Proteggere i database SAP HANA

SnapCenter Software 4.8

NetApp
January 18, 2024

Sommario

Proteggere i database SAP HANA

Plug-in SnapCenter per database SAP HANA

Panoramica del plug-in SnapCenter per il database SAP HANA

Il plug-in SnapCenter per database SAP HANA è un componente lato host del software NetApp SnapCenter che consente la gestione della protezione dei dati applicativa dei database SAP HANA. Il plug-in per il database SAP HANA automatizza il backup, il ripristino e la clonazione dei database SAP HANA nel tuo ambiente SnapCenter.

SnapCenter supporta container singoli e container di database multi-tenant (MDC). È possibile utilizzare il plug-in per il database SAP HANA in ambienti Windows e Linux. Il plug-in non installato sull'host del database HANA è noto come plug-in host centralizzato. Il plug-in host centralizzato è in grado di gestire più database HANA su diversi host.

Una volta installato il plug-in per il database SAP HANA, è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror dei set di backup su un altro volume. È inoltre possibile utilizzare il plug-in con la tecnologia NetApp SnapVault per eseguire la replica del backup disk-to-disk per garantire la conformità agli standard.

Operazioni che è possibile eseguire utilizzando il plug-in SnapCenter per il database SAP HANA

Quando installi il plug-in per il database SAP HANA nel tuo ambiente, puoi utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione dei database SAP HANA e delle relative risorse. È inoltre possibile eseguire attività a supporto di tali operazioni.

- Aggiungere database.
- Creare backup.
- Ripristinare dai backup.
- Clonare i backup.
- Pianificare le operazioni di backup.
- Monitorare le operazioni di backup, ripristino e clonazione.
- Visualizza i report per le operazioni di backup, ripristino e clonazione.

Plug-in SnapCenter per le funzionalità del database SAP HANA

SnapCenter si integra con l'applicazione plug-in e con le tecnologie NetApp del sistema storage. Per utilizzare il plug-in per il database SAP HANA, utilizzare l'interfaccia grafica utente di SnapCenter.

- **Interfaccia utente grafica unificata**

  L'interfaccia SnapCenter offre standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia di SnapCenter consente di completare operazioni di backup, ripristino e clonazione coerenti tra i plug-in, utilizzare report centralizzati, utilizzare visualizzazioni dashboard a colpo d'occhio, impostare RBAC (role-

based access control) e monitorare i processi in tutti i plug-in.

- **Amministrazione centrale automatizzata**

  È possibile pianificare le operazioni di backup, configurare la conservazione dei backup basata su policy ed eseguire operazioni di ripristino. Puoi anche monitorare in modo proattivo il tuo ambiente configurando SnapCenter per l'invio di avvisi e-mail.

- **Tecnologia di copia Snapshot NetApp senza interruzioni**

  SnapCenter utilizza la tecnologia di copia Snapshot di NetApp con il plug-in per il database SAP HANA per eseguire il backup delle risorse.

L'utilizzo del plug-in per il database SAP HANA offre anche i seguenti vantaggi:

- Supporto per flussi di lavoro di backup, ripristino e clonazione
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli

  È inoltre possibile impostare le credenziali in modo che gli utenti SnapCenter autorizzati dispongano delle autorizzazioni a livello di applicazione.

- Creazione di copie delle risorse efficienti in termini di spazio e point-in-time per il test o l'estrazione dei dati utilizzando la tecnologia NetApp FlexClone

  È necessaria una licenza FlexClone sul sistema storage in cui si desidera creare il clone.

- Supporto per la funzione di copia Snapshot del gruppo di coerenza (CG) di ONTAP durante la creazione dei backup.
- Possibilità di eseguire più backup contemporaneamente su più host di risorse

  In una singola operazione, le copie Snapshot vengono consolidate quando le risorse di un singolo host condividono lo stesso volume.

- Possibilità di creare copie Snapshot utilizzando comandi esterni.
- Supporto per il backup basato su file.
- Supporto per Linux LVM su file system XFS.

Tipi di storage supportati dal plug-in SnapCenter per database SAP HANA

SnapCenter supporta un'ampia gamma di tipi di storage su macchine fisiche e macchine virtuali (VM). Prima di installare il plug-in SnapCenter per il database SAP HANA, è necessario verificare il supporto per il tipo di storage in uso.

Macchina	Tipo di storage
Server fisici e virtuali	LUN connessi a FC
Server fisico	LUN connessi a iSCSI
Server fisici e virtuali	Volumi connessi a NFS

Privilegi ONTAP minimi richiesti per il plug-in SAP HANA

I privilegi minimi di ONTAP richiesti variano in base ai plug-in di SnapCenter utilizzati per la protezione dei dati.

All-access comands (comandi all-access): Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
event generate-autosupport-log
mostra la cronologia dei lavori interruzione del lavoro

All-access comands (comandi all-access): Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
lun
lun create (crea lun)
lun delete (elimina lun)
lun igroup add
lun igroup create
lun igroup delete (elimina igroup lun)
lun igroup rename (rinomina lun igroup)
lun igroup show
lun mapping add-reporting-node
creazione mappatura lun
eliminazione della mappatura lun
nodi di remove-reporting-mapping lun
visualizzazione della mappatura del lun
modifica del lun
lun move-in-volume
lun offline
lun online
lun persistent-reservation clear
ridimensionamento del lun
lun seriale
lun show

All-access comands (comandi all-access): Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
regola aggiuntiva del criterio snapmirror regola-modifica del criterio snapmirror regola di rimozione del criterio snapmirror policy di snapmirror ripristino di snapmirror spettacolo di snapmirror storia di snapmirror aggiornamento di snapmirror snapmirror update-ls-set elenco-destinazioni snapmirror
versione

All-access comands (comandi all-access): Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
creazione del clone del volume
visualizzazione del clone del volume
avvio della divisione del clone del volume
interruzione della divisione del clone del volume
creazione del volume
distruggere il volume
creazione del clone del file di volume
file di volume show-disk-usage
volume offline
volume online
modifica del volume
creazione del qtree del volume
eliminazione del qtree del volume
modifica del qtree del volume
visualizzazione del qtree del volume
limitazione del volume
presentazione del volume
creazione di snapshot di volume
eliminazione dello snapshot del volume
modifica dello snapshot del volume
rinominare lo snapshot del volume
ripristino dello snapshot del volume
file di ripristino dello snapshot del volume
visualizzazione di snapshot di volume
smontare il volume

All-access comands (comandi all-access): Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
cifs vserver
creazione condivisione cifs vserver
eliminazione condivisione cifs vserver
vserver cifs shadowcopy mostra
show di condivisione di vserver cifs
vserver cifs show
policy di esportazione di vserver
creazione policy di esportazione vserver
eliminazione della policy di esportazione di vserver
creazione della regola dei criteri di esportazione di vserver
visualizzazione della regola dei criteri di esportazione di vserver
visualizzazione della policy di esportazione di vserver
iscsi vserver
visualizzazione della connessione iscsi del vserver
show di vserver

Comandi di sola lettura: Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
interfaccia di rete
visualizzazione dell'interfaccia di rete
server virtuale

Preparazione dei sistemi storage per la replica di SnapMirror e SnapVault per i database SAP HANA

È possibile utilizzare un plug-in SnapCenter con la tecnologia SnapMirror di ONTAP per creare copie mirror dei set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replica del backup disk-to-disk per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti di SnapMirror e SnapVault dopo aver completato l'operazione di copia

Snapshot. Gli aggiornamenti di SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter; non creare una pianificazione ONTAP separata.

Se vieni a SnapCenter da un prodotto NetApp SnapManager e sei soddisfatto delle relazioni di protezione dei dati che hai configurato, puoi saltare questa sezione.

Una relazione di protezione dei dati replica i dati sullo storage primario (il volume di origine) nello storage secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui fa riferimento il volume di origine al volume di destinazione.

SnapCenter non supporta le relazioni a cascata tra SnapMirror e i volumi SnapVault (**primario** > **Mirror** > **Vault**). Si consiglia di utilizzare le relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per ulteriori informazioni sulle relazioni SnapMirror flessibili per la versione e su come configurarle, vedere "Documentazione ONTAP".

SnapCenter non supporta la replica **Sync_mirror**.

Strategia di backup per i database SAP HANA

Definire una strategia di backup per i database SAP HANA

La definizione di una strategia di backup prima della creazione dei processi di backup consente di ottenere i backup necessari per ripristinare o clonare correttamente le risorse. Il tuo SLA (Service-Level Agreement), RTO (Recovery Time Objective) e RPO (Recovery Point Objective) determinano in gran parte la tua strategia di backup.

A proposito di questa attività

Uno SLA definisce il livello di servizio previsto e risolve molti problemi relativi al servizio, tra cui la disponibilità e le performance del servizio. RTO è il momento in cui un processo di business deve essere ripristinato dopo un'interruzione del servizio. RPO definisce la strategia per l'età dei file che devono essere ripristinati dallo storage di backup per consentire il ripristino delle normali operazioni dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di protezione dei dati.

Fasi

1. Stabilire quando eseguire il backup delle risorse.
2. Decidere il numero di processi di backup necessari.
3. Decidere come assegnare un nome ai backup.
4. Decidere se si desidera creare una policy basata su copia Snapshot per eseguire il backup delle copie Snapshot coerenti con l'applicazione del database.
5. Decidere se verificare l'integrità del database.
6. Decidere se utilizzare la tecnologia NetApp SnapMirror per la replica o la tecnologia NetApp SnapVault per la conservazione a lungo termine.
7. Determinare il periodo di conservazione delle copie Snapshot sul sistema di storage di origine e sulla destinazione di SnapMirror.
8. Determinare se si desidera eseguire qualsiasi comando prima o dopo l'operazione di backup e fornire una

prescrizione o postscript.

Rilevamento automatico delle risorse sull'host Linux

Le risorse sono database SAP HANA e volumi non dati sull'host Linux gestiti da SnapCenter. Dopo aver installato il plug-in SnapCenter per il database SAP HANA, i database SAP HANA su quell'host vengono automaticamente rilevati e visualizzati nella pagina risorse.

Il rilevamento automatico è supportato per le seguenti risorse SAP HANA:

- Contenitori singoli

  Dopo l'installazione o l'aggiornamento del plug-in, le singole risorse container situate in un plug-in host centralizzato continueranno come risorse aggiunte manualmente.

  Dopo aver installato o aggiornato il plug-in, i database SAP HANA vengono rilevati automaticamente solo sugli host SAP HANA Linux, che sono direttamente registrati in SnapCenter.

- Container di database multi-tenant (MDC)

  Dopo aver installato o aggiornato il plug-in, le risorse MDC che si trovano in un plug-in host centralizzato continueranno come risorse aggiunte manualmente.

  È necessario continuare ad aggiungere manualmente le risorse MDC nel plug-in host centralizzato dopo l'aggiornamento a SnapCenter 4.3.

  Per gli host SAP HANA Linux registrati direttamente in SnapCenter, l'installazione o l'aggiornamento del plug-in attiverà un rilevamento automatico delle risorse sull'host. Dopo l'aggiornamento del plug-in, per ogni risorsa MDC che si trovava sull'host del plug-in, un'altra risorsa MDC verrà automaticamente rilevata con un formato GUID diverso e registrata in SnapCenter. La nuova risorsa sarà bloccata.

  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.

