



Tech refresh

SnapCenter software

NetApp
January 09, 2026

This PDF was generated from https://docs.netapp.com/it-it/snapcenter/tech-refresh/task_tech_refresh_server_host.html on January 09, 2026. Always check docs.netapp.com for the latest.

Sommario

- Tech refresh 1
 - Aggiornamento tecnico dell'host server SnapCenter 1
 - Tech refresh di un nodo nel cluster F5 2
 - Smantellamento del vecchio host del server SnapCenter 2
 - Eseguire il rollback dell'host del server SnapCenter precedente 2
 - Disaster recovery 2
 - Tech refresh degli host plug-in SnapCenter 4
 - Tech refresh del sistema storage 6
 - Aggiornare i backup dello storage primario 7
 - Aggiornare i backup dello storage secondario 9

Tech refresh

Aggiornamento tecnico dell'host server SnapCenter

Quando l'host del server SnapCenter richiede l'aggiornamento, è possibile installare la stessa versione del server SnapCenter sul nuovo host e quindi eseguire le API per eseguire il backup di SnapCenter dal vecchio server e ripristinarlo sul nuovo server.

Fasi

1. Distribuire il nuovo host ed eseguire le seguenti operazioni:
 - a. Installare la stessa versione del server SnapCenter.
 - b. (Facoltativo) configurare i certificati CA e abilitare SSL bidirezionale. Per ulteriori informazioni, fare riferimento a. ["Configurare il certificato CA"](#) e. ["Configurare e abilitare SSL bidirezionale"](#).
 - c. (Opzionale) configurare l'autenticazione a più fattori. Per ulteriori informazioni, fare riferimento a. ["Abilitare l'autenticazione a più fattori"](#).
2. Accedere come utente amministratore SnapCenter.
3. Creare un backup del server SnapCenter sul vecchio host utilizzando l'API: O il cmdlet:
`/<snapcenter_version>/server/backup New-SmServerBackup.`



Prima di eseguire il backup, sospendere tutti i processi pianificati e assicurarsi che non siano in esecuzione.



Se si desidera ripristinare il backup sul server SnapCenter in esecuzione su un nuovo dominio, prima di eseguire un backup è necessario aggiungere il nuovo utente di dominio nel vecchio host SnapCenter e assegnare il ruolo di amministratore SnapCenter.

4. Copiare il backup dal vecchio host al nuovo host.
5. Ripristinare il backup del server SnapCenter sul nuovo host utilizzando l'API: O il cmdlet:
`/<snapcenter_version>/server/restore Restore-SmServerBackup.`

Per impostazione predefinita, Restore aggiornerà il nuovo URL del server SnapCenter in tutti gli host. Se si desidera ignorare l'aggiornamento, utilizzare l'attributo `-SkipSMSURLInHosts` e aggiornare separatamente l'URL del server eseguendo l'API: O il cmdlet: `/<snapcenter_version>/server/configureurl Set-SmServerConfig.`



Se l'host del plug-in non è in grado di risolvere il nome host del server, accedere a ciascun host del plug-in e aggiungere la voce `etc/host` per il nuovo IP nel formato `<New IP> SC_Server_Name`.



Le voci del server `etc/host` non verranno ripristinate. È possibile ripristinarlo manualmente dal vecchio server.

Se il backup viene ripristinato sul server SnpCenter in esecuzione su un nuovo dominio e si desidera continuare a utilizzare i vecchi utenti di dominio, è necessario registrare il vecchio dominio nel nuovo server SnapCenter.



Se il file `web.config` è stato aggiornato manualmente nel vecchio host SnapCenter, gli aggiornamenti non verranno copiati nel nuovo host. È necessario apportare manualmente le stesse modifiche nel file `web.config` del nuovo host.

6. Se è stato saltato l'aggiornamento dell'URL del server SnapCenter o uno qualsiasi degli host è rimasto inattivo durante il processo di ripristino, aggiornare il nuovo nome del server in tutti gli host o host specificati gestiti da SnapCenter utilizzando l'API: `/<snapcenter_version>/server/configureurl` O il cmdlet: `Set-SmServerConfig`.
7. Attivare i processi pianificati su tutti gli host dal nuovo server SnapCenter.

Tech refresh di un nodo nel cluster F5

Puoi fare un tech refresh di qualsiasi nodo nel cluster F5 rimuovendo il nodo e aggiungendo il nuovo nodo. Se il nodo da aggiornare è attivo, rendere attivo un altro nodo del cluster e quindi rimuovere il nodo.

