Proteger PostgreSQL

SnapCenter Software 6.0

NetApp
July 23, 2024

Tabla de contenidos

Proteger PostgreSQL

Complemento de SnapCenter para PostgreSQL

Información general sobre el plugin de SnapCenter para PostgreSQL

El plugin de SnapCenter para PostgreSQL es un componente en el lado del host de NetApp SnapCenter Software que permite la gestión de protección de datos para aplicaciones de clústeres PostgreSQL. El clúster del plugin para PostgreSQL automatiza el backup, la restauración y la clonado de clústeres de PostgreSQL en el entorno de SnapCenter.

SnapCenter admite configuraciones PostgreSQL en un solo clúster y múltiples clústeres. Es posible utilizar el plugin para clústeres de PostgreSQL en entornos Linux y Windows. En entornos Windows, PostgreSQL será soportado como recurso manual.

Cuando se instala el clúster del plugin para PostgreSQL, es posible utilizar SnapCenter con la tecnología SnapMirror de NetApp para crear copias de reflejo de conjuntos de backups en otro volumen. También es posible utilizar el plugin con la tecnología SnapVault de NetApp para realizar replicaciones de backup disco a disco para cumplimiento de normativas.

El complemento de SnapCenter para PostgreSQL es compatible con NFS y SAN en distribuciones de almacenamiento de archivos de ONTAP y Azure NetApp.

Se admite la distribución de almacenamiento virtual o VMDK.

Tareas que pueden llevarse a cabo con el plugin de SnapCenter para PostgreSQL

Cuando se instala el clúster del plugin para PostgreSQL en el entorno, es posible usar SnapCenter para realizar backup, restaurar y clonar clústeres de PostgreSQL y sus recursos. También es posible ejecutar tareas complementarias a estas operaciones.

- Añadir clústeres.
- Crear backups.
- Restaurar desde backups.
- Clonar backups.
- Programar operaciones de backup.
- Supervisar operaciones de backup, de restauración y de clonado.
- Ver informes para operaciones de backup, restauración y clonado.

Funciones del plugin de SnapCenter para PostgreSQL

SnapCenter se integra con la aplicación de plugins y con tecnologías de NetApp en el sistema de almacenamiento. Para trabajar con el plugin para clúster PostgreSQL, se utiliza la interfaz gráfica de usuario de SnapCenter.

- **Interfaz gráfica de usuario unificada**

La interfaz de SnapCenter ofrece estandarización y consistencia entre plugins y entornos. La interfaz de SnapCenter permite completar operaciones de backup, restauración y clonado consistentes entre plugins, utilizar informes centralizados, utilizar visualizaciones de consola rápidas, configurar el RBAC y supervisar trabajos en todos los plugins.

- **Administración central automatizada**

  Es posible programar operaciones de backup, configurar la retención de backup basado en políticas y realizar operaciones de restauración. También es posible supervisar de manera proactiva el entorno configurando SnapCenter para que envíe alertas por correo electrónico.

- **Tecnología de copia instantánea NetApp no disruptiva**

  SnapCenter utiliza la tecnología Snapshot de NetApp con el clúster del plugin para PostgreSQL para realizar backups de recursos.

Usar el plugin para PostgreSQL también ofrece los siguientes beneficios:

- Compatibilidad con flujos de trabajo de backup, restauración y clonado
- Seguridad compatible con RBAC y delegación de roles centralizada

  También es posible configurar las credenciales para que los usuarios de SnapCenter autorizados tengan permisos en el nivel de las aplicaciones.

- Creación de copias de recursos con gestión eficiente del espacio y en un momento específico con fines de prueba o de extracción de datos con la tecnología FlexClone de NetApp

  Se requiere una licencia de FlexClone en el sistema de almacenamiento donde desea crear el clon.

- Compatibilidad con la función Snapshot del grupo de coherencia (CG) de ONTAP como parte de la creación de backups.
- Capacidad para ejecutar varios backups de forma simultánea entre varios hosts de recursos

  En una sola operación se consolidan Snapshot cuando los recursos en un solo host comparten el mismo volumen.

- Capacidad para crear snapshots con comandos externos
- Compatibilidad con LVM de Linux en el sistema de archivos XFS.

Tipos de almacenamiento compatibles con el plugin de SnapCenter para PostgreSQL

SnapCenter es compatible con una amplia gama de tipos de almacenamiento tanto en máquinas físicas como máquinas virtuales (VM). Antes de instalar el plugin de SnapCenter para PostgreSQL, debe comprobar la compatibilidad de su tipo de almacenamiento.

Máquina	Tipo de almacenamiento
Servidores físicos y virtuales	LUN conectados a FC

Máquina	Tipo de almacenamiento
Servidor físico	LUN conectados a iSCSI
Servidores físicos y virtuales	Volúmenes conectados en NFS

Privilegios mínimos de ONTAP requeridos para el plugin de PostgreSQL

Los privilegios mínimos requeridos de ONTAP varían en función de los plugins de SnapCenter que utilice para la protección de datos.

- Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.3.0 y versiones posteriores
  - event generate-autosupport-log
  - se muestra el historial del trabajo
  - detención de trabajo
  - lun
  - lun create
  - lun create
  - lun create
  - eliminación de lun
  - igroup de lun añadido
  - crear lun igroup
  - lun igroup eliminado
  - cambio de nombre de lun igroup
  - cambio de nombre de lun igroup
  - lun igroup show
  - asignación de lun de nodos adicionales
  - se crea la asignación de lun
  - se elimina la asignación de lun
  - asignación de lun quitar nodos de generación de informes
  - se muestra el mapa de lun
  - modificación de lun
  - movimiento de lun en volumen
  - lun desconectada
  - lun conectada
  - reserva persistente de lun clara
  - cambio de tamaño de lun
  - serie de lun
  - muestra de lun

- regla adicional de la política de snapmirror
- regla de modificación de la política de snapmirror
- regla de eliminación de la política de snapmirror
- la política de snapmirror
- restauración de snapmirror
- de snapmirror
- historial de snapmirror
- actualización de snapmirror
- conjunto de actualizaciones de snapmirror
- destinos de listas de snapmirror
- versión
- crear el clon de volumen
- show de clon de volumen
- inicio de división de clon de volumen
- detención de división de clon de volumen
- cree el volumen
- destrucción del volumen
- crear el archivo de volumen
- uso show-disk del archivo de volumen
- volumen sin conexión
- volumen en línea
- modificación del volumen
- crear el qtree de volúmenes
- eliminación de qtree de volumen
- modificación del qtree del volumen
- se muestra volume qtree
- restricción de volumen
- visualización de volumen
- crear snapshots de volumen
- eliminación de snapshots de volumen
- modificación de las copias de snapshot de volumen
- modificación de snapshot de volumen: snaplock: tiempo de caducidad
- cambio de nombre de copias de snapshot de volumen
- restauración de copias snapshot de volumen
- archivo de restauración de snapshots de volumen
- visualización de copias de snapshot de volumen
- desmonte el volumen

- vserver cifs
- vserver cifs share create
- eliminación de vserver cifs share
- se muestra vserver shadowcopy
- visualización de vserver cifs share
- visualización de vserver cifs
- política de exportación de vserver
- creación de política de exportación de vserver
- eliminación de la política de exportación de vserver
- creación de reglas de política de exportación de vserver
- aparece la regla de política de exportación de vserver
- visualización de la política de exportación de vserver
- vserver iscsi
- se muestra la conexión iscsi del vserver
- se muestra vserver

- Comandos de solo lectura: Privilegios mínimos requeridos para ONTAP 8.3.0 y versiones posteriores
  - interfaz de red
  - se muestra la interfaz de red
  - vserver

Preparar sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para PostgreSQL

Es posible utilizar un complemento de SnapCenter con la tecnología SnapMirror de ONTAP para crear copias de reflejo de conjuntos de backups en otro volumen, y con la tecnología ONTAP SnapVault para realizar replicaciones de backup disco a disco para cumplimiento de normativas y otros fines relacionados con la gobernanza. Antes de ejecutar estas tareas, debe configurar una relación de protección de datos entre los volúmenes de origen y de destino, e inicializar la relación.

SnapCenter realiza las actualizaciones a SnapMirror y SnapVault después de que finaliza la operación de Snapshot. Las actualizaciones de SnapMirror y SnapVault se realizan como parte del trabajo de SnapCenter; no cree una programación de ONTAP aparte.

Si llegó a SnapCenter desde un producto NetApp SnapManager y está satisfecho con las relaciones de protección de datos que ha configurado, puede omitir esta sección.

Una relación de protección de datos replica los datos en el almacenamiento primario (el volumen de origen) en el almacenamiento secundario (el volumen de destino). Cuando se inicializa la relación, ONTAP transfiere los bloques de datos a los que se hace referencia en el volumen de origen al volumen de destino.

SnapCenter no admite relaciones en cascada entre volúmenes de SnapMirror y SnapVault (**Primary** > **Mirror** > **Vault**). Debe utilizar las relaciones con fanout.

SnapCenter permite la gestión de relaciones de SnapMirror de versión flexible. Si quiere información detallada sobre las relaciones de SnapMirror con versión flexible y sobre cómo configurarlas, consulte "Documentación de ONTAP".

Estrategia de backup para PostgreSQL

Defina una estrategia de backup para PostgreSQL

Definir una estrategia de backup antes de crear las tareas de backup ayuda a garantizar que se cuente con todos los backups necesarios para restaurar o clonar correctamente los recursos. La estrategia de backup queda determinada principalmente por el SLA, el RTO y el RPO.

Acerca de esta tarea

Un acuerdo de nivel de servicio define el nivel de servicio que se espera y aborda varios problemas vinculados con el servicio, como su disponibilidad y rendimiento. El objetivo de tiempo de recuperación es el plazo de recuperación después de una interrupción del servicio. El RPO define la estrategia respecto de la antigüedad de los archivos que se deben recuperar del almacenamiento de backup para reanudar las operaciones regulares después de un fallo. El acuerdo de nivel de servicio, el objetivo de tiempo de recuperación y el RPO ayudan a establecer una estrategia de protección de datos.

Pasos

1. Determinar cuándo se debe realizar el backup de los recursos.
2. Decidir cuántas tareas de backup se necesitan.
3. Decidir el nombre que se asignará a los backups.
4. Decidir si se desea crear una política basada en copias de Snapshot para realizar backup de copias de Snapshot consistentes con las aplicaciones del clúster.
5. Decidir si se desean usar la tecnología NetApp SnapMirror para la replicación o la tecnología NetApp SnapVault para la retención a largo plazo.
6. Determinar el período de retención para las snapshots en el sistema de almacenamiento de origen y el destino de SnapMirror.
7. Determinar si se desean ejecutar comandos antes o después de la operación de backup y proporcionar un script previo o posterior.

Detección automática de recursos en el host Linux

Los recursos son clústeres e instancias de PostgreSQL en el host Linux que son administrados por SnapCenter. Después de instalar el plugin de SnapCenter para PostgreSQL, los clústeres PostgreSQL de todas las instancias de ese host Linux se detectan automáticamente y se muestran en la página Resources.

Tipo de backups admitido

El tipo de backup especifica el tipo de backup que desea crear. SnapCenter admite el tipo de backup basado en copias de Snapshot para clústeres de PostgreSQL.

Backup basado en copia de Snapshot

Los backups basados en copia de Snapshot aprovechan la tecnología de copia Snapshot de NetApp para crear copias en línea y de solo lectura de los volúmenes en los cuales residen los clústeres de PostgreSQL.

Cómo usa el plugin de SnapCenter para PostgreSQL las snapshots de grupos de consistencia

Es posible usar el plugin para crear copias Snapshot de grupos de coherencia para los grupos de recursos. Un grupo de consistencia es un contenedor que puede albergar varios volúmenes para que se gestionen como una misma entidad. Un grupo de coherencia es un conjunto de snapshots simultáneas de varios volúmenes, que ofrece copias consistentes de un grupo de volúmenes.

También es posible especificar un tiempo de espera para la controladora de almacenamiento a fin de agrupar de forma coherente las copias de Snapshot. Las opciones de tiempo de espera disponibles son **Urgent**, **Medium** y **Relaxed**. También es posible habilitar o deshabilitar la sincronización de Write Anywhere File Layout (WAFL) durante la operación de snapshot de grupos consistentes. La sincronización WAFL mejora el rendimiento de una snapshot de grupo de coherencia.

Cómo hace SnapCenter para gestionar el mantenimiento de backups de datos

SnapCenter gestiona el mantenimiento de los backups de datos en los niveles de sistema de almacenamiento y sistema de archivos.

Las instantáneas en el almacenamiento primario o secundario y sus entradas correspondientes en el catálogo PostgreSQL se eliminan de acuerdo con la configuración de retención.

Consideraciones para determinar programaciones de backup para PostgreSQL

El factor más importante para determinar una programación de backup es la tasa de cambio del recurso. Puede ser recomendable realizar el backup de un recurso muy utilizado una vez por hora, mientras que, en el caso de un recurso de poco uso, es suficiente hacerlo una vez por día. Otros factores que se deben tener en cuenta son la importancia del recurso para la organización, el SLA y el RPO.

Las programaciones de backup están compuestas por dos partes:

- Frecuencia de backup (cada cuánto se realizan los backups)

  La frecuencia de backup, también denominada tipo de programación para algunos plugins, es parte de una configuración de políticas. Por ejemplo, se puede configurar una frecuencia de backup horaria, diaria, semanal o mensual.

- Programaciones de backup (exactamente cuándo se realizan los backups)

  Las programaciones de backup forman parte de la configuración de un recurso o un grupo de recursos. Por ejemplo, si hay un grupo de recursos con una política configurada para realizar un backup semanal, es posible configurar la programación para que se realice un backup todos los jueves a las 00:10

Cantidad de tareas de backup necesarias para PostgreSQL

Algunos factores que determinan la cantidad de trabajos de backup que se necesitan son el tamaño del recurso, la cantidad de volúmenes que se usan, la tasa de cambio del recurso y el acuerdo de nivel de servicio.

