Proteger bases de datos de Microsoft SQL Server

SnapCenter Software 4.9

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/es-es/snapcenter-49/protect-scsql/concept_snapcenter_plug_in_for_microsoft_sql_server_overview.html on September 26, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Proteger bases de datos de Microsoft SQL Server . . . 1
Plugin de SnapCenter para Microsoft SQL Server . . . 1
Información general sobre el plugin de SnapCenter para Microsoft SQL Server . . . 1
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para Microsoft SQL Server . . . 1
Funciones del plugin de SnapCenter para Microsoft SQL Server . . . 2
Compatibilidad con asignación de LUN asimétrica en clústeres de Windows . . . 3
Tipos de almacenamiento compatibles con los plugins de SnapCenter para Microsoft Windows y Microsoft SQL Server . . . 4
Recomendaciones sobre distribución de almacenamiento para el plugin de SnapCenter para Microsoft SQL Server . . . 7
Privilegios mínimos de ONTAP requeridos para el plugin de SQL . . . 9
Preparar los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para el plugin para SQL Server . . . 11
Estrategia de backup para recursos de SQL Server . . . 12
Estrategia de restauración para SQL Server . . . 17
Defina una estrategia de clonación para SQL Server . . . 20
Inicio rápido de instalar el plugin de SnapCenter para Microsoft SQL Server . . . 21
Prepare la instalación del servidor de SnapCenter y del plugin . . . 21
Instale SnapCenter Server para Microsoft SQL Server . . . 24
Instale el plugin de SnapCenter para Microsoft SQL Server . . . 25
Preparar la instalación del plugin de SnapCenter para Microsoft SQL Server . . . 26
Flujo de trabajo de instalación del plugin de SnapCenter para Microsoft SQL Server . . . 26
Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para Microsoft SQL Server . . . 26
Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows . . . 27
Configure credenciales para el paquete de plugins de SnapCenter para Windows . . . 28
Configure las credenciales para un recurso individual de SQL Server . . . 30
Configurar GMSA en Windows Server 2012 o posterior . . . 32
Instale el plugin de SnapCenter para Microsoft SQL Server . . . 33
Configurar certificado de CA . . . 39
Configure la recuperación ante desastres . . . 43
Instale el plugin de SnapCenter para VMware vSphere . . . 45
Implemente el certificado de CA . . . 45
Configure el archivo CRL . . . 45
Prepárese para la protección de datos . . . 45
Requisitos previos para utilizar el plugin de SnapCenter para Microsoft SQL Server . . . 45
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger SQL Server . . . 46
Realizar backup de base de datos de SQL Server, instancia o grupo de disponibilidad . . . 47
Flujo de trabajo de backup . . . 47
Determine si hay recursos disponibles para backup . . . 48
Migrar recursos al sistema de almacenamiento de NetApp . . . 50
Crear políticas de backup para bases de datos de SQL Server . . . 52
Crear grupos de recursos y asociar políticas para SQL Server . . . 59
Requisitos para realizar backups de recursos de SQL . . . 61

Realice backups de recursos de SQL . . . 62
Realizar un backup de grupos de recursos de SQL Server . . . 65
Supervisar las operaciones de backup . . . 65
Crear una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell . . . 67
Realizar backup de recursos con cmdlets de PowerShell . . . 68
Cancelar las operaciones de backup del plugin de SnapCenter para Microsoft SQL Server . . . 70
Consulte los backups y los clones de SQL Server en la página Topology . . . 71
Quitar los backups con el cmdlet de PowerShell . . . 72
Borre el número de backup secundario con cmdlets de PowerShell . . . 73
Restaure recursos de SQL Server . . . 73
Restaure el flujo de trabajo . . . 74
Requisitos para restaurar una base de datos . . . 74
Restaurar backups de base de datos de SQL Server . . . 75
Restaurar una base de datos de SQL Server a partir de almacenamiento secundario . . . 80
Propagación de bases de datos de grupos de disponibilidad . . . 80
Restaurar recursos mediante los cmdlets de PowerShell . . . 81
Supervisar operaciones de restauración de recursos de SQL . . . 83
Cancelar las operaciones de restauración de recursos de SQL . . . 84
Clone recursos de bases de datos de SQL Server . . . 85
Flujo de trabajo de clonado . . . 85
Clonar a partir de un backup de base de datos de SQL Server . . . 86
Clonar backups mediante cmdlets de PowerShell . . . 89
Ejecute el ciclo de vida del clon . . . 93
Supervisar operaciones de clonado de bases de datos de SQL . . . 96
Cancelar las operaciones de clonado de recursos SQL . . . 97
Divida un clon . . . 97

Proteger bases de datos de Microsoft SQL Server

Plugin de SnapCenter para Microsoft SQL Server

Información general sobre el plugin de SnapCenter para Microsoft SQL Server

El plugin de SnapCenter para Microsoft SQL Server es un componente en el lado del host de NetApp SnapCenter Software que permite la gestión de protección de datos para aplicaciones de bases de datos de Microsoft SQL Server. El plugin para SQL Server automatiza las operaciones de backup, verificación, restauración y clonado de bases de datos de SQL Server en el entorno de SnapCenter.

Cuando se instala el plugin para SQL Server, es posible utilizar SnapCenter con la tecnología SnapMirror de NetApp para crear copias de reflejo de conjuntos de backups en otro volumen, y también con la tecnología SnapVault de NetApp para realizar replicaciones de backup disco a disco para cumplimiento de normativas o fines de archivado.

Tareas que pueden llevarse a cabo con el plugin de SnapCenter para Microsoft SQL Server

Cuando el plugin de SnapCenter para Microsoft SQL Server está instalado en el entorno, es posible usar SnapCenter para realizar backup, restaurar y clonar bases de datos de SQL Server.

Es posible ejecutar las siguientes tareas complementarias a las operaciones de backup, de restauración y de clonado de las bases de datos de SQL Server y sus recursos:

- Realizar backup de bases de datos de SQL Server y los registros de transacciones asociados

  No es posible crear un backup de registros para las bases de datos maestra y msdb. Sin embargo, puede crear backups de registros para la base de datos modelo del sistema.

- Restaurar recursos de bases de datos
  - Se pueden restaurar bases de datos de sistema maestras, msdb y modelo.
  - No es posible restaurar varias bases de datos, instancias y grupos de disponibilidad.
  - No puede restaurar la base de datos del sistema en una ruta alternativa.
- Crear clones de un momento específico para las bases de datos de producción

  No es posible ejecutar operaciones de backup, restauración, clonado o ciclo de vida en las bases de datos del sistema tempdb.

- Verifique las operaciones de backup de inmediato o aplace la verificación hasta más adelante

  No se admite la verificación de la base de datos del sistema SQL Server. SnapCenter clona las bases de datos para realizar una operación de verificación. SnapCenter no puede clonar bases de datos del sistema SQL Server y, por lo tanto, no se admite la verificación de estas bases de datos.

- Programar operaciones de backup y de clonado
- Supervisar operaciones de backup, de restauración y de clonado

> El plugin para SQL Server no es compatible con el backup y la recuperación de las bases de datos de SQL Server en los recursos compartidos SMB.

Funciones del plugin de SnapCenter para Microsoft SQL Server

El plugin para SQL Server se integra con Microsoft SQL Server en el host Windows y con la tecnología de copia de Snapshot de NetApp en el sistema de almacenamiento. Para trabajar con el plugin para SQL Server, se utiliza la interfaz de SnapCenter.

El plugin para SQL Server incluye estas características principales:

- **Interfaz gráfica de usuario unificada con tecnología SnapCenter**

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

- **Administración central automatizada**

  Es posible programar backups rutinarios de SQL Server, configurar retención de backups basada en políticas y configurar operaciones de restauración de momento específico y de último minuto. Si desea supervisar de manera proactiva el entorno de SQL Server, configure SnapCenter para que envíe alertas por correo electrónico.

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

  El plugin para SQL Server utiliza la tecnología de copia de Snapshot de NetApp con el plugin de SnapCenter para Microsoft Windows de NetApp. Esto permite realizar backups de bases de datos en cuestión de segundos y restaurarlos rápidamente sin necesidad de dejar sin conexión a SQL Server. Las copias de Snapshot consumen un espacio de almacenamiento mínimo.

Además de estas funciones principales, el plugin para SQL Server ofrece los siguientes beneficios:

- Compatibilidad con flujos de trabajo de backup, restauración, clonado y verificación
- Seguridad compatible con RBAC y delegación de roles centralizada
- Creación de copias de bases de datos de producción 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 está el clon.

- Verificación de backups no disruptiva y automatizada
- Capacidad para ejecutar varios backups al mismo tiempo entre varios servidores
- Cmdlets de PowerShell para crear scripts de operaciones de backup, verificación, restauración y clonado
- Compatibilidad con grupos de disponibilidad (AG) AlwaysOn en SQL Server para acelerar las operaciones de configuración, backup y restauración de AG

- Base de datos en memoria y extensión de espacio libre (BPE) como parte de SQL Server 2014
- Compatibilidad con backup de LUN y VMDK
- Compatibilidad con infraestructuras físicas y virtualizadas
- Compatibilidad con iSCSI, Fibre Channel, FCoE, asignación de dispositivos sin formato (RDM) y VMDK sobre NFS y VMFS

  Los volúmenes NAS deben tener una política de exportación predeterminada en la máquina virtual de almacenamiento (SVM).

- Compatibilidad con FileStream y grupos de archivos en bases de datos independientes de SQL Server.

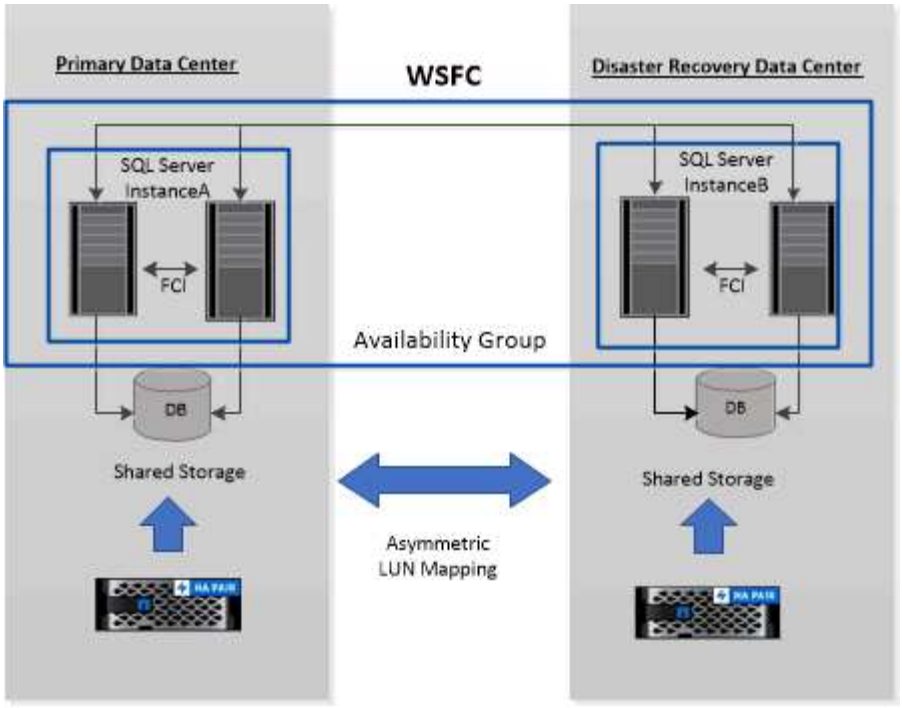
Compatibilidad con asignación de LUN asimétrica en clústeres de Windows

El plugin de SnapCenter para Microsoft SQL Server admite la detección en SQL Server 2012 y posterior, configuraciones de asignación de LUN asimétrica (ALM) para alta disponibilidad y grupos de disponibilidad para recuperación ante desastres. Al detectar recursos, SnapCenter detecta bases de datos en host locales y remotos en configuraciones de ALM.

Una configuración de ALM es un solo clúster de conmutación al nodo de respaldo del servidor Windows que contiene uno o varios nodos en un centro de datos primario y uno o varios nodos en un centro de recuperación ante desastres.

A continuación se muestra un ejemplo de configuración de ALM:

- Dos instancias de clúster de conmutación al nodo de respaldo (FCI) en un centro de datos multisitio
- FCI for local High Availability (ha) y Availability Group (AG) para la recuperación ante desastres con una instancia independiente en el centro de recuperación ante desastres



WSFC----Windows Server Failover Cluster

El almacenamiento en el centro de datos principal se comparte entre los nodos FCI presentes en el centro de datos principal. El almacenamiento en el centro de datos de recuperación ante desastres se comparte entre los nodos FCI presentes en el centro de datos de recuperación ante desastres.

El almacenamiento del centro de datos principal no es visible para los nodos en el centro de datos de recuperación ante desastres y viceversa.

La arquitectura DE ALM combina dos soluciones de almacenamiento compartido utilizadas por FCI con una solución de almacenamiento no compartido o dedicado utilizada por SQL AG. La solución AG utiliza letras de unidad idénticas para los recursos de discos compartidos entre centros de datos. Esta disposición de almacenamiento, donde un disco de clúster se comparte entre un subconjunto de nodos dentro de un WSFC, se conoce como ALM.

Tipos de almacenamiento compatibles con los plugins de SnapCenter para Microsoft Windows y Microsoft SQL Server

SnapCenter es compatible con una gran variedad de tipos de almacenamiento, tanto en máquinas físicas como virtuales. Antes de instalar el paquete para el host, es necesario verificar que el tipo de almacenamiento sea compatible.

Windows Server es compatible con el aprovisionamiento y la protección de datos de SnapCenter. Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Máquina	Tipo de almacenamiento	Aprovisionamiento con	Notas de soporte
Servidor físico	LUN conectados a FC	Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell	

Máquina	Tipo de almacenamiento	Aprovisionamiento con	Notas de soporte
Servidor físico	LUN conectados a iSCSI	Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell	
Servidor físico	Recursos compartidos de SMB3 (CIFS) que residen en una máquina virtual de almacenamiento (SVM)	Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell	Compatibilidad solo para aprovisionamiento. No puede utilizar SnapCenter para realizar backup de datos o recursos compartidos mediante el protocolo SMB.
Máquina virtual de VMware	LUN de RDM conectados por un adaptador de bus de host FC o iSCSI	Cmdlets de PowerShell	
Máquina virtual de VMware	LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI	Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell	
Máquina virtual de VMware	Sistemas de archivos de máquina virtual (VMFS) o almacenes de datos NFS	VSphere de VMware	
Máquina virtual de VMware	Un sistema invitado conectado a recursos compartidos de SMB3 que residen en una SVM	Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell	Compatibilidad solo para aprovisionamiento. No puede utilizar SnapCenter para realizar backup de datos o recursos compartidos mediante el protocolo SMB.

