



Eseguire il backup delle risorse SAP HANA

SnapCenter software

NetApp
November 06, 2025

This PDF was generated from https://docs.netapp.com/it-it/snapcenter-61/protect-hana/task_back_up_sap_hana_resources.html on November 06, 2025. Always check docs.netapp.com for the latest.

Sommario

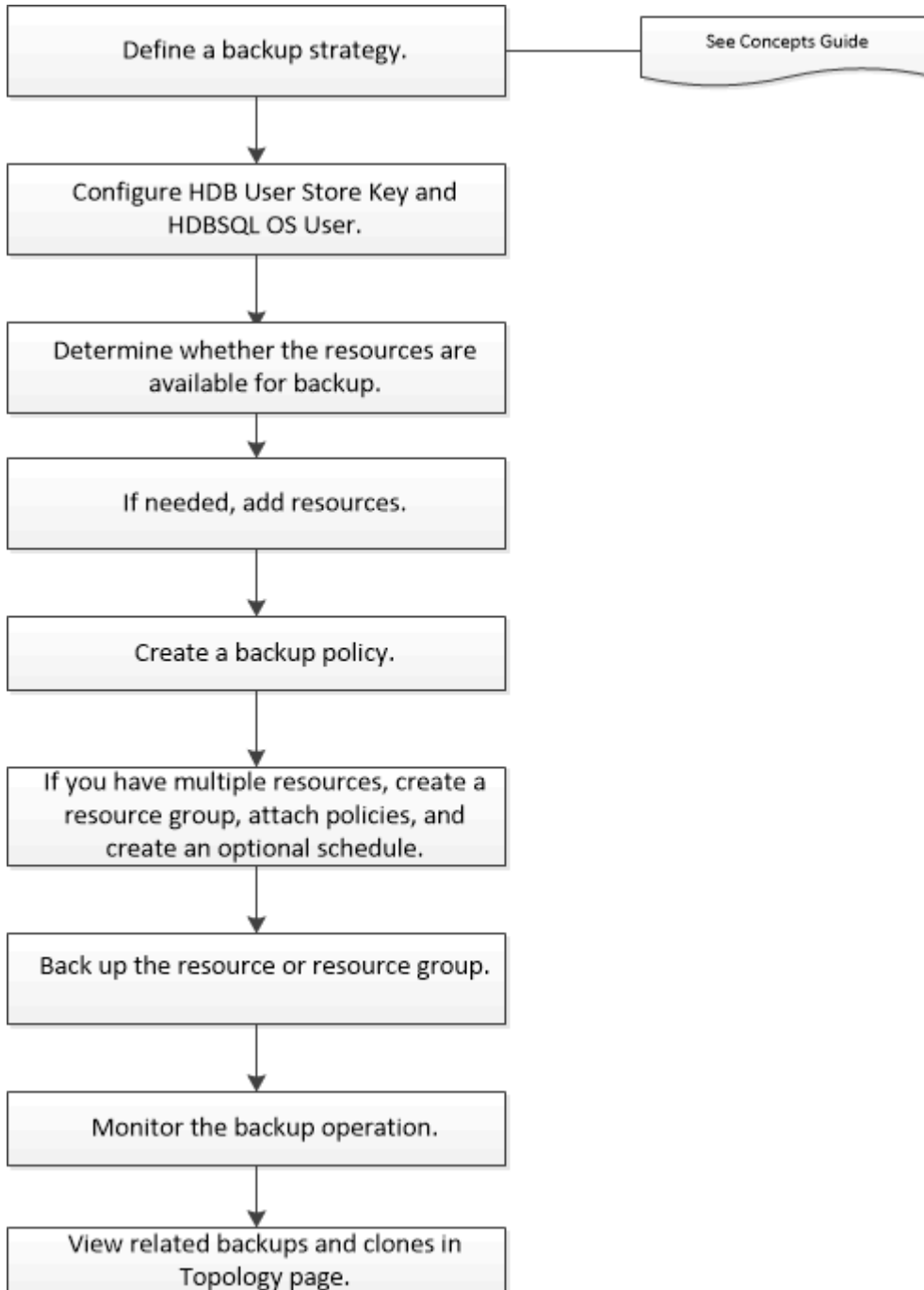
Eseguire il backup delle risorse SAP HANA	1
Eseguire il backup delle risorse SAP HANA	1
Configurare la chiave di archivio utente HDB e l'utente del sistema operativo HDBSQL per il database SAP HANA	2
Scopri le risorse e prepara i contenitori di database multitenant per la protezione dei dati	2
Scopri automaticamente i database	2
Preparare contenitori di database multitenant per la protezione dei dati	4
Aggiungere manualmente le risorse all'host del plug-in	5
Creare policy di backup per i database SAP HANA	7
Crea gruppi di risorse e allega criteri	12
Crea gruppi di risorse e abilita la protezione secondaria per le risorse SAP HANA sui sistemi ASA r2	16
Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per il database SAP HANA	19
Eseguire il backup dei database SAP HANA	20
Eseguire il backup dei gruppi di risorse	28
Monitorare le operazioni di backup dei database SAP HANA	28
Monitorare le operazioni di protezione dei dati sui database SAP HANA nel riquadro Attività	29
Annulla le operazioni di backup per SAP HANA	29
Visualizza i backup e i cloni del database SAP HANA nella pagina Topologia	30

Eseguire il backup delle risorse SAP HANA

Eseguire il backup delle risorse SAP HANA

È possibile creare un backup di una risorsa (database) o di un gruppo di risorse. Il flusso di lavoro del backup include la pianificazione, l'identificazione dei database per il backup, la gestione dei criteri di backup, la creazione di gruppi di risorse e l'associazione di criteri, la creazione di backup e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di backup:



È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono ulteriori informazioni sui cmdlet di PowerShell. ["Guida di riferimento ai cmdlet del software SnapCenter"](#).

Configurare la chiave di archivio utente HDB e l'utente del sistema operativo HDBSQL per il database SAP HANA

È necessario configurare HDB User Store Key e HDBSQL OS User per eseguire operazioni di protezione dei dati sui database SAP HANA.

Prima di iniziare

- Se nel database SAP HANA non sono configurati né la chiave HDB Secure User Store né l'utente HDB SQL OS, viene visualizzata un'icona a forma di lucchetto rosso solo per le risorse rilevate automaticamente. Se durante una successiva operazione di individuazione, la chiave HDB Secure User Store configurata risulta errata o non consente l'accesso al database stesso, l'icona del lucchetto rosso riapparirà.
- È necessario configurare la chiave HDB Secure User Store e l'utente HDB SQL OS per poter proteggere il database o aggiungerlo a un gruppo di risorse per eseguire operazioni di protezione dei dati.
- È necessario configurare HDB SQL OS User per accedere al database di sistema. Se l'utente HDB SQL OS è configurato per accedere solo al database tenant, l'operazione di individuazione non riuscirà.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse** e quindi selezionare SnapCenter Plug-in per database SAP HANA dall'elenco.
2. Nella pagina Risorse, seleziona il tipo di risorsa dall'elenco **Visualizza**.
3. (Facoltativo) Fare clic  e seleziona il nome host.

