



# **Proteja las aplicaciones que se ejecutan en Azure NetApp Files**

## SnapCenter software

NetApp  
January 09, 2026

# Tabla de contenidos

Proteja las aplicaciones que se ejecutan en Azure NetApp Files .....	1
Proteja las aplicaciones que se ejecutan en Azure NetApp Files .....	1
Limitaciones .....	1
Instale SnapCenter y cree las credenciales .....	1
Instalar SnapCenter en la máquina virtual de Azure .....	1
Cree las credenciales de Azure en SnapCenter .....	3
Configure la cuenta de almacenamiento de Azure .....	4
Cree la credencial para añadir el host del plugin .....	4
Proteger las bases de datos SAP HANA .....	5
Añadir hosts e instalar el plugin de SnapCenter para base de datos SAP HANA .....	5
Añada una base de datos SAP HANA .....	6
Crear políticas de backup para bases de datos SAP HANA .....	6
Cree grupos de recursos y conecte políticas de backup de SAP HANA .....	7
Realizar un backup de las bases de datos SAP HANA que se ejecutan en Azure NetApp Files .....	8
Realice un backup de grupos de recursos SAP HANA .....	9
Restaurar y recuperar bases de datos SAP HANA .....	9
Clone el backup de base de datos SAP HANA .....	10
Proteger bases de datos de Microsoft SQL Server .....	12
Añadir hosts e instalar el plugin de SnapCenter para base de datos de SQL Server .....	12
Crear políticas de backup para bases de datos de SQL Server .....	12
Cree grupos de recursos y asocie las políticas de backup de SQL .....	14
Realizar backups de bases de datos de SQL Server que se ejecutan en Azure NetApp Files .....	15
Realizar un backup de grupos de recursos de SQL Server .....	16
Restaurar y recuperar bases de datos de SQL Server .....	16
Clone el backup de base de datos de SQL Server .....	18
Proteger bases de datos de Oracle .....	19
Añadir hosts e instalar el plugin de SnapCenter para base de datos de Oracle .....	20
Crear políticas de backup para bases de datos de Oracle .....	20
Crear grupos de recursos y asociar las políticas de backup de Oracle .....	21
Realizar backups de las bases de datos de Oracle que se ejecutan en Azure NetApp Files .....	22
Realice un backup de los grupos de recursos de Oracle .....	23
Restaurar y recuperar bases de datos de Oracle .....	23
Clone el backup de base de datos de Oracle .....	26

# Proteja las aplicaciones que se ejecutan en Azure NetApp Files

## Proteja las aplicaciones que se ejecutan en Azure NetApp Files

SnapCenter admite la protección de aplicaciones como Oracle, SQL y SAP HANA que residen en Azure NetApp Files. A partir de la versión 6.0.1, SnapCenter admite la función de backup de Azure NetApp Files que amplía las funcionalidades de protección de datos de Azure NetApp Files al proporcionar una solución de backup totalmente gestionada para la recuperación, el archivado y el cumplimiento de normativas a largo plazo.

Azure NetApp Files es una solución de almacenamiento premium que puede ser costosa para la retención de backup a largo plazo. Para optimizar los costes, puede mover los backups desde el almacenamiento de Azure NetApp Files a un almacén de objetos de Azure. A partir de SnapCenter 6.0.1, puede realizar backups y clonar aplicaciones que residen en Azure NetApp Files en Azure Blob Storage (almacén de objetos). Puede conservar dos copias de sus datos, copias snapshot de volúmenes en almacenamiento de Azure NetApp Files para recuperación a corto plazo y otra copia en Azure Blob Storage para recuperación a largo plazo.

Cuando se habilita una política con el backup de Azure NetApp Files y se asocia con un recurso, SnapCenter gestiona la creación de copias Snapshot de volúmenes y el backup de ellas en Azure Blob Storage.

SnapCenter crea el almacén de backup y habilita el backup del volumen. Si habilitó el backup para el volumen, SnapCenter utiliza el almacén existente.

### Limitaciones

- No se admiten las funcionalidades de almacenamiento de objetos para los sistemas de almacenamiento FAS, ASA o AFF ONTAP y Amazon FSx para NetApp ONTAP.
- Los flujos de trabajo de montaje y catálogo de Oracle y SAP HANA no son compatibles con los backups de almacenamiento de objetos, pero sí con las copias Snapshot.
- No se admiten los clones de Oracle PDB para los backups de almacenamiento de objetos, pero sí para las Snapshot.
- No se admite la verificación de backups en el almacenamiento de objetos, la compatibilidad con API DE REST, la gestión del ciclo de vida de clones desde el almacenamiento de objetos e las funciones de generación de informes para los backups de almacenamiento de objetos.
- No se admite la restauración desde backups en Azure Blob Storage a Azure NetApp Files. También puede usar la opción clone.
- No se admite la división de clones.

## Instale SnapCenter y cree las credenciales

### Instalar SnapCenter en la máquina virtual de Azure

Puede descargar el software SnapCenter del sitio de soporte de NetApp e instalar el software en la máquina virtual de Azure.

#### Antes de empezar

- Asegúrese de que la máquina virtual de Azure Windows cumple los requisitos de instalación del servidor SnapCenter. Para obtener más información, consulte "["Requisitos para instalar el servidor SnapCenter"](#)".
- Si es nuevo en Azure NetApp Files y no tiene una cuenta de NetApp existente, asegúrese de que se ha registrado para poder acceder al software de SnapCenter. Para obtener más información, consulte "["Regístrese para acceder al software de SnapCenter"](#)".

## Pasos

1. Descargue el paquete de instalación del servidor SnapCenter desde "["Sitio de soporte de NetApp"](#)".
2. Inicie la instalación del servidor SnapCenter haciendo doble clic en el archivo .exe descargado.

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

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

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



El carácter especial "%" no está soportado en la ruta de acceso personalizada de la base de datos del repositorio. Si incluye "%" en la ruta, la instalación falla.

4. Haga clic en **instalar ahora**.

Si ha especificado valores que no son válidos, se mostrarán los mensajes de error adecuados. Debe volver a introducir los valores e iniciar la instalación.



Si hace clic en el botón **Cancelar**, se completará el paso que se está ejecutando y, a continuación, se iniciará la operación de reversión. El servidor SnapCenter se eliminará por completo del host.

Sin embargo, si hace clic en **Cancelar** cuando se están realizando las operaciones "reinicio del sitio del servidor SnapCenter" o "esperando inicio del servidor SnapCenter", la instalación continuará sin cancelar la operación.

## Registre el producto para habilitar la asistencia

Si es nuevo en NetApp y no tiene una cuenta de NetApp existente, debe registrar el producto para habilitar el soporte.

## Pasos

1. Después de instalar SnapCenter, vaya a **Ayuda > Acerca de**.
2. En el cuadro de diálogo *About SnapCenter*, anote la instancia de SnapCenter, un número de 20 dígitos que comienza por 971.
3. Haga clic en <https://register.netapp.com>.
4. Haga clic en **no soy un cliente registrado de NetApp**.
5. Especifique sus datos para registrarse.
6. Deje en blanco el campo Número de serie de referencia de NetApp.

