Proteggere PostgreSQL

SnapCenter software

NetApp
November 06, 2025

Sommario

Proteggere PostgreSQL . . . 1
Plug-in SnapCenter per PostgreSQL . . . 1
Panoramica del plug-in SnapCenter per PostgreSQL . . . 1
Cosa puoi fare utilizzando il plug-in SnapCenter per PostgreSQL . . . 1
Funzionalità del plug-in SnapCenter per PostgreSQL . . . 1
Tipi di archiviazione supportati dal plug-in SnapCenter per PostgreSQL . . . 2
Privilegi ONTAP minimi richiesti per il plug-in PostgreSQL . . . 3
Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per PostgreSQL . . . 6
Strategia di backup per PostgreSQL . . . 6
Strategia di ripristino e recupero per PostgreSQL . . . 9
Prepararsi all'installazione del plug-in SnapCenter per PostgreSQL . . . 10
Flusso di lavoro di installazione del plug-in SnapCenter per PostgreSQL . . . 10
Prerequisiti per aggiungere host e installare il plug-in SnapCenter per PostgreSQL . . . 10
Requisiti host per installare il pacchetto plug-in SnapCenter per Windows . . . 14
Requisiti host per l'installazione del pacchetto plug-in SnapCenter per Linux . . . 15
Imposta le credenziali per il plug-in SnapCenter per PostgreSQL . . . 16
Configurare gMSA su Windows Server 2016 o versioni successive . . . 18
Installa il plug-in SnapCenter per PostgreSQL . . . 19
Configurare il certificato CA . . . 25
Prepararsi alla protezione dei dati . . . 32
Prerequisiti per l'utilizzo del plug-in SnapCenter per PostgreSQL . . . 33
Come vengono utilizzate le risorse, i gruppi di risorse e le policy per proteggere PostgreSQL . . . 33
Eseguire il backup delle risorse PostgreSQL . . . 33
Eseguire il backup delle risorse PostgreSQL . . . 33
Scopri automaticamente i cluster . . . 35
Aggiungere manualmente le risorse all'host del plug-in . . . 35
Creare policy di backup per PostgreSQL . . . 37
Crea gruppi di risorse e allega criteri . . . 40
Crea gruppi di risorse e abilita la protezione secondaria per le risorse PostgreSQL sui sistemi ASA r2 . . . 44
Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per PostgreSQL . . . 46
Eseguire il backup di PostgreSQL . . . 48
Eseguire il backup dei gruppi di risorse . . . 53
Monitorare le operazioni di backup di PostgreSQL . . . 54
Annulla le operazioni di backup per PostgreSQL . . . 55
Visualizza i backup e i cloni di PostgreSQL nella pagina Topologia . . . 56
Ripristina PostgreSQL . . . 57
Ripristina flusso di lavoro . . . 57
Ripristina e recupera un backup di risorse aggiunto manualmente . . . 58
Ripristina e recupera un backup del cluster rilevato automaticamente . . . 62
Ripristinare le risorse utilizzando i cmdlet di PowerShell . . . 64
Monitorare le operazioni di ripristino di PostgreSQL . . . 67
Clona i backup delle risorse PostgreSQL . . . 68

Flusso di lavoro di clonazione . . . 68
Clonare un backup PostgreSQL . . . 69
Monitorare le operazioni di clonazione di PostgreSQL . . . 72
Dividi un clone . . . 73
Elimina o dividi i cloni del cluster PostgreSQL dopo l'aggiornamento SnapCenter . . . 74

Proteggere PostgreSQL

Plug-in SnapCenter per PostgreSQL

Panoramica del plug-in SnapCenter per PostgreSQL

Il plug-in SnapCenter per cluster PostgreSQL è un componente lato host del software NetApp SnapCenter software che consente la gestione della protezione dei dati basata sulle applicazioni dei cluster PostgreSQL. Il plug-in per il cluster PostgreSQL automatizza il backup, il ripristino e la clonazione dei cluster PostgreSQL nel tuo ambiente SnapCenter .

SnapCenter supporta configurazioni PostgreSQL a cluster singolo e multi-cluster. È possibile utilizzare il plug-in per i cluster PostgreSQL sia in ambienti Linux che Windows. Negli ambienti Windows, PostgreSQL sarà supportato come risorsa manuale.

Una volta installato il plug-in per il cluster PostgreSQL, 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 replicazione del backup da disco a disco per la conformità agli standard.

Il plug-in SnapCenter per PostgreSQL supporta NFS e SAN su layout di archiviazione ONTAP e Azure NetApp File.

Sono supportati i layout di archiviazione virtuale VMDK, vVol e RDM.

Cosa puoi fare utilizzando il plug-in SnapCenter per PostgreSQL

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

- Aggiungere cluster.
- Creare backup.
- Ripristina dai backup.
- Backup clonati.
- Pianificare le operazioni di backup.
- Monitorare le operazioni di backup, ripristino e clonazione.
- Visualizza i report per le operazioni di backup, ripristino e clonazione.

Funzionalità del plug-in SnapCenter per PostgreSQL

SnapCenter si integra con l’applicazione plug-in e con le tecnologie NetApp sul sistema di storage. Per lavorare con il plug-in per PostgreSQL Cluster, è necessario utilizzare l’interfaccia utente grafica SnapCenter .

- **Interfaccia utente grafica unificata**

L'interfaccia SnapCenter garantisce standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia SnapCenter consente di completare operazioni di backup, ripristino e clonazione coerenti su tutti i plug-in, utilizzare report centralizzati, utilizzare viste dashboard immediate, impostare il controllo degli accessi basato sui ruoli (RBAC) e monitorare i processi su tutti i plug-in.

- **Amministrazione centrale automatizzata**

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

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

  SnapCenter utilizza la tecnologia snapshot NetApp con il plug-in per il cluster PostgreSQL per eseguire il backup delle risorse.

L'utilizzo del plug-in per PostgreSQL offre inoltre i seguenti vantaggi:

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

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

- Creazione di copie di risorse efficienti in termini di spazio e puntuali per test o estrazione dati utilizzando la tecnologia NetApp FlexClone

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

- Supporto per la funzionalità snapshot del gruppo di coerenza (CG) di ONTAP come parte della creazione di backup.
- Capacità di eseguire più backup contemporaneamente su più host di risorse

  In un'unica operazione, gli snapshot vengono consolidati quando le risorse in un singolo host condividono lo stesso volume.

- Possibilità di creare snapshot utilizzando comandi esterni.
- Supporto per Linux LVM sul file system XFS.

Tipi di archiviazione supportati dal plug-in SnapCenter per PostgreSQL

SnapCenter supporta un'ampia gamma di tipi di archiviazione sia su macchine fisiche che su macchine virtuali (VM). Prima di installare il plug-in SnapCenter per PostgreSQL, è necessario verificare il supporto per il tipo di archiviazione in uso.

Macchina	Tipo di archiviazione
Server fisico	• LUN connesse a FC • LUN connesse tramite iSCSI • Volumi connessi tramite NFS

Macchina	Tipo di archiviazione
VMware ESXi	• LUN RDM connesse tramite FC o iSCSI ESXi HBA. La scansione degli adattatori bus host (HBA) potrebbe richiedere molto tempo perché SnapCenter esegue la scansione di tutti gli adattatori bus host presenti nell'host. È possibile modificare il file **LinuxConfig.pm** che si trova in */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* per impostare il valore del parametro **SCSI_HOSTS_OPTIMIZED_RESCAN** su 1 per rieseguire la scansione solo degli HBA elencati in HBA_DRIVER_NAMES. • LUN iSCSI collegate direttamente al sistema guest dall'iniziatore iSCSI • VMDK su datastore NFS • VMDK su VMFS • Volumi NFS connessi direttamente al sistema guest • Datastore vVol sia su NFS che su SAN Il provisioning del datastore vVol può essere effettuato solo con ONTAP Tools per VMware vSphere.

Privilegi ONTAP minimi richiesti per il plug-in PostgreSQL

I privilegi ONTAP minimi richiesti variano a seconda dei plug-in SnapCenter utilizzati per la protezione dei dati.

