



# Administración de UNIX

## SnapManager for SAP

NetApp  
April 19, 2024

# Tabla de contenidos

- Administración de UNIX . . . . . 1
  - Información general del producto . . . . . 1
  - Configurando SnapManager . . . . . 21
  - Seguridad y gestión de credenciales . . . . . 30
  - Gestionar perfiles para backups eficientes . . . . . 40
  - Realizar backups de bases de datos . . . . . 58
  - Programación de backups de bases de datos . . . . . 94
  - Restaurar backups de base de datos . . . . . 100
  - Clonar el backup de bases de datos . . . . . 137
  - Introducción a la protección de datos en SnapManager . . . . . 157
  - SnapManager para SAP utiliza Protection Manager para proteger un backup de base de datos . . . . . 175
  - Realizando operaciones de gestión . . . . . 194
  - Configuración de una notificación por correo electrónico . . . . . 196
  - Creación de archivos de especificación de tareas y secuencias de comandos para operaciones de SnapManager . . . . . 206
  - Actualizar el nombre del sistema de almacenamiento y el nombre de host de la base de datos de destino asociados con un perfil . . . . . 230
  - Mantener el historial de operaciones de SnapManager . . . . . 234
  - Uso de BR\*Tools con SnapManager para SAP . . . . . 237
  - Referencia de comandos de SnapManager para SAP . . . . . 248
  - Resolución de problemas de SnapManager . . . . . 369
  - Clasificación de mensajes de error . . . . . 401
  - Mensajes de error . . . . . 403

# Administración de UNIX

## Información general del producto

SnapManager para SAP automatiza y simplifica los procesos manuales asociados a operaciones como el backup, la recuperación y el clonado de bases de datos, tareas de gran complejidad y que requieren mucho tiempo. Puede usar SnapManager con la tecnología SnapMirror de ONTAP para crear copias de backups en otro volumen, y también con la tecnología ONTAP SnapVault para archivar backups de forma eficiente a disco.

SnapManager proporciona las herramientas necesarias, como Unified Manager de OnCommand e integración con BR\* Tools de SAP, para realizar la administración de datos basada en normativas, programar y crear backups regulares de bases de datos, así como restaurar datos de estos backups en caso de pérdida o desastre.

SnapManager también se integra con tecnologías nativas de Oracle, como Real Application Clusters (Oracle RAC) y Oracle Recovery Manager (RMAN) para conservar la información de backup. Posteriormente, se pueden utilizar estos backups en operaciones de restauración a nivel de bloque o de recuperación de un momento específico en el espacio de tabla.

## Aspectos destacados de SnapManager

SnapManager integra perfectamente con bases de datos en el host UNIX y con las tecnologías de Snapshot, SnapRestore y FlexClone en back-end. Ofrece una interfaz de usuario (UI) fácil de usar y una interfaz de línea de comandos (CLI) para funciones administrativas.

SnapManager permite realizar las siguientes operaciones de base de datos y gestionar los datos de forma eficiente:

- Creación de backups con gestión eficiente del espacio en almacenamiento primario o secundario

SnapManager permite realizar backups de los archivos de datos y los archivos de registro de archivos por separado.

- Programación de backups
- Restauración de bases de datos completas o parciales mediante una operación de restauración basada en archivos o volúmenes
- Recuperación de bases de datos mediante la detección, el montaje y la aplicación de archivos de registro de archivos a partir de backups
- Eliminar archivos de registro de archivos de destinos de registro de archivos cuando se crean backups solo de los registros de archivos
- Si se conserva un número mínimo de backups de registros de archivos automáticamente, solo se deben retener los backups que contienen archivos únicos de registro de archivos
- Realizar un seguimiento de los detalles de las operaciones y generar informes
- Verificación de copias de seguridad para garantizar que las copias de seguridad tienen un formato de bloque válido y que ninguno de los archivos de copia de seguridad está dañado
- Mantener un historial de operaciones realizadas en el perfil de base de datos

Un perfil contiene información acerca de la base de datos que va a gestionar SnapManager.

- Crear clones de backups con gestión eficiente del espacio en el almacenamiento principal o secundario

SnapManager permite dividir el clon de una base de datos.

## Crear backups usando copias de Snapshot

SnapManager permite crear backups en el almacenamiento primario (local) y en el almacenamiento secundario (remoto) mediante políticas de protección o scripts postprocesamiento.

Los backups que se crean como copias Snapshot son copias virtuales de la base de datos y se almacenan en el mismo medio físico que la base de datos. Por consiguiente, la operación de backup requiere menos tiempo y mucho menos espacio que los backups completos de disco a disco. SnapManager permite realizar el backup de los siguientes elementos:

- Todos los archivos de datos, los archivos de registro de archivo y los archivos de control
- Los archivos de datos o espacios de tablas seleccionados, todos los archivos de registro de archivo y los archivos de control

SnapManager 3.2 o posterior le permite realizar, opcionalmente, el backup de lo siguiente:

- Todos los archivos de datos y los archivos de control
- Los archivos de datos o tablespaces seleccionados junto con los archivos de control
- Archivos de registro de archivo



Los archivos de datos, los archivos de registro de archivos y los archivos de control pueden ubicarse en diferentes sistemas de almacenamiento, volúmenes de sistema de almacenamiento y números de unidad lógica (LUN). También se puede usar SnapManager para realizar backup de una base de datos cuando hay varias bases de datos en el mismo volumen o LUN.

## Por qué debe prune los archivos de registro de archivos

SnapManager para SAP le permite eliminar archivos de registro de archivos del sistema de archivos activo de del que ya se ha realizado un backup.

Eliminar permite a SnapManager crear backups de diferentes archivos de registro de archivos. Eliminar, junto con la política de retención de backups, libera espacio en los registros de archivos cuando se purgan los backups.



No es posible reducir los archivos de registro de archivos cuando el área de recuperación flash (FRA) está habilitada para los archivos de registro de archivos. Si especifica la ubicación del registro de archivos en el área de recuperación de flash, asegúrese de especificar también la ubicación del registro de archivos en el `archive_log_dest` parámetro.

## Consolidación de registros de archivo

SnapManager (3.2 o posterior) para SAP consolida los backups de registros de archivos

a fin de mantener un número mínimo de backups para los archivos de registro de archivos. SnapManager para SAP identifica y libera los backups que contienen archivos de registros de archivos que son subconjuntos de otros backups.

## **Restauración total o parcial de bases de datos**

SnapManager proporciona la flexibilidad necesaria para restaurar bases de datos completas, espacios de tablas específicos, archivos, archivos de control o una combinación de estas entidades. SnapManager le permite restaurar datos mediante un procesador de restauración basado en archivos un proceso de restauración más rápido y basado en volúmenes. Los administradores de bases de datos pueden seleccionar el proceso que desean utilizar o dejar que SnapManager decida qué proceso es apropiado.

SnapManager permite a los administradores de bases de datos obtener una vista previa de las operaciones de restauración. La función de vista previa permite a los administradores de bases de datos ver cada operación de restauración archivo por archivo.

Los administradores de bases de datos pueden especificar el nivel en el que SnapManager restaura y recupera la información cuando se ejecutan operaciones de restauración. Por ejemplo, los administradores de bases de datos pueden restaurar y recuperar datos en momentos específicos. El punto de restauración puede ser una fecha y hora, o un número de cambio de sistema (SCN) de Oracle.

SnapManager (3.2 o posterior) permite restaurar y recuperar backups de bases de datos de forma automática sin intervención del administrador de base de datos. Es posible usar SnapManager para crear backups de registros de archivo, y luego usarlos para restaurar y recuperar los backups de bases de datos. Aunque los archivos de registro de archivo del backup se gestionen en una ubicación de un registro de archivo externo, puede especificar esa ubicación externa para que los registros de archivos puedan ayudar a recuperar la base de datos restaurada.

## **Comprobar el estado del backup**

SnapManager puede confirmar la integridad del backup mediante las operaciones estándar de verificación de backup de Oracle.

Los administradores de bases de datos pueden realizar la verificación como parte de la operación de backup o al mismo tiempo. Los administradores de bases de datos pueden configurar la operación de verificación para que se produzca durante un tiempo de pico de actividad cuando la carga en los servidores host es menor o durante un período de mantenimiento programado.

## **Clones de backups de bases de datos**

SnapManager utiliza la tecnología FlexClone para crear un clon modificable de un backup de base de datos con un uso eficiente del espacio. Es posible modificar un clon sin cambiar el origen de backup.

Quizás sería conveniente clonar bases de datos para permitir pruebas o actualizaciones en entornos no productivos. Es posible clonar una base de datos que reside en el almacenamiento secundario primor. Puede ubicarse un clon en el mismo host o en otro que la base de datos.

La tecnología FlexClone permite a SnapManager utilizar copias snapshot de la base de datos para evitar crear una copia física completa de disco a disco. Las copias Snapshot requieren menos tiempo de creación y

ocupan mucho menos espacio que las copias físicas.

Consulte la documentación de Data ONTAP para obtener más información sobre la tecnología FlexClone.

## Información relacionada

["Documentación de Data ONTAP"](#)

## Realizar un seguimiento de los detalles y generar informes

SnapManager reduce el nivel de detalle que los administradores de las bases de datos necesitan para realizar un seguimiento del estado de las diferentes operaciones mediante la oferta de métodos para supervisar las operaciones desde una única interfaz.

Una vez que los administradores especifican qué bases de datos deben realizarse backups, SnapManager identifica automáticamente los archivos de la base de datos para el backup. SnapManager muestra información sobre repositorios, hosts, perfiles, backups y clones. Puede supervisar las operaciones en hosts o bases de datos específicos. También puede identificar los backups protegidos y determinar si los backups están en proceso o si están programados para producirse.

## Qué repositorios son

SnapManager organiza la información en perfiles, que a continuación se asocian con repositorios. Los perfiles contienen información acerca de la base de datos que se está gestionando, mientras que el repositorio contiene datos acerca de las operaciones que se realizan en los perfiles.

El repositorio registra el momento en que se realizó un backup, qué archivos se hicieron de backup y si se creó un clon a partir del backup. Cuando los administradores de bases de datos restauran una base de datos o recuperan una parte del mismo, SnapManager consulta el repositorio para determinar qué se ha realizado un backup.

Como el repositorio almacena los nombres de las copias Snapshot de la base de datos creadas durante las operaciones de backup, la base de datos del repositorio no puede existir en la misma base de datos y tampoco puede formar parte de la misma base de datos de la que se realiza el backup de SnapManager. Debe tener al menos dos bases de datos (la base de datos del repositorio de SnapManager y la base de datos de destino que gestiona SnapManager) en funcionamiento cuando se ejecutan operaciones de SnapManager.

Si intenta abrir la interfaz gráfica de usuario (GUI) cuando la base de datos del repositorio está inactiva, el siguiente mensaje de error se registra en el `sm_gui.log` Archivo: [ADVERTIR]: SMSAP-01106: Error occurred while querying the repository: No more data to read from socket. Además, se produce un error en las operaciones de SnapManager cuando la base de datos del repositorio está inactiva. Para obtener más información acerca de los diferentes mensajes de error, consulte *solución de problemas conocidos*.

Es posible usar cualquier nombre de host, nombre de servicio o nombre de usuario válido para realizar operaciones. Para que un repositorio admita operaciones SnapManager, el nombre de usuario y el nombre de servicio del repositorio sólo deben contener los siguientes caracteres: Caracteres alfabéticos (A-Z), dígitos (0-9), signo menos (-), guión bajo (\_) y punto (.).

El puerto de repositorio puede ser cualquier número de puerto válido y el nombre de host del repositorio puede ser cualquier nombre de host válido. El nombre de host debe estar formado por caracteres alfabéticos (A-Z), dígitos (0-9), signo menos (-) y punto (.), pero no un guión bajo (\_).

El repositorio debe crearse en una base de datos de Oracle. La base de datos que utiliza SnapManager debe configurarse de acuerdo con los procedimientos de Oracle para la configuración de la base de datos.

Un único repositorio puede contener información acerca de varios perfiles; sin embargo, cada base de datos normalmente se asocia a un único perfil. Puede tener varios repositorios, donde cada repositorio contiene varios perfiles.

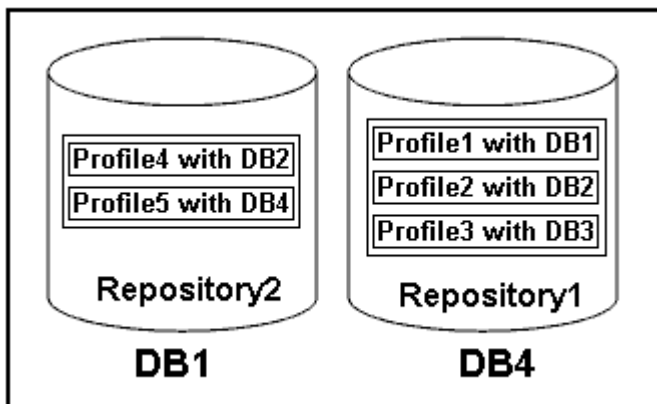
## Qué perfiles son

SnapManager utiliza perfiles para almacenar la información necesaria para realizar operaciones en una base de datos determinada. Un perfil contiene información sobre la base de datos, incluidas sus credenciales, backups y clones. Al crear un perfil, no es necesario especificar los detalles de la base de datos cada vez que se realiza una operación en esa base de datos.

Un perfil sólo puede hacer referencia a una base de datos. Más de un perfil puede hacer referencia a la misma base de datos. No es posible acceder a los backups creados con un perfil desde otro perfil, aunque ambos perfiles hagan referencia a la misma base de datos.

La información del perfil se almacena en un repositorio. El repositorio contiene información de perfil de la base de datos e información sobre las copias de Snapshot que sirven como backup de base de datos. Las copias Snapshot reales se almacenan en el sistema de almacenamiento. Los nombres de las copias Snapshot se almacenan en el repositorio que contiene el perfil de esa base de datos. Cuando se realiza una operación en una base de datos, debe seleccionar el perfil en el repositorio.

La siguiente figura muestra cómo los repositorios pueden contener varios perfiles, pero también que cada perfil puede definir sólo una base de datos:



En el ejemplo anterior, deleteRepository2 se encuentra en la base de datos DB1 y deleteRepository1 en la base de datos DB4.

Cada perfil contiene las credenciales de la base de datos asociada al perfil. Las credenciales permiten que SnapManager se conecte a la base de datos y trabaje con ella. Las credenciales almacenadas incluyen el nombre de usuario y las parejas de contraseñas para acceder al host, al repositorio, a la base de datos y a la información de conexión necesaria si utiliza Oracle Recovery Manager (RMAN).

No se puede acceder a un backup que se creó con un perfil de otro perfil, incluso si los dos perfiles están asociados con la misma base de datos. SnapManager coloca un bloqueo en la base de datos para evitar que se realicen dos operaciones incompatibles a la vez.

## Perfil para crear copias de seguridad completas y parciales

Puede crear perfiles para realizar copias de seguridad completas o parciales.

Los perfiles que se especifican para crear las copias de seguridad completas y parciales contienen tanto los archivos de datos como los archivos de registro de archivos. SnapManager no permite que dichos perfiles separen los backups de registros de archivo de los backups del archivo de datos. Los backups completos y parciales se retienen en función de las políticas de retención de backup existentes y se protegen de acuerdo con las políticas de protección existentes. Puede programar copias de seguridad completas y parciales en función del tiempo y la frecuencia que mejor le convenga.

## Perfiles para la creación de copias de seguridad sólo de archivos de datos y copias de seguridad de sólo registro de archivos

SnapManager (3.2 o posterior) permite crear perfiles para realizar backups de los archivos de registro de archivos independientemente de los archivos de datos. Después de usar el perfil para separar los tipos de backup, es posible crear backups de solo los archivos de datos o backups de solo registros de archivos de la base de datos. También es posible crear un backup que contenga los archivos de datos y los archivos de registro de archivos juntos.

La política de retención se aplica a todos los backups de la base de datos cuando no están separados los backups de registros de archivos. Después de separar los backups de registros de archivos, SnapManager permite especificar diferentes duraciones de retención y políticas de protección para los backups de registros de archivos.

## Política de retención

SnapManager determina si se debe retener un backup teniendo en cuenta el número de retención (por ejemplo, 15 backups) y la duración de la retención (por ejemplo, 10 días de backups diarios). Una copia de seguridad caduca cuando su antigüedad supera el período de retención establecido para su clase de retención y la cantidad de backups supera el número de retención. Por ejemplo, si el número de backup es 15 (lo que significa que SnapManager ha tomado 15 backups correctos) y se establece el requisito de duración para 10 días de backups diarios, los cinco backups más antiguos, correctos y elegibles caducan.

## Duración de la retención del registro de archivo


Una vez separados los backups de los registros de archivos, se retienen en función de la duración de la retención de los registros de archivos. Los backups de registros de archivo que se realizan con los backups de archivos de datos siempre se conservan junto con estos backups de archivos de datos, independientemente de la duración de la retención de registros de archivo.

## Qué son los estados de operación de SnapManager

Las operaciones de SnapManager (backup, restauración y clonado) pueden estar en diferentes estados y cada estado indica el progreso de la operación.

Estado de la operación	Descripción
Correcto	La operación se ha completado correctamente.



Estado de la operación	Descripción
Ejecutando	La operación se inició, pero no ha finalizado. Por ejemplo, se programa que un backup, que tarda dos minutos, se lleve a cabo a las 11:00. Al ver la ficha <b>Programación</b> a las 11:01 a.m., la operación aparece como en ejecución.
No se ha encontrado ninguna operación	La programación no se ha ejecutado o se ha eliminado la última copia de seguridad ejecutada.
Error	<p data-bbox="402 491 1489 562">Error en la operación. SnapManager ha ejecutado automáticamente el proceso de anulación y ha limpiado la operación.</p> <div data-bbox="435 590 1489 716" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p data-bbox="553 604 1484 709">Es posible dividir el clon que se crea. Cuando se detiene la operación de división de clones que se inició y la operación se detiene correctamente, el estado de la operación de división de clones muestra como error.</p> </div>

### Eventos recuperables e irrecuperables

Un evento SnapManager recuperable tiene los siguientes problemas:

- La base de datos no se almacena en un sistema de almacenamiento que ejecuta Data ONTAP.
- SnapDrive para UNIX no está instalado o no puede acceder al sistema de almacenamiento.
- SnapManager no puede crear una copia Snapshot o aprovisionar almacenamiento si el volumen no tiene espacio, se alcanzó el número máximo de copias Snapshot o se produce una excepción no prevista.

Cuando se produce un evento recuperable, SnapManager realiza un proceso de anulación e intenta devolver el host, la base de datos y el sistema de almacenamiento al estado inicial. Si el proceso de anulación falla, SnapManager trata el incidente como un evento irrecuperable.

Un evento irrecuperable (fuera de banda) se produce cuando se produce cualquiera de los siguientes acontecimientos:

- Se produce un problema con el sistema, como cuando se produce un error en un host.
- Se ha detenido el proceso SnapManager.
- Se produce un error en una operación de anulación en banda cuando el sistema de almacenamiento falla, el número de unidad lógica (LUN) o el volumen de almacenamiento están sin conexión o la red falla.

Cuando se produce un evento irrecuperable, SnapManager realiza un proceso de cancelación inmediatamente. Es posible que el host, la base de datos y el sistema de almacenamiento no regresen a los estados iniciales. Si este es el caso, debe realizar una limpieza después de que la operación SnapManager falle; para ello, elimine la copia snapshot huérfana y elimine el archivo de bloqueo de SnapManager.

Si desea eliminar el archivo de bloqueo de SnapManager, vaya a. \$ORACLE\_HOME en la máquina de destino y elimine sm\_lock\_TargetDBName archivo. Después de eliminar el archivo, debe reiniciar SnapManager para el servidor SAP.

## Cómo mantiene SnapManager la seguridad

Es posible realizar operaciones de SnapManager solo si cuenta con las credenciales adecuadas. La seguridad en SnapManager está regida por la autenticación de usuarios y el control de acceso basado en roles (RBAC). RBAC permite que los administradores de bases de datos restrinjan las operaciones que SnapManager puede realizar en los volúmenes y LUN que contienen los archivos de datos de una base de datos.

Los administradores de bases de datos habilitan el RBAC para SnapManager mediante SnapDrive. A continuación, los administradores de bases de datos asignan permisos a los roles de SnapManager y asignan estos roles a los usuarios en la interfaz gráfica de usuario (GUI) o la interfaz de línea de comandos (CLI) de Operations Manager. Las comprobaciones de permisos de RBAC se realizan en DataFabric Manager Server.

Además del acceso basado en roles, SnapManager mantiene la seguridad mediante la solicitud de autenticación de usuario mediante solicitudes de contraseña o la configuración de credenciales de usuario. Un usuario efectivo se autentica y autoriza con el servidor SnapManager.

Las credenciales de SnapManager y la autenticación de usuario difieren significativamente de SnapManager 3.0:

- En las versiones de SnapManager anteriores a la 3.0, debe establecer una contraseña de servidor arbitraria al instalar SnapManager. Cualquier persona que desee utilizar el servidor SnapManager necesitará la contraseña del servidor SnapManager. La contraseña del servidor SnapManager se debería añadir a las credenciales de usuario mediante el `smsap credential set -host` comando.
- En SnapManager (3.0 y posterior), la contraseña del servidor SnapManager ha sido sustituida por la autenticación individual del sistema operativo (SO) de usuario. Si no ejecuta el cliente desde el mismo servidor que el host, el servidor SnapManager realiza la autenticación con los nombres de usuario y contraseñas del sistema operativo. Si no desea que se le soliciten las contraseñas del sistema operativo, puede guardar los datos en la caché de credenciales de usuario de SnapManager mediante el `smsap credential set -host` comando.



La `smsap credential set -host` el comando recuerda sus credenciales cuando el `host.credentials.persist` la propiedad del archivo `smsap.config` está establecida en **true**.

### ejemplo

User1 y User2 comparten un perfil denominado Pro2. User2 no puede realizar una copia de seguridad de Database1 en Host1 sin permiso para acceder a Host1. User1 no puede clonar una base de datos a Host3 sin permiso para acceder a Host3.

En la siguiente tabla se describen los diferentes permisos asignados a los usuarios:

Tipo de permiso	Usuario1	Usuario2
Contraseña del host	Host1, Host2	Host2, Host3
Contraseña de repositorio	Repo. 1	Repo. 1
Contraseña de perfil	Pro1, Pro2	Profeca2

En caso de que User1 y User2 no tengan ningún perfil compartido, supongamos que User1 tiene permisos para los hosts denominados Host1 y Host2 y que User2 tiene permisos para el host denominado Host2. User2 no puede ejecutar ni siquiera los comandos que no son de perfil, como `dump y. system verify` En Host1.

## Acceder a la ayuda en línea e imprimirla

La Ayuda en línea proporciona instrucciones para las tareas que puede realizar mediante la interfaz gráfica de usuario de SnapManager. La Ayuda en línea también proporciona descripciones de los campos de las ventanas y asistentes.

### Pasos

1. Ejecute una de las siguientes acciones:
  - En la ventana principal, haga clic en **Ayuda > Contenido de la Ayuda**.
  - En cualquier ventana o asistente, haga clic en **Ayuda** para ver la ayuda específica de esa ventana.
2. Utilice **Tabla de contenido** en el panel izquierdo para navegar por los temas.
3. Haga clic en el icono impresora situado en la parte superior de la ventana de ayuda para imprimir temas individuales.

## Diseños generales de bases de datos y configuraciones de almacenamiento recomendados

Conocer los diseños generales recomendados de las bases de datos y las configuraciones de almacenamiento puede ayudarle a evitar problemas relacionados con los grupos de discos, los tipos de archivos y los espacios de tablas.

- No incluya archivos de más de un tipo de sistema de archivos SAN o administrador de volúmenes en la base de datos.

Todos los archivos que conforman una base de datos deben residir en el mismo tipo de sistema de archivos.

- SnapManager requiere un gran tamaño de bloque de 4 KB.
- Incluya el identificador del sistema de la base de datos en la `oratab` archivo.

Incluya una entrada en la `oratab` archivo para cada base de datos que se va a gestionar. SnapManager confía en el `oratab` Archivo para determinar qué directorio raíz de Oracle utilizar.

Si desea aprovechar la nueva restauración basada en volúmenes o la restauración de grupos de discos completos, tenga en cuenta las siguientes directrices relacionadas con los sistemas de archivos y los grupos de discos:

- Un grupo de discos que contiene archivos de datos no puede contener otros tipos de archivos.
- El número de unidad lógica (LUN) para el grupo de discos de archivos de datos debe ser el único objeto del volumen de almacenamiento.

A continuación se muestran algunas directrices para la separación de volúmenes:

- Los archivos de datos de una sola base de datos deben estar en el volumen.

- Debe utilizar volúmenes independientes para cada una de las siguientes clasificaciones de archivos: Archivos binarios de base de datos, archivos de datos, archivos redo log en línea, archivos redo log archivados y archivos de control.
- No es necesario crear un volumen separado para los archivos de base de datos temporales, ya que SnapManager no realiza backups de archivos de base de datos temporales.

SAP utiliza un diseño estándar para instalaciones de bases de datos Oracle. En este diseño, SAP coloca copias del archivo de control de Oracle en E:\oracle\SID\origlogA, E:\oracle\SID\origlogB, y E:\oracle\SID\sapdata1 file systems.

El archivo de control del sistema de archivos sapdata1 entra en conflicto con los requisitos de la SnapManager para separar los archivos de control y los archivos de datos en volúmenes separados y se debe ajustar para permitir una funcionalidad de restauración rápida.



Como los backups BR\*Tools incluyen los perfiles Oracle y SAP ubicados en el subdirectorio DBS de la instalación de Oracle, la instalación de Oracle debe estar ubicada en el almacenamiento.

En el caso de una nueva instalación, puede modificar la ubicación de los archivos de control utilizando SAPINST y mover el archivo de control normalmente colocado en el sistema de archivos sapdata1 a un sistema de archivos que no reside en el mismo volumen que los archivos de datos. (SAPINST es la herramienta que proporciona SAP para la instalación de sistemas SAP.)

Sin embargo, en el caso de un sistema que ya se ha instalado, debe mover el archivo de control desde el sistema de archivos para permitir una restauración rápida mediante SnapManager. Para ello, cree un nuevo sistema de archivos en un volumen que no contenga archivos de datos, mueva el archivo de control a ese sistema de archivos y, a continuación, cree un enlace simbólico desde el sistema de archivos anterior al directorio del nuevo sistema de archivos. Es necesario detener SAP y Oracle Database al mover el archivo de control para evitar errores en la base de datos.

Antes de realizar cualquier modificación, la lista de los archivos en el directorio sapdata1 que contiene el archivo de control podría tener este aspecto:

```
hostname:/
# ls -l /oracle/SID/sapdata1/cntrl
-rw-r----- 1 orasid dba 9388032 Jun 19 01:51 cntrlSID.dbf
```

Después de la modificación, el listado podría tener este aspecto:

```
hostname:/
# ls -sl /oracle/SID/sapdata1
0 lrwxrwxrwx 1 root root 19 2008-08-06 14:55 cntrl -> /oracle/SID/control
0 -rw-r--r-- 1 root root 0 2008-08-06 14:57 data01.dbf

# ls -sl /oracle/SID/control
0 -rw-r--r-- 1 root root 0 2008-08-06 14:56 cntrlSID.dbf
```

## Defina el inicio de la base de datos con el archivo oratab

SnapManager utiliza la `oratab` Archivo durante las operaciones para determinar el directorio inicial de la base de datos Oracle. Debe haber una entrada para la base de datos de Oracle en `oratab` Archivo para que SnapManager funcione correctamente. La `oratab` El archivo se crea durante la instalación del software Oracle.



El directorio inicial de Oracle se establece en la `oratab` Archivo para sistemas SAP, del mismo modo que lo es para sistemas Oracle. Los sistemas SAP también disponen de un directorio inicial de la base de datos, que se suele utilizar `/oracle/SID/xxx_yy`, donde `xxx` representa la versión de la base de datos y `yy` es 32 o 64.

La `oratab` el archivo reside en diferentes ubicaciones según el sistema operativo del host, como se muestra en la siguiente tabla:

Sistema operativo del host	Ubicación del archivo
Linux	<code>/etc/oratab</code>
Solaris	<code>/var/opt/oracle/oratab</code>
IBM AIX	<code>/etc/oratab</code>

La muestra `oratab` el archivo contiene la siguiente información:

```
+ASM1:/u01/app/11.2.0/grid:N # line added by Agent
oelpro:/u01/app/11.2.0/oracle:N # line added by Agent
# SnapManager generated entry (DO NOT REMOVE THIS LINE)
smsapclone:/u01/app/11.2.0/oracle:N
```



Después de instalar Oracle, debe asegurarse de que `oratab` el archivo reside en la ubicación especificada en la tabla anterior. Si la `oratab` el archivo no reside en la ubicación correcta de acuerdo con su sistema operativo, debe ponerse en contacto con el soporte técnico para obtener ayuda.

## Requisitos para usar bases de datos de RAC con SnapManager

Debe conocer las recomendaciones para usar bases de datos de Real Application Clusters (RAC) con SnapManager. Las recomendaciones incluyen números de puerto, contraseñas y modo de autenticación.

- En el modo de autenticación de la base de datos, el listener de cada nodo que interactúa con una instancia de la base de datos RAC debe configurarse para que utilice el mismo número de puerto.

El listener que interactúa con la instancia de base de datos primaria debe iniciarse antes de iniciar el backup.

- En modo de autenticación del sistema operativo, el servidor SnapManager debe estar instalado y ejecutándose en cada nodo del entorno RAC.
- La contraseña de usuario de la base de datos (por ejemplo, para un administrador del sistema o un usuario con el privilegio sysdba) debe ser la misma para todas las instancias de la base de datos Oracle en un entorno RAC.

### Dispositivos de partición compatibles

Debe conocer los diferentes dispositivos de partición compatibles con SnapManager.

La siguiente tabla proporciona información de partición y cómo se puede activar para diferentes sistemas operativos:

De NetApp	Partición única	Partición múltiple	Dispositivos sin partición	Sistema de archivos o dispositivos RAW
5 veces Red Hat Enterprise Linux o. 5 veces Oracle Enterprise Linux	Sí	No	No	ext3*
Red Hat Enterprise Linux 6 veces o. 6 veces Oracle Enterprise Linux	Sí	No	No	ext3 o ext4*
SUSE Linux Enterprise Server 11	Sí	No	No	ext3*
SUSE Linux Enterprise Server 10	No	No	Sí	ext3***

Para obtener más información sobre las versiones compatibles del sistema operativo, consulte la matriz de interoperabilidad.

### Requisitos para usar bases de datos con NFS y SnapManager

Debe conocer los requisitos para usar las bases de datos con sistema de archivos de red (NFS) y SnapManager. Las recomendaciones incluyen ejecutarse como raíz, caché de atributos y enlaces simbólicos.

- Debe ejecutar SnapManager como raíz; SnapManager debe poder acceder a los sistemas de archivos que contienen archivos de datos, archivos de control, registros de recuperación en línea, registros de archivos y el origen de la base de datos.

Establezca una de las siguientes opciones de exportación NFS para garantizar que root pueda acceder a los sistemas de archivos:

- raíz=*host name*

◦ `rw=host name, anon=0`

- Debe deshabilitar el almacenamiento en caché de atributos para todos los volúmenes que contienen archivos de datos de base de datos, archivos de control, registros de recuperación y archivos, así como el inicio de la base de datos.

Exporte los volúmenes con las opciones `noac` (para Solaris y AIX) o `actimeo=0` (para Linux).

- Debe vincular los archivos de datos de la base de datos del almacenamiento local a NFS para admitir enlaces simbólicos solamente en el nivel de punto de montaje.

## Ejemplos de distribuciones de volúmenes de base de datos

Puede consultar ejemplos de diseños de volumen de base de datos para obtener ayuda en la configuración de la base de datos.

### Bases de datos de instancia única

Tipos de archivo	Nombres de volúmenes	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Binarios de Oracle	<code>orabin_host name</code>	Sí	Encendido
Archivos de datos	<code>oradata_sid</code>	Sí	Apagado
Archivos de datos temporales	<code>temp_sid</code>	Sí	Apagado
Archivos de control	<code>oracntrl01_sid</code> (Multiplexado) <code>oracntrl02_sid</code> (Multiplexado)	Sí	Apagado
Rehacer registros	<code>oralog01_sid</code> (Multiplexado) <code>oralog02_sid</code> (Multiplexado)	Sí	Apagado
Registros de archivo	<code>oraarch_sid</code>	Sí	Apagado

### Bases de datos de Real Application Clusters (RAC)

Tipos de archivo	Nombres de volúmenes	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Binarios de Oracle	<i>orabin_host name</i>	Sí	Encendido
Archivos de datos	<i>oradata_dbname</i>	Sí	Apagado
Archivos de datos temporales	<i>temp_dbname</i>	Sí	Apagado
Archivos de control	<i>oracntrl01_dbname</i> (Multiplexado) <i>oracntrl02_dbname</i> (Multiplexado)	Sí	Apagado
Rehacer registros	<i>oralog01_dbname</i> (Multiplexado) <i>oralog02_dbname</i> (Multiplexado)	Sí	Apagado
Registros de archivo	<i>oraarch_dbname</i>	Sí	Apagado
Archivos de cluster	<i>oracrs_clustername</i>	Sí	Encendido

## Limitaciones al trabajar con SnapManager

Debe conocer las situaciones y las limitaciones que pueden afectar a su entorno.

### Limitaciones relacionadas con diseños y plataformas de bases de datos

- SnapManager admite archivos de control en un sistema de archivos y no admite archivos de control en dispositivos RAW.
- SnapManager funciona en un entorno de cluster Microsoft (MSCS), pero no reconoce el estado de la configuración MSCS (activo o pasivo) y no transfiere la administración activa de un repositorio a un servidor en espera en un clúster MSCS.
- En Red Hat Enterprise Linux (RHEL) y Oracle Enterprise Linux 4.7, 5.0, 5.1, 5.2 y 5.3 El sistema de archivos ext3 no es compatible al poner en marcha Oracle en dispositivos sin formato mediante multivía dinámica (DMP) en un entorno de I/O de red multivía (MPIO).

Este problema se observa en SnapManager solo cuando se utiliza SnapDrive 4.1 para UNIX o versiones anteriores.

- SnapManager en RHEL no admite particiones de discos mediante la utilidad **parted**.



Esto es un problema con la utilidad RHEL **parted**.

- En una configuración de RAC, cuando se actualiza un nombre de perfil desde el nodo RAC A, el archivo de programación del perfil se actualiza sólo para el nodo RAC A.

El archivo de programación para el mismo perfil en el nodo B de RAC no se actualiza y contiene la información de programación anterior. Cuando se activa un backup programado en el nodo B, se produce un error en la operación de backup programada, ya que el nodo B contiene el archivo de programación anterior. Sin embargo, la operación de copia de seguridad programada se realiza correctamente desde el nodo A, en el que se cambia el nombre del perfil. Puede reiniciar el servidor SnapManager para recibir el archivo de programación más reciente para el perfil en el nodo B.

- La base de datos del repositorio puede existir en un host al que se puede acceder mediante más de una dirección IP.

Si para acceder al repositorio se utiliza más de una dirección IP, se crea el archivo de programación para cada una de las direcciones IP. Si se crea la copia de seguridad de la programación para un perfil (por ejemplo, perfil A) bajo una de las direcciones IP (por ejemplo, IP1), se actualizará el archivo de planificación para sólo esa dirección IP. Si se accede al perfil A desde otra dirección IP (por ejemplo, IP2), la copia de seguridad programada no aparece porque el archivo de programación de IP2 no tiene una entrada para la programación que se creó en IP1.

Puede esperar a que la programación se active desde esa dirección IP y el archivo de programación que se actualizará o puede reiniciar el servidor.

### **Limitaciones relacionadas con la configuración de SnapManager**

- SnapDrive para UNIX admite más de un tipo de sistema de archivos y administrador de volúmenes en determinadas plataformas.

El sistema de archivos y el gestor de volúmenes utilizados para los archivos de la base de datos deben especificarse en el archivo de configuración de SnapDrive como el sistema de archivos predeterminado y el gestor de volúmenes.

- SnapManager admite bases de datos en sistemas de almacenamiento de MultiStore con los siguientes requisitos:
  - Debe configurar SnapDrive para establecer contraseñas para los sistemas de almacenamiento MultiStore.
  - SnapDrive no puede crear una copia snapshot de una LUN o un archivo que reside en un qtree de un sistema de almacenamiento de MultiStore si el volumen subyacente no está en el mismo sistema de almacenamiento de MultiStore.
- SnapManager no admite el acceso a dos servidores SnapManager que se ejecutan en puertos diferentes desde un único cliente (tanto desde la CLI como desde la GUI).

Los números de puerto deben ser los mismos en los hosts remotos y destino.

- Todas las LUN de un volumen deben estar a nivel de volumen o dentro de qtrees, pero no ambos.

Esto se debe a que, si los datos residen en los qtrees y se monta el volumen, los datos que hay dentro de los qtrees no están protegidos.

- Se produce un error en las operaciones de SnapManager y no se puede acceder a la interfaz gráfica de usuario cuando la base de datos del repositorio está inactiva.

Es necesario verificar que la base de datos del repositorio esté en ejecución cuando se realiza cualquier operación de SnapManager.

- SnapManager no es compatible con la movilidad de particiones activas (LPM) ni con la movilidad de aplicaciones activas (LAM).
- SnapManager no es compatible con Oracle Wallet Manager ni con el cifrado de datos transparente (TDE).
- SnapManager no admite configuraciones MetroCluster en entornos de asignación de dispositivos sin formato (RDM), ya que las configuraciones de MetroCluster aún deben ser compatibles con Virtual Storage Console (VSC).

### Limitaciones relacionadas con la gestión de perfiles

- Si actualiza el perfil para separar los backups de los registros de archivos, no se puede realizar una operación de reversión en el host.
- Si activa un perfil desde la GUI para crear copias de seguridad de registros de archivo y después intenta actualizar el perfil mediante la ventana actualización de perfiles múltiples o la ventana actualización de perfiles, no puede modificar dicho perfil para crear una copia de seguridad completa.
- Si actualiza varios perfiles en la ventana actualización de varios perfiles y algunos perfiles tienen activada la opción **copia de seguridad de archivos** por separado y otros perfiles tienen desactivada la opción, la opción **copia de seguridad de archivos por separado** se desactiva.
- Si actualiza varios perfiles y algunos perfiles tienen activada la opción **copia de seguridad de archivos por separado** y otros perfiles tienen desactivada la opción, la opción **copia de seguridad de archivos por separado** de la ventana actualización de perfiles múltiples está desactivada.
- Si cambia el nombre del perfil, no puede revertir el host.

### Limitaciones relacionadas con las operaciones de actualización o reversión

- Si intenta instalar una versión anterior de SnapManager para un host sin realizar la operación de reversión en el host en el repositorio, es posible que no pueda realizar lo siguiente:
  - Ver los perfiles que se crearon en versiones anteriores o posteriores de SnapManager para el host.
  - Acceda a los backups o clones que se crearon en las versiones anteriores o posteriores de SnapManager.
  - Realice operaciones de reversión o actualización en el host.
- Después de separar los perfiles para crear backups de registro de archivos, no se puede ejecutar una operación de reversión en el repositorio de host relacionado.

### Limitaciones relacionadas con las operaciones de copia de seguridad

- Durante la recuperación, si el backup ya está montado, SnapManager no volverá a montar el backup y utiliza el backup ya montado.

Si el backup está montado por un usuario diferente y no tiene acceso al backup montado anteriormente, el otro usuario debe proporcionarle el permiso.

Todos los archivos de registro de archivos tienen permiso de lectura para los usuarios asignados a un grupo; es posible que no tenga el permiso de acceso al archivo de registro de archivos, si el backup se monta por un grupo de usuarios diferente. Los usuarios pueden otorgar permiso a los archivos de registro de archivos montados manualmente y, a continuación, volver a intentar la operación de restauración o recuperación.

- SnapManager establece el estado de backup como «PROTEGIDO», incluso cuando una de las copias Snapshot del backup de la base de datos se transfiere al sistema de almacenamiento secundario.
- Puede utilizar el archivo de especificación de tareas para la copia de seguridad programada sólo desde SnapManager 3.2 o posterior.
- La integración de SnapManager con Protection Manager permite realizar el backup de varios volúmenes en el almacenamiento principal a un único volumen en el almacenamiento secundario para SnapVault y SnapMirror para qtrees.

No se admite el ajuste de tamaño dinámico de volúmenes secundarios. En la Guía de administración de Provisioning Manager y Protection Manager para usar con DataFabric Manager Server 3.8 encontrará más información al respecto.

- SnapManager no admite copias vault de backups con el script de posprocesamiento.
- Si la base de datos del repositorio apunta a más de una dirección IP y cada dirección IP tiene un nombre de host diferente, la operación de programación de backup se realiza correctamente para una dirección IP, pero falla para la otra dirección IP.
- Después de actualizar a SnapManager 3.4 o una versión posterior, no se podrán actualizar los backups programados con scripts de posprocesamiento que utilicen SnapManager 3.3.1.

Debe eliminar la programación existente y crear una nueva.

### **Limitaciones relacionadas con las operaciones de restauración**

- Cuando se utiliza un método indirecto para realizar una operación de restauración y los archivos de registro de archivos necesarios para la recuperación solo están disponibles en backups desde el sistema de almacenamiento secundario, SnapManager no logra recuperar la base de datos.

Esto se debe a que SnapManager no puede montar el backup de los archivos de registro de archivos desde el sistema de almacenamiento secundario.

- Cuando SnapManager realiza una operación de restauración de volúmenes, no se purgan las copias de backup de registros de archivos que se realizan una vez restaurado el backup correspondiente.

Cuando en el mismo volumen existen los archivos de datos y el destino del archivo de registro de archivos, es posible restaurar los archivos de datos mediante una operación de restauración de volumen si no hay archivos de registro de archivos disponibles en el destino del archivo de registro de archivos. En este caso, se pierden las copias snapshot del registro de archivos que se crean después de la copia de seguridad de los archivos de datos.

No debe eliminar todos los archivos de registro de archivos del destino del registro de archivos.

### **Limitaciones relacionadas con las operaciones de clonación**

- No se puede ver ningún valor numérico entre 0 y 100 en cuanto al progreso de la operación de división de clones debido a la velocidad con la que se detectan y procesan los inodos el sistema de almacenamiento que contiene el volumen flexible.
- SnapManager no admite recibir correos electrónicos solo para las operaciones de división de clones correctamente.
- SnapManager solo admite la división de un FlexClone.
- Se produce un error en la clonación del backup de la base de datos en línea de la base de datos RAC donde se usa la ubicación del archivo de registro de archivos externo debido a un error en la recuperación.

Se produce un error en la clonado porque Oracle no encuentra y aplica los archivos de registro de archivos para la recuperación desde la ubicación del registro de archivos externo. Esta es una limitación de Oracle. Para obtener más información, consulte el ID de error de Oracle: 13528007. Oracle no aplica el registro de archivo desde la ubicación no predeterminada en la "[Sitio de soporte de Oracle](#)". Debe tener un nombre de usuario y una contraseña de Oracle metalink válidos.

- SnapManager 3.3 o versiones posteriores no admiten el uso del archivo XML de especificación del clon creado en las versiones anteriores a SnapManager 3.2.
- Si los espacios de tablas temporales se encuentran en una ubicación diferente a la ubicación de los archivos de datos, una operación de clonado crea los espacios de tabla en la ubicación de los archivos de datos.

Sin embargo, si los espacios de tablas temporales son Oracle Managed Files (OMF) ubicados en una ubicación diferente a la ubicación de los archivos de datos, la operación de clonado no crea los espacios de tablas en la ubicación de los archivos de datos. SnapManager no gestiona los OMF.

- SnapManager no puede clonar una base de datos de RAC si selecciona el `-resetlogs` opción.

### **Limitaciones relacionadas con archivos de registro de archivos y copias de seguridad**

- SnapManager no admite la eliminación de archivos de registro de archivos desde el destino de área de recuperación flash.
- SnapManager no admite la eliminación de archivos de registro de archivos desde el destino en espera.
- Los backups de registros de archivos se retienen en función de la duración de la retención y la clase de retención por horas predeterminada.

Cuando la clase de retención de backup de registros de archivos se modifica mediante la interfaz de línea de comandos o la interfaz gráfica de usuario de SnapManager, la clase de retención modificada no se considera para el backup porque los backups de registros de archivo se retienen en función de la duración de la retención.

- Si elimina los archivos de registro de archivos de los destinos de registro de archivos, el backup de registros de archivos no incluye los archivos de registro de archivos más antiguos que el archivo de registro de archivos faltante.

Si falta el archivo de registro de archivos más reciente, la operación de backup del registro de archivos falla.

- Si elimina los archivos de registro de archivos de los destinos de registro de archivos, se produce un error en la eliminación de archivos de registro de archivos.
- SnapManager consolida los backups de registros de archivos incluso cuando se eliminan los archivos de registro de archivos de los destinos de registros de archivos o cuando los archivos de registro de archivos están dañados.

### **Limitaciones relacionadas con el cambio del nombre de host de la base de datos de destino**

No se admiten las siguientes operaciones de SnapManager cuando se cambia el nombre de host de la base de datos de destino:

- Cambiar el nombre de host de la base de datos de destino desde la interfaz gráfica de usuario de SnapManager.
- Reversión de la base de datos del repositorio después de actualizar el nombre de host de la base de datos de destino del perfil.

- Al mismo tiempo, se actualizan varios perfiles para un nuevo nombre de host de base de datos de destino.
- Cambiar el nombre de host de la base de datos de destino cuando se ejecuta cualquier operación de SnapManager.

### Limitaciones relacionadas con la CLI o GUI de SnapManager

- Los comandos de la CLI de SnapManager para `profile create` La operación que se genera desde la interfaz gráfica de usuario de SnapManager no tiene opciones de configuración del historial.

No puede utilizar el `profile create` Comando para configurar los ajustes de retención de historial desde la CLI de SnapManager.

- SnapManager no muestra la GUI en Mozilla Firefox cuando no hay Java Runtime Environment (JRE) disponible en el cliente UNIX.
- Al actualizar el nombre de host de la base de datos de destino mediante la interfaz de línea de comandos de SnapManager, si hay una o más sesiones abiertas de la interfaz gráfica de usuario de SnapManager, todas las sesiones abiertas de la interfaz gráfica de usuario de SnapManager no pueden responder.

### Limitaciones relacionadas con SnapMirror y SnapVault

- El script de posprocesamiento de SnapVault no es compatible si se utiliza Data ONTAP en 7-Mode.
- Si utiliza ONTAP, no puede ejecutar SnapRestore (VBSR) basada en volúmenes en los backups creados en los volúmenes que tienen relaciones de SnapMirror establecidas.

Esto se debe a una limitación de ONTAP, que no permite romper la relación al realizar una VBSR. Sin embargo, se puede ejecutar un VBSR en el backup último o más reciente creado solo cuando los volúmenes tienen relaciones de SnapVault establecidas.

- Si utiliza Data ONTAP operando en 7-Mode y desea ejecutar un VBSR en los backups creados en los volúmenes que tienen relaciones de SnapMirror establecidas, puede configurar la `override-vbsr-snapmirror-check` opción a **ON** En SnapDrive para UNIX.

La documentación de SnapDrive contiene más información al respecto.

- En algunos casos, no se puede eliminar el último backup asociado con la primera copia Snapshot cuando se ha establecido una relación de SnapVault en el volumen.

Puede eliminar el backup solo cuando se rompa la relación. Este problema se debe a una restricción de la ONTAP con copias Snapshot base. En una relación de SnapMirror, la copia de Snapshot básica se crea mediante el motor de SnapMirror y, en una relación de SnapVault, la copia de Snapshot base es el backup creado mediante SnapManager. Para cada actualización, la copia snapshot básica señala el backup más reciente creado mediante SnapManager.

### Limitaciones relacionadas con las bases de datos en espera de Data Guard

- SnapManager no admite bases de datos lógicas en espera de Data Guard.
- SnapManager no admite bases de datos en espera de Active Data Guard.
- SnapManager no permite realizar backups en línea de bases de datos Data Guard en espera.
- SnapManager no permite backups parciales de bases de datos en espera de Data Guard.
- SnapManager no permite la restauración de bases de datos Data Guard en espera.
- SnapManager no permite eliminar archivos de registro de archivos para bases de datos en espera de Data

Guard.

- SnapManager no admite Data Guard Broker.

### Información relacionada

["Documentación en el sitio de soporte de NetApp"](#)

### Limitaciones de SnapManager para Clustered Data ONTAP

Debe conocer las limitaciones de algunas funcionalidades y operaciones de SnapManager si utiliza Clustered Data ONTAP.

Las siguientes funcionalidades no son compatibles si utiliza SnapManager en Clustered Data ONTAP:

- Funcionalidades de protección de datos si SnapManager se integra con Unified Manager de OnCommand
- Una base de datos en la que una LUN pertenece a un sistema que ejecuta Data ONTAP en 7-Mode y la otra LUN pertenece a un sistema que ejecuta Clustered Data ONTAP
- SnapManager para SAP no admite la migración de un Vserver, que no es compatible con Clustered Data ONTAP
- SnapManager para SAP no admite la funcionalidad Clustered Data ONTAP 8.2.1 para especificar diferentes políticas de exportación para volúmenes y qtrees

### Limitaciones relacionadas con Oracle Database

Antes de empezar a trabajar con SnapManager, debe conocer las limitaciones relacionadas con la base de datos de Oracle.

Estas limitaciones son las siguientes:

- SnapManager es compatible con Oracle versión 10gR2 y no es compatible con Oracle 10gR1 como repositorio o base de datos de destino.
- SnapManager no es compatible con Oracle Cluster File System (OCFS).
- La compatibilidad con bases de datos Oracle 9i se usa en SnapManager 3.2.
- La compatibilidad con la base de datos Oracle 10gR2 (anterior a 10.2.0.5) queda obsoleta en SnapManager 3.3.1.



Identifique las distintas versiones de las bases de datos de Oracle que se admiten en la matriz de interoperabilidad.

### Información relacionada

["Matriz de interoperabilidad"](#)

### Versiones obsoletas de la base de datos Oracle

SnapManager 3.2 o posterior no admite la base de datos Oracle 9i, y la base de datos Oracle 10gR2 (anterior a 10.2.0.4) no es compatible con SnapManager 3.3.1 o posterior.

Si utiliza bases de datos de Oracle 9i o 10gR2 (anteriores a 10.2.0.4) y desea actualizar a SnapManager 3.2 o posterior, no puede crear perfiles nuevos; se muestra un mensaje de advertencia.