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

Tipo di backup supportati

Il tipo di backup specifica il tipo di backup che si desidera creare. SnapCenter supporta i tipi di backup basati su file e snapshot per i database SAP HANA.

Backup basato su file

I backup basati su file verificano l'integrità del database. È possibile pianificare l'esecuzione dell'operazione di backup basata su file a intervalli specifici. Viene eseguito il backup solo dei tenant attivi. Non è possibile ripristinare e clonare i backup basati su file da SnapCenter.

Backup basato su copia Snapshot

I backup basati su copia Snapshot sfruttano la tecnologia di copia Snapshot di NetApp per creare copie online di sola lettura dei volumi su cui risiedono i database SAP HANA.

In che modo il plug-in SnapCenter per il database SAP HANA utilizza le copie Snapshot del gruppo di coerenza

È possibile utilizzare il plug-in per creare copie Snapshot del gruppo di coerenza per i gruppi di risorse. Un gruppo di coerenza è un container che può ospitare più volumi in modo da poterli gestire come un'unica entità. Un gruppo di coerenza è costituito da copie Snapshot simultanee di più volumi, che forniscono copie coerenti di un gruppo di volumi.

È inoltre possibile specificare il tempo di attesa per il controller dello storage per raggruppare in modo coerente le copie Snapshot. Le opzioni di tempo di attesa disponibili sono **urgente**, **Medio** e **rilassato**. È inoltre possibile attivare o disattivare la sincronizzazione del layout di file WAFL (Write Anywhere file Layout) durante un'operazione di copia Snapshot di gruppo coerente. WAFL Sync migliora le prestazioni di una copia Snapshot di un gruppo di coerenza.

In che modo SnapCenter gestisce l'housekeeping dei backup di log e dati

SnapCenter gestisce la gestione dei backup di log e dati a livello di sistema storage e file system e all'interno del catalogo di backup SAP HANA.

Le copie Snapshot sullo storage primario o secondario e le relative voci nel catalogo SAP HANA vengono eliminate in base alle impostazioni di conservazione. Le voci del catalogo SAP HANA vengono eliminate anche durante il backup e l'eliminazione del gruppo di risorse.

Considerazioni per la determinazione delle pianificazioni di backup per il database SAP HANA

Il fattore più critico per determinare una pianificazione di backup è il tasso di cambiamento per la risorsa. È possibile eseguire il backup di una risorsa utilizzata in modo pesante ogni ora, mentre è possibile eseguire il backup di una risorsa utilizzata raramente una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo SLA (Service Level Agreement) e l'RPO (Recovery Point Objective).

Le pianificazioni dei backup sono in due parti, come segue:

- Frequenza del backup (frequenza con cui devono essere eseguiti i backup)

  La frequenza di backup, chiamata anche tipo di pianificazione per alcuni plug-in, fa parte di una configurazione di policy. Ad esempio, è possibile configurare la frequenza di backup come oraria, giornaliera, settimanale o mensile.

- Pianificazioni di backup (esattamente quando devono essere eseguiti i backup

Le pianificazioni dei backup fanno parte di una configurazione di risorse o gruppi di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per i backup settimanali, è possibile configurare la pianificazione per il backup ogni giovedì alle 10:00

Numero di processi di backup necessari per i database SAP HANA

I fattori che determinano il numero di processi di backup necessari includono la dimensione della risorsa, il numero di volumi utilizzati, il tasso di cambiamento della risorsa e il contratto SLA (Service Level Agreement).

Convenzioni di denominazione del backup per il plug-in per i database SAP HANA

È possibile utilizzare la convenzione di denominazione predefinita per la copia Snapshot o una convenzione di denominazione personalizzata. La convenzione di denominazione predefinita per il backup aggiunge un indicatore data e ora ai nomi delle copie Snapshot che consente di identificare quando sono state create le copie.

La copia Snapshot utilizza la seguente convenzione di denominazione predefinita:

`resourcegroupname_hostname_timestamp`

È necessario assegnare un nome logico ai gruppi di risorse di backup, come nell'esempio seguente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In questo esempio, gli elementi di sintassi hanno i seguenti significati:

- *dts1* è il nome del gruppo di risorse.
- *mach1x88* è il nome host.
- *03-12-2015_23.17.26* indica data e ora.

In alternativa, è possibile specificare il formato del nome della copia Snapshot proteggendo le risorse o i gruppi di risorse selezionando **Usa il formato del nome personalizzato per la copia Snapshot**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, il suffisso dell'indicatore orario viene aggiunto al nome della copia Snapshot.

Strategia di ripristino e recovery per i database SAP HANA

Definire una strategia di ripristino per le risorse SAP HANA

È necessario definire una strategia prima di ripristinare e ripristinare il database in modo da poter eseguire correttamente le operazioni di ripristino e ripristino.

Fasi

1. Determinare le strategie di ripristino supportate per le risorse SAP HANA aggiunte manualmente
2. Determinare le strategie di ripristino supportate per i database SAP HANA rilevati automaticamente
3. Decidere il tipo di operazioni di ripristino che si desidera eseguire.

Tipi di strategie di ripristino supportate per le risorse SAP HANA aggiunte manualmente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter. Esistono due tipi di strategie di ripristino per le risorse SAP HANA aggiunte manualmente. Non è possibile ripristinare le risorse SAP HANA aggiunte manualmente.

Non è possibile ripristinare le risorse SAP HANA aggiunte manualmente.

Ripristino completo delle risorse

- Ripristina tutti i volumi, le qtree e le LUN di una risorsa

Se la risorsa contiene volumi o qtree, le copie Snapshot eseguite dopo la copia Snapshot selezionata per il ripristino su tali volumi o qtree vengono eliminate e non possono essere ripristinate. Inoltre, se un'altra risorsa è ospitata sugli stessi volumi o qtree, anche tale risorsa viene eliminata.

Ripristino a livello di file

- Ripristina i file da volumi, qtree o directory
- Ripristina solo i LUN selezionati

Tipi di strategie di ripristino supportate per i database SAP HANA rilevati automaticamente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter. Esistono due tipi di strategie di ripristino per i database SAP HANA rilevati automaticamente.

Ripristino completo delle risorse

- Ripristina tutti i volumi, le qtree e le LUN di una risorsa
  - Per ripristinare l'intero volume, selezionare l'opzione **Volume Revert** (Ripristina volume).

Se la risorsa contiene volumi o qtree, le copie Snapshot eseguite dopo la copia Snapshot selezionata per il ripristino su tali volumi o qtree vengono eliminate e non possono essere ripristinate. Inoltre, se un'altra risorsa è ospitata sugli stessi volumi o qtree, anche tale risorsa viene eliminata.

Database tenant

- Ripristina il database tenant

Se l'opzione **Database tenant** è selezionata, per eseguire l'operazione di ripristino è necessario utilizzare gli script di ripristino HANA studio o HANA esterni a SnapCenter.

Tipi di operazioni di ripristino per i database SAP HANA rilevati automaticamente

SnapCenter supporta i tipi di ripristino VBSR (Volume-Based SnapRestore), Single file SnapRestore e Connect-and-copy per i database SAP HANA rilevati automaticamente.

Il volume-based SnapRestore (VBSR) viene eseguito in ambienti NFS per i seguenti scenari:

- Quando il backup selezionato per il ripristino viene eseguito su release precedenti a SnapCenter 4.3 e solo se è selezionata l'opzione **completa risorsa**
- Quando il backup selezionato per il ripristino viene eseguito in SnapCenter 4.3 e se è selezionata l'opzione **Ripristino volume**

Single file SnapRestore viene eseguito in ambienti NFS per i seguenti scenari:

- Quando il backup selezionato per il ripristino viene eseguito in SnapCenter 4.3 e se è selezionata solo l'opzione **completa risorsa**
- Per i contenitori di database multi-tenant (MDC), quando il backup selezionato per il ripristino viene eseguito su SnapCenter 4.3 e l'opzione **Database tenant** è selezionata
- Quando il backup selezionato proviene da una posizione secondaria SnapMirror o SnapVault e l'opzione **completa risorsa** è selezionata

Single file SnapRestore viene eseguito negli ambienti SAN per i seguenti scenari:

- Quando i backup vengono eseguiti su release precedenti a SnapCenter 4.3 e solo se è selezionata l'opzione **completa risorsa**
- Quando i backup vengono eseguiti in SnapCenter 4.3 e solo se è selezionata l'opzione **completa risorsa**
- Quando si seleziona il backup da una posizione secondaria SnapMirror o SnapVault e si seleziona l'opzione **completa risorsa**

Il ripristino basato su connessione e copia viene eseguito negli ambienti SAN per il seguente scenario:

- Per MDC, quando il backup selezionato per il ripristino viene eseguito in SnapCenter 4.3 e l'opzione **Database tenant** è selezionata

Le opzioni **complete Resource**, **Volume Revert** e **Database tenant** sono disponibili nella pagina Restore Scope.

Tipi di operazioni di recovery supportati per i database SAP HANA

SnapCenter consente di eseguire diversi tipi di operazioni di recovery per i database SAP HANA.

- Ripristinare il database fino allo stato più recente
- Ripristinare il database fino a un momento specifico

  Specificare la data e l'ora per il ripristino.

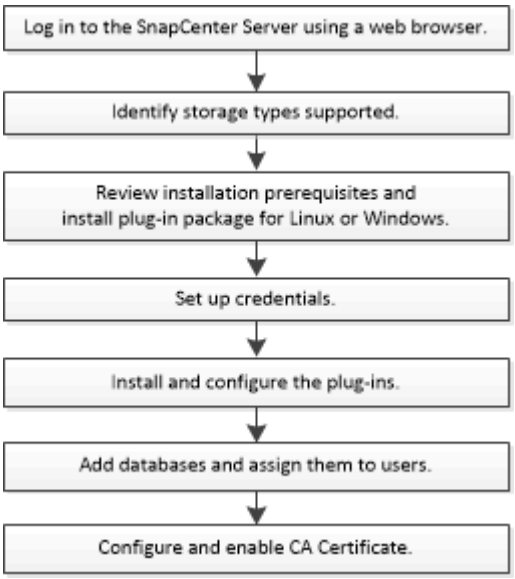
- Ripristinare il database fino a un backup dei dati specifico

SnapCenter offre anche l'opzione No recovery per i database SAP HANA.

Preparare l'installazione del plug-in SnapCenter per il database SAP HANA

Workflow di installazione del plug-in SnapCenter per database SAP HANA

Se si desidera proteggere i database SnapCenter HANA, è necessario installare e configurare il plug-in SAP per il database SAP HANA.



Prerequisiti per l'aggiunta di host e l'installazione del plug-in SnapCenter per il database SAP HANA

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario completare tutti i requisiti. Il plug-in SnapCenter per database SAP HANA è disponibile sia in ambienti Windows che Linux.

- È necessario aver installato Java a 1.8 64 bit sull'host.

  IBM Java non è supportato.

- È necessario aver installato il terminale interattivo del database SAP HANA (client HDBSQL) sull'host.
- Per Windows, il servizio di creazione del plug-in deve essere eseguito utilizzando l'utente di Windows "LocalSystem", che è il comportamento predefinito quando il plug-in per il database SAP HANA viene installato come amministratore di dominio.
- Per Windows, le chiavi dell'archivio utente devono essere create come utente DI SISTEMA.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host. Il plug-in SnapCenter per Microsoft Windows verrà implementato per impostazione predefinita con il plug-in SAP HANA sugli host Windows.
- Per l'host Linux, le chiavi HDB Secure User Store sono accessibili come utente del sistema operativo HDBSQL.
- Il server SnapCenter deve avere accesso alla porta 8145 o alla porta personalizzata del plug-in per l'host del database SAP HANA.