Convenciones de nomenclatura de backups para clústeres del plugin para PostgreSQL

Es posible usar la convención de nomenclatura de Snapshot predeterminada o usar una convención de nomenclatura personalizada. la convención de nomenclatura de backups predeterminada añade la fecha/hora a los nombres de Snapshot, lo cual ayuda a identificar cuándo se crearon las copias.

La Snapshot usa la siguiente convención de nomenclatura predeterminada:

```
resourcegroupname_hostname_timestamp
```

Es necesario asignar un nombre a los grupos de recursos de backup de forma lógica, como en el ejemplo siguiente:

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

En este ejemplo, los elementos de la sintaxis tienen los siguientes significados:

- *dts1* es el nombre del grupo de recursos.
- *mach1x88* es el nombre de host.
- *03-12-2015_23.17.26* es la fecha y la marca de hora.

Como alternativa, es posible especificar el formato del nombre de Snapshot y proteger los recursos o grupos de recursos si se selecciona **Use custom name format for Snapshot copy**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la Snapshot.

Estrategia de restauración y recuperación para PostgreSQL

Defina una estrategia de restauración y recuperación para recursos PostgreSQL

Para poder ejecutar operaciones de restauración y recuperación correctamente, es necesario definir una estrategia antes de restaurar y recuperar un clúster.

Solo se admite la recuperación manual del clúster.

Pasos

1. Determinar las estrategias de restauración compatibles con los recursos PostgreSQL añadidos manualmente
2. Determinar las estrategias de restauración compatibles con clústeres PostgreSQL detectados automáticamente
3. Decidir el tipo de operaciones de recuperación que se desea ejecutar.

Tipos de estrategias de restauración compatibles con los recursos PostgreSQL añadidos manualmente

Para poder ejecutar correctamente las operaciones de restauración, es necesario definir una estrategia mediante SnapCenter.

No se pueden recuperar recursos PostgreSQL añadidos manualmente.

Restauración de recursos completa

- Restaura todos los volúmenes, qtrees y LUN de un recurso

Si el recurso contiene volúmenes o qtrees, las copias de Snapshot tomadas después de la copia de Snapshot seleccionada para restaurar en los volúmenes o qtrees se eliminan y no pueden recuperarse. Además, si hay algún otro recurso alojado en los mismos volúmenes o qtrees, también se lo elimina.

NOTA: El plugin para PostgreSQL crea una etiqueta de copia de seguridad y un mapa de tablespace en la carpeta */<OS_temp_folder>/postgresql_sc_recovery*<Restore_JobId>/_ para ayudar a recuperar manualmente.

Tipo de estrategia de restauración compatible con PostgreSQL detectado automáticamente

Para poder ejecutar correctamente las operaciones de restauración, es necesario definir una estrategia mediante SnapCenter.

La restauración completa de recursos es la estrategia de restauración compatible con los clústeres de PostgreSQL detectados automáticamente. Esto restaura todos los volúmenes, qtrees y LUN de un recurso.

Tipos de operaciones de restauración para PostgreSQL auto descubierta

El plugin de SnapCenter para PostgreSQL es compatible con SnapRestore de archivo único, y los tipos de restauración por conexión y copia para los clústeres de PostgreSQL detectados automáticamente.

Single File SnapRestore se realiza en entornos NFS en los siguientes casos:

- Si solo se selecciona la opción **Complete Resource**
- Cuando la copia de seguridad seleccionada se realiza desde una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **completar recurso**

Single File SnapRestore se realiza en entornos SAN en los siguientes casos:

- Si solo se selecciona la opción **Complete Resource**
- Cuando se selecciona la copia de seguridad de una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **Complete Resource**

Tipos de operaciones de recuperación compatibles con los clústeres PostgreSQL

SnapCenter permite ejecutar diferentes tipos de operaciones de recuperación para clústeres de PostgreSQL.

- Recupere el clúster hasta el estado más reciente
- Recupere el clúster hasta un momento específico

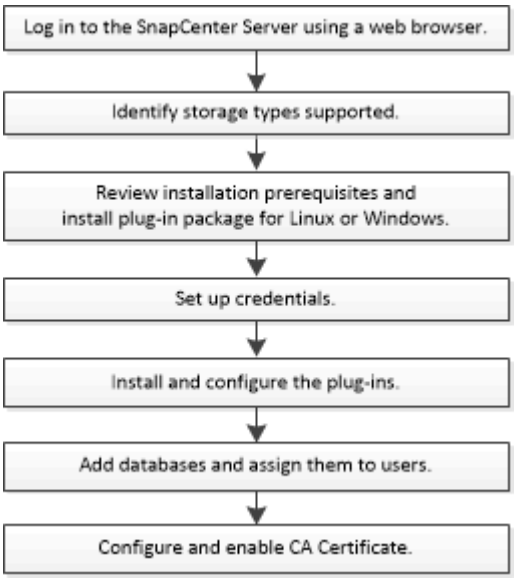
  Debe especificar la fecha y la hora de la recuperación.

SnapCenter también proporciona la opción No recovery para los clústeres PostgreSQL.

Prepare la instalación del plugin de SnapCenter para PostgreSQL

Flujo de trabajo de instalación del plugin de SnapCenter para PostgreSQL

Debe instalar y configurar el plugin de SnapCenter para PostgreSQL si desea proteger los clústeres de PostgreSQL.



Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para PostgreSQL

Antes de añadir un host e instalar los paquetes de plugins, debe cumplir con todos los requisitos. El complemento SnapCenter para PostgreSQL está disponible en entornos Windows y Linux.

- Debe haber instalado Java 11 en el host.

  IBM Java no es compatible.

- Para Windows, el plugin Creator Service debe ejecutarse con el usuario de Windows 'LocalSystem', que es el comportamiento predeterminado cuando el plugin para PostgreSQL se instala como administrador de dominio.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está integrada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host. El plugin de SnapCenter para Microsoft Windows se pondrá en marcha de forma predeterminada con el plugin

PostgreSQL en hosts de Windows.

- El servidor de SnapCenter debe tener acceso al puerto 8145 o un puerto personalizado de plugin para el host de PostgreSQL.

Host Windows

- Debe tener un usuario de dominio con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto.
- Al instalar el plugin para PostgreSQL en un host de Windows, el plugin de SnapCenter para Microsoft Windows se instala automáticamente.
- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 11 en el host de Windows.

  "Descargas de Java para todos los sistemas operativos"

  "Herramienta de matriz de interoperabilidad de NetApp"

Hosts Linux

- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 11 en el host Linux.

  "Descargas de Java para todos los sistemas operativos"

  "Herramienta de matriz de interoperabilidad de NetApp"

- Para los clústeres PostgreSQL que se ejecutan en un host Linux, cuando se instala el plugin para PostgreSQL, el plugin de SnapCenter para UNIX se instala de forma automática.
- Debe tener **bash** como shell por defecto para la instalación del plug-in.

Comandos suplementarios

Para ejecutar un comando complementario en el plugin de SnapCenter para PostgreSQL, debe incluirlo en `allowed_commands.config` el archivo.

`allowed_commands.config` El archivo está ubicado en el subdirectorio «etc» del directorio del plugin de SnapCenter para PostgreSQL.

Host Windows

Valor predeterminado: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

Ruta personalizada: `<Custom_Directory>\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`

Hosts Linux

Valor predeterminado: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`

Ruta personalizada: `<Custom_Directory>allowed_commands.config`

Para permitir comandos complementarios en el host del plugin, abra `allowed_commands.config` archivo en un editor. Introduzca cada comando en una línea independiente. No distingue mayúsculas de minúsculas. Por ejemplo:

comando: mount

comando: umount

Asegúrese de especificar el nombre de ruta completo. El nombre de ruta debe escribirse entre comillas si contiene espacios. Por ejemplo:

Comando: «C:\Program Files\NetApp\SnapCreator commands\sdcli.exe»

comando: myscript.bat

Si la `allowed_commands.config` el archivo no está presente, los comandos o la ejecución del script se bloquearán y el flujo de trabajo fallará con el siguiente error:

ejecución '[/mnt/mount -a] no permitida. Autorizar agregando el comando en el archivo %s en el host del plugin.

Si el comando o el script no está presente en `allowed_commands.config`, el comando o la ejecución del script se bloqueará y el flujo de trabajo fallará con el siguiente error:

ejecución '[/mnt/mount -a] no permitida. Autorizar agregando el comando en el archivo %s en el host del plugin.

No debe utilizar una entrada comodín (*) para permitir todos los comandos.

Configure privilegios sudo para usuarios que no son raíz para el host Linux

SnapCenter 2.0 y versiones posteriores permiten que un usuario no raíz instale el paquete de plugins de SnapCenter para Linux e inicie el proceso del plugin. Los procesos del plug-in se ejecutan como un usuario efectivo que no es raíz. Tiene que configurar los privilegios sudo para el usuario que no sea raíz con el fin de ofrecer acceso a varias rutas.

Lo que necesitará

- Sudo versión 1.8.7 o posterior.
- Para el usuario que no es root, asegúrese de que el nombre del usuario que no es root y del grupo del usuario debe ser el mismo.
- Edite el archivo */etc/ssh/sshd_config* para configurar los algoritmos de código de autenticación de mensajes: Macs hmac-sha2-256 y MACs hmac-sha2-512.

  Reinicie el servicio sshd después de actualizar el archivo de configuración.

  Ejemplo:

```
#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
```

Acerca de esta tarea

Tiene que configurar los privilegios sudo para usuarios que no son raíz con el fin de ofrecer acceso a las rutas siguientes:

- /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
- Pasos*
  1. Inicie sesión en el host Linux en el que desee instalar el paquete de plugins de SnapCenter para Linux.
  2. Añada las siguientes líneas al archivo /etc/sudoers mediante la función visudo de 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/Con
fig_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
```

Si tiene una configuración de RAC, junto con otros comandos permitidos, debe agregar lo siguiente al archivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Puede obtener el valor de *crs_home* del archivo */etc/oracle/olr.loc*.

LINUX_USER es el nombre del usuario que no es raíz que ha creado.

Puede obtener el *checksum_value* del archivo **sc_unix_plugins_checksum.txt**, que se encuentra en:

- _C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _ si el servidor SnapCenter está instalado en el host de Windows.
- _/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ si el servidor SnapCenter está instalado en el host Linux.

Se debe utilizar el ejemplo solo como referencia para crear sus propios datos.

Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows

Antes de instalar el paquete de plugins de SnapCenter para Windows, debe estar familiarizado con algunos requisitos básicos de espacio y tamaño del sistema host.

Elemento	Requisitos
Sistemas operativos	Microsoft Windows Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".
RAM mínima para el plugin de SnapCenter en el host	1 GB
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	5 GB Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía en función de la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente.

Elemento	Requisitos
Paquetes de software obligatorios	• DOTNET Core 8.0.5 • PowerShell Core 7.4.2 Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet."

Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux

Antes de instalar el paquete de plugins de SnapCenter para Linux, tiene que conocer bien algunos requisitos básicos de espacio y tamaño del sistema host.

Elemento	Requisitos
Sistemas operativos	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".
RAM mínima para el plugin de SnapCenter en el host	1 GB
Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host	2 GB Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía, según la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente.

Elemento	Requisitos
Paquetes de software obligatorios	Java 11 Oracle Java y OpenJDK Si ha actualizado JAVA a la versión más reciente, debe asegurarse de que la opción JAVA_HOME ubicada en /var/opt/snapcenter/spl/etc/spl.properties esté configurada en la versión DE JAVA correcta y en la ruta de acceso correcta. Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Configure credenciales para el plugin de SnapCenter para PostgreSQL

SnapCenter utiliza credenciales para autenticar usuarios para las operaciones de SnapCenter. Debe crear credenciales para instalar los plugins de SnapCenter, y credenciales adicionales para realizar operaciones de protección de datos en clústeres o sistemas de archivos Windows.

Acerca de esta tarea

- Hosts Linux

  Debe configurar credenciales para instalar plugins en hosts Linux.

  Debe configurar las credenciales para el usuario raíz o un usuario que no sea raíz que tenga privilegios sudo para instalar e iniciar el proceso del plugin.

  Práctica recomendada: aunque se permite crear credenciales para Linux después de implementar hosts e instalar plugins, la práctica recomendada es crear credenciales después de añadir SVM, antes de implementar hosts e instalar plugins.

- Host Windows

  Debe configurar credenciales de Windows antes de instalar plugins.

  Debe configurar las credenciales con privilegios de administrador, incluidos los derechos de administrador en el host remoto.

Si se configuran las credenciales para grupos de recursos individuales y el nombre de usuario no tiene privilegios de administrador completos, debe asignar al menos los privilegios de grupo de recursos y backup al nombre de usuario.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
2. En la página Settings, haga clic en **Credential**.
3. Haga clic en **Nuevo**.
4. En la página Credential, especifique la información necesaria para configurar las credenciales:

Para este campo…	Realice lo siguiente…
Nombre de credencial	Introduzca un nombre para las credenciales.
Nombre de usuario	Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación. • Administrador de dominio o cualquier miembro del grupo de administradores Especifique el administrador de dominio o cualquier miembro del grupo de administrador en el sistema en el que va a instalar el plugin de SnapCenter. Los formatos válidos para el campo Nombre de usuario son: ◦ *NetBIOS\Username* ◦ *Domain FQDN\Username* • Administrador local (sólo para grupos de trabajo) Para los sistemas que pertenecen a un grupo de trabajo, especifique el administrador local integrado en el sistema en el que va a instalar el plugin de SnapCenter. Puede especificar una cuenta de usuario local que pertenezca al grupo de administradores local si la cuenta de usuario tiene privilegios elevados o si la función de control de acceso de usuario está desactivada en el sistema host. El formato válido para el campo Username es: *Username* No utilice comillas dobles (") ni marcas de retroceso (') en las contraseñas. No debe usar el signo menos de (<) y el signo de exclamación (!) los símbolos juntos en las contraseñas. Por ejemplo, arrendhan<!10, les10<!, backtick'12.
Contraseña	Introduzca la contraseña usada para autenticación.
Modo de autenticación	Seleccione el modo de autenticación que desea utilizar.
Use privilegios sudo	Seleccione la casilla de verificación **Use sudo Privileges** si va a crear credenciales para usuarios que no son raíz. Aplicable únicamente a usuarios Linux.

5. Haga clic en **Aceptar**.

Después de terminar de configurar las credenciales, se recomienda asignar el mantenimiento de credenciales a un usuario o un grupo de usuarios en la página User and Access.

Configurar GMSA en Windows Server 2016 o posterior

Windows Server 2016 o posterior le permite crear una cuenta de servicio administrado de grupo (GMSA) que proporciona gestión automatizada de contraseñas de cuenta de servicio desde una cuenta de dominio administrado.

Antes de empezar

- Debe tener un controlador de dominio de Windows Server 2016 o posterior.
- Debe tener un host de Windows Server 2016 o posterior, que es miembro del dominio.

Pasos

1. Cree una clave raíz KDS para generar contraseñas únicas para cada objeto de su GMSA.
2. Para cada dominio, ejecute el siguiente comando desde el controlador de dominio de Windows: Add-KDSRootKey -EffectiveImmediately
3. Crear y configurar su GMSA:
   a. Cree una cuenta de grupo de usuarios con el siguiente formato:

```
 domainName\accountName$
.. Agregar objetos de equipo al grupo.
.. Utilice el grupo de usuarios que acaba de crear para crear el
GMSA.
```

   Por ejemplo:

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Ejecución `Get-ADServiceAccount` comando para verificar la cuenta
de servicio.
```

4. Configure el GMSA en sus hosts:
   a. Active el módulo de Active Directory para Windows PowerShell en el host en el que desea utilizar la cuenta de GMSA.

   Para ello, ejecute el siguiente comando desde 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. Reinicie el host.

b. Instale el GMSA en su host ejecutando el siguiente comando desde el símbolo del sistema de PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique su cuenta de GMSA ejecutando el siguiente comando: `Test-AdServiceAccount <gMSA>`

5. Asigne los privilegios administrativos al GMSA configurado en el host.
6. Agregue el host de Windows especificando la cuenta GMSA configurada en el servidor SnapCenter.

   El servidor SnapCenter instalará los plugins seleccionados en el host y el GMSA especificado se utilizará como cuenta de registro de servicio durante la instalación del plugin.

Instale el plugin de SnapCenter para PostgreSQL

Añada hosts e instale paquetes de plugins en hosts remotos

Debe usar la página SnapCenter Add Host para añadir hosts y, a continuación, instalar los paquetes de los plugins. Los plugins se instalan automáticamente en hosts remotos. Puede añadir el host e instalar paquetes de plugins para un host individual.

Antes de empezar

- Si el sistema operativo del host de SnapCenter Server es Windows 2019 y el sistema operativo del host del plugin es Windows 2022, debe realizar lo siguiente:
  - Actualice a Windows Server 2019 (compilación del sistema operativo 17763,5936) o posterior
  - Actualice a Windows Server 2022 (compilación del sistema operativo 20348,2402) o posterior
- Debe ser un usuario al que se ha asignado una función que tenga permisos de instalación y desinstalación de plugins, como el rol de administrador de SnapCenter.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está incorporada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.

- Debe asegurarse de que el servicio de cola de mensajes está en ejecución.
- La documentación de administración contiene información sobre la gestión de los hosts.
- Si está utilizando la cuenta de servicio gestionado en grupo (GMSA), debe configurar GMSA con privilegios administrativos.

  "Configure la cuenta de servicio administrada de grupo en Windows Server 2016 o posterior para PostgreSQL"

Acerca de esta tarea

- No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
3. Haga clic en **Agregar**.
4. En la página hosts, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Tipo de host	Seleccione el tipo de host: • Windows • Linux El plugin para PostgreSQL está instalado en el host de cliente PostgreSQL, y este host puede estar en un sistema Windows o Linux.
Nombre de host	Introduzca el nombre de host de comunicación. Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host. SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el FQDN.

Para este campo…	Realice lo siguiente…
Credenciales	Seleccione el nombre de credencial que ha creado o cree nuevas credenciales. Las credenciales deben tener derechos de administrador en el host remoto. Para obtener más detalles, consulte la información acerca de crear credenciales. Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha proporcionado. El modo de autenticación de las credenciales se determina por el tipo de host que especifique en el asistente Add host.

5. En la sección Select Plug-ins to Install, seleccione los plugins que desea instalar.

   Mientras utiliza la API de REST para instalar el plugin para PostgreSQL, debe pasar la versión como 3,0. Por ejemplo, PostgreSQL:3,0

6. (Opcional) haga clic en **más opciones**.

Para este campo…	Realice lo siguiente…
Puerto	Conserve el número de puerto predeterminado o especifique el número de puerto. El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado. Si ha instalado plugins manualmente y ha especificado un puerto personalizado, debe especificar el mismo puerto. De lo contrario, la operación dará error.

Para este campo…	Realice lo siguiente…
Ruta de instalación	El plugin para PostgreSQL está instalado en el host de cliente PostgreSQL, y este host puede estar en un sistema Windows o Linux. • En el caso del paquete de plugins de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\NetApp\SnapCenter. Opcionalmente, puede personalizar la ruta. • Para el paquete de plugins de SnapCenter para Linux, la ruta predeterminada es /opt/NetApp/snapcenter. Opcionalmente, puede personalizar la ruta.
Omitir comprobaciones previas a la instalación	Seleccione esta casilla de comprobación si ya ha instalado los plugins manualmente y no desea validar si el host cumple con los requisitos para la instalación del plugin.
Añada todos los hosts del clúster	Seleccione esta casilla de comprobación para añadir todos los nodos del clúster.
Utilice Group Managed Service Account (GMSA) para ejecutar los servicios de plug-in	En el caso de host de Windows, seleccione esta casilla de comprobación si desea utilizar una cuenta de servicio gestionado de grupo (GMSA) para ejecutar los servicios de plugin. Proporcione el nombre de GMSA con el siguiente formato: Nombre_de_dominio\accountName$. GMSA se utilizará como cuenta de servicio de inicio de sesión solo en el complemento SnapCenter para el servicio de Windows.

7. Haga clic en **Enviar**.

   Si no ha seleccionado la casilla de comprobación Skip prechecks, el host se valida para comprobar si cumple con los requisitos para la instalación del plugin. El espacio en disco, RAM, versión de PowerShell, versión de .NET, ubicación (para plugins de Windows) y versión de Java (para plugins de Linux) se validan frente a los requisitos mínimos. Si no se satisfacen los requisitos mínimos, se muestran los mensajes de error o advertencia correspondientes.

   Si el error está relacionado con el espacio en disco o RAM, es posible actualizar el archivo web.config ubicado en C:\Program Files\NetApp\SnapCenter WebApp para modificar los valores predeterminados. Si el error está relacionado con otros parámetros, primero debe solucionar el problema.

En una configuración de alta disponibilidad, si actualiza el archivo web.config, debe actualizar el archivo en ambos nodos.

8. Si el tipo de host es Linux, verifique la huella digital y, a continuación, haga clic en **Confirmar y enviar**.

   En una configuración de clúster, debe comprobar la huella de cada uno de los nodos del clúster.

   La verificación de huellas digitales es obligatoria aunque se haya añadido anteriormente el mismo host a SnapCenter y se haya confirmado la huella.

9. Supervise el progreso de la instalación.
   - Para el plugin de Windows, los registros de instalación y actualización se encuentran en: *C:\Windows\SnapCenter plugin\Install*<JOBID>_
   - Para el plugin de Linux, los registros de instalación se encuentran en: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log_ y los registros de actualización se encuentran en: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log_

Instale paquetes de plugins de SnapCenter para Linux o Windows en varios hosts remotos mediante cmdlets

Puede instalar los paquetes de plugins de SnapCenter para Linux o Windows en varios hosts a la vez mediante el cmdlet de PowerShell Install-SmHostPackage.

Antes de empezar

Debe haberse registrado en SnapCenter como usuario del dominio con derechos de administrador local en cada host en el que desee instalar el paquete de plugins.

Pasos

1. Inicie PowerShell.
2. En el host de SnapCenter Server, establezca una sesión mediante el cmdlet Open-SmConnection y, a continuación, introduzca sus credenciales.
3. Instale el plugin en varios hosts mediante el cmdlet Install-SmHostPackage y los parámetros requeridos.

   La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

   Puede utilizar la opción -skipprecheck cuando haya instalado los plugins manualmente y no quiera validar si el host cumple los requisitos para instalar el plugin.

4. Introduzca sus credenciales para la instalación remota.

Instale el plugin de SnapCenter para PostgreSQL en hosts Linux mediante la interfaz de la línea de comandos

Debe instalar el plugin de SnapCenter para clúster PostgreSQL mediante la interfaz de usuario de SnapCenter. Si el entorno no permite la instalación remota del plugin desde la interfaz de usuario de SnapCenter, puede instalar el plugin para clúster PostgreSQL en el modo de consola o en el modo silencioso mediante la interfaz de línea de comandos

(CLI).

Antes de empezar

- Debe instalar el clúster del plugin para PostgreSQL en cada host Linux en el que resida el cliente PostgreSQL.
- El host Linux en el que se instala el plugin de SnapCenter para PostgreSQL debe cumplir con los requisitos dependientes de software, clúster y sistema operativo.

  La herramienta de matriz de interoperabilidad (IMT) contiene la última información sobre las configuraciones soportadas.

  "Herramienta de matriz de interoperabilidad de NetApp"

- El plugin de SnapCenter para el clúster PostgreSQL forma parte del paquete de plugins de SnapCenter para Linux. Antes de instalar el paquete de plugins de SnapCenter para Linux, debe haber instalado SnapCenter en un host de Windows.

Pasos

1. Copie el archivo de instalación del paquete de plugins de SnapCenter para Linux (snapcenter_linux_host_plugin.bin) desde C:\ProgramData\NetApp\SnapCenter\Package Repository en el host en el que desea instalar el plugin para PostgreSQL.

   Puede acceder a esta ruta desde el host en el que está instalado el servidor SnapCenter.

2. Desde el símbolo del sistema, desplácese hasta el directorio en el que copió el archivo de instalación.
3. Instale el plugin: `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 indica el puerto de comunicación HTTPS de SMCore.
   - -DSERVER_IP indica la dirección IP del servidor SnapCenter.
   - -DSERVER_HTTPS_PORT indica el puerto HTTPS del servidor SnapCenter.
   - -DUSER_INSTALL_DIR indica el directorio en el que desea instalar el paquete de plugins de SnapCenter para Linux.
   - DINSTALL_LOG_NAME indica el nombre del archivo de registro.

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

4. Edite el archivo /<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties y, a continuación, añada el parámetro PLUGINS_ENABLED = PostgreSQL:3,0.
5. Añada el host al servidor de SnapCenter con el cmdlet Add-Smhost y los parámetros requeridos.

   La información relativa a los parámetros que se pueden utilizar con el comando y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Supervise el estado de instalación del plugin para PostgreSQL

Puede supervisar el progreso de la instalación del paquete de plugins de SnapCenter mediante la página Jobs. Tal vez desee comprobar el progreso de la instalación para determinar si está completo o si hay algún problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **Jobs**, para filtrar la lista de modo que solo se enumeren las operaciones de instalación de plug-in, haga lo siguiente:
   a. Haga clic en **filtro**.
   b. Opcional: Indique las fechas de inicio y finalización.
   c. En el menú desplegable Tipo, seleccione **instalación Plug-in**.
   d. En el menú desplegable de estado, seleccione el estado de instalación.
   e. Haga clic en **aplicar**.
4. Seleccione el trabajo de instalación y haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

Configurar certificado de CA

Genere un archivo CSR de certificado de CA

Es posible generar una solicitud de firma de certificación (CSR) e importar el certificado que puede obtenerse de una entidad de certificación (CA) con la CSR generada. El certificado tendrá una clave privada asociada.

CSR es un bloque de texto codificado que se da a un proveedor de certificados autorizado para obtener el certificado de CA firmado.

La longitud de la clave RSA del certificado de CA debe ser de 3072 bits como mínimo.

Para obtener información sobre cómo generar una CSR, consulte "Cómo generar el archivo CSR de certificado de CA".

Si posee el certificado de CA para su dominio (*.domain.company.com) o su sistema (machine1.domain.company.com), puede omitir la generación del archivo CSR del certificado de CA. Puede implementar el certificado de CA existente con SnapCenter.

Para las configuraciones de clúster, el nombre de clúster (FQDN de clúster virtual) y los respectivos nombres de host se deben mencionar en el certificado de CA. El certificado se puede actualizar rellenando el campo Nombre alternativo del sujeto (SAN) antes de obtener el certificado. Para un certificado de comodines (*.domain.company.com), el certificado contendrá implícitamente todos los nombres de host del dominio.

Importar certificados de CA

Debe importar los certificados de CA a SnapCenter Server y a los plugins de host de Windows mediante la consola de gestión de Microsoft (MMC).

Pasos

1. Vaya a la consola de administración de Microsoft (MMC) y, a continuación, haga clic en **Archivo** > **Agregar o quitar Snapin**.
2. En la ventana Agregar o quitar complementos, seleccione **certificados** y, a continuación, haga clic en **Agregar**.
3. En la ventana del complemento certificados, seleccione la opción **cuenta de equipo** y, a continuación, haga clic en **Finalizar**.
4. Haga clic en **raíz de consola** > **certificados – Equipo local** > **entidades de certificación raíz de confianza** > **certificados**.
5. Haga clic con el botón secundario en la carpeta “entidades de certificación raíz de confianza” y, a continuación, seleccione **todas las tareas** > **Importar** para iniciar el asistente de importación.
6. Complete el asistente de la siguiente manera:

En esta ventana del asistente…	Haga lo siguiente…
Importar clave privada	Seleccione la opción **Sí**, importe la clave privada y, a continuación, haga clic en **Siguiente**.
Importar formato de archivo	No realice cambios; haga clic en **Siguiente**.
Seguridad	Especifique la nueva contraseña que se utilizará para el certificado exportado y, a continuación, haga clic en **Siguiente**.
Finalización del Asistente para importación de certificados	Revise el resumen y, a continuación, haga clic en **Finalizar** para iniciar la importación.

El certificado de importación se debe empaquetar con la clave privada (los formatos admitidos son: *.pfx, *.p12 y *.p7b).

7. Repita el paso 5 para la carpeta “personal”.

Obtenga la huella digital del certificado de CA

Una huella digital de certificado es una cadena hexadecimal que identifica un certificado. La huella digital se calcula a partir del contenido del certificado mediante un algoritmo de huella digital.

Pasos

1. Realice lo siguiente en la interfaz gráfica de usuario:
   a. Haga doble clic en el certificado.
   b. En el cuadro de diálogo Certificado, haga clic en la ficha **Detalles**.
   c. Desplácese por la lista de campos y haga clic en **Thumbprint**.
   d. Copie los caracteres hexadecimales del cuadro.
   e. Quite los espacios entre los números hexadecimales.

      Por ejemplo, si la huella digital es: "a9 09 50 2d 2a e4 e4 14 33 f8 38 86 b0 0d 42 77 a3 2a 7b", después de quitar los espacios, será: "a90d8 2dd82a41433e6f83886b00d4277a32a7b".

2. Realice lo siguiente desde PowerShell:
   a. Ejecute el siguiente comando para enumerar la huella digital del certificado instalado e identificar el certificado instalado recientemente por el nombre del sujeto.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copie la huella digital.

Configure el certificado de CA con servicios de plugins de host de Windows

Debe configurar el certificado de CA con servicios de plugins del host de Windows para activar el certificado digital instalado.

Realice los siguientes pasos en el servidor de SnapCenter y en todos los hosts del plugin donde ya se hayan implementado certificados de CA.

Pasos

1. Elimine el enlace existente del certificado con el puerto 8145 predeterminado de SMCore. Para ello, ejecute el siguiente comando:

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

   Por ejemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Enlace el certificado recientemente instalado con los servicios de
   plugins del host de Windows mediante la ejecución de los siguientes
   comandos:
   ```

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

Por ejemplo:

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

Configure el certificado de CA para el servicio de plugins PostgreSQL de SnapCenter en el host Linux

Debe gestionar la contraseña del almacén de claves de los plugins personalizados y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios en el almacén de confianza de plugins personalizados y configurar la pareja de claves firmada de CA en el almacén de confianza de plugins personalizados con el servicio de plugins personalizados de SnapCenter para activar el certificado digital instalado.

Los plugins personalizados utilizan el archivo 'keystore.jks', que se encuentra en */opt/NetApp/snapcenter/scc/etc* tanto como en su almacén de confianza como en su almacén de claves.

Gestionar contraseña para el almacén de claves del plugin personalizado y el alias de la pareja de claves firmada de CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del plugin personalizado desde el archivo de propiedades del agente del plugin personalizado.

   Es el valor correspondiente a la clave 'KEYSTORE_PASS'.

2. Cambie la contraseña del almacén de claves:

```
 keytool -storepasswd -keystore keystore.jks
. Cambie la contraseña para todos los alias de las entradas de clave
privada en el almacén de claves por la misma contraseña utilizada para
el almacén de claves:
```

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

   Actualice lo mismo para el archivo key KEYSTORE_PASS en *agent.properties*.

3. Reinicie el servicio después de cambiar la contraseña.

La contraseña para el almacén de claves de plugin personalizado y para toda la contraseña de alias asociada de la clave privada debe ser la misma.

Configure los certificados intermedios o de raíz para el almacén de confianza del plugin personalizado

Debe configurar los certificados intermedios o de raíz sin la clave privada para personalizar el almacén de confianza del plugin.

Pasos

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado: /Opt/NetApp/snapcenter/scc/etc.
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

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

4. Añada un certificado raíz o intermedio:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Reinicie el servicio después de configurar los certificados raíz o
intermedios en el almacén de confianza del plugin personalizado.
```

Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado

Debe configurar la pareja de claves firmadas de CA en el almacén de confianza del plugin personalizado.

Pasos

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado /opt/NetApp/snapcenter/scc/etc.
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

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

4. Agregue el certificado de CA con clave pública y privada.

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

5. Enumere los certificados añadidos al almacén de claves.

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

6. Compruebe que el almacén de claves contiene el alias correspondiente al nuevo certificado de CA, que se añadió al almacén de claves.