Puoi quindi fare clic  per chiudere il riquadro del filtro.
4. Selezionare il database, quindi fare clic su **Configura database**.
5. Nella sezione Configura impostazioni database, immettere la chiave HDB Secure User Store.



Viene visualizzato il nome host del plug-in e l'utente del sistema operativo HDB SQL viene automaticamente inserito in <sid>adm.

6. Fare clic su **OK**.

È possibile modificare la configurazione del database dalla pagina Topologia.

Scopri le risorse e prepara i contenitori di database multitenant per la protezione dei dati

Scopri automaticamente i database

Le risorse sono i database SAP HANA e il volume non dati sull'host Linux gestiti da SnapCenter. È possibile aggiungere queste risorse ai gruppi di risorse per eseguire operazioni di protezione dei dati dopo aver individuato i database SAP HANA disponibili.

Prima di iniziare

- È necessario aver già completato attività quali l'installazione di SnapCenter Server, l'aggiunta della chiave di archiviazione utente HDB, l'aggiunta di host e la configurazione delle connessioni del sistema di archiviazione.
- È necessario aver configurato la chiave HDB Secure User Store e l'utente HDB SQL OS sull'host Linux.
 - È necessario configurare la chiave dell'archivio utenti HDB con SID adm user. Ad esempio, per il sistema HANA con A22 come SID, la chiave di archiviazione utente HDB deve essere configurata con a22adm.
- Il plug-in SnapCenter per il database SAP HANA non supporta il rilevamento automatico delle risorse residenti negli ambienti virtuali RDM/VMDK. È necessario fornire le informazioni di archiviazione per gli ambienti virtuali durante l'aggiunta manuale dei database.

Informazioni su questo compito

Dopo aver installato il plug-in, tutte le risorse presenti sull'host Linux vengono automaticamente rilevate e visualizzate nella pagina Risorse.

Le risorse rilevate automaticamente non possono essere modificate o eliminate.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in per il database SAP HANA dall'elenco.
2. Nella pagina Risorse seleziona il tipo di risorsa dall'elenco Visualizza.
3. (Facoltativo) Fai clic su  *, quindi selezionare il nome host.

Puoi quindi cliccare su  * per chiudere il riquadro del filtro.

4. Fare clic su **Aggiorna risorse** per scoprire le risorse disponibili sull'host.

Le risorse vengono visualizzate insieme a informazioni quali tipo di risorsa, nome host, gruppi di risorse associati, tipo di backup, criteri e stato generale.

- Se il database si trova su un archivio NetApp e non è protetto, nella colonna Stato generale viene visualizzato Non protetto.
- Se il database si trova su un sistema di archiviazione NetApp ed è protetto e non viene eseguita alcuna operazione di backup, nella colonna Stato generale viene visualizzato Backup non eseguito. In caso contrario, lo stato cambierà in Backup non riuscito o Backup riuscito in base allo stato dell'ultimo backup.



Se nel database SAP HANA non è configurata una chiave HDB Secure User Store, accanto alla risorsa viene visualizzata un'icona a forma di lucchetto rosso. Se durante una successiva operazione di individuazione, la chiave HDB Secure User Store configurata risulta errata o non consente l'accesso al database stesso, l'icona del lucchetto rosso riapparirà.



È necessario aggiornare le risorse se i database vengono rinominati all'esterno di SnapCenter.

Dopo aver finito

È necessario configurare la chiave HDB Secure User Store e l'utente HDBSQL OS per poter proteggere il database o aggiungerlo al gruppo di risorse per eseguire operazioni di protezione dei dati.

["Configurare la chiave di archivio utente HDB e l'utente del sistema operativo HDBSQL per il database SAP"](#)

Preparare contenitori di database multitenant per la protezione dei dati

Per gli host SAP HANA registrati direttamente in SnapCenter, l'installazione o l'aggiornamento del plug-in SnapCenter per il database SAP HANA attiverà un rilevamento automatico delle risorse sull'host. Dopo aver installato o aggiornato il plug-in, per ogni risorsa MDC (Multitenant Database Container) presente sull'host del plug-in, verrà automaticamente rilevata un'altra risorsa MDC con un formato GUID diverso e registrata in SnapCenter. La nuova risorsa sarà nello stato "bloccato".

Informazioni su questo compito

Ad esempio, in SnapCenter 4.2, se la risorsa E90 MDC si trovava sull'host del plug-in ed era stata registrata manualmente, dopo l'aggiornamento a SnapCenter 4.3, un'altra risorsa E90 MDC con un GUID diverso verrà rilevata e registrata in SnapCenter.



I backup associati alla risorsa di SnapCenter 4.2 e versioni precedenti devono essere conservati fino alla scadenza del periodo di conservazione. Una volta scaduto il periodo di conservazione, è possibile eliminare la vecchia risorsa MDC e continuare a gestire la nuova risorsa MDC rilevata automaticamente.

‘Old MDC resource’ è la risorsa MDC per un host plug-in aggiunto manualmente in SnapCenter 4.2 o versioni precedenti.

Per iniziare a utilizzare la nuova risorsa individuata in SnapCenter 4.3 per le operazioni di protezione dei dati, procedere come segue:

Passi

1. Nella pagina Risorse, seleziona la vecchia risorsa MDC con i backup aggiunti alla versione precedente SnapCenter e mettila in “modalità di manutenzione” dalla pagina Topologia.

Se la risorsa fa parte di un gruppo di risorse, impostare il gruppo di risorse in “modalità di manutenzione”.

2. Configurare la nuova risorsa MDC rilevata dopo l'aggiornamento a SnapCenter 4.3 selezionando la nuova risorsa dalla pagina Risorse.

“Nuova risorsa MDC” è la nuova risorsa MDC scoperta dopo che SnapCenter Server e l'host del plug-in sono stati aggiornati alla versione 4.3. La nuova risorsa MDC può essere identificata come una risorsa con lo stesso SID della vecchia risorsa MDC, per un dato host e con un'icona a forma di lucchetto rosso accanto nella pagina Risorse.

3. Proteggi la nuova risorsa MDC scoperta dopo l'aggiornamento a SnapCenter 4.3 selezionando criteri di protezione, pianificazioni e impostazioni di notifica.
4. Eliminare i backup eseguiti in SnapCenter 4.2 o versioni precedenti in base alle impostazioni di conservazione.
5. Eliminare il gruppo di risorse dalla pagina Topologia.
6. Eliminare la vecchia risorsa MDC dalla pagina Risorse.