- Comandi di accesso completo: privilegi minimi richiesti per ONTAP 9.12.1 e versioni successive
  - evento genera-autosupport-log
  - spettacolo di storia lavorativa
  - interruzione del lavoro
  - luna
  - lun crea
  - lun crea
  - lun crea
  - lun cancella
  - lun igroup aggiungi
  - lun igroup create
  - lun igroup elimina

- rinomina lun igroup
- rinomina lun igroup
- spettacolo di gruppo lun
- mappatura lun aggiungi-nodi-di-segnalazione
- creazione di mappatura lun
- eliminazione della mappatura LUN
- rimozione-nodi-di-segnalazione-mapping-lun
- spettacolo di mappatura lun
- lun modifica
- lun sposta-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- ridimensionamento lun
- serie lun
- spettacolo di lunedì
- aggiunta regola politica snapmirror
- modifica regola policy snapmirror
- regola di rimozione della policy di SnapMirror
- mostra politica di SnapMirror
- ripristino snapmirror
- spettacolo snapmirror
- snapmirror mostra-cronologia
- aggiornamento snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione di cloni di volume
- spettacolo di clonazione del volume
- inizio divisione clone volume
- volume clone divisione stop
- creazione del volume
- distruzione del volume
- creazione di clonazione di file di volume
- file di volume mostra-utilizzo-disco
- volume offline
- volume online

    - modifica del volume
    - creazione di volume qtree
    - eliminazione del volume qtree
    - modifica del volume qtree
    - volume qtree mostra
    - limitazione del volume
    - spettacolo di volume
    - creazione di snapshot del volume
    - eliminazione snapshot volume
    - modifica snapshot volume
    - modifica-scadenza-snaplock-istantanea-volume
    - rinomina snapshot volume
    - ripristino snapshot del volume
    - file di ripristino dello snapshot del volume
    - mostra snapshot del volume
    - smontare il volume
    - server virtuale cifs
    - vserver cifs share create
    - vserver cifs share delete
    - vserver cifs shadowcopy mostra
    - vserver cifs share show
    - spettacolo cifs del server virtuale
    - politica di esportazione del server virtuale
    - creazione di criteri di esportazione vserver
    - eliminazione della policy di esportazione del server virtuale
    - creazione regola policy di esportazione vserver
    - regola di esportazione-politica del vserver mostra
    - mostra politica di esportazione vserver
    - server virtuale iscsi
    - visualizzazione della connessione vserver iscsi
    - spettacolo vserver
- Comandi di sola lettura: privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
    - interfaccia di rete
    - mostra interfaccia di rete
    - server virtuale

Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per PostgreSQL

È possibile utilizzare un plug-in SnapCenter con la tecnologia ONTAP SnapMirror per creare copie mirror di set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replicazione del backup da disco a disco 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 a SnapMirror e SnapVault dopo aver completato l'operazione Snapshot. Gli aggiornamenti SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter ; non creare una pianificazione ONTAP separata.

Se si SnapCenter da un prodotto NetApp SnapManager e si è soddisfatti delle relazioni di protezione dei dati configurate, è possibile saltare questa sezione.

Una relazione di protezione dei dati replica i dati dall'archivio primario (il volume di origine) all'archivio secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui si fa riferimento sul volume di origine al volume di destinazione.

SnapCenter non supporta relazioni a cascata tra volumi SnapMirror e SnapVault (**Primario** > **Mirror** > **Vault**). Dovresti usare relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per i dettagli sulle relazioni SnapMirror flessibili in base alla versione e su come impostarle, vedere "Documentazione ONTAP" .

Strategia di backup per PostgreSQL

Definire una strategia di backup per PostgreSQL

Definire una strategia di backup prima di creare i processi di backup ti aiuta a disporre dei backup necessari per ripristinare o clonare correttamente le tue risorse. Il contratto di servizio (SLA), l'obiettivo del tempo di ripristino (RTO) e l'obiettivo del punto di ripristino (RPO) determinano in larga misura la strategia di backup.

Informazioni su questo compito

Un SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. L'RTO è il tempo entro il quale un processo aziendale deve essere ripristinato dopo un'interruzione del servizio. RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di protezione dei dati.

Passi

1. Determina quando eseguire il backup delle tue risorse.
2. Decidi quanti processi di backup ti servono.
3. Decidi come denominare i tuoi backup.
4. Decidi se vuoi creare una policy basata sulla copia di snapshot per eseguire il backup di snapshot coerenti con l'applicazione del cluster.

5. Decidi se vuoi utilizzare la tecnologia NetApp SnapMirror per la replica o la tecnologia NetApp SnapVault per la conservazione a lungo termine.
6. Determinare il periodo di conservazione per gli snapshot sul sistema di archiviazione di origine e sulla destinazione SnapMirror .
7. Stabilisci se desideri eseguire dei comandi prima o dopo l'operazione di backup e fornisci un prescript o un postscript.

Rilevamento automatico delle risorse sull'host Linux

Le risorse sono cluster e istanze PostgreSQL sull'host Linux gestiti da SnapCenter. Dopo aver installato il plug-in SnapCenter per PostgreSQL, i cluster PostgreSQL di tutte le istanze su quell'host Linux vengono automaticamente rilevati e visualizzati nella pagina Risorse.

Tipo di backup supportati

Tipo di backup specifica il tipo di backup che si desidera creare. SnapCenter supporta il tipo di backup basato sulla copia snapshot per i cluster PostgreSQL.

Backup basato su copia snapshot

I backup basati su copie snapshot sfruttano la tecnologia snapshot NetApp per creare copie online di sola lettura dei volumi su cui risiedono i cluster PostgreSQL.

Come il plug-in SnapCenter per PostgreSQL utilizza gli snapshot del gruppo di coerenza

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

È anche possibile specificare il tempo di attesa affinché il controller di archiviazione raggruppi in modo coerente gli snapshot. Le opzioni di tempo di attesa disponibili sono **Urgente**, **Medio** e **Rilassato**. È anche possibile abilitare o disabilitare la sincronizzazione Write Anywhere File Layout (WAFL) durante l'operazione di snapshot di gruppo coerente. La sincronizzazione WAFL migliora le prestazioni di uno snapshot del gruppo di coerenza.

Come SnapCenter gestisce la manutenzione dei backup dei dati

SnapCenter gestisce la manutenzione dei backup dei dati a livello di sistema di archiviazione e di file system.

Gli snapshot sullo storage primario o secondario e le voci corrispondenti nel catalogo PostgreSQL vengono eliminati in base alle impostazioni di conservazione.

Considerazioni per la determinazione delle pianificazioni di backup per PostgreSQL

Il fattore più critico nella determinazione di una pianificazione di backup è la velocità di modifica della risorsa. Potresti eseguire il backup di una risorsa molto utilizzata ogni ora, mentre potresti eseguire il backup di una risorsa raramente utilizzata una volta al giorno.

Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo contratto di servizio (SLA) e il tuo obiettivo del punto di ripristino (RPO).

Le pianificazioni dei backup sono composte da due parti, come segue:

- Frequenza di backup (con quale frequenza devono essere eseguiti i backup)

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

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

  Le pianificazioni di backup fanno parte della configurazione di una risorsa o di un gruppo 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 in modo che il backup venga eseguito ogni giovedì alle 22:00.

Numero di processi di backup necessari per PostgreSQL

I fattori che determinano il numero di processi di backup necessari includono la dimensione della risorsa, il numero di volumi utilizzati, la frequenza di modifica della risorsa e il contratto di servizio (SLA).

Convenzioni di denominazione del backup per i cluster Plug-in per PostgreSQL

È possibile utilizzare la convenzione di denominazione predefinita di Snapshot oppure una convenzione di denominazione personalizzata. La convenzione di denominazione predefinita per i backup aggiunge un timestamp ai nomi degli snapshot che consente di identificare quando sono state create le copie.

Lo Snapshot utilizza la seguente convenzione di denominazione predefinita:

```
resourcegroupname_hostname_timestamp
```

Dovresti assegnare nomi logici ai gruppi di risorse di backup, come nell'esempio seguente:

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

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

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

In alternativa, è possibile specificare il formato del nome dello snapshot durante la protezione delle risorse o dei gruppi di risorse selezionando **Usa formato nome personalizzato per la copia dello snapshot**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, il suffisso timestamp viene aggiunto al nome dello Snapshot.

Strategia di ripristino e recupero per PostgreSQL

Definire una strategia di ripristino e recupero per le risorse PostgreSQL

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

È supportato solo il ripristino manuale del cluster.

Passi

1. Determinare le strategie di ripristino supportate per le risorse PostgreSQL aggiunte manualmente
2. Determinare le strategie di ripristino supportate per i cluster PostgreSQL rilevati automaticamente
3. Decidi il tipo di operazioni di ripristino che vuoi eseguire.

Tipi di strategie di ripristino supportate per le risorse PostgreSQL aggiunte manualmente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter.

Non è possibile recuperare le risorse PostgreSQL aggiunte manualmente.

Ripristino completo delle risorse

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

Se la risorsa contiene volumi o qtree, gli snapshot acquisiti dopo lo snapshot selezionato per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata.

NOTA: il plug-in per PostgreSQL crea un backup_label e una tablespace_map nella cartella */<OS_temp_folder>/postgresql_sc_recovery*<Restore_JobId>/_ per facilitare il ripristino manuale.

Tipo di strategia di ripristino supportata per PostgreSQL rilevato automaticamente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter.

Il ripristino completo delle risorse è la strategia di ripristino supportata per i cluster PostgreSQL rilevati automaticamente. Ripristina tutti i volumi, i qtree e i LUN di una risorsa.

Tipi di operazioni di ripristino per PostgreSQL rilevato automaticamente

Il plug-in SnapCenter per PostgreSQL supporta Single File SnapRestore e i tipi di ripristino connect-and-copy per i cluster PostgreSQL rilevati automaticamente.

Single File SnapRestore viene eseguito negli ambienti NFS per i seguenti scenari:

- Se è selezionata solo l'opzione **Completa Risorsa**
- Quando il backup selezionato proviene da una posizione secondaria SnapMirror o SnapVault e l'opzione

Risorsa completa è selezionata

Single File SnapRestore viene eseguito in ambienti SAN per i seguenti scenari:

- Se è selezionata solo l'opzione **Completa Risorsa**
- Quando il backup viene selezionato da una posizione secondaria SnapMirror o SnapVault e l'opzione **Risorsa completa** è selezionata

Tipi di operazioni di ripristino supportate per i cluster PostgreSQL

SnapCenter consente di eseguire diversi tipi di operazioni di ripristino per i cluster PostgreSQL.