7. Seleccione **SnapCenter** en la lista desplegable Línea de productos.
8. Seleccione el proveedor de facturación.
9. Introduzca el identificador de instancia de SnapCenter de 20 dígitos.
10. Haga clic en **Enviar**.

## Cree las credenciales de Azure en SnapCenter

Debe crear la credencial de Azure en SnapCenter para acceder a la cuenta de Azure NetApp.

### Antes de empezar

- Asegúrese de haber creado el principal de servicio en Azure.
- Asegúrese de que tiene disponibles el ID de inquilino, el ID de cliente y la clave secreta asociada al principal de servicio.
  - El ID de inquilino se puede encontrar en Azure Portal en la página Visión General de Entra ID.
  - El ID de cliente también se conoce como ID de aplicación para Enterprise App/Service Principal. Esto se puede encontrar en el portal de Azure en la página Visión general de la aplicación empresarial que ha creado para actuar como principal de servicios para SnapCenter.
  - La clave secreta de cliente también se conoce como valor secreto. Puede crear este secreto de cliente en Azure Portal navegando a **Registros de aplicaciones** bajo Entra ID. Después de seleccionar la aplicación empresarial que creó, navegue a **Certificados y secretos** y luego a **Nuevo secreto de cliente**.



Solo se puede acceder al valor secreto cuando se crea. No podrá acceder a él más tarde.

- Se deben otorgar permisos al principal de servicio. La función de Contributor permitirá al director de servicio realizar las acciones necesarias en Azure. Esto se puede otorgar desde la página Control de Acceso (IAM) de la página Suscripción.

### 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 siguiente información necesaria para crear la credencial.

Para este campo...	Realice lo siguiente...
Nombre de credencial	Escriba un nombre para la credencial.
Modo de autenticación	Seleccione <b>Azure Credential</b> de la lista desplegable.
ID de inquilino	Introduzca el ID de inquilino.
ID del cliente	Introduzca el ID de cliente.

Para este campo...	Realice lo siguiente...
Clave secreta de cliente	Introduzca la clave secreta del cliente.

5. Haga clic en **Aceptar**.

## Configure la cuenta de almacenamiento de Azure

Debe configurar la cuenta de almacenamiento de Azure en SnapCenter.

La cuenta de almacenamiento de Azure contiene detalles sobre el ID de suscripción, las credenciales de Azure y la cuenta de Azure NetApp.



Las licencias estándar y basadas en capacidad no son requeridas para Azure NetApp Files.

### Pasos

1. En el panel de navegación izquierdo, haga clic en **sistemas de almacenamiento**.
2. En la página Sistemas de almacenamiento, seleccione **Azure NetApp Files** y haga clic en **Nuevo**.
3. Seleccione la credencial, el ID de suscripción y la cuenta de NetApp en las listas desplegables correspondientes.
4. Haga clic en **Enviar**.

## Cree la credencial para añadir el host del plugin

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.

### 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 siguiente información necesaria para crear la credencial.

Para este campo...	Realice lo siguiente...
Nombre de credencial	Escriba un nombre para la credencial.
Modo de autenticación	Seleccione el modo de autenticación de la lista desplegable.
Tipo de autenticación	Seleccione <b>Basado en contraseña</b> o <b>Basado en clave SSH</b> (solo para host Linux).
Nombre de usuario	Especifique el nombre de usuario.

Para este campo...	Realice lo siguiente...
Contraseña	Si seleccionó autenticación basada en contraseña, especifique la contraseña.
Clave privada SSH	Si seleccionó la autenticación basada en clave SSH, especifique la clave privada.
Use privilegios sudo	Seleccione la casilla de comprobación Use sudo privileges si va a crear credenciales para usuarios que no son raíz.   Esto solo se aplica a usuarios Linux.

5. Haga clic en **Aceptar**.

## Proteger las bases de datos SAP HANA

### Añadir hosts e instalar el plugin de SnapCenter para base de datos SAP HANA

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.

#### Antes de empezar

- Debe ser un usuario al que se ha asignado una función que tenga permisos de instalación y desinstalación de plugins, como el rol de administrador de SnapCenter.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está incorporada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.
- Si está instalando en el host centralizado, asegúrese de que el software cliente SAP HANA esté instalado en ese host y abra los puertos necesarios en el host de la base de datos SAP HANA para ejecutar las consultas SQL HDB de forma remota.

#### Pasos

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. Verifique que la pestaña **Managed Hosts** esté seleccionada.
3. Haga clic en **Agregar**.
4. En la página hosts, realice las siguientes acciones:
  - a. En el campo Tipo de host, seleccione el tipo de host.
  - b. En el campo Host name, introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host.
  - c. En el campo Credenciales, introduzca la credencial que ha creado.
5. En la sección Select Plug-ins to Install, seleccione los plugins que desea instalar.
6. (Opcional) Haga clic en **Más opciones** y especifique los detalles.
7. Haga clic en **Enviar**.

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.

9. Supervise el progreso de la instalación.

## Añada una base de datos SAP HANA

Debe añadir manualmente la base de datos SAP HANA.

### Acerca de esta tarea

Los recursos se deben añadir manualmente si el plugin está instalado en un servidor centralizado. Si el plugin de SAP HANA se instala en el host de la base de datos de HANA, el sistema HANA se detecta de forma automática.



La detección automática no es compatible con la configuración de varios hosts HANA. Solo es necesario añadir a través del plugin centralizado.

### 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:
  - a. Introduzca el tipo de recurso como Single Container, Multitenant Database Container o Non-data Volume.
  - b. Introduzca el nombre del sistema SAP HANA.
  - c. Introduzca el ID del sistema (SID).
  - d. Seleccione el host del plugin.
  - e. Introduzca la clave para conectarse al sistema SAP HANA.
  - f. Introduzca el nombre de usuario para el que se configuró la clave de almacenamiento de usuario seguro HDB.
4. En la página Proporcionar espacio de almacenamiento, seleccione **Azure NetApp Files** como tipo de almacenamiento.
  - a. Seleccione la cuenta de Azure NetApp.
  - b. Seleccione el pool de capacidad y los volúmenes asociados.
  - c. Haga clic en **Guardar**.
5. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## 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.

### Pasos

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.

2. En la página Configuración, haga clic en **Directivas**.
3. Haga clic en **Nuevo**.
4. En la página Name, escriba el nombre de la política y una descripción.
5. En la página Policy type, realice los siguientes pasos:
  - a. Seleccione **Azure NetApp Files** como tipo de almacenamiento.
  - b. Seleccione **Basado en archivos** si desea realizar una comprobación de integridad de la base de datos.
  - c. Seleccione **Basado en Snapshot** si desea crear una copia de seguridad utilizando la tecnología Snapshot.
6. En la página Snapshot and backup, realice los siguientes pasos:
  - a. Seleccione la frecuencia del backup programado.
  - b. Especifique la configuración de retención.
  - c. Si desea habilitar la copia de seguridad de Azure NetApp Files, seleccione **Habilitar copia de seguridad** y especifique la configuración de retención.
7. Revise el resumen y haga clic en **Finalizar**.

