Eseguire il backup delle risorse SAP HANA

SnapCenter Software 4.8

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/it-it/snapcenter-48/protect-hana/task_back_up_sap_hana_resources.html on September 26, 2025. Always check docs.netapp.com for the latest.

Sommario

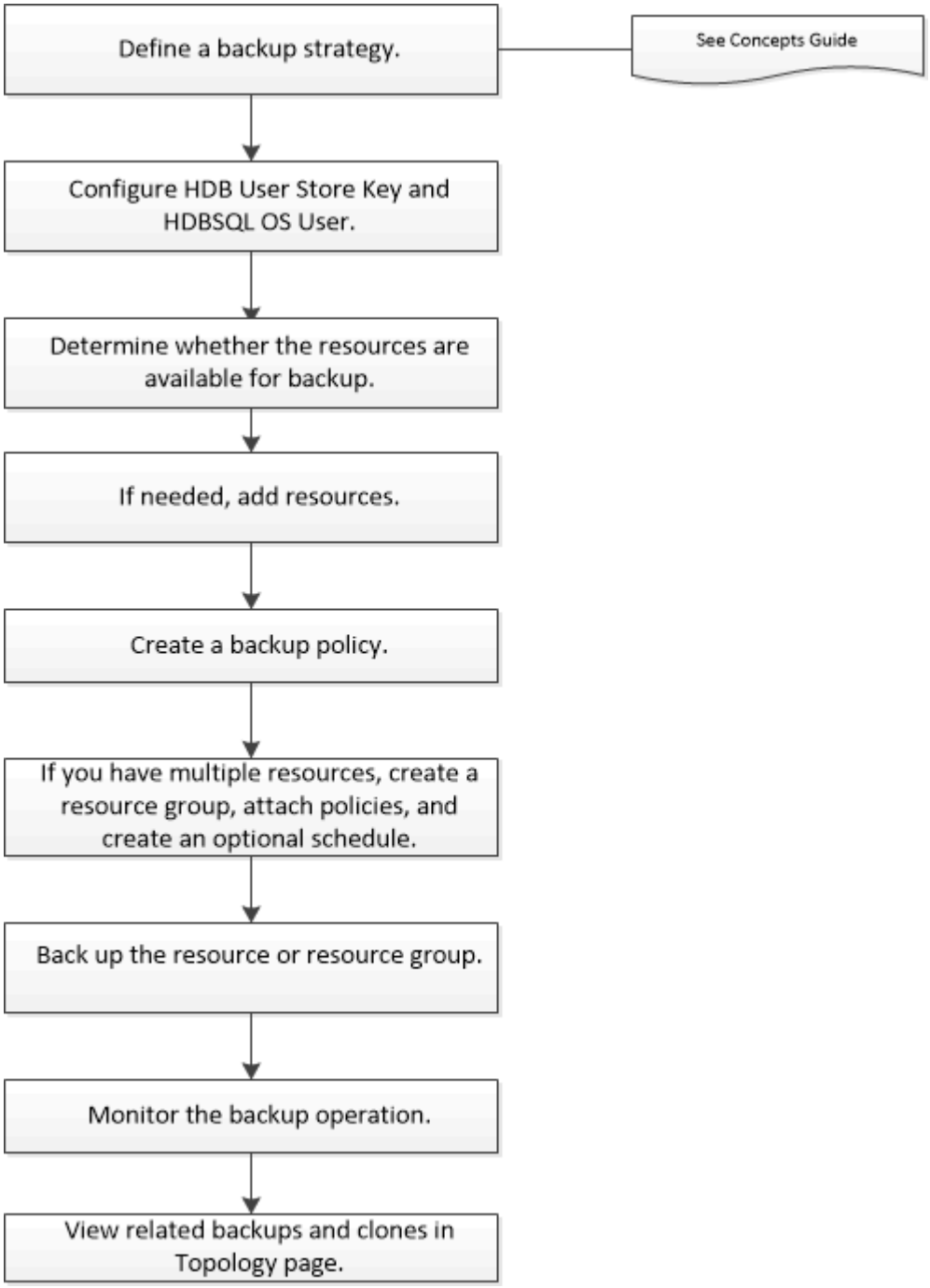
Eseguire il backup delle risorse SAP HANA . . . 1
- Eseguire il backup delle risorse SAP HANA . . . 1
- Configurare HDB User Store Key e HDBSQL OS User per il database SAP HANA . . . 2
- Scopri le risorse e prepara i container di database multi-tenant per la protezione dei dati . . . 2
  - Rilevare automaticamente i database . . . 2
  - Preparare container di database multi-tenant per la protezione dei dati . . . 4
- Aggiungere le risorse manualmente all'host del plug-in . . . 5
- Creare policy di backup per i database SAP HANA . . . 7
- Creare gruppi di risorse e allegare policy . . . 12
- Eseguire il backup dei database SAP HANA . . . 16
- Eseguire il backup dei gruppi di risorse . . . 19
- Creare una connessione al sistema storage e una credenziale utilizzando i cmdlet PowerShell per il database SAP HANA . . . 20
- Eseguire il backup dei database utilizzando i cmdlet PowerShell . . . 22
- Monitorare le operazioni di backup . . . 25
  - Monitorare le operazioni di backup dei database SAP HANA . . . 25
  - Monitorate le operazioni di protezione dei dati sui database SAP HANA nel riquadro attività . . . 26
- Annulla le operazioni di backup per SAP HANA . . . 27
- Visualizzare i backup e i cloni del database SAP HANA nella pagina topologia . . . 28

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 workflow di backup include la pianificazione, l'identificazione dei database per il backup, la gestione delle policy di backup, la creazione di gruppi di risorse e l'aggiunta di policy, 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 inoltre possibile utilizzare i cmdlet PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida in linea del cmdlet di SnapCenter e le informazioni di riferimento del cmdlet contengono ulteriori informazioni sui cmdlet di PowerShell. "Guida di riferimento al cmdlet del software SnapCenter".