Si utiliza bases de datos de Oracle 9i o 10gR2 (anteriores a 10.2.0.4) y desea actualizar a SnapManager 3.2 o una versión posterior, debe realizar una de las siguientes acciones:

- Actualice las bases de datos de Oracle 9i o 10gR2 (anteriores a 10.2.0.4) a bases de datos de Oracle 10gR2 (10.2.0.5), 11gR1 o 11gR2 y, a continuación, actualice a SnapManager 3.2 o 3.3.

Si va a actualizar a Oracle 12c, debe actualizar a SnapManager 3.3.1 o posterior.



La base de datos Oracle 12c sólo se admite desde SnapManager 3.3.1.

- Gestión de las bases de datos Oracle 9i mediante una versión de revisión de SnapManager 3.1.

Puede utilizar SnapManager 3.2 o 3.3 si desea gestionar bases de datos Oracle 10gR2, 11gR1 o 11gR2 y utilizar SnapManager 3.3.1 o posterior si desea gestionar bases de datos Oracle 12c junto con otras bases de datos compatibles.

### Restricciones en la gestión de volúmenes

SnapManager tiene ciertas restricciones de gestión de volúmenes que pueden afectar al entorno.

Es posible tener varios grupos de discos para una base de datos; sin embargo, las siguientes limitaciones se aplican a todos los grupos de discos de una base de datos determinada:

- Los grupos de discos de la base de datos solo pueden gestionarse un gestor de volúmenes.
- Un entorno Linux sin gestión de volúmenes lógicos requiere una partición.


## Configurando SnapManager

Después de instalar SnapManager, debe realizar algunas tareas de configuración adicionales según el entorno que utilice.


### Parámetros de configuración de SnapManager


SnapManager proporciona una lista de parámetros de configuración que se pueden editar en función de sus requisitos. Los parámetros de configuración se almacenan en el archivo smSAP.config. Sin embargo, es posible que el archivo smSAP.config no contenga todos los parámetros de configuración admitidos. Puede agregar los parámetros de configuración, según sus necesidades.



En la siguiente tabla, se enumeran todos los parámetros de configuración de SnapManager compatibles y también se explica cuándo usar estos parámetros:

Parámetros	Descripción
<ul style="list-style-type: none"> <li>• <code>retain.hourly.count</code></li> <li>• <code>retain.hourly.duration</code></li> <li>• <code>retain.monthly.count</code></li> <li>• <code>retain.monthly.duration</code></li> </ul>	<p>Estos parámetros configuran la política de retención al crear un perfil. Por ejemplo, puede asignar los siguientes valores:</p> <pre>retain.hourly.count = 12 retain.hourly.duration = 2 retain.monthly.count = 2 retain.monthly.duration = 6</pre>
<code>restore.secondaryAccessPolicy</code>	<p>Este parámetro define cómo SnapManager puede acceder a los datos en el almacenamiento secundario cuando no puede restaurarse directamente con Protection Manager. Las diferentes maneras de acceder a los datos en el almacenamiento secundario son las siguientes:</p> <ul style="list-style-type: none"> <li>• Directo (predeterminado)</li> </ul> <p>Quando <code>restore.secondaryAccessPolicy</code> se establece en <b>direct</b>, SnapManager clona los datos en el almacenamiento secundario, monta los datos clonados del almacenamiento secundario en el host y, a continuación, copia los datos del clon en el entorno activo.</p> <ul style="list-style-type: none"> <li>• Indirecto</li> </ul> <p>Si asigna <b>indirect</b> para <code>restore.secondaryAccessPolicy</code>, SnapManager copia los datos a un volumen temporal en el almacenamiento primario, monta los datos del volumen temporal en el host y, a continuación, copia los datos del volumen temporal en el entorno activo.</p> <p>El método indirecto se debe utilizar solo si el host no tiene acceso directo al sistema de almacenamiento secundario. Este método tarda el doble de tiempo que el método directo porque se realizan dos copias de los datos.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;">  <p>En una red de área de almacenamiento (SAN) con sistema de archivos de red (NFS) como protocolo, SnapManager no necesita conectarse directamente al almacenamiento secundario para realizar una restauración.</p> </div>
<code>restore.tmpVolumeName</code>	<p>Este parámetro asigna un nombre al volumen temporal. Cuando SnapManager utiliza el método indirecto para restaurar datos desde el almacenamiento secundario, requiere un volumen de desecho en el almacenamiento principal para conservar una copia temporal de los datos hasta que se copian en los archivos de la base de datos y se recupera la base de datos. No hay un valor predeterminado. Si no especifica un valor, debe introducir un nombre en el comando restore que utilice el método indirecto. Por ejemplo, puede asignar los siguientes valores:</p> <pre>restore.tmpVolumeName = smsap_temp_volume</pre>




Parámetros	Descripción
<code>retain.alwaysFreeExpiredBackups</code>	<p>Este parámetro permite a SnapManager liberar backups cuando caduquen y cuando se realice una restauración rápida, incluso si no se configuró la protección de datos. Este parámetro libera los backups protegidos que caducan y eliminan los backups sin proteger que caducan. Los posibles valores que puede asignar son los siguientes:</p> <ul style="list-style-type: none"> <li>• Verdadero</li> </ul> <p>Si asigna <b>true</b> para <code>retain.alwaysFreeExpiredBackups</code>, SnapManager libera las copias de seguridad caducadas independientemente de si las copias de seguridad están protegidas.</p> <p>Los backups se eliminan cuando no están protegidos o si las copias protegidas en el almacenamiento secundario también han caducado.</p> <ul style="list-style-type: none"> <li>• Falso</li> </ul> <p>Si asigna <b>false</b> para <code>retain.alwaysFreeExpiredBackups</code>, SnapManager libera las copias de seguridad caducadas que están protegidas.</p>
<code>host.credentials.persist</code>	<p>Este parámetro permite que SnapManager almacene credenciales del host. De manera predeterminada, las credenciales del host no se almacenan. Sin embargo, es necesario almacenar las credenciales de host si cuenta con un script personalizado que se ejecuta en un clon remoto y requiere acceso a un servidor remoto. Para habilitar el almacenamiento de credenciales de host, asigne el valor TRUE a <code>host.credentials.persist</code>. SnapManager cifra y guarda las credenciales del host.</p>
<code>restorePlanMaxFilesDisplayed</code>	<p>Este parámetro permite definir el número máximo de archivos que se mostrarán en la vista previa de la restauración. de forma predeterminada, SnapManager muestra un máximo de 20 archivos en la vista previa de la restauración. Sin embargo, puede cambiar a un valor mayor que 0. Por ejemplo, puede asignar el siguiente valor:</p> <ul style="list-style-type: none"> <li>• <code>restorePlanMaxFilesDisplayed = 30</code></li> </ul> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Si especifica un valor no válido, se muestra el número predeterminado de archivos.</p> </div>

Parámetros	Descripción
<code>snapshot.list.timeout.min</code>	<p>Este parámetro permite definir la hora en minutos a la que debe esperar SnapManager <code>snap list</code> Comando para ejecutar cuando realiza cualquier operación de SnapManager.de forma predeterminada, SnapManager espera 30 minutos. Sin embargo, puede cambiar a un valor mayor que 0. Por ejemplo, puede asignar el siguiente valor:</p> <ul style="list-style-type: none"> <li>• <code>snapshot.list.timeout.min = 40</code></li> </ul> <p> Si especifica un valor no válido, se utiliza el valor predeterminado.</p> <p>Para cualquier operación de SnapManager, si el tiempo de ejecución del comando de lista de <code>snap</code> excede el valor asignado a <code>snapshot.list.timeout.min</code>, la operación falla con un mensaje de error de tiempo de espera.</p>
<code>pruneIfFileExistsInOtherDestination</code>	<p>Este parámetro de eliminación permite definir el destino de los archivos de registros de archivos. Los archivos de registro de archivos se almacenan en varios destinos. Al eliminar los archivos de registro de archivos, SnapManager debe conocer el destino de los archivos de registro de archivos. Los posibles valores que puede asignar son los siguientes:</p> <ul style="list-style-type: none"> <li>• Cuando desee comprimir los archivos de registro de archivos desde un destino especificado, debe asignar <b>false</b> para <code>pruneIfFileExistsInOtherDestination</code>.</li> <li>• Si desea comprimir los archivos de registro de archivo desde un destino externo, debe asignar <b>true</b> para <code>pruneIfFileExistsInOtherDestination</code>.</li> </ul>
<code>prune.archivelogs.backedup.from.otherdestination</code>	<p>Este parámetro de eliminación permite reducir los archivos de registro de archivos de los que se ha realizado una copia de seguridad desde los destinos de registro de archivos especificados o del que se ha realizado una copia de seguridad desde destinos de registros de archivos externos. Los posibles valores que puede asignar son los siguientes:</p> <ul style="list-style-type: none"> <li>• Si desea comprimir los archivos de registro de archivos desde los destinos especificados y si se realiza una copia de seguridad de los archivos de registro de archivos desde los destinos especificados mediante <code>-prune -dest</code>, debe asignar <b>false</b> para <code>prune.archivelogs.backedup.from.otherdestination</code>.</li> <li>• Si desea comprimir los archivos de registro de archivos desde destinos especificados y si se realiza una copia de seguridad de los archivos de registro de archivos al menos una vez desde cualquiera de los otros destinos, debe asignar <b>true</b> para <code>prune.archivelogs.backedup.from.otherdestination</code>.</li> </ul>

Parámetros	Descripción
<code>maximum.archivelog.files.topprune.atATime</code>	<p>Este parámetro de eliminación permite definir el número máximo de archivos de registro de archivos que puede recortar en un momento dado. Por ejemplo, puede asignar el siguiente valor:</p> <pre>maximum.archivelog.files.topprune.atATime = 998</pre> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>El valor al que se puede asignar <code>maximum.archivelog.files.topprune.atATime</code> debe ser inferior a 1000.</p> </div>
<code>archivelogs consolidate</code>	<p>Este parámetro permite que SnapManager libere los backups duplicados de los registros de archivos si asigna <b>true</b> para <code>archivelogs consolidate</code>.</p>
<code>suffix.backup.label.with.logs</code>	<p>Este parámetro permite especificar el sufijo que se desea añadir para diferenciar los nombres de las etiquetas del backup de datos y del backup de los registros de archivo.</p> <p>Por ejemplo, cuando asigna <b>logs</b> para <code>suffix.backup.label.with.logs</code>, <code>_logs</code> se agrega como sufijo a la etiqueta de copia de seguridad del registro de archivos. En ese caso, la etiqueta de backup del registro de archivos sería <code>arch_logs</code>.</p>
<code>backup.archivelogs.beyond.missingfiles</code>	<p>Este parámetro permite que SnapManager incluya los archivos de registro de archivos faltantes en el backup.</p> <p>Los archivos de registro de archivos que no existen en el sistema de archivos activo no se incluyen en la copia de seguridad. Si desea incluir todos los archivos de registro de archivos, incluso los que no existen en el sistema de archivos activo, debe asignar <b>true</b> para <code>backup.archivelogs.beyond.missingfiles</code>.</p> <p>Puede asignar <b>false</b> para ignorar los archivos de registro de archivos faltantes.</p>
<code>srvctl.timeout</code>	<p>Este parámetro permite definir el valor de tiempo de espera para <code>srvctl</code> comando.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>Server Control (SRVCTL) es una utilidad para administrar instancias de RAC.</p> </div> <p>Cuando SnapManager tarda más tiempo en ejecutar el <code>srvctl</code> Comando que el valor de tiempo de espera, la operación de SnapManager genera el siguiente mensaje de error: <code>Error: Timeout occurred while executing command: srvctl status.</code></p>

Parámetros	Descripción
<code>snapshot.restore.storageNameCheck</code>	<p>Este parámetro permite a SnapManager realizar la operación de restauración con copias Snapshot que se crearon antes de migrar desde operaciones Data ONTAP en 7-Mode a Clustered Data ONTAP. el valor predeterminado asignado al parámetro es <b>false</b>. Si ha migrado de Data ONTAP operando en 7-Mode a Clustered Data ONTAP, pero desea usar las copias Snapshot creadas antes de la migración, establecidas <code>snapshot.restore.storageNameCheck=true</code>.</p>
<code>services.common.disableAbort</code>	<p>Este parámetro deshabilita la limpieza tras el fallo de las operaciones de ejecución prolongada. Puede ajustar <code>services.common.disableAbort=true</code>. Por ejemplo, si está realizando una operación de clonado que se ejecuta mucho y genera un error debido a un error de Oracle, es posible que no desee limpiar el clon. Si ha configurado <code>services.common.disableAbort=true</code>, el clon no se eliminará. Puede corregir el problema de Oracle y reiniciar la operación de clonado desde el punto en que falló.</p>
<ul style="list-style-type: none"> <li>• <code>backup.sleep.dnfs.layout</code></li> <li>• <code>backup.sleep.dnfs.secs</code></li> </ul>	<p>Estos parámetros activan el mecanismo de suspensión en el diseño Direct NFS (dNFS). Después de crear la copia de seguridad de los archivos de control utilizando dNFS o un sistema de archivos de red (NFS), SnapManager intenta leer los archivos de control, pero es posible que no se encuentren los archivos.</p> <p>Para activar el mecanismo de suspensión, asegúrese de que <code>backup.sleep.dnfs.layout=true</code>. El valor predeterminado es <b>true</b>.</p> <p>Al activar el mecanismo de suspensión, debe asignar el tiempo de suspensión <code>backup.sleep.dnfs.secs</code>. El tiempo de inactividad asignado es en segundos y el valor depende de su entorno. El valor predeterminado es 5 segundos.</p> <p>Por ejemplo:</p> <ul style="list-style-type: none"> <li>• <code>backup.sleep.dnfs.layout=true</code></li> <li>• <code>backup.sleep.dnfs.secs=2</code></li> </ul>

Parámetros	Descripción
<ul style="list-style-type: none"> <li>• <code>override.default.backup.pattern</code></li> <li>• <code>new.default.backup.pattern</code></li> </ul>	<p>Cuando no se especifica la etiqueta de backup, SnapManager crea una etiqueta de backup predeterminada. Estos parámetros SnapManager permiten personalizar la etiqueta de backup predeterminada.</p> <p>Para poder personalizar la etiqueta de backup, asegúrese de que el valor de <code>override.default.backup.pattern</code> se establece en <b>true</b>. El valor predeterminado es <b>false</b>.</p> <p>Para asignar el nuevo patrón de la etiqueta de backup, se pueden asignar palabras clave como el nombre de la base de datos, el nombre del perfil, el ámbito, el modo y el nombre del host <code>new.default.backup.pattern</code>. Las palabras clave se deben separar con un guión bajo. Por ejemplo:  <code>new.default.backup.pattern=dbname_profile_hostname_scope_mod e</code>.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>La Marca de hora se incluye automáticamente al final de la etiqueta generada.</p> </div>
<code>allow.underscore.in.clone.sid</code>	<p>Oracle admite el uso de guion bajo en el SID de clonado de Oracle 11gR2. Este parámetro SnapManager permite incluir un guión bajo en el nombre del SID del clon.</p> <p>Para incluir un guion bajo en el nombre SID del clon, asegúrese de que el valor de <code>allow.underscore.in.clone.sid</code> se establece en <b>true</b>. El valor predeterminado es TRUE.</p> <p>Si utiliza una versión de Oracle anterior a Oracle 11gR2 o si no desea incluir un guión bajo en el nombre del SID del clon, establezca el valor en <b>false</b>.</p>
<code>oracle.parameters.with.comma</code>	<p>Este parámetro le permite especificar todos los parámetros de Oracle que tienen coma (,) como valor. mientras realiza cualquier operación que utilice SnapManager <code>oracle.parameters.with.comma</code> Para comprobar todos los parámetros de Oracle y omitir la división de los valores.</p> <p>Por ejemplo, si el valor de <code>nls_numeric_characters=,</code> a continuación, especifique <code>oracle.parameters.with.comma=nls_numeric_characters</code>. Si existen varios parámetros de Oracle con coma como valor, debe especificar todos los parámetros en <code>oracle.parameters.with.comma</code>.</p>

Parámetros	Descripción
<ul style="list-style-type: none"> <li>• <code>archivedLogs.exclude</code></li> <li>• <code>archivedLogs.exclude.fileslike</code></li> <li>• <code>&lt;db-unique-name&gt;.archivedLogs.exclude.fileslike</code></li> </ul>	<p>Estos parámetros permiten que SnapManager excluya los archivos de registro de archivos de los perfiles y los backups si la base de datos no está en un sistema de almacenamiento habilitado para copias de Snapshot y desea ejecutar las operaciones de SnapManager en ese sistema de almacenamiento.</p> <p> Debe incluir los parámetros <code>exclude</code> en el archivo de configuración antes de crear un perfil.</p> <p>Los valores asignados a estos parámetros pueden ser un directorio de nivel superior o un punto de montaje donde están presentes los archivos de registro de archivos o un subdirectorio. Si se especifica un directorio de nivel superior o un punto de montaje y si la protección de datos está habilitada para un perfil en el host, ese punto o directorio de montaje no se incluye en el conjunto de datos que se crea en Protection Manager. Cuando existen varios archivos de registro de archivos para excluirse del host, debe separar las rutas de los archivos de registro de archivos mediante comas.</p> <p>Para excluir los archivos de registro de archivos de que se incluyan en el perfil y se realice una copia de seguridad, debe incluir uno de los parámetros siguientes:</p> <ul style="list-style-type: none"> <li>• <code>archivedLogs.exclude</code> para especificar una expresión regular para excluir archivos de registro de archivos de todos los perfiles o copias de seguridad.</li> </ul> <p>Los archivos de registro de archivos que coinciden con la expresión regular se excluyen de todos los perfiles y copias de seguridad.</p> <p>Por ejemplo, puede establecer <code>archivedLogs.Exclude = /arch/logs/on/local/disk1/.*/arch/logs/on/local/disk2/..</code>  <b>Para las bases de datos de ASM, se puede configurar <code>archivedLogs.exclude = \\+KHDB_ARCH_DEST/khdb/archivelog/.*/\\+KHDB_NONNAARCHTWO/khdb/archivelog/.*</code></b></p> <ul style="list-style-type: none"> <li>• <code>archivedLogs.exclude.fileslike</code> Para especificar una expresión SQL para excluir archivos de registro de archivos de todos los perfiles o copias de seguridad.</li> </ul> <p>Los archivos de registro de archivos que coinciden con la expresión SQL se excluyen de todos los perfiles y las copias de seguridad.</p> <p>Por ejemplo, puede establecer <code>archivedLogs.exclude.fileslike = /arch/logs/on/local/disk1/%,/arch/logs/on/local/disk2/%</code>.</p> <ul style="list-style-type: none"> <li>• <code>&lt;db-unique-name&gt;.archivedLogs.exclude.fileslike</code> Para especificar una expresión SQL para excluir los archivos de registro de archivos sólo del perfil o la copia de seguridad creada para la base de datos con el especificado <code>db-unique-name</code>.</li> </ul> <p>Los archivos de registro de archivos que coinciden con la expresión SQL se excluyen del perfil y las copias de seguridad.</p> <p>Por ejemplo, puede establecer <code>mydb.archivedLogs.exclude.fileslike = /arch/logs/on/local/disk1/%,/arch/logs/on/local/disk2/%</code>.</p>

## Edite los parámetros de configuración

Según el entorno, puede cambiar los valores predeterminados asignados al parámetro de configuración.



El DR Tools no admite los siguientes parámetros aunque estos parámetros estén configurados para excluir archivos de registro de archivos:

### Pasos

1. Abra el archivo de configuración desde la siguiente ubicación predeterminada:

```
default installation location/properties/smsap.conf
```

2. Cambie los valores predeterminados de los parámetros de configuración.



También puede agregar parámetros de configuración compatibles que no se incluyen en el archivo de configuración y asignarles valores.

3. Reinicie SnapManager para el servidor SAP.

## Configurar SnapDrive para UNIX para un entorno activo/activo de Veritas SFRAC

Si ha incluido el `host-cluster-sw-restore-warn` parámetro in `snapdrive.conf` Y haber asignado el valor, debe cambiar el valor para admitir la operación de restauración en el entorno activo/activo de Veritas Storage Foundation para Oracle RAC (SFRAC).

Cuando se utiliza el entorno Active/Active Veritas Storage Foundation para Oracle RAC (SFRAC), si es el `host-cluster-sw-restore-warn` el parámetro se establece en **on**, aparece un mensaje de advertencia y se detiene la operación de restauración. Si desea ejecutar la operación de restauración en un entorno Veritas SFRAC activo/activo, debe configurar `host-cluster-sw-restore-warn` para **off**.

Para obtener información sobre `snapdrive.conf`, Consulte la documentación de SnapDrive.

### Pasos

1. Inicie sesión como usuario root.
2. Abra el `snapdrive.conf` archivo mediante un editor de texto.
3. Cambie el valor de `host-cluster-sw-restore-warn` para **off**.

### Después de terminar

Tras la configuración, reinicie el servidor SnapDrive para UNIX.

### Información relacionada

["Documentación en el sitio de soporte de NetApp"](#)

## Configure SnapManager para que sea compatible con el entorno de Veritas SFRAC

Cuando se instala SnapManager en Solaris, puede configurar SnapManager para que sea compatible con el entorno de Veritas Storage Foundation para Oracle RAC (SFRAC).

### Lo que necesitará

- El host debe tener Solaris, utilidades host y Veritas instalados.

## Pasos

1. Cree un grupo de discos compartidos y un sistema de archivos para SnapManager mediante SnapDrive para UNIX para que los sistemas de archivos se monten simultáneamente en ambos nodos de Real Application Clusters (RAC).

Para obtener información acerca de cómo crear un grupo de discos compartidos y un sistema de archivos, consulte la documentación de SnapDrive.

2. Instalar y configurar la base de datos SAP que se va a montar en los sistemas de archivos compartidos.
3. Inicie una instancia de base de datos en cualquier nodo del RAC.

["Documentación en el sitio de soporte de NetApp"](#)

## Seguridad y gestión de credenciales

Puede gestionar la seguridad en SnapManager aplicando la autenticación del usuario y el control de acceso basado en roles (RBAC). El método de autenticación de usuario permite acceder a recursos como repositorios, hosts y perfiles. El control de acceso basado en roles permite restringir las operaciones que SnapManager puede realizar en los volúmenes y LUN que contienen los archivos de datos de la base de datos.

Cuando se realiza una operación mediante la interfaz de línea de comandos (CLI) o la interfaz gráfica de usuario (GUI), SnapManager recupera las credenciales establecidas para repositorios y perfiles. SnapManager guarda las credenciales de instalaciones anteriores.

El repositorio y los perfiles se pueden proteger con una contraseña. Una credencial es la contraseña configurada para el usuario de un objeto y la contraseña no está configurada en el objeto en sí.

Puede gestionar la autenticación y las credenciales realizando las siguientes tareas:

- Gestione la autenticación de usuario mediante solicitudes de contraseña en las operaciones o mediante el `smsap credential set` comando.

Configurar credenciales para un repositorio, host o perfil.

- Vea las credenciales que rigen los recursos a los que tiene acceso.
- Borre las credenciales de un usuario para todos los recursos (hosts, repositorios y perfiles).
- Eliminar credenciales de un usuario para recursos individuales (hosts, repositorios y perfiles).

Para gestionar el acceso basado en roles, debe realizar las siguientes tareas:

- Habilite RBAC para SnapManager mediante SnapDrive.
- Asigne usuarios a las funciones y establezca las funciones mediante la consola de Operations Manager.
- De manera opcional, habilite SnapManager para almacenar contraseñas cifradas mediante la edición de `smsap.config file`.

Si está instalado Protection Manager, el acceso a las funciones se ve afectado de las siguientes maneras:



- Si se instala Protection Manager, al crear un perfil de base de datos, SnapManager crea un conjunto de datos y rellena el conjunto de datos con los volúmenes que contienen los archivos de base de datos.

Después de una operación de backup, SnapManager mantiene el contenido del conjunto de datos sincronizado con los archivos de la base de datos.

- Si Protection Manager no está instalado, SnapManager no puede crear un conjunto de datos y no podrá establecer la protección en los perfiles.

## Qué es la autenticación de usuario

Además de utilizar el control de acceso basado en roles (RBAC), SnapManager autentica al usuario por medio de un inicio de sesión en el sistema operativo (SO) en el host en el que se ejecuta el servidor SnapManager. Puede habilitar la autenticación de usuario mediante solicitudes de contraseña en las operaciones o mediante el `smsap credential set`.

Los requisitos de autenticación de usuario dependen de dónde se realice la operación.

- Si el cliente SnapManager está en el mismo servidor que el host SnapManager, se autenticará mediante las credenciales del sistema operativo.

No se le solicita una contraseña porque ya ha iniciado sesión en el host donde se ejecuta el servidor SnapManager.

- Si el cliente SnapManager y el servidor SnapManager están en hosts diferentes, SnapManager debe autenticarse con ambas credenciales de sistema operativo.

SnapManager solicita contraseñas para cualquier operación si no se guardaron las credenciales del sistema operativo en la caché de credenciales del usuario SnapManager. Si introduce el `smsap credential set -host Comando`, puede guardar las credenciales del sistema operativo en su archivo de caché de credenciales de SnapManager, por lo que SnapManager no solicita la contraseña de ninguna operación.

Si está autenticado con el servidor SnapManager, se considera el usuario efectivo. El usuario efectivo para cualquier operación debe ser una cuenta de usuario válida en el host donde se ejecuta la operación. Por ejemplo, si ejecuta una operación de clonado, debe poder iniciar sesión en el host de destino del clon.



SnapManager para SAP podría fallar al autorizar a los usuarios creados en Servicios de Active Directory central, como LDAP Y ANUNCIOS. Para garantizar que la autenticación no falle, debe configurar `configurable auth.disableServerAuthorization` para **true**.

Como usuario eficaz, puede gestionar las credenciales de las siguientes maneras:

- De manera opcional, es posible configurar SnapManager para almacenar credenciales de usuario en el archivo de credenciales de usuario de SnapManager.

De manera predeterminada, SnapManager no almacena las credenciales del host. Puede resultar conveniente cambiar esto, por ejemplo, si tiene scripts personalizados que requieren acceso en un host remoto. La operación de clonado remoto es un ejemplo de una operación SnapManager que necesita las credenciales de inicio de sesión de un usuario para un host remoto. Para que SnapManager recuerde credenciales de inicio de sesión de host de usuario en la caché de credenciales de usuario de

SnapManager, configure el `host.credentials.persist` propiedad a **true** en la `smsap.config` archivo.

- Puede autorizar el acceso de los usuarios al repositorio.
- Puede autorizar el acceso de los usuarios a los perfiles.
- Es posible ver todas las credenciales de usuario.
- Es posible borrar las credenciales de un usuario para todos los recursos (hosts, repositorios y perfiles).
- Es posible eliminar credenciales de recursos individuales (hosts, repositorios y perfiles).

## Acerca del control de acceso basado en roles

El control de acceso basado en roles permite controlar quién tiene acceso a las operaciones de SnapManager. Con RBAC, los administradores pueden gestionar grupos de usuarios al definir roles y asignar usuarios a esos roles. Puede ser conveniente utilizar el control de acceso basado en roles de SnapManager en entornos donde ya se encuentra el control de acceso basado en roles.

El control de acceso basado en roles incluye los siguientes componentes:

- Recursos: Volúmenes y LUN que contienen los archivos de datos que componen la base de datos.
- Capabilities: Tipos de operaciones que se pueden realizar en un recurso.
- Usuarios: Personas a las que usted concede capacidades.
- Funciones: Un conjunto de recursos y capacidades que se permiten en los recursos. Asigne un rol específico a un usuario que deba realizar esas capacidades.

Es posible habilitar el control de acceso basado en roles en SnapDrive. A continuación, puede configurar capacidades específicas por función en la interfaz gráfica de usuario web o en la interfaz de línea de comandos de Operations Manager. Las comprobaciones de RBAC se realizan en DataFabric Manager Server.

En la tabla siguiente se enumeran algunas funciones y sus tareas típicas, tal como se establece en el Administrador de operaciones.

<b>Función</b>	<b>Tareas típicas</b>
Administrador de base SAP	<ul style="list-style-type: none"><li>• Crear, mantener y supervisar una base de datos de Oracle que reside en un host</li><li>• Programar y crear backups de bases de datos</li><li>• Garantizar que los backups sean válidos y se puedan restaurar</li><li>• Clonar bases de datos</li></ul>
Administrador de servidores	<ul style="list-style-type: none"><li>• Configuración de sistemas de almacenamiento y agregados</li><li>• Supervisar los volúmenes para obtener espacio libre</li><li>• Aprovisionamiento de almacenamiento para solicitudes de usuarios</li><li>• Configuración y supervisión de mirroring de recuperación de desastres</li></ul>

Función	Tareas típicas
Arquitecto de almacenamiento	<ul style="list-style-type: none"> <li>• Tomar decisiones sobre la arquitectura en el almacenamiento</li> <li>• Planificación del crecimiento de la capacidad de almacenamiento</li> <li>• Planificación de las estrategias de recuperación ante desastres</li> <li>• Delegación de capacidades a los miembros del equipo</li> </ul>

Si está en uso RBAC (es decir, que Operations Manager está instalado y que el RBAC está habilitado en SnapDrive), el administrador de almacenamiento debe asignar permisos de RBAC en todos los volúmenes y sistemas de almacenamiento para los archivos de base de datos.

### Habilite el control de acceso basado en roles

El control de acceso basado en roles (RBAC) de SnapManager está habilitado mediante SnapDrive. Tras la instalación de SnapDrive, el control de acceso basado en roles está deshabilitado de forma predeterminada. Después de habilitar el control de acceso basado en roles en SnapDrive, SnapManager ejecuta operaciones con RBAC habilitado.

### Acerca de esta tarea

La `snapdrive.config` File en SnapDrive establece diversas opciones, una de las cuales permite RBAC.

La documentación de SnapDrive contiene detalles sobre SnapDrive.

### Pasos

1. Abra el `snapdrive.conf` archivo en un editor.
2. Cambie el valor de para habilitar RBAC `rbac-method` parámetro de **native** para **dfm**.

El valor predeterminado de este parámetro es **native**, Que deshabilita RBAC.

["Documentación en el sitio de soporte de NetApp"](#)

### Defina funciones y funcionalidades de control de acceso basado en roles

Después de habilitar el control de acceso basado en roles (RBAC) para SnapManager mediante SnapDrive, es posible añadir funcionalidades de RBAC y usuarios a roles para ejecutar operaciones de SnapManager.

### Lo que necesitará

Debe crear un grupo en el servidor de Data Fabric Manager y añadir el grupo a los sistemas de almacenamiento primario y secundario. Ejecute los siguientes comandos:

- `dfm group create smsap_grp`
- `dfm group add smsap_grpprimary_storage_system`
- `dfm group add smsap_grpsecondary_storage_system`

### Acerca de esta tarea

Es posible usar la interfaz web de Operations Manager o la interfaz de línea de comandos (CLI) del servidor de Data Fabric Manager para modificar las funcionalidades y los roles de RBAC.

En la tabla, se enumeran las capacidades de RBAC necesarias para ejecutar operaciones de SnapManager:

Operaciones de SnapManager	Funcionalidades de RBAC necesarias cuando la protección de datos no está habilitada	Funcionalidades de RBAC necesarias cuando la protección de datos está habilitada
Creación de perfiles o actualización de perfiles	SD.Storage.Read (smsap_grp)	SD.Storage.Read (SMSAP_profile conjunto de datos)
Protección de perfiles	DFM.Database.Write (smSAP_grp) SD.Storage.Read (smsap_grp) SD.Config.Read (smsap_grp) SD.Config.Write (smsap_grp) SD.Config.Delete (smsap_grp) GlobalDataProtection	Ninguno
Crear backup	SD.Storage.Read (smsap_grp) SD.Snapshot.Write (smSAP_grp) SD.Snapshot.Read (smSAP_grp) SD.Snapshot.Delete (smsap_grp)	SD.Storage.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Write (SMSAP_profile conjunto de datos) SD.Snapshot.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Delete (SMSAP_profile conjunto de datos)
Creación de backup (con DBVerify)	SD.Storage.Read (smsap_grp) SD.Snapshot.Write (smSAP_grp) SD.Snapshot.Read (smSAP_grp) SD.Snapshot.Delete (smsap_grp) SD.snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Write (SMSAP_profile conjunto de datos) SD.Snapshot.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Delete (SMSAP_profile conjunto de datos) SD.snapshot.Clone (SMSAP_profile conjunto de datos)

Operaciones de SnapManager	Funcionalidades de RBAC necesarias cuando la protección de datos no está habilitada	Funcionalidades de RBAC necesarias cuando la protección de datos está habilitada
Crear copia de seguridad (con RMAN)	SD.Storage.Read (smsap_grp) SD.Snapshot.Write (smSAP_grp) SD.Snapshot.Read (smSAP_grp) SD.Snapshot.Delete (smsap_grp) SD.snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Write (SMSAP_profile conjunto de datos) SD.Snapshot.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Delete (SMSAP_profile conjunto de datos) SD.snapshot.Clone (SMSAP_profile conjunto de datos)
Restauración de backup	SD.Storage.Read (smsap_grp) SD.Snapshot.Write (smSAP_grp) SD.Snapshot.Read (smSAP_grp) SD.Snapshot.Delete (smsap_grp) SD.snapshot.Clone (smsap_grp) SD.Snapshot.Restore (smSAP_grp)	SD.Storage.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Write (SMSAP_profile conjunto de datos) SD.Snapshot.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Delete (SMSAP_profile conjunto de datos) SD.snapshot.Clone (SMSAP_profile conjunto de datos) SD.Snapshot.Restore (SMSAP_profile conjunto de datos)
Eliminación de copia de seguridad	SD.Snapshot.Delete (smsap_grp)	SD.Snapshot.Delete (SMSAP_profile conjunto de datos)
Verificación de backup	SD.Storage.Read (smsap_grp) SD.Snapshot.Read (smSAP_grp) SD.Snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Clone (SMSAP_profile conjunto de datos)

Operaciones de SnapManager	Funcionalidades de RBAC necesarias cuando la protección de datos no está habilitada	Funcionalidades de RBAC necesarias cuando la protección de datos está habilitada
Montaje de backup	SD.Storage.Read (smsap_grp) SD.Snapshot.Read (smSAP_grp) SD.Snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Clone (SMSAP_profile conjunto de datos)
Desmontaje de backups	SD.Snapshot.Clone (smsap_grp)	SD.Snapshot.Clone (SMSAP_profile conjunto de datos)
Clone create	SD.Storage.Read (smsap_grp) SD.Snapshot.Read (smSAP_grp) SD.snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Read (SMSAP_profile conjunto de datos) SD.snapshot.Clone (SMSAP_profile conjunto de datos)
Clonar eliminación	SD.Snapshot.Clone (smsap_grp)	SD.Snapshot.Clone (SMSAP_profile conjunto de datos)
División de clones	SD.Storage.Read (smsap_grp) SD.Snapshot.Read (smSAP_grp) SD.snapshot.Clone (smsap_grp) SD.Snapshot.Delete (smsap_grp) SD.Storage.Write (smSAP_grp)	SD.Storage.Read (SMSAP_profile conjunto de datos) SD.Snapshot.Read (SMSAP_profile conjunto de datos) SD.snapshot.Clone (SMSAP_profile conjunto de datos) SD.Snapshot.Delete (SMSAP_profile conjunto de datos) SD.Storage.Write (SMSAP_profile conjunto de datos)

Para obtener detalles sobre la definición de las funcionalidades de RBAC, consulte la *Guía de administración del gestor de operaciones de Unified Manager de OnCommand*.

### Pasos

1. Acceda a la consola de Operations Manager.
2. En el menú Configuración, seleccione **roles**.
3. Seleccione un rol existente o cree uno nuevo.

4. Para asignar operaciones a los recursos de almacenamiento de la base de datos, haga clic en **Agregar capacidades**.
5. En la página Editar configuración de función, para guardar los cambios realizados en la función, haga clic en **Actualizar**.

## Información relacionada

["Guía de administración del gestor de operaciones de OnCommand Unified Manager"](#)

## Almacenar contraseñas cifradas para scripts personalizados

De forma predeterminada, SnapManager no almacena credenciales de host en la caché de credenciales de usuario. Sin embargo, puede cambiar esto. Puede editar el `smsap.config` archivo para permitir el almacenamiento de credenciales de host.

### Pasos

La `smsap.config` el archivo está ubicado en `<default installation location>/properties/smsap.config`

1. Edite el `smsap.config` archivo.
2. Configurado `host.credentials.persist` para **true**.

## Autorizar el acceso al repositorio

Además del control de acceso basado en roles (RBAC), SnapManager permite configurar credenciales para que los usuarios de la base de datos accedan al repositorio. Con las credenciales, puede restringir o evitar el acceso a hosts, repositorios, perfiles y bases de datos de SnapManager.

### Acerca de esta tarea

Si ha configurado las credenciales con el comando set de credenciales, SnapManager no le solicita una contraseña.

Es posible configurar credenciales de usuario al instalar SnapManager o una versión posterior.

### Paso

1. Introduzca el siguiente comando:

```
smsap credential set -repository -dbname repo_service_name -host repo_host -login -username repo_username [-password repo_password] -port repo_port
```

## Autorizar el acceso a los perfiles

Además del control de acceso basado en roles (RBAC), SnapManager permite configurar una contraseña para un perfil para evitar el acceso no autorizado.

### Paso

1. Introduzca el siguiente comando:

```
smsap credential set -profile -name profile_name [-password password]
```

## Ver las credenciales de usuario

Puede enumerar los hosts, perfiles y repositorios a los que tiene acceso.

### Paso

1. Para enumerar los recursos a los que tiene acceso, escriba este comando:

```
smsap credential list
```

## Ejemplo de visualización de credenciales de usuario

En este ejemplo, se muestran los recursos a los que tiene acceso.

```
smsap credential list
```

```
Credential cache for OS user "user1":  
Repositories:  
Host1_test_user@SMSAPREPO/hotspur:1521  
Host2_test_user@SMSAPREPO/hotspur:1521  
user1_1@SMSAPREPO/hotspur:1521  
Profiles:  
HSDBR (Repository: user1_2_1@SMSAPREPO/hotspur:1521)  
PBCASM (Repository: user1_2_1@SMSAPREPO/hotspur:1521)  
HSDB (Repository: Host1_test_user@SMSAPREPO/hotspur:1521) [PASSWORD NOT  
SET]  
Hosts:  
Host2  
Host5
```

## Borrar credenciales de usuario para todos los hosts, repositorios y perfiles

Puede borrar la caché de sus credenciales para recursos (hosts, repositorios y perfiles). Esto elimina todas las credenciales de recursos del usuario que ejecuta el comando. Después de borrar la caché, debe volver a autenticar las credenciales para obtener acceso a estos recursos protegidos.

### Pasos

1. Para borrar sus credenciales, introduzca el comando `smsap credential clear` de la CLI de SnapManager o seleccione **Admin > credenciales > Clear Cache** de la GUI de SnapManager.



## 2. Salga de la interfaz gráfica de usuario de SnapManager.



- Si borró la caché de credenciales de la interfaz gráfica de usuario de SnapManager, no es necesario salir de la interfaz gráfica de usuario de SnapManager.
- Si borró la caché de credenciales de la interfaz de línea de comandos de SnapManager, debe reiniciar la interfaz gráfica de usuario de SnapManager.
- Si ha eliminado manualmente el archivo de credenciales cifrado, deberá reiniciar de nuevo la interfaz gráfica de usuario de SnapManager.

3. Para volver a configurar las credenciales, repita el proceso con el fin de establecer las credenciales para el repositorio, el host del perfil y el perfil. Para obtener información adicional sobre cómo volver a configurar las credenciales de usuario, consulte "Configuración de credenciales tras borrar caché de credenciales".

### Configure las credenciales después de borrar la caché de credenciales

Después de borrar la caché para quitar las credenciales de usuario almacenadas, puede configurar las credenciales para hosts, repositorios y perfiles.

#### Acerca de esta tarea

Debe asegurarse de establecer las mismas credenciales de usuario para el repositorio, el host del perfil y el perfil que había especificado anteriormente. Se crea un archivo de credenciales cifrado al configurar las credenciales de usuario.

El archivo de credenciales está ubicado en `/root/.netapp/smsap/3.3.0`.

Desde la interfaz gráfica de usuario (GUI) de SnapManager, si no hay ningún repositorio en repositorios, realice los siguientes pasos:

#### Pasos

1. Haga clic en **tareas > Agregar repositorio existente** para agregar un repositorio existente.
2. Ejecute los siguientes pasos para configurar las credenciales del repositorio:
  - a. Haga clic con el botón derecho del ratón en el repositorio y seleccione **Abrir**.
  - b. En la ventana **autenticación de credenciales de repositorio**, introduzca las credenciales de usuario.
3. Realice los siguientes pasos para configurar las credenciales del host:
  - a. Haga clic con el botón derecho del ratón en el host bajo el repositorio y seleccione **Abrir**.
  - b. En la ventana **autenticación de credenciales de host**, introduzca las credenciales de usuario.
4. Realice los siguientes pasos para configurar las credenciales del perfil:
  - a. Haga clic con el botón derecho del ratón en el perfil bajo el host y seleccione **Abrir**.
  - b. En la ventana **autenticación de credenciales de perfil**, introduzca las credenciales de usuario.

### Eliminar credenciales de recursos individuales

Puede eliminar las credenciales de uno de los recursos protegidos, como un perfil, un repositorio o un host. De este modo, puede quitar las credenciales de un solo recurso, en lugar de borrar las credenciales del usuario de todos los recursos.

## Eliminar credenciales de usuario para repositorios

Es posible eliminar las credenciales para que un usuario ya no pueda acceder a un repositorio en particular. Este comando permite quitar las credenciales de un solo recurso, en lugar de borrar las credenciales del usuario para todos los recursos.

### Paso

1. Para eliminar credenciales de repositorio de un usuario, escriba este comando:

```
smsap credential delete -repository-dbname repo_service_name -host repo_host
-login -username repo_username -port repo_port
```

## Eliminar credenciales de usuario para hosts

Es posible eliminar las credenciales de un host para que un usuario ya no pueda acceder a él. Este comando permite quitar las credenciales de un solo recurso, en lugar de borrar todas las credenciales del usuario para todos los recursos.

### Paso

1. Para eliminar credenciales de host de un usuario, escriba este comando:

```
smsap credential delete -host-name host_name -username username
```

## Eliminar credenciales de usuario para perfiles

Es posible eliminar las credenciales de usuario de un perfil para que un usuario ya no pueda acceder a él.

### Paso

1. Para eliminar las credenciales de perfil de un usuario, escriba el siguiente comando:

```
smsap credential delete -profile -name profile_name
```

# Gestionar perfiles para backups eficientes

Debe crear un perfil en SnapManager para la base de datos donde desea realizar una operación. Debe seleccionar el perfil y, a continuación, seleccionar la operación que desea realizar.

## Tareas relacionadas con perfiles

Es posible realizar las siguientes tareas:

- Cree perfiles para permitir backups completos o parciales y backups en almacenamiento primario, secundario o incluso terciario.

También es posible crear perfiles para separar los backups de registros de archivo de los backups de archivos de datos.

- Verificar perfiles.
- Actualizar perfiles.
- Eliminar perfiles.

## Acerca de los perfiles y la autenticación

Al crear un perfil, puede especificar una base de datos y elegir uno de los siguientes métodos para conectarse a la base de datos:

- Autenticación de Oracle con un nombre de usuario, contraseña y puerto
- Autenticación del sistema operativo (SO) sin nombre de usuario, contraseña ni puerto.

Para la autenticación del sistema operativo, debe introducir la información de usuario y del grupo de cuenta del sistema operativo.



Para utilizar la autenticación del sistema operativo para las bases de datos de Real Application Cluster (RAC), el servidor SnapManager debe estar en ejecución en cada nodo del entorno RAC y la contraseña de la base de datos debe ser la misma para todas las instancias de Oracle de un entorno RAC. SnapManager utiliza el nombre de usuario y la contraseña de la base de datos para conectarse a cada instancia de RAC del perfil.

- Autenticación de base de datos cuando `sqlnet.authentication_services` se establece en **NONE**. A continuación, SnapManager utiliza el nombre de usuario y la contraseña de la base de datos para todas las conexiones con la base de datos de destino.



Para utilizar la autenticación de la base de datos para una instancia de Automatic Storage Management (ASM), se debe introducir el nombre de usuario y la contraseña que se utilizan para iniciar sesión en la instancia de ASM.

Puede ajustar `sqlnet.authentication_services` para **NONE** sólo en los siguientes entornos:

Distribución de la base de datos	Versión de Oracle	Es compatible con la autenticación de la base de datos de destino	Es compatible con la autenticación de base de datos para la instancia de ASM
Cualquier base de datos que no sea ASM y que no sea RAC	Oracle 10g y Oracle 11g (inferior a 11.2.0.3)	Sí	No
Base de datos ASM independiente en UNIX	Oracle 11.2.0.3 y posterior	Sí	Sí
Instancia de ASM en base de datos RAC en UNIX	Oracle 11.2.0.3	No	No
Base de datos RAC en NFS	Oracle 11.2.0.3	Sí	No



Después de deshabilitar `sqlnet.authentication_services` y cambie el método de autenticación a autenticación de base de datos, debe configurar `sqlnet.authentication_services` para **NONE**.

Si accede a un perfil por primera vez, debe introducir la contraseña de su perfil. Después de introducir sus credenciales, es posible ver los backups de la base de datos dentro del perfil.

## Crear perfiles

Al crear perfiles, puede asignar una cuenta de usuario de base de datos Oracle concreta al perfil. Puede establecer la política de retención para el perfil, habilitar la protección de backup en el almacenamiento secundario para todos los backups mediante este perfil, y establecer el número de retención y la duración de cada clase de retención.

### Acerca de esta tarea

Si no se proporcionan los valores de `-login`, `-password`, y `-port` Parámetros de la base de datos, el modo de autenticación del sistema operativo (SO) utiliza las credenciales predeterminadas.

Al crear un perfil, SnapManager realiza una comprobación de elegibilidad de restauración para determinar el mecanismo de restauración que puede usarse para restaurar la base de datos. Si la base de datos se encuentra en un qtree y el volumen principal no es apto para una restauración rápida o basada en el volumen, es posible que el análisis no se realice correctamente.

SnapManager (3.2 o posterior) permite separar los archivos de registro de archivos de los archivos de datos al crear un nuevo perfil o actualizar un perfil existente. Después de separar el backup con el perfil, se puede crear únicamente el backup de los archivos de datos o el backup de solo registro del archivo de la base de datos. Se puede usar el nuevo perfil o el perfil actualizado para crear el backup que contiene tanto los archivos de datos como los archivos de registro de archivos. Sin embargo, no se puede utilizar el perfil para crear el backup completo ni revertir la configuración.

### Perfiles para crear copias de seguridad completas y parciales

Es posible crear perfiles para crear un backup completo de la base de datos que contenga los archivos de datos, los archivos de control, los archivos de registro de archivos y el backup parcial de la base de datos que contenga los archivos de datos o espacios de tablas especificados, todos los archivos de control y todos los archivos de registro de archivos. SnapManager no permite crear backups de registros de archivos independientes con los perfiles creados para backups completos y parciales.

### Perfiles para la creación de copias de seguridad sólo de archivos de datos y copias de seguridad sólo archivogs

Al crear un perfil nuevo, puede incluir `-separate-archivelog-backups` para separar el backup de los registros de archivo de la copia de seguridad del archivo de datos. También puede actualizar el perfil existente para separar la copia de seguridad del archivo de datos.

Al usar las opciones nuevas de perfil para separar los backups de los registros de archivos, es posible realizar las siguientes operaciones de SnapManager:

- Cree un backup de registro de archivos
- Eliminar un backup de registro de archivos
- Montar un backup de registro de archivos

- Liberar un backup de registro de archivo

Al crear el perfil para separar los backups de los registros de archivos del backup de archivos de datos, si los archivos de registro de archivos no existen en la base de datos para la cual se crea el perfil, se muestra un mensaje de advertencia.



Archived log file does not exist in the active file system. The archived log file versions earlier than the <archive log thread version> log file will not be included in the backup

Incluso si se crean backups para esta base de datos, los archivos de registro de archivos no están disponibles en los backups de la base de datos.



Si encuentra un error al crear un perfil, utilice `smsap system dump` comando. Después de crear un perfil, si encuentra un error, utilice `smsap operation volcado` y `smsap profile dump` comandos.

1. Para crear un perfil con un nombre de usuario, una contraseña y un puerto (autenticación de Oracle), introduzca el comando siguiente:

```

smsap profile create -profileprofile [-profile-password profile_password]
-repository-dbname repo_dbname -host repo_host -port repo_port -login
-username repo_username -database -dbname db_dbname -host db_host [-siddb_sid]
[-login [-username db_username-password db_password -port db_port][-
asminstance -asmusername asminstance_username -asmpassword
asminstance_password]] [-rman {-controlfile | {-login-username rman_username
-password rman_password -tnsname rman_tnsname} } ] -osaccount osaccount-
osgroup osgroup [-retain [-hourly [-count n] [-duration m]] [-daily [-count n]
[-duration m]] [-weekly [-count n] [-duration m]] [-monthly [-count n] [-
duration m]]] [-comment comment][-snapname-pattern pattern][-protect [-
protection-policy policy_name]] [-summary-notification] [-notification [-
success-email email_address1, email_address2 -subject subject_pattern] [-
failure-email email_address1, email_address2 -subject subject_pattern]][-
separate-archivelog-backups-retain-archivelog-backups-hours hours | -days days
| -weeks weeks | -months months [-protect [-protection-policy policy_name] |
-noprotect] [-include-with-online-backups | -no-include-with-online-backups]]
[-dump]

```

Las demás opciones para este comando son las siguientes:

```
[-force] [-noprompt]
```

```
[-quiet | verbose]
```





Para entornos de Real Application Clusters (RAC), al crear un perfil nuevo debe proporcionar el valor de `db_unique_name` parámetro como `db_dbname`.

También puede incluir otras opciones al crear perfiles, dependiendo de cómo desee tener acceso a la base de datos.