## Cree grupos de recursos y conecte políticas de backup de SAP HANA

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 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.
Etiquetas	Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos.
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 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**.

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 Policies, realice los siguientes pasos:
  - a. Seleccione una o varias políticas de la lista desplegable.
  - b.
    - En la columna Configure Schedules, haga clic en  en la política que desea configurar.
    - En el cuadro de diálogo Agregar programas para la directiva *policy\_name*, configure la programación y, a continuación, haga clic en **Aceptar**.
7. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
8. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## **Realizar un backup de las bases de datos SAP HANA que se ejecutan en Azure NetApp Files**

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

### **Pasos**

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Recursos, filtre los recursos de la lista desplegable **Ver** en función del tipo de recurso.
3. Seleccione el recurso que desea incluir en el backup.
4. En la página Recursos, seleccione **Use custom name format for Snapshot copy** y, a continuación, escriba el formato del nombre personalizado que deseé usar para el nombre de Snapshot.
5. En la página Application Settings, realice lo siguiente:
  - a. Seleccione la flecha **backups** para establecer opciones de copia de seguridad adicionales.
  - b. Seleccione la flecha **Scripts** para ejecutar los comandos PRE y POST para las operaciones de inactividad, instantánea y desactivación.
  - c. Seleccione la flecha **Configuraciones personalizadas** y, a continuación, introduzca los pares de valores personalizados necesarios para todos los trabajos que utilizan este recurso.
  - d. Seleccione la **Herramienta de copia de instantáneas > SnapCenter sin consistencia del sistema de archivos** para crear instantáneas.

La opción **File System Consistency** solo se aplica a las aplicaciones que se ejecutan en hosts de Windows.

6. En la página Policies, realice los siguientes pasos:
  - a. Seleccione una o varias políticas de la lista desplegable.
  - b.
    - Seleccione  en la columna Configure Schedules correspondiente a la política para la cual desea configurar una programación.
    - En el cuadro de diálogo Add schedules for policy *policy\_name*, configure la programación y, a continuación, seleccione **OK**.
  - policy\_name es el nombre de la directiva seleccionada.

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

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

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

9. Seleccione **Back up Now**.

10. En la página Backup, realice los siguientes pasos:

- a. Si hay varias políticas asociadas con el recurso, 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.

11. Seleccione **copia de seguridad**.

12. Supervise el progreso de la operación haciendo clic en **Monitor > Jobs**.

## Realice un backup de grupos de recursos SAP HANA

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

### Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.
3. En la página Resource Groups, seleccione el grupo de recursos del que desea realizar un backup y, a continuación, seleccione **Back up Now**.
4. En la página Backup, realice los siguientes pasos:
  - a. Si hay varias políticas asociadas con el grupo de recursos, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.

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

  - b. Seleccione **copia de seguridad**.
5. Supervise el progreso de la operación seleccionando **Monitor > Trabajos**.

## Restaurar y recuperar bases de datos SAP HANA

Es posible restaurar y recuperar datos de los backups.

### Acerca de esta tarea

Para los sistemas Auto Discovered HANA, si se selecciona la opción **Complete Resource**, la restauración se realiza utilizando la tecnología Single File snapshot restore. Si la casilla de verificación **Fast Restore** está seleccionada, se utiliza la tecnología Volume Revert.

Para los recursos agregados manualmente, siempre se utiliza la tecnología Volume Revert.

## 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.
3. Seleccione el recurso, o bien seleccione un grupo de recursos y, a continuación, elija un recurso de ese grupo.
4. En la vista Manage Copies, seleccione **copias de seguridad** ya sea en los sistemas de almacenamiento primario o secundario (reflejado o en almácen).
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**.

Se restauran todos los volúmenes de datos configurados de la base de datos SAP HANA.

7. Para los sistemas HANA detectados automáticamente, en la página Restore Scope, realice las siguientes acciones:
  - a. Seleccione **Recuperar al estado más reciente** si desea recuperarse lo más cerca posible de la hora actual.
  - b. Seleccione **Recuperar a punto en el tiempo** si desea recuperar al punto en el tiempo especificado.
  - c. Seleccione **Recuperar a copia de seguridad de datos especificada** si desea recuperar una copia de seguridad de datos específica.
  - d. Seleccione **No recovery** si no desea recuperar ahora.
  - e. Especifique la ubicación de backup de registros.
  - f. Especifique la ubicación del catálogo de backups.
8. 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.
9. 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.
10. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.

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

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

## Clone el backup de base de datos SAP HANA

Puede utilizar SnapCenter para clonar una base de datos SAP HANA con el backup de esa base de datos. Los clones creados son clones gruesos y se crean en el pool de capacidad primario.

## 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.
3. Seleccione el recurso o el grupo de recursos.
4. En la vista Administrar copias, seleccione **Copias de seguridad** en el sistema de almacenamiento primario.
5. Seleccione el backup de datos de la tabla y haga clic en .
6. En la página Location, lleve a cabo las siguientes acciones:
  - a. Seleccione el host que tiene el plugin SAP HANA instalado para gestionar el sistema HANA clonado.

Puede ser un host de plugin centralizado o un host de sistema HANA.



Si el plugin de HANA se instala en un host centralizado que gestiona bases de datos de HANA en otros hosts, mientras crea o elimina clones, SnapCenter omite intencionalmente las operaciones del lado del host (montar o desmontar sistema de archivos) como servidor de destino es un host centralizado. Es necesario utilizar scripts previos o posteriores a la clonado para realizar las operaciones de montaje y desmontaje.

- a. Introduzca el SID de SAP HANA para clonar a partir de los backups existentes.
- b. Introduzca las direcciones IP o los nombres de host a los que se van a exportar los volúmenes clonados.
- c. Si los volúmenes de ANF de base de datos SAP HANA están configurados en un pool de CAPACIDAD DE CALIDAD DE SERVICIO manual, especifique la CALIDAD DE SERVICIO de los volúmenes clonados.

Si no se especifica LA CALIDAD DE SERVICIO para los volúmenes clonados, se usará la CALIDAD DE SERVICIO del volumen de origen. Si se utiliza el pool de capacidad automática DE CALIDAD DE SERVICIO, se ignorará el valor de CALIDAD DE SERVICIO especificado.

7. En la página Scripts, realice los siguientes pasos:
  - a. Introduzca los comandos para el clon previo o posterior que se deben ejecutar antes o después de la operación de clonado, respectivamente.
  - b. Escriba el comando de montaje para montar un sistema de archivos en un host.

Si se detecta automáticamente el sistema HANA de origen y se instala el plugin del host de destino del clon en el host SAP HANA, SnapCenter desmonta automáticamente los volúmenes de datos de HANA existentes en el host de destino del clonado y monta los volúmenes de datos de HANA recién clonados.

8. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
9. Revise el resumen y, a continuación, haga clic en **Finalizar**.
10. Supervise el progreso de la operación haciendo clic en **Monitor > Jobs**.



La división de clones está deshabilitada para los clones de ANF porque el clon de ANF ya es un volumen independiente creado a partir de la snapshot seleccionada.