Configurare HDB User Store Key e HDBSQL OS User 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.

Cosa ti serve

- Se il database SAP HANA non dispone della chiave HDB Secure User Store e dell'utente HDB SQL OS, viene visualizzata un'icona a forma di lucchetto rosso solo per le risorse rilevate automaticamente. Se durante un'operazione di rilevamento successiva, la chiave di memorizzazione utente sicura HDB configurata non è corretta o non ha consentito l'accesso al database stesso, viene visualizzata nuovamente l'icona del lucchetto rosso.
- È necessario configurare la chiave di archiviazione utente sicura HDB e l'utente SQL OS HDB per 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 HDB SQL OS User è configurato per accedere solo al database tenant, l'operazione di rilevamento non riesce.

Fasi

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

   È quindi possibile fare clic su per chiudere il riquadro del filtro.
4. Selezionare il database, quindi fare clic su **Configura database**.
5. Nella sezione Configure database settings (Configura impostazioni database), immettere HDB Secure User Store Key (chiave archivio utente sicura HDB).

   Viene visualizzato il nome host del plug-in e l'utente SQL del sistema operativo HDB viene automaticamente inserito nel campo <sid>.
6. Fare clic su **OK**.

È possibile modificare la configurazione del database dalla pagina topologia.

Scopri le risorse e prepara i container di database multi-tenant per la protezione dei dati

Rilevare automaticamente i database

Le risorse sono database SAP HANA e volumi 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.

Cosa ti serve

- È necessario aver già completato attività come l'installazione del server SnapCenter, l'aggiunta della chiave di archiviazione utente HDB, l'aggiunta di host e la configurazione delle connessioni del sistema di storage.
- È necessario aver configurato la chiave di archiviazione utente sicura HDB e l'utente del sistema operativo SQL HDB sull'host Linux.
  - È necessario configurare la chiave di memorizzazione utente HDB con l'utente SID adm. Ad esempio, per il sistema HANA con A22 come SID, la chiave di memorizzazione utente HDB deve essere configurata con a22adm.
- Il plug-in SnapCenter per database SAP HANA non supporta il rilevamento automatico delle risorse che risiedono negli ambienti virtuali RDM/VMDK. Durante l'aggiunta manuale dei database, è necessario fornire le informazioni di storage per gli ambienti virtuali.

A proposito di questa attività

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

Le risorse rilevate automaticamente non possono essere modificate o eliminate.

Fasi

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

   È quindi possibile fare clic su * *per chiudere il riquadro del filtro.

4. Fare clic su **Refresh Resources** (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 uno storage NetApp e non è protetto, nella colonna Stato generale viene visualizzato non protetto.
   - Se il database si trova su un sistema storage NetApp e viene protetto e non viene eseguita alcuna operazione di backup, nella colonna Stato generale viene visualizzato Backup Not run (Backup non eseguito). In caso contrario, lo stato cambia in Backup failed (Backup non riuscito) o Backup successed (Backup riuscito) in base allo stato dell'ultimo backup.

   Se il database SAP HANA non dispone di una chiave di memorizzazione utente sicura HDB configurata, accanto alla risorsa viene visualizzata un'icona a forma di lucchetto rosso. Se durante un'operazione di rilevamento successiva, la chiave di memorizzazione utente sicura HDB configurata non è corretta o non ha consentito l'accesso al database stesso, viene visualizzata nuovamente l'icona del lucchetto rosso.

È necessario aggiornare le risorse se i database vengono rinominati al di fuori di SnapCenter.

Al termine

È necessario configurare la chiave di archiviazione utente sicura HDB e l'utente del sistema operativo HDBSQL per proteggere il database o aggiungerlo al gruppo di risorse per eseguire operazioni di protezione dei dati.

"Configurare HDB User Store Key e HDBSQL OS User per il database SAP HANA"

Preparare container di database multi-tenant 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 l'installazione o l'aggiornamento del plug-in, per ogni risorsa MDC (Multitenant Database Container) che si trovava sull'host del plug-in, un'altra risorsa MDC verrà rilevata automaticamente con un formato GUID diverso e registrata in SnapCenter. La nuova risorsa sarà in stato "Locked".

A proposito di questa attività

Ad esempio, in SnapCenter 4.2, se la risorsa MDC E90 era localizzata nell'host del plug-in e registrata manualmente, dopo l'aggiornamento a SnapCenter 4.3, un'altra risorsa MDC E90 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.

