SnapCenter"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



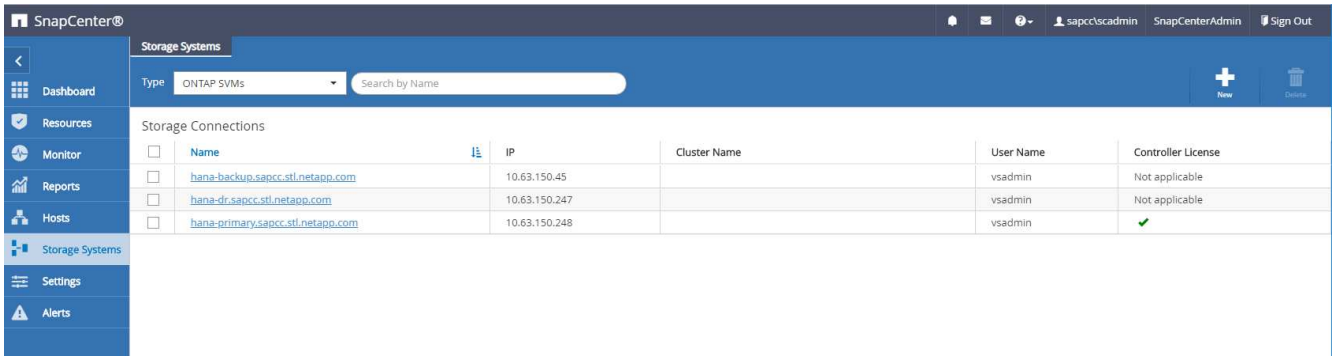
4. Fare clic su More Options (altre opzioni) per configurare la piattaforma di storage.

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.

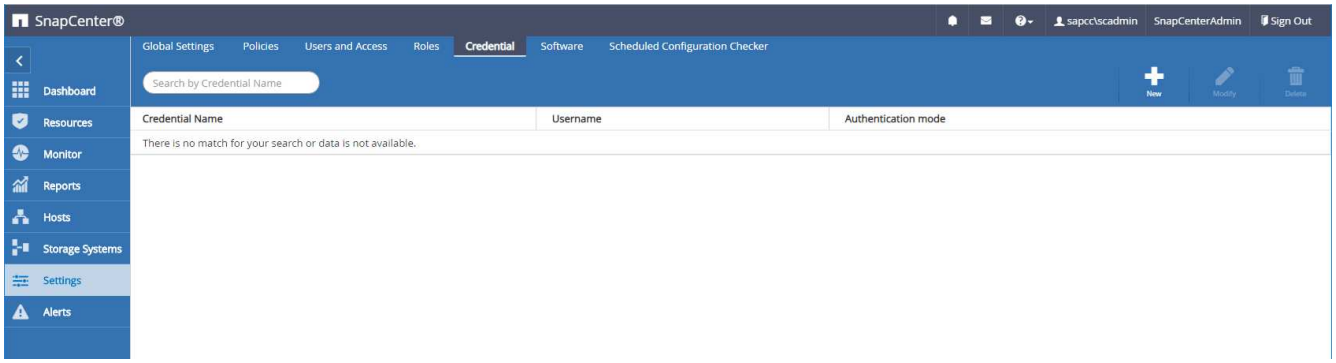


5. Aggiungere altri sistemi storage secondo necessità. Nel nostro esempio, sono stati aggiunti uno storage aggiuntivo per il backup fuori sede e uno per il disaster recovery.

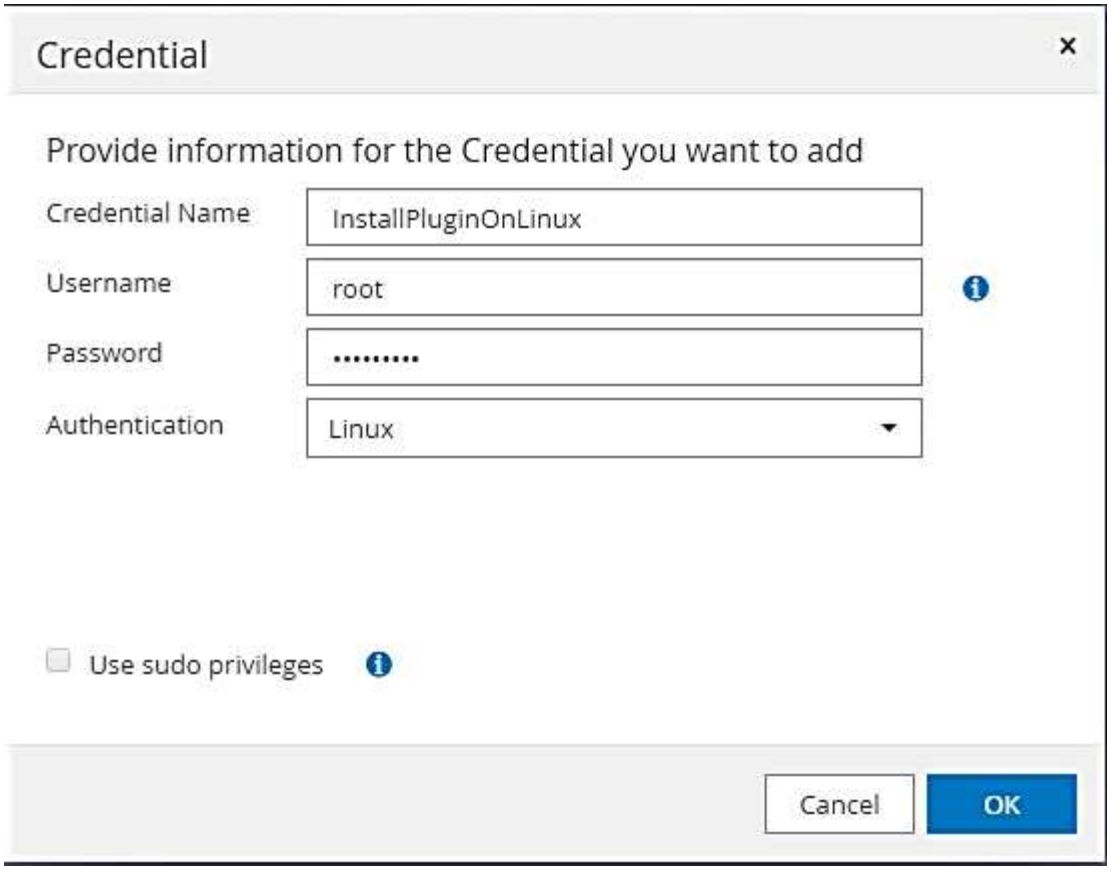


Configurazione delle credenziali

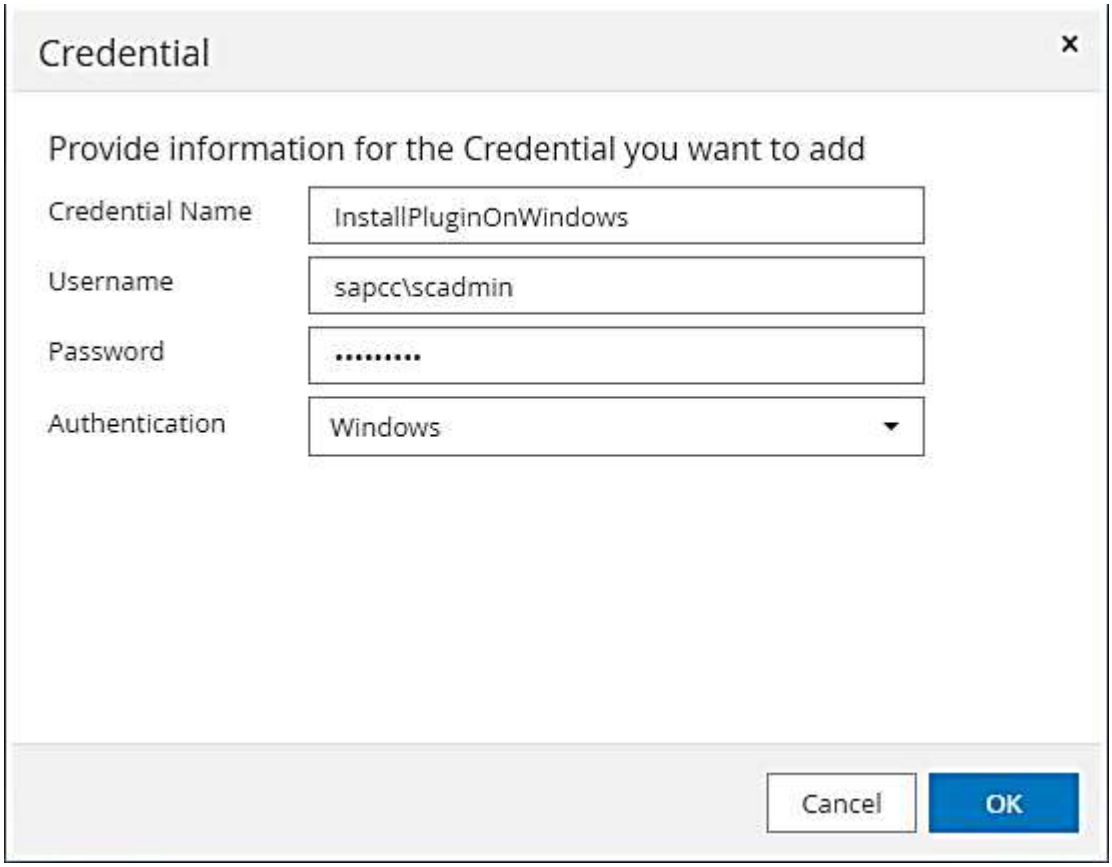
1. Accedere a Impostazioni, selezionare credenziali e fare clic su nuovo.



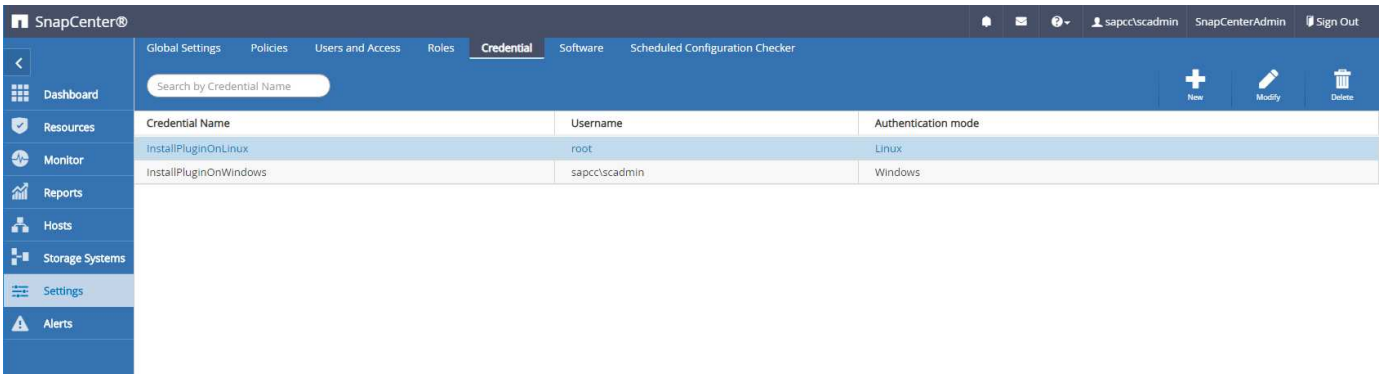
2. Fornire le credenziali per l'utente utilizzato per le installazioni plug-in sui sistemi Linux.



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.

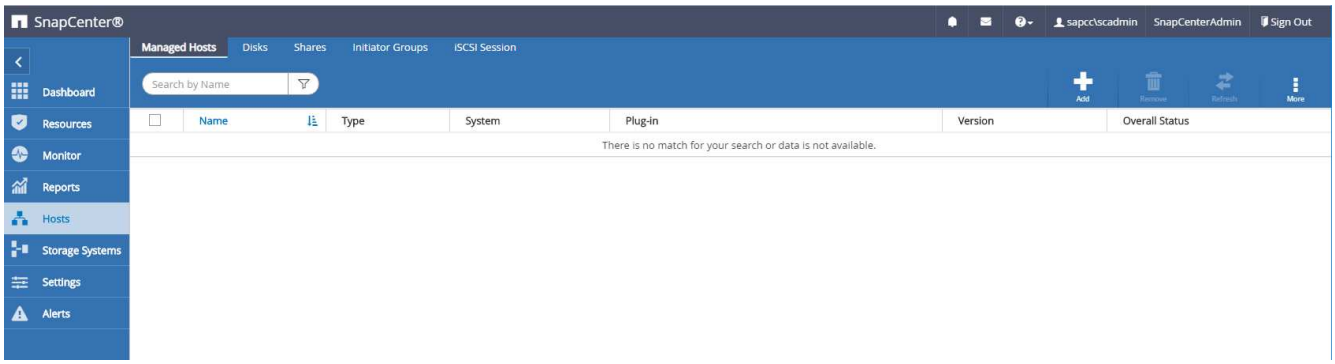


Installazione del plug-in SAP HANA su un host plug-in centrale

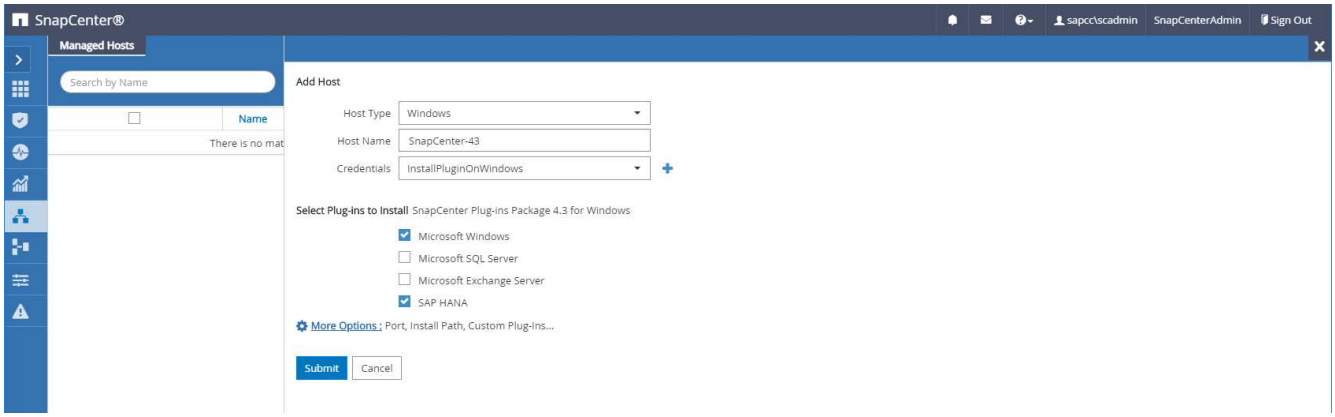
Nella configurazione di laboratorio, il server SnapCenter viene utilizzato anche come host plug-in HANA centrale. L'host Windows su cui viene eseguito il server SnapCenter viene aggiunto come host e il plug-in SAP HANA viene installato sull'host Windows.

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.

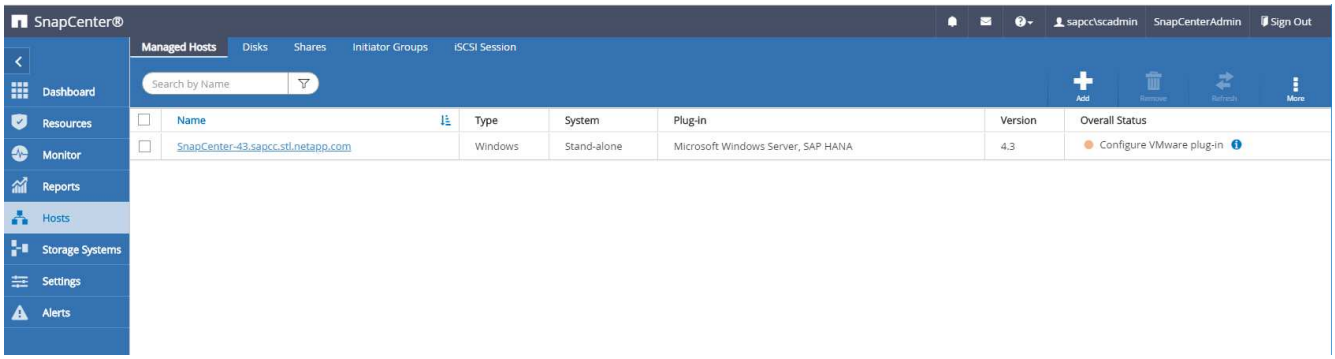
1. Accedere a hosts e fare clic su Add (Aggiungi).



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 di solito configurate indipendentemente dalla risorsa e possono essere utilizzate da più database SAP HANA.

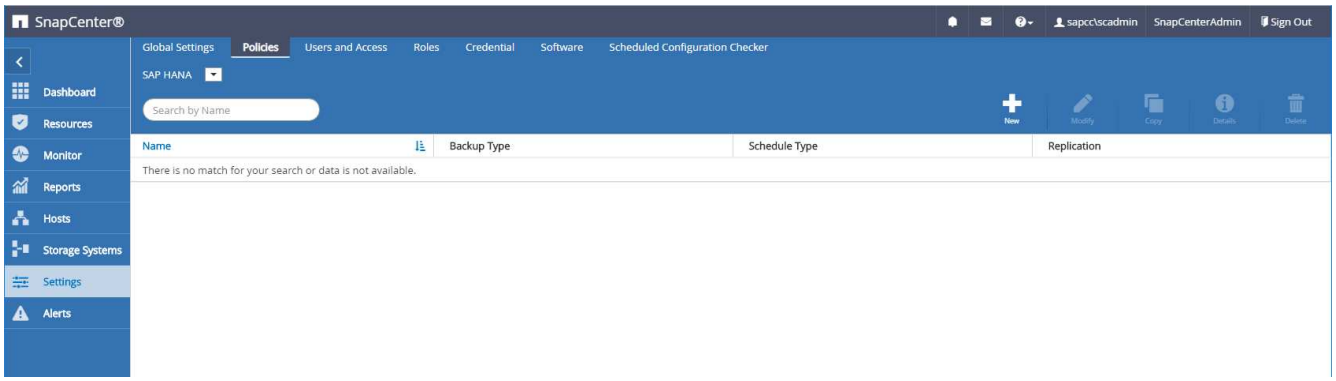
Una configurazione minima tipica è costituita dai seguenti criteri:

- 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`

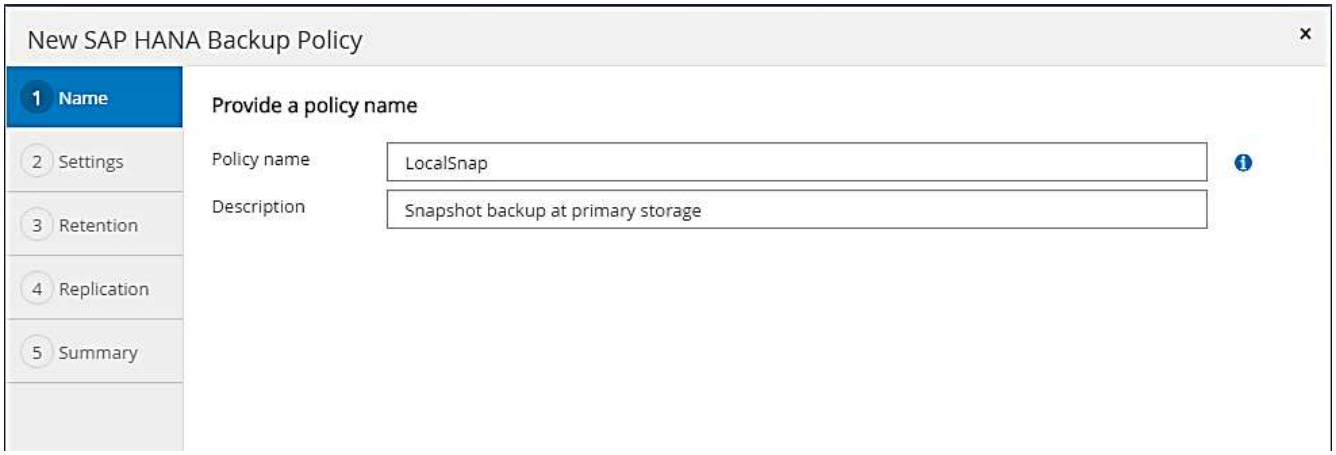
Le sezioni seguenti descrivono la configurazione di questi tre criteri.

Policy per backup Snapshot orari

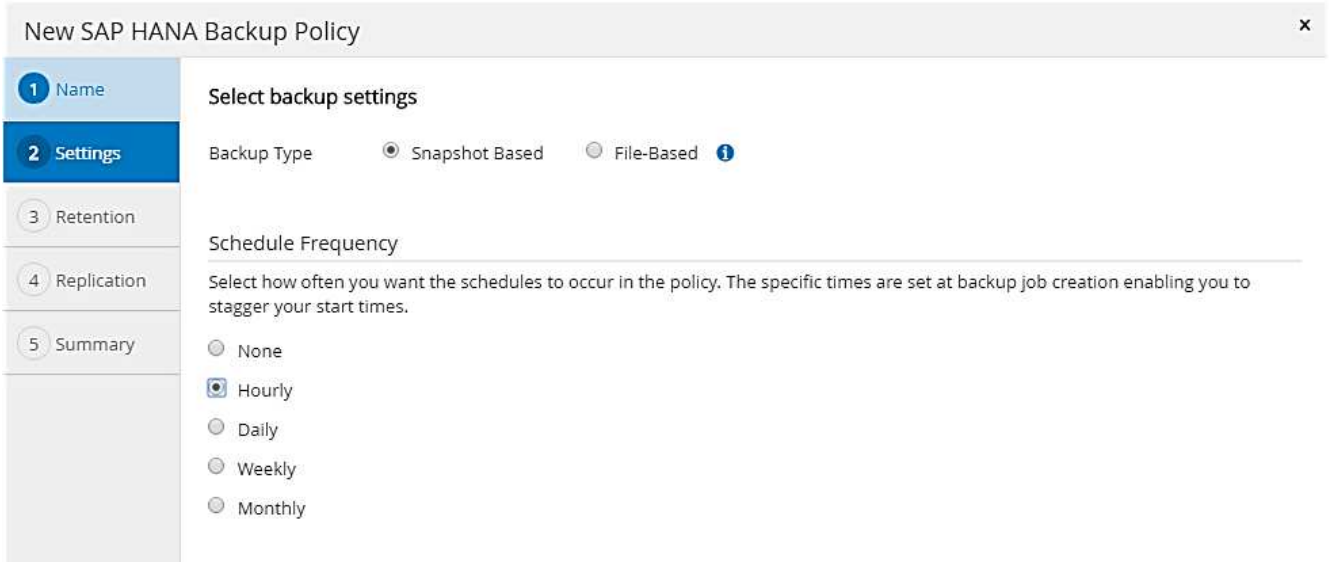
1. Accedere a Impostazioni > Criteri e fare clic su nuovo.



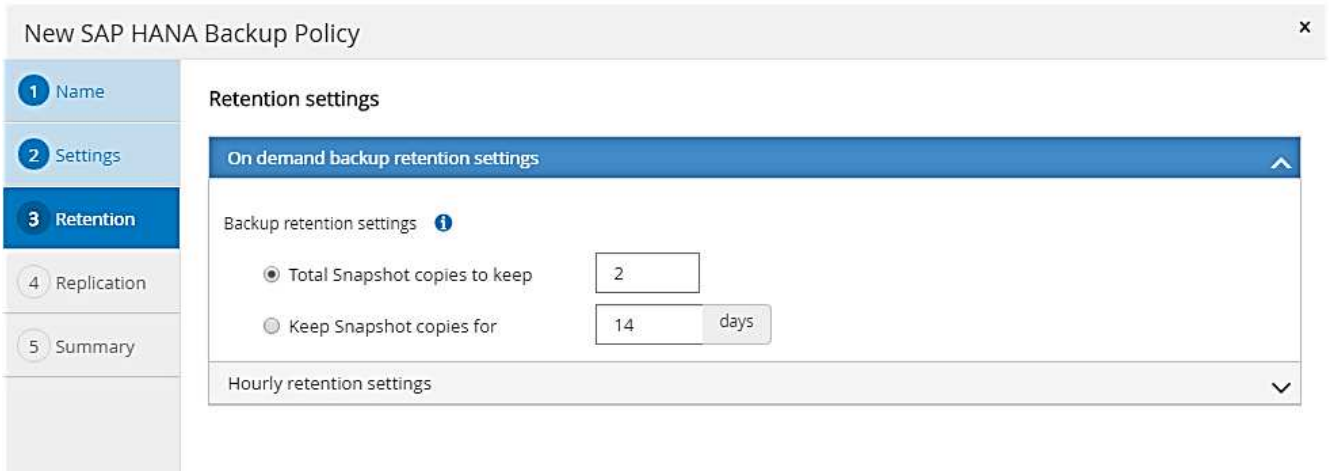
2. Immettere il nome e la descrizione della policy. Fare clic su Avanti.



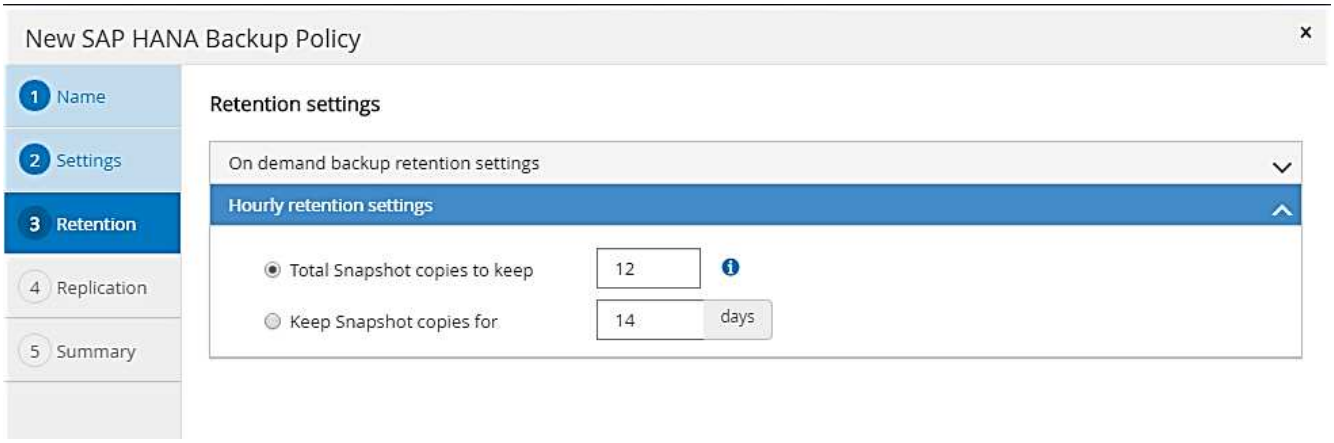
3. Selezionare il tipo di backup basato su Snapshot e selezionare orario per la frequenza di pianificazione.



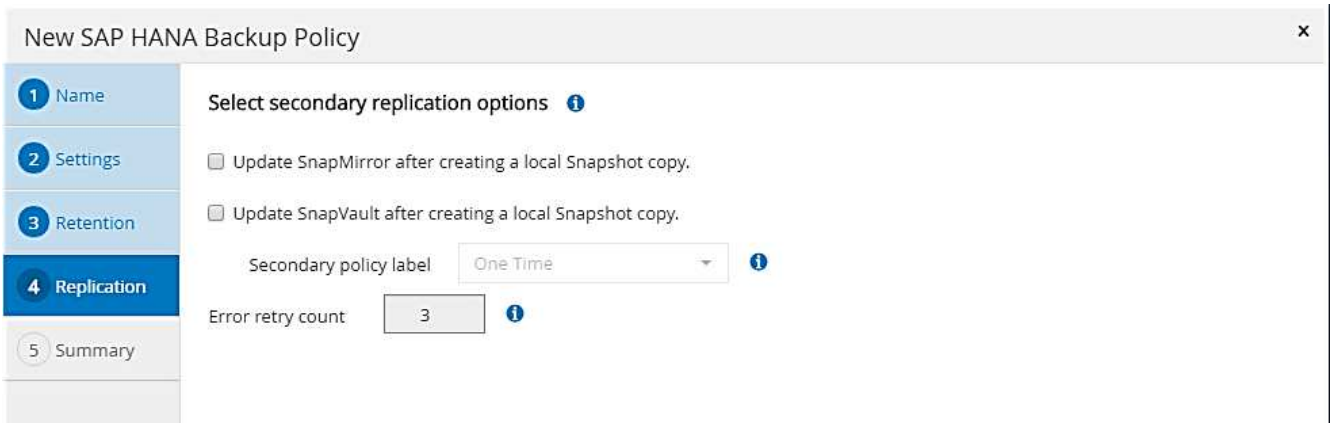
4. Configurare le impostazioni di conservazione per i backup on-demand.



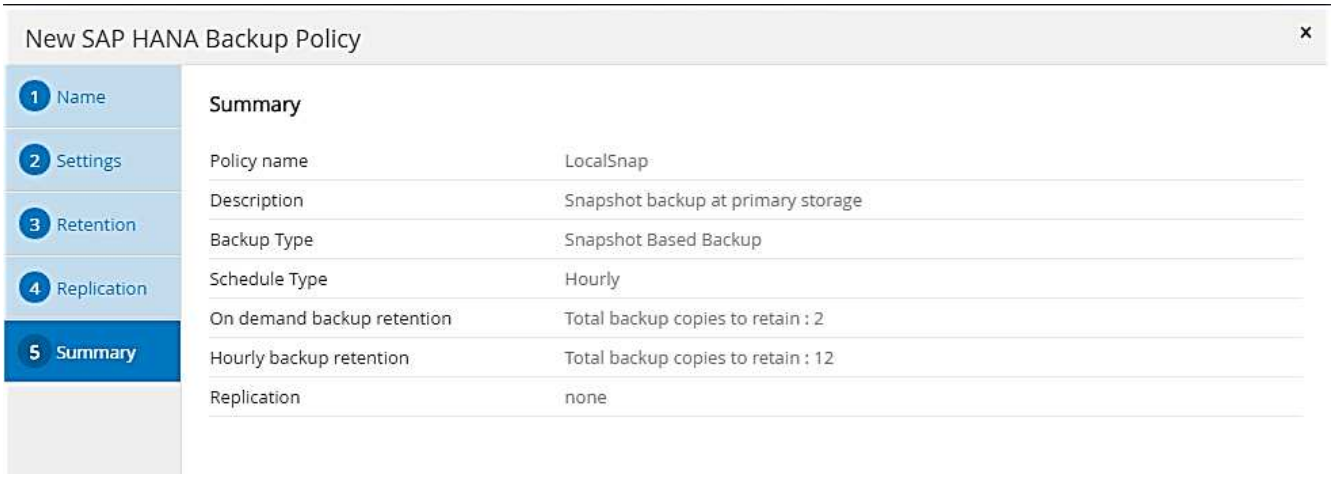
5. Configurare le impostazioni di conservazione per i backup pianificati.



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

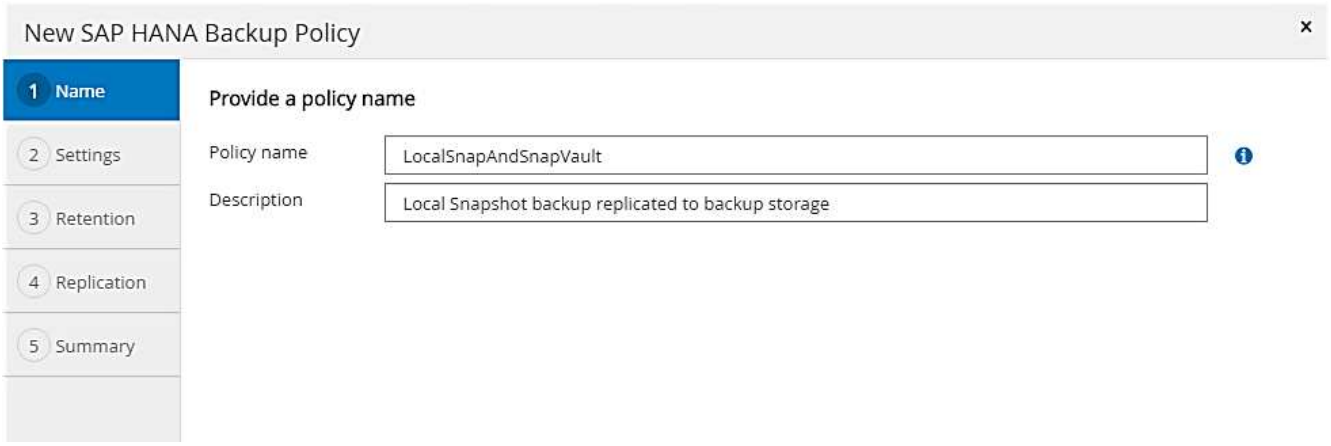


7. Nella pagina Riepilogo, fare clic su fine.

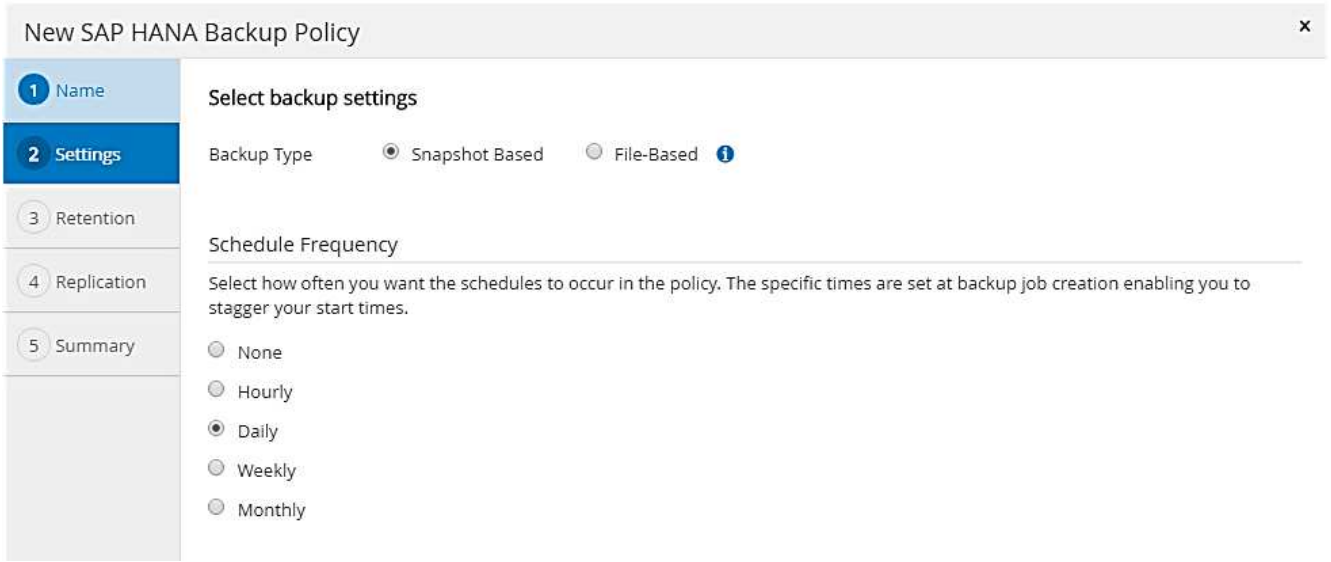


Policy per backup Snapshot giornalieri con replica SnapVault

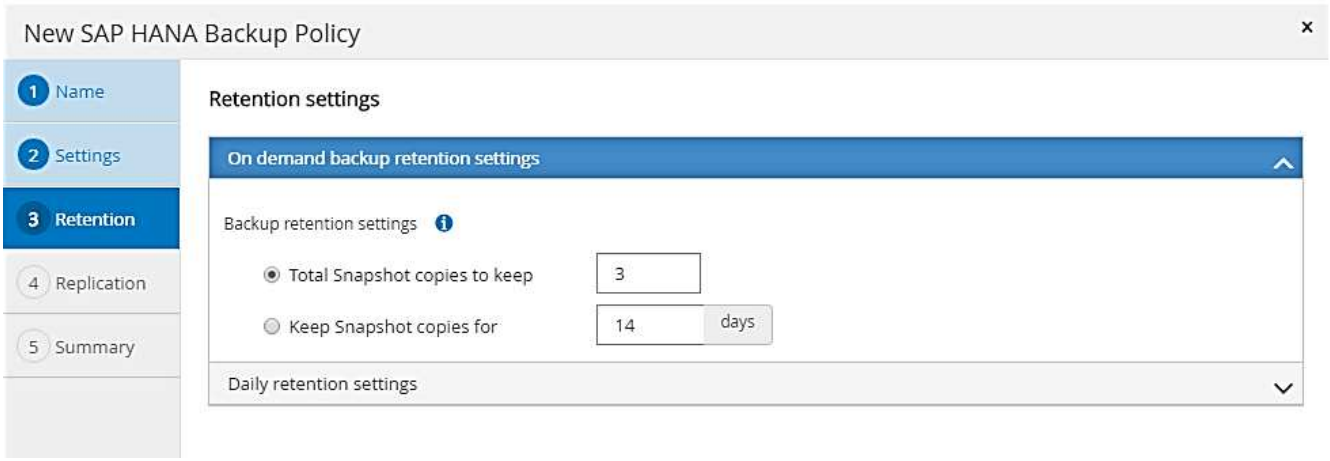
1. Accedere a Impostazioni > Criteri e fare clic su nuovo.
2. Immettere il nome e la descrizione della policy. Fare clic su Avanti.



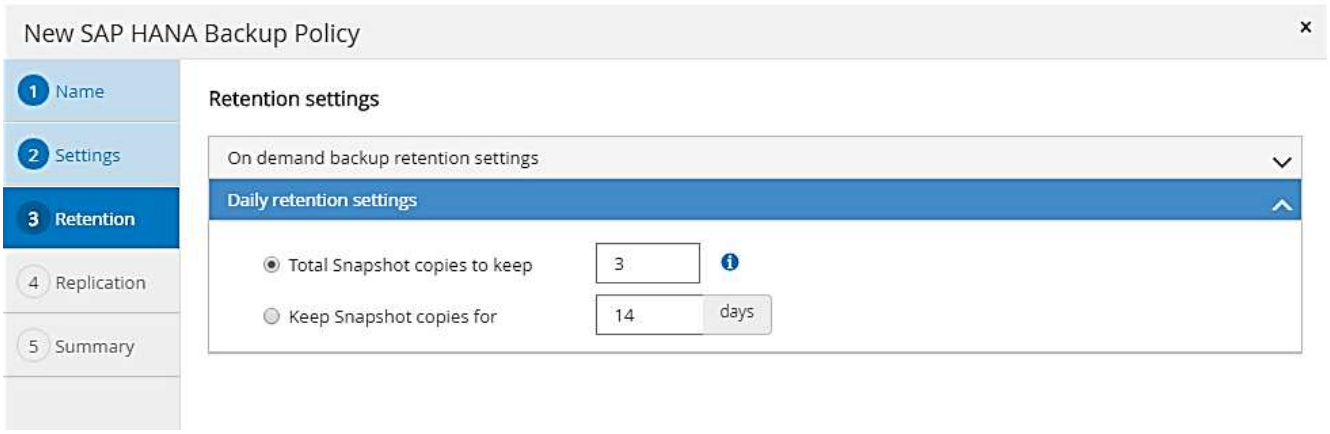
3. Impostare il tipo di backup su Snapshot Based (basato su snapshot) e la frequenza di pianificazione su Daily (giornaliero).



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

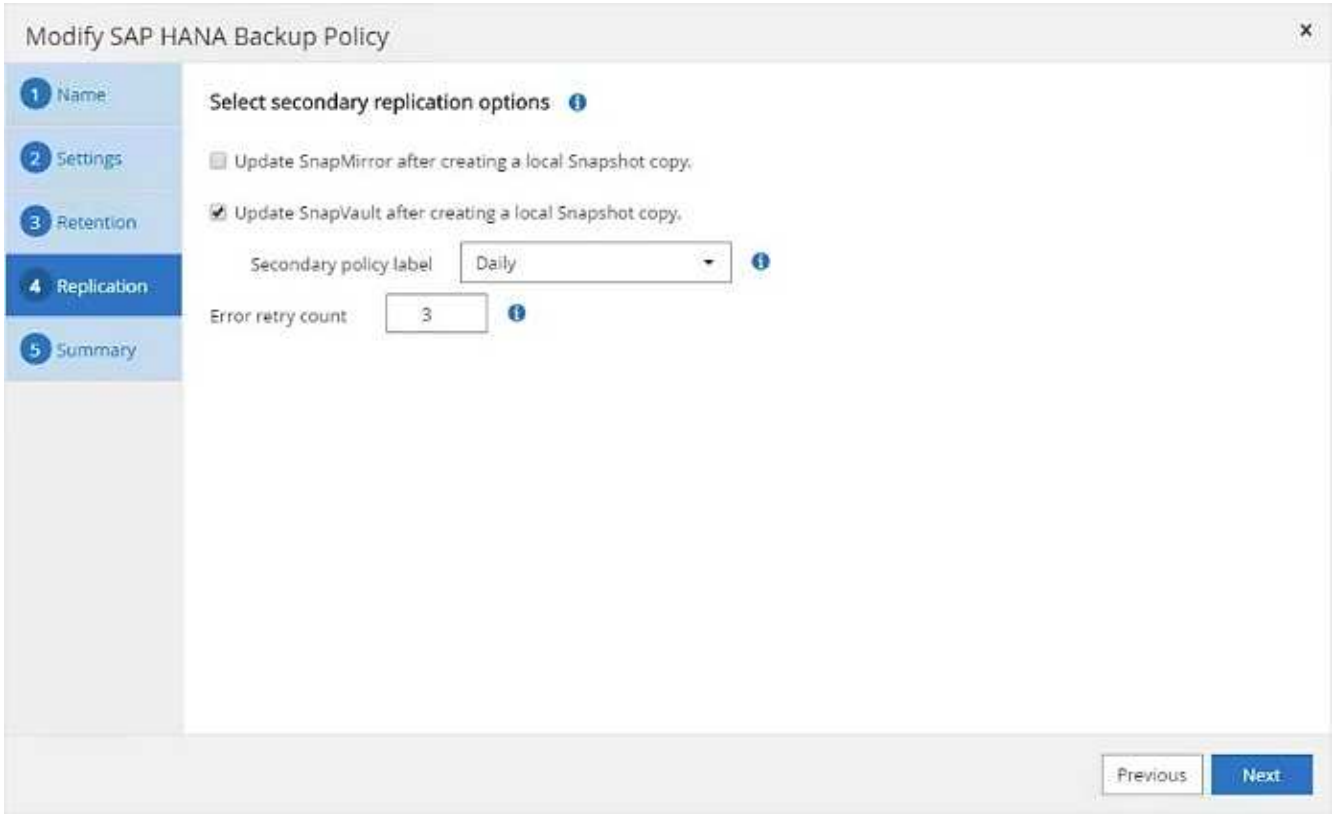


5. Configurare le impostazioni di conservazione per i backup pianificati.

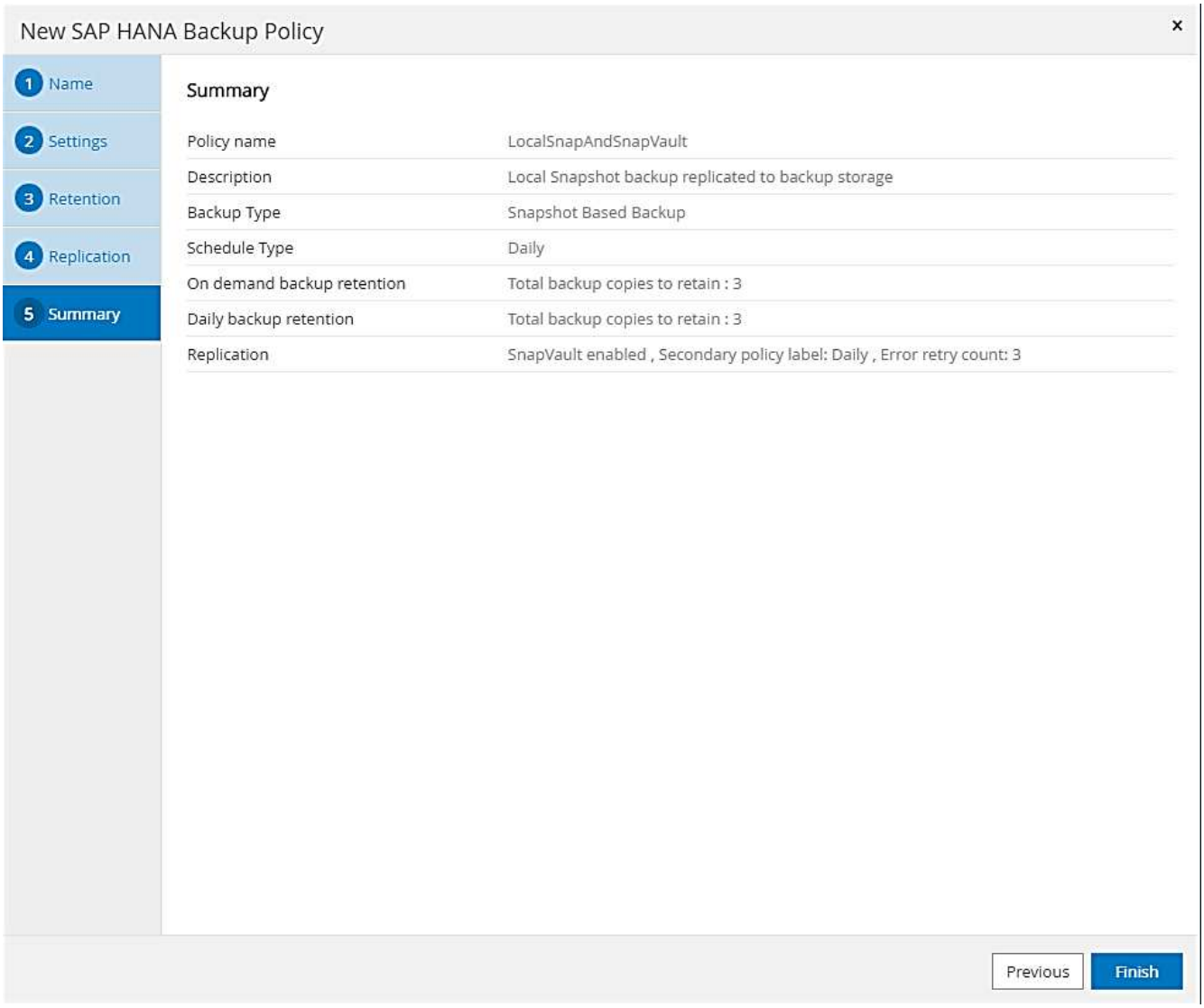


6. Selezionare Aggiorna SnapVault dopo aver creato una copia Snapshot locale.

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"."

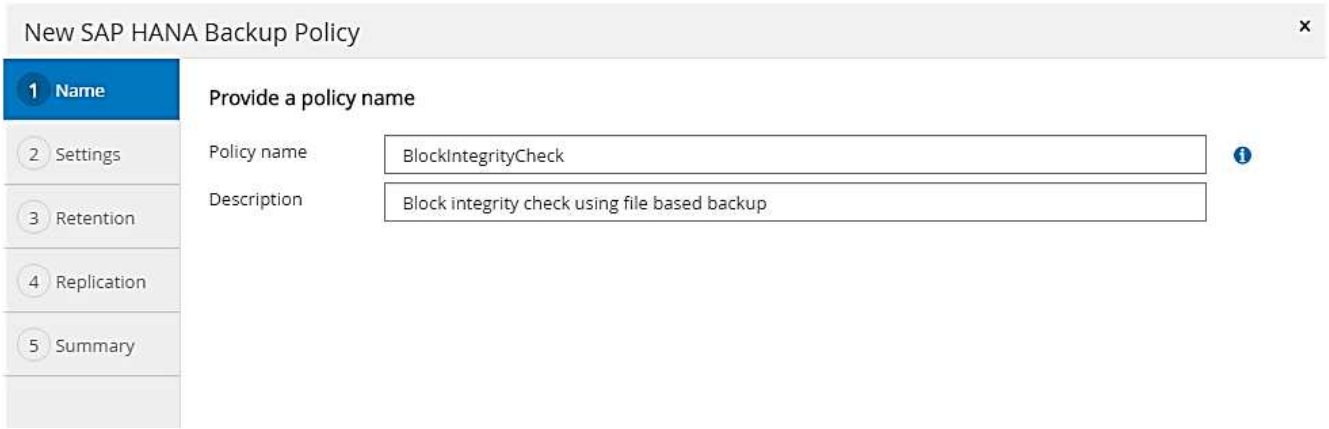


7. Nella pagina Riepilogo, fare clic su fine.

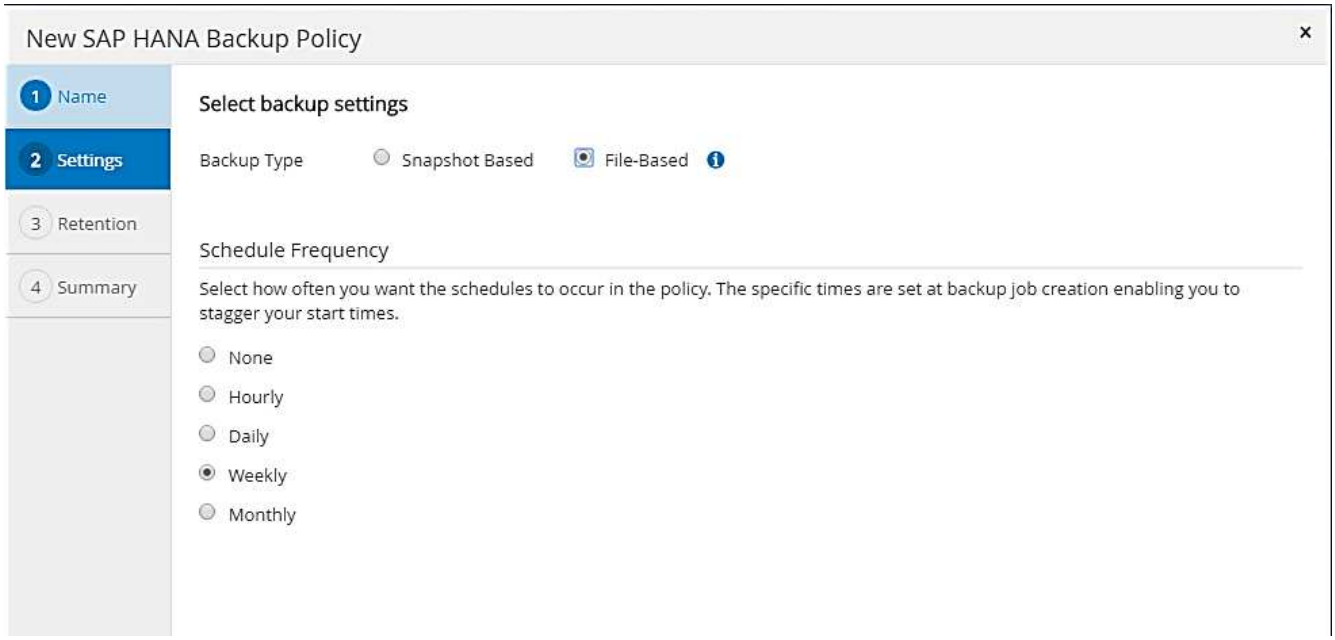


Policy per il controllo settimanale dell'integrità del blocco

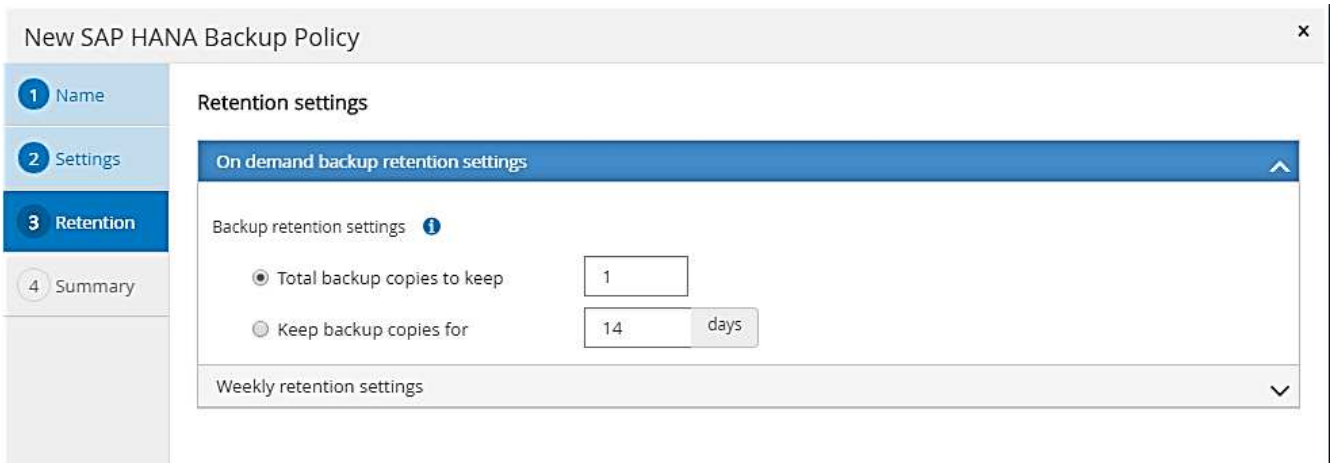
1. Accedere a Impostazioni > Criteri e fare clic su nuovo.
2. Immettere il nome e la descrizione della policy. Fare clic su Avanti.



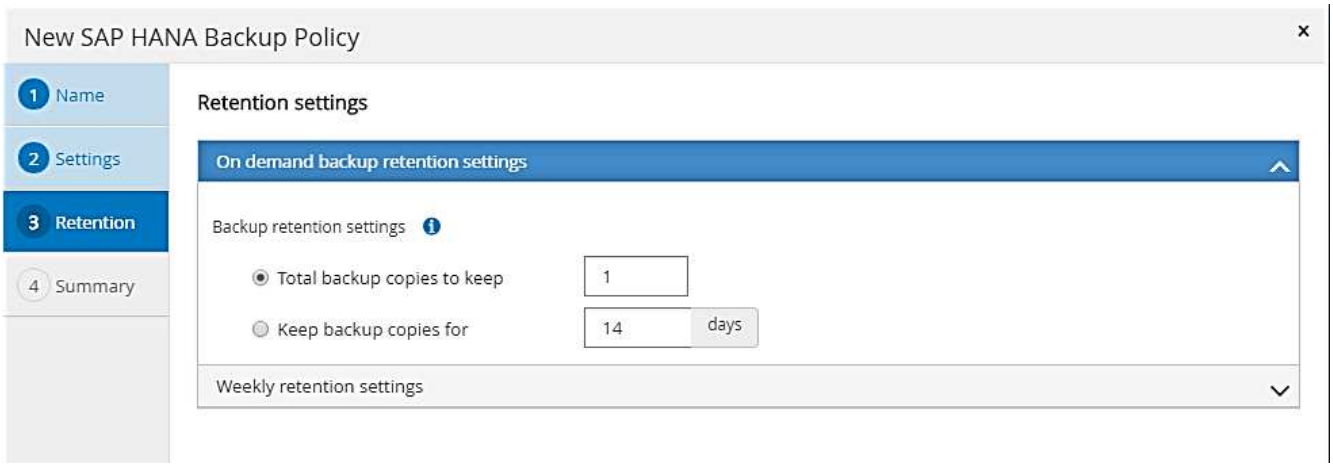
3. Impostare il tipo di backup su file-based (basato su file) e la frequenza di pianificazione su Weekly (settimanale).



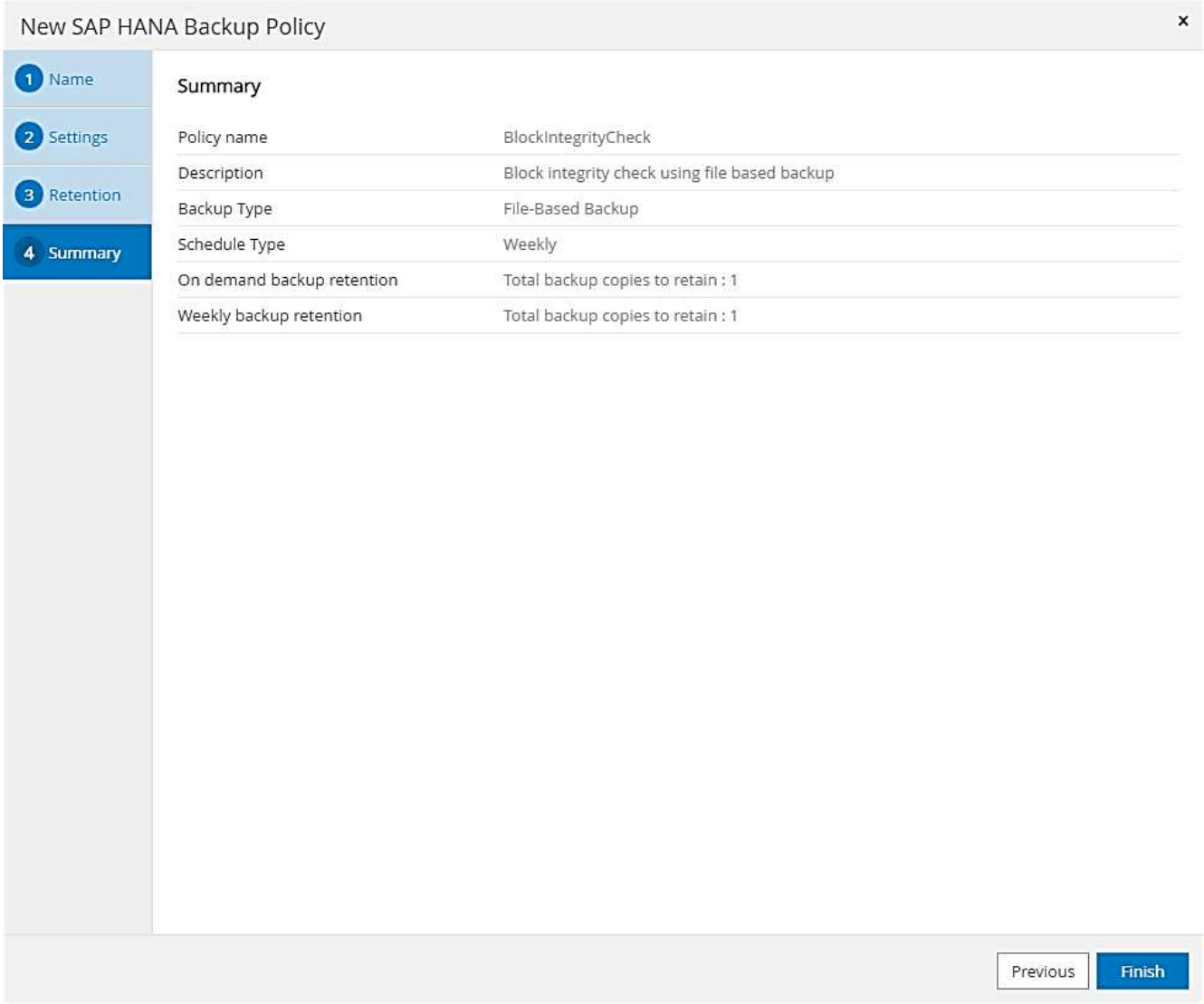
4. Configurare le impostazioni di conservazione per i backup on-demand.



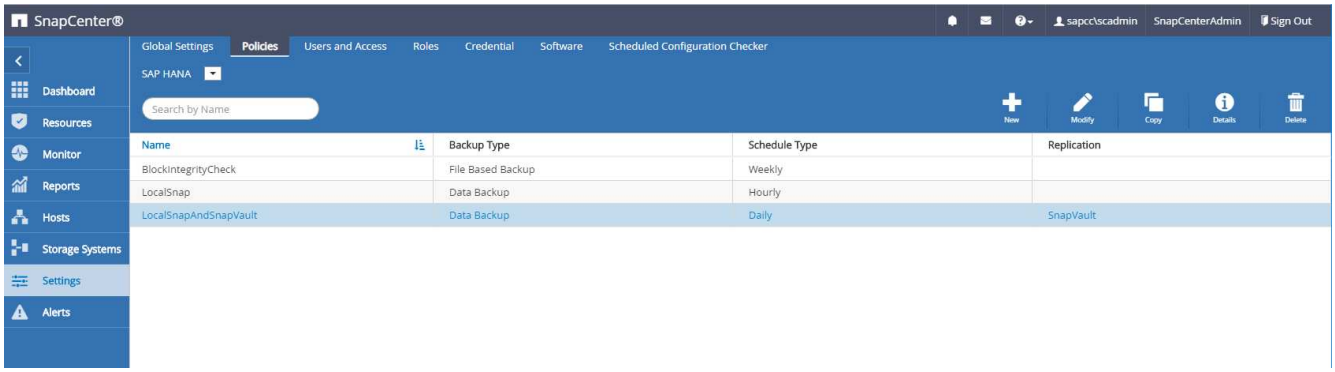
5. Configurare le impostazioni di conservazione per i backup pianificati.



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.

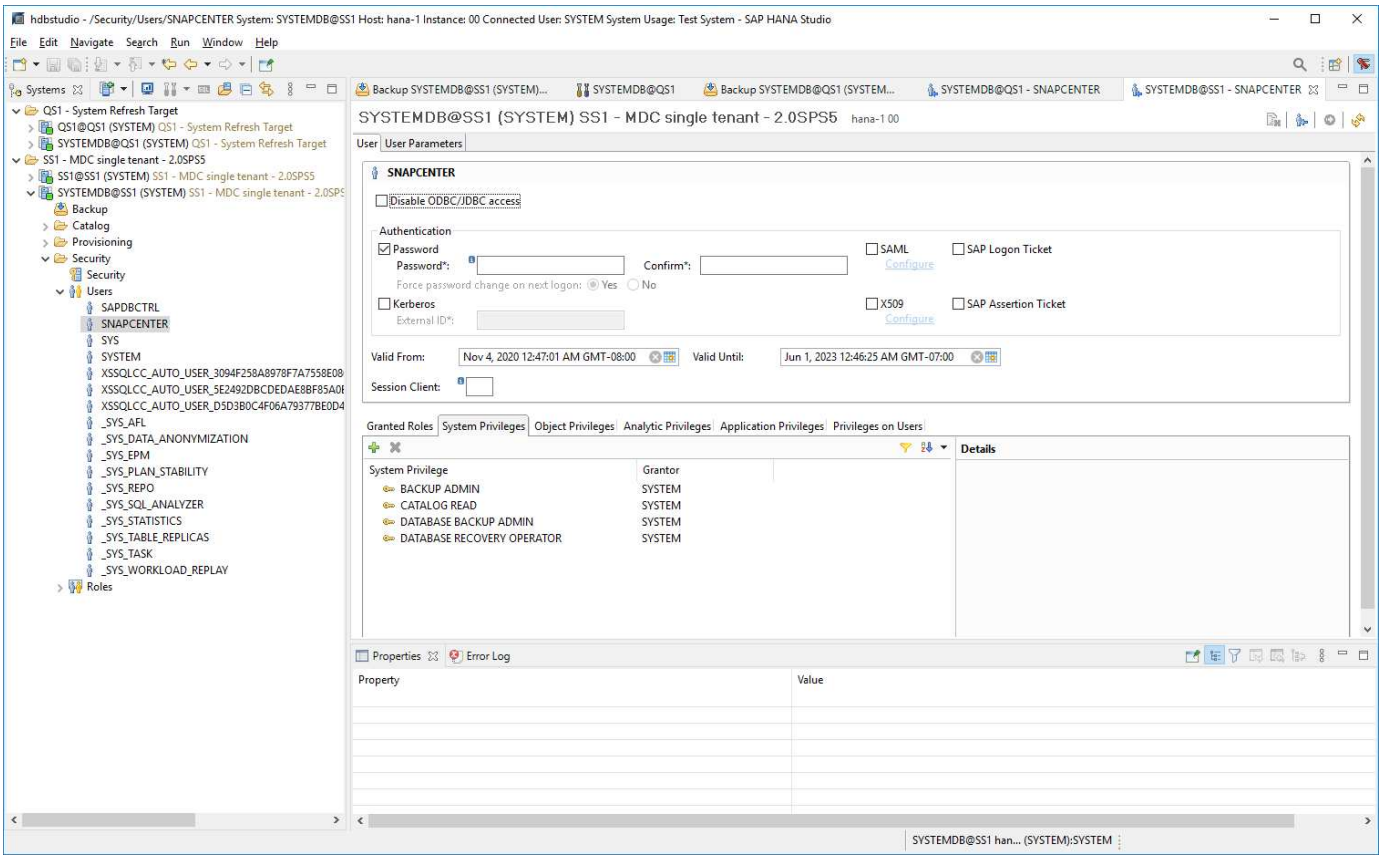
Configurazione di SAP HANA backup user e hdbuserstore

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.

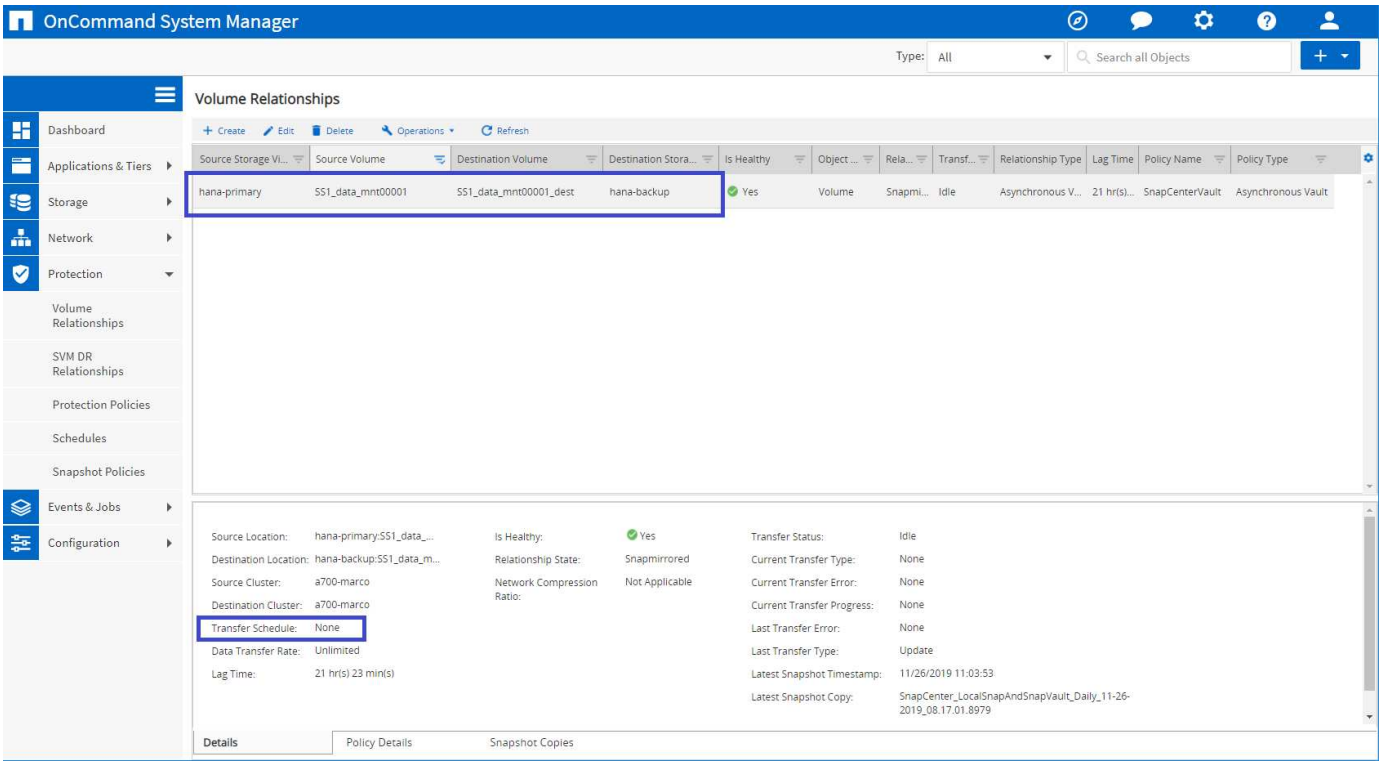
```
hdbuserstore.exe -u SYSTEM set MS1KEYHOST1 hana-4:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST2 hana-5:30013 SNAPCENTER
password
hdbuserstore.exe -u SYSTEM set MS1KEYHOST3 hana-6:30013 SNAPCENTER
password
C:\Program Files\sap\hdbclient>hdbuserstore.exe -u SYSTEM list
DATA FILE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

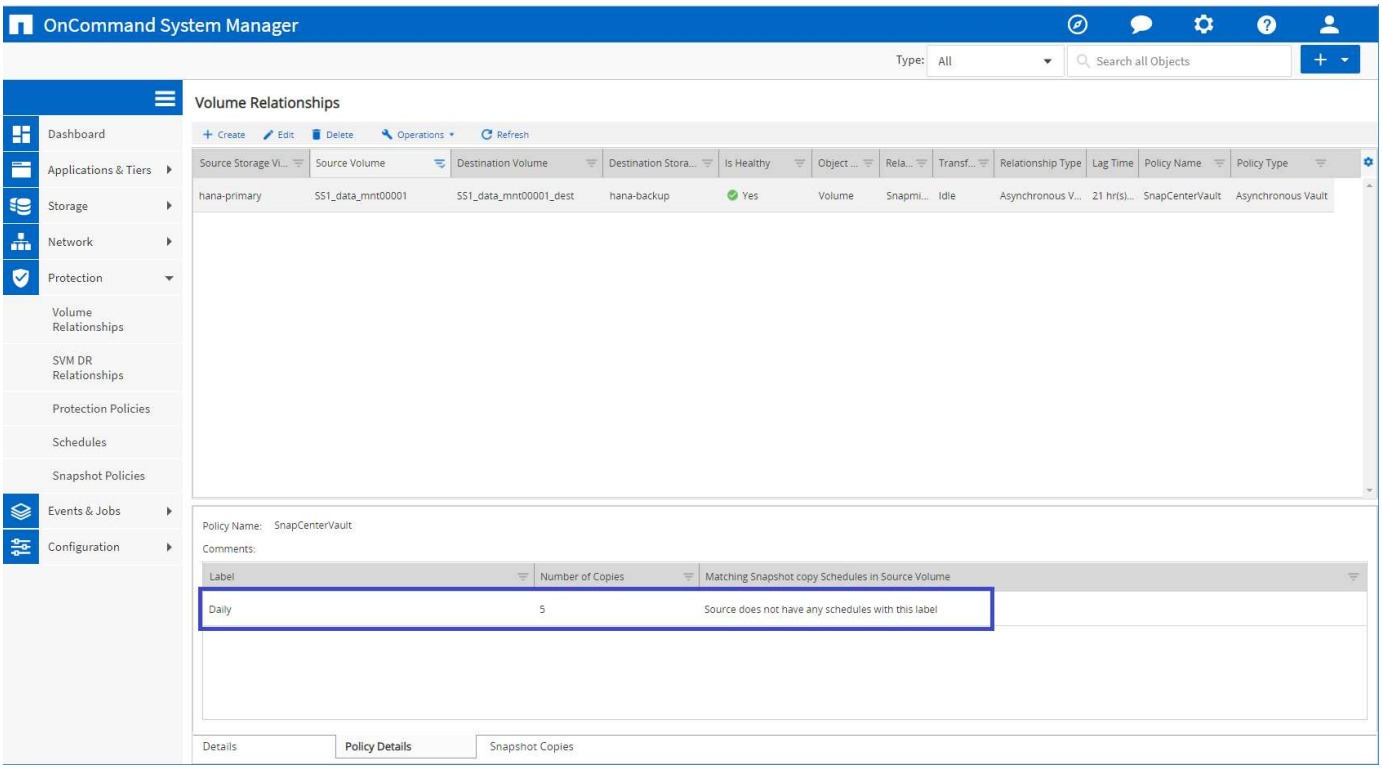
La pianificazione della relazione deve essere impostata su Nessuno, perché SnapCenter attiva l'aggiornamento di SnapVault.



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 alla "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).

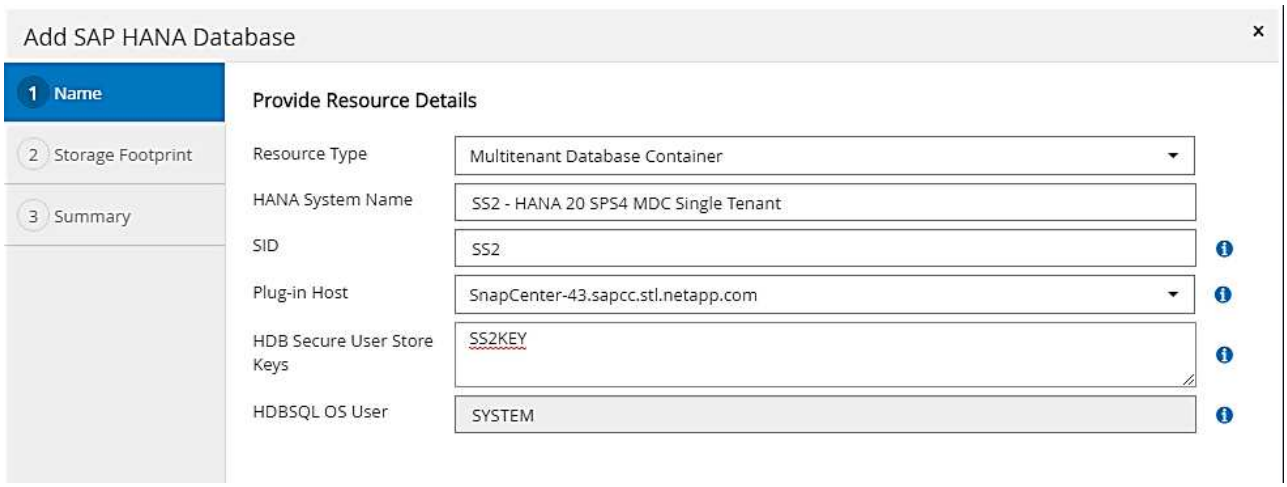
Selezionare il tipo di risorsa nel nostro esempio, Container di database multi-tenant.

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

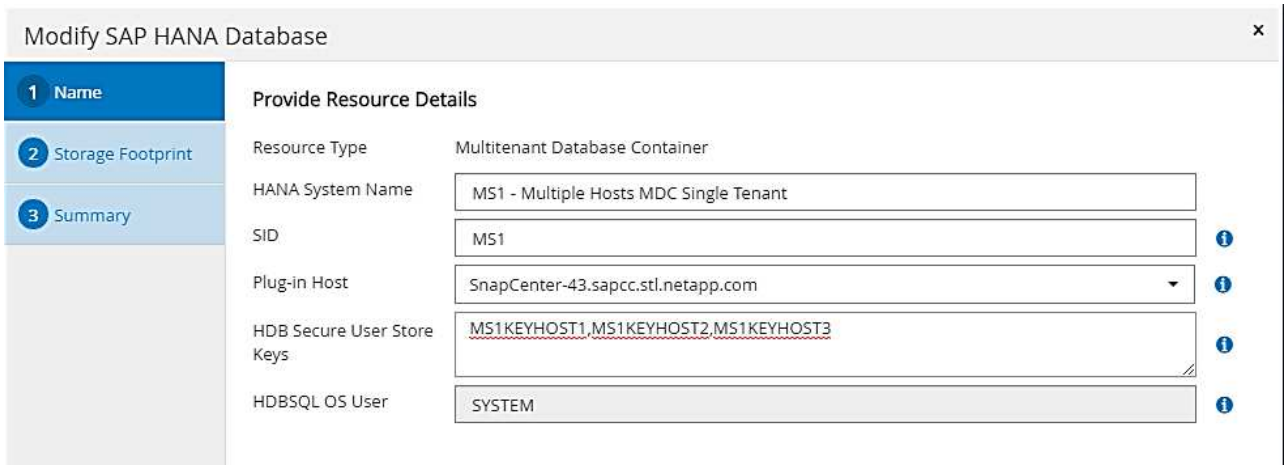
Per il nostro sistema SAP HANA, il SID è SS2.

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

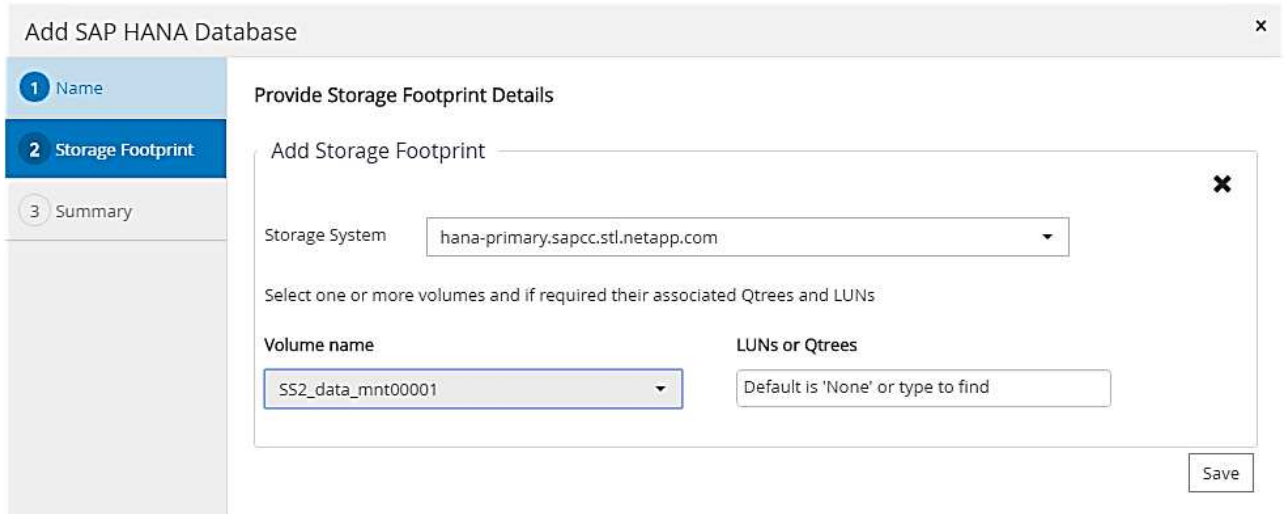
La chiave hdbuserstore deve corrispondere alla chiave configurata per il database HANA SS2. Nel nostro esempio è SS2KEY.



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.

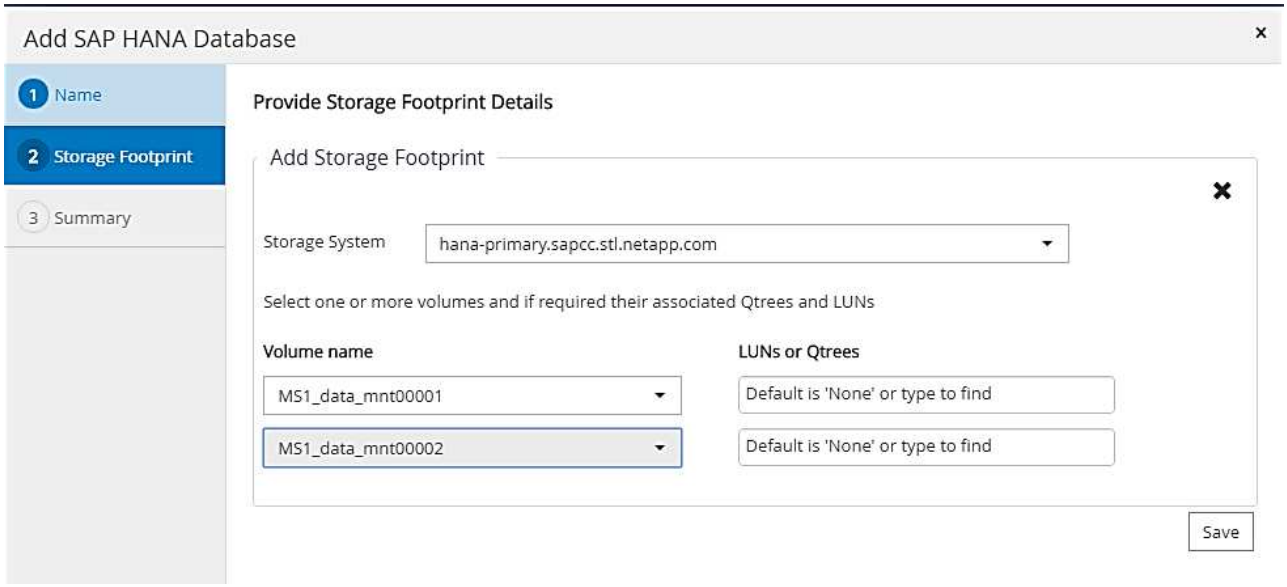


c. Selezionare i dati richiesti per il sistema di storage (SVM) e il nome del volume.



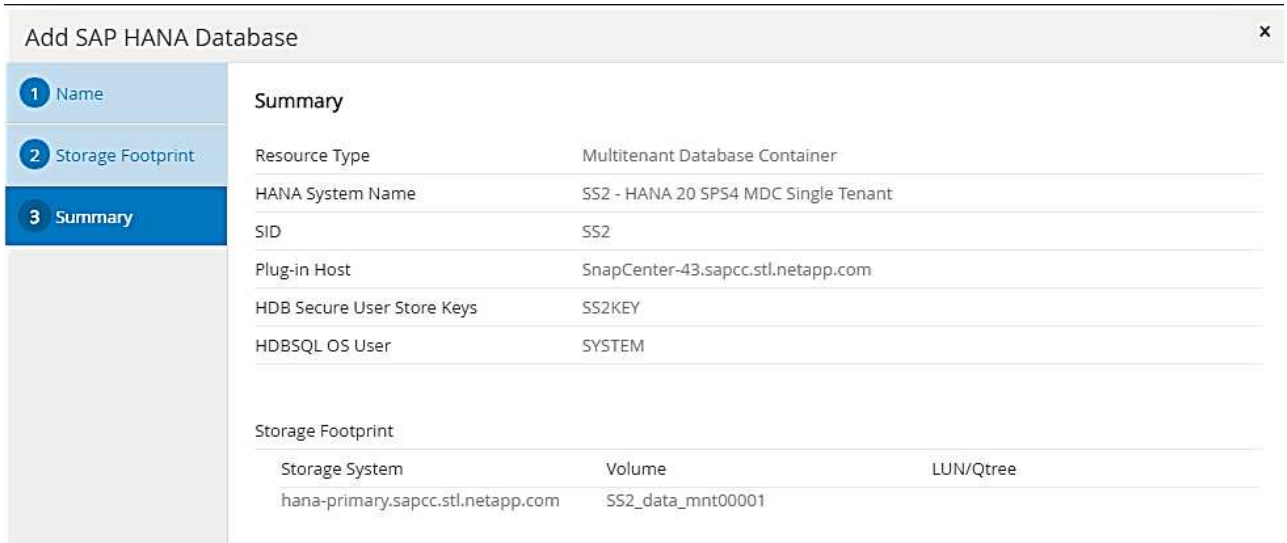
Per una configurazione SAN Fibre Channel, è necessario selezionare anche il LUN.

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.



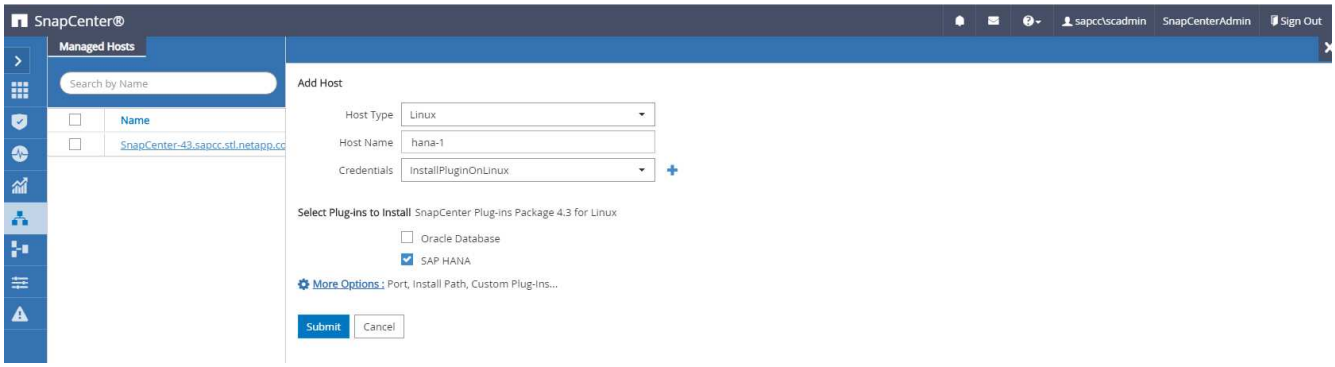
b. Al termine della configurazione delle risorse, eseguire la configurazione della protezione delle risorse come descritto nella sezione "Configurazione della protezione delle risorse".

Rilevamento automatico dei database HANA

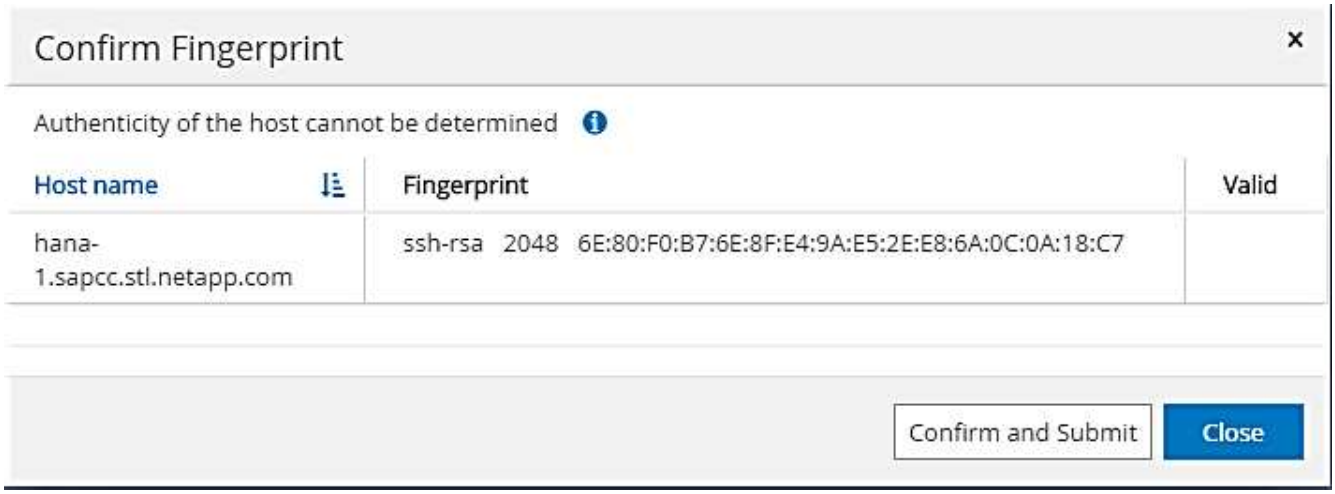
Questa sezione descrive il rilevamento automatico della risorsa SAP HANA SS1 (sistema single-tenant MDC host con NFS). Tutti i passaggi descritti sono identici per un singolo container HANA, per i sistemi di tenant multipli HANA MDC e per un sistema HANA che utilizza SAN Fibre Channel.

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.

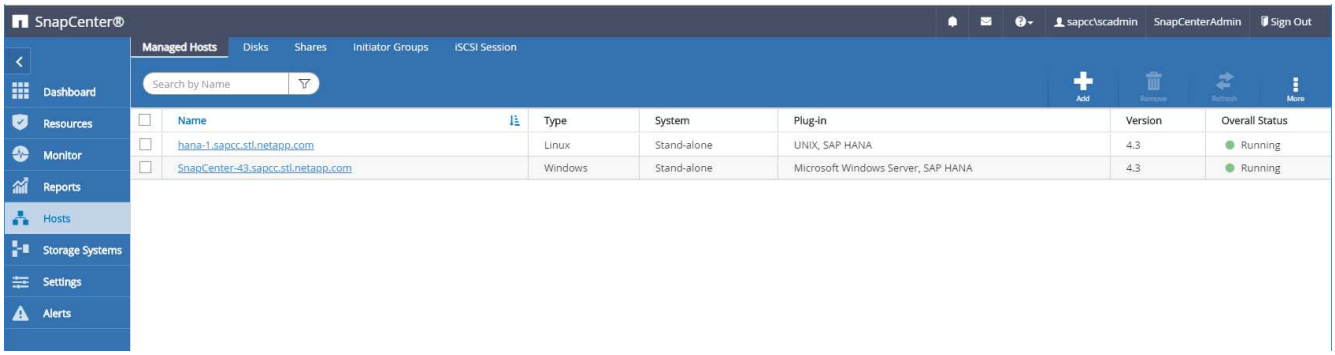
1. Dalla scheda host, fare clic su Add (Aggiungi).
2. Fornire informazioni sull'host e selezionare il plug-in SAP HANA da installare. Fare clic su Invia.



3. Confermare l'impronta digitale.



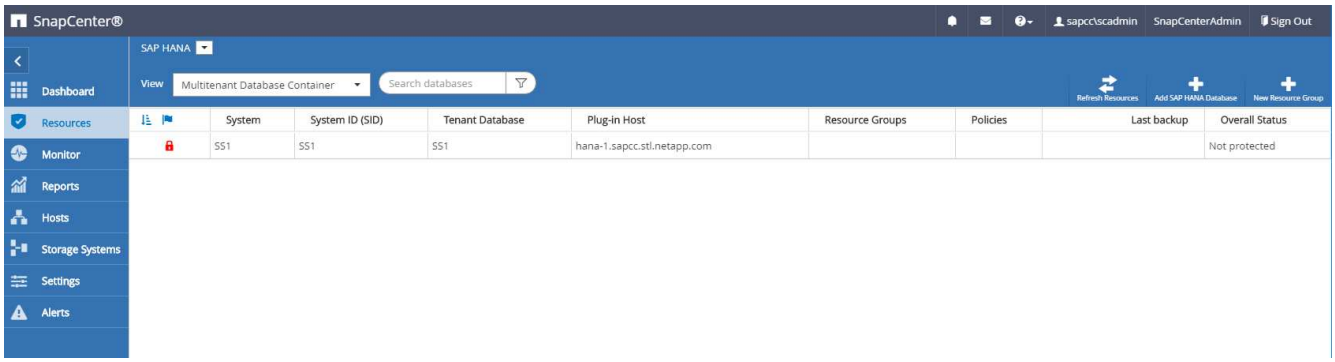
L'installazione del plug-in HANA e del plug-in Linux si avvia automaticamente. Al termine dell'installazione, la colonna di stato dell'host mostra in esecuzione. La schermata mostra inoltre che il plug-in Linux è installato insieme al plug-in HANA.



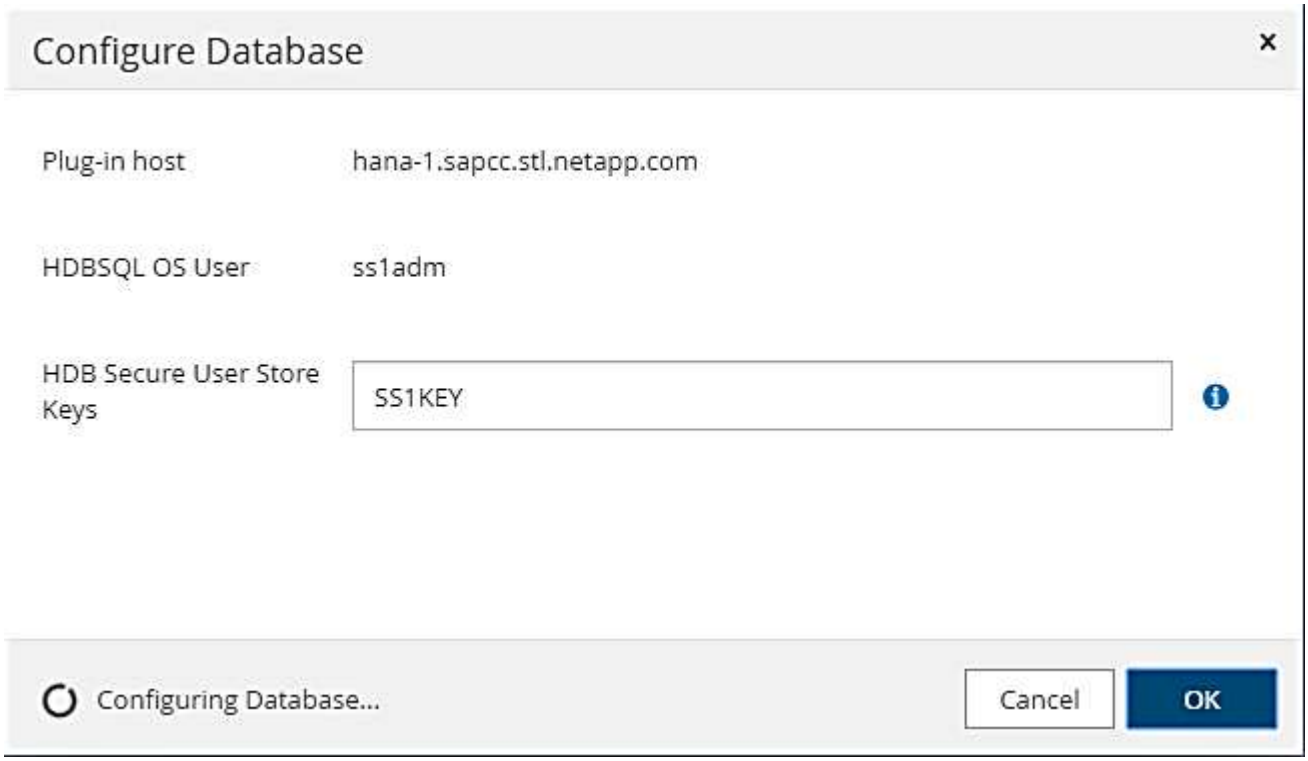
Dopo l'installazione del plug-in, il processo di rilevamento automatico della risorsa HANA viene avviato automaticamente. Nella schermata Resources (risorse) viene creata una nuova risorsa, contrassegnata come bloccata con l'icona del lucchetto rosso.

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.

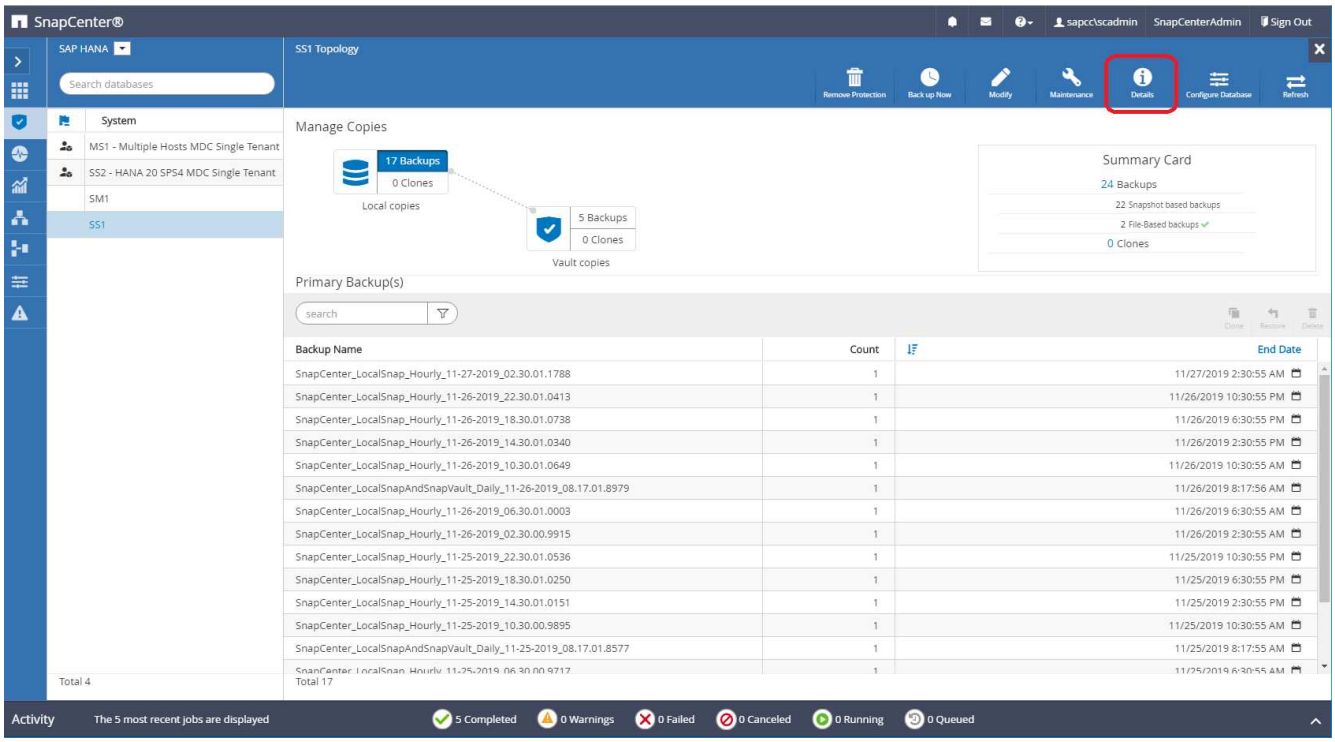


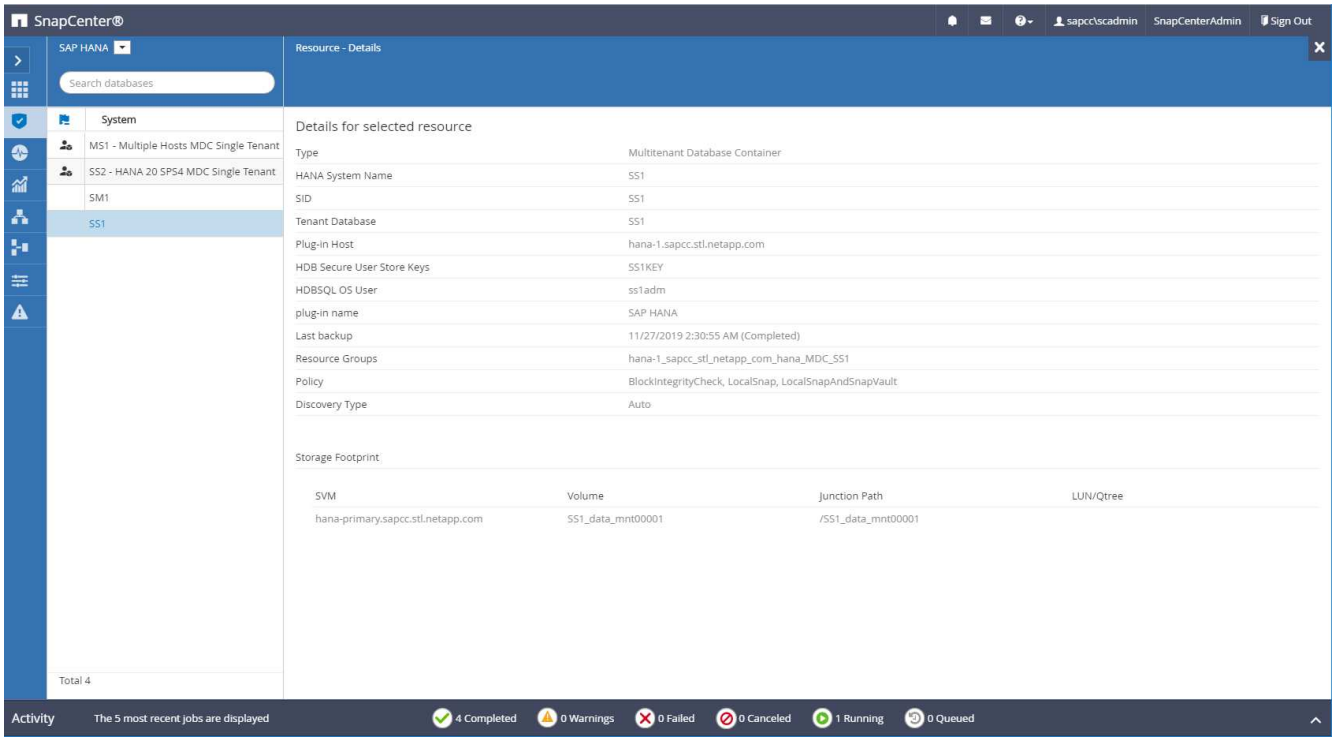
5. Fornire la chiave dell'archivio utenti per il database HANA.



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.

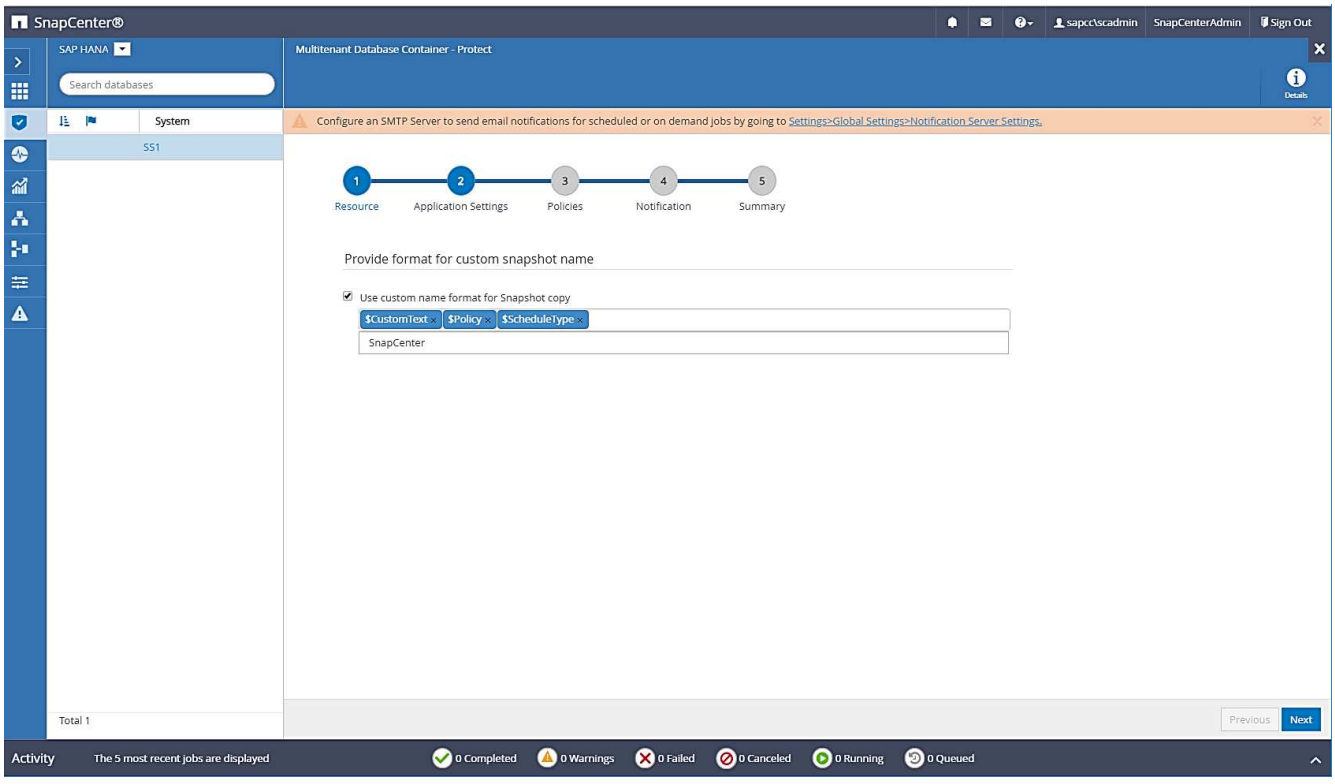
1. Dalla scheda risorse, fare doppio clic sulla risorsa.
2. Configurare un formato nome personalizzato per la copia Snapshot.

> 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`.

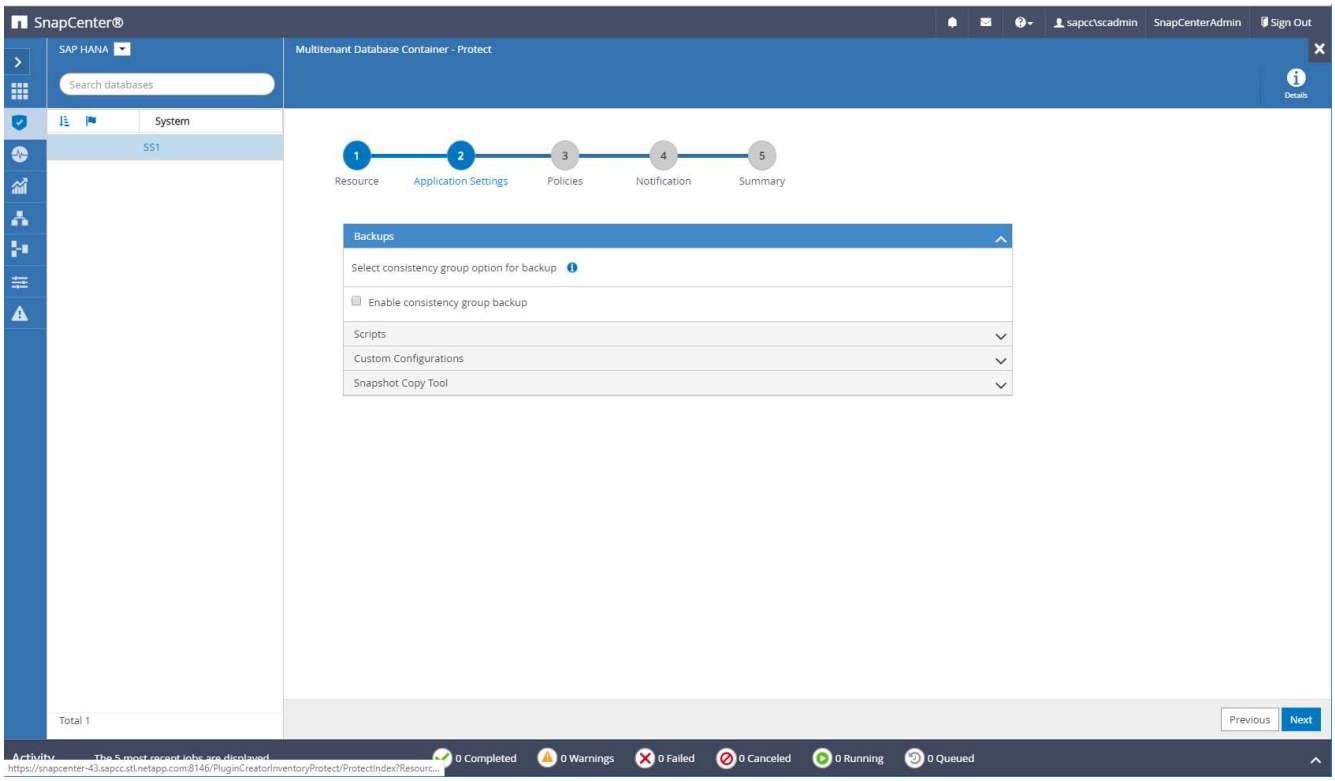
Nella configurazione illustrata nella figura seguente, i nomi delle copie Snapshot e di backup hanno il seguente formato:

- 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>`

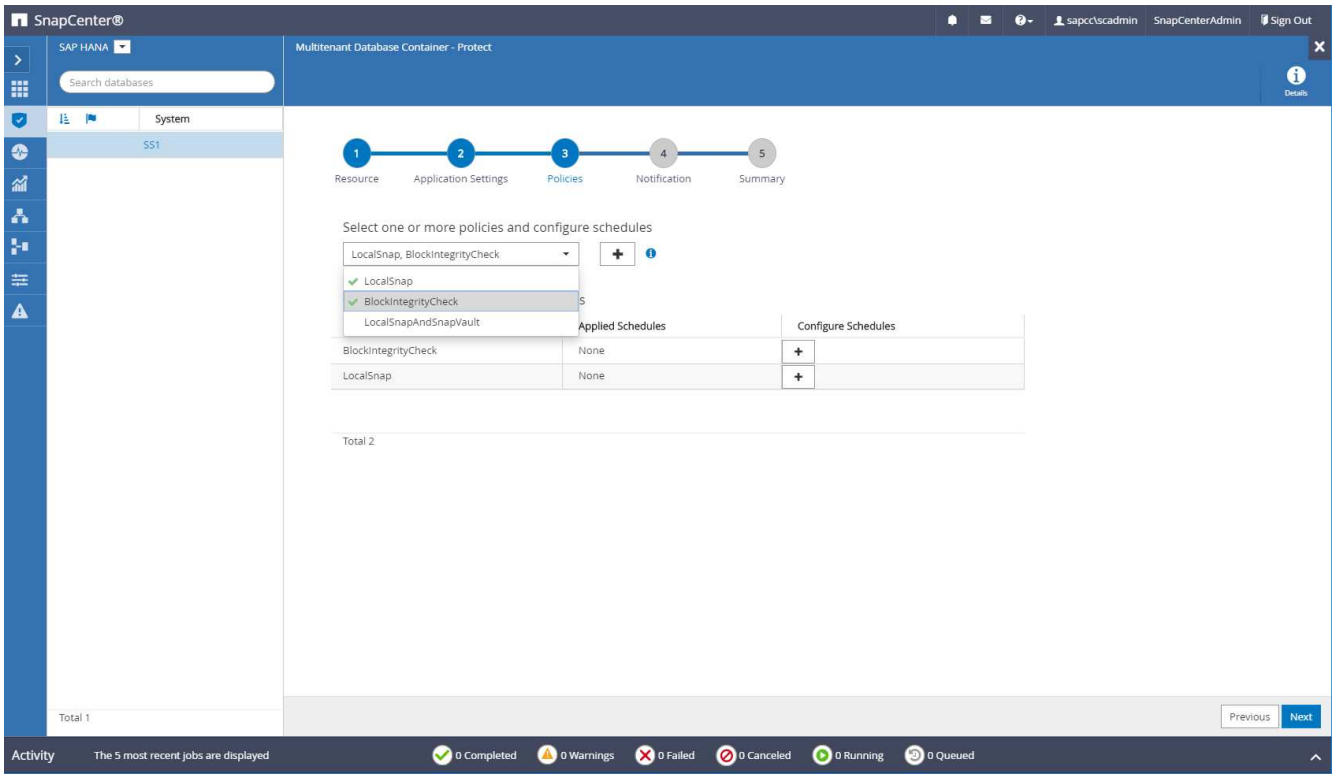
> Anche se viene definita una conservazione per i backup on-demand nella configurazione dei criteri, la pulizia viene eseguita solo quando viene eseguito un altro backup on-demand. Di conseguenza, i backup on-demand devono in genere essere cancellati manualmente in SnapCenter per assicurarsi che questi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



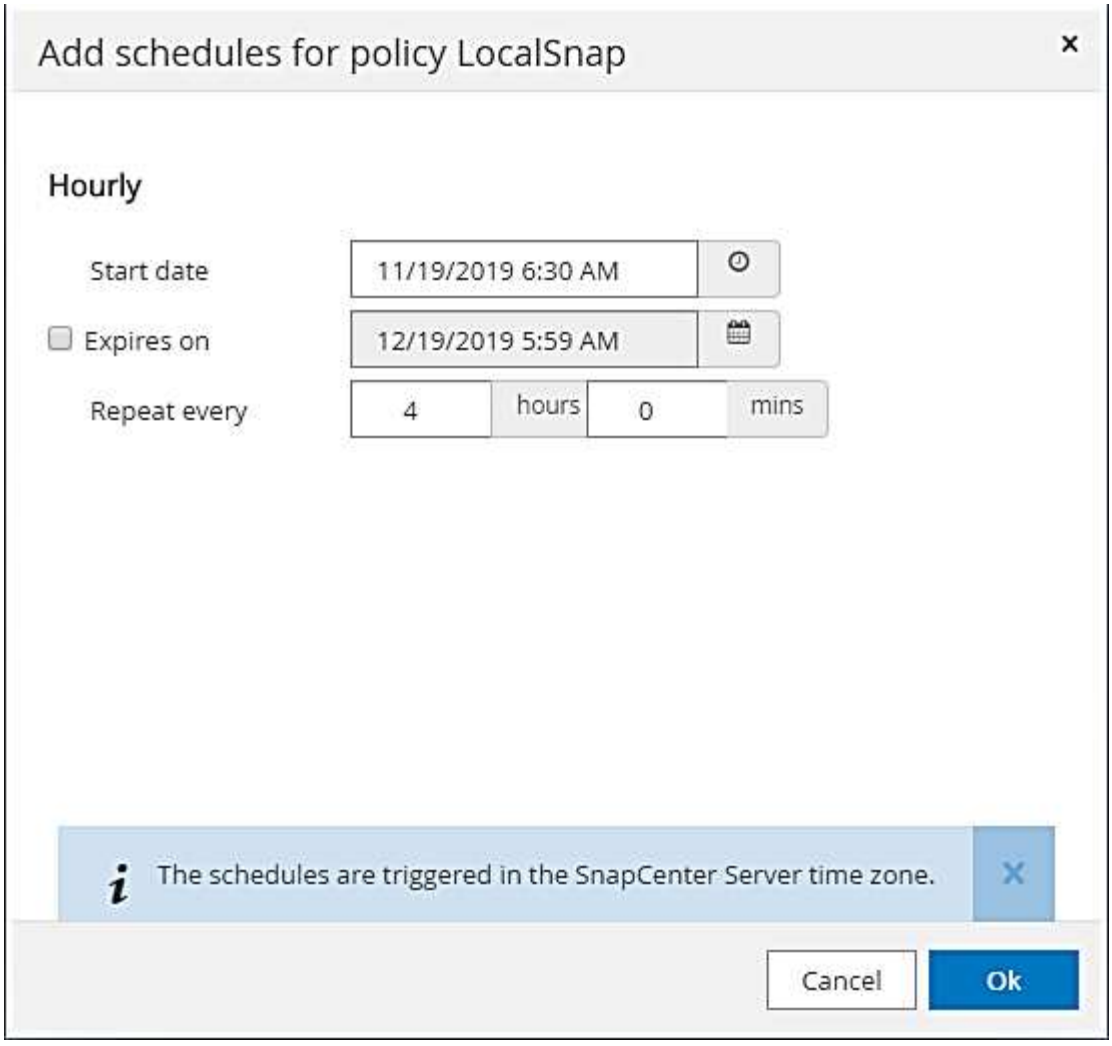
3. Non è necessario impostare impostazioni specifiche nella pagina Impostazioni applicazione. Fare clic su Avanti.



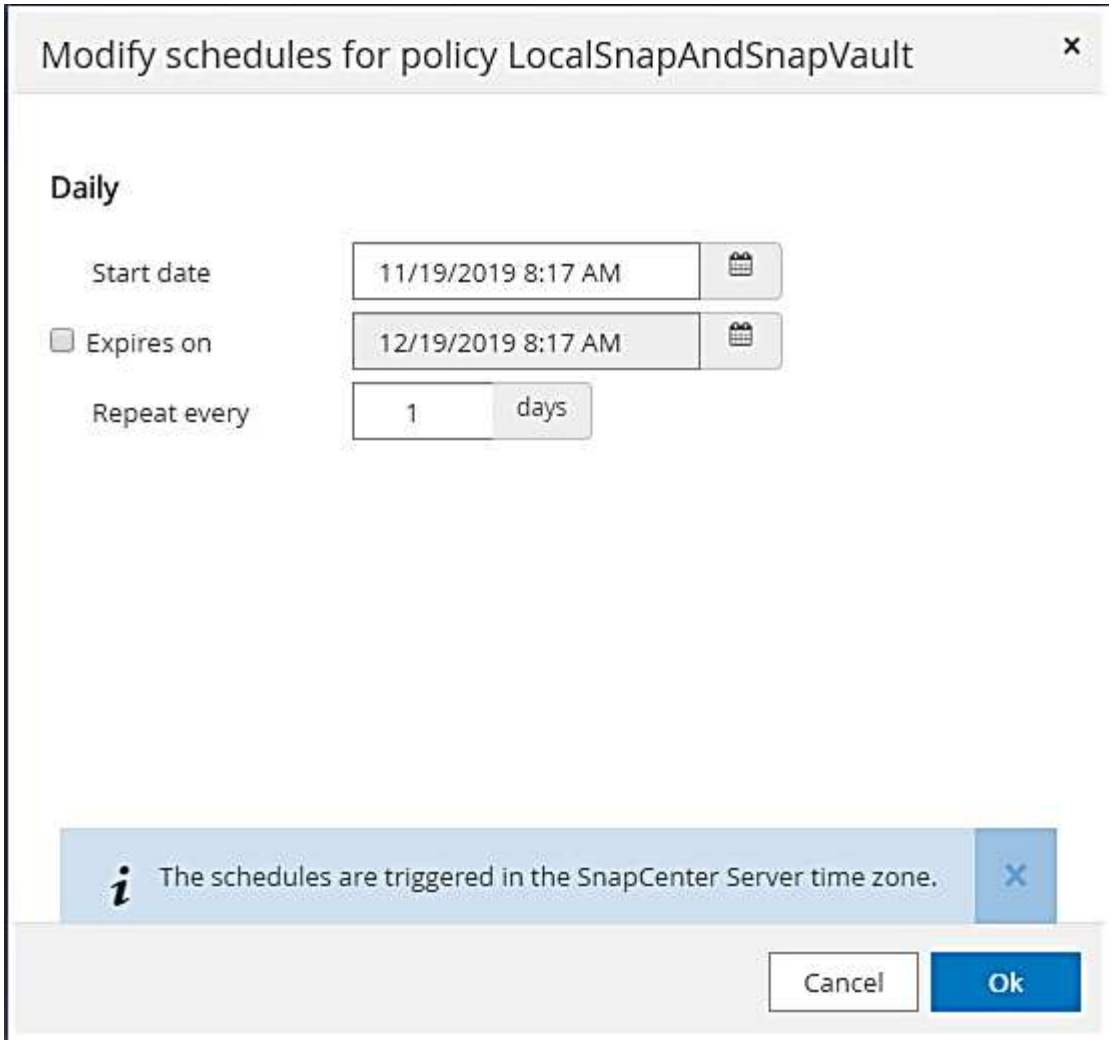
4. Selezionare i criteri da aggiungere alla risorsa.



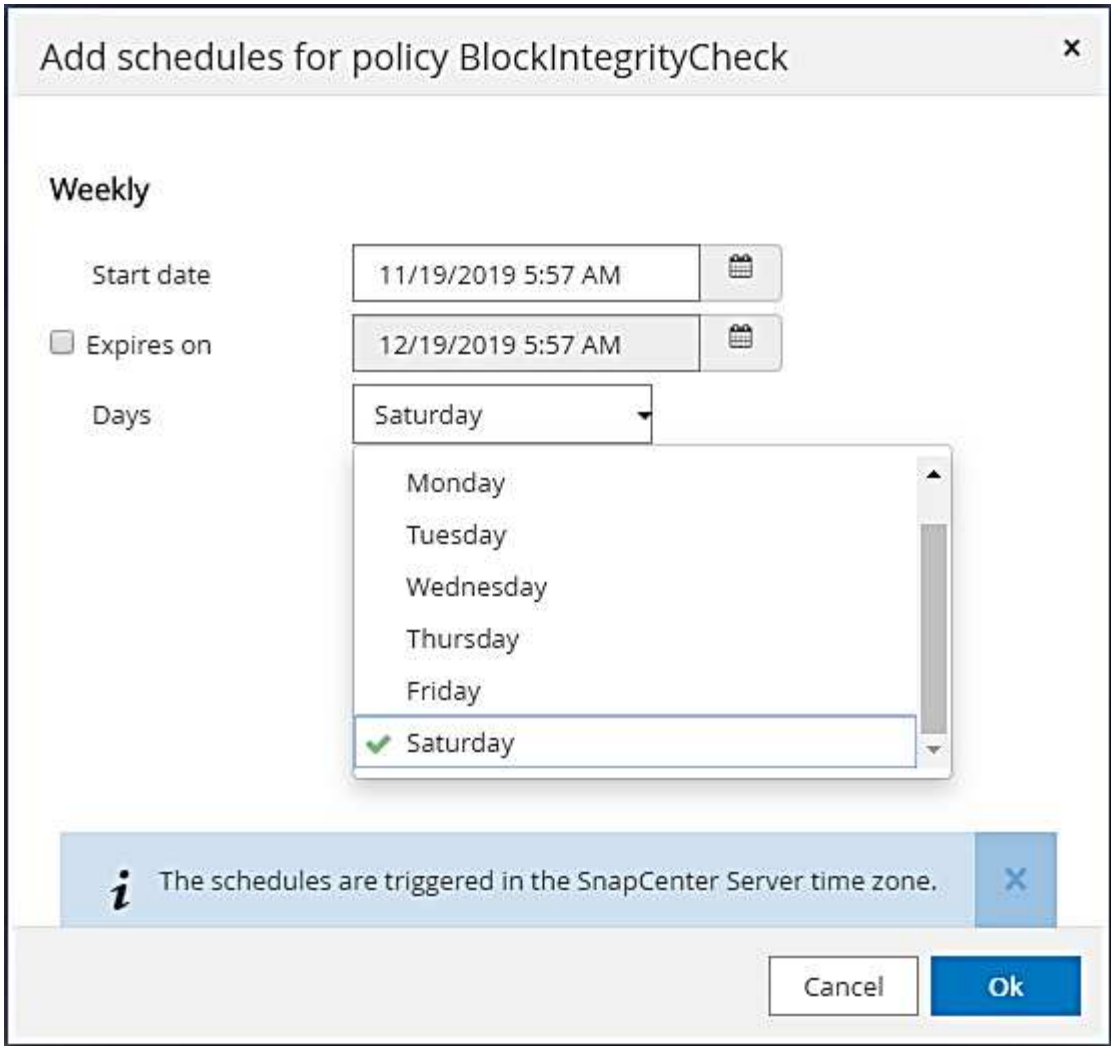
5. Definire la pianificazione per il criterio LocalSnap (in questo esempio, ogni quattro ore).



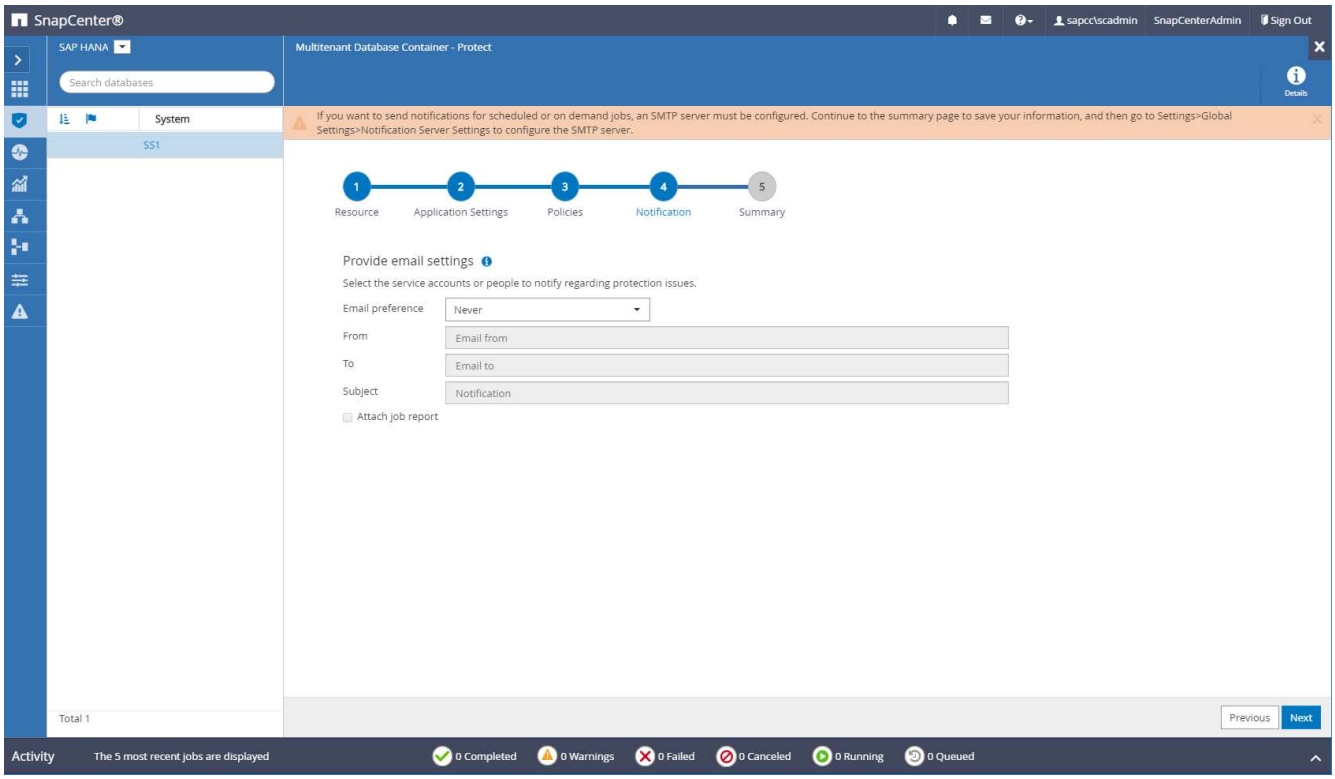
6. Definire la pianificazione per la policy LocalSnapAndSnapVault (in questo esempio, una volta al giorno).



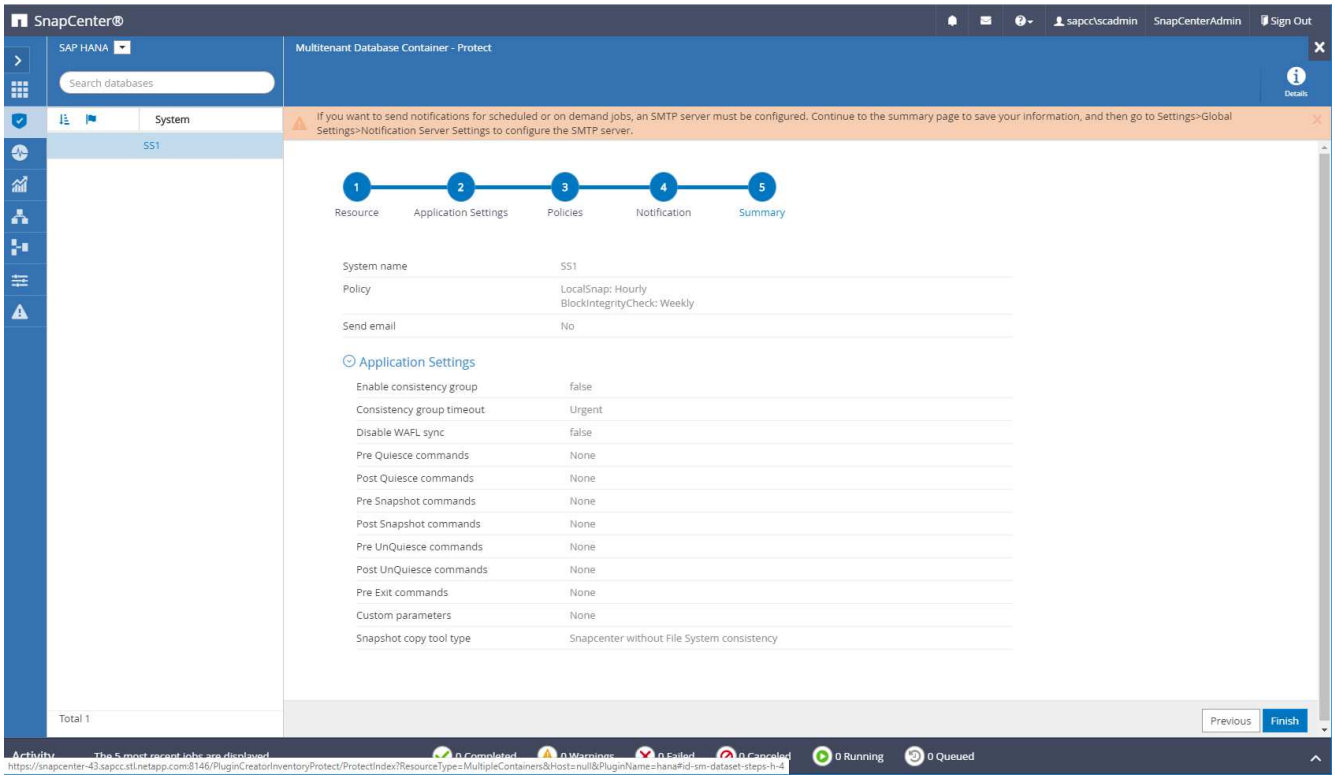
7. Definire la pianificazione per la policy di controllo dell'integrità del blocco (in questo esempio, una volta alla settimana).



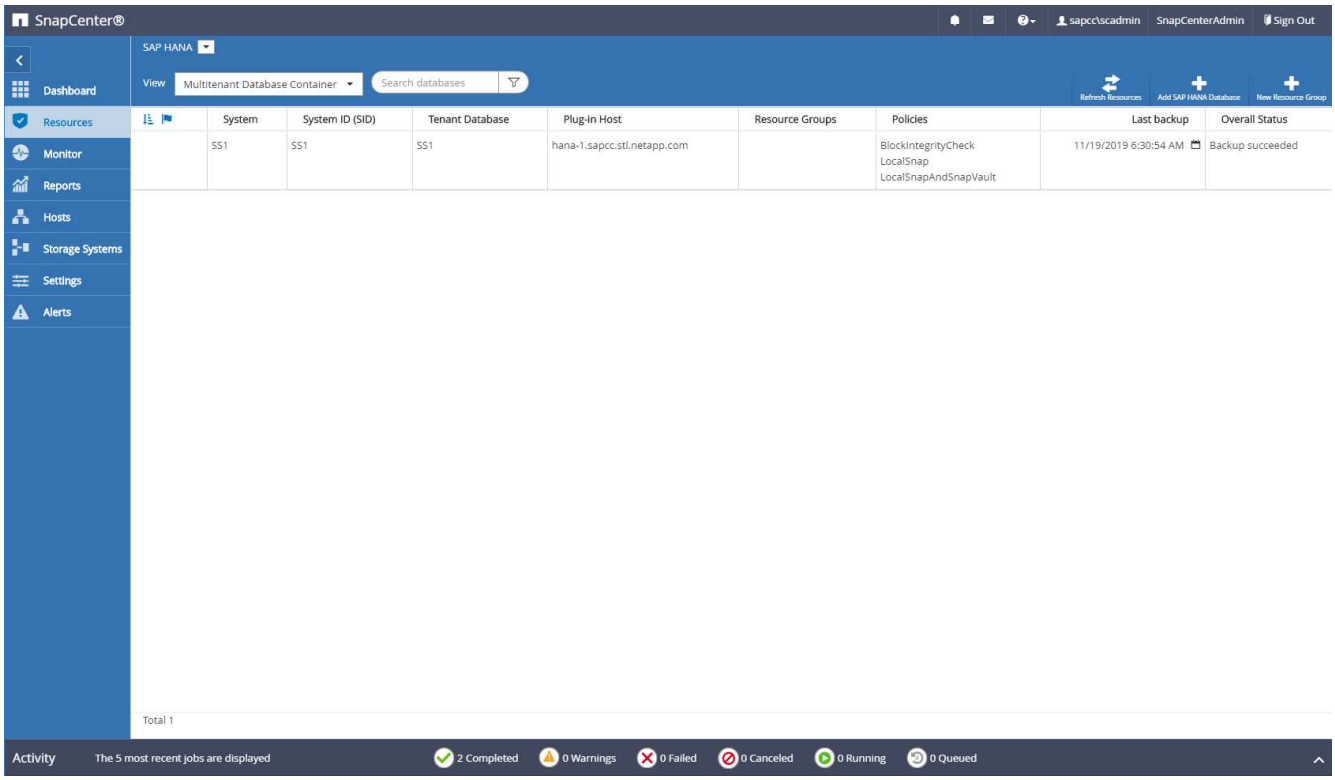
8. Fornire informazioni sulla notifica via email.



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.

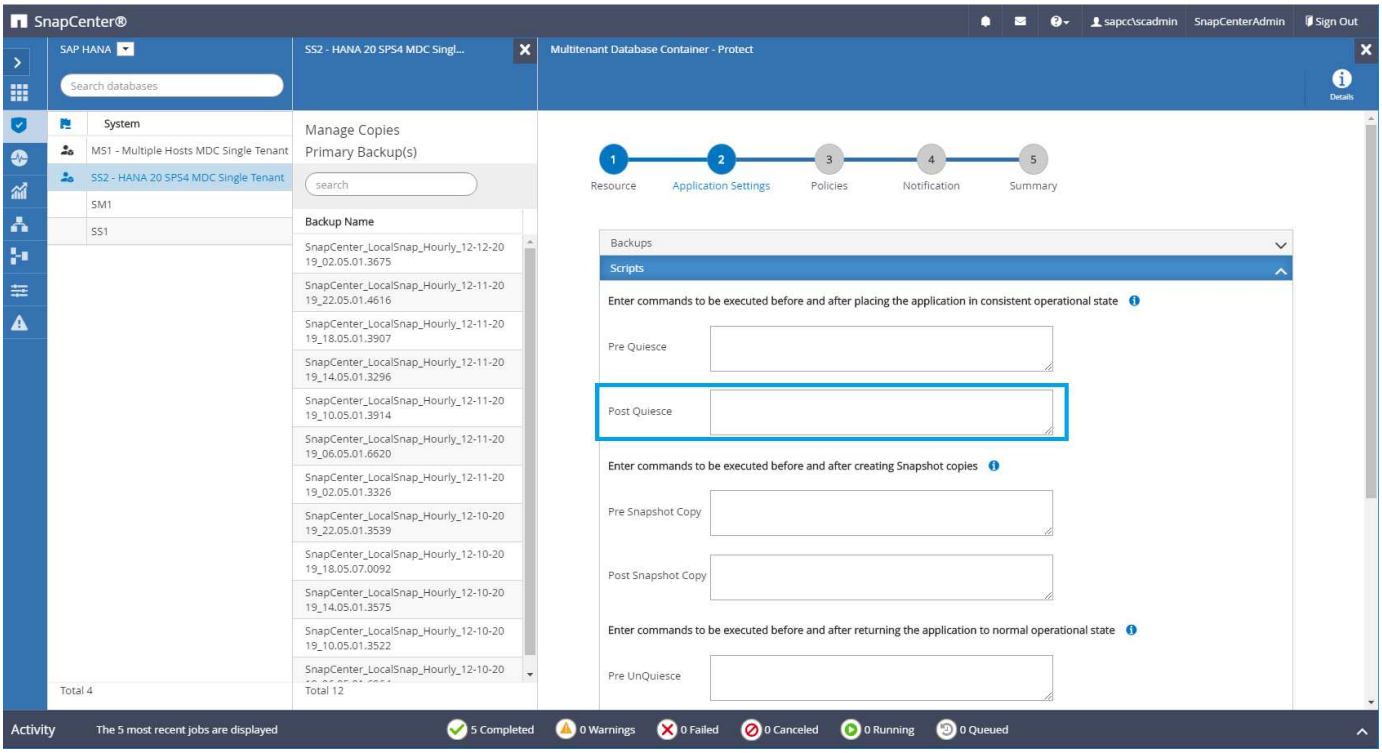
Se il server SnapCenter viene utilizzato come host plug-in HANA centrale, è possibile utilizzare un file batch. Il file batch deve avere il seguente contenuto:

```
@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.

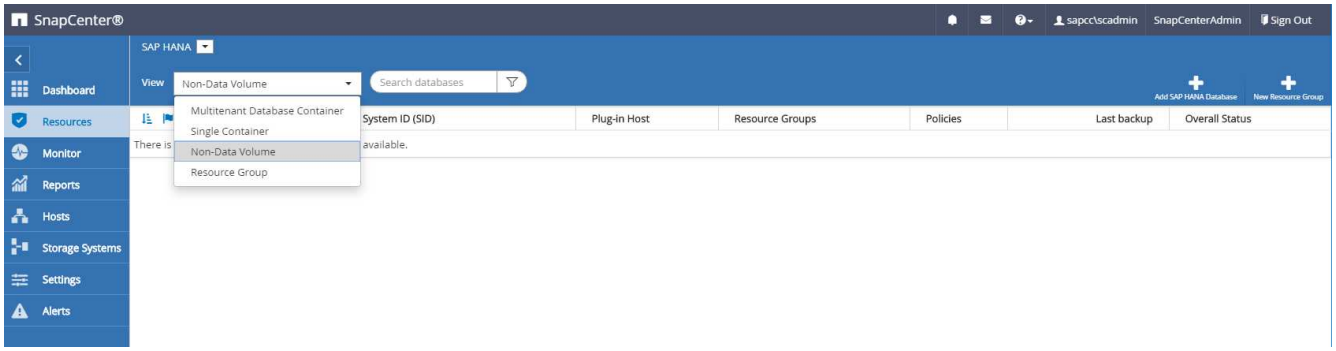
Per eseguire il ripristino da situazioni in cui devono essere ripristinati altri file non di dati, NetApp consiglia di sviluppare una strategia di backup aggiuntiva per i volumi non di dati per aumentare il backup del database SAP HANA. A seconda dei requisiti specifici, il backup dei volumi non dati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

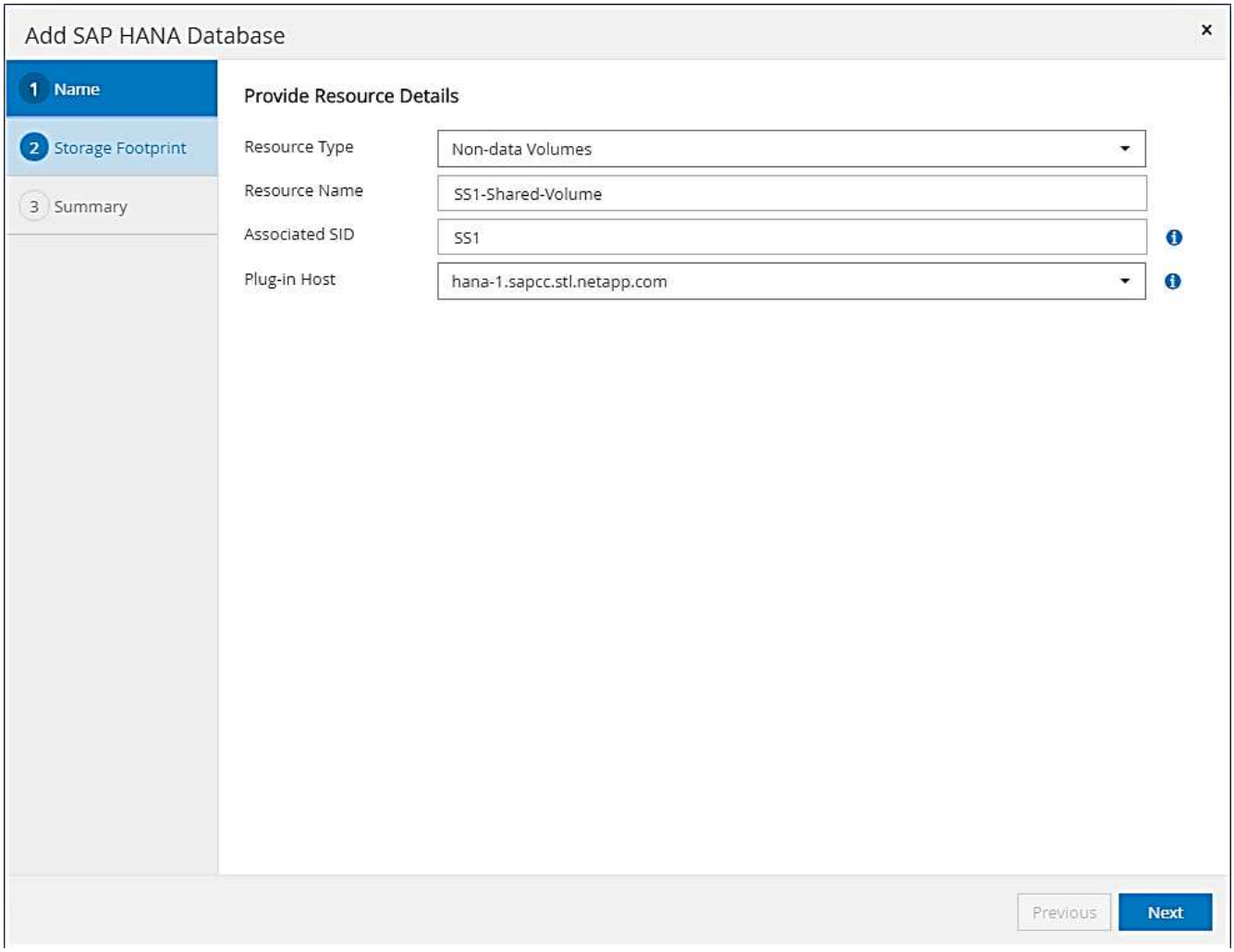
Configurazione di risorse non di volumi di dati

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

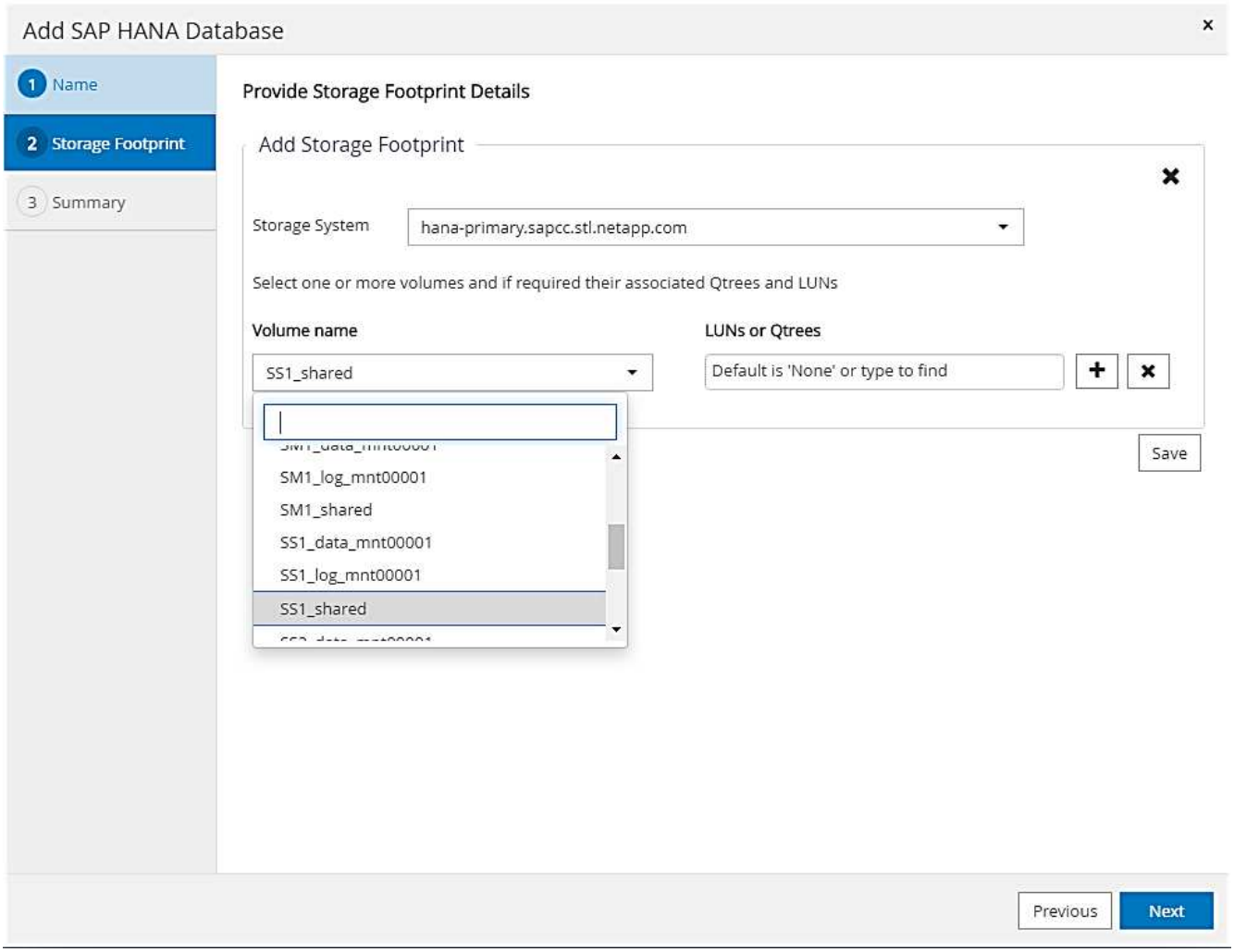
1. Dalla scheda Resource, selezionare non-Data-Volume e fare clic su Add SAP HANA Database (Aggiungi database SAP HANA).



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.



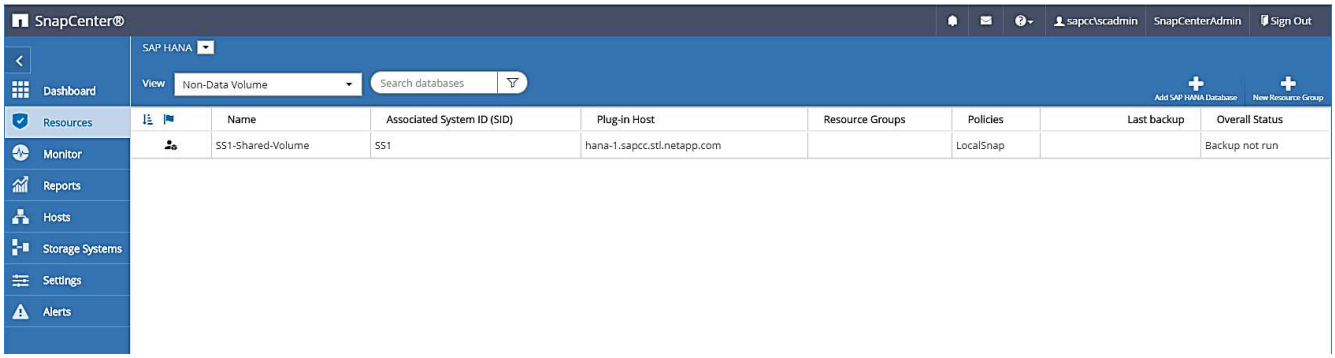
3. Aggiungere la SVM e il volume di storage come footprint dello storage, quindi fare clic su Next (Avanti).



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 dettagli 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.

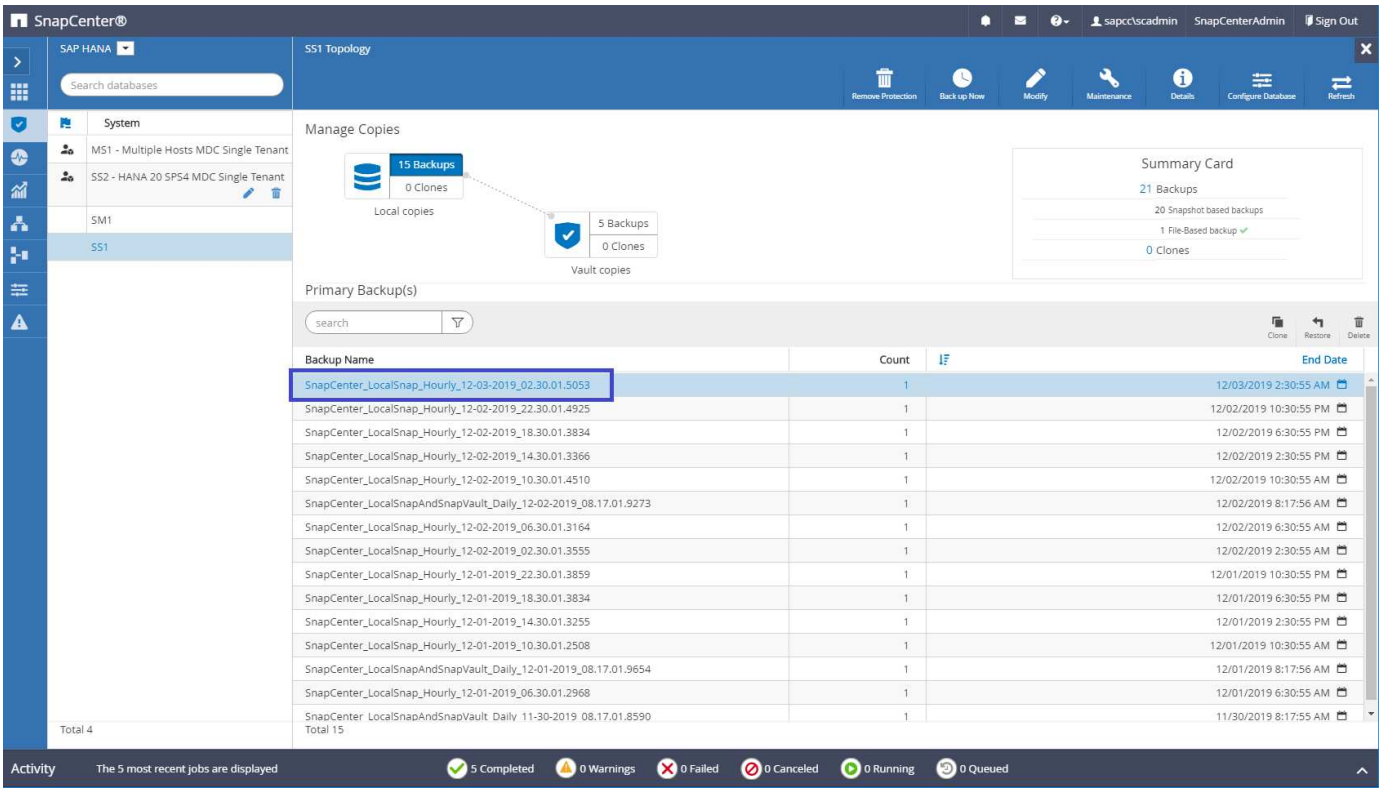
Backup del database

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.

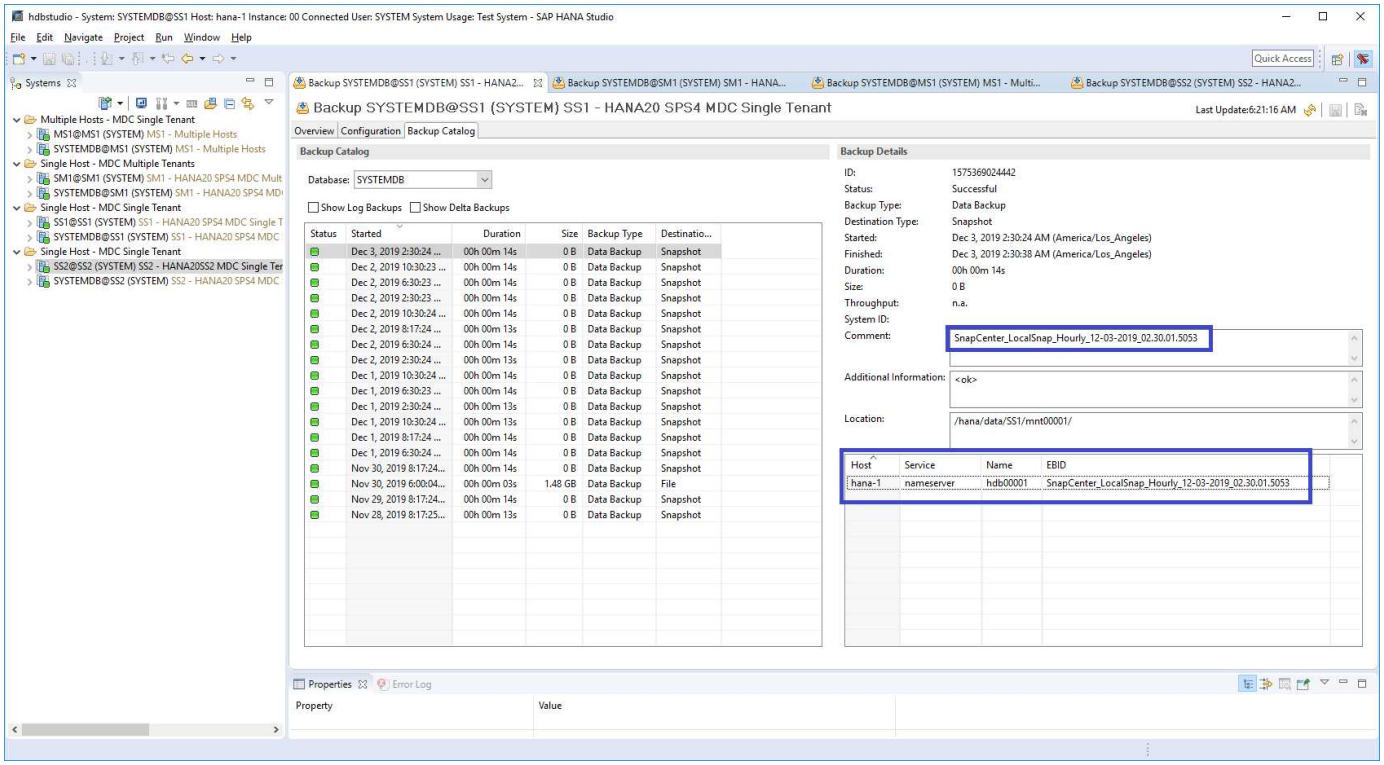


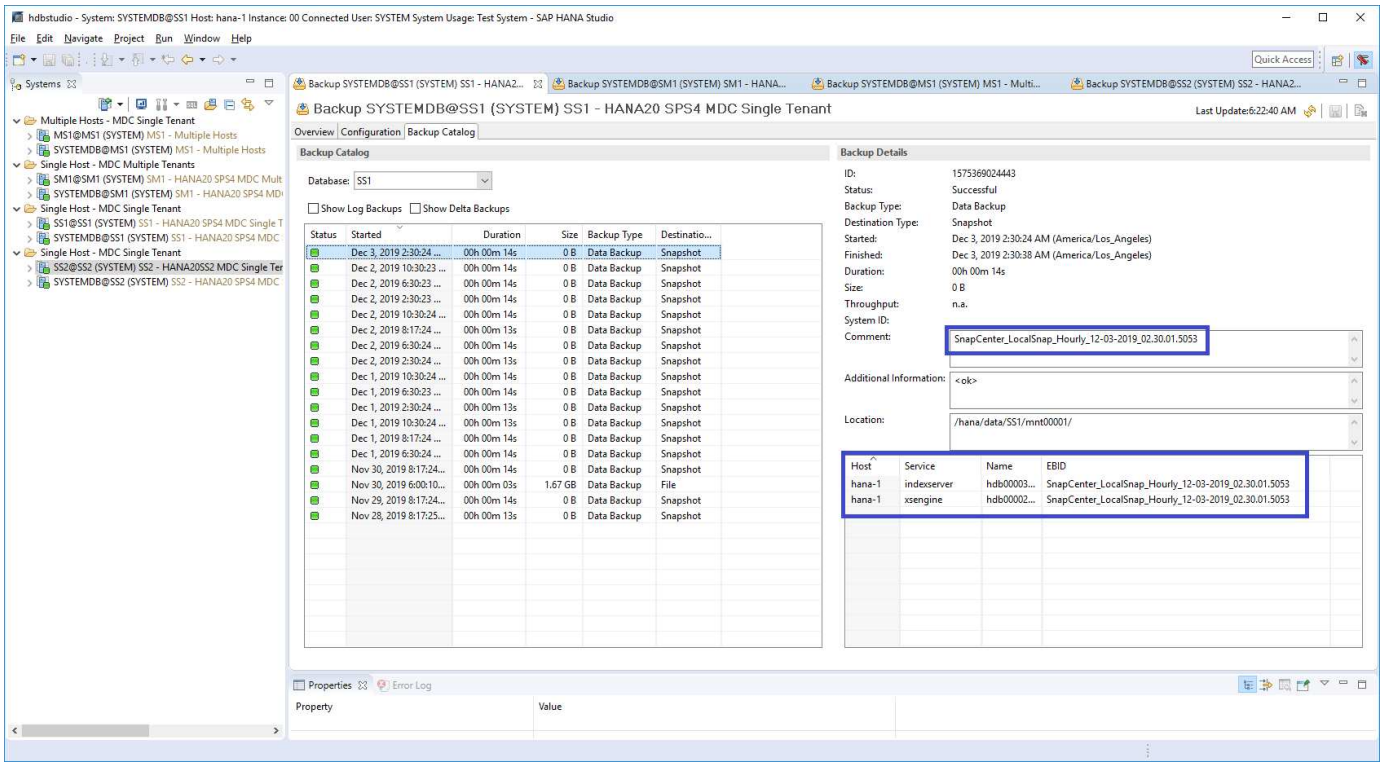
Quando si esegue un backup utilizzando le copie Snapshot dello storage per un sistema SAP HANA MDC, viene creata una copia Snapshot del volume di dati. Questo volume di dati contiene i dati del database di sistema e i dati di tutti i database tenant. Per riflettere questa architettura fisica, SAP HANA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

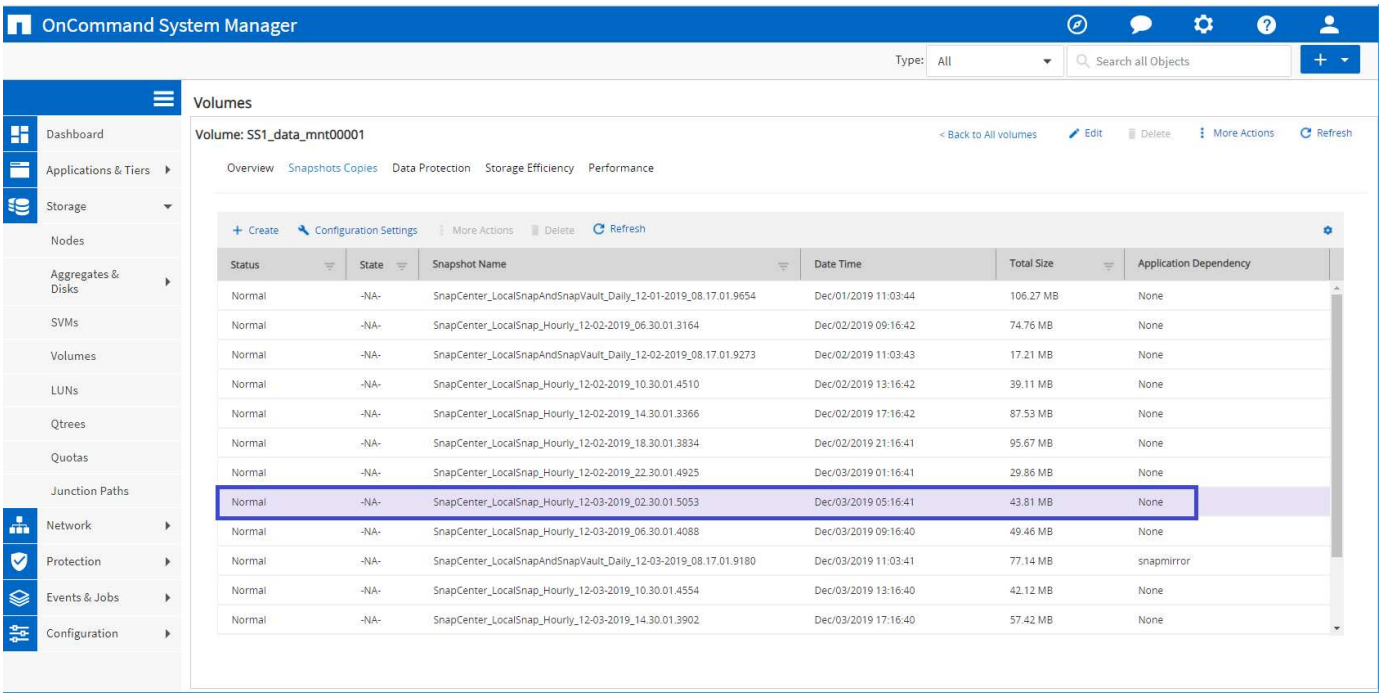




SnapCenter è consapevole solo dei propri backup. I backup aggiuntivi creati, ad esempio, con SAP HANA Studio, sono visibili nel catalogo SAP HANA, ma non in SnapCenter.

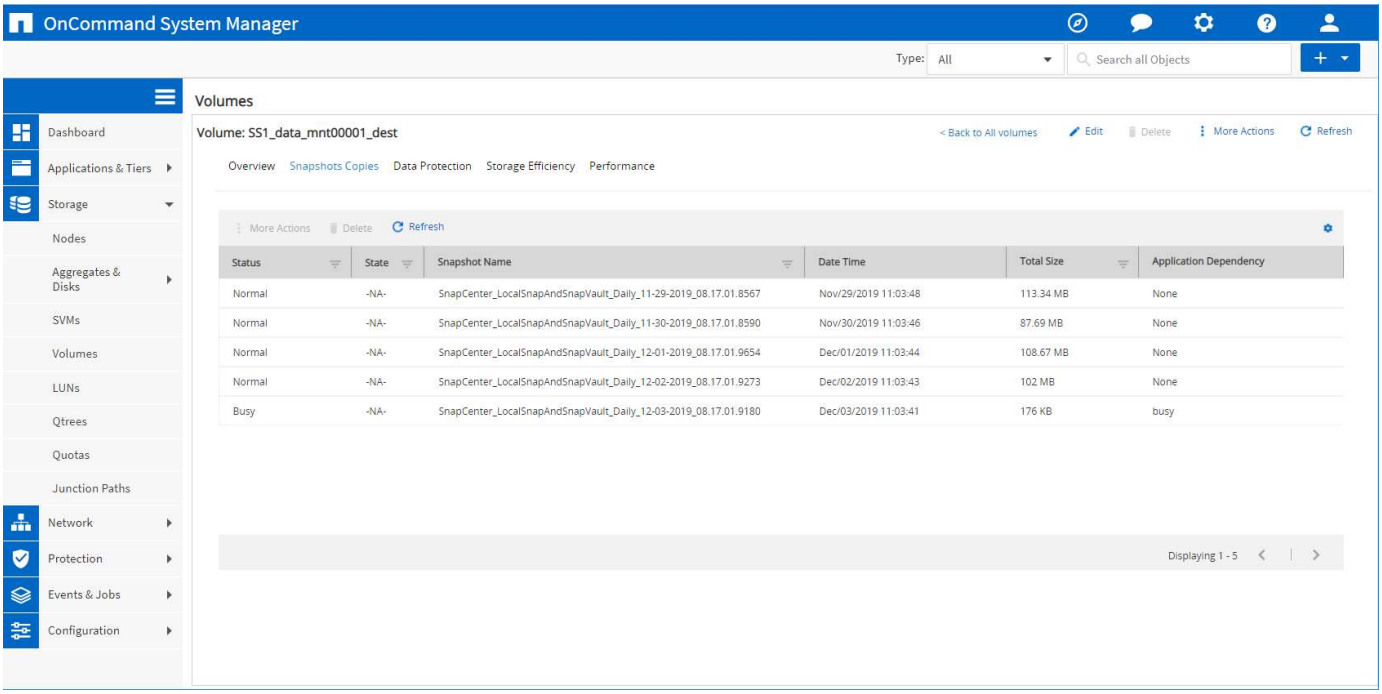
Identificazione dei backup SnapCenter sui sistemi storage

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.



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

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

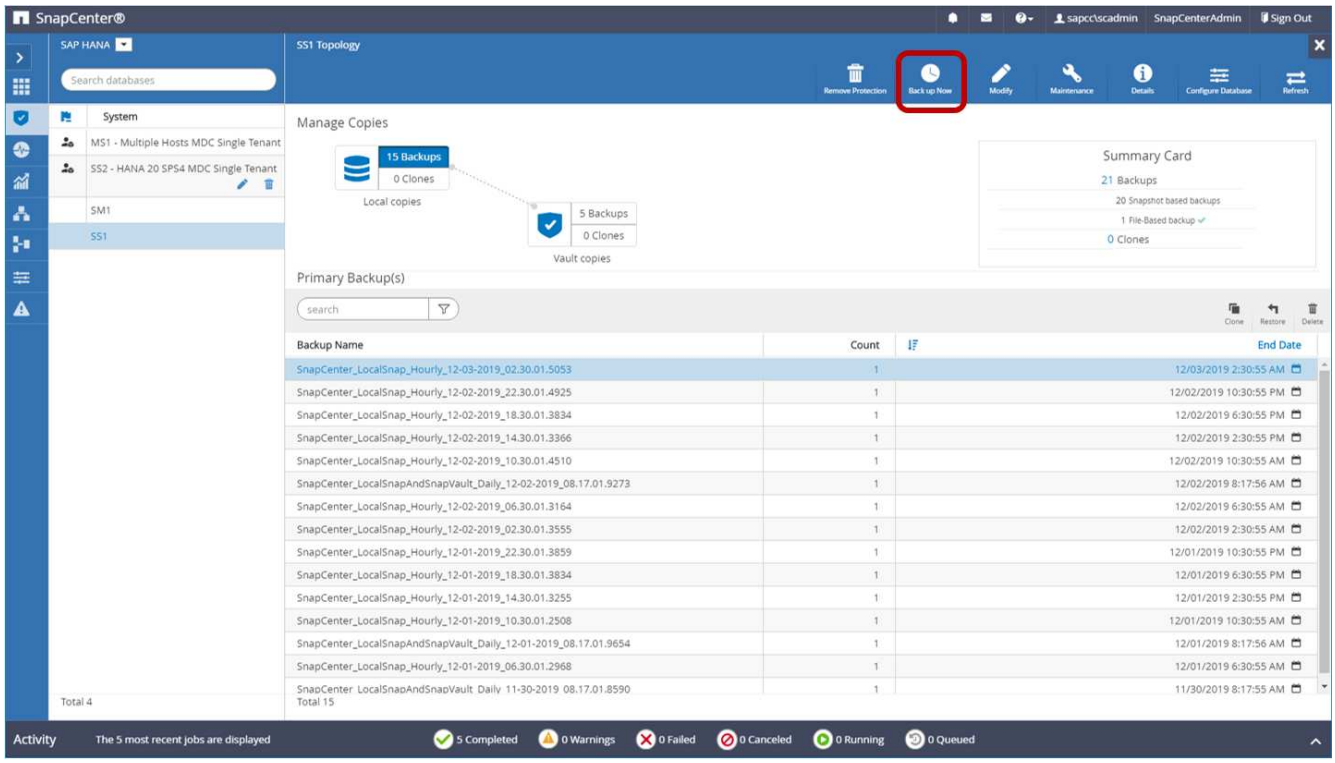


Status	State	Snapshot Name	Date Time	Total Size	Application Dependency
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_11-29-2019_08.17.01.8567	Nov/29/2019 11:03:48	113.34 MB	None
Normal	-NA-	SnapCenter_LocalSnapAndSnapVault_Daily_11-30-2019_08.17.01.8590	Nov/30/2019 11:03:46	87.69 MB	None
Normal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

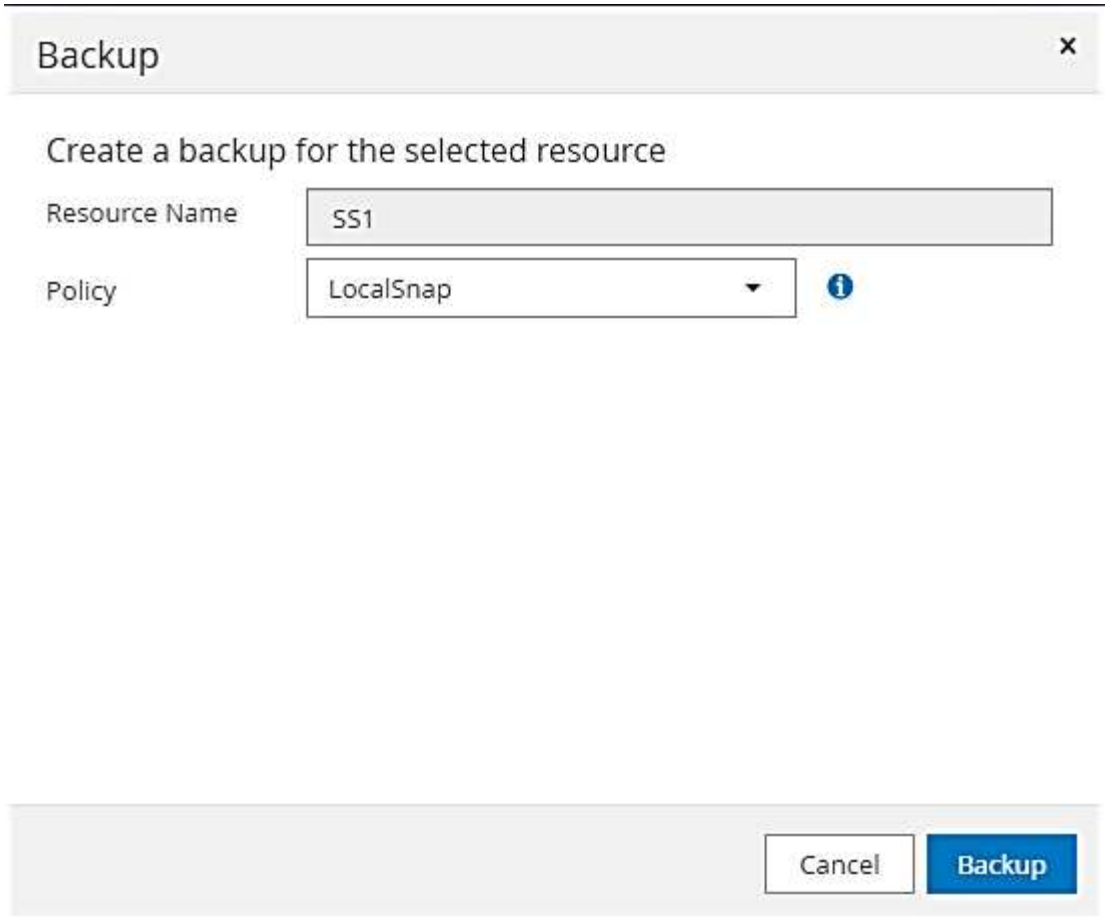
Backup del database on-demand sullo storage primario

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

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

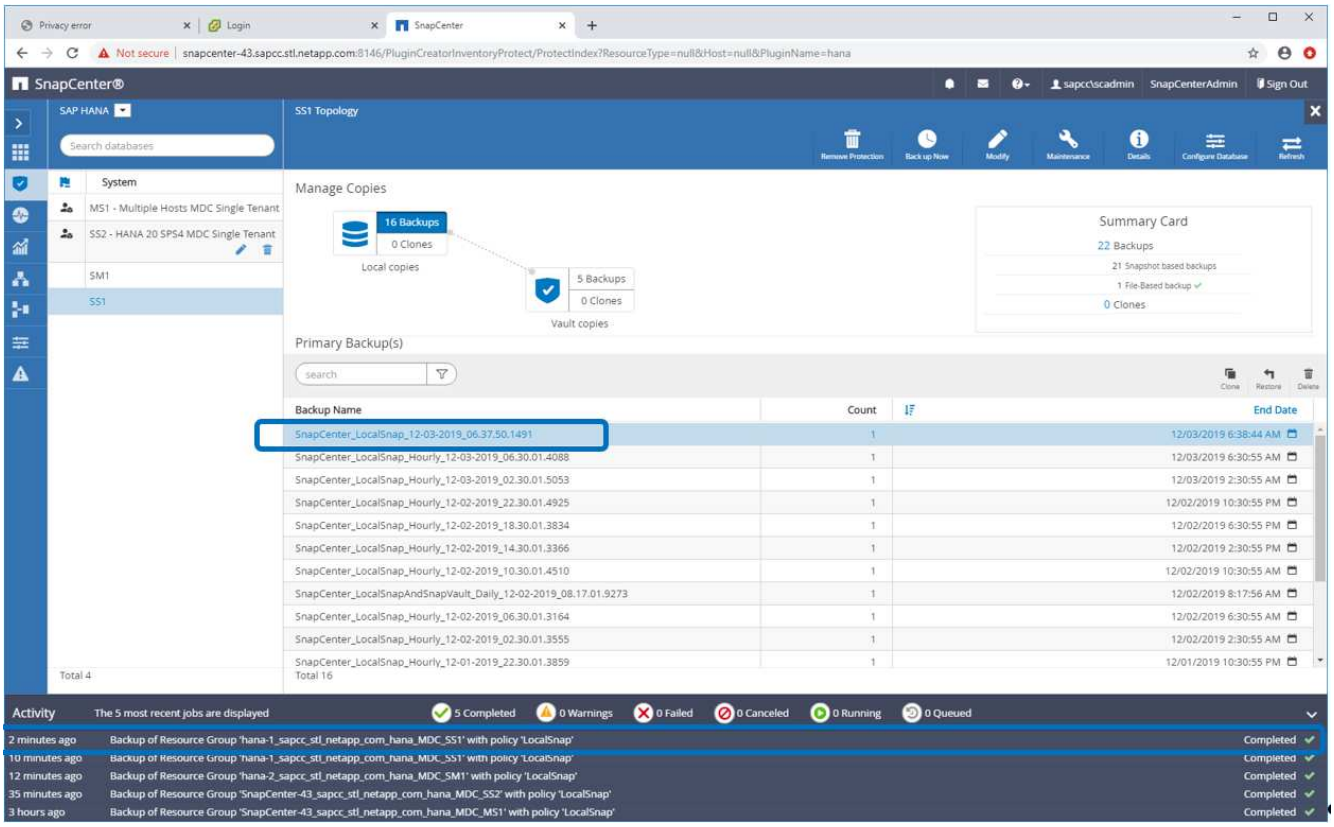


2. Nella riga superiore, selezionare l'icona Backup Now per avviare un backup on-demand. Dall'elenco a discesa, selezionare il criterio di backup `LocalSnap` Quindi fare clic su Backup per avviare il backup on-demand.

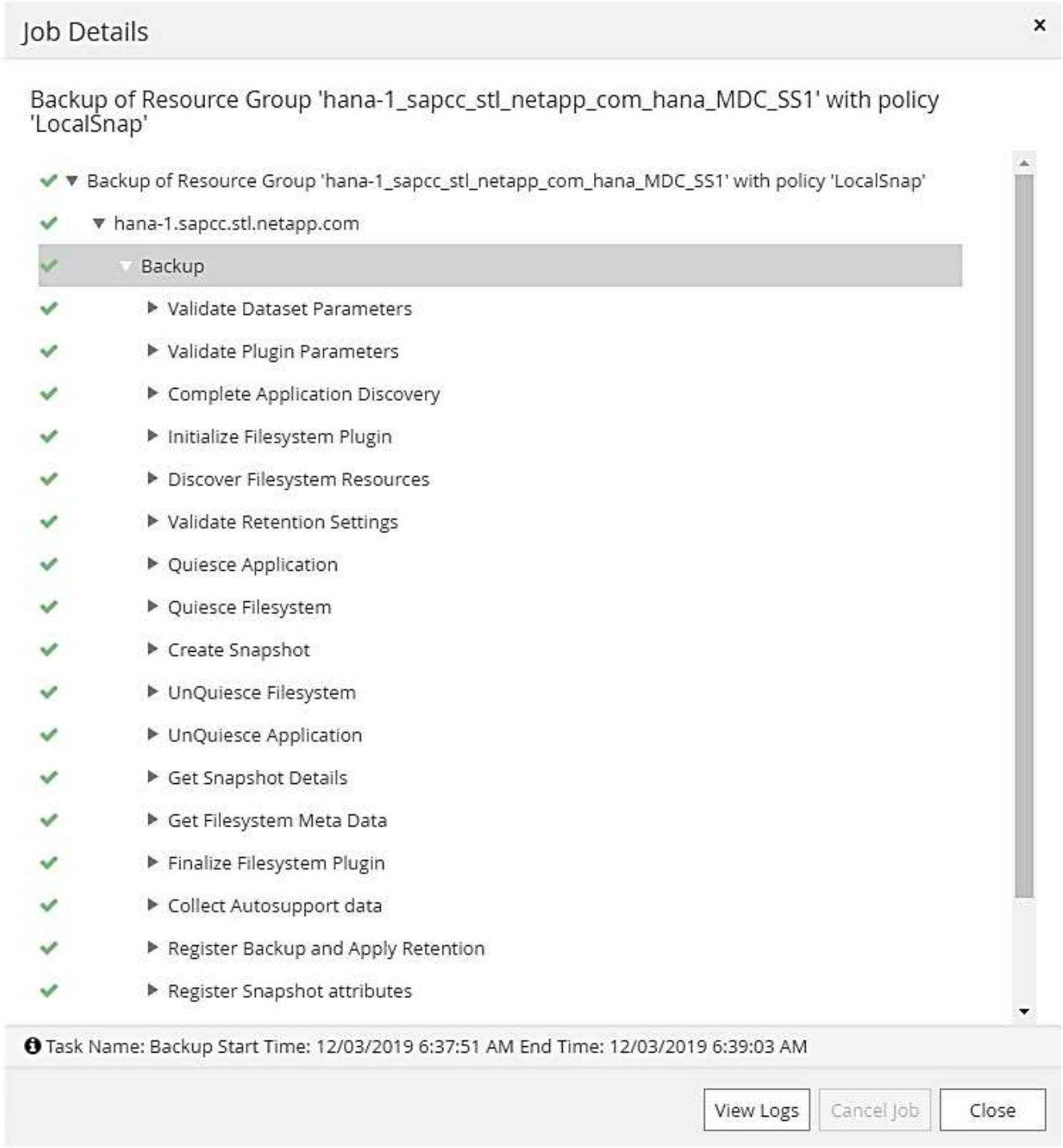


Viene avviato il processo di backup. Un registro dei cinque job precedenti viene visualizzato nell'area Activity (attività) sotto la vista della topologia. Al termine del backup, viene visualizzata una nuova voce nella vista della topologia. I nomi dei backup seguono la stessa convenzione di denominazione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

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



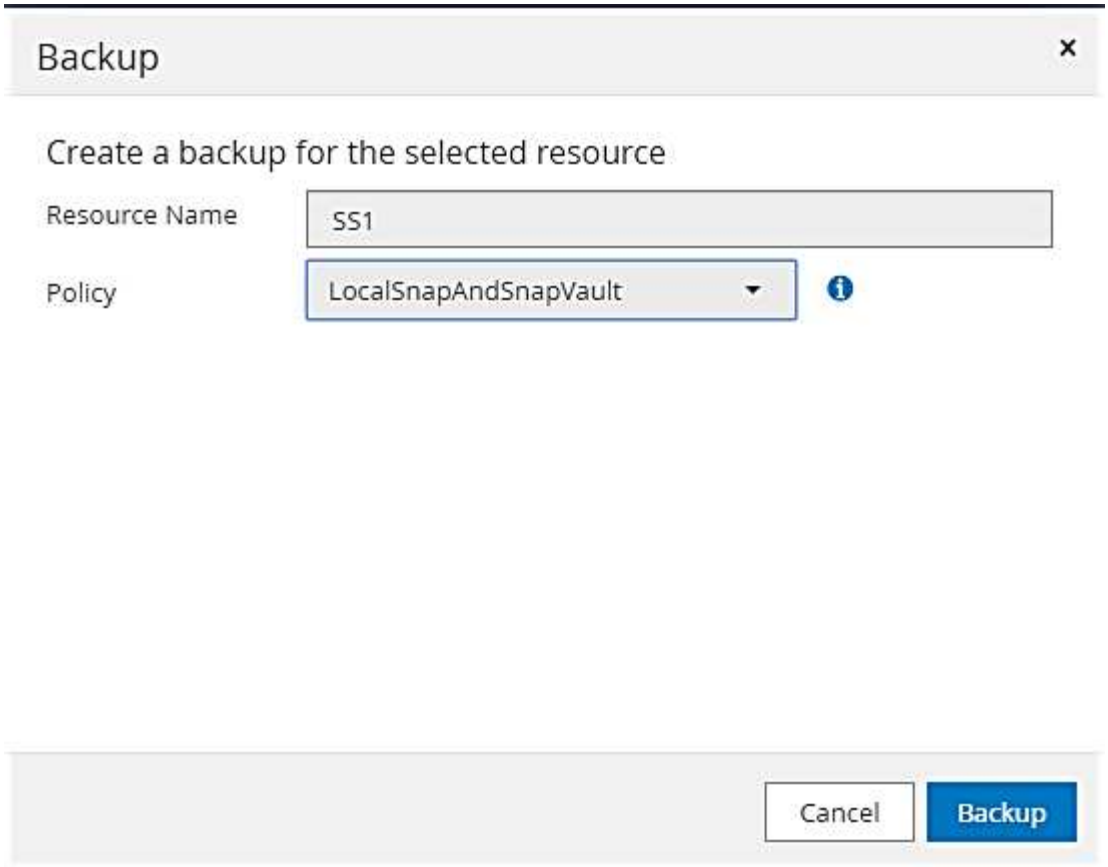
3. I dettagli della commessa vengono visualizzati facendo clic sulla riga dell'attività della commessa nell'area Activity (attività). È possibile aprire un registro dettagliato dei processi facendo clic su View Logs (Visualizza registri).



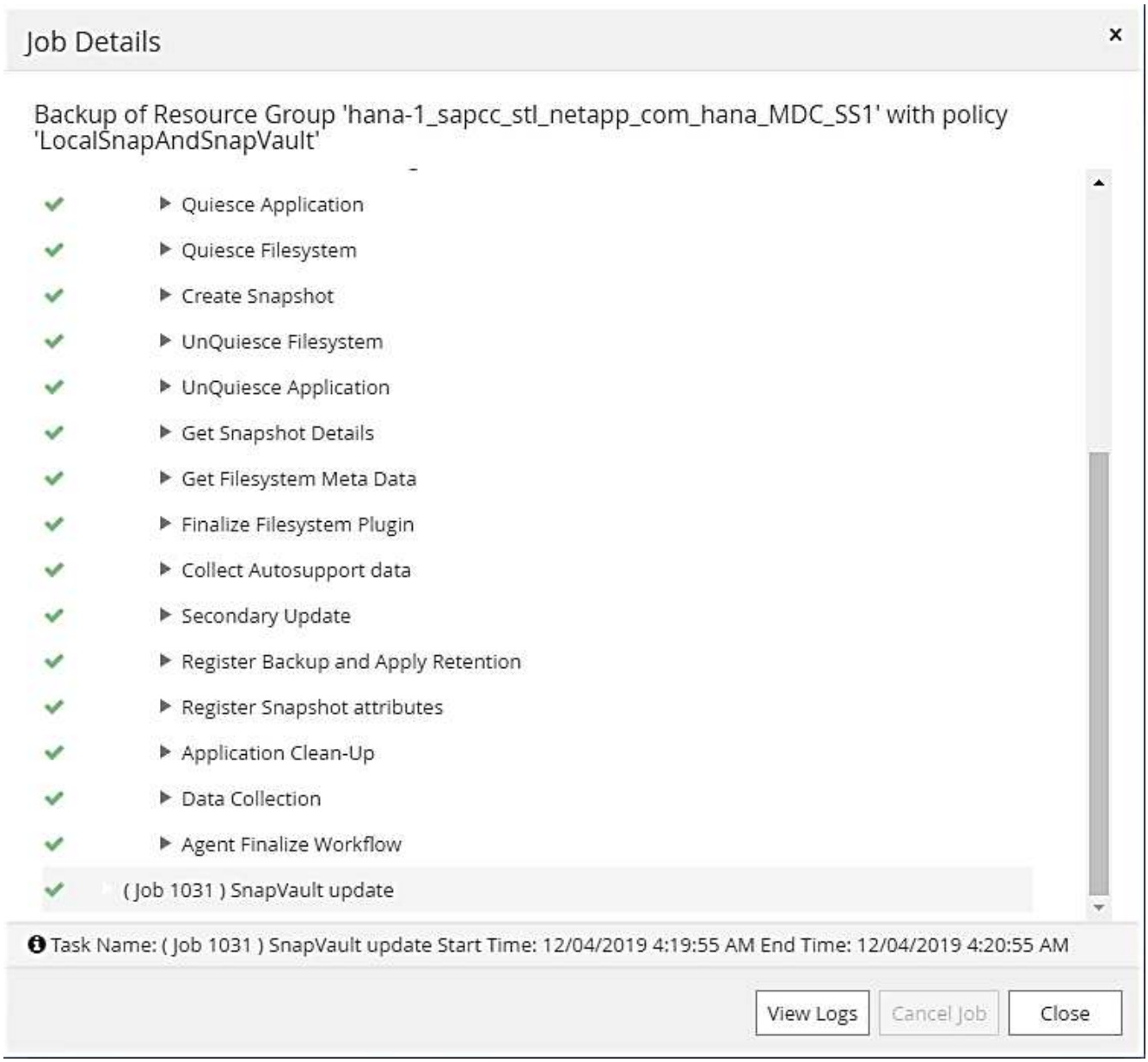
4. In SAP HANA Studio, il nuovo backup è visibile nel catalogo di backup. Lo stesso nome di backup in SnapCenter viene utilizzato anche nel campo comment e EBID nel catalogo di backup.

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.

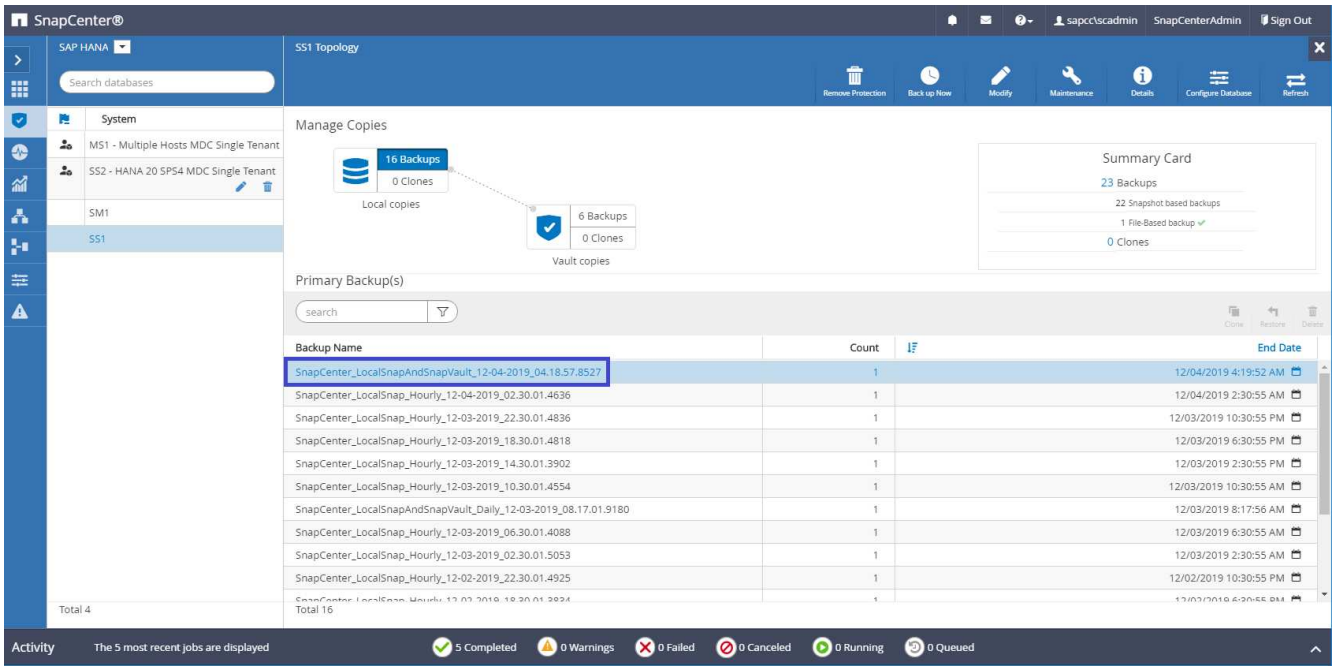


3. I dettagli della commessa vengono visualizzati facendo clic sulla riga dell'attività della commessa nell'area Activity (attività).

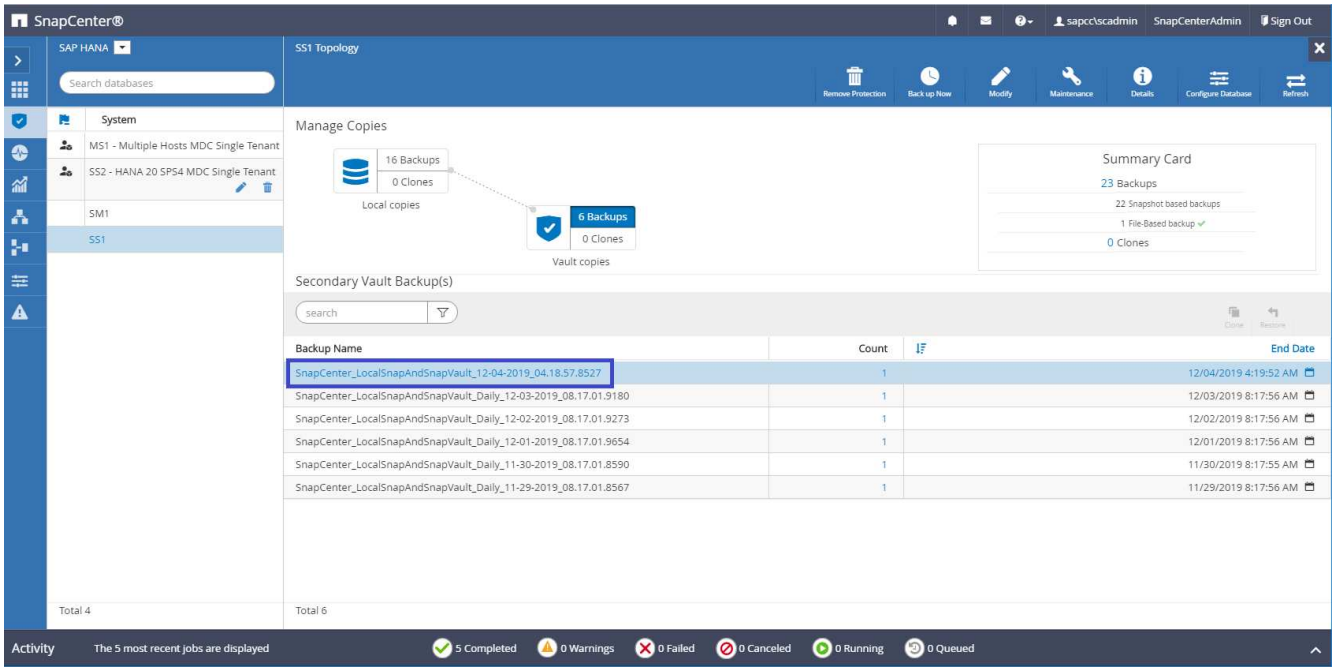


4. Al termine del backup, viene visualizzata una nuova voce nella vista della topologia. I nomi dei backup seguono la stessa convenzione di denominazione del nome dell'istantanea definita nella sezione ""Configurazione della protezione delle risorse"."

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.



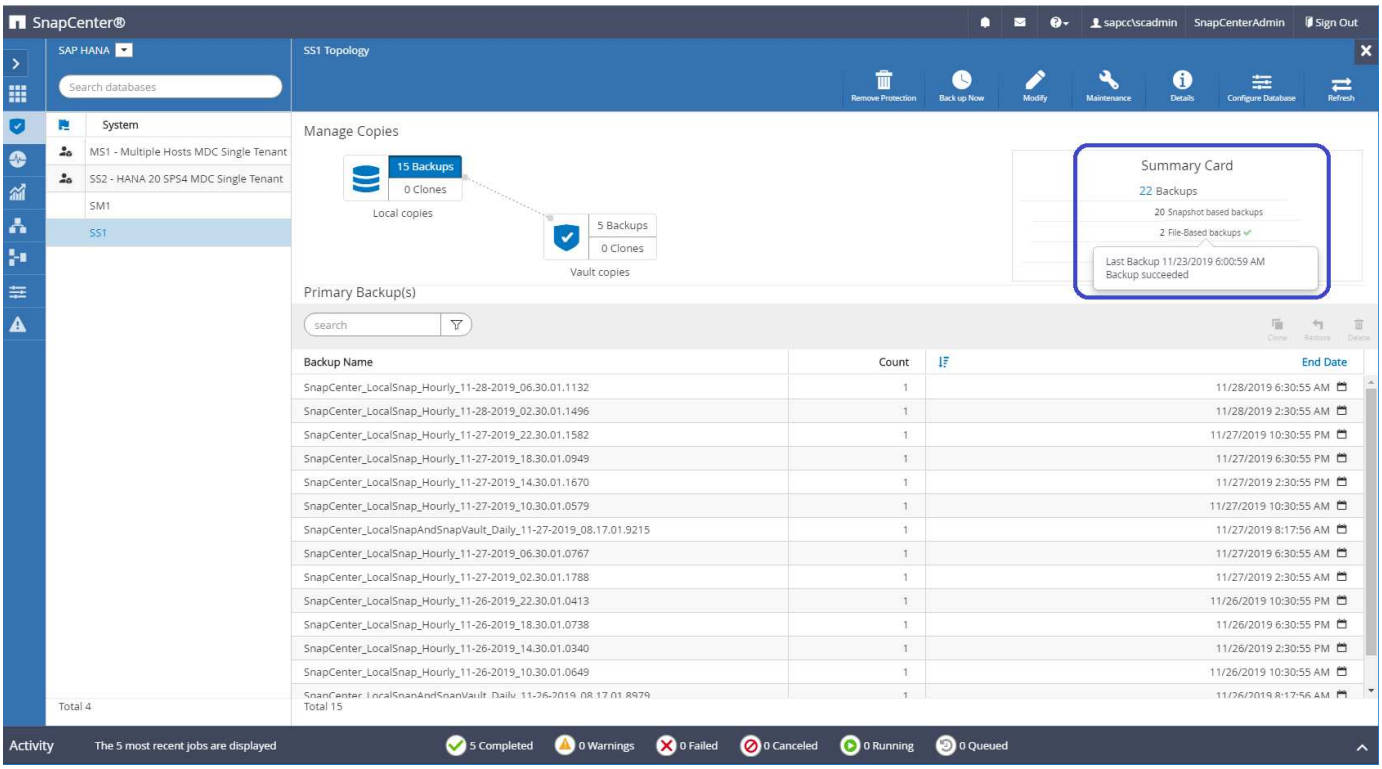
6. In SAP HANA Studio, il nuovo backup è visibile nel catalogo di backup. Lo stesso nome di backup in SnapCenter viene utilizzato anche nel campo comment e EBID nel catalogo di backup.

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

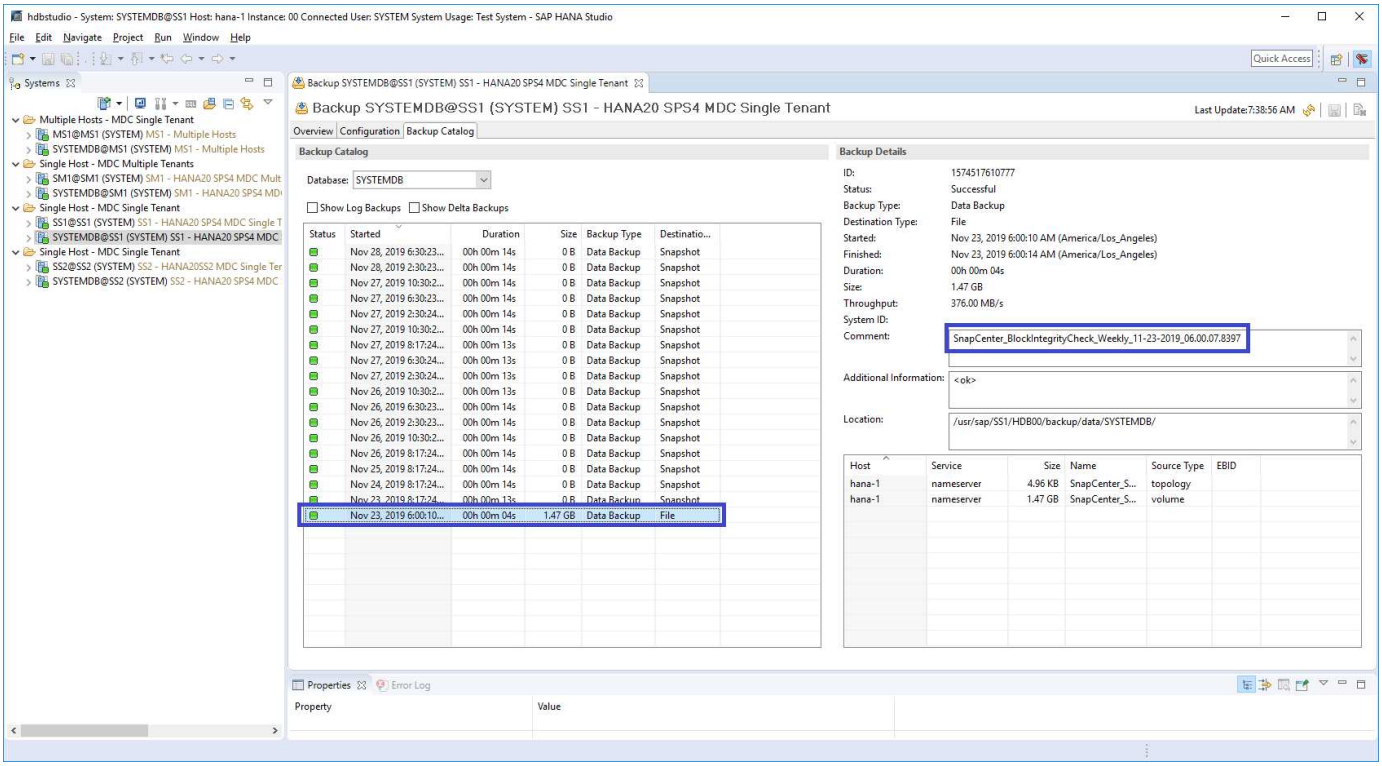
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"): y


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:

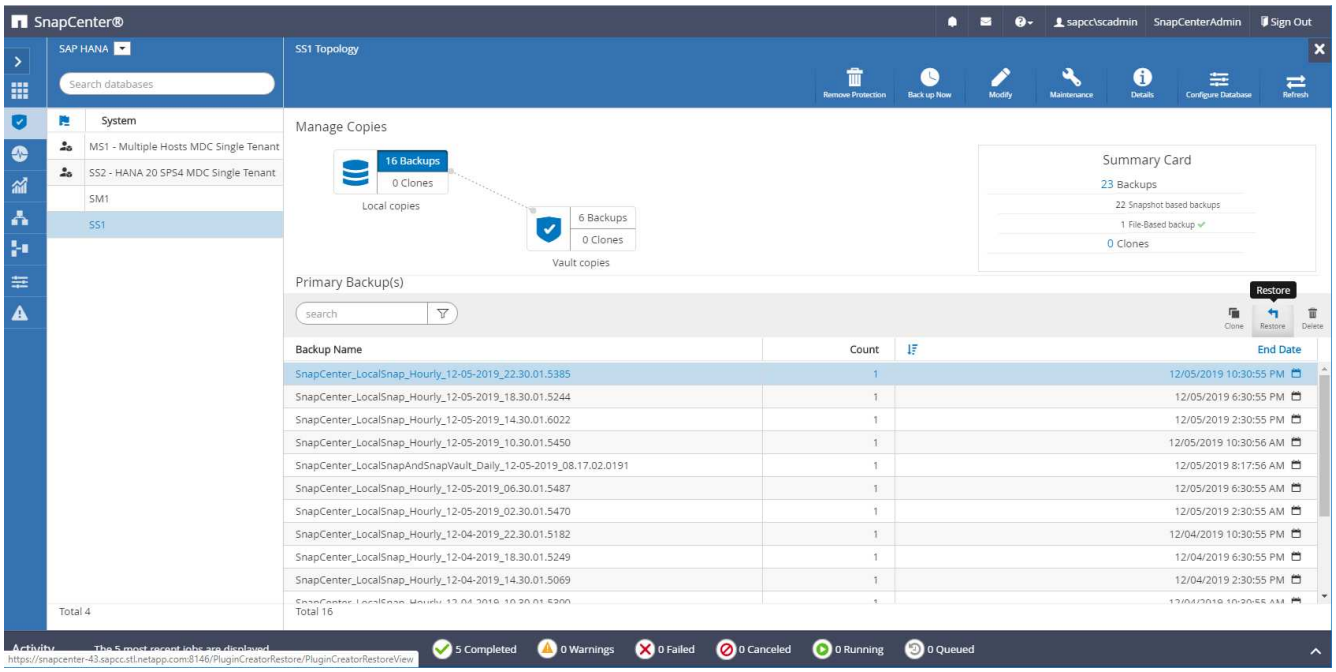
c. Avvia il database HANA.

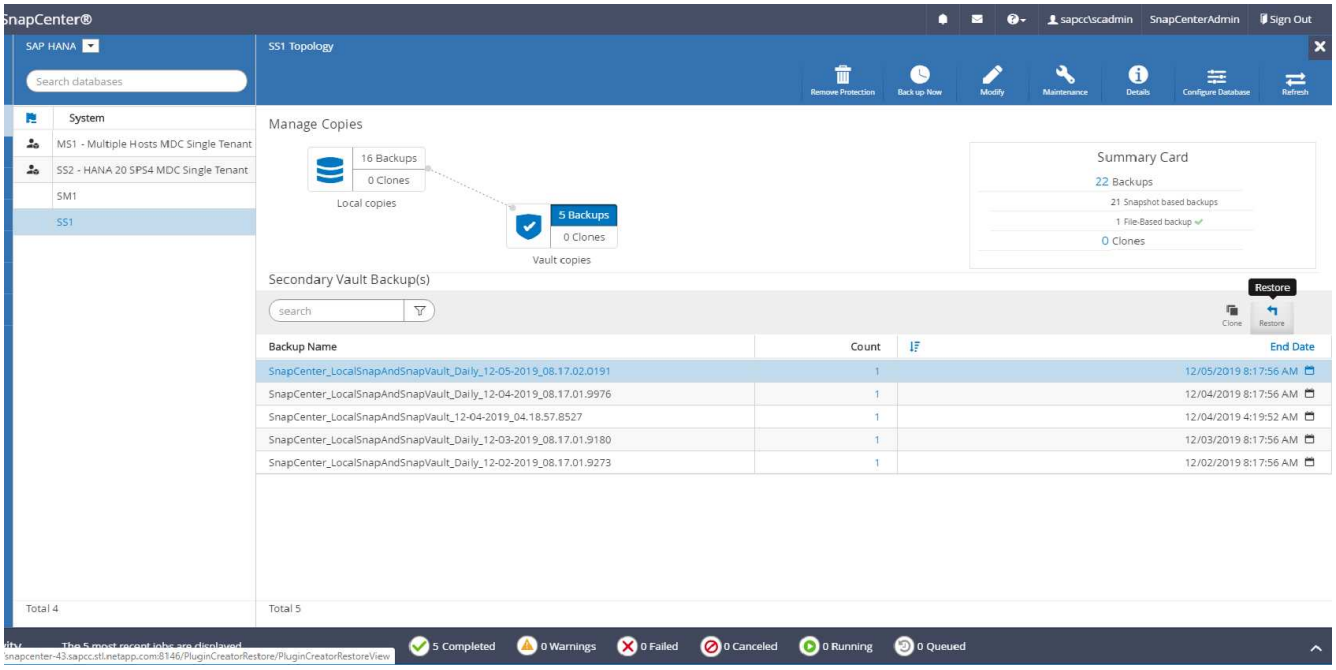
Se si seleziona No Recovery (Nessun ripristino), SnapCenter viene chiuso e l'operazione di ripristino del sistema e del database tenant deve essere eseguita manualmente.

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.



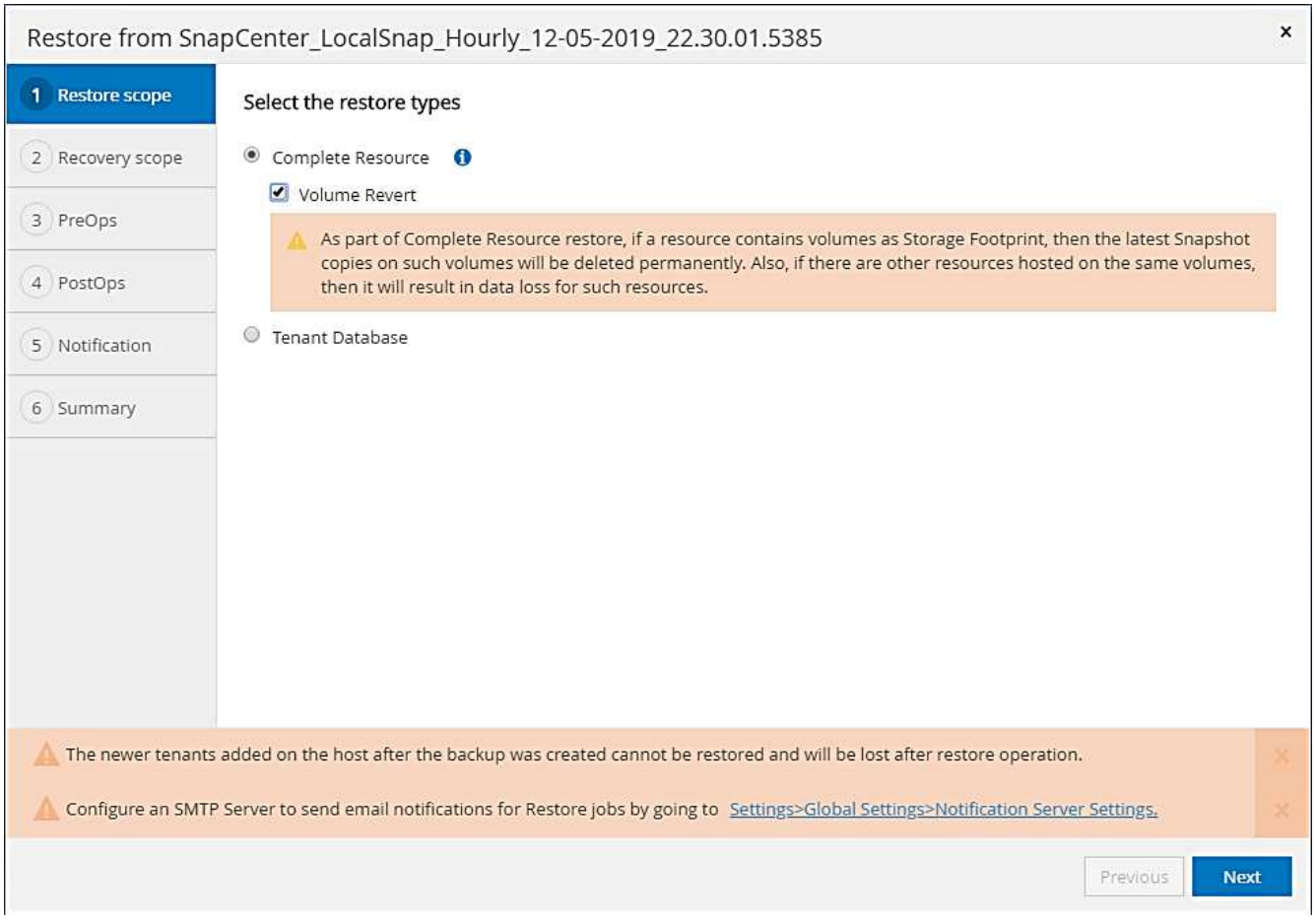


2. Selezionare l'ambito e il tipo di ripristino.

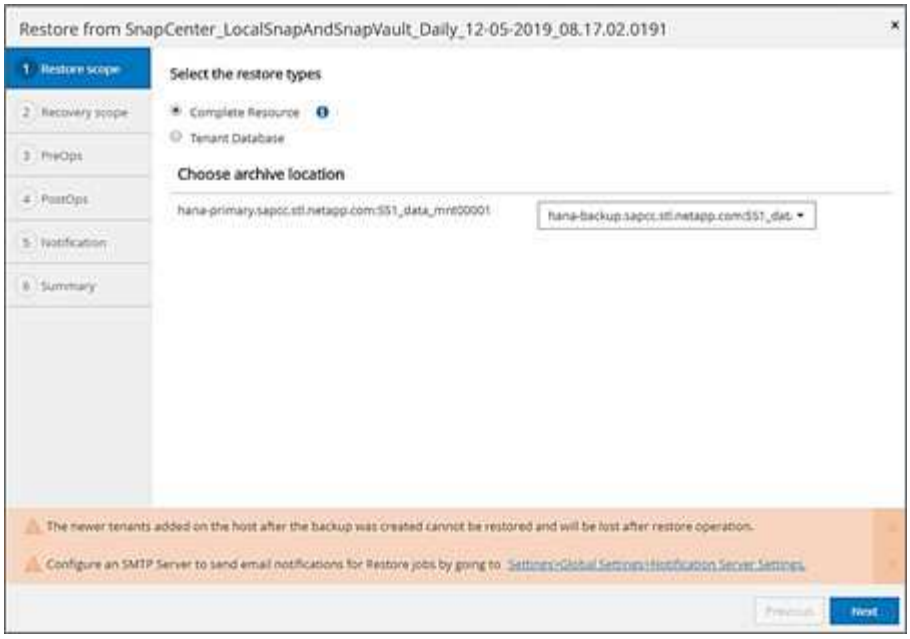
   Le tre schermate seguenti mostrano le opzioni di ripristino per il ripristino da primario con NFS, il ripristino da secondario con NFS e il ripristino da primario con SAN Fibre Channel.