- Ripristina il cluster fino allo stato più recente
- Ripristina il cluster fino a un punto specifico nel tempo

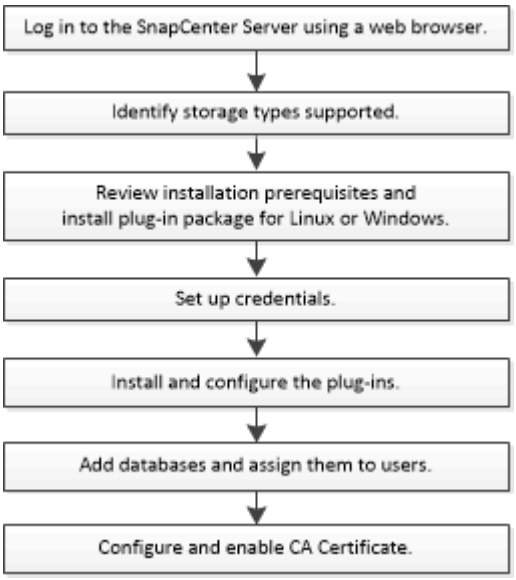
  È necessario specificare la data e l'ora del ripristino.

SnapCenter fornisce anche l'opzione Nessun ripristino per i cluster PostgreSQL.

Prepararsi all'installazione del plug-in SnapCenter per PostgreSQL

Flusso di lavoro di installazione del plug-in SnapCenter per PostgreSQL

Se si desidera proteggere i cluster PostgreSQL, è necessario installare e configurare il plug-in SnapCenter per PostgreSQL.



Prerequisiti per aggiungere host e installare il plug-in SnapCenter per PostgreSQL

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario soddisfare tutti i requisiti. Il plug-in SnapCenter per PostgreSQL è disponibile sia negli ambienti Windows che Linux.

- Devi aver installato Java 11 sul tuo host.

  IBM Java non è supportato su host Windows e Linux.

- Per Windows, il servizio Creator del plug-in dovrebbe essere eseguito utilizzando l'utente Windows "LocalSystem", che è il comportamento predefinito quando il plug-in per PostgreSQL è installato come amministratore di dominio.
- 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 di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host. Il plug-in SnapCenter per Microsoft Windows verrà distribuito per impostazione predefinita con il plug-in PostgreSQL sugli host Windows.
- SnapCenter Server dovrebbe avere accesso alla porta 8145 o personalizzata dell'host Plug-in per PostgreSQL.

Host Windows

- È necessario disporre di un utente di dominio con privilegi di amministratore locale e autorizzazioni di accesso locale sull'host remoto.
- Durante l'installazione del plug-in per PostgreSQL su un host Windows, il plug-in SnapCenter per Microsoft Windows viene installato automaticamente.
- È necessario aver abilitato la connessione SSH basata su password per l'utente root o non root.
- Devi aver installato Java 11 sul tuo host Windows.

  "Scarica JAVA per tutti i sistemi operativi"

  "Strumento matrice di interoperabilità NetApp"

Host Linux

- È necessario aver abilitato la connessione SSH basata su password per l'utente root o non root.
- Devi aver installato Java 11 sul tuo host Linux.

  "Scarica JAVA per tutti i sistemi operativi"

  "Strumento matrice di interoperabilità NetApp"

- Per i cluster PostgreSQL in esecuzione su un host Linux, durante l'installazione del plug-in per PostgreSQL, viene installato automaticamente il plug-in SnapCenter per UNIX.
- Dovresti avere **bash** come shell predefinita per l'installazione del plug-in.

Comandi supplementari

Per eseguire un comando supplementare sul plug-in SnapCenter per PostgreSQL, è necessario includerlo nel file *allowed_commands.config*.

- Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Per consentire comandi supplementari sull'host del plug-in, aprire il file *allowed_commands.config* in un editor.

Immettere ogni comando su una riga separata e i comandi non fanno distinzione tra maiuscole e minuscole. Assicurarsi di specificare il percorso completo e di racchiuderlo tra virgolette (") se contiene spazi.

Per esempio:

comando: mount comando: umount comando: "C:\Programmi\ NetApp\SnapCreator commands\sdcli.exe" comando: myscript.bat

Se il file *allowed_commands.config* non è presente, l'esecuzione dei comandi o degli script verrà bloccata e il flusso di lavoro non riuscirà con il seguente errore:

"[/mnt/mount -a] esecuzione non consentita. Autorizza aggiungendo il comando nel file %s sull'host del plugin."

Se il comando o lo script non è presente in *allowed_commands.config*, l'esecuzione del comando o dello script verrà bloccata e il flusso di lavoro non riuscirà con il seguente errore:

"[/mnt/mount -a] esecuzione non consentita. Autorizza aggiungendo il comando nel file %s sull'host del plugin."

Non dovresti usare un carattere jolly (*) per consentire tutti i comandi.

Configurare i privilegi sudo per gli utenti non root per l'host Linux

SnapCenter consente a un utente non root di installare il pacchetto plug-in SnapCenter per Linux e di avviare il processo di plug-in. I processi del plug-in verranno eseguiti come utente non root effettivo. È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso a diversi percorsi.

Cosa ti servirà

- Sudo versione 1.8.7 o successiva.
- Se l'umask è 0027, assicurarsi che la cartella java e tutti i file al suo interno abbiano l'autorizzazione 555. In caso contrario l'installazione del plug-in potrebbe non riuscire.
- Per l'utente non root, assicurarsi che il nome dell'utente non root e il nome del gruppo dell'utente siano gli stessi.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione dei messaggi: MAC hmac-sha2-256 e MAC hmac-sha2-512.

  Riavviare il servizio sshd dopo aver aggiornato il file di configurazione.

  Esempio:

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

Informazioni su questo compito

È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso ai seguenti percorsi:

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /posizione_personalizzata/ NetApp/snapcenter/spl/bin/spl

Passi

1. Accedi all'host Linux su cui desideri installare il pacchetto plug-in SnapCenter per Linux.
2. Aggiungere le seguenti righe al file /etc/sudoers utilizzando l'utilità Linux visudo.

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

LINUX_USER è il nome dell'utente non root che hai creato.

È possibile ottenere il valore *checksum_value* dal file **sc_unix_plugins_checksum.txt**, che si trova in:

- _C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _ se SnapCenter Server è installato sull'host Windows.
- _/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ se SnapCenter Server è installato sull'host Linux.

L'esempio deve essere utilizzato solo come riferimento per la creazione dei propri dati.

Requisiti host per installare il pacchetto plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario acquisire familiarità con alcuni requisiti di base di spazio e dimensioni del sistema host.

Articolo	Requisiti
Sistemi operativi	Microsoft Windows Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .
RAM minima per il plug-in SnapCenter sull'host	1 GB
Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host	5 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati.

Articolo	Requisiti
Pacchetti software richiesti	• Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive) • PowerShell Core 7.4.2 Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce nei sistemi legacy che non dispongono di connettività Internet."

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

Prima di installare il pacchetto di plug-in SnapCenter per Linux, è necessario acquisire familiarità con alcuni requisiti di base relativi allo spazio e alle dimensioni del sistema host.

Articolo	Requisiti
Sistemi operativi	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .
RAM minima per il plug-in SnapCenter sull'host	1 GB
Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host	2 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati.

Articolo	Requisiti
Pacchetti software richiesti	Java 11 Oracle Java e OpenJDK Se hai aggiornato JAVA alla versione più recente, devi assicurarti che l'opzione JAVA_HOME situata in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto. Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .

Imposta le credenziali per il plug-in SnapCenter per PostgreSQL

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 eseguire operazioni di protezione dei dati su cluster o file system Windows.

Informazioni su questo compito

- Host Linux

  È necessario impostare le credenziali per installare i plug-in sugli host Linux.

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

  Procedura consigliata: Sebbene sia consentito creare credenziali per Linux dopo aver distribuito gli host e installato i plug-in, la procedura consigliata è quella di creare le credenziali dopo aver aggiunto le SVM, prima di distribuire gli host e installare i 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 al nome utente almeno i privilegi di gruppo di risorse e di backup.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Credenziali**.
3. Fare clic su **Nuovo**.
4. Nella pagina Credenziali, specificare le informazioni richieste per la configurazione delle credenziali:

Per questo campo…	Fai questo…
Nome della credenziale	Inserisci un nome per le credenziali.
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 un membro del gruppo di amministratori sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo Nome utente sono: ◦ *NetBIOS\NomeUtente* ◦ *FQDN dominio\Nome utente* • Amministratore locale (solo per gruppi di lavoro) Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale predefinito sul sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host. Il formato valido per il campo Nome utente è: *UserName* Non utilizzare virgolette doppie (") o apici inversi (`) nelle password. Non dovresti usare insieme i simboli minore (<) e punto esclamativo (!) nelle password. Ad esempio, lessthan<!10, lessthan10<!, backtick`12.
Password	Inserisci la password utilizzata per l'autenticazione.
Modalità di autenticazione	Seleziona la modalità di autenticazione che desideri 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**.

Dopo aver completato la configurazione delle credenziali, potresti voler assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina Utente e accesso.

Configurare gMSA su Windows Server 2016 o versioni successive

Windows Server 2016 o versioni successive consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatizzata delle password degli account di servizio da un account di dominio gestito.

Prima di iniziare

- Dovresti avere un controller di dominio Windows Server 2016 o versione successiva.
- Dovresti avere un host Windows Server 2016 o versione successiva, che sia membro del dominio.

Passi

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

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

   Per esempio,

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

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

   Per fare ciò, 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. Riavvia il tuo host.

b. Installa gMSA sul tuo host eseguendo il seguente comando dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifica il tuo 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 .

   SnapCenter Server 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.

