



# **Backup e ripristino della replica del sistema SAP HANA con SnapCenter**

NetApp Solutions SAP

NetApp  
March 11, 2024

This PDF was generated from <https://docs.netapp.com/it-it/netapp-solutions-sap/backup/saphana-sr-scs-sap-hana-system-replication-overview.html> on March 11, 2024. Always check docs.netapp.com for the latest.

# Sommario

- Backup e ripristino della replica del sistema SAP HANA con SnapCenter ..... 1
  - TR-4719: Replica del sistema SAP HANA - Backup e ripristino con SnapCenter ..... 1
  - Backup Snapshot dello storage e replica del sistema SAP ..... 2
  - Opzioni di configurazione SnapCenter per la replica del sistema SAP ..... 4
  - Configurazione di SnapCenter 4.6 mediante un gruppo di risorse ..... 5
  - Configurazione di SnapCenter con una singola risorsa ..... 16
  - Ripristino e ripristino da un backup creato sull'altro host ..... 29
  - Dove trovare ulteriori informazioni ..... 34
  - Cronologia delle versioni ..... 34

# Backup e ripristino della replica del sistema SAP HANA con SnapCenter

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

Nils Bauer, NetApp

SAP HANA System Replication viene comunemente utilizzato come soluzione ad alta disponibilità o di disaster recovery per i database SAP HANA. SAP HANA System Replication offre diverse modalità operative che è possibile utilizzare in base al caso d'utilizzo o ai requisiti di disponibilità.

È possibile combinare due casi di utilizzo principali:

- Alta disponibilità con un obiettivo del punto di ripristino (RPO) pari a zero e un obiettivo RTO (Recovery Time Objective) minimo utilizzando un host SAP HANA secondario dedicato.
- Disaster recovery su larga distanza. L'host SAP HANA secondario può essere utilizzato anche per lo sviluppo o il test durante il normale funzionamento.

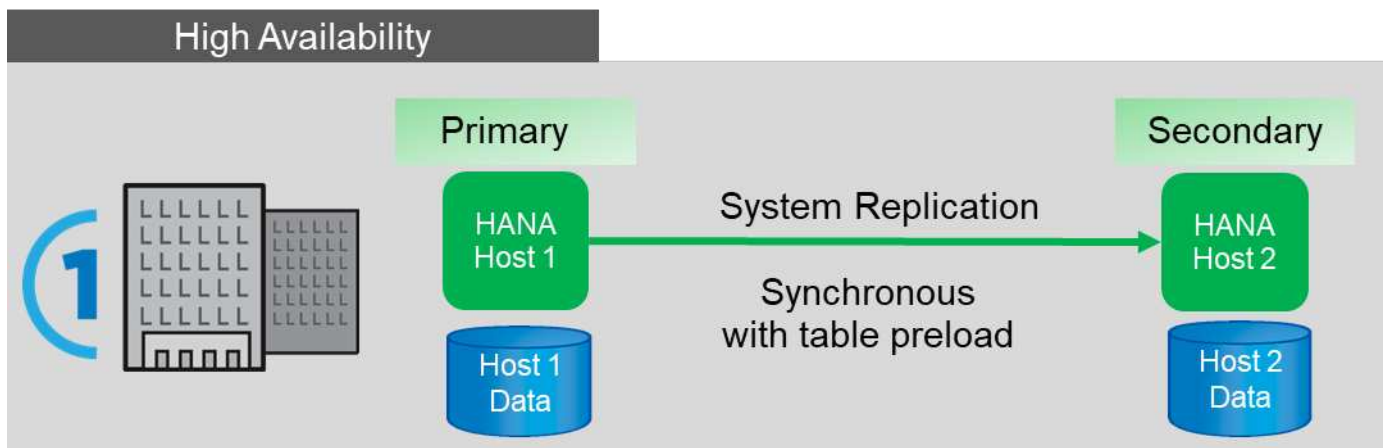
### Alta disponibilità con un RPO pari a zero e un RTO minimo

La replica di sistema viene configurata con la replica sincrona utilizzando tabelle precaricate in memoria sull'host SAP HANA secondario. Questa soluzione ad alta disponibilità può essere utilizzata per risolvere i guasti hardware o software e per ridurre i downtime pianificati durante gli aggiornamenti del software SAP HANA (operazioni di downtime quasi pari a zero).

Le operazioni di failover vengono spesso automatizzate utilizzando software di cluster di terze parti o con un semplice clic del workflow con il software SAP Landscape Management.

Dal punto di vista dei requisiti di backup, devi essere in grado di creare backup indipendenti dall'host SAP HANA principale o secondario. Un'infrastruttura di backup condivisa viene utilizzata per ripristinare qualsiasi backup, indipendentemente dall'host su cui è stato creato il backup.

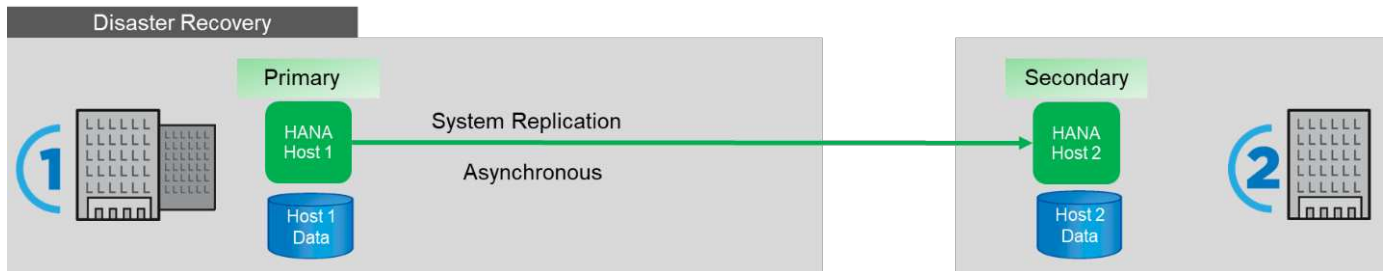
Il resto di questo documento si concentra sulle operazioni di backup con la replica del sistema SAP configurata come soluzione ad alta disponibilità.



## Disaster recovery su larga distanza

La replica del sistema può essere configurata con una replica asincrona senza alcuna tabella precaricata nella memoria dell'host secondario. Questa soluzione viene utilizzata per risolvere i guasti del data center e le operazioni di failover vengono in genere eseguite manualmente.

Per quanto riguarda i requisiti di backup, è necessario essere in grado di creare backup durante il normale funzionamento nel data center 1 e durante il disaster recovery nel data center 2. Nei data center 1 e 2 è disponibile un'infrastruttura di backup separata e le operazioni di backup vengono attivate come parte del disaster failover. L'infrastruttura di backup in genere non è condivisa e non è possibile eseguire un'operazione di ripristino di un backup creato nell'altro data center.



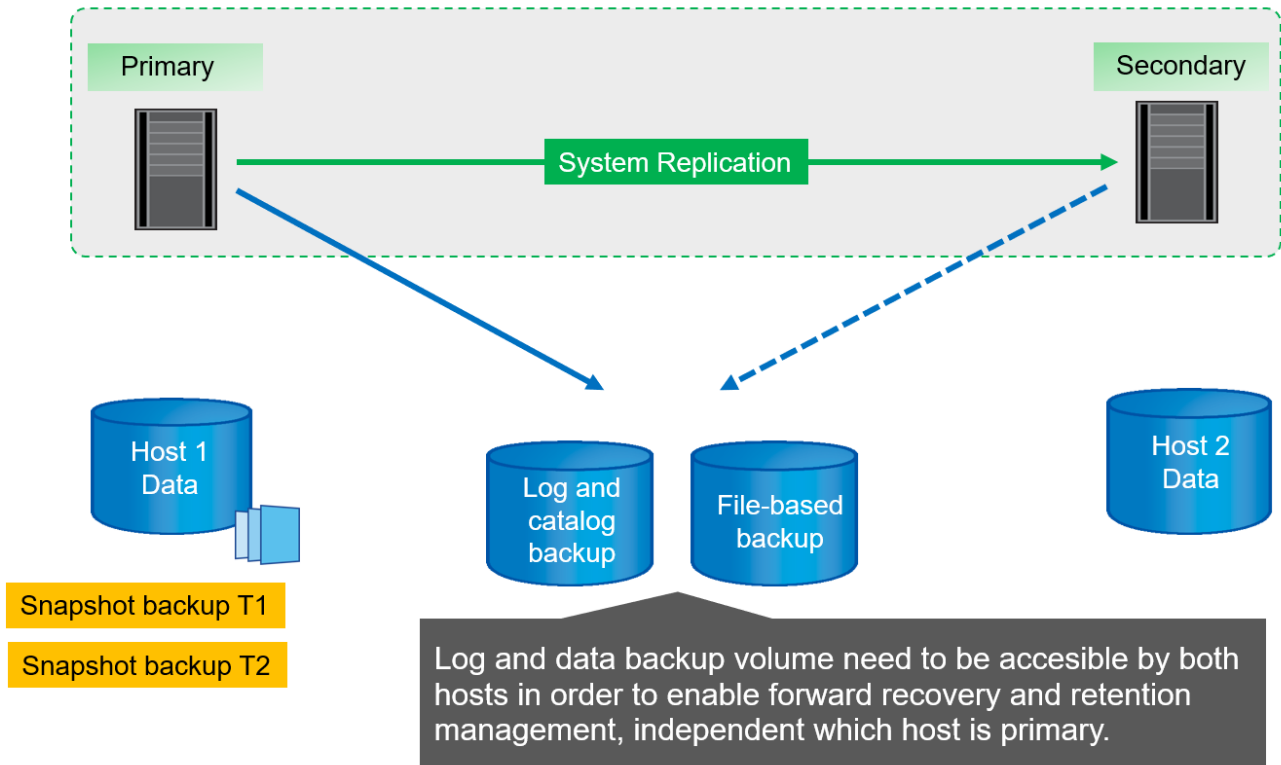
## Backup Snapshot dello storage e replica del sistema SAP

Le operazioni di backup vengono sempre eseguite sull'host SAP HANA primario. I comandi SQL richiesti per l'operazione di backup non possono essere eseguiti sull'host SAP HANA secondario.

Per le operazioni di backup SAP HANA, gli host SAP HANA primari e secondari sono una singola entità. Condividono lo stesso catalogo di backup SAP HANA e utilizzano i backup per il ripristino, indipendentemente dal fatto che il backup sia stato creato nell'host SAP HANA primario o secondario.

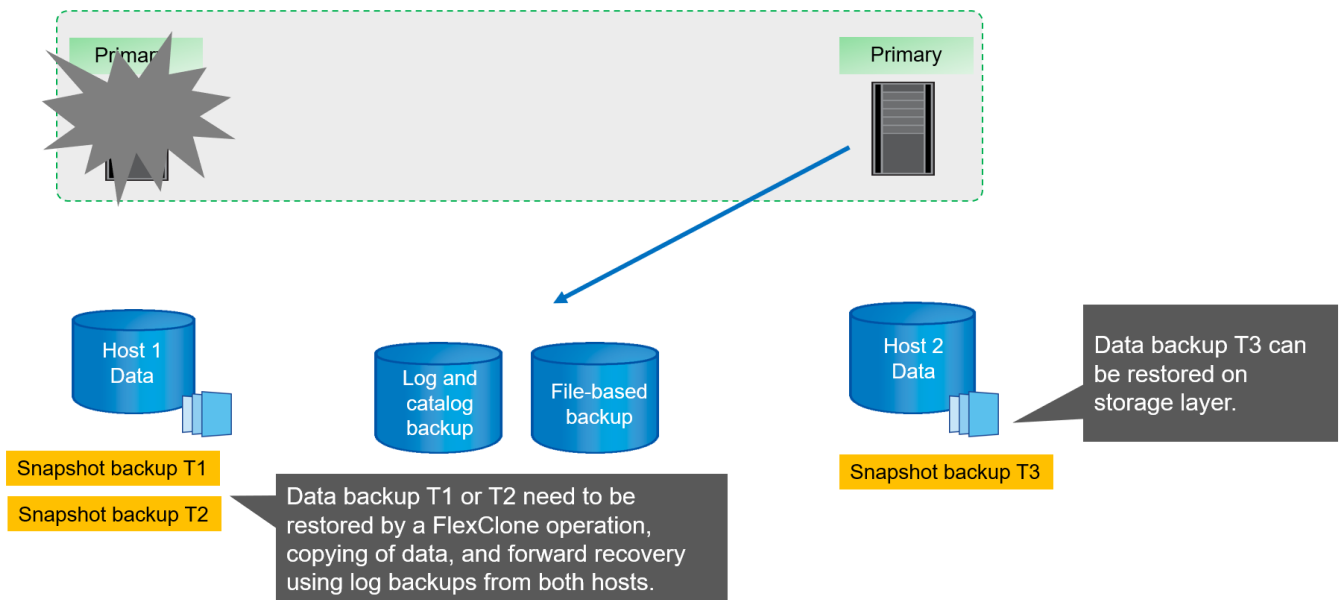
La possibilità di utilizzare qualsiasi backup per il ripristino e l'inoltro del ripristino utilizzando i backup dei log da entrambi gli host richiede una posizione di backup dei log condivisa accessibile da entrambi gli host. NetApp consiglia di utilizzare un volume di storage condiviso. Tuttavia, occorre anche separare la destinazione di backup del log in sottodirectory all'interno del volume condiviso.

Ogni host SAP HANA dispone di un proprio volume di storage. Quando si utilizza un'istantanea basata su storage per eseguire un backup, viene creata un'istantanea coerente con il database sul volume di storage dell'host SAP HANA primario.



Quando viene eseguito un failover sull'host 2, l'host 2 diventa l'host primario, i backup vengono eseguiti sull'host 2 e i backup Snapshot vengono creati sul volume di storage dell'host 2.

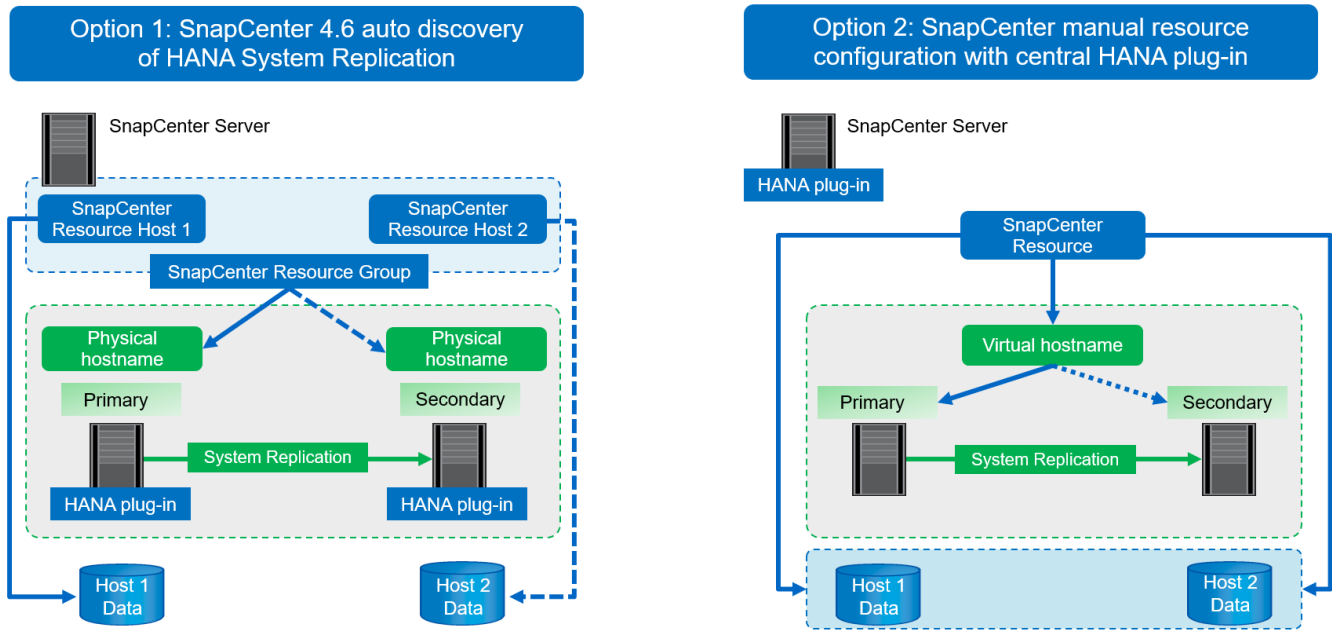
Il backup creato sull'host 2 può essere ripristinato direttamente al livello di storage. Se è necessario utilizzare un backup creato sull'host 1, il backup deve essere copiato dal volume di storage dell'host 1 al volume di storage dell'host 2. Forward Recovery utilizza i backup dei log di entrambi gli host.



# Opzioni di configurazione SnapCenter per la replica del sistema SAP

Sono disponibili due opzioni per la configurazione della protezione dei dati con il software NetApp SnapCenter in un ambiente di replica del sistema SAP HANA:

- Un gruppo di risorse SnapCenter che include host SAP HANA e il rilevamento automatico con SnapCenter versione 4.6 o superiore.
- Una singola risorsa SnapCenter per entrambi gli host SAP HANA che utilizzano un indirizzo IP virtuale.



