# Proteger las bases de datos SAP HANA

SnapCenter Software 4.8

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/es-es/snapcenter-48/protect-hana/concept_snapcenter_plug_in_for_sap_hana_database_overview.html on September 26, 2025. Always check docs.netapp.com for the latest.

# Tabla de contenidos


Proteger las bases de datos SAP HANA . . . 1
Plugin de SnapCenter para base de datos SAP HANA . . . 1
Información general sobre el plugin de SnapCenter para bases de datos de SAP HANA . . . 1
Tareas que pueden llevarse a cabo con el plugin de SnapCenter para base de datos SAP HANA . . . 1
Funciones del plugin de SnapCenter para base de datos SAP HANA . . . 1
Tipos de almacenamiento compatibles con el plugin de SnapCenter para base de datos SAP HANA . . . 2
Privilegios mínimos ONTAP requeridos para el plugin de SAP HANA . . . 3
Preparar los sistemas de almacenamiento para la replicación SnapMirror y SnapVault para las bases de datos SAP HANA . . . 7
Estrategia de backup para las bases de datos SAP HANA . . . 8
Estrategia de restauración y recuperación para bases de datos SAP HANA . . . 11
Prepare la instalación del plugin de SnapCenter para las bases de datos SAP HANA . . . 14
Flujo de trabajo de instalación del plugin de SnapCenter para base de datos SAP HANA . . . 14
Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para bases de datos SAP HANA . . . 14
Requisitos del host para instalar el paquete de plugins de SnapCenter para Windows . . . 15
Requisitos del host para instalar el paquete de plugins de SnapCenter para Linux . . . 16
Credenciales de configuración del plugin de SnapCenter para la base de datos SAP HANA . . . 17
Configurar GMSA en Windows Server 2012 o posterior . . . 20
Instale el plugin de SnapCenter para base de datos SAP HANA . . . 21
Configurar certificado de CA . . . 27
Instale el plugin de SnapCenter para VMware vSphere . . . 35
Implemente el certificado de CA . . . 35
Configure el archivo CRL . . . 36
Prepárese para la protección de datos . . . 36
Requisitos previos para usar el plugin de SnapCenter para base de datos SAP HANA . . . 36
Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger bases de datos SAP HANA . . . 36
Realice un backup de los recursos de SAP HANA . . . 37
Realice un backup de los recursos de SAP HANA . . . 37
Configure la clave de almacenamiento de usuario HDB y el usuario del sistema operativo HDBSQL para la base de datos SAP HANA . . . 38
Descubra recursos y prepare contenedores de bases de datos multitenant para la protección de datos . . . 39
Añada recursos manualmente al host del plugin . . . 42
Crear políticas de backup para bases de datos SAP HANA . . . 44
Crear grupos de recursos y añadir políticas . . . 49
Realice un backup de las bases de datos SAP HANA . . . 53
Realice un backup de los grupos de recursos . . . 56
Cree una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para la base de datos SAP HANA . . . 57
Realizar un backup de bases de datos mediante cmdlets de PowerShell . . . 59
Supervisar las operaciones de backup . . . 62

Cancele las operaciones de backup para SAP HANA . . . 64
Consulte los backups y los clones de la base de datos SAP HANA en la página Topology . . . 64
Restaure bases de datos de SAP HANA . . . 66
Restaure el flujo de trabajo . . . 66
Restaurar y recuperar un backup de recurso añadido manualmente . . . 66
Restaurar y recuperar un backup de base de datos detectado automáticamente . . . 68
Restaurar una base de datos SAP HANA mediante cmdlets de PowerShell . . . 72
Restaurar recursos mediante los cmdlets de PowerShell . . . 74
Supervisar las operaciones de restauración de bases de datos SAP HANA . . . 77
Clonar backups de recursos SAP HANA . . . 78
Flujo de trabajo de clonado . . . 78
Clonar un backup de base de datos SAP HANA . . . 79
Clonar backups de la base de datos SAP HANA mediante cmdlets de PowerShell . . . 81
Supervise las operaciones de clonado de base de datos SAP HANA . . . 83
Divida un clon . . . 84
Elimine o divida los clones de las bases de datos SAP HANA después de actualizar SnapCenter . . . 85

# Proteger las bases de datos SAP HANA

## Plugin de SnapCenter para base de datos SAP HANA

### Información general sobre el plugin de SnapCenter para bases de datos de SAP HANA

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

SnapCenter admite contenedores individuales y contenedores de bases de datos multitenant (MDC). Es posible utilizar el plugin para base de datos SAP HANA tanto en entornos de Windows como de Linux. El plugin que no está instalado en el host de la base de datos HANA se conoce como plugin de host centralizado. El complemento de host centralizado puede gestionar varias bases de datos HANA en diferentes hosts.

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

### Tareas que pueden llevarse a cabo con el plugin de SnapCenter para base de datos SAP HANA

Cuando el plugin para base de datos SAP HANA está instalado en el entorno, es posible usar SnapCenter para realizar backup, restaurar y clonar bases de datos SAP HANA y sus recursos. También es posible ejecutar tareas complementarias a estas operaciones.

- Agregar bases de datos.
- Crear backups.
- Restaurar desde backups.
- Clonar backups.
- Programar operaciones de backup.
- Supervisar operaciones de backup, de restauración y de clonado.
- Ver informes para operaciones de backup, restauración y clonado.

### Funciones del plugin de SnapCenter para base de datos SAP HANA

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

- **Interfaz gráfica de usuario unificada**

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

- **Administración central automatizada**

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

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

  SnapCenter utiliza la tecnología de copias de Snapshot de NetApp con el plugin para bases de datos de SAP HANA para realizar backups de recursos.

Usar el plugin para bases de datos de SAP HANA también ofrece los siguientes beneficios:

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

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

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

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

- Compatibilidad con la función de copia de Snapshot de grupo de consistencia de ONTAP como parte de la creación de backups.
- Capacidad para ejecutar varios backups de forma simultánea entre varios hosts de recursos

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

- Capacidad para crear copias de Snapshot con comandos externos.
- Compatibilidad con backups basados en archivos.
- Compatibilidad con LVM de Linux en el sistema de archivos XFS.

## Tipos de almacenamiento compatibles con el plugin de SnapCenter para base de datos SAP HANA

SnapCenter es compatible con una amplia gama de tipos de almacenamiento tanto en máquinas físicas como máquinas virtuales (VM). Debe verificar la compatibilidad de su tipo de almacenamiento antes de instalar el plugin de SnapCenter para base de datos SAP HANA.

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

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

## Privilegios mínimos ONTAP requeridos para el plugin de SAP HANA

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<br><br>detención de trabajo |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.3.0 y versiones posteriores |
| --- |
| 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 |
| reserva persistente de lun clara |
| cambio de tamaño de lun |
| serie de lun |
| muestra de lun |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.3.0 y versiones posteriores |
| --- |
| regla adicional de la política de snapmirror<br>regla de modificación de la política de snapmirror<br>regla de eliminación de la política de snapmirror<br>la política de snapmirror<br>restauración de snapmirror<br>de snapmirror<br>historial de snapmirror<br>actualización de snapmirror<br>conjunto de actualizaciones de snapmirror<br>destinos de listas de snapmirror |
| versión |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.3.0 y versiones posteriores |
| --- |
| 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 |

| Comandos de acceso total: Privilegios mínimos requeridos para ONTAP 8.3.0 y versiones posteriores |
| --- |
| vserver cifs |
| vserver cifs share create |
| eliminación de vserver cifs share |
| se muestra vserver shadowcopy |
| visualización de vserver cifs share |
| visualización de vserver cifs |
| política de exportación de vserver |
| creación de política de exportación de vserver |
| eliminación de la política de exportación de vserver |
| creación de reglas de política de exportación de vserver |
| aparece la regla de política de exportación de vserver |
| visualización de la política de exportación de vserver |
| vserver iscsi |
| se muestra la conexión iscsi del vserver |
| se muestra vserver |

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

## Preparar los sistemas de almacenamiento para la replicación SnapMirror y SnapVault para las bases de datos SAP HANA

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 las bases de datos SAP HANA

### Defina una estrategia de backup para las bases de datos SAP HANA

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

#### Acerca de esta tarea

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

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

proporcionar un script previo o posterior.

**Detección automática de recursos en el host Linux**

Los recursos son bases de datos de SAP HANA y volumen de datos no data en el host Linux que gestiona SnapCenter. Después de instalar el plugin de SnapCenter para el plugin de base de datos SAP HANA, las bases de datos SAP HANA en ese host Linux se detectan automáticamente y se muestran en la página Resources.

La detección automática es compatible con los siguientes recursos de SAP HANA:

- Contenedores individuales

  Después de instalar o actualizar el plugin, los recursos de contenedor único ubicados en un plugin de host centralizado continuarán siendo recursos añadidos manualmente.

  Después de instalar o actualizar el plugin, las bases de datos SAP HANA se detectan de forma automática solo en los hosts SAP HANA Linux, que se registran directamente en SnapCenter.

- Contenedor de base de datos multitenant (MDC)

  Después de instalar o actualizar el plugin, los recursos de MDC ubicados en un plugin de host centralizado continuarán siendo un recurso añadido manualmente.

  Debe continuar añadiendo manualmente los recursos del MDC en el plugin del host centralizado después de actualizar a SnapCenter 4.3.

  Para los hosts SAP HANA Linux registrados directamente en SnapCenter, instalar o actualizar el plugin provocará una detección automática de los recursos del host. Después de actualizar el plugin, para cada recurso MDC ubicado en el host del plugin, se descubre automáticamente otro recurso MDC con un formato GUID diferente y se registra en SnapCenter. El nuevo recurso estará bloqueado.

  Por ejemplo, en SnapCenter 4.2, si el recurso de E90 MDC se encuentra en el host del plugin y se registró manualmente, después de actualizar a SnapCenter 4.3, se detecta otro recurso de E90 MDC con un GUID diferente y se registra en SnapCenter.

La detección automática no es compatible con las siguientes configuraciones:

- Distribución con RDM y VMDK

  Si se detectan los recursos anteriores, las operaciones de protección de datos no son compatibles con estos recursos.

- Configuración de varios hosts DE HANA
- Varias instancias en el mismo host
- Escalado horizontal de varios niveles replicación de sistemas HANA
- Entorno de replicación en cascada en modo de replicación de sistemas

**Tipo de backups admitido**

El tipo de backup especifica el tipo de backup que desea crear. SnapCenter admite los tipos de backups basados en archivos y backups basados en copias de Snapshot para

bases de datos de SAP HANA.

#### Backups basados en archivos

Los backups basados en archivos verifican la integridad de la base de datos. Es posible programar una operación de backup basado en archivos para que se produzca en intervalos específicos. Solo se realiza un backup de los inquilinos activos. No es posible restaurar ni clonar backups basados en archivos desde SnapCenter.

#### Backup basado en copia de Snapshot

Los backups basados en copia de Snapshot aprovechan la tecnología de copia de Snapshot de NetApp para crear copias en línea y de solo lectura de los volúmenes en los cuales residen las bases de datos de SAP HANA.

### Cómo usa el plugin de SnapCenter para base de datos SAP HANA las copias de Snapshot de grupos de consistencia

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

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

### Cómo hace SnapCenter para gestionar el mantenimiento de backups de registros y datos

SnapCenter gestiona el mantenimiento de los backups de registros y de datos en los niveles de sistema de almacenamiento y sistema de archivos, y dentro del catálogo de backup SAP HANA.

Las copias de Snapshot en el almacenamiento primario y secundario y sus entradas correspondientes en el catálogo SAP HANA se eliminan de acuerdo con la configuración de retención. Las entradas del catálogo SAP HANA también se eliminan durante la eliminación de grupos de backup y recursos.

### Consideraciones para determinar programaciones de backup para base de datos SAP HANA

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

Las programaciones de backup están compuestas por dos partes:

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

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

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

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

#### Cantidad de tareas de backup necesarias para bases de datos SAP HANA

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

#### Convenciones de nomenclatura de backups para bases de datos del plugin para SAP HANA

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.

## Estrategia de restauración y recuperación para bases de datos SAP HANA

#### Defina una estrategia de restauración y recuperación para recursos de SAP HANA

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

- Pasos*
  1. Determinar las estrategias de restauración compatibles con los recursos SAP HANA añadidos manualmente
  2. Determinar las estrategias de restauración compatibles con las bases de datos SAP HANA detectadas automáticamente
  3. Decidir el tipo de operaciones de recuperación que se desea ejecutar.

#### Tipos de estrategias de restauración compatibles con los recursos de SAP HANA añadidos manualmente

Para poder ejecutar correctamente las operaciones de restauración, es necesario definir una estrategia mediante SnapCenter. Existen dos tipos de estrategias de restauración para los recursos de SAP HANA que se añaden manualmente. No puede recuperar los recursos de SAP HANA añadidos manualmente.

No puede recuperar los recursos de SAP HANA añadidos manualmente.

##### Restauración de recursos completa

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

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

##### Restauración de nivel de archivos

- Restaura los archivos de volúmenes, qtrees o directorios
- Restaura solo los LUN seleccionados

#### Tipos de estrategias de restauración compatibles para las bases de datos SAP HANA detectadas automáticamente

Para poder ejecutar correctamente las operaciones de restauración, es necesario definir una estrategia mediante SnapCenter. Existen dos tipos de estrategias de restauración para las bases de datos SAP HANA detectadas automáticamente.

##### Restauración de recursos completa

- Restaura todos los volúmenes, qtrees y LUN de un recurso
  - Debe seleccionarse la opción **revertir volumen** para restaurar todo el volumen.

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

**Base de datos de tenant**

- Restaura la base de datos de tenant

Si se selecciona la opción **base de datos de inquilino**, deben utilizarse secuencias de comandos de recuperación de HANA Studio o HANA externas a SnapCenter para realizar la operación de recuperación.

### Tipos de operaciones de restauración para las bases de datos SAP HANA detectadas automáticamente

SnapCenter admite tipos de restauración SnapRestore (VBSR) basada en volúmenes, SnapRestore de archivos individuales y restauración por conexión y copia para bases de datos SAP HANA detectadas automáticamente.

**La SnapRestore basada en volúmenes (VBSR) se realiza en entornos NFS para las siguientes situaciones:**

- Cuando la copia de seguridad seleccionada para restaurar se realiza en versiones anteriores a SnapCenter 4.3 y sólo si se selecciona la opción **Complete Resource**
- Cuando la copia de seguridad seleccionada para restaurar se realiza en SnapCenter 4.3, y si la opción **revertir volumen** está seleccionada

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

- Cuando la copia de seguridad seleccionada para restaurar se realiza en SnapCenter 4.3, y si sólo se selecciona la opción **completar recurso**
- Para contenedores de bases de datos multitenant (MDC), cuando la copia de seguridad seleccionada para restaurar se realiza en SnapCenter 4.3 y se selecciona la opción **base de datos de tenant**
- Cuando la copia de seguridad seleccionada se realiza desde una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **completar recurso**

**Single File SnapRestore se realiza en entornos SAN en las siguientes situaciones:**

- Cuando se realizan copias de seguridad en versiones anteriores a SnapCenter 4.3, y sólo si se selecciona la opción **recurso completo**
- Cuando se realizan copias de seguridad en SnapCenter 4.3 y sólo si se selecciona la opción **recurso completo**
- Cuando se selecciona la copia de seguridad de una ubicación secundaria de SnapMirror o SnapVault y se selecciona la opción **Complete Resource**

**La restauración basada en la conexión y la copia se realiza en entornos SAN para el siguiente escenario:**

- Para MDC, cuando la copia de seguridad seleccionada para restore se realiza en SnapCenter 4.3 y se selecciona la opción **base de datos de inquilinos**

Las opciones **Complete Resource**, **Volume Revert** y **Tenant Database** están disponibles en la página Restore Scope.

### Tipos de operaciones de recuperación compatibles con las bases de datos SAP HANA

SnapCenter le permite realizar diferentes tipos de operaciones de recuperación para las bases de datos SAP HANA.

- Recupere la base de datos hasta el estado más reciente
- Recupere la base de datos hasta un momento específico

  Debe especificar la fecha y la hora de la recuperación.

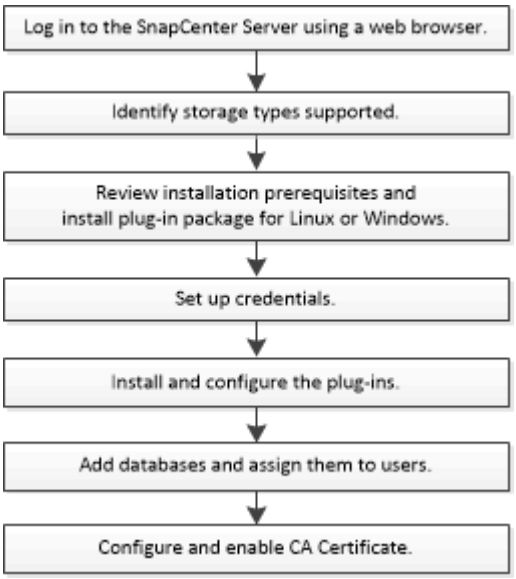
- Recuperar la base de datos hasta un backup de datos específico

SnapCenter también proporciona la opción no recovery para las bases de datos SAP HANA.

# Prepare la instalación del plugin de SnapCenter para las bases de datos SAP HANA

## Flujo de trabajo de instalación del plugin de SnapCenter para base de datos SAP HANA

Debe instalar y configurar el plugin de SnapCenter para base de datos SAP HANA si desea proteger las bases de datos SAP HANA.




## Requisitos previos para añadir hosts e instalar el plugin de SnapCenter para bases de datos SAP HANA

Antes de añadir un host e instalar los paquetes de plugins, debe cumplir con todos los requisitos. Plugin SnapCenter para base de datos SAP HANA está disponible en entornos Windows y Linux.

- Debe haber instalado Java 1.8 64 bit en su host.

  IBM Java no es compatible.

- Debe haber instalado el terminal interactivo de base de datos SAP HANA (cliente HDBSQL) en el host.
- Para Windows, el plugin Creator Service debe ejecutarse con el usuario de Windows "'LocalSystem'", que es el comportamiento predeterminado cuando el plugin para base de datos SAP HANA se instala como administrador de dominio.

- Para Windows, se deben crear claves de almacenamiento como usuario SYSTEM.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está integrada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host. El plugin de SnapCenter para Microsoft Windows se pondrá en marcha de forma predeterminada con el plugin de SAP HANA en hosts Windows.
- Para host Linux, se accede a las claves de almacenamiento de usuario seguro HDB como usuario de sistema operativo HDBSQL.
- El servidor de SnapCenter debe tener acceso al puerto 8145 o un puerto personalizado de plugin para el host de base de datos SAP HANA.

**Host Windows**

- Debe tener un usuario de dominio con privilegios de administrador local y permisos locales para iniciar sesión en el host remoto.
- Cuando se instala el plugin para base de datos SAP HANA en un host Windows, el plugin de SnapCenter para Microsoft Windows se instala automáticamente.
- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 1.8 64 bit en su host de Windows.

  "Descargas de Java para todos los sistemas operativos"

  "Herramienta de matriz de interoperabilidad de NetApp"

**Hosts Linux**

- Debe haber habilitado la conexión SSH por contraseña para el usuario raíz o no raíz.
- Debe haber instalado Java 1.8 64 bit en su host Linux.

  "Descargas de Java para todos los sistemas operativos"

  "Herramienta de matriz de interoperabilidad de NetApp"

- Para bases de datos SAP HANA que se ejecutan en un host Linux, mientras se instala el plugin para base de datos SAP HANA, el plugin de SnapCenter para UNIX se instala automáticamente.

## 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<br><br>Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". |

| Elemento | Requisitos |
| --- | --- |
| RAM mínima para el plugin de SnapCenter en el host | 1 GB |
| Espacio de registro e instalación mínimo para el plugin de SnapCenter en el host | 5 GB<br>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<br>• Windows Management Framework (WMF) 4.0 o posterior<br>• PowerShell 4.0 o posterior<br>Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp".<br>Para obtener información específica sobre la solución de problemas de .NET, consulte "La actualización o instalación de SnapCenter falla en sistemas heredados que no tienen conexión a Internet." |

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

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

| Elemento | Requisitos |
| --- | --- |
| Sistemas operativos | • Red Hat Enterprise Linux<br>• SUSE Linux Enterprise Server (SLES)<br>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 | 2 GB<br><br>Debe asignar el espacio en disco suficiente y supervisar el consumo de almacenamiento en la carpeta de registros. El espacio de registro necesario varía, según la cantidad de entidades que se han de proteger y la frecuencia de las operaciones de protección de datos. Si no hay espacio en disco suficiente, no se crearán registros de las operaciones ejecutadas recientemente. |
| Paquetes de software obligatorios | Tipos Java 1.8.x (64 bits)Oracle Java y OpenJDK<br><br>Si ha actualizado JAVA a la versión más reciente, debe asegurarse de que la opción JAVA_HOME ubicada en /var/opt/snapcenter/spl/etc/spl.properties esté configurada en la versión DE JAVA correcta y en la ruta de acceso correcta.<br><br>Para obtener la información más reciente sobre las versiones compatibles, consulte "Herramienta de matriz de interoperabilidad de NetApp". |

## Credenciales de configuración del plugin de SnapCenter para la base de datos SAP HANA

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.

### Acerca de esta tarea

- Hosts Linux

  Debe configurar credenciales para instalar plugins en hosts Linux.

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

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

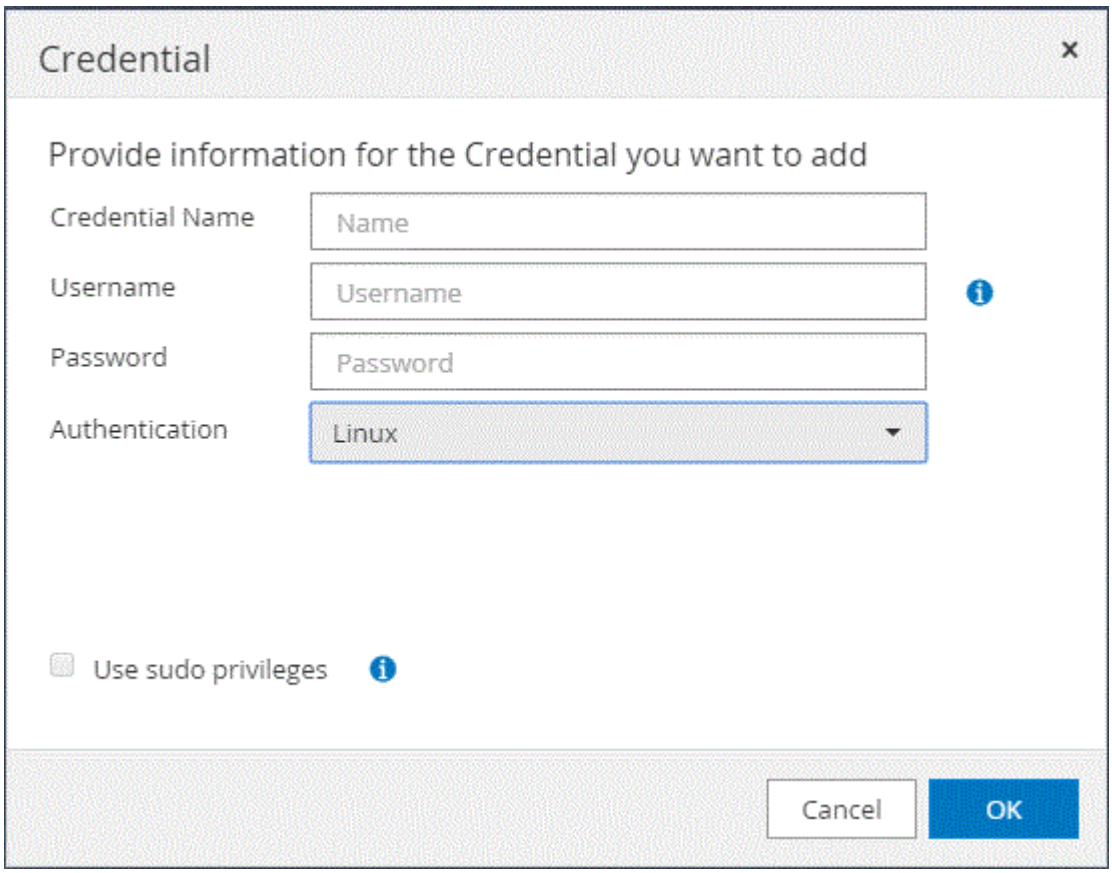
- Host Windows

Debe configurar credenciales de Windows antes de instalar plugins.

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

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

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Settings, haga clic en **Credential**.
  3. Haga clic en **Nuevo**.




  4. En la página Credential, especifique la información necesaria para configurar las credenciales:

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

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre de usuario | Introduzca el nombre de usuario y la contraseña que se utilizarán para la autenticación.<br><br>• Administrador de dominio o cualquier miembro del grupo de administradores<br><br>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:<br><br>◦ *NetBIOS\Username*<br>◦ *Domain FQDN\Username*<br><br>• Administrador local (sólo para grupos de trabajo)<br><br>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*<br><br>No utilice comillas dobles (") ni marcas de retroceso (') en las contraseñas. No debe usar el signo menos de (<) y el signo de exclamación (!) los símbolos juntos en las contraseñas. Por ejemplo, arrendhan<!10, les10<!, backtick'12. |
| Contraseña | Introduzca la contraseña usada para autenticación. |
| Modo de autenticación | Seleccione el modo de autenticación que desea utilizar. |
| Use privilegios sudo | Seleccione la casilla de verificación **Use sudo Privileges** si va a crear credenciales para usuarios que no son raíz.<br><br>Aplicable únicamente a usuarios Linux. |

5. Haga clic en **Aceptar**.

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

## Configurar GMSA en Windows Server 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.

**Lo que necesitará**

- 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>`

   1. Asigne los privilegios administrativos al GMSA configurado en el host.
   2. 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 base de datos SAP HANA

### Añada hosts e instale paquetes de plugins en hosts remotos

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

#### Lo que necesitará

- Debe ser un usuario al que se ha asignado una función que tenga permisos de instalación y desinstalación de plugins, como el rol de administrador de SnapCenter.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está incorporada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.
- Debe asegurarse de que el servicio de cola de mensajes está en ejecución.
- La documentación de administración contiene información sobre la gestión de los hosts.

- Si está utilizando la cuenta de servicio gestionado en grupo (GMSA), debe configurar GMSA con privilegios administrativos.

  "Configure la cuenta de servicio gestionado de grupo en Windows Server 2012 o posterior para SAP HANA"

**Acerca de esta tarea**

- No es posible añadir un servidor SnapCenter como host de plugins a otro servidor SnapCenter.
- Para que la replicación de sistemas SAP HANA detecte recursos en los sistemas primarios y secundarios, se recomienda añadir los sistemas primario y secundario mediante el usuario root o sudo.
- Pasos*

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

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

| 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.<br><br>Puede ver detalles sobre las credenciales colocando el cursor sobre el nombre de las credenciales que ha proporcionado.<br><br>El modo de autenticación de las credenciales se determina por el tipo de host que especifique en el asistente Add host. |

5. En la sección Select Plug-ins to Install, seleccione los plugins que desea instalar.
6. (Opcional) haga clic en **más opciones**.

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Puerto | Conserve el número de puerto predeterminado o especifique el número de puerto. El número de puerto predeterminado es 8145. Si el servidor SnapCenter se instaló en un puerto personalizado, ese número de puerto se mostrará como el puerto predeterminado.<br><br>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 | El plugin para SAP HANA está instalado en el host de cliente de HDBSQL, y este host puede estar en un sistema Windows o Linux.<br><br>• En el caso del paquete de plugins de SnapCenter para Windows, la ruta predeterminada es C:\Program Files\NetApp\SnapCenter. Opcionalmente, puede personalizar la ruta.<br>• Para el paquete de plugins de SnapCenter para Linux, la ruta predeterminada es /opt/NetApp/snapcenter. Opcionalmente, puede personalizar la ruta. |

| 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 | En el caso de host de Windows, seleccione esta casilla de comprobación si desea utilizar una cuenta de servicio gestionado de grupo (GMSA) para ejecutar los servicios de plugin.<br>Proporcione el nombre de GMSA con el siguiente formato: Nombre_de_dominio\accountName$.<br>GMSA se utilizará como cuenta de servicio de inicio de sesión solo en el complemento SnapCenter para el servicio de Windows. |

7. Haga clic en **Enviar**.

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

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

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

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

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

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

1. Supervise el progreso de la instalación.

   Los archivos de registro específicos de la instalación están en /custom_location/snapcenter/logs.

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

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

#### Lo que necesitará

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

- Pasos*

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

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

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

  1. Introduzca sus credenciales para la instalación remota.

### Instale el plugin de SnapCenter para base de datos SAP HANA en hosts Linux mediante la interfaz de la línea de comandos

Debe instalar el plugin de SnapCenter para base de datos SAP HANA mediante la interfaz de usuario de SnapCenter. Si el entorno no permite la instalación remota del plugin desde la interfaz de usuario de SnapCenter, puede instalar el plugin para base de datos SAP HANA en el modo de consola o en el modo silencioso mediante la interfaz de línea de comandos (CLI).

#### Lo que necesitará

- Debe instalar el plugin para base de datos SAP HANA en cada host Linux en el que resida el cliente HDBSQL.
- El host Linux en el que se instala el plugin de SnapCenter para base de datos SAP HANA debe cumplir con los requisitos dependientes de software, base de datos y sistema operativo.

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

  "Herramienta de matriz de interoperabilidad de NetApp"

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

- Pasos*

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

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

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

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

1. Edite el archivo /<installation directory>/NetApp/snapcenter/scc/etc/SC_SMS_Services.properties y añada el parámetro PLUGINS_ENABLED = hana:3.0.
2. Añada el host al servidor de SnapCenter con el cmdlet Add-Smhost y los parámetros requeridos.

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

**Supervise el estado de la instalación del plugin para SAP HANA**

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 **Jobs**.
  3. En la página Jobs, para filtrar la lista de modo que solo se incluyan las operaciones de instalación de plugins, proceda como sigue:
     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.

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"
```

**Configure el certificado de CA para el servicio de plugins SAP HANA de SnapCenter en el host Linux**

## Debe gestionar la contraseña del almacén de claves de plugins personalizados y su certificado, configurar el certificado de CA, configurar los certificados intermedios o raíz

para el almacén de confianza de los plugins personalizados, y configurar la pareja de claves firmadas de CA como almacén de confianza de plugins personalizados con el servicio de plugins personalizados de SnapCenter para activar el certificado digital instalado.

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

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

- Pasos*

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

   Es el valor correspondiente a la clave 'KEYSTORE_PASS'.

2. Cambie la contraseña del almacén de claves:

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

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

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

3. Reinicie el servicio después de cambiar la contraseña.

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

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

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

- Pasos*

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

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

4. Añada un certificado raíz o intermedio:

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

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

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

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

- Pasos*

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

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

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

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

5. Enumere los certificados añadidos al almacén de claves.

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

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

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

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

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

Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

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

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

**Acerca de esta tarea**

- Los complementos personalizados de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado de los archivos CRL de los plugins personalizados de SnapCenter es ' opt/NetApp/snapcenter/scc/etc/crl'.
- Pasos*
  1. Puede modificar y actualizar el directorio predeterminado del archivo agent.properties en función de la CLAVE CRL_PATH.

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

### Configure el certificado de CA para el servicio de plugins SAP HANA de SnapCenter en el host Windows

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

Los plugins personalizados utilizan el archivo *keystore.jks*, que se encuentra en *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*, tanto como su almacén de confianza como su almacén de claves.

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

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

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

2. Cambie la contraseña del almacén de claves:

   *keytool -storepasswd -keystore.jks*

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

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

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

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

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

1. Reinicie el servicio después de cambiar la contraseña.

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

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

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

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

     *keytool -list -v -keystore.jks*

  4. Añada un certificado raíz o intermedio:

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

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

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

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

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

- Pasos*

  1. Desplácese hasta la carpeta que contiene el almacén de claves del plugin personalizado *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*

2. Busque el archivo *keystore.jks*.
3. Enumere los certificados añadidos al almacén de claves:

   *keytool -list -v -keystore.jks*

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

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

5. Enumere los certificados añadidos al almacén de claves.

   *keytool -list -v -keystore.jks*

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

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

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

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

   Actualice este valor con la clave SCC_CERTIFICATE_ALIAS.

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

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

### Acerca de esta tarea

- Para descargar el último archivo CRL del certificado de CA relacionado, consulte "Cómo actualizar el archivo de lista de revocación de certificados en el certificado de CA de SnapCenter".
- Los complementos personalizados de SnapCenter buscarán los archivos CRL en un directorio preconfigurado.
- El directorio predeterminado de los archivos CRL de los plugins personalizados de SnapCenter es *'C:\Archivos de programa\NetApp\SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.
- Pasos*
  1. Puede modificar y actualizar el directorio predeterminado del archivo *agent.properties* en función de la CLAVE CRL_PATH.
  2. Puede colocar más de un archivo CRL en este directorio.

     Los certificados entrantes se verificarán en cada CRL.

### Habilite certificados de CA para plugins

Debe configurar los certificados de CA e implementar los certificados de CA en

SnapCenter Server y los hosts de plugin correspondientes. Debe habilitar la validación de certificado de CA para los plugins.

**Lo que necesitará**

- 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.

# 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 usar el plugin de SnapCenter para base de datos SAP HANA

Antes de utilizar el plugin de SnapCenter para base de datos SAP HANA, el administrador de SnapCenter debe instalar y configurar SnapCenter Server y realizar las tareas de requisitos previos.

- Instalar y configurar SnapCenter Server.
- Inicie sesión en el servidor SnapCenter.
- Configure el entorno de SnapCenter añadiendo conexiones con el sistema de almacenamiento y creando credenciales, si es necesario.
- Instale Java 1.7 o Java 1.8 en su host Linux o Windows.

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

- Configure SnapMirror y SnapVault si quiere realizar una replicación de backup.
- Instale el cliente HDBSQL en el host donde va a instalar el plugin para base de datos SAP HANA.

  Configure las claves de almacenamiento de usuario para los nodos SAP HANA que va a gestionar a través de este host.

- En el caso de la base de datos SAP HANA 2.0SPS05, si va a utilizar una cuenta de usuario de base de datos SAP HANA, asegúrese de tener los siguientes permisos para realizar operaciones de backup, restauración y clonado en SnapCenter Server:
  - Administrador de backups
  - Catálogo leído
  - Administrador de backup de bases de datos
  - Operador de recuperación de bases de datos

## Cómo se utilizan los recursos, los grupos de recursos y las políticas para proteger bases de datos SAP HANA

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

- Los recursos normalmente son bases de datos SAP HANA que se clonan o se incluyen en un backup mediante SnapCenter.
- Un grupo de recursos de SnapCenter es una agrupacion de recursos en un host.

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

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

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

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

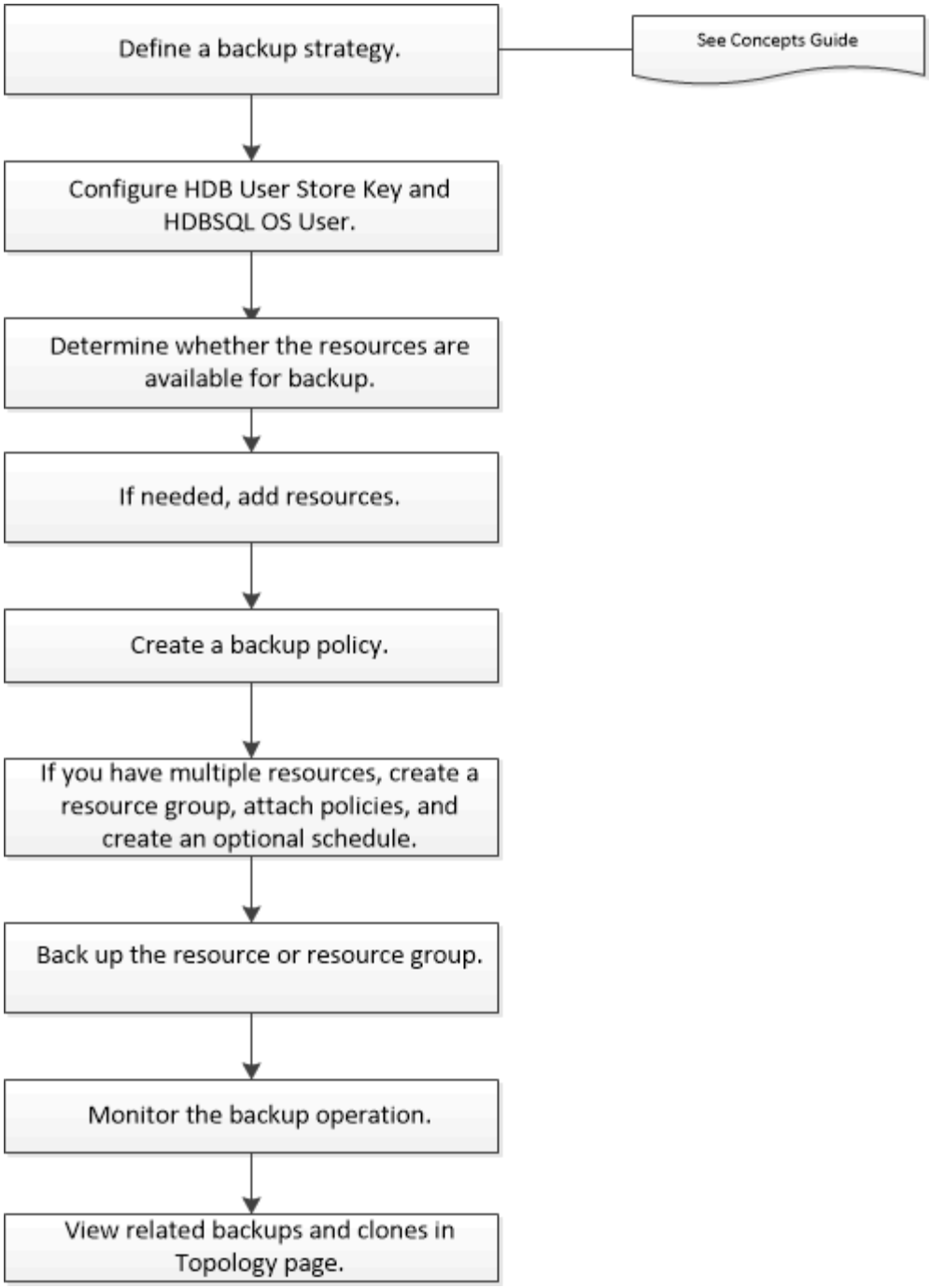
Un grupo de recursos se encarga de definir qué se desea proteger y cuándo se quiere proteger en términos de día y hora. Una política se encarga de definir cómo se aplica la protección. Si realiza backups de bases de datos, por ejemplo, puede crear un grupo de recursos que incluya todas las bases de datos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

# Realice un backup de los recursos de SAP HANA

## Realice un backup de los recursos de SAP HANA

Es posible crear un backup de un recurso (base de datos) o un grupo de recursos. El flujo de trabajo de backup incluye planificar, identificar las bases de datos para backup, gestionar las políticas de backup, crear grupos de recursos y adjuntar políticas, crear backups y supervisar las operaciones.

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




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

## Configure la clave de almacenamiento de usuario HDB y el usuario del sistema operativo HDBSQL para la base de datos SAP HANA

Debe configurar la clave de almacenamiento de usuario HDB y el usuario del sistema operativo HDBSQL para realizar operaciones de protección de datos en bases de datos SAP HANA.

**Lo que necesitará**

- Si la base de datos SAP HANA no tiene la clave de almacenamiento de usuario seguro HDB y el usuario de sistema operativo SQL HDB configurados, aparece un icono de candado rojo solo para los recursos detectados automáticamente. Si durante una operación de detección posterior, se encontró que la clave de almacenamiento de usuario seguro HDB configurada era incorrecta o no proveía acceso a la base de datos, entonces el icono de candado rojo volverá a aparecer.
- Es necesario configurar la clave de almacenamiento de usuario seguro HDB y el usuario del sistema operativo HDB SQL para proteger la base de datos, o bien añadirla a un grupo de recursos para realizar operaciones de protección de datos.
- Debe configurar HDB SQL OS User para acceder a la base de datos del sistema. Si HDB SQL OS User está configurado para acceder solo a la base de datos de tenant, se producirá un error en la operación de detección.
- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Resources** y seleccione SnapCenter Plug-in for SAP HANA Database en la lista.
  2. En la página Resources, seleccione el tipo de recurso en la lista **View**.
  3. (Opcional) Haga clic en y seleccione el nombre de host.

     A continuación, puede hacer clic en para cerrar el panel de filtros.
  4. Seleccione la base de datos y, a continuación, haga clic en **Configurar base de datos**.
  5. En la sección Configure database settings, introduzca una clave de almacenamiento de usuario seguro HDB.

     Se muestra el nombre de host del plugin y el usuario de sistema operativo SQL HDB se rellena automáticamente a <sid>-.
  6. Haga clic en **Aceptar**.

La configuración de la base de datos se puede modificar desde la página Topology.

## Descubra recursos y prepare contenedores de bases de datos multitenant para la protección de datos

### Detectar las bases de datos automáticamente

Los recursos son bases de datos de SAP HANA y volumen de datos no data en el host Linux que gestiona SnapCenter. Puede añadir estos recursos a grupos de recursos para realizar operaciones de protección de datos después de detectar las bases de datos SAP HANA disponibles.

### Lo que necesitará

- Debe haber completado ciertas tareas, como instalar el servidor SnapCenter, añadir una clave de almacenamiento de usuario HDB, añadir hosts y configurar las conexiones del sistema de almacenamiento.
- Debe haber configurado la clave de almacenamiento de usuario seguro HDB y el usuario sistema operativo HDB SQL en el host Linux.
  - Debe configurar la clave de almacenamiento de usuario HDB con el usuario SID adm. Por ejemplo, para el sistema HANA con A22 como SID, la clave de almacenamiento de usuario HDB debe

configurarse con a22adm.

- El plugin de SnapCenter para base de datos SAP HANA no es compatible con la detección automática de los recursos que residen en entornos virtuales RDM/VMDK. Debe proporcionar la información de almacenamiento para entornos virtuales al mismo tiempo que añade las bases de datos de forma manual.

**Acerca de esta tarea**

Después de instalar el plugin, todos los recursos en ese host Linux se detectan de forma automática y se muestran en la página Resources.

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

- Pasos*

1. En el panel de navegación de la izquierda, haga clic en **Resources** y seleccione el plugin para base de datos de SAP HANA en la lista.
2. En la página Resources, seleccione el tipo de recurso en la lista View.
3. (Opcional) Haga clic en y seleccione el nombre de host.

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

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

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

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

Si la base de datos SAP HANA no tiene una clave de almacenamiento de usuario seguro HDB configurada, aparece un icono de candado rojo junto al recurso. Si durante una operación de detección posterior, se encontró que la clave de almacenamiento de usuario seguro HDB configurada era incorrecta o no proveía acceso a la base de datos, entonces el icono de candado rojo volverá a aparecer.

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

**Después de terminar**

Es necesario configurar la clave de almacenamiento de usuario seguro HDB y el usuario del sistema operativo HDBSQL para proteger la base de datos o añadirla al grupo de recursos para realizar operaciones de protección de datos.

"Configure la clave de almacenamiento de usuario HDB y el usuario del sistema operativo HDBSQL para la base de datos SAP HANA"

**Prepare contenedores de bases de datos multitenant para la protección de datos**

Para los hosts SAP HANA registrados directamente en SnapCenter, instalar o actualizar el plugin de SnapCenter para base de datos SAP HANA dará lugar a una detección automática de los recursos en el host. Después de instalar o actualizar el plugin, para cada recurso de contenedores de bases de datos multitenant (MDC) que se encontraba en el host del plugin, otro recurso de MDC se descubre automáticamente con un formato GUID diferente y se registra en SnapCenter. El nuevo recurso se encontrará en el estado «bloqueado».

**Acerca de esta tarea**

Por ejemplo, en SnapCenter 4.2, si el recurso de E90 MDC se encuentra en el host del plugin y se registró manualmente, después de actualizar a SnapCenter 4.3, se detecta otro recurso de E90 MDC con un GUID diferente y se registra en SnapCenter.

> Los backups asociados con el recurso de SnapCenter 4.2 y las versiones anteriores deben conservarse hasta que finalice el período de retención. Después de que caduque el período de retención, puede eliminar el recurso de MDC antiguo y continuar gestionando el nuevo recurso de MDC detectado automáticamente.

`Old MDC resource` Es el recurso MDC para un host de plugins que se añadió manualmente en SnapCenter 4.2 o versiones anteriores.

Ejecute los siguientes pasos para empezar a utilizar el nuevo recurso detectado en SnapCenter 4.3 para las operaciones de protección de datos:

- Pasos*
  1. En la página Resources, seleccione el antiguo recurso MDC con copias de seguridad añadidas a la versión anterior de SnapCenter, y colóquelo en "modo de mantenimiento" de la página Topology.

     Si el recurso forma parte de un grupo de recursos, coloque al grupo de recursos en «modo de mantenimiento».

  2. Configure el nuevo recurso MDC detectado después de actualizar a SnapCenter 4.3. Para ello, seleccione el nuevo recurso de la página Resources.

     "'Nuevo recurso MDC'" es el recurso de MDC recientemente descubierto que se descubrió una vez que el servidor SnapCenter y el host del plugin se actualizaron a 4.3. El nuevo recurso MDC puede identificarse como un recurso con el mismo SID que el recurso MDC anterior, para un host dado, y con un icono de candado rojo junto a él en la página Resources.

  3. Proteja el nuevo recurso MDC detectado después de actualizar a SnapCenter 4.3. Para ello, seleccione políticas de protección, programaciones y configuraciones de notificaciones.
  4. Elimine los backups realizados en SnapCenter 4.2 o versiones anteriores según la configuración de retención.
  5. Elimine el grupo de recursos en la página Topology.
  6. Elimine el recurso MDC antiguo de la página Resources.

     Por ejemplo, si el período de retención de las copias de Snapshot primarias es de 7 días y la retención de copias de Snapshot secundarias es de 45 días, después de completar 45 días y después de

eliminar todos los backups, debe eliminar el grupo de recursos y el recurso MDC antiguo.

**Más información**

"Configure la clave de almacenamiento de usuario HDB y el usuario del sistema operativo HDBSQL para la base de datos SAP HANA"

"Consulte los backups y los clones de la base de datos SAP HANA en la página Topology"

## Añada recursos manualmente al host del plugin

La detección automática no es compatible con determinadas instancias de HANA. Debe añadir estos recursos manualmente.

**Lo que necesitará**

- Debe haber completado ciertas tareas, como instalar el servidor SnapCenter, añadir hosts, configurar conexiones del sistema de almacenamiento y añadir una clave de almacenamiento de usuario HDB.
- Para la replicación del sistema SAP HANA, se recomienda añadir todos los recursos de ese sistema HANA a un grupo de recursos y realizar un backup de grupo de recursos. Esto garantiza una copia de seguridad sin problemas durante el modo de recuperación tras fallos.

"Crear grupos de recursos y añadir políticas".

**Acerca de esta tarea**

La detección automática no es compatible con las siguientes configuraciones:

- Distribución con RDM y VMDK

  Si se detectan los recursos anteriores, las operaciones de protección de datos no son compatibles con estos recursos.

- Configuración de varios hosts DE HANA
- Varias instancias en el mismo host
- Escalado horizontal de varios niveles replicación de sistemas HANA
- Entorno de replicación en cascada en modo de replicación de sistemas
- Pasos*

  1. En el panel de navegación de la izquierda, seleccione el plugin de SnapCenter para base de datos SAP HANA en la lista desplegable y, a continuación, haga clic en **Resources**.
  2. En la página Resources, haga clic en **Add SAP HANA Database**.
  3. En la página Provide Resource Details, realice las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Tipo de recurso | Introduzca el tipo de recurso. Los tipos de recurso son Single Container, Multitenant Database Container (MDC) y Non-data Volume. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre del sistema HANA | Introduzca el nombre descriptivo del sistema SAP HANA. Esta opción solo está disponible si seleccionó los tipos de recursos Single Container o MDC. |
| SID | Introduzca el ID del sistema (SID). El sistema SAP HANA instalado se identifica por un SID exclusivo. |
| Host de plugin | Seleccione el host del plugin. |
| Claves de almacenamiento de usuario seguras HDB | Introduzca la clave para conectarse al sistema SAP HANA.<br><br>La clave contiene la información de inicio de sesión para conectarse a la base de datos.<br><br>Para la replicación de sistemas SAP HANA, la clave de usuario secundario no está validada. Esto se utilizará durante la toma de control. |
| Usuario de sistema operativo de HDBSQL | Introduzca el nombre de usuario para el que se configuró la clave de almacenamiento de usuario seguro HDB. Para Windows, es obligatorio que el usuario de sistema operativo de HDBSQL sea el usuario SISTEMA. Por lo tanto, debe configurar la clave de almacenamiento de usuario seguro HDB para el usuario SISTEMA. |

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

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

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

   Las bases de datos se muestran junto con información como el SID, host del plugin, políticas y grupos de recursos asociados, y el estado general

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

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

Después de añadir las bases de datos, puede modificar los detalles de la base de datos SAP HANA.

No puede modificar la siguiente información si hay backups asociados con el recurso SAP HANA:

- Contenedores de bases de datos multitenant (MDC): SID o host de HDBSQL Client (plugin)
- Contenedor único: Host de SID o cliente de HDBSQL (plugin)
- Volumen sin datos: Nombre del recurso, SID asociado o host del plugin

## Crear políticas de backup para bases de datos SAP HANA

Antes de usar SnapCenter para realizar un backup de los recursos de la base de datos SAP HANA, debe crear una política de backup para el recurso o grupo de recursos que desea incluir en el backup. Una política de backup es un conjunto de reglas que rigen cómo gestionar, programar y retener backups.

**Lo que necesitará**

- Debe tener definida una estrategia de backup.

  Para obtener más detalles, consulte cómo definir una estrategia de protección de datos para las bases de datos SAP HANA.

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

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

**Acerca de esta tarea**

- Replicación de sistemas SAP HANA
  - Puede proteger el sistema SAP HANA principal y llevar a cabo todas las operaciones de protección de datos.
  - Puede proteger el sistema SAP HANA secundario, pero no es posible crear los backups.

    Tras la conmutación al respaldo, toda la operación de protección de datos se puede realizar mientras el sistema SAP HANA secundario se convierte en el sistema SAP HANA principal.

  No puede crear un backup para el volumen de datos SAP HANA, pero SnapCenter sigue protegiendo los volúmenes no data (NDV).

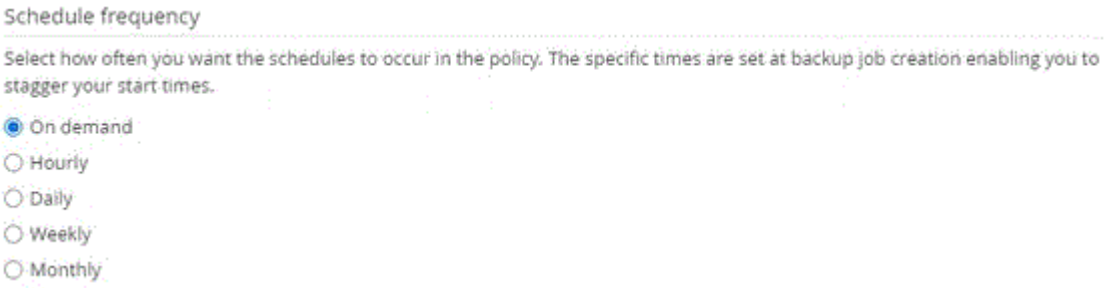
- Pasos*

  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página Configuración, haga clic en **Directivas**.
  3. Haga clic en **Nuevo**.
  4. En la página Name, escriba el nombre de la política y una descripción.
  5. En la página Settings, realice los siguientes pasos:
     - Elija el tipo de backup:

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Realice una comprobación de integridad de la base de datos | Seleccione **copia de seguridad basada en archivos**. Solo se realiza un backup de los inquilinos activos. |
| Crear un backup mediante la tecnología de copia de Snapshot | Seleccione **Snapshot Based**. |

- Especifique el tipo de programa seleccionando **a petición**, **hora**, **Diario**, **Semanal** o **Mensual**.

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




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

◦ En la sección **Configuración de copia de seguridad personalizada**, proporcione cualquier configuración de copia de seguridad específica que tenga que pasarse al plugin en formato de clave-valor.

Puede pasar varios pares de clave-valor al plugin.

1. En la página Retention, especifique la configuración de retención para el tipo de backup y el tipo de programación seleccionados en la página Backup Type:

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Conservar una cierta cantidad de copias de Snapshot | Seleccione **total Snapshot copies to keep** y, a continuación, especifique el número de copias Snapshot que desea conservar.<br><br>Si la cantidad de copias de Snapshot supera el número especificado, las copias se eliminan empezando por las más antiguas.<br><br>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.<br><br>Para los backups basados en copias de Snapshot, debe establecer el número de retención en 2 o más si va a habilitar la replicación de SnapVault. Si establece el número de retención en 1, la operación puede generar un error, ya que la primera copia de Snapshot es la de referencia para la relación de SnapVault hasta que se replica una nueva copia de Snapshot en el destino.<br><br>Para la replicación de sistemas SAP HANA, se recomienda añadir todos los recursos del sistema SAP HANA a un grupo de recursos. De este modo se garantiza la conservación de la cantidad adecuada de backups. |

| Si desea… | Realice lo siguiente… |
| --- | --- |
| Conserve las copias de Snapshot por una cierta cantidad de días | Seleccione **mantener copias Snapshot para** y, a continuación, especifique el número de días durante los que desea conservar las copias Snapshot antes de eliminarlas. |

eliminación de la copia Snapshot más antigua se basa en que nodo se encuentra la copia Snapshot más antigua. Por

2. Para los backups basados en copias de Snapshot, especifique la configuración de replicación en la página Replication:

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| **Actualizar SnapMirror después de crear una copia Snapshot local** | Seleccione este campo para crear copias reflejadas de los conjuntos de backup en otro volumen (replicación de SnapMirror).<br><br>Si la relación de protección en ONTAP es del tipo reflejo y almacén y si selecciona solo esta opción, la copia de Snapshot creada en el origen no se transferirá al destino, pero sí aparecerá en el destino. Si esta copia de Snapshot se selecciona desde el destino para realizar una operación de restauración, entonces aparece el mensaje de error Secondary Location is not available for the selected vaulted/mirrored backup. |
| **Actualizar SnapVault después de crear una copia Snapshot local** | Seleccione esta opción para realizar una replicación de backup disco a disco (backups de SnapVault). |
| **Etiqueta de política secundaria** | Seleccione una etiqueta de Snapshot.<br><br>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.<br><br>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. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| **Número de reintentos de error** | Escriba el número máximo de intentos de replicación que se permitirán antes de que la operación se detenga. |

Debe configurar la política de retención de SnapMirror en ONTAP para el almacenamiento secundario a fin de evitar alcanzar el límite máximo de copias de Snapshot en el almacenamiento secundario.

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

## Crear grupos de recursos y añadir políticas

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

**Acerca de esta tarea**

Para crear backups de replicación del sistema SAP HANA, se recomienda añadir todos los recursos del sistema SAP HANA a un grupo de recursos. Esto garantiza una copia de seguridad sin problemas durante el modo de recuperación tras fallos.

- Pasos*

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

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Nombre | Escriba un nombre para el grupo de recursos.<br>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.<br>Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta. |

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Utilice un formato de nombre personalizado para la copia de Snapshot | Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de la copia de Snapshot.<br><br>Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot. |

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

   Esto permite filtrar información en la pantalla.

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

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

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

| Para este campo… | Realice lo siguiente… |
| --- | --- |
| Permitir que se complete la operación de snapshot del grupo de consistencia | Seleccione **Urgent**, **Medium** o **Relaxed** para especificar el tiempo de espera para completar la operación de copia snapshot.<br><br>Urgent = 5 segundos, Medium = 7 segundos y Relaxed = 20 segundos. |
| Deshabilite la sincronización WAFL | Seleccione este campo para evitar forzar un punto de coherencia de WAFL. |

+


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

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

| Parámetro | Ajuste | Descripción |
|---|---|---|
| ARCHIVE_LOG_ENABLE | (S/N) | Activa la gestión de archive log para eliminar los archive logs. |
| RETENCIÓN_LOG_ARCHIVO | número_de_días | Especifica el número de días del se conservan los registros de archivo.<br><br>Este ajuste debe ser igual o mayor que SNAPSHOT_NTAP_ RETENCIONES. |
| ARCHIVE_LOG_DIR | change_info_directory/logs | Especifica la ruta al directorio que contiene los archive logs. |

| Parámetro | Ajuste | Descripción |
|---|---|---|
| ARCHIVO_LOG_EXT | extensión_archivo | Especifica el archivo archive log longitud de extensión.<br><br>Por ejemplo, si la el archive log es backup_registro_0_0_0_0,1615 18551942 9 y si el valor file_extension es 5, a continuación, la extensión del registro será conserve 5 dígitos, que son 16151. |
| ARCHIVE_LOG_RECURSIVE_ SE ARQ | (S/N) | Permite la gestión del archivado registros dentro de subdirectorios.<br><br>Usted debe usar este parámetro si el los archive logs se encuentran en subdirectorios. |

Los pares personalizados de clave-valor son compatibles con los sistemas del plugin de SAP HANA Linux y no son compatibles con la base de datos SAP HANA registrada como un plugin de Windows centralizado.

c. Haga clic en la flecha **Snapshot Copy Tool** para seleccionar la herramienta que permite crear copias Snapshot:

| Si desea que… | Realice lo siguiente… |
|---|---|
| SnapCenter utilice el plugin para Windows y coloque el sistema de archivos en estado coherente antes de crear una copia de Snapshot. En el caso de recursos de Linux, esta opción no es aplicable. | Seleccione **SnapCenter with File System Consistency**.<br><br>Esta opción no es aplicable para el plugin de SnapCenter para la base de datos SAP HANA. |
| SnapCenter cree una copia de Snapshot en el nivel del almacenamiento | Seleccione **SnapCenter sin coherencia del sistema de archivos**. |
| Se escriba el comando que se ejecutará en el host a fin de crear copias de Snapshot. | Seleccione **otros** y, a continuación, escriba el comando que se ejecutará en el host para crear una copia Snapshot. |

7. 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 + .

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

b. En la columna Configure Schedules, haga clic en en la política que desea configurar.

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

Policy_name es el nombre de la política seleccionada.

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

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

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

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

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

## Realice un backup de las bases de datos SAP HANA

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

**Lo que necesitará**

- Debe tener creada una política de backup.
- Si desea realizar un backup de un recurso que tenga una relación de SnapMirror con un almacenamiento secundario, la función ONTAP asignada al usuario de almacenamiento debería incluir el privilegio «sinapmirror all». Sin embargo, si usted está utilizando el rol "'vsadmin'", entonces no se requiere el privilegio "nnapmirror all".
- Para realizar una operación de backup basada en copia de Snapshot, asegúrese de que todas las bases de datos de tenant sean válidas y estén activas.
- Para crear backups de replicación del sistema SAP HANA, se recomienda añadir todos los recursos del sistema SAP HANA a un grupo de recursos. Esto garantiza una copia de seguridad sin problemas durante el modo de recuperación tras fallos.

  "Crear grupos de recursos y añadir políticas".

  "Realice un backup de los grupos de recursos"

- Si desea crear un backup basado en archivos cuando una o varias bases de datos de arrendatarios están fuera de servicio, defina el parámetro ALLOW_FILE_BASED_BACKUP_IFINACTIVE_ARRENDATARIOS_PRESSE en **YES** en el archivo de propiedades de HANA mediante `Set-SmConfigSettings` cmdlet.

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

- Para los comandos previos y posteriores para la pausa, la copia de Snapshot y la reanudación de la copia, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:

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

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

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

- 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, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

   Haga clic en * * y, a continuación, seleccione el nombre de host y el tipo de recurso para filtrar los recursos. A continuación, puede hacer clic en para cerrar el panel de filtros.

3. Haga clic en el recurso que desea incluir en el backup.
4. En la página Resources, seleccione **Use custom name format for Snapshot copy** y, a continuación, escriba un 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.

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

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

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

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

   - Haga clic en la flecha **Scripts** para ejecutar comandos previos y posteriores para la pausa, la copia de Snapshot y la reanudación de la copia.

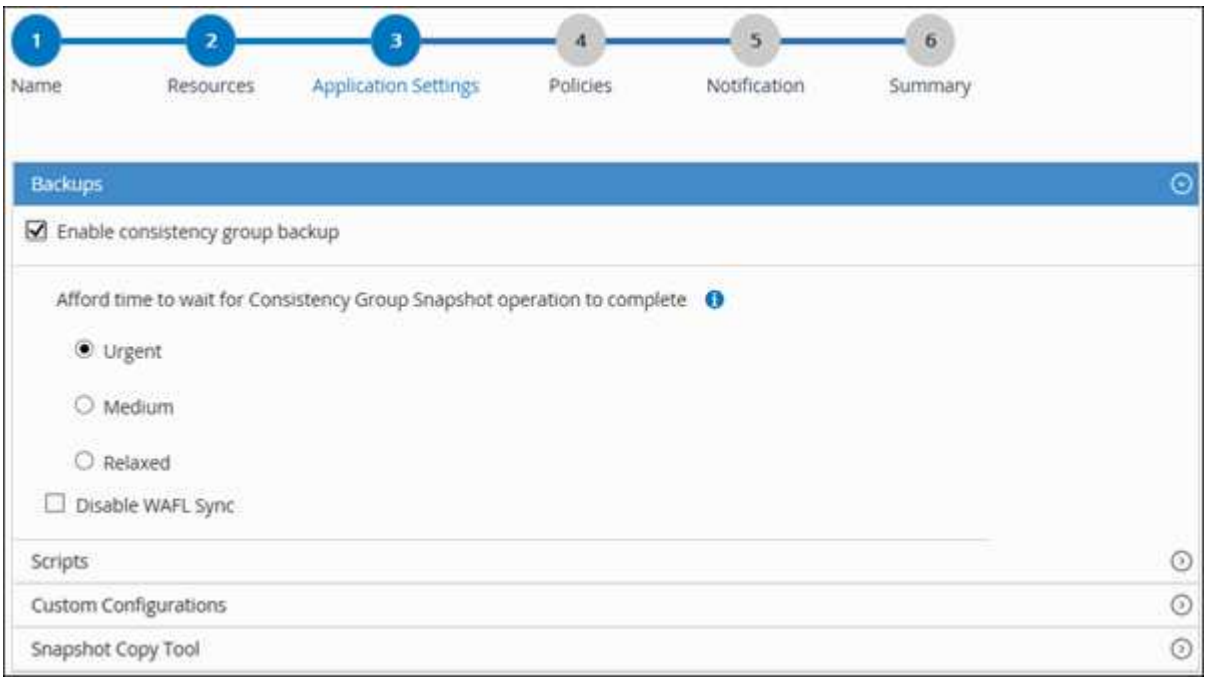
     También puede ejecutar los comandos previos antes de salir de la operación de backup. Los scripts previos y posteriores se ejecutan en el servidor de SnapCenter.

   - Haga clic en la flecha **Custom Configurations**y, a continuación, escriba las parejas de valor

personalizadas necesarias para todos los trabajos que utilicen este recurso.

- Haga clic en la flecha **Snapshot Copy Tool** para seleccionar la herramienta que permite crear copias Snapshot:

| Si desea que… | Realice lo siguiente… |
|---|---|
| SnapCenter cree una copia de Snapshot a nivel del almacenamiento | Seleccione **SnapCenter sin coherencia del sistema de archivos**. |
| SnapCenter utilice el plugin para Windows y coloque el sistema de archivos en estado coherente para luego crear una copia de Snapshot | Seleccione **SnapCenter with File System Consistency**. |
| Se escriba el comando para crear una copia de Snapshot | Seleccione **otros** y, a continuación, escriba el comando para crear una copia Snapshot. |




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.

   a. Haga clic en + * en la columna Configure Schedules correspondiente a la política para la cual desea configurar una programación.

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

*policy_name* es el nombre de la directiva seleccionada.

Las programaciones configuradas figuran en la columna Applied Schedules.

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

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

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

   Se muestra la página de topología de los recursos.

3. Haga clic en **copia de seguridad ahora**.
4. En la página Backup, realice los siguientes pasos:
   a. Si aplicó varias políticas al recurso, en la lista desplegable **Política**, seleccione la directiva que desea utilizar para la copia de seguridad.

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

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

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

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

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

## Realice un backup de los grupos de recursos

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

### Lo que necesitará

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

**Acerca de esta tarea**

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

- Pasos*
  1. En el panel de navegación de la izquierda, haga clic en **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
  2. En la página Resources, seleccione **Resource Group** en la lista **View**.

     Se puede buscar el grupo de recursos escribiendo su nombre en el cuadro de búsqueda o haciendo clic en y, luego, seleccionar la etiqueta. A continuación, puede hacer clic en para cerrar el panel de filtros.
  3. En la página Resource Groups, seleccione el grupo de recursos que desea incluir en un backup y, a continuación, haga clic en **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. Haga clic en **copia de seguridad**.
  5. Supervise el progreso de la operación haciendo clic en **Monitor** > **Jobs**.

## Cree una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para la base de datos SAP HANA

Es posible crear una conexión de máquina virtual de almacenamiento (SVM) y una credencial antes de usar cmdlets de PowerShell para realizar backup, restaurar o clonar bases de datos SAP HANA.

**Lo que necesitará**

- 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 datos única.

- Pasos*

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

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

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

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

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

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

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

4. Añada el host de comunicación de SAP HANA a servidor SnapCenter.

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

5. Instale el paquete y el plugin de SnapCenter para base de datos SAP HANA en el host.

   Para Linux:

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

   Para Windows:

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

6. Defina la ruta al cliente de HDBSQL.

   Para Windows:

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61
-PluginCode hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program
Files\sap\hdbclient\hdbsql.exe"}
```

Para Linux:

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com
-PluginCode hana -configSettings
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

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 un backup de bases de datos mediante cmdlets de PowerShell

Realizar un backup de una base de datos incluye establecer una conexión con SnapCenter Server, añadir recursos, añadir una política, crear un grupo de recursos de backup y realizar backups.

**Lo que necesitará**

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

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

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

   Se muestra una solicitud de nombre de usuario y contraseña.

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

   Este ejemplo muestra cómo añadir una base de datos SAP HANA del tipo SingleContainer:

   ```
   C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'
   -DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint
   (@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary"
   }) -SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys
   'HS10' -osdbuser 'h10adm' -filebackupprefix 'H10_'
   ```

   Este ejemplo muestra cómo añadir una base de datos SAP HANA del tipo MultipleContainers:

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType
MultipleContainers -StorageFootPrint
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.neta
pp.com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType
'MultiTenant'
```

Este ejemplo muestra cómo crear un recurso de volúmenes sin datos:

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sccore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

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

   Este ejemplo crea una política de backup para un backup basado en copias de Snapshot:

```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType Backup
-PluginPolicyType hana -BackupType SnapShotBasedBackup
```

   Este ejemplo crea una política de backup para un backup basado en archivos:

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
-PluginPolicyType hana -BackupType FileBasedBackup
```

4. Proteja el recurso o añada un nuevo grupo de recursos a SnapCenter mediante el cmdlet Add-SmResourceGroup.

   Este ejemplo protege un recurso de contenedor único:

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

   Este ejemplo protege un recurso de varios contenedores:

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="MDC\SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

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

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sccore.test.com";"Uid"="SID"},@{"Host"="scc
orelinux62.sccore.test.com";"Uid"="MDC\SID"})
  -Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency  -plugincode 'HANA'
```

Este ejemplo crea un grupo de recursos de volumen sin datos:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="H11";"PluginName"="
hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="MDC\H31";"Plug
inName"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="NonDa
taVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies
hanaprimary
```

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

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

   ```
   C:\PS> New-SMBackup -ResourceGroupName
   'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
   -Policy hana_snapshotbased
   ```

   Este ejemplo realiza un backup de un recurso protegido:

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

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

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

2. Supervise los detalles del trabajo de backup como ID de backup, nombre de backup para realizar una operación de restauración o clonado mediante el cmdlet Get-SmBackupReport.

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

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

## Supervisar las operaciones de backup

### Supervisar las operaciones de backup de las bases de datos SAP HANA

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

#### Acerca de esta tarea

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

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

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

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

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

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

#### Supervise las operaciones de protección de datos en bases de datos SAP HANA 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, se muestran sus detalles en la página Job Details.

## Cancele las operaciones de backup para SAP HANA

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

### Lo que necesitará

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

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

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

## Consulte los backups y los clones de la base de datos SAP HANA en la página Topology

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

### Acerca de esta tarea

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

- muestra la cantidad de backups y clones que están disponibles en el almacenamiento principal.
- Muestra la cantidad de backups y clones que estan copiados en el almacenamiento secundario mediante SnapMirror.
- Muestra la cantidad de backups y clones que se replican en el almacenamiento secundario mediante la tecnología SnapVault.

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

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

Para los recursos principales de replicación del sistema SAP HANA, las operaciones de restauración y eliminación son compatibles y para recursos secundarios, la operación de clonado es compatible.

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

- Pasos*

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

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

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

     La sección **Tarjeta de resumen** muestra el número total de copias de seguridad basadas en archivos, copias de seguridad de instantáneas y clones.

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

  1. 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.

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

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

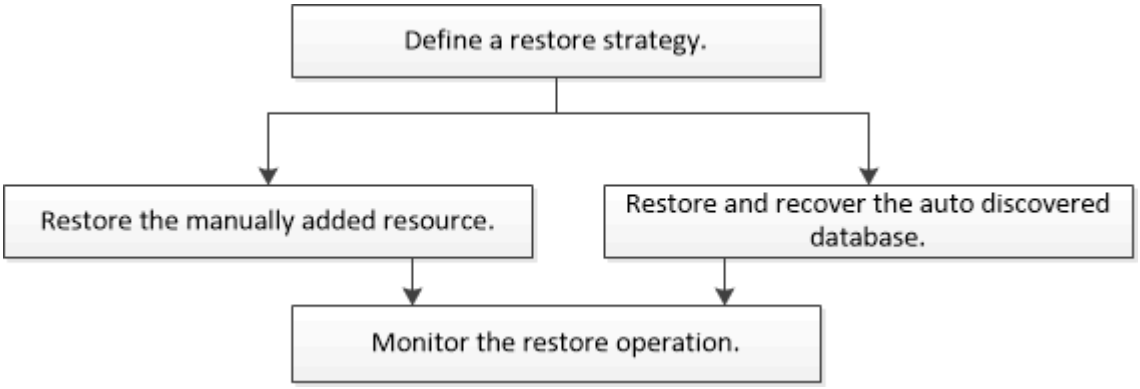
3. Si desea eliminar un clon, selecciónelo de la tabla y, a continuación, haga clic en .
4. Si desea dividir un clon, selecciónelo de la tabla y, a continuación, haga clic en .

# Restaure bases de datos de SAP HANA

## Restaure el flujo de trabajo

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

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




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

"Guía de referencia de cmdlets de SnapCenter Software".

## Restaurar y recuperar un backup de recurso añadido manualmente

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

### Lo que necesitará

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

  Para Windows: *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in*

*Creator\etc\allowed_Commands_list.txt*

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

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

**Acerca de esta tarea**

- Las copias de backup basadas de archivos no se pueden restaurar desde SnapCenter.
- Después de actualizar a SnapCenter 4.3, se pueden restaurar los backups realizados en SnapCenter 4.2, pero no se pueden recuperar. Para recuperar los backups realizados en SnapCenter 4.2, debe usar el estudio HANA o secuencias de comandos de recuperación HANA externas a SnapCenter.
- Pasos*

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

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

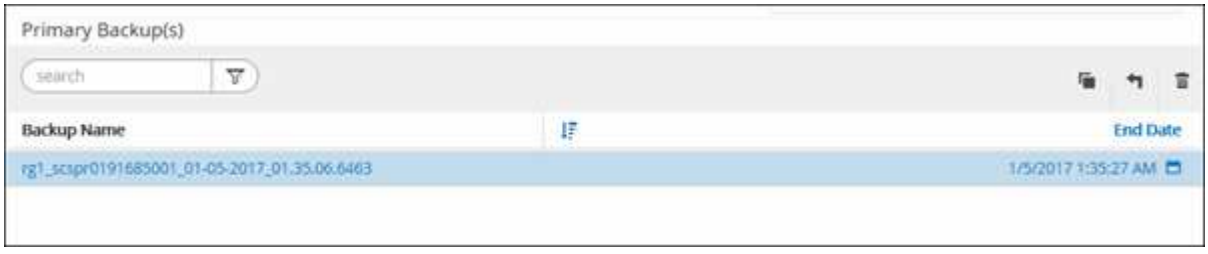
   Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

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

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

   Se muestra la página con el resumen.

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




6. En la página Restore Scope, seleccione **Complete Resource** o **File Level**.
   a. Si selecciona **Complete Resource**, se restauran todos los volúmenes de datos configurados de la base de datos SAP HANA.

      Si el recurso contiene volúmenes o qtrees, se eliminan las copias de Snapshot realizadas después de la copia de Snapshot seleccionada para restaurar en tales volúmenes o qtrees y no pueden

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

b. Si selecciona **nivel de archivo**, puede seleccionar **todo** o seleccionar los volúmenes o qtrees específicos y, a continuación, introducir la ruta relacionada con esos volúmenes o qtrees, separados por comas
   - Puede seleccionar varios volúmenes y qtrees.
   - Si el tipo de recurso es LUN, se restaura todo el LUN.

     Puede seleccionar varios LUN.

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

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

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

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

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

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

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

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

## Restaurar y recuperar un backup de base de datos detectado automáticamente

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

**Lo que necesitará**

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

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

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

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

**Acerca de esta tarea**

- Las copias de backup basadas de archivos no se pueden restaurar desde SnapCenter.
- Después de actualizar a SnapCenter 4.3, se pueden restaurar los backups realizados en SnapCenter 4.2, pero no se pueden recuperar. Para recuperar los backups realizados en SnapCenter 4.2, debe usar el estudio HANA o secuencias de comandos de recuperación HANA externas a SnapCenter.
- Pasos*

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

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

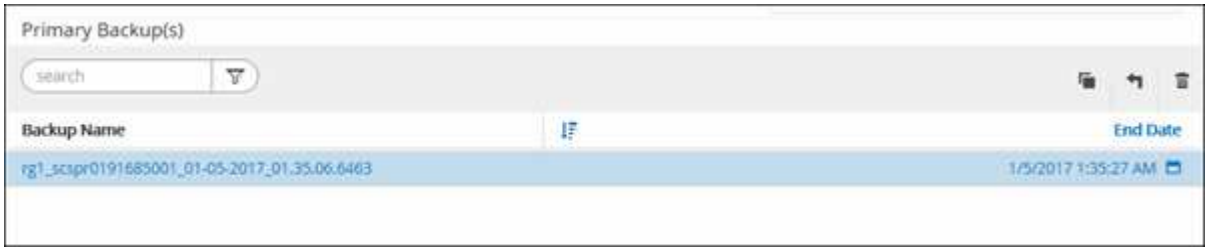
   Aunque se puede realizar un backup del grupo de recursos, al restaurar, debe seleccionar los recursos individuales que restaurará.

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

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

   Se muestra la página con el resumen.

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




6. En la página Restore Scope, seleccione **Complete Resource** para restaurar los volúmenes de datos configurados de la base de datos SAP HANA.

   Puede seleccionar **Complete Resource** (con o sin **Volume Revert**) o **Inquilino**.

   El servidor SnapCenter no admite la operación de recuperación para varios inquilinos cuando el usuario selecciona la opción **base de datos de inquilinos** o **Restaurar completa**. Debe usar HANA Studio o el script HANA python para realizar la operación de recuperación.

   a. Seleccione **revertir volumen** si desea restaurar todo el volumen.

      Esta opción está disponible para backups realizados en SnapCenter 4.3 en entornos NFS.

Si el recurso contiene volúmenes o qtrees, se eliminan las copias de Snapshot realizadas después de la copia de Snapshot seleccionada para restaurar en tales volúmenes o qtrees y no pueden recuperarse. Además, si hay algún otro recurso alojado en los mismos volúmenes o qtrees, también se lo elimina. Esto se aplica cuando se selecciona la opción **Complete Resource** with **Volume Revert** para restaurar.

b. Seleccione **base de datos de arrendatario**.

Esta opción solo está disponible para recursos MDC.

Asegúrese de detener la base de datos de tenant antes de realizar la operación de restauración.

Si selecciona la opción **base de datos de inquilino**, debe usar HANA Studio o utilizar secuencias de comandos de recuperación de HANA externas a SnapCenter para realizar la operación de recuperación.

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

| **Si…** | **Realice lo siguiente…** |
| --- | --- |
| Desea recuperar el mayor cierre posible a la hora actual | Seleccione **recuperar al estado más reciente**. Para los recursos de contenedor único, especifique una o más ubicaciones de backup de registro y catálogo.<br><br>Para los recursos de contenedor de base de datos multitenant (MDC) especifican una o varias ubicaciones de backup de registros y la ubicación del catálogo de backups.<br><br>Para los recursos del MDC, la ruta de acceso debe contener tanto registros de la base de datos del sistema como de la base de datos de tenant. |

| Si… | Realice lo siguiente… |
| --- | --- |
| Desea recuperar al punto en el tiempo especificado | Seleccione **Recover to point in time**.<br><br>a. Seleccione la zona horaria.<br><br>De forma predeterminada, la zona horaria del navegador se completa.<br><br>La zona horaria seleccionada junto con la hora de entrada se convierte en GMT absoluta.<br><br>b. Introduzca la fecha y la hora. Por ejemplo, el host Linux para HANA se encuentra en Sunnyvale, CA y el usuario en Raleigh, NC está recuperando los registros en SnapCenter.<br><br>La diferencia horaria entre ambas ubicaciones es de 3 horas, y como el usuario ha iniciado sesión en Raleigh, NC, la zona horaria predeterminada del navegador que se seleccionará en la GUI es GMT-04:00.<br><br>Si el usuario desea realizar una recuperación a 5:07 a.m .Sunnyvale, CA, el usuario debe configurar la zona horaria del navegador para la zona horaria del host Linux de HANA, que es GMT-00 y especificar la fecha y la hora como 5:00 a.m.<br><br>Para los recursos de contenedor único, especifique una o más ubicaciones de backup de registro y catálogo.<br><br>Para los recursos MDC, especifique una o más ubicaciones de backup de registros y la ubicación del catálogo de backups.<br><br>Para los recursos del MDC, la ruta de acceso debe contener tanto registros de la base de datos del sistema como de la base de datos de tenant. |
| Desea recuperar a un backup de datos específico | Seleccione **Recover to specified data backup**. |
| No desea recuperar | Seleccione **sin recuperación**. La operación de recuperación debe realizarse manualmente desde el estudio HANA. |

Solo es posible recuperar los backups que se realizan después de la actualización a SnapCenter 4.3, siempre y cuando el host y el plugin se actualicen a SnapCenter 4.3 y los backups seleccionados para

la restauración se tomen después de que el recurso se convierta o se detecte como recurso automático.

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

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

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

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

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

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

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

## Restaurar una base de datos SAP HANA mediante cmdlets de PowerShell

La restauración de un backup de base de datos SAP HANA incluye iniciar una sesión de conexión con SnapCenter Server, mostrar una lista de backups y recuperar información de los backups, así como restaurar un backup.

**Lo que necesitará**

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

   Este ejemplo muestra que hay dos backups disponibles para restaurar:

```
 PS C:\> Get-SmBackup

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

En este ejemplo, se muestra información detallada sobre el backup del 29 de enero de 2015 al 3 de febrero de 2015:

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

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

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

3. Inicie el proceso de recuperación en el estudio HANA.

   La base de datos se cierra.

4. Puede restaurar los datos del backup mediante el cmdlet Restore-SmBackup.

   > AppObjectId es "Host\Plugin\UID", donde UID = SID es para un recurso de tipo de contenedor único y UID = MDC\SID es para un recurso de varios contenedores. Puede obtener el ResourceID a partir del cmdlet Get-smResources.

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

   Este ejemplo muestra cómo restaurar la base de datos desde el almacenamiento primario:

   ```
   Restore-SmBackup -PluginCode HANA -AppObjectId
   cn24.sccore.test.com\hana\H10 -BackupId 3
   ```

   Este ejemplo muestra cómo restaurar la base de datos desde el almacenamiento secundario:

```
Restore-SmBackup -PluginCode 'HANA' -AppObjectId
cn24.sccore.test.com\hana\H10 -BackupId 399 -Confirm:$false  -Archive @(
@{"Primary"="<Primary Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
Vserver>:<SecondaryVolume>"})
```

+ Los backups estarán disponibles en el estudio HANA para recuperación.

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

## Restaurar recursos mediante los cmdlets de PowerShell

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

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

- Pasos*

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

   ```
   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
```

1. Puede restaurar los datos del backup mediante el cmdlet Restore-SmBackup.

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

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

## Supervisar las operaciones de restauración de bases de datos SAP HANA

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 **Jobs**.
3. En la página Jobs, 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.

# Clonar backups de recursos SAP HANA

## Flujo de trabajo de clonado

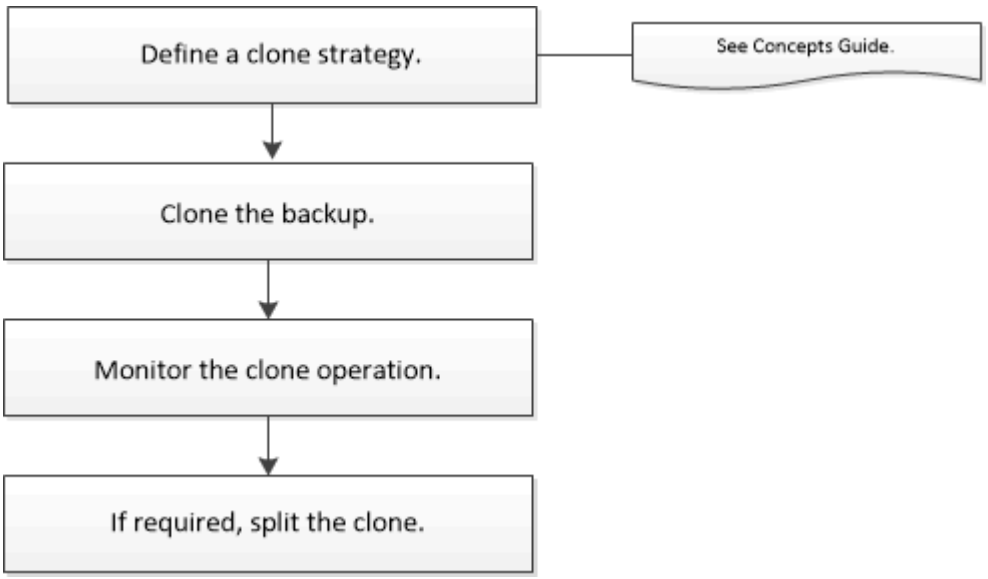
El flujo de trabajo de clonado incluye realizar la operación de clonado y supervisarla.

### Acerca de esta tarea

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

◦ Para recuperar datos que se eliminaron o se modificaron por error

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




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

## Clonar un backup de base de datos SAP HANA

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

**Lo que necesitará**

- Debe tener un backup de los recursos o del grupo de recursos.
- Debe asegurarse de que los agregados donde se alojan los volúmenes deben estar en la lista de agregados asignados de la máquina virtual de almacenamiento (SVM).
- No puede clonar backups basados en archivos.
- El servidor de clones de destino debe tener el mismo SID de instancia de SAP HANA que se proporciona en el campo SID de clon de destino.
- Para los comandos previos o posteriores a la clonado, debe comprobar si los comandos existen en la lista de comandos disponible en el host del plugin desde las rutas siguientes:

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

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

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

**Acerca de esta tarea**

Para obtener más información sobre las limitaciones de las operaciones de división de clones, consulte "Guía de gestión de almacenamiento lógico de ONTAP 9".

- Pasos*

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

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

3. Seleccione el recurso o el grupo de recursos.

   Debe seleccionar un recurso para seleccionar un grupo de recursos.

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

4. En la vista Manage Copies, seleccione **copias de seguridad** ya sea en los sistemas de almacenamiento primario o secundario (reflejado o en almacén).
5. Seleccione el backup de datos de la tabla y haga clic en .
6. En la página Location, lleve a cabo las siguientes acciones:

| Para este campo… | Realice lo siguiente… |
|---|---|
| Host de plugin | Seleccione el host en el que se debe alojar el clon y está instalado el plugin. |
| SID del clon de destino | Introduzca el ID de instancia de SAP HANA que se va a clonar desde los backups existentes. |
| Dirección IP de exportación NFS | Introduzca las direcciones IP o los nombres de host a los que se van a exportar los volúmenes clonados. |
| Iniciador iSCSI | Introduzca el nombre del iniciador de iSCSI del host al que se van a exportar los LUN. Esta opción está disponible solo si seleccionó el tipo de recurso LUN. |
| Protocolo | Introduzca el protocolo de LUN. Esta opción está disponible solo si seleccionó el tipo de recurso LUN. |

   Si el recurso seleccionado es un LUN y lo clona desde un backup secundario, entonces se enumeran los volúmenes de destino. Un único recurso puede tener varios volúmenes de destino.

   Antes de la clonado, debe asegurarse de que el iniciador de iSCSI o FCP estén presentes y estén configurados y conectados a hosts alternativos.

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

   Los scripts se ejecutan en el host del plugin.

   a. Introduzca los comandos para el clon previo o posterior que se deben ejecutar antes o después de la operación de clonado, respectivamente.
      - Comando previo a la clonado: Elimine las bases de datos existentes con el mismo nombre
      - Comando posterior a la clonado: Verifique o inicie una base de datos.
   b. Escriba el comando de montaje para montar un sistema de archivos en un host.

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

   Ejemplo para NFS:

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

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

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

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

## Clonar backups de la base de datos SAP HANA mediante cmdlets de PowerShell

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

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

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

- Pasos*

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

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

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

   Este ejemplo muestra que hay dos backups disponibles para clonar:

```
 C:\PS> Get-SmBackup

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

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

   Este ejemplo muestra que el backup que se va a clonar tiene una dirección NFSExportIPs de 10.232.206.169:

```
New-SmClone -AppPluginCode hana -BackupName
scsccore1_sccore_test_com_hana_H73_scsccore1_06-07-2017_02.54.29.3817
-Resources @{"Host"="scsccore1.sccore.test.com";"Uid"="H73"}
-CloneToInstance shivscc4.sccore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data' -preclonecreatecommands
'/home/scripts/scpre_clone.sh' -postclonecreatecommands
'/home/scripts/scpost_clone.sh'
```

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

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

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

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

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

## Supervise las operaciones de clonado de base de datos SAP HANA

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 **Jobs**.
  3. En la página Jobs, realice los siguientes pasos:

a. Haga clic en para filtrar la lista de modo que solo figuren las operaciones de clonado.
b. Especifique las fechas de inicio y finalización.
c. En la lista desplegable **Tipo**, seleccione **Clonar**.
d. En la lista desplegable **Estado**, seleccione el estado del clon.
e. Haga clic en **aplicar** para ver las operaciones que se han completado correctamente.

4. Seleccione el trabajo de clonado y, a continuación, haga clic en **Detalles** para ver los detalles del trabajo.
5. En la página Detalles del trabajo, haga clic en **Ver registros**.

## Divida un clon

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

### Acerca de esta tarea

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

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

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

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

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

| 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 Manage Copies, seleccione el recurso clonado (por ejemplo, la base de datos o el 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.

**Más información**

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

## Elimine o divida los clones de las bases de datos SAP HANA después de actualizar SnapCenter

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

**Acerca de esta tarea**

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

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

     Se muestra la página con el resumen.

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

7. Haga clic en **Aceptar**.

## 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.