Installa il plug-in SnapCenter per PostgreSQL

Aggiungere host e installare pacchetti plug-in su host remoti

È necessario utilizzare la pagina Aggiungi host SnapCenter per aggiungere host e quindi installare i pacchetti plug-in. I plug-in vengono installati automaticamente sugli host remoti. È possibile aggiungere l'host e installare pacchetti plug-in per un singolo host.

Prima di iniziare

- Se il sistema operativo dell'host del server SnapCenter è Windows 2019 e il sistema operativo dell'host del plug-in è Windows 2022, è necessario eseguire le seguenti operazioni:
  - Aggiorna a Windows Server 2019 (build del sistema operativo 17763.5936) o versione successiva
  - Aggiorna a Windows Server 2022 (build del sistema operativo 20348.2402) o versione successiva
- Devi essere un utente a cui è assegnato un ruolo che dispone delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore 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 di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host.

- È necessario 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 l'account del servizio gestito del gruppo su Windows Server 2016 o versioni successive per PostgreSQL"

Informazioni su questo compito

- Non è possibile aggiungere uno SnapCenter Server come host plug-in a un altro SnapCenter Server.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata in alto.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, eseguire le seguenti azioni:

Per questo campo…	Fai questo…
Tipo di host	Seleziona il tipo di host: • Finestre • Linux Il plug-in per PostgreSQL viene installato sull'host client PostgreSQL, che può trovarsi sia su un sistema Windows che su un sistema Linux.
Nome host	Immettere il nome host della comunicazione. Immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla corretta configurazione del DNS. Pertanto, la prassi migliore è quella di immettere il nome di dominio completo (FQDN).

Per questo campo…	Fai questo…
Credenziali	Seleziona il nome delle credenziali che hai creato oppure creane di nuove. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per maggiori dettagli, consultare le informazioni sulla creazione delle credenziali. Puoi visualizzare i dettagli sulle credenziali posizionando il cursore sul nome della credenziale che hai fornito. La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.

5. Nella sezione Seleziona plug-in da installare, seleziona i plug-in da installare.

   Quando si utilizza l'API REST per installare il plug-in per PostgreSQL, è necessario passare la versione come 3.0. Ad esempio, PostgreSQL:3.0

6. (Facoltativo) Fare clic su **Altre opzioni**.

Per questo campo…	Fai questo…
Porta	Mantenere il numero di porta predefinito oppure specificare il numero di porta. Il numero di porta predefinito è 8145. Se SnapCenter Server è stato installato su una porta personalizzata, tale numero di porta verrà visualizzato come porta predefinita. Se hai installato manualmente i plug-in e hai specificato una porta personalizzata, devi specificare la stessa porta. In caso contrario, l'operazione fallisce.
Percorso di installazione	Il plug-in per PostgreSQL viene installato sull'host client PostgreSQL, che può trovarsi sia su un sistema Windows che su un sistema Linux. • Per il pacchetto di plug-in SnapCenter per Windows, il percorso predefinito è C:\Programmi\ NetApp\ SnapCenter. Facoltativamente, puoi personalizzare il percorso. • Per il pacchetto di plug-in SnapCenter per Linux, il percorso predefinito è /opt/ NetApp/snapcenter. Facoltativamente, puoi personalizzare il percorso.

Per questo campo…	Fai questo…
Salta i controlli pre-installazione	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.
Aggiungi tutti gli host nel cluster	Selezionare questa casella di controllo per aggiungere tutti i nodi del cluster.
Utilizzare l'account di servizio gestito del 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 del gruppo (gMSA) per eseguire i servizi plug-in. Fornire il nome gMSA nel seguente formato: domainName\accountName$. gMSA verrà utilizzato come account di accesso al servizio solo per il plug-in SnapCenter per il servizio Windows.

7. Fare clic su **Invia**.

   Se non hai selezionato la casella di controllo "Ignora controlli preliminari", l'host verrà convalidato per verificare se 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) vengono convalidati rispetto ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati.

   Se l'errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config che si trova in C:\Programmi\ 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 **Conferma e invia**.

   In una configurazione cluster, è necessario verificare l'impronta digitale di ciascun nodo 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.
   - Per il plug-in di Windows, i registri di installazione e aggiornamento si trovano in: *C:\Windows\ SnapCenter plugin\Install*<JOBID>_
   - Per il plug-in Linux, i registri di installazione si trovano in:

/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log_ e i registri di aggiornamento si trovano in: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log_

Installa 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 di PowerShell.

Prima di iniziare

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 plug-in.

Passi

1. Avvia 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, puoi anche fare riferimento a "Guida di riferimento ai 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. Inserisci le tue credenziali per l'installazione remota.

Installa il plug-in SnapCenter per PostgreSQL su host Linux utilizzando l'interfaccia della riga di comando

È necessario installare il plug-in SnapCenter per il cluster PostgreSQL utilizzando l'interfaccia utente (UI) SnapCenter . Se l'ambiente non consente l'installazione remota del plug-in dall'interfaccia utente SnapCenter , è possibile installare il plug-in per il cluster PostgreSQL in modalità console o in modalità silenziosa utilizzando l'interfaccia della riga di comando (CLI).

Prima di iniziare

- Dovresti installare il plug-in per il cluster PostgreSQL su ciascun host Linux in cui risiede il client PostgreSQL.
- L'host Linux su cui si installa il plug-in SnapCenter per il cluster PostgreSQL deve soddisfare i requisiti software, cluster e sistema operativo dipendenti.

  Lo strumento Interoperability Matrix (IMT) contiene le informazioni più recenti sulle configurazioni supportate.

  "Strumento matrice di interoperabilità NetApp"

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

Passi

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 PostgreSQL.

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

2. Dal prompt dei comandi, vai alla directory in cui hai copiato il file di installazione.
3. Installa 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 di 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 plug-in SnapCenter per Linux.
   - DINSTALL_LOG_NAME specifica il nome del file di registro.

   ```
   /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 /<directory di installazione>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties, quindi aggiungere il parametro PLUGINS_ENABLED = PostgreSQL:3.0.
5. Aggiungere l'host al server SnapCenter utilizzando il cmdlet Add-Smhost e i parametri richiesti.

   Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo *Get-Help nome_comando*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

Monitorare lo stato di installazione del plug-in per PostgreSQL

È possibile monitorare l'avanzamento dell'installazione del pacchetto plug-in SnapCenter tramite la pagina Lavori. Potrebbe essere opportuno controllare l'avanzamento dell'installazione per stabilire quando è completa o se si è verificato un problema.

Informazioni su questo compito

Le seguenti icone compaiono nella pagina Lavori e indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
-

Completato con avvisi o non è stato possibile avviarlo a causa di avvisi

- In coda

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, per filtrare l'elenco in modo che vengano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filtro**.
   b. Facoltativo: specificare la data di inizio e di fine.
   c. Dal menu a discesa Tipo, seleziona **Installazione plug-in**.
   d. Dal menu a discesa Stato, selezionare lo stato dell'installazione.
   e. Fare clic su **Applica**.
4. Selezionare il lavoro di installazione e fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

Configurare il certificato CA

Genera 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 sarà associata una chiave privata.

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

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

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

Se possiedi il certificato CA per il tuo dominio (*.domain.company.com) o per il tuo sistema (machine1.domain.company.com), puoi saltare la generazione del file CSR del certificato CA. È possibile distribuire il certificato CA esistente con SnapCenter.

Per le configurazioni cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere menzionati nel certificato CA. È possibile aggiornare il certificato compilando il campo Subject Alternative Name (SAN) prima di ottenere il certificato. Per un certificato con caratteri jolly (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

Importa certificati CA

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

Passi

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

In questa finestra della procedura guidata…	Procedi come segue…
Importa chiave privata	Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**.
Formato 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 della procedura guidata di importazione del certificato	Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione.

> Il certificato di importazione deve essere incluso nella chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

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

Ottieni l'impronta digitale del certificato CA

L'impronta digitale di un certificato è una stringa esadecimale che identifica un certificato. L'impronta digitale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione digitale.

Passi

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. Scorri l'elenco dei campi e clicca su **Impronta digitale**.
   d. Copia i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se l'impronta digitale 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: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il seguente comando per elencare l'identificazione personale del certificato installato e

identificare il certificato installato di recente tramite il nome dell'oggetto.

Get-ChildItem -Percorso Cert:\LocalMachine\My

b. Copia l'impronta digitale.

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

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

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

Passi

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>
   ```

   Per esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in host di
   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"
   ```

   Per 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 SnapCenter PostgreSQL Plug-ins sull'host Linux

È necessario gestire la password del keystore dei plug-in e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file 'keystore.jks', che si trova in */opt/ NetApp/snapcenter/scc/etc* sia come archivio

attendibile che come archivio chiavi.

Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso

Passi

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

   È il valore corrispondente alla chiave 'KEYSTORE_PASS'.

2. Cambia la password del keystore:

   ```
    keytool -storepasswd -keystore keystore.jks
   . Modificare la password per tutti gli alias delle voci di chiave
   privata 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 e per tutte le password alias associate alla chiave privata devono essere le stesse.

Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

Passi

1. Passare alla cartella contenente il keystore del plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

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

4. Aggiungi un certificato radice o intermedio:

   ```
    keytool -import -trustcacerts -alias myRootCA -file
   /root/USERTrustRSA_Root.cer -keystore keystore.jks
   . Riavviare il servizio dopo aver configurato i certificati radice o
   intermedi per collegare trust-store.
   ```

> Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

Passi

1. Passare alla cartella contenente il keystore del plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

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

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

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

5. Elenca 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 con la password del keystore.

   La password predefinita del keystore del plug-in 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 in un nome
   semplice:
   ```

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

   Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

8. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

Configurare l'elenco di revoche dei certificati (CRL) per i plug-in

Informazioni su questo compito

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

Passi

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

   È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

Configurare il certificato CA per il servizio plug-in SnapCenter PostgreSQL sull'host Windows

È necessario gestire la password del keystore dei plug-in e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file *keystore.jks*, che si trova in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* sia come archivio attendibile che come archivio chiavi.

Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso

Passi

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

   È il valore corrispondente alla chiave *KEYSTORE_PASS*.

2. Cambia la password del keystore:

   keytool -storepasswd -keystore keystore.jks

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

   C:\Programmi\Java\<versione_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks

3. Modificare la password per tutti gli alias delle voci di chiave privata 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 e per tutte le password alias associate alla chiave privata devono essere le stesse.

Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

Passi

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*

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

   keytool -list -v -keystore keystore.jks

4. Aggiungi un certificato radice o intermedio:

   keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Riavviare il servizio dopo aver configurato i certificati radice o intermedi per collegare trust-store.

   Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

Passi

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Individuare il file *keystore.jks*.
3. Elenca i certificati aggiunti nel keystore:

   keytool -list -v -keystore keystore.jks

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

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

5. Elenca 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 con la password del keystore.

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

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

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

   Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

9. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

Configurare l'elenco di revoche dei certificati (CRL) per i plug-in SnapCenter

Informazioni su questo compito

- Per scaricare l'ultimo file CRL per il certificato CA correlato, vedere "Come aggiornare il file dell'elenco di revoche dei certificati in SnapCenter CA Certificate" .

- I plug-in SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in SnapCenter è *'C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

Passi

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

   I certificati in arrivo saranno verificati rispetto a ciascun CRL.

Abilita i certificati CA per i plug-in

È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

Prima di iniziare

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *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, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.
4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

Dopo aver finito

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- *  * indica che il certificato CA non è abilitato né assegnato all'host del plug-in.
- *  * indica che il certificato CA è stato convalidato correttamente.
- *  * indica che il certificato CA non è stato convalidato.
- *  * indica che non è stato possibile recuperare le informazioni di connessione.

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

Prepararsi alla protezione dei dati

Prerequisiti per l'utilizzo del plug-in SnapCenter per PostgreSQL

Prima di utilizzare il plug-in SnapCenter per PostgreSQL, l'amministratore SnapCenter deve installare e configurare SnapCenter Server ed eseguire le attività preliminari.

- Installa e configura SnapCenter Server.
- Accedi a SnapCenter Server.
- Configurare l'ambiente SnapCenter aggiungendo connessioni al sistema di archiviazione e creando credenziali, se applicabile.
- Installa Java 11 sul tuo host Linux o Windows.

  È necessario impostare il percorso Java nella variabile del percorso ambientale della macchina host.

- Se desideri la replica del backup, imposta SnapMirror e SnapVault.

Come vengono utilizzate le risorse, i gruppi di risorse e le policy per proteggere PostgreSQL

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.

- Le risorse sono in genere cluster PostgreSQL di cui si esegue il backup o la clonazione con SnapCenter.
- Un gruppo di risorse SnapCenter è una raccolta 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 anche possibile eseguire backup pianificati per singole risorse e gruppi di risorse.

- Le policy 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 una o più policy per quel gruppo. È anche possibile selezionare un criterio quando si esegue un backup su richiesta per una singola risorsa.

Pensa a un gruppo di risorse come a qualcosa che definisce cosa vuoi proteggere e quando vuoi proteggerlo in termini di giorno e ora. Pensa a una polizza come a qualcosa che definisce il modo in cui vuoi proteggerla. Ad esempio, se si esegue il backup di tutti i cluster, è possibile creare un gruppo di risorse che includa tutti i cluster nell'host. È quindi possibile associare due policy al gruppo di risorse: una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e si associano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup completo ogni giorno.

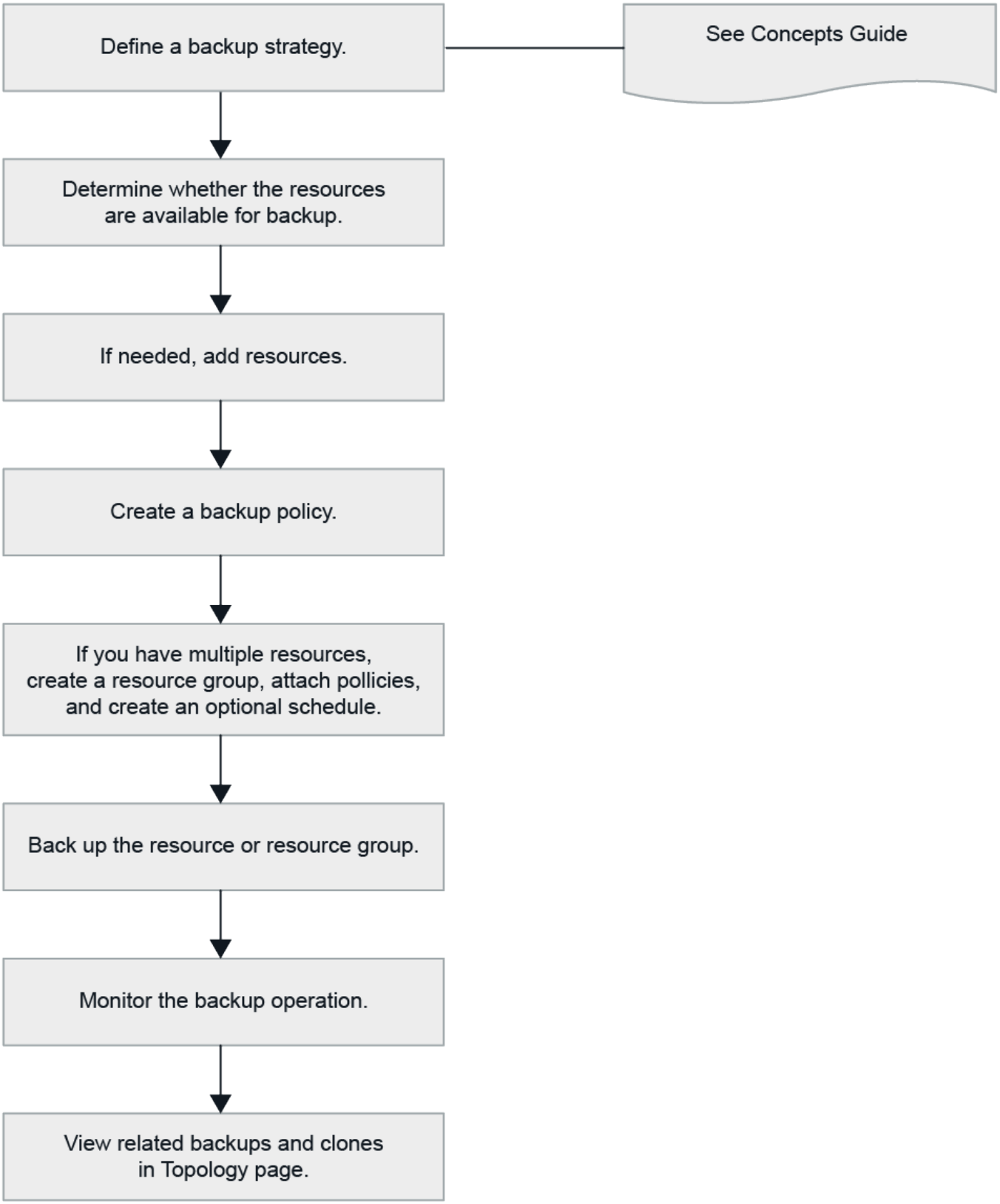
Eseguire il backup delle risorse PostgreSQL

Eseguire il backup delle risorse PostgreSQL

È possibile creare un backup di una risorsa (cluster) o di un gruppo di risorse. Il flusso di lavoro del backup include la pianificazione, l'identificazione dei cluster per il backup, la

gestione delle policy di backup, la creazione di gruppi di risorse e l'associazione 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 anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono ulteriori informazioni sui cmdlet di PowerShell. "Guida di riferimento ai cmdlet del software SnapCenter" .

Scopri automaticamente i cluster

Le risorse sono cluster PostgreSQL sull'host Linux gestiti da SnapCenter. È possibile aggiungere le risorse ai gruppi di risorse per eseguire operazioni di protezione dei dati dopo aver individuato i cluster PostgreSQL disponibili.

Prima di iniziare

- È necessario aver già completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host e la configurazione delle connessioni del sistema di archiviazione.
- Il plug-in SnapCenter per PostgreSQL non supporta il rilevamento automatico delle risorse residenti negli ambienti virtuali RDM/VMDK.

Informazioni su questo compito

- Dopo aver installato il plug-in, tutti i cluster presenti sull'host Linux vengono automaticamente rilevati e visualizzati nella pagina Risorse.
- Solo i cluster vengono rilevati automaticamente.

Le risorse rilevate automaticamente non possono essere modificate o eliminate.

Passi

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

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

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

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

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

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

Aggiungere manualmente le risorse all'host del plug-in

Il rilevamento automatico non è supportato sull'host Windows. È necessario aggiungere manualmente le risorse del cluster Postgresql.

Prima di iniziare

- È necessario aver completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host e la configurazione delle connessioni al sistema di archiviazione.

Informazioni su questo compito

Il rilevamento automatico non è supportato per le seguenti configurazioni:

- Layout RDM e VMDK

Passi

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

Per questo campo…	Fai questo…
Nome	Specificare il nome del cluster.
Nome host	Inserisci il nome host.
Tipo	Seleziona cluster.
Esempio	Specificare il nome dell'istanza, che è l'istanza padre del cluster.
Credenziali	Seleziona le credenziali o aggiungi informazioni per le credenziali. Questo è facoltativo.

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

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

5. Facoltativo: nella pagina Impostazioni risorse, per le risorse sull'host Windows, immettere coppie chiave-valore personalizzate per il plug-in PostgreSQL
6. Rivedi il riepilogo e poi clicca su **Fine**.

   I cluster vengono visualizzati insieme a informazioni quali il nome host, i gruppi di risorse e le policy associate e lo stato generale

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

"Aggiungi un utente o un gruppo e assegna ruoli e risorse"

Dopo aver finito

- Dopo aver aggiunto i cluster, è possibile modificare i dettagli del cluster PostgreSQL.
- Le risorse migrate (tablespace e cluster) da SnapCenter 5.0 saranno contrassegnate come tipo di cluster PostgreSQL in SnapCenter 6.0.
- Quando si modificano le risorse aggiunte manualmente e migrate da SnapCenter 5.0 o versioni precedenti, procedere come segue nella pagina **Impostazioni risorse** per le coppie chiave-valore personalizzate:
  - Specificare il termine "PORTA" nel campo **Nome**.
  - Specificare il numero di porta nel campo **Valore**.

Creare policy di backup per PostgreSQL

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

Prima di iniziare

- Devi aver definito la tua strategia di backup.

  Per maggiori dettagli, vedere le informazioni sulla definizione di una strategia di protezione dei dati per i cluster PostgreSQL.

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

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

Informazioni su questo compito

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **Nuovo**.
4. Nella pagina Nome, immettere il nome e i dettagli della policy.

5. Nella pagina Tipo di policy, procedere come segue:
   a. Seleziona il tipo di archiviazione.
   b. Nella sezione **Impostazioni di backup personalizzate**, specificare eventuali impostazioni di backup specifiche che devono essere trasmesse al plug-in in formato chiave-valore.

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

6. Nella pagina Backup e replica, eseguire le seguenti azioni:
   a. Specificare la frequenza di programmazione selezionando **Su richiesta**, **Ogni ora**, **Giornaliera**, **Settimanale** o **Mensile**.

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

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

   a. Nella sezione Impostazioni snapshot, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina **Tipo di backup**:

Se lo desidera…	**Poi…**
Conserva un certo numero di snapshot	Seleziona **Copie da conservare**, quindi specifica il numero di snapshot che desideri conservare. Se il numero di Snapshot supera il numero specificato, gli Snapshot vengono eliminati partendo dalle copie più vecchie. Se si prevede di abilitare la replica SnapVault , è necessario impostare il conteggio di conservazione su 2 o su un valore superiore. Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è lo Snapshot di riferimento per la relazione SnapVault finché uno Snapshot più recente non viene replicato sulla destinazione. Il valore massimo di ritenzione è 1018. I backup non riusciranno se la conservazione è impostata su un valore superiore a quello supportato dalla versione ONTAP .

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

7. Selezionare un'etichetta di criterio.

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

8. Nella sezione Seleziona opzioni di replicazione secondaria, seleziona una o entrambe le seguenti opzioni di replicazione secondaria:

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

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

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

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

Crea gruppi di risorse e allega criteri

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

Informazioni su questo compito

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot SnapLock Vault come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.

2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:

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

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

   Ciò aiuta a filtrare le informazioni sullo schermo.

5. Seleziona le risorse dalla sezione **Risorse disponibili**, quindi fai clic sulla freccia destra per spostarle nella sezione **Risorse selezionate**.
6. Nella pagina Impostazioni applicazione, procedere come segue:

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

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

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

+ 

a. Fare clic sulla freccia **Script** e immettere i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce. È anche possibile immettere i comandi pre da eseguire prima di uscire in caso di errore.

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

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

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

Le coppie chiave-valore personalizzate sono supportate per i sistemi plug-in Linux PostgreSQL e non sono supportate per i cluster PostgreSQL registrati come plug-in Windows centralizzato.

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

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

7. Nella pagina Criteri, procedere come segue:

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

Puoi anche creare una policy cliccando * + *.

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

b.

Nella colonna Configura pianificazioni, fare clic su *  * per la policy che vuoi configurare.

c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi fare clic su **OK**.

Dove policy_name è il nome della policy selezionata.

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

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

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

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

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

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

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

Prima di iniziare

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

Informazioni su questo compito

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

Passi

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

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

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

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

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

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

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

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

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

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

5. Selezionare le risorse ASA r2 dalla sezione Risorse disponibili e spostarle nella sezione Risorse selezionate.
6. Nella pagina Impostazioni applicazione, seleziona l'opzione di backup.
7. Nella pagina Criteri, procedere come segue:

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

Puoi anche creare una policy cliccando + .

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

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

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

Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

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

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

a. Selezionare il tipo di criterio di replica.

La politica di replica sincrona non è supportata.

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

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

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

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

1. Nella pagina Verifica, procedere come segue:

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

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

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

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

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

   e. Fare clic su **OK**.

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

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

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

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

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

Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per PostgreSQL

È necessario creare una connessione alla macchina virtuale di archiviazione (SVM) e

delle credenziali prima di utilizzare i cmdlet di PowerShell per eseguire il backup, il ripristino o la clonazione dei cluster PostgreSQL.

Prima di iniziare

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

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

- I nomi dei sistemi di archiviazione devono essere univoci.

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

Passi

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

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

2. Creare una nuova connessione al sistema di archiviazione 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 PostgreSQL a SnapCenter Server.

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

5. Installare il pacchetto e il plug-in SnapCenter per PostgreSQL sull'host.

Per Linux:

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

Per Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL -FilesystemCode scw -RunAsName FinanceAdmin
```

