Realizar backup de base de datos de SQL Server, instancia o grupo de disponibilidad

SnapCenter Software 5.0

NetApp
July 18, 2024

Tabla de contenidos

Realizar backup de base de datos de SQL Server, instancia o grupo de disponibilidad

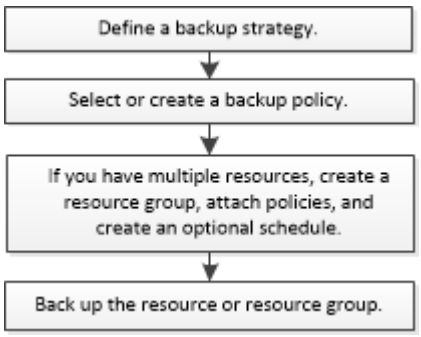
Flujo de trabajo de backup

Al instalar el plugin de SnapCenter para Microsoft SQL Server en el entorno, puede utilizar SnapCenter para realizar backup de los recursos de SQL Server.

Es posible programar varios backups para que se realicen simultáneamente en diferentes servidores.

No se pueden ejecutar en simultáneo operaciones de backup y restauración en el mismo recurso.

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



Las opciones Backup Now, Restore, Manage backups y Clone de la página Resources están deshabilitadas si selecciona un LUN que no pertenece a NetApp, una base de datos dañada o una base de datos que se está restaurando.

También puede utilizar los cmdlets de PowerShell manualmente o en scripts para realizar operaciones de backup, restauración, recuperación, verificación y clonado. Para obtener información detallada sobre los cmdlets de PowerShell, use la ayuda de cmdlets de SnapCenter o consulte la "Guía de referencia de cmdlets de SnapCenter Software"

Cómo SnapCenter hace backups de base de datos

SnapCenter utiliza la tecnología Snapshot para realizar backup de las bases de datos de SQL Server que residen en LUN o VMDK. Para crear el backup, SnapCenter crea Snapshot de las bases de datos.

Cuando se selecciona una base de datos para un backup de base de datos completo en la página Resources, SnapCenter selecciona automáticamente todas las demás bases de datos que residen en el mismo volumen de almacenamiento. Si el LUN o el VMDK se almacenan en una sola base de datos, puede desactivar o volver a seleccionar la base de datos individualmente. Si el LUN o el VMDK alojan varias bases de datos, debe desactivar o volver a seleccionar las bases de datos como un grupo.

Se realiza un backup simultáneo de todas las bases de datos que residen en un único volumen mediante Snapshot. Si el número máximo de bases de datos de backup simultáneo es 35 y residen más de 35 bases de datos en un volumen de almacenamiento, el número total de Snapshots que se crean es igual al número de bases de datos dividido por 35.

Puede configurar el número máximo de bases de datos para cada Snapshot en la política de backups.

Cuando SnapCenter crea una copia Snapshot, se captura todo el volumen del sistema de almacenamiento en la copia Snapshot. Sin embargo, el backup solo es válido para el servidor de host SQL para el cual se creó el backup.

Si residen datos de otros servidores de host SQL en el mismo volumen, estos datos no puede restaurarse a partir de la Snapshot.

Más información

"Realizar backup de recursos con cmdlets de PowerShell"

"Error de operaciones de inactivación o agrupación de recursos"

Determine si hay recursos disponibles para backup

Los recursos son las bases de datos, las instancias de aplicaciones, los grupos de disponibilidad y los componentes similares que se mantienen mediante los plugins instalados. Es posible añadir esos recursos a grupos de recursos para ejecutar tareas de protección de datos, pero primero es necesario identificar qué recursos están disponibles. Identificar los recursos disponibles también permite verificar que el plugin se haya instalado correctamente.

Antes de empezar

- Debe haber completado ciertas tareas, como instalar SnapCenter Server, añadir hosts, crear conexiones de sistema de almacenamiento y añadir credenciales.
- Para detectar las bases de datos de Microsoft SQL, se debe cumplir una de las siguientes condiciones.
  - El usuario que se utilizó para añadir el host del plugin a SnapCenter Server debe tener los permisos requeridos (sysadmin) en Microsoft SQL Server.
  - Si no se cumple la condición anterior, en el servidor SnapCenter debe configurar el usuario que tiene los permisos necesarios (sysadmin) en Microsoft SQL Server. El usuario debe configurarse en el nivel de instancia de Microsoft SQL Server y el usuario puede ser un usuario de SQL o Windows.
- Para detectar las bases de datos de Microsoft SQL en un clúster de Windows, debe desbloquear el puerto TCP/IP de la instancia de clúster de conmutación por error (FCI).
- Si las bases de datos residen en LUN o VMDK de VMware, debe implementar el plugin de SnapCenter para VMware vSphere y registrar el plugin en SnapCenter.

  Para obtener más información, consulte "Ponga en marcha el plugin de SnapCenter para VMware vSphere"

- Si el host se agrega con GMSA y si el GMSA tiene privilegios de inicio de sesión y administrador del sistema, el GMSA se utilizará para conectarse a la instancia de SQL.

Acerca de esta tarea

No se puede realizar una copia de seguridad de las bases de datos si la opción **Estado general** de la página Detalles está establecida en no disponible para la copia de seguridad. La opción **Estado general** se establece en no disponible para copia de seguridad cuando se cumple alguna de las siguientes condiciones:

- Las bases de datos no se encuentran en un LUN de NetApp.
- Las bases de datos no están en estado normal.

  Las bases de datos no se encuentran en el estado normal cuando están sin conexión, en restauración, pendientes de recuperación, suspendidas, etc.

- Las bases de datos tienen privilegios insuficientes.

  Por ejemplo, si un usuario solo tiene acceso para ver la base de datos, no será posible identificar los archivos y las propiedades de la base de datos, por lo que no se podrá realizar un backup.

SnapCenter sólo puede realizar una copia de seguridad de la base de datos primaria si tiene una configuración de grupo de disponibilidad en SQL Server Standard Edition.

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 **Database**, **Instance** o **Availability Group** en la lista desplegable **View**.

   Haga clic en y seleccione el nombre de host y la instancia de SQL Server para filtrar los recursos. A continuación, puede hacer clic en para cerrar el panel de filtros.

3. Haga clic en **Actualizar recursos**.

   Los recursos recién agregados, cuyo nombre se ha cambiado o eliminado se actualizan al inventario de SnapCenter Server.

   Es necesario actualizar los recursos si se cambia el nombre de las bases de datos fuera de SnapCenter.

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

   - Si la base de datos está en un almacenamiento que no es de NetApp, `Not available for backup` se muestra en la columna **Estado general**.

     No es posible ejecutar operaciones de protección de datos en una base de datos que se encuentra en un almacenamiento de terceros.

   - Si la base de datos está en un almacenamiento NetApp y no está protegida, `Not protected` se muestra en la columna **Estado general**.
   - Si la base de datos está en un sistema de almacenamiento NetApp y está protegida, la interfaz de usuario muestra `Backup not run` el mensaje en la columna **Estado general**.
   - Si la base de datos está en un sistema de almacenamiento NetApp y está protegida y si se activa la copia de seguridad para la base de datos, la interfaz de usuario muestra `Backup succeeded` el mensaje en la columna **Estado general**.

Si ha habilitado una autenticación SQL al configurar las credenciales, la instancia o base de datos detectadas se mostrarán con un icono de candado rojo. Si aparece el icono de candado, debe especificar las credenciales de la instancia o la base de datos para añadir correctamente la instancia o la base de datos al grupo de recursos.

1. Después de que el administrador de SnapCenter asigne los recursos a un usuario de RBAC, el usuario de RBAC debe iniciar sesión y hacer clic en **Actualizar recursos** para ver la última **Estado general** de los recursos.

Migrar recursos al sistema de almacenamiento de NetApp

Después de haber aprovisionado el sistema de almacenamiento de NetApp con el plugin de SnapCenter para Microsoft Windows, puede migrar los recursos al sistema de almacenamiento de NetApp o de un LUN de NetApp a otro LUN de NetApp mediante la interfaz gráfica de usuario (GUI) de SnapCenter o los cmdlets de PowerShell.

Antes de empezar

- Debe haber añadido sistemas de almacenamiento al servidor SnapCenter.
- Debe haber actualizado (detectado) los recursos de SQL Server.

La mayoría de los campos en estas páginas del asistente son claros y explicativos. La siguiente información describe algunos de los campos que pueden requerir explicación.

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 **Database** o **Instance** en la lista desplegable **View**.
3. Seleccione la base de datos o la instancia de la lista y haga clic en **migrar**.
4. En la página Resources, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Nombre de la base de datos (opcional)	Si ha seleccionado una instancia para la migración, debe seleccionar las bases de datos de esa instancia en la lista desplegable **bases de datos**.
Elija Destinos	Seleccione la ubicación objetivo para los archivos de datos y de registro. Los archivos de datos y de registro se mueven a la carpeta Data and Log correspondiente en la unidad de NetApp seleccionada. Si falta alguna carpeta en la estructura de carpetas, se crea una carpeta y se migra el recurso.

Para este campo…	Realice lo siguiente…
Mostrar detalles del archivo de base de datos (opcional)	Seleccione esta opción si desea migrar varios archivos de una única base de datos. Esta opción no se muestra cuando selecciona el recurso **Instance**.
Opciones	Seleccione **Delete copy of Migrated Database at original Location** para eliminar la copia de la base de datos del origen. Opcional: **EJECUTE ESTADÍSTICAS DE ACTUALIZACIÓN en tablas antes de desvincular la base de datos**.

5. En la página Verify, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Opciones de comprobación de consistencia de base de datos	Seleccione **Ejecutar antes de** para comprobar la integridad de la base de datos antes de la migración. Seleccione **Ejecutar después de** para comprobar la integridad de la base de datos después de la migración.

Para este campo…	Realice lo siguiente…
Opciones de DBCC CHECKDB	• Seleccione la opción **PHYSICAL_ONLY** para limitar la comprobación de integridad a la estructura física de la base de datos y detectar páginas dañadas, errores de sumas de comprobación y errores de hardware habituales que afecten a la base de datos. • Seleccione la opción **NO_INFOMSGS** para suprimir todos los mensajes informativos. • Seleccione la opción **ALL_ERRORMSGS** para visualizar todos los errores notificados por objeto. • Seleccione la opción **NOINDEX** si no desea comprobar los índices no almacenados en clúster. La base de datos de SQL Server utiliza la comprobación de la consistencia de base de datos de Microsoft SQL Server para comprobar la integridad lógica y física de los objetos de la base de datos. Se recomienda seleccionar esta opción para disminuir el tiempo de ejecución. • Seleccione la opción **TABLOCK** para limitar las comprobaciones y obtener bloqueos en lugar de utilizar una instantánea interna de la base de datos.

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

Crear políticas de backup para bases de datos de SQL Server

Es posible crear una política de backup para el recurso o el grupo de recursos antes de usar SnapCenter con el fin de realizar un backup de los recursos de SQL Server. También es posible crear una política de backup en el momento de crear un grupo de recursos o realizar un backup de un único recurso.

Antes de empezar

- Debe estar definida la estrategia de protección de datos.
- Debe haberse preparado para la protección de datos completando ciertas tareas, como instalar SnapCenter, añadir hosts, identificar recursos y crear conexiones con el sistema de almacenamiento.
- Debe haber configurado el directorio de registro del host para backup de registro.
- Debe haber actualizado (detectado) los recursos de SQL Server.

- Si va a replicar snapshots en un reflejo o almacén, el administrador de SnapCenter debe haberle asignado las máquinas virtuales de almacenamiento (SVM) para los volúmenes de origen y de destino.

  Para obtener información sobre cómo los administradores asignan recursos a los usuarios, consulte la información de instalación de SnapCenter.

- Si desea ejecutar los scripts de PowerShell en scripts previos y posteriores, debe establecer el valor del parámetro usePowershellProcessforScripts en TRUE en el archivo web.config.

  El valor predeterminado es FALSE.

- Para obtener más información sobre continuidad del negocio con SnapMirror (SM-BC), consulte los requisitos previos y las limitaciones "Límites de objetos para la continuidad del negocio de SnapMirror".

Acerca de esta tarea

- Una política de backup es un conjunto de reglas que rigen cómo gestionar y conservar backups, y con qué frecuencia se realizará un backup del recurso o del grupo de recursos. De forma adicional, se puede especificar la configuración de replicación y script. Puede especificar opciones en la política para ahorrar tiempo cuando desee reutilizarla con otro grupo de recursos.

  LA RUTA_DE_SCRIPTS se define mediante la clave PredefinedWindowsScriptsDirectory ubicada en el archivo SMCoreServiceHost.exe.Config del host del plugin.

  Si es necesario, puede cambiar esta ruta y reiniciar el servicio SMcore. Se recomienda utilizar la ruta predeterminada para la seguridad.

  El valor de la tecla se puede mostrar desde swagger a través de la API: API /4.7/config settings

  Puede usar LA API GET para mostrar el valor de la clave. No se admite LA CONFIGURACIÓN de API.

- 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 Snapshot, se evita la eliminación de las snapshots hasta que caduque el período de retención. Esto podría llevar a retener 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.

Paso 1: Crear nombre de política

1. En el panel de navegación izquierdo, selecciona **Configuración**.
2. En la página Configuración, selecciona **Políticas**.
3. Selecciona **Nuevo**.

4. En la página **Nombre**, introduzca el nombre y la descripción de la directiva.

Paso 2: Configure las opciones de copia de seguridad

1. Seleccione el tipo de backup

Backup completo y backup de registros

Realizar un backup de los archivos de la base de datos y los registros de transacciones y para truncar los registros de transacciones.

1. Seleccione **copia de seguridad completa y copia de seguridad de registro**.
2. Introduzca el número máximo de bases de datos que se deben incluir en un backup para cada Snapshot.

Debe aumentar dicho valor si desea ejecutar varias operaciones de backup en forma simultánea.

Backup completo

Realice un backup de los archivos de la base de datos.

1. Seleccione **copia de seguridad completa**.
2. Introduzca el número máximo de bases de datos que se deben incluir en un backup para cada Snapshot. El valor predeterminado es 100

Debe aumentar dicho valor si desea ejecutar varias operaciones de backup en forma simultánea.

Backup de registros

Realice un backup de los registros de transacciones. . Seleccione **copia de seguridad de registro**.

Copiar solo backup

1. Si va a realizar una copia de seguridad de los recursos mediante otra aplicación de copia de seguridad, seleccione **copia sólo copia de seguridad**.

Mantener los registros de transacciones intactos permite a cualquier aplicación de backup restaurar la base de datos. Por lo general, no debe utilizar la opción de solo copiar en ningún otro caso.

Microsoft SQL no es compatible con la opción **copia de seguridad sólo** junto con la opción **copia de seguridad completa y copia de seguridad de registro** para almacenamiento secundario.

1. En la sección Availability Group Settings, realice las siguientes acciones:

   a. Backup únicamente en la réplica de backup preferida.

      Seleccione esta opción para realizar un backup solo en la réplica de backup preferida. La réplica de backup preferida se decide mediante las preferencias de backup configuradas para el AG en SQL Server.

b. Seleccione replicas for backup.

   Seleccione la réplica principal o secundaria del AG para el backup.

c. Seleccionar prioridad de backup (prioridad de backup mínima y máxima)

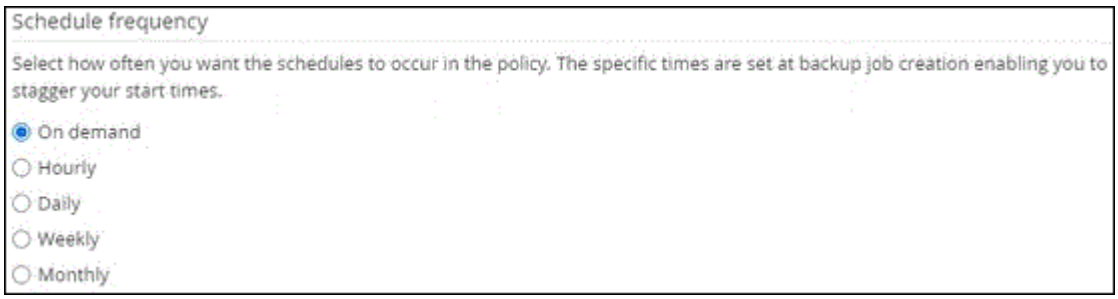
   Indique un número mínimo y un número máximo de prioridad de backup mediante los cuales se determine la réplica de AG para backup. Por ejemplo, puede tener una prioridad mínima de 10 y una prioridad máxima de 50. En este caso, se tendrán en cuenta para el backup todas las réplicas de AG que tengan una prioridad superior a 10 e inferior a 50.

   De forma predeterminada, la prioridad mínima es 1 y la máxima es 100.

> En las configuraciones de clúster, los backups se conservan en cada nodo del clúster según la configuración de retención establecida en la política. Si cambia el nodo propietario del AG, las copias de seguridad se realizan según la configuración de retención y se conservarán las copias de seguridad del nodo propietario anterior. La retención de AG solo se aplica a nivel de nodo.

2. Programe la frecuencia de backup para esta política. Especifique el tipo de horario seleccionando **On Demand**, **Hourly**, **Daily**, **Weekly** o **Monthly**.

   Solo puede seleccionar un tipo de programación por política.



> Puede especificar la programación (fecha de inicio, fecha de finalización y frecuencia) para la operación de backup mientras crea un grupo de recursos. De este modo, se pueden crear grupos de recursos que comparten la misma política y frecuencia de backup, pero se pueden 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.

Paso 3: Configure los ajustes de retención

En la página Retention, según el tipo de backup seleccionado en la página de tipo de backup, realice una o más de las siguientes acciones:

1. En la sección Retention settings para la operación de restauración de último minuto, realice una de las siguientes acciones:

Número específico de copias

Conserve únicamente una cantidad específica de snapshots.

1. Seleccione la opción **Keep log backups aplicable a Last <number> Days** y especifique el número de días que se conservarán. Si se acerca a ese límite, tal vez deba eliminar copias más antiguas.

Número específico de días

Retener las copias de backup por una cantidad determinada de días.

1. Seleccione la opción **Keep log backups applicable to last <number> days of full backups** y especifique el número de días que se conservarán las copias de seguridad de registros.

1. En la sección **Configuración de copias de seguridad completas** para la configuración de retención a petición, realice las siguientes acciones:
   a. Especifique el número total de snapshots que desea conservar
      i. Para especificar el número de instantáneas que se deben conservar, seleccione **Total de copias snapshot que se deben conservar**.
      ii. Si la cantidad de snapshots supera el número especificado, las snapshots se eliminan empezando por las más antiguas.

De forma predeterminada, el valor del número de retención se establece en 2. 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.

El valor de retención máximo es 1018 para recursos en ONTAP 9.4 o posterior, y 254 para recursos en ONTAP 9.3 o anterior. Se producirá un error en los backups si la retención se establece en un valor superior a la versión de ONTAP subyacente.

1. Tiempo que se conservan las Snapshots
   a. Si desea especificar el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas, seleccione **Mantener copias instantáneas para**.
2. Si desea especificar el período de bloqueo de la instantánea, seleccione **Período de bloqueo de la copia de instantánea** y seleccione Días, meses o años.

   El período de retención de SnapLock debe ser inferior a 100 años.

3. En la sección **Configuración de copias de seguridad completas** para la configuración de retención por hora, por día, por semana y por mes, especifique la configuración de retención para el tipo de programación seleccionado en la página Tipo de copia de seguridad.
   a. Especifique el número total de snapshots que desea conservar
      i. Para especificar el número de instantáneas que se deben conservar, seleccione **Total de copias snapshot que se deben conservar**. Si la cantidad de snapshots supera el número especificado, las snapshots se eliminan empezando por las más antiguas.

Debe establecer el número de retención en 2 o un valor más alto si tiene pensado 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.

1. Tiempo que se conservan las Snapshots
   a. Para especificar el número de días durante los cuales desea conservar las instantáneas antes de eliminarlas, seleccione **Mantener copias instantáneas para**.
2. Si desea especificar el período de bloqueo de la instantánea, seleccione **Período de bloqueo de la copia de instantánea** y seleccione Días, meses o años.

   El período de retención de SnapLock debe ser inferior a 100 años.

   De forma predeterminada, la retención de Snapshot de registro se establece en 7 días. Use el cmdlet Set-SmPolicy para cambiar la retención de Snapshot de registro.

En este ejemplo, se establece la retención de Snapshot de registro en 2:

Ejemplo 1. Muestra el ejemplo

```
Set-SmPolicy -PolicyName 'newpol' -PolicyType 'Backup' -PluginPolicyType 'SCSQL' -sqlbackuptype
'FullBackupAndLogBackup' -RetentionSettings
@{BackupType='DATA';ScheduleType='Hourly';RetentionCount=2},@{BackupType='LOG_SNAPSHOT';
ScheduleType='None'=HoRetentionCount='Hourly';RetentionType='2';RetentionType='Hourly';RetentionC
ount=2}
```

"SnapCenter conserva copias Snapshot de la base de datos"

Paso 4: Configure los ajustes de replicación

1. En la página Replication, especifique la replicación en el sistema de almacenamiento secundario:

Actualice SnapMirror

Actualice SnapMirror después de crear una copia snapshot local.

1. Seleccione esta opción para crear copias de SnapMirror de conjuntos de backups en otro volumen (SnapMirror).

   Esta opción debe estar habilitada para continuidad del negocio con SnapMirror (SM-BC) o para SnapMirror Sync (SM-S).

   Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP.

   Consulte "Consulte los backups y los clones de SQL Server en la página Topology".

Actualizar SnapVault

Actualice SnapVault después de crear una copia snapshot.

1. Seleccione esta opción para realizar una replicación de backup de disco a disco.

   Durante la replicación secundaria, el tiempo de caducidad del SnapLock carga el tiempo de caducidad del SnapLock principal. Al hacer clic en el botón **Refrescar** de la página Topología, se actualiza el tiempo de caducidad de SnapLock secundario y primario que se recuperan de ONTAP.

   Cuando SnapLock se configura solo en el secundario desde ONTAP conocido como Almacén de SnapLock, al hacer clic en el botón **Refrescar** de la página Topología se actualiza el período de bloqueo en el secundario que se recupera de ONTAP.

   Para obtener más información sobre el Almacén SnapLock, consulte "Confirmar copias Snapshot a WORM en un destino de almacén"

   Consulte "Consulte los backups y los clones de SQL Server en la página Topology".

Etiqueta de política secundaria

1. Seleccione una etiqueta de Snapshot.

Según la etiqueta de Snapshot que seleccione, ONTAP aplicará la política de retención de Snapshot secundaria que corresponda a esa etiqueta.

> Si ha seleccionado **Actualizar SnapMirror después de crear una copia Snapshot local**, puede especificar opcionalmente la etiqueta de la directiva secundaria. Sin embargo, si ha seleccionado **Actualizar SnapVault después de crear una copia Snapshot local**, debe especificar la etiqueta de la directiva secundaria.

Recuento de reintentos de error

1. Introduzca el número de intentos de replicación que deben producirse antes de que se interrumpa el proceso.

Paso 5: Configurar los ajustes de script

1. En la página Script, introduzca la ruta y los argumentos del script previo o script posterior que se deben ejecutar antes o después de la operación de backup, según corresponda.

   Por ejemplo, se puede ejecutar un script para actualizar capturas SNMP, automatizar alertas y enviar registros.

   La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

   Debe configurar la política de retención de SnapMirror en ONTAP para que el almacenamiento secundario no alcance el límite máximo de Snapshots.

Paso 6: Configure los ajustes de verificación

En la página Verification, realice los siguientes pasos:

1. En la sección Run verification for following backup schedules, seleccione la frecuencia de backup.
2. En la sección Database consistency check options, realice las siguientes acciones:
   a. Limitar la estructura de integridad a la estructura física de la base de datos (PHYSICAL_ONLY)
      i. Seleccione **limitar la estructura de integridad a la estructura física de la base de datos (PHYSICAL_ONLY)** para limitar la comprobación de integridad a la estructura física de la base de datos y detectar páginas dañadas, errores de sumas de comprobación y errores de hardware habituales que afecten a la base de datos.
   b. Suprimir todos los mensajes de información (NO INFOMSGS)
      i. Seleccione **Supress all information messages (NO INFOMSGS)** para suprimir todos los mensajes informativos. Seleccionado de forma predeterminada.
   c. Visualizar todos los mensajes de error notificados por objeto (ALL_ERRORMSGS)
      i. Seleccione **Display all reported error messages per object (ALL_ERRORMSGS)** para visualizar todos los errores notificados por objeto.
   d. No comprobar los índices no almacenados en clúster (NOINDEX)
      i. Seleccione **no comprobar los índices no almacenados en clúster (NOINDEX)** si no desea comprobar los índices no almacenados en clúster. La base de datos de SQL Server utiliza la comprobación de la consistencia de base de datos de Microsoft SQL Server para comprobar la integridad lógica y física de los objetos de la base de datos.
   e. Limitar las comprobaciones y obtener los bloqueos en lugar de utilizar una instantánea de la base de datos interna (TABLOCK)
      i. Seleccione **Limitar las comprobaciones y obtener los bloqueos en lugar de utilizar una copia Snapshot interna de la base de datos (TABLOCK)** para limitar las comprobaciones y obtener bloqueos en lugar de utilizar una instantánea interna de la base de datos.
3. En la sección **Backup de registro**, seleccione **verificar copia de seguridad de registro al finalizar** para verificar la copia de seguridad de registro al finalizar.
4. En la sección **Verification script settings**, introduzca la ruta de acceso y los argumentos del script previo o posterior que deben ejecutarse antes o después de la operación de verificación, respectivamente.

La ruta scripts previos o posteriores no debe incluir unidades o recursos compartidos. La ruta debe ser relativa a LA RUTA DE ACCESO_SCRIPTS.

Paso 7: Resumen de la revisión

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

Crear grupos de recursos y asociar políticas para SQL Server

Un grupo de recursos es un contenedor al cual se añaden recursos que se quieren incluir en un backup y proteger en su conjunto. Un grupo de recursos permite realizar un backup en simultáneo de 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.

Puede proteger los recursos individualmente sin crear un grupo de recursos nuevo. Puede realizar backups del recurso protegido.

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.
- No se permite añadir bases de datos nuevas sin SM-BC a un grupo de recursos existente que contiene recursos con SM-BC.
- No se admite la adición de bases de datos nuevas a un grupo de recursos existente en modo de conmutación al nodo de respaldo de SM-BC. Puede añadir recursos al grupo de recursos solo en estado normal o de conmutación por error.

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 **Database** en la lista **View**.

   Si recientemente ha agregado un recurso a SnapCenter, haga clic en **Actualizar recursos** para ver el recurso recién añadido.

3. Haga clic en **Nuevo grupo de recursos**.
4. En la página Name, realice los siguientes pasos:

Para este campo…	Realice lo siguiente…
Nombre	Escriba el nombre del grupo de recursos. El nombre del grupo de recursos no debe superar los 250 caracteres.
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.
Utilice un formato de nombre personalizado para la copia de Snapshot	Opcional: Introduzca un nombre y un formato de Snapshot personalizados. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la Snapshot.

5. En la página Resources, realice los siguientes pasos:
   a. Seleccione el nombre del host, el tipo de recurso y la instancia de SQL Server en las listas desplegables para filtrar la lista de recursos.

      Si recientemente añadió recursos, aparecerán en la lista Available Resources solo después de actualizar la lista de recursos.

   b. Para mover recursos de la sección **Recursos disponibles** a la sección Recursos seleccionados, realice uno de los siguientes pasos:
      - Seleccione **Autoselect all resources on same Storage volume** para mover todos los recursos del mismo volumen a la sección Selected Resources.
      - 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 Policies, realice los siguientes pasos:
   a. Seleccione una o varias políticas de la lista desplegable.

      También puede crear una política haciendo clic en + .

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

   b. En la sección Configure schedules for selected policies, haga clic en * + en la columna Configure Schedules de la política para la cual desea configurar la programación.
   c. En el cuadro de diálogo Add schedules for policy *policy_name*, configure la programación especificando la fecha de inicio, la fecha de caducidad y la frecuencia y, a continuación, haga clic en **Aceptar**.

Debe hacerlo con cada frecuencia que figure en la política. Los horarios configurados se enumeran en la columna Applied Schedules en la sección **Configure schedules for selected policies**.

d. Seleccione Microsoft SQL Server Scheduler.

También debe seleccionar una instancia de programador para asociar con la política de programación.

Si no selecciona Microsoft SQL Server Scheduler, el valor predeterminado es Microsoft Windows Scheduler.

No se admiten programas de backup de terceros cuando se solapan con los programas de backup de SnapCenter. No debe modificar las programaciones y cambiar el nombre del trabajo de backup creado en el programador de Windows o el agente de SQL Server.

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

a. Seleccione el servidor de verificación de la lista desplegable **servidor de verificación**.

La lista incluye todos los servidores SQL agregados en SnapCenter. Puede seleccionar varios servidores de verificación (host local o remoto).

La versión del servidor de verificación debe coincidir con la versión y edición del servidor SQL que aloja la base de datos principal.

a. Haga clic en **Load locators** para cargar los volúmenes de SnapMirror y SnapVault y realizar la verificación en el almacenamiento secundario.

b. Seleccione la política para la que desea configurar la programación de verificación y haga clic en * *.

c. En el cuadro de diálogo Add Verification Schedules policy_name, realice las siguientes acciones:

Si desea…	Realice lo siguiente…
Ejecutar la verificación después del backup	Seleccione **Ejecutar verificación después de la copia de seguridad**.
Programar una verificación	Seleccione **Ejecutar verificación programada**.

d. Haga clic en **Aceptar**.

Las programaciones configuradas figuran en la columna Applied Schedules. Para revisar y editar, haga clic en * * o en para eliminar, haga clic en .

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. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.

Para habilitar la notificación por correo electrónico, debe tener especificados los detalles del servidor SNMP ya sea mediante la GUI o el comando Set-SmSmtpServer de PowerShell.

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

Información relacionada

"Crear políticas de backup para bases de datos de SQL Server"

Requisitos para realizar backups de recursos de SQL

Antes de realizar el backup de un recurso de SQL, debe asegurarse de que se cumplan varios requisitos.

- Debe haber migrado el recurso de un sistema de almacenamiento que no sea de NetApp a un sistema de almacenamiento de NetApp.
- 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".
- Se produce un error en la operación de backup iniciada por un usuario de Active Directory (AD) si la credencial de la instancia de SQL no está asignada al usuario o grupo de AD. Debe asignar la credencial de instancia SQL a un usuario o grupo de AD desde la página **Configuración** > **acceso de usuario**.
- Debe tener creado un grupo de recursos con una política anexada.
- Si un grupo de recursos tiene varias bases de datos de diferentes hosts, es posible que la operación de backup en algunos hosts se active tarde debido a problemas de red. Debe configurar el valor de FMaxRetryForUninitializedHosts en web.config con el cmdlet Set-SmConfigSettings de PS.

Realice backups de recursos de SQL

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

Acerca de esta tarea

- Para la autenticación de credenciales de Windows, debe configurar la credencial antes de instalar los plugins.
- Para la autenticación de la instancia de SQL Server, debe añadir la credencial después de instalar los plugins.
- Para la autenticación GMSA, debe configurar GMSA mientras registra el host con SnapCenter en la página **Agregar host** o **Modificar host** para activar y utilizar el GMSA.
- Si el host se agrega con GMSA y si el GMSA tiene privilegios de inicio de sesión y administrador del sistema, el GMSA se utilizará para conectarse a la instancia de SQL.

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 **Database** ,or **Instance**, o **Availability Group** en la lista desplegable

View.

a. Seleccione la base de datos, la instancia o el grupo de disponibilidad que desea incluir en un backup.

   Cuando se realiza el backup de una instancia, la información acerca del último estado de backup o sobre la fecha/hora de esa instancia no están disponibles en la página de recursos.

En la vista de topología, no puede diferenciar si el estado del backup, la fecha/hora o el backup corresponden a una instancia o a una base de datos.

3. En la página Resources, active la casilla de comprobación **custom name format for Snapshot copy** y, a continuación, introduzca un formato de 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.

4. En la página Policies, ejecute las siguientes tareas:

   a. En la sección Policies, seleccione una o más políticas de la lista desplegable.

      Puede crear una política seleccionando  para iniciar el asistente de políticas.

      En la sección **Configurar horarios para directivas seleccionadas**, se muestran las directivas seleccionadas.

   b. Seleccione  en la columna Configure Schedules correspondiente a la política para la cual desea configurar una programación.

   c. En el cuadro de diálogo **Agregar horarios para política** `policy_name` , configure el horario y luego seleccione **Aceptar**.

      Este `policy_name` es el nombre de la política que ha seleccionado.

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

   a. Seleccione **Use Microsoft SQL Server Scheduler** y, a continuación, seleccione la instancia del programador en la lista desplegable **Scheduler Instance** asociada con la directiva de programación.

5. En la página Verification, realice los siguientes pasos:

   a. Seleccione el servidor de verificación de la lista desplegable **servidor de verificación**.

      Puede seleccionar varios servidores de verificación (host local o remoto).

      La versión del servidor de verificación debe ser igual o superior a la versión de la edición del servidor SQL que aloja la base de datos principal.

   a. Seleccione **cargar localizadores secundarios para verificar copias de seguridad en secundario** para verificar las copias de seguridad en el sistema de almacenamiento secundario.

   b. Seleccione la política para la que desea configurar la programación de verificación y, a continuación, seleccione * *  .

c. En el cuadro de diálogo Add Verification Schedules *policy_name*, realice las siguientes acciones:

Si desea…	Realice lo siguiente…
Ejecutar la verificación después del backup	Seleccione **Ejecutar verificación después de la copia de seguridad**.
Programar una verificación	Seleccione **Ejecutar verificación programada**.

Si el servidor de verificación no tiene una conexión de almacenamiento, la operación de verificación genera un error: No se pudo montar el disco.

d. Seleccione **OK**.

Las programaciones configuradas figuran en la columna Applied Schedules.

6. 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. Si desea adjuntar el informe de la operación realizada en el grupo de recursos, seleccione **Adjuntar informe de trabajo**.

Para habilitar la notificación por correo electrónico, debe tener especificados los detalles del servidor SNMP ya sea mediante la GUI o el comando Set-SmSmtpServer de PowerShell.

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

Se muestra la página de topología de la base de datos.

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

a. Si ha aplicado 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 **verificar después de la copia de seguridad** para verificar la copia de seguridad.

c. Seleccione **copia de seguridad**.

No debe cambiar el nombre del trabajo de backup creado en el programador de Windows o el agente de SQL Server.

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.

Se crea un grupo de recursos implícito. Para ver esto, seleccione el usuario o grupo correspondiente en la

página acceso de usuario. El tipo de grupo de recursos implícito es "'recurso'".

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

Después de terminar

- En las configuraciones de MetroCluster, es posible que SnapCenter no pueda detectar una relación de protección tras una conmutación por error.

  "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/scvservice. En ese script, el `do_start method` comando inicia el servicio del plugin de VMware de SnapCenter. Actualice ese comando a lo siguiente `Java -jar -Xmx8192M -Xms4096M:` .

Información relacionada

"Crear políticas de backup para bases de datos de SQL Server"

"Realizar backup de recursos con cmdlets de PowerShell"

"Se produce un error en las operaciones de backup con un error de conexión de MySQL debido a una demora en TCP_TIMEOUT"

"Error de backup con programador de Windows"

"Error de operaciones de inactivación o agrupación de recursos"

Realizar un backup de grupos de recursos de SQL Server

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 ingresando su nombre en el cuadro de búsqueda o seleccionando * * y, luego, seleccionando la[Icono de filtro]etiqueta. A continuación, puede seleccionar **[Icono de filtro]** 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. Después de la copia de seguridad, seleccione **Verify** para verificar la copia de seguridad bajo demanda.

La opción **verificar** de la directiva sólo se aplica a los trabajos programados.

c. Seleccione **copia de seguridad**.

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

Información relacionada

"Crear políticas de backup para bases de datos de SQL Server"

"Crear grupos de recursos y asociar políticas para SQL Server"

"Realizar backup de recursos con cmdlets de PowerShell"

"Se produce un error en las operaciones de backup con un error de conexión de MySQL debido a una demora en TCP_TIMEOUT"

"Error de backup con programador de Windows"

Supervisar las operaciones de backup

Supervise las operaciones de backup de los recursos de SQL en la página SnapCenter Jobs

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
- Con errores
- 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 se muestra el estado del trabajo de copia de seguridad ✔ , al hacer clic en los detalles del trabajo, es posible que algunas de las tareas secundarias de la operación de copia de seguridad estén aún 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 recursos de SQL 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**.

Crear una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell

Debe crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar los cmdlets de PowerShell para realizar operaciones de protección de datos.

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 complementos de host en curso al añadir una conexión a sistemas de almacenamiento, ya que puede que la caché del host no se actualice y que el estado de las bases de

datos pueda aparecer en la interfaz gráfica de usuario de SnapCenter como «'no disponible para el backup' o «'no en el almacenamiento de NetApp'».

- 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 gestión única.

Pasos

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

   En este ejemplo, se abre una sesión de PowerShell:

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

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

   En este ejemplo, se crea una nueva conexión con el sistema de almacenamiento:

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

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

   En este ejemplo, se crea una nueva credencial llamada FinanceAdmin con las credenciales de Windows:

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

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".

Realizar backup de recursos con cmdlets de PowerShell

Puede utilizar los cmdlets de PowerShell para realizar backup de bases de datos de SQL Server o sistemas de archivos Windows. Esto incluye la realización de backups de una base de datos de SQL Server o de un sistema de archivos de Windows incluye establecer una conexión con SnapCenter Server, determinar las instancias de la base de datos de SQL Server o los sistemas de archivos Windows, crear un grupo de recursos de backup, realizar el backup y verificar.

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.
- Es necesario haber añadido los hosts y detectado los recursos.

Pasos

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

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

   Se muestra una solicitud de nombre de usuario y contraseña.

2. Cree una política de backup mediante el cmdlet Add-SmPolicy.

   En este ejemplo, se crea una nueva política de backup con el tipo de backup de SQL fullbackup:

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

   En este ejemplo, se crea una nueva política de backup con el tipo de backup de sistema de archivos Windows CrashConsistent:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Para detectar recursos de host se usa el cmdlet Get-SmResources.

   En este ejemplo, se determinan los recursos para el plugin de Microsoft SQL en el host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

   En este ejemplo, se determinan los recursos para los sistemas de archivos Windows en el host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Añada un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.

   En este ejemplo, se crea un nuevo grupo de recursos de backup de base de datos de SQL con la política y los recursos especificados:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

En este ejemplo, se crea un nuevo grupo de recursos de backup de sistema de archivos Windows con la política y los recursos especificados:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Para iniciar una tarea de backup se usa el cmdlet New-SmBackup.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Consulte el estado del trabajo de backup mediante el cmdlet Get-SmBackupReport.

   Este ejemplo muestra un informe con un resumen de todos los trabajos realizados en la fecha especificada:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

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".

Cancelar las operaciones de backup del plugin de SnapCenter para Microsoft SQL Server

Es posible cancelar las operaciones de backup que se ejecutan, se encuentran en cola o no responden. Cuando se cancela una operación de backup, el servidor de SnapCenter detiene la operación y quita todas las snapshots del almacenamiento si el backup creado no se registró en el servidor de SnapCenter. Si la copia de seguridad ya está registrada en el servidor de SnapCenter, no revertirá la copia snapshot ya creada incluso después de que se active la cancelación.

Antes de empezar

- Inició sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones de restauración.

- Solo es posible cancelar las operaciones de registro o backup completo que se encuentran en cola o en ejecución.
- No se puede cancelar la operación una vez iniciada la verificación.

  Si cancela la operación antes de verificarlo, se cancelará la operación y no realizará la operación de verificación.

- Es posible cancelar una operación de backup desde la página Monitor o el panel Activity.
- Además de usar la interfaz gráfica de usuario de SnapCenter, es posible usar los cmdlets de PowerShell para cancelar las operaciones.
- 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

Ejecute una de las siguientes acciones:

Del…	Acción
Página Monitor	1. En el panel de navegación izquierdo, selecciona **Monitor** > **Trabajos**. 2. Seleccione el trabajo y seleccione **Cancelar trabajo** .
Panel de actividades	1. Después de iniciar la tarea de backup, seleccione en el panel Activity para ver las cinco operaciones más recientes. 2. Seleccione la operación. 3. En la página Detalles del trabajo, seleccione **Cancelar trabajo**.

Resultado

Se cancela la operación y el recurso se revierte al estado anterior. Si la operación que canceló no responde en el estado de cancelación o ejecución, debe ejecutar el `Cancel-SmJob -JobID <int> -Force` cmdlet para detener forzosamente la operación de backup.

Consulte los backups y los clones de SQL Server 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

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.

Puede consultar los siguientes iconos en la vista **Administrar copias** para determinar si las copias de seguridad y clones están disponibles en el almacenamiento principal y secundario (copias reflejadas o copias vault).

-  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 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.

Si tiene una relación secundaria como Continuidad empresarial de SnapMirror (SM-BC), verá los siguientes iconos adicionales:

-  implica que el sitio de réplica está activo.
-  implica que el sitio de réplica está caído.
-  implica que no se restableció la relación de reflejo o almacén secundario.

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 seleccionado es una base de datos clonada, protéjala. El origen del clon se muestra en la página Topology. Haga clic en **Detalles** para ver la copia de seguridad utilizada para clonar.

   Si el recurso está protegido, se muestra la página Topology del recurso seleccionado.
4. Consulte Summary Card para ver un resumen de la cantidad de backups y clones disponibles en el

almacenamiento principal y secundario.

La sección **Tarjeta de resumen** muestra el número total de copias de seguridad 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.

Para la continuidad del negocio con SnapMirror (SM-BC), al hacer clic en el botón **Actualizar**, se actualiza el inventario de backup de SnapCenter consultando ONTAP tanto para los sitios primarios como de réplica. Una programación semanal también realiza esta actividad para todas las bases de datos que contienen una relación SM-BC.

- Para las relaciones SM-BC, Mirror asíncrono, Vault o MirrorVault con el nuevo destino primario se deben configurar manualmente después de la conmutación al nodo de respaldo.
- Después de la conmutación por error, es necesario crear un backup para que SnapCenter detecte la conmutación al nodo de respaldo. Puede hacer clic en **Actualizar** solo después de que se haya creado una copia de seguridad.

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 en la tabla y haga clic en los iconos de protección de datos para realizar operaciones de restauración, clonado, cambio de nombre y eliminación.

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

7. Seleccione un clon de la tabla y haga clic en **Clonar división**.
8. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en .

Quitar los backups con el cmdlet de PowerShell

Puede utilizar el cmdlet Remove-SmBackup para eliminar backups si ya no los necesita para otras operaciones de protección de datos.

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.

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

2. Elimine uno o varios backups con el cmdlet Remove-SmBackup.

   Este ejemplo elimina dos backups según sus ID de backup:

```
Remove-SmBackup -BackupIds 3,4
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Borre el número de backup secundario con cmdlets de PowerShell

Puede utilizar el cmdlet Remove-SmBackup para borrar el número de backups de backups secundarios que no tienen Snapshot. Se recomienda utilizar este cmdlet cuando el total de las Snapshot que se muestran en la topología Manage Copies no corresponde al valor de retención de Snapshot del almacenamiento secundario.

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.

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

2. Borre el número de backups secundarios con el parámetro -CleanupSecondaryBackups.

   Este ejemplo borra el número de backups para backups secundarios sin snapshots:

```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```