A partire da SnapCenter 4.6, SnapCenter supporta il rilevamento automatico dei sistemi HANA configurati in una relazione di replica del sistema HANA. Ciascun host viene configurato utilizzando il proprio indirizzo IP fisico (nome host) e il proprio volume di dati sul layer di storage. Le due risorse SnapCenter sono combinate in un gruppo di risorse e SnapCenter identifica automaticamente l'host primario o secondario ed esegue le operazioni di backup richieste di conseguenza. La gestione della conservazione per Snapshot e backup basati su file creati da SnapCenter viene eseguita su entrambi gli host per garantire che i vecchi backup vengano cancellati anche sull'host secondario corrente.

Con una configurazione a singola risorsa per entrambi gli host SAP HANA, la singola risorsa SnapCenter viene configurata utilizzando l'indirizzo IP virtuale degli host di replica del sistema SAP HANA. Entrambi i volumi di dati degli host SAP HANA sono inclusi nella risorsa SnapCenter. Poiché si tratta di una singola risorsa SnapCenter, la gestione della conservazione per Snapshot e i backup basati su file creati da SnapCenter funziona indipendentemente dall'host attualmente primario o secondario. Queste opzioni sono possibili con tutte le versioni di SnapCenter.

La seguente tabella riassume le differenze principali delle due opzioni di configurazione.

	Gruppo di risorse con SnapCenter 4.6	Singola risorsa SnapCenter e indirizzo IP virtuale
Operazione di backup (Snapshot e basato su file)	Identificazione automatica dell'host primario nel gruppo di risorse	Utilizza automaticamente l'indirizzo IP virtuale

	Gruppo di risorse con SnapCenter 4.6	Singola risorsa SnapCenter e indirizzo IP virtuale
Gestione della conservazione (Snapshot e basato su file)	Eseguito automaticamente su entrambi gli host	Utilizza automaticamente una singola risorsa
Requisiti di capacità per il backup	I backup vengono creati solo sul volume host primario	I backup vengono sempre creati su entrambi i volumi host. Il backup del secondo host è coerente solo con il crash e non può essere utilizzato per eseguire un rollforward.
Ripristinare l'operazione	I backup dall'host attivo corrente sono disponibili per l'operazione di ripristino	Script di pre-backup necessario per identificare i backup validi e che possono essere utilizzati per il ripristino
Operazione di recovery	Tutte le opzioni di ripristino disponibili, come per qualsiasi risorsa rilevata automaticamente	Ripristino manuale richiesto



In generale, NetApp consiglia di utilizzare l'opzione di configurazione del gruppo di risorse con SnapCenter 4.6 per proteggere i sistemi HANA con la replica del sistema HANA abilitata. L'utilizzo di una singola configurazione delle risorse SnapCenter è necessario solo se l'approccio operativo SnapCenter è basato su un host plug-in centrale e il plug-in HANA non è distribuito sugli host del database HANA.

Le due opzioni sono descritte in dettaglio nelle sezioni seguenti.

## Configurazione di SnapCenter 4.6 mediante un gruppo di risorse

SnapCenter 4.6 supporta il rilevamento automatico per i sistemi HANA configurati con la replica del sistema HANA. SnapCenter 4.6 include la logica per identificare gli host HANA primari e secondari durante le operazioni di backup e gestisce anche la gestione della conservazione su entrambi gli host HANA. Inoltre, il ripristino e il ripristino automatici sono ora disponibili anche per gli ambienti di replica del sistema HANA.

### Configurazione di SnapCenter 4.6 per gli ambienti di replica del sistema HANA

La figura seguente mostra la configurazione di laboratorio utilizzata per questo capitolo. Due host HANA, hana-3 e hana-4, sono stati configurati con la replica di sistema HANA.

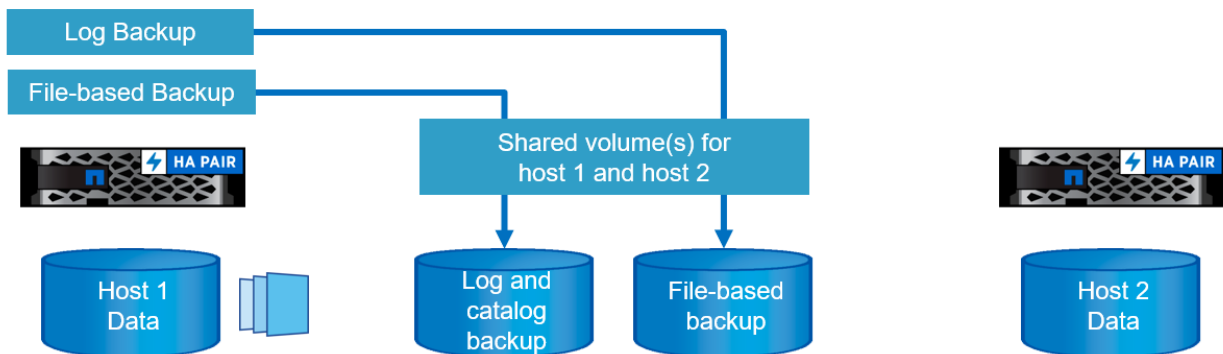
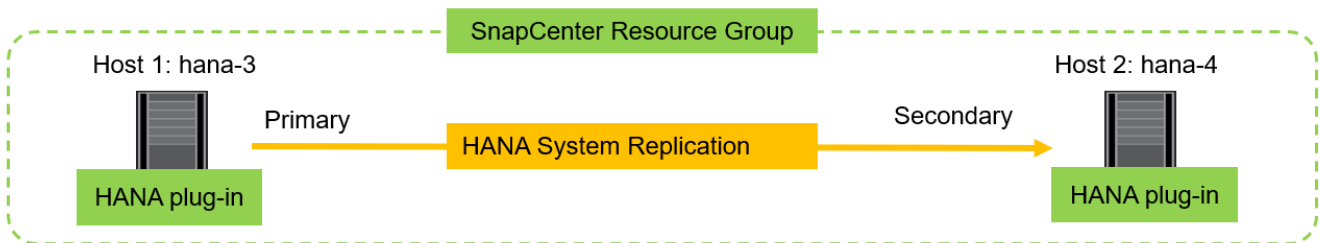
È stato creato un utente di database "SnapCenter" per il database di sistema HANA con i privilegi necessari per eseguire le operazioni di backup e ripristino (vedere ["Backup e ripristino SAP HANA con SnapCenter"](#)). È necessario configurare una chiave di memorizzazione utente HANA su entrambi gli host utilizzando l'utente del database indicato sopra.

```
ss2adm@hana- 3: / > hdbuserstore set SS2KEY hana- 3:33313 SNAPCENTER
<password>
```

```
ss2adm@hana- 4:/ > hdbuserstore set SS2KEY hana-4:33313 SNAPCENTER
<password>
```

Da un punto di vista di alto livello, è necessario eseguire i seguenti passaggi per configurare la replica del sistema HANA in SnapCenter.

1. Installare il plug-in HANA sull'host primario e secondario. Viene eseguita la rilevazione automatica e viene rilevato lo stato di replica del sistema HANA per ogni host primario o secondario.
2. Eseguire `SnapCenter configure database` e fornire il `hdbuserstore` chiave. Vengono eseguite ulteriori operazioni di rilevamento automatico.
3. Creare un gruppo di risorse, inclusi entrambi gli host e configurare la protezione.



Dopo aver installato il plug-in HANA di SnapCenter su entrambi gli host HANA, i sistemi HANA vengono visualizzati nella vista delle risorse di SnapCenter allo stesso modo delle altre risorse rilevate automaticamente. A partire da SnapCenter 4.6, viene visualizzata una colonna aggiuntiva che mostra lo stato della replica del sistema HANA (attivata/disattivata, primaria/secondaria).

NetApp SnapCenter®									
SAP HANA									
View: Multitenant Database Container Search databases									
Resources	System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
	SS2	SS2	SS2	Enabled (Primary)	hana-3.sapcc.stl.netapp.com				Not protected
	SS2	SS2	SS2	Enabled (Secondary)	hana-4.sapcc.stl.netapp.com				Not protected

Facendo clic sulla risorsa, SnapCenter richiede la chiave di archivio utente HANA per il sistema HANA.



Configure Database

Plug-in host

hana-3.sapcc.stl.netapp.com

HDBSQL OS User

ss2adm

HDB Secure User Store Key

SS2KEY

Cancel

OK

Vengono eseguite ulteriori operazioni di rilevamento automatico e SnapCenter mostra i dettagli delle risorse. In SnapCenter 4.6, lo stato della replica del sistema e il server secondario sono elencati in questa vista.

NetApp SnapCenter

SAP HANA

Search databases

System

SS2

SS2

Total 2

Resource - Details

Details for selected resource

Type

Multitenant Database Container

HANA System Name

SS2

SID

SS2

Tenant Databases

SS2

Plug-in Host

hana-3.sapcc.stl.netapp.com

HDB Secure User Store Key

SS2KEY

HDBSQL OS User

ss2adm

Log backup location

/mnt/backup/SS2

Backup catalog location

/mnt/backup/SS2

System Replication

Enabled (Primary)

Secondary Servers

hana-4

plug-in name

SAP HANA

Last backup

None

Resource Groups

None

Policy

None

Discovery Type

Auto

Storage Footprint

SVM	Volume	Junction Path	LUN/Qtree
hana-primary.sapcc.stl.netapp.com	SS2_data_mnt00001	/SS2_data_mnt00001	

Activity

The 5 most recent jobs are displayed

0 Completed

0 Warnings

0 Failed

0 Canceled

0 Running

0 Queued

Dopo aver eseguito le stesse operazioni per la seconda risorsa HANA, il processo di individuazione automatica è completo e entrambe le risorse HANA sono configurate in SnapCenter.

NetApp SnapCenter

SAP HANA

View Multitenant Database Container

Search databases

Resources

System

System ID (SID)

Tenant Databases

Replication

Plug-in Host

Resource Groups

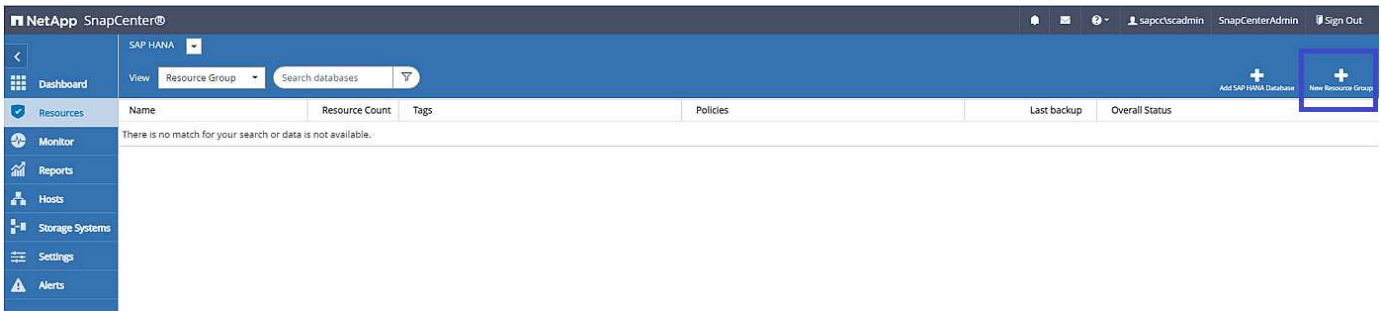
Policies

Last backup

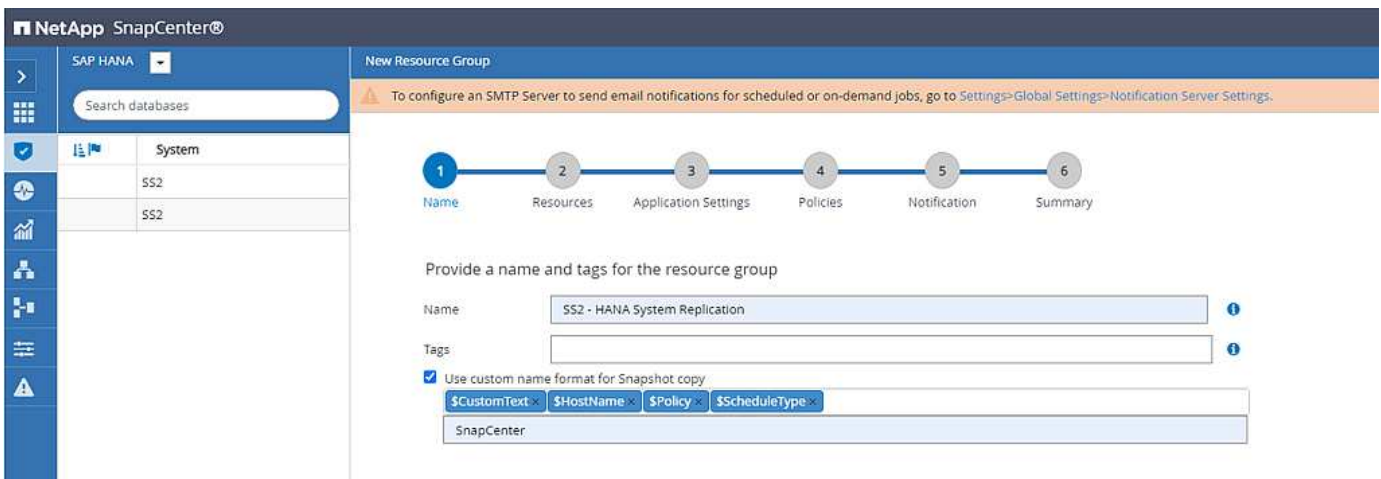
Overall Status

SS2	SS2	SS2	Enabled (Primary)	hana-3.sapcc.stl.netapp.com				Not protected
SS2	SS2	SS2	Enabled (Secondary)	hana-4.sapcc.stl.netapp.com				Not protected

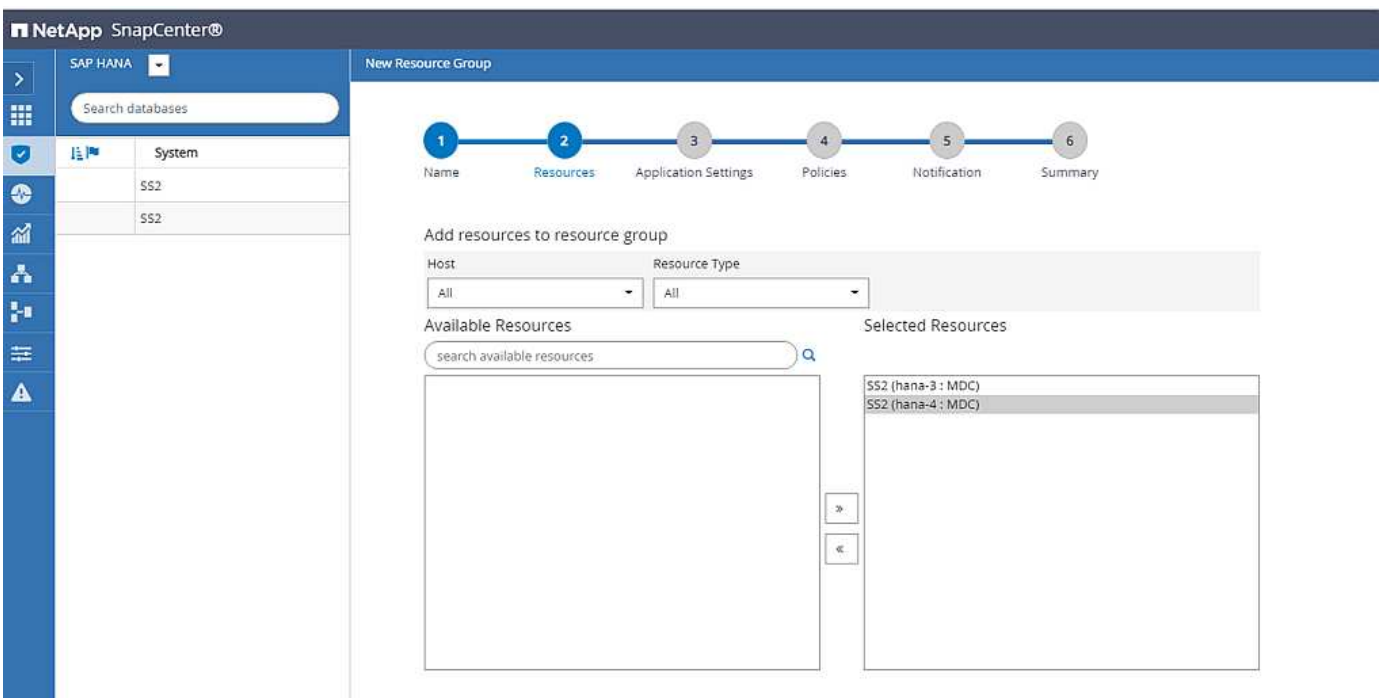
Per i sistemi abilitati alla replica del sistema HANA, è necessario configurare un gruppo di risorse SnapCenter, incluse entrambe le risorse HANA.



NetApp consiglia di utilizzare un formato nome personalizzato per il nome Snapshot, che deve includere il nome host, la policy e la pianificazione.



È necessario aggiungere entrambi gli host HANA al gruppo di risorse.



I criteri e le pianificazioni vengono configurati per il gruppo di risorse.



La conservazione definita nel criterio viene utilizzata in entrambi gli host HANA. Se, ad esempio, nel criterio viene definita una conservazione di 10, la somma dei backup di entrambi gli host viene utilizzata come criterio per l'eliminazione del backup. SnapCenter elimina il backup meno recente indipendentemente se è stato creato sull'host primario o secondario corrente.