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

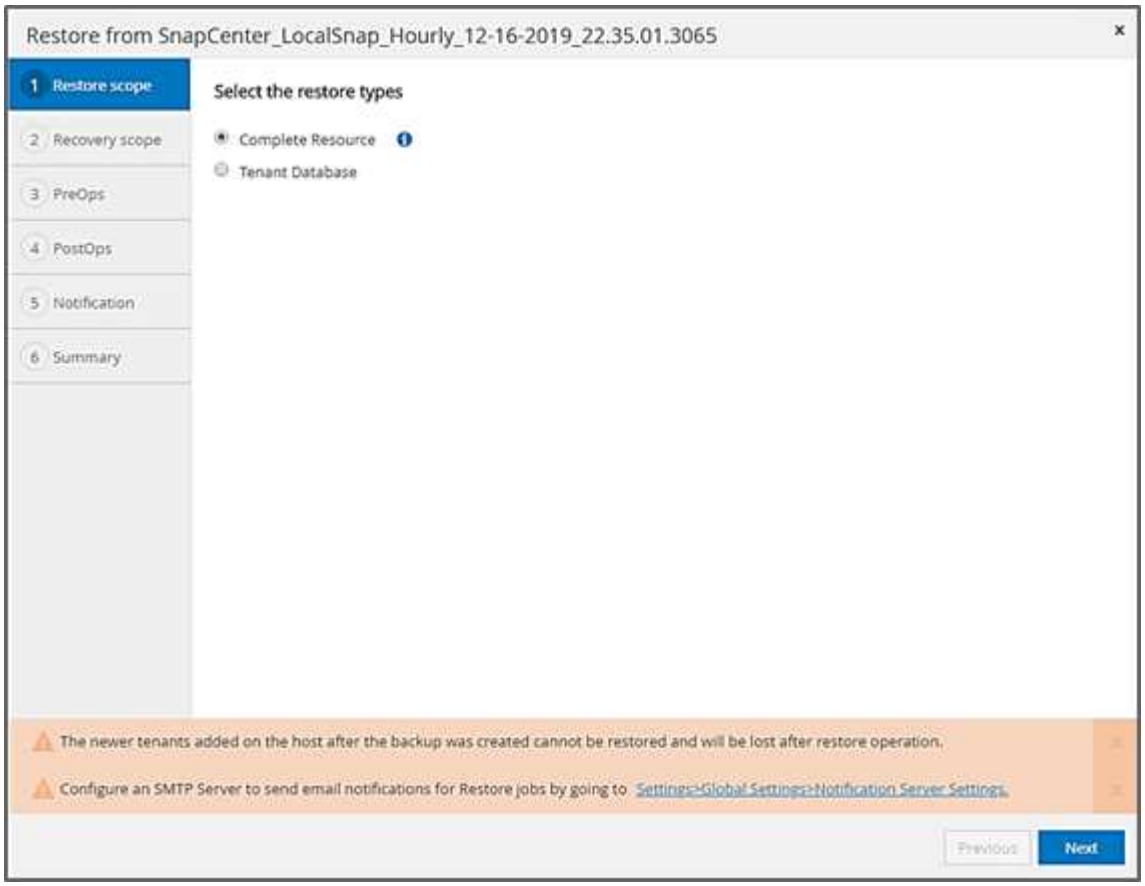
   > L'opzione di ripristino del volume è disponibile solo per le operazioni di ripristino da primarie con NFS.



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

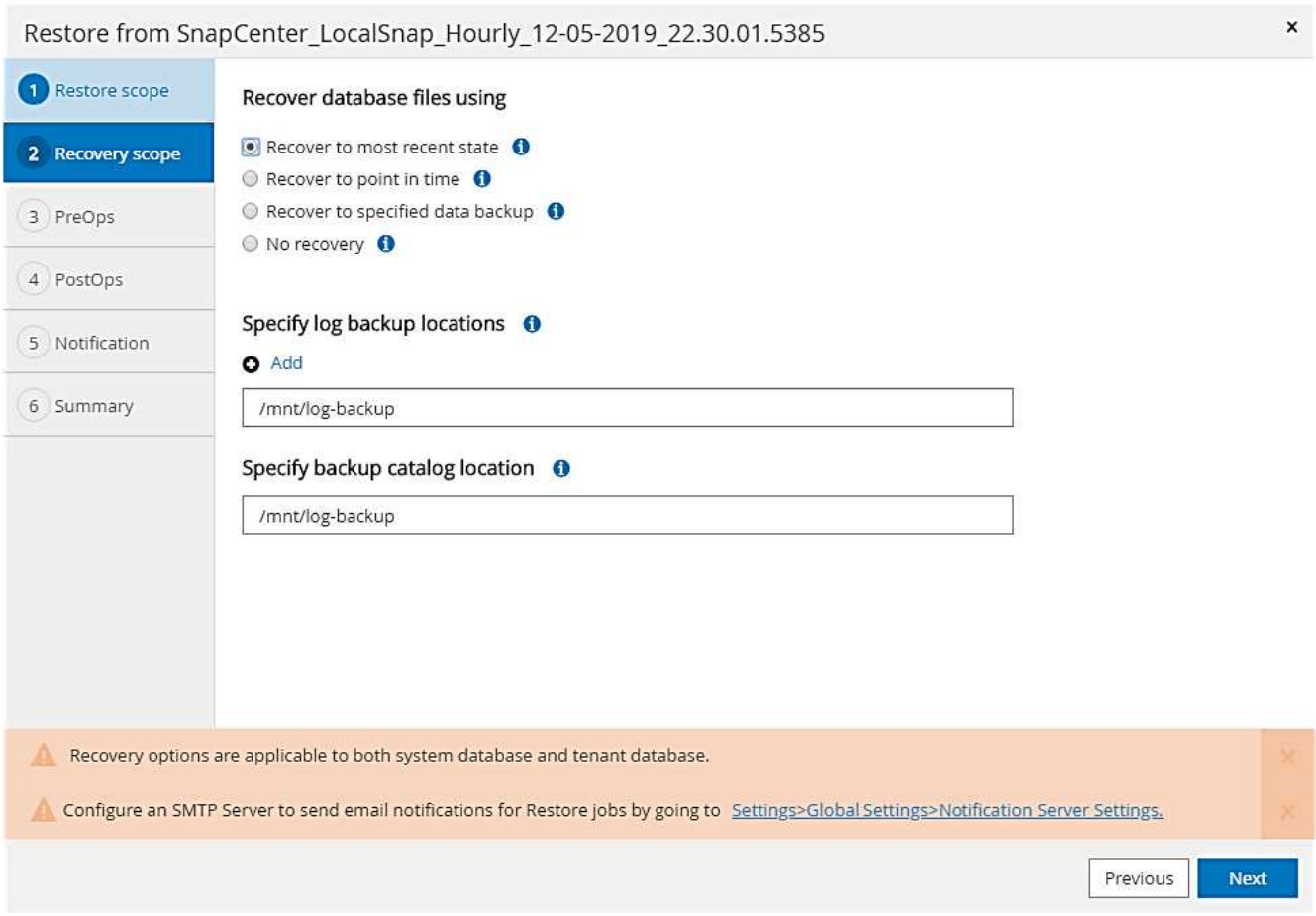


Opzioni del tipo di ripristino per il ripristino dallo storage primario con SAN Fibre Channel.

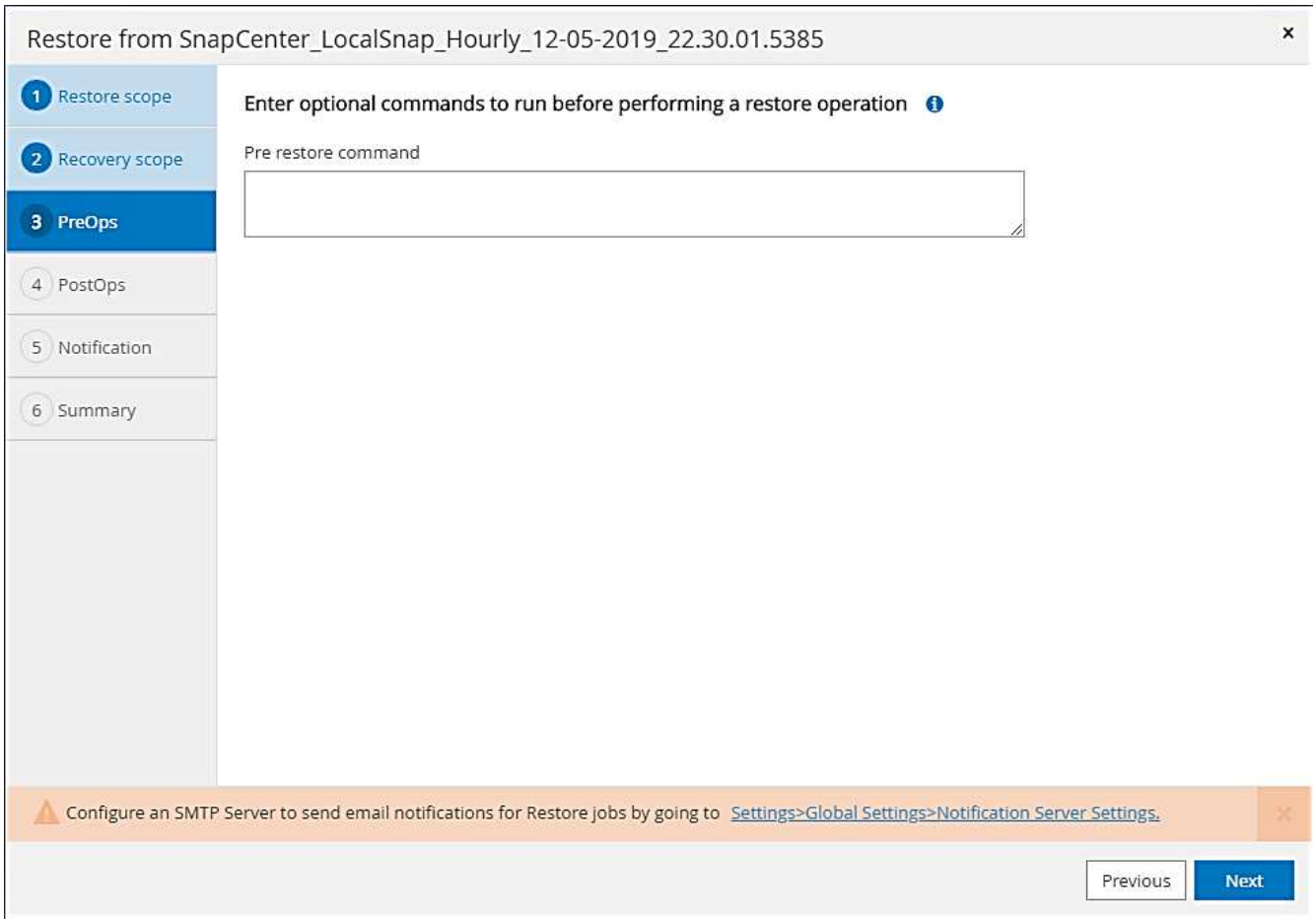


3. Selezionare Recovery Scope (ambito ripristino) e specificare la posizione per il backup del registro e del catalogo.

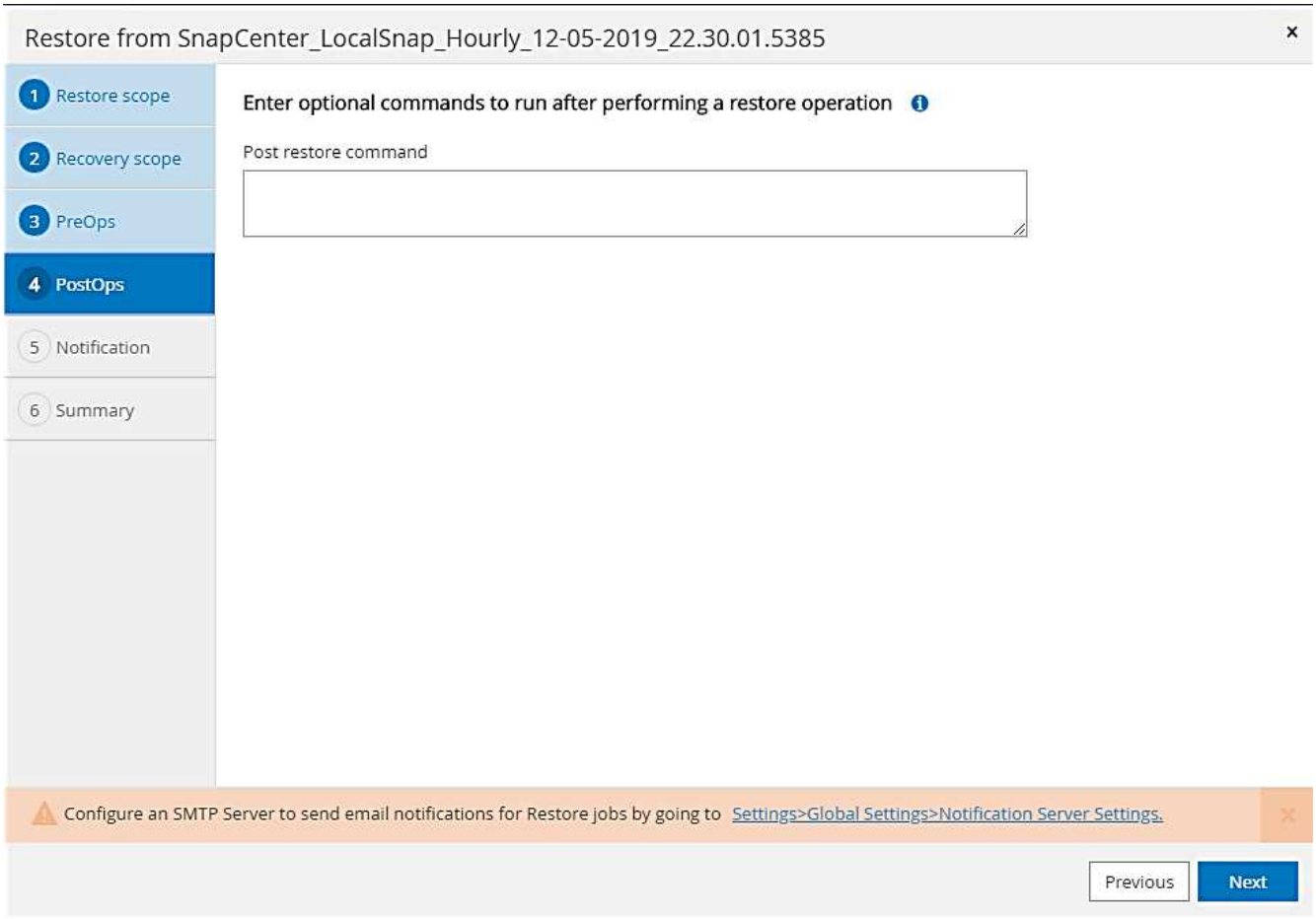
SnapCenter utilizza il percorso predefinito o i percorsi modificati nel file HANA global.ini per prepopolare le posizioni di backup del registro e del catalogo.



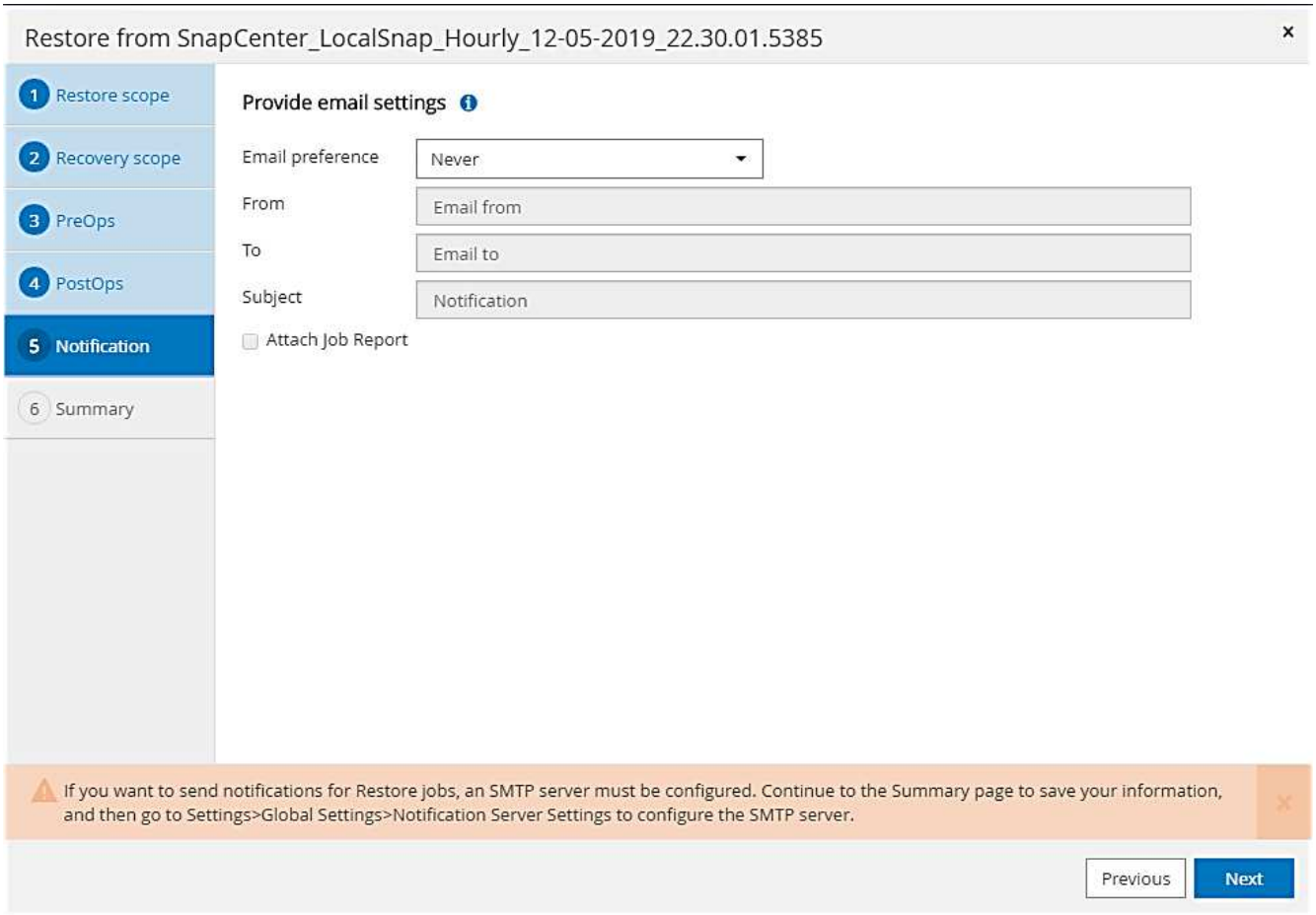
4. Immettere i comandi opzionali di prerestore.



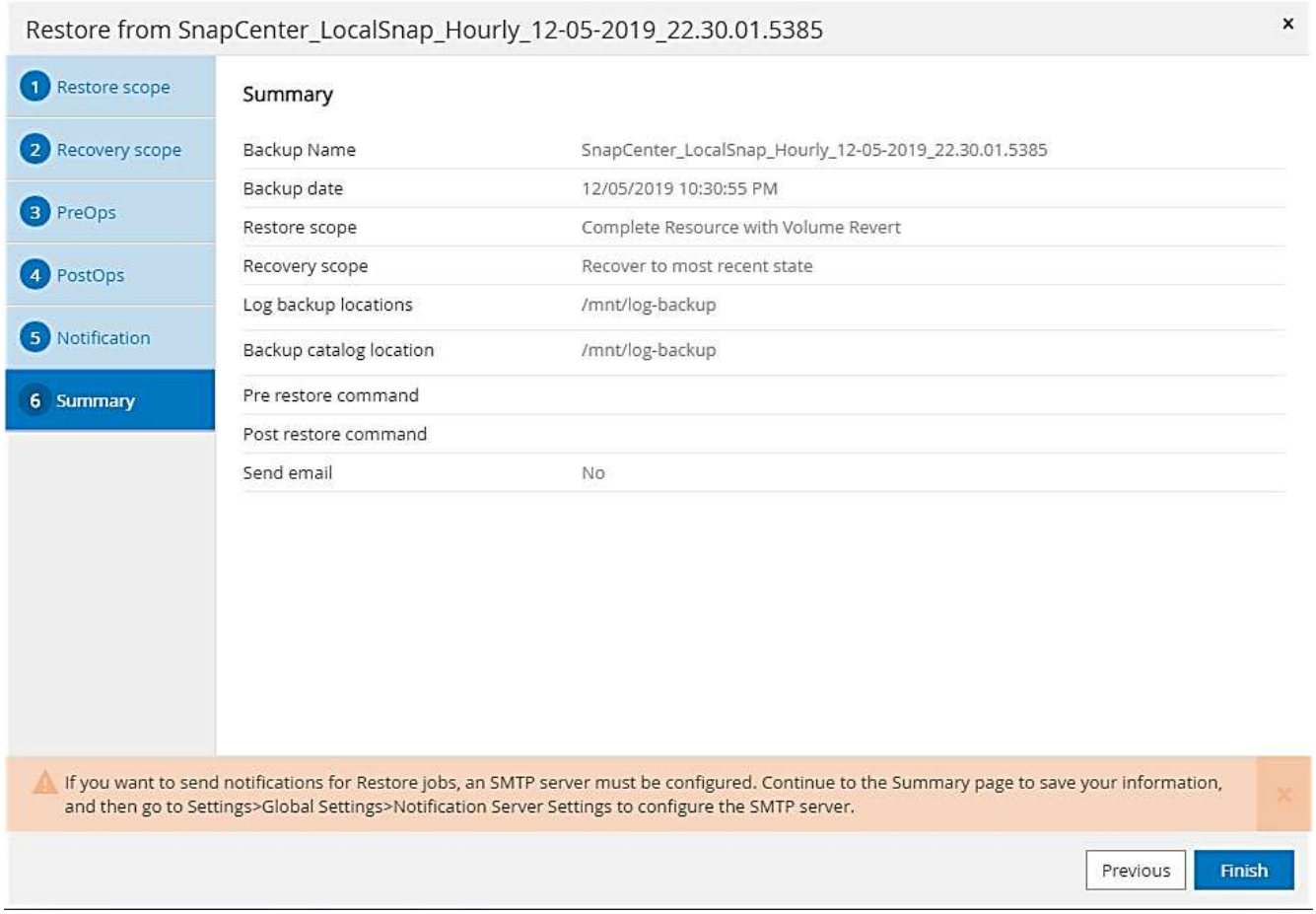
5. Immettere i comandi post-ripristino opzionali.



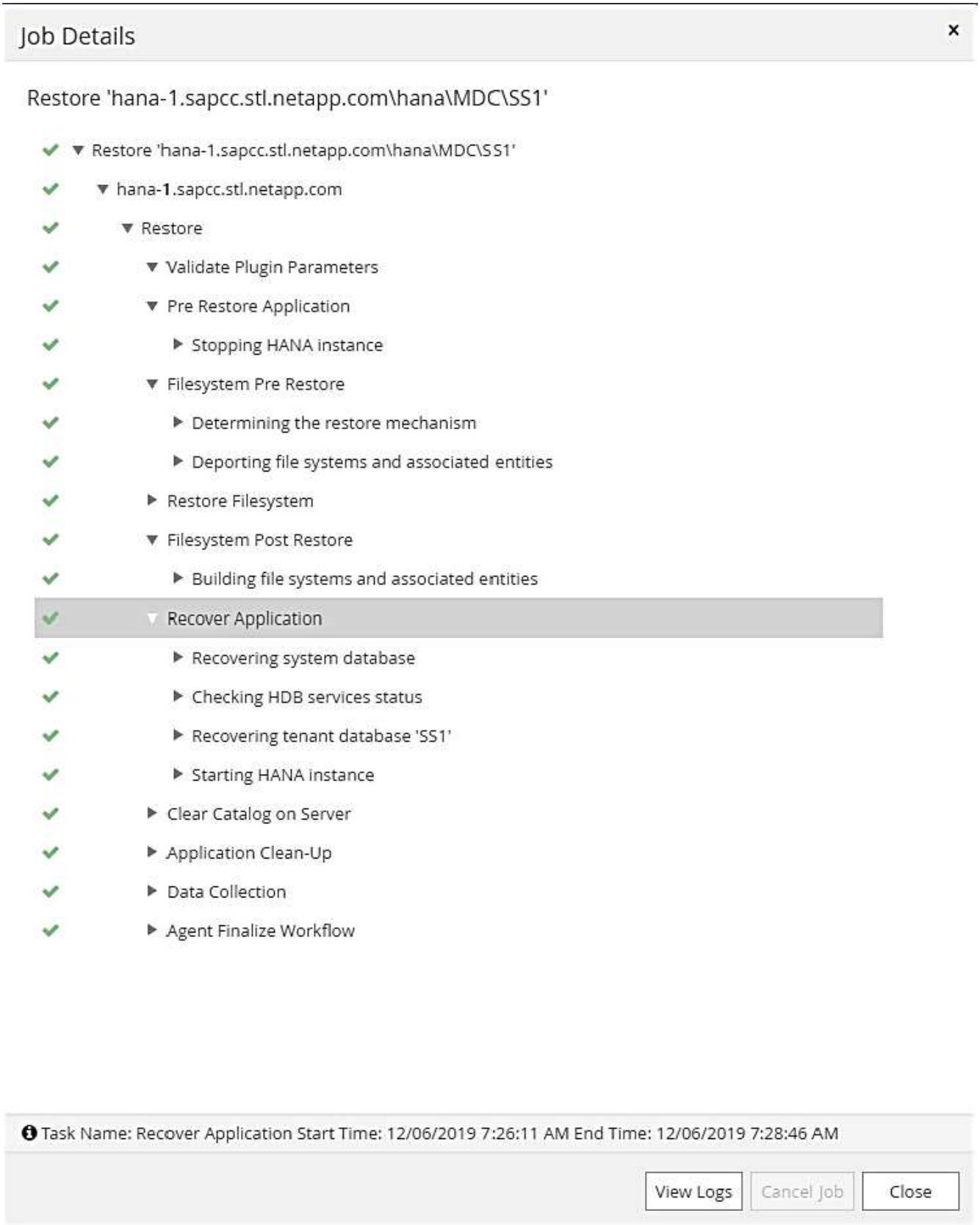
6. Immettere le impostazioni e-mail opzionali.



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:

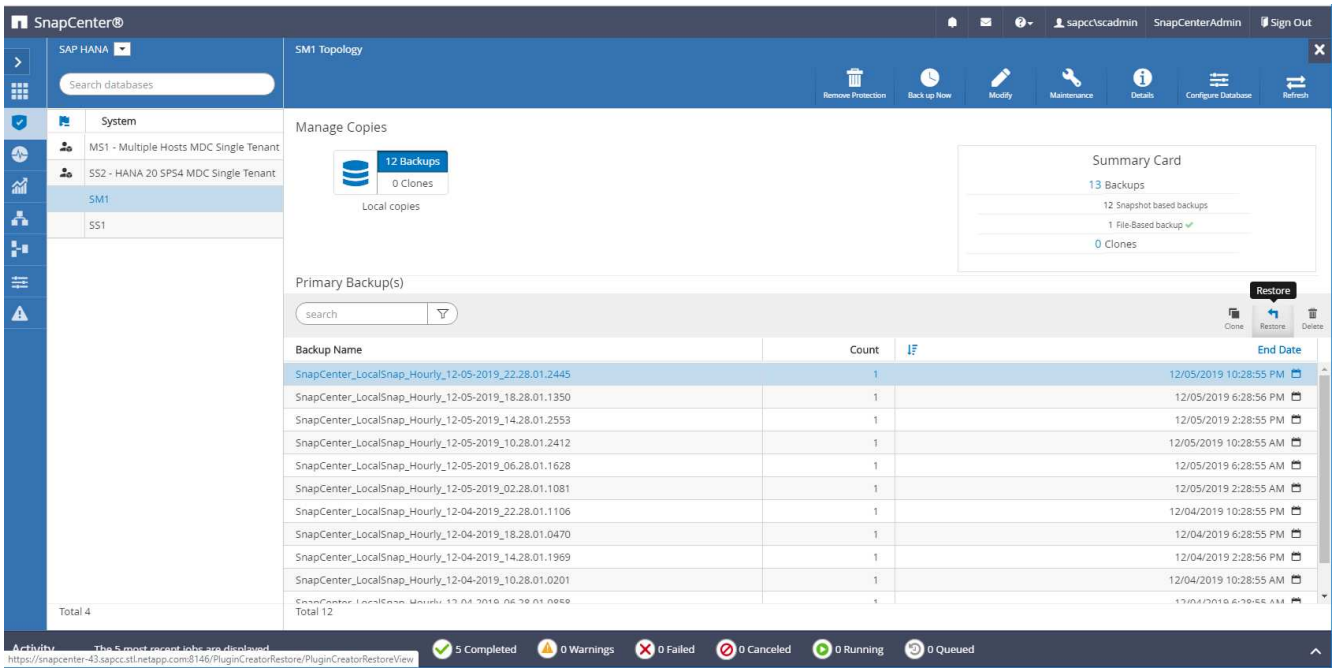
1. Arrestare il tenant da ripristinare e ripristinare.
2. Ripristinare il tenant con SnapCenter.
   - Per un ripristino dallo storage primario, SnapCenter esegue le seguenti operazioni:
     - **NFS.** Storage operazioni Single file SnapRestore per tutti i file del database tenant.
     - **SAN.** Clona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

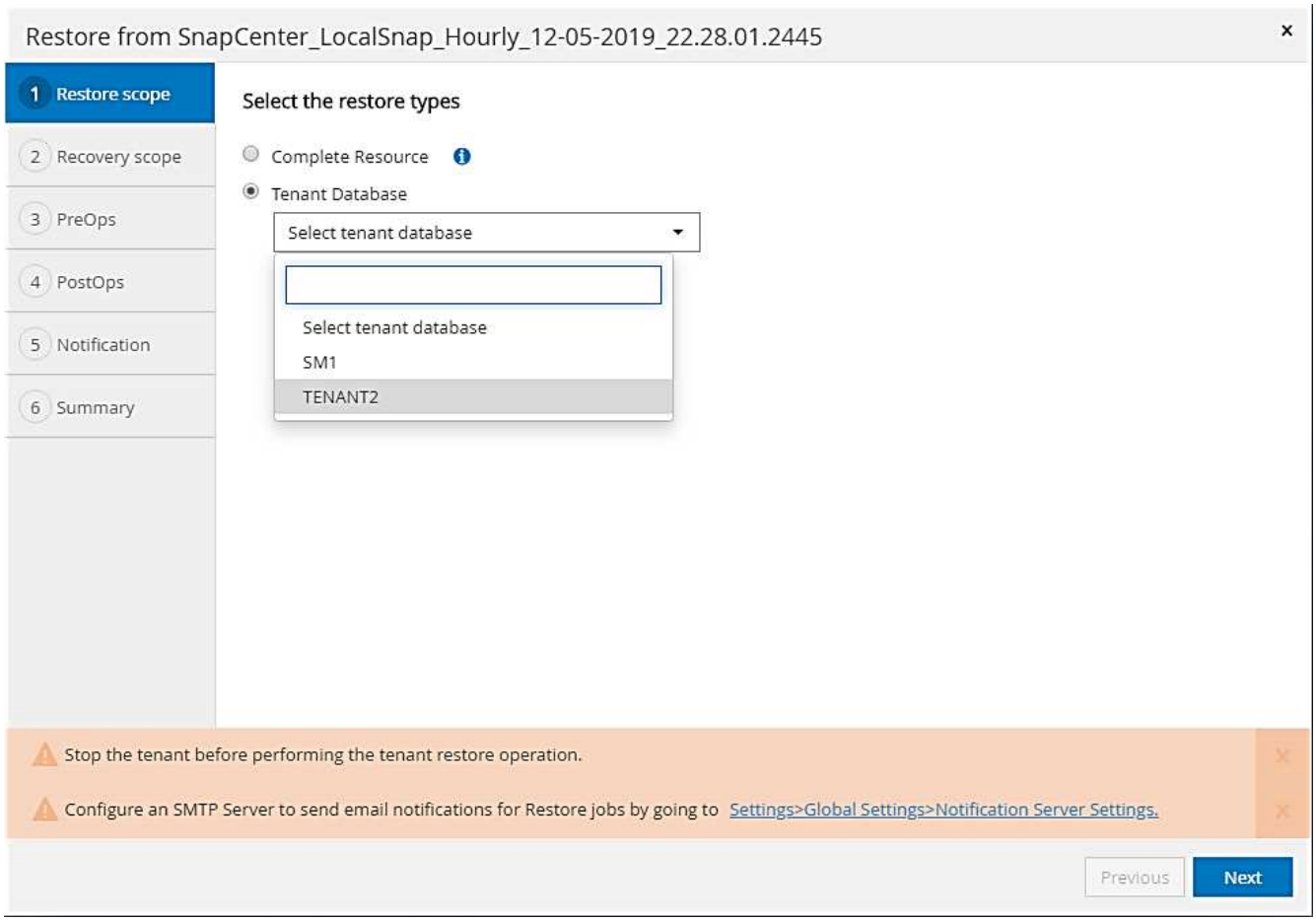
```
sm1adm@hana-2:/usr/sap/SM1/HDB00> hdbsql -U SYSKEY
Welcome to the SAP HANA Database interactive terminal.
Type:  \h for help with commands
       \q to quit
hdbsql=>
hdbsql SYSTEMDB=> alter system stop database tenant2;
0 rows affected (overall time 14.215281 sec; server time 14.212629 sec)
hdbsql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

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

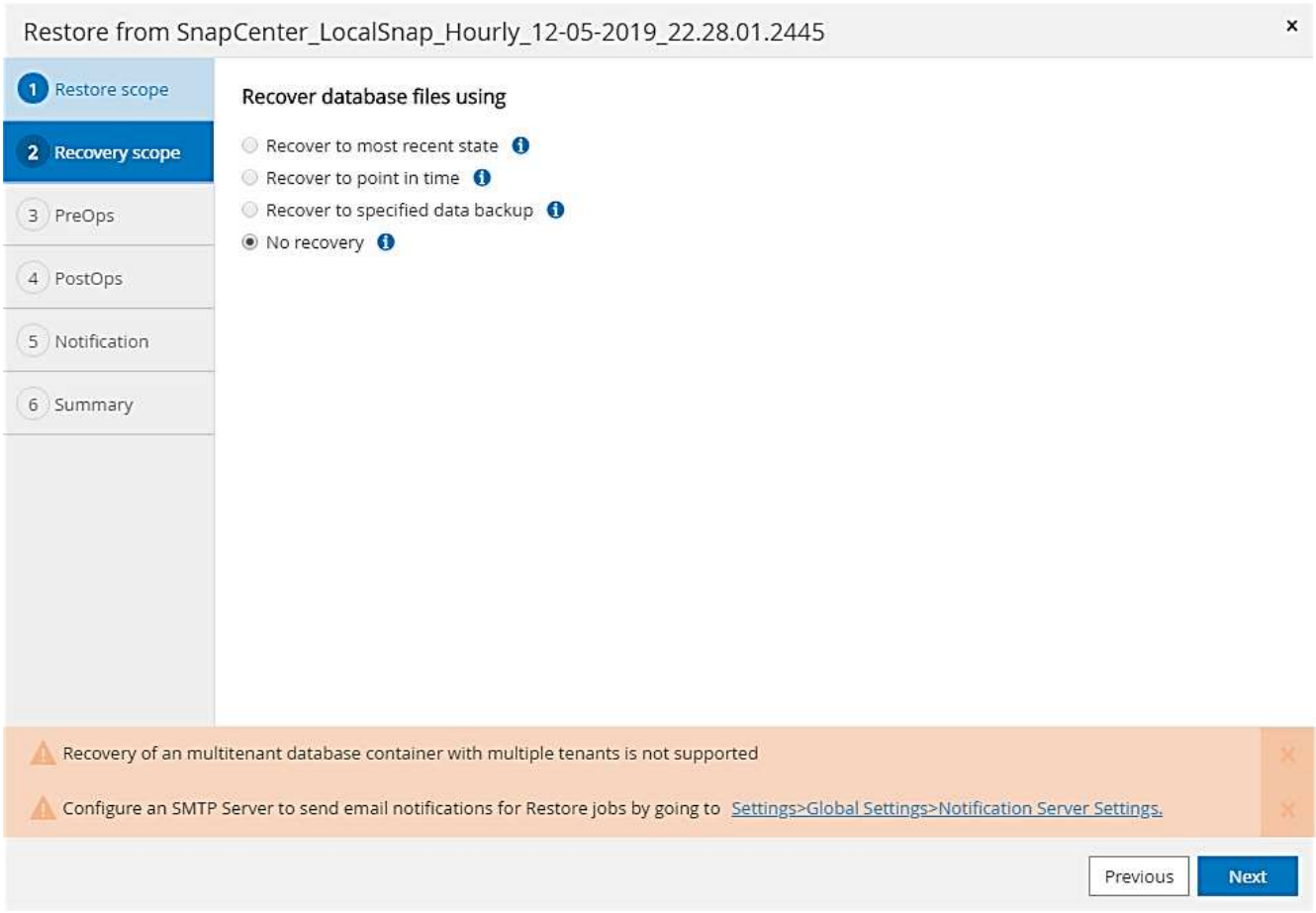


3. Selezionare il tenant da ripristinare.

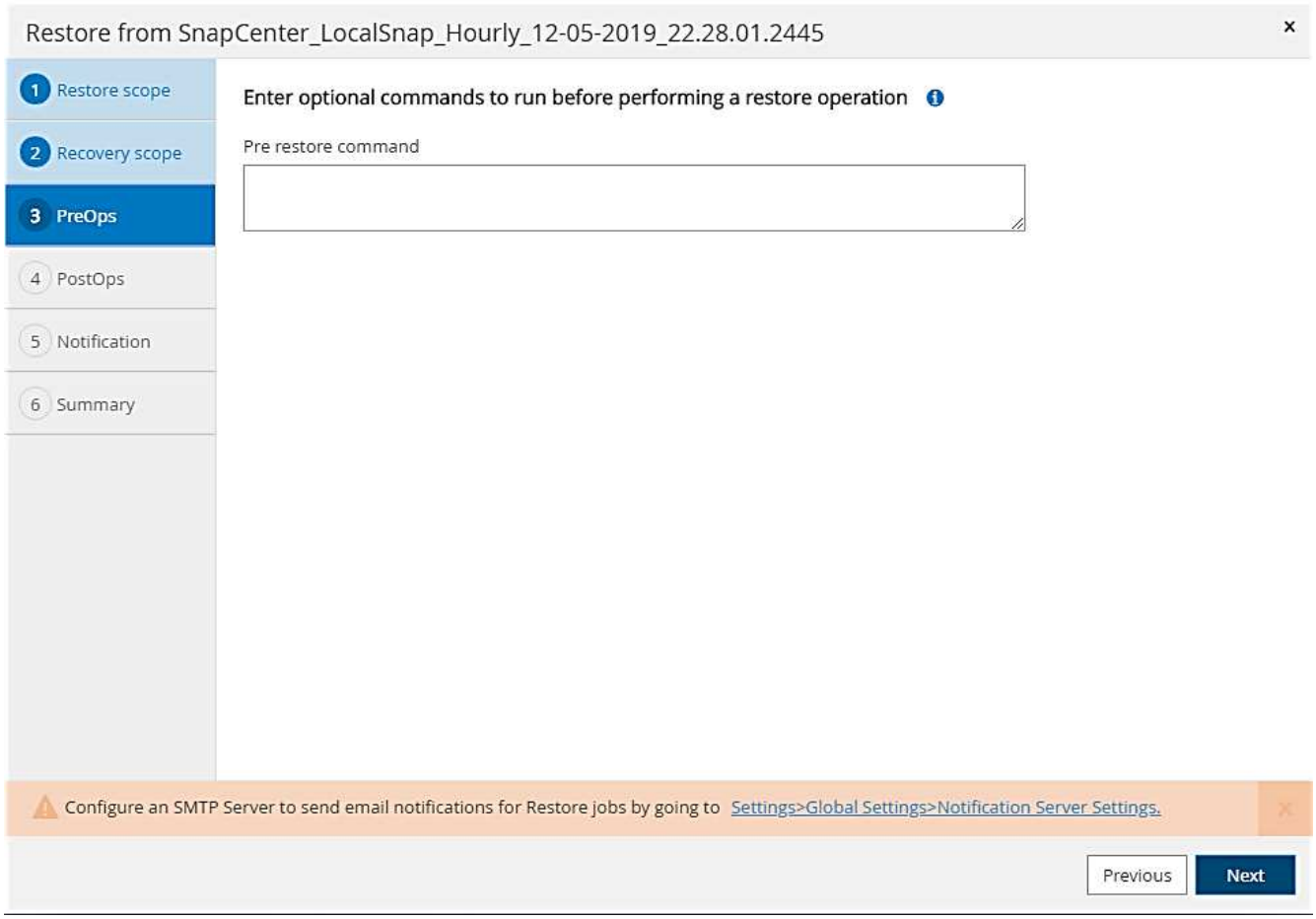
SnapCenter mostra un elenco di tutti i tenant inclusi nel backup selezionato.



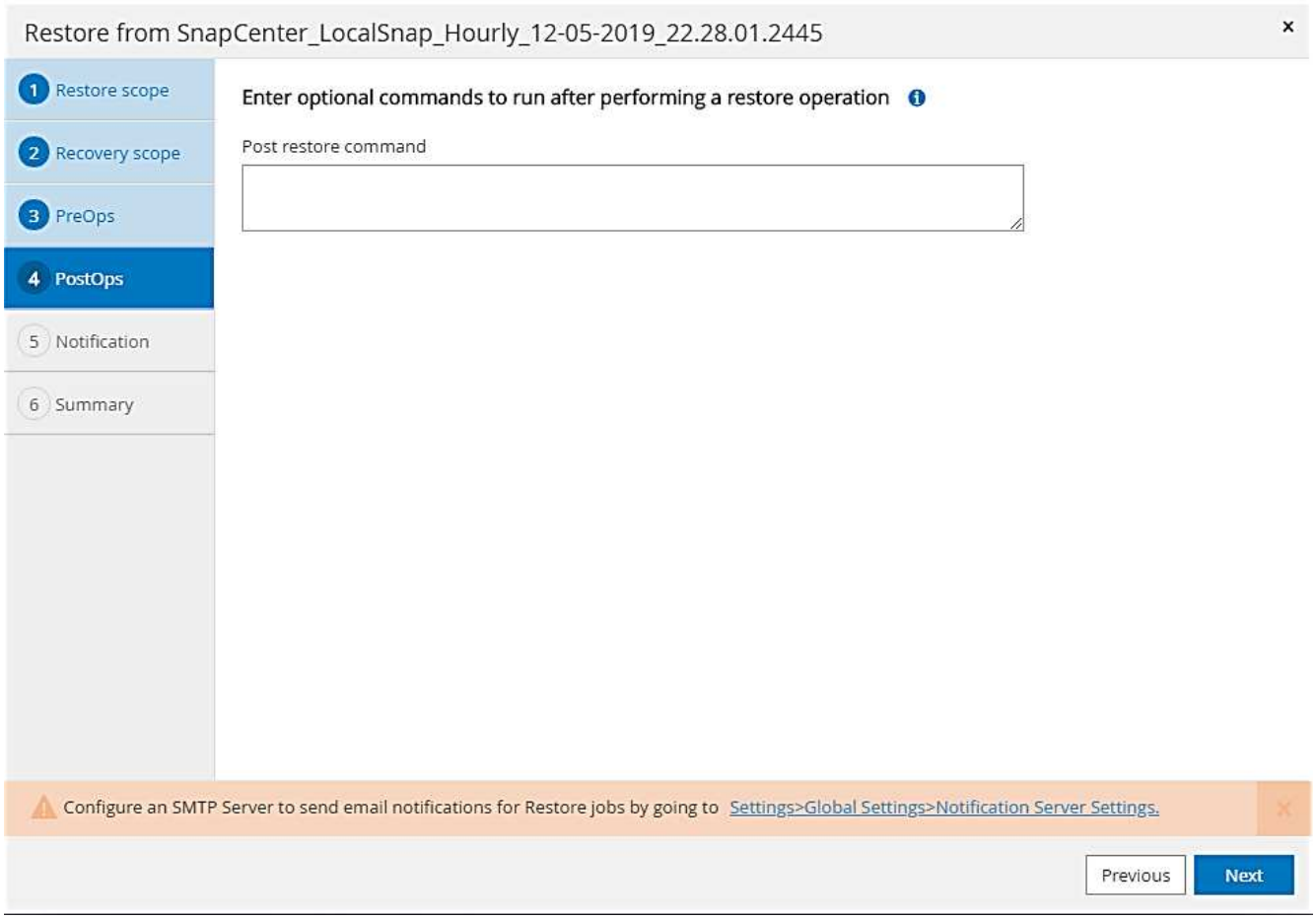
Il ripristino single-tenant non è supportato con SnapCenter 4.3. Nessun ripristino preselezionato e non modificabile.



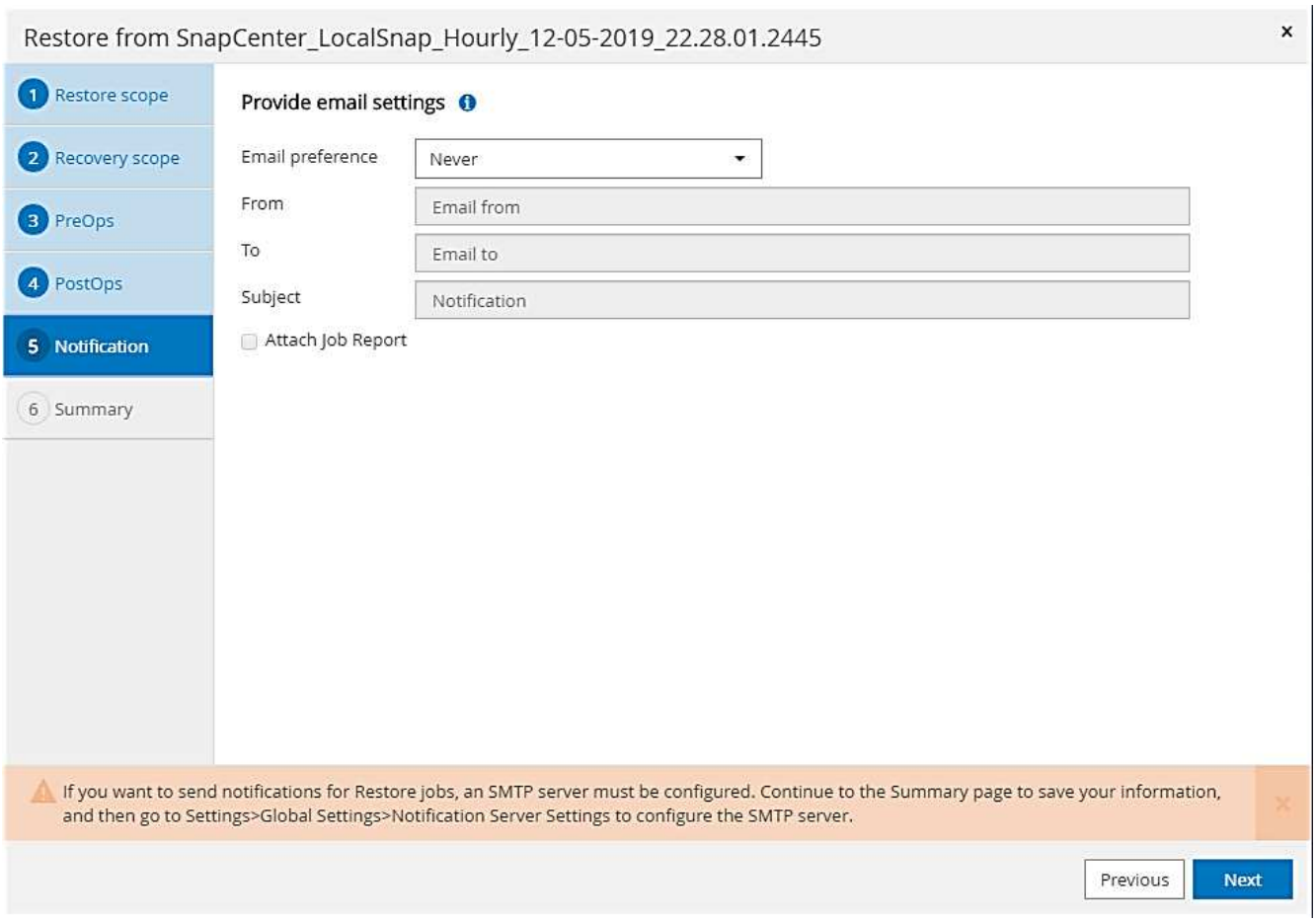
4. Immettere i comandi opzionali di prerestore.



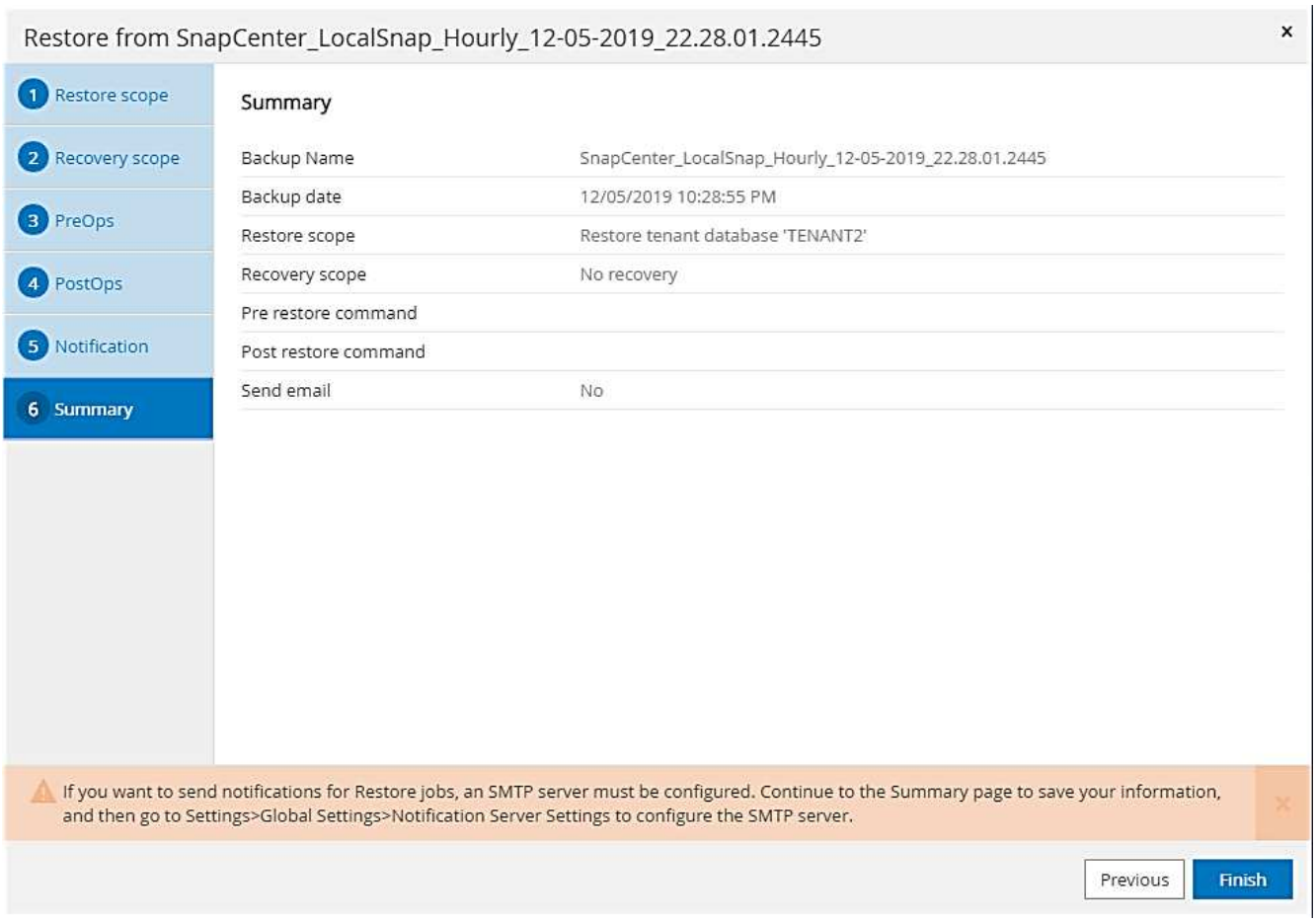
5. Immettere comandi post-ripristino opzionali.



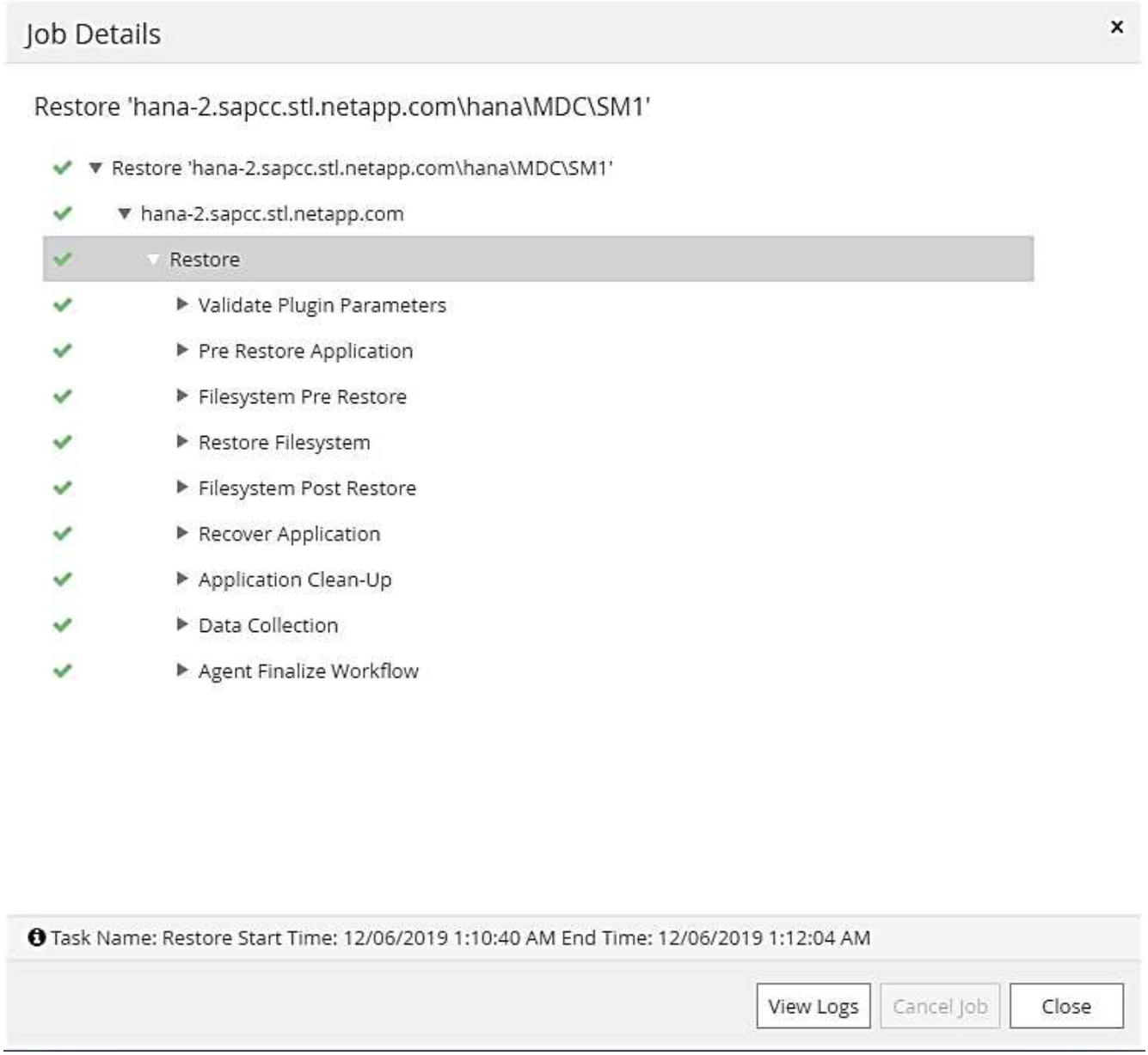
6. Immettere le impostazioni e-mail opzionali.



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



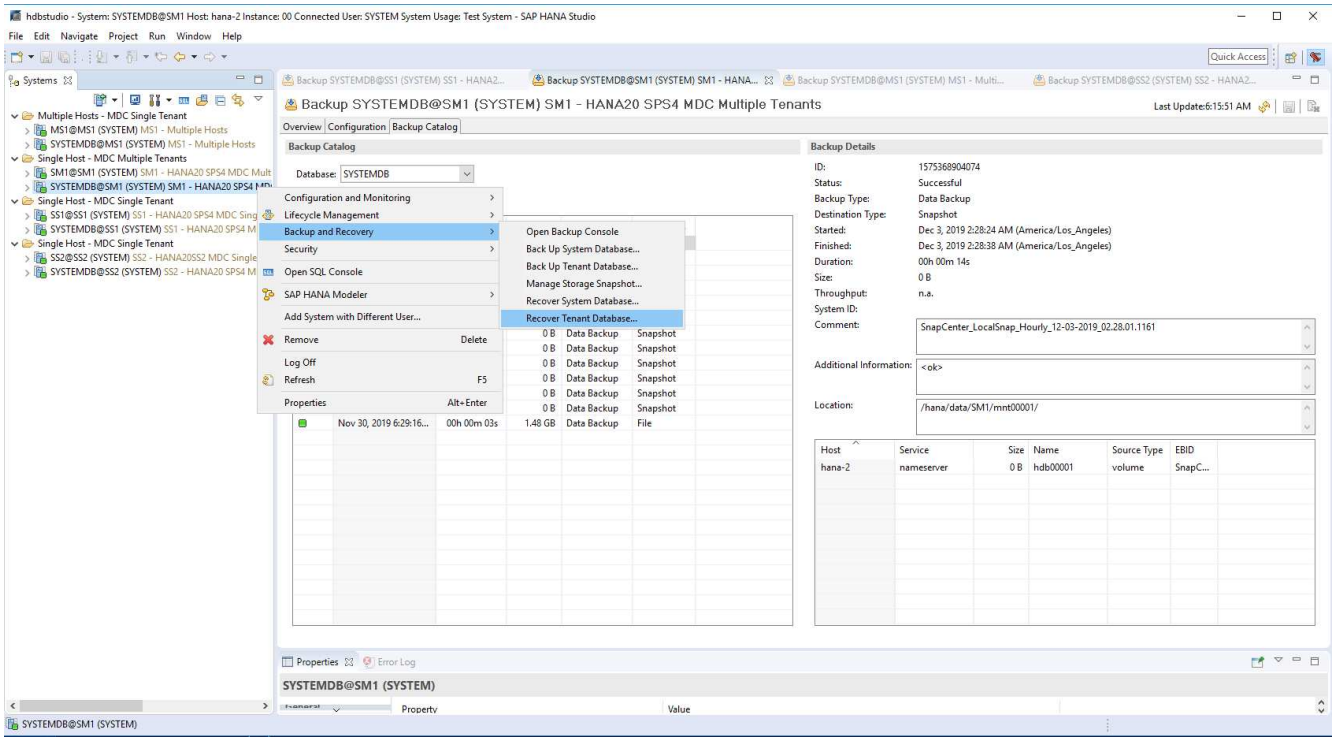
L’operazione di ripristino viene eseguita da SnapCenter. Questo esempio mostra i dettagli del lavoro di ripristino.



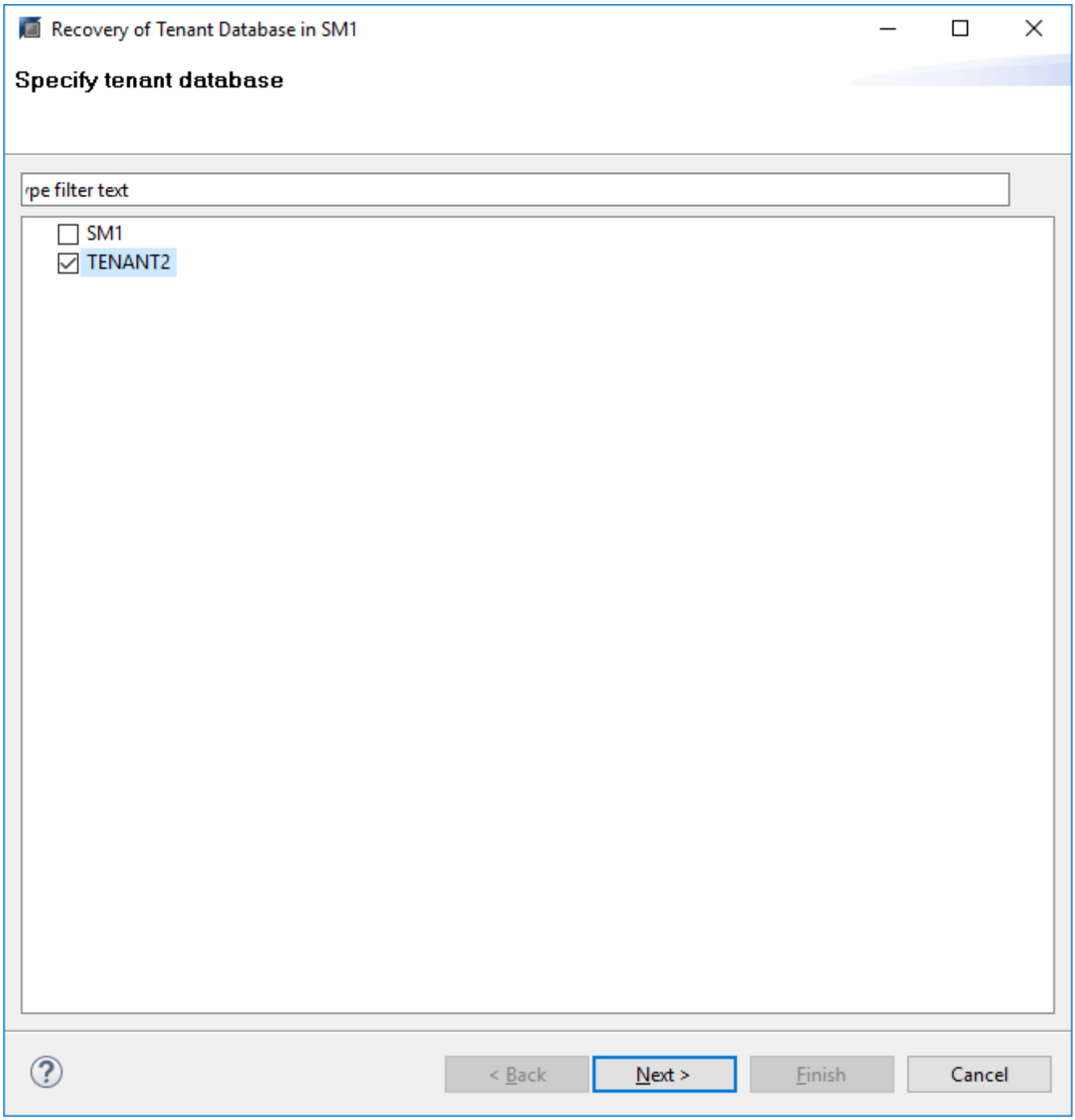
Al termine dell'operazione di ripristino del tenant, vengono ripristinati solo i dati rilevanti del tenant. Sul file system dell'host del database HANA, sono disponibili il file di dati ripristinato e il file ID di backup Snapshot del tenant.

```
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>
```

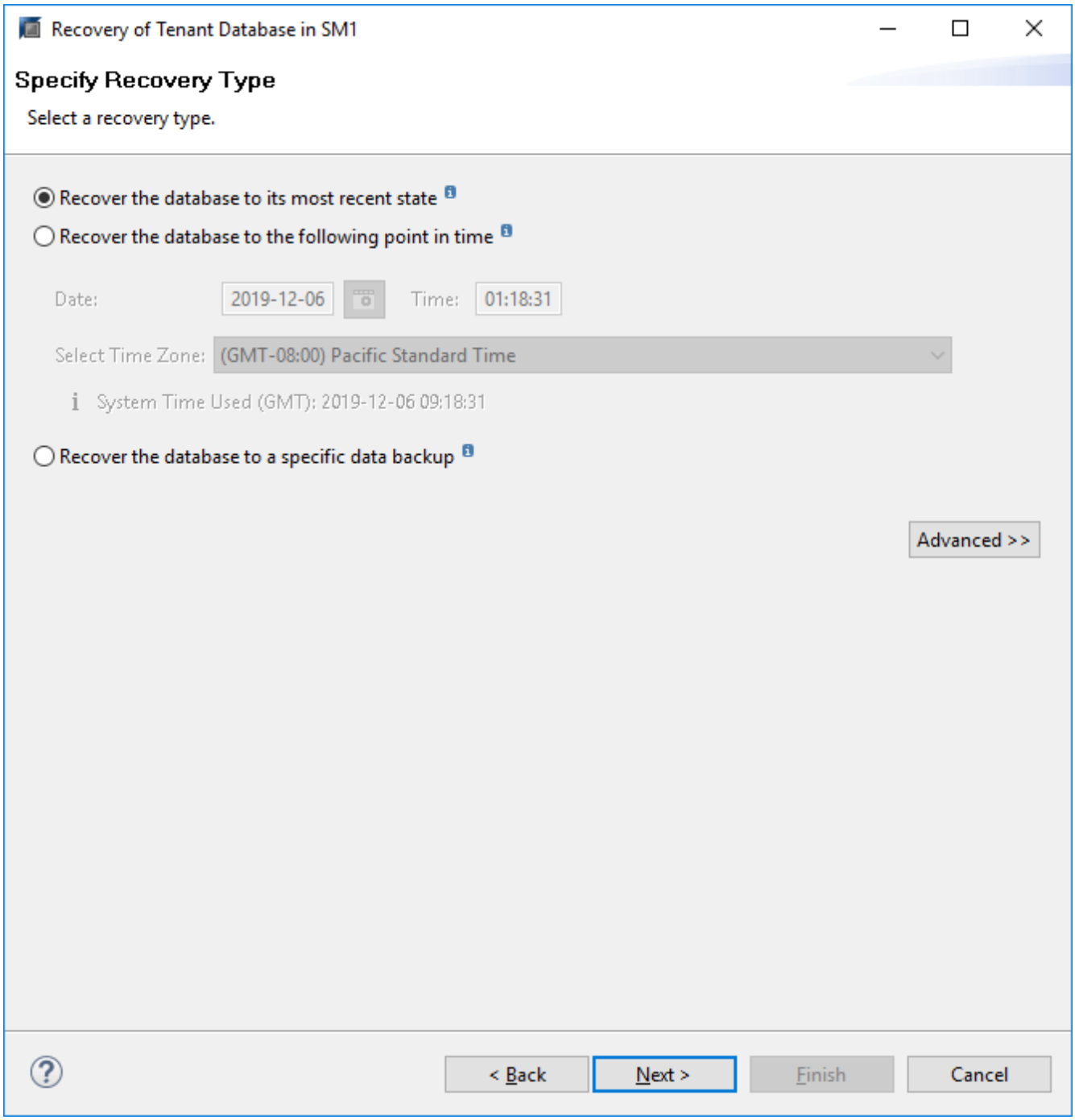
8. Avviare il ripristino con HANA Studio.



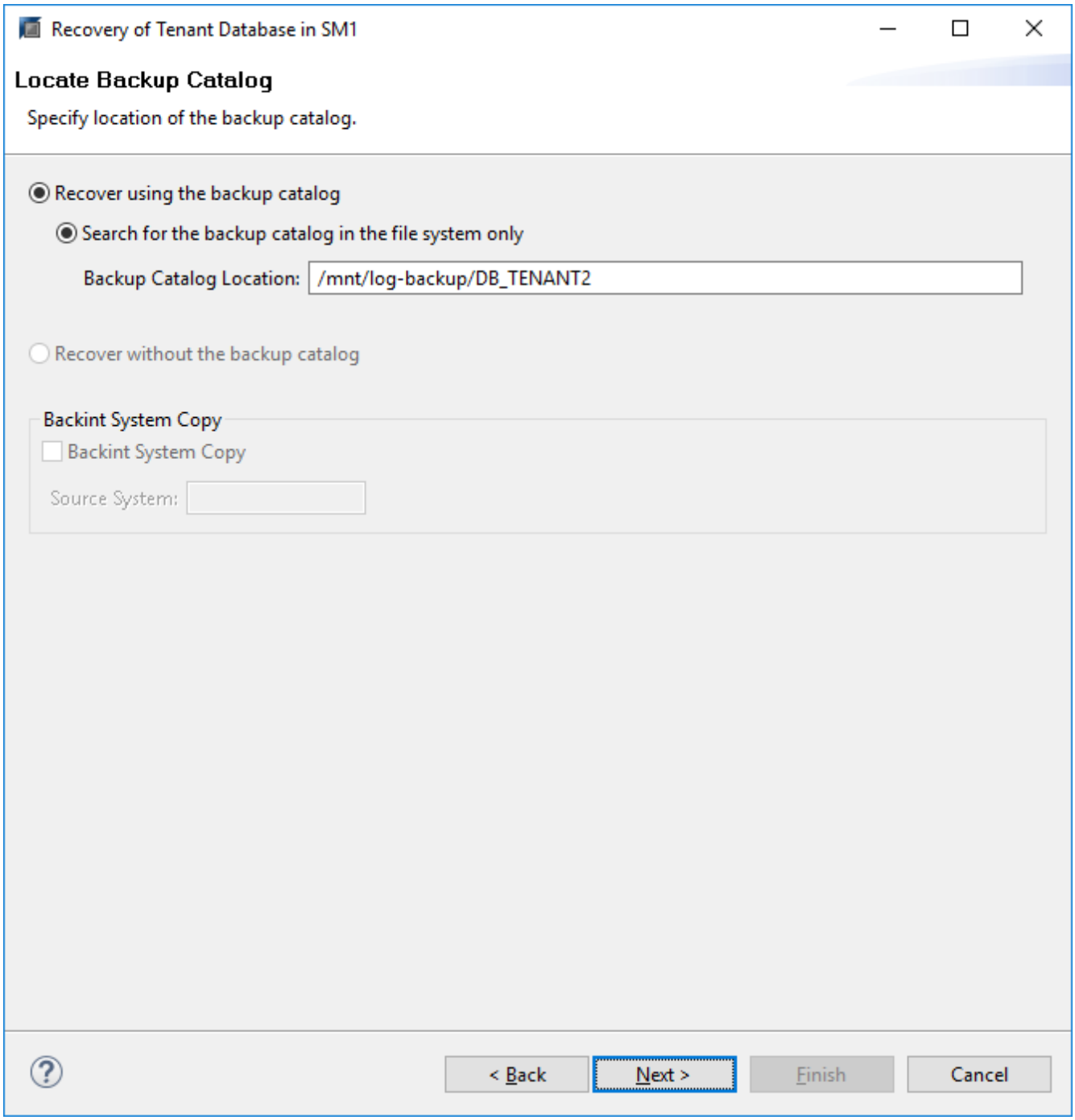
9. Selezionare il tenant.

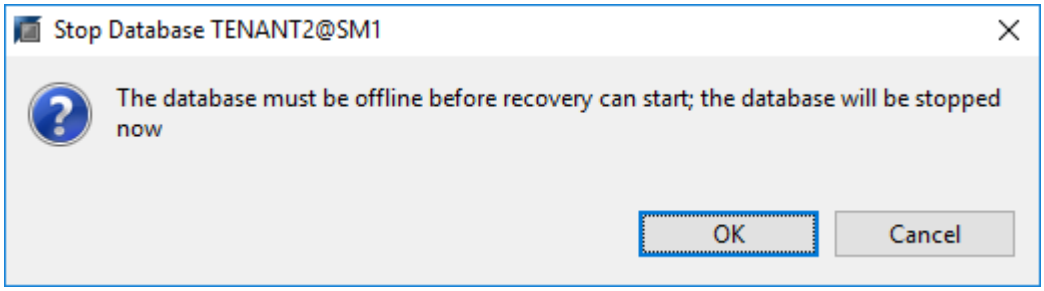


10. Selezionare il tipo di ripristino.



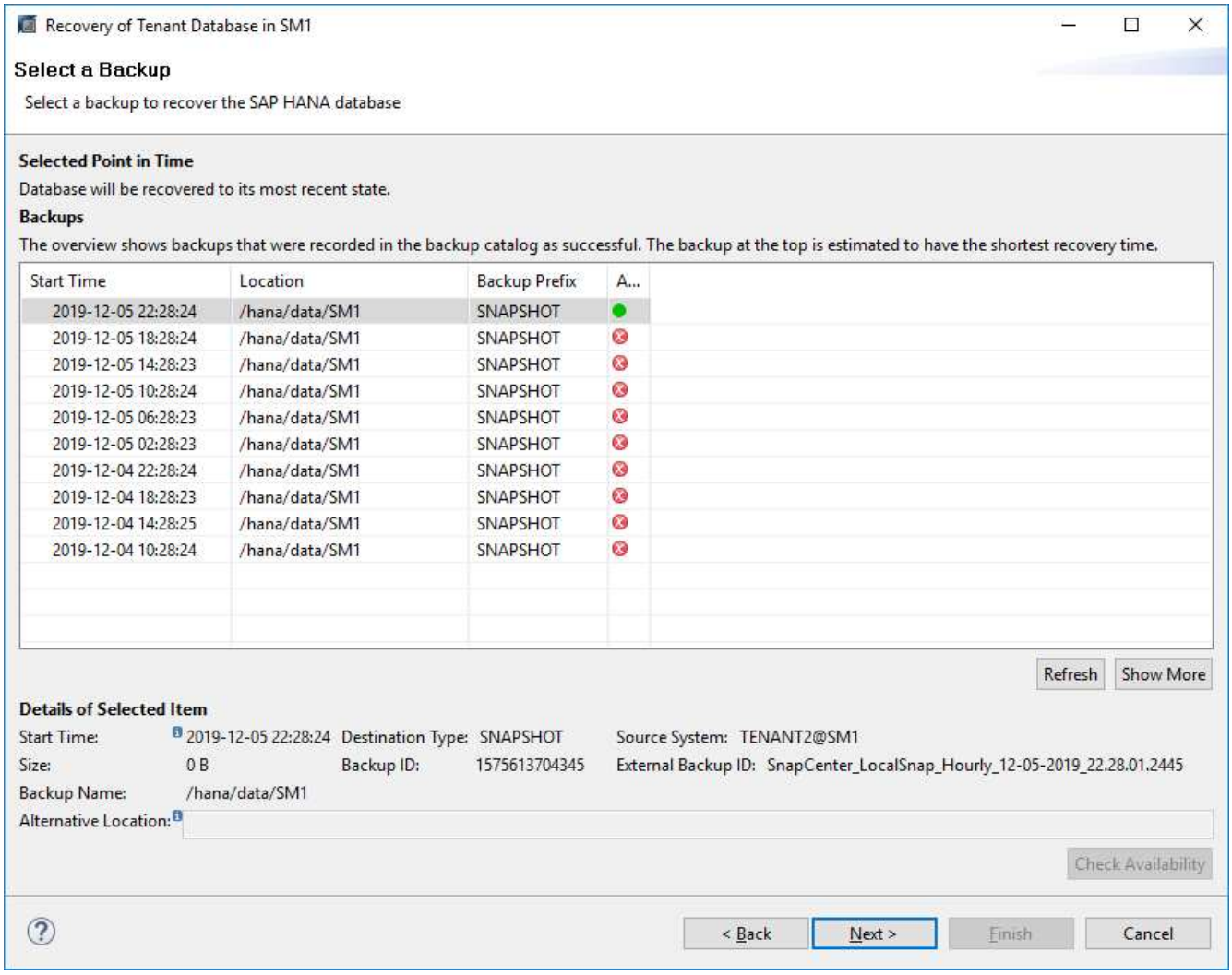
11. Fornire la posizione del catalogo di backup.



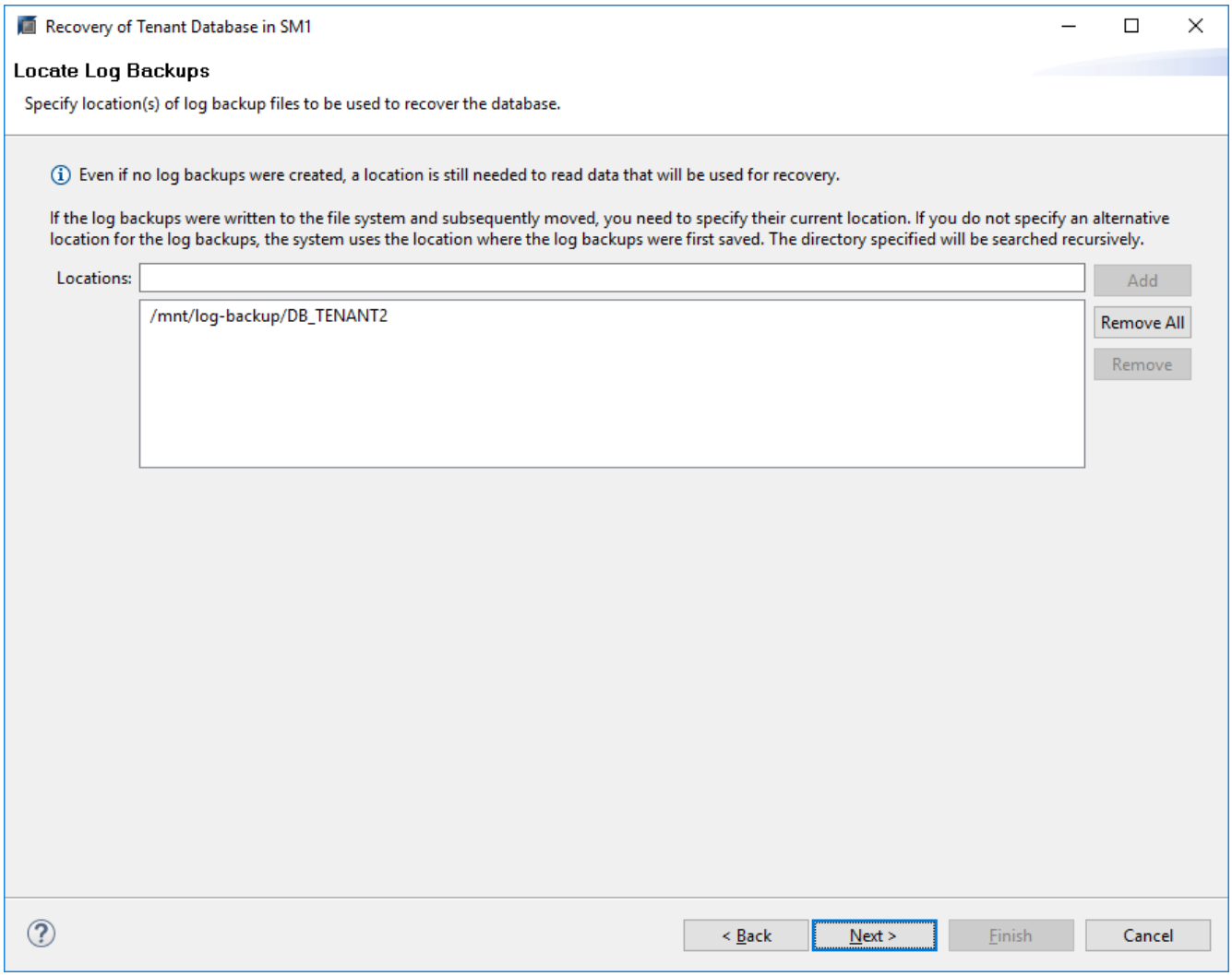


All'interno del catalogo di backup, il backup ripristinato viene evidenziato con un'icona verde. L'ID del backup esterno mostra il nome del backup precedentemente selezionato in SnapCenter.

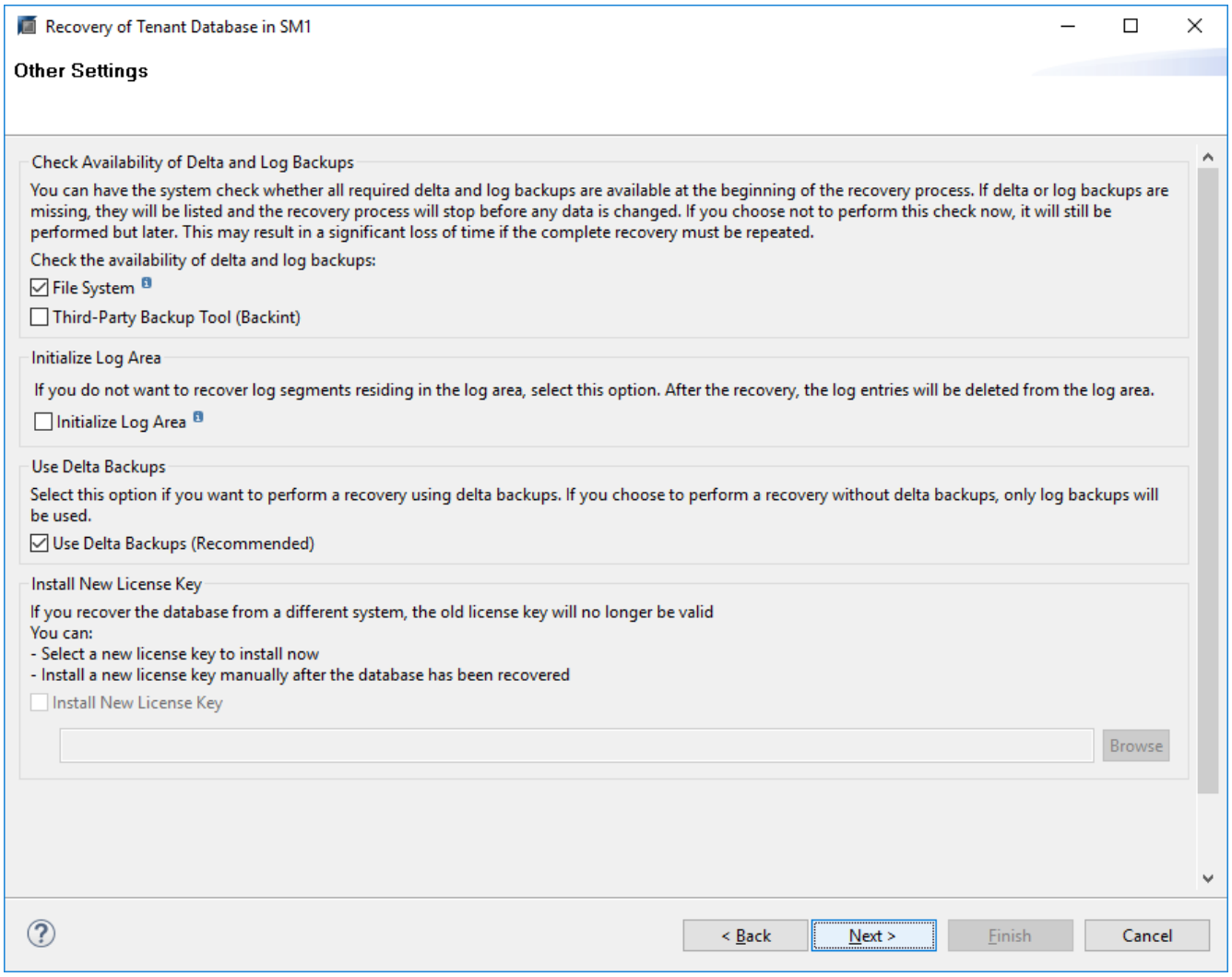
12. Selezionare la voce con l'icona verde e fare clic su Next (Avanti).



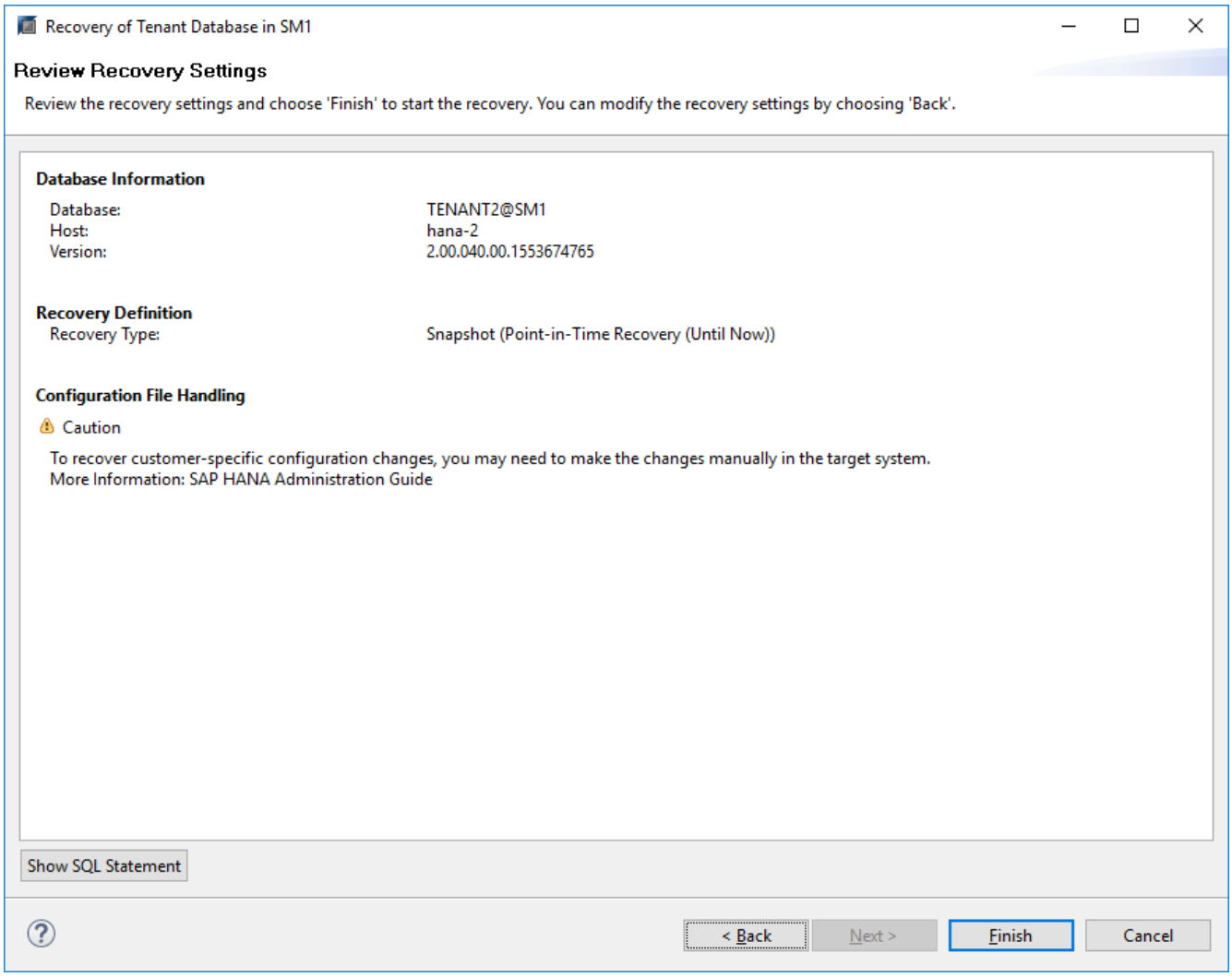
13. Fornire la posizione di backup del registro.

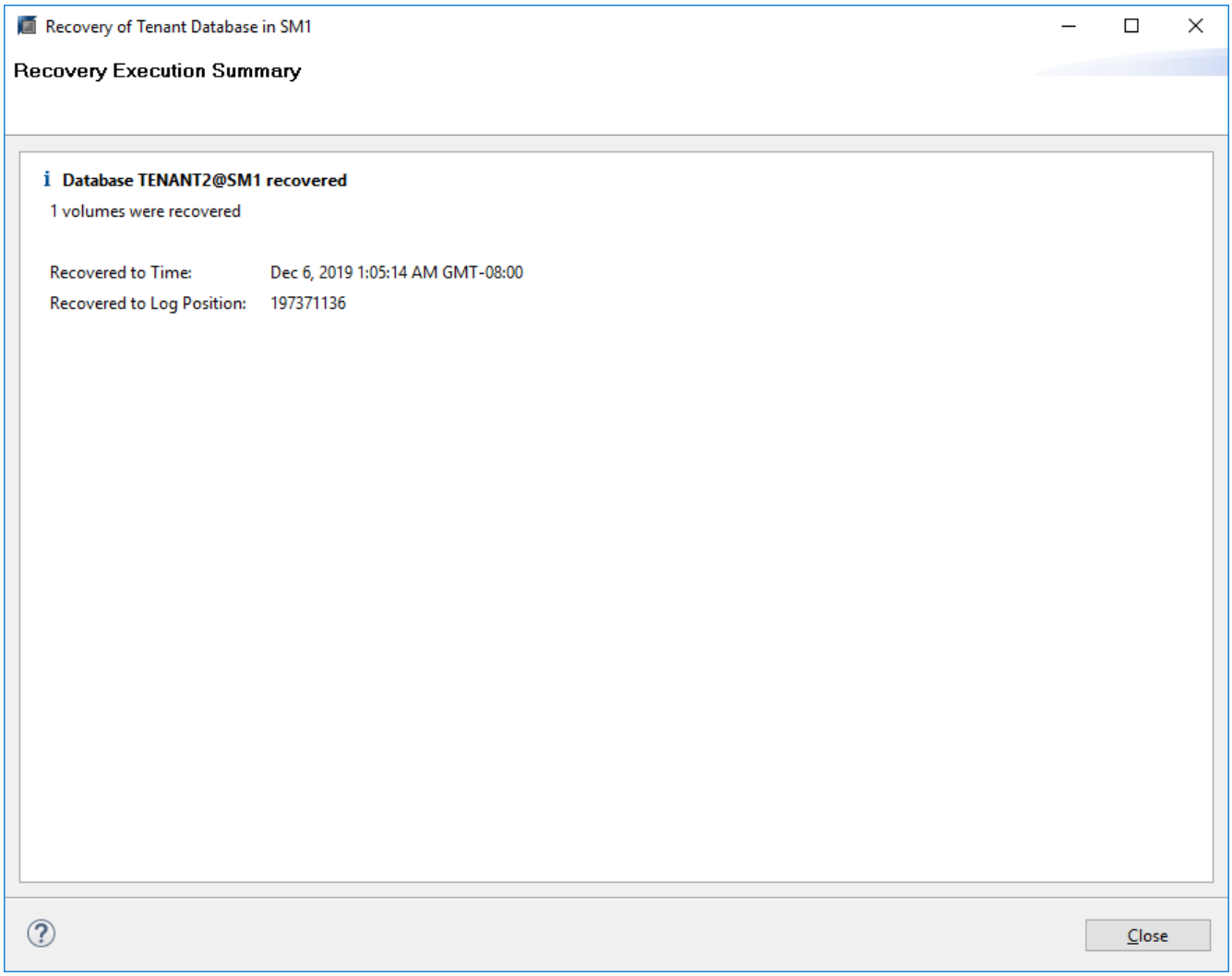


14. Selezionare le altre impostazioni desiderate.



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.

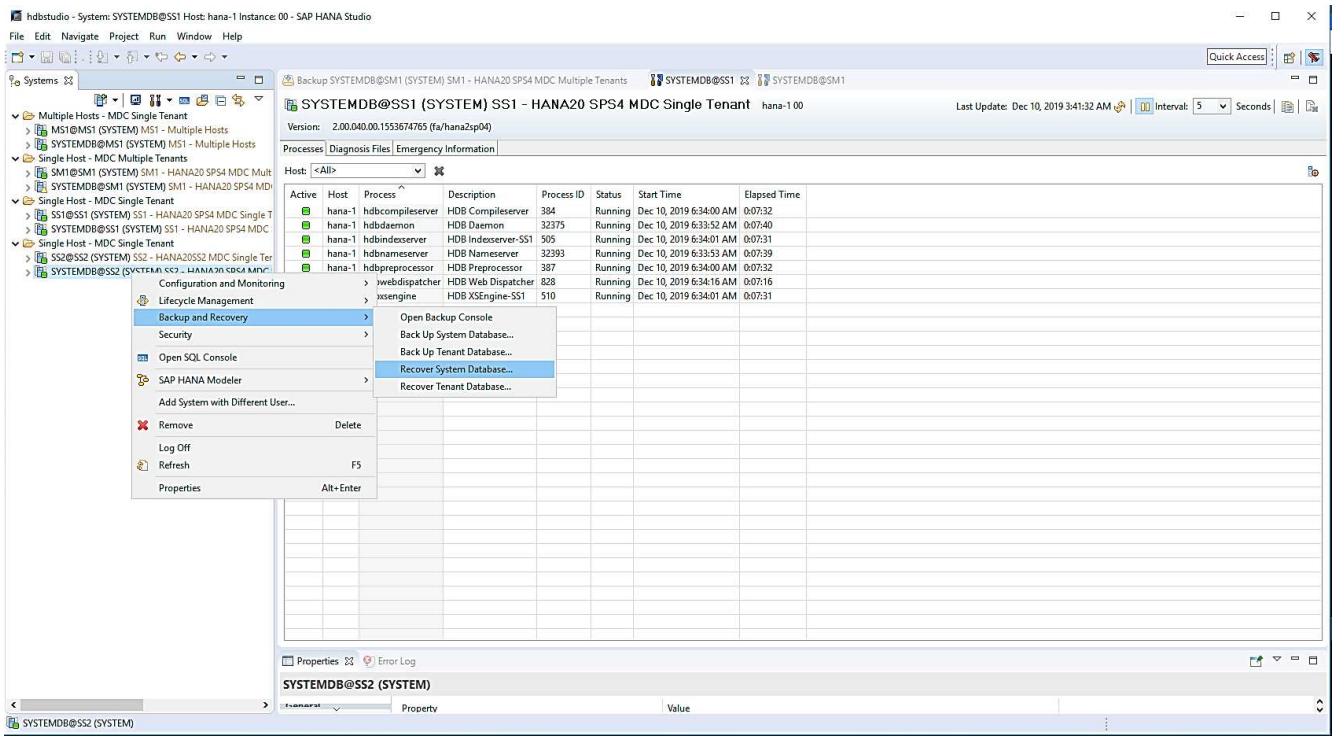
3. Eseguire il processo di ripristino del database di sistema con SAP HANA Studio:
   a. Fare clic su Refresh (Aggiorna) dall'elenco dei backup e selezionare il backup disponibile per il ripristino (indicato da un'icona verde).
   b. Avviare il processo di ripristino. Al termine del processo di ripristino,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

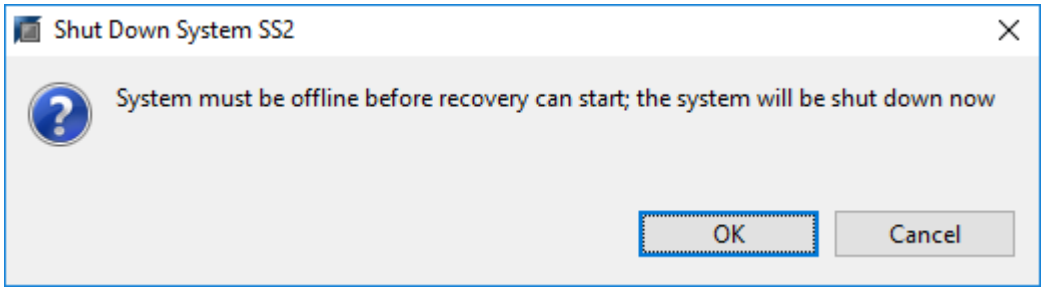
   c. Selezionare questo backup e avviare il processo di ripristino. Al termine del processo di ripristino, il database del tenant viene avviato automaticamente.

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.

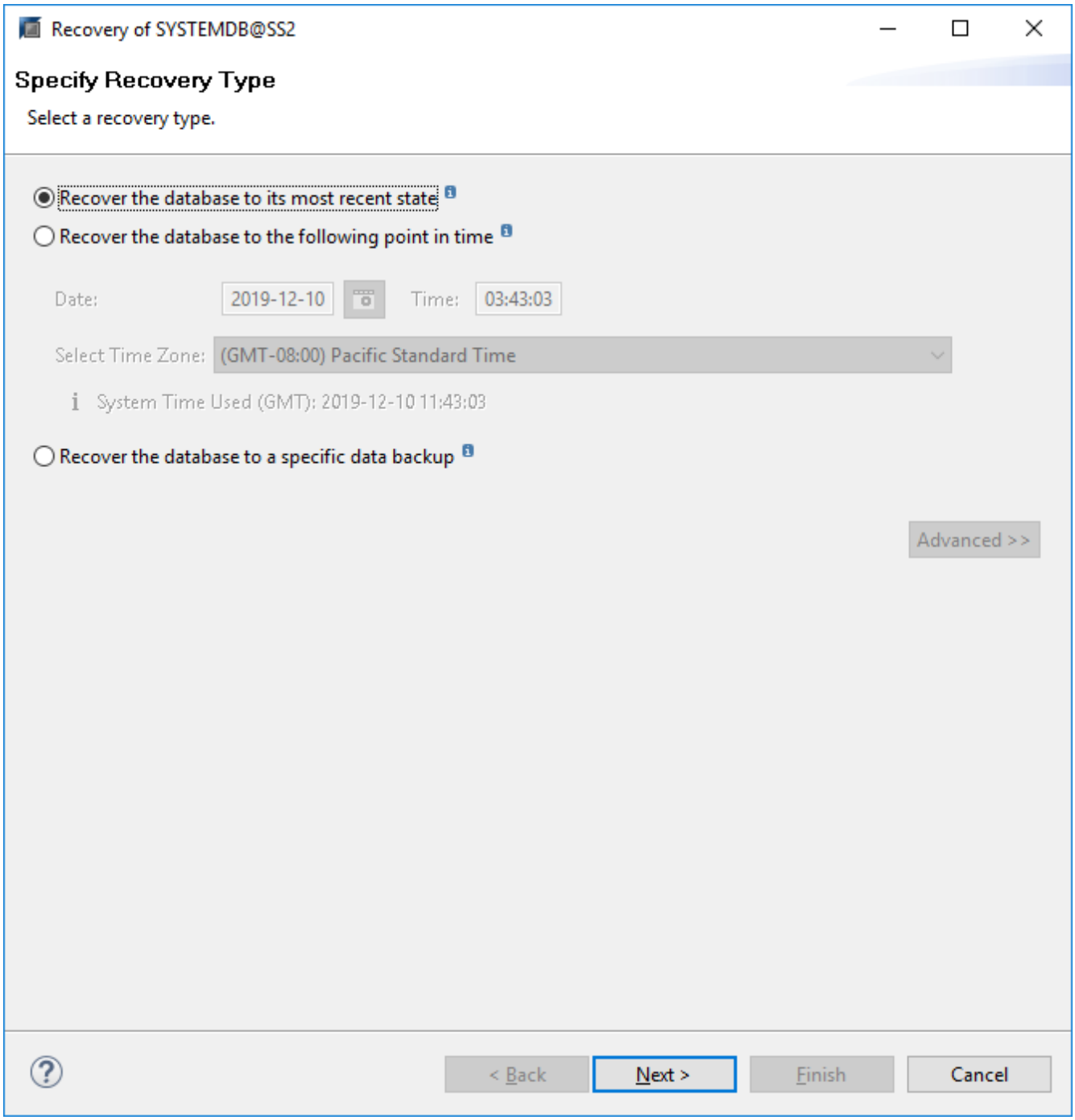


2. Fare clic su OK per chiudere il database SAP HANA.

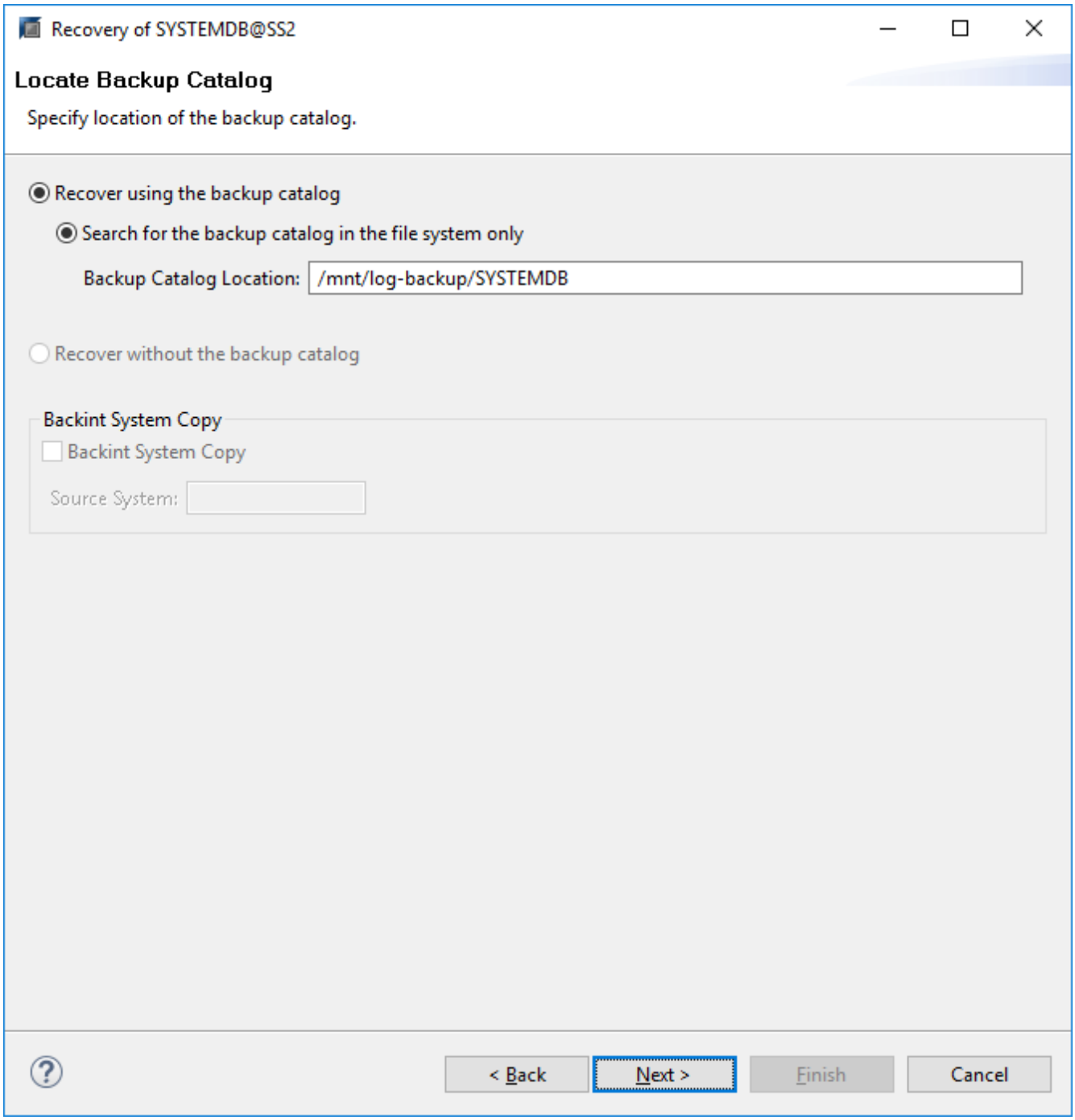


Il sistema SAP HANA si spegne e viene avviata la procedura guidata di ripristino.

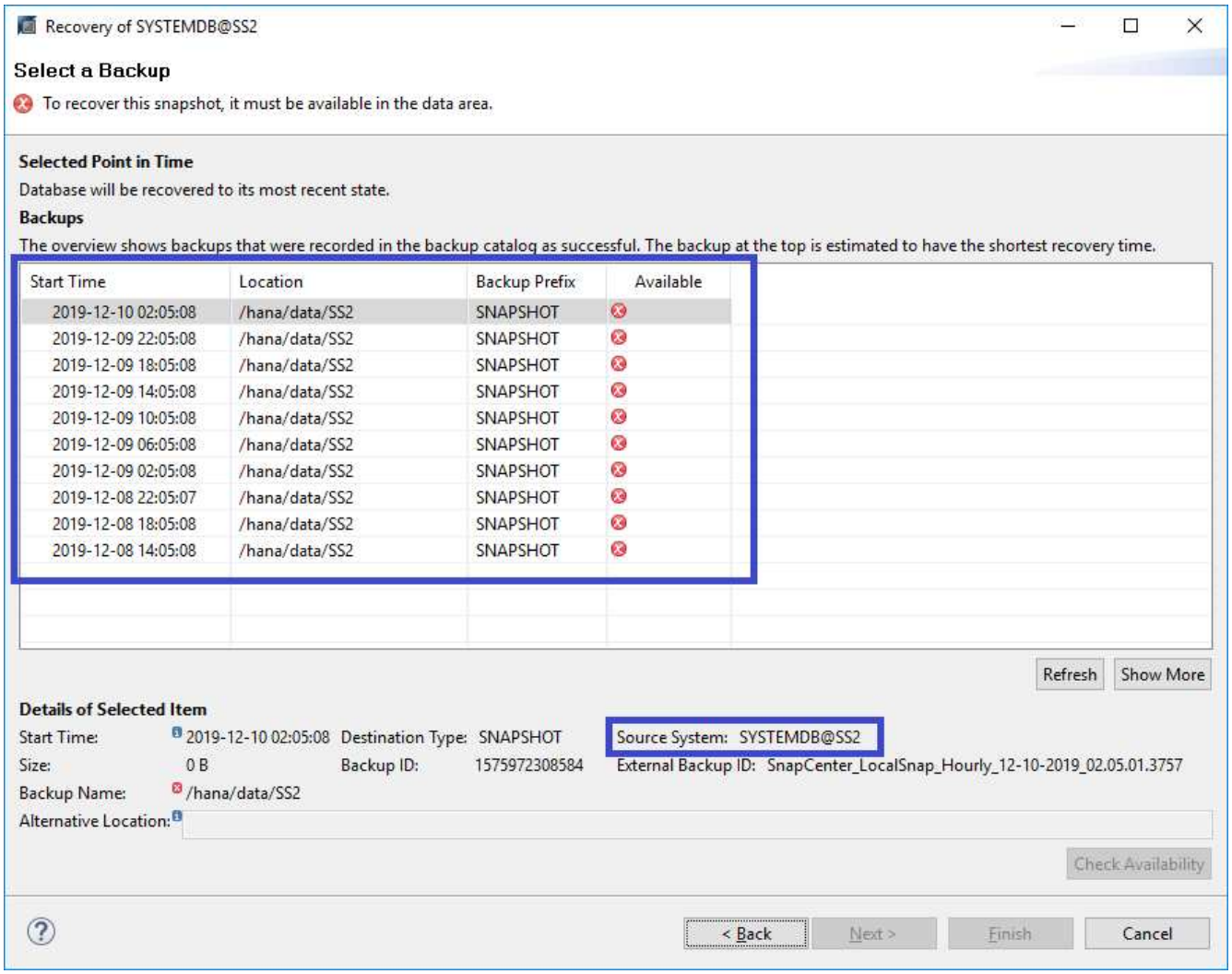
3. Selezionare il tipo di ripristino e fare clic su Next (Avanti).



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.



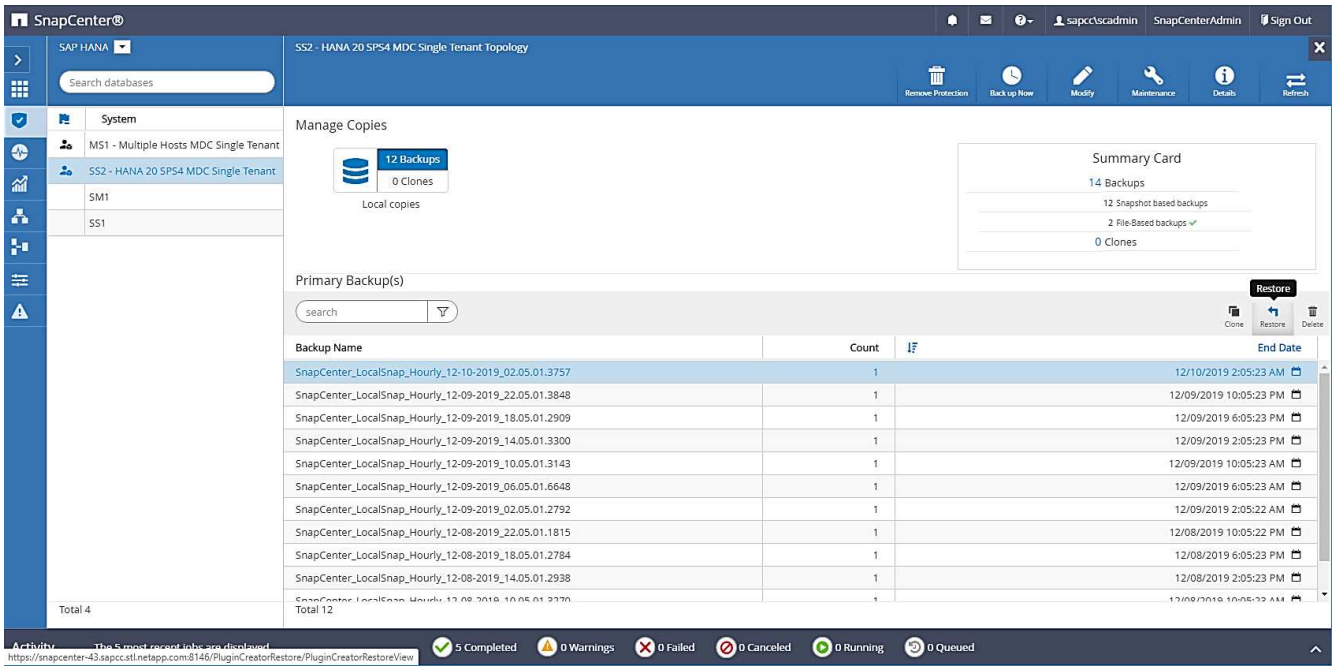
6. Smontare tutti i volumi di dati.

```
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.

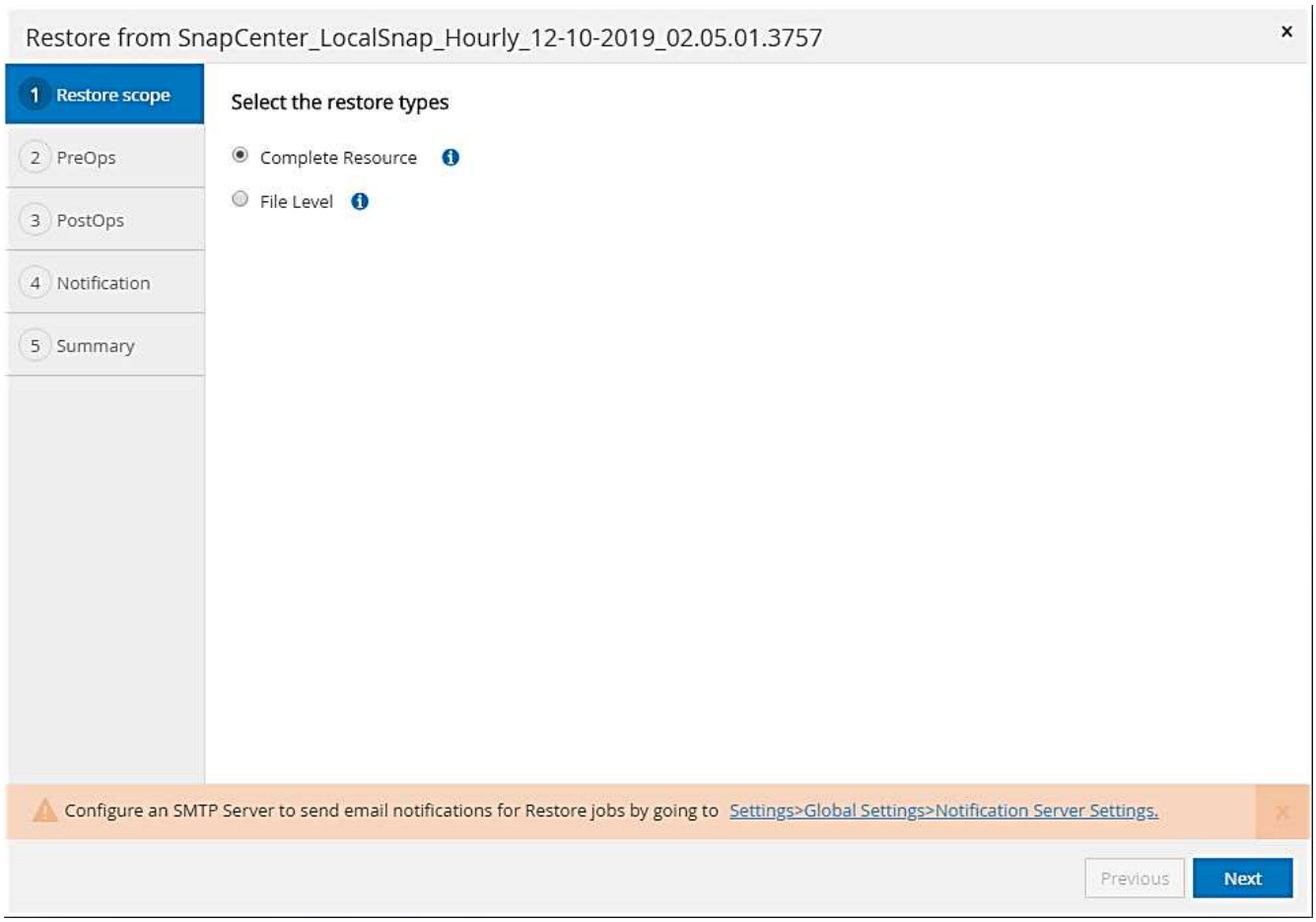
7. Dalla GUI di SnapCenter, selezionare la vista della topologia delle risorse e selezionare il backup da ripristinare; nel nostro esempio, il backup primario più recente. Fare clic sull'icona Restore (Ripristina) per avviare il ripristino.



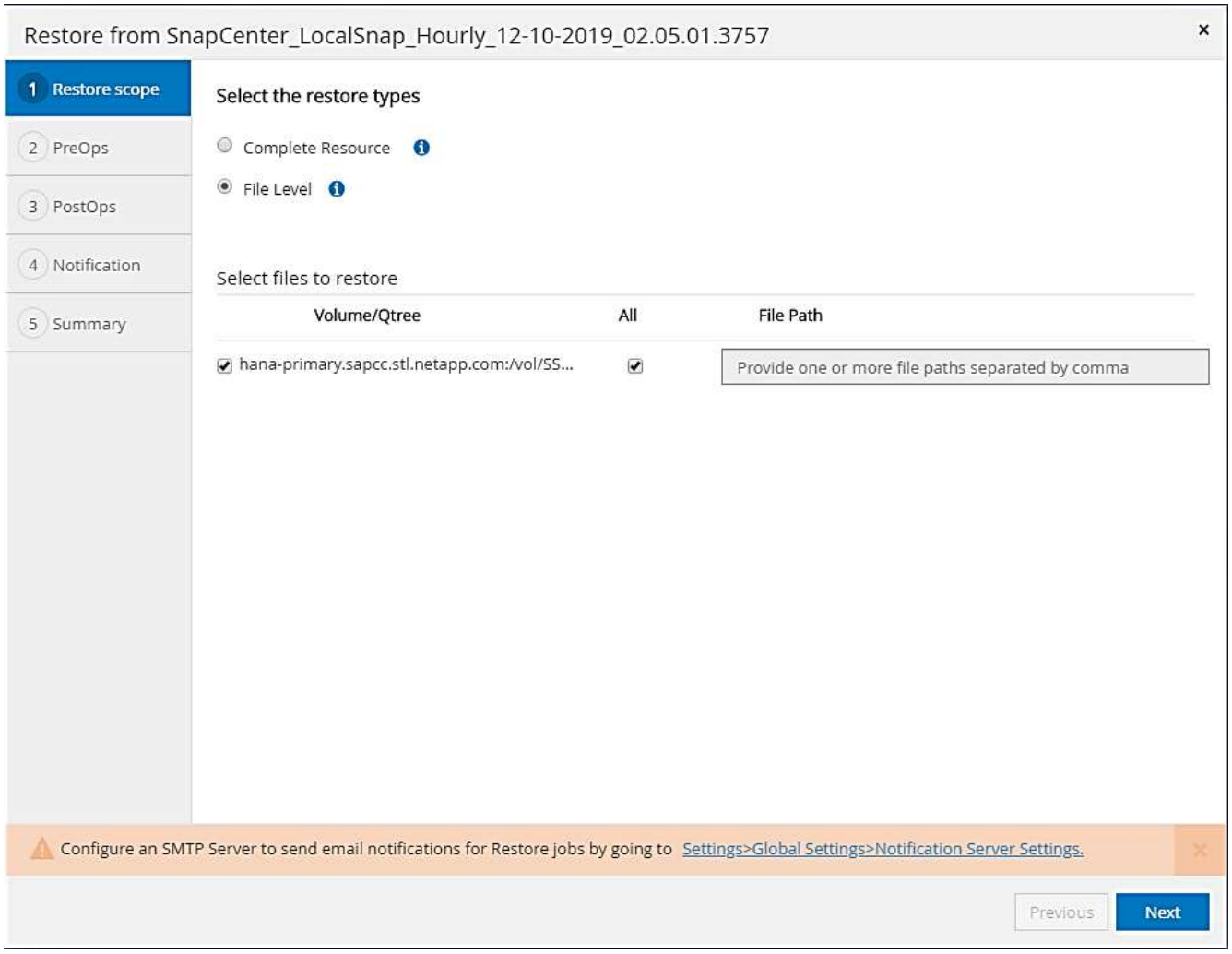
Viene avviata la procedura guidata di ripristino di SnapCenter.

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

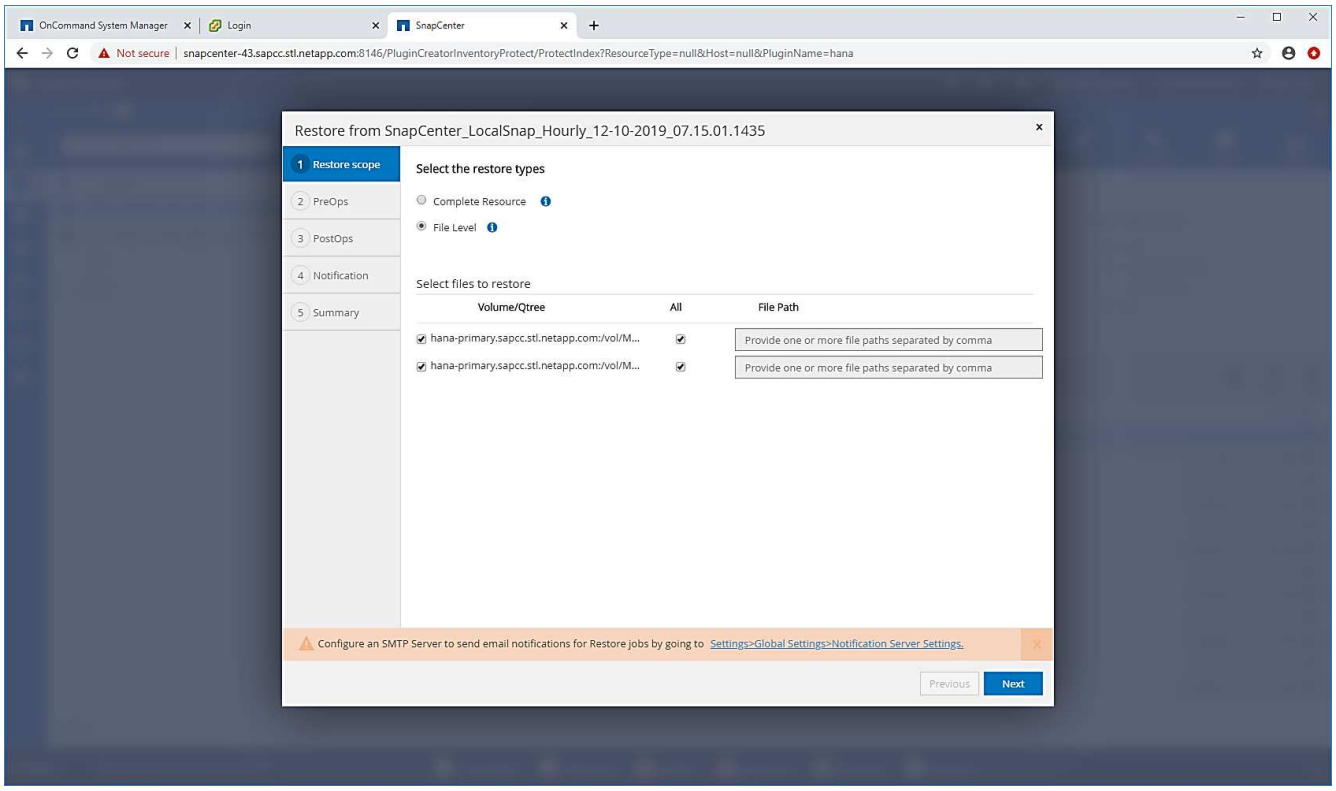
   Selezionare completa risorsa per utilizzare un ripristino basato su volume.



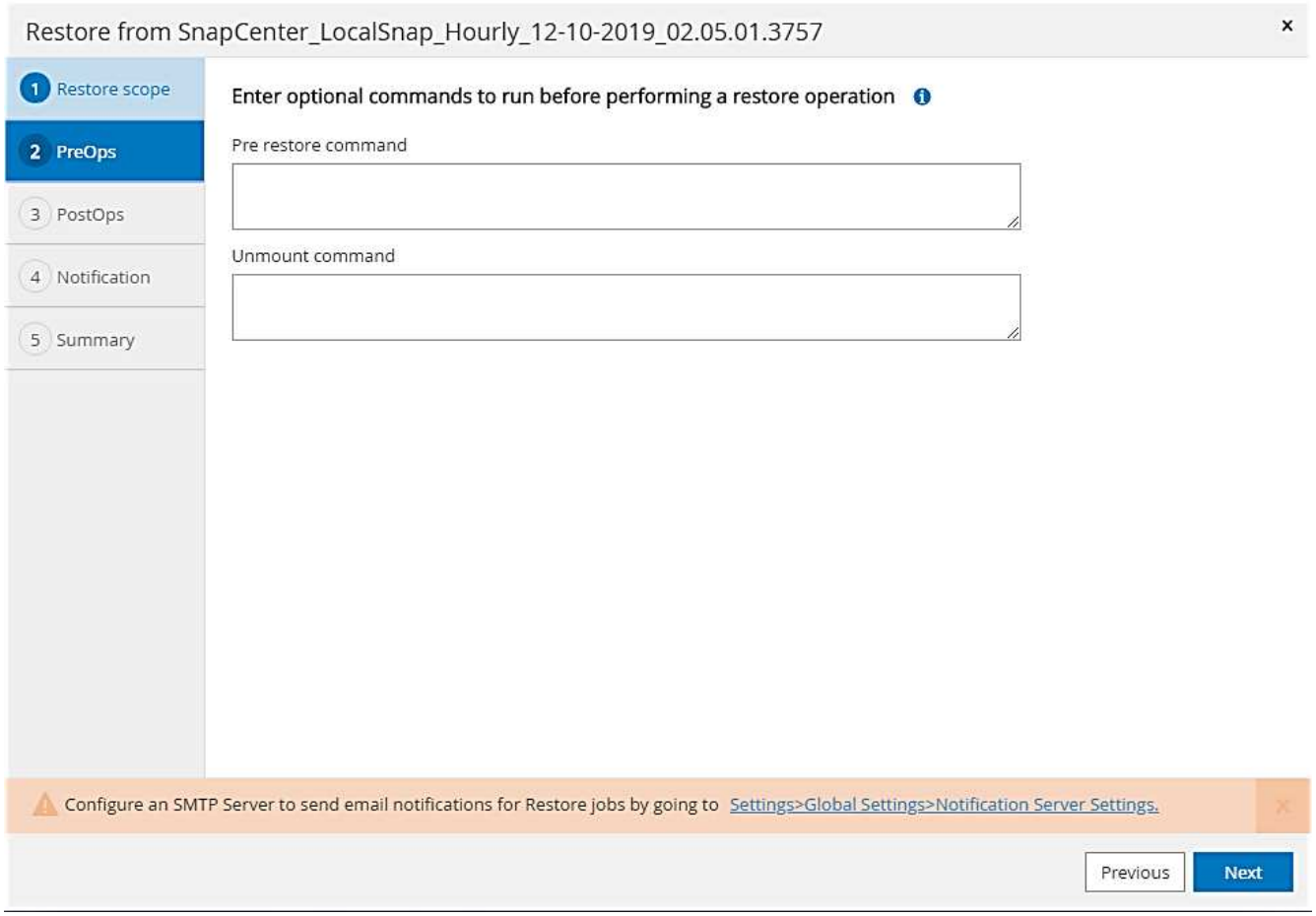
9. Selezionare livello file e tutto per utilizzare un'operazione SnapRestore a file singolo per tutti i file.



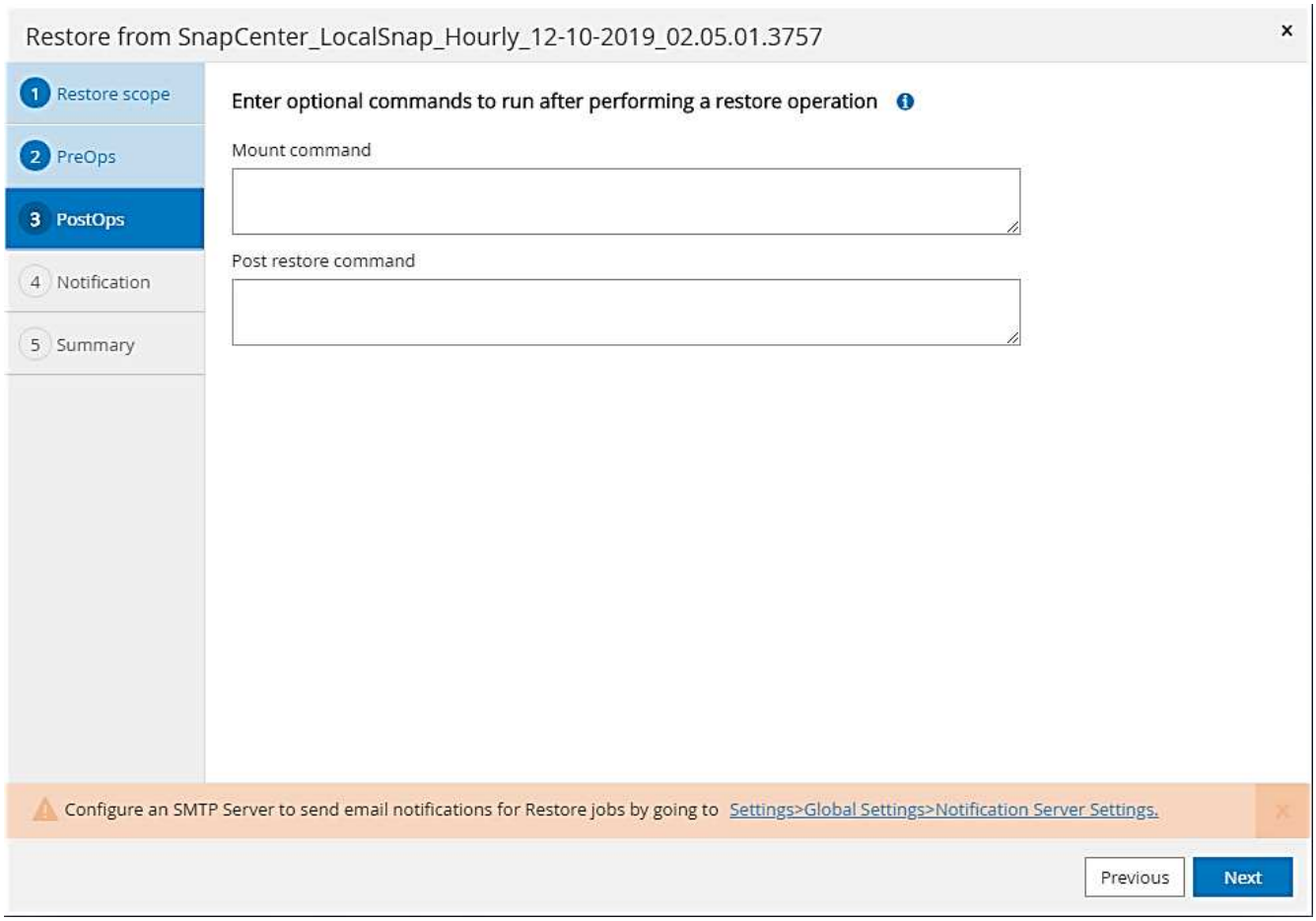
Per un ripristino a livello di file di un sistema host multiplo SAP HANA, selezionare tutti i volumi.



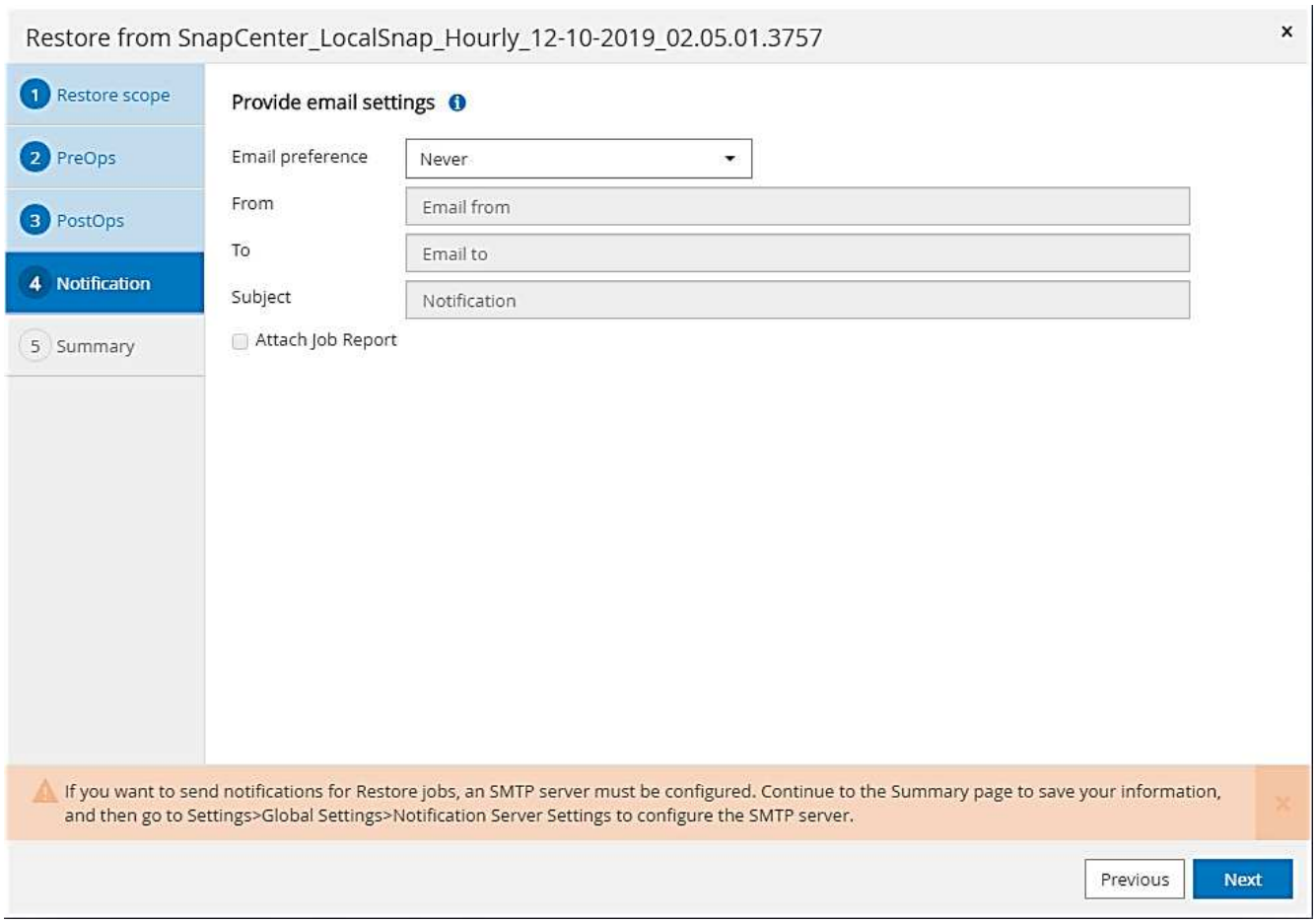
10. (Facoltativo) specificare i comandi da eseguire dal plug-in SAP HANA in esecuzione sull'host del plug-in HANA centrale. Fare clic su Avanti.



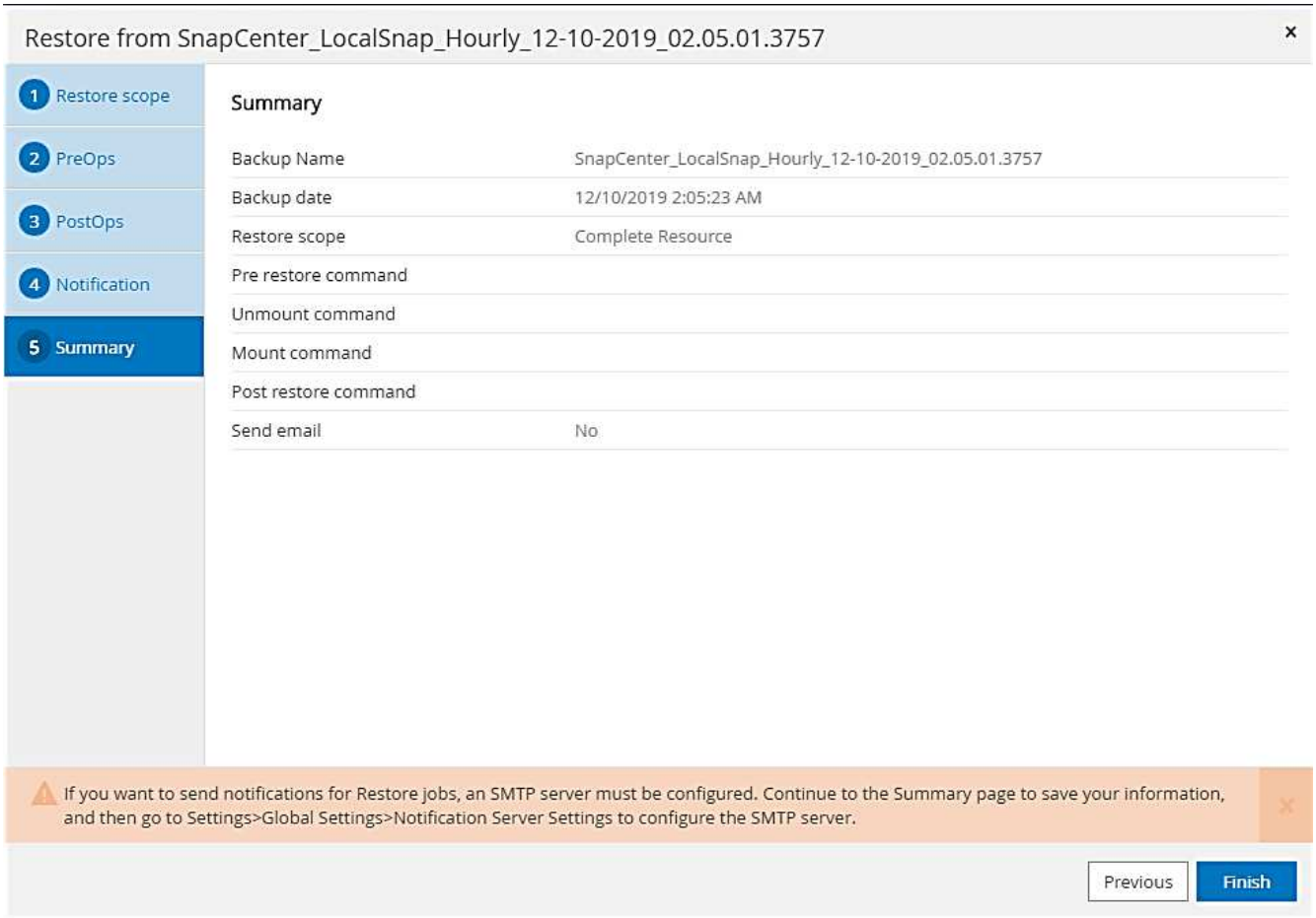
11. Specificare i comandi opzionali e fare clic su Next (Avanti).



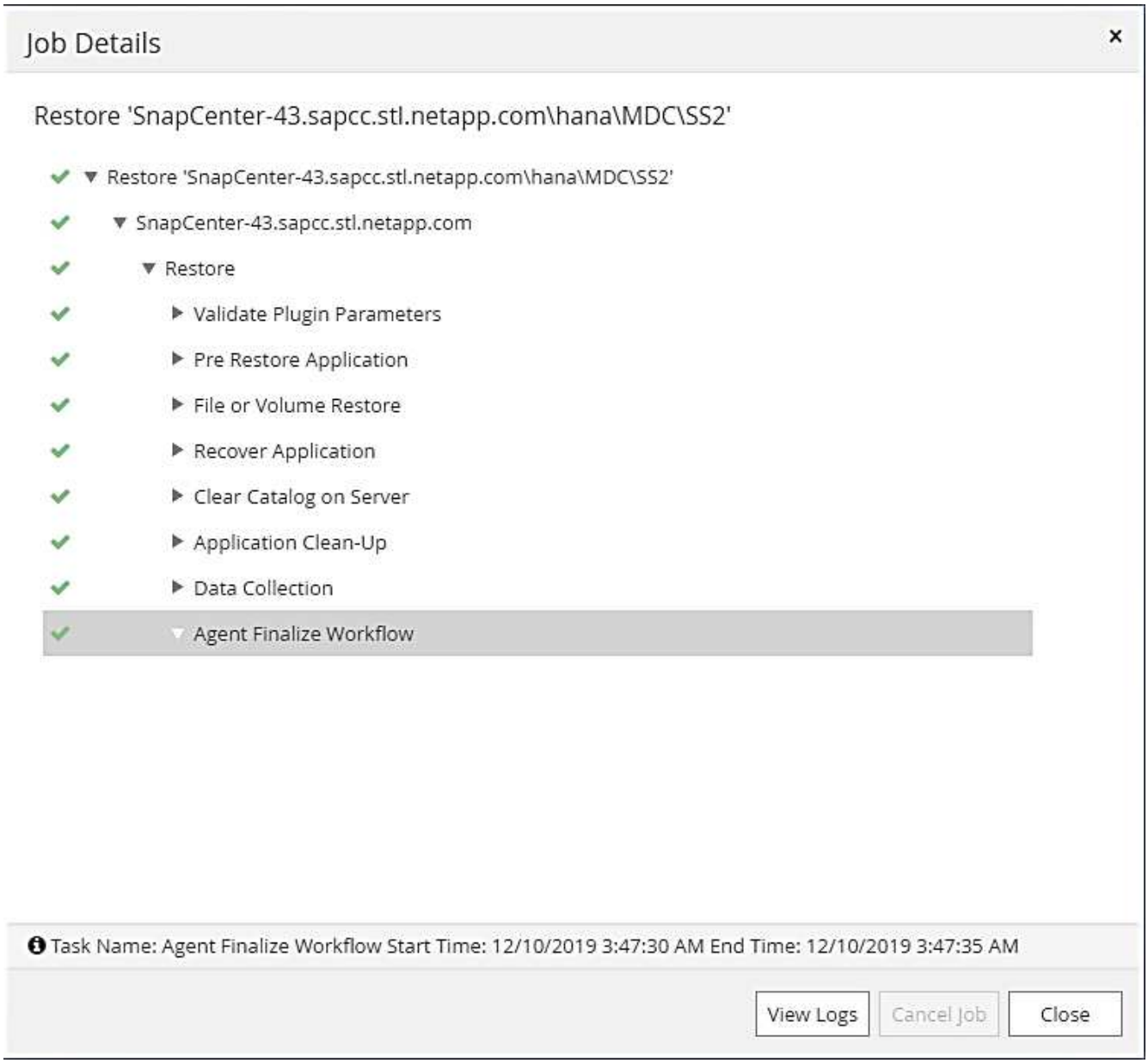
12. Specificare le impostazioni di notifica in modo che SnapCenter possa inviare un'e-mail di stato e un registro dei processi. Fare clic su Avanti.



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



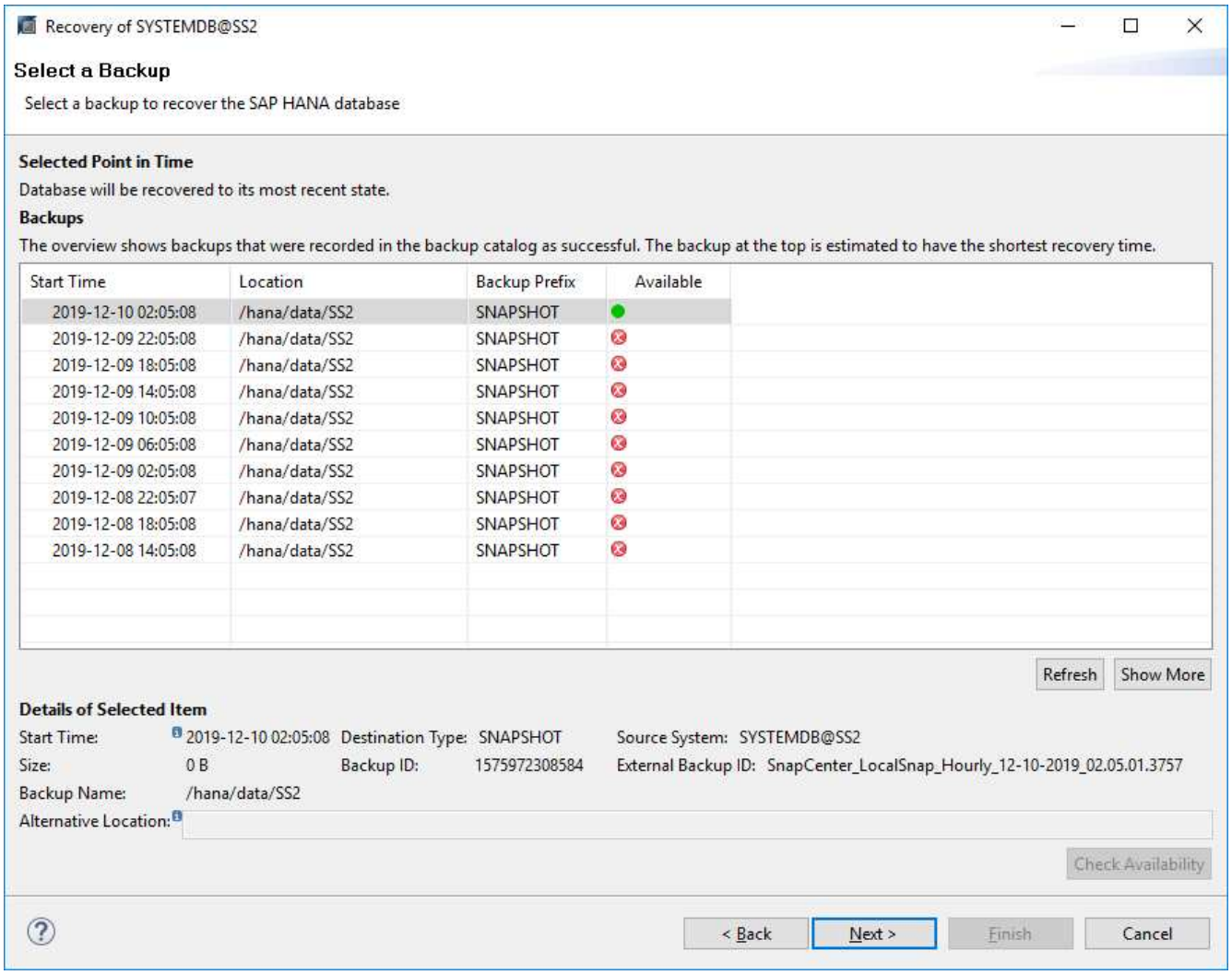
14. Il lavoro di ripristino viene avviato e il log dei lavori può essere visualizzato facendo doppio clic sulla riga del log nel riquadro delle attività.



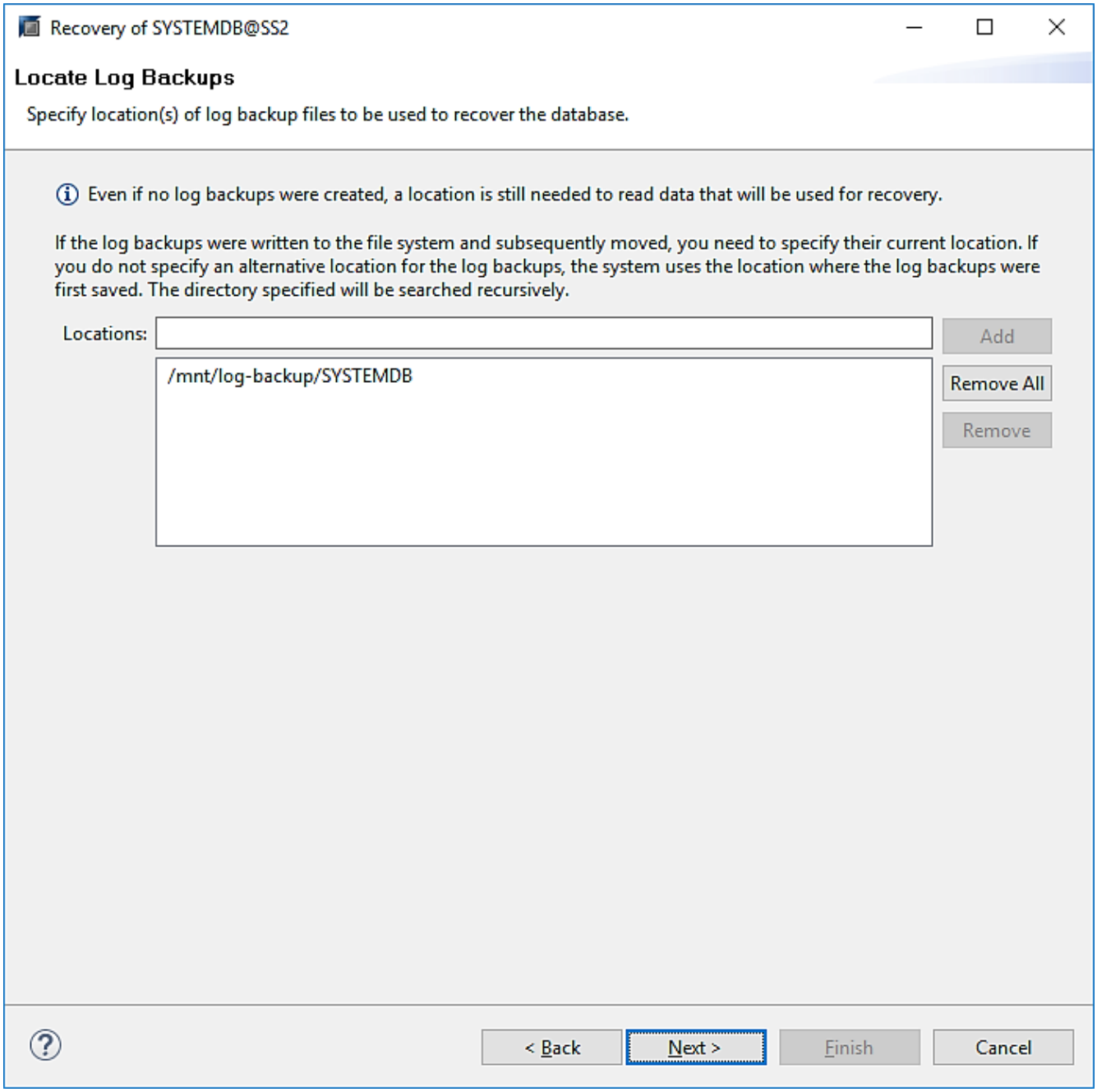
15. Attendere il completamento del processo di ripristino. Su ciascun host di database, montare tutti i volumi di dati. Nel nostro esempio, è necessario rimontare un solo volume sull'host del database.

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

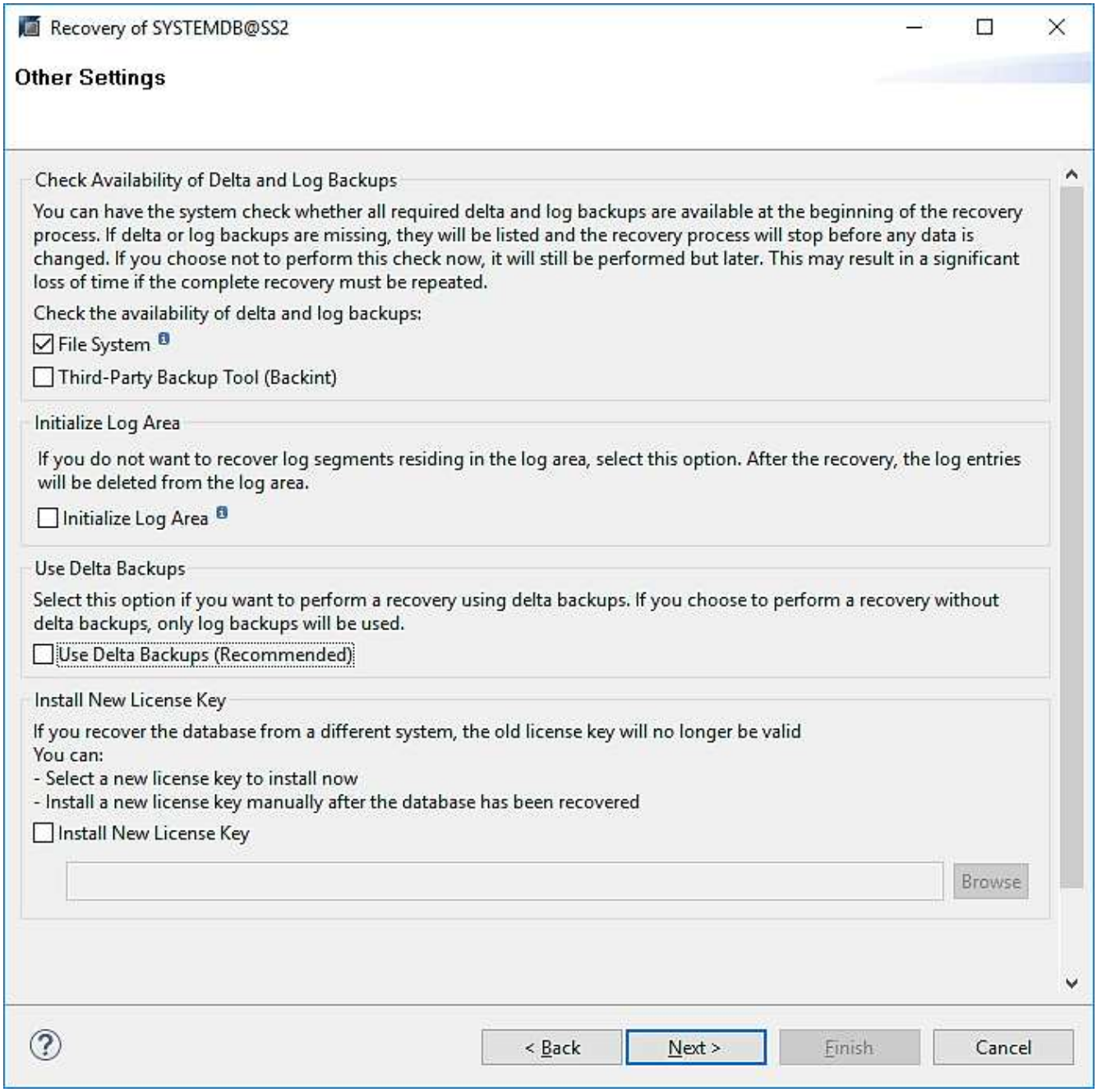
16. Accedere a SAP HANA Studio e fare clic su Refresh (Aggiorna) per aggiornare l'elenco dei backup disponibili. Il backup ripristinato con SnapCenter viene visualizzato con un'icona verde nell'elenco dei backup. Selezionare il backup e fare clic su Next (Avanti).



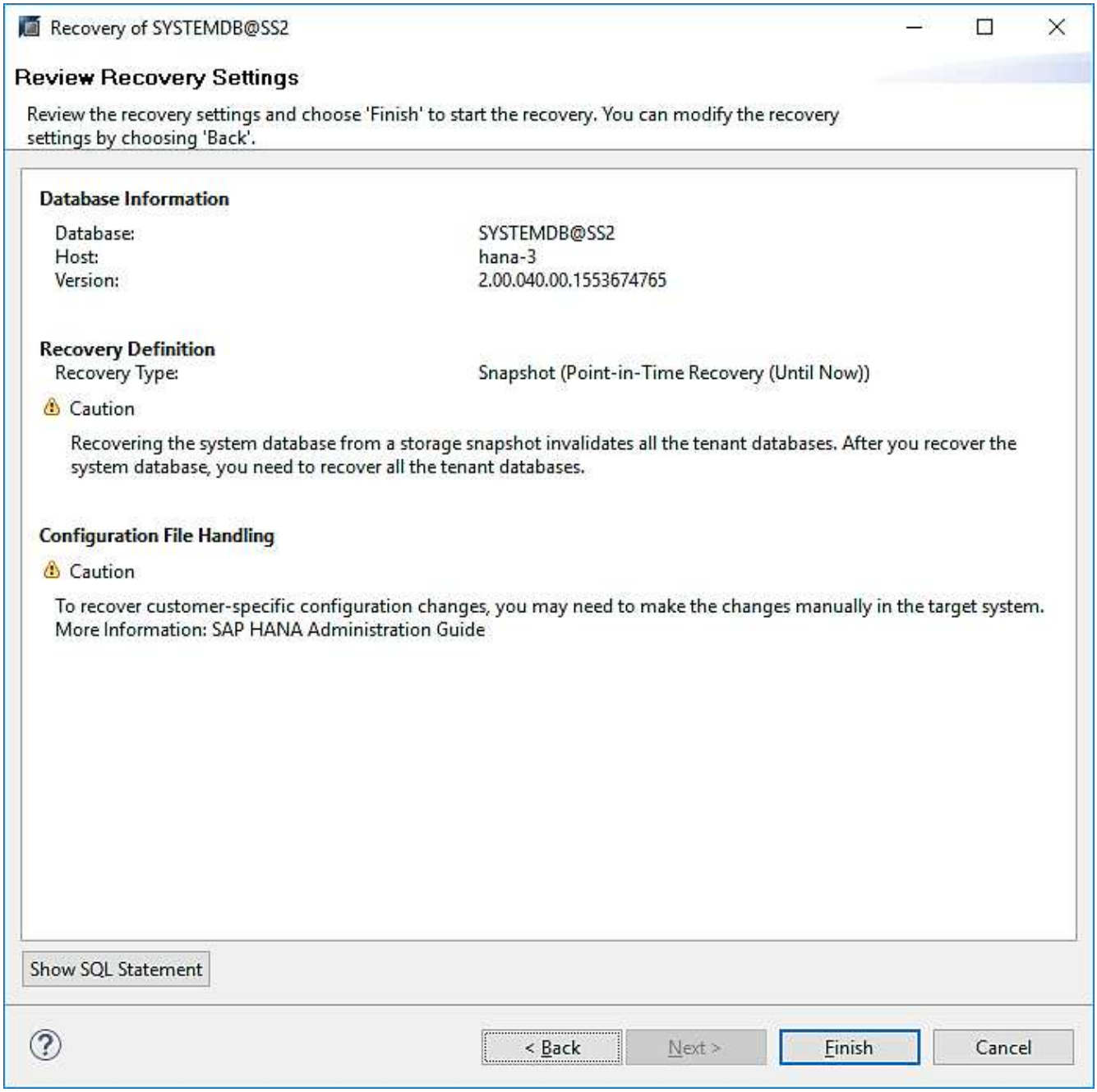
17. Fornire la posizione dei backup del registro. Fare clic su Avanti.



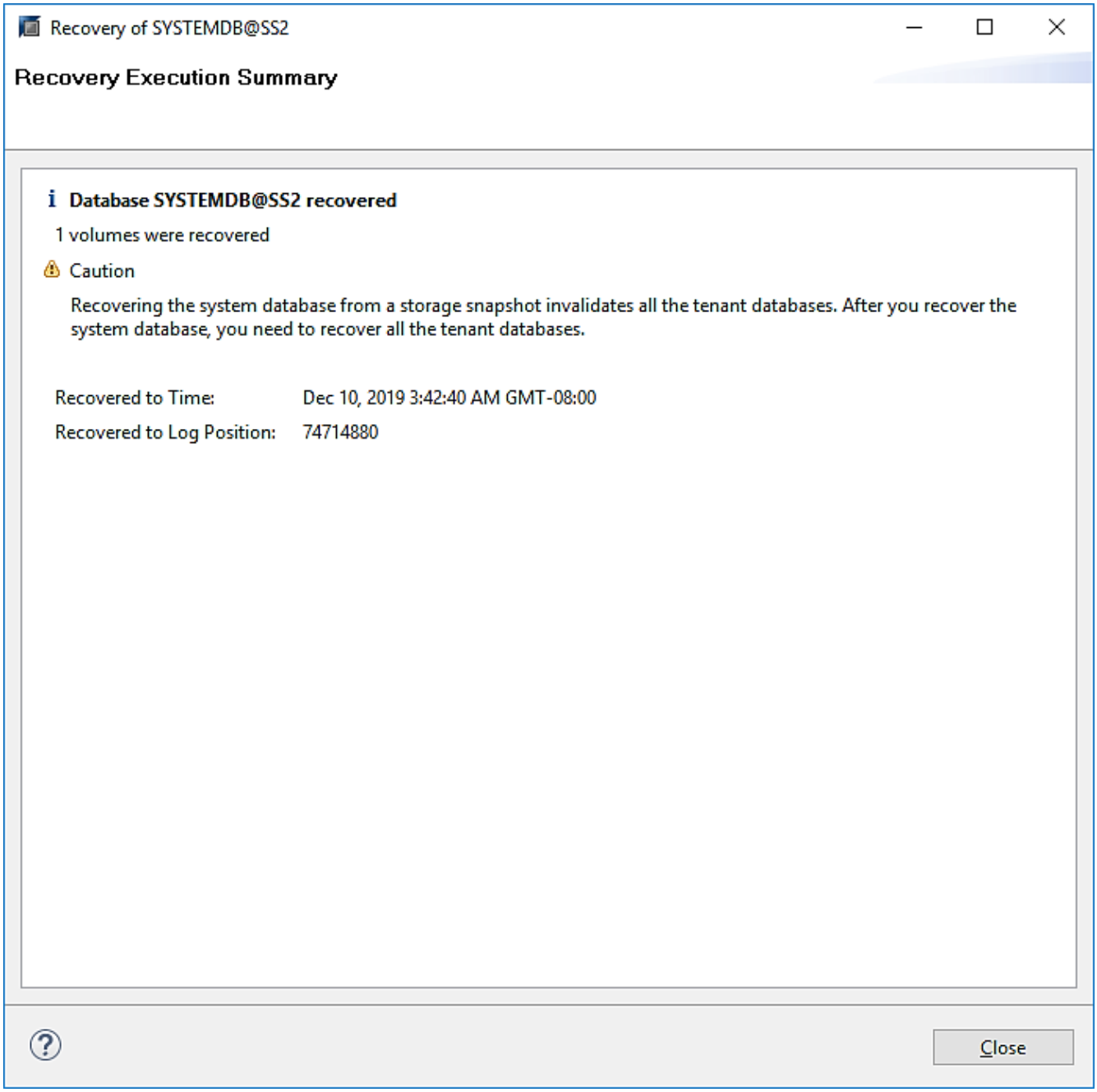
18. Selezionare le altre impostazioni desiderate. Assicurarsi che l'opzione Usa backup delta non sia selezionata. Fare clic su Avanti.



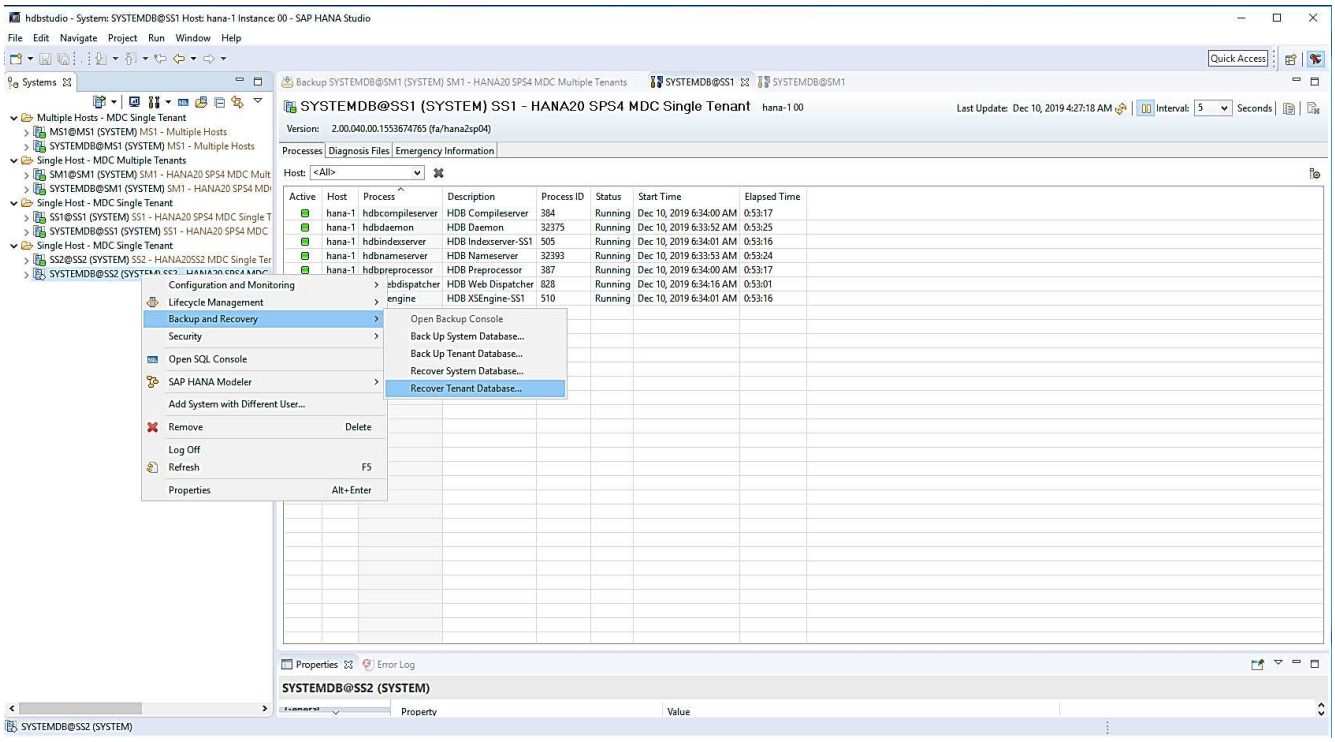
19. Rivedere le impostazioni di ripristino e fare clic su fine.



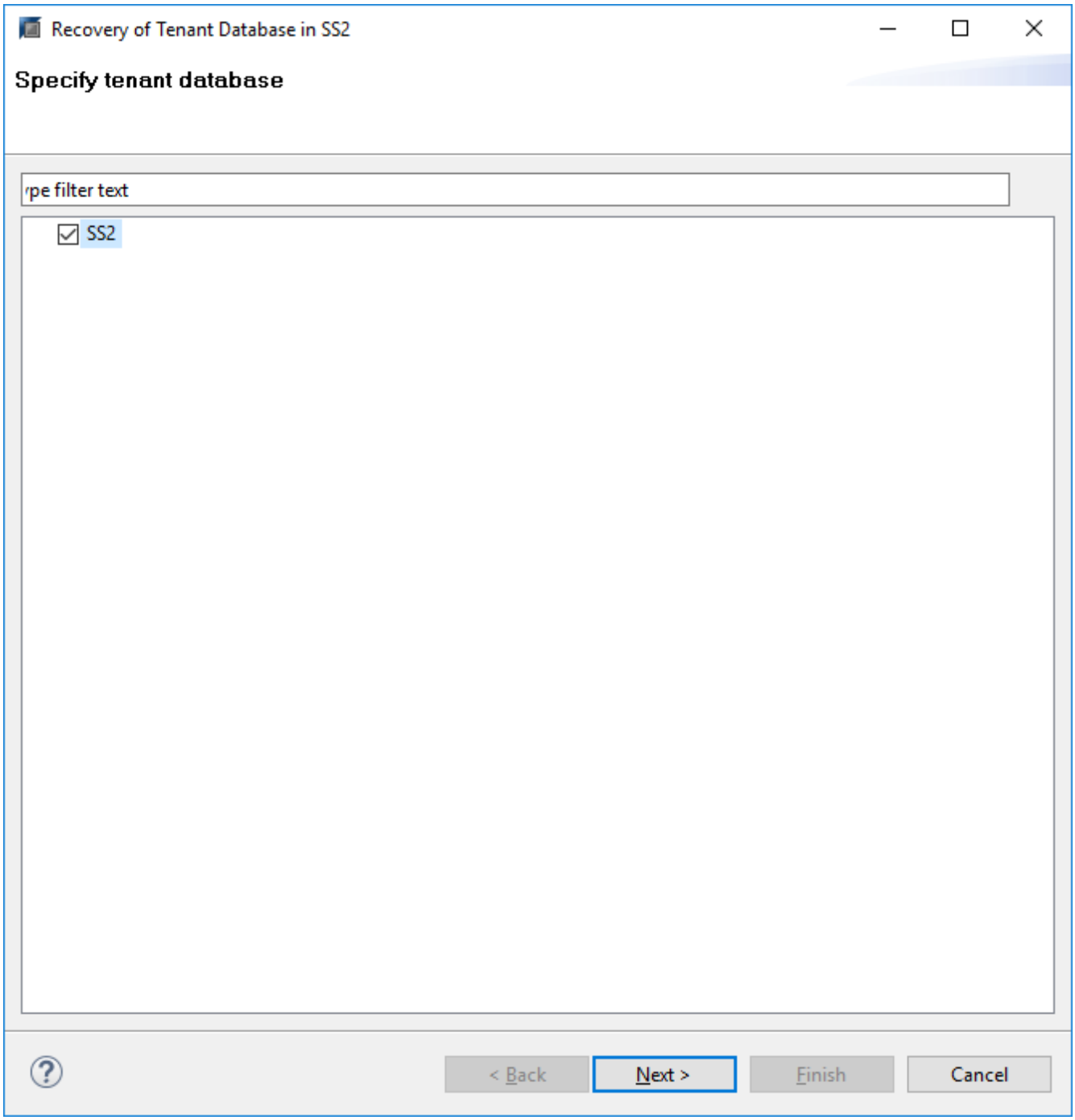
20. Viene avviato il processo di ripristino. Attendere il completamento del ripristino del database di sistema.



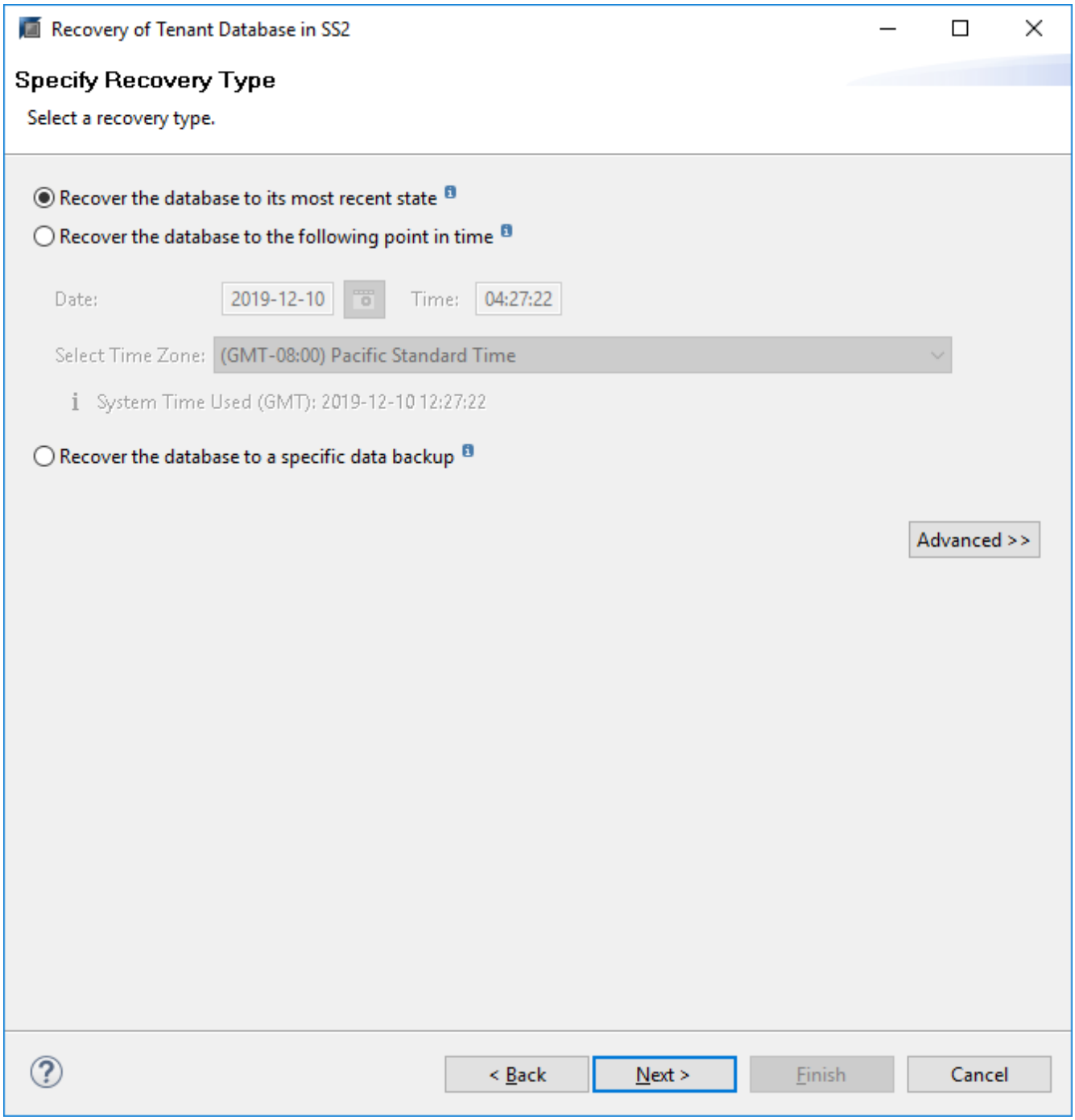
21. In SAP HANA Studio, selezionare la voce per il database di sistema e avviare Backup Recovery - Recover Tenant Database.



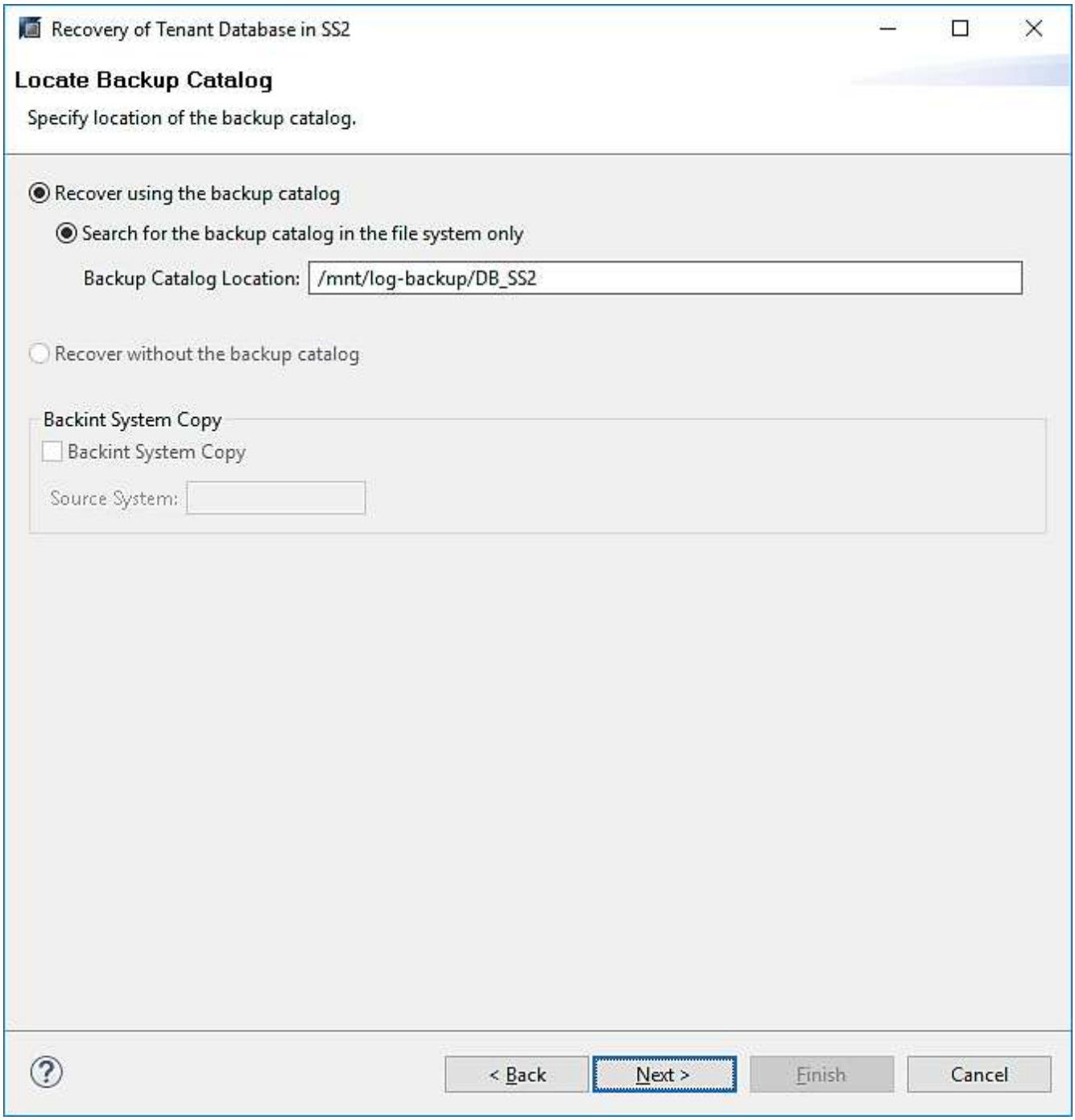
22. Selezionare il tenant da ripristinare e fare clic su Next (Avanti).



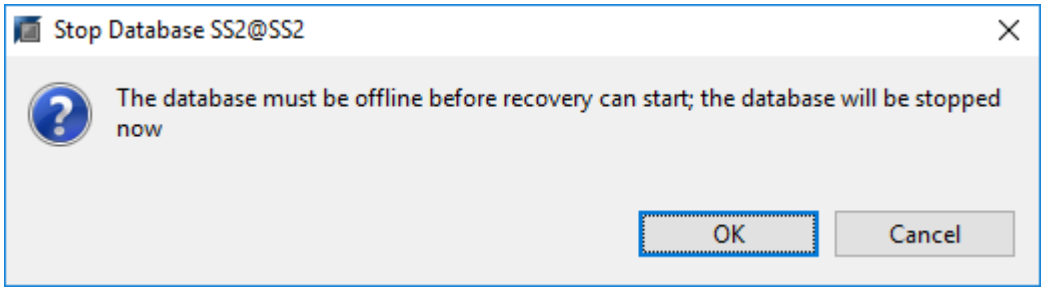
23. Specificare il tipo di ripristino e fare clic su Next (Avanti).



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

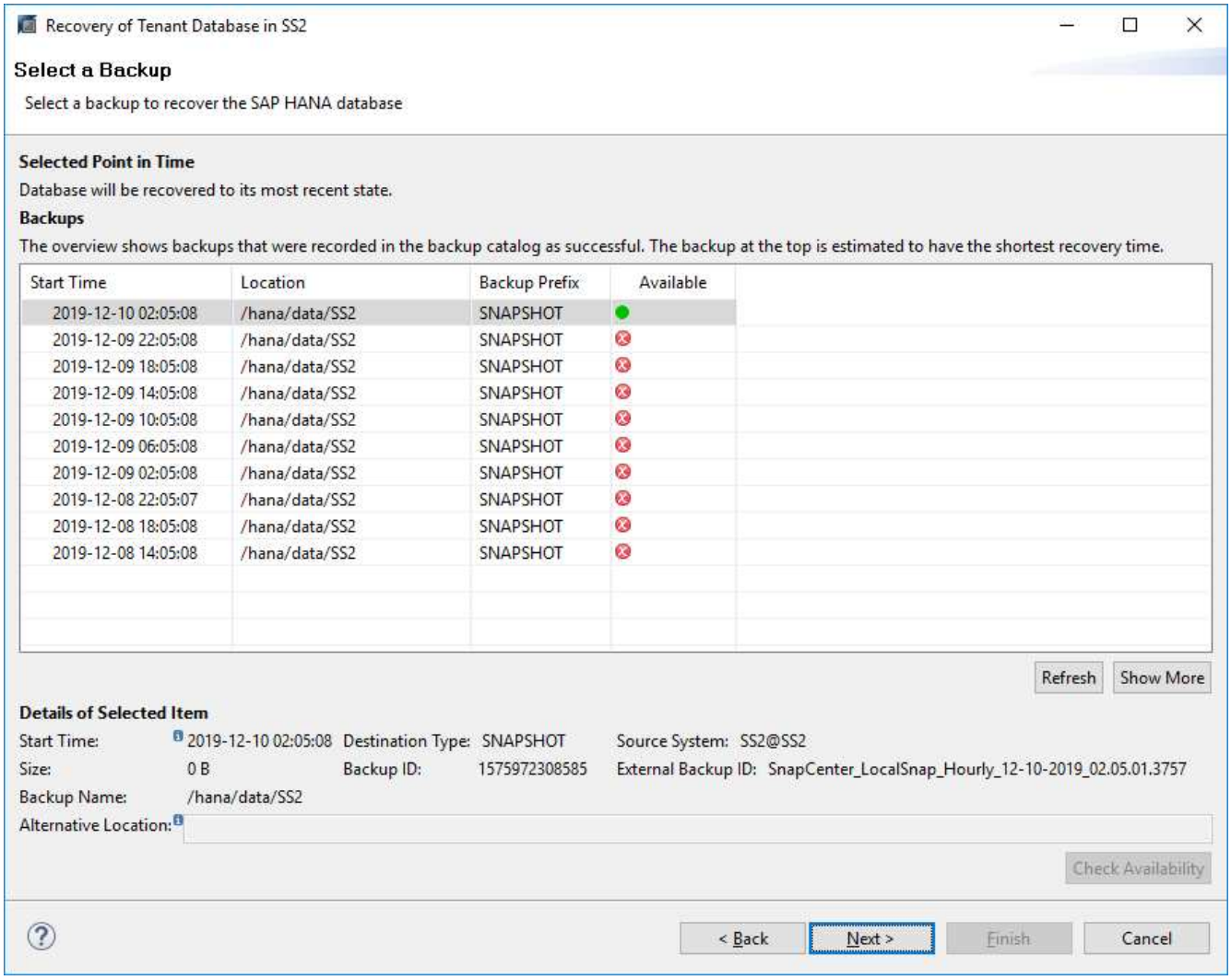


25. Verificare che il database del tenant sia offline. Fare clic su OK per continuare.

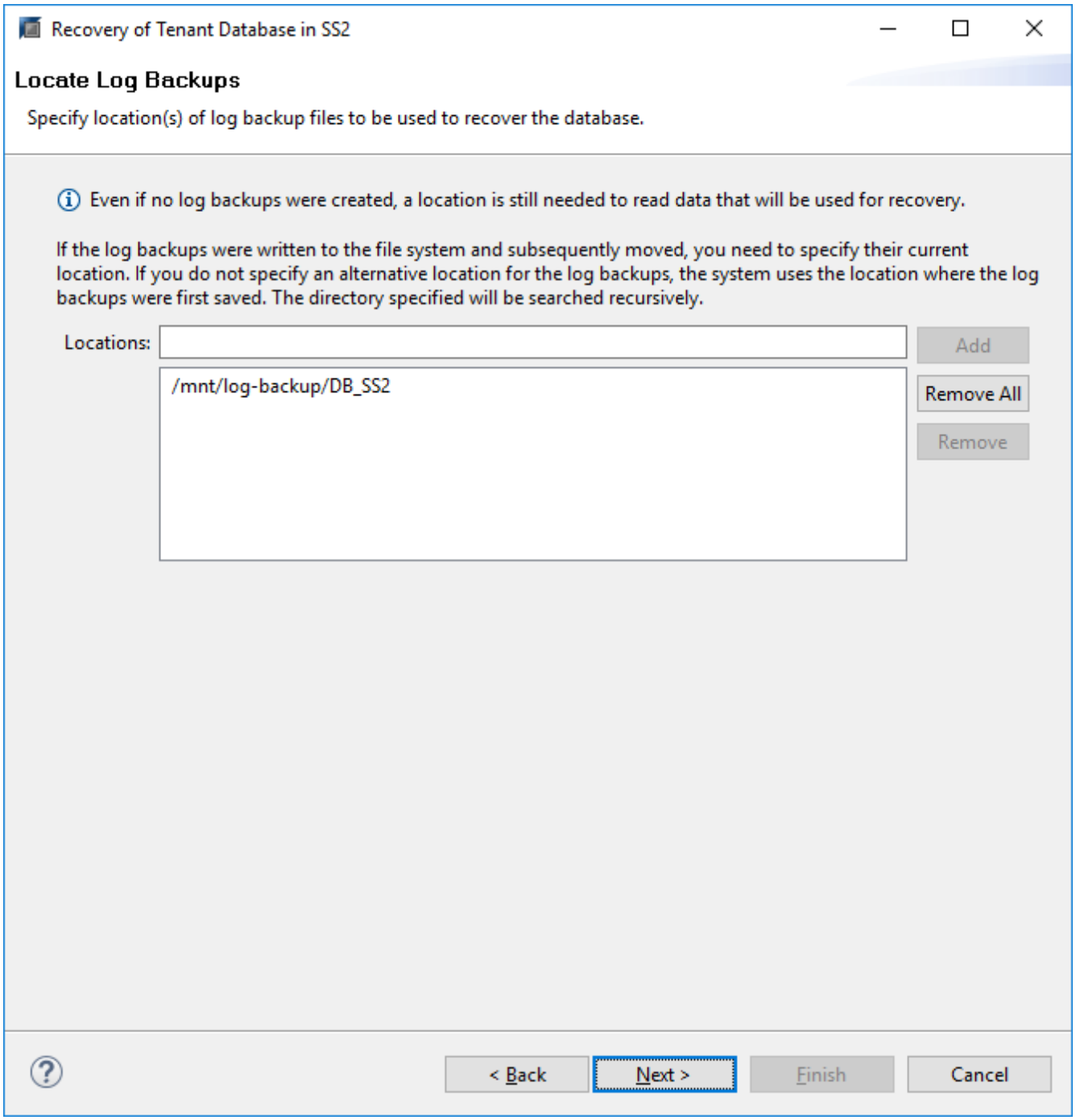


26. Poiché il ripristino del volume di dati si è verificato prima del ripristino del database di sistema, il backup del tenant è immediatamente disponibile. Selezionare il backup evidenziato in verde e fare clic su Next

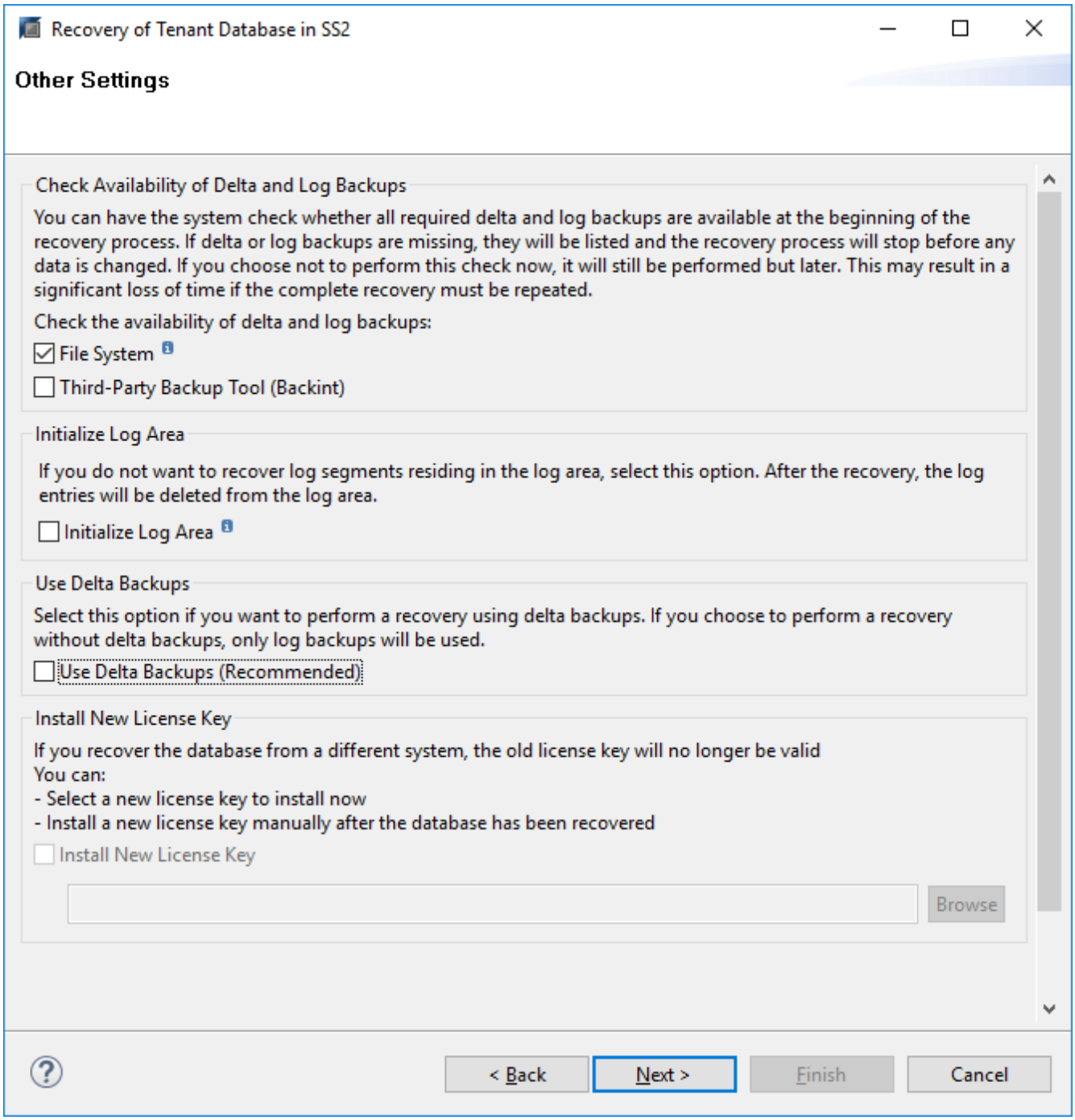
(Avanti).



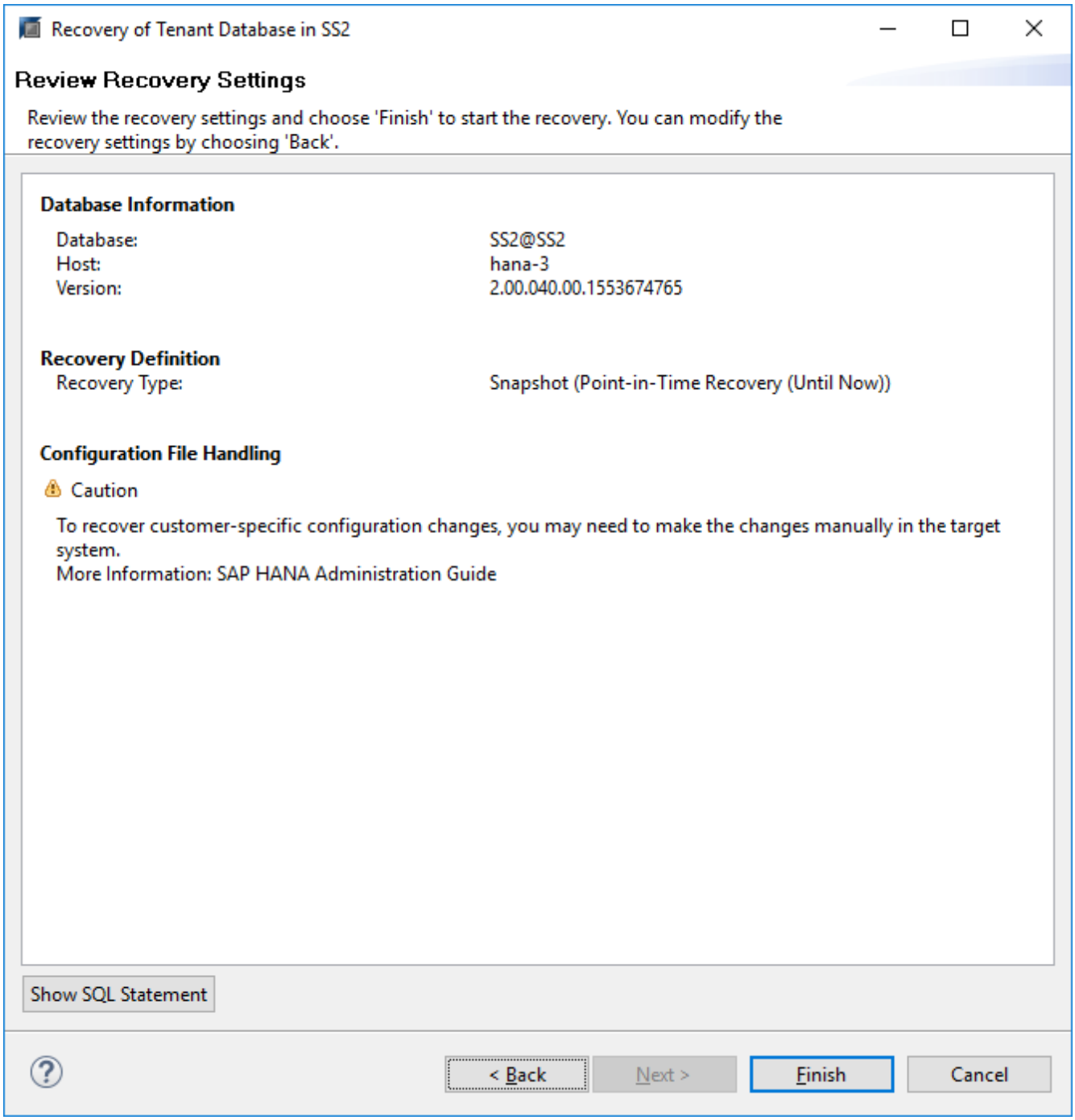
27. Confermare la posizione di backup del registro e fare clic su Next (Avanti).



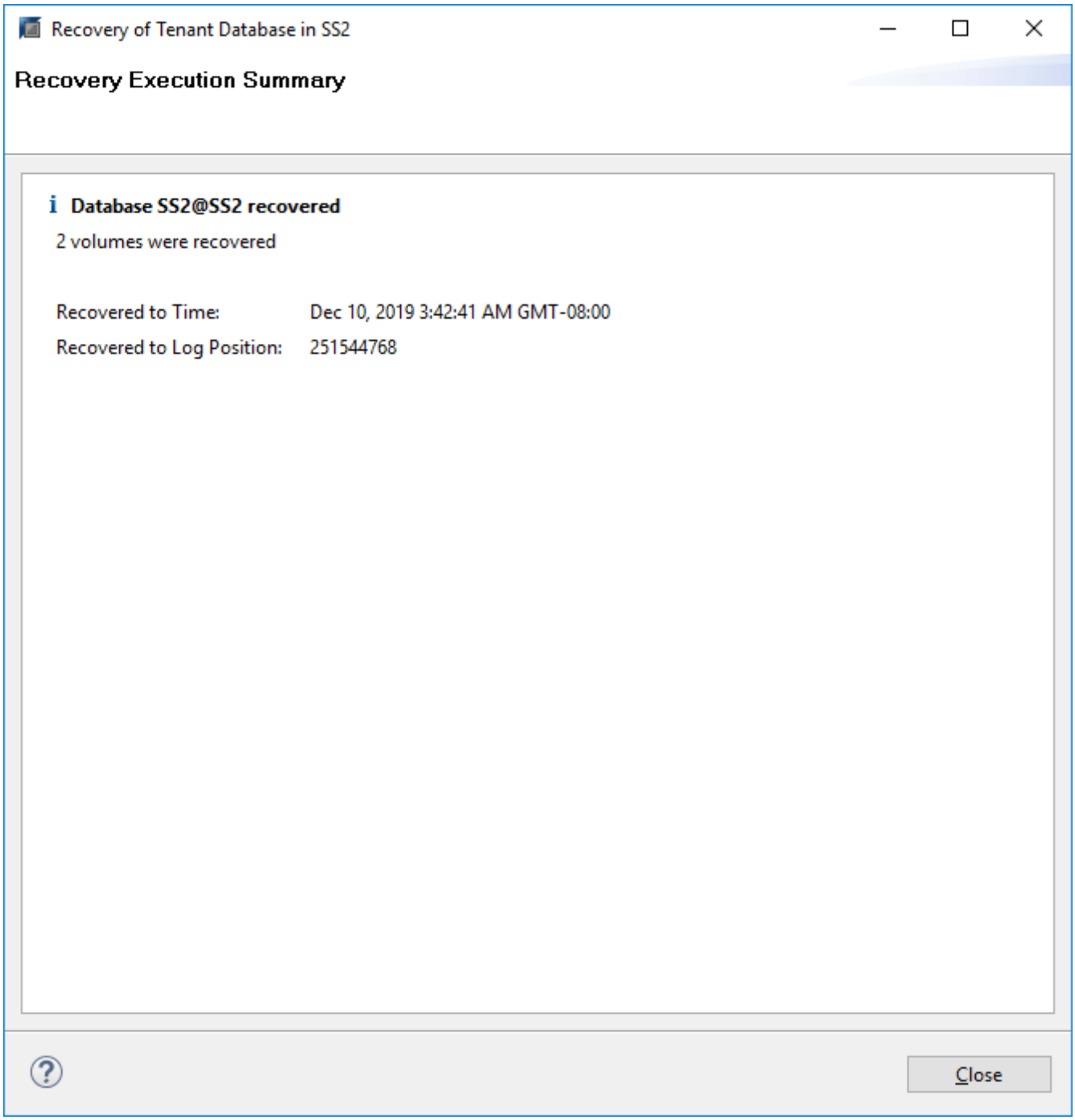
28. Selezionare le altre impostazioni desiderate. Assicurarsi che l'opzione Usa backup delta non sia selezionata. Fare clic su Avanti.



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

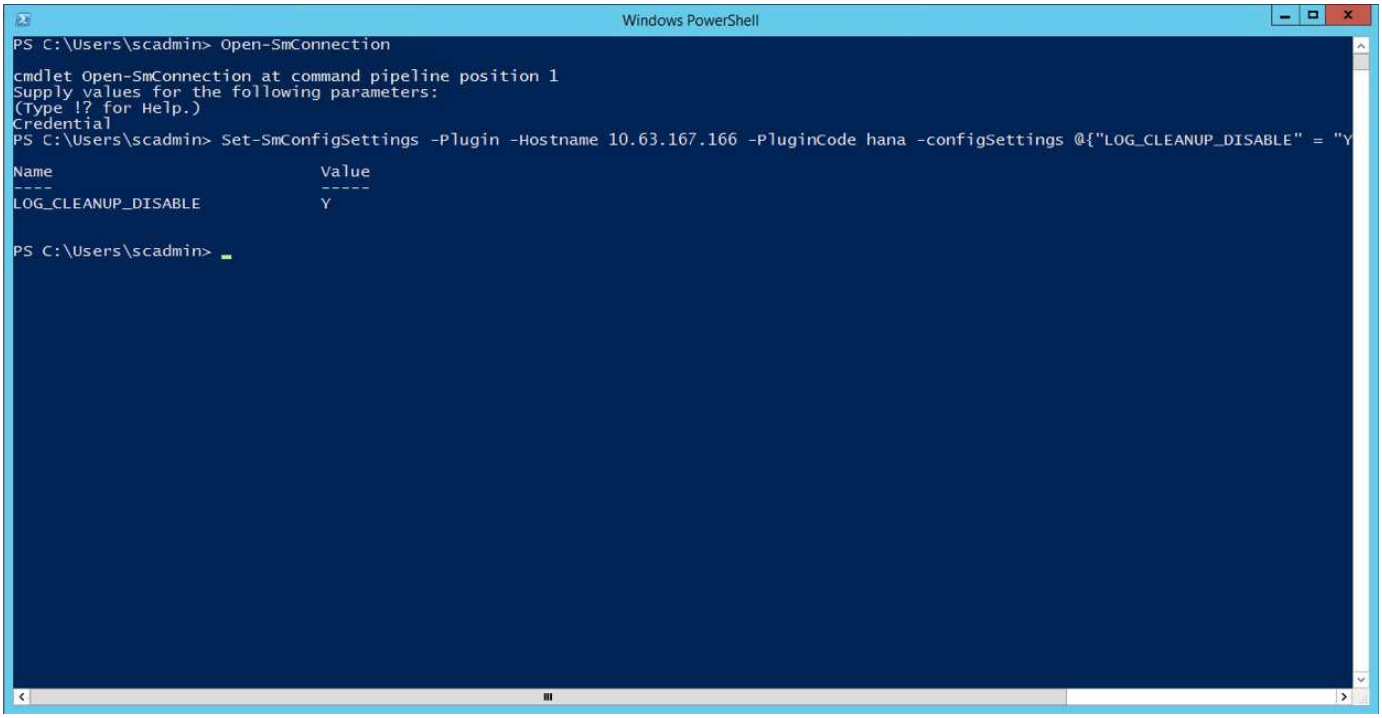
backup del log per tutte le risorse che utilizzano questo host plug-in SAP HANA come host di comunicazione:

- 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

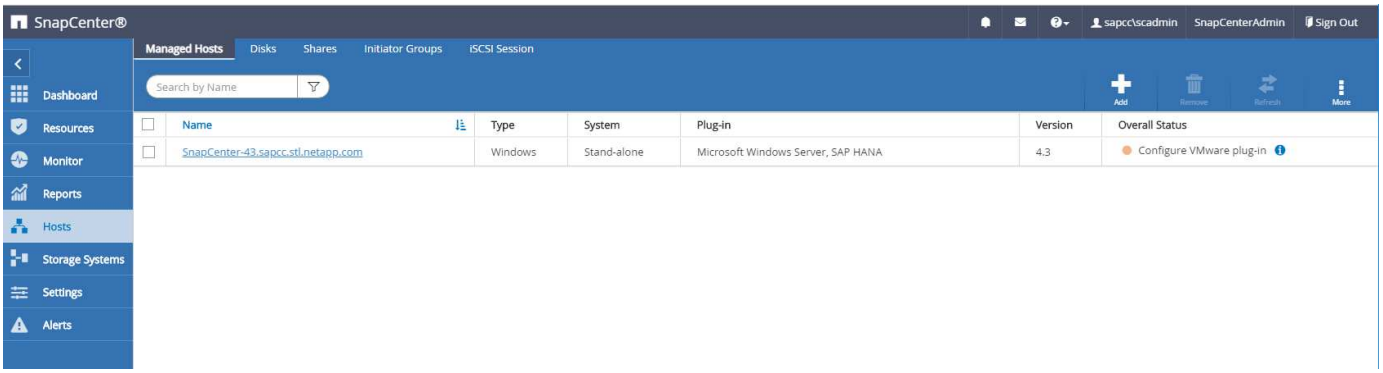
Una seconda opzione per configurare queste impostazioni consiste nell'utilizzare un comando PowerShell di SnapCenter.

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

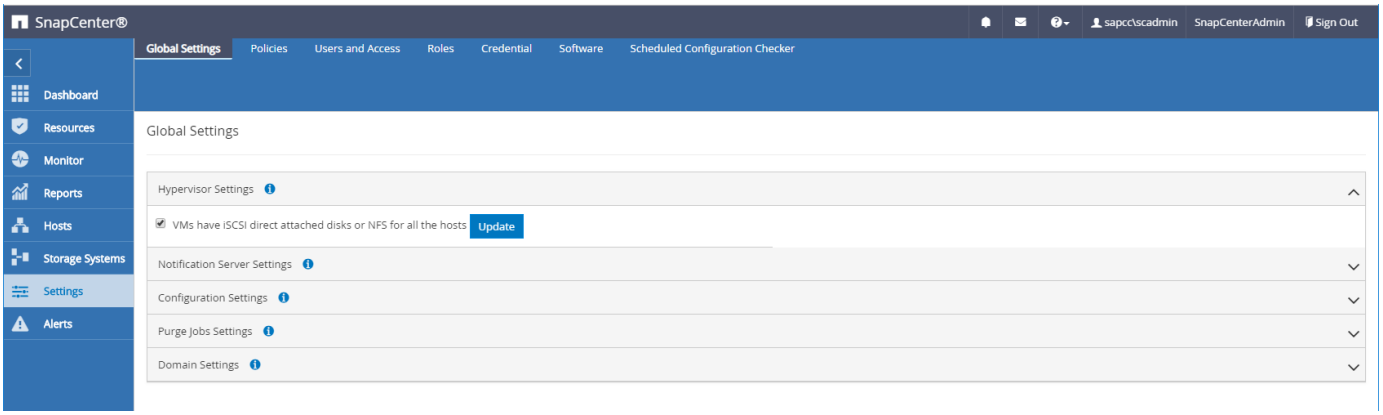
SnapCenter rileva se il plug-in SAP HANA è installato in un ambiente virtualizzato. Potrebbe trattarsi di un ambiente VMware o di un'installazione SnapCenter presso un provider di cloud pubblico. In questo caso, SnapCenter visualizza un avviso per la configurazione dell'hypervisor, come illustrato nella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

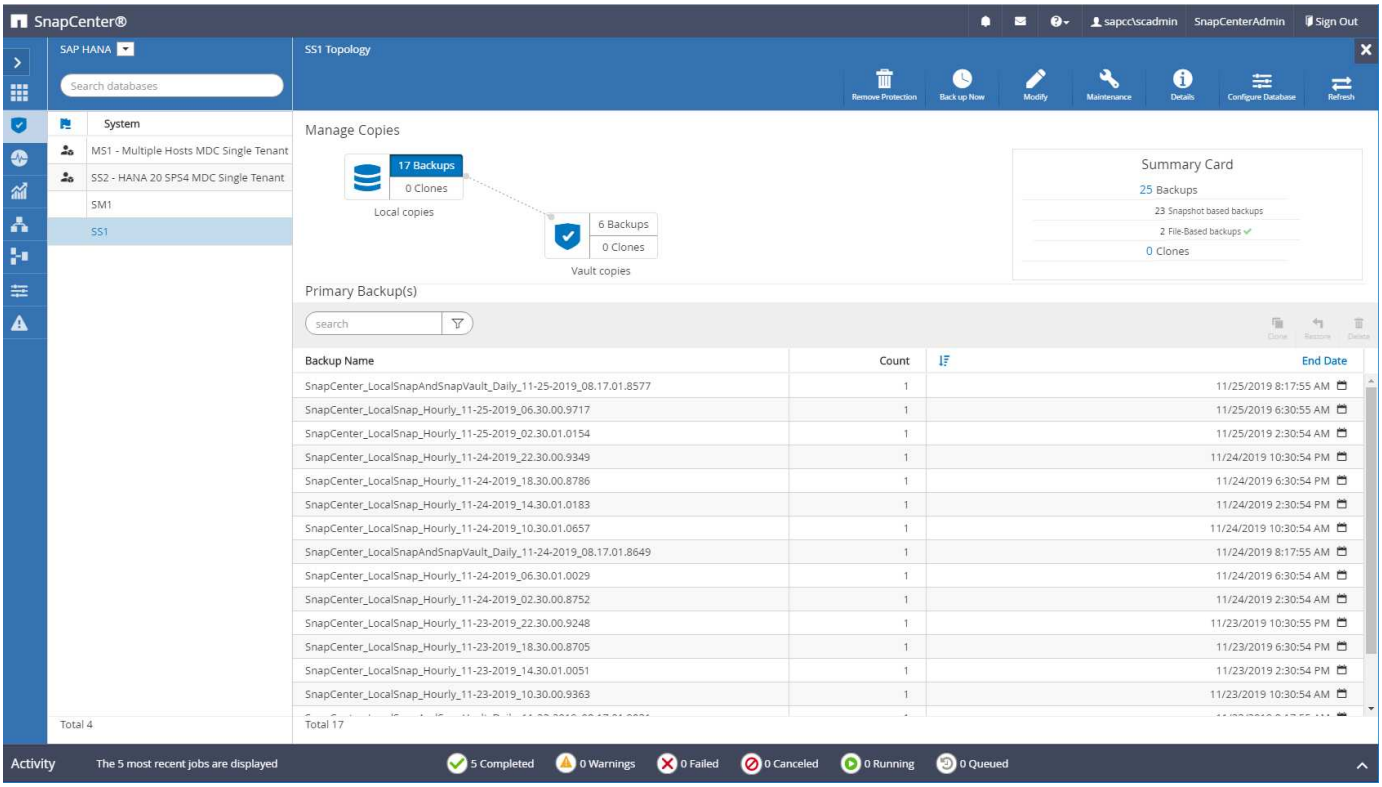
Fino al termine della pulizia pianificata, SAP HANA e SnapCenter potrebbero ancora mostrare i backup che sono già stati eliminati dallo storage di backup off-site.