Si...	Realice lo siguiente...
<p><b>Desea utilizar la autenticación del sistema operativo para crear el perfil</b></p>	<p>Especifique las variables para una cuenta de sistema operativo en el grupo DBA (normalmente la cuenta utilizada para instalar Oracle). En lugar de agregar el nombre de usuario, la contraseña y el puerto, especifique lo siguiente:</p> <ul style="list-style-type: none"> <li>• <code>-osaccount account_name</code> como nombre de la cuenta del sistema operativo</li> <li>• <code>-osgroup osgroup</code> como grupo asociado a la cuenta del sistema operativo</li> </ul>
<p><b>Desea utilizar la autenticación de instancia de Automatic Storage Management (ASM) para crear el perfil</b></p>	<p>Especifique las credenciales para la autenticación de instancias de ASM.</p> <ul style="list-style-type: none"> <li>• <code>-asmusername asminstance_username</code> Es el nombre de usuario utilizado para iniciar sesión en la instancia de ASM.</li> <li>• <code>-asmpassword asminstance_password</code> Es la contraseña que se utiliza para iniciar sesión en la instancia de ASM.</li> </ul>
<p><b>Desea utilizar la autenticación de base de datos para crear un perfil</b></p>	<p>Especifique los detalles de inicio de sesión de la base de datos. Si la contraseña contiene caracteres especiales como el signo de exclamación (!), el signo de dólar (\$) o el acento grave ('), SnapManager no permite crear el perfil autenticado de la base de datos desde la interfaz de línea de comandos (CLI).</p>
<p><b>Está utilizando un catálogo como repositorio de Oracle Recovery Manager (RMAN)</b></p>	<p>Especifique las siguientes opciones y variables:</p> <ul style="list-style-type: none"> <li>• <code>-tnsname tnsname</code> como el nombre de tnsname definido en <code>tnsnames.ora</code> archivo.</li> <li>• <code>-login -username username</code> Como nombre de usuario requerido para conectarse al catálogo de RMAN.</li> </ul> <p>Si no se especifica, SnapManager utiliza la información de autenticación del sistema operativo. No se puede usar la autenticación del sistema operativo con bases de datos RAC.</p> <ul style="list-style-type: none"> <li>• <code>-password password</code> Como contraseña de RMAN necesaria para conectarse al catálogo de RMAN.</li> </ul>
<p><b>Está utilizando el archivo de control como repositorio de RMAN</b></p>	<p>Especifique el <code>-controlfile</code> opción.</p>

Si...	Realice lo siguiente...
<b>Desea especificar una política de retención de copias de seguridad para copias de seguridad</b>	<p data-bbox="841 159 1482 296">Especifique el recuento de retención o la duración de una clase de retención, o ambos. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora, días por día).</p> <ul data-bbox="865 331 1482 936" style="list-style-type: none"><li data-bbox="865 331 1482 468">• <code>-hourly</code> es la clase de retención por hora, para la cual <code>[-count n]</code> <code>[-duration m]</code> son el recuento de retención y la duración de la retención, respectivamente.</li><li data-bbox="865 489 1482 625">• <code>-daily</code> es la clase de retención diaria, para la cual <code>[-count n]</code> <code>[-duration m]</code> son el recuento de retención y la duración de la retención, respectivamente.</li><li data-bbox="865 646 1482 783">• <code>-weekly</code> es la clase de retención semanal, para la cual <code>[-count n]</code> <code>[-duration m]</code> son el recuento de retención y la duración de la retención, respectivamente.</li><li data-bbox="865 804 1482 940">• <code>-monthly</code> es la clase de retención mensual, para la cual <code>[-count n]</code> <code>[-duration m]</code> son el recuento de retención y la duración de la retención, respectivamente.</li></ul>

Si...	Realice lo siguiente...
<p><b>Desea activar la protección de copia de seguridad para el perfil</b></p>	<p>Especifique las siguientes opciones y variables:</p> <ul style="list-style-type: none"> <li>• <code>-protect</code> permite la protección de backups.</li> </ul> <p>Si utiliza Data ONTAP funcionando en 7-Mode, esta opción crea un conjunto de datos de aplicación en el servidor de Data Fabric Manager (DFM) y añade miembros relacionados con la base de datos, los archivos de datos, los archivos de control y los registros de archivos. Si el conjunto de datos ya existe, se vuelve a utilizar el mismo conjunto de datos cuando se crea un perfil.</p> <ul style="list-style-type: none"> <li>• <code>-protection-policy policy</code> permite especificar la política de protección.</li> </ul> <p>Si se usa Data ONTAP en 7-Mode y SnapManager se integra con Protection Manager, es necesario especificar una de las políticas de Protection Manager.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> Para enumerar las posibles políticas de protección, utilice <code>smSAP protection-policy list</code> comando.</p> </div> <p>Si utiliza Clustered Data ONTAP, debe seleccionar <i>SnapManager_CDOT_Mirror</i> o <i>SnapManager_CDOT_Vault</i>.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> Se produce un error en la operación de creación de perfiles en las siguientes situaciones:</p> <ul style="list-style-type: none"> <li>◦ Si utiliza Clustered Data ONTAP, pero seleccione Protection Manager policy</li> <li>◦ Si utiliza Data ONTAP operando en 7-Mode, pero seleccione la política de <i>SnapManager_CDOT_Mirror</i> o <i>SnapManager_CDOT_Vault</i></li> <li>◦ Si creó la relación de SnapMirror pero seleccionó <i>SnapManager_CDOT_Vault</i> o creó la relación de SnapVault, pero seleccionó la política <i>SnapManager_CDOT_Mirror</i></li> <li>◦ Si no ha creado la relación de SnapMirror o SnapVault, pero ha seleccionado la política <i>SnapManager_CDOT_Vault</i> o <i>SnapManager_CDOT_Mirror</i></li> </ul> </div> <p><code>-noprotect</code> indica que no se protegen los backups de la base de datos creados con el perfil.</p>



Si...	Realice lo siguiente...
<p><b>Desea activar la notificación por correo electrónico para el estado de finalización de las operaciones de la base de datos</b></p>	<p>Especifique las siguientes opciones y variables:</p> <ul style="list-style-type: none"> <li>• <code>-summary-notification</code> permite configurar una notificación por correo electrónico de resumen para varios perfiles en una base de datos de repositorio.</li> <li>• <code>-notification</code> permite recibir una notificación por correo electrónico para comprobar el estado de finalización de la operación de la base de datos de un perfil.</li> <li>• <code>-success-email email_address2</code> permite recibir una notificación por correo electrónico sobre la operación correcta de la base de datos mediante un perfil nuevo o existente.</li> <li>• <code>-failure-email email_address2</code> permite recibir una notificación por correo electrónico en la operación de base de datos fallida realizada mediante un perfil nuevo o existente.</li> <li>• <code>-subject subject_text</code> especifica el texto del asunto para la notificación por correo electrónico mientras se crea un perfil nuevo o un perfil existente. Si los ajustes de notificación no están configurados para el repositorio y intenta configurar las notificaciones de perfil o resumen mediante la CLI, se registra el siguiente mensaje en el registro de consola: SMSAP-14577: Notification Settings not configured.</li> </ul> <p>Si configuró los ajustes de notificación e intenta configurar la notificación de resumen mediante la CLI sin habilitar la notificación de resumen para el repositorio, se muestra el siguiente mensaje en el registro de consola: SMSAP-14575: Summary notification configuration not available for this repository</p>

Si...	Realice lo siguiente...
<p><b>Desea hacer una copia de seguridad de los archivos de registro de archivos por separado de los archivos de datos</b></p>	<p>Especifique las siguientes opciones y variables:</p> <ul style="list-style-type: none"> <li>• <code>-separate-archivelog-backups</code> permite separar el backup de registros de archivo del backup del archivo de datos.</li> <li>• <code>-retain-archivelog-backups</code> establece la duración de la retención para los backups de registros de archivo. Debe especificar una duración de retención positiva.</li> </ul> <p>Los backups de los registros de archivos se conservan según la duración de retención de los registros de archivo. Los backups de los archivos de datos se retienen en función de las políticas de retención existentes.</p> <ul style="list-style-type: none"> <li>• <code>-protect</code> permite la protección en los backups de registros de archivos.</li> <li>• <code>-protection-policy</code> establece la política de protección en los backups de registros de archivo.</li> </ul> <p>Los backups de registros de archivos se protegen de acuerdo con la política de protección de registros de archivos. Los backups de los archivos de datos se protegen de acuerdo con las políticas de protección existentes.</p> <ul style="list-style-type: none"> <li>• <code>-include-with-online-backups</code> incluye el backup de registros de archivos junto con el backup de la base de datos en línea.</li> </ul> <p>Esta opción permite crear un backup de archivos de datos en línea y un backup de registros de archivos juntos para el clonado. Cuando se configura esta opción, siempre que se crea un backup de archivos de datos en línea, se crean los backups de los registros de archivos junto con los archivos de datos inmediatamente.</p> <ul style="list-style-type: none"> <li>• <code>-no-include-with-online-backups</code> no incluye el backup de registros de archivo junto con el backup de la base de datos.</li> </ul>
<p><b>Puede recopilar los archivos de volcado después de que la operación de creación de perfil se haya realizado correctamente</b></p>	<p>Especifique la opción <code>-dump</code> al final del <code>profile create</code> comando.</p>

Cuando se crea un perfil, SnapManager analiza los archivos en caso de que posteriormente se desee realizar una operación de restauración basada en volumen en los archivos especificados en el perfil.

## Nomenclatura de copias Snapshot

Puede especificar una convención o un patrón de nomenclatura para describir las copias de Snapshot relacionadas con el perfil que crea o actualiza. También puede incluir texto personalizado en todos los nombres de copias de Snapshot.

Puede cambiar el patrón de nomenclatura de las copias Snapshot al crear un perfil o después de crear el perfil. El patrón actualizado se aplica solo a las copias Snapshot que todavía no se han producido; las copias Snapshot que existen conservan el patrón de snapname anterior.

Los siguientes ejemplos muestran los dos nombres de copias Snapshot tomados de un volumen. La segunda copia snapshot que se muestra tiene *F\_H\_1* en la mitad de su nombre. El "1" indica que es la primera copia snapshot tomada en el conjunto de backup. La primera copia Snapshot enumerada es la más reciente y tiene una «2», lo que significa que se toma la segunda copia Snapshot. La copia Snapshot "1" incluye los archivos de datos; la copia Snapshot "2" incluye los archivos de control. Dado que las copias snapshot del archivo de control deben realizarse después de realizar la copia snapshot del archivo de datos, se necesitan dos copias snapshot.

```
smsap_profile_sid_f_h_2_8ae482831ad14311011ad14328b80001_0  
smsap_profile_sid_f_h_1_8ae482831ad14311011ad14328b80001_0
```

El patrón predeterminado incluye el smid requerido, como se muestra en la siguiente:

- Patrón predeterminado: Smsap\_{profile}\_{dB-sid}\_{scope}\_{mode}\_{smid}
- Ejemplo: Smsap\_my\_profile\_rac51\_f\_h\_2\_8abc01e915a55ac50115a55acc8d0001\_0

Es posible usar las siguientes variables en el nombre de la copia Snapshot:

Nombre de la variable	Descripción	Valor de ejemplo
smid (obligatorio)	El ID único de SnapManager es el único elemento requerido cuando se crea un nombre para la copia Snapshot. Este ID garantiza la creación de un nombre de snapshot único.	8abc01e915a55ac50115a55ac8d0001_0
Clase (opcional)	Clase de retención asociada al backup para el perfil e indicada por cada hora (h), día (d), semanal (w), mensual (m) o ilimitado (u).	d
Comentario (opcional)	Comentario asociado al backup del perfil. Los espacios en este campo se convertirán en guiones bajos cuando se complete el nombre de la copia Snapshot.	sample_comment_spaces_rereemplazado

Nombre de la variable	Descripción	Valor de ejemplo
Fecha (opcional)	Fecha en la que se realiza la copia de seguridad para el perfil. Los valores de fecha se rellenarán con ceros si es necesario. (aaaammdd)	20070218
db-host (opcional)	Nombre de host de la base de datos asociado con el perfil que se va a crear o actualizar.	mi_host
db-name (opcional)	Nombre de la base de datos asociada con la copia de Snapshot que crea.	rac5
db-sid (opcional)	sid de base de datos asociado con la copia de Snapshot que crea.	racer51
Etiqueta (opcional)	Etiqueta asociada al backup para el perfil.	etiqueta_muestra
Modo (opcional)	Especifica si el backup se completa en línea (h) o sin conexión (c).	h
Perfil (opcional)	El nombre del perfil asociado con el backup que cree.	mi_perfil
Alcance (opcional)	Especifica si el backup está completo (f) o parcial (p).	f
Tiempo (opcional)	Hora a la que se produce el backup para el perfil. Los valores de hora de esta variable utilizan el reloj de 24 horas y están acolchados con ceros si es necesario. Por ejemplo, 5:32 y 8 segundos se muestran como 053208 (hhmmss).	170530
Zona horaria (opcional)	Zona horaria especificada para el host de la base de datos de destino.	EST
Usertext (opcional)	Texto personalizado que puede introducir.	prod



SnapManager para SAP no admite el símbolo de dos puntos (:) en formas largas de los nombres para las copias Snapshot.

## Cambiar el nombre de los perfiles

SnapManager le permite cambiar el nombre del perfil al actualizar el perfil. Las funcionalidades de SnapManager establecidas en el perfil y las operaciones que se pueden realizar antes de cambiar de nombre se conservan para el perfil cuyo nombre ha cambiado.

## Lo que necesitará

- Debe asegurarse de que no haya operaciones SnapManager en ejecución en el perfil mientras cambia el nombre del perfil.

## Acerca de esta tarea

Es posible cambiar el nombre del perfil tanto en la interfaz de línea de comandos (CLI) de SnapManager como en la interfaz gráfica de usuario (GUI). Al actualizar el perfil, SnapManager verifica y actualiza el nombre del perfil en el repositorio.



SnapManager no admite cambiar el nombre del perfil en la ventana de actualización de varios perfiles.

Cuando proporcione un nuevo nombre de perfil, el nuevo nombre de perfil se añadirá a la caché de credenciales del cliente y se eliminará el nombre del perfil anterior. Al cambiar el nombre del perfil desde un cliente, sólo se actualiza la caché de credenciales de ese cliente. Debe ejecutar el `smsap profile sync` comando de cada cliente para actualizar la nueva caché de credenciales con el nuevo nombre de perfil.

Puede establecer la contraseña del perfil mediante `smsap credential set` comando.

Si se incluyó el nombre de perfil en un patrón de nomenclatura de copias Snapshot, al cambiar el nombre de un perfil, se actualiza el nuevo nombre del perfil. Todas las operaciones SnapManager que se realizan en el perfil utilizan el nuevo nombre del perfil. Los backups creados con el perfil anterior siguen teniendo el nombre del perfil anterior y se usan para realizar otras operaciones de SnapManager.

Si va a realizar la actualización gradual de los hosts del servidor SnapManager, debe asegurarse de realizar la actualización completa antes de cambiar el nombre del perfil.

El nuevo nombre del perfil sólo se actualiza desde el cliente SnapManager desde el que se realiza la solicitud. Los clientes SnapManager conectados al servidor SnapManager no reciben notificaciones sobre el cambio en el nombre del perfil. Puede comprobar el registro de operaciones para conocer el cambio en el nombre del perfil.



Si una operación de backup programada comienza en el momento de cambiar el perfil, entonces se produce un error en la operación programada.

## Paso

1. Introduzca el siguiente comando:

```
smsap profile update -profileprofile [-new-profile new_profile_name]
```

## Cambiar contraseñas de perfil

Para proteger los perfiles existentes en el repositorio, debe actualizar las contraseñas de los perfiles. Puede aplicar esta contraseña actualizada al crear una copia de seguridad con este perfil.

## Paso

1. Para actualizar la contraseña de perfil de un perfil existente, escriba este comando:

```
smsap profile update -profile profile_name -profile-password password
```

## Restablecer la contraseña del perfil

Puede restablecer la contraseña del perfil si no recuerda la contraseña que ha proporcionado al crear el perfil.

### Lo que necesitará

- Debe asegurarse de que el servidor SnapManager esté en ejecución en la base de datos del repositorio.
- Debe tener las credenciales de usuario raíz del host en el que reside la base de datos del repositorio.
- Debe asegurarse de que el perfil no esté en uso para ninguna operación cuando se restablezca la contraseña para ese perfil.

### Acerca de esta tarea

Puede restablecer la contraseña desde la interfaz de línea de comandos o desde la interfaz gráfica de usuario de SnapManager. Al restablecer la contraseña, SnapManager consulta al servidor SnapManager en el host de repositorios para identificar el sistema operativo para el host de repositorios. Debe introducir las credenciales de usuario autorizado para conectarse con el host de repositorios. El servidor SnapManager autentica a los usuarios con sus credenciales de raíz en la base de datos de repositorios. Cuando la autenticación se realiza correctamente, SnapManager restablece la contraseña del perfil en el servidor SnapManager con la nueva contraseña.



SnapManager no mantiene el historial de las operaciones de restablecimiento de contraseña.

### Paso

1. Restablezca la contraseña del perfil. Para ello, introduzca el siguiente comando:

```
smsap password reset -profile profile [-profile-password profile_password] [-repository-hostadmin-password admin_password]
```

## Autorizar el acceso a los perfiles

Además del control de acceso basado en roles (RBAC), SnapManager permite configurar una contraseña para un perfil para evitar el acceso no autorizado.

### Paso

1. Introduzca el siguiente comando:

```
smsap credential set -profile -name profile_name [-password password]
```

## Verificar perfiles

Puede comprobar que un perfil existente está configurado correctamente. Cuando se verifica un perfil, SnapManager comprueba si el entorno del perfil que se ha especificado y verifica que el perfil está configurado y que la base de datos de este perfil esté accesible.

### Paso

1. Para verificar si el perfil está configurado correctamente, escriba el siguiente comando:

```
smsap profile verify -profile profile_name
```

## Actualizar perfiles

Puede actualizar los perfiles para modificar la contraseña del perfil, la cantidad de backups que se deben retener, el acceso a la base de datos, la autenticación del sistema operativo (SO) con la autenticación de la base de datos y viceversa, e información sobre el host. Si cambia la información de contraseña de la base de datos Oracle, también debe cambiar esa información en el perfil.

### Acerca de esta tarea

Si la política de protección está habilitada en el perfil, no podrá cambiar la política mediante SnapManager. El administrador de almacenamiento debe cambiar la política mediante la consola de Protection Manager.

SnapManager (3.2 o posterior) permite actualizar el perfil para separar los backups de registros de archivos de los backups de archivos de datos mediante el `-separate-archivelog-backups` opción. Es posible especificar una duración de retención y una política de protección separadas para el backup de registros de archivos. SnapManager le permite incluir el backup de registros de archivos junto con el backup de base de datos en línea. También puede crear un backup de archivo de datos en línea y un backup de registro de archivo juntos para clonar. Cuando se crea un backup de archivos de datos en línea, los backups de registros de archivos se crean inmediatamente junto con los archivos de datos.

### Pasos

1. Introduzca el siguiente comando:

```
smsap profile update -profile profile [-new-profile new_profile_name] [-profile-password profile_password] [-database-dbname db_dbname -host db_host [-sid db_sid] [-login -username db_username -password db_password -port db_port] [-asminstance -asmusername asminstance_username -asmpassword asminstance_password] [{-rman{-controlfile | {-login -username rman_username -password rman_password -tnsname rman_tnsname}} | -remove-rman]-osaccount osaccount -osgroup osgroup [-retain [-hourly [-count n] [-duration m]] [-daily [-count n] [-duration m]] [-weekly [-count n] [-duration m]] [-monthly [-count n] [-duration m]]] [-comment comment] [-snapname -pattern pattern] [[-protect [-protection-policy policy_name]] | [-noprotect]] [-summary-notification] [-notification [-success-email email_address1, email_address2 -subject subject_pattern] [-failure-email email_address1, email_address2 -subject subject_pattern]] [-separate-archivelog-backups-retain-archivelog-backups-hours hours | -days days | -weeks weeks | -months months [-protect [-protection-policy policy_name] | -noprotect] [-include-with-online-backups | -no-include-with-online-backups]] [-dump]
```

Las demás opciones para este comando son las siguientes:

```
[-force] [-noprompt]
```


```
[-quiet | verbose]
```

Si desea...	Realice lo siguiente...
<b>Cambie el perfil para utilizar la autenticación del sistema operativo</b>	<p>En lugar de agregar el nombre de usuario, la contraseña y el puerto, especifique lo siguiente:</p> <ul style="list-style-type: none"> <li>• <code>-osaccount account_name</code> como nombre de la cuenta del sistema operativo</li> <li>• <code>-osgroup osgroup</code> Como grupo asociado a la cuenta del sistema operativo, normalmente la cuenta utilizada para instalar Oracle</li> </ul>
<b>Utilice la autenticación de instancia de Automatic Storage Management (ASM) para crear el perfil</b>	<p>Especifique las credenciales para la autenticación de instancias de ASM.</p> <ul style="list-style-type: none"> <li>• <code>-asmusername asminstance_username</code> Es el nombre de usuario utilizado para iniciar sesión en la instancia de ASM.</li> <li>• <code>-asmpassword asminstance_password</code> Es la contraseña que se utiliza para iniciar sesión en la instancia de ASM.</li> </ul>
<b>Utilice un catálogo como repositorio de Oracle Recovery Manager (RMAN) o elimine RMAN</b>	<p>Especifique las siguientes opciones y variables:</p> <ul style="list-style-type: none"> <li>• <code>-tnsname tnsname</code> como el nombre de tnsname definido en <code>tnsnames.ora</code> archivo.</li> <li>• <code>-login -username username</code> Como nombre de usuario requerido para conectarse al catálogo de RMAN.</li> </ul> <p>Si no se especifica, SnapManager utiliza la información de autenticación del sistema operativo. No se puede utilizar la autenticación del sistema operativo con bases de datos de Real Application Clusters (RAC).</p> <ul style="list-style-type: none"> <li>• <code>-password password</code> Como contraseña de RMAN necesaria para conectarse al catálogo de RMAN.</li> <li>• <code>-controlfile</code> Si utiliza el archivo de control como repositorio de RMAN.</li> <li>• <code>-remove-rman</code> Para quitar RMAN.</li> </ul>



Si desea...	Realice lo siguiente...
<b>Cambiar la política de retención de copias de seguridad para copias de seguridad de la base de datos en el perfil</b>	<p>Especifique el recuento de retención o la duración de la retención para una clase de retención, o ambos, para cambiar la política de retención. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora, días por día).</p> <ul style="list-style-type: none"> <li>• <code>-hourly</code> es la clase de retención por hora, para la cual <code>[-count n] [-duration m]</code> son el recuento de retención y la duración de la retención, respectivamente.</li> <li>• <code>-daily</code> es la clase de retención diaria, para la cual <code>[-count n] [-duration m]</code> son el recuento de retención y la duración de la retención, respectivamente.</li> <li>• <code>-weekly</code> es la clase de retención semanal, para la cual <code>[-count n] [-duration m]</code> son el recuento de retención y la duración de la retención, respectivamente.</li> <li>• <code>-monthly</code> es la clase de retención mensual, para la cual <code>[-count n] [-duration m]</code> son el recuento de retención y la duración de la retención, respectivamente.</li> </ul>
<b>Desactive la protección de copia de seguridad para el perfil</b>	<p>Especifique <code>-noprotect</code> para no proteger los backups de la base de datos creados con el perfil. Para un perfil que tenga <code>-protect</code> activado, si desea deshabilitar la protección, se mostrará un mensaje de advertencia que indica que esta acción eliminará el conjunto de datos y no podrá restaurar o clonar backups para este perfil.</p>

Si desea...	Realice lo siguiente...
<p><b>Activar notificaciones por correo electrónico para el estado de finalización de las operaciones de la base de datos</b></p>	<p>Especifique las siguientes opciones y variables:</p> <ul style="list-style-type: none"> <li>• <code>-summary-notification</code> permite configurar una notificación por correo electrónico de resumen para varios perfiles en una base de datos de repositorio.</li> <li>• <code>-notification</code> permite recibir una notificación por correo electrónico sobre el estado de finalización de la operación de la base de datos de un perfil.</li> <li>• <code>-success -email email_address2</code> permite recibir una notificación por correo electrónico tras la finalización de una operación de base de datos correcta mediante un perfil nuevo o existente.</li> <li>• <code>-failure -email email_address2</code> permite recibir una notificación por correo electrónico en una operación de base de datos fallida realizada mediante un perfil nuevo o existente.</li> <li>• <code>-subject subject_text</code> especifica el texto del asunto para la notificación por correo electrónico al crear un perfil nuevo o un perfil existente. Si los ajustes de notificación no están configurados para el repositorio y intenta configurar las notificaciones de perfil o resumen mediante la interfaz de línea de comandos (CLI), se registra el siguiente mensaje en el registro de consola: SMSAP-14577: Notification Settings not configured.</li> </ul> <p>Si configuró los ajustes de notificación e intenta configurar las notificaciones de resumen mediante la CLI sin habilitar la notificación de resumen para el repositorio, se registra el siguiente mensaje en el registro de consola: SMSAP-14575: Summary notification configuration not available for this repository</p>

Si desea...	Realice lo siguiente...
<p><b>Actualice el perfil para crear una copia de seguridad de los archivos de registro de archivos por separado</b></p>	<p>Especifique las siguientes opciones y variables:</p> <ul style="list-style-type: none"> <li>• <code>-separate-archivelog-backups</code> permite crear un backup de los archivos de registro de archivos independientemente de los archivos de la base de datos.</li> </ul> <p>Después de especificar esta opción, puede crear una copia de seguridad sólo de archivos de datos o una copia de seguridad sólo de archivelogs. No es posible crear un backup completo. Además, no puede revertir la configuración del perfil separando la copia de seguridad. SnapManager conserva los backups según la política de retención de los backups que se crearon antes de usar un backup de solo archivado.</p> <ul style="list-style-type: none"> <li>• <code>-retain-archivelog-backups</code> establece la duración de la retención para los backups de registros de archivo.</li> </ul> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> Si actualiza el perfil por primera vez, es posible separar los backups del registro de archivos de los archivos de datos mediante el <code>-separate-archivelog-backups</code> opción; debe proporcionar la duración de la retención de los backups de registros de archivos mediante la <code>-retain-archivelog-backups</code> opción. La configuración de la duración de la retención es opcional cuando se actualiza el perfil más adelante.</p> </div> <ul style="list-style-type: none"> <li>• <code>-protect</code> Crea un conjunto de datos de la aplicación en el servidor de Data Fabric Manager (DFM) y añade miembros relacionados con la base de datos, los archivos de datos, los archivos de control y los registros de archivos.</li> </ul> <p>Si el conjunto de datos existe, se vuelve a utilizar cuando se crea un perfil.</p> <ul style="list-style-type: none"> <li>• <code>-protection-policy</code> establece la política de protección en los backups de registros de archivo.</li> <li>• <code>-include-with-online-backups</code> especifica que el backup de registros de archivo se incluya junto con el backup de la base de datos.</li> <li>• <code>-no-include-with-online-backups</code> especifica que el backup del archivo de registro de archivos no se incluye junto con el backup de base de datos.</li> </ul>
<p><b>Cambiar el nombre de host de la base de datos de destino</b></p>	<p>Especifique <code>-host new_db_host</code> para cambiar el nombre de host del perfil.</p>

Si desea...	Realice lo siguiente...
<b>Recopilar los archivos de volcado después de la operación de actualización de perfil</b>	Especifique el <code>-dump</code> opción.

2. Para ver el perfil actualizado, escriba el comando siguiente: `smsap profile show`

## Eliminar perfiles

Puede eliminar un perfil en cualquier momento, siempre que no contenga copias de seguridad correctas o incompletas. Es posible eliminar perfiles que contengan copias de seguridad liberadas o eliminadas.

### Paso

1. Para eliminar un perfil, escriba este comando:

```
smsap profile delete -profile profile_name
```

## Realizar backups de bases de datos

SnapManager permite realizar backups de datos en recursos de almacenamiento local mediante un scriptor de posprocesamiento gracias a la protección de backups en recursos de almacenamiento secundarios o terciarios. La opción de realizar backups en el almacenamiento secundario proporciona una capa adicional que conserva los datos en caso de desastre.

SnapManager también permite a los administradores de almacenamiento configurar sus backups según sus planes de normativas. Mediante el uso de SnapManager, los administradores pueden identificar backups que no cumplan con los requisitos de las normativas y rectificarlos de inmediato.

SnapManager ofrece las siguientes opciones para realizar backups, restaurar y recuperar los datos de la base de datos:

- Realice una copia de seguridad de toda la base de datos o de una parte de ella.

Si realiza una copia de seguridad de una parte de la misma, especifique un grupo de tablespaces o un grupo de archivos de datos.

- Realice una copia de seguridad de los archivos de datos y de los archivos de registro de archivo por separado.
- Realice un backup de las bases de datos en el almacenamiento primario (también llamado almacenamiento local) y protéjalas al realizar un backup en un almacenamiento secundario o terciario (también llamado almacenamiento remoto).
- Programar copias de seguridad rutinarias.

### La diferencia entre SnapManager (3.2 o posterior) y las versiones anteriores de SnapManager

SnapManager (3.1 o anterior) permite crear backups completos de la base de datos que contienen archivos de datos, archivos de control y archivos de registro de archivos.

SnapManager (3.1 o anterior) solo administra los archivos de datos. Los archivos de registro de archivos se mantienen usando soluciones fuera de SnapManager.

SnapManager (3.1 o anterior) impone las siguientes restricciones en la gestión de los backups de las bases de datos:

- Impacto en el rendimiento

Cuando se realiza un backup de base de datos en línea completo (cuando la base de datos está en modo de backup), el rendimiento de la base de datos se reduce durante el periodo de tiempo hasta que se crea el backup. En SnapManager (3.2 o posterior), pueden realizarse backups de bases de datos limitados y backups frecuentes de registros de archivo. La realización de backups frecuentes de registros de archivos ayuda a evitar que la base de datos se coloque en modo de backup.

- Restauración y recuperación manuales

Cuando los archivos de registro de archivos necesarios no existen en el sistema de archivos activo, los administradores de la base de datos deben identificar qué backup contiene los archivos de registro de archivos, montar los backups de la base de datos y recuperar la base de datos restaurada. Este proceso requiere mucho tiempo.

- Restricciones de espacio

Cuando se crea un backup de la base de datos, los destinos de registro de archivos se llenan, lo que hace que la base de datos no responda hasta que se crea espacio suficiente en el almacenamiento. En SnapManager (3.2 o posterior), se pueden quitar los archivos de registro de archivos del sistema de archivos activo para liberar espacio periódicamente.

## **Por qué son importantes las copias de seguridad de archivos de registro**

Los archivos de registro de archivos son necesarios para avanzar la base de datos después de ejecutar una operación de restauración. Cada transacción en una base de datos Oracle se captura en los archivos archive log (si la base de datos está en el modo archive log). Los administradores de bases de datos pueden restaurar los backups de la base de datos con los archivos de registro de archivos.

## **Ventajas de las copias de seguridad archivelog-only**

- Proporciona una duración de retención independiente para backups de solo archivado

Puede tener menos duración de retención para los backups de solo archivado que se requieren para la recuperación.

- Protege los backups de solo archivado basados en políticas de protección de registros de archivos

Puede seleccionar diferentes políticas de protección para backups de solo archivado en función de sus necesidades.

- Mejora el rendimiento de la base de datos

- Consolida los backups de registros de archivos

SnapManager consolida los backups de registros de archivos cada vez que se realiza un backup liberando las copias de seguridad duplicadas de los registros de archivo.

## Qué son los backups de la base de datos SnapManager

SnapManager permite realizar distintas tareas de backup. Puede asignar clases de retención para especificar cuánto tiempo se puede retener la copia de seguridad; una vez alcanzado ese límite de tiempo, se elimina la copia de seguridad.

- Crear backups en el almacenamiento principal
- Cree backups protegidos en los recursos de almacenamiento secundario
- Compruebe que los backups se han realizado correctamente
- Ver una lista de backups
- Programar las copias de seguridad utilizando la interfaz gráfica de usuario
- Gestión de la cantidad de backups incorporados
- Libere recursos de backup
- Montar y desmontar backups
- Eliminar backups

SnapManager crea backups mediante una de las siguientes clases de retención:

- Cada hora
- Todos los días
- Semanal
- Mensual
- Ilimitada

Protection Manager debe instalarse para utilizar políticas de protección a fin de proteger los backups. Un backup puede tener uno de los siguientes estados de protección: No solicitado, no protegido o protegido.

Si se agregan nuevos archivos de datos a la base de datos, debe crear una copia de seguridad inmediatamente. Además, si restaura una copia de seguridad realizada antes de agregar los nuevos archivos de datos e intenta recuperarse a un punto después de agregar los nuevos archivos de datos, el proceso de recuperación automática podría fallar. Consulte la documentación de Oracle para obtener más información sobre el proceso de recuperación de los archivos de datos agregados después de una copia de seguridad.

## Qué son los backups completos y parciales

Puede elegir hacer una copia de seguridad de toda la base de datos o sólo una parte de ella. Si decide realizar una copia de seguridad de una parte de la base de datos, puede optar por realizar una copia de seguridad de un grupo de tablespaces o archivos de datos. Puede optar por realizar un backup separado de los espacios de tablas y los archivos de datos.

En la siguiente tabla, se enumeran los beneficios y las consecuencias de cada tipo de backup:

Tipo de backup	Ventajas	Desventajas
Lleno	Minimiza el número de copias de Snapshot. Para los backups en línea, cada espacio de tabla está en modo de backup durante todo el tiempo que lleva la operación de backup. SnapManager toma una copia snapshot por cada volumen que utiliza la base de datos, además de una copia snapshot por cada volumen que ocupan los archivos de registro.	Para los backups en línea, cada espacio de tabla está en modo de backup durante todo el tiempo que lleva la operación de backup.
Parcial	Minimiza la cantidad de tiempo que cada espacio de tabla pasa en modo de backup. SnapManager agrupa las copias snapshot que toma por espacio de tabla. Cada espacio de tabla está en modo de backup solo suficientemente tiempo para crear las copias Snapshot. Este método de agrupación de las copias Snapshot minimiza las escrituras de bloque físico en los archivos de registro durante un backup en línea.	El backup puede requerir la creación de copias Snapshot de varios espacios de tablas en el mismo volumen. Este método puede provocar que SnapManager cree varias copias Snapshot de un solo volumen durante la operación de backup.



Aunque puede realizar un backup parcial de, siempre debe realizar un backup completo de toda la base de datos.

### Los tipos de backup y la cantidad de copias de Snapshot

El tipo de backup (completo o parcial) afecta al número de copias Snapshot que crea SnapManager. Para un backup completo, SnapManager crea una copia snapshot de cada volumen, mientras que, para un backup parcial, SnapManager crea una copia snapshot de cada archivo de espacio de tabla.



Data ONTAP limita el número máximo de copias snapshot a 255 por volumen. Solo puede alcanzar este máximo si configura SnapManager para retener un gran número de backups en los que cada backup esté compuesto por numerosas copias de Snapshot.

Para mantener un pool adecuado de backups disponible a la vez que garantiza que no se alcance el límite máximo de copias Snapshot por volumen, debe eliminar backups cuando ya no sean necesarios. Puede configurar la política de retención de SnapManager para eliminar los backups correctos después de alcanzar un umbral específico para una frecuencia de backup específica. Por ejemplo, una vez que SnapManager crea cuatro backups diarios correctos, SnapManager elimina los backups diarios creados en el día anterior.

En las siguientes tablas, se muestra cómo SnapManager crea copias Snapshot según el tipo de backup. El ejemplo de las tablas supone que la base de datos Z incluye dos volúmenes, cada volumen incluye dos tablespaces (TS1 y TS2) y cada tablespace incluye dos archivos de base de datos (`ts1.data1`, `ts1.data2`, `ts2.data1`, y `ts2.data2`).

En estas tablas, se muestra cómo los dos tipos de backups producen diferentes cantidades de copias Snapshot.

SnapManager crea copias Snapshot a nivel de volumen en lugar del espacio de tabla, lo que reduce normalmente el número de copias Snapshot que debe crear.



Ambos backups también crean copias Snapshot de los archivos de registro.

Volúmenes en la base de datos	Tablespace TS1 (incluye 2 archivos de base de datos)	Tablespace TS2 (incluye 2 archivos de base de datos)	Se crearon copias Snapshot	Número total de copias Snapshot
/Vol/Vola	TS1.data1	TS2.data1	1 por volumen	2

Volúmenes en la base de datos	Tablespace TS1 (incluye 2 archivos de base de datos)	Tablespace TS2 (incluye 2 archivos de base de datos)	Se crearon copias Snapshot	Número total de copias Snapshot
/Vol/Vola	TS1.data1	TS2.data1	2 por archivo	4

### Backups completos en línea

Durante un backup online completo, SnapManager realiza un backup de toda la base de datos y crea copias Snapshot en el nivel del volumen (no en el nivel de espacio de tabla).

SnapManager crea dos copias Snapshot para cada backup. Si todos los archivos necesarios para la base de datos se encuentran en un único volumen, las dos copias de Snapshot aparecen en ese volumen.

Cuando se especifica un backup completo, SnapManager realiza las siguientes acciones:

1. Coloca toda la base de datos en el modo de copia de seguridad en línea
2. Crea copias snapshot de todos los volúmenes que contienen archivos de base de datos
3. Saca la base de datos del modo de backup en línea
4. Fuerza un conmutador de registro y, a continuación, archiva los archivos de registro

Esto también vacía la información de redo en el disco.

5. Genera archivos de control de copia de seguridad
6. Crea una copia snapshot de los archivos de registro y los archivos de control de copia de seguridad

Cuando se realiza un backup completo, SnapManager coloca toda la base de datos en el modo de backup en línea. Un tablespace individual (por ejemplo, /oracle/CER/sapdata1/system\_1/system.data1) está en el modo de copia de seguridad en línea más largo que determinados tablespaces o archivos de datos que se especificaron.

Cuando una base de datos entra en modo de backup, Oracle escribe bloques completos en los registros y no se limita a escribir el delta entre backups. Como las bases de datos trabajan más en modo de backup en línea, elegir un backup completo supone una mayor carga en el host.

Aunque realizar backups completos supone una mayor carga en el host, los backups completos requieren menos copias Snapshot, lo que produce menos requisitos de almacenamiento.



## Backups parciales en línea

En lugar de un backup completo, se puede optar por realizar un backup parcial de los espacios de tablas en una base de datos. Mientras SnapManager realiza una copia Snapshot de volúmenes para realizar backups *Full*, SnapManager realiza una copia Snapshot de cada espacio de tabla especificado para *parciales* backups.

Debido a que el nivel de tablespace es el nivel más bajo que Oracle permite en el modo de copia de seguridad, SnapManager procesa las copias de seguridad a nivel de tablespace, incluso si se especifica un archivo de datos en un tablespace.

Con un backup parcial, cada espacio de tabla existe en modo de backup durante un menor tiempo que en un backup completo. Durante un backup en línea, la base de datos siempre está disponible para los usuarios. No obstante, la base de datos debe realizar más trabajo y el host debe ejecutar más operaciones de I/O físicas. Asimismo, debido a que se realizan copias Snapshot de cada espacio de tabla especificado o cada espacio de tabla que contiene un archivo de datos especificado en lugar de todo el volumen, SnapManager realiza más copias Snapshot.

SnapManager realiza copias Snapshot de espacios de tablas o archivos de datos específicos. El algoritmo de copia de seguridad parcial es un bucle que SnapManager repite hasta que ha tomado una copia snapshot de cada tablespace o archivo de datos especificado.



Aunque se puede realizar un backup parcial, se recomienda realizar siempre un backup completo de toda la base de datos.

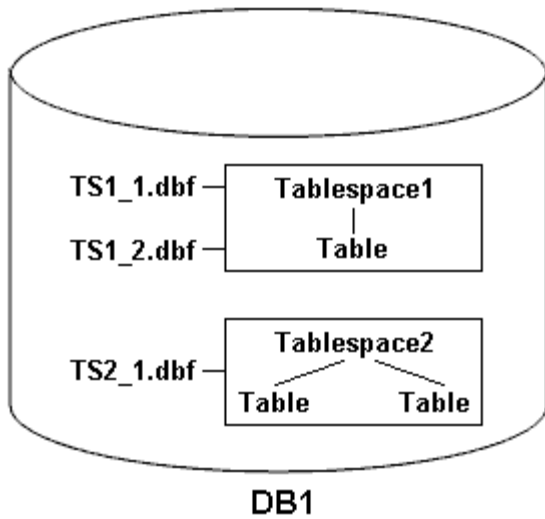
Durante un backup parcial, SnapManager realiza las siguientes acciones:

1. Coloca el tablespace que contiene los archivos de datos en modo de copia de seguridad.
2. Toma una copia Snapshot de todos los volúmenes utilizados por el espacio de tablas.
3. Quita el tablespace del modo de copia de seguridad.
4. Continúa este proceso, hasta que ha tomado una copia snapshot de todos los espacios de tablas o archivos.
5. Fuerza un conmutador de registro y, a continuación, archiva los archivos de registro.
6. Genera archivos de control de copia de seguridad.
7. Toma una copia snapshot de los archivos de registro y los archivos de control de copia de seguridad.

## Ejemplos de operaciones de backup, restauración y recuperación

Puede encontrar información sobre algunos de los escenarios de backup, restauración y recuperación que puede usar para lograr sus objetivos de protección de datos.

En la siguiente ilustración se muestra el contenido del tablespace:



En la ilustración, Tablespace1 tiene una tabla y dos archivos de base de datos asociados. Tablespace2 tiene dos tablas y un archivo de base de datos asociado.

En las siguientes tablas se describen algunos escenarios de backup, restauración y recuperación completos y parciales:

**Ejemplos de operaciones de backup, restauración y recuperación completas**

Backup completo	Restaurar	Recuperación
<p>SnapManager realiza un backup del todo en la base de datos DB1, incluidos los archivos de datos, los registros de archivo y los ficheros de control.</p>	<p>La restauración completa con archivos de control SnapManager restaura todos los archivos de datos, espacios de tablas y archivos de control en el backup.</p>	<p>Puede especificar una de las opciones siguientes:</p> <ul style="list-style-type: none"> <li>• SCN: Introduzca un SCN, como 384641.</li> <li>• Fecha/hora: Introduzca una fecha y hora de la copia de seguridad, como 2005-11-25:19:06:22.</li> <li>• La última transacción realizada a la base de datos.</li> </ul>
<p>Restauración completa sin archivos de control SnapManager restaura todos los espacios de tablas y archivos de datos, sin los archivos de control.</p>	<p>Cuando se restauran los archivos de datos o los espacios de tablas con archivos de control, se especifica una de las siguientes opciones:</p> <ul style="list-style-type: none"> <li>• Espacios de tabla</li> <li>• Archivos de datos</li> </ul>	<p>SnapManager recupera los datos a la última transacción realizada a la base de datos.</p>

**Ejemplos de operaciones de backup, restauración y recuperación parciales**

<b>Copia de seguridad parcial</b>	<b>Restaurar</b>	<b>Recuperación</b>
<p>Es posible elegir una de las siguientes opciones:</p> <ul style="list-style-type: none"> <li>• Espacios de tabla</li> </ul> <p>Puede especificar Tablespace1 y Tablespace2 o sólo uno de ellos.</p> <ul style="list-style-type: none"> <li>• Archivos de datos</li> </ul> <p>Puede especificar los tres archivos de base de datos (TS1_1.dbf, TS1_2.dbf y TS2_1.dbf), dos archivos o un archivo.</p> <p>Independientemente de la opción que seleccione, el backup incluirá todos los archivos de control. Los archivos de registro de archivos se incluyen en el backup parcial si el perfil no está habilitado para crear los backups de los registros de archivos por separado.</p>	<p>La restauración completa de SnapManager restaura todos los archivos de datos, los espacios de tablas y los archivos de control especificados en el backup parcial.</p>	<p>SnapManager recupera los datos a la última transacción realizada a la instancia de la base de datos.</p>

Copia de seguridad parcial	Restaurar	Recuperación
<p>Restaurar los archivos de datos o los espacios de tablas con los archivos de control SnapManager restaura uno de los siguientes elementos:</p> <ul style="list-style-type: none"> <li>• Todos los archivos de datos especificados</li> <li>• Todos los espacios de tablas especificados</li> </ul>	<p>Restaurar los archivos de datos o los espacios de tablas sin los archivos de control SnapManager restaura uno de los siguientes elementos:</p> <ul style="list-style-type: none"> <li>• Espacios de tabla <p>Especifique cualquiera de los espacios de tablas. SnapManager restaura solo los espacios de tablas especificados. Si la copia de seguridad contiene tablespace1, SnapManager sólo restaura ese tablespace.</p> </li> <li>• Archivos de datos <p>Especifique cualquiera de los archivos de la base de datos. SnapManager solo restaura los archivos de datos especificados. Si la copia de seguridad contiene archivos de base de datos (TS1_1.dbf y TS1_2.dbf), SnapManager sólo restaura esos archivos.</p> </li> </ul>	<p>Únicamente restaurar los archivos de control</p>

## Acerca del manejo de archivos de registro de archivo y archivos de control

SnapManager incluye los archivos de control y, opcionalmente, incluye los archivos de registro de archivo en cada backup. Los archivos de registro de archivo se usan para operaciones de recuperación.

La base de datos utiliza archivos de control para identificar nombres, ubicaciones y tamaños de los archivos de base de datos. SnapManager incluye los archivos de control en cada backup porque los archivos de control se utilizan en el proceso de restauración.

Se hace un seguimiento de los cambios en una base de datos mediante los redo logs en línea, que finalmente se archivan y se conocen como redo logs archivados (o archive logs). SnapManager (3.2 o posterior) permite realizar backups de los archivos de datos y los archivos de registro de archivos de forma independiente con diferentes retentions y frecuencias. SnapManager puede realizar backups únicamente de los registros de archivo o los backups combinados de archivos de datos y registros de archivos. SnapManager ofrece una gestión automatizada completa de los registros de archivos, y no requiere intervención manual para la recuperación de bases de datos. Además, permite la eliminación de registros de archivos de uno o más destinos de registros de archivos después de realizar el backup.



Para ver qué tablespaces y archivos de datos se incluyen en una copia de seguridad, utilice el comando backup show o la ventana Backup Properties.

La siguiente tabla muestra cómo SnapManager gestiona los archivos de control y de registro de archivo durante cada operación:

<b>Tipo de operación</b>	<b>Archivos de control</b>	<b>Archivos de registro de archivo</b>
Backup	Incluidas con cada backup	Se puede incluir con cada backup
Restaurar	Se pueden restaurar por separado o junto con los espacios de tablas o los ficheros de datos	Se puede usar para el proceso de recuperación

## Qué es la programación de backups de base de datos

Puede programar, actualizar y supervisar las copias de seguridad de las bases de datos mediante la ficha Programación de la interfaz gráfica de usuario.

La siguiente tabla aborda algunas preguntas frecuentes sobre la programación:

<b>Pregunta</b>	<b>Responda</b>
¿Qué ocurre con los backups programados al reiniciarse el servidor de SnapManager?	Cuando se reinicia el servidor SnapManager, éste reinicia automáticamente todas las programaciones. Sin embargo, SnapManager no realiza seguimiento de ninguna incidencia perdida.

Pregunta	Responda
<p>¿Qué sucede cuando se programan dos backups en dos bases de datos a la vez?</p>	<p>SnapManager inicia las operaciones de backup de uno en uno y luego permite que los backups se ejecuten en paralelo. Por ejemplo, si un administrador de bases de datos crea seis programaciones de backup diarias para seis perfiles de base de datos diferentes a las 00:00, los seis backups se ejecutan en paralelo.</p> <p>Si se programan varios backups en un único perfil de base de datos en un breve periodo de tiempo, el servidor SnapManager ejecutará solo la operación de backup con la duración de retención más larga.</p> <p>Antes de iniciar una operación de backup, SnapManager primero determina lo siguiente:</p> <ul style="list-style-type: none"> <li>• En los últimos 30 minutos, ¿ha creado otra programación correctamente un backup, con mayor retención, para el mismo perfil?</li> <li>• En los próximos 30 minutos, ¿intentará otra programación crear un backup, con mayor retención, para el mismo perfil?</li> </ul> <p>Si la respuesta a cualquiera de las dos preguntas es sí, SnapManager omite el backup.</p> <p>Por ejemplo, un administrador de bases de datos puede crear una programación diaria, semanal y mensual para un perfil de base de datos, y se prevé que todos los backups se realicen a las 1:00 a.m. En ese día del mes en el que se programan tres backups a la vez a las 1:00, SnapManager únicamente ejecutará la operación de backup en función de la programación mensual.</p> <p>La ventana de tiempo de 30 minutos se puede cambiar en un archivo de propiedades de SnapManager.</p>
<p>¿Con qué usuario se ejecuta la operación de backup?</p>	<p>La operación se ejecuta bajo el usuario que creó la programación. Sin embargo, es posible cambiarlo por su propio ID de usuario, si cuenta con credenciales válidas tanto para el perfil de base de datos como para el host. Por ejemplo, al iniciar las propiedades de copia de seguridad programada para la programación de copia de seguridad creada por Avida Davis, Stella Morrow puede seleccionar su ID de usuario en realizar esta operación como usuario para ejecutar la copia de seguridad programada.</p>

<b>Pregunta</b>	<b>Responda</b>
¿Cómo interactúa el programador de SnapManager con el programador del sistema operativo nativo?	En el servidor SnapManager, no se pueden ver los backups programados a través del planificador nativo del sistema operativo. Por ejemplo, después de crear una copia de seguridad programada, no se ve ninguna entrada adicional en cron.