NetApp SnapCenter®

SAP HANA

Search databases

Name

There is no match for your search or data is not available.

1 Name 2 Resources 3 Application Settings 4 Policies 5 Notification 6 Summary

Select one or more policies and configure schedules

LocalSnap

LocalSnap

BlockIntegrityCheck

Policy

Applied Schedules

Hourly: Repeat every 1 hours

Configure Schedules

Total 1

La configurazione del gruppo di risorse è terminata ed è possibile eseguire i backup.

NetApp SnapCenter®

SAP HANA

SS2 - HANA System Replication Details

Name	Resource Name	Type	Host
SS2 - HANA System Replication	SS2	MultipleContainers	hana-3.sapcc.stl.netapp.com
	SS2	MultipleContainers	hana-4.sapcc.stl.netapp.com

NetApp SnapCenter®

SAP HANA

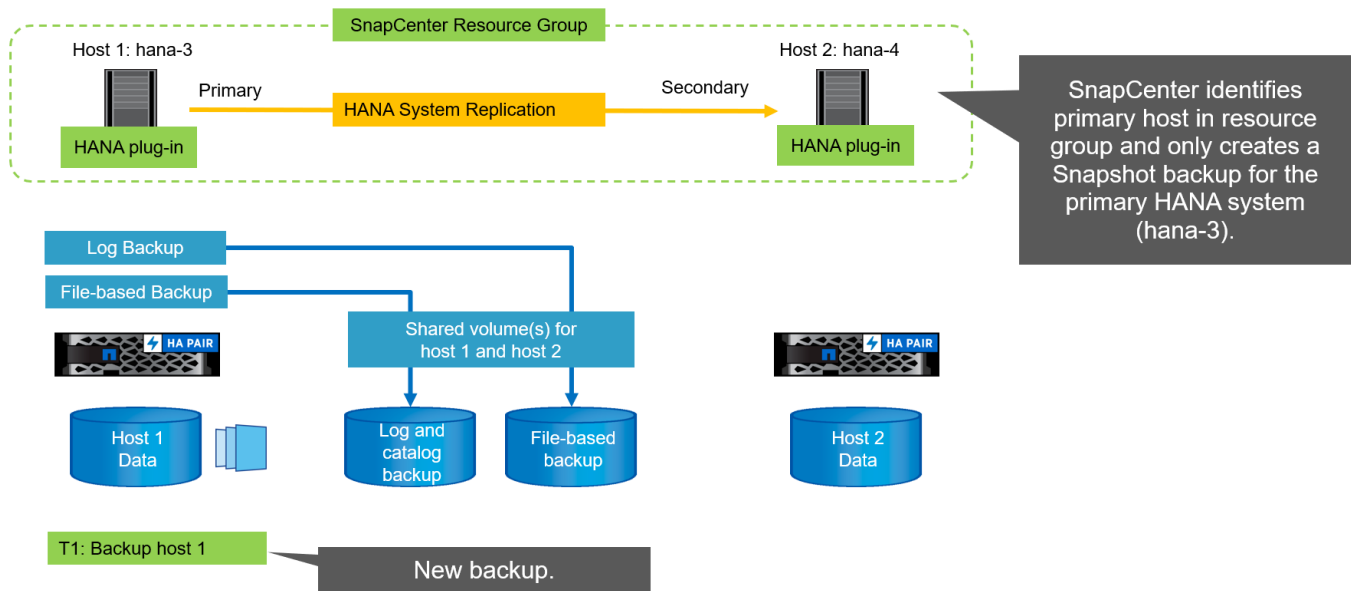
View: Multitenant Database Container

Search databases

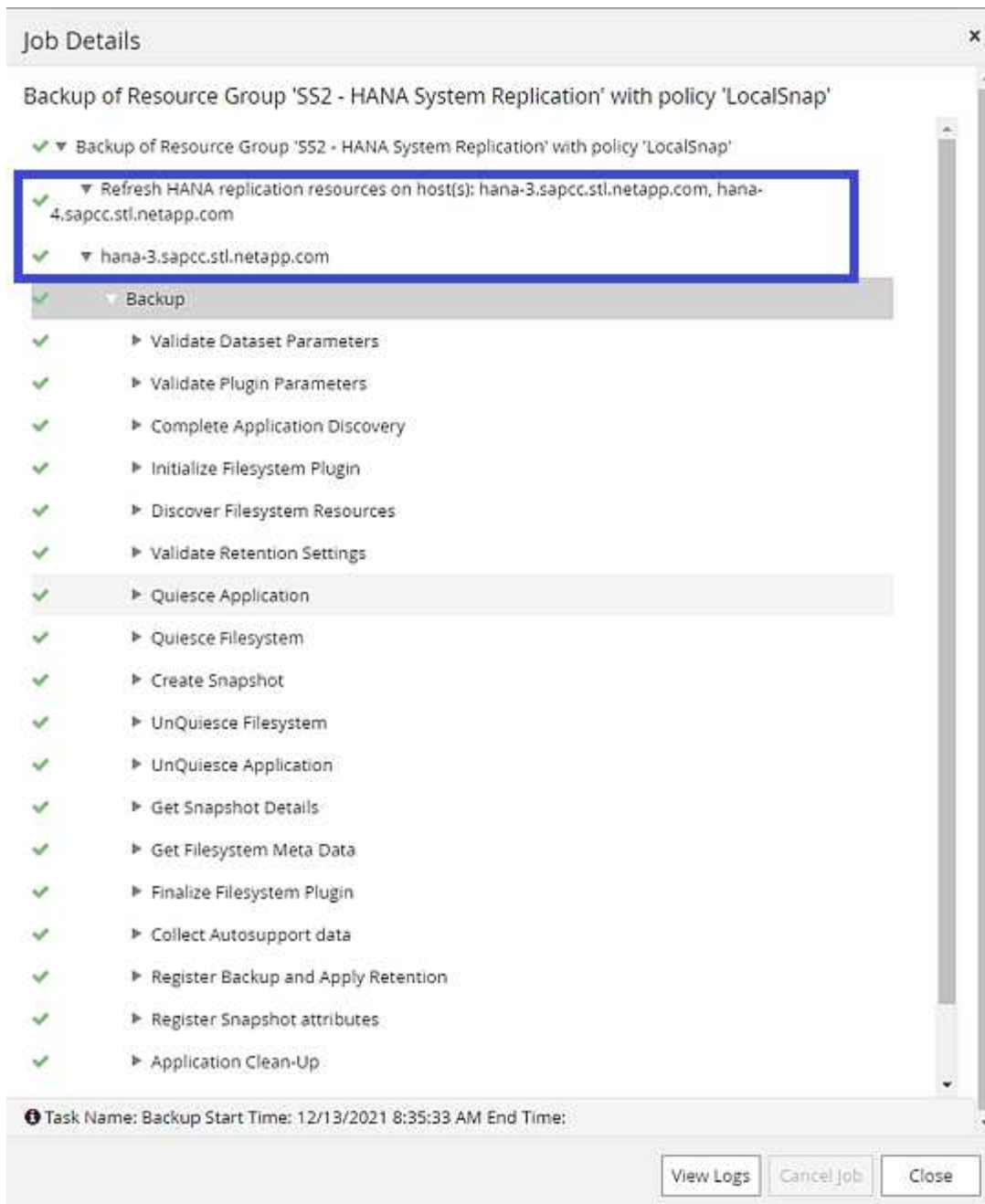
System	System ID (SID)	Tenant Databases	Replication	Plug-in Host	Resource Groups	Policies	Last backup	Overall Status
SS2	SS2	SS2	Enabled (Primary)	hana-3.sapcc.stl.netapp.com	SS2 - HANA System Replication	LocalSnap		Backup not run
SS2	SS2	SS2	Enabled (Secondary)	hana-4.sapcc.stl.netapp.com	SS2 - HANA System Replication	LocalSnap		Backup not run

## Operazioni di backup di Snapshot

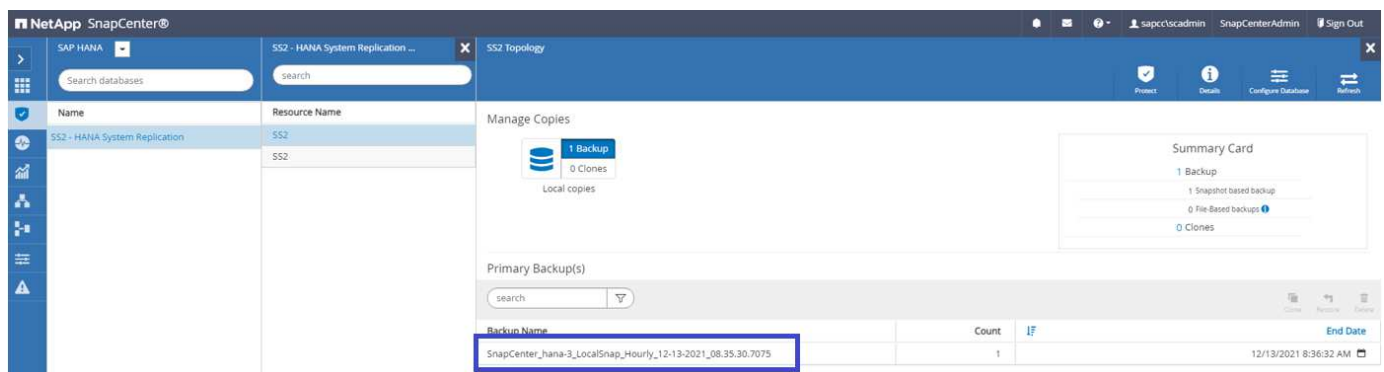
Quando viene eseguita un'operazione di backup del gruppo di risorse, SnapCenter identifica l'host primario e attiva un backup solo sull'host primario. In questo modo, verrà attivato lo snap-shoting solo del volume di dati dell'host primario. Nel nostro esempio, hana-3 è l'host primario corrente e viene eseguito un backup su questo host.



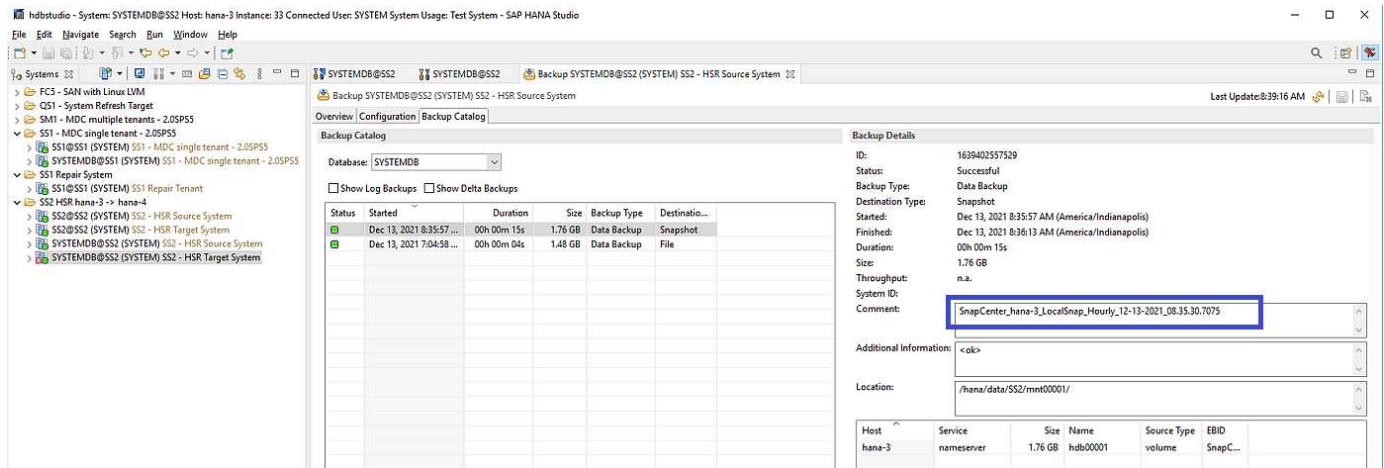
Il log dei lavori di SnapCenter mostra l'operazione di identificazione e l'esecuzione del backup sull'host primario corrente hana-3.



È stato creato un backup Snapshot nella risorsa HANA principale. Il nome host incluso nel nome del backup mostra hana-3.



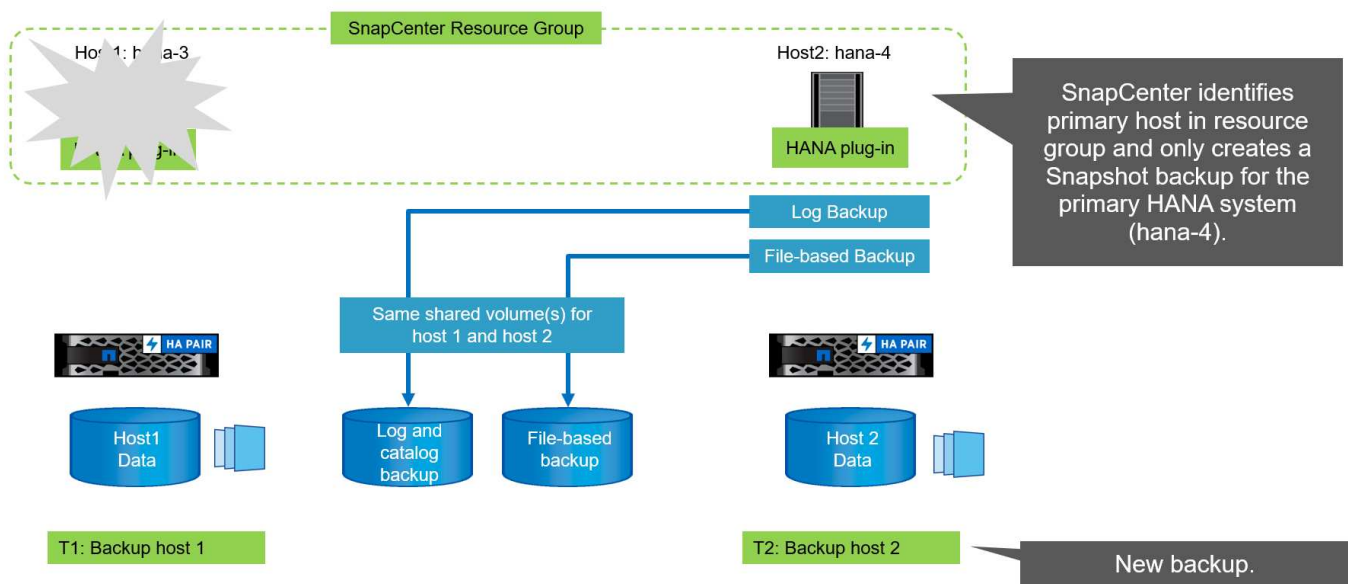
Lo stesso backup Snapshot è anche visibile nel catalogo di backup HANA.



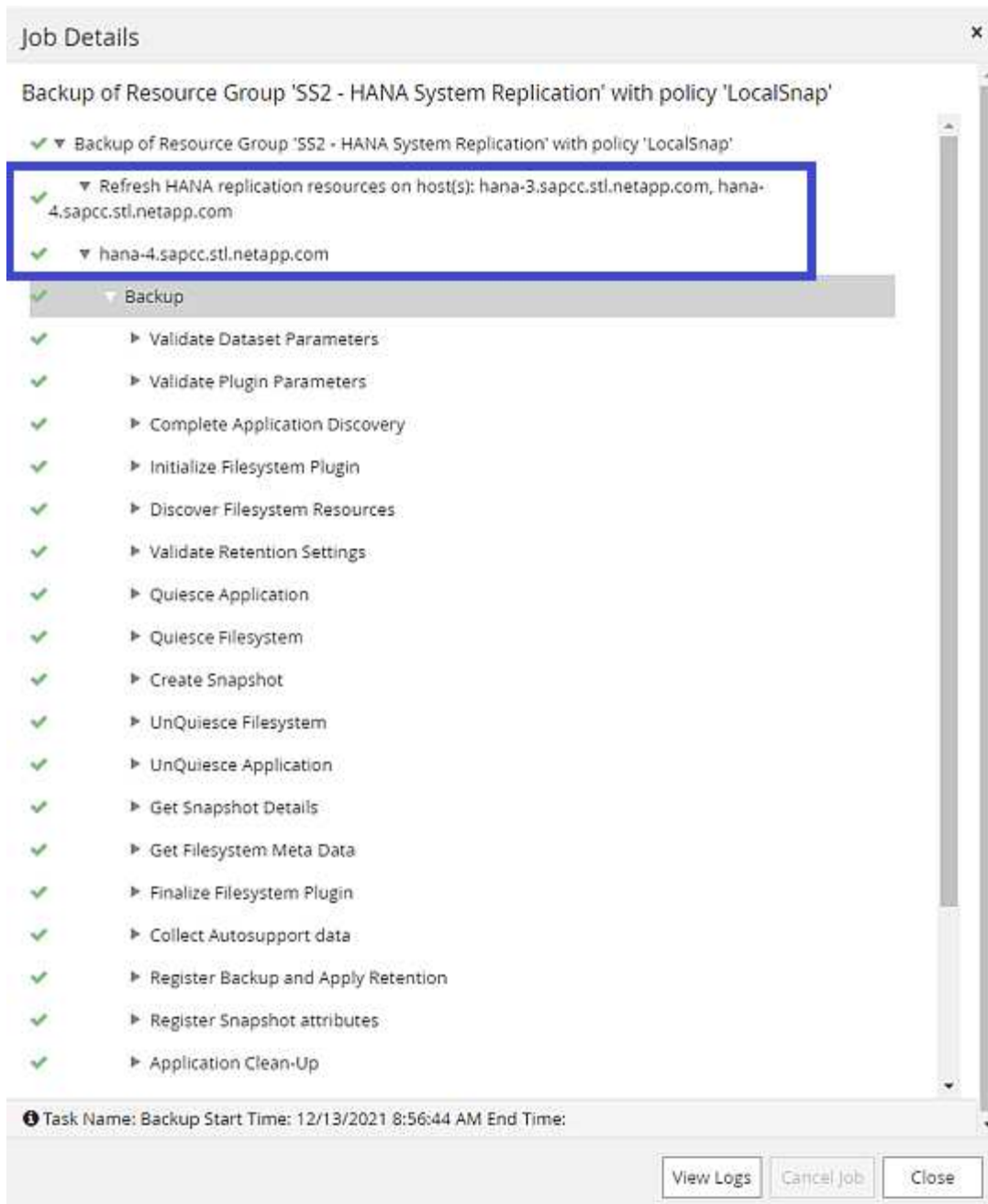
Se viene eseguita un'operazione di Takeover, ulteriori backup SnapCenter identificano ora il precedente host secondario (hana-4) come primario e l'operazione di backup viene eseguita in hana-4. Anche in questo caso, viene attivato solo il volume di dati del nuovo host primario (hana-4).