Attenersi alla seguente procedura per iniziare a utilizzare la nuova risorsa scoperta in SnapCenter 4.3 per le operazioni di protezione dei dati:

Fasi

1. Nella pagina risorse, selezionare la vecchia risorsa MDC con i backup aggiunti alla release precedente di SnapCenter e posizionarla in "maintage mode" dalla pagina topologia.

   Se la risorsa fa parte di un gruppo di risorse, posizionare il gruppo di risorse in "maintance mode".

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 risorsa MDC scoperta di recente e scoperta dopo l'aggiornamento del server SnapCenter e dell'host plug-in alla versione 4.3. La nuova risorsa MDC può essere identificata come risorsa con lo stesso SID della vecchia risorsa MDC, per un determinato host e con un'icona a forma di lucchetto rosso accanto alla risorsa nella pagina risorse.

3. Proteggere la nuova risorsa MDC rilevata 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 Resources (risorse).

   Ad esempio, se il periodo di conservazione delle copie Snapshot primarie è di 7 giorni e la conservazione delle copie Snapshot secondarie è di 45 giorni, dopo il completamento di 45 giorni e dopo l'eliminazione di tutti i backup, è necessario eliminare il gruppo di risorse e la risorsa MDC precedente.

Ulteriori informazioni

"Configurare HDB User Store Key e HDBSQL OS User per il database SAP HANA"

"Visualizzare i backup e i cloni del database SAP HANA nella pagina topologia"

Aggiungere le risorse manualmente all'host del plug-in

Il rilevamento automatico non è supportato per alcune istanze di HANA. È necessario aggiungere queste risorse manualmente.

Cosa ti serve

- È necessario completare attività come l'installazione del server SnapCenter, l'aggiunta di host, la configurazione delle connessioni del sistema di storage e l'aggiunta della chiave di archiviazione utente HDB.
- Per la replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse del sistema HANA in un unico gruppo di risorse e di eseguire il backup di un gruppo di risorse. Ciò garantisce un backup perfetto durante la modalità takeover-failback.

"Creare gruppi di risorse e allegare policy".

A proposito di questa attività

Il rilevamento automatico non è supportato per le seguenti configurazioni:

- Layout RDM e VMDK

  Nel caso in cui vengano rilevate le suddette risorse, le operazioni di protezione dei dati non sono supportate da queste risorse.

- Configurazione di più host HANA
- Istanze multiple sullo stesso host
- Replica del sistema HANA con scalabilità orizzontale multi-Tier
- Ambiente di replica a cascata in modalità di replica del sistema

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare il plug-in SnapCenter per il database SAP HANA dall'elenco a discesa, quindi fare clic su **risorse**.

2. Nella pagina Resources (risorse), fare clic su **Add SAP HANA Database** (Aggiungi database SAP HANA).
3. Nella pagina fornire dettagli sulle risorse, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Tipo di risorsa	Inserire il tipo di risorsa. I tipi di risorse sono container singolo, container database multi-tenant (MDC) e Volume non dati.
Nome sistema HANA	Inserire il nome descrittivo del sistema SAP HANA. Questa opzione è disponibile solo se sono stati selezionati i tipi di risorse Single Container o MDC.
SID	Inserire l'ID di sistema (SID). Il sistema SAP HANA installato viene identificato da un singolo SID.
Host plug-in	Selezionare l'host del plug-in.
Chiavi di memorizzazione utente sicure HDB	Inserire la chiave per connettersi al sistema SAP HANA. La chiave contiene le informazioni di accesso per la connessione al database. Per SAP HANA System Replication, la chiave utente secondaria non viene convalidata. Questo verrà utilizzato durante il takeover.
Utente del sistema operativo HDBSQL	Immettere il nome utente per il quale è configurata la chiave di memorizzazione utente sicura HDB. Per Windows, è obbligatorio che l'utente del sistema operativo HDBSQL sia l'utente DEL SISTEMA. Pertanto, è necessario configurare la chiave di memorizzazione utente sicura HDB per l'utente DI SISTEMA.

4. Nella pagina fornire footprint dello storage, selezionare un sistema storage e scegliere uno o più volumi, LUN e qtree, quindi fare clic su **Salva**.

   Opzionale: Puoi fare clic sull'icona * * per aggiungere ulteriori volumi, LUN e qtree da altri sistemi storage.

5. Esaminare il riepilogo, quindi fare clic su **fine**.

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

Se si desidera fornire agli utenti l'accesso alle risorse, è necessario assegnarle agli utenti. In questo modo, gli utenti possono eseguire le azioni per le quali dispongono delle autorizzazioni per le risorse ad essi assegnate.

"Aggiungere un utente o un gruppo e assegnare ruolo 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 multitenant (MDC): SID o host client HDBSQL (plug-in)
- Container singolo: Host client (plug-in) SID o HDBSQL
- Volume non dati: Nome della risorsa, SID associato o host plug-in

Creare policy di backup per i database SAP HANA

Prima di utilizzare SnapCenter per eseguire il backup delle risorse di 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. Un criterio di backup è un insieme di regole che regolano la gestione, la pianificazione e la conservazione dei backup.

Cosa ti serve

- È necessario aver definito la strategia di backup.

  Per ulteriori informazioni, consulta le informazioni sulla definizione di una strategia di protezione dei dati per i database SAP HANA.