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

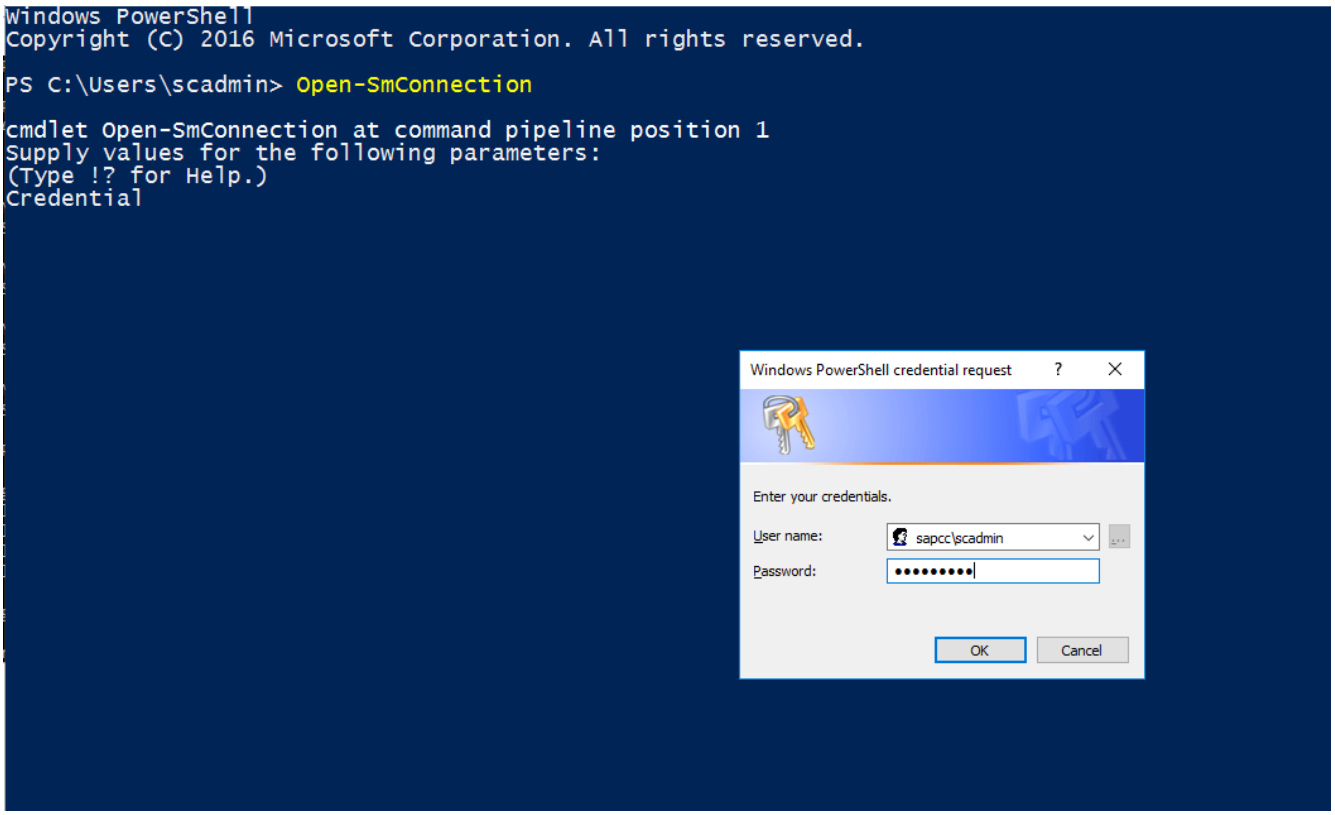
Nella vista della topologia di una risorsa, SnapCenter visualizza i backup sullo storage di backup off-site quando si selezionano i backup secondari, come illustrato nella seguente schermata. SnapCenter esegue un'operazione di pulizia con l'icona Refresh (Aggiorna) per sincronizzare i backup di questa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

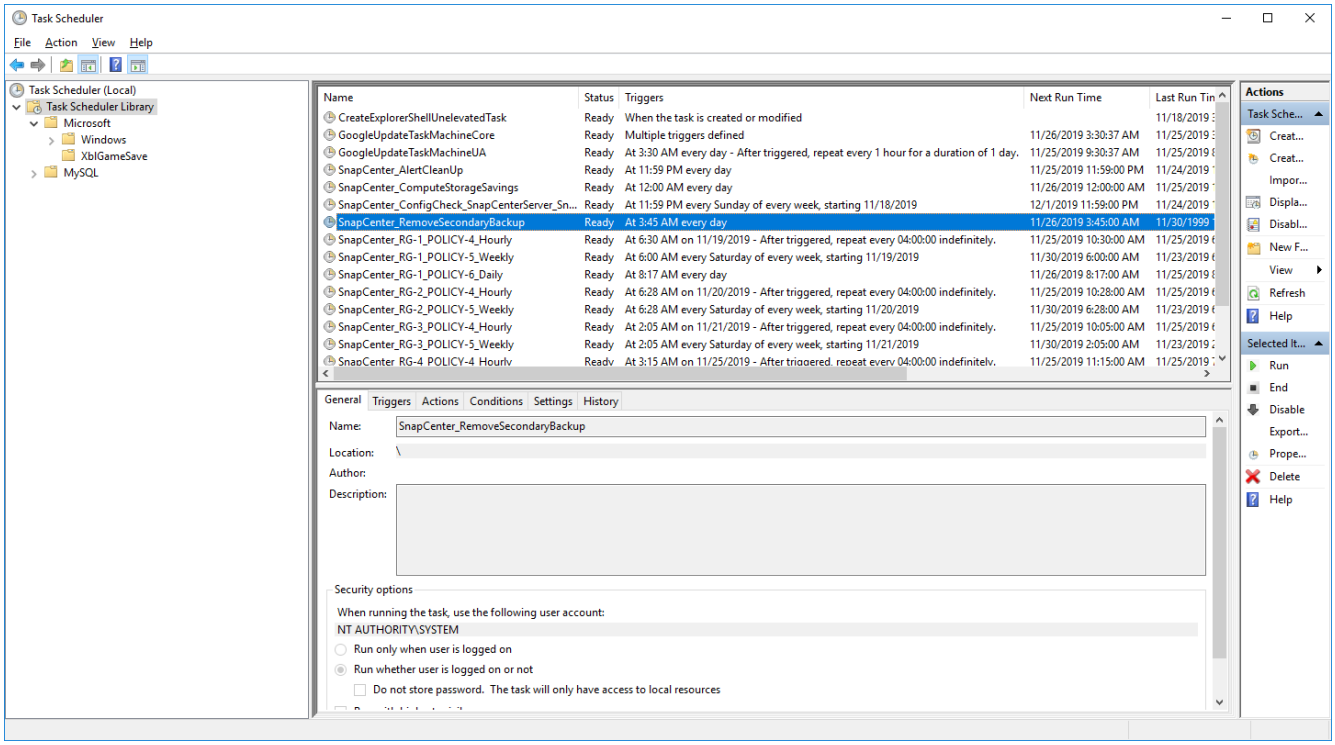
1. Avviare una finestra di comando PowerShell sul server SnapCenter.
2. Aprire la connessione al server SnapCenter e immettere le credenziali di amministratore SnapCenter nella finestra di accesso.



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

  "Automazione di copie del sistema SAP con SnapCenter"

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

  "Replica di sistema, backup e recovery per SAP HANA con SnapCenter"

- 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.

Data Protection e high Availability di SAP HANA con SnapCenter, SnapMirror Active Sync e VMware Metro Storage Cluster

Data Protection e high Availability di SAP HANA con SnapCenter, SnapMirror Active Sync e VMware Metro Storage Cluster

Questo documento fornisce Best practice per la protezione dei dati con SnapCenter in un ambiente VMware combinato con SnapMirror Active Sync come soluzione ad alta disponibilità per le risorse di storage HANA.

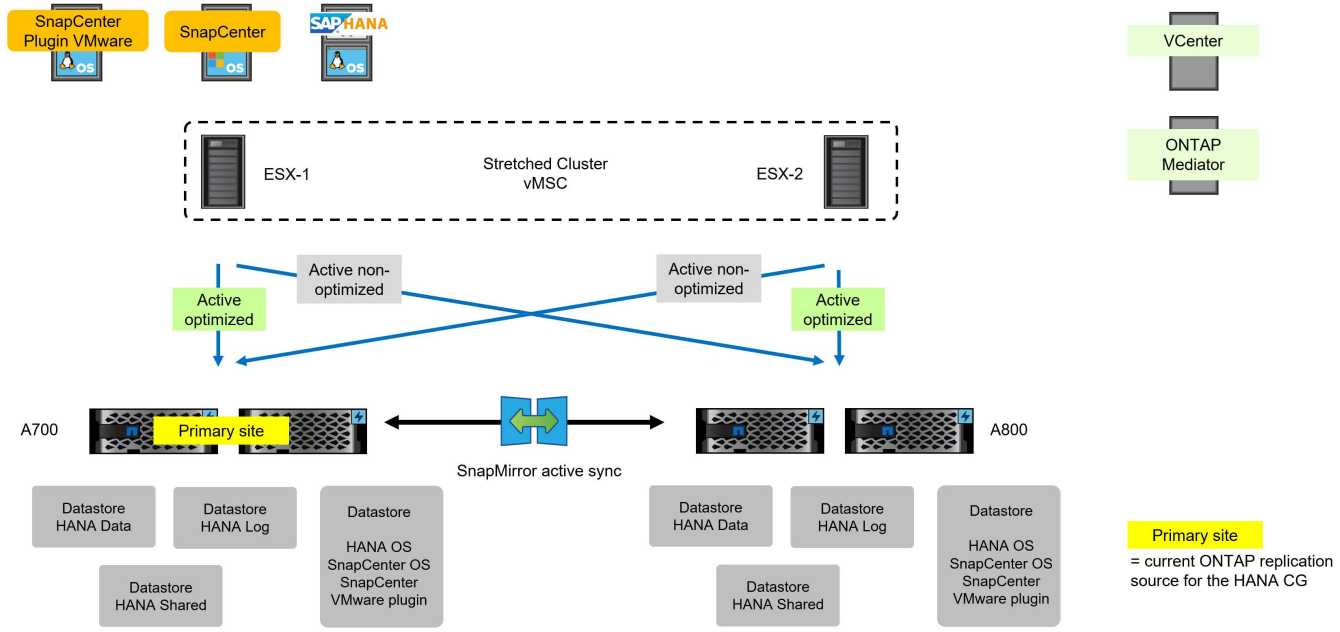
Autore: Nils Bauer, NetApp

Scopo del presente documento

Il documento non intende essere una descrizione passo passo di come configurare l'ambiente completo, ma tratterà i concetti e i dettagli relativi a:

- Configurazione dei sistemi SAP HANA con VMware VMFS
- Configurazione Active Sync di SnapMirror per SAP HANA
- Configurazione di SnapCenter per HANA su VMware con VMFS
- Configurazione di SnapCenter per la sincronizzazione attiva di SnapMirror
- Operazioni SnapCenter con HANA su VMware e SnapMirror Active Sync

Ci concentreremo su una configurazione vMSC (VMware Metro Storage Cluster) che utilizza una configurazione ad accesso uniforme della sincronizzazione attiva SnapMirror, come illustrato nella figura seguente, ma toccheremo anche in breve le configurazioni di accesso non uniformi e bare metal.



Panoramica sull'high Availability di SAP HANA

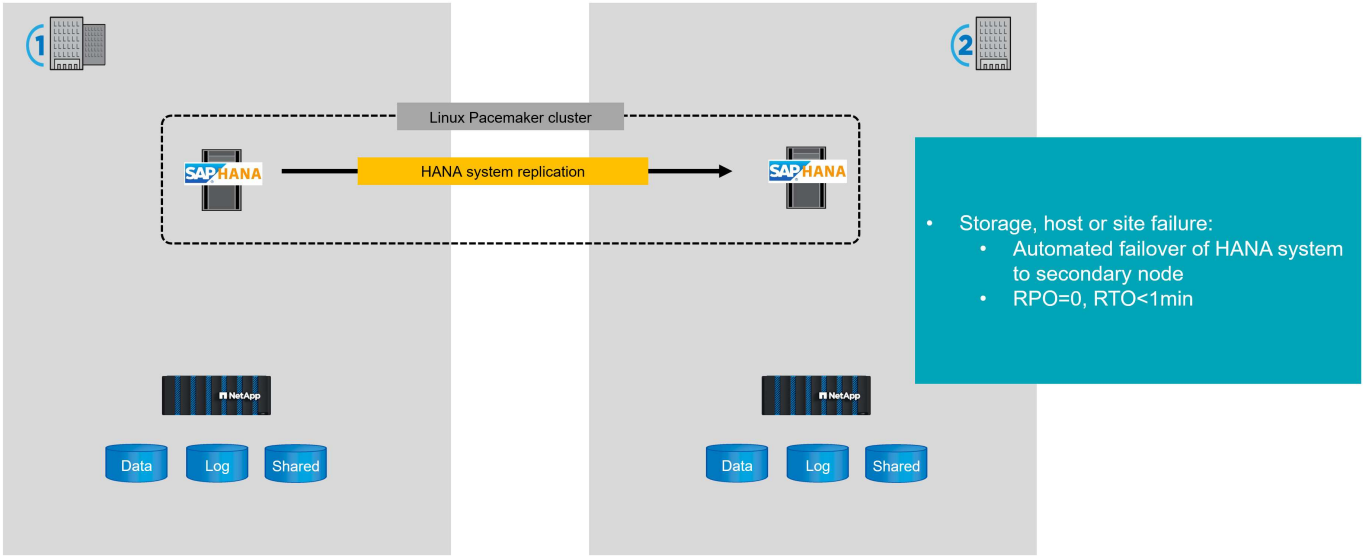
Questo capitolo offre una panoramica delle opzioni di alta disponibilità per SAP HANA confrontando la replica sul layer applicativo con la replica dello storage.

Replica del sistema SAP HANA (HSR)

La replica del sistema SAP HANA offre una modalità operativa in cui i dati vengono replicati in modo sincrono, precaricati in memoria e aggiornati costantemente sull'host secondario. Questa modalità attiva valori RTO molto bassi, pari a circa 1 minuto o meno, ma richiede anche un server dedicato che viene utilizzato solo per ricevere i dati di replica dal sistema di origine. A causa del basso tempo di failover, spesso la replica del sistema SAP HANA viene utilizzata anche per operazioni di manutenzione near-zero-downtime, come gli upgrade del software HANA. Le soluzioni cluster pacemaker Linux vengono generalmente utilizzate per automatizzare le operazioni di failover.

In caso di guasto nel sito primario, nello storage, nell'host o nel sito completo, il sistema HANA esegue automaticamente il failover sul sito secondario controllato dal cluster Linux Pacemaker.

Per una descrizione completa di tutte le opzioni di configurazione e degli scenari di replica, vedere "Replica di sistema SAP HANA | Portale Guida SAP".



Sincronizzazione attiva NetApp SnapMirror

SnapMirror Active Sync consente ai servizi di business di continuare a funzionare anche in caso di guasto completo del sito, supportando le applicazioni per il failover in modo trasparente con una copia secondaria. Non sono richiesti interventi manuali o script personalizzati per attivare un failover con la sincronizzazione attiva di SnapMirror. La sincronizzazione attiva SnapMirror è supportata su cluster AFF, cluster ASA (All-Flash SAN Array) e C-Series (AFF o ASA). La sincronizzazione attiva di SnapMirror protegge le applicazioni con LUN iSCSI o FCP.

A partire da ONTAP 9.15.1, la sincronizzazione attiva SnapMirror supporta una funzionalità Active/Active simmetrica. Active/Active simmetrico consente operazioni di i/o in lettura e scrittura da entrambe le copie di una LUN protetta con replica sincrona bidirezionale, in modo che entrambe le copie LUN possano servire le operazioni di i/o a livello locale.

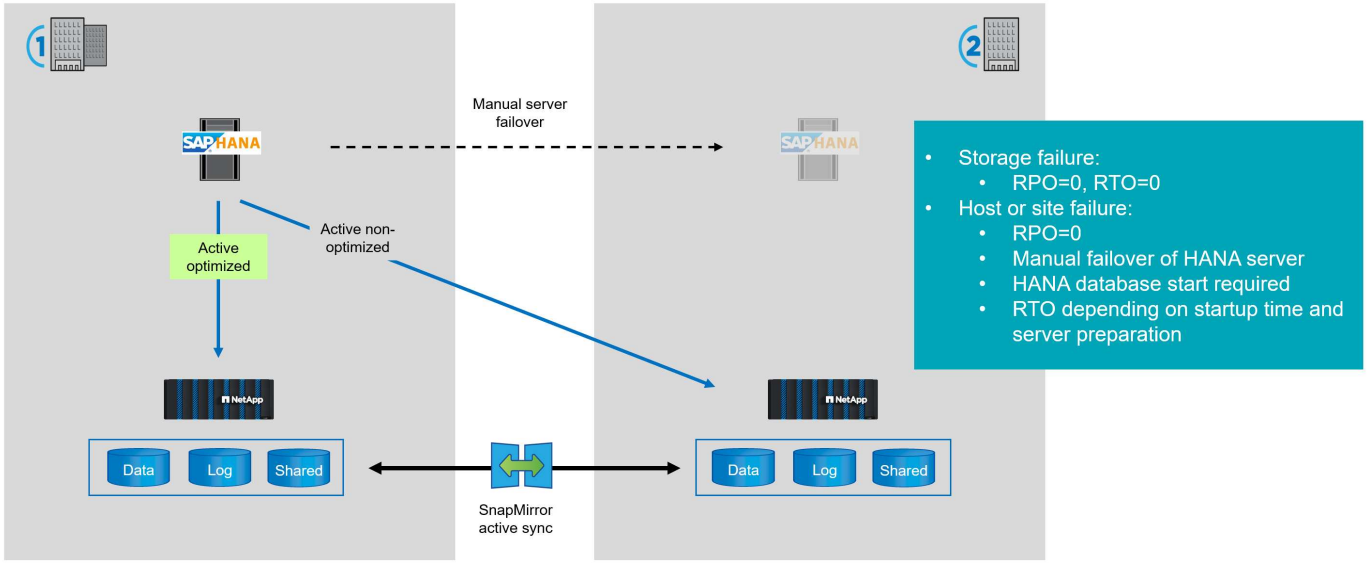
Ulteriori informazioni sono disponibili all'indirizzo "Panoramica della sincronizzazione attiva di SnapMirror in ONTAP".

Bare metal HANA

Quando esegui SAP HANA su un server bare metal, puoi utilizzare la sincronizzazione attiva di SnapMirror per fornire una soluzione storage ad alta disponibilità. I dati vengono replicati in modo sincrono, fornendo quindi un RPO=0.

In caso di guasto allo storage, il sistema HANA accederà in modo trasparente alla copia con mirroring nel sito secondario, utilizzando il secondo percorso FCP, fornendo un RTO=0.

In caso di errore di un host o di un sito completo, è necessario fornire un nuovo server nel sito secondario per accedere ai dati dall'host guasto. Si tratta in genere di un sistema di test o di controllo qualità delle stesse dimensioni della produzione che verrà ora arrestato e utilizzato per eseguire il sistema di produzione. Dopo che le LUN del sito secondario sono state connesse al nuovo host, è necessario avviare il database HANA. L'RTO totale dipende quindi dal tempo necessario per il provisioning dell'host e dai tempi di avvio del database HANA.

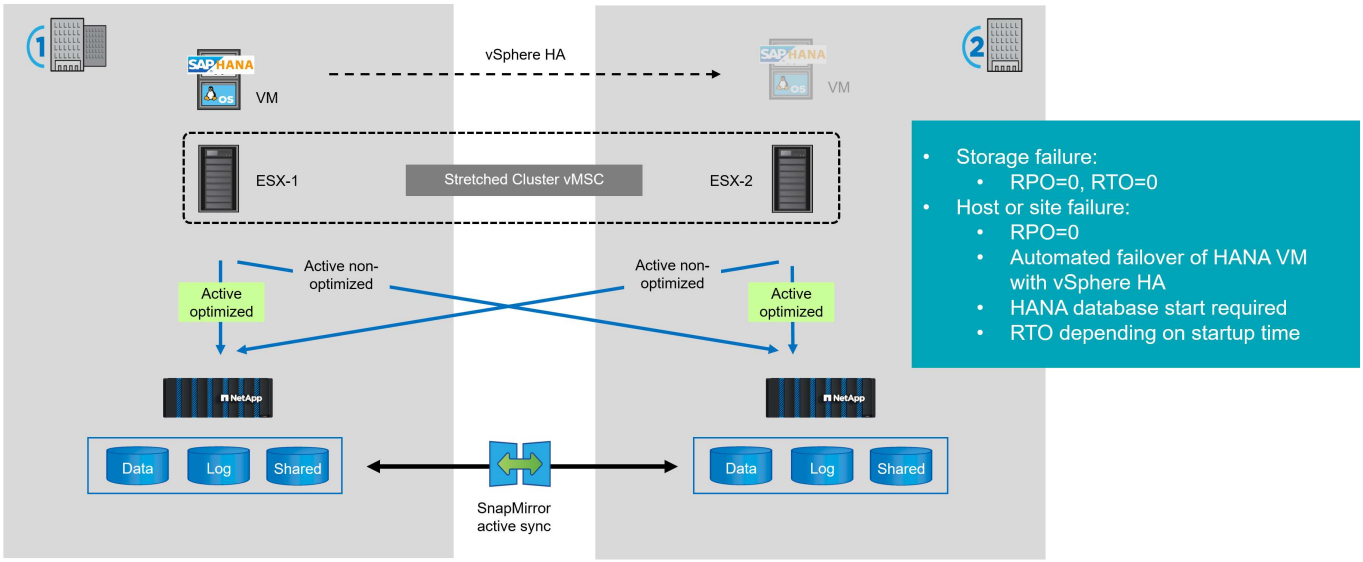


VSphere Metro Storage Cluster (vMSC)

Quando si esegue SAP HANA in un ambiente VMware utilizzando datastore collegati al protocollo FCP, è possibile utilizzare la sincronizzazione attiva di SnapMirror per creare un cluster storage VMware Metro. In questo tipo di setup, i datastore utilizzati dal sistema HANA vengono replicati in modo sincrono sul sito secondario.

In caso di errore dello storage, l'host ESX accede automaticamente alla copia con mirroring nel sito secondario, fornendo un RTO=0.

In caso di guasto a un host o a un sito completo, vSphere ha viene utilizzato per avviare la VM HANA sull'host ESX secondario. Quando la VM di HANA è in esecuzione, il database HANA deve essere avviato. L'RTO totale dipende quindi principalmente dal tempo di avvio del database HANA.



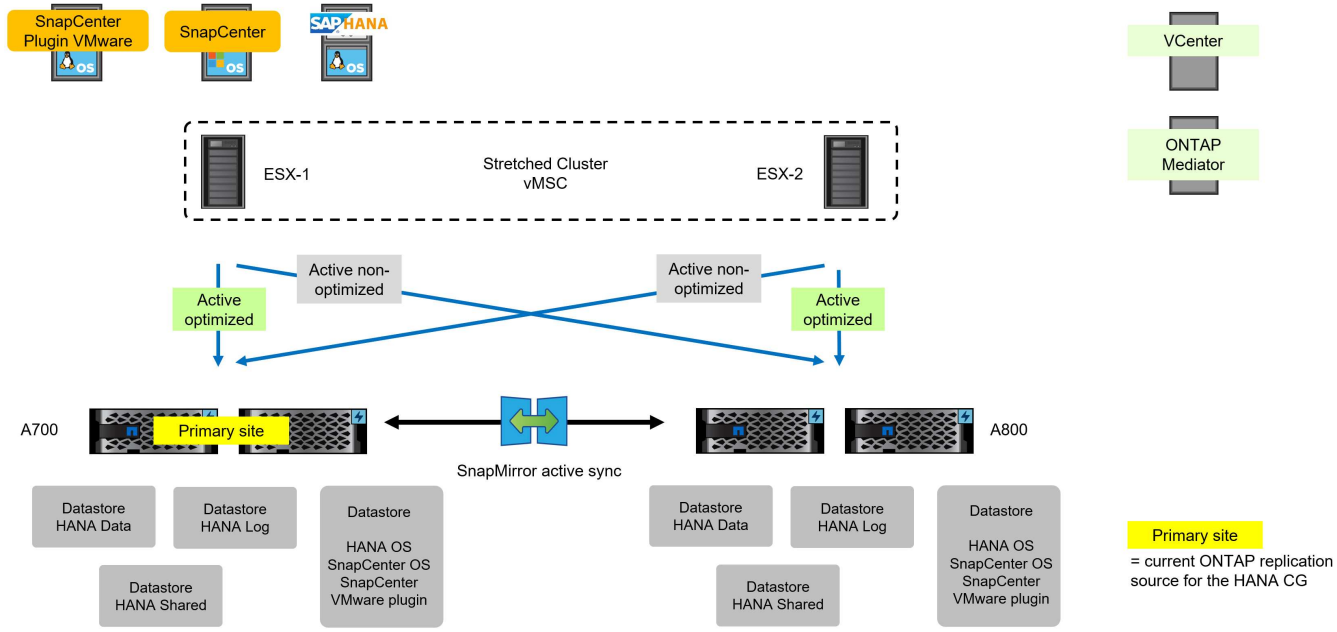
Confronto tra soluzioni

La tabella seguente fornisce un riepilogo delle caratteristiche chiave delle soluzioni descritte in precedenza.

	Replica di sistema HANA	Sincronizzazione attiva di SnapMirror: Bare metal	Sincronizzazione attiva SnapMirror: VMware vMSC
RPO con qualsiasi guasto	RPO=0 + replica sincrona		
RTO con errore dello storage	RTO < 1min	RTO=0 + failover dello storage trasparente	
RTO + con errore di sito o host	RTO < 1min	RTO: In base al tempo richiesto per la preparazione del server e l'avvio del database HANA.	RTO: In base al tempo richiesto per l'avvio del database HANA.
Automazione del failover	Sì, Failover automatico su host HSR secondario controllato da un gruppo pacemaker.	Sì, in caso di guasto dello storage No, in caso di guasti a un host o a un sito (Provisioning dell'host, connessione delle risorse storage, avvio del database HANA)	Sì, in caso di guasto dello storage Sì, in caso di guasti a un host o a un sito (Failover della VM su un altro sito automatizzato con vSphere ha, avvio del database HANA)
È richiesto un server dedicato nel sito secondario	Sì, richiesto per precaricare i dati nella memoria e abilitare il failover rapido senza avvio del database.	No, il server è necessario solo in caso di failover. In genere, il server utilizzato per il controllo qualità viene utilizzato per la produzione.	No, Le risorse dell'host ESX sono necessarie solo in caso di failover. In genere, le risorse di controllo qualità vengono utilizzate per la produzione.

Esempio di panoramica della configurazione

Durante il setup in laboratorio utilizziamo una configurazione di accesso uniforme, in cui entrambi gli host ESX hanno accesso a entrambi i cluster di storage. Nelle sezioni successive descriveremo la configurazione di accesso uniforme, ma evidenzieremo anche le differenze per una configurazione non uniforme.



Versioni software

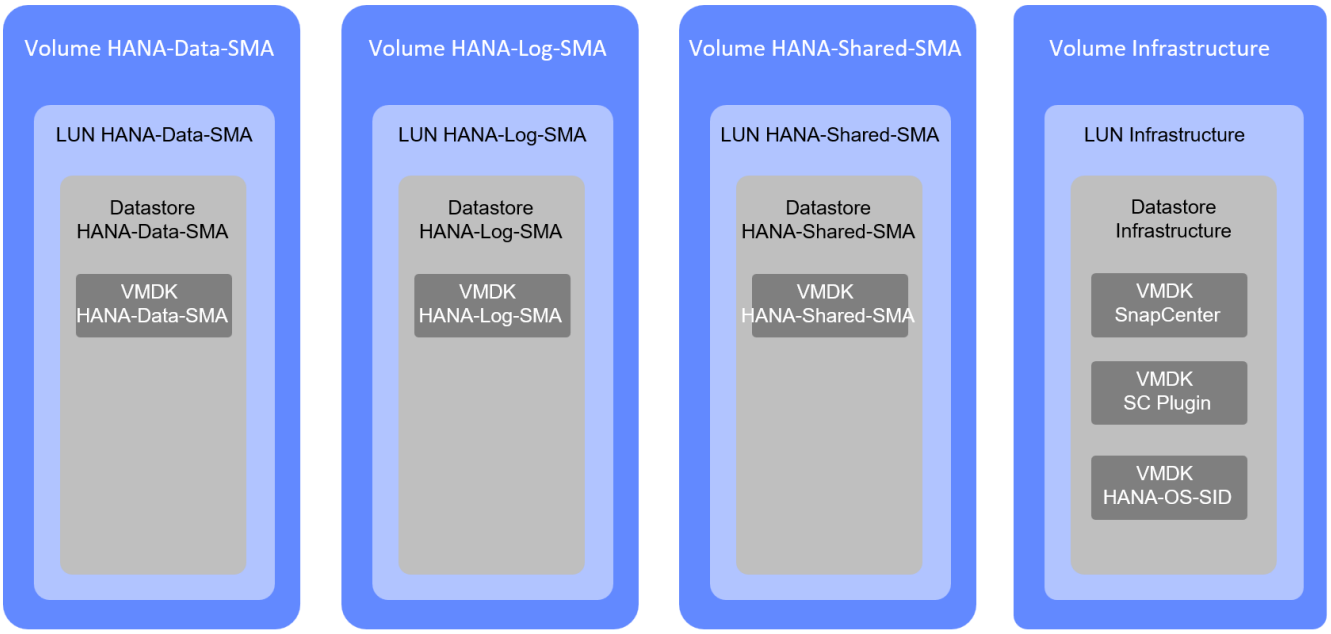
Software	Versione
ONTAP	A700: 9.15.1P7, A800: 9.16.1RC1
Client vSphere	8.0.3
ESXi	8.0.3
Plug-in SnapCenter per vSphere	6.0.1
OS Linux	SLES PER SAP 15 SP5
SAP HANA	2,0 SPS8
SnapCenter	6.0.1

Provisioning e installazione del sistema HANA

Questo capitolo descrive l'installazione e la configurazione del sistema SAP HANA specifico per una configurazione VMware utilizzando VMFS. Ulteriori procedure consigliate generiche sono disponibili all'indirizzo "SAP HANA su sistemi NetApp AFF con protocollo Fibre Channel".

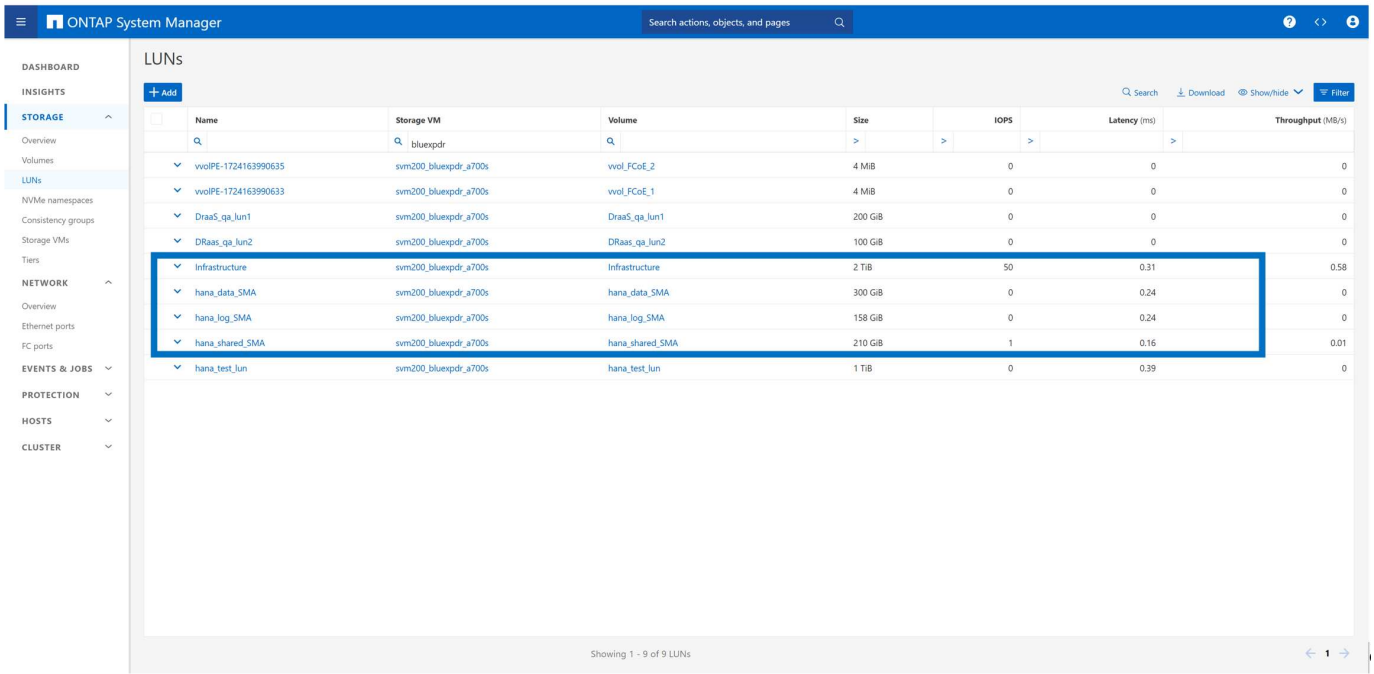
Configurazione dello storage

La figura qui sotto mostra la configurazione dello storage e del datastore per il sistema HANA. Devi configurare un volume dedicato, LUN, datastore per ogni filesystem del sistema HANA. I datastore non devono essere condivisi su sistemi HANA multipli o altri carichi di lavoro.



Tutte e tre le LUN del sistema HANA (hana++data++_++SMA, hanalogSAM e hanashared+++SMA) oltre al LUN per le immagini del sistema operativo e i componenti SnapCenter sono stati sottoposti a provisioning nel cluster di storage A700.

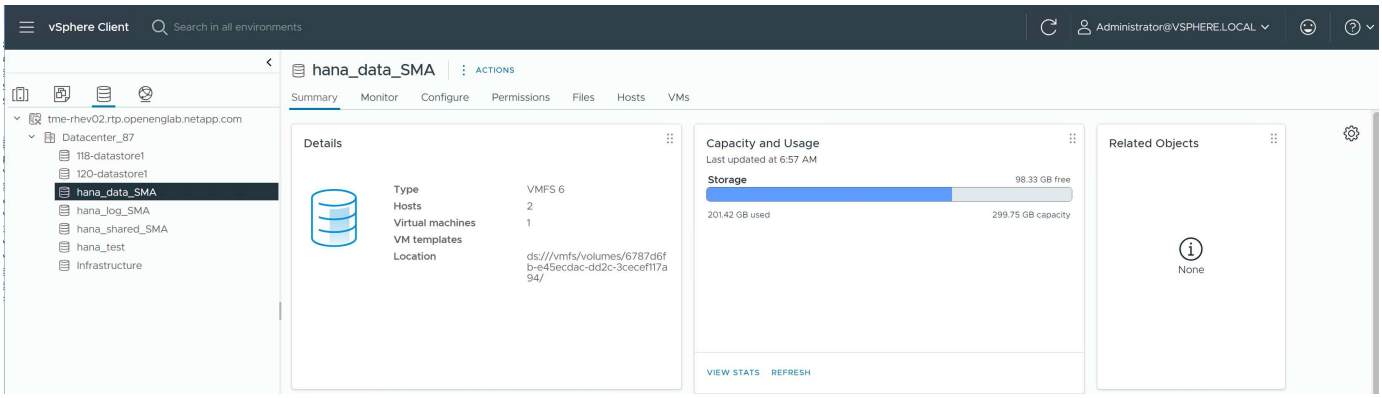
È necessario eseguire il provisioning di tutti i volumi del sistema HANA nella stessa SVM. Nella configurazione Active Sync di SnapMirror descritta in seguito, creeremo un gruppo di coerenza su tutti e tre i volumi HANA, che richiede che i volumi siano nella stessa SVM. Il volume dell'infrastruttura farà parte di un gruppo di coerenza diverso e potrebbe quindi trovarsi in una SVM diversa.



È necessario configurare un gruppo iniziatore e mappare i LUN sopra indicati all'host ESX-1, che si trova in prossimità del sistema di storage A700 nella configurazione del laboratorio.

Provisioning dei datastore

Abbiamo creato tre datastore per il sistema HANA utilizzando le tre LUN oggetto del provisioning precedente. Inoltre, abbiamo creato un datastore di infrastruttura utilizzando la LUN dell'infrastruttura.

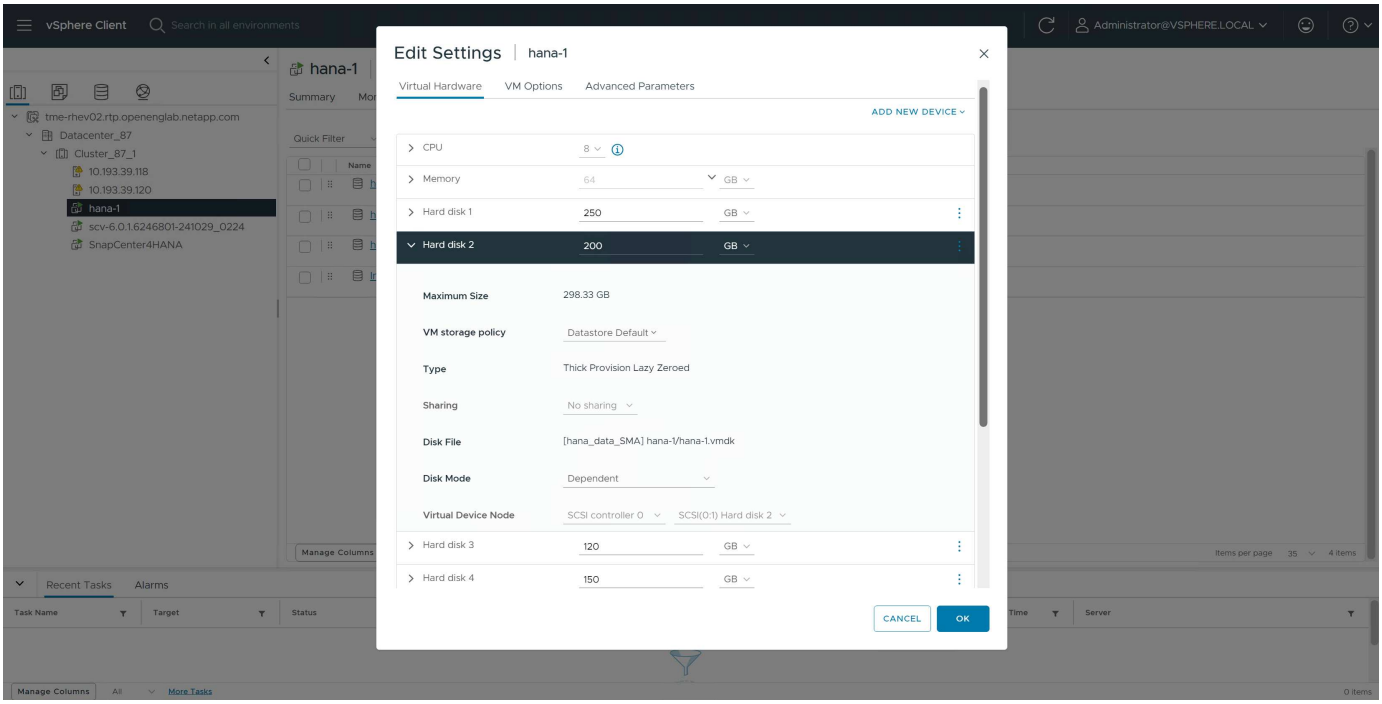


Provisioning delle macchine virtuali e installazione del sistema operativo

Durante il setup del laboratorio abbiamo implementato una nuova VM e inserito il VMDK per il sistema operativo Linux nel datastore dell'infrastruttura.

Configurazione dei dischi delle macchine virtuali

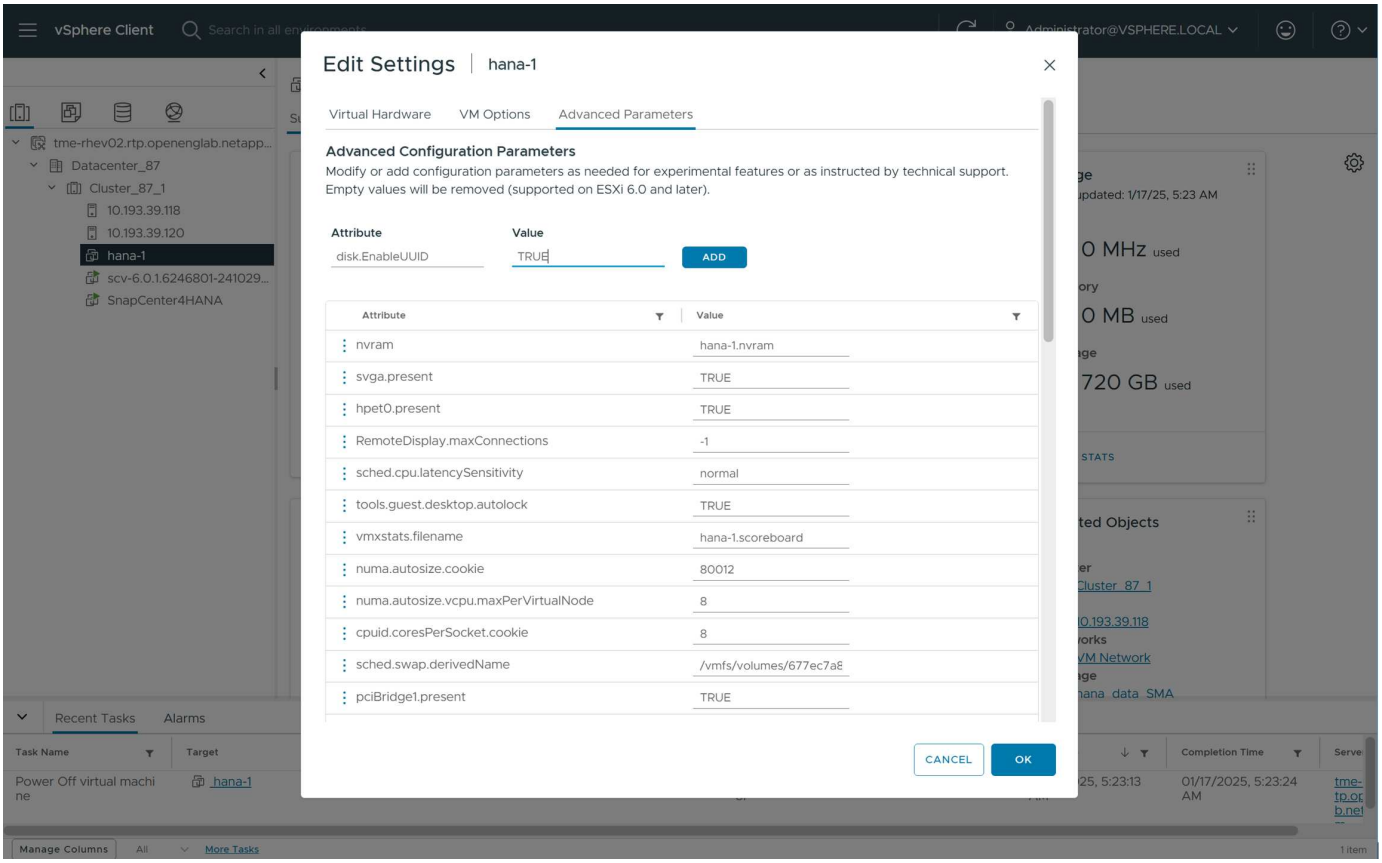
Alla VM HANA sono stati aggiunti tre nuovi dischi, ciascuno dei quali è all'interno di uno dei datastore creati per il sistema HANA.



Impostazione dei parametri VM

Il parametro disk.EnableUUID deve essere aggiunto e impostato su TRUE . Il parametro è richiesto da SnapCenter. In caso contrario, l'operazione di "individuazione delle risorse virtuali" di SnapCenter non verrà eseguita correttamente.

La VM deve essere arrestata prima di poter aggiungere il parametro.



La funzionalità può essere verificata con il comando seguente.

```
hana-1:~ # sg_inq /dev/sdd
standard INQUIRY:
PQual=0 PDT=0 RMB=0 LU_CONG=0 hot_pluggable=0 version=0x06 [SPC-4]
[AERC=0] [TrmTsk=] NormACA=0 HiSUP=0 Resp_data_format=2
SCCS=0 ACC=0 TPGS=0 3PC=0 Protect=0 [BQue=0]
EncServ=0 MultiP=0 [MChngr=0] [ACKREQQ=0] Addr16=0
[RelAdr=0] WBus16=1 Sync=1 [Linked=0] [TranDis=0] CmdQue=1
length=36 (0x24) Peripheral device type: disk
Vendor identification: VMware
Product identification: Virtual disk
Product revision level: 2.0
Unit serial number: 6000c293fecf25ac6bc457af67fe1f54
```

Preparazione del file system all'host Linux

Creazione del filesystem xfs su nuovi dischi

I nomi dei dispositivi dei nuovi dischi possono essere controllati con il comando seguente.

```
hana-1:/install # lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 250G 0 disk
├─sda1 8:1 0 256M 0 part /boot/efi
└─sda2 8:2 0 82G 0 part
├─system-root 254:0 0 60G 0 lvm /root
│ /var
│ /usr/local
│ /tmp
│ /srv
│ /opt
│ /home
│ /boot/grub2/x86++_++64-efi
│ /boot/grub2/i386-pc
│ /.snapshots
│ /
└─system-swap 254:1 0 2G 0 lvm SWAP
sdb 8:16 0 200G 0 disk
sdc 8:32 0 120G 0 disk
sdd 8:48 0 150G 0 disk
sr0 11:0 1 1024M 0 rom
hana-1:/install #
```

Su ciascuno dei tre nuovi dischi è stato creato un file system xfs.

```
hana-1:/install # mkfs.xfs /dev/sdb
meta-data=/dev/sdb isize=512 agcount=4, agsize=7864320 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=31457280, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=15360, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0

hana-1:/install # mkfs.xfs /dev/sdc
meta-data=/dev/sdc isize=512 agcount=4, agsize=7864320 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=31457280, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=15360, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0

hana-1:/install # mkfs.xfs /dev/sdd
meta-data=/dev/sdd isize=512 agcount=4, agsize=9830400 blks
sectsz=512 attr=2, projid32bit=1
crc=1 finobt=1, sparse=1, rmapbt=0
reflink=0 bigtime=0 inobtcount=0
data = bsize=4096 blocks=39321600, imaxpct=25
sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=19200, version=2
sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
hana-1:/install #
```

Creazione di punti di montaggio

```
hana-1:/ # mkdir -p /hana/data/SMA/mnt00001
hana-1:/ # mkdir -p /hana/log/SMA/mnt00001
hana-1:/ # mkdir -p /hana/shared
hana-1:/ # chmod –R 777 /hana/log/SMA
hana-1:/ # chmod –R 777 /hana/data/SMA
hana-1:/ # chmod -R 777 /hana/shared
```

Configurazione di /etc/fstab

```
hana-1:/install # cat /etc/fstab
/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=/@/var 0 0
/dev/system/root /usr/local btrfs subvol=/@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=/@/tmp 0 0
/dev/system/root /srv btrfs subvol=/@/srv 0 0
/dev/system/root /root btrfs subvol=/@/root 0 0
/dev/system/root /opt btrfs subvol=/@/opt 0 0
/dev/system/root /home btrfs subvol=/@/home 0 0
/dev/system/root /boot/grub2/x86_64-efi btrfs subvol=/@/boot/grub2/x86_64-
efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=/@/.snapshots 0 0
UUID=2E8C-48E1 /boot/efi vfat utf8 0 2
/dev/sdb /hana/data/SMA/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/SMA/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
hana-1:/install #

hana-1:/install # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 4.0K 49G 1% /dev/shm
tmpfs 13G 26M 13G 1% /run
tmpfs 4.0M 0 4.0M 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 35G 25G 58% /
/dev/mapper/system-root 60G 35G 25G 58% /.snapshots
/dev/mapper/system-root 60G 35G 25G 58% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 35G 25G 58% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 35G 25G 58% /home
/dev/mapper/system-root 60G 35G 25G 58% /opt
/dev/mapper/system-root 60G 35G 25G 58% /srv
/dev/mapper/system-root 60G 35G 25G 58% /tmp
/dev/mapper/system-root 60G 35G 25G 58% /usr/local
/dev/mapper/system-root 60G 35G 25G 58% /var
/dev/mapper/system-root 60G 35G 25G 58% /root
/dev/sda1 253M 5.1M 247M 3% /boot/efi
tmpfs 6.3G 56K 6.3G 1% /run/user/0
/dev/sdb 200G 237M 200G 1% /hana/data/SMA/mnt00001
/dev/sdc 120G 155M 120G 1% /hana/log/SMA/mnt00001
/dev/sdd 150G 186M 150G 1% /hana/shared
hana-1:/install #
```

Installazione HANA

Ora è possibile eseguire l'installazione HANA.

> Con la configurazione descritta, la directory /usr/sap/SMA sarà sul VMDK del sistema operativo. Se /usr/sap/SMA deve essere memorizzato nel VMDK condiviso, il disco condiviso hana potrebbe essere partizionato per fornire un altro file system per /usr/sap/SMA.

Chiave Userstore per SnapCenter

È necessario creare un archivio utenti per un utente del database di sistema, che dovrebbe essere utilizzato da SnapCenter. Il numero dell'istanza HANA deve essere impostato di conseguenza per la porta di comunicazione. Nell'istanza di installazione viene utilizzato il numero "00".

Una descrizione più dettagliata è disponibile all'indirizzo "Configurazione specifica delle risorse SnapCenter per i backup dei database SAP HANA"

```
smaadm@hana-1:/usr/sap/SMA/HDB00> hdbuserstore set SMAKEY hana-1:30013
SNAPCENTER <password>
Operation succeed.
```

La connettività può essere controllata con il comando seguente.

```
smaadm@hana-1:/usr/sap/SMA/HDB00> hdbsql -U SMAKEY
Welcome to the SAP HANA Database interactive terminal.
Type: \h for help with commands
\q to quit
hdbsql SYSTEMDB=> exit
smaadm@hana-1:/usr/sap/SMA/HDB00
```

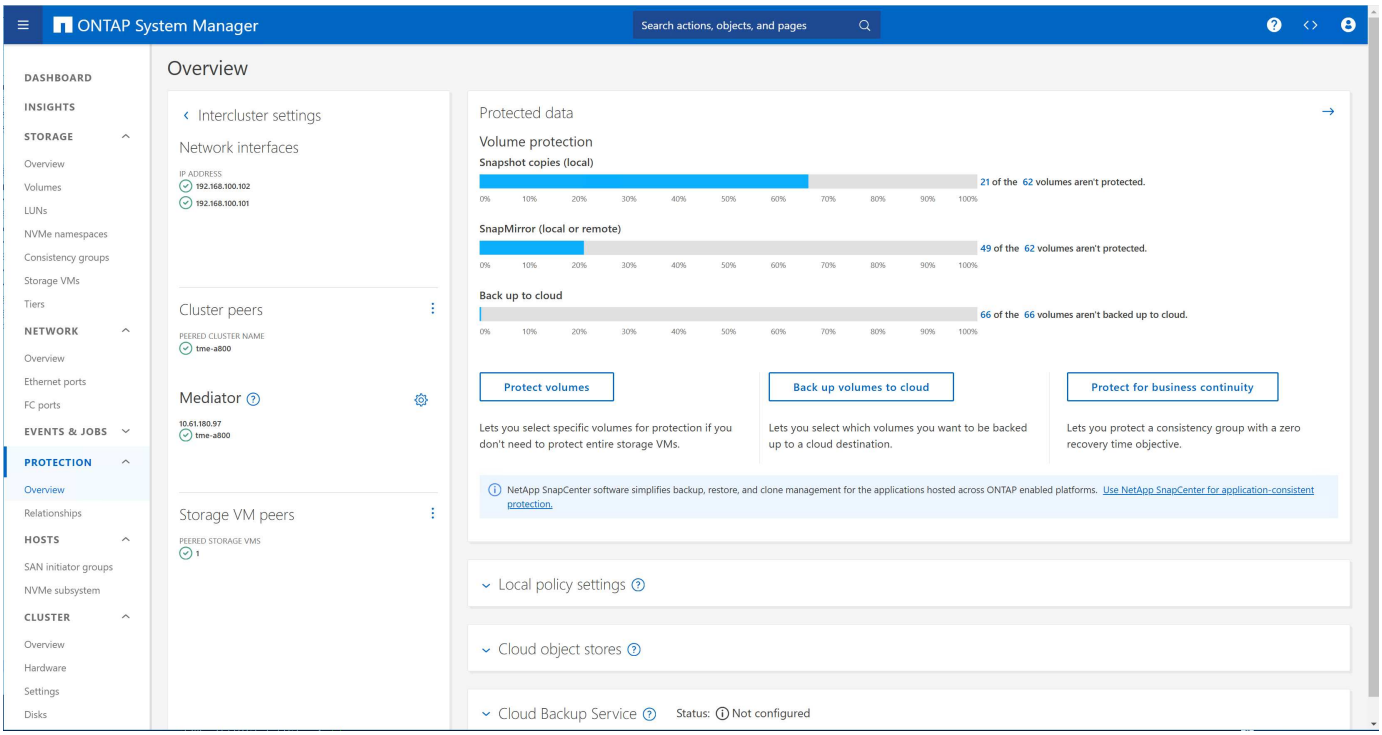
Configurazione della sincronizzazione attiva di SnapMirror

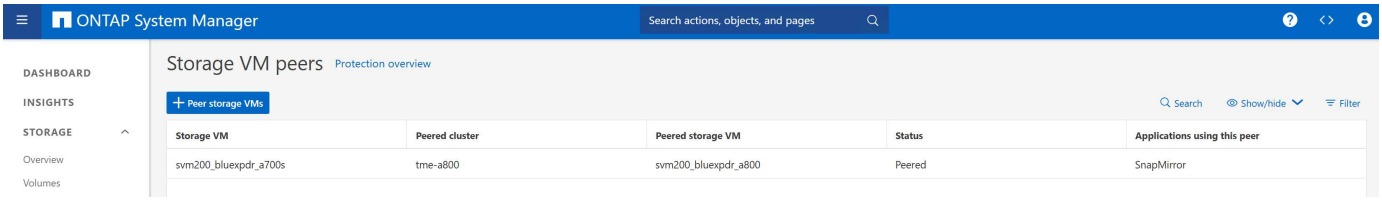
In questo articolo vengono descritte le fasi di configurazione necessarie per questa soluzione.

Prerequisiti

È necessario eseguire il peering dei cluster di storage e delle SVM rilevanti.

ONTAP mediator deve essere disponibile e configurato in entrambi i cluster di storage.





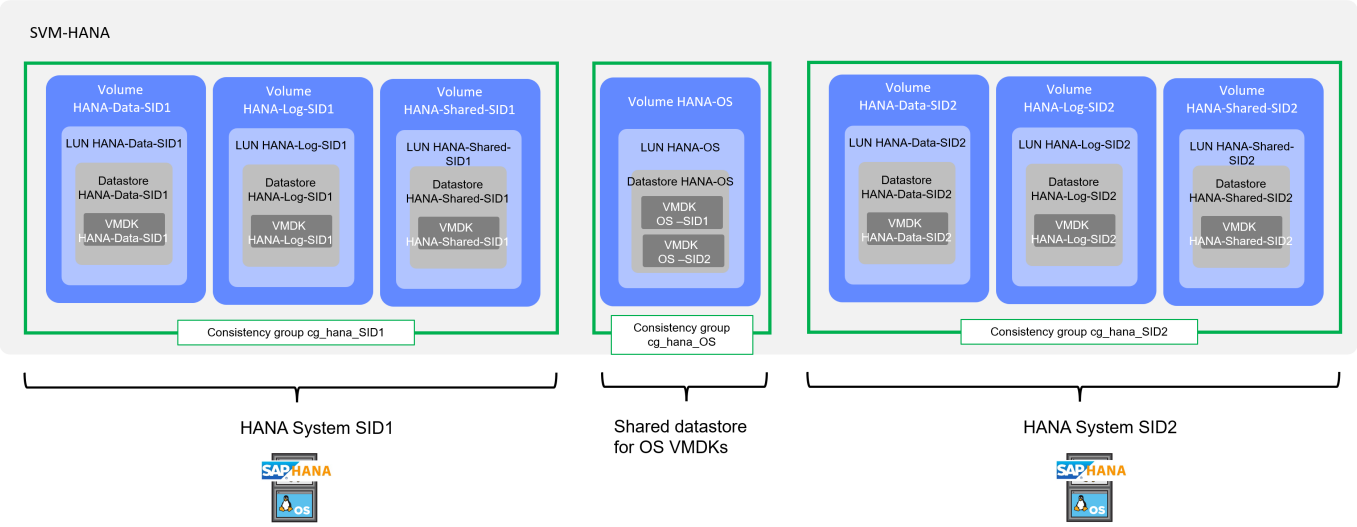
Configurazione del layout dello storage e del gruppo di coerenza

Nella documentazione di ONTAP "Panoramica della sincronizzazione attiva di SnapMirror in ONTAP", il concetto di gruppi di coerenza con sincronizzazione attiva di SnapMirror viene descritto come segue:

Un gruppo di coerenza è una raccolta di volumi FlexVol che offrono una garanzia di coerenza per il workload dell'applicazione che deve essere protetto per la business continuity.

Lo scopo di un gruppo di coerenza è quello di acquisire immagini snapshot simultanee di più volumi, garantendo così copie coerenti con i crash di una raccolta di volumi in un point-in-time. Un gruppo di coerenza garantisce che tutti i volumi di un set di dati siano inattivi e quindi schioccati esattamente nello stesso momento. In questo modo, si otterrà un punto di ripristino coerente con i dati nei volumi che supportano il set di dati. Un gruppo di coerenza mantiene quindi la coerenza dell'ordine di scrittura dipendente. Se si decide di proteggere le applicazioni per la business continuity, il gruppo di volumi corrispondenti a questa applicazione deve essere aggiunto a un gruppo di coerenza in modo da stabilire una relazione di protezione dei dati tra un gruppo di coerenza di origine e uno di destinazione. La coerenza di origine e destinazione deve contenere lo stesso numero e tipo di volumi.

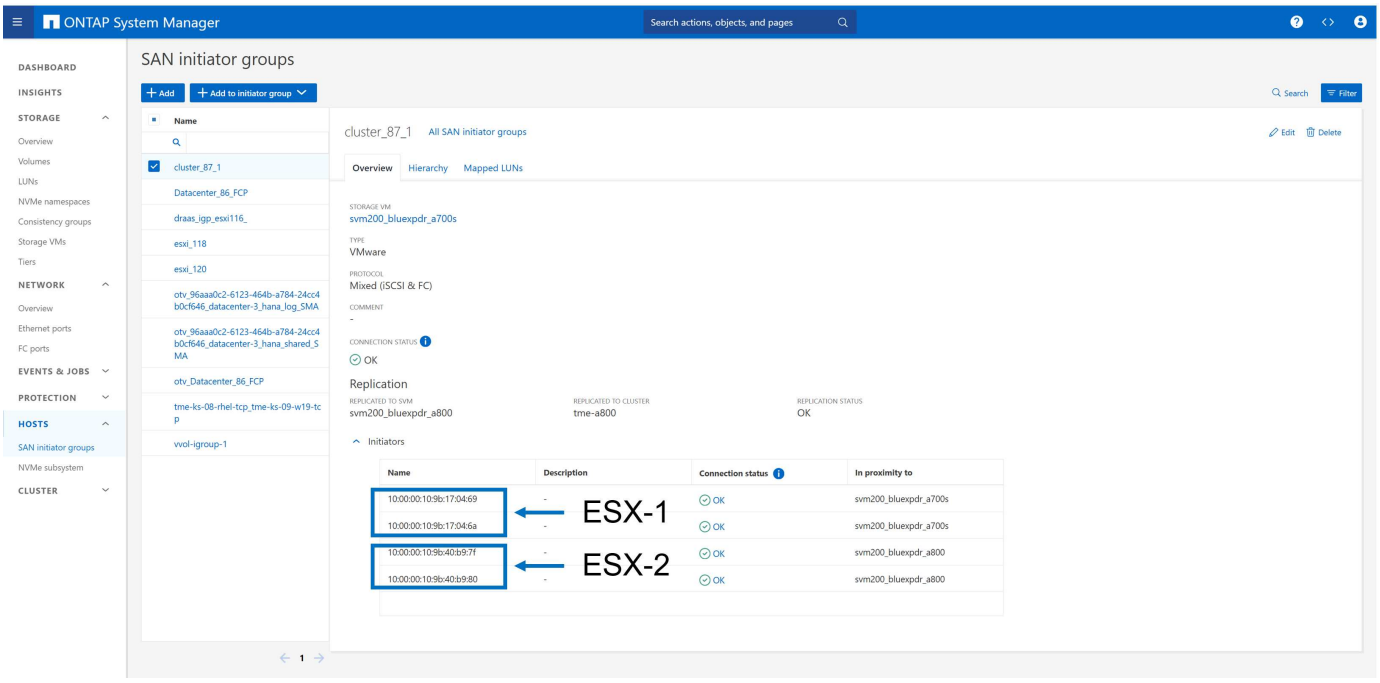
Per la replica dei sistemi HANA, il gruppo di coerenza deve includere tutti i volumi utilizzati dal singolo sistema HANA (dati, log e condivisi). I volumi che devono far parte di un gruppo di coerenza devono essere archiviati nella stessa SVM. Le immagini del sistema operativo possono essere memorizzate in un volume separato con un proprio gruppo di coerenza. La figura seguente illustra un esempio di configurazione con due sistemi HANA.

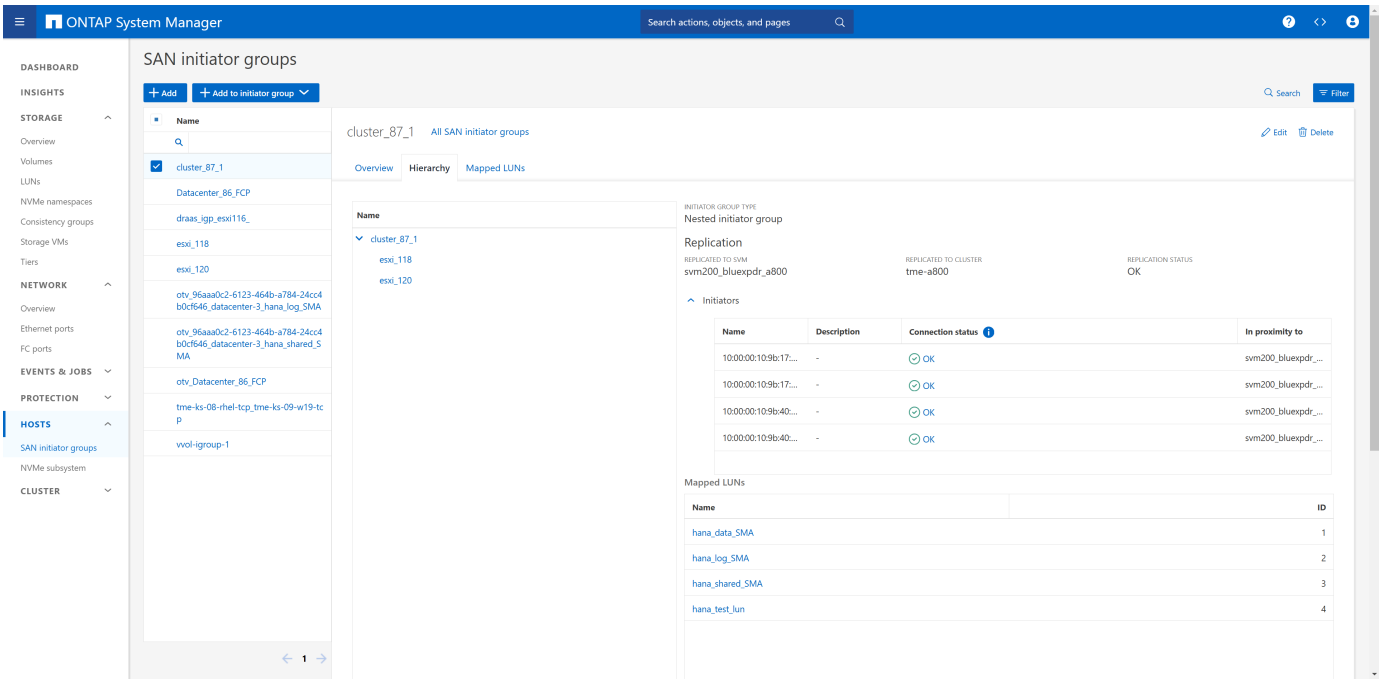


Configurazione del gruppo iniziatore

Durante il setup in laboratorio è stato creato un gruppo iniziatore che include entrambe le SVM di storage utilizzate per la replica sincrona attiva SnapMirror. Nella configurazione di sincronizzazione attiva di SnapMirror descritta in seguito, verrà definito che il gruppo iniziatore farà parte della replica.

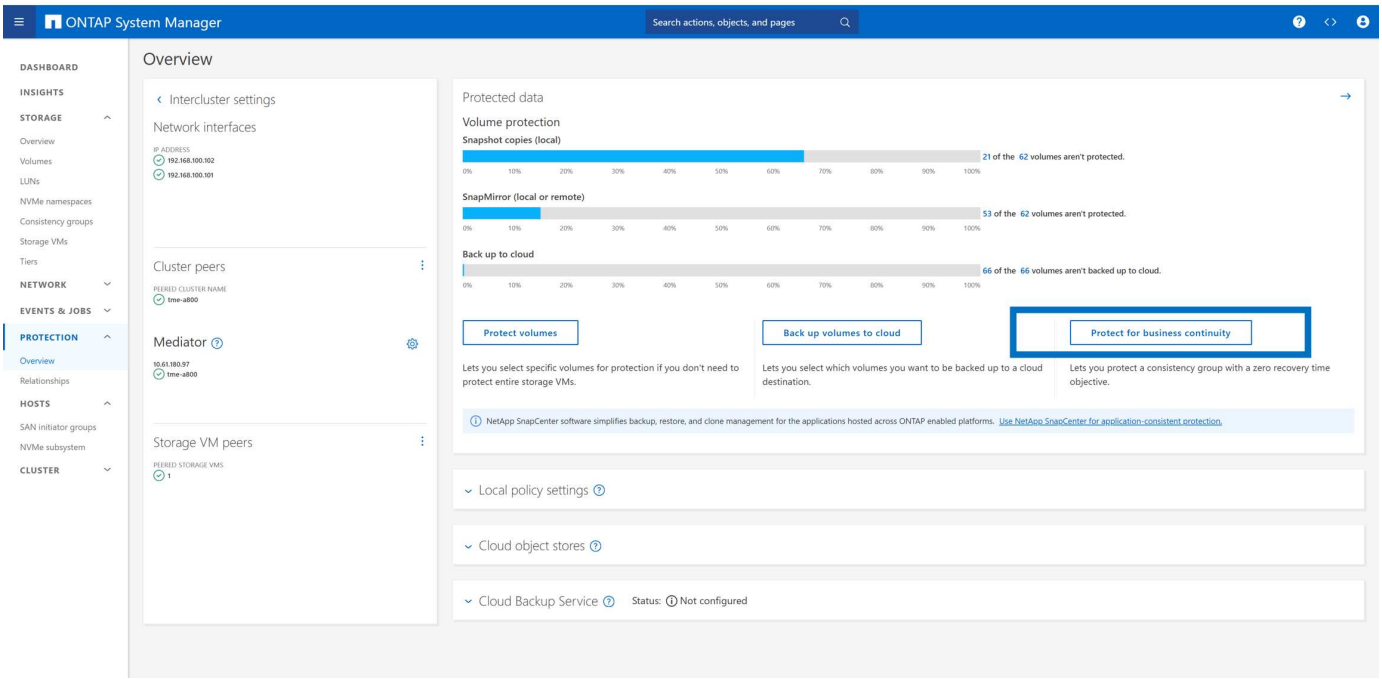
Utilizzando le impostazioni di prossimità, abbiamo definito l'host ESX più vicino a quale cluster di storage. Nel nostro caso, A700 è vicino a ESX-1 e A800 è vicino a ESX-2.





In una configurazione ad accesso non uniforme, il gruppo iniziatore nel cluster di storage primario (A700) deve includere solo gli iniziatori dell'host ESX-1, poiché non è presente alcuna connessione SAN a ESX-2. Inoltre, è necessario configurare un altro gruppo iniziatore nel secondo cluster di storage (A800) che includa solo gli iniziatori dell'host ESX-2. La configurazione di prossimità e la replica del gruppo iniziatore non sono necessarie.

Configurare la protezione con ONTAP System Manager

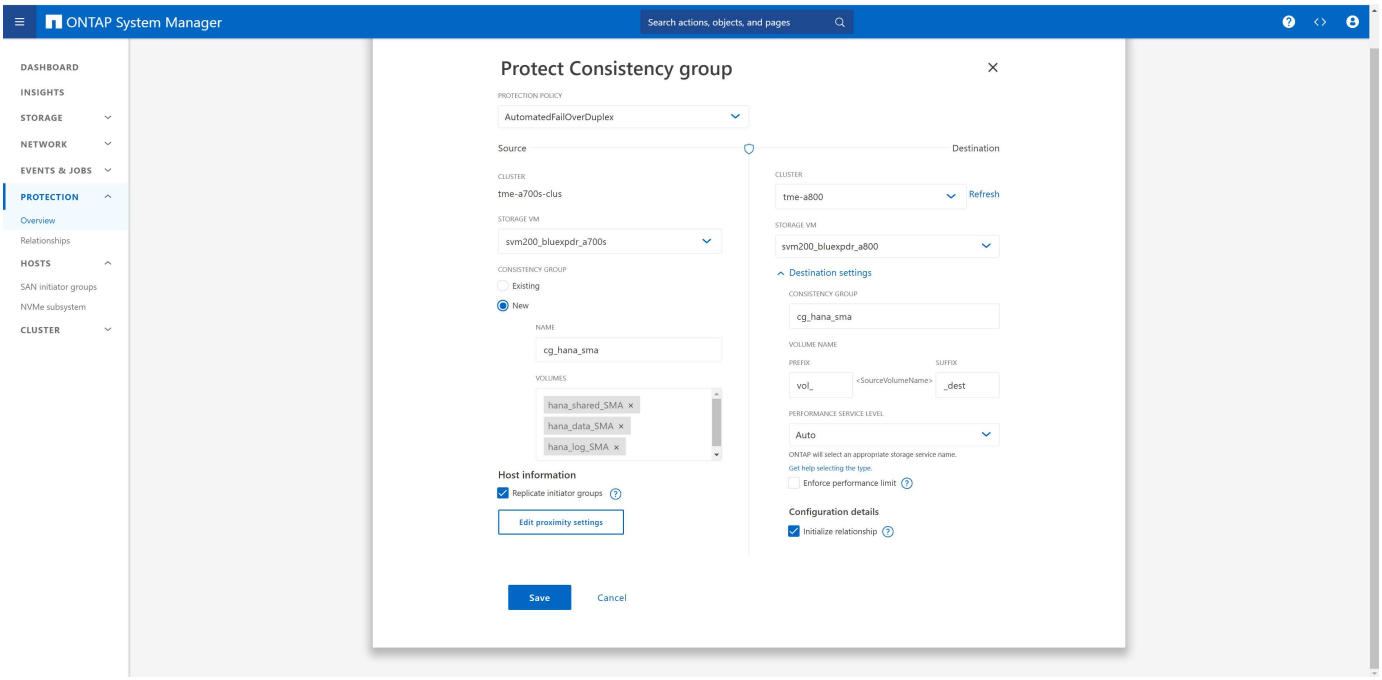


Replica di gruppi di coerenza e gruppi iniziatori

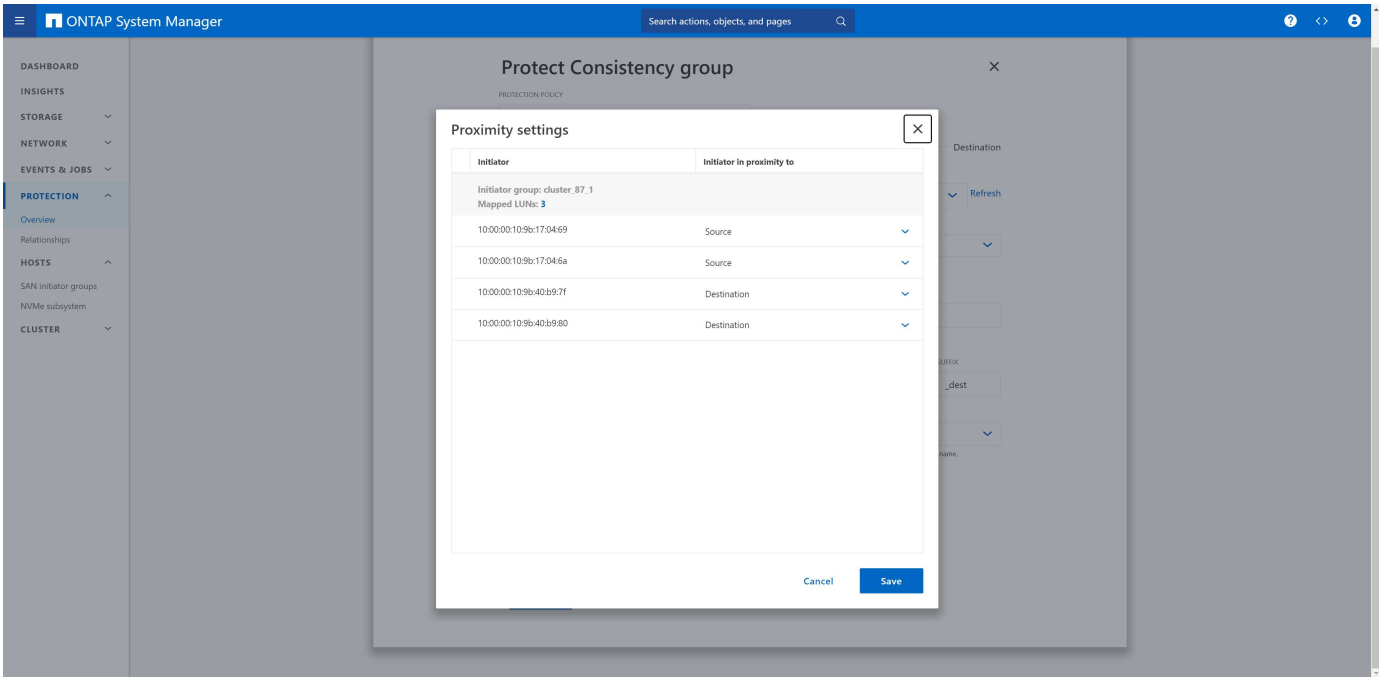
Occorre creare un nuovo gruppo di coerenza e aggiungere tutte e tre le LUN del sistema HANA al gruppo di coerenza.

Il "gruppo iniziatore di replica" è stato attivato. Il gruppo di imitator rimarrà quindi in-Sync indipendente dove vengono apportate le modifiche.

In una configurazione con accesso non uniforme, il gruppo iniziatore non deve essere replicato, poiché un gruppo iniziatore separato deve essere configurato nel secondo cluster di storage.



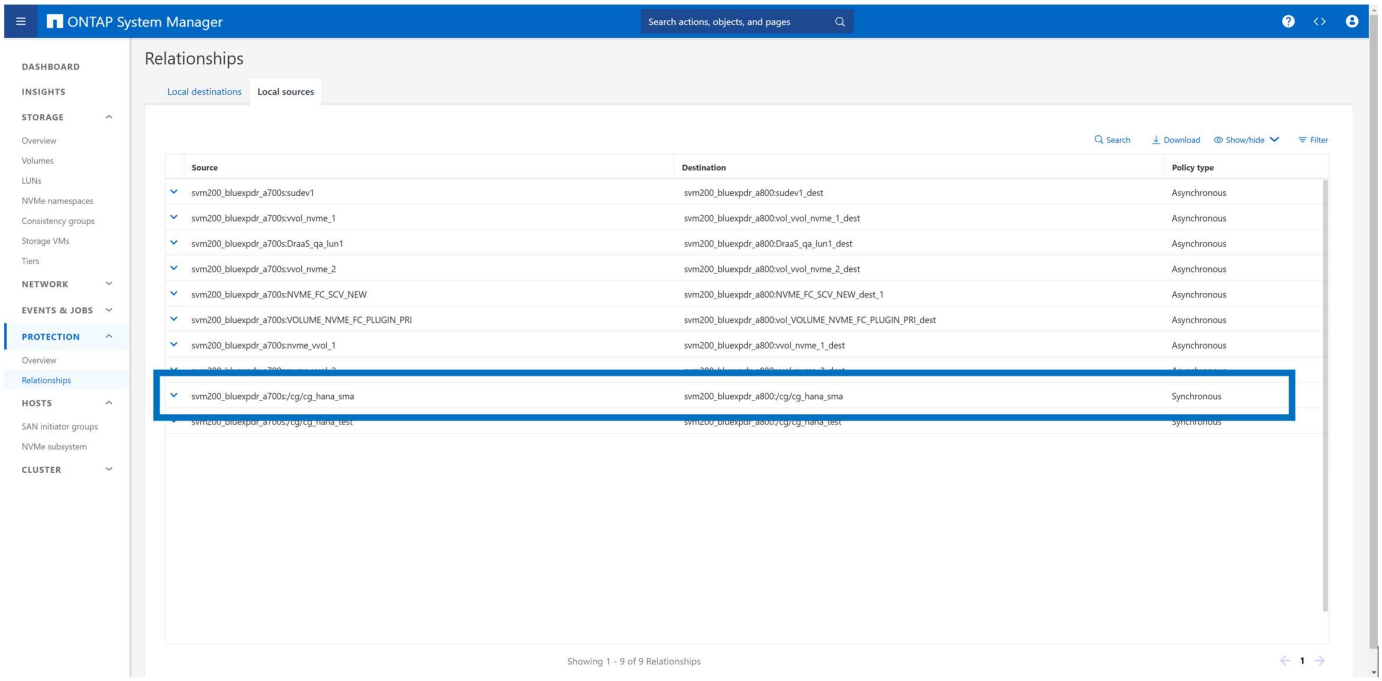
Facendo clic sulle impostazioni di prossimità, è possibile rivedere la configurazione eseguita in precedenza nell'impostazione del gruppo iniziatore.



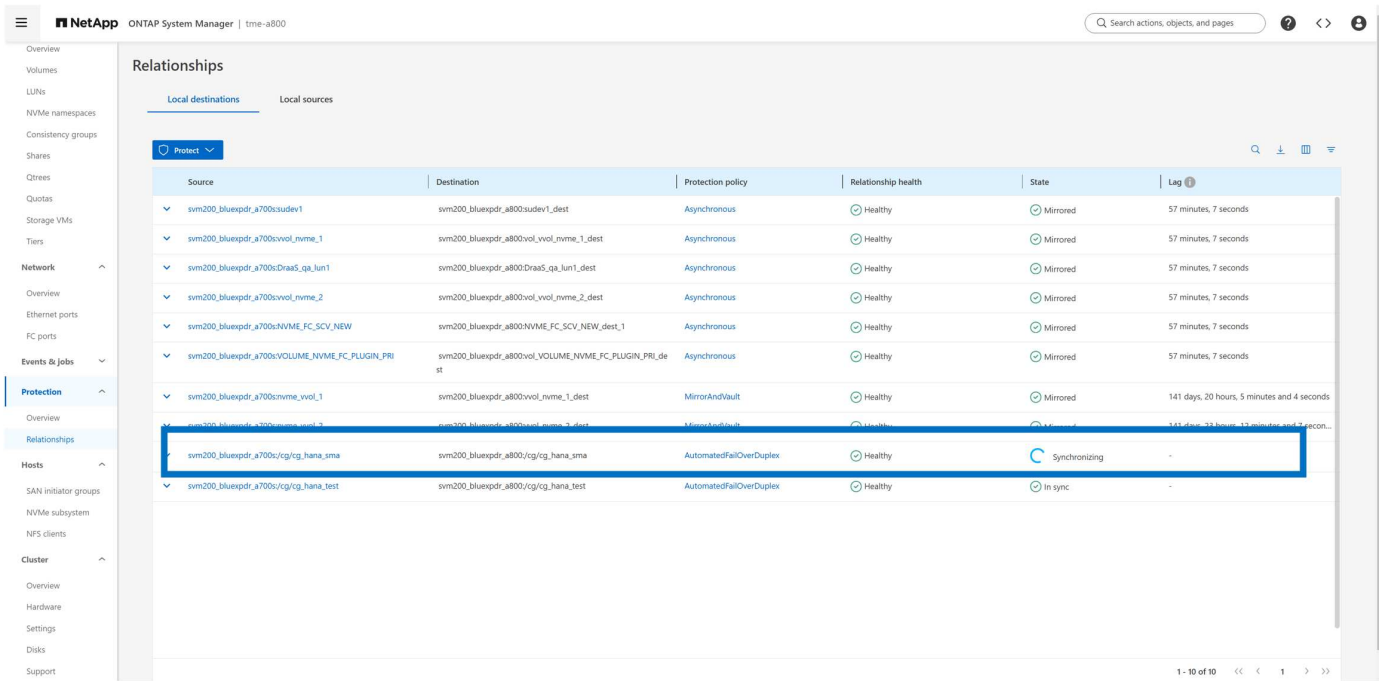
È necessario configurare il cluster di storage di destinazione e attivare la funzione di inizializzazione delle relazioni.

Sincronizzazione

Nel cluster di storage A700 (origine), viene elencata la nuova relazione.



Nel cluster di storage A800 (destinazione) vengono elencate la nuova relazione e lo stato della replica.



Datastore dell'infrastruttura

Il datastore, dove sono memorizzate le immagini del sistema operativo HANA, SnapCenter e il plug-in vSphere, viene replicato nello stesso modo descritto per i datastore del database HANA.

Sede principale

Il comportamento di sincronizzazione attiva di SnapMirror è simmetrico, con una eccezione importante: La configurazione del sito primario.

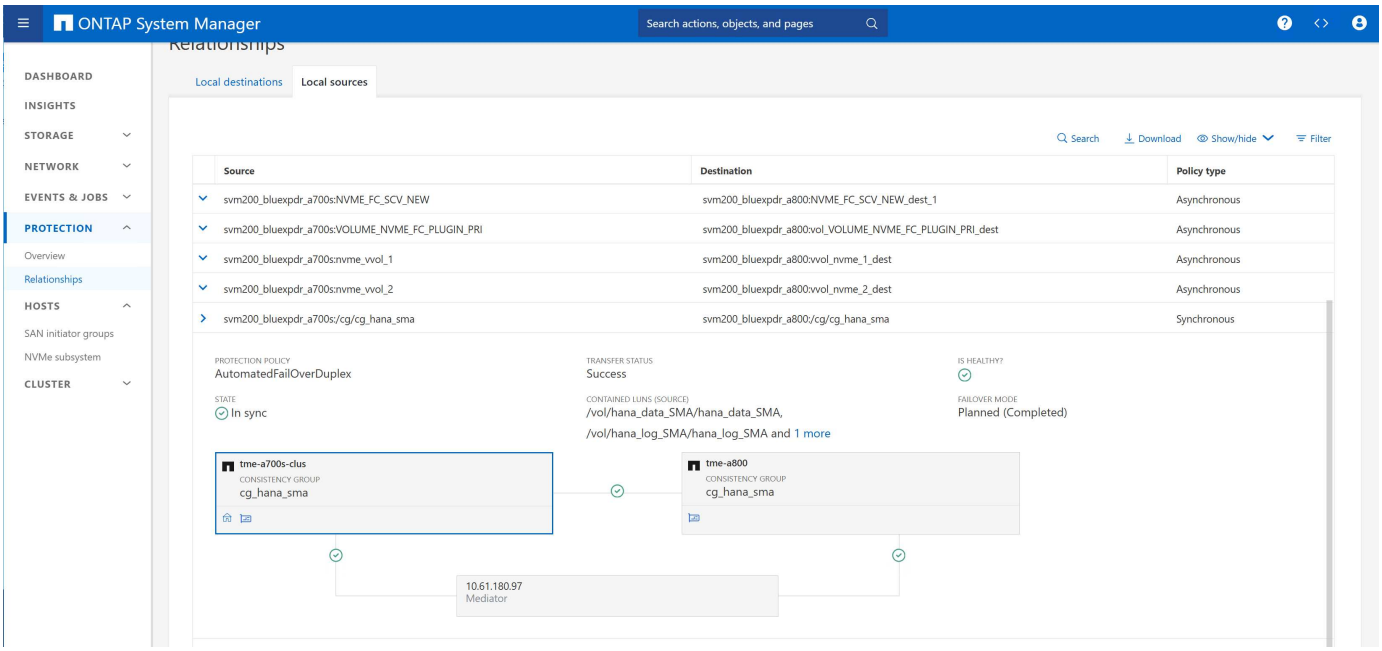
La sincronizzazione attiva di SnapMirror considererà un sito la "fonte" e l'altro la "destinazione". Ciò implica una relazione di replica unidirezionale, ma ciò non si applica al comportamento io. La replica è bidirezionale e simmetrica, mentre i tempi di risposta io sono identici su entrambi i lati del mirror.

In caso di perdita del link di replica, i percorsi delle LUN nella copia di origine continueranno a fornire i dati mentre i percorsi delle LUN nella copia di destinazione non saranno disponibili finché la replica non viene ristabilita e SnapMirror ritorna allo stato sincrono. I percorsi riprenderanno a fornire i dati.

L'effetto della designazione di un cluster come origine controlla semplicemente quale cluster sopravvive come sistema di storage in lettura e scrittura in caso di perdita del link di replica.

Il sito primario viene rilevato da SnapCenter e utilizzato per eseguire operazioni di backup, ripristino e cloning.

Ricorda che origine e destinazione non sono legate a SVM o cluster di storage, ma possono essere diverse per ogni relazione di replica.



Configurazione di SnapCenter

Come indicato all'inizio del documento, lo scopo del documento è quello di fornire Best practice per un ambiente HANA che utilizzi VMware con VMFS e SnapMirror Active Sync. Verranno trattati solo i dettagli e le fasi importanti relative a questa specifica soluzione e non verranno illustrati i concetti generali di SnapCenter. Questi concetti e altre informazioni aggiuntive su SnapCenter sono disponibili all'indirizzo:

"TR-4614: Backup e recovery SAP HANA con SnapCenter"

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

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

Prerequisiti

In generale, la sincronizzazione attiva di SnapMirror deve essere configurata prima di aggiungere le risorse protette a SnapCenter. Se i backup sono stati creati prima della configurazione della sincronizzazione attiva di SnapMirror, esisteranno solo nello storage primario originale e non verranno replicati successivamente.

La risorsa SnapCenter HANA deve essere scoperta automaticamente

Le risorse configurate con VMware VMFS o le risorse protette con la sincronizzazione attiva di SnapMirror devono essere rilevate automaticamente da SnapCenter per consentire operazioni specifiche richieste per queste configurazioni.

Poiché i volumi HANA non di dati sono sempre risorse configurate manualmente in SnapCenter, non sono supportati da SnapCenter out of the box. Verranno illustrate le opzioni e le soluzioni alternative per i volumi non di dati più avanti in questo documento.

I sistemi host multipli SAP HANA devono essere configurati usando un plug-in HANA centrale e sono pertanto risorse configurate manualmente per impostazione predefinita. Tali sistemi HANA non sono supportati da SnapCenter, quando si utilizza la sincronizzazione attiva di VMware VMFS o SnapMirror.

Plug-in SnapCenter per VMware vSphere

Il plug-in di SnapCenter per VMware vSphere deve essere implementato nell'ambiente VMware.

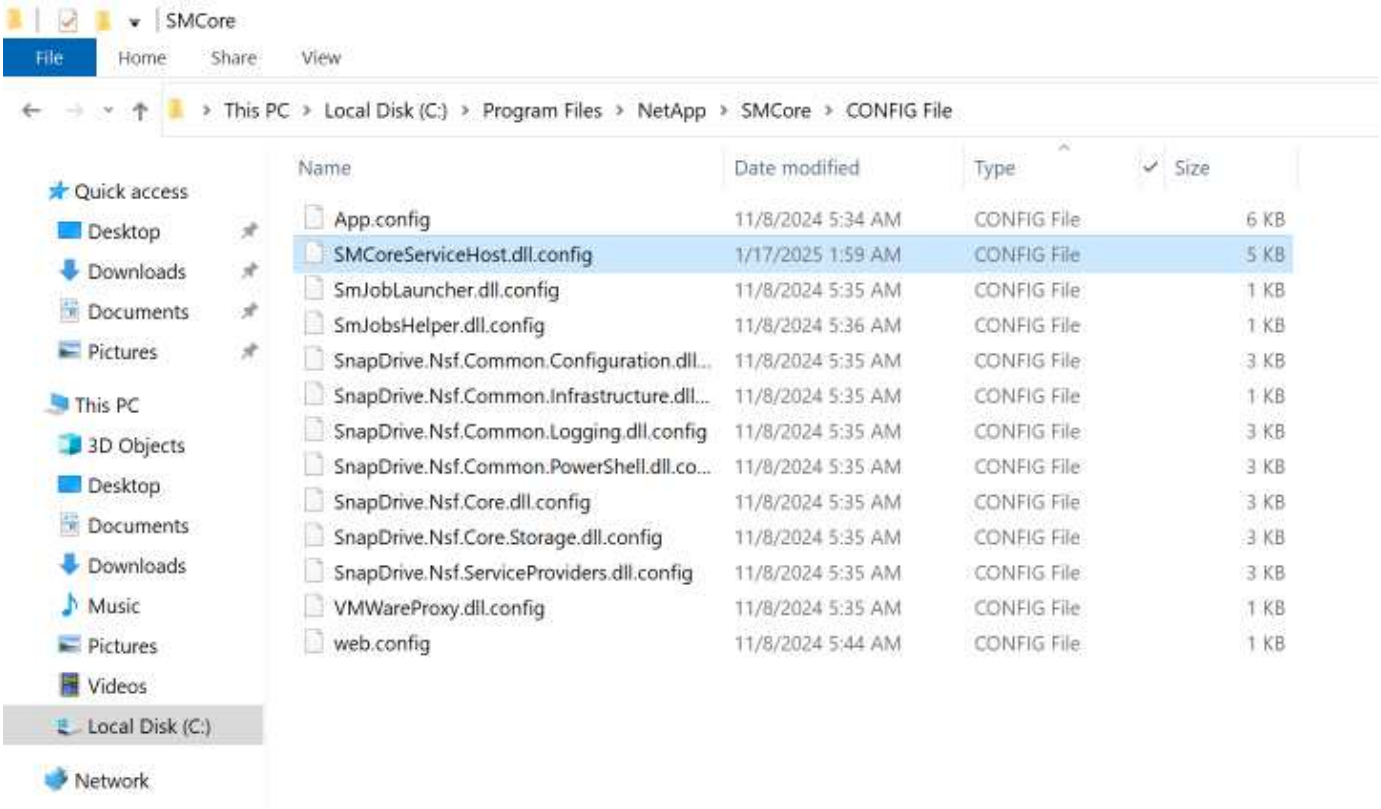
Indirizzo IP di gestione su SVM che ospitano i volumi

Anche se i cluster verranno aggiunti a SnapCenter, le SVM che ospitano i volumi di origine e destinazione devono avere configurato un indirizzo IP di gestione.

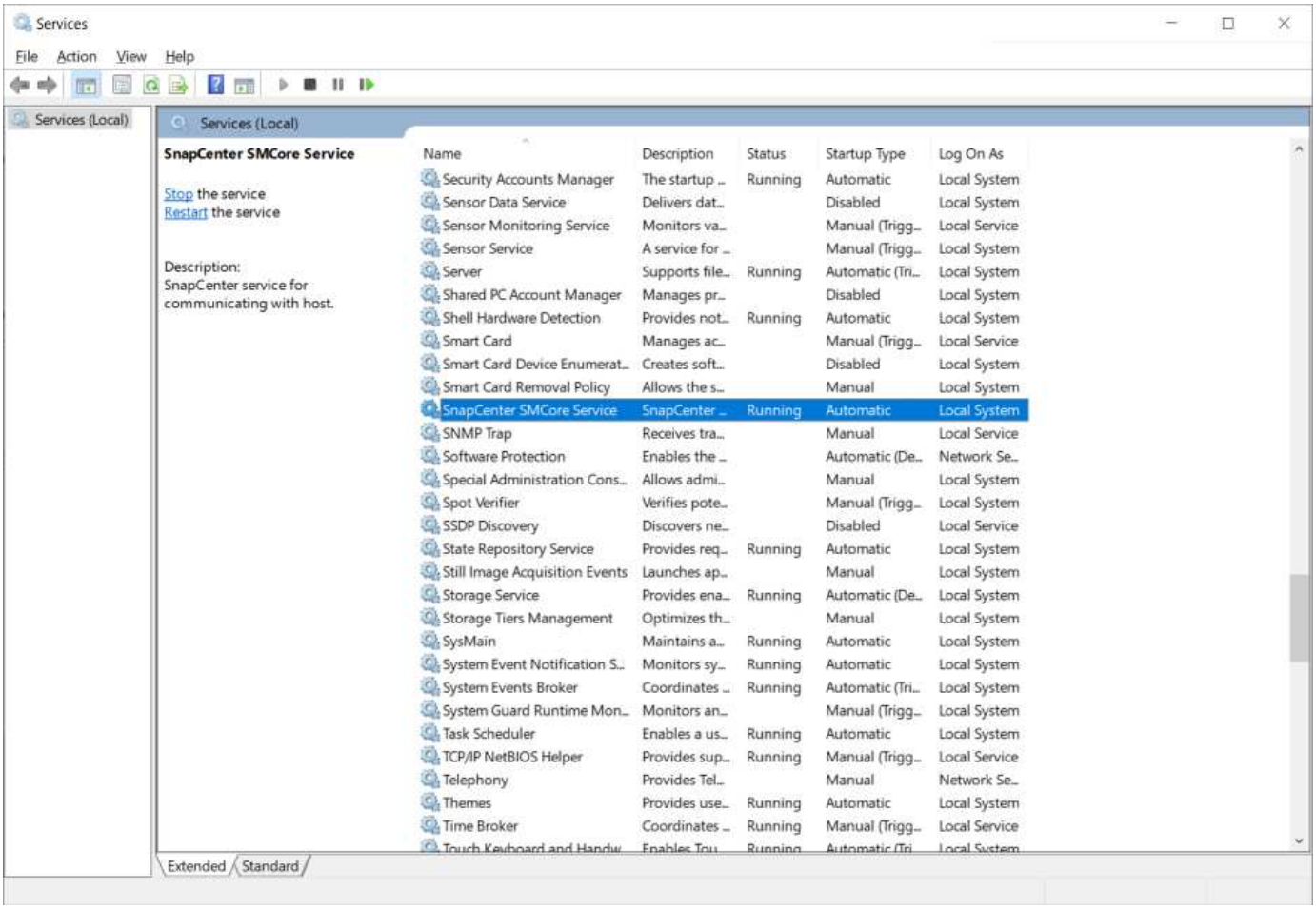
API REST per la comunicazione dello storage

La gestione e il monitoring della sincronizzazione attiva di SnapMirror richiede l'accesso alle API REST. Pertanto, SnapCenter deve essere configurato per utilizzare le API REST per le comunicazioni dello storage. Il parametro "IsRestEnabledForStorageConnection" nel file di configurazione + C:\Program Files\NetApp\SMCore\SMCoreServiceHost.dll.config deve essere impostato su true.

```
<add key="IsRestEnabledForStorageConnection" value="true">
```

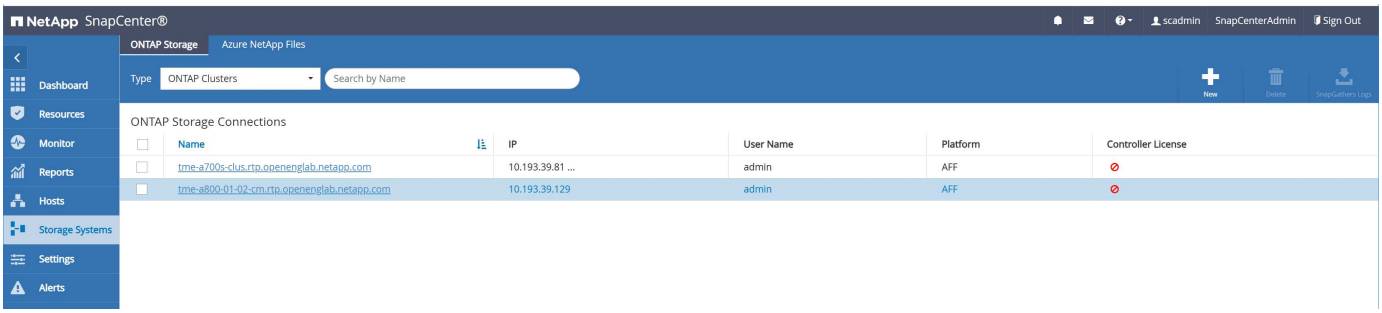


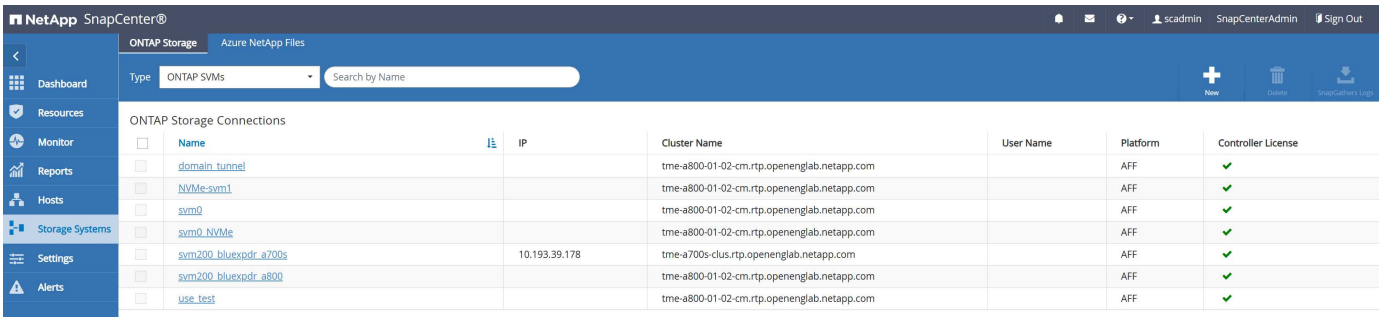
Dopo la modifica del parametro, è necessario riavviare il servizio SMCore di SnapCenter.



Aggiungere sistemi storage

È possibile aggiungere sistemi storage dopo l'abilitazione dell'API REST per SnapCenter. È necessario aggiungere entrambi i cluster di storage, non le singole SVM.



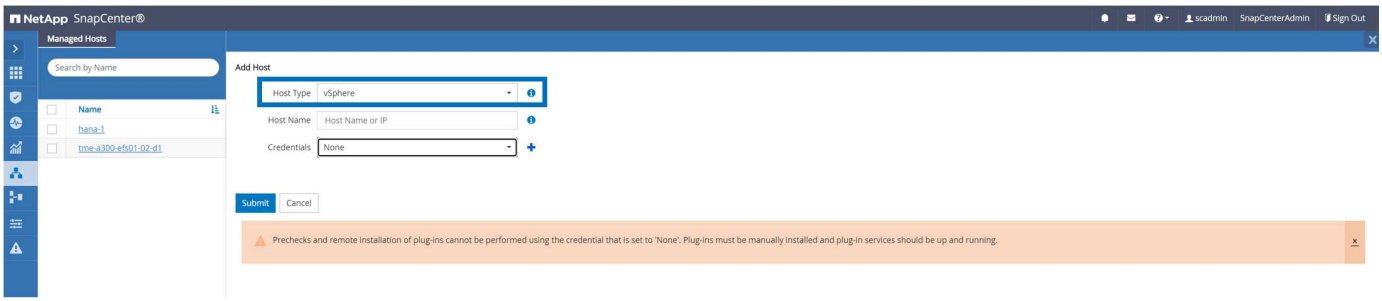


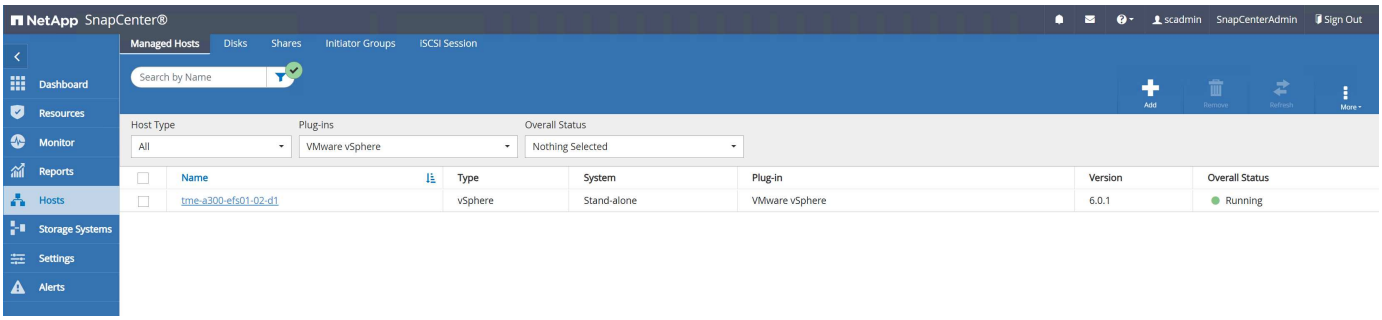
Add host – plugin SnapCenter per VMware vSphere

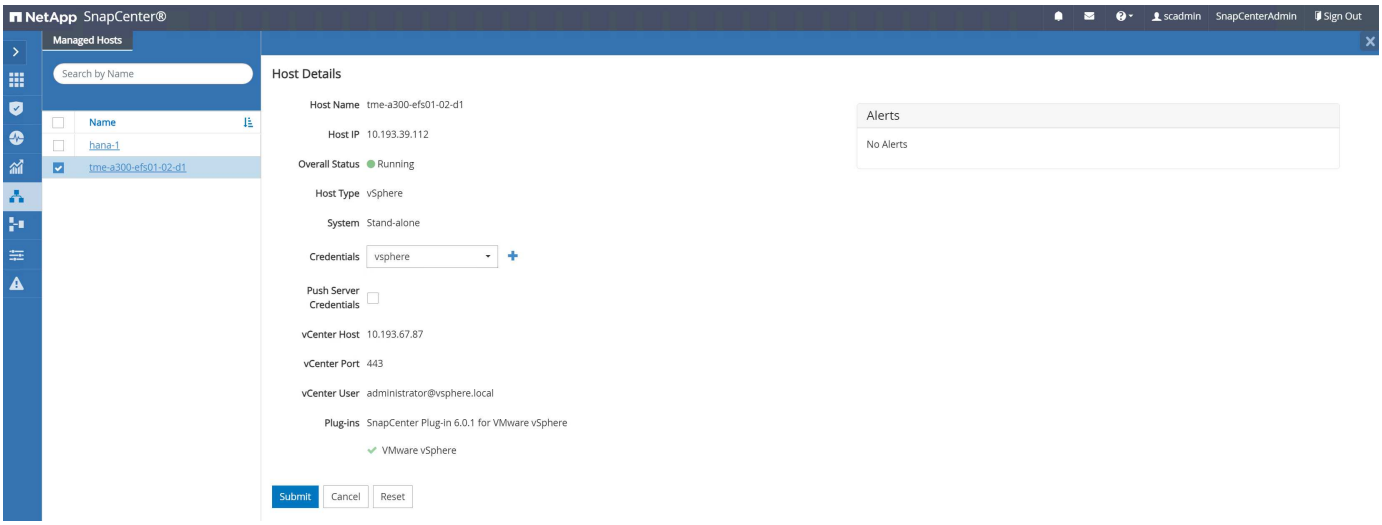
Se una risorsa in SnapCenter viene eseguita in un ambiente VMware virtualizzato, SnapCenter sfrutta il plug-in SnapCenter per VMware vSphere per estendere i flussi di lavoro di backup, ripristino e cloning di SnapCenter seguendo i passaggi richiesti a livello VMware.

Prima di poter aggiungere l'host in SnapCenter, è necessario distribuire il plug-in SnapCenter per VMware vSphere all'interno dell'ambiente VMware.

ⓘ È necessario impostare le credenziali durante il flusso di lavoro di aggiunta dell'host, in cui vSphere può essere selezionato come tipo di host.







Non è necessaria alcuna configurazione aggiuntiva nel plug-in SnapCenter per vSphere.

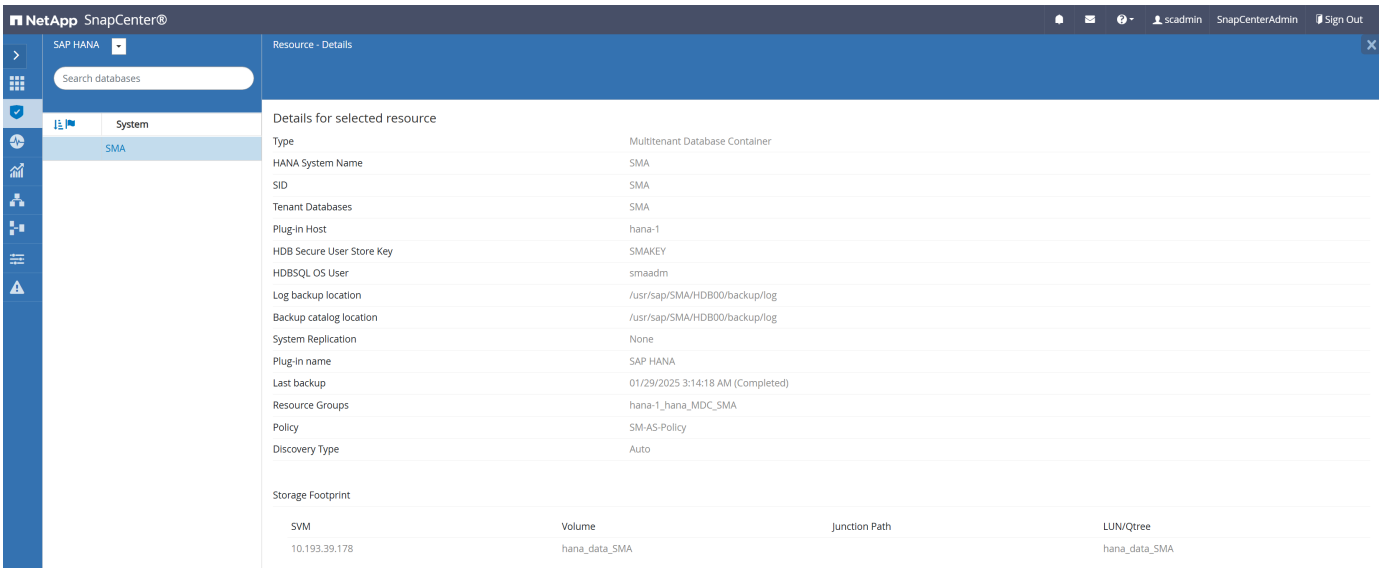
Aggiunta di host - sistema HANA

Nessun requisito specifico. La distribuzione del plugin e il rilevamento automatico vengono eseguiti come di consueto.

Con il processo di auto-Discovery, SnapCenter rileva che la risorsa HANA è in esecuzione virtualizzata con VMFS/VMDK. SnapCenter rileva inoltre la configurazione di sincronizzazione attiva di SnapMirror e identifica il sito primario corrente.

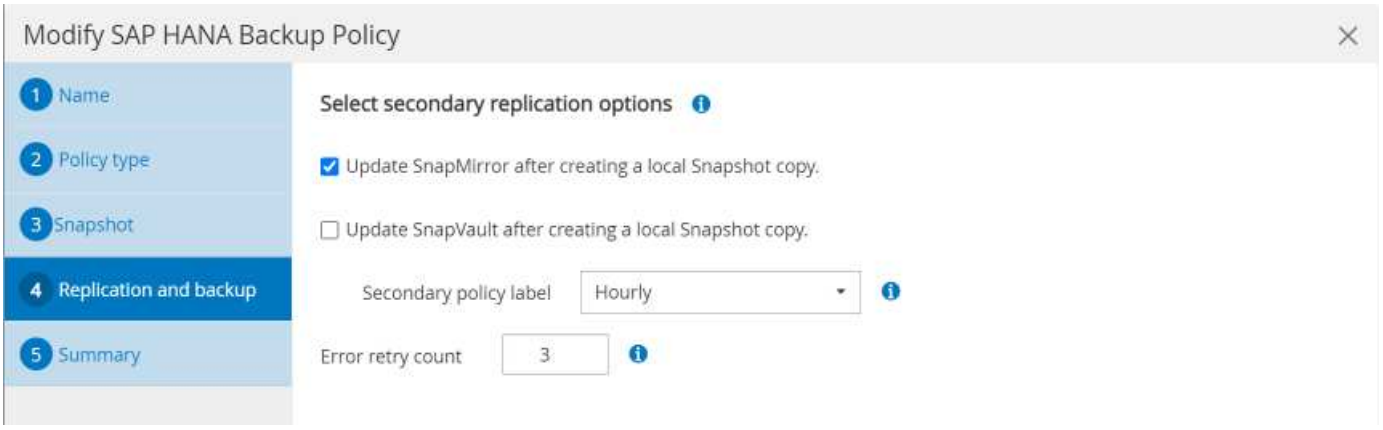
Dopo il rilevamento automatico delle risorse, il sito primario corrente viene mostrato nella sezione Storage Footprint della vista delle risorse. Il rilevamento del sistema di storage master si basa sull'output del comando ONTAP, utilizzato da SnapCenter.

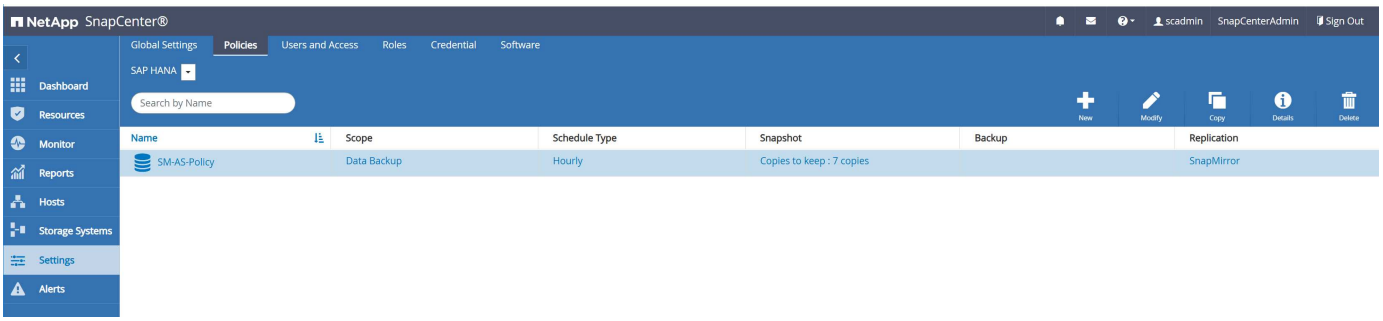
```
volume show -vserver <vs> -volume <vol> -fields smbc-consensus,is-smbc-
master
```



Configurazione dei criteri

Il criterio utilizzato per la risorsa protetta con la sincronizzazione attiva di SnapMirror deve essere configurato utilizzando la replica di SnapMirror anche se SnapCenter non attiva alcuna operazione di aggiornamento di SnapMirror.





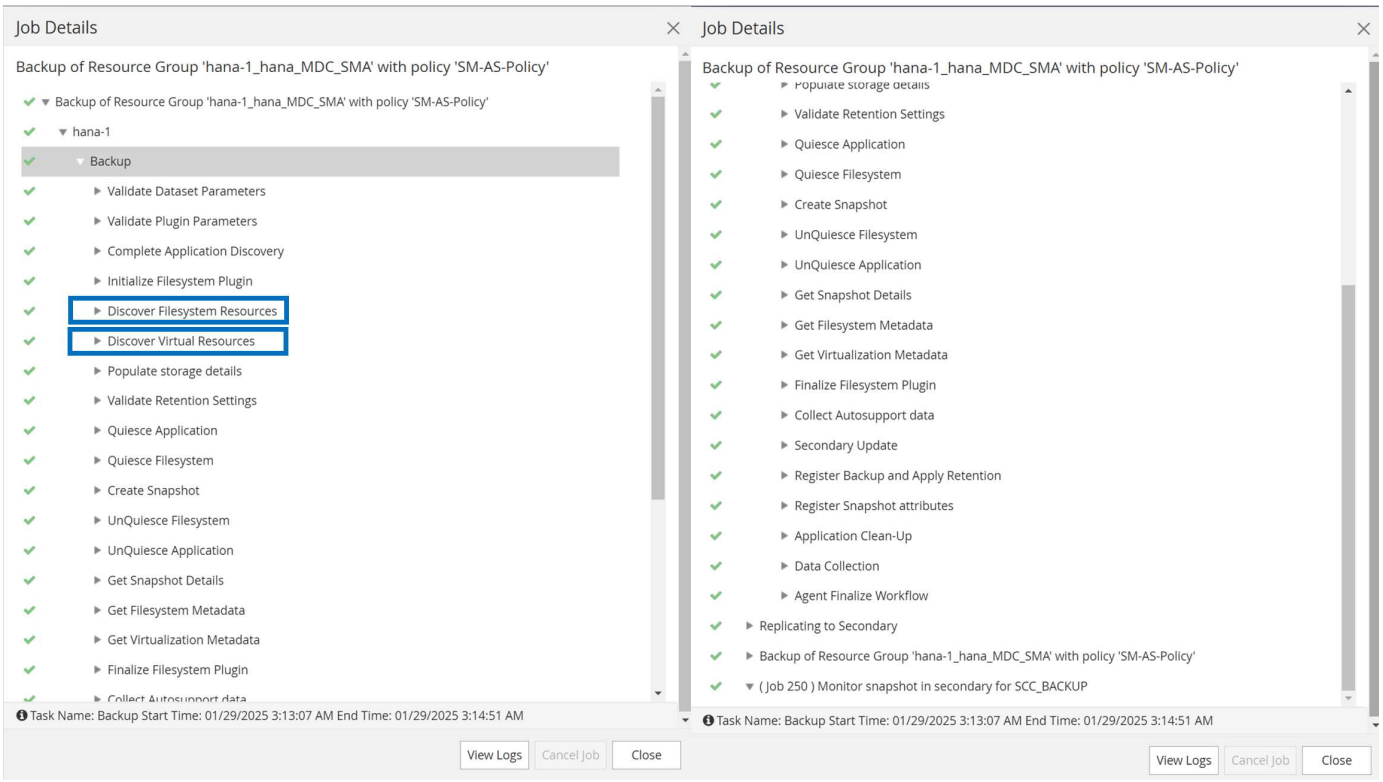
Configurazione di protezione delle risorse HANA

Nessun requisito specifico. La configurazione di protezione delle risorse viene eseguita come di consueto.

Operazioni di backup di SnapCenter

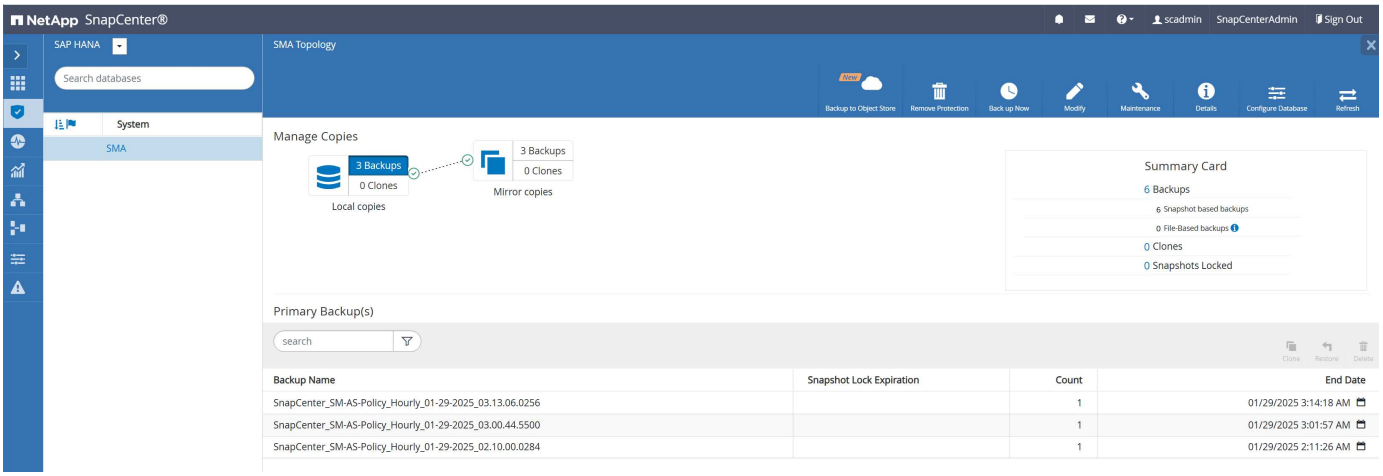
Ad ogni operazione di backup, SnapCenter esegue il rilevamento sul lato VMware e sul

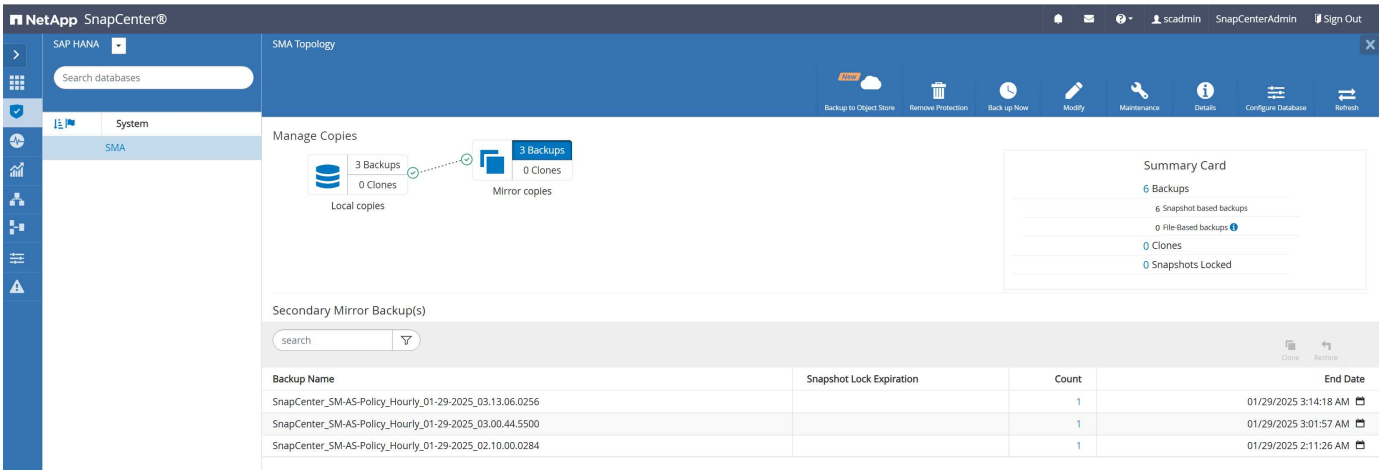
rilevamento del sito primario. In caso di failover dello storage, SnapCenter rileva il nuovo sito primario non appena viene eseguito un backup per la risorsa.



Vista topologia

All'interno della vista della topologia, SnapCenter mostra i backup dei cluster di storage di origine e di destinazione.





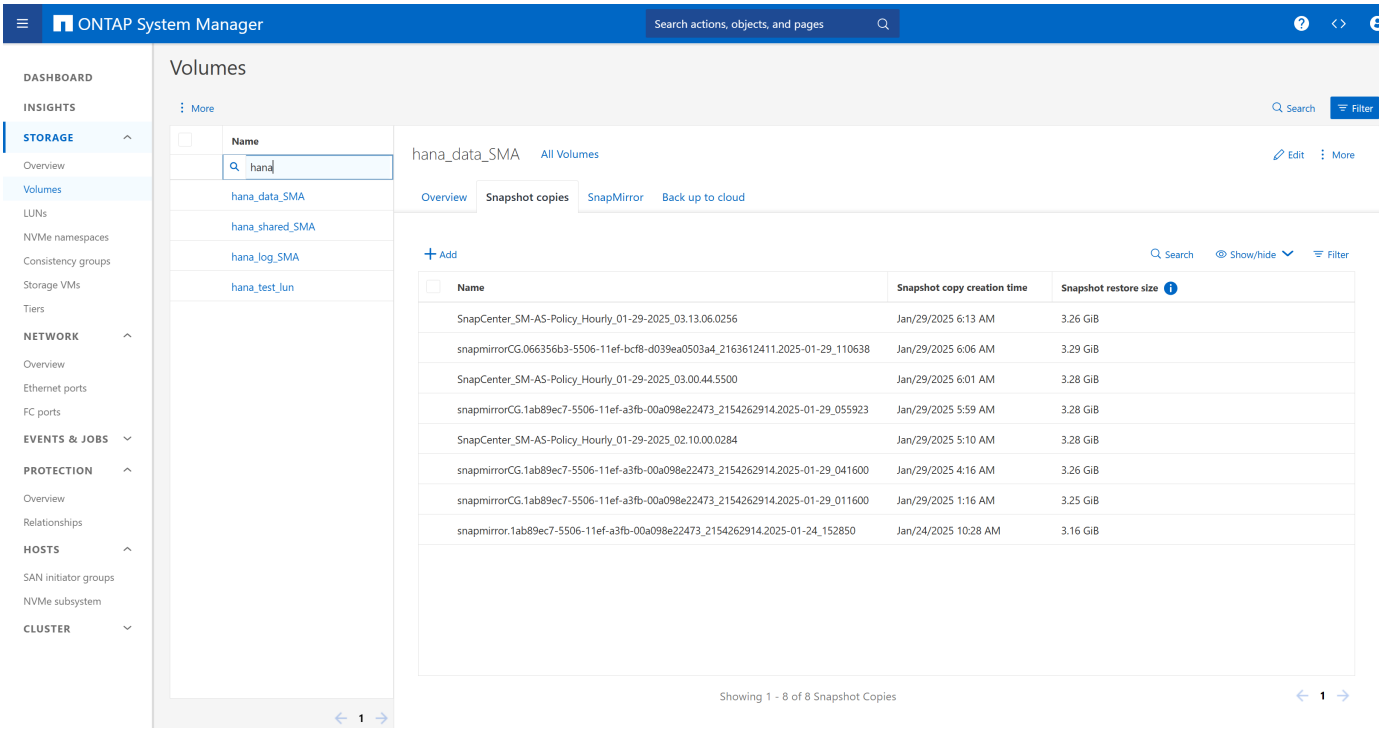
Facendo clic sul numero di conteggio nello storage secondario, viene visualizzata la relazione corrente e la direzione della replica. L'origine è sempre il sito primario corrente. In seguito a un failover dello storage, il sito primario cambierà e la visualizzazione verrà adattata di conseguenza. Tutti i backup hanno sempre la stessa relazione a seconda del sistema di storage che è attualmente il sito primario.



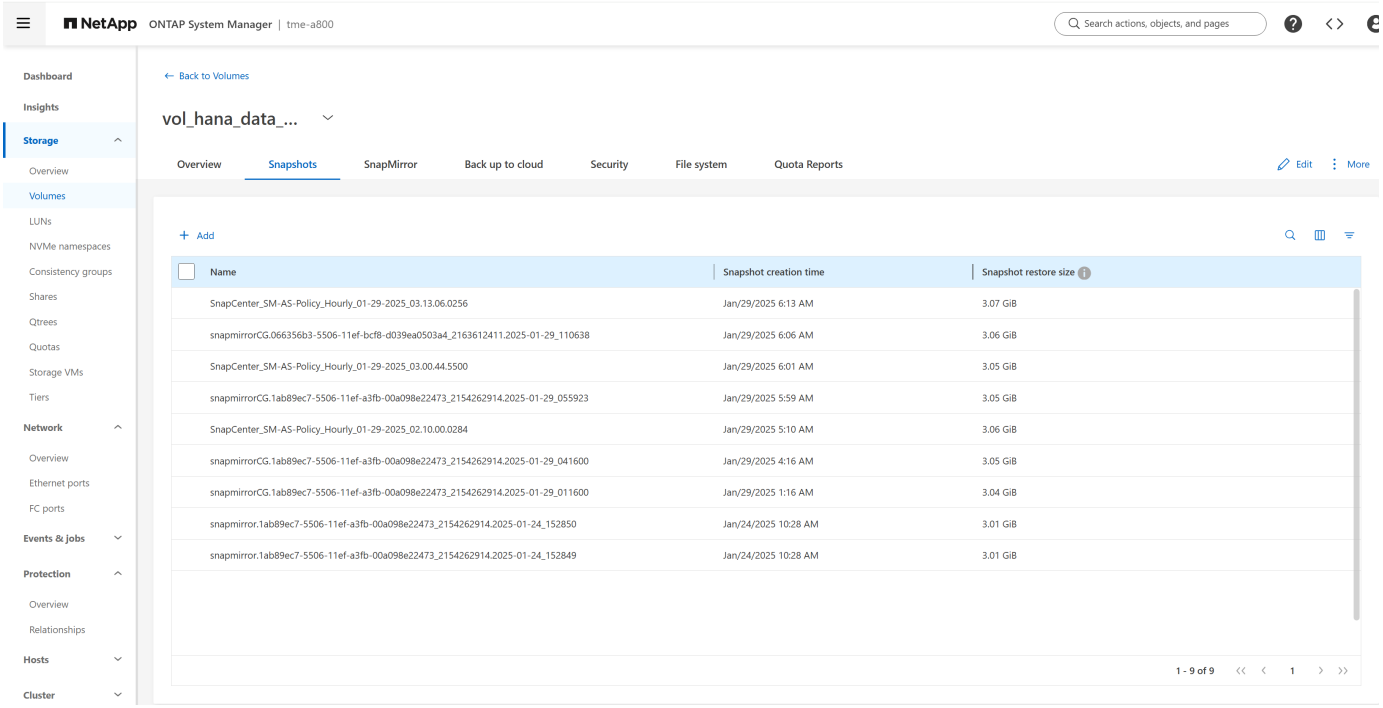
Snapshot nei sistemi di storage

I backup Snapshot creati da SnapCenter sono disponibili per entrambi i volumi di dati HANA in entrambi i sistemi storage. ONTAP crea Snapshot aggiuntive a livello di gruppo di coerenza, disponibili anche per tutti gli altri volumi HANA.

La figura seguente mostra le Snapshot del volume di dati HANA nel cluster A700.



La figura seguente mostra le Snapshot del volume di dati HANA nel cluster A800.



Ripristino e recovery di SnapCenter

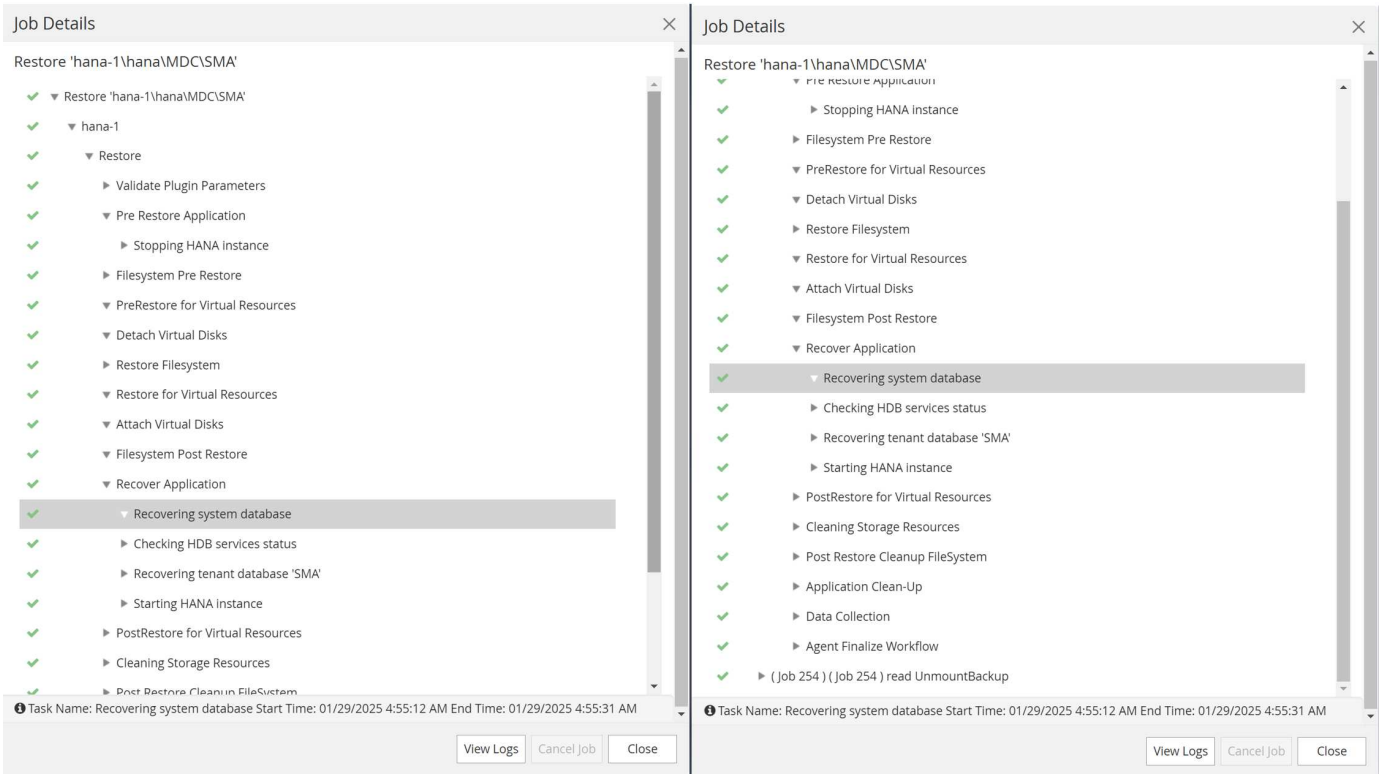
Con le risorse virtuali memorizzate su VMFS/VMDK, un'operazione di ripristino SnapCenter viene sempre eseguita da un'operazione di cloning, montaggio e copia.

1. SnapCenter crea un clone del volume in base alla snapshot selezionata
2. SnapCenter monta la LUN nel volume clonato come nuovo datastore sull'host ESX

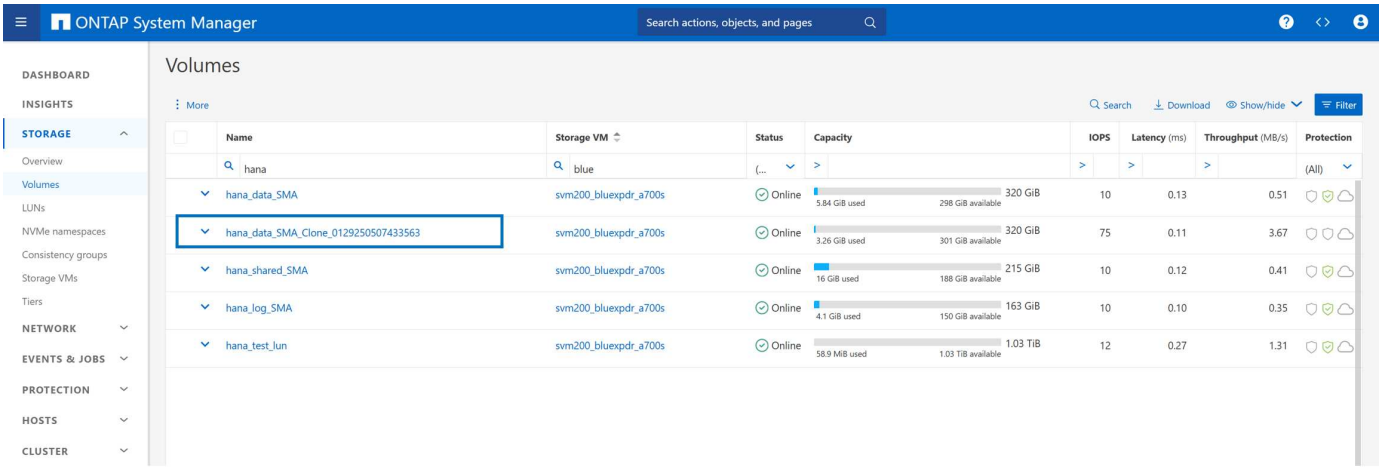
3. SnapCenter aggiunge il VMDK al datastore come nuovo disco alla VM di HANA
4. SnapCenter monta il nuovo disco sul sistema operativo Linux
5. SnapCenter copia i dati dal nuovo disco nella posizione originale
6. Al termine dell'operazione di copia, tutte le risorse precedenti vengono rimosse di nuovo
7. Il recovery di HANA viene eseguito come al solito

Il runtime complessivo dell'operazione di ripristino dipende quindi dalle dimensioni del database e dalla velocità effettiva della connessione FC tra i cluster di storage e gli host ESX.

Inoltre, quando una risorsa è configurata con la sincronizzazione attiva SnapMirror, l'operazione di ripristino SnapCenter può essere selezionata solo nel sito primario corrente.



Durante l'operazione di ripristino e recovery, è possibile visualizzare un nuovo volume clonato, creato nel sito primario corrente.



Nell'host HANA Linux, è possibile vedere un nuovo disco, che è stato montato sull'host. Al termine dell'operazione di ripristino, il disco, il datastore e i volumi verranno rimossi di nuovo da SnapCenter.

```
hana-1:~ # df -h
Filesystem Size Used Avail Use% Mounted on
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 4.0K 49G 1% /dev/shm
tmpfs 13G 58M 13G 1% /run
tmpfs 4.0M 0 4.0M 0% /sys/fs/cgroup
/dev/mapper/system-root 60G 36G 24G 60% /
/dev/mapper/system-root 60G 36G 24G 60% /.snapshots
/dev/mapper/system-root 60G 36G 24G 60% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 36G 24G 60% /home
/dev/mapper/system-root 60G 36G 24G 60% /boot/grub2/x86_64-efi
/dev/mapper/system-root 60G 36G 24G 60% /opt
/dev/mapper/system-root 60G 36G 24G 60% /srv
/dev/mapper/system-root 60G 36G 24G 60% /usr/local
/dev/mapper/system-root 60G 36G 24G 60% /tmp
/dev/mapper/system-root 60G 36G 24G 60% /root
/dev/mapper/system-root 60G 36G 24G 60% /var
/dev/sdb 200G 8.0G 192G 4% /hana/data/SMA/mnt00001
/dev/sdc 120G 7.0G 113G 6% /hana/log/SMA/mnt00001
/dev/sda1 253M 5.1M 247M 3% /boot/efi
/dev/sdd 150G 28G 123G 19% /hana/shared
tmpfs 6.3G 48K 6.3G 1% /run/user/467
tmpfs 6.3G 28K 6.3G 1% /run/user/0
/dev/sde 200G 8.0G 192G 4%
/var/opt/snapcenter/scu/clones/hana_data_SMAmnt00001_255_scu_clone_1
hana-1:~ #
```

Operazione di refresh del sistema SAP

Le operazioni di cloning possono essere eseguite sul sito primario o sullo storage secondario.

Il volume clonato non farà parte del gruppo di coerenza HANA e non verrà replicato con la sincronizzazione attiva SnapMirror.

Informazioni dettagliate sui flussi di lavoro di aggiornamento del sistema sono disponibili all'indirizzo: "TR-4667: Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter"

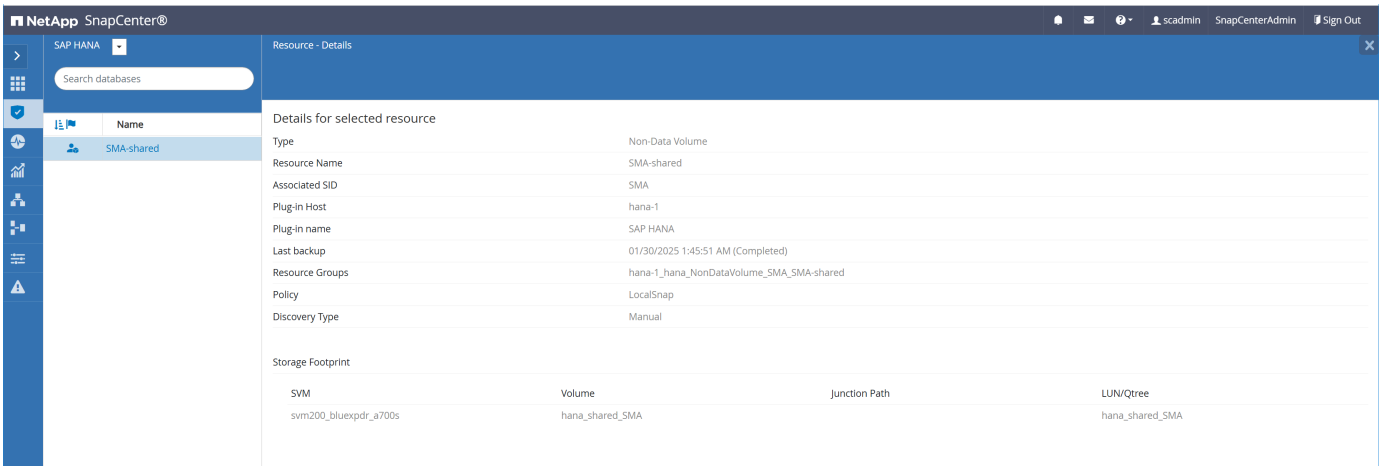
Volumi SnapCenter non dati

Quando le risorse vengono configurate manualmente in SnapCenter e non vengono rilevate automaticamente, SnapCenter non è a conoscenza della sincronizzazione attiva di VMware e SnapMirror. Pertanto, non sono supportati in modo nativo da SnapCenter.

Per i volumi non di dati come HANA condivisi, le operazioni di backup e ripristino potevano comunque essere eseguite utilizzando SnapCenter quando si prendono in considerazione ulteriori passaggi manuali.

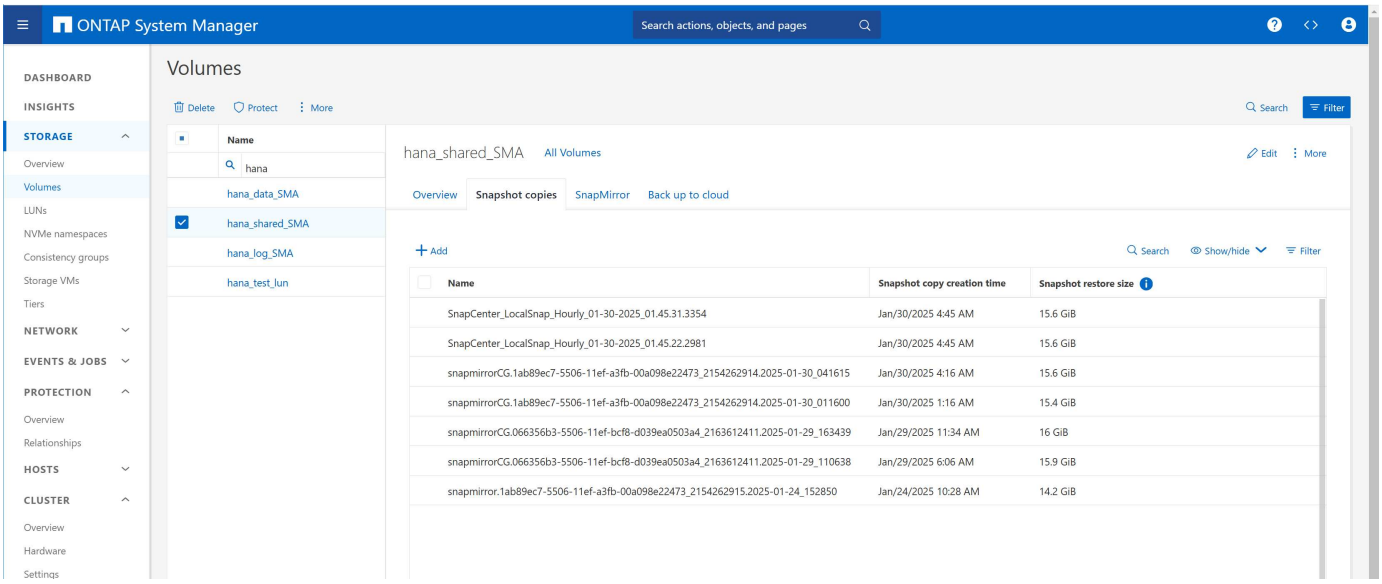
Guasto del sistema storage configurato in SnapCenter

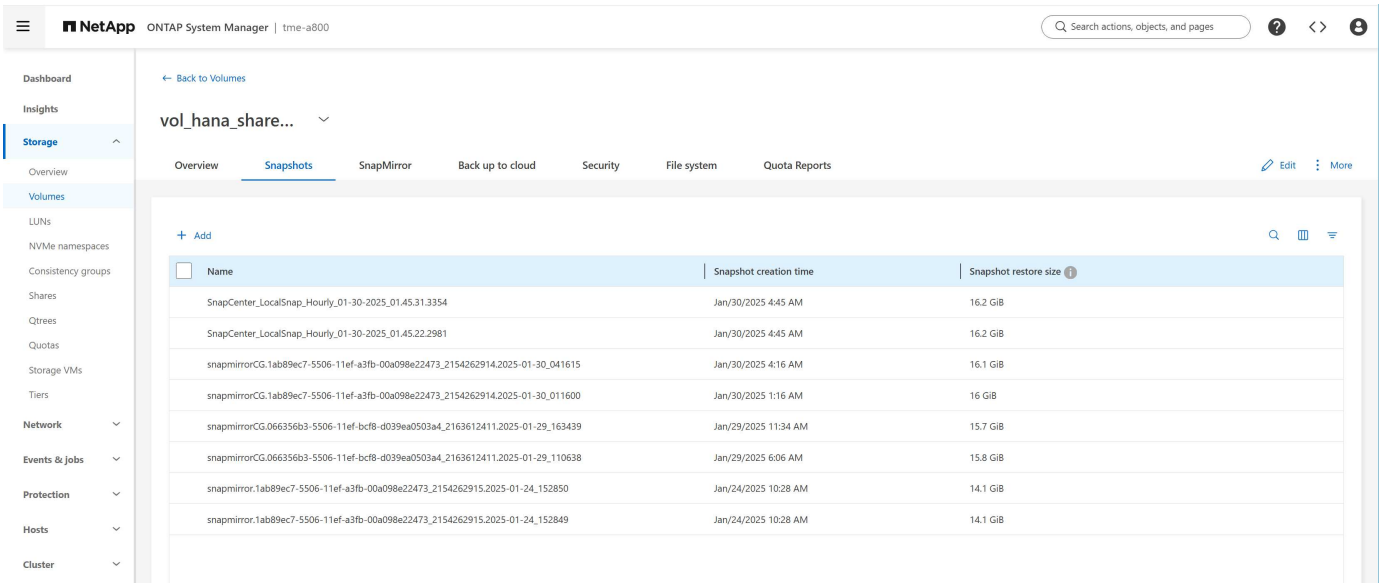
In caso di errore del sistema storage configurato in SnapCenter, SnapCenter non passerà automaticamente all'altro sistema storage. La risorsa del volume non di dati deve essere adattata manualmente in modo che la copia speculare del volume sia utilizzata per le operazioni di backup e ripristino.



Operazioni di backup

Anche se SnapCenter non conosce la configurazione di sincronizzazione attiva di SnapMirror per il volume condiviso HANA, Snapshot viene replicato su entrambi i siti.





Ripristinare l'operazione

In caso di ripristino, SnapCenter eseguirà un ripristino dei volumi senza eseguire alcun passaggio specifico di VMware. Normalmente sarebbe necessario smontare il volume condiviso HANA sull'host Linux, scollegare il datastore, quindi eseguire il ripristino del volume, connettere di nuovo il datastore e montare il file system sull'host Linux. Come operazione manuale, puoi arrestare la VM HANA, ripristinare il volume condiviso HANA con SnapCenter e riavviare nuovamente la VM.

Scenari di failover

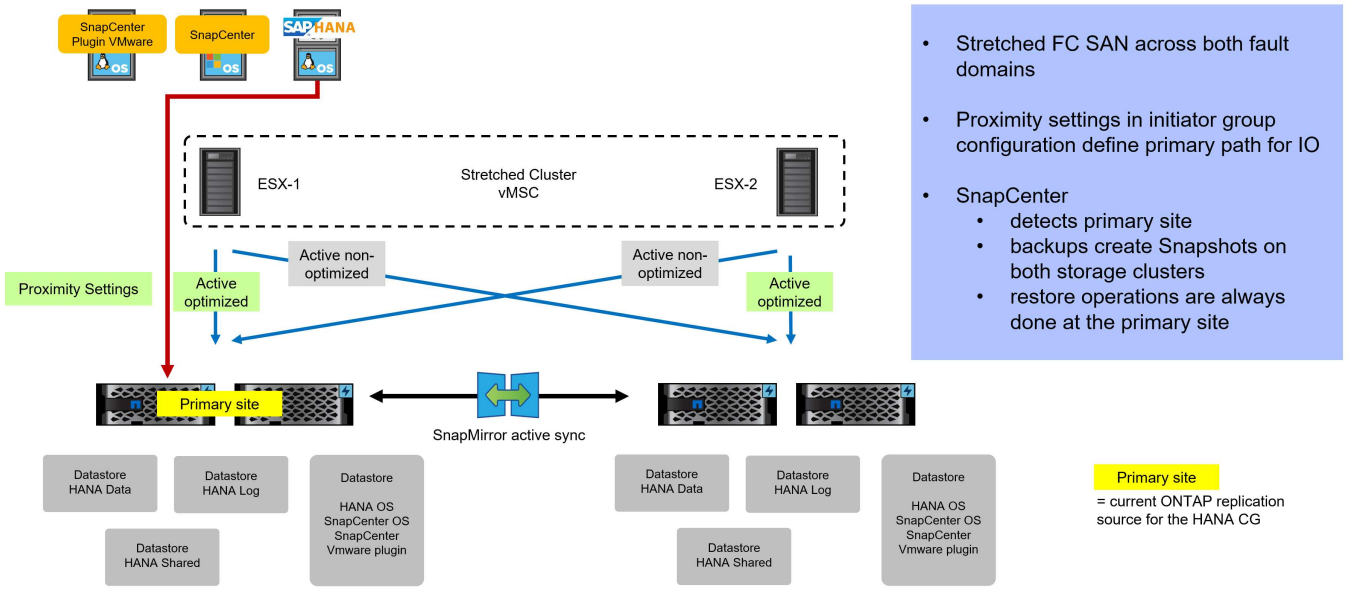
In questo articolo vengono illustrati gli scenari di failover per questa soluzione.

Impostazione dell'accesso uniforme

Con una configurazione di accesso uniforme, la SAN Fibre Channel è estesa a entrambi i siti. Gli host ESX in entrambi i siti possono accedere a entrambe le copie dei set di dati. Durante il normale funzionamento, l'host ESX che esegue il sistema HANA sta accedendo alla copia locale dei dati in base alle impostazioni di prossimità nella configurazione del gruppo iniziatore. Ogni host ESX dispone di un percorso attivo ottimizzato per la copia locale e di un percorso attivo non ottimizzato per la copia con mirroring.

Funzionamento normale

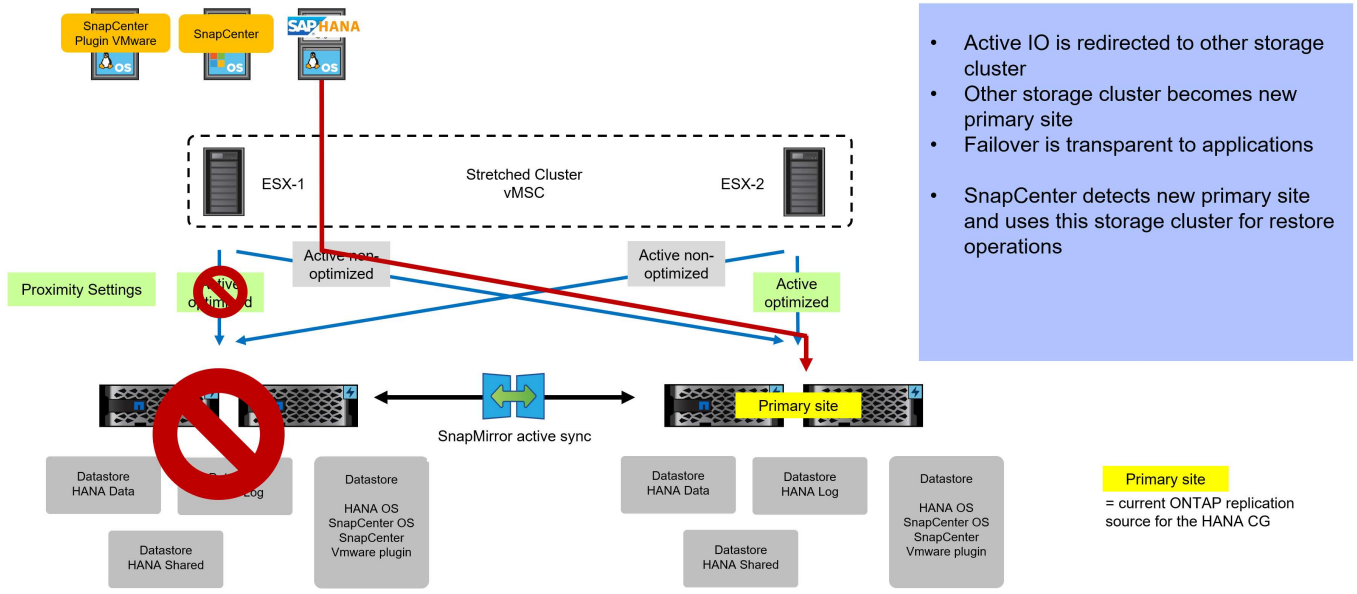
Durante il normale funzionamento, il sistema HANA legge e scrive da/nella copia locale in base al percorso attivo ottimizzato dall'host ESX ESX ESX-1. Ad ogni operazione di backup, SnapCenter rileva il sito primario corrente per la relazione di replica ed esegue le operazioni di backup sul sito primario. Le snapshot vengono replicate nella copia con mirroring e sono disponibili in entrambi i siti. Un'operazione di ripristino SnapCenter viene eseguita sul sito primario.



- Stretched FC SAN across both fault domains
- Proximity settings in initiator group configuration define primary path for IO
- SnapCenter
  - detects primary site
  - backups create Snapshots on both storage clusters
  - restore operations are always done at the primary site

Guasto allo storage

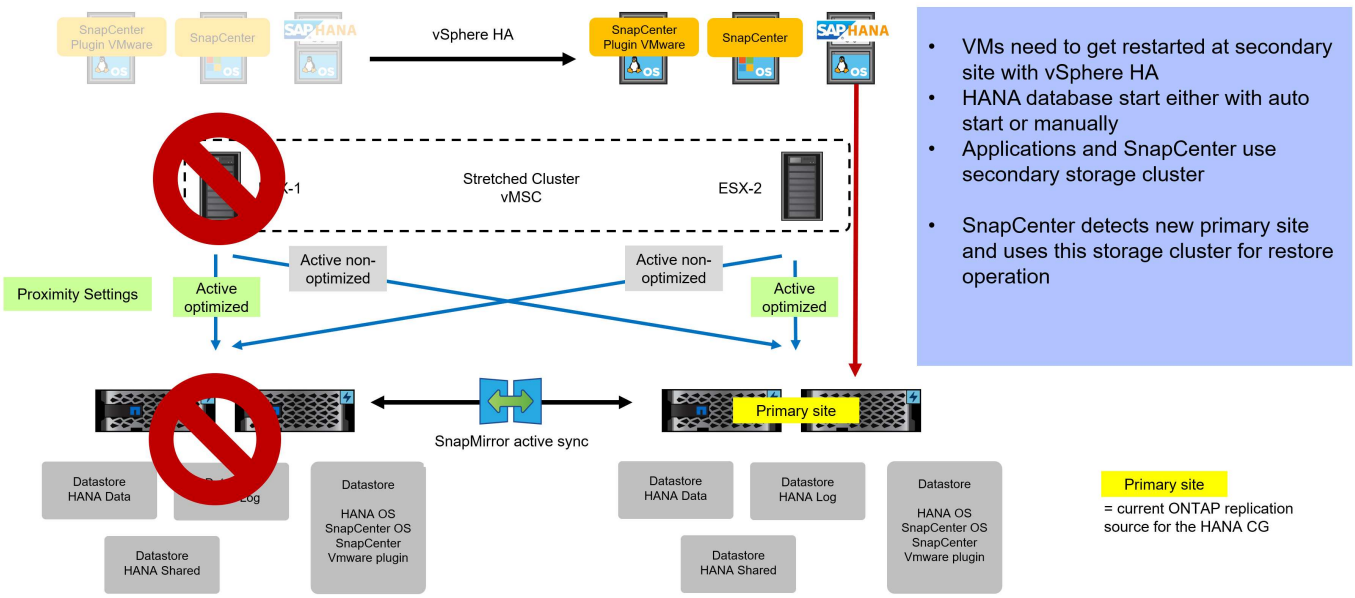
In caso di guasto al sistema storage del sito 1, i sistemi HANA accedono alla copia mirrorata sul sito 2 e continuano a funzionare. Gli switch del sito primario al sito secondario, mentre SnapCenter ora esegue operazioni di backup e ripristino nel nuovo sito primario.



- Active IO is redirected to other storage cluster
- Other storage cluster becomes new primary site
- Failover is transparent to applications
- SnapCenter detects new primary site and uses this storage cluster for restore operations

Guasto del sito

In caso di guasto a un sito, la VM di HANA, SnapCenter e il plug-in VM di SnapCenter per VMware eseguiranno il failover sull'host ESX nel sito secondario, utilizzando vSphere ha. Il database HANA deve essere avviato e quindi accedere alla copia con mirroring nel secondo sito. Gli switch del sito primario al sito secondario, mentre SnapCenter ora esegue operazioni di backup e ripristino nel nuovo sito primario.

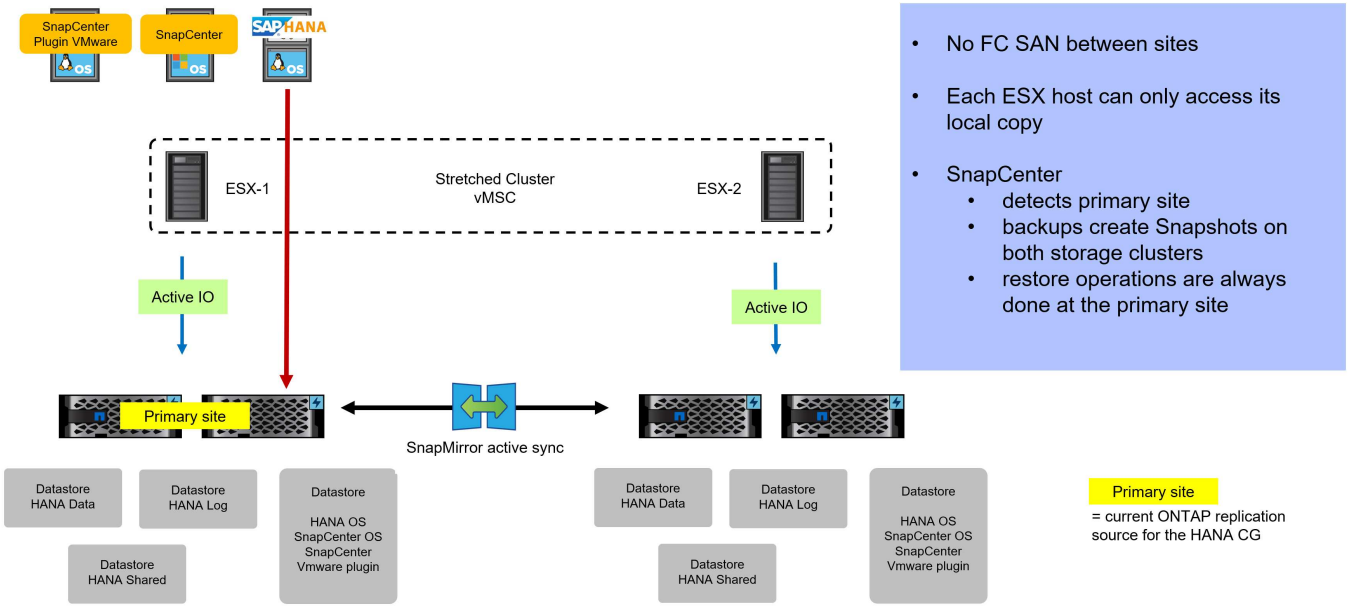


Impostazione accesso non uniforme

Con una configurazione di accesso non uniforme, la SAN Fibre Channel non è limitata ad entrambi i siti. Ogni host ESX di ciascun sito può accedere solo alla copia locale dei set di dati.

Funzionamento normale

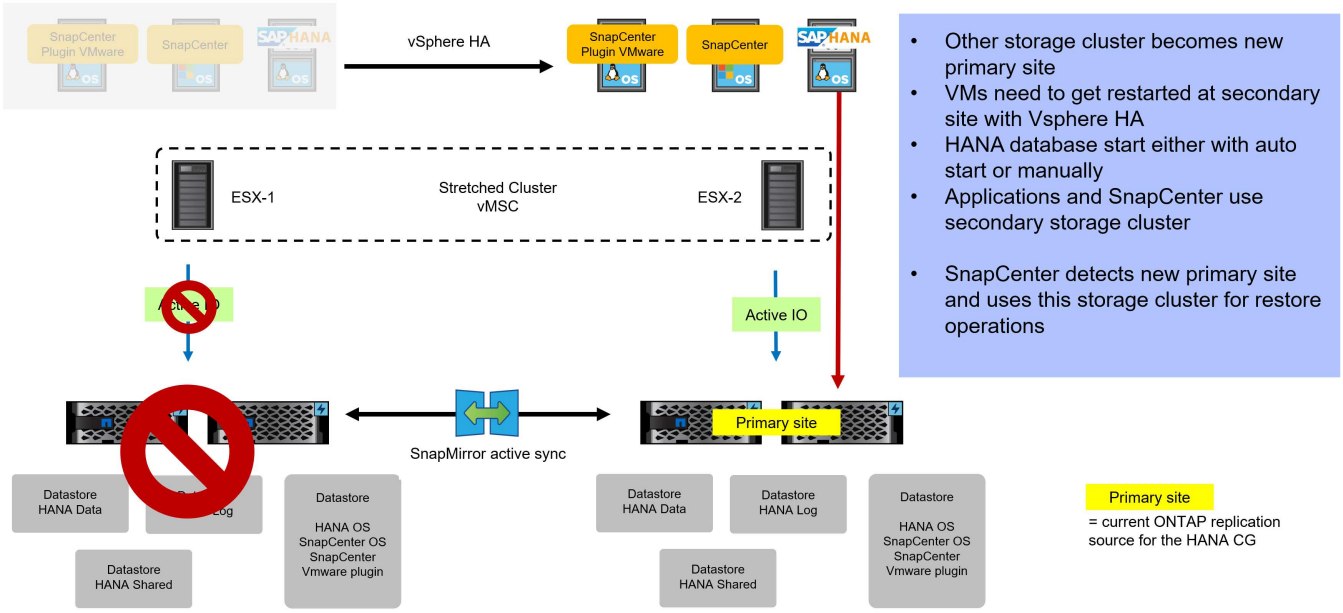
Durante il normale funzionamento, il sistema HANA legge e scrive da/sulla copia locale. Ad ogni operazione di backup, SnapCenter rileva il sito primario corrente per la relazione di replica ed esegue le operazioni di backup sul sito primario. Le snapshot vengono replicate nella copia con mirroring e sono disponibili in entrambi i siti. Un'operazione di ripristino SnapCenter viene eseguita sul sito primario.



Guasto allo storage

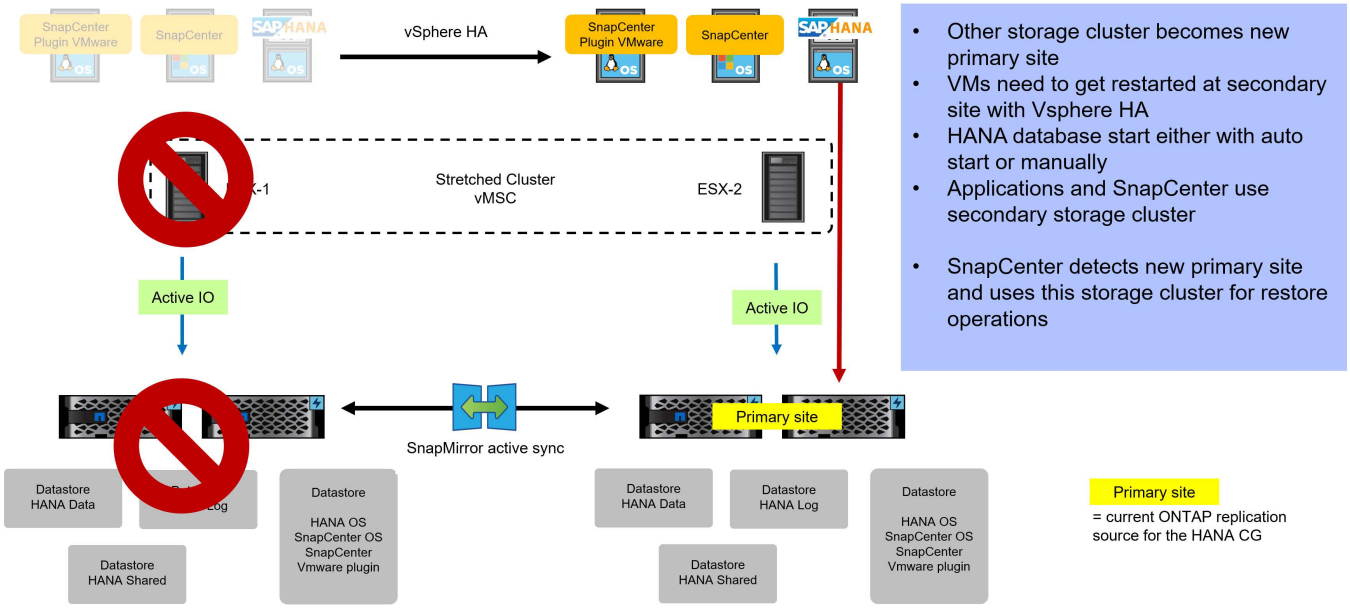
In caso di guasto dello storage, la VM HANA così come SnapCenter e il plug-in SnapCenter per VMware eseguiranno il failover sull'host ESX nel sito secondario, utilizzando vSphere ha. Il database HANA deve essere avviato e quindi accedere alla copia con mirroring nel secondo sito. Gli switch del sito primario al sito

secondario, mentre SnapCenter ora esegue operazioni di backup e ripristino nel nuovo sito primario.



Guasto del sito

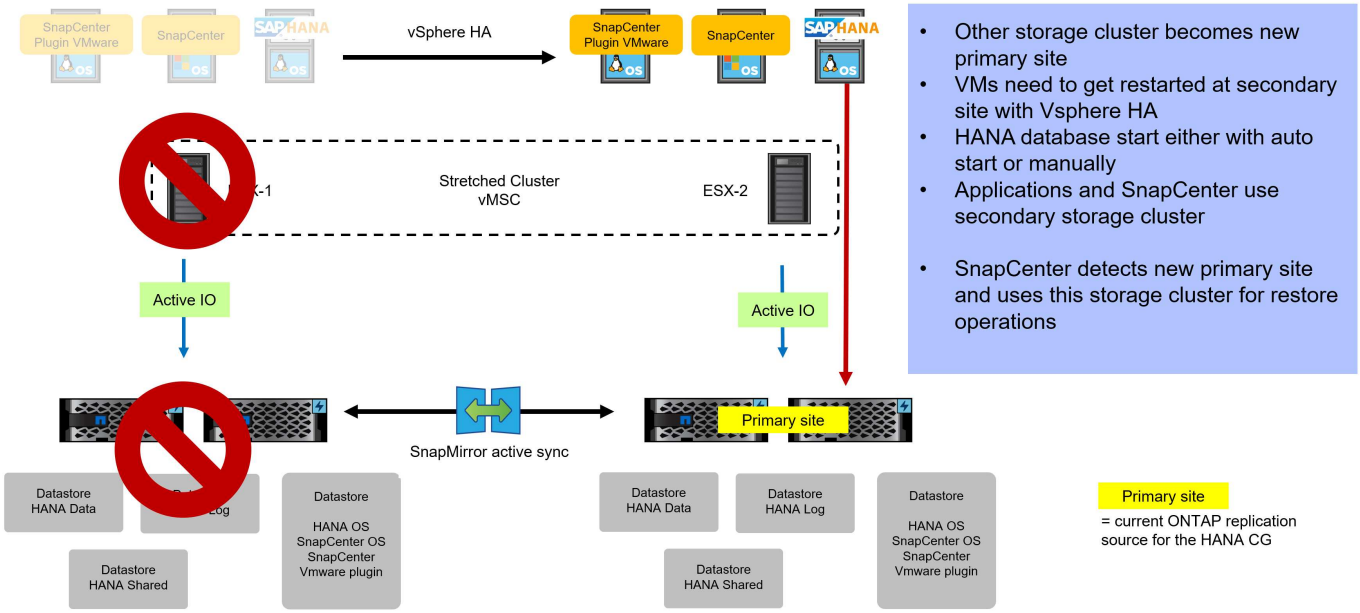
Come per il guasto dello storage.



Trasferimento di HANA VM o sito primario

Se la VM di HANA viene ricollocata sull'altro host ESX e il sito primario dello storage rimane invariato, un'operazione di ripristino con SnapCenter fallirà. Poiché SnapCenter utilizza il sito primario per eseguire le operazioni di ripristino, il clone verrà creato a sinistra, mentre la VM HANA viene eseguita a destra. Poiché non vi è alcun percorso di dati tra i siti, SnapCenter non verrà copia i dati.

Per risolvere il problema, è necessario assicurarsi che il trasferimento della VM e del lato primario avvenga insieme oppure è necessario eseguire il failover del sito primario prima dell'operazione di ripristino con SnapCenter.



- Other storage cluster becomes new primary site
- VMs need to get restarted at secondary site with Vsphere HA
- HANA database start either with auto start or manually
- Applications and SnapCenter use secondary storage cluster
- SnapCenter detects new primary site and uses this storage cluster for restore operations

Informazioni aggiuntive e cronologia delle versioni

In questo articolo vengono forniti collegamenti a ulteriori risorse rilevanti per questa soluzione.

SnapCenter:

"TR-4614: Backup e recovery SAP HANA con SnapCenter"

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

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

"Documentazione del software SnapCenter"

Sincronizzazione attiva SnapMirror:

"Panoramica della sincronizzazione attiva di SnapMirror in ONTAP"

"NetApp ONTAP con sincronizzazione attiva NetApp SnapMirror con VMware vSphere Metro Storage Cluster (vMSC)."

"Cluster di storage VMware vSphere Metro con sincronizzazione attiva SnapMirror"

"VMware vSphere Metro Storage Cluster (vMSC)"

Cronologia versioni:

Versione	Data	Commento
Versione 1.0	Marzo 2025	Versione iniziale

Protezione dei dati SAP HANA con SnapCenter con sistemi VMware VMFS e NetApp ASA

Protezione dei dati SAP HANA con SnapCenter con sistemi VMware VMFS e NetApp ASA

In questo documento vengono illustrate le best practice per la protezione dei dati mediante SnapCenter per sistemi HANA in esecuzione su VMware con datastore che utilizzano VMFS e LUN archiviate su sistemi NetApp ASA .

Autore: Nils Bauer, NetApp

Scopo del presente documento

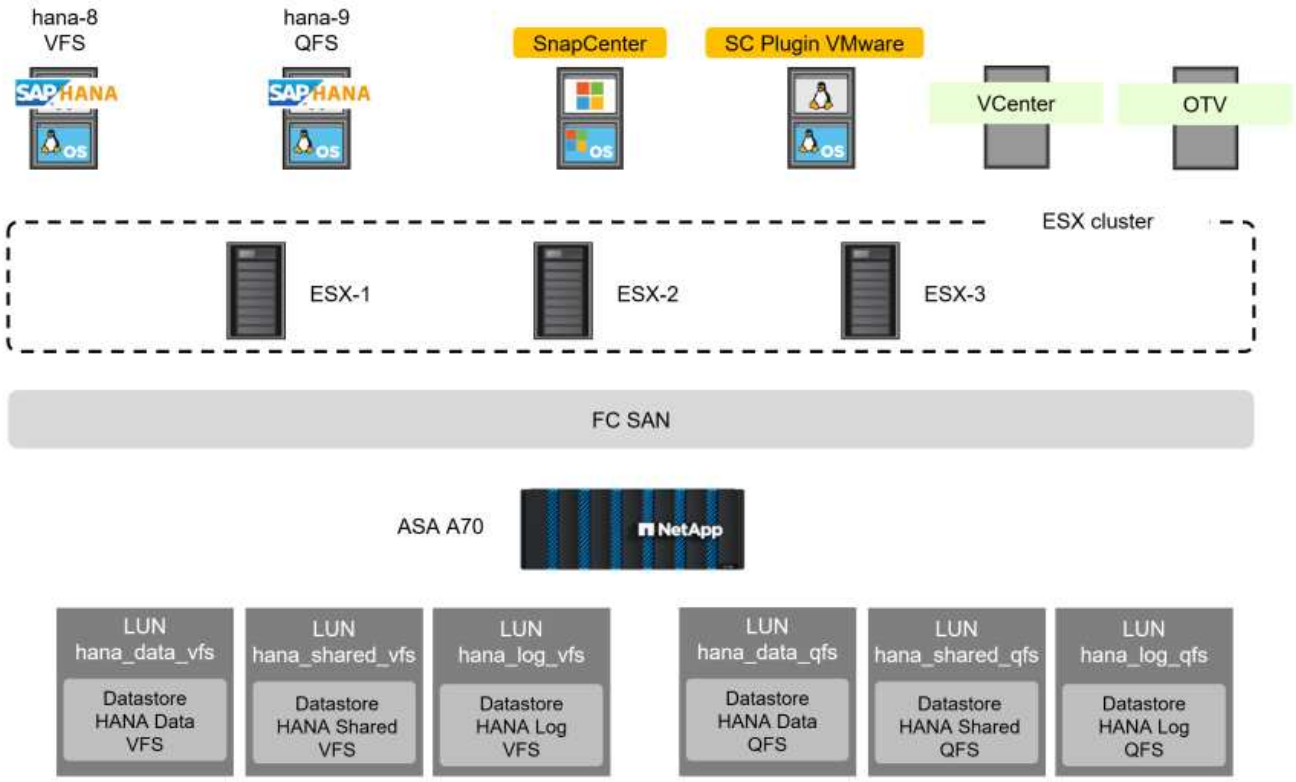
Non costituisce una guida dettagliata per la configurazione dell'intero ambiente, ma si concentra sui dettagli specifici di SnapCenter e HANA su VMFS, tra cui:

- Configurazione dei sistemi SAP HANA con VMware VMFS
- Configurazioni specifiche SnapCenter per HANA su VMware con VMFS
- Operazioni di backup, ripristino e ripristino SnapCenter per HANA su VMware con VMFS
- Operazioni di aggiornamento del sistema SAP SnapCenter per HANA su VMware con VMFS

Per ulteriori informazioni e istruzioni dettagliate sulla configurazione, fare riferimento ai documenti elencati nella ""Informazioni aggiuntive"" capitolo.

Configurazione di laboratorio utilizzata per questo documento

La figura seguente presenta una panoramica generale della configurazione di laboratorio utilizzata. Due sistemi MDC HANA a host singolo vengono utilizzati per dimostrare le varie operazioni. Il VFS del sistema HANA è destinato all'esecuzione di operazioni di backup, ripristino e ripristino, mentre il QFS del sistema HANA funge da sistema di destinazione per le operazioni di aggiornamento del sistema SAP. Il plug-in SnapCenter per VMware è essenziale per consentire a SnapCenter di gestire le risorse HANA configurate con VMware VMFS. Sebbene siano stati utilizzati strumenti ONTAP per VMware per il provisioning delle unità di storage per i sistemi HANA, questi non sono un componente obbligatorio.



Versioni software

Software	Versione
ONTAP	ASA A70 ONTAP 9.16.1
Client vSphere	8.0.3
ESXi	8.0.3
Plug-in SnapCenter per vSphere	6.1.0
Strumenti ONTAP per VMware vSphere	10,4
OS Linux	SLES PER SAP 15 SP6
SAP HANA	2,0 SPS8
SnapCenter	6.1P1

Provisioning e installazione del sistema HANA

Questo capitolo descrive l'installazione e la configurazione del sistema SAP HANA specifico per una configurazione VMware utilizzando VMFS. Ulteriori procedure consigliate generiche sono disponibili all'indirizzo "SAP HANA su sistemi NetApp ASA con protocollo Fibre Channel".

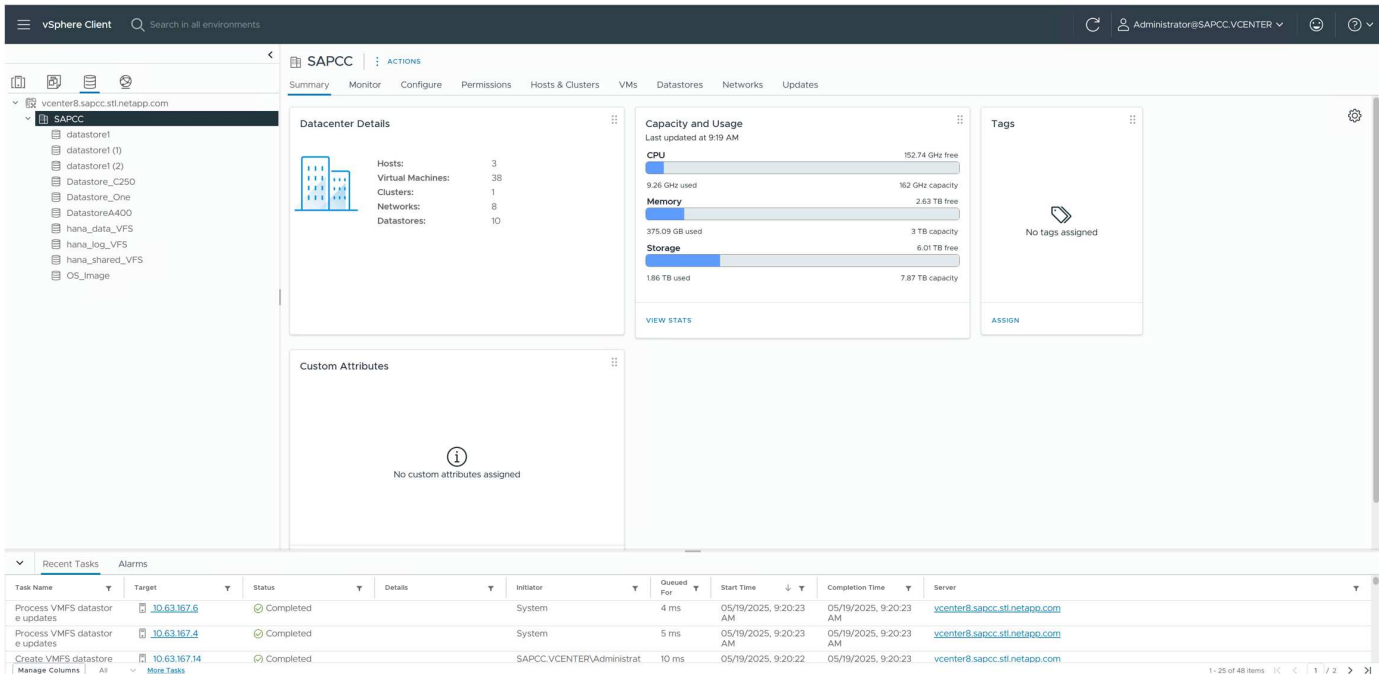
Configurazione dello storage

Per soddisfare i KPI di prestazioni di storage definiti da SAP per i sistemi HANA di produzione, è necessario configurare LUN e datastore dedicati per i file system di dati e log del sistema HANA. I datastore non devono essere condivisi tra più sistemi HANA o altri carichi di lavoro.

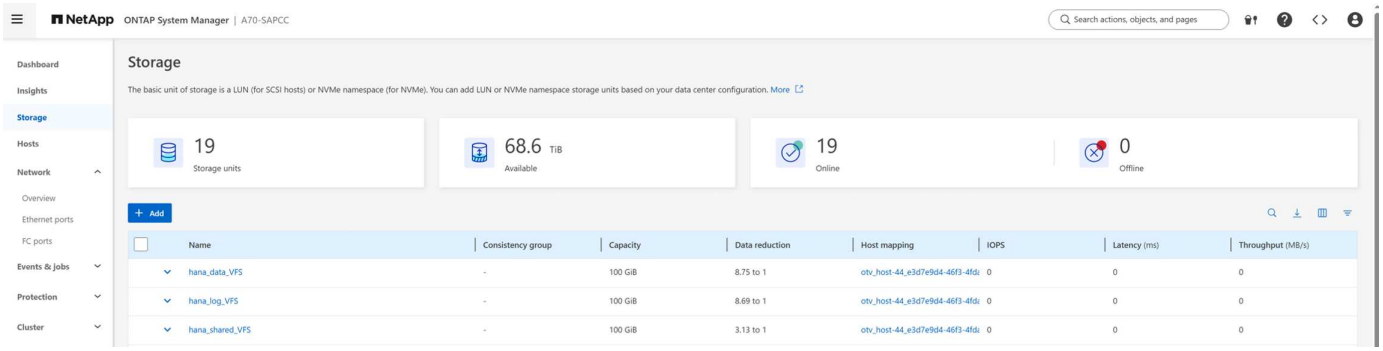
Per predisporre i tre datastore per il sistema HANA VFS sono stati utilizzati gli strumenti ONTAP per VMware (OTV).

- hana_dati_VFS
- hana_log_VFS
- hana_condiviso_VFS

> L'archivio dati per il file system condiviso HANA può essere condiviso anche tra più sistemi HANA.

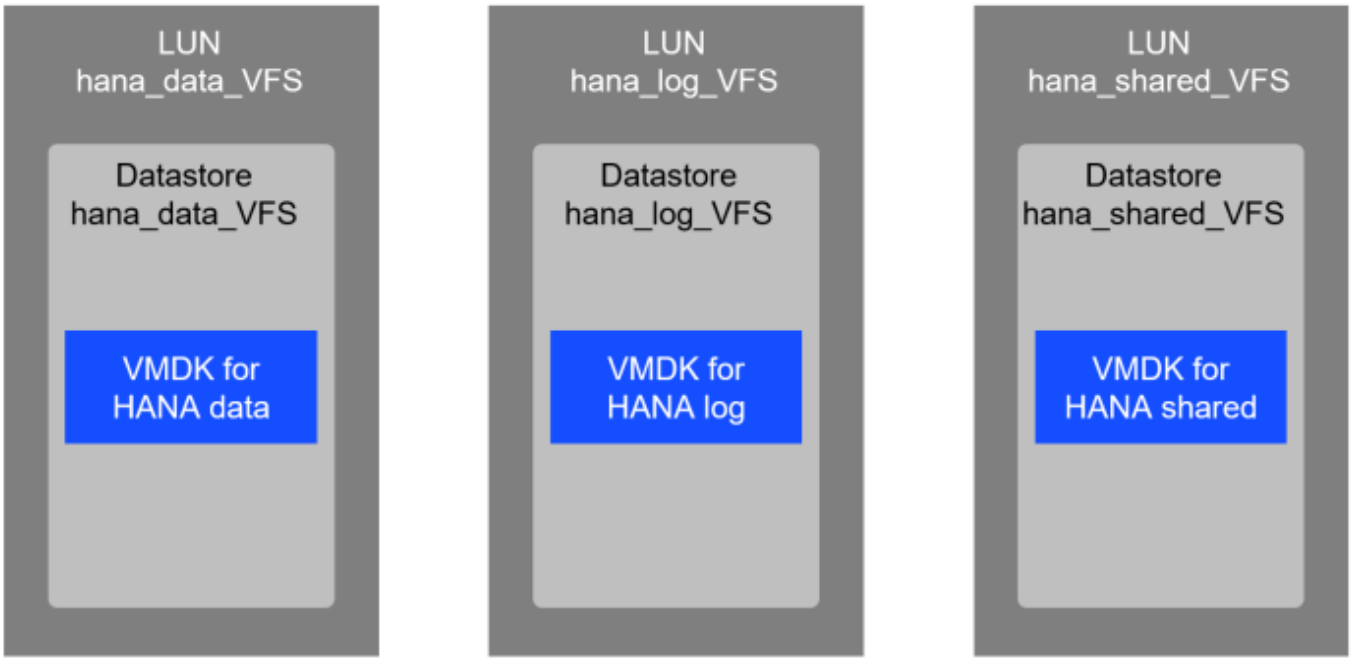


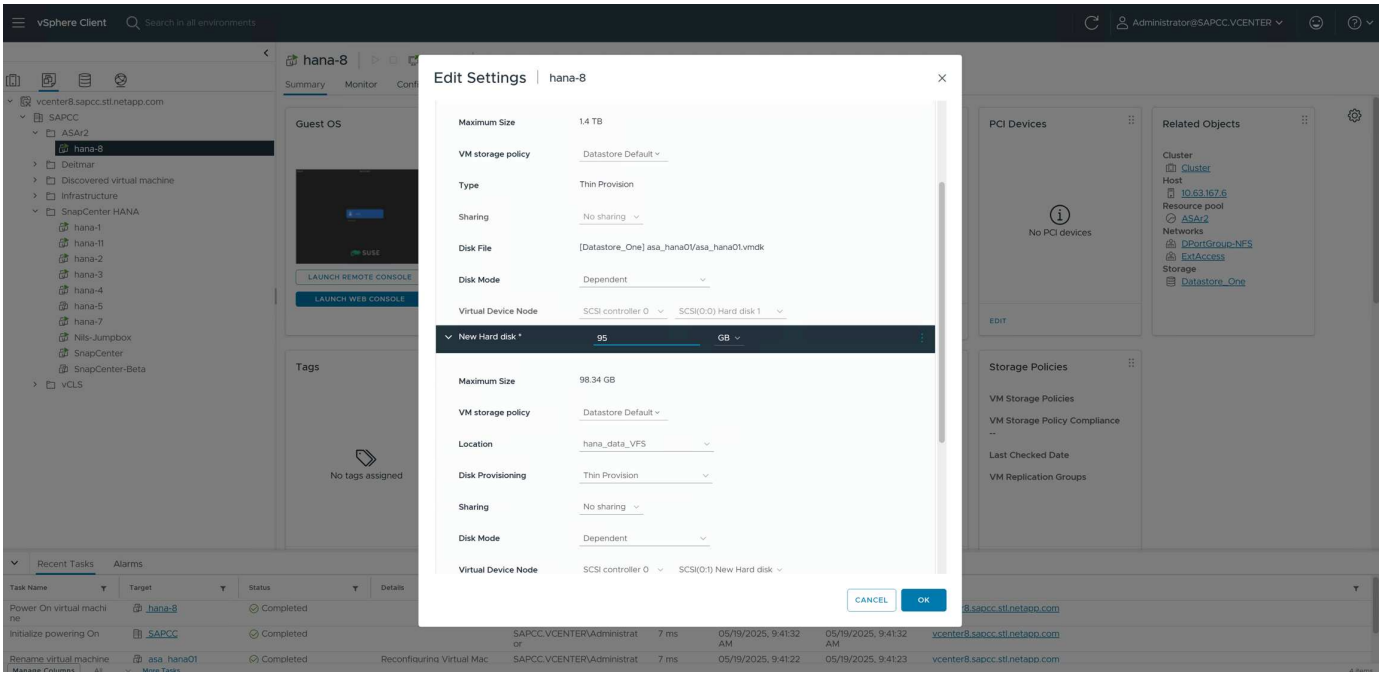
Nel sistema di archiviazione sono state create tre LUN da OTV.

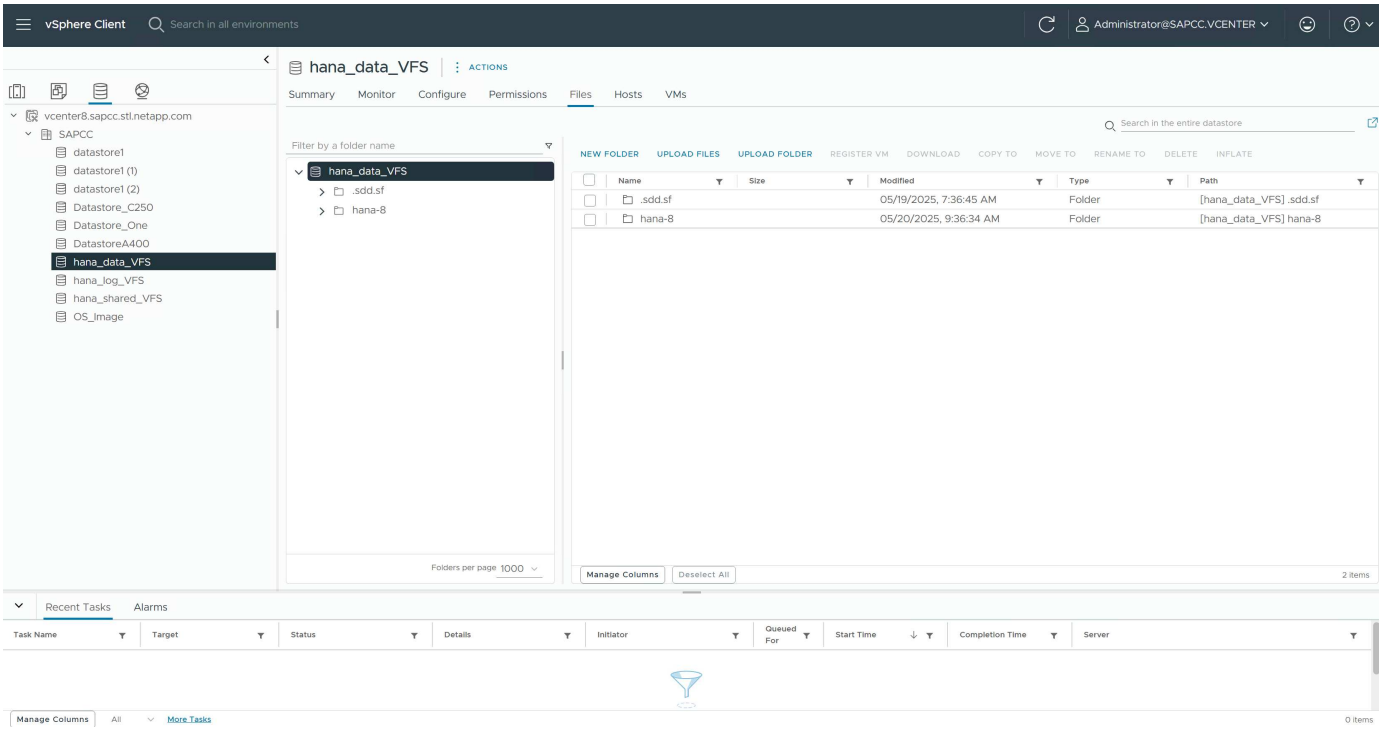


Configurazione dei dischi delle macchine virtuali

È necessario aggiungere tre nuovi dischi (VMDK) alla VM HANA. Ogni disco deve essere all'interno di uno dei datastore creati in precedenza, come illustrato nell'immagine seguente.


LUN
hana_data_VFS
Datastore
hana_data_VFS
VMDK for
HANA data
LUN
hana_log_VFS
Datastore
hana_log_VFS
VMDK for
HANA log
LUN
hana_shared_VFS
Datastore
hana_shared_VFS
VMDK for
HANA shared


vSphere Client
Edit Settings
hana-8
Maximum Size
1.4 TB
VM storage policy
Datastore Default
Type
Thin Provision
Sharing
No sharing
Disk File
[Datastore_One] asa_hana01/asa_hana01.vmdk
Disk Mode
Dependent
Virtual Device Node
SCSI controller 0
SCSI(0:0) Hard disk 1
New Hard disk *
95
GB
Maximum Size
98.34 GB
VM storage policy
Datastore Default
Location
hana_data_VFS
Disk Provisioning
Thin Provision
Sharing
No sharing
Disk Mode
Dependent
Virtual Device Node
SCSI controller 0
SCSI(0:1) New Hard disk
CANCEL
OK



Una volta aggiunti i tre dischi alla VM, è possibile elencarli a livello di sistema operativo.

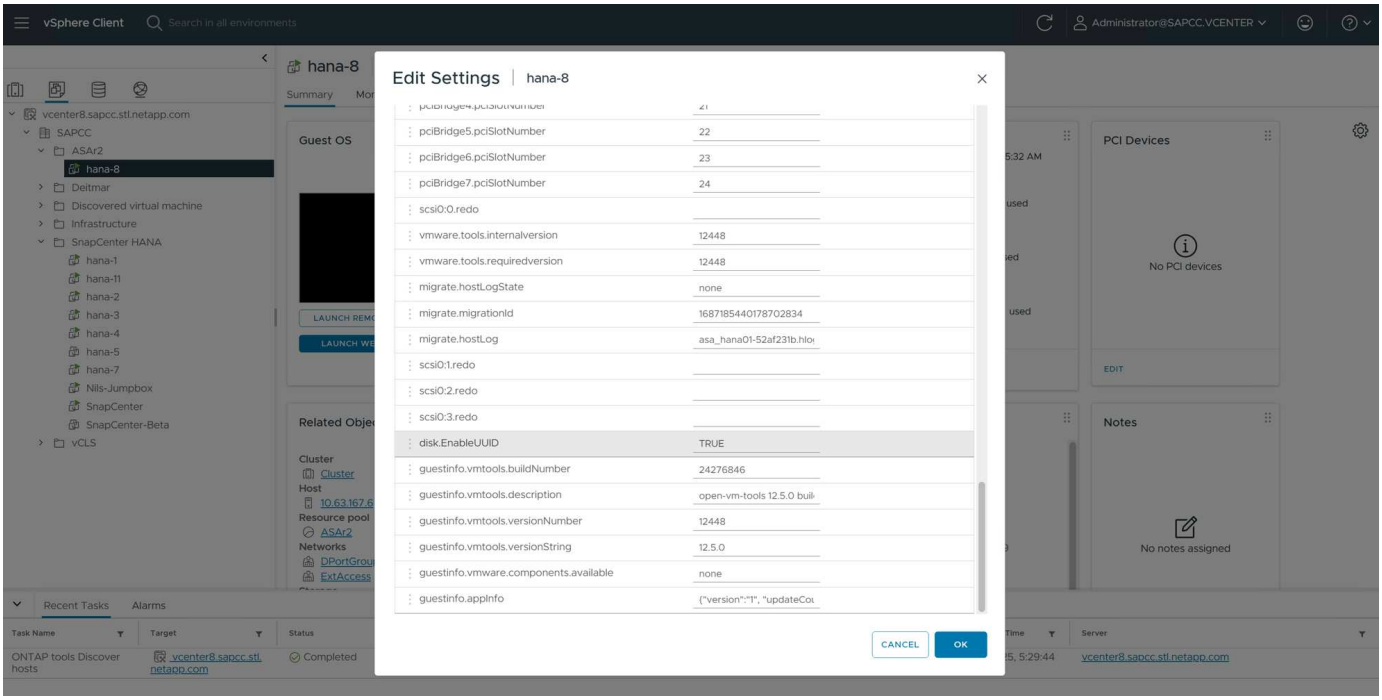
```
hana-8:~ # lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 100G 0 disk
├─sda1 8:1 0 256M 0 part /boot/efi
└─sda2 8:2 0 82G 0 part
├─system-root 254:0 0 60G 0 lvm /root
│ /var
│ /usr/local
│ /tmp
│ /srv
│ /opt
│ /home
│ /boot/grub2/x86++_++64-efi
│ /boot/grub2/i386-pc
│ /.snapshots
│ /
└─system-swap 254:1 0 2G 0 lvm [SWAP]
sdb 8:16 0 95G 0 disk
sdc 8:32 0 95G 0 disk
sdd 8:48 0 95G 0 disk
sr0 11:0 1 17.1G 0 rom
```

Parametro VM disk.EnableUUID

Questo parametro deve essere impostato di conseguenza, altrimenti il rilevamento automatico del database

SnapCenter fallirà.

1. Arresto della macchina virtuale
2. Aggiungere il nuovo parametro “disk.EnableUUID” e impostarlo su “TRUE”
3. Avvia VM



Preparazione del file system all’host Linux

Creazione del filesystem xfs su nuovi dischi

Su ciascuno dei tre nuovi dischi è stato creato un file system xfs.

```
hana-8:~ # mkfs.xfs /dev/sdb
meta-data=/dev/sdb isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nrext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.

hana-8:~ # mkfs.xfs /dev/sdc
meta-data=/dev/sdc isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nrext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.

hana-8:~ # mkfs.xfs /dev/sdd
meta-data=/dev/sdd isize=512 agcount=4, agsize=6225920 blks
= sectsz=512 attr=2, projid32bit=1
= crc=1 finobt=1, sparse=1, rmapbt=1
= reflink=1 bigtime=1 inobtcount=0 nrext64=0
data = bsize=4096 blocks=24903680, imaxpct=25
= sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0, ftype=1
log =internal log bsize=4096 blocks=16384, version=2
= sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
Discarding blocks...Done.

hana-8:~ #
```

Creazione di punti di montaggio

```
hana-8:/ # mkdir -p /hana/data/VFS/mnt00001
hana-8:/ # mkdir -p /hana/log/VFS/mnt00001
hana-8:/ # mkdir -p /hana/shared
hana-8:/ # chmod –R 777 /hana/log/SMA
hana-8:/ # chmod –R 777 /hana/data/SMA
hana-8:/ # chmod -R 777 /hana/shared
```

Configurazione di /etc/fstab

```
hana-8:/ # cat /etc/fstab

/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=/@/var 0 0
/dev/system/root /usr/local btrfs subvol=/@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=/@/tmp 0 0
/dev/system/root /srv btrfs subvol=/@/srv 0 0
/dev/system/root /root btrfs subvol=/@/root 0 0
/dev/system/root /opt btrfs subvol=/@/opt 0 0
/dev/system/root /home btrfs subvol=/@/home 0 0
/dev/system/root /boot/grub2/x86++_++64-efi btrfs
subvol=/@/boot/grub2/x86++_++64-efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=/@/.snapshots 0 0
UUID=FB79-24DC /boot/efi vfat utf8 0 2
### SAPCC_share
192.168.175.86:/sapcc_share /mnt/sapcc-share nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
/dev/sdb /hana/data/VFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/VFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
hana-8:/ #

hana-8:/ # df -h
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 4.4G 54G 8% /
devtmpfs 4.0M 0 4.0M 0% /dev
tmpfs 49G 0 49G 0% /dev/shm
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 18M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
```

```
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/mapper/system-root 60G 4.4G 54G 8% /.snapshots
/dev/mapper/system-root 60G 4.4G 54G 8% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 4.4G 54G 8% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 4.4G 54G 8% /home
/dev/mapper/system-root 60G 4.4G 54G 8% /opt
/dev/mapper/system-root 60G 4.4G 54G 8% /srv
/dev/mapper/system-root 60G 4.4G 54G 8% /tmp
/dev/mapper/system-root 60G 4.4G 54G 8% /usr/local
/dev/mapper/system-root 60G 4.4G 54G 8% /var
/dev/sda1 253M 5.9M 247M 3% /boot/efi
/dev/mapper/system-root 60G 4.4G 54G 8% /root
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
192.168.175.86:/sapcc_share 1.4T 840G 586G 59% /mnt/sapcc-share
/dev/sdb 95G 1.9G 94G 2% /hana/data/VFS/mnt00001
/dev/sdc 95G 1.9G 94G 2% /hana/log/VFS/mnt00001
/dev/sdd 95G 1.9G 94G 2% /hana/shared

hana-8:/ #
```

Installazione HANA

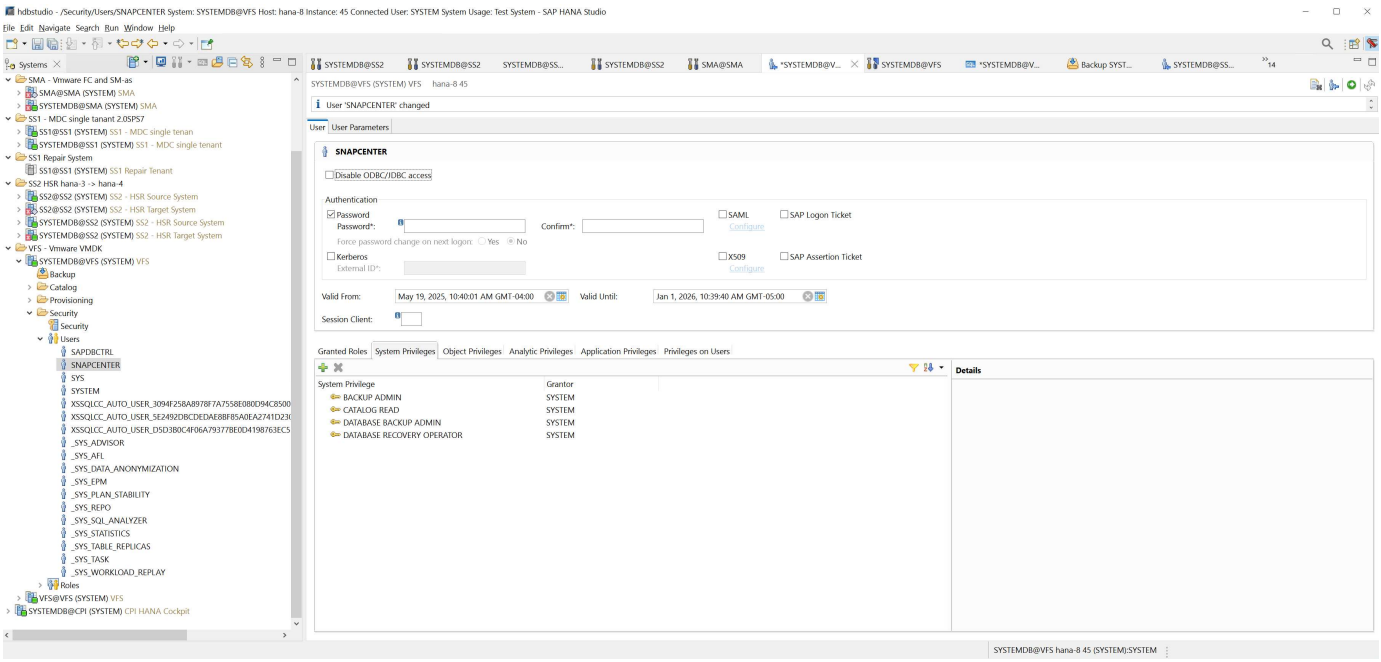
Ora è possibile eseguire l'installazione HANA.

> Con la configurazione descritta, la directory /usr/sap/VFS sarà sul VMDK del sistema operativo. Se /usr/sap/VFS deve essere memorizzato nel VMDK condiviso, il disco condiviso hana potrebbe essere partizionato per fornire un altro file system per /usr/sap/VFS.

Configurazione HANA

Configurare l'utente del database SnapCenter

È necessario creare un archivio utenti per un utente del database di sistema, che dovrebbe essere utilizzato da SnapCenter.



Configurare la chiave dell'archivio utenti hdb

È necessario creare una chiave di archivio utente per l'utente vfsadm. Il numero di istanza HANA deve essere impostato di conseguenza per la comunicazione sulla porta. Nell'istanza di installazione viene utilizzato il numero "45".

```
vfsadm@hana-8:/usr/sap/VFS/HDB45> hdbuserstore SET VFSKEY hana-8:34513
SNAPCENTER <password>

Retroactive report: Operation succeed.
```

Verificare l'accesso con:

```
vfsadm@hana-8:/usr/sap/VFS/HDB45> hdbsql -U VFSKEY

Welcome to the SAP HANA Database interactive terminal.
Type: \h for help with commands
\q to quit
hdbsql SYSTEMDB=> exit

vfsadm@hana-8:/usr/sap/VFS/HDB45>
```

Configurazione di SnapCenter

Prerequisiti

La risorsa SnapCenter HANA deve essere scoperta automaticamente

Le risorse configurate con VMware VMFS devono essere rilevate automaticamente da SnapCenter per abilitare le operazioni specifiche richieste per queste configurazioni.

Poiché i volumi non dati HANA sono sempre risorse configurate manualmente in SnapCenter, non sono supportati da SnapCenter con VMFS.

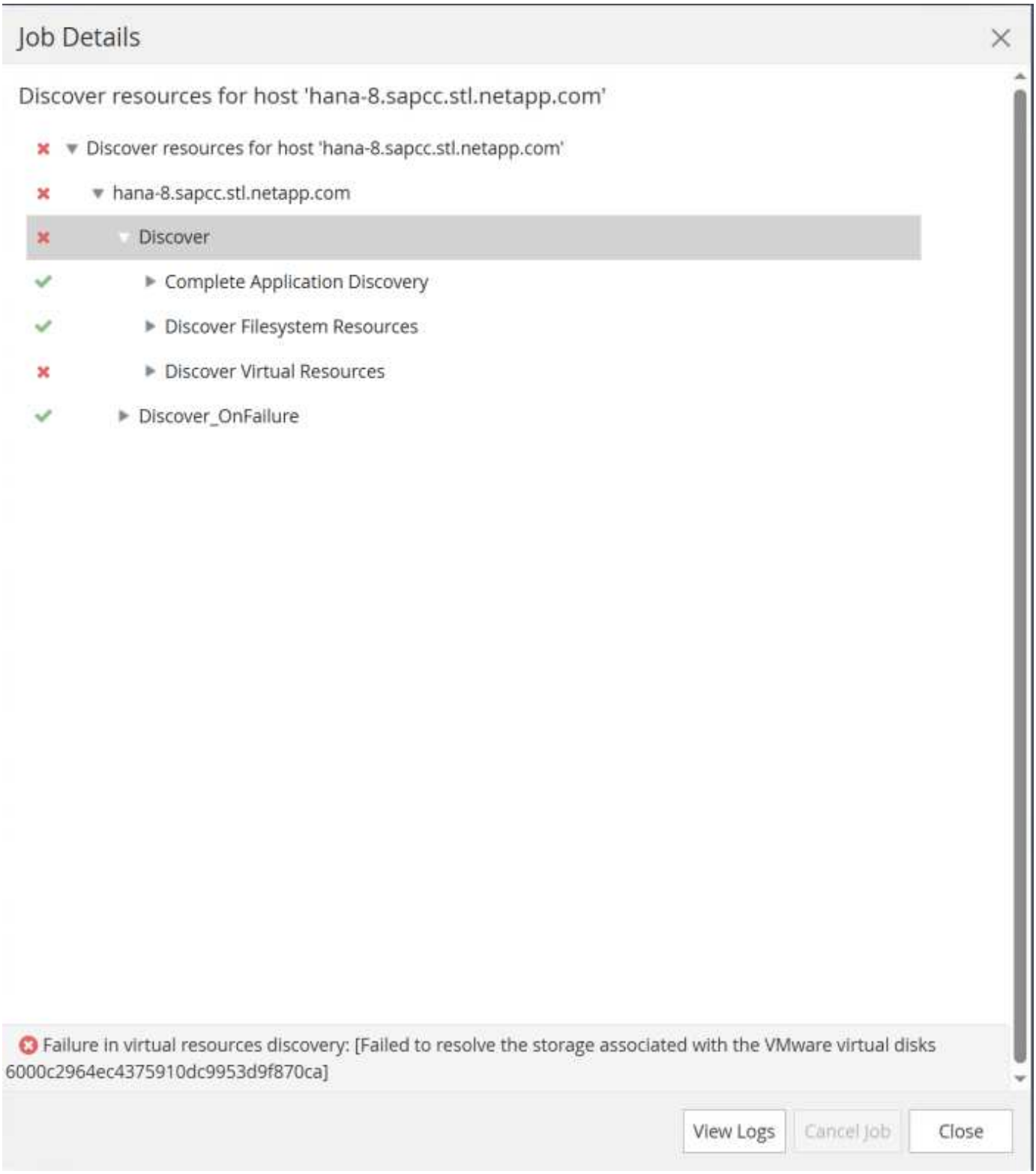
I sistemi host multipli SAP HANA devono essere configurati utilizzando un plugin HANA centrale e, pertanto, vengono configurati manualmente per impostazione predefinita. Tali sistemi non sono supportati da SnapCenter quando si utilizza VMware VMFS.

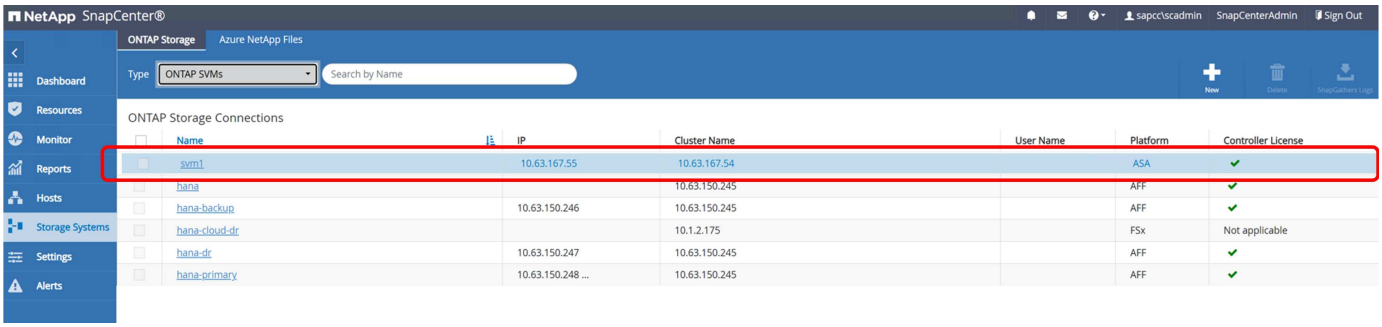
Plug-in SnapCenter per VMware vSphere

Il plug-in di SnapCenter per VMware vSphere deve essere implementato nell'ambiente VMware.

IP di gestione SVM di archiviazione

Le SVM di archiviazione che ospitano le LUN devono avere un'interfaccia di gestione configurata, altrimenti le SVM non verranno elencate in SnapCenter quando si aggiunge l'archiviazione con l'opzione "Aggiungi cluster" e l'operazione di rilevamento automatico fallirà.


Job Details
Discover resources for host 'hana-8.sapcc.stl.netapp.com'
Discover resources for host 'hana-8.sapcc.stl.netapp.com'
hana-8.sapcc.stl.netapp.com
Discover
Complete Application Discovery
Discover Filesystem Resources
Discover Virtual Resources
Discover_OnFailure
Failure in virtual resources discovery: [Failed to resolve the storage associated with the VMware virtual disks 6000c2964ec4375910dc9953d9f870ca]
View Logs
Cancel Job
Close



Parametro del disco VM

Il parametro deve essere impostato come descritto nel capitolo ""Parametro VM disk.EnableUUID"" , altrimenti il rilevamento automatico del database SnapCenter fallirà.



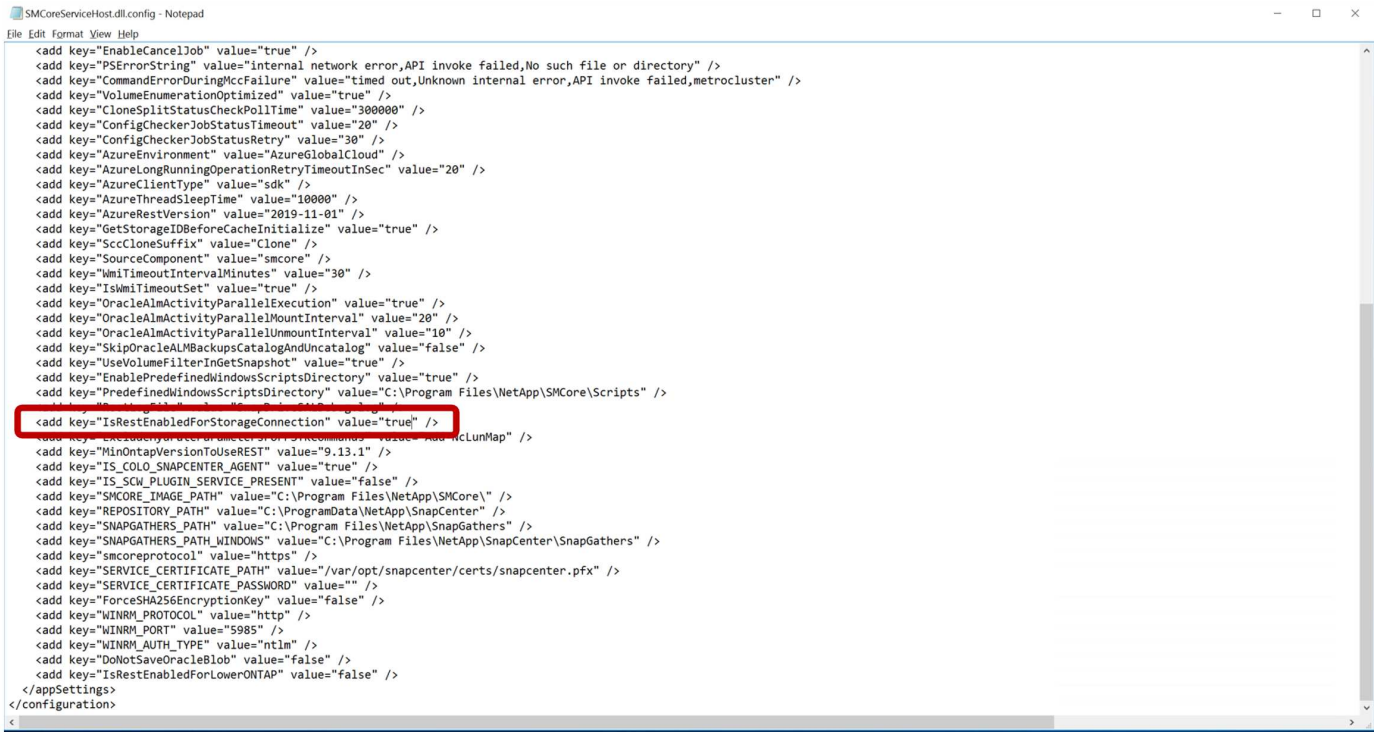
Configurare SnapCenter per utilizzare le API REST per la comunicazione di archiviazione

SnapCenter deve essere configurato per utilizzare le API REST per le comunicazioni di storage. In caso contrario, l'operazione di creazione dello Snapshot fallirà e verrà visualizzato il messaggio di errore riportato di seguito.