# Proteger bases de datos de Microsoft SQL Server

## Añadir hosts e instalar el plugin de SnapCenter para base de datos de SQL Server

SnapCenter admite la protección de datos de instancias de SQL en recursos compartidos de SMB en Azure NetApp Files. Se admiten las configuraciones de grupos de disponibilidad (AG) independientes.

Debe usar la página SnapCenter Add Host para añadir hosts y, a continuación, instalar el paquete de los plugins. Los plugins se instalan automáticamente en hosts remotos.

### Antes de empezar

- Debe ser un usuario al que se ha asignado una función que tenga permisos de instalación y desinstalación de plugins, como el rol de administrador de SnapCenter.
- Al instalar un plugin en un host de Windows, si especifica una credencial que no está incorporada o si el usuario pertenece a un usuario de grupo de trabajo local, debe deshabilitar UAC en el host.

### Pasos

1. En el panel de navegación izquierdo, seleccione **hosts**.
2. Compruebe que la ficha **Managed hosts** está seleccionada en la parte superior.
3. Seleccione **Agregar**.
4. En la página hosts, haga lo siguiente:
  - a. En el campo Tipo de host, seleccione el tipo de host.
  - b. En el campo Host name, introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host.
  - c. En el campo Credenciales, introduzca la credencial que ha creado.
5. En la sección **Seleccione Plug-ins to Install**, seleccione los plugins que deseé instalar.
6. (Opcional) Haga clic en **Más opciones** y especifique los detalles.
7. Seleccione **Enviar**.
8. Seleccione **Configurar directorio de registro** y en la página Configurar directorio de registro de host, introduzca la ruta SMB del directorio de registro de host y haga clic en **Guardar**.
9. Haga clic en **Enviar** y supervise el progreso de la instalación.

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

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

También es posible crear una política de backup en el momento de crear un grupo de recursos o realizar un backup de un único recurso.

### Pasos

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

4. En la página Name, escriba el nombre de la política y una descripción.
5. En la página Policy type, realice los siguientes pasos:
  - a. Seleccione **Azure NetApp Files** como tipo de almacenamiento.
  - b. Seleccione el tipo de backup.
    - i. Seleccione **Full Backup and Log Backup** si desea realizar una copia de seguridad de los archivos de la base de datos y los registros de transacciones.
    - ii. Seleccione **Full Backup** si desea realizar una copia de seguridad solo de los archivos de la base de datos.
    - iii. Seleccione **Log Backup** si desea realizar una copia de seguridad solo de los registros de transacciones.
    - iv. Seleccione **Copia de seguridad de solo copia** si desea realizar una copia de seguridad de sus recursos utilizando otra aplicación.
  - c. En la sección Availability Group Settings, realice las siguientes acciones:
    - i. Seleccione Backup on preferred backup replica si desea realizar un backup solo en la réplica.
    - ii. Seleccione la réplica principal o secundaria del AG para el backup.
    - iii. Seleccione la prioridad de backup.
6. En la página Snapshot and backup, realice los siguientes pasos:
  - a. Seleccione la frecuencia del backup programado.
  - b. Especifique la configuración de retención según el tipo de backup seleccionado.
  - c. Si desea habilitar la copia de seguridad de Azure NetApp Files, seleccione **Habilitar copia de seguridad** y especifique la configuración de retención.
7. En la página Verification, realice los siguientes pasos:
  - a. En la sección Run verification for following backup schedules, seleccione la frecuencia de backup.
  - b. En la sección Database consistency check options, realice las siguientes acciones:
    - i. Seleccione **limitar la estructura de integridad a la estructura física de la base de datos (PHYSICAL\_ONLY)** para limitar la comprobación de integridad a la estructura física de la base de datos y detectar páginas dañadas, errores de sumas de comprobación y errores de hardware habituales que afecten a la base de datos.
    - ii. Seleccione **Suprimir todos los mensajes informativos (NO INFOMSGS)** para suprimir todos los mensajes informativos.

Seleccionado de forma predeterminada.
    - iii. Seleccione **Display all reported error messages per object (ALL\_ERRORMSG)** para visualizar todos los errores notificados por objeto.
    - iv. Seleccione **no comprobar los índices no almacenados en clúster (NOINDEX)** si no desea comprobar los índices no almacenados en clúster.
  - La base de datos de SQL Server utiliza la comprobación de la consistencia de base de datos de Microsoft SQL Server para comprobar la integridad lógica y física de los objetos de la base de datos.
  - v. Seleccione **Limitar las comprobaciones y obtener los bloqueos en lugar de utilizar una copia Snapshot interna de la base de datos (TABLOCK)** para limitar las comprobaciones y obtener bloqueos en lugar de utilizar una instantánea interna de la base de datos.

- c. En la sección **Backup de registro**, seleccione **verificar copia de seguridad de registro al finalizar** para verificar la copia de seguridad de registro al finalizar.
  - d. En la sección **Verification script settings**, introduzca la ruta de acceso y los argumentos del script previo o posterior que deben ejecutarse antes o después de la operación de verificación, respectivamente.
8. Revise el resumen y haga clic en **Finalizar**.

## Cree grupos de recursos y asocie las políticas de backup de SQL

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 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.
Etiquetas	Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos.
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 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**.
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 Policies, realice los siguientes pasos:
  - a. Seleccione una o varias políticas de la lista desplegable.
  - 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**.
  - d. Seleccione Microsoft SQL Server Scheduler.
7. En la página Verification, realice los siguientes pasos:

- a. Seleccione el servidor de verificación.
  - b. Seleccione la política para la que desea configurar la programación de verificación y haga clic en  \* .
  - c. Seleccione **Ejecutar verificación después de copia de seguridad** o **Ejecutar verificación programada**.
  - d. Haga clic en **Aceptar**.
8. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
9. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## Realizar backups de bases de datos de SQL Server que se ejecutan en Azure NetApp Files

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

### Antes de empezar

Debe crear un balanceador de carga si el clúster de conmutación por error de Azure Windows no tiene una IP de clúster asignada o si no es accesible desde SnapCenter. La IP del equilibrador de carga se debe configurar y es posible acceder a ella desde el servidor de SnapCenter.

### Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Recursos, seleccione **Base de datos**, **Instancia** o **Grupo de disponibilidad** en la lista desplegable Ver.
3. En la página Recursos, seleccione **Use custom name format for Snapshot copy** y, a continuación, escriba el formato del nombre personalizado que deseé usar para el nombre de Snapshot.
4. En la página Policies, realice los siguientes pasos:
  - a. Seleccione una o varias políticas de la lista desplegable.
  - b. Seleccione  en la columna Configure Schedules correspondiente a la política para la cual desea configurar una programación.
  - c. En el cuadro de diálogo Add schedules for policy *policy\_name*, configure la programación y, a continuación, seleccione **OK**.

*policy\_name* es el nombre de la directiva seleccionada.

- d. Seleccione **Use Microsoft SQL Server scheduler** y, a continuación, seleccione la instancia del programador en la lista desplegable **Scheduler Instance** que está asociada con la política de programación.
5. En la página Verification, realice los siguientes pasos:
  - a. Seleccione el servidor de verificación.
  - b. Seleccione la política para la que desea configurar la programación de verificación y haga clic en  \* .