Per informazioni su come aggiungere un nodo al cluster F5, fare riferimento alla sezione ["Configurare i server SnapCenter per l'alta disponibilità utilizzando F5"](#).



Se l'URL del cluster F5 cambia, l'URL può essere aggiornato in tutti gli host utilizzando l'API: O il cmdlet: `/<snapcenter_version>/server/configureurl` `Set-SmServerConfig`.

Smantellamento del vecchio host del server SnapCenter

È possibile rimuovere il vecchio host del server SnapCenter dopo aver verificato che il nuovo server SnapCenter sia attivo e funzionante e che tutti gli host dei plug-in siano in grado di comunicare con il nuovo host del server SnapCenter.

Eseguire il rollback dell'host del server SnapCenter precedente

In caso di problemi, è possibile ripristinare il vecchio host del server SnapCenter aggiornando l'URL del server SnapCenter in tutti gli host utilizzando l'API: O il cmdlet:

`/<snapcenter_version>/server/configureurl` `Set-SmServerConfig`.

Disaster recovery

Disaster recovery dell'host SnapCenter standalone

È possibile eseguire il ripristino di emergenza ripristinando il backup del server nel nuovo host.

Prima di iniziare

Assicurarsi di disporre di un backup del vecchio server SnapCenter.

Fasi

1. Distribuire il nuovo host ed eseguire le seguenti operazioni:
 - a. Installare la stessa versione del server SnapCenter.
 - b. Configurare i certificati CA e abilitare SSL bidirezionale. Per ulteriori informazioni, fare riferimento a ["Configurare il certificato CA"](#) e ["Configurare e abilitare SSL bidirezionale"](#).
2. Copiare il vecchio backup del server SnapCenter nel nuovo host.
3. Accedere come utente amministratore SnapCenter.

4. Ripristinare il backup del server SnapCenter sul nuovo host utilizzando l'API: O il cmdlet:
`/<snapcenter_version>/server/restore Restore-SmServerBackup`.

Per impostazione predefinita, Restore aggiornerà il nuovo URL del server SnapCenter in tutti gli host. Se si desidera ignorare l'aggiornamento, utilizzare l'attributo `-SkipSMSURLInHosts` e aggiornare separatamente l'URL del server utilizzando l'API: O il cmdlet: `/<snapcenter_version>/server/configureurl Set-SmServerConfig`.



Se l'host del plug-in non è in grado di risolvere il nome host del server, accedere a ciascun host del plug-in e aggiungere la voce `etc/host` per il nuovo IP nel formato `<New IP> SC_Server_Name`.



Le voci del server `etc/host` non verranno ripristinate. È possibile ripristinarlo manualmente dal vecchio server.

5. Se è stato saltato l'aggiornamento dell'URL o uno qualsiasi degli host è stato inattivo durante il processo di ripristino, aggiornare il nuovo nome del server in tutti gli host o host specificati che sono gestiti da SnapCenter utilizzando l'API: `/<snapcenter_version>/server/configureurl` O il cmdlet: `Set-SmServerConfig`.

Disaster recovery del cluster SnapCenter F5

È possibile eseguire il ripristino di emergenza ripristinando il backup del server nel nuovo host e convertendo quindi l'host standalone in un cluster.

Prima di iniziare

Assicurarsi di disporre di un backup del vecchio server SnapCenter.

Fasi

1. Distribuire il nuovo host ed eseguire le seguenti operazioni:
 - a. Installare la stessa versione del server SnapCenter.
 - b. Configurare i certificati CA e abilitare SSL bidirezionale. Per ulteriori informazioni, fare riferimento a ["Configurare il certificato CA"](#) e ["Configurare e abilitare SSL bidirezionale"](#).
2. Copiare il vecchio backup del server SnapCenter nel nuovo host.
3. Accedere come utente amministratore SnapCenter.
4. Ripristinare il backup del server SnapCenter sul nuovo host utilizzando l'API: O il cmdlet:
`/<snapcenter_version>/server/restore Restore-SmServerBackup`.

Per impostazione predefinita, Restore aggiornerà il nuovo URL del server SnapCenter in tutti gli host. Se si desidera ignorare l'aggiornamento, utilizzare l'attributo `-SkipSMSURLInHosts` e aggiornare separatamente l'URL del server utilizzando l'API: O il cmdlet: `/<snapcenter_version>/server/configureurl Set-SmServerConfig`.