Pregunta	Respuesta
<p>¿Qué sucede si los relojes de la interfaz gráfica de usuario y el servidor no están sincronizados?</p>	<p>Los relojes del cliente y del servidor no están sincronizados. Por lo tanto, puede programar una copia de seguridad en la que la hora de inicio esté en el futuro en el cliente pero en el pasado en el servidor.</p> <p>Para realizar backups periódicos, el servidor sigue cumpliendo la solicitud. Por ejemplo, si el servidor recibe una solicitud para realizar copias de seguridad cada hora a partir del 01/30/08 a las 3:00 p.m. pero la hora actual es a las 3:30 p.m. ese día, el servidor realiza su primer backup a las 4:00 p.m. y continúa realizando backups cada hora.</p> <p>Sin embargo, durante los backups que solo se realizan una vez, el servidor gestiona la solicitud de la siguiente forma:</p> <ul style="list-style-type: none"> <li>• Si la hora de inicio está dentro de los últimos cinco minutos de la hora del servidor actual, SnapManager inicia de inmediato el backup.</li> <li>• Si la hora de inicio es superior a cinco minutos, SnapManager no inicia el backup.</li> </ul> <p>Por ejemplo, piense en el siguiente escenario:</p> <ul style="list-style-type: none"> <li>• El reloj del host de la interfaz gráfica está a tres minutos de distancia del tiempo real.</li> <li>• La hora actual en el cliente es 8:58 a.m.</li> <li>• Se programa un backup puntual a las 9:00</li> <li>• Se programa otro backup que se realice una vez a las 8:30</li> </ul> <p>Cuando el servidor recibe la primera solicitud, la hora en el servidor es 9:01 a.m. Aunque la hora de inicio del backup es anterior, SnapManager realiza el backup de forma inmediata.</p> <p>Cuando el servidor recibe la segunda solicitud, la hora de inicio del backup ha pasado más de cinco minutos. Recibirá un mensaje indicando que la solicitud de programa ha fallado porque la hora de inicio ha pasado.</p> <p>Puede cambiar el tiempo de cinco minutos en un archivo de propiedades de SnapManager.</p>
<p>¿Qué ocurre en los backups programados para un perfil cuando se elimina el perfil?</p>	<p>Cuando se elimina un perfil de base de datos, el servidor SnapManager elimina los backups programados definidos para ese perfil.</p>



Pregunta	Respuesta
<p>¿Cómo se comportan los backups programados durante el horario de verano o cuando se cambia la hora del servidor SnapManager?</p>	<p>Las programaciones de backups de SnapManager se ven afectadas por el horario de verano o al cambiar la hora del servidor SnapManager.</p> <p>Tenga en cuenta las siguientes implicaciones cuando cambie el tiempo del servidor SnapManager:</p> <ul style="list-style-type: none"> <li>• Después de activar la programación de copia de seguridad, si la hora del servidor SnapManager se reduce, la programación de copia de seguridad no se activa de nuevo.</li> <li>• Si la hora de verano comienza antes de la hora de inicio programada, las programaciones de backup se activan automáticamente.</li> <li>• Por ejemplo, si se encuentra en los Estados Unidos y se programan los backups cada hora a las 4:00 esto se debe producir cada 4 horas, se realizará un backup a las 4:00, 8:00, 12:00, 4:00, 8:00, Y medianoche los días antes y después de los ajustes de horario de verano en marzo y noviembre.</li> <li>• Tenga en cuenta lo siguiente si las copias de seguridad están programadas para las 2:30 a.m. todas las noches: <ul style="list-style-type: none"> <li>◦ Cuando los relojes se atrasan una hora, ya que el backup se activa, el backup no se activa de nuevo.</li> <li>◦ Cuando los relojes se adelantan una hora, el backup se activa inmediatamente. Si se encuentra en los Estados Unidos y desea evitar este problema, debe programar las copias de seguridad para que comiencen fuera de las 2:00 a.m. a las 3:00 horas intervalo.</li> </ul> </li> </ul>

## Crear backups de la base de datos

Puede crear backups de bases de datos completas o de partes de bases de datos, incluidos espacios de tabla, archivos de datos o archivos de control.

### Acerca de esta tarea

SnapManager proporciona funcionalidades de copia Snapshot para bases de datos en numerosas pilas de almacenamiento del lado del host, incluidas NFS, Veritas, etc.



Para configuraciones de Real Application Clusters (RAC), SnapManager realiza el backup en el lado del host en el perfil.

Los administradores pueden opcionalmente registrar backups con Oracle RMAN, lo que facilita el uso de RMAN para restaurar y recuperar la base de datos con granularidades más finas como bloques.

Al definir el perfil, puede personalizar los nombres de las copias Snapshot creadas por backups de ese perfil. Por ejemplo, puede insertar una cadena de prefijo de

## HOPS

Para indicar backups de operaciones altas.

Además de definir nombres únicos para las copias de Snapshot creadas por backups, también puede crear etiquetas únicas para los propios backups. Cuando crea una copia de seguridad, es una buena práctica proporcionar un nombre para la copia de seguridad de forma que disponga de una forma sencilla de identificarla mediante la `-label` parámetro. Este nombre debe ser único para todos los backups creados dentro de un perfil determinado. El nombre puede contener letras, números, guiones bajos (`_`) y guiones (`-`). No puede comenzar con un guión. Las etiquetas distinguen mayúsculas de minúsculas. Puede incluir información como variables de entorno del sistema operativo, fecha del sistema y tipo de backup.

Si no proporciona una etiqueta, SnapManager creará un nombre de etiqueta predeterminado en el formulario `scope_mode_datestring`, donde el ámbito está completo o parcial y el modo es sin conexión, en línea o automático (la letra `c` para frío, `h` para caliente o `a` para automático).

Desde SnapManager 3.4, puede proporcionar su propia etiqueta de backup reemplazando la etiqueta de backup predeterminada que creó SnapManager. Debe configurar el valor de `override.default.backup.pattern` parámetro en `true` y especifique la nueva etiqueta de backup en la `new.default.backup.pattern` parámetro. El patrón de etiqueta de backup puede contener palabras clave como el nombre de la base de datos, el nombre del perfil, el ámbito, el modo y el nombre de host, que deben separarse con el guión bajo. Por ejemplo:

```
new.default.backup.pattern=dbname_profile_hostname_scope_mode.
```



La Marca de hora se incluirá automáticamente al final de la etiqueta generada.

Al introducir un comentario, puede incluir espacios y caracteres especiales. Por el contrario, cuando introduzca una etiqueta, no incluya espacios ni caracteres especiales.

Para cada backup, SnapManager genera automáticamente un GUID, que es una cadena HEXADECIMAL de 32 caracteres. Para determinar el GUID, debe ejecutar el `backup list` con el `-verbose` opción.

Es posible crear un backup completo de una base de datos mientras está en línea o sin conexión. Para que SnapManager gestione el backup de una base de datos independientemente de si está en línea o sin conexión, debe usar la `-auto` opción.

Al crear un backup, si se habilitó la eliminación y se habilitó la notificación de resumen en el perfil, se activan dos correos electrónicos independientes. Un correo electrónico es para la operación de backup y el otro para la eliminación. Es posible correlacionar estos correos electrónicos comparando el nombre de la copia de seguridad y el ID de copia de seguridad incluidos en estos correos electrónicos.

Es posible crear un backup en frío cuando la base de datos está en estado de apagado. Si la base de datos está en estado montado, cambie a estado de apagado y realice el backup sin conexión (backup en frío).

SnapManager (3.2 o posterior) permite realizar un backup de los archivos de registro de archivos independientemente de los archivos de datos, lo que permite gestionar los archivos de registro de archivos de forma eficiente.

Para crear los backups de registros de archivos por separado, debe crear un nuevo perfil o actualizar el perfil existente para separar los backups de los registros de archivos mediante el `-separate-archivelog -backups` opción. Con el perfil, es posible realizar las siguientes operaciones de SnapManager:

- Cree un backup de registro de archivos.
- Eliminar un backup de registro de archivos.
- Montar un backup de registro de archivos.
- Liberar un backup de registro de archivo.

Las opciones de copia de seguridad varían en función de la configuración del perfil:

- Si se utiliza un perfil que no está separado para realizar backups de registros de archivos de forma independiente, se puede hacer lo siguiente:
  - Cree un backup completo.
  - Crear un backup parcial.
  - Especifique los destinos de registros de archivos que se incluirán en el backup para los archivos de registro de archivos.
  - Especifique los destinos de registro de archivos que se excluirán de la copia de seguridad.
  - Especifique las opciones de eliminación para eliminar los archivos de registro de archivos de los destinos de registro de archivos.
- El uso de un perfil separado para tomar backups de registros de archivos permite hacer lo siguiente:
  - Cree una copia de seguridad sólo de archivos de datos.
  - Cree un backup solo de archivado.
  - Durante la creación de un backup solo de archivos de datos, incluya el backup de registro de archivos junto con el backup en línea de solo los archivos de datos para el clonado.

Si ha incluido copias de seguridad de registros de archivos junto con archivos de datos en la página **Configuración de perfiles** del asistente **creación de perfiles** de la interfaz gráfica de usuario de SnapManager, Y si no ha seleccionado la opción **Archivelogs** en el asistente **creación de copia de seguridad**, SnapManager siempre crea la copia de seguridad del registro de archivos junto con los archivos de datos para todas las copias de seguridad en línea.

En tal situación, en la CLI de SnapManager, puede tener en cuenta todos los destinos de los registros de archivos para el backup, excepto los destinos de exclusión especificados en el archivo de configuración SnapManager. Pero no puede eliminar estos archivos de registro de archivos. Sin embargo, todavía puede utilizar el `-archivelogs` Opción para especificar el destino del archivo de registro de archivos y pinar los archivos de registro de archivos desde la CLI de SnapManager.

Si crea el backup con el `-auto` y especifique la `--archivelogs` SnapManager crea un backup en línea o sin conexión según el estado actual del backup.

- SnapManager crea un backup sin conexión cuando la base de datos está sin conexión y no incluye los archivos de registro de archivos en el backup.
- SnapManager crea un backup en línea incluidos los archivos de registro de archivos cuando la base de datos está en línea.
- Mientras se crea el backup de solo archivado:
  - Especifique el destino de registro de archivos que se realizará el backup junto con el backup solo de archivmogs

- Especifique los destinos de registro de archivos que se excluirán del backup solo de registros de archivo
- Especifique las opciones de eliminación para eliminar los archivos de registro de archivos de los destinos de registro de archivos

#### • Escenarios no admitidos

- No puede crear el backup solo de archivado junto con un backup de solo archivos de datos sin conexión.
- No se pueden reducir los archivos de registro de archivos cuando no se realiza el backup de los archivos de registro de archivos.
- No es posible reducir los archivos de registro de archivos cuando el área de recuperación flash (FRA) está habilitada para los archivos de registro de archivos.

Si especifica la ubicación del registro de archivos en el área de recuperación de flash, asegúrese de especificar también la ubicación del registro de archivos en el `archive_log_dest` parámetro.

Cuando especifique la etiqueta para la copia de seguridad de archivos de datos en línea con la copia de seguridad de archivos de archivo incluida, la etiqueta se aplicará para la copia de seguridad de archivos de datos y la copia de seguridad del registro de archivo será con sufijo (`_logs`). Este sufijo se puede configurar cambiando el parámetro `suffix.backup.label.with.logs` En el archivo de configuración SnapManager.

Por ejemplo, puede especificar el valor como `suffix.backup.label.with.logs=arc` de modo que el valor predeterminado de `_logs` se cambia a `_arc`.

Si no se especificaron destinos de registro de archivos para su inclusión en el backup, SnapManager incluye todos los destinos de registro de archivos configurados en la base de datos.

Si falta algún archivo de registro de archivo en alguno de los destinos, SnapManager omite todos estos archivos de registro de archivos creados antes de los archivos de registro de archivos que faltan aunque estos archivos estén disponibles en otro destino de registro de archivos.

Al crear backups de registros de archivos, es necesario especificar los destinos de archivos de registro de archivos que se incluirán en el backup. Además, puede configurar el parámetro Configuration para incluir los archivos de registro de archivos siempre más allá de los archivos faltantes en el backup.



De manera predeterminada, este parámetro de configuración se establece en **true** para incluir todos los archivos de registro de archivos, más allá de los archivos faltantes. Si utiliza sus propios scripts de eliminación de registros de archivos o eliminación manual de archivos de registro de archivos de los destinos de registro de archivos, puede deshabilitar este parámetro, para que SnapManager pueda omitir los archivos de registro de archivos y continuar con el backup.

SnapManager no admite las siguientes operaciones SnapManager para backups de registros de archivos:

- Clonar el backup de registros de archivos
- Restaurar el backup de registros de archivos
- Verificar el backup de registros de archivos


SnapManager también admite la copia de seguridad de los archivos de registro de archivos desde los destinos de área de recuperación flash.


1. Introduzca el siguiente comando:

```
smsap backup create -profile profile_name {[-full {-online | -offline | -auto}
[-retain {-hourly | -daily | -weekly | -monthly | -unlimited}] [-verify] | [-
data [[-files files [files]] | [-tablespaces -tablespaces [-tablespaces]] [-
datalabel label] {-online | -offline | -auto} [-retain {-hourly | -daily |
-weekly | -monthly | -unlimited}] [-verify] | [-archivelogs [-label label] [-
comment comment] [-snapvaultlabel SnapVault_label][-protect | -noprotect |
-protectnow] [-backup-destpath1 [,path2]] [-exclude-dest path1 [,path2]] [-
prunelogs {-all | -untilSCN untilSCN | -until-date yyyy-MM-dd:HH:mm:ss |
-before {-months | -days | -weeks | -hours}} -prune-dest prune_dest1
, [prune_dest2]] [-taskspec taskspec]} [-dump] [-force] [-quiet | -verbose]
```

Si desea...	Realice lo siguiente...
<b>Cree una copia de seguridad en el almacenamiento secundario mediante la directiva de protección de SnapManager_CDOT_Vault_</b>	<p>Especifique <code>-snapvaultlabel</code>.</p> <p>Debe proporcionar la etiqueta de SnapMirror que haya especificado en las reglas de la política de SnapMirror al configurar la relación de SnapVault como valor.</p>
<b>Especifique si desea realizar una copia de seguridad de una base de datos en línea o sin conexión, en lugar de permitir que SnapManager controle si está en línea o sin conexión</b>	<p>Especifique <code>-offline</code> para realizar una copia de seguridad de la base de datos sin conexión.</p> <p>Especifique <code>-online</code> para realizar una copia de seguridad de la base de datos en línea.</p> <p>Si utiliza estas opciones, no podrá utilizar la <code>-auto</code> opción.</p>
<b>Especifique si desea que SnapManager gestione la copia de seguridad de una base de datos independientemente de si está en línea o sin conexión</b>	<p>Especifique el <code>-auto</code> opción. Si usa esta opción, no puede usar la <code>--offline</code> o <code>-online</code> opción.</p>

Si desea...	Realice lo siguiente...
<p><b>Especifique si desea realizar una copia de seguridad parcial de archivos específicos</b></p>	<p>Especifique el <code>-data-files</code> y, a continuación, lista la <i>files</i>, separados por comas. Por ejemplo, una lista de los nombres de archivo f1, f2 y f3 después de la opción.</p> <p>Ejemplo para crear una copia de seguridad parcial de un archivo de datos en UNIX</p> <pre data-bbox="513 394 1484 573"> smsap backup create -profile nosepl -data -files /user/user.dbf -online -label partial_datafile_backup -verbose </pre>
<p><b>Especifique si desea realizar una copia de seguridad parcial de tablespaces específicos</b></p>	<p>Especifique el <code>-data-tablespaces</code> y, a continuación, lista la <i>tablespaces</i>, separados por comas. Por ejemplo, utilice ts1, ts2 y ts3 después de la opción.</p> <p>SnapManager admite el backup de espacios de tablas de solo lectura. Al crear el backup, SnapManager cambia los espacios de tabla de solo lectura a lectura y escritura. Después de crear el backup, los espacios de tabla se modifican a modo de solo lectura.</p> <p>Ejemplo de creación de una copia de seguridad de tablespace parcial</p> <pre data-bbox="513 961 1484 1140"> smsap backup create -profile nosepl -data -tablespaces tb2 -online -label partial_tablespace_bkup -verbose </pre>
<p><b>Especifique si desea crear una etiqueta única para cada copia de seguridad en el siguiente formato: Full_hot_mybackup_label</b></p>	<p>Para Linux, puede introducir este ejemplo:</p> <pre data-bbox="513 1255 1484 1434"> smsap backup create -profile targetdb1_prof1 -label full_hot_my_backup_label -online -full -verbose </pre>

Si desea...	Realice lo siguiente...
<p><b>Especifique si desea crear una copia de seguridad de los archivos de registro de archivos por separado de los archivos de datos</b></p>	<p>Especifique las siguientes opciones y variables:</p> <ul style="list-style-type: none"> <li>• <code>-archivelogs</code> crea un backup de los archivos de registro de archivos.</li> <li>• <code>-backup-dest</code> especifica los destinos de archivos de registro de archivos que se incluirán en el backup.</li> <li>• <code>-exclude-dest</code> especifica los destinos de registro de archivos que se van a excluir.</li> <li>• <code>-label</code> especifica la etiqueta para el backup del archivo de registro de archivos.</li> <li>• <code>-protect</code> permite la protección en los backups de registros de archivos.</li> </ul> <p> Debe proporcionar cualquiera de los dos <code>-backup-dest</code> o la <code>-exclude-dest</code> opción.</p> <p>Al ofrecer ambas opciones junto con la copia de seguridad se muestra un mensaje de error <code>You have specified an invalid backup option. Specify any one of the options: -backup-dest, or exclude-dest.</code></p> <p>Ejemplo de creación de backups de archivos de registro de archivos por separado en UNIX</p> <pre>smsap backup create -profile nosepe -archivelogs -backup-dest /mnt/archive_dest_2/ -label archivelog_bkup -verbose</pre>
<p><b>Especifique si desea crear una copia de seguridad de archivos de datos y archivos de registro de archivos juntos</b></p>	<p>Especifique las siguientes opciones y variables:</p> <ul style="list-style-type: none"> <li>• <code>-data</code> opción para especificar los archivos de datos.</li> <li>• <code>-archivelogs</code> opción para especificar los archivos de registro de archivos. Ejemplo para realizar backups de archivos de datos y archivos de registro de archivos juntos en UNIX</li> </ul> <pre>smsap backup create -profile nosepe -data -online -backup-dest mnt/archive_dest_2 -label data_arch_backup -verbose</pre>

Si desea...	Realice lo siguiente...
<p><b>Especifique si desea eliminar los archivos de registro de archivos mientras crea una copia de seguridad</b></p>	<p>Especifique las siguientes opciones y variables:</p> <ul style="list-style-type: none"> <li>• <code>-prunelogs</code> especifica la eliminación de los archivos de registro de archivos de los destinos de registro de archivos. <ul style="list-style-type: none"> <li>◦ <code>-all</code> especifica que se eliminen todos los archivos de registro de archivos de los destinos de registro de archivos.</li> <li>◦ <code>-until-scn until-scn</code> Especifica la eliminación de los archivos de registro de archivos hasta un SCN especificado.</li> <li>◦ <code>-until-date yyyy-MM-dd:HH:mm:ss</code> especifica la eliminación de los archivos de registro de archivos hasta el período de tiempo especificado.</li> <li>◦ <code>-before</code> la opción especifica la eliminación de los archivos de registro de archivos antes del período de tiempo especificado (días, meses, semanas, horas).</li> <li>◦ <code>-prune-destprune_dest1, [prune_dest2</code> especifica la eliminación de los archivos de registro de archivos de los destinos de registro de archivos mientras se crea el backup.</li> </ul> </li> </ul> <p> No es posible reducir los archivos de registro de archivos cuando el área de recuperación flash (FRA) está habilitada para los archivos de registro de archivos.</p> <p>Ejemplo de eliminación de todos los archivos de registro de archivos mientras se crea una copia de seguridad en UNIX</p> <pre data-bbox="513 1125 1484 1339"> smsap backup create -profile nosepl   -archivelogs -label archive_prunebackup1 -backup   -dest /mnt/arc_1,/mnt/arc_2 -prunelogs -all -prune   -dest /mnt/arc_1,/mnt/arc_2 -verbose </pre>
<p><b>Especifique si desea añadir un comentario sobre la copia de seguridad</b></p>	<p>Especifique <code>-comment</code> seguido de la cadena de descripción.</p>
<p><b>Especifique si desea forzar la base de datos al estado que ha especificado para realizar la copia de seguridad, independientemente del estado en el que se encuentre</b></p>	<p>Especifique el <code>-force</code> opción.</p>



Si desea...	Realice lo siguiente...
<b>Especifique si desea verificar la copia de seguridad al mismo tiempo que la crea</b>	Especifique el <code>-verify</code> opción.
<b>Especifique si desea recopilar los archivos de volcado después de la operación de copia de seguridad de la base de datos</b>	Especifique <code>-dump</code> opción al final del comando <code>backup create</code> .

## Ejemplo

```

smsap backup create -profile targetdb1_prof1 -full -online -force -verify

```

## Archivos de registro de archivo de Prune

Puede reducir los archivos de registro de archivos desde las ubicaciones del registro de archivos mientras crea una copia de seguridad.

### Lo que necesitará

- La operación de backup actual debe realizar un backup de los archivos de registro de archivos.

Si se especifica la eliminación junto con otros backups que no contienen archivos de registro de archivos, no se reducen los archivos de registro de archivos.

- La base de datos debe estar en el estado montado.

Si la base de datos no está en estado montado, introduzca la opción `-force` junto con el comando de backup.

### Acerca de esta tarea

Al realizar una operación de backup, se puede especificar lo siguiente:

- **Ámbito de la eliminación:**
  - Elimine todos los archivos de registro de archivos.
  - Elimine los archivos de registro de archivos hasta que el SCN especificado.
  - Elimine los archivos de registro de archivos hasta la hora especificada.
  - Elimine los archivos de registro de archivos antes del período de tiempo especificado.

- Destino desde el que se deben quitar los archivos de registro de archivos.



Aunque se produzca un error al eliminar el archivo de registro de archivos en un destino, SnapManager continúa depurando los archivos de registro de archivos de los otros destinos.

Antes de eliminar los archivos de registro de archivos, SnapManager verifica lo siguiente:

- Se realiza un backup de los archivos de registro de archivo al menos una vez.
- Los archivos de registro de archivo se envían a la base de datos Oracle Dataguard Standby, si los hubiera.
- El proceso de captura de Oracle Streams captura los archivos de registro de archivo, si los hay.

Si se realiza un backup de los archivos de registro de archivos, se envían al estado de espera y se capturan mediante el proceso de captura, SnapManager elimina todos los archivos de registro de archivos en una sola ejecución. Sin embargo, si hay archivos de registro de archivos que no se incluyen en un backup, que no se envían a en espera o que no están capturados por el proceso de captura, SnapManager elimina los archivos de registro de archivos uno por uno. La eliminación de archivos de registros de archivos en una sola ejecución es más rápida que la eliminación de registros de archivos uno por uno.

SnapManager también puede agrupar los archivos de registro de archivos y eliminarlos por lotes. Cada lote tendrá un máximo de 998 archivos. Este valor se puede configurar por debajo de 998 utilizando el parámetro Configuration `maximum.archive.log.files.toprun.atATime` en la `smsap.config` archivo.

SnapManager utiliza los comandos de Oracle Recovery Manager (RMAN) para eliminar los archivos de registro de archivo. Sin embargo, SnapManager no se integra con las políticas de retención y de eliminación de RMAN.



Si elimina los archivos de registro de archivos de los destinos de registro de archivos, se produce un error en la eliminación de archivos de registro de archivos.

SnapManager no admite la eliminación de archivos de registro de archivos en las siguientes situaciones:

- Los archivos de registro de archivo se encuentran en el área de recuperación de flash.
- Los archivos de registro de archivo se encuentran en la base de datos en espera.
- SnapManager y RMAN gestionan los archivos de registro de archivo.

## Paso

1. Introduzca el siguiente comando:

```
smsap backup create -profile profile_name {[-full {-online | -offline | -auto}
[-retain {-hourly | [-daily | -weekly | -monthly | -unlimited]} [-verify] | [-
data [[-files files [files]] | [-tablespaces -tablespaces [-tablespaces]] [-
datalabel label] {-online | -offline | -auto} [-retain {-hourly | [-daily |
-weekly | -monthly | -unlimited]} [-verify] | [-archivelogs [-label label] [-
comment comment] [-protect | -noprotect | -protectnow] [-backup-dest path1
[,path2]] [-exclude-dest path1 [,path2]]] [-prunelogs {-all | -untilSCN
untilSCN | -until -date yyyy-MM-dd:HH:mm:ss | -before {-months | -days |
-weeks | -hours}} -prune-dest prune_dest1 [,prune_dest2]] [-taskspec taskspec]}
-dump [-force] [-quiet | -verbose]
```

Si desea...	Realice lo siguiente...
<b>Prune archive log files</b>	<p>Especifique las siguientes opciones:</p> <ul style="list-style-type: none"> <li>• <code>-prunelogs</code> especifica la eliminación de los archivos de registro de archivos mientras se crea un backup. <ul style="list-style-type: none"> <li>◦ <code>-all</code> especifica la eliminación de todos los archivos de registro de archivos.</li> <li>◦ <code>-untilSCN</code> Especifica la eliminación de los archivos de registro de archivos hasta el SCN especificado.</li> <li>◦ <code>-until-date</code> especifica la eliminación de los registros de archivos, incluida la fecha y la hora especificadas.</li> <li>◦ <code>-before`{-months</code></li> </ul> </li> </ul>
<code>-days</code>	<code>-weeks</code>
<code>-hours}` especifica la eliminación de los archivos de registro de archivos antes del período de tiempo especificado.</code>	<ul style="list-style-type: none"> <li>• Incluir el destino desde donde se van a quitar los archivos de registro *</li> </ul>

## Consolide los backups de registros de archivos

SnapManager consolida los backups de solo archivado cada vez que realiza un backup liberando únicamente los backups duplicados de archivvelog. La consolidación está habilitada de forma predeterminada.

### Acerca de esta tarea

SnapManager identifica los backups solo de archivado que tienen archivos de registro de archivos en otros backups y los libera para mantener la cantidad mínima de backups de solo archivado con archivos de registro únicos.

Si la consolidación libera los backups de solo archivado, estos backups se eliminan según la duración de la retención del registro de archivos.

Cuando la base de datos se encuentra en el estado shutdown o nomount durante la consolidación del registro de archivo, SnapManager cambia la base de datos al estado Mount.

Si se produce un error en la copia de seguridad o la eliminación de archivos de registro de archivos, no se realizará la consolidación. La consolidación de backups de solo archivvelog se sigue solo después de backups correctos y de operaciones de eliminación correctas.

### Pasos

1. Para permitir la consolidación de los backups de solo archivvelog, modifique el parámetro Configuration `consolidation` y establezca el valor como `true` En el archivo de configuración de SnapManager (`smsap.config`).

Una vez configurado el parámetro, se consolidan los backups de solo archivado.

Si el backup de solo archivado creado recientemente contiene los mismos archivos de registro de archivos en cualquiera de los backups de solo archivado anteriores, se liberan los backups de solo registros de archivos anteriores.



SnapManager no consolida el backup de registros de archivos realizado junto con el backup de archivos de datos. SnapManager consolida el backup de solo archivado.



SnapManager consolida los backups de registros de archivos, incluso cuando el usuario elimina manualmente los archivos de registro de archivos de los destinos de registros de archivos o cuando los archivos de registro de archivos están dañados y pueden incluirse el backup.

2. Para deshabilitar la consolidación de los backups de registros de archivos, modifique el parámetro `Configuration consolidation` y establezca el valor como `false` En el archivo de configuración de SnapManager (`smsap.config`).

## Programar la eliminación del archivo de registro de archivo

Cuando se crea un backup, es posible programar la eliminación de los archivos de registro de archivos para que se produzca en un momento determinado.

### Acerca de esta tarea

SnapManager permite reducir periódicamente los archivos de registro de archivos desde el sistema de archivos activo.

### Paso

1. Introduzca el siguiente comando:

```
smsap schedule create -profile profile_name {[-full {-online | -offline | -auto}[-retain [-hourly | -daily | -weekly | -monthly | -unlimited] [-verify]] | [-data [-files files [files]] | [-tablespaces -tablespaces [-tablespaces]] {-online | -offline | -auto}[-retain [-hourly | -daily | -weekly | -monthly | -unlimited] [-verify]] | [-archivelogs]} [-comment comment] [-protect | -protectnow | -noprotect] [-backup-dest path1 [,path2]] [-exclude-dest path1 [,path2]] [-prunelogs{-all | -untilSCN untilSCN | -before {-date yyyy-MM-dd HH:mm:ss | -months months | -weeks weeks | -days days | -hours hours}} -prune -dest prune_dest1 [,prune_dest2] -schedule-name schedule_name [-schedule-commentschedule comment] -interval {-hourly | -daily | -weekly | -monthly | -onetimeonly} -cronstring cronstring -start-time {start-time start_time <yyyy-MM-dd HH:mm>} -runasuser -runasuser [-force] [-quiet | -verbose]
```

Si desea...	Realice lo siguiente...
Programar la eliminación de archivos de registro de archivos	Especifique las siguientes opciones: <ul style="list-style-type: none"> <li>• <code>-prunelogs</code> para programar la eliminación de los archivos de registro de archivo</li> <li>• <code>-prune-dest</code> para eliminar los archivos de registro de archivos de los destinos de registro de archivos</li> </ul>
Incluya un nombre para el horario	Especifique el <code>-schedule-name</code> opción.
Programar la eliminación de archivos de registro de archivos en un intervalo de tiempo específico	Especifique el <code>interval</code> e indique si los archivos de registro de archivo deben recordarse en función de las siguientes clases de intervalo: <ul style="list-style-type: none"> <li>• <code>-hourly</code></li> <li>• <code>-daily</code></li> <li>• <code>-weekly</code></li> <li>• <code>-monthly</code></li> <li>• <code>-onetimeonly</code></li> </ul>
Agregar un comentario sobre la operación de horario	Especifique el <code>-schedule-comment</code> opción seguida de la cadena de descripción.
Especifique la hora de inicio de la operación de programación	Especifique el <code>-start-time</code> opción en formato <code>yyyy-mm-dd hh:mm</code> .

## Proteger los backups de registros de archivos

Al crear perfiles, puede habilitar la protección para los backups del registro de archivos según la política de protección de los registros de archivos.

### Paso

1. Introduzca el siguiente comando:

```
smsap profile create -profile profile [-profile-password profile_password]
-repository -dbname repo_dbname -host repo_host -port repo_port -login
-username repo_username -database -dbname db_dbname -host db_host [-sid
db_sid] [-login-username db_username -password db_password -port db_port] [-
rman {-controlfile | {-login-username rman_username -password rman_password
-tnsname rman_tnsname} } ] -osaccount osaccount -osgroup osgroup [-retain [-
hourly [-count n] [-duration m]] [-daily [-count n] [-duration m]] [-weekly [-
count n] [-duration m]] [-monthly [-count n] [-duration m]]] [-comment
comment] [-snapname-pattern pattern] [-protect [-protection-policy policy_name]]
[-summary-notification] [-notification [-success-email email_address1,
email_address2 -subject subject_pattern] [-failure-email email_address1,
```

```
email_address2 -subject subject_pattern]] [-separate-archivelog-backups-retain-archivelog-backups-hours hours | -days days | -weeks weeks | -months months [-protect [-protection-policy policy_name] | -noprotect] [-include-with-online-backups | -no-include-with-online-backups]] [-dump]
```

Si...	Realice lo siguiente...
Desea realizar una copia de seguridad de las copias de seguridad de archive log por separado y proteger los archivos archive log	<p>Especifique las siguientes opciones:</p> <ul style="list-style-type: none"> <li>• <code>-separate-archivelog-backups</code> permite separar los archivos de registro de archivos de los archivos de datos.</li> <li>• <code>-protect</code> asigna una política de protección independiente para los backups de registros de archivo de registros de archivo.</li> <li>• <code>-protection-policy</code> asigna la política de protección para los backups de registros de archivo.</li> </ul>

## Qué es AutoSupport

La función AutoSupport permite que el servidor SnapManager envíe mensajes de AutoSupport al sistema de almacenamiento una vez completada la operación de backup.



SnapManager envía mensajes de AutoSupport solo para las operaciones de backup correctas.

Puede habilitar o deshabilitar AutoSupport asignando los siguientes valores a `auto_support.on` parámetro de configuración en `smsap.config` archivo de configuración:

- **TRUE** - Activa AutoSupport
- **FALSE** - Desactiva AutoSupport



De manera predeterminada, AutoSupport se habilita en SnapManager.

## Añada sistemas de almacenamiento que funcionen en Clustered Data ONTAP al host del servidor SnapManager

Debe añadir los sistemas de almacenamiento operativos en Clustered Data ONTAP al host del servidor de SnapManager para habilitar AutoSupport. En SnapManager 3.3 y versiones anteriores, AutoSupport solo era compatible con sistemas de almacenamiento que funcionaban en 7-Mode.

### Paso

1. Añada sistemas de almacenamiento que funcionen en Clustered Data ONTAP al host del servidor SnapManager.

Si...	Después, ejecute el siguiente comando...
La máquina virtual de almacenamiento de administración (SVM, antes denominada Vserver) está funcionando en Clustered Data ONTAP	<code>snapdrive config set -cserver user_name storage_name</code>
SVM opera en Clustered Data ONTAP	<code>snapdrive config set -vserver user_name storage_name</code>

### Habilite AutoSupport en SnapManager

Debe habilitar AutoSupport, de modo que los sistemas de almacenamiento reciban mensajes del servidor SnapManager para cada operación de backup realizada correctamente.

#### Acerca de esta tarea

AutoSupport se puede habilitar de dos formas:

- De forma predeterminada, la nueva instalación de SnapManager no contiene `auto_support.on` en la `smsap.config` archivo de configuración. Esto implica que AutoSupport está habilitado.
- Puede configurar manualmente el `auto_support.on` parámetro.

#### Pasos

1. Detenga el servidor SnapManager.
2. En la `smsap.config` archivo de configuración, establezca el valor de `auto_support.on` parámetro a **TRUE**.

#### ejemplo

```
auto_support.on=TRUE
```

3. Reinicie el servidor SnapManager.

### Deshabilite AutoSupport en SnapManager

Debe deshabilitar AutoSupport si no desea que el sistema de almacenamiento reciba mensajes del servidor SnapManager para cada operación de backup exitosa.

#### Acerca de esta tarea

De forma predeterminada, AutoSupport se habilita si el archivo de configuración no contiene `auto_support.on` parámetro. En este escenario, debe agregar la `auto_support.on` parámetro en el archivo de configuración y establezca el valor en **FALSE**.

1. Detenga el servidor SnapManager.

2. En la `smsap.config` archivo de configuración, establezca el valor de `auto_support.on` parámetro a **FALSE**.

### ejemplo

```
auto_support.on=FALSE
```

3. Reinicie el servidor SnapManager.

## Verificar los backups de la base de datos

Puede utilizar el `backup verify` comando para verificar que los bloques del backup de la base de datos no están dañados. La operación Verify invoca la utilidad Oracle Database Verify para cada archivo de datos de la copia de seguridad.

### Acerca de esta tarea

SnapManager permite realizar la operación de verificación cuando lo desee, tanto para usted como para los usuarios del sistema. Es posible realizar la verificación inmediatamente después de crear el backup. Debe especificar el perfil que contiene el backup y la etiqueta o el ID del backup creado.



Es posible especificar `-dump` para recoger los archivos de volcado después de la operación de verificación de backup.

### Paso

1. Introduzca el siguiente comando:

```
smsap backup verify -profile profile_name [-label label | -id id] [-force] [-dump] [-quiet | -verbose]
```

## Cambie la política de retención de backups

Puede cambiar las propiedades de un backup para que sea elegible o inelegible para su eliminación de acuerdo con la política de retención.

### Acerca de esta tarea

Al crear un backup, se puede establecer su política de retención. Posteriormente, se puede optar por conservar el backup durante un período más largo del que permite la política de retención o especificar que ya no es necesario el backup y desea que la política de retención lo gestione.

### Conserve las copias de seguridad para siempre

Puede especificar que una copia de seguridad no sea elegible para su eliminación por parte de la política de retención, con el fin de conservar el backup de forma indefinida.

### Paso

1. Para especificar que una copia de seguridad se conserve sin límite, escriba el siguiente comando:

```
smsap backup update -profile profile_name {-label label [data | -archivelogs] | -id id} -retain -unlimited
```



## Asigne backups con una clase de retención específica

Los administradores de bases de datos pueden asignar una clase de retención específica por hora, día, semana o mes a los backups. La asignación de una clase de retención específica hace que los backups realizados bajo este cambio sean aptos para su eliminación.

### Paso

1. Para asignar una clase de retención de copia de seguridad específica, introduzca este comando:

```
smsap backup update -profile profile_name {-label label [data | -archive]logs]
| -id id} -retain [-hourly | -daily | -weekly | -monthly ]
```

## Cambie el comportamiento predeterminado de la política de retención

Cuando caduca un backup según la política de retención, SnapManager determina si se elimina el backup según la configuración de retención. La eliminación de copias de seguridad es el comportamiento predeterminado. Puede cambiar este comportamiento predeterminado y liberar en su lugar las copias de seguridad no protegidas.

### Acerca de esta tarea

De forma predeterminada, SnapManager elimina o libera backups en función de si están protegidos o no de la siguiente manera:

- En el caso de los backups protegidos, SnapManager libera los backups locales cuando caducan.
- Para backups sin protección, SnapManager elimina los backups locales cuando caducan.

Puede cambiar este comportamiento predeterminado.

Para los backups protegidos, SnapManager no tiene en cuenta lo siguiente a la hora de determinar si se debe eliminar la copia local:

- El backup en el almacenamiento secundario presenta un error o está en proceso de protección.

Esto permite la transferencia de backups a un almacenamiento secundario antes de aplicar la normativa de retención.

- La copia se eliminó posteriormente del almacenamiento secundario.

### Pasos

1. Acceda a la siguiente ubicación predeterminada:

```
default smsap installation location/properties/smsap.config
```

2. Edite el `smsap.config` archivo.
3. Ajuste la `retain.alwaysFreeExpiredBackups` propiedad en la `smsap.config` archivo en `true`.

Por ejemplo:

```
retain.alwaysFreeExpiredBackups = true
```

## Backups exentos de la política de retención o eliminarlos

Los backups con clase de retención "ilimitada" no se pueden eliminar ni liberar directamente. Para eliminar o liberar estos backups, primero se debe asignar otra clase de retención, como por ejemplo cada hora, día, semana o mes. Para eliminar o liberar una copia de seguridad que esté exenta de la política de retención, primero debe actualizar la copia de seguridad para que sea elegible para su eliminación o su liberación.

### Pasos

1. Para actualizar el backup y poder borrarlo mediante la política de retención, escriba este comando:

```
smsap backup update -profile profile_name {-label label [data | -archivelogs] | -id id} -retain [-hourly | -daily | -weekly | -monthly]
```

2. Después de actualizar el backup de modo que sea apto para su eliminación, puede eliminar el backup o liberar recursos de backup.

- Para eliminar el backup, introduzca este comando:

```
smsap backup delete -profile profile_name {-label label [data | -archivelogs] | -id id | -all}
```

- Para liberar los recursos del backup, en lugar de eliminarlo, escriba este comando:

```
smsap backup free -profile profile_name {-label label [data | -archivelogs] | -id id | -all} [-force] [ -dump] [-quiet | -verbose]
```

## Ver una lista de backups

Puede comprobar qué backups se crearon para un perfil y su estado de backup mediante la `smsap backup list` comando. Para cada perfil, el comando muestra primero la información sobre el backup más reciente y, a continuación, continúa hasta que se muestra la información de todos los backups.

### Paso

1. Introduzca el siguiente comando:

```
smsap backup list -profile profile_name [-delimiter character] [data | -archivelogs] [-quiet | -verbose]
```

## Ver detalles de backup

Puede ver la información detallada sobre un backup concreto de un perfil mediante `smSAP backup show` comando.

### Acerca de esta tarea

La `smsap backup show` el comando muestra la siguiente información de cada backup:

- El ID de la copia de seguridad
- Si la copia de seguridad se ha realizado correctamente o ha fallado
- Alcance de backup (completo, parcial, en línea o sin conexión)
- Modo de backup
- Estado de montaje
- La etiqueta de backup
- Comentar
- La fecha y la hora en que se inició y finalizó la operación
- Información sobre si se verificó el backup
- La clase de retención de copias de seguridad
- La base de datos y el nombre de host
- El número de cambio de sistema de punto de comprobación (SCN)
- El SCN de backup final (solo para backups en línea)
- Los espacios de tablas y los archivos de datos de la base de datos de la que se realizó un backup
- Los archivos de control de la base de datos de la que se realizó un backup
- Los registros de archivos de la base de datos de la que se realizó un backup
- El sistema de almacenamiento y los volúmenes donde se encuentran los archivos
- Las copias Snapshot realizadas y su ubicación
- El estado de los recursos de almacenamiento principales
- El estado de la protección de backup
- Una lista de copias en el almacenamiento secundario, con el formato backup\_copy ID - node name
- Modo de backup

Si especifica el `-verbose` opción, se muestra la siguiente información adicional:

- Los clones del backup, si los hay
- Información de verificación
- Si se monta el backup, SnapManager muestra los puntos de montaje que están en uso

Para el backup de archivos de registro de archivos, se muestra la misma información que la del otro backup de base de datos excepto la siguiente información:

- SCN de punto de comprobación
- SCN de backup final
- Tablespace
- Archivos de control

Sin embargo, el backup del archivo de registro de archivos contiene la siguiente información adicional:

- El primer número de cambio del backup
- El siguiente número de cambio del backup

- Número de rosca
- Restablecer ID de registros
- Encarnación
- Nombre de archivo de registro

## Paso

1. Introduzca el siguiente comando:

```
smsap backup show -profile profile_name [-label label | -archivelogs] |
-id id [-quiet | -verbose]
```

## Montar backups

SnapManager se encarga automáticamente del montaje de un backup para que el host esté disponible. También es posible montar backups en situaciones en las que se utilice una herramienta externa, como Oracle Recovery Manager (RMAN), para acceder a los archivos de la copia de seguridad.

### Acerca de esta tarea

La `smsap backup mount` Comando muestra una lista de las rutas en las que se han montado las copias Snapshot que constan del backup.

Puede utilizar el `-from-secondary` opción para montar el backup desde el almacenamiento secundario. Si no utiliza esta opción, SnapManager monta el backup desde el almacenamiento principal.

Debe especificar el `-copy-id` siempre que especifique la `-from-secondary` opción. Si existe más de un backup en el sistema de almacenamiento secundario, el `-copy-id` se utiliza la opción para especificar qué copia de backup en el almacenamiento secundario se debe usar para montar el backup.6



Si utiliza Data ONTAP operando en 7-Mode, debe especificar un valor válido para `-copy-id` opción. Sin embargo, si utiliza Clustered Data ONTAP, el `-copy-id` la opción no es necesaria.

Si va a montar un backup de base de datos en un host remoto, debe asegurarse de que las credenciales de Automatic Storage Management (ASM) sean las mismas en ambos hosts.



Opcionalmente, es posible recoger los archivos de volcado después de una operación de montaje de backup exitosa o con errores.

## Paso

1. Para montar un backup, introduzca el siguiente comando:

```
smsap backup mount -profile profile_name label [data | -archivelogs] | -id id
[-host host] [-from-secondary [-copy-id id]] [-dump] [-quiet | -verbose]
```

## Desmontar backups

SnapManager desmonta automáticamente el backup para que no esté disponible para el

servidor host. SnapManager también permite desmontar si se utiliza una herramienta externa, como Oracle Recovery Manager (RMAN), para acceder a los archivos de la copia de seguridad y para cambiar el estado del backup para quitar el acceso.

### Acerca de esta tarea

Si va a desmontar un backup de base de datos de un host remoto, debe asegurarse de que las credenciales de Automatic Storage Management (ASM) sean las mismas en ambos hosts.

Otra opción es recoger los archivos de volcado después de una operación de backup realizó una operación de desmontaje correcta o con errores.

Es posible que la operación de desmontaje falle en algún momento con un mensaje de error si el punto de montaje está ocupado, por ejemplo, `--[ERROR] FLOW-11019: Failure in Disconnect: SD-10046: You cannot unmount the backup as the mount point is busy with the following mount paths and PID's: /opt/NetApp/smsap/mnt/-mnt-neuse_nfsvrdb_arch-20120427052319903_0 with PID 6598.`

Debe identificar el PID de la sesión que tiene como resultado un fallo en la operación de desmontaje. Detenga la sesión ejecutando el siguiente comando:

```
kill pid
```

Posteriormente, puede ejecutar la operación de desmontaje correctamente.

### Paso

1. Introduzca el siguiente comando:

```
smsap backup unmount -profile profile_name {label label [data | -archive]logs  
| -id id} [-quiet | -verbose]
```

## Backups gratuitos

Es posible liberar backups, lo que elimina las copias Snapshot sin eliminar los metadatos de los backups. Esta función libera el espacio ocupado por la copia de seguridad. Puede utilizar el comando `smsap backup free` para liberar las copias de seguridad.

### Lo que necesitará

Para que un backup pueda ser apto para liberar, debe asegurarse de lo siguiente:

- La copia de seguridad se ha realizado correctamente
- La copia de seguridad no se va a montar
- El backup no tiene clones
- El backup no se conservará mediante una política de retención ilimitada
- El backup no se ha liberado todavía

### Acerca de esta tarea

Si la protección está habilitada en el perfil y la política de protección contiene conexiones del nodo principal que usan una relación de mirroring, se eliminan copias Snapshot en el nodo principal cuando se libera un

backup. Esas copias Snapshot también se eliminan de los nodos reflejados cuando se produce la próxima transferencia a almacenamiento secundario.

Cuando libera un backup protegido, SnapManager solicita que Protection Manager elimine las copias Snapshot locales para el backup. Si la operación libre de backup se realiza correctamente para los backups protegidos, Protection Manager elimina las copias de Snapshot de forma asíncrona.

<b>Estado de protección</b>	<b>Estado local</b>	<b>De datos en cuanto al almacenamiento primario</b>	<b>Acción en el almacenamiento secundario</b>	<b>Explicación</b>
No solicitado (protegido)	Existe	Libera el backup	No se requiere ninguna acción	SnapManager libera el backup local.
Liberado	No se requiere ninguna acción	No se requiere ninguna acción	La copia de seguridad local ya está liberada.	Sin proteger
Existe	Libera el backup	No se requiere ninguna acción	SnapManager libera el backup local aunque no haya copias en el almacenamiento secundario.	Liberado
No se requiere ninguna acción	No se requiere ninguna acción	La copia de seguridad local ya está liberada.	Protegido	Existe
Libera el backup	No se requiere ninguna acción; el backup en el secundario permanece	SnapManager libera el backup local. Las copias se conservan en el almacenamiento secundario.	Liberado	No se requiere ninguna acción

Es posible especificar la opción -dump como un parámetro opcional para recoger los archivos de volcado después de la operación de backup libre exitosa o con errores.

## **Paso**

1. Introduzca el siguiente comando:

```
smsap backup free -profile profile_name {-label label [data | -archivelogs] |  
-id id | -all} -force[-dump] [-quiet] [-force]
```

## Eliminar backups

Debe eliminar backups cuando ya no los necesite, lo que libera el espacio que estos backups ocupan. Si elimina los backups, reducirá la posibilidad de alcanzar el límite de 255 copias snapshot por volumen.

### Lo que necesitará

- Debe asegurarse de que el backup no se haya usado para crear un clon.

### Acerca de esta tarea

Cuando se elimina un backup protegido, SnapManager elimina el backup del almacenamiento secundario y el repositorio de SnapManager. En la siguiente tabla, se muestran las acciones emprendidas en el almacenamiento primario y secundario al eliminar un backup local:

Estado de protección	Estado local	De datos en cuanto al almacenamiento primario	Acción en el almacenamiento secundario	Explicación
No solicitado (protegido)	Existe	Elimina las copias Snapshot	No se requiere ninguna acción	SnapManager eliminará el backup local.
Liberado	No se requiere ninguna acción	No se requiere ninguna acción	La copia de seguridad local ya está liberada. Si se elimina un backup liberado, los metadatos del backup se eliminan del repositorio.	Sin proteger
Existe	Elimina las copias Snapshot	No se requiere ninguna acción	SnapManager elimina el backup local tanto si se ha protegido como si no.	Liberado
No se requiere ninguna acción	No se requiere ninguna acción	La copia de seguridad local ya está liberada. Si se elimina un backup liberado, los metadatos del backup se eliminan del repositorio.	Protegido	Existe

Estado de protección	Estado local	De datos en cuanto al almacenamiento primario	Acción en el almacenamiento secundario	Explicación
Elimina las copias Snapshot	SnapManager elimina el backup en el almacenamiento secundario	SnapManager elimina el backup local y las copias secundarias.	Liberado	No se requiere ninguna acción

Si intenta eliminar un backup que está protegido por el almacenamiento secundario, es posible que las copias de Snapshot se marquen para eliminarse y, posteriormente, Protection Manager las elimina.

Puede eliminar backups retenidos de forma ilimitada sin cambiar la clase de retención.

Opcionalmente, es posible recoger los archivos de volcado después de la operación de eliminación de backup exitosa o con errores.

Si desea eliminar los backups de registros de archivos, debe comprobar la duración de retención establecida para el backup de registros de archivos. Si el backup de registros de archivos se encuentra dentro de la duración de retención y se requieren archivos de registro de archivos para la recuperación de una base de datos restaurada, no se puede eliminar el backup de registros de archivos.

## Pasos

1. Compruebe que las operaciones se han completado introduciendo el comando siguiente:

```
smsap operation list -profile profile_name-dump-quiet-verbose
```

2. Para eliminar un backup, introduzca el siguiente comando:

```
smsap backup delete -profile profile_name [-label label [data | -archivelogs] | -id id | -all] [-force] [ -dump] [-quiet | -verbose]
```

Utilice la opción `-force` para forzar la eliminación del backup. Forzar la eliminación de un backup que tenga operaciones incompletas podría dejar el backup en estado incoherente.

## Programación de backups de bases de datos

SnapManager (3.2 o posterior) para SAP le permite programar backups de bases de datos de forma regular durante las horas de menor actividad para mantener un alto rendimiento. Para programar un backup, puede crear un perfil, que incluya la información de la base de datos y la política de retención, y luego establecer programaciones para el backup.





Debe programar los backups como usuario raíz o como usuario de Oracle. Si intenta programar los backups como usuario no existente, SnapManager muestra un mensaje de error: Invalid user: username: No puede crear un backup de programación para un usuario determinado

A continuación, se muestran algunas de las tareas relacionadas con la programación:

- Programar un backup de base de datos para que se realice por hora, día, semana, mes o una sola vez.
- Ver una lista de los backups programados asociados con un perfil.
- Actualizar una copia de seguridad programada.
- Suspender temporalmente una programación.
- Reanude la programación suspendida.
- Eliminar una programación.



La casilla de verificación **operación del menú Ejecutar ahora** está desactivada cuando se está ejecutando una copia de seguridad programada para esa programación.

## Cree programaciones de backup

Es posible programar un backup en el momento y la frecuencia que sean adecuados para sus datos y entorno.

### Acerca de esta tarea

Desde SnapManager 3.2 para SAP, puede programar las copias de seguridad de los archivos de registro de archivos por separado. Sin embargo, debe utilizar el perfil que ha creado para separar los archivos de registro de archivos.

Si programó los backups de los archivos de datos y los archivos de registro de archivos al mismo tiempo, SnapManager creará primero el backup de los archivos de datos.