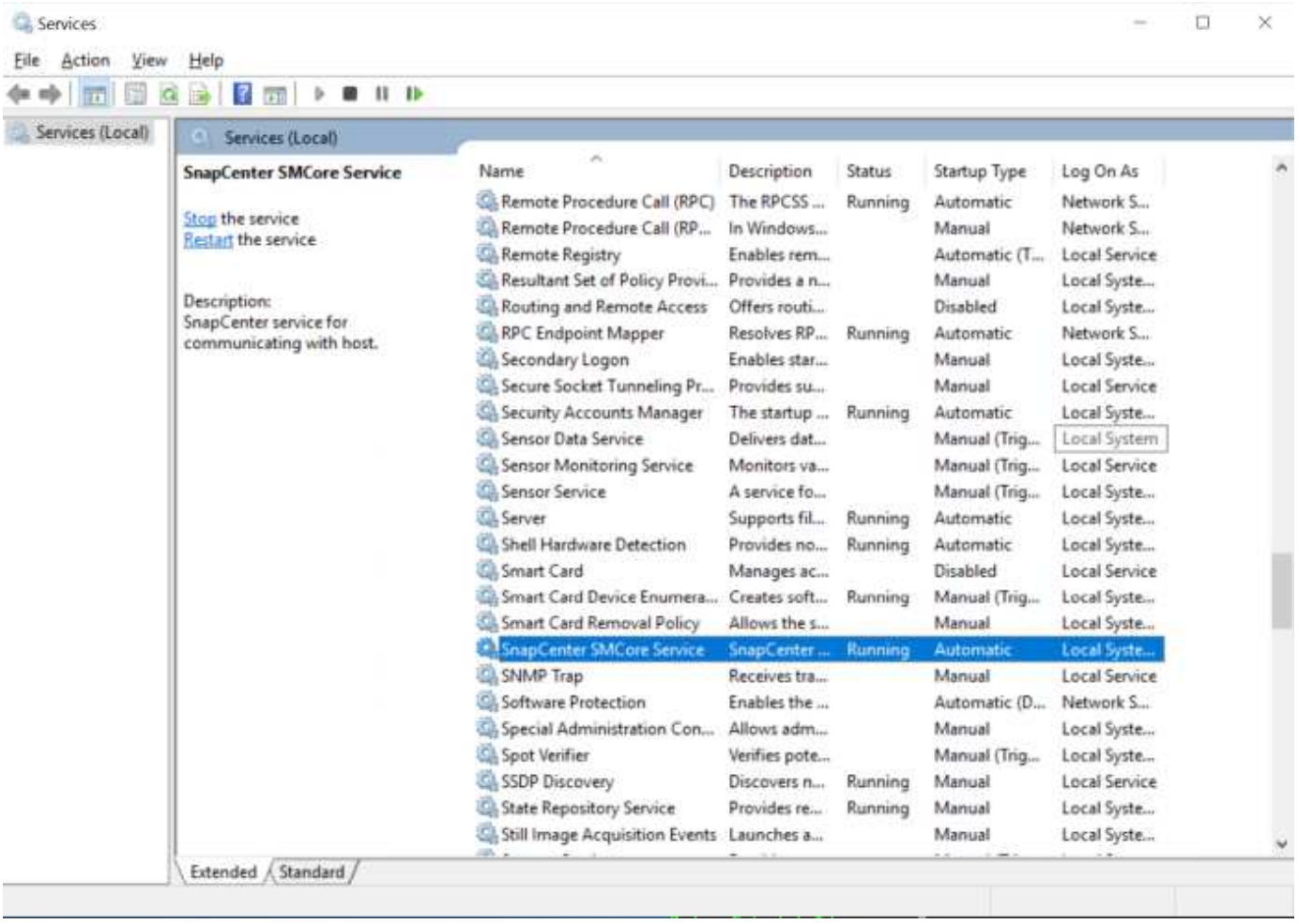


Il parametro "IsRestEnabledForStorageConnection" nel file di configurazione + C:\Program Files\NetApp\SMCore\SMCoreServiceHost.dll.config deve essere impostato su "true".

<aggiungi chiave="IsRestEnabledForStorageConnection" valore="vero" />



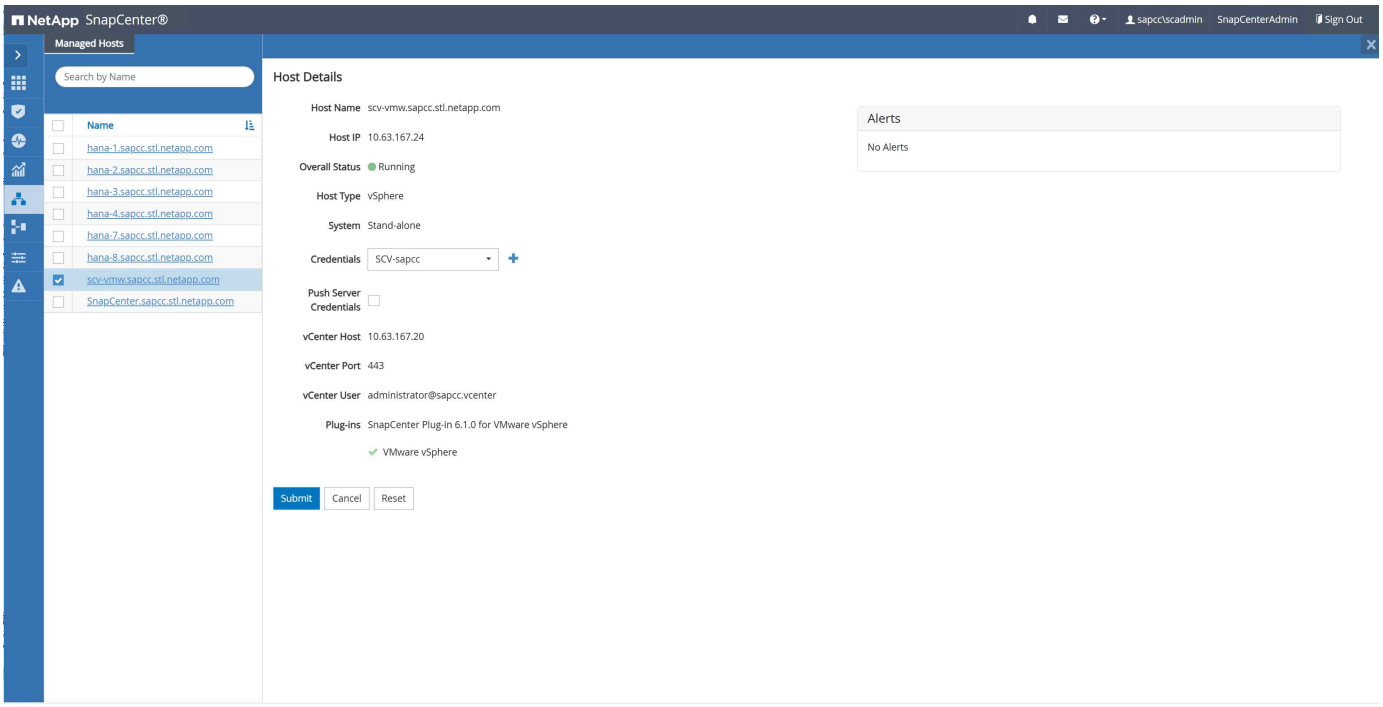
Dopo aver apportato la modifica, è necessario arrestare e riavviare il servizio SnapCenter SMCore.



Aggiungi il plugin VMware a SnapCenter

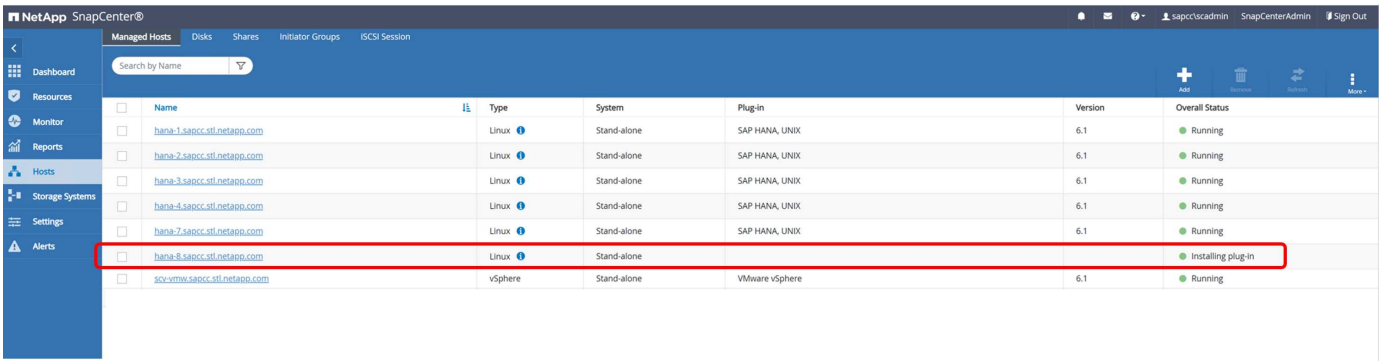
Prima di poter aggiungere l'host in SnapCenter, è necessario distribuire il plug-in SnapCenter per VMware vSphere all'interno dell'ambiente VMware. Vedere anche "Implementare il plug-in SnapCenter per VMware vSphere".

È necessario impostare le credenziali durante il flusso di lavoro di aggiunta dell'host, in cui vSphere può essere selezionato come tipo di host.

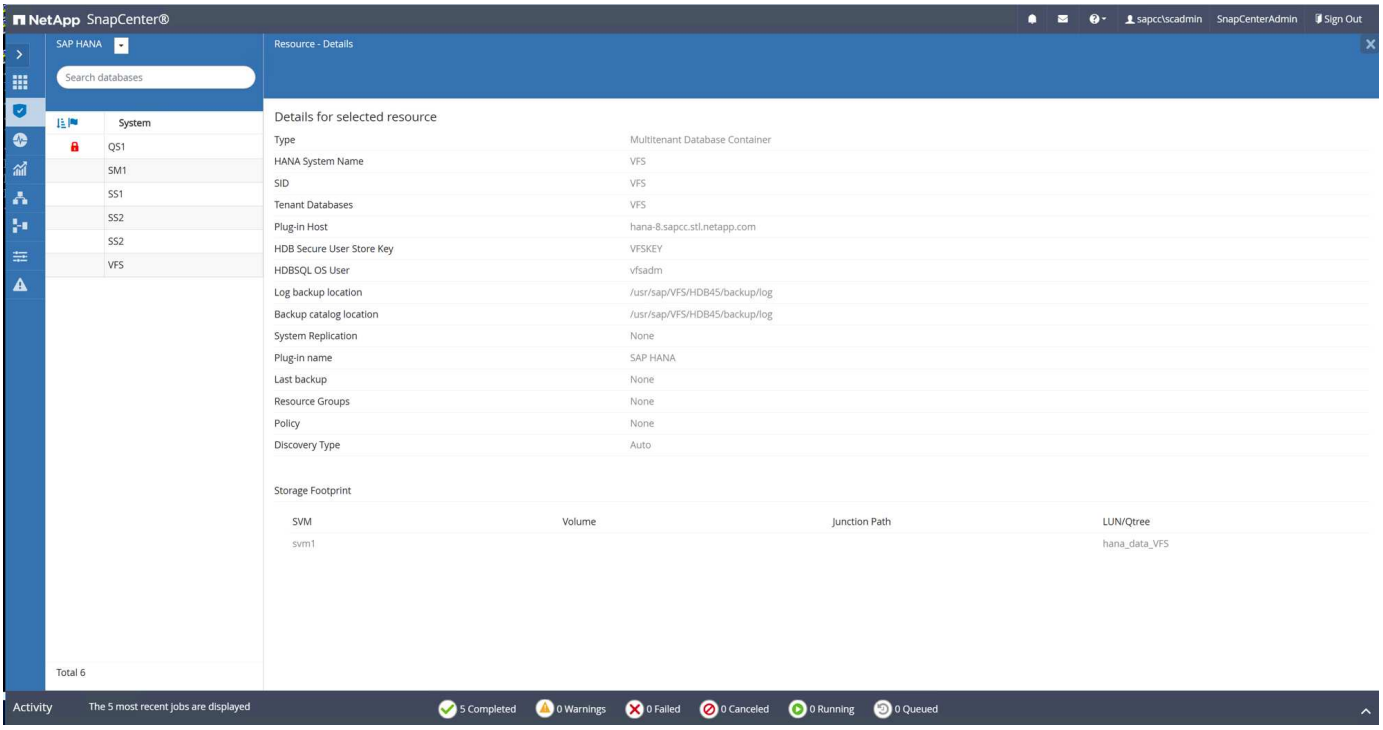


Aggiungi host HANA

Nessun requisito specifico. La distribuzione del plugin e il rilevamento automatico vengono eseguiti come di consueto.



Grazie al processo di rilevamento automatico, SnapCenter rileva che la risorsa HANA è in esecuzione virtualizzata con VMFS.

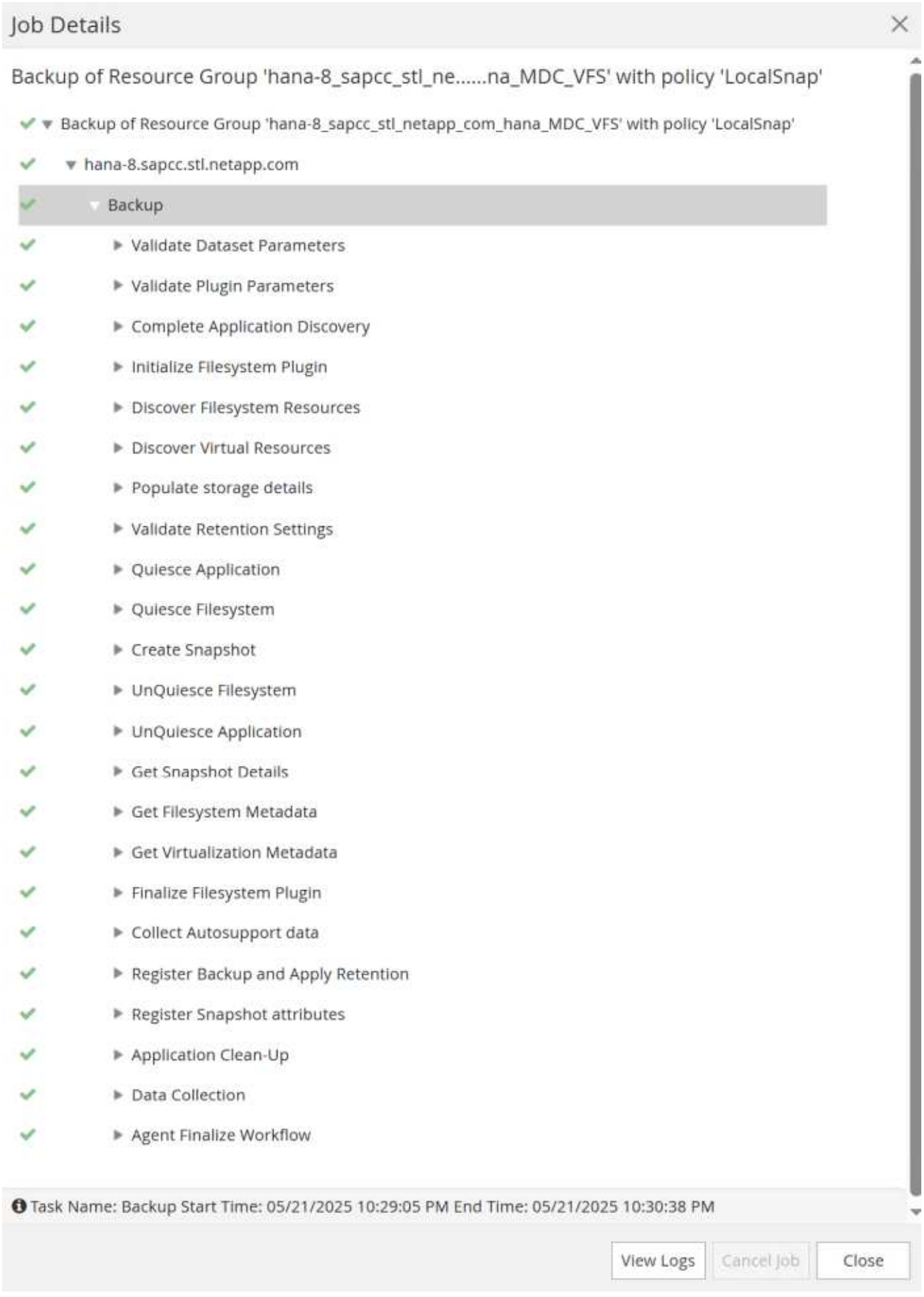


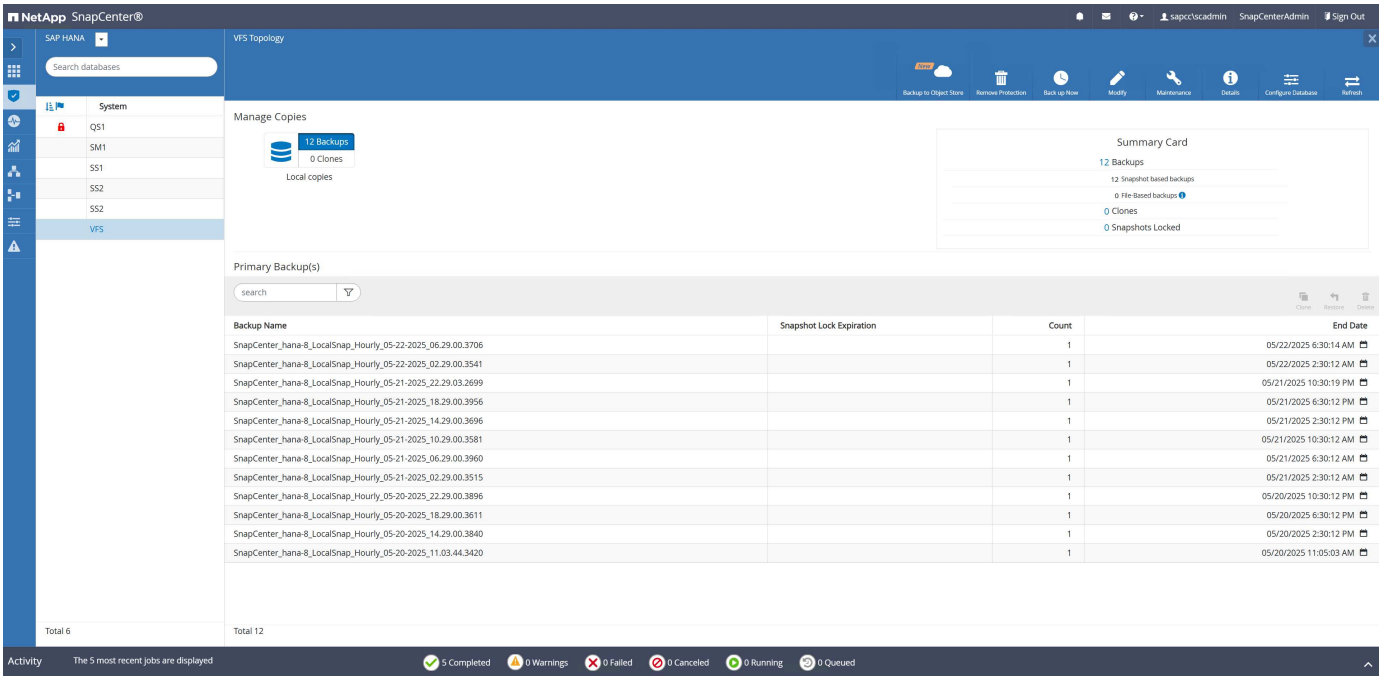
Configurazione della protezione delle risorse e delle policy

Niente di specifico per VMware con VMFS.

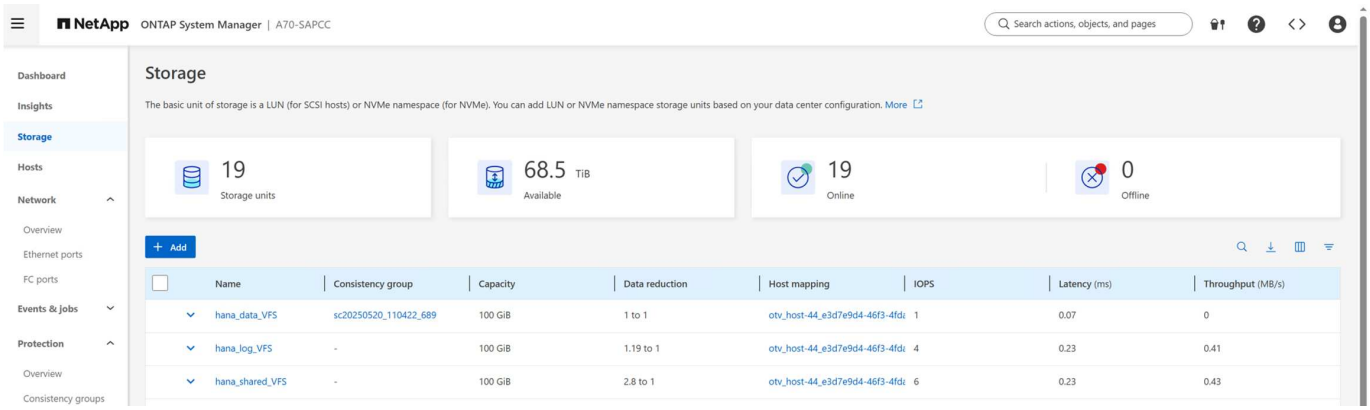
Operazioni di backup

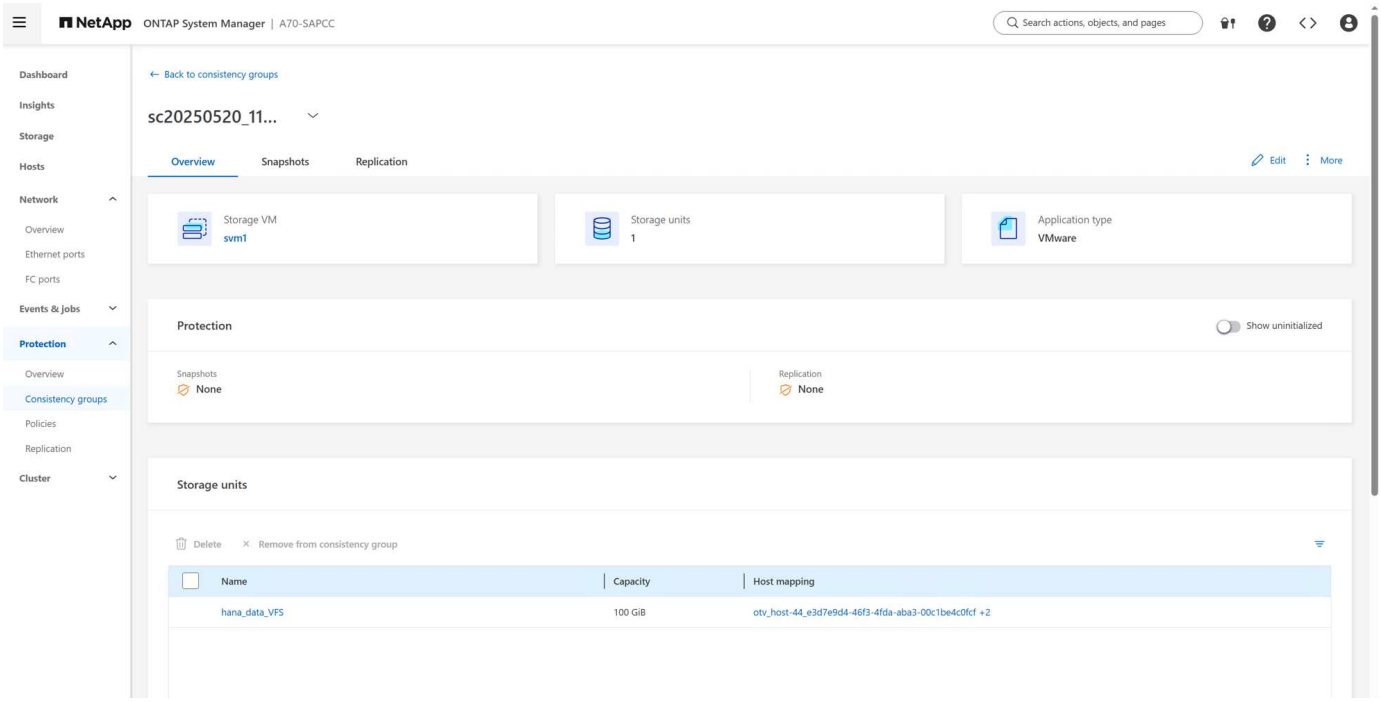
Niente di specifico per VMware con VMFS.

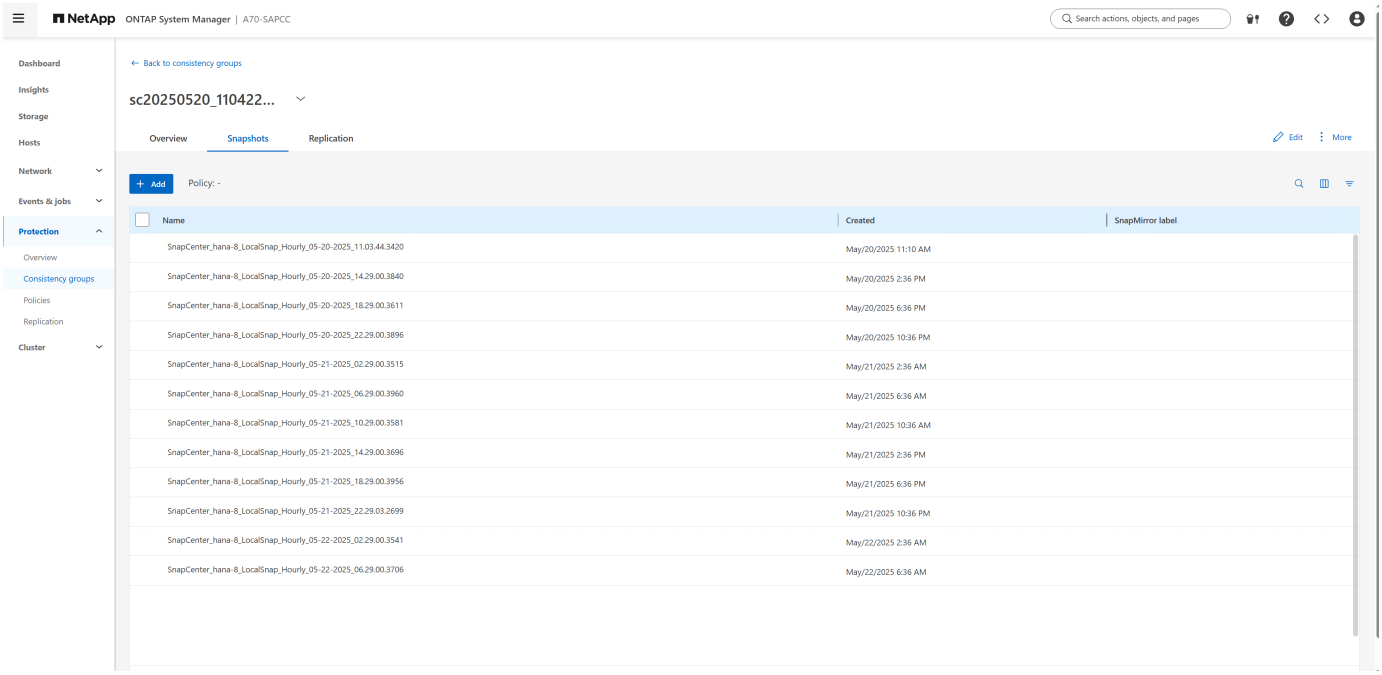

Job Details
Backup of Resource Group 'hana-8_sapcc_stl_ne.....na_MDC_VFS' with policy 'LocalSnap'
Backup of Resource Group 'hana-8_sapcc_stl_netapp_com_hana_MDC_VFS' with policy 'LocalSnap'
hana-8.sapcc.stl.netapp.com
Backup
Validate Dataset Parameters
Validate Plugin Parameters
Complete Application Discovery
Initialize Filesystem Plugin
Discover Filesystem Resources
Discover Virtual Resources
Populate storage details
Validate Retention Settings
Quiesce Application
Quiesce Filesystem
Create Snapshot
UnQuiesce Filesystem
UnQuiesce Application
Get Snapshot Details
Get Filesystem Metadata
Get Virtualization Metadata
Finalize Filesystem Plugin
Collect Autosupport data
Register Backup and Apply Retention
Register Snapshot attributes
Application Clean-Up
Data Collection
Agent Finalize Workflow
Task Name: Backup Start Time: 05/21/2025 10:29:05 PM End Time: 05/21/2025 10:30:38 PM
View Logs
Cancel Job
Close



SnapCenter crea un gruppo di coerenza (CG) e aggiunge l'unità di storage hana_data_VFS al CG. Gli snapshot vengono creati a livello di CG.







Operazioni di ripristino e recovery

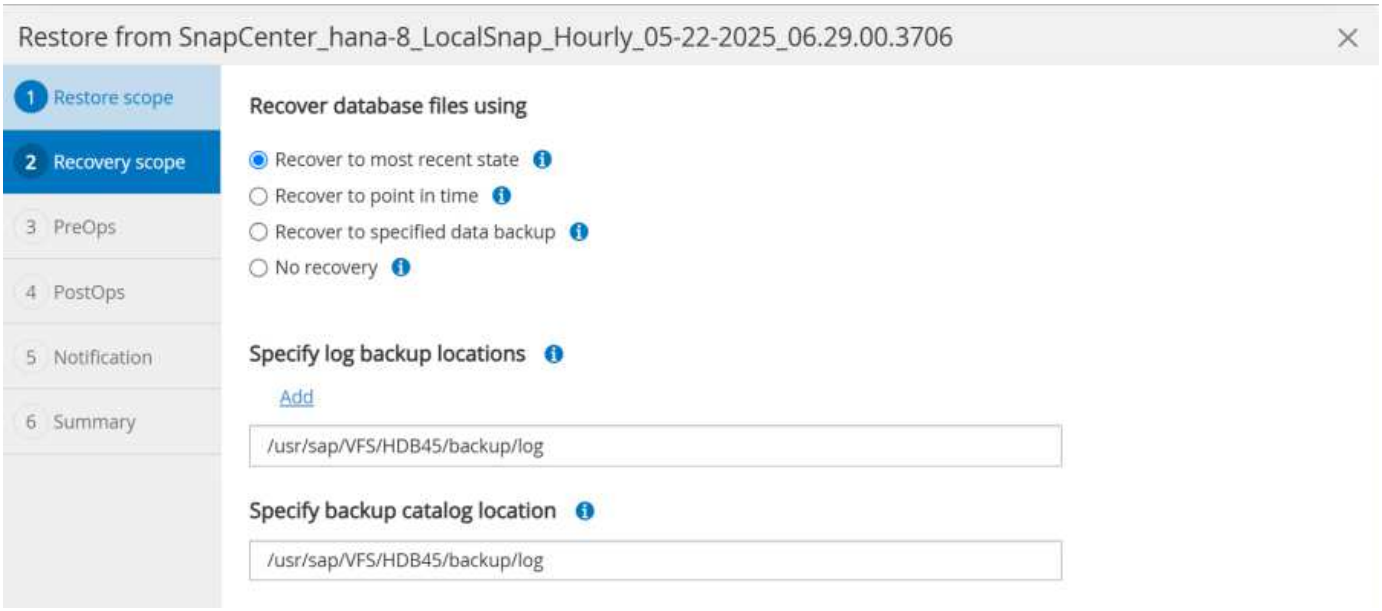
Con le risorse virtuali archiviate su SnapCenter di VMFS/VMDK, le operazioni di ripristino vengono sempre eseguite tramite un'operazione di clonazione, montaggio e copia.

1. SnapCenter crea un clone di archiviazione basato sullo Snapshot selezionato
2. SnapCenter monta la LUN come nuovo datastore sull'host ESX
3. SnapCenter aggiunge il VMDK al datastore come nuovo disco alla VM di HANA
4. SnapCenter monta il nuovo disco sul sistema operativo Linux
5. SnapCenter copia i dati dal nuovo disco nella posizione originale

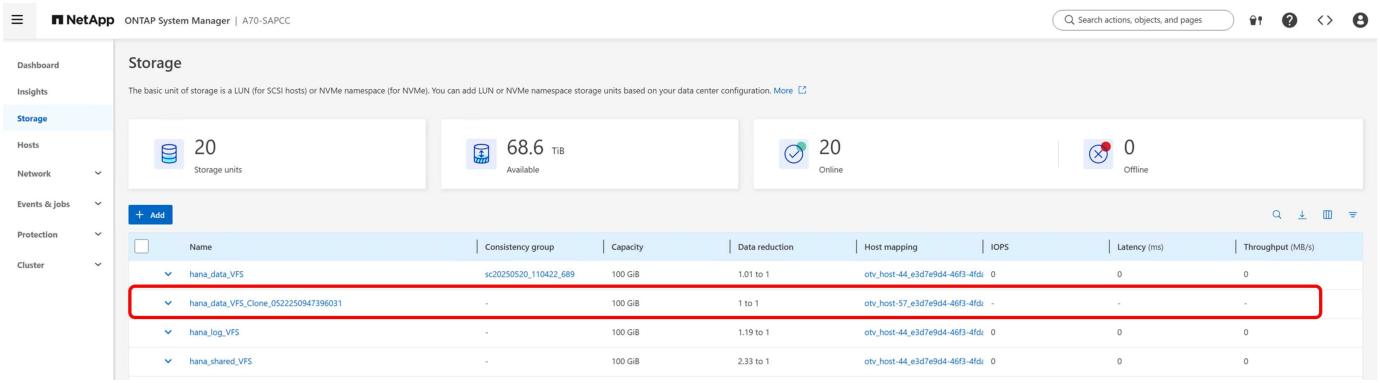
6. Al termine dell'operazione di copia, tutte le risorse precedenti vengono rimosse di nuovo
7. SnapCenter esegue il ripristino del database di sistema HANA
8. SnapCenter esegue il ripristino del database tenant HANA

Il tempo di esecuzione complessivo dell'operazione di ripristino dipende dalle dimensioni del database e dalla velocità effettiva della connessione FC tra i cluster di storage e gli host ESX. Nella nostra configurazione di laboratorio con un'installazione iniziale di HANA, il tempo di esecuzione è stato di circa 12 minuti.

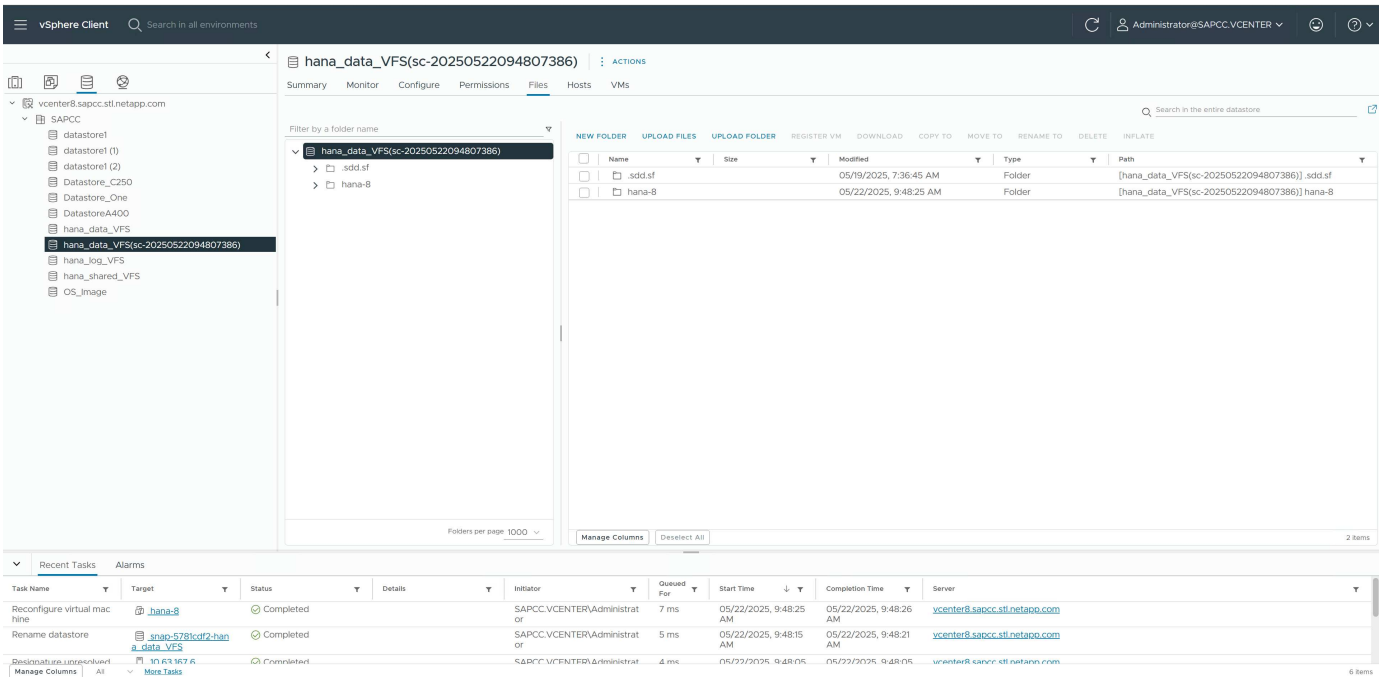




Mentre è in esecuzione l'operazione di ripristino e recupero, è possibile visualizzare una nuova unità di archiviazione clonata.



Il nuovo LUN (datastore) basato sull'unità di archiviazione clonata viene collegato al cluster ESX.

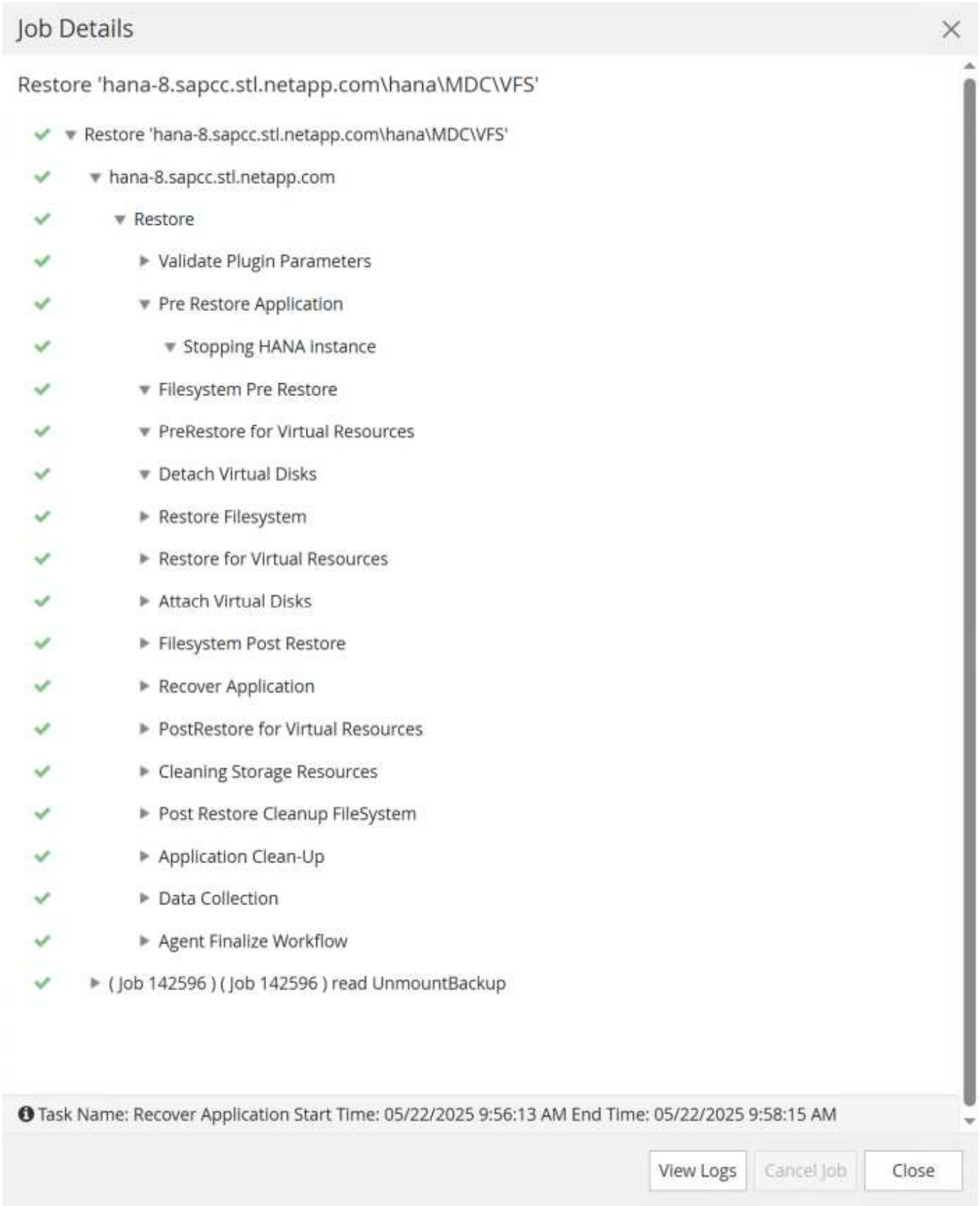


Il VMDK all'interno del datastore viene mappato sulla VM HANA di destinazione e montato sul sistema HANA.

```
hana-8:~ # df -h

Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 5.3G 54G 9% /
devtmpfs 4.0M 8.0K 4.0M 1% /dev
tmpfs 49G 0 49G 0% /dev/shm
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 26M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysusers.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
/dev/mapper/system-root 60G 5.3G 54G 9% /.snapshots
/dev/mapper/system-root 60G 5.3G 54G 9% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 5.3G 54G 9% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 5.3G 54G 9% /home
/dev/mapper/system-root 60G 5.3G 54G 9% /opt
/dev/mapper/system-root 60G 5.3G 54G 9% /root
/dev/mapper/system-root 60G 5.3G 54G 9% /srv
/dev/mapper/system-root 60G 5.3G 54G 9% /usr/local
/dev/mapper/system-root 60G 5.3G 54G 9% /tmp
/dev/mapper/system-root 60G 5.3G 54G 9% /var
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/sdc 95G 8.9G 87G 10% /hana/log/VFS/mnt00001
/dev/sdb 95G 7.6G 88G 8% /hana/data/VFS/mnt00001
/dev/sdd 95G 15G 81G 16% /hana/shared
/dev/sda1 253M 5.9M 247M 3% /boot/efi
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
192.168.175.86:/sapcc_share 1.4T 858G 568G 61% /mnt/sapcc-share
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
/dev/sde 95G 9.2G 86G 10%
/var/opt/snapcenter/scu/clones/hana_data_VFS_mnt00001_142592_scu_clone_1

hana-8:~ #
```



Aggiornamento del sistema SAP

Informazioni dettagliate sulle operazioni di aggiornamento del sistema SAP tramite SnapCenter sono disponibili all'indirizzo "TR-4667: Automazione delle operazioni di copia e clonazione del sistema SAP HANA

con SnapCenter" .

Il secondo sistema HANA QFS è stato fornito nello stesso modo descritto nel capitolo ""“Provisioning e installazione del sistema HANA”"" .

Prerequisiti

La versione corrente di SnapCenter (6.1P1) presenta alcune limitazioni che si prevede verranno risolte nelle prossime versioni.

1. È necessario riavviare il processo spl dopo ogni flusso di lavoro "clone create" e "clone delete" utilizzando il comando "systemctl restart spl" sull’host HANA di destinazione.
2. Le VM HANA utilizzate come origine e destinazione dell’operazione di aggiornamento del sistema SAP devono essere eseguite sullo stesso host ESX.

Riepilogo del flusso di lavoro

Prima di poter eseguire la prima operazione di aggiornamento del sistema SAP, è necessario installare il sistema HANA di destinazione e aggiungere l’host a SnapCenter. Successivamente, il sistema HANA deve essere arrestato e il disco dati HANA deve essere smontato dall’host.

Flusso di lavoro di creazione clone SnapCenter

1. Crea un clone di archiviazione
2. Configurare la mappatura host per il clone di storage
3. Collega il clone di storage (datastore) all’host ESX
4. Aggiungere un nuovo disco dal datastore alla VM HANA di destinazione
5. Montare il disco sul sistema operativo HANA VM
6. Ripristina il sistema HANA utilizzando post-script

Durata: 12 minuti

> Rispetto all’operazione di ripristino, il tempo di esecuzione dell’operazione di clonazione è indipendente dalle dimensioni del database HANA. Il tempo di esecuzione dei passaggi da 1 a 5 sarà simile anche per database di grandi dimensioni. Il ripristino richiederà ovviamente più tempo per i sistemi HANA più grandi.

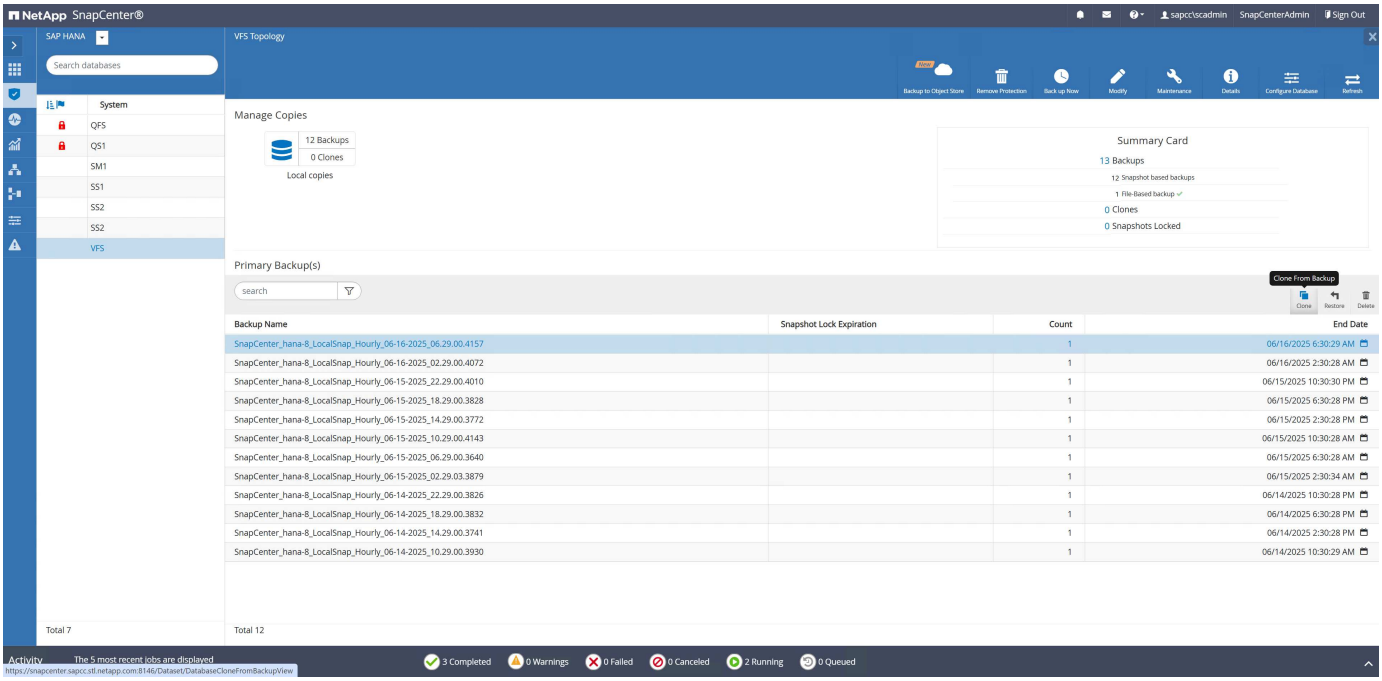
Flusso di lavoro di eliminazione della clonazione SnapCenter

1. Arresto del sistema HANA utilizzando lo script preimpostato
2. Smonta il disco dal sistema operativo HANA VM
3. Rimuovere il disco dalla VM HANA
4. Rimuovere il datastore dall’host ESX
5. Elimina il clone di archiviazione

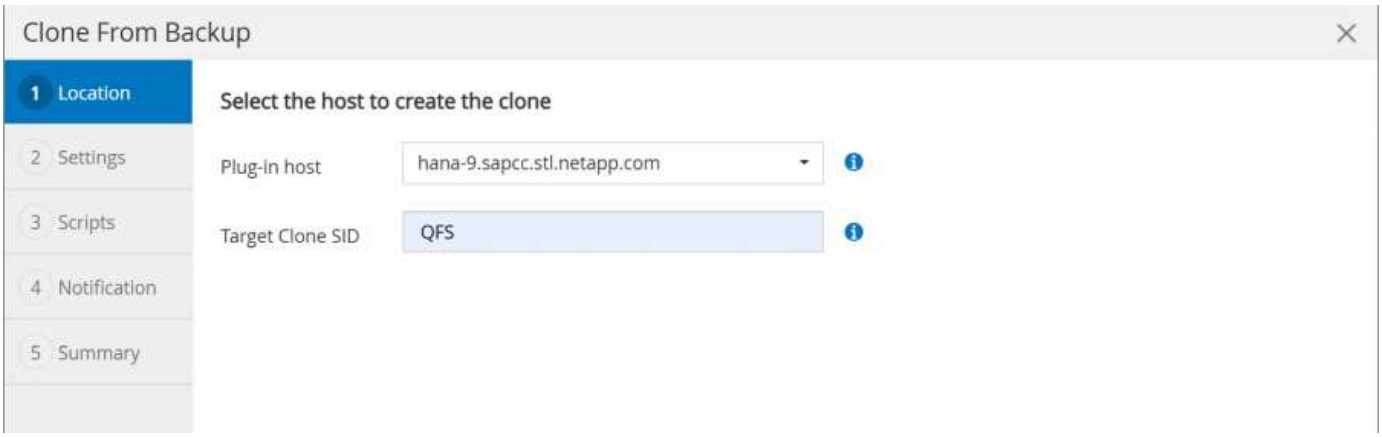
Durata: 11 minuti

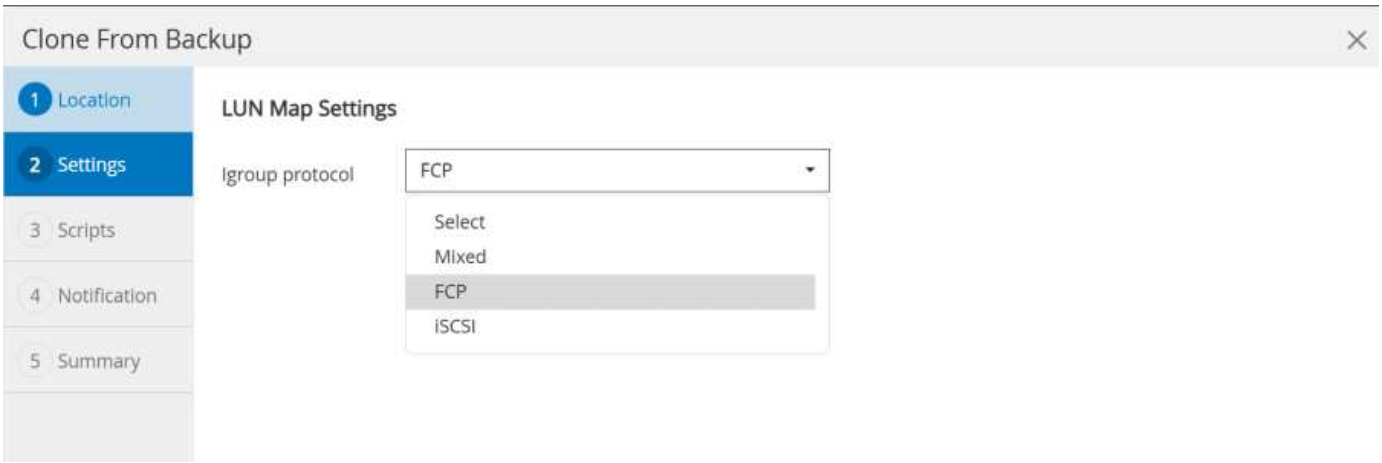
Flusso di lavoro di creazione clone SnapCenter

Il flusso di lavoro per la creazione del clone viene avviato selezionando lo Snapshot desiderato e facendo clic sul pulsante Clona.

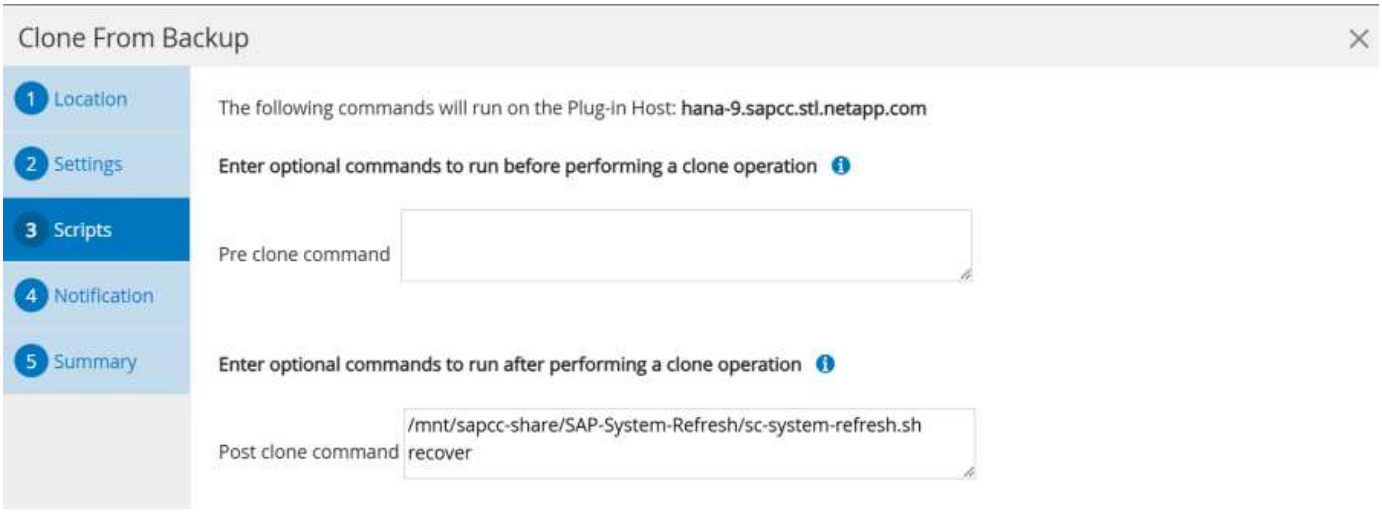


È necessario fornire l'host di destinazione e il SID.

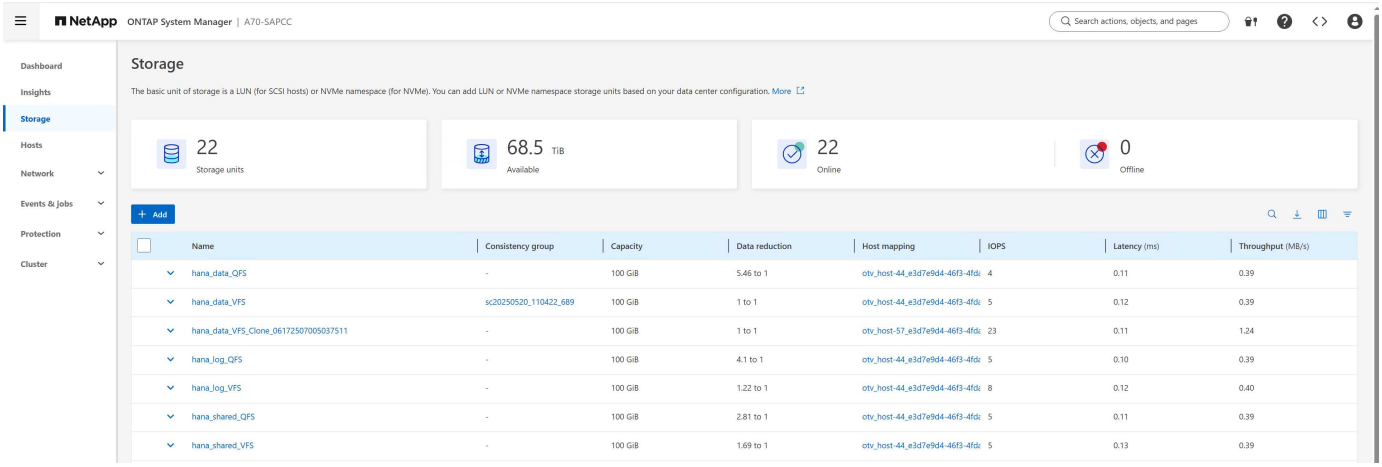




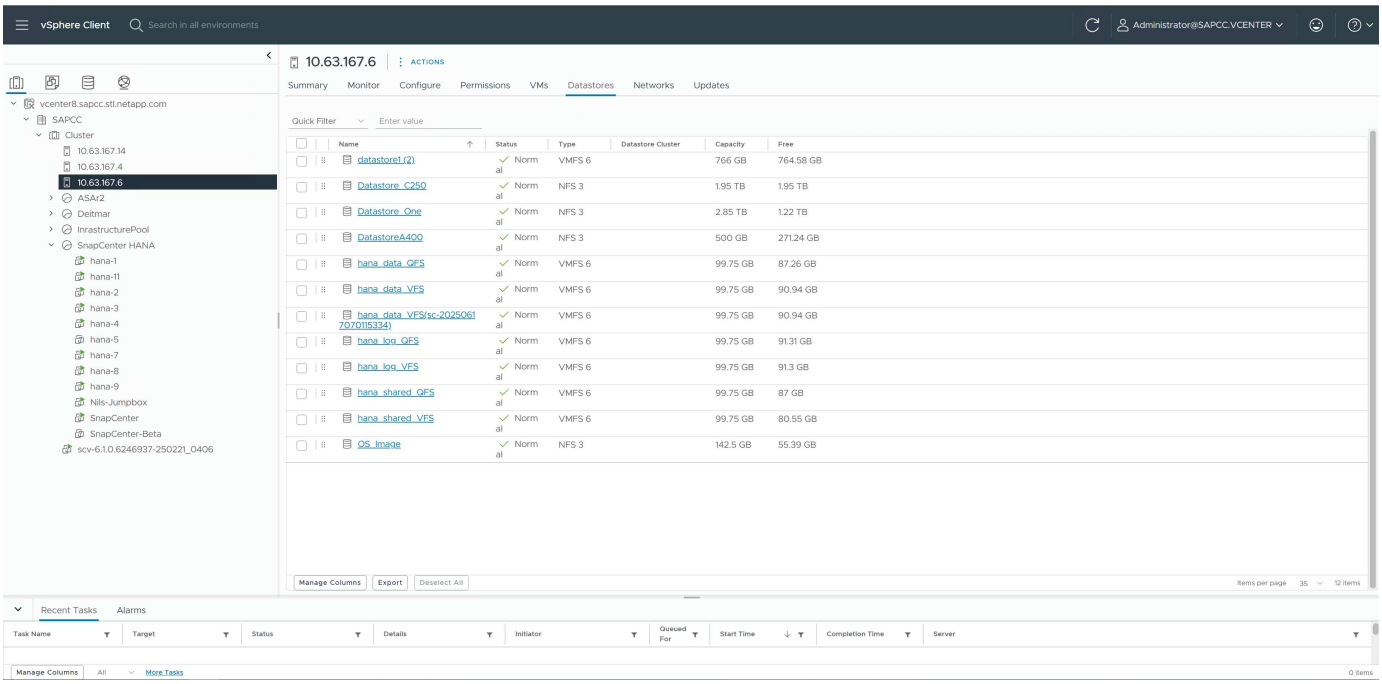
Nel nostro esempio utilizziamo un post-script per eseguire il ripristino sull'host di destinazione.



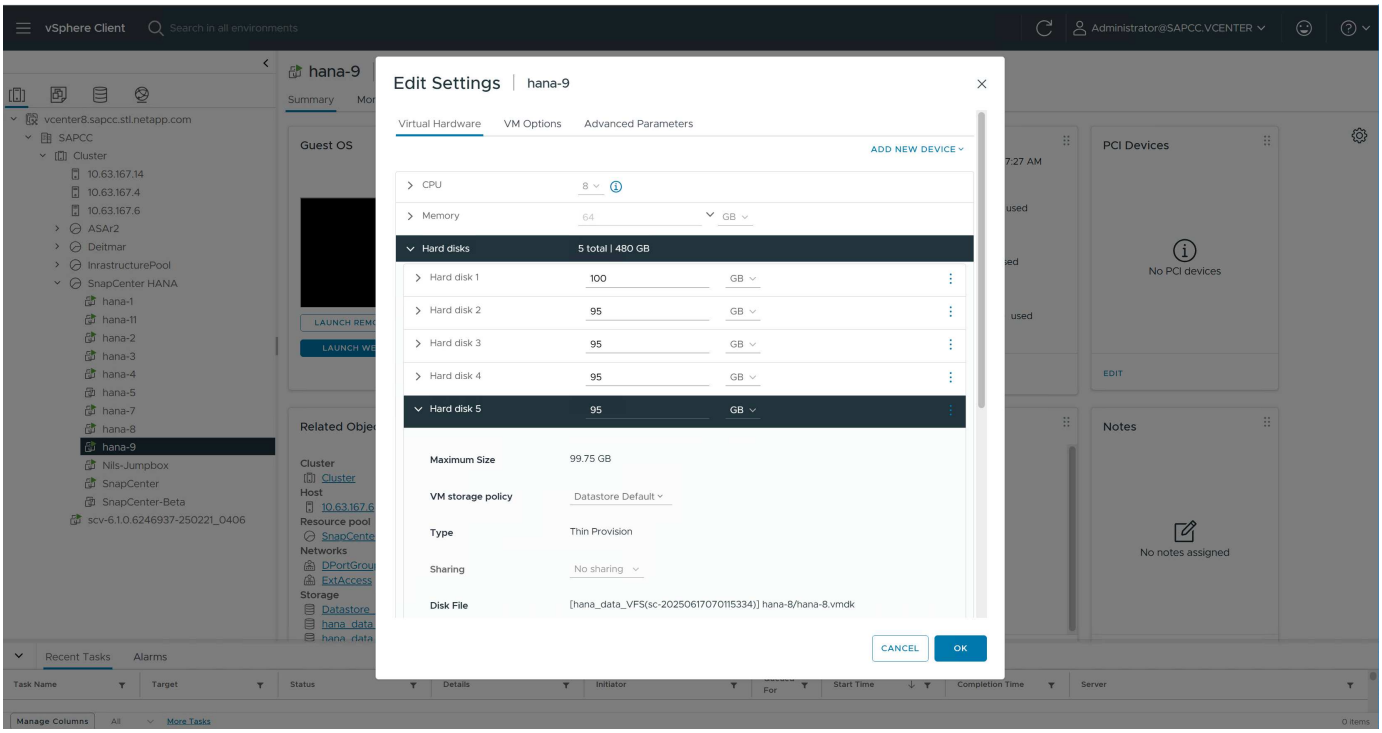
Quando il flusso di lavoro viene avviato, SnapCenter crea un'unità di archiviazione clonata in base allo Snapshot selezionato.



SnapCenter collega quindi la LUN (datastore) all'host ESX su cui è in esecuzione la VM HANA di destinazione.



Il VMDK all'interno del nuovo datastore viene quindi aggiunto alla VM HANA.



SnapCenter quindi configura e monta il nuovo disco sul sistema HANA Linux.

```
hana-9:/mnt/sapcc-share/SAP-System-Refresh # df -h

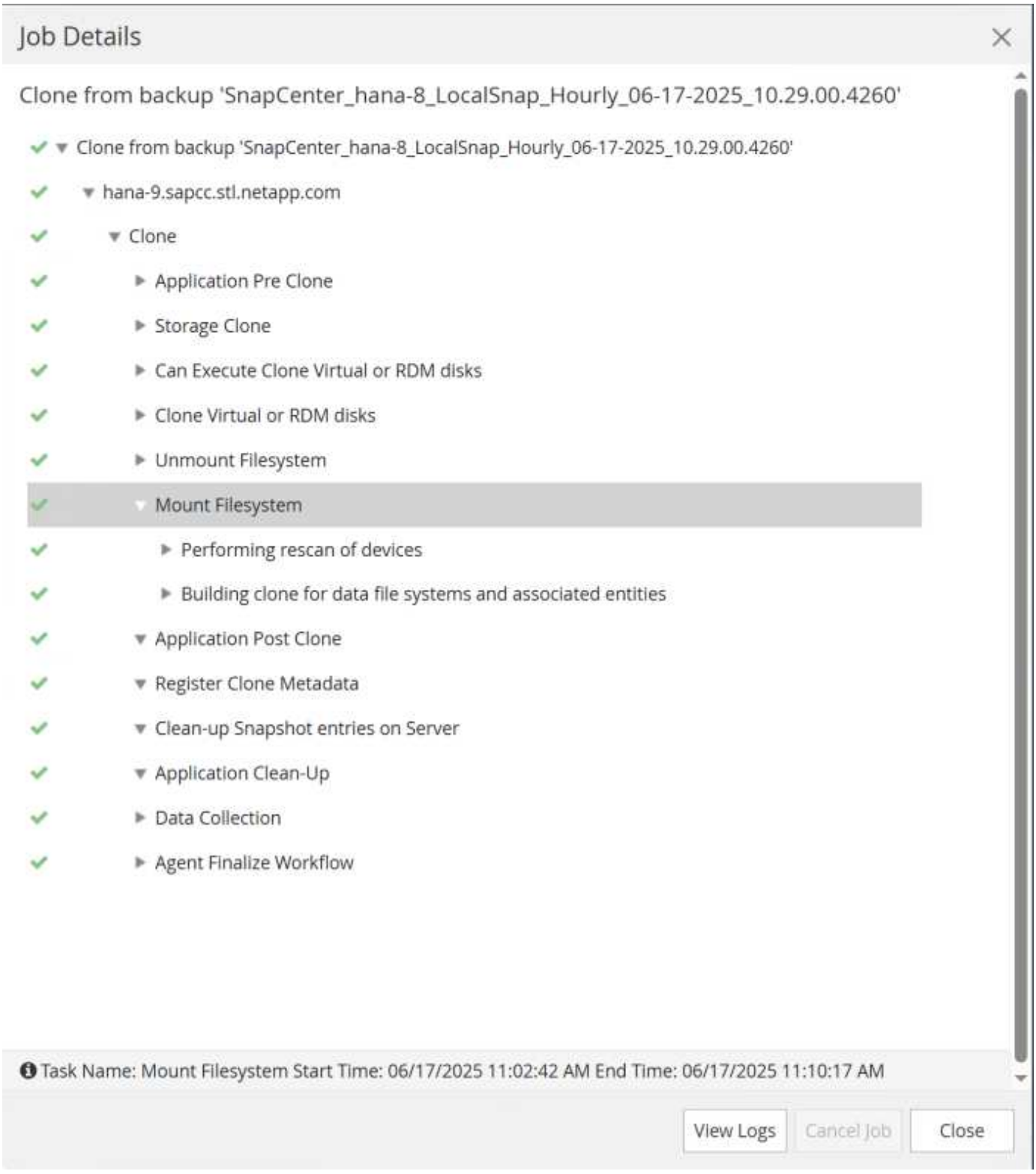
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/system-root 60G 5.2G 52G 10% /
devtmpfs 4.0M 4.0K 4.0M 1% /dev
tmpfs 49G 0 49G 0% /dev/shm
```

```
efivarfs 256K 57K 195K 23% /sys/firmware/efi/efivars
tmpfs 13G 26M 13G 1% /run
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev-
early.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysctl.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-sysusers.service
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup-dev.service
/dev/mapper/system-root 60G 5.2G 52G 10% /.snapshots
/dev/mapper/system-root 60G 5.2G 52G 10% /boot/grub2/i386-pc
/dev/mapper/system-root 60G 5.2G 52G 10% /boot/grub2/x86++_++64-efi
/dev/mapper/system-root 60G 5.2G 52G 10% /home
/dev/mapper/system-root 60G 5.2G 52G 10% /opt
/dev/mapper/system-root 60G 5.2G 52G 10% /srv
/dev/mapper/system-root 60G 5.2G 52G 10% /root
/dev/mapper/system-root 60G 5.2G 52G 10% /tmp
/dev/mapper/system-root 60G 5.2G 52G 10% /usr/local
/dev/mapper/system-root 60G 5.2G 52G 10% /var
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-vconsole-setup.service
/dev/sdc 95G 8.9G 87G 10% /hana/log/QFS/mnt00001
/dev/sdd 95G 14G 82G 14% /hana/shared
/dev/sda1 253M 5.9M 247M 3% /boot/efi
tmpfs 1.0M 0 1.0M 0% /run/credentials/systemd-tmpfiles-setup.service
192.168.175.86:/sapcc++_++share 1.4T 858G 568G 61% /mnt/sapcc-share
tmpfs 6.3G 72K 6.3G 1% /run/user/464
tmpfs 1.0M 0 1.0M 0% /run/credentials/getty@tty1.service
tmpfs 6.3G 52K 6.3G 1% /run/user/0
/dev/sde 95G 9.2G 86G 10% /hana/data/QFS/mnt00001
tmpfs 6.3G 56K 6.3G 1% /run/user/1001
hana-9:/mnt/sapcc-share/SAP-System-Refresh #

hana-9:/mnt/sapcc-share/SAP-System-Refresh # cat /etc/fstab
/dev/system/root / btrfs defaults 0 0
/dev/system/root /var btrfs subvol=/@/var 0 0
/dev/system/root /usr/local btrfs subvol=/@/usr/local 0 0
/dev/system/root /tmp btrfs subvol=/@/tmp 0 0
/dev/system/root /srv btrfs subvol=/@/srv 0 0
/dev/system/root /root btrfs subvol=/@/root 0 0
/dev/system/root /opt btrfs subvol=/@/opt 0 0
/dev/system/root /home btrfs subvol=/@/home 0 0
/dev/system/root /boot/grub2/x86++_++64-efi btrfs
subvol=/@/boot/grub2/x86++_++64-efi 0 0
/dev/system/root /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/i386-pc 0
0
/dev/system/swap swap swap defaults 0 0
/dev/system/root /.snapshots btrfs subvol=/@/.snapshots 0 0
UUID=FB79-24DC /boot/efi vfat utf8 0 2
```

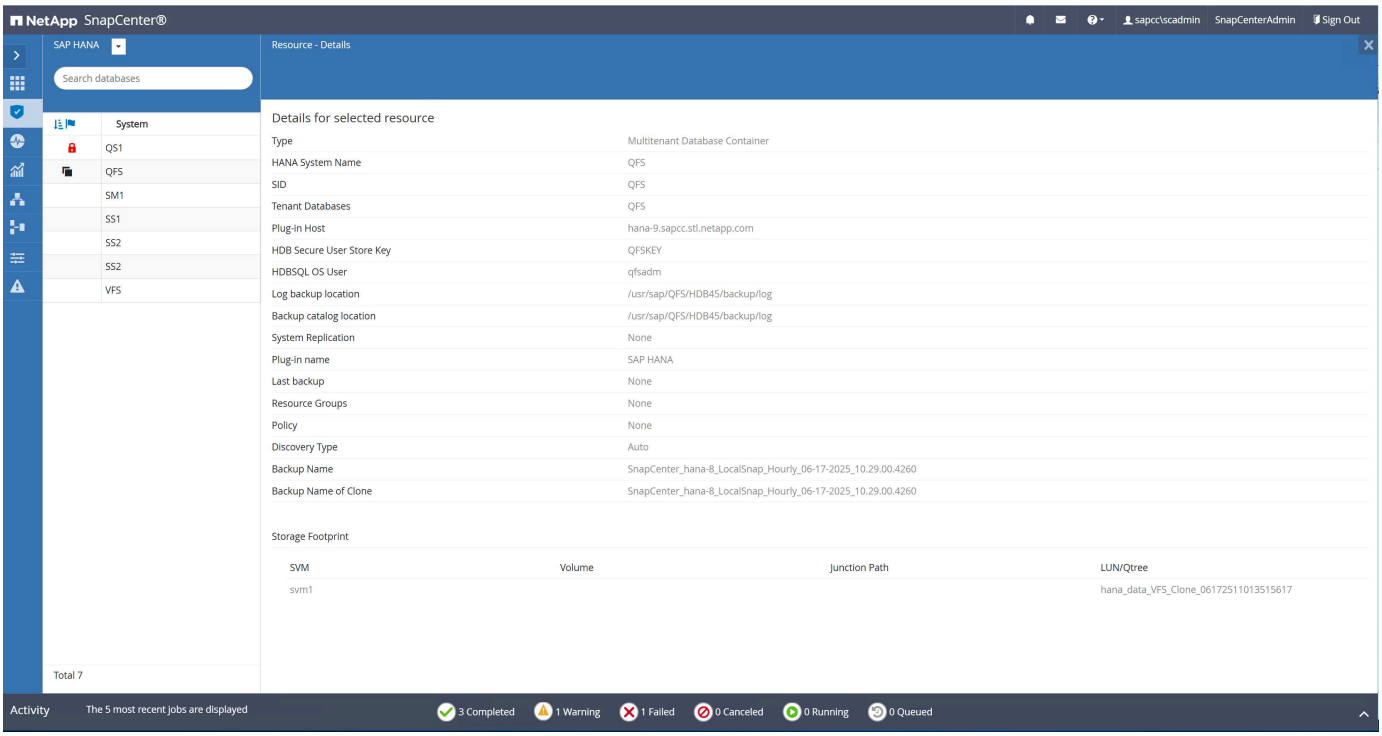
```
192.168.175.86:/sapcc++_++share /mnt/sapcc-share nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
#/dev/sdb /hana/data/QFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdc /hana/log/QFS/mnt00001 xfs relatime,inode64 0 0
/dev/sdd /hana/shared xfs defaults 0 0
# The following entry has been added by NetApp (SnapCenter Plug-in for
UNIX)
/dev/sde /hana/data/QFS/mnt00001 xfs
rw,relatime,attr2,inode64,logbufs=8,logbsize=32k,noquota 0 0
hana-9:/mnt/sapcc-share/SAP-System-Refresh #
```

La seguente schermata mostra i passaggi del processo eseguiti da SnapCenter.



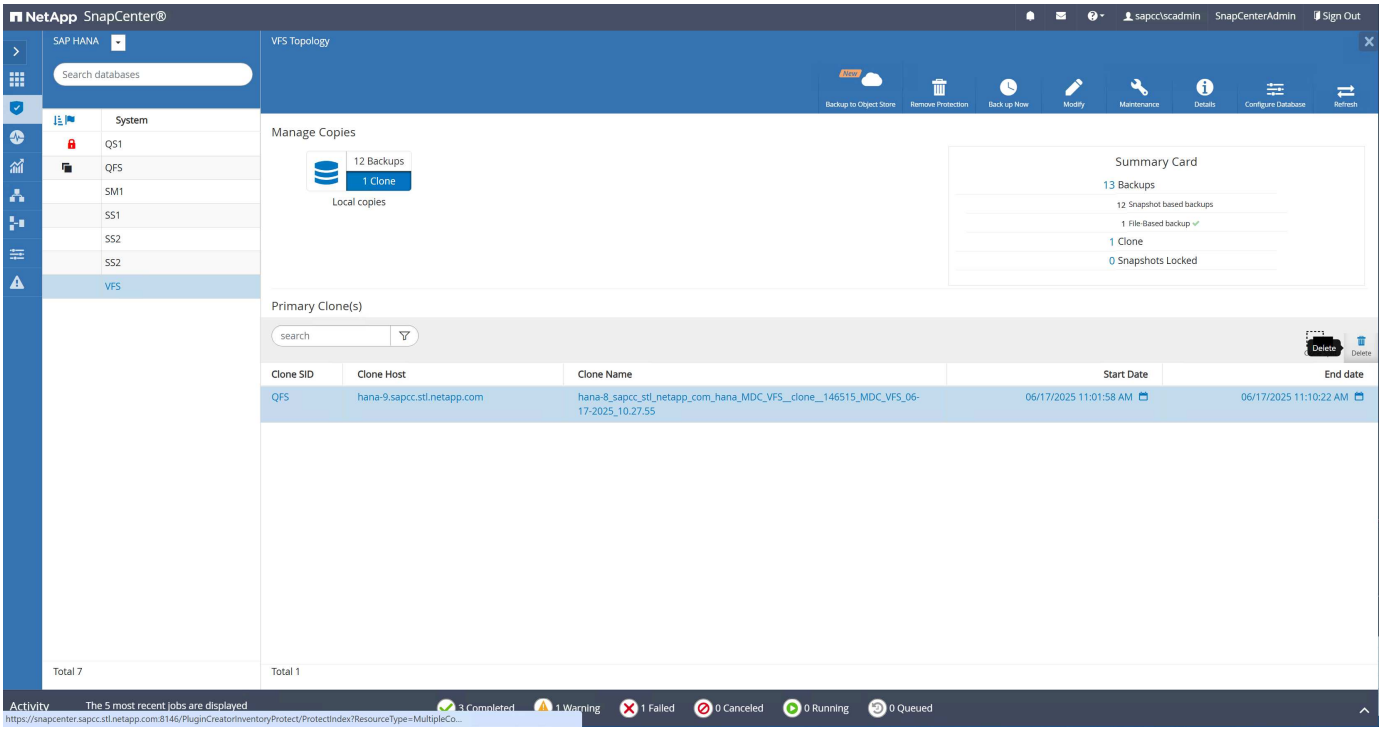
Come accennato nella sezione "Prerequisiti", il servizio SnapCenter SPL sull'host HANA deve essere riavviato utilizzando il comando "systemctl restart spl" per avviare la pulizia corretta. Questa operazione deve essere eseguita al termine del processo.

Al termine del flusso di lavoro di clonazione, è possibile avviare il rilevamento automatico facendo clic sulla risorsa QFS. Al termine del processo di rilevamento automatico, il nuovo spazio di archiviazione viene elencato nella vista dettagli della risorsa.

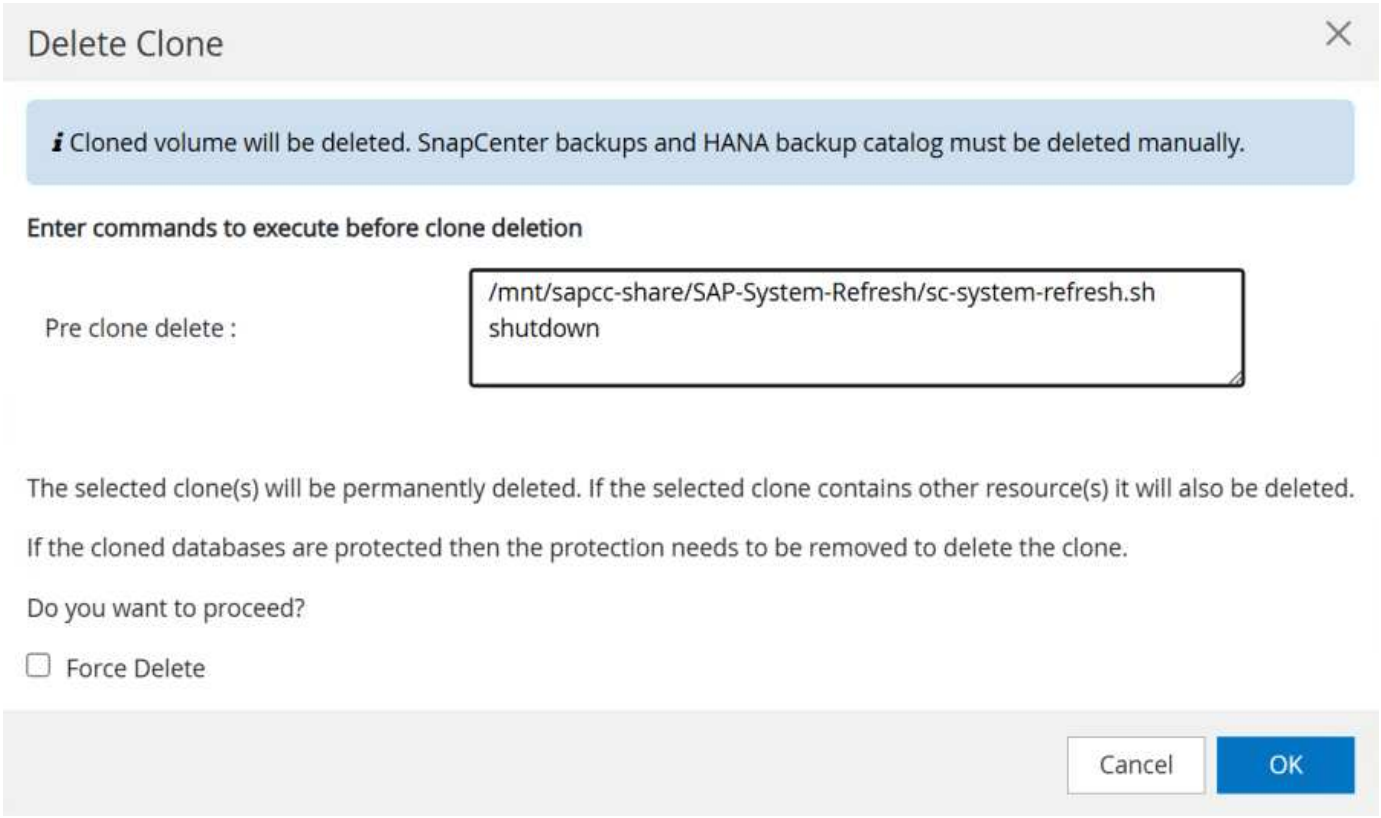


Flusso di lavoro di eliminazione della clonazione SnapCenter

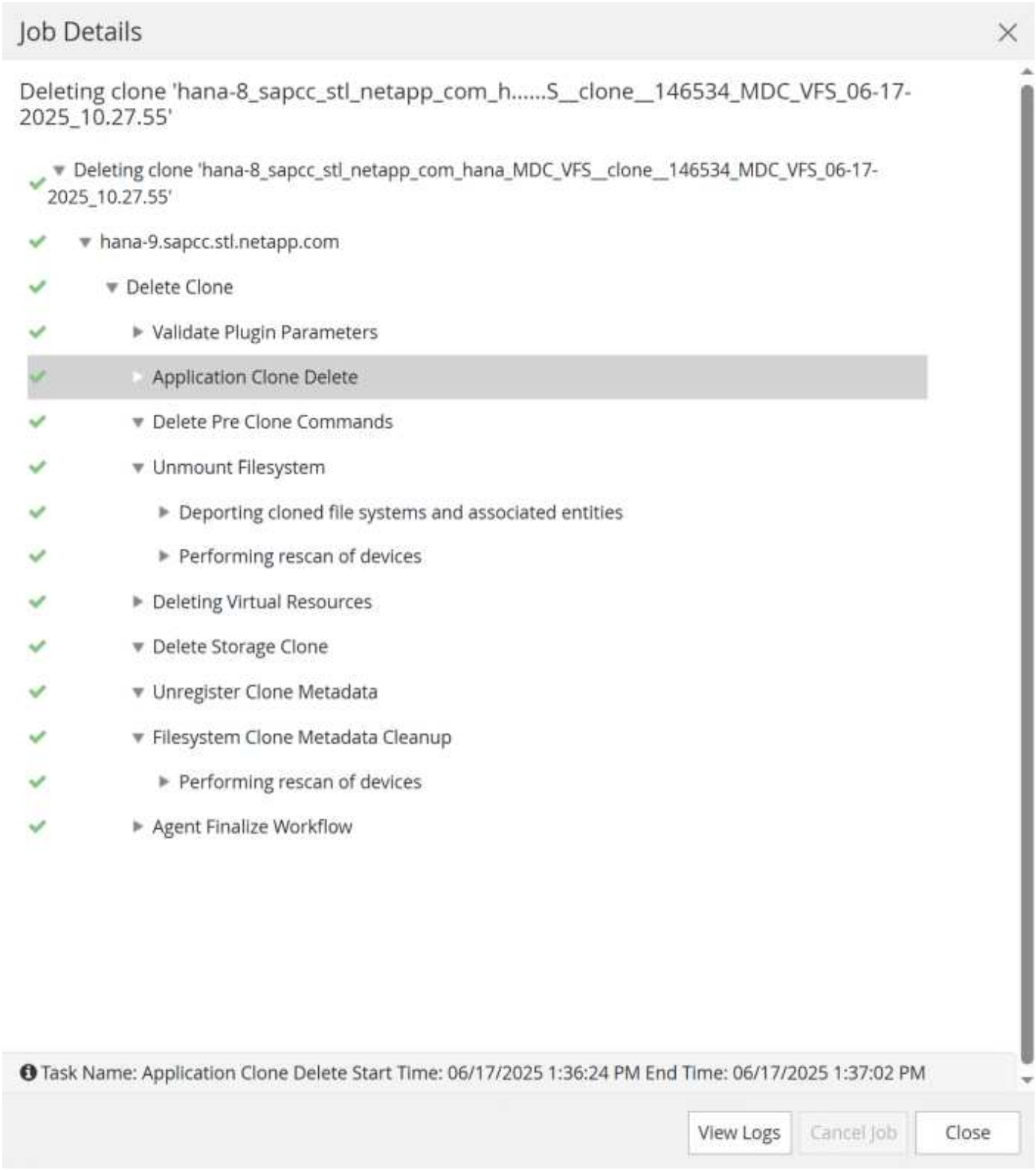
Il flusso di lavoro di eliminazione del clone viene avviato selezionando il clone nella risorsa HANA di origine e facendo clic sul pulsante Elimina.



Nel nostro esempio utilizziamo uno script predefinito per arrestare il database HANA di destinazione.



La seguente schermata mostra i passaggi del processo eseguiti da SnapCenter.



Come menzionato nella sezione "Prerequisiti", il servizio SnapCenter spl sull'host HANA deve essere riavviato utilizzando il comando "systemctl restart spl" per avviare la pulizia corretta.

Informazioni aggiuntive e cronologia delle versioni

Buone pratiche HANA:

- "SAP HANA su sistemi NetApp ASA con protocollo Fibre Channel".

SnapCenter:

- "TR-4614: Backup e recovery SAP HANA con SnapCenter"
- "TR-4719: Replica del sistema SAP HANA - Backup e ripristino con SnapCenter"
- "TR-4667: Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter"
- "Protezione dei dati SAP HANA e alta disponibilità con SnapCenter, SnapMirror ActiveSync e VMware Metro Storage Cluster"
- "Documentazione del software SnapCenter"

Cronologia versioni:

Versione	Data	Commento
Versione 1.0	07/2025	Versione iniziale

Backup e ripristino della replica del sistema SAP HANA con SnapCenter

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

SAP HANA System Replication viene comunemente utilizzato come soluzione ad alta disponibilità o di disaster recovery per i database SAP HANA. SAP HANA System Replication offre diverse modalità operative che è possibile utilizzare in base al caso d'utilizzo o ai requisiti di disponibilità.

Autore: Nils Bauer, NetApp

È possibile combinare due casi di utilizzo principali:

- Alta disponibilità con un obiettivo del punto di ripristino (RPO) pari a zero e un obiettivo RTO (Recovery Time Objective) minimo utilizzando un host SAP HANA secondario dedicato.
- Disaster recovery su larga distanza. L'host SAP HANA secondario può essere utilizzato anche per lo sviluppo o il test durante il normale funzionamento.

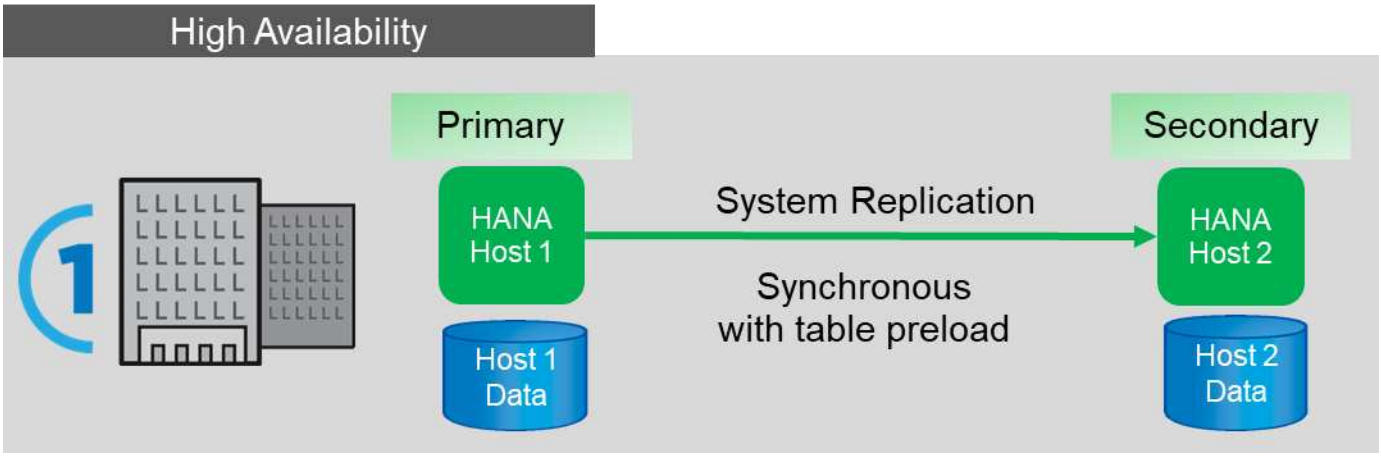
Alta disponibilità con un RPO pari a zero e un RTO minimo

La replica di sistema viene configurata con la replica sincrona utilizzando tabelle precaricate in memoria sull'host SAP HANA secondario. Questa soluzione ad alta disponibilità può essere utilizzata per risolvere i guasti hardware o software e per ridurre i downtime pianificati durante gli aggiornamenti del software SAP HANA (operazioni di downtime quasi pari a zero).

Le operazioni di failover vengono spesso automatizzate utilizzando software di cluster di terze parti o con un semplice clic del workflow con il software SAP Landscape Management.

Dal punto di vista dei requisiti di backup, devi essere in grado di creare backup indipendenti dall'host SAP HANA principale o secondario. Un'infrastruttura di backup condivisa viene utilizzata per ripristinare qualsiasi backup, indipendentemente dall'host su cui è stato creato il backup.

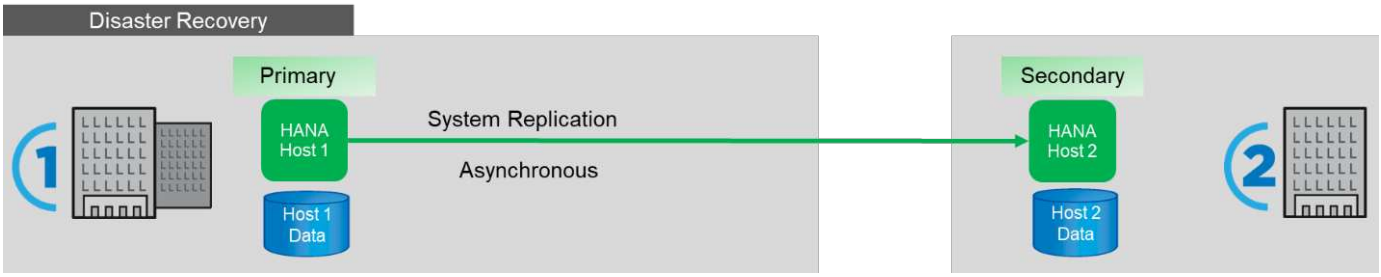
Il resto di questo documento si concentra sulle operazioni di backup con la replica del sistema SAP configurata come soluzione ad alta disponibilità.



Disaster recovery su larga distanza

La replica del sistema può essere configurata con una replica asincrona senza alcuna tabella precaricata nella memoria dell'host secondario. Questa soluzione viene utilizzata per risolvere i guasti del data center e le operazioni di failover vengono in genere eseguite manualmente.

Per quanto riguarda i requisiti di backup, è necessario essere in grado di creare backup durante il normale funzionamento nel data center 1 e durante il disaster recovery nel data center 2. Nei data center 1 e 2 è disponibile un'infrastruttura di backup separata e le operazioni di backup vengono attivate come parte del disaster failover. L'infrastruttura di backup in genere non è condivisa e non è possibile eseguire un'operazione di ripristino di un backup creato nell'altro data center.



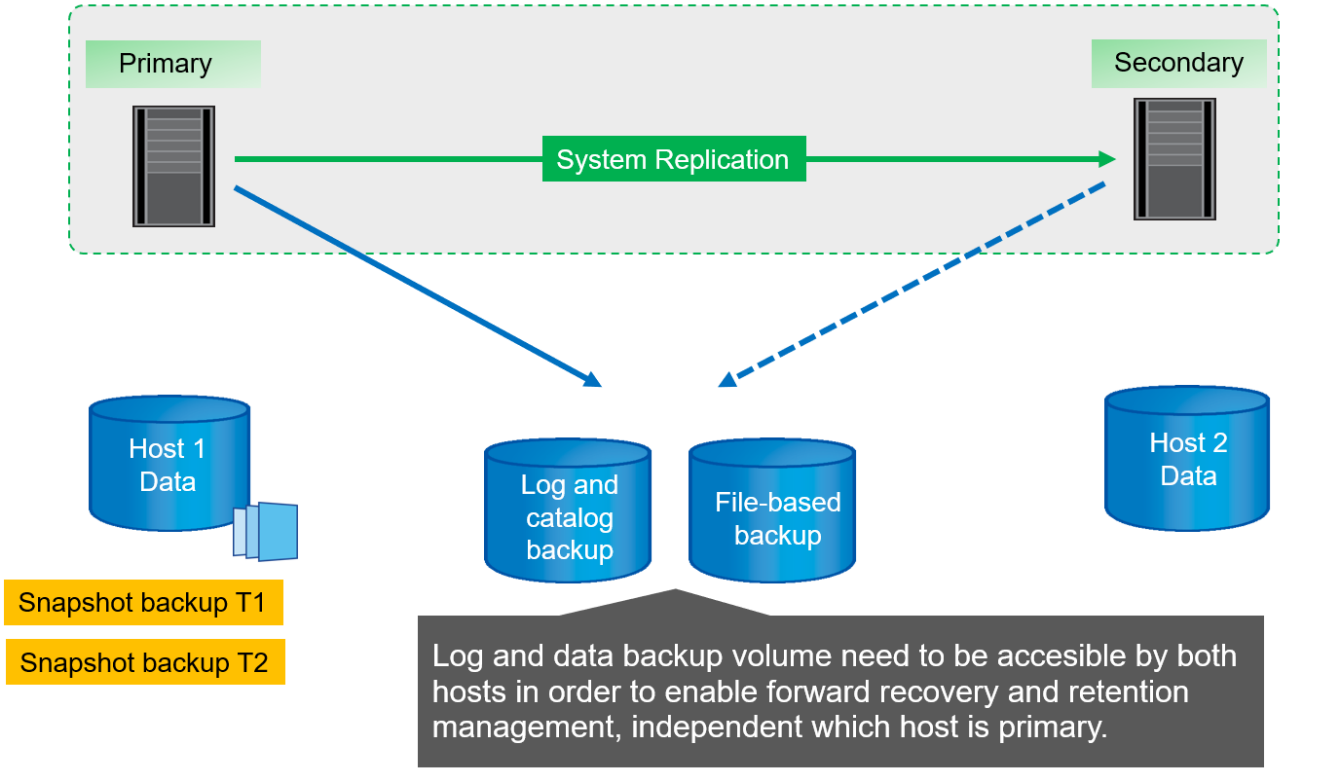
Backup Snapshot dello storage e replica del sistema SAP

Le operazioni di backup vengono sempre eseguite sull'host SAP HANA primario. I comandi SQL richiesti per l'operazione di backup non possono essere eseguiti sull'host SAP HANA secondario.

Per le operazioni di backup SAP HANA, gli host SAP HANA primari e secondari sono una singola entità. Condividono lo stesso catalogo di backup SAP HANA e utilizzano i backup per il ripristino, indipendentemente dal fatto che il backup sia stato creato nell'host SAP HANA primario o secondario.

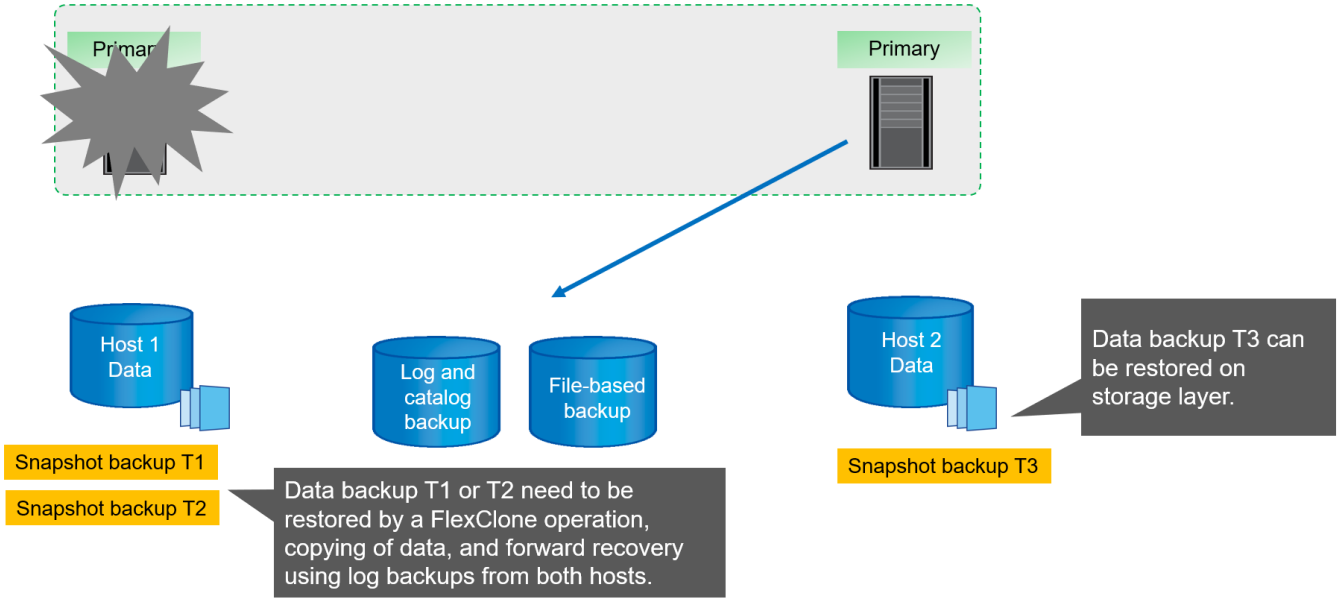
La possibilità di utilizzare qualsiasi backup per il ripristino e l'inoltro del ripristino utilizzando i backup dei log da entrambi gli host richiede una posizione di backup dei log condivisa accessibile da entrambi gli host. NetApp consiglia di utilizzare un volume di storage condiviso. Tuttavia, occorre anche separare la destinazione di backup del log in sottodirectory all'interno del volume condiviso.

Ogni host SAP HANA dispone di un proprio volume di storage. Quando si utilizza un'istantanea basata su storage per eseguire un backup, viene creata un'istantanea coerente con il database sul volume di storage dell'host SAP HANA primario.



Quando viene eseguito un failover sull'host 2, l'host 2 diventa l'host primario, i backup vengono eseguiti sull'host 2 e i backup Snapshot vengono creati sul volume di storage dell'host 2.

Il backup creato sull'host 2 può essere ripristinato direttamente al livello di storage. Se è necessario utilizzare un backup creato sull'host 1, il backup deve essere copiato dal volume di storage dell'host 1 al volume di storage dell'host 2. Forward Recovery utilizza i backup dei log di entrambi gli host.

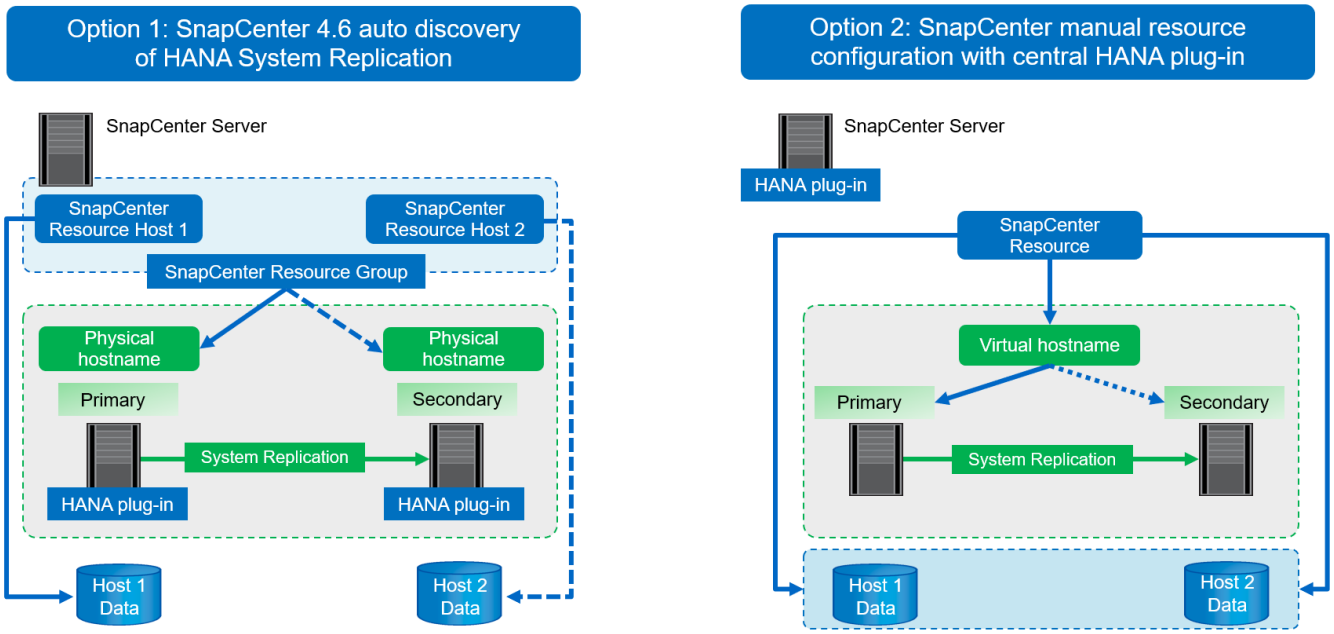


Opzioni di configurazione SnapCenter per la replica del sistema SAP

Sono disponibili due opzioni per la configurazione della protezione dei dati con il software

NetApp SnapCenter in un ambiente di replica del sistema SAP HANA:

- Un gruppo di risorse SnapCenter che include host SAP HANA e il rilevamento automatico con SnapCenter versione 4.6 o superiore.
- Una singola risorsa SnapCenter per entrambi gli host SAP HANA che utilizzano un indirizzo IP virtuale.



A partire da SnapCenter 4.6, SnapCenter supporta il rilevamento automatico dei sistemi HANA configurati in una relazione di replica del sistema HANA. Ciascun host viene configurato utilizzando il proprio indirizzo IP fisico (nome host) e il proprio volume di dati sul layer di storage. Le due risorse SnapCenter sono combinate in un gruppo di risorse e SnapCenter identifica automaticamente l'host primario o secondario ed esegue le operazioni di backup richieste di conseguenza. La gestione della conservazione per Snapshot e backup basati su file creati da SnapCenter viene eseguita su entrambi gli host per garantire che i vecchi backup vengano cancellati anche sull'host secondario corrente.

Con una configurazione a singola risorsa per entrambi gli host SAP HANA, la singola risorsa SnapCenter viene configurata utilizzando l'indirizzo IP virtuale degli host di replica del sistema SAP HANA. Entrambi i volumi di dati degli host SAP HANA sono inclusi nella risorsa SnapCenter. Poiché si tratta di una singola risorsa SnapCenter, la gestione della conservazione per Snapshot e i backup basati su file creati da SnapCenter funziona indipendentemente dall'host attualmente primario o secondario. Queste opzioni sono possibili con tutte le versioni di SnapCenter.

La seguente tabella riassume le differenze principali delle due opzioni di configurazione.

	Gruppo di risorse con SnapCenter 4.6	**Singola risorsa SnapCenter e indirizzo IP virtuale**
Operazione di backup (Snapshot e basato su file)	Identificazione automatica dell'host primario nel gruppo di risorse	Utilizza automaticamente l'indirizzo IP virtuale
Gestione della conservazione (Snapshot e basato su file)	Eseguito automaticamente su entrambi gli host	Utilizza automaticamente una singola risorsa

	Gruppo di risorse con SnapCenter 4.6	Singola risorsa SnapCenter e indirizzo IP virtuale
Requisiti di capacità per il backup	I backup vengono creati solo sul volume host primario	I backup vengono sempre creati su entrambi i volumi host. Il backup del secondo host è coerente solo con il crash e non può essere utilizzato per eseguire un rollforward.
Ripristinare l'operazione	I backup dall'host attivo corrente sono disponibili per l'operazione di ripristino	Script di pre-backup necessario per identificare i backup validi e che possono essere utilizzati per il ripristino
Operazione di recovery	Tutte le opzioni di ripristino disponibili, come per qualsiasi risorsa rilevata automaticamente	Ripristino manuale richiesto

In generale, NetApp consiglia di utilizzare l'opzione di configurazione del gruppo di risorse con SnapCenter 4.6 per proteggere i sistemi HANA con la replica del sistema HANA abilitata. L'utilizzo di una singola configurazione delle risorse SnapCenter è necessario solo se l'approccio operativo SnapCenter è basato su un host plug-in centrale e il plug-in HANA non è distribuito sugli host del database HANA.

Le due opzioni sono descritte in dettaglio nelle sezioni seguenti.

Configurazione di SnapCenter 4.6 mediante un gruppo di risorse

SnapCenter 4.6 supporta il rilevamento automatico per i sistemi HANA configurati con la replica del sistema HANA. SnapCenter 4.6 include la logica per identificare gli host HANA primari e secondari durante le operazioni di backup e gestisce anche la gestione della conservazione su entrambi gli host HANA. Inoltre, il ripristino e il ripristino automatici sono ora disponibili anche per gli ambienti di replica del sistema HANA.

Configurazione di SnapCenter 4.6 per gli ambienti di replica del sistema HANA

La figura seguente mostra la configurazione di laboratorio utilizzata per questo capitolo. Due host HANA, hana-3 e hana-4, sono stati configurati con la replica di sistema HANA.

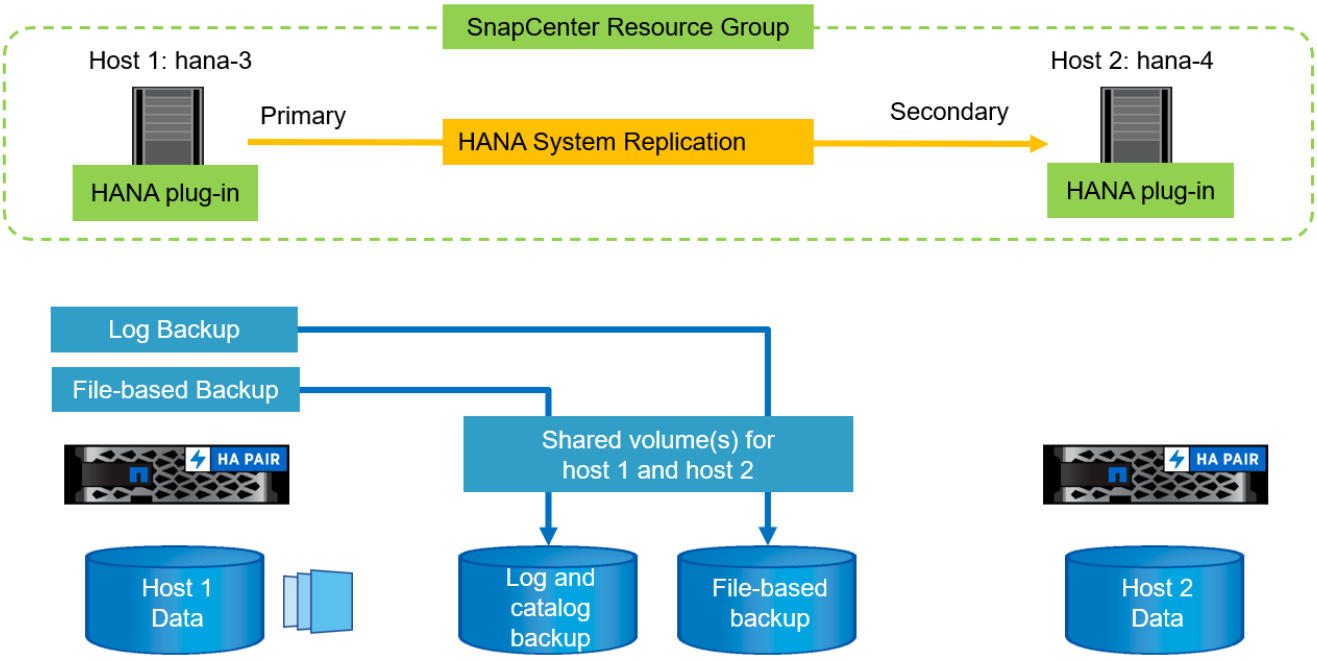
Un utente di database "SnapCenter" è stato creato per il database del sistema HANA con il Privileges richiesto per eseguire le operazioni di backup e ripristino (vedere "Backup e ripristino SAP HANA con SnapCenter"). È necessario configurare una chiave di memorizzazione utente HANA su entrambi gli host utilizzando l'utente del database indicato sopra.

```
ss2adm@hana- 3: / > hdbuserstore set SS2KEY hana- 3:33313 SNAPCENTER
<password>
```

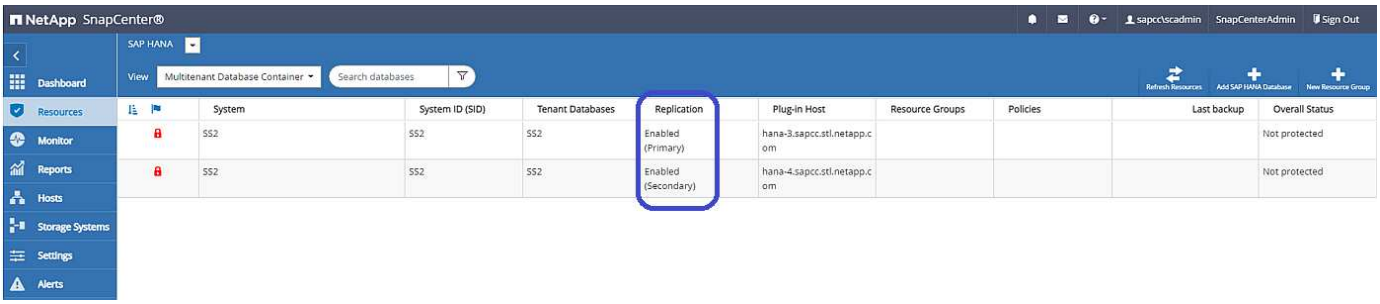
```
ss2adm@hana- 4:/ > hdbuserstore set SS2KEY hana-4:33313 SNAPCENTER
<password>
```

Da un punto di vista di alto livello, è necessario eseguire i seguenti passaggi per configurare la replica del sistema HANA in SnapCenter.

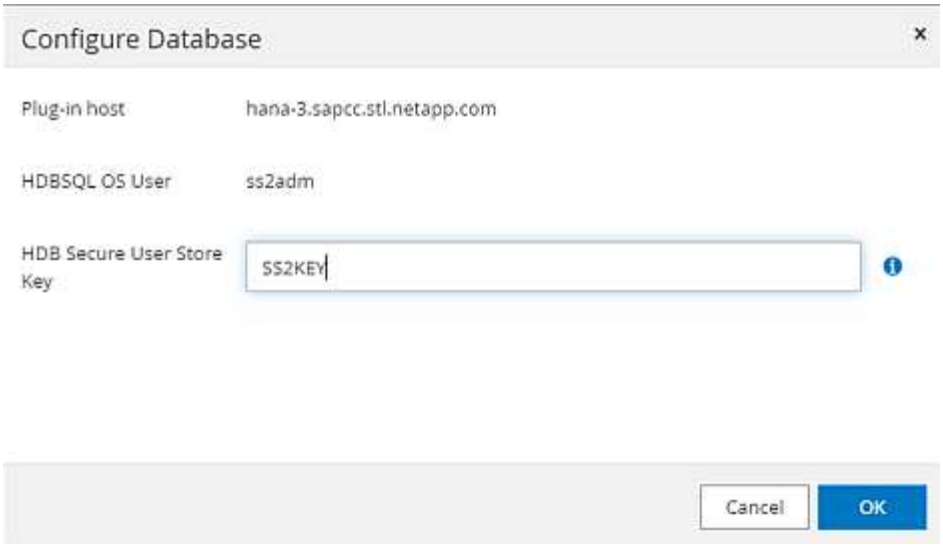
1. Installare il plug-in HANA sull'host primario e secondario. Viene eseguita la rilevazione automatica e viene rilevato lo stato di replica del sistema HANA per ogni host primario o secondario.
2. Eseguire SnapCenter `configure database` e fornire il `hdbuserstore` chiave. Vengono eseguite ulteriori operazioni di rilevamento automatico.
3. Creare un gruppo di risorse, inclusi entrambi gli host e configurare la protezione.



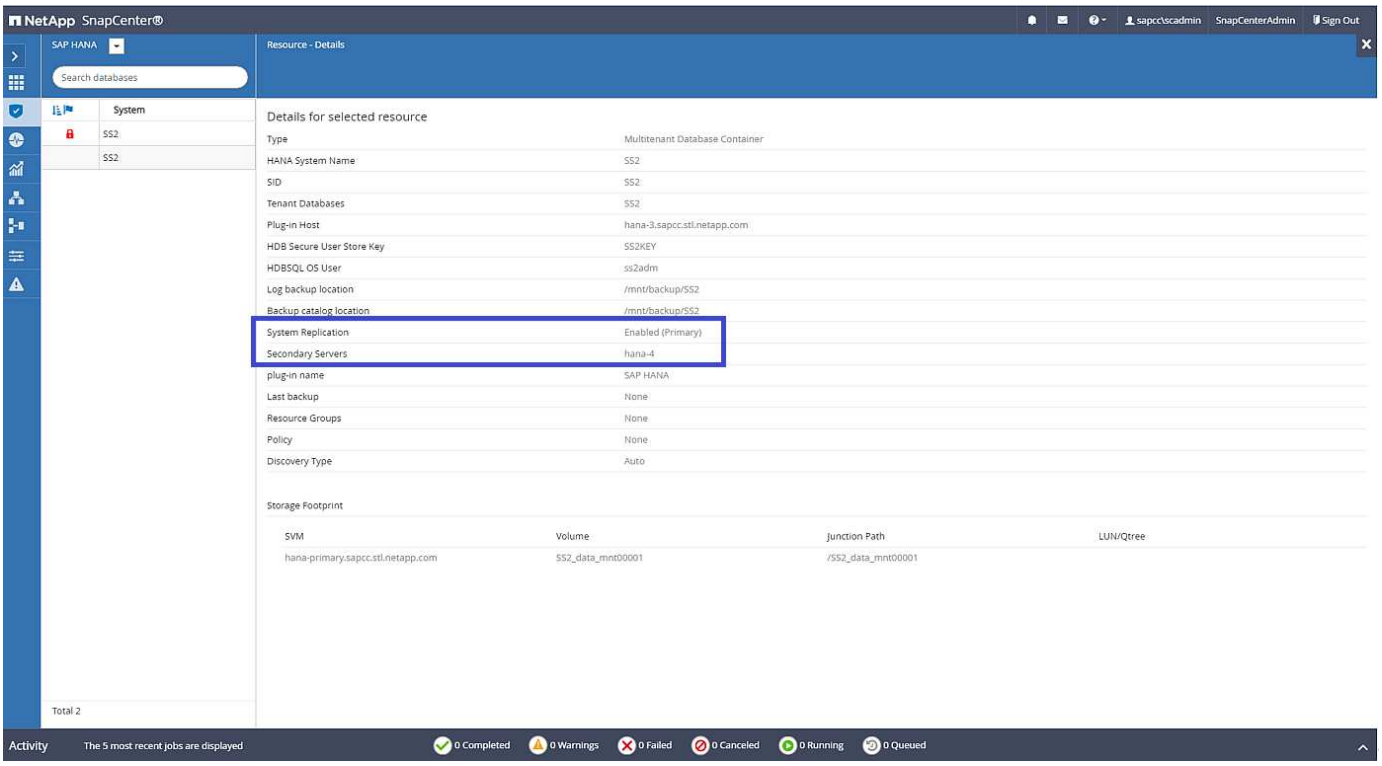
Dopo aver installato il plug-in HANA di SnapCenter su entrambi gli host HANA, i sistemi HANA vengono visualizzati nella vista delle risorse di SnapCenter allo stesso modo delle altre risorse rilevate automaticamente. A partire da SnapCenter 4.6, viene visualizzata una colonna aggiuntiva che mostra lo stato della replica del sistema HANA (attivata/disattivata, primaria/secondaria).



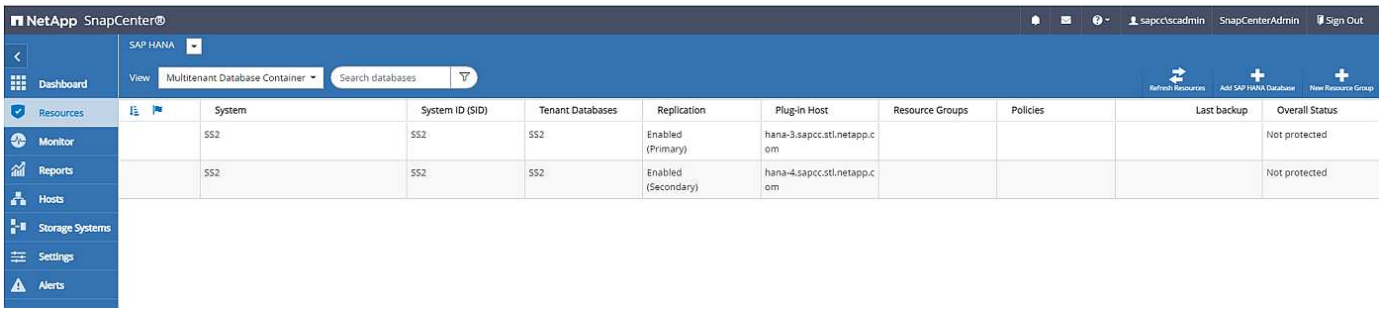
Facendo clic sulla risorsa, SnapCenter richiede la chiave di archivio utente HANA per il sistema HANA.



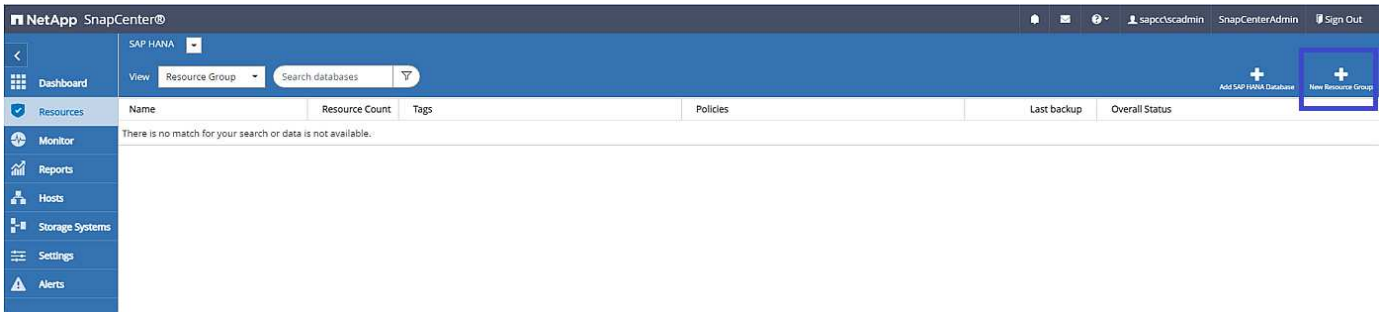
Vengono eseguite ulteriori operazioni di rilevamento automatico e SnapCenter mostra i dettagli delle risorse. In SnapCenter 4.6, lo stato della replica del sistema e il server secondario sono elencati in questa vista.



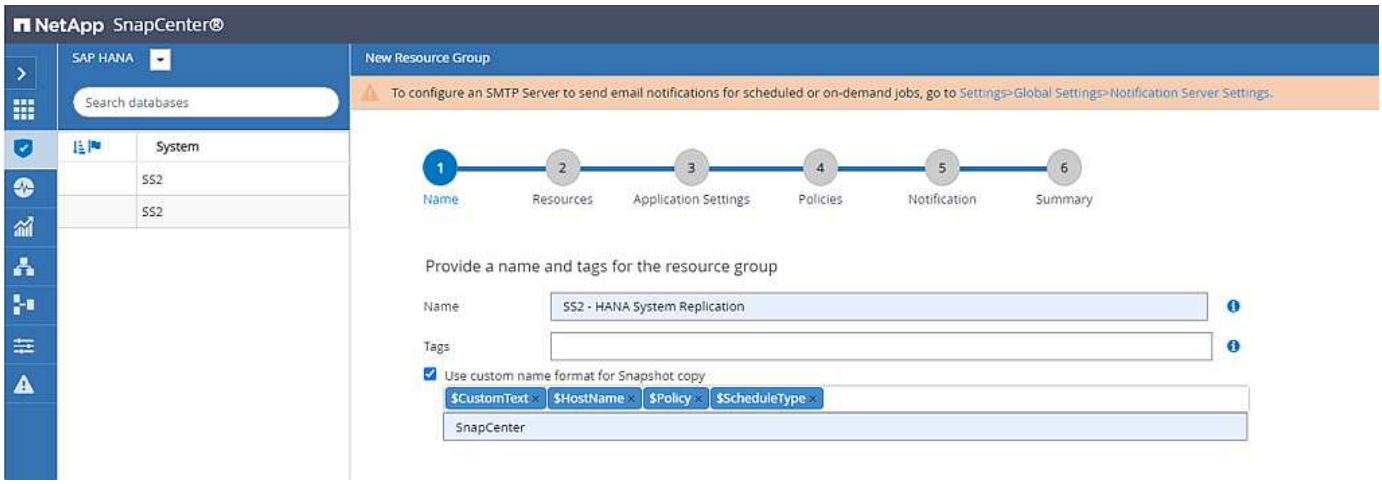
Dopo aver eseguito le stesse operazioni per la seconda risorsa HANA, il processo di individuazione automatica è completo e entrambe le risorse HANA sono configurate in SnapCenter.



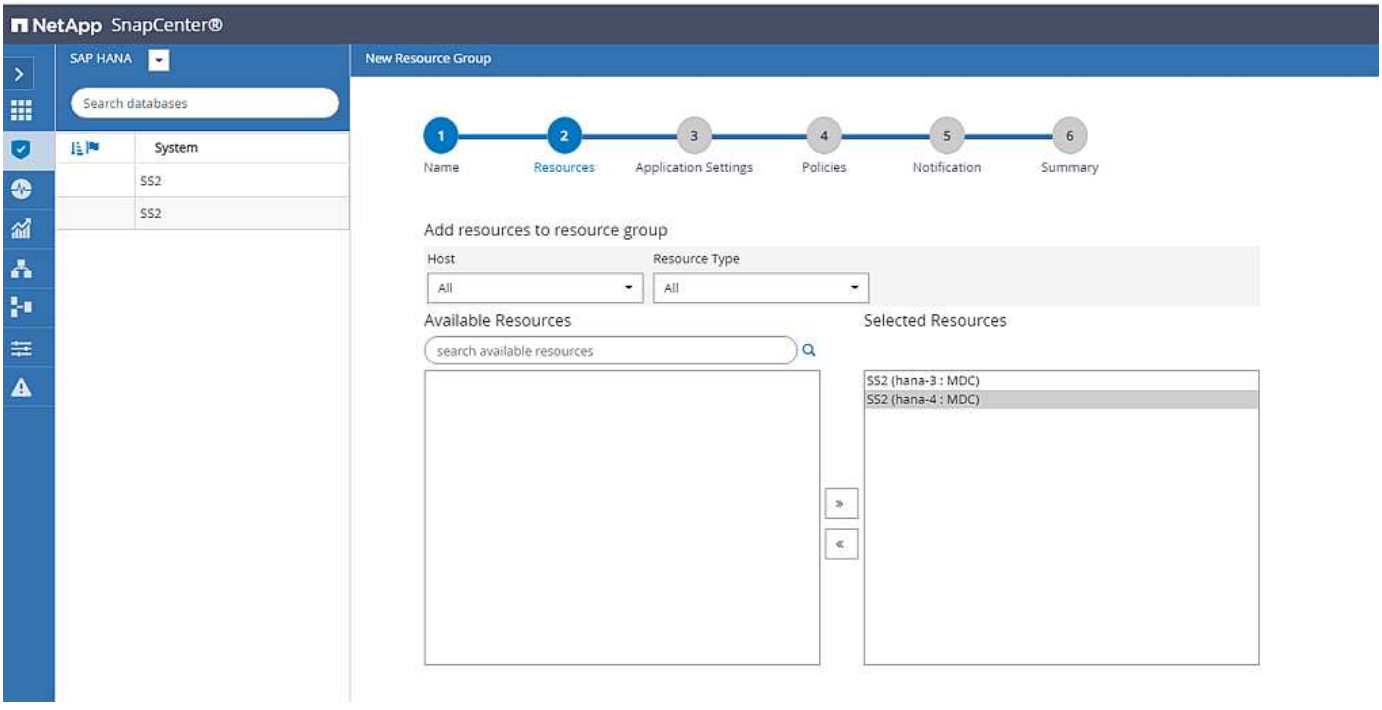
Per i sistemi abilitati alla replica del sistema HANA, è necessario configurare un gruppo di risorse SnapCenter, incluse entrambe le risorse HANA.



NetApp consiglia di utilizzare un formato nome personalizzato per il nome Snapshot, che deve includere il nome host, la policy e la pianificazione.

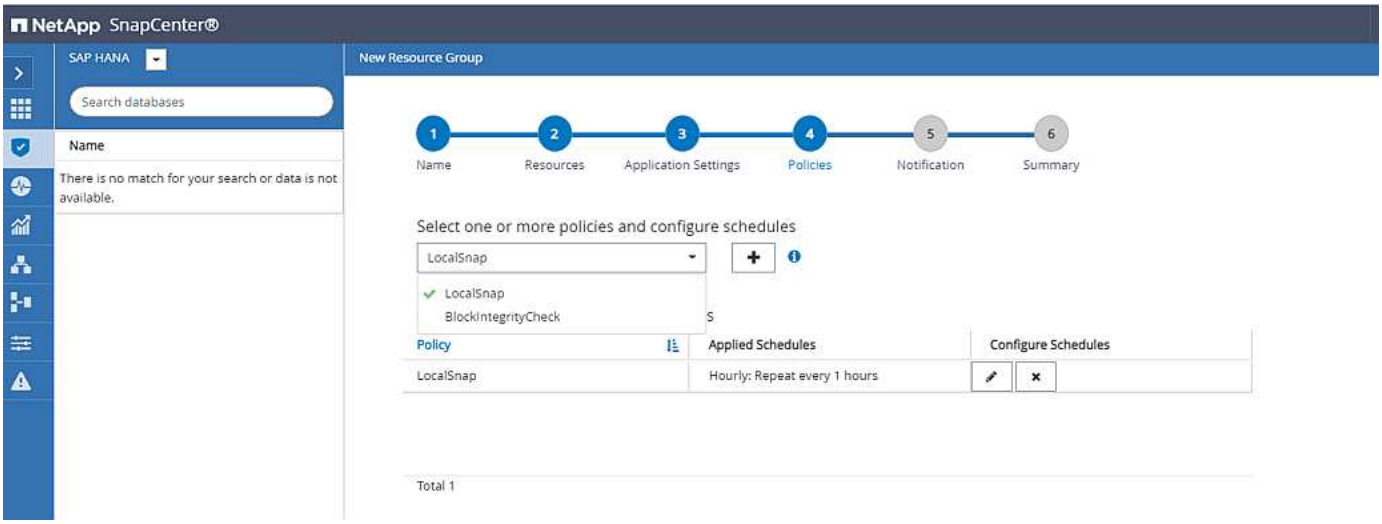


È necessario aggiungere entrambi gli host HANA al gruppo di risorse.

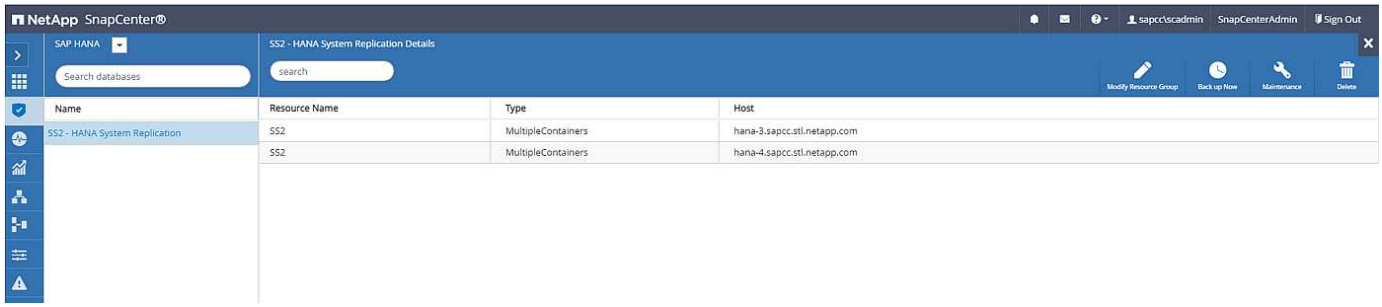


I criteri e le pianificazioni vengono configurati per il gruppo di risorse.

La conservazione definita nel criterio viene utilizzata in entrambi gli host HANA. Se, ad esempio, nel criterio viene definita una conservazione di 10, la somma dei backup di entrambi gli host viene utilizzata come criterio per l'eliminazione del backup. SnapCenter elimina il backup meno recente indipendentemente se è stato creato sull'host primario o secondario corrente.



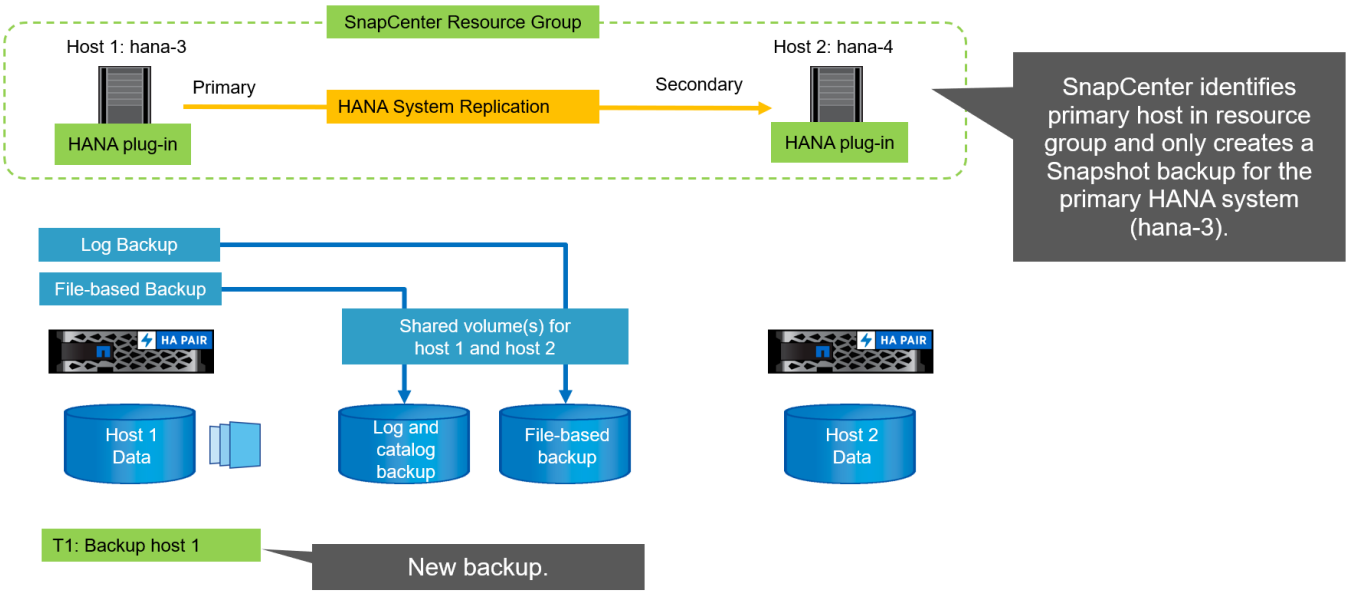
La configurazione del gruppo di risorse è terminata ed è possibile eseguire i backup.



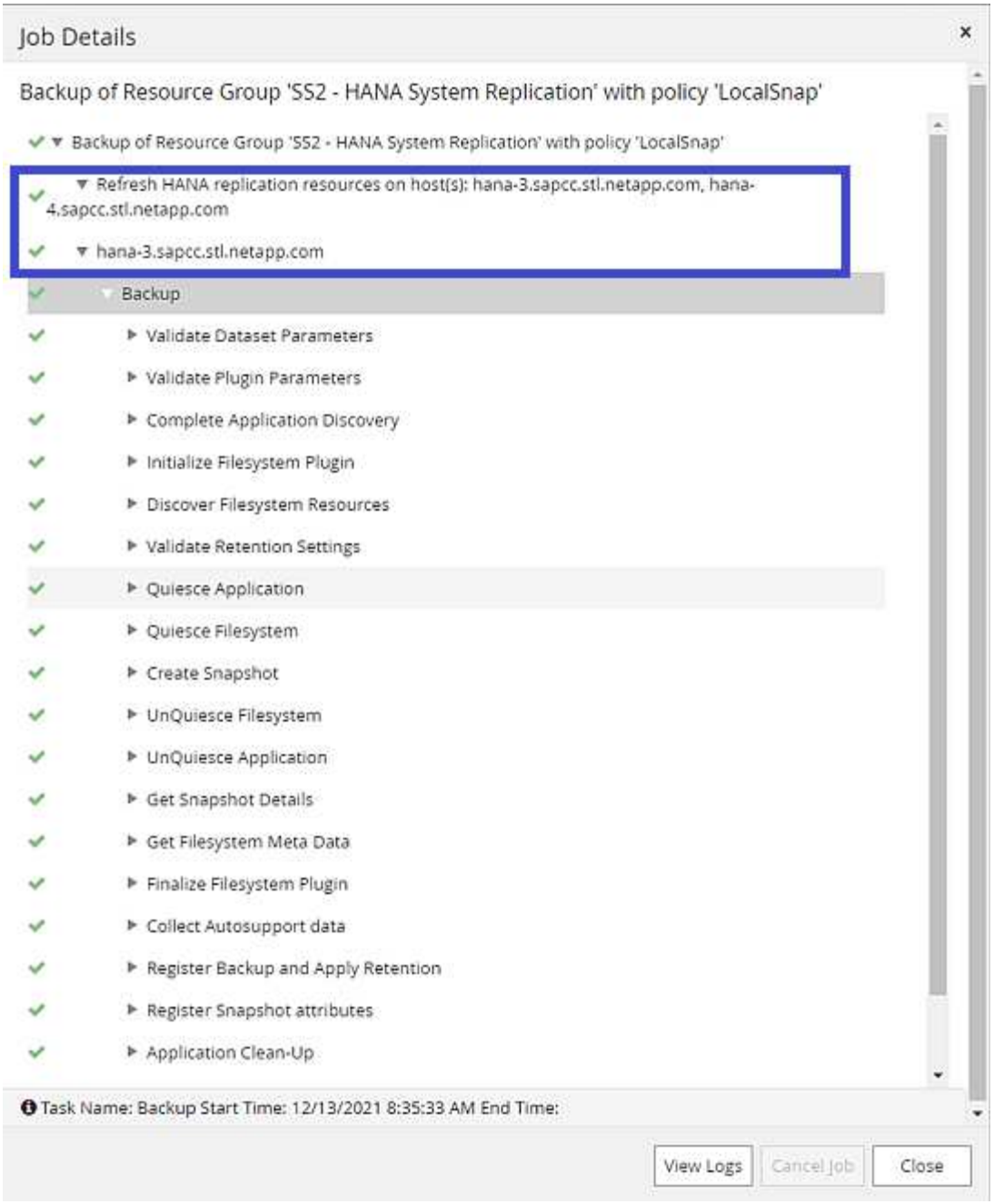


Operazioni di backup di Snapshot

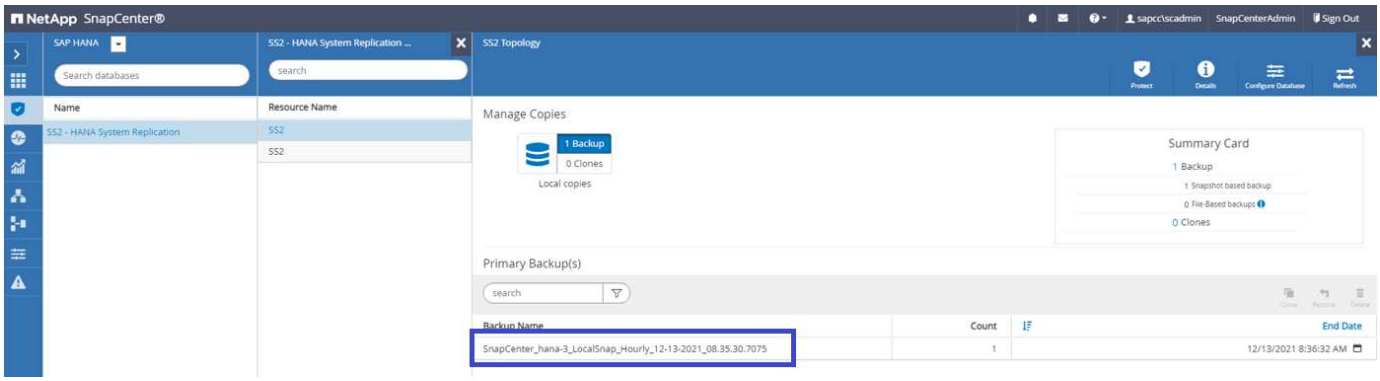
Quando viene eseguita un'operazione di backup del gruppo di risorse, SnapCenter identifica l'host primario e attiva un backup solo sull'host primario. In questo modo, verrà attivato lo snap-shoting solo del volume di dati dell'host primario. Nel nostro esempio, hana-3 è l'host primario corrente e viene eseguito un backup su questo host.



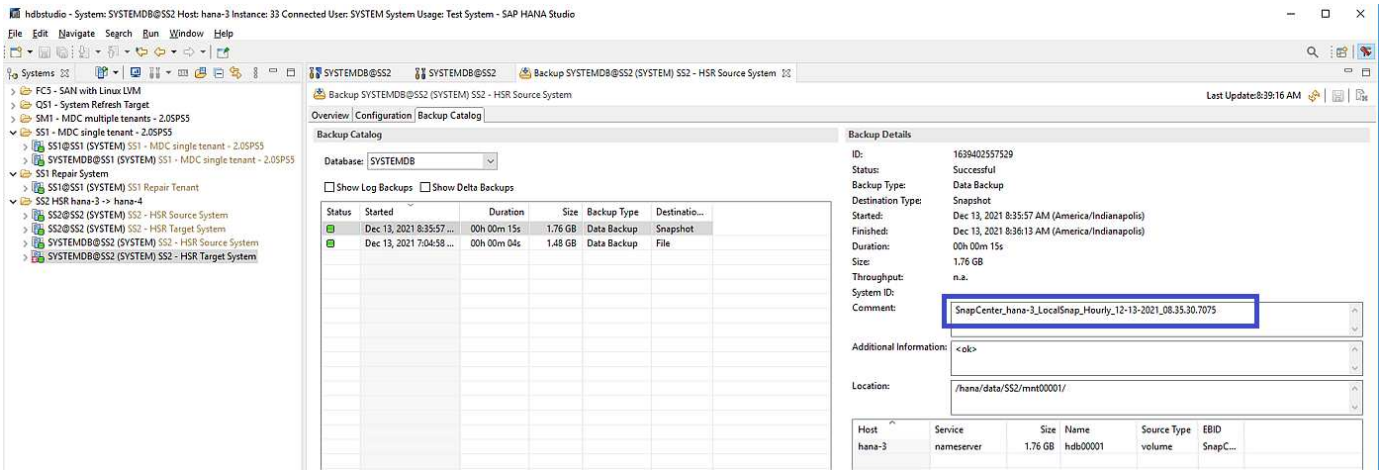
Il log dei lavori di SnapCenter mostra l'operazione di identificazione e l'esecuzione del backup sull'host primario corrente hana-3.



È stato creato un backup Snapshot nella risorsa HANA principale. Il nome host incluso nel nome del backup mostra hana-3.

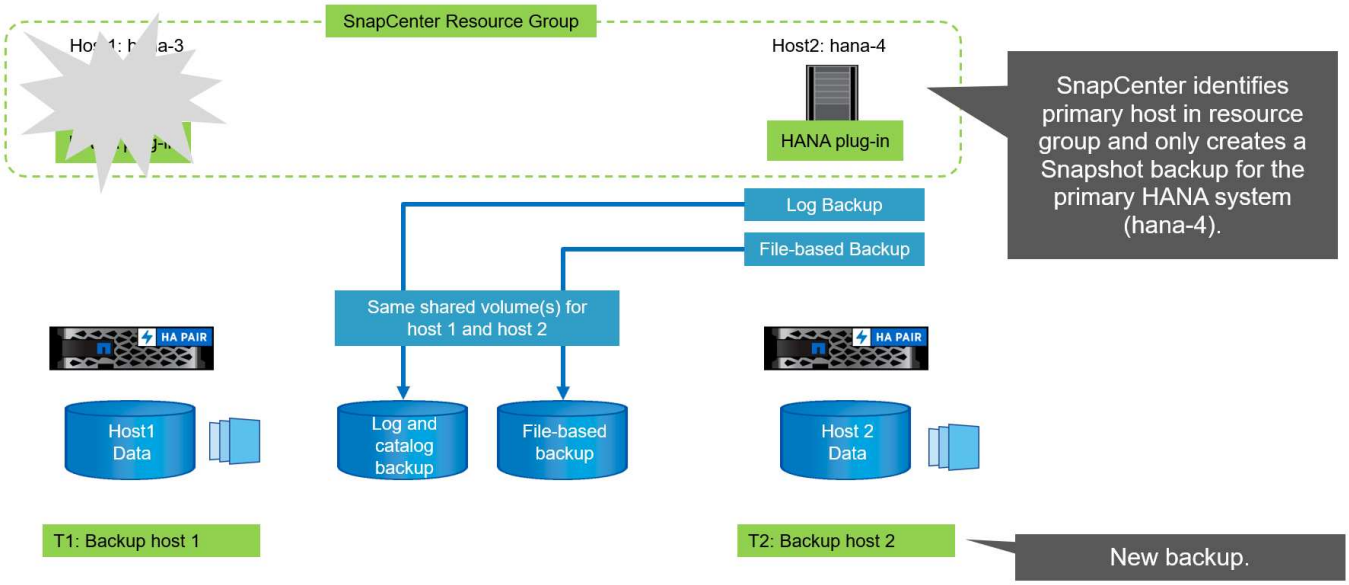


Lo stesso backup Snapshot è anche visibile nel catalogo di backup HANA.

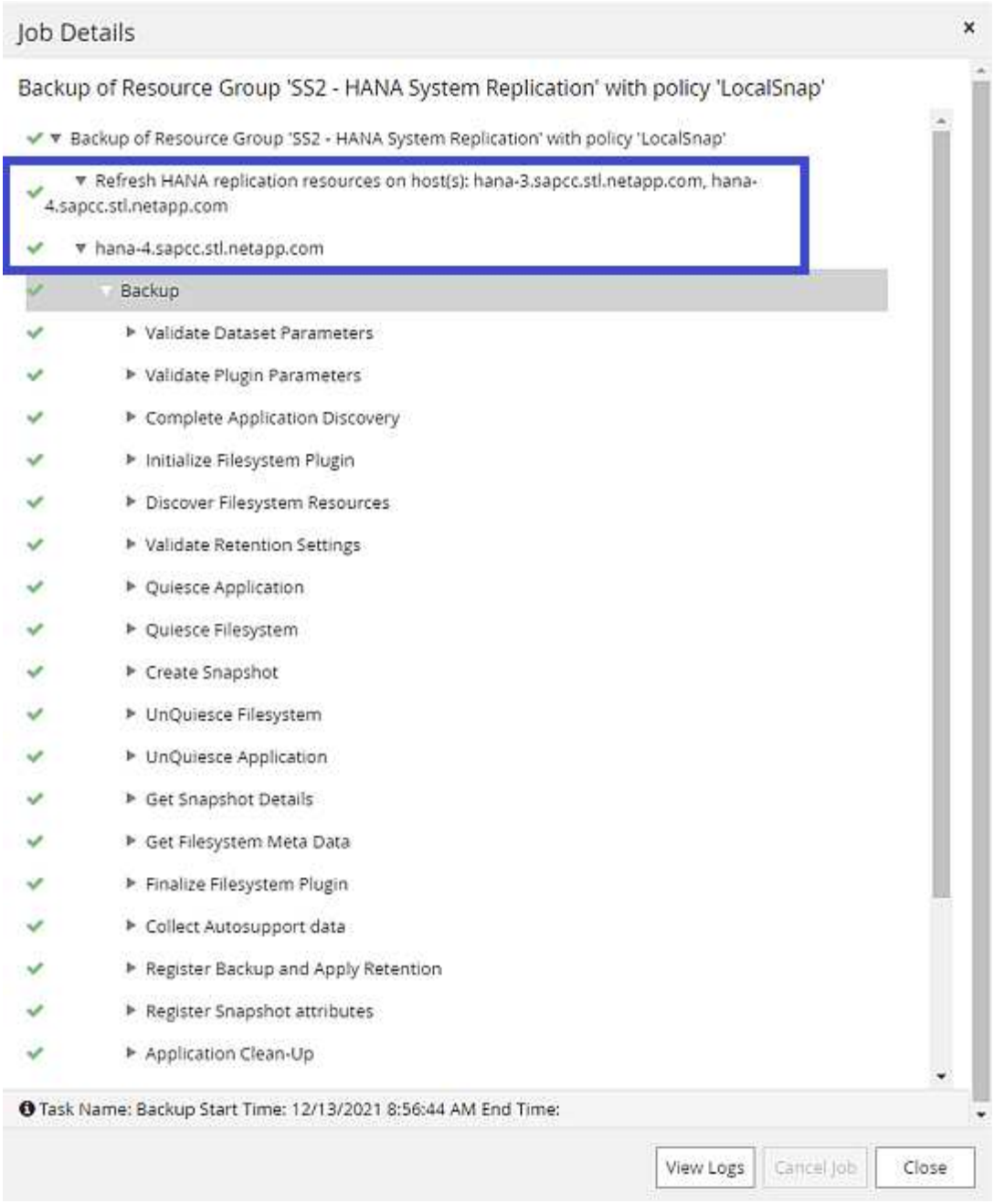


Se viene eseguita un'operazione di Takeover, ulteriori backup SnapCenter identificano ora il precedente host secondario (hana-4) come primario e l'operazione di backup viene eseguita in hana-4. Anche in questo caso, viene attivato solo il volume di dati del nuovo host primario (hana-4).

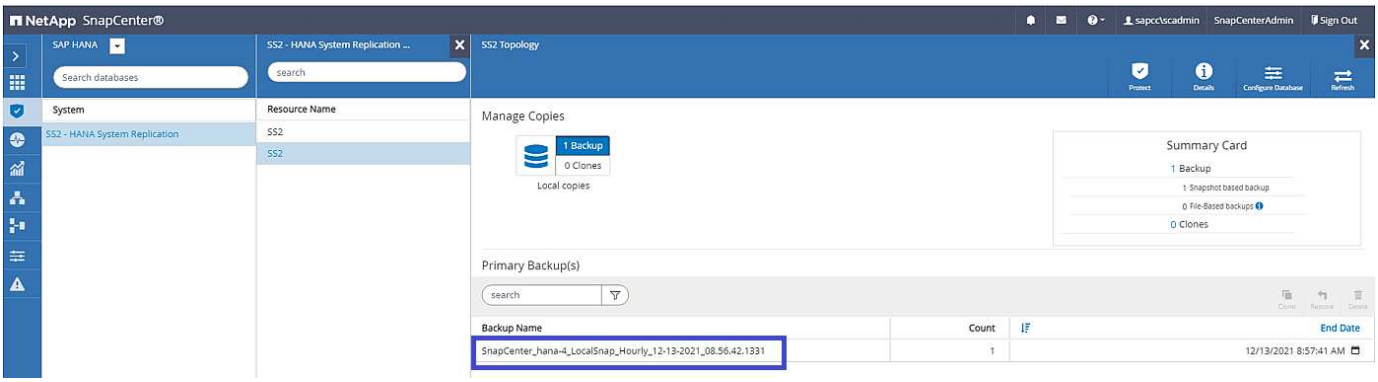
La logica di identificazione SnapCenter copre solo gli scenari in cui gli host HANA si trovano in una relazione primaria-secondaria o quando uno degli host HANA è offline.



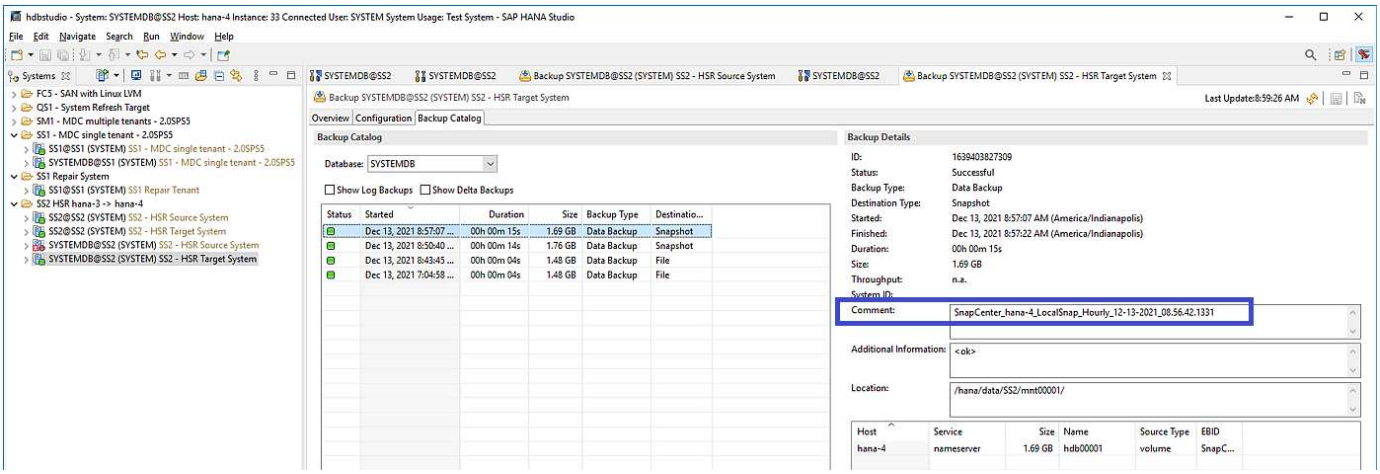
Il log dei lavori di SnapCenter mostra l'operazione di identificazione e l'esecuzione del backup sull'host primario corrente hana-4.



È stato creato un backup Snapshot nella risorsa HANA principale. Il nome host incluso nel nome del backup mostra hana-4.



Lo stesso backup Snapshot è anche visibile nel catalogo di backup HANA.



Operazioni di controllo dell'integrità dei blocchi con backup basati su file

SnapCenter 4.6 utilizza la stessa logica descritta per le operazioni di backup Snapshot per le operazioni di controllo dell'integrità dei blocchi con backup basati su file. SnapCenter identifica l'host HANA primario corrente ed esegue il backup basato su file per questo host. La gestione della conservazione viene eseguita anche su entrambi gli host, in modo che il backup più vecchio venga cancellato indipendentemente dall'host attualmente primario.

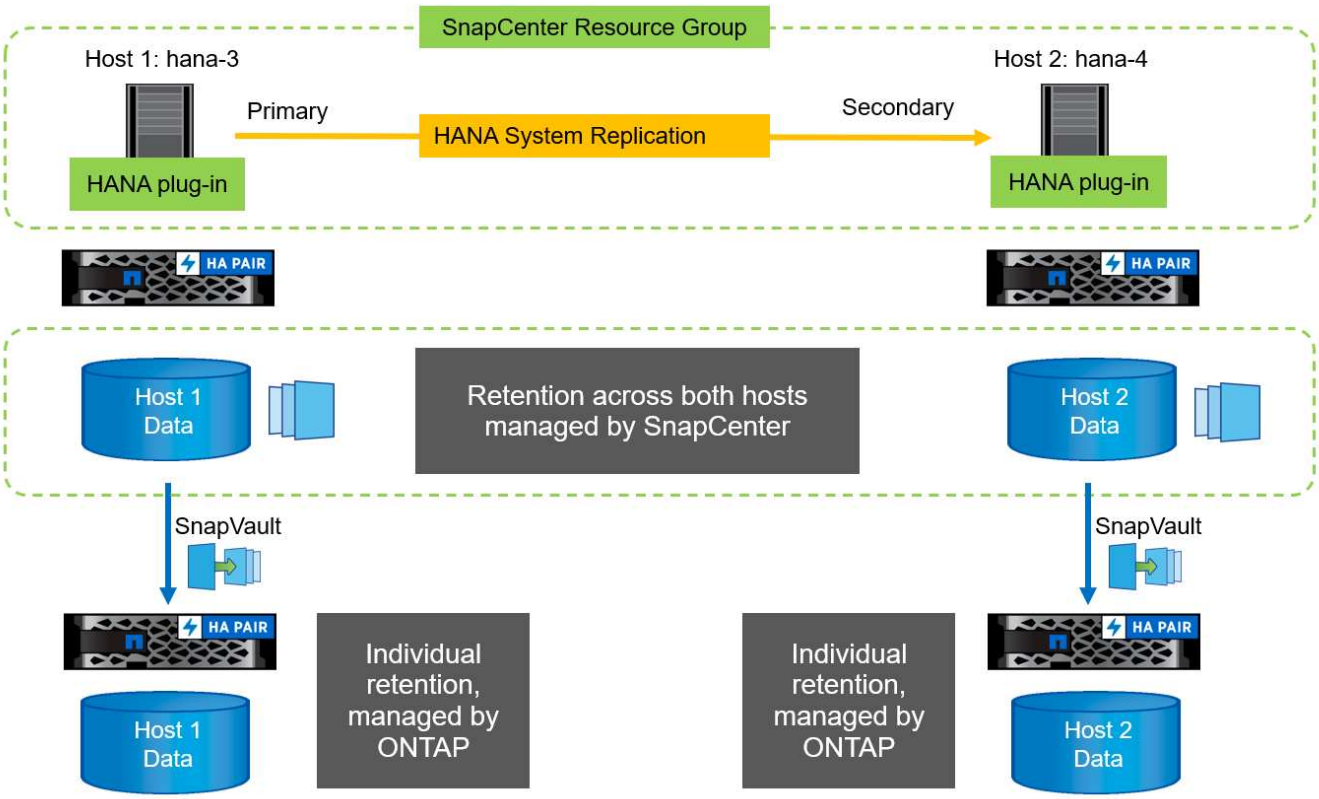
Replica SnapVault

Per consentire operazioni di backup trasparenti senza l'interazione manuale in caso di Takeover e indipendentemente da quale host HANA sia attualmente l'host primario, è necessario configurare una relazione SnapVault per i volumi di dati di entrambi gli host. SnapCenter esegue un'operazione di aggiornamento del SnapVault per l'host primario corrente ad ogni esecuzione del backup.

> Se un takeover all'host secondario non viene eseguito per molto tempo, il numero di blocchi modificati per il primo aggiornamento SnapVault sull'host secondario sarà elevato.

Poiché la gestione della conservazione presso la destinazione SnapVault viene gestita da ONTAP al di fuori di SnapCenter, la conservazione non può essere gestita su entrambi gli host HANA. Pertanto, i backup creati prima di un Takeover non vengono cancellati con le operazioni di backup sul precedente secondario. Questi backup rimangono fino a quando il primo primario non diventa nuovamente primario. Affinché questi backup non blocchino la gestione della conservazione dei backup dei log, devono essere eliminati manualmente nella destinazione SnapVault o all'interno del catalogo di backup HANA.

> Non è possibile eseguire la pulizia di tutte le copie Snapshot di SnapVault, poiché una copia Snapshot viene bloccata come punto di sincronizzazione. Se è necessario eliminare anche la copia Snapshot più recente, è necessario eliminare la relazione di replica SnapVault. In questo caso, NetApp consiglia di eliminare i backup nel catalogo di backup HANA per sbloccare la gestione della conservazione dei backup dei log.



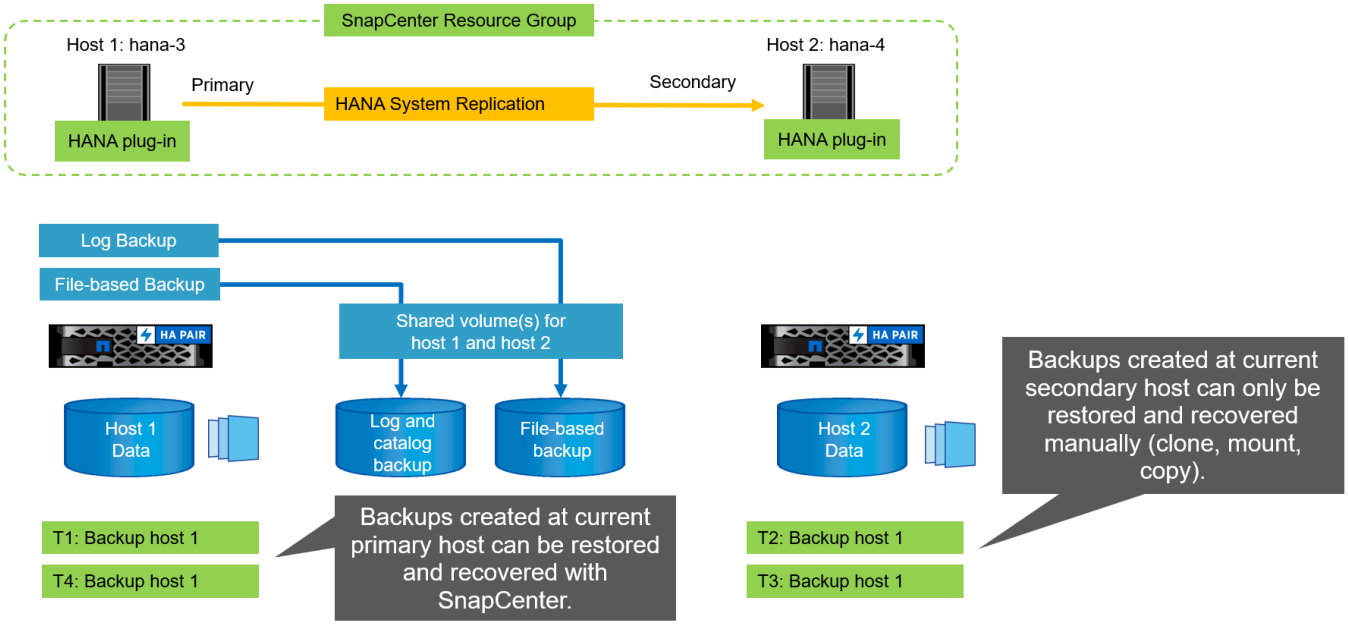
Gestione della conservazione

SnapCenter 4.6 gestisce la conservazione per i backup Snapshot, le operazioni di controllo dell'integrità dei blocchi, le voci del catalogo di backup HANA e i backup dei log (se non disattivati) su entrambi gli host HANA, quindi non importa quale host sia attualmente primario o secondario. I backup (dati e log) e le voci del catalogo HANA vengono cancellati in base alla conservazione definita, indipendentemente dal fatto che sia necessaria un'operazione di eliminazione sull'host primario o secondario corrente. In altre parole, non è richiesta alcuna interazione manuale se viene eseguita un'operazione di Takeover e/o la replica viene configurata nell'altra direzione.

Se la replica di SnapVault fa parte della strategia di protezione dei dati, è necessaria un'interazione manuale per scenari specifici, come descritto nella sezione "Replica SnapVault"

Ripristino e ripristino

La figura seguente mostra uno scenario in cui sono stati eseguiti più takeover e sono stati creati backup Snapshot in entrambi i siti. Con lo stato corrente, l'host hana-3 è l'host primario e l'ultimo backup è T4, creato sull'host hana-3. Se è necessario eseguire un'operazione di ripristino e ripristino, i backup T1 e T4 sono disponibili per il ripristino e il ripristino in SnapCenter. I backup creati sull'host hana-4 (T2, T3) non possono essere ripristinati utilizzando SnapCenter. Questi backup devono essere copiati manualmente nel volume di dati di hana-3 per il ripristino.



Le operazioni di ripristino e ripristino per una configurazione del gruppo di risorse di SnapCenter 4.6 sono identiche a quelle di una configurazione della replica non di sistema rilevata automaticamente. Sono disponibili tutte le opzioni per il ripristino e il ripristino automatizzato. Per ulteriori informazioni, vedere il rapporto tecnico "TR-4614: Backup e ripristino SAP HANA con SnapCenter".

Un'operazione di ripristino da un backup creato nell'altro host è descritta nella sezione "Ripristino e ripristino da un backup creato sull'altro host".

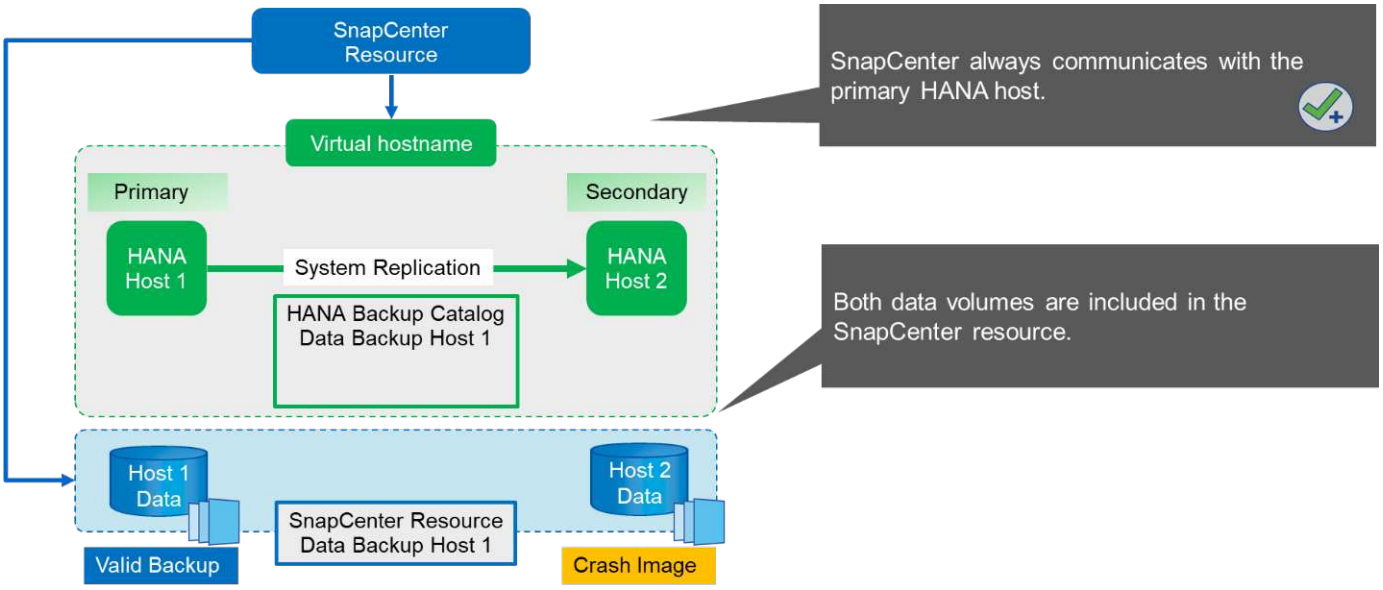
Configurazione di SnapCenter con una singola risorsa

Una risorsa SnapCenter viene configurata con l'indirizzo IP virtuale (nome host) dell'ambiente di replica del sistema HANA. Con questo approccio, SnapCenter comunica sempre con l'host primario, indipendentemente dal fatto che l'host 1 o l'host 2 sia primario. I volumi di dati di entrambi gli host SAP HANA sono inclusi nella risorsa SnapCenter.

> Si presuppone che l'indirizzo IP virtuale sia sempre associato all'host SAP HANA primario. Il failover dell'indirizzo IP virtuale viene eseguito all'esterno di SnapCenter come parte del workflow di failover della replica del sistema HANA.

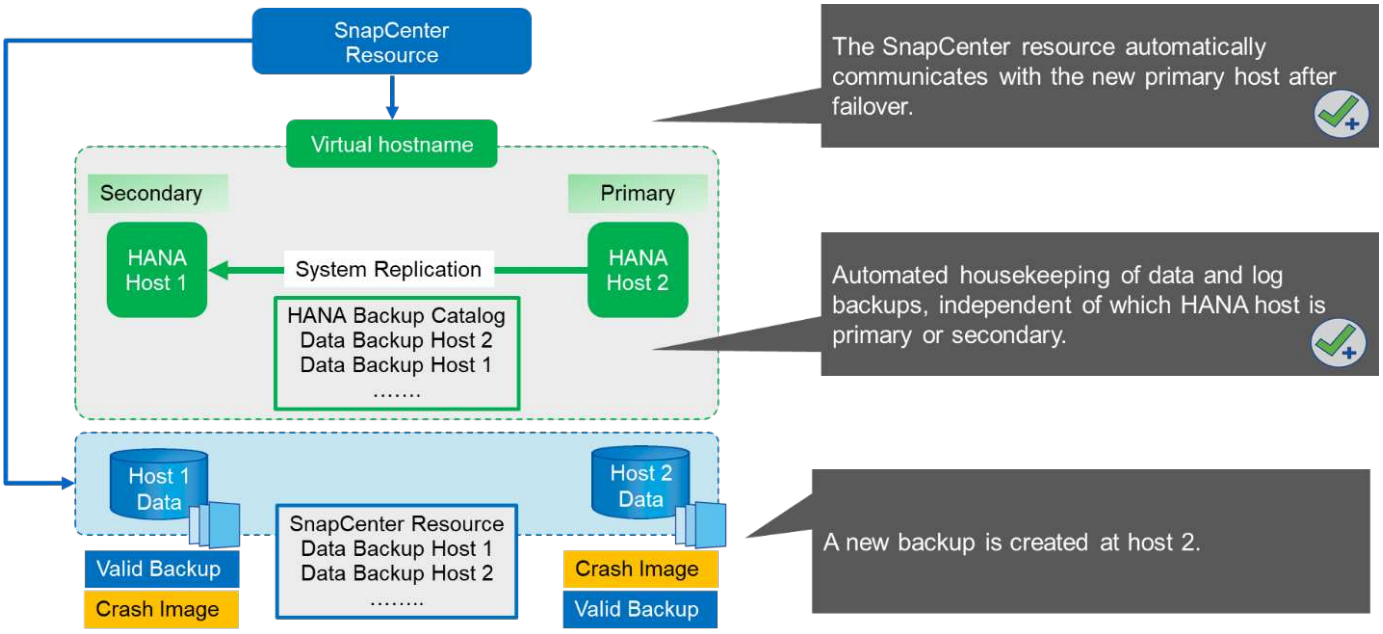
Quando viene eseguito un backup con host 1 come host primario, viene creato un backup Snapshot coerente con il database nel volume di dati dell'host 1. Poiché il volume di dati dell'host 2 fa parte della risorsa SnapCenter, viene creata un'altra copia Snapshot per questo volume. Questa copia Snapshot non è coerente con il database, ma è solo un'immagine di crash dell'host secondario.

Il catalogo di backup SAP HANA e la risorsa SnapCenter includono il backup creato sull'host 1.



La figura seguente mostra l'operazione di backup dopo il failover sull'host 2 e la replica dall'host 2 all'host 1. SnapCenter comunica automaticamente con l'host 2 utilizzando l'indirizzo IP virtuale configurato nella risorsa SnapCenter. I backup vengono ora creati sull'host 2. SnapCenter crea due copie Snapshot: Un backup coerente con il database nel volume di dati dell'host 2 e una copia Snapshot dell'immagine di crash nel volume di dati dell'host 1. Il catalogo di backup SAP HANA e la risorsa SnapCenter ora includono il backup creato sull'host 1 e il backup creato sull'host 2.

La gestione dei backup dei dati e dei log si basa sulla policy di conservazione di SnapCenter definita e i backup vengono cancellati indipendentemente dall'host primario o secondario.

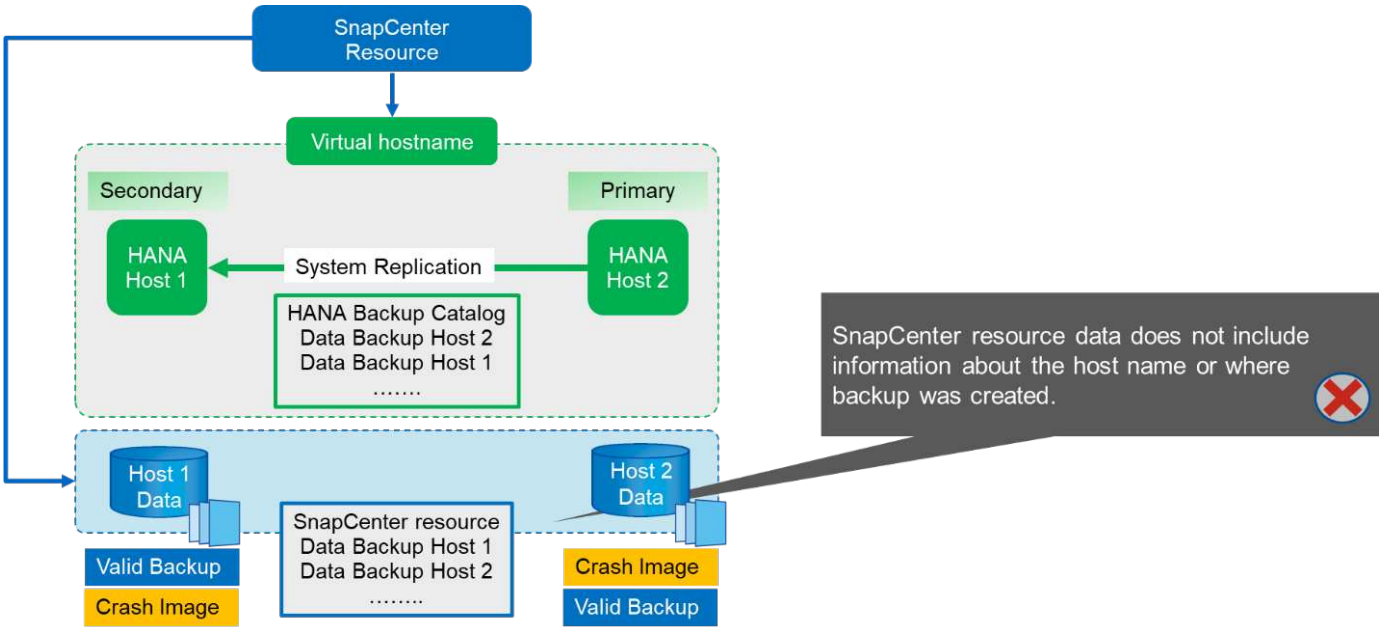


Come illustrato nella sezione "Backup Snapshot dello storage e replica del sistema SAP", un'operazione di ripristino con backup Snapshot basati su storage è diversa, a seconda del backup da ripristinare. È importante identificare l'host in cui è stato creato il backup per determinare se il ripristino può essere eseguito sul volume di storage locale o se il ripristino deve essere eseguito sul volume di storage dell'altro host.

Con la configurazione SnapCenter a singola risorsa, SnapCenter non è a conoscenza della posizione in cui è stato creato il backup. Pertanto, NetApp consiglia di aggiungere uno script di prebackup al workflow di backup

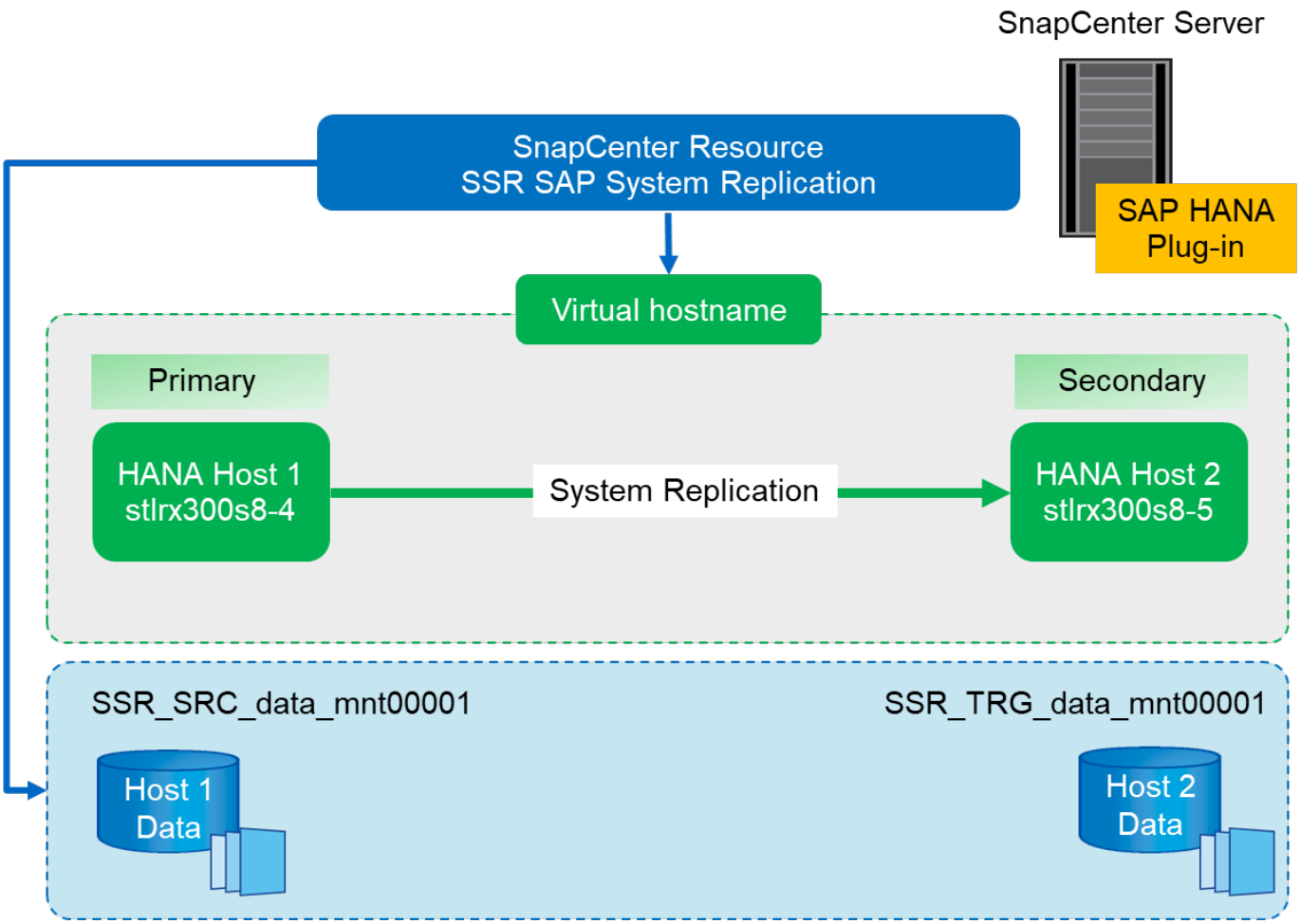
di SnapCenter per identificare quale host è attualmente l'host SAP HANA primario.

La figura seguente mostra l'identificazione dell'host di backup.



Configurazione di SnapCenter

La figura seguente mostra la configurazione di laboratorio e una panoramica della configurazione SnapCenter richiesta.



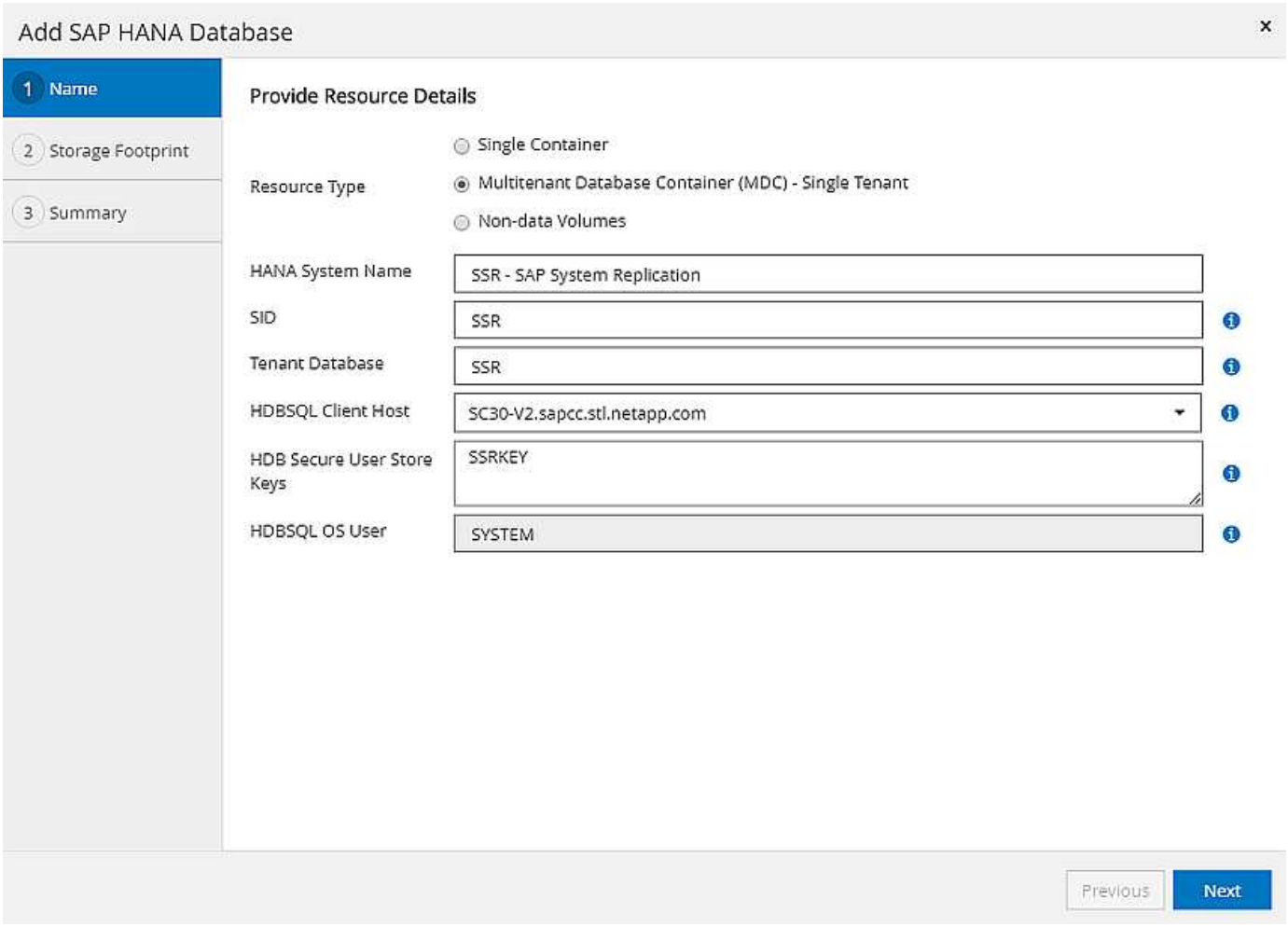
Per eseguire operazioni di backup indipendentemente dall'host SAP HANA primario e anche quando un host è inattivo, il plug-in SAP HANA di SnapCenter deve essere implementato su un host plug-in centrale. Nella nostra configurazione di laboratorio, abbiamo utilizzato il server SnapCenter come host plug-in centrale e abbiamo implementato il plug-in SAP HANA sul server SnapCenter.

Nel database HANA è stato creato un utente per eseguire operazioni di backup. Una chiave di archivio utente è stata configurata sul server SnapCenter su cui è stato installato il plug-in SAP HANA. La chiave dell'archivio utente include l'indirizzo IP virtuale degli host di replica del sistema SAP HANA (`ssr-vip`).

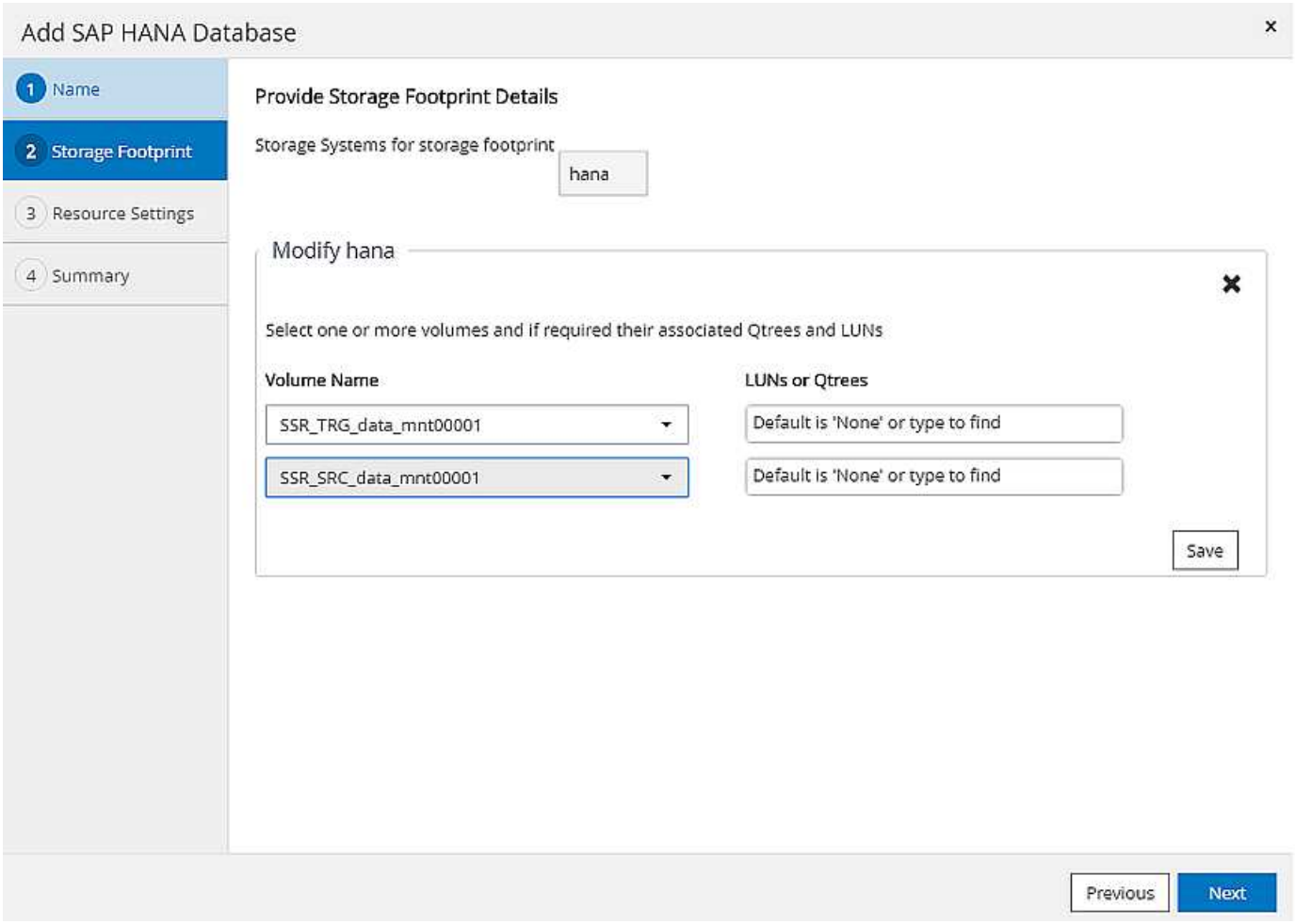
```
hdbuserstore.exe -u SYSTEM set SSRKEY ssr-vip:31013 SNAPCENTER <password>
```

Per ulteriori informazioni sulle opzioni di implementazione dei plug-in SAP HANA e sulla configurazione dell'archivio utenti, consulta il report tecnico TR-4614: "Backup e ripristino SAP HANA con SnapCenter".

In SnapCenter, la risorsa viene configurata come mostrato nella figura seguente utilizzando la chiave di memorizzazione utente, configurata in precedenza, e il server SnapCenter come `hdbsql` host di comunicazione.

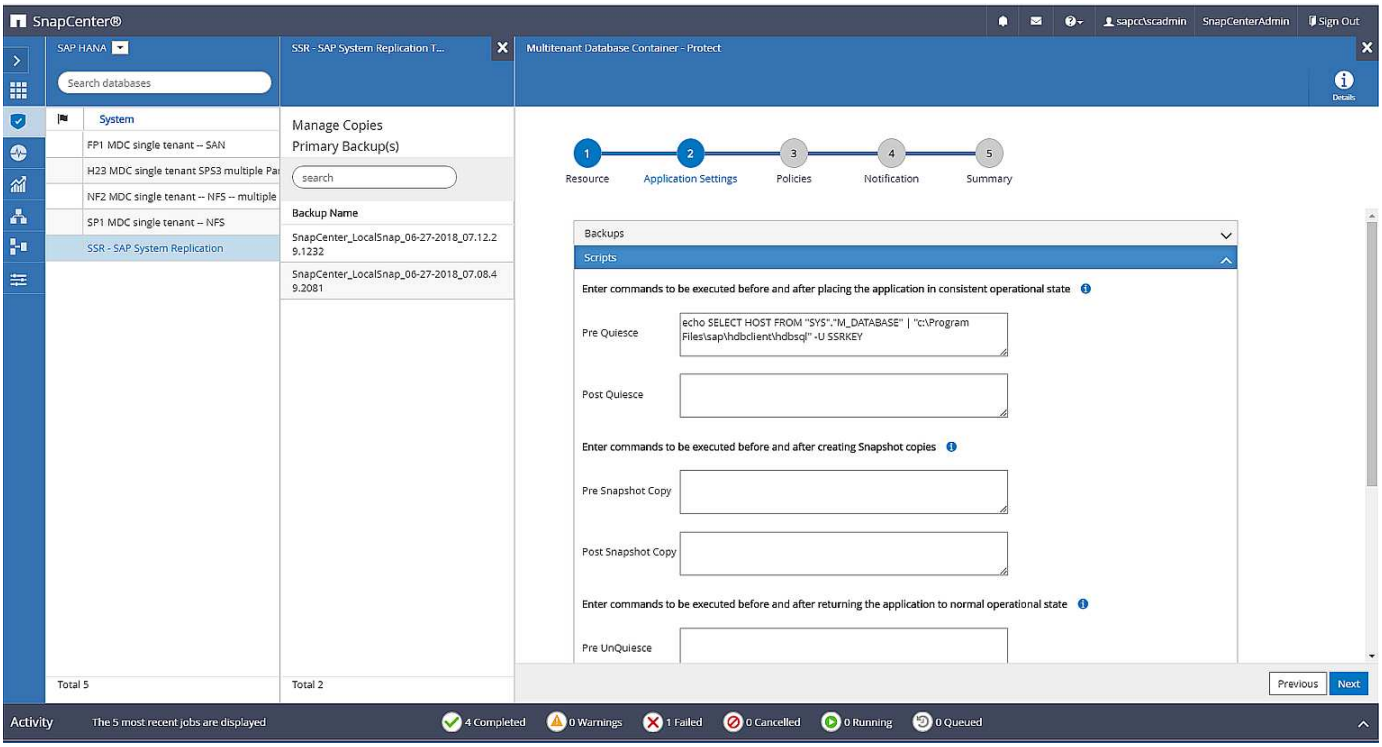


I volumi di dati di entrambi gli host SAP HANA sono inclusi nella configurazione del footprint dello storage, come mostrato nella figura seguente.



Come discusso in precedenza, SnapCenter non è a conoscenza della posizione in cui è stato creato il backup. NetApp consiglia pertanto di aggiungere uno script di pre-backup nel flusso di lavoro di backup di SnapCenter per identificare quale host è attualmente l'host SAP HANA primario. È possibile eseguire questa identificazione utilizzando un'istruzione SQL aggiunta al flusso di lavoro di backup, come illustrato nella figura seguente.

```
Select host from "SYS".M_DATABASE
```

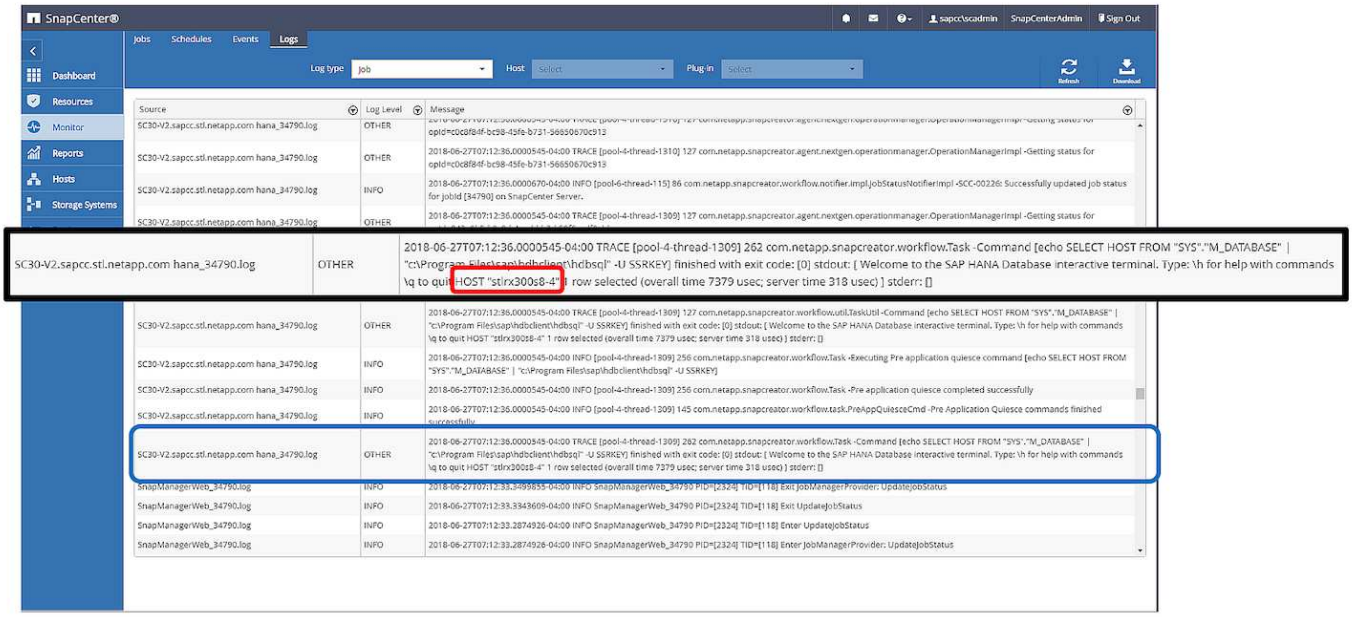


Operazione di backup di SnapCenter

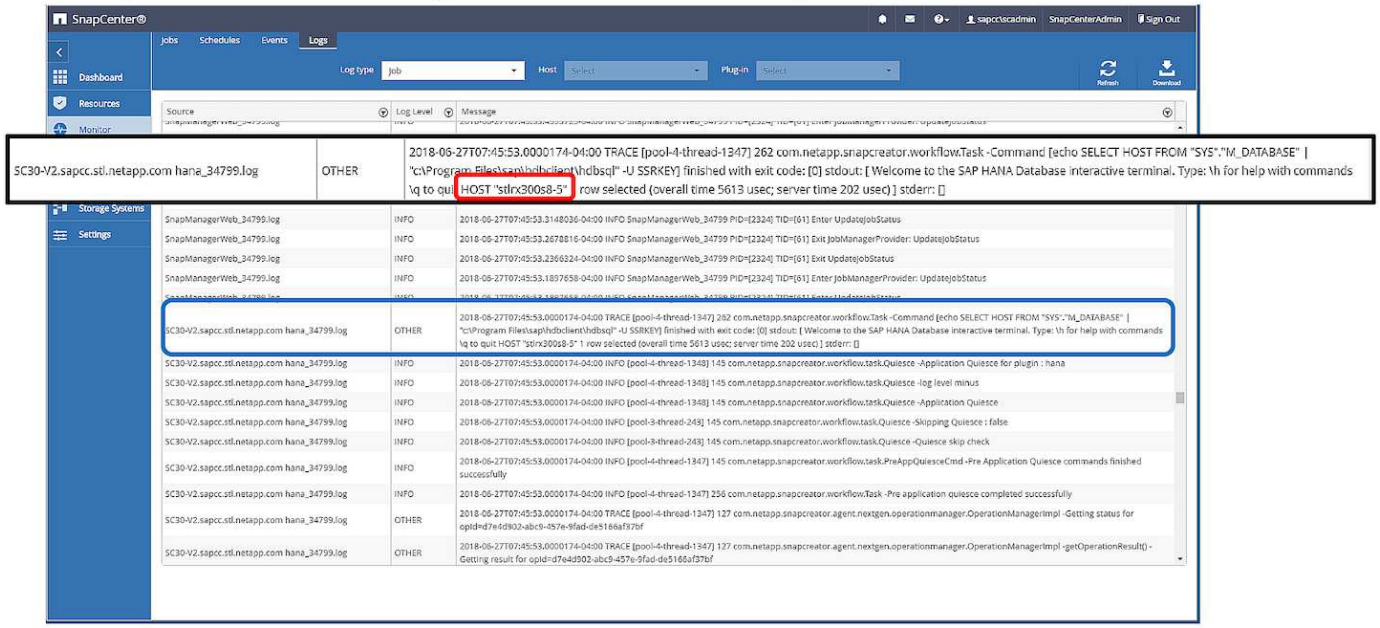
Le operazioni di backup vengono ora eseguite come di consueto. La gestione dei backup dei dati e dei log viene eseguita indipendentemente dall'host SAP HANA primario o secondario.

I log dei processi di backup includono l'output dell'istruzione SQL, che consente di identificare l'host SAP HANA in cui è stato creato il backup.

La figura seguente mostra il log del processo di backup con l'host 1 come host primario.

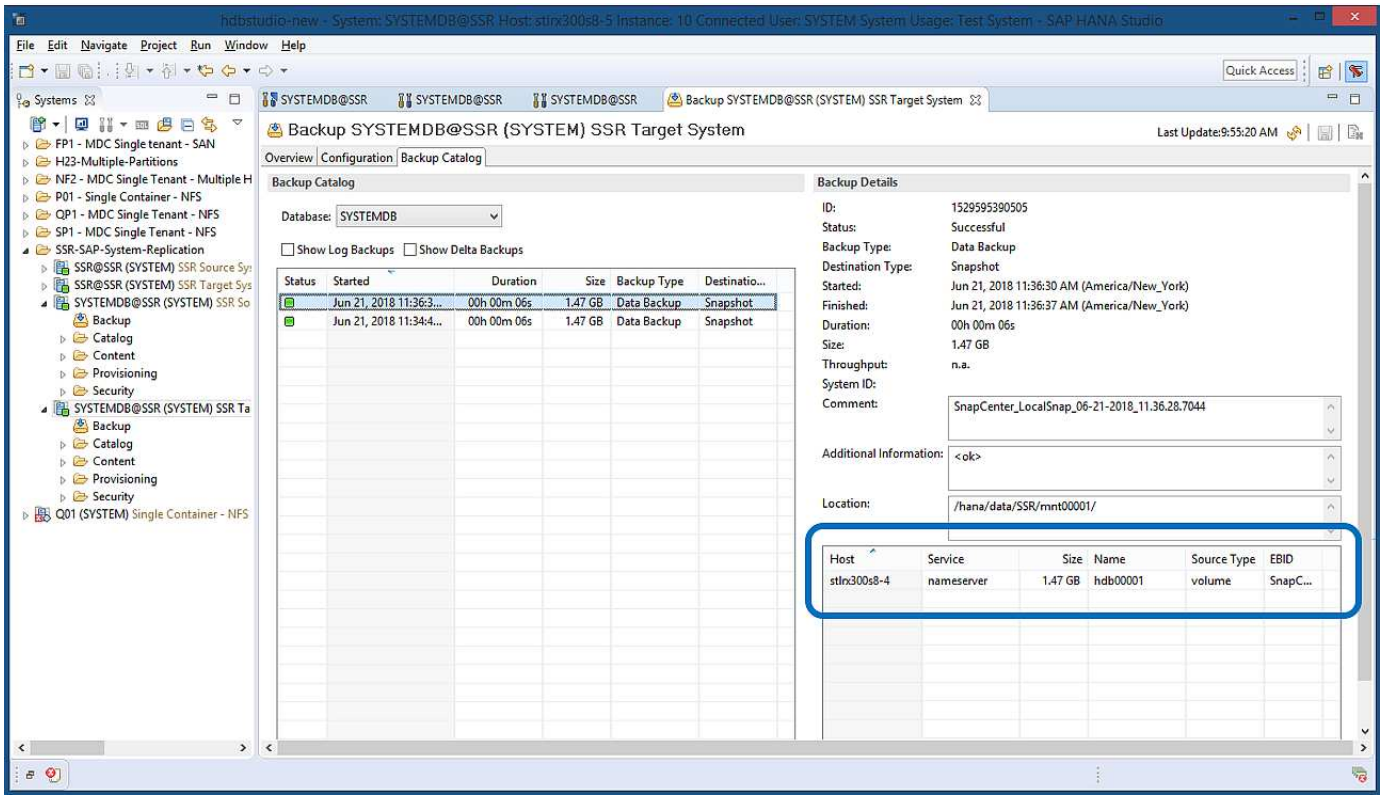


Questa figura mostra il log del processo di backup con l'host 2 come host primario.



La figura seguente mostra il catalogo di backup SAP HANA in SAP HANA Studio. Quando il database SAP HANA è online, l'host SAP HANA in cui è stato creato il backup è visibile in SAP HANA Studio.

Il catalogo di backup SAP HANA sul file system, utilizzato durante un'operazione di ripristino e ripristino, non include il nome host in cui è stato creato il backup. L'unico modo per identificare l'host quando il database è inattivo consiste nel combinare le voci del catalogo di backup con `backup.log` File di entrambi gli host SAP HANA.



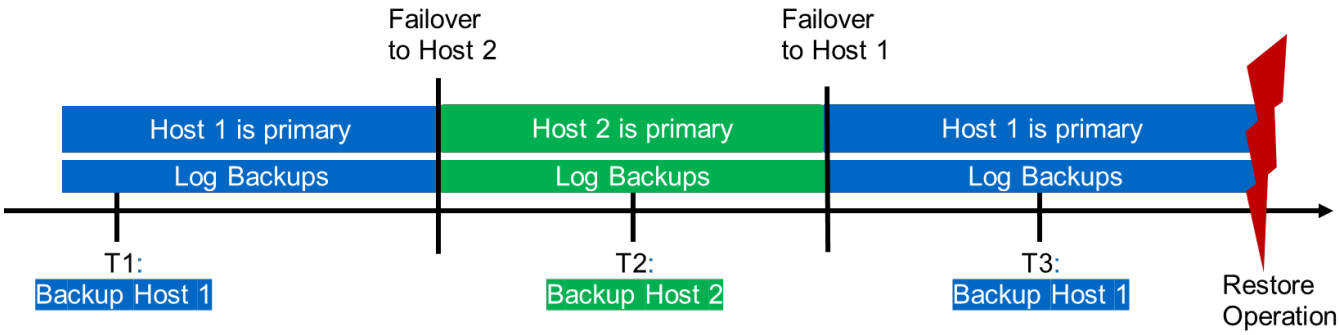
Ripristino e ripristino

Come discusso in precedenza, è necessario essere in grado di identificare la posizione in cui è stato creato il backup selezionato per definire l'operazione di ripristino richiesta. Se il database SAP HANA è ancora online, è possibile utilizzare SAP HANA Studio per identificare l'host in cui è stato creato il backup. Se il database non è in linea, le informazioni sono disponibili solo nel log del processo di backup di SnapCenter.

La figura seguente illustra le diverse operazioni di ripristino a seconda del backup selezionato.

Se è necessario eseguire un'operazione di ripristino dopo l'indicazione di data e ora T3 e l'host 1 è il principale, è possibile ripristinare il backup creato in T1 o T3 utilizzando SnapCenter. Questi backup Snapshot sono disponibili nel volume di storage collegato all'host 1.

Se è necessario eseguire il ripristino utilizzando il backup creato nell'host 2 (T2), ovvero una copia Snapshot nel volume di storage dell'host 2, il backup deve essere reso disponibile per l'host 1. È possibile rendere disponibile questo backup creando una copia di NetApp FlexClone dal backup, montando la copia di FlexClone sull'host 1 e copiando i dati nella posizione originale.



Restore Operation With	
Backup T1	SnapCenter
Backup T2	Create FlexClone from „Backup host 2“, mount and copy
Backup T3	SnapCenter

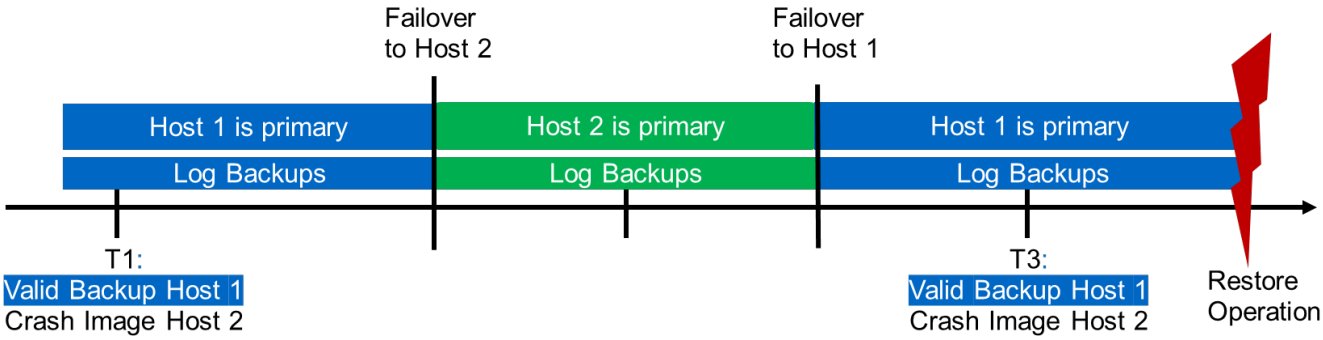
Con una singola configurazione delle risorse SnapCenter, le copie Snapshot vengono create su entrambi i volumi di storage di entrambi gli host di replica del sistema SAP HANA. Solo il backup Snapshot creato nel volume di storage dell'host SAP HANA primario è valido per il forward recovery. La copia Snapshot creata nel volume di storage dell'host SAP HANA secondario è un'immagine di crash che non può essere utilizzata per il forward recovery.

Un'operazione di ripristino con SnapCenter può essere eseguita in due modi diversi:

- Ripristinare solo il backup valido
- Ripristinare la risorsa completa, incluso il backup valido e l'immagine del crash.le sezioni seguenti illustrano in dettaglio le due diverse operazioni di ripristino.

Un'operazione di ripristino da un backup creato nell'altro host è descritta nella sezione "Ripristino e ripristino da un backup creato sull'altro host".

La figura seguente illustra le operazioni di ripristino con una singola configurazione delle risorse SnapCenter.

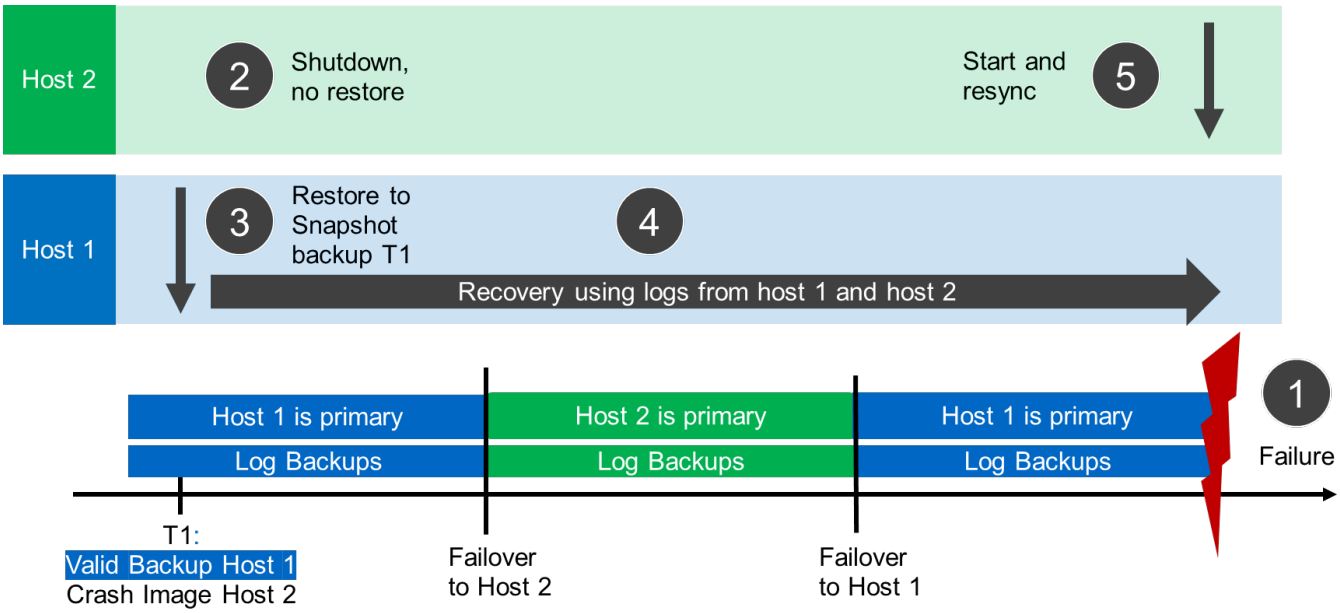


Ripristino SnapCenter solo del backup valido

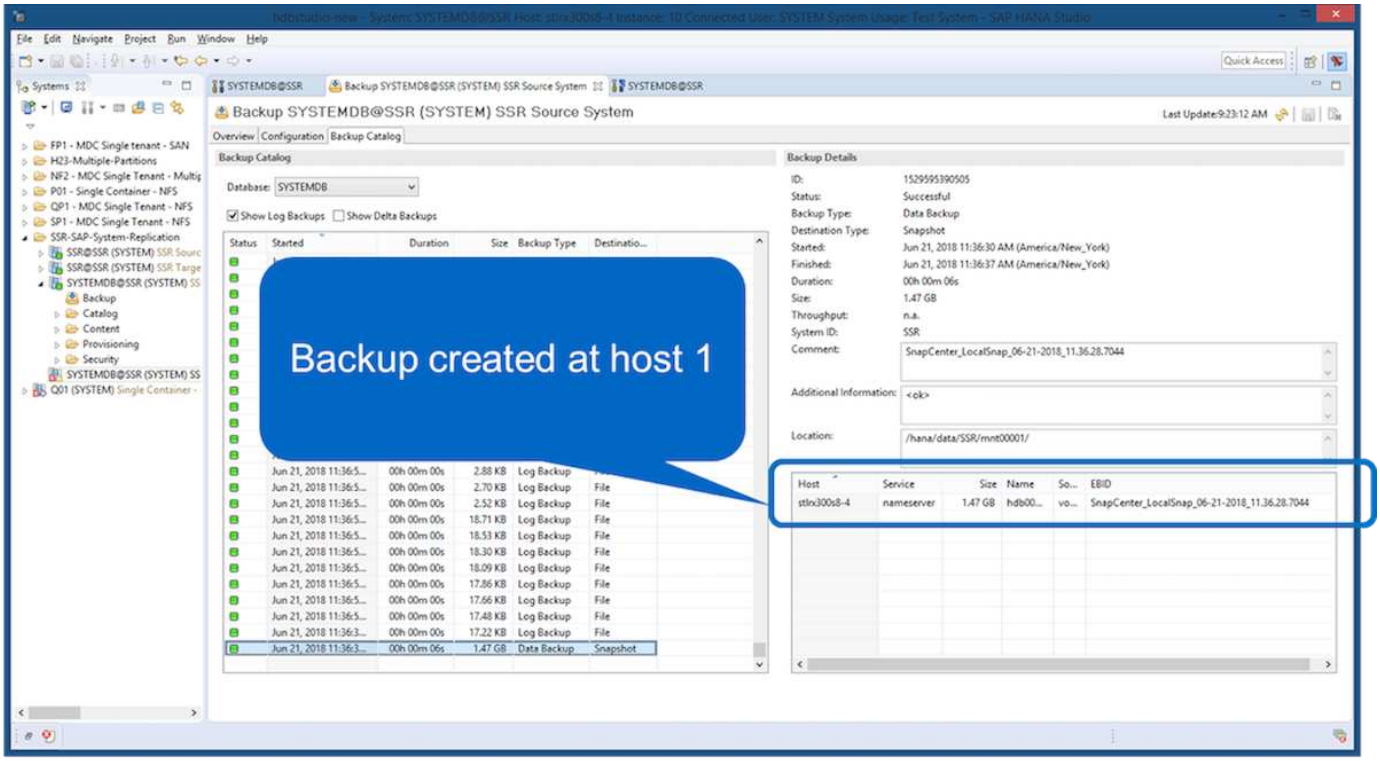
La figura seguente mostra una panoramica dello scenario di ripristino e ripristino descritto in questa sezione.

È stato creato un backup in T1 sull'host 1. È stato eseguito un failover sull'host 2. Dopo un certo punto di tempo, è stato eseguito un altro failover verso l'host 1. Al momento attuale, l'host 1 è l'host primario.

1. Si è verificato un errore ed è necessario ripristinare il backup creato in T1 sull'host 1.
2. L'host secondario (host 2) viene arrestato, ma non viene eseguita alcuna operazione di ripristino.
3. Il volume di storage dell'host 1 viene ripristinato nel backup creato in T1.
4. Viene eseguito un forward recovery con i log degli host 1 e 2.
5. Viene avviato l'host 2 e viene avviata automaticamente una risincronizzazione della replica di sistema dell'host 2.