Ad esempio, se il periodo di conservazione degli snapshot primari è di 7 giorni e quello degli snapshot secondari è di 45 giorni, una volta trascorsi 45 giorni e dopo l'eliminazione di tutti i backup, è necessario eliminare il gruppo di risorse e la vecchia risorsa MDC.

Informazioni correlate

["Configurare la chiave di archivio utente HDB e l'utente del sistema operativo HDBSQL per il database SAP HANA"](#)

["Visualizza i backup e i cloni del database SAP HANA nella pagina Topologia"](#)

Aggiungere manualmente le risorse all'host del plug-in

La scoperta automatica non è supportata per alcune istanze HANA. È necessario aggiungere queste risorse manualmente.

Prima di iniziare

- È necessario aver completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host, la configurazione delle connessioni al sistema di archiviazione e l'aggiunta della chiave di archiviazione utente HDB.
- Per la replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse di tale sistema HANA in un gruppo di risorse ed eseguire un backup del gruppo di risorse. Ciò garantisce un backup senza interruzioni durante la modalità takeover-failback.

["Crea gruppi di risorse e allega criteri"](#) .

Informazioni su questo compito

Il rilevamento automatico non è supportato per le seguenti configurazioni:

- Layout RDM e VMDK



Nel caso in cui vengano scoperte le risorse di cui sopra, le operazioni di protezione dei dati non saranno supportate su tali risorse.

- Configurazione multi-host HANA
- Più istanze sullo stesso host
- Replicazione del sistema HANA con scalabilità multilivello
- Ambiente di replica a cascata in modalità di replicazione del sistema

Passi

1. Nel riquadro di navigazione a sinistra, seleziona il plug-in SnapCenter per il database SAP HANA dall'elenco a discesa, quindi fai clic su **Risorse**.
2. Nella pagina Risorse, fare clic su **Aggiungi database SAP HANA**.
3. Nella pagina Fornisci dettagli risorsa, esegui le seguenti azioni:

Per questo campo...	Fai questo...
Tipo di risorsa	Inserisci il tipo di risorsa. I tipi di risorsa sono Contenitore singolo, Contenitore di database multitenant (MDC) e Volume non dati.

Per questo campo...	Fai questo...
Nome del sistema HANA	Immettere il nome descrittivo del sistema SAP HANA. Questa opzione è disponibile solo se sono stati selezionati i tipi di risorsa Contenitore singolo o MDC.
SID	Inserire l'ID del sistema (SID). Il sistema SAP HANA installato è identificato da un singolo SID.
Host plug-in	Selezionare l'host del plug-in.
Chiavi di archiviazione utente protette HDB	Inserisci la chiave per connetterti al sistema SAP HANA. La chiave contiene le informazioni di accesso per connettersi al database. Per la replica del sistema SAP HANA, la chiave utente secondaria non viene convalidata. Verrà utilizzato durante l'acquisizione.
Utente del sistema operativo HDBSQL	Immettere il nome utente per il quale è configurata la chiave HDB Secure User Store. Per Windows, è obbligatorio che l'utente del sistema operativo HDBSQL sia l'utente SYSTEM. Pertanto, è necessario configurare la chiave HDB Secure User Store per l'utente SYSTEM.

4. Nella pagina Fornisci impronta di archiviazione, seleziona un sistema di archiviazione e scegli uno o più volumi, LUN e qtree, quindi fai clic su **Salva**.

Facoltativo: puoi cliccare su *  * icona per aggiungere più volumi, LUN e qtree da altri sistemi di archiviazione.

5. Rivedi il riepilogo e poi clicca su **Fine**.

I database vengono visualizzati insieme a informazioni quali SID, host del plug-in, gruppi di risorse e policy associati e stato generale

Se si desidera consentire agli utenti di accedere alle risorse, è necessario assegnare le risorse agli utenti. Ciò consente agli utenti di eseguire le azioni per le quali dispongono delle autorizzazioni sulle risorse loro assegnate.

["Aggiungi un utente o un gruppo e assegna ruoli e risorse"](#)

Dopo aver aggiunto i database, è possibile modificare i dettagli del database SAP HANA.

Non è possibile modificare quanto segue se sono presenti backup associati alla risorsa SAP HANA:

- Contenitori di database multi-tenant (MDC): SID o host client (plug-in) HDBSQL

- Contenitore singolo: host client (plug-in) SID o HDBSQL
- Volume non dati: nome della risorsa, SID associato o host del plug-in

Creare policy di backup per i database SAP HANA

Prima di utilizzare SnapCenter per eseguire il backup delle risorse del database SAP HANA, è necessario creare una policy di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup. Una policy di backup è un insieme di regole che regolano il modo in cui si gestiscono, si pianificano e si conservano i backup.

Prima di iniziare

- Devi aver definito la tua strategia di backup.

Per maggiori dettagli, consultare le informazioni sulla definizione di una strategia di protezione dei dati per i database SAP HANA.

- È necessario prepararsi alla protezione dei dati completando attività quali l'installazione di SnapCenter, l'aggiunta di host, la configurazione delle connessioni al sistema di archiviazione e l'aggiunta di risorse.
- Se si stanno replicando gli snapshot su un mirror o un vault, l'amministratore SnapCenter deve aver assegnato le SVM sia per il volume di origine che per quello di destinazione.

Inoltre, è possibile specificare le impostazioni di replica, script e applicazione nel criterio. Queste opzioni consentono di risparmiare tempo quando si desidera riutilizzare il criterio per un altro gruppo di risorse.

- Esaminare i prerequisiti e le limitazioni specifici SnapMirror ActiveSync. Per informazioni fare riferimento ["Limiti degli oggetti per la sincronizzazione attiva SnapMirror"](#).

Informazioni su questo compito

- Replica del sistema SAP HANA
 - È possibile proteggere il sistema SAP HANA primario e possono essere eseguite tutte le operazioni di protezione dei dati.
 - È possibile proteggere il sistema SAP HANA secondario, ma non è possibile creare backup.

Dopo il failover, tutte le operazioni di protezione dei dati possono essere eseguite poiché il sistema SAP HANA secondario diventa il sistema SAP HANA primario.

Non è possibile creare un backup per il volume dati SAP HANA, ma SnapCenter continua a proteggere i volumi non dati (NDV).