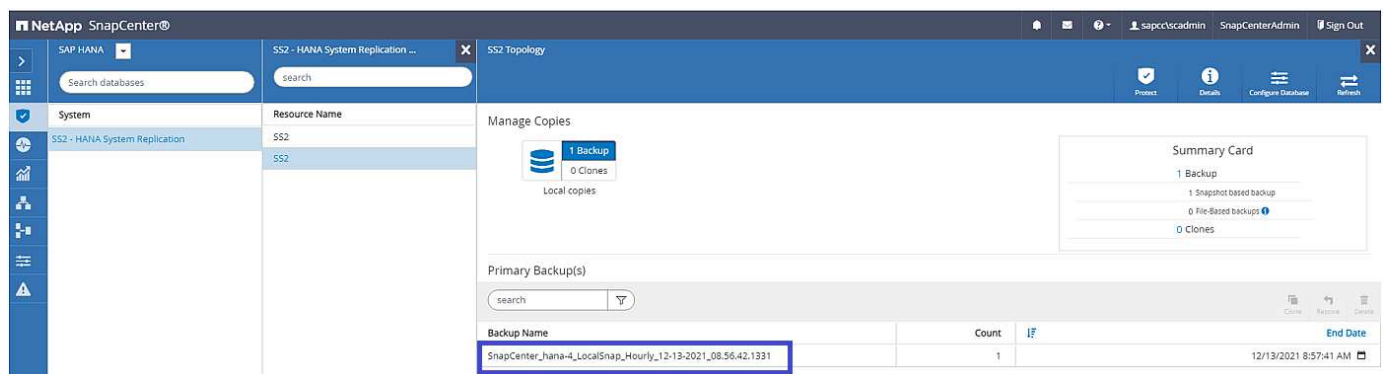
La logica di identificazione SnapCenter copre solo gli scenari in cui gli host HANA si trovano in una relazione primaria-secondaria o quando uno degli host HANA è offline.



Il log dei lavori di SnapCenter mostra l'operazione di identificazione e l'esecuzione del backup sull'host primario corrente hana-4.

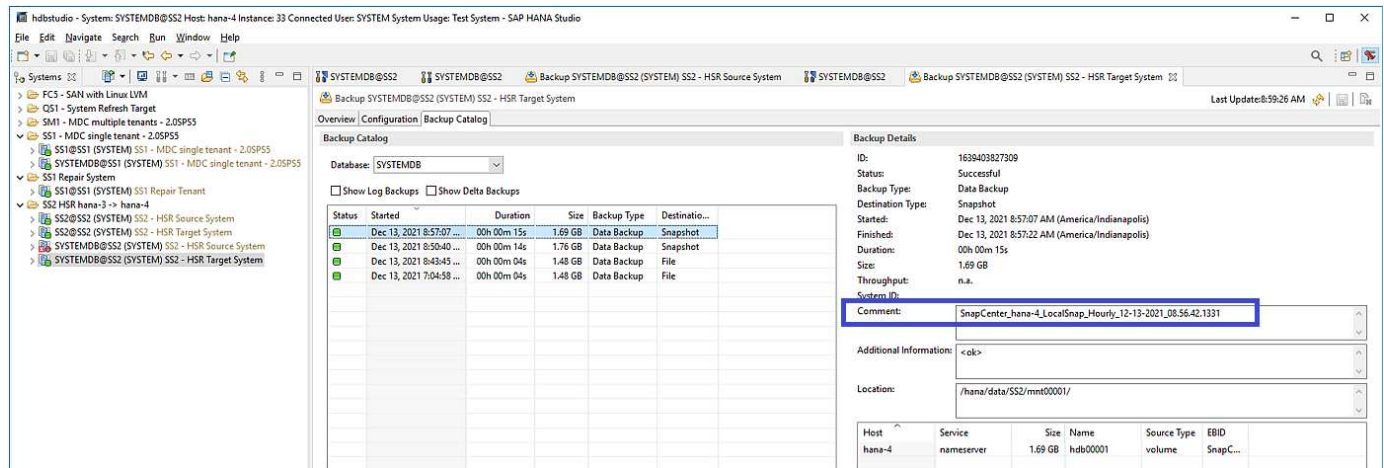


È stato creato un backup Snapshot nella risorsa HANA principale. Il nome host incluso nel nome del backup mostra hana-4.





Lo stesso backup Snapshot è anche visibile nel catalogo di backup HANA.



## Operazioni di controllo dell'integrità dei blocchi con backup basati su file

SnapCenter 4.6 utilizza la stessa logica descritta per le operazioni di backup Snapshot per le operazioni di controllo dell'integrità dei blocchi con backup basati su file. SnapCenter identifica l'host HANA primario corrente ed esegue il backup basato su file per questo host. La gestione della conservazione viene eseguita anche su entrambi gli host, in modo che il backup più vecchio venga cancellato indipendentemente dall'host attualmente primario.

## Replica SnapVault

Per consentire operazioni di backup trasparenti senza l'interazione manuale in caso di Takeover e indipendentemente da quale host HANA sia attualmente l'host primario, è necessario configurare una relazione SnapVault per i volumi di dati di entrambi gli host. SnapCenter esegue un'operazione di aggiornamento del SnapVault per l'host primario corrente ad ogni esecuzione del backup.



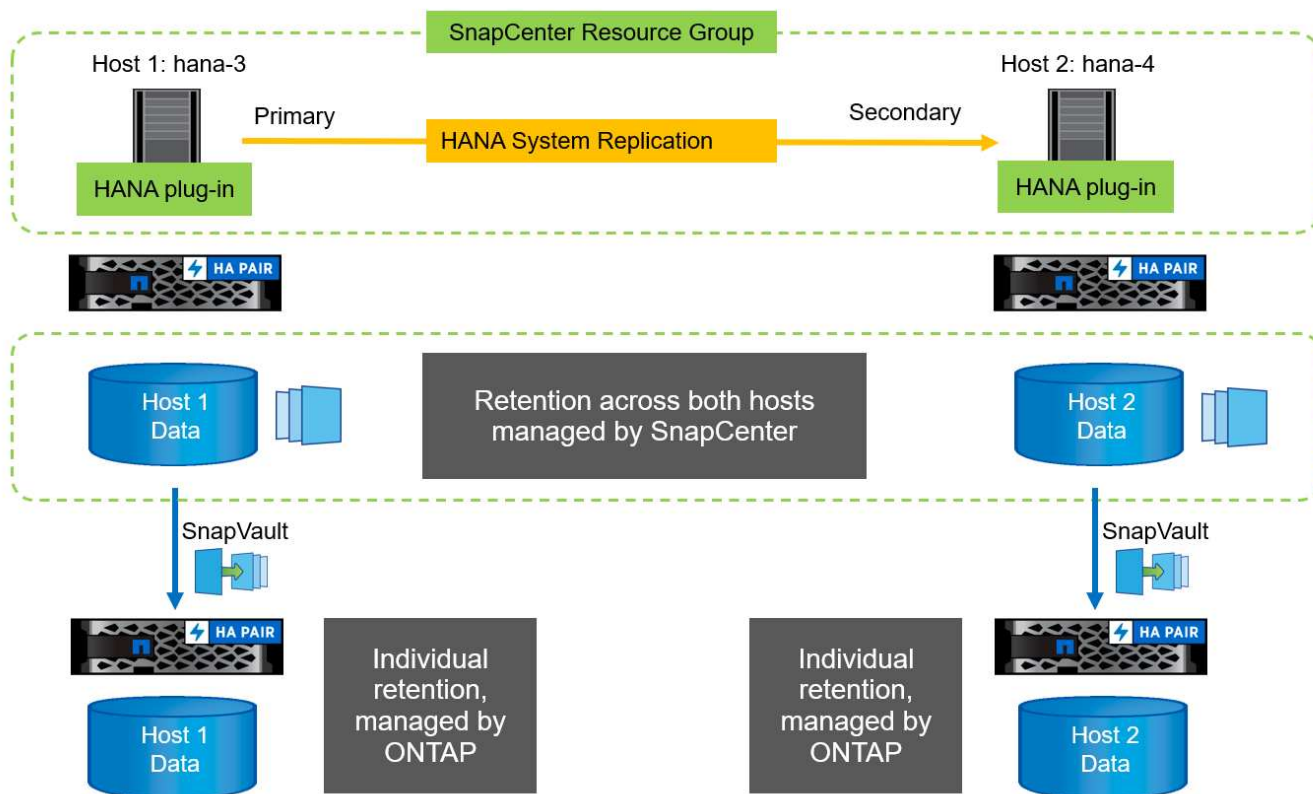
Se un takeover all'host secondario non viene eseguito per molto tempo, il numero di blocchi modificati per il primo aggiornamento SnapVault sull'host secondario sarà elevato.

Poiché la gestione della conservazione presso la destinazione SnapVault viene gestita da ONTAP al di fuori di SnapCenter, la conservazione non può essere gestita su entrambi gli host HANA. Pertanto, i backup creati prima di un Takeover non vengono cancellati con le operazioni di backup sul precedente secondario. Questi backup rimangono fino a quando il primo primario non diventa nuovamente primario. Affinché questi backup non blocchino la gestione della conservazione dei backup dei log, devono essere eliminati manualmente nella destinazione SnapVault o all'interno del catalogo di backup HANA.



Non è possibile eseguire la pulizia di tutte le copie Snapshot di SnapVault, poiché una copia Snapshot viene bloccata come punto di sincronizzazione. Se è necessario eliminare anche la copia Snapshot più recente, è necessario eliminare la relazione di replica SnapVault. In questo caso, NetApp consiglia di eliminare i backup nel catalogo di backup HANA per sbloccare la gestione della conservazione dei backup dei log.





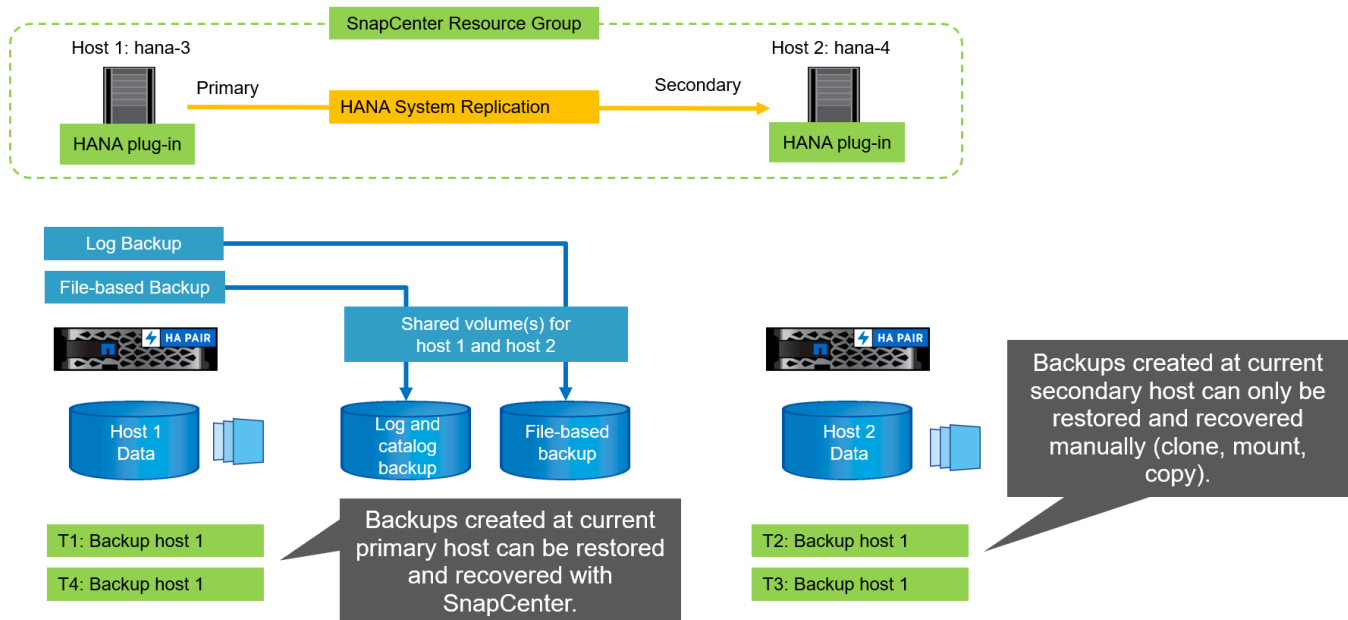
## Gestione della conservazione

SnapCenter 4.6 gestisce la conservazione per i backup Snapshot, le operazioni di controllo dell'integrità dei blocchi, le voci del catalogo di backup HANA e i backup dei log (se non disattivati) su entrambi gli host HANA, quindi non importa quale host sia attualmente primario o secondario. I backup (dati e log) e le voci del catalogo HANA vengono cancellati in base alla conservazione definita, indipendentemente dal fatto che sia necessaria un'operazione di eliminazione sull'host primario o secondario corrente. In altre parole, non è richiesta alcuna interazione manuale se viene eseguita un'operazione di Takeover e/o la replica viene configurata nell'altra direzione.

Se la replica di SnapVault fa parte della strategia di protezione dei dati, è necessaria un'interazione manuale per scenari specifici, come descritto nella sezione [\[SnapVault Replication\]](#).

## Ripristino e ripristino

La figura seguente mostra uno scenario in cui sono stati eseguiti più takeover e sono stati creati backup Snapshot in entrambi i siti. Con lo stato corrente, l'host hana-3 è l'host primario e l'ultimo backup è T4, creato sull'host hana-3. Se è necessario eseguire un'operazione di ripristino e ripristino, i backup T1 e T4 sono disponibili per il ripristino e il ripristino in SnapCenter. I backup creati sull'host hana-4 (T2, T3) non possono essere ripristinati utilizzando SnapCenter. Questi backup devono essere copiati manualmente nel volume di dati di hana-3 per il ripristino.



Le operazioni di ripristino e ripristino per una configurazione del gruppo di risorse di SnapCenter 4.6 sono identiche a quelle di una configurazione della replica non di sistema rilevata automaticamente. Sono disponibili tutte le opzioni per il ripristino e il ripristino automatizzato. Per ulteriori dettagli, consultare il report tecnico "[TR-4614: Backup e ripristino SAP HANA con SnapCenter](#)".

Nella sezione viene descritta un'operazione di ripristino da un backup creato sull'altro host "[Ripristino e ripristino da un backup creato sull'altro host](#)".