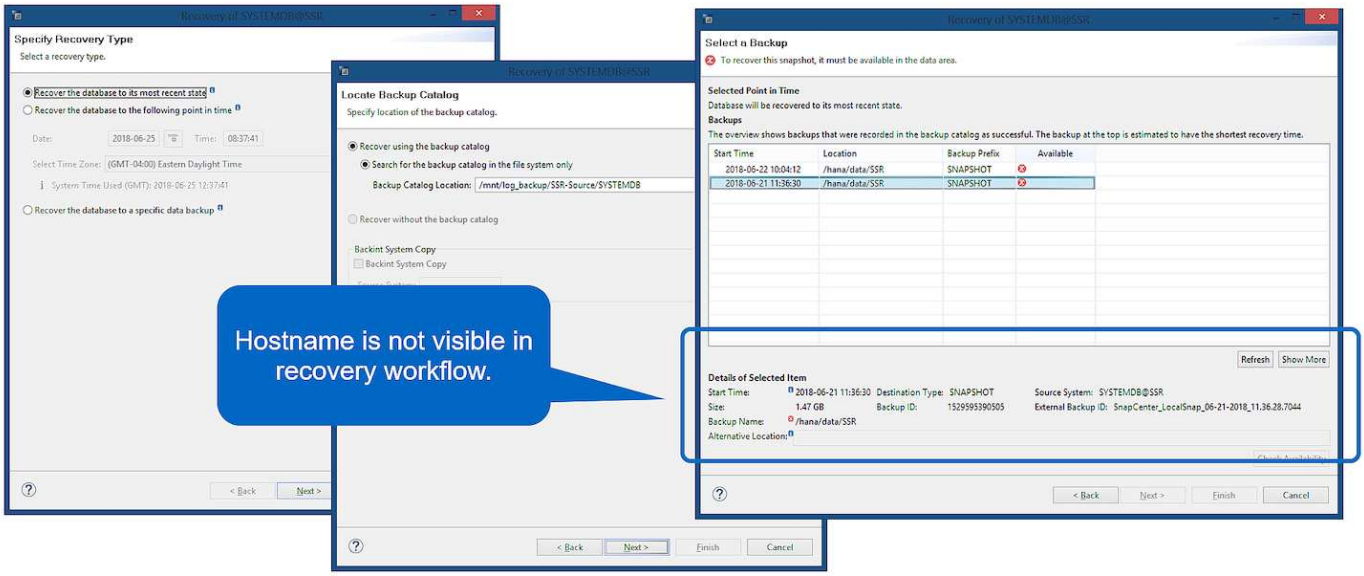
La figura seguente mostra il catalogo di backup SAP HANA in SAP HANA Studio. Il backup evidenziato mostra il backup creato in T1 sull'host 1.



25

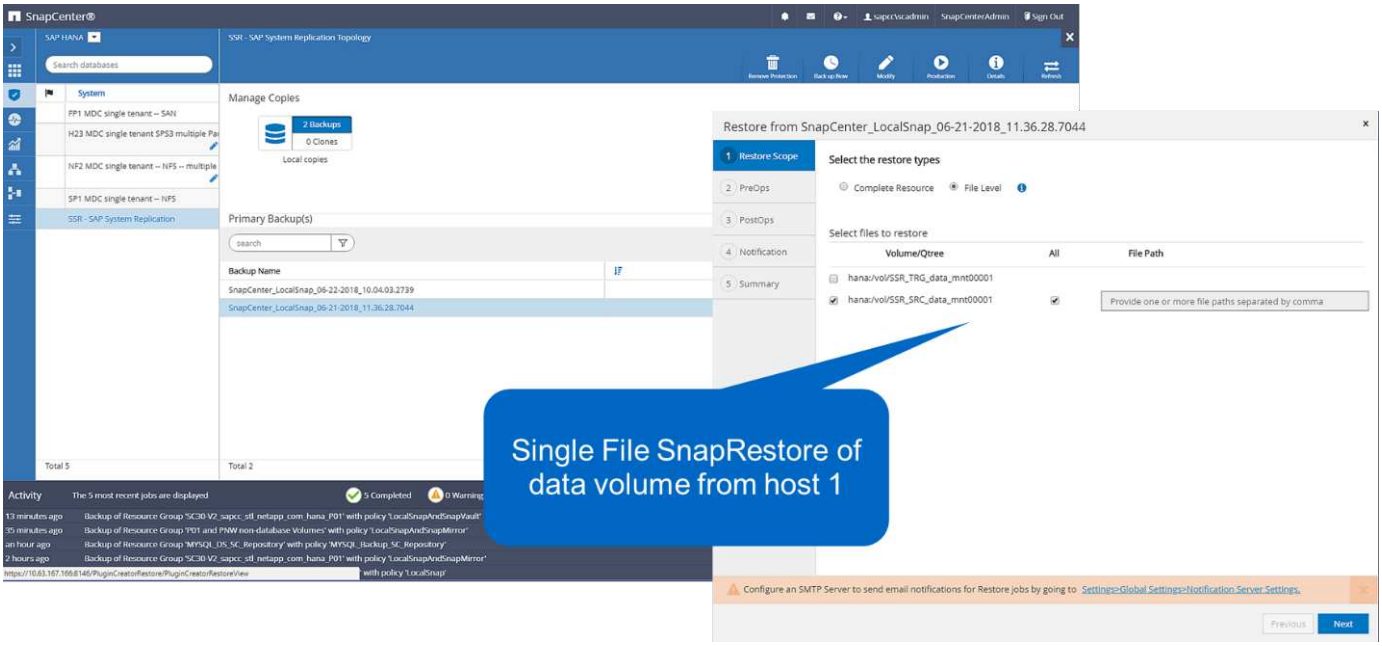
Viene avviata un'operazione di ripristino e ripristino in SAP HANA Studio. Come mostrato nella figura seguente, il nome dell'host in cui è stato creato il backup non è visibile nel flusso di lavoro di ripristino e ripristino.

Nel nostro scenario di test, siamo stati in grado di identificare il backup corretto (il backup creato nell'host 1) in SAP HANA Studio quando il database era ancora online. Se il database non è disponibile, controllare il log del processo di backup di SnapCenter per identificare il backup corretto.

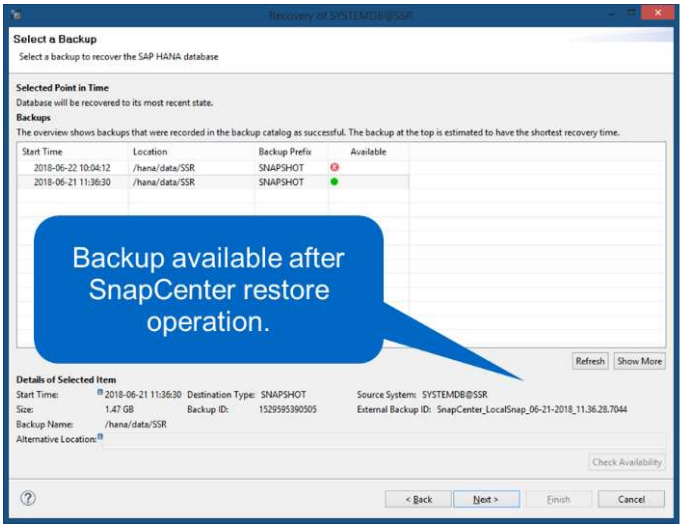


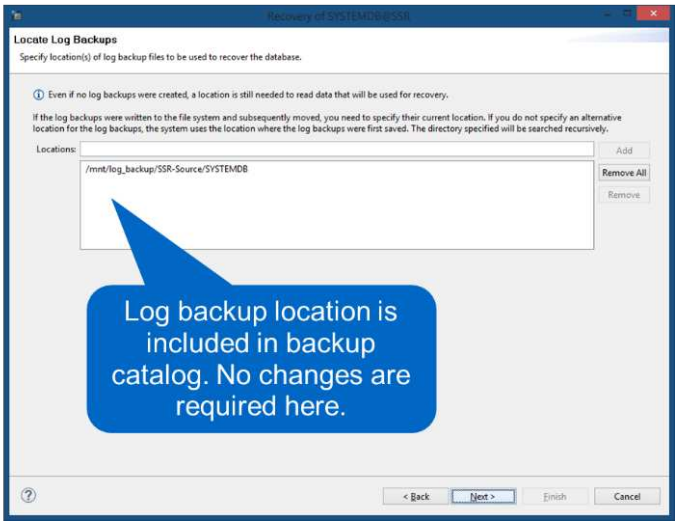
In SnapCenter, viene selezionato il backup e viene eseguita un'operazione di ripristino a livello di file. Nella

schermata di ripristino a livello di file, viene selezionato solo il volume host 1 in modo che venga ripristinato solo il backup valido.



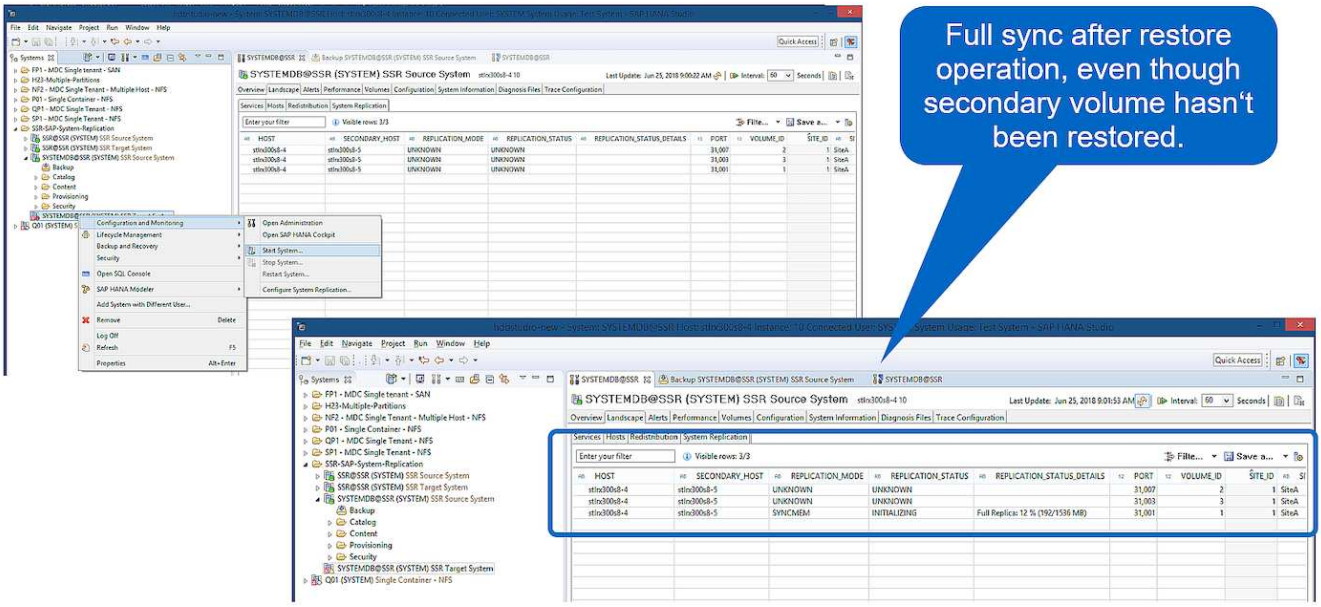
Dopo l'operazione di ripristino, il backup viene evidenziato in verde in SAP HANA Studio. Non è necessario inserire un'ulteriore posizione di backup del log, in quanto il percorso del file di backup del log degli host 1 e 2 è incluso nel catalogo di backup.





Al termine del forward recovery, viene avviato l'host secondario (host 2) e viene avviata la risincronizzazione della replica del sistema SAP HANA.

Anche se l'host secondario è aggiornato (non è stata eseguita alcuna operazione di ripristino per l'host 2), SAP HANA esegue una replica completa di tutti i dati. Questo comportamento è standard dopo un'operazione di ripristino e recovery con SAP HANA System Replication.

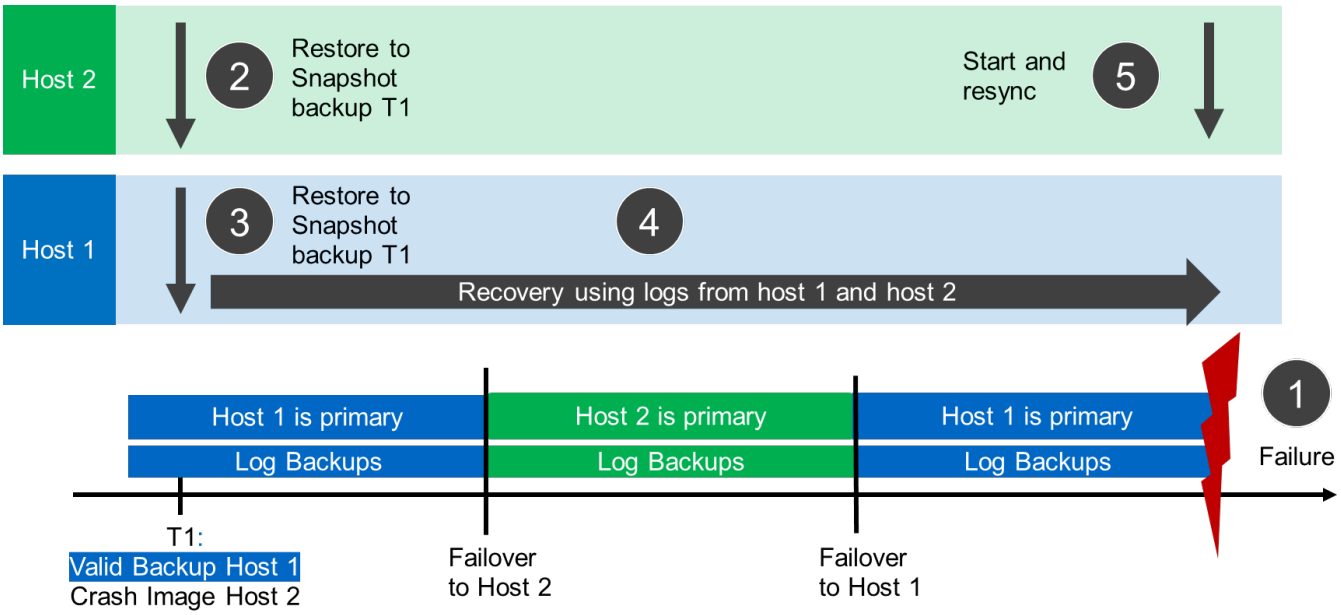


Ripristino SnapCenter di un backup valido e di un'immagine di arresto anomalo

La figura seguente mostra una panoramica dello scenario di ripristino e ripristino descritto in questa sezione.

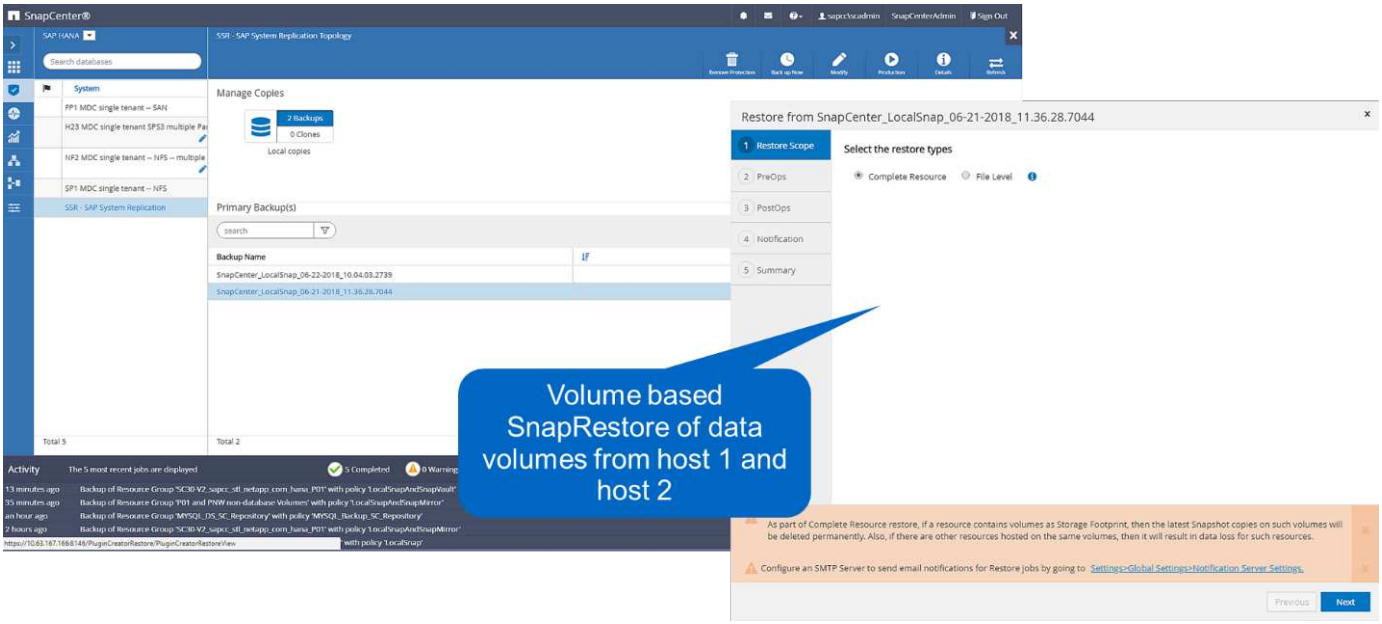
È stato creato un backup in T1 sull'host 1. È stato eseguito un failover sull'host 2. Dopo un certo punto di tempo, è stato eseguito un altro failover verso l'host 1. Al momento attuale, l'host 1 è l'host primario.

1. Si è verificato un errore ed è necessario ripristinare il backup creato in T1 sull'host 1.
2. L'host secondario (host 2) viene arrestato e l'immagine del crash T1 viene ripristinata.
3. Il volume di storage dell'host 1 viene ripristinato nel backup creato in T1.
4. Viene eseguito un forward recovery con i log degli host 1 e 2.
5. Viene avviato l'host 2 e viene avviata automaticamente una risincronizzazione della replica di sistema dell'host 2.

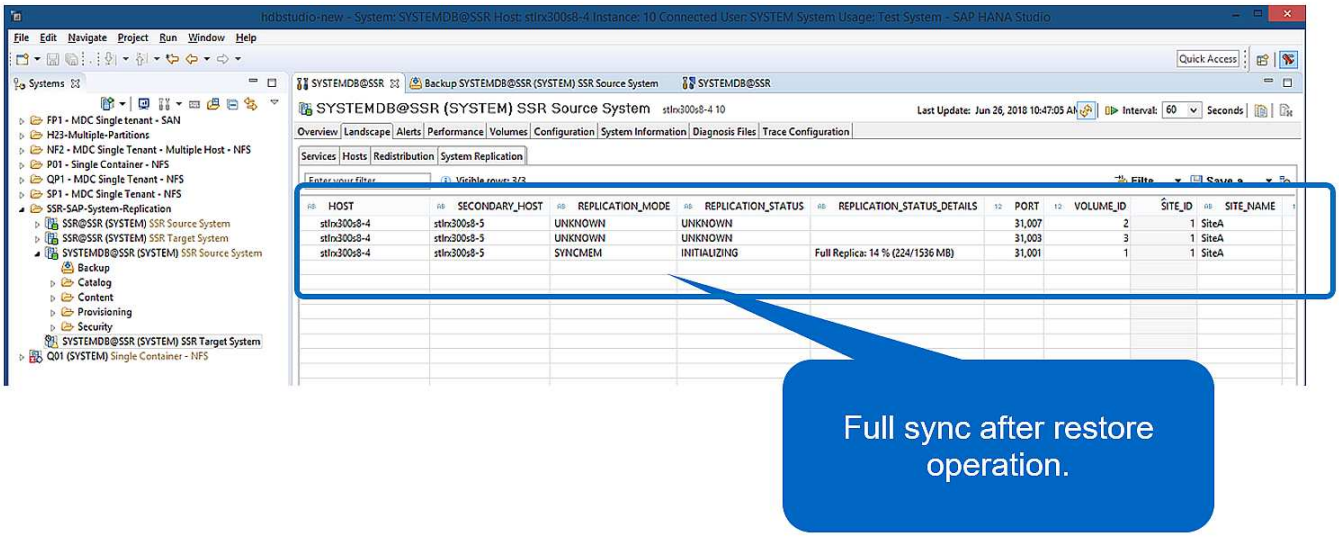


L'operazione di ripristino e ripristino con SAP HANA Studio è identica alla procedura descritta nella sezione "Ripristino SnapCenter solo del backup valido".

Per eseguire l'operazione di ripristino, selezionare completa risorsa in SnapCenter. I volumi di entrambi gli host vengono ripristinati.



Una volta completato il forward recovery, viene avviato l'host secondario (host 2) e viene avviata la risincronizzazione della replica del sistema SAP HANA. Viene eseguita la replica completa di tutti i dati.



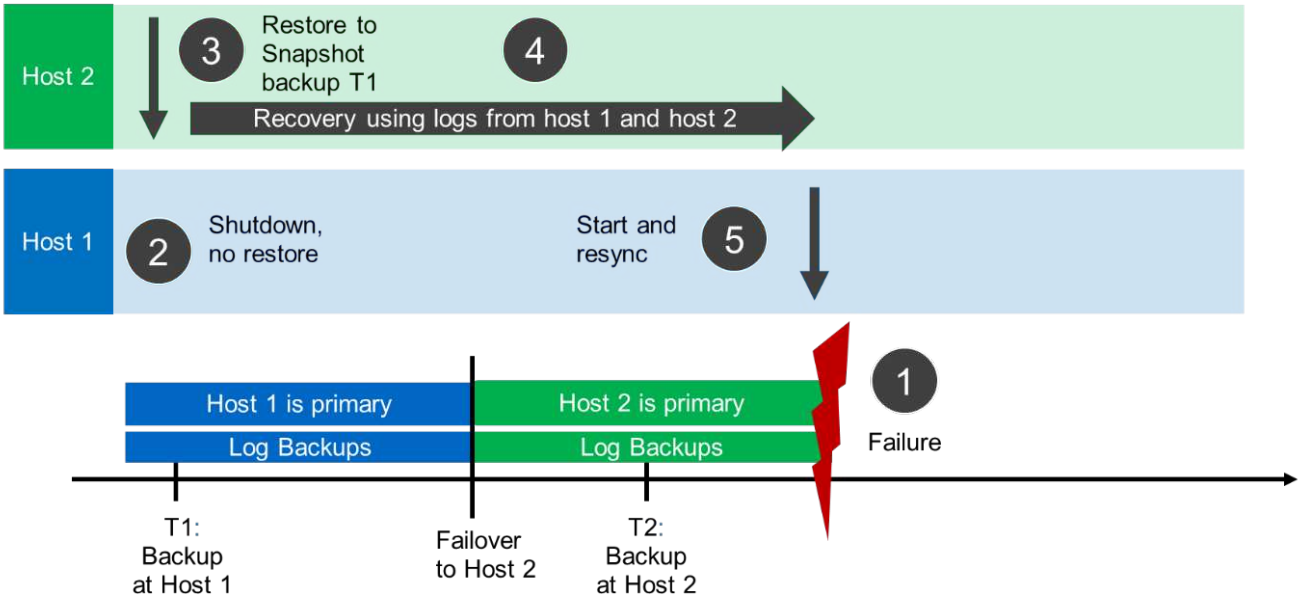
Ripristino e ripristino da un backup creato sull'altro host

Un'operazione di ripristino da un backup creato sull'altro host SAP HANA è uno scenario valido per entrambe le opzioni di configurazione di SnapCenter.

La figura seguente mostra una panoramica dello scenario di ripristino e ripristino descritto in questa sezione.

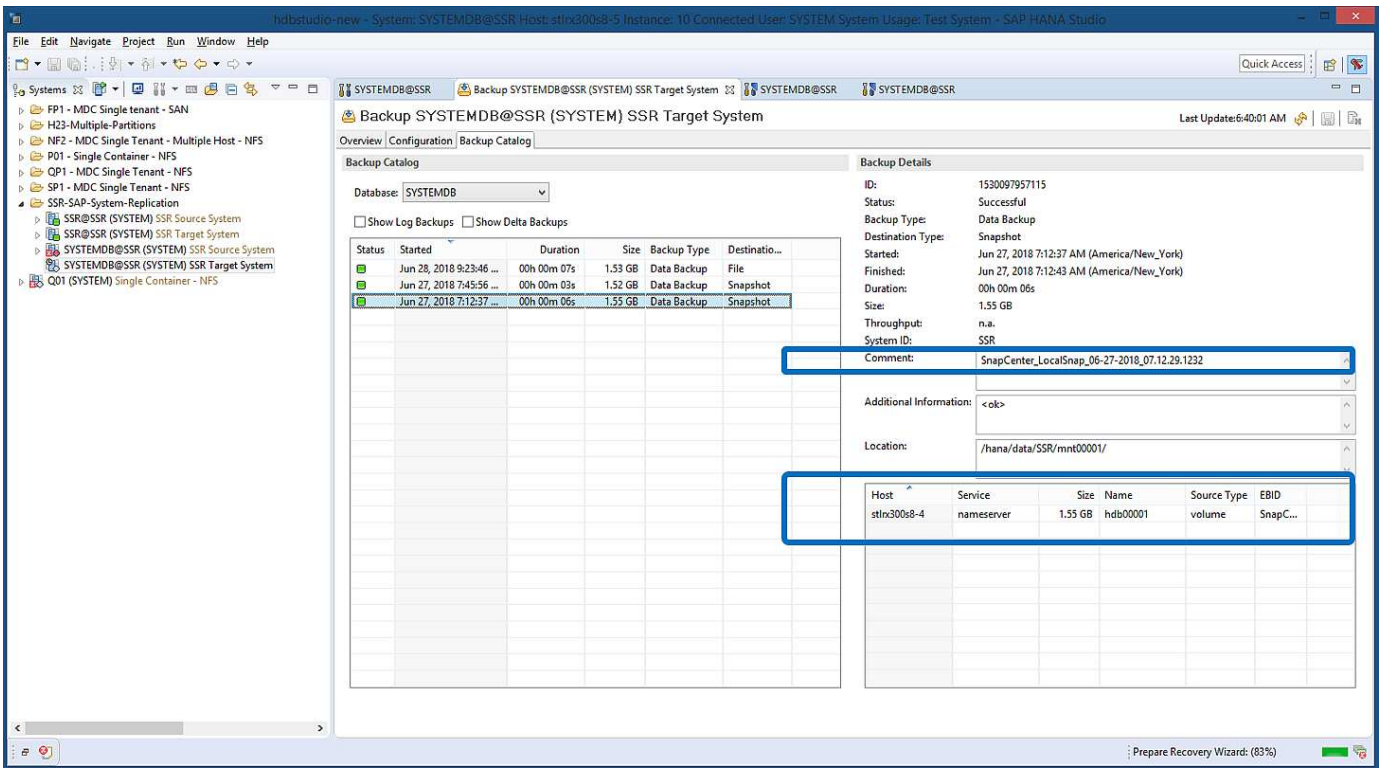
È stato creato un backup in T1 sull'host 1. È stato eseguito un failover sull'host 2. Al momento attuale, l'host 2 è l'host primario.

1. Si è verificato un errore ed è necessario ripristinare il backup creato in T1 sull'host 1.
2. L'host primario (host 1) viene arrestato.
3. I dati di backup T1 dell'host 1 vengono ripristinati nell'host 2.
4. Il ripristino in avanti viene eseguito utilizzando i registri dell'host 1 e dell'host 2.
5. Viene avviato l'host 1 e viene avviata automaticamente una risincronizzazione della replica di sistema dell'host 1.



31

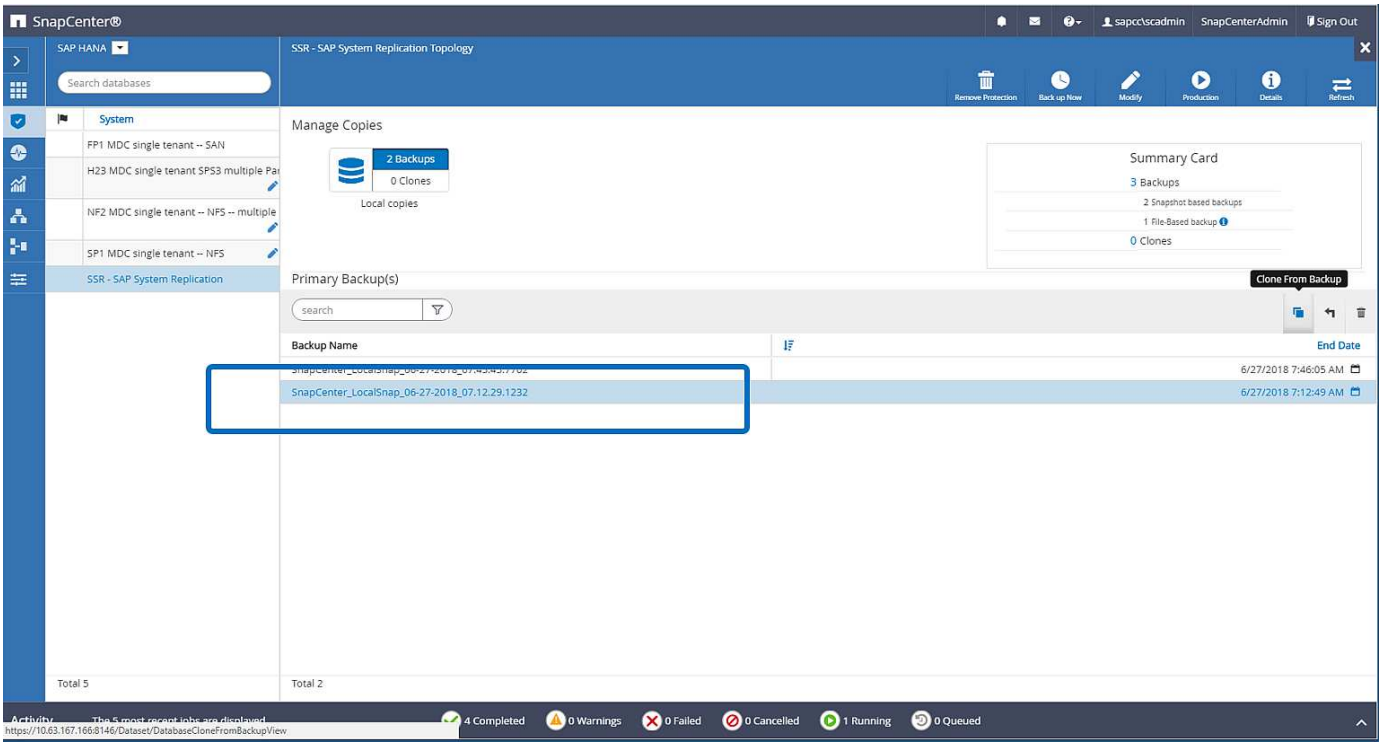
La figura seguente mostra il catalogo di backup SAP HANA ed evidenzia il backup, creato sull'host 1, utilizzato per l'operazione di ripristino.



L’operazione di ripristino prevede i seguenti passaggi:

1. Creare un clone dal backup creato sull’host 1.
2. Montare il volume clonato sull’host 2.
3. Copiare i dati dal volume clonato nella posizione originale.

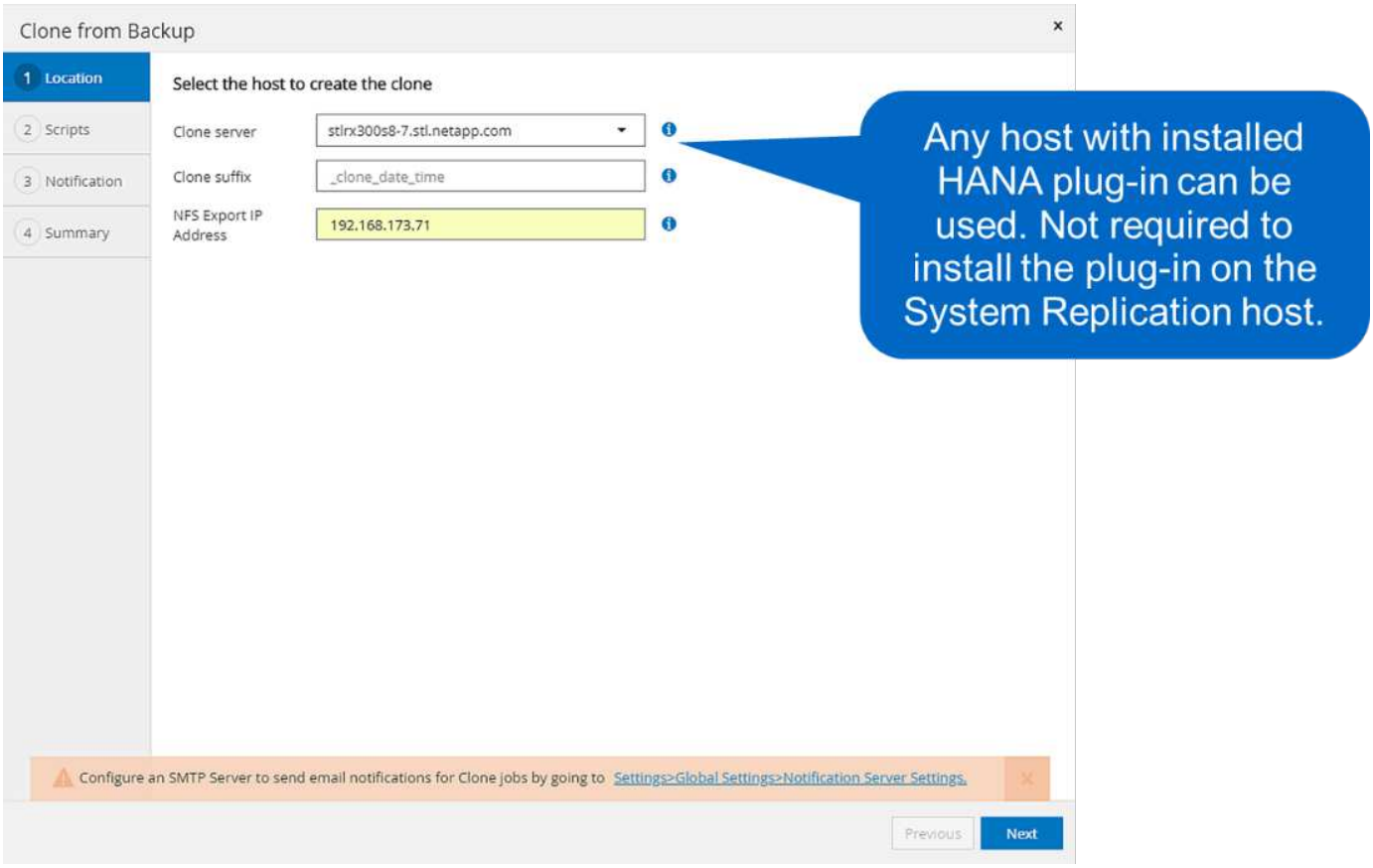
In SnapCenter, viene selezionato il backup e viene avviata l’operazione di clonazione.



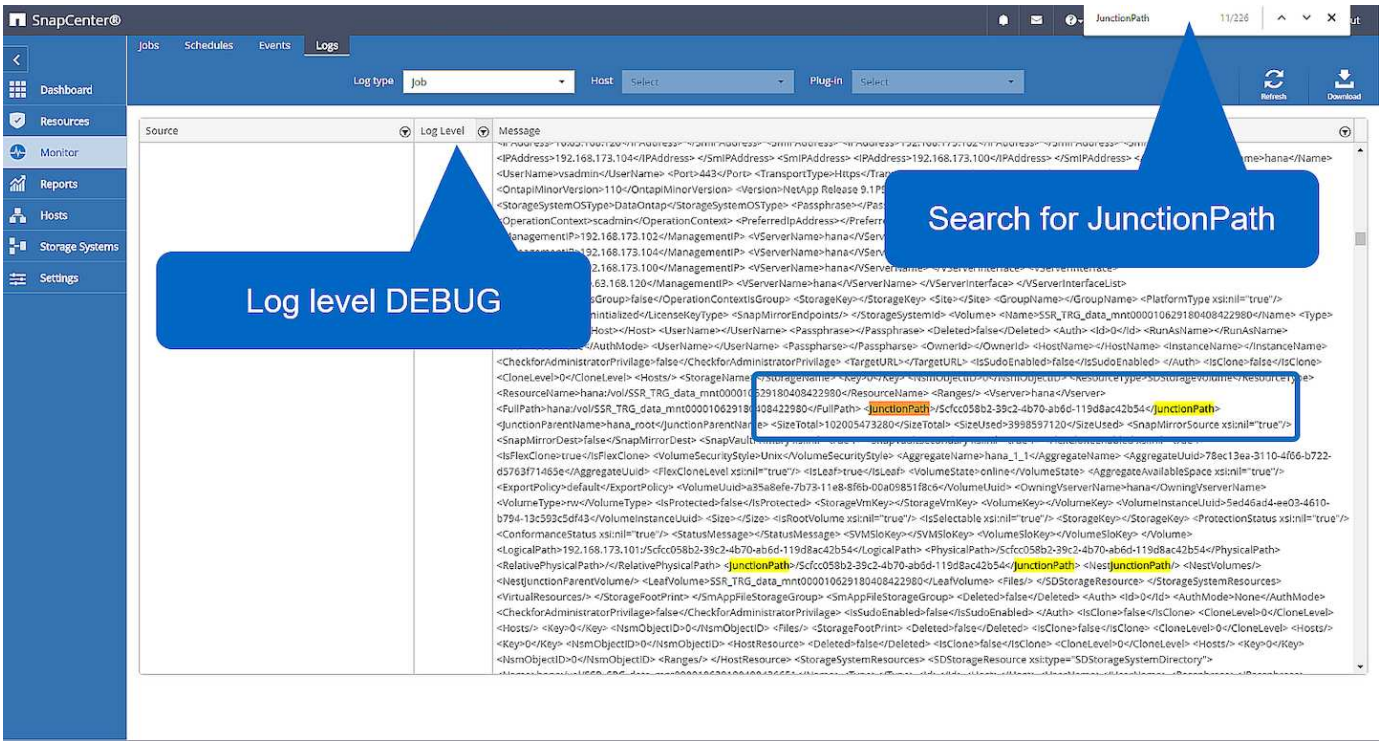
È necessario fornire il server clone e l’indirizzo IP di esportazione NFS.

> In una configurazione SnapCenter a risorsa singola, il plug-in SAP HANA non viene installato sull’host del database. Per eseguire il flusso di lavoro del clone di SnapCenter, è possibile utilizzare come server clone qualsiasi host con un plug-in HANA installato.

In una configurazione SnapCenter con risorse separate, l’host del database HANA viene selezionato come server clone e viene utilizzato uno script di montaggio per montare il clone sull’host di destinazione.



Per determinare il percorso di giunzione richiesto per montare il volume clonato, controllare il log del lavoro di clonazione, come mostrato nella figura seguente.



È ora possibile montare il volume clonato.

```
stlrx300s8-5:/mnt/tmp # mount 192.168.173.101:/Scc373da37-00ff-4694-b1e1-
8153dbd46caf /mnt/tmp
```

Il volume clonato contiene i dati del database HANA.

```
stlrx300s8-5:/mnt/tmp/# ls -al
drwxr-x--x 2 ssradm sapsys 4096 Jun 27 11:12 hdb00001
drwx------ 2 ssradm sapsys 4096 Jun 21 09:38 hdb00002.00003
drwx------ 2 ssradm sapsys 4096 Jun 27 11:12 hdb00003.00003
-rw-r--r-- 1 ssradm sapsys   22 Jun 27 11:12 nameserver.lck
```

I dati vengono copiati nella posizione originale.

```
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00001 /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00002.00003/ /hana/data/SSR/mnt00001/
stlrx300s8-5:/mnt/tmp # cp -Rp hdb00003.00003/ /hana/data/SSR/mnt00001/
```

Il ripristino con SAP HANA Studio viene eseguito come descritto nella sezione "Ripristino SnapCenter solo del backup valido".

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti:

- "Backup e ripristino SAP HANA con SnapCenter"
- "Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter"
- Disaster recovery SAP HANA con replica dello storage

  "https://www.netapp.com/us/media/tr-4646.pdf"

Cronologia delle versioni

Cronologia versioni:

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Ottobre 2018	Versione iniziale
Versione 2.0	Gennaio 2022	Aggiornamento per il supporto della replica di sistema HANA di SnapCenter 4.6

Disaster recovery SAP HANA con Azure NetApp Files

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

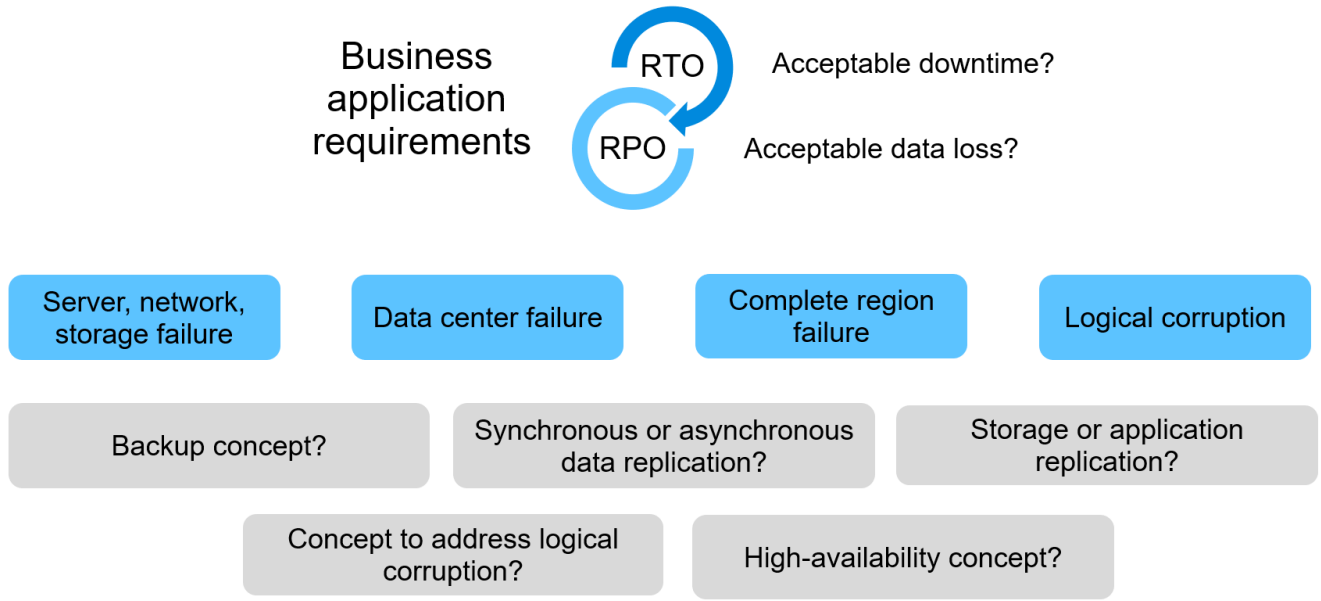
Gli studi hanno dimostrato che il downtime delle applicazioni di business ha un impatto negativo significativo sul business delle aziende.

Autori: Nils Bauer, NetApp Ralf Klahr, Microsoft

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

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

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



Requisiti delle applicazioni di business

Sono disponibili due indicatori chiave per le applicazioni aziendali:

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

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

impatto significativo sulle opzioni tecniche disponibili.

Alta disponibilità

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

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

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

Corruzione logica

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

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

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

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

Backup

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

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

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

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

Replica sincrona o asincrona dei dati

L’RPO determina principalmente il metodo di replica dei dati da utilizzare. Se l’RPO deve essere pari a zero, anche in caso di perdita dello storage primario e di backup, i dati devono essere replicati in modo sincrono. Tuttavia, esistono limiti tecnici per la replica sincrona, ad esempio la distanza tra due aree Azure. Nella maggior parte dei casi, la replica sincrona non è appropriata per distanze superiori a 100 km a causa della latenza, pertanto non è un’opzione per la replica dei dati tra le regioni di Azure.

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

Replica di sistema HANA con o senza precaricamento dei dati

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

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

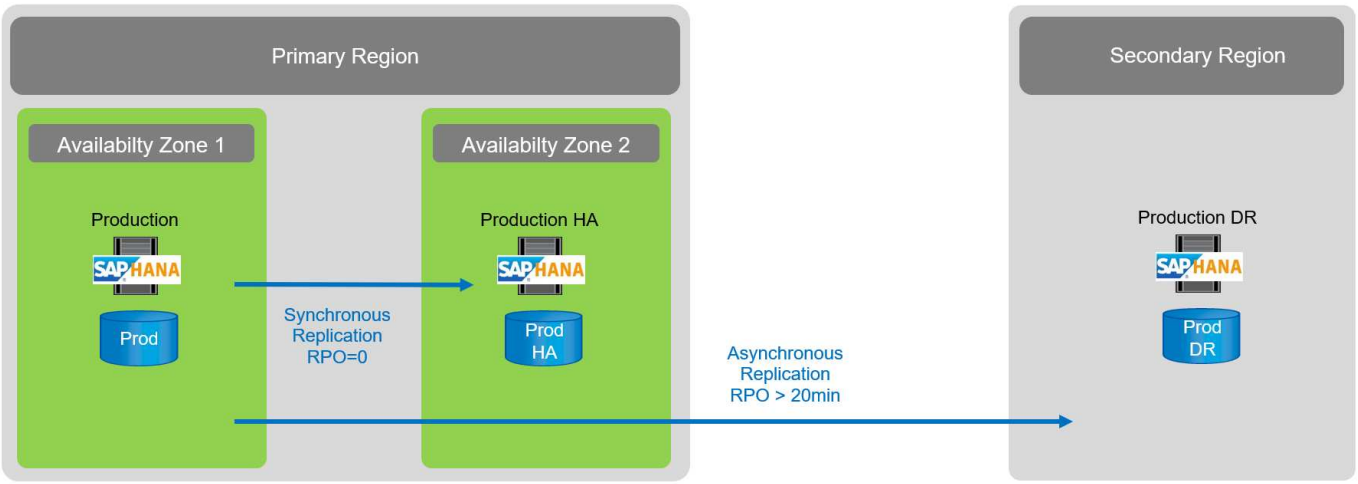
Confronto tra soluzioni di disaster recovery

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

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

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

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



Replica di sistema SAP HANA

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

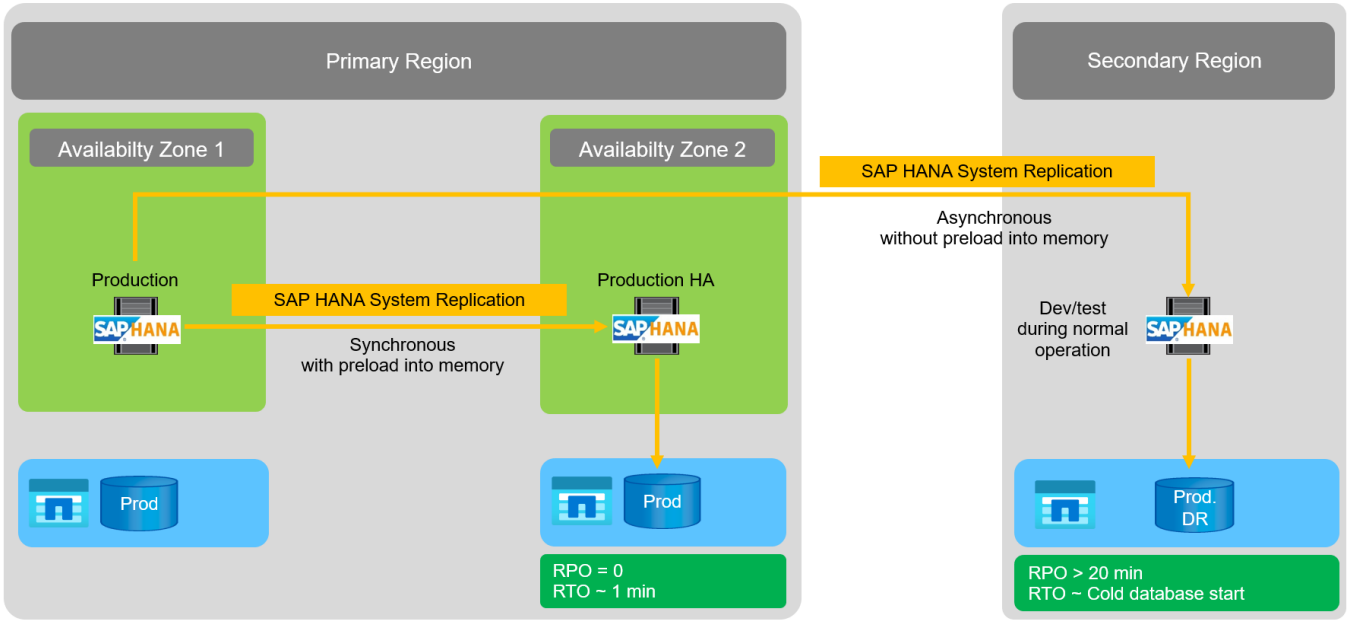
La replica del sistema SAP HANA può essere utilizzata in due modalità:

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

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

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

La seguente figura illustra la replica di sistema SAP HANA.



Replica di sistema SAP HANA con dati precaricati in memoria

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

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

Replica del sistema SAP senza dati precaricati in memoria

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

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

Disaster recovery SAP HANA con replica cross-Region ANF

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

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

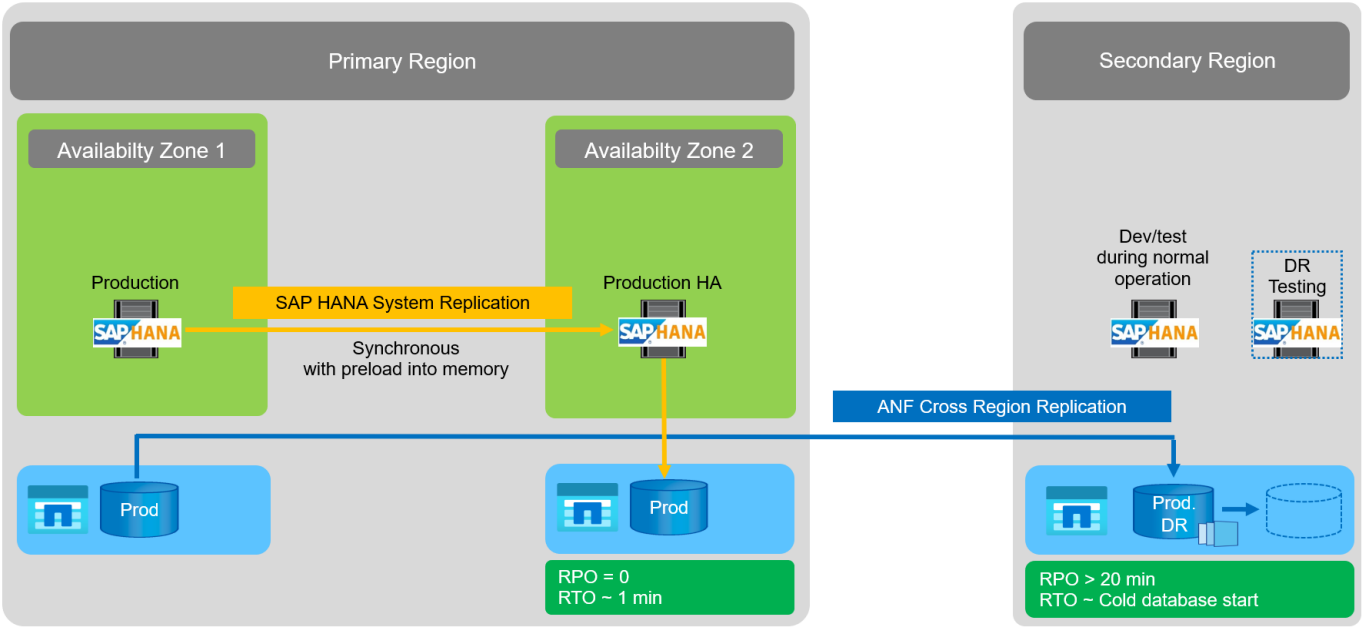
ANF Cross-Region. In questo esempio, il sistema HANA è protetto con la replica del sistema HANA all'interno della regione principale, come descritto nel capitolo precedente. La replica in una regione secondaria viene eseguita utilizzando la replica ANF cross-region. L'RPO è definito dalla pianificazione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

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

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

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

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



Riepilogo delle soluzioni di disaster recovery

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

I risultati principali sono i seguenti:

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

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

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

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

ANF Replication cross-Region con SAP HANA

ANF Replication cross-Region con SAP HANA

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

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

Opzioni di configurazione per la replica interregionale con SAP HANA

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

recovery.

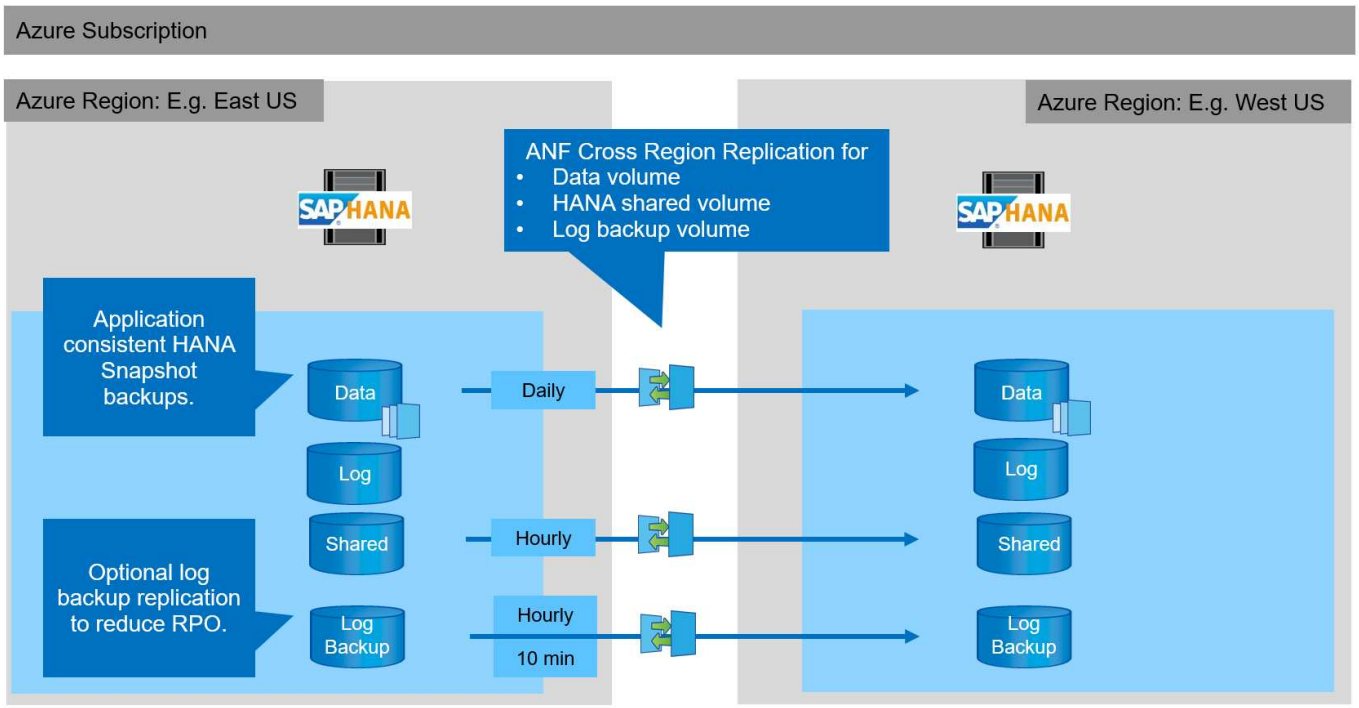
> Il termine "backup del log" utilizzato in questo documento include il backup del log e il backup del catalogo di backup HANA. Il catalogo di backup HANA è necessario per eseguire le operazioni di ripristino in avanti.

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

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

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

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



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

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

Requisiti e Best practice

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

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

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

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

Setup di laboratorio

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

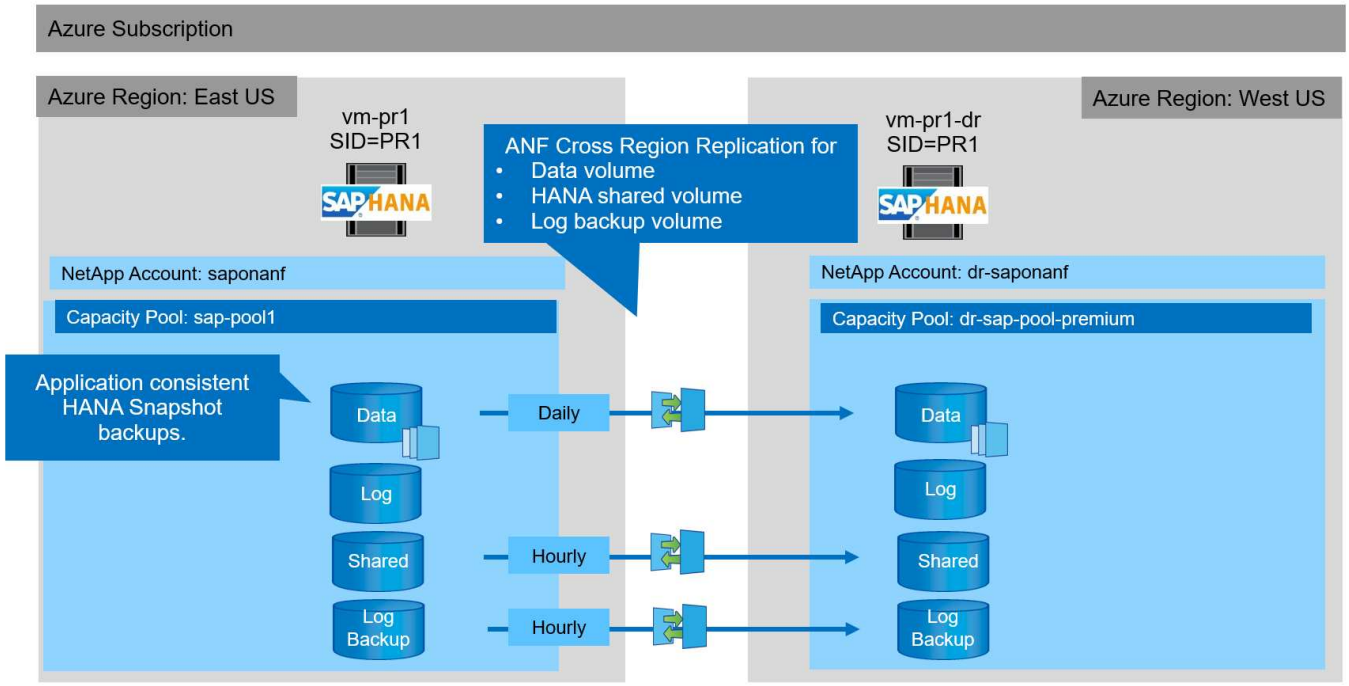
salvataggio e con operazioni di forward recovery.

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

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

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

La seguente figura illustra la configurazione di laboratorio.

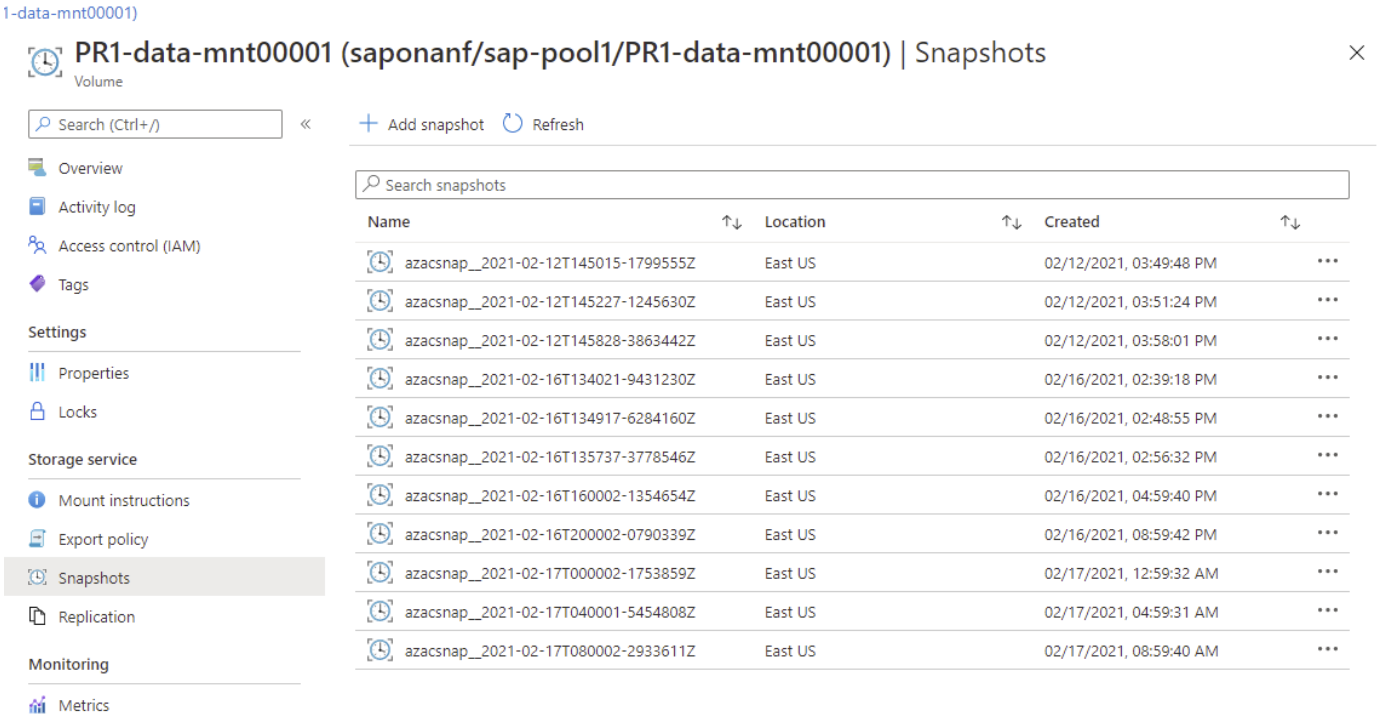


Configurazione del backup Snapshot con AzAcSnap

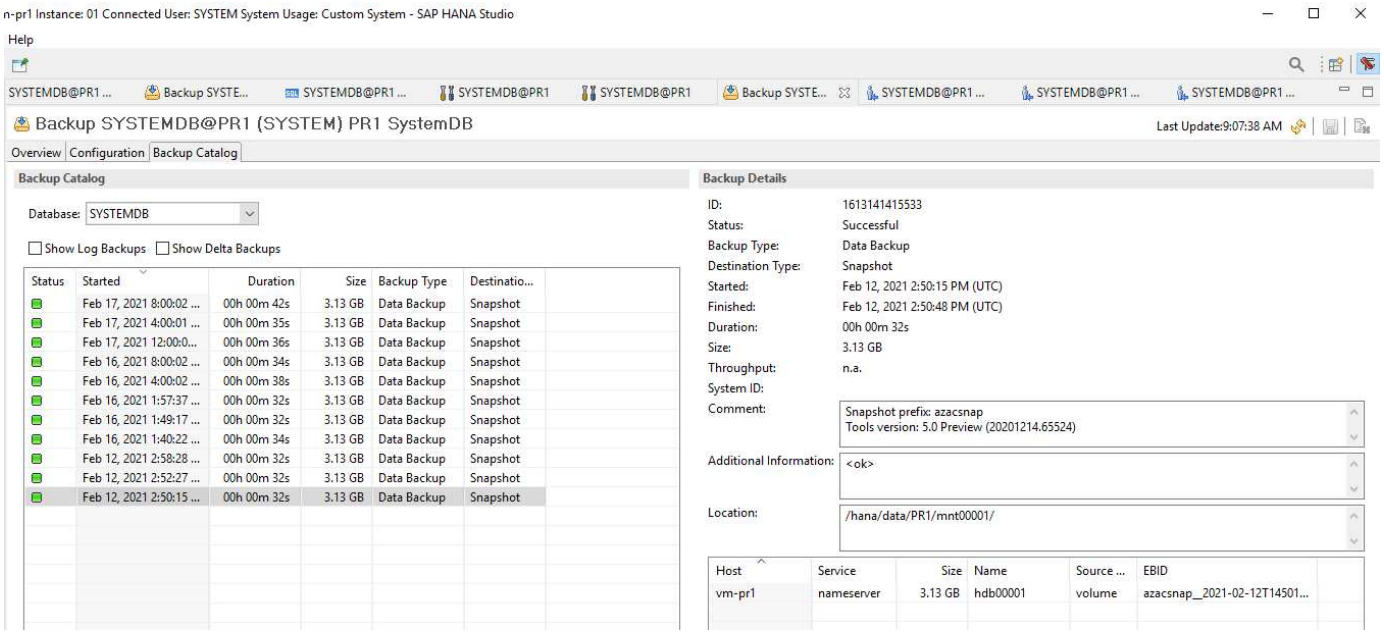
Nel sito principale, AzAcSnap è stato configurato per creare backup Snapshot coerenti con l'applicazione del sistema HANA PR1. Questi backup Snapshot sono disponibili nel volume di dati ANF del sistema PR1 HANA e sono registrati anche nel catalogo di backup SAP HANA, come mostrato nelle due figure seguenti.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

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

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



La figura seguente mostra il catalogo di backup SAP HANA.



Procedura di configurazione per la replica ANF Cross-Region

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

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

ANF.

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

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

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

Per ciascun volume, è necessario eseguire le seguenti operazioni:

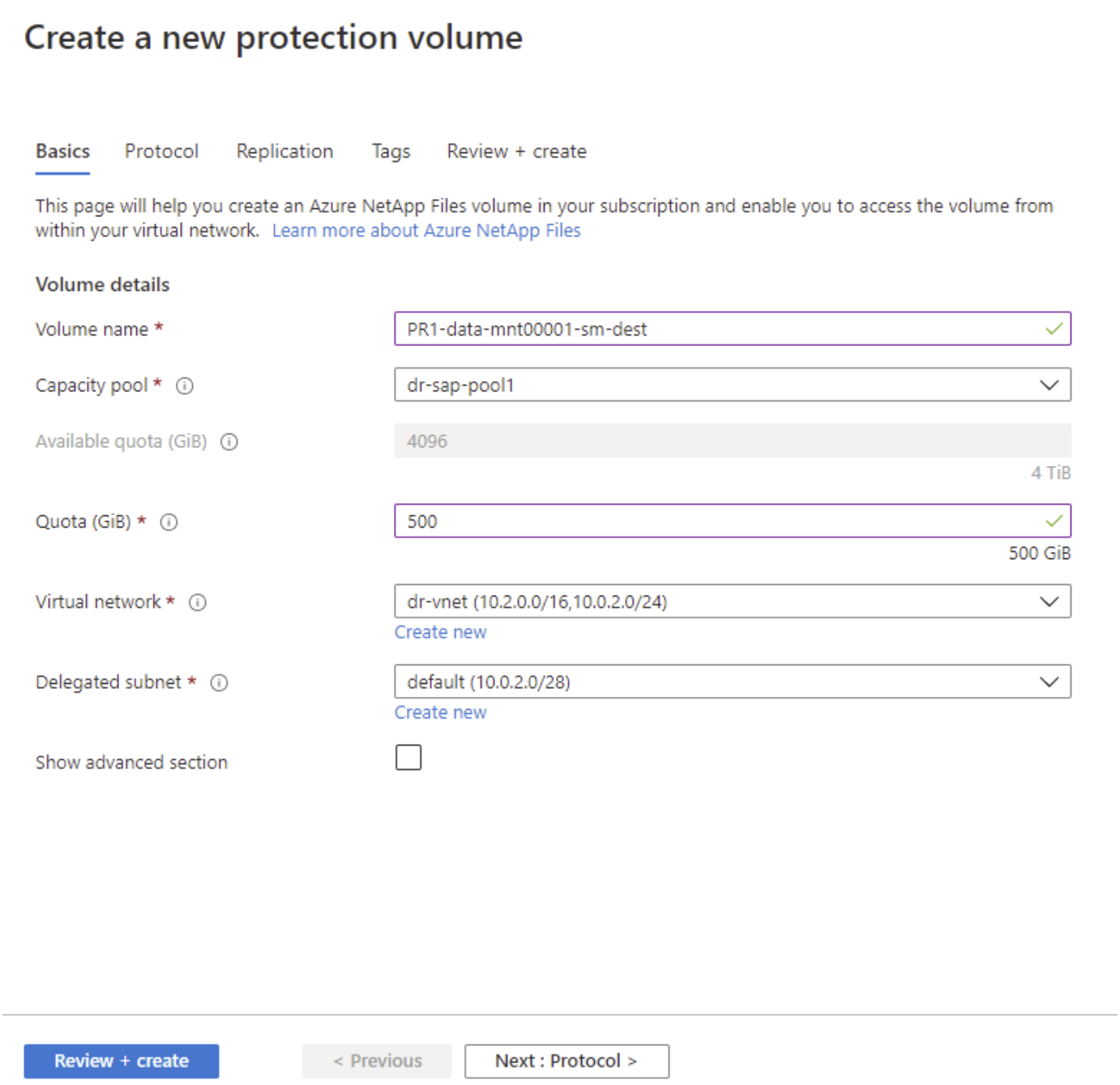
1. Creare un nuovo volume di protezione nel sito DR:
   a. Fornire il nome del volume, il pool di capacità, la quota e le informazioni di rete.
   b. Fornire le informazioni relative al protocollo e all'accesso al volume.
   c. Fornire l'ID del volume di origine e una pianificazione di replica.
   d.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

Le seguenti schermate mostrano in dettaglio i passaggi di configurazione.

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

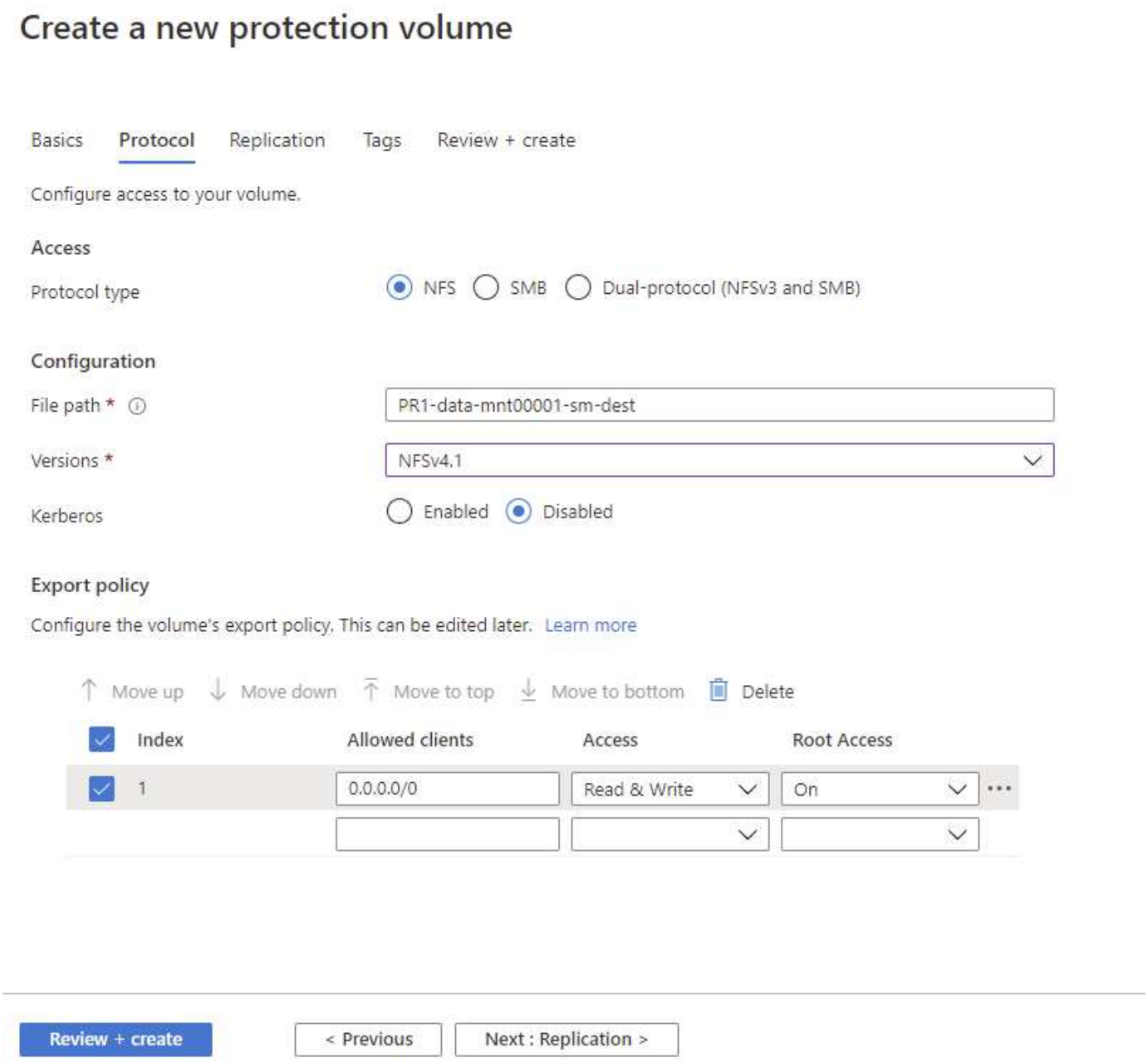
> La quota del volume può essere impostata in base ai requisiti di capacità, poiché le prestazioni del volume non influiscono sul processo di replica. In caso di failover del disaster recovery, la quota deve essere regolata per soddisfare i requisiti di performance reali.

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



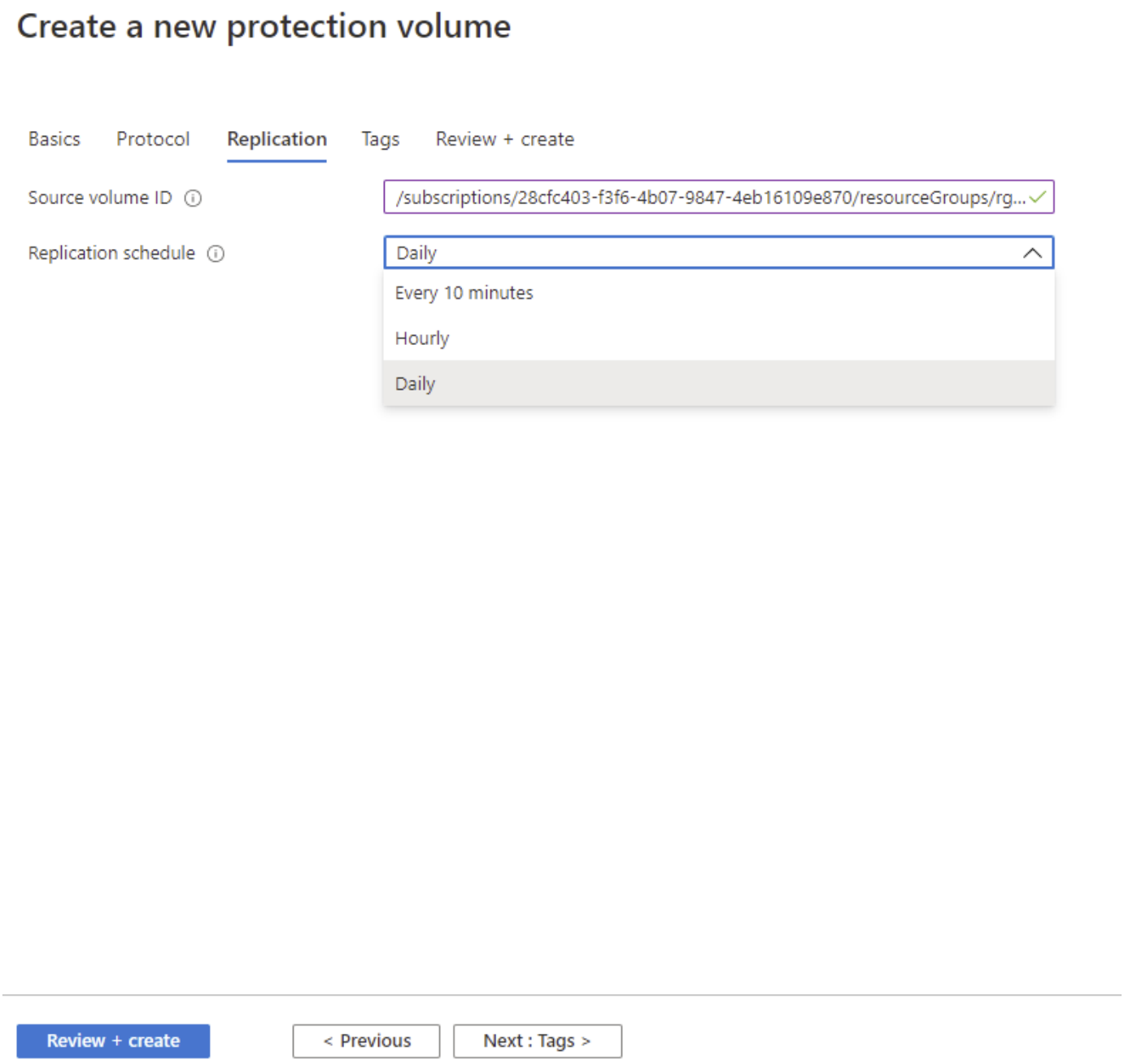
Nella scheda Protocol (protocollo), specificare il protocollo di rete, il percorso di rete e il criterio di esportazione.

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



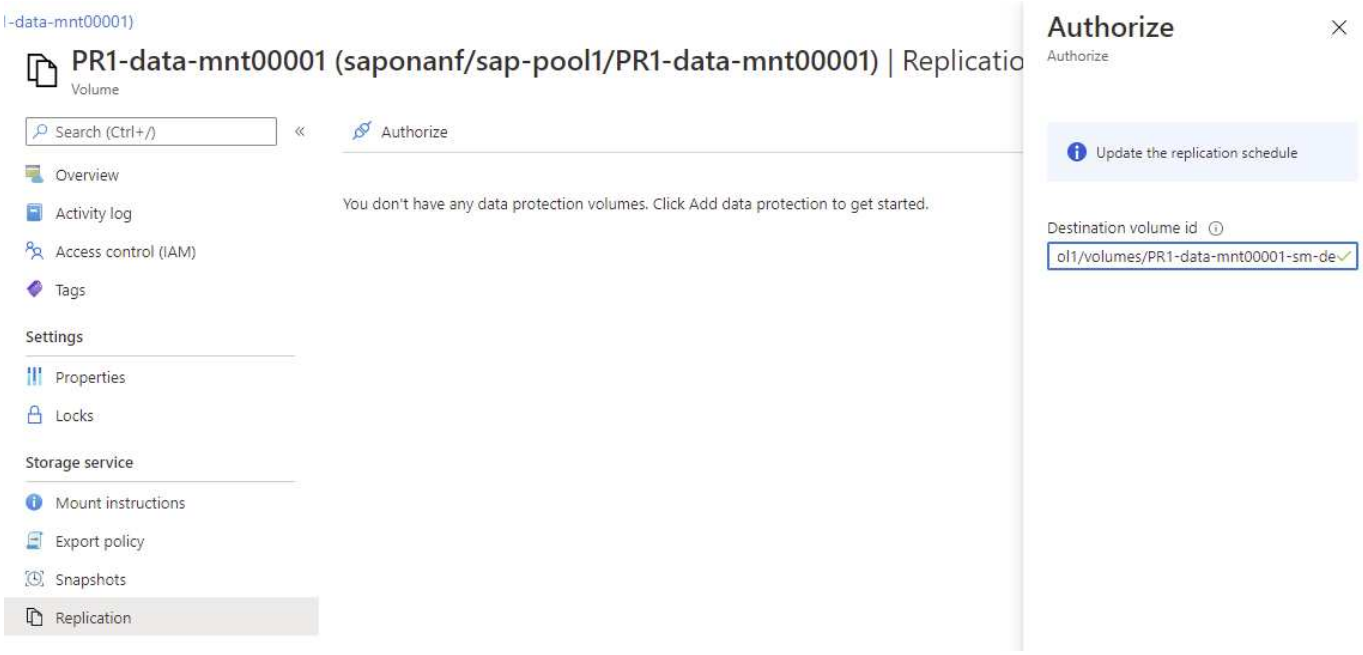
Nella scheda Replication (Replica), è necessario configurare l'ID del volume di origine e la pianificazione della replica. Per la replica dei volumi di dati, abbiamo configurato una pianificazione di replica giornaliera per la nostra configurazione di laboratorio.

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



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

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



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

Monitoraggio della replica ANF tra regioni

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

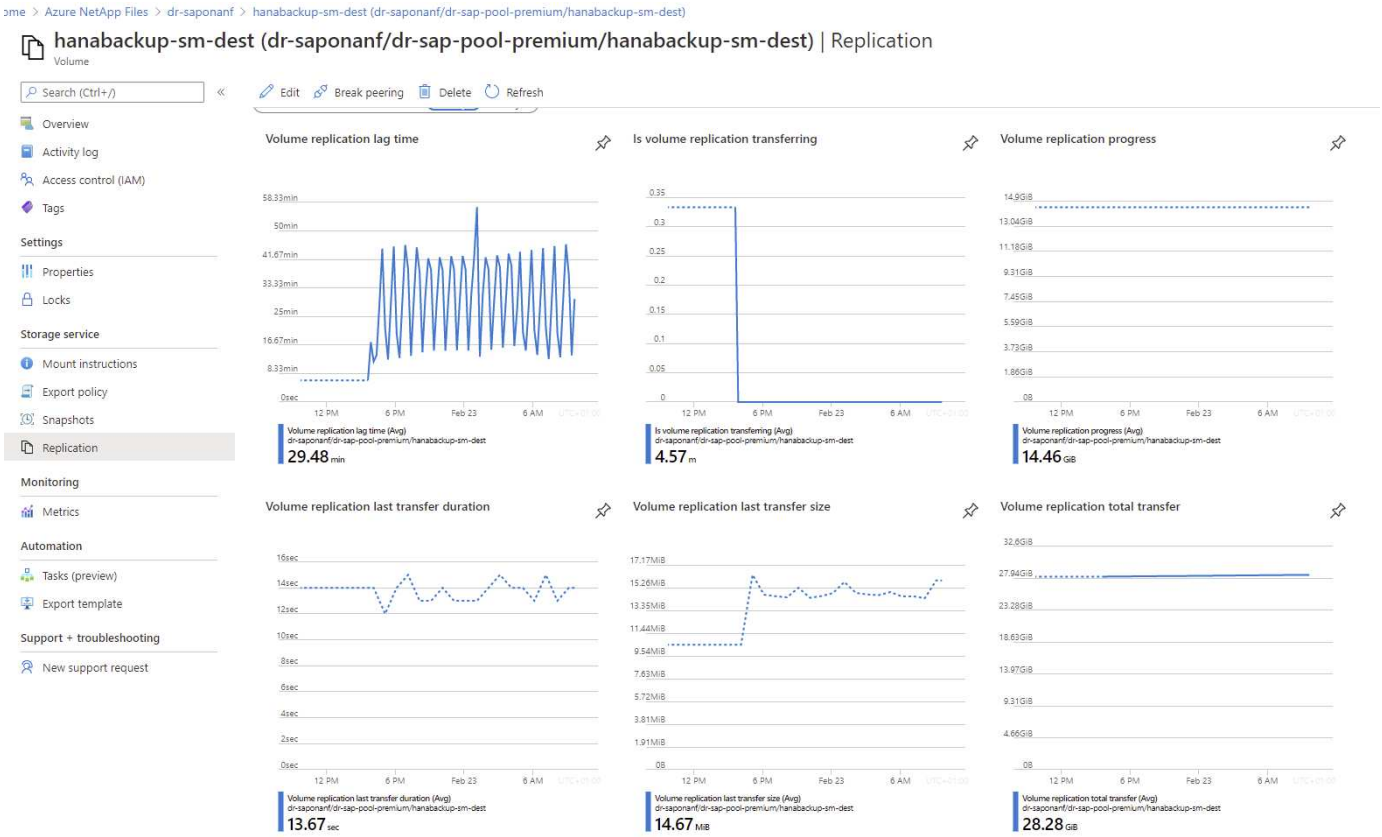
Il ritardo della replica del volume è un valore utile per comprendere le aspettative RPO. Ad esempio, la replica del volume di backup del registro mostra un ritardo massimo di 58 minuti, il che significa che l'RPO massimo ha lo stesso valore.

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

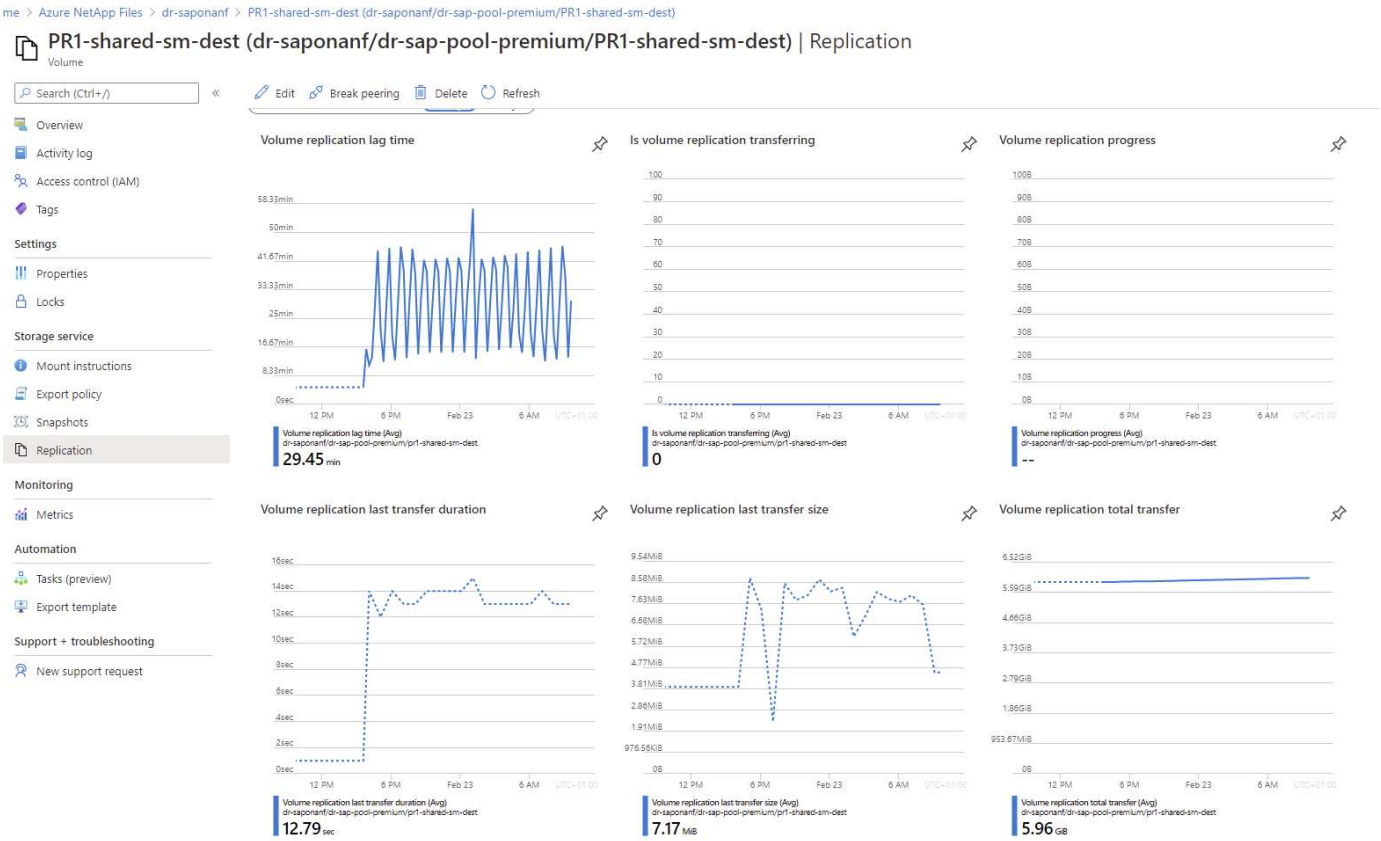
La seguente schermata mostra lo stato di replica del volume di dati HANA.



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



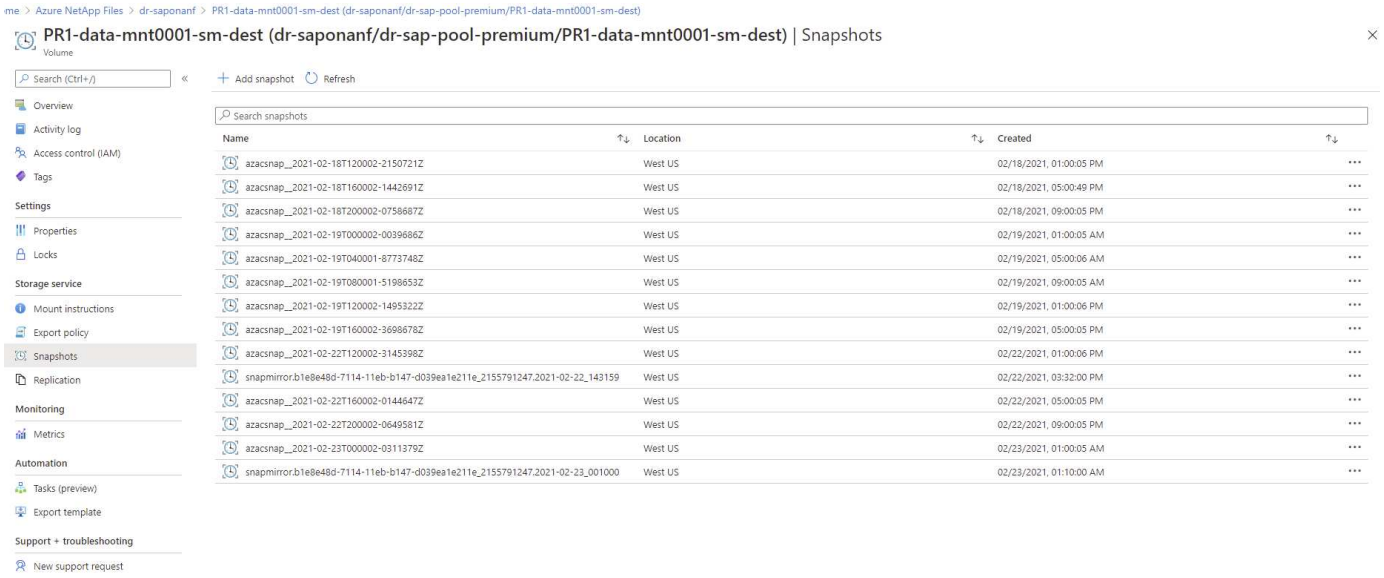
La seguente schermata mostra lo stato di replica del volume condiviso HANA.



Backup snapshot replicati

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

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



Test di disaster recovery

Test di disaster recovery

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

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

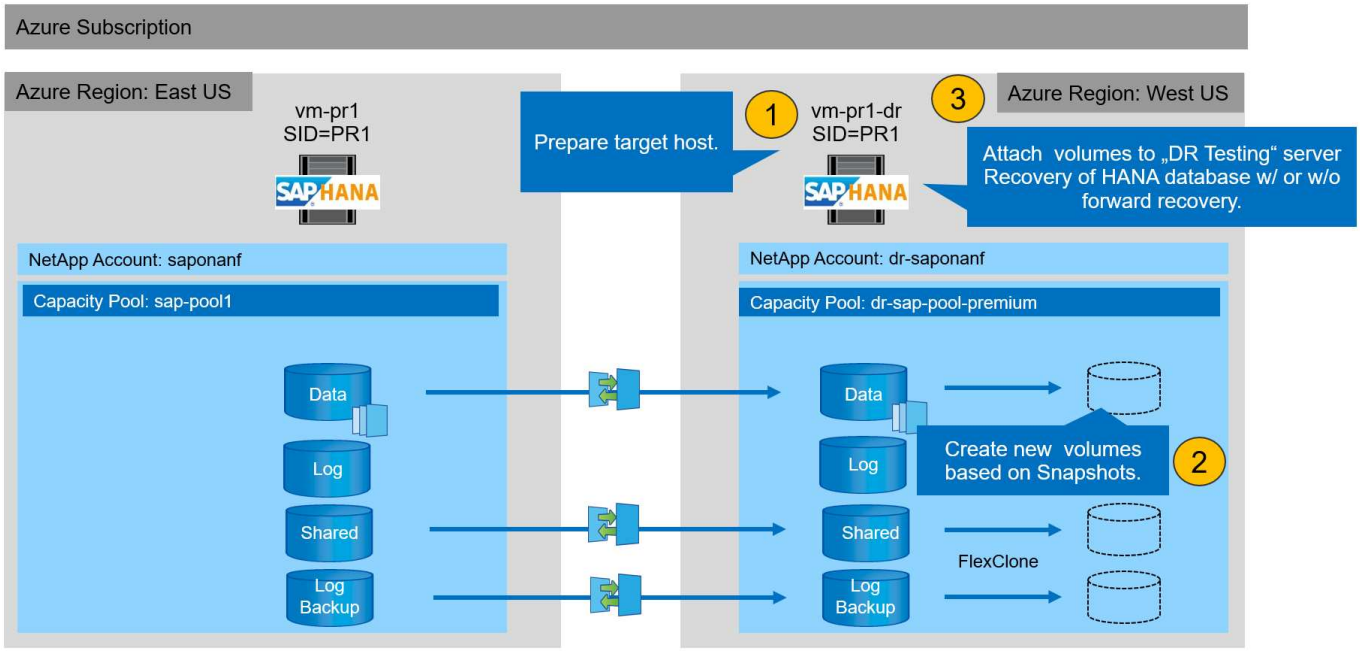
Il workflow di test del disaster recovery sfrutta il set di funzionalità ANF per creare nuovi volumi in base ai backup Snapshot esistenti nella destinazione del disaster recovery. Vedere "Funzionamento delle istantanee di Azure NetApp Files | documenti Microsoft".

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

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

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

Le seguenti sottosezioni descrivono in dettaglio questi passaggi.



Preparare l’host di destinazione

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

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

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

Nome host e indirizzo IP del server di destinazione

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

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

Installare il software richiesto

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

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

Configurare utenti, porte e servizi SAP

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

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

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

Preparare il volume di log HANA

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

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

Preparare il volume di backup del log

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

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

Preparare i montaggi del file system

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

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

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

Ecco i requisiti `/etc/fstab` voci.

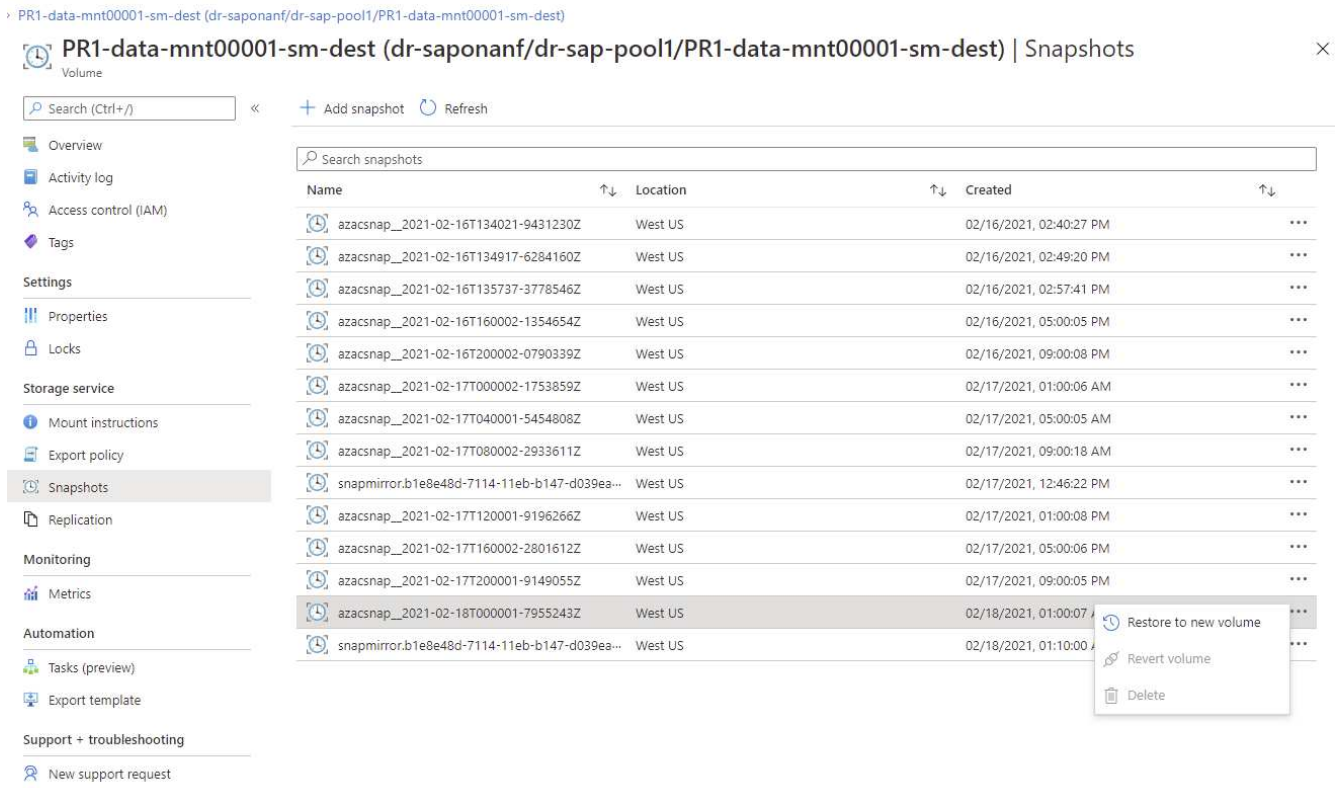
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa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

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

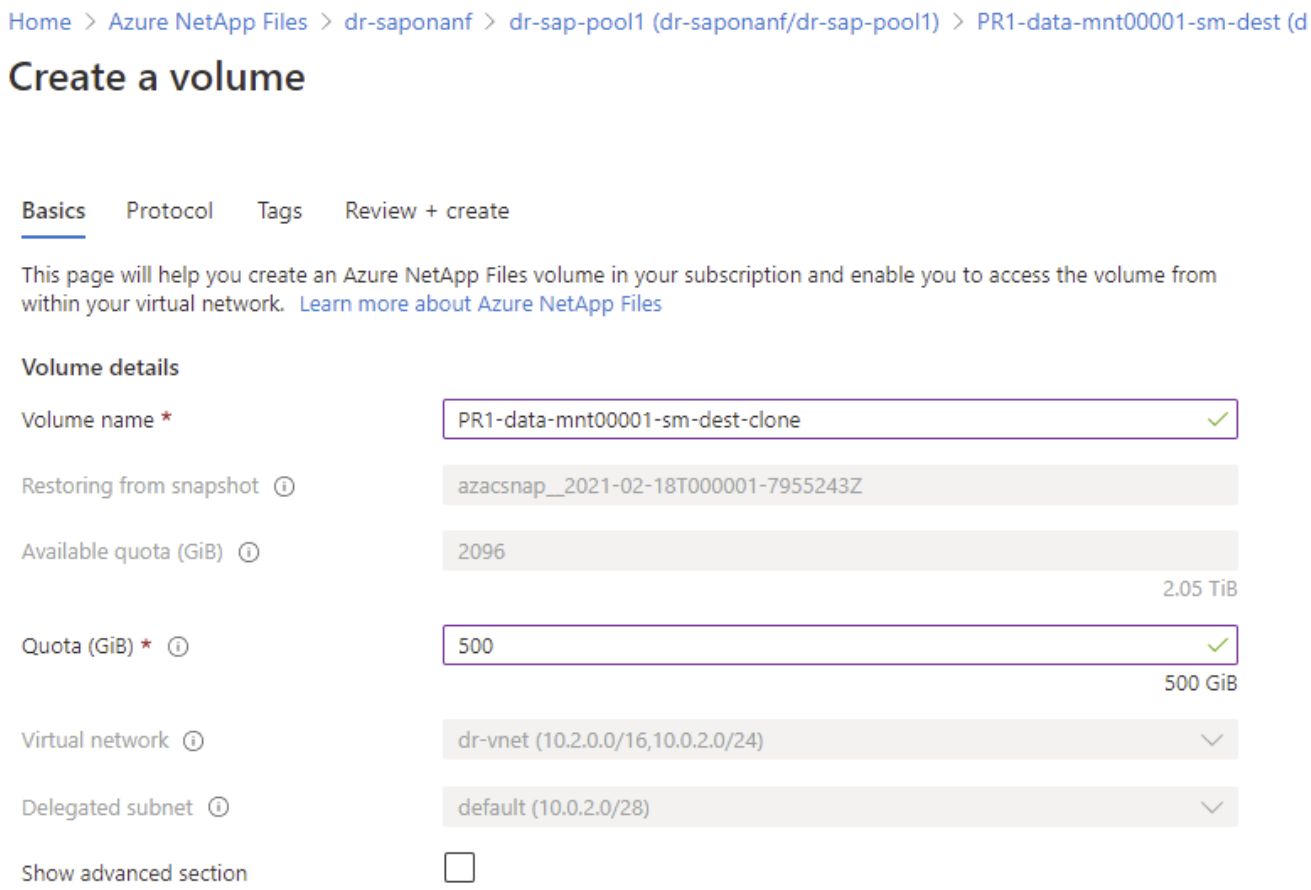
A seconda della configurazione del disaster recovery (con o senza replica del backup del log), è necessario creare due o tre nuovi volumi basati sui backup snapshot. In entrambi i casi, è necessario creare un nuovo volume dei dati e il volume condiviso HANA.

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

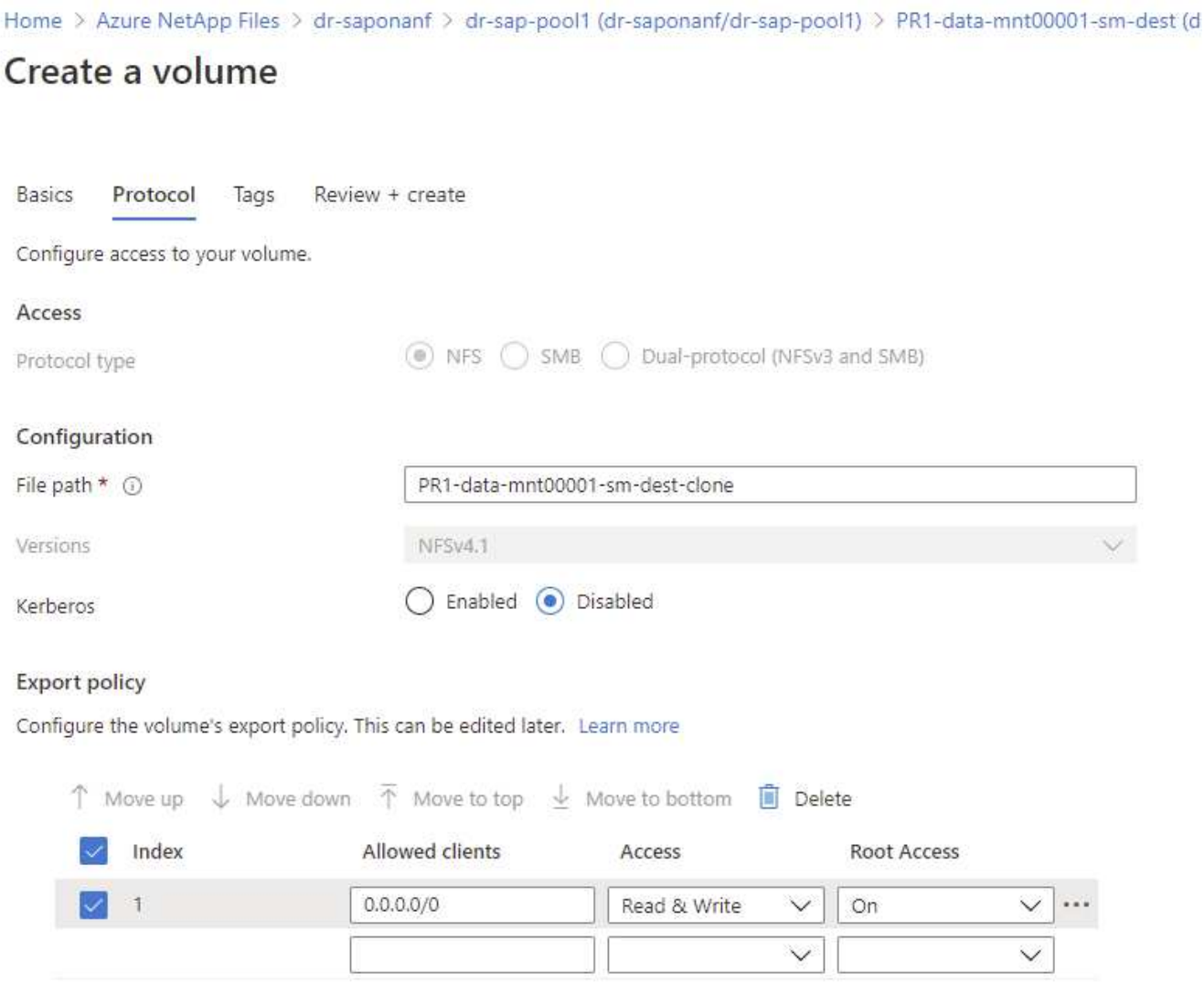
1. Uno dei backup snapshot coerenti con l'applicazione viene selezionato come origine per il nuovo volume del volume di dati HANA. L'opzione Restore to New Volume (Ripristina su nuovo volume) è selezionata per creare un nuovo volume in base al backup dello snapshot.



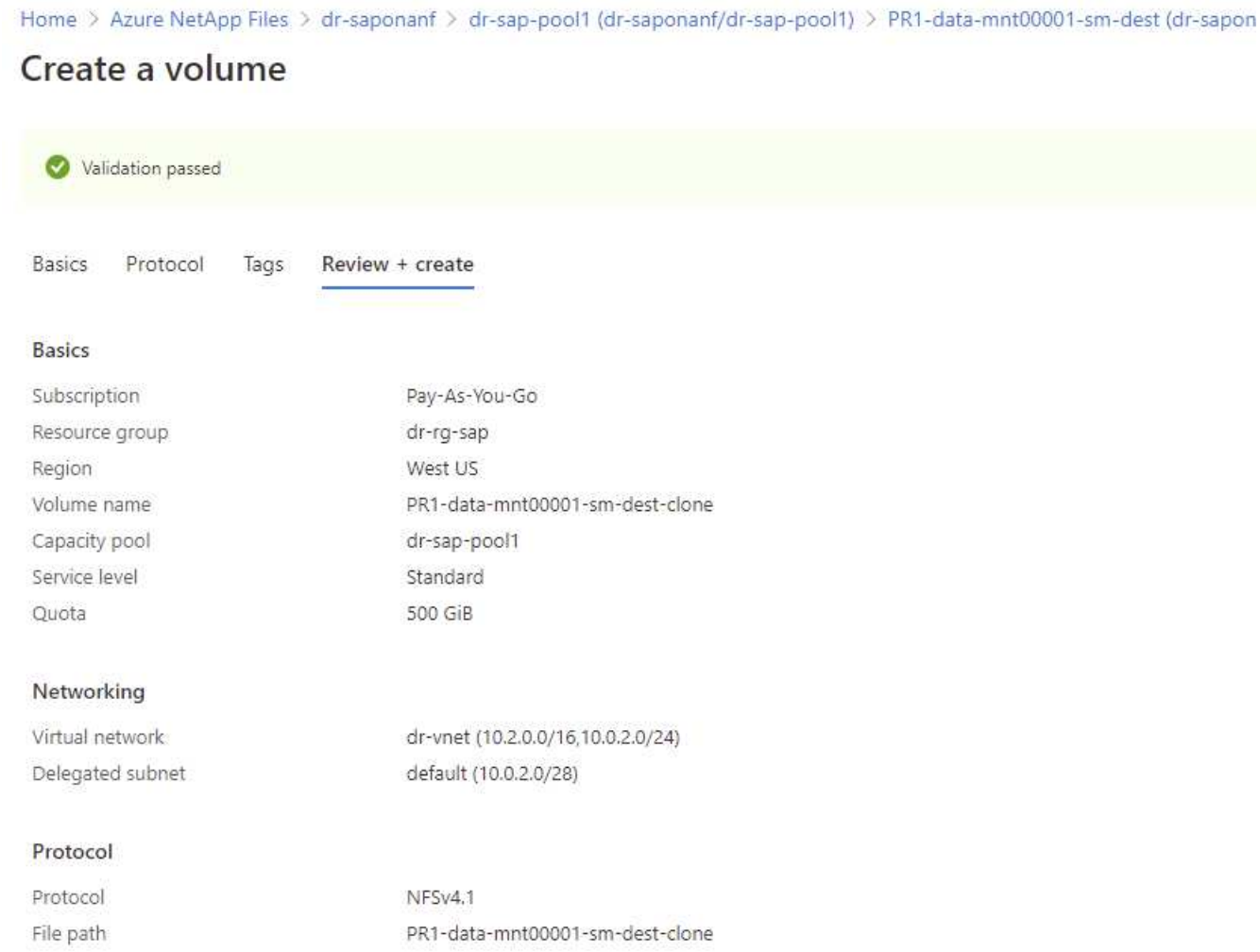
2. Il nuovo nome del volume e la nuova quota devono essere forniti nell'interfaccia utente.



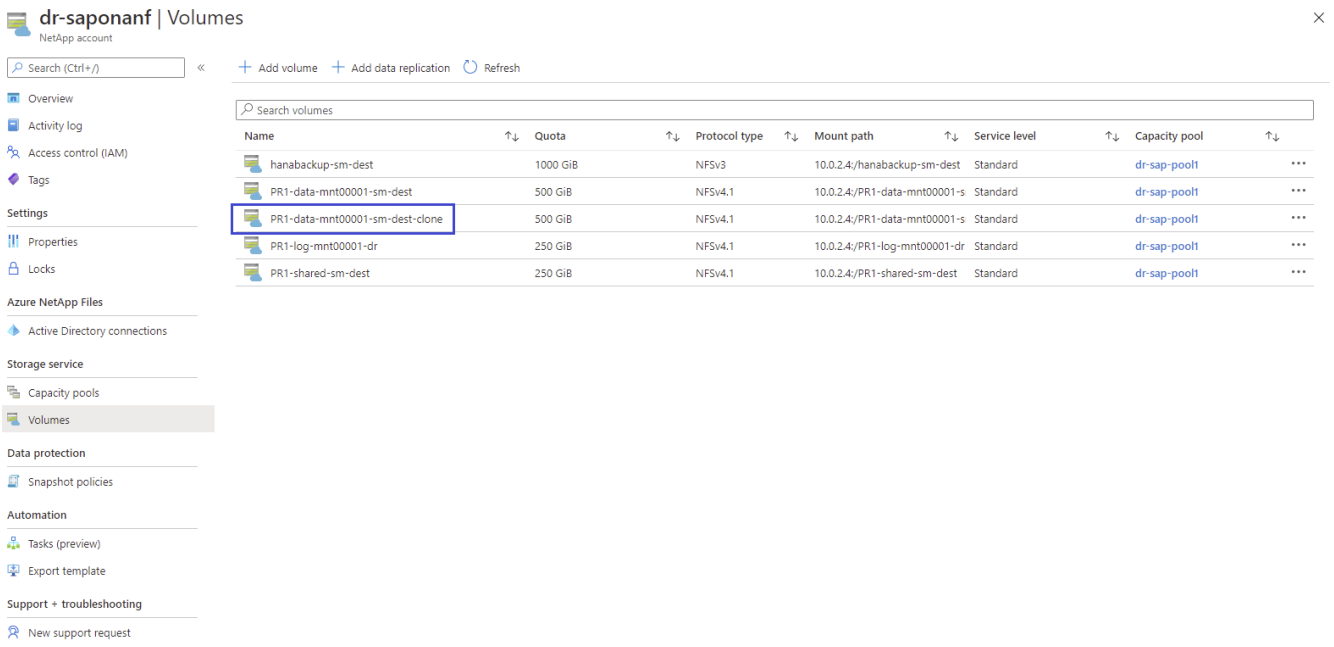
3. Nella scheda Protocol (protocollo), vengono configurati il percorso del file e la policy di esportazione.



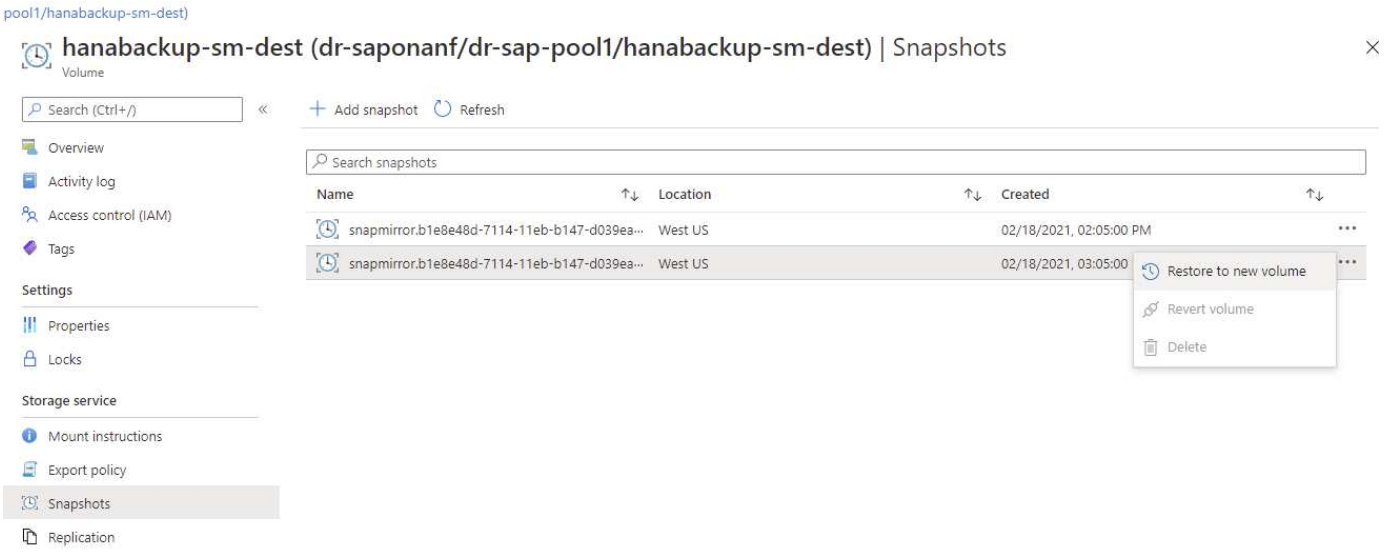
4. La schermata Create and Review (Crea e rivedi) riassume la configurazione.



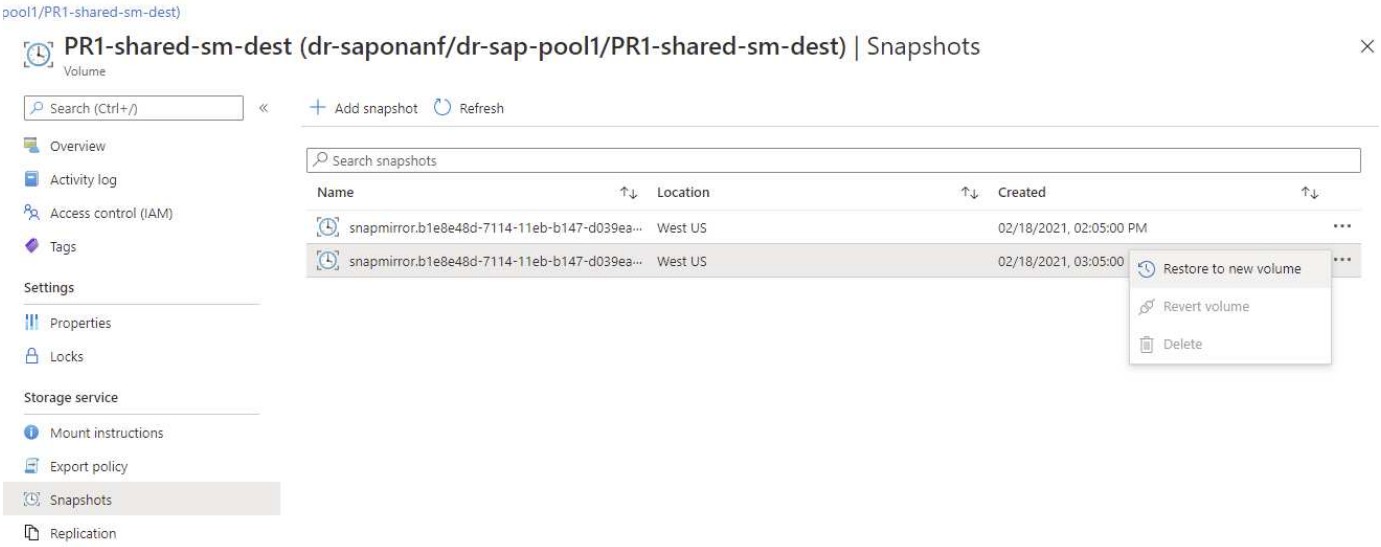
5. È stato creato un nuovo volume in base al backup di snapshot HANA.



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



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



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

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

Montare i nuovi volumi sull'host di destinazione

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

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

Il seguente output mostra i file system richiesti.

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

Ripristino del database HANA

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

Avviare i servizi SAP richiesti.

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

Il seguente output mostra i processi richiesti.

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

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

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

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

- Database di sistema

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

- Database tenant

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

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

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

Recovery del database di sistema

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

Recovery del database tenant

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

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

Il ripristino del tenant viene ora eseguito con hdbsql.

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

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

Recovery con forward recovery utilizzando backup di log/catalogo

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

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

- Database di sistema

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

- Database tenant

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

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

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

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

Recovery del database di sistema

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

Recovery del database tenant

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

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

hdbsql SYSTEMDB=>
```

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

Verificare la coerenza dei backup dei log più recenti

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

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

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

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

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

Failover del disaster recovery

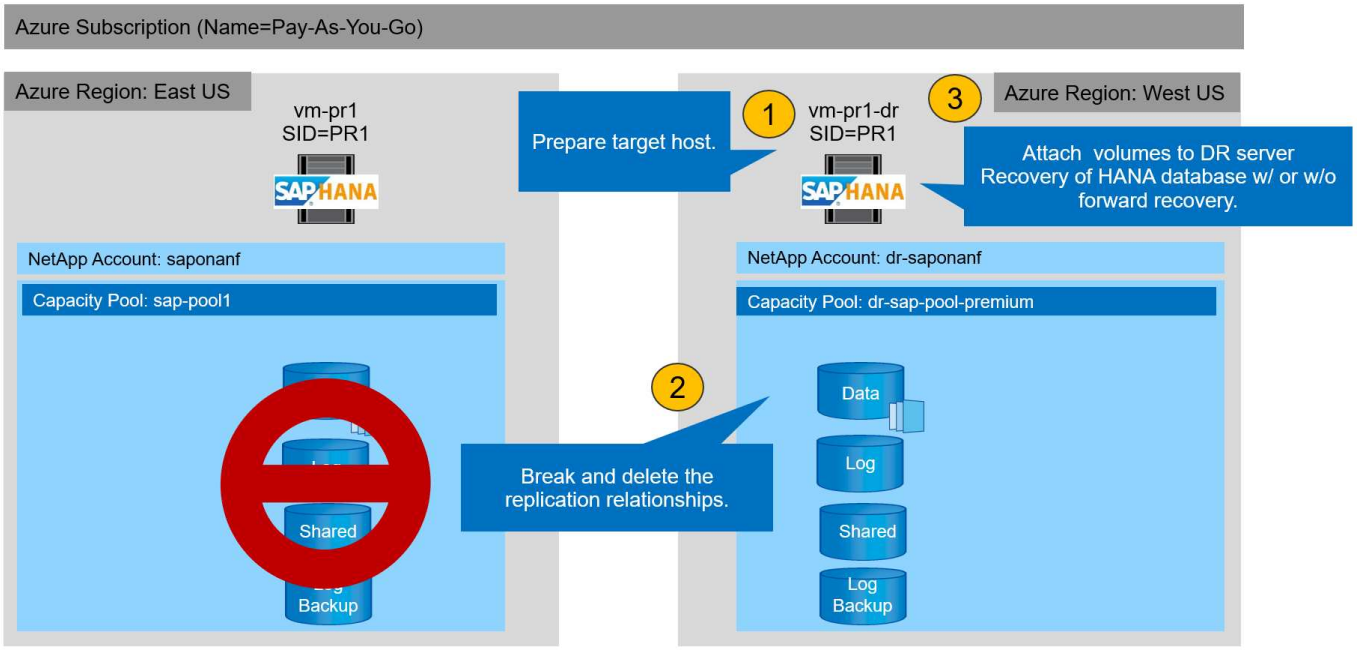
Failover del disaster recovery

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

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

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

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



Preparare l'host di destinazione

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

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

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

Nome host e indirizzo IP del server di destinazione

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

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

Installare il software richiesto

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

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

Configurare utenti, porte e servizi SAP

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

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

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

Preparare il volume di log HANA

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

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

Preparare il volume di backup del log

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

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

Preparare i montaggi del file system

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

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

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

Ecco i requisiti `/etc/fstab` voci.

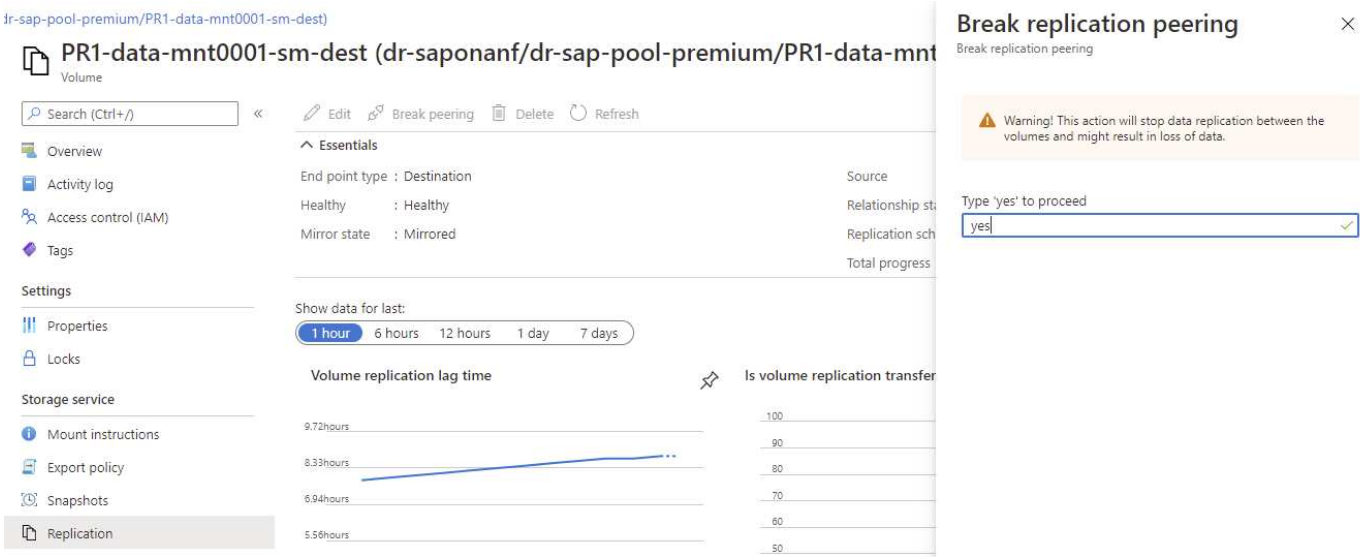
```
vm-pr1:~ # cat /etc/fstab
# HANA ANF DB Mounts
10.0.2.4:/PR1-data-mnt0001-sm-dest /hana/data/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa
time,lock,_netdev,sec=sys  0  0
10.0.2.4:/PR1-log-mnt00001-dr /hana/log/PR1/mnt00001 nfs
rw,vers=4,minorversion=1,hard,timeo=600,rsize=262144,wsize=262144,intr,noa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

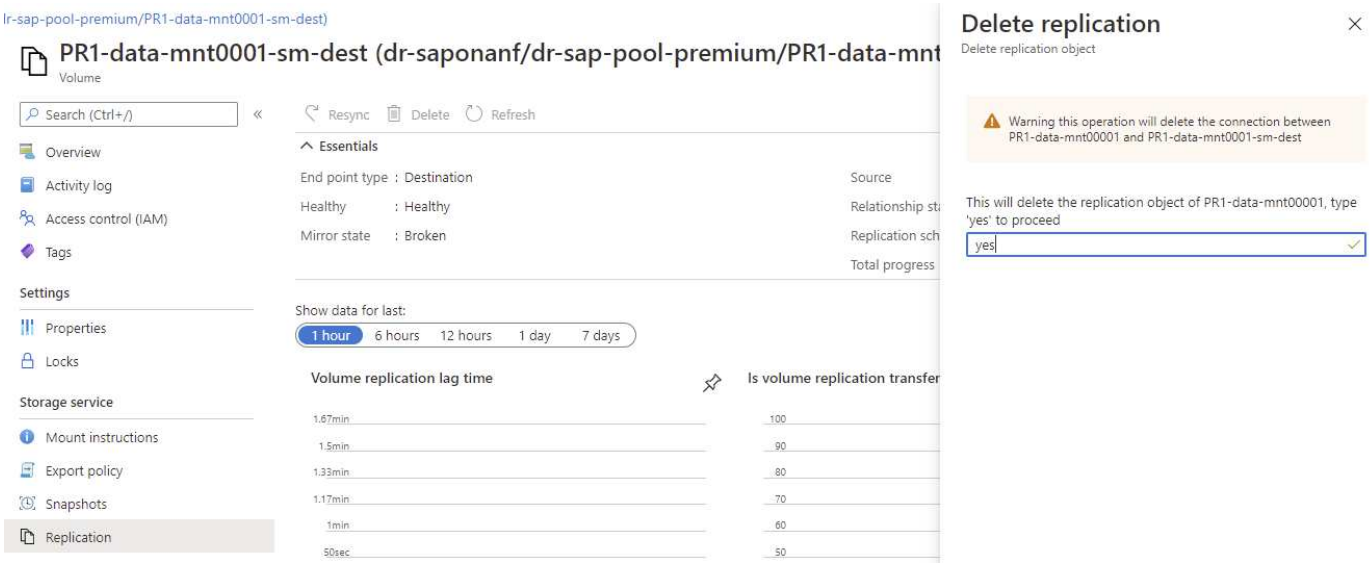
Interrompere ed eliminare il peering delle repliche

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

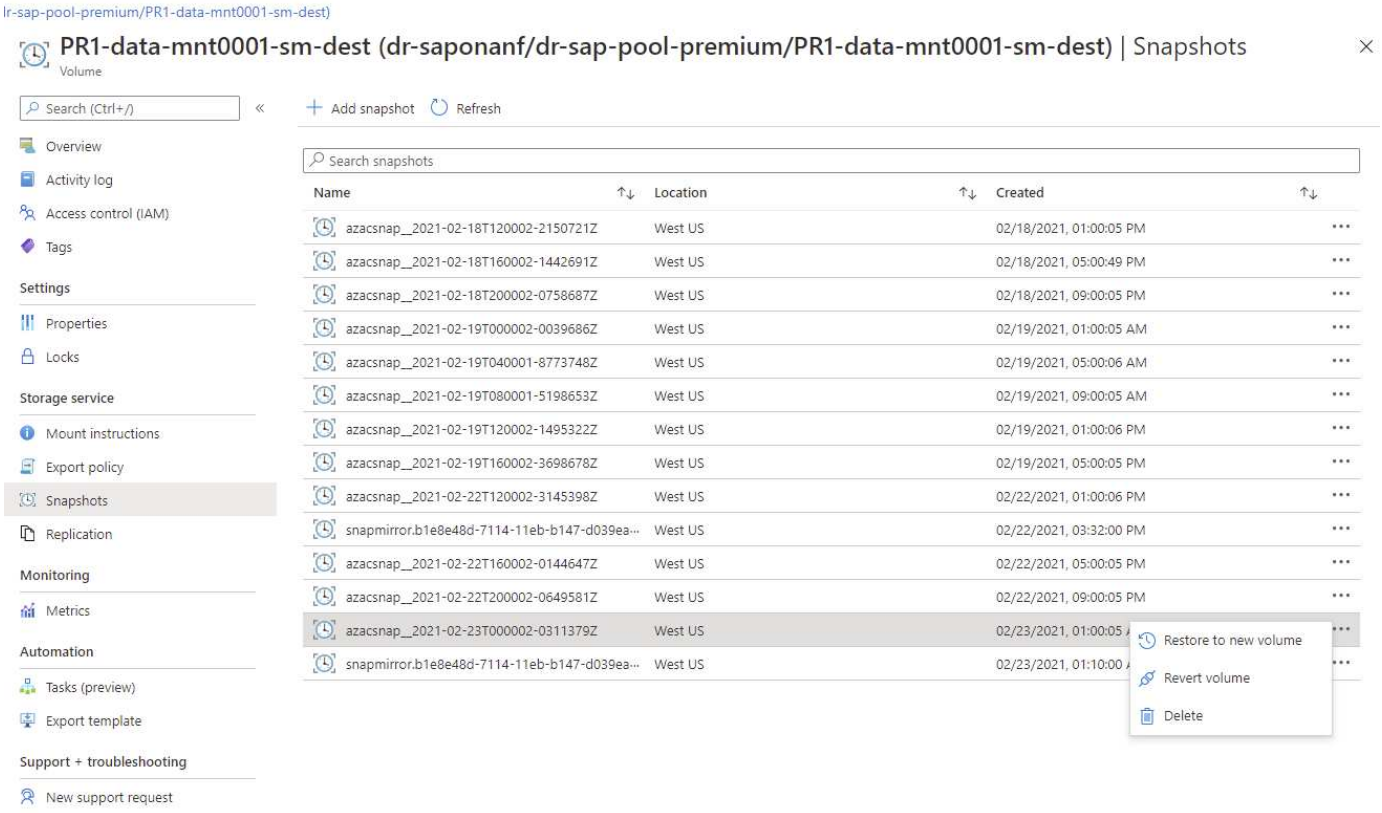
Per il volume di dati HANA, è necessario ripristinare il volume all'ultimo backup di snapshot HANA creato con AzAcSnap. Questa operazione di revert del volume non è possibile se l'ultimo snapshot di replica è contrassegnato come occupato a causa del peering della replica. Pertanto, è necessario eliminare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

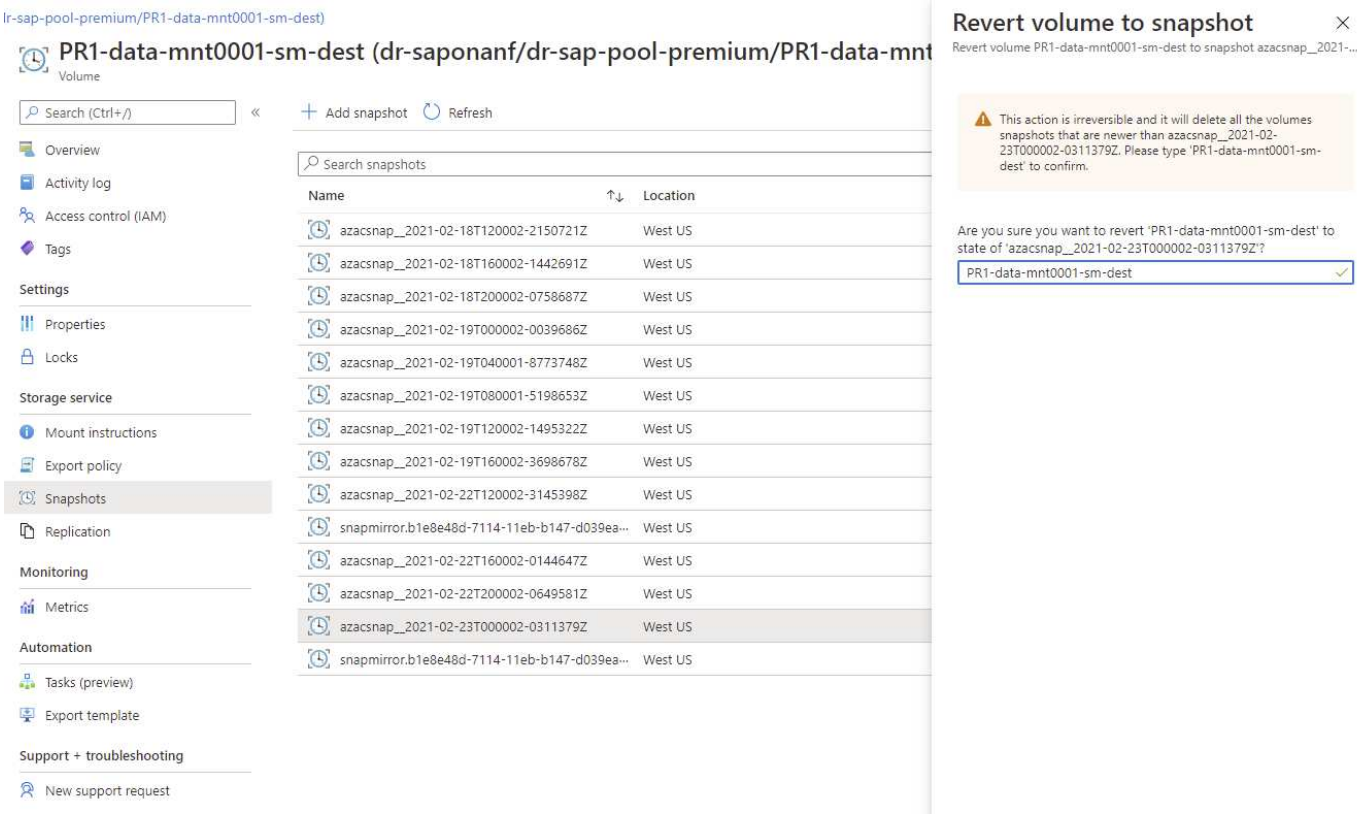
Le due schermate successive mostrano l'operazione di peering break e delete per il volume di dati HANA. Le stesse operazioni devono essere eseguite anche per il backup del log e per il volume condiviso HANA.





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





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

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

Montare i volumi sull'host di destinazione

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

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

Il seguente output mostra i file system richiesti.

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

Ripristino del database HANA

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

Avviare i servizi SAP richiesti.

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

Il seguente output mostra i processi richiesti.

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

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

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

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

- Database di sistema

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

- Database tenant

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

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

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

Recovery del database di sistema

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

Recovery del database tenant

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

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

Il ripristino del tenant viene ora eseguito con hdbsql.

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

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

Recovery con forward recovery utilizzando backup di log/catalogo

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

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

- Database di sistema

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

- Database tenant

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

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

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

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

Recovery del database di sistema

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

Recovery del database tenant

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

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

hdbsql SYSTEMDB=>
```

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

Verificare la coerenza dei backup dei log più recenti

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

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

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

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

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

Aggiornare la cronologia

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

Versione	Data	Riepilogo degli aggiornamenti
Versione 1.0	Aprile 2021	Versione iniziale

TR-4646: Disaster recovery SAP HANA con replica dello storage

TR-4646 è una panoramica delle opzioni per la protezione del disaster recovery per SAP HANA. Include informazioni dettagliate sull'installazione e una descrizione del caso di utilizzo di una soluzione di disaster recovery a tre siti basata sulla replica sincrona e asincrona dello storage NetApp SnapMirror. La soluzione descritta utilizza NetApp SnapCenter con il plug-in SAP HANA per gestire la coerenza del database.

Autore: Nils Bauer, NetApp

https://www.netapp.com/pdf.html?item=/media/8584-tr4646pdf.pdf

TR-4711: Backup e ripristino SAP HANA con sistemi di storage NetApp e software CommVault

TR-4711 descrive la progettazione di una soluzione NetApp e CommVault per SAP HANA, che include la tecnologia di gestione delle snapshot CommVault IntelliSnap e la tecnologia NetApp Snapshot. La soluzione si basa sullo storage NetApp e sulla suite di protezione dei dati CommVault.

Autori: Marco Schoen, NetApp; Dr. Tristan DAUDE, CommVault Systems

https://www.netapp.com/pdf.html?item=/media/17050-tr4711pdf.pdf

Integrazione SnapCenter per database SAP ASE

Questo documento descrive le specifiche di integrazione di SnapCenter per il database SAP ASE utilizzato in un ambiente SAP.

Introduzione

Il documento non intende essere una descrizione passo passo di come configurare l'ambiente completo, ma tratterà i concetti e i dettagli relativi a:

- Esempio di panoramica della configurazione
- Esempio di layout
- Proteggere l'istanza SAP ASE
- Ripristinare l'istanza SAP ASE

Autore: Michael Schlosser, NetApp

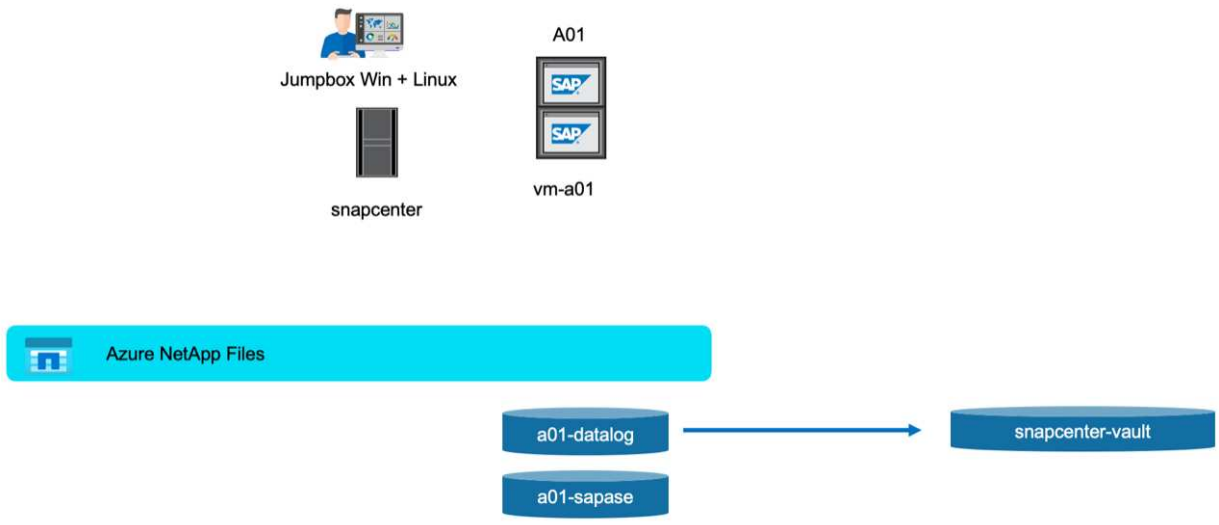
Esempio di panoramica della configurazione

Implementazione di esempio per il plug-in SnapCenter ASE per un sistema SAP in esecuzione sulla piattaforma Azure.

Questa implementazione descrive la configurazione minima richiesta del volume. I backup di dump dei dati e i backup di dump dei registri sono configurati in base alla nota SAP 1588316.

In alternativa, si potrebbe utilizzare la struttura volumetrica descritta in questa"Blog della community tecnica di MS".

Ambiente demo



Versioni software

Software	Versione
OS Linux	SLES PER SAP 15 SP5
SAP	SAP NetWeaver 7,5
SAP ASE	16,0 SP04 PL06 HF1
SnapCenter	6,1

Progettazione del volume ASE

Il seguente layout del volume minimo deve essere utilizzato per abilitare il backup/recovery e i casi d'utilizzo dei cloni per il database SAP ASE. La configurazione di esempio utilizza <SID>: A01.

Nome volume	Directory (qtree) su Volume	Mount Point sul server	Commento
<SID>-sapasi	sybase	/sybase	Directory principale per i file correlati ad ASE
		/Sybase/<SID>/backups	Backup di data dump (possono essere posizionati su un volume diverso)
		/Sybase/<SID>/log_archives	Log Dump Backup (backup di dump registro) (possono essere posizionati su un volume diverso)
	<sid>	/home/<sid> min	Home directory degli utenti <sid> adecimal
	usrsaptrans	/usr/sap/trans	Directory di trasporto
	<SID>	/Usr/sap/<SID>	Usr sap

Nome volume	Directory (qtree) su Volume	Mount Point sul server	Commento
	Sapmnt<SID>	/Sapmnt/<SID>	Dir. GlobalHost SAP
<SID>-datalog	sapdata_1	/Sybase/<SID>/sapdata_1	Dati DB (SID)
	saplog_1	/Sybase/<SID>/saplog_1	Log DB (SID)
	saptemp	/Sybase/<SID>/saptemp	PSAPTEMP
	sicurezza	/Sybase/<SID>/sybsecurity	Database di protezione Sybase
	sistema	/Sybase/<SID>/sybsystem	Database del sistema Sybase
	sibtemp	/Sybase/<SID>/sybtemp	Sistema Sybase DB - Temp
	sapdiag	/Sybase/<SID>/sapdiag	database 'strumenti di scansione'

Procedura per proteggere il database A01

- Controllare la distribuzione dei file, in base al layout di esempio
- Verificare i prerequisiti per l'host (vm-A01)
- Verifica dei prerequisiti per il database (A01)
- Distribuzione/installazione dell'agente SnapCenter sull'host (vm-A01)
- Creare la configurazione delle risorse di istanza di SnapCenter

Prerequisiti sull'host

Potrebbero essere disponibili informazioni più aggiornate "qui".

Prima di aggiungere un host e installare il pacchetto plug-in per Linux, è necessario completare tutti i requisiti.

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È possibile utilizzare l'autenticazione basata su password per l'utente root o non root oppure l'autenticazione basata su chiave SSH.
- Il plug-in SnapCenter per file system Unix può essere installato da un utente non root. Tuttavia, è necessario configurare i privilegi sudo per l'utente non root per installare e avviare il processo di plug-in. Dopo aver installato il plug-in, i processi verranno eseguiti come utenti non root.
- Creare credenziali con la modalità di autenticazione come Linux per l'utente di installazione.
- È necessario aver installato Java 11 sull'host Linux.
- Assicurarsi di aver installato solo l'edizione certificata di JAVA 11 sull'host Linux
- Per informazioni sul download di JAVA, vedere: Download di Java per tutti i sistemi operativi
- Si dovrebbe avere bash come shell di default per l'installazione del plug-in.

Prerequisiti per il database: Abilitare la registrazione e i backup

- Creare directory per backup e archivi_log (/sybase/A01/backups, /sybase/A01/log_archives)
- Connettersi al database A01 (come utente OS syba01)
  - Isql -S A01 -U sapsa -X -w 1024

- Creare la configurazione di scarico per I DATI (A01DB) secondo la nota SAP 1588316
  - usa master
  - vai
  - exec SP_config_dump @config_name='A01DB', @stripe_dir = '/sybase/A01/backups' , @compression = '101' , @verify = 'header'
  - vai
- Creare la configurazione di scarico per il REGISTRO (A01LOG) in base alla nota SAP 1588316
  - usa master
  - vai
  - SP_config_dump @config_name='A01LOG', @stripe_dir = '/sybase/A01/log_archives' , @compression = '101' , @verify = 'header'
  - vai
- Abilitare la registrazione completa per il database A01
  - SP_dboption A01, 'trunc log on chkpt' , false
  - vai
  - SP_dboption A01, 'full logging for all', 'true'
  - vai
  - SP_dboption A01, 'Imponi sequenza tran dump', 'true'
  - vai
- Backup DUMP del database per abilitare il backup DUMP DEL registro
  - Scaricare il database A01 usando config ='A01DB'
  - vai
  - Scarico registro
  - Eseguire il dump della transazione A01 utilizzando la configurazione = 'A01LOG'
  - vai
- Assicurarsi che i normali backup dei registri siano configurati, in base alla nota SAP 1588316

Opzionale – consente di creare un utente database dedicato

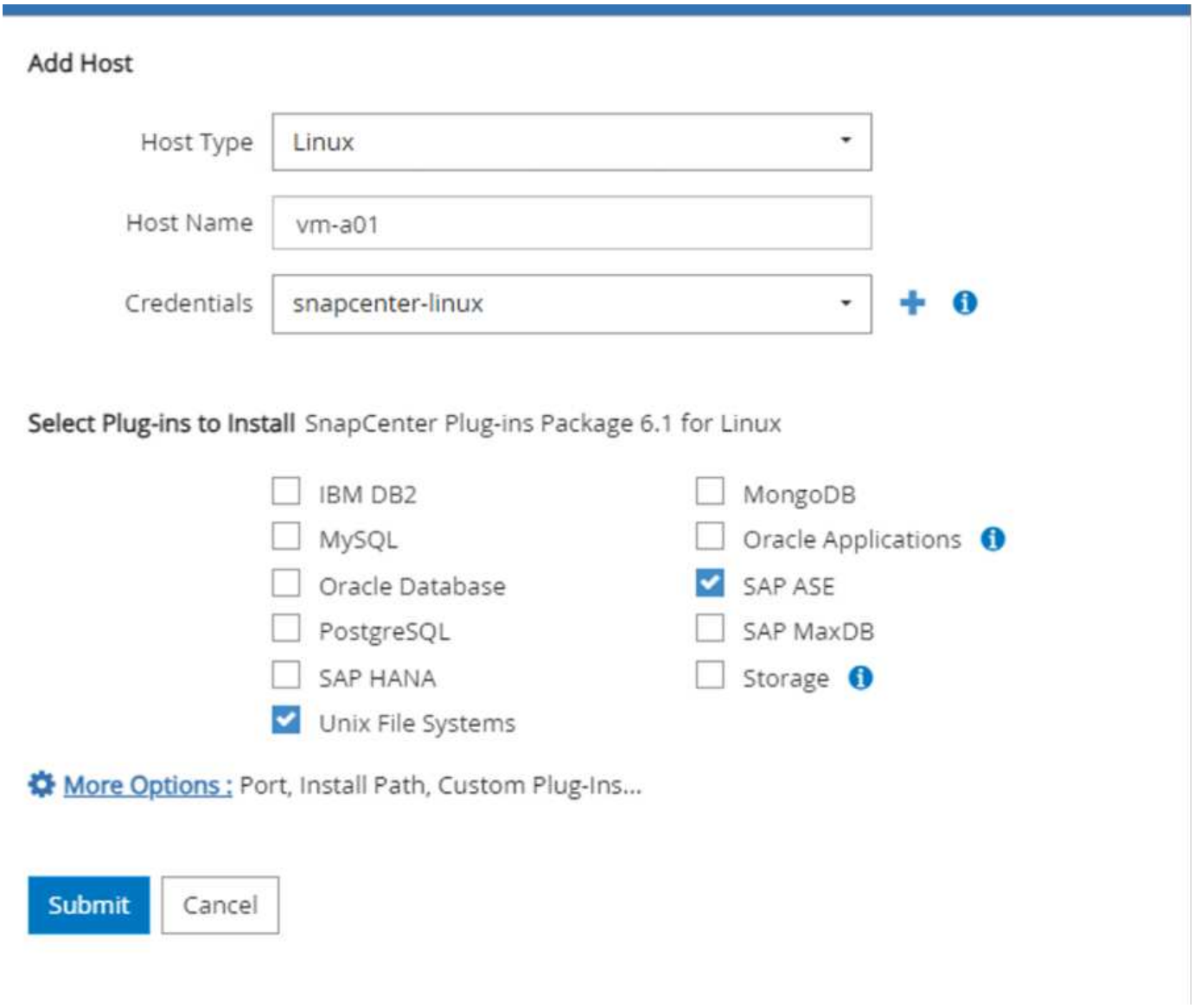
Per gli ambienti SAP è possibile utilizzare l'utente sapsa.

- Connettersi al database A01 (come utente OS syba01)
  - Isql -S A01 -U sapsa -X -w 1024
- crea utente
  - creare il backup dell'accesso con password <password>
  - vai
- assegnare i permissoni/ruoli all'utente
  - assegnare il ruolo sa_role,sso_role,oper_role,sybase_ts_role al backup
  - vai

Distribuire l'agente SnapCenter per ospitare vm-A01

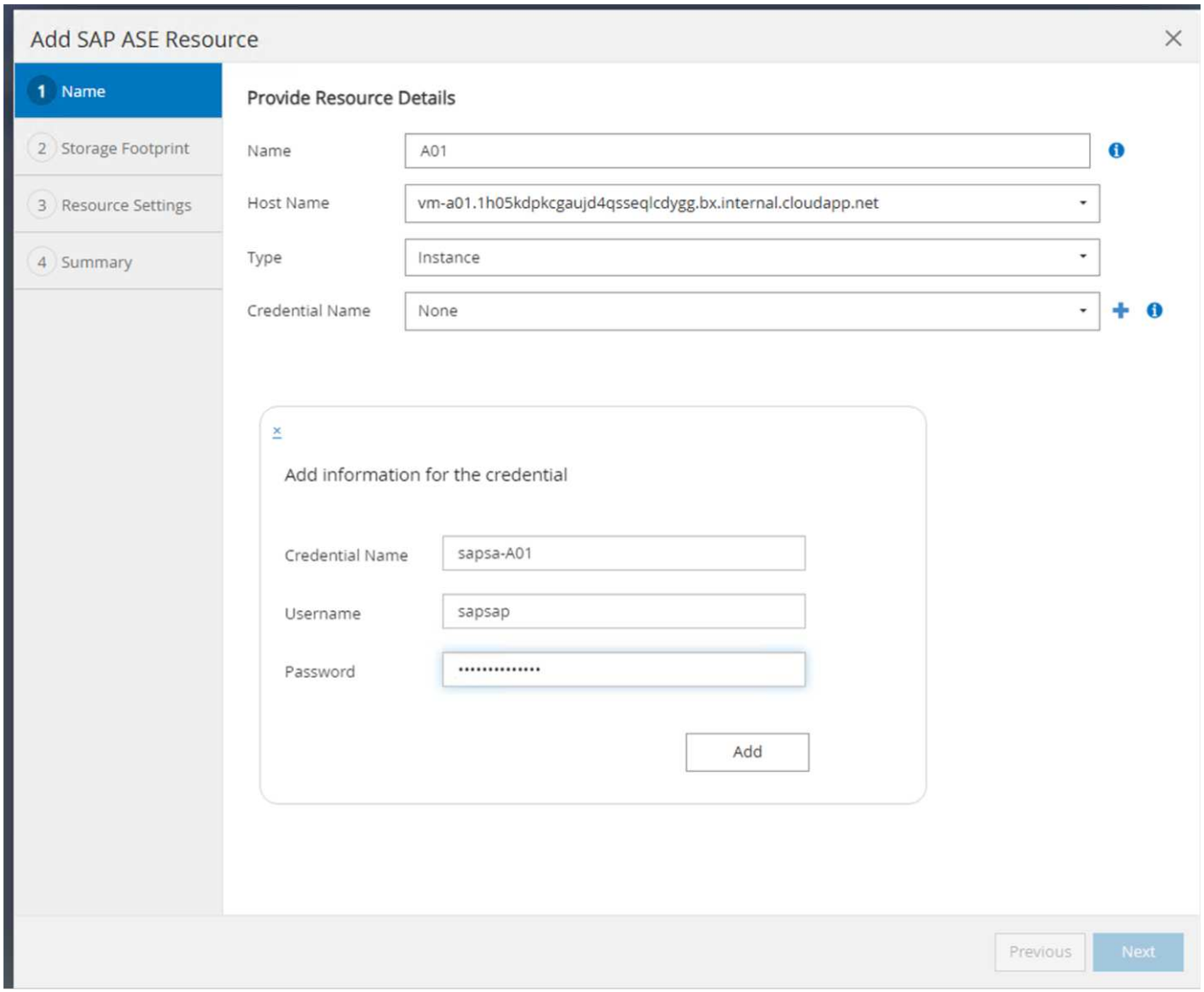
Ulteriori informazioni sono disponibili nella "Documentazione SnapCenter".

Selezionare SAP ASE e Unix file Systems Plugin.

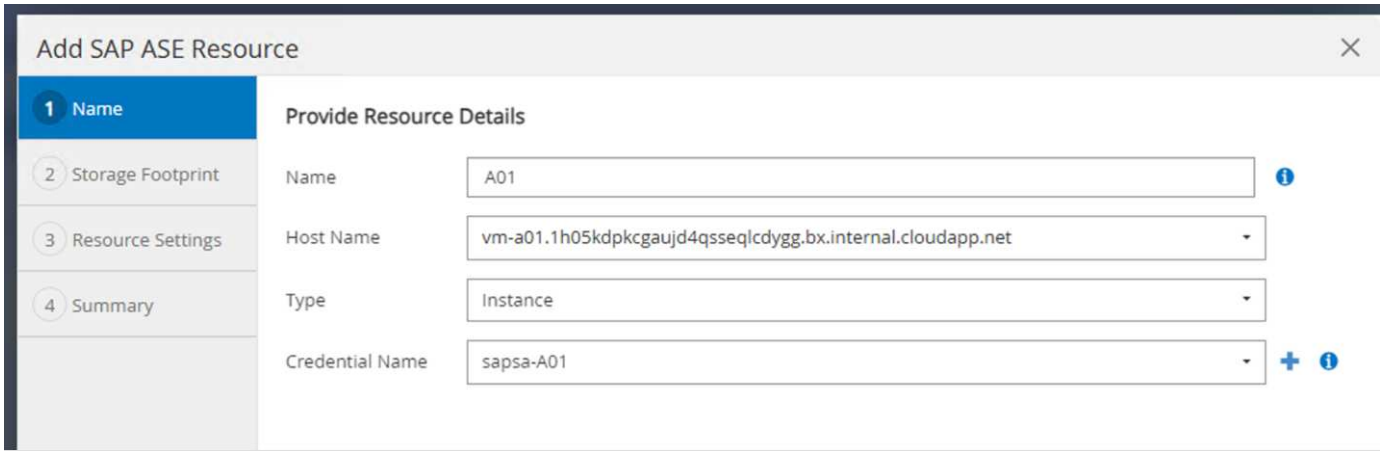


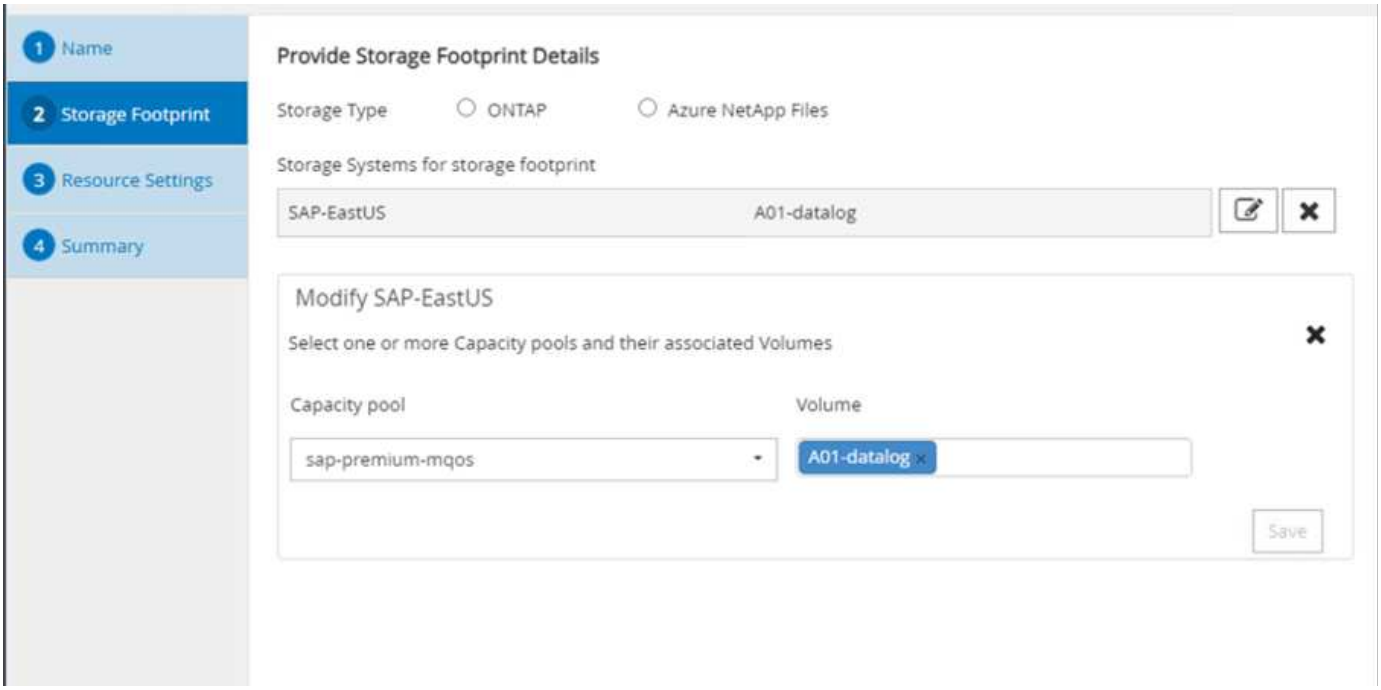
Creare la configurazione delle risorse delle istanze di SnapCenter per il database A01

Risorse → SAP ASE → Aggiungi risorse



Se la password contiene caratteri speciali, è necessario mascherarli con una barra rovesciata. Ad es. Test!123! → Test\!123\!

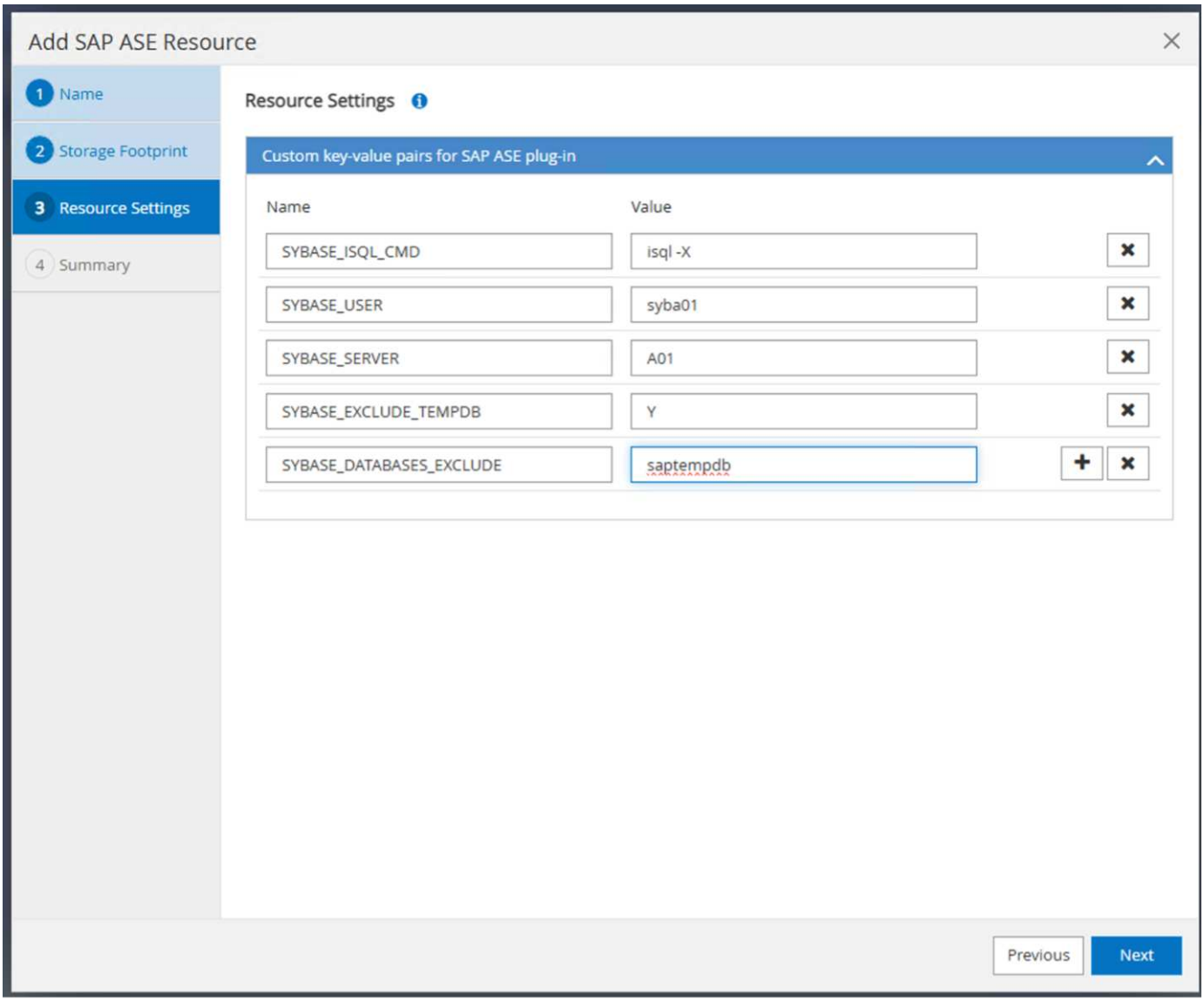




Se si sta utilizzando la progettazione del volume di "Blog della community tecnica di MS".

I volumi /base <SID> SecureEasySetup, /unità <SID>, /unità <SID> estesa devono essere configurati come spazio di archiviazione

È necessario effettuare (almeno) coppie chiave-valore personalizzate nelle seguenti impostazioni delle risorse.



La tabella seguente elenca i parametri del plug-in Sybase, ne fornisce le impostazioni e li descrive:

Parametro	Impostazione	Descrizione
SYBASE_ISQL_CMD	Esempio: /Opt/sybase/OCS-15__0/bin/isql -X.	Definisce il percorso del comando isql. Opzioni disponibili: https://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.dc34237.1500/html/mvsinst/CIHHFDGC.htm
SYBASE_USER	nome_utente	Specifica l'utente del sistema operativo che può eseguire il comando isql. Questo parametro è obbligatorio per UNIX. Questo parametro è necessario se l'utente che esegue i comandi Agentstart e stop di Snap Creator (di solito l'utente root) e l'utente che esegue il comando isql sono diversi.
SERVER_SYBASE	nome_server_dati	Specifica il nome del server di dati Sybase (opzione-S sul comando isql).ad esempio: A01

Parametro	Impostazione	Descrizione
DATABASE_SYBASE	db_name:nome_utente/password	Elenca i database all'interno dell'istanza di cui eseguire il backup. Viene aggiunto il database master; ad esempio: DBAtest2:sa/53616c7404351e.se viene utilizzato un database denominato +ALL, viene utilizzato il rilevamento automatico del database e vengono esclusi i database sybsyntax, sybsystemdb, sybsystemprocs e tempdb. Ad esempio: +ALL:sa/53616c71a6351e le password crittografate sono supportate se è impostato il parametro NTAP_PWD_PROTECTION.
SYBASE_DATABASES_EXCLUDE	nome_db	Consente di escludere i database se viene utilizzato il costrutto +ALL. È possibile specificare più database utilizzando un elenco separato da punto e virgola.ad esempio, pubs2;test_DB1
SYBASE_TRAN_DUMP	db_name:percorso_directory	Consente di eseguire un dump delle transazioni Sybase dopo la creazione di una copia Snapshot.ad esempio: pubs2:/sybasedump/pubs2 è necessario specificare ogni database che richiede un dump delle transazioni.
SYBASE_TRAN_DUMP_FORMAT	%S_%D_%T.CMN	Consente di specificare la convenzione di naming dump. È possibile specificare le seguenti chiavi: %S = nome istanza da SYBASE_SERVER %D = database da SYBASE_DATABASES %T = timestamp univoco Ecco un esempio: %S_%D_%T.log
SYBASE_TRAN_DUMP_COMPRESS	(Y / N)	Attiva o disattiva la compressione nativa del dump delle transazioni Sybase.
SYBASE	Esempio: /Sybase	Specifica la posizione dell'installazione di Sybase.
MANIFESTO_SYBASE	Esempio: A01:/sybase/A01/sapdiag	Specifica i database per i quali deve essere creato il file manifest, insieme alla posizione in cui deve essere posizionato il file manifest.
SYBASE_MANIFEST_FORMAT	%S__%D_.esempio manifesto: %S_%D_.manifesto	Consente di specificare la convenzione di denominazione del file manifest. È possibile specificare le seguenti chiavi: %S = Nome istanza da SYBASE_SERVER %D = database da SYBASE_DATABASES
SYBASE_MANIFEST_DELETE	(Y / N)	Consente di eliminare il manifesto dopo la creazione della copia Snapshot. Il file manifest deve essere acquisito nella copia Snapshot in modo che sia sempre disponibile con il backup.
SYBASE_EXCLUDE_TEMPDB	(Y / N)	Consente l'esclusione automatica dei database temporanei creati dall'utente.

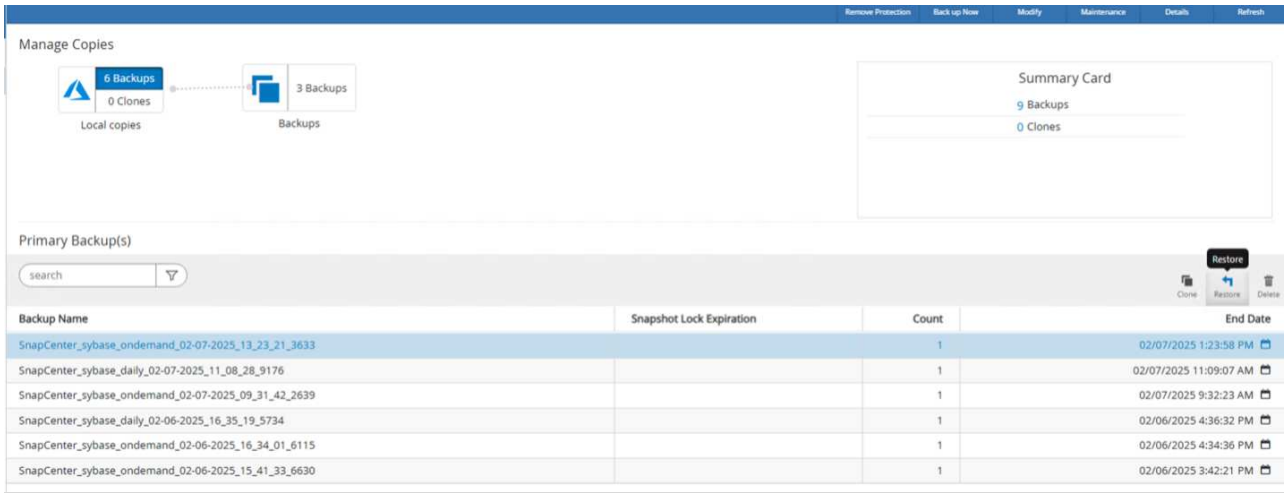
Sequenza di ripristino del sistema A01

1. Arrestare SAP System A01 (incluso il database), arrestare sapinit
2. Montare i file system

3. Ripristina i volumi A01-datalog (utilizzando SnapCenter)
4. Montare i filesystem
5. Avviare il database A01 (con l'opzione –q, per evitare l'accesso automatico online e mantenere il database in avanti recuperabile – secondo la nota SAP 1887068)
6. Avviare BackupServer A01
7. online database saptools, sybsecurity , sybmgmtdb
8. Recupera database A01 (utilizzando isql)
9. Database online A01
10. Avviare sapinit, sistema SAP A01

Recupera istanza A01

- Arrestare il sistema SAP + DB A01 sulla vm-A01 host
  - Utente a01adm: Stopsap
  - Utente root: /Etc/init.d/sapinit stop
  - Root utente: Umount -a -t nfs
- Ripristina backup
  - GUI SnapCenter: Selezionare il backup richiesto per il ripristino



  - Per la distribuzione ANF: È disponibile solo la risorsa completa

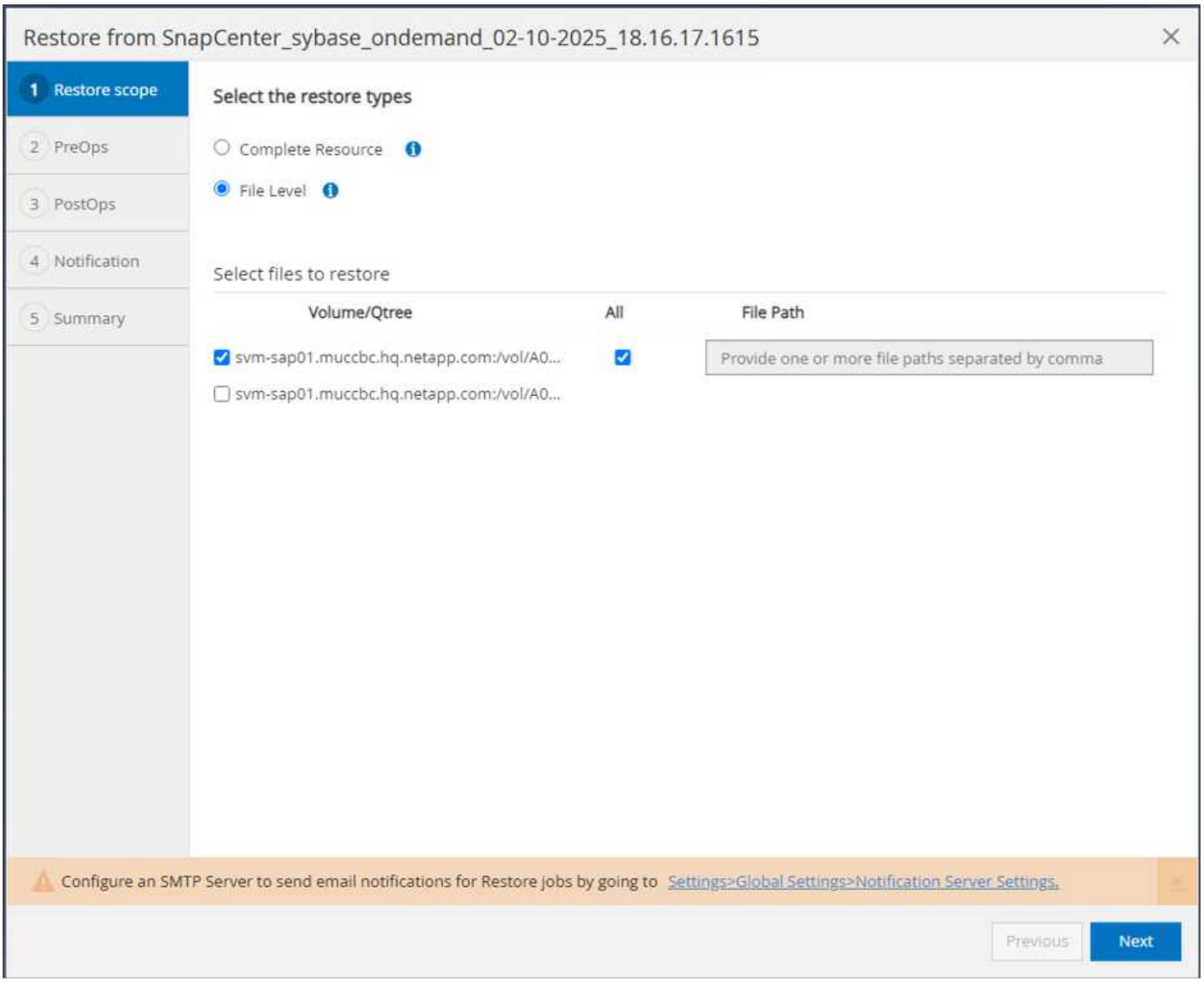


Se si seleziona complete Resource (risorsa completa), viene attivato un VBSR (Volume Based Snap Restore). All'interno di Azure viene chiamato "ripristino volume".

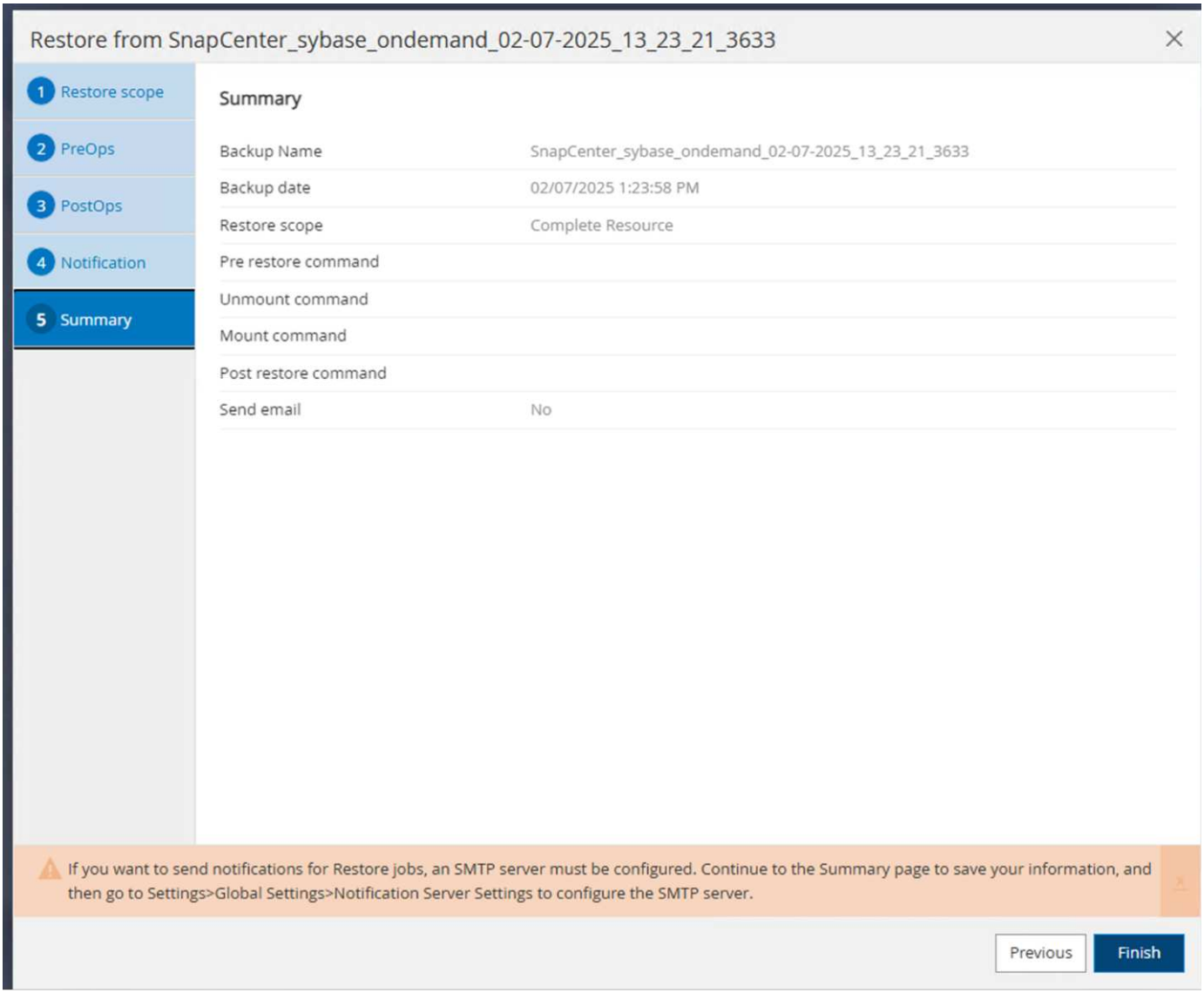
Important

Active filesystem data and snapshots that were taken after the selected snapshot will be lost. The snapshot revert operation will replace *all* the data in the targeted volume with the data in the selected snapshot. You should pay attention to the snapshot contents and creation date when you select a snapshot. You cannot undo the snapshot revert operation.

Per altri tipi di distribuzione (ad esempio, on-premise ANF) è possibile orchestrare un'operazione SFSR (Single file Snap Restore). Selezionare file Level (livello file) e il volume corrispondente e selezionare "All" (tutti). Vedere la seguente schermata.



Viene visualizzato Summary (Riepilogo) e con Finish (fine) viene avviato il ripristino effettivo.



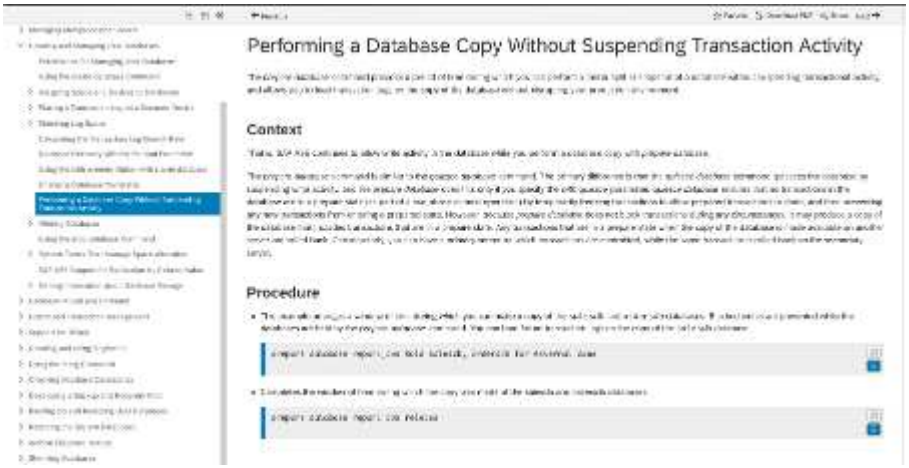
- Montare i file system (vm-A01)
  - Utente root: Mount -a -t nfs
- Avviare Database A01 + BackupServer
  - Modificare RUN_A01 e aggiungere -q \ (in base alla nota SAP 1887068)
  - Utente syba01: RUN_A01 &
  - Utente syba01: RUN_A01_BS&
- Database online saptools, sybsecurity , sybmgmtdb
  - Utente syba01: Isql -S A01 -U sapsa -X -w 1024
  - saptools di database online
  - vai
  - sicurezza del database online
  - vai
  - database online sybmgmtdb
  - vai

- Recuperare il database A01
  - SP_dump_history (per visualizzare i dump del log delle transazioni)
  - vai
  - Caricare i dump del registro delle transazioni in base alle proprie esigenze. Per ulteriori informazioni, vedere la documentazione: https://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.dc36272.1572/html/commands/X75212.htm
  - Esempio: CARICA TRAN A01 DA '/sybase/A01/log_archives/A01.TRAN.20250207.140248.6.000'
  - vai
  - Database online A01
  - vai
- Rimuovere -q da RUN_A01
- Avviare il sistema SAP
  - Utente root: /Etc/init.d/sapinit start
  - Utente a01adm: Startsap

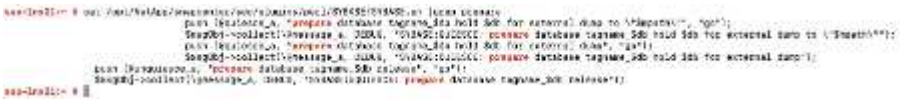
Informazioni aggiuntive e cronologia delle versioni

Quiescenza vs. Preparazione

Consultare la documentazione al xref:./backup/Pagina di aiuto di SAP.



Il plugin SAP ASE di SnapCenter utilizza il comando quiesce database, tuttavia potrebbe essere sostituito dal comando prepara. Se necessario, deve essere modificato in SYBASE.pm nelle righe 473, 475, 479, 481, 673, 675, ad esempio



Demo registrate

Le seguenti demo riportate di seguito sono disponibili a supporto della documentazione.

Installazione e configurazione del plug-in ASE, backup del database ASE

Ripristino del database ASE

Documentazione esterna

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

- "Installazione SAP Azure su ANF"
- "Prerequisiti SnapCenter per i plug-in"
- "Plug-in di installazione di SnapCenter"
- "Infocentro Sybase - isql"
- "Sybase Infocenter - carica dump del log delle transazioni"
- Note SAP (accesso richiesto)
  - 1887068 - SYB: Utilizzo di backup e ripristino esterni con SAP ASE: https://me.sap.com/notes/1887068/E
  - 1618817 - SYB: Come ripristinare un server di database SAP ASE (UNIX): https://me.sap.com/notes/1618817/E
  - 1585981 - SYB: Garanzia di recuperabilità per SAP ASE: https://me.sap.com/notes/1585981/E
  - 1588316 - SYB: Configurare i backup automatici di database e log: https://me.sap.com/notes/1588316/E
  - Documentazione del prodotto NetApp: https://www.netapp.com/support-and-training/documentation/
  - "Soluzioni SAP di NetApp – informazioni su casi d'utilizzo, Best practice e vantaggi"

Cronologia delle versioni

Versione	Data	Cronologia della versione del documento
Versione 1.0	Aprile 2025	Versione iniziale – backup/ripristino database ASE

Integrazione SnapCenter per database IBM DB2

Questo documento descrive le specifiche di integrazione di SnapCenter per il database IBM DB2 utilizzato in un ambiente SAP.

Introduzione

Il documento non intende essere una descrizione passo passo di come configurare l'ambiente completo, ma tratterà i concetti e i dettagli relativi a:

- Esempio di panoramica della configurazione
- Esempio di layout
- Proteggere il database DB2
- Ripristinare e ripristinare il database DB2

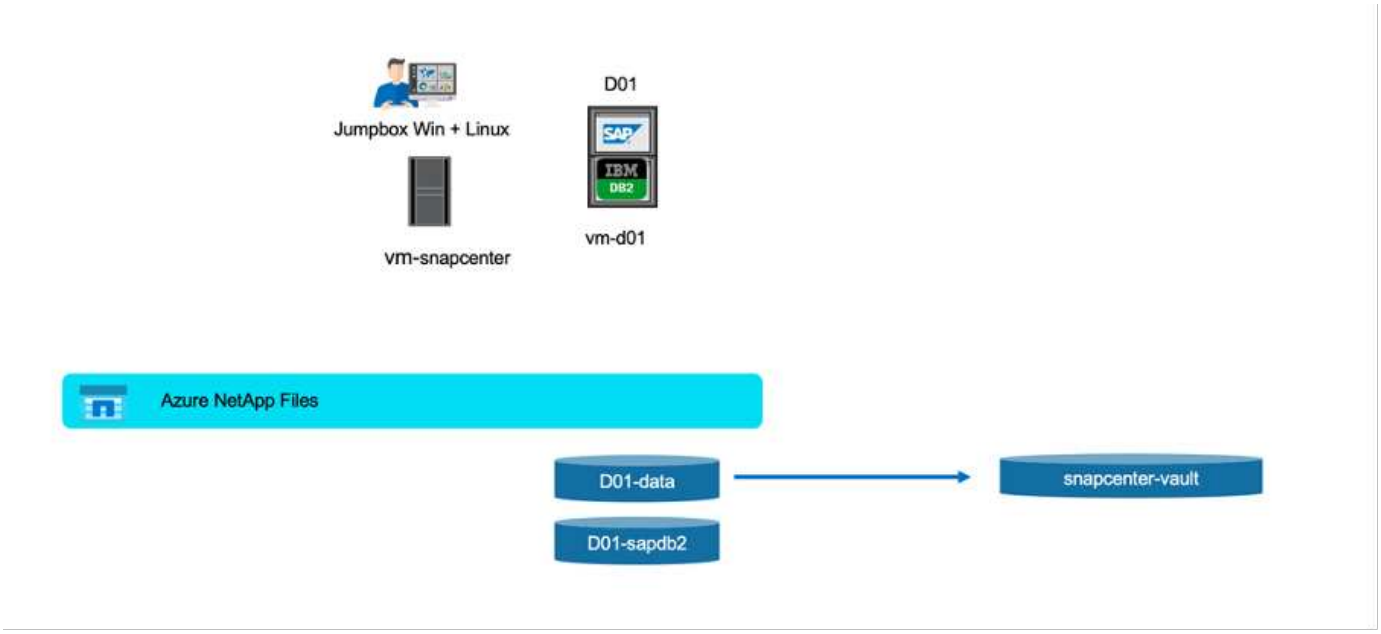
Autore: Michael Schlosser, NetApp

Esempio di panoramica della configurazione

Esempio di implementazione per il plugin SnapCenter DB2 per un sistema SAP in esecuzione sulla piattaforma Azure.

Questa implementazione descrive la configurazione minima richiesta del volume.

In alternativa, si potrebbe utilizzare la struttura volumetrica descritta in questa"Blog della Microsoft Technical Community".



Ambiente demo

Versioni software

Software	Versione
OS Linux	SLES PER SAP 15 SP5
SAP	SAP NetWeaver 7,5
DB2	10.5.0.7
SnapCenter	6,1

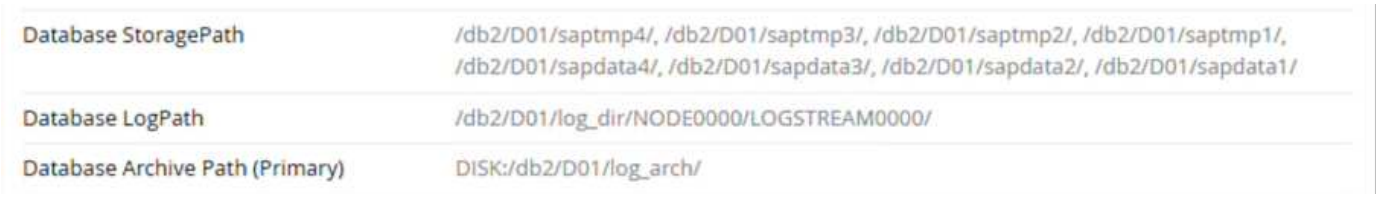
DB2 Volume Design

Il seguente Least Volume Layout deve essere utilizzato per abilitare il backup/recovery e i casi di utilizzo dei cloni per il database DB2. La configurazione di esempio utilizza <SID>: D01.

Nome volume	Directory (qtree) su Volume	Mount Point sul server	Commento
<SID>-sapdb2	db2	/db2	
		/DB2/<SID>	Directory principale per i file correlati a DB2

Nome volume	Directory (qtree) su Volume	Mount Point sul server	Commento
		/db2/db2 <sid>	Home directory degli utenti db2 <sid> e DB2 Software
		/DB2/<SID>/db2dump	DB2 Registro diagnostico e file di dump
		/DB2/<SID>/backup	Trasferimento di backup (potrebbe essere posizionato su un volume diverso)
		/DB2/<SID>/log_arch	Registri di ripetizione offline (potrebbe essere posizionato su un volume diverso, verrà attivata l'istantanea)
		/DB2/<SID>/log_dir	Registri di ripetizione online (possono essere posizionati su un volume diverso, verrà attivata l'istantanea)
	<sid>	/home/<sid> min	Home directory degli utenti <sid> adecimal
	<sid>	/home/hedge <sid>	Home directory degli utenti <sid>
	usrsaptrans	/usr/sap/trans	Directory di trasporto
	<SID>	/Usr/sap/<SID>	Usr sap
	Sapmnt<SID>	/Sapmnt/<SID>	Dir. GlobalHost SAP
Dati <SID>	sapdata1	/DB2/<SID>/sapdata1	Dati DB
	sapdata2	/DB2/<SID>/sapdata2	Dati DB
	sapdata3	/DB2/<SID>/sapdata3	Dati DB
	sapdata4	/DB2/<SID>/sapdata4	Dati DB
	saptmp1	/DB2/<SID>/saptmp1	File temp DB
	saptmp2	/DB2/<SID>/saptmp2	File temp DB
	saptmp3	/DB2/<SID>/saptmp3	File temp DB
	saptmp4	/DB2/<SID>/saptmp4	File temp DB
	db2 <sid>	/DB2/<SID>/db2 <sid>	File di istanza

Poiché il rilevamento automatico è abilitato per impostazione predefinita per il plug-in DB2, viene creato uno snapshot per i volumi che corrispondono ai seguenti percorsi di file.



Procedura per proteggere il database D01

- Controllare la distribuzione dei file, in base al layout di esempio
- Verificare i prerequisiti per l'host (vm-D01)
- Verifica dei prerequisiti per il database (D01)
- Distribuzione/installazione dell'agente SnapCenter sull'host (vm-D01)
- Creare la configurazione delle risorse di istanza di SnapCenter

Prerequisiti sull'host

Informazioni più aggiornate sono disponibili qui:

- https://docs.netapp.com/us-en/snapcenter/protect-scu/reference_prerequisites_for_adding_hosts_and_installing_snapcenter_plug_ins_package_for_linux.html
- https://docs.netapp.com/us-en/snapcenter/protect-db2/prerequisites-for-using-snapcenter-plug-in-for-ibm-db2.html

Prima di aggiungere un host e installare il pacchetto plug-in per Linux, è necessario completare tutti i requisiti.

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È possibile utilizzare l'autenticazione basata su password per l'utente root o non root oppure l'autenticazione basata su chiave SSH.
- Il plug-in SnapCenter per file system Unix può essere installato da un utente non root. Tuttavia, è necessario configurare i privilegi sudo per l'utente non root per installare e avviare il processo di plug-in. Dopo aver installato il plug-in, i processi verranno eseguiti come utenti non root.
- Creare credenziali con la modalità di autenticazione come Linux per l'utente di installazione.
- È necessario aver installato Java 11 sull'host Linux.
- Assicurarsi di aver installato solo l'edizione certificata di JAVA 11 sull'host Linux
- Per informazioni sul download di JAVA, vedere: Download di Java per tutti i sistemi operativi
- Si dovrebbe avere bash come shell di default per l'installazione del plug-in.

Prerequisiti per il database: Abilitare la registrazione e i backup

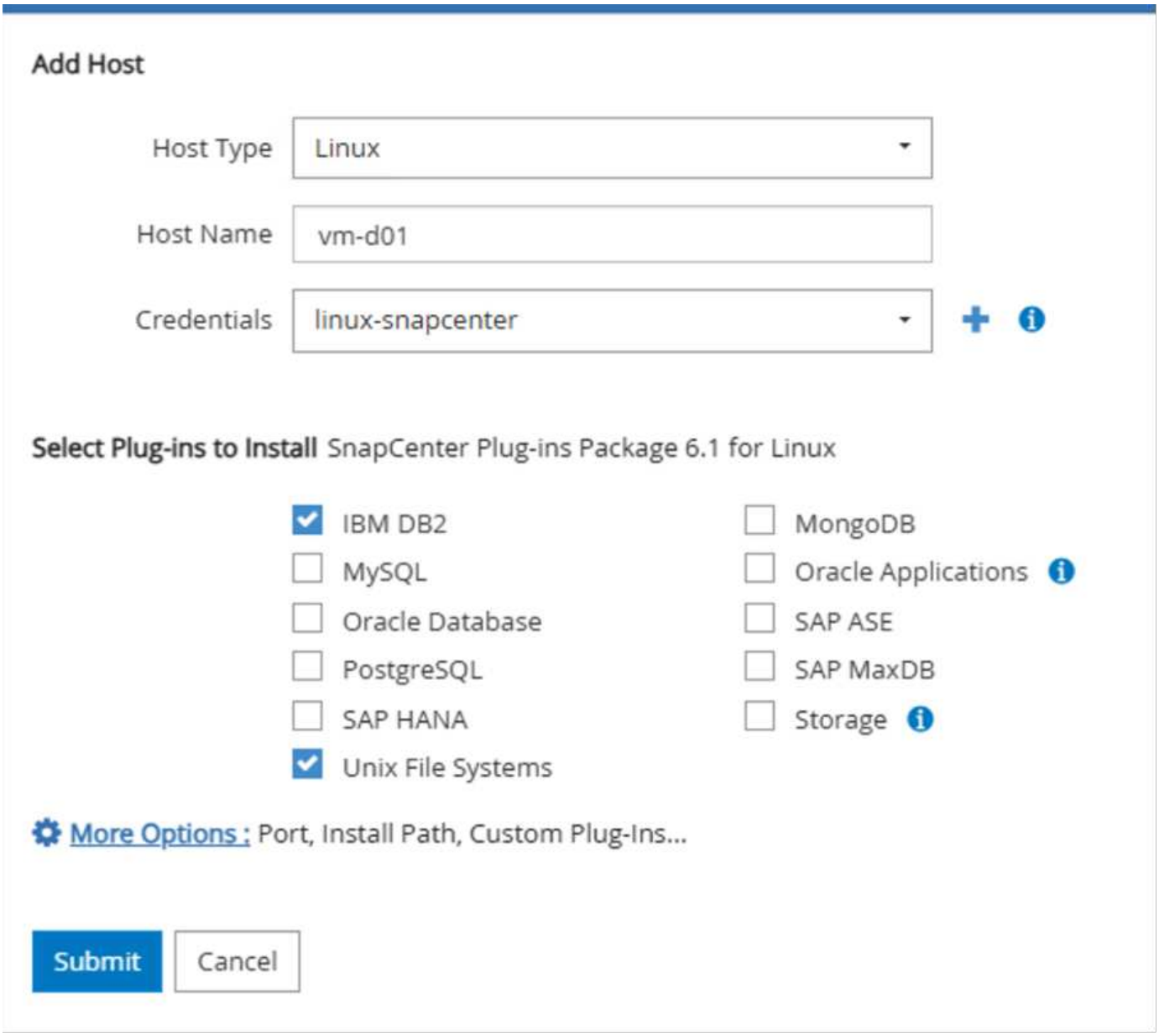
per abilitare i registri offline è necessario eseguire un backup completo del database offline. In genere è già abilitato per i sistemi produttivi.

- Creare directory per backup e log_arch (/DB2/D01/backup, /sybase/D01/log_arch)
- Attiva logarchmeth1 (come utente-sistema operativo db2d01)
  - DB2 aggiornare db cfg per D01 usando logarchmeth1 DISK:/DB2/D01/log_arch/
- Creare il backup offline (come db2d01 utente del sistema operativo)
  - db2stop forza
  - db2start accesso limitato in modalità amministratore
  - DB2 backup db D01 in /DB2/D01/backup
  - DB2 attivare db D01

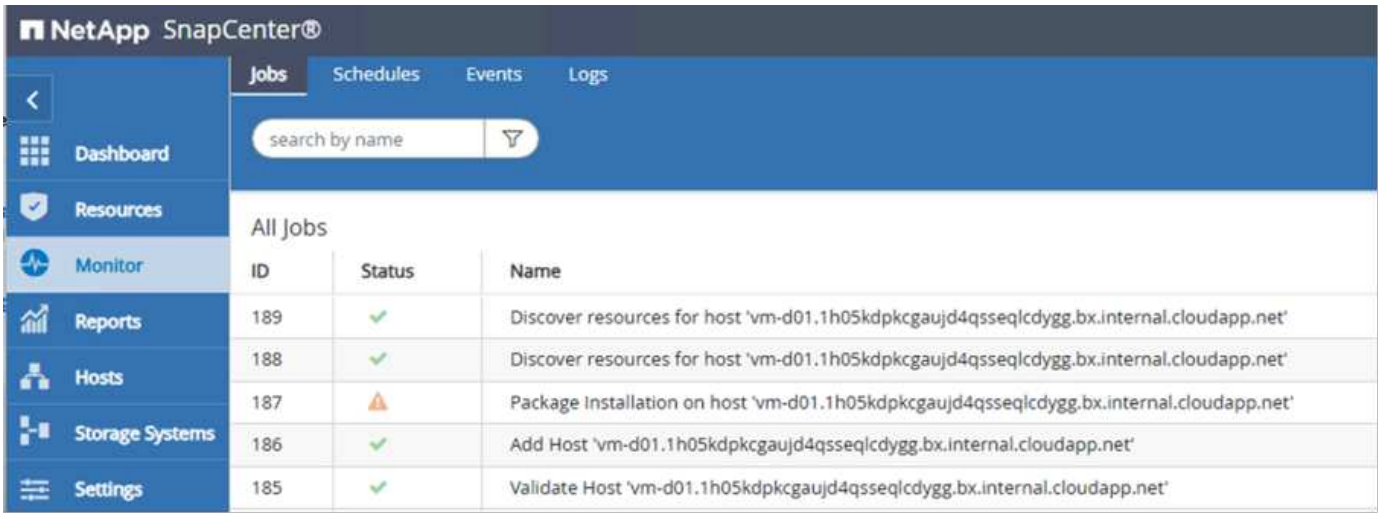
Distribuire l'agente SnapCenter per ospitare vm-D01

Ulteriori informazioni sono disponibili nella "Documentazione SnapCenter".

Selezionare IBM DB2 e Unix file Systems Plugin.



Dopo l'installazione viene attivata la ricerca dei database sull'host.

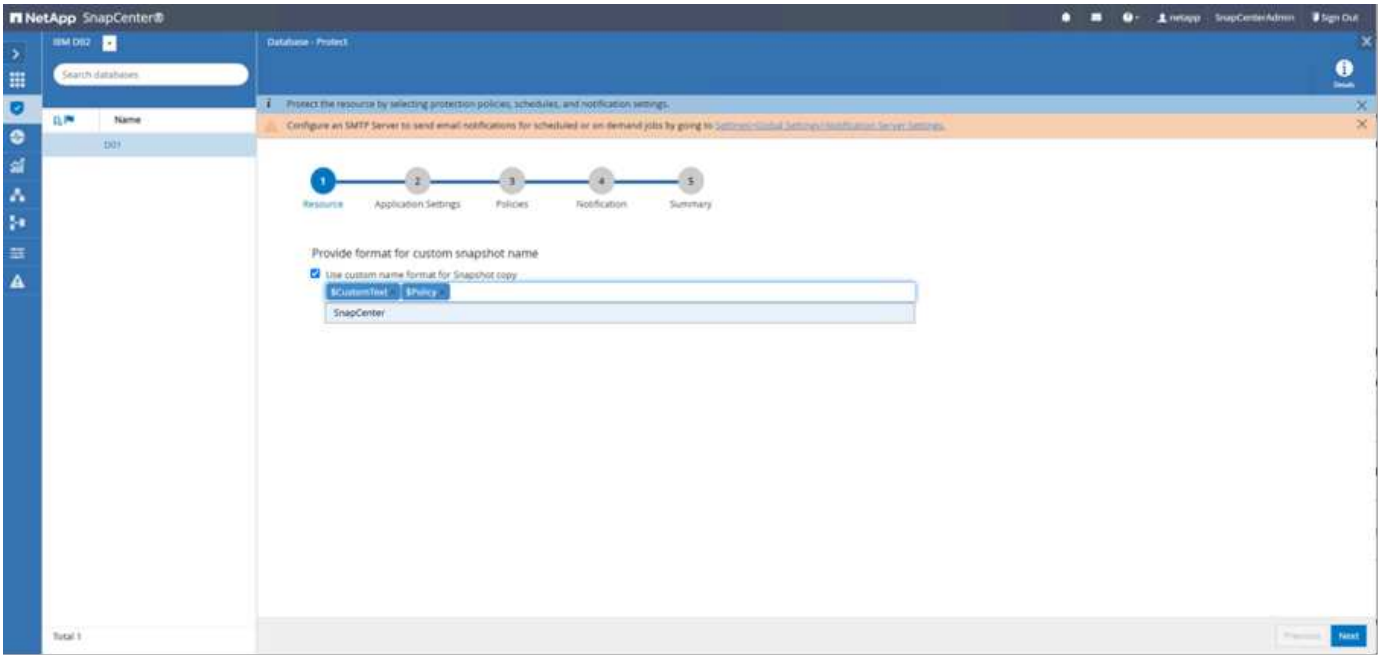


Creare la configurazione delle risorse per il database D01

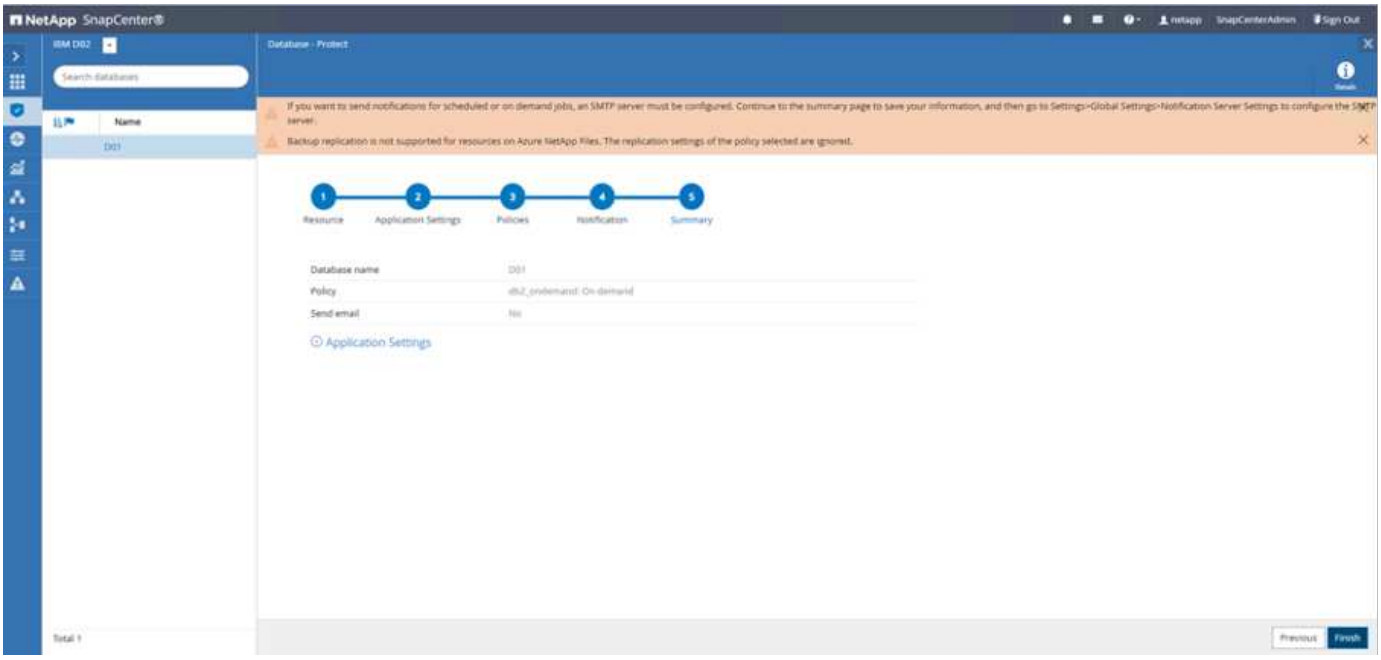
Selezionare risorsa rilevata D01



Configurare il nome dell'istantanea



Non sono richieste impostazioni specifiche dell'applicazione, configurare le impostazioni di criteri e notifiche come richiesto.



E terminare la configurazione.

Sequenza di ripristino del sistema D01

1. Arresto di SAP System D01 (incluso il database)
2. Ripristino del backup SnapCenter (volume D01-data)
   a. Smontare i file system
   b. Ripristina volume
   c. Montare i filesystem
   d. Init database as mirror db
3. Ripristino del database D01 (utilizzando il rollforward DB2)
4. Avviare il sistema SAP D01

Recuperare il database D01

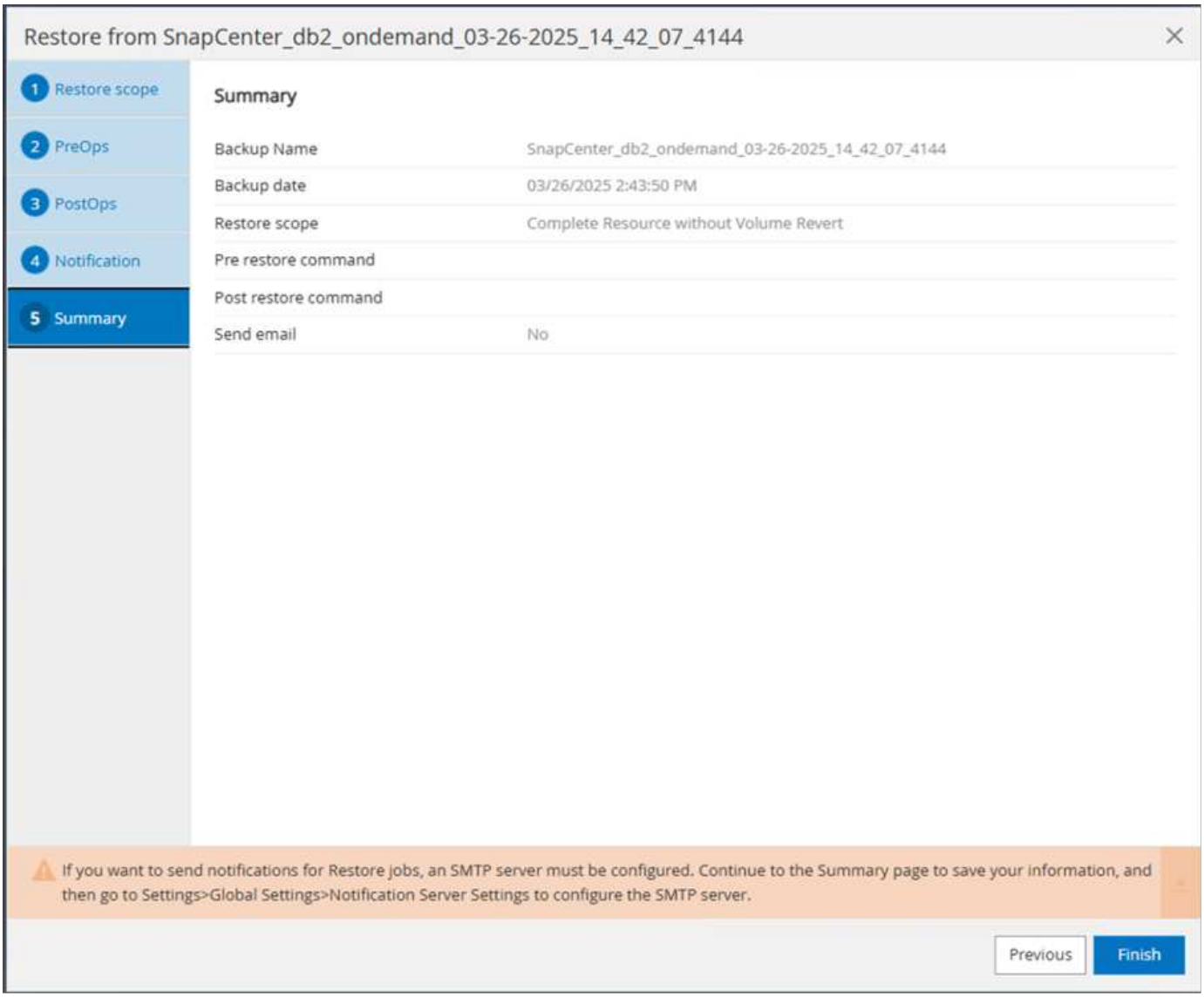
- Arrestare il sistema SAP + DB D01 sulla vm-D01 host
  - Utente d01adm: Stopsap
- Ripristina backup
  - GUI SnapCenter: Selezionare il backup richiesto per il ripristino



- Per la distribuzione ANF: È disponibile solo la risorsa completa



Viene visualizzato Summary (Riepilogo) e con Finish (fine) viene avviato il ripristino effettivo.



"db2inidb D01 come mirror" fa parte del flusso di lavoro di ripristino di SnapCenter.

- Controllare il database di stato di recupero D01 (come utente db2d01)
  - Stato query DB2 rollforward db D01
- Recuperare il database secondo necessità – qui viene inizializzato un recupero senza perdita (come utente db2d01)
  - DB2 rollforward db D01 alla fine dei log
- Arrestare il ripristino del database e il database online D01 (come utente db2d01)
  - DB2 rollforward db D01 stop
- Avviare il sistema SAP (come utente d01adm)
  - startsap

Informazioni aggiuntive e cronologia delle versioni

Le seguenti demo riportate di seguito sono disponibili a supporto della documentazione.

Installazione e configurazione DB2 Plugin, Backup del database DB2

Ripristino e ripristino del database DB2

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

- "Installazione di SAP su DB2 Azure su ANF"
- "Prerequisiti SnapCenter per i plug-in"
- "Plug-in di installazione di SnapCenter"
- "Documentazione del plugin SnapCenter DB2"
- Note SAP (accesso richiesto)
  - 83000 - DB2/390: Opzioni di backup e ripristino: https://me.sap.com/notes/83000
  - 594301 - DB6: Strumenti di amministrazione e Split Mirror: https://me.sap.com/notes/594301
- Documentazione del prodotto NetApp: https://www.netapp.com/support-and-training/documentation/
- "Soluzioni SAP di NetApp – informazioni su casi d'utilizzo, Best practice e vantaggi"

Cronologia delle versioni

Versione	Data	Cronologia della versione del documento
Versione 1.0	Aprile 2025	Versione iniziale – backup/ripristino del database DB2

Integrazione SnapCenter per database SAP MaxDB

Questo documento descrive le specifiche di integrazione di SnapCenter per SAP MaxDB Database utilizzato in un ambiente SAP.

Introduzione

Il documento non intende essere una descrizione passo passo di come configurare l'ambiente completo, ma tratterà i concetti e i dettagli relativi a:

- Esempio di panoramica della configurazione
- Esempio di layout
- Proteggere l'istanza SAP MaxDB
- Ripristinare l'istanza SAP MaxDB

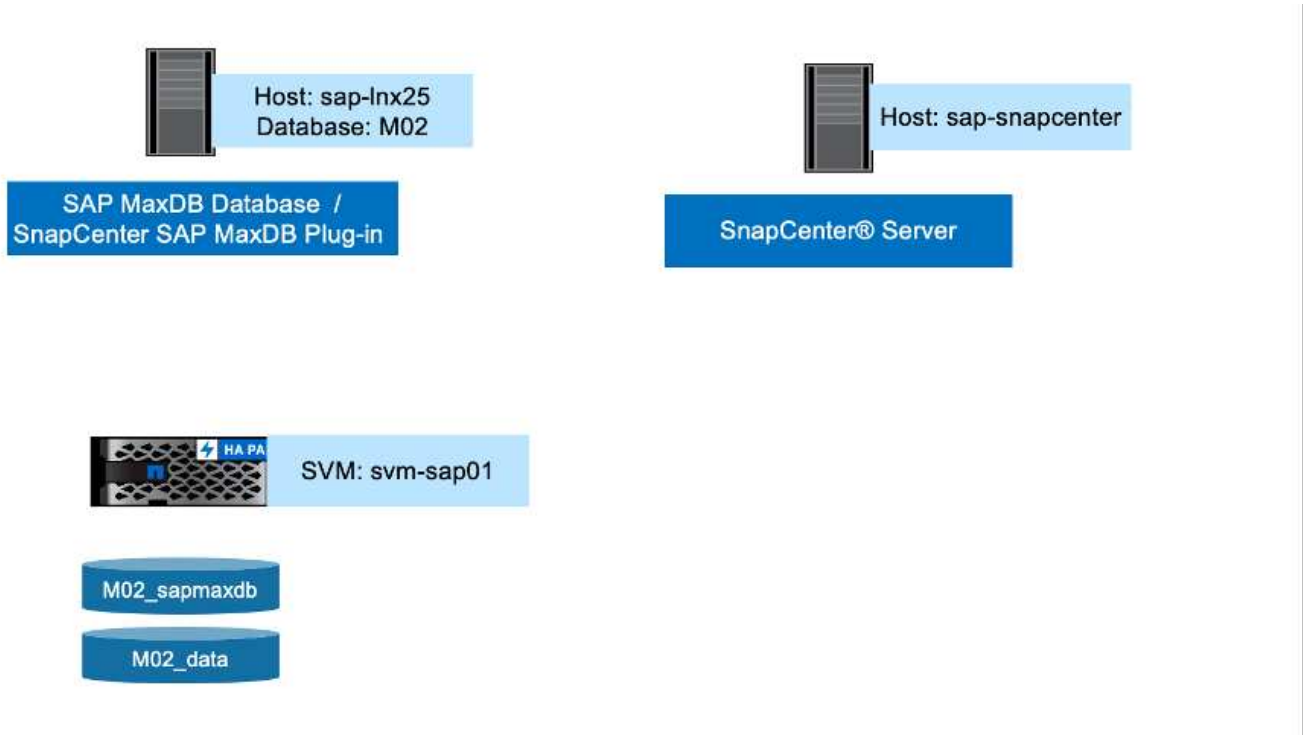
Esempio di panoramica della configurazione

Esempio di implementazione per il plugin MaxDB SnapCenter per un sistema SAP in esecuzione nel nostro Centro demo.

Questa implementazione descrive la configurazione minima richiesta del volume. I backup di data dump e log dump, il modello di backup e così via sono configurati in base alla nota SAP "1928060 - Backup e ripristino dei dati con backup del file system" e alle note di riferimento.

In alternativa, si potrebbe utilizzare la struttura volumetrica descritta in"Blog della community di MS Techcommunity".

Ambiente demo



Versioni software

Software	Versione
OS Linux	SLES PER SAP 15 SP5
SAP	SAP NetWeaver 7,5
SAP MaxDB	DBMServer 7.9.10 Build 004-123-265-969
SnapCenter	6,1

Progettazione di volumi maxdb

Il seguente layout del volume minimo deve essere utilizzato per abilitare il backup/ripristino e i casi d'utilizzo dei cloni per il database SAP MaxDB. La configurazione di esempio utilizza <SID>: M02.

Nome volume	Directory (qtree) su Volume	Mount Point sul server	Commento
<SID>_sapmaxdb	sapdb	/sapdb	Directory principale per i file correlati a MaxDB
		/sapdb/<SID>/saplog	Redo Logs (Ripristina registri) (potrebbe essere posizionato su un volume diverso)
		/sapdb/<SID>/backup	Backup dei dump (dati + registro) (possono essere posizionati su un volume diverso)

Nome volume	Directory (qtree) su Volume	Mount Point sul server	Commento
	<sid>	/home/<sid> min	Home directory degli utenti <sid> adecimal
	sdb	/home/sdb	Home directory di User sdb
	<sid>	/home/<sid>	Home directory degli utenti <sid>
	usrsaptrans	/usr/sap/trans	Directory di trasporto
	<SID>	/Usr/sap/<SID>	Usr sap
	Sapmnt<SID>	/Sapmnt/<SID>	Dir. GlobalHost SAP
<SID>_data	sapdata	/sapdb/<SID>/sapdata	File di dati DB (SID)

Procedura per proteggere il database M02

- Controllare la distribuzione dei file, in base al layout di esempio
- Verificare i prerequisiti per l'host (sap-lnx25)
- Verifica dei prerequisiti per il database (M02)
- Distribuzione/installazione dell'agente SnapCenter sull'host (sap-lnx25)
- Creare la configurazione delle risorse di istanza di SnapCenter

Prerequisiti sull'host

Potrebbero essere disponibili informazioni più aggiornate "qui".

Prima di aggiungere un host e installare il pacchetto plug-in per Linux, è necessario completare tutti i requisiti.

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È possibile utilizzare l'autenticazione basata su password per l'utente root o non root oppure l'autenticazione basata su chiave SSH.
- Il plug-in SnapCenter per file system Unix può essere installato da un utente non root. Tuttavia, è necessario configurare i privilegi sudo per l'utente non root per installare e avviare il processo di plug-in. Dopo aver installato il plug-in, i processi verranno eseguiti come utenti non root.
- Creare credenziali con la modalità di autenticazione come Linux per l'utente di installazione.
- È necessario aver installato Java 11 sull'host Linux.
- Assicurarsi di aver installato solo l'edizione certificata di JAVA 11 sull'host Linux
- Per informazioni sul download di JAVA, vedere: Download di Java per tutti i sistemi operativi
- Si dovrebbe avere bash come shell di default per l'installazione del plug-in.

Prerequisiti per il database: Creazione di modelli di backup, attivazione del backup di accesso

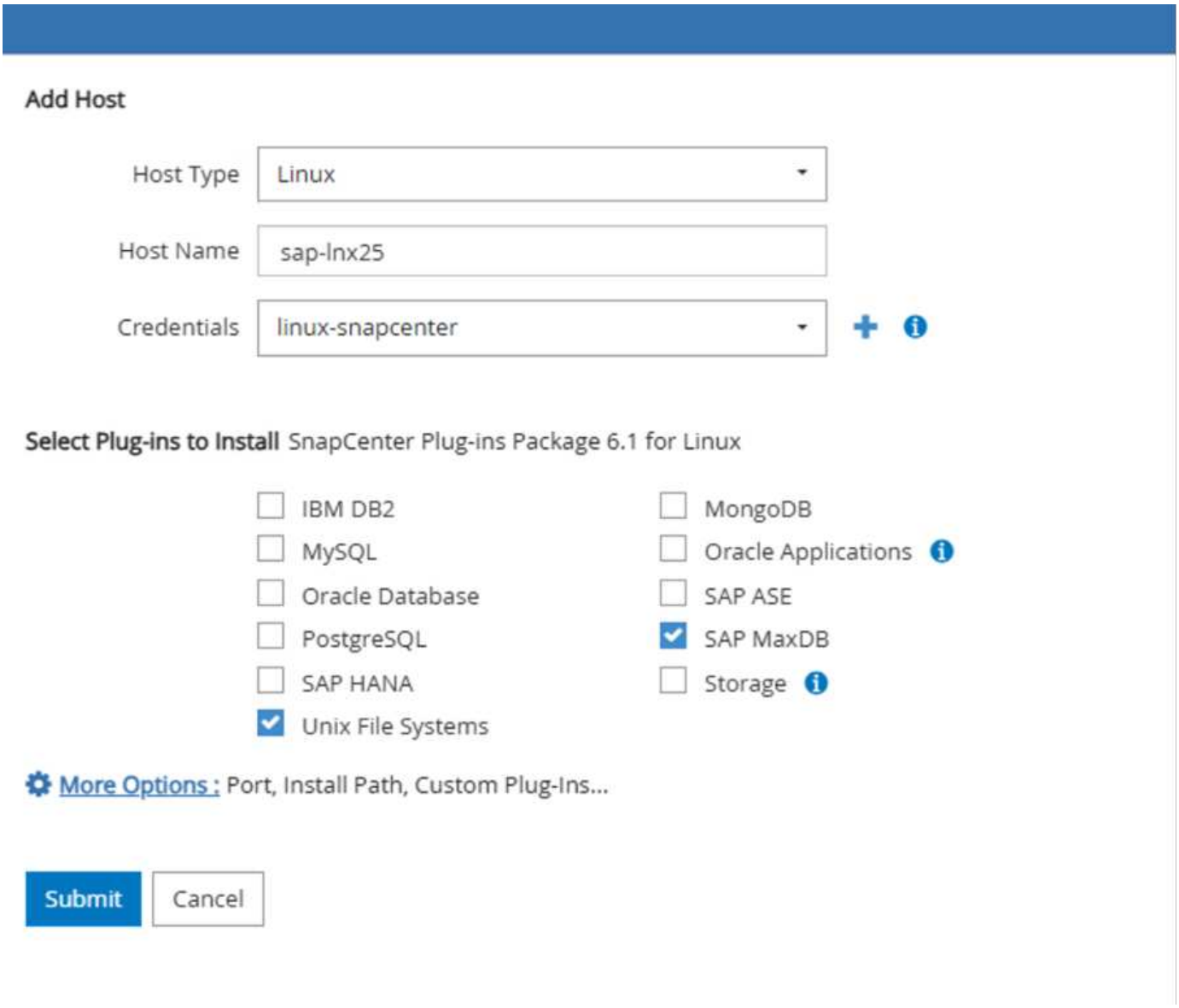
- Creare directory per il backup di dati e log (/sapdb/M02/backup/data, /sapdb/M02/backup/log – owner sdb:sdba – Permissions 755)
- Connettersi al database M02 (come utente OS sqdm02)

    - Dbmcli -d M02 -u CONTROL,<password>
- Creare un modello di backup dei file di dati (M02_DATA) secondo la nota SAP 1928060
    - Backup_template_create M02_DATA nel FILE /sapdb/M02/backup/DATA/M02_DATA content DATA
- Creare un modello di backup dei dati (M02_LOG) in base alla nota SAP 1928060
    - Backup_template_create M02_LOG nel FILE /sapdb/M02/backup/log/M02_log content log
- Creare un modello di backup Data Snapshot (M02_SNAP) in base alla nota SAP 1928060
    - Backup_template_create M02_SNAP su UNO SNAPSHOT ESTERNO
- Create Fake-Backup per attivare il backup del REGISTRO
    - util_connect
    - Backup_start M02_SNAP
    - Backup_finish M02_SNAP ExternalBackupID first_full_fake_backup
- Passare alla modalità di registrazione del database
    - arresto automatico
    - autolog_on INTERVALLO M02_LOG 300
    - autolog_show

Distribuire l'agente SnapCenter per ospitare sap-lnx25

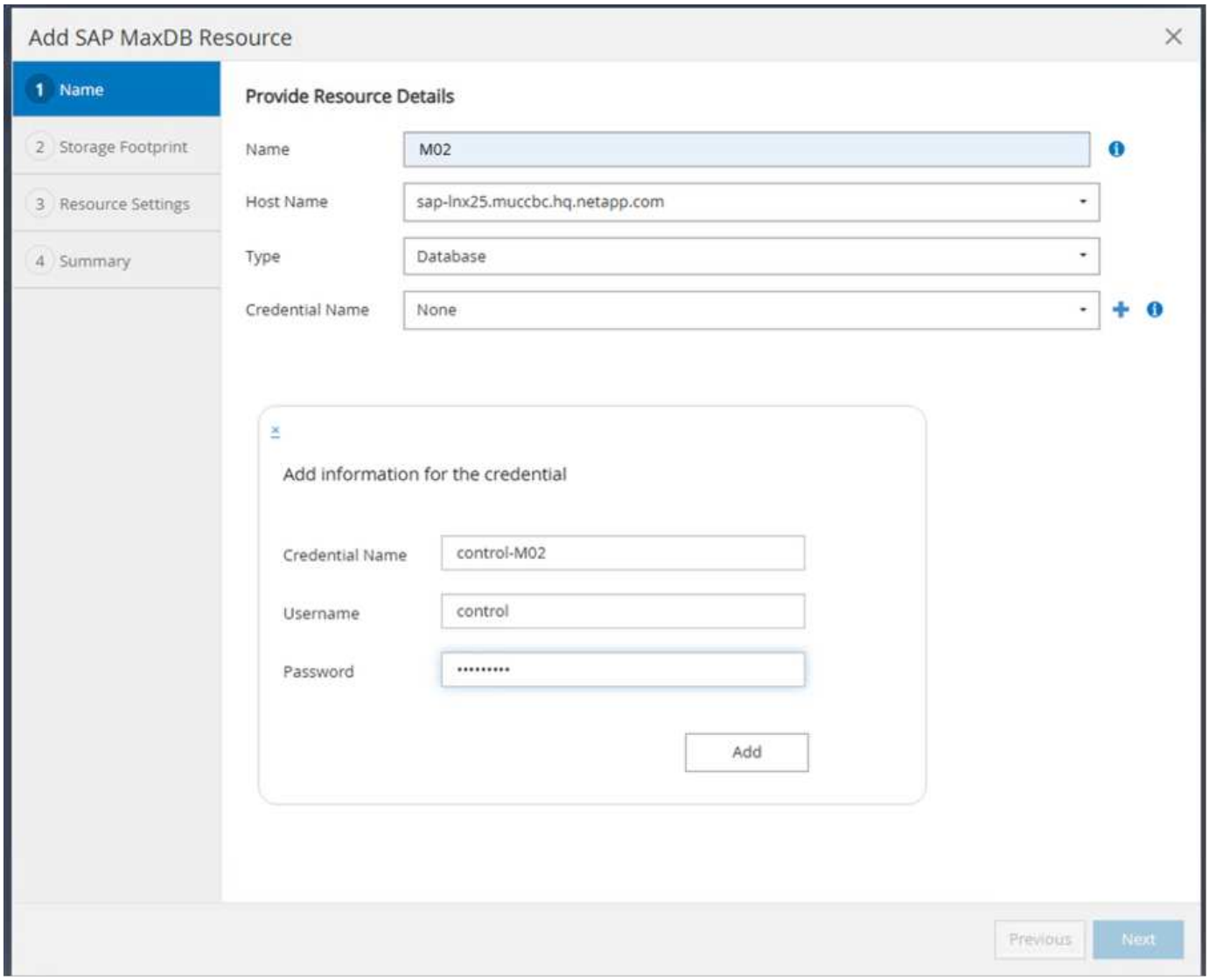
Ulteriori informazioni sono disponibili nella "Documentazione SnapCenter".

Selezionare SAP MaxDB e Unix file Systems Plugin.

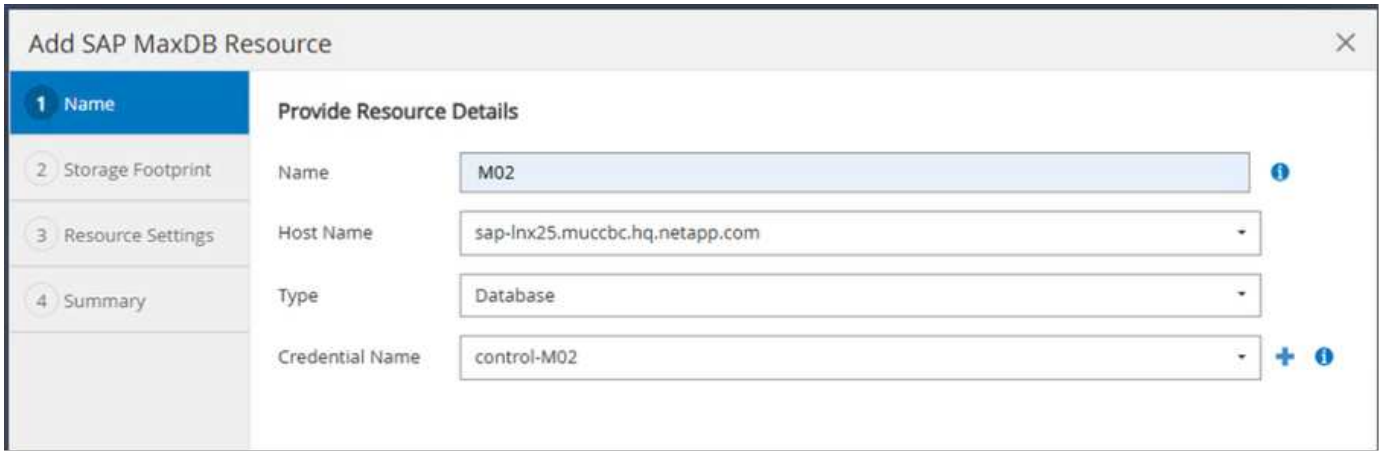


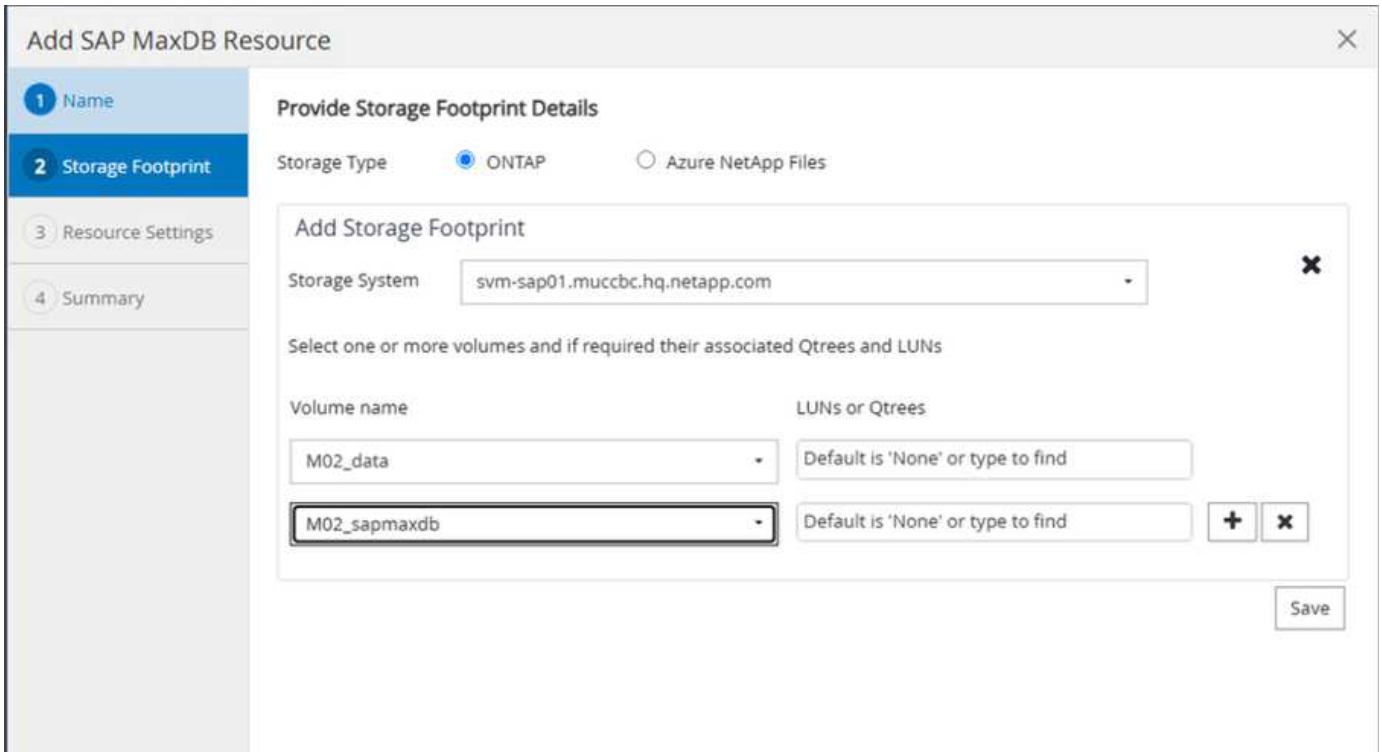
Creare la configurazione delle risorse SnapCenter per il database M02

Risorse → SAP MaxDB → Aggiungi risorse

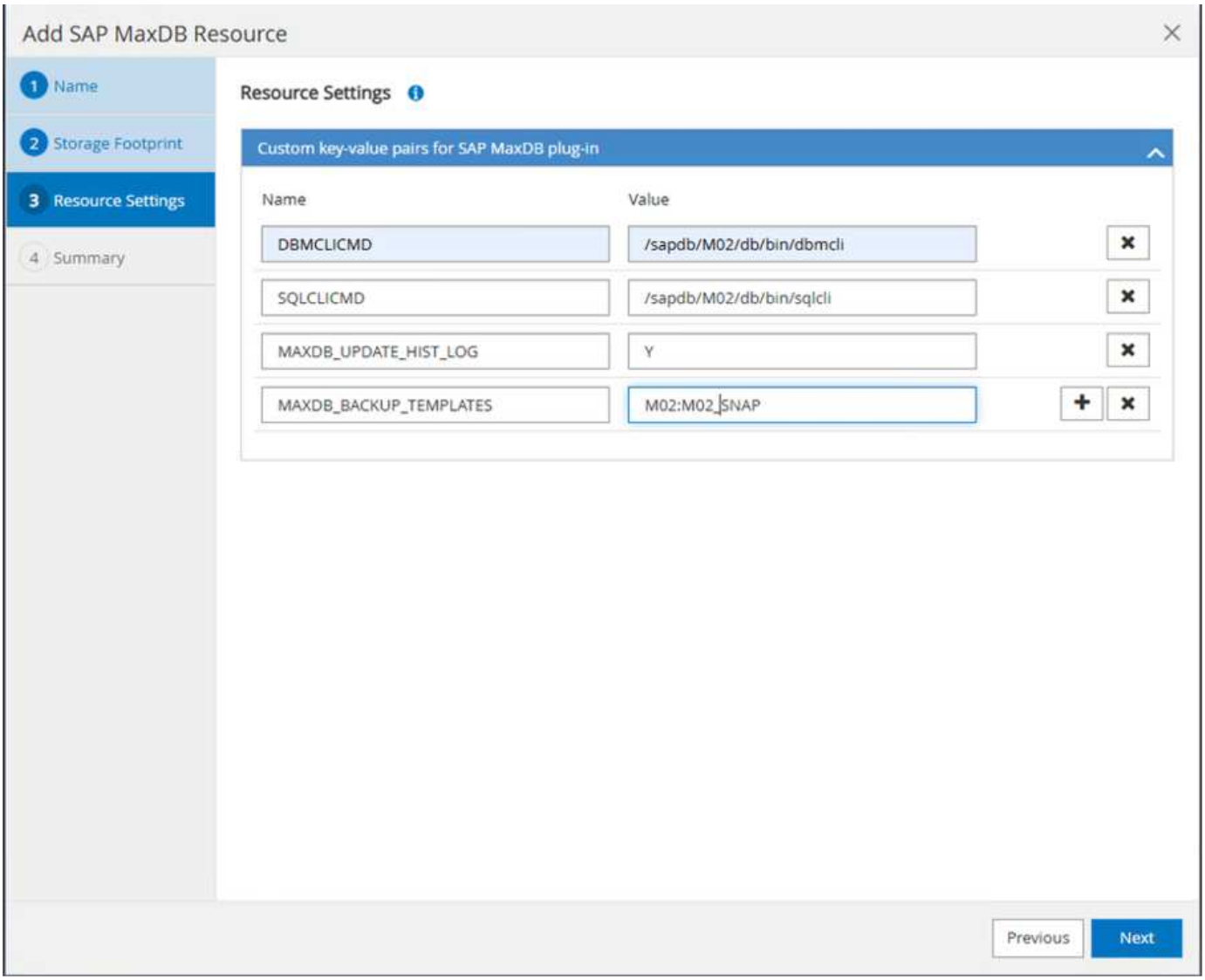


Se la password contiene caratteri speciali, è necessario mascherarli con una barra rovesciata (ad esempio Test!123! → Test\!123\!).





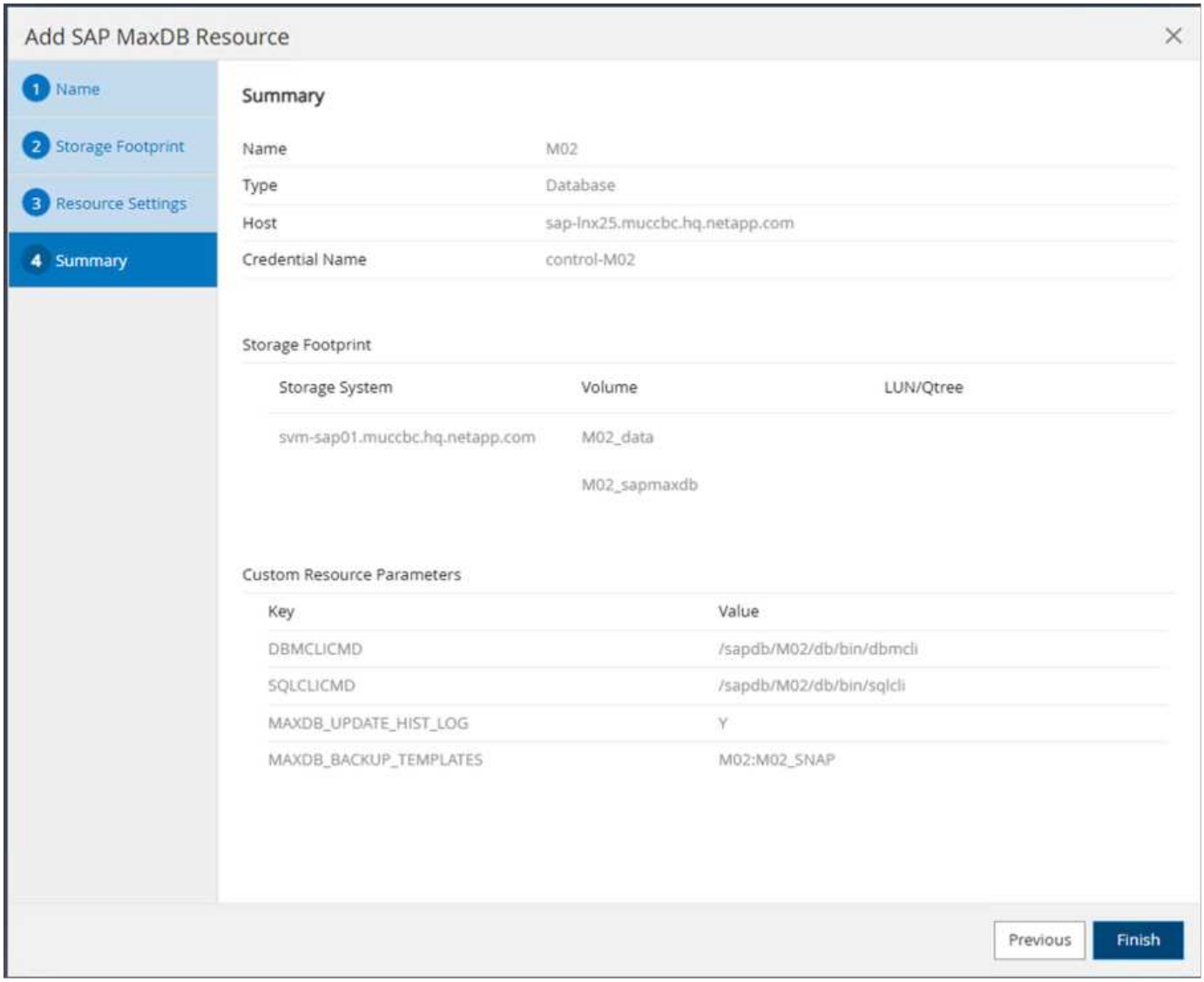
È necessario effettuare (almeno) coppie chiave-valore personalizzate nelle seguenti impostazioni delle risorse.



La seguente tabella elenca i parametri del plug-in MaxDB, ne fornisce le impostazioni e li descrive:

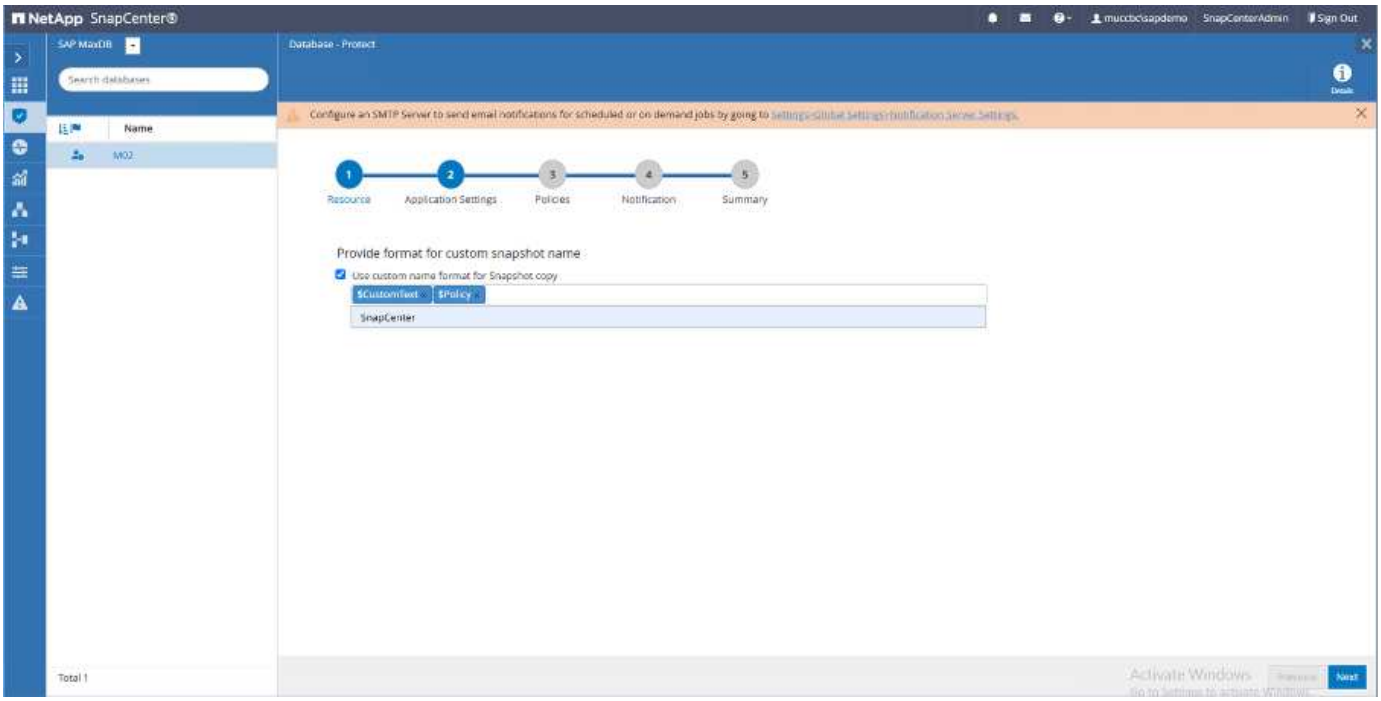
Parametro	Impostazione	Descrizione
HANDLE_LOGWRITER	(Y / N)	Esegue le operazioni di sospensione del logwriter (N) o ripristino del logwriter (Y).
DBMCLICMD	path_to_dbmcli_cmd	Specifica il percorso del comando MaxDB dbmcli.se non impostato, viene utilizzato dbmcli sul percorso di ricerca.
SQLCLICMD	percorso_a_sqlcli_cmd	Specifica il percorso per il comando sqlcli di MaxDB.se non impostato, sqlcli viene utilizzato nel percorso di ricerca.
MAXDB_UPDATE_HIST_LOG	(Y / N)	Indica al programma di backup di MaxDB se aggiornare o meno il registro della cronologia di MaxDB.

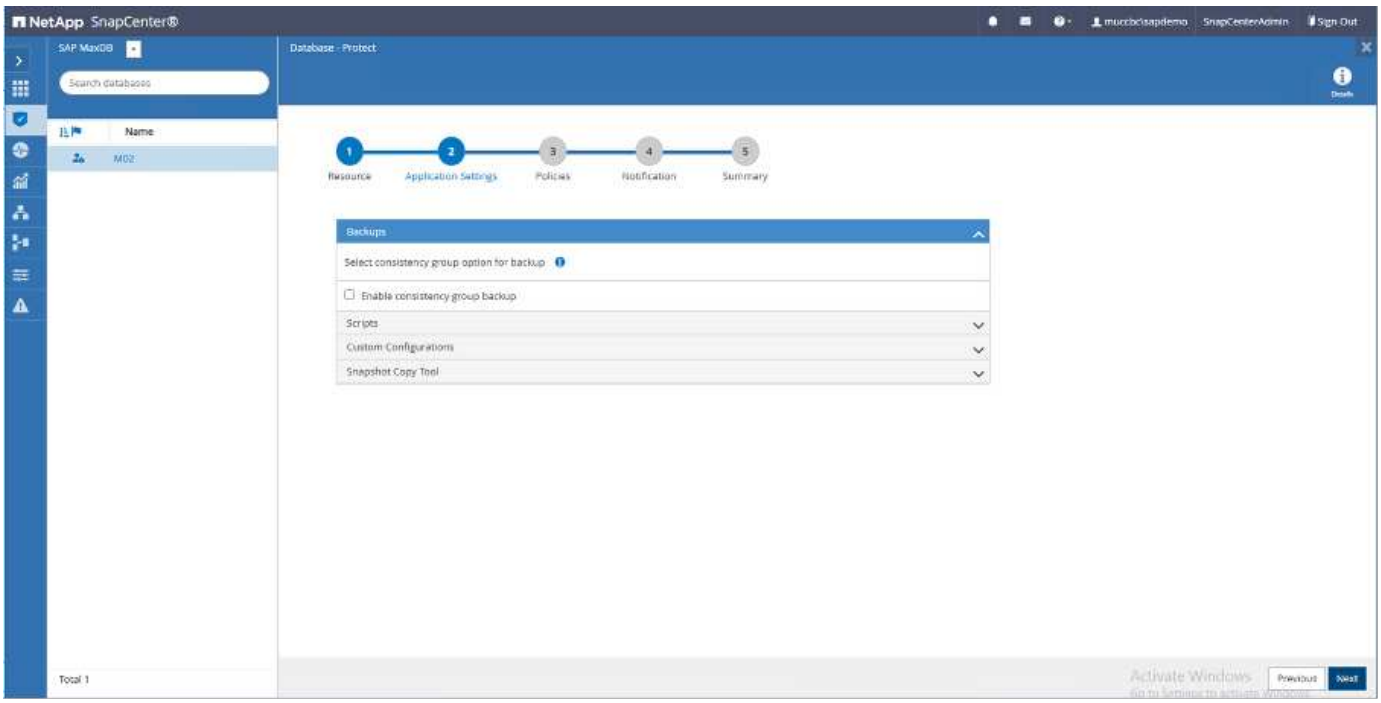
Parametro	Impostazione	Descrizione
MAXDB_BACKUP_TEMPLATES	nome_modello (ad esempio `M02_SNAP`)	Specifica un modello di backup per ogni database. Il modello deve già esistere ed essere un tipo esterno di modello di backup. Per abilitare l'integrazione delle copie Snapshot per MaxDB 7.8 e versioni successive, è necessario disporre della funzionalità server in background di MaxDB e del modello di backup di MaxDB già configurato.
MAXDB_BG_SERVER_PREFIX	bg_server_prefix (ad esempio `na_bg`)	Specifica il prefisso per il nome del server in background. Se il parametro MAXDB_BACKUP_TEMPLATES è impostato, è necessario impostare anche IL parametro MAXDB_BG_SERVER_PREFIX. Se non si imposta il prefisso, viene utilizzato il valore predefinito na_bg_DATABASE.

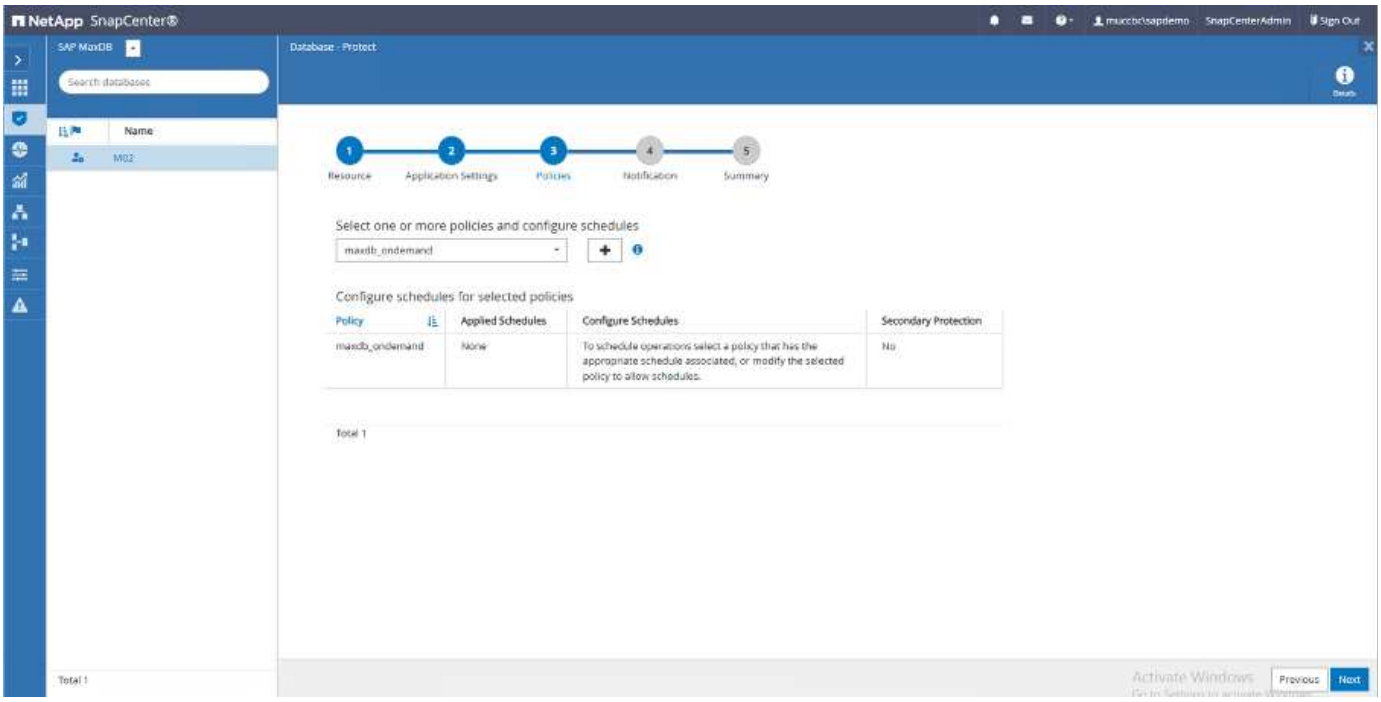


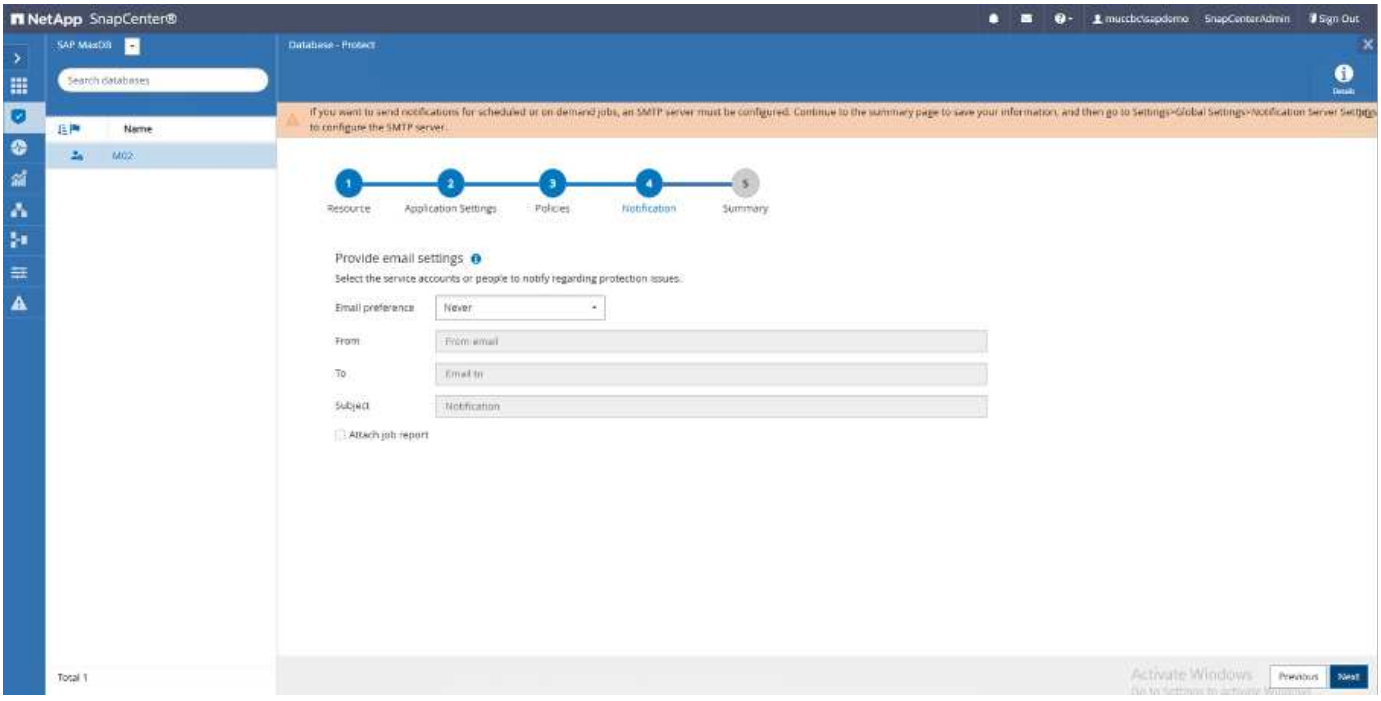
A questo punto, la configurazione potrebbe essere completata e Backup pianificato in base al concetto di protezione generale.

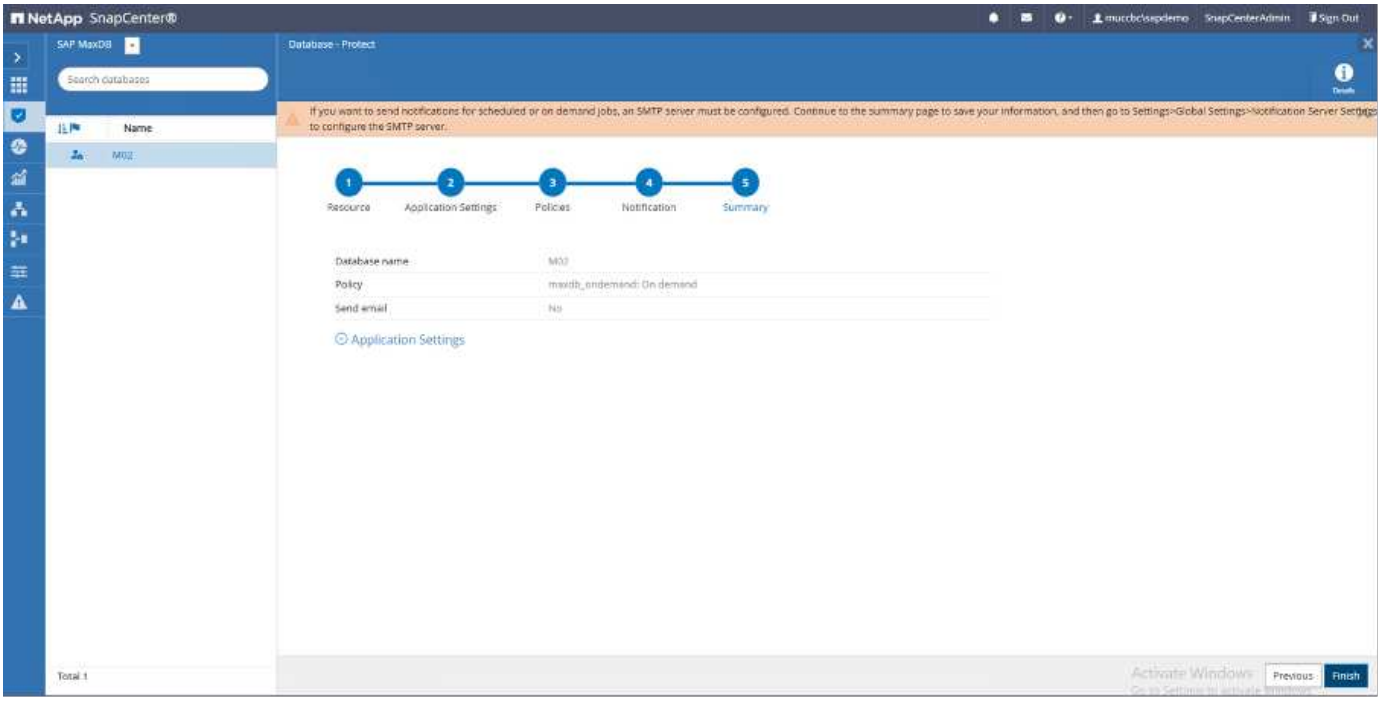

NetApp SnapCenter®
SAP MaxDB
View
Database
Search databases
Dashboard
Resources
Monitor
Reports
Hosts
Storage Systems
Settings
Alerts
Name
Type
Host
Resource Groups
Policies
Last backup
Overall Status
M02
Database
Not protected


NetApp SnapCenter®
SAP MaxDB
Search databases
Name
M02
Total 1
Database - Protect
Configure an SMTP Server to send email notifications for scheduled or on demand jobs by going to Settings>Global Settings>Notification Server Settings.
1 Resource
2 Application Settings
3 Policies
4 Notification
5 Summary
Provide format for custom snapshot name
Use custom name format for Snapshot copy
$CustomText
$Policy
SnapCenter
Next


NetApp SnapCenter®
SAP MaxDB
Search databases
Name
M02
Total 1
Database - Protect
1 Resource
2 Application Settings
3 Policies
4 Notification
5 Summary
Backups
Select consistency group option for backup
Enable consistency group backup
Scripts
Custom Configurations
Snapshot Copy Tool
Previous
Next


NetApp SnapCenter®
muccbc\sapdemo
SnapCenterAdmin
Sign Out
SAP MaxDB
Search databases
Name
M02
Total 1
Database - Protect
Details
1 Resource
2 Application Settings
3 Policies
4 Notification
5 Summary
Select one or more policies and configure schedules
maxdb_ondemand
Configure schedules for selected policies
Policy
Applied Schedules
Configure Schedules
Secondary Protection
maxdb_ondemand
None
To schedule operations select a policy that has the appropriate schedule associated, or modify the selected policy to allow schedules.
No
Total 1
Activate Windows
Previous
Next


NetApp SnapCenter®
muccbc\sapdemo
SnapCenterAdmin
Sign Out
SAP MaxDB
Search databases
Name
M02
Total 1
Database - Protect
Details
If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.
1 Resource
2 Application Settings
3 Policies
4 Notification
5 Summary
Provide email settings
Select the service accounts or people to notify regarding protection issues.
Email preference
Never
From
From email
To
Email to
Subject
Notification
Attach job report
Activate Windows
Previous
Next

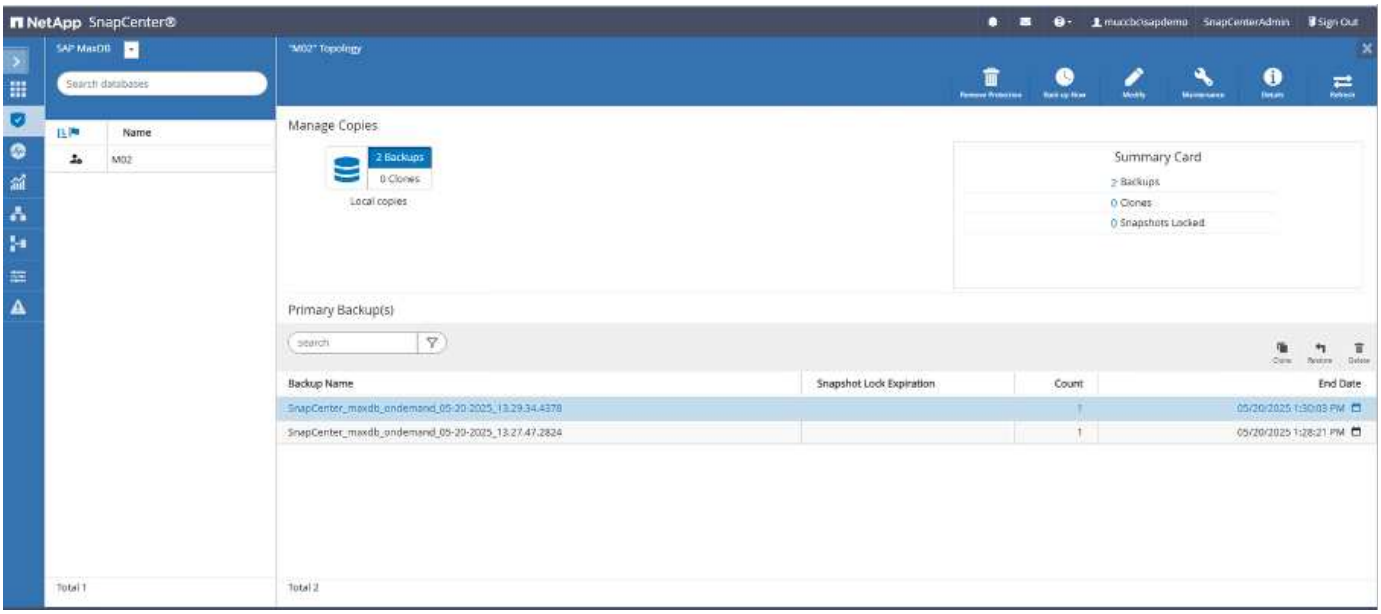


Sequenza di ripristino del sistema M02

1. Arrestare SAP System M02 (incluso il database), arrestare sapinit
2. Umount filesystem /sapdb/M02/sapdata
3. Ripristino dei volumi M02_data (utilizzando SnapCenter)
4. Montare il filesystem /sapdb/M02/sapdata
5. Avviare il database M02 e connettersi (modalità amministratore)
6. Raccogliere informazioni di backup
7. ripristinare il backup dei dati del database
8. ripristinare i backup dei log dei database
9. arrestare il database
10. Avviare sapinit, sistema SAP M02

Recupera istanza M02

- Arrestare SAP System + DB M02 sull'host sap-lnx25
  - Utente m02adm: Stopsap
  - Facoltativo – se il database non è stato arrestato correttamente – utente: sqdm02
  - Dbmcli -d M02 -u CONTROL,<password>
    - db_offline
  - Utente root: /Etc/init.d/sapinit stop
  - Utente root: Umount /sapdb/M02/sapdata
- Ripristina backup
  - SnapCenter GUI (GUI): Selezionare il tipo richiesto per il ripristino

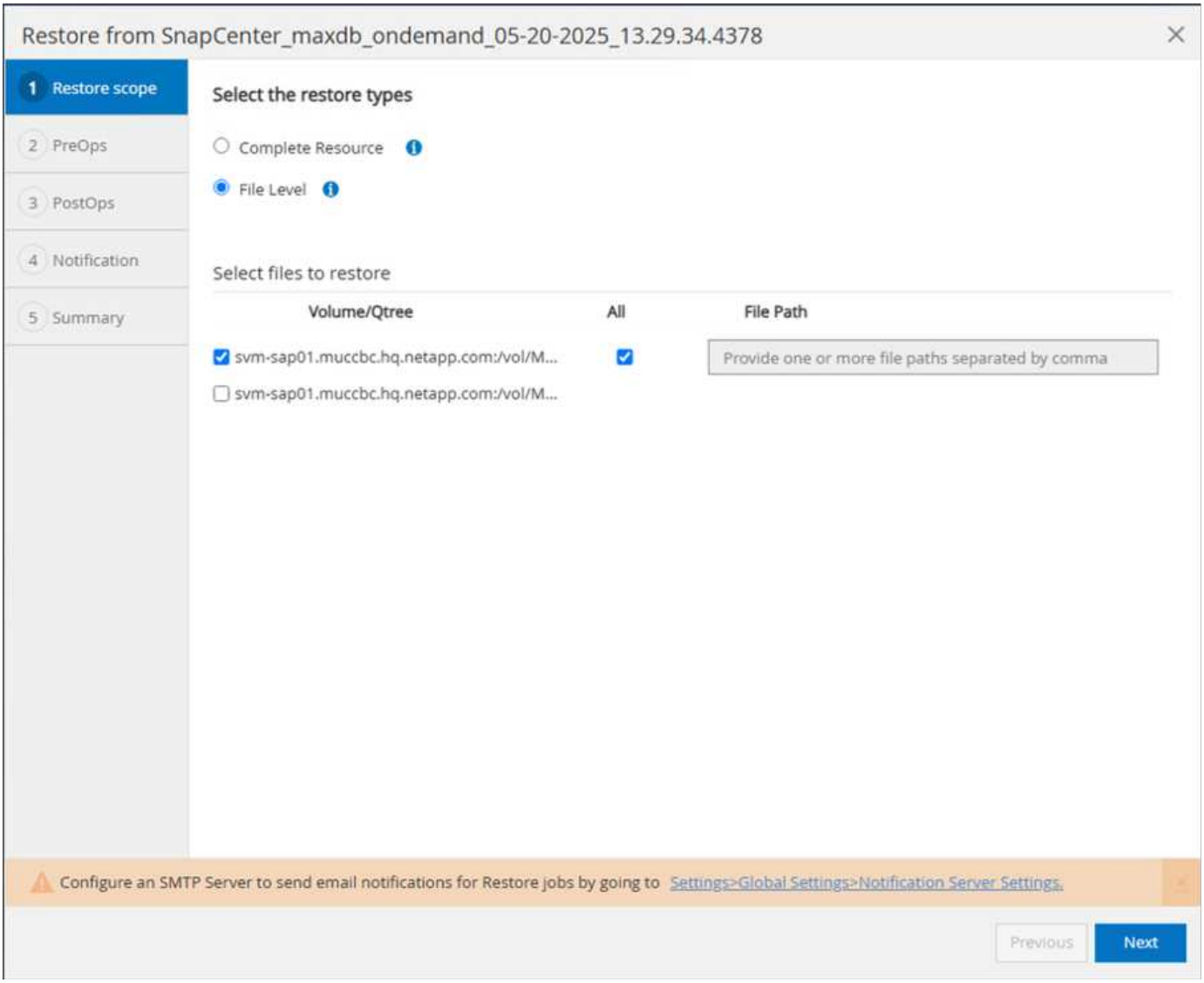


Se si seleziona complete Resource (risorsa completa), viene attivato un VBSR (Volume Based Snap Restore). All'interno di Azure viene chiamato "ripristino volume". Per la distribuzione ANF **è disponibile solo la risorsa completa**.

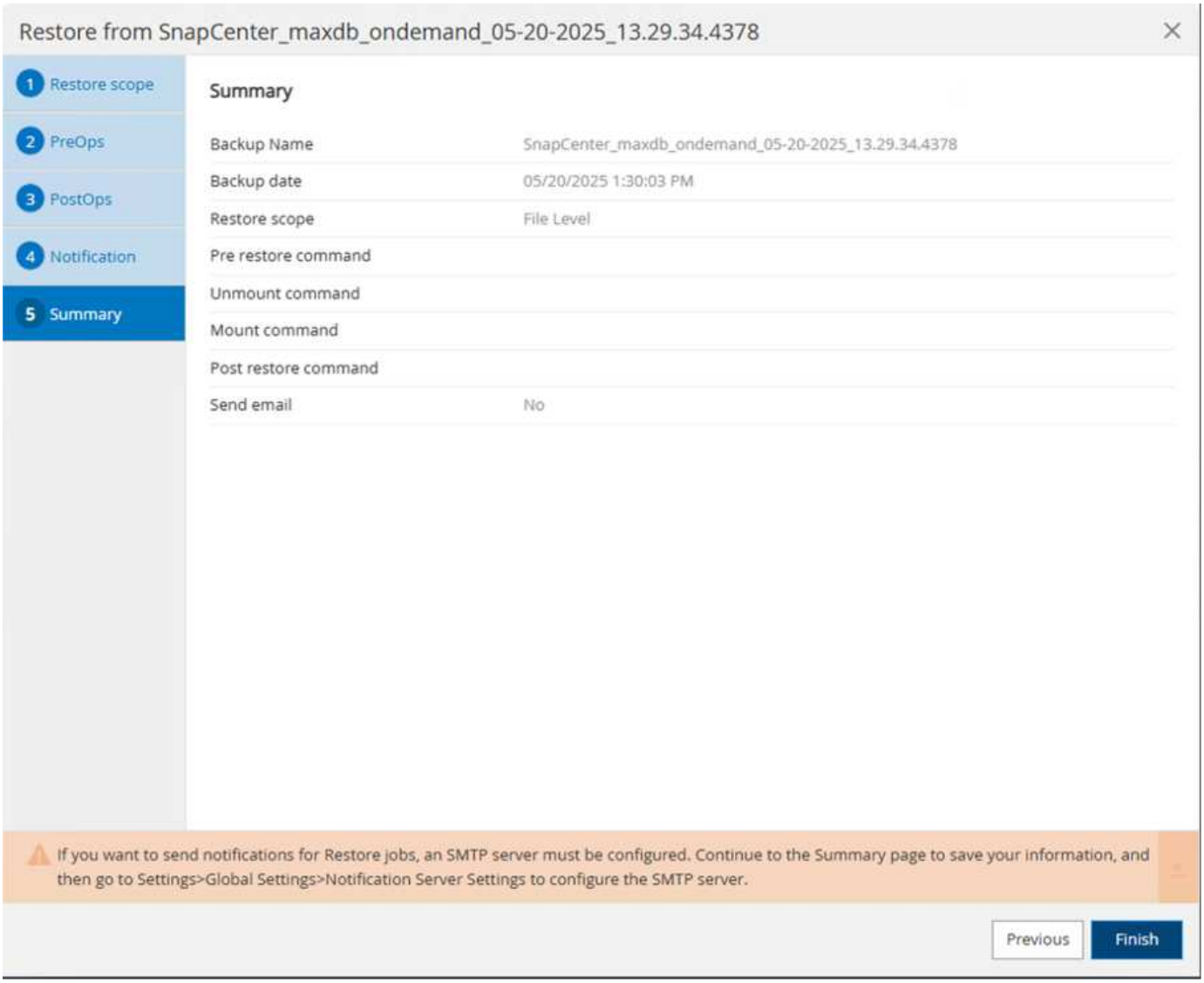
Important

Active filesystem data and snapshots that were taken after the selected snapshot will be lost. The snapshot revert operation will replace *all* the data in the targeted volume with the data in the selected snapshot. You should pay attention to the snapshot contents and creation date when you select a snapshot. You cannot undo the snapshot revert operation.

Per altri tipi di distribuzione (ad esempio, on-premise ANF) è possibile orchestrare un'operazione SFSR (Single file Snap Restore). Selezionare file Level (livello file) e il volume corrispondente e selezionare "All" (tutti). Vedere la seguente schermata.



Viene visualizzato Summary (Riepilogo) e con Finish (fine) viene avviato il ripristino effettivo.



- Montare i file system (sap-lnx25)
  - Utente root: Mount /sapdb/M02/sapdata
- Avviare Database M02 in modalità amministratore e connettersi
  - Utente: sqdm02: Dbmcli -d M02 -u CONTROL,<password>
    - db_admin
    - db_connect
- Raccogliere informazioni di backup
  - backup_history_open
  - backup_history_list -c label,action,pages,stop,media -r last

