Realice un backup de los recursos de SAP HANA

SnapCenter Software 4.5

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/es-es/snapcenter-45/protect-hana/task_back_up_sap_hana_resources.html on September 29, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

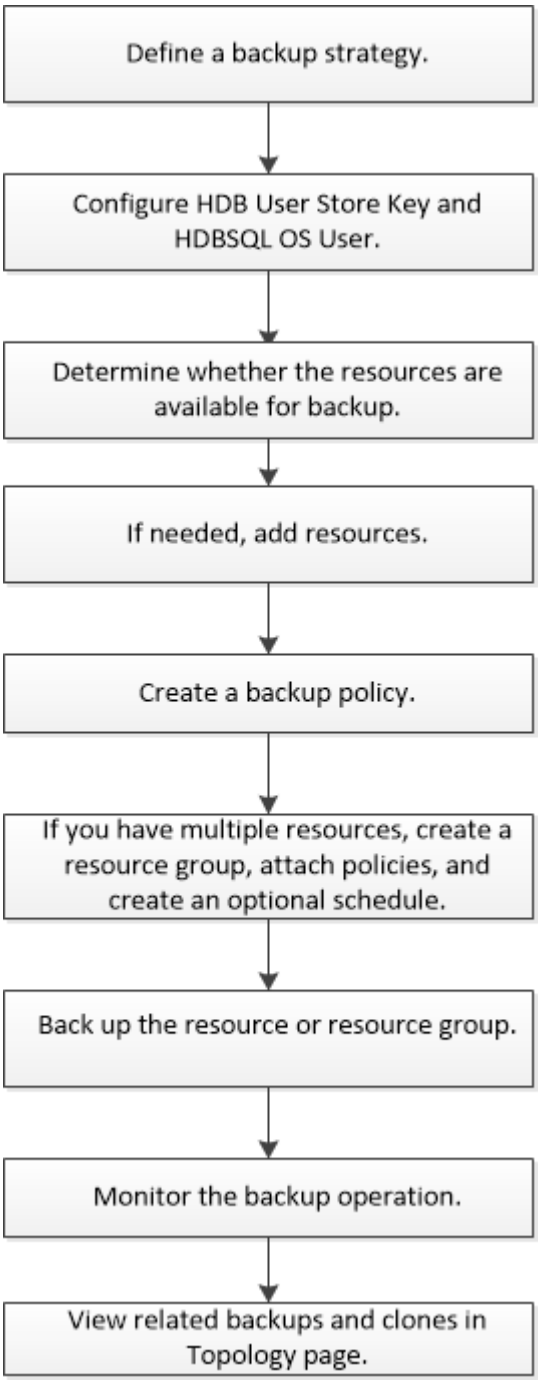
Realice un backup de los recursos de SAP HANA . . . 1
Realice un backup de los recursos de SAP HANA . . . 1
Configure la clave de almacenamiento de usuario HDB y el usuario del sistema operativo HDBSQL para la base de datos SAP HANA . . . 2
Descubra recursos y prepare contenedores de bases de datos multitenant para la protección de datos . . . 3
Detectar las bases de datos automáticamente . . . 3
Prepare contenedores de bases de datos multitenant para la protección de datos . . . 4
Añada recursos manualmente al host del plugin . . . 5
Crear políticas de backup para bases de datos SAP HANA . . . 7
Crear grupos de recursos y añadir políticas . . . 11
Realice un backup de las bases de datos SAP HANA . . . 14
Realice un backup de los grupos de recursos . . . 17
Cree una conexión del sistema de almacenamiento y una credencial mediante cmdlets de PowerShell para la base de datos SAP HANA . . . 18
Realizar un backup de bases de datos mediante cmdlets de PowerShell . . . 20
Supervisar las operaciones de backup . . . 23
Supervisar las operaciones de backup de las bases de datos SAP HANA . . . 23
Supervise las operaciones de protección de datos en bases de datos SAP HANA en el panel Activity . . . 24
Consulte los backups y los clones de la base de datos SAP HANA en la página Topology . . . 25

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.https://library.netapp.com/ecm/ecm_download_file/ECMLP2877143["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 **Recursos**, seleccione el tipo de recurso en la lista **Ver**.
  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 **Recursos**, seleccione el tipo de recurso en la lista Ver.
  3. (Opcional) haga clic en y, a continuación, seleccione el nombre de host.

     A continuación, puede hacer clic en para cerrar el panel de filtros.
  4. Haga clic en **Actualizar recursos** para descubrir los recursos disponibles en el host.

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

     - Si 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.

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 **Recursos**, 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.

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
- Replicación de sistemas HANA
- Varias instancias en el mismo host
- 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 **Recursos**, haga clic en **Agregar base de datos SAP HANA**.

3. En la página **proporcionar detalles del recurso**, 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.
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. La clave contiene la información de inicio de sesión para conectarse a la base de datos.
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.

La siguiente información no se puede modificar si el recurso SAP HANA tiene backups asociados:

- 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.

- Pasos*

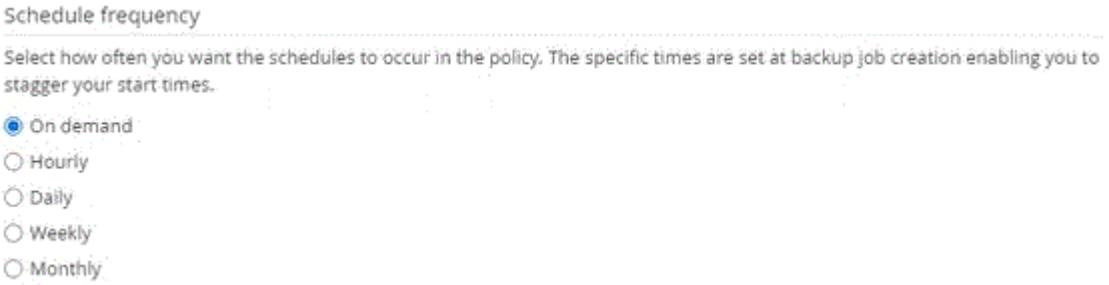
  1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
  2. En la página **Configuración**, haga clic en **Directivas**.
  3. Haga clic en **Nuevo**.
  4. En la página **Nombre**, introduzca el nombre y la descripción de la directiva.
  5. En la página **Configuración**, realice 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 copia de seguridad y el tipo de programación seleccionados en la página Tipo de copia de seguridad:

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. Si la cantidad de copias de Snapshot supera el número especificado, las copias se eliminan empezando por las más antiguas. 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. 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.
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.

2. Para las copias de seguridad basadas en copias de Snapshot, especifique la configuración de replicación en la página **replicación**:

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). 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. Según la etiqueta de copia de Snapshot que seleccione, ONTAP aplicará la política de retención de copias de Snapshot secundarias que corresponda a esa etiqueta. Si ha seleccionado **Actualizar SnapMirror después de crear una copia Snapshot local**, puede especificar opcionalmente la etiqueta de la directiva secundaria. Sin embargo, si ha seleccionado **Actualizar SnapVault después de crear una copia Snapshot local**, debe especificar la etiqueta de la directiva secundaria.
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.

- 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**, haga clic en **Nuevo grupo de recursos**.
3. En la página **Nombre**, realice las siguientes acciones:

Para este campo…	Realice lo siguiente…
Nombre	Escriba un nombre para el grupo de recursos. El nombre del grupo de recursos no debe superar los 250 caracteres.
Etiquetas	Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos. Por ejemplo, si añadió HR como etiqueta a varios grupos de recursos, más adelante encontrará todos los grupos de recursos asociados usando esa etiqueta.
Utilice un formato de nombre personalizado para la copia de Snapshot	Marque esta casilla de comprobación e introduzca un formato de nombre personalizado que desee usar para el nombre de la copia de Snapshot. Por ejemplo, customtext_resource group_policy_hostname o resource group_hostname. De forma predeterminada, se añade una fecha/hora al nombre de la copia de Snapshot.

4. En la página **Recursos**, 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.

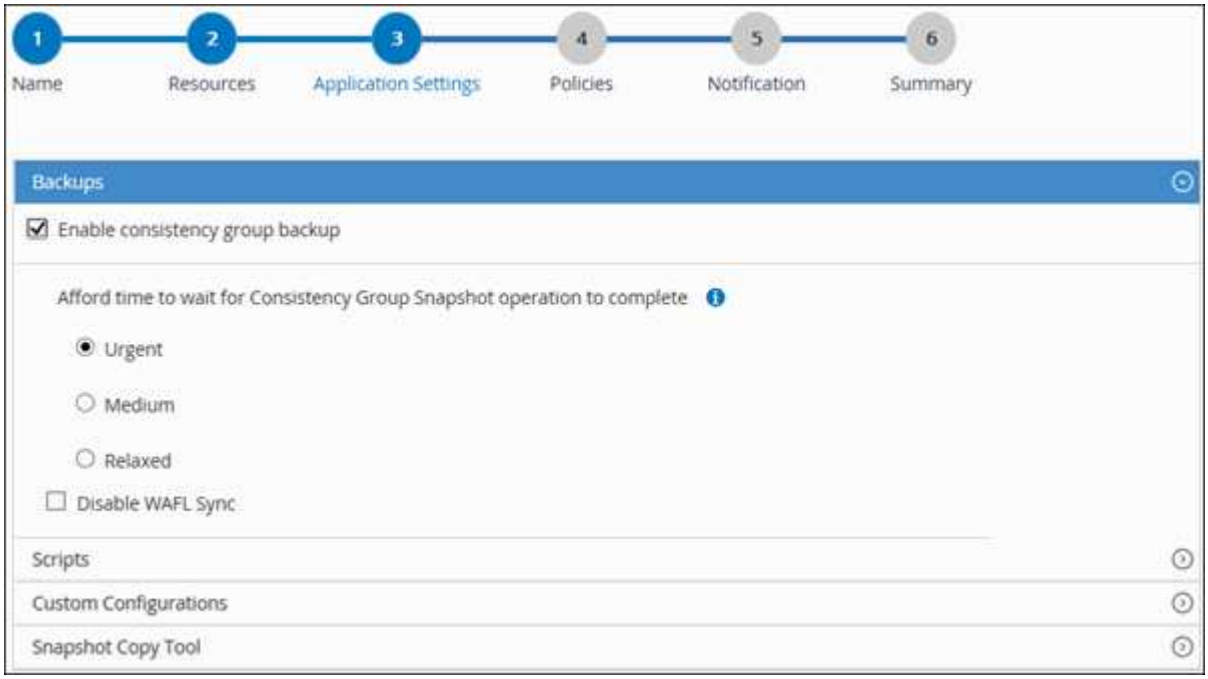
5. Seleccione los recursos de la sección **Recursos disponibles** y, a continuación, haga clic en la flecha derecha para moverlos a la sección **Recursos seleccionados**.

6. En la página **Configuración de la aplicación**, haga 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. 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)	Permite la gestión del registro de archivos para eliminar los registros de archivos.

Parámetro	Ajuste	Descripción
RETENCIÓN_LOG_ARCHIVO	número_de_días	Especifica la cantidad de días que se conservan los registros de archivo. Este valor debe ser igual o mayor que las RETENTIONS NTAP_SNAPSHOT_.
ARCHIVE_LOG_DIR	change_info_directory/logs	Especifica la ruta de acceso al directorio que contiene los registros de archivo.
ARCHIVO_LOG_EXT	extensión_archivo	Especifica la longitud de la extensión del archivo de registro de archivos. Por ejemplo, si el registro de archivos es log_backup_0_0_0_0.1615185 51942 9 y si el valor file_extension es 5, la extensión del registro conservará 5 dígitos, que son 16151.
ARCO ARCHIVE_LOG_RECURSIVE_ SE	(S/N)	Permite la gestión de registros de ficheros en subdirectorios. Debe utilizar este parámetro si los registros de archivo se encuentran en subdirectorios.

Los pares 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**. 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**.

Si desea que…	Realice lo siguiente…
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 **Directivas**, realice los siguientes pasos:

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

   También puede crear una directiva haciendo clic en + .

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

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

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

   Policy_name es el nombre de la política seleccionada.

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

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

1. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. 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.
- Si desea crear un backup basado en archivos cuando una o varias bases de datos de tenant están inactivos, establezca el parámetro

ALLOW_FILE_BASED_BACKUP_IFINACTIVE_ARRENDATARIOS_PRESENT en **YES** en el archivo de propiedades de HANA con el cmdlet Set-SmConfigSettings.

La información relativa a los parámetros que se pueden utilizar con el cmdlet y sus descripciones se puede obtener ejecutando Get-Help *command_name*. Como alternativa, 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 **Recursos** y, a continuación, seleccione el plugin adecuado en la lista.
2. En la página **recurso**, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.

   Haga clic en y luego 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 **recurso**, seleccione **usar formato de nombre personalizado para copia Snapshot** y, a continuación, escriba un formato de nombre personalizado que desee utilizar para el nombre de copia 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 **Configuración de la aplicación**, haga lo siguiente:

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

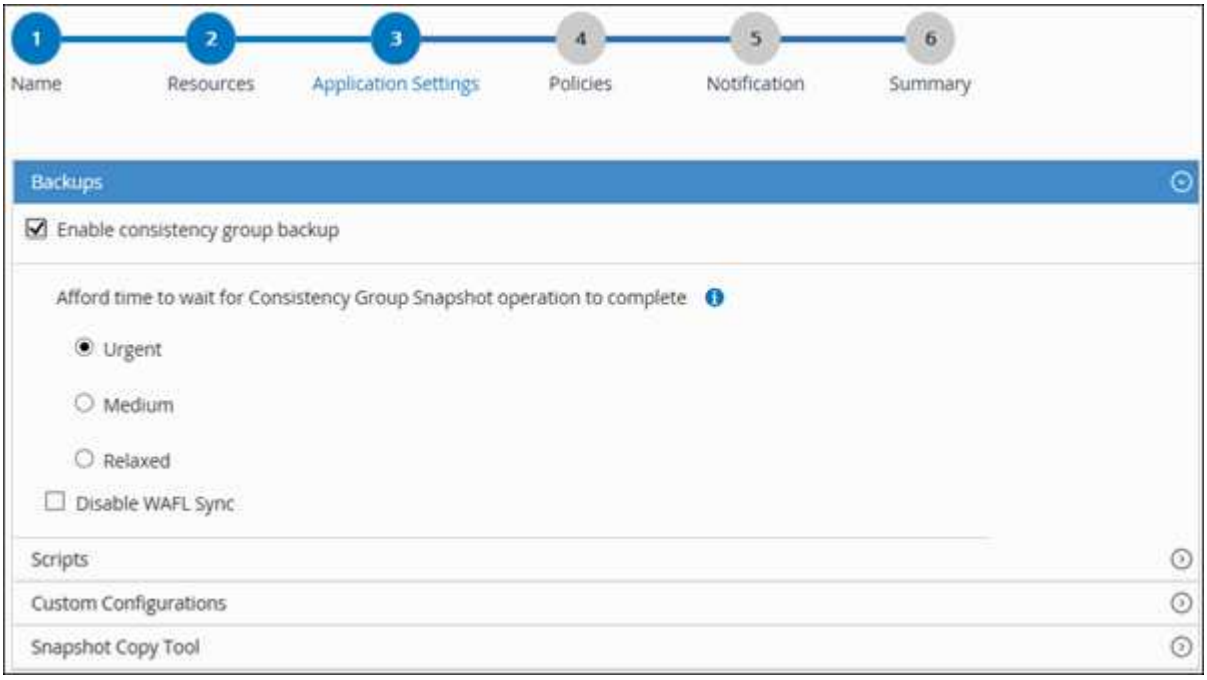
     Habilite el backup del grupo de consistencia y, si es necesario, realice las siguientes tareas:

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 **Directivas**, realice los siguientes pasos:

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

   También puede crear una directiva haciendo clic en + .

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

   a. Haga clic en + En la columna Configurar programaciones de la directiva para la que 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 **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.

   También debe especificar las direcciones de correo electrónico del remitente y los destinatarios, así como el asunto del correo. 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 **copia de seguridad**, 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 hacer una copia de seguridad de un grupo de recursos bajo demanda desde la página **Recursos**. 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 ingresando su nombre en el cuadro de búsqueda o haciendo clic en y, a continuación, seleccione 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*. Como alternativa, 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*. Como alternativa, 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.

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.

En la página **Topology**, puede ver todas las copias de seguridad y clones disponibles para el recurso o 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 **Recursos**, seleccione el recurso o el grupo de recursos de la lista desplegable **Ver**.
  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 .

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.