Proteggere PostgreSQL

SnapCenter Software 6.0

NetApp
January 31, 2025

Sommario

Proteggere PostgreSQL

Plug-in SnapCenter per PostgreSQL

Panoramica del plug-in SnapCenter per PostgreSQL

Il plug-in SnapCenter per il cluster PostgreSQL è un componente lato host del software NetApp SnapCenter che consente la gestione della protezione dei dati integrata con l'applicazione dei cluster PostgreSQL. Il plug-in per il cluster PostgreSQL automatizza il backup, il ripristino e la clonazione dei cluster PostgreSQL nell'ambiente SnapCenter.

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

Quando viene 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 replica del backup disk-to-disk per garantire la conformità agli standard.

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

È supportato il layout VMDK o dello storage virtuale.

Cosa si può fare utilizzando il plug-in SnapCenter per PostgreSQL

Quando si installa il cluster Plug-in per PostgreSQL nel proprio ambiente, è possibile utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione dei cluster PostgreSQL e delle relative risorse. È inoltre possibile eseguire attività a supporto di tali operazioni.

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

Plug-in SnapCenter per funzioni PostgreSQL

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

- **Interfaccia utente grafica unificata**

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

- **Amministrazione centrale automatizzata**

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

- **Tecnologia di copia istantanea 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 anche i seguenti vantaggi:

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

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

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

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

- Supporto della funzionalità snapshot del gruppo di coerenza (CG) di ONTAP durante la creazione dei backup.
- Possibilità di eseguire più backup contemporaneamente su più host di risorse

  In una singola operazione, gli snapshot vengono consolidati quando le risorse di un singolo host condividono lo stesso volume.

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

Tipi di archiviazione supportati dal plug-in SnapCenter per PostgreSQL

SnapCenter supporta un'ampia gamma di tipi di storage su macchine fisiche e macchine virtuali (VM). È necessario verificare il supporto per il tipo di archiviazione prima di installare il plug-in SnapCenter per PostgreSQL.

Macchina	Tipo di storage
Server fisico	• LUN connessi a FC • LUN connessi a iSCSI • Volumi connessi a NFS

Macchina	Tipo di storage
VMware ESXi	• Il completamento delle LUN RDM collegate da un HBASCAN ESXi FC o iSCSI degli HBA (host bus adapter) potrebbe richiedere molto tempo, in quanto SnapCenter esegue la scansione di tutti gli adattatori bus host presenti nell'host. È possibile modificare il file **LinuxConfig.pm** situato in */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* per impostare il valore del parametro **SCSI_HOSTS_OPTIMIZED_RESCAN** su 1 per ripetere la scansione solo degli HBA elencati in HBA_DRIVER_NAMES. • LUN iSCSI collegati direttamente al sistema guest dall'iniziatore iSCSI • VMDK su datastore NFS • VMDK su VMFS • Volumi NFS collegati direttamente al sistema guest • Datastore vVol in NFS e SAN È possibile eseguire il provisioning del datastore vVol solo con i tool ONTAP per VMware vSphere.

Privilegi ONTAP minimi richiesti per il plug-in PostgreSQL

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

- All-access comands (comandi all-access): Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
  - event generate-autosupport-log
  - mostra la cronologia dei lavori
  - interruzione del lavoro
  - lun
  - lun create (crea lun)
  - lun create (crea lun)
  - lun create (crea lun)
  - lun delete (elimina lun)
  - lun igroup add
  - lun igroup create
  - lun igroup delete (elimina igroup lun)
  - lun igroup rename (rinomina lun igroup)

- lun igroup rename (rinomina lun igroup)
- lun igroup show
- lun mapping add-reporting-node
- creazione mappatura lun
- eliminazione della mappatura lun
- nodi di remove-reporting-mapping lun
- visualizzazione della mappatura del lun
- modifica del lun
- lun move-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- ridimensionamento del lun
- lun seriale
- lun show
- regola aggiuntiva del criterio snapmirror
- regola-modifica del criterio snapmirror
- regola di rimozione del criterio snapmirror
- policy di snapmirror
- ripristino di snapmirror
- spettacolo di snapmirror
- storia di snapmirror
- aggiornamento di snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione del clone del volume
- visualizzazione del clone del volume
- avvio della divisione del clone del volume
- interruzione della divisione del clone del volume
- creazione del volume
- distruggere il volume
- creazione del clone del file di volume
- file di volume show-disk-usage
- volume offline
- volume online
- modifica del volume

    - creazione del qtree del volume
    - eliminazione del qtree del volume
    - modifica del qtree del volume
    - visualizzazione del qtree del volume
    - limitazione del volume
    - presentazione del volume
    - creazione di snapshot di volume
    - eliminazione dello snapshot del volume
    - modifica dello snapshot del volume
    - modifica snapshot del volume-tempo di scadenza snaplock
    - rinominare lo snapshot del volume
    - ripristino dello snapshot del volume
    - file di ripristino dello snapshot del volume
    - visualizzazione di snapshot di volume
    - smontare il volume
    - cifs vserver
    - creazione condivisione cifs vserver
    - eliminazione condivisione cifs vserver
    - vserver cifs shadowcopy mostra
    - show di condivisione di vserver cifs
    - vserver cifs show
    - policy di esportazione di vserver
    - creazione policy di esportazione vserver
    - eliminazione della policy di esportazione di vserver
    - creazione della regola dei criteri di esportazione di vserver
    - visualizzazione della regola dei criteri di esportazione di vserver
    - visualizzazione della policy di esportazione di vserver
    - iscsi vserver
    - visualizzazione della connessione iscsi del vserver
    - show di vserver
- Comandi di sola lettura: Privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
    - interfaccia di rete
    - visualizzazione dell’interfaccia di rete
    - server virtuale

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

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

SnapCenter esegue gli aggiornamenti di SnapMirror e SnapVault al termine dell'operazione di Snapshot. Gli aggiornamenti di SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter; non creare una pianificazione ONTAP separata.

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

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

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

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per ulteriori informazioni sulle relazioni di SnapMirror flessibili per la versione e sulla loro configurazione, vedere la "Documentazione ONTAP".

Strategia di backup per PostgreSQL

Definire una strategia di backup per PostgreSQL

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

A proposito di questa attività

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

Fasi

1. Stabilire quando eseguire il backup delle risorse.
2. Decidere il numero di processi di backup necessari.
3. Decidere come assegnare un nome ai backup.
4. È possibile decidere se creare una policy basata su copie Snapshot per eseguire il backup di snapshot del

cluster coerenti con l'applicazione.

5. Decidere se utilizzare la tecnologia NetApp SnapMirror per la replica o la tecnologia NetApp SnapVault per la conservazione a lungo termine.
6. Determina il periodo di conservazione per gli Snapshot sul sistema storage di origine e sulla destinazione di SnapMirror.
7. Determinare se si desidera eseguire qualsiasi comando prima o dopo l'operazione di backup e fornire una prescrizione o postscript.

Rilevamento automatico delle risorse sull'host Linux

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

Tipo di backup supportati

Il 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.

In che modo il plug-in SnapCenter per PostgreSQL utilizza gli snapshot dei gruppi di coerenza

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

Puoi anche specificare il tempo di attesa per lo storage controller che raggruppa le snapshot in modo coerente. Le opzioni di tempo di attesa disponibili sono **urgente**, **Medio** e **rilassato**. È inoltre possibile attivare o disattivare la sincronizzazione WAFL (Write Anywhere file Layout) durante l'operazione di snapshot di gruppo coerente. WAFL Sync migliora le prestazioni di una snapshot del gruppo di coerenza.

Modalità di gestione dei backup dei dati da parte di SnapCenter

SnapCenter gestisce l'amministrazione dei backup dei dati a livello di file system e del sistema di storage.

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

Considerazioni per determinare le pianificazioni di backup per PostgreSQL

Il fattore più critico per determinare una pianificazione di backup è il tasso di cambiamento per la risorsa. È possibile eseguire il backup di una risorsa utilizzata in modo pesante ogni ora, mentre è possibile eseguire il backup di una risorsa utilizzata

raramente una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo SLA (Service Level Agreement) e l'RPO (Recovery Point Objective).

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

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

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

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

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

Numero di processi di backup necessari per PostgreSQL

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

Convenzioni di denominazione per il backup del plug-in per i cluster PostgreSQL

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

L'istantanea utilizza la seguente convenzione di denominazione predefinita:

```
resourcegroupname_hostname_timestamp
```

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

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

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

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

In alternativa, è possibile specificare il formato del nome dell'istantanea mentre si proteggono le risorse o i gruppi di risorse selezionando **Usa il formato del nome personalizzato per la copia dell'istantanea**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, il suffisso dell'indicatore data e ora viene aggiunto al nome dell'istantanea.

Strategia di ripristino e ripristino per PostgreSQL

Definire una strategia di ripristino e ripristino per le risorse PostgreSQL

È necessario definire una strategia prima di ripristinare e ripristinare il cluster per poter eseguire correttamente le operazioni di ripristino e recovery.

È supportato solo il ripristino manuale del cluster.

Fasi

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. Decidere il tipo di operazioni di ripristino che si desidera 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, le qtree e le 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 un'altra risorsa è ospitata sugli stessi volumi o qtree, anche tale risorsa viene eliminata.

NOTA: Il plug-in per PostgreSQL crea un backup_label e 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. Questo consente di ripristinare tutti i volumi, i qtree e le LUN di una risorsa.

Tipi di operazioni di ripristino per PostgreSQL rilevato automaticamente

Il plug-in SnapCenter per PostgreSQL supporta Single file SnapRestore e 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

completa risorsa è selezionata

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

- Se è selezionata solo l'opzione **completa risorsa**
- Quando si seleziona il backup da una posizione secondaria SnapMirror o SnapVault e si seleziona l'opzione **completa risorsa**

Tipi di operazioni di ripristino supportate per i cluster PostgreSQL

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

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

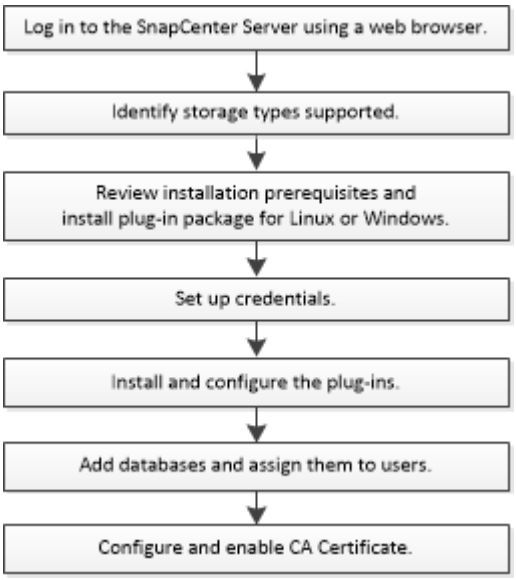
  Specificare la data e l'ora per il ripristino.

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

Preparare l'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 completare tutti i requisiti. Il plug-in SnapCenter per PostgreSQL è disponibile sia in ambienti Windows che Linux.

- È necessario aver installato Java 11 sull'host.

  IBM Java non è supportato.

- Per Windows, il plug-in Creator Service dovrebbe essere in esecuzione utilizzando l'utente di Windows "`LocalSystem"', che è il comportamento predefinito quando 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 del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host. Il plug-in SnapCenter per Microsoft Windows verrà distribuito per impostazione predefinita con il plug-in PostgreSQL sugli host Windows.
- Il server SnapCenter deve avere accesso alla porta 8145 o personalizzata del plug-in per l'host PostgreSQL.

Host Windows

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

  "Download Java per tutti i sistemi operativi"

  "Tool di matrice di interoperabilità NetApp"

Host Linux

- È necessario aver attivato la connessione SSH basata su password per l'utente root o non root.
- È necessario aver installato Java 11 sull'host Linux.

  "Download Java per tutti i sistemi operativi"

  "Tool di matrice di interoperabilità NetApp"

- Per i cluster PostgreSQL in esecuzione su un host Linux, durante l'installazione del plug-in per PostgreSQL, il plug-in SnapCenter per UNIX viene installato automaticamente.
- Si dovrebbe 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 ciascun comando su una riga separata; i comandi non rilevano la distinzione tra maiuscole e minuscole. Assicurarsi di specificare il percorso completo e racchiudere il percorso tra virgolette (") se contiene spazi.

Ad 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, i comandi o l'esecuzione dello script verranno bloccati e il flusso di lavoro non riuscirà con il seguente errore:

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

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

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

SnapCenter 2.0 e versioni successive consentono a un utente non root di installare il pacchetto di plug-in SnapCenter per Linux e avviare il processo di plug-in. I processi di plug-in verranno eseguiti come utenti non root. È necessario configurare i privilegi sudo per l'utente non root per fornire l'accesso a diversi percorsi.

Cosa ti serve

- Sudo versione 1.8.7 o successiva.
- Se l'umask è 0027, assicurarsi che la cartella java e tutti i file all'interno dovrebbero avere l'autorizzazione di 555. In caso contrario, l'installazione dei plug-in potrebbe non riuscire.
- Per l'utente non root, assicurarsi che il nome dell'utente non root e del gruppo dell'utente siano identici.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione del messaggio: 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
```

A proposito di questa attività

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

- /Home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /Custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/snapcenter/spl/bin/spl

Fasi

1. Accedere all'host Linux su cui si desidera installare il pacchetto di plug-in SnapCenter per Linux.
2. Aggiungere le seguenti righe al file /etc/sudoers usando l'utility visudo Linux.

```
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 !visiblepw
Defaults: LINUX_USER !requiretty
```

Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, aggiungere quanto segue al file /etc/sudoers: '/<crs_home>/bin/olsnodes'

È possibile ottenere il valore di *crs_home* dal file */etc/oracle/olr.loc*.

LINUX_USER è il nome dell'utente non root creato.

È possibile ottenere il *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 il server SnapCenter è installato sull'host Linux.

L'esempio deve essere utilizzato solo come riferimento per la creazione di dati personali.

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

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

Elemento	Requisiti
Sistemi operativi	Microsoft Windows Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".
RAM minima per il plug-in SnapCenter sull'host	1 GB
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	5 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.

Elemento	Requisiti
Pacchetti software richiesti	• DOTNET Core che inizia con la versione 8.0.5 e include tutte le patch .NET 8 successive • PowerShell Core 7.4.2 Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp". Per . Per informazioni specifiche sulla risoluzione dei problemi, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet."

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

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

Elemento	Requisiti
Sistemi operativi	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".
RAM minima per il plug-in SnapCenter sull'host	1 GB
Spazio minimo di installazione e registrazione per il plug-in SnapCenter sull'host	2 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di storage da parte della cartella dei log. Lo spazio di log richiesto varia in base al numero delle entità da proteggere e alla frequenza delle operazioni di protezione dei dati. Se lo spazio su disco non è sufficiente, i registri non verranno creati per le operazioni eseguite di recente.

Elemento	Requisiti
Pacchetti software richiesti	Java 11 Oracle Java e OpenJDK Se JAVA è stato aggiornato alla versione più recente, assicurarsi che l'opzione JAVA_HOME disponibile in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto. Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Impostare le credenziali per il plug-in SnapCenter per PostgreSQL

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter. Devi creare credenziali per l'installazione di plug-in SnapCenter e credenziali aggiuntive per eseguire operazioni di protezione dei dati su cluster o file system Windows.

A proposito di questa attività

- Host Linux

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

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

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

- Host Windows

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

  È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore sull'host remoto.

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

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **credenziale**.
3. Fare clic su **nuovo**.
4. Nella pagina credenziale, specificare le informazioni necessarie per la configurazione delle credenziali:

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

5. Fare clic su **OK**.

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

Configurare gMSA su Windows Server 2016 o versione successiva

Windows Server 2016 o versione successiva consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatica delle password dell'account di servizio da un account di dominio gestito.

Prima di iniziare

- È necessario disporre di un controller di dominio Windows Server 2016 o versione successiva.
- È necessario disporre di un host Windows Server 2016 o versione successiva, membro del dominio.

Fasi

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

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

   Ad esempio,

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

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

      A tale scopo, eseguire il seguente comando da PowerShell:

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

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


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

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

a. Riavviare l'host.

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

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

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

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

Installare il plug-in SnapCenter per PostgreSQL

Aggiungere host e installare pacchetti plug-in su host remoti

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

Prima di iniziare

- Se il sistema operativo dell'host SnapCenter Server è Windows 2019 e il sistema operativo dell'host plug-in è Windows 2022, è necessario effettuare le seguenti operazioni:
  - Eseguire l'aggiornamento a Windows Server 2019 (OS Build 17763,5936) o versione successiva
  - Eseguire l'aggiornamento a Windows Server 2022 (OS Build 20348,2402) o versione successiva
- È necessario essere un utente assegnato a un ruolo che disponga delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore di SnapCenter.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se

l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disattivare il controllo dell'account utente sull'host.

- Assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.
- La documentazione di amministrazione contiene informazioni sulla gestione degli host.
- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi.

  "Configurare l'account del servizio gestito di gruppo su Windows Server 2016 o versioni successive per PostgreSQL"

A proposito di questa attività

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

Fasi

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

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

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

5. Nella sezione Select Plug-in to Install (Seleziona plug-in da installare), selezionare i plug-in da installare.

   Quando si utilizza l'API REST per installare 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…	Eseguire questa operazione…
Porta	Mantenere il numero di porta predefinito o specificare il numero di porta. Il numero di porta predefinito è 8145. Se il server SnapCenter è stato installato su una porta personalizzata, tale numero di porta viene visualizzato come porta predefinita. Se i plug-in sono stati installati manualmente e si è specificata una porta personalizzata, è necessario specificare la stessa porta. In caso contrario, l'operazione non riesce.
Percorso di installazione	Il plug-in per PostgreSQL è installato sull'host client PostgreSQL e può essere installato su un sistema Windows o Linux. • Per il pacchetto di plug-in SnapCenter per Windows, il percorso predefinito è C: In alternativa, è possibile personalizzare il percorso. • Per il pacchetto di plug-in SnapCenter per Linux, il percorso predefinito è /opt/NetApp/snapcenter. In alternativa, è possibile personalizzare il percorso.

Per questo campo…	Eseguire questa operazione…
Ignorare i controlli di preinstallazione	Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.
Aggiungere tutti gli host nel cluster	Selezionare questa casella di controllo per aggiungere tutti i nodi cluster.
Utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in	Per l'host Windows, selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito di gruppo (gMSA) per eseguire i servizi plug-in. Fornire il nome gMSA nel seguente formato: Nome dominio/nome account. GMSA verrà utilizzato come account del servizio di accesso solo per il servizio del plug-in SnapCenter per Windows.

7. Fare clic su **Invia**.

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

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

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

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

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

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

9. Monitorare l'avanzamento dell'installazione.
   - Per i plug-in di Windows, i log di installazione e aggiornamento si trovano in: *C:\Windows\SnapCenter plugin\Install*<JOBID>_

◦ Per i plug-in Linux, i log di installazione si trovano in: */var/opt/snapcenter/logs/SnapCenter_Linux_host_Plug-in_Install*<JOBID>.log_ e i log di aggiornamento si trovano in: */var/opt/snapcenter/logs/SnapCenter_Linux_host_Plug-in_Upgrade*<JOBID>.log_

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

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

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 del plug-in.

Fasi

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

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

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

4. Inserire le credenziali per l'installazione remota.

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

Prima di iniziare

- È necessario installare il plug-in per il cluster PostgreSQL su ciascuno degli host Linux in cui risiede il client PostgreSQL.
- L'host Linux su cui si sta installando il plug-in SnapCenter per il cluster PostgreSQL deve soddisfare i requisiti del software, del cluster e del sistema operativo dipendenti.

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

  "Tool di matrice di interoperabilità NetApp"

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

SnapCenter su un host Windows.

Fasi

1. Copiare il file di installazione del pacchetto di plug-in SnapCenter per Linux (snapcenter_linux_host_plugin.bin) da C:\ProgramData\NetApp\SnapCenter\Package Repository nell'host in cui si desidera installare il plug-in per PostgreSQL.

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

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

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

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

4. Modificare il file /<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties, quindi aggiungere il parametro PLUGINS_ENABLED = PostgreSQL:3,0 .
5. Aggiungere l'host al server SnapCenter utilizzando il cmdlet Add-Smhost e i parametri richiesti.

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

Monitorare lo stato dell'installazione del plug-in per PostgreSQL

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

A proposito di questa attività

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

- In corso
- Completato correttamente

- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, per filtrare l'elenco in modo che siano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filter** (filtro).
   b. Facoltativo: Specificare la data di inizio e di fine.
   c. Dal menu a discesa Type (tipo), selezionare **Plug-in installation** (Installazione plug-in).
   d. Dal menu a discesa Status (Stato), selezionare lo stato dell'installazione.
   e. Fare clic su **Apply** (Applica).
4. Selezionare il processo di installazione e fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

Configurare il certificato CA

Generare il file CSR del certificato CA

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

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

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

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

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

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

Importare i certificati CA

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

Fasi

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

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

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

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

Ottenere il thumbprint del certificato CA

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

Fasi

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

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

2. Eseguire le seguenti operazioni da PowerShell:

a. Eseguire il comando seguente per elencare l'identificazione del certificato installato e identificare il certificato installato di recente in base al nome del soggetto.

   Get-ChildItem -Path Certate: LocalMachine/My

b. Copiare la stampa personale.

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

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

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

Fasi

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

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

   Ad esempio:

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

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

   Ad esempio:

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

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

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

personalizzati di SnapCenter per attivare il certificato digitale installato.

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

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

Fasi

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

   È il valore corrispondente alla chiave 'KEYSTORE_PASS'.

2. Modificare la password del keystore:

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

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

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

3. Riavviare il servizio dopo aver modificato la password.

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

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

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

Fasi

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

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

4. Aggiungere un certificato root o intermedio:

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

Aggiungere il certificato CA principale e i certificati CA intermedi.

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

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

Fasi

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

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

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

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

5. Elencare i certificati aggiunti nel keystore.

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

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

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

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

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

   Aggiornare questo valore con la chiave SCC_CERTIFICATE_ALIAS.

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

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

A proposito di questa attività

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

Fasi

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

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

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

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

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

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

Fasi

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

   È il valore corrispondente alla chiave *KEYSTORE_PASS*.

2. Modificare la password del keystore:

   keytool -storepasswd -keystore keystore.jks

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

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

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

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

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

4. Riavviare il servizio dopo aver modificato la password.

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

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

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

Fasi

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

   keytool -list -v -keystore keystore.jks

4. Aggiungere un certificato root o intermedio:

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

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

   Aggiungere il certificato CA principale e i certificati CA intermedi.

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

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

Fasi

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

   keytool -list -v -keystore keystore.jks

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

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

5. Elencare i certificati aggiunti nel keystore.

   keytool -list -v -keystore keystore.jks

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

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

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

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

Aggiornare questo valore con la chiave SCC_CERTIFICATE_ALIAS.

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

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

A proposito di questa attività

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

Fasi

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

   I certificati in entrata verranno verificati per ciascun CRL.

Abilitare i certificati CA per i plug-in

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

Prima di iniziare

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

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

Fasi

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

Al termine

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

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

- * * Indica che il certificato CA non può essere 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 vengono 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 di SnapCenter deve installare e configurare il server SnapCenter ed eseguire le attività dei prerequisiti.

- Installare e configurare il server SnapCenter.
- Accedere al server SnapCenter.
- Configurare l'ambiente SnapCenter aggiungendo connessioni al sistema di storage e creando credenziali, se applicabili.
- Installare Java 11 sull'host Linux o Windows.

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

- Impostare SnapMirror e SnapVault, se si desidera eseguire la replica del backup.

Modalità di utilizzo di risorse, gruppi di risorse e criteri per la protezione di 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.

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

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

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

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

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

Un gruppo di risorse definisce ciò che si desidera proteggere e quando si desidera proteggerlo in termini di giorno e ora. Pensa a una policy come a come vuoi proteggerla. Se si esegue il backup di tutti i cluster, ad esempio, è possibile creare un gruppo di risorse che includa tutti i cluster nell'host. È quindi possibile associare due criteri al gruppo di risorse: Una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e

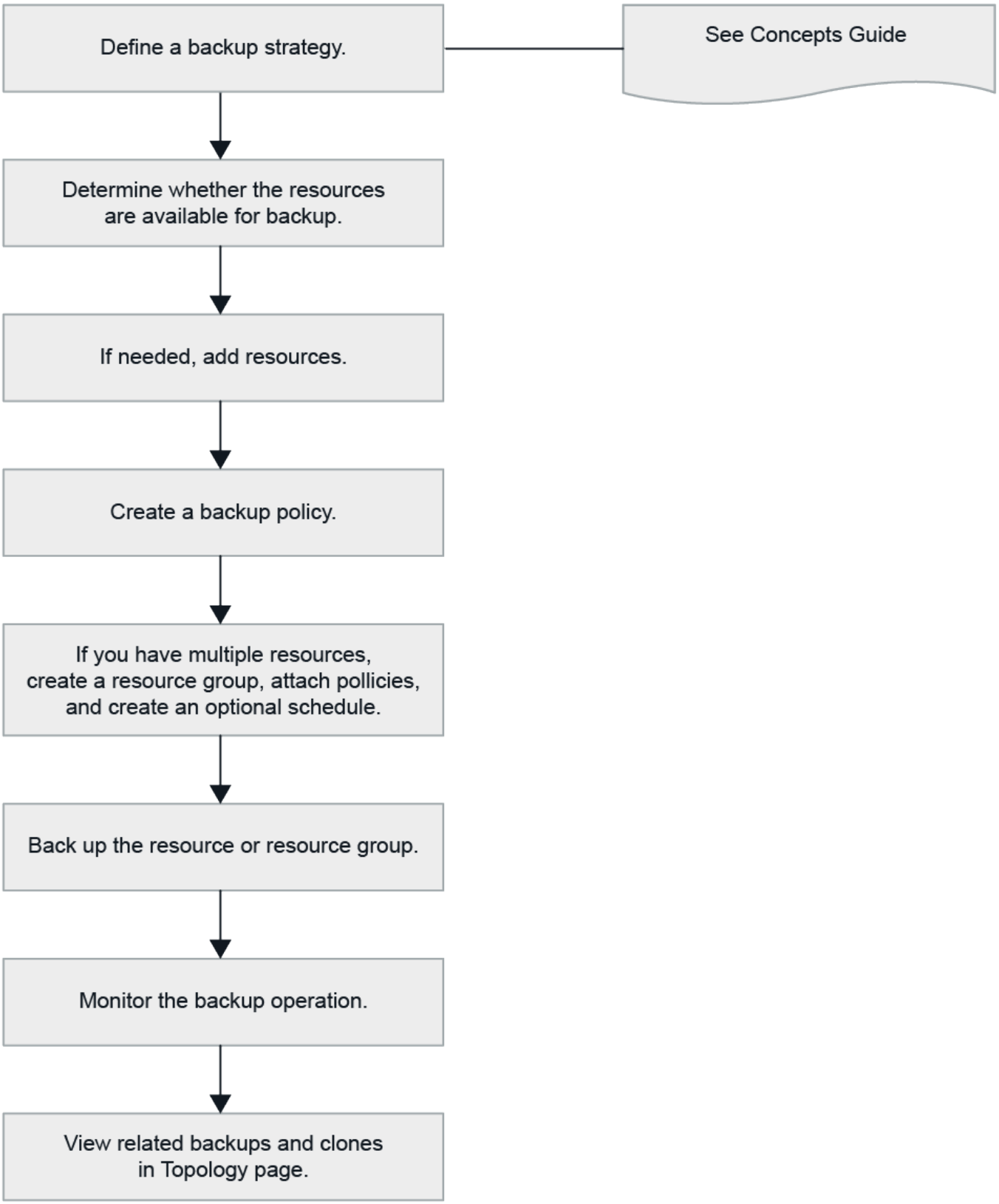
si allegano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup completo ogni giorno.

Eseguire il backup delle risorse PostgreSQL

Eseguire il backup delle risorse PostgreSQL

È possibile creare un backup di una risorsa (cluster) o di un gruppo di risorse. Il workflow di backup comprende planning, identificazione dei cluster per il backup, gestione dei criteri di backup, creazione di gruppi di risorse e aggiunta di criteri, creazione di backup e monitoraggio delle operazioni.

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



È inoltre possibile utilizzare i cmdlet PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida in linea del cmdlet di SnapCenter e le informazioni di riferimento del cmdlet contengono ulteriori informazioni sui cmdlet di PowerShell. "Guida di riferimento al cmdlet del software SnapCenter".

Rilevare automaticamente i cluster

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

Prima di iniziare

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

A proposito di questa attività

- Dopo aver installato il plug-in, tutti i cluster su quell'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.

Fasi

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

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

4. Fare clic su **Refresh Resources** (Aggiorna risorse) per scoprire le risorse disponibili sull'host.

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

   - Se il 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 e protetto, e se non viene eseguita alcuna operazione di backup, viene visualizzato il messaggio Backup non eseguito nella colonna Stato generale. In caso contrario, lo stato cambia in Backup failed (Backup non riuscito) o Backup successed (Backup riuscito) in base allo stato dell'ultimo backup.

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

Aggiungere le risorse manualmente 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 del server SnapCenter, l'aggiunta di host e l'impostazione delle connessioni al sistema di storage.

A proposito di questa attività

Il rilevamento automatico non è supportato per le seguenti configurazioni:

- Layout RDM e VMDK

Fasi

1. Nel riquadro di spostamento di sinistra, selezionare il plug-in SnapCenter per PostgreSQL dall'elenco a discesa, quindi fare clic su **risorse**.
2. Nella pagina risorse, fare clic su **Aggiungi risorse PostgreSQL**.
3. Nella pagina fornire dettagli sulle risorse, eseguire le seguenti operazioni:

Per questo campo…	Eseguire questa operazione…
Nome	Specificare il nome del cluster.
Host Name (Nome host)	Immettere il nome host.
Tipo	Selezionare cluster.
Istanza	Specificare il nome dell'istanza, che è il padre del cluster.
Credenziali	Selezionare le credenziali o aggiungere informazioni per la credenziale. Questa opzione è facoltativa.

4. Nella pagina fornire spazio di archiviazione, selezionare un tipo di archiviazione e scegliere uno o più volumi, LUN e qtree, quindi fare clic su **Salva**.

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

5. Facoltativo: Nella pagina Impostazioni risorse, per le risorse sull'host Windows, immettere coppie di valori chiave personalizzati per il plug-in PostgreSQL
6. Esaminare il riepilogo, quindi fare clic su **fine**.

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

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

"Aggiungere un utente o un gruppo e assegnare ruolo e risorse"

Al termine

- Dopo aver aggiunto i cluster, è possibile modificare i dettagli del cluster PostgreSQL.
- Le risorse migrate (tablespace e cluster) da SnapCenter 5,0 verranno contrassegnate come tipo di cluster PostgreSQL in SnapCenter 6,0.

- Quando si modificano le risorse aggiunte manualmente migrate da SnapCenter 5,0 o versioni precedenti, effettuare le seguenti operazioni nella pagina **Impostazioni risorse** per le coppie di valori chiave personalizzate:
  - Specificare il termine "PORTA" nel campo **Nome**.
  - Specificare il numero di porta nel campo **valore**.

Creare criteri di backup per PostgreSQL

Prima di utilizzare SnapCenter per eseguire il backup delle risorse PostgreSQL, è necessario creare un criterio di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup. Un criterio di backup è un insieme di regole che regolano la gestione, la pianificazione e la conservazione dei backup.

Prima di iniziare

- È necessario aver definito la strategia di backup.

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

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

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

A proposito di questa attività

- SnapLock
  - Se è selezionata l'opzione "conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere minore o uguale ai giorni di conservazione menzionati.
  - La specifica di un periodo di blocco dello snapshot impedisce l'eliminazione degli snapshot fino alla scadenza del periodo di conservazione. Ciò potrebbe portare a mantenere un numero maggiore di snapshot rispetto al conteggio specificato nel criterio.
  - Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Le impostazioni SnapLock primarie vengono gestite nel criterio di backup SnapCenter e le impostazioni SnapLock secondarie vengono gestite da ONTAP.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **nuovo**.
4. Nella pagina Name (Nome), immettere il nome e la descrizione della policy.
5. Nella pagina tipo di criterio, effettuare le seguenti operazioni:

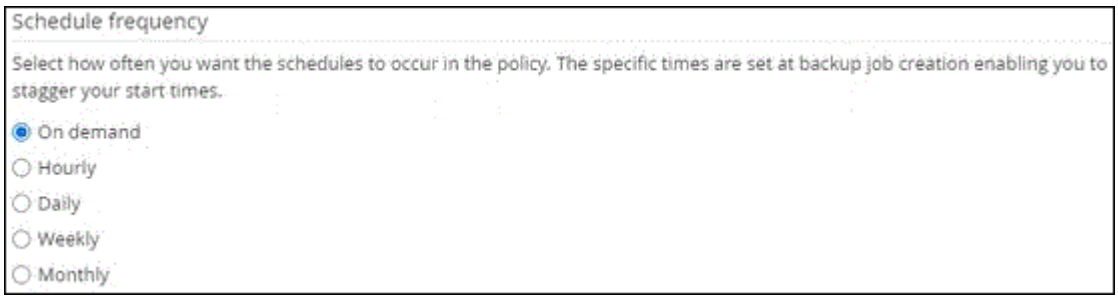
a. Selezionare il tipo di archiviazione.

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

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

6. Nella pagina istantanea, specificare il tipo di pianificazione selezionando **su richiesta**, **orario**, **giornaliero**, **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 frequenza di backup, ma consente anche di assegnare diverse pianificazioni di backup a ogni policy.



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

7. Nella sezione Impostazioni istantanea, specificare il numero di istantanee che si desidera conservare.
8. Nella pagina conservazione, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina tipo di backup:

Se si desidera…	Quindi…
Conservare un certo numero di snapshot	Selezionare **copie da conservare**, quindi specificare il numero di istantanee che si desidera conservare. Se il numero di istantanee supera il numero specificato, le istantanee vengono eliminate con le copie meno recenti eliminate per prime.

> Per i backup basati su copia Snapshot, è necessario impostare il numero di conservazione su 2 o superiore se si intende attivare la replica SnapVault. Se si imposta il conteggio della conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo snapshot è lo snapshot di riferimento per la relazione SnapVault finché non viene replicato nella destinazione uno snapshot più recente.

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

Creare gruppi di risorse e allegare policy

Un gruppo di risorse è il container al quale è necessario aggiungere risorse di cui si

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

A proposito di questa attività

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

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

Per questo campo…	Eseguire questa operazione…
Nome	Immettere un nome per il gruppo di risorse. Il nome del gruppo di risorse non deve superare i 250 caratteri.
Tag	Inserire una o più etichette per facilitare la ricerca del gruppo di risorse in un secondo momento. Ad esempio, se si aggiunge HR come tag a più gruppi di risorse, è possibile trovare in seguito tutti i gruppi di risorse associati al tag HR.
Utilizzare il formato del nome personalizzato per la copia dell'istantanea	Selezionare questa casella di controllo e immettere un formato del nome personalizzato che si desidera utilizzare per il nome dell'istantanea. Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un indicatore data e ora.

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

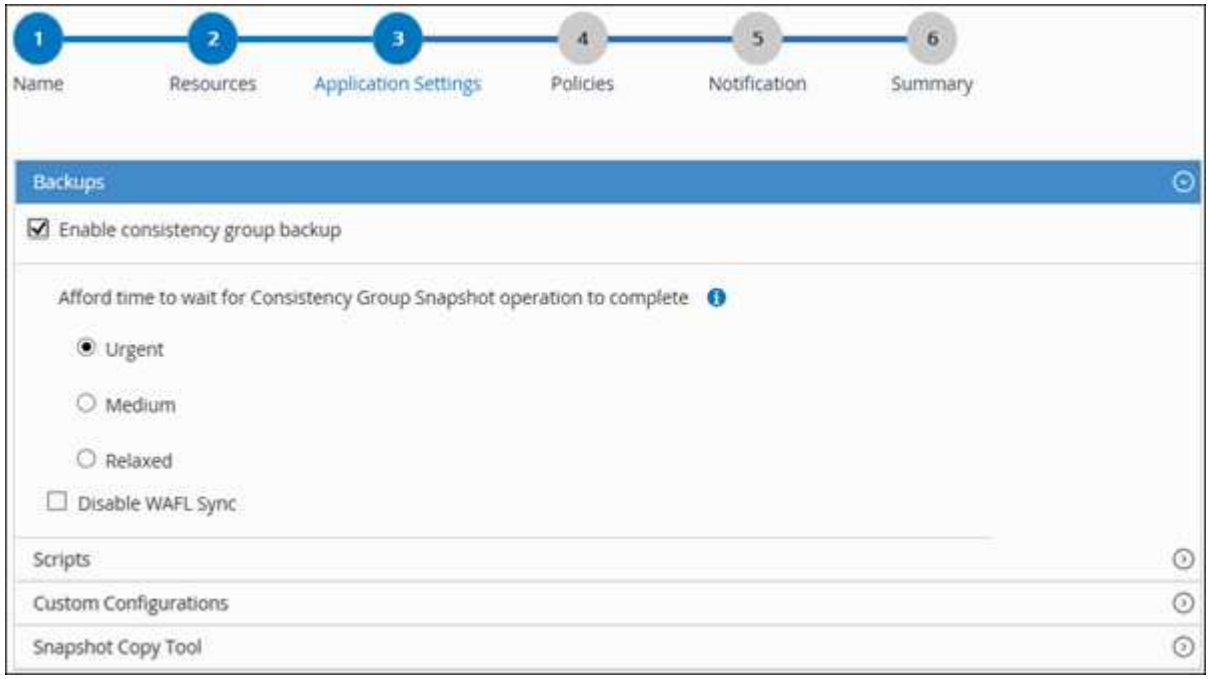
   In questo modo è possibile filtrare le informazioni sullo schermo.

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

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

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

Per questo campo…	Eseguire questa operazione…
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 snapshot. Urgente = 5 secondi, Medio = 7 secondi e rilassato = 20 secondi.
Disattiva sincronizzazione WAFL	Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL.

+ 

a. Fare clic sulla freccia **Scripts** e immettere i comandi pre e post per le operazioni quiescenza, snapshot e inquiescenza. In caso di errore, è anche possibile inserire i pre-comandi da eseguire prima di uscire.

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

Parametro	Impostazione	Descrizione
ARCHIVE_LOG_ENABLE	(S/N)	Consente alla gestione del log di archiviazione di eliminare i log di archiviazione.

Parametro	Impostazione	Descrizione
ARCHIVE_LOG_RETENTION	numero_di_giorni	Specifica il numero di giorni in cui i registri di archiviazione vengono conservati. Questa impostazione deve essere uguale o superiore a NTAP_SNAPSHOT_ RETENTIONS.
ARCHIVE_LOG_DIR	change_info_directory/logs	Specifica il percorso della directory che contiene i log di archiviazione.
ARCHIVE_LOG_EXT	estensione_file	Specifica la lunghezza dell'estensione del file di log dell'archivio. Ad esempio, se il log di archiviazione è log_backup_0_0_0_0.16151855 1942 9 e il valore di estensione_file è 5, l'estensione del log conserverà 5 cifre, ossia 16151.
ARCHIVE_LOG_RECURSIVE_ SE ARCH	(S/N)	Attiva la gestione dei log di archiviazione all'interno delle sottodirectory. Utilizzare questo parametro se i log di archiviazione si trovano nelle sottodirectory.

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

c. Fare clic sulla freccia **Snapshot Copy Tool** (strumento di copia istantanea) per selezionare lo strumento che consente di creare le istantanee:

Se vuoi…	Quindi…
SnapCenter deve utilizzare il plug-in per Windows e mettere il file system in uno stato coerente prima di creare uno snapshot. Per le risorse Linux, questa opzione non è applicabile.	Selezionare **SnapCenter with file system Consistency**.
SnapCenter per creare una snapshot a livello di storage	Selezionare **SnapCenter senza coerenza del file system**.

Se vuoi…	Quindi…
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, attenersi alla seguente procedura:
   a. Selezionare uno o più criteri dall'elenco a discesa.

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

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

   b. Nella colonna Configura pianificazioni, fare clic su * * per il criterio che si desidera configurare.
   c. Nella finestra di dialogo Add schedules for policy *policy_name*, configurare la pianificazione, quindi fare clic su **OK**.

      Dove, policy_name è il nome del criterio selezionato.

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

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

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

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

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

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

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

Prima di iniziare

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

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

- I nomi dei sistemi di storage devono essere univoci.

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

Fasi

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

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

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

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

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

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

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

4. Aggiungere l'host di comunicazione PostgreSQL al server SnapCenter.

```
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. Impostare il percorso su 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 comando seguente.

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

Eseguire il backup di PostgreSQL

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

Prima di iniziare

- È necessario aver creato una policy di backup.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con uno storage secondario, il ruolo ONTAP assegnato all’utente dello storage deve includere il privilegio “snapmirror all”. Tuttavia, se si utilizza il ruolo “vsadmin”, il privilegio “snapmirror all” non è richiesto.
- Per le operazioni di backup basate su copie Snapshot, assicurati che tutti i cluster di tenant siano validi e attivi.
- Per i comandi pre e post per le operazioni quiescenza, Snapshot e Unquiesce, è necessario controllare 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 avrà esito negativo.

SnapCenter UI

Fasi

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

   Selezionare , quindi selezionare il nome host e il tipo di risorsa per filtrare le risorse. È quindi possibile scegliere di chiudere il riquadro del filtro.
3. Selezionare la risorsa di cui si desidera eseguire il backup.
4. Nella pagina risorsa, selezionare **Usa formato nome personalizzato per copia istantanea**, quindi immettere un formato nome personalizzato che si desidera utilizzare per il nome istantanea.

   Ad esempio, *customtext_policy_hostname* o *resource_hostname*. Per impostazione predefinita, al nome dell'istantanea viene aggiunto un indicatore data e ora.
5. Nella pagina Impostazioni applicazione, effettuare le seguenti operazioni:
   - Selezionare la freccia **Backup** per impostare opzioni di backup aggiuntive:

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

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

   - Selezionare la freccia **Scripts** per eseguire i comandi pre e post per le operazioni quiescenza, istantanea e inquiescenza.

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

Se vuoi…	**Quindi…**
SnapCenter per creare una Snapshot a livello di storage	Selezionare **SnapCenter senza coerenza del file system**.

Se vuoi…	Quindi…
SnapCenter utilizzare il plug-in per Windows per impostare lo stato coerente del file system e quindi creare una Snapshot	Selezionare **SnapCenter with file system Consistency**.
Per immettere il comando per creare un'istantanea	Selezionare **Altro**, quindi immettere il comando per creare un'istantanea.

6. Nella pagina Criteri, attenersi alla seguente procedura:

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

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

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

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

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

      policy_name è il nome del criterio selezionato.

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

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

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

8. Esaminare il riepilogo, quindi selezionare **fine**.

   Viene visualizzata la pagina della topologia delle risorse.

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

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

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

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

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

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

Cmdlet PowerShell

Fasi

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

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

   Viene visualizzato il prompt di nome utente e password.

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

   Questo esempio mostra come aggiungere un'istanza di 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 di backup, nome del backup per eseguire operazioni di ripristino o clonazione, utilizzando il cmdlet Get-SmBackupReport.

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

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

Eseguire il backup dei gruppi di risorse

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

Prima di iniziare

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

A proposito di questa attività

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

automaticamente in base alla pianificazione.

Fasi

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

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

      Se il criterio selezionato per il backup on-demand è associato a una pianificazione di backup, i backup on-demand verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.
   b. Selezionare **Backup**.
5. Monitorare l'avanzamento dell'operazione selezionando **Monitor** > **Jobs**.

Monitorare le operazioni di backup di PostgreSQL

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

A proposito di questa attività

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

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Jobs**.
3. Nella pagina lavori, attenersi alla seguente procedura:

a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
b. Specificare le date di inizio e di fine.
c. Dall'elenco a discesa **tipo**, selezionare **Backup**.
d. Dal menu a discesa **Status** (Stato), selezionare lo stato del backup.
e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.

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

> Sebbene venga visualizzato lo stato del processo di backup , quando si fa clic sui dettagli del processo, è possibile che alcune delle attività secondarie dell'operazione di backup siano ancora in corso o contrassegnate da segnali di avviso.

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

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

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

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

Il riquadro Activity (attività) visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificati.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Fare clic sul riquadro attività per visualizzare le cinque operazioni più recenti.

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

Annullare le operazioni di backup per PostgreSQL

È possibile annullare le operazioni di backup inserite nella coda.

Cosa ti serve

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

Fasi

1. Eseguire una delle seguenti operazioni:

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

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

Visualizzare i backup e i cloni di PostgreSQL nella pagina topologia

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

A proposito di questa attività

È possibile esaminare le seguenti icone nella vista Manage Copies (Gestisci copie) per determinare se i backup e i cloni sono disponibili sullo storage primario o secondario (copie Mirror o copie Vault).

- visualizza il numero di backup e cloni disponibili sullo storage primario.
- Visualizza il numero di backup e cloni su cui viene eseguito il mirroring dello storage secondario utilizzando la tecnologia SnapMirror.
- Visualizza il numero di backup e cloni replicati sullo storage secondario utilizzando la tecnologia SnapVault.

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

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

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

Fasi

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

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

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

   La sezione **scheda di riepilogo** visualizza il numero totale di backup basati su copia Snapshot e cloni.

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

   Se viene eseguito il backup abilitato SnapLock, facendo clic sul pulsante **Aggiorna** si aggiornano i tempi di scadenza SnapLock primari e secondari recuperati da ONTAP. Inoltre, una pianificazione settimanale aggiorna il tempo di scadenza SnapLock primario e secondario recuperato da ONTAP.

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

   Dopo il backup su richiesta, facendo clic sul pulsante **Refresh** (Aggiorna) vengono aggiornati i dettagli del backup o della clonazione.

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

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

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

   Non è possibile rinominare o eliminare i backup presenti nello storage secondario.

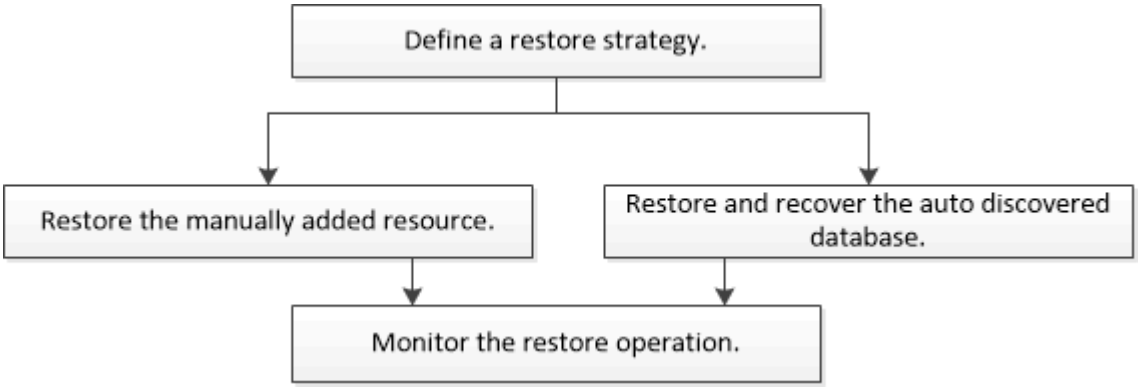
7. Se si desidera eliminare un clone, selezionarlo dalla tabella, quindi fare clic su  .
8. Se si desidera dividere un clone, selezionarlo dalla tabella e fare clic su  .

Ripristinare PostgreSQL

Ripristinare il flusso di lavoro

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

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



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

"Guida di riferimento al cmdlet del software SnapCenter".

Ripristinare e ripristinare un backup delle risorse aggiunto manualmente

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

Prima di iniziare

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

A proposito di questa attività

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

SnapCenter UI

Fasi

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

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

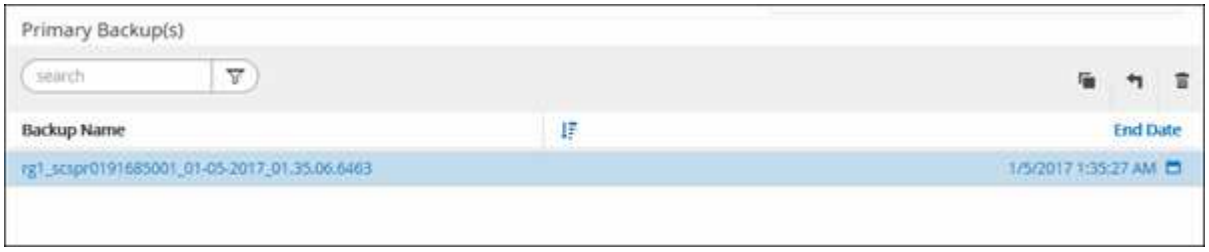
   Anche se un backup potrebbe essere per un gruppo di risorse, quando si esegue il ripristino, è necessario selezionare le singole risorse da ripristinare.

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

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

   Viene visualizzata la pagina della topologia delle risorse.

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



6. Nella pagina Ripristina ambito, selezionare **completa risorsa**.

   a. Se si seleziona **complete Resource**, vengono ripristinati tutti i volumi di dati configurati del cluster PostgreSQL.

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

      È possibile selezionare più LUN.

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

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

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

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

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

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

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

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

Cmdlet PowerShell

Fasi

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

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

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

   Questo esempio mostra informazioni su tutti i backup disponibili:

```
PS C:\> Get-SmBackup

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

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

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

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

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

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

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

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

Ripristino e ripristino di un backup del cluster rilevato automaticamente

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

Prima di iniziare

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

A proposito di questa attività

- 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 del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

Fasi

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

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

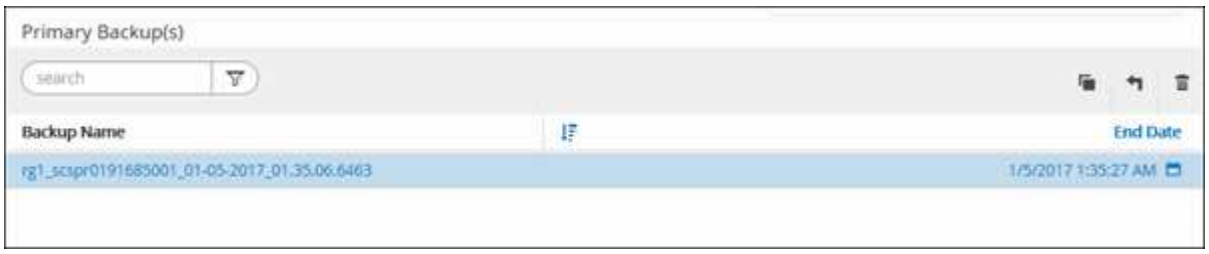
   Anche se un backup potrebbe essere per un gruppo di risorse, quando si esegue il ripristino, è necessario selezionare le singole risorse da ripristinare.

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

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

   Viene visualizzata la pagina della topologia delle risorse.

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



6. Nella pagina ambito di ripristino, selezionare **completa risorsa** per ripristinare i volumi di dati configurati del cluster PostgreSQL.
7. Nella pagina Recovery Scope (ambito ripristino), selezionare una delle seguenti opzioni:

Se…	Eseguire questa operazione…

Desidera ripristinare il più vicino possibile all'ora corrente	Selezionare **Ripristina allo stato più recente**. Per le risorse container singole, specificare una o più posizioni di backup del registro e del catalogo.
Si desidera ripristinare al punto di tempo specificato	Selezionare **Recover to point in time** (Ripristina al punto nel tempo). a. Inserire data e ora. Inserire data e ora. Ad esempio, l'host PostgreSQL Linux si trova a Sunnyvale, CA e l'utente in Raleigh, NC sta recuperando i log in SnapCenter. Se l'utente desidera eseguire un ripristino alle 5:00 . Sunnyvale, CA, quindi l'utente deve impostare il fuso orario del browser sul fuso orario dell'host PostgreSQL Linux, che è GMT-07:00 e specificare la data e l'ora come 5:00:00
Non si desidera eseguire il ripristino	Selezionare **Nessun ripristino**.

Non è possibile recuperare le risorse PostgreSQL aggiunte manualmente.

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

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

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

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

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

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

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

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

Ripristinare le risorse utilizzando i cmdlet PowerShell

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

ripristino di un backup.

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

Fasi

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

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

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

   Questo esempio mostra informazioni su tutti i backup disponibili:

```
PS C:\> Get-SmBackup

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

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

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

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

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

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

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

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

Monitorare le operazioni di ripristino di PostgreSQL

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

A proposito di questa attività

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

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

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Jobs**.
3. Nella pagina **lavori**, attenersi alla seguente procedura:
   a. Fare clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e di fine.
   c. Dall'elenco a discesa **tipo**, selezionare **Ripristina**.
   d. Dall'elenco a discesa **Status** (Stato), selezionare lo stato di ripristino.
   e. Fare clic su **Apply** (Applica) per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

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

Clona i backup delle risorse PostgreSQL

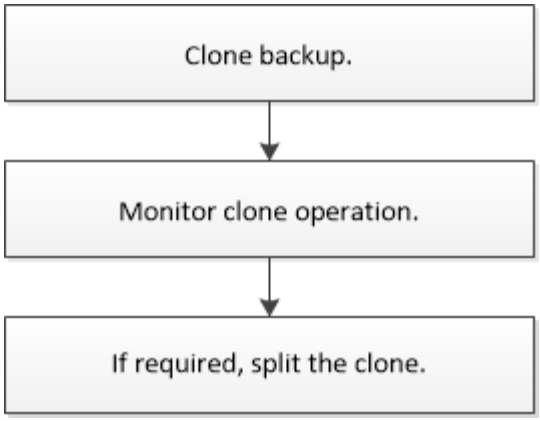
Clonare il flusso di lavoro

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

A proposito di questa attività

- È possibile clonare sul server PostgreSQL di origine.
- È possibile clonare i backup delle risorse per i seguenti motivi:
  - Per testare le funzionalità che devono essere implementate utilizzando la struttura e il contenuto delle risorse correnti durante i cicli di sviluppo delle applicazioni
  - Per l'estrazione e la manipolazione dei dati durante il popolamento dei data warehouse
  - Per ripristinare i dati cancellati o modificati per errore

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



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

Clona un backup PostgreSQL

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

Prima di iniziare

- È necessario aver eseguito il backup delle risorse o del gruppo di risorse.
- Assicurarsi che gli aggregati che ospitano i volumi siano inclusi nell'elenco degli aggregati assegnati della macchina virtuale di storage (SVM).
- Per i comandi pre-clone o post-clone, controllare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - 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 avrà esito negativo.

A proposito di questa attività

- Per informazioni sulle limitazioni delle operazioni di suddivisione clone, vedere "Guida alla gestione dello storage logico di ONTAP 9".
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli Snapshot del vault di SnapLock come parte del ripristino ereditano il tempo di scadenza del vault di SnapLock. L'amministratore dello storage dovrebbe ripulire manualmente i cloni dopo il tempo di scadenza del SnapLock.

SnapCenter UI

Fasi

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

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

3. Selezionare la risorsa o il gruppo di risorse.

   Selezionare una risorsa se si seleziona un gruppo di risorse.

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

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

Per questo campo…	Eseguire questa operazione…
Server clone	Scegliere un host su cui creare il clone.
Porta di destinazione	Immettere la porta di destinazione PostgreSQL da clonare dai backup esistenti.
NFS Export IP Address (Indirizzo IP esportazione NFS)	Inserire gli indirizzi IP o i nomi host su cui esportare i volumi clonati. Applicabile solo alla risorsa del tipo di storage NFS.
Pool di capacità max. Throughput (MIB/s)	Immettere la velocità massima di un pool di capacità. Questo è applicabile solo per la risorsa tipo di archiviazione ANF.

7. Nella pagina script, attenersi alla seguente procedura:

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

   a. Immettere i comandi per pre-clone o post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clone.
      - Comando pre-clone: Elimina i cluster esistenti con lo stesso nome
      - Comando post clone: Verifica di un cluster o avvio di un cluster.

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

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

Esempio per NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

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

È inoltre necessario specificare gli indirizzi e-mail del mittente e del destinatario e l'oggetto dell'e-mail.

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

Cmdlet PowerShell

Fasi

1. Avviare una sessione di connessione con il server SnapCenter per un utente specifico 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. Avviare un'operazione di clonazione da un backup esistente e specificare gli indirizzi IP di esportazione NFS su cui esportare i volumi clonati.

Questo esempio mostra che il backup da clonare ha un indirizzo IP NFSExportIPs di 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 NFSExportIP non viene specificato, il valore predefinito viene esportato nell'host di destinazione del clone.

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

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

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

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

Monitorare le operazioni dei cloni di PostgreSQL

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

A proposito di questa attività

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

- In corso
- Completato correttamente
- Non riuscito
- Completato con avvertenze o impossibile avviarsi a causa di avvertenze
- In coda
- Annullato

Fasi

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

Separare un clone

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

A proposito di questa attività

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

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

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

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

Fasi

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

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

3. Selezionare la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

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

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

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

   Ad esempio:

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

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

Informazioni correlate

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

Dopo l'aggiornamento di SnapCenter, eliminare o dividere i cloni del cluster PostgreSQL

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

A proposito di questa attività

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

Fasi

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

   Viene visualizzata la pagina della topologia delle risorse.

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

Informazioni sul copyright

Informazioni sul marchio commerciale