## Configurazione di SnapCenter con una singola risorsa

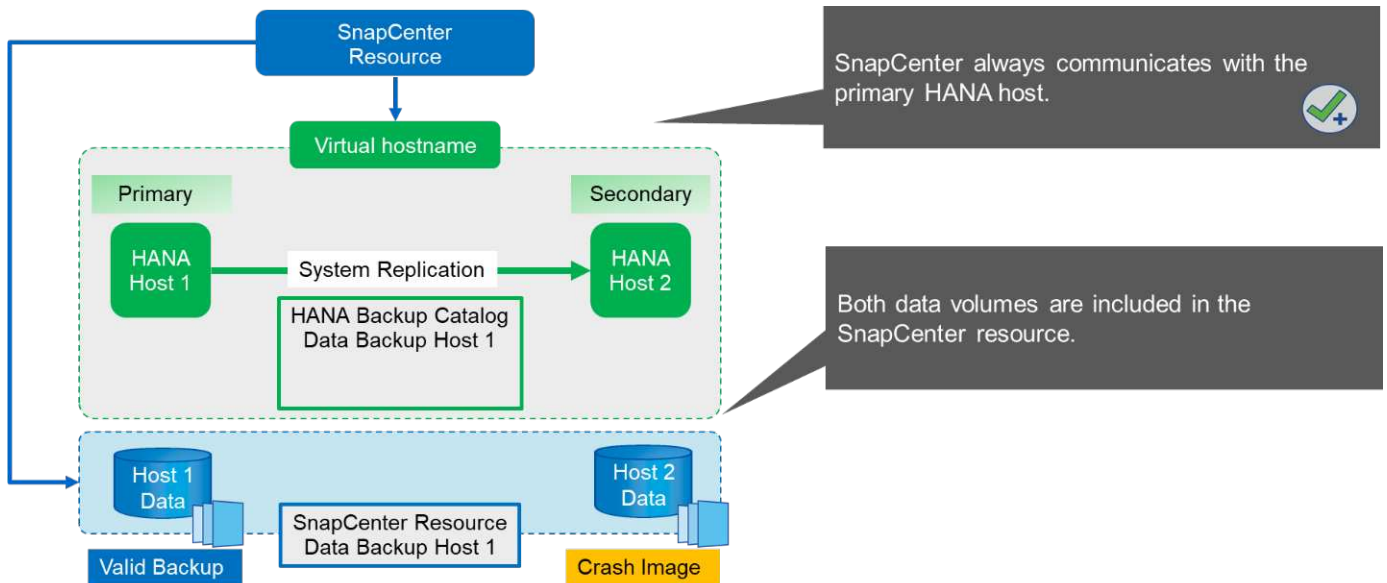
Una risorsa SnapCenter viene configurata con l'indirizzo IP virtuale (nome host) dell'ambiente di replica del sistema HANA. Con questo approccio, SnapCenter comunica sempre con l'host primario, indipendentemente dal fatto che l'host 1 o l'host 2 sia primario. I volumi di dati di entrambi gli host SAP HANA sono inclusi nella risorsa SnapCenter.



Si presuppone che l'indirizzo IP virtuale sia sempre associato all'host SAP HANA primario. Il failover dell'indirizzo IP virtuale viene eseguito all'esterno di SnapCenter come parte del workflow di failover della replica del sistema HANA.

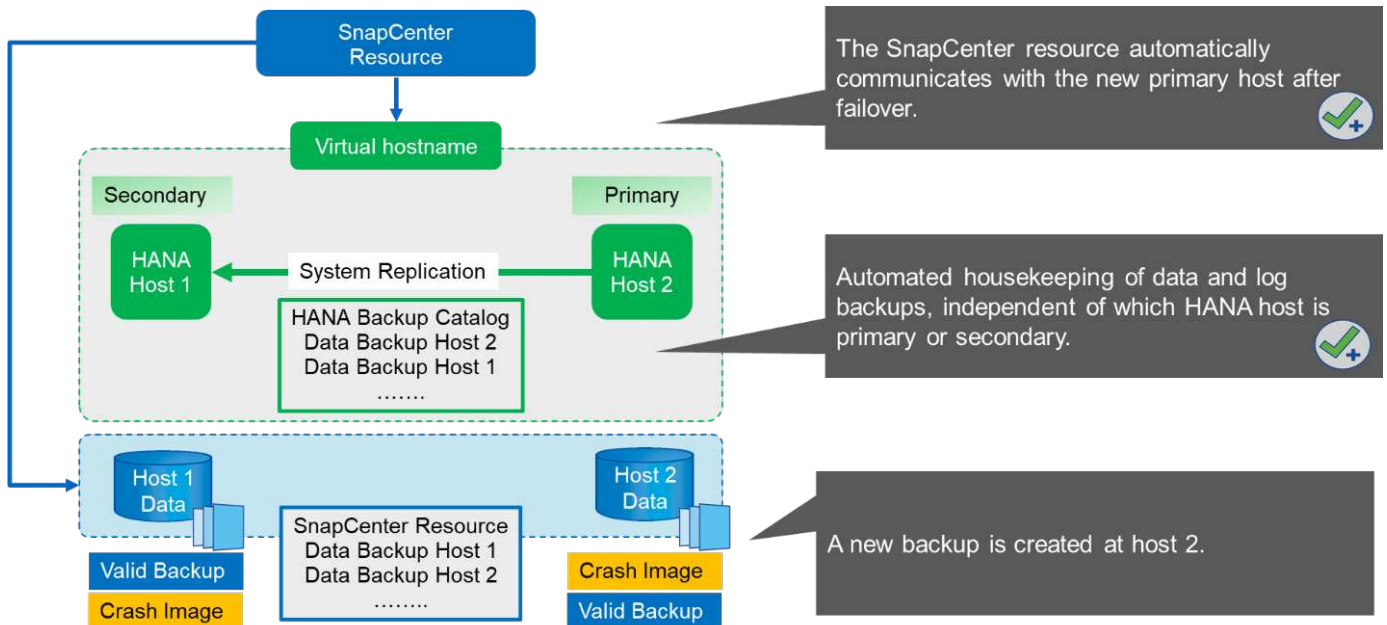
Quando viene eseguito un backup con host 1 come host primario, viene creato un backup Snapshot coerente con il database nel volume di dati dell'host 1. Poiché il volume di dati dell'host 2 fa parte della risorsa SnapCenter, viene creata un'altra copia Snapshot per questo volume. Questa copia Snapshot non è coerente con il database, ma è solo un'immagine di crash dell'host secondario.

Il catalogo di backup SAP HANA e la risorsa SnapCenter includono il backup creato sull'host 1.



La figura seguente mostra l'operazione di backup dopo il failover sull'host 2 e la replica dall'host 2 all'host 1. SnapCenter comunica automaticamente con l'host 2 utilizzando l'indirizzo IP virtuale configurato nella risorsa SnapCenter. I backup vengono ora creati sull'host 2. SnapCenter crea due copie Snapshot: Un backup coerente con il database nel volume di dati dell'host 2 e una copia Snapshot dell'immagine di crash nel volume di dati dell'host 1. Il catalogo di backup SAP HANA e la risorsa SnapCenter ora includono il backup creato sull'host 1 e il backup creato sull'host 2.

La gestione dei backup dei dati e dei log si basa sulla policy di conservazione di SnapCenter definita e i backup vengono cancellati indipendentemente dall'host primario o secondario.

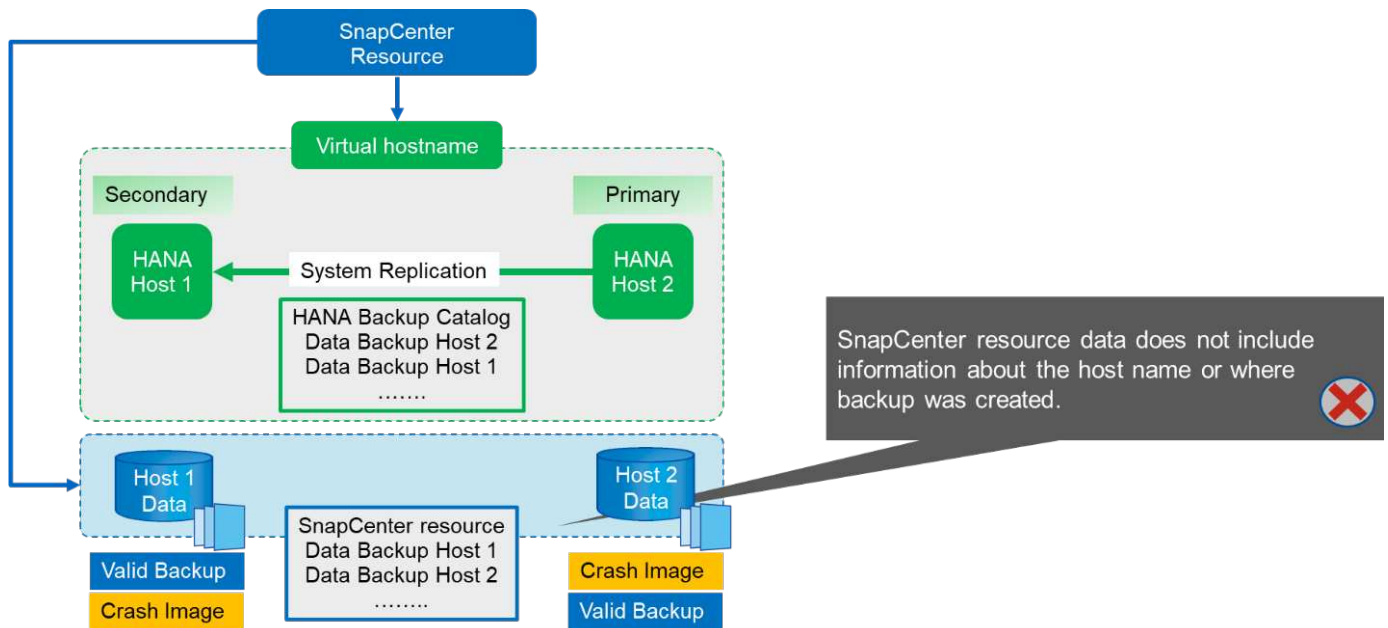


Come discusso nella sezione ["Backup Snapshot dello storage e replica del sistema SAP"](#), Un'operazione di ripristino con backup Snapshot basati sullo storage è diversa, a seconda del backup da ripristinare. È importante identificare l'host in cui è stato creato il backup per determinare se il ripristino può essere eseguito sul volume di storage locale o se il ripristino deve essere eseguito sul volume di storage dell'altro host.

Con la configurazione SnapCenter a singola risorsa, SnapCenter non è a conoscenza della posizione in cui è stato creato il backup. Pertanto, NetApp consiglia di aggiungere uno script di prebackup al workflow di backup

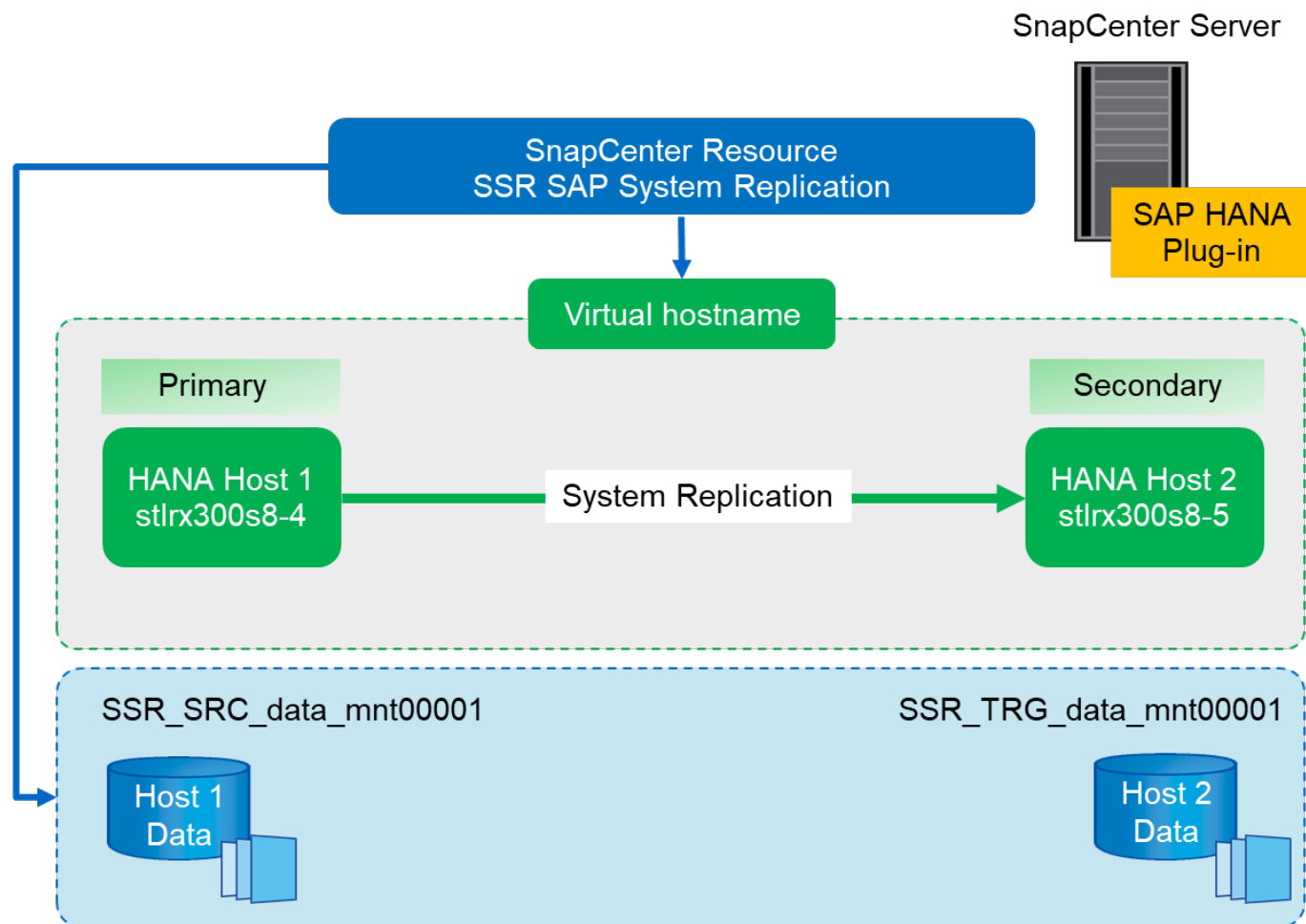
di SnapCenter per identificare quale host è attualmente l'host SAP HANA primario.

La figura seguente mostra l'identificazione dell'host di backup.



## Configurazione di SnapCenter

La figura seguente mostra la configurazione di laboratorio e una panoramica della configurazione SnapCenter richiesta.



Per eseguire operazioni di backup indipendentemente dall'host SAP HANA primario e anche quando un host è inattivo, il plug-in SAP HANA di SnapCenter deve essere implementato su un host plug-in centrale. Nella nostra configurazione di laboratorio, abbiamo utilizzato il server SnapCenter come host plug-in centrale e abbiamo implementato il plug-in SAP HANA sul server SnapCenter.

Nel database HANA è stato creato un utente per eseguire operazioni di backup. Una chiave di archivio utente è stata configurata sul server SnapCenter su cui è stato installato il plug-in SAP HANA. La chiave dell'archivio utente include l'indirizzo IP virtuale degli host di replica del sistema SAP HANA (`ssr-vip`).

```
hdbuserstore.exe -u SYSTEM set SSRKEY ssr-vip:31013 SNAPCENTER <password>
```

Per ulteriori informazioni sulle opzioni di implementazione del plug-in SAP HANA e sulla configurazione dell'archivio utenti, consultare il report tecnico TR-4614: ["Backup e ripristino SAP HANA con SnapCenter"](#).

In SnapCenter, la risorsa viene configurata come mostrato nella figura seguente utilizzando la chiave di memorizzazione utente, configurata in precedenza, e il server SnapCenter come `hdbsql` host di comunicazione.

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Summary

Provide Resource Details

☐ Single Container

☒ Multitenant Database Container (MDC) - Single Tenant

☐ Non-data Volumes

Resource Type

HANA System Name

SSR - SAP System Replication

SID

SSR

Tenant Database

SSR

HDBSQL Client Host

SC30-V2.sapcc.stl.netapp.com

HDB Secure User Store Keys

SSRKEY

HDBSQL OS User

SYSTEM

Previous

Next

I volumi di dati di entrambi gli host SAP HANA sono inclusi nella configurazione del footprint dello storage, come mostrato nella figura seguente.