- Devi essere preparato per la protezione dei dati completando attività come l'installazione di SnapCenter, l'aggiunta di host, la configurazione delle connessioni del sistema di storage e l'aggiunta di risorse.
- L'amministratore di SnapCenter deve aver assegnato all'utente le SVM per i volumi di origine e di destinazione se si stanno replicando le copie Snapshot in un mirror o in un vault.

  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.

A proposito di questa attività

- Replica di sistema SAP HANA
  - È possibile proteggere il sistema SAP HANA primario ed eseguire tutte le operazioni di protezione dei dati.
  - È possibile proteggere il sistema SAP HANA secondario, ma i backup non possono essere creati.

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

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

Fasi

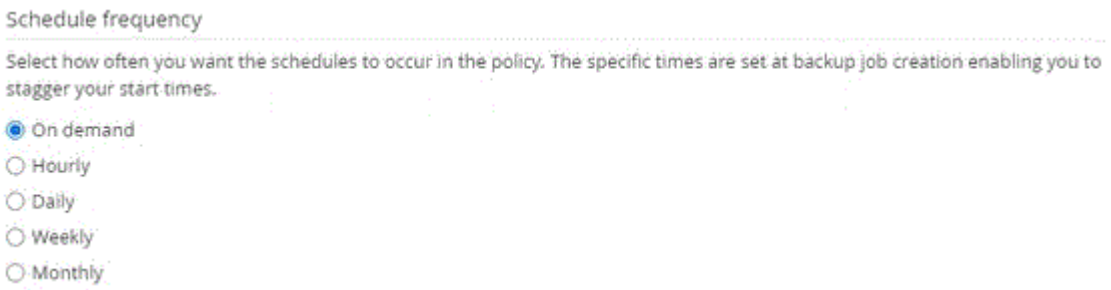
1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.

3. Fare clic su **nuovo**.
4. Nella pagina Name (Nome), immettere il nome e la descrizione della policy.
5. Nella pagina Impostazioni, attenersi alla seguente procedura:
   - Scegliere il tipo di backup:

Se si desidera…	Eseguire questa operazione…
Eseguire un controllo dell'integrità del database	Selezionare **Backup basato su file**. Viene eseguito il backup solo dei tenant attivi.
Creare un backup utilizzando la tecnologia di copia Snapshot	Selezionare **basato su snapshot**.

   - Specificare il tipo di pianificazione selezionando **on demand**, **Hourly**, **Daily**, **Weekly** o **Monthly**.

> 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 frequenza di backup, ma consente anche di assegnare diverse pianificazioni di backup a ogni policy.



> Se sono previste le 2:00, la programmazione non verrà attivata durante l'ora legale (DST).

   - Nella sezione **Impostazioni di backup personalizzate**, specificare le impostazioni di backup specifiche da passare al plug-in in formato key-value.

     È possibile fornire più valori chiave da passare al plug-in.

6. Nella pagina conservazione, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina tipo di backup:

Se si desidera…	Quindi…
Conservare un certo numero di copie Snapshot	Selezionare **copie Snapshot totali da conservare**, quindi specificare il numero di copie Snapshot che si desidera conservare. Se il numero di copie Snapshot supera il numero specificato, le copie Snapshot vengono eliminate prima con le copie meno recenti. Il valore massimo di conservazione è 1018 per le risorse su ONTAP 9.4 o versioni successive e 254 per le risorse su ONTAP 9.3 o versioni precedenti. I backup non avranno esito positivo se la conservazione viene impostata su un valore superiore a quello supportato dalla versione di ONTAP sottostante. Per i backup basati su copia Snapshot, è necessario impostare il numero di conservazione su 2 o superiore se si intende attivare la replica SnapVault. Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché la prima copia Snapshot è la copia Snapshot di riferimento per la relazione SnapVault fino a quando una copia Snapshot più recente non viene replicata nella 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 il corretto numero di backup.

Se si desidera…	Quindi…
Conservare le copie Snapshot per un certo numero di giorni	Selezionare **Mantieni copie Snapshot per**, quindi specificare il numero di giorni per i quali si desidera conservare le copie Snapshot prima di eliminarle.

risorse. La rimozione della copia Snapshot meno recente si basa sul nodo in cui si trova la copia Snapshot

7. Per i backup basati su copia Snapshot, specificare le impostazioni di replica nella pagina Replication:

Per questo campo…	Eseguire questa operazione…
Aggiornare 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). Se la relazione di protezione in ONTAP è di tipo Mirror e Vault e se si seleziona solo questa opzione, la copia Snapshot creata sul primario non verrà trasferita alla destinazione, ma verrà elencata nella destinazione. Se questa copia Snapshot viene selezionata dalla destinazione per eseguire un'operazione di ripristino, viene visualizzato il messaggio di errore percorso secondario non disponibile per il backup nel vault/mirror selezionato.
Aggiornare SnapVault dopo aver creato una copia Snapshot locale	Selezionare questa opzione per eseguire la replica del backup disk-to-disk (backup SnapVault).
Etichetta del criterio secondario	Selezionare un'etichetta Snapshot. A seconda dell'etichetta della copia Snapshot selezionata, ONTAP applica la policy di conservazione della copia Snapshot secondaria corrispondente all'etichetta. Se è stato selezionato **Update SnapMirror dopo la creazione di una copia Snapshot locale**, è possibile specificare l'etichetta del criterio secondario. Tuttavia, se è stato selezionato **Aggiorna SnapVault dopo la creazione di una copia Snapshot locale**, è necessario specificare l'etichetta del criterio secondario.
Numero tentativi di errore	Immettere il numero massimo di tentativi di replica consentiti prima dell'interruzione dell'operazione.