Se l'host del plug-in non è in grado di risolvere il nome host del server, accedere a ciascun host del plug-in e aggiungere la voce `etc/host` per il nuovo IP nel formato `<New IP> SC_Server_Name`.



Le voci del server `etc/host` non verranno ripristinate. È possibile ripristinarlo manualmente dal vecchio server.

5. Se è stato saltato l'aggiornamento dell'URL o uno qualsiasi degli host è stato inattivo durante il processo di ripristino, aggiornare il nuovo nome del server in tutti gli host o host specificati che sono gestiti da SnapCenter utilizzando l'API: `/<snapcenter_version>/server/configureurl` O il cmdlet: `Set-SmServerConfig`.
6. Conversione dell'host standalone in cluster F5.

Per informazioni sulla configurazione di F5, consultare la ["Configurare i server SnapCenter per l'alta disponibilità utilizzando F5"](#).

Informazioni correlate

Per informazioni sulle API, è necessario accedere alla pagina Swagger. vedere ["Come accedere alle API REST utilizzando la pagina web delle API di swagger"](#).

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo `Get-Help command_name`. In alternativa, è anche possibile fare riferimento a ["Guida di riferimento al cmdlet del software SnapCenter"](#).

Tech refresh degli host plug-in SnapCenter

Quando gli host dei plug-in SnapCenter richiedono un aggiornamento, è necessario spostare le risorse dal vecchio host al nuovo host. Quando il nuovo host viene aggiunto a SnapCenter, scoprirà tutte le risorse ma sarà trattato come nuove risorse.

A proposito di questa attività

È necessario eseguire l'API o il cmdlet che prenderà il vecchio nome host e il nuovo nome host come input, confrontare le risorse per nome e ricollegare gli oggetti delle risorse corrispondenti dal vecchio host al nuovo host. Le risorse corrispondenti verranno contrassegnate come protette.

- Il parametro `IsDryRun` è impostato su `True` per impostazione predefinita e identifica le risorse corrispondenti del vecchio e del nuovo host.

Dopo aver verificato le risorse corrispondenti, impostare il parametro `IsDryRun` su `False` per ricollegare gli oggetti delle risorse corrispondenti dal vecchio host al nuovo host.

- Per impostazione predefinita, il parametro `AutoMigrateManuallyAddedResources` è impostato su `True` e in modo da copiare automaticamente le risorse aggiunte manualmente dal vecchio host al nuovo host.

Il parametro `AutoMigrateManuallyAddedResources` è applicabile solo alle risorse Oracle e SAP HANA.

- Il parametro `SQLInstanceMapping` deve essere utilizzato se il nome dell'istanza è diverso tra il vecchio host e il nuovo host. Se si tratta di un'istanza predefinita, utilizzare `default_instance` come nome dell'istanza.

Il tech refresh è supportato per i seguenti plug-in SnapCenter:

- Plug-in SnapCenter per Microsoft SQL Server
 - Se i database SQL sono protetti a livello di istanza e come parte dell'aggiornamento tecnico dell'host vengono spostate solo le risorse parziali nel nuovo host, la protezione a livello di istanza esistente verrà convertita nella protezione del gruppo di risorse e le istanze di entrambi gli host verranno aggiunte al gruppo di risorse.
 - Se si utilizza un host SQL (ad esempio host1) come scheduler o come server di verifica per le risorse

di un altro host (ad esempio Host2), durante l'esecuzione dell'aggiornamento tecnico su host1, i dettagli della pianificazione o della verifica non verranno migrati e continueranno a essere eseguiti su host1. Se dovete modificare, allora dovrete cambiarlo manualmente nei rispettivi host.

- Se si utilizza il setup delle istanze del cluster di failover SQL (FCI), è possibile eseguire l'aggiornamento tecnico aggiungendo il nuovo nodo al cluster FCI e aggiornando l'host del plug-in in SnapCenter.
- Se si utilizza la configurazione di SQL Availability Group (AG), l'aggiornamento tecnico non è necessario. È possibile aggiungere il nuovo nodo ad AG e aggiornare l'host in SnapCenter.

- Plug-in SnapCenter per Windows
- Plug-in SnapCenter per database Oracle

Se si utilizza il setup di Oracle Real Application Cluster (RAC), è possibile eseguire l'aggiornamento tecnico aggiungendo il nuovo nodo al cluster RAC e aggiornando l'host plug-in in SnapCenter.