20

Add SAP HANA Database

1 Name

2 Storage Footprint

3 Resource Settings

4 Summary

Provide Storage Footprint Details

Storage Systems for storage footprint

hana

Modify hana

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

Volume Name

SSR\_TRG\_data\_mnt00001

SSR\_SRC\_data\_mnt00001

LUNs or Qtrees

Default is 'None' or type to find

Default is 'None' or type to find

Save

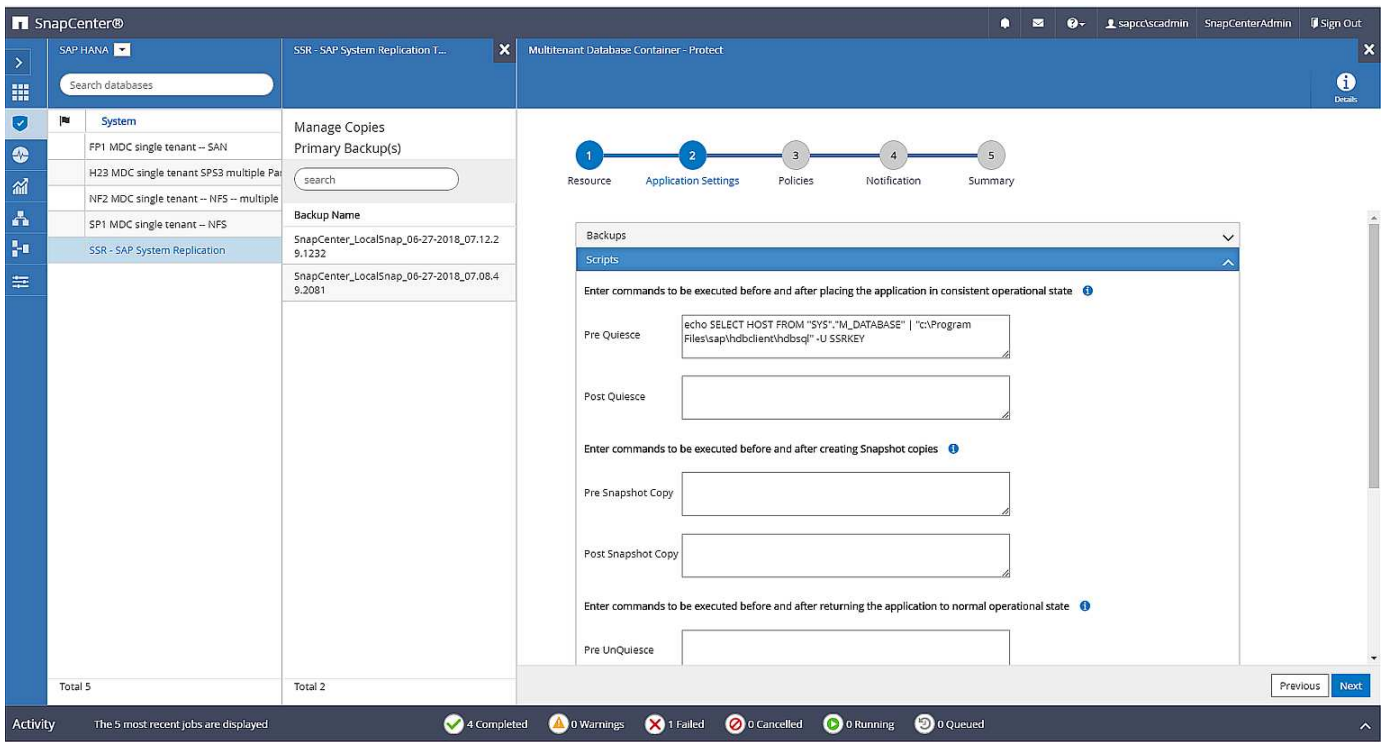
Previous

Next

Come discusso in precedenza, SnapCenter non è a conoscenza della posizione in cui è stato creato il backup. NetApp consiglia pertanto di aggiungere uno script di pre-backup nel flusso di lavoro di backup di SnapCenter per identificare quale host è attualmente l'host SAP HANA primario. È possibile eseguire questa identificazione utilizzando un'istruzione SQL aggiunta al flusso di lavoro di backup, come illustrato nella figura seguente.

```
Select host from "SYS".M_DATABASE
```



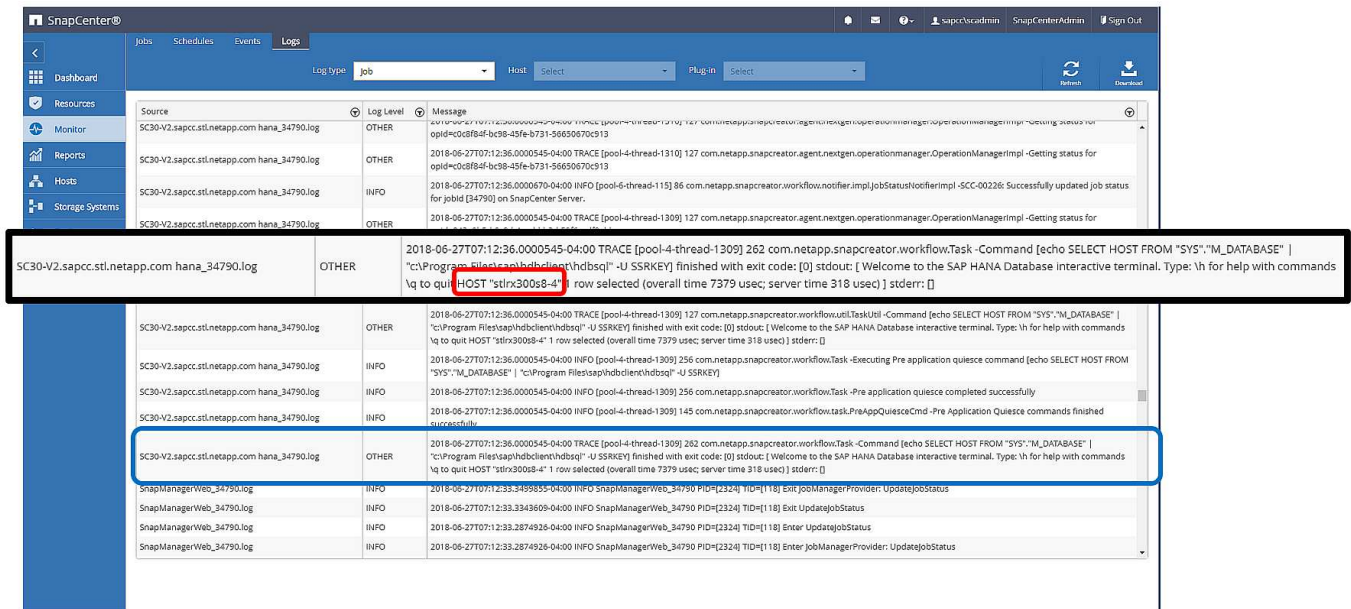


## Operazione di backup di SnapCenter

Le operazioni di backup vengono ora eseguite come di consueto. La gestione dei backup dei dati e dei log viene eseguita indipendentemente dall'host SAP HANA primario o secondario.

I log dei processi di backup includono l'output dell'istruzione SQL, che consente di identificare l'host SAP HANA in cui è stato creato il backup.

La figura seguente mostra il log del processo di backup con l'host 1 come host primario.



Questa figura mostra il log del processo di backup con l'host 2 come host primario.



The screenshot shows the SAP HANA Studio Logs window. The log entry for 'SC30-V2.sapcc.stl.netapp.com hana\_34799.log' is highlighted, showing a successful backup of the SYSTEMDB database. The log entry is as follows:

```

2018-06-27T07:45:53.0000174-04:00 INFO [pool-4-thread-1347] 145 com.netapp.snapcreator.workflow.task.Quiesce -Application Quiesce for plugin : hana
2018-06-27T07:45:53.0000174-04:00 INFO [pool-4-thread-1348] 145 com.netapp.snapcreator.workflow.task.Quiesce -log level minus
2018-06-27T07:45:53.0000174-04:00 INFO [pool-4-thread-1348] 145 com.netapp.snapcreator.workflow.task.Quiesce -Application Quiesce
2018-06-27T07:45:53.0000174-04:00 INFO [pool-3-thread-243] 145 com.netapp.snapcreator.workflow.task.Quiesce -Skipping Quiesce : false
2018-06-27T07:45:53.0000174-04:00 INFO [pool-3-thread-243] 145 com.netapp.snapcreator.workflow.task.Quiesce -Quiesce skip check
2018-06-27T07:45:53.0000174-04:00 INFO [pool-4-thread-1347] 145 com.netapp.snapcreator.workflow.task.PreAppQuiesceCmd -Pre Application Quiesce commands finished successfully
2018-06-27T07:45:53.0000174-04:00 INFO [pool-4-thread-1347] 256 com.netapp.snapcreator.workflow.task -Pre application quiesce completed successfully
2018-06-27T07:45:53.0000174-04:00 TRACE [pool-4-thread-1347] 127 com.netapp.snapcreator.agent.nextgen.operationmanager.OperationManagerImpl -Getting status for opid=d7e4d902-abc3-457e-9fad-d6516af97bf
2018-06-27T07:45:53.0000174-04:00 TRACE [pool-4-thread-1347] 127 com.netapp.snapcreator.agent.nextgen.operationmanager.OperationManagerImpl -getOperationResult() -Getting result for opid=d7e4d902-abc3-457e-9fad-d6516af97bf

```

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.

The screenshot shows the SAP HANA Studio Backup Catalog window. The backup details are visible, including the host name 'stlx300s8-4'. The backup details are as follows:

Host	Service	Size	Name	Source Type	EBID
stlx300s8-4	nameserver	1.47 GB	hdb0001	volume	SnapC...

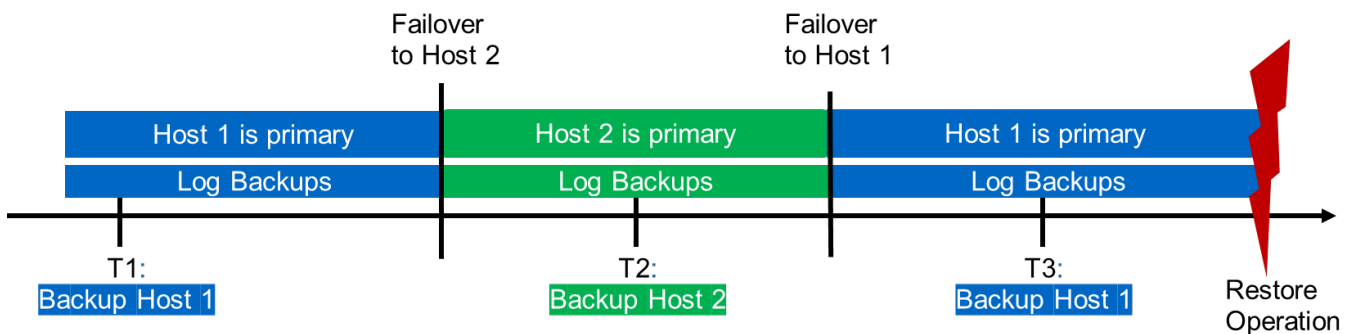
## Ripristino e ripristino

Come discusso in precedenza, è necessario essere in grado di identificare la posizione in cui è stato creato il backup selezionato per definire l'operazione di ripristino richiesta. Se il database SAP HANA è ancora online, è possibile utilizzare SAP HANA Studio per identificare l'host in cui è stato creato il backup. Se il database non è in linea, le informazioni sono disponibili solo nel log del processo di backup di SnapCenter.

La figura seguente illustra le diverse operazioni di ripristino a seconda del backup selezionato.

Se è necessario eseguire un'operazione di ripristino dopo l'indicazione di data e ora T3 e l'host 1 è il principale, è possibile ripristinare il backup creato in T1 o T3 utilizzando SnapCenter. Questi backup Snapshot sono disponibili nel volume di storage collegato all'host 1.

Se è necessario eseguire il ripristino utilizzando il backup creato nell'host 2 (T2), ovvero una copia Snapshot nel volume di storage dell'host 2, il backup deve essere reso disponibile per l'host 1. È possibile rendere disponibile questo backup creando una copia di NetApp FlexClone dal backup, montando la copia di FlexClone sull'host 1 e copiando i dati nella posizione originale.



Restore Operation With	
Backup T1	SnapCenter
Backup T2	Create FlexClone from „Backup host 2“, mount and copy
Backup T3	SnapCenter

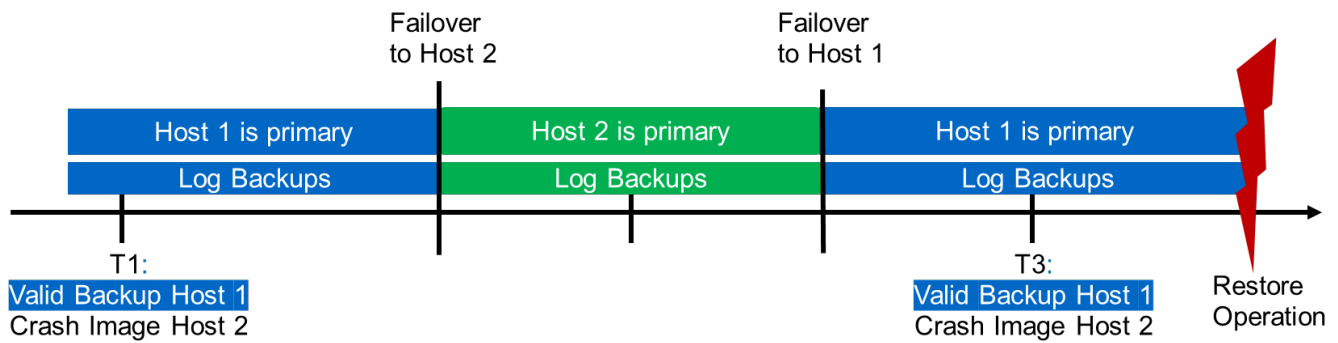
Con una singola configurazione delle risorse SnapCenter, le copie Snapshot vengono create su entrambi i volumi di storage di entrambi gli host di replica del sistema SAP HANA. Solo il backup Snapshot creato nel volume di storage dell'host SAP HANA primario è valido per il forward recovery. La copia Snapshot creata nel volume di storage dell'host SAP HANA secondario è un'immagine di crash che non può essere utilizzata per il forward recovery.

Un'operazione di ripristino con SnapCenter può essere eseguita in due modi diversi:

- Ripristinare solo il backup valido
- Ripristinare la risorsa completa, incluso il backup valido e l'immagine del crash. Le sezioni seguenti illustrano in dettaglio le due diverse operazioni di ripristino.

Nella sezione viene descritta un'operazione di ripristino da un backup creato sull'altro host "[Ripristino e ripristino da un backup creato sull'altro host](#)".

La figura seguente illustra le operazioni di ripristino con una singola configurazione delle risorse SnapCenter.

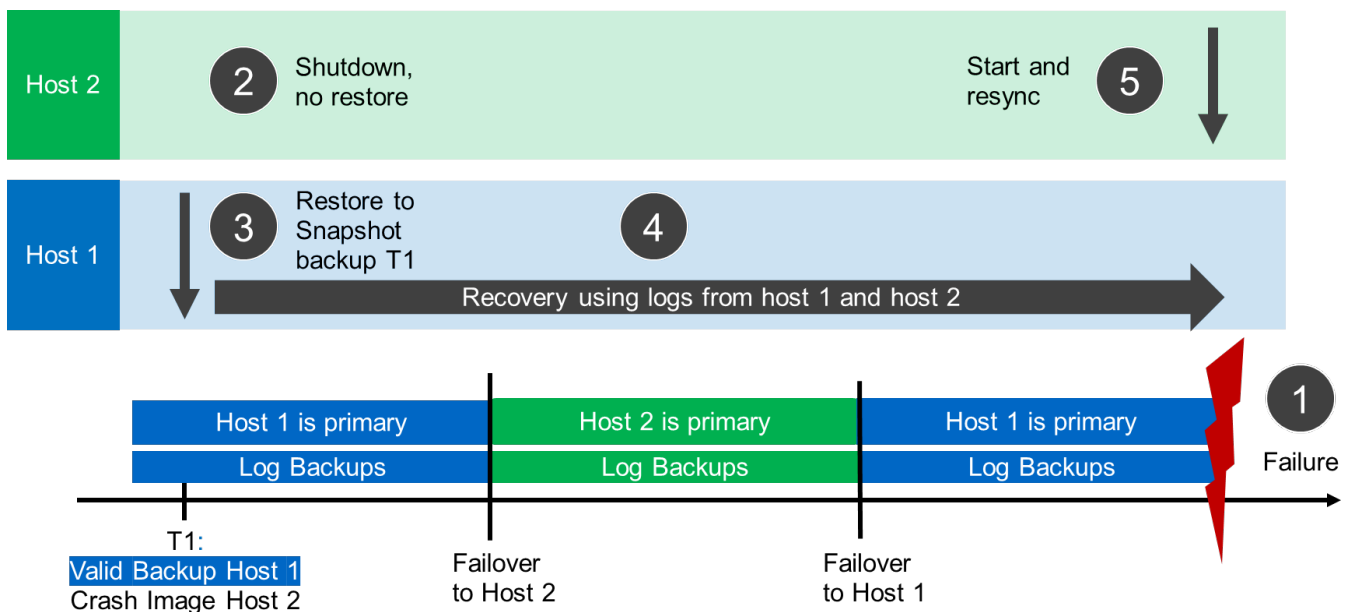


### Ripristino SnapCenter solo del backup valido

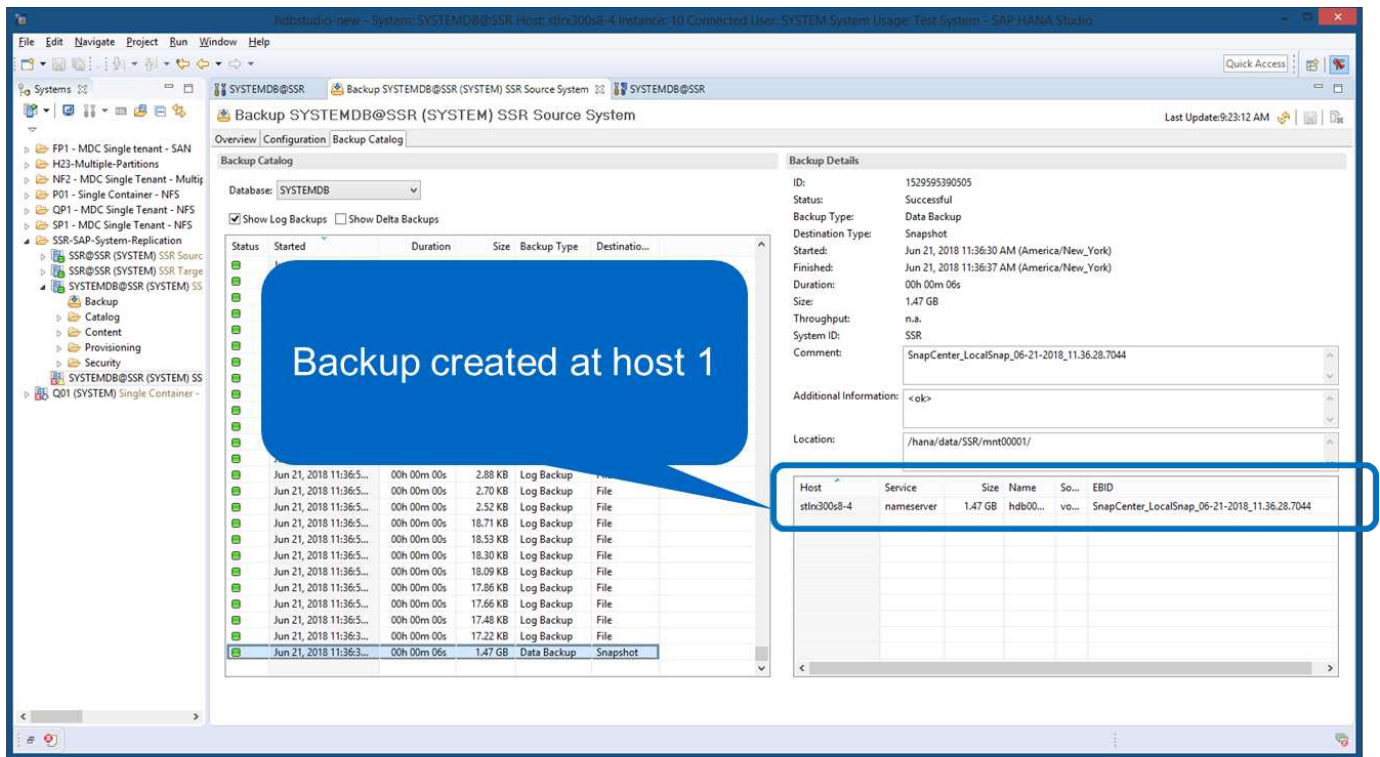
La figura seguente mostra una panoramica dello scenario di ripristino e ripristino descritto in questa sezione.