```
dbmcli on M02>backup_history_list -c label,action,pages,stop,media -r last
OK
END
DAT_000000008|SAVE WARM|         0|2025-05-20 13:29:50|M02_SNAP

---
```

- Ripristino del database

◦ Ripristina backup dei dati

▪ Recover_start M02_SNAP data ExternalBackupID DAT_000000008

```
dbmcli on M02>recover_start M02_SNAP data ExternalBackupID DAT_000000008
OK
Returncode              0
Date                    20250520
Time                    00151550
Server                  sap-lnx25
Database                M02
Kernel Version          Kernel    7.9.10   Build 004-123-265-969
Pages Transferred       0
Pages Left
Volumes
Medianame               M02_SNAP
Location
Errortext
Label                   DAT_000000008
Is Consistent           true
First LOG Page          512226
Last LOG Page
DB Stamp 1 Date         20250520
DB Stamp 1 Time         00132933
DB Stamp 2 Date
DB Stamp 2 Time
Page Count
Devices Used            0
Database ID             sap-lnx25:M02_20241203_104036
Max Used Data Page      3187892
Converter Page Count

---
```

◦ Recuperare il backup del registro secondo necessità

▪ Ad esempio, Recover_start M02_LOG LOG 147

```
[dbmcli on M02>recover_start M02_LOG LOG 147
OK
Returncode              0
Date                    20250521
Time                    00112001
Server                  sap-lnx25
Database                M02
Kernel Version          Kernel    7.9.10   Build 004-123-265-969
Pages Transferred       24
Pages Left              0
Volumes                 1
Medianame               M02_LOG
Location                /sapdb/M02/backup/log/M02_LOG.147
Errortext
Label                   LOG_000000147
Is Consistent
First LOG Page          514072
Last LOG Page           514075
DB Stamp 1 Date         20250520
DB Stamp 1 Time         00180238
DB Stamp 2 Date         20250520
DB Stamp 2 Time         00180539
Page Count              4
Devices Used            1
Database ID             sap-lnx25:M02_20241203_104036
Max Used Data Page
Converter Page Count
```

- Informazioni opzionali – autorecover a un indicatore orario specifico (senza necessità di specificare dati dedicati / backp di registro
  - ad esempio, autorecover fino al 20250520 200000

```
---
[dbmcli on M02>autorecover until 20250520 200000
OK
Returncode              0
Date                    20250521
Time                    00131559
Server                  sap-lnx25
Database                M02
Kernel Version          Kernel    7.9.10   Build 004-123-265-969
Pages Transferred       10096
Pages Left              0
Volumes                 1
Medianame               M02_LOG
Location                /sapdb/M02/backup/log/M02_LOG.102
Errortext
Label                   LOG_000000102
Is Consistent
First LOG Page          256227
Last LOG Page           341559
DB Stamp 1 Date         20241203
DB Stamp 1 Time         00190348
DB Stamp 2 Date         20241226
DB Stamp 2 Time         00193615
Page Count              85333
Devices Used            1
Database ID             sap-lnx25:M02_20241203_104036
Max Used Data Page
Converter Page Count

---
```

- Terminare il recupero e arrestare il database

- db_offline

> Ulteriori informazioni sul ripristino sono disponibili nella "Documentazione maxdb"

- Avviare il sistema SAP
  - Utente root: /Etc/init.d/sapinit start
  - Utente m02adm: Startsap

Informazioni aggiuntive e cronologia delle versioni

Demo registrate

Le seguenti demo riportate di seguito sono disponibili a supporto della documentazione.

Installazione MaxDB Plugin, Configurazione MaxDB Plugin, Backup del database MaxDB

Ripristino e ripristino del database MaxDB

Documentazione esterna

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

- "Installazione SAP Azure su ANF"
- "Prerequisiti SnapCenter per i plug-in"
- "Plug-in di installazione di SnapCenter"
- "Documentazione di ripristino maxdb"
- Note SAP (accesso richiesto)
  - "1928060 - Backup e ripristino dei dati con backup del file system"
  - "2282054 - Server DBM in background"
  - "616814 - Sospendi il masterizzatore di log per il mirror diviso o l'istantanea"
- "HOWTO - SAP MaxDB Backup con Database Manager CLI"
- "HOWTO - recupero SAP MaxDB con CLI di Database Manager"
- "Documentazione sui prodotti NetApp"
- "Soluzioni SAP di NetApp – informazioni su casi d'utilizzo, Best practice e vantaggi"

Cronologia delle versioni

Versione	Data	Cronologia della versione del documento
Versione 1.0	Maggio 2025	Versione iniziale – backup / ripristino database MaxDB

Gestione del ciclo di vita

NetApp SAP Landscape Management Integration con Ansible

TR-4953: Integrazione della gestione del panorama SAP di NetApp con Ansible

SAP Landscape Management (lama) consente agli amministratori di sistema SAP di automatizzare le operazioni del sistema SAP, incluse le operazioni end-to-end di cloning, copia e refresh del sistema SAP.

Autori: Michael Schlosser, Nils Bauer, NetApp

NetApp offre un'ampia gamma di moduli Ansible che consentono a SAP lama di accedere a tecnologie come NetApp Snapshot e FlexClone attraverso SAP lama Automation Studio. Queste tecnologie aiutano a semplificare e accelerare le operazioni di cloning, copia e refresh del sistema SAP.

L'integrazione può essere utilizzata dai clienti che eseguono le soluzioni di storage NetApp on-premise o dai clienti che utilizzano i servizi di storage NetApp presso provider di cloud pubblico come Amazon Web Services, Microsoft Azure o Google Cloud Platform.

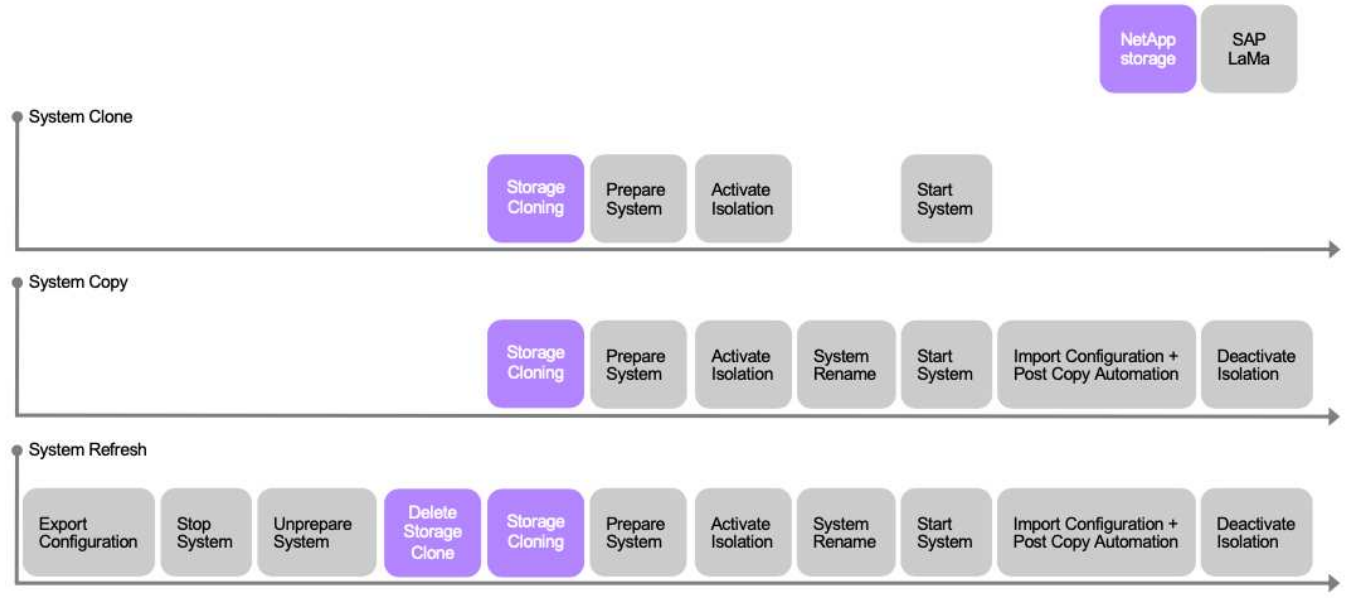
Questo documento descrive la configurazione di SAP lama con le funzionalità di storage NetApp per le operazioni di copia, clonazione e refresh del sistema SAP utilizzando l'automazione Ansible.

Scenari di cloning, copia e refresh del sistema SAP

Il termine copia del sistema SAP viene spesso utilizzato come sinonimo per tre diversi processi: Clone del sistema SAP, copia del sistema SAP o refresh del sistema SAP. È importante distinguere tra le diverse operazioni, in quanto i flussi di lavoro e i casi di utilizzo sono diversi per ciascuno di essi.

- **Clone di sistema SAP.** un clone di sistema SAP è un clone identico di un sistema SAP di origine. I cloni di sistema SAP vengono in genere utilizzati per affrontare la corruzione logica o per testare gli scenari di disaster recovery. Con un'operazione di clone del sistema, il nome host, il numero di istanza e il SID rimangono invariati. È quindi importante stabilire un corretto scherma di rete per il sistema di destinazione per assicurarsi che non vi sia comunicazione con l'ambiente di produzione.
- **SAP system copy.** una copia del sistema SAP è una configurazione di un nuovo sistema SAP di destinazione con i dati di un sistema SAP di origine. Il nuovo sistema di destinazione potrebbe essere, ad esempio, un sistema di test aggiuntivo con i dati del sistema di produzione. Il nome host, il numero di istanza e il SID sono diversi per i sistemi di origine e di destinazione.
- **SAP system refresh.** un refresh del sistema SAP è un refresh di un sistema SAP di destinazione esistente con i dati di un sistema SAP di origine. Il sistema di destinazione fa generalmente parte di un ambiente di trasporto SAP, ad esempio un sistema di quality assurance, che viene aggiornato con i dati del sistema di produzione. Il nome host, il numero di istanza e il SID sono diversi per i sistemi di origine e di destinazione.

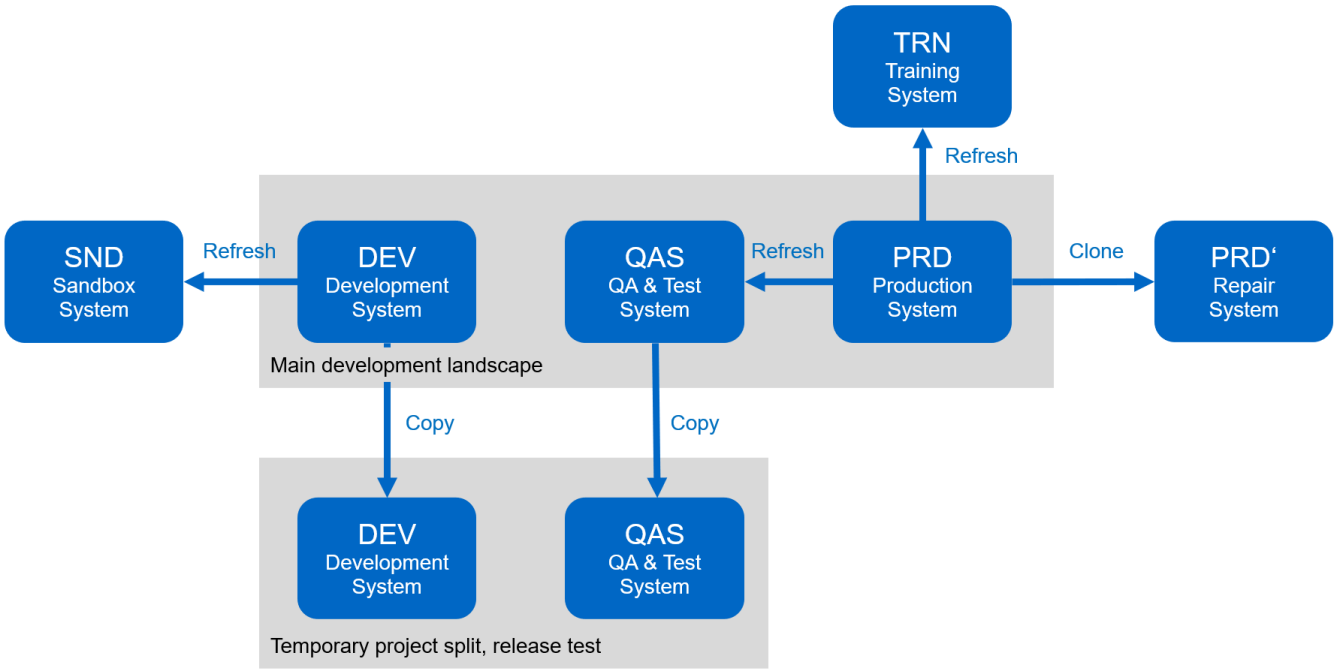
La figura seguente illustra i passaggi principali da eseguire durante un'operazione di clonazione del sistema, copia del sistema o aggiornamento del sistema. Le caselle viola indicano i passaggi in cui è possibile integrare le funzionalità di storage NetApp. Tutte e tre le operazioni possono essere completamente automatizzate utilizzando SAP lama.



Casi d'utilizzo per l'aggiornamento, la copia e la clonazione del sistema

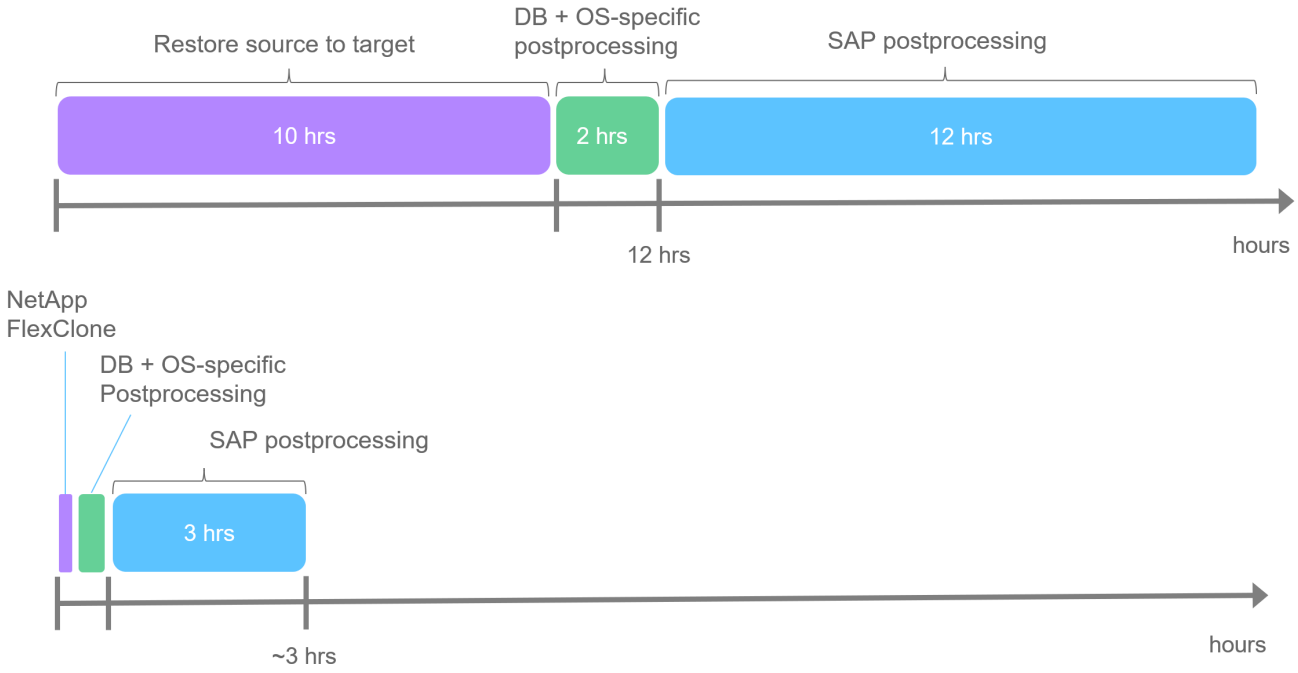
Esistono diversi scenari in cui i dati di un sistema di origine devono essere resi disponibili a un sistema di destinazione per scopi di test o formazione. Questi sistemi di test e formazione devono essere aggiornati regolarmente con i dati del sistema di origine per assicurarsi che i test e la formazione vengano eseguiti con il set di dati corrente.

Queste operazioni di refresh del sistema consistono in più attività a livello di infrastruttura, database e applicazioni, che possono richiedere più giorni a seconda del livello di automazione.



I flussi di lavoro di clonazione SAP lama e NetApp possono essere utilizzati per accelerare e automatizzare le attività richieste a livello di infrastruttura e database. Invece di ripristinare un backup dal sistema di origine al

sistema di destinazione, SAP lama utilizza la copia Snapshot di NetApp e la tecnologia FlexClone di NetApp, in modo che le attività richieste fino a un database HANA avviato possano essere eseguite in pochi minuti invece che in ore, come mostrato nella figura seguente. Il tempo necessario per il processo di cloning è indipendente dalle dimensioni del database, pertanto è possibile creare anche sistemi molto grandi in un paio di minuti. Un'ulteriore riduzione del runtime viene ottenuta automatizzando le attività a livello di sistema operativo e database, nonché a livello di post-elaborazione SAP.



Risolvere il danneggiamento logico

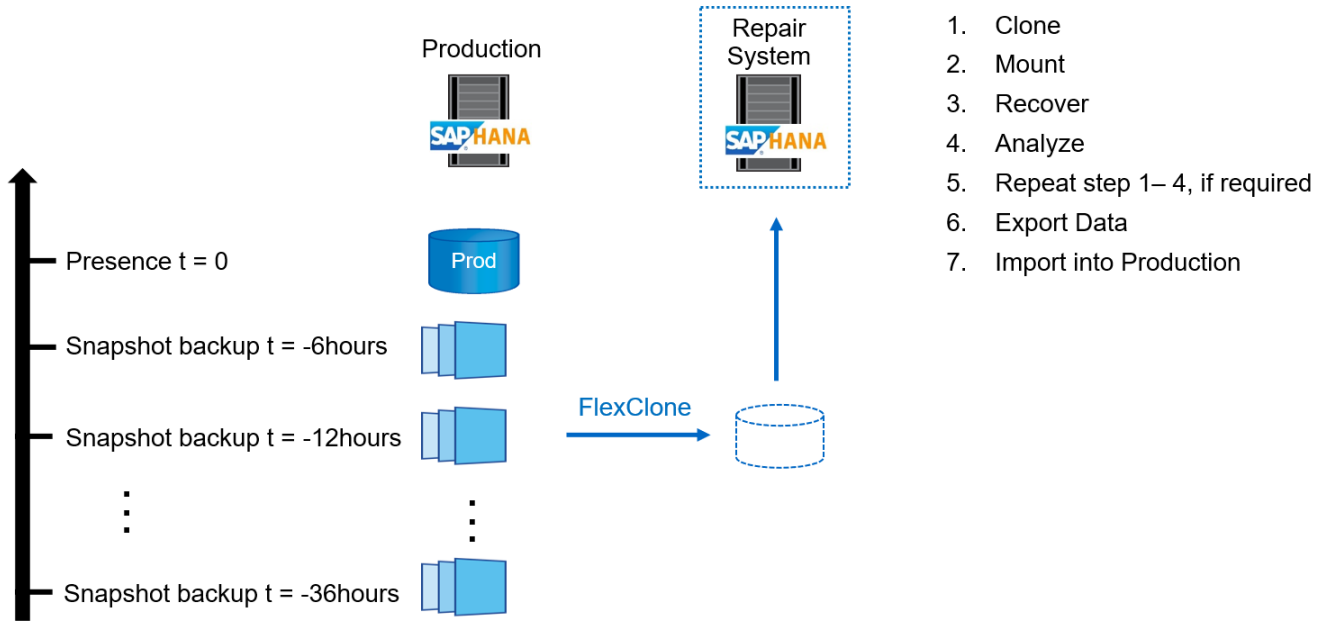
La corruzione logica può essere causata da errori software, errori umani o sabotaggio. Purtroppo, spesso la corruzione logica non può essere affrontata con soluzioni standard di alta disponibilità e disaster recovery. Di conseguenza, a seconda del livello, dell'applicazione, del file system o dello storage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

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

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

Quando si configura il sistema di riparazione, la flessibilità e la velocità sono fondamentali. Con i backup Snapshot basati su storage NetApp, sono disponibili più immagini di database coerenti per creare un clone del

sistema di produzione utilizzando la tecnologia NetApp FlexClone. I volumi FlexClone possono essere creati in pochi secondi anziché in più ore se per configurare il sistema di riparazione viene utilizzato un ripristino reindirizzato da un backup basato su file.

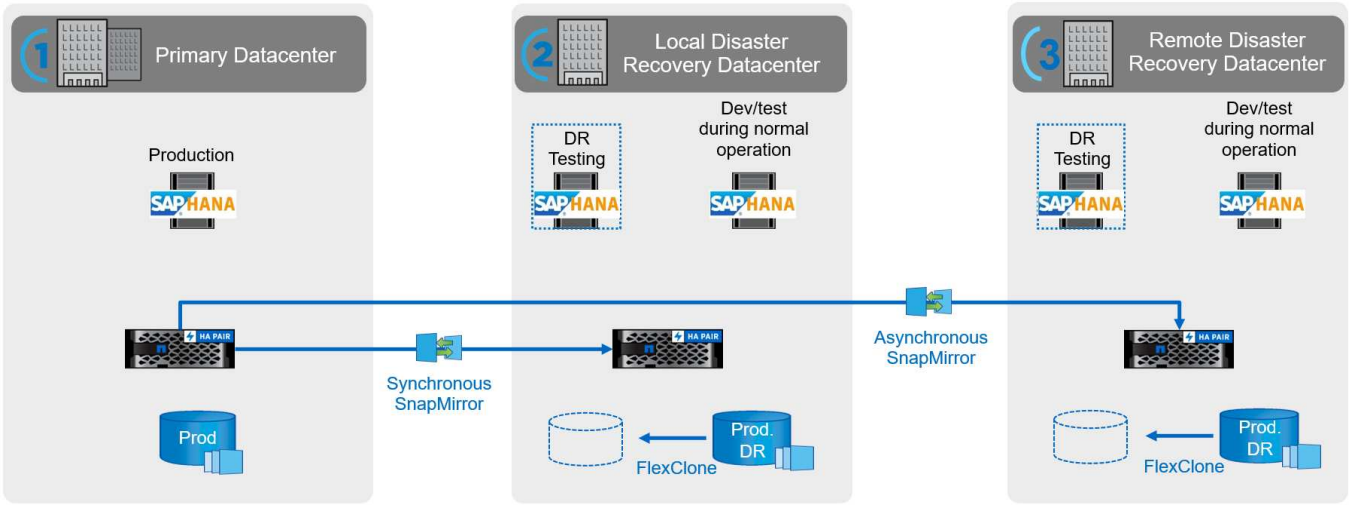


Test di disaster recovery

Una strategia di disaster recovery efficace richiede la verifica del flusso di lavoro richiesto. I test dimostrano se la strategia funziona e se la documentazione interna è sufficiente. Consente inoltre agli amministratori di seguire le procedure richieste.

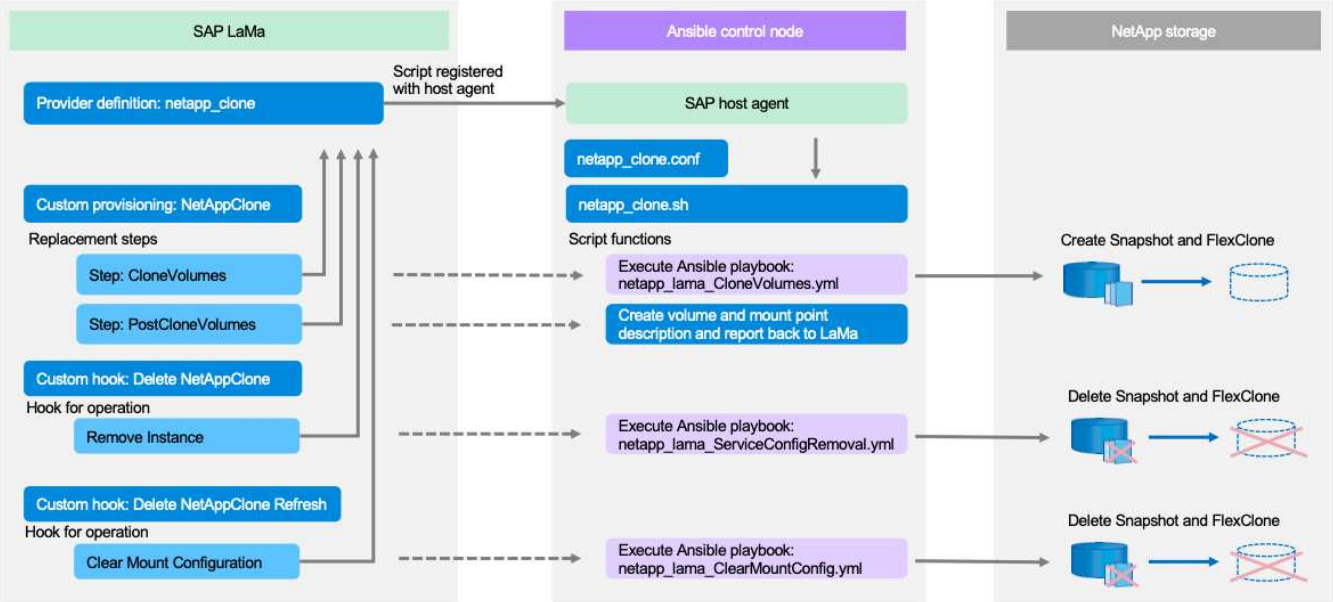
La replica dello storage con SnapMirror consente di eseguire test di disaster recovery senza mettere a rischio RTO e RPO. I test di disaster recovery possono essere eseguiti senza interrompere la replica dei dati. I test di disaster recovery per SnapMirror asincrono e sincrono utilizzano i backup Snapshot e i volumi FlexClone alla destinazione del disaster recovery.

SAP lama può essere utilizzato per orchestrare l'intera procedura di test e si occupa anche di scherma di rete, manutenzione degli host di destinazione e così via.



Integrazione di NetApp SAP lama con Ansible

L'approccio all'integrazione utilizza il provisioning personalizzato e gli hook operativi di SAP lama combinati con i playbook Ansible per la gestione dello storage NetApp. La figura seguente mostra una panoramica di alto livello della configurazione dal lato lama e dei componenti corrispondenti dell'implementazione dell'esempio.



Un host centrale che agisce come nodo di controllo Ansible viene utilizzato per eseguire le richieste da SAP lama e per attivare le operazioni di storage NetApp utilizzando i playbook Ansible. I componenti dell'agente host SAP devono essere installati su questo host in modo che l'host possa essere utilizzato come gateway di comunicazione per SAP lama.

In lama Automation Studio, viene definito un provider registrato presso l'agente host SAP dell'host Ansible. Un file di configurazione dell'agente host punta a uno script shell chiamato da SAP lama con un insieme di parametri della riga di comando, a seconda dell'operazione richiesta.

All'interno di lama Automation Studio, vengono definiti il provisioning personalizzato e un hook personalizzato per eseguire le operazioni di cloning dello storage durante il provisioning e anche durante le operazioni di cleanup quando il sistema viene deprovisioning. Lo script della shell sul nodo di controllo Ansible esegue quindi i corrispondenti playbook Ansible, che attivano le operazioni Snapshot e FlexClone, nonché l'eliminazione dei cloni con il flusso di lavoro di deprovisioning.

Ulteriori informazioni sui moduli Ansible di NetApp e sulle definizioni dei provider lama sono disponibili all'indirizzo:

- "Moduli NetApp Ansible"
- "Documentazione SAP lama – definizioni dei provider"

Esempio di implementazione

A causa dell'elevato numero di opzioni disponibili per le configurazioni di sistema e storage, l'implementazione di esempio deve essere utilizzata come modello per i requisiti

di configurazione e configurazione del sistema.

> Gli script di esempio vengono forniti così come sono e non sono supportati da NetApp. Puoi richiedere la versione corrente degli script via email a ng-sapcc@netapp.com.

Configurazioni e limitazioni validate

I seguenti principi sono stati applicati all'implementazione di esempio e potrebbero dover essere adattati per soddisfare le esigenze dei clienti:

- I sistemi SAP gestiti utilizzavano NFS per accedere ai volumi di storage NetApp e sono stati configurati in base al principio di progettazione adattiva.
- È possibile utilizzare tutte le release di ONTAP supportate dai moduli Ansible di NetApp (ZAPI e REST API).
- Le credenziali per un singolo cluster NetApp e SVM erano codificate come variabili nello script del provider.
- La clonazione dello storage è stata eseguita sullo stesso sistema storage utilizzato dal sistema SAP di origine.
- I volumi di storage per il sistema SAP di destinazione avevano gli stessi nomi dell'origine con un'appendice.
- Non è stato implementato alcun cloning nello storage secondario (SV/SM).
- Lo split FlexClone non è stato implementato.
- I numeri delle istanze erano identici per i sistemi SAP di origine e di destinazione.

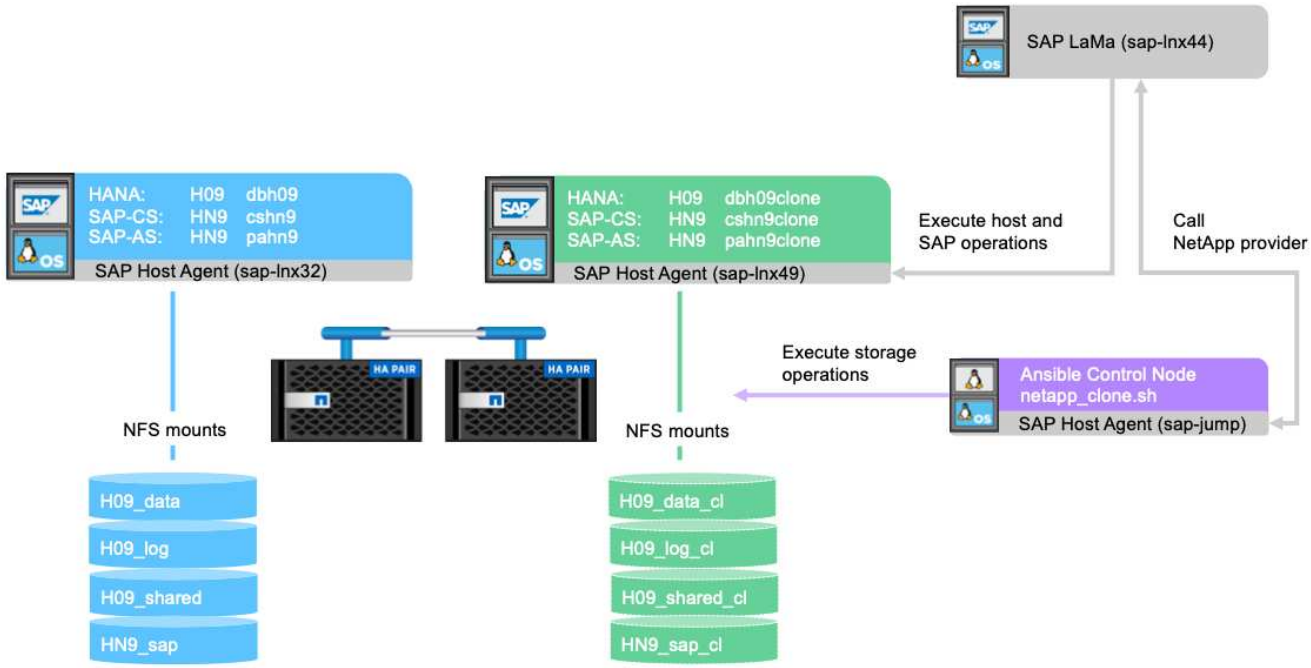
Setup di laboratorio

La figura seguente mostra la configurazione di laboratorio utilizzata. Il sistema SAP di origine HN9 utilizzato per l'operazione di clone del sistema era costituito dal database H09, dal SAP CS e dal SAP AS Services in esecuzione sullo stesso host (sap-lnx32) con installato "design adattivo" attivato. Un nodo di controllo Ansible è stato preparato secondo la "Playbook Ansible per NetApp ONTAP" documentazione.

Anche l'agente host SAP è stato installato su questo host. Lo script del provider NetApp e i playbook Ansible sono stati configurati sul nodo di controllo Ansible come descritti nella ""Appendice: Configurazione script provider.""

L'host `sap-lnx49` È stato utilizzato come destinazione per le operazioni di cloning di SAP lama ed è stata configurata la funzionalità di isolamento-ready.

Sono stati utilizzati diversi sistemi SAP (HNA come origine e HN2 come destinazione) per le operazioni di copia e refresh del sistema, perché è stata abilitata l'automazione post-copia (PCA).



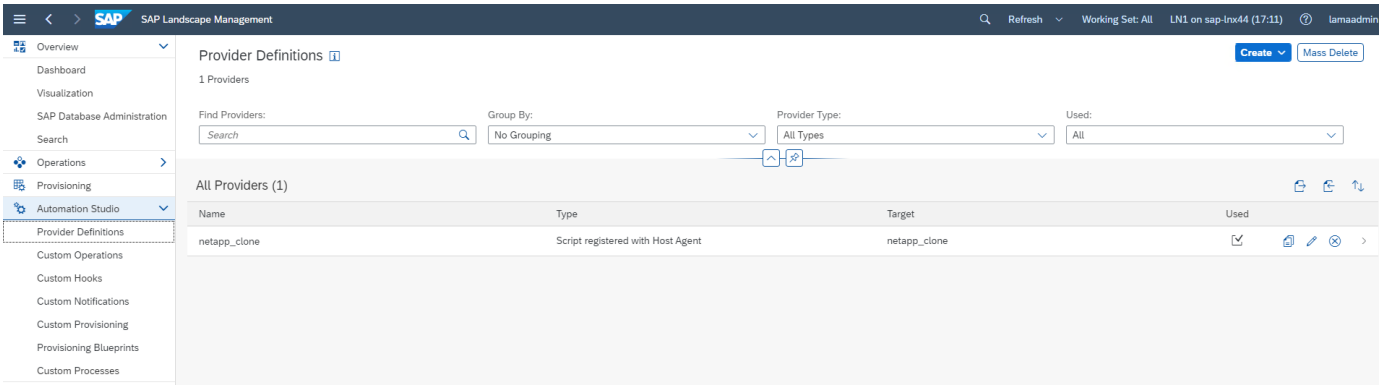
Nella configurazione di laboratorio sono state utilizzate le seguenti versioni software:

- SAP lama Enterprise Edition 3.00 SP23_2
- SAP HANA 2.00.052.00.1599235305
- SAP 7.77 PATCH 27 (S/4 HANA 1909)
- SAP host Agent 7.22 Patch 56
- SAPACEXT 7.22 Patch 69
- Linux SLES 15 SP2
- Ansible 2. 13.7
- NetApp ONTAP 9.8P8

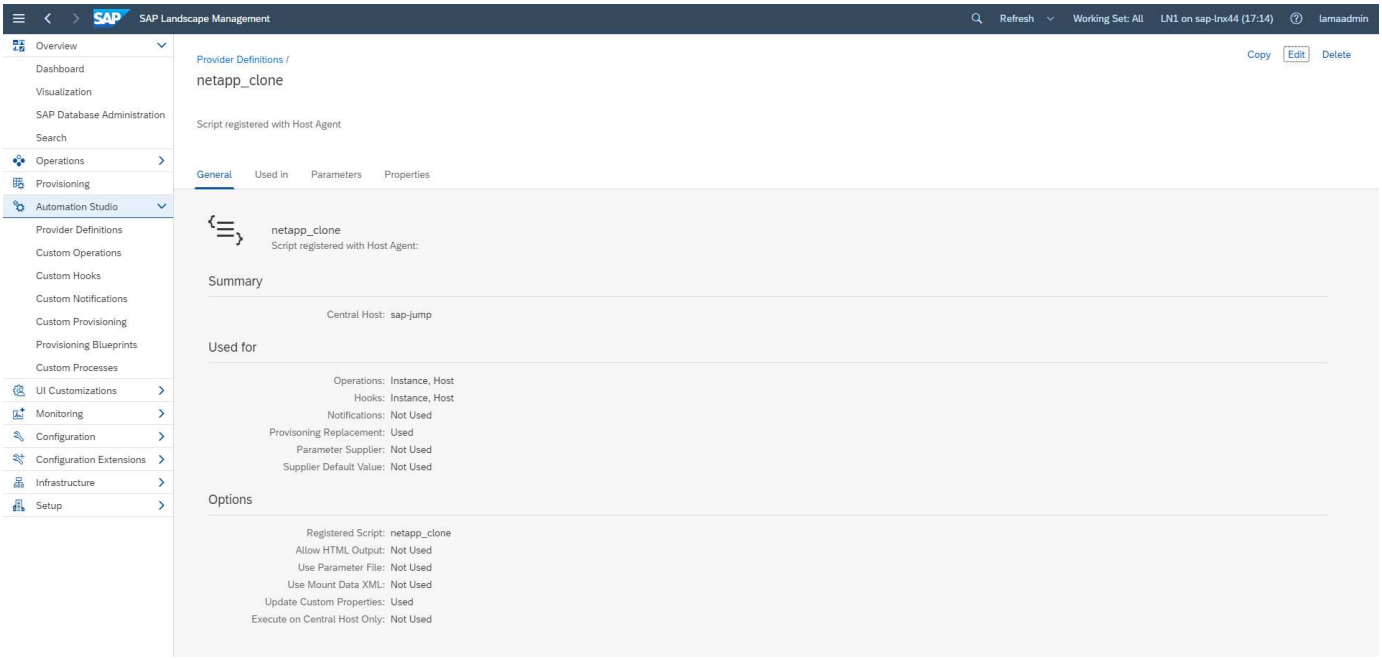
Configurazione di SAP lama

Definizione del provider SAP lama

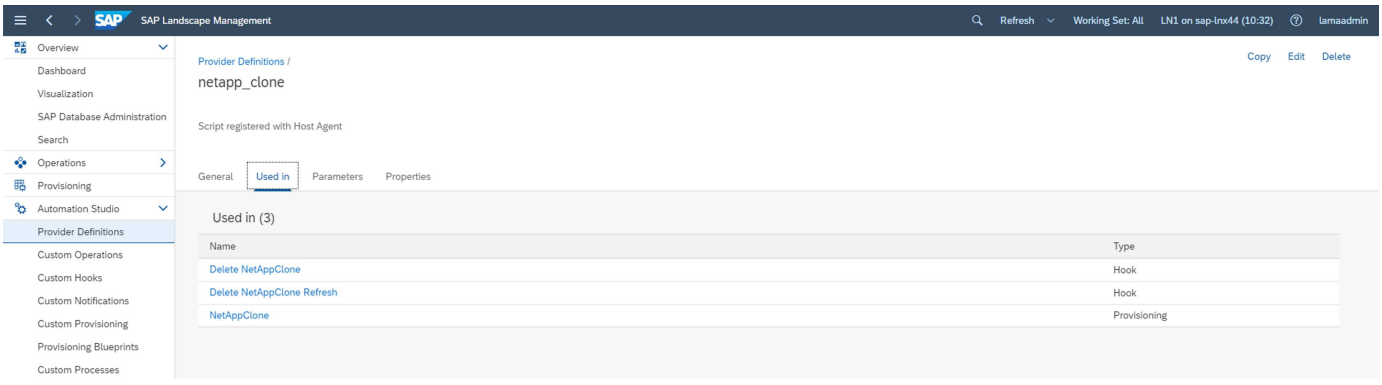
La definizione del provider viene eseguita in Automation Studio di SAP lama, come mostrato nella seguente schermata. L'implementazione di esempio utilizza una singola definizione di provider utilizzata per diverse fasi di provisioning personalizzate e per le operazioni hook, come spiegato in precedenza.



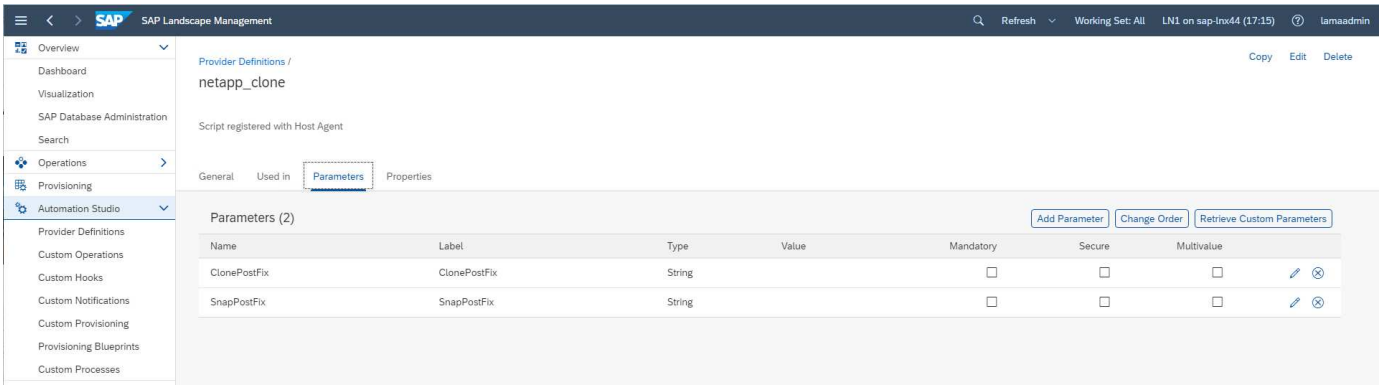
Il provider `netapp_clone` viene definito come script `netapp_clone.sh` Registrato presso l'agente host SAP. L'agente host SAP viene eseguito sull'host centrale `sap-jump`, Che funge anche da nodo di controllo Ansible.



La scheda **utilizzato in** mostra le operazioni personalizzate per cui viene utilizzato il provider. La configurazione per il provisioning personalizzato **NetAppClone** e gli hook personalizzati **Delete NetAppClone** e **Delete NetAppClone Refresh** sono illustrati nei capitoli successivi.

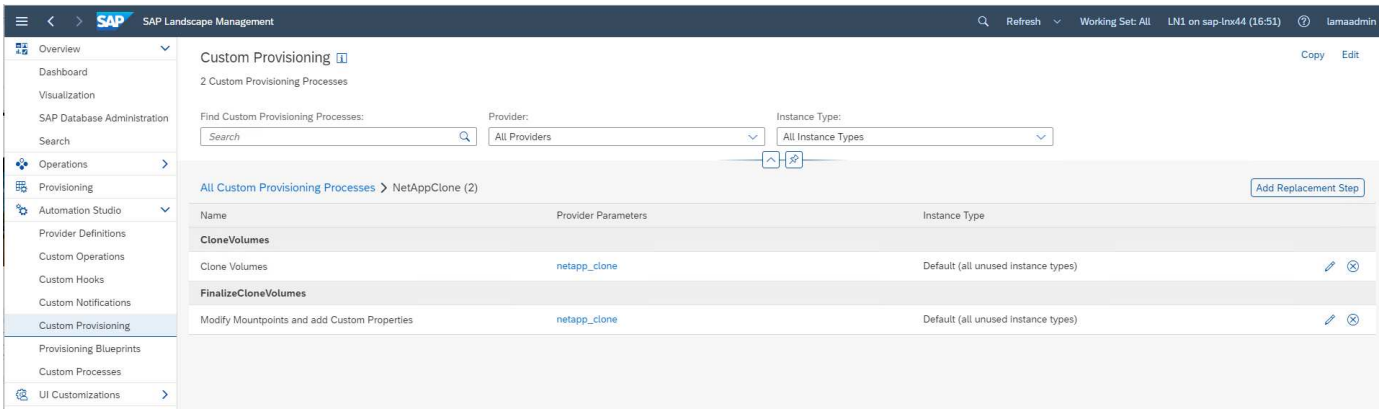


I parametri **ClonePostFix** e **SnapPostFix** vengono richiesti durante l'esecuzione del flusso di lavoro di provisioning e utilizzati per i nomi dei volumi Snapshot e FlexClone.



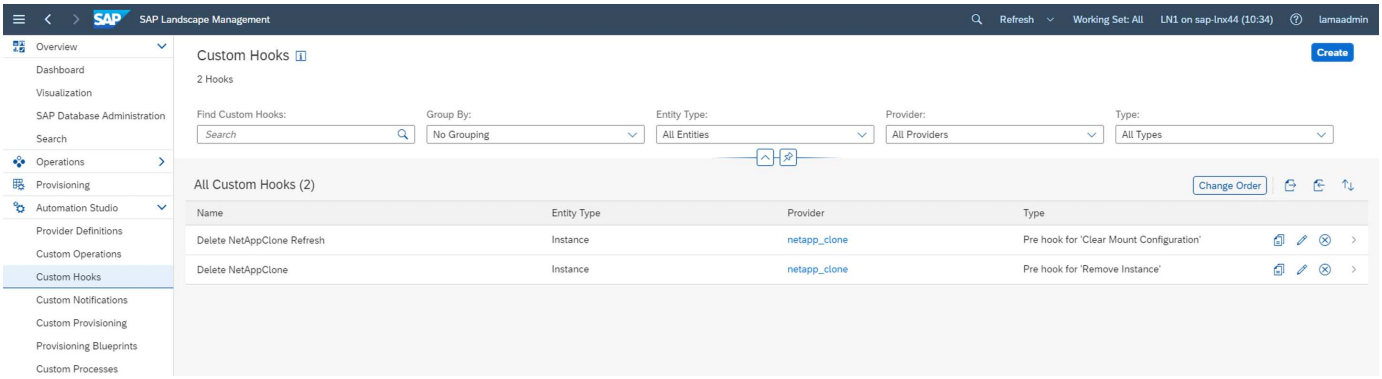
Provisioning personalizzato SAP lama

Nella configurazione di provisioning personalizzata di SAP lama, il provider del cliente descritto in precedenza viene utilizzato per sostituire le fasi del workflow di provisioning **Clone Volumes** e **PostCloneVolumes**.

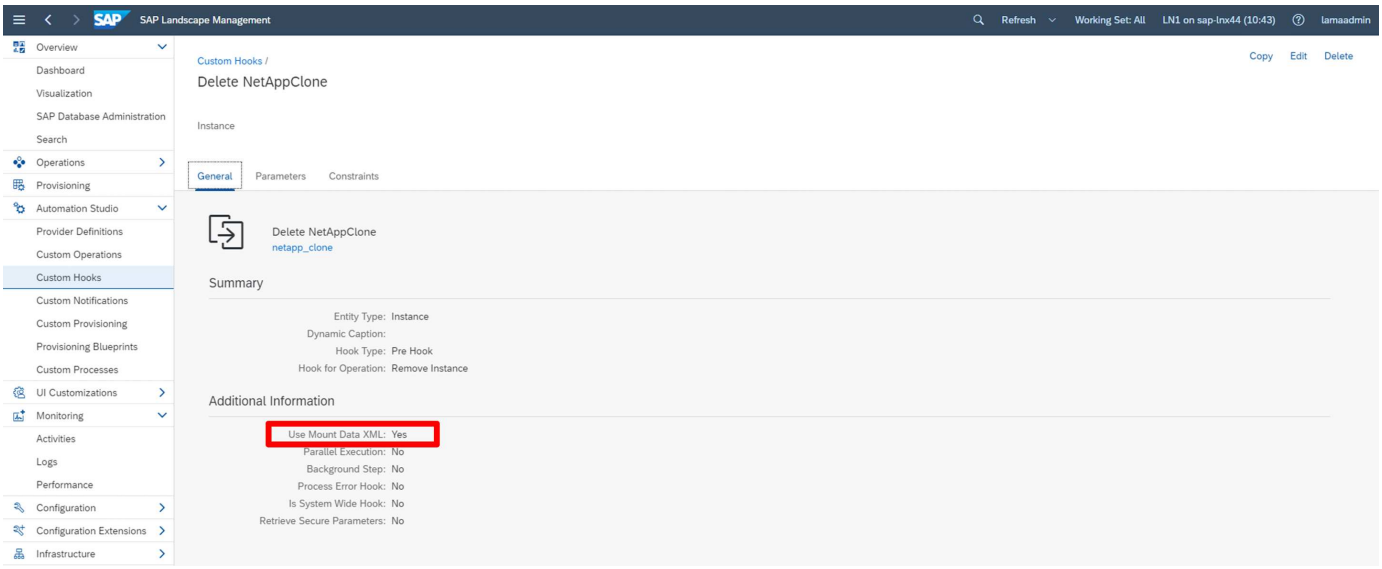


Gancio personalizzato SAP lama

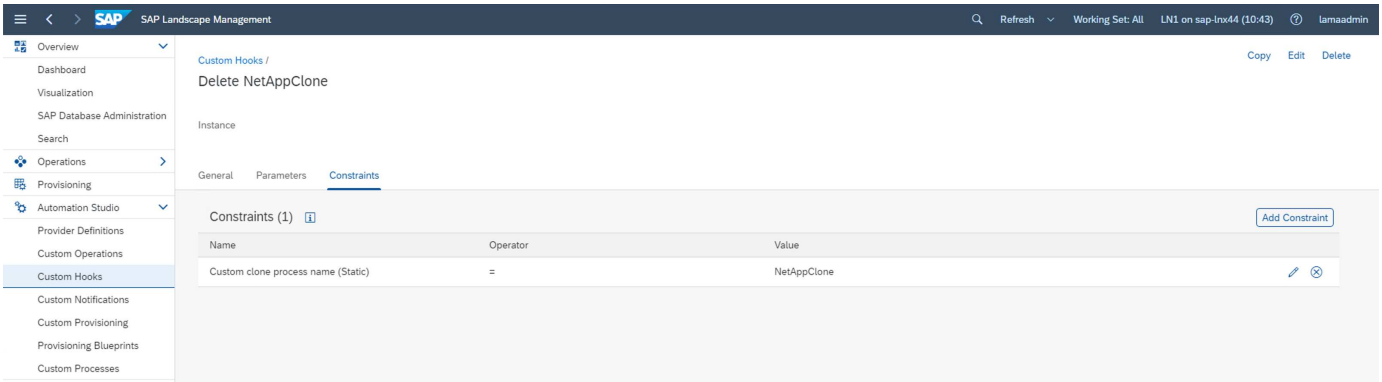
Se un sistema viene cancellato con il flusso di lavoro System Destroy, viene utilizzato Hook **Delete NetAppClone** per chiamare la definizione del provider `netapp_clone`. L'hook **Delete NetApp Clone Refresh** viene utilizzato durante il flusso di lavoro di refresh del sistema perché l'istanza viene conservata durante l'esecuzione.



È importante configurare **Usa Mount Data XML** per il gancio personalizzato, in modo che SAP lama fornisca al provider le informazioni sulla configurazione del punto di montaggio.



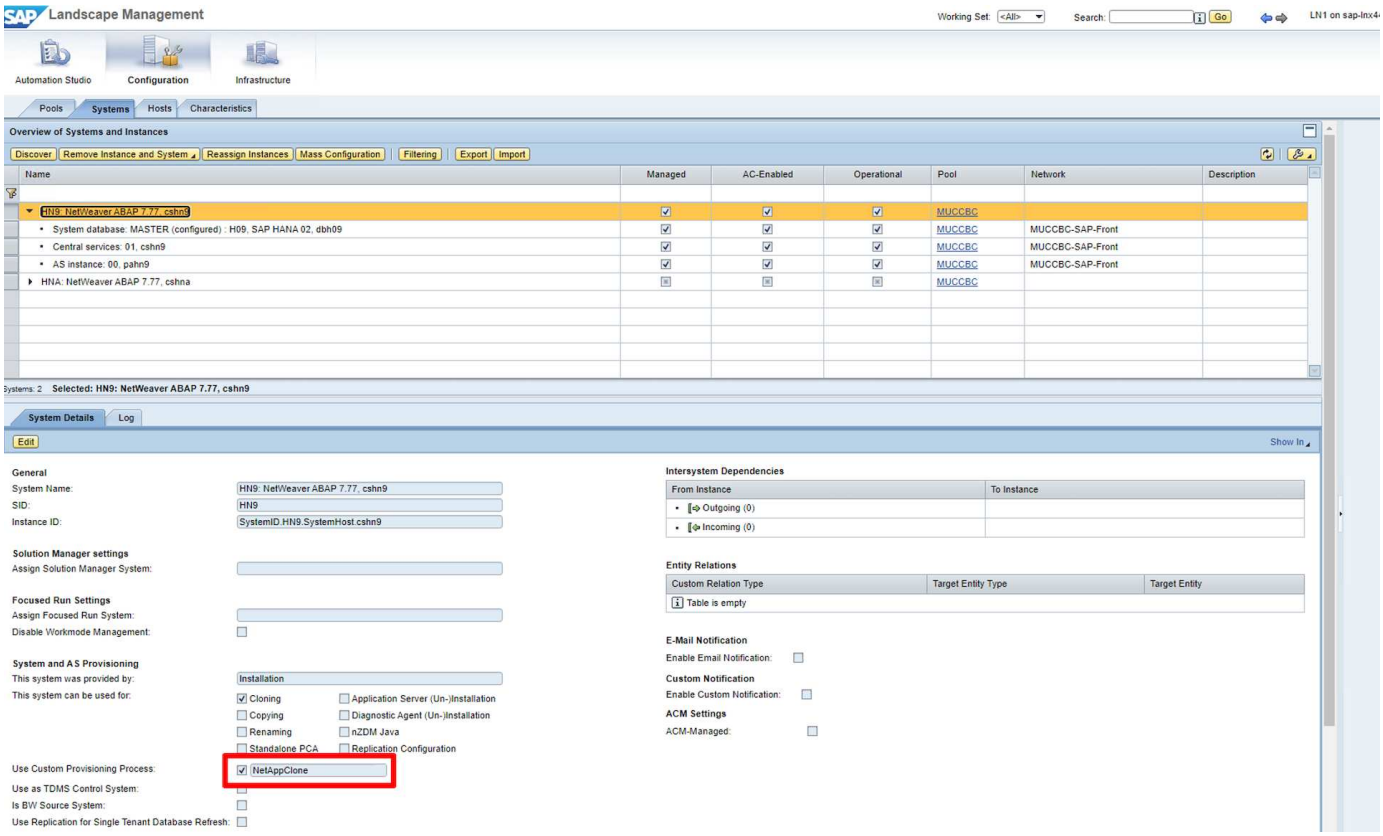
Per garantire che il gancio personalizzato venga utilizzato ed eseguito solo quando il sistema è stato creato con un workflow di provisioning personalizzato, viene aggiunto il seguente vincolo.



Ulteriori informazioni sull'utilizzo di ganci personalizzati sono disponibili nella "Documentazione SAP lama".

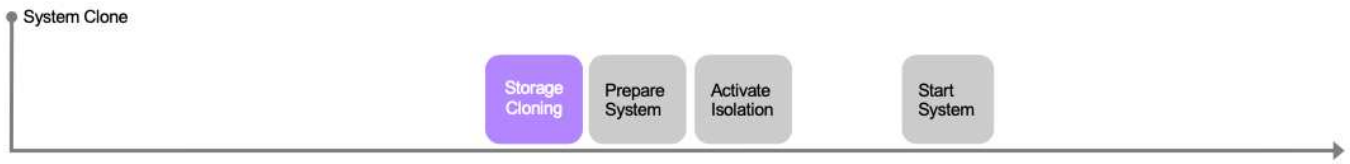
Abilitare un workflow di provisioning personalizzato per il sistema di origine SAP

Per abilitare il workflow di provisioning personalizzato per il sistema di origine, è necessario adattarlo nella configurazione. Selezionare la casella di controllo **Usa processo di provisioning personalizzato** con la definizione di provisioning personalizzato corrispondente.

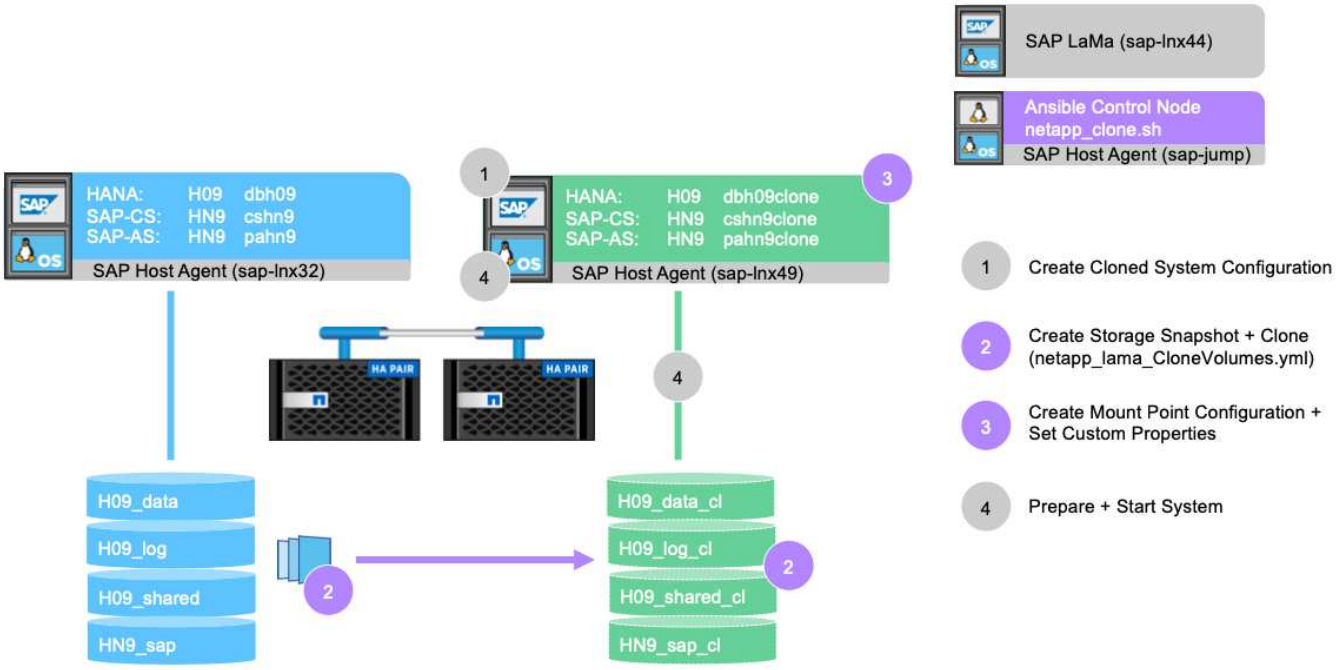


Workflow di provisioning SAP lama - sistema clone

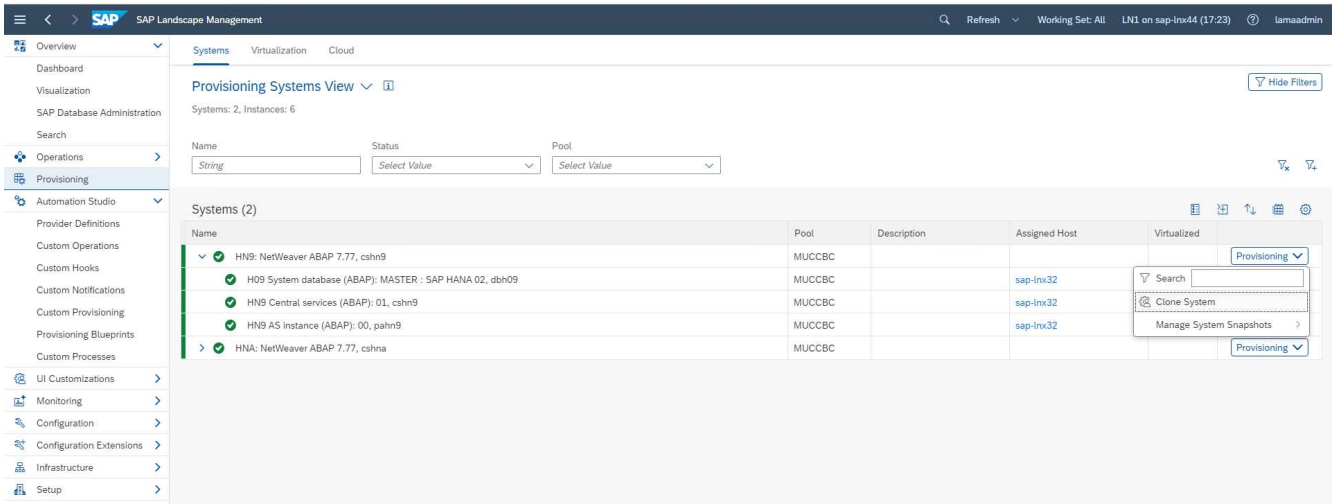
La figura seguente evidenzia i passaggi principali eseguiti con il flusso di lavoro dei cloni di sistema.



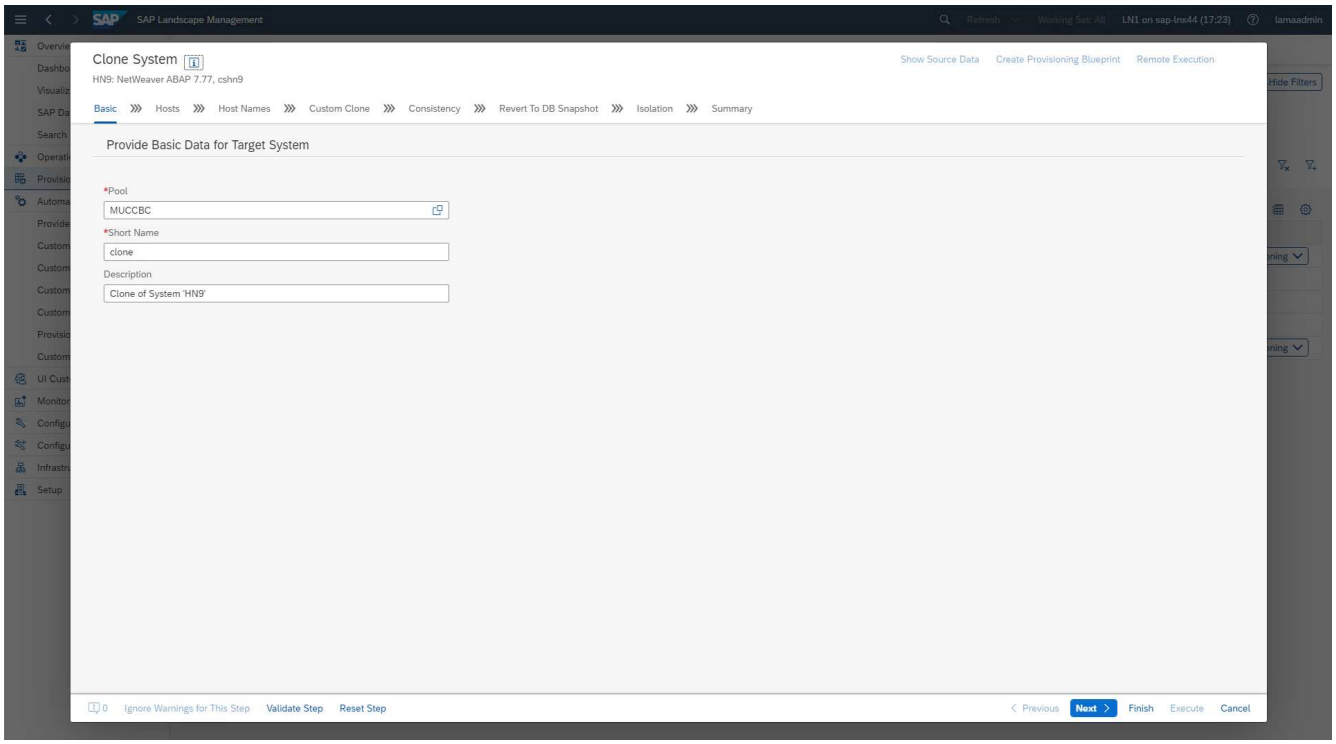
In questa sezione, viene descritto il workflow completo di cloning del sistema SAP lama basato sul sistema SAP di origine HN9 con database HANA H09. La figura seguente fornisce una panoramica delle fasi eseguite durante il flusso di lavoro.



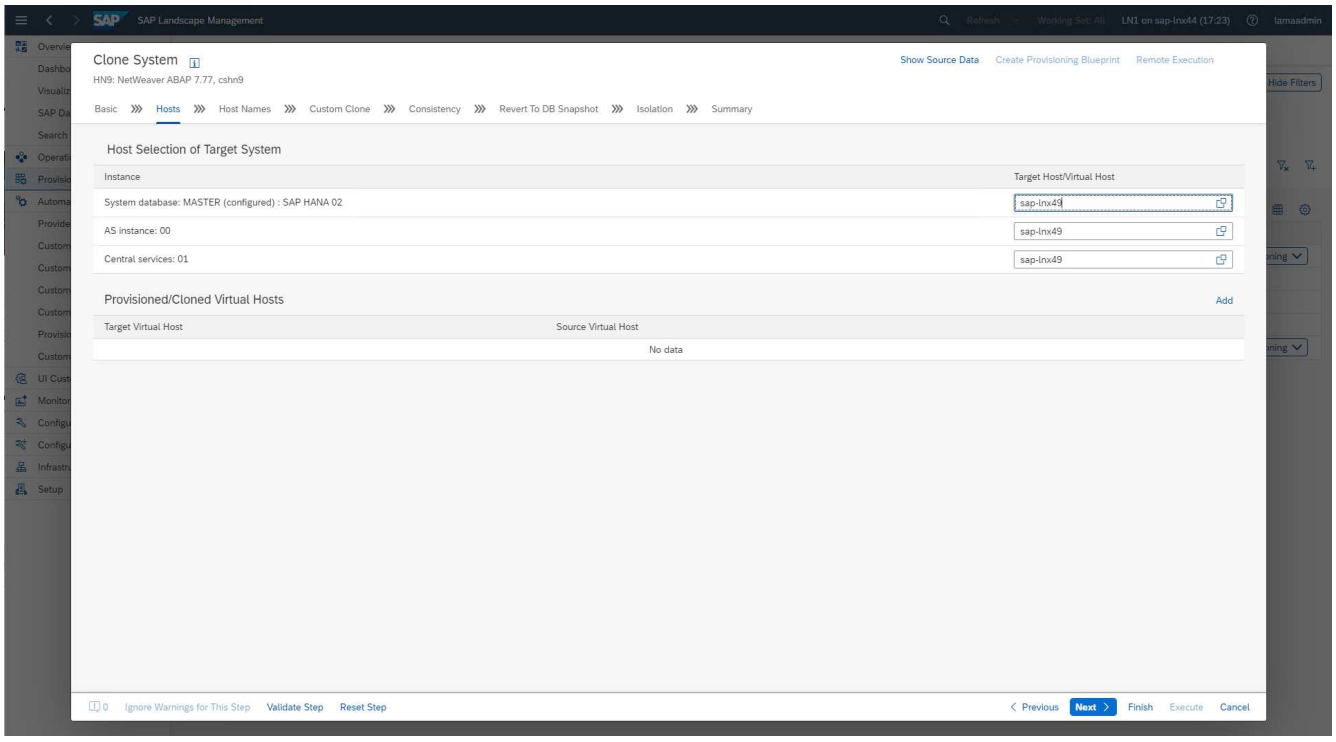
1. Per avviare il flusso di lavoro di cloning, aprire **Provisioning** nella struttura dei menu e selezionare il sistema di origine (nel nostro esempio HN9). Quindi avviare la procedura guidata **Clone System**.



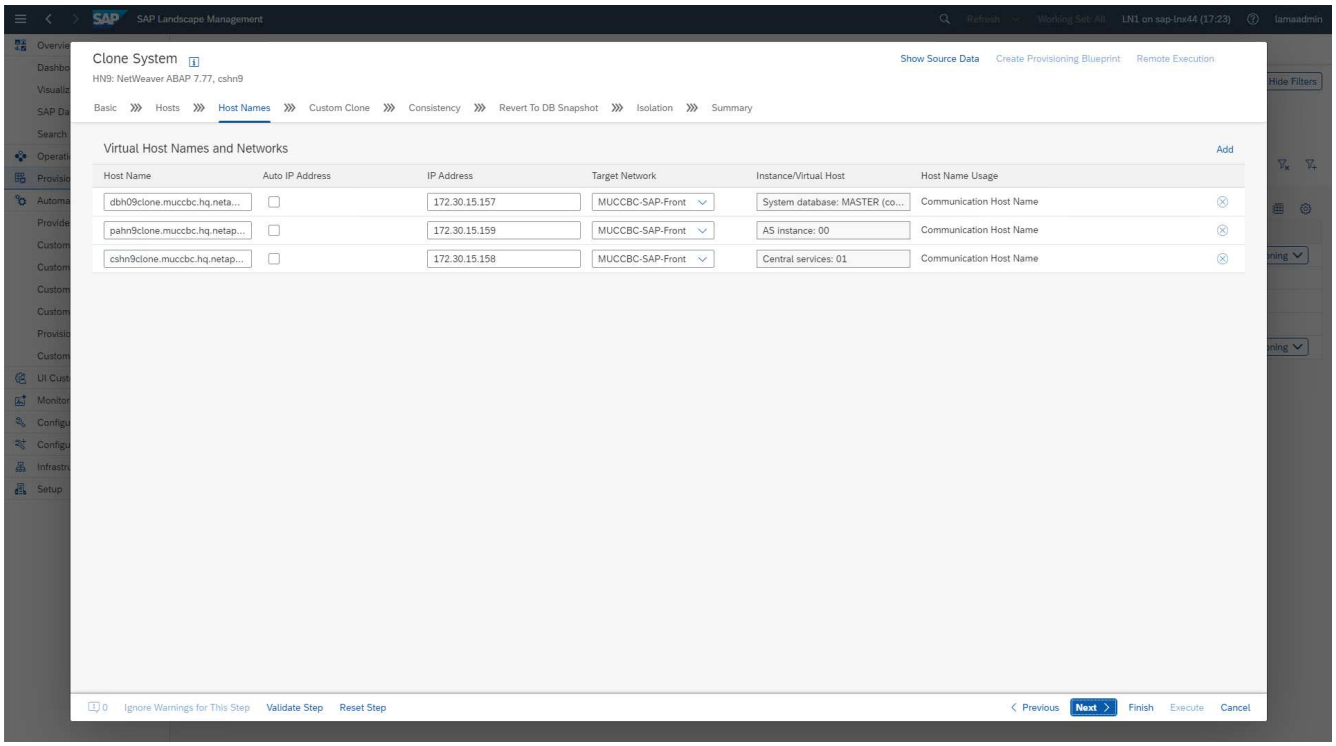
2. Inserire i valori richiesti. La schermata 1 della procedura guidata richiede il nome del pool per il sistema clonato. Questa fase specifica le istanze (virtuali o fisiche) su cui verrà avviato il sistema clonato. Per impostazione predefinita, il sistema viene clonato nello stesso pool del sistema di destinazione.



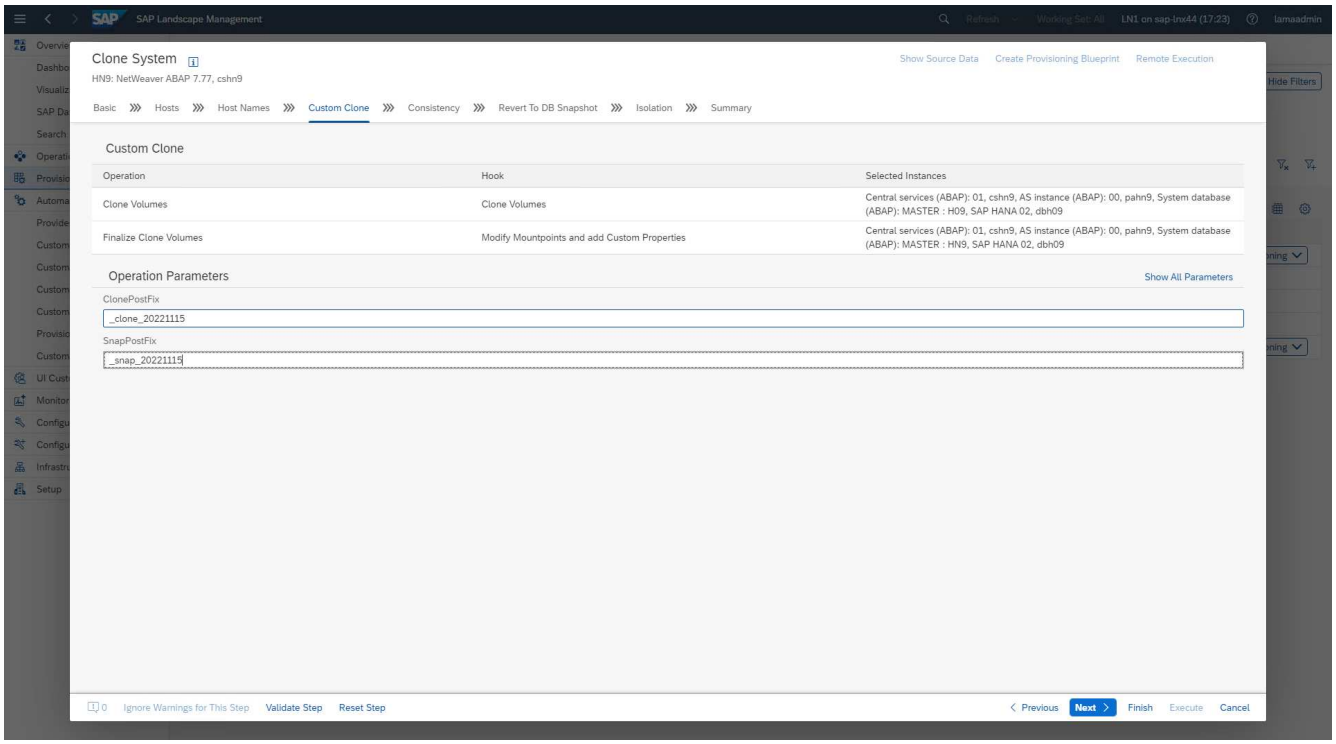
3. La schermata 2 della procedura guidata richiede gli host di destinazione su cui vengono avviate le nuove istanze SAP. È possibile selezionare gli host di destinazione per queste istanze al di fuori del pool di host specificato nella schermata precedente. Ogni istanza o servizio può essere avviato su un host diverso. Nel nostro esempio, tutti e tre i servizi vengono eseguiti sullo stesso host.



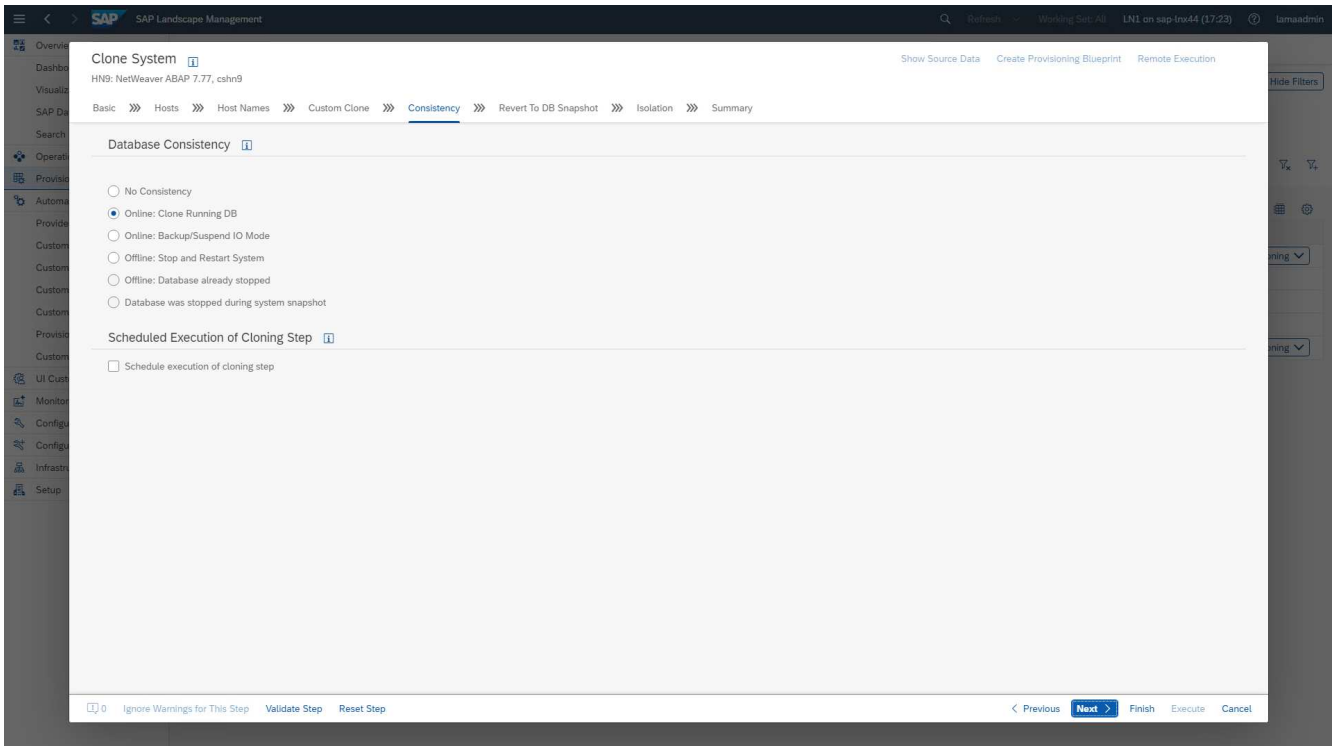
4. Fornire le informazioni richieste nella schermata 3, che richiede i nomi degli host virtuali e le reti. In genere, i nomi host vengono mantenuti in DNS, quindi gli indirizzi IP vengono prepopolati di conseguenza.



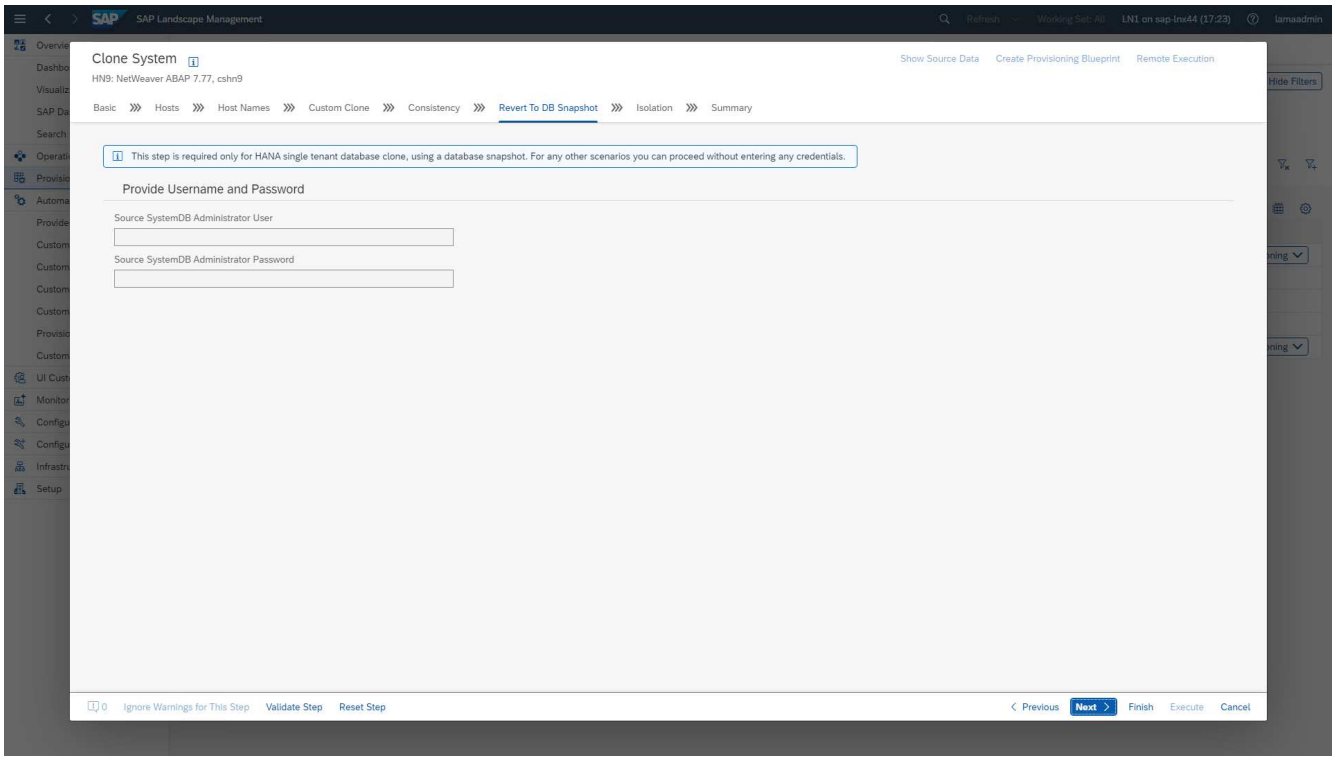
5. Nella schermata 4 sono elencate le operazioni di clonazione personalizzate. Vengono forniti un clone e un nome **SnapPostfix**, utilizzati durante l'operazione di clone dello storage per il volume FlexClone e il nome Snapshot, rispettivamente. Se si lasciano vuoti questi campi, il valore predefinito configurato nella sezione variabile dello script del provider `netapp_clone.sh` viene utilizzato.



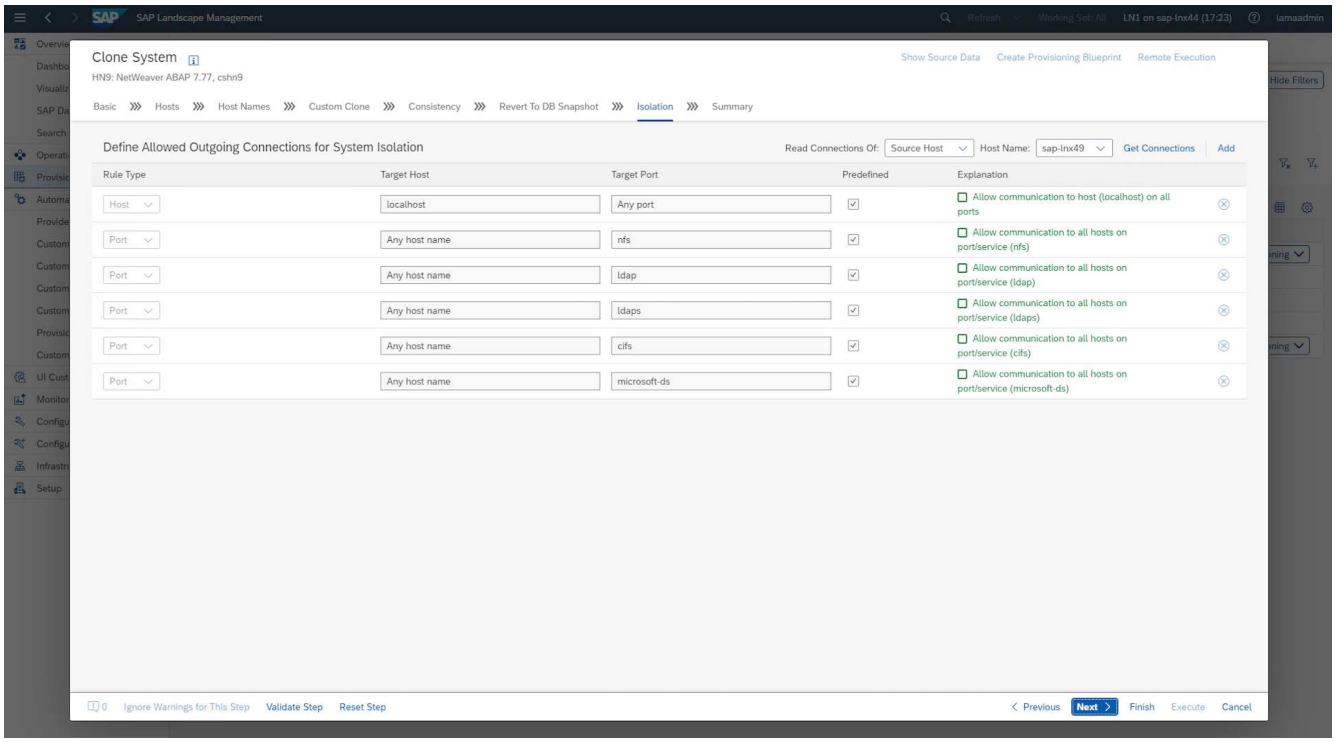
6. Nella schermata 5, viene selezionata l'opzione di coerenza del database. Nel nostro esempio, abbiamo selezionato **Online: Clone che esegue DB**.



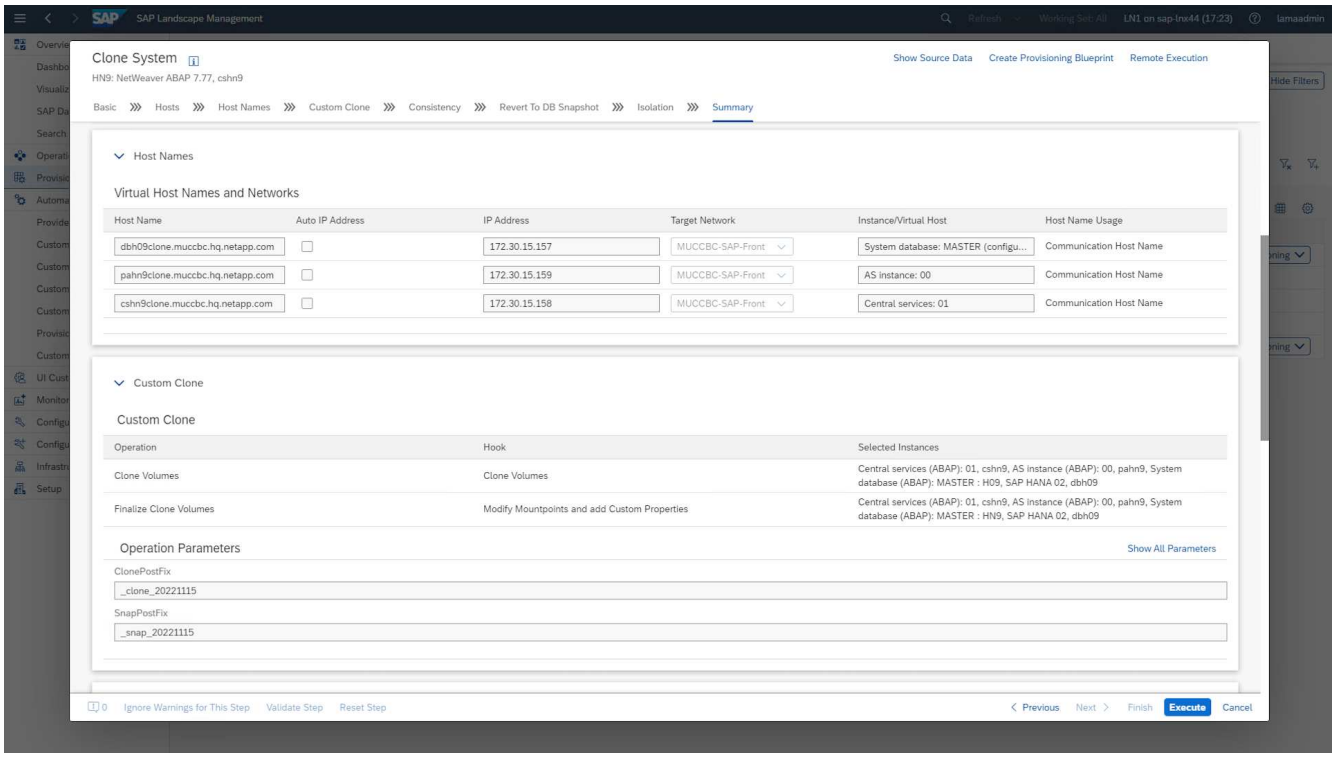
7. Nella schermata 6, l'input è necessario solo se si esegue un clone del tenant.



8. Nella schermata 7, è possibile configurare l'isolamento del sistema.

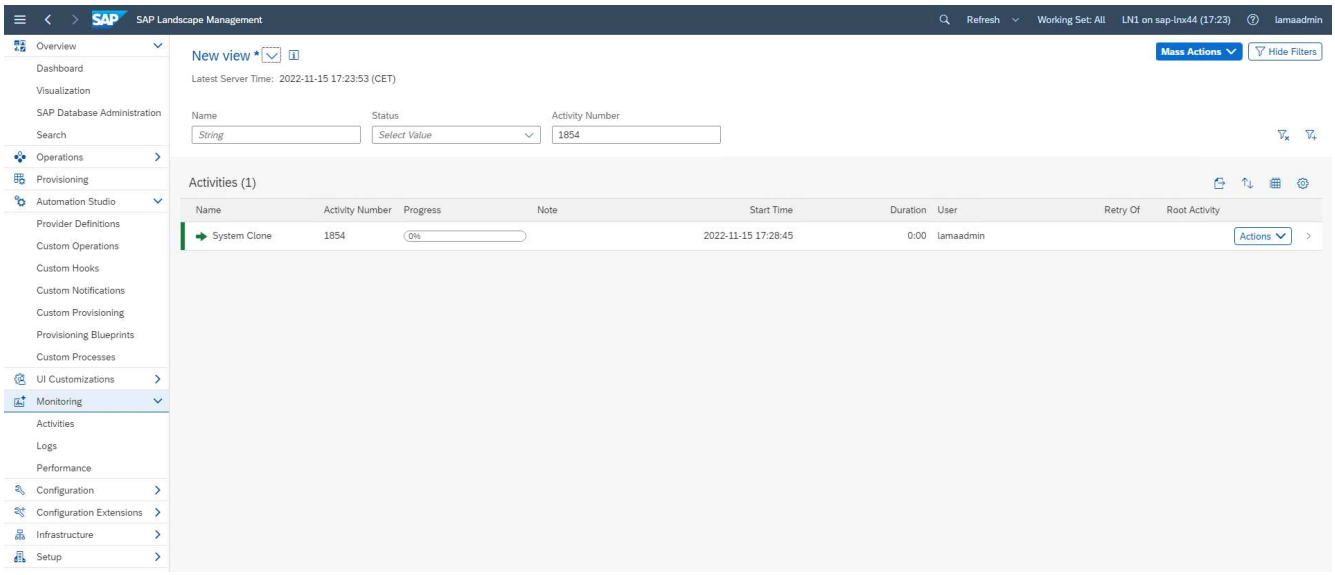


9. Nella schermata 8, una pagina di riepilogo contiene tutte le impostazioni per la conferma finale prima dell'avvio del flusso di lavoro. Fare clic su **Execute** (Esegui) per avviare il flusso di lavoro.

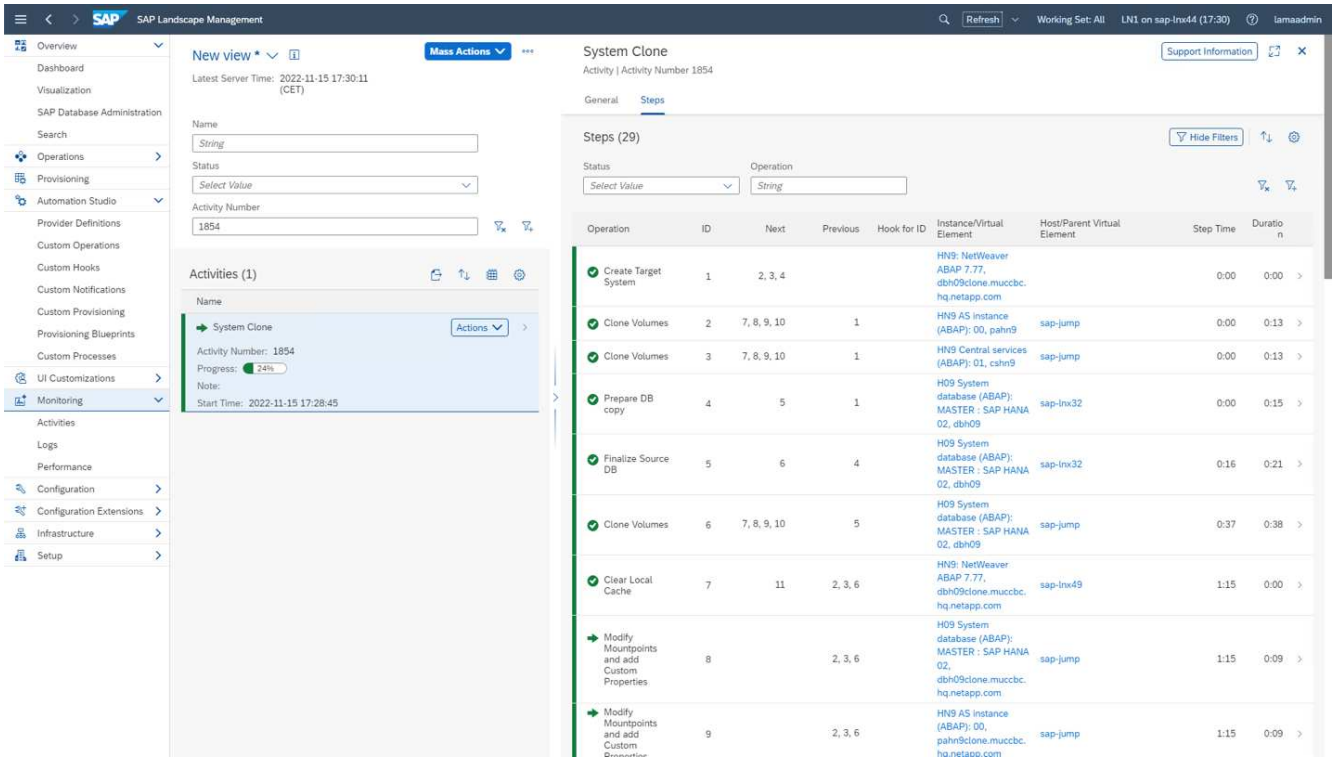


SAP lama esegue ora tutte le azioni indicate nella configurazione. Queste azioni includono la creazione di cloni ed esportazioni del volume di storage, il montaggio nell'host di destinazione, l'aggiunta di regole firewall per l'isolamento e l'avvio del database HANA e dei servizi SAP.

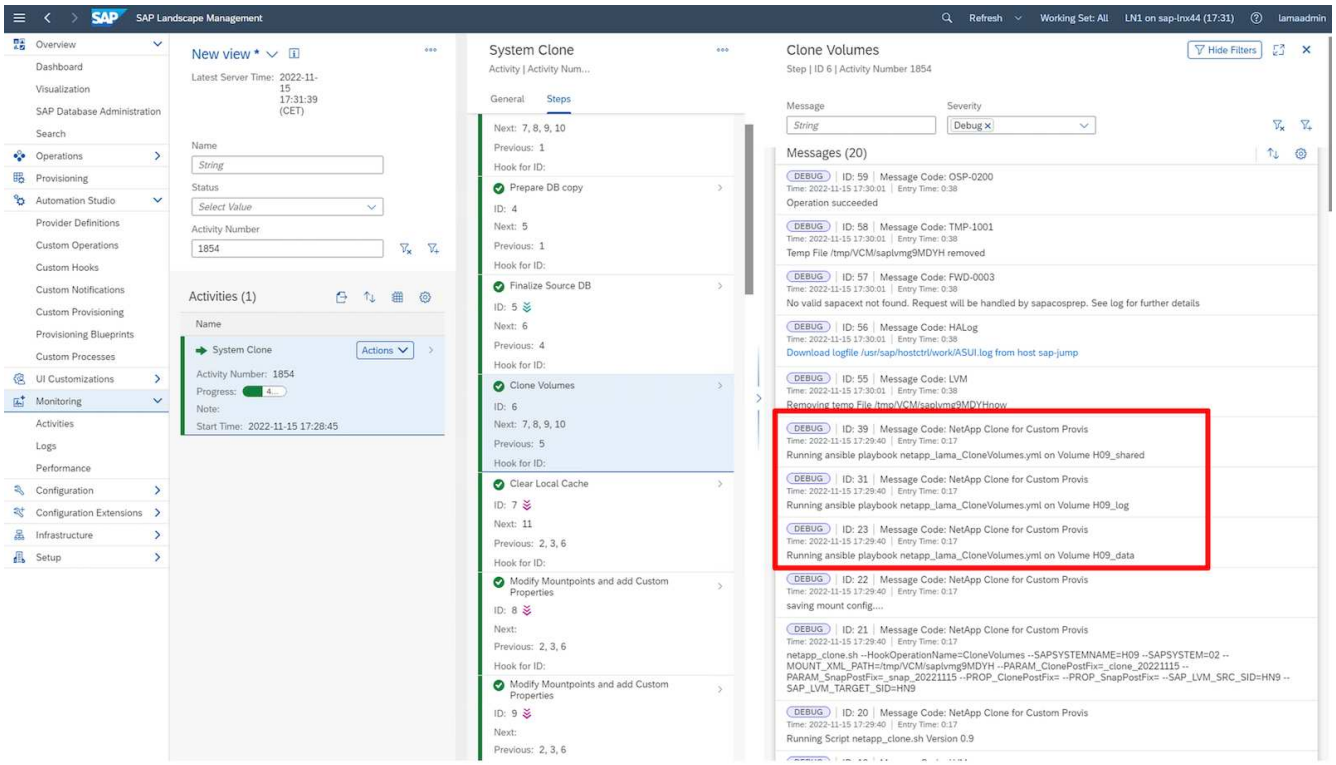
10. È possibile monitorare l'avanzamento del flusso di lavoro dei cloni nel menu **Monitoring**.



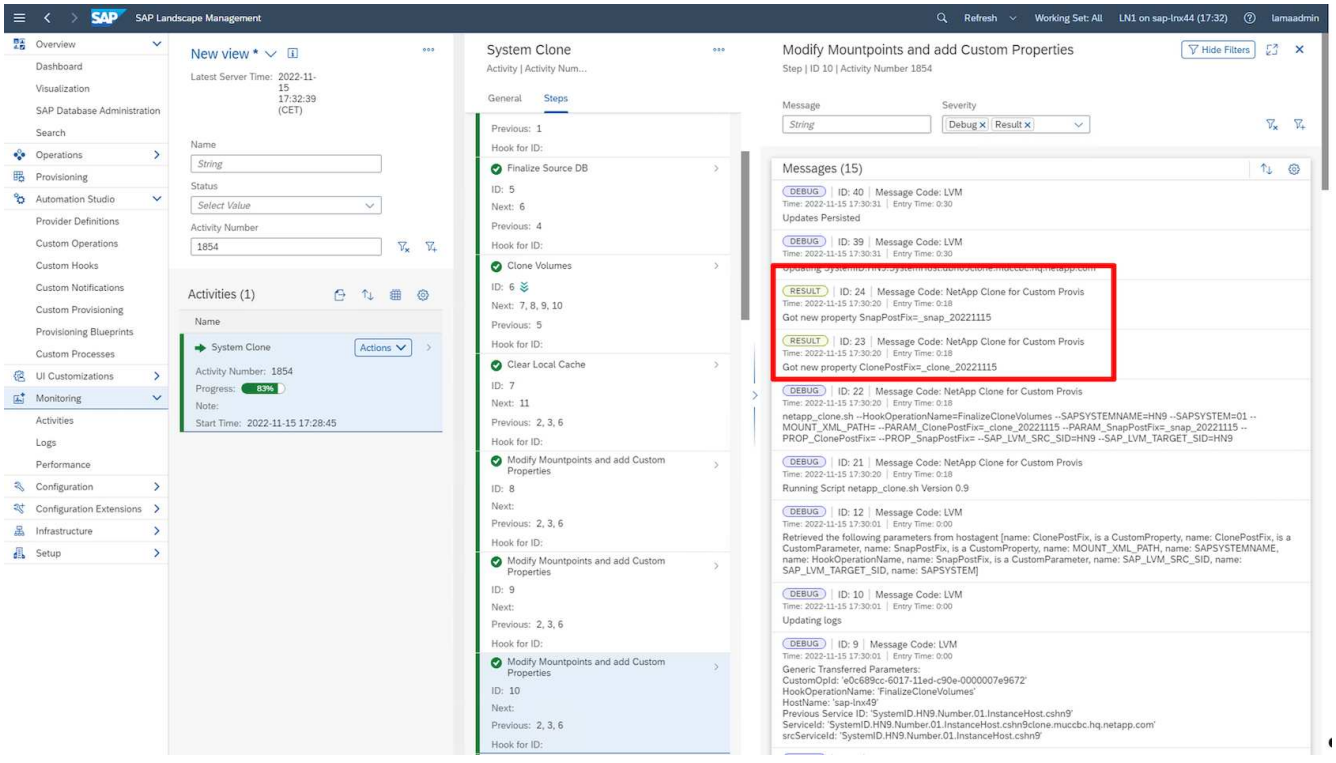
All'interno del log dettagliato, le operazioni **Clone Volume** e **Modify mountpoint e add Custom Properties** vengono eseguite nel nodo Ansible, il `sap-jump` host. Questi passaggi vengono eseguiti per ogni servizio, per il database HANA, per i servizi centrali SAP e per il servizio SAP AS.



11. Selezionando l'attività **Clone Volumes**, viene visualizzato il log dettagliato di quel passaggio e l'esecuzione del manuale Ansible Playbook viene mostrata qui. Puoi vedere, che il playbook Ansible `netapp_lama_CloneVolumes.yml` Viene eseguito per ogni volume di database HANA, dati, log e condiviso.



12. Nella vista dettagli dell'istruzione **Modifica punti di montaggio e Aggiungi proprietà personalizzate**, è possibile trovare informazioni sui punti di montaggio e sulle proprietà personalizzate consegnate dallo script di esecuzione.



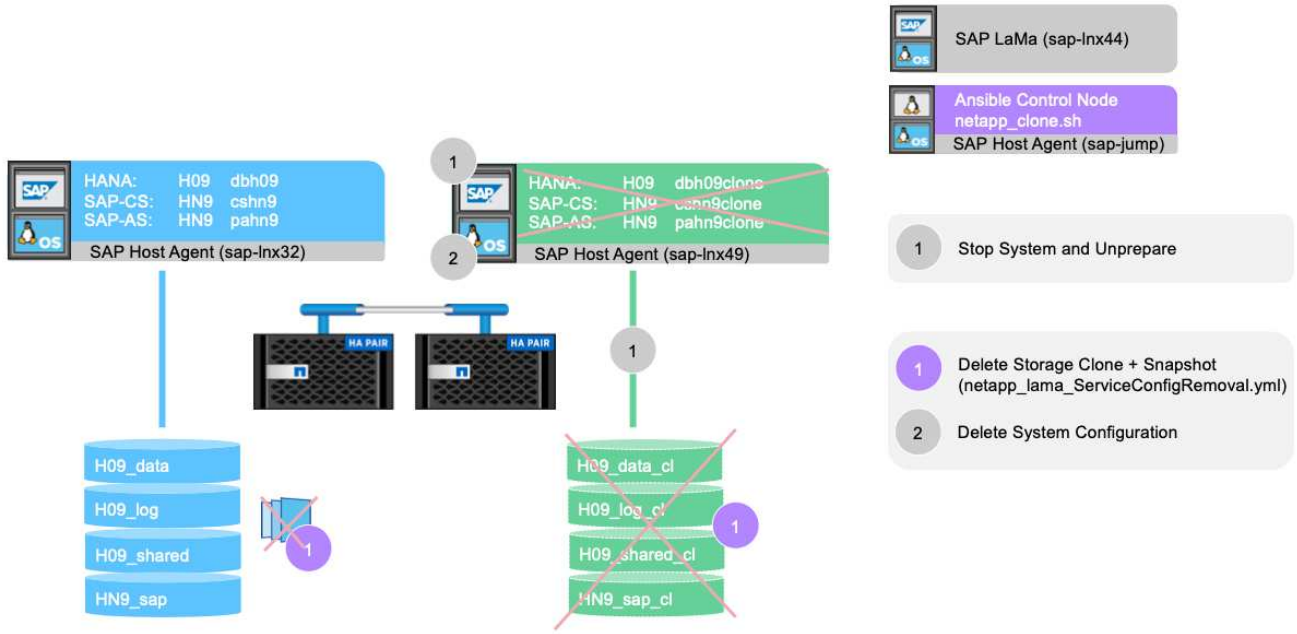
Una volta completato il workflow, il sistema SAP clonato viene preparato, avviato e pronto per l'uso.

Workflow di deprovisioning SAP lama - distruzione del sistema

La figura seguente evidenzia i passaggi principali eseguiti con il flusso di lavoro System Destroy.

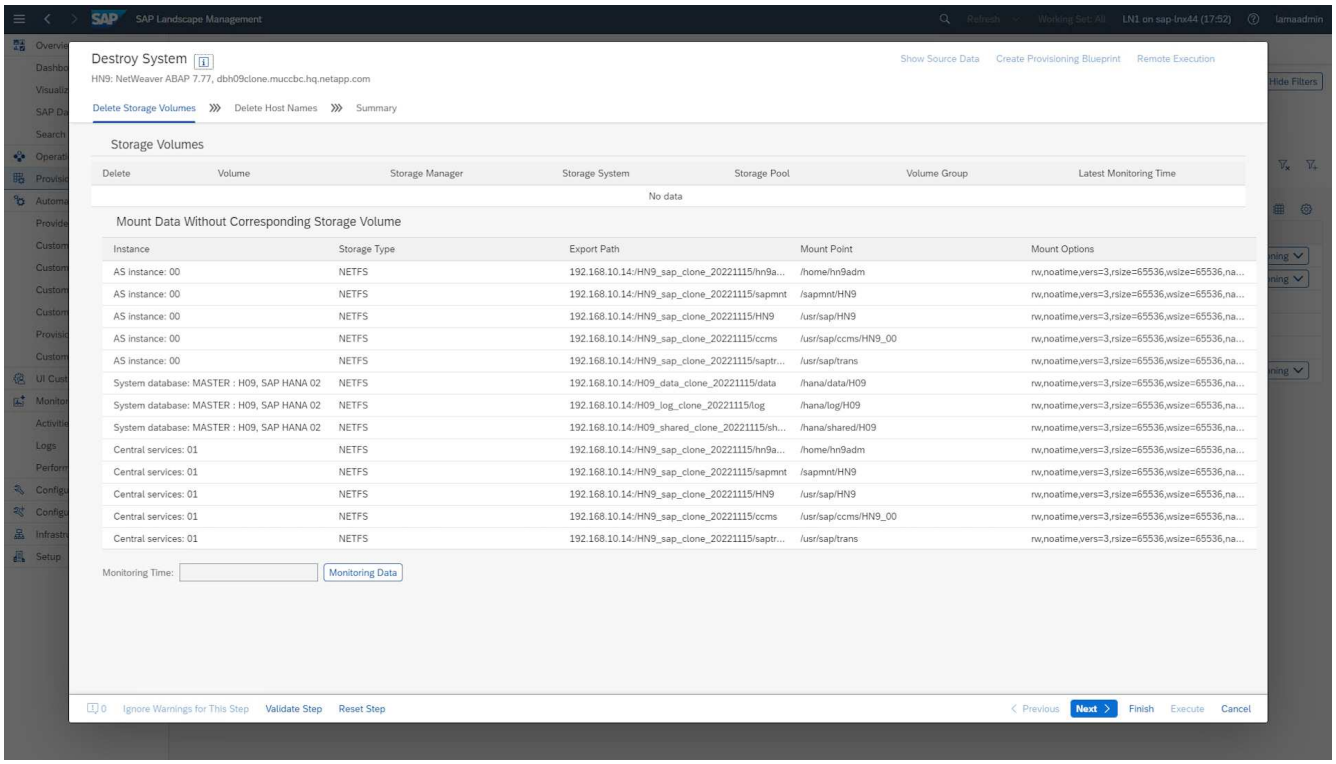


1. Per decommissionare un sistema clonato, occorre arrestarlo e prepararlo in anticipo. In seguito, è possibile avviare il flusso di lavoro System Destroy.

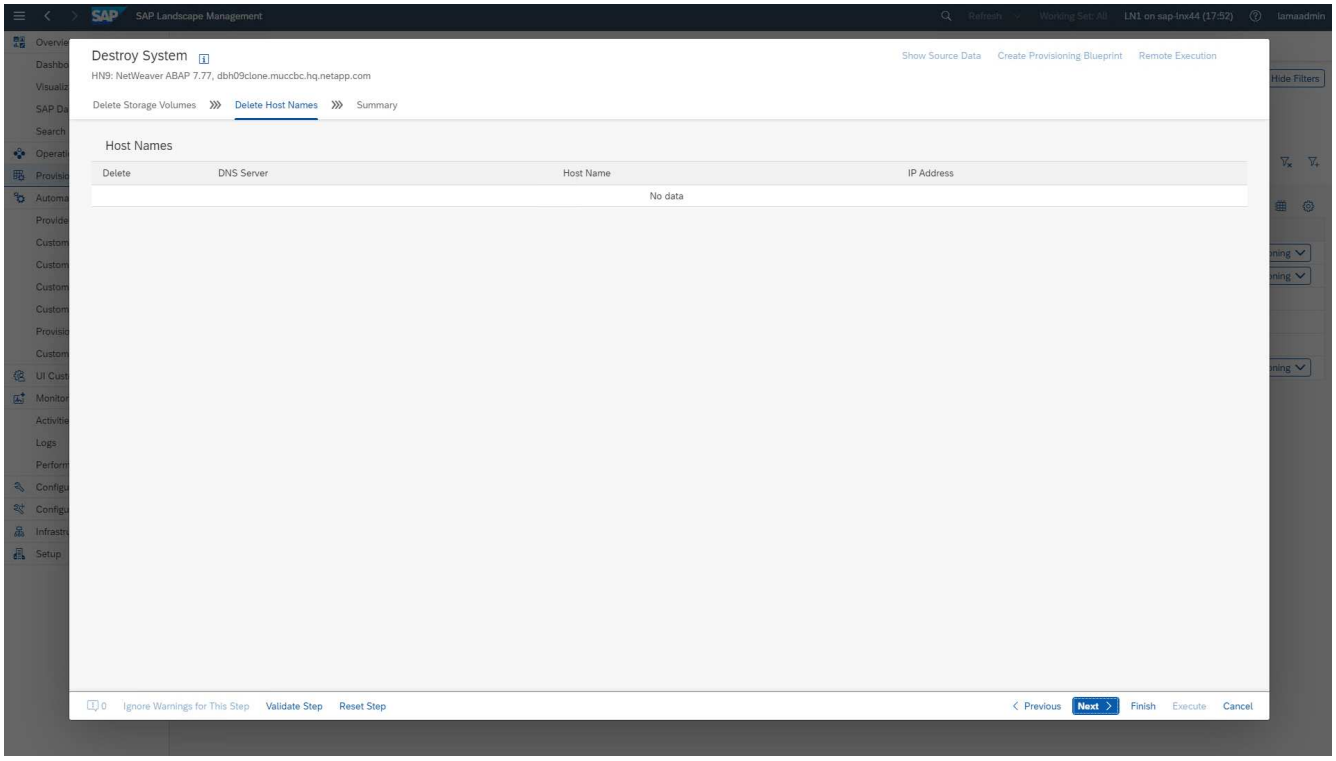


2. In questo esempio, eseguiamo il flusso di lavoro System Destroy per il sistema creato in precedenza. Selezioniamo il sistema nella schermata **Vista sistema** e avviamo il workflow di distruzione del sistema in **Destroy processes**.

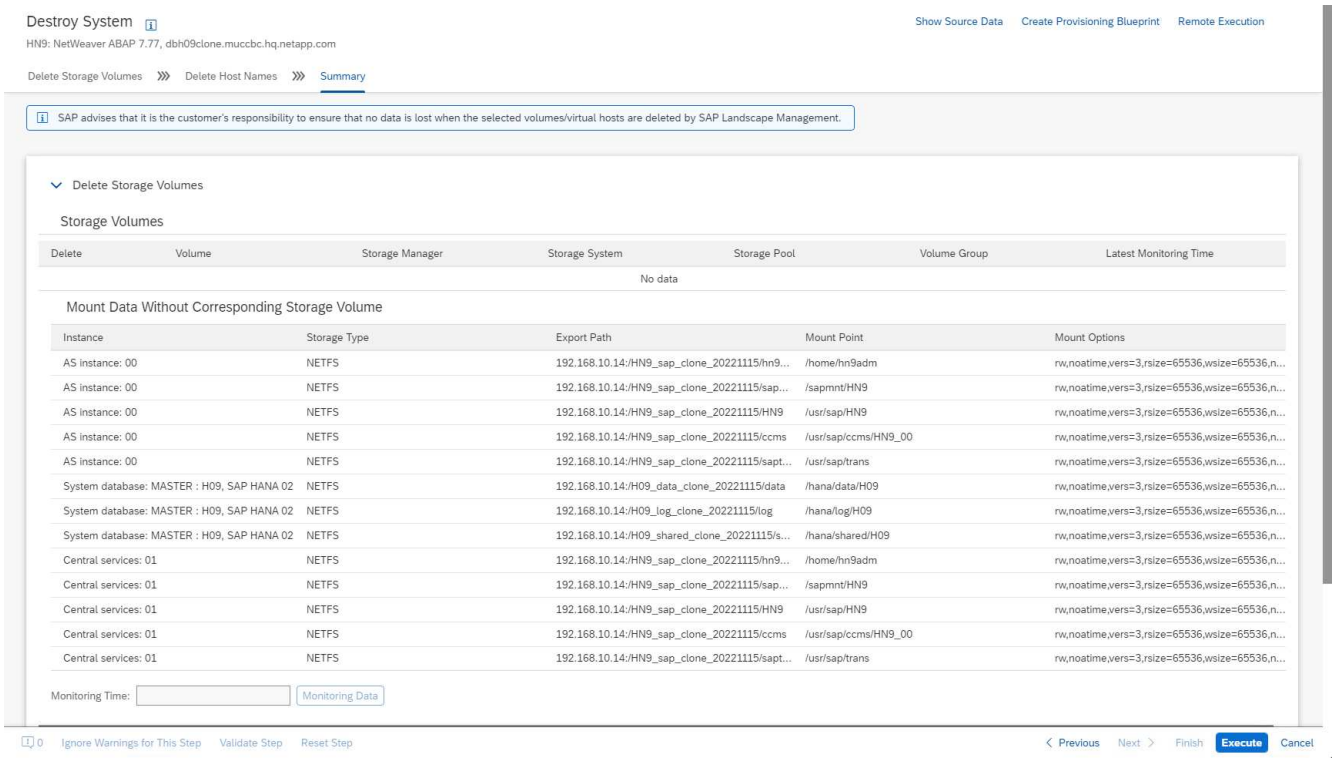
3. Tutti i punti di montaggio mantenuti durante la fase di provisioning vengono mostrati qui e cancellati durante il processo di workflow di system Destroy.



Nessun nome host virtuale viene cancellato perché vengono mantenuti tramite DNS e assegnati automaticamente.

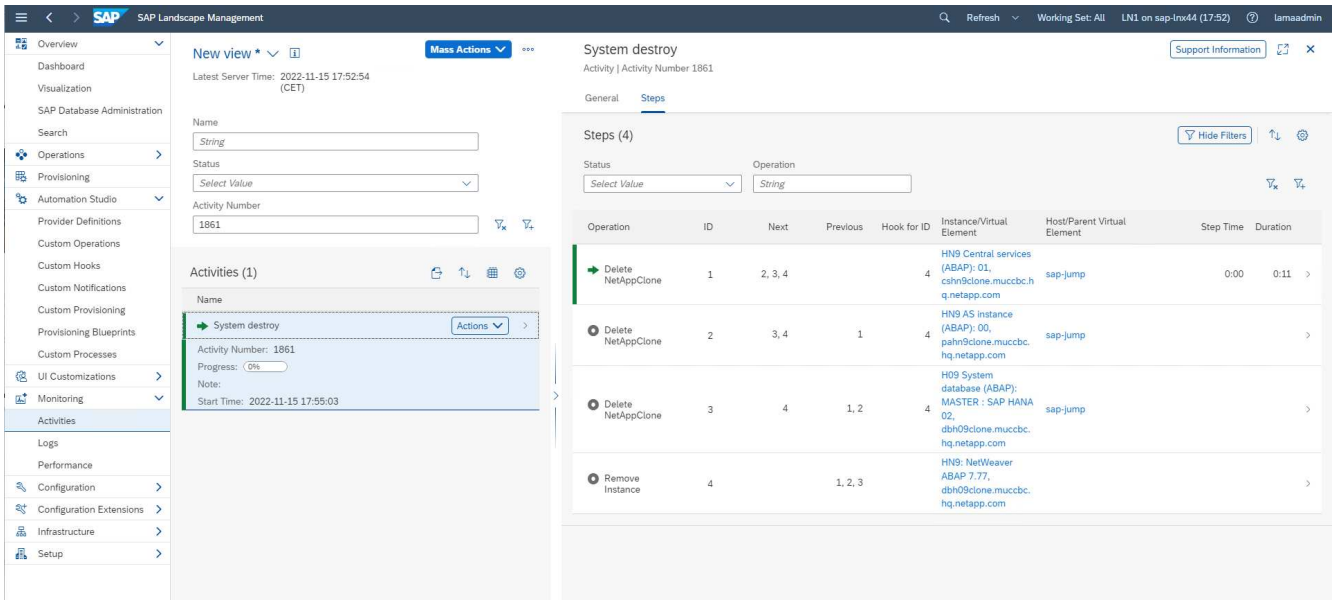


4. Per avviare l'operazione, fare clic sul pulsante Execute (Esegui).

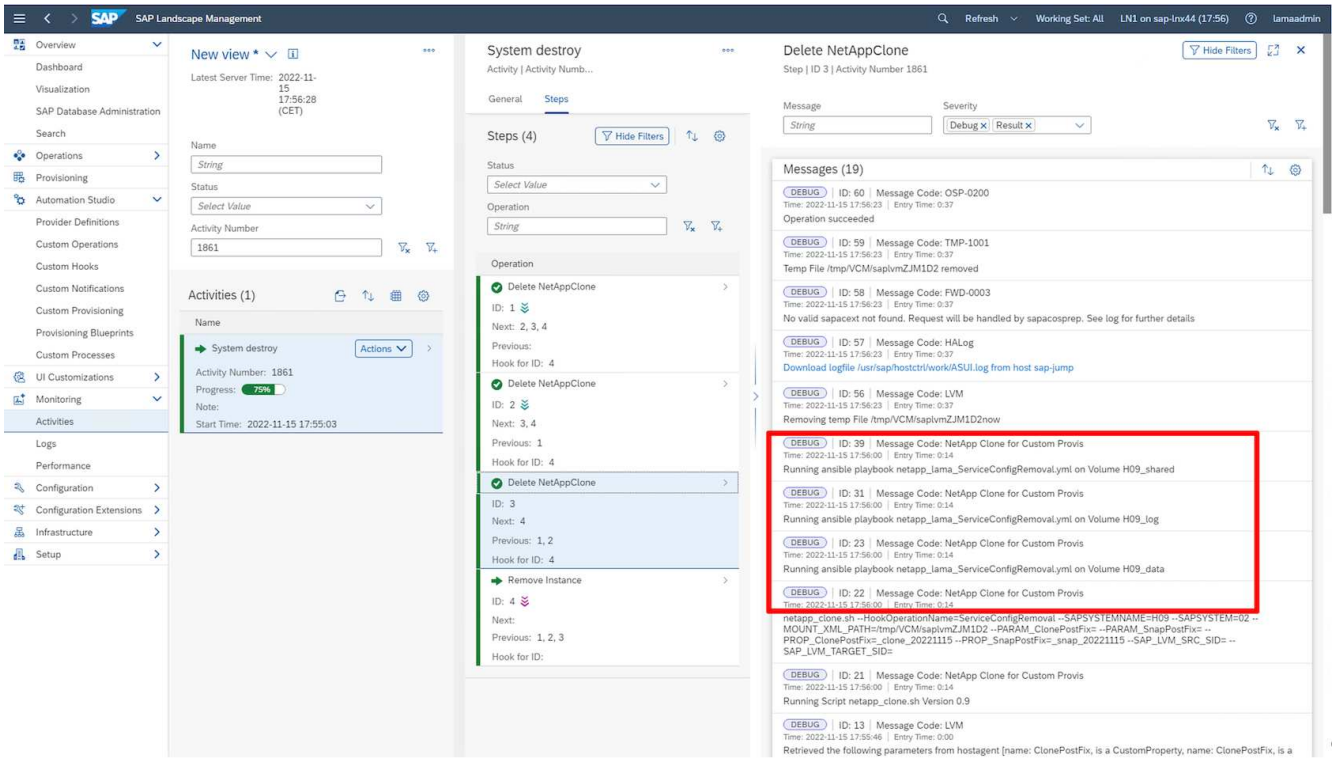


SAP lama ora esegue l'eliminazione dei cloni del volume ed elimina la configurazione del sistema clonato.

5. È possibile monitorare l'avanzamento del flusso di lavoro dei cloni nel menu **Monitoring**.

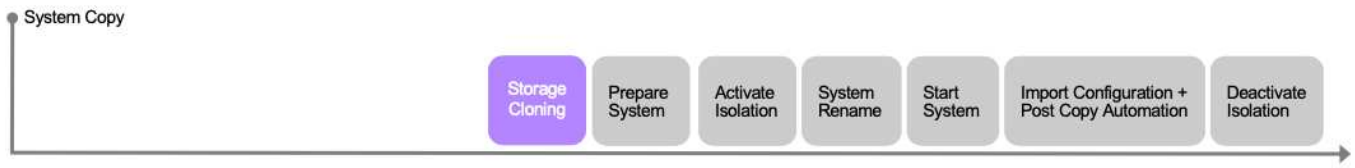


6. Selezionando l'attività **Delete NetAppClone** (Elimina NetAppClone*), viene visualizzato il log dettagliato di tale operazione. L'esecuzione del manuale Ansible è illustrata qui. Come puoi vedere, il playbook Ansible `netapp_lama_ServiceConfigRemoval.yml` Viene eseguito per ogni volume di database HANA, dati, log e condiviso.

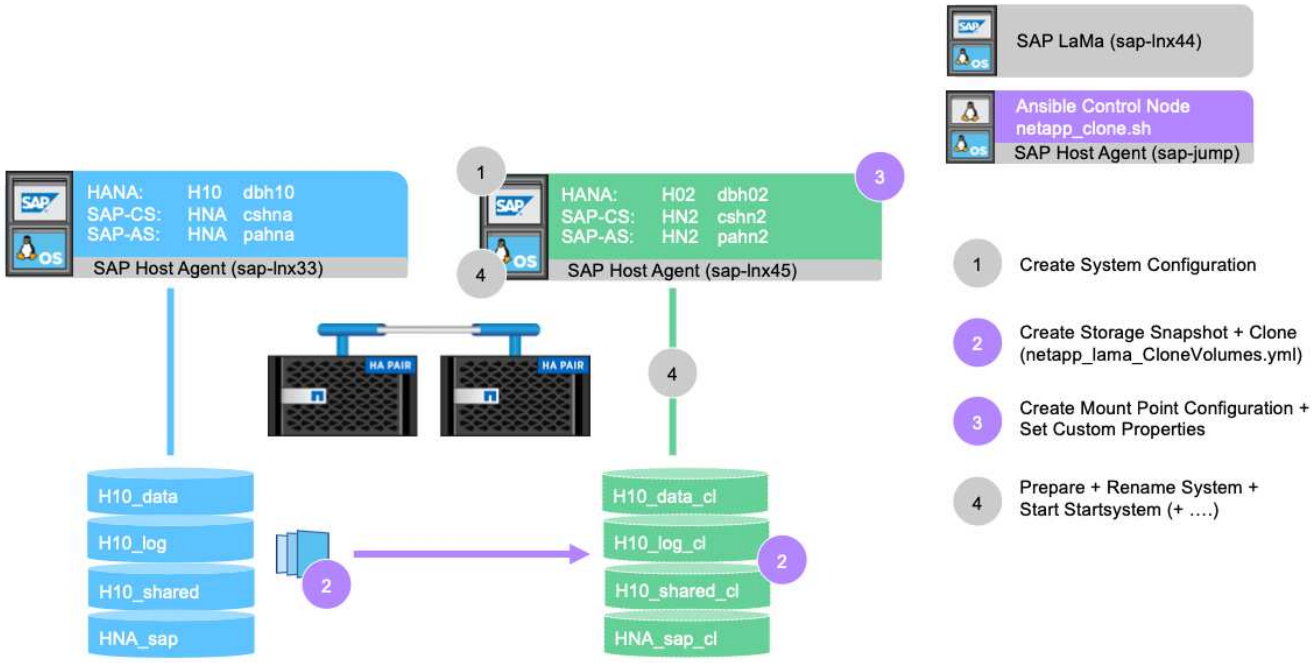


Workflow di provisioning SAP lama - sistema di copia

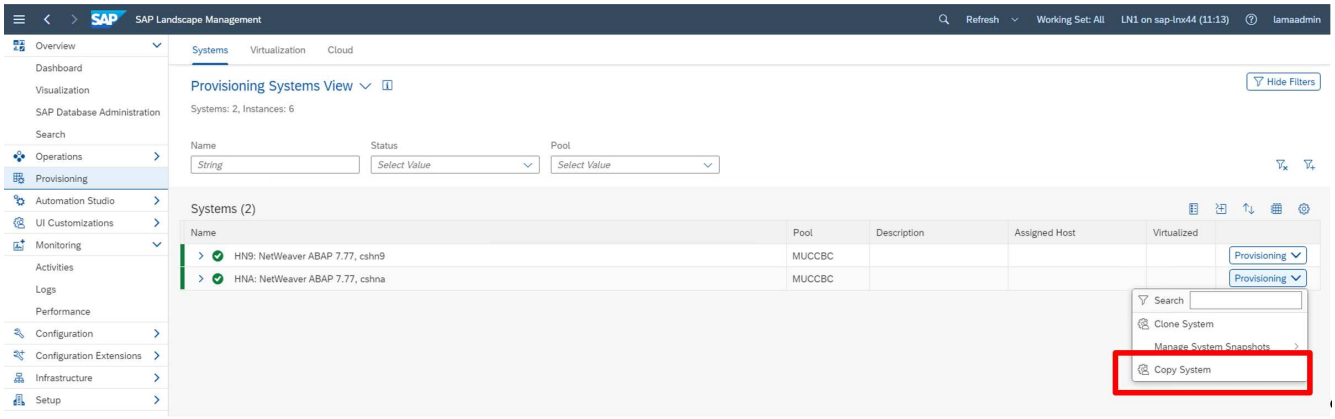
La figura seguente evidenzia i passaggi principali eseguiti con il flusso di lavoro di copia del sistema.



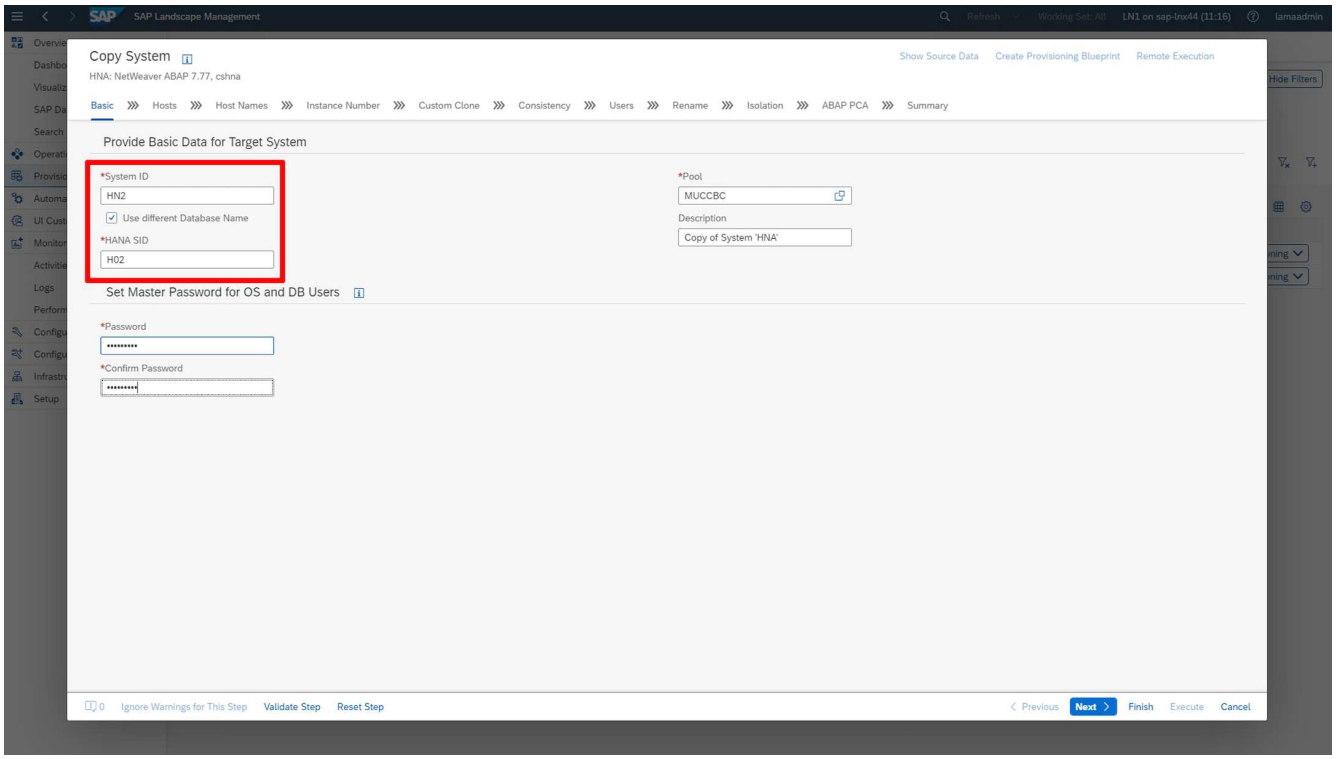
In questo capitolo, discuteremo brevemente delle differenze per il flusso di lavoro dei cloni di sistema e le schermate di input. Come si può vedere nell'immagine seguente, non cambia nulla nel flusso di lavoro dello storage.



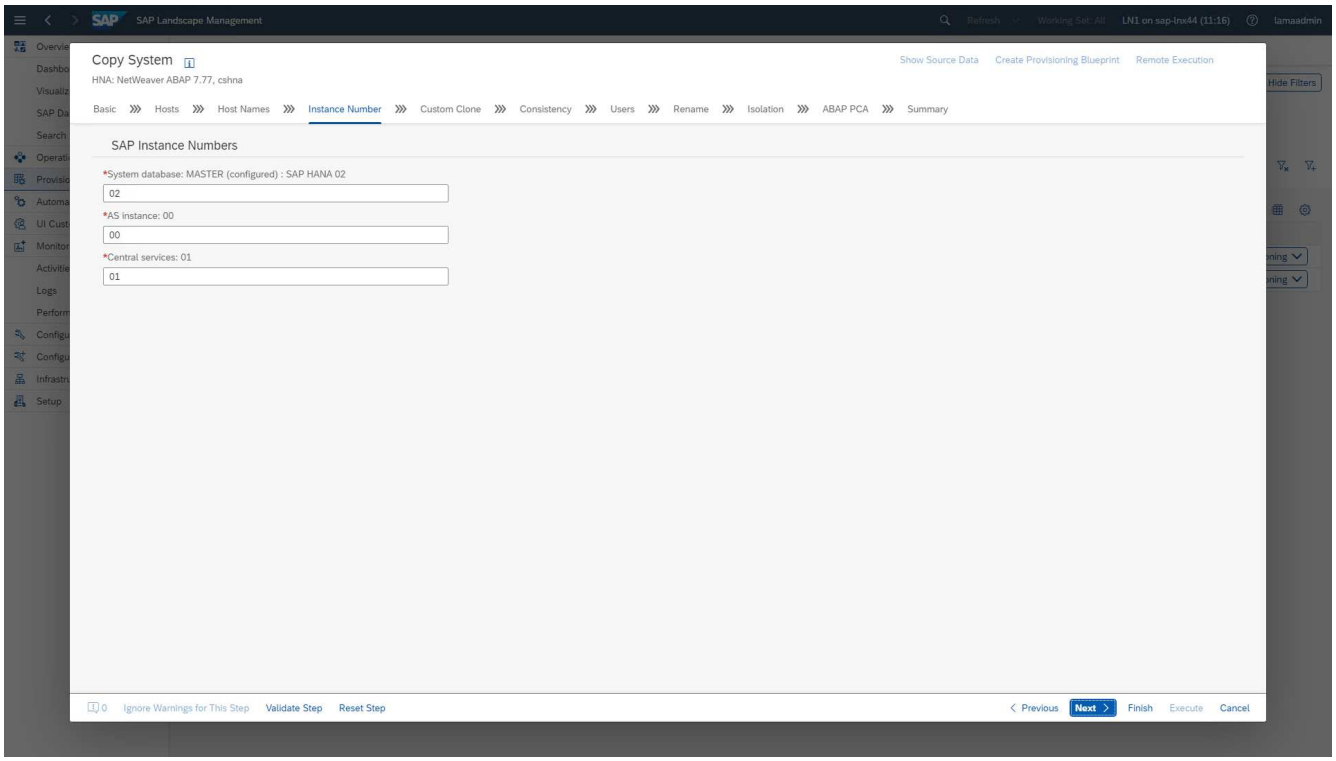
1. Il flusso di lavoro di copia del sistema può essere avviato quando il sistema viene preparato di conseguenza. Non si tratta di un'attività specifica per questa configurazione e non viene spiegata in dettaglio. Per ulteriori informazioni, consulta la documentazione di SAP lama.



2. Durante il flusso di lavoro di copia, il sistema viene rinominato, come deve essere specificato nella prima schermata.

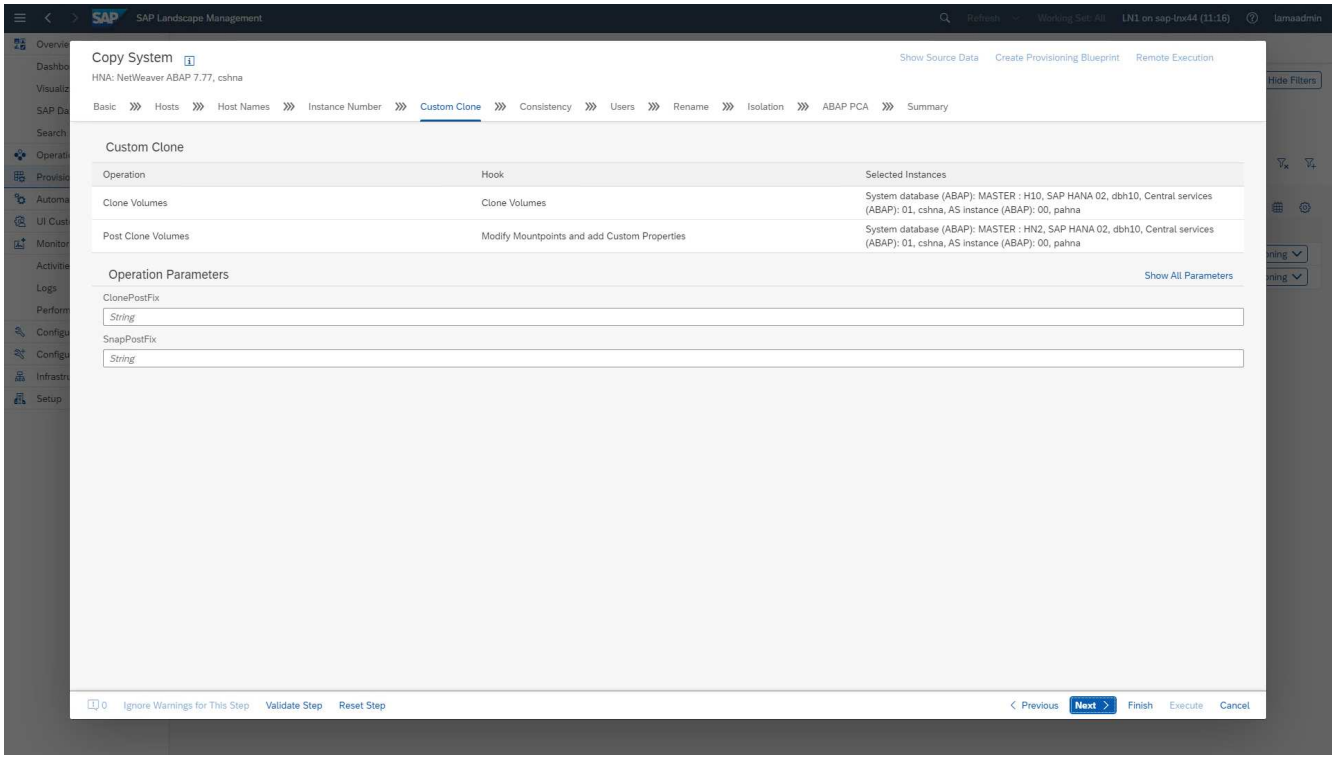


3. Durante il flusso di lavoro, è possibile modificare i numeri di istanza.

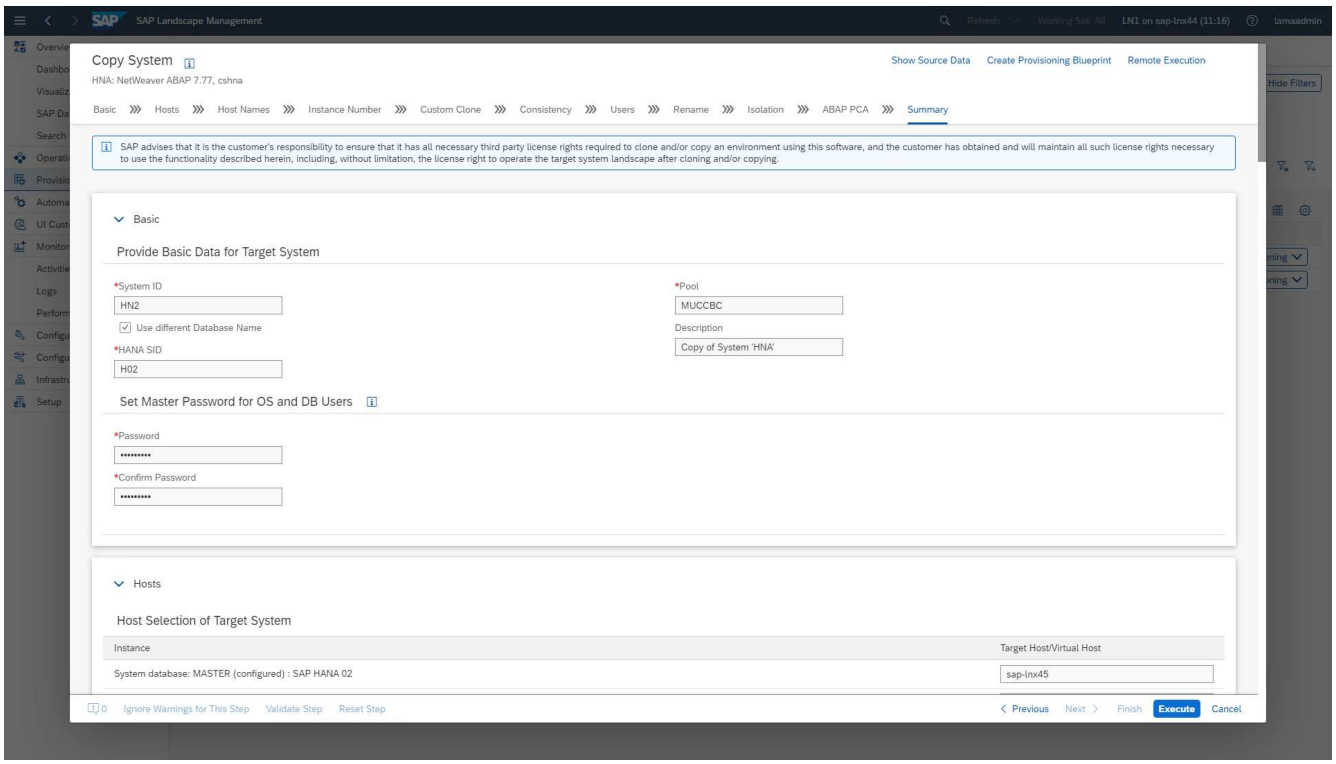


> La modifica dei numeri di istanza non è stata testata e potrebbe richiedere modifiche nello script del provider.

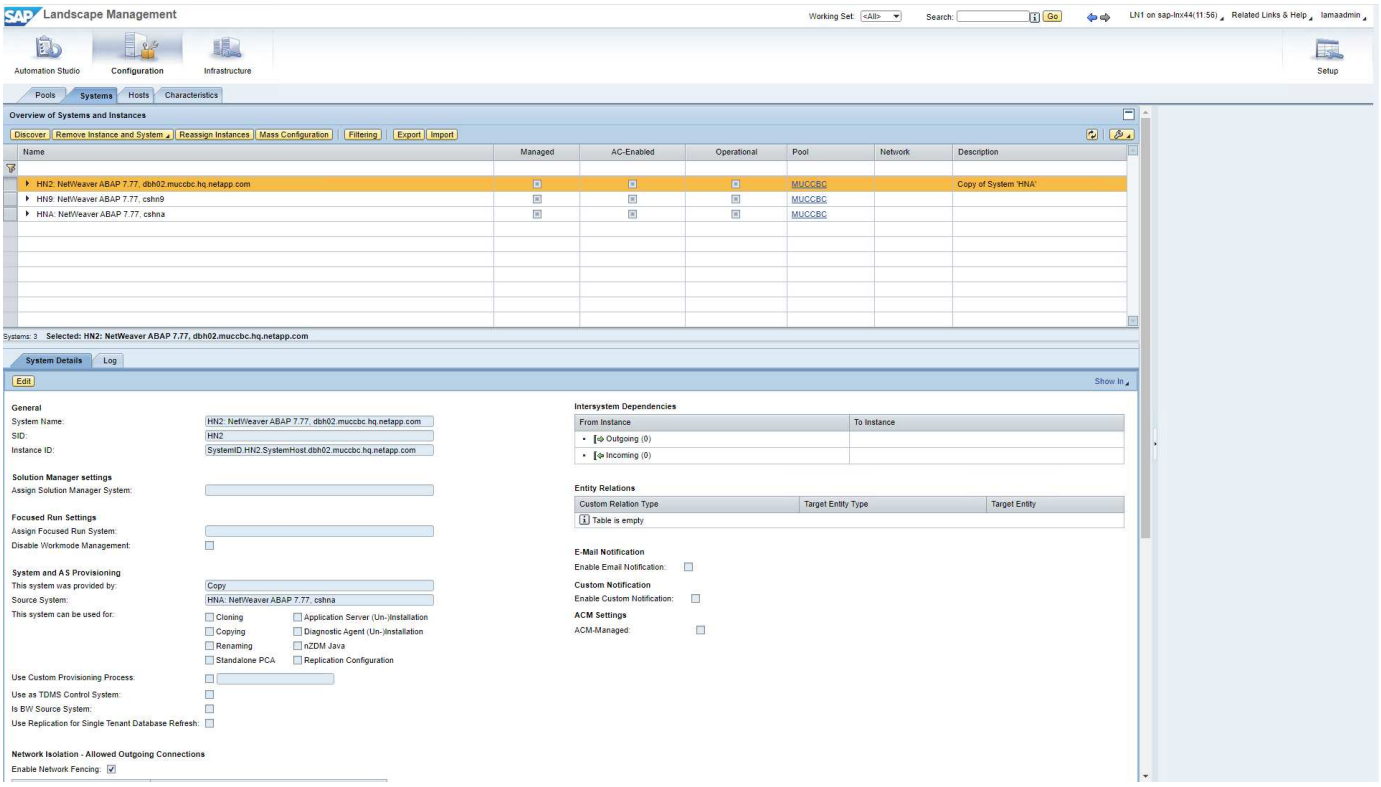
4. Come descritto, la schermata **Custom Clone** non differisce dal flusso di lavoro di cloning, come illustrato di seguito.



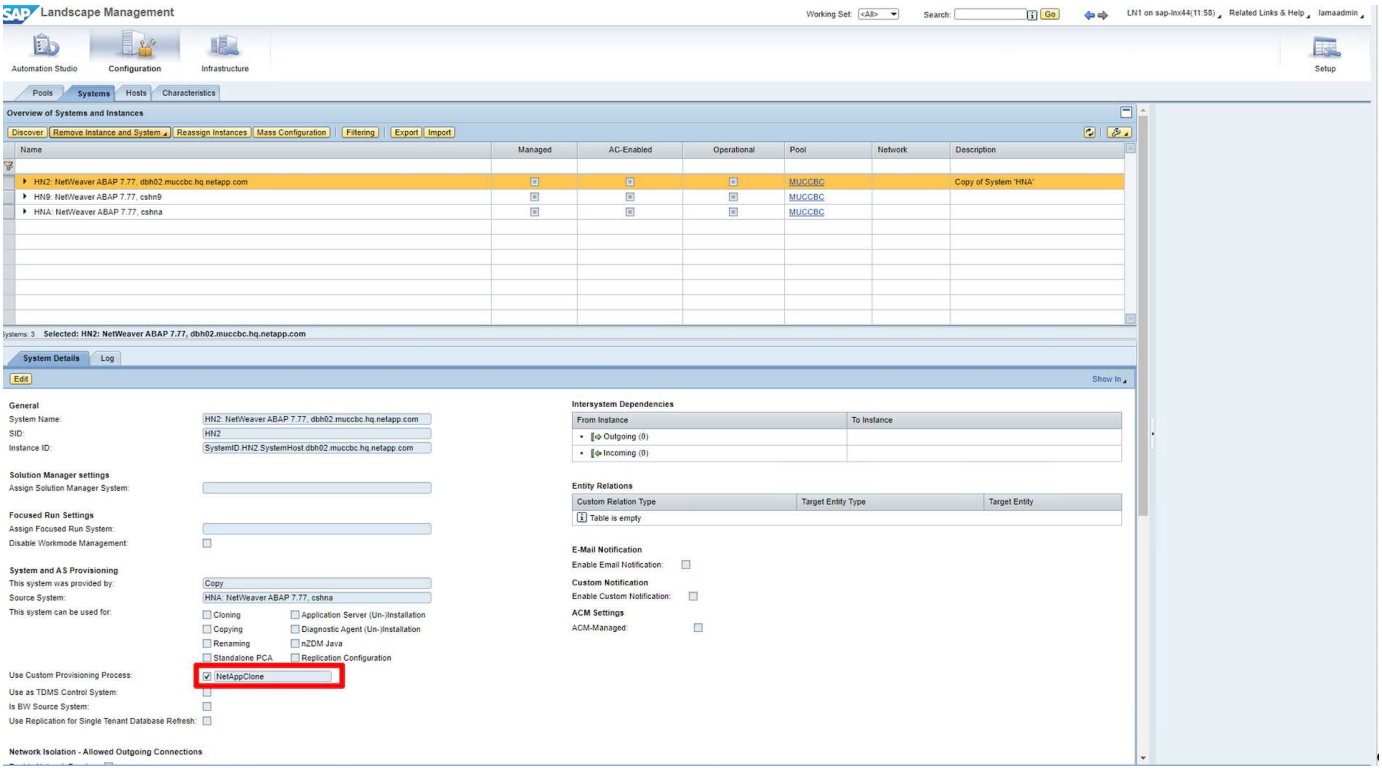
5. Come abbiamo già descritto, le restanti maschere di input non si discostano dallo standard e non vengono ulteriormente descritte in questa sede. La schermata finale mostra un riepilogo e ora è possibile avviare l'esecuzione.



Dopo il processo di copia, l'istanza di destinazione non viene attivata per il processo di clonazione personalizzato.

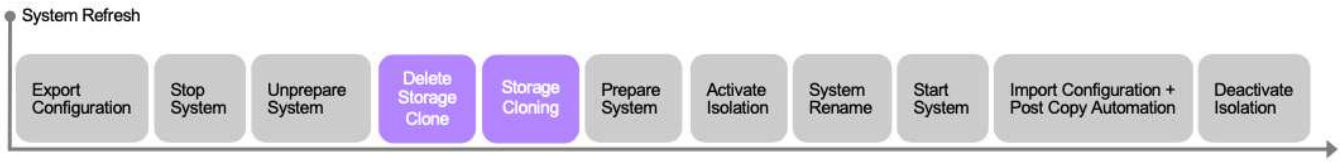


Deve essere adottato manualmente per eseguire la fase di pre-hook durante il processo di distruzione del sistema, in quanto viene impostato un vincolo che impedirebbe l'esecuzione.

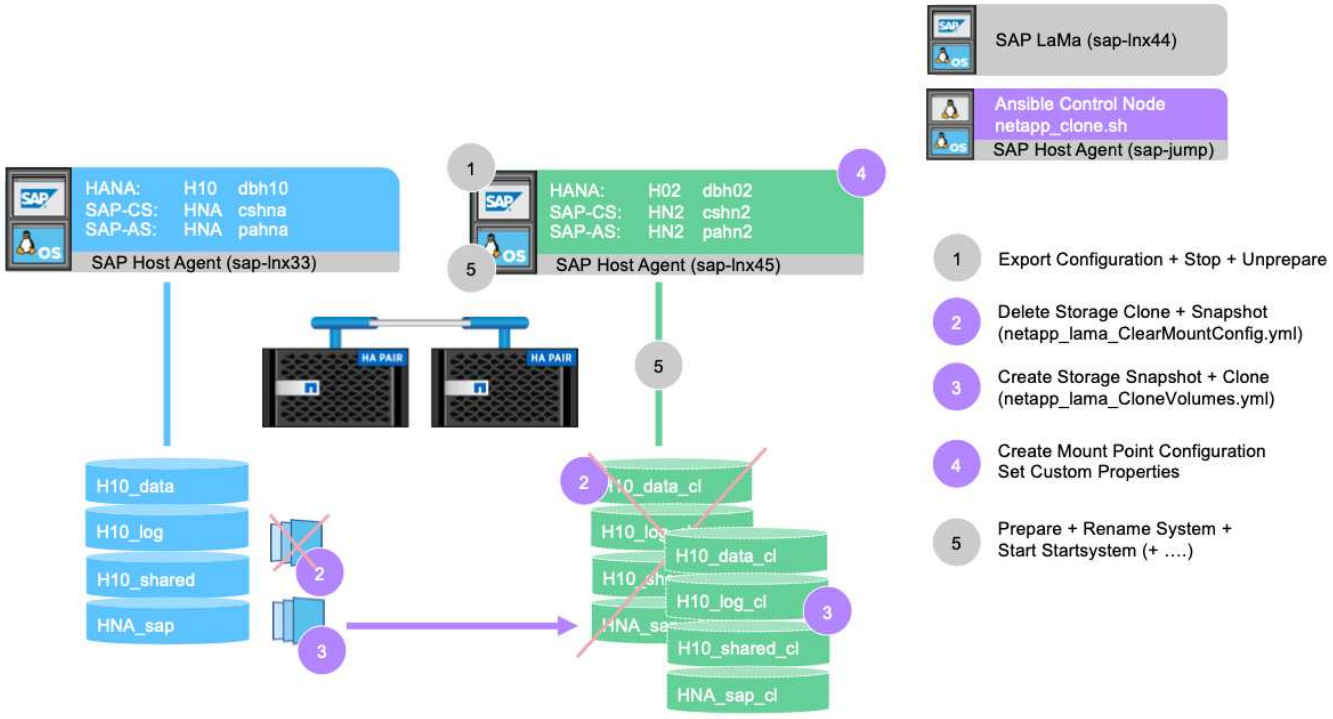


Workflow di provisioning SAP lama - refresh del sistema

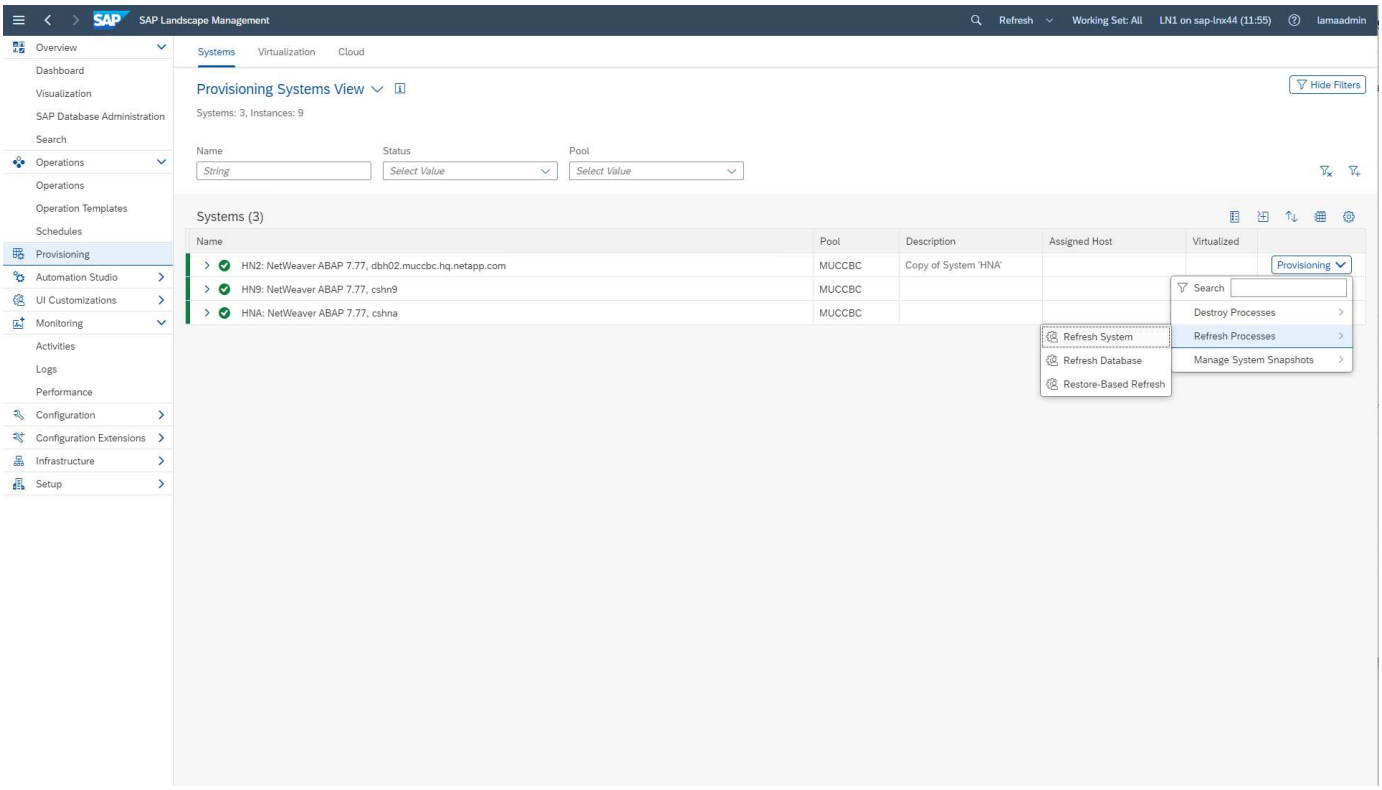
La figura seguente evidenzia i passaggi principali eseguiti con il flusso di lavoro di refresh del sistema.



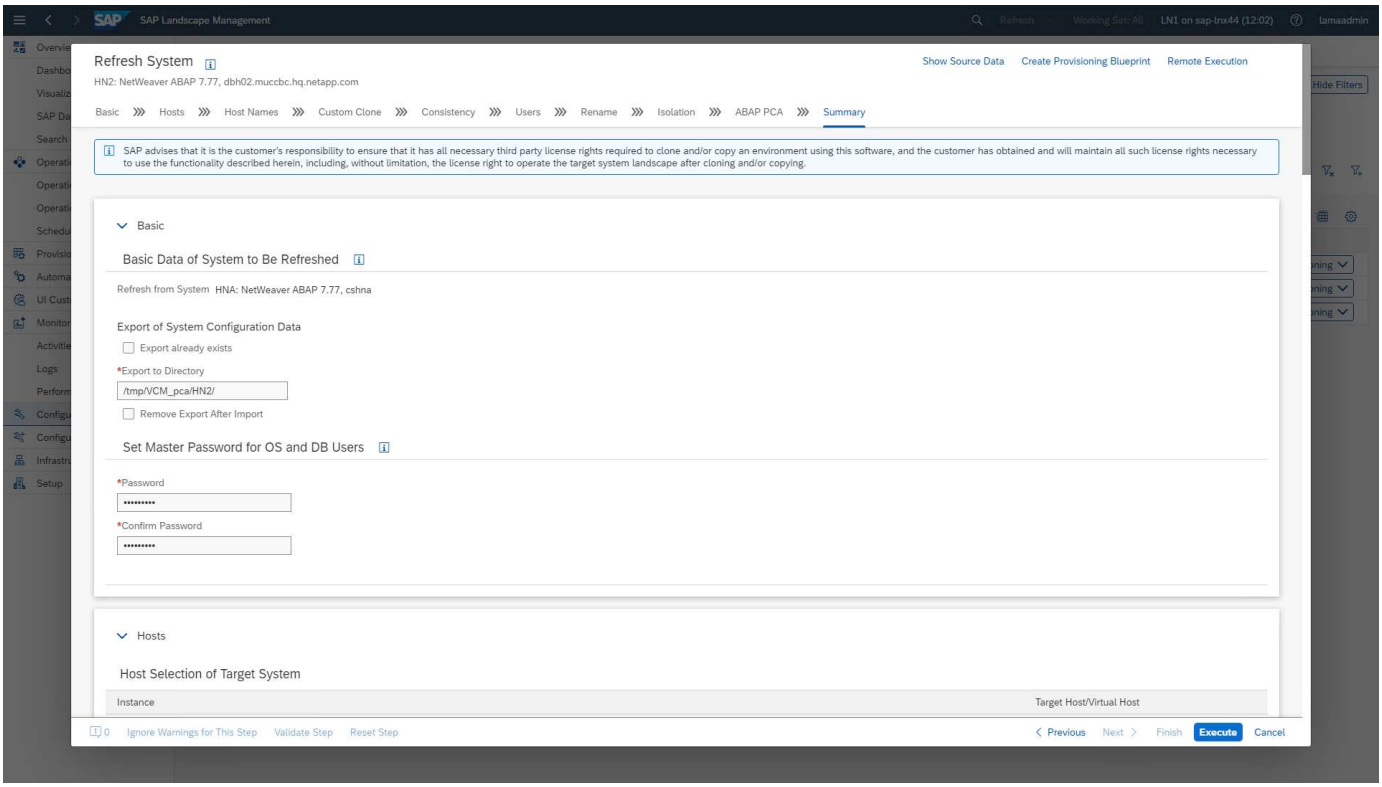
Durante il flusso di lavoro di refresh, il clone dello storage deve essere cancellato. È possibile utilizzare lo stesso playbook Ansible del flusso di lavoro System Destroy. Tuttavia, il gancio personalizzato viene definito in base a un passo diverso, quindi il playbook viene chiamato di conseguenza. La fase del processo per il clonen´t diversa.



Il flusso di lavoro di refresh può essere attivato attraverso la schermata di provisioning per un sistema copiato.



Anche in questo caso, nulla differenzia le schermate di input dallo standard e l'esecuzione del workflow può essere avviata dalla schermata di riepilogo.



Configurazione dello script del provider e playbook Ansible

I seguenti file di configurazione del provider, script di esecuzione e playbook Ansible

vengono utilizzati durante l'implementazione di esempio e l'esecuzione del flusso di lavoro in questa documentazione.

Gli script di esempio vengono forniti così come sono e non sono supportati da NetApp. Puoi richiedere la versione corrente degli script via email a ng-sapcc@netapp.com.

File di configurazione del provider netapp_clone.conf

Il file di configurazione viene creato come descritto in "Documentazione SAP lama - Configurazione degli script registrati SAP host Agent". Questo file di configurazione deve trovarsi nel nodo di controllo Ansible in cui è installato l'agente host SAP.

L'utente del sistema operativo configurato `sapuser` Deve disporre delle autorizzazioni appropriate per eseguire lo script e i playbook Ansible denominati. È possibile inserire lo script in una directory di script comune. SAP lama può fornire più parametri quando si chiama lo script.

Oltre ai parametri personalizzati, `PARAM_ClonePostFix`, `PROP_ClonePostFix`, `PARAM_ClonePostFix`, e. `PROP_ClonePostFix`, molti altri possono essere consegnati, come mostrato nella "Documentazione SAP lama".