Host Windows

- È necessario disporre di un utente di dominio con privilegi di amministratore locale con autorizzazioni di accesso locale sull'host remoto.
- Durante l'installazione del plug-in per database SAP HANA su un host Windows, il plug-in SnapCenter per Microsoft Windows viene installato automaticamente.
- È necessario aver attivato la connessione SSH basata su password per l'utente root o non root.
- È necessario aver installato Java a 1.8 64 bit sull'host Windows.

  "Download Java per tutti i sistemi operativi"

  "Tool di matrice di interoperabilità NetApp"

Host Linux

- È necessario aver attivato la connessione SSH basata su password per l'utente root o non root.
- È necessario aver installato Java a 1.8 64 bit sull'host Linux.

  "Download Java per tutti i sistemi operativi"

  "Tool di matrice di interoperabilità NetApp"

- Per i database SAP HANA in esecuzione su un host Linux, durante l'installazione del plug-in per il database SAP HANA, il plug-in SnapCenter per UNIX viene installato automaticamente.

Requisiti dell'host per installare il pacchetto di plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario conoscere alcuni requisiti di base relativi allo spazio del sistema host e al dimensionamento.

Elemento	Requisiti
Sistemi operativi	Microsoft Windows Per informazioni aggiornate sulle versioni supportate, consultare "Tool di matrice di interoperabilità NetApp".
RAM minima per il plug-in SnapCenter sull'host	1 GB

Elemento	Requisiti
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	5 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	• Microsoft .NET Framework 4.7.2 o versione successiva • Windows Management Framework (WMF) 4.0 o versione successiva • PowerShell 4.0 o versione successiva Per informazioni aggiornate sulle versioni supportate, consultare "Tool di matrice di interoperabilità NetApp". Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet."

Requisiti dell'host per l'installazione del pacchetto di plug-in SnapCenter per Linux

Prima di installare il pacchetto di plug-in SnapCenter per Linux, è necessario conoscere alcuni requisiti di spazio e dimensionamento di base del sistema host.

Elemento	Requisiti
Sistemi operativi	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) Per informazioni aggiornate sulle versioni supportate, consultare "Tool di matrice di interoperabilità NetApp".
RAM minima per il plug-in SnapCenter sull'host	1 GB

Elemento	Requisiti
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	2 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.
Pacchetti software richiesti	Java 1.8.x (64-bit)Oracle Java e OpenJDK Flavors Se JAVA è stato aggiornato alla versione più recente, assicurarsi che l'opzione JAVA_HOME disponibile in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto. Per informazioni aggiornate sulle versioni supportate, consultare "Tool di matrice di interoperabilità NetApp".

Impostare le credenziali per il plug-in SnapCenter per il database SAP HANA

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter. È necessario creare credenziali per l'installazione dei plug-in SnapCenter e credenziali aggiuntive per l'esecuzione delle operazioni di protezione dei dati su database o file system Windows.

A proposito di questa attività

- Host Linux

  È necessario impostare le credenziali per l'installazione dei plug-in sugli host Linux.

  Per installare e avviare il processo di plug-in, è necessario impostare le credenziali per l'utente root o per un utente non root che dispone dei privilegi di sudo.

  Best practice: sebbene sia consentito creare credenziali per Linux dopo l'implementazione degli host e l'installazione dei plug-in, la Best practice consiste nel creare credenziali dopo l'aggiunta di SVM, prima di distribuire host e installare plug-in.

- Host Windows

  Prima di installare i plug-in, è necessario impostare le credenziali di Windows.

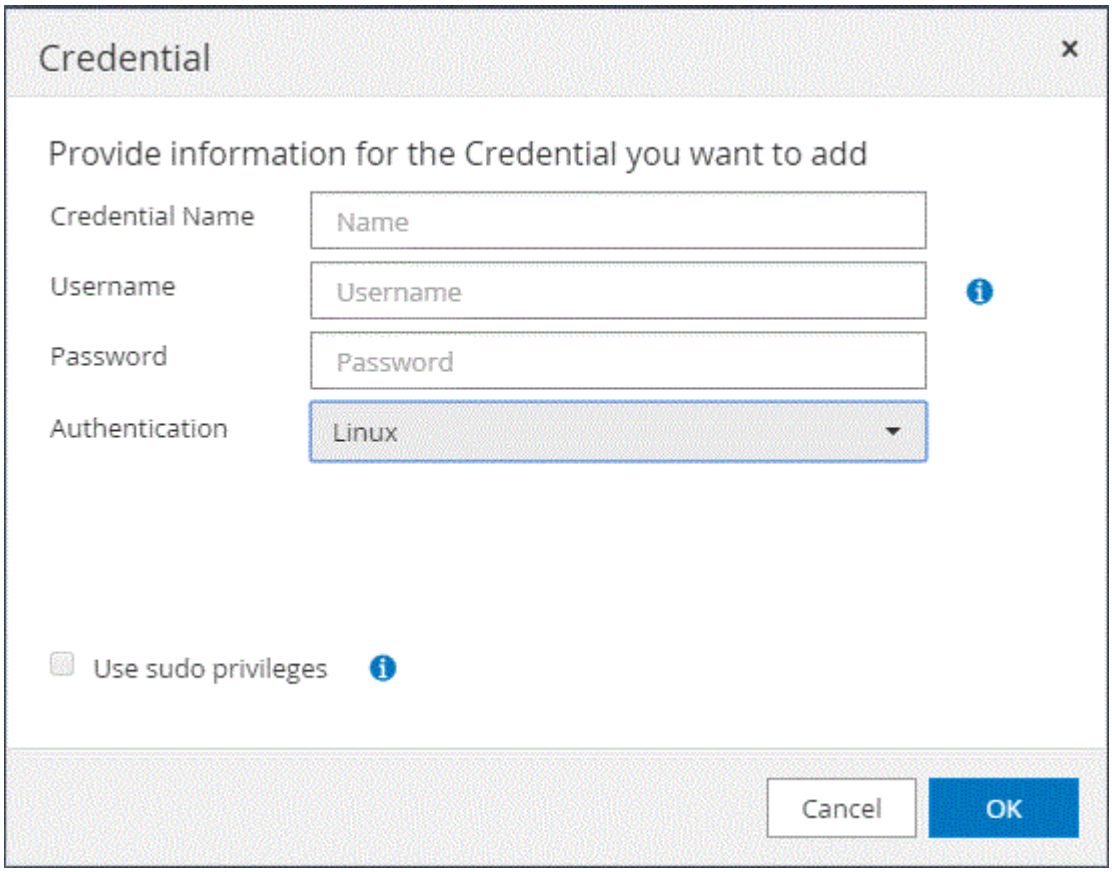
  È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore

sull'host remoto.

Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare almeno il gruppo di risorse e i privilegi di backup al nome utente.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **credenziale**.
3. Fare clic su **nuovo**.



4. Nella pagina credenziale, specificare le informazioni necessarie per la configurazione delle credenziali:

Per questo campo…	Eseguire questa operazione…
Nome della credenziale	Immettere un nome per le credenziali.

Per questo campo…	Eseguire questa operazione…
Nome utente	Immettere il nome utente e la password da utilizzare per l'autenticazione. • Amministratore di dominio o qualsiasi membro del gruppo di amministratori Specificare l'amministratore di dominio o qualsiasi membro del gruppo di amministratori nel sistema in cui si installa il plug-in SnapCenter. I formati validi per il campo Nome utente sono: ◦ *NetBIOS/nome utente* ◦ *Dominio FQDN/nome utente* • Amministratore locale (solo per gruppi di lavoro) Per i sistemi appartenenti a un gruppo di lavoro, specificare l'amministratore locale incorporato nel sistema in cui si installa il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locali se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata sul sistema host. Il formato valido per il campo Nome utente è: *Nome utente* Non utilizzare virgolette doppie (") o backtick (`) nelle password. Non utilizzare il valore inferiore a (<) e il punto esclamativo (!) simboli insieme nelle password. Ad esempio, meno di<!10, meno di 10<!, backtick`12.
Password	Inserire la password utilizzata per l'autenticazione.
Modalità di autenticazione	Selezionare la modalità di autenticazione che si desidera utilizzare.
Utilizzare i privilegi sudo	Selezionare la casella di controllo **Usa privilegi sudo** se si stanno creando credenziali per un utente non root. Applicabile solo agli utenti Linux.

5. Fare clic su **OK**.

Al termine dell'impostazione delle credenziali, è possibile assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina User and Access (utenti e accesso).

Configurare gMSA su Windows Server 2012 o versione successiva

Windows Server 2012 o versione successiva consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatica delle password dell'account di servizio da un account di dominio gestito.

Cosa ti serve

- È necessario disporre di un controller di dominio Windows Server 2012 o versione successiva.
- È necessario disporre di un host Windows Server 2012 o versione successiva, membro del dominio.

Fasi

1. Creare una chiave root KDS per generare password univoche per ogni oggetto in gMSA.
2. Per ciascun dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -EffectiveImmediately
3. Creare e configurare gMSA:
   a. Creare un account di gruppo utenti nel seguente formato:

```
 domainName\accountName$
.. Aggiungere oggetti computer al gruppo.
.. Utilizzare il gruppo di utenti appena creato per creare gMSA.
```