È stato creato un backup in T1 sull'host 1. È stato eseguito un failover sull'host 2. Dopo un certo punto di tempo, è stato eseguito un altro failover verso l'host 1. Al momento attuale, l'host 1 è l'host primario.

1. Si è verificato un errore ed è necessario ripristinare il backup creato in T1 sull'host 1.
2. L'host secondario (host 2) viene arrestato, ma non viene eseguita alcuna operazione di ripristino.
3. Il volume di storage dell'host 1 viene ripristinato nel backup creato in T1.
4. Viene eseguito un forward recovery con i log degli host 1 e 2.
5. Viene avviato l'host 2 e viene avviata automaticamente una risincronizzazione della replica di sistema dell'host 2.



La figura seguente mostra il catalogo di backup SAP HANA in SAP HANA Studio. Il backup evidenziato mostra il backup creato in T1 sull'host 1.

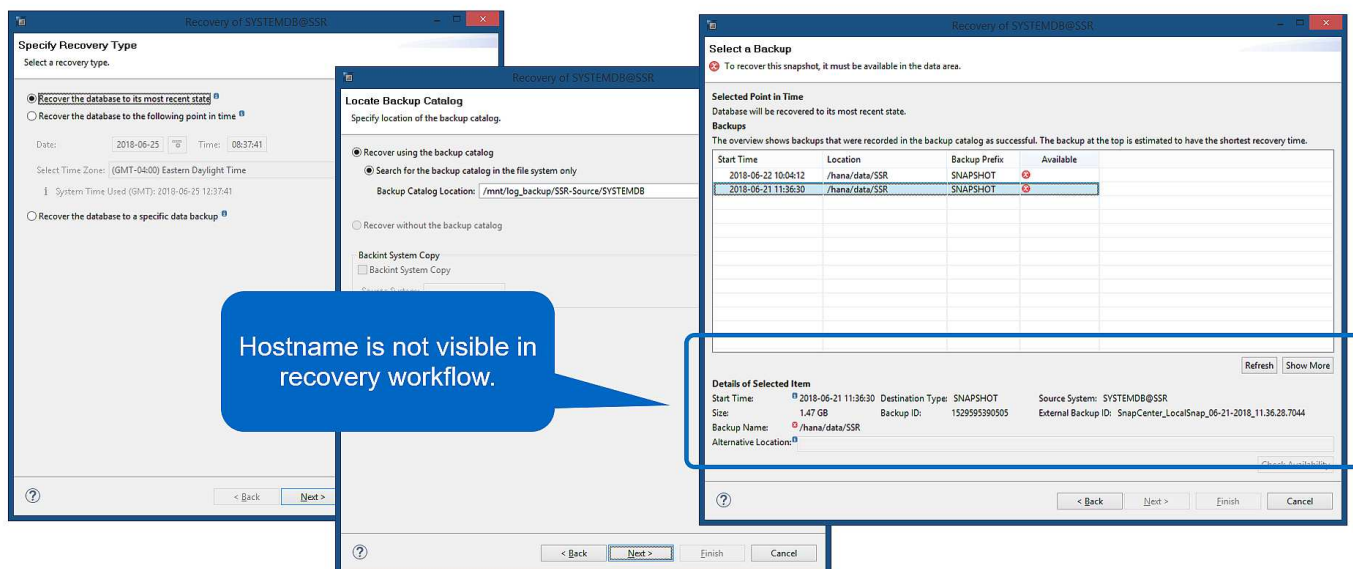


25

Viene avviata un'operazione di ripristino e ripristino in SAP HANA Studio. Come mostrato nella figura seguente, il nome dell'host in cui è stato creato il backup non è visibile nel flusso di lavoro di ripristino e ripristino.

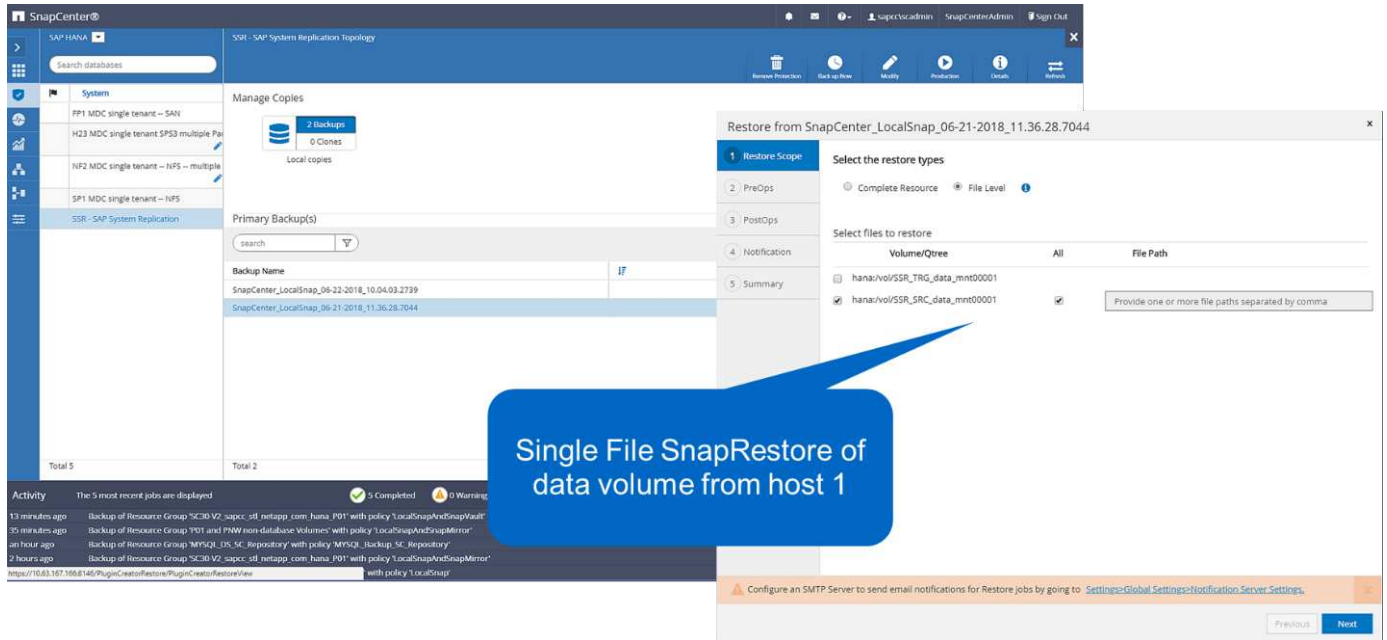


Nel nostro scenario di test, siamo stati in grado di identificare il backup corretto (il backup creato nell'host 1) in SAP HANA Studio quando il database era ancora online. Se il database non è disponibile, controllare il log del processo di backup di SnapCenter per identificare il backup corretto.

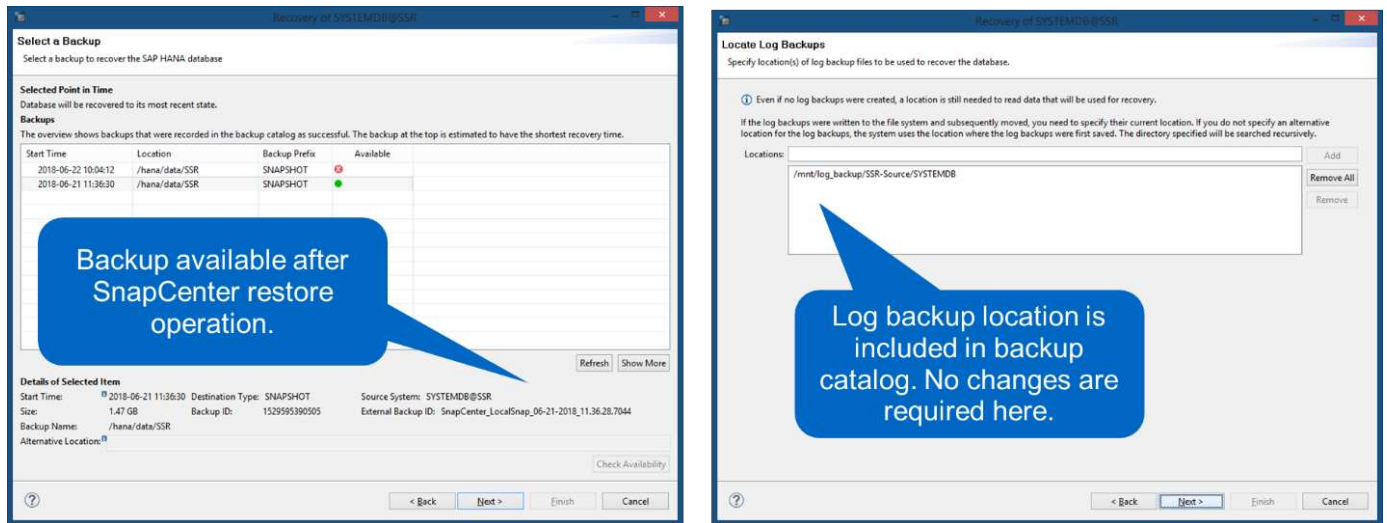


In SnapCenter, viene selezionato il backup e viene eseguita un'operazione di ripristino a livello di file. Nella

schermata di ripristino a livello di file, viene selezionato solo il volume host 1 in modo che venga ripristinato solo il backup valido.



Dopo l'operazione di ripristino, il backup viene evidenziato in verde in SAP HANA Studio. Non è necessario inserire un'ulteriore posizione di backup del log, in quanto il percorso del file di backup del log degli host 1 e 2 è incluso nel catalogo di backup.

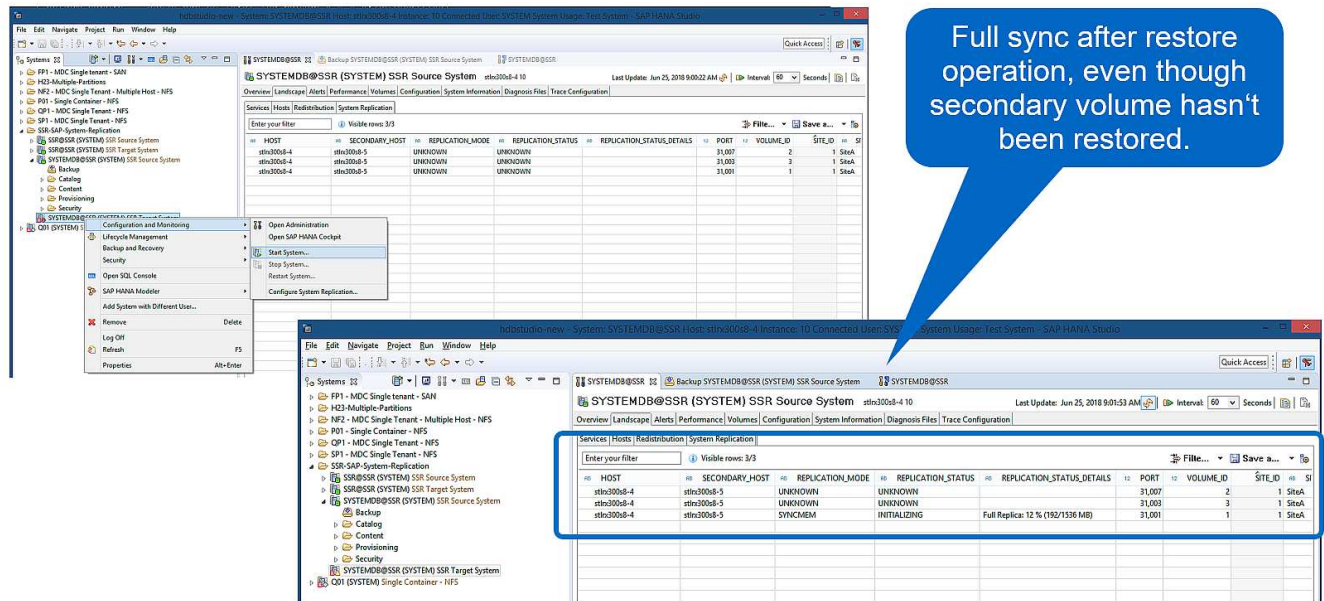


Al termine del forward recovery, viene avviato l'host secondario (host 2) e viene avviata la risincronizzazione della replica del sistema SAP HANA.



Anche se l'host secondario è aggiornato (non è stata eseguita alcuna operazione di ripristino per l'host 2), SAP HANA esegue una replica completa di tutti i dati. Questo comportamento è standard dopo un'operazione di ripristino e recovery con SAP HANA System Replication.



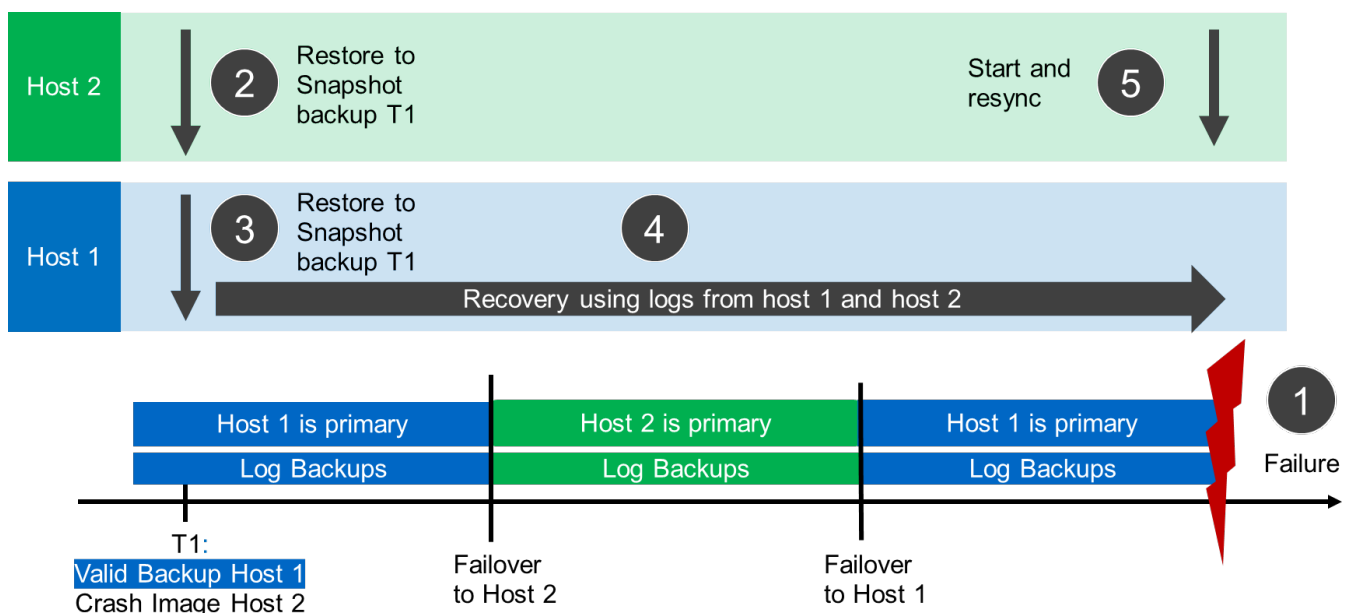


## Ripristino SnapCenter di un backup valido e di un'immagine di arresto anomalo

La figura seguente mostra una panoramica dello scenario di ripristino e ripristino descritto in questa sezione.