```
root@sap-jump:~# cat /usr/sap/hostctrl/exe/operations.d/netapp_clone.conf
Name: netapp_clone
Username: sapuser
Description: NetApp Clone for Custom Provisioning
Command: /usr/sap/scripts/netapp_clone.sh
--HookOperationName=$[HookOperationName] --SAPSYSTEMNAME=$[SAPSYSTEMNAME]
--SAPSYSTEM=$[SAPSYSTEM] --MOUNT_XML_PATH=$[MOUNT_XML_PATH]
--PARAM_ClonePostFix=$[PARAM-ClonePostFix] --PARAM_SnapPostFix=$[PARAM
-SnapPostFix] --PROP_ClonePostFix=$[PROP-ClonePostFix]
--PROP_SnapPostFix=$[PROP-SnapPostFix]
--SAP_LVM_SRC_SID=$[SAP_LVM_SRC_SID]
--SAP_LVM_TARGET_SID=$[SAP_LVM_TARGET_SID]
ResulConverter: hook
Platform: Unix
```

Script del provider netapp_clone.sh

Lo script del provider deve essere memorizzato in `/usr/sap/scripts` come configurato nel file di configurazione del provider.

Variabili

Le seguenti variabili sono codificate nello script e devono essere adattate di conseguenza.

- `PRIMARY_CLUSTER`=<hostname of netapp cluster>
- `PRIMARY_SVM`=<SVM name where source system volumes are stored>

I file di certificato `PRIMARY_KEYFILE=/usr/sap/scripts/ansible/certs/ontap.key` e. `PRIMARY_CERTFILE=/usr/sap/scripts/ansible/certs/ontap.pem` deve essere fornito come

descritto in "Moduli NetApp Ansible - preparazione di ONTAP".

> Se sono richiesti cluster o SVM diversi per diversi sistemi SAP, queste variabili possono essere aggiunte come parametri nella definizione del provider SAP lama.

Funzione: Creazione del file di inventario

Per rendere l'esecuzione di Ansible Playbook più dinamica, un `inventory. yml` il file viene creato in tempo reale. Alcuni valori statici sono configurati nella sezione delle variabili e alcuni vengono creati dinamicamente durante l'esecuzione.

Funzione: Eseguire il playbook Ansible

Questa funzione viene utilizzata per eseguire il playbook Ansible insieme a quello creato dinamicamente `inventory.yml` file. La convenzione di naming per i playbook è `netapp_lama_${HookOperationName}.yml`. I valori per `${HookOperationName}` Dipende dall'operazione lama e viene consegnato da lama come parametro della riga di comando.

Sezione principale

Questa sezione contiene il principale piano di esecuzione. La variabile `${HookOperationName}` Contiene il nome del passo lama replacement e viene fornito da lama quando lo script viene chiamato.

- Valori con il clone di sistema e il workflow di provisioning delle copie di sistema:
  - CloneVolumes
  - PostCloneVolumes
- Valore con il workflow di distruzione del sistema:
  - ServiceConfigRemoval
- Valore con il workflow di refresh del sistema:
  - ClearMountConfig

HookOperationName = CloneVolumes

Con questo passaggio, viene eseguito il playbook Ansible, che attiva l'operazione di copia e clonazione Snapshot. I nomi dei volumi e la configurazione del montaggio vengono trasferiti da SAP lama attraverso un file XML definito nella variabile `$MOUNT_XML_PATH`. Questo file viene salvato perché viene utilizzato successivamente nel passo `FinalizeCloneVolumes` per creare la nuova configurazione del punto di montaggio. I nomi dei volumi vengono estratti dal file XML e viene eseguito il playbook di clonazione Ansible per ciascun volume.

> In questo esempio, l'istanza AS e i servizi centrali condividono lo stesso volume. Pertanto, la clonazione del volume viene eseguita solo quando il numero dell'istanza SAP (`$SAPSYSTEM`) non lo è `01`. Questo potrebbe differire in altri ambienti e deve essere modificato di conseguenza.

HookOperationName = PostCloneVolumes

Durante questa fase, le proprietà personalizzate `ClonePostFix` e. `SnapPostFix` e la configurazione del punto di montaggio per il sistema di destinazione viene mantenuta.

Le proprietà personalizzate vengono utilizzate in seguito come input quando il sistema viene dismesso durante il `ServiceConfigRemoval` oppure `ClearMountConfig` fase. Il sistema è progettato per conservare le

impostazioni dei parametri personalizzati specificati durante il flusso di lavoro di provisioning del sistema.

I valori utilizzati in questo esempio sono `ClonePostFix=_clone_20221115` e. `SnapPostFix=_snap_20221115`.

Per il volume `HN9_sap`, Il file Ansible creato dinamicamente include i seguenti valori: `datavolumename: HN9_sap`, `snapshotpostfix: _snap_20221115`, e. `clonepostfix: _clone_20221115`.

Che porta al nome dello snapshot sul volume HN9_sap `HN9_sap_snap_20221115` e il nome del clone del volume creato `HN9_sap_clone_20221115`.

> Le proprietà personalizzate possono essere utilizzate in qualsiasi modo per preservare i parametri utilizzati durante il processo di provisioning.

La configurazione del punto di montaggio viene estratta dal file XML consegnato da lama in `CloneVolume` fase. Il `ClonePostFix` Viene aggiunto ai nomi dei volumi e inviato a lama attraverso l'output dello script predefinito. La funzionalità è descritta in "Nota SAP 1889590".

> In questo esempio, i qtree sul sistema storage vengono utilizzati come metodo comune per posizionare dati diversi su un singolo volume. Ad esempio, `HN9_sap` contiene i punti di montaggio per `/usr/sap/HN9`, `/sapmnt/HN9`, e. `/home/hn9adm`. Le sottodirectory funzionano allo stesso modo. Questo potrebbe differire in altri ambienti e deve essere modificato di conseguenza.

HookOperationName = ServiceConfigRemoval

In questa fase, è in esecuzione il playbook Ansible responsabile dell'eliminazione dei cloni dei volumi.

I nomi dei volumi vengono trasferiti da SAP lama attraverso il file di configurazione del montaggio e le proprietà personalizzate `ClonePostFix` e. `SnapPostFix` vengono utilizzati per consegnare i valori dei parametri originariamente specificati durante il flusso di lavoro di provisioning del sistema (vedere la nota all'indirizzo `HookOperationName = PostCloneVolumes`).

I nomi dei volumi vengono estratti dal file xml e viene eseguito il playbook di clonazione Ansible per ciascun volume.

> In questo esempio, l'istanza AS e i servizi centrali condividono lo stesso volume. Pertanto, l'eliminazione del volume viene eseguita solo quando il numero dell'istanza SAP (`$SAPSYSTEM`) non lo è `01`. Questo potrebbe differire in altri ambienti e deve essere modificato di conseguenza.

HookOperationName = ClearMountConfig

In questa fase, è in esecuzione il playbook Ansible, responsabile dell'eliminazione dei cloni dei volumi durante un flusso di lavoro di refresh del sistema.

I nomi dei volumi vengono trasferiti da SAP lama attraverso il file di configurazione del montaggio e le proprietà personalizzate `ClonePostFix` e. `SnapPostFix` vengono utilizzati per consegnare i valori dei parametri originariamente specificati durante il flusso di lavoro di provisioning del sistema.

I nomi dei volumi vengono estratti dal file XML e viene eseguito il playbook di clonazione Ansible per ciascun volume.

In questo esempio, l'istanza AS e i servizi centrali condividono lo stesso volume. Pertanto, l'eliminazione del volume viene eseguita solo quando il numero dell'istanza SAP (`$SAPSYSTEM`) non lo è `01`. Questo potrebbe differire in altri ambienti e deve essere modificato di conseguenza.

```
root@sap-jump:~# cat /usr/sap/scripts/netapp_clone.sh
#!/bin/bash
#Section - Variables
########################################
VERSION="Version 0.9"
#Path for ansible play-books
ANSIBLE_PATH=/usr/sap/scripts/ansible
#Values for Ansible Inventory File
PRIMARY_CLUSTER=grenada
PRIMARY_SVM=svm-sap01
PRIMARY_KEYFILE=/usr/sap/scripts/ansible/certs/ontap.key
PRIMARY_CERTFILE=/usr/sap/scripts/ansible/certs/ontap.pem
#Default Variable if PARAM ClonePostFix / SnapPostFix is not maintained in
LaMa
DefaultPostFix=_clone_1
#TMP Files - used during execution
YAML_TMP=/tmp/inventory_ansible_clone_tmp_$$.yml
TMPFILE=/tmp/tmpfile.$$
MY_NAME="`basename $0`"
BASE_SCRIPT_DIR="`dirname $0`"
#Sendig Script Version and run options to LaMa Log
echo "[DEBUG]: Running Script $MY_NAME $VERSION"
echo "[DEBUG]: $MY_NAME $@"
#Command declared in the netapp_clone.conf Provider definition
#Command: /usr/sap/scripts/netapp_clone.sh
--HookOperationName=$[HookOperationName] --SAPSYSTEMNAME=$[SAPSYSTEMNAME]
--SAPSYSTEM=$[SAPSYSTEM] --MOUNT_XML_PATH=$[MOUNT_XML_PATH]
--PARAM_ClonePostFix=$[PARAM-ClonePostFix] --PARAM_SnapPostFix=$[PARAM
-SnapPostFix] --PROP_ClonePostFix=$[PROP-ClonePostFix]
--PROP_SnapPostFix=$[PROP-SnapPostFix]
--SAP_LVM_SRC_SID=$[SAP_LVM_SRC_SID]
--SAP_LVM_TARGET_SID=$[SAP_LVM_TARGET_SID]
#Reading Input Variables hand over by LaMa
for i in "$@"
do
case $i in
--HookOperationName=*)
HookOperationName="${i#*=}";shift;;
--SAPSYSTEMNAME=*)
SAPSYSTEMNAME="${i#*=}";shift;;
--SAPSYSTEM=*)
```

```
SAPSYSTEM="${i#*=}";shift;;
--MOUNT_XML_PATH=*)
MOUNT_XML_PATH="${i#*=}";shift;;
--PARAM_ClonePostFix=*)
PARAM_ClonePostFix="${i#*=}";shift;;
--PARAM_SnapPostFix=*)
PARAM_SnapPostFix="${i#*=}";shift;;
--PROP_ClonePostFix=*)
PROP_ClonePostFix="${i#*=}";shift;;
--PROP_SnapPostFix=*)
PROP_SnapPostFix="${i#*=}";shift;;
--SAP_LVM_SRC_SID=*)
SAP_LVM_SRC_SID="${i#*=}";shift;;
--SAP_LVM_TARGET_SID=*)
SAP_LVM_TARGET_SID="${i#*=}";shift;;
*)
# unknown option
;;
esac
done
#If Parameters not provided by the User - defaulting to DefaultPostFix
if [ -z $PARAM_ClonePostFix ]; then PARAM_ClonePostFix=$DefaultPostFix;fi
if [ -z $PARAM_SnapPostFix ]; then PARAM_SnapPostFix=$DefaultPostFix;fi
#Section - Functions
########################################
#Function Create (Inventory) YML File
########################################
create_yml_file()
{
echo "ontapservers:">$YAML_TMP
echo " hosts:">>$YAML_TMP
echo "  ${PRIMARY_CLUSTER}:">>$YAML_TMP
echo "   ansible_host: "'"'$PRIMARY_CLUSTER'"'">>$YAML_TMP
echo "   keyfile: "'"'$PRIMARY_KEYFILE'"'">>$YAML_TMP
echo "   certfile: "'"'$PRIMARY_CERTFILE'"'">>$YAML_TMP
echo "   svmname: "'"'$PRIMARY_SVM'"'">>$YAML_TMP
echo "   datavolumename: "'"'$datavolumename'"'">>$YAML_TMP
echo "   snapshotpostfix: "'"'$snapshotpostfix'"'">>$YAML_TMP
echo "   clonepostfix: "'"'$clonepostfix'"'">>$YAML_TMP
}
#Function run ansible-playbook
########################################
run_ansible_playbook()
{
echo "[DEBUG]: Running ansible playbook
netapp_lama_${HookOperationName}.yml on Volume $datavolumename"
```

```
ansible-playbook -i $YAML_TMP
$ANSIBLE_PATH/netapp_lama_${HookOperationName}.yml
}
#Section - Main
########################################
#HookOperationName - CloneVolumes
########################################
if [ $HookOperationName = CloneVolumes ] ;then
#save mount xml for later usage - used in Section FinalizeCloneVolues to
generate the mountpoints
echo "[DEBUG]: saving mount config...."
cp $MOUNT_XML_PATH /tmp/mount_config_${SAPSYSTEMNAME}_${SAPSYSTEM}.xml
#Instance 00 + 01 share the same volumes - clone needs to be done once
if [ $SAPSYSTEM != 01 ]; then
#generating Volume List - assuming usage of qtrees - "IP-
Adress:/VolumeName/qtree"
xmlFile=/tmp/mount_config_${SAPSYSTEMNAME}_${SAPSYSTEM}.xml
if [ -e $TMPFILE ];then rm $TMPFILE;fi
numMounts=`xml_grep --count "/mountconfig/mount" $xmlFile | grep "total: "
| awk '{ print $2 }'`
i=1
while [ $i -le $numMounts ]; do
     xmllint --xpath "/mountconfig/mount[$i]/exportpath/text()" $xmlFile
|awk -F"/" '{print $2}' >>$TMPFILE
i=$((i + 1))
done
DATAVOLUMES=`cat  $TMPFILE |sort -u`
#Create yml file and rund playbook for each volume
for I in $DATAVOLUMES; do
datavolumename="$I"
snapshotpostfix="$PARAM_SnapPostFix"
clonepostfix="$PARAM_ClonePostFix"
create_yml_file
run_ansible_playbook
done
else
echo "[DEBUG]: Doing nothing .... Volume cloned in different Task"
fi
fi
#HookOperationName - PostCloneVolumes
########################################
if [ $HookOperationName = PostCloneVolumes] ;then
#Reporting Properties back to LaMa Config for Cloned System
echo "[RESULT]:Property:ClonePostFix=$PARAM_ClonePostFix"
echo "[RESULT]:Property:SnapPostFix=$PARAM_SnapPostFix"
#Create MountPoint Config for Cloned Instances and report back to LaMa
```

```
according to SAP Note: https://launchpad.support.sap.com/#/notes/1889590
echo "MountDataBegin"
echo '<?xml version="1.0" encoding="UTF-8"?>'
echo "<mountconfig>"
xmlFile=/tmp/mount_config_${SAPSYSTEMNAME}_${SAPSYSTEM}.xml
numMounts=`xml_grep --count "/mountconfig/mount" $xmlFile | grep "total: "
| awk '{ print $2 }'`
i=1
while [ $i -le $numMounts ]; do
MOUNTPOINT=`xmllint --xpath "/mountconfig/mount[$i]/mountpoint/text()"
$xmlFile`;
        EXPORTPATH=`xmllint --xpath
"/mountconfig/mount[$i]/exportpath/text()" $xmlFile`;
        OPTIONS=`xmllint --xpath "/mountconfig/mount[$i]/options/text()"
$xmlFile`;
#Adopt Exportpath and add Clonepostfix - assuming usage of qtrees - "IP-
Adress:/VolumeName/qtree"
TMPFIELD1=`echo $EXPORTPATH|awk -F":/" '{print $1}'`
TMPFIELD2=`echo $EXPORTPATH|awk -F"/" '{print $2}'`
TMPFIELD3=`echo $EXPORTPATH|awk -F"/" '{print $3}'`
EXPORTPATH=$TMPFIELD1":/"${TMPFIELD2}$PARAM_ClonePostFix"/"$TMPFIELD3
echo -e '\t<mount fstype="nfs" storagetype="NETFS">'
echo -e "\t\t<mountpoint>${MOUNTPOINT}</mountpoint>"
echo -e "\t\t<exportpath>${EXPORTPATH}</exportpath>"
echo -e "\t\t<options>${OPTIONS}</options>"
echo -e "\t</mount>"
i=$((i + 1))
done
echo "</mountconfig>"
echo "MountDataEnd"
#Finished MountPoint Config
#Cleanup Temporary Files
rm $xmlFile
fi
#HookOperationName – ServiceConfigRemoval
########################################
if [ $HookOperationName = ServiceConfigRemoval ] ;then
#Assure that Properties ClonePostFix and SnapPostfix has been configured
through the provisioning process
if [ -z $PROP_ClonePostFix ]; then echo "[ERROR]: Propertiy ClonePostFix
is not handed over - please investigate";exit 5;fi
if [ -z $PROP_SnapPostFix ]; then echo "[ERROR]: Propertiy SnapPostFix is
not handed over - please investigate";exit 5;fi
#Instance 00 + 01 share the same volumes - clone delete needs to be done
once
if [ $SAPSYSTEM != 01 ]; then
```

```
#generating Volume List - assuming usage of qtrees - "IP-
Adress:/VolumeName/qtree"
xmlFile=$MOUNT_XML_PATH
if [ -e $TMPFILE ];then rm $TMPFILE;fi
numMounts=`xml_grep --count "/mountconfig/mount" $xmlFile | grep "total: "
| awk '{ print $2 }'`
i=1
while [ $i -le $numMounts ]; do
     xmllint --xpath "/mountconfig/mount[$i]/exportpath/text()" $xmlFile
|awk -F"/" '{print $2}' >>$TMPFILE
i=$((i + 1))
done
DATAVOLUMES=`cat  $TMPFILE |sort -u| awk -F $PROP_ClonePostFix '{ print $1
}'`
#Create yml file and rund playbook for each volume
for I in $DATAVOLUMES; do
datavolumename="$I"
snapshotpostfix="$PROP_SnapPostFix"
clonepostfix="$PROP_ClonePostFix"
create_yml_file
run_ansible_playbook
done
else
echo "[DEBUG]: Doing nothing .... Volume deleted in different Task"
fi
#Cleanup Temporary Files
rm $xmlFile
fi
#HookOperationName - ClearMountConfig
########################################
if [ $HookOperationName = ClearMountConfig ] ;then
        #Assure that Properties ClonePostFix and SnapPostfix has been
configured through the provisioning process
        if [ -z $PROP_ClonePostFix ]; then echo "[ERROR]: Propertiy
ClonePostFix is not handed over - please investigate";exit 5;fi
        if [ -z $PROP_SnapPostFix ]; then echo "[ERROR]: Propertiy
SnapPostFix is not handed over - please investigate";exit 5;fi
        #Instance 00 + 01 share the same volumes - clone delete needs to
be done once
        if [ $SAPSYSTEM != 01 ]; then
                #generating Volume List - assuming usage of qtrees - "IP-
Adress:/VolumeName/qtree"
                xmlFile=$MOUNT_XML_PATH
                if [ -e $TMPFILE ];then rm $TMPFILE;fi
                numMounts=`xml_grep --count "/mountconfig/mount" $xmlFile
| grep "total: " | awk '{ print $2 }'`
```

```
                i=1
                while [ $i -le $numMounts ]; do
                        xmllint --xpath
"/mountconfig/mount[$i]/exportpath/text()" $xmlFile |awk -F"/" '{print
$2}' >>$TMPFILE
                        i=$((i + 1))
                done
                DATAVOLUMES=`cat  $TMPFILE |sort -u| awk -F
$PROP_ClonePostFix '{ print $1 }'`
                #Create yml file and rund playbook for each volume
                for I in $DATAVOLUMES; do
                        datavolumename="$I"
                        snapshotpostfix="$PROP_SnapPostFix"
                        clonepostfix="$PROP_ClonePostFix"
                        create_yml_file
                        run_ansible_playbook
                done
        else
                echo "[DEBUG]: Doing nothing .... Volume deleted in
different Task"
        fi
        #Cleanup Temporary Files
        rm $xmlFile
fi
#Cleanup
########################################
#Cleanup Temporary Files
if [ -e $TMPFILE ];then rm $TMPFILE;fi
if [ -e $YAML_TMP ];then rm $YAML_TMP;fi
exit 0
```

Ansible Playbook netapp_lama_CloneVolumes.yml

Il playbook che viene eseguito durante la fase CloneVolumes del flusso di lavoro dei cloni del sistema lama è una combinazione di `create_snapshot.yml` e. `create_clone.yml` (vedere "Moduli NetApp Ansible - file YAML"). Questo manuale può essere facilmente esteso per coprire ulteriori casi di utilizzo come la clonazione da operazioni secondarie e di suddivisione dei cloni.

```
root@sap-jump:~# cat /usr/sap/scripts/ansible/netapp_lama_CloneVolumes.yml
---
- hosts: ontapservers
  connection: local
  collections:
    - netapp.ontap
  gather_facts: false
  name: netapp_lama_CloneVolumes
  tasks:
  - name: Create SnapShot
    na_ontap_snapshot:
      state: present
      snapshot: "{{ datavolumename }}{{ snapshotpostfix }}"
      use_rest: always
      volume: "{{ datavolumename }}"
      vserver: "{{ svmname }}"
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
  - name: Clone Volume
    na_ontap_volume_clone:
      state: present
      name: "{{ datavolumename }}{{ clonepostfix }}"
      use_rest: always
      vserver: "{{ svmname }}"
      junction_path: '/{{ datavolumename }}{{ clonepostfix }}'
      parent_volume: "{{ datavolumename }}"
      parent_snapshot: "{{ datavolumename }}{{ snapshotpostfix }}"
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
```

Ansible Playbook netapp_lama_ServiceConfigRemoval.yml

Il playbook eseguito durante il `ServiceConfigRemoval` Fase del sistema lama il workflow Destroy è una combinazione di `delete_clone.yml` e. `delete_snapshot.yml` (vedere "Moduli NetApp Ansible - file YAML"). Deve essere allineato alle fasi di esecuzione di `netapp_lama_CloneVolumes` playbook.

```
root@sap-jump:~# cat
/usr/sap/scripts/ansible/netapp_lama_ServiceConfigRemoval.yml
---
- hosts: ontapservers
  connection: local
  collections:
    - netapp.ontap
  gather_facts: false
  name: netapp_lama_ServiceConfigRemoval
  tasks:
  - name: Delete Clone
    na_ontap_volume:
      state: absent
      name: "{{ datavolumename }}{{ clonepostfix }}"
      use_rest: always
      vserver: "{{ svmname }}"
      wait_for_completion: True
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
  - name: Delete SnapShot
    na_ontap_snapshot:
      state: absent
      snapshot: "{{ datavolumename }}{{ snapshotpostfix }}"
      use_rest: always
      volume: "{{ datavolumename }}"
      vserver: "{{ svmname }}"
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
root@sap-jump:~#
```

Ansible Playbook netapp_lama_ClearMountConfig.yml

Il manuale, che viene eseguito durante il `netapp_lama_ClearMountConfig` La fase del flusso di lavoro di refresh del sistema lama è una combinazione di `delete_clone.yml` e. `delete_snapshot.yml` (vedere "Moduli NetApp Ansible - file YAML"). Deve essere allineato alle fasi di esecuzione di `netapp_lama_CloneVolumes` playbook.

```
root@sap-jump:~# cat
/usr/sap/scripts/ansible/netapp_lama_ServiceConfigRemoval.yml
---
- hosts: ontapservers
  connection: local
  collections:
    - netapp.ontap
  gather_facts: false
  name: netapp_lama_ServiceConfigRemoval
  tasks:
  - name: Delete Clone
    na_ontap_volume:
      state: absent
      name: "{{ datavolumename }}{{ clonepostfix }}"
      use_rest: always
      vserver: "{{ svmname }}"
      wait_for_completion: True
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
  - name: Delete SnapShot
    na_ontap_snapshot:
      state: absent
      snapshot: "{{ datavolumename }}{{ snapshotpostfix }}"
      use_rest: always
      volume: "{{ datavolumename }}"
      vserver: "{{ svmname }}"
      hostname: "{{ inventory_hostname }}"
      cert_filepath: "{{ certfile }}"
      key_filepath: "{{ keyfile }}"
      https: true
      validate_certs: false
root@sap-jump:~#
```

Esempio di Ansible inventory.yml

Questo file di inventario viene creato in modo dinamico durante l'esecuzione del workflow e viene mostrato qui solo a scopo illustrativo.

```
ontapservers:
 hosts:
  grenada:
   ansible_host: "grenada"
   keyfile: "/usr/sap/scripts/ansible/certs/ontap.key"
   certfile: "/usr/sap/scripts/ansible/certs/ontap.pem"
   svmname: "svm-sap01"
   datavolumename: "HN9_sap"
   snapshotpostfix: " _snap_20221115"
   clonepostfix: "_clone_20221115"
```

Conclusione

L'integrazione di un framework di automazione moderno come Ansible nei flussi di lavoro di provisioning di SAP lama offre ai clienti una soluzione flessibile per soddisfare requisiti di infrastruttura standard o più complessi.

Dove trovare ulteriori informazioni

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

- Raccolte nello spazio dei nomi NetApp

  "https://docs.ansible.com/ansible/latest/collections/netapp/index.html"

- Documentazione sull'integrazione di Ansible e esempi di Playbook Ansible

  "https://github.com/sap-linuxlab/demo.netapp_ontap"

- General Ansible e integrazione NetApp

  "https://www.ansible.com/integrations/infrastructure/netapp"

- Blog sull'integrazione di SAP lama con Ansible

  "https://blogs.sap.com/2020/06/08/outgoing-api-calls-from-sap-landscape-management-lama-with-automation-studio/"

- SAP Landscape Management 3.0, documentazione Enterprise Edition

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/4df88a8f418c5059e10000000a42189c.html#loio4df88a8f418c5059e10000000a42189c"

- Documentazione SAP lama – definizioni dei provider

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/bf6b3e43340a4cbcb0c0f3089715c068.html"

- Documentazione SAP lama - Hooks personalizzati

"https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/139eca2f925e48738a20dbf0b56674c5.html"

- Documentazione SAP lama - Configurazione degli script registrati SAP host Agent

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/250dfc5eef4047a38bab466c295d3a49.html"

- Documentazione SAP lama - parametri per operazioni personalizzate e ganci personalizzati

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/0148e495174943de8c1c3ee1b7c9cc65.html"

- Documentazione SAP lama - progettazione adattiva

  "https://help.sap.com/doc/700f9a7e52c7497cad37f7c46023b7ff/3.0.11.0/en-US/737a99e86f8743bdb8d1f6cf4b862c79.html"

- Documentazione sui prodotti NetApp

  "https://www.netapp.com/support-and-training/documentation/"

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Gennaio 2023	Release iniziale

Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter

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

Nel dinamico ambiente di business di oggi, le aziende devono fornire innovazione continua e reagire rapidamente ai mercati in continua evoluzione. In queste circostanze competitive, le aziende che implementano una maggiore flessibilità nei propri processi di lavoro possono adattarsi alle esigenze del mercato in modo più efficace.

Autore: Nils Bauer, NetApp

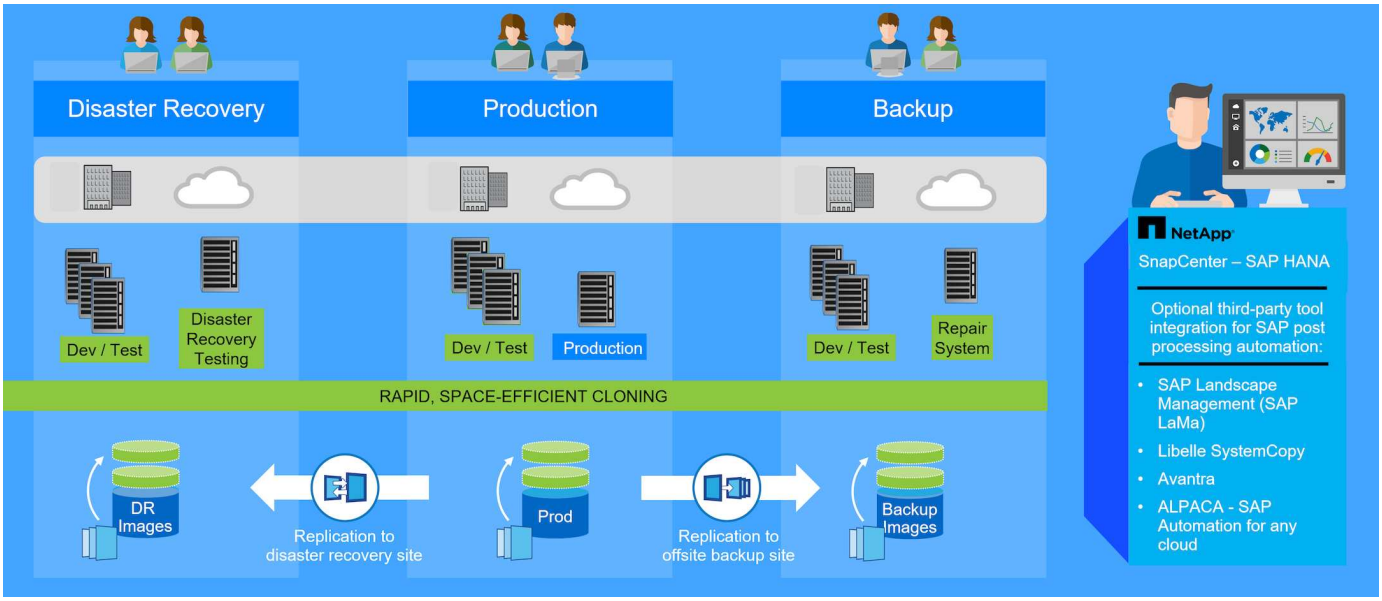
Introduzione

Le mutevoli esigenze di mercato influiscono anche sugli ambienti SAP di un'azienda, in modo da richiedere integrazioni, modifiche e aggiornamenti regolari. I reparti IT devono implementare queste modifiche con meno risorse e in periodi di tempo più brevi. Ridurre al minimo i rischi durante l'implementazione di tali modifiche richiede test e formazione completi che richiedono sistemi SAP aggiuntivi con dati effettivi provenienti dalla produzione.

Gli approcci tradizionali di gestione del ciclo di vita SAP per il provisioning di questi sistemi si basano principalmente su processi manuali. Questi processi manuali sono spesso soggetti a errori e richiedono molto

tempo, ritardando l'innovazione e la risposta ai requisiti di business.

Le soluzioni NetApp per l'ottimizzazione della gestione del ciclo di vita SAP sono integrate nei database SAP HANA e negli strumenti di gestione del ciclo di vita, combinando una protezione dei dati efficiente e integrata con l'applicazione con il provisioning flessibile dei sistemi di test SAP, come mostrato nella figura seguente. Queste soluzioni sono disponibili per SAP HANA on-premise o eseguito nel cloud su Azure NetApp Files (ANF) o Amazon FSX per NetApp ONTAP (FSX per ONTAP).



Operazioni di backup Snapshot integrate nelle applicazioni

La possibilità di creare backup Snapshot coerenti con l'applicazione nel layer di storage è la base per le operazioni di copia del sistema e cloning del sistema descritte in questo documento. I backup Snapshot basati sullo storage vengono creati utilizzando il plug-in NetApp SnapCenter per SAP HANA e le interfacce fornite dal database SAP HANA. SnapCenter registra i backup Snapshot nel catalogo di backup SAP HANA in modo che possano essere utilizzati per il ripristino e il ripristino, nonché per le operazioni di cloning.

Backup off-site e/o replica dei dati di disaster recovery

I backup Snapshot coerenti con l'applicazione possono essere replicati sul layer di storage in un sito di backup off-site o in un sito di disaster recovery controllato da SnapCenter. La replica si basa su blocchi nuovi e modificati e risulta pertanto efficiente in termini di spazio e larghezza di banda.

Utilizzare qualsiasi backup Snapshot per le operazioni di copia del sistema SAP o clonazione

La tecnologia NetApp e l'integrazione del software consentono di utilizzare qualsiasi backup Snapshot di un sistema di origine per un'operazione di copia o clonazione del sistema SAP. Questo backup Snapshot può essere selezionato dallo stesso storage utilizzato per i sistemi di produzione SAP, dallo storage utilizzato per i backup off-site o dallo storage del sito di disaster recovery. Questa flessibilità consente di separare i sistemi di sviluppo e test dalla produzione, se necessario, e copre altri scenari, come il test del disaster recovery nel sito di disaster recovery.

Il cloning dallo storage di backup o disaster recovery off-site è supportato per i sistemi NetApp on-premise e per Amazon FSX per NetApp ONTAP. Con Azure NetApp Files i cloni possono essere creati solo sul volume di origine.

Automazione con integrazione

Esistono diversi scenari e casi di utilizzo per il provisioning dei sistemi di test SAP, oltre a requisiti diversi per il livello di automazione. I prodotti software NetApp per SAP si integrano nei prodotti SAP per la gestione del ciclo di vita e dei database per supportare diversi scenari e livelli di automazione.

NetApp SnapCenter con il plug-in per SAP HANA viene utilizzato per eseguire il provisioning dei volumi di storage richiesti in base a un backup Snapshot coerente con l'applicazione e per eseguire tutte le operazioni di host e database necessarie fino a un database SAP HANA avviato. A seconda del caso d'utilizzo, potrebbero essere necessarie la copia del sistema SAP, la clonazione del sistema, il refresh del sistema o ulteriori operazioni manuali, come la post-elaborazione SAP. Ulteriori dettagli sono illustrati nella sezione successiva.

È possibile eseguire un provisioning end-to-end completamente automatizzato dei sistemi di test SAP utilizzando strumenti di terze parti e l'integrazione delle funzionalità di NetApp. Ulteriori dettagli sono disponibili all'indirizzo:

"TR-4953: Integrazione della gestione del panorama SAP di NetApp con Ansible"

"TR-4929: Automazione delle operazioni di copia del sistema SAP con libelle SystemCopy (netapp.com)"

"Automazione di copy del sistema SAP;#44; refresh, e clonazione dei flussi di lavoro con ALPACA e NetApp SnapCenter"

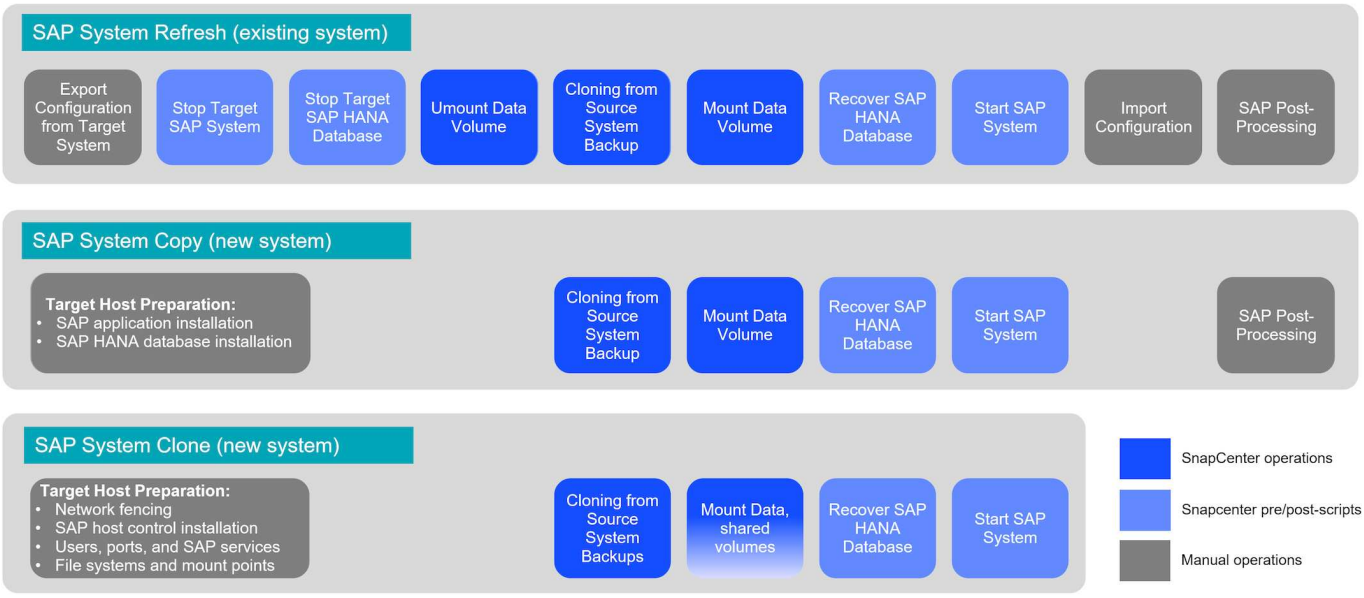
"Automazione di copy del sistema SAP;#44; refresh, e clonazione dei flussi di lavoro con Avantra e NetApp SnapCenter"

Scenari di copia, aggiornamento e clonazione del sistema SAP

Il termine copia del sistema SAP viene spesso utilizzato come sinonimo per tre diversi processi: Aggiornamento del sistema SAP, copia del sistema SAP o operazioni di clonazione del sistema SAP. È importante distinguere tra le diverse operazioni, in quanto i flussi di lavoro e i casi di utilizzo sono diversi per ciascuno di essi.

- **SAP system refresh.** un refresh del sistema SAP è un refresh di un sistema SAP di destinazione esistente con i dati di un sistema SAP di origine. Il sistema di destinazione fa generalmente parte di un ambiente di trasporto SAP, ad esempio un sistema di quality assurance, che viene aggiornato con i dati del sistema di produzione. Il nome host, il numero di istanza e il SID sono diversi per i sistemi di origine e di destinazione.
- **SAP system copy.** una copia del sistema SAP è una configurazione di un nuovo sistema SAP di destinazione con i dati di un sistema SAP di origine. Il nuovo sistema di destinazione potrebbe essere, ad esempio, un sistema di test aggiuntivo con i dati del sistema di produzione. Il nome host, il numero di istanza e il SID sono diversi per i sistemi di origine e di destinazione.
- **Clone di sistema SAP.** un clone di sistema SAP è un clone identico di un sistema SAP di origine. I cloni di sistema SAP vengono in genere utilizzati per affrontare la corruzione logica o per testare gli scenari di disaster recovery. Con un'operazione di clone del sistema, il nome host, il numero di istanza e il SID rimangono invariati. È quindi importante stabilire un corretto scherma di rete per il sistema di destinazione per assicurarsi che non vi sia comunicazione con l'ambiente di produzione.

La figura riportata di seguito illustra i principali passaggi da eseguire durante un'operazione di refresh di sistema, di copia del sistema o di clone del sistema. Le caselle blu indicano i passaggi che possono essere automatizzati con SnapCenter, mentre le caselle grigie indicano i passaggi che devono essere eseguiti al di fuori di SnapCenter, manualmente o utilizzando strumenti di terze parti.

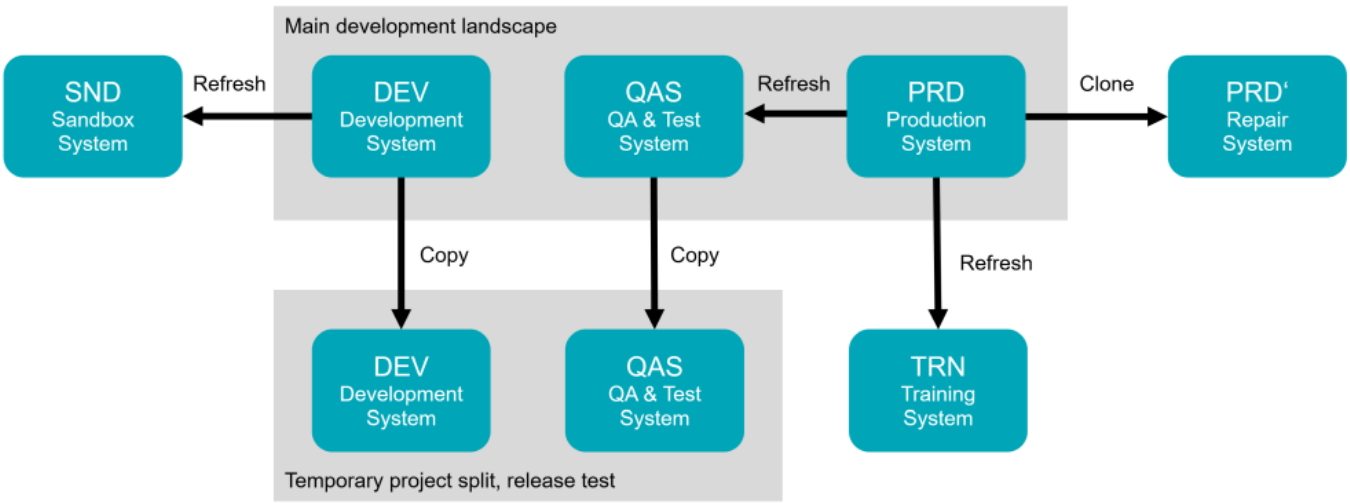


Casi d'utilizzo per il refresh e la clonazione del sistema

Le soluzioni NetApp per l'ottimizzazione del Lifecycle management SAP sono integrate nel database SAP HANA e negli strumenti di Lifecycle management, combinando una data Protection integrata con l'efficiente applicazione con il provisioning flessibile dei sistemi di test SAP.

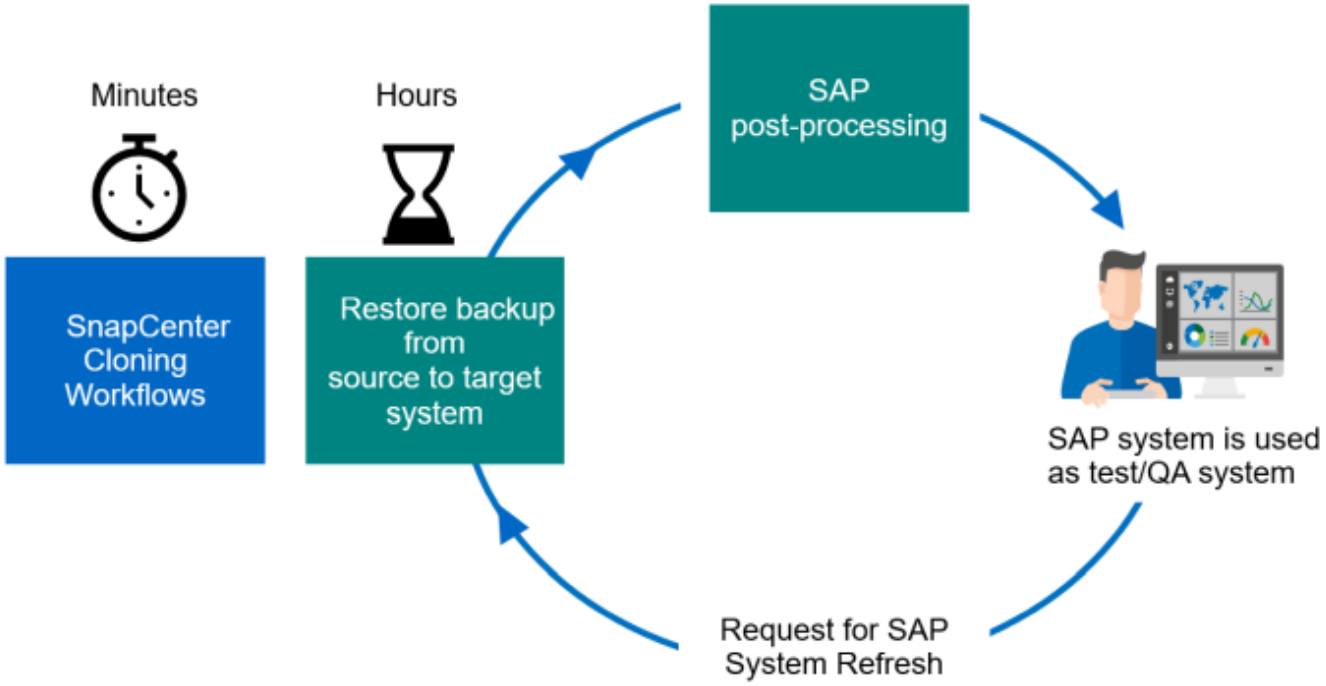
Aggiornamento dei dati di sistemi di QA, test, sandbox o training

Esistono diversi scenari in cui i dati di un sistema di origine devono essere resi disponibili a un sistema di destinazione per scopi di test o formazione. Questi sistemi di test e formazione devono essere aggiornati regolarmente con i dati del sistema di origine per assicurarsi che i test e la formazione vengano eseguiti con il set di dati corrente. Queste operazioni di refresh del sistema consistono in più attività a livello di infrastruttura, database e applicazioni, che possono richiedere più giorni a seconda del livello di automazione.



I workflow di cloning di SnapCenter possono essere utilizzati per accelerare e automatizzare i task richiesti a livello dell'infrastruttura e del database. Invece di ripristinare un backup dal sistema di origine al sistema di destinazione, SnapCenter utilizza la copia Snapshot di NetApp e la tecnologia NetApp FlexClone, per consentire di eseguire le attività necessarie fino a un database SAP HANA avviato in pochi minuti e non più in

ore. Il tempo necessario per il processo di cloning è indipendente dalle dimensioni del database, pertanto è possibile creare anche sistemi molto grandi in un paio di minuti. Il tempo di avvio dipende solo dalle dimensioni del database e dalla connettività tra il server database e il sistema di archiviazione.



Il flusso di lavoro per le operazioni di aggiornamento del sistema è descritto nella sezione ""Aggiornamento del sistema SAP HANA con SnapCenter"."

Risolvere il danneggiamento logico

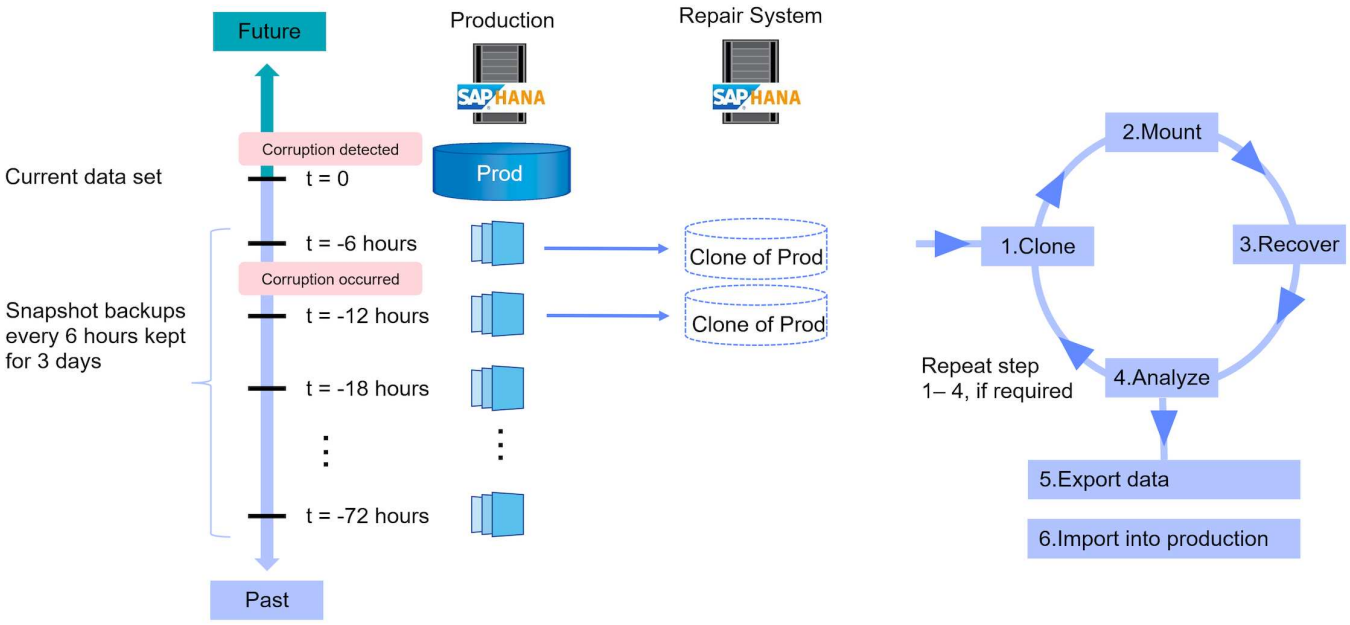
La corruzione logica può essere causata da errori software, errori umani o sabotaggio. Purtroppo, spesso la corruzione logica non può essere affrontata con soluzioni standard di alta disponibilità e disaster recovery. Di conseguenza, a seconda del livello, dell'applicazione, del file system o dello storage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

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

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

Quando si configura il sistema di riparazione, la flessibilità e l'agilità sono fondamentali. Quando si utilizzano i

backup Snapshot basati su storage NetApp, sono disponibili più immagini di database coerenti per creare un clone del sistema di produzione utilizzando la tecnologia FlexClone di NetApp. I volumi FlexClone possono essere creati in pochi secondi anziché in più ore se per configurare il sistema di riparazione viene utilizzato un ripristino reindirizzato da un backup basato su file.



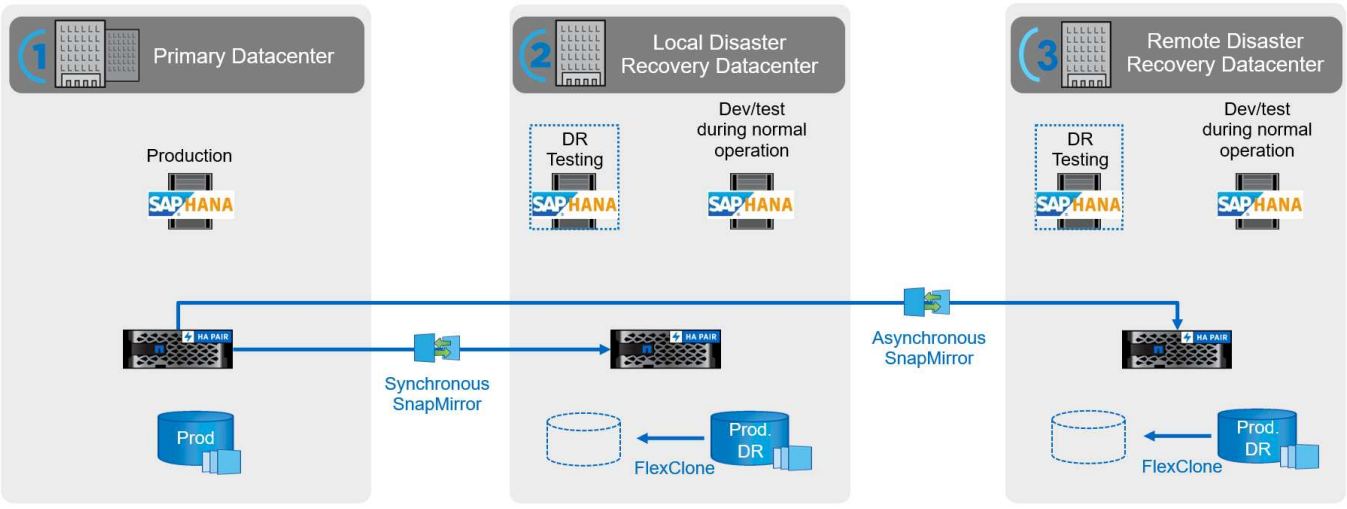
Il flusso di lavoro per la creazione del sistema di riparazione è descritto nella sezione ""Clone del sistema SAP con SnapCenter"."

Test di disaster recovery

Una strategia di disaster recovery efficace richiede il test del flusso di lavoro richiesto. I test dimostrano se la strategia funziona e se la documentazione interna è sufficiente. Consente inoltre agli amministratori di addestrare le procedure richieste.

La replica dello storage con SnapMirror consente di eseguire test di disaster recovery senza mettere a rischio RTO e RPO. I test di disaster recovery possono essere eseguiti senza interrompere la replica dei dati.

I test di disaster recovery per SnapMirror asincrono e sincrono utilizzano i backup Snapshot e i volumi FlexClone alla destinazione del disaster recovery.



Nei rapporti tecnici è disponibile una descrizione dettagliata

"TR-4646: Disaster recovery SAP HANA con replica storage (netapp.com)"

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

Infrastruttura e scenari supportati

Questo documento prende in esame gli scenari di refresh e cloning del sistema SAP per sistemi SAP HANA in esecuzione su sistemi NetApp on-premise, su Amazon FSX per sistemi NetApp ONTAP e su Azure NetApp Files. Tuttavia, non tutte le funzionalità e gli scenari sono disponibili su ogni piattaforma storage. La tabella seguente riassume le configurazioni supportate.

All'interno del documento, stiamo utilizzando un ambiente SAP HANA in esecuzione su sistemi NetApp on-premise con NFS come protocollo storage. La maggior parte dei passaggi del flusso di lavoro sono identici per le diverse piattaforme e, in caso di differenze, sono evidenziati in questo documento.

	Sistemi NetApp in loco	AWS FSX per NetApp ONTAP	Azure NetApp Files
Protocollo storage	NFS e Fibre Channel	NFS	NFS
Thin clone (FlexClone)	Sì	Sì	No, con la versione ANF corrente, il volume clonato viene sempre suddiviso
Operazione di suddivisione dei cloni	Sì	Sì	N/A.
Clonazione dallo storage primario	Sì	Sì	Sì
Clonazione da backup off-site	Sì	Sì	No
Clonazione nel sito di DR	Sì	Sì	Sì, ma non integrato in SnapCenter

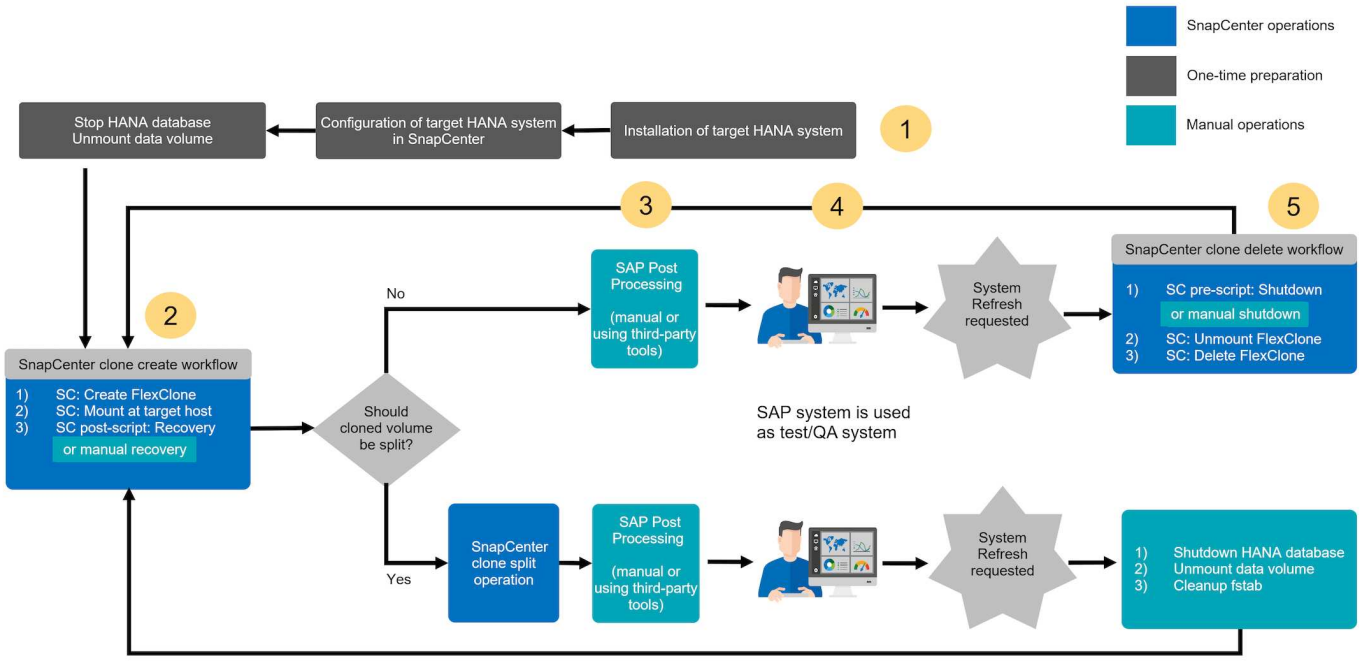
Panoramica del workflow di refresh del sistema SAP con SnapCenter

SnapCenter offre workflow che consentono di gestire cloni di set di dati da qualsiasi backup Snapshot esistente. Questo set di dati clonato, un volume FlexClone, può essere utilizzato per eseguire rapidamente il provisioning di un volume di dati HANA da un sistema di origine e collegarlo a un sistema di destinazione. Si tratta quindi di una soluzione perfetta per eseguire operazioni di refresh del sistema per QA, test, sandbox o sistemi di training.

I flussi di lavoro di cloning di SnapCenter gestiscono tutte le operazioni richieste sul layer di storage e possono essere estesi utilizzando script per eseguire operazioni specifiche dell'host e del database HANA. In questo documento, utilizziamo uno script per eseguire operazioni di recovery e shutdown del database HANA. I flussi di lavoro SnapCenter con ulteriore automazione utilizzando lo script gestiscono tutte le operazioni di database HANA richieste, ma non coprono alcuna procedura di post-elaborazione SAP richiesta. La post-elaborazione SAP deve essere eseguita manualmente o con strumenti di terze parti.

Il flusso di lavoro di refresh del sistema SAP con SnapCenter consiste in cinque passaggi principali, come illustrato nella figura seguente.

1. Installazione iniziale e preparazione del sistema di destinazione
   a. Il plug-in SnapCenter HANA deve essere installato sul nuovo sistema di destinazione e il sistema HANA deve essere configurato in SnapCenter
   b. Il sistema di destinazione deve essere arrestato e il volume di dati HANA deve essere smontato
2. Il flusso di lavoro di creazione del clone di SnapCenter
   a. SnapCenter crea un volume FlexClone della Snapshot selezionata del sistema di origine
   b. SnapCenter monta il volume FlexClone sul sistema di destinazione
   c. Il recovery del database HANA di destinazione può essere automatizzato usando `sc-system-refresh` lo script come post-script o può essere eseguito manualmente
3. Post-elaborazione SAP (manuale o con uno strumento di terze parti)
4. Il sistema può ora essere utilizzato come sistema di test/QA.
5. Quando viene richiesto un nuovo refresh di sistema, il flusso di lavoro di eliminazione dei cloni SnapCenter viene utilizzato per rimuovere il volume FlexClone
   a. Se il sistema HANA di destinazione è stato protetto in SnapCenter, la protezione deve essere rimossa prima di avviare il workflow di eliminazione dei cloni.
   b. Il sistema HANA deve essere arrestato manualmente o automaticamente, usando `sc-system-refresh` lo script come pre-script di SnapCenter
   c. SnapCenter sblocca il volume di dati HANA
   d. SnapCenter elimina il volume FlexClone
   e. Un aggiornamento viene riavviato con il passaggio 2.



Nella maggior parte dei casi, i sistemi di test/controllo qualità target vengono utilizzati per almeno un paio di settimane. Poiché il volume FlexClone blocca la Snapshot del volume di sistema di origine, questo Snapshot richiederà capacità aggiuntiva in base alla velocità di modifica dei blocchi nel volume di sistema di origine. Per

i sistemi di origine della produzione e con una frequenza di modifica media del 20% al giorno, la snapshot bloccata raggiungerà il 100% dopo 5 giorni. Pertanto, NetApp consiglia di suddividere il volume FlexClone immediatamente o dopo un paio di giorni, se il clone è basato su un sistema di origine della produzione. L'operazione di suddivisione dei cloni non blocca l'utilizzo del volume clonato e può quindi essere eseguita in qualsiasi momento mentre il database HANA è in uso.

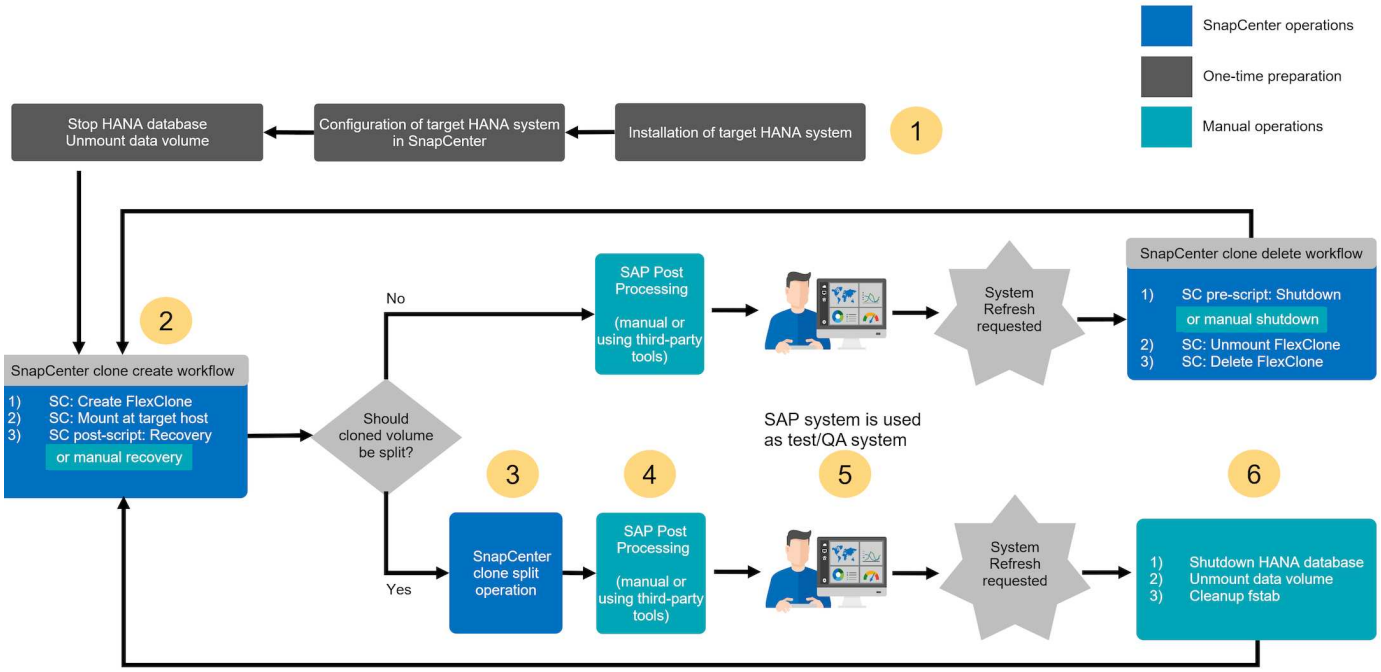
> Quando si suddivide il volume FlexClone, SnapCenter elimina tutti i backup creati nel sistema di destinazione.

> Con SnapCenter e Azure NetApp Files, l'operazione di clone split non è disponibile, poiché Azure NetApp Files divide sempre il clone dopo la creazione.

L'operazione di refresh, incluso il clone split, consiste nei seguenti passaggi.

1. Installazione iniziale e preparazione del sistema di destinazione
   a. Il plug-in SnapCenter HANA deve essere installato sul nuovo sistema di destinazione e il sistema HANA deve essere configurato in SnapCenter
   b. Il sistema di destinazione deve essere arrestato e il volume di dati HANA deve essere smontato
2. Il flusso di lavoro di creazione del clone di SnapCenter
   a. SnapCenter crea un volume FlexClone della Snapshot selezionata del sistema di origine
   b. SnapCenter monta il volume FlexClone sul sistema di destinazione
   c. Il recovery del database HANA di destinazione può essere automatizzato usando `sc-system-refresh` lo script come post-script o può essere eseguito manualmente
3. Il volume FlexClone viene diviso utilizzando il workflow dello split dei cloni di SnapCenter.
4. Post-elaborazione SAP (manuale o con uno strumento di terze parti)
5. Il sistema può ora essere utilizzato come sistema di test/QA.
6. Quando viene richiesto un nuovo aggiornamento del sistema, la pulizia viene eseguita con i seguenti passaggi manuali
   a. Se il sistema HANA di destinazione è stato protetto in SnapCenter, la protezione deve essere rimossa.
   b. Il sistema HANA deve essere arrestato manualmente
   c. È necessario smontare il volume di dati HANA e rimuovere la voce fstab da SnapCenter (task manuale)
   d. Un aggiornamento viene riavviato con il passaggio 2.

> Il vecchio volume di dati, precedentemente suddiviso, deve essere cancellato manualmente sul sistema di storage.



La sezione ""Aggiornamento del sistema SAP HANA con SnapCenter"" fornisce una descrizione dettagliata di entrambi i flussi di lavoro di aggiornamento del sistema.

Panoramica del workflow dei cloni di sistema SAP con SnapCenter

Come discusso nella sezione precedente, SnapCenter è in grado di gestire cloni di set di dati da qualsiasi backup Snapshot esistente e di eseguire rapidamente il provisioning di questi set di dati su qualsiasi sistema di destinazione. Il provisioning flessibile e agile dei dati di produzione in un sistema di riparazione per risolvere la corruzione logica è fondamentale, poiché spesso è necessario reimpostare il sistema di riparazione e scegliere un diverso set di dati di produzione. La tecnologia FlexClone consente un rapido processo di provisioning e offre un notevole risparmio di capacità, poiché il sistema di riparazione viene in genere utilizzato solo per un breve periodo di tempo.

La figura seguente riassume i passaggi necessari per un'operazione di cloning di sistema SAP con SnapCenter.

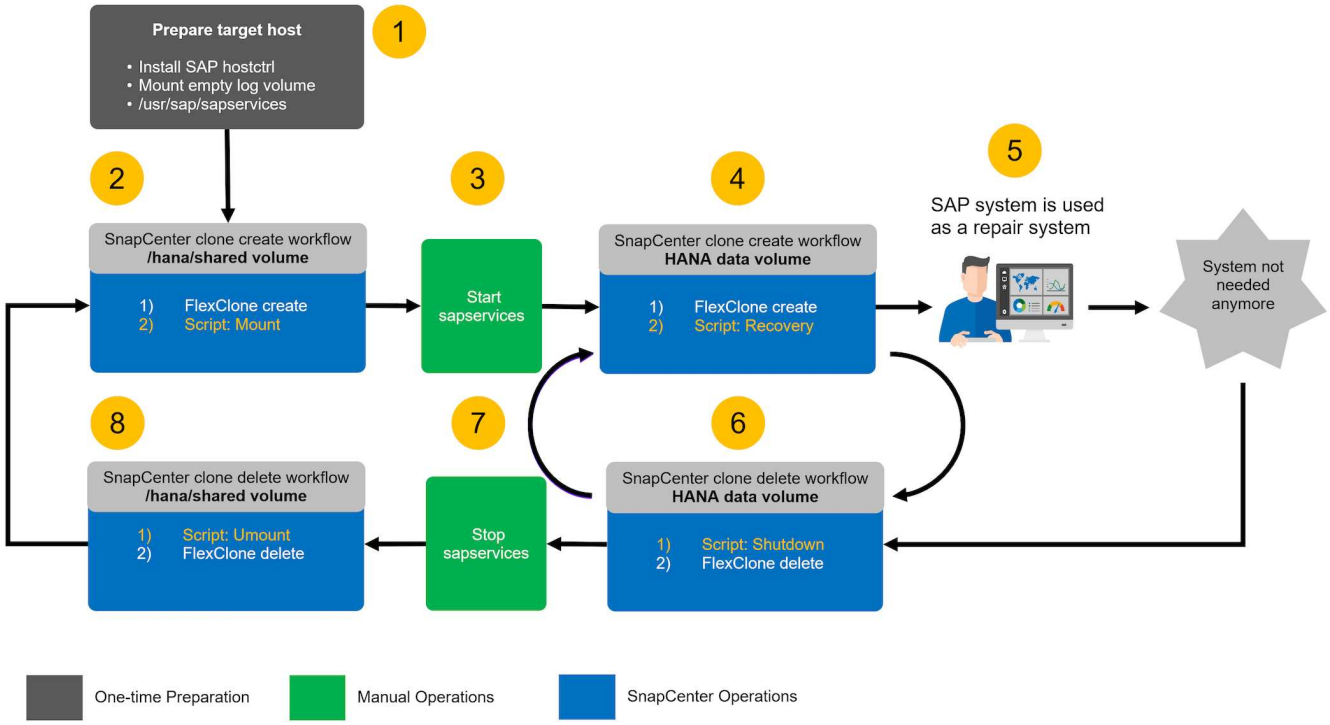
1. Preparare l'host di destinazione.
2. Il clone di SnapCenter crea un workflow per il volume condiviso di SAP HANA.
3. Avviare i servizi SAP HANA.
4. Il clone di SnapCenter crea il workflow per il volume di dati SAP HANA, incluso il recovery del database.
5. Il sistema SAP HANA può ora essere utilizzato come sistema di riparazione.

Se il sistema non è più necessario, il processo di pulizia viene eseguito con le seguenti operazioni.

1. Flusso di lavoro di eliminazione dei cloni SnapCenter per il volume di dati SAP HANA, incluso l'arresto del database (quando si utilizza lo script di automazione).
2. Arrestare i servizi SAP HANA.

3. Flusso di lavoro di eliminazione dei cloni SnapCenter per il volume condiviso SAP HANA.

Se è necessario ripristinare il sistema su un backup Snapshot diverso, i passaggi 6 e 4 sono sufficienti. Non è necessario un refresh del volume condiviso SAP HANA.



La sezione ""Clone del sistema SAP con SnapCenter"" fornisce una descrizione dettagliata dettagliata del flusso di lavoro dei cloni del sistema.

Considerazioni sulle operazioni di refresh del sistema SAP HANA utilizzando backup snapshot dello storage

Le soluzioni NetApp per l'ottimizzazione del Lifecycle management SAP sono integrate nel database SAP HANA e negli strumenti di Lifecycle management, combinando una data Protection integrata con l'efficiente applicazione con il provisioning flessibile dei sistemi di test SAP.

Nomi dei tenant nel sistema di destinazione

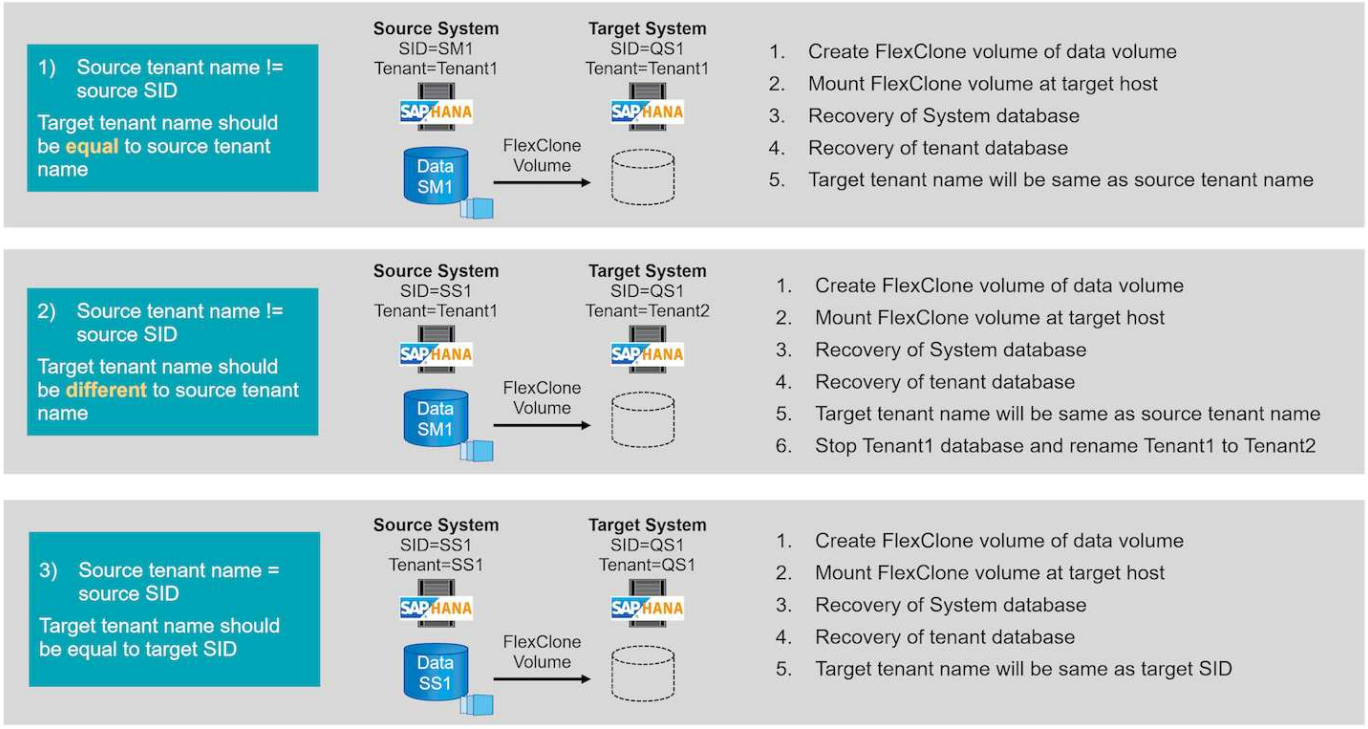
I passaggi necessari per un refresh del sistema SAP HANA dipendono dalla configurazione del tenant del sistema di origine e dal nome richiesto del tenant nel sistema di destinazione, come mostrato nella figura sotto.

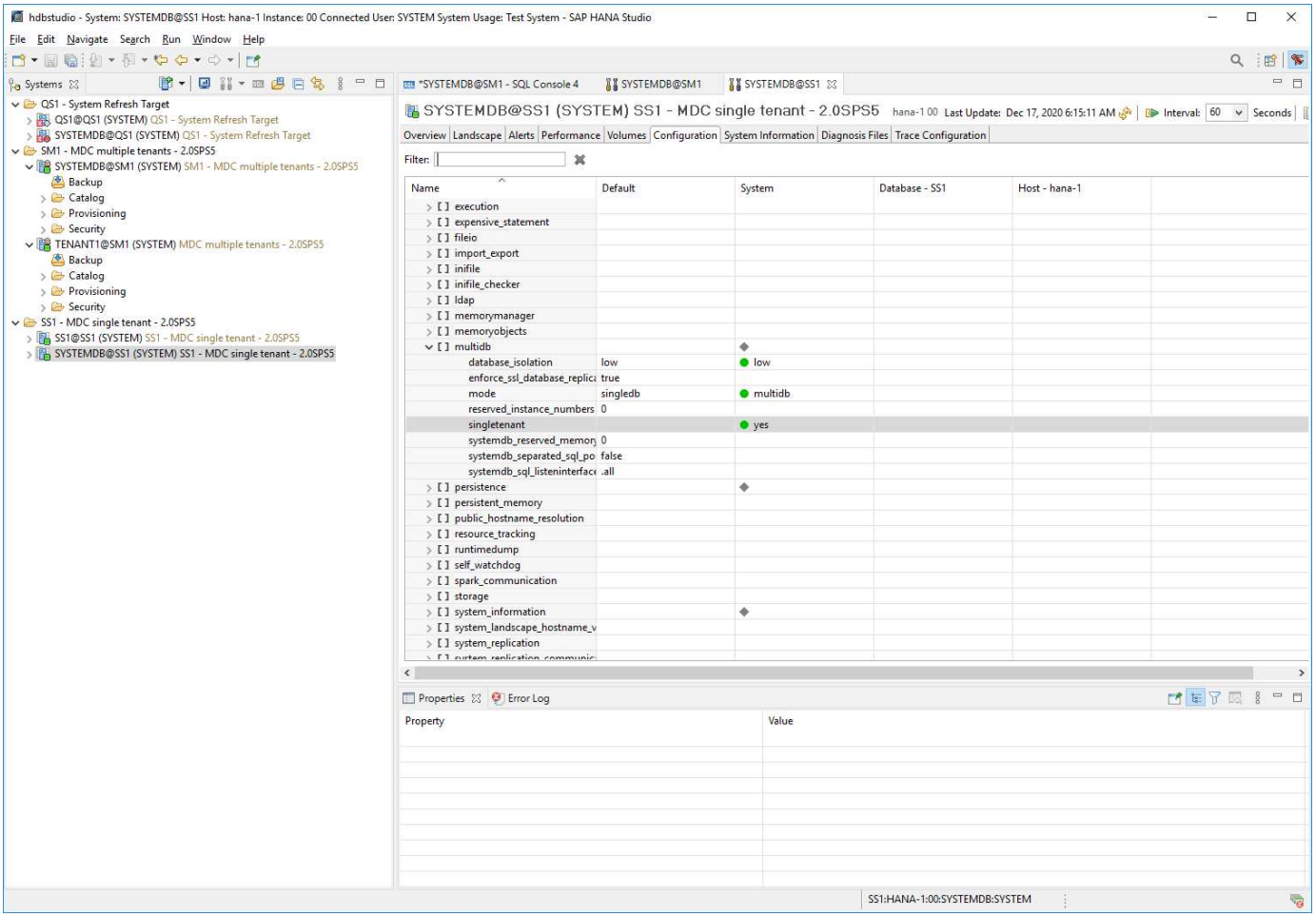
Poiché il nome del tenant è configurato nel database di sistema, il nome del tenant del sistema di origine è disponibile anche nel sistema di destinazione dopo il ripristino del database di sistema. Pertanto, è possibile ripristinare il tenant del sistema di destinazione solo con lo stesso nome del tenant di origine, come illustrato nell'opzione 1. Se il nome del tenant nel sistema di destinazione deve essere diverso, il tenant deve essere recuperato con lo stesso nome del tenant di origine e quindi rinominato nel nome del tenant di destinazione richiesto. Questa è l'opzione 2.

Un'eccezione di questa regola è un sistema SAP HANA con un singolo tenant, con nome del tenant identico al SID del sistema. Questa configurazione è quella predefinita dopo un'installazione SAP HANA iniziale. Questa

configurazione specifica è contrassegnata dal database SAP HANA. In questo caso, il ripristino del tenant nel sistema di destinazione può essere eseguito con il nome del tenant del sistema di destinazione, che deve essere identico anche al SID di sistema del sistema di destinazione. Questo flusso di lavoro è mostrato nell'opzione 3.

Non appena qualsiasi operazione di creazione, ridenominazione o abbandono del tenant viene eseguita sul sistema di origine, questo flag di configurazione viene eliminato dal database SAP HANA. Pertanto, anche se la configurazione è stata riportata al tenant = SID, il flag non è più disponibile e l'eccezione relativa al ripristino del tenant con il workflow 3 non è più possibile. In questo caso, l'opzione 2 è il flusso di lavoro richiesto.





Workflow di refresh del sistema con crittografia SAP HANA abilitata

Quando la crittografia di persistenza SAP HANA è abilitata, sono necessari ulteriori passaggi prima di poter recuperare il database SAP HANA nel sistema di destinazione.

Nel sistema di origine è necessario creare un backup delle chiavi root di crittografia per il database del sistema e per tutti i database tenant. I file di backup devono essere copiati nel sistema di destinazione e le chiavi principali devono essere importate dal backup prima di eseguire l'operazione di ripristino.

Vedere anche "Guida all'amministrazione di SAP HANA".

Backup delle chiavi principali

Se sono state apportate modifiche alle chiavi principali, è sempre necessario eseguire un backup delle chiavi principali. Il comando di backup richiede dbid come parametro CLI. I dbid possono essere identificati utilizzando l'istruzione SQL riportata di seguito.



L'istruzione SQL e l'ulteriore documentazione sono disponibili nella SAP HANA Admin Guide ai "Back Up Root Keys | Portale della Guida di SAP" passaggi seguenti che illustrano le operazioni richieste per un sistema HANA con un singolo tenant SS1 e sono eseguite sul sistema di origine.

1. Impostare la password di backup per i database del sistema e del tenant (SS1) (se non è ancora stata effettuata).

```
hdbsql SYSTEMDB=> ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD
Netapp123;
0 rows affected (overall time 3658.128 msec; server time 3657.967 msec)
hdbsql SYSTEMDB=>
hdbsql SS1=> ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD
Netapp123;
0 rows affected (overall time 2424.236 msec; server time 2424.010 msec)
hdbsql SS1=>
```

1. Creare il backup delle chiavi root per database di sistemi e tenant (SS1).

```
ss1adm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-backupRootKeys root-key-backup-SS1-SYSTEMDB.rkb --dbid=1 --type='ALL'
Exporting root key backup for database SYSTEMDB (DBID: 1) to
/usr/sap/SS1/home/root-key-backup-SS1-SYSTEMDB.rkb
done.
ss1adm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-backupRootKeys root-key-backup-SS1-SS1.rkb --dbid=3 --type='ALL'
Exporting root key backup for database SS1 (DBID: 3) to
/usr/sap/SS1/home/root-key-backup-SS1-SS1.rkb
done.
```

1. Convalidare i backup della chiave principale (opzionali)

```
ss1adm@hana-1:/usr/sap/SS1/home> ls -al root*
-rw-r----- 1 ss1adm sapsys 1440 Apr 24 07:00 root-key-backup-SS1-SS1.rkb
-rw-r----- 1 ss1adm sapsys 1440 Apr 24 06:54 root-key-backup-SS1-
SYSTEMDB.rkb
ss1adm@hana-1:/usr/sap/SS1/home>

ss1adm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-validateRootKeysBackup root-key-backup-SS1-SS1.rkb
Please Enter the password:
Successfully validated SSFS backup file /usr/sap/SS1/home/root-key-backup-
SS1-SS1.rkb
done.

ss1adm@hana-1:/usr/sap/SS1/home> /usr/sap/SS1/HDB00/exe/hdbnsutil
-validateRootKeysBackup root-key-backup-SS1-SYSTEMDB.rkb
Please Enter the password:
Successfully validated SSFS backup file /usr/sap/SS1/home/root-key-backup-
SS1-SYSTEMDB.rkb
done.
```

Importazione delle chiavi principali nel sistema di destinazione

L'importazione delle chiavi principali è necessaria inizialmente per la prima operazione di aggiornamento del sistema. Se le chiavi principali non vengono modificate nel sistema di origine, non è necessaria alcuna importazione aggiuntiva. Il comando import richiede dbid come parametro CLI. I dbid possono essere identificati nello stesso modo descritto per il backup della chiave root.

1. Nel nostro setup le chiavi root vengono copiate dal sistema di origine in una condivisione NFS

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

1. Le chiavi root possono ora essere importate usando hdbnsutil. Il dbid per il sistema e il database tenant deve essere fornito con il comando. È necessaria anche la password di backup.

```
qs1adm@hana-7:/usr/sap/QS1/HDB11> ./exe/hdbnsutil -recoverRootKeys
/mnt/sapcc-share/SAP-System-Refresh/root-key-backup-SS1-SYSTEMDB.rkb
--dbid=1 --type=ALL
Please Enter the password:
Importing root keys for DBID: 1 from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SYSTEMDB.rkb
Successfully imported root keys from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SYSTEMDB.rkb
done.

qs1adm@hana-7:/usr/sap/QS1/HDB11> ./exe/hdbnsutil -recoverRootKeys
/mnt/sapcc-share/SAP-System-Refresh/root-key-backup-SS1-SS1.rkb --dbid=3
--type=ALL Please Enter the password:
Importing root keys for DBID: 3 from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SS1.rkb
Successfully imported root keys from /mnt/sapcc-share/SAP-System-
Refresh/root-key-backup-SS1-SS1.rkb
done.
qs1adm@hana-7:/usr/sap/QS1/HDB11>
```

Importazione della chiave principale, se dbid non esiste al target

Come descritto nel capitolo precedente, il dbid è necessario per importare la chiave root per il sistema e per tutti i database tenant. Mentre il database del sistema è sempre dbid=0, i database tenant possono avere diversi dbid.



La produzione sopra riportata mostra due locatari con dbid=3 e dbid=4. Se il sistema di destinazione non ha ancora ospitato un tenant con dbid=4, l'importazione della chiave root non riesce. In tal caso è necessario recuperare prima il database di sistema e quindi importare la chiave per il tenant con dbid=4.

Script di esempio di automazione

In questo documento vengono utilizzati due script per automatizzare ulteriormente le operazioni di creazione e cancellazione dei cloni SnapCenter.

- Lo script `sc-system-refresh.sh` viene utilizzato per l'aggiornamento del sistema e il flusso di lavoro del clone del sistema per eseguire operazioni di ripristino e arresto del database SAP HANA.
- Lo script `sc-mount-volume.sh` viene utilizzato per il workflow di cloni del sistema per eseguire operazioni di montaggio e smontaggio per il volume condiviso SAP HANA.

> Gli script di esempio vengono forniti così come sono e non sono supportati da NetApp. È possibile richiedere gli script tramite e-mail all'indirizzo ng-sapcc@netapp.com.

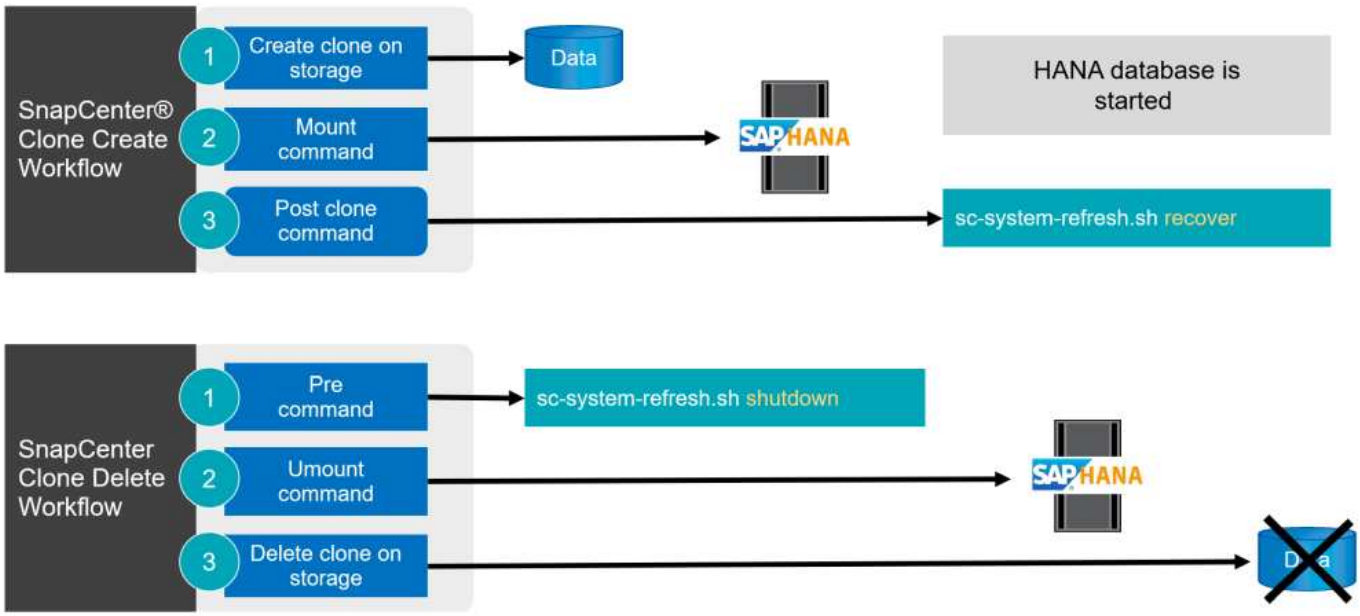
Script sc-system-refresh.sh

Lo script di esempio `sc-system-refresh.sh` viene utilizzato per eseguire operazioni di ripristino e arresto. Lo script viene chiamato con opzioni specifiche della riga di comando all'interno dei flussi di lavoro SnapCenter che clonano la creazione e l'eliminazione dei cloni, come illustrato nella figura sotto.

Lo script è generico e legge tutti i parametri richiesti, come il SID dal sistema di destinazione. Lo script deve essere disponibile nell'host di destinazione dell'operazione di aggiornamento del sistema. È necessario configurare una chiave di memorizzazione utente hdb per il punto di vista <SID> dell'utente nel sistema di destinazione. La chiave deve consentire l'accesso al database del sistema SAP HANA e fornire i privilegi per le operazioni di recovery. La chiave deve avere il nome <TARGET-SID> (Avanti).

Lo script scrive un file di registro `sc-system-refresh-SID.log``nella stessa directory in cui viene eseguito.

> La versione corrente dello script supporta sistemi host singoli MDC single tenant o configurazioni multi tenant MDC. Non supporta sistemi SAP HANA con host multipli.



Operazioni di recovery tenant supportate

Come descritto nella sezione "i workflow delle operazioni di refresh del sistema SAP HANA usando la snapshot dello storage" le possibili operazioni di recovery del tenant nel sistema di destinazione dipendono dalla configurazione del tenant del sistema di origine. Lo script `sc-system-refresh.sh` supporta tutte le operazioni di recovery dei tenant, possibili in base alla configurazione del sistema di origine, come illustrato nella tabella seguente.

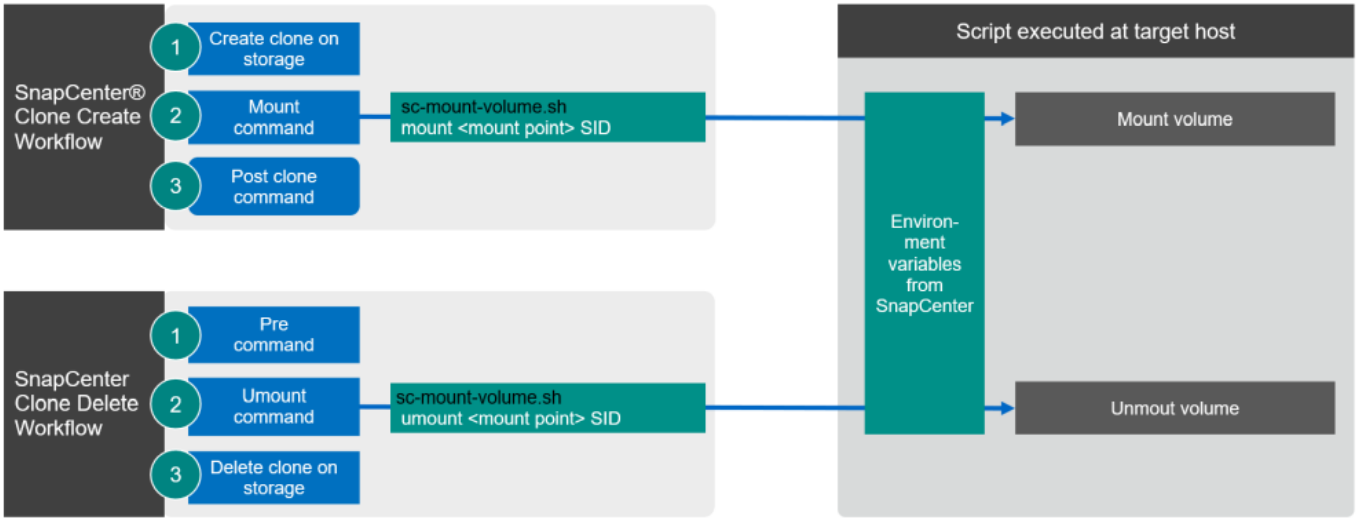
Se nel sistema di destinazione è richiesto un nome tenant diverso, il tenant deve essere rinominato manualmente dopo l'operazione di ripristino.

Sistema SAP HANA	Configurazione tenant + nel sistema di origine	Configurazione del tenant risultante + sul sistema di destinazione
Tenant singolo MDC	Nome del tenant di origine uguale al SID di origine	Il nome del tenant di destinazione è uguale al SID di destinazione
Tenant singolo MDC	Il nome del tenant di origine non corrisponde al SID di origine	Il nome del tenant di destinazione è uguale al nome del tenant di origine
Tenant multipli MDC	Qualsiasi nome tenant	Tutti i locatari vengono recuperati e avranno lo stesso nome dei locatari di origine.

Script sc-mount-volume.sh

Lo script di esempio `sc-mount-volume.sh` viene utilizzato per eseguire mount e unmount per ogni volume. Lo script viene utilizzato per montare il volume condiviso di SAP HANA con l'operazione dei cloni del sistema SAP HANA. Lo script viene chiamato con opzioni specifiche della riga di comando all'interno dei flussi di lavoro SnapCenter che clonano la creazione e l'eliminazione dei cloni, come illustrato nella figura sotto.

Lo script supporta i sistemi SAP HANA utilizzando NFS come protocollo storage.



Variabili di ambiente SnapCenter

SnapCenter fornisce un insieme di variabili di ambiente disponibili all'interno dello script eseguito sull'host di destinazione. Lo script utilizza queste variabili per determinare le impostazioni di configurazione pertinenti.

- Le variabili di script `STORAGE, JUNCTION_PATH` vengono utilizzate per l'operazione di mount.
- Derivato da `CLONED_VOLUMES_MOUNT_PATH` variabile di ambiente.
- `CLONED_VOLUMES_MOUNT_PATH=${STORAGE}:/${JUNCTION_PATH}`
- Ad esempio:
  `CLONED_VOLUMES_MOUNT_PATH=192.168.175.117:/SS1_shared_Clone_05112206115489411`

Script per ottenere le variabili di ambiente SnapCenter

Se gli script di automazione non devono essere utilizzati e i passaggi devono essere eseguiti manualmente, è necessario conoscere il percorso di giunzione del sistema di storage del volume FlexClone. Il percorso di giunzione non è visibile in SnapCenter, quindi è necessario cercare il percorso di giunzione direttamente nel sistema di storage oppure utilizzare un semplice script che fornisca le variabili di ambiente SnapCenter all'host di destinazione. Questo script deve essere aggiunto come script dell'operazione di montaggio all'interno dell'operazione di creazione del clone di SnapCenter.

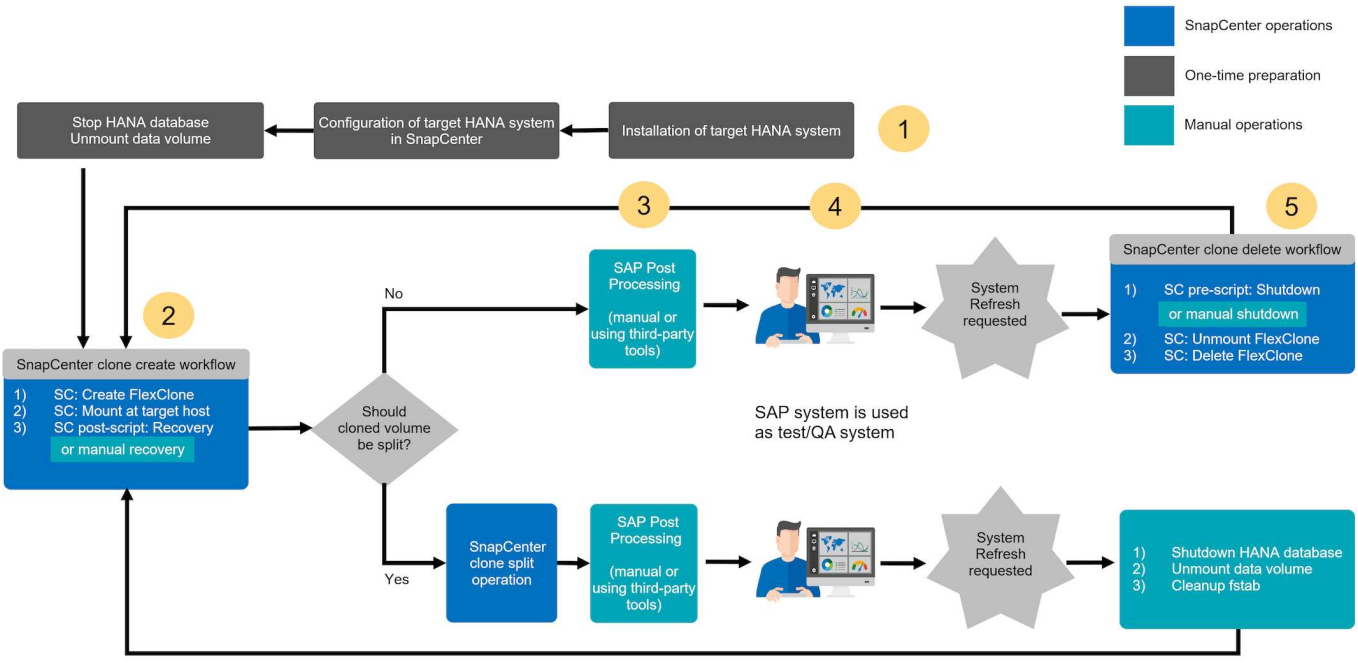
```
ss1adm@hana-1:/mnt/sapcc-share/SAP-System-Refresh> cat get-env.sh
#!/bin/bash
env > /tmp/env-from-sc.txt
ss1adm@hana-1:/mnt/sapcc-share/SAP-System-Refresh>
```

All'interno di `env-from-sc.txt` cercare la variabile `CLONED_VOLUMES_MOUNT_PATH` Per ottenere l'indirizzo IP del sistema storage e il percorso di giunzione del volume FlexClone.

Ad esempio:
`CLONED_VOLUMES_MOUNT_PATH=192.168.175.117:/SS1_data_mnt00001_Clone_05112206115489411`

Aggiornamento del sistema SAP HANA con SnapCenter

La sezione seguente fornisce una descrizione dettagliata delle diverse opzioni di aggiornamento del sistema di un database SAP HANA.



A seconda della configurazione del database di SAP HANA, vengono eseguiti o devono essere preparati altri passaggi. La tabella riportata di seguito fornisce un riepilogo.

Sistema di origine	Configurazione del sistema di origine	Operazioni SnapCenter e SAP HANA
MDC single tenant + SID = nome del tenant	Configurazione standard	Operazione di cloning SnapCenter ed esecuzione opzionale dello script di recovery.
	Crittografia di persistenza di SAP HANA	Inizialmente, o se le chiavi principali sono state modificate nel sistema di origine, i backup delle chiavi principali devono essere importati nel sistema di destinazione prima di poter eseguire il ripristino.
	Origine replica sistema SAP HANA	Non sono necessari passaggi aggiuntivi. Se il sistema di destinazione non ha HSR configurato, rimarrà un sistema autonomo.
	Partizioni multiple SAP HANA	Non è necessario alcun passaggio aggiuntivo, ma i punti di montaggio per le partizioni di volume SAP HANA devono essere disponibili nel sistema di destinazione con la stessa convenzione di denominazione (solo SID è diverso).
Tenant multipli MDC O MDC single tenant + con SID <> nome tenant	Configurazione standard	Operazione di cloning SnapCenter ed esecuzione opzionale dello script di recovery. Script recupera tutti i tenant. Se i nomi dei tenant o dei tenant non esistono nei nomi del sistema di destinazione, le directory richieste verranno create automaticamente durante l'operazione di recovery di SAP HANA. I nomi dei tenant saranno gli stessi dell'origine e, se necessario, dovranno essere rinominati dopo il ripristino.
	Crittografia di persistenza di SAP HANA	Se un DBID del sistema di origine non esiste in precedenza nel sistema di destinazione, è necessario prima ripristinare il database di sistema, prima di poter importare il backup della chiave root di questo tenant.
	Origine replica sistema HANA	Non sono necessari passaggi aggiuntivi. Se il sistema di destinazione non ha HSR configurato, rimarrà un sistema autonomo.
	Partizioni multiple HANA	Non è necessario alcun passaggio aggiuntivo, ma i punti di montaggio per le partizioni di volume SAP HANA devono essere disponibili nel sistema di destinazione con la stessa convenzione di denominazione (solo SID è diverso).

In questa sezione vengono descritti i seguenti scenari.

- Aggiornamento del sistema SAP HANA senza un'operazione di suddivisione dei cloni.
- Clonazione dallo storage primario con nome tenant uguale al SID
- Clonazione dallo storage per il backup off-site

- Cloning da storage primario con tenant multipli
- Operazione di eliminazione dei cloni
- Aggiornamento del sistema SAP HANA con un'operazione di suddivisione dei cloni
- Clonazione dallo storage primario con nome tenant uguale al SID
- Operazione di suddivisione dei cloni

Prerequisiti e limitazioni

I flussi di lavoro descritti nelle sezioni seguenti presentano alcuni prerequisiti e limitazioni relativi all'architettura di sistema SAP HANA e alla configurazione SnapCenter.

- I flussi di lavoro descritti sono validi solo per SnapCenter versione 5,0 o superiore.
- I flussi di lavoro descritti sono validi per sistemi SAP HANA MDC a host singolo con tenant singoli o multipli. I sistemi host multipli SAP HANA non sono coperti.
- Il plug-in SAP HANA di SnapCenter deve essere implementato sull'host di destinazione per consentire il rilevamento automatico di SnapCenter e l'esecuzione degli script di automazione.
- I flussi di lavoro sono validi per i sistemi SAP HANA che utilizzano NFS o FCP su host fisici o per host virtuali utilizzando i mount NFS in-guest.

Setup di laboratorio

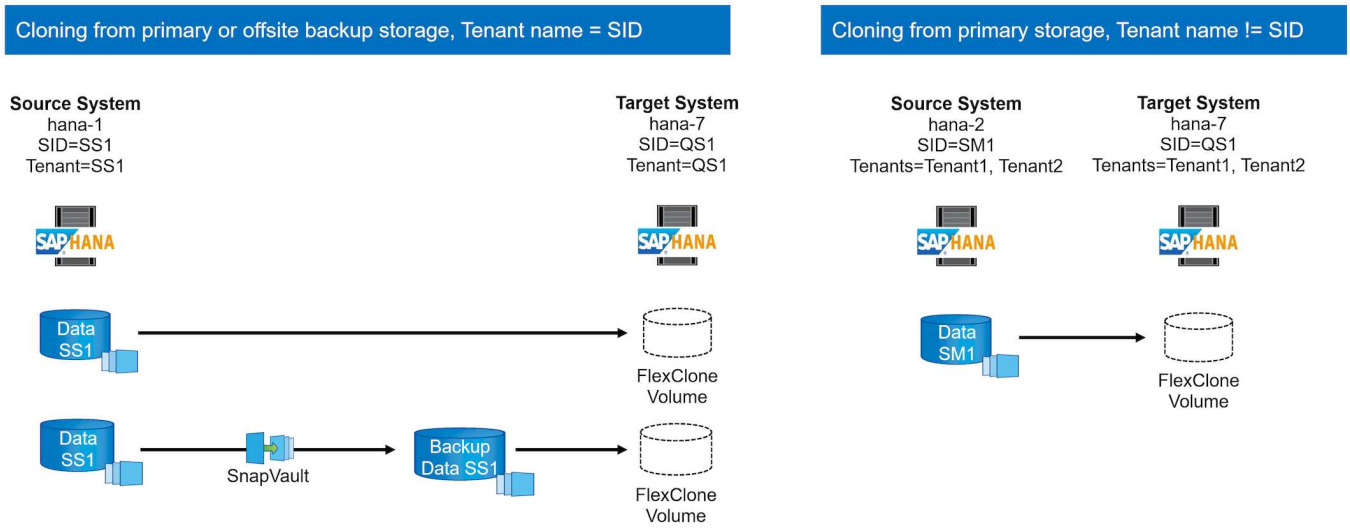
La figura riportata di seguito mostra la configurazione di laboratorio utilizzata per le diverse opzioni di aggiornamento del sistema.

- Clonazione da storage primario o storage di backup off-site; il nome del tenant è uguale al SID.
  - Sistema SAP HANA di origine: SS1 con tenant SS1
  - Sistema SAP HANA di destinazione: QS1 con tenant QS1
- Cloning da storage primario; tenant multipli.
  - Sistema SAP HANA di origine: SM1 con Tenant1 e Tenant2
  - Sistema SAP HANA di destinazione: QS1 con Tenant1 e Tenant2

Sono state utilizzate le seguenti versioni software:

- SnapCenter 5,0
- Sistemi SAP HANA: HANA 2,0 SPS7 rev,73
- SLES 15
- ONTAP 9.14P1

Tutti i sistemi SAP HANA devono essere configurati in base alla guida alla configurazione "SAP HANA su sistemi NetApp AFF con NFS". SnapCenter e le risorse SAP HANA sono state configurate in base alla guida alle Best practice "Backup e ripristino SAP HANA con SnapCenter".



Fasi iniziali di preparazione una tantum

Come passaggio iniziale, è necessario configurare il sistema SAP HANA di destinazione all'interno di SnapCenter.

1. Installazione del sistema di destinazione SAP HANA
2. Configurazione del sistema SAP HANA in SnapCenter, come descritto in "TR-4614: Backup e ripristino SAP HANA con SnapCenter"
   a. Configurazione dell'utente del database SAP HANA per le operazioni di backup SnapCenter questo utente deve essere identico sul sistema di origine e di destinazione.
   b. Configurazione della chiave hdbuserstore per il server di base <sid> con l'utente di backup sopra indicato. Se lo script di automazione viene utilizzato per il ripristino, il nome della chiave deve essere <SID> 10
   c. Implementazione del plug-in SAP HANA SnapCenter sull'host di destinazione. Il sistema SAP HANA è scoperto automaticamente da SnapCenter.
   d. Configurazione della protezione delle risorse di SAP HANA (opzionale)

La prima operazione di refresh del sistema SAP dopo l'installazione iniziale viene preparata con i seguenti passaggi:

1. Chiudi il sistema SAP HANA di destinazione
2. Disinstalla volume di dati SAP HANA.

È necessario aggiungere gli script che devono essere eseguiti sul sistema di destinazione al file di configurazione dei comandi consentiti da SnapCenter.

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

Clonazione dallo storage primario con nome tenant uguale a SID

Questa sezione descrive il workflow di refresh del sistema SAP HANA, in cui il nome del tenant sul sistema di origine e di destinazione è identico al SID. La clonazione dello storage viene eseguita nello storage primario e il ripristino viene automatizzato con lo script `sc-system-refresh.sh`.

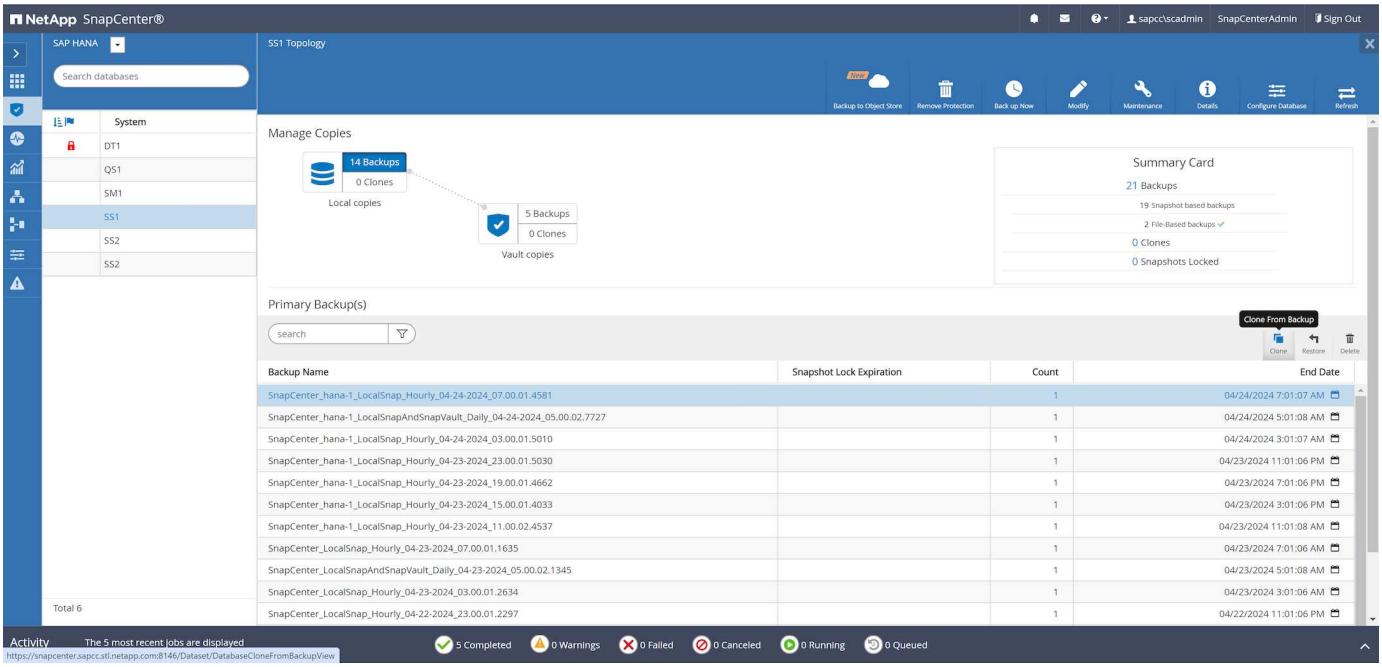


Il flusso di lavoro è costituito dai seguenti passaggi:

1. Se la crittografia di persistenza SAP HANA è abilitata sul sistema di origine, le chiavi root di crittografia devono essere importate una volta. Un'importazione è necessaria anche se le chiavi sono state modificate nel sistema di origine. Vedere il capitolo ""Considerazioni per le operazioni di refresh del sistema SAP HANA utilizzando i backup delle snapshot di storage""
2. Se il sistema SAP HANA di destinazione è stato protetto in SnapCenter, occorre rimuovere per primo la protezione.
3. Workflow di creazione dei cloni SnapCenter.
   a. Seleziona il backup Snapshot dal sistema SAP HANA di origine SS1.
   b. Seleziona l'host di destinazione e fornisci un'interfaccia di storage network dell'host di destinazione.
   c. Fornire il SID del sistema di destinazione, nell'esempio QS1
   d. In alternativa, fornire script per il recovery come operazione post-clone.
4. Operazione di cloning SnapCenter.
   a. Crea un volume FlexClone in base al backup Snapshot selezionato del sistema SAP HANA di origine.
   b. Esporta il volume FlexClone nell'interfaccia o igroup della rete di storage host di destinazione.
   c. Esegue l'operazione di montaggio del volume FlexClone di Monts sull'host di destinazione.
   d. Esegue lo script di ripristino dell'operazione post-clone, se configurato in precedenza. In caso contrario, il ripristino deve essere eseguito manualmente al termine del flusso di lavoro SnapCenter.
      - Ripristino del database di sistema.
      - Ripristino del database tenant con nome tenant = QS1.
5. In alternativa, proteggi la risorsa SAP HANA di destinazione in SnapCenter.

Le seguenti schermate mostrano i passaggi necessari.

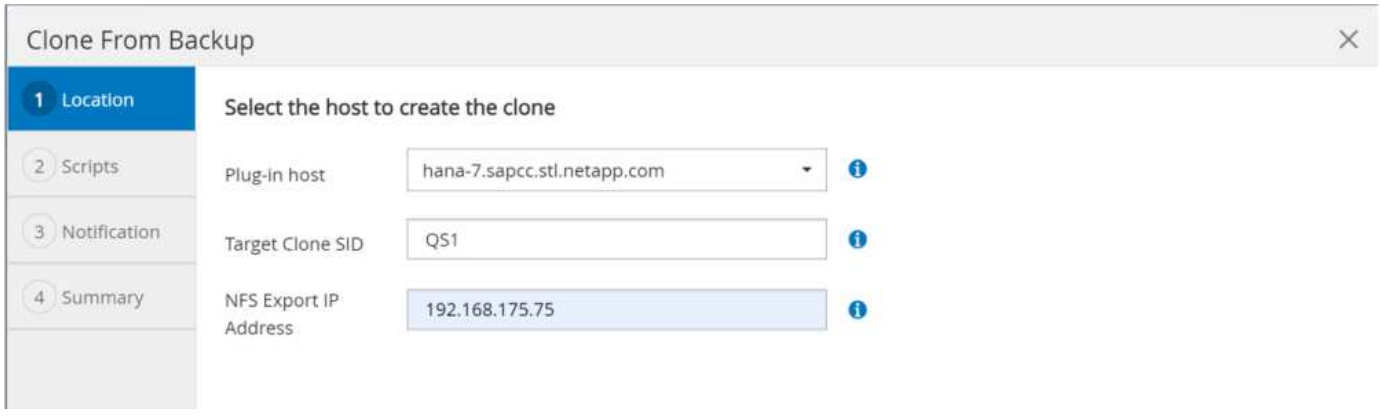
1. Selezionare un backup Snapshot dal sistema di origine SS1 e fare clic su Clone (Clona).



1. Selezionare l'host in cui è installato il sistema di destinazione QS1. Inserire QS1 come SID di destinazione. L'indirizzo IP di esportazione NFS deve essere l'interfaccia di rete dello storage dell'host di destinazione.

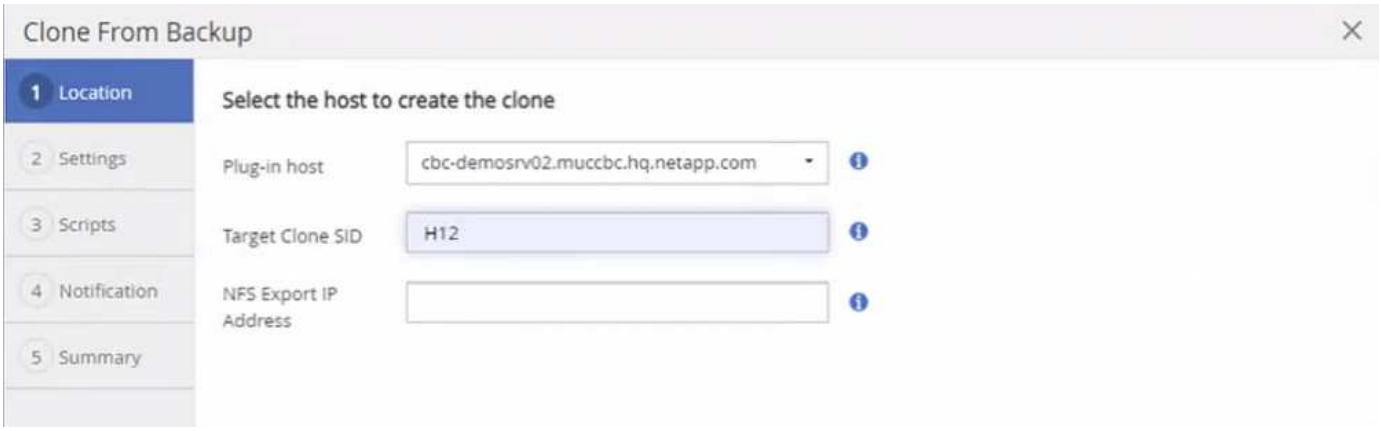
> Il SID di destinazione immesso controlla il modo in cui SnapCenter gestisce la risorsa clonata. Se una risorsa con il SID di destinazione è già configurata in SnapCenter e corrisponde all'host del plug-in, SnapCenter assegna semplicemente il clone a questa risorsa. Se il SID non è configurato sull'host di destinazione, SnapCenter crea una nuova risorsa.

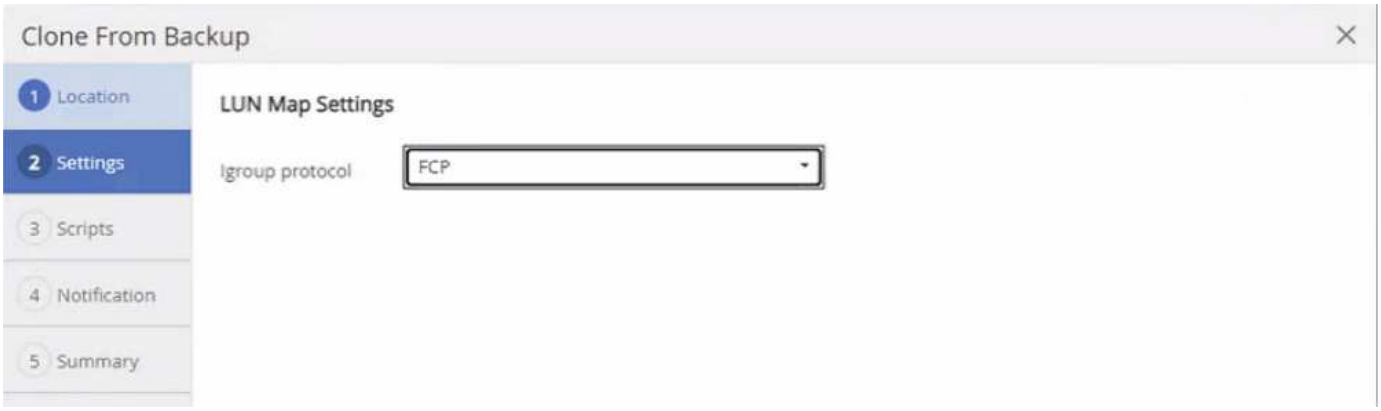
> Prima di avviare il workflow di cloning, è fondamentale che la risorsa e l'host del sistema di destinazione siano stati configurati in SnapCenter. In caso contrario, la nuova risorsa creata da SnapCenter non supporterà il rilevamento automatico e i flussi di lavoro descritti non funzioneranno.



In una configurazione Fibre Channel SAN non è richiesto alcun indirizzo IP per l'esportazione, ma è necessario fornire il protocollo utilizzato nella schermata successiva.

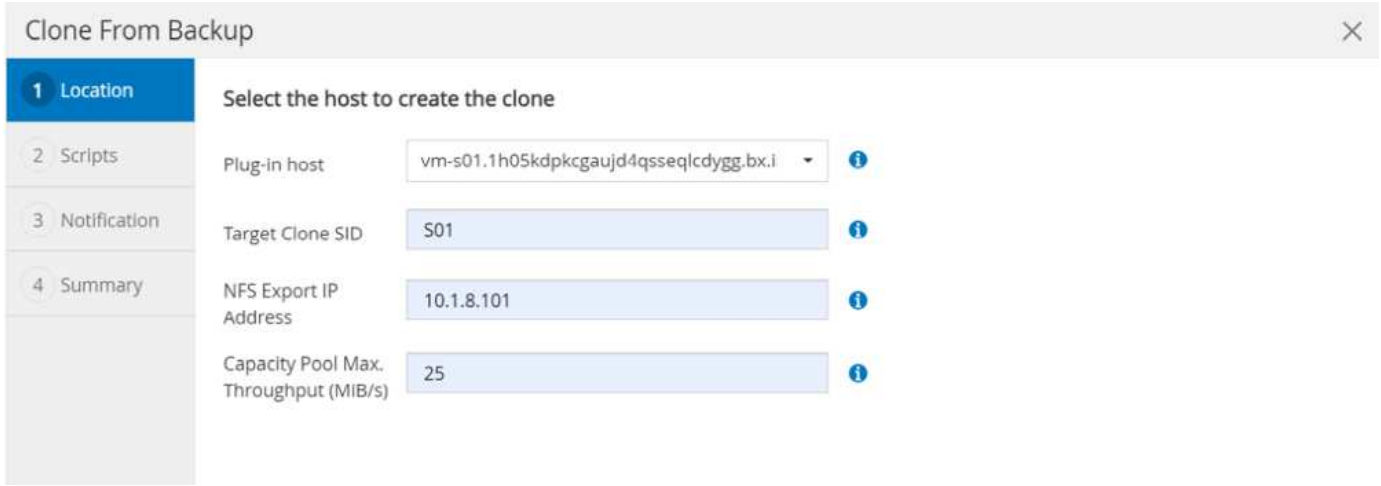
Le schermate mostrano una diversa configurazione di laboratorio utilizzando una connettività FibreChannel.



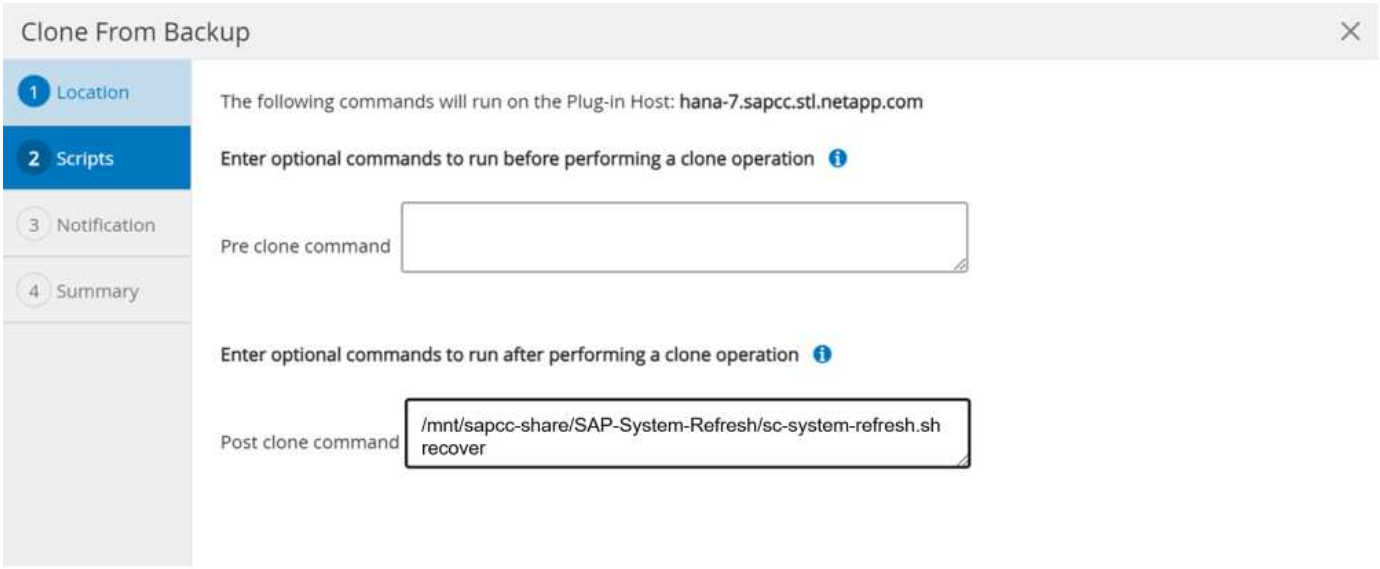


Grazie a Azure NetApp Files e a un pool di capacità QoS manuale, devi offrire il throughput massimo per il nuovo volume. Assicurati che il pool di capacità abbia spazio sufficiente, altrimenti il workflow di cloning fallirà.

Le schermate mostrano una diversa configurazione di laboratorio eseguita in Microsoft Azure con Azure NetApp Files.



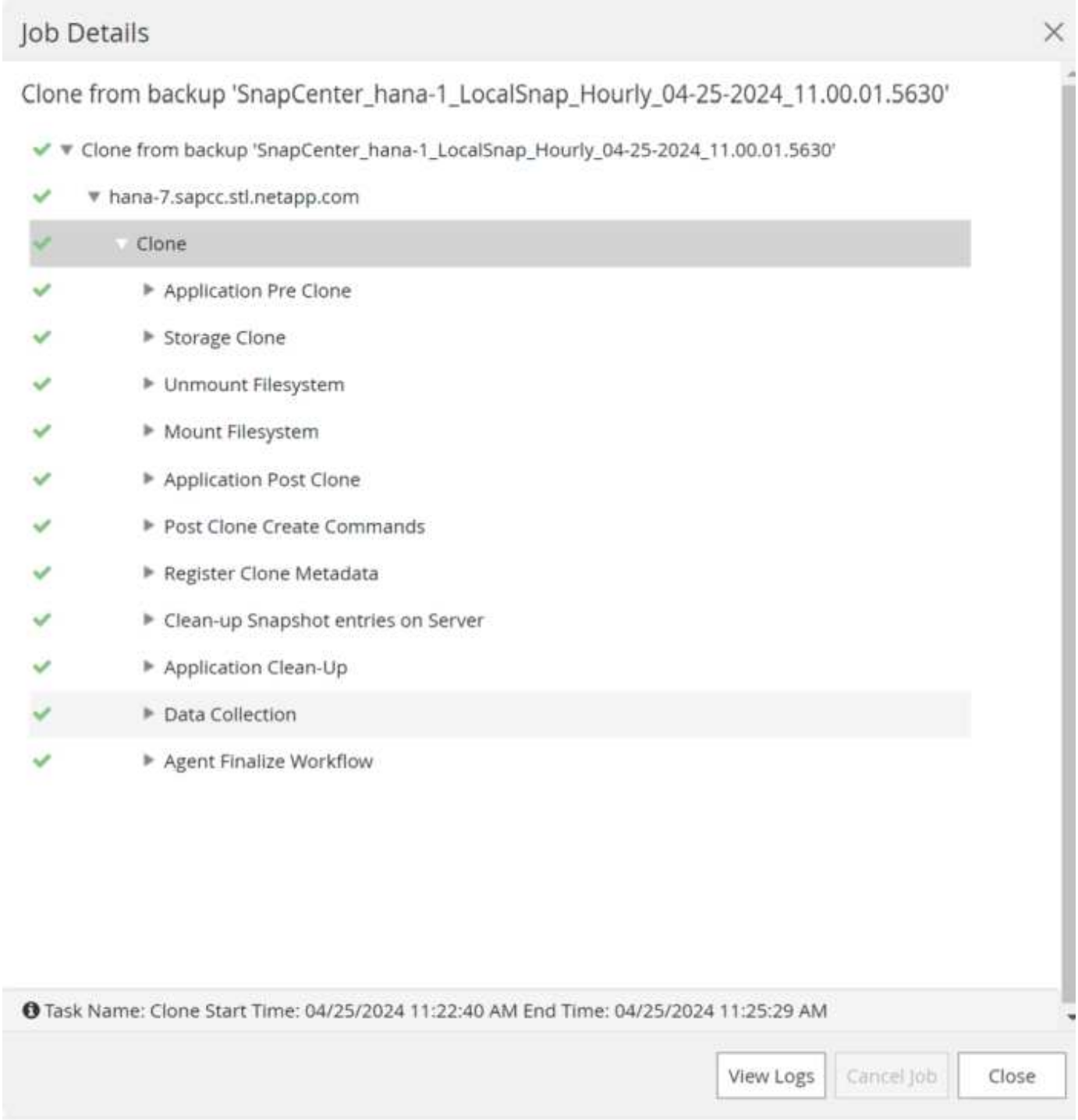
1. Immettere gli script post-clone opzionali con le opzioni della riga di comando richieste. Con il nostro esempio utilizziamo uno script post-clone per eseguire il recovery del database SAP HANA.



Come discusso in precedenza, l'utilizzo dello script di ripristino è facoltativo. Il recovery può essere eseguito anche manualmente al termine del workflow di cloning di SnapCenter.

Lo script per l'operazione di recovery recupera il database SAP HANA fino al point-in-time della Snapshot utilizzando l'operazione di clear logs e non esegue alcun recovery in avanti. Se è necessario un ripristino in avanti a un determinato momento, il ripristino deve essere eseguito manualmente. Un forward recovery manuale richiede inoltre che i backup del log dal sistema di origine siano disponibili sull'host di destinazione.

1. La schermata Dettagli lavoro in SnapCenter mostra lo stato di avanzamento dell'operazione. I dettagli del processo mostrano inoltre che il runtime complessivo, incluso il ripristino del database, è stato inferiore a 3 minuti.

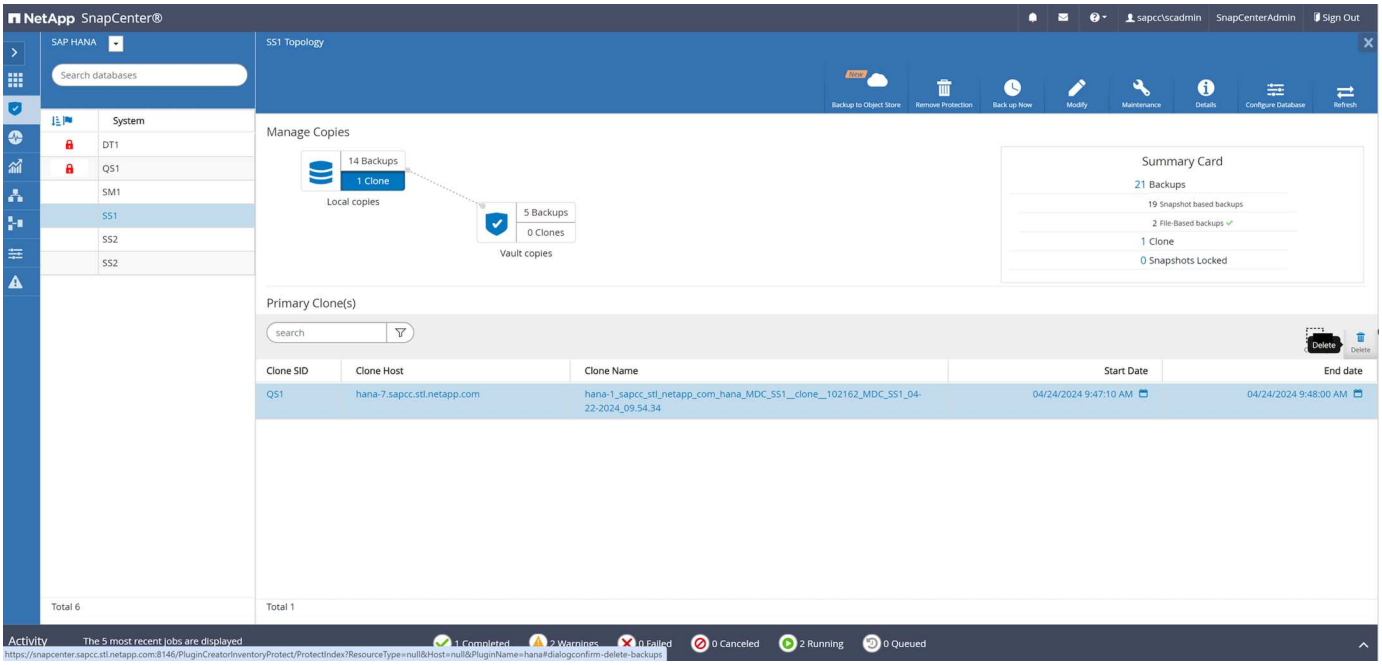


1. Il file di log dello `sc-system-refresh` script mostra le diverse istruzioni eseguite per l'operazione di ripristino. Lo script legge l'elenco dei tenant dal database di sistema ed esegue un ripristino di tutti i tenant esistenti.

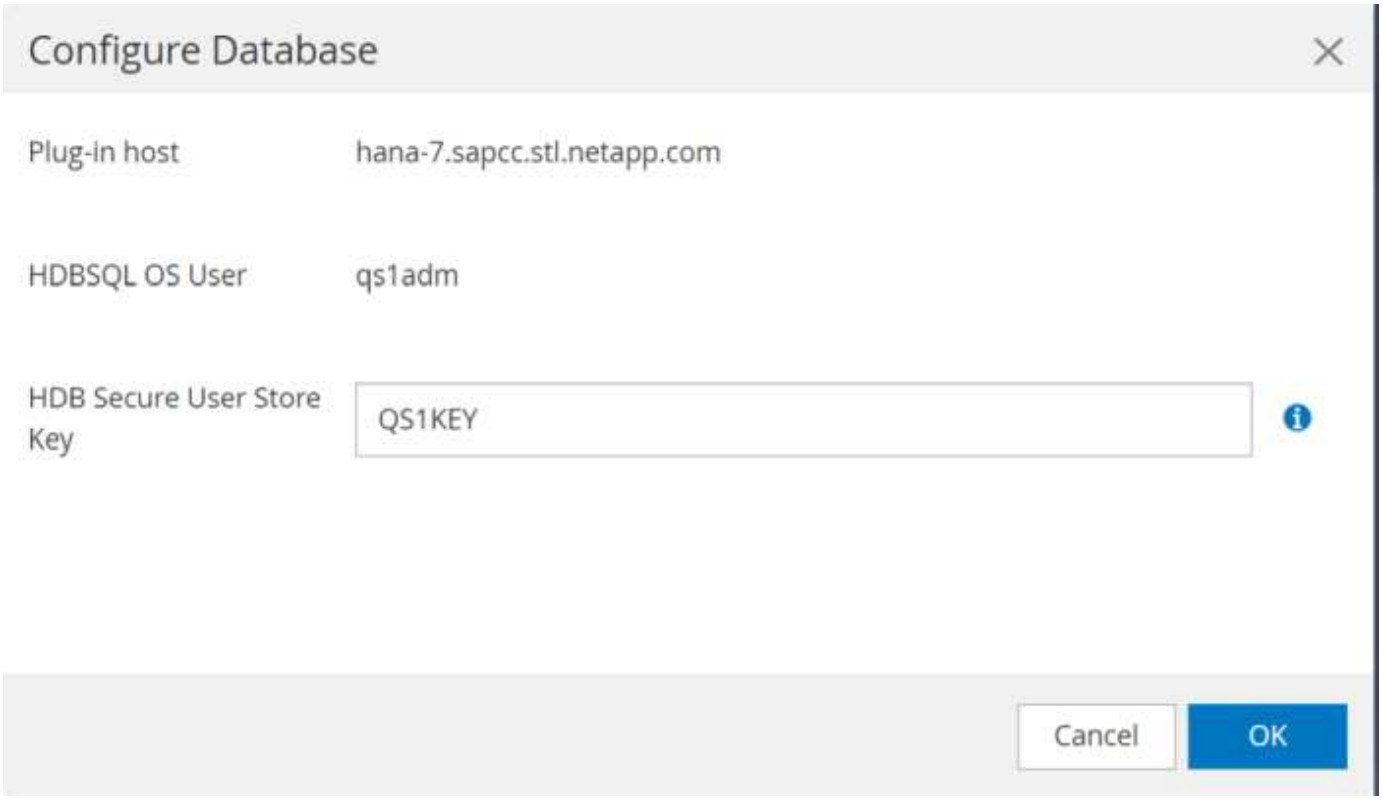
```
20240425112328###hana-7###sc-system-refresh.sh: Script version: 3.0
hana-7:/mnt/sapcc-share/SAP-System-Refresh # cat sap-system-refresh-
QS1.log
20240425112328###hana-7###sc-system-refresh.sh: ******************
Starting script: recovery operation ************************
20240425112328###hana-7###sc-system-refresh.sh: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

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

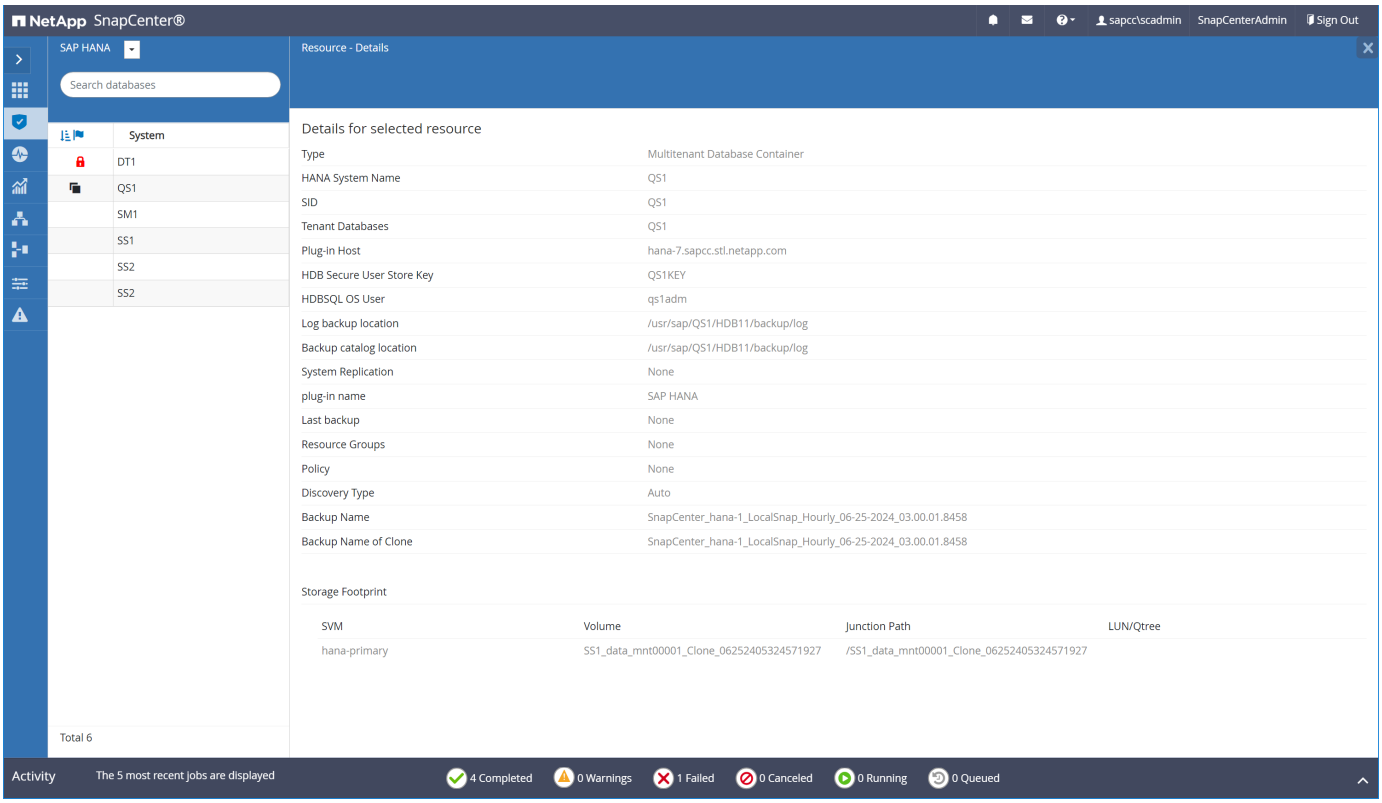
1. Al termine del lavoro SnapCenter, il clone è visibile nella vista topologia del sistema di origine.



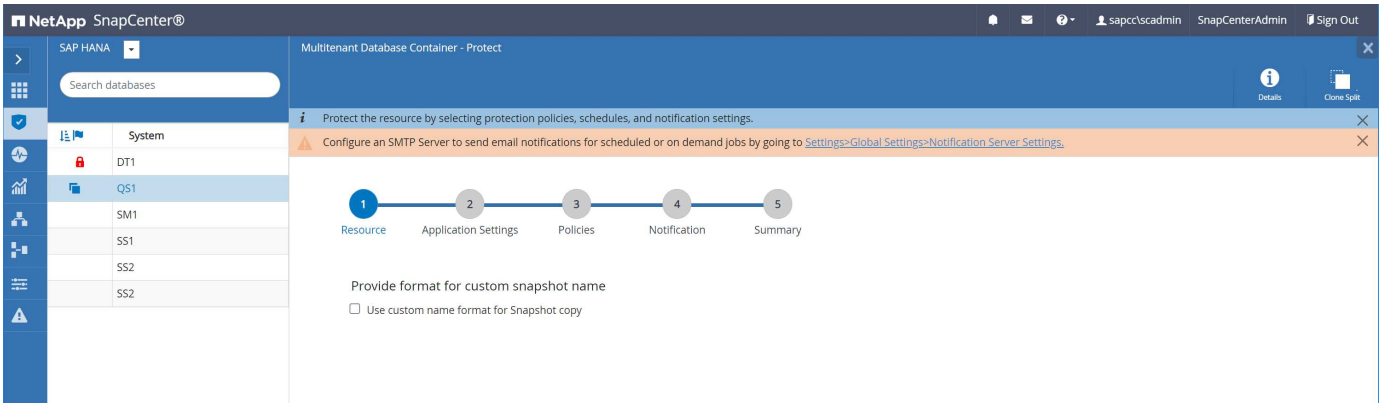
1. Il database SAP HANA è ora in esecuzione.
2. Per proteggere il sistema SAP HANA di destinazione, è necessario eseguire il rilevamento automatico facendo clic sulla risorsa di sistema di destinazione.



Al termine del processo di auto-Discovery, il nuovo volume clonato è elencato nella sezione relativa all'ingombro dello storage.

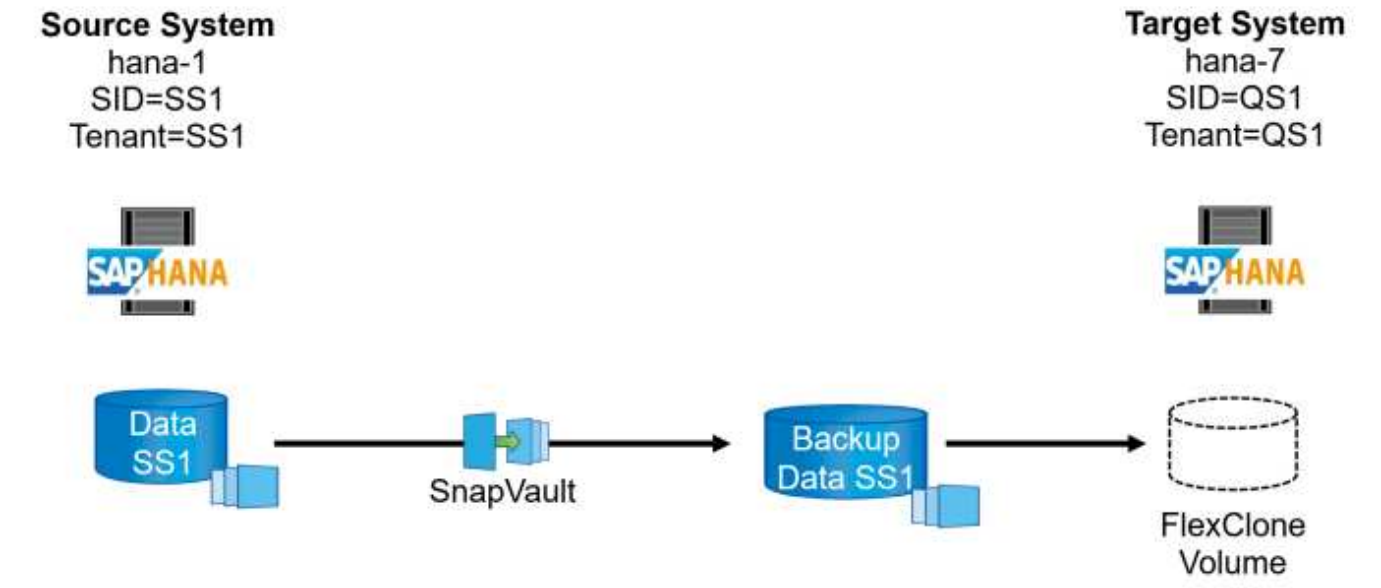


Facendo nuovamente clic sulla risorsa, è possibile configurare la protezione dei dati per il sistema QS1 aggiornato.

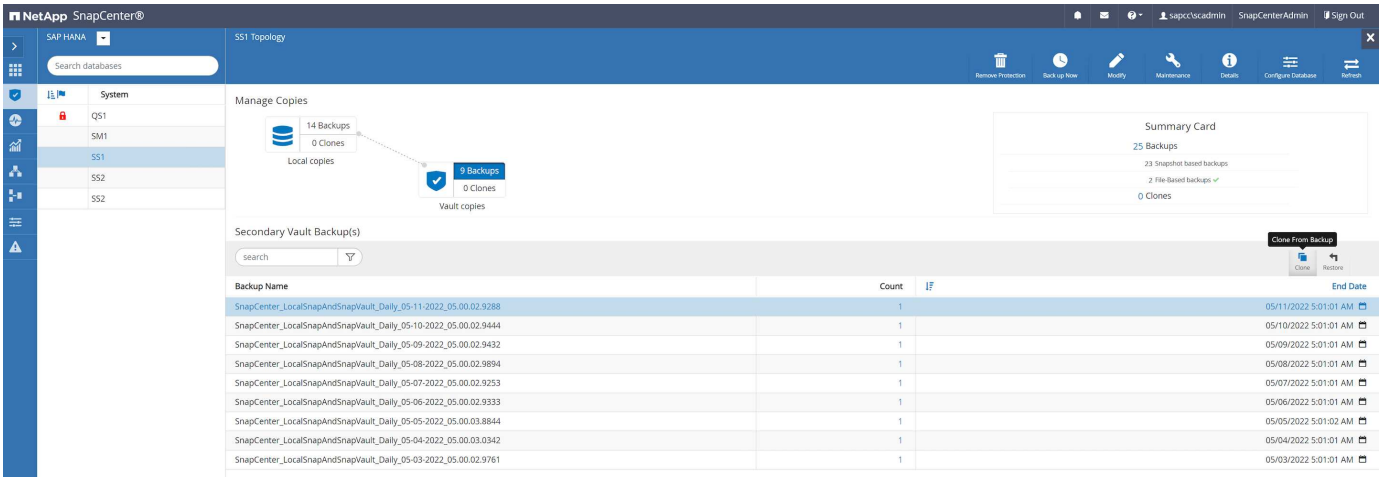


Clonazione dallo storage per il backup off-site

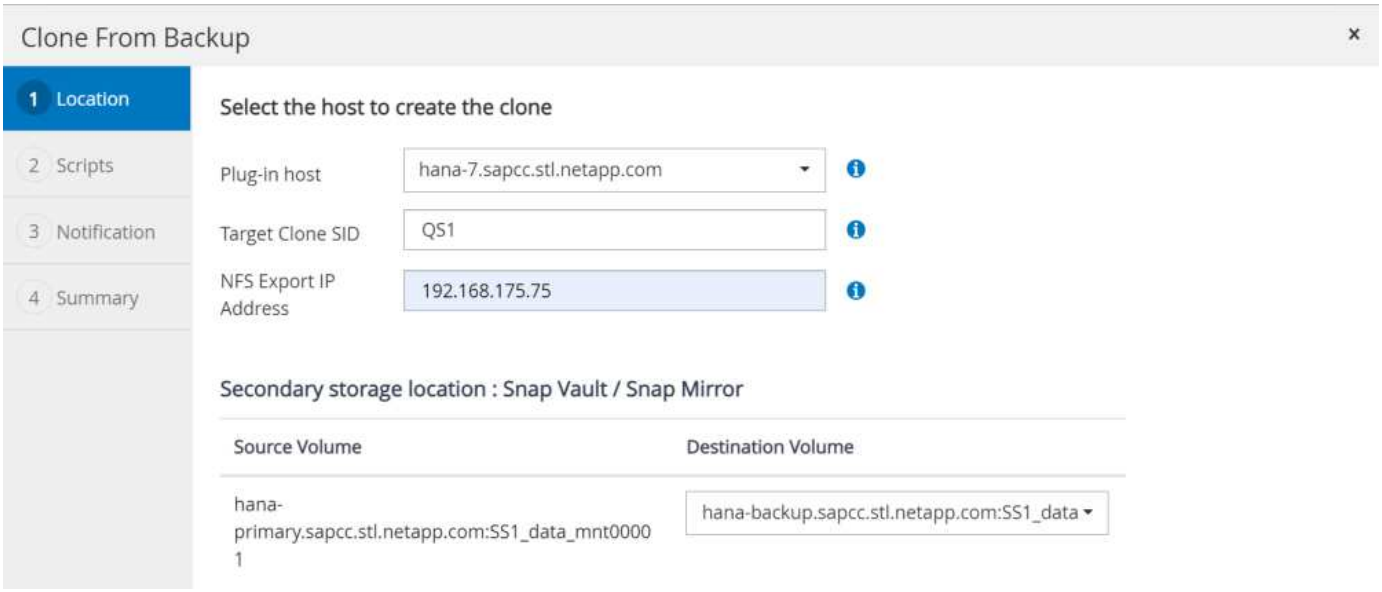
Questa sezione descrive il workflow di refresh del sistema SAP HANA per il quale il nome del tenant sul sistema di origine e di destinazione è identico al SID. La clonazione dello storage viene eseguita nello storage di backup off-site e ulteriormente automatizzata utilizzando lo script sc-system-refresh.sh.



L’unica differenza nel workflow di refresh del sistema SAP HANA tra il cloning dello storage di backup primario e off-site è la selezione del backup Snapshot in SnapCenter. Per il cloning dello storage di backup off-site, occorre selezionare prima i backup secondari, quindi selezionare il backup Snapshot.



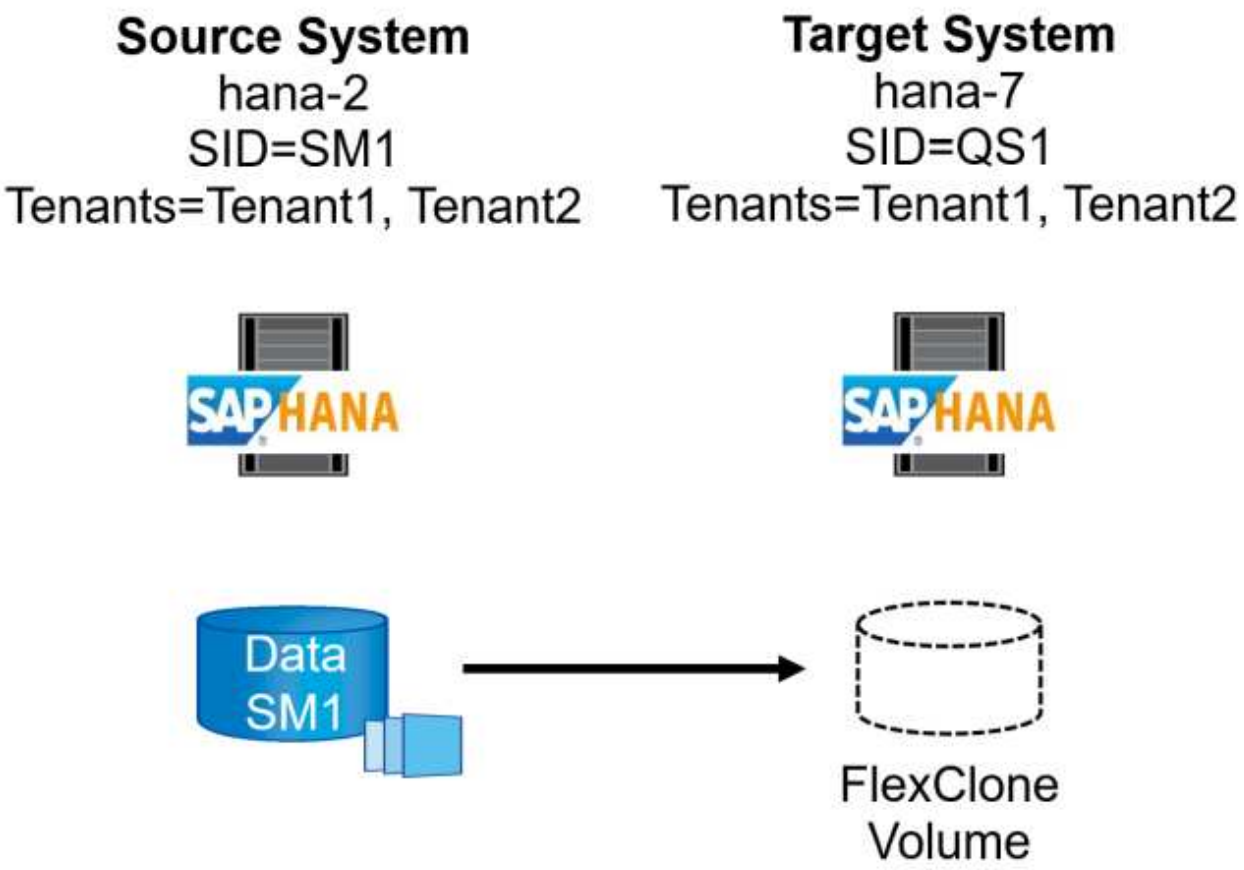
Se sono presenti più posizioni di storage secondario per il backup selezionato, è necessario scegliere il volume di destinazione richiesto.



Tutti i passaggi successivi sono identici al flusso di lavoro per il cloning dallo storage primario.

Cloning di un sistema SAP HANA con tenant multipli

Questa sezione descrive il workflow di refresh del sistema SAP HANA con tenant multipli. La clonazione dello storage viene eseguita nello storage primario e ulteriormente automatizzata utilizzando lo script `sc-system-refresh.sh`.



La procedura necessaria in SnapCenter è identica a quella descritta nella sezione "clonazione dello storage primario con nome tenant uguale a SID". L'unica differenza è nell'operazione di recupero del tenant all'interno dello script `sc-system-refresh.sh`, dove tutti i tenant vengono recuperati.

```
20240430070214###hana-7###sc-system-refresh.sh:
**********************************************************************
********
20240430070214###hana-7###sc-system-refresh.sh: Script version: 3.0
20240430070214###hana-7###sc-system-refresh.sh: ******************
Starting script: recovery operation *************************
20240430070214###hana-7###sc-system-refresh.sh: Recover system database.
20240430070214###hana-7###sc-system-refresh.sh:
/usr/sap/QS1/HDB11/exe/Python/bin/python
/usr/sap/QS1/HDB11/exe/python_support/recoverSys.py --command "RECOVER
DATA USING SNAPSHOT CLEAR LOG"
[140310725887808, 0.008] >> starting recoverSys (at Tue Apr 30 07:02:15
2024)
[140310725887808, 0.008] args: ()
[140310725887808, 0.008] keys: \{'command': 'RECOVER DATA USING SNAPSHOT
CLEAR LOG'}
using logfile /usr/sap/QS1/HDB11/hana-7/trace/backup.log
recoverSys started: ============2024-04-30 07:02:15 ============
testing master: hana-7
hana-7 is master
shutdown database, timeout is 120
stop system
stop system on: hana-7
stopping system: 2024-04-30 07:02:15
stopped system: 2024-04-30 07:02:15
creating file recoverInstance.sql
restart database
restart master nameserver: 2024-04-30 07:02:20
start system: hana-7
sapcontrol parameter: ['-function', 'Start']
sapcontrol returned successfully:
2024-04-30T07:02:32-04:00 P0023828 18f2eab9331 INFO RECOVERY RECOVER DATA
finished successfully
recoverSys finished successfully: 2024-04-30 07:02:33
[140310725887808, 17.548] 0
[140310725887808, 17.548] << ending recoverSys, rc = 0 (RC_TEST_OK), after
17.540 secs
20240430070233###hana-7###sc-system-refresh.sh: Wait until SAP HANA
database is started ....
20240430070233###hana-7###sc-system-refresh.sh: Status: GRAY
20240430070243###hana-7###sc-system-refresh.sh: Status: GRAY
20240430070253###hana-7###sc-system-refresh.sh: Status: GRAY
```

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

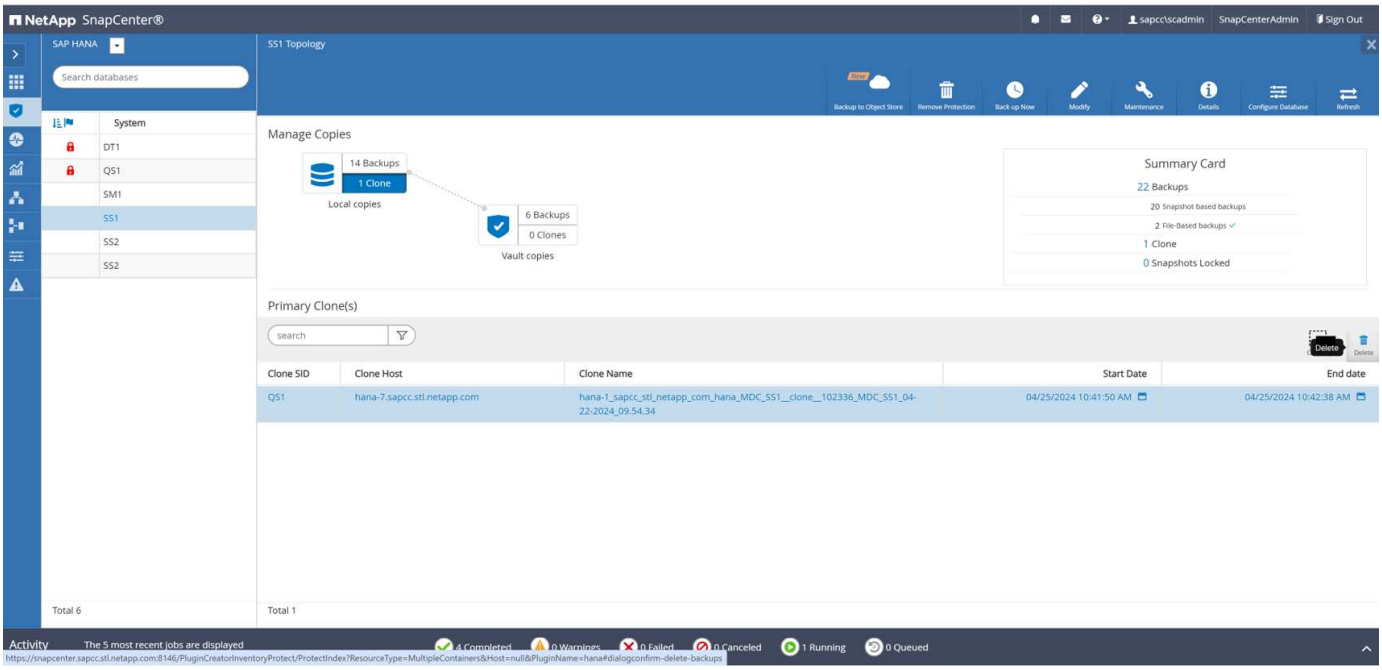
Operazione di eliminazione dei cloni

Una nuova operazione di refresh del sistema SAP HANA viene avviata mediante la pulizia del sistema di destinazione mediante l'operazione di eliminazione del clone SnapCenter.

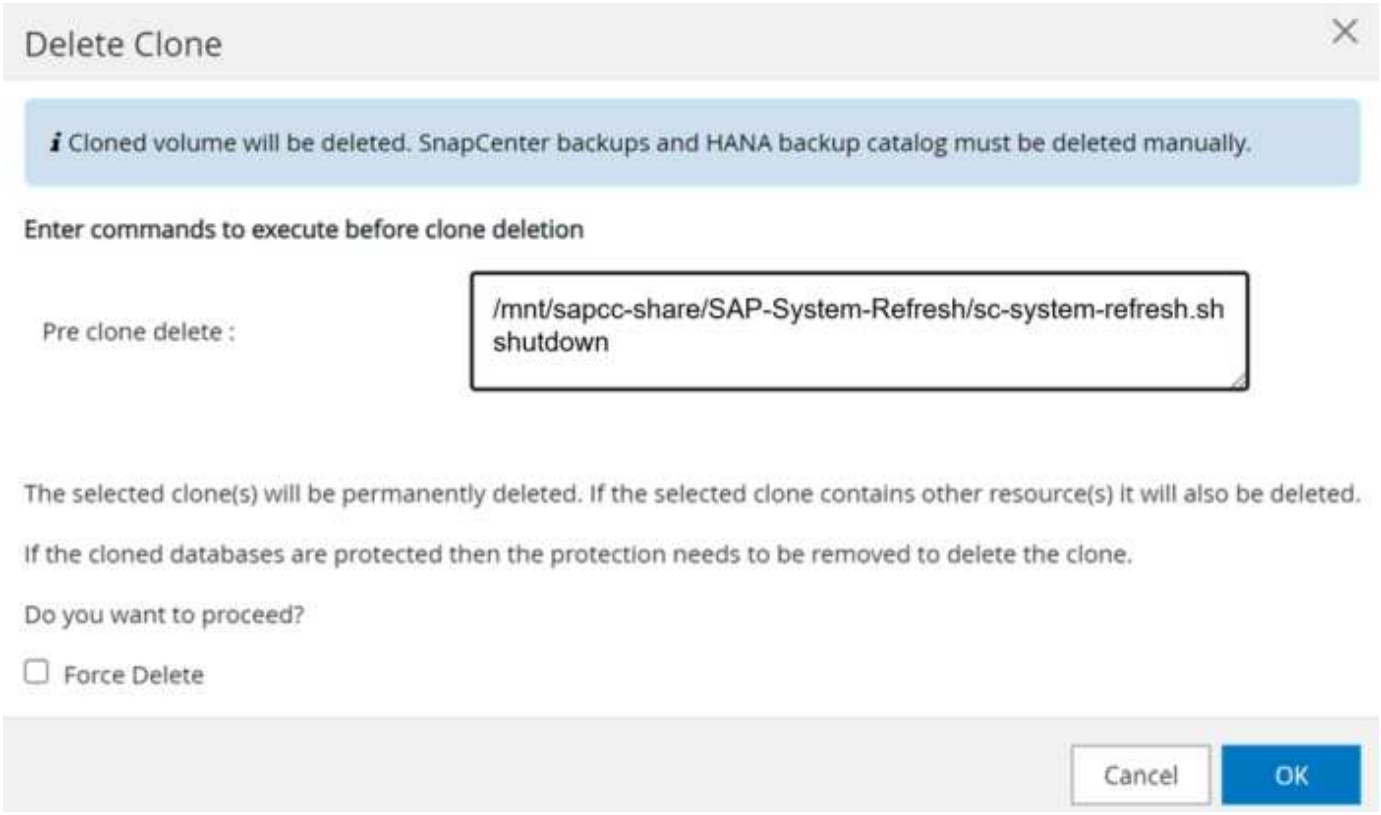
Se il sistema SAP HANA di destinazione è stato protetto in SnapCenter, occorre rimuovere per primo la protezione. Nella vista della topologia del sistema di destinazione, fare clic su Remove Protection (Rimuovi protezione).

Il flusso di lavoro di eliminazione dei cloni viene eseguito mediante la seguente procedura.

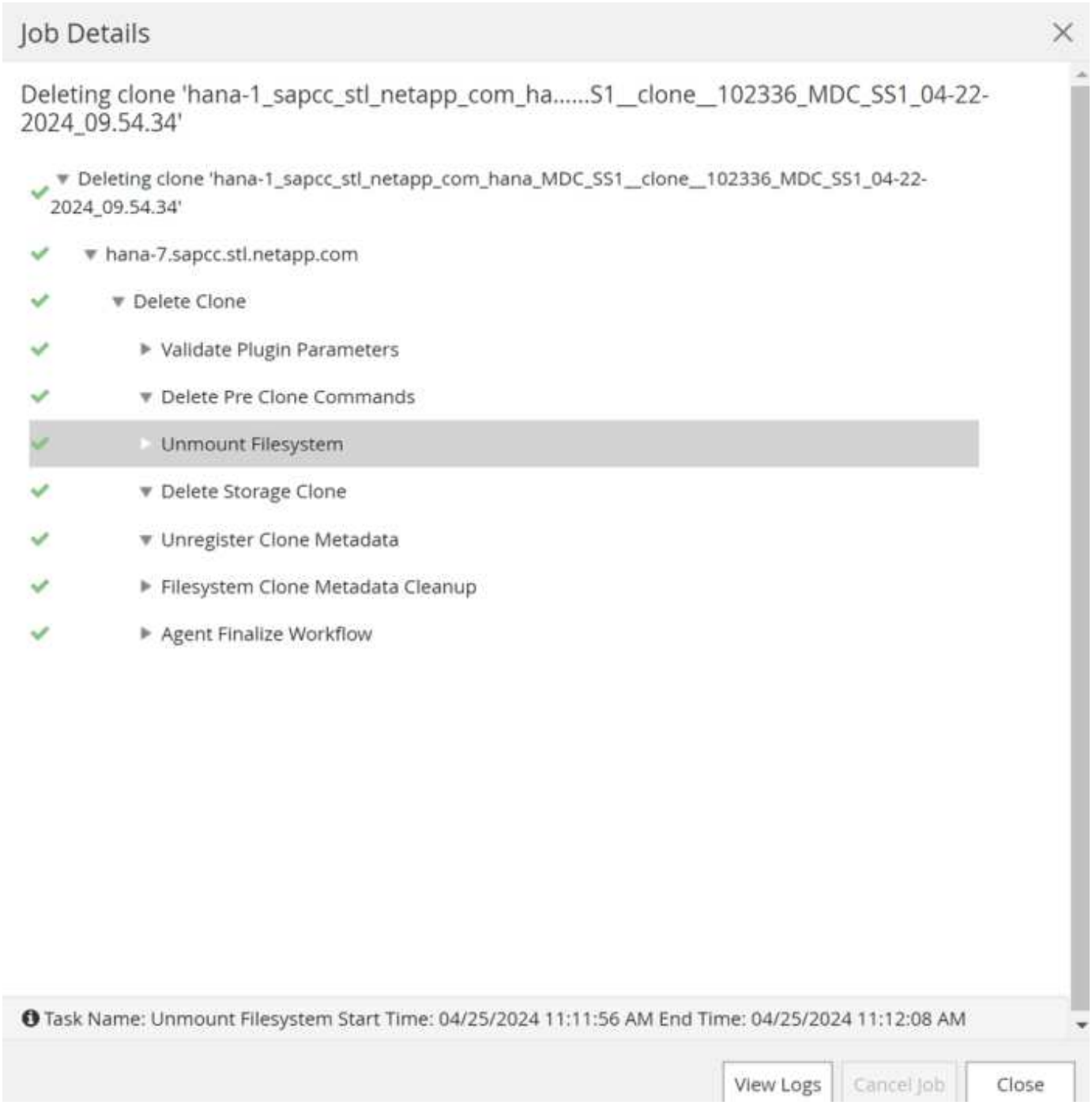
1. Selezionare il clone all'interno della vista topologica del sistema di origine e fare clic su Elimina.



1. Immettere gli script pre-clone e dismount con le opzioni della riga di comando richieste.



1. La schermata dei dettagli del lavoro in SnapCenter mostra lo stato di avanzamento dell'operazione.



1. Il file di registro dello `sc-system-refresh` script mostra le istruzioni per l'operazione di arresto e smontaggio.

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

1. L'operazione di refresh SAP HANA può ora essere riavviata utilizzando l'operazione di creazione del clone SnapCenter.

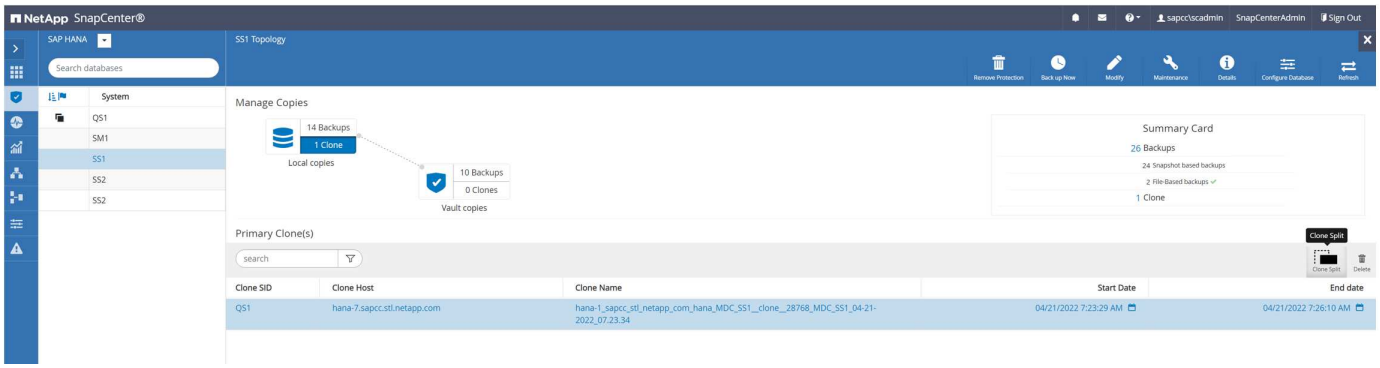
Aggiornamento del sistema SAP HANA con operazione di suddivisione dei cloni

Se si prevede di utilizzare il sistema di destinazione dell'operazione di refresh del sistema per un periodo di tempo più lungo, conviene suddividere il volume FlexClone nell'ambito dell'operazione di refresh del sistema.

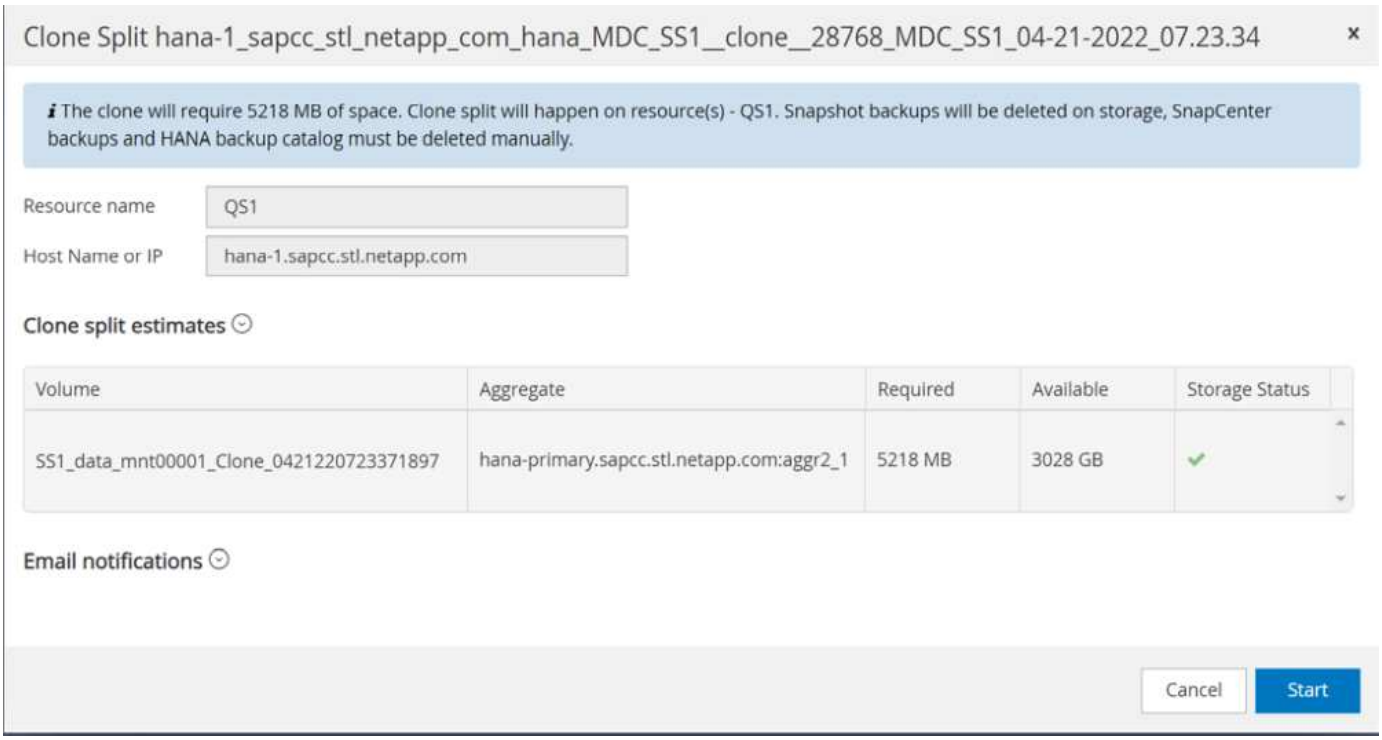
> L'operazione clone split non blocca l'utilizzo del volume clonato e può quindi essere eseguita in qualsiasi momento mentre il database SAP HANA è in uso.

> Con Azure NetApp Files, l'operazione di clone split non è disponibile, poiché Azure NetApp Files suddivide sempre il clone dopo la creazione.

Il flusso di lavoro di divisione dei cloni in SnapCenter viene avviato nella vista topologia del sistema di origine selezionando il clone e facendo clic su divisione dei cloni.



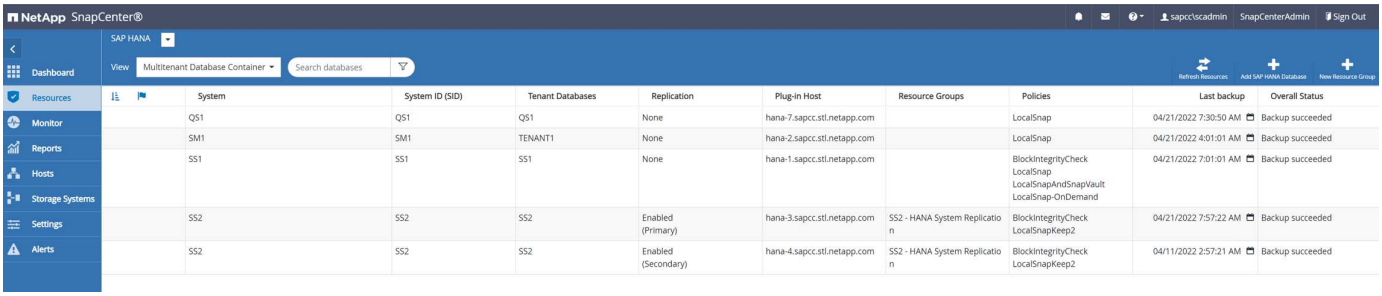
Nella schermata successiva viene visualizzata un'anteprima che fornisce informazioni sulla capacità richiesta per il volume suddiviso.

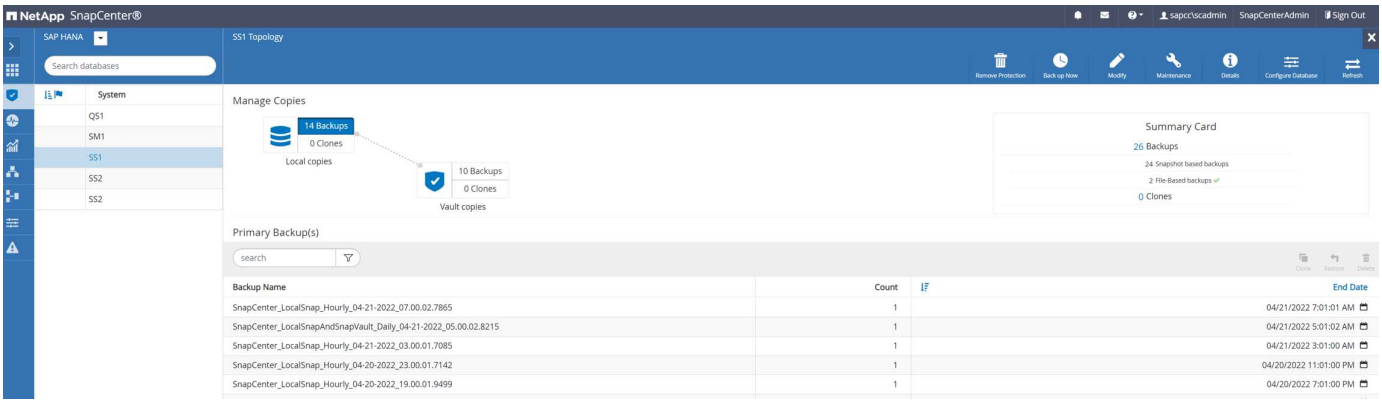


Il log dei lavori di SnapCenter mostra lo stato di avanzamento dell'operazione di suddivisione dei cloni.



Nella vista delle risorse in SnapCenter il sistema target QS1 non è ora più contrassegnato come una risorsa clonata. Quando si torna alla vista della topologia del sistema di origine, il clone non è più visibile. Il volume suddiviso è ora indipendente dal backup Snapshot del sistema di origine.





Il flusso di lavoro di refresh dopo un'operazione di suddivisione dei cloni appare leggermente diverso rispetto all'operazione senza suddivisione dei cloni. Dopo un'operazione di cloning split, non è più necessaria alcuna operazione di eliminazione dei cloni, poiché il volume dei dati di destinazione non è più un volume FlexClone.

Il flusso di lavoro è costituito dai seguenti passaggi:

1. Se il sistema SAP HANA di destinazione è stato protetto in SnapCenter, occorre rimuovere per primo la protezione.
2. Il database SAP HANA deve essere arrestato, il volume di dati deve essere smontato e la voce fstab creata da SnapCenter deve essere rimossa. Questi passaggi devono essere eseguiti manualmente.
3. Ora il workflow di creazione dei cloni di SnapCenter può essere eseguito come descritto in precedenza nelle sezioni.
4. Dopo l'operazione di refresh, il vecchio volume di dati di destinazione esiste ancora e deve essere eliminato manualmente con, ad esempio, Gestore di sistema di ONTAP.

Automazione del workflow SnapCenter con script PowerShell

Nelle sezioni precedenti, i diversi flussi di lavoro sono stati eseguiti utilizzando l'interfaccia utente di SnapCenter. Tutti i flussi di lavoro possono essere eseguiti anche con script PowerShell o chiamate API REST, consentendo un'ulteriore automazione. Le sezioni seguenti descrivono esempi di script PowerShell di base per i seguenti flussi di lavoro.

- Creare un clone
- Elimina clone

> Gli script di esempio vengono forniti così come sono e non sono supportati da NetApp.

Tutti gli script devono essere eseguiti in una finestra di comando PowerShell. Prima di poter eseguire gli script, è necessario stabilire una connessione al server SnapCenter utilizzando `Open-SmConnection` comando.

Creare un clone

Il semplice script riportato di seguito mostra come è possibile eseguire un'operazione di creazione di un clone SnapCenter utilizzando i comandi PowerShell. SnapCenter `New-SmClone` il comando viene eseguito con l'opzione della riga di comando richiesta per l'ambiente di laboratorio e lo script di automazione discusso in precedenza.

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

L'output della schermata mostra l'esecuzione dello script di creazione del clone PowerShell.

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

Elimina clone

Il semplice script riportato di seguito mostra come è possibile eseguire un'operazione di eliminazione dei cloni

di SnapCenter utilizzando i comandi PowerShell. SnapCenter `Remove-SmClone` il comando viene eseguito con l'opzione della riga di comando richiesta per l'ambiente di laboratorio e lo script di automazione discusso in precedenza.

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

L'output della schermata mostra l'esecuzione dello script PowerShell clone –delete.ps1.

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

Clone del sistema SAP con SnapCenter

In questa sezione viene fornita una descrizione dettagliata dell'operazione di clonazione del sistema SAP, che può essere utilizzata per configurare un sistema di riparazione per risolvere il problema della corruzione logica.

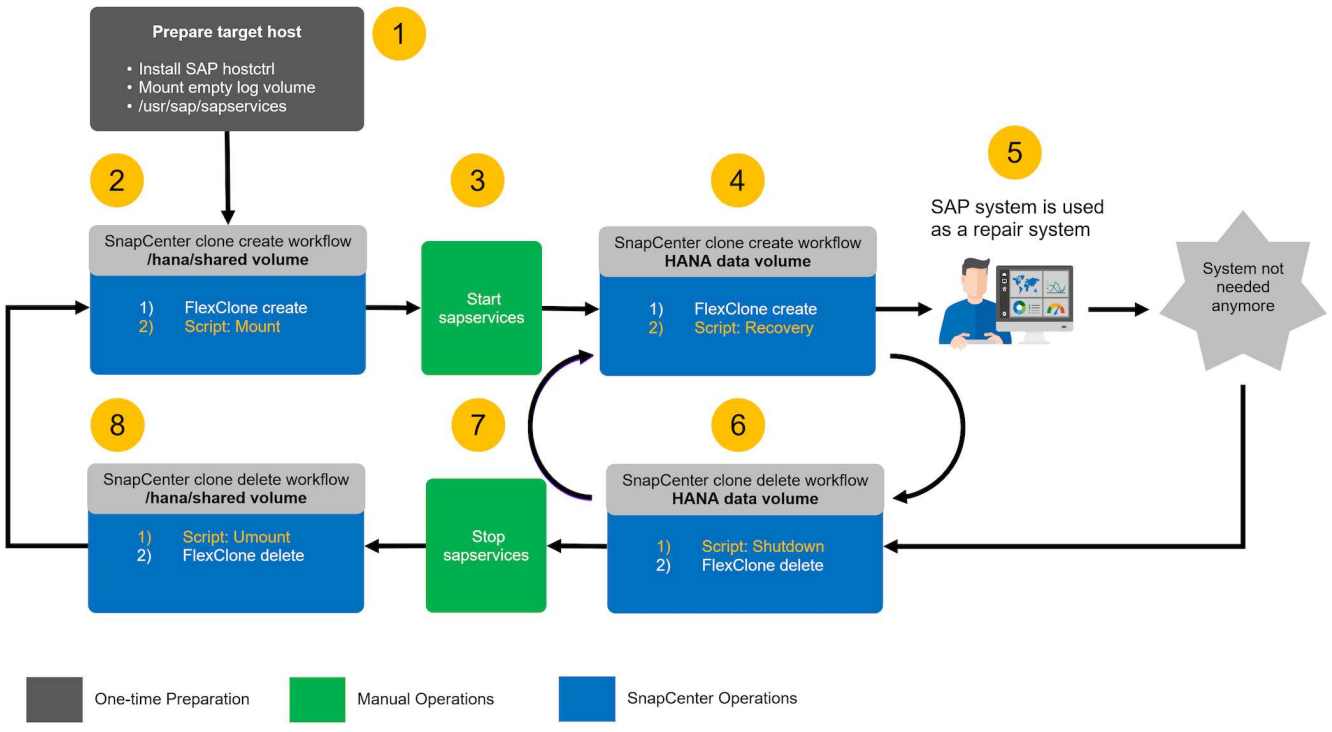
La figura seguente riassume i passaggi necessari per un'operazione di cloning di sistema SAP con SnapCenter.

1. Preparare l'host di destinazione.
2. Il clone di SnapCenter crea un workflow per il volume condiviso di SAP HANA.
3. Avviare i servizi SAP HANA.
4. Il clone di SnapCenter crea il workflow per il volume di dati SAP HANA, incluso il recovery del database.
5. Il sistema SAP HANA può ora essere utilizzato come sistema di riparazione.

> Se è necessario ripristinare il sistema su un backup Snapshot diverso, i passaggi 6 e 4 sono sufficienti. Il volume condiviso di SAP HANA può continuare a essere montato.

Se il sistema non è più necessario, il processo di pulizia viene eseguito con le seguenti operazioni.

6. Flusso di lavoro di eliminazione dei cloni SnapCenter per il volume di dati SAP HANA, incluso l'arresto del database.
7. Arrestare i servizi SAP HANA.
8. Flusso di lavoro di eliminazione dei cloni SnapCenter per il volume condiviso SAP HANA.



Prerequisiti e limitazioni

I flussi di lavoro descritti nelle sezioni seguenti presentano alcuni prerequisiti e limitazioni relativi all'architettura di sistema SAP HANA e alla configurazione SnapCenter.

- Il flusso di lavoro descritto è valido per sistemi SAP HANA MDC a host singolo. Non sono supportati più sistemi host.
- Il plug-in SAP HANA di SnapCenter deve essere implementato sull'host di destinazione per consentire l'esecuzione degli script di automazione.

- Il workflow è stato validato per NFS. L'automazione `script sc-mount-volume.sh`, utilizzata per montare il volume condiviso SAP HANA, non supporta FCP. Questa operazione deve essere eseguita manualmente o estendendo lo script.
- Il flusso di lavoro descritto è valido solo per SnapCenter 5,0 o versioni successive.

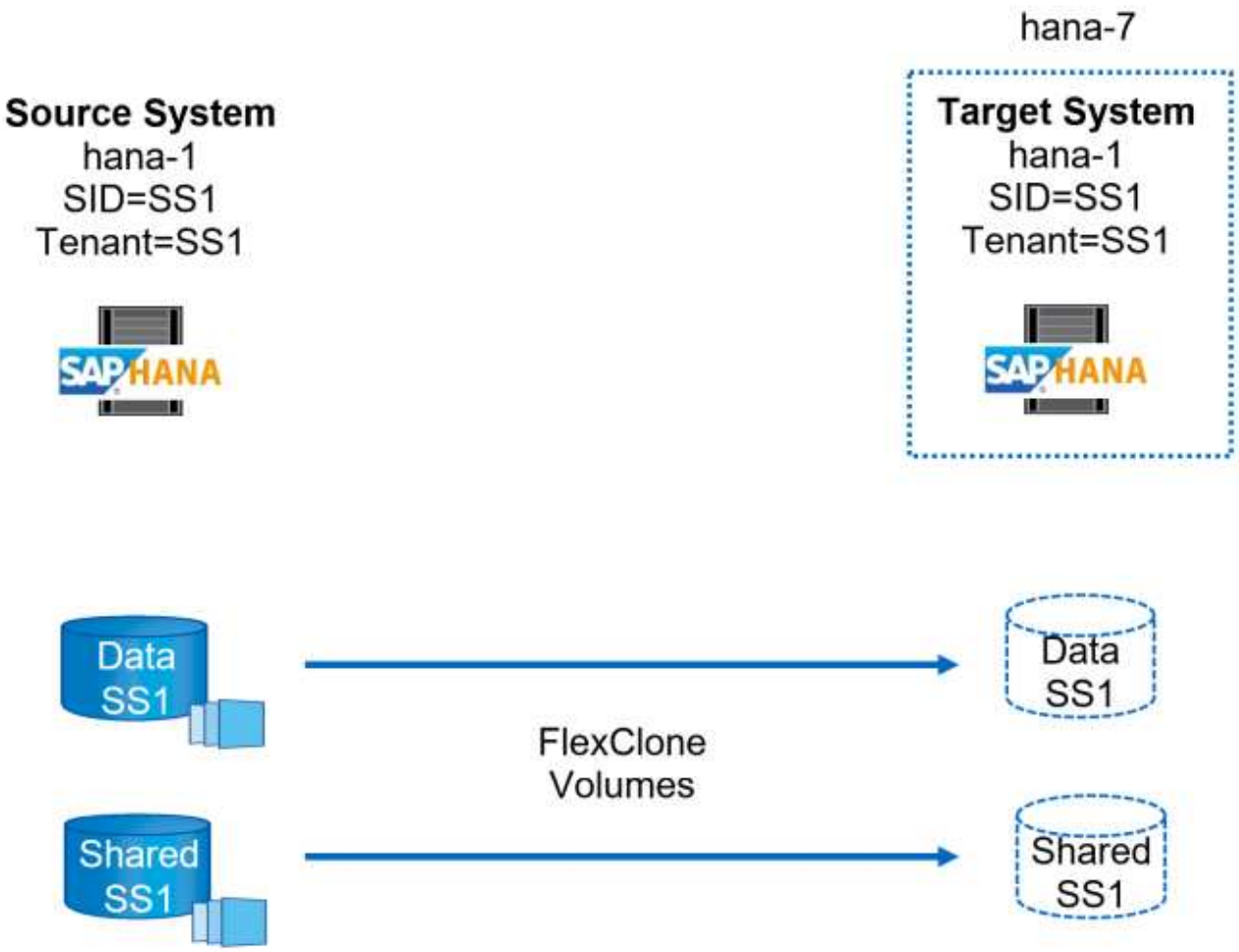
Setup di laboratorio

La figura riportata di seguito mostra la configurazione di laboratorio utilizzata per il funzionamento dei cloni del sistema.

Sono state utilizzate le seguenti versioni software:

- SnapCenter 5,0
- Sistemi SAP HANA: HANA 2,0 SPS6 rev,61
- SLES 15
- ONTAP 9.7P7

Tutti i sistemi SAP HANA devono essere configurati in base alla guida alla configurazione "SAP HANA su sistemi NetApp AFF con NFS". SnapCenter e le risorse SAP HANA sono state configurate in base alla guida alle Best practice "Backup e ripristino SAP HANA con SnapCenter".



Preparazione dell'host di destinazione

In questa sezione vengono descritte le fasi di preparazione richieste per un server utilizzato come destinazione di un clone di sistema.

Durante il normale funzionamento, l'host di destinazione può essere utilizzato per altri scopi, ad esempio come sistema di test o QA SAP HANA. Pertanto, la maggior parte delle fasi descritte deve essere eseguita quando viene richiesta l'operazione di cloni del sistema. D'altra parte, i file di configurazione rilevanti, come `/etc/fstab` e `/usr/sap/sapservices`, possono essere preparati e poi messi in produzione semplicemente copiando il file di configurazione.

La preparazione dell'host di destinazione include anche l'arresto del sistema di QA o di test SAP HANA.

Nome host e indirizzo IP del server di destinazione

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

È necessario stabilire un corretto scherma del server di destinazione in modo che non possa comunicare con altri sistemi. Se non si dispone di un corretto sistema di recinzione, il sistema di produzione clonato potrebbe scambiare dati con altri sistemi di produzione.

Nella configurazione di laboratorio, abbiamo modificato il nome host del sistema di destinazione solo internamente dal punto di vista del sistema di destinazione. Esternamente l'host era ancora accessibile con il nome host hana-7. Una volta effettuato l'accesso all'host, l'host stesso è hana-1.

Installare il software richiesto

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

Il plug-in SAP HANA di SnapCenter deve essere implementato sull'host di destinazione utilizzando l'operazione add host all'interno di SnapCenter.

Configurare utenti, porte e servizi SAP

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

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

```
#!/bin/sh
LD_LIBRARY_PATH=/usr/sap/SS1/HDB00/exe:$LD_LIBRARY_PATH;export
LD_LIBRARY_PATH;/usr/sap/SS1/HDB00/exe/sapstartsrv
pf=/usr/sap/SS1/SYS/profile/SS1_HDB00_hana-1 -D -u ss1adm
limit.descriptors=1048576
```

Preparare il volume di backup del log e del log

Poiché non è necessario clonare il volume di log dal sistema di origine e viene eseguito un ripristino con l'opzione Clear log, è necessario preparare un volume di log vuoto sull'host di destinazione.

Poiché il sistema di origine è stato configurato con un volume di backup del registro separato, è necessario preparare e montare un volume di backup del registro vuoto nello stesso punto di montaggio del sistema di origine.

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

All'interno del volume di log hdb*, è necessario creare le sottodirectory nello stesso modo del sistema di origine.

```
hana-1:/ # ls -al /hana/log/SS1/mnt00001/
total 16
drwxrwxrwx 5 root root 4096 Dec 1 06:15 .
drwxrwxrwx 1 root root 16 Nov 30 08:56 ..
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:14 hdb00001
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:15 hdb00002.00003
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:15 hdb00003.00003
```

All'interno del volume di backup del registro, è necessario creare sottodirectory per il sistema e il database tenant.

```
hana-1:/ # ls -al /mnt/log-backup/
total 12
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 04:48 .
drwxr-xr-- 2 ss1adm sapsys 4896 Dec 1 03:42 ..
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:15 DB_SS1
drwxr-xr-- 2 ss1adm sapsys 4096 Dec 1 06:14 SYSTEMDB
```

Preparare i montaggi del file system

È necessario preparare i punti di montaggio per i dati e il volume condiviso.

Con il nostro esempio, le directory `/hana/data/SS1/mnt00001`, `/hana/shared` e `usr/sap/SS1` devono essere create.

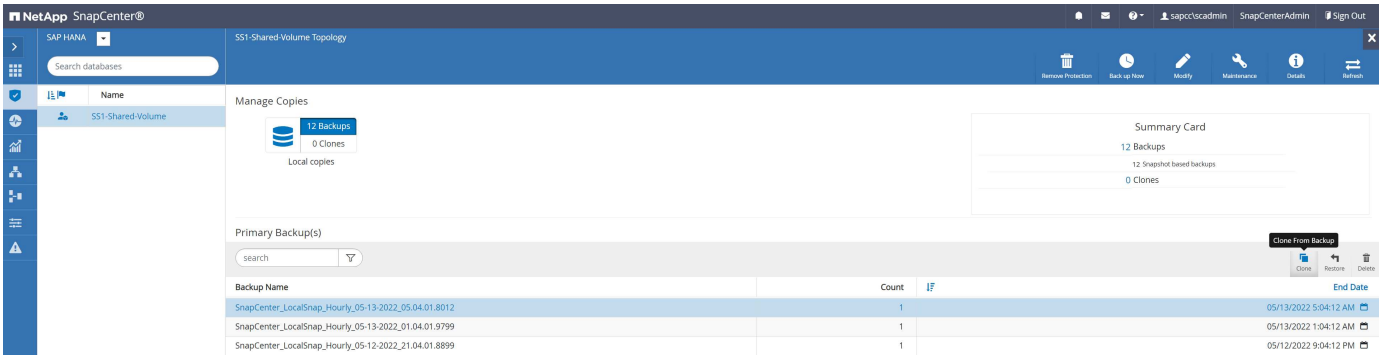
Preparare l'esecuzione dello script

È necessario aggiungere gli script che devono essere eseguiti sul sistema di destinazione al file di configurazione dei comandi consentiti da SnapCenter.

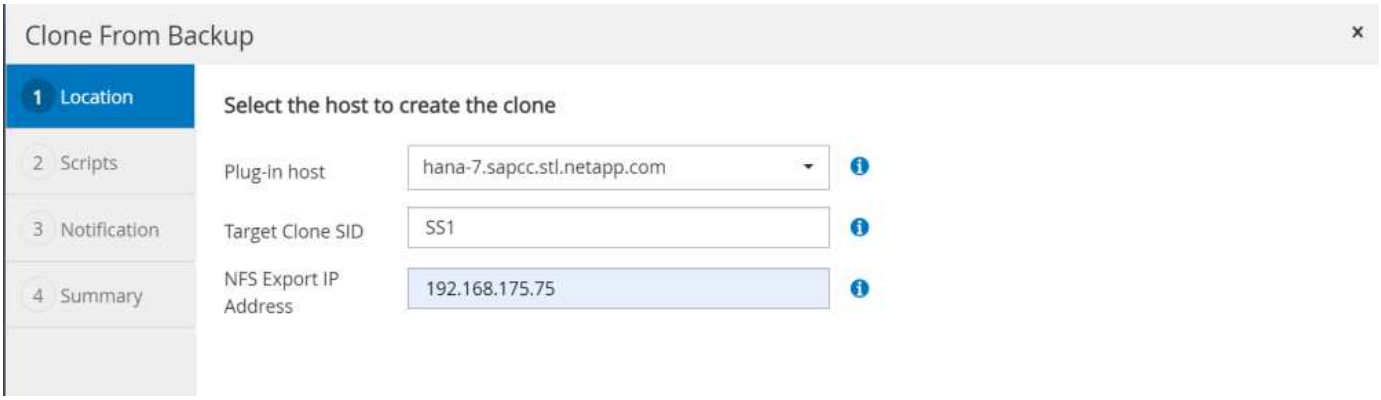
```
hana-7:/opt/NetApp/snapcenter/scc/etc # cat
/opt/NetApp/snapcenter/scc/etc/allowed_commands.config
command: mount
command: umount
command: /mnt/sapcc-share/SAP-System-Refresh/sc-system-refresh.sh
command: /mnt/sapcc-share/SAP-System-Refresh/sc-mount-volume.sh
hana-7:/opt/NetApp/snapcenter/scc/etc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

Clonazione del volume condiviso HANA

1. Selezionare un backup Snapshot dal volume condiviso SS1 del sistema di origine e fare clic su Clone (Clona).

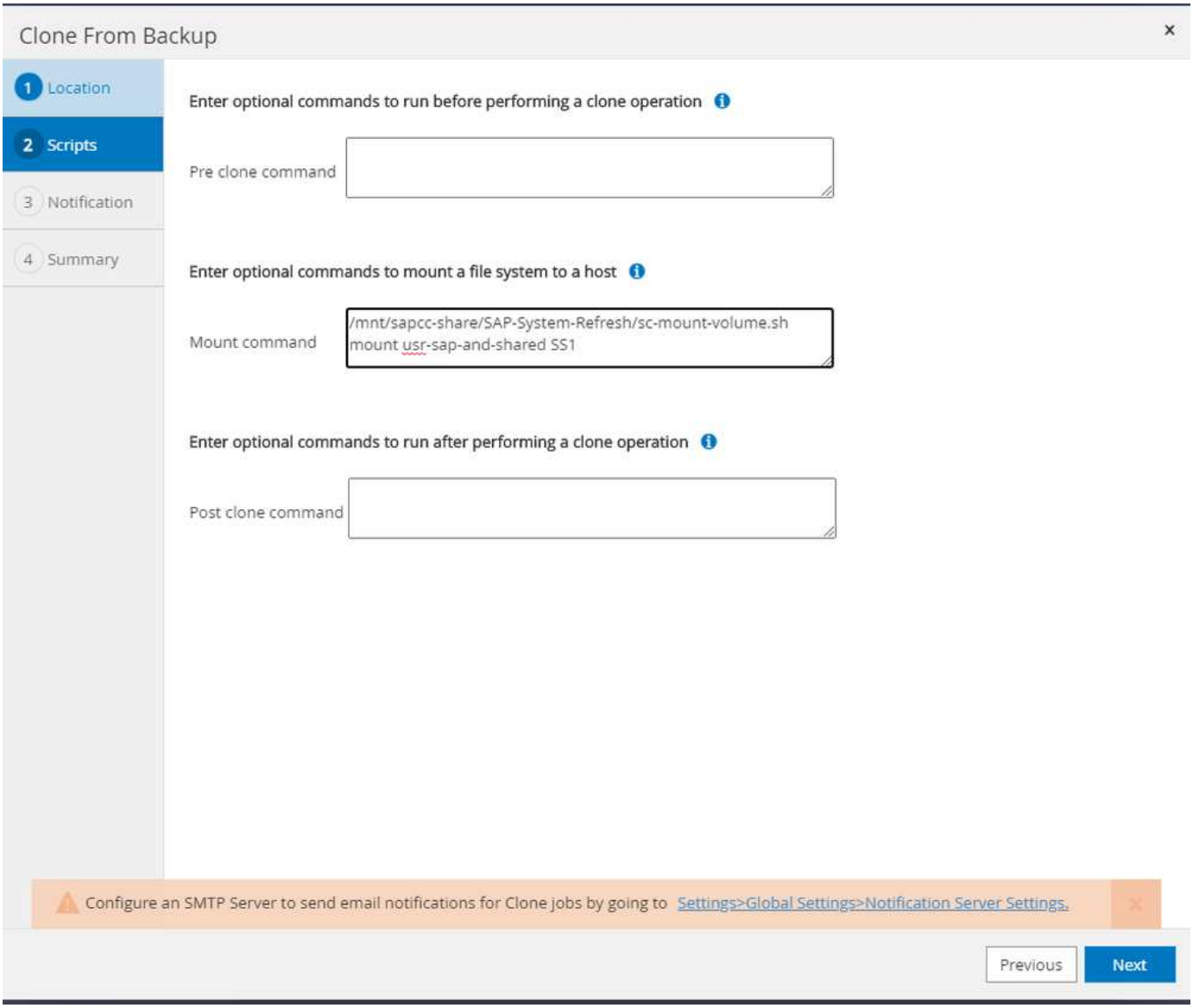


1. Selezionare l'host in cui è stato preparato il sistema di riparazione di destinazione. L'indirizzo IP di esportazione NFS deve essere l'interfaccia di rete dello storage dell'host di destinazione. Come SID di destinazione, mantenere lo stesso SID del sistema di origine. Nel nostro esempio SS1.

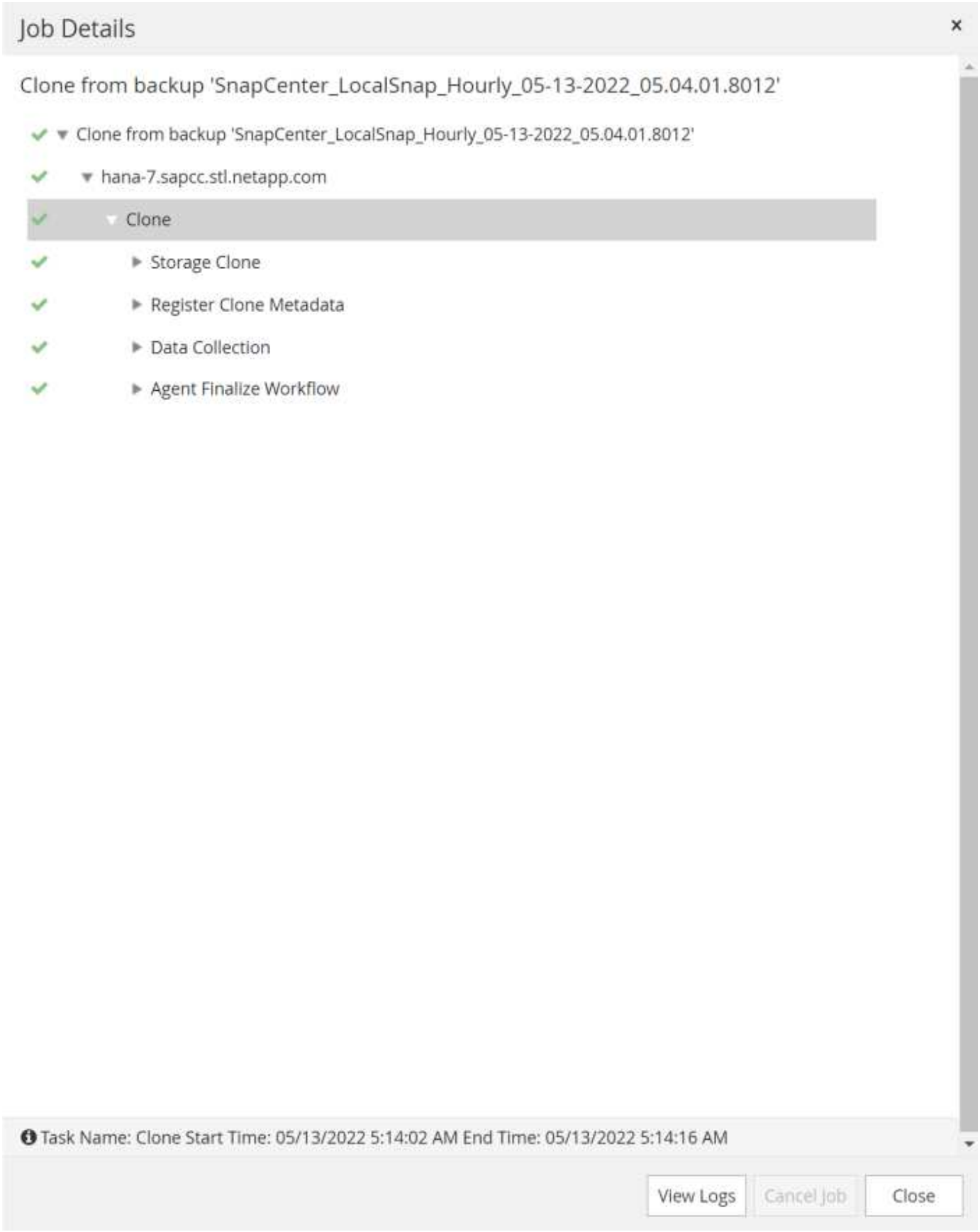


1. Inserire lo script di montaggio con le opzioni della riga di comando richieste.

Il sistema SAP HANA utilizza un singolo volume per `/hana/shared` e per `/usr/sap/SS1`, separato in sottodirectory come consigliato nella guida alla configurazione "SAP HANA su sistemi NetApp AFF con NFS". Lo script `sc-mount-volume.sh` supporta questa configurazione utilizzando una speciale opzione della riga di comando per il percorso di mount. Se l'opzione della riga di comando del percorso di mount è uguale a usr-sap-and-shared, lo script monta le sottodirectory condivise e usr-sap nel volume di conseguenza.



1. La schermata Dettagli lavoro in SnapCenter mostra lo stato di avanzamento dell'operazione.



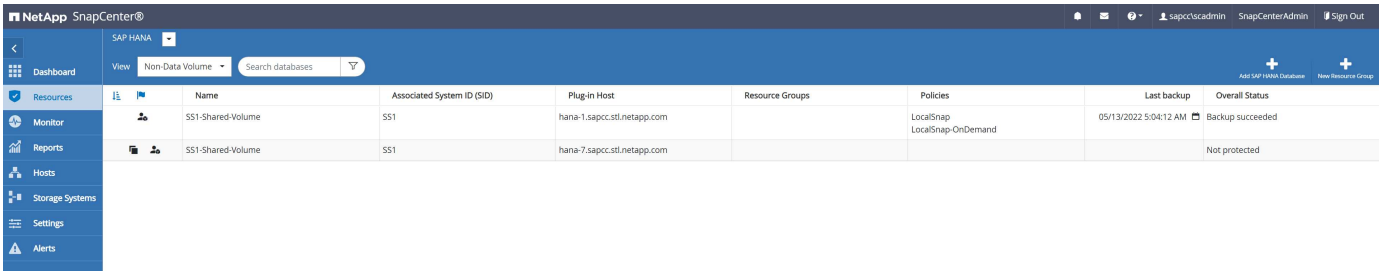
1. Il file di log dello script sc-mount-volume.sh mostra le diverse fasi eseguite per l'operazione di mount.