- c. Seleccione **Ejecutar verificación después de copia de seguridad** o **Ejecutar verificación programada**.
  - d. Haga clic en Aceptar.
6. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
  7. Revise el resumen y, a continuación, haga clic en **Finalizar**.
  8. Seleccione **Back up Now**.
  9. En la página Backup, realice los siguientes pasos:
    - a. Si hay varias políticas asociadas con el recurso, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.
    - b. Seleccione **Verificar después de la copia de seguridad**.
    - c. Seleccione **copia de seguridad**.
  10. Supervise el progreso de la operación haciendo clic en **Monitor > Jobs**.

## Realizar un backup de grupos de recursos de SQL Server

Puede realizar el backup de los grupos de recursos que consten de varios recursos. Se realiza una operación de backup del grupo de recursos con todos los recursos definidos en el grupo.

### Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.
3. En la página Resource Groups, seleccione el grupo de recursos del que desea realizar un backup y, a continuación, seleccione **Back up Now**.
4. En la página Backup, realice los siguientes pasos:
  - a. Si hay varias políticas asociadas con el grupo de recursos, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.
  - b. Después de la copia de seguridad, seleccione **Verify** para verificar la copia de seguridad bajo demanda.
  - c. Seleccione **copia de seguridad**.
5. Supervise el progreso de la operación seleccionando **Monitor > Trabajos**.

## Restaurar y recuperar bases de datos de SQL Server

Puede utilizar SnapCenter para restaurar bases de datos de SQL Server. La restauración de una base de datos es un proceso multifásico que copia todos los datos y las páginas de registro de una copia de seguridad específica de SQL Server a una base de datos específica.

### Antes de empezar

- Configure la instancia de destino con un usuario de Active Directory que pertenezca al dominio de Active Directory de SMB AD y tenga permisos para establecer los permisos de archivo adecuadamente.

- Configure las credenciales a nivel de instancia de SnapCenter .
- Si la base de datos SQL existe en un recurso compartido CIFS, entonces la cuenta RunAS y la cuenta de servicio SQL (cuenta de dominio) del host del complemento deben formar parte de BUILTIN\Administrators grupo del servidor CIFS en ONTAP.
- Las configuraciones SMB no admiten la autenticación SQL para la instancia de destino. Configure la instancia de destino en SnapCenter con un usuario de Active Directory que tenga los permisos necesarios.
- Si la cuenta de servicio del complemento SnapCenter no es un usuario de Active Directory, asegúrese de que haya disponible un usuario con control total sobre los volúmenes de origen al restaurar en un host alternativo.

## 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 **Base de datos o Grupo de recursos** en la lista Ver.
3. Seleccione la base de datos o el grupo de recursos en la lista.
4. En la vista Administrar copias, seleccione **Copias de seguridad** del sistema de almacenamiento.
5. Seleccione el backup en la tabla y haga clic en el  .
6. En la página Restore Scope, seleccione una de las siguientes opciones:
  - a. Seleccione **Restaurar la base de datos en el mismo host donde se creó la copia de seguridad** para restaurar la base de datos en el mismo servidor SQL.
  - b. Seleccione **Restaurar la base de datos en un host alternativo** si desea restaurar la base de datos en un servidor SQL diferente en el mismo host o en otro donde se realizan las copias de seguridad.
7. En la página Restore Scope, seleccione una de las siguientes opciones:
  - a. Seleccione **Ninguno** cuando necesite restaurar sólo la copia de seguridad completa sin ningún registro.
  - b. Seleccione **All log backups** up-to-the-minute backup restore operation para restaurar todas las copias de seguridad de registros disponibles después de la copia de seguridad completa.
  - c. Seleccione **by log backups** para realizar una operación de restauración a un momento específico, que restaura la base de datos en función de los registros de copia de seguridad hasta el registro de copia de seguridad con la fecha seleccionada.
  - d. Seleccione **by specific date until** para especificar la fecha y la hora después de las cuales no se aplican registros de transacciones a la base de datos restaurada.
  - e. Si ha seleccionado **todas las copias de seguridad de registro, por copias de seguridad de registro o por fecha específica hasta** y los registros se encuentran en una ubicación personalizada, seleccione **usar directorio de registro personalizado** y, a continuación, especifique la ubicación del registro.
8. En la página Pre-Ops and Post Ops, especifique los detalles obligatorios.
9. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el proceso de restauración mediante la página **Monitor > Jobs**.

## Clone el backup de base de datos de SQL Server

Es posible utilizar SnapCenter para clonar una base de datos de SQL con el backup de esa base de datos. Los clones creados son clones gruesos y se crean en el pool de capacidad primario.

### Acerca de esta tarea

Debe asegurarse de que la instancia de destino para el clon esté configurada con un usuario de Active Directory que pertenezca al dominio de directorio SMB ADactive y que tenga permisos para establecer los permisos de archivo adecuadamente. Debe configurar las credenciales en SnapCenter a nivel de instancia.

La autenticación SQL para la instancia de destino no se admitirá para las configuraciones SMB. La instancia de destino se debe configurar en SnapCenter con el usuario de Active Directory que tenga los permisos necesarios.

Si la cuenta de servicio de servicios del plugin de SnapCenter no es un usuario de directorio activo, se requiere el usuario con control total sobre los volúmenes de origen para poder suplantar la trama y realizar la operación requerida.

### Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Database** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos o el grupo de recursos.
4. En la página de vista **Administrar copias**, seleccione la copia de seguridad desde el sistema de almacenamiento primario.
5. Seleccione el backup y, a continuación, seleccione .
6. En la página **Clonar opciones**, proporcione todos los detalles requeridos.
7. En la página ubicación, seleccione una ubicación de almacenamiento para crear un clon.

Si los volúmenes de ANF de bases de datos de SQL Server se configuran en un pool de CAPACIDAD DE CALIDAD DE SERVICIO manual, especifique la CALIDAD DE SERVICIO de los volúmenes clonados.

Si no se especifica LA CALIDAD DE SERVICIO para los volúmenes clonados, se usará la CALIDAD DE SERVICIO del volumen de origen. Si se utiliza el pool de capacidad automática DE CALIDAD DE SERVICIO, se ignorará el valor de CALIDAD DE SERVICIO especificado.

8. En la página Logs, seleccione una de las siguientes opciones:
  - a. Seleccione **Ninguno** si desea clonar solo la copia de seguridad completa sin ningún registro.
  - b. Seleccione **All log backups** si desea clonar todas las copias de seguridad de registros disponibles con fecha posterior a la copia de seguridad completa.
  - c. Seleccione **by log backups until** si desea clonar la base de datos en función de los registros de copia de seguridad que se crearon hasta el registro de copia de seguridad con la fecha seleccionada.
  - d. Seleccione **Por fecha específica hasta** si no desea aplicar los registros de transacciones después de la fecha y hora especificadas.
9. En la página **Script**, introduzca el tiempo de espera del script, la ruta y los argumentos del script previo o script posterior que deben ejecutarse antes o después de la operación de clonado, respectivamente.

10. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
11. Revisa el resumen y luego selecciona **Finalizar**.
12. Supervise el progreso de la operación seleccionando **Monitor > Trabajos**.