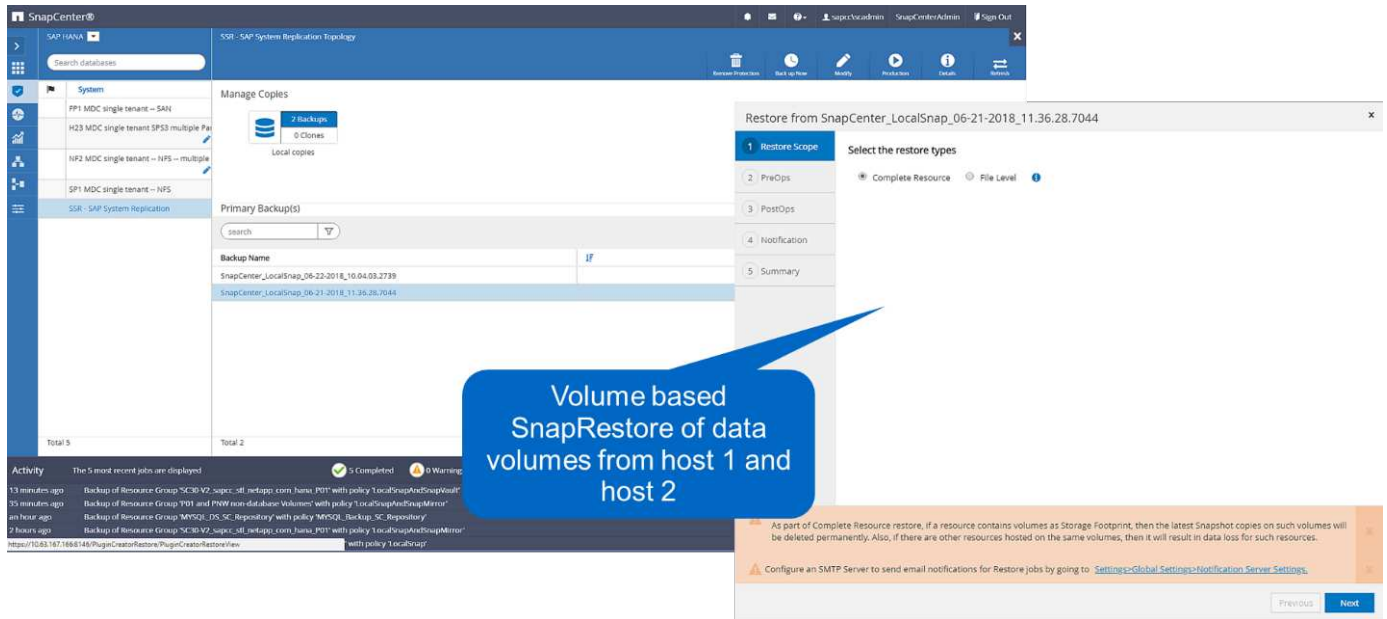
È stato creato un backup in T1 sull'host 1. È stato eseguito un failover sull'host 2. Dopo un certo punto di tempo, è stato eseguito un altro failover verso l'host 1. Al momento attuale, l'host 1 è l'host primario.

1. Si è verificato un errore ed è necessario ripristinare il backup creato in T1 sull'host 1.
2. L'host secondario (host 2) viene arrestato e l'immagine del crash T1 viene ripristinata.
3. Il volume di storage dell'host 1 viene ripristinato nel backup creato in T1.
4. Viene eseguito un forward recovery con i log degli host 1 e 2.
5. Viene avviato l'host 2 e viene avviata automaticamente una risincronizzazione della replica di sistema dell'host 2.

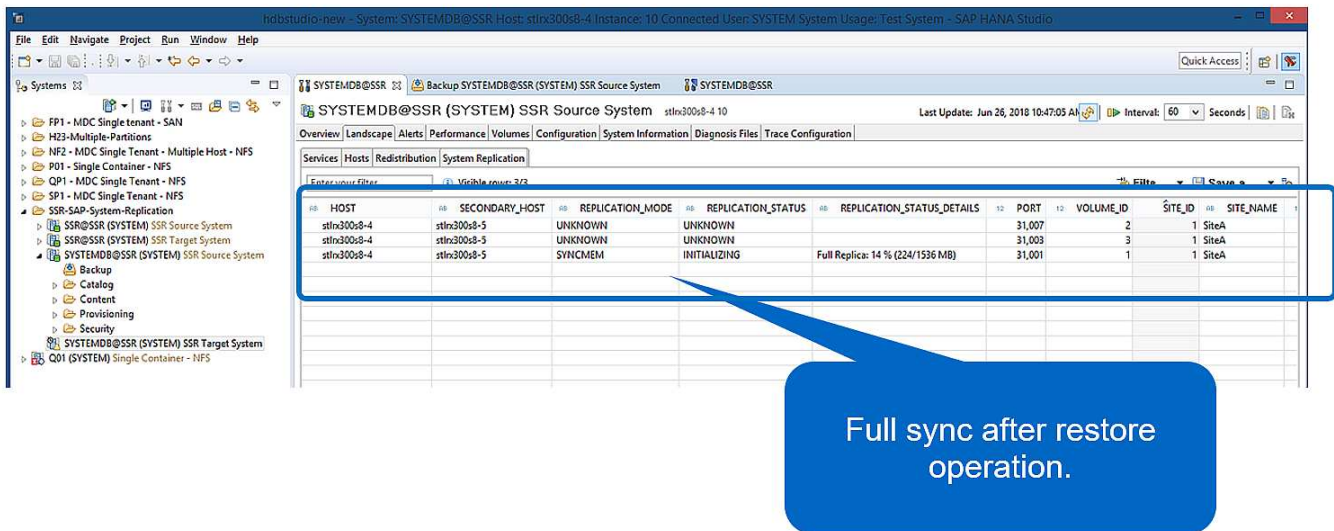


L'operazione di ripristino con SAP HANA Studio è identica a quella descritta nella sezione **"Ripristino SnapCenter solo del backup valido"**.

Per eseguire l'operazione di ripristino, selezionare completa risorsa in SnapCenter. I volumi di entrambi gli host vengono ripristinati.



Una volta completato il forward recovery, viene avviato l'host secondario (host 2) e viene avviata la risincronizzazione della replica del sistema SAP HANA. Viene eseguita la replica completa di tutti i dati.



## Ripristino e ripristino da un backup creato sull'altro host

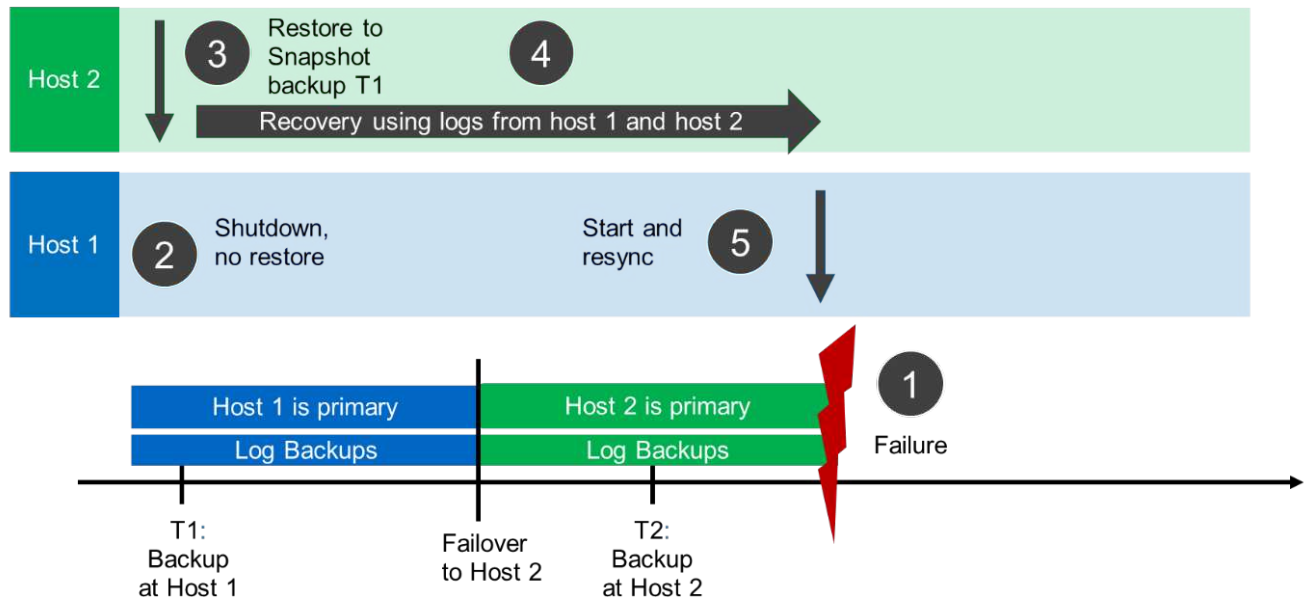
Un'operazione di ripristino da un backup creato sull'altro host SAP HANA è uno scenario valido per entrambe le opzioni di configurazione di SnapCenter.

La figura seguente mostra una panoramica dello scenario di ripristino e ripristino descritto in questa sezione.

È stato creato un backup in T1 sull'host 1. È stato eseguito un failover sull'host 2. Al momento attuale, l'host 2

è l'host primario.

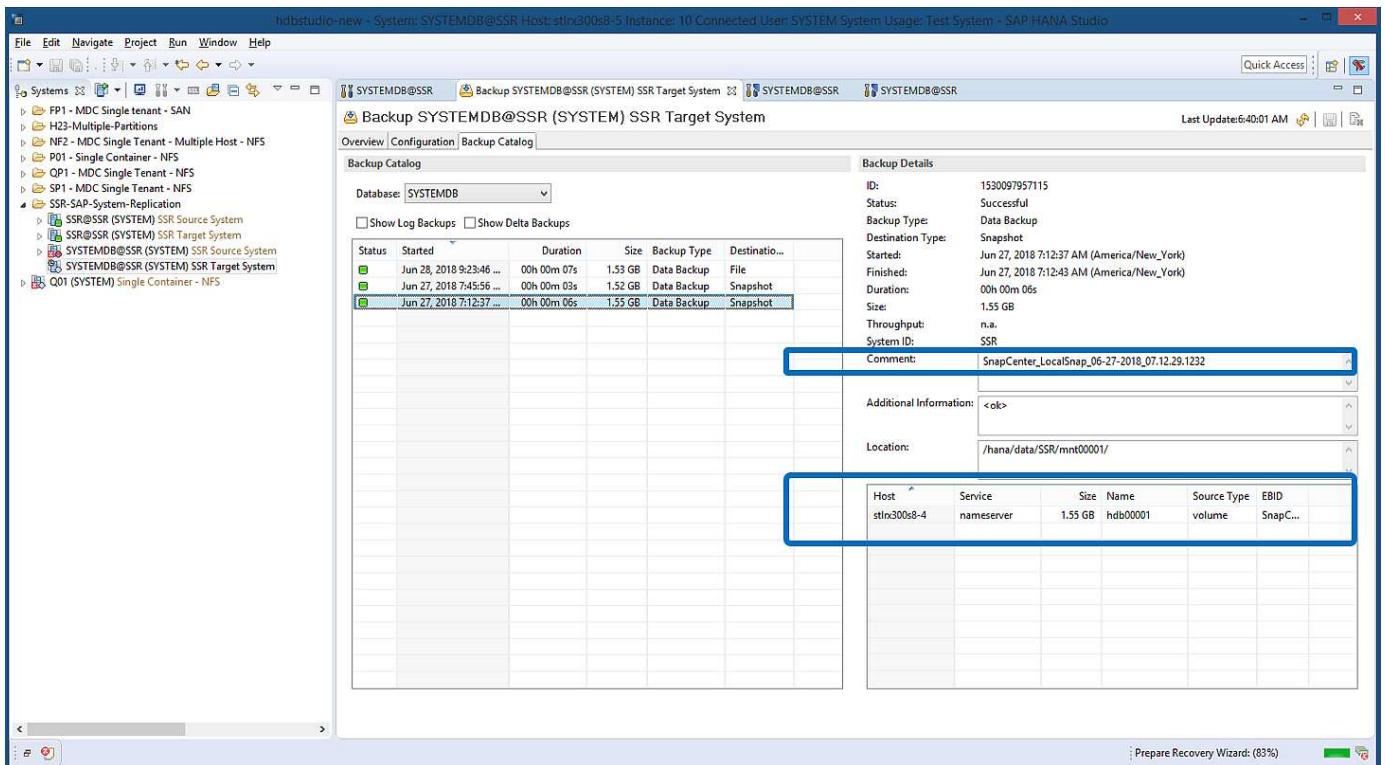
1. Si è verificato un errore ed è necessario ripristinare il backup creato in T1 sull'host 1.
2. L'host primario (host 1) viene arrestato.
3. I dati di backup T1 dell'host 1 vengono ripristinati nell'host 2.
4. Il ripristino in avanti viene eseguito utilizzando i registri dell'host 1 e dell'host 2.
5. Viene avviato l'host 1 e viene avviata automaticamente una risincronizzazione della replica di sistema dell'host 1.



31

La figura seguente mostra il catalogo di backup SAP HANA ed evidenzia il backup, creato sull'host 1, utilizzato per l'operazione di ripristino.

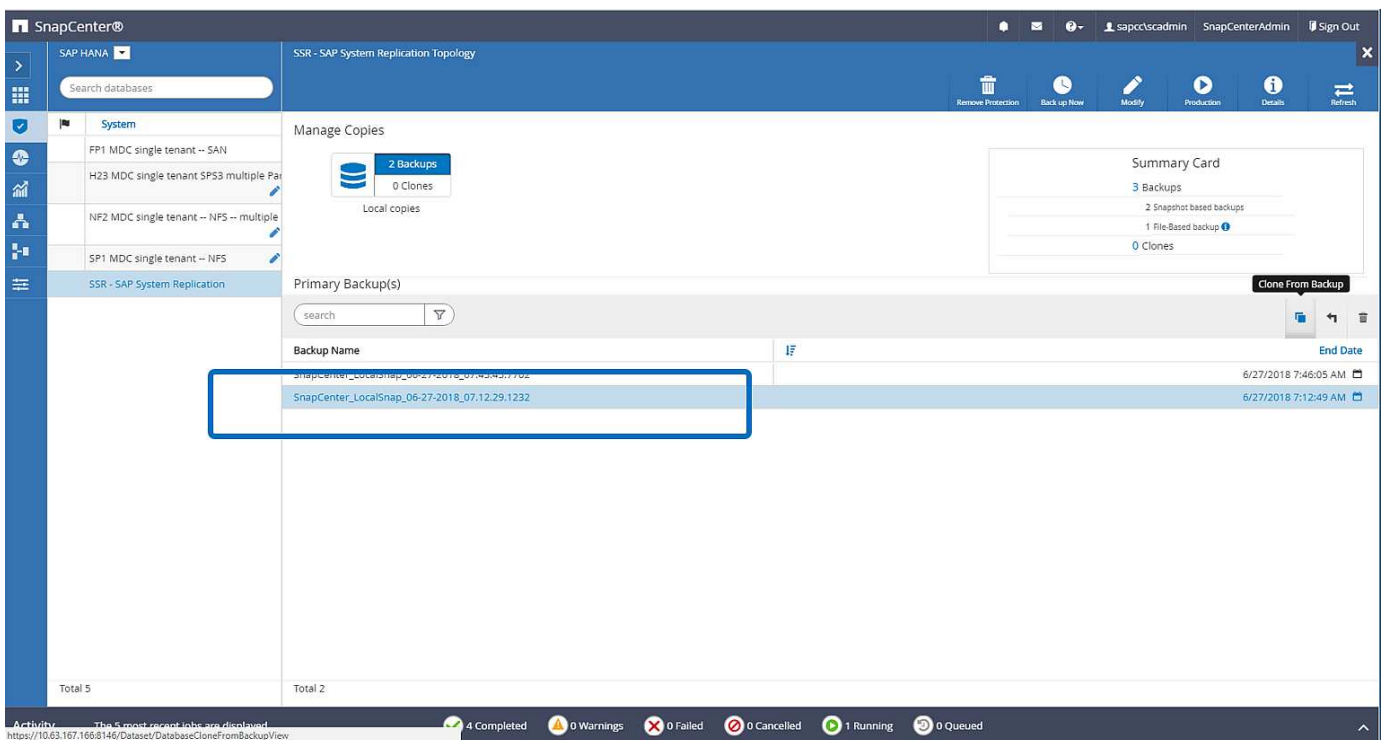




L'operazione di ripristino prevede i seguenti passaggi:

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.

Clone from Backup

1 Location

Select the host to create the clone

Clone server: stlrx300s8-7.stl.netapp.com

Clone suffix: \_clone\_date\_time

NFS Export IP Address: 192.168.173.71

Any host with installed HANA plug-in can be used. Not required to install the plug-in on the System Replication host.

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

Previous Next

Per determinare il percorso di giunzione richiesto per montare il volume clonato, controllare il log del lavoro di clonazione, come mostrato nella figura seguente.



## Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti:

- Backup e ripristino SAP HANA con SnapCenter

["https://www.netapp.com/us/media/tr-4614.pdf"](https://www.netapp.com/us/media/tr-4614.pdf)

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

["https://docs.netapp.com/us-en/netapp-solutions-sap/lifecycle/sc-copy-clone-introduction.html"](https://docs.netapp.com/us-en/netapp-solutions-sap/lifecycle/sc-copy-clone-introduction.html)

- Disaster recovery SAP HANA con replica dello storage

["https://www.netapp.com/us/media/tr-4646.pdf"](https://www.netapp.com/us/media/tr-4646.pdf)

## Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Ottobre 2018	Versione iniziale
Versione 2.0	Gennaio 2022	Aggiornamento per il supporto della replica di sistema HANA di SnapCenter 4.6

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.