```
20201201041441###hana-1###sc-mount-volume.sh: Adding entry in /etc/fstab.
20201201041441###hana-1###sc-mount-volume.sh:
192.168.175.117://SS1_shared_Clone_05132205140448713/usr-sap /usr/sap/SS1
nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
20201201041441###hana-1###sc-mount-volume.sh: Mounting volume: mount
/usr/sap/SS1.
20201201041441###hana-1###sc-mount-volume.sh:
192.168.175.117:/SS1_shared_Clone_05132205140448713/shared /hana/shared
nfs
rw,vers=3,hard,timeo=600,rsize=1048576,wsize=1048576,intr,noatime,nolock 0
0
20201201041441###hana-1###sc-mount-volume.sh: Mounting volume: mount
/hana/shared.
20201201041441###hana-1###sc-mount-volume.sh: usr-sap-and-shared mounted
successfully.
20201201041441###hana-1###sc-mount-volume.sh: Change ownership to ss1adm.
```

1. Al termine del flusso di lavoro di SnapCenter, i file system /usr/sap/SS1 e /hana/shared vengono montati sull'host di destinazione.

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

1. In SnapCenter, è visibile una nuova risorsa per il volume clonato.



1. Ora che il volume /HANA/condiviso è disponibile, è possibile avviare i servizi SAP HANA.

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

1. I processi SAP host Agent e sapstartsrv sono stati avviati.

```
hana-1:/mnt/sapcc-share/SAP-System-Refresh # ps -ef |grep sap
root 12377 1 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saphostexec
pf=/usr/sap/hostctrl/exe/host_profile
sapadm 12403 1 0 04:34 ? 00:00:00 /usr/lib/systemd/systemd --user
sapadm 12404 12403 0 04:34 ? 00:00:00 (sd-pam)
sapadm 12434 1 1 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/sapstartsrv
pf=/usr/sap/hostctrl/exe/host_profile -D
root 12485 12377 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saphostexec
pf=/usr/sap/hostctrl/exe/host_profile
root 12486 12485 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
ss1adm 12504 1 0 04:34 ? 00:00:00 /usr/sap/SS1/HDB00/exe/sapstartsrv
pf=/usr/sap/SS1/SYS/profile/SS1_HDB00_hana-1 -D -u ss1adm
root 12582 12486 0 04:34 ? 00:00:00 /usr/sap/hostctrl/exe/saposcol -l -w60
pf=/usr/sap/hostctrl/exe/host_profile
root 12585 7613 0 04:34 pts/0 00:00:00 grep --color=auto sap
hana-1:/mnt/sapcc-share/SAP-System-Refresh #
```

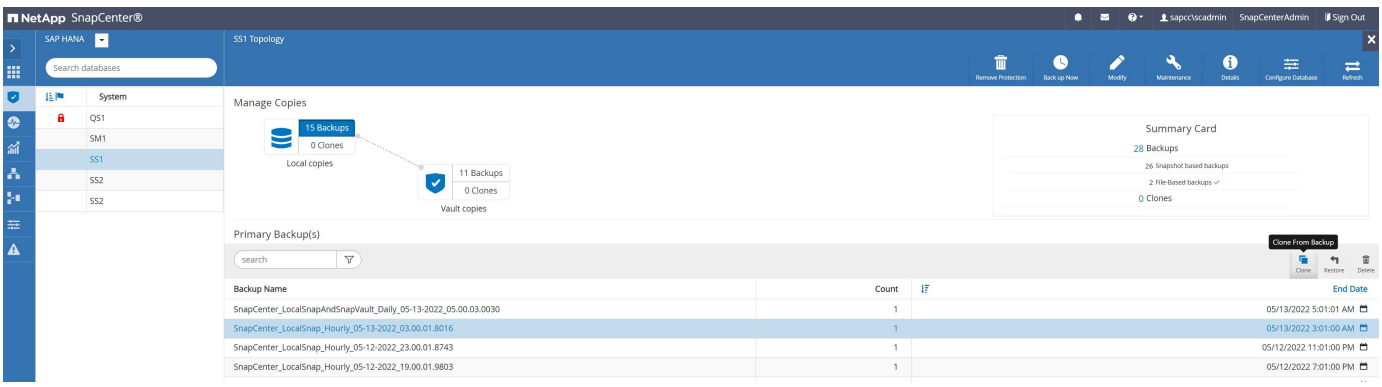
Clonare servizi applicativi SAP aggiuntivi

Vengono clonati altri servizi applicativi SAP nello stesso modo del volume condiviso SAP HANA, come descritto nella sezione "Cloning del volume condiviso SAP HANA". Naturalmente, anche i volumi di storage richiesti dei server applicazioni SAP devono essere protetti con SnapCenter.

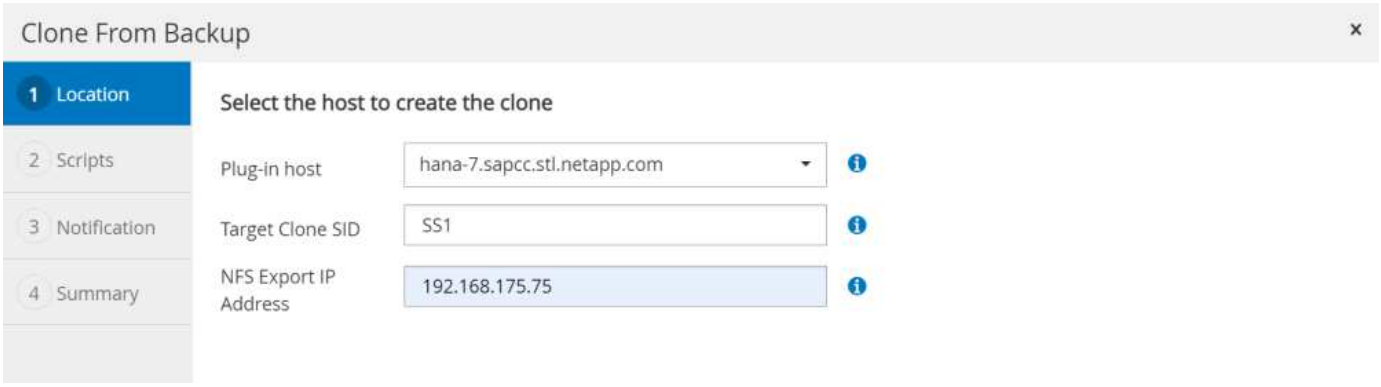
È necessario aggiungere le voci di servizi richieste a /usr/sap/sapServices, e le porte, gli utenti e i punti di montaggio del file system (ad esempio, /usr/sap/SID) devono essere preparati.

Clonazione del volume di dati e ripristino del database HANA

1. Seleziona un backup SAP HANA Snapshot dal sistema di origine SS1.

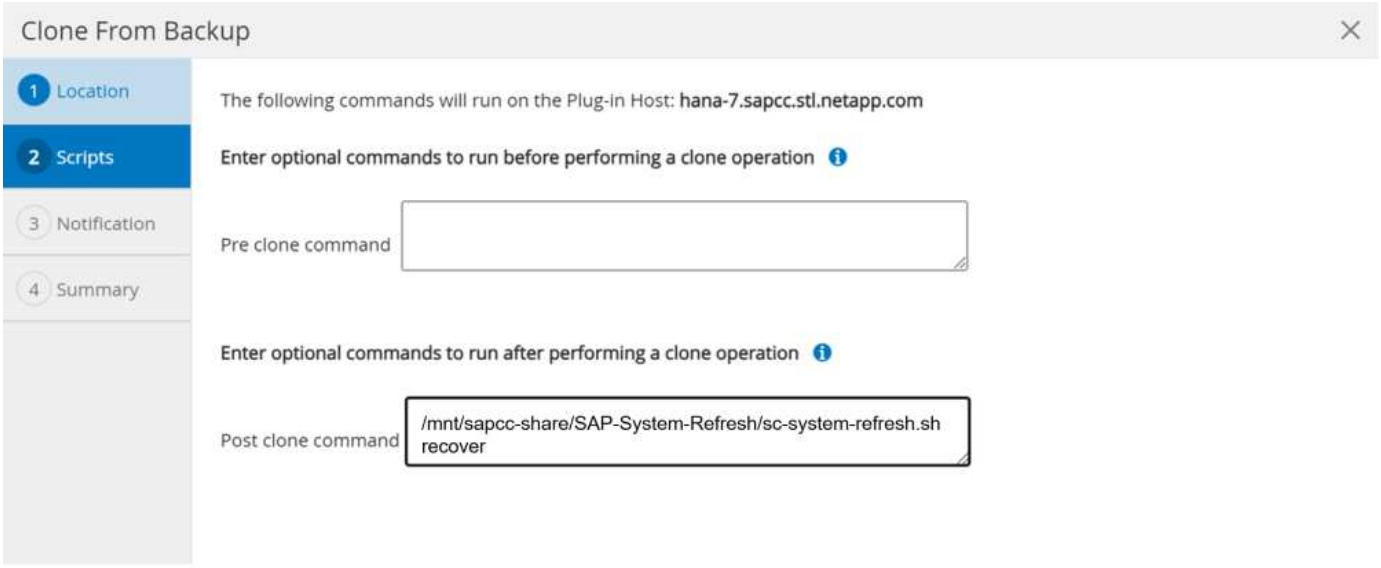


1. Selezionare l'host in cui è stato preparato il sistema di riparazione di destinazione. L'indirizzo IP di esportazione NFS deve essere l'interfaccia di rete dello storage dell'host di destinazione. Come SID di destinazione, mantenere lo stesso SID del sistema di origine. Nel nostro esempio SS1

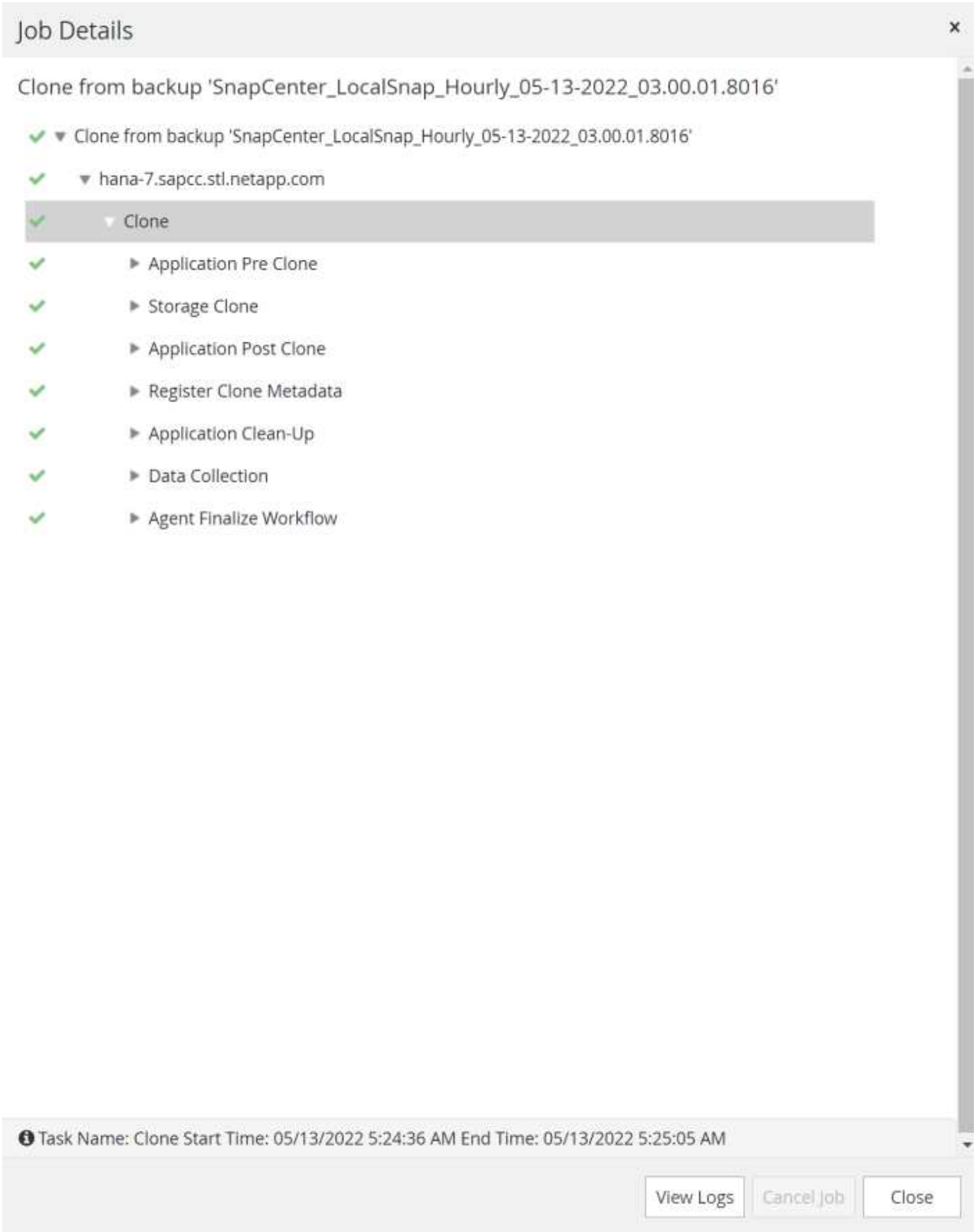


1. Immettere gli script post-clone con le opzioni della riga di comando richieste.

Lo script per l'operazione di recovery recupera il database SAP HANA fino al point-in-time dell'operazione Snapshot e non esegue alcun recovery in avanti. Se è necessario un ripristino in avanti a un determinato momento, il ripristino deve essere eseguito manualmente. Un forward recovery manuale richiede inoltre che i backup del log dal sistema di origine siano disponibili sull'host di destinazione.



La schermata dei dettagli del lavoro in SnapCenter mostra lo stato di avanzamento dell'operazione.



Il file di log dello `sc-system-refresh` script mostra le diverse fasi eseguite per l'operazione di mount e di ripristino.

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

Il sistema SAP HANA è ora disponibile e può essere utilizzato, ad esempio, come sistema di riparazione.

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:

- "Soluzioni per applicazioni aziendali SAP e database SAP HANA (netapp.com)"
- "TR-4614: Backup e ripristino SAP HANA con SnapCenter"
- "TR-4436: SAP HANA su sistemi NetApp All Flash FAS con protocollo Fibre Channel"
- "TR-4435: SAP HANA su sistemi NetApp All Flash FAS con NFS"
- "TR-4926: SAP HANA su Amazon FSX per NetApp ONTAP - Backup e recovery con SnapCenter"
- "TR-4953: Integrazione della gestione del panorama SAP di NetApp con Ansible"
- "TR-4929: Automazione delle operazioni di copia del sistema SAP con libelle SystemCopy (netapp.com)"
- "Automazione di copia, refresh e cloning del sistema SAP dei workflow con ALPACA e NetApp SnapCenter"
- "Automazione di copia, refresh e cloning dei flussi di lavoro del sistema SAP con Avantra e NetApp SnapCenter"

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Febbraio 2018	Release iniziale.
Versione 2.0	Febbraio 2021	Riscrittura completa di SnapCenter 4.3 e script di automazione migliorati. + Nuova descrizione del workflow per il refresh di sistema e le operazioni dei cloni di sistema.
Versione 3.0	Maggio 2022	Adattato al flusso di lavoro modificato con SnapCenter 4,6 P1
Versione 4.0	Luglio 2024	Il documento riguarda i sistemi NetApp on-premise, FSX per ONTAP e Azure NetApp Files + nuove operazioni di SnapCenter 5,0 si montano e sbloccano durante la creazione e l'eliminazione dei cloni + aggiunta di istruzioni specifiche per Fibre Channel SAN + aggiunta di istruzioni specifiche per Azure NetApp Files + script adattato e semplificato `sc-system-refresh` + istruzioni incluse per SAP HANA abilitato crittografia dei volumi

Automazione delle operazioni di copia del sistema SAP con libelle SystemCopy

TR-4929: Automazione delle operazioni di copia del sistema SAP con libelle SystemCopy

Le soluzioni NetApp per l'ottimizzazione della gestione del ciclo di vita SAP sono integrate nei database SAP AnyDB e SAP HANA. Inoltre, NetApp si integra negli strumenti di gestione del ciclo di vita SAP, combinando un'efficiente protezione dei dati integrata con le applicazioni con il provisioning flessibile dei sistemi di test SAP.

Autori:

Holger Zecha, Tobias Brandl, NetApp Franz Diegruber, libelle

Nel dinamico ambiente di business di oggi, le aziende devono fornire innovazione continua e reagire rapidamente ai mercati in continua evoluzione. In queste circostanze competitive, le aziende che implementano una maggiore flessibilità nei propri processi di lavoro possono adattarsi alle esigenze del mercato in modo più efficace.

Le mutevoli esigenze di mercato influiscono anche sugli ambienti SAP di un'azienda, in modo da richiedere integrazioni, modifiche e aggiornamenti regolari. I reparti IT devono implementare queste modifiche con meno risorse e in periodi di tempo più brevi. Ridurre al minimo i rischi durante l'implementazione di tali modifiche richiede test e formazione completi che richiedono sistemi SAP aggiuntivi con dati effettivi provenienti dalla produzione.

Gli approcci tradizionali di gestione del ciclo di vita SAP per il provisioning di questi sistemi si basano principalmente su processi manuali. Questi processi manuali sono spesso soggetti a errori e richiedono molto tempo, ritardando l'innovazione e la risposta ai requisiti di business.

Le soluzioni NetApp per l'ottimizzazione della gestione del ciclo di vita SAP sono integrate nei database SAP AnyDB e SAP HANA. Inoltre, NetApp si integra negli strumenti di gestione del ciclo di vita SAP, combinando un'efficiente protezione dei dati integrata con le applicazioni con il provisioning flessibile dei sistemi di test SAP.

Mentre queste soluzioni NetApp risolvono il problema della gestione efficiente di enormi quantità di dati anche per i database più grandi, le operazioni complete di copia e refresh del sistema SAP end-to-end devono includere attività pre e post-copia per modificare completamente l'identità del sistema SAP di origine nel sistema di destinazione. SAP descrive le attività richieste nel loro "Guida di copia omogenea del sistema SAP". Per ridurre ulteriormente il numero di processi manuali e migliorare la qualità e la stabilità di un processo di copia del sistema SAP, il nostro partner "Libelle" ha sviluppato il "Libelle SystemCopy (LSC)" tool. Abbiamo collaborato con Libelle per integrare le soluzioni NetApp per le copie dei sistemi SAP in LSC da fornire "copie di sistema automatiche end-to-end complete in tempi record".

Operazione di copia Snapshot integrata nell'applicazione

La possibilità di creare copie Snapshot NetApp coerenti con l'applicazione sul layer di storage è la base per le operazioni di copia del sistema e di cloni del sistema descritte in questo documento. Le copie Snapshot basate su storage vengono create con il plug-in NetApp SnapCenter per SAP HANA o SAP qualsiasi DBS su sistemi NetApp ONTAP nativi o utilizzando "Tool Microsoft Azure Application coerente Snapshot" (AzAcSnap) e le interfacce fornite dal database SAP HANA e Oracle in esecuzione in Microsoft Azure. Quando si utilizza SAP HANA, SnapCenter e AzAcSnap registrano le copie Snapshot nel catalogo di backup SAP HANA in modo che i backup possano essere utilizzati per operazioni di ripristino e ripristino e per operazioni di cloning.

Backup off-site e/o replica dei dati di disaster recovery

Le copie Snapshot coerenti con l'applicazione possono essere replicate sul layer di storage in un sito di backup off-site o in un sito di disaster recovery controllato da SnapCenter on-premise. La replica si basa sulle modifiche dei blocchi ed è quindi efficiente in termini di spazio e larghezza di banda. La stessa tecnologia è disponibile per i sistemi SAP HANA e Oracle in esecuzione in Azure con Azure NetApp Files utilizzando la funzione di replica tra regioni (CRR) per replicare in modo efficiente i volumi Azure NetApp Files tra regioni Azure.

Utilizzare qualsiasi copia Snapshot per operazioni di copia o clonazione del sistema SAP

La tecnologia NetApp e l'integrazione del software consentono di utilizzare qualsiasi copia Snapshot di un sistema di origine per un'operazione di copia o clonazione del sistema SAP. Questa copia Snapshot può

essere selezionata dallo stesso storage utilizzato per i sistemi di produzione SAP, dallo storage utilizzato per i backup off-site (come il backup Azure NetApp Files in Azure) o dallo storage nel sito di disaster recovery (volumi di destinazione CRR Azure NetApp Files). Questa flessibilità consente di separare i sistemi di sviluppo e test dalla produzione, se necessario, e copre altri scenari, come il test del disaster recovery nel sito di disaster recovery.

Automazione con integrazione

Esistono diversi scenari e casi di utilizzo per il provisioning dei sistemi di test SAP, oltre a requisiti diversi per il livello di automazione. I prodotti software NetApp per SAP si integrano nei prodotti di gestione del ciclo di vita e dei database di SAP e di altri vendor di terze parti (ad esempio, libelle) per supportare diversi scenari e livelli di automazione.

NetApp SnapCenter con il plug-in per SAP HANA e SAP AnyDB o AzAcSnap su Azure viene utilizzato per eseguire il provisioning dei cloni di volumi di storage richiesti in base a una copia Snapshot coerente con l'applicazione e per eseguire tutte le operazioni di host e database necessarie fino a un database SAP avviato. A seconda del caso d'utilizzo, potrebbero essere necessarie la copia del sistema SAP, la clonazione del sistema, il refresh del sistema o ulteriori operazioni manuali, come la post-elaborazione SAP. Ulteriori dettagli sono illustrati nella sezione successiva.

È possibile eseguire un provisioning end-to-end completamente automatizzato o un refresh dei sistemi di test SAP utilizzando l'automazione Libelle SystemCopy (LSC). L'integrazione di SnapCenter o AzAcSnap in LSC è descritta più dettagliatamente in questo documento.

Libelle SystemCopy

Libelle SystemCopy è una soluzione software basata su framework per creare copie di sistema e orizzontale completamente automatizzate. Con il tocco proverbiale di un pulsante, i sistemi di QA e test possono essere aggiornati con nuovi dati di produzione. Libelle SystemCopy supporta tutti i database e i sistemi operativi convenzionali, fornisce i propri meccanismi di copia per tutte le piattaforme ma, allo stesso tempo, integra procedure di backup/ripristino o tool di storage come le copie Snapshot di NetApp e i volumi FlexClone di NetApp. Le attività necessarie durante una copia del sistema sono controllate dall'esterno dello stack SAP ABAP. In questo modo, non sono richiesti trasporti o altre modifiche nelle applicazioni SAP. In genere, tutti i passaggi necessari per completare correttamente una procedura di copia del sistema possono essere suddivisi in quattro fasi:

- **Fase di controllo.** controllare gli ambienti di sistema interessati.
- **Fase preliminare.** preparare il sistema di destinazione per una copia del sistema.
- **Copy phase.** fornire una copia del database di produzione effettivo nel sistema di destinazione dall'origine.
- **Fase post.** tutte le attività successive alla copia per completare la procedura di copia omogenea del sistema e fornire un sistema di destinazione aggiornato.

Durante la fase di copia, le funzionalità NetApp Snapshot e FlexClone vengono utilizzate per ridurre al minimo il tempo necessario a un paio di minuti anche per i database più grandi.

Per le fasi Check, Pre e Post, LSC include oltre 450 attività preconfigurate che coprono il 95% delle tipiche operazioni di refresh. Di conseguenza, LSC adotta l'automazione seguendo gli standard SAP. Grazie alla natura software-defined di LSC, i processi di refresh del sistema possono essere facilmente modificati e migliorati per soddisfare le esigenze specifiche degli ambienti SAP dei clienti.

Casi d'utilizzo per il refresh e la clonazione del sistema SAP

Esistono diversi scenari in cui i dati di un sistema di origine devono essere resi disponibili a un sistema di

destinazione:

- Aggiornamento regolare dei sistemi di quality assurance e test e training
- Creazione di ambienti di sistema di riparazione o riparazione per risolvere il danneggiamento logico
- Scenari di test per il disaster recovery

Sebbene i sistemi di riparazione e i sistemi di test per il disaster recovery siano generalmente forniti utilizzando cloni di sistema SAP (che non richiedono operazioni di post-elaborazione estese) per sistemi di test e training aggiornati, queste fasi di post-elaborazione devono essere applicate per consentire la coesistenza con il sistema di origine. Pertanto, questo documento si concentra sugli scenari di refresh del sistema SAP. Ulteriori dettagli sui diversi casi di utilizzo sono disponibili nel report tecnico "TR-4667: Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter".

Il resto di questo documento è suddiviso in due parti. La prima parte descrive l'integrazione di NetApp SnapCenter con i sistemi libelle SystemCopy per SAP HANA e SAP AnyDB in esecuzione su sistemi NetApp ONTAP on-premise. La seconda parte descrive l'integrazione di AzAcSnap con LSC per sistemi SAP HANA in esecuzione in Microsoft Azure con Azure NetApp Files fornito. Sebbene la tecnologia ONTAP sottostante sia identica, Azure NetApp Files fornisce interfacce e strumenti diversi (ad esempio, AzAcSnap) rispetto all'installazione ONTAP nativa.

Aggiornamento del sistema SAP HANA con LSC e SnapCenter

Questa sezione descrive come integrare LSC con NetApp SnapCenter. L'integrazione tra LSC e SnapCenter supporta tutti i database supportati da SAP. Tuttavia, dobbiamo differenziarci tra SAP AnyDB e SAP HANA perché SAP HANA fornisce un host centrale per le comunicazioni che non è disponibile per SAP AnyDB.

L'installazione predefinita dell'agente SnapCenter e del plug-in del database per gli AnyDB SAP è un'installazione locale dell'agente SnapCenter oltre al plug-in del database corrispondente per il server database.

In questa sezione, l'integrazione tra LSC e SnapCenter viene descritta utilizzando un database SAP HANA come esempio. Come indicato in precedenza per SAP HANA, sono disponibili due diverse opzioni per l'installazione dell'agente SnapCenter e del plug-in del database SAP HANA:

- **Un agente SnapCenter standard e un'installazione del plug-in SAP HANA.** in un'installazione standard, l'agente SnapCenter e il plug-in SAP HANA vengono installati localmente sul server di database SAP HANA.
- **Un'installazione di SnapCenter con un host centrale di comunicazione.** Un host centrale di comunicazione viene installato con l'agente SnapCenter, il plug-in SAP HANA e il client di database HANA che gestisce tutte le operazioni relative al database necessarie per eseguire il backup e il ripristino di un database SAP HANA per diversi sistemi SAP HANA nell'ambiente. Pertanto, un host di comunicazione centrale non deve avere un sistema di database SAP HANA completo installato.

Per ulteriori informazioni su questi diversi agenti SnapCenter e sulle opzioni di installazione dei plug-in del database SAP HANA, vedere il report tecnico "TR-4614: Backup e recovery SAP HANA con SnapCenter".

Le sezioni seguenti evidenziano le differenze tra l'integrazione di LSC con SnapCenter mediante l'installazione standard o l'host centrale di comunicazione. In particolare, tutte le fasi di configurazione non evidenziate sono le stesse indipendentemente dall'opzione di installazione e dal database utilizzato.

Per eseguire un backup automatizzato basato sulla copia di Snapshot dal database di origine e creare un clone per il nuovo database di destinazione, l'integrazione descritta tra LSC e SnapCenter utilizza le opzioni di

configurazione e gli script descritti in "TR-4667: Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter".

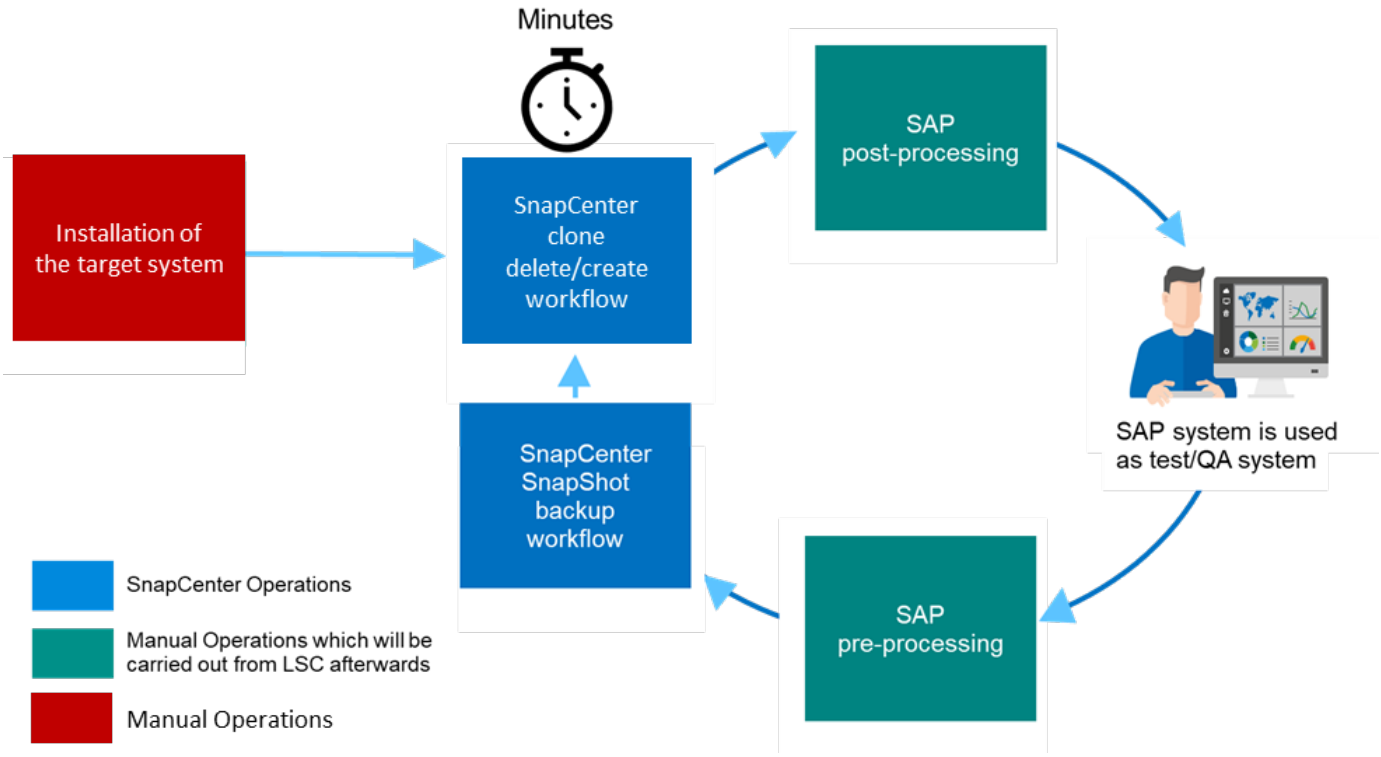
Panoramica

La figura seguente mostra un tipico workflow di alto livello per un ciclo di vita di refresh del sistema SAP con SnapCenter senza LSC:

1. Installazione e preparazione del sistema di destinazione una tantum.
2. Pre-elaborazione manuale (esportazione di licenze, utenti, stampanti e così via).
3. Se necessario, l'eliminazione di un clone già esistente sul sistema di destinazione.
4. La clonazione di una copia Snapshot esistente del sistema di origine nel sistema di destinazione eseguita da SnapCenter.
5. Operazioni di post-elaborazione SAP manuali (importazione di licenze, utenti, stampanti, disattivazione dei processi batch e così via).
6. Il sistema può quindi essere utilizzato come sistema di test o QA.
7. Quando viene richiesto un nuovo aggiornamento del sistema, il flusso di lavoro viene riavviato alla fase 2.

I clienti SAP sanno che i passaggi manuali colorati in verde nella figura seguente sono lunghi e soggetti a errori. Quando si utilizza l'integrazione di LSC e SnapCenter, questi passaggi manuali vengono eseguiti con LSC in modo affidabile e ripetibile con tutti i registri necessari per gli audit interni ed esterni.

La figura seguente fornisce una panoramica della procedura generale di aggiornamento del sistema SAP basata su SnapCenter.



Prerequisiti e limitazioni

Devono essere soddisfatti i seguenti prerequisiti:

- SnapCenter deve essere installato. Il sistema di origine e di destinazione deve essere configurato in SnapCenter, in un'installazione standard o utilizzando un host di comunicazione centrale. Le copie Snapshot possono essere create sul sistema di origine.
- Il backend dello storage deve essere configurato correttamente in SnapCenter, come mostrato nell'immagine seguente.

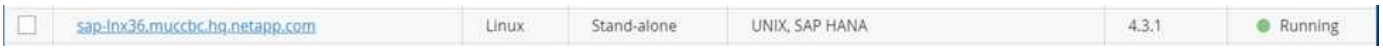


Le due immagini successive riguardano l'installazione standard in cui l'agente SnapCenter e il plug-in SAP HANA sono installati localmente su ciascun server di database.

L'agente SnapCenter e il plug-in del database appropriato devono essere installati nel database di origine.



L'agente SnapCenter e il plug-in del database appropriato devono essere installati nel database di destinazione.

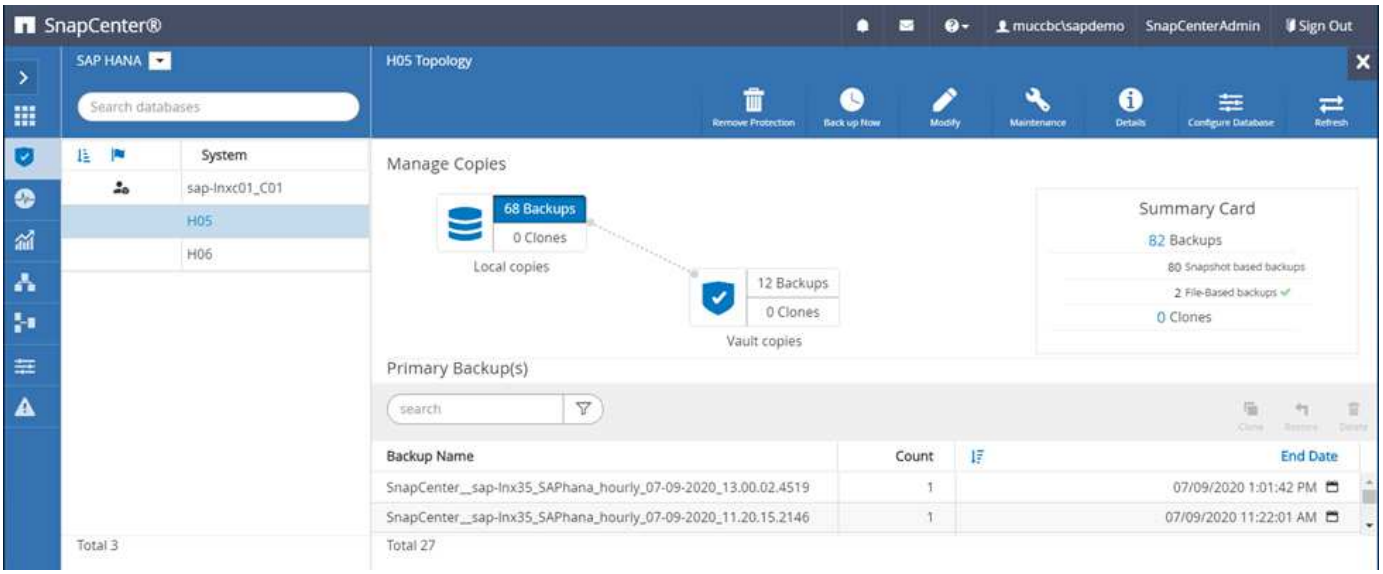


La seguente immagine descrive l'implementazione centrale degli host di comunicazione in cui l'agente SnapCenter, il plug-in SAP HANA e il client di database SAP HANA sono installati su un server centralizzato (come il server SnapCenter) per gestire diversi sistemi SAP HANA nell'ambiente.

L'agente SnapCenter, il plug-in del database SAP HANA e il client del database HANA devono essere installati sull'host centrale di comunicazione.



Il backup per il database di origine deve essere configurato correttamente in SnapCenter in modo che la copia Snapshot possa essere creata correttamente.



Il master LSC e il worker LSC devono essere installati nell'ambiente SAP. In questa implementazione, abbiamo anche installato il master LSC sul server SnapCenter e il worker LSC sul server di database SAP di destinazione, che deve essere aggiornato. Ulteriori informazioni sono descritte nella sezione seguente "Setup di laboratorio."

Risorse di documentazione:

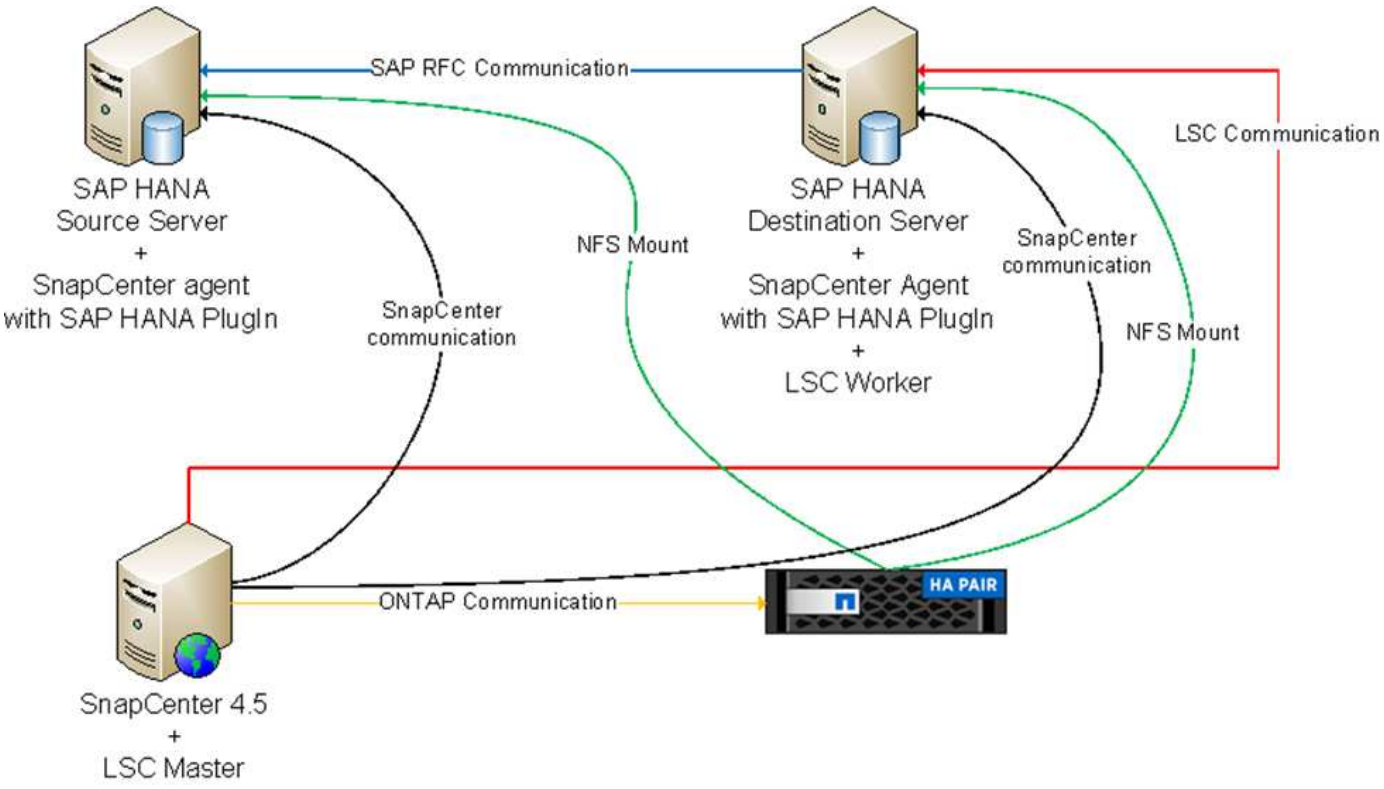
- "Centro di documentazione SnapCenter"
- "TR-4700: Plug-in SnapCenter per database Oracle"
- "TR-4614: Backup e ripristino SAP HANA con SnapCenter"
- "TR-4667: Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter"
- "TR-4769 - Best practice SnapCenter e linee guida per il dimensionamento"
- "Guida di riferimento ai cmdlet di SnapCenter 4.6"

Setup di laboratorio

Questa sezione descrive un'architettura di esempio che è stata configurata in un data center dimostrativo. L'installazione è stata divisa in un'installazione standard e in un'installazione che utilizza un host di comunicazione centrale.

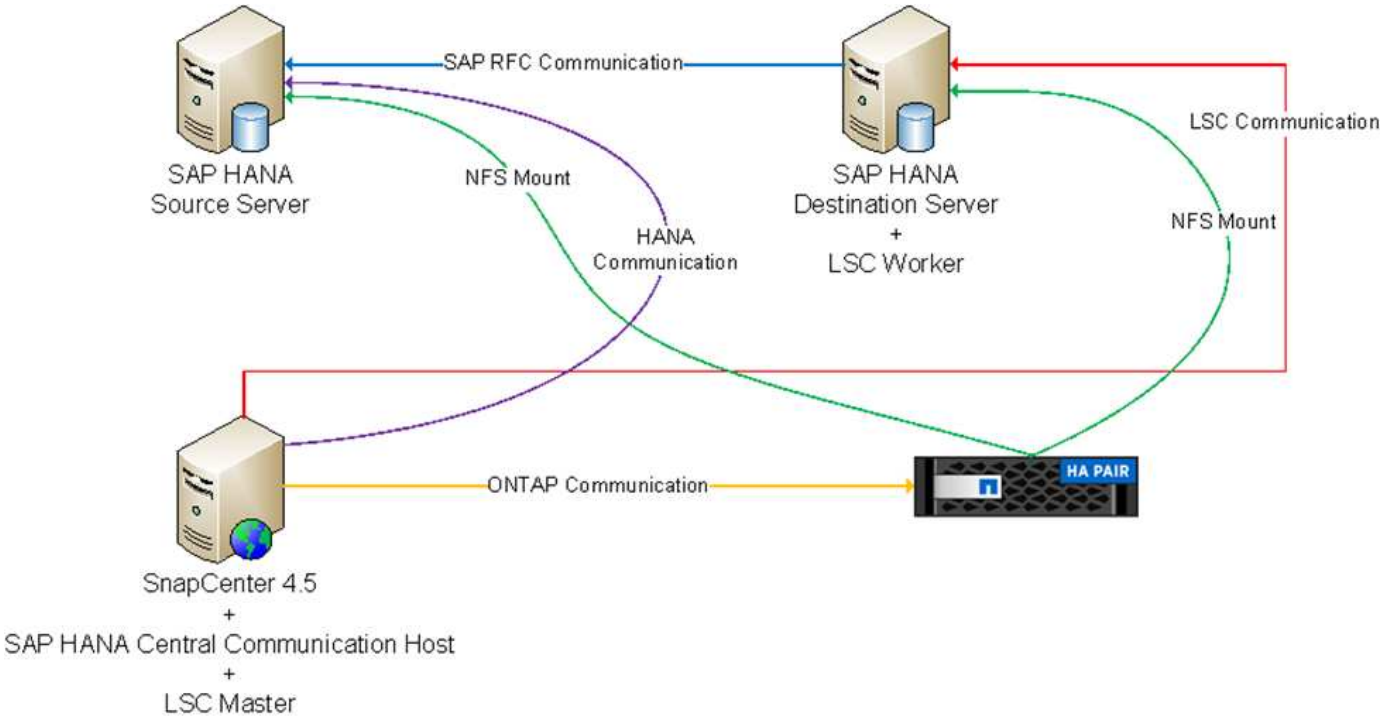
Installazione standard

La figura seguente mostra un'installazione standard in cui l'agente SnapCenter e il plug-in del database sono stati installati localmente sul server del database di origine e di destinazione. Nella configurazione di laboratorio, abbiamo installato il plug-in SAP HANA. Inoltre, il worker LSC è stato installato anche sul server di destinazione. Per semplificare e ridurre il numero di server virtuali, abbiamo installato il master LSC sul server SnapCenter. La comunicazione tra i diversi componenti è illustrata nella figura seguente.



Host centrale di comunicazione

La figura seguente mostra la configurazione mediante un host di comunicazione centrale. In questa configurazione, l'agente SnapCenter, il plug-in SAP HANA e il client del database HANA sono stati installati su un server dedicato. In questa configurazione, abbiamo utilizzato il server SnapCenter per installare l'host centrale per le comunicazioni. Inoltre, il worker LSC è stato nuovamente installato sul server di destinazione. Per semplificare e ridurre il numero di server virtuali, abbiamo deciso di installare anche il master LSC sul server SnapCenter. La comunicazione tra i diversi componenti è illustrata nella figura seguente.



Fasi iniziali di preparazione una tantum per libelle SystemCopy

Esistono tre componenti principali di un'installazione LSC:

- **LSC master.** come suggerisce il nome, questo è il componente master che controlla il flusso di lavoro automatico di una copia di sistema basata su libelle. Nell'ambiente demo, il master LSC è stato installato sul server SnapCenter.
- **LSC Worker.** un LSC Worker è la parte del software Libelle che in genere viene eseguito sul sistema SAP di destinazione ed esegue gli script richiesti per la copia automatica del sistema. Nell'ambiente demo, il worker LSC è stato installato sul server applicativo SAP HANA di destinazione.
- **Satellite LSC.** un satellite LSC fa parte del software libelle che viene eseguito su un sistema di terze parti su cui devono essere eseguiti ulteriori script. Il master LSC può anche svolgere il ruolo di sistema satellitare LSC allo stesso tempo.

Per prima cosa abbiamo definito tutti i sistemi coinvolti all'interno di LSC, come mostrato nella seguente immagine:

- **172.30.15.35.** Indirizzo IP del sistema di origine SAP e del sistema di origine SAP HANA.
- **172.30.15.3.** Indirizzo IP del master LSC e del sistema satellitare LSC per questa configurazione. Poiché è stato installato il master LSC sul server SnapCenter, i cmdlet PowerShell di SnapCenter 4.x sono già disponibili su questo host Windows perché sono stati installati durante l'installazione del server SnapCenter. Abbiamo quindi deciso di abilitare il ruolo satellite LSC per questo sistema ed eseguire tutti i cmdlet PowerShell di SnapCenter su questo host. Se si utilizza un sistema diverso, assicurarsi di installare i cmdlet PowerShell di SnapCenter su questo host in base alla documentazione di SnapCenter.
- **172.30.15.36.** l'indirizzo IP del sistema di destinazione SAP, del sistema di destinazione SAP HANA e dell'operatore LSC.

Invece di indirizzi IP, è possibile utilizzare anche nomi host o nomi di dominio completi.

La seguente immagine mostra la configurazione LSC di master, worker, satellite, origine SAP, destinazione SAP, database di origine e database di destinazione.

System Identifier	Worker	Source SAP	Source Database	Target SAP	Target Database	Satellite System
172.30.15.35		☑	☑	☐	☐	☐
172.30.15.3	172.30.15.3:9000	☐	☐	☐	☐	☑
172.30.15.36	172.30.15.36:9000	☐	☐	☑	☑	☐

Per l'integrazione principale, è necessario separare nuovamente le fasi di configurazione nell'installazione standard e nell'installazione utilizzando un host di comunicazione centrale.

Installazione standard

In questa sezione vengono descritte le procedure di configurazione necessarie quando si utilizza un'installazione standard in cui l'agente SnapCenter e il plug-in del database necessari sono installati sui sistemi di origine e di destinazione. Quando si utilizza un'installazione standard, tutte le attività necessarie per montare il volume clone e ripristinare e ripristinare il sistema di destinazione vengono eseguite dall'agente SnapCenter in esecuzione sul sistema di database di destinazione sul server stesso. In questo modo è possibile accedere a tutti i dettagli relativi ai cloni disponibili tramite le variabili ambientali dell'agente SnapCenter. Pertanto, nella fase di copia LSC è necessario creare un'unica attività aggiuntiva. Questa attività esegue il processo di copia Snapshot sul sistema di database di origine e il processo di clonazione e ripristino e ripristino sul sistema di database di destinazione. Tutte le attività correlate a SnapCenter vengono attivate utilizzando uno script PowerShell inserito nell'attività LSC `NTAP_SYSTEM_CLONE`.

L’immagine seguente mostra la configurazione dell’attività LSC nella fase di copia.

	copy	Copy Phase		phase
	copy 1	NTAP_SYSTEM_CLONE	NetApp SnapShot and Clone	psh
	copy 2	NTAP_SYSTEM_CLONE_CP	NetApp SnapShot and Clone	psh
	copy 3	NTAP_MNT_RECOVER_CP	Mount Volume and Recover HANA Database	cmd
	copy 4	LPDBBCKP	Backup Source DB in Filesystem	lsh
	copy 5	LPDBCPYFLS	Copy DB Backup Files From Source to Target System	lsh
	copy 6	LTDBRESTORE	Restore DB Files	lsh
	copy 7	LTDBRESTORE_TENANT	Restore DB Files for Tenant Database	lsh
	post	Post Phase		phase

La seguente immagine evidenzia la configurazione di `NTAP_SYSTEM_CLONE` processo. Poiché si sta eseguendo uno script PowerShell, questo script di Windows PowerShell viene eseguito sul sistema satellitare. In questo caso, si tratta del server SnapCenter con il master LSC installato che funge anche da sistema satellitare.

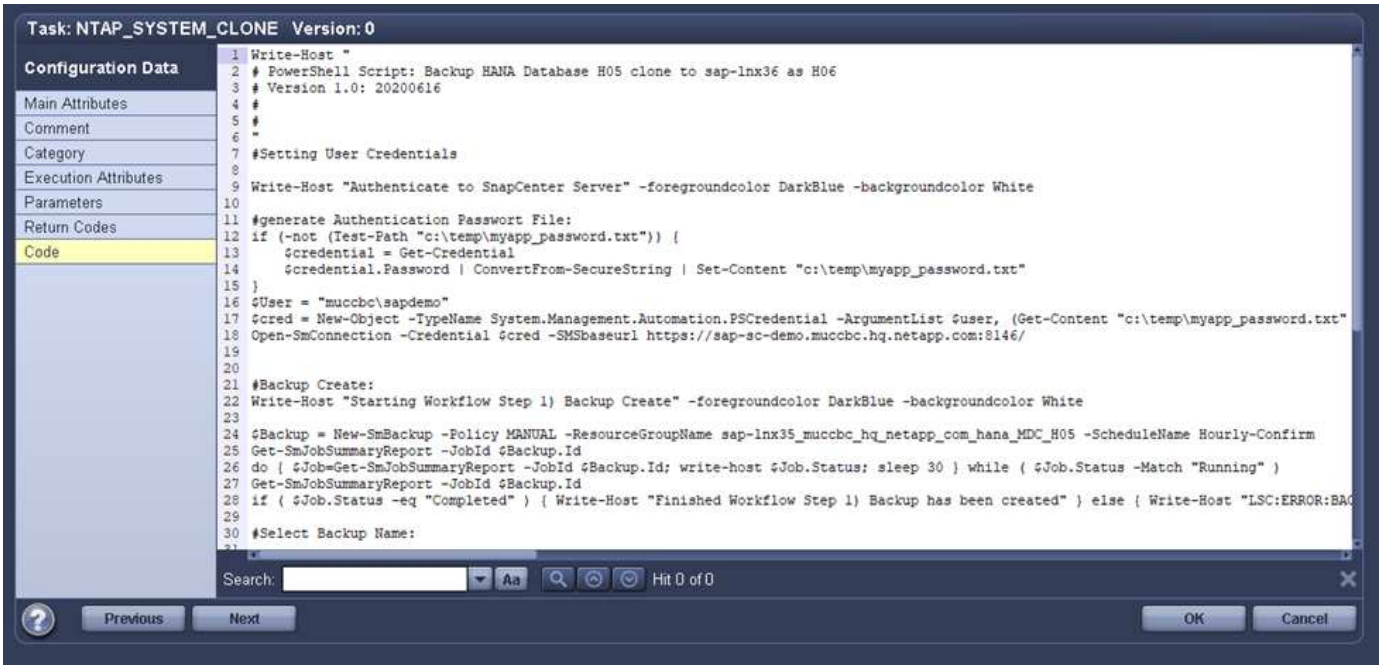


Poiché l’LSC deve essere consapevole dell’esito positivo delle operazioni di copia, clonazione e ripristino di Snapshot, è necessario definire almeno due tipi di codice di ritorno. Un codice serve per eseguire correttamente lo script, mentre l’altro per eseguire lo script in modo non riuscito, come illustrato nell’immagine seguente.

- `LSC:OK` deve essere scritto dallo script in standard out se l’esecuzione ha avuto esito positivo.
- `LSC:ERROR` deve essere scritto dallo script in standard out se l’esecuzione non è riuscita.



L'immagine seguente mostra parte dello script PowerShell che deve essere eseguito per eseguire un backup basato su Snapshot sul sistema di database di origine e un clone sul sistema di database di destinazione. Lo script non deve essere completo. Piuttosto, lo script mostra l'aspetto dell'integrazione tra LSC e SnapCenter e la facilità di configurazione.



Poiché lo script viene eseguito sul master LSC (che è anche un sistema satellite), il master LSC sul server SnapCenter deve essere eseguito come utente Windows che dispone delle autorizzazioni appropriate per eseguire operazioni di backup e clonazione in SnapCenter. Per verificare se l'utente dispone delle autorizzazioni appropriate, deve essere in grado di eseguire una copia Snapshot e un clone nell'interfaccia utente di SnapCenter.

Non è necessario eseguire il master LSC e il satellite LSC sul server SnapCenter stesso. Il master LSC e il satellite LSC possono essere eseguiti su qualsiasi macchina Windows. Il prerequisito per l'esecuzione dello script PowerShell sul satellite LSC è che i cmdlet PowerShell di SnapCenter siano stati installati sul server Windows.

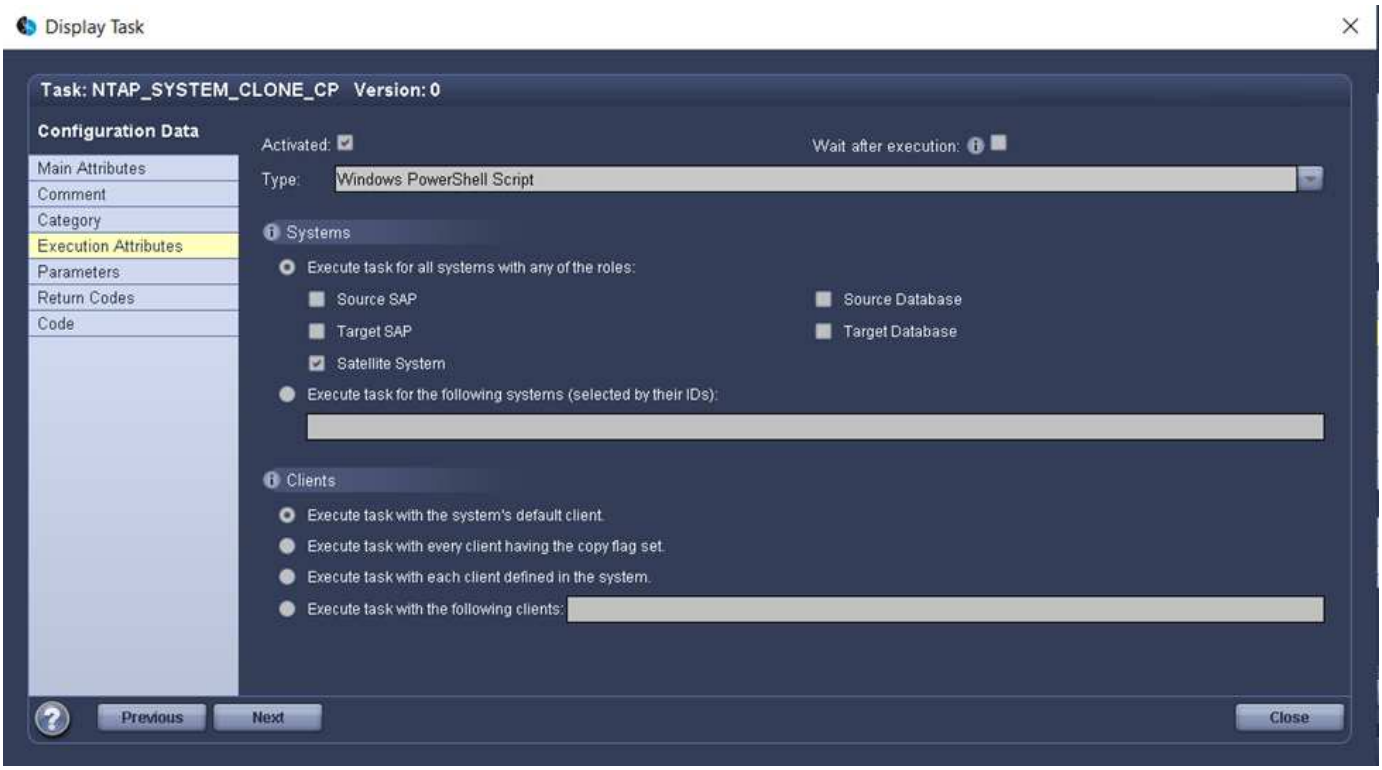
Host centrale di comunicazione

Per l'integrazione tra LSC e SnapCenter utilizzando un host di comunicazione centrale, le uniche modifiche da eseguire vengono eseguite nella fase di copia. La copia Snapshot e il clone vengono creati utilizzando l'agente SnapCenter sull'host di comunicazione centrale. Pertanto, tutti i dettagli sui volumi appena creati sono disponibili solo sull'host centrale di comunicazione e non sul server del database di destinazione. Tuttavia, questi dettagli sono necessari sul server di database di destinazione per montare il volume clone ed eseguire il ripristino. Questo è il motivo per cui sono necessarie due attività aggiuntive nella fase di copia. Un'attività viene eseguita sull'host centrale di comunicazione e un'attività viene eseguita sul server del database di destinazione. Queste due attività sono mostrate nell'immagine seguente.

- **NTAP_SYSTEM_CLONE_CP.** questa attività crea la copia Snapshot e il clone utilizzando uno script PowerShell che esegue le necessarie funzioni SnapCenter sull'host centrale di comunicazione. Questa attività viene quindi eseguita sul satellite LSC, che nella nostra istanza è il master LSC eseguito su Windows. Questo script raccoglie tutti i dettagli relativi al clone e ai volumi appena creati e lo passa alla seconda attività `NTAP_MNT_RECOVER_CP`, Che viene eseguito sul worker LSC in esecuzione sul server del database di destinazione.
- **NTAP_MNT_RECOVER_CP.** questa attività arresta il sistema SAP di destinazione e il database SAP HANA, smonta i vecchi volumi e monta i volumi dei cloni di storage appena creati in base ai parametri passati dall'attività precedente `NTAP_SYSTEM_CLONE_CP`. Il database SAP HANA di destinazione viene quindi ripristinato e ripristinato.

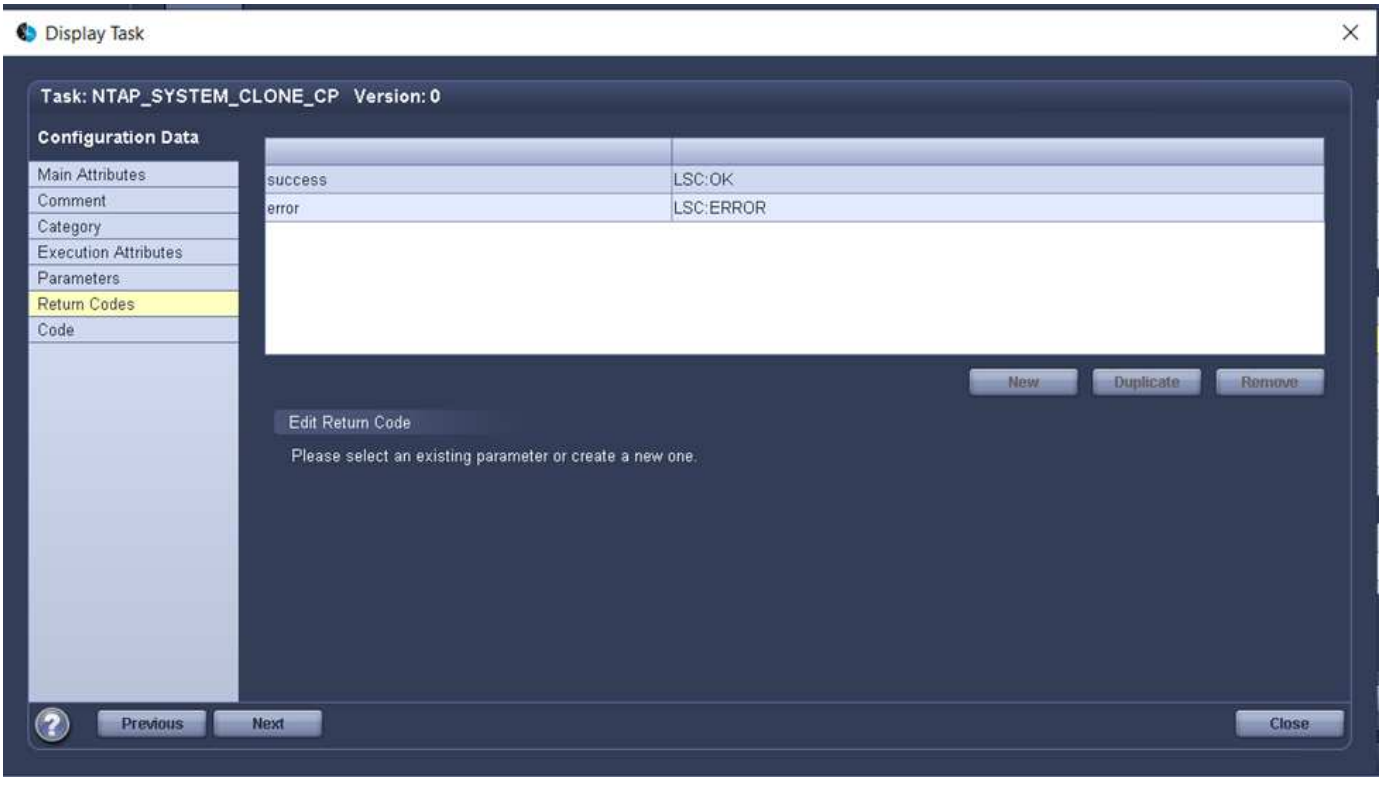
	copy	Copy Phase		phase
	copy 1	*NTAP_SYSTEM_CLONE*	*NetApp SnapShot and Clone*	*psh*
	copy 2	NTAP_SYSTEM_CLONE_CP	NetApp SnapShot and Clone	psh
	copy 3	NTAP_MNT_RECOVER_CP	Mount Volume and Recover HANA Database	cmd
	copy 4	*LPDBBCKP*	*Backup Source DB in Filesystem*	*lsh*
	copy 5	*LPDBCPYFLS*	*Copy DB Backup Files From Source to Target System*	*lsh*
	copy 6	*LTDBRESTORE*	*Restore DB Files*	*lsh*
	copy 7	*LTDBRESTORE_TENANT*	*Restore DB Files for Tenant Database*	*lsh*
	post	Post Phase		phase

La seguente immagine evidenzia la configurazione dell'attività `NTAP_SYSTEM_CLONE_CP`. Si tratta dello script di Windows PowerShell eseguito sul sistema satellitare. In questo caso, il sistema satellitare è il server SnapCenter con il master LSC installato.

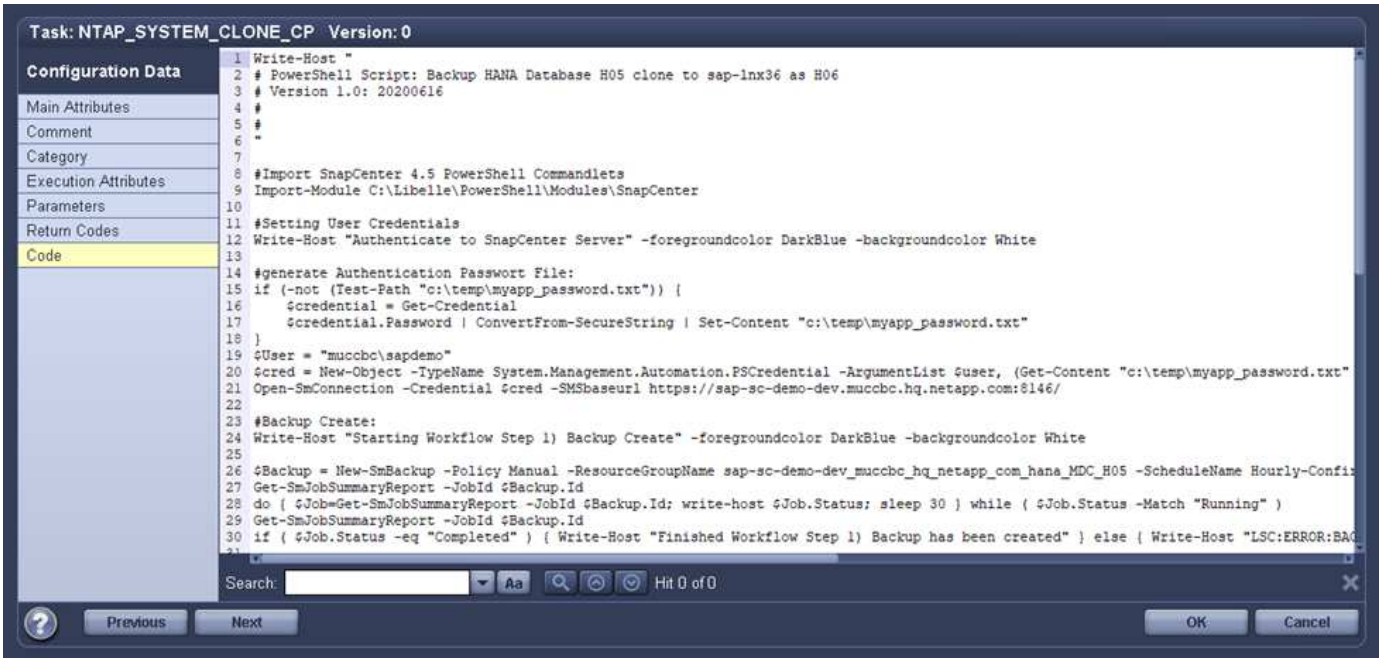


Poiché LSC deve essere consapevole dell'esito positivo dell'operazione di copia e clonazione Snapshot, è necessario definire almeno due tipi di codice di ritorno: Un codice di ritorno per l'esecuzione corretta dello script e l'altro per l'esecuzione non riuscita dello script, come illustrato nell'immagine seguente.

- `LSC:OK` deve essere scritto dallo script in standard out se l'esecuzione ha avuto esito positivo.
- `LSC:ERROR` deve essere scritto dallo script in standard out se l'esecuzione non è riuscita.



L'immagine seguente mostra parte dello script PowerShell che deve essere eseguito per eseguire una copia Snapshot e un clone utilizzando l'agente SnapCenter sull'host di comunicazione centrale. Lo script non deve essere completo. Lo script viene invece utilizzato per mostrare l'aspetto dell'integrazione tra LSC e SnapCenter e la facilità di configurazione.

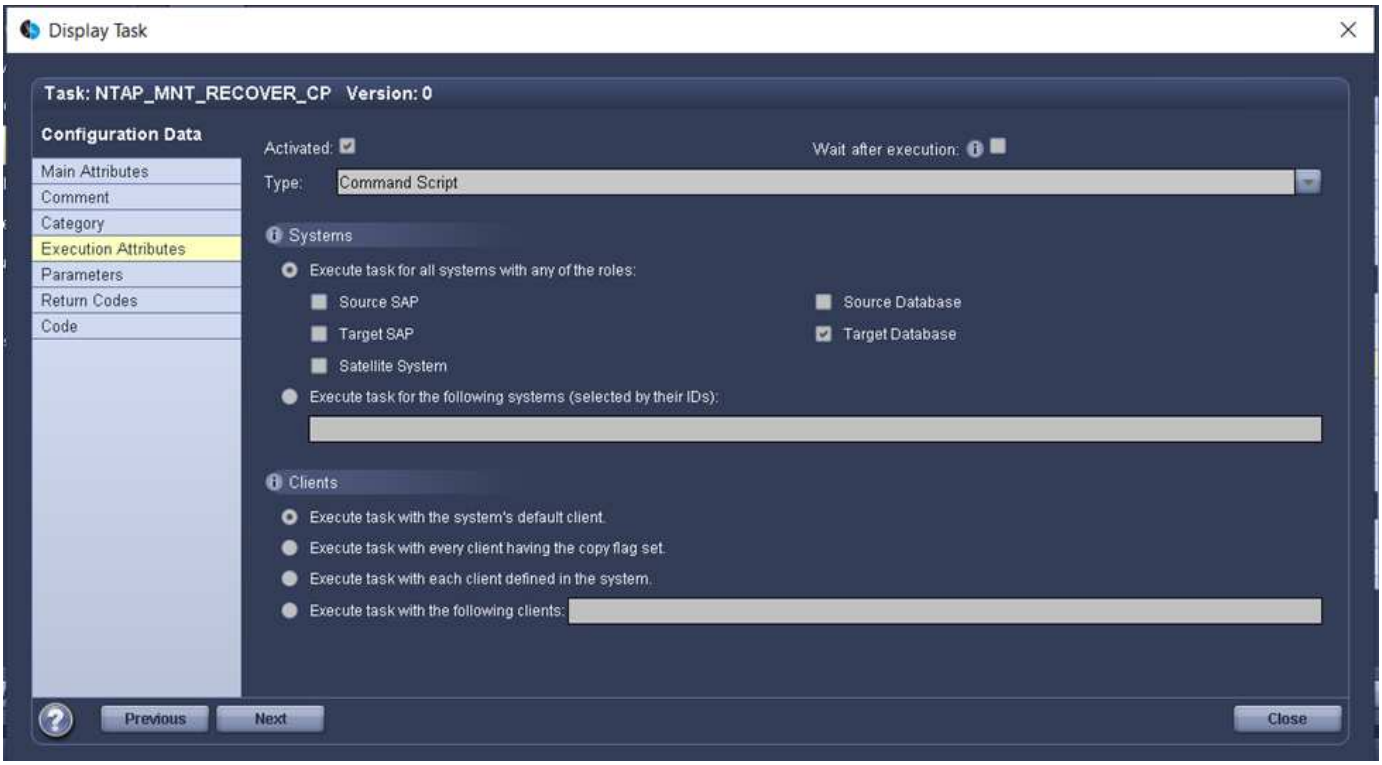


Come indicato in precedenza, è necessario consegnare il nome del volume clone all'attività successiva `NTAP_MNT_RECOVER_CP` per montare il volume clone sul server di destinazione. Il nome del volume clone, noto anche come percorso di giunzione, viene memorizzato nella variabile `$JunctionPath`. Il trasferimento a un'attività LSC successiva viene ottenuto attraverso una variabile LSC personalizzata.

```
echo $JunctionPath > $_task(current, custompath1)_$
```

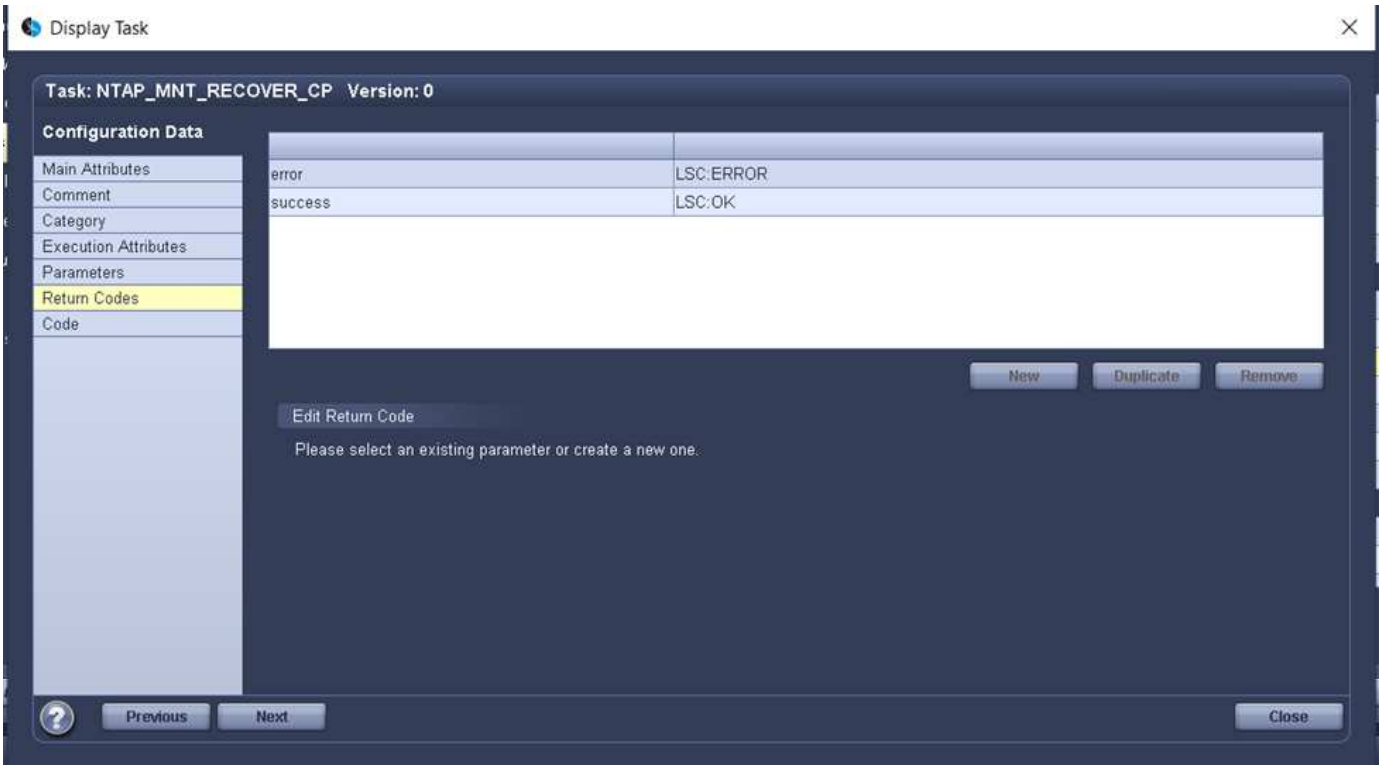
Poiché lo script viene eseguito sul master LSC (che è anche un sistema satellite), il master LSC sul server SnapCenter deve essere eseguito come utente Windows che dispone delle autorizzazioni appropriate per eseguire le operazioni di backup e clonazione in SnapCenter. Per verificare se dispone delle autorizzazioni appropriate, l'utente deve essere in grado di eseguire una copia Snapshot e un clone nella GUI di SnapCenter.

La figura seguente evidenzia la configurazione dell'attività `NTAP_MNT_RECOVER_CP`. Poiché si desidera eseguire uno script Linux Shell, si tratta di uno script di comando eseguito sul sistema di database di destinazione.



Poiché LSC deve essere consapevole del montaggio dei volumi clone e dell'esito positivo del ripristino e del ripristino del database di destinazione, è necessario definire almeno due tipi di codice di ritorno. Un codice serve per eseguire correttamente lo script e uno per eseguire lo script in modo non riuscito, come illustrato nella figura seguente.

- `LSC:OK` deve essere scritto dallo script in standard out se l'esecuzione ha avuto esito positivo.
- `LSC:ERROR` deve essere scritto dallo script in standard out se l'esecuzione non è riuscita.

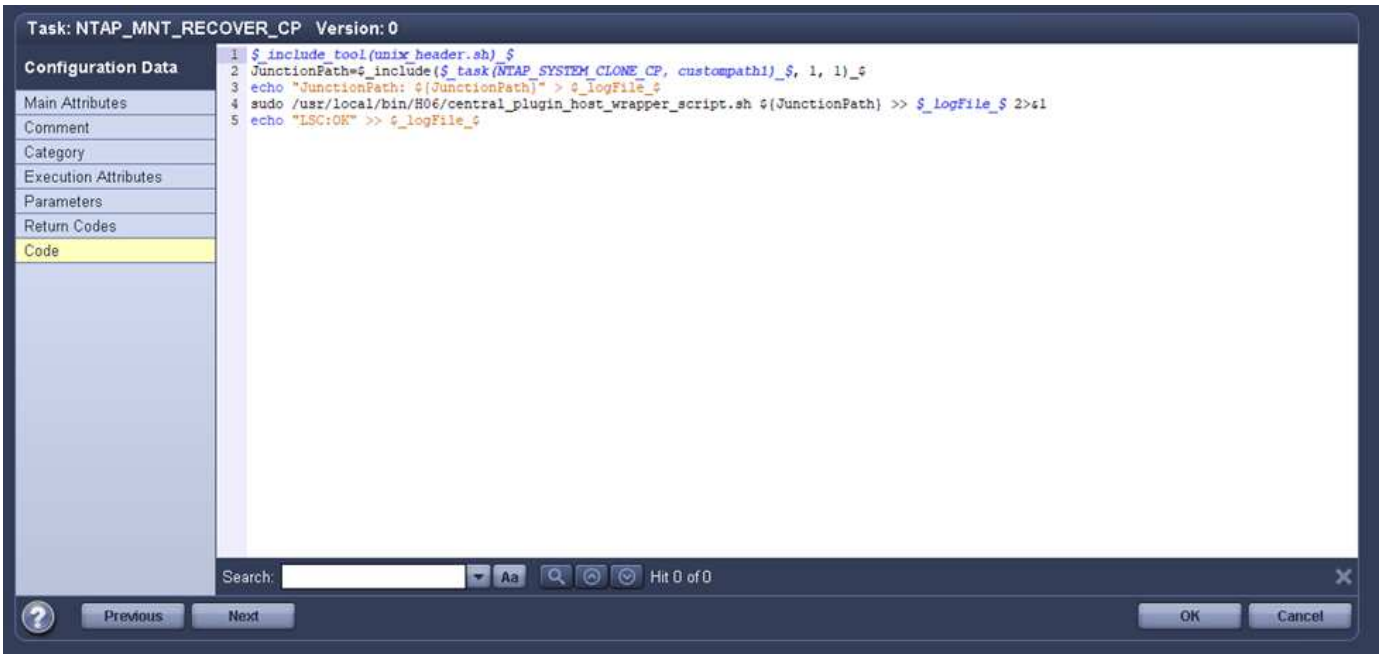


La figura seguente mostra parte dello script della shell Linux utilizzato per arrestare il database di destinazione, smontare il vecchio volume, montare il volume clone e ripristinare e ripristinare il database di destinazione. Nell'attività precedente, il percorso di giunzione è stato scritto in una variabile LSC. Il comando seguente legge questa variabile LSC e memorizza il valore in `$JunctionPath` Variabile dello script della shell Linux.

```
JunctionPath=$_include($_task(NTAP_SYSTEM_CLONE_CP, custompath1)_$, 1,
1)_$
```

L'operatore LSC sul sistema di destinazione viene eseguito come `<sidaadm>`, ma i comandi mount devono essere eseguiti come utente root. Per questo motivo è necessario creare `central_plugin_host_wrapper_script.sh`. Lo script `central_plugin_host_wrapper_script.sh` viene chiamato dall'attività `NTAP_MNT_RECOVERY_CP` utilizzando il `sudo` comando. Utilizzando il `sudo` Lo script viene eseguito con UID 0 e siamo in grado di eseguire tutte le fasi successive, come smontare i vecchi volumi, montare i volumi clone e ripristinare e ripristinare il database di destinazione. Per attivare l'esecuzione dello script con `sudo`, la seguente riga deve essere aggiunta in `/etc/sudoers`:

```
hn6adm ALL=(root)
NOPASSWD:/usr/local/bin/H06/central_plugin_host_wrapper_script.sh
```



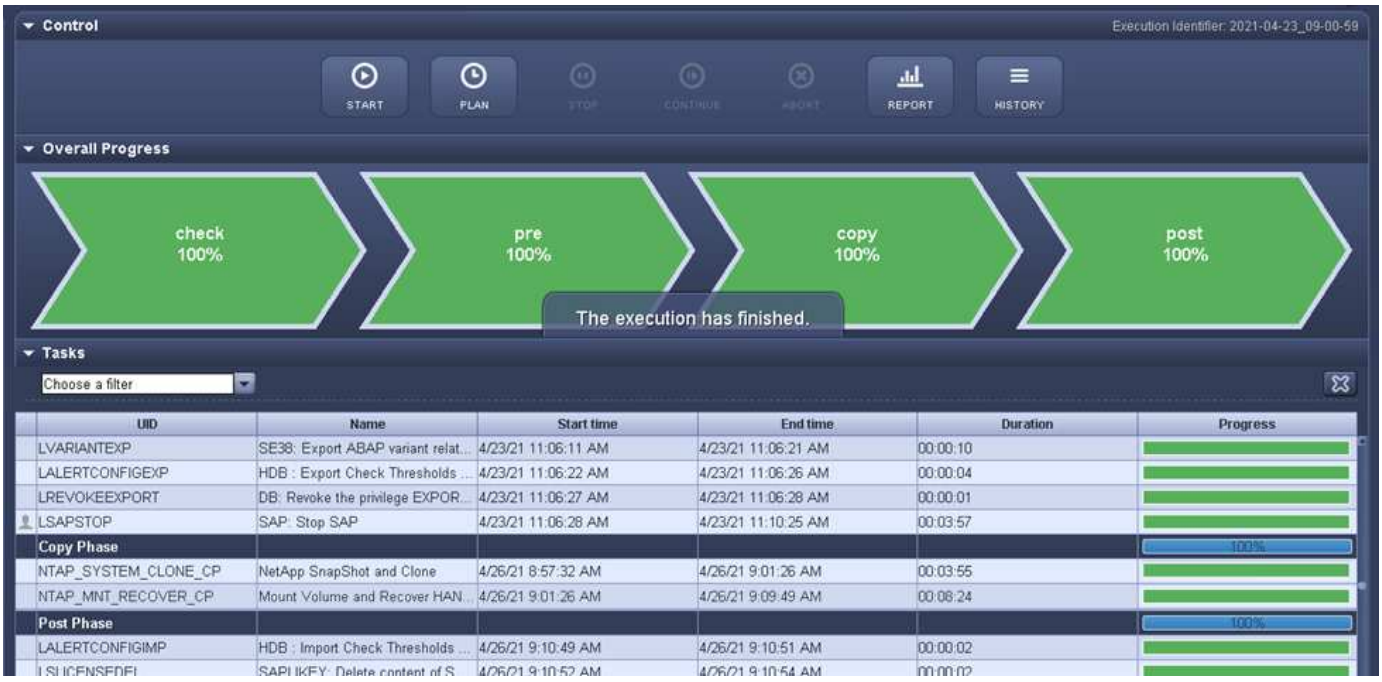
Operazione di refresh del sistema SAP HANA

Ora che sono state eseguite tutte le attività di integrazione necessarie tra LSC e NetApp SnapCenter, avviare un aggiornamento del sistema SAP completamente automatizzato è un'operazione con un solo clic.

La figura seguente mostra l'attività `NTAP``SYSTEM``CLONE` in un'installazione standard. Come si può vedere, la creazione di una copia Snapshot e di un clone, il montaggio del volume clone sul server del database di destinazione e il ripristino e il ripristino del database di destinazione hanno richiesto circa 14 minuti. Sorprendentemente, con la tecnologia Snapshot e NetApp FlexClone, la durata di questa attività rimane quasi la stessa, indipendentemente dalle dimensioni del database di origine.



La figura seguente mostra le due attività `NTAP_SYSTEM_CLONE_CP` e. `NTAP_MNT_RECOVERY_CP` quando si utilizza un host di comunicazione centrale. Come si può vedere, la creazione di una copia Snapshot, di un clone, il montaggio del volume clone sul server del database di destinazione e il ripristino e il ripristino del database di destinazione hanno richiesto circa 12 minuti. Questo tempo è più o meno lo stesso necessario per eseguire queste operazioni quando si utilizza un'installazione standard. Anche in questo caso, la tecnologia Snapshot e NetApp FlexClone consente il completamento rapido e coerente di queste attività, indipendentemente dalle dimensioni del database di origine.



Aggiornamento del sistema SAP HANA con LSC, AzAcSnap e Azure NetApp Files

Utilizzo di "Azure NetApp Files per SAP HANA", Oracle e DB2 su Azure offrono ai clienti le funzionalità avanzate di gestione dei dati e protezione dei dati di NetApp ONTAP con il servizio nativo Microsoft Azure NetApp Files. "AzAcSnap" È la base per operazioni di

refresh dei sistemi SAP molto veloci per creare copie Snapshot NetApp coerenti con le applicazioni dei sistemi SAP HANA e Oracle (DB2 non è attualmente supportato da AzAcSnap).

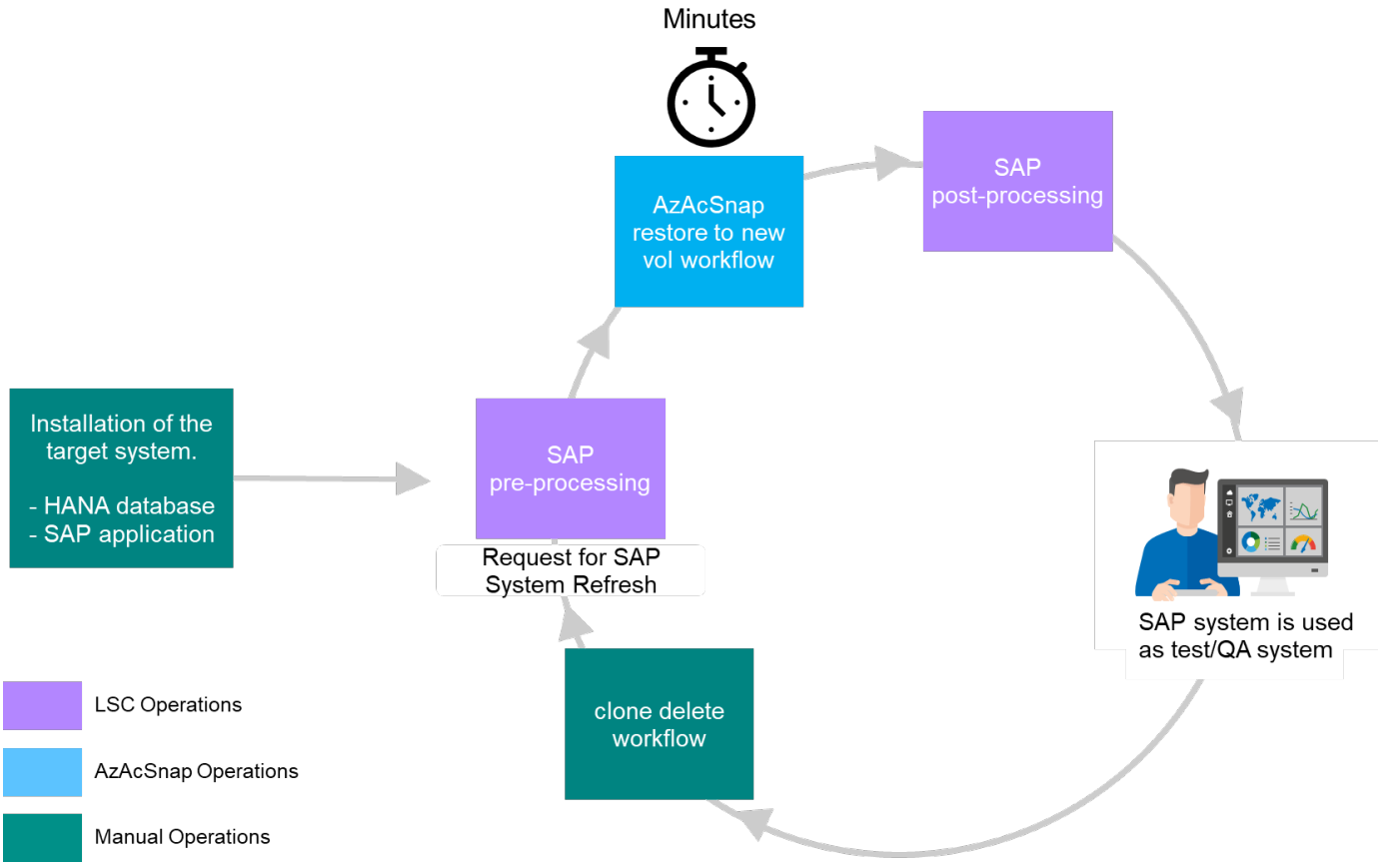
I backup delle copie Snapshot, creati on-demand o su base regolare come parte della strategia di backup, possono quindi essere clonati in modo efficiente su nuovi volumi e utilizzati per aggiornare rapidamente i sistemi di destinazione. AzAcSnap fornisce i flussi di lavoro necessari per creare backup e clonarli in nuovi volumi, mentre libelle SystemCopy esegue le fasi di pre e post-elaborazione necessarie per un refresh completo del sistema end-to-end.

In questo capitolo, descriveremo un refresh automatico del sistema SAP utilizzando AzAcSnap e libelle SystemCopy utilizzando SAP HANA come database sottostante. Poiché AzAcSnap è disponibile anche per Oracle, la stessa procedura può essere implementata anche utilizzando AzAcSnap per Oracle. In futuro, AzAcSnap potrebbe supportare altri database, che consentirebbero di eseguire operazioni di copia del sistema per tali database con LSC e AzAcSnap.

La figura seguente mostra un tipico workflow di alto livello di un ciclo di vita di refresh del sistema SAP con AzAcSnap e LSC:

- Installazione e preparazione del sistema di destinazione una tantum.
- Operazioni di pre-elaborazione SAP eseguite da LSC.
- Ripristino (o clonazione) di una copia Snapshot esistente del sistema di origine nel sistema di destinazione eseguito da AzAcSnap.
- Operazioni di post-elaborazione SAP eseguite da LSC.

Il sistema può quindi essere utilizzato come sistema di test o QA. Quando viene richiesto un nuovo aggiornamento del sistema, il flusso di lavoro viene riavviato con il passaggio 2. Tutti i volumi clonati rimanenti devono essere cancellati manualmente.

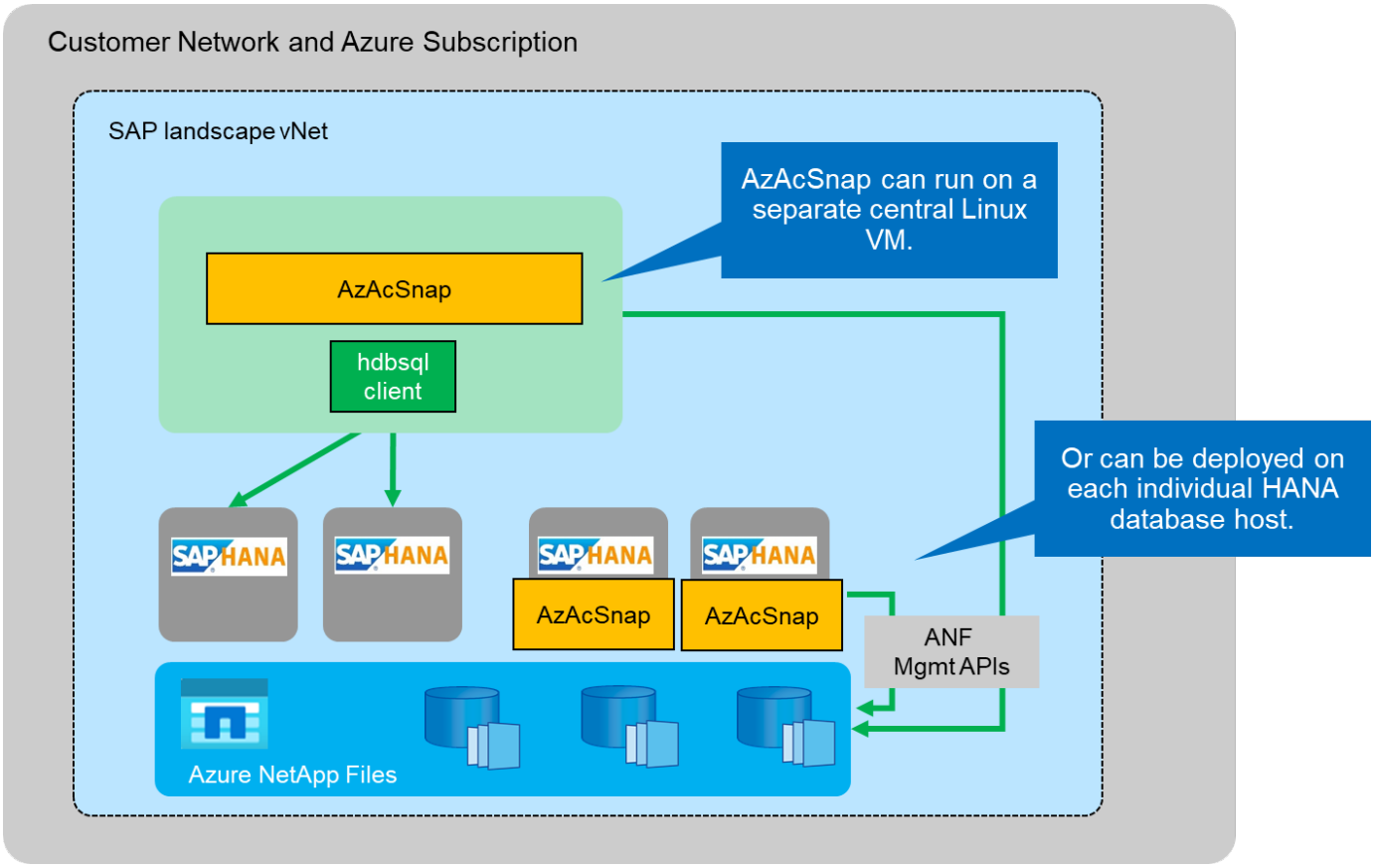


Prerequisiti e limitazioni

Devono essere soddisfatti i seguenti prerequisiti.

AzAcSnap installato e configurato per il database di origine

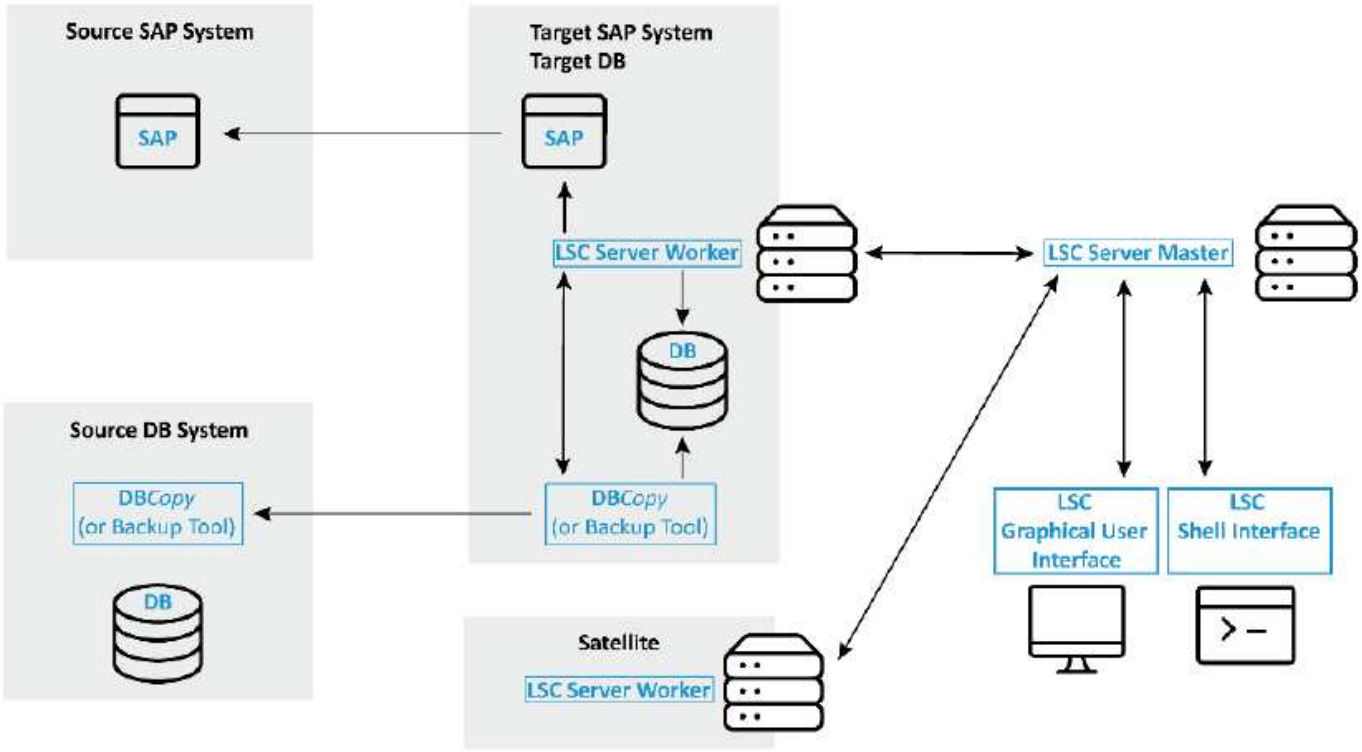
In generale, sono disponibili due opzioni di implementazione per AzAcSnap, come illustrato nella figura seguente.



AzAcSnap può essere installato ed eseguito su una macchina virtuale Linux centrale per la quale tutti i file di configurazione del DB sono memorizzati centralmente e AzAcSnap ha accesso a tutti i database (tramite il client hdbsql) e alle chiavi dell'archivio utenti HANA configurate per tutti questi database. Con un'implementazione decentralizzata, AzAcSnap viene installato singolarmente su ciascun host di database in cui viene in genere memorizzata solo la configurazione del database locale. Entrambe le opzioni di implementazione sono supportate per l'integrazione LSC. Tuttavia, abbiamo seguito un approccio ibrido nella configurazione di laboratorio per questo documento. AzAcSnap è stato installato su una condivisione NFS centrale insieme a tutti i file di configurazione del database. Questa condivisione di installazione centrale è stata montata su tutte le macchine virtuali in `/mnt/software/AZACSNAP/snapshot-tool`. L'esecuzione dello strumento è stata quindi eseguita localmente sulle macchine virtuali DB.

Libelle SystemCopy installato e configurato per il sistema SAP di origine e di destinazione

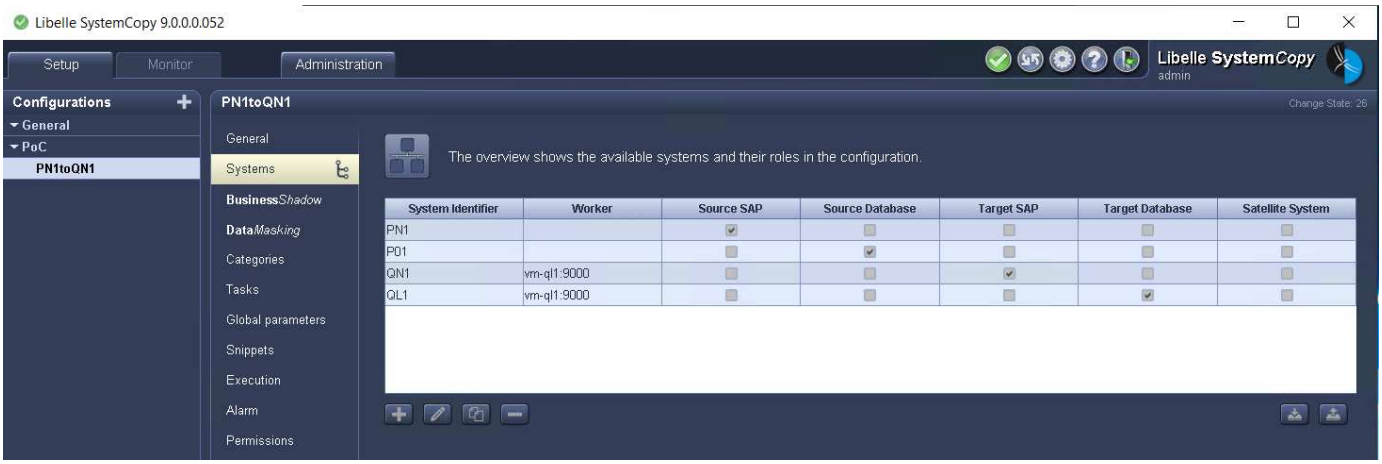
Le implementazioni di libelle SystemCopy sono costituite dai seguenti componenti:



- **LSC Master.** come suggerisce il nome, questo è il componente master che controlla il flusso di lavoro automatico di una copia di sistema basata su libelle.
- **LSC Worker.** un lavoratore LSC esegue di solito sul sistema SAP di destinazione ed esegue gli script richiesti per la copia automatica del sistema.
- **Satellite LSC.** un satellite LSC viene eseguito su un sistema di terze parti su cui devono essere eseguiti ulteriori script. Il master LSC può anche svolgere il ruolo di sistema satellitare LSC.

La GUI di Libelle SystemCopy (LSC) deve essere installata su una macchina virtuale adatta. In questa configurazione di laboratorio, la GUI LSC è stata installata su una macchina virtuale Windows separata, ma può essere eseguita anche sull'host DB insieme all'operatore LSC. Il lavoratore LSC deve essere installato almeno sulla macchina virtuale del DB di destinazione. A seconda dell'opzione di implementazione di AzAcSnap scelta, potrebbero essere necessarie ulteriori installazioni di worker LSC. È necessario disporre di un'installazione di lavoro LSC sulla macchina virtuale in cui viene eseguito AzAcSnap.

Una volta installato LSC, la configurazione di base per il database di origine e di destinazione deve essere eseguita in base alle linee guida LSC. Le immagini seguenti mostrano la configurazione dell'ambiente di laboratorio per questo documento. Per ulteriori informazioni sui sistemi e i database SAP di origine e di destinazione, consulta la sezione successiva.



È inoltre necessario configurare un elenco di attività standard adatto per i sistemi SAP. Per ulteriori informazioni sull'installazione e la configurazione di LSC, consultare il manuale utente di LSC incluso nel pacchetto di installazione di LSC.

Limitazioni note

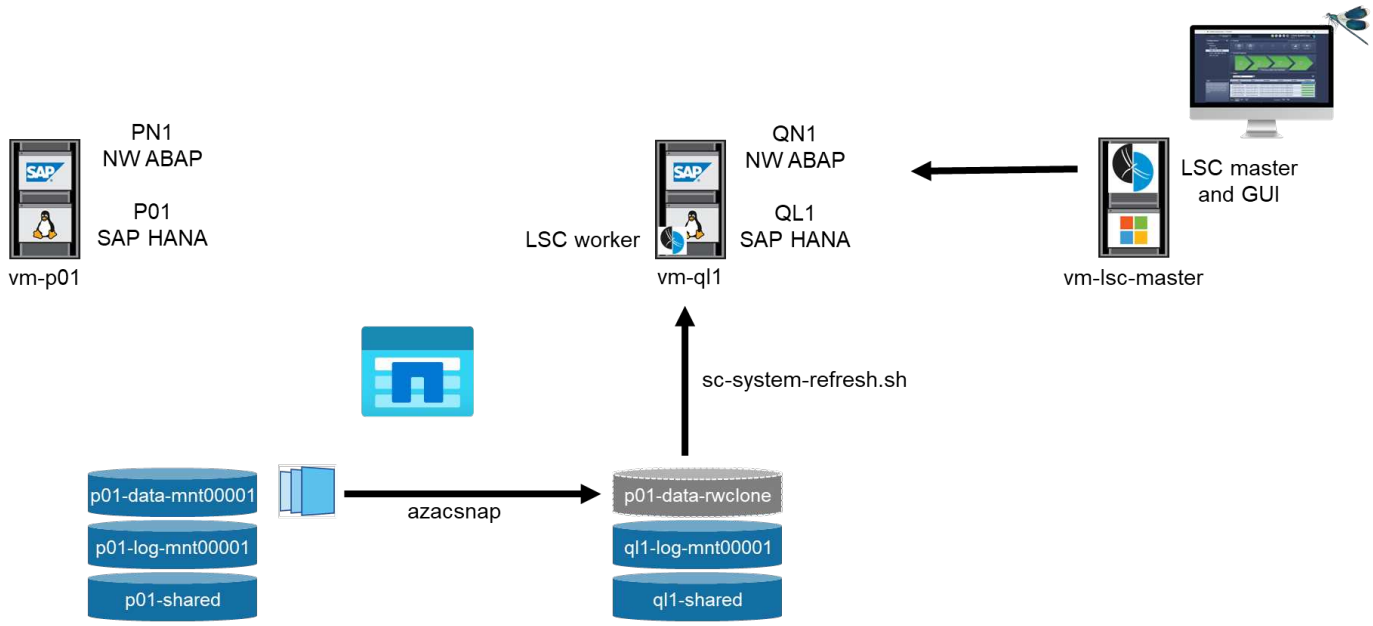
L'integrazione di AzAcSnap e LSC descritta qui funziona solo per i database SAP HANA a host singolo. È possibile supportare anche le implementazioni di più host (o scale-out) SAP HANA, ma tali implementazioni richiedono alcune modifiche o miglioramenti alle attività personalizzate LSC per la fase di copia e gli script di understing. Tali miglioramenti non sono trattati in questo documento.

L'integrazione del refresh del sistema SAP utilizza sempre l'ultima copia Snapshot del sistema di origine per eseguire il refresh del sistema di destinazione. Se si desidera utilizzare altre copie Snapshot meno recenti, la logica corrispondente in ZAZACSNAPRESTORE l'attività personalizzata deve essere regolata. Questo processo non rientra nell'ambito del presente documento.

Setup di laboratorio

Il setup di laboratorio è costituito da un sistema SAP di origine e da un sistema SAP di destinazione, entrambi eseguiti su database SAP HANA a host singolo.

La figura seguente mostra la configurazione del laboratorio.

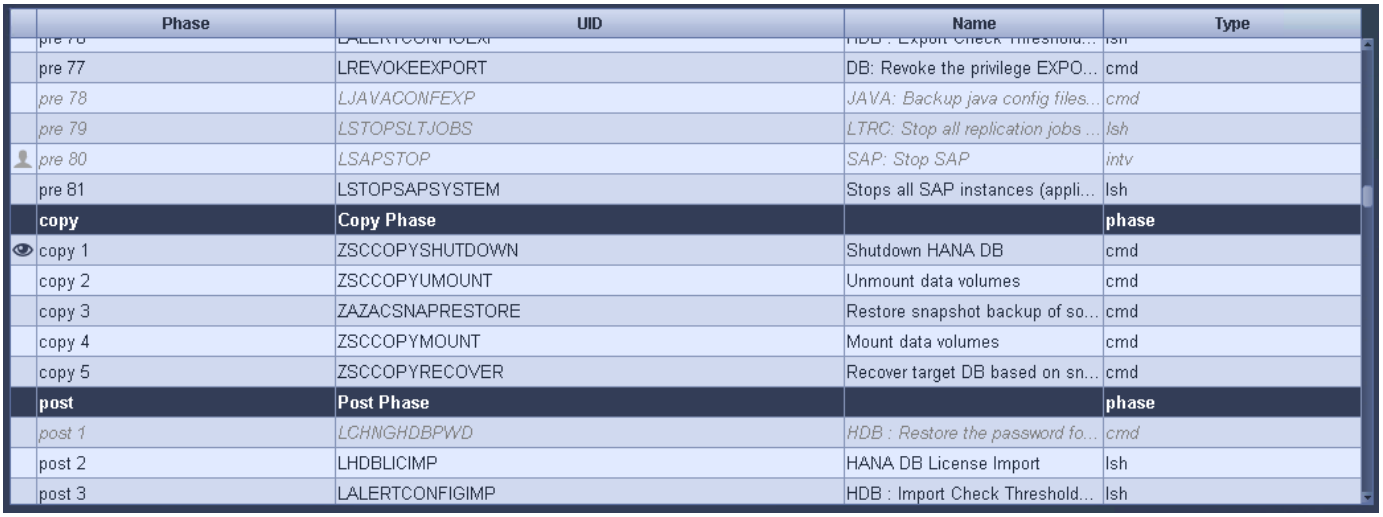


Contiene i seguenti sistemi, versioni software e volumi Azure NetApp Files:

- **P01.** DATABASE SAP HANA 2.0 SP5. Database di origine, host singolo, tenant utente singolo.
- **PN1.** SAP NETWEAVER ABAP 7.51. Sistema SAP di origine.
- **vm-p01.** SLES 15 SP2 con AzAcSnap installato. VM di origine che ospita P01 e PN1.
- **QL1.** DATABASE SAP HANA 2.0 SP5. Aggiornamento del sistema database di destinazione, host singolo, tenant per singolo utente.
- **QN1.** SAP NETWEAVER ABAP 7.51. Refresh del sistema di destinazione sistema SAP.
- **vm-ql1.** SLES 15 SP2 con LSC Worker installato. VM di destinazione che ospitano QL1 e QN1.
- LSC master versione 9.0.0.0.052.
- **vm- lsc-master.** Windows Server 2016. Ospita LSC master e LSC GUI.
- Volumi Azure NetApp Files per dati, log e condivisi per P01 e QL1 montati sugli host DB dedicati.
- Volume Azure NetApp Files centrale per script, installazione di AzAcSnap e file di configurazione montati su tutte le macchine virtuali.

Fasi iniziali di preparazione una tantum

Prima di eseguire il primo aggiornamento del sistema SAP, è necessario integrare le operazioni di storage basate su copia e clonazione Snapshot di Azure NetApp Files eseguite da AzAcSnap. È inoltre necessario eseguire uno script ausiliario per avviare e arrestare il database e montare o smontare i volumi Azure NetApp Files. Tutte le attività richieste vengono eseguite come attività personalizzate in LSC come parte della fase di copia. La figura seguente mostra le attività personalizzate nell'elenco di attività LSC.



Phase	UID	Name	Type
pre 77	LREVOKEEXPORT	DB: Revoke the privilege EXPO...	cmd
pre 78	*LJAVACONFEXP*	*JAVA: Backup java config files...*	*cmd*
pre 79	*LSTOPSLTJOBS*	*LTRC: Stop all replication jobs ...*	*lsh*
pre 80	*LSAPSTOP*	*SAP: Stop SAP*	*intv*
pre 81	LSTOPSAPSYSTEM	Stops all SAP instances (appli...	lsh
copy	**Copy Phase**		**phase**
copy 1	ZSCCOPYSHUTDOWN	Shutdown HANA DB	cmd
copy 2	ZSCCOPYUMOUNT	Unmount data volumes	cmd
copy 3	ZAZACSNAPRESTORE	Restore snapshot backup of so...	cmd
copy 4	ZSCCOPYMOUNT	Mount data volumes	cmd
copy 5	ZSCCOPYRECOVER	Recover target DB based on sn...	cmd
post	**Post Phase**		**phase**
post 1	*LCHNGHDBPWD*	*HDB : Restore the password fo...*	*cmd*
post 2	LHDBLICIMP	HANA DB License Import	lsh
post 3	LALERTCONFIGIMP	HDB : Import Check Threshold...	lsh

Le cinque attività di copia sono descritte in dettaglio. In alcune di queste attività, uno script di esempio `sc-system-refresh.sh` Viene utilizzato per automatizzare ulteriormente l'operazione di ripristino del database SAP HANA richiesta e il montaggio e lo smontaggio dei volumi di dati. Lo script utilizza un `LSC: success` Messaggio nell'output di sistema per indicare che l'esecuzione a LSC è riuscita. I dettagli sulle attività personalizzate e sui parametri disponibili sono disponibili nel manuale dell'utente di LSC e nella guida per gli sviluppatori di LSC. Tutte le attività in questo ambiente di laboratorio vengono eseguite sulla macchina virtuale DB di destinazione.

Lo script di esempio viene fornito così com'è e non è supportato da NetApp. Puoi richiedere lo script via email a ng-sapcc@netapp.com.

Sc-system-refresh.sh file di configurazione

Come accennato in precedenza, viene utilizzato uno script ausiliario per avviare e arrestare il database, per montare e smontare i volumi Azure NetApp Files e per ripristinare il database SAP HANA da una copia Snapshot. Lo script `sc-system-refresh.sh` Viene memorizzato nella condivisione NFS centrale. Lo script richiede un file di configurazione per ogni database di destinazione che deve essere memorizzato nella stessa cartella dello script stesso. Il file di configurazione deve avere il seguente nome: `sc-system-refresh-<target DB SID>.cfg` (ad esempio `sc-system-refresh-QL1.cfg` in questo ambiente di laboratorio). Il file di configurazione utilizzato qui utilizza un SID del DB di origine fisso/con codifica hardware. Con alcune modifiche, lo script e il file di configurazione possono essere migliorati per assumere il SID del DB di origine come parametro di input.

I seguenti parametri devono essere regolati in base all'ambiente specifico:

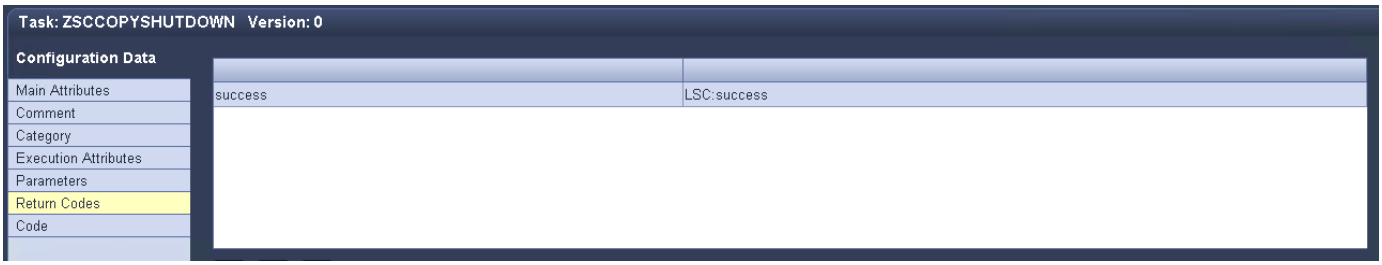
```
# hdbuserstore key, which should be used to connect to the target database
KEY=”QL1SYSTEM”
# single container or MDC
export P01_HANA_DATABASE_TYPE=MULTIPLE_CONTAINERS
# source tenant names { TENANT_SID [, TENANT_SID]* }
export P01_TENANT_DATABASE_NAMES=P01
# cloned vol mount path
export CLONED_VOLUMES_MOUNT_PATH=`tail -2
/mnt/software/AZACSNAP/snapshot_tool/logs/azacsnap-restore-azacsnap-
P01.log | grep -oe “[0-9]*\.[0-9]*\.[0-9]*\.[0-9]*:/.* “`
```

ZSCCOPYSHUTDOWN

Questa attività arresta il database SAP HANA di destinazione. La sezione Code di questa attività contiene il seguente testo:

```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/scripts/sc-system-refresh/sc-system-refresh.sh shutdown
$_system(target_db, id)_$ > $_logfile_$
```

Lo script `sc-system-refresh.sh` utilizza due parametri, il `shutdown` E il DB SID, per arrestare il database SAP HANA utilizzando sapcontrol. L’output di sistema viene reindirizzato al file di log LSC standard. Come accennato in precedenza, un `LSC: success` viene utilizzato per indicare che l’esecuzione è riuscita.



ZSCCOPYUMOUNT

Questa attività disinstalla il vecchio volume di dati Azure NetApp Files dal sistema operativo del DB di destinazione. La sezione code di questa attività contiene il seguente testo:

```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/scripts/sc-system-refresh/sc-system-refresh.sh umount
$_system(target_db, id)_$ > $_logfile_$
```

Vengono utilizzati gli stessi script dell’attività precedente. I due parametri passati sono `umount` E il DB SID.

ZAZACSNAPRESTORE

Questa attività esegue AzAcSnap per clonare l’ultima copia Snapshot del database di origine in un nuovo

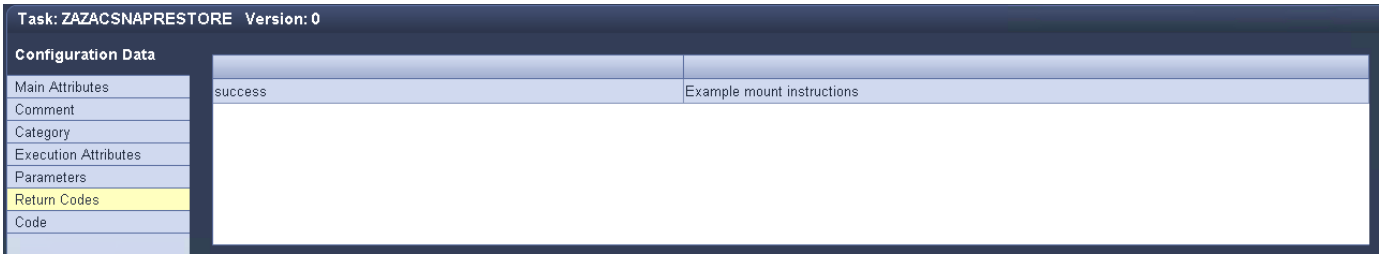
volume per il database di destinazione. Questa operazione equivale a un ripristino reindirizzato del backup negli ambienti di backup tradizionali. Tuttavia, la funzionalità di copia e clonazione Snapshot consente di eseguire questa attività in pochi secondi anche per i database più grandi, mentre, con i backup tradizionali, questa attività potrebbe richiedere diverse ore. La sezione code di questa attività contiene il seguente testo:

```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/AZACSNAP/snapshot_tool/azacsnap -c restore --restore
snaptovol --hanasid $_system(source_db, id)_$
--configfile=/mnt/software/AZACSNAP/snapshot_tool/azacsnap
-$_system(source_db, id)_$.json > $_logfile_$
```

Documentazione completa delle opzioni della riga di comando AzAcSnap per `restore` Il comando è disponibile nella documentazione di Azure qui: "Eseguire il ripristino utilizzando lo strumento Snapshot coerente dell'applicazione Azure". La chiamata presuppone che il file di configurazione del database json per il database di origine possa essere trovato nella condivisione NFS centrale con la seguente convenzione di denominazione: `azacsnap-<source DB SID>. json`, (ad esempio, `azacsnap-P01.json` in questo ambiente di laboratorio).

> Poiché l'output del comando AzAcSnap non può essere modificato, l'impostazione predefinita `LSC: success` impossibile utilizzare il messaggio per questa attività. Pertanto, la stringa `Example mount instructions` L'output di AzAcSnap viene utilizzato come codice di ritorno corretto. Nella versione GA 5.0 di AzAcSnap, questo output viene generato solo se il processo di cloning ha avuto esito positivo.

La figura seguente mostra il messaggio di ripristino di AzAcSnap sul nuovo volume riuscito.



ZSCCOPIMOUNT

Questa attività consente di montare il nuovo volume di dati Azure NetApp Files sul sistema operativo del DB di destinazione. La sezione code di questa attività contiene il seguente testo:

```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/scripts/sc-system-refresh/sc-system-refresh.sh mount
$_system(target_db, id)_$ > $_logfile_$
```

Lo script sc-system-refresh.sh viene nuovamente utilizzato, passando il `mount` E il SID del DB di destinazione.

ZSCCOPIRECOVER

Questa attività esegue un ripristino del database SAP HANA del database di sistema e del database tenant in base alla copia Snapshot ripristinata (clonata). L'opzione di ripristino utilizzata in questa sezione riguarda il

backup specifico del database, ad esempio l'assenza di registri aggiuntivi, che vengono applicati per il ripristino in avanti. Pertanto, il tempo di ripristino è molto breve (al massimo pochi minuti). L'esecuzione di questa operazione è determinata dall'avvio del database SAP HANA che avviene automaticamente dopo il processo di ripristino. Per accelerare il tempo di avvio, è possibile aumentare temporaneamente il throughput del volume di dati Azure NetApp Files, se necessario, come descritto nella presente documentazione: "Aumento o diminuzione dinamica della quota di volume". La sezione code di questa attività contiene il seguente testo:

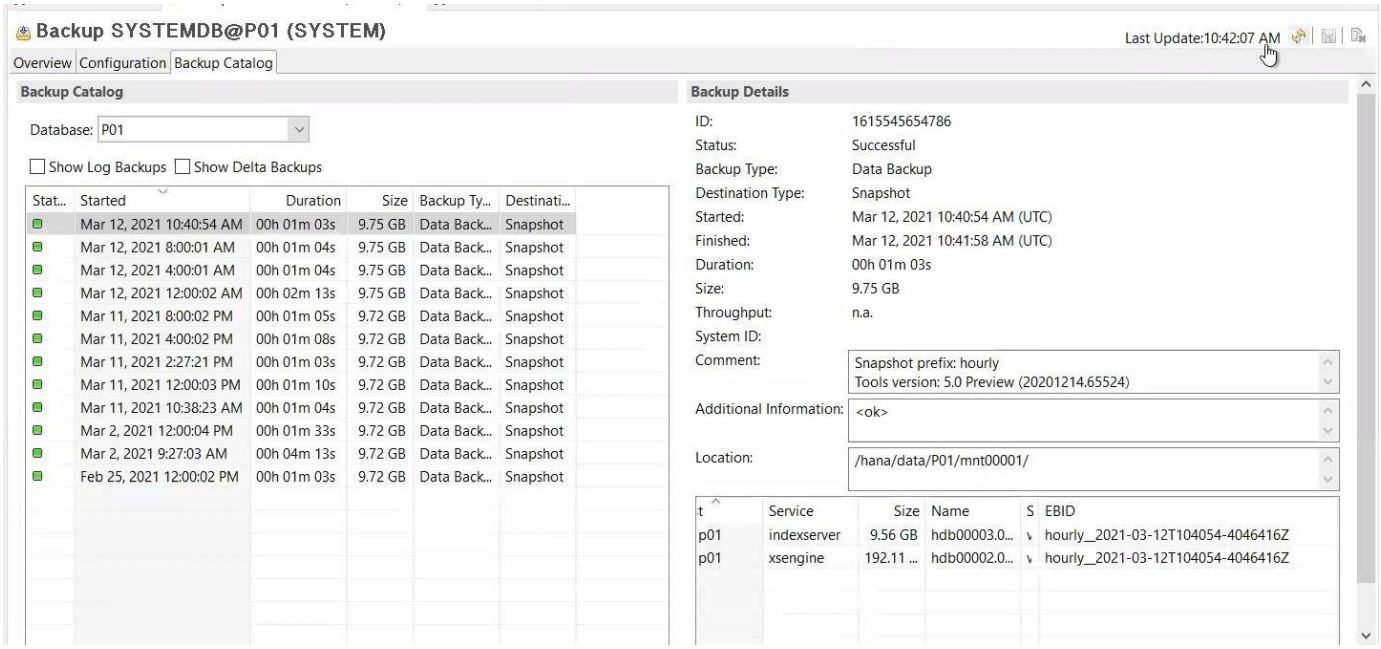
```
$_include_tool(unix_header.sh)_$
sudo /mnt/software/scripts/sc-system-refresh/sc-system-refresh.sh recover
$_system(target_db, id)_$ > $_logfile_$
```

Questo script viene utilizzato nuovamente con `recover` E il SID del DB di destinazione.

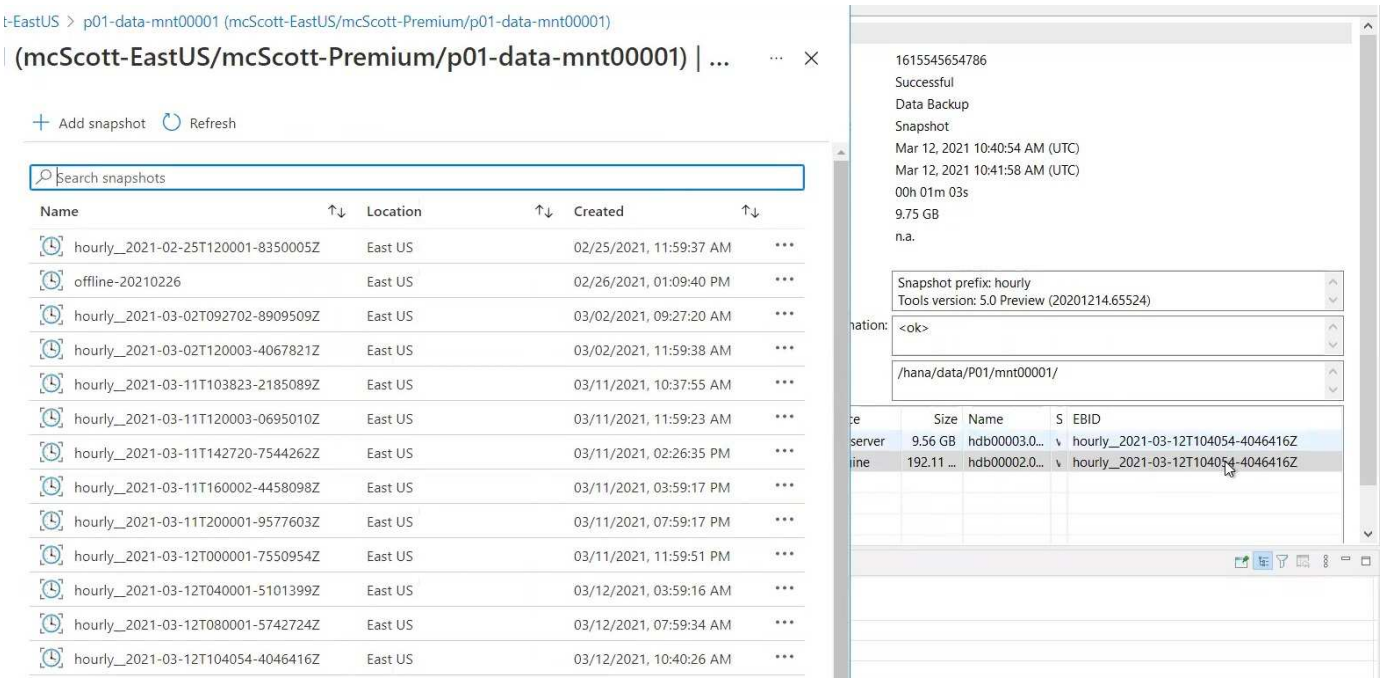
Operazione di refresh del sistema SAP HANA

In questa sezione, un esempio di operazione di refresh dei sistemi di laboratorio mostra le fasi principali di questo flusso di lavoro.

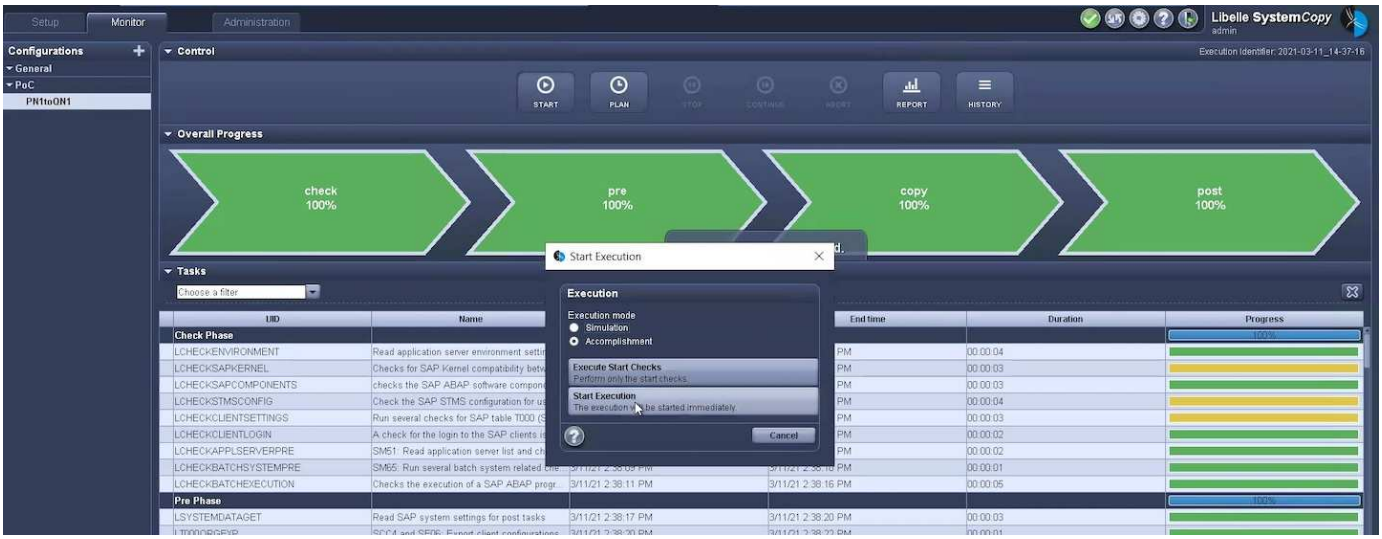
Sono state create copie Snapshot regolari e on-demand per il database di origine P01, come elencato nel catalogo di backup.



Per l'operazione di refresh, è stato utilizzato l'ultimo backup del 12 marzo. Nella sezione relativa ai dettagli del backup, viene elencato l'ID di backup esterno (EBID) per questo backup. Si tratta del nome della copia Snapshot del backup della copia Snapshot corrispondente sul volume di dati Azure NetApp Files, come mostrato nella figura seguente.



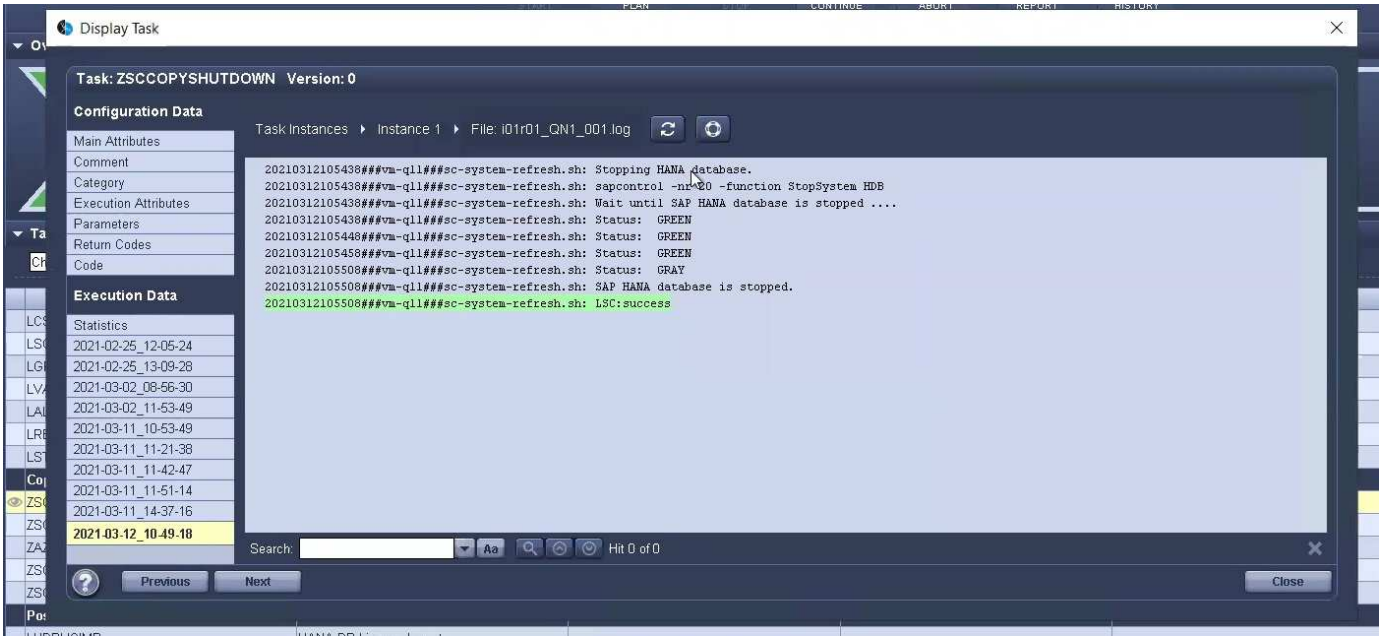
Per avviare l'operazione di refresh, selezionare la configurazione corretta nella GUI LSC, quindi fare clic su Start Execution (Avvia esecuzione).



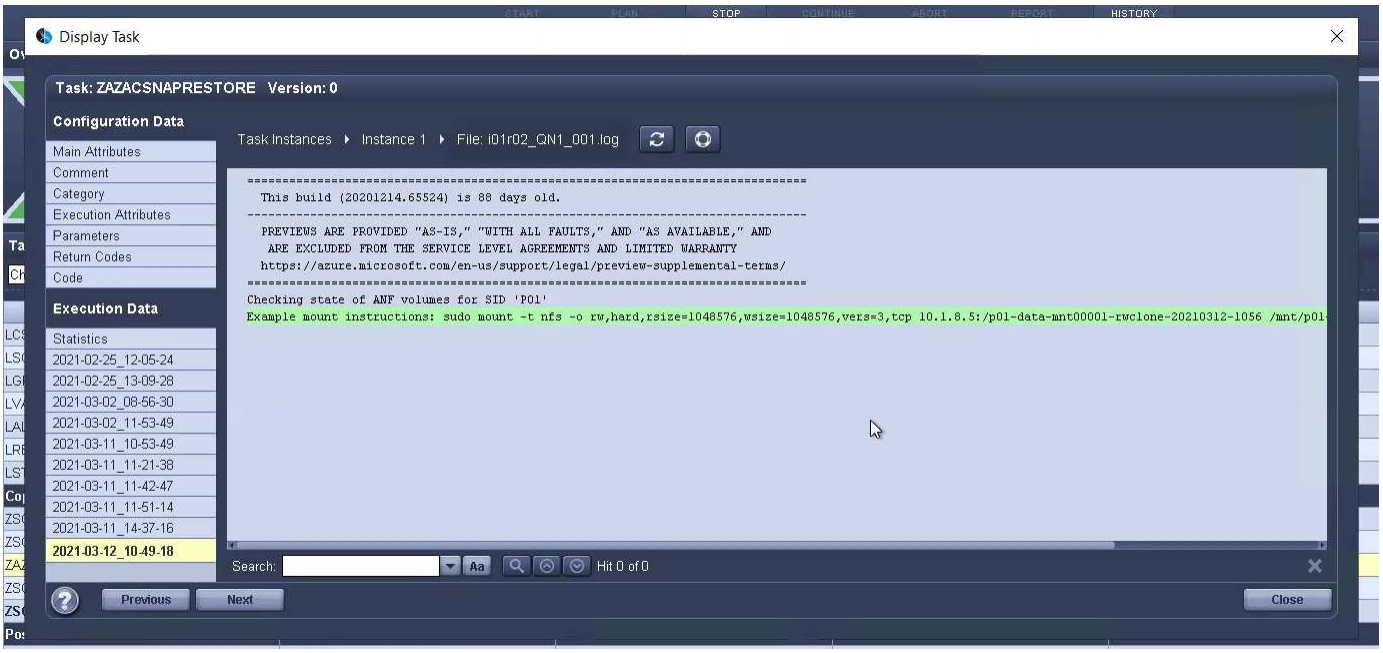
LSC inizia a eseguire le attività della fase di verifica, seguite dalle attività configurate della fase preliminare.

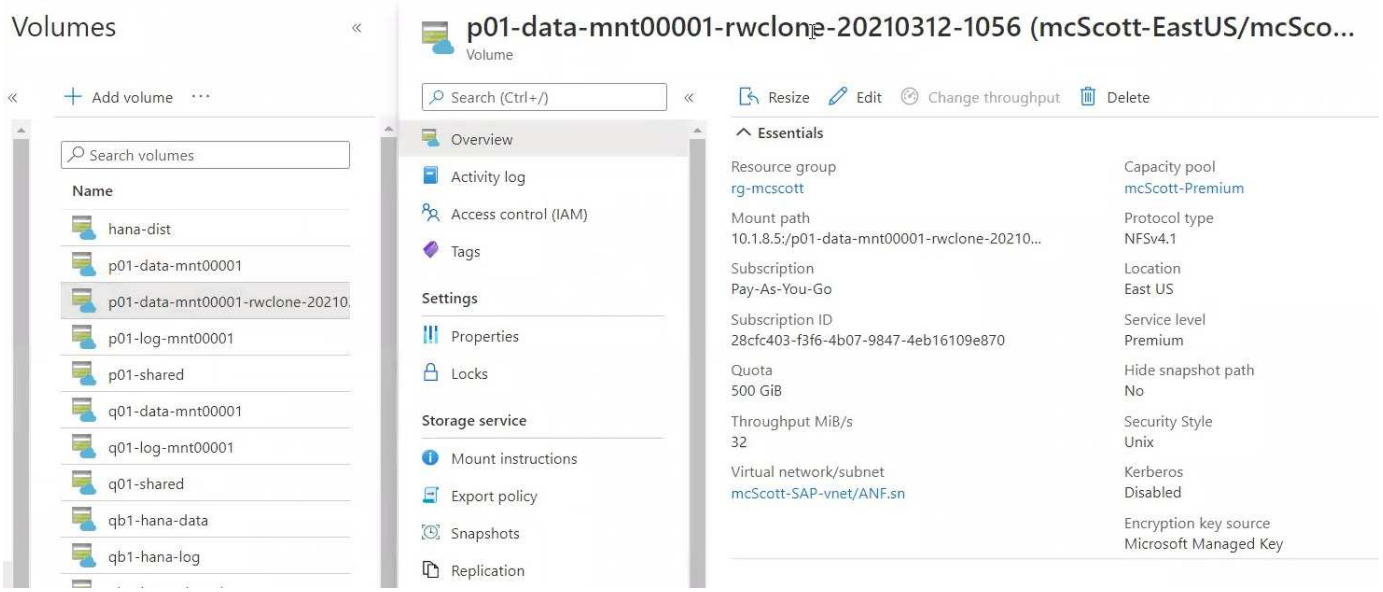


Come ultima fase della fase preliminare, il sistema SAP di destinazione viene arrestato. Nella fase di copia successiva, vengono eseguite le operazioni descritte nella sezione precedente. Innanzitutto, il database SAP HANA di destinazione viene arrestato e il vecchio volume Azure NetApp Files viene dismontato dal sistema operativo.

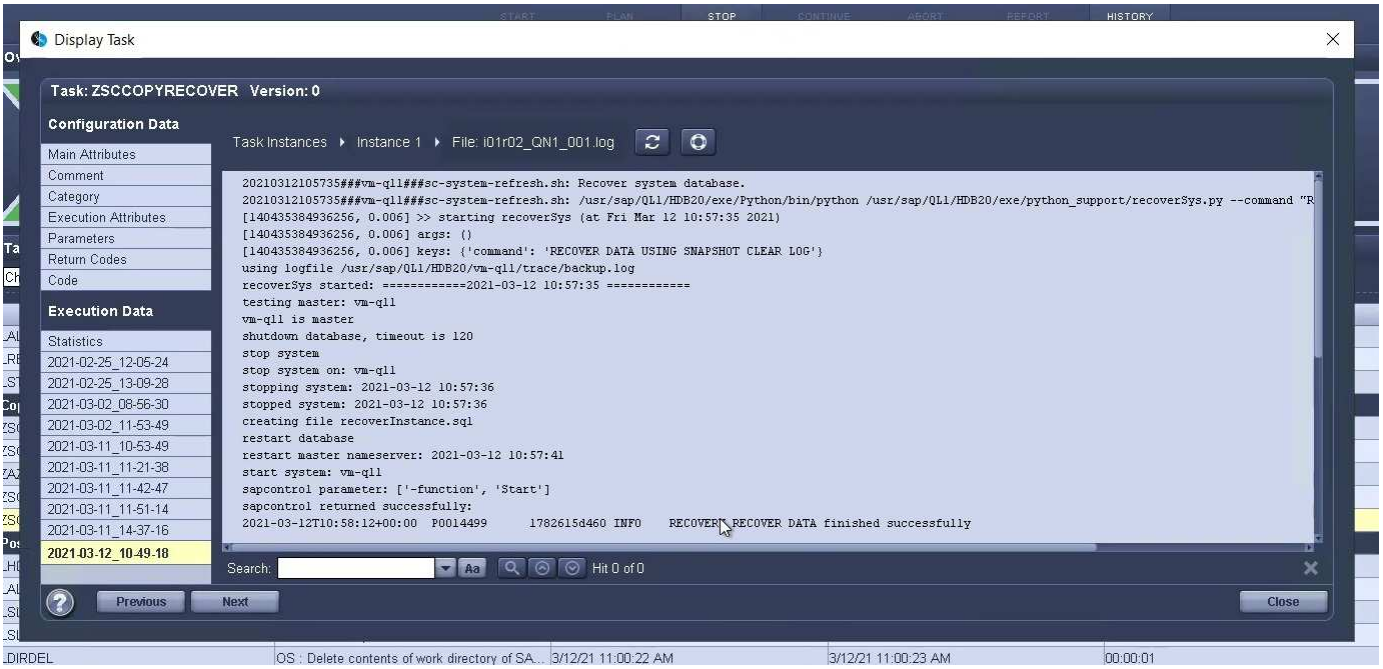


L’attività ZAZACSNAPRESTORE crea quindi un nuovo volume come clone dalla copia Snapshot esistente del sistema P01. Le due immagini seguenti mostrano i log dell’attività nella GUI LSC e il volume Azure NetApp Files clonato nel portale Azure.





Questo nuovo volume viene quindi montato sull'host DB di destinazione e il database di sistema e il database tenant vengono ripristinati utilizzando la copia Snapshot contenente. Una volta completato il ripristino, il database SAP HANA viene avviato automaticamente. Questo avvio del database SAP HANA occupa la maggior parte del tempo della fase di copia. Le fasi rimanenti in genere terminano in pochi secondi o pochi minuti, indipendentemente dalle dimensioni del database. L'immagine seguente mostra come il database di sistema viene recuperato utilizzando gli script di recovery python forniti da SAP.



Dopo la fase di copia, l'LSC continua con tutte le fasi definite della fase successiva. Al termine del processo di aggiornamento del sistema, il sistema di destinazione è nuovamente operativo e pienamente utilizzabile. Con questo sistema di laboratorio, il runtime totale per il refresh del sistema SAP è stato di circa 25 minuti, di cui la fase di copia ha consumato poco meno di 5 minuti.



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:

- Documentazione sui prodotti NetApp

  "https://docs.netapp.com"

Cronologia delle versioni

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

Solution Brief

SB-3978: Gestione del ciclo di vita per SAP HANA

NetApp sta affrontando le sfide legate alla lenta implementazione delle funzionalità, alla mancanza di automazione e alla perdita di produttività fornendo una soluzione per la gestione del ciclo di vita completamente integrata negli strumenti utilizzati dagli amministratori SAP per le operazioni quotidiane, come SAP Landscape Management (SAP lama). L'obiettivo è semplificare il flusso di lavoro di provisioning dalla pre-elaborazione alla post-elaborazione, incluse tutte le attività software e a livello di storage necessarie per creare una copia del sistema di produzione. Con questa soluzione, gli amministratori possono creare un ambiente di sviluppo e test con un paio di clic del mouse, migliorando così la gestione del ciclo di vita.

https://www.netapp.com/pdf.html?item=/media/6996-sb-3978pdf.pdf

SB-3965: Backup e ripristino per SAP HANA

La sfida

Con le operazioni di backup e ripristino di SAP HANA, la tua organizzazione deve affrontare le seguenti sfide: • Operazioni di backup prolungate con degrado delle prestazioni sui sistemi SAP di produzione • Tempi di inattività del sistema inaccettabili dovuti a lunghe operazioni di ripristino e recupero • Finestre di backup ridotte a causa della criticità delle applicazioni • La necessità di una soluzione flessibile per mitigare la corruzione logica

La soluzione

Con le soluzioni di storage NetApp® che utilizzano il software di gestione dati NetApp ONTAP®, in combinazione con il software di protezione dati NetApp SnapCenter®, puoi affrontare tutte queste sfide. Grazie alla tecnologia NetApp Snapshot™ inclusa nel software ONTAP , è possibile creare backup o eseguire operazioni di ripristino di set di dati di qualsiasi dimensione in pochi secondi. SAP HANA supporta l'utilizzo di copie Snapshot basate sull'archiviazione come operazione di backup valida.

https://www.netapp.com/pdf.html?item=/media/6997-sb-3965pdf.pdf

SB-3968: Disaster Recovery per SAP HANA

La sfida

La continuità aziendale è essenziale nelle organizzazioni IT. Devono essere in grado di fornire servizi ad alta disponibilità per le applicazioni mission-critical di cui i loro clienti hanno bisogno per gestire le loro attività. In caso contrario, i loro clienti subiranno un calo di produttività e le aziende di e-commerce potrebbero subire un impatto diretto sui loro ricavi.

La soluzione

NetApp ha sviluppato un portafoglio completo di tecnologie e strumenti per aiutare le organizzazioni IT a creare o adattare i propri piani di disaster recovery per rispondere a tutte le esigenze aziendali:

https://www.netapp.com/pdf.html?item=/media/6998-sb-3968pdf.pdf

SB-4292: Automazione SAP con Ansible

Questo documento si concentra sull'integrazione dei sistemi di storage NetApp®, che siano gestiti on-premise, in un ambiente IaaS (Infrastructure as a Service) di cloud pubblico o nel cloud ibrido, in SAP Landscape Management (lama) utilizzando Playbook Ansible e script personalizzati.

Panoramica della soluzione

I sistemi SAP sono molto complessi. Tuttavia, per le aziende che utilizzano SAP, questi sistemi sono fondamentali per i loro processi di business. Automatizzando i task operativi quotidiani ricorrenti, gli amministratori di sistema SAP possono gestire più sistemi con meno sforzo, produrre risultati ripetibili e ridurre l'errore umano.

Questo documento si concentra sull'integrazione dei sistemi di storage NetApp®, che siano gestiti on-premise, in un ambiente IaaS (Infrastructure as a Service) di cloud pubblico o nel cloud ibrido, in SAP Landscape Management (lama) utilizzando Playbook Ansible e script personalizzati. Questa integrazione consente agli amministratori SAP di velocizzare le attività di aggiornamento dei sistemi SAP utilizzando NetApp Snapshot™ e la tecnologia NetApp FlexClone®.

Pubblico di riferimento

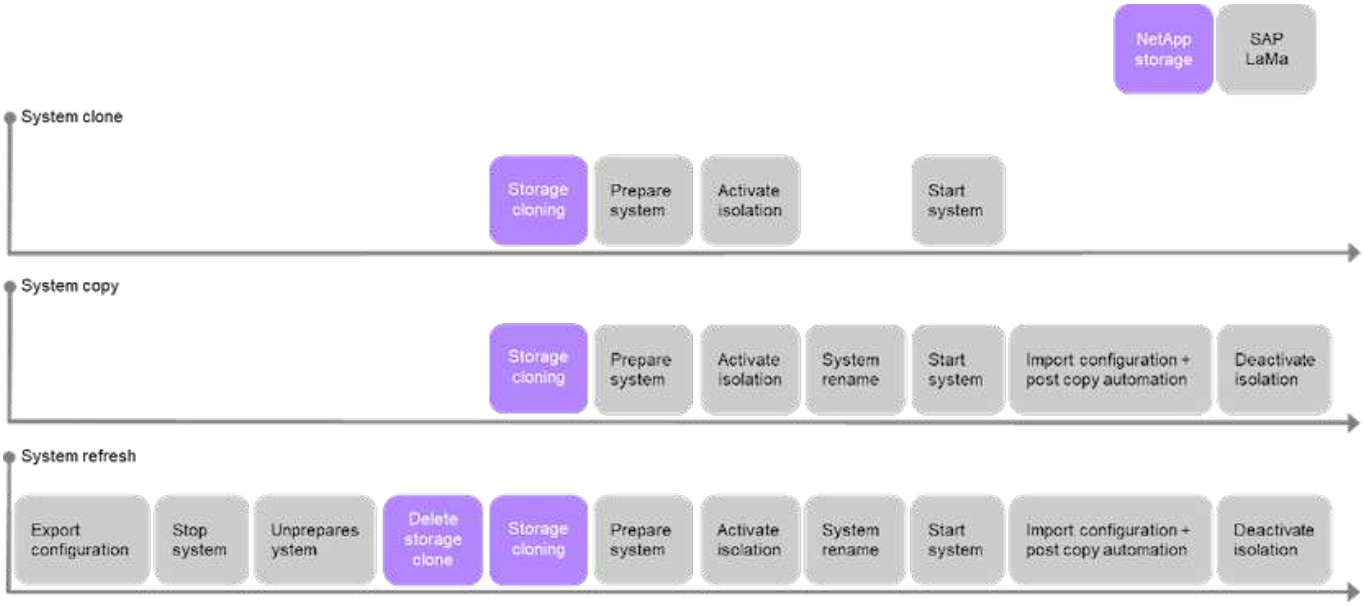
Questo documento è rivolto agli amministratori di sistema SAP che non hanno avuto molta (o nessuna) esperienza con l'automazione Ansible. Questo dovrebbe aiutarti a iniziare con Ansible, eseguire i primi playbook e configurare ed eseguire la tua prima operazione di refresh di sistema basato su SAP lama.

Scenari di cloning, copia e refresh del sistema SAP

Il termine copia del sistema SAP viene spesso utilizzato come sinonimo di tre processi diversi: Clone del sistema SAP, copia del sistema SAP e refresh del sistema SAP. È importante distinguere tra le diverse operazioni, poiché i flussi di lavoro e i casi di utilizzo sono diversi.

- **Clone del sistema SAP**. Un clone del sistema SAP è un clone identico di un sistema SAP di origine. I cloni di sistema SAP vengono in genere utilizzati per affrontare la corruzione logica o per testare gli scenari di disaster recovery. Con un'operazione di clonazione del sistema, il nome host, il numero di istanza e l'identificatore sicuro (SID) rimangono invariati. È quindi importante stabilire un corretto scherma di rete per il sistema di destinazione per assicurarsi che non vi sia comunicazione con l'ambiente di produzione.
- **Copia del sistema SAP**. Una copia del sistema SAP è il setup di un nuovo sistema SAP di destinazione con dati provenienti da un sistema SAP di origine. Ad esempio, il nuovo sistema target potrebbe essere un sistema di test aggiuntivo con i dati provenienti dal sistema di produzione. Il nome host, il numero di istanza e il SID sono diversi per i sistemi di origine e di destinazione.
- **Aggiornamento del sistema SAP**. Un refresh di sistema SAP è un refresh di un sistema SAP di destinazione esistente con dati provenienti da un sistema SAP di origine. Il sistema di destinazione fa generalmente parte di un ambiente di trasporto SAP, ad esempio un sistema di controllo della qualità, aggiornato con i dati del sistema di produzione. Il nome host, il numero di istanza e il SID sono diversi per i sistemi di origine e di destinazione.

L'immagine seguente mostra i passaggi del workflow lama di cloning, copia e refresh del sistema SAP correlati allo storage NetApp.

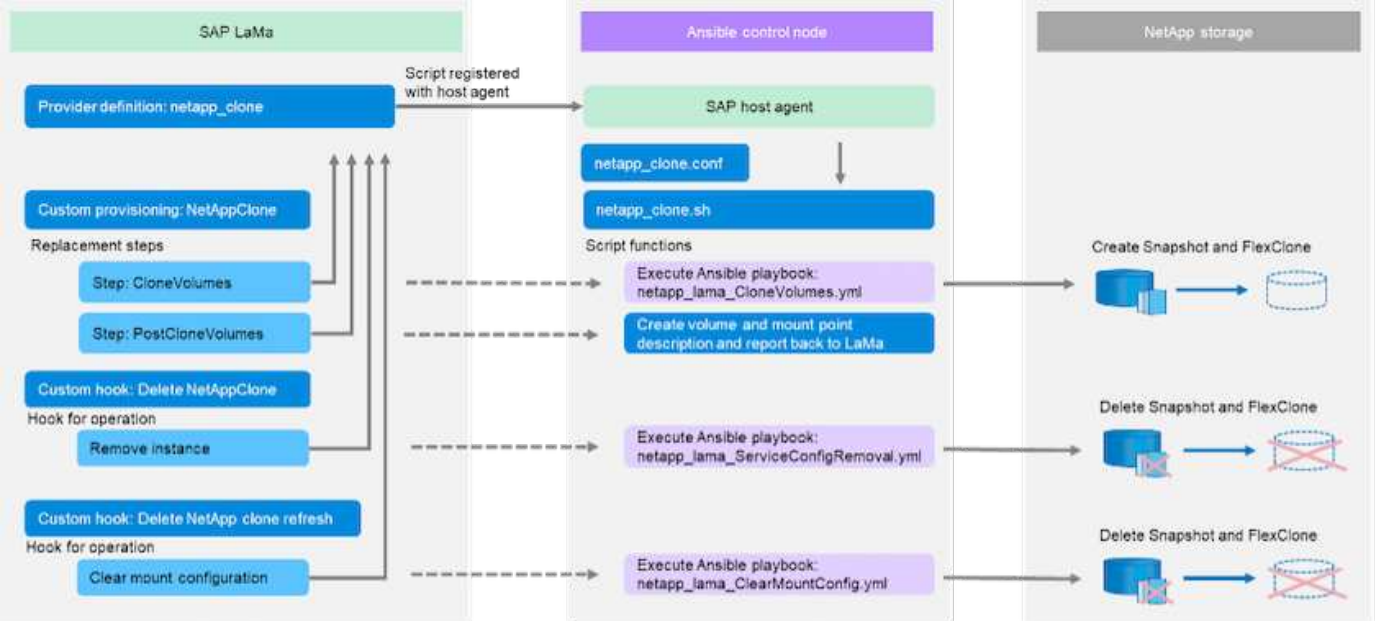


Tecnologia della soluzione

La soluzione globale è costituita dai seguenti componenti principali:

- Sistema SAP lama
- Sistema di storage NetApp
- Nodo di controllo Ansible con agente host SAP installato. Consigliamo di utilizzare la piattaforma di automazione Red Hat Ansible, in quanto offre ulteriori benefici, quali:
  - Utilizzo di ai per generare consigli di codice per i task di automazione
  - Riduzione delle attività manuali con l'automazione basata sugli eventi
  - Essere definiti, coerenti e portatili
  - Automazione e scalabilità in più ambienti
  - Accelerazione dell'automazione con contenuti preconfezionati
  - Monitoraggio e gestione dell'automazione con rich reporting e metriche di osservabilità
  - Creazione di attività, moduli e playbook

L'immagine seguente mostra come i sistemi storage SAP lama e NetApp si integrano attraverso i Playbook Ansible su un host Ansible dedicato, attivati da shell script eseguiti da SAP host Agent.

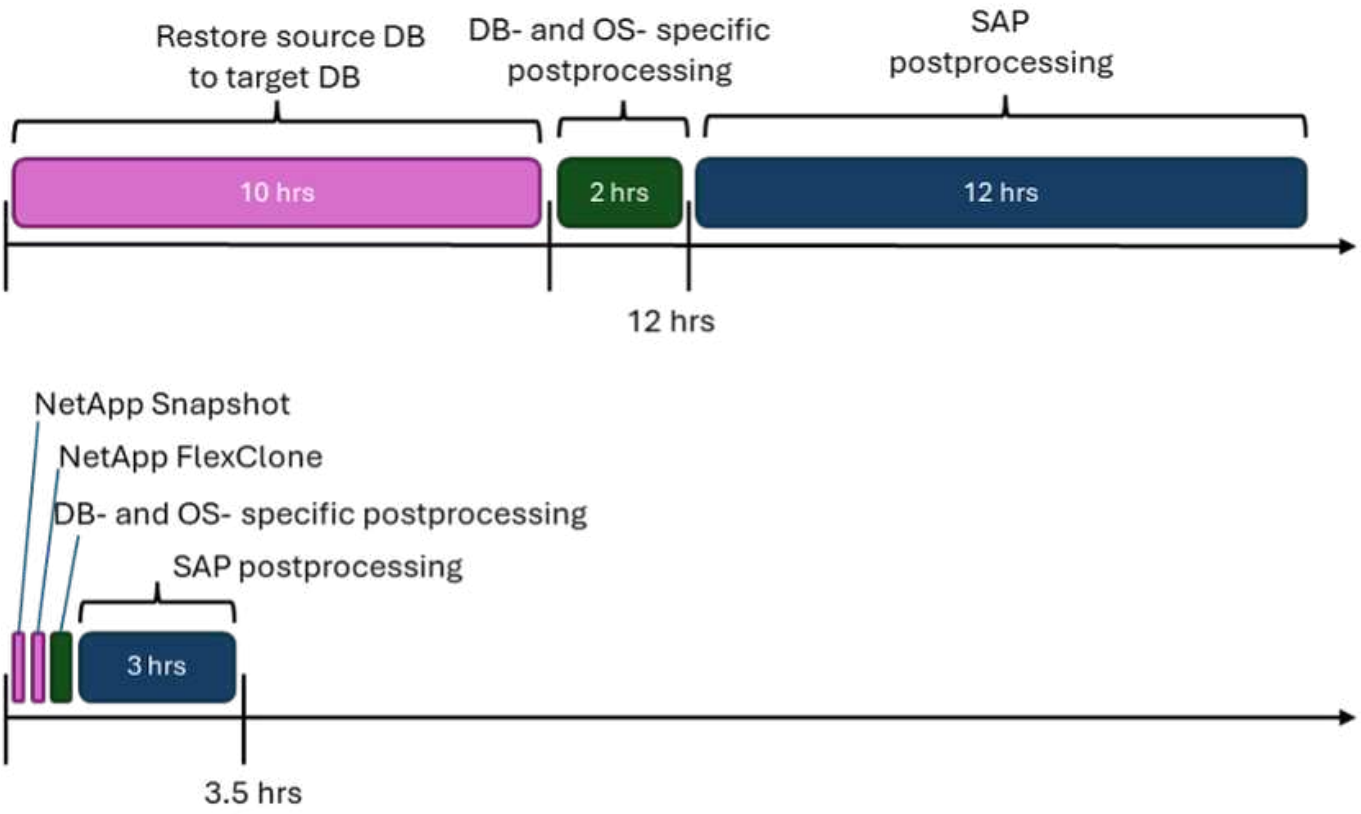


Riepilogo del caso d'utilizzo

Esistono diversi scenari in cui i dati di un sistema di origine devono essere resi disponibili a un sistema di destinazione per scopi di test o formazione. Questi sistemi di test e formazione devono essere aggiornati regolarmente con i dati del sistema di origine per assicurarsi che i test e la formazione vengano eseguiti con il set di dati corrente. Queste operazioni di refresh del sistema sono costituite da più task a livello di infrastruttura, database e applicazione e possono richiedere diversi giorni, in base al livello di automazione.

Per accelerare e automatizzare i task richiesti a livello di infrastruttura e database, puoi utilizzare i flussi di lavoro di cloning SAP lama e NetApp. Invece di ripristinare un backup dal sistema di origine al sistema di destinazione, SAP lama utilizza le tecnologie Snapshot e FlexClone di NetApp in modo che le attività necessarie per avviare un database possano essere eseguite in pochi minuti anziché in ore, come mostrato nella figura seguente. Il tempo necessario per il processo di clonazione non dipende dalle dimensioni del database; pertanto, in pochi minuti è possibile creare anche sistemi molto grandi. Puoi ridurre ulteriormente i tempi di esecuzione automatizzando i task sul sistema operativo e sul livello di database, oltre che sul lato di post-elaborazione SAP.

L'immagine seguente mostra i possibili miglioramenti dell'efficienza operativa quando si utilizza l'automazione.



Integrare i diversi componenti tecnologici

Per integrare SAP lama con i sistemi storage NetApp utilizzando Ansible, hai bisogno di un nodo su cui eseguire i Playbook Ansible. Consigliamo di utilizzare la piattaforma di automazione Ansible. Per eseguire shell script e Playbook Ansible su questo host, avviati da SAP lama, è necessario disporre di un agente host SAP in esecuzione su questo server. SAP host Agent prende il controllo della comunicazione bidirezionale con SAP lama ed esegue script di shell che attiveranno i playbook effettivi.

Questa architettura accoppiata in modo lasco ti offre la libertà di avviare i workflow da SAP lama e anche al di fuori di SAP lama. I playbook e la logica corrispondente devono essere configurati una sola volta e possono essere utilizzati per diversi scenari e casi di utilizzo.

Conclusione

La combinazione di NetApp, SAP lama e piattaforma di automazione Ansible fornisce una soluzione potente che può ridurre drasticamente il tempo e gli sforzi necessari per i task più complessi e lunghi correlati all'amministrazione del sistema SAP. Questa combinazione può anche aiutare a evitare la deriva di configurazione che l'errore umano può causare tra i sistemi.

Dato che i refresh del sistema, le copie, i cloni e i test di disaster recovery sono procedure molto sensibili l'implementazione di una soluzione di questo tipo può far risparmiare tempo prezioso di amministrazione. Può anche rafforzare la fiducia che il resto dell'organizzazione avrà negli amministratori di sistema SAP: Vedrà quanto più facile è copiare i sistemi per test o altri scopi, e quanto tempo di risoluzione dei problemi può essere risparmiato.

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e

siti Web:

- "Automatizzazione delle operazioni quotidiane 1 e 2 utilizzando i Playbook Ansible per NetApp ONTAP®"
- "Documentazione Ansible specifica di NetApp"
- "Moduli Ansible NetApp ONTAP e documentazione completa"
- "Piattaforma di automazione Red Hat Ansible"

Cronologia delle versioni

Versione	Data	Riepilogo degli aggiornamenti
Versione 0,1	03,2023	1st bozza.
Versione 0,2	01,2024	Rivedere e alcune correzioni minori
Versione 0,3	06,2024	Convertito in formato html

SB-4293: Automazione dei flussi di lavoro di copia, refresh e cloning del sistema SAP con ALPACA e NetApp SnapCenter

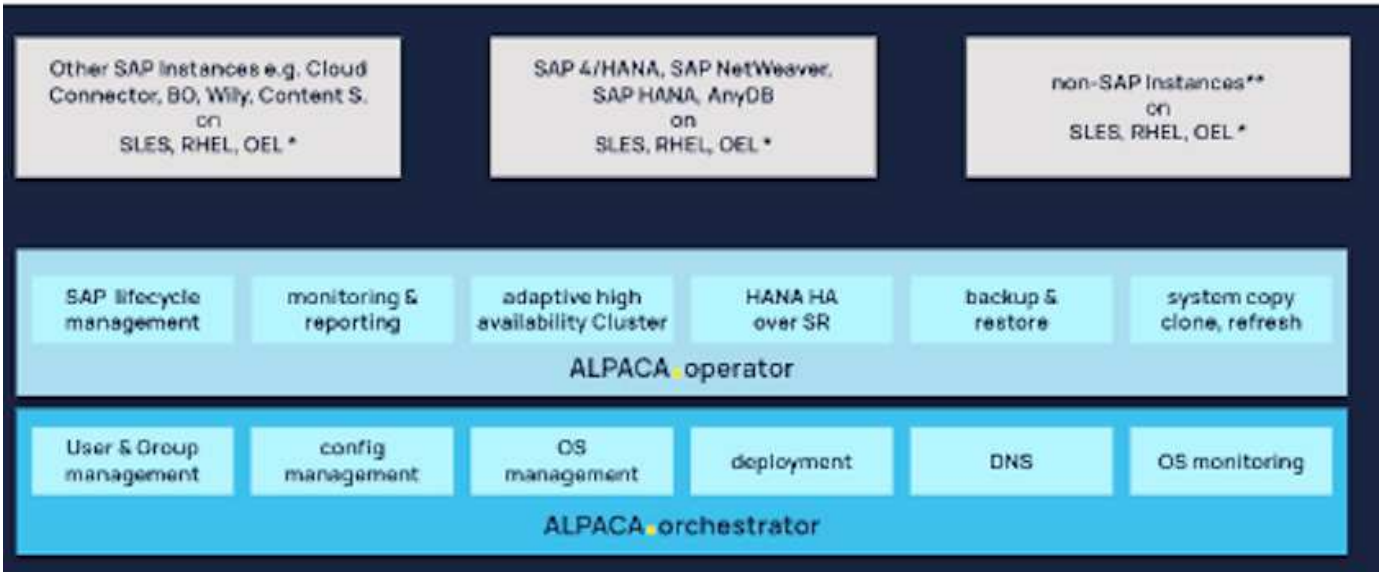
Questo documento si concentra sull'integrazione delle tecnologie NetApp® Snapshot™ e FlexClone® nei flussi di lavoro di ALPACA automation.

Panoramica della soluzione

Le operazioni dei sistemi e delle soluzioni SAP sono molto complesse. Tuttavia, per le aziende che utilizzano SAP, i sistemi e i servizi sono fondamentali per i loro processi aziendali. Attraverso l'automazione delle attività operative quotidiane ricorrenti, come le operazioni di copia di sistema e refresh, gli amministratori di sistema SAP possono gestire più sistemi con meno sforzo, produrre risultati ripetibili e ridurre l'errore umano.

Questo documento si concentra sull'integrazione delle tecnologie NetApp® Snapshot™ e FlexClone® nei flussi di lavoro di ALPACA automation.

La suite di automazione dei panorami in modo proattivo: Cloud e ovunque (ALPACA) è un'interfaccia di gestione completa che consente supervisione e monitoraggio dettagliati in tutti i panorami SAP. ALPACA ottimizza e accelera le operazioni dell'infrastruttura SAP, garantendo disponibilità e trasparenza ottimali. Fornisce una gamma completa di strumenti per la gestione dell'intero panorama, inclusa l'infrastruttura, e notifica in modo proattivo anomalie come interruzioni del servizio, arresti dei processi e congestione. La suite è progettata per funzionare perfettamente in ambienti on-premise, ibridi e all-cloud, inclusi scenari multicloud, garantendo l'adattabilità a qualsiasi infrastruttura. Questo framework basato su moduli automatizza le attività di amministrazione SAP standard e regolari, nonché scenari complessi come il failover durante un'interruzione del servizio. Amministratori/esperti, operatori e manager, ALPACA offre a questi professionisti un elevato livello di controllo e automazione.



In questo documento viene descritto come ALPACA si integra con NetApp SnapCenter®, lo strumento per orchestrare i backup basati su Snapshot, eseguire ripristini e creare volumi FlexClone. Questa integrazione consente agli amministratori SAP di accelerare significativamente i task operativi quotidiani del sistema SAP. Le tecnologie Snapshot, FlexClone e SnapRestore® di NetApp accelerano le operazioni di backup, ripristino e clonazione perché la tecnologia di storage NetApp è basata sul puntatore. Questo approccio è veloce e riduce inoltre l'overhead dello storage durante le operazioni di cloning, perché sul supporto storage devono essere scritti solo i dati nuovi e modificati (non i dati esistenti). Ciò vale indipendentemente dal fatto che si tratti di un sistema storage NetApp on-premise o di una soluzione storage NetApp presso uno dei tre principali cloud provider.

Pubblico di riferimento

Questo documento è rivolto agli amministratori di sistema SAP che hanno eseguito copie di sistema SAP manualmente e desiderano automatizzare questa attività con ALPACA. L'obiettivo della combinazione delle tecnologie Snapshot e FlexClone di NetApp, orchestrata da NetApp SnapCenter e dei workflow di ALPACA, è ridurre la durata delle copie di sistema SAP completamente automatizzate.

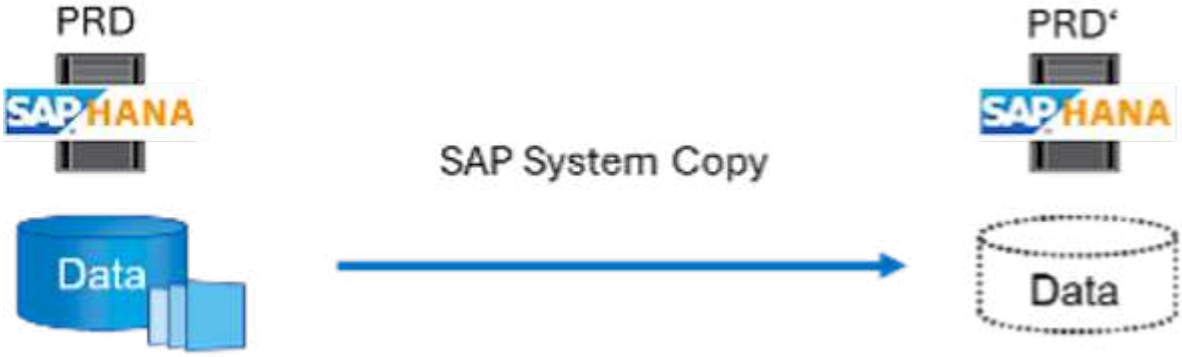
Scenari di cloning, copia e refresh del sistema SAP

Il termine copia del sistema SAP viene spesso utilizzato come sinonimo di tre processi diversi: Clone del sistema SAP, copia del sistema SAP e refresh del sistema SAP. È importante fare una distinzione tra queste operazioni, poiché i flussi di lavoro e i casi di utilizzo sono diversi.

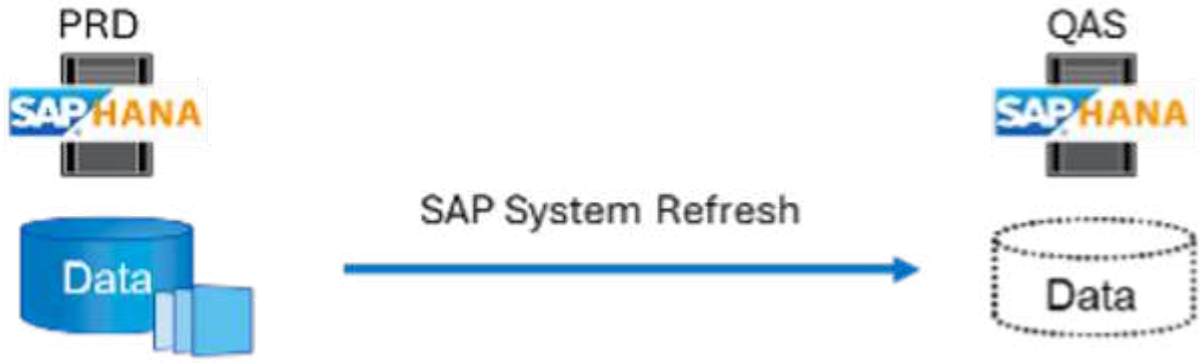
- **Clone del sistema SAP**. Un clone del sistema SAP è un clone identico di un sistema SAP di origine. I cloni di sistema SAP vengono in genere utilizzati per affrontare la corruzione logica o per testare gli scenari di disaster recovery. Con un'operazione di clonazione del sistema, il nome host, il numero di istanza e l'identificatore sicuro (SID) rimangono invariati. È quindi importante stabilire una corretta scherma di rete per il sistema bersaglio per assicurarsi che non vi sia alcuna comunicazione con l'ambiente di produzione.



- **Copia del sistema SAP**. Una copia del sistema SAP è il setup di un nuovo sistema SAP di destinazione con dati provenienti da un sistema SAP di origine. Ad esempio, il nuovo sistema target potrebbe essere un sistema di test aggiuntivo con i dati provenienti dal sistema di produzione. Il nome host, il numero di istanza e il SID sono diversi per i sistemi di origine e di destinazione. Il nuovo sistema non è isolato dal sistema di origine.



- **Aggiornamento del sistema SAP**. Un refresh di sistema SAP è un refresh di un sistema SAP di destinazione esistente con dati provenienti da un sistema SAP di origine. Il sistema di destinazione fa generalmente parte di un ambiente di trasporto SAP, ad esempio un sistema sandbox, aggiornato con i dati del sistema di produzione. Il nome host, il numero di istanza e il SID sono diversi per i sistemi di origine e di destinazione.



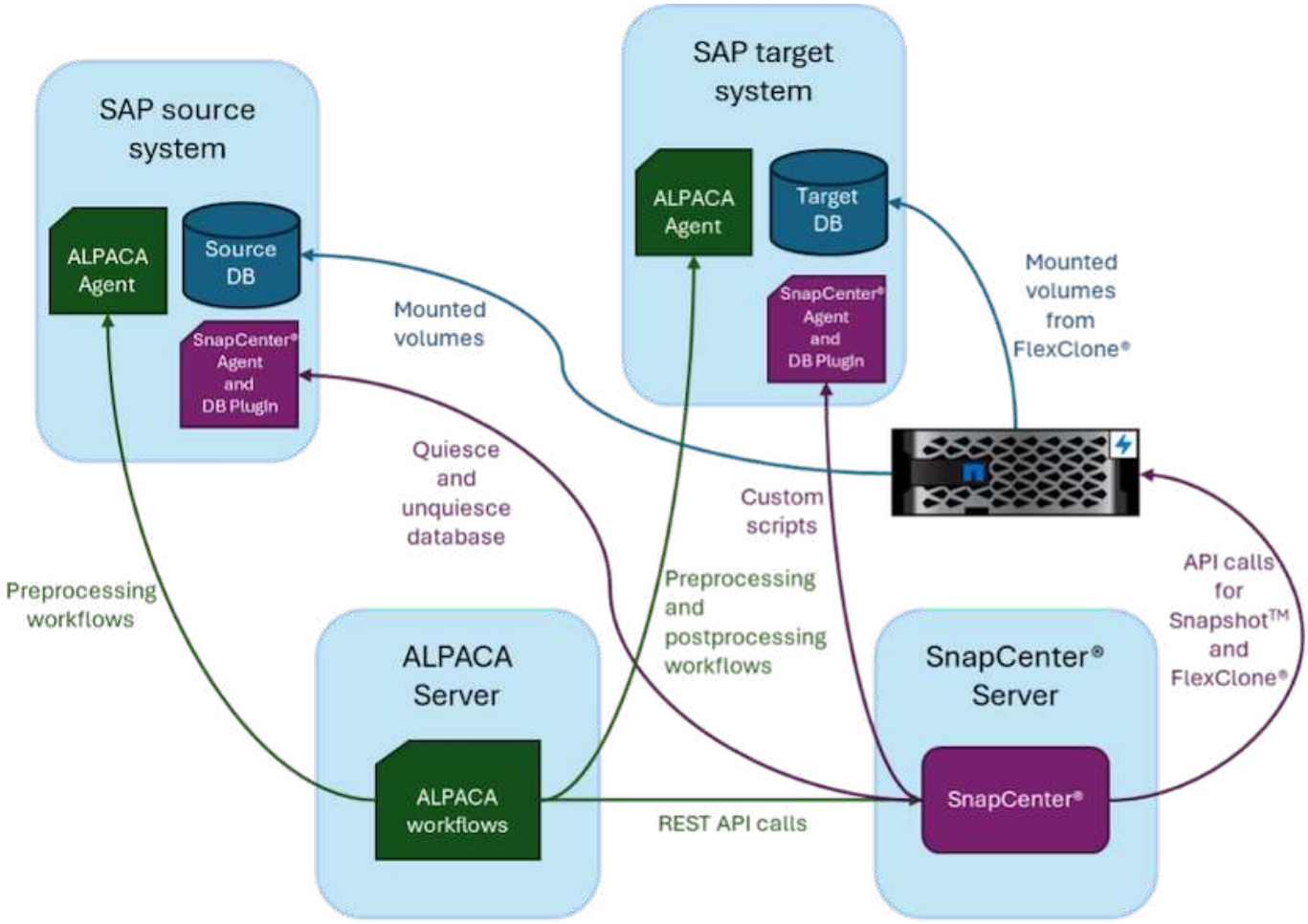
Anche se si tratta di tre casi d'utilizzo diversi, il processo di gestione dei dati rimane invariato. Tutti e tre i casi d'utilizzo utilizzano la stessa tecnologia per la gestione dei dati sottostante: NetApp Snapshot e FlexClone.

Tecnologia della soluzione

La soluzione globale è costituita dai seguenti componenti principali:

- Sistema di origine SAP con agente SnapCenter installato e plug-in database SnapCenter
- Sistema di destinazione SAP con agente SnapCenter installato e plug-in database SnapCenter
- Sistema ALPACA con sorgente SAP configurata e sistema di destinazione SAP
- Server NetApp SnapCenter
- Sistema storage NetApp:
  - Hardware fisico on-premise: Serie AFF-A, AFF-C, ASA-A, ASA-C o FAS
  - Storage software-defined on Premises: ONTAP® Select
  - Cloud storage NetApp:
    - Cloud Volumes ONTAP per AWS, Google Cloud o Azure
    - Azure NetApp Files
    - Amazon FSX per NetApp ONTAP

L'immagine seguente mostra l'ALPACA server, il server NetApp SnapCenter, il sistema di storage NetApp, i sistemi di origine SAP e di destinazione SAP e l'integrazione di ogni elemento. L'obiettivo è rendere l'integrazione il più flessibile possibile utilizzando l'API REST SnapCenter per garantire il massimo riutilizzo del lavoro di configurazione già eseguito all'interno dei componenti in uscita.



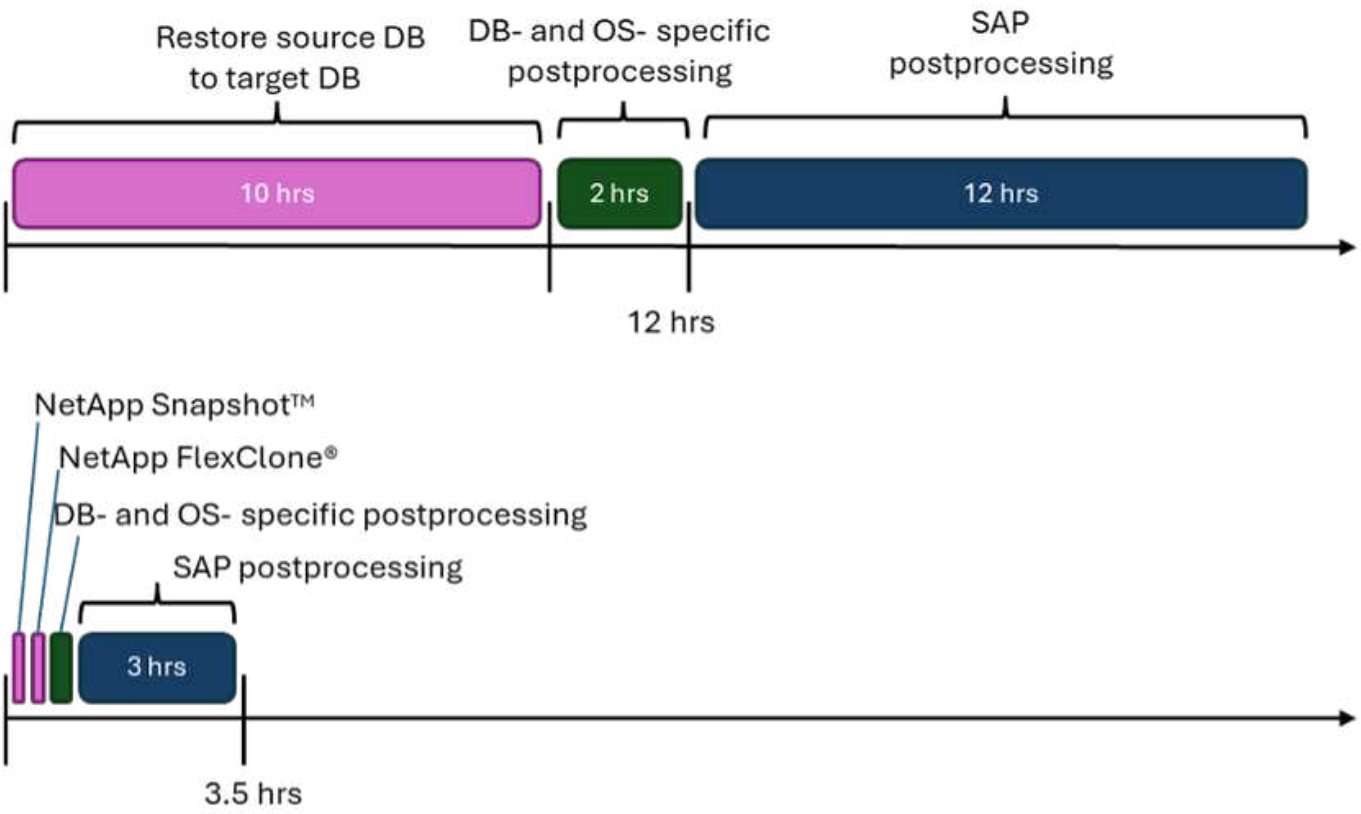
Riepilogo del caso d'utilizzo

Esistono diversi scenari in cui i dati di un sistema di origine devono essere resi disponibili a un sistema di destinazione per scopi di test o formazione. Questi sistemi di test e formazione devono essere aggiornati

regolarmente con i dati del sistema di origine per assicurarsi che i test e la formazione vengano eseguiti con il set di dati corrente. Queste operazioni di refresh del sistema sono costituite da più task a livello di infrastruttura, database e applicazione e possono richiedere diversi giorni, in base al livello di automazione.

Per accelerare le operazioni, automatizzare le attività ed eliminare gli errori umani a livello di infrastruttura, database e applicazione, è possibile utilizzare i workflow ALPACA. Invece di ripristinare un backup dal sistema di origine al sistema di destinazione, un processo dispendioso in termini di tempo e che comporta un elevato consumo delle risorse, questa integrazione utilizza le tecnologie Snapshot e FlexClone di NetApp. Tutte le attività necessarie per accelerare un database vengono completate in pochi minuti invece che in ore. Il tempo richiesto dal processo di clonazione non dipende dalle dimensioni del database; pertanto, in pochi minuti è possibile creare anche sistemi molto grandi. ALPACA riduce ulteriormente i tempi di esecuzione automatizzando i task a livello di sistema operativo e database, oltre che sul fronte di post-elaborazione SAP.

L'immagine seguente mostra i possibili miglioramenti dell'efficienza operativa quando si utilizza l'automazione.



Integrazione dei componenti tecnologici

L'effettiva integrazione di SnapCenter in un workflow di ALPACA consiste nell'utilizzo di shell script per accedere all'API REST di NetApp SnapCenter. Questa integrazione REST API-based crea una copia Snapshot del sistema di origine SAP, crea un volume FlexClone e lo monta sul sistema di destinazione SAP. Gli amministratori dello storage e SAP sanno come sviluppare script attivati da SnapCenter ed eseguiti dall'agente SnapCenter per automatizzare le attività quotidiane ricorrenti. Questa architettura accoppiata in modo lasco, che attiva le attività SnapCenter tramite script shell, consente loro di riutilizzare le procedure di automazione esistenti per ottenere i risultati desiderati più rapidamente utilizzando ALPACA come motore del flusso di lavoro per l'automazione end-to-end.

Conclusione

La combinazione di ALPACA e della tecnologia di gestione dei dati NetApp offre una potente soluzione che può ridurre drasticamente il tempo e l'impegno richiesti per i task più complessi e dispendiosi in termini di tempo correlati all'amministrazione del sistema SAP. Questa combinazione può anche aiutare a evitare la deriva di configurazione che l'errore umano può causare tra i sistemi.

Poiché i refresh del sistema, le copie, i cloni e i test di disaster recovery sono procedure molto sensibili, l'implementazione di una soluzione di questo tipo può liberare tempo prezioso da dedicare all'amministrazione. Può inoltre rafforzare la fiducia che i membri del personale line-of-business hanno negli amministratori di sistema SAP. Il team verificherà quanto tempo per la risoluzione dei problemi può essere risparmiato e quanto è più semplice copiare i sistemi per i test o per altri scopi. Questo vale indipendentemente da dove vengono gestiti i sistemi di origine e destinazione: On-premise, in un cloud pubblico, cloud ibrido o multicloud ibrido.

Dove trovare ulteriori informazioni

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

- "ALPACA"
- "Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter"
- "API REST supportate per server e plug-in SnapCenter"

Cronologia delle versioni

Versione	Data	Riepilogo degli aggiornamenti
Versione 0,1	04,2024	1st bozza.
Versione 0,2	06,2024	Convertito in formato html

SB-4294: Automazione dei flussi di lavoro di copia, refresh e cloning del sistema SAP con Avantra e NetApp SnapCenter

Questo documento descrive come Avantra si integra con la piattaforma NetApp SnapCenter®.

Panoramica della soluzione

Le operazioni dei sistemi e delle soluzioni SAP sono molto complesse. Tuttavia, per le aziende che utilizzano SAP, questi sistemi e servizi sono fondamentali per i loro processi aziendali. Grazie all'automazione delle attività operative quotidiane ricorrenti, come le operazioni di copia del sistema e refresh, gli amministratori di sistema SAP possono gestire più sistemi con meno sforzo, produrre risultati ripetibili e ridurre l'errore umano.

Questo documento si concentra sull'integrazione delle tecnologie NetApp® Snapshot™ e FlexClone® nei flussi di lavoro di automazione Avantra. Avantra è una piattaforma di gestione IT incentrata sulla gestione automatizzata delle operazioni e dei servizi IT. Fornisce soluzioni per il monitoraggio, l'automazione e la gestione delle infrastrutture IT per migliorare l'efficienza e l'affidabilità dei sistemi IT. Avantra consente alle aziende di monitorare in modo proattivo i propri ambienti IT, rilevare tempestivamente i problemi ed eseguire azioni automatizzate per la risoluzione dei problemi o l'ottimizzazione delle prestazioni del sistema. La

piattaforma si integra di norma con altri tool di gestione dell'IT ed è implementabile in vari ambienti come cloud, on-premise e infrastrutture ibride.

Questo documento descrive come Avantra si integra con la piattaforma NetApp SnapCenter®. NetApp SnapCenter è il tool per l'orchestrazione di backup basati su Snapshot, l'esecuzione di ripristini e la creazione di volumi FlexClone. Questa integrazione consente agli amministratori SAP di accelerare significativamente i task operativi quotidiani per i sistemi SAP utilizzando le tecniche NetApp. Snapshot, FlexClone e NetApp SnapRestore® accelerano le operazioni di backup, ripristino e clonazione, perché la tecnologia di storage NetApp è basata sul puntatore. Questo approccio è veloce. Riduce inoltre l'overhead dello storage durante le operazioni di cloning, perché sul supporto storage vengono scritti solo i dati nuovi e modificati, indipendentemente dal fatto che si tratti di un sistema storage NetApp on-premise o di una soluzione storage NetApp presso uno dei tre principali cloud provider.

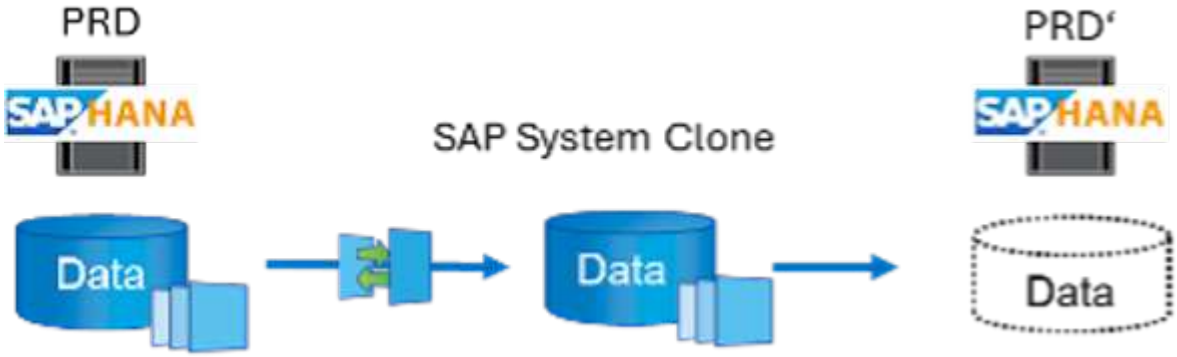
Pubblico di riferimento

Questo documento è rivolto agli amministratori di sistema SAP che hanno precedentemente eseguito copie di sistema SAP manualmente e desiderano automatizzare questa attività con Avantra. L'obiettivo della combinazione delle tecnologie Snapshot di NetApp e FlexClone, orchestrata da NetApp SnapCenter, con i workflow Avantra è quello di accelerare le copie di sistema SAP automatizzandole completamente.

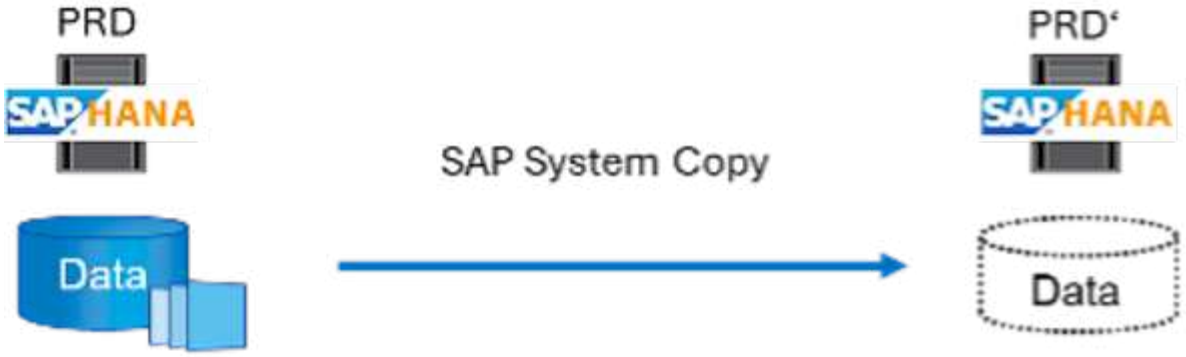
Scenari di cloning, copia e refresh del sistema SAP

Il termine copia del sistema SAP viene spesso utilizzato come termine generale per tre processi diversi: Clone del sistema SAP, copia del sistema SAP e refresh del sistema SAP. È importante distinguere tra le diverse operazioni, poiché i flussi di lavoro e i casi di utilizzo sono diversi.

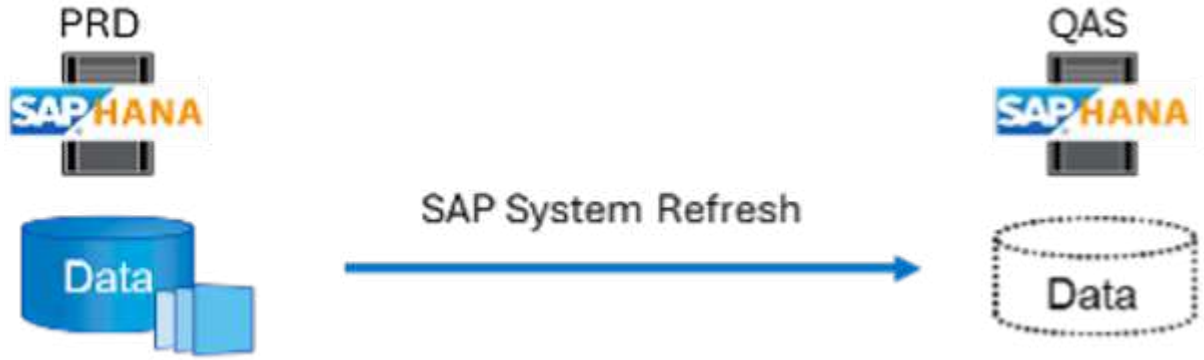
- **Clone del sistema SAP**. Un clone del sistema SAP è un clone identico di un sistema SAP di origine. I cloni di sistema SAP vengono in genere utilizzati per affrontare la corruzione logica o per testare gli scenari di disaster recovery. Con un'operazione di clonazione del sistema, il nome host, il numero di istanza e l'identificatore sicuro (SID) rimangono invariati. È quindi importante stabilire un corretto scherma di rete per il sistema di destinazione per assicurarsi che non vi sia comunicazione con l'ambiente di produzione.



- **Copia del sistema SAP**. Una copia del sistema SAP è il setup di un nuovo sistema SAP di destinazione con dati provenienti da un sistema SAP di origine. Ad esempio, il sistema di destinazione potrebbe essere un sistema di test aggiuntivo con dati provenienti dal sistema di produzione. Il nome host, il numero di istanza e il SID sono diversi per i sistemi di origine e di destinazione. Il nuovo sistema non è isolato dal sistema di origine.



- **Aggiornamento del sistema SAP.** Un refresh di sistema SAP è un refresh di un sistema SAP di destinazione esistente con dati provenienti da un sistema SAP di origine. Il sistema di destinazione fa generalmente parte di un ambiente di trasporto SAP, ad esempio un sistema sandbox, aggiornato con i dati del sistema di produzione. Il nome host, il numero di istanza e il SID sono diversi per il sistema di origine e di destinazione.



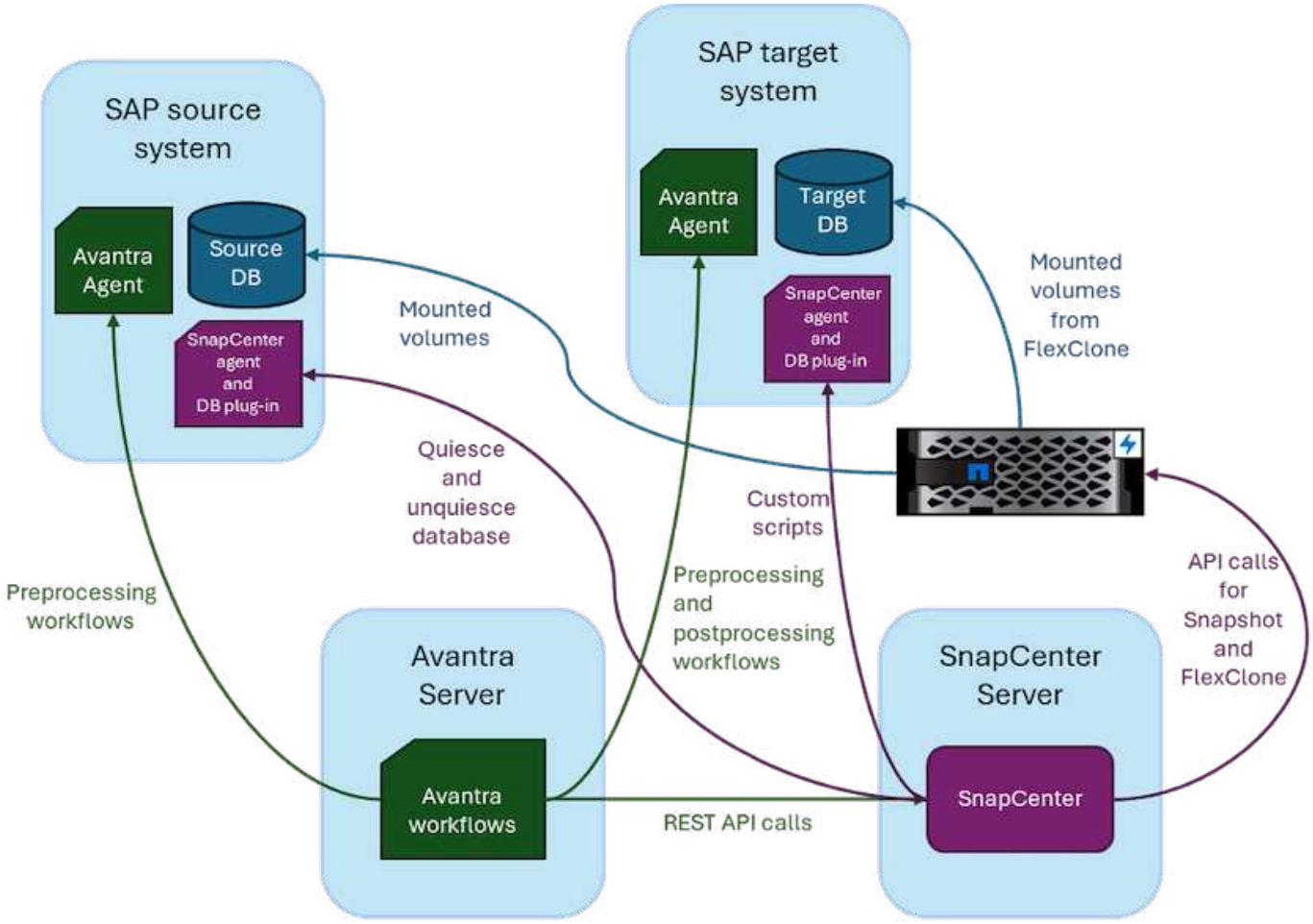
Anche se abbiamo tre casi di utilizzo diversi, il processo di gestione dei dati rimane invariato. Tutti e tre i casi d’utilizzo sfruttano la stessa tecnologia sottostante per la gestione dei dati, ovvero Snapshot di NetApp e FlexClone.

Tecnologia della soluzione

La soluzione globale è costituita dai seguenti componenti principali:

- Sistema di origine SAP con agente SnapCenter installato e plug-in del database SnapCenter
- Sistema di destinazione SAP con agente SnapCenter installato e plug-in del database SnapCenter
- Sistema Avantra con sorgente SAP configurata e sistema di destinazione SAP
- Server NetApp SnapCenter
- Sistema storage NetApp:
  - Hardware fisico on-premise: Serie NetApp AFF A, AFF C-Series, ASA A-Series, ASA C-Series o FAS
  - Storage software-defined on Premises: NetApp ONTAP® Select
  - Cloud storage NetApp:
    - NetApp Cloud Volumes ONTAP® in AWS, Google Cloud o Azure
    - Azure NetApp Files
    - Amazon FSX per NetApp ONTAP (AWS)

L’immagine seguente mostra il server Avantra, il server NetApp SnapCenter, il sistema di storage NetApp, i sistemi di origine SAP e di destinazione SAP e il modo in cui tutto si integra. L’obiettivo era rendere l’integrazione il più flessibile possibile utilizzando l’API REST SnapCenter per il massimo riutilizzo del lavoro di configurazione già eseguito all’interno dei componenti esistenti.

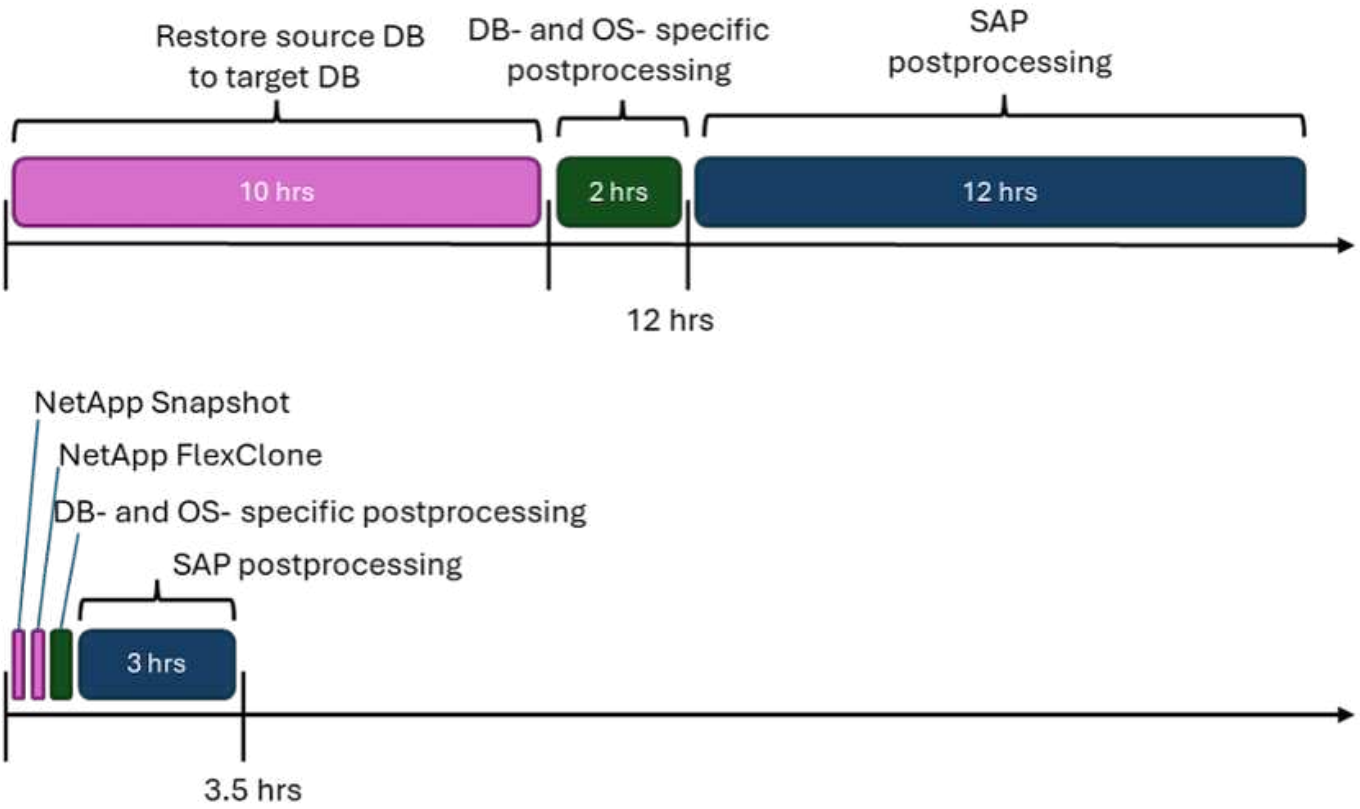


Riepilogo del caso d’utilizzo

Esistono diversi scenari in cui i dati di un sistema di origine devono essere resi disponibili a un sistema di destinazione per scopi di test o formazione. Questi sistemi di test e formazione devono essere aggiornati regolarmente con i dati del sistema di origine per assicurarsi che i test e la formazione vengano eseguiti con il set di dati corrente. Queste operazioni di refresh del sistema sono costituite da più task a livello di infrastruttura, database e applicazione e possono richiedere diversi giorni, in base al livello di automazione.

Per ridurre i tempi, automatizzare le attività operative ed eliminare gli errori umani a livello di infrastruttura, database e applicazione, puoi utilizzare i workflow Avantra. Invece di ripristinare un backup dal sistema di origine al sistema di destinazione, un processo dispendioso in termini di tempo e che comporta un consumo elevato delle risorse, questa integrazione utilizza le copie Snapshot di NetApp e la tecnologia FlexClone. Tutte le attività necessarie per accelerare un database vengono completate in pochi minuti anziché in ore. Il tempo richiesto dal processo di clonazione non dipende dalle dimensioni del database; pertanto, in pochi minuti è possibile creare anche sistemi molto grandi. Avantra riduce ulteriormente i tempi di esecuzione automatizzando i task a livello di sistema operativo e database e sul lato di post-elaborazione SAP.

L’immagine seguente mostra i possibili miglioramenti dell’efficienza operativa quando si utilizza l’automazione.



Integrare i diversi componenti tecnologici

L'effettiva integrazione di SnapCenter in un flusso di lavoro Avantra consiste nell'utilizzo di JavaScript per accedere all'API REST NetApp SnapCenter. Questa integrazione REST API-based crea una copia Snapshot del sistema di origine SAP, crea un volume FlexClone e lo monta sul sistema di destinazione SAP.

Gli amministratori dello storage e SAP hanno investito tempo e know-how nello sviluppo di script attivati da SnapCenter ed eseguiti dall'agente SnapCenter per automatizzare le attività quotidiane che si ripetono. Questa architettura, che utilizza JavaScript per attivare le attività SnapCenter, consente loro di riutilizzare le procedure di automazione esistenti per ottenere i risultati desiderati più rapidamente utilizzando Avantra come motore del flusso di lavoro per l'automazione end-to-end.

Conclusione

La combinazione della tecnologia di gestione dei dati Avantra e NetApp offre una soluzione potente che può ridurre drasticamente i tempi e gli sforzi necessari per le attività più complesse e dispendiose in termini di tempo legate all'amministrazione dei sistemi SAP. Questa combinazione può anche aiutare a evitare la deriva di configurazione che l'errore umano può causare tra i sistemi.

Poiché i refresh del sistema, le copie, i cloni e i test di disaster recovery sono procedure molto sensibili, l'implementazione di una soluzione di questo tipo può liberare tempo prezioso da dedicare all'amministrazione. Può inoltre rafforzare la fiducia che i membri del personale delle linee di business hanno negli amministratori di sistema SAP: Vedranno quanto tempo per la risoluzione dei problemi può essere risparmiato e quanto è più facile copiare i sistemi per test o altri scopi. La soluzione offre questi vantaggi indipendentemente da dove vengono utilizzati i sistemi di origine e destinazione: On-premise, in un cloud pubblico o in un ambiente multicloud ibrido o ibrido.

Dove trovare ulteriori informazioni

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

- "Avantra"
- "Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter"
- "API REST supportate per il server e i plug-in SnapCenter"

Cronologia delle versioni

Versione	Data	Riepilogo degli aggiornamenti
Versione 0,1	03,2024	1st bozza.
Versione 0,2	03,2024	Integrazione del feedback dei colleghi NetApp.
Versione 0,3	04,2024	Modifiche richieste integrate per essere conformi al branding NetApp
Versione 0,4	06,2024	Convertito in formato html

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.