Si selecciona el intervalo de programación como `-onetimeonly`, todas las opciones de poda están disponibles. Si selecciona un intervalo de programación distinto de `-onetimeonly`, a continuación, las opciones de poda `-until-SCN` y `-until-date` no son compatibles y se muestra el siguiente mensaje de error: `The archive log pruning option you have specified, -until-scn or -until-date for the schedule interval hourly is invalid. Specify either the -onetimeonly option for the schedule interval, or prune the archive logs using any one of the option all, or -before {-months | -days | -weeks| -hours}.`

Cuando se produce una conmutación por error en un entorno de multiprocesamiento de clústeres de alta disponibilidad (HACMP), debe reiniciar el servidor SnapManager para SAP para que la dirección de servicio (virtual) se asigne al host activo y las programaciones de SnapManager se ajusten al host SnapManager activo. Puede agregar esta información en las secuencias de comandos de conmutación por error de HACMP de multiprocesamiento o después del procesamiento.



Si existe el mismo perfil y nombre de programación en otro repositorio, no se inicia la operación de programación de backup en ese repositorio. La operación se cerrará con el siguiente mensaje: `operation is already running.`

### Paso

1. Introduzca el siguiente comando:

```
smsap schedule create -profile profile_name {[-full {-online | -offline |
-auto}[-retain [-hourly | -daily | -weekly | -monthly | -unlimited] [-verify]]
| [-data [-files files [files]] | [-tablespaces -tablespaces [-tablespaces]]
{-online | -offline | -auto}[-retain [-hourly | -daily | -weekly | -monthly |
-unlimited] [-verify]] | [-archivelogs]} [-comment comment] [-protect |
-protectnow | -noprotect] [-backup-dest path1 [,path2]] [-exclude-destpath1
[,path2]] [-prunelogs{-all | -untilSCN untilSCN | -until-date yyyy-MM-dd
HH:mm:ss | -before {-months | -weeks | -days | -hours}} -prune-dest
prune_dest1,prune_dest2] -schedule-name schedule_name [-schedule-comment
schedule_comment] -interval {-hourly | -daily | -weekly | -monthly |
-onetimeonly} -cronstring cronstring -start-time {start-timestart_time <yyyy-
MM-dd HH:mm>} -runasuser -runasuser [-force] [-taskspec -taskspec] [-quiet |
-verbose]
```

Si desea...	Realice lo siguiente...
<b>Programar una copia de seguridad de una base de datos en línea o sin conexión</b>	Especifique <code>-offline</code> o <code>-online</code> para programar un backup de la base de datos sin conexión o en línea. Si especifica las opciones mencionadas, no puede utilizar <code>-auto</code> .
<b>Deje que SnapManager gestione la programación de una base de datos independientemente de si está en línea o sin conexión</b>	Especifique <code>-auto</code> . Si especifica <code>-auto</code> , no puede utilizar <code>--offline</code> o <code>-online</code> .
<b>Programar una copia de seguridad de archivos de datos</b>	Especifique <code>-data</code> <code>-files</code> para mostrar los archivos separados por comas. Por ejemplo, utilice los nombres de archivo <code>f1,f2,f3</code> .
<b>Programar una copia de seguridad parcial de tablespaces específicos</b>	Especifique <code>-tablespaces</code> para mostrar los tablespaces separados por comas. Por ejemplo, utilice <code>ts1,ts2,ts3</code> .
<b>Programar copia de seguridad de archivos de registro de archivo</b>	Especifique lo siguiente: <ul style="list-style-type: none"> <li>• <code>-archivelogs</code> para programar la copia de seguridad de los archivos de registro de archivo</li> <li>• <code>-backup-dest</code> para programar los destinos de archivos de registro de archivos que se incluirán en el backup</li> <li>• <code>-exclude-dest</code> para programar los destinos de registro de archivos que se excluirán de la copia de seguridad</li> </ul>

Si desea...	Realice lo siguiente...
<b>Especifique los valores de la clase de retención</b>	<p>Especifique <code>-retain</code> e indique si el backup debe conservarse según una de las siguientes clases de retención:</p> <ul style="list-style-type: none"> <li>• <code>-hourly</code></li> <li>• <code>-daily</code></li> <li>• <code>-weekly</code></li> <li>• <code>-monthly</code></li> <li>• <code>-unlimited</code></li> </ul> <p>La configuración predeterminada de SnapManager es cada hora.</p>
<b>Programar la eliminación de archivos de registro de archivos</b>	<p>Especifique lo siguiente:</p> <ul style="list-style-type: none"> <li>• <code>-prunelogs</code> para comprimir los archivos de registro de archivo mientras se programa una copia de seguridad</li> <li>• <code>-prune-dest</code> para especificar el destino del registro de archivos a partir del cual se reducen los archivos de registro de archivos</li> </ul>
<b>Incluya un nombre para el horario</b>	<p>Especifique <code>-schedule-name</code>.</p>
<b>Programar copia de seguridad de la base de datos en un intervalo de tiempo específico</b>	<p>Especifique el <code>interval</code> y seleccione el intervalo de tiempo desde la siguiente, mediante el cual se deben crear los backups:</p> <ul style="list-style-type: none"> <li>• <code>-hourly</code></li> <li>• <code>-daily</code></li> <li>• <code>-weekly</code></li> <li>• <code>-monthly</code></li> <li>• <code>-onetimeonly</code></li> </ul>

Si desea...	Realice lo siguiente...
<b>Configurar un horario</b>	<p>Especifique <code>-cronstring</code> e incluya las siguientes siete subexpresiones que describen la opción individual:</p> <ul style="list-style-type: none"> <li>• 1 se refiere a segundos.</li> <li>• 2 se refiere a minutos.</li> <li>• 3 se refiere a horas.</li> <li>• 4 se refiere a un día en un mes.</li> <li>• 5 se refiere al mes.</li> <li>• 6 se refiere a un día en una semana.</li> <li>• <b>Opcional:</b> 7 se refiere al año.</li> </ul> <p><b>Nota:</b> Si usted programó su copia de seguridad con diferentes horas en <code>-cronstring</code> y <code>-start-time</code>, luego la programación de la copia de seguridad se sobrescribe y activa por el <code>-start-time</code>.</p>
<b>Agregar un comentario sobre el programa de copia de seguridad</b>	Especifique <code>-schedule-comment</code> seguido de la cadena de descripción.
<b>Especifique la hora de inicio de la operación de programación</b>	Especifique <code>-start-time</code> en el formato <code>yyyy-mm-dd hh:mm</code> .
<b>Cambiar el usuario de la operación de copia de seguridad programada mientras se programa la copia de seguridad</b>	Especifique <code>-runasuser</code> . La operación se ejecuta como el usuario (usuario raíz o usuario de Oracle) que creó la programación. Sin embargo, puede utilizar su propio ID de usuario si tiene credenciales válidas tanto para el perfil de base de datos como para el host.
<b>Active una actividad de tareas previas o posteriores a la tarea de la operación de programación de copia de seguridad mediante el archivo XML de especificación de tareas previas y posteriores</b>	Especifique el <code>-taskspec</code> Y proporcionar la ruta absoluta del archivo XML de especificación de tareas para realizar un preprocesamiento o una actividad de post-procesamiento antes o después de la operación de programación de copia de seguridad.

## Actualizar una programación de copia de seguridad

Puede ver una lista de operaciones programadas y actualizarlas si es necesario. Puede actualizar la frecuencia de programación, la hora de inicio de la programación, la expresión `cronstring` y el usuario que programó la copia de seguridad.

### Paso

1. Para actualizar la programación de un backup, escriba el siguiente comando:

```
smsap schedule update -profile profile_name -schedule-name schedulename [-  
schedule-comment schedule comment] -interval {-hourly | -daily | -weekly |  
-monthly | -onetimeonly} -start-time starttime -cronstring cronstring  
-runasuser runasuser [-quiet | -verbose]
```

## Consulte una lista de operaciones programadas

Es posible ver una lista de las operaciones programadas para un perfil.

### Paso

1. Para mostrar la información sobre el funcionamiento programado, escriba el siguiente comando:

```
smsap schedule list -profile profile_name [-quiet | -verbose]
```

## Suspender las programaciones de backup

SnapManager permite suspender una programación de backup hasta que se reanude la programación de backup.

### Acerca de esta tarea

Puede suspender las programaciones activas. Si intenta suspender la programación de backup que ya se encuentra suspendida, es posible que aparezca un mensaje de error "Cannot suspend: schedule <schedulename> already in suspend state".

### Paso

1. Para suspender temporalmente la programación del backup, introduzca este comando:

```
smsap schedule suspend -profile profile_name -schedule-name schedulename [-  
quiet | -verbose]
```

## Reanudar programaciones de backup

Los administradores tienen la opción de reanudar la programación de backup suspendida.

### Acerca de esta tarea

Si intenta reanudar las programaciones activas, es posible que se muestre el mensaje de error: "Cannot resume: schedule <schedulename> already in resume state".

1. Para reanudar la programación de backup suspendida, introduzca este comando:

```
smsap schedule resume -profile profile_name -schedule-name schedulename [-  
quiet | -verbose]
```

## Eliminar programaciones de backup

Es posible eliminar programaciones de backup cuando ya no sean necesarias.

## Paso

1. Para eliminar la programación de backup, introduzca este comando:

```
smsap schedule delete -profile profile_name -schedule-name schedulename [-quiet | -verbose]
```

## Restaurar backups de base de datos

SnapManager para SAP le permite restaurar una base de datos al estado que tenía cuando se tomó una copia Snapshot. Además del proceso de restauración basada en archivos, SnapManager admite la tecnología de restauración rápida basada en volúmenes, lo que reduce el tiempo de restauración de forma significativa en comparación con otros métodos de recuperación. Debido a que los backups se crean con más frecuencia, se reduce el número de registros que se debe aplicar, lo que reduce el tiempo medio de recuperación (MTTR) de una base de datos.

A continuación, se muestran algunas de las tareas que se pueden realizar en relación con la restauración y la recuperación de datos en bases de datos:

- Realizar una restauración basada en archivos o una restauración basada en volúmenes, que es el método más rápido de restaurar backups de base de datos y es el valor predeterminado que utiliza SnapManager.
- Restaure todo el backup o parte del mismo.

Cuando se restaura una parte de la misma, se especifica un grupo de espacios de tablas o un grupo de archivos de datos. También puede restaurar los archivos de control junto con los datos o solo los propios archivos de control.

- Recupere los datos en función de un momento específico o de todos los registros disponibles, que almacena la última transacción comprometida con la base de datos.

El punto en el tiempo puede ser un número de cambio de sistema (SCN) de Oracle o una fecha y hora (aaaa-mm-dd:hh:mm:ss). SnapManager utiliza el reloj de 24 horas.

- Restauración desde backups en el almacenamiento principal (backups locales).
- Restaurar y recuperar la copia de seguridad mediante SnapManager, o usar SnapManager para restaurar la copia de seguridad y utilizar otra herramienta, como Recovery Manager (RMAN), para recuperar los datos.
- Restaurar backups desde ubicaciones alternativas.
- Restaure los backups protegidos del almacenamiento secundario (backups remotos) y desde una ubicación alternativa mediante el archivo de especificación de restauración.

Puede restaurar una copia de seguridad realizada por una versión anterior de SnapManager utilizando SnapManager 3.0 y versiones posteriores.

Los administradores pueden realizar operaciones de restauración o recuperación mediante la interfaz gráfica de usuario (GUI) de SnapManager o mediante la interfaz de línea de comandos (CLI).

## Qué es la restauración de base de datos

SnapManager permite ejecutar operaciones de backup y restauración basadas en archivos o basadas en volúmenes.

En la siguiente tabla se describen los métodos de restauración:

Proceso de restauración	Detalles
Restauraciones rápidas basadas en volúmenes (desde el almacenamiento primario)	SnapManager restaura los archivos de datos de una base de datos mediante la restauración de un volumen completo. Este proceso predeterminado es el método más rápido para restaurar la base de datos.
Restauraciones basadas en archivos	Restauración de sistema de archivos completo en el almacenamiento (desde el principal o el secundario): SnapManager realiza una restauración completa del número de unidad lógica (LUN).
Restauración de archivos del lado del almacenamiento: SnapManager realiza una restauración de snap de archivos única (SFSR) en un entorno NAS. En SFSR, se restaura cada uno de los archivos o LUN que representan los objetos protegidos.	Restauración de copias de archivos del lado del host (desde el principal o secundario): SnapManager clona el backup local con una LUN o un FlexClone. El clon se monta y, a continuación, SnapManager copia los archivos host del clon en el sistema de archivos activo.



No es posible restaurar un backup desde el almacenamiento secundario si el backup también existe en el almacenamiento principal.

Cuando se completa la operación de restauración rápida, SnapManager realiza las siguientes tareas:

- Libera backups más recientes (que se toman después de la restauración del backup) en el mismo perfil, ya que sus copias Snapshot ya no existen en el almacenamiento principal.
- Elimina todas las copias Snapshot para backups del mismo perfil que tenía cualquier copia Snapshot eliminada automáticamente por el proceso de restauración rápida.

Esto evita que los backups se liberen parcialmente. Por ejemplo, primero se creó Backup\_A y, a continuación, se creó Backup\_B. Cada uno tiene una copia snapshot para los archivos de datos y uno para los registros de archivos. Una vez que SnapManager restaura Backup\_A mediante el proceso de restauración rápida, SnapManager elimina automáticamente la copia snapshot de los archivos de datos de Backup\_B. Dado que el registro de archivos no se restaura en el proceso de restauración rápida, SnapManager debe eliminar la copia Snapshot de los registros de archivos de Backup\_B una vez completado el proceso de restauración rápida.

### Restauración rápida

La restauración rápida o la restauración basada en volúmenes se denominan porque es el método de

restauración más rápido posible. Todo el volumen del sistema de almacenamiento vuelve a una copia Snapshot. En el nivel de almacenamiento, esta restauración es casi instantánea. No obstante, al restaurar un volumen, se pueden producir las siguientes consecuencias negativas y, por lo tanto, se debe usar con precaución:

- Se revierte todo el volumen en el lado del almacenamiento, incluidos los siguientes:
  - Archivos que no se consideraron como parte de la copia de seguridad
  - Otros archivos, sistemas de archivos o LUN en el volumen
- Se eliminan todas las copias Snapshot que se crearon después de la copia Snapshot en la que se revierte el volumen.

Por ejemplo, ya no puede restaurar el backup del martes si el backup del lunes fue restaurado.

- Las relaciones con los sistemas de almacenamiento secundario se interrumpen si la copia Snapshot restaurada es más antigua que la copia Snapshot básica de la relación.

### **Restauración de todo el sistema de archivos en el lado del almacenamiento**

Se realiza una restauración de sistema de archivos completo en el lado del almacenamiento cuando no es posible realizar una restauración de volumen, pero es posible restaurar todo el sistema de archivos en el sistema de almacenamiento.

Cuando se realiza una restauración del sistema de archivos en el almacenamiento, se produce lo siguiente:

- En un entorno SAN, todas las LUN utilizadas por el sistema de archivos (y el grupo de volúmenes subyacente, si las hubiera) se restauran en el sistema de almacenamiento.
- En un entorno NAS, todos los archivos del sistema de archivos se restauran en el sistema de almacenamiento.

En los entornos NAS, este mecanismo de restauración no proporciona ventajas adicionales con respecto a la restauración de archivos del almacenamiento.

Cuando se realiza una restauración del sistema de archivos en el almacenamiento, se produce lo siguiente, según la ubicación del almacenamiento:

- Cuando las restauraciones de SnapManager desde sistemas de almacenamiento primario, se restauran las LUN (SAN) o los archivos (NAS) mediante SFSR.
- Cuando SnapManager restaura desde sistemas de almacenamiento secundario, los LUN (SAN) o los archivos (NAS) se copian desde los sistemas de almacenamiento secundario de vuelta al sistema de almacenamiento primario a través de la red.

Como el sistema de archivos se restaura por completo, se revierten los archivos que no sean parte del backup. Se requiere una anulación si los archivos, que no forman parte de la restauración, se encuentran en el sistema de archivos que se está restaurando.

### **Restauración de archivos del lado del almacenamiento**

En ocasiones, se realiza una restauración de archivos en el lado del almacenamiento cuando no se puede realizar una restauración del sistema de archivos en el lado del almacenamiento. En una restauración de archivos del almacenamiento, los archivos individuales de un sistema de archivos se restauran directamente en los sistemas de almacenamiento.



Este tipo de restauración solo se puede realizar en entornos NFS o, en ciertos casos, en entornos ASM.

Cuando se realiza una restauración de archivos en el almacenamiento, se produce lo siguiente:

- Cuando SnapManager restaura archivos NFS de sistemas de almacenamiento primario, se restauran los archivos individuales mediante SFSR.
- Cuando SnapManager restaura archivos NFS desde sistemas de almacenamiento secundario, los archivos individuales se vuelven a copiar en el sistema de almacenamiento primario a través de la red de almacenamiento.

### **Restauración de archivos del lado del host**

Una restauración de copias de archivos en el lado del host se usa como último recurso en entornos SAN cuando no se pueden realizar restauraciones rápidas, restauraciones del sistema de archivos en el lado del almacenamiento y restauración de archivos en el lado del almacenamiento.

Una restauración de copias de archivos del host implica las siguientes tareas:

- Clonar el almacenamiento
- Conectar el almacenamiento clonado al host
- Copiar archivos de los sistemas de archivos clonados de nuevo en los sistemas de archivos activos
- Desconectar el almacenamiento de clones del host
- Eliminar el almacenamiento del clon

Cuando se restaura desde el almacenamiento secundario, SnapManager intenta primero restaurar los datos directamente desde el sistema de almacenamiento secundario al sistema de almacenamiento primario (sin afectar el host). Si SnapManager no puede realizar este tipo de restauración (por ejemplo, si los archivos no forman parte de la restauración existen en un sistema de archivos), SnapManager realizará una restauración de copia de archivos del lado del host. SnapManager tiene dos métodos para realizar una restauración de copia de archivos en el lado del host desde el almacenamiento secundario. El método SnapManager selecciona se configura en la `smsap.config` archivo.

- Directo: SnapManager clona los datos del almacenamiento secundario, monta los datos clonados del sistema de almacenamiento secundario en el host, y después copia los datos del clon en el entorno activo. Esta es la directiva de acceso secundaria predeterminada.
- Indirecto: SnapManager copia primero los datos en un volumen temporal del sistema de almacenamiento primario y, a continuación, monta los datos del volumen temporal en el host y, a continuación, copia los datos del volumen temporal en el entorno activo. Esta normativa de acceso secundario se debe utilizar solo si el host no tiene acceso directo al sistema de almacenamiento secundario. Las restauraciones mediante este método tardan el doble de tiempo que la normativa de acceso secundario directo, ya que se realizan dos copias de los datos.

La decisión de utilizar el método directo o indirecto se controla mediante el valor del `restore.secondaryAccessPolicy` en la `smsap.config` archivo de configuración. El valor predeterminado es `directa`.

### **Directrices sobre cuándo utilizar la restauración rápida**

Existen reglas específicas que se aplican para usar la restauración rápida con el fin de lograr un rendimiento óptimo de la restauración. En algunos casos, no se puede utilizar una restauración rápida.

Para lograr un rendimiento de restauración óptimo (restauración de volúmenes o restauración de grupos de discos completos), se deben cumplir las siguientes reglas:

- Solo las restauraciones completas de backups completos pueden ser válidas para una restauración rápida.
- Solo los archivos de datos pueden optar a una restauración rápida.
- Los archivos de datos deben ser los únicos archivos de un volumen que puedan optar a una restauración rápida.

Aunque los archivos de datos temporales pueden residir en el volumen, los archivos de control, los registros, los archivos pfiles u otros archivos deben residir en un volumen independiente de los archivos de datos. Debe configurar una base de datos de Oracle con archivos de datos en un volumen aparte de los archivos de control, registros archivados y archivos de registro en línea.

- Los archivos de datos de una sola base de datos deben estar presentes en el volumen.
- Se pueden utilizar varios sistemas de archivos, pero los archivos de dichos sistemas de archivos deben ser archivos de datos para una única base de datos.
- SAP requiere una distribución de archivos ligeramente diferente.

La sección «"disposición general y configuración»» contiene detalles.

- Si `BRRESTORE` se utiliza para restaurar la base de datos, la restauración rápida se utiliza con el parámetro `fast` en el archivo de parámetros de la utilidad de copia de seguridad.



Para comprobar si un backup creado previamente se restaura mediante una restauración rápida, puede usar la `-preview` opción de `smsap backup restore` comando.

El proceso de restauración rápida no se puede utilizar en los siguientes casos:

- En backups parciales
- En backups desde el almacenamiento secundario si el backup también existe en el almacenamiento primario

No es posible restaurarlos mediante la restauración basada en archivos o volúmenes.

- En backups protegidos con SnapVault

El proceso de restauración rápida no se puede utilizar para backups creados con anterioridad al último backup protegido. No obstante, se puede utilizar el proceso de restauración rápida de los backups creados después del último backup protegido. Considere, por ejemplo, los backups A, B y C. B es el último backup a transferir a almacenamiento secundario mediante SnapVault. Puede restaurar B y C rápidamente, pero no puede restaurar A rápidamente porque se creó antes que la última copia de seguridad protegida. SnapVault necesita una SnapVault básica para calcular la diferencia de tiempo y enviar al almacenamiento secundario la próxima vez que se transfiere un backup al almacenamiento secundario. El último backup protegido actúa como la copia Snapshot de referencia. Por lo tanto, si se utiliza el proceso de restauración rápida, SnapVault no podrá reconocer la línea de base.

- Clones de FlexClones o LUN que utilizan copias de Snapshot que se crearon después de la copia Snapshot en la que se está recreando el volumen

Por ejemplo, los clones pueden ser el resultado de un backup posterior que SnapManager está montado o clonado.

- LUN que no forman parte de la copia snapshot activa de SnapDrive

No es posible realizar una restauración rápida junto con otros tipos de restauraciones para la misma copia de seguridad. Por ejemplo, si se puede restaurar un volumen de datos mediante el proceso de restauración rápida pero no puede otro volumen de datos, ninguno de los cuales se restaurará mediante el proceso de restauración rápida. En este caso, es posible elegir una restauración basada en archivos.

Además, debe tener en cuenta los puntos siguientes sobre las restauraciones de bases de datos:

- SnapManager nunca restaura registros de archivos ni registros de reconstrucción, pero monta la copia de seguridad de archivos de registro de archivos y los utiliza para la recuperación.
- SnapManager nunca restaura los archivos de control mediante la restauración de volúmenes.
- Si desea restaurar archivos de control y archivos de datos, SnapManager realiza la restauración en dos pasos.

SnapManager restaura los archivos de control primero y después los archivos de datos.

- Si SnapManager encuentra archivos temporales en el mismo volumen que los archivos de espacio de tabla estándar, no es necesario emitir una sobrescritura para realizar una restauración a nivel de volumen.

Después de una restauración de volumen, el espacio de tabla TEMPORAL vuelve a estar en línea.

Tanto SnapManager for SAP como la interfaz BACKINT usan la misma lógica al determinar qué mecanismo de restauración se puede usar. Todos los métodos de restauración se pueden usar tanto si la copia de seguridad se realizó con SnapManager for SAP como con la interfaz BACKINT, y si la restauración se realiza a través de SnapManager for SAP o de la interfaz BACKINT.

## Información relacionada

["Documentación en el sitio de soporte de NetApp: mysupport.netapp.com"](http://mysupport.netapp.com)

## Ventajas e inconvenientes del uso de la restauración rápida

Los administradores de bases de datos deben conocer las ventajas y desventajas que supone el uso de restauraciones rápidas basadas en volúmenes.

La restauración de backups de base de datos mediante restauraciones rápidas ofrece las siguientes ventajas:

- Las restauraciones basadas en volúmenes reducen el tiempo necesario para restaurar backups.
- SnapManager ofrece comprobaciones rápidas de los requisitos para las restauraciones. SnapManager analiza el backup de la base de datos y muestra información sobre si puede ejecutar la restauración basada en volúmenes.
- Puede obtener una vista previa de la operación de restauración y decidir si continuar con la ruta recomendada o anular la recomendación con el proceso seleccionado.

La restauración de backups de base de datos mediante restauraciones rápidas presenta las siguientes desventajas:

- Se revierte todo el sistema de archivos, incluidos los archivos que no se consideraron parte de la copia de seguridad. También se revierten otros archivos, sistemas de archivos o LUN del volumen.
- SnapManager quita todas las copias Snapshot que se realizaron después de que la Snapshot a la que se está revirtiendo. De hecho, pierde el historial después de la fecha de la copia Snapshot. Por ejemplo, no

puede restaurar la copia de seguridad del martes si ya ha restaurado la copia de seguridad del lunes.

Puede evitar estas desventajas si sigue estas recomendaciones:

- Optimice el diseño de la base de datos de acuerdo con prácticas recomendadas.
- Proteger los backups en el almacenamiento secundario. Sin embargo, si elimina copias Snapshot del almacenamiento primario, no puede usar restauraciones rápidas para restaurarlas desde el almacenamiento secundario.

### Rápidas comprobaciones de cumplimiento de la restauración

Cuando decide realizar una restauración rápida de un backup, SnapManager realiza en primer lugar una comprobación de idoneidad para determinar si puede utilizar el proceso de restauración rápida.

SnapManager ofrece los siguientes tipos de comprobaciones:

- Comprobaciones obligatorias: SnapManager puede realizar el proceso de restauración rápida sólo si se cumplen todas las condiciones en esta fase de comprobación.
- Comprobaciones anulables: Si las condiciones de esta comprobación fallan, los administradores pueden anular la comprobación para forzar un proceso de restauración rápida. Sin embargo, debe anular estas comprobaciones con precaución.

En la siguiente tabla se enumeran los problemas que puede encontrar e indican si la comprobación de elegibilidad de la restauración rápida puede anularse:

Problema	Se requiere pasar	Detalles
ACFS, Voting Disk o OCR está presente en el grupo de discos ASM en 11gR2	Sí	No se puede realizar una restauración rápida. Resolución: Ninguna  No se puede anular.
Solo los backups creados con SnapManager 3.0 o posterior se pueden restaurar rápidamente	Sí	No se puede anular.
Sólo se pueden restaurar rápidamente las copias snapshot creadas con SnapDrive para UNIX 4.0 o posterior	Sí	No se puede anular.
El volumen es un volumen raíz	Sí	El volumen que se restaura es un volumen raíz en el sistema de almacenamiento. Resolución: No utilice el volumen raíz en el sistema de almacenamiento.  No se puede anular.

Problema	Se requiere pasar	Detalles
La restauración de volúmenes no está disponible en Windows	Sí	<p>El volumen que se restaura es un volumen raíz en el sistema de almacenamiento. Resolución: Ninguna</p> <p>No se puede anular.</p>
Se deshabilita la restauración de volumen	Sí	<p>Se deshabilitó la restauración de volúmenes. Resolución: Active la restauración de volúmenes seleccionando diferentes opciones al iniciar la restauración. En la interfaz de línea de comandos de, no se debe utilizar <code>-fast -off</code>.</p> <p>No se puede anular.</p>

Problema	Se requiere pasar	Detalles
<p>Controle los archivos y los archivos de datos del mismo volumen</p>	<p>Sí</p>	<p>Para los backups en línea, los archivos de control y los archivos de datos no pueden estar en el mismo volumen porque SnapManager toma dos copias snapshot del volumen (una en la que los archivos de datos son consistentes en el modo de backup dinámico, y uno en el que los archivos de control de copia de seguridad son consistentes después de completar el modo de copia de seguridad en caliente). La restauración del volumen volverá a la primera copia snapshot, lo que elimina la segunda copia snapshot que contiene los archivos de control de backup. Si se produce una restauración solo de archivos de datos, los archivos de control se restauran en un estado incoherente, SnapManager restaura el archivo de control de backup y abre la base de datos con la opción reaslogs, lo cual no es el comportamiento deseado.</p> <p>Resolución: Migre los archivos de control y los archivos de datos a sistemas de archivos independientes que no compartan el mismo volumen subyacente. Esto no ayuda a la restauración en la cual la comprobación falló, pero sí a las operaciones de restauración de backup futuras.</p> <p>No se puede anular.</p>

Problema	Se requiere pasar	Detalles
<p>Los registros de archivo y los archivos de datos no deben existir en el mismo volumen</p>	<p>Sí</p>	<p>Los registros de archivo de bases de datos y los archivos de datos residen en sistemas de archivos respaldados por el mismo volumen del sistema de almacenamiento. Si se ejecutó una restauración de volumen, SnapManager no puede abrir la base de datos después de la restauración de un backup en línea debido a que el archivo de registro archivado que se escribe una vez que la base de datos se desconecta del modo de backup dinámico no está disponible. Además, no podría avanzar por transacciones posteriores que podrían haber estado en los archivos de registro de archivos.</p> <p>Resolución: Migre los registros de archivos y los archivos de datos a sistemas de archivos independientes que no compartan el mismo volumen de sistema de almacenamiento subyacente. Esto no ayuda a la restauración en la cual la comprobación falló, pero sí a las operaciones de restauración de backup futuras.</p> <p>No se puede anular.</p>

Problema	Se requiere pasar	Detalles
<p>Los registros en línea y los archivos de datos no deben existir en el mismo volumen</p>	<p>Sí</p>	<p>Los registros de recuperación y los archivos de datos en línea de la base de datos residen en sistemas de archivos respaldados por el mismo volumen del sistema de almacenamiento. Si se realizó una restauración de volumen, la recuperación no puede utilizar los registros de recuperación en línea porque se habrían revertido.</p> <p>Solución: Migre los redo logs y los archivos de datos en línea a sistemas de archivos independientes que no compartan el mismo volumen de sistema de almacenamiento subyacente. Esto no ayuda a la restauración en la cual la comprobación falló, pero sí a las operaciones de restauración de backup futuras.</p> <p>No se puede anular.</p>



Problema	Se requiere pasar	Detalles
Se revierten los archivos del sistema de archivos que no formen parte del ámbito de restauración	Sí	<p>Los archivos visibles en el host, excepto los archivos que se van a restaurar, existen en un sistema de archivos del volumen. Si se realizó una restauración rápida o una restauración de sistema de archivos en el lado del almacenamiento, los archivos visibles en el host se revertirían a su contenido original al crear la copia Snapshot. Si SnapManager descubre 20 o menos archivos, se enumeran en la comprobación de elegibilidad. De lo contrario, SnapManager muestra un mensaje que debería investigar el sistema de archivos.</p> <p>Resolución: Migre los archivos no utilizados por la base de datos a un sistema de archivos diferente que utilice un volumen diferente. También puede eliminar los archivos.</p> <p>Si SnapManager no puede determinar el propósito del archivo, puede anular el fallo de comprobación. Si se anula la comprobación, se revierten los archivos que no estén en el ámbito de restauración. Anule esta comprobación sólo si está seguro de que al revertir los archivos no se afectará negativamente a nada.</p>

Problema	Se requiere pasar	Detalles
<p>Se revierten los sistemas de archivos del grupo de volúmenes especificado que no formen parte del alcance de restauración</p>	<p>No</p>	<p>Hay varios sistemas de archivos en el mismo grupo de volúmenes, pero no se solicitan que se restauren todos los sistemas de archivos. La restauración del sistema de archivos del almacenamiento y la restauración rápida no se pueden usar para restaurar sistemas de archivos individuales dentro de un grupo de volúmenes, ya que las LUN que utiliza el grupo de volúmenes contienen datos de todos los sistemas de archivos. Todos los sistemas de archivos de un grupo de volúmenes deben restaurarse a la vez para utilizar una restauración rápida o una restauración del sistema de archivos del lado del almacenamiento. Si SnapManager descubre 20 archivos o menos, SnapManager los enumera en la comprobación de elegibilidad. De lo contrario, SnapManager proporciona un mensaje que debería investigar el sistema de archivos.</p> <p>Resolución: Migre los archivos que no utiliza la base de datos a un grupo de volúmenes diferente. Otra opción es eliminar los sistemas de archivos del grupo de volúmenes.</p> <p>Puede anular.</p>

Problema	Se requiere pasar	Detalles
Se revierten los volúmenes de host de un grupo de volúmenes especificado que no forman parte del alcance de restauración	No	<p>Varios volúmenes de host (volúmenes lógicos) están en el mismo grupo de volúmenes, pero no todos los volúmenes de host se solicitan que se restauren. Esta comprobación es similar a los sistemas de archivos del grupo de volúmenes que no forman parte del ámbito de restauración se revertirá excepto que los demás volúmenes de host del grupo de volúmenes no se montan como sistemas de archivos en el host. Resolución: Migre los volúmenes de hosts que utiliza la base de datos a otro grupo de volúmenes. O bien, elimine los otros volúmenes de host del grupo de volúmenes.</p> <p>Si anula la comprobación, se restauran todos los volúmenes de host del grupo de volúmenes. Anule esta comprobación solo si tiene la seguridad de que la reversión de los otros volúmenes de host no afecta negativamente en nada.</p>
Las extensiones de archivo han cambiado desde la última copia de seguridad	Sí	No se puede anular.

Problema	Se requiere pasar	Detalles
<p>Los LUN asignados en el volumen no forman parte del ámbito de restauración se revierten</p>	<p>Sí</p>	<p>Las LUN distintas de las solicitadas para restaurar en el volumen están actualmente asignadas a un host. No se puede realizar una restauración de volúmenes porque otros hosts o aplicaciones que utilizan estos LUN se volverán inestables. Si los nombres de las LUN terminan con un guión bajo y un índice entero (por ejemplo, _0 o _1), normalmente estas LUN son clones de otras LUN dentro del mismo volumen. Es posible que se monte otro backup de la base de datos o que exista un clon de otro backup.</p> <p>Resolución: Migre los LUN que la base de datos no usa en un volumen diferente. Si las LUN asignadas son clones, busque backups montados de la misma base de datos o clones de la base de datos, y desmonte el backup o quite el clon.</p> <p>No se puede anular.</p>

Problema	Se requiere pasar	Detalles
<p>LAS LUN sin asignar en el volumen que no forman parte del ámbito de restauración se reversionen</p>	<p>No</p>	<p>Existen otras LUN distintas de las solicitadas para restaurar en el volumen. Estas LUN no están actualmente asignadas a ningún host, por lo que al restaurarse no se interrumpen los procesos activos. Sin embargo, se puede quitar la asignación de las LUN temporalmente. Solución: Migre los LUN que la base de datos no usa en un volumen diferente o elimine los LUN.</p> <p>Si anula esta comprobación, la restauración de volumen revertirá estas LUN al estado en que se realizó la copia Snapshot. Si la LUN no existía cuando se hizo la copia Snapshot, la LUN no existirá después de la restauración de un volumen. Anule esta comprobación solo si tiene la seguridad de que al revertir las LUN no se afectará de forma negativa en nada.</p>
<p>Las LUN presentes en la copia Snapshot de volumen pueden no ser coherentes al revertirse</p>	<p>No</p>	<p>Durante la creación de copias Snapshot, en el volumen existían LUN diferentes a las que se solicitó la copia Snapshot. Es posible que estas otras LUN no estén en un estado consistente. Solución: Migre los LUN que la base de datos no usa en un volumen diferente o elimine los LUN. Esto no facilita el proceso de restauración en el que falló la comprobación, pero ayudará a restaurar futuros backups creados después de mover o eliminar las LUN.</p> <p>Si anula esta comprobación, las LUN se reversionen al estado incoherente en el que se ha hecho la copia Snapshot. Anule esta comprobación solo si tiene la seguridad de que al revertir las LUN no se afectará de forma negativa en nada.</p>

Problema	Se requiere pasar	Detalles
Las nuevas copias Snapshot tienen un clon de volúmenes	Sí	<p>Se han creado clones de las copias Snapshot que se crearon después de solicitar la restauración de la copia Snapshot. Dado que una restauración de volumen eliminará las copias Snapshot más adelante y no se puede eliminar una copia Snapshot si tiene un clon, no se puede realizar una restauración de volumen. Resolución: Elimine clones de copias snapshot más adelante.</p> <p>No se puede anular.</p>
Se montan backups más recientes	Sí	<p>Se montan los backups realizados después de restaurar el backup. Dado que una restauración de volúmenes elimina copias de Snapshot posteriores, no es posible eliminar una copia de Snapshot si tiene un clon, una operación de montaje de backup crea un almacenamiento clonado y no se puede ejecutar una restauración de volumen. Resolución: Desmonte la copia de seguridad posterior o restaure a partir de una copia de seguridad realizada después de la copia de seguridad montada.</p> <p>No se puede anular.</p>
Existen clones de backups más recientes	Sí	<p>Se clonan los backups realizados después de la restauración del backup. Dado que una restauración de volumen elimina copias Snapshot más adelante y no se puede eliminar una copia Snapshot si tiene un clon, no se puede realizar una restauración de volumen. Resolución: Elimine el clon del backup más nuevo o restaure desde un backup realizado después de los backups que tienen clones.</p> <p>No se puede anular.</p>

Problema	Se requiere pasar	Detalles
Se pierden nuevas copias Snapshot de volumen	No	<p>Al realizar una restauración de volumen, se eliminan todas las copias Snapshot creadas después de la copia Snapshot en la que se restaura el volumen. Si SnapManager puede asignar una copia Snapshot más adelante a un backup de SnapManager con el mismo perfil, aparecerá el mensaje "se liberarán o se eliminarán los backups más recientes". Si SnapManager no puede asignar una copia Snapshot más tarde a un backup de SnapManager en el mismo perfil, este mensaje no aparece. Solución: Restaure a partir de un backup posterior o elimine las copias snapshot más adelante.</p> <p>Puede anular.</p>

Problema	Se requiere pasar	Detalles
Los backups más recientes se liberarán o se eliminarán	No	<p>Al realizar una restauración de volúmenes, se eliminan todas las copias Snapshot creadas después de la copia Snapshot en la que se restaura el volumen. Por consiguiente, los backups creados después del backup que se va a restaurar se eliminan o se liberan. Los backups posteriores se eliminan en las siguientes situaciones:</p> <ul style="list-style-type: none"> <li>• El estado del backup no está <b>PROTEGIDO</b></li> <li>• <code>retain.alwaysFreeExpiredBackups</code> es <b>false</b> <code>pulg smsap.config</code></li> </ul> <p>Los backups posteriores se liberan en las siguientes situaciones:</p> <ul style="list-style-type: none"> <li>• El estado del backup está <b>PROTEGIDO</b></li> <li>• <code>retain.alwaysFreeExpiredBackups</code> es cierto <b>false</b> <code>pulg smsap.config</code></li> </ul> <p>Resolución: Restaure a partir de una copia de seguridad posterior o libere o elimine copias de seguridad posteriores.</p> <p>Si anula esta comprobación, los backups creados después del backup que se está restaurando se eliminan o se liberan.</p>



Problema	Se requiere pasar	Detalles
Se pierde la relación de SnapMirror para los volúmenes	Sí (si está deshabilitado el control de acceso basado en roles o no tiene permiso de control de acceso basado en roles)	<p>Al restaurar un volumen en una copia Snapshot con anterioridad a la copia Snapshot de referencia en una relación de SnapMirror, se destruye la relación. Resolución: Restauración a partir de un backup creado después de la copia Snapshot básica de la relación. Como alternativa, divida la relación de almacenamiento manualmente (y luego vuelva a crear y vuelva a establecer la base de la relación una vez finalizada la restauración).</p> <p>Es posible anular la sustitución si el control de acceso basado en roles está habilitado y existe permiso de control de acceso basado en roles.</p>
La relación de SnapVault para el volumen se pierde si se ha producido el proceso de restauración rápida	Sí (si está deshabilitado el control de acceso basado en roles o no tiene permiso de control de acceso basado en roles)	<p>Al restaurar un volumen en una copia Snapshot con anterioridad a la copia Snapshot de referencia en una relación de SnapVault, se destruye la relación. Resolución: Restauración a partir de un backup creado después de la copia Snapshot básica de la relación. Como alternativa, divida la relación de almacenamiento manualmente (y luego vuelva a crear y vuelva a establecer la base de la relación una vez finalizada la restauración).</p> <p>No se puede reemplazar, si el control de acceso basado en roles está habilitado y tiene permiso de control de acceso basado en roles.</p>
Se revierten los archivos NFS del volumen que no formen parte del ámbito de restauración	No	<p>Los archivos presentes en el volumen del sistema de almacenamiento, que no son visibles en el host, se revierten si se realiza una restauración de volumen. Resolución: Migre los archivos no utilizados por la base de datos a un volumen diferente o elimine los archivos.</p> <p>Puede anular. Si anula este fallo de comprobación, se eliminan las LUN.</p>

Problema	Se requiere pasar	Detalles
Los recursos compartidos de CIFS existen para el volumen	No	El volumen que se restaura tiene recursos compartidos CIFS. Es posible que otros hosts estén accediendo a los archivos del volumen durante la restauración del volumen. Resolución: Elimine los recursos compartidos CIFS innecesarios.  Puede anular.
Restauración desde una ubicación alternativa	Sí	Se proporcionó una especificación de restauración para la operación de restauración que especifica que los archivos se restauren desde una ubicación alternativa. Solo se pueden utilizar las utilidades de copia del lado del host para restaurar desde una ubicación alternativa.  Resolución: Ninguna.  No se puede anular.
No se admite la restauración del sistema de archivos en el lado del almacenamiento en una base de datos de RAC	Sí	No se puede anular.

## Recuperación de backups

En SnapManager, se deben ejecutar las operaciones de restauración y recuperación al mismo tiempo. No se puede realizar una operación de restauración y, posteriormente, se puede realizar una operación de recuperación de SnapManager.

En SnapManager 3.2 o anterior, se puede utilizar SnapManager para restaurar y recuperar la copia de seguridad o utilizar SnapManager para restaurar la copia de seguridad y utilizar otra herramienta, como Oracle Recovery Manager (RMAN), para recuperar los datos. Puesto que SnapManager puede registrar sus copias de seguridad con RMAN, puede utilizar RMAN para restaurar y recuperar la base de datos con granularidades más finas como los bloques. Esta integración combina las ventajas de la velocidad y la eficiencia del espacio de las copias Snapshot con el nivel de control preciso para la restauración mediante RMAN.



Debe recuperar una base de datos antes de poder utilizarla. Puede utilizar cualquier herramienta o script para recuperar una base de datos.

A partir de SnapManager 3.2 para SAP, SnapManager permite restaurar automáticamente los backups de bases de datos mediante los backups de registros de archivos. Incluso cuando los backups de registros de archivos están disponibles en la ubicación externa, SnapManager utiliza los backups de registros de archivos desde la ubicación externa para restaurar los backups de la base de datos.

Si se agregan nuevos archivos de datos a la base de datos, Oracle recomienda realizar una nueva copia de seguridad inmediatamente. Además, si restaura una copia de seguridad realizada antes de agregar los nuevos archivos de datos e intenta recuperar a un punto después de agregar los nuevos archivos de datos, el proceso de recuperación automática de Oracle podría fallar, ya que no puede crear archivos de datos. Consulte la documentación de Oracle para conocer el proceso de recuperación de los archivos de datos agregados después de una copia de seguridad.

### Estado de la base de datos necesario para el proceso de restauración

El estado de la base de datos que se va a restaurar depende del tipo de proceso de restauración que se desee realizar y del tipo de archivos que se incluirán.

En la siguiente tabla, se muestra el estado en el que la base de datos debe estar según la opción de restauración seleccionada y el tipo de archivos que se desea incluir en la restauración:

Tipo de restauración	Archivos incluidos	Estado de la base de datos para esta instancia	Estado de la base de datos para otra instancia (solo RAC)
Solo restauración	Archivos de control	Apagado	Apagado
	Archivos del sistema	Montaje o apagado	Montaje o apagado
	No hay archivos del sistema	Cualquier estado	Cualquier estado
Restauración y recuperación	Archivos de control	Apagado	Apagado
	Archivos del sistema	Montaje	Montaje o apagado
	No hay archivos del sistema	Montar o abrir	Cualquiera

El estado de la base de datos que requiere SnapManager para una operación de restauración depende del tipo de restauración que se ejecute (archivos completos, parciales o de control). SnapManager no realiza la transición de la base de datos a un estado inferior (por ejemplo, de Open a Mount) a menos que se especifique la opción force.

SnapManager para SAP no verifica si se está ejecutando SAP. SnapManager para SAP espera a que transcurra un tiempo de espera y luego cierra la base de datos, que puede agregar una hora de tiempo de restauración adicional.

### Qué planes de vista previa de restauración son

SnapManager ofrece planes de restauración antes y después de que se completa una operación de restauración. Los planes de restauración se utilizan para obtener una vista previa, revisar y analizar con respecto a los diferentes métodos de restauración.

#### Estructura del plan de restauración

El plan de restauración consta de las dos secciones siguientes:

- Vista previa/revisión: Esta sección describe cómo restaurará SnapManager cada archivo (o lo ha restaurado).
- Análisis: En esta sección se describe por qué no se utilizaron algunos mecanismos de restauración

durante la operación de restauración.

### La sección Vista previa/revisión

Esta sección muestra cómo se restaurará o se restaurará cada archivo. Al ver el plan de restauración antes de una operación de restauración, se denomina vista previa. Cuando se visualiza después de completar una operación de restauración, se denomina revisión.

El siguiente ejemplo de vista previa muestra que los archivos se restauran utilizando métodos rápidos basados en volúmenes, restauración del sistema de archivos en el lado del almacenamiento y restauración del sistema en el lado del almacenamiento. Para determinar por qué no se restaurarían todos los archivos utilizando el mismo método de restauración, consulte la sección Análisis.

```
Preview:
The following files will be restored completely via: fast restore
+DG1/rac6/users.dbf

The following files will be restored completely via: storage side file
system restore
+DG2/rac6/sysaux.dbf
+DG2/rac6/system.dbf
The following files will be restored completely via: storage side system
restore
+DG2/rac6/undotbs1.dbf
+DG2/rac6/undotbs2.dbf
```

Cada método de restauración tiene una subsección que contiene información sobre los archivos que se pueden restaurar mediante ese método de restauración. Las subsecciones se ordenan según niveles decrecientes de eficiencia de los métodos de almacenamiento. En el ejemplo anterior, el método de restauración rápida es más eficiente que el método de restauración del sistema de archivos de almacenamiento, y así se muestra primero.

Es posible restaurar un archivo mediante varios métodos de restauración. Se utilizan varios métodos de restauración cuando los números de unidad lógica (LUN) subyacentes utilizados en un sistema de archivos se distribuyen entre los volúmenes del sistema de almacenamiento diferentes y algunos volúmenes son aptos para la restauración de volúmenes, mientras que otros no lo son. Si se utilizan varios métodos de restauración para restaurar el mismo archivo, la sección de vista previa será similar a la siguiente:

```
The following files will be restored via a combination of:
[fast restore, storage side file system restore. storage side system
restore]
```

### La sección Análisis

La sección Análisis presenta las razones por las que algunos mecanismos de restauración no se utilizarán o no. Puede usar esta información para determinar qué es necesario para habilitar mecanismos de restauración más eficientes.

En el siguiente ejemplo se muestra una sección de análisis:

## Analysis:

The following reasons prevent certain files from being restored completely via: fast restore

- \* LUNs present in snapshot of volume fas960:  
/vol/rac\_6\_asm\_disks may not be consistent when reverted:  
[fas960:/vol/rac6\_asm\_disks/DG4D1.lun]  
Mapped LUNs in volume fas960:/vol/rac\_6\_asm\_disks  
not part of the restore scope will be reverted: [DG4D1.lun]

## Files to restore:

- +DG2/rac6/sysaux.dbf
- +DG2/rac6/system.dbf
- +DG2/rac6/undotbs1.dbf
- +DG2/rac6/undotbs2.dbf

\* Reasons denoted with an asterisk (\*) are overridable.

En el ejemplo, el primer fallo se puede anular mediante el uso `-fast -override` Desde la interfaz de línea de comandos (CLI) o seleccionando **Anular** en la interfaz gráfica de usuario (GUI). El segundo fallo en las LUN asignadas del volumen es obligatorio y no se puede superar.

Puede resolver las comprobaciones haciendo lo siguiente:

- Para resolver un fallo de comprobación obligatorio, cambie el entorno de modo que se apruebe la comprobación.
- Para resolver un fallo de comprobación anulable, puede cambiar el entorno o anular la comprobación.

Sin embargo, debe tener cuidado porque la anulación de la comprobación puede resultar en consecuencias no deseadas.

## Obtener una vista previa de la información de restauración de copia

Puede obtener una vista previa de la información sobre un proceso de restauración de backup antes de que se produzca para ver información sobre la idoneidad para la restauración que SnapManager para SAP encuentra en el backup. SnapManager analiza los datos del backup para determinar si el proceso de restauración puede completarse correctamente.

### Acerca de esta tarea

La vista previa de la restauración proporciona la siguiente información:

- Qué mecanismo de restauración (restauración rápida, restauración de sistema de archivos en el lado del almacenamiento, restauración de archivos en el lado del almacenamiento o restauración de copias de archivos del lado del host) se puede utilizar para restaurar cada archivo.
- Por qué no se utilizaron mecanismos más eficientes para restaurar cada archivo, al especificar el

-verbose opción.

Si especifica el `-preview` en la `backup restore` SnapManager no restaura nada, pero enumera los archivos que se van a restaurar e indica cómo se restaurarán.



Puede obtener una vista previa de todos los tipos de mecanismos de restauración. La vista previa muestra información acerca de un máximo de 20 archivos.

## Pasos

1. Introduzca el siguiente comando:

```
smsap backup restore -profile profile_name -label label -complete -preview  
-verbose
```

### ejemplo

Por ejemplo, introduzca:

```
smsap backup restore -profile targetdb1_prof1  
-label full_bkup_sales_nov_08 -complete -preview -verbose
```

En el siguiente ejemplo, se muestran algunos archivos que se restauran con el proceso de restauración de copias de archivos del lado del host, además de explicar por qué algunos archivos no se pueden restaurar con la opción de restauración rápida. Si especifica el `-verbose` SnapManager muestra una sección de vista previa y una sección de análisis para explicar por qué no se puede restaurar cada archivo mediante el proceso de restauración rápida.