7. Cambie la contraseña de clave privada añadida para el certificado de CA a la contraseña del almacén de claves.

   La contraseña predeterminada del plugin personalizado keystore es el valor de key KEYSTORE_PASS en el archivo agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Si el nombre del alias del certificado de CA es largo y contiene
   espacio o caracteres especiales ("*",","), cambie el nombre del alias
   por un nombre simple:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Configure el nombre del alias del certificado de CA en el archivo
   agent.properties.
   ```

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

8. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza del plugin personalizado.

Configurar la lista de revocación de certificados (CRL) para los plugins personalizados de SnapCenter

Acerca de esta tarea

- Los complementos personalizados de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado de los archivos CRL de los plugins personalizados de SnapCenter es ' opt/NetApp/snapcenter/scc/etc/crl'.

Pasos

1. Puede modificar y actualizar el directorio predeterminado del archivo agent.properties en función de la CLAVE CRL_PATH.

   Puede colocar más de un archivo CRL en este directorio. Los certificados entrantes se verificarán en cada CRL.

Configure el certificado de CA para el servicio de plugins PostgreSQL de SnapCenter en el host Windows

Debe gestionar la contraseña del almacén de claves de los plugins personalizados y su certificado, configurar el certificado de CA, configurar los certificados raíz o intermedios en el almacén de confianza de plugins personalizados y configurar la pareja de claves firmada de CA en el almacén de confianza de plugins personalizados con el servicio de plugins personalizados de SnapCenter para activar el certificado digital instalado.

Los plugins personalizados utilizan el archivo *keystore.jks*, que se encuentra en *C:\Program*

Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc, tanto como su almacén de confianza como su almacén de claves.

Gestionar contraseña para el almacén de claves del plugin personalizado y el alias de la pareja de claves firmada de CA en uso

Pasos

1. Puede recuperar la contraseña predeterminada del almacén de claves del plugin personalizado desde el archivo de propiedades del agente del plugin personalizado.

   Es el valor que corresponde a la clave *KEYSTORE_PASS*.

2. Cambie la contraseña del almacén de claves:

   keytool -storepasswd -keystore.jks

   > Si el comando "keytool" no se reconoce en el símbolo del sistema de Windows, reemplace el comando keytool por su ruta completa.

   C:\Archivos de programa\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore.jks

3. Cambie la contraseña para todos los alias de las entradas de clave privada en el almacén de claves por la misma contraseña utilizada para el almacén de claves:

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

   Actualice lo mismo para el archivo key KEYSTORE_PASS en *agent.properties*.

4. Reinicie el servicio después de cambiar la contraseña.

   > La contraseña para el almacén de claves de plugin personalizado y para toda la contraseña de alias asociada de la clave privada debe ser la misma.

Configure los certificados intermedios o de raíz para el almacén de confianza del plugin personalizado

Debe configurar los certificados intermedios o de raíz sin la clave privada para personalizar el almacén de confianza del plugin.

Pasos

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Busque el archivo 'keystore.jks'.
3. Enumere los certificados añadidos al almacén de claves:

   keytool -list -v -keystore.jks

4. Añada un certificado raíz o intermedio:

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

5. Reinicie el servicio después de configurar los certificados raíz o intermedios en el almacén de confianza del plugin personalizado.

Debe añadir el certificado de CA raíz y luego los certificados de CA intermedios.

Configure el par de claves firmadas de CA para el almacén de confianza del plugin personalizado

Debe configurar la pareja de claves firmadas de CA en el almacén de confianza del plugin personalizado.

Pasos

1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. Busque el archivo *keystore.jks*.
3. Enumere los certificados añadidos al almacén de claves:

   keytool -list -v -keystore.jks

4. Agregue el certificado de CA con clave pública y privada.

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

5. Enumere los certificados añadidos al almacén de claves.

   keytool -list -v -keystore.jks

6. Compruebe que el almacén de claves contiene el alias correspondiente al nuevo certificado de CA, que se añadió al almacén de claves.
7. Cambie la contraseña de clave privada añadida para el certificado de CA a la contraseña del almacén de claves.

   La contraseña predeterminada del plugin personalizado keystore es el valor de key KEYSTORE_PASS en el archivo agent.properties.

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

8. Configure el nombre del alias del certificado de CA en el archivo *agent.properties*.

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

9. Reinicie el servicio después de configurar el par de claves firmado de CA en el almacén de confianza del plugin personalizado.

Configurar la lista de revocación de certificados (CRL) para los plugins personalizados de SnapCenter

Acerca de esta tarea

- Para descargar el último archivo CRL del certificado de CA relacionado, consulte "Cómo actualizar el archivo de lista de revocación de certificados en el certificado de CA de SnapCenter".
- Los complementos personalizados de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado de los archivos CRL de los plugins personalizados de SnapCenter es *'C:\Archivos de programa\NetApp\SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

Pasos

1. Puede modificar y actualizar el directorio predeterminado del archivo *agent.properties* en función de la

CLAVE CRL_PATH.

2. Puede colocar más de un archivo CRL en este directorio.

   Los certificados entrantes se verificarán en cada CRL.

Habilite certificados de CA para plugins

Debe configurar los certificados de CA e implementar los certificados de CA en SnapCenter Server y los hosts de plugin correspondientes. Debe habilitar la validación de certificado de CA para los plugins.

Antes de empezar

- Es posible habilitar o deshabilitar los certificados de CA con el cmdlet run *set-SmCertificateSettings*.
- Puede mostrar el estado del certificado de los plugins con el *Get-SmCertificateSettings*.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Pasos

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. En la página hosts, haga clic en **Managed hosts**.
3. Seleccione uno o varios hosts de plugins.
4. Haga clic en **más opciones**.
5. Seleccione **Activar validación de certificados**.

Después de terminar

El host de la pestaña Managed hosts muestra un candado y el color del candado indica el estado de la conexión entre SnapCenter Server y el host del plugin.

- Indica que el certificado de CA no está habilitado ni asignado al host del plugin.
- Indica que el certificado de CA se ha validado correctamente.
- Indica que el certificado de CA no se ha podido validar.
- indica que no se pudo recuperar la información de conexión.

> Cuando el estado es amarillo o verde, las operaciones de protección de datos se completan correctamente.

Prepárese para la protección de datos

Requisitos previos para usar el plugin de SnapCenter para PostgreSQL

Antes de utilizar el plugin de SnapCenter para PostgreSQL, el administrador de SnapCenter debe instalar y configurar el servidor SnapCenter y ejecutar las tareas de requisitos previos.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en el servidor SnapCenter.
- Configure el entorno de SnapCenter añadiendo conexiones con el sistema de almacenamiento y creando credenciales, si es necesario.
- Instale Java 11 en su host Linux o Windows.

  Debe configurar la ruta de Java en la variable de rutas del entorno del equipo host.

- Configure SnapMirror y SnapVault si quiere realizar una replicación de backup.

Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger PostgreSQL

Antes de usar SnapCenter, es necesariol comprender ciertos conceptos básicos vinculados con las operaciones de backup, clonado y restauración que se ejecutan. El usuario interactúa con recursos, grupos de recursos y políticas para diferentes operaciones.

- Los recursos normalmente son clústeres PostgreSQL que se clonan o se incluyen en un backup mediante SnapCenter.
- Un grupo de recursos de SnapCenter es una agrupacion de recursos en un host.

  Al realizar una operación con un grupo de recursos, esta se ejecuta en los recursos definidos en el grupo de acuerdo con la programación que se especificó para dicho grupo de recursos.

  Es posible realizar un backup bajo demanda de un solo recurso o de un grupo de recursos. También puede realizar backups programados para recursos individuales y para grupos de recursos.

- Las políticas especifican la frecuencia de backup, la replicación, los scripts y otras características de las operaciones de protección de datos.

  Cuando se crea un grupo de recursos, se seleccionan una o varias políticas para él. Asimismo, puede seleccionar una política al realizar un backup bajo demanda para un recurso individual.

Un grupo de recursos se encarga de definir qué se desea proteger y cuándo se quiere proteger en términos de día y hora. Una política se encarga de definir cómo se aplica la protección. Si realiza backups de todos los clústeres, por ejemplo, puede crear un grupo de recursos que incluya todos los clústeres del host. Luego, se pueden vincular dos políticas al grupo de recursos: Una diaria y una horaria. Cuando crea el grupo de recursos y asocia las políticas, puede configurar el grupo de recursos para que lleve a cabo un backup completo a diario.

Hacer backup de recursos de PostgreSQL

Hacer backup de recursos de PostgreSQL

Es posible crear un backup de un recurso (clúster) o un grupo de recursos. El flujo de trabajo de backup incluye planificar, identificar los clústeres para backup, gestionar las políticas de backup, crear grupos de recursos y añadir políticas, crear backups y supervisar las operaciones.

Los siguientes flujos de trabajo muestran la secuencia que debe seguirse para realizar la operación de backup:

[Flujo de trabajo de backup de PostgreSQL] | *../media/db2_backup_workflow.gif*

También puede usar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración y clonado. La ayuda sobre cmdlet de SnapCenter y la información de referencia sobre cmdlet contienen más información acerca de cmdlets de PowerShell. "Guía de referencia de cmdlets de SnapCenter Software".

Detecte los clústeres automáticamente

Los recursos son clústeres PostgreSQL en el host Linux que administra SnapCenter. Es posible añadir los recursos a grupos de recursos para realizar operaciones de protección de datos después de detectar los clústeres de PostgreSQL disponibles.

Antes de empezar

- Debe haber completado ciertas tareas, como instalar SnapCenter Server, añadir hosts y configurar las conexiones del sistema de almacenamiento.
- El plugin de SnapCenter para PostgreSQL no admite la detección automática de los recursos que residen en entornos virtuales de RDM/VMDK.

Acerca de esta tarea

- Después de instalar el plugin, se detectan automáticamente todos los clústeres en ese host Linux y se muestran en la página Resources.
- Solo los clústeres se detectan automáticamente.

Los recursos de detección automática no se pueden modificar ni eliminar.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Resources** y, a continuación, seleccione el plugin para PostgreSQL de la lista.
2. En la página Resources, seleccione el tipo de recurso en la lista View.
3. (Opcional) haga clic en y, a continuación, seleccione el nombre de host.

   A continuación, puede hacer clic en para cerrar el panel de filtros.

4. Haga clic en **Actualizar recursos** para descubrir los recursos disponibles en el host.

   Los recursos se muestran junto con cierta información, como el tipo de recurso, el nombre del host, los grupos de recursos asociados, el tipo de backup, las políticas y el estado general.

   - Si el clúster está en un almacenamiento de NetApp y no está protegido, se muestra Not protected en la columna Overall Status.
   - Si el clúster se encuentra en un sistema de almacenamiento de NetApp y está protegido, y si no hay operación de backup ejecutada, se muestra Backup not run en la columna Overall Status. El estado cambiará de otro modo a Backup failed o Backup succeeded según el estado de la última copia de seguridad.

Los recursos se deben actualizar si se cambia el nombre de los clústeres fuera de SnapCenter.

Añada recursos manualmente al host del plugin

El host Windows no admite la detección automática. Debe añadir manualmente los recursos del clúster de PostgreSQL.

Antes de empezar

- Debe haber completado tareas como instalar SnapCenter Server, añadir hosts y configurar conexiones del sistema de almacenamiento.

Acerca de esta tarea

La detección automática no es compatible con las siguientes configuraciones:

- Distribución con RDM y VMDK

Pasos

1. En el panel de navegación izquierdo, seleccione el plugin de SnapCenter para PostgreSQL en la lista desplegable y, a continuación, haga clic en * Recursos *.
2. En la página Recursos, haga clic en **Agregar recursos PostgreSQL**.
3. En la página Provide Resource Details, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Nombre	Especifique el nombre del clúster.
Nombre de host	Introduzca el nombre de host.
Tipo	Seleccione el clúster.
Instancia	Especifique el nombre de la instancia, que es el elemento principal del clúster.
Credenciales	Seleccione las credenciales o agregue información para la credencial. Esto es opcional.

4. En la página Provide Storage Footprint, seleccione un tipo de almacenamiento y elija uno o más volúmenes, LUN y qtrees y, a continuación, haga clic en **Save**.

   Opcional: Puede hacer clic en el + Icono para añadir más volúmenes, LUN y qtrees desde otros sistemas de almacenamiento.

5. Opcional: En la página Resource Settings, en el caso de los recursos del host de Windows, introduzca pares de clave-valor personalizados para el plugin de PostgreSQL
6. Revise el resumen y, a continuación, haga clic en **Finalizar**.

   Los clústeres se muestran junto con información, como el nombre del host, las políticas y los grupos de recursos asociados, y el estado general

Si desea proporcionar a los usuarios acceso a los recursos, debe asignar los recursos a los usuarios. De este modo, los usuarios pueden realizar las acciones para las cuales tienen permisos sobre los activos que les asignaron.

"Añada un usuario o grupo y asigne roles y activos"

Después de terminar

- Después de añadir los clústeres, puede modificar los detalles del clúster PostgreSQL.
- Los recursos migrados (tablespace y clusters) de SnapCenter 5,0 se etiquetarán como tipo de cluster PostgreSQL en SnapCenter 6,0.
- Cuando modifique los recursos agregados manualmente que se migran desde SnapCenter 5,0 o inferior, haga lo siguiente en la página **Configuración de recursos** para pares de valor de clave personalizados:
  - Especifique el término “PUERTO” en el campo **Nombre**.
  - Especifique el número de puerto en el campo **Valor**.

Crear políticas de backup para PostgreSQL

Antes de usar SnapCenter para realizar un backup de recursos de PostgreSQL, debe crear una política de backup para el recurso o grupo de recursos que desee incluir en el backup. Una política de backup es un conjunto de reglas que rigen cómo gestionar, programar y retener backups.

Antes de empezar

- Debe tener definida una estrategia de backup.

  Para obtener más detalles, consulte la información sobre cómo definir una estrategia de protección de datos para clústeres de PostgreSQL.

- Debe haberse preparado para la protección de datos completando tareas como instalar SnapCenter, añadir hosts, configurar las conexiones del sistema de almacenamiento y añadir recursos.
- El administrador de SnapCenter debe haberle asignado las instancias de SVM de los volúmenes de origen y de destino en caso de que replique snapshots en un reflejo o almacén.

  Además, puede definir la configuración de replicación, script y aplicaciones en la política. Estas opciones ahorran tiempo cuando se desea volver a utilizar la política con otro grupo de recursos.

Acerca de esta tarea

- SnapLock
  - Si se selecciona la opción 'Retain the backup copies for a specific number of days', el período de retención de SnapLock debe ser menor o igual que los días de retención mencionados.
  - Si se especifica un período de bloqueo de instantáneas, se evita la eliminación de las instantáneas hasta que caduque el período de retención. Esto podría provocar que se retenga un número mayor de instantáneas que el recuento especificado en la política.
  - Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

La configuración principal de SnapLock se gestiona en la política de backup de SnapCenter y la configuración secundaria de SnapLock se gestiona mediante ONTAP.

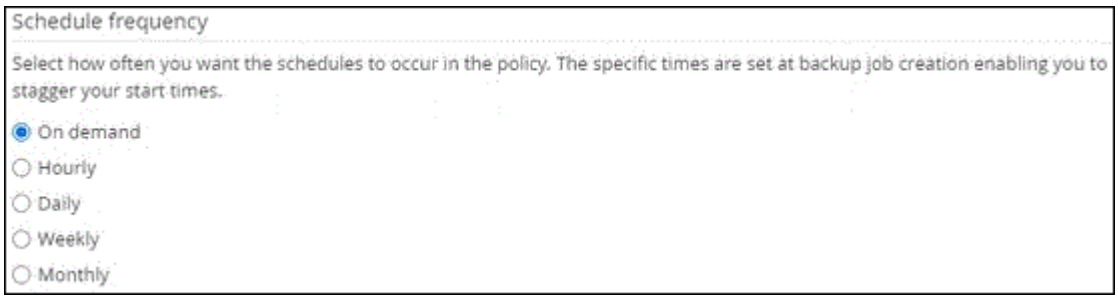
Pasos

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
2. En la página Configuración, haga clic en **Directivas**.
3. Haga clic en **Nuevo**.
4. En la página Name, escriba el nombre de la política y una descripción.
5. En la página Policy type, realice lo siguiente:
   a. Seleccione el tipo de almacenamiento.
   b. En la sección **Configuración de copia de seguridad personalizada**, proporcione cualquier configuración de copia de seguridad específica que tenga que pasarse al plugin en formato de clave-valor.

      Puede pasar varios pares de clave-valor al plugin.

6. En la página Instantánea, especifique el tipo de programación seleccionando **On Demand**, **Hourly**, **Daily**, **Weekly** o **Monthly**.

   Puede especificar la programación (fecha de inicio, fecha de finalización y frecuencia) para la operación de backup mientras crea un grupo de recursos. Esto le permite crear grupos de recursos que comparten la misma política y frecuencia de backup, pero también le permite asignar diferentes programaciones de backup a cada política.



   Si ha programado para las 2:00 a.m., la programación no se activará durante el horario de verano.

7. En la sección Snapshot settings, especifique el número de instantáneas que desea conservar.
8. En la página Retention, especifique la configuración de retención para el tipo de backup y el tipo de programación seleccionados en la página Backup Type:

Si desea…	Realice lo siguiente…
Conserve un cierto número de instantáneas	Seleccione **Copias para mantener** y, a continuación, especifique el número de instantáneas que desea conservar. Si la cantidad de copias de Snapshot supera el número especificado, las copias de Snapshot se eliminan empezando por las más antiguas.

Para los backups basados en copias de Snapshot, debe establecer el número de retención en 2 o más si va a habilitar la replicación de SnapVault. Si establece el número de retención en 1, la operación puede generar un error, ya que la primera snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva snapshot en el destino.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Crear grupos de recursos y añadir políticas

Un grupo de recursos es el contenedor al que debe añadir los recursos que desea proteger e incluir en un backup. Permite realizar un backup en simultáneo con todos los datos que están asociados con una determinada aplicación. Un grupo de recursos es necesario para cualquier trabajo de protección de datos. También debe añadir una o más políticas al grupo de recursos para definir el tipo de trabajo de protección de datos que desea realizar.

Acerca de esta tarea

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:

Para este campo…	Realice lo siguiente…
Nombre	Escriba un nombre para el grupo de recursos. El nombre del grupo de recursos no debe superar los 250 caracteres.

Para este campo…	Realice lo siguiente…
Etiquetas	Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos. Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.
Use un formato de nombre personalizado para la copia de Snapshot	Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de snapshot. Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la snapshot.

4. En la página Resources, seleccione un nombre de host de la lista desplegable **Host** y un tipo de recurso de la lista desplegable **Tipo de recurso**.

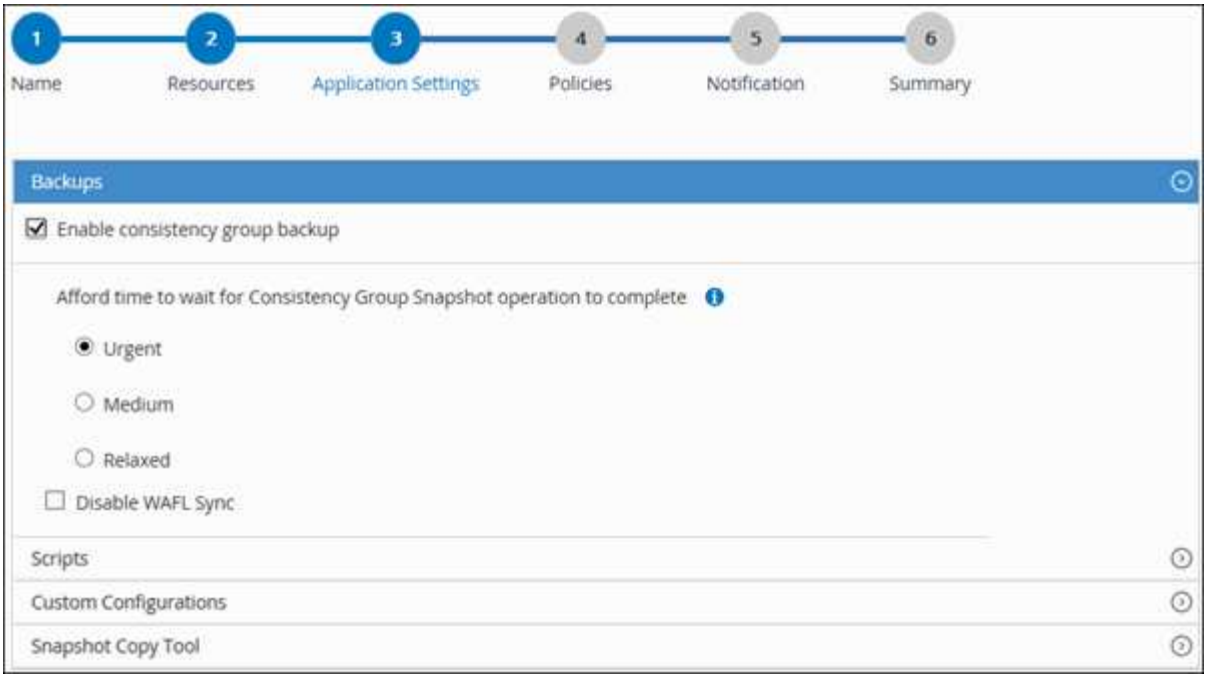
   Esto permite filtrar información en la pantalla.

5. Seleccione los recursos de la sección **Recursos disponibles** y, a continuación, haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.
6. En la página Application Settings, realice lo siguiente:

   a. Haga clic en la flecha **copias de seguridad** para establecer las opciones de copia de seguridad adicionales:

      Habilite el backup del grupo de consistencia y realice las siguientes tareas:

Para este campo…	Realice lo siguiente…
Espere tiempo a que finalice la operación de snapshot de grupo de consistencia	Seleccione **Urgente**, **Medio** o **Relacionado** para especificar el tiempo de espera para que se complete la operación de instantánea. Urgent = 5 segundos, Medium = 7 segundos y Relaxed = 20 segundos.
Deshabilite la sincronización WAFL	Seleccione este campo para evitar forzar un punto de coherencia de WAFL.

+ 

a. Haga clic en la flecha **Scripts** e introduzca los comandos PRE y POST para las operaciones de inactividad, instantánea y desactivación. También puede escribir los comandos previos para que se ejecuten antes de salir en caso de un fallo.

b. Haga clic en la flecha **configuraciones personalizadas** e introduzca los pares personalizados clave-valor requeridos para todas las operaciones de protección de datos que utilizan este recurso.

Parámetro	Ajuste	Descripción
ARCHIVE_LOG_ENABLE	(S/N)	Permite la gestión del registro de archivos para eliminar los registros de archivos.
RETENCIÓN_LOG_ARCHIVO	número_de_días	Especifica la cantidad de días que se conservan los registros de archivo. Este valor debe ser igual o mayor que las RETENTIONS NTAP_SNAPSHOT_.
ARCHIVE_LOG_DIR	change_info_directory/logs	Especifica la ruta de acceso al directorio que contiene los registros de archivo.

Parámetro	Ajuste	Descripción
ARCHIVO_LOG_EXT	extensión_archivo	Especifica la longitud de la extensión del archivo de registro de archivos. Por ejemplo, si el registro de archivos es log_backup_0_0_0_0.16151855 1942 9 y si el valor file_extension es 5, la extensión del registro conservará 5 dígitos, que son 16151.
ARCO ARCHIVE_LOG_RECURSIVE_ SE	(S/N)	Permite la gestión de registros de ficheros en subdirectorios. Debe utilizar este parámetro si los registros de archivo se encuentran en subdirectorios.

Los pares clave-valor personalizados son compatibles con los sistemas de plugins de Linux PostgreSQL y no son compatibles con el clúster PostgreSQL registrado como un plugin centralizado de Windows.

c. Haga clic en la flecha * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

Si desea que…	Realice lo siguiente…
SnapCenter utilice el plugin para Windows y coloque el sistema de archivos en estado coherente antes de crear una copia de Snapshot. En el caso de recursos de Linux, esta opción no es aplicable.	Seleccione **SnapCenter with File System Consistency**.
SnapCenter para crear una snapshot a nivel del almacenamiento	Seleccione **SnapCenter sin coherencia del sistema de archivos**.
Se escriba el comando que se ejecutará en el host a fin de crear copias de Snapshot.	Seleccione **Otro** y, a continuación, introduzca el comando que se ejecutará en el host para crear una instantánea.

7. En la página Policies, realice los siguientes pasos:

a. Seleccione una o varias políticas de la lista desplegable.

También puede crear una directiva haciendo clic en + .

Las políticas figuran en la sección Configure schedules for selected policies.

b. En la columna Configure Schedules, haga clic en + para la directiva que desea configurar.

c. En el cuadro de diálogo Agregar programas para la directiva *policy_name* , configure la programación y, a continuación, haga clic en **Aceptar**.

Policy_name es el nombre de la política seleccionada.

Los horarios configurados se enumeran en la columna **programas aplicados**.

No se admiten programas de backup de terceros cuando se solapan con los programas de backup de SnapCenter.

8. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. El servidor SMTP debe configurarse en **Ajustes** > **Ajustes globales**.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.

Backup de PostgreSQL

Si un recurso aún no es parte de ningún grupo de recursos, es posible realizar backups del recurso desde la página Resources.

Antes de empezar

- Debe tener creada una política de backup.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, la función ONTAP asignada al usuario de almacenamiento debería incluir el privilegio «sinapmirror all». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".
- Para la operación de backup basado en copias de Snapshot, asegúrese de que todos los clústeres de inquilinos sean válidos y estén activos.
- Para los comandos previos y posteriores para operaciones de inactividad, Snapshot y la reanudación de la copia, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin con las rutas siguientes:

Para Windows: *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_Commands_list.txt*

Para Linux: */var/opt/snapcenter/scc/allowed_Commands_list.txt*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

Seleccione y luego seleccione el nombre de host y el tipo de recurso para filtrar los recursos. A continuación, puede seleccionar para cerrar el panel de filtros.

3. Seleccione el recurso que desea incluir en el backup.
4. En la página Recursos, seleccione **Use custom name format for Snapshot copy** y, a continuación, escriba el formato del nombre personalizado que desee usar para el nombre de Snapshot.

   Por ejemplo, *customtext_policy_hostname* o *resource_hostname*. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

5. En la página Application Settings, realice lo siguiente:

   - Seleccione la flecha **backups** para establecer opciones de copia de seguridad adicionales:

     Habilite el backup del grupo de consistencia y, si es necesario, realice las siguientes tareas:

Para este campo…	**Realice lo siguiente…**
Permitir que se complete la operación de "Snapshot de grupo de consistencia"	Seleccione **Urgente**, **Medio** o **Relacionado** para especificar el tiempo de espera para que finalice la operación de instantánea. Urgent = 5 segundos, Medium = 7 segundos y Relaxed = 20 segundos.
Deshabilite la sincronización WAFL	Seleccione este campo para evitar forzar un punto de coherencia de WAFL.

   - Seleccione la flecha **Scripts** para ejecutar los comandos PRE y POST para las operaciones de inactividad, instantánea y desactivación.

     También puede ejecutar los comandos previos antes de salir de la operación de backup. Los scripts previos y posteriores se ejecutan en el servidor de SnapCenter.

   - Seleccione la flecha **Configuraciones personalizadas**y, a continuación, introduzca los pares de valores personalizados necesarios para todos los trabajos que utilizan este recurso.
   - Seleccione la flecha * Herramienta de copia de instantáneas * para seleccionar la herramienta para crear instantáneas:

Si desea que…	**Realice lo siguiente…**
SnapCenter cree una snapshot a nivel del almacenamiento	Seleccione **SnapCenter sin coherencia del sistema de archivos**.
SnapCenter utilice el plugin para Windows y coloque el sistema de archivos en estado coherente para luego crear una copia de Snapshot	Seleccione **SnapCenter with File System Consistency**.
Para escribir el comando para crear una snapshot	Seleccione **Otro** y luego ingrese el comando para crear una instantánea.

6. En la página Policies, realice los siguientes pasos:

   a. Seleccione una o varias políticas de la lista desplegable.

      También puede crear una directiva haciendo clic en + .

      En la sección Configure schedules for selected policies, se muestran las políticas seleccionadas.

   b. Seleccione + En la columna Configurar programaciones de la directiva para la que desea configurar una programación.

   c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación y, a continuación, seleccione **OK**.

      policy_name es el nombre de la directiva seleccionada.

   Las programaciones configuradas figuran en la columna Applied Schedules.

7. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. SMTP también debe configurarse en **Ajustes** > **Ajustes globales**.

8. Revisa el resumen y luego selecciona **Finalizar**.

   Se muestra la página de topología de los recursos.

9. Seleccione **Back up Now**.
10. En la página Backup, realice los siguientes pasos:

    a. Si aplicó varias políticas al recurso, en la lista desplegable **Política**, seleccione la directiva que desea utilizar para la copia de seguridad.

Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

b. Seleccione **copia de seguridad**.

11. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.
    - En las configuraciones de MetroCluster, es posible que SnapCenter no pueda detectar una relación de protección tras una conmutación por error.

      Para obtener más información, consulte: "No es posible detectar la relación de SnapMirror o SnapVault tras un fallo en MetroCluster"

    - Si va a realizar el backup de datos de aplicación en VMDK y el tamaño de pila de Java para el plugin de SnapCenter para VMware vSphere no es suficientemente grande, se puede producir un error en el backup.

      Para aumentar el tamaño de pila de Java, busque el archivo de script */opt/netapp/init_scripts/svservice*. En ese script, el comando *do_start method* inicia el servicio de complemento de VMware de SnapCenter. Actualice este comando a lo siguiente: *Java -jar -Xmx8192M -Xms4096M*

Realice un backup de los grupos de recursos

Un grupo de recursos es una agrupacion de recursos en un host. Se realiza una operación de backup del grupo de recursos con todos los recursos definidos en el grupo.

Antes de empezar

- Debe tener creado un grupo de recursos con una política anexada.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, la función ONTAP asignada al usuario de almacenamiento debería incluir el privilegio «sinapmirror all». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".

Acerca de esta tarea

Puede realizar un backup del grupo de recursos bajo demanda en la página Resources. Si un grupo de recursos tiene una política anexada y una programación configurada, los backups se realizan automáticamente según esa programación.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.

   Puede buscar el grupo de recursos escribiendo el nombre en el cuadro de búsqueda o seleccionando y, a continuación, seleccione la etiqueta. A continuación, puede seleccionar para cerrar el panel de filtros.

3. En la página Resource Groups, seleccione el grupo de recursos del que desea realizar un backup y, a continuación, seleccione **Back up Now**.
4. En la página Backup, realice los siguientes pasos:
   a. Si asoció varias políticas al grupo de recursos, en la lista desplegable **Policy**, seleccione la política

que desea usar para la copia de seguridad.

Si la política seleccionada para el backup bajo demanda está asociada a una programación de backup, los backups bajo demanda se retendrán en función de la configuración de retención especificada para el tipo de programación.

b. Seleccione **copia de seguridad**.

5. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

Cree una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para PostgreSQL

Es necesario crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar cmdlets de PowerShell para realizar backup, restaurar o clonar clústeres PostgreSQL.

Antes de empezar

- Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.
- Debe tener los permisos necesarios en el rol de administrador de infraestructura para crear conexiones de almacenamiento.
- Debe asegurarse de que no se encuentren en curso las instalaciones de plugins.

  No debe haber instalaciones de plugins de host en curso mientras se añade una conexión a sistemas de almacenamiento, porque la caché del host puede no estar actualizada y el estado de los clústeres puede mostrarse en la interfaz gráfica de usuario de SnapCenter con el formato «`Not available for backup`» o «`Not on NetApp storage`».

- Los nombres de los sistemas de almacenamiento deben ser únicos.

  SnapCenter no admite varios sistemas de almacenamiento con el mismo nombre en clústeres diferentes. Cada uno de los sistemas de almacenamiento que admite SnapCenter debe tener un nombre único y una dirección IP de LIF de datos única.

Pasos

1. Inicie una sesión de conexión de PowerShell Core mediante el cmdlet Open-SmConnection.

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

2. Cree una nueva conexión con el sistema de almacenamiento mediante el cmdlet Add-SmStorageConnection.

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

3. Cree una credencial nueva mediante el cmdlet Add-SmCredential.

   Este ejemplo muestra cómo crear una nueva credencial llamada FinanceAdmin con las credenciales de Windows:

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

4. Agregue el host de comunicación PostgreSQL al servidor SnapCenter.

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

5. Instale el paquete y el plugin de SnapCenter para PostgreSQL en el host.

   Para Linux:

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

   Para Windows:

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

6. Defina la ruta de acceso a SQLLIB.

   Para Windows, el plugin PostgreSQL utilizará la ruta predeterminada para la carpeta SQLLIB: “C:\Program Files\IBM\SQLLIB\BIN”

   Si desea anular la ruta predeterminada, utilice el comando siguiente.

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

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. También puede consultar https://docs.netapp.com/us-en/snapcenter-cmdlets/index.htmlnapCenter la Guía de referencia del cmdlet de software Software Reference Guide^].

Realizar un backup de los clústeres mediante cmdlets de PowerShell

El backup de un clúster implica establecer una conexión con SnapCenter Server, añadir recursos, añadir una política, crear una política de recursos de backup y realizar el backup.

Antes de empezar

- Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.
- Debe añadir la conexión con el sistema de almacenamiento y crear una credencial.

Pasos

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

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

   Se muestra una solicitud de nombre de usuario y contraseña.

2. Añada recursos manuales mediante el cmdlet Add-SmResources.

   Este ejemplo muestra cómo agregar una instancia PostgreSQL:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode PostgreSQL
-ResourceType Instance -ResourceName postgresqlinst1 -StorageFootPrint
(@{"VolumeName"="winpostgresql01_data01";"LUNName"="winpostgresql01_data
01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Cree una política de backup mediante el cmdlet Add-SmPolicy.
4. Proteja el recurso o añada un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.
5. Para iniciar una tarea de backup se usa el cmdlet New-SmBackup.

   Este ejemplo muestra cómo realizar un backup de un grupo de recursos:

```
C:\PS> New-SMBackup -ResourceGroupName 'ResourceGroup_wback-up-clusters-
using-powershell-cmdlets-postgresql.adocith_Resources'  -Policy
postgresql_policy1
```

   Este ejemplo realiza un backup de un recurso protegido:

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

6. Supervise el estado de la tarea (running, completed o failed) mediante el cmdlet Get-smJobSummaryReport.

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

7. Supervise los detalles del trabajo de backup como ID de backup, nombre de backup para realizar una

operación de restauración o clonado mediante el 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 :
```

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Supervisar las operaciones de backup

Supervisar las operaciones de backup de PostgreSQL

Es posible supervisar el progreso de diferentes operaciones de backup mediante la página Jobs de SnapCenter. Se recomienda comprobar el progreso para determinar cuándo se completó la tarea o si existe un problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado correspondiente de las operaciones:

-  En curso

- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página Monitor, haga clic en **Jobs**.
3. En la página Jobs, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo se muestren las operaciones de backup.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **copia de seguridad**.
   d. En la lista desplegable **Estado**, seleccione el estado de copia de seguridad.
   e. Haga clic en **aplicar** para ver las operaciones completadas correctamente.
4. Seleccione un trabajo de copia de seguridad y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.

   Aunque el estado del trabajo de backup indique , al hacer clic en los detalles del trabajo, puede ver que algunas de las tareas secundarias de la operación de copia de seguridad aún están en curso o marcadas con señales de advertencia.

5. En la página Detalles del trabajo, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

Supervise las operaciones de protección de datos en clústeres PostgreSQL en el panel Activity

El panel Activity muestra las cinco operaciones más recientes que se ejecutaron. También muestra el momento en que se inició la operación y su estado.

El panel Activity muestra información sobre las operaciones de backup, restauración, clonado y backup programado.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. Haga clic en En el panel Activity para ver las cinco operaciones más recientes.

   Al hacer clic en una de las operaciones, los detalles de la operación se enumeran en la página **Detalles del trabajo**.

Cancelar las operaciones de backup para PostgreSQL

Es posible cancelar las operaciones de backup que se encuentran en cola.

Lo que necesitará

- Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones.
- Puede cancelar una operación de copia de seguridad desde la página **Monitor** o el panel **Activity**.
- No es posible cancelar una operación de backup en ejecución.
- Es posible utilizar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de backup.
- El botón **Cancelar trabajo** está desactivado para operaciones que no se pueden cancelar.
- Si seleccionó **todos los miembros de esta función pueden ver y operar en otros objetos de miembros** en la página usuarios\grupos mientras crea una función, puede cancelar las operaciones de copia de seguridad en cola de otros miembros mientras utiliza esa función.
- Pasos*

1. Ejecute una de las siguientes acciones:

Del…	Acción
Página Monitor	a. En el panel de navegación izquierdo, haga clic en **Monitor** > **Jobs**. b. Seleccione la operación y, a continuación, haga clic en **Cancelar trabajo**.
Panel de actividades	a. Tras iniciar la operación de backup, haga clic en  En el panel Activity para ver las cinco operaciones más recientes. b. Seleccione la operación. c. En la página Detalles del trabajo, haga clic en **Cancelar trabajo**.