6. Imposta il percorso per SQLLIB.

   Per Windows, il plug-in PostgreSQL utilizzerà il percorso predefinito per la cartella SQLLIB: "C:\Programmi\IBM\SQLLIB\BIN"

   Se si desidera sovrascrivere il percorso predefinito, utilizzare il seguente comando.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
PostgreSQL -configSettings @{“PostgreSQL_SQLLIB_CMD” =
“<custom_path>\IBM\SQLLIB\BIN”}
```

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

Eseguire il backup di PostgreSQL

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

Prima di iniziare

- Devi aver creato una policy di backup.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo ONTAP assegnato all’utente dell’archivio deve includere il privilegio “snapmirror all”. Tuttavia, se si utilizza il ruolo “vsadmin”, il privilegio “snapmirror all” non è richiesto.
- Per l’operazione di backup basata su copia snapshot, assicurarsi che tutti i cluster tenant siano validi e attivi.
- Per i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce, è necessario verificare se i comandi sono presenti nell’elenco dei comandi disponibile sull’host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull’host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull’host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

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

Interfaccia utente SnapCenter

Passi

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

   Seleziona * *, quindi selezionare il nome host e il tipo di risorsa per filtrare le risorse. Puoi quindi selezionare per chiudere il riquadro del filtro.
3. Seleziona la risorsa di cui vuoi eseguire il backup.
4. Nella pagina Risorsa, seleziona **Usa formato nome personalizzato per copia Snapshot**, quindi immetti un formato nome personalizzato che desideri utilizzare per il nome Snapshot.

   Ad esempio, *customtext_policy_hostname* o *resource_hostname*. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.
5. Nella pagina Impostazioni applicazione, procedere come segue:
   - Selezionare la freccia **Backup** per impostare opzioni di backup aggiuntive:

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

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

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

     È anche possibile eseguire i comandi pre prima di uscire dall'operazione di backup. I prescript e i postscript vengono eseguiti nel server SnapCenter .
   - Selezionare la freccia **Configurazioni personalizzate**, quindi immettere le coppie di valori personalizzati richieste per tutti i processi che utilizzano questa risorsa.
   - Selezionare la freccia **Strumento Copia snapshot** per selezionare lo strumento per creare snapshot:

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

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

6. Nella pagina Criteri, procedere come segue:

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

      Puoi anche creare una policy cliccando * + *.

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

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

   c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi selezionare **OK**.

      policy_name è il nome della policy selezionata.

   Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

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

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

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

   Viene visualizzata la pagina della topologia delle risorse.

9. Seleziona **Esegui backup adesso**.
10. Nella pagina Backup, procedere come segue:
    a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa **Criterio** seleziona il criterio che desideri utilizzare per il backup.

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

    b. Selezionare **Backup**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.
    - Nelle configurazioni MetroCluster , SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

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

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

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

Cmdlet di PowerShell

Passi

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

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

   Viene visualizzata la richiesta di nome utente e password.

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

   Questo esempio mostra come aggiungere un'istanza PostgreSQL:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode PostgreSQL
-ResourceType Instance -ResourceName postgresqlinst1
-StorageFootPrint
(@{"VolumeName"="winpostgresql01_data01";"LUNName"="winpostgresql01_
data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.
4. Proteggere la risorsa o aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.
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_wback-up-
   clusters-using-powershell-cmdlets-postgresql.adocith_Resources'
   -Policy postgresql_policy1
   ```

   Questo esempio esegue il backup di una risorsa protetta:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}
   -Policy postgresql_policy2
   ```

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

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

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

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

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

Eseguire il backup dei gruppi di risorse

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

Prima di iniziare

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

Informazioni su questo compito

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

base alla pianificazione.

Passi

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

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

3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi seleziona **Esegui backup ora**.
4. Nella pagina Backup, procedere come segue:
   a. Se hai associato più policy al gruppo di risorse, dall'elenco a discesa **Policy** seleziona la policy che desideri utilizzare per il backup.

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

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

Monitorare le operazioni di backup di PostgreSQL

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

Informazioni su questo compito

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

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Lavori**.
3. Nella pagina Lavori, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.

b. Specificare le date di inizio e fine.

c. Dall'elenco a discesa **Tipo**, selezionare **Backup**.

d. Dal menu a discesa **Stato**, seleziona lo stato del backup.

e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.

4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

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

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

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

Monitorare le operazioni di protezione dei dati sui cluster PostgreSQL nel riquadro Attività

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

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

Passi

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

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

Annulla le operazioni di backup per PostgreSQL

È possibile annullare le operazioni di backup in coda.

Cosa ti servirà

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

Passi

1. Eseguire una delle seguenti azioni:

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

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

Visualizza i backup e i cloni di PostgreSQL nella pagina Topologia

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

Informazioni su questo compito

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

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

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

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

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

Passi

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

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

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

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

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

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

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

   Dopo il backup su richiesta, facendo clic sul pulsante **Aggiorna** si aggiornano i dettagli del backup o del clone.

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

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

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

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

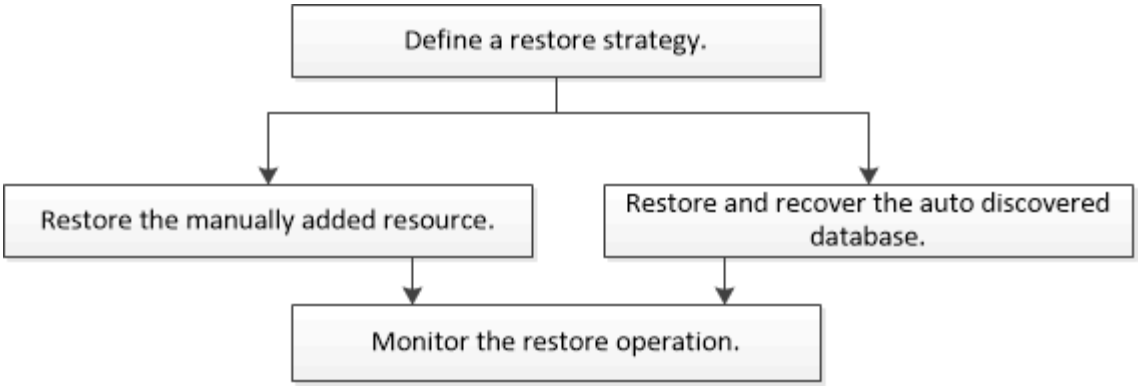
7. Se si desidera eliminare un clone, selezionare il clone dalla tabella, quindi fare clic su .
8. Se vuoi dividere un clone, seleziona il clone dalla tabella, quindi fai clic su .

Ripristina PostgreSQL

Ripristina flusso di lavoro

Il flusso di lavoro di ripristino e recupero 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 anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono informazioni dettagliate sui cmdlet di PowerShell.

"Guida di riferimento ai cmdlet del software SnapCenter" .

Ripristina e recupera un backup di risorse aggiunto manualmente

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

Prima di iniziare

- È necessario aver eseguito il backup della risorsa o dei gruppi di risorse.
- È necessario aver annullato tutte le operazioni di backup in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi pre-ripristino, post-ripristino, montaggio e smontaggio, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

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

Informazioni su questo compito

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

Interfaccia utente SnapCenter

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra 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 associati, ai criteri e allo stato.

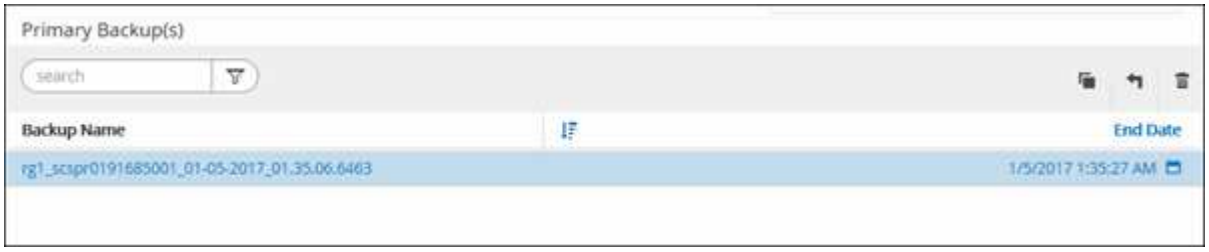
   Sebbene un backup possa riguardare un gruppo di risorse, quando si esegue il ripristino è necessario selezionare le singole risorse che si desidera ripristinare.

   Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato "Non protetto". Ciò può significare che la risorsa non è protetta oppure che è stata sottoposta a backup da un utente diverso.

3. Selezionare la risorsa oppure selezionare un gruppo di risorse e quindi selezionare una risorsa in quel gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Nella tabella Backup primari, seleziona il backup da cui desideri effettuare il ripristino, quindi fai clic su * * *.



6. Nella pagina Ambito di ripristino, seleziona **Risorsa completa**.

   a. Se si seleziona **Risorsa completa**, verranno ripristinati tutti i volumi di dati configurati del cluster PostgreSQL.

      Se la risorsa contiene volumi o qtree, gli snapshot acquisiti dopo lo snapshot selezionato per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata.

      È possibile selezionare più LUN.

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

7. Nella pagina Pre ops, immettere i comandi pre restore e unmount da eseguire prima di eseguire un processo di ripristino.

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

8. Nella pagina Post ops, immettere i comandi mount e post restore da eseguire dopo aver eseguito un processo di ripristino.

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

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

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

10. Rivedi il riepilogo e poi clicca su **Fine**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

Cmdlet di PowerShell

Passi

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

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

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

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
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, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

Ripristina e recupera un backup del cluster rilevato automaticamente

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

Prima di iniziare

- È necessario aver eseguito il backup della risorsa o dei gruppi di risorse.
- È necessario aver annullato tutte le operazioni di backup in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi pre-ripristino, post-ripristino, montaggio e smontaggio, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in*

Creator\etc\allowed_commands.config

- Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

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

Informazioni su questo compito

- Le copie di backup basate su file non possono essere ripristinate da SnapCenter.
- Per le risorse rilevate automaticamente, il ripristino è supportato con SFSR.
- Il ripristino automatico non è supportato.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot SnapLock Vault come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra 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 associati, ai criteri e allo stato.

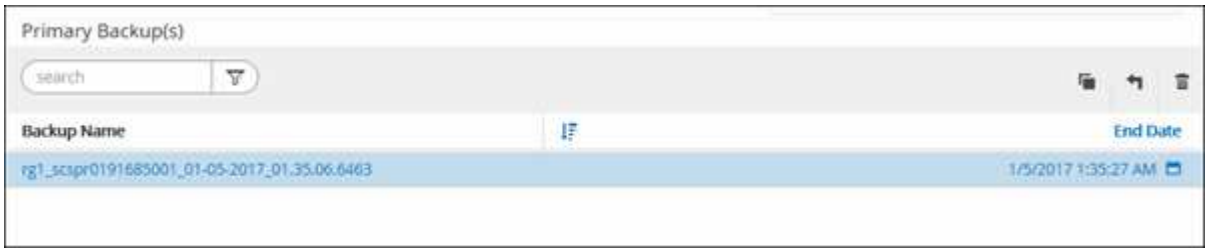
   Sebbene un backup possa riguardare un gruppo di risorse, quando si esegue il ripristino è necessario selezionare le singole risorse che si desidera ripristinare.

   Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato "Non protetto". Ciò può significare che la risorsa non è protetta oppure che è stata sottoposta a backup da un utente diverso.

3. Selezionare la risorsa oppure selezionare un gruppo di risorse e quindi selezionare una risorsa in quel gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Nella tabella Backup primari, seleziona il backup da cui desideri effettuare il ripristino, quindi fai clic su * * *.



6. Nella pagina Ripristina ambito, seleziona **Risorsa completa** per ripristinare i volumi di dati configurati del cluster PostgreSQL.
7. Nella pagina Ambito di ripristino, seleziona una delle seguenti opzioni:

Se tu…	Fai questo…

Vuoi recuperare il più vicino possibile all'ora corrente	Seleziona **Ripristina allo stato più recente**. Per le risorse di un singolo contenitore, specificare una o più posizioni di backup di log e cataloghi.
Vuoi ripristinare il punto temporale specificato	Seleziona **Recupera fino a un punto nel tempo**. a. Inserisci data e ora. Inserisci data e ora. Ad esempio, l'host Linux PostgreSQL si trova a Sunnyvale, CA e l'utente a Raleigh, NC sta recuperando i log in SnapCenter. Se l'utente desidera eseguire un ripristino alle 5 del mattino a Sunnyvale, CA, deve impostare il fuso orario del browser sul fuso orario dell'host Linux PostgreSQL, ovvero GMT-07:00, e specificare la data e l'ora come 5:00.
Non voglio recuperare	Selezionare **Nessun recupero**.

Non è possibile recuperare le risorse PostgreSQL aggiunte manualmente.

Il plug-in SnapCenter per PostgreSQL crea un backup_label e una tablespace_map nella cartella */<OS_temp_folder>/postgresql_sc_recovery*<Restore_JobId>/_ per facilitare il ripristino manuale.

1. Nella pagina Pre ops, immettere i comandi pre restore e unmount da eseguire prima di eseguire un processo di ripristino.

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

2. Nella pagina Post ops, immettere i comandi mount e post restore da eseguire dopo aver eseguito un processo di ripristino.

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

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

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

4. Rivedi il riepilogo e poi clicca su **Fine**.
5. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

Ripristinare le risorse utilizzando i cmdlet di PowerShell

Il ripristino di un backup delle risorse include l'avvio di una sessione di connessione con SnapCenter Server, 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.

Passi

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

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

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

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
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, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

Monitorare le operazioni di ripristino di PostgreSQL

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

Informazioni su questo compito

Gli stati post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi ulteriore azione di ripristino che è possibile intraprendere.

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

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Ripristina**.
   d. Dall'elenco a discesa **Stato**, selezionare lo stato di ripristino.
   e. Fare clic su **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 **Dettagli lavoro**, fare clic su **Visualizza registri**.

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

Clona i backup delle risorse PostgreSQL

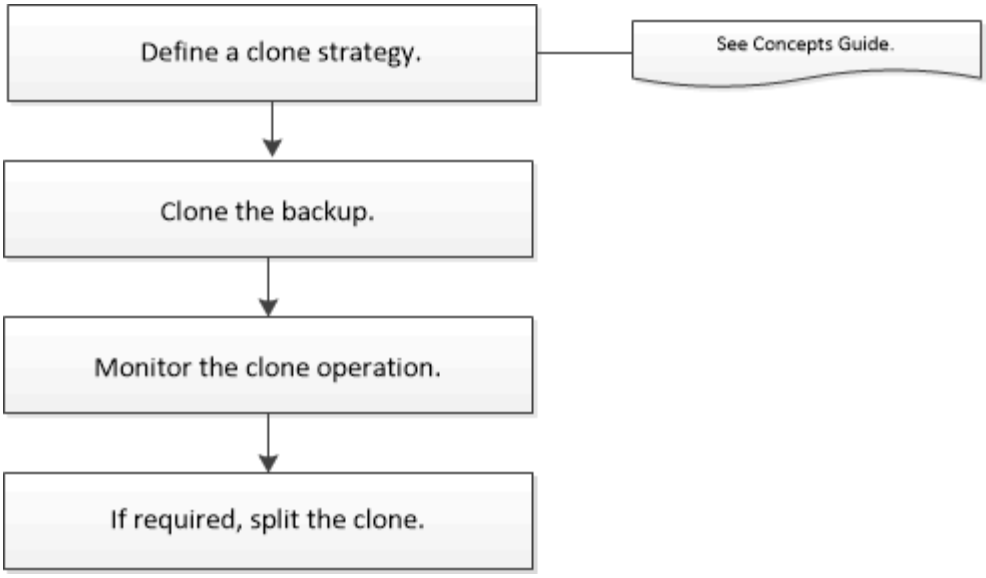
Flusso di lavoro di clonazione

Il flusso di lavoro della clonazione include l'esecuzione dell'operazione di clonazione e il monitoraggio dell'operazione.

Informazioni su questo compito

- È possibile clonare sul server PostgreSQL di origine.
- È possibile clonare i backup delle risorse per i seguenti motivi:
  - Per testare la funzionalità che deve essere implementata utilizzando la struttura e il contenuto delle risorse correnti durante i cicli di sviluppo dell'applicazione
  - Per strumenti di estrazione e manipolazione dei dati durante il popolamento dei data warehouse
  - Per recuperare dati che sono stati cancellati o modificati per errore

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



È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono informazioni dettagliate sui cmdlet di PowerShell.

Clonare un backup PostgreSQL

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

Prima di iniziare

- Avresti dovuto eseguire il backup delle risorse o del gruppo di risorse.
- È necessario assicurarsi che gli aggregati che ospitano i volumi siano presenti nell'elenco degli aggregati assegnati della macchina virtuale di archiviazione (SVM).
- Per i comandi pre-clone o post-clone, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

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

Informazioni su questo compito

- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere,https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html["Dividere un volume FlexClone dal suo volume padre"] .
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

Interfaccia utente SnapCenter

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra 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 policy associati e stato.

3. Selezionare la risorsa o il gruppo di risorse.

   Se si seleziona un gruppo di risorse, è necessario selezionare una risorsa.

   Viene visualizzata la pagina della topologia della risorsa o del gruppo di risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Selezionare il backup dei dati dalla tabella, quindi fare clic su  .
6. Nella pagina Posizione, eseguire le seguenti azioni:

Per questo campo…	Fai questo…
Server clone	Scegliere un host su cui creare il clone.
Porta di destinazione	Immettere la porta di destinazione PostgreSQL da clonare dai backup esistenti.
Indirizzo IP di esportazione NFS	Immettere gli indirizzi IP o i nomi host su cui verranno esportati i volumi clonati. Questo è applicabile solo alle risorse di tipo archiviazione NFS.
Capacità massima del pool (MiB/s)	Immettere la capacità massima di un pool di capacità. Ciò è applicabile solo per le risorse di tipo storage ANF.

7. Nella pagina Script, procedere come segue:

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

   a. Immettere i comandi per il pre-clone o il post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clonazione.
      - Comando pre-clone: elimina i cluster esistenti con lo stesso nome
      - Comando post-clonazione: verifica un cluster o avvia un cluster.

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

Comando di montaggio 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 **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email.

9. Rivedi il riepilogo e poi clicca su **Fine**.
10. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

Cmdlet di PowerShell

Passi

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

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

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. Avvia un'operazione di clonazione da un backup esistente e specifica gli indirizzi IP di esportazione NFS su cui vengono esportati i volumi clonati.

Questo esempio mostra che il backup da clonare ha un indirizzo NFSExportIPs pari a 10.32.212.14:

Per il cluster PostgreSQL:

```
PS C:\> New-SmClone -AppPluginCode PostgreSQL -BackupName "
scpostgresql01_ openenglab_netapp_com_PostgreSQL_postgres_5432_06-
26-2024_00_33_41_1570" -Resources @{"Host"="
10.32.212.13";"Uid"="postgres_5432"} -port 2345 -CloneToHost
10.32.212.14
```

Se NFSExportIPs non è specificato, l'impostazione predefinita è l'esportazione 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 di clonazione.

   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 di PostgreSQL

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

Informazioni su questo compito

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

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

Passi

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

Dividi un clone

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

Informazioni su questo compito

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

  Ad esempio, dopo aver creato clone1 da un backup del database, è possibile creare un backup di clone1 e quindi clonare questo backup (clone2). Dopo aver creato clone2, clone1 è un clone intermedio e non è possibile eseguire l'operazione di divisione del clone su clone1. Tuttavia, è possibile eseguire l'operazione di divisione del clone su clone2.

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

- Quando si divide un clone, le copie di backup e i processi di clonazione del clone vengono eliminati.
- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere, "Dividere un volume FlexClone dal suo volume padre" .
- Assicurarsi che il volume o l'aggregato sul sistema di archiviazione sia online.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **Risorse**, seleziona l'opzione appropriata dall'elenco Visualizza:

Opzione	Descrizione
Per applicazioni di database	Selezionare **Database** dall'elenco Visualizza.
Per i file system	Selezionare **Percorso** dall'elenco Visualizza.

3. Seleziona la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista **Gestisci copie**, seleziona la risorsa clonata (ad esempio, il database o il LUN), quindi fai clic su *  *.
5. Verificare la dimensione stimata del clone da dividere e lo spazio disponibile richiesto sull'aggregato, quindi fare clic su **Avvia**.
6. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

   L'operazione di suddivisione del clone smette di rispondere se il servizio SMCore viene riavviato. È necessario eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione.

   Se si desidera un tempo di polling più lungo o più breve per verificare 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 per SMCore per il polling dello stato dell'operazione di divisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

   Per esempio:

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

   L'operazione di avvio della suddivisione del clone fallisce se è in corso un backup, un ripristino o un'altra suddivisione del clone. È necessario riavviare l'operazione di suddivisione del clone solo dopo aver completato le operazioni in esecuzione.

Informazioni correlate

"La clonazione o la verifica SnapCenter non riesce perché l'aggregato non esiste"

Elimina o dividi i cloni del cluster PostgreSQL dopo l'aggiornamento SnapCenter

Dopo l'aggiornamento a SnapCenter 4.3, i cloni non saranno più visibili. È possibile eliminare il clone o dividere i cloni dalla pagina Topologia della risorsa da cui sono stati creati i cloni.

Informazioni su questo compito

Se si desidera individuare l'impronta di archiviazione dei cloni nascosti, eseguire il seguente comando: `Get-`

```
SmClone -ListStorageFootprint
```

Passi

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-smresourcegroup.
3. Rimuovere la protezione della risorsa clonata utilizzando il cmdlet remove-smprotectresource.
4. Selezionare la risorsa padre dalla pagina Risorse.

   Viene visualizzata la pagina della topologia delle risorse.

5. Dalla vista Gestisci copie, selezionare i cloni dai sistemi di archiviazione primari o secondari (con mirroring o replica).
6. Seleziona i cloni e poi clicca  per eliminare i cloni o fare clic  per dividere i cloni.
7. Fare clic su **OK**.

Informazioni sul copyright

Informazioni sul marchio commerciale