   Ad esempio,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Eseguire `Get-ADServiceAccount` per verificare l'account del
servizio.
```

4. Configurare gMSA sugli host:
   a. Attivare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

   A tale scopo, eseguire il seguente comando da PowerShell:

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                            Name                Install State
------------                            ----                -------------
[ ] Active Directory Domain Services    AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. Riavviare l'host.

b. Installare gMSA sull'host eseguendo il seguente comando dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verificare l'account gMSA eseguendo il seguente comando: `Test-AdServiceAccount <gMSA>`

5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.
6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter.

   Il server SnapCenter installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

Installare il plug-in SnapCenter per i database SAP HANA

Aggiungere host e installare pacchetti plug-in su host remoti

Utilizzare la pagina Aggiungi host di SnapCenter per aggiungere host e installare i pacchetti dei plug-in. I plug-in vengono installati automaticamente sugli host remoti. È possibile aggiungere un host e installare pacchetti plug-in per un singolo host o per un cluster.

Cosa ti serve

- È necessario essere un utente assegnato a un ruolo che disponga delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore di SnapCenter.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host.
- Assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.
- La documentazione di amministrazione contiene informazioni sulla gestione degli host.

- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi.

  "Configurare account di servizio gestito di gruppo su Windows Server 2012 o versione successiva per SAP HANA"

A proposito di questa attività

- Non è possibile aggiungere un server SnapCenter come host plug-in a un altro server SnapCenter.
- Per consentire a SAP HANA System Replication di rilevare le risorse sui sistemi primario e secondario, si consiglia di aggiungere sia il sistema primario che quello secondario utilizzando l'utente root o sudo.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Verificare che la scheda **Managed hosts** sia selezionata nella parte superiore.
3. Fare clic su **Aggiungi**.
4. Nella pagina host, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Tipo di host	Selezionare il tipo di host: • Windows • Linux Il plug-in per SAP HANA viene installato sull'host client HDBSQL e questo host può essere installato su un sistema Windows o Linux.
Nome host	Inserire il nome host della comunicazione. Inserire il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla configurazione corretta del DNS. Pertanto, la procedura consigliata consiste nell'inserire l'FQDN. È necessario configurare il client HDBSQL e HDBUserStore su questo host.

Per questo campo…	Eseguire questa operazione…
Credenziali	Selezionare il nome della credenziale creata o creare nuove credenziali. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per ulteriori informazioni, vedere le informazioni sulla creazione delle credenziali. È possibile visualizzare i dettagli relativi alle credenziali posizionando il cursore sul nome fornito. La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.

5. Nella sezione Select Plug-in to Install (Seleziona plug-in da installare), selezionare i plug-in da installare.
6. (Facoltativo) fare clic su **altre opzioni**.

Per questo campo…	Eseguire questa operazione…
Porta	Mantenere il numero di porta predefinito o specificare il numero di porta. Il numero di porta predefinito è 8145. Se il server SnapCenter è stato installato su una porta personalizzata, tale numero di porta viene visualizzato come porta predefinita. Se i plug-in sono stati installati manualmente e si è specificata una porta personalizzata, è necessario specificare la stessa porta. In caso contrario, l'operazione non riesce.
Percorso di installazione	Il plug-in per SAP HANA viene installato sull'host client HDBSQL e questo host può essere installato su un sistema Windows o Linux. • Per il pacchetto di plug-in SnapCenter per Windows, il percorso predefinito è C: In alternativa, è possibile personalizzare il percorso. • Per il pacchetto di plug-in SnapCenter per Linux, il percorso predefinito è /opt/NetApp/snapcenter. In alternativa, è possibile personalizzare il percorso.
Ignorare i controlli di preinstallazione	Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

Per questo campo…	Eseguire questa operazione…
Utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in	Per l'host Windows, selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in. Fornire il nome gMSA nel seguente formato: Nome dominio/nome account. GMSA verrà utilizzato come account del servizio di accesso solo per il servizio del plug-in SnapCenter per Windows.

7. Fare clic su **Invia**.

   Se non è stata selezionata la casella di controllo Ignora precheck, l'host viene validato per verificare se l'host soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione di PowerShell, la versione di .NET, la posizione (per i plug-in Windows) e la versione di Java (per i plug-in Linux) sono validati in base ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati messaggi di errore o di avviso appropriati.

   Se l'errore riguarda lo spazio su disco o la RAM, è possibile aggiornare il file web.config che si trova in C: File di programma NetApp SnapCenter WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

   In una configurazione ha, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Se il tipo di host è Linux, verificare l'impronta digitale, quindi fare clic su **Confirm and Submit** (Conferma e invia).

   In una configurazione del cluster, verificare l'impronta digitale di ciascuno dei nodi del cluster.

   La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l'avanzamento dell'installazione.

   I file di log specifici dell'installazione si trovano in /custom_location/snapcenter/logs.

Installare i pacchetti plug-in SnapCenter per Linux o Windows su più host remoti utilizzando i cmdlet

È possibile installare i pacchetti plug-in SnapCenter per Linux o Windows su più host contemporaneamente utilizzando il cmdlet Install-SmHostPackage PowerShell.

Cosa ti serve

È necessario aver effettuato l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale

su ciascun host su cui si desidera installare il pacchetto del plug-in.

Fasi

1. Avviare PowerShell.
2. Sull'host del server SnapCenter, stabilire una sessione utilizzando il cmdlet Open-SmConnection, quindi immettere le credenziali.
3. Installare il plug-in su più host utilizzando il cmdlet Install-SmHostPackage e i parametri richiesti.

   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 alla "Guida di riferimento al cmdlet del software SnapCenter".

   È possibile utilizzare l'opzione -skipprecheck quando i plug-in sono stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

4. Inserire le credenziali per l'installazione remota.

Installare il plug-in SnapCenter per il database SAP HANA su host Linux utilizzando l'interfaccia della riga di comando

Installare il plug-in SnapCenter per il database SAP HANA utilizzando l'interfaccia utente (UI) di SnapCenter. Se l'ambiente in uso non consente l'installazione remota del plug-in dall'interfaccia utente di SnapCenter, è possibile installare il plug-in per il database SAP HANA in modalità console o silent utilizzando l'interfaccia a riga di comando (CLI).

Cosa ti serve

- Installare il plug-in per il database SAP HANA su ciascun host Linux in cui risiede il client HDBSQL.
- L'host Linux su cui si installa il plug-in SnapCenter per il database SAP HANA deve soddisfare i requisiti di software, database e sistema operativo dipendenti.

  Lo strumento matrice di interoperabilità (IMT) contiene le informazioni più recenti sulle configurazioni supportate.

  "Tool di matrice di interoperabilità NetApp"

- Il plug-in SnapCenter per il database SAP HANA fa parte del pacchetto di plug-in SnapCenter per Linux. Prima di installare il pacchetto di plug-in SnapCenter per Linux, è necessario aver già installato SnapCenter su un host Windows.

Fasi

1. Copiare il file di installazione del pacchetto plug-in SnapCenter per Linux (Snapcenter_linux_host_plugin.bin) da C: ProgramData/NetApp SnapCenter/Package Repository all'host in cui si desidera installare il plug-in per il database SAP HANA.

   È possibile accedere a questo percorso dall'host in cui è installato il server SnapCenter.

2. Dal prompt dei comandi, accedere alla directory in cui è stato copiato il file di installazione.
3. Installare il plug-in: `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`

- -DPORT specifica la porta di comunicazione HTTPS SMCore.
- -DSERVER_IP specifica l'indirizzo IP del server SnapCenter.
- -DSERVER_HTTPS_PORT specifica la porta HTTPS del server SnapCenter.
- -DUSER_INSTALL_DIR specifica la directory in cui si desidera installare il pacchetto di plug-in SnapCenter per Linux.
- DINSTALL_LOG_NAME specifica il nome del file di log.

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Modificare il file /<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties, quindi aggiungere IL parametro PLUGINS_ENABLED = hana:3.0.
5. Aggiungere l'host al server SnapCenter utilizzando il cmdlet Add-Smhost e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, fare riferimento alla "Guida di riferimento al cmdlet del software SnapCenter".

Monitorare lo stato dell'installazione del plug-in per SAP HANA

È possibile monitorare lo stato di avanzamento dell'installazione del pacchetto plug-in di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento dell'installazione per determinare quando è completa o se si è verificato un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

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

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Jobs**.
3. Nella pagina lavori, per filtrare l'elenco in modo che siano elencate solo le operazioni di installazione del plug-in, attenersi alla seguente procedura:

a. Fare clic su **Filter** (filtro).
b. Facoltativo: Specificare la data di inizio e di fine.
c. Dal menu a discesa Type (tipo), selezionare **Plug-in installation** (Installazione plug-in).
d. Dal menu a discesa Status (Stato), selezionare lo stato dell'installazione.
e. Fare clic su **Apply** (Applica).

4. Selezionare il processo di installazione e fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

Configurare il certificato CA

Generare il file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato verrà associata una chiave privata.

CSR è un blocco di testo codificato fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

Per informazioni su come generare una CSR, vedere "Come generare il file CSR del certificato CA".

> Se si possiede il certificato CA per il dominio (*.domain.company.com) o il sistema (machine1.domain.company.com), è possibile ignorare la generazione del file CSR del certificato CA. È possibile implementare il certificato CA esistente con SnapCenter.

Per le configurazioni del cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere indicati nel certificato CA. Il certificato può essere aggiornato compilando il campo Subject alternative Name (SAN) (Nome alternativo soggetto) prima di procurarsi il certificato. Per un certificato wild card (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

Importare i certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host di Windows utilizzando la console di gestione Microsoft (MMC).

Fasi

1. Accedere alla console di gestione Microsoft (MMC), quindi fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
2. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
3. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
4. Fare clic su **root console** > **certificati – computer locale** > **autorità di certificazione root attendibili** > **certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Trusted Root Certification Authorities", quindi selezionare **All Tasks** > **Import** per avviare l'importazione guidata.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Effettuare le seguenti operazioni…
Importa chiave privata	Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**.
Formato del file di importazione	Non apportare modifiche; fare clic su **Avanti**.
Sicurezza	Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**.
Completamento dell'importazione guidata certificati	Esaminare il riepilogo, quindi fare clic su **fine** per avviare l'importazione.

Il certificato di importazione deve essere fornito in bundle con la chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personal".

Ottenere il thumbprint del certificato CA

Un'identificazione personale del certificato è una stringa esadecimale che identifica un certificato. Un'identificazione personale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione personale.

Fasi

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo certificato, fare clic sulla scheda **Dettagli**.
   c. Scorrere l'elenco dei campi e fare clic su **Thumbprint**.
   d. Copiare i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se la stampa personale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "A909502ddd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il comando seguente per elencare l'identificazione del certificato installato e identificare il certificato installato di recente in base al nome del soggetto.

      Get-ChildItem -Path Certate: LocalMachine/My

   b. Copiare la stampa personale.

Configurare il certificato CA con i servizi plug-in dell'host Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire le seguenti operazioni sul server SnapCenter e su tutti gli host plug-in in cui sono già implementati i certificati CA.

Fasi

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Ad esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in
   dell'host Windows eseguendo i seguenti comandi:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Ad esempio:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

Configurare il certificato CA per il servizio plug-in SAP HANA di SnapCenter sull'host Linux

È necessario gestire la password dell'archivio chiavi dei plug-in personalizzati e il relativo certificato, configurare il certificato CA, configurare i certificati root o intermedi per l'archivio certificati attendibili dei plug-in personalizzati e configurare la coppia di chiavi firmate CA per l'archivio di fiducia dei plug-in personalizzati con il servizio Plug-in personalizzati di SnapCenter per attivare il certificato digitale installato.

I plug-in personalizzati utilizzano il file 'keystore.jks', che si trova in */opt/NetApp/snapcenter/scc/etc* sia come Trust-store che come keystore.

Gestire la password per l'archivio chiavi del plug-in personalizzato e l'alias della coppia di chiavi firmate CA in uso

Fasi

1. È possibile recuperare la password predefinita del keystore del plug-in personalizzato dal file di proprietà dell'agente del plug-in personalizzato.

È il valore corrispondente alla chiave 'KEYSTORE_PASS'.

2. Modificare la password del keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle chiavi private nel
keystore con la stessa password utilizzata per il keystore:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

3. Riavviare il servizio dopo aver modificato la password.

La password per il keystore del plug-in personalizzato e per tutte le password alias associate della chiave privata deve essere la stessa.

Configurare i certificati root o intermedi per l'archivio di trust del plug-in personalizzato

È necessario configurare i certificati root o intermedi senza la chiave privata per l'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato: /Opt/NetApp/snapcenter/scc/ecc.
2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungere un certificato root o intermedio:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Riavviare il servizio dopo aver configurato i certificati root o
intermedi in un archivio di trust plug-in personalizzato.
```

Aggiungere il certificato CA principale e i certificati CA intermedi.

Configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato

È necessario configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato /opt/NetApp/snapcenter/scc/ecc.

2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Aggiungere il certificato CA con chiave pubblica e privata.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. Elencare i certificati aggiunti nel keystore.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA in password archivio chiavi.

   La password predefinita customizzato del plug-in keystore è il valore della chiave KEYSTORE_PASS nel file agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Se il nome alias nel certificato CA è lungo e contiene spazi o
   caratteri speciali ("*",","), modificare il nome alias con un nome
   semplice:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Configurare il nome alias del certificato CA nel file
   agent.properties.
   ```

   Aggiornare questo valore con la chiave SCC_CERTIFICATE_ALIAS.

8. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Configurare l'elenco CRL (Certificate Revocation List) per i plug-in personalizzati di SnapCenter

A proposito di questa attività

- I plug-in personalizzati di SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in personalizzati di SnapCenter è ' opt/NetApp/snapcenter/scc/etc/crl'.

Fasi

1. È possibile modificare e aggiornare la directory predefinita nel file agent.properties in base alla chiave CRL_PATH.

È possibile inserire più file CRL in questa directory. I certificati in entrata verranno verificati per ciascun CRL.

Configurare il certificato CA per il servizio plug-in SAP HANA di SnapCenter sull'host Windows

È necessario gestire la password dell'archivio chiavi dei plug-in personalizzati e il relativo certificato, configurare il certificato CA, configurare i certificati root o intermedi per l'archivio certificati attendibili dei plug-in personalizzati e configurare la coppia di chiavi firmate CA per l'archivio di fiducia dei plug-in personalizzati con il servizio Plug-in personalizzati di SnapCenter per attivare il certificato digitale installato.

I plug-in personalizzati utilizzano il file *keystore.jks*, che si trova in _C: File di programma NetApp, SnapCenter, Snapcenter Plug-in Creator, ecc., sia come archivio di fiducia che come archivio chiavi.

Gestire la password per l'archivio chiavi del plug-in personalizzato e l'alias della coppia di chiavi firmate CA in uso

Fasi

1. È possibile recuperare la password predefinita del keystore del plug-in personalizzato dal file di proprietà dell'agente del plug-in personalizzato.

   È il valore corrispondente alla chiave *KEYSTORE_PASS*.

2. Modificare la password del keystore:

   keytool -storepasswd -keystore keystore.jks

   > Se il comando "keytool" non viene riconosciuto dal prompt dei comandi di Windows, sostituire il comando keytool con il relativo percorso completo.

   C: File di programma Java <jdk_version> keytool.exe" -storepasswd -keystore keystore.jks

3. Modificare la password per tutti gli alias delle chiavi private nel keystore con la stessa password utilizzata per il keystore:

   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks

   Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

4. Riavviare il servizio dopo aver modificato la password.

   > La password per il keystore del plug-in personalizzato e per tutte le password alias associate della chiave privata deve essere la stessa.

Configurare i certificati root o intermedi per l'archivio di trust del plug-in personalizzato

È necessario configurare i certificati root o intermedi senza la chiave privata per l'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato _C: File di

programma/NetApp/SnapCenter/Snapcenter Plug-in Creator

2. Individuare il file 'keystore.jks'.
3. Elencare i certificati aggiunti nel keystore:

   keytool -list -v -keystore keystore.jks

4. Aggiungere un certificato root o intermedio:

   Keytool -import -trustcaacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Riavviare il servizio dopo aver configurato i certificati root o intermedi in un archivio di trust plug-in personalizzato.

Aggiungere il certificato CA principale e i certificati CA intermedi.

Configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato

È necessario configurare la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Fasi

1. Accedere alla cartella contenente il keystore del plug-in personalizzato _C: File di programma/NetApp/SnapCenter/Snapcenter Plug-in Creator
2. Individuare il file *keystore.jks*.
3. Elencare i certificati aggiunti nel keystore:

   keytool -list -v -keystore keystore.jks

4. Aggiungere il certificato CA con chiave pubblica e privata.

   Keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS

5. Elencare i certificati aggiunti nel keystore.

   keytool -list -v -keystore keystore.jks

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA in password archivio chiavi.

   La password predefinita customizzato del plug-in keystore è il valore della chiave KEYSTORE_PASS nel file agent.properties.

   Keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore keystore.jks

8. Configurare il nome alias del certificato CA nel file *agent.properties*.

   Aggiornare questo valore con la chiave SCC_CERTIFICATE_ALIAS.

9. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate della CA nell'archivio di trust del plug-in personalizzato.

Configurare l'elenco CRL (Certificate Revocation List) per i plug-in personalizzati di SnapCenter

A proposito di questa attività

- Per scaricare il file CRL più recente per il certificato CA correlato, vedere "Come aggiornare il file dell'elenco di revoca dei certificati nel certificato CA di SnapCenter".
- I plug-in personalizzati di SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in personalizzati di SnapCenter è _'C: File di programma, NetApp, SnapCenter, SnapCenter Plug-in Creator, ecc.

Fasi

1. È possibile modificare e aggiornare la directory predefinita nel file *agent.properties* in base alla chiave CRL_PATH.
2. È possibile inserire più file CRL in questa directory.

   I certificati in entrata verranno verificati per ciascun CRL.

Abilitare i certificati CA per i plug-in

È necessario configurare i certificati CA e implementarne i certificati nel server SnapCenter e negli host plug-in corrispondenti. Attivare la convalida del certificato CA per i plug-in.

Cosa ti serve

- È possibile attivare o disattivare i certificati CA utilizzando il cmdlet Esegui *set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando le *Get-SmCertificateSettings*.

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 alla "Guida di riferimento al cmdlet del software SnapCenter".

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **hosts**.
2. Nella pagina hosts, fare clic su **Managed hosts**.
3. Selezionare uno o più host plug-in.
4. Fare clic su **altre opzioni**.
5. Selezionare **attiva convalida certificato**.

Al termine

L'host della scheda host gestiti visualizza un lucchetto e il colore del lucchetto indica lo stato della connessione tra il server SnapCenter e l'host del plug-in.

- Indica che il certificato CA non è né abilitato né assegnato all'host del plug-in.
- Indica che il certificato CA è stato validato correttamente.
- Indica che non è stato possibile validare il certificato CA.

- indica che non è stato possibile recuperare le informazioni di connessione.

> Quando lo stato è giallo o verde, le operazioni di protezione dei dati vengono completate correttamente.

Installare il plug-in SnapCenter per VMware vSphere

Se il database viene memorizzato su macchine virtuali (VM) o se si desidera proteggere macchine virtuali e datastore, è necessario implementare il plug-in SnapCenter per l'appliance virtuale VMware vSphere.

Per informazioni sulla distribuzione, vedere "Panoramica sull'implementazione".

Implementare il certificato CA

Per configurare il certificato CA con il plug-in SnapCenter per VMware vSphere, vedere "Creare o importare un certificato SSL".

Configurare il file CRL

Il plug-in SnapCenter per VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il plug-in SnapCenter per VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più file CRL in questa directory. I certificati in entrata verranno verificati per ciascun CRL.

Prepararsi alla protezione dei dati

Prerequisiti per l'utilizzo del plug-in SnapCenter per il database SAP HANA

Prima di utilizzare il plug-in SnapCenter per il database SAP HANA, l'amministratore di SnapCenter deve installare e configurare il server SnapCenter ed eseguire le attività necessarie.

- Installare e configurare il server SnapCenter.
- Accedere al server SnapCenter.
- Configurare l'ambiente SnapCenter aggiungendo connessioni al sistema di storage e creando credenziali, se applicabili.
- Installare Java 1.7 o Java 1.8 sull'host Linux o Windows.

  È necessario impostare il percorso Java nella variabile di percorso ambientale del computer host.

- Impostare SnapMirror e SnapVault, se si desidera eseguire la replica del backup.
- Installare il client HDBSQL sull'host in cui verrà installato il plug-in per il database SAP HANA.

  Configurare le chiavi dell'archivio utente per i nodi SAP HANA che verranno gestiti tramite questo host.

- Per il database SAP HANA 2.0SPS05, se si utilizza un account utente del database SAP HANA, assicurarsi di disporre delle seguenti autorizzazioni per eseguire operazioni di backup, ripristino e

clonazione nel server SnapCenter:

- Amministratore del backup
- Catalogo letto
- Amministratore del backup del database
- Operatore di ripristino del database

Utilizzo di risorse, gruppi di risorse e policy per la protezione dei database SAP HANA

Prima di utilizzare SnapCenter, è utile comprendere i concetti di base relativi alle operazioni di backup, clonazione e ripristino che si desidera eseguire. Interagisci con risorse, gruppi di risorse e policy per diverse operazioni.

- In genere, le risorse sono database SAP HANA di cui si esegue il backup o la clonazione con SnapCenter.
- Un gruppo di risorse SnapCenter è un insieme di risorse su un host.

  Quando si esegue un'operazione su un gruppo di risorse, tale operazione viene eseguita sulle risorse definite nel gruppo di risorse in base alla pianificazione specificata per il gruppo di risorse.

  È possibile eseguire il backup su richiesta di una singola risorsa o di un gruppo di risorse. È inoltre possibile eseguire backup pianificati per singole risorse e gruppi di risorse.

- I criteri specificano la frequenza di backup, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  Quando si crea un gruppo di risorse, si selezionano uno o più criteri per tale gruppo. È inoltre possibile selezionare un criterio quando si esegue un backup su richiesta per una singola risorsa.

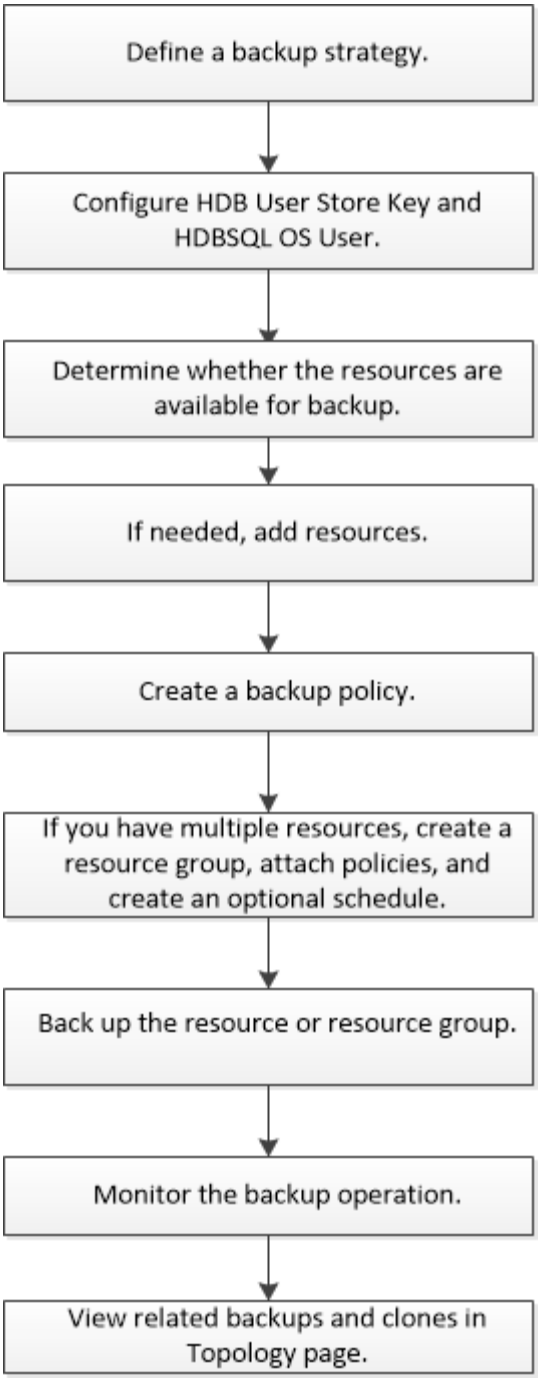
Un gruppo di risorse definisce ciò che si desidera proteggere e quando si desidera proteggerlo in termini di giorno e ora. Pensa a una policy come a come vuoi proteggerla. Ad esempio, se si esegue il backup di tutti i database, è possibile creare un gruppo di risorse che includa tutti i database dell'host. È quindi possibile associare due criteri al gruppo di risorse: Una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e si allegano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup completo ogni giorno.

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.

   Quindi 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.

   Quindi 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.

Per questo campo…	Eseguire questa operazione…
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**.

   Facoltativo: È possibile fare clic su  Per aggiungere più 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).

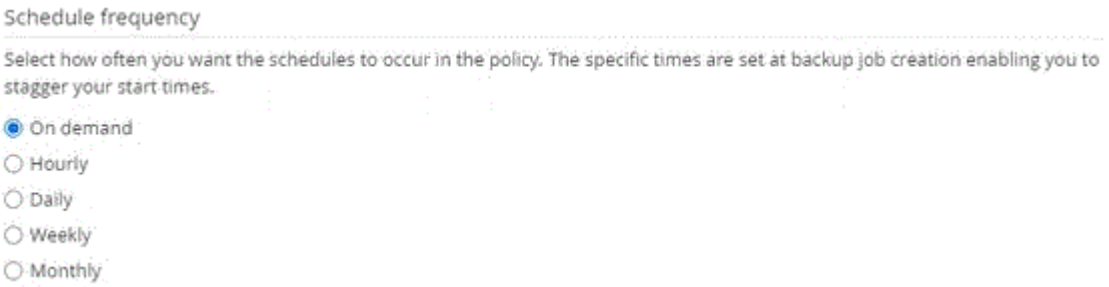
Fasi

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**.

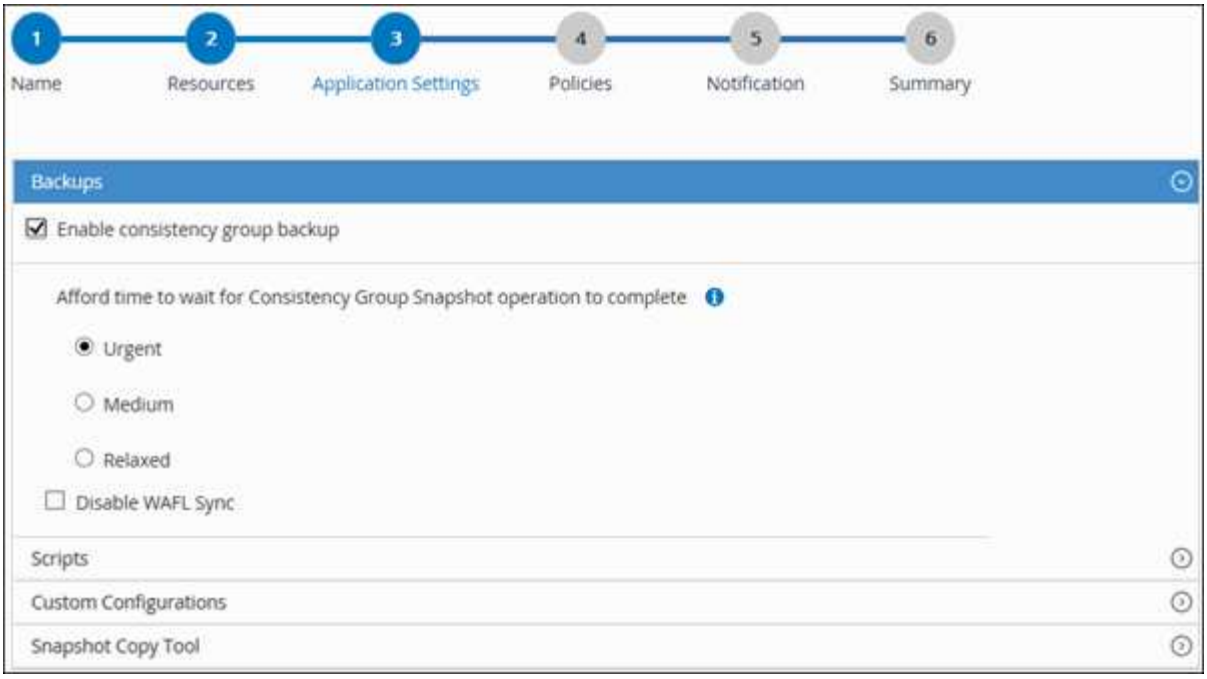
   In questo modo è possibile filtrare le informazioni sullo schermo.

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.

Puoi anche creare una policy facendo clic su + .

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

b.

Nella colonna Configure Schedules (Configura pianificazioni), fare clic su  per la policy 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 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. Quindi 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.