È necessario configurare il criterio di conservazione di SnapMirror in ONTAP per lo storage secondario per evitare di raggiungere il limite massimo di copie Snapshot sullo storage secondario.

8. Esaminare il riepilogo, quindi fare clic su **fine**.

Creare gruppi di risorse e allegare policy

Un gruppo di risorse è il container al quale è necessario aggiungere risorse di cui si desidera eseguire il backup e la protezione. Un gruppo di risorse consente di eseguire contemporaneamente il backup di tutti i dati associati a una determinata applicazione. Per qualsiasi lavoro di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario associare uno o più criteri al gruppo di risorse per definire il tipo di lavoro di protezione dei dati che si desidera eseguire.

A proposito di questa attività

Per creare backup di replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse del sistema SAP HANA in un unico gruppo di risorse. Ciò garantisce un backup perfetto durante la modalità takeover-failback.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), fare clic su **New Resource Group** (nuovo gruppo di risorse).
3. Nella pagina Name (Nome), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome	Immettere un nome per il gruppo di risorse. Il nome del gruppo di risorse non deve superare i 250 caratteri.
Tag	Inserire una o più etichette per facilitare la ricerca del gruppo di risorse in un secondo momento. Ad esempio, se si aggiunge HR come tag a più gruppi di risorse, è possibile trovare in seguito tutti i gruppi di risorse associati al tag HR.

Per questo campo…	Eseguire questa operazione…
USA il formato nome personalizzato per la copia Snapshot	Selezionare questa casella di controllo e immettere un formato nome personalizzato da utilizzare per il nome della copia Snapshot. Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome della copia Snapshot viene aggiunto un indicatore data e ora.

4. Nella pagina risorse, selezionare un nome host dall'elenco a discesa **host** e il tipo di risorsa dall'elenco a discesa **tipo di risorsa**.

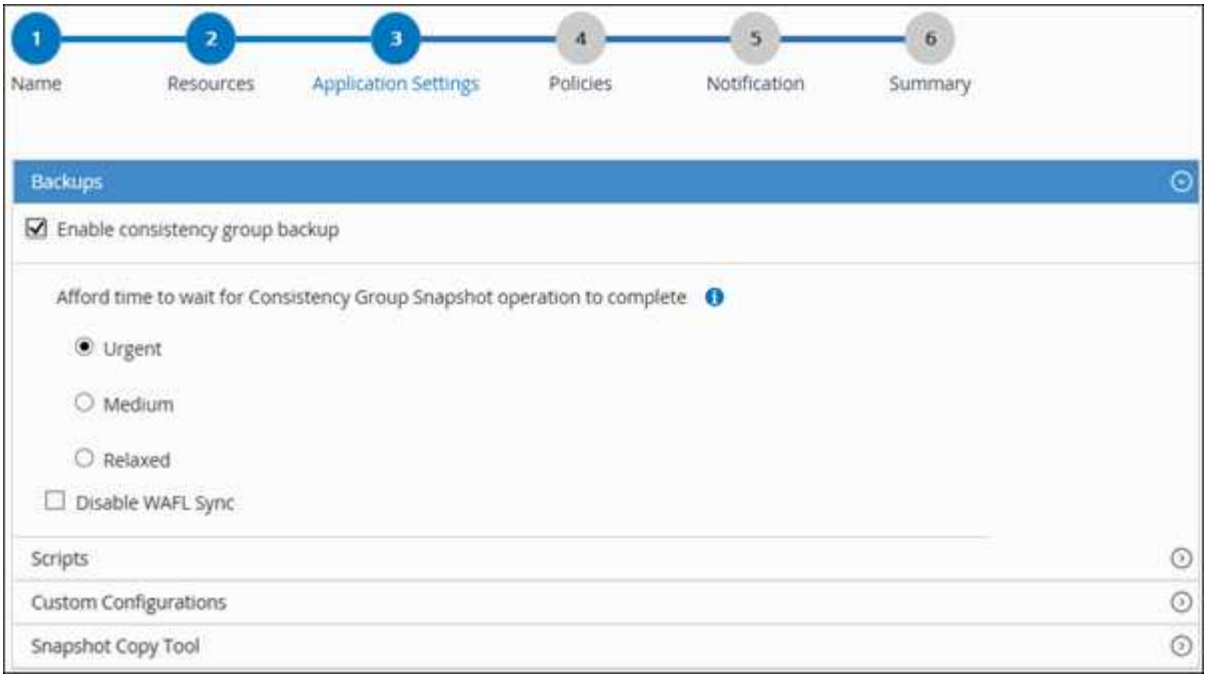
   In questo modo è possibile filtrare le informazioni sullo schermo.