- Plug-in SnapCenter per database SAP HANA

I casi d'utilizzo supportati sono:

- Migrazione delle risorse da un host a un altro host.
- Migrazione delle risorse da più host a uno o meno host.
- Migrazione delle risorse da un host a più host.

Gli scenari supportati sono:

- Il nuovo host ha un nome diverso dal vecchio host
- L'host esistente è stato rinominato

Prima di iniziare

Poiché questo workflow modifica i dati nel repository SnapCenter, si consiglia di eseguire il backup del repository SnapCenter. In caso di problemi con i dati, il repository SnapCenter può essere riportato allo stato precedente utilizzando il backup.

Per ulteriori informazioni, fare riferimento a. "[Eseguire il backup del repository SnapCenter](#)".

Fasi

1. Distribuire il nuovo host e installare l'applicazione.
2. Sospendere le pianificazioni del vecchio host.
3. Spostare le risorse necessarie dal vecchio host al nuovo host.
 - a. Acquisizione dei database richiesti nel nuovo host dallo stesso storage.
 - Assicurarsi che lo spazio di archiviazione sia mappato sulla stessa unità o sullo stesso percorso di montaggio del vecchio host. Se l'archiviazione non è mappata correttamente, i backup creati nel vecchio host non possono essere utilizzati per il ripristino.



Per impostazione predefinita, Windows assegna automaticamente la successiva unità disponibile.

- Se il DR di archiviazione è abilitato, il relativo storage deve essere montato nel nuovo host.
- b. Verificare la compatibilità in caso di modifica della versione dell'applicazione.

- c. Solo per l'host del plug-in Oracle, assicurarsi che gli UID e i GID di Oracle e degli utenti del gruppo siano identici a quelli del vecchio host.

Per informazioni, fare riferimento a:

- ["Come eseguire la migrazione del database SQL dal vecchio host al nuovo host"](#)
- ["Come migrare il database Oracle dal vecchio host al nuovo host"](#)
- ["Come attivare il database SAP HANA nel nuovo host"](#)

4. Aggiungere il nuovo host a SnapCenter.
5. Verificare se tutte le risorse sono state rilevate.
6. Eseguire l'API di aggiornamento dell'host: O il cmdlet: `/<snapcenter_version>/techrefresh/host Invoke-SmTechRefreshHost`.



La seriografia a secco è attivata per impostazione predefinita e vengono identificate le risorse corrispondenti da ricollegare. È possibile verificare le risorse eseguendo l'API: `'/Jobs/{jobid}'` o il cmdlet `get-SmJobSummaryReport`.

Se le risorse sono state migrate da più host, è necessario eseguire l'API o il cmdlet per tutti gli host. Se l'unità o il percorso di montaggio nel nuovo host non è lo stesso del vecchio host, le seguenti operazioni di ripristino non avranno esito positivo:

- Il ripristino SQL sul posto non avrà esito positivo. Tuttavia, la funzione RTAL può essere sfruttata.
- Il ripristino dei database Oracle e SAP HANA non avrà esito positivo.

Se si desidera migrare a più host, è necessario eseguire tutti i passaggi dal punto 1 per tutti gli host.



È possibile eseguire più volte l'API o il cmdlet sullo stesso host, che verrà ricollegato solo se è stata identificata una nuova risorsa.

7. (Facoltativo) rimuovere il vecchio host o gli host da SnapCenter.

Informazioni correlate

Per informazioni sulle API, è necessario accedere alla pagina Swagger. vedere ["Come accedere alle API REST utilizzando la pagina web delle API di swagger"](#).

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo `Get-Help command_name`. In alternativa, è anche possibile fare riferimento a ["Guida di riferimento al cmdlet del software SnapCenter"](#).

Tech refresh del sistema storage

Quando lo storage viene tech refresh, i dati vengono migrati al nuovo storage e gli host delle applicazioni vengono montati con nuovo storage. Il workflow di backup di SnapCenter identifica il nuovo storage e crea la snapshot se il nuovo storage viene registrato in SnapCenter.

Puoi eseguire il ripristino, il montaggio e il cloning sui nuovi backup creati in seguito all'aggiornamento dello storage. Tuttavia, queste operazioni non avranno esito positivo quando vengono eseguite sui backup creati prima dell'aggiornamento dello storage, in quanto i backup contengono i dettagli dello storage precedente. È

necessario eseguire l'API di refresh della tecnologia storage o il cmdlet per aggiornare i vecchi backup in SnapCenter con i nuovi dettagli storage.