## Ejecute el ciclo de vida del clon

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

### Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Database** o **Resource Group** en la lista **View**.
3. Seleccione la base de datos o el grupo de recursos.
4. En la página de vista **Administrar copias**, seleccione la copia de seguridad desde el sistema de almacenamiento primario.
5. Seleccione el backup y, a continuación, seleccione .
6. En la página **Clonar opciones**, proporcione todos los detalles requeridos.
7. En la página ubicación, seleccione una ubicación de almacenamiento para crear un clon.

Si los volúmenes de ANF de bases de datos de SQL Server se configuran en un pool de CAPACIDAD DE CALIDAD DE SERVICIO manual, especifique la CALIDAD DE SERVICIO de los volúmenes clonados.

Si no se especifica LA CALIDAD DE SERVICIO para los volúmenes clonados, se usará la CALIDAD DE SERVICIO del volumen de origen. Si se utiliza el pool de capacidad automática DE CALIDAD DE SERVICIO, se ignorará el valor de CALIDAD DE SERVICIO especificado.

8. En la página **Script**, introduzca el tiempo de espera del script, la ruta y los argumentos del script previo o script posterior que deben ejecutarse antes o después de la operación de clonado, respectivamente.
9. En la página Schedule, realice una de las siguientes acciones:
  - Seleccione **Ejecutar ahora** si desea ejecutar el trabajo de clonado inmediatamente.
  - Seleccione **Configure schedule** cuando deseé determinar con qué frecuencia debe producirse la operación de clonación, cuándo debe iniciarse la programación de clonación, en qué día debe producirse la operación de clonación, cuándo debe caducar la programación y si los clones deben eliminarse después de que caduque la programación.
10. En la página **notificación**, en la lista desplegable **preferencia de correo electrónico**, seleccione los escenarios en los que desea enviar los correos electrónicos.
11. Revisa el resumen y luego selecciona **Finalizar**.
12. Supervise el progreso de la operación seleccionando **Monitor > Trabajos**.

## Proteger bases de datos de Oracle

## Añadir hosts e instalar el plugin de SnapCenter para base de datos de Oracle

Puede utilizar la página Add Host para añadir hosts y, a continuación, instalar el paquete de plugins de SnapCenter para Linux o el paquete de plugins de SnapCenter para AIX. 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. Si instala el plugin en un clúster (Oracle RAC), el plugin se instala en todos los nodos del clúster. Para Oracle RAC One Node, debe instalar el plugin en nodos activos y pasivos.

### Pasos

1. En el panel de navegación de la izquierda, haga clic en **hosts**.
2. Verifique que la pestaña **Managed Hosts** esté seleccionada.
3. Haga clic en **Agregar**.
4. En la página hosts, realice las siguientes acciones:
  - a. En el campo Tipo de host, seleccione el tipo de host.
  - b. En el campo Host name, introduzca el nombre de dominio completamente cualificado (FQDN) o la dirección IP del host.
  - c. En el campo Credenciales, introduzca la credencial que ha creado.
5. En la sección Select Plug-ins to Install, seleccione los plugins que desea instalar.
6. (Opcional) Haga clic en **Más opciones** y especifique los detalles.
7. Haga clic en **Enviar**.
8. Compruebe la huella 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.

9. Supervise el progreso de la instalación.

## Crear políticas de backup para bases de datos de Oracle

Antes de usar SnapCenter para realizar backups de recursos de base de datos de Oracle, debe crear una política de backup para el recurso o el grupo de recursos que se respaldará.

### Pasos

1. En el panel de navegación de la izquierda, haga clic en **Configuración**.
2. En la página Configuración, haga clic en **Directivas**.
3. Seleccione Oracle Database en la lista desplegable.
4. Haga clic en **Nuevo**.
5. En la página Name, escriba el nombre de la política y una descripción.
6. En la página Policy type, realice los siguientes pasos:
  - a. Seleccione **Azure NetApp Files** como tipo de almacenamiento.
  - b. Seleccione el tipo de backup como backup online o sin conexión.
  - c. Si desea catalogar la copia de seguridad con Oracle Recovery Manager (RMAN), seleccione **Catalog**

#### **backup with Oracle Recovery Manager (RMAN).**

- d. Si desea reducir los registros de archivos después de la copia de seguridad, seleccione **Prune archive logs after backup**.
  - e. Especifique la configuración de eliminación de archive log.
7. En la página Snapshot and backup, realice los siguientes pasos:
- a. Seleccione la frecuencia del backup programado.
  - b. Especifique la configuración de retención.
  - c. Si desea habilitar la copia de seguridad de Azure NetApp Files, seleccione **Habilitar copia de seguridad** y especifique la configuración de retención.
8. En la página Script, introduzca la ruta y los argumentos del script previo o script posterior que desea ejecutar antes o después de la operación de backup, según corresponda.
9. En la página Verification, seleccione la programación de backup para la que desea realizar la operación de verificación e introduzca la ruta y los argumentos del script previo o posterior que desea ejecutar antes o después de la operación de verificación, según corresponda.
10. Revise el resumen y haga clic en **Finalizar**.

### **Crear grupos de recursos y asociar las políticas de backup de Oracle**

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 Resources, haga clic en **New Resource Group**.
3. En la página Name, realice los siguientes pasos:

<b>Para este campo...</b>	<b>Realice lo siguiente...</b>
Nombre	Escriba un nombre para el grupo de recursos.
Etiquetas	Escriba una o más etiquetas que más adelante le permitirán buscar el grupo de recursos.
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 Snapshot.
Destino del archivo archive log	Especifique los destinos de los archivos de registro de archivos.

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**.
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 Policies, realice los siguientes pasos:
  - a. Seleccione una o varias políticas de la lista desplegable.
  - 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**.
7. En la página Verification, realice los siguientes pasos:
  - a. Seleccione el servidor de verificación.
  - b. Seleccione la política para la que desea configurar el programa de verificación y haga clic en \*.
  - c. Seleccione **Ejecutar verificación después de copia de seguridad** o **Ejecutar verificación programada**.
  - d. Haga clic en **Aceptar**.
8. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
9. Revise el resumen y, a continuación, haga clic en **Finalizar**.

## **Realizar backups de las bases de datos de Oracle que se ejecutan en Azure NetApp Files**

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

### **Pasos**

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Recursos, seleccione **Base de datos** en la lista desplegable Ver.
3. En la página Recursos, seleccione **Use custom name format for Snapshot copy** y, a continuación, escriba el formato del nombre personalizado que deseé usar para el nombre de Snapshot.
4. En la página Policies, realice los siguientes pasos:
  - a. Seleccione una o varias políticas de la lista desplegable.
  - b. Seleccione en la columna Configure Schedules correspondiente a la política para la cual desea configurar una programación.
  - c. En el cuadro de diálogo Add schedules for policy *policy\_name*, configure la programación y, a continuación, seleccione **OK**.
5. En la página Verification, realice los siguientes pasos:
  - a. Seleccione el servidor de verificación.
  - b. Seleccione la política para la que desea configurar la programación de verificación y haga clic en \*.

- \*.
- c. Seleccione **Ejecutar verificación después de copia de seguridad** o **Ejecutar verificación programada**.
  - d. Haga clic en Aceptar.
  6. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
  7. Revise el resumen y, a continuación, haga clic en **Finalizar**.
  8. Seleccione **Back up Now**.
  9. En la página Backup, realice los siguientes pasos:
    - a. Si hay varias políticas asociadas con el recurso, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.
    - b. Haga clic en **copia de seguridad**.
  10. Supervise el progreso de la operación haciendo clic en **Monitor > Jobs**.

## Realice un backup de los grupos de recursos de Oracle

Puede realizar el backup de los grupos de recursos que consten de varios recursos. Se realiza una operación de backup del grupo de recursos con todos los recursos definidos en el grupo.

### Pasos

1. En el panel de navegación izquierdo, seleccione **Recursos** y, a continuación, seleccione el plugin apropiado de la lista.
2. En la página Resources, seleccione **Resource Group** en la lista **View**.
3. En la página Resource Groups, seleccione el grupo de recursos del que desea realizar un backup y, a continuación, seleccione **Back up Now**.
4. En la página Backup, realice los siguientes pasos:
  - a. Si hay varias políticas asociadas con el grupo de recursos, en la lista desplegable **Policy**, seleccione la política que desea usar para la copia de seguridad.
  - b. Seleccione **copia de seguridad**.
5. Supervise el progreso de la operación seleccionando **Monitor > Trabajos**.

## Restaurar y recuperar bases de datos de Oracle

En caso de pérdida de datos, es posible usar SnapCenter para restaurar datos desde uno o más backups en el sistema de archivos activo para luego recuperar la base 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 **Base de datos** o **Grupo de recursos** en la lista Ver.
3. Seleccione la base de datos o el grupo de recursos en la lista.
4. En la vista Administrar copias, seleccione **Copias de seguridad** en el sistema de almacenamiento

primario.

5. Seleccione el backup en la tabla y haga clic en .
6. En la página Restore Scope, realice las siguientes tareas:
  - a. Seleccione RAC si seleccionó un backup de una base de datos en el entorno RAC.
  - b. Realice las siguientes acciones:
    - i. Seleccione **Todos los archivos de datos** si desea restaurar solo los archivos de la base de datos.
    - ii. Seleccione **Tablespaces** si desea restaurar solo los tablespaces.
    - iii. Seleccione **Redo log files** si desea restaurar los archivos redo log de las bases de datos en espera de Data Guard o Active Data Guard.
    - iv. Seleccione **Pluggable databases** y especifique las PDB que desea restaurar.
    - v. Seleccione \* tablespaces de base de datos conectables (PDB)\* y, a continuación, especifique la PDB y los tablespaces de esa PDB que desea restaurar.
    - vi. Seleccione **Restaurar la base de datos en el mismo host donde se creó la copia de seguridad** si desea restaurar la base de datos en el mismo servidor SQL donde se realizan las copias de seguridad.
    - vii. Seleccione **Restaurar la base de datos a un host alternativo** si desea que la base de datos se restaure en un servidor SQL diferente en el mismo host o en otro donde se realicen las copias de seguridad.
    - viii. Seleccione **Cambiar el estado de la base de datos si es necesario para restaurar y recuperar** para cambiar el estado de la base de datos al estado requerido para realizar operaciones de restauración y recuperación.
    - ix. Seleccione **Force in place restore** si desea realizar restauraciones in situ en los escenarios en los que se agregan nuevos archivos de datos después de la copia de seguridad o cuando se agregan, eliminan o recrean LUN en un grupo de discos de LVM.
7. En la página Restore Scope, seleccione una de las siguientes opciones:
  - a. Seleccione **All Logs** si desea recuperar la última transacción.
  - b. Seleccione **Until SCN (System Change Number)** si desea recuperar un SCN específico.
  - c. Seleccione **Fecha y hora** si desea recuperar una fecha y hora específicas.
  - d. Seleccione **No recovery** si no desea recuperar.
  - e. Seleccione **Especificar ubicaciones de archive log externas** si desea especificar la ubicación de los archivos archive log externos.
8. En la página Pre-Ops and Post Ops, especifique los detalles obligatorios.
9. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el progreso de la operación haciendo clic en **Monitor > Jobs**.

### **Restauración y recuperación de espacios de tablas mediante la recuperación de un momento específico**

Puede restaurar un subconjunto de espacios de tablas que se hayan dañado o borrado sin que el resto de espacios de tablas de la base de datos se vea afectado. SnapCenter utiliza RMAN para realizar una recuperación puntual (PITR) de los tablespaces.

## 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 **Base de datos o Grupo de recursos** en la lista Ver.
3. Seleccione la base de datos del tipo instancia única (multitenant).
4. En la vista Manage Copies, seleccione **copias de seguridad** en el sistema de almacenamiento.

Si la copia de seguridad no está catalogada, debe seleccionar la copia de seguridad y hacer clic en **Catálogo**.

5. Seleccione el backup catalogado y haga clic en .
6. En la página Restore Scope, realice las siguientes tareas:
  - a. Seleccione **RAC** si ha seleccionado una copia de seguridad de una base de datos en el entorno RAC.
  - b. Seleccione **Tablespaces** si desea restaurar solo los tablespaces.
  - c. Seleccione **Cambiar el estado de la base de datos si es necesario para restaurar y recuperar** para cambiar el estado de la base de datos al estado requerido para realizar operaciones de restauración y recuperación.
7. En la página Restore Scope, seleccione una de las siguientes opciones:
  - a. Seleccione **Until SCN (System Change Number)** si desea recuperar un SCN específico.
  - b. Seleccione **Fecha y hora** si desea recuperar una fecha y hora específicas.
8. En la página Pre-Ops and Post Ops, especifique los detalles obligatorios.
9. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el proceso de restauración mediante la página **Monitor > Jobs**.

## Restaure y recupere una base de datos conectable mediante la recuperación de un momento específico

Puede restaurar y recuperar una base de datos conectables (PDB) que se dañó o se borró sin afectar a las otras PDB de la base de datos de contenedores (CDB). SnapCenter utiliza RMAN para realizar una recuperación de un momento específico (PITR) de la PDB.

## 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 **Base de datos o Grupo de recursos** en la lista Ver.
3. Seleccione la base de datos del tipo instancia única (multitenant).
4. En la vista Manage Copies, seleccione **copias de seguridad** en el sistema de almacenamiento.

Si la copia de seguridad no está catalogada, debe seleccionar la copia de seguridad y hacer clic en **Catálogo**.

5. Seleccione el backup catalogado y haga clic en .

6. En la página Restore Scope, realice las siguientes tareas:
  - a. Seleccione **RAC** si ha seleccionado una copia de seguridad de una base de datos en el entorno RAC.
  - b. Según si desea restaurar la PDB o los espacios de tablas en una PDB, realice una de las acciones:
    - Seleccione **Pluggable databases (PDBs)** si desea restaurar una PDB.
    - Seleccione **Pluggable database (PDB) tablespaces** si desea restaurar los espacios de tabla en una PDB.
7. En la página Restore Scope, seleccione una de las siguientes opciones:
  - a. Seleccione **Until SCN (System Change Number)** si desea recuperar un SCN específico.
  - b. Seleccione **Fecha y hora** si desea recuperar una fecha y hora específicas.
8. En la página Pre-Ops and Post Ops, especifique los detalles obligatorios.
9. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
10. Revise el resumen y, a continuación, haga clic en **Finalizar**.
11. Supervise el proceso de restauración mediante la página **Monitor > Jobs**.