- SnapLock
 - Se è selezionata l'opzione "Conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere inferiore o uguale ai giorni di conservazione indicati.
 - Specificando un periodo di blocco degli snapshot si impedisce l'eliminazione degli snapshot fino alla scadenza del periodo di conservazione. Ciò potrebbe comportare la conservazione di un numero di snapshot maggiore rispetto al conteggio specificato nella policy.
 - Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **Nuovo**.
4. Nella pagina Nome, immettere il nome e i dettagli della policy.
5. Nella pagina Tipo di policy, procedere come segue:
 - Scegli il tipo di archiviazione
 - Scegli il tipo di backup:

Se lo desidera...	Fai questo...
Crea un backup utilizzando la tecnologia Snapshot	Selezionare Basato su snapshot .
Eseguire un controllo di integrità del database	Selezionare Backup basato su file . Viene eseguito il backup solo dei tenant attivi.

6. Nella pagina Snapshot e replica, procedere come segue:

- Specificare il tipo di pianificazione selezionando **Su richiesta, Ora, Giornaliera, Settimanale o Mensile**.



È possibile specificare la pianificazione (data di inizio, data di fine e frequenza) per l'operazione di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e la stessa frequenza di backup, ma consente anche di assegnare pianificazioni di backup diverse a ciascuna policy.



Se hai programmato per le 2:00, la pianificazione non verrà attivata durante l'ora legale (DST).

7. Nella pagina Snapshot e replica, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina Tipo di backup:

Se lo desidera...	Poi...
Conserva un certo numero di snapshot	Seleziona Copie da conservare, quindi specifica il numero di snapshot che desideri conservare. Se il numero di Snapshot supera il numero specificato, gli Snapshot più vecchi vengono eliminati per primi.  Il valore massimo di ritenzione è 1018. I backup non riusciranno se la conservazione è impostata su un valore superiore a quello supportato dalla versione ONTAP .  Per i backup basati su copie Snapshot, è necessario impostare il conteggio di conservazione su 2 o superiore se si prevede di abilitare la replica SnapVault . Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è lo Snapshot di riferimento per la relazione SnapVault finché uno Snapshot più recente non viene replicato sulla destinazione.  Per la replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse del sistema SAP HANA in un unico gruppo di risorse. In questo modo si garantisce che venga conservato il numero corretto di backup.  Per la replica del sistema SAP HANA, il numero totale di snapshot acquisiti sarà pari al set di conservazione per il gruppo di risorse. La rimozione dello Snapshot più vecchio si basa sul nodo in cui si trova lo Snapshot più vecchio. Ad esempio, la conservazione è impostata su 7 per un gruppo di risorse con SAP HANA System Replication primario e SAP HANA System Replication secondario. È possibile acquisire un massimo di 7 snapshot alla volta, inclusi sia SAP HANA System Replication primario che SAP HANA System Replication secondario.

Se lo desidera...	Poi...
Conserva gli snapshot per un certo numero di giorni	Selezionare Conserva copie per , quindi specificare il numero di giorni per cui si desidera conservare gli snapshot prima di eliminarli.
Periodo di blocco della copia snapshot	Selezionare Periodo di blocco della copia snapshot e specificare giorni, mesi o anni. Il periodo di conservazione SnapLock dovrebbe essere inferiore a 100 anni.

8. Selezionare un'etichetta Snapshot.



È possibile assegnare etichette SnapMirror agli snapshot primari per la replica remota, consentendo agli snapshot primari di trasferire l'operazione di replica degli snapshot da SnapCenter ai sistemi secondari ONTAP. Questa operazione può essere eseguita senza abilitare l'opzione SnapMirror o SnapVault nella pagina dei criteri.

9. Per i backup basati su copie snapshot, nella sezione Seleziona opzioni di replica secondaria, seleziona una o entrambe le seguenti opzioni di replica secondaria:

Per questo campo...	Fai questo...
Aggiorna SnapMirror dopo aver creato una copia Snapshot locale	Selezionare questo campo per creare copie mirror dei set di backup su un altro volume (replica SnapMirror). Questa opzione dovrebbe essere abilitata per la sincronizzazione attiva SnapMirror. Se la relazione di protezione in ONTAP è di tipo Mirror e Vault e si seleziona solo questa opzione, lo Snapshot creato sul primario non verrà trasferito alla destinazione, ma verrà elencato nella destinazione. Se si seleziona questo snapshot dalla destinazione per eseguire un'operazione di ripristino, viene visualizzato il messaggio di errore "La posizione secondaria non è disponibile per il backup con vault/mirroring selezionato". Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario. Facendo clic sul pulsante Aggiorna nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP. Vedere "Visualizza i backup e i cloni del database SAP HANA nella pagina Topologia".

Per questo campo...	Fai questo...
Aggiorna SnapVault dopo aver creato una copia Snapshot locale	Selezionare questa opzione per eseguire la replica del backup da disco a disco (backup SnapVault). Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario. Facendo clic sul pulsante Aggiorna nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP. Quando SnapLock è configurato solo sul secondario da ONTAP noto come SnapLock Vault, facendo clic sul pulsante Aggiorna nella pagina Topologia si aggiorna il periodo di blocco sul secondario recuperato da ONTAP. Per maggiori informazioni su SnapLock Vault vedere "Eseguire il commit delle copie Snapshot su WORM in una destinazione vault" Vedere "Visualizza i backup e i cloni del database SAP HANA nella pagina Topologia" .
Errore nel conteggio dei nuovi tentativi	Immettere il numero massimo di tentativi di replica consentiti prima che l'operazione venga interrotta.



È necessario configurare i criteri di conservazione SnapMirror in ONTAP per l'archiviazione secondaria per evitare di raggiungere il limite massimo di snapshot sull'archiviazione secondaria.

10. Rivedi il riepilogo e poi clicca su **Fine**.

Crea gruppi di risorse e allega criteri

Un gruppo di risorse è il contenitore a cui è necessario aggiungere le risorse di cui si desidera eseguire il backup e la protezione. Un gruppo di risorse consente di eseguire il backup simultaneo di tutti i dati associati a una determinata applicazione. Per qualsiasi attività di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario allegare una o più policy al gruppo di risorse per definire il tipo di processo di protezione dei dati che si desidera eseguire.

Informazioni su questo compito

- Per creare backup di replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse del sistema SAP HANA in un gruppo di risorse. Ciò garantisce un backup senza interruzioni durante la modalità takeover-failback.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino ereditano il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

- L'aggiunta di nuovi database senza SnapMirror ActiveSync a un gruppo di risorse esistente che contiene risorse con SnapMirror ActiveSync non è supportata.
- L'aggiunta di nuovi database a un gruppo di risorse esistente in modalità failover di SnapMirror ActiveSync non è supportata. È possibile aggiungere risorse al gruppo di risorse solo nello stato normale o di failback.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:

Per questo campo...	Fai questo...
Nome	Immettere un nome per il gruppo di risorse.  Il nome del gruppo di risorse non deve superare i 250 caratteri.
Etichette	Inserisci una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse. Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.
Utilizza il formato nome personalizzato per la copia Snapshot	Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot. Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

4. Nella pagina Risorse, seleziona un nome host dall'elenco a discesa **Host** e il tipo di risorsa dall'elenco a discesa **Tipo di risorsa**.