5. Selezionare le risorse dalla sezione **risorse disponibili**, quindi fare clic sulla freccia destra per spostarle nella sezione **risorse selezionate**.
6. Nella pagina Impostazioni applicazione, effettuare le seguenti operazioni:

   a. Fare clic sulla freccia **Backup** per impostare opzioni di backup aggiuntive:

      Abilitare il backup dei gruppi di coerenza ed eseguire le seguenti attività:

Per questo campo…	Eseguire questa operazione…
Tempo di attesa per il completamento dell'operazione Consistency Group Snapshot	Selezionare **urgente**, **Medio** o **rilassato** per specificare il tempo di attesa per il completamento dell'operazione di copia Snapshot. Urgente = 5 secondi, Medio = 7 secondi e rilassato = 20 secondi.
Disattiva sincronizzazione WAFL	Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL.

+ 

a. Fare clic sulla freccia **Scripts** e immettere i comandi pre e post per le operazioni quiesce, copia Snapshot e senza richieste. In caso di errore, è anche possibile inserire i pre-comandi da eseguire prima di uscire.

b. Fare clic sulla freccia **Custom Configurations** (configurazioni personalizzate) e immettere le coppie chiave-valore personalizzate richieste per tutte le operazioni di protezione dei dati che utilizzano questa risorsa.

Parametro	Impostazione	Descrizione
ARCHIVE_LOG_ENABLE	(S/N)	Attiva la gestione del log di archiviazione per eliminare i log di archiviazione.
ARCHIVE_LOG_RETENTION	numero_di_giorni	Specifica il numero di giorni in i registri di archivio vengono conservati. Questa impostazione deve essere uguale o maggiore di NTAP_SNAPSHOT_ RITENTIONI.
ARCHIVE_LOG_DIR	change_info_directory/logs	Specifica il percorso della directory che contiene i log di archiviazione.

Parametro	Impostazione	Descrizione
ARCHIVE_LOG_EXT	estensione_file	Specifica il file di log dell'archivio lunghezza dell'estensione. Ad esempio, se il log di archiviazione è log_backup_0_0_0_0.16151855 1942 9 e se il valore di estensione_file è 5, l'estensione del log conservare 5 cifre, ossia 16151.
ARCHIVE_LOG_RECURSIVE_ SE ARCH	(S/N)	Attiva la gestione dell'archivio esegue il log all'interno delle sottodirectory. Tu utilizzare questo parametro se il i registri di archiviazione si trovano in sottodirectory.

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

c. Fare clic sulla freccia **Snapshot Copy Tool** per selezionare lo strumento per creare le copie Snapshot:

Se vuoi…	Quindi…
SnapCenter per utilizzare il plug-in per Windows e mettere il file system in uno stato coerente prima di creare una copia Snapshot. Per le risorse Linux, questa opzione non è applicabile.	Selezionare **SnapCenter with file system Consistency**. Questa opzione non è applicabile al plug-in SnapCenter per database SAP HANA.
SnapCenter per creare una copia Snapshot a livello di storage	Selezionare **SnapCenter senza coerenza del file system**.
Per inserire il comando da eseguire sull'host per creare copie Snapshot.	Selezionare **Altro**, quindi immettere il comando da eseguire sull'host per creare una copia Snapshot.

7. Nella pagina Criteri, attenersi alla seguente procedura:

a. Selezionare uno o più criteri dall'elenco a discesa.

È anche possibile creare una policy facendo clic su * * .

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

b.

Nella colonna Configura pianificazioni, fare clic su * * per il criterio che si desidera configurare.

c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione, quindi fare clic su **OK**.

   Dove, policy_name è il nome del criterio selezionato.

   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 di SnapCenter.

8. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

   È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail. Il server SMTP deve essere configurato in **Impostazioni** > **Impostazioni globali**.

9. Esaminare il riepilogo, quindi fare clic su **fine**.

Eseguire il backup dei database SAP HANA

Se una risorsa non fa ancora parte di un gruppo di risorse, è possibile eseguire il backup della risorsa dalla pagina risorse.

Cosa ti serve

- È necessario aver creato una policy di backup.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con uno storage secondario, il ruolo ONTAP assegnato all'utente dello storage deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- Per le operazioni di backup basate su copia Snapshot, assicurarsi che tutti i database del 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 unico gruppo di risorse. Ciò garantisce un backup perfetto durante la modalità takeover-failback.

  "Creare gruppi di risorse e allegare policy".

  "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_IFINATTIVO_TENANTS_PRESENT su **YES** nel file di 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, fare riferimento anche alla "Guida di riferimento al cmdlet del software SnapCenter"

- Per i comandi pre e post per le operazioni quiesce, Snapshot copy e unquiesce, controllare se i comandi esistono nell'elenco dei comandi disponibile sull'host plug-in dai seguenti percorsi:

  Per Windows: *C: File di programma NetApp, SnapCenter, Snapcenter Plug-in Creator, ecc.,*

allowed_comands_list.txt

Per Linux: */var/opt/snapcenter/scc/allowed_comands_list.txt*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione avrà esito negativo.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resource, filtrare le risorse dall'elenco a discesa **View** in base al tipo di risorsa.

   Fare clic su * * , quindi selezionare il nome host e il tipo di risorsa per filtrare le risorse. È quindi possibile fare clic su per chiudere il riquadro del filtro.
3. Fare clic sulla risorsa di cui si desidera eseguire il backup.
4. Nella pagina Resource, selezionare **Use customed name format for Snapshot copy** (Usa formato nome personalizzato per la copia Snapshot), quindi immettere un formato nome personalizzato da utilizzare per il nome della copia Snapshot.