Il tech refresh è supportato per i seguenti plug-in SnapCenter:

- Plug-in SnapCenter per Microsoft SQL Server
- Plug-in SnapCenter per Windows
- Plug-in SnapCenter per database Oracle
- Plug-in SnapCenter per database SAP HANA
- Plug-in SnapCenter per server Microsoft Exchange

I casi d'utilizzo supportati sono:

- Refresh dello storage primario

L'aggiornamento tecnologico dello storage è supportato per sostituire lo storage primario con il nuovo storage. Non è possibile convertire lo storage secondario esistente in uno storage primario.

- Refresh dello storage secondario

Aggiornare i backup dello storage primario

Quando lo storage viene tech refresh, è necessario eseguire l'API o il cmdlet per l'aggiornamento dei vecchi backup in SnapCenter con i nuovi dettagli dello storage.

Prima di iniziare

Poiché questo workflow modifica i dati nel repository SnapCenter, si consiglia di eseguire il backup del repository SnapCenter. In caso di problemi con i dati, il repository SnapCenter può essere riportato allo stato precedente utilizzando il backup.

Per ulteriori informazioni, fare riferimento a. ["Eseguire il backup del repository SnapCenter"](#).

Fasi

1. Migrazione dei dati dal vecchio storage al nuovo storage.

Per informazioni su come eseguire la migrazione, fare riferimento a:

- ["Come migrare i dati in un nuovo storage"](#)
- ["Come si copia un volume e come si conservano tutte le copie Snapshot?"](#)

2. Impostare l'host sulla modalità di manutenzione.
3. Montare il nuovo storage nei rispettivi host e visualizzare i database.

Il nuovo dispositivo di archiviazione deve essere collegato all'host come in precedenza. Ad esempio, se fosse connessa come SAN, deve essere connessa come SAN.

Il nuovo storage deve essere montato sulla stessa unità o percorso del vecchio storage.

4. Verificare che tutte le risorse siano attive e in funzione.
5. Aggiungere il nuovo storage in SnapCenter.

Assicurati di avere un nome SVM univoco tra i cluster in SnapCenter. Se stai utilizzando lo stesso nome

SVM nel nuovo storage e se è possibile migrare tutti i volumi della SVM prima di eseguire il refresh dello storage, si consiglia quindi di eliminare la SVM nel vecchio cluster e riscoprire il vecchio cluster in SnapCenter, in modo da rimuovere la SVM dalla cache.

6. Impostare l'host in modalità di produzione.
7. In SnapCenter, creare un backup delle risorse di cui viene eseguita la migrazione dello storage. È necessario un nuovo backup affinché SnapCenter possa identificare l'impatto più recente dello storage, che verrà utilizzato per aggiornare i metadati dei vecchi backup esistenti.



Ogni volta che un nuovo LUN viene collegato all'host, avrà un nuovo numero di serie. Durante il rilevamento del file system di Windows, SnapCenter tratterà ogni numero seriale univoco come nuova risorsa. Durante l'aggiornamento tecnico dello storage, quando il LUN del nuovo storage viene collegato all'host con la stessa lettera o percorso dell'unità, il rilevamento del file system di Windows in SnapCenter contrassegnerà la risorsa esistente come eliminata anche se è montata con la stessa lettera o percorso di unità e visualizzerà il nuovo LUN come nuova risorsa. Poiché la risorsa viene contrassegnata come eliminata, non verrà presa in considerazione per il tech refresh dello storage in SnapCenter e tutti i backup della risorsa precedente andranno persi. In caso di aggiornamento dello storage, per le risorse del file system Windows, il rilevamento delle risorse non deve essere eseguito prima di eseguire l'API di refresh dello storage o il cmdlet.

8. Eseguire l'API di aggiornamento dello storage: O il cmdlet:

`/<snapcenter_version>/techrefresh/primarystorage Invoke-SmTechRefreshPrimaryStorage.`



Se la risorsa è configurata con un criterio abilitato per la replica, il backup più recente dopo l'aggiornamento dello storage dovrebbe contenere i dettagli dello storage secondario.