Ciò aiuta a filtrare le informazioni sullo schermo.
5. Seleziona le risorse dalla sezione **Risorse disponibili**, quindi fai clic sulla freccia destra per spostarle nella sezione **Risorse selezionate**.
6. Nella pagina Impostazioni applicazione, procedere come segue:
 - a. Fare clic sulla freccia **Backup** per impostare opzioni di backup aggiuntive:

Abilitare il backup del gruppo di coerenza ed eseguire le seguenti attività:

Per questo campo...	Fai questo...
Concediti del tempo per attendere il completamento dell'operazione Consistency Group Snapshot	Selezionare Urgente , Medio o Rilassato per specificare il tempo di attesa per il completamento dell'operazione Snapshot. Urgente = 5 secondi, Medio = 7 secondi e Rilassato = 20 secondi.
Disabilita la sincronizzazione WAFL	Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL .

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

Backups

☒ Enable consistency group backup

Afford time to wait for Consistency Group Snapshot operation to complete ⓘ

☒ Urgent

☐ Medium

☐ Relaxed

☐ Disable WAFL Sync

Scripts ⓘ

Custom Configurations ⓘ

Snapshot Copy Tool ⓘ

- Fare clic sulla freccia **Script** e immettere i comandi pre e post per le operazioni di quiesce, Snapshot e unquiesce. È anche possibile immettere i comandi pre da eseguire prima di uscire in caso di errore.
- Fare clic sulla freccia **Configurazioni personalizzate** e immettere le coppie chiave-valore personalizzate richieste per tutte le operazioni di protezione dei dati che utilizzano questa risorsa.

Parametro	Collocamento	Descrizione
ARCHIVE_LOG_ENABLE	(S/N)	Abilita la gestione dei log di archivio per eliminare i log di archivio.
CONSERVAZIONE_ARCHIVIO_LOG	numero_di_giorni	Specifica il numero di giorni per cui vengono conservati i registri di archivio. Questa impostazione deve essere uguale o maggiore di NTAP_SNAPSHOT_RETENTIONS.

Parametro	Collocamento	Descrizione
ARCHIVE_LOG_DIR	change_info_directory/logs	Specifica il percorso della directory che contiene i log di archivio.
ARCHIVE_LOG_EXT	estensione_file	Specifica la lunghezza dell'estensione del file di registro dell'archivio. Ad esempio, se il registro di archivio è log_backup_0_0_0_0.161518551942 9 e se il valore file_extension è 5, l'estensione del registro conserverà 5 cifre, ovvero 16151.
ARCHIVE_LOG_RECURSIVE_SE ARCH	(S/N)	Consente la gestione dei log di archivio all'interno delle sottodirectory. È necessario utilizzare questo parametro se i registri di archivio si trovano in sottodirectory.



Le coppie chiave-valore personalizzate sono supportate per i sistemi plug-in Linux SAP HANA e non sono supportate per il database SAP HANA registrato come plug-in centralizzato di Windows.

c. Fare clic sulla freccia **Strumento Copia snapshot** per selezionare lo strumento per creare snapshot:

Se vuoi...	Poi...
SnapCenter per utilizzare il plug-in per Windows e impostare il file system in uno stato coerente prima di creare uno snapshot. Per le risorse Linux, questa opzione non è applicabile.	Selezionare * SnapCenter con coerenza del file system*. Questa opzione non è applicabile al plug-in SnapCenter per il database SAP HANA.
SnapCenter per creare uno Snapshot del livello di archiviazione	Selezionare * SnapCenter senza coerenza del file system*.
Per immettere il comando da eseguire sull'host per creare copie Snapshot.	Selezionare Altro , quindi immettere il comando da eseguire sull'host per creare uno snapshot.

7. Nella pagina Criteri, procedere come segue:

a. Selezionare una o più policy dall'elenco a discesa.



Puoi anche creare una policy cliccando *  *.

I criteri sono elencati nella sezione Configura pianificazioni per i criteri selezionati.

- b. Nella colonna Configura pianificazioni, fare clic su *  * per la policy che vuoi configurare.
- c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi fare clic su **OK**.

Dove policy_name è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna **Pianificazioni applicate**.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Il server SMTP deve essere configurato in **Impostazioni > Impostazioni globali**.

9. Rivedi il riepilogo e poi clicca su **Fine**.

Crea gruppi di risorse e abilita la protezione secondaria per le risorse SAP HANA sui sistemi ASA r2

È necessario creare il gruppo di risorse per aggiungere le risorse presenti sui sistemi ASA r2. È anche possibile predisporre la protezione secondaria durante la creazione del gruppo di risorse.

Prima di iniziare

- È necessario assicurarsi di non aggiungere risorse ONTAP 9.x e risorse ASA r2 allo stesso gruppo di risorse.
- È necessario assicurarsi di non disporre di un database con risorse ONTAP 9.x e risorse ASA r2.

Informazioni su questo compito

- La protezione secondaria è disponibile solo se all'utente connesso è assegnato il ruolo per cui è abilitata la funzionalità **SecondaryProtection**.
- Se è stata abilitata la protezione secondaria, il gruppo di risorse viene messo in modalità di manutenzione durante la creazione dei gruppi di coerenza primario e secondario. Dopo aver creato i gruppi di coerenza primari e secondari, il gruppo di risorse esce dalla modalità di manutenzione.
- SnapCenter non supporta la protezione secondaria per una risorsa clone.

Passi

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:

- a. Immettere un nome per il gruppo di risorse nel campo Nome.



Il nome del gruppo di risorse non deve superare i 250 caratteri.

- b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

- c. Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

Ad esempio, `customtext_resource group_policy_hostname` o `resource group_hostname`. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

- d. Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup.



Dovresti usare esattamente la stessa destinazione impostata nell'applicazione, incluso il prefisso, se necessario.

4. Nella pagina Risorse, seleziona il nome host del database dall'elenco a discesa **Host**.



Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Selezionare le risorse ASA r2 dalla sezione Risorse disponibili e spostarle nella sezione Risorse selezionate.

6. Nella pagina Impostazioni applicazione, seleziona l'opzione di backup.

7. Nella pagina Criteri, procedere come segue:

- a. Selezionare una o più policy dall'elenco a discesa.



Puoi anche creare una policy cliccando  .

Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

- b. Clic  nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

- c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Se la protezione secondaria è abilitata per il criterio selezionato, viene visualizzata la pagina Protezione secondaria ed è necessario eseguire i seguenti passaggi:

- a. Selezionare il tipo di criterio di replica.



La politica di replica sincrona non è supportata.