   Ad esempio, *customtext_policy_hostname* o *resource_hostname*. Per impostazione predefinita, al nome della copia Snapshot viene aggiunto un indicatore data e ora.
5. Nella pagina Impostazioni applicazione, effettuare le seguenti operazioni:
   - Fare clic sulla freccia **Backup** per impostare opzioni di backup aggiuntive:

     Attivare il backup dei gruppi di coerenza, se necessario, ed eseguire le seguenti attività:

Per questo campo…	Eseguire questa operazione…
Attendere il completamento dell'operazione "Consistency Group Snapshot"	Selezionare **urgente**, **Medio** o **rilassato** per specificare il tempo di attesa per il completamento dell'operazione di copia Snapshot. Urgente = 5 secondi, Medio = 7 secondi e rilassato = 20 secondi.
Disattiva sincronizzazione WAFL	Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL.

   - Fare clic sulla freccia **Scripts** per eseguire i comandi pre e post per le operazioni di quiesce, copia Snapshot e senza richieste.

     È inoltre possibile eseguire i comandi preliminari prima di uscire dall'operazione di backup. Le prescrizioni e i postscript vengono eseguiti nel server SnapCenter.
   - Fare clic sulla freccia **configurazioni personalizzate**, quindi immettere le coppie di valori personalizzate richieste per tutti i lavori che utilizzano questa risorsa.
   - Fare clic sulla freccia **Snapshot Copy Tool** per selezionare lo strumento per creare le copie Snapshot:

Se vuoi…	Quindi…
SnapCenter per creare una copia Snapshot a livello di storage	Selezionare **SnapCenter senza coerenza del file system**.
SnapCenter utilizza il plug-in per Windows per mettere il file system in uno stato coerente e quindi creare una copia Snapshot	Selezionare **SnapCenter with file system Consistency**.
Per immettere il comando per creare una copia Snapshot	Selezionare **Altro**, quindi immettere il comando per creare una copia Snapshot.

6. Nella pagina Criteri, attenersi alla seguente procedura:

   a. Selezionare uno o più criteri dall'elenco a discesa.

      È anche possibile creare una policy facendo clic su * * + .

      Nella sezione Configure schedules for selected policies (Configura pianificazioni per policy selezionate), vengono elencati i criteri selezionati.

   b. Fare clic su * * + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

   c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione, quindi fare clic su **OK**.

      policy_name è il nome del criterio selezionato.

Le pianificazioni configurate sono elencate nella colonna Applied Schedules (Pianificazioni applicate).

7. Nella pagina notifica, dall'elenco a discesa **Email preference** (Preferenze email), selezionare gli scenari in cui si desidera inviare i messaggi e-mail.

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

8. Esaminare il riepilogo, quindi fare clic su **fine**.

   Viene visualizzata la pagina della topologia delle risorse.

9. Fare clic su **Esegui backup ora**.
10. Nella pagina Backup, attenersi alla seguente procedura:
    a. Se sono stati applicati più criteri alla risorsa, selezionare il criterio da utilizzare per il backup dall'elenco a discesa **Policy**.

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

    b. Fare clic su **Backup**.
11. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.
    - Nelle configurazioni MetroCluster, SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

      Per ulteriori informazioni, vedere: "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover di MetroCluster"

    - Se si esegue il backup dei dati delle applicazioni su VMDK e la dimensione dell'heap Java per il plug-in SnapCenter per VMware vSphere non è sufficiente, il backup potrebbe non riuscire.

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

Eseguire il backup dei gruppi di risorse

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

Cosa ti serve

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

A proposito di questa attività

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

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Resources (risorse), selezionare **Resource Group** (Gruppo di risorse) dall'elenco **View** (Visualizza).

   È possibile eseguire una ricerca nel gruppo di risorse immettendo il nome del gruppo di risorse nella casella di ricerca oppure facendo clic su , quindi selezionando il tag. È quindi possibile fare clic su per chiudere il riquadro del filtro.
3. Nella pagina gruppi di risorse, selezionare il gruppo di risorse di cui si desidera eseguire il backup, quindi fare clic su **Esegui backup ora**.
4. Nella pagina Backup, attenersi alla seguente procedura:
   a. Se sono stati associati più criteri al gruppo di risorse, selezionare il criterio da utilizzare per il backup dall'elenco a discesa **Policy**.

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

   b. Fare clic su **Backup**.
5. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

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

È necessario creare una connessione SVM (Storage Virtual Machine) e una credenziale prima di utilizzare i cmdlet PowerShell per eseguire il backup, il ripristino o la clonazione dei database SAP HANA.

Cosa ti serve

- L'ambiente PowerShell dovrebbe essere stato preparato per l'esecuzione dei cmdlet PowerShell.
- Per creare le connessioni storage, è necessario disporre delle autorizzazioni necessarie nel ruolo Infrastructure Admin.
- Assicurarsi che le installazioni dei plug-in non siano in corso.

  Le installazioni dei plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage perché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nella GUI di SnapCenter come "non disponibile per il backup" o "non su storage NetApp".
- I nomi dei sistemi di storage devono essere univoci.

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

Fasi

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

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

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

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -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 al server SnapCenter.

```
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. Impostare il percorso del 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, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Eseguire il backup dei database utilizzando i cmdlet PowerShell

Il backup di un database include la connessione con il server SnapCenter, l'aggiunta di risorse, l'aggiunta di un criterio, la creazione di un gruppo di risorse di backup e il backup.

Cosa ti serve

- È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- È necessario aver aggiunto la connessione al sistema di storage e creato una credenziale.

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico utilizzando il cmdlet Open-SmConnection.

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

   Viene visualizzato il prompt 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.netapp.
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 una policy 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 di container:

   ```
   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 di container multipli:

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

In questo esempio viene creato un nuovo gruppo di risorse con le risorse e i criteri specificati:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sccore.test.com";"Uid"="SID"},@{"Host"="sccore
linux62.sccore.test.com";"Uid"="MDC\SID"})
  -Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency  -plugincode 'HANA'
```

In questo esempio viene creato un gruppo di risorse di volumi non dati:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="H11";"PluginName"="han
a"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="MDC\H31";"PluginName
"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="NonDataVolume\
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 di backup, 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, fare riferimento anche a "Guida di riferimento al cmdlet del software SnapCenter".

Monitorare le operazioni di backup

Monitorare le operazioni di backup dei database SAP HANA

È possibile monitorare l'avanzamento di diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere necessario controllare i progressi per determinare quando sono stati completati o se si è verificato un problema.

A proposito di questa attività

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

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvisi o impossibile avviarlo a causa di avvisi
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Jobs**.
3. Nella pagina lavori, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Status** (Stato), selezionare lo stato del backup.
   e. Fare clic su **Apply** (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 venga visualizzato lo stato del processo di backup , facendo clic sui dettagli del lavoro, è possibile che alcune delle attività secondarie dell'operazione di backup siano ancora in corso o contrassegnate da segnali di avviso.

5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

   Il pulsante **View logs** (Visualizza registri) visualizza i registri dettagliati per l'operazione selezionata.

Monitorate le operazioni di protezione dei dati sui database SAP HANA nel riquadro attività

Il riquadro Activity (attività) visualizza le cinque operazioni più recenti eseguite. Il riquadro Activity (attività) visualizza anche il momento in cui l'operazione è stata avviata e lo stato dell'operazione.

Il riquadro Activity (attività) visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificati. Se si utilizza il plug-in per SQL Server o il plug-in per Exchange Server, nel riquadro attività vengono visualizzate anche le informazioni relative all'operazione di riseeding.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Fare clic sul 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 inserite nella coda.

Cosa ti serve

- Per annullare le operazioni, è necessario accedere come amministratore SnapCenter o come proprietario del processo.
- È possibile annullare un'operazione di backup dalla pagina **Monitor** o dal riquadro **Activity**.
- Non è possibile annullare un'operazione di backup in esecuzione.
- Per annullare le operazioni di backup, è possibile utilizzare l'interfaccia grafica utente di SnapCenter, i cmdlet PowerShell o i comandi CLI.
- Il pulsante **Annulla lavoro** è disattivato per le operazioni che non possono essere annullate.
- Se si seleziona **tutti i membri di questo ruolo possono visualizzare e operare su altri oggetti membri** nella pagina utenti/gruppi durante la creazione di un ruolo, è possibile annullare le operazioni di backup in coda degli altri membri durante l'utilizzo di tale ruolo.

Fasi

1. Eseguire una delle seguenti operazioni:

Dal…	Azione
Pagina Monitor	a. Nel riquadro di spostamento di sinistra, fare clic su **Monitor** > **Jobs**. b. Selezionare l'operazione, quindi fare clic su **Annulla lavoro**.
Riquadro delle 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 processo, fare clic su **Annulla processo**.

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

Visualizzare i backup e i cloni del database SAP HANA nella pagina topologia

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

A proposito di questa attività

È possibile esaminare le seguenti icone nella vista Manage Copies (Gestisci copie) per determinare se i backup e i cloni sono disponibili sullo storage 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 mirrorati sullo storage secondario utilizzando la tecnologia SnapMirror.
- Visualizza il numero di backup e cloni replicati sullo storage secondario utilizzando la tecnologia SnapVault.

  Il numero di backup visualizzati include i backup eliminati dallo storage secondario. Ad esempio, se sono stati creati 6 backup utilizzando un criterio per conservare solo 4 backup, il numero di backup visualizzato è 6.

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

Per le risorse primarie di replica del sistema SAP HANA, sono supportate le operazioni di ripristino ed eliminazione, mentre per le risorse secondarie è supportata l'operazione di clonazione.

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 selezionarli per eseguire le operazioni di protezione dei dati.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina risorse, selezionare 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 **Summary** per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   La sezione **Summary Card** mostra il numero totale di backup basati su file, backup di copie Snapshot e cloni.

   Facendo clic sul pulsante **Refresh** viene avviata una query dello storage per visualizzare un conteggio accurato.

5. Nella vista Gestisci copie, fare clic su **backup** o **cloni** dallo storage primario o secondario per visualizzare i dettagli di un backup o 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 nello storage secondario.

7. Se si desidera eliminare un clone, selezionarlo dalla tabella, quindi fare clic su .
8. Se si desidera dividere un clone, selezionarlo dalla tabella e fare 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 COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

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

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

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

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

Informazioni sul marchio commerciale

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