## Clone el backup de base de datos de Oracle

Es posible utilizar SnapCenter para clonar una base de datos de Oracle con el backup de esa base de datos. Los clones creados son clones gruesos y se crean en el pool de capacidad primario.

### 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 **Base de datos** o **Grupo de recursos** en la lista Ver.
3. Seleccione la base de datos.
4. En la página Manage Copies view, seleccione el backup en el sistema de almacenamiento principal.
5. Seleccione la copia de seguridad de datos y, a continuación, haga clic en .
6. En la página Name, seleccione si desea clonar una base de datos (CDB o no CDB) o clonar una base de datos conectables (PDB).
7. En la página Locations, especifique los detalles necesarios.

Si los volúmenes de ANF de la base de datos de Oracle están configurados en un pool de CAPACIDAD de CALIDAD DE SERVICIO manual, especifique la CALIDAD DE SERVICIO de los volúmenes clonados.

Si no se especifica LA CALIDAD DE SERVICIO para los volúmenes clonados, se usará la CALIDAD DE SERVICIO del volumen de origen. Si se utiliza el pool de capacidad automática DE CALIDAD DE SERVICIO, se ignorará el valor de CALIDAD DE SERVICIO especificado.

8. En la página Credentials, realice una de las siguientes acciones:
  - a. Para el nombre de credencial para el usuario sys, seleccione la credencial que se utilizará para definir la contraseña de usuario sys de la base de datos clonada.
  - b. Para el nombre de credencial de instancia de ASM, seleccione **Ninguno** si la autenticación del sistema operativo está activada para conectarse a la instancia de ASM en el host del clon.

De lo contrario, seleccione la credencial de Oracle ASM configurada con el usuario «sys» o un usuario con el privilegio «sysasm» aplicable al host de clonado.

9. En la página Pre-Ops, especifique la ruta y los argumentos de los scripts previos, y en la sección Database Parameter settings, modifique los valores de los parámetros de la base de datos completados automáticamente que se utilizan para inicializar la base de datos.
10. En la página Post-Ops, se seleccionan por defecto **Recover database** y **Until Cancel** para realizar la recuperación de la base de datos clonada.
  - a. Si selecciona **Until Cancel**, SnapCenter realiza la recuperación mediante el montaje de la última copia de seguridad de registros que tiene la secuencia ininterrumpida de registros de archivos después de esa copia de seguridad de datos que se seleccionó para la clonación.
  - b. Si selecciona **Fecha y hora**, SnapCenter recupera la base de datos hasta una fecha y hora especificadas.
  - c. Si selecciona **Until SCN**, SnapCenter recupera la base de datos hasta un SCN especificado.
  - d. Si selecciona **Especificar ubicaciones de archive log externas**, SnapCenter identifica y monta el número óptimo de copias de seguridad de log según el SCN especificado o la fecha y hora seleccionadas.
  - e. Por defecto, la casilla de verificación **Crear nuevo DBID** está seleccionada para generar un número único (DBID) para la base de datos clonada diferenciándola de la base de datos de origen.

Desactive la casilla de comprobación si desea asignar el DBID de la base de datos de origen a la base de datos clonada. En esta situación, si desea registrar la base de datos clonada en el catálogo de RMAN externo donde la base de datos de origen ya está registrada, se produce un error en la operación.
  - f. Active la casilla de verificación **Create tempfile for temporary tablespace** si desea crear un archivo temporal para el tablespace temporal por defecto de la base de datos clonada.
  - g. En **Introduzca las entradas sql que se aplicarán cuando se cree el clon**, agregue las entradas sql que desea aplicar cuando se cree el clon.
  - h. En **Introduzca los scripts que se ejecutarán después de la operación de clonación**, especifique la ruta de acceso y los argumentos del postscript que desea ejecutar después de la operación de clonación.
11. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
12. Revisa el resumen y luego selecciona **Finalizar**.
13. Supervise el progreso de la operación seleccionando **Monitor > Trabajos**.

### Clonar una base de datos conectable

Es posible clonar una base de datos conectables (PDB) en una base de datos diferente o la misma CDB objetivo en el mismo host o alternativo. También es posible recuperar la PDB clonada en un SCN o la fecha y la hora que deseé.

### 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 **Base de datos o Grupo de recursos** en la lista Ver.
3. Seleccione la base de datos del tipo instancia única (multitenant).

4. En la página Manage Copies view, seleccione el backup en el sistema de almacenamiento principal.
5. Seleccione el backup y, a continuación, haga clic en .
6. En la página Nombre, seleccione **PDB Clone** y especifique los otros detalles.
7. En la página Locations, especifique los detalles necesarios.
8. En la página Pre-Ops, especifique la ruta y los argumentos de los scripts previos, y en la sección Database Parameter settings, modifique los valores de los parámetros de la base de datos completados automáticamente que se utilizan para inicializar la base de datos.
9. En la página Post-Ops, se selecciona **Until Cancel** de forma predeterminada para realizar la recuperación de la base de datos clonada.
  - a. Si selecciona **Until Cancel**, SnapCenter realiza la recuperación mediante el montaje de la última copia de seguridad de registros que tiene la secuencia ininterrumpida de registros de archivos después de esa copia de seguridad de datos que se seleccionó para la clonación.
  - b. Si selecciona **Fecha y hora**, SnapCenter recupera la base de datos hasta una fecha y hora especificadas.
  - c. Si selecciona **Especificar ubicaciones de archive log externas**, SnapCenter identifica y monta el número óptimo de copias de seguridad de log según el SCN especificado o la fecha y hora seleccionadas.
  - d. Por defecto, la casilla de verificación **Crear nuevo DBID** está seleccionada para generar un número único (DBID) para la base de datos clonada diferenciándola de la base de datos de origen.

Desactive la casilla de comprobación si desea asignar el DBID de la base de datos de origen a la base de datos clonada. En esta situación, si desea registrar la base de datos clonada en el catálogo de RMAN externo donde la base de datos de origen ya está registrada, se produce un error en la operación.
  - e. Active la casilla de verificación **Create tempfile for temporary tablespace** si desea crear un archivo temporal para el tablespace temporal por defecto de la base de datos clonada.
  - f. En **Introduzca las entradas sql que se aplicarán cuando se cree el clon**, agregue las entradas sql que desea aplicar cuando se cree el clon.
  - g. En **Introduzca los scripts que se ejecutarán después de la operación de clonación**, especifique la ruta de acceso y los argumentos del postscript que desea ejecutar después de la operación de clonación.
10. En la página Notification, en la lista desplegable **Email preference**, seleccione los escenarios en los que desea enviar los correos electrónicos.
11. Revisa el resumen y luego selecciona **Finalizar**.
12. Supervise el progreso de la operación seleccionando **Monitor > Trabajos**.

## **Información de copyright**

Copyright © 2026 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.