- b. Specificare il suffisso del gruppo di coerenza che si desidera utilizzare.

- c. Dai menu a discesa Cluster di destinazione e SVM di destinazione, seleziona il cluster peer e l'SVM che desideri utilizzare.



Il cluster e il peering SVM non sono supportati da SnapCenter. Per eseguire il peering di cluster e SVM, è necessario utilizzare System Manager o ONTAP CLI.



Se le risorse sono già protette all'esterno di SnapCenter, verranno visualizzate nella sezione Risorse secondarie protette.

1. Nella pagina Verifica, procedere come segue:

- a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror o SnapVault ed eseguire la verifica sull'archiviazione secondaria.

- b. Clic  nella colonna Configura pianificazioni per configurare la pianificazione di verifica per tutti i tipi di pianificazione del criterio.

- c. Nella finestra di dialogo Aggiungi pianificazioni di verifica policy_name, eseguire le seguenti azioni:

Se lo desidera...	Fai questo...
Esegui la verifica dopo il backup	Selezionare Esegui verifica dopo il backup .
Pianifica una verifica	Selezionare Esegui verifica pianificata , quindi selezionare il tipo di pianificazione dall'elenco a discesa.

- d. Seleziona **Verifica su posizione secondaria** per verificare i backup sul sistema di archiviazione secondario.

- e. Fare clic su **OK**.

Le pianificazioni di verifica configurate sono elencate nella colonna Pianificazioni applicate.

2. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.



Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtServer.

3. Rivedi il riepilogo e poi clicca su **Fine**.

Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per il database SAP HANA

È necessario creare una connessione alla macchina virtuale di archiviazione (SVM) e delle credenziali prima di utilizzare i cmdlet di PowerShell per eseguire il backup, il ripristino o la clonazione dei database SAP HANA.

Prima di iniziare

- Dovresti aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- Per creare connessioni di archiviazione è necessario disporre delle autorizzazioni necessarie nel ruolo di amministratore dell'infrastruttura.
- È necessario assicurarsi che non siano in corso installazioni di plug-in.

Le installazioni di plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage, poiché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nell'interfaccia utente grafica SnapCenter come "Non disponibile per il backup" o "Non su storage NetApp".

- I nomi dei sistemi di archiviazione devono essere univoci.

SnapCenter non supporta più sistemi di archiviazione con lo stesso nome su cluster diversi. Ogni sistema di archiviazione supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF dati univoco.

Passi

1. Avviare una sessione di connessione PowerShell utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-SmStorageConnection
```

2. Creare una nuova connessione al sistema di archiviazione utilizzando il cmdlet Add-SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap  
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Creare una nuova credenziale utilizzando il cmdlet Add-SmCredential.

Questo esempio mostra come creare una nuova credenziale denominata FinanceAdmin con credenziali Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. Aggiungere l'host di comunicazione SAP HANA a SnapCenter Server.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName FinanceAdmin -PluginCode hana
```

5. Installare il pacchetto e il plug-in SnapCenter per il database SAP HANA sull'host.

Per Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana
```

Per Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana -FileSystemCode scw -RunAsName FinanceAdmin
```

6. Imposta il percorso per il client HDBSQL.

Per Windows:

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program Files\sap\hdbclient\hdbsql.exe"}
```

Per Linux:

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com -PluginCode hana -configSettings @{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

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, puoi anche fare riferimento a ["Guida di riferimento ai cmdlet del software SnapCenter"](#).

Eseguire il backup dei database SAP HANA

Se una risorsa non fa ancora parte di alcun gruppo di risorse, è possibile eseguirne il backup dalla pagina Risorse.

Prima di iniziare

- Devi aver creato una policy di backup.

- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo ONTAP assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- Per l'operazione di backup basata su copia snapshot, assicurarsi che tutti i database tenant siano validi e attivi.
- Per creare backup di replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse del sistema SAP HANA in un gruppo di risorse. Ciò garantisce un backup senza interruzioni durante la modalità takeover-failback.

"Crea gruppi di risorse e allega criteri" .

"Eseguire il backup dei gruppi di risorse"

- Se si desidera creare un backup basato su file quando uno o più database tenant sono inattivi, impostare il parametro ALLOW_FILE_BASED_BACKUP_IFINACTIVE_TENANTS_PRESENT su **YES** nel file delle proprietà HANA utilizzando Set-SmConfigSettings cmdlet.

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, puoi anche fare riferimento a ["Guida di riferimento ai cmdlet del software SnapCenter"](#)

- Per i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
 - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*



Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

Interfaccia utente SnapCenter

Passi

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorsa, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

Seleziona  *, quindi selezionare il nome host e il tipo di risorsa per filtrare le risorse. Puoi quindi selezionare  per chiudere il riquadro del filtro.

3. Seleziona la risorsa di cui vuoi eseguire il backup.
4. Nella pagina Risorsa, seleziona **Usa formato nome personalizzato per copia Snapshot**, quindi immetti un formato nome personalizzato che desideri utilizzare per il nome Snapshot.

Ad esempio, *customtext_policy_hostname* o *resource_hostname*. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

5. Nella pagina Impostazioni applicazione, procedere come segue:

- Selezionare la freccia **Backup** per impostare opzioni di backup aggiuntive:

Se necessario, abilitare il backup del gruppo di coerenza ed eseguire le seguenti attività:

Per questo campo...	Fai questo...
Concediti del tempo per attendere il completamento dell'operazione "Consistency Group Snapshot"	Selezionare Urgente , Medio o Rilassato per specificare il tempo di attesa per il completamento dell'operazione Snapshot. Urgente = 5 secondi, Medio = 7 secondi e Rilassato = 20 secondi.
Disabilita la sincronizzazione WAFL	Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL .

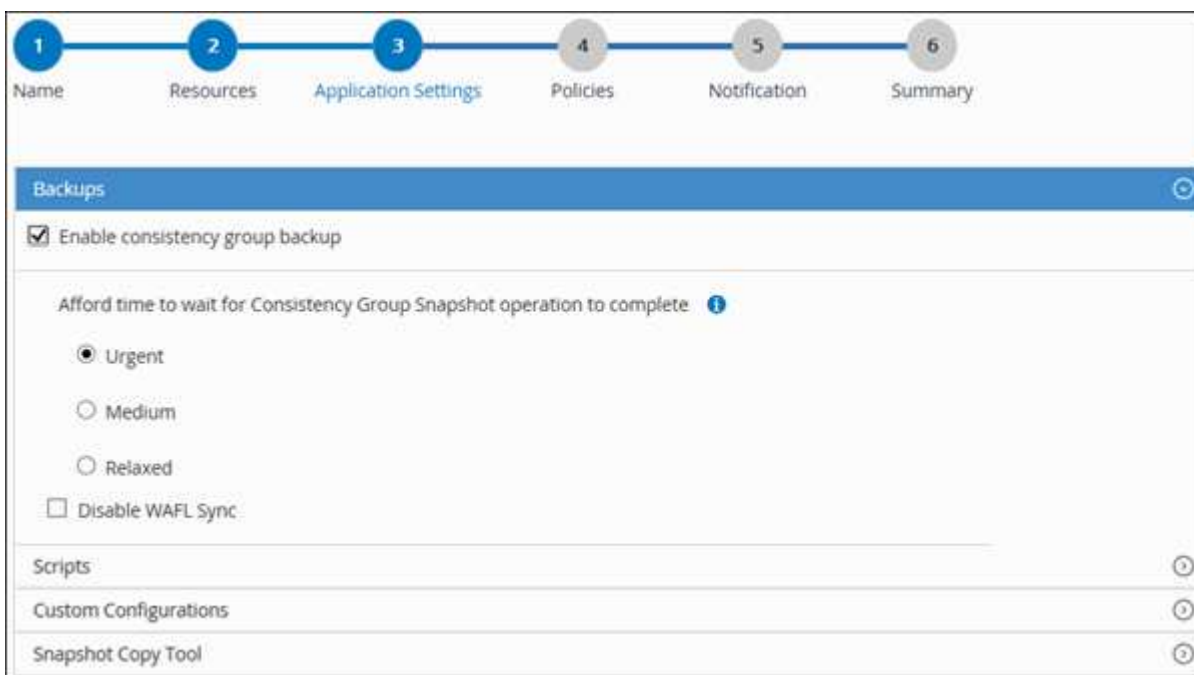
- Selezionare la freccia **Script** per eseguire i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce.

È anche possibile eseguire i comandi pre prima di uscire dall'operazione di backup. I prescript e i postscript vengono eseguiti nel server SnapCenter .

- Selezionare la freccia **Configurazioni personalizzate**, quindi immettere le coppie di valori personalizzati richieste per tutti i processi che utilizzano questa risorsa.
- Selezionare la freccia **Strumento Copia snapshot** per selezionare lo strumento per creare snapshot:

Se vuoi...	Poi...
SnapCenter per creare uno Snapshot a livello di archiviazione	Selezionare * SnapCenter senza coerenza del file system*.

Se vuoi...	Poi...
SnapCenter per utilizzare il plug-in per Windows per mettere il file system in uno stato coerente e quindi creare uno Snapshot	Selezionare * SnapCenter con coerenza del file system*.
Per immettere il comando per creare uno Snapshot	Selezionare Altro , quindi immettere il comando per creare uno Snapshot.



6. Nella pagina Criteri, procedere come segue:

- a. Selezionare una o più policy dall'elenco a discesa.



Puoi anche creare una policy cliccando *  *.

Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

- b. Seleziona *  * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.
- c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi selezionare **OK**.

policy_name è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

7. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. SMTP deve essere configurato anche in **Impostazioni > Impostazioni globali**.

8. Rivedi il riepilogo e seleziona **Fine**.

Viene visualizzata la pagina della topologia delle risorse.

9. Seleziona **Esegui backup adesso**.

10. Nella pagina Backup, procedere come segue:

- a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa **Criterio** seleziona il criterio che desideri utilizzare per il backup.

Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

- b. Selezionare **Backup**.

11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio > Lavori**.

- Nelle configurazioni MetroCluster, SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

Per informazioni, vedere: ["Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover MetroCluster"](#)

- Se si esegue il backup dei dati dell'applicazione su VMDK e la dimensione dell'heap Java per il SnapCenter Plug-in for VMware vSphere non è sufficientemente grande, il backup potrebbe non riuscire.

Per aumentare la dimensione dell'heap Java, individuare il file di script `/opt/netapp/init_scripts/scvservice`. In quello script, il comando `do_start method` avvia il servizio plug-in SnapCenter VMware. Aggiornare il comando come segue: `Java -jar -Xmx8192M -Xms4096M`

Cmdlet di PowerShell

Passi

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet `Open-SmConnection`.

```
Open-smconnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\
```

Viene visualizzata la richiesta di nome utente e password.

2. Aggiungere risorse utilizzando il cmdlet `Add-SmResources`.

Questo esempio mostra come aggiungere un database SAP HANA di tipo `SingleContainer`:

```
C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'
-DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint
(@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary
"}) -SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys
'HS10' -osdbuser 'h10adm' -filebackupprefix 'H10_'
```

Questo esempio mostra come aggiungere un database SAP HANA di tipo MultipleContainers:

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType
MultipleContainers -StorageFootPrint
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.net
app.com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType
'MultiTenant'
```

Questo esempio mostra come creare una risorsa di volume non dati:

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sccore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

3. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.

Questo esempio crea un criterio di backup per un backup basato su copia Snapshot:

```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType
Backup -PluginPolicyType hana -BackupType SnapShotBasedBackup
```

Questo esempio crea un criterio di backup per un backup basato su file:

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
-PluginPolicyType hana -BackupType FileBasedBackup
```

4. Proteggere la risorsa o aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.

Questo esempio protegge una singola risorsa contenitore:

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies
hana_snapshotbased,hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

Questo esempio protegge una risorsa composta da più contenitori:

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies
hana_snapshotbased,hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="MDC\SID"}
-Description test -usesnapcenterwithoutfilesystemconsistency
```

Questo esempio crea un nuovo gruppo di risorse con i criteri e le risorse specificati:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sscore.test.com";"Uid"="SID"},@{"Host"="sc
corelinux62.sscore.test.com";"Uid"="MDC\SID"})
-Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency -plugincode 'HANA'
```

Questo esempio crea un gruppo di risorse di volume non dati:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="H11";"PluginName"=
"hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="MDC\H31";"Pl
uginName"="hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="No
nDataVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies
hanaprimary
```

5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

Questo esempio mostra come eseguire il backup di un gruppo di risorse:

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

Questo esempio esegue il backup di una risorsa protetta:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
-Policy hana_Filebased
```

6. Monitorare lo stato del processo (in esecuzione, completato o non riuscito) utilizzando il cmdlet `Get-smJobSummaryReport`.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Monitorare i dettagli del processo di backup, come ID del backup e nome del backup, per eseguire operazioni di ripristino o clonazione utilizzando il cmdlet `Get-SmBackupReport`.

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

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, puoi anche fare riferimento a ["Guida di riferimento ai cmdlet del software SnapCenter"](#).

Eseguire il backup dei gruppi di risorse

Un gruppo di risorse è una raccolta di risorse su un host. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

Prima di iniziare

- È necessario aver creato un gruppo di risorse con un criterio associato.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo ONTAP assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.

Informazioni su questo compito

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina Risorse. Se a un gruppo di risorse è associato un criterio e configurata una pianificazione, i backup vengono eseguiti automaticamente in base alla pianificazione.

Passi

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.

È possibile cercare il gruppo di risorse inserendo il nome del gruppo di risorse nella casella di ricerca oppure selezionando  e quindi selezionando il tag. Puoi quindi selezionare  per chiudere il riquadro del filtro.

3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi seleziona **Esegui backup ora**.
4. Nella pagina Backup, procedere come segue:

- a. Se hai associato più policy al gruppo di risorse, dall'elenco a discesa **Policy** seleziona la policy che desideri utilizzare per il backup.

Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

- b. Selezionare **Backup**.

5. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio > Lavori**.

Monitorare le operazioni di backup dei database SAP HANA

È possibile monitorare l'avanzamento delle diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere opportuno controllare lo stato di avanzamento per determinare quando il processo è completato o se si è verificato un problema.

Informazioni su questo compito

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

-  In corso

-  Completato con successo
-  Fallito
-  Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
-  In coda
-  Annullato

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Lavori**.
3. Nella pagina Lavori, procedere come segue:
 - a. Clic  per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
 - b. Specificare le date di inizio e fine.
 - c. Dall'elenco a discesa **Tipo**, selezionare **Backup**.
 - d. Dal menu a discesa **Stato**, seleziona lo stato del backup.
 - e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.



Sebbene lo stato del processo di backup venga visualizzato  , quando fai clic sui dettagli del processo, potresti vedere che alcune delle attività secondarie dell'operazione di backup sono ancora in corso o contrassegnate con segnali di avviso.

5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

Monitorare le operazioni di protezione dei dati sui database SAP HANA nel riquadro Attività

Il riquadro Attività visualizza le cinque operazioni eseguite più di recente. Nel riquadro Attività viene inoltre visualizzato quando è stata avviata l'operazione e il suo stato.

Il riquadro Attività visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificato.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Clic  nel riquadro Attività per visualizzare le cinque operazioni più recenti.

Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli lavoro**.

Annulla le operazioni di backup per SAP HANA

È possibile annullare le operazioni di backup in coda.

Cosa ti servirà

- Per annullare le operazioni, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del lavoro.
- È possibile annullare un'operazione di backup dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di backup in esecuzione.
- È possibile utilizzare l'interfaccia utente grafica SnapCenter, i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di backup.
- Il pulsante **Annulla lavoro** è disabilitato per le operazioni che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di backup in coda degli altri membri mentre utilizzi quel ruolo.

Passi

1. Eseguire una delle seguenti azioni:

Dal...	Azione
Pagina di monitoraggio	a. Nel riquadro di navigazione a sinistra, fare clic su Monitor > Lavori. b. Selezionare l'operazione, quindi fare clic su Annulla lavoro.
Riquadro attività	a. Dopo aver avviato l'operazione di backup, fare clic su ** nel riquadro Attività per visualizzare le cinque operazioni più recenti. b. Selezionare l'operazione. c. Nella pagina Dettagli lavoro, fare clic su Annulla lavoro.

L'operazione viene annullata e la risorsa torna allo stato precedente.

Visualizza i backup e i cloni del database SAP HANA nella pagina Topologia

Quando ci si prepara a eseguire il backup o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup e i cloni sullo storage primario e secondario.

Informazioni su questo compito

È possibile esaminare le seguenti icone nella vista Gestisci copie per determinare se i backup e i cloni sono disponibili nell'archivio primario o secondario (copie mirror o copie Vault).

•



visualizza il numero di backup e cloni disponibili sullo storage primario.

-  visualizza il numero di backup e cloni di cui è stato eseguito il mirroring sullo storage secondario mediante la tecnologia SnapMirror .
-  visualizza il numero di backup e cloni replicati sullo storage secondario mediante la tecnologia SnapVault .



Il numero di backup visualizzato include i backup eliminati dall'archivio secondario. Ad esempio, se hai creato 6 backup utilizzando un criterio per conservarne solo 4, il numero di backup visualizzato è 6.



I cloni di un backup di un mirror con versione flessibile su un volume di tipo mirror-vault vengono visualizzati nella vista topologia, ma il conteggio dei backup mirror nella vista topologia non include il backup con versione flessibile.

Nella pagina Topologia è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e quindi selezionarli per eseguire operazioni di protezione dei dati.

Se si dispone di una relazione secondaria come SnapMirror ActiveSync (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC]), è possibile visualizzare le seguenti icone aggiuntive:

-  Il sito replica è attivo.
-  Il sito replica è inattivo.
-  La relazione tra specchio secondario e volta non è stata ristabilita.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

Se la risorsa è protetta, viene visualizzata la pagina della topologia della risorsa selezionata.

4. Consultare la **scheda Riepilogo** per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

La sezione **Scheda riepilogativa** mostra il numero totale di backup basati su file, backup basati su copie snapshot e cloni.

Facendo clic sul pulsante **Aggiorna** viene avviata una query dello spazio di archiviazione per visualizzare un conteggio accurato.

Se viene eseguito un backup abilitato per SnapLock , facendo clic sul pulsante **Aggiorna** vengono aggiornati i tempi di scadenza SnapLock primario e secondario recuperati da ONTAP. Una pianificazione settimanale aggiorna anche il tempo di scadenza primario e secondario SnapLock recuperato da ONTAP.

Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza SnapLock per il backup sarà il tempo di scadenza SnapLock più lungo impostato per uno Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

Per la sincronizzazione attiva SnapMirror , facendo clic sul pulsante **Aggiorna** si aggiorna l'inventario di backup SnapCenter interrogando ONTAP sia per i siti primari che per quelli di replica. Una pianificazione settimanale esegue questa attività anche per tutti i database contenenti la relazione di sincronizzazione attiva SnapMirror .

- Per SnapMirror ActiveSync e solo per ONTAP 9.14.1, le relazioni Async Mirror o Async MirrorVault con la nuova destinazione primaria devono essere configurate manualmente dopo il failover. Da ONTAP 9.15.1 in poi, Async Mirror o Async MirrorVault vengono configurati automaticamente sulla nuova destinazione primaria.
- Dopo il failover, è necessario creare un backup affinché SnapCenter sia a conoscenza del failover. È possibile fare clic su **Aggiorna** solo dopo aver creato un backup.

5. Nella vista Gestisci copie, fare clic su **Backup** o **Cloni** dall'archivio primario o secondario per visualizzare i dettagli di un backup o di un clone.

I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione ed eliminazione.



Non è possibile rinominare o eliminare i backup presenti nell'archivio secondario.

7. Se si desidera eliminare un clone, selezionare il clone dalla tabella, quindi fare clic su  .
8. Se vuoi dividere un clone, seleziona il clone dalla tabella, quindi fai clic su  .

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 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.