Máquina	Tipo de almacenamiento	Aprovisionamiento con	Notas de soporte
Máquina virtual Hyper-V.	LUN de Virtual FC (VFC) conectados por un switch Fibre Channel virtual	Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell	Para aprovisionar LUN de Virtual FC (VFC) conectados por un switch Fibre Channel virtual se debe usar Hyper-V Manager. No se admiten los discos de acceso directo Hyper-V ni el backup de bases de datos en VHD(x) con aprovisionamiento en almacenamiento de NetApp.
Máquina virtual Hyper-V.	LUN iSCSI conectados directamente al sistema invitado por el iniciador de iSCSI	Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell	No se admiten los discos de acceso directo Hyper-V ni el backup de bases de datos en VHD(x) con aprovisionamiento en almacenamiento de NetApp.

Máquina	Tipo de almacenamiento	Aprovisionamiento con	Notas de soporte
Máquina virtual Hyper-V.	Un sistema invitado conectado a recursos compartidos de SMB3 que residen en una SVM	Interfaz gráfica de usuario de SnapCenter o cmdlets de PowerShell	Compatibilidad solo para aprovisionamiento. No puede utilizar SnapCenter para realizar backup de datos o recursos compartidos mediante el protocolo SMB. No se admiten los discos de acceso directo Hyper-V ni el backup de bases de datos en VHD(x) con aprovisionamiento en almacenamiento de NetApp.

Recomendaciones sobre distribución de almacenamiento para el plugin de SnapCenter para Microsoft SQL Server

Una buena distribución de almacenamiento permite que SnapCenter Server realice backups de bases de datos para que pueda cumplir sus objetivos de recuperación. Se deben tener en cuenta diferentes factores al definir la distribución de almacenamiento, como el tamaño de la base de datos, la tasa de cambio de la base de datos y la frecuencia con la que se realizan backups.

Las siguientes secciones definen las recomendaciones y restricciones de distribución de almacenamiento para LUN y discos de máquina virtual (VMDK) con el plugin de SnapCenter para Microsoft SQL Server instalado en el entorno.

En este caso, los LUN pueden incluir discos VMware RDM y LUN iSCSI de conexión directa asignados al invitado de the guest.

Requisitos de LUN y VMDK

Opcionalmente, puede utilizar LUN o VMDK específicos para optimizar el rendimiento y la gestión de las siguientes bases de datos:

- Bases de datos maestra y de sistema modelo
- Tempdb

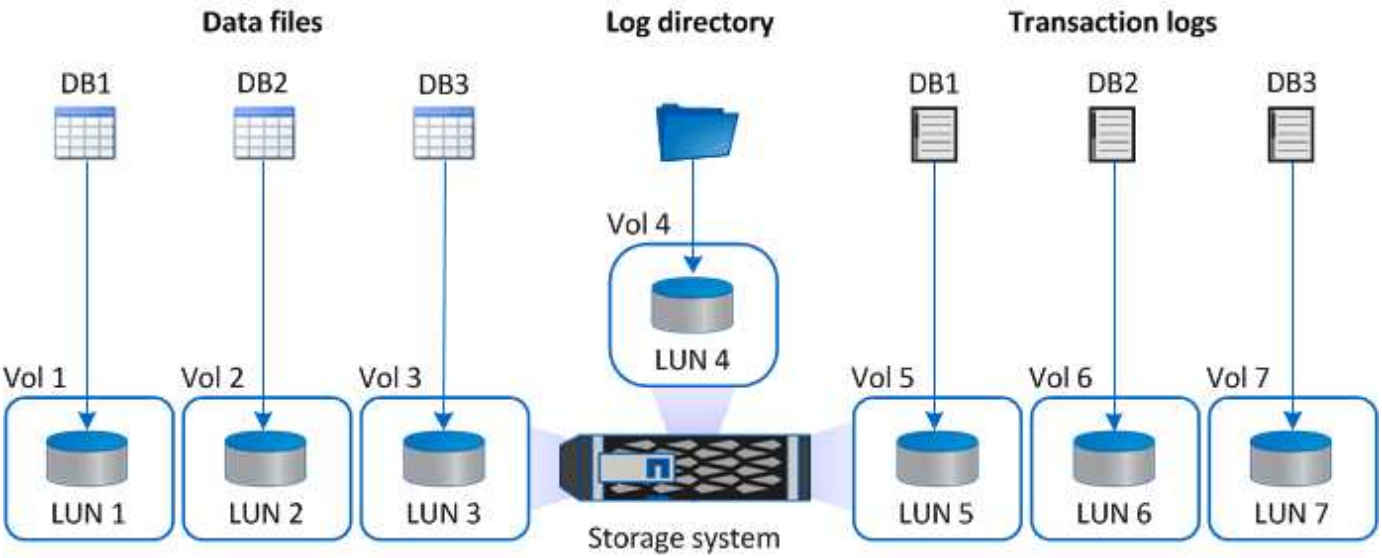
- Archivos de bases de datos del usuario (.mdf y .ndf)
- Archivos de registro de transacciones de bases de datos (.ldf)
- Directorio de registro

Para restaurar grandes bases de datos, la práctica recomendada es utilizar LUN o VMDK específicos El tiempo que se necesita para restaurar un LUN o un VMDK completos es inferior al que se requiere para restaurar los archivos individuales almacenados en el LUN o el VMDK

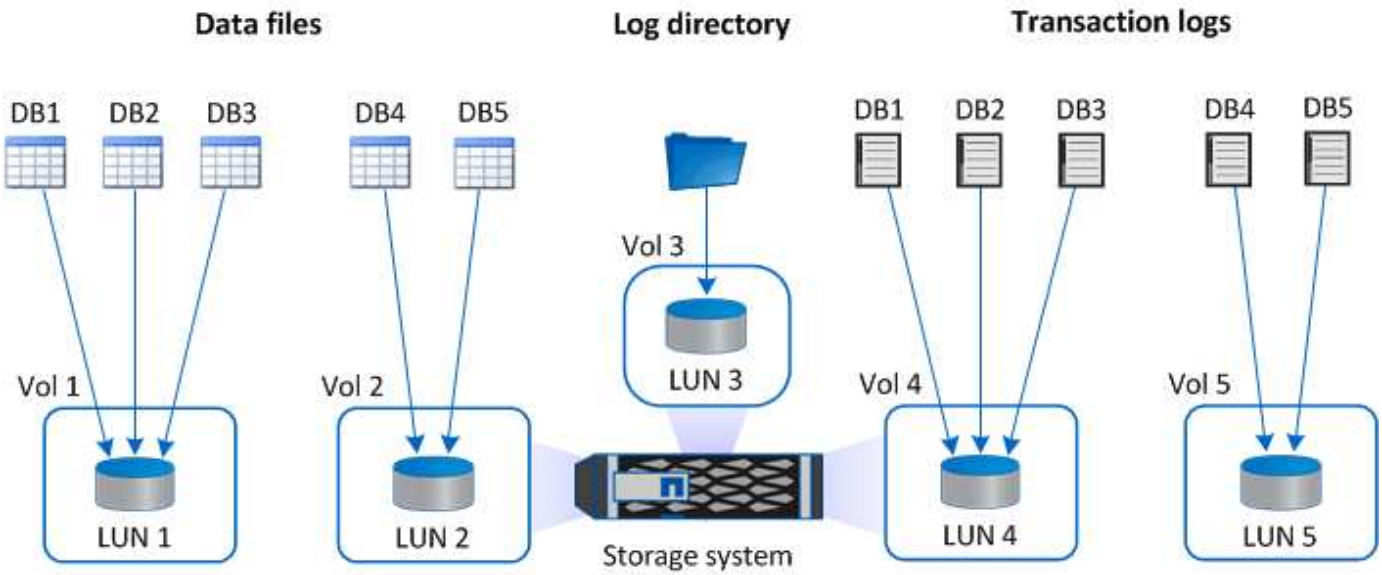
Para el directorio de registro, deber crear un LUN o un VMDK por separado para que haya espacio libre suficiente en los discos de archivos de registro o archivos de datos

Ejemplos de distribución de LUN y VMDK

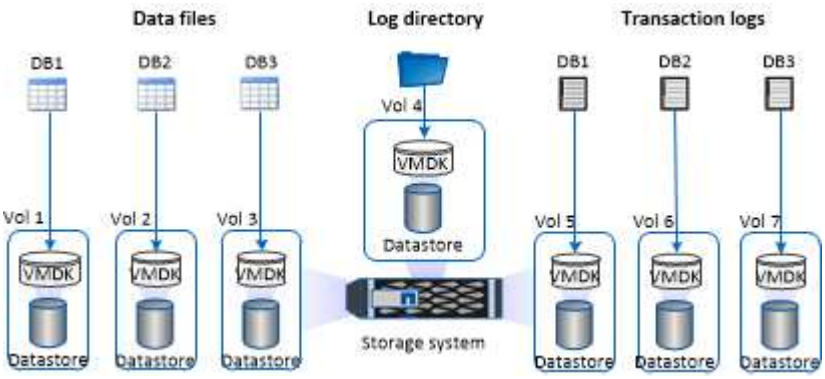
El gráfico siguiente muestra cómo puede configurar la distribución almacenamiento para bases de datos grandes en LUN:



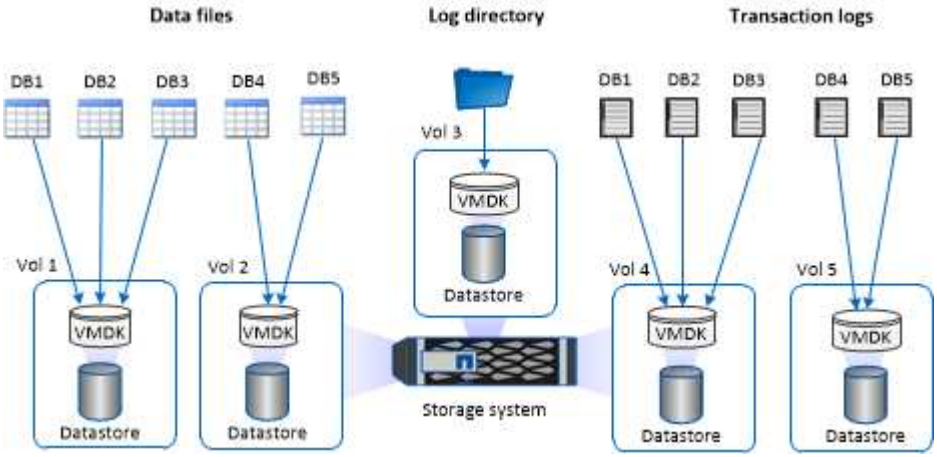
El gráfico siguiente muestra cómo puede configurar la distribución de almacenamiento para bases de datos medianas o pequeñas en LUN:



El gráfico siguiente muestra cómo puede configurar la distribución almacenamiento para bases de datos grandes en VMDK:



El gráfico siguiente muestra cómo puede configurar la distribución de almacenamiento para bases de datos medianas o pequeñas en VMDK:



Privilegios mínimos de ONTAP requeridos para el plugin de SQL

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
  - eliminación de lun
  - igroup de lun añadido
  - crear lun igroup
  - lun igroup eliminado
  - 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
- 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
- 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
- interfaz de red
- se muestra la interfaz de red
- vserver
- MetroCluster show

Preparar los sistemas de almacenamiento para la replicación de SnapMirror y SnapVault para el plugin para SQL Server

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 actualizaciones en SnapMirror y SnapVault después de completar la operación de copia 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".

SnapCenter no admite replicación **SYNC_mirror**.

Estrategia de backup para recursos de SQL Server

Defina una estrategia de backup para recursos de SQL Server

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 las bases de datos. La estrategia de backup queda determinada principalmente por el SLA, el RTO y el RPO.

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 objetivo de punto de recuperación contribuyen a la estrategia de backup.

Tipo de backups admitido

El backup de bases de datos SQL Server del sistema y del usuario con SnapCenter requiere seleccionar el tipo de recurso, como bases de datos, instancias de SQL Server y grupos de disponibilidad (AG). Se aprovecha la tecnología de copia de Snapshot para crear copias en línea y de solo lectura de los volúmenes donde residen los recursos.

Puede seleccionar la opción de solo copia para especificar que SQL Server no trunque los registros de transacciones. Debe utilizar esta opción cuando gestiona SQL Server con otras aplicaciones de backup. Mantener intactos los registros de transacciones permite que cualquier aplicación de backup restaure las bases de datos del sistema. Los backups de solo copia son independientes de la secuencia de backups programados, y no afectan los procedimientos de backup y restauración de la base de datos.

Tipo de backup	Descripción	Opción de solo copia con el tipo de backup
Backup completo y backup de registros	Realiza un backup de la base de datos del sistema y acorta los registros de transacciones. La instancia de SQL Server acorta los registros de transacciones eliminando las entradas que ya están confirmadas en la base de datos. Después de finalizar el backup completo, esta opción crea un registro de transacciones que captura la información de la transacción. En términos generales, debe elegir esta opción. Sin embargo, si el tiempo de backup es corto, puede optar por no ejecutar un backup del registro de transacciones junto con el backup completo. No es posible crear un backup de registros para las bases de datos maestra y msdb. Sin embargo, puede crear backups de registros para la base de datos modelo del sistema.	Realiza un backup de los archivos de la base de datos del sistema y los registros de transacciones sin acortarlos. Un backup de solo copia actúa como un backup de la base diferencial o un backup diferencial, y no afecta la base diferencial. Restaurar un backup completo de solo copia es igual que restaurar cualquier otro backup completo.
Backup completo de la base de datos	Realiza un backup de los archivos de la base de datos del sistema. Es posible crear un backup completo de la base de datos para las bases de datos maestra, modelo y msdb del sistema.	Realiza un backup de los archivos de la base de datos del sistema.
Backup de registros de transacciones	Realiza un backup de los registros de transacciones acortados, copiando solo las transacciones que se confirmaron desde el backup más reciente del registro de transacciones. Si programa backups del registro de transacciones frecuentes junto con backups completos de la base de datos, puede elegir puntos de recuperación granulares.	Realiza un backup de los registros de transacciones sin acortarlos. Este tipo de backup no afecta la secuencia de los backups de registros regulares. Los backups de registros solo de copia son útiles para realizar operaciones de restauración en línea

Programaciones de backups para el plugin para SQL Server

La frecuencia de los backups (tipo de programación) se especifica en las políticas; la programación de los backups se especifica en la configuración del grupo de recursos. El factor más crítico para determinar la frecuencia o la programación de los backups es la tasa de cambio del recurso y la importancia de los datos. 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 son la importancia del recurso para la organización, el SLA y el RPO.

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 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 SLA y el RPO contribuyen a la estrategia de protección de datos.

Incluso en el caso de un recurso utilizado intensivamente, no existe el requisito de ejecutar un backup completo más de una o dos veces al día. Por ejemplo, es posible que sea suficiente realizar backups regulares de registros de transacciones para garantizar los backups necesarios Cuanto mayor sea la frecuencia con que realiza backups de las bases de datos, menos registros de transacciones deberá utilizar SnapCenter en el momento de la restauración, lo que puede dar como resultado operaciones más rápidas.

Las programaciones de backup están compuestas por dos partes:

- Frecuencia de backup

  La frecuencia de los backups (cada cuánto tiempo deben realizarse los backups), denominada *schedule type* para algunos plugins, forma parte de la configuración de una política. Se puede seleccionar una frecuencia de backups por hora, por día, por semana o por mes para la política. Si no selecciona ninguna de estas frecuencias, la política creada es de sólo bajo demanda. Puede acceder a las directivas haciendo clic en **Configuración** > **Directivas**.