PREVIEW:

The following files will be restored via host side file copy restore:

+DG2/sid/datafile10.dbf  
+DG2/sid/datafile11.dbf

ANALYSIS:

The following reasons prevent certain files from being restored via fast restore:

Reasons:

Newer snapshots of /vol/volume2 have volume clones: SNAP\_1  
\*Newer backups will be freed: nightly2, nightly3

Files to Restore:

/mnt/systemB/volume2/system.dbf  
/mnt/systemB/volume2/users.dbf  
/mnt/systemB/volume2/sysaux.dbf  
/mnt/systemB/volume2/datafile04.dbf  
/mnt/systemB/volume2/datafile05.dbf

The following reasons prevent certain files from being restored via fast restore:

Reasons:

\* Newer snapshots of /vol/adm\_disks will be lost: ADM\_SNAP\_5  
\* Luns present which were created after snapshot SNAP\_0 was created:  
/vol/adm\_disks/disk5.lun  
\* Files not part of the restore scope will be reverted in file system:  
+DG2

Files Not in Restore Scope: +DG2/someothersid/data01.dbf  
+DG2/someothersid/data02.dbf

Files to Restore:

+DG2/sid/datafile08.dbf +DG2/sid/datafile09.dbf  
+DG2/sid/datafile10.dbf +DG2/sid/datafile11.dbf

\* Reasons denoted with an asterisk (\*) are overridable.

2. Revise los motivos por los que no pueden usarse otros procesos de restauración.
3. Inicie la operación de restauración sin `-preview` si sólo se muestran los motivos que se pueden anular.

Aún puede anular comprobaciones no obligatorias.

## Restauración de backups mediante la restauración rápida

Si se cumplen todas las condiciones obligatorias de restauración rápida, puede forzar a SnapManager para SAP que utilice el proceso de SnapRestore basado en volúmenes en lugar de otros procesos de restauración.

## Acerca de esta tarea

Es posible usar el comando `backup restore` con `-fast`:

**`backup restore -fast [require | override | fallback | off]`**

Puede utilizar el `-fast` opción solo si desea realizar una restauración completa de un backup completo. La `-fast` la opción incluye los siguientes parámetros:

- `require`: Permite realizar una restauración de volumen si se cumplen todas las condiciones de elegibilidad de restauración obligatorias y no se encuentran comprobaciones que puedan realizarse.

Si especifica el `-fast` opción, pero no se debe especificar ningún parámetro para `-fast`, SnapManager utiliza la `-require` parámetro como valor predeterminado.

- `override`: Permite anular las comprobaciones de elegibilidad no obligatorias y realizar la restauración rápida basada en volumen.
- `fallback`: Permite restaurar la base de datos utilizando cualquier método que SnapManager determine.

Si no especifica `-fast`, SnapManager utiliza la `-fallback` parámetro como el predeterminado.

- `off`: Le permite evitar el tiempo necesario para realizar todas las comprobaciones de elegibilidad, para realizar un proceso de restauración basado en archivos en lugar del proceso de restauración rápida.

Si la copia de seguridad no supera las comprobaciones de elegibilidad obligatorias, la restauración rápida no se puede completar correctamente.

SnapManager realiza restauraciones rápidas basadas en volúmenes únicamente en entornos basados en UNIX; SnapManager no realiza restauraciones rápidas en el entorno Windows.

Al realizar VBSR en la copia de seguridad del archivo de datos, si los archivos de datos y los archivos de registro de archivos están presentes en el mismo volumen y si los archivos de registro de archivos no están presentes en el sistema de archivos activo, la restauración y recuperación de la base de datos se realiza correctamente. Sin embargo, las futuras snapshots de registros de archivos se eliminan como parte de VBSR. Esto provoca una entrada obsoleta del backup de registros de archivos en el repositorio.

## Pasos

1. Introduzca el siguiente comando:

```
smsap backup restore -profile profile_name -label label -complete-fast  
require-verbose
```

### ejemplo

```
smsap backup restore -profile targetdbl_prof1  
-label full_bkup_sales_nov_08 -complete -fast require -verbose
```

2. Revisar las comprobaciones de cumplimiento de la restauración rápida.
3. Si la comprobación de elegibilidad determina que no se han producido errores en las comprobaciones obligatorias, si se pueden anular ciertas condiciones y si desea continuar con el proceso de restauración, escriba el siguiente comando:



**backup restore -fast override**

## Restaurar backups mediante Single File SnapRestore

Para restaurar los backups, se puede utilizar el método Single File SnapRestore (SFSR).

### Pasos

1. Cree un perfil desde la interfaz gráfica de usuario (GUI) de SnapManager.
2. Realice una copia de seguridad de la base de datos mediante la GUI.
3. Desenlazar los grupos de servicios de Oracle y Network File System (NFS) de los grupos de servicios de cluster y congelarlos.
4. Asegúrese de que Secure Shell (SSH) esté configurado entre los hosts y SnapDrive para UNIX mediante la configuración `#secure-communication-among-cluster-nodes` para **on** en la `snapdrive.conf` archivo.
5. Desde la interfaz gráfica de usuario de SnapManager, puede realizar una restauración y recuperación de backup completa mediante `--alllogs`.
6. Descongele los grupos de servicios y vincúlelos al grupo de servicios del clúster.



Esta configuración sólo se aplica cuando se utiliza SnapDrive 4.1.1 D2 para UNIX y SnapDrive 4.2 para UNIX.

Si una operación de restauración es seguida de otra, existe la posibilidad de que se produzca un error en la creación de la copia de Snapshot de backup. Si se ejecutan operaciones de restauración sucesivas en el periodo especificado en el que se puede completar SFSR, SnapManager para SAP encontrará errores de creación de copias Snapshot.

Para evitar errores de creación de copias de Snapshot, asegúrese de que se realicen operaciones de restauración después del periodo durante el cual se SFSR en curso.

Para ello, compruebe el estado del proceso de división de clones de la LUN. Para ello, introduzca el siguiente comando desde la interfaz de línea de comandos (CLI) del sistema de almacenamiento:

```
rsh filername lun clone split status lun-name
```

Sample Output:

```
/vol/delaware_760gb/lun700gb (64% complete)..
```



El SnapRestore basado en volúmenes (VBSR) no es compatible con los hosts Solaris que ejecutan Veritas stack con entornos SFRAC y VCS.

## Restaura backups en el almacenamiento principal

Puede utilizar el `backup restore` comando para restaurar un backup de base de datos en el almacenamiento primario.

### Acerca de esta tarea

SnapManager intenta realizar una restauración rápida basada en volúmenes de forma predeterminada y proporciona información de comprobación de elegibilidad. Si es necesario, puede anular algunas comprobaciones de elegibilidad. Si está seguro de que no se puede realizar una copia de seguridad mediante una restauración rápida, puede deshabilitar la verificación de elegibilidad rápida para la restauración y realizar una restauración basada en archivos.

Puede utilizar el `backup restore` Opciones del comando para especificar si SnapManager debe restaurar todo el backup o parte de él. SnapManager también permite restaurar archivos de control junto con los archivos de datos o los espacios de tablas desde los backups en una sola operación de usuario. Puede incluir `-controlfiles` con `-complete` para restaurar los ficheros de control, así como los espacios de tablas y los ficheros de datos.

Se pueden seleccionar una de las siguientes opciones para restaurar el backup:

Si desea restaurar...	Usar...
Todo el backup con todos los espacios de tablas y ficheros de datos	<code>-complete</code>
Lista de tablespaces específicos	<code>-tablespaces</code>
Archivos de datos específicos	<code>-files</code>
Solo los archivos de control	<code>-controlfiles</code>
Espacios de tabla, archivos de datos y archivos de control	<code>-complete -controlfiles</code>

También puede restaurar el backup desde una ubicación alternativa si especifica `-restorespec`.

Si incluye `-recover`, puede recuperar la base de datos en:

- La última transacción que se produjo en la base de datos (todos los registros)
- Una fecha y hora específicas
- Un número de cambio de sistema (SCN) específico
- La hora del backup (sin registros)
- Solo restauración



Tanto la recuperación de fecha y hora como la recuperación de SCN son recuperaciones puntuales.

SnapManager (3.2 o posterior) permite recuperar los backups de la base de datos restaurada automáticamente mediante los archivos de registro de archivos. Incluso si los archivos de registro de archivos están disponibles en la ubicación externa, si se especifica el `-recover-from-location` option, SnapManager utiliza los archivos de registro de archivo de la ubicación externa para recuperar las copias de seguridad de la base de datos restauradas.

SnapManager proporciona la ubicación externa a Oracle. Sin embargo, Oracle no identifica los archivos desde el destino externo. Este comportamiento se aprecia en el destino de área de recuperación de flash. Se trata de

problemas con Oracle y la solución alternativa es tener siempre una copia de seguridad de los archivos de registro de archivos en dichos diseños de bases de datos.

Si se proporciona un SCN o fecha incoherentes, la recuperación se detendrá en el último punto consistente recuperado con el mensaje de error `Recovery succeeded, but insufficient`. Es necesario realizar manualmente la recuperación a un estado consistente.

Para la recuperación cuando no se aplican registros, SnapManager se recupera hasta el último SCN del último archivo de registro de archivos creado durante el backup. Si la base de datos es coherente hasta este SCN, la base de datos se abrirá correctamente. Si la base de datos no es coherente en este momento, SnapManager sigue intentando abrir la base de datos, que se abrirá correctamente si la base de datos ya es coherente.



SnapManager no admite la recuperación de los backups de solo registro de archivos.

Si la separación de registros de archivos en un punto de montaje NFS no es un almacenamiento compatible con Snapshot, SnapManager permite recuperar los backups de la base de datos restaurada mediante el perfil. Antes de ejecutar operaciones de SnapManager en un almacenamiento no compatible con Snapshot, debe añadir los destinos de `archivedLogs.exclude pulg smsap.config`.

Debe asegurarse de establecer el parámetro `Exclude` antes de crear un perfil. Sólo después de establecer el parámetro `exclude` en el archivo de configuración de SnapManager, la creación de perfiles se realiza correctamente.

Si el backup ya está montado, SnapManager no monta el backup de nuevo y utiliza el backup ya montado. Si la copia de seguridad está montada por un usuario diferente y si el usuario actual no tiene acceso a la copia de seguridad previamente montada, otros usuarios tienen que proporcionar los permisos. Todos los archivos de registro de archivos tienen permisos de lectura para los propietarios de los grupos; es posible que el usuario actual no obtenga los permisos, si el backup está montado por otro grupo de usuarios. Los usuarios pueden proporcionar permisos a los archivos de registro de archivos montados manualmente y, a continuación, volver a intentar la restauración o recuperación.

#### Recuperar backups de una base de datos en un entorno RAC

Durante la recuperación de los backups de la base de datos en un entorno RAC, cuando no se encuentra el archivo de registro de archivo necesario, Oracle solicita archivos de registro de archivo y cambia entre diferentes subprocesos y número de cambio en la base de datos RAC. SnapManager para SAP intenta recuperar la base de datos como un esfuerzo. La recuperación correcta de los backups de base de datos en el entorno RAC depende de la disponibilidad de los archivos de registro de archivos en los backups.

El mecanismo de recuperación recomendado para la base de datos RAC es el siguiente:

- Asegúrese de que todos los archivos de registro de archivos estén disponibles en los backups o que todos los archivos de registro de archivos estén disponibles en el único destino de registro de archivos externo.
- Si se proporcionan varios destinos de registros de archivos externos, puede proporcionar solapamiento de los archivos de registro de archivos al tiempo que especifica los destinos de registros de archivos externos para todos los subprocesos.

Por ejemplo, la ubicación del archivo de registro externo: Puedo tener entre 1 y 100 archivos de registro de archivo, la ubicación del archivo de registro externo - II puede tener entre 98 y 200 archivos de registro de archivo y la ubicación del archivo de registro externo - III puede tener entre 198 y 300 archivos de registro de archivo.

- Al eliminar los archivos de registro de archivos, en lugar de eliminar todos los archivos de registro de

archivos, es posible eliminar los archivos de registro de archivos hasta SCN o fecha para que los backups puedan tener los mismos archivos de registro de archivos.

Es posible especificar la opción `-dump` como un parámetro opcional para recoger los archivos de volcado después de la operación de restauración correcta o con errores.

## Pasos

1. Introduzca el siguiente comando:

```
smsap backup restore -profile profile_name -label label -complete-recover  
-alllogs [-recover-from-location path [,path2]]-dump-verbose
```

### ejemplo

```
smsap backup restore -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -  
complete -recover -alllogs -verbose
```

2. Para restaurar datos en diferentes situaciones, complete una de las siguientes acciones:

Si desea restaurar...	Ejemplo de comando
Complete Database sin archivos de control y recupere un número SCN en particular (3794392). En este caso, existen los archivos de control actuales, pero todos los archivos de datos están dañados o perdidos. Restaure y recupere la base de datos de una copia de seguridad en línea completa existente a un punto inmediatamente anterior a ese SCN.	<pre>smsap backup restore -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -complete -recover -until 3794392 -verbose</pre>
Completar la base de datos sin archivos de control y recuperar hasta una fecha y hora.	<pre>smsap backup restore -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -complete -recover -until 2008-09-15:15:29:23 -verbose</pre>

Si desea restaurar...	Ejemplo de comando
<p>Completar la base de datos sin archivos de control y recuperar hasta datos y tiempo. En este caso, existen los archivos de control actuales, pero todos los archivos de datos están dañados o se pierden o se produjo un error lógico después de un momento específico. Restaure y recupere la base de datos de una copia de seguridad en línea completa existente a una fecha y hora inmediatamente antes del punto de fallo.</p>	<pre>smsap backup restore -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -complete -recover -until "2008-09-15:15:29:23" -verbose</pre>
<p>Base de datos parcial (uno o más archivos de datos) sin archivos de control y recuperación mediante todos los registros disponibles. En este caso, existen los archivos de control actuales, pero uno o más archivos de datos están dañados o perdidos. Restaure esos archivos de datos y recupere la base de datos de una copia de seguridad en línea completa existente utilizando todos los registros disponibles.</p>	<pre>smsap backup restore -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -files /oracle/FLA/sapdata1/sr3_1/sr3.data1 /oracle/FLA/sapdata1/sr3_2/sr3.data2 /oracle/FLA/sapdata1/sr3_3/sr3.data3 -recover -alllogs -verbose (where "FLA" is the &lt;SID&gt;</pre>
<p>Base de datos parcial (uno o más tablespaces) sin archivos de control y recuperación mediante todos los registros disponibles. En este caso, existen los archivos de control actuales, pero se pierden uno o más tablespaces o se pierde uno de los más archivos de datos pertenecientes al tablespace. Restaure esos tablespaces y recupere la base de datos a partir de una copia de seguridad en línea completa existente utilizando todos los registros disponibles.</p>	<pre>smsap backup restore -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -tablespaces users -recover -alllogs -verbose</pre>

Si desea restaurar...	Ejemplo de comando
<p>Sólo archivos de control y recuperación mediante todos los registros disponibles. En este caso, los archivos de datos existen, pero todos los archivos de control están dañados o perdidos. Restaure sólo los archivos de control y recupere la base de datos de una copia de seguridad en línea completa existente utilizando todos los registros disponibles.</p>	<pre>smsap backup restore -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -controlfiles -recover -alllogs -verbose</pre>
<p>Complete la base de datos sin archivos de control y recupérese usando los archivos de control de copia de seguridad y todos los registros disponibles. En este caso, todos los archivos de datos están dañados o perdidos. Restaure sólo los archivos de control y recupere la base de datos de una copia de seguridad en línea completa existente utilizando todos los registros disponibles.</p>	<pre>smsap backup restore -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -complete -using -backup-controlfile -recover -alllogs -verbose</pre>
<p>Recupere la base de datos restaurada utilizando los archivos archive log de la ubicación externa del archive log.</p>	<pre>smsap backup restore -profile targetdb1_prof1 -label full_bkup_sales_nov_08 -complete -using -backup-controlfile -recover -alllogs -recover-from -location /user1/archive -verbose</pre>

3. Revisar las comprobaciones de cumplimiento de la restauración rápida.

#### ejemplo

Introduzca el siguiente comando:

```
smsap backup restore -profile targetdb1_prof1 -label full_bkup_sales_nov_08
-complete -recover -alllogs -recover-from-location /user1/archive -verbose
```

4. Si la comprobación de elegibilidad muestra que no se han producido errores en las comprobaciones obligatorias y si se pueden anular ciertas condiciones y si desea continuar con el proceso de restauración, introduzca lo siguiente:

```
backup restore -fast override
```

5. Especifique las ubicaciones de los registros de archivos externos mediante el `-recover-from -location` opción.

## Restaurar los archivos de una ubicación alternativa

SnapManager le permite restaurar archivos de datos y archivos de control desde una ubicación distinta a la de las copias Snapshot del volumen original.

La ubicación original es la ubicación del archivo en el sistema de archivos activo en el momento de la copia de seguridad. La ubicación alternativa es la ubicación desde la cual se restaurará un archivo.

Puede restaurar los siguientes datos desde una ubicación alternativa:

- Los archivos de datos de un sistema de archivos intermedio a un sistema de archivos activo
- Bloques de datos de un dispositivo RAW intermedio en un dispositivo RAW activo

SnapManager automatiza la recuperación. Al recuperar archivos de ubicaciones externas, SnapManager utiliza `recovery automatic from location` comando.

SnapManager también usa Oracle Recovery Manager (RMAN) para recuperar archivos. Oracle debe reconocer los archivos que se van a recuperar. Los nombres de archivo deben tener el formato predeterminado. Al recuperarse del área de recuperación de flash, SnapManager ofrece la ruta traducida a Oracle. Sin embargo, Oracle no se recupera del área de recuperación de flash porque no puede generar el nombre de archivo correcto. Lo ideal es que el área de recuperación de flash sea un destino diseñado para trabajar con RMAN.

## Restaurar backups desde una ubicación alternativa

Para restaurar una copia de seguridad de la base de datos desde una ubicación alternativa, utilice los siguientes pasos principales, cada uno de los cuales se describe más adelante en esta sección.

- Realice una de las siguientes acciones, según la distribución de la base de datos y qué debe restaurarse:
  - Restaurar los archivos de datos necesarios desde cinta, SnapVault, SnapMirror o cualquier otro medio en cualquier sistema de archivos montado en el host de la base de datos.
  - Restaurar el sistema de archivos requerido y montarlo en el host de la base de datos.
  - Conéctese a los dispositivos RAW necesarios que existen en el host local.
- Cree un archivo XML (Lenguaje de marcado extensible) de especificación de restauración que incluya las asignaciones que SnapManager necesita para restaurar desde la ubicación alternativa a la ubicación original. Guarde el archivo en una ubicación a la que SnapManager pueda acceder.
- Utilice SnapManager para restaurar y recuperar los datos con el archivo XML de especificación de restauración.

### Restauración de los datos de los archivos

Antes de restaurar desde una ubicación alternativa, debe restaurar los archivos necesarios desde cualquier medio de almacenamiento y restaurar los archivos de aplicaciones como SnapVault o SnapMirror a un sistema de archivos montado en el host local.

Es posible utilizar la restauración desde una operación de ubicación alternativa para copiar los archivos de un sistema de archivos alternativo a un sistema de archivos activo.

Debe especificar las ubicaciones alternativas desde las que desea restaurar los archivos originales mediante la creación de una especificación de restauración.

### Restauración de datos desde el sistema de ficheros

Antes de restaurar datos desde una ubicación alternativa, debe restaurar el sistema de archivos necesario y montarlo en el host local.

Se puede invocar la operación de restauración desde una ubicación alternativa para copiar los archivos de sistemas de archivos alternativos a sistemas de archivos activos.

Para realizar esta operación, debe especificar los puntos de montaje alternativos desde los que se restaurarán los puntos de montaje originales y los nombres de las copias Snapshot originales creando un archivo de especificación de restauración.



El nombre de copia Snapshot es un componente necesario porque el mismo sistema de archivos puede ajustarse varias veces en una única operación de backup (por ejemplo, una vez para los archivos de datos y otra para el archivo de registro).

### Restauración de los datos desde dispositivos sin configurar

Antes de restaurar desde una ubicación alternativa, debe conectarse a los dispositivos sin formato necesarios que existan en el host local.

Puede invocar la restauración desde una operación de ubicación alternativa para copiar los bloques de datos de dispositivos sin formato alternativos a dispositivos sin formato activos. Para realizar esta operación, debe especificar el dispositivo RAW alternativo desde el que restaurar el dispositivo RAW original creando una especificación de restauración.

### Cree especificaciones de restauración

El archivo de especificación de restauración es un archivo XML que contiene las ubicaciones originales y alternativas desde las que se puede restaurar el archivo. SnapManager utiliza este archivo de especificación para restaurar los archivos desde la ubicación especificada.

### Acerca de esta tarea

Puede crear el archivo de especificación de restauración usando cualquier editor de texto. Se debe usar la extensión .xml del archivo.

### Pasos

1. Abra un archivo de texto.
2. Introduzca lo siguiente:

```
<restore-specification xmlns="http://www.netapp.com">
```

3. Introduzca cualquier información de asignación de archivos con el formato que se muestra en el ejemplo siguiente:



```
<file-mapping>
  <original-location>/path/dbfilename.dbf</original-location>
  <alternate-location>/path/dbfilename1.dbf</alternate-location>
</file-mapping>
```

La asignación de archivos especifica desde dónde se restaura un archivo. La ubicación original es la ubicación del archivo en el sistema de archivos activo en el momento de la copia de seguridad. La ubicación alternativa es la ubicación desde la que se restaura el archivo.

4. Introduzca cualquier información de asignación del sistema de archivos montado con el formato que se muestra en el ejemplo:

```
<mountpoint-mapping>
  <original-location>/path/db_name</original-location>
  <snapname>snapname</snapname>
  <alternate-location>/path/vaultlocation</alternate-location>
</mountpoint-mapping>
<mountpoint-mapping>
  <original-location>+DiskGroup_1</original-location>
  <snapname>snapname</snapname>
  <alternate-location>+DiskGroup_2</alternate-location>
</mountpoint-mapping>
```

Mountpoint hace referencia a la ruta del directorio `/mnt/myfs/`). La asignación de punto de montaje especifica el punto de montaje desde el que se restauran los archivos. La ubicación original es la ubicación del punto de montaje en el sistema de archivos activo en el momento de la copia de seguridad. La ubicación alternativa es el punto de montaje desde el que se restauran los archivos de la ubicación original. La *snapname* Es el nombre de la copia Snapshot en la que se hizo copia de seguridad de los archivos originales.



El nombre de copia Snapshot es un componente necesario porque el mismo sistema de archivos se puede usar varias veces en una única operación de backup (por ejemplo, una vez para los archivos de datos y una vez para los registros).

5. Introduzca las etiquetas y ubicaciones de asignación de dispositivos sin procesar con el formato que se muestra en el ejemplo:

```
<raw-device-mapping>
  <original-location>/path/raw_device_name</original-location>
  <alternate-location>/path/raw_device_name</alternate-location>
</raw-device-mapping>
```

La asignación de dispositivos sin formato especifica la ubicación desde la que se restaura un dispositivo sin formato.

6. Introduzca lo siguiente:

**</restore-specification>**

7. Guarde el archivo como un archivo .xml y cierre la especificación.

### Restaurar ejemplo de especificación

En el ejemplo siguiente se muestra la estructura de especificación de restauración:

```
<?xml version="1.0" encoding="UTF-8"?>
<restore-specification xmlns="http://www.netapp.com">
<!-- "Restore from file(s)" -->
  <file-mapping>
    <original-location>/mnt/pathname/dbname/users01.dbf</original-
location>
    <alternate-location>/mnt/vault/users01.dbf</alternate-location>
  </file-mapping>
<!-- "Restore from host mounted file system(s)" -->
  <mountpoint-mapping>
    <original-location>/mnt/pathname/dbname/fs</original-location>
    <snapname>Snapshotname</snapname>
    <alternate-location>/mnt/vaultlocation</alternate-location>
  </mountpoint-mapping>
<!-- "Restore from raw device" -->
  <raw-device-mapping>
    <original-location>/pathname/devicename</original-location>
    <alternate-location>/pathname/devicename</alternate-location>
  </raw-device-mapping>
</restore-specification>
```

### Restaurar backups desde una ubicación alternativa

Es posible restaurar backups desde una ubicación alternativa para restaurar los archivos de datos desde un sistema de archivos intermedio a un sistema de archivos activo, o bien restaurar los bloques de datos desde un dispositivo sin formato intermedio en un dispositivo sin formato activo.

#### Lo que necesitará

- Cree un archivo XML de especificación de restauración y especifique el tipo de método de restauración que desea utilizar.

#### Acerca de esta tarea

Puede usar `smsap backup restore` Y especifique el archivo XML de especificación de restauración que creó para restaurar el backup desde una ubicación alternativa.

1. Introduzca el siguiente comando:

```
smsap backup restore -profile profile -label label -complete -alllogs  
-restorespec restorespec
```

## Clonar el backup de bases de datos

Si clona una base de datos, puede realizar tareas como probar una actualización a una base de datos sin afectar a la base de datos en producción, duplicar una instalación maestra a varios sistemas de entrenamiento o duplicar una instalación maestra como instalación básica a otros servidores, que tienen requisitos similares.

Puede ejecutar las siguientes tareas relacionadas con la clonado:

- Clonar una base de datos a partir de un backup existente.
- Clonar una base de datos en su estado actual, lo que permite crear el backup y el clon en un procedimiento.
- Clone un backup protegido en el almacenamiento secundario o incluso terciario.
- Clone una base de datos y utilice scripts de plugins personalizados, que se ejecutan antes o después de la operación de clonado.
- Clone una base de datos en el mismo host en el que reside la base de datos.
- Clone una base de datos con los archivos de registro de archivos desde la ubicación del registro de archivos externo.
- Clonar una base de datos en un host alternativo.
- Clonar una base de datos RAC.
- Consulte una lista de clones.
- Ver información detallada sobre clones.
- Eliminar clones.

## Qué es la clonación

Puede clonar una base de datos para crear una réplica exacta de la base de datos original. Es posible crear el clon a partir de un backup completo o desde el estado actual de la base de datos.

A continuación se presentan algunas de las ventajas de crear un clon con SnapManager:

Ventajas	Detalles
Velocidad	La operación de clonación de SnapManager usa la función FlexClone disponible con Data ONTAP. Esto permite clonar rápidamente grandes volúmenes de datos.
Gestión eficiente del espacio	Cuando crea un clon con SnapManager, solo se necesita espacio para los cambios entre el backup y el clon. Un clon SnapManager es una copia Snapshot editable de la base de datos original y puede crecer según sea necesario. Por el contrario, un clon físico de la base de datos requiere que disponga de espacio suficiente para copiar la base de datos completa.

Ventajas	Detalles
Copia virtual	Puede utilizar la base de datos clonada como si fuera la base de datos original. Por ejemplo, puede usar un clon para pruebas, comprobaciones de plataformas y actualizaciones, simulaciones múltiples aplicadas a un conjunto de datos de gran tamaño, y pruebas y almacenamiento provisional en oficinas remotas. Los cambios en el clon no afectan a la base de datos original. Una vez clonada la base, la base de datos clonada queda totalmente operativa.
Sencillez	Es posible clonar una base de datos a cualquier host con los comandos de SnapManager.

Es posible clonar un backup en el almacenamiento primario (local) o un backup protegido que está en el almacenamiento secundario (remoto). Sin embargo, no es posible clonar un backup si la operación de backup está en curso o si el backup se transfirió al almacenamiento secundario.

Para poder clonar una base de datos, debe asegurarse de que se cumplen los siguientes requisitos previos:

- Asegúrese de que el [/etc|/var/opt/oracle]/oratab el directorio no contiene una entrada que apunte al identificador del sistema de destino.
- Elimine el `spfile<SID>.ora` archivo desde `$ORACLE_HOME/dbs`.
- Elimine el `init<SID>.ora` archivo desde `$ORACLE_HOME/dbs`.
- Elimine los destinos de volcado de Oracle que estén especificados en el archivo de especificación del clon.
- Elimine los archivos de control de Oracle que estén especificados en el archivo de especificación del clon.
- Elimine los archivos de registro de recuperación de Oracle especificados en el archivo de especificación del clon.

Debe proporcionar al clon un nuevo identificador del sistema. No se pueden ejecutar simultáneamente dos bases de datos con el mismo identificador de sistema en el mismo host. Es posible tener un clon en otro host con el mismo identificador de sistema. Es posible asignar al clon una etiqueta o dejar que SnapManager cree una etiqueta con el identificador del sistema, la fecha y la hora en que se creó el clon.

Cuando introduce una etiqueta, no debe incluir espacios ni caracteres especiales.

Como parte del proceso de clonado, SnapManager crea los parámetros y archivos de Oracle necesarios para la base de datos clonada. Un ejemplo de un archivo Oracle necesario es `init<SID>.ora`.

Al clonar una base de datos, SnapManager crea un nuevo `init<SID>.ora` archivo de la base de datos en la `$ORACLE_HOME/dbs` directorio.

Puede clonar una base de datos de Real Application Cluster (RAC) y una base de datos no cluster. Un clon de RAC se inicia como una sola base de datos.

Es posible clonar un backup de base de datos en el host en el que reside la base de datos o en un host alternativo.

Si la base de datos clonada utilizaba un `spfile`, SnapManager crea un `spfile` para el clon. Coloca este archivo en el `$ORACLE_HOME/dbs` directorio y crea la estructura de directorios para los archivos de diagnóstico. El nombre de archivo es `spfile <SID>.ora`.

## Métodos de clonación

Es posible clonar una base de datos mediante uno de estos dos métodos. El método que elija afecta al `clone create` funcionamiento.

En la siguiente tabla se describen los métodos de clonado y su efecto en el `clone create` funcionamiento y su `-reserve` opción. Una LUN se puede clonar mediante cualquiera de los dos métodos.

Método de clonación	Descripción	<code>clone create -reserve</code>
Clonado de LUN	Se crea un nuevo LUN clon en el mismo volumen.	Cuando <code>-reserve</code> Para una LUN está configurada en <code>yes</code> , Se reserva espacio para el tamaño completo de LUN en el volumen.
Clonado de volúmenes	Se crea un nuevo FlexClone y la LUN clonada existe dentro del nuevo volumen clonado. Utiliza la tecnología FlexClone.	Cuando <code>-reserve</code> para un volumen se establece en <code>yes</code> , se reserva espacio para el tamaño de volumen completo dentro del agregado.

## Cree especificaciones de clon

SnapManager para SAP utiliza un archivo XML de especificación del clon, que incluye las asignaciones, las opciones y los parámetros que se deben utilizar en la operación de clonado. SnapManager utiliza esta información para determinar dónde colocar los archivos que clona y cómo tratar información de diagnóstico, archivos de control, parámetros, etc.

### Acerca de esta tarea

Es posible crear el archivo de especificación del clon con la interfaz gráfica de usuario (GUI) de SnapManager, la interfaz de línea de comandos (CLI) o un editor de texto.

Cuando crea el archivo de especificación del clon con un editor de texto, debe guardarlo como un `.xml` archivo. Es posible usar este archivo XML para otras operaciones de clonado.

También puede crear una plantilla de especificación de clon y personalizarla. Puede utilizar el `smsap clone template O` en la interfaz gráfica de usuario, utilice el asistente Clone.

SnapManager para SAP agrega una cadena de versión a cualquier plantilla de especificación de clon que genere. SnapManager para SAP asume la versión más reciente de cualquier archivo de especificación del clon que no tenga una cadena de versión.

Si desea realizar la clonado remota, no cambie las ubicaciones predeterminadas de los archivos de datos, los archivos de registro de recuperación y los archivos de control en el archivo de especificación del clon. Si cambia la ubicación predeterminada, SnapManager no puede crear el clon o crear el clon en una base de datos que no es compatible con la funcionalidad de Snapshot. Por lo tanto, la creación automática de perfil falla.



Aunque la información del punto de montaje y del grupo de discos de ASM se puede editar desde la interfaz gráfica de usuario, solo se puede cambiar el nombre del archivo y no las ubicaciones del archivo.

Puede ejecutar una tarea varias veces, ya sea con combinaciones de parámetros y valores iguales o diferentes.

SAP utiliza ajustes de Oracle específicos para la configuración de bases de datos. Puede encontrar estos ajustes en `init<SID>.ora` situado en `$ORACLE_HOME/dbs`. Debe incluirlas en la especificación del clon.

## Pasos

1. Abra un archivo de texto e introduzca texto como se muestra en el ejemplo siguiente:

### ejemplo

```
<clone-specification xmlns="http://www.example.com">
  <storage-specification/>
  <database-specification/>
</clone-specification>
```

2. En el componente de especificación de almacenamiento, introduzca los puntos de montaje para los archivos de datos.

La especificación de almacenamiento enumera las ubicaciones para el nuevo almacenamiento creado para el clon, como puntos de montaje de archivos de datos y dispositivos sin formato. Estos elementos se deben asignar del origen al destino.

En el siguiente ejemplo se muestra un solo punto de montaje NFS en un almacenamiento conectado mediante NFS:

### ejemplo

```
<mountpoint>
  <source>/oracle/<SOURCE SID>_sapdata</source>
  <destination>/oracle/<TARGET SID>_sapdata</destination>
</mountpoint>
```

3. **Opcional:** Si tiene un dispositivo RAW en la fuente, debe especificar la ruta del dispositivo RAW en la fuente y, a continuación, especificarlo

**destination auto-generate="true"**

para el destino.

A diferencia del archivo de asignación de clones de versiones anteriores de SnapManager para SAP, no se puede especificar una ubicación para el dispositivo sin configurar en el destino. SnapManager para SAP selecciona el siguiente nombre de dispositivo disponible para el dispositivo RAW clonado.

### ejemplo

En el ejemplo siguiente se muestra la sintaxis de dispositivo sin configurar que se utiliza en la especificación del clon:

```
<raw-device>
  <source>/dev/raw/raw1</source>
  <destination auto-generate="true"/>
</raw-device>
```

4. En el componente de especificación de la base de datos, identifique la información del archivo de control como una lista de los archivos de control que desea crear para el clon.

La especificación de la base de datos especifica las opciones de la base de datos para el clon, como los archivos de control, los registros de recuperación, los registros de archivos y los parámetros de Oracle.

### **ejemplo**

En el ejemplo siguiente se muestra la sintaxis del archivo de control que se utiliza en la especificación del clon:

```
<controlfiles>
  <file>/oracle/<TARGET SID>/origlogA/cntrl/cntrl<TARGET
SID>.dbf</file>
  <file>/oracle/<TARGET SID>/origlogB/cntrl/cntrl<TARGET
SID>.dbf</file>
  <file>/oracle/<TARGET SID>/sapdata1/cntrl/cntrl<TARGET
SID>.dbf</file>
</controlfiles>
```

5. Especifique la estructura del registro de recuperación para el clon.

### **ejemplo**

En el ejemplo siguiente se muestra la estructura de directorio redo log para la clonado:

```

<redologs>
  <redogroup>
    <file>/oracle/<TARGET SID>/origlogA/log_g11m1.dbf</file>
    <file>/oracle/<TARGET SID>/mirrlogA/log_g11m2.dbf</file>
    <number>1</number>
    <size unit="M">100</size>
  </redogroup>
  <redogroup>
    <file>/oracle/<TARGET SID>/origlogB/log_g12m1.dbf</file>
    <file>/oracle/<TARGET SID>/mirrlogB/log_g12m2.dbf</file>
    <number>2</number>
    <size unit="M">100</size>
  </redogroup>
  <redogroup>
    <file>/oracle/<TARGET SID>/origlogA/log_g13m1.dbf</file>
    <file>/oracle/<TARGET SID>/mirrlogA/log_g13m2.dbf</file>
    <number>3</number>
    <size unit="M">100</size>
  </redogroup>
  <redogroup>
    <file>/oracle/<TARGET SID>/origlogB/log_g14m1.dbf</file>
    <file>/oracle/<TARGET SID>/mirrlogB/log_g14m2.dbf</file>
    <number>4</number>
    <size unit="M">100</size>
  </redogroup>
</redologs>

```

6. Especifique los parámetros de Oracle que deben establecerse con diferentes valores en la base de datos clonada. Si utiliza Oracle 10, debe especificar los siguientes parámetros:

- Volcado en segundo plano
- Volcado de memoria
- Volcado de usuario
- **Opcional:** Archivos de registro



Si los valores de los parámetros no están configurados correctamente, la operación de clonado se detiene y se recibe un mensaje de error.

Si no especifica la ubicación donde se almacenan los registros de archivos, SnapManager crea el clon en noarchive log modo. SnapManager copia esta información del parámetro en la `init.ora` archivo del clon.

### ejemplo

En el ejemplo siguiente se muestra la sintaxis de los parámetros que se utiliza en la especificación del clon:



```

<parameters>
  <parameter>
    <name>log_archive_dest</name>
    <value>LOCATION=>/oracle/<TARGET SID>/oraarch</value>
  </parameter>
  <parameter>
    <name>background_dump_dest</name>
    <value>/oracle/<TARGET SID>/saptrace/background</value>
  </parameter>
  <parameter>
    <name>core_dump_dest</name>
    <value>/oracle/<TARGET SID>/saptrace/background</value>
  </parameter>
  <parameter>
    <name>user_dump_dest</name>
    <value>/oracle/<TARGET SID>/saptrace/usertrace</value>
  </parameter>
</parameters>

```

### ejemplo

Puede utilizar un valor predeterminado mediante un elemento default dentro del elemento Parameter. En el siguiente ejemplo, la `os_authentication_prefix` el parámetro tomará el valor predeterminado porque se especifica el elemento predeterminado:

```

<parameters>
  <parameter>
    <name>os_authent_prefix</name>
    <default></default>
  </parameter>
</parameters>

```

### ejemplo

Puede especificar una cadena vacía como valor de un parámetro mediante un elemento vacío. En el siguiente ejemplo, la `os_authentication_prefix` se establecerá en una cadena vacía:

```

<parameters>
  <parameter>
    <name>os_authent_prefix</name>
    <value></value>
  </parameter>
</parameters>

```



Puede utilizar el valor de la base de datos de origen `init.ora` archivo para el parámetro no especificando ningún elemento.

### ejemplo

Si un parámetro tiene varios valores, puede proporcionar los valores de los parámetros separados por comas. Por ejemplo, si desea mover los archivos de datos de una ubicación a otra, puede utilizar la `db_file_name_convert` y especifique las rutas de los archivos de datos separadas por comas, tal como se muestra en el siguiente ejemplo:

### ejemplo

Si desea mover los archivos de registro de una ubicación a otra, a continuación puede utilizar `log_file_name_convert` defina y especifique las rutas de acceso del archivo de registro separadas por comas, tal como se muestra en el ejemplo:

1. **Opcional:** especifique sentencias SQL arbitrarias que se ejecutarán en el clon cuando esté en línea.

Puede utilizar las sentencias SQL para realizar tareas como la recreación de la `temp files` en la base de datos clonada.



Debe asegurarse de que no se incluya un punto y coma al final de la instrucción SQL.

A continuación se muestra una sentencia SQL de muestra que se ejecuta como parte de la operación de clonado:

```
<sql-statements>
  <sql-statement>
    ALTER TABLESPACE TEMP ADD
    TEMPFILE '/mnt/path/clonename/temp_user01.dbf'
    SIZE 41943040 REUSE AUTOEXTEND ON NEXT 655360
    MAXSIZE 32767M
  </sql-statement>
</sql-statements>
```

### Ejemplo de especificación de clon

En el ejemplo siguiente se muestra la estructura de especificaciones del clon, incluidos los componentes de especificación de base de datos y almacenamiento:

```
<clone-specification xmlns="http://www.example.com">
  <storage-specification>
    <storage-mapping>
      <mountpoint>
        <source>/oracle/<SOURCE SID>_sapdata</source>
        <destination>/oracle/<TARGET SID>_sapdata</destination>
      </mountpoint>
    </storage-mapping>
  </storage-specification>
</clone-specification>
```

```

<raw-device>
  <source>/dev/raw/raw1</source>
  <destination auto-generate="true"/>
</raw-device>
<raw-device>
  <source>/dev/raw/raw2</source>
  <destination auto-generate="true"/>
</raw-device>
</storage-mapping>
</storage-specification>

<database-specification>
  <controlfiles>
    <file>/oracle/<TARGET SID>/origlogA/cntrl/cntrl<TARGET
SID>.dbf</file>
    <file>/oracle/<TARGET SID>/origlogB/cntrl/cntrl<TARGET
SID>.dbf</file>
    <file>/oracle/<TARGET SID>/sapdata1/cntrl/cntrl<TARGET
SID>.dbf</file>
  </controlfiles>

  <redologs>
    <redogroup>
      <file>/oracle/<TARGET SID>/origlogA/log_g11m1.dbf</file>
      <file>/oracle/<TARGET SID>/mirrlogA/log_g11m2.dbf</file>
      <number>1</number>
      <size unit="M">100</size>
    </redogroup>
    <redogroup>
      <file>/oracle/<TARGET SID>/origlogB/log_g12m1.dbf</file>
      <file>/oracle/<TARGET SID>/mirrlogB/log_g12m2.dbf</file>
      <number>2</number>
      <size unit="M">100</size>
    </redogroup>
    <redogroup>
      <file>/oracle/<TARGET SID>/origlogA/log_g13m1.dbf</file>
      <file>/oracle/<TARGET SID>/mirrlogA/log_g13m2.dbf</file>
      <number>3</number>
      <size unit="M">100</size>
    </redogroup>
    <redogroup>
      <file>/oracle/<TARGET SID>/origlogB/log_g14m1.dbf</file>
      <file>/oracle/<TARGET SID>/mirrlogB/log_g14m2.dbf</file>
      <number>4</number>
      <size unit="M">100</size>
    </redogroup>
  </redologs>

```

```

</redologs>

<parameters>
  <parameter>
    <name>log_archive_dest</name>
    <value>LOCATION= >/oracle/<TARGET SID>/oraarch</value>
  </parameter>
  <parameter>
    <name>background_dump_dest</name>
    <value>/oracle/<TARGET SID>/saptrace/background</value>
  </parameter>
  <parameter>
    <name>core_dump_dest</name>
    <value>/oracle/<TARGET SID>/saptrace/background</value>
  </parameter>
  <parameter>
    <name>user_dump_dest</name>
    <value>/oracle/<TARGET SID>/saptrace/usertrace</value>
  </parameter>
</parameters>
</database-specification>
</clone-specification>

```

## Clonar bases de datos y usar scripts de plugins personalizados

SnapManager proporciona un método para usar scripts personalizados antes y después de que se produzca una operación de clonado. Por ejemplo, podría haber creado un script personalizado que valida un SID de base de datos de clon y garantiza que el SID lo permita la política de nomenclatura. Mediante el plugin de clonado de SnapManager, puede incluir scripts personalizados y hacerlos ejecutar automáticamente antes o después de una operación de clonado de SnapManager.

### Pasos

1. Ver scripts de plugins de muestra.
2. Cree una secuencia de comandos desde cero o modifique una de las secuencias de comandos del plug-in de ejemplo.

Cree su script personalizado de acuerdo con las directrices de script del plugin de SnapManager.

3. Coloque la secuencia de comandos personalizada en una ubicación de directorio especificada.
4. Actualice el archivo XML de especificación del clon e incluya información sobre el script personalizado que debe utilizarse durante el proceso de clonado.
5. Mediante un comando de SnapManager, compruebe que los scripts personalizados estén operativos.

6. Cuando inicia la operación de clonado, incluya el nombre de script y los parámetros opcionales.

## Clonar bases de datos a partir de backups

Es posible clonar una base de datos a partir de un backup con la `clone create` comando.

### Acerca de esta tarea

Primero debe crear un archivo de especificación del clon para la base de datos. SnapManager crea el clon según la información de este archivo de especificación.

Después de clonar una base de datos, es posible que desee actualizar el `tnsnames.ora` archivos en los equipos cliente con la nueva información de conexión de base de datos clonada. La `tnsnames.ora` Los archivos se utilizan para conectarse a una instancia de Oracle sin tener que especificar la información completa de la base de datos. SnapManager no actualiza el `tnsnames.ora` archivos.

SnapManager siempre crea un backup, incluidos los archivos de registro de archivos, si se utiliza el perfil creado con `-include-with-online-backups`. SnapManager permite clonar únicamente los backups completos de la base de datos.

SnapManager (3.2 o posterior) permite clonar los backups que contienen los archivos de datos y los archivos de registro de archivos.

Si el registro de archivos está disponible desde una ubicación externa, puede especificar la ubicación externa durante la clonado para recuperar la base de datos clonada en un estado coherente. Debe asegurarse de que Oracle pueda acceder a la ubicación externa. No se admite la clonado de backups de solo registro de archivos.

Aunque se crea el backup de registros de archivos junto con el backup parcial en línea, no se puede crear un clon de la base de datos con este backup.

Es posible clonar el backup de base de datos desde la ubicación de archivo de registro de archivos externo solo para una base de datos independiente.

Se produce un error en la clonado del backup de la base de datos en línea de la base de datos de Real Application Clusters (RAC) mediante la ubicación del archivo de registro de archivos externo debido a un fallo en la recuperación. Esto se debe a que la base de datos de Oracle no puede encontrar y aplicar los archivos de registro de archivos para la recuperación desde la ubicación del registro de archivos externo al clonar el backup de la base de datos.

Puede especificar el `-dump` opción como parámetro opcional para recoger los archivos de volcado después de la operación de creación de clones con errores o realizados correctamente.

### Clonación de copia de seguridad de archivo de datos sin copia de seguridad de archivo de registro

Cuando el backup de archivos de datos no incluye el backup de registro de archivos, SnapManager para SAP clona la base de datos según el número de cambio del sistema (SCN) registrado durante el backup. Si no es posible recuperar la base de datos clonada, el `Archived log file for thread <number> and change <SCN> required to complete recovery` Se muestra un mensaje de error, aunque SnapManager para SAP sigue clonando la base de datos y, por último, se produce correctamente la creación del clon.

Al clonar con el backup de archivos de datos sin incluir el backup de registros de archivos, SnapManager

recupera la base de datos clonada hasta el último SCN de registro de archivos, que se registra durante el backup.

### Pasos

1. Cree un archivo de especificación del clon.
2. Para crear un clon, introduzca el siguiente comando:

```
smsap clone create-backup-label backup_name -newsid new_sid -label clone_label  
-profile profile_name -clonespec full_path_to_clonespecfile [-taskspec  
taskspec] [-recover-from-location] path1 [,<path2>...] [-dump]
```

## Clonar bases de datos en el estado actual

Puede crear un backup y un clon de la base de datos desde el estado actual de la base de datos mediante un solo comando.

### Acerca de esta tarea

Cuando especifique el perfil con el `-current` Opción, SnapManager primero crea un backup y, a continuación, un clon del estado actual de la base de datos.

En la configuración de perfil, si habilitó el backup de archivos de datos y registros de archivos juntos para la clonación, siempre que se realice un backup de los archivos de datos en línea, también se realizará un backup de los registros de archivos. Al clonar la base de datos, SnapManager crea el backup de archivos de datos junto con el backup del registro de archivos y crea el clon de la base de datos. Si no se incluye el backup de registros de archivos, SnapManager no crea el backup de registros de archivos y, por lo tanto, no puede crear el clon de la base de datos.

### Paso

1. Para clonar la base de datos en su estado actual, introduzca el comando siguiente:

```
smsap clone create -profile profile_name -current -label clone_name -clonespec  
./clonespec_filename.xml
```

Este comando realiza un backup completo automático (generando la etiqueta de backup) e inmediatamente crea un clon a partir de ese backup mediante una especificación de clon existente que desea utilizar.



Puede especificar el `-dump` opción como parámetro opcional para recoger los archivos de volcado después de las operaciones realizadas correctamente o con errores. El volcado se recoge tanto para las operaciones de backup como de clonado.

## Clonar backups de bases de datos sin reasentar registros

SnapManager le permite realizar clonados flexibles, de modo que puede recuperar la base de datos clonada manualmente en un momento determinado sin necesidad de abrir la base de datos mediante reaslogs. También puede configurar manualmente la base de datos clonada como una base de datos en espera de Data Guard.

### Acerca de esta tarea

Cuando pueda seleccionar la `-no-resetlogs` Opción al crear el clon, SnapManager realiza las siguientes actividades para crear la base de datos clonada:

1. Ejecuta la actividad de tarea de preprocesamiento, si se especifica, antes de iniciar la operación de clonado
2. Crea la base de datos clonada con el SID especificado por el usuario
3. Ejecuta las sentencias SQL emitidas con la base de datos clonada.

Sólo se ejecutan correctamente las sentencias SQL que se pueden ejecutar en estado de montaje.

4. Ejecuta la actividad de la tarea de posprocesamiento, si se especifica.

### Qué tareas debe realizar para recuperar la base de datos clonada manualmente

1. Monte los backups de registros de archivos y recupere la base de datos clonada manualmente mediante los archivos de registro de archivos desde la ruta montada.
2. Después de realizar la recuperación manual, abra la base de datos clonada recuperada con `-resetlogs` opción.
3. Cree espacios de tablas temporales, si es necesario.
4. Ejecute la utilidad DBNEWID.
5. Conceda un privilegio sysdba a las credenciales de la base de datos clonada.

Al clonar los backups de la base de datos con la `-no-resetlogs` SnapManager deja la base de datos clonada en el estado montado para la recuperación manual.



La base de datos clonada creada con la `-no-resetlogs` la opción no es una base de datos completa. Por lo tanto, no debe ejecutar ninguna operación de SnapManager en esta base de datos, si bien SnapManager no le restringe la posibilidad de realizar ninguna operación.

Si no especifica el `-no-resetlogs` SnapManager aplica los archivos de registro de archivo y abre la base de datos con `reaslogs`.

### Paso

1. Introduzca el siguiente comando:

```
smsap clone create -profile profile_name [-backup-label backup_name | -backup  
-id backup_id | current] -newsid new_sid -clonespec full_path_to_clonespecfile  
-no-resetlogs
```

Si intenta especificar ambas `-no-resetlogs` y `recover-from-location` Options, SnapManager no permite especificar ambas opciones juntas y muestra el mensaje de error: SMSAP-04084: You must specify either one of the options: `-no-resetlogs` or `-recover-from-location`.

### Ejemplo

```
smsap clone create -profile product -backup-label full_offline -newsid  
PROD_CLONE -clonespec prod_clonespec.xml -label prod_clone-reserve -no  
-reset-logs
```

## Consideraciones para clonar una base de datos en un host alternativo

Para poder clonar en un host distinto al que reside la base de datos, deben cumplirse algunos requisitos.