- a. Se si utilizza il setup delle istanze del cluster di failover SQL (FCI), i backup vengono mantenuti a livello di cluster. Fornire il nome del cluster come input per l'aggiornamento della tecnologia di storage.
- b. Se si utilizza l'installazione di SQL Availability Group (AG), i backup vengono mantenuti a livello di nodo. Fornire il nome del nodo come input per l'aggiornamento tecnologico dello storage.
- c. Se si utilizza l'installazione di Oracle Real Application Clusters (RAC), è possibile eseguire l'aggiornamento tecnico dello storage su qualsiasi nodo.

L'attributo *IsDryRun* è impostato su True per impostazione predefinita. Consente di identificare le risorse per le quali viene aggiornato lo storage. È possibile visualizzare la risorsa e i dettagli di archiviazione modificati eseguendo l'API: '`<SnapCenter_version>/Jobs/{jobid}`' o il cmdlet *get-SmJobSummaryReport*.

9. Dopo aver verificato i dettagli dello storage, impostare l'attributo *IsDryRun* su False ed eseguire l'API di aggiornamento dello storage: O il cmdlet: `/<snapcenter_version>/techrefresh/primarystorage Invoke-SmTechRefreshPrimaryStorage.`

In questo modo verranno aggiornati i dettagli di archiviazione nei backup precedenti.

È possibile eseguire più volte l'API o il cmdlet sullo stesso host; i dettagli dello storage nei backup meno recenti verranno aggiornati solo se lo storage viene aggiornato.



Non è possibile migrare la gerarchia di cloni in ONTAP. Se lo storage da migrare contiene metadati cloni in SnapCenter, la risorsa clonata verrà contrassegnata come risorsa indipendente. I cloni dei metadati dei cloni verranno rimossi in modo ricorsivo.

10. (Facoltativo) se tutti gli snapshot non vengono spostati dal vecchio storage primario al nuovo storage primario, eseguire la seguente API:

`/<snapcenter_version>/hosts/primarybackupsexistencecheck` O il cmdlet *Invoke-SmPrimaryBackupsExistenceCheck*.

In questo modo verrà eseguito il controllo dell'esistenza dello snapshot sul nuovo storage primario e verranno contrassegnati i rispettivi backup non disponibili per alcuna operazione in SnapCenter.

Aggiornare i backup dello storage secondario

Quando lo storage viene tech refresh, è necessario eseguire l'API o il cmdlet per l'aggiornamento dei vecchi backup in SnapCenter con i nuovi dettagli dello storage.

Prima di iniziare

Poiché questo workflow modifica i dati nel repository SnapCenter, si consiglia di eseguire il backup del repository SnapCenter. In caso di problemi con i dati, il repository SnapCenter può essere riportato allo stato precedente utilizzando il backup.

Per ulteriori informazioni, fare riferimento a ["Eseguire il backup del repository SnapCenter"](#).

Fasi

1. Migrazione dei dati dal vecchio storage al nuovo storage.

Per informazioni su come eseguire la migrazione, fare riferimento a:

- ["Come migrare i dati in un nuovo storage"](#)
- ["Come si copia un volume e come si conservano tutte le copie Snapshot?"](#)

2. Stabilire la relazione SnapMirror tra lo storage primario e il nuovo storage secondario e verificare che lo stato della relazione sia integro.
3. In SnapCenter, creare un backup delle risorse di cui viene eseguita la migrazione dello storage.

È necessario un nuovo backup affinché SnapCenter identifichi l'impatto più recente dello storage e venga utilizzato per aggiornare i metadati dei vecchi backup esistenti.



Attendere il completamento di questa operazione. Se si passa alla fase successiva prima del completamento, SnapCenter perderà completamente i metadati dello snapshot secondario precedente.

4. Dopo aver creato correttamente il backup di tutte le risorse in un host, eseguire l'API di aggiornamento dello storage secondario: O il cmdlet: `/<snapcenter_version>/techrefresh/secondarystorage` *Invoke-SmTechRefreshSecondaryStorage*.

In questo modo verranno aggiornati i dettagli dello storage secondario dei backup precedenti nell'host specificato.

Se si desidera eseguire questa operazione a livello di risorsa, fare clic su **Aggiorna** per ogni risorsa per aggiornare i metadati di archiviazione secondari.

5. Dopo aver aggiornato con successo i backup meno recenti, è possibile interrompere la vecchia relazione tra lo storage secondario e lo storage primario.

Informazioni sul copyright

Copyright © 2026 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.