- Programaciones de backup

  Las programaciones de los backups (el momento exacto en que se realizan los backups) forman parte de una configuración de grupo de recursos. Por ejemplo, si tiene un grupo de recursos que posee una política configurada para backups semanales, quizás sea conveniente configurar la programación para que realice backups todos los jueves a las 00:10. Puede acceder a los programas de grupos de recursos haciendo clic en **Recursos** > **grupos de recursos**.

Cantidad de tareas de backup necesarias para bases de datos

Algunos factores que determinan la cantidad de tareas de backup que se necesitan son el tamaño de la base de datos, la cantidad de volúmenes que se usan, la tasa de cambio de la base de datos y el acuerdo de nivel de servicio.

Para los backups de bases de datos, la cantidad de trabajos de backup que se selecciona depende de la cantidad de volúmenes en los que se colocaron las bases de datos. Por ejemplo, si se colocó un grupo de bases de datos pequeñas en un volumen y una base de datos grande en otro volumen, puede ser necesario crear un trabajo de backup para las bases de datos pequeñas y otro trabajo para la base de datos grande.

Convenciones de nomenclatura de backups para el plugin para SQL Server

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

La copia 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, puede especificar el formato de nombre de la copia Snapshot mientras protege los recursos o grupos de recursos seleccionando **usar formato de nombre personalizado para copia Snapshot**. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade el sufijo de fecha y hora al nombre de la copia de Snapshot.

Opciones de retención de backups para el plugin para SQL Server

Es posible elegir la cantidad de días durante los cuales se retendrán las copias de backup o especificar la cantidad de copias de backup que se desean retener, con un máximo de 255 copias en ONTAP. Por ejemplo, una organización puede necesitar retener 10 días de copias de backup o 130 copias de backup.

Al crear una política, es posible especificar las opciones de retención para cada tipo y programación de backup.

Si se configura la replicación de SnapMirror, la política de retención se refleja en el volumen de destino.

SnapCenter elimina los backups previos que tengan etiquetas de retención que coincidan con el tipo de programación. Si se modifica el tipo de programación para el recurso o el grupo de recursos, los backups con la etiqueta del tipo de programación anterior podrían conservarse en el sistema.

Para la retención a largo plazo de copias de backup, es conveniente usar el backup de SnapVault.

Cuánto tiempo se retienen los backups de registros de transacciones en el sistema de almacenamiento de origen

El plugin de SnapCenter para Microsoft SQL Server necesita backups de registros de

transacciones para ejecutar operaciones de restauración de último minuto, que restauran la base de datos a un momento entre dos backups completos.

Por ejemplo, si el plugin para SQL Server hizo un backup completo a las 8:00 y otro backup completo a las 8:00 p. m., se podía utilizar el último backup de registros de transacciones para restaurar la base de datos a cualquier momento entre las 5:00 y las 5:00 Si no se cuenta con registros de transacciones, el plugin para SQL Server solamente puede ejecutar operaciones de restauración a un momento específico, que restaura una base de datos al momento en que el plugin para SQL Server finalizó un backup completo.

En general, se requieren operaciones de restauración de último minuto únicamente durante un día o dos. De forma predeterminada, SnapCenter conserva un mínimo de dos días.

Varias bases de datos en el mismo volumen

Es posible colocar todas las bases de datos en el mismo volumen, ya que la política de backup incluye una opción para configurar la cantidad máxima de bases de datos por backup (el valor predeterminado es 100).

Por ejemplo, si hay 200 bases de datos en el mismo volumen, se crean dos copias de Snapshot con 100 bases de datos en cada copia.

Verificación de copias de backup con un volumen de almacenamiento primario o secundario para el plugin para SQL Server

Es posible verificar las copias de backups en el volumen de almacenamiento principal o en el volumen de almacenamiento secundario de SnapMirror y SnapVault. La verificación con un volumen de almacenamiento secundario reduce la carga para el volumen de almacenamiento principal.

Cuando se verifica un backup que se encuentra en el volumen de almacenamiento primario o secundario, todas las copias de Snapshot primarias y secundarias se marcan como verificadas.

Se necesita una licencia de SnapRestore para verificar copias de backup en un volumen de almacenamiento secundario de SnapMirror o SnapVault.

Cuándo programar tareas de verificación

Si bien SnapCenter puede verificar los backups de inmediato después de crearlos, esta tarea puede aumentar significativamente el tiempo necesario para finalizar la tarea de backup y consume muchos recursos. Por lo tanto, casi siempre es conveniente programar la verificación en una tarea independiente más tarde. Por ejemplo, si se realiza el backup de una base de datos a las 5:00 todos los días, se puede programar la verificación una hora después, a las 6:00

Por el mismo motivo, generalmente no es necesario ejecutar una verificación de backup cada vez que se realiza un backup. Ejecutar la verificación regularmente aunque con un intervalo menos frecuente suele ser suficiente para garantizar la integridad del backup. Una misma tarea de verificación puede verificar varios backups a la vez.

Estrategia de restauración para SQL Server

Defina una estrategia de restauración para SQL Server

Definir una estrategia de restauración para SQL Server permite restaurar correctamente la base de datos.

Orígenes y destinos para una operación de restauración

Es posible restaurar una base de datos de SQL Server desde una copia de backup en el almacenamiento primario o secundario. También es posible restaurar la base de datos a diferentes destinos además de su ubicación original, para poder elegir el destino que cumpla determinados requisitos.

Orígenes para una operación de restauración

Es posible restaurar bases de datos desde almacenamiento primario o secundario.

Destinos para una operación de restauración

Es posible restaurar bases de datos a varios destinos:

Destino	Descripción
La ubicación original	De forma predeterminada, SnapCenter restaura la base de datos a la misma ubicación y en la misma instancia de SQL Server.
Otra ubicación	Es posible restaurar la base de datos a otra ubicación en cualquier instancia de SQL Server dentro del mismo host.
Ubicación original u otra ubicación con otro nombre de la base de datos	Es posible restaurar la base de datos con otro nombre a cualquier instancia de SQL Server en el mismo host donde se creó el backup.

No se admite la restauración en un host alternativo entre servidores ESX para bases de datos de SQL en VMDK (NFS y almacenes de datos de VMFS).

Modelos de recuperación de SQL Server admitidos por SnapCenter

De forma predeterminada, se asignan modelos de recuperación específicos a cada tipo de base de datos. El administrador de la base de datos de SQL Server puede reasignar cada base de datos a otro modelo de recuperación.

SnapCenter admite tres tipos de modelos de recuperación de SQL Server:

- Modelo de recuperación simple

  Cuando utiliza el modelo de recuperación simple, no puede realizar un backup de los registros de

transacciones.

- Modelo de recuperación completa

  Cuando se utiliza el modelo de recuperación completa, es posible restaurar una base de datos a su estado anterior desde el punto de error.

- Modelo de recuperación de registro masivo

  Cuando se utiliza el modelo de recuperación de registro masivo, debe volver a ejecutarse manualmente la operación de registro masivo. Debe realizar la operación de registro masivo si antes de la restauración no se ha realizado un backup del registro de transacciones que contiene el registro de confirmación de la operación. Si la operación de registro masivo inserta 10 millones de filas en una base de datos, y la base de datos genera errores antes de someterse a un backup, la base de datos restaurada no incluye las filas que se insertaron en la operación de registro masivo.

Tipos de operaciones de restauración

Es posible usar SnapCenter para ejecutar diferentes tipos de operaciones de restauración de los recursos de SQL Server.

- Restauración de último minuto
- Restauración a un momento específico

Es posible hacer una restauración de último minuto o a un momento específico previo en las siguientes situaciones:

- Restauración desde un almacenamiento secundario de SnapMirror o SnapVault
- Restauración en una ruta (ubicación) alternativa

SnapCenter no es compatible con SnapRestore basado en volúmenes.

Restauración de último minuto

En una operación de restauración de último minuto (seleccionada de forma predeterminada), se recuperan las bases de datos hasta el punto de error. SnapCenter usa la siguiente secuencia para este proceso:

1. Realiza el backup del último registro de transacciones activo antes de restaurar la base de datos.
2. Restaura las bases de datos desde el backup completo de la base de datos que se seleccione.
3. Aplica todos los registros de transacciones que no estaban comprometidos con las bases de datos (incluidos los registros de transacciones de los backups desde el momento en que se creó el backup hasta el punto más reciente).

   Se mueven los registros de transacciones y se aplican a las bases de datos seleccionadas.

Una operación de restauración de último minuto requiere un conjunto de registros de transacciones contiguos.

Debido a que SnapCenter no puede restaurar registros de transacciones de bases de datos de SQL Server a partir de archivos de backup de envío de registros (el envío de registros permite enviar automáticamente backups de registros de transacciones desde una base de datos principal en una instancia de servidor principal a una o varias bases de datos secundarias en instancias de servidor secundarias independientes), no se puede ejecutar una operación de restauración de último minuto desde los backups de registros de

transacciones. Por este motivo, es conveniente usar SnapCenter para realizar el backup de los archivos de registros de transacciones de bases de datos de SQL Server.

Si no se necesita la funcionalidad de restauración de último minuto para todos los backups, es posible configurar la retención de backup de los registros de transacciones del sistema mediante las políticas de backup.

Ejemplo de una operación de restauración de último minuto

Supongamos que se ejecuta un backup de SQL Server todos los días al mediodía, y un miércoles a las 4:00 es necesario hacer una restauración desde un backup. Por algún motivo, el backup del miércoles al mediodía no pasó la verificación, por lo que se decide restaurar desde el backup del martes al mediodía. Después de eso, si se restaura el backup, todos los registros de transacciones se mueven hacia adelante y se aplican a las bases de datos restauradas, a partir de las que no se confirmaron al crear el backup del martes y continuar con el último registro de transacciones escrito el miércoles a las 4:00 (si se realizó el backup de los registros de transacciones).

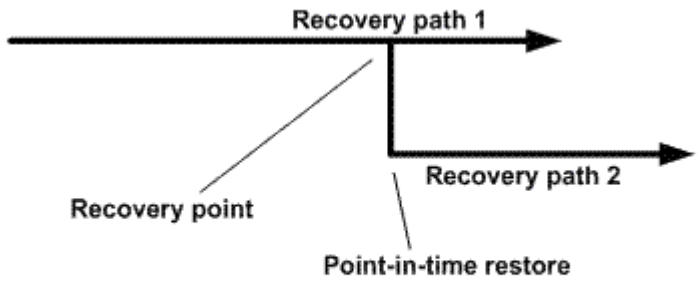
Restauración a un momento específico

En una operación de restauración a un momento específico, las bases de datos se restauran únicamente a un punto específico. Esta operación se ejecuta en las siguientes situaciones:

- La base de datos se restaura a un punto específico en un registro de transacciones incluido en un backup.
- Se restaura la base de datos, y solo se aplica un subconjunto de los registros de transacciones del backup.

Cuando se restaura una base de datos a un momento específico, se crea una nueva ruta de recuperación.

En la siguiente imagen, se ilustran los problemas cuando se ejecuta una operación de restauración a un momento específico:



En la imagen, la ruta de recuperación 1 consta de un backup completo seguido por varios backups de registros de transacciones. Se restaura la base de datos a un momento específico. Se crean nuevos backups de registros de transacciones después de la operación de restauración a un momento específico, lo cual da lugar a la ruta de recuperación 2. Se crean nuevos backups de registros de transacciones sin crear un backup completo nuevo. Debido a que hay datos dañados u otros problemas, no es posible restaurar la base de datos actual hasta que se cree un nuevo backup completo. Tampoco es posible aplicar los registros de transacciones creados en la ruta de recuperación 2 al backup completo que pertenece a la ruta de recuperación 1.

Si se aplican backups de registros de transacciones, también es posible especificar una fecha y hora particulares en las que se detendrá la aplicación de las transacciones del backup. Para esto, se especifica una fecha y hora dentro del intervalo disponible, y SnapCenter quita las transacciones que no estuvieran comprometidas antes de ese momento específico. Este método permite restaurar bases de datos a un momento específico antes de que se dañara, o recuperar contenido tras la eliminación accidental de una base de datos o una tabla.

Ejemplo de una operación de restauración a un momento específico

Supongamos que se realiza un backup completo de las bases de datos a la medianoche y un backup de los registros de transacciones cada hora. La base de datos falla a las 9:45, pero igual se realiza el backup de los registros de transacciones de la base de datos con errores. Es posible elegir entre las siguientes situaciones de restauración a un momento específico:

- Restaurar el backup completo de las bases de datos de la medianoche y aceptar la pérdida de los cambios hechos posteriormente. (Opción: None).
- Restaurar el backup completo de las bases de datos y aplicar todos los backups de registros de transacciones hasta las 9:45 (Opción: Log until).
- Restaurar el backup completo de las bases de datos y aplicar los backups de registros de transacciones especificando un intervalo de transacciones que se restaurarán del último conjunto de backups de registros de transacciones. (Opción: By specific time).

En este caso, es necesario calcular la fecha y hora en que se informó el error. Las transacciones que no estuvieran comprometidas antes de la fecha y hora especificada se quitan.

Defina una estrategia de clonación para SQL Server

Definir una estrategia de clonado permite clonar correctamente la base de datos.

1. Revisar las limitaciones de las operaciones de clonado.
2. Decidir el tipo de clon que se necesita.

Limitaciones de las operaciones de clonado

Antes de clonar las bases de datos, es necesario tener en cuenta las limitaciones de las operaciones de clonado.

- Si utiliza cualquier versión de Oracle de 11.2.0.4 a 12,1.0,1, la operación de clonado estará en estado colgado al ejecutar el comando *renamedg*. Puede aplicar el parche de Oracle 19544733 para solucionar este problema.
- Clonado de bases de datos de un LUN conectado directamente a un host (por ejemplo, mediante Iniciador iSCSI de Microsoft en un host de Windows) en un VMDK o un LUN de RDM en el mismo No se admite el host de Windows ni otro host de Windows, ni viceversa.
- El directorio raíz del punto de montaje del volumen no puede ser un directorio compartido.
- Si se mueve un LUN que contiene un clon de un volumen nuevo, no es posible eliminar el clon.

Tipos de operaciones de clonado

Es posible utilizar SnapCenter para clonar un backup de una base de datos de SQL Server o una base de datos de producción.

- Clonación de un backup de base de datos

  La base de datos clonada puede actuar como base de referencia para las aplicaciones y ayudar a aislar errores de aplicación que se producen en el entorno de producción. La base de datos clonada también puede incluir se utiliza para la recuperación de errores de la base de datos de software.

- Ciclo de vida de clon

  Es posible utilizar SnapCenter para programar trabajos de clonado recurrentes que se producirán durante la producción la base de datos no está ocupada.

Inicio rápido de instalar el plugin de SnapCenter para Microsoft SQL Server

Prepare la instalación del servidor de SnapCenter y del plugin

Proporciona un conjunto condensado de instrucciones de preparación para instalar SnapCenter Server y el plugin de SnapCenter para Microsoft SQL Server.

Requisitos de dominio y grupo de trabajo

SnapCenter Server se puede instalar en sistemas que estén en un dominio o en un grupo de trabajo.

Si utiliza un dominio de Active Directory, debe utilizar un usuario de dominio con derechos de administrador local. El usuario de dominio debe ser miembro del grupo de administrador local en el host de Windows.

Si utiliza grupos de trabajo, debe utilizar una cuenta local con derechos de administrador locales.

Requisitos de licencia

El tipo de licencia que instale dependerá del entorno.

Licencia	Donde se la requiere
Basado en controladora estándar de SnapCenter	Necesario para las controladoras de almacenamiento FAS o AFF La licencia estándar de SnapCenter es una licencia basada en la controladora y se incluye como parte del paquete Premium. Si tiene la licencia de conjunto de SnapManager, también obtendrá el derecho de licencia estándar de SnapCenter. Si desea instalar SnapCenter a modo de prueba con almacenamiento FAS o AFF, puede obtener una licencia de evaluación Premium Bundle poniéndose en contacto con el representante de ventas.
SnapCenter basada en capacidad estándar	Necesario con ONTAP Select y Cloud Volumes ONTAP Si es cliente de Cloud Volumes ONTAP o ONTAP Select, necesita adquirir una licencia basada en capacidad por TB en función de los datos gestionados por SnapCenter. De forma predeterminada, SnapCenter envía una licencia de prueba integrada basada en capacidad estándar de SnapCenter de 90 días y 100 TB. Si desea obtener más detalles, póngase en contacto con el representante de ventas.

Licencia	Donde se la requiere
SnapMirror o SnapVault	ONTAP Se requieren licencias de SnapMirror o SnapVault si la replicación se habilita en SnapCenter.
Licencias adicionales (opcional)	Consulte "Licencias SnapCenter".
Licencias estándar de SnapCenter (opcional)	Destinos secundarios Se recomienda, pero no es obligatorio, añadir licencias estándar de SnapCenter a destinos secundarios. Si las licencias estándar de SnapCenter están deshabilitadas en destinos secundarios, no puede usar SnapCenter para realizar un backup de los recursos en el destino secundario después de realizar una operación de conmutación al nodo de respaldo. Sin embargo, se requiere una licencia de FlexClone en destinos secundarios para realizar operaciones de clonado y verificación.

Requisitos del host y puerto

Para ver los requisitos mínimos del ONTAP y el complemento de la aplicación, consulte "Herramienta de matriz de interoperabilidad".

Hosts	Requisitos mínimos
Sistema operativo (64 bits)	Consulte "Herramienta de matriz de interoperabilidad"
CPU	• Host del servidor: 4 núcleos • Host de plugin: 1 núcleo
RAM	• Host del servidor: 8 GB • Host de plugins: 1 GB
Espacio en el disco duro	Host del servidor: • 4 GB para software y registros de SnapCenter Server • 6 GB para el repositorio de SnapCenter • Cada host de plugin: 2 GB para la instalación y los registros de un plugin, esto es obligatorio solo si el plugin está instalado en un host dedicado.

Hosts	Requisitos mínimos
Bibliotecas de terceros	Requerida en el host de servidor de SnapCenter y el host de plugins: • Microsoft .NET Framework 4.7.2 o posterior • Windows Management Framework (WMF) 4.0 o posterior • PowerShell 4.0 o posterior
Exploradores	Chrome, Internet Explorer y Microsoft Edge

Tipo de puerto	Puerto predeterminado
Puerto SnapCenter	8146 (HTTPS), bidireccional, personalizable, como en la url *https://server:8146*
Puerto de comunicación SMCore de SnapCenter	8145 (HTTPS), bidireccional, personalizable
Base de datos del repositorio	3306 (HTTPS), bidireccional
Hosts de plugins de Windows	135 DE FEBRERO DE 445 (TCP) Además de los puertos 135 y 445, el intervalo de puertos dinámico especificado por Microsoft también debería estar abierto. Operaciones de instalación remota Utilice el servicio Instrumental de administración de Windows (WMI), que busca dinámicamente este intervalo de puertos. Para obtener información sobre el intervalo de puertos dinámicos admitido, consulte "Descripción general del servicio y requisitos de puertos de red para Windows".
Plugin de SnapCenter para Windows	8145 (HTTPS), bidireccional, personalizable
Puerto de comunicación del clúster de ONTAP o de SVM	443 (HTTPS), bidireccional; 80 (HTTP), bidireccional El puerto se utiliza para establecer la comunicación entre el host del servidor de SnapCenter, el host del plugin y SVM o el clúster de ONTAP.

Requisitos del plugin de SnapCenter para Microsoft SQL Server

Debe tener un usuario con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto. Si gestiona nodos de clúster, necesita un usuario con privilegios de administrador para todos los nodos del clúster.

Debe tener un usuario con permisos de administrador del sistema en SQL Server. El plugin utiliza Microsoft VDI Framework, para lo que se requiere acceso de sysadmin.

Instale SnapCenter Server para Microsoft SQL Server

Proporciona un conjunto condensado de instrucciones de instalación para instalar SnapCenter Server para Microsoft SQL Server.

Paso 1: Descargue e instale el servidor SnapCenter

1. Descargue el paquete de instalación del servidor SnapCenter desde el "Sitio de soporte de NetApp" y, a continuación, haga doble clic en el archivo exe.

   Tras iniciar la instalación, se realizan todas las comprobaciones previas y si los requisitos mínimos no son los correctos, se muestran mensajes de error o de advertencia. Puede ignorar los mensajes de advertencia y continuar con la instalación; sin embargo, los errores deben corregirse.

2. Revise los valores rellenados previamente necesarios para la instalación del servidor SnapCenter y modifíquelos si es necesario.

   No es necesario especificar la contraseña para la base de datos de repositorio del servidor MySQL. Durante la instalación del servidor SnapCenter, la contraseña se genera automáticamente.

   > El carácter especial “%” no se admite en la ruta personalizada para la instalación. Si incluye “%” en la ruta, la instalación falla.

3. Haga clic en **instalar ahora**.

Paso 2: Inicie sesión en SnapCenter

1. Inicie SnapCenter desde un acceso directo en el escritorio del host o desde la URL proporcionada por la instalación (*https://server:8146* para el puerto predeterminado 8146 donde está instalado el servidor SnapCenter).
2. Introduzca las credenciales.

   Para un formato de nombre de usuario de administrador de dominio integrado, utilice: *NetBIOS\<username>* o *<username>@<domain>* o *<DomainFQDN>\<username>*.

   Para un formato de nombre de usuario de administrador local integrado, utilice *<username>*.

3. Haga clic en **Iniciar sesión**.

Paso 3: Añada una licencia estándar basada en controladora de SnapCenter

1. Inicie sesión en la controladora con la línea de comandos de ONTAP e introduzca lo siguiente:

   ```
   system license add -license-code <license_key>
   ```

2. Compruebe la licencia:

   ```
   license show
   ```

Paso 4: Añadir una licencia basada en capacidad de SnapCenter

1. En el panel izquierdo de la GUI de SnapCenter, haga clic en **Configuración > Software** y, a continuación, en la sección Licencia, haga clic en **+**.

2. Seleccione uno de los dos métodos para obtener la licencia:
   - Introduzca sus credenciales de inicio de sesión en el sitio de soporte de NetApp para importar licencias.
   - Desplácese hasta la ubicación del archivo de licencia de NetApp y haga clic en **Open**.
3. En la página Notifications del asistente, utilice el umbral de capacidad predeterminado del 90 %.
4. Haga clic en **Finalizar**.

Paso 5: Configure las conexiones al sistema de almacenamiento

1. En el panel izquierdo, haga clic en **sistemas de almacenamiento > Nuevo**.
2. En la página Add Storage System, realice lo siguiente:
   a. Introduzca el nombre o la dirección IP del sistema de almacenamiento.
   b. Introduzca las credenciales que se utilizan para acceder al sistema de almacenamiento.
   c. Active las casillas para habilitar el sistema de gestión de eventos (EMS) y AutoSupport.
3. Haga clic en **más opciones** si desea modificar los valores predeterminados asignados a la plataforma, el protocolo, el puerto y el tiempo de espera.
4. Haga clic en **Enviar**.

Instale el plugin de SnapCenter para Microsoft SQL Server

Proporciona un conjunto condensado de instrucciones de instalación para el plugin de SnapCenter para Microsoft SQL Server.

Paso 1: Configure credenciales Run As para instalar el plugin para Microsoft SQL Server

1. En el panel izquierdo, haga clic en **Configuración > credenciales > Nuevo**.
2. Introduzca las credenciales.

   Para un formato de nombre de usuario de administrador de dominio integrado, utilice: *NetBIOS*\<*username*> o <*username*>@<*domain*> o <*DomainFQDN*>\<*username*>.

   Para un formato de nombre de usuario de administrador local integrado, utilice <*username*>.

Paso 2: Añada un host e instale el plugin para Microsoft SQL Server

1. En el panel izquierdo de la interfaz gráfica de usuario de SnapCenter, haga clic en **hosts > Managed hosts > Add**.
2. En la página hosts del asistente, realice lo que sigue:
   a. Host Type: Seleccione el tipo de host Windows.
   b. Nombre de host: Utilice el host SQL o especifique el FQDN de un host Windows dedicado.
   c. Credenciales: Seleccione el nombre de credencial válido del host que creó o cree nuevas credenciales.
3. En la sección Select Plug-ins to Install, seleccione **Microsoft SQL Server**.
4. Haga clic en **más opciones** para especificar los siguientes detalles:
   a. Puerto: Conserve el número de puerto predeterminado o especifique el número de puerto.

b. Ruta de instalación: La ruta predeterminada es *C:\Program Files\NetApp\SnapCenter*. Opcionalmente, puede personalizar la ruta.

c. Añadir todos los hosts del clúster: Seleccione esta casilla de comprobación si está usando SQL en WSFC.

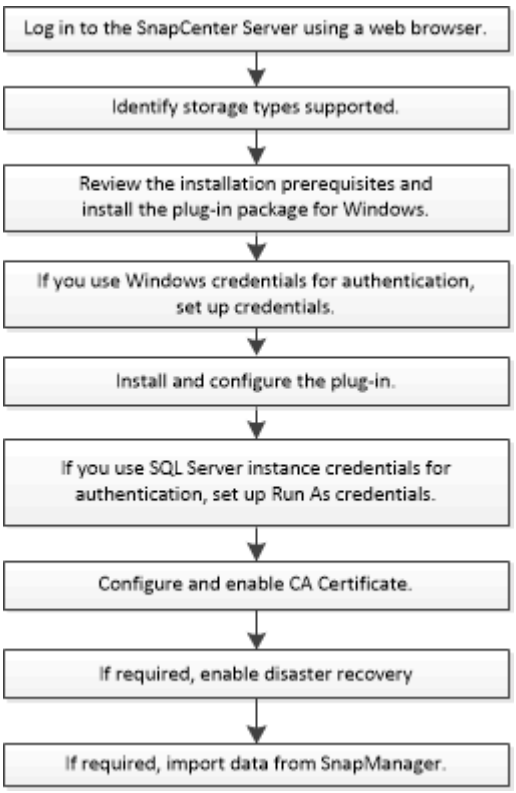
d. Skip preinstall checks: Seleccione esta casilla de comprobación si ya ha instalado los plugins manualmente o no desea validar si el host cumple los requisitos para instalar el plugin.

5. Haga clic en **Enviar**.

Preparar la instalación del plugin de SnapCenter para Microsoft SQL Server

Flujo de trabajo de instalación del plugin de SnapCenter para Microsoft SQL Server

Tendrá que instalar y configurar el plugin de SnapCenter para Microsoft SQL Server si desea proteger las bases de datos de SQL Server.



Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para Microsoft SQL Server

Antes de añadir un host e instalar los paquetes de plugins, debe satisfacer todos los requisitos.

- Si utiliza iSCSI, el servicio iSCSI debe estar en ejecución.
- Debe tener un usuario con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto.

- Si gestiona nodos de clúster en SnapCenter, debe tener un usuario con privilegios de administrador para todos los nodos del clúster.
- Debe tener un usuario con permisos de administrador del sistema en SQL Server.

  El plugin de SnapCenter para Microsoft SQL Server utiliza Microsoft VDI Framework, para lo que se requiere acceso de sysadmin.

  "Artículo de soporte de Microsoft 2926557: Las operaciones de backup y restauración de VDI de SQL Server requieren privilegios de administrador del sistema"
- 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.
- Si está instalado SnapManager para Microsoft SQL Server, debe haber detenido o deshabilitado el servicio y las programaciones.

  Si prevé importar tareas de backup o clonado a SnapCenter, no desinstale SnapManager para Microsoft SQL Server.
- El host debe poder resolverse con el nombre de dominio completo (FQDN) del servidor.

  Si el archivo hosts se modifica para que pueda resolverse y si se especifican tanto el nombre corto como el FQDN en el archivo hosts, cree una entrada en el archivo hosts SnapCenter con el siguiente formato: <ip_address> <host_fqdn> <host_name>

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

Elemento	Requisitos
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.
Paquetes de software obligatorios	• Microsoft .NET Framework 4.7.2 o posterior • Windows Management Framework (WMF) 4.0 o posterior • PowerShell 4.0 o posterior 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."

Configure credenciales para el paquete de plugins de SnapCenter para Windows

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 sistemas de archivos Windows o bases de datos.

Antes de empezar

- 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.
- Autenticación SQL en hosts Windows

  Debe configurar credenciales de SQL después de instalar plugins.

  Si va a implementar el plugin de SnapCenter para Microsoft SQL Server, debe configurar las credenciales de SQL después de instalar plugins. Configure una credencial para un usuario con permisos de administrador del sistema en SQL Server.

  El método de autenticación de SQL se verifica de acuerdo con una instancia de SQL Server. Esto significa

que debe detectarse una instancia de SQL Server en SnapCenter. Por lo tanto, antes de añadir una credencial de SQL, debe añadir un host, instalar paquetes de plugins y actualizar los recursos. Se necesita la autenticación de SQL Server para realizar operaciones como la programación o la detección de recursos.

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	Escriba un nombre para la credencial.
Nombre de usuario/Contraseña	Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación. • Administrador del dominio Especifique el administrador de dominio 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.

Para este campo…	Realice lo siguiente…
Modo de autenticación	Seleccione el modo de autenticación que desea utilizar. Si selecciona el modo de autenticación de SQL, también debe especificar la instancia de SQL Server y el host donde está ubicada esa instancia.

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.

Configure las credenciales para un recurso individual de SQL Server

Es posible configurar credenciales para realizar trabajos de protección de datos en un recurso individual de SQL Server para cada usuario. Si bien es posible configurar las credenciales de manera global, se recomienda hacerlo solo para un recurso particular.

Acerca de esta tarea

- Si utiliza credenciales de Windows para la autenticación, debe configurar las credenciales para poder instalar plugins.

  Sin embargo, si utiliza una instancia de SQL Server para la autenticación, debe añadir la credencial después de instalar los plugins.

- Si ha habilitado la autenticación SQL durante la configuración de las credenciales, la instancia o base de datos detectadas se mostrarán con un icono de candado de color 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.

- Debe asignar la credencial a un usuario de control de acceso basado en roles (RBAC) sin acceso de administrador del sistema cuando se cumplan las siguientes condiciones:
  - La credencial se asigna a una instancia de SQL.
  - La instancia o el host de SQL se asignan a un usuario de RBAC.

    El usuario debe tener privilegios tanto del grupo de recursos como de backup.

Paso 1: Agregar y configurar credenciales

1. En el panel de navegación izquierdo, selecciona **Configuración**.
2. En la página Configuración, selecciona **Credencial**.
   a. Para agregar una nueva credencial, seleccione **Nuevo**.
   b. En la página Credential, configure las credenciales:

Para este campo…	Realice lo siguiente…
Nombre de credencial	Introduzca un nombre para las credenciales.

Para este campo…	Realice lo siguiente…
Nombre de usuario	Introduzca el nombre de usuario utilizado para autenticación de SQL Server. • 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 locales si la cuenta de usuario tiene privilegios elevados o el usuario La función de control de acceso está deshabilitada en el sistema host. El formato válido para el campo **Nombre de usuario** es: *Username*
Contraseña	Introduzca la contraseña usada para autenticación.
Modo de autenticación	Seleccione el modo de autenticación SQL Server. También es posible seleccionar la autenticación de Windows si el usuario de Windows tiene privilegios de administrador del sistema en el servidor SQL.
Host	Seleccione el host.
Instancia de SQL Server	Seleccione la instancia de SQL Server.

c. Seleccione **OK** para agregar la credencial.

Paso 2: Configurar instancias

1. En el panel de navegación izquierdo, selecciona **Recursos**.
2. En la página Resources, seleccione **Instance** en la lista **View**.
   a. Seleccione y, a continuación, seleccione el nombre de host para filtrar las instancias.
   b. Seleccione para cerrar el panel de filtros.
3. En la página Instance Protect, proteja la instancia y, si es necesario, seleccione **Configure Credentials**.

   Si el usuario que ha iniciado sesión en el servidor SnapCenter no tiene acceso al complemento SnapCenter para Microsoft SQL Server, el usuario deberá configurar las credenciales.

   La opción de credencial no se aplica a las bases de datos y los grupos de disponibilidad.
4. Seleccione **Actualizar recursos**.

Configurar GMSA en Windows Server 2012 o posterior

Windows Server 2012 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 2012 o posterior.
- Debe tener un host de Windows Server 2012 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 Microsoft SQL Server

Añada hosts e instale el paquete de plugins de SnapCenter para Windows

Debe utilizar la página SnapCenter **Add Host** para añadir hosts e instalar el paquete de plugins. Los plugins se instalan automáticamente en hosts remotos.

Antes de empezar

- 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, deberá deshabilitar UAC en el host.
- Debe asegurarse de que el servicio de cola de mensajes esté en estado en ejecución.
- Si está utilizando la cuenta de servicio gestionado en grupo (GMSA), debe configurar GMSA con privilegios administrativos.

  "Configurar la cuenta de servicio administrado de grupo en Windows Server 2012 o posterior para SQL"

Acerca de esta tarea

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

Puede añadir un host e instalar los paquetes de los plugins para un host individual o para un clúster. Si está instalando los plugins en un clúster o clustering de conmutación al nodo de respaldo de Windows Server (WSFC), los plugins se instalan en todos los nodos del clúster.

Para obtener información sobre la gestión de los hosts, consulte "Gestionar hosts".

Pasos

1. En el panel de navegación izquierdo, seleccione **hosts**.
2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
3. Seleccione **Agregar**.
4. En la página hosts, haga lo siguiente:

Para este campo…	Realice lo siguiente…
Tipo de host	Seleccione Windows como tipo de host. El servidor de SnapCenter añade el host e instala el plugin para Windows si el plugin todavía no está instalado en el host. Si selecciona la opción de Microsoft SQL Server en la página Plug-ins, SnapCenter Server instala el plugin para SQL Server.
Nombre de host	Introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host. La dirección IP es compatible con hosts de dominio que no son de confianza solo si se resuelve en el FQDN. SnapCenter depende de una configuración adecuada del DNS. Por lo tanto, lo más recomendable es introducir el FQDN. Puede introducir las direcciones IP o el FQDN de uno de los siguientes: • Host independiente • WSFC Si va a añadir un host mediante SnapCenter y el host forma parte de un subdominio, debe proporcionar 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 los detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha especificado. El modo de autenticación de las credenciales se determina por el tipo de host que especifique en el asistente Add host.

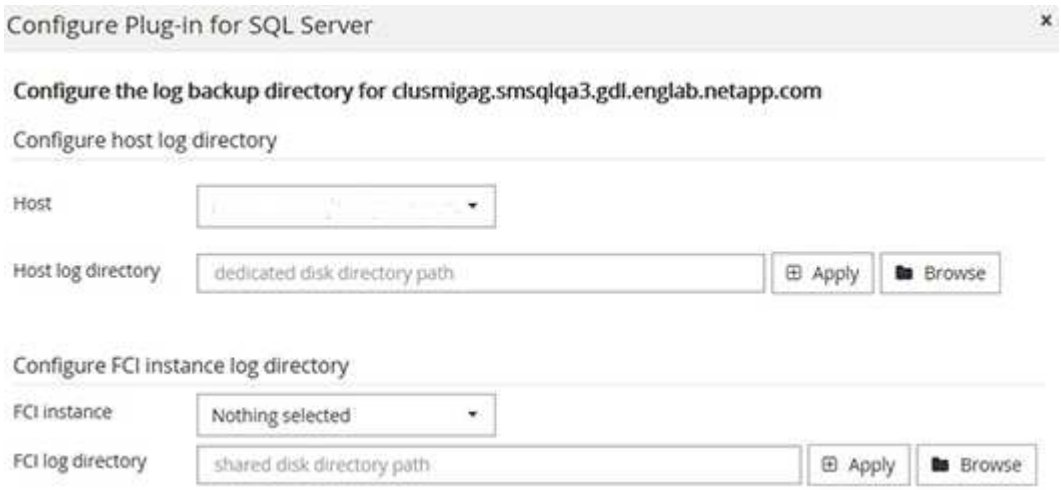
5. En la sección **Seleccione Plug-ins to Install**, seleccione los plugins que desee instalar.
6. Seleccione **más opciones**.

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.
Ruta de instalación	La ruta predeterminada es C:\Program Files\NetApp\SnapCenter. Opcionalmente, puede personalizar la ruta.
Añada todos los hosts del clúster	Seleccione esta casilla de comprobación para añadir todos los nodos del clúster en un WSFC o un Availability Group de SQL. Debe añadir todos los nodos del clúster seleccionando la casilla de comprobación correspondiente del clúster en la GUI si desea gestionar e identificar varios grupos de disponibilidad SQL disponibles en un clúster.

Para este campo…	Realice lo siguiente…
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.
Utilice Group Managed Service Account (GMSA) para ejecutar los servicios de plug-in	Seleccione esta casilla de verificación si desea utilizar la cuenta de servicio gestionado de grupo (GMSA) para ejecutar los servicios de complemento. Proporcione el nombre de GMSA con el siguiente formato: Nombre_de_dominio\accountName$. Si el host se agrega con GMSA y si el GMSA tiene privilegios de inicio de sesión y administrador de sistema, el GMSA se utilizará para conectarse a la instancia de SQL.

7. Seleccione **Enviar**.
8. Para el plugin de SQL, seleccione el host para configurar el directorio de registro.
   a. Seleccione **Configurar directorio de registro** y en la página Configurar directorio de registro de host, seleccione **Examinar** y complete los siguientes pasos:

      Tan solo se enumeran las unidades NetApp LUN como disponibles para su selección. SnapCenter realiza un backup y replica el directorio de registro del host como parte de la operación de backup.



      i. Seleccione la letra de la unidad o el punto de montaje del host donde se almacenará el registro del host.
      ii. Si es necesario, elija un subdirectorio.
      iii. Seleccione **Guardar**.
9. Seleccione **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.

10. Supervise el progreso de la instalación.

Instale el plugin de SnapCenter para Microsoft SQL Server en varios hosts remotos mediante cmdlets

Puede instalar el plugin de SnapCenter para Microsoft SQL Server 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 de SnapCenter para Microsoft SQL Server en varios hosts remotos 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 ya haya instalado los plugins manualmente y no desee 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 Microsoft SQL Server silenciosamente desde la línea de comandos

Debe instalar el plugin de SnapCenter para Microsoft SQL Server desde la interfaz de usuario de SnapCenter. Sin embargo, si no puede hacerlo por algún motivo, puede ejecutar el programa de instalación del plugin para SQL Server sin supervisión en el modo silencioso desde la línea de comandos de Windows.

Antes de empezar

- Debe eliminar la versión anterior del plugin de SnapCenter para Microsoft SQL Server antes de instalar.

  Para obtener más información, consulte "Cómo instalar un plugin de SnapCenter de forma manual y

directa desde el host del plugin".

Pasos

1. Compruebe si existe una carpeta C:\temp en el host del plugin y el usuario que ha iniciado sesión tiene acceso completo a ella.
2. Descargue el software del plugin para SQL Server desde C:\ProgramData\NetApp\SnapCenter\Package Repository.

   Es posible acceder a esta ruta desde el host en el que se ha instalado el servidor SnapCenter.
3. Copie el archivo de instalación en el host en el que desea instalar el plugin.
4. Desde el símbolo del sistema de Windows en el host local, desplácese hasta el directorio en el que guardó los archivos de instalación del plugin.
5. Instale el software del plugin para SQL Server:

   ```
   "snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"
   /log"Log_Path" BI_SNAPCENTER_PORT=Num
   SUITE_INSTALLDIR="Install_Directory_Path"
   BI_SERVICEACCOUNT=domain\\administrator BI_SERVICEPWD=password
   ISFeatureInstall=SCW,SCSQL
   ```

   Sustituya los valores del marcador de posición por sus datos

   - Debug_Log_Path es el nombre y la ubicación del archivo de registro del instalador de la suite.
   - Log_Path es la ubicación de los registros de instalación de los componentes del plugin (SCW, SCSQL y SMCore).
   - Num es el puerto en el que SnapCenter se comunica con SMCore
   - Install_Directory_Path es el directorio de instalación del paquete de plugins del host.
   - Domain\Administrator es la cuenta de servicio web del plugin de SnapCenter para Microsoft Windows.
   - La contraseña es la contraseña de la cuenta de servicio web del plugin de SnapCenter para Microsoft Windows.
     ```
     "snapcenter_windows_host_plugin.exe"/silent
     /debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\" BI_SNAPCENTER_PORT=8145
     SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"
     BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
     ISFeatureInstall=SCW,SCSQL
     ```

   Todos los parámetros que se pasan durante la instalación del plugin para SQL Server distinguen entre mayúsculas y minúsculas.
6. Supervise el programador de tareas de Windows, el archivo de registro de instalación principal C:\Installdebug.log y los archivos de instalación adicionales en C:\Temp.
7. Supervise el directorio %temp% para comprobar que los msiexe.exe instaladores están instalando el software sin errores.

   La instalación del plugin para SQL Server registra el plugin en el host y no en el servidor de SnapCenter. Es posible registrar el plugin en SnapCenter Server. Para ello, se debe añadir el host mediante la interfaz gráfica de usuario de SnapCenter o el cmdlet de PowerShell. Una vez añadido el host, el plugin se detecta automáticamente.

Supervise el estado de la instalación del plugin para SQL Server

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 Asunto (SAN) antes de adquirir 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"
```

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.

Configure la recuperación ante desastres

Recuperación ante desastres del plugin de SnapCenter para SQL Server

Cuando el plugin de SnapCenter para SQL Server está inactivo, siga los siguientes pasos para cambiar a un host de SQL diferente y recuperar los datos.

Antes de empezar

- El host secundario debe tener el mismo sistema operativo, aplicación y nombre de host que el host primario.
- Inserte el complemento SnapCenter para SQL Server en un host alternativo utilizando la página **Agregar host** o **Modificar host**. Consulte "Gestionar hosts" si quiere más información.

Pasos

1. Seleccione el host en la página **hosts** para modificar e instalar el plugin de SnapCenter para SQL Server.
2. (Opcional) reemplace los archivos de configuración del plugin de SnapCenter para SQL Server desde un backup de recuperación ante desastres (DR) a la máquina nueva.
3. Importe las programaciones de Windows y SQL desde la carpeta del plugin de SnapCenter para SQL Server desde el backup de recuperación ante desastres.

Información relacionada

Vea "API de recuperación ante desastres" el vídeo.

Recuperación ante desastres de almacenamiento (DR) para el plugin de SnapCenter para SQL Server

Para recuperar el almacenamiento del plugin de SnapCenter para SQL Server, habilitar el modo DR para almacenamiento en la página Global Settings.

Antes de empezar

- Compruebe que los plugins estén en modo de mantenimiento.
- Rompa la relación de SnapMirror/SnapVault. "Romper las relaciones de SnapMirror"
- Conecte el LUN de secundario al equipo host con la misma letra de unidad.
- Asegúrese de que todos los discos estén conectados utilizando las mismas letras de unidad que se usaron antes de la recuperación ante desastres.
- Reinicie el servicio de servidor MSSQL.
- Asegúrese de que los recursos SQL vuelven a estar en línea.

Acerca de esta tarea

No se admite la recuperación ante desastres en las configuraciones VMDK y RDM.

Pasos

1. En la página Configuración, vaya a **Ajustes** > **Ajustes globales** > **recuperación ante desastres**.
2. Seleccione **Activar recuperación ante desastres**.
3. Haga clic en **aplicar**.
4. Compruebe si el trabajo DR está activado o no haciendo clic en **Monitor** > **trabajos**.

Después de terminar

- Si se crean bases de datos nuevas después de la conmutación al nodo de respaldo, las bases de datos se pondrán en modo sin recuperación ante desastres.

  Las nuevas bases de datos seguirán funcionando como lo hicieron antes del fallo.

- Los backups nuevos que se crearon en modo de recuperación ante desastres se enumeran en SnapMirror o SnapVault (secundario) en la página Topology.

  Se muestra un icono "i" junto a los nuevos backups para indicar que estos backups se han creado durante el modo de recuperación ante desastres.

- Puede eliminar los backups del plugin de SnapCenter para SQL Server que se crearon durante la conmutación por error usando la interfaz de usuario o el siguiente cmdlet de: `Remove-SmBackup`
- Después de la conmutación por error, si desea que algunos de los recursos estén en modo no DR, use el cmdlet siguiente: `Remove-SmResourceDRMode`

  Para obtener más información, consulte el "Guía de referencia de cmdlets de SnapCenter Software".

- SnapCenter Server gestionará los recursos de almacenamiento individuales (bases de datos SQL) que están en modo DR o no DR, pero no el grupo de recursos con recursos de almacenamiento que se encuentran en modo DR o en modo no DR.

Conmutación tras recuperación del plugin de SnapCenter para almacenamiento secundario de SQL Server al almacenamiento principal

Una vez que el almacenamiento primario del plugin de SnapCenter para SQL Server vuelve a estar en línea, debe recuperar el almacenamiento principal.

Antes de empezar

- Coloque el plugin de SnapCenter para SQL Server en el modo **Mantenimiento** de la página Managed hosts.
- Desconecte el almacenamiento secundario del host y conéctelo del almacenamiento primario.
- Para volver a realizar la conmutación tras recuperación al almacenamiento principal, asegúrese de que la dirección de la relación sigue siendo la misma que antes de la conmutación por error realizando la operación de resincronización inversa.

  Para conservar los roles del almacenamiento primario y secundario después de la operación de resincronización inversa, vuelva a ejecutar la operación de resincronización inversa.

  Para obtener más información, consulte "Volver a sincronizar las relaciones de reflejos"

- Reinicie el servicio de servidor MSSQL.
- Asegúrese de que los recursos SQL vuelven a estar en línea.

> Durante la conmutación por error o la conmutación tras recuperación del plugin, el estado general del plugin no se actualiza de forma inmediata. El estado general del host y el plugin se actualiza durante la operación de actualización del host posterior.

Pasos

1. En la página Configuración, vaya a **Ajustes** > **Ajustes globales** > **recuperación ante desastres**.
2. Deseleccione **Activar recuperación ante desastres**.

3. Haga clic en **aplicar**.
4. Compruebe si el trabajo DR está activado o no haciendo clic en **Monitor** > **trabajos**.

Después de terminar

Puede eliminar los backups del plugin de SnapCenter para SQL Server que se crearon durante la conmutación por error usando la interfaz de usuario o el siguiente cmdlet de: `Remove-SmDRFailoverBackups`

Instale el plugin de SnapCenter para VMware vSphere

Si la base de datos está almacenada en máquinas virtuales (VM) o si desea proteger máquinas virtuales y almacenes de datos, debe implementar el dispositivo virtual del plugin de SnapCenter para VMware vSphere.

Para obtener información sobre la implementación, consulte "Visión General de la implementación".

Implemente el certificado de CA

Para configurar el certificado de CA con el plugin de SnapCenter para VMware vSphere, consulte "Crear o importar certificado SSL".

Configure el archivo CRL

El plugin de SnapCenter para VMware vSphere busca los archivos CRL en un directorio preconfigurado. El directorio predeterminado de los archivos CRL del plugin SnapCenter para VMware vSphere es */opt/netapp/config/crl*.

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

Prepárese para la protección de datos

Requisitos previos para utilizar el plugin de SnapCenter para Microsoft SQL Server

Antes de empezar a utilizar el plugin para SQL Server, el administrador de SnapCenter debe instalar y configurar SnapCenter Server y realizar tareas de requisitos previos.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en SnapCenter.
- Configure el entorno de SnapCenter. Para ello, añada o asigne conexiones de sistema de almacenamiento, y cree credenciales.

  SnapCenter no admite varias SVM con el mismo nombre en clústeres diferentes. Cada SVM compatible con SnapCenter debe tener un nombre exclusivo.

- Añada hosts, instale los plugins, detecte (actualice) los recursos y configure los plugins.
- Mueva una base de datos de Microsoft SQL Server existente desde un disco local hacia un LUN de NetApp o viceversa ejecutando Invoke-SmConfigureResources.

Para obtener información sobre cómo ejecutar el cmdlet, consulte "Guía de referencia de cmdlets de SnapCenter Software"

- Si va a utilizar SnapCenter Server para proteger las bases de datos de SQL que residen en LUN o VMDK de VMware RDM, debe implementar el plugin de SnapCenter para VMware vSphere y registrar el plugin con SnapCenter. La documentación del plugin de SnapCenter para VMware vSphere tiene más información.

  "Documentación del plugin de SnapCenter para VMware vSphere"

- Ejecutar el aprovisionamiento de almacenamiento en el host mediante el plugin de SnapCenter para Microsoft Windows.
- Configure las relaciones de SnapMirror y SnapVault si quiere realizar una replicación de backup.

Para ver más detalles, consulte la información de SnapCenter.

Para los usuarios de SnapCenter 4.1.1, la documentación del plugin de SnapCenter para VMware vSphere 4.1.1 tiene información sobre la protección de las bases de datos y los sistemas de archivos virtualizados. Para los usuarios de SnapCenter 4.2.x, la documentación de NetApp Data Broker 1.0 y 1.0.1 ofrece información sobre la protección de bases de datos y sistemas de archivos virtualizados mediante el plugin de SnapCenter para VMware vSphere que proporciona el dispositivo virtual de agente de datos de NetApp basado en Linux (formato de dispositivo virtual abierto). Para los usuarios de SnapCenter 4.3.x, la documentación del plugin de SnapCenter para VMware vSphere 4.3 tiene información sobre la protección de bases de datos y sistemas de archivos virtualizados mediante el dispositivo virtual del plugin de SnapCenter para VMware vSphere basado en Linux (formato de dispositivo virtual abierto).

"Documentación del plugin de SnapCenter para VMware vSphere"

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

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 son, por lo general, bases de datos, instancias de bases de datos o grupos de disponibilidad de Microsoft SQL Server que se incluyen en backups o clones con SnapCenter.
- Un grupo de recursos de SnapCenter es una agrupacion de recursos en un host o un clúster.

  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.

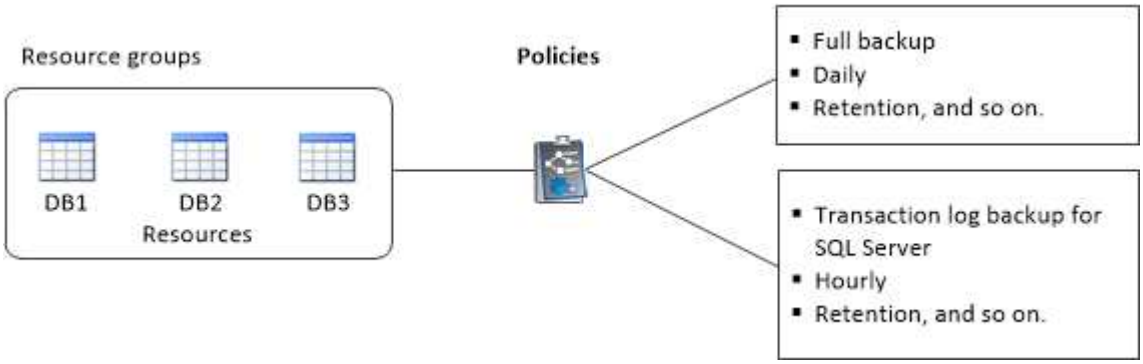
- Las políticas especifican la frecuencia de backup, la retención de copias, la replicación, los scripts y otras características de las operaciones de protección de datos.

  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.

Piense en un grupo de recursos como definir *qué* desea proteger y cuándo desea protegerlo en términos de

día y hora. Piense en una directiva como definir *how* desea protegerla. Cuando se realiza un backup de todas las bases de datos o todos los sistemas de archivos de un host, por ejemplo, puede crearse un grupo de recursos que incluya todas las bases de datos o todos los sistemas de archivos del host. Luego, se pueden vincular dos políticas al grupo de recursos: Una diaria y una horaria. Cuando se crea el grupo de recursos y se vinculan las políticas, es posible configurar el grupo de recursos para que se ejecute un backup completo todos los días, y agregar una programación que ejecute un backup del registro por hora.

En la siguiente imagen, se muestra la relación entre los recursos, los grupos de recursos y las políticas para las bases de datos:



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

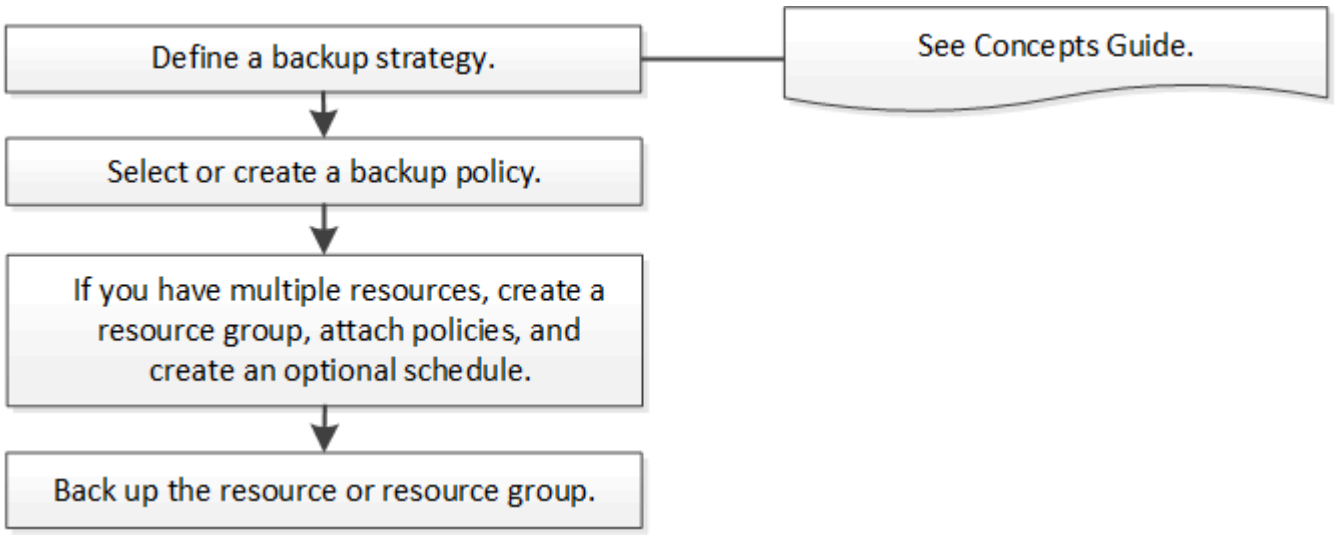
Flujo de trabajo de backup

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

Con las copias de Snapshot, se realiza un backup de todas las bases de datos que residen en un único volumen de forma simultánea. 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 copias de Snapshot 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 copia de Snapshot en la política de backups.

Cuando SnapCenter crea una copia de Snapshot, se captura todo el volumen del sistema de almacenamiento en la copia de 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 copia de 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 se encuentra en un almacenamiento de terceros, `Not available for backup` Aparece 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 se encuentra en un almacenamiento de NetApp y no está protegida, `Not protected` Aparece en la columna **Estado general**.
- Si una base de datos se encuentra en un sistema de almacenamiento de NetApp y está protegida, se muestra la interfaz de usuario `Backup not run` Mensaje en la columna **Estado general**.
- Si una base de datos se encuentra en un sistema de almacenamiento de NetApp y está protegida, y se activa el backup para la base de datos, aparece la interfaz de usuario de `Backup succeeded` 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.
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 copia de Snapshot 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 copias de Snapshot 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.

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.

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 copia de 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 copia de 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)

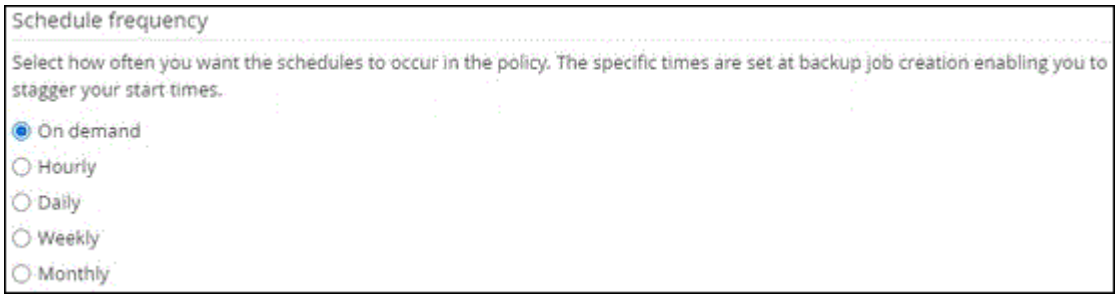
Indique un número mínimo y un número máximo de prioridad de backup mediante los cuales se determine la réplica de AG para backup. Por ejemplo, puede tener una prioridad mínima de 10 y una prioridad máxima de 50. En este caso, se tendrán en cuenta para el backup todas las réplicas de AG que tengan una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

Retener únicamente una cantidad específica de copias de Snapshot.

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 copias de Snapshot que se van a conservar
      i. Para especificar el número de copias snapshot que se deben conservar, seleccione **Total de copias snapshot que se deben conservar**.
      ii. Si la cantidad de copias de Snapshot supera el número especificado, las copias 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 copia de Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva copia de 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 copias de Snapshot
   a. Si desea especificar el número de días durante los que desea conservar las copias Snapshot antes de eliminarlas, seleccione **mantener copias Snapshot para**.
2. 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 copias de Snapshot que se van a conservar
      i. Para especificar el número de copias snapshot que se deben conservar, seleccione **Total de copias snapshot que se deben conservar**. Si la cantidad de copias de Snapshot supera el número especificado, las copias 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 copia de Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva copia de Snapshot en el destino.

1. Tiempo que se conservan las copias de Snapshot
   a. Para especificar el número de días durante los cuales desea conservar las copias snapshot antes de

eliminarlas, seleccione **Mantener copias snapshot para**.

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

En este ejemplo se establece la retención de la copia Snapshot del 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).

Actualizar SnapVault

Actualice SnapVault después de crear una copia snapshot.

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

Etiqueta de política secundaria

1. Seleccione una etiqueta de Snapshot.

Según la etiqueta de copia de Snapshot que seleccione, ONTAP aplicará la política de retención de copias de Snapshot secundarias 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 copias de Snapshot.

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 copia de Snapshot de la base de datos interna (TABLOCK)
      i. Seleccione **Limite las comprobaciones y obtenga los bloqueos en lugar de utilizar una copia de Snapshot de la base de datos interna (TABLOCK)** para limitar las comprobaciones y obtener bloqueos en lugar de utilizar una copia de Snapshot 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.

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: Escriba un nombre de copia de Snapshot personalizado y su formato. Por ejemplo, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la copia de 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. Puede revisar y editar haciendo clic en o eliminar haciendo 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 verificación **formato de nombre personalizado para copia de Snapshot** y, a continuación, introduzca un formato de nombre personalizado que desee usar para el nombre de la copia de Snapshot.

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

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

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

      Si desea crear una política, seleccione + 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 la sección **Agregar horarios para la directiva** `policy_name` Cuadro de diálogo, configure la programación y, a continuación, seleccione * Aceptar *.

Aquí `policy_name` es el nombre de la política seleccionada.

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, la `do_start method` Command inicia el servicio de plugin de VMware de SnapCenter. Actualice este 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 escribiendo el nombre en el cuadro de búsqueda o seleccionando y, a continuación, seleccionar 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. 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
- 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 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. Si utiliza el plugin para SQL Server o el plugin para Exchange Server, el panel Activity también muestra información sobre la operación de propagación.

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 copias de Snapshot del almacenamiento si el backup creado no se registra en SnapCenter Server. Si el backup ya está registrado en el servidor SnapCenter, no retrocederá la copia de 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** .

Del…	Acción
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 cancelando o ejecutando, debe ejecutar la `Cancel-SmJob -JobID <int> -Force` cmdlet para detener forzar 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 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.

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.

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 copias de Snapshot. Puede ser conveniente usar este cmdlet cuando las copias de Snapshot totales que se muestran en la topología Manage Copies no coinciden con la configuración de retención de copias de Snapshot de 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.

   En este ejemplo, se borra el número de backups secundarios sin copias de Snapshot:

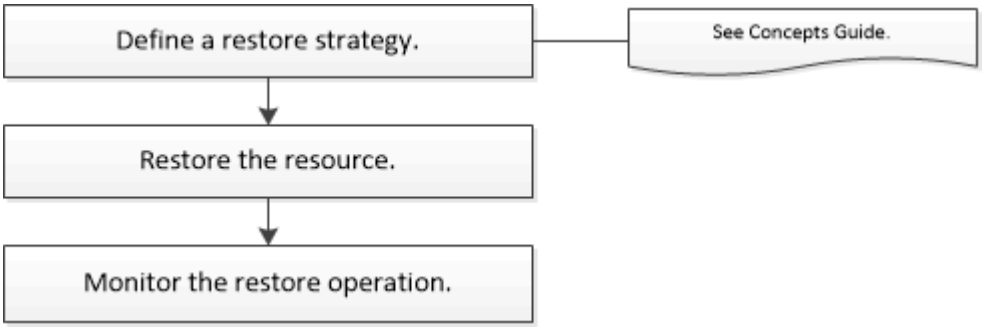
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Restaure recursos de SQL Server

Restaure el flujo de trabajo

Puede utilizar SnapCenter para restaurar bases de datos de SQL Server. Para ello, debe restaurar los datos a partir de uno o más backups en el sistema de archivos activo y, posteriormente, recuperar la base de datos. También puede restaurar las bases de datos que están en grupos de disponibilidad y después añadirlas a esos grupos. Antes de restaurar una base de datos de SQL Server, debe realizar varias tareas preparatorias.

El siguiente flujo de trabajo muestra la secuencia en la que debe realizar las operaciones de restauración de bases de datos:



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"

Más información

"Restaurar una base de datos de SQL Server a partir de almacenamiento secundario"

"Restaurar y recuperar recursos con cmdlets de PowerShell"

"Es posible que se produzca un error en la operación de restauración en Windows 2008 R2"

Requisitos para restaurar una base de datos

Antes de restaurar una base de datos de SQL Server a partir de un backup del plugin de SnapCenter para Microsoft SQL Server, debe asegurarse de que se cumplan diversos requisitos.

- La instancia de SQL Server de destino debe estar en línea y en ejecución para poder restaurar una base de datos.

  Esto se aplica tanto a operaciones de restauración de bases de datos del usuario como a operaciones de restauración de bases de datos del sistema.

- Deben deshabilitarse las operaciones de SnapCenter que están programadas para ejecutarse con los datos de SQL Server que se van a restaurar, lo que incluye cualquier trabajo programado en servidores de gestión remota o de verificación remota.
- Si las bases de datos del sistema no son funcionales, debe reconstruir primero las bases de datos del sistema con una utilidad de SQL Server.

- Si va a instalar el plugin, asegúrese de conceder permisos para que otros roles restauren los backups del grupo de disponibilidad (AG).

  La restauración de AG falla cuando se cumple alguna de las siguientes condiciones:

  - Si el plugin se instala mediante un usuario de RBAC y un administrador intenta restaurar un backup de AG
  - Si el plugin se instala mediante un administrador y un usuario de RBAC intenta restaurar un backup de AG
- Si va a restaurar backups de directorio de registro personalizado en un host alternativo, SnapCenter Server y el host del plugin deben tener instalada la misma versión de SnapCenter.
- Debe tener instalada la revisión KB2887595 de Microsoft. El sitio de asistencia técnica de Microsoft contiene más información acerca de KB2887595.

  "Artículo de soporte de Microsoft 2887595: Paquete acumulativo de actualizaciones de Windows RT 8.1, Windows 8.1 y Windows Server 2012 R2: Noviembre de 2013"
- Debe tener un backup de los grupos de recursos o de las bases de datos.
- Si va a replicar copias de Snapshot 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.
- Todos los trabajos de backup y clonado deben detenerse antes de restaurar la base de datos.
- Se puede agotar el tiempo de espera de la operación de restauración si el tamaño de la base de datos está en terabytes (TB).

  Aumente el valor del parámetro RESTTimeout de SnapCenter Server a 20000000 ms. Para ello, ejecute el siguiente comando: Set-SmConfigSettings -Agent -configSettings @{"RESTTimeout" = "20000000"}. Según el tamaño de la base de datos, el valor del tiempo de espera puede cambiarse y el valor máximo que puede configurarse es de 86400000 ms.

Si desea restaurar mientras las bases de datos están en línea, la opción de restauración en línea debe estar habilitada en la página Restore.

Restaurar backups de base de datos de SQL Server

Puede utilizar SnapCenter para restaurar bases de datos de SQL Server con backup. La restauración de bases de datos es un proceso multifásico que copia todos los datos y las páginas de registro de un backup de SQL Server en una base de datos especificada.

Acerca de esta tarea

- Puede restaurar las bases de datos de SQL Server con backup en una instancia diferente de SQL Server en el mismo host en que se creó el backup.

  Puede utilizar SnapCenter para restaurar las bases de datos de SQL Server con backup en una ruta alternativa para no sustituir una versión de producción.
- SnapCenter puede restaurar bases de datos en un clúster de Windows sin que el grupo de clústeres de SQL Server quede sin conexión.

- Si se produce un fallo de clúster (una operación de movimiento de grupos de clústeres) durante una operación de restauración (por ejemplo, si se desactiva el nodo al que pertenecen los recursos), debe volver a conectarse a la instancia de SQL Server y reiniciar la operación de restauración.
- No puede restaurar la base de datos cuando los usuarios o los trabajos de SQL Server Agent acceden a la base de datos.
- No puede restaurar bases de datos del sistema en una ruta alternativa.
- 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.

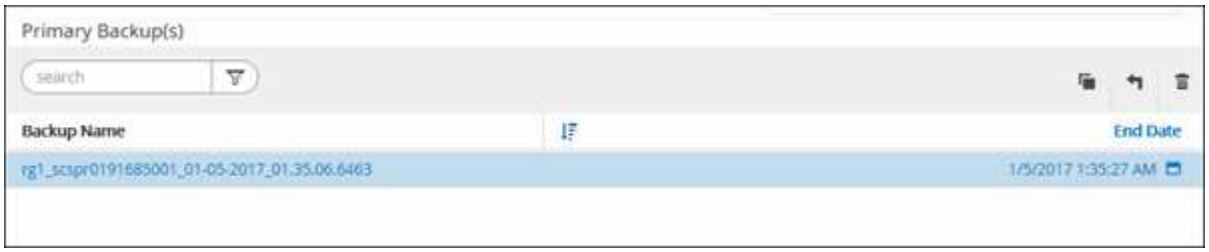
- La mayoría de los campos del asistente Restore son claros y explicativos. Aquí se ofrece información sobre los campos que podrían presentar dificultades.

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 **Resource Group** en la lista **View**.
3. Seleccione la base de datos o el grupo de recursos en la lista.

   Se muestra la página de topología.

4. En la vista Manage Copies, seleccione **copias de seguridad** en el sistema de almacenamiento.
5. Seleccione el backup en la tabla y haga clic en el .



6. En la página Restore Scope, seleccione una de las siguientes opciones:

Opción	Descripción
Restaure la base de datos en el mismo host en el que se creó el backup	Seleccione esta opción si desea restaurar la base de datos en la misma instancia de SQL Server donde se realizan los backups.

Opción	Descripción
Restaurar la base de datos en un host alternativo	Seleccione esta opción si desea que la base de datos se restaure en un servidor SQL diferente en el mismo host o diferente donde se realizan los backups. Seleccione un nombre de host, proporcione un nombre de base de datos (opcional), seleccione una instancia y especifique las rutas de restauración. La extensión de archivo proporcionada en la ruta alternativa debe ser la misma que la del archivo de base de datos original. Si la opción **Restaurar la base de datos a un host alternativo** no aparece en la página Restaurar ámbito, borre la memoria caché del explorador.
Restaurar la base de datos con archivos de base de datos existentes	Seleccione esta opción si desea que la base de datos se restaure en un SQL Server alternativo en el mismo host o en otro donde se realizan los backups. Los archivos de bases de datos ya deben estar presentes en las rutas de archivos existentes dadas. Seleccione un nombre de host, proporcione un nombre de base de datos (opcional), seleccione una instancia y especifique las rutas de restauración.

7. En la página Restore Scope, seleccione una de las siguientes opciones:

Opción	Descripción
Ninguno	Seleccione **Ninguno** cuando necesite restaurar sólo la copia de seguridad completa sin ningún registro.
Todos los backups de registros	Seleccione **All log backups** up-to-the-minute backup restore operation para restaurar todas las copias de seguridad de registros disponibles después de la copia de seguridad completa.

Opción	Descripción
Mediante backups de registros hasta que	Seleccione **by log backups** para realizar una operación de restauración a un momento específico, que restaura la base de datos en función de los registros de copia de seguridad hasta el registro de copia de seguridad con la fecha seleccionada.
Por fecha específica hasta	Seleccione **by specific date until** para especificar la fecha y la hora después de las cuales no se aplican registros de transacciones a la base de datos restaurada. Esta operación de restauración a un momento específico detiene la restauración de entradas de registro registradas después de la fecha y la hora especificadas.
Utilizar directorio de registro personalizado	Si ha seleccionado **todas las copias de seguridad de registro**, **por copias de seguridad de registro** o **por fecha específica hasta** y los registros se encuentran en una ubicación personalizada, seleccione **usar directorio de registro personalizado** y, a continuación, especifique la ubicación del registro. La opción **Usar directorio de registro personalizado** solo está disponible si ha seleccionado **Restaurar la base de datos a un host alternativo** o **Restaurar la base de datos utilizando archivos de base de datos existentes**. También puede utilizar la ruta de acceso compartida, pero asegúrese de que el usuario de SQL puede acceder a la ruta de acceso. El directorio de registro personalizado no se admite en la base de datos de grupos de disponibilidad.

8. En la página Pre OPS, realice los siguientes pasos:

   a. En la página Pre Restore Options, seleccione una de las siguientes opciones:

      - Seleccione **Sobrescribir la base de datos con el mismo nombre durante la restauración** para restaurar la base de datos con el mismo nombre.
      - Seleccione **mantener la configuración de replicación de bases de datos SQL** para restaurar la base de datos y mantener la configuración de replicación existente.
      - Seleccione **Crear copia de seguridad del registro de transacciones antes de restaurar** para crear un registro de transacciones antes de que comience la operación de restauración.

- Seleccione **Quit restore if transaction log backup before restore fails** para anular la operación de restauración si falla la copia de seguridad del registro de transacciones.

b. Especifique scripts opcionales que ejecutar antes de realizar un trabajo de restauración.

Por ejemplo, es posible ejecutar un script para actualizar las capturas SNMP, automatizar alertas, enviar registros, etc.

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

9. En la página Post OPS, realice los siguientes pasos:

a. En la sección Choose database state after restore completes, seleccione una de las siguientes opciones:

- Seleccione **Operational, but unavailable for restoring additional transaction logs** si va a restaurar todas las copias de seguridad necesarias ahora.

  Este es el comportamiento predeterminado, que deja la base de datos preparada para su uso revirtiendo las transacciones no comprometidas. No podrá restaurar registros de transacciones adicionales hasta que cree un backup.

- Seleccione **no operativo, pero disponible para restaurar registros transaccionales adicionales** para dejar la base de datos no operativa sin revertir las transacciones no comprometidas.

  Pueden restaurarse registros de transacciones adicionales. No podrá utilizar la base de datos hasta que esta se recupere.

- Seleccione **modo de sólo lectura, disponible para restaurar registros transaccionales adicionales** para dejar la base de datos en modo de sólo lectura.

  Esta opción deshace las transacciones no comprometidas, pero guarda las acciones deshechas en un archivo en espera para que puedan revertirse los efectos de recuperación.

Si se habilita la opción Undo directory, se restauran más registros de transacciones. Si la operación de restauración para el registro de transacciones no se realiza correctamente, pueden revertirse los cambios. La documentación de SQL Server contiene más información.

b. Especifique scripts opcionales tras realizar un trabajo de restauración.

Por ejemplo, es posible ejecutar un script para actualizar las capturas SNMP, automatizar alertas, enviar registros, etc.

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

10. 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.

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

12. Supervise el proceso de restauración mediante la página **Monitor** > **Jobs**.

Información relacionada

"Restaurar y recuperar recursos con cmdlets de PowerShell"

"Restaurar una base de datos de SQL Server a partir de almacenamiento secundario"

Restaurar una base de datos de SQL Server a partir de almacenamiento secundario

Puede restaurar bases de datos de SQL Server con backup a partir de LUN físicos (RDM, iSCSI o FCP) en un sistema de almacenamiento secundario. La función de restauración es un proceso multifásico que copia todos los datos y las páginas de registro a partir de un backup de SQL Server especificado que reside en el sistema de almacenamiento secundario en una base de datos especificada.

Antes de empezar

- Debe haber replicado las copias de Snapshot a desde el sistema de almacenamiento principal hasta el secundario.
- Debe asegurarse de que SnapCenter Server y el host del plugin puedan conectarse al sistema de almacenamiento secundario.
- La mayoría de los campos del asistente Restore se explican en el proceso de restauración básico. Aquí se ofrece información sobre algunos de los campos que podrían presentar dificultades.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione **complemento SnapCenter para SQL Server** en la lista.
2. En la página Resources, seleccione **Database** o **Resource Group** en la lista desplegable **View**.
3. Seleccione la base de datos o el grupo de recursos.

   Se muestra la página de topología de la base de datos o el grupo de recursos.

4. En la sección Manage Copies, seleccione **copias de seguridad** en el sistema de almacenamiento secundario (reflejado o almacén).
5. Seleccione el backup en la lista y haga clic en .
6. En la página Location, elija el volumen de destino para restaurar el recurso seleccionado.
7. Complete el asistente Restaurar, revise el resumen y, a continuación, haga clic en **Finalizar**.

Si restauró una base de datos en una ruta diferente compartida por otras bases de datos, debe realizar un backup completo y una verificación de backup para confirmar que la base de datos restaurada no tiene daños de nivel físico.

Propagación de bases de datos de grupos de disponibilidad

La propagación es una opción para restaurar las bases de datos de grupos de disponibilidad (AG). Si una base de datos secundaria deja de estar sincronizada con la base de datos principal de un AG, puede propagar la base de datos secundaria.

Antes de empezar

- Debe tener creado un backup de la base de datos de AG secundaria que desea restaurar.
- El servidor de SnapCenter y el host del plugin deben tener instalada la misma versión de SnapCenter.

Acerca de esta tarea

- No puede ejecutar la operación de propagación con bases de datos principales.
- No puede realizar una operación de propagación si la base de datos de réplica se quita del grupo de disponibilidad. Cuando se elimina la réplica, la operación de propagación genera un error.
- Mientras ejecuta la operación de propagación con la base de datos de SQL Availability Group, no debe activar los backups de registro en las bases de datos de réplica de esa base de datos de grupo de disponibilidad. Si activa los backups de registros durante la operación de propagación, la operación de propagación con la base de datos de reflejo, "database_name" tiene datos de registro de transacciones insuficientes para preservar la cadena de backup de registros del mensaje de error principal de la base de datos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Recursos** y, a continuación, seleccione **complemento SnapCenter para SQL Server** en la lista.
2. En la página Resources, seleccione **Database** en la lista **View**.
3. Seleccione la base de datos secundaria de AG de la lista.
4. Haga clic en **reseed**.
5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

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.

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

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:

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

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

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 operaciones de restauración de recursos de SQL

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.

Tras la operación de restauración basada en volumen, los metadatos del backup se eliminan del repositorio de SnapCenter, pero las entradas de catálogo de backup permanecen en el catálogo SAP HANA. Aunque el estado del trabajo de restauración indique , debe hacer clic en los detalles del trabajo para ver el signo de advertencia de algunas de las tareas secundarias. Haga clic en el signo de advertencia y elimine las entradas del catálogo de backup indicadas.

Cancelar las operaciones de restauración de recursos de SQL

Es posible cancelar los trabajos de restauración que se encuentran en cola.

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

Acerca de esta tarea

- Puede cancelar una operación de restauración en cola desde la página **Monitor** o desde el panel **actividad**.
- No se puede cancelar una operación de restauración en ejecución.
- Es posible usar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de restauración en cola.
- El botón **Cancelar trabajo** está desactivado para operaciones de restauración 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 restauración en cola de otros miembros mientras utiliza esa función.

Paso

Ejecute una de las siguientes acciones:

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

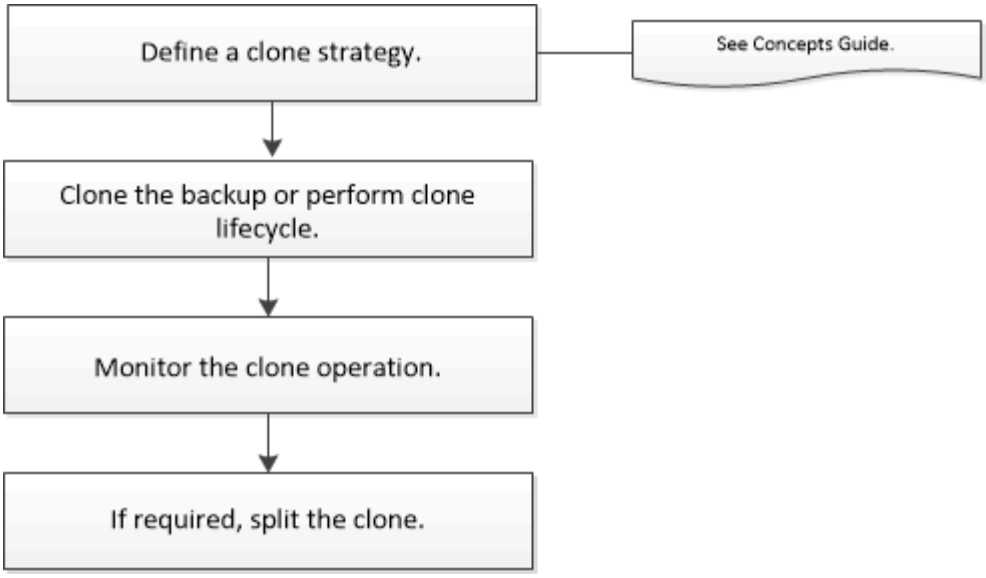
Clone recursos de bases de datos de SQL Server

Flujo de trabajo de clonado

Debe ejecutar varias tareas con SnapCenter Server antes de clonar los recursos de bases de datos a partir de un backup. La clonado de base de datos es el proceso de crear una copia de un momento específico de una base de datos de producción o su conjunto de backups. Puede clonar bases de datos para probar la funcionalidad que se debe implementar utilizando la estructura y el contenido actuales de la base de datos durante los ciclos de desarrollo de aplicaciones, para usar las herramientas de extracción y manipulación de datos al rellenar almacenes de datos, o bien ara recuperar datos que se eliminaron o cambiaron por error.

Las operaciones de clonado de bases de datos generan informes basados en los ID de trabajo.

El siguiente flujo de datos muestra la secuencia en la que debe ejecutar las operaciones de clonado:



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"

Más información

"Clonar a partir de un backup de base de datos de SQL Server"

"Ejecute el ciclo de vida del clon"

"Es posible que la operación de clonado produzca errores o tarde más tiempo en finalizar con el valor TCP_TIMEOUT predeterminado"

Clonar a partir de un backup de base de datos de SQL Server

Puede utilizar SnapCenter para clonar un backup de base de datos de SQL Server. Si desea acceder a o restaurar una versión anterior de los datos, puede clonar backups de base de datos bajo demanda.

Antes de empezar

- Debe haberse preparado para la protección de datos completando ciertas tareas, como añadir hosts, identificar recursos y crear conexiones de sistema de almacenamiento.
- Debe tener un backup de las bases de datos o de los grupos de recursos.
- El tipo de protección, como reflejo, almacén o reflejo-almacén para el LUN de datos y el LUN de registro, debe ser el mismo para detectar localizadores secundarios durante la clonado en un host alternativo mediante backups de registros.
- Si no se puede encontrar la unidad de clonado montada durante una operación de clonado de SnapCenter, debe cambiar el parámetro CloneRetryTimeout de SnapCenter Server a 300.
- 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).

Acerca de esta tarea

- Mientras se clona en una instancia de base de datos independiente, asegúrese de que exista la ruta de

acceso del punto de montaje y sea un disco dedicado.

- Al realizar la clonación en una instancia de clúster de conmutación por error (FCI, Failover Cluster Instance), asegúrese de que los puntos de montaje existen, son un disco compartido y la ruta de acceso y el FCI deben pertenecer al mismo grupo de recursos SQL.
- Asegúrese de que solo hay un iniciador VFC o FC conectado a cada host. Esto se debe a que, SnapCenter solo admite un iniciador por host.
- Si la base de datos de origen o la instancia de destino se encuentran en un volumen compartido de clúster (csv), la base de datos clonada se realizará en csv.
- 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.

Para los entornos virtuales (VMDK/RDM), asegúrese de que el punto de montaje es un disco dedicado.

Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione **SnapCenter Plug-in for SQL Server** de la lista.
2. En la página Resources, seleccione **Database** o **Resource Group** en la lista **View**.

   No se admite la clonado del backup de una instancia.

3. Seleccione la base de datos o el grupo de recursos.
4. En la página de visualización de **Manage Copies**, seleccione la copia de seguridad del sistema de almacenamiento principal o secundario (reflejado o en almacén).
5. Seleccione el backup y, a continuación, seleccione .
6. En la página **Clone Options**, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Clone el servidor	Elija el host donde se debe crear el clon.
Instancia de clon	Seleccione la instancia de clonado en la que desea que se clone el backup de base de datos. Esta instancia de SQL debe estar ubicada en el servidor de clones especificado.

Para este campo…	Realice lo siguiente…
Sufijo de clon	Introduzca el sufijo que se incorporará al nombre de archivo del clon para identificar que la base de datos es un clon. Por ejemplo, *db1_clone*. Si clona en la misma ubicación que la de la base de datos original, debe proporcionar un sufijo para diferenciar la base de datos clonada de la original. De lo contrario, la operación dará error.
Auto assign Mount point o Auto assign volume Mount point under path	Elija si asignar automáticamente un punto de montaje o un punto de montaje de volumen en una ruta. Auto assign volume Mount point under path: El punto de montaje en una ruta permite proporcionar un directorio específico. Los puntos de montaje se crearán dentro de ese directorio. Antes de seleccionar esta opción, debe asegurarse de que el directorio esté vacío. Si hay una base de datos en ese directorio, la base de datos presentará un estado no válido después de la operación de montaje.

7. En la página Logs, seleccione una de las siguientes opciones:

Para este campo…	Realice lo siguiente…
Ninguno	Seleccione esta opción si solo desea clonar el backup completo sin ningún registro.
Todos los backups de registros	Seleccione esta opción para clonar todos los backups de registro disponibles con fecha posterior al backup completo.
Mediante backups de registros hasta que	Seleccione esta opción para clonar la base de datos según los registros de backup que se crearon hasta el registro de backup con la fecha seleccionada.
Por fecha específica hasta	Indique la fecha y la hora después de las cuales los registros de transacciones no se aplican a la base de datos clonada. Esta clonado de momento específico detiene la clonado de las entradas del registro de transacciones que se registraron después de la fecha y la hora especificadas.

8. En la página **Script**, introduzca el tiempo de espera del script, la ruta y los argumentos del script previo o script posterior que deben ejecutarse antes o después de la operación de clonado, respectivamente.

   Por ejemplo, es posible ejecutar un script para actualizar las capturas SNMP, automatizar alertas, enviar registros, etc.

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

   El tiempo de espera predeterminado del script es 60 segundos.

9. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, 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 de clonado realizada, seleccione **Adjuntar informe de trabajo**.

   > Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell Set-SmSmtpServer.

   Para EMS, consulte "Gestione la recogida de datos de EMS"

10. Revisa el resumen y luego selecciona **Finalizar**.
11. Supervise el progreso de la operación seleccionando **Monitor** > **Trabajos**.

Después de terminar

Después de crear el clon, no debe cambiar nunca el nombre.

Información relacionada

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

"Clonar backups mediante cmdlets de PowerShell"

"Es posible que la operación de clonado produzca errores o tarde más tiempo en finalizar con el valor TCP_TIMEOUT predeterminado"

"Se produce un error en el clon de la base de datos de la instancia de clúster"

Clonar backups 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.

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. Enumere los backups que pueden clonarse mediante el cmdlet Get-SmBackup o Get-SmResourceGroup.

   Este ejemplo muestra información sobre todos los backups disponibles:

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

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

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

   En este ejemplo, se muestra información sobre un grupo de recursos especificado, sus recursos y sus políticas asociadas:

```
PS C:\> Get-SmResourceGroup -ListResources –ListPolicies

Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMaping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
```

```
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeOut : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
```

```
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
```

3. Inicie una operación de clonado a partir de un backup existente con el cmdlet New-SmClone.

   En este ejemplo, se crea un clon a partir de un determinado backup con todos los registros:

```
PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

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

   En este ejemplo, se crea un clon en una instancia concreta de Microsoft SQL Server:

```
PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. Puede consultar el estado del trabajo de clonado mediante el cmdlet Get-SmCloneReport.

   En este ejemplo, se muestra un informe de clonado con el correspondiente ID de trabajo:

```
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}
```

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".

Ejecute el ciclo de vida del clon

Mediante SnapCenter, puede crear clones a partir de un grupo de recursos o una base de datos. Puede realizar un clon bajo demanda o programar operaciones de clonado periódicas de un grupo de recursos o una base de datos. Si clona un backup periódicamente, puede utilizar el clon para desarrollar aplicaciones, completar datos o recuperar datos.

SnapCenter permite programar varias operaciones de clonado para que se ejecuten simultáneamente ente

varios servidores.

Antes de empezar

- Mientras se clona en una instancia de base de datos independiente, asegúrese de que exista la ruta de acceso del punto de montaje y sea un disco dedicado.
- Al realizar la clonación en una instancia de clúster de conmutación por error (FCI, Failover Cluster Instance), asegúrese de que los puntos de montaje existen, son un disco compartido y la ruta de acceso y el FCI deben pertenecer al mismo grupo de recursos SQL.
- Si la base de datos de origen o la instancia de destino se encuentran en un volumen compartido de clúster (csv), la base de datos clonada se realizará en csv.

Para los entornos virtuales (VMDK/RDM), asegúrese de que el punto de montaje es un disco dedicado.

Acerca de esta tarea

- 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.

- La mayoría de los campos de las páginas del asistente Clone Lifecycle son autoexplicativos. Aquí se ofrece información sobre los campos que podrían presentar dificultades.

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 **Resource Group** en la lista **View**.
3. Seleccione el grupo de recursos o la base de datos y, a continuación, haga clic en **Clone Lifecycle**.
4. En la página Options, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Nombre del trabajo de clonado	Especifique el nombre de trabajo de ciclo de vida de clon que ayuda en la supervisión y la modificación del trabajo de ciclo de vida de clon.
Clone el servidor	Elija el host en el que debe colocarse el clon.
Instancia de clon	Elija la instancia de clon en la que desea clonar la base de datos. Esta instancia de SQL debe estar ubicada en el servidor de clones especificado.

Para este campo…	Realice lo siguiente…
Sufijo de clon	Introduzca el sufijo que se incorporará a la base de datos de clones para identificar que se trata de un clon. Cada instancia de SQL que se utiliza para crear un grupo de recursos de clon debe tener un nombre de base de datos único. Por ejemplo, si el grupo de recursos del clon contiene una base de datos de origen «nb1» de una instancia de SQL «'inst1'» y «db1» se clona en «'inst1'», el nombre de la base de datos del clon deberá ser «db1*clone».* *'"*clone'" es un sufijo obligatorio definido por el usuario porque la base de datos se clona en la misma instancia. Si se clona «db1» en la instancia de SQL «'inst2'», el nombre de la base de datos clonada puede permanecer «db1» (el sufijo es opcional) porque la base de datos se clona en una instancia diferente.
Auto assign Mount point o Auto assign volume Mount point under path	Elija si asignar automáticamente un punto de montaje o un punto de montaje de volumen en una ruta. Si opta por asignar automáticamente un punto de montaje de volumen en una ruta, puede proporcionar un directorio específico. Los puntos de montaje se crearán dentro de ese directorio. Antes de seleccionar esta opción, debe asegurarse de que el directorio esté vacío. Si hay una base de datos en ese directorio, la base de datos presentará un estado no válido después de la operación de montaje.

5. En la página ubicación, seleccione una ubicación de almacenamiento para crear un clon.
6. 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 clonado, según corresponda.

   Por ejemplo, es posible ejecutar un script para actualizar las capturas SNMP, automatizar alertas, enviar registros, etc.

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

   El tiempo de espera predeterminado del script es 60 segundos.

7. En la página Schedule, realice una de las siguientes acciones:
   - Seleccione **Ejecutar ahora** si desea ejecutar el trabajo de clonado inmediatamente.
   - Seleccione **Configure schedule** cuando desea determinar la frecuencia con la que debe producirse la operación de clonado, cuándo debe iniciarse la programación de clonado, en qué día debe producirse la programación de clonado, cuándo debe caducar la programación y si los clones tienen que eliminarse cuando caduque la programación.
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 de clonado realizada, seleccione **Adjuntar informe de trabajo**.

> Para las notificaciones de correo electrónico, se deben haber especificado los detalles del servidor SMTP desde la interfaz gráfica de usuario o desde el comando de PowerShell Set-SmSmtpServer.

Para EMS, consulte "Gestione la recogida de datos de EMS"

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

Debe supervisar el proceso de clonación mediante la página **Monitor** > **Jobs**.

Supervisar operaciones de clonado de bases de datos de SQL

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**.

Cancelar las operaciones de clonado de recursos SQL

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

Debe iniciar sesión como administrador de SnapCenter o propietario del trabajo para cancelar las operaciones de clonado.

Acerca de esta tarea

- Puede cancelar una operación de clonación en cola desde la página **Monitor** o desde el panel **actividad**.
- No se puede cancelar una operación de clonado en ejecución.
- Es posible usar la interfaz gráfica de usuario de SnapCenter, los cmdlets de PowerShell o los comandos de la CLI para cancelar las operaciones de clonado en cola.
- 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 clonación en cola de otros miembros mientras utiliza esa función.

Paso

Ejecute una de las siguientes acciones:

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

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"

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.