      Puoi anche 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 Configure Schedules (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 cercare il gruppo di risorse inserendo il nome del gruppo di risorse nella casella di ricerca o facendo clic su , quindi selezionare il tag. Quindi 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 alla "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 alla "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 su 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 su Nel riquadro Activity (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.

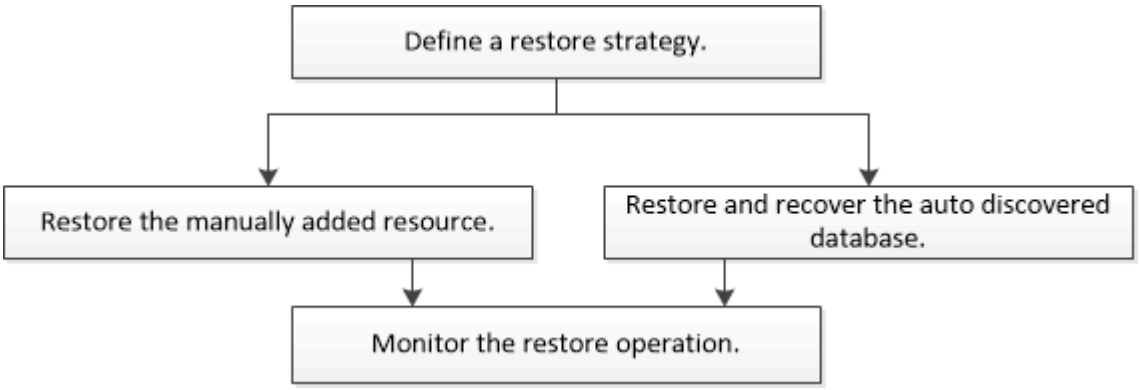
7. Se si desidera eliminare un clone, selezionarlo dalla tabella, quindi fare clic su .
8. Se si desidera suddividere un clone, selezionarlo dalla tabella, quindi fare clic su .

Ripristinare i database SAP HANA

Ripristinare il flusso di lavoro

Il flusso di lavoro di ripristino e ripristino include la pianificazione, l'esecuzione delle operazioni di ripristino e il monitoraggio delle operazioni.

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



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 informazioni dettagliate sui cmdlet di PowerShell.

"Guida di riferimento al cmdlet del software SnapCenter".

Ripristinare e ripristinare un backup delle risorse aggiunto manualmente

È possibile utilizzare SnapCenter per ripristinare e ripristinare i dati da uno o più backup.

Cosa ti serve

- È necessario aver eseguito il backup delle risorse o dei gruppi di risorse.
- È necessario annullare qualsiasi operazione di backup attualmente in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi di pre-restore, post-restore, mount e unmount, controllare se i comandi esistono nell'elenco dei comandi disponibile sull'host del 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.

A proposito di questa attività

- Le copie di backup basate su file non possono essere ripristinate da SnapCenter.
- Dopo l'aggiornamento a SnapCenter 4.3, i backup eseguiti in SnapCenter 4.2 possono essere ripristinati ma non ripristinati. Per ripristinare i backup eseguiti in SnapCenter 4.2, è necessario utilizzare script di ripristino HANA Studio o HANA esterni a SnapCenter.

Fasi

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

   Le risorse vengono visualizzate insieme al tipo, all'host, ai gruppi di risorse e ai criteri associati e allo stato.

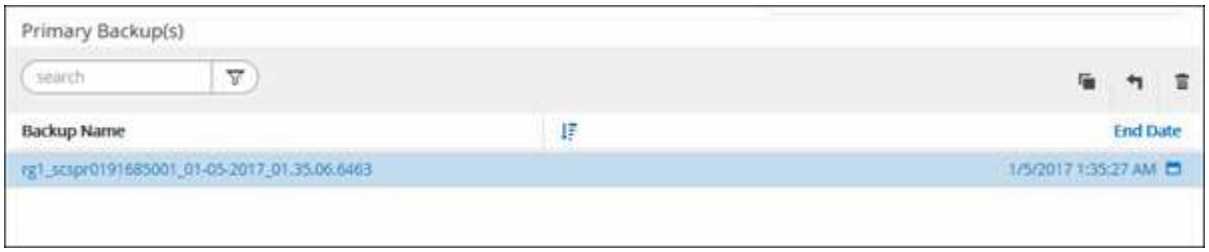
   Anche se un backup potrebbe essere per un gruppo di risorse, quando si esegue il ripristino, è necessario selezionare le singole risorse da ripristinare.

   Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato "NOT Protected". Ciò può significare che la risorsa non è protetta o che il backup della risorsa è stato eseguito da un altro utente.

3. Selezionare la risorsa o un gruppo di risorse, quindi selezionare una risorsa in tale gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dai sistemi di storage primario o secondario (mirrorati o vault).
5. Nella tabella Primary backup(s) (Backup primari), selezionare il backup da cui si desidera ripristinare, quindi fare clic su  .



6. Nella pagina Restore Scope (ambito ripristino), selezionare **complete Resource** (completa risorsa) o **file Level** (livello file).

   a. Se si seleziona **complete Resource** (completa risorsa), vengono ripristinati tutti i volumi di dati configurati del database SAP HANA.

      Se la risorsa contiene volumi o qtree, le copie Snapshot eseguite dopo la copia Snapshot selezionata per il ripristino su tali volumi o qtree vengono eliminate e non possono essere ripristinate. Inoltre, se un'altra risorsa è ospitata sugli stessi volumi o qtree, anche tale risorsa viene eliminata.

   b. Se si seleziona **file Level**, è possibile selezionare **All** o selezionare i volumi o le qtree specifici, quindi immettere il percorso relativo a tali volumi o qtree, separati da virgole

- È possibile selezionare più volumi e qtree.
- Se il tipo di risorsa è LUN, viene ripristinato l'intero LUN.

  È possibile selezionare più LUN.

Se si seleziona **tutto**, vengono ripristinati tutti i file presenti nei volumi, nei qtree o nei LUN.

7. Nella pagina Pre Ops (operazioni preliminari), immettere i comandi di pre-ripristino e disinstallazione da eseguire prima di eseguire un processo di ripristino.

   I comandi di disinstallazione non sono disponibili per le risorse rilevate automaticamente.

8. Nella pagina Post Ops (operazioni post), immettere i comandi di montaggio e post ripristino da eseguire dopo l'esecuzione di un processo di ripristino.

   I comandi di montaggio non sono disponibili per le risorse rilevate automaticamente.

9. 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 nella pagina **Impostazioni** > **Impostazioni globali**.

10. Esaminare il riepilogo, quindi fare clic su **fine**.
11. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Ripristinare e ripristinare un backup del database rilevato automaticamente

È possibile utilizzare SnapCenter per ripristinare e ripristinare i dati da uno o più backup.

Cosa ti serve

- È necessario aver eseguito il backup delle risorse o dei gruppi di risorse.
- È necessario annullare qualsiasi operazione di backup attualmente in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi di pre-restore, post-restore, mount e unmount, controllare se i comandi esistono nell'elenco dei comandi disponibile sull'host del 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.

A proposito di questa attività

- Le copie di backup basate su file non possono essere ripristinate da SnapCenter.
- Dopo l'aggiornamento a SnapCenter 4.3, i backup eseguiti in SnapCenter 4.2 possono essere ripristinati ma non ripristinati. Per ripristinare i backup eseguiti in SnapCenter 4.2, è necessario utilizzare script di ripristino HANA Studio o HANA esterni a SnapCenter.

Fasi

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

   Le risorse vengono visualizzate insieme al tipo, all'host, ai gruppi di risorse e ai criteri associati e allo stato.

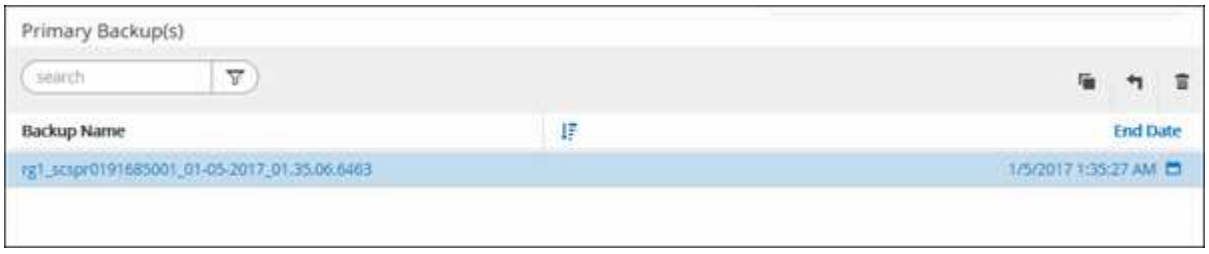
   Anche se un backup potrebbe essere per un gruppo di risorse, quando si esegue il ripristino, è necessario selezionare le singole risorse da ripristinare.

   Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato "NOT Protected". Ciò può significare che la risorsa non è protetta o che il backup della risorsa è stato eseguito da un altro utente.

3. Selezionare la risorsa o un gruppo di risorse, quindi selezionare una risorsa in tale gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dai sistemi di storage primario o secondario (mirrorati o vault).
5. Nella tabella Primary backup(s) (Backup primari), selezionare il backup da cui si desidera ripristinare, quindi fare clic su .



6. Nella pagina Restore Scope (ambito ripristino), selezionare **complete Resource** (completa risorsa) per ripristinare i volumi di dati configurati del database SAP HANA.

   È possibile selezionare **complete Resource** (con o senza **Volume Revert**) o **Tenant Database**.

   L'operazione di recovery non è supportata dal server SnapCenter per più tenant quando l'utente seleziona l'opzione **Database tenant** o **Ripristino completo**. Per eseguire l'operazione di ripristino, è necessario utilizzare lo script HANA studio o HANA python.

   a. Selezionare **Volume Revert** (Ripristina volume) per ripristinare l'intero volume.

      Questa opzione è disponibile per i backup eseguiti in SnapCenter 4.3 in ambienti NFS.

      Se la risorsa contiene volumi o qtree, le copie Snapshot eseguite dopo la copia Snapshot selezionata per il ripristino su tali volumi o qtree vengono eliminate e non possono essere ripristinate. Inoltre, se un'altra risorsa è ospitata sugli stessi volumi o qtree, anche tale risorsa viene eliminata. Questa opzione è applicabile quando l'opzione **completa risorsa** con **Ripristino volume** è selezionata per il ripristino.

   b. Selezionare **Database tenant**.

Questa opzione è disponibile solo per le risorse MDC.

Assicurarsi di arrestare il database tenant prima di eseguire l'operazione di ripristino.

Se si seleziona l'opzione **Database tenant**, è necessario utilizzare HANA studio o gli script di ripristino HANA esterni a SnapCenter per eseguire l'operazione di ripristino.

7. Nella pagina Recovery Scope (ambito ripristino), selezionare una delle seguenti opzioni:

Se…	**Eseguire questa operazione…**
Desidera ripristinare il più vicino possibile all'ora corrente	Selezionare **Ripristina allo stato più recente**. Per le risorse container singole, specificare una o più posizioni di backup del registro e del catalogo. Per le risorse MDC (Multitenant Database Container), specificare una o più posizioni di backup dei log e la posizione del catalogo di backup. Per le risorse MDC, il percorso deve contenere sia i log del database del sistema che quelli del tenant.

Se…	Eseguire questa operazione…
Si desidera ripristinare al punto di tempo specificato	Selezionare **Recover to point in time** (Ripristina al punto nel tempo). a. Selezionare il fuso orario. Il fuso orario del browser viene popolato per impostazione predefinita. Il fuso orario selezionato e l'ora di immissione vengono convertiti in GMT assoluto. b. Inserire data e ora. Ad esempio, l'host HANA Linux si trova a Sunnyvale, CA e l'utente di Raleigh, NC, sta recuperando i log in a SnapCenter. La differenza di tempo tra queste due posizioni è di 3 ore e, poiché l'utente ha effettuato l'accesso da Raleigh, NC, il fuso orario predefinito del browser che verrà selezionato nella GUI è GMT-04:00. Se l'utente desidera eseguire un ripristino a 5.sunnyvale, CA, l'utente deve impostare il fuso orario del browser sul fuso orario dell'host HANA Linux, GMT-07:00, specificando data e ora alle 5:00 Per le risorse container singole, specificare una o più posizioni di backup del registro e del catalogo. Per le risorse MDC, specificare una o più posizioni di backup del registro e la posizione del catalogo di backup. Per le risorse MDC, il percorso deve contenere sia i log del database del sistema che quelli del tenant.
Ripristinare un backup dei dati specifico	Selezionare **Recover to specified data backup** (Ripristina backup dati specificati).
Non si desidera eseguire il ripristino	Selezionare **Nessun ripristino**. È necessario eseguire manualmente l'operazione di ripristino da HANA Studio.

È possibile ripristinare solo i backup eseguiti dopo l'aggiornamento a SnapCenter 4.3, a condizione che l'host e il plug-in siano aggiornati a SnapCenter 4.3 e che i backup selezionati per il ripristino vengano eseguiti dopo la conversione o il rilevamento automatico della risorsa.

8. Nella pagina Pre Ops (operazioni preliminari), immettere i comandi di pre-ripristino e disinstallazione da eseguire prima di eseguire un processo di ripristino.

   I comandi di disinstallazione non sono disponibili per le risorse rilevate automaticamente.

9. Nella pagina Post Ops (operazioni post), immettere i comandi di montaggio e post ripristino da eseguire dopo l'esecuzione di un processo di ripristino.

   I comandi di montaggio non sono disponibili per le risorse rilevate automaticamente.

10. 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 nella pagina **Impostazioni** > **Impostazioni globali**.

11. Esaminare il riepilogo, quindi fare clic su **fine**.
12. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Ripristinare il database SAP HANA utilizzando i cmdlet PowerShell

Il ripristino di un backup del database SAP HANA include l'avvio di una sessione di connessione con il server SnapCenter, l'elenco dei backup e il recupero delle informazioni di backup e il ripristino di un backup.

Cosa ti serve

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

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/
   ```

2. Identificare il backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio mostra che sono disponibili due backup per il ripristino:

```
 PS C:\> Get-SmBackup

        BackupId    BackupName                    BackupTime
BackupType
        --------    ----------                    ----------
----------
         1          Payroll Dataset_vise-f6_08... 8/4/2015 11:02:32 AM
Full Backup
         2          Payroll Dataset_vise-f6_08... 8/4/2015 11:23:17 AM
```

Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. Avviare il processo di ripristino in HANA Studio.

Il database viene chiuso.

4. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

   AppObjectId è "host/Plugin/UID", dove UID = SID è per la risorsa di tipo container singolo e UID = MDC/SID è per la risorsa di container multipli. È possibile ottenere ResourceID dal cmdlet Get-smResources.

   ```
   Get-smResources  -HostName cn24.sccore.test.com  -PluginCode HANA
   ```

   Questo esempio mostra come ripristinare il database dallo storage primario:

   ```
   Restore-SmBackup -PluginCode HANA -AppObjectId
   cn24.sccore.test.com\hana\H10 -BackupId 3
   ```

   Questo esempio mostra come ripristinare il database dallo storage secondario:

   ```
   Restore-SmBackup -PluginCode 'HANA' -AppObjectId
   cn24.sccore.test.com\hana\H10 -BackupId 399 -Confirm:$false  -Archive @(
   @{"Primary"="<Primary Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
   Vserver>:<SecondaryVolume>"})
   ```

   I backup saranno disponibili in HANA Studio per il recovery.

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 alla "Guida di riferimento al cmdlet del software SnapCenter".

Ripristinare le risorse utilizzando i cmdlet PowerShell

Il ripristino di un backup delle risorse include l'avvio di una sessione di connessione con il server SnapCenter, l'elenco dei backup, il recupero delle informazioni di backup e il ripristino di un backup.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

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/
   ```

2. Recuperare le informazioni relative a uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

Questo esempio mostra informazioni su tutti i backup disponibili:

```
 C:\PS>PS C:\> Get-SmBackup

BackupId                      BackupName                    BackupTime
BackupType
--------                      ----------                    ----------
----------
  1               Payroll Dataset_vise-f6_08... 8/4/2015    11:02:32 AM
Full Backup
  2               Payroll Dataset_vise-f6_08... 8/4/2015    11:23:17 AM
```

Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

   SmBackupId           : 113
   SmJobId              : 2032
   StartDateTime        : 2/2/2015 6:57:03 AM
   EndDateTime          : 2/2/2015 6:57:11 AM
   Duration             : 00:00:07.3060000
   CreatedDateTime      : 2/2/2015 6:57:23 AM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
   VerificationStatus   : NotVerified

   SmBackupId           : 114
   SmJobId              : 2183
   StartDateTime        : 2/2/2015 1:02:41 PM
   EndDateTime          : 2/2/2015 1:02:38 PM
   Duration             : -00:00:03.2300000
   CreatedDateTime      : 2/2/2015 1:02:53 PM
   Status               : Completed
   ProtectionGroupName  : Clone
   SmProtectionGroupId  : 34
   PolicyName           : Vault
   SmPolicyId           : 18
   BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
   VerificationStatus   : NotVerified
```

3. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

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 alla "Guida di riferimento al cmdlet del software SnapCenter".

Monitorare le operazioni di ripristino dei database SAP HANA

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino di SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

gli stati di post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi altra azione di ripristino che è possibile eseguire.

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- 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 su per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Ripristina**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato di ripristino.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
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.

Dopo l'operazione di ripristino basata sul volume, i metadati di backup vengono cancellati dal repository SnapCenter, ma le voci del catalogo di backup rimangono nel catalogo SAP HANA. Sebbene venga visualizzato lo stato del processo di ripristino , fare clic sui dettagli del lavoro per visualizzare il segnale di avviso relativo ad alcune attività secondarie. Fare clic sul simbolo di avviso ed eliminare le voci del catalogo di backup indicate.

Clonare i backup delle risorse SAP HANA

Clonare il flusso di lavoro

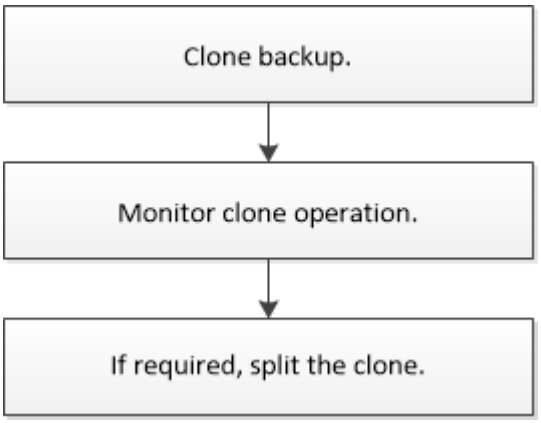
Il flusso di lavoro dei cloni include l'esecuzione dell'operazione di cloni e il monitoraggio dell'operazione.

A proposito di questa attività

- È possibile clonare sul server SAP HANA di origine.
- È possibile clonare i backup delle risorse per i seguenti motivi:
  - Per testare le funzionalità che devono essere implementate utilizzando la struttura e il contenuto delle risorse correnti durante i cicli di sviluppo delle applicazioni

- Per l’estrazione e la manipolazione dei dati durante il popolamento dei data warehouse
- Per ripristinare i dati cancellati o modificati per errore

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



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 informazioni dettagliate sui cmdlet di PowerShell.

Clonare un backup del database SAP HANA

È possibile utilizzare SnapCenter per clonare un backup. È possibile clonare dal backup primario o secondario.

Cosa ti serve

- È necessario aver eseguito il backup delle risorse o del gruppo di risorse.
- Assicurarsi che gli aggregati che ospitano i volumi siano inclusi nell’elenco degli aggregati assegnati della macchina virtuale di storage (SVM).
- Non è possibile clonare backup basati su file.
- Il server clone di destinazione deve avere lo stesso SID dell’istanza SAP HANA fornito nel campo SID clone di destinazione.
- Per i comandi pre-clone o post-clone, controllare se i comandi sono presenti nell’elenco dei comandi disponibile sull’host del 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.

A proposito di questa attività

Per informazioni sulle limitazioni delle operazioni di suddivisione dei cloni, vedere "Guida alla gestione dello storage logico di ONTAP 9".

Fasi

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

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

3. Selezionare la risorsa o il gruppo di risorse.

   Selezionare una risorsa se si seleziona un gruppo di risorse.

   Viene visualizzata la pagina della topologia di risorse o gruppi di risorse.

4. Dalla vista Manage Copies (Gestisci copie), selezionare **Backup** dai sistemi di storage primario o secondario (mirrorati o vault).
5. Selezionare il backup dei dati dalla tabella, quindi fare clic su  .
6. Nella pagina Location (posizione), eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Host plug-in	Selezionare l'host su cui montare il clone e installare il plug-in.
SID clone di destinazione	Inserire l'ID dell'istanza SAP HANA da clonare dai backup esistenti.
NFS Export IP Address (Indirizzo IP esportazione NFS)	Inserire gli indirizzi IP o i nomi host su cui esportare i volumi clonati.
ISCSI Initiator	Inserire il nome iSCSI Initiator dell'host in cui vengono esportati i LUN. Questa opzione è disponibile solo se è stato selezionato il tipo di risorsa LUN.
Protocollo	Inserire il protocollo LUN. Questa opzione è disponibile solo se è stato selezionato il tipo di risorsa LUN.

   Se la risorsa selezionata è un LUN e si sta clonando da un backup secondario, vengono elencati i volumi di destinazione. Una singola origine può avere più volumi di destinazione.

   Prima di eseguire la clonazione, è necessario assicurarsi che l'iniziatore iSCSI o il pannello FCP sia presente e che siano configurati e collegati a host alternativi.

7. Nella pagina script, attenersi alla seguente procedura:

   Gli script vengono eseguiti sull'host del plug-in.

   a. Immettere i comandi per pre-clone o post-clone che devono essere eseguiti rispettivamente prima o

dopo l'operazione di clone.

- Comando pre-clone: Elimina i database esistenti con lo stesso nome
- Comando post clone: Verifica di un database o avvia un database.

b. Immettere il comando mount per montare un file system su un host.

Comando mount per un volume o qtree su una macchina Linux:

Esempio per NFS:

```
mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt
```

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.

9. Esaminare il riepilogo, quindi fare clic su **fine**.
10. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

Clonare i backup del database SAP HANA utilizzando i cmdlet PowerShell

Il flusso di lavoro dei cloni include la pianificazione, l'esecuzione dell'operazione di cloni e il monitoraggio dell'operazione.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

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 alla "Guida di riferimento al cmdlet del software SnapCenter".

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/
```

2. Recuperare i backup per eseguire l'operazione di clonazione utilizzando il cmdlet Get-SmBackup.

Questo esempio mostra che sono disponibili due backup per la clonazione:

```
 C:\PS> Get-SmBackup

        BackupId                        BackupName
BackupTime                    BackupType
        --------                        ----------
----------                    ----------
         1                     Payroll Dataset_vise-f6_08... 8/4/2015
11:02:32 AM          Full Backup
         2                     Payroll Dataset_vise-f6_08... 8/4/2015
11:23:17 AM
```

3. Avviare un'operazione di clonazione da un backup esistente e specificare gli indirizzi IP di esportazione NFS su cui esportare i volumi clonati.

   Questo esempio mostra che il backup da clonare ha un indirizzo NFSExportIPs 10.232.206.169:

```
New-SmClone -AppPluginCode hana -BackupName
scsccore1_sccore_test_com_hana_H73_scsccore1_06-07-2017_02.54.29.3817
-Resources @{"Host"="scsccore1.sccore.test.com";"Uid"="H73"}
-CloneToInstance shivscc4.sccore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data' -preclonecreatecommands
'/home/scripts/scpre_clone.sh' -postclonecreatecommands
'/home/scripts/scpost_clone.sh'
```

   Se NFSExportIP non viene specificato, il valore predefinito viene esportato nell'host di destinazione del clone.

4. Verificare che i backup siano stati clonati correttamente utilizzando il cmdlet Get-SmCloneReport per visualizzare i dettagli del processo clone.

   È possibile visualizzare dettagli quali ID clone, data e ora di inizio, data e ora di fine.

```
PS C:\> Get-SmCloneReport -JobId 186

    SmCloneId           : 1
    SmJobId             : 186
    StartDateTime       : 8/3/2015 2:43:02 PM
    EndDateTime         : 8/3/2015 2:44:08 PM
    Duration            : 00:01:06.6760000
    Status              : Completed
    ProtectionGroupName : Draper
    SmProtectionGroupId : 4
    PolicyName          : OnDemand_Clone
    SmPolicyId          : 4
    BackupPolicyName    : OnDemand_Full_Log
    SmBackupPolicyId    : 1
    CloneHostName       : SCSPR0054212005.mycompany.com
    CloneHostId         : 4
    CloneName           : Draper__clone__08-03-2015_14.43.53
    SourceResources     : {Don, Betty, Bobby, Sally}
    ClonedResources     : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
    SmJobError          :
```

Monitorare le operazioni di clonazione del database SAP HANA

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina lavori. Potrebbe essere necessario controllare lo stato di avanzamento di un'operazione per determinare quando è completa o se si verifica un problema.

A proposito di questa attività

Nella pagina lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- 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 su per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Clone**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato del clone.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro clone, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Job Details (Dettagli processo), fare clic su **View logs** (Visualizza registri).

Separare un clone

È possibile utilizzare SnapCenter per separare una risorsa clonata dalla risorsa principale. Il clone diviso diventa indipendente dalla risorsa padre.

A proposito di questa attività

- Non è possibile eseguire l'operazione di suddivisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato il clone1 da un backup del database, è possibile creare un backup del clone1 e clonare il backup (clone2). Dopo aver creato il clone2, il clone1 è un clone intermedio e non è possibile eseguire l'operazione di suddivisione del clone sul clone1. Tuttavia, è possibile eseguire l'operazione di suddivisione dei cloni sul clone2.

  Dopo aver diviso il clone2, è possibile eseguire l'operazione di divisione del clone sul clone1, poiché il clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup e i lavori di clonazione del clone vengono eliminati.
- Per informazioni sulle limitazioni delle operazioni di suddivisione dei cloni, vedere "Guida alla gestione dello storage logico di ONTAP 9".
- Assicurarsi che il volume o l'aggregato sul sistema di storage sia online.

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 l'opzione appropriata dall'elenco Visualizza:

Opzione	Descrizione
Per applicazioni di database	Selezionare **Database** dall'elenco View (Visualizza).
Per file system	Selezionare **Path** dall'elenco View (Visualizza).

3. Selezionare la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Manage Copies (Gestisci copie), selezionare la risorsa clonata (ad esempio, il database o il LUN), quindi fare clic su  .
5. Esaminare le dimensioni stimate del clone da dividere e lo spazio richiesto disponibile sull'aggregato, quindi fare clic su **Start**.
6. Monitorare l'avanzamento dell'operazione facendo clic su **Monitor** > **Jobs**.

   Se il servizio SMCore viene riavviato, l'operazione di split clone smette di rispondere. Eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione di suddivisione del clone.

   Se si desidera un tempo di polling più lungo o più breve per controllare se il clone è diviso o meno, è possibile modificare il valore del parametro *CloneSplitStatusCheckPollTime* nel file *SMCoreServiceHost.exe.config* per impostare l'intervallo di tempo in cui SMCore deve eseguire il polling per lo stato dell'operazione di suddivisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

   Ad esempio:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   L'operazione di avvio del clone split non riesce se sono in corso operazioni di backup, ripristino o altro clone split. È necessario riavviare l'operazione di suddivisione dei cloni solo al termine delle operazioni in esecuzione.

Ulteriori informazioni

"Il clone o la verifica di SnapCenter non riesce e l'aggregato non esiste"

Eliminare o separare i cloni del database SAP HANA dopo l'aggiornamento di SnapCenter

Dopo l'aggiornamento a SnapCenter 4.3, i cloni non verranno più visualizzati. È possibile eliminare il clone o suddividere i cloni dalla pagina topologia della risorsa da cui sono stati creati i cloni.

A proposito di questa attività

Se si desidera individuare l'impatto dello storage dei cloni nascosti, eseguire il seguente comando: `Get-SmClone -ListStorageFootprint`

Fasi

1. Eliminare i backup delle risorse clonate utilizzando il cmdlet remove-smbackup.
2. Eliminare il gruppo di risorse delle risorse clonate utilizzando il cmdlet remove-sresourcegroup.
3. Rimuovere la protezione della risorsa clonata utilizzando il cmdlet remove-smprotectresource.
4. Selezionare la risorsa principale dalla pagina risorse.

   Viene visualizzata la pagina della topologia delle risorse.

5. Dalla vista Manage Copies (Gestisci copie), selezionare i cloni dai sistemi di storage primario o secondario (mirrorati o replicati).
6. Selezionare i cloni, quindi fare clic su  per eliminare i cloni o fare clic su  per separare i cloni.
7. Fare clic su **OK**.

Informazioni sul copyright

Informazioni sul marchio commerciale