Se cancela la operación y el recurso se revierte al estado anterior.

Consulte los backups y los clones de PostgreSQL en la página Topology

Al prepararse para clonar un recurso o incluirlo en un backup, puede resultar útil ver una representación gráfica de todos los backups y clones del almacenamiento principal y secundario.

Acerca de esta tarea

Puede consultar los siguientes iconos de la vista gestionar copias para determinar si los backups o clones están disponibles en el almacenamiento principal y secundario (copias reflejadas o en almacén).

-  muestra la cantidad de backups y clones que están disponibles en el almacenamiento principal.
-

 Muestra la cantidad de backups y clones que estan copiados en el almacenamiento secundario mediante SnapMirror.

-  Muestra la cantidad de backups y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault.

La cantidad de backups que se muestra incluye los backups eliminados del almacenamiento secundario. Por ejemplo, si creó 6 backups con una política para retener solamente 4 backups, se muestran 6 backups.

Los clones de un backup de un reflejo con versión flexible en un volumen de tipo reflejo-almacén se muestran en la vista de topología, pero el número de backups de reflejo no incluye el backup con versión flexible.

En la página Topology, es posible ver todos los backups y clones que están disponibles para el recurso o el grupo de recursos seleccionado. Pueden verse los detalles de estos backups y clones, y luego seleccionarlos para realizar operaciones de protección de datos.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, seleccione el recurso o el grupo de recursos de la lista desplegable **View**.
3. Seleccione el recurso desde la vista de detalles del recurso o desde la vista de detalles del grupo de recursos.

   Si el recurso está protegido, se muestra la página con el resumen seleccionado.

4. Consulte **Summary Card** para ver un resumen del número de copias de seguridad y clones disponibles en el almacenamiento principal y secundario.

   La sección **Summary Card** muestra el número total de copias de Snapshot y clones.

   Al hacer clic en el botón **Actualizar** se inicia una consulta del almacenamiento para mostrar un recuento preciso.

   Si se realiza una copia de seguridad habilitada para SnapLock, al hacer clic en el botón **Actualizar** se actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP. Una programación semanal también actualiza el tiempo de caducidad de SnapLock principal y secundario recuperado de ONTAP.

   Cuando el recurso de la aplicación se distribuya entre varios volúmenes, el tiempo de caducidad de SnapLock para el backup será el tiempo de caducidad de SnapLock más largo que se establezca para una snapshot en un volumen. El tiempo de caducidad de SnapLock más largo se recupera de ONTAP.

   Después de la copia de seguridad a petición, haciendo clic en el botón **Actualizar** actualiza los detalles de la copia de seguridad o clonación.

5. En la vista Administrar copias, haga clic en **copias de seguridad** o **clones** en el almacenamiento principal o secundario para ver los detalles de una copia de seguridad o un clon.

Estos detalles se muestran en forma de tabla.

6. Seleccione el backup de la tabla y, a continuación, haga clic en los iconos de protección de datos para llevar a cabo operaciones de restauración, clonado y eliminación.

> Los backups que figuran en el almacenamiento secundario no pueden eliminarse ni cambiar de nombre.

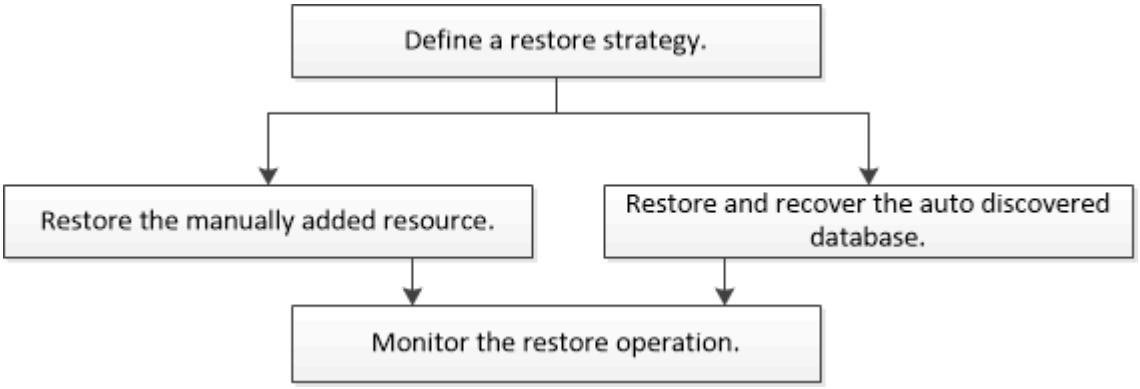
7. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en .
8. Si desea dividir un clon, selecciónelo de la tabla y, a continuación, haga clic en .

Restaurar PostgreSQL

Restaure el flujo de trabajo

El flujo de trabajo de restauración y recuperación incluye planificar, realizar las operaciones de restauración y supervisarlas.

El siguiente flujo de trabajo muestra la secuencia que debe seguirse para realizar la operación de restauración:



También puede usar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración y clonado. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen detalles sobre los cmdlets de PowerShell.

"Guía de referencia de cmdlets de SnapCenter Software".

Restaurar y recuperar un backup de recurso añadido manualmente

Puede utilizar SnapCenter para restaurar y recuperar datos de uno o varios backups.

Antes de empezar

- Debe tener un backup de los recursos o del grupo de recursos.
- Cancele la operación de backup que se encuentra en curso y que corresponde al recurso o grupo de recursos que desea restaurar.
- Para los comandos previos a la restauración, después de la restauración, el montaje y el desmontaje, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:

Para Windows: *C:\Archivos de programa\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*

Para Linux: */var/opt/snapcenter/scc/allowed_commands.config*

Si no hay comandos en la lista de comandos, se producirá un error en la operación.

Acerca de esta tarea

- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, filtre los recursos de la lista desplegable **View** en función del tipo de recurso.

   Los recursos se muestran junto con el tipo, el host, las políticas y los grupos de recursos asociados, y el estado.

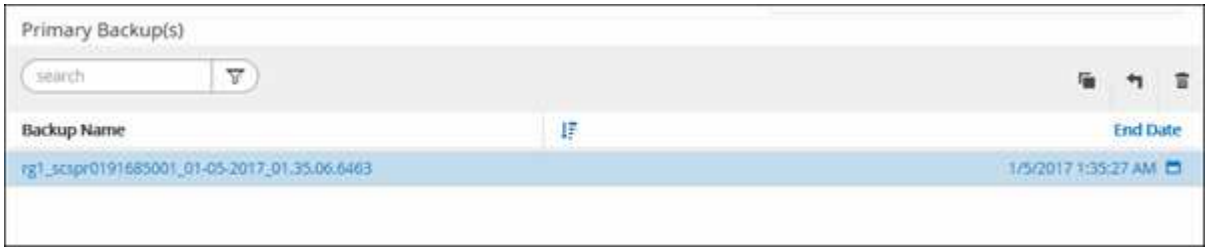
   Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

   Si el recurso no está protegido, se muestra "'no protegido'" en la columna Estado general. Esto significa que el recurso no está protegido o que otro usuario hizo el backup de este recurso.

3. Seleccione el recurso o seleccione un grupo de recursos y, a continuación, seleccione un recurso de ese grupo.

   Se muestra la página con el resumen.

4. En la vista Manage Copies, seleccione **copias de seguridad** ya sea en los sistemas de almacenamiento primario o secundario (reflejado o en almacén).
5. En la tabla de backups primarios, seleccione el backup desde el cual quiere restaurar y, a continuación, haga clic en .



6. En la página Restore Scope, seleccione **Complete Resource**.

   a. Si selecciona **Recurso completo**, se restauran todos los volúmenes de datos configurados del clúster PostgreSQL.

      Si el recurso contiene volúmenes o qtrees, las snapshots realizadas después de la Snapshot seleccionada para restaurar en los volúmenes o qtrees se eliminan y no pueden recuperarse. Además,

si hay algún otro recurso alojado en los mismos volúmenes o qtrees, también se lo elimina.

Puede seleccionar varios LUN.

Si selecciona **todo**, se restauran todos los archivos de los volúmenes, qtrees o LUN.

7. En la página Pre OPS, escriba los comandos previos a la restauración y los comandos de desmontaje que se ejecutarán antes de realizar un trabajo de restauración.

   Los comandos de desmontaje no están disponibles para los recursos de detección automática.

8. En la página Post OPS, escriba los comandos de montaje y los comandos posteriores a la restauración que se ejecutarán después de realizar un trabajo de restauración.

   Los comandos de montaje no están disponibles para los recursos detectados automáticamente.

   Para los comandos previos y posteriores para operaciones de inactividad, Snapshot y reanudación, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin en la ruta */opt/snapcenter/snapenter/scc/allowed_commands.config* para Linux y *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config* para Windows.

9. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. SMTP también debe configurarse en la página **Ajustes** > **Ajustes globales**.

10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Restaure y recupere un backup de clúster detectado automáticamente

Puede utilizar SnapCenter para restaurar y recuperar datos de uno o varios backups.

Antes de empezar

- Debe tener un backup de los recursos o del grupo de recursos.
- Cancele la operación de backup que se encuentra en curso y que corresponde al recurso o grupo de recursos que desea restaurar.
- Para los comandos previos a la restauración, después de la restauración, el montaje y el desmontaje, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:

  Para Windows: *C:\Archivos de programa\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*

  Para Linux: */var/opt/snapcenter/scc/allowed_commands.config*

  Si no hay comandos en la lista de comandos, se producirá un error en la operación.

Acerca de esta tarea

- Las copias de backup basadas de archivos no se pueden restaurar desde SnapCenter.
- Para los recursos detectados automáticamente, se admite la restauración con SFSR.
- No se admite la recuperación automática.
- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, filtre los recursos de la lista desplegable **View** en función del tipo de recurso.

   Los recursos se muestran junto con el tipo, el host, las políticas y los grupos de recursos asociados, y el estado.

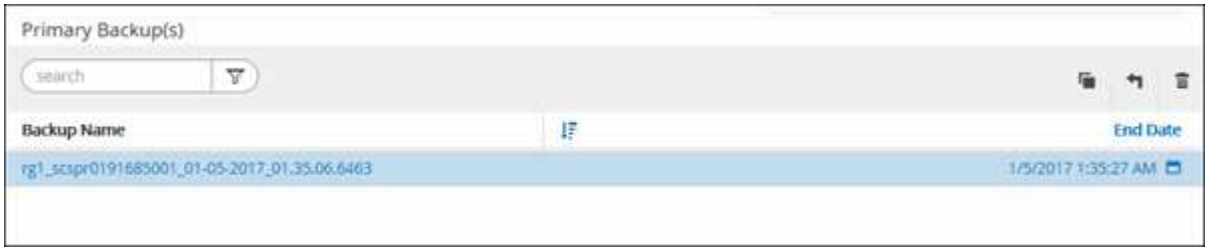
   Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

   Si el recurso no está protegido, se muestra "'no protegido'" en la columna Estado general. Esto significa que el recurso no está protegido o que otro usuario hizo el backup de este recurso.

3. Seleccione el recurso o seleccione un grupo de recursos y, a continuación, seleccione un recurso de ese grupo.

   Se muestra la página con el resumen.

4. En la vista Manage Copies, seleccione **copias de seguridad** ya sea en los sistemas de almacenamiento primario o secundario (reflejado o en almacén).
5. En la tabla de backups primarios, seleccione el backup desde el cual quiere restaurar y, a continuación, haga clic en .



6. En la página Restore Scope, seleccione **Complete Resource** para restaurar los volúmenes de datos configurados del clúster PostgreSQL.
7. En la página Restore Scope, seleccione una de las siguientes opciones:

Si…	Realice lo siguiente…
Desea recuperar el mayor cierre posible a la hora actual	Seleccione **recuperar al estado más reciente**. Para los recursos de contenedor único, especifique una o más ubicaciones de backup de registro y catálogo.

Desea recuperar al punto en el tiempo especificado	Seleccione **Recover to point in time**. a. Introduzca la fecha y la hora. Introduzca la fecha y la hora. Por ejemplo, el host PostgreSQL Linux se encuentra en Sunnyvale, CA y el usuario en Raleigh, NC está recuperando los registros en SnapCenter. Si el usuario desea realizar una recuperación a 5 a.m . Sunnyvale, CA, entonces el usuario debe establecer la zona horaria del navegador en la zona horaria del host de PostgreSQL Linux, que es GMT-07:00 y especificar la fecha y la hora como 5:00 a.m.
No desea recuperar	Seleccione **sin recuperación**.

No se pueden recuperar recursos PostgreSQL añadidos manualmente.

El plugin de SnapCenter para PostgreSQL crea una etiqueta de backup y un tablespace_map en la carpeta */<OS_temp_folder>/postgresql_sc_recovery*<Restore_JobId>/_ que ayuda a la recuperación manual.

1. En la página Pre OPS, escriba los comandos previos a la restauración y los comandos de desmontaje que se ejecutarán antes de realizar un trabajo de restauración.

   Los comandos de desmontaje no están disponibles para los recursos de detección automática.

2. En la página Post OPS, escriba los comandos de montaje y los comandos posteriores a la restauración que se ejecutarán después de realizar un trabajo de restauración.

   Los comandos de montaje no están disponibles para los recursos detectados automáticamente.

   Para los comandos previos y posteriores para operaciones de inactividad, Snapshot y reanudación, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin en la ruta */opt/snapcenter/snapenter/scc/allowed_commands.config* para Linux y *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config* para Windows.

3. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. SMTP también debe configurarse en la página **Ajustes** > **Ajustes globales**.

4. Revise el resumen y, a continuación, haga clic en **Finalizar**.
5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Restaurar un clúster PostgreSQL mediante cmdlets de PowerShell

La restauración de una copia de seguridad PostgreSQL incluye iniciar una sesión de conexión con el servidor SnapCenter, mostrar una lista de backups y recuperar información de los backups, y restaurar una copia de seguridad.

Antes de empezar

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

Pasos

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

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

2. Identifique el backup que desea restaurar mediante los cmdlets Get-SmBackup y Get-SmBackupReport.

   Este ejemplo muestra que hay dos backups disponibles para restaurar:

```
 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
```

   En este ejemplo, se muestra información detallada sobre el backup del 29 de enero de 2015 al 3 de febrero de 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. Puede restaurar los datos del backup mediante el cmdlet Restore-SmBackup.

> AppObjectId es «Host\Plugin\UID», donde UID = <instance_name> es para un recurso de instancia de PostgreSQL detectado manualmente y UID = <instance_name>\<databse_name> es para un recurso de clúster PostgreSQL. Puede obtener el ResourceID a partir del cmdlet Get-smResources.

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

Este ejemplo muestra cómo restaurar el clúster desde el almacenamiento principal:

```
Restore-SmBackup -PluginCode PostgreSQL -AppObjectId
cn24.sccore.test.com\PostgreSQL\PostgreSQLinst1\DB01 -BackupId 3
```

Este ejemplo muestra cómo restaurar el clúster desde el almacenamiento secundario:

```
Restore-SmBackup -PluginCode 'PostgreSQL' -AppObjectId
cn24.sccore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false
-Archive @( @{"Primary"="<Primary
Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
Vserver>:<SecondaryVolume>"})
```

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Restaurar recursos mediante los cmdlets de PowerShell

La restauración de un backup de recursos incluye el inicio de una sesión de conexión con el servidor SnapCenter, el listado de los backups y la recuperación de información de los backups, y la restauración de un backup.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

Pasos

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

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

2. Para recuperar la información sobre los backups que desea restaurar, puede usar los cmdlets Get-SmBackup y Get-SmBackupReport.

   Este ejemplo muestra información sobre todos los backups disponibles:

```
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
```

En este ejemplo, se muestra información detallada sobre el backup del 29 de enero de 2015 al 3 de febrero de 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. Puede restaurar los datos del backup mediante el 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           :
```

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Supervisar las operaciones de restauración de PostgreSQL

Es posible supervisar el progreso de diferentes operaciones de restauración de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

Acerca de esta tarea

los estados posteriores a la restauración describen las condiciones del recurso una vez ejecutada la operación de restauración, así como otras acciones de restauración que pueden realizarse.

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso

- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
2. En la página **Monitor**, haga clic en **trabajos**.
3. En la página **trabajos**, realice los siguientes pasos:
   a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de restauración.
   b. Especifique las fechas de inicio y finalización.
   c. En la lista desplegable **Tipo**, seleccione **Restaurar**.
   d. En la lista desplegable **Estado**, seleccione el estado de restauración.
   e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
4. Seleccione el trabajo de restauración y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página **Detalles del trabajo**, haga clic en **Ver registros**.

   El botón **Ver registros** muestra los registros detallados para la operación seleccionada.

Clonar backups de recursos de PostgreSQL

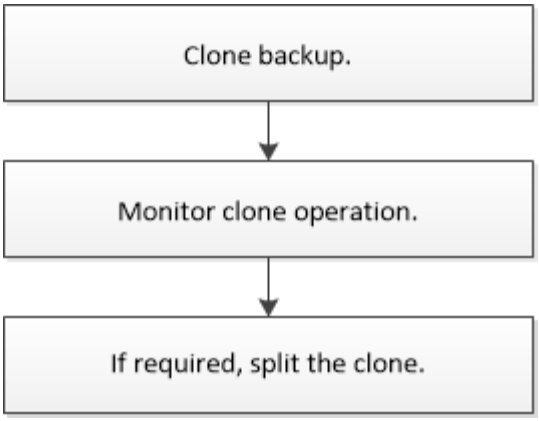
Flujo de trabajo de clonado

El flujo de trabajo de clonado incluye realizar la operación de clonado y supervisarla.

Acerca de esta tarea

- Puede clonar en el servidor PostgreSQL de origen.
- Es posible clonar backups de recursos por los siguientes motivos:
  - Para probar la funcionalidad que debe implementarse mediante la estructura de recursos actuales y el contenido durante los ciclos de desarrollo de aplicaciones
  - Para herramientas de manipulación y extracción de datos cuando se rellenan almacenes de datos
  - Para recuperar datos que se eliminaron o se modificaron por error

Los siguientes flujos de trabajo muestran la secuencia que debe seguirse para realizar la operación de clonado:



También puede usar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración y clonado. La ayuda del cmdlet de SnapCenter y la información de referencia del cmdlet contienen detalles sobre los cmdlets de PowerShell.

Clonar un backup de PostgreSQL

Es posible usar SnapCenter para clonar un backup. Es posible clonar desde un backup primario o secundario.

Antes de empezar

- Debe tener un backup de los recursos o del grupo de recursos.
- Debe asegurarse de que los agregados donde se alojan los volúmenes deben estar en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).
- Para los comandos previos o posteriores a la clonado, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:

  Para Windows: *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_Commands_list.txt*

  Para Linux: */var/opt/snapcenter/scc/allowed_Commands_list.txt*

  Si no hay comandos en la lista de comandos, se producirá un error en la operación.

Acerca de esta tarea

- Para obtener más información sobre las limitaciones de las operaciones de división de clones, consulte "Guía de gestión de almacenamiento lógico de ONTAP 9".
- Para ONTAP 9.12.1 y versiones anteriores, los clones creados a partir de las instantáneas de almacén de SnapLock como parte de la restauración heredarán el tiempo de caducidad de almacén de SnapLock. El administrador de almacenamiento debe limpiar manualmente los clones después de la hora de caducidad de SnapLock.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página Resources, filtre los recursos de la lista desplegable **View** en función del tipo de recurso.

   Los recursos se muestran junto con cierta información, como el tipo, el host, las políticas y los grupos de

recursos asociados, y el estado.

3. Seleccione el recurso o el grupo de recursos.

   Debe seleccionar un recurso para seleccionar un grupo de recursos.

   Se muestra la página con el resumen o grupo de recursos.

4. En la vista Manage Copies, seleccione **copias de seguridad** ya sea en los sistemas de almacenamiento primario o secundario (reflejado o en almacén).

5. Seleccione el backup de datos de la tabla y haga clic en  .

6. En la página Location, lleve a cabo las siguientes acciones:

Para este campo…	Realice lo siguiente…
Clone el servidor	Elija el host donde se debe crear el clon.
Puerto de destino	Introduzca el puerto de destino PostgreSQL para clonar a partir de los backups existentes.
Dirección IP de exportación NFS	Introduzca las direcciones IP o los nombres de host a los que se van a exportar los volúmenes clonados. Esto solo se aplica al recurso de tipo de almacenamiento NFS.
Pool de capacidad máx. Rendimiento (MiB/s)	Introduzca el rendimiento máximo de un pool de capacidad. Esto solo es aplicable a los recursos del tipo de almacenamiento ANF.

7. En la página Scripts, realice los siguientes pasos:

   Los scripts se ejecutan en el host del plugin.

   a. Introduzca los comandos para el clon previo o posterior que se deben ejecutar antes o después de la operación de clonado, respectivamente.
      - Comando previo a la clonado: Elimine los clústeres existentes con el mismo nombre
      - Comando posterior a la clonado: Verifique un clúster o inicie un clúster.

   b. Escriba el comando de montaje para montar un sistema de archivos en un host.

      Comando de montaje para un volumen o qtree en un equipo Linux:

      Ejemplo para NFS:

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

Para los comandos previos y posteriores para operaciones de inactividad, Snapshot y reanudación, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin en la ruta */opt/snapcenter/snapenter/scc/allowed_commands.config* para Linux y *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands_list.txt* para Windows.

8. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo.

9. Revise el resumen y, a continuación, haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

Clone backups de clústeres PostgreSQL mediante cmdlets de PowerShell

El flujo de trabajo de clonado incluye planificar, realizar la operación de clonado y supervisar la operación.

Debe haber preparado el entorno de PowerShell para ejecutar los cmdlets de PowerShell.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando *Get-Help nombre_comando*. Alternativamente, también puede consultar la "Guía de referencia de cmdlets de SnapCenter Software".

Pasos

1. Inicie una sesión de conexión con el servidor de SnapCenter para el usuario especificado mediante el cmdlet de Open-SmConnection.

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

2. Recupere los backups para realizar la operación de clonado mediante el cmdlet Get-SmBackup.

   Este ejemplo muestra que hay dos backups disponibles para clonar:

```
 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. Inicie una operación de clonado a partir de un backup existente y especifique las direcciones IP de exportación de NFS a las que se van a exportar los volúmenes clonados.

   Este ejemplo muestra que el backup que se va a clonar tiene una dirección NFSExportIPs de 10.32.212.14:

   Para clúster 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
```

   Si no se especificó NFSExportIPs, el valor predeterminado se exporta al host de destino del clon.

4. Compruebe que los backups se hayan clonado correctamente mediante el cmdlet Get-SmCloneReport para ver los detalles del trabajo de clonado.

   Puede ver detalles como el ID del clon, la fecha y hora de inicio, y la fecha y hora de finalización.

```
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          :
```

Supervise las operaciones de clonación de PostgreSQL

Es posible supervisar el progreso de las operaciones de clonado de SnapCenter mediante la página Jobs. El progreso de una operación puede revisarse para determinar cuándo está completa o si hay un problema.

Acerca de esta tarea

Los siguientes iconos aparecen en la página Jobs e indican el estado de la operación:

- En curso
- Completado correctamente
- Error
- Completado con advertencias o no pudo iniciarse debido a advertencias
- En cola
- Cancelada
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Monitor**.
  2. En la página **Monitor**, haga clic en **trabajos**.
  3. En la página **trabajos**, realice los siguientes pasos:
     a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de clonado.
     b. Especifique las fechas de inicio y finalización.
     c. En la lista desplegable **Tipo**, seleccione **Clonar**.
     d. En la lista desplegable **Estado**, seleccione el estado del clon.
     e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.
  4. Seleccione el trabajo de clonado y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
  5. En la página Detalles del trabajo, haga clic en **Ver registros**.

Divida un clon

Es posible usar SnapCenter para dividir un recurso clonado de un recurso primario. El clon que se divide se independiza del recurso primario.

Acerca de esta tarea

- No se puede ejecutar la operación de división de clones en un clon intermedio.

  Por ejemplo, después de crear el clon 1 a partir de un backup de la base de datos, puede realizar un backup del clon 1 y luego clonar este backup (que sería el clon 2). Una vez creado el clon 2, el clon 1 se convierte en un clon intermedio y la operación de división de clones puede hacerse con el clon 1. No obstante, esta operación también puede ejecutarse con el clon 2.

  Después de dividir el clon 2, puede ejecutar la operación de división de clones con el clon 1, ya que este deja de ser el clon intermedio.

- Cuando divide un clon, se eliminan las copias de backup y los trabajos de clonado del clon.
- Para obtener más información sobre las limitaciones de las operaciones de división de clones, consulte "Guía de gestión de almacenamiento lógico de ONTAP 9".
- Asegúrese de que el volumen o el agregado del sistema de almacenamiento estén en línea.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **Recursos**, seleccione la opción adecuada en la lista Ver:

Opción	Descripción
Para aplicaciones de base de datos	Seleccione **base de datos** en la lista View.
Para sistemas de archivos	Seleccione **Ruta** en la lista Ver.

3. Seleccione el recurso adecuado de la lista.

   Se muestra la página con el resumen.

4. En la vista **Administrar copias**, seleccione el recurso clonado (por ejemplo, la base de datos o LUN) y, a continuación, haga clic en  .
5. Revise el tamaño estimado del clon que se va a dividir y el espacio necesario disponible en el agregado y, a continuación, haga clic en **Inicio**.
6. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

   La operación de división de clones se detiene si se reinicia el servicio de SMCore. Debe ejecutar el cmdlet Stop-SmJob para detener la operación de división de clones y luego volver a intentar la operación de división de clones.

   Si necesita más o menos tiempo de sondeo para comprobar si el clon está dividido o no, puede cambiar el valor del parámetro *CloneSplitStatusCheckPollTime* en el archivo *SMCoreServiceHost.exe.config* para establecer un intervalo para que SMCore sondee el estado de la operación de división de clones. El valor se registra en milisegundos; el predeterminado son 5 minutos.

   Por ejemplo:

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

   Se produce un error en la operación de inicio de división de clones si hay un backup, una restauración u otra división de clones en curso. Solo debe reiniciar la operación de división de clones una vez que hayan finalizado las operaciones en ejecución.

Información relacionada

"Se produce un error en la verificación o el clon de SnapCenter porque no existe agregado"

Elimine o divida clones de clústeres de PostgreSQL después de actualizar SnapCenter

Después de actualizar a SnapCenter 4.3, ya no se muestran los clones. Puede eliminar el clon o dividir los clones desde la página Topology del recurso desde el cual se crearon los clones.

Acerca de esta tarea

Si desea localizar el espacio de almacenamiento de los clones ocultos, ejecute el siguiente comando: `Get-SmClone -ListStorageFootprint`

Pasos

1. Elimine los backups de los recursos clonados con el cmdlet remove-smbackup.
2. Elimine el grupo de recursos de los recursos clonados mediante el cmdlet remove-smresourcegroup.
3. Quite la protección del recurso clonado mediante el cmdlet remove-smprotectresource.
4. Seleccione el recurso primario de la página Resources.

   Se muestra la página con el resumen.

5. En la vista Manage Copies, seleccione los clones de los sistemas de almacenamiento principal o secundario (reflejado o replicado).
6. Seleccione los clones y, a continuación, haga clic en  para eliminar clones o haga clic en  para dividir los clones.
7. Haga clic en **Aceptar**.