En la siguiente tabla se muestran los requisitos de configuración del host de origen y de destino:

Requisitos previos de configuración	Requisito
Arquitectura	Debe ser igual en los hosts de origen y objetivo
Sistema operativo y versión	Debe ser igual en los hosts de origen y objetivo
SnapManager para SAP	Se debe instalar y ejecutar en los hosts de origen y objetivo
Credenciales	Se debe configurar para que el usuario acceda al host de destino
Oracle	Se debe instalar la misma versión de software en los hosts de origen y destino.  Oracle Listener debe ejecutarse en el host de destino.
Pila de almacenamiento compatible	Debe ser igual en los hosts de origen y objetivo
Protocolo utilizado para acceder a los archivos de datos	Debe ser igual en los hosts de origen y objetivo
Gestores de volúmenes	Debe configurarse en los hosts de origen y destino y debe tener versiones compatibles

### Clonar una base de datos en un host alternativo

Puede utilizar el `clone create` comando para clonar un backup de base de datos en un host alternativo.

#### Lo que necesitará

- Cree un perfil o tenga un perfil existente.
- Crear una copia de seguridad completa o tener una copia de seguridad de la base de datos existente.



- Cree una especificación de clon o tenga una especificación de clon existente.

### Paso

1. Para clonar una base de datos en un host alternativo, introduzca el siguiente comando:

```
smsap clone create -backup-label backup_label_name -newsid new_sid -host  
target_host -label clone_label -comment comment_text -profile profile_name  
-clonespec full_path_to_clonespecfile
```

Oracle no permite ejecutar dos bases de datos con el mismo SID simultáneamente en el mismo host. Por este motivo, debe suministrar un SID nuevo para cada clon. Sin embargo, puede tener una base de datos en otro host con el mismo SID.

## Consulte una lista de clones

Puede ver una lista de clones asociados con un perfil determinado.

### Acerca de esta tarea

La lista incluye la siguiente información sobre los clones de un perfil:

- El ID del clon
- Estado de la operación de clonado
- SID de Oracle para el clon
- Host donde reside el clon
- Etiqueta del clon

Si especifica el `-verbose` opción, el resultado también muestra los comentarios introducidos para el clon.

### Paso

1. Para mostrar una lista de todos los clones de un perfil, introduzca el siguiente comando

```
smsap clone list -profile profile_name [-quiet | -verbose]
```

## Ver información detallada sobre clones

Puede ver información detallada sobre un clon específico mediante el `clone show` comando.

### Acerca de esta tarea

La `clone show` comando muestra la siguiente información:

- Identificador del sistema del clon e ID del clon
- Estado de la operación de clonado
- Clonar crear fecha y hora de inicio y finalización
- Etiqueta del clon
- Clonar comentario

- Etiqueta e ID de copia de seguridad
- Base de datos de origen
- Hora de inicio y de finalización de la copia de seguridad
- Nombre de la base de datos, tablespaces y archivos de datos
- El nombre del host y los sistemas de archivos que contienen archivos de datos
- Los volúmenes del sistema de almacenamiento y las copias Snapshot respaldan el clon
- Si el clon se creó con el backup en el almacenamiento primario o secundario

### Paso

1. Introduzca el siguiente comando:

```
smsap clone show -profile profile_name [-label label | -id guid]
```

## Eliminar clones

Puede eliminar los clones cuando el tamaño de la copia Snapshot alcance entre un 10% y un 20% del backup. Así también se garantiza que el clon tenga los datos más recientes.

### Acerca de esta tarea

La etiqueta es el identificador único de cada clon en un perfil. Puede usar la etiqueta o el ID del clon, pero no el identificador del sistema (SID) para eliminar el clon.



El SID del clon y la etiqueta del clon no son iguales.

Cuando elimina un clon, la base de datos debe estar en ejecución. De lo contrario, no se eliminarán muchos ficheros y directorios del clon existente, lo que hará que se realice más trabajo antes de crear otro clon.

Los directorios especificados para ciertos parámetros de Oracle del clon se destruyen cuando se elimina el clon y solo deben contener datos para la base de datos clonada: Destinos de registro de archivo, destinos de fondo, núcleo y destinos de volcado de usuario. No se eliminan los archivos de auditoría.



No es posible eliminar un clon cuando se utiliza en otras operaciones.

Opcionalmente, es posible recoger los archivos de volcado después de una operación de eliminación de clonado correcta o con errores.

### Paso

1. Introduzca el siguiente comando:

```
smsap clone delete -profile profile_name [-label label | -id guid] [-sypassword sypassword] | [login-username db_username -password] db_password -port db_port] [-asminstance- asmusername asm_username -asmpassword asm_password] [-force] [-dump] [-quiet] | [-verbose]
```

## Ejemplo

```
smsap clone delete -profile targetdbl_prof1 -label sales0908_clone1
```

## Dividir un clon

SnapManager le permite dividir y gestionar un clon existente creado mediante la tecnología FlexClone. En la tecnología FlexClone, el clon y la base de datos original comparten los mismos bloques de datos físicos.

Antes de ejecutar la operación de división de clones, puede saber que el tamaño estimado del clon se dividirá y el espacio requerido disponible en el agregado.

SnapManager genera un nuevo perfil si la operación de división de clones se realiza correctamente. Si SnapManager no puede crear el nuevo perfil, puede crear manualmente un nuevo perfil. Puede utilizar el nuevo perfil para crear backups de bases de datos, restaurar datos y crear clones. Si la operación de división de clones se realiza correctamente, independientemente de si se crea el perfil nuevo o no, los metadatos relacionados con la clonación se eliminan de la base de datos del repositorio.

Puede realizar las siguientes tareas relacionadas con la división de clones:

- Ver la estimación de división de clones.
- Divida un clon en un almacenamiento primario.
- Divida un clon en un almacenamiento secundario.
- Ver el estado de la operación de división de clones.
- Detenga la operación de división de clones.
- Destruir el perfil junto con el almacenamiento subyacente.
- Elimine el perfil creado para un clon dividido.

Cuando divide un clon de su volumen principal, se eliminan las copias Snapshot asociadas con el volumen clonado. No se pueden utilizar los backups creados para la base de datos clonada antes del proceso de división de clones porque las copias de Snapshot de estos backups se eliminan y los backups permanecen como entradas obsoletas en el repositorio.

## Ver una estimación de división de clones

La estimación de división de clones ayuda a conocer el espacio libre total disponible en el agregado, la cantidad de espacio compartido entre el clon y la base de datos original, y el espacio utilizado exclusivamente por el clon. Además, puede ver la fecha y la hora en que se creó el clon subyacente y la antigüedad del clon. Según esta estimación, usted decide si dividir un clon o no.

## Acerca de esta tarea

Para ver la estimación de división de clones, debe introducir el nombre del perfil del clon original y la etiqueta o GUID de la operación de clonación. Si el clon está en otro host, es posible especificar el nombre de host.

## Paso

1. Para ver la estimación de división de clones, introduzca el siguiente comando:

```
smsap clone split-estimate -profile profile [-host hostname] [-label clone-label | -id clone-id] [-quiet | -verbose]
```

En el siguiente ejemplo, se muestra el comando para la estimación de almacenamiento de división de clones:

```
smsap clone split-estimate  
-profile p1 -label clone_test_label
```

## Divida un clon en el almacenamiento primario o secundario

Puede utilizar el `clone split` comando para dividir el clon. Una vez finalizada la división de clones, los metadatos del clon se eliminan de la base de datos del repositorio y es posible eliminar o liberar el backup asociado con el clon.

### Acerca de esta tarea

El nuevo perfil creado después de la operación de división correcta se utiliza para gestionar el clon de división. El nuevo perfil será como cualquier otro perfil existente en SnapManager. Este perfil se puede usar para llevar a cabo operaciones de backup, restauración y clonado.

Además, también es posible configurar las notificaciones por correo electrónico para el nuevo perfil. Esto permite al administrador de la base de datos recibir notificaciones sobre el estado de la operación de la base de datos realizada mediante el perfil.



SnapManager admite la operación de separación cuando se realiza únicamente en FlexClone.

Si la operación de división falla, se muestra un mensaje de error adecuado con el motivo del fallo. El estado de varias operaciones también se muestra en el registro de operaciones. Por ejemplo:

```
--[ INFO] The following operations were completed:  
Clone Split : Success  
Profile Create : Failed  
Clone Detach : Success
```

Opcionalmente, es posible recoger los archivos de volcado después de una operación de división de clones realizada correctamente o con errores.



Después de introducir el `clone split` No debe detener el servidor SnapManager hasta que se haya iniciado la operación de división de clones.



SnapManager genera el perfil aunque no proporcione ningún valor para la cuenta de Oracle (osaccount y osgroup).

## Paso

1. Introduzca el siguiente comando:

```
smsap clone split -profile clone-profile -host hostname [-label clone-label |  
-id clone-id]-split-label split-operation-label -comment comment new-profile  
new-profile-name [-profile-password new-profile_password] -repository -dbname  
repo_service_name -host repo_host -port repo_port -login-username  
repo_username -database -dbname db_dbname -host db_host [-siddb_sid] [-login-  
username db_username -password db_password -port db_port] [-rman {-controlfile  
| {-login-username rman_username -password rman_password -tnsname  
rman_tnsname} } ] -osaccount osaccount -osgroup osgroup [-retain [-hourly-  
count n] [-duration m]] [-daily-count n] [-duration m]] [-weekly-count n] [-  
duration m]] [-monthly-count n] [-duration m]]] [-profile-comment profile-  
comment][-snapname-pattern pattern][-protect [-protection-policy policy_name]]  
| [-noprotect]][-summary-notification] [-notification [-success-email  
email_address1, email_address2 -subject subject_pattern] [-failure-email  
email_address1, email_address2 -subject subject_pattern]][-quiet | -verbose]  
-dump
```

## Consulte el estado del proceso de división de clones

Puede ver el progreso del proceso de división iniciado.

## Paso

1. Para ver el progreso del proceso de división de clones, introduzca el siguiente comando:

```
smsap clone split-status -profile profile [-host hostname] [-label split-label  
| -id split-id] [-quiet | -verbose]
```

```
smsap clone split-status -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

## Vea el resultado del proceso de división de clones

Es posible ver el resultado del proceso de división de clones iniciado.

## Paso

1. Para ver el resultado del proceso de división de clones, introduzca el siguiente comando:

```
smsap clone split-result -profile profile [-host hostname] [-label split-label  
| -id split-id] [-quiet | -verbose]
```

```
smsap clone split-result -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

## Detenga el proceso de división de clones

Es posible detener el proceso de división de clones en ejecución.

### Acerca de esta tarea

Después de detener el proceso de división, no podrá reanudarlo.

### Paso

1. Para detener la operación de división de clones, introduzca el siguiente comando:

```
smsap clone split-stop -profile profile [-host hostname] [-label split-label |  
-id split-id] [-quiet | -verbose]
```

```
smsap clone split-stop -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

## Eliminar un perfil

Es posible eliminar un perfil siempre que no contenga backups correctos que se estén utilizando actualmente en otras operaciones. Es posible eliminar perfiles que contengan copias de seguridad liberadas o eliminadas.

1. Introduzca el siguiente comando: `smsap profile delete -profile profile [-quiet | -verbose]`

Es posible eliminar un nuevo perfil creado para la división de clones. Mientras se elimina, Si elimina el perfil, no puede destruir el perfil más tarde se muestra el mensaje de advertencia en la interfaz de línea de comandos de SnapManager.

```
smsap profile delete -profile AUTO-REVEN
```

## Destruir un perfil

SnapManager permite destruir el perfil asociado con el clon dividido (base de datos) junto con el almacenamiento subyacente. Antes de destruir el perfil, asegúrese de eliminar los backups y clones asociados.

### Paso

1. Para destruir un perfil creado con la operación de división de clones y la base de datos de división de clones, introduzca el siguiente comando:

```
smsap profile destroy -profileprofile [-host hostname] [-quiet | -verbose]
```

```
smsap profile destroy -profile AUTO-REVEN
```

## Elimine un ciclo de operaciones de división de clones de una base de datos del repositorio

Puede eliminar una entrada de ciclo de operaciones de división de clones desde una base de datos de repositorio.

### Paso

1. Para eliminar una entrada de ciclo de operaciones de división de clones desde una base de datos de repositorio, introduzca el siguiente comando:

```
smsap clone split-delete -profile profile [-host hostname] [-label split-label  
| -id split-id] [-quiet | -verbose]
```

```
smsap clone split-delete -profile p1 -id 8abc01ec0e78f3e2010e78f3fdd00001
```

## Introducción a la protección de datos en SnapManager

SnapManager admite protección de datos para proteger los backups en sistemas de almacenamiento secundarios o terciarios. Debe configurar las relaciones de SnapMirror y SnapVault entre los volúmenes de origen y de destino.

Si se utiliza Data ONTAP en 7-Mode, SnapManager ofrece protección de datos condicionada por políticas al integrarse con Protection Manager (OnCommand Unified Manager). De este modo se automatiza la replicación de backups de SnapManager en un sistema de almacenamiento principal a un sistema de almacenamiento secundario o incluso a un sistema de almacenamiento terciario gracias a las políticas de SnapVault o SnapMirror creadas por el administrador de almacenamiento o backup en Protection Manager. La retención en el almacenamiento principal es controlada por SnapManager según la retención definida durante la creación de perfiles y la clase de retención etiquetada durante la creación de backups. La retención de los backups de almacenamiento secundario es controlada por la política definida en Protection Manager.

Si utiliza Clustered Data ONTAP, SnapManager 3.4 proporciona políticas de *SnapManager\_CDOT\_Mirror* y *SnapManager\_CDOT\_Vault* para la protección de datos. Al crear un perfil, puede seleccionar estas políticas en función de la relación de SnapMirror o SnapVault que se haya establecido mediante la CLI de Clustered Data ONTAP o System Manager. Cuando se crea un backup, en el que se selecciona el perfil para el cual se

habilita la protección, los backups se protegen en un sistema de almacenamiento secundario.



Los backups creados con BR\*Tools no se pueden proteger con SnapManager para SAP.

Si utilizaba SnapManager 3.3.1 con Clustered Data ONTAP, los backups estaban protegidos usando secuencias de comandos posteriores que se seleccionaron al crear perfiles. Si desea utilizar esos perfiles, después de actualizar a SnapManager 3.4, debe realizar las siguientes operaciones.

- Debe actualizar los perfiles para seleccionar la política *SnapManager\_CDOT\_Mirror* o *SnapManager\_CDOT\_Vault* y eliminar el script posterior que se utilizó para la protección de datos.
- Después de actualizar el perfil para utilizar la política *SnapManager\_CDOT\_Vault*, debe eliminar las programaciones de backup existentes y crear nuevas programaciones para especificar la etiqueta de SnapVault para los backups.
- Si los perfiles se crearon en SnapManager 3.3.1 sin seleccionar los scripts posteriores, debe actualizar los perfiles para seleccionar la política *SnapManager\_CDOT\_Mirror* o *SnapManager\_CDOT\_Vault* para habilitar la protección de datos.



Si tiene backups en el sistema de almacenamiento secundario que fueron reflejados o en almacén con scripts posteriores de SnapManager 3.3.1, no podrá utilizar dichos backups para restaurar o clonar con SnapManager 3.4.

Si utiliza Clustered Data ONTAP, SnapManager 3.4.2 admite varias relaciones de protección (SnapMirror y SnapVault) en los volúmenes de origen. Solo se admiten una relación de SnapMirror y una relación de SnapVault por volumen. Debe crear perfiles independientes, cada uno con el *SnapManager\_cDOT\_Mirror* y la *SnapManager\_cDOT\_Vault* política seleccionada.



SnapDrive para Unix 5.3.2 y posterior es necesario para usar múltiples políticas de protección.

## ¿Qué son las políticas de protección

Las políticas de protección son reglas que rigen el modo en que se protegen los backups de la base de datos. Puede seleccionar las políticas de protección mientras crea el perfil.

Una política de protección define los siguientes parámetros:

- El momento de transferir copias a un almacenamiento secundario
- La cantidad máxima de datos que se deben transferir a las horas programadas
- El tiempo de retención de las copias de cada ubicación de respaldo
- Umbrales de advertencia y error para tiempos de retraso

Cuando la protección está habilitada, SnapManager crea un conjunto de datos para la base de datos. Un conjunto de datos consta de una colección de conjuntos de almacenamiento junto con la información de configuración asociada con sus datos. Los conjuntos de almacenamiento asociados a un conjunto de datos incluyen un conjunto de almacenamiento principal utilizado para exportar datos a clientes y el conjunto de réplicas y archivos que existen en otros conjuntos de almacenamiento. Los conjuntos de datos representan datos de usuario exportables. Si el administrador deshabilita la protección de una base de datos, SnapManager elimina el conjunto de datos.



## Qué estados de protección son

SnapManager muestra el estado de cada backup. Los administradores deben conocer los distintos estados y supervisar el estado de sus backups.

Un backup de la base de datos puede tener los siguientes estados de protección:

Estado	Definición	Explicación
Protegido	Se solicitó protección y se ha activado.	La protección está habilitada para el backup en SnapManager y Protection Manager copió correctamente el backup en otro conjunto de discos físicos (también denominado almacenamiento secundario). Si Protection Manager quita un backup del almacenamiento secundario debido a una política de retención, puede que el backup regrese a un estado no protegido.
Sin proteger	Se solicitó protección, pero no se completó.	La protección se habilita para el backup, pero el backup no se copia en otro conjunto de discos físicos. El backup aún no está protegido o falló la protección, o estaba protegido antes, pero ya no está protegido. Cuando se crea un backup, el estado de protección inicial del backup no se solicita o no está protegido. Si el backup no está protegido, se protege al transferirse a un almacenamiento secundario.
No solicitado	No se solicitó protección.	La protección no está habilitada para el backup. Existe una copia lógica de los datos en los mismos discos físicos (también conocidos como backup local). Si el backup no se solicita con la protección, la protección del backup siempre se muestra como no solicitada.

## Qué pools de recursos son

Un pool de recursos es una colección de almacenamiento físico sin usar (como sistemas de almacenamiento o agregados) del cual se pueden aprovisionar volúmenes o LUN nuevos para contener datos. Si asigna un sistema de almacenamiento a un pool de recursos, todos los agregados de ese sistema de almacenamiento se mostrarán disponibles para el aprovisionamiento.

Los administradores de almacenamiento usan la consola de Protection Manager para asignar un conjunto de recursos a las copias de respaldo y de duplicación. La aplicación de aprovisionamiento puede entonces aprovisionar automáticamente volúmenes fuera de los recursos físicos del conjunto de recursos para contener backups y copias de mirroring.

Para perfiles protegidos, SnapManager muestra información sobre un perfil e indica si se ha asignado un conjunto de recursos de almacenamiento a ese perfil. Si no es así, el perfil se considera "no conforme". Tras asignar un pool de recursos de almacenamiento al conjunto de datos del perfil correspondiente, el perfil se considera "conforme".

## Acerca de diferentes políticas de protección

Puede seleccionar diferentes políticas para proteger los backups en los sistemas de almacenamiento secundario o terciario.

Si utiliza Data ONTAP en 7-Mode y SnapManager se integra con Protection Manager, debe seleccionar una de las siguientes políticas de protección al crear el perfil. La consola de gestión de Protection Manager proporciona plantillas para configurar políticas de protección de los conjuntos de datos. Aunque las políticas de protección de recuperación tras desastres se enumeran en la interfaz de usuario de SnapManager, estas políticas no son compatibles.

Política	Descripción
Realice un backup	Mediante SnapVault o SnapMirror, se realiza un backup de un conjunto de datos de forma local y también del almacenamiento principal al secundario.
Realice copias de seguridad y, a continuación, haga mirroring	Se realiza un backup de un conjunto de datos del almacenamiento primario al secundario mediante SnapVault o SnapMirror, y luego se crea mirroring en un partner de SnapMirror.
Únicamente copias Snapshot locales	Un conjunto de datos solo utiliza copias Snapshot locales en el almacenamiento principal.
Replicación	Un conjunto de datos se refleja del almacenamiento primario al secundario mediante SnapMirror.
Mirroring y backup	Mediante SnapMirror, un conjunto de datos se refleja del almacenamiento primario al secundario y, a continuación, se realiza un backup en el almacenamiento secundario mediante SnapVault o SnapMirror.
Espejo y espejo	Un conjunto de datos se refleja del almacenamiento principal al secundario en dos partners de SnapMirror distintos.
Mirror, y, a continuación, backup	Mediante SnapMirror, un conjunto de datos se refleja del almacenamiento principal al secundario y, posteriormente, se realiza un backup del mismo a un almacenamiento terciario mediante SnapVault o SnapMirror.
Haga simetría y, a continuación, haga simetría	Un conjunto de datos se refleja del almacenamiento primario al secundario mediante SnapMirror y, a continuación, se refleja en un partner de SnapMirror adicional.
Sin protección	Un conjunto de datos no tiene copias Snapshot, backups ni protección contra copias reflejadas de ningún tipo.
Solo backup remoto	Mediante SnapVault o SnapMirror, se realiza un backup de los datos en un sistema de almacenamiento de forma remota a un almacenamiento secundario. La aplicación con licencia no realiza backups locales en el almacenamiento primario. Esta política de protección se puede aplicar a sistemas de terceros con Open Systems SnapVault instalado.

Si utiliza Clustered Data ONTAP, debe seleccionar una de las siguientes políticas de protección mientras crea el perfil.

Política	Descripción
SnapManager_CDOT_Mirror	Duplica el backup.
SnapManager_CDOT_Vault	Almacena la copia de seguridad.

## Configuración y habilitación de la protección de datos condicionada por políticas

Debe configurar SnapDrive y DataFabric Manager Server para permitir la protección de datos en el perfil a fin de proteger backups en sistemas de almacenamiento secundario. Puede seleccionar las políticas de protección en la consola de Protection Manager para especificar cómo se protegerán los backups de la base de datos.



Debe asegurarse de que Unified Manager de OnCommand se encuentre instalado en un servidor aparte para habilitar la protección de datos.

### Configure DataFabric Manager Server y SnapDrive cuando el control de acceso basado en roles está habilitado

Cuando se habilita el control de acceso basado en roles (RBAC), debe configurar DataFabric Manager Server para que incluya las funcionalidades de RBAC. También debe registrar al usuario de SnapDrive creado en DataFabric Manager Server y al usuario raíz del sistema de almacenamiento en SnapDrive.

#### Pasos

1. Configure DataFabric Manager Server.
  - a. Para actualizar DataFabric Manager Server para actualizar los cambios realizados directamente en el sistema de almacenamiento mediante la base de datos de destino, introduzca el siguiente comando:

```
dfm host discover storage_system
```

- b. Cree un usuario nuevo en DataFabric Manager Server y defina la contraseña.
- c. Para añadir un usuario del sistema operativo a la lista de administración del servidor de DataFabric Manager, escriba el siguiente comando:

```
dfm user add sd-admin
```

- d. Para crear una función nueva en DataFabric Manager Server, introduzca el siguiente comando:

```
dfm role create sd-admin-role
```

- e. Para agregar la funcionalidad DFM.Core.AccessCheck Global a la función, escriba el siguiente comando:

```
dfm role add sd-admin-role DFM.Core.AccessCheck Global
```

- f. Para añadir `sd-admin-role` para el usuario del sistema operativo, introduzca el siguiente comando:

```
dfm user role set sd-adminsd-admin-role
```

- g. Para crear otra función en DataFabric Manager Server para el usuario raíz de SnapDrive, escriba el siguiente comando:

```
dfm role create sd-protect
```

- h. Para añadir funcionalidades de RBAC al rol creado para el usuario raíz de SnapDrive o el administrador, escriba los siguientes comandos:

```
dfm role add sd-protect SD.Config.Read Global
```

```
dfm role add sd-protect SD.Config.Write Global
```

```
dfm role add sd-protect SD.Config.Delete Global
```

```
dfm role add sd-protect SD.Storage.Read Global
```

```
dfm role add sd-protect DFM.Database.Write Global
```

```
dfm role add sd-protect GlobalDataProtection
```

- a. Para añadir el usuario de oracle de la base de datos de destino a la lista de administradores del servidor DataFabric Manager y asignar el rol `sd-Protect`, introduzca el siguiente comando:

```
dfm user add -r sd-protecttardb_host1\oracle
```

- b. Para añadir el sistema de almacenamiento utilizado por la base de datos de destino en DataFabric Manager Server, escriba el siguiente comando:

```
dfm host set storage_system hostLogin=oracle hostPassword=password
```

- c. Para crear una función nueva en el sistema de almacenamiento utilizado por la base de datos de destino en DataFabric Manager Server, introduzca el siguiente comando:

```
dfm host role create -h storage_system-c "api-,login-" storage-rbac-role
```

- d. Para crear un grupo nuevo en el sistema de almacenamiento y asignar el nuevo rol creado en DataFabric Manager Server, introduzca el siguiente comando:

```
dfm host usergroup create -h storage_system-r storage-rbac-rolestorage-rbac-group
```

- e. Para crear un nuevo usuario en el sistema de almacenamiento y asignar la nueva función y el grupo creado en DataFabric Manager Server, introduzca el siguiente comando:

```
dfm host user create -h storage_system-r storage-rbac-role -p password -g storage-rbac-grouptardb_host1
```

## 2. Configure SnapDrive.

- a. Para registrar las credenciales de `sd-admin` Usuario con SnapDrive, introduzca el comando

siguiente:

```
snapdrive config set -dfm sd-admin dfm_host
```

- b. Para registrar el usuario raíz o el administrador del sistema de almacenamiento en SnapDrive, escriba el siguiente comando:

```
snapdrive config set tar db_host | storage_system
```

### **Configure SnapDrive cuando el control de acceso basado en roles no esté habilitado**

Para habilitar la protección de datos, debe registrar en SnapDrive al usuario raíz o al administrador de DataFabric Manager Server y al usuario raíz del sistema de almacenamiento.

#### **Pasos**

1. Para actualizar DataFabric Manager Server para actualizar los cambios realizados directamente en el sistema de almacenamiento mediante la base de datos de destino, introduzca el siguiente comando:

#### **ejemplo**

```
dfm host discover storage_system
```

2. Para registrar el usuario raíz o el administrador de DataFabric Manager Server en SnapDrive, introduzca el siguiente comando:

#### **ejemplo**

```
snapdrive config set -dfm Administrator dfm_host
```

3. Para registrar el usuario raíz o el administrador del sistema de almacenamiento con SnapDrive, escriba el siguiente comando:

#### **ejemplo**


```
snapdrive config set root storage_system
```

### **Comprender la habilitación o deshabilitación de la protección de datos en el perfil**

Puede habilitar o deshabilitar la protección de datos al crear o actualizar un perfil de base de datos.

Para crear un backup protegido de una base de datos en los recursos de almacenamiento secundario, los administradores de bases de datos y los administradores de almacenamiento realizan las siguientes acciones.

Si desea...	Realice lo siguiente...
Cree o edite un perfil	<p>Para crear o editar un perfil, realice lo siguiente:</p> <ul style="list-style-type: none"> <li>• Habilite la protección de backup en el almacenamiento secundario.</li> <li>• Si utiliza Data ONTAP en 7-Mode y tiene instalado Protection Manager, puede seleccionar las políticas creadas por el administrador de almacenamiento o backup en Protection Manager.</li> </ul> <p>Si utiliza Data ONTAP en 7-Mode y la protección está habilitada, SnapManager crea un conjunto de datos para la base de datos. Un conjunto de datos consta de una colección de conjuntos de almacenamiento junto con la información de configuración asociada con sus datos. Los conjuntos de almacenamiento asociados a un conjunto de datos incluyen un conjunto de almacenamiento principal utilizado para exportar datos a clientes y el conjunto de réplicas y archivos que existen en otros conjuntos de almacenamiento. Los conjuntos de datos representan datos de usuario exportables. Si el administrador deshabilita la protección de una base de datos, SnapManager elimina el conjunto de datos.</p> <ul style="list-style-type: none"> <li>• Si utiliza ONTAP, debe seleccionar la política <i>SnapManager_CDOT_Mirror</i> o <i>SnapManager_CDOT_Vault</i> en función de la relación de SnapMirror o SnapVault creada.</li> </ul> <p>Al deshabilitar la protección de copia de seguridad, se muestra un mensaje de advertencia que indica que el conjunto de datos se eliminará y no será posible restaurar o clonar copias de seguridad para este perfil.</p>
Ver el perfil	<p>Dado que el administrador de almacenamiento aún no ha asignado recursos de almacenamiento para implementar la normativa de protección, el perfil se muestra como no conforme tanto en la interfaz gráfica de usuario de SnapManager como en la <code>profile show</code> resultado del comando.</p>
Asigne recursos de almacenamiento en la consola de gestión de Protection Manager	<p>En Protection Manager Management Console, el administrador de almacenamiento ve el conjunto de datos no protegido y asigna un pool de recursos a cada nodo del conjunto de datos que está asociado con el perfil. A continuación, el administrador de almacenamiento garantiza que los volúmenes secundarios estén aprovisionados y que se inicialicen las relaciones de protección.</p>
Ver el perfil conforme en SnapManager	<p>En SnapManager, el administrador de la base de datos ve que el perfil ha cambiado al estado conforme tanto en la interfaz gráfica de usuario como en la <code>profile show</code> resultado del comando, que indica que se han asignado recursos.</p>

Si desea...	Realice lo siguiente...
Cree el backup	<ul style="list-style-type: none"> <li>• Seleccione Full backup.</li> <li>• Además, seleccione si el backup debe estar protegido y seleccione la clase de retención primaria (por ejemplo, por hora o por día).</li> <li>• Si utiliza Data ONTAP operando en 7-Mode y desea proteger el backup inmediatamente al almacenamiento secundario, anule la programación de protección de Protection Manager, especifique el <code>-protectnow</code> opción.</li> <li>• Si utiliza ONTAP y desea proteger el backup inmediatamente en el almacenamiento secundario, especifique el <code>protect</code> opción.</li> </ul> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>La <code>protectnow</code> La opción no es aplicable en Clustered Data ONTAP.</p> </div>
Vea el backup	El nuevo backup se muestra como programado para la protección, pero no está protegido (en la interfaz SnapManager y en la <code>backup show</code> resultado del comando). El estado de protección se muestra como «"no protegido"».
Consulte la lista de copias de seguridad	Una vez que el administrador de almacenamiento haya verificado que el backup se ha copiado a un sistema de almacenamiento secundario, SnapManager cambia el estado «sin protección» a «protegido».

## Cómo SnapManager retiene los backups en el almacenamiento local

SnapManager permite crear backups que cumplen las políticas de retención, lo cual especifica cuántos backups se deben conservar correctamente en el almacenamiento local. Puede especificar la cantidad de backups correctos que debe conservarse en el perfil de una determinada base de datos.

Es posible crear backups para lo siguiente:

- 10 días de backup diarios en almacenamiento primario
- 2 meses de backups mensuales en almacenamiento primario
- 7 días de backup diarios en almacenamiento secundario
- 4 semanas de backups semanales en el almacenamiento secundario
- 6 meses de backups mensuales en almacenamiento secundario

Para cada perfil de SnapManager, puede cambiar los valores de las siguientes clases de retención no limitadas:

- Cada hora
- Todos los días
- Semanal

- Mensual

SnapManager determina si se debe retener un backup teniendo en cuenta el número de retención (por ejemplo, 15 backups) y la duración de la retención (por ejemplo, 10 días de backups diarios). Un backup caduca cuando su antigüedad supera el período de retención establecido para su clase de retención o la cantidad de backups supera el número de retenciones. Por ejemplo, si el número de backup es 15 (SnapManager ha tomado 15 backups correctos) y se establece el requisito de duración para 10 días de backups diarios, los cinco backups elegibles más antiguos caducan.

Cuando se caduca un backup, SnapManager libera o elimina el backup caducado. SnapManager siempre conserva el último backup realizado.

SnapManager solo cuenta la cantidad de backups realizados correctamente para el número de retención y no considera lo siguiente:

<b>Backups no incluidos en el número de retención</b>	<b>Detalles adicionales</b>
Backups con errores	SnapManager conserva la información sobre backups realizados correctamente y sin errores. Aunque los backups sin éxito requieren solo un espacio mínimo en el repositorio, es posible que desee eliminarlos. Los backups sin éxito permanecen en el repositorio hasta que se eliminan.
Backups designados para retenerse en cuenta de forma ilimitada o con backups para otra clase de retención	SnapManager no elimina los backups designados para que se conserven de forma ilimitada. Además, SnapManager solo considera los backups en la misma clase de retención (por ejemplo, SnapManager sólo considera los backups por horas para el número de retención por horas).
Backups montados desde el almacenamiento local	Cuando se montan las copias Snapshot, también se clonan y por lo que no se consideran aptos para la retención. SnapManager no puede eliminar las copias Snapshot si están clonadas.
Backups que se utilizan para crear un clon en el almacenamiento local	SnapManager conserva todos los backups que se usan para crear clones, pero no los considera para el número de retención de backups.
Backups que se clonan o se montan en un almacenamiento secundario y que utilizan la política de protección de reflejos	Si SnapManager elimina las copias Snapshot para el backup en el recurso de almacenamiento primario y se duplican las copias Snapshot, producirá un error en el próximo backup en el almacenamiento secundario.

Cuando se libera un backup de sus recursos de almacenamiento primario, se destruyen los recursos primarios (copias Snapshot) utilizados por el backup, pero los metadatos de backup siguen estando disponibles. SnapManager no considera los backups liberados en el número de retención de backups.

SnapManager proporciona un recuento de retención y una duración predeterminados para cada clase de retención. Por ejemplo, para el recuento de clases de retención cada hora, SnapManager, de forma



predeterminada, retiene cuatro backups por hora. Puede anular estos valores predeterminados y establecer los valores al crear o actualizar el perfil o cambiar los valores predeterminados para el recuento de retención y la duración en `smsap.config` archivo.

Los backups en el almacenamiento primario se pueden proteger mediante la realización de backups en el almacenamiento secundario. Mientras SnapManager gestiona la retención y la programación de backups en el almacenamiento principal, Protection Manager gestiona la retención y la programación de los backups en el almacenamiento secundario.

Cuando los backups locales caducan en función de su política de retención, se eliminan o se liberan, en función de si están protegidos.

- Si están protegidos, se liberan los backups locales. Sus recursos de almacenamiento o las copias Snapshot se eliminan, pero los backups permanecen en el repositorio de SnapManager y están disponibles para su restauración desde el almacenamiento secundario. No es necesario liberar backups (por ejemplo, con el comando `backup libre`). Los backups se liberan hasta que el backup ya no exista en el almacenamiento secundario y, en ese momento, se elimina el backup.
- Si no están protegidos, los backups locales se eliminan.

En una operación de backup solo de archivado, SnapManager no archiva los archivos de registro de recuperación, a diferencia del proceso de backup de base de datos en línea. Debe agregar una secuencia de comandos de pretarea para archivar los archivos redo log antes de realizar la operación de copia de seguridad de `archivvelog-only`. La secuencia de comandos de pretarea debe ejecutar `alter system switch logfile` comando.

El siguiente ejemplo muestra las acciones que SnapManager realiza en diversos tipos de backups, según una política de retención de backups de tres días (con el número establecido en `retener 3`):

Fecha de la copia de seguridad	Estado	Se han adoptado medidas para la política de retención	Explicación
5/10	Exitoso	Mantenga	Este es el backup exitoso más reciente, por lo que se mantendrá.
5/9	Clonado correcto	Omitir	SnapManager no considera los backups utilizados para la clonado en el número de políticas de retención. Este backup se omite del número de backups realizados correctamente.
5/8	Correcto, montado	Omitir	SnapManager no considera los backups montados en el número de políticas de retención. Este backup se omite del número de backups realizados correctamente.

Fecha de la copia de seguridad	Estado	Se han adoptado medidas para la política de retención	Explicación
5/7	Error	Omitir	Los backups con errores no se cuentan.
5/5	Exitoso	Mantenga	SnapManager mantiene este segundo backup diario de éxito.
5/3	Exitoso	Mantenga	SnapManager mantiene este tercer backup diario de éxito.
5/2	Exitoso	Eliminar	SnapManager cuenta este backup correctamente, pero después de que SnapManager alcanza tres backups diarios correctos, este backup se elimina.

### Información relacionada

["Documentación en el sitio de soporte de NetApp"](#)

## Aspectos que se deben tener en cuenta al realizar la protección de datos

Debe tener en cuenta ciertas consideraciones para realizar la protección de datos.

- Para realizar operaciones de clonado o restauración desde sistemas secundarios, se debe montar el volumen de destino en el espacio de nombres y exportarlo correctamente.
- Debe deshabilitar el parámetro SnapDrive Configuration `check-export-permission-nfs-clone` estableciendo el valor en **off**.

La documentación de SnapDrive para UNIX en el sitio de soporte de NetApp contiene información adicional sobre `check-export-permission-nfs-clone` parámetro.

- Debe configurar la relación de SnapMirror para los volúmenes de almacenamiento secundario solicitados en el sistema de almacenamiento secundario.
- Debe configurar la relación de SnapVault para los qtrees de almacenamiento secundario solicitados en el sistema de almacenamiento secundario para Data ONTAP que funciona en 7-Mode.
- Debe definir una política y reglas para la etiqueta de SnapMirror definida por el usuario si utiliza SnapVault post-script para Clustered Data ONTAP.

La copia posterior de SnapVault es compatible con los volúmenes de Clustered Data ONTAP y los tipos de relación de SnapMirror DP y XDP. La documentación de ONTAP en el sitio de soporte de NetApp contiene información sobre la configuración de SnapMirror y SnapVault.

- En entornos NAS, debe configurar la ruta de datos NAS primaria y secundaria mediante el `snapdrive config set -mgmtpath management_path management_path management_path datapath_path` comando.

Por ejemplo: `snapdrive config set -mgmtpath f3050-197-91 f3050-197-91 f3050-197-91 f3050-220-91`, donde `f3050-197-91` es la ruta de gestión y `f3050-220-91` es la ruta de datos.

["Documentación en el sitio de soporte de NetApp"](#)

## Licencias necesarias para la protección de datos en SnapManager

Debe asegurarse de que las licencias requeridas para la protección de datos estén instaladas y habilitadas en los sistemas de almacenamiento primario y secundario.

Los sistemas de almacenamiento primario reciben las últimas actualizaciones de transacciones para la base de datos Oracle, almacenan los datos y proporcionan protección de copia de seguridad local de la base de datos. El sistema de almacenamiento principal también conserva los archivos de datos de la base de datos, los archivos de registro y los archivos de control. Los sistemas de almacenamiento secundario actúan como almacenamiento remoto para los backups protegidos.

Para la protección de datos, deben instalarse y activarse las siguientes licencias en los sistemas de almacenamiento primario:



Si desea habilitar la protección de datos en los sistemas de almacenamiento secundario, también debe instalar y habilitar estas licencias en los sistemas de almacenamiento secundario.

- Data ONTAP funcionando en 7-Mode (7.3.1 o posterior) o en Clustered Data ONTAP (8.2 o posterior)
- SnapVault (en función de la política de protección)
- SnapRestore
- SnapMirror (en función de la política de protección)
- Se requiere FlexClone para el sistema de archivos de red (NFS) y la clonación.

Además, FlexClone es necesario para la red de área de almacenamiento (SAN) solo si SnapDrive está configurado para utilizar FlexClone en entornos SAN.

- El protocolo adecuado, por ejemplo, NFS, Internet Small Computer System Interface (iSCSI) o Fibre Channel (FC).

SnapVault o SnapMirror deben estar en los sistemas de almacenamiento primario y secundario en función de las políticas de protección utilizadas. Las políticas de protección de backup básicas requieren únicamente SnapVault instalado en los sistemas de soporte. Las políticas que incluyen protección con mirroring requieren la instalación de SnapMirror en los sistemas de soporte. Las políticas de recuperación ante desastres de backup y mirroring requieren la instalación de SnapMirror en los sistemas de soporte.

## Proteja los backups de bases de datos en almacenamiento secundario o terciario

Puede usar SnapManager para proteger las copias de backup en sistemas de almacenamiento secundarios o terciarios.

### Acerca de esta tarea


No es posible proteger de inmediato el backup creado mediante el comando BRBACKUP al almacenamiento secundario después de realizar un backup exitoso en el almacenamiento primario.

**Paso**

1. Introduzca el siguiente comando:

```
smsap backup create -profile profile_name {[-full {-online | -offline | -auto}
[-retain {-hourly | -daily | -weekly | -monthly | -unlimited}] [-verify] | [-
data {[-files files [files]] | [-tablespaces -tablespaces [-tablespaces]] [-
datalabel label] {-online | -offline | -auto} [-retain {-hourly | [-daily |
-weekly | -monthly | -unlimited}] [-verify] | [-archivelogs [-label label] [-
comment comment] [-snapvaultlabel SnapVault_label][-protect | -noprotect |
-protectnow] [-backup-dest path1 [, [path2]]] [-exclude-dest path1 [, path2]]]
[-prunelogs {-all | -untilSCN untilSCN | -until-date yyyy-MM-dd:HH:mm:ss |
-before {-months | -days | -weeks | -hours}} -prune-dest prune_dest1
[, [prune_dest2]] [-taskspec taskspec]} [-dump] [-force] [-quiet | -verbose]
```

Si desea...	Realice lo siguiente...
<b>Cree una copia de seguridad de una base de datos en línea o sin conexión, en lugar de permitir que SnapManager administre si está en línea o sin conexión</b>	Especifique el <code>-offline</code> o <code>-online</code> opción para crear un backup de la base de datos sin conexión o la base de datos en línea. Si utiliza la <code>-offline</code> o <code>-online</code> no puede usar la opción <code>-auto</code> .
<b>Deje que SnapManager gestione la copia de seguridad de una base de datos, independientemente de si está en línea o sin conexión</b>	Especifique el <code>-auto</code> opción. Si utiliza la opción <code>-auto</code> , no puede utilizar la <code>-offline</code> o <code>-online</code> opción.
<b>Agregar un comentario sobre la copia de seguridad</b>	Especifique el <code>-comment</code> opción, seguida de la cadena de descripción.
<ul style="list-style-type: none"> <li>Forzar la base de datos al estado en el que usted ha especificado para realizar una copia de seguridad, independientemente del estado en el que esté actualmente*</li> </ul>	Especifique el <code>-force</code> opción.

Si desea...	Realice lo siguiente...
<b>Verificar la copia de seguridad en el momento de la creación</b>	Especifique el <code>-verify</code> opción.
<b>Crear una copia de seguridad en almacenamiento secundario</b>	<p>Especifique el <code>-protect</code> opción.</p> <ul style="list-style-type: none"> <li>• Si utiliza ONTAP y desea proteger el backup inmediatamente en el almacenamiento secundario, especifique el <code>-protect</code> opción.</li> </ul> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin: 10px 0;">  La <code>-protectnow</code> La opción no es aplicable en Clustered Data ONTAP. </div> <ul style="list-style-type: none"> <li>• Si utiliza Data ONTAP operando en 7-Mode y desea proteger el backup inmediatamente al almacenamiento secundario, anule la programación de protección de Protection Manager, especifique el <code>-protectnow</code> opción.</li> <li>• Para impedir el backup en el almacenamiento secundario, especifique la <code>-noprotect</code> opción. Si utiliza ONTAP y ha seleccionado la política de protección <i>SnapManager_CDOT_Vault</i> durante la creación del perfil, debe especificar el <code>-snapvaultlabel</code> opción. Debe proporcionar la etiqueta de SnapMirror que haya especificado en las reglas de la política de SnapMirror al configurar la relación de SnapVault como valor.</li> </ul>
<b>Especifique los valores de la clase de retención</b>	<p>Especifique el <code>-retain</code> e indique si el backup debe conservarse en función de una de las siguientes clases de retención:</p> <ul style="list-style-type: none"> <li>• <code>-hourly</code></li> <li>• <code>-daily</code></li> <li>• <code>-weekly</code></li> <li>• <code>-monthly</code></li> <li>• <code>-unlimited</code></li> </ul> <p>Si no se especifica la clase de retención, SnapManager utiliza <code>-Hourly</code> de forma predeterminada.</p>

## Ejemplos

El siguiente comando protege una copia de seguridad de la base de datos:

```
smsap backup create -profile PAYDB -protect -retain -daily -full auto
-label full_bkup_sales
```

El siguiente comando protege inmediatamente un backup de la base de datos:

```
smsap backup create -profile PAYDB -protectnow -retain -daily -full auto  
-label full_bkup_sales
```

## Restaurar backups protegidos a partir del almacenamiento secundario

Es posible restaurar backups protegidos desde almacenamiento secundario. No obstante, no puede restaurar backups desde el almacenamiento secundario si el backup también existe en el almacenamiento principal.

### Información general sobre restauraciones de backups protegidos

Puede elegir el método de restauración que desee utilizar para restaurar los datos de backup del almacenamiento secundario al almacenamiento primario.

En la siguiente tabla se explican los diferentes escenarios y métodos que se pueden utilizar para restaurar un backup desde el almacenamiento secundario:

Destino de restauración	Explicación
Directamente al almacenamiento primario	<p>Devuelve los datos desde el sistema de almacenamiento secundario directamente a la ubicación original del sistema de almacenamiento principal a través de la misma red que se utilizó para proteger los datos.</p> <p>SnapManager utiliza el método de almacenamiento directo siempre que es posible. Este método no es posible si los datos están en un sistema de archivos en una red DE área de almacenamiento (SAN) y si se aplica alguna de las siguientes condiciones:</p> <ul style="list-style-type: none"><li>• No se restauran otros archivos que no son de las bases de datos en el mismo sistema de archivos.</li><li>• Se llevaron a cabo copias snapshot de los archivos de control y de datos de un sistema de archivos que se estaba restaurando en momentos diferentes.</li><li>• El número de unidad lógica (LUN) está en un grupo de volúmenes, pero otros LUN en el mismo grupo de volúmenes no se están restaurando.</li></ul>
Directamente al host	<p>Clona los datos en el sistema de almacenamiento secundario y monta los datos clonados en el host. Tras clonar y montar los datos, SnapManager los copia en su ubicación original.</p>

Destino de restauración	Explicación
Indirectamente al almacenamiento o host	<p>Devuelve los datos del sistema de almacenamiento secundario a una nueva ubicación del sistema primario a través de la misma red que se utilizó para proteger los datos y montar el nuevo almacenamiento en el host. Después de devolver y montar los datos, SnapManager los copia en su ubicación original. El método de almacenamiento indirecto puede requerir mucho tiempo para devolver los datos.</p> <p>SnapManager copia primero los datos en un volumen de desecho en el host primario antes de que SnapManager los utilice para restaurar y recuperar la base de datos. El hecho de que los datos reutilizables se eliminen automáticamente depende del protocolo utilizado.</p> <ul style="list-style-type: none"> <li>• Para SAN, SnapManager elimina los datos que se devuelven.</li> <li>• En el caso del almacenamiento conectado a la red (NAS), SnapManager elimina el contenido de los qtrees devueltos, pero no elimina los qtrees mismos. Para eliminar los qtrees, los administradores deben montar el volumen reutilizable y quitar los qtrees mediante el comando UNIX rmdir.</li> </ul>

Si no puede devolver datos directamente al almacenamiento, SnapManager puede devolver los datos directamente al host o indirectamente al almacenamiento o al host. El método depende de la normativa que regule si la organización permite la conexión directamente al almacenamiento secundario o necesita que los datos se copien a través de la red de almacenamiento. Puede administrar esta directiva estableciendo la información de configuración en el archivo `smSAP.config`.

### Restaurar backups desde el almacenamiento secundario

Es posible restaurar backups protegidos desde el almacenamiento secundario y elegir cómo desea volver a copiar los datos en el almacenamiento primario.

#### Acerca de esta tarea

Puede utilizar el `backup restore` con el `-from-secondary` opción de restaurar los datos desde el almacenamiento secundario. Si no especifica el `-from-secondary` Opción, SnapManager restaura los datos desde las copias Snapshot en el almacenamiento primario.

No puede utilizar el `-from-secondary` opción si el backup existe en el almacenamiento primario, es necesario liberar el backup primario antes de que pueda restaurarse desde el almacenamiento secundario. Si se utiliza un volumen temporal, se debe especificar el volumen con el `-temp-volume` opción.

Debe especificar el `-copy-id` siempre que especifique la `-from-secondary` opción. Si existe más de un backup en el sistema de almacenamiento secundario, el `-copy-id` la opción se utiliza para especificar qué copia de backup del almacenamiento secundario debe usarse en la operación de restauración.



Si utiliza Data ONTAP operando en 7-Mode, debe especificar un valor válido para `-copy-id` opción. Sin embargo, si utiliza Clustered Data ONTAP, el `-copy-id` la opción no es necesaria.

Cuando se restauran datos desde un almacenamiento secundario, SnapManager intenta primero restaurar los datos directamente desde el sistema de almacenamiento secundario al sistema de almacenamiento primario (sin involucrar al host). Si SnapManager no puede realizar este tipo de restauración (por ejemplo, si los archivos no forman parte del sistema de archivos), SnapManager recuperará una restauración de copia de

archivos del lado del host. SnapManager tiene dos métodos para realizar una restauración de copia de archivos en el lado del host desde el almacenamiento secundario. El método que selecciona SnapManager se configura en la `smsap.config` archivo.

- Si `restore.secondaryAccessPolicy = direct`, SnapManager clona los datos en el almacenamiento secundario, monta los datos clonados del sistema de almacenamiento secundario en el host y, a continuación, copia los datos del clon en el entorno activo.

Esta es la directiva de acceso secundaria predeterminada.

- Si `restore.secondaryAccessPolicy = indirect`, SnapManager copia primero los datos a un volumen temporal en el almacenamiento primario, monta los datos del volumen temporal en el host y, a continuación, copia los datos del volumen temporal en el entorno activo.

Esta política se debe utilizar solo si el host no tiene acceso directo al sistema de almacenamiento secundario. Las restauraciones mediante el método indirecto demorarán el doble de tiempo que el método directo porque se crean dos copias de los datos.

## Paso

1. Ejecute una de las siguientes acciones:

Si desea...	Realice lo siguiente...
Restaura una base de datos completa si el backup seleccionado existe en el almacenamiento principal	Introduzca el siguiente comando:  <pre>smsap backup restore -profile profile_name -label label -complete -recover -alllogs[-copy-id id]</pre>
Restaura una base de datos completa si el backup seleccionado no existe en el almacenamiento primario	Introduzca el siguiente comando: <code>smsap backup restore -profile profile_name -label label -complete-recover -alllogs-from -secondary [-temp-volume &lt;temp_volume&gt;] [-copy-id id]</code>

## Ejemplo

El siguiente comando restaura un backup protegido desde el sistema de almacenamiento secundario:

```
smsap backup restore -profile PAYDB -label daily_monday -complete
-recover alllogs -from-secondary -copy-id 3042 -temp-volume
smsap_scratch_restore_volume
Operation Id [8abc011215d385920115d38599470001] succeeded.
```



## Clonar backups protegidos

Es posible usar SnapManager para clonar una copia de un backup que se ha protegido.

### Lo que necesitará

El host (seleccionado para el clon) debe tener acceso al almacenamiento secundario con el mismo protocolo de almacenamiento (por ejemplo, SAN o NAS).

Puede utilizar el `-from-secondary` opción para especificar que desea clonar desde el almacenamiento secundario.

### Acerca de esta tarea

Debe especificar el `-copy-id` siempre que especifique la `-from-secondary` opción. Si existe más de un backup en el sistema de almacenamiento secundario, la opción `-copy-id` se utiliza para especificar qué copia de backup en el almacenamiento secundario se debe usar para clonar.



Si utiliza Data ONTAP operando en 7-Mode, debe especificar un valor válido para `-copy-id` opción. Sin embargo, si utiliza Clustered Data ONTAP, el `-copy-id` la opción no es necesaria.

Puede producirse un error al eliminar clones de backups protegidos en sistemas de almacenamiento secundario. Este problema se produce cuando la hora del sistema de los sistemas de almacenamiento primario y secundario no están sincronizados.

### Paso

1. Crear el clon de una copia de backup protegida:

```
smsap clone create -backup-label backup_name -newsid new_sid -label  
clone_label -profile profile_name -clonespec full_path_to_clonespecfile -from  
-secondary -copy-id id
```

### Ejemplo

```
smsap clone create -label testdb_clone_clstest  
-profile sys_db_finance -from-secondary -copy-id 3042  
sys_db_finance_sept_08
```

## SnapManager para SAP utiliza Protection Manager para proteger un backup de base de datos

Cuando SnapManager para SAP y Protection Manager están instalados en un host UNIX y en el servidor respectivamente, proporcionan al administrador de la base de datos de SnapManager la capacidad de configurar y realizar backups de bases de datos Oracle basados en normativas en el almacenamiento secundario, y restaurar, si es necesario,

los datos de los que se ha realizado un backup del almacenamiento secundario al primario.

En el siguiente ejemplo, un administrador de bases de datos que utiliza SnapManager, crea un perfil para un backup local en el almacenamiento primario y otro perfil para un backup protegido en el almacenamiento secundario. A continuación, este administrador de base de datos trabaja con su administrador de almacenamiento en red, que utiliza la consola de Protection Manager, para configurar un backup basado en normativas de esa base de datos, desde el almacenamiento primario al secundario.

## Detalles de la base de datos de destino

Este ejemplo de protección integrada de bases de datos describe la protección de una base de datos de nóminas. En el ejemplo se utilizan los datos siguientes.

El administrador de la base de datos (DBA) de TechCo, una empresa de 3000 personas con sede en Atlanta, debe crear una copia de seguridad coherente de la base de datos de nóminas de producción, PAYDB. La estrategia de protección para realizar la backup en el almacenamiento primario y secundario requiere que el administrador de almacenamiento y el administrador de bases de datos Oracle trabajen conjuntamente para realizar backups de la base de datos Oracle tanto de forma local en el almacenamiento primario como remota, en un almacenamiento secundario en una ubicación remota.

### • Información del perfil

Al crear un perfil en SnapManager, necesita los siguientes datos:

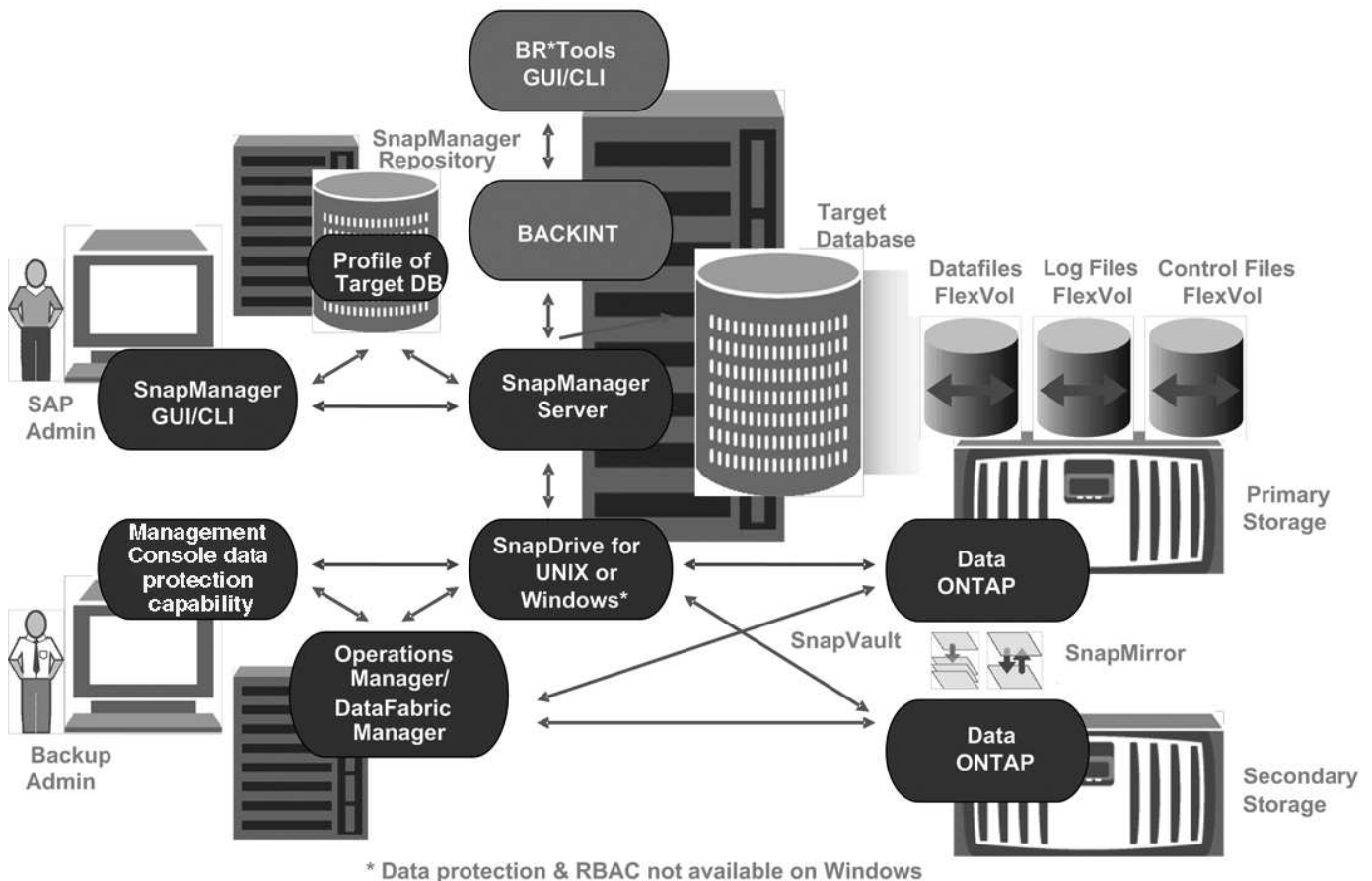
- Nombre de la base de datos: P01
- Nombre del host: prod01.sample.com
- ID de base de datos: P01
- Nombre del perfil: P01\_BACKUP
- Modo de conexión: Autenticación de base de datos
- Esquema de nomenclatura de Snapshot:  
*smsap\_hostname\_dbsid\_smsaprofile\_scope\_mode\_smid* (que se traduce en "smsap\_prod01.sample.com\_p01\_p01\_backup\_f\_h\_x")
- Usuario repositorio: <sid> Linternas, que se traduce a p01rep.

## Configuración y topología de almacenamiento principal y secundario

En este ejemplo, TechCo administra su base de datos de nóminas en un servidor de bases de datos que también es un host de SnapManager para SAP y almacena los datos de configuración y las bases de datos de nóminas en los sistemas de almacenamiento primario de la sede central de la empresa. El requisito corporativo es proteger la base de datos con backups diarios y semanales en un almacenamiento local, así como backups a sistemas de almacenamiento de un sitio de almacenamiento secundario situado a 50 kilómetros de distancia.

En la siguiente ilustración, se muestran SnapManager para SAP y los componentes de capacidad de protección de datos de la consola de gestión de NetApp necesarios para admitir la protección de backup local y secundario.

# SnapManager for SAP Architecture



Para gestionar la base de datos de nóminas y respaldar su protección de copia de seguridad local y secundaria como se muestra en el gráfico anterior, se utiliza la siguiente implementación.

- **SnapManager host**

El host SnapManager, payroll.techco.com, se encuentra en la sede de la empresa y se ejecuta en un servidor UNIX, que también ejecuta el programa de base de datos que genera y mantiene la base de datos de nóminas.

- **Conexiones**

Para admitir la protección de backups locales y secundarios, el host SnapManager tiene conexiones de red a los siguientes componentes:

- SnapManager para el cliente SAP
- Repositorio de SnapManager, que ejecuta el programa de bases de datos, SnapDrive para UNIX y SnapManager
- Sistemas de almacenamiento primario
- Sistemas de almacenamiento secundario
- DataFabric Manager Server

- **Productos instalados**

El host SnapManager se instala con los siguientes productos para este ejemplo:

- Servidor SnapManager
- SnapDrive para UNIX
- Utilidades de host

- **Sistemas de almacenamiento primario TechCo**

La base de datos de nóminas, incluidos los archivos de datos asociados, los archivos de registro y los archivos de control, residen en los sistemas de almacenamiento principales. Estas se encuentran en la sede central de la empresa TechCo, junto con el host de SnapManager y la red que conecta el almacenamiento primario con el host de SnapManager. Las últimas transacciones y actualizaciones de la base de datos de nóminas se escriben en los sistemas de almacenamiento primarios. Las copias Snapshot, que proporcionan protección mediante backup local de la base de datos de nóminas, también residen en los sistemas de almacenamiento primarios.

- **Conexiones**

Para admitir la protección de backups secundarios, los sistemas de almacenamiento primario tienen conexiones de red a los siguientes componentes:

- Host SnapManager que ejecuta el programa de bases de datos, SnapDrive para UNIX y SnapManager
- Sistemas de almacenamiento secundario
- DataFabric Manager Server

- **Productos instalados**

Para este ejemplo, deben habilitarse las siguientes licencias en estos sistemas:

- Data ONTAP 7.3.1 o posterior
- ONTAP primario de SnapVaultData
- FlexVol (necesario para NFS)
- SnapRestore
- Protocolo NFS

- **Sistemas de almacenamiento secundario TechCo**

Los sistemas de almacenamiento secundario, ubicados en un sitio de almacenamiento secundario conectado a la red, a 50 km de distancia, se utilizan para almacenar backups secundarios de la base de datos de nóminas.

- **Conexiones**

Para admitir la protección de backup secundario, los sistemas de almacenamiento secundario tienen conexiones de red a los siguientes componentes:

- Sistemas de almacenamiento primario
- DataFabric Manager Server

- **Productos instalados**

Para este ejemplo, deben habilitarse las siguientes licencias en los sistemas de almacenamiento secundario:

- Data ONTAP
- SnapVaultData ONTAP secundario
- SnapRestore
- FlexVol (necesario para NFS)
- Protocolo NFS

#### • **DataFabric Manager Server**

DataFabric Manager Server, techco\_dfm, se encuentra en la sede de la empresa en una ubicación accesible por el administrador de almacenamiento. DataFabric Manager Server, entre otras funciones, coordina las tareas de backup entre el almacenamiento principal y el secundario.

##### ◦ **Conexiones**

Para admitir una protección de backup secundaria, DataFabric Manager Server mantiene conexiones de red con los siguientes componentes:

- Consola de gestión de NetApp
- Sistemas de almacenamiento primario
- Sistemas de almacenamiento secundario

##### ◦ **Productos instalados**

Para este ejemplo, DataFabric Manager Server cuenta con licencia para los siguientes productos de servidor:

- DataFabric Manager

#### • **Repositorio de SnapManager**

El repositorio de SnapManager, ubicado en un servidor dedicado, almacena datos sobre las operaciones realizadas por SnapManager, por ejemplo, el momento de realizar backups, los espacios de tablas y archivos de datos de los que se ha realizado backup, los sistemas de almacenamiento utilizados, los clones realizados y las copias Snapshot creadas. Cuando un administrador de bases de datos intenta realizar una restauración completa o parcial, SnapManager consulta al repositorio para identificar los backups creados por SnapManager para SAP para su restauración.

##### ◦ **Conexiones**

Para admitir la protección de backup secundario, los sistemas de almacenamiento secundario tienen conexiones de red a los siguientes componentes:

- Host SnapManager
- SnapManager para el cliente SAP

#### • **Consola de gestión de NetApp**

La consola de gestión de NetApp es la consola de interfaz gráfica de usuario que utiliza el administrador de almacenamiento para configurar programaciones, políticas, conjuntos de datos y asignaciones de pools de recursos con el fin de permitir el backup en sistemas de almacenamiento secundarios, a los que el administrador de almacenamiento puede acceder.

##### ◦ **Conexiones**

Para admitir la protección de backups secundarios, NetApp Management Console tiene conexiones de red a los siguientes componentes:

- Sistemas de almacenamiento primario
- Sistemas de almacenamiento secundario
- DataFabric Manager Server

#### • **SnapManager para cliente SAP**

El cliente SnapManager para SAP es la interfaz gráfica de usuario y la consola de línea de comandos que usa el administrador de bases de datos para la base de datos de nóminas de este ejemplo para configurar y realizar respaldo local y respaldo en el almacenamiento secundario.

##### ◦ **Conexiones**

Para admitir la protección de backups locales y secundarios, SnapManager para clientes SAP tiene conexiones de red a los siguientes componentes:

- Host SnapManager
- SnapManager Repository, ejecuta el programa de bases de datos, SnapDrive para UNIX y SnapManager
- Host de base de datos (si está separado del host que ejecuta SnapManager)
- DataFabric Manager Server

##### ◦ **Productos instalados**

Para admitir la protección de backup local y secundario, se debe instalar el software SnapManager para cliente SAP en este componente.

## **Programa de backup y estrategia de retención**

El administrador de bases de datos quiere asegurarse de que los backups estén disponibles en caso de pérdida de datos, en caso de siniestro y por motivos normativos. Esto requiere una política de retención de pensamiento detenidamente para las distintas bases de datos.

Para la base de datos de nóminas de producción, el DBA se adhiere a la siguiente estrategia de retención de TechCo:

<b>Frecuencia de backup</b>	<b>Duración de la retención</b>	<b>El tiempo de los backups</b>	<b>Tipo de almacenamiento</b>
Una vez al día	10 días	7 p. m.	Primario (local)
Una vez al día	10 días	7 p. m.	Secundario (archivado)
Una vez por semana	52 semanas	Sábados 1:00 a.m.	Secundario (archivado)

#### • **Ventajas de copia de seguridad local**

El backup local diario proporciona protección de bases de datos, que es instantánea, utiliza cero ancho de

banda de red, utiliza un mínimo de espacio de almacenamiento adicional, ofrece una restauración instantánea y ofrece funciones de backup y restauración de datos muy detalladas.

Como los backups semanales finales de la base de datos de nóminas se conservan durante un mínimo de 52 semanas en un site de almacenamiento secundario, no es necesario conservar los backups diarios durante más de 10 días.

- **Ventajas de copia de seguridad protegida**

Los backups diarios y semanales a un almacenamiento secundario en una ubicación remota garantizan que si los datos del site de almacenamiento principal presentan daños, la base de datos objetivo sigue estando protegida y podrá restaurarse a partir del almacenamiento secundario.

Se realizan los backups diarios al almacenamiento secundario para protegerse frente a daños en el sistema de almacenamiento primario. Como los backups semanales finales de la base de datos de nóminas se conservan durante un mínimo de 52 semanas, no es necesario conservar los backups diarios durante más de 10 días.

## **Resumen de flujo de trabajo para backup de bases de datos local y secundario**

En este ejemplo, el administrador de bases de datos (con SnapManager) y el administrador de almacenamiento (con la función de protección de datos Management Console de NetApp) coordinan las acciones para configurar los backups locales y secundarios (también conocidos como backup protegido) de la base de datos de destino.

La secuencia de acciones realizadas se resume de la siguiente manera:

- **Configuración del pool de recursos secundario**

El administrador de almacenamiento usa la funcionalidad de protección de datos de NetApp Management Console para configurar un conjunto de recursos de sistemas de almacenamiento en el sitio secundario que puede usarse para almacenar el backup de base de datos de nóminas.

- **Programación de copia de seguridad secundaria**

El administrador de almacenamiento usa la funcionalidad de protección de datos de NetApp Management Console para configurar programaciones de backup secundarias.

- **Configuración de la política de protección**

El administrador de almacenamiento usa la funcionalidad de protección de datos de NetApp Management Console para configurar una normativa de protección de backup secundaria para la base de datos de destino. La política de protección incluye las programaciones y especifica el tipo base de protección para implementar la protección de backups (backup, reflejo o una combinación de ambos), y nombra políticas de retención para los datos primarios, secundarios y, en ocasiones, nodos de almacenamiento terciarios.

- **Asignación de políticas de protección y configuración de perfiles de base de datos**

El DBA utiliza SnapManager para crear o editar un perfil de la base de datos de destino que admita una copia de seguridad secundaria. Al configurar el perfil, el DBA:

- Permite la protección de backups en el almacenamiento secundario.
- Asigna a este perfil la nueva política de protección, que se creó en la funcionalidad de protección de

datos de NetApp Management Console y se recuperó de ella.

La asignación de la normativa de protección incluye automáticamente la base de datos de destino en un conjunto de datos parcialmente aprovisionado, pero no conforme con el conjunto de datos de la funcionalidad de protección de datos de la Consola de gestión de NetApp. Cuando está totalmente aprovisionado, la configuración del conjunto de datos permite realizar backups de la base de datos de destino en un almacenamiento secundario.

El nombre del conjunto de datos utiliza la siguiente sintaxis: *smsap\_hostname\_databasename*, que se traduce a "smsap\_prod01.sample.com\_p01".

- **Aprovisionamiento de almacenamiento secundario y terciario**

El administrador de almacenamiento usa la funcionalidad de protección de datos de Management Console de NetApp para asignar pools de recursos con el fin de aprovisionar los nodos de almacenamiento secundario y, en ocasiones, terciario (si la política de protección asignada especifica nodos de almacenamiento terciarios).

- **Backup en almacenamiento local**

El administrador de bases de datos abre el perfil con la protección habilitada en SnapManager y crea un backup completo al almacenamiento local. El nuevo backup se muestra en SnapManager como programado para la protección, pero no protegido todavía.

- **Confirmación de copia de seguridad secundaria**

Como el backup se basa en un perfil habilitado para la protección, el backup se transfiere al volumen secundario según la programación de la política de protección. El administrador de bases de datos utiliza SnapManager para confirmar la transferencia del backup a un almacenamiento secundario. Una vez que el backup se ha copiado al almacenamiento secundario, SnapManager cambia el estado de protección de backup de "no protegido" a "protegido".

## **Protección de la configuración y ejecución de backups**

Es necesario configurar SnapManager y Protection Manager para admitir backups de bases de datos en el almacenamiento secundario. El administrador de la base de datos y el administrador de almacenamiento deben coordinar las acciones correspondientes.

### **Utilice SnapManager para SAP para crear el perfil de base de datos para un backup local**

Los administradores de bases de datos utilizan SnapManager para crear un perfil de base de datos que se utilizará para iniciar una copia de seguridad en el almacenamiento local en un sistema de almacenamiento primario. Los procesos de creación de perfiles y de creación de backups se realizan por completo en SnapManager; no implican Protection Manager.

### **Acerca de esta tarea**

Un perfil contiene información sobre la base de datos que se gestiona, incluidas sus credenciales, su configuración de backup y la configuración de protección para las copias de seguridad. Al crear un perfil, no es necesario especificar los detalles de la base de datos cada vez que se realiza una operación en esa base de datos, en su lugar sólo se proporciona el nombre del perfil. Un perfil sólo puede hacer referencia a una base de datos. Se puede hacer referencia a esa misma base de datos por más de un perfil.



## Pasos

1. Acceda al cliente de SnapManager para SAP.
2. En el árbol repositorios SnapManager, haga clic con el botón secundario del ratón en el host que desee asociar a este perfil y seleccione **Crear perfil**.
3. En la página Información de configuración del perfil, introduzca la siguiente información y haga clic en **Siguiente**.
  - Nombre del perfil: Payroll\_prod
  - Contraseña de perfil: Payroll123
  - Comentario: Base de datos de nóminas de producción
4. En la página Database Configuration Information (Información de configuración de la base de datos), introduzca la siguiente información y haga clic en **Next** (Siguiente).
  - Nombre de la base de datos: PAYDB
  - SID de base de datos: Payroldb
  - Host de la base de datos: Acepte el valor predeterminado

Debido a que está creando un perfil a partir de un host en el árbol de repositorios, SnapManager muestra el nombre de host.

5. En la segunda página Información de configuración de la base de datos, acepte la siguiente información de la base de datos y haga clic en **Siguiente**:
  - Cuenta de host, que representa la cuenta de usuario de Oracle (para orWindows <sid>): Orapayroldb
  - Host Group, que representa al grupo Oracle: dba
6. En la página Información de conexión a la base de datos, seleccione **utilizar autenticación de base de datos** para permitir que los usuarios se autenticquen mediante la información de la base de datos.

Para este ejemplo, introduzca la siguiente información y haga clic en **Siguiente**.

- SYSDBA Privileged User Name, que representa al administrador de la base de datos del sistema que tiene privilegios administrativos: Sys
  - Contraseña (contraseña SYSDBA): oracle
  - Puerto para conectarse al host de la base de datos: 1527
7. En la página Snapshot Naming Information, especifique una convención de nomenclatura para las Snapshot asociadas con este perfil seleccionando variables. La única variable que se requiere es la variable **smid**, que crea un identificador de instantánea único.

Para este ejemplo, haga lo siguiente:

- a. En la lista símbolo de variable, seleccione la variable **{usertext}** y haga clic en **Agregar**.
- b. Introduzca "prod01.sample.com\_" como nombre de host y haga clic en **Aceptar**.
- c. Haga clic en **izquierda** hasta que el nombre de host aparezca justo después de "smSAP" en el cuadro Formato .
- d. Haga clic en **Siguiente**.

La convención de nomenclatura Snapshot de

*smsap\_hostname\_smsaprofile\_dbsid\_scope\_mode\_smid* Se convierte en "smsap\_prpd01.sample.com\_P01\_BACKUP\_P01\_f\_a\_x" (donde "f" indica una copia de seguridad completa, la "a" indica el modo automático y la "x" representa el SMID único).

8. En la página realizar operación, compruebe la información y haga clic en **Crear**.
9. Haga clic en **Detalles de operación** para ver información acerca de la operación de creación de perfiles e información de elegibilidad de restauración basada en volumen.

### Use Protection Manager para configurar un pool de recursos secundario

Para admitir el backup de la base de datos en el almacenamiento secundario, el administrador de almacenamiento usa Protection Manager para organizar los sistemas de almacenamiento secundario habilitados con la licencia secundaria de SnapVault en un conjunto de recursos para los backups.

#### Lo que necesitará

Lo ideal es que los sistemas de almacenamiento de un conjunto de recursos sean intercambiables en cuanto a su aceptación como destinos para los backups. Por ejemplo, al desarrollar la estrategia de protección para la base de datos de nóminas, como administrador de almacenamiento, identificó los sistemas de almacenamiento secundarios con niveles de servicio y rendimiento similares que serían miembros adecuados del mismo conjunto de recursos.

Ya creó agregados de espacio no utilizado en sistemas de almacenamiento que piensa asignar a pools de recursos. De este modo se garantiza que haya espacio adecuado para contener las copias de seguridad.

#### Pasos

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **datos > grupos de recursos**.

Aparecerá la ventana Pools de recursos.

3. Haga clic en **Agregar**.

Se iniciará el asistente Add Resource Pool.

4. Complete los pasos del asistente para crear el pool de recursos **paydb\_backup\_resource**.

Utilice los siguientes ajustes:

- Nombre: Use **paydb-backup\_resource**
- Umbrales de espacio (utilice los valores predeterminados):
  - Umbrales de utilización del espacio: Activado
  - Umbral casi completo (para el conjunto de recursos): 80%
  - Umbral completo (para el conjunto de recursos): 90%

### Use Protection Manager para configurar las programaciones de backups secundarios

Para admitir el backup de la base de datos en el almacenamiento secundario, el administrador de almacenamiento usa Protection Manager para configurar una programación de backups.

#### Lo que necesitará

Antes de configurar la programación para las copias de seguridad secundarias, el administrador de almacenamiento consulta al partner DBA la siguiente información:

- La programación que el administrador de bases de datos desea que se sigan los backups secundarios.

En este caso, los backups únicos diarios se realizan a las 7 p. m. Y los backups una vez semanales se realizan el sábado a las 1:00

## Pasos

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **políticas > Protección > programas**.

Se muestra la pestaña Schedules de la ventana Protection Policies.

3. Seleccione el horario diario **Diario a las 8:00 PM** en la lista de horarios.
4. Haga clic en **Copiar**.

En la lista se muestra un nuevo horario diario, **copia del diario a las 8:00 PM**. Ya está seleccionado.

5. Haga clic en **Editar**.

La hoja de propiedades Editar horario diario se abre a la ficha Programación.

6. Cambie el nombre del programa a **nómina diaria a las 7 PM**, actualice la descripción y, a continuación, haga clic en **aplicar**.

Se guardan los cambios.

7. Haga clic en la ficha **Eventos diarios**.

La hora actual de copia de seguridad diaria de la programación es de 8:00 p.m. aparece en pantalla.

8. Haga clic en **Agregar** e introduzca **7:00 PM** en el nuevo campo Hora y, a continuación, haga clic en **aplicar**.

La hora actual de copia de seguridad diaria del programa es ahora a las 7:00 p.m.

9. Haga clic en **Aceptar** para guardar los cambios y salir de la hoja de propiedades.

Su nuevo horario diario, **Payroll Daily a las 7 PM**, se muestra en la lista de horarios.

10. Seleccione el horario semanal **Domingo a las 8:00 PM más diariamente** en la lista de horarios.

11. Haga clic en **Copiar**.

En la lista se muestra un nuevo horario semanal, **copia del domingo a las 8:00 PM más diario**. Ya está seleccionado.

12. Haga clic en **Editar**.

La hoja de propiedades Editar horario semanal se abre a la ficha Programación.

13. Cambie el nombre del programa a **Payroll Saturday a la 1 AM PLUS Daily a las 7 PM** y actualice la descripción.

14. En la lista desplegable **Horario diario**, seleccione el horario diario que acaba de crear, **Payroll Daily a las 7 PM**.

Seleccionar **nómina diaria a las 7 PM** significa que este programa define cuándo se producen las operaciones diarias cuando se aplica a una política el programa **nómina de sábado a la 1 AM más diario a las 7 PM**.

15. Haga clic en **Aceptar** para guardar los cambios y salir de la hoja de propiedades.

Su nuevo horario semanal, **Payroll Saturday a la 1 AM más diariamente a las 7 PM**, se muestra en la lista de horarios.

## Use Protection Manager para configurar una política de protección de backups secundarios

Después de configurar la programación de backup, el administrador de almacenamiento configura una normativa de almacenamiento de backup protegido en la que se incluirá dicha programación.

### Lo que necesitará

Antes de configurar la normativa de protección, el administrador de almacenamiento le ofrece al partner DBA la siguiente información:

- Duración de retención que se debe especificar para el almacenamiento secundario
- Tipo de protección del almacenamiento secundario requerida

### Acerca de esta tarea

La política de protección que se crea, puede figurar en SnapManager para SAP por el partner de administrador de bases de datos y asignarse a un perfil de base de datos para la protección de los datos.

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **políticas > Protección > Descripción general**.

Se muestra la pestaña Overview de la ventana Protection Policies.

3. Haga clic en **Agregar directiva** para iniciar el asistente **Agregar directiva de protección**.
4. Complete el asistente con los siguientes pasos:

- a. Especifique un nombre de política descriptivo.

Para este ejemplo, introduzca **TechCo Payroll Data: Copia de seguridad** y una descripción y, a continuación, haga clic en **Siguiente**.

- b. Seleccione una política base.

Para este ejemplo, seleccione **copia de seguridad** y haga clic en **Siguiente**.

- c. En la hoja de propiedades de la directiva del nodo **datos primarios**, acepte la configuración predeterminada y haga clic en **Siguiente**.



En este ejemplo, se aplica la programación de backup local configurada en SnapManager. Se ignora cualquier programación de backup local especificada con este método.

- d. En la hoja de propiedades de la conexión **datos primarios a copia de seguridad**, seleccione un programa de copia de seguridad.

Para este ejemplo, seleccione **Payroll Saturday a la 1 AM más diariamente a las 7 PM** como su programa de copia de seguridad y, a continuación, haga clic en **Next**.

En este ejemplo, la programación seleccionada incluye tanto las programaciones semanales como diarias que se configuraron anteriormente.

- e. En la hoja de propiedades **Política de copia de seguridad**, especifique el nombre del nodo de copia de seguridad y los tiempos de retención de copias de seguridad diarias, semanales o mensuales.

Para este ejemplo, especifique una retención de backup diaria de 10 días y una retención de backup semanal de 52 semanas. Después de completar cada hoja de propiedades, haga clic en **Siguiente**.

Una vez completadas todas las hojas de propiedades, el asistente para agregar directivas de protección muestra una hoja de resumen de la directiva de protección que desea crear.

5. Haga clic en **Finalizar** para guardar los cambios.

## resultado

La política de protección de **TechCo Payroll Data: Backup** se incluye entre las demás políticas configuradas para Protection Manager.

## Después de terminar

El partner de DBA puede ahora usar SnapManager para SAP para enumerar y asignar esta normativa al crear el perfil de base de datos para proteger los datos.

## Utilice SnapManager para SAP para crear el perfil de base de datos y asignar una normativa de protección

Debe crear un perfil en SnapManager para SAP, habilitar la protección en el perfil y asignar una política de protección para crear un backup protegido.

## Acerca de esta tarea

Un perfil contiene información sobre la base de datos que se gestiona, incluidas sus credenciales, su configuración de backup y la configuración de protección para backups. Después de crear un perfil, no es necesario especificar los detalles de la base de datos cada vez que se realiza una operación. Un perfil sólo puede hacer referencia a una base de datos, pero es posible hacer referencia a esa misma base de datos mediante más de un perfil.

## Pasos

1. Acceda al cliente de SnapManager para SAP.
2. En el árbol repositorios, haga clic con el botón secundario del ratón en el host y seleccione **Crear perfil**.
3. En la página **Información de configuración del perfil**, introduzca los detalles del perfil y haga clic en **Siguiente**.

## ejemplo

Puede introducir la siguiente información:

- Nombre del perfil: P01\_BACKUP
- Contraseña de perfil: Payroll123
- Comentario: Base de datos de nóminas de producción

4. En las páginas **Información de configuración de la base de datos**, introduzca los detalles de la base de datos y haga clic en **Siguiente**.

## ejemplo

Puede introducir la siguiente información:

- Nombre de la base de datos: P01
- SID de base de datos: P01
- Host de la base de datos: Acepte el valor predeterminado. Debido a que está creando un perfil a partir de un host en el árbol de repositorios, SnapManager muestra el nombre de host.
- Cuenta de host, que representa la cuenta de usuario de Oracle (para orWindows <sid>): Orapayroldb
- Host Group, que representa al grupo Oracle: dba

5. En la página **Información de conexión a la base de datos**, haga clic en **usar autenticación de base de datos** para permitir que los usuarios autenticuen mediante información de la base de datos.
6. Introduzca los detalles de conexión de la base de datos y haga clic en **Siguiente**.

## ejemplo

Puede introducir la siguiente información:

- SYSDBA Privileged User Name, que representa al administrador de la base de datos del sistema que tiene privilegios administrativos: Sys
- Contraseña (contraseña SYSDBA): oracle
- Puerto para conectarse al host de la base de datos: 1527

7. En la página Snapshot Naming Information, especifique una convención de nomenclatura para las Snapshot asociadas con este perfil seleccionando variables.

La *smid* la variable crea un identificador snapshot único.

Realice lo siguiente:

- a. En la lista **símbolo de variable**, seleccione *usertext* Y haga clic en **Agregar**.
- b. Introduzca *prod01.sample.com\_* Como nombre de host y haga clic en **Aceptar**.
- c. Haga clic en **izquierda** hasta que el nombre de host aparezca justo después de smsap en el cuadro Formato .
- d. Haga clic en **Siguiente**.

La convención de nomenclatura Snapshot de

*smsap\_hostname\_smsaprofile\_dbsid\_scope\_mode\_smid* Se convierte en "smsap\_prpd01.sample.com\_P01\_BACKUP\_P01\_f\_a\_x" (donde "f" indica una copia de seguridad

completa, "a" indica el modo automático y "x" representa el SMID único).

#### 8. Seleccione **Directiva de protección de Protection Manager**.

**La normativa de protección de Protection Manager** le permite seleccionar una directiva de protección configurada mediante la Consola de gestión de NetApp.

#### 9. Seleccione **TechCo Payroll Data: Backup** como política de protección de las políticas de protección recuperadas de NetApp Management Console y haga clic en **Siguiente**.

#### 10. En la página **realizar operación**, compruebe la información y haga clic en **Crear**.

#### 11. Haga clic en **Detalles de operación** para ver información acerca de la operación de creación de perfiles e información de elegibilidad de restauración basada en volumen.

### resultado

- La asignación de una normativa de protección de NetApp Management Console al perfil de base de datos crea automáticamente un conjunto de datos no conforme, visible para el operador de la Consola de gestión de NetApp, con el nombre convención smSAP\_<hostname>\_<profilename> o en este ejemplo: smsap\_prod01.sample.com\_P01\_BACKUP.
- Si el perfil no es apto para la restauración de volumen (también llamado "restauración rápida"), se produce lo siguiente:
  - La ficha **resultados** indica que la creación del perfil se ha realizado correctamente y que se han producido advertencias durante la operación.
  - La ficha **Detalles de operación** incluye un registro DE ADVERTENCIA, que indica que el perfil no es elegible para una restauración rápida y explica por qué.

### Utilice Protection Manager para aprovisionar el nuevo conjunto de datos

Una vez creado el conjunto de datos smsap\_paydb, el administrador de almacenamiento utiliza Protection Manager para asignar recursos del sistema de almacenamiento a fin de aprovisionar el nodo Backup del conjunto de datos.

### Lo que necesitará

Antes de aprovisionar el conjunto de datos recién creado, el administrador de almacenamiento consulta al partner DBA el nombre del conjunto de datos especificado en el perfil.

En este caso, el nombre del conjunto de datos es smsap\_prod01.sample.com\_P01.

### Pasos

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **datos > conjuntos de datos > Descripción general**.

La pestaña Datasets de la ventana Datasets muestra una lista de conjuntos de datos que incluye el conjunto de datos que acaba de crear mediante SnapManager.

3. Localice y seleccione el conjunto de datos **smsap\_prod01.sample.com\_p01**.

Al seleccionar este conjunto de datos, el área del gráfico muestra el conjunto de datos smSAP\_p01 sin aprovisionar con su nodo de backup. Su estado de conformidad se Marca como no conforme.

4. Con el conjunto de datos smsap\_p01 todavía resaltado, haga clic en **Editar**.

La consola de gestión de NetApp de Protection Manager muestra la ventana Editar conjunto de datos para el conjunto de datos **msap\_prod01.sample.com\_p01**. El panel de navegación de la ventana muestra las opciones de configuración del nodo principal del conjunto de datos, la conexión de backup y el nodo de backup.

5. En el panel de navegación, busque las opciones del nodo de copia de seguridad del conjunto de datos y seleccione **agrupaciones de aprovisionamiento/recursos**.

La ventana Edit Dataset muestra una configuración de la política de aprovisionamiento predeterminada y una lista de pools de recursos disponibles.

6. Para este ejemplo, seleccione el pool de recursos **p01\_backup\_resource** y haga clic en **>**.

El pool de recursos seleccionado aparece en el campo "Pools de recursos para este nodo".

7. Haga clic en **Finalizar** para guardar los cambios.

## resultado

Protection Manager aprovisiona automáticamente el nodo de copia de seguridad secundario con recursos del pool de recursos paydb\_backup\_resource.

## Use SnapManager para SAP para crear un backup protegido

Al crear un backup para este ejemplo, el administrador de bases de datos selecciona la creación de un backup completo, define las opciones de backup y selecciona la protección para el almacenamiento secundario. Si bien el backup se realiza inicialmente en el almacenamiento local, ya que este backup se basa en un perfil con protección habilitada, el backup se transfiere luego al almacenamiento secundario según la programación de la política de protección definida en Protection Manager.

## Pasos

1. Acceda al cliente de SnapManager para SAP.
2. En el árbol del repositorio de SnapManager, haga clic con el botón derecho del ratón en el perfil que contiene la base de datos de la que desea realizar la copia de seguridad y seleccione **copia de seguridad**.

Se iniciará el Asistente para copia de seguridad de SnapManager para SAP.

3. Introduzca

**Production\_payroll**

como etiqueta.

4. Introduzca

**Production payroll Jan 19 backup**

como comentario.



5. Seleccione **Auto** como el tipo de copia de seguridad que desea crear.

Esto permite a SnapManager determinar si se debe realizar un backup en línea o sin conexión.

6. Seleccione **Diario** o **Semanal** como la frecuencia de la copia de seguridad.

7. Para confirmar que la copia de seguridad tiene un formato válido para Oracle, marque la casilla junto a **verificar copia de seguridad**.

Esta operación utiliza Oracle DBVerify para comprobar el formato de bloque y la estructura.

8. Para forzar el estado de la base de datos al modo apropiado (por ejemplo, de abierto a montado), seleccione **permitir inicio o cierre de la base de datos, si es necesario**, y haga clic en **Siguiente**.

9. En la página Database, Tablespaces o Datafiles to Backup, seleccione **Full Backup** y haga clic en **Next**.

10. Para proteger la copia de seguridad en almacenamiento secundario, seleccione **proteger la copia de seguridad** y haga clic en **Siguiente**.

11. En la página realizar operación, compruebe la información suministrada y haga clic en **copia de seguridad**.

12. En la página Progress, consulte el progreso y los resultados de la creación de backup.

13. Para ver los detalles de la operación, haga clic en **Detalles de la operación**.

### Utilice SnapManager para SAP para confirmar la protección del backup

Con SnapManager para SAP, se puede ver una lista de backups asociados a un perfil, determinar si los backups estaban habilitados para la protección y ver la clase de retención (diaria o semanal, en este ejemplo).

#### Acerca de esta tarea

Al principio, el nuevo backup en este ejemplo se muestra como programado para la protección, pero no está protegido aún (en la interfaz gráfica de usuario de SnapManager y en el resultado del comando backup show). Una vez que el administrador de almacenamiento garantiza que el backup se haya copiado al almacenamiento secundario, SnapManager cambia el estado de protección de backup de "no protegido" a "protegido" en la interfaz gráfica de usuario y con el comando backup list.

1. Acceda al cliente de SnapManager para SAP.

2. En el árbol del repositorio de SnapManager, expanda el perfil para mostrar sus copias de seguridad.

3. Haga clic en la ficha **copias de seguridad/clones**.

4. En el panel Informes, seleccione **Detalles de copia de seguridad**.

5. Consulte la columna Protection y asegúrese de que el estado sea "Protected".

### Restauración de bases de datos desde backup

Si el contenido activo de la base de datos de nóminas se pierde o destruye accidentalmente, SnapManager y la función de protección de datos de la consola de gestión de NetApp permiten la restauración de esos datos desde un backup local o un almacenamiento secundario.

## Use SnapManager para SAP para restaurar un backup local en el almacenamiento primario

Es posible restaurar backups locales que estén en el almacenamiento principal. Todo el proceso se realiza mediante SnapManager para SAP.

### Acerca de esta tarea

También puede obtener una vista previa de la información acerca de un proceso de restauración de copia de seguridad. Puede que desee hacer esto para ver información acerca de la elegibilidad de restauración de un backup. SnapManager analiza los datos de un backup para determinar si puede completarse el proceso de restauración usando la restauración basada en volúmenes o el método de restauración basada en archivos.

La vista previa de la restauración muestra la siguiente información:

- Qué mecanismo de restauración (restauración rápida, restauración de sistema de archivos en el lado del almacenamiento, restauración de archivos en el lado del almacenamiento o restauración de copias de archivos del lado del host) se utilizará para restaurar cada archivo.
- Por qué no se utilizaron mecanismos más eficientes para restaurar cada archivo.

En la vista previa del plan de restauración, SnapManager no restaura nada. La vista previa muestra información de hasta 20 archivos.

Si desea obtener una vista previa de una restauración de archivos de datos pero la base de datos no está montada, SnapManager monta la base de datos. Si no se puede montar la base de datos, la operación genera un error y SnapManager devuelve la base de datos a su estado original.

### Pasos

1. En el árbol **Repository**, haga clic con el botón derecho del ratón en la copia de seguridad que desea restaurar y seleccione **Restaurar**.
2. En la página de bienvenida del Asistente para restauración y recuperación, haga clic en **Siguiente**.
3. En la página **Restore Configuration Information**, seleccione **Complete Datafile/Tablespace Restore with Control Files**.
4. Haga clic en **permitir cierre de la base de datos si es necesario**.

SnapManager cambia el estado de la base de datos, si es necesario. Por ejemplo, si la base de datos está sin conexión y debe estar en línea, SnapManager la fuerza a la conexión.

5. En la página **Información de configuración de recuperación**, haga clic en **todos los registros**.

SnapManager restaura y recupera la base de datos a la última transacción y aplica todos los registros requeridos.

6. En la página **Restore Source Location Configuration**, vea la información sobre la copia de seguridad en primario y haga clic en **Next**.

Si el backup solo se realiza en el almacenamiento primario, SnapManager restaura el backup desde el almacenamiento primario.

7. En la página **Información de configuración de la restauración de volumen**, seleccione **intentar la restauración de volumen** para intentar el método de restauración de volumen.
8. Haga clic en **Volver a restauración basada en archivos**.

Así, SnapManager puede utilizar el método de restauración basada en archivos si no se puede utilizar el

método de restauración de volumen.

9. Haga clic en **Vista previa** para ver las comprobaciones de elegibilidad para obtener una rápida restauración e información sobre comprobaciones obligatorias y anulables.
10. En la página **realizar operación**, compruebe la información introducida y haga clic en **Restaurar**.
11. Para ver detalles sobre el proceso, haga clic en **Detalles de la operación**.

### Utilice SnapManager para SAP para restaurar backups desde almacenamiento secundario

Los administradores pueden restaurar backups protegidos a partir de almacenamiento secundario y elegir cómo desean copiar los datos de nuevo en el almacenamiento primario.

#### Lo que necesitará

Antes de intentar restaurar el backup, compruebe las propiedades del backup y asegúrese de que el backup se libere en el sistema de almacenamiento principal y esté protegido en el almacenamiento secundario.

#### Pasos

1. En el árbol de SnapManager for SAP Repository, haga clic con el botón derecho del ratón en la copia de seguridad que desea restaurar y seleccione **Restaurar**.
2. En la página de bienvenida del Asistente para restauración y recuperación, haga clic en **Siguiente**.
3. En la página Restore Configuration Information, haga clic en **Complete Datafile/Tablespace Restore with Control Files**.
4. Haga clic en **permitir cierre de la base de datos si es necesario** y, a continuación, haga clic en **Siguiente**.

SnapManager cambia el estado de la base de datos, si es necesario. Por ejemplo, si la base de datos está sin conexión y debe estar en línea, SnapManager la fuerza a la conexión.

5. En la página Información de configuración de recuperación, haga clic en **todos los registros**. A continuación, haga clic en **Siguiente**.

SnapManager restaura y recupera la base de datos a la última transacción y aplica todos los registros requeridos.

6. En la página Restore Source Location Configuration (Restaurar configuración de ubicación de origen), seleccione el ID del origen de copia de seguridad protegida y haga clic en **Next** (Siguiente).
7. En la página Información de configuración de la restauración de volumen, haga clic en **intentar la restauración de volumen** para intentar la restauración de volumen.
8. Haga clic en **Volver a restauración basada en archivos**.

Esto permite a SnapManager utilizar el método de restauración basada en archivos si no se puede completar el método de restauración de volúmenes.

9. Para ver las comprobaciones de elegibilidad para obtener una rápida restauración e información sobre comprobaciones obligatorias y anulables, haga clic en **Vista previa**.
10. En la página realizar operación, compruebe la información que ha proporcionado y haga clic en **Restaurar**.
11. Para ver detalles sobre el proceso, haga clic en **Detalles de la operación**.

# Realizando operaciones de gestión

Es posible realizar tareas de gestión después de instalar y configurar SnapManager. Estas tareas le permiten gestionar las operaciones normales más allá del backup, la restauración y la clonación.

Los administradores pueden realizar operaciones mediante la interfaz gráfica de usuario o la interfaz de línea de comandos.

## Ver una lista de operaciones

Es posible ver una lista con un resumen de todas las operaciones realizadas en un perfil.

### Acerca de esta tarea

Puede ver la siguiente información cuando enumere operaciones asociadas a un perfil en particular:

- Fecha de inicio y finalización cuando se ejecutó la operación
- Estado de la operación
- ID de la operación
- Tipo de operación
- Host en el que se ejecutó

### Paso

1. Para enumerar la información resumida de todas las operaciones, utilice el siguiente comando:

```
smsap operation list profile -profile profile_name -delimiter character [-quiet | -verbose]
```

Cuando se especifica la opción `-delimitador`, el comando enumera cada fila en una línea separada y los atributos de esa fila están separados por el carácter especificado.

## Ver detalles de la operación

Puede ver información detallada acerca de un perfil determinado para verificar el éxito o el fracaso de una operación. También puede ayudar a determinar los recursos de almacenamiento que se están utilizando para una operación en particular.

### Acerca de esta tarea

Es posible ver los siguientes detalles sobre una operación en particular:

- ID de la operación
- Tipo de operación
- Si la operación se ha forzado
- Información de tiempo de ejecución, incluido el estado, la fecha de inicio y de finalización de la operación
- El host donde se ejecutó la operación, incluidos el ID de proceso y la versión de SnapManager

- Información del repositorio
- Recursos de almacenamiento en uso

#### Paso

1. Para ver la información detallada de un ID de operación específico, escriba el siguiente comando:

```
smsap operation show -profile profile_name [-label label | -id id] [-quiet | -verbose]
```

## Emita comandos desde un host alternativo

Puede emitir comandos de la CLI desde un host distinto al host de la base de datos y SnapManager enrutará los comandos que introduzca al host adecuado.

#### Acerca de esta tarea

Para que el sistema pueda enviar una operación al host correcto, primero debe saber dónde encontrar el perfil para la operación. En este procedimiento, el sistema mantiene el perfil en la información de asignación de repositorios para un archivo en el directorio principal del usuario en el host local.

#### Paso

1. Para que el directorio principal del usuario local conozca las asignaciones de perfil a repositorio de modo que pueda enrutar la solicitud de operación, introduzca el siguiente comando:

```
smsap profile sync -repository-dbname repo_dbname -host repo_host -port repo_port -login-username repo_username [-quiet | -verbose]
```

## Compruebe la versión del software SnapManager

Puede determinar qué versión del producto se ejecuta en el host local ejecutando el `version` comando.

#### Paso

1. Para comprobar la versión de SnapManager, introduzca este comando: **smsap version**

## Detenga el servidor host SnapManager

Cuando termine de utilizar SnapManager, quizás desee detener el servidor.

#### Paso

1. Para detener el servidor, escriba el siguiente comando, como usuario raíz:

```
smsap_server stop
```

## Reinicie el servidor host UNIX de SnapManager

Puede reiniciar el servidor en un host UNIX utilizando la CLI.

#### Paso

1. Para reiniciar el servidor, introduzca el siguiente comando:

```
smsap_server restart
```

## Desinstale el software desde un host UNIX

Si ya no necesita el software SnapManager, puede desinstalarlo desde el servidor host.

### Pasos

1. Inicie sesión como root.
2. Para detener el servidor, escriba el siguiente comando:

```
smsap_server stop
```

3. Para quitar el software SnapManager, introduzca el siguiente comando:

```
UninstallSmsap
```

4. Después del texto de introducción, pulse **Intro** para continuar.

Se completa la desinstalación.

## Configuración de una notificación por correo electrónico

SnapManager permite recibir una notificación por correo electrónico acerca del estado de finalización de las operaciones de base de datos ejecutadas por perfil. SnapManager genera el correo electrónico y ayuda a realizar la acción adecuada en función del estado de finalización de la operación de la base de datos. La configuración de las notificaciones por correo electrónico es un parámetro opcional.

Puede configurar una notificación por correo electrónico para un perfil individual como notificación de perfil y para varios perfiles en una base de datos de repositorio como notificación de resumen.

### Notificación de perfiles

Para un perfil individual, es posible recibir un correo electrónico para las operaciones de base de datos correctas o fallidas.



De forma predeterminada, la notificación por correo electrónico está habilitada para las operaciones con bases de datos fallidas.

### Notificación de resumen

La notificación de resumen permite recibir un mensaje de correo electrónico resumido sobre las operaciones de la base de datos realizadas mediante varios perfiles. Se pueden habilitar notificaciones por hora, por día, por semana o por mes.



En SnapManager 3.3, las notificaciones de resumen se envían solo si se especifica el servidor host que tiene que enviar la notificación. Si se actualiza SnapManager desde una versión anterior a 3.3, es posible que las notificaciones de resumen no se envíen si no se especificó el servidor host en la configuración de notificaciones de resumen.



Si crea un repositorio en un nodo de una base de datos que se encuentra en un entorno RAC y habilita la notificación de resumen, posteriormente cuando agrega el mismo repositorio a otro nodo de la base de datos, el correo electrónico de notificación de resumen se envía dos veces.

Puede usar notificación a nivel de perfil o notificación de resumen al mismo tiempo.

SnapManager habilita la notificación por correo electrónico para las siguientes operaciones de bases de datos ejecutadas por perfiles:

- Crear backup en el almacenamiento principal
- Restaurar backups
- Crear clones
- Divida los clones
- Verificar backups

Después de crear o actualizar perfiles con la notificación de correo electrónico activada, puede desactivarla. Si deshabilita la notificación por correo electrónico, ya no recibirá alertas por correo electrónico para esas operaciones de base de datos ejecutadas por perfil.

El correo electrónico que recibe contiene los siguientes detalles:

- Nombre de la operación de base de datos, por ejemplo, backup, restauración o clonado
- Nombre de perfil utilizado para la operación de base de datos
- Nombre del servidor host
- Identificador del sistema de la base de datos
- Hora de inicio y finalización de la operación de base de datos
- Estado de la operación de base de datos
- Mensaje de error, si lo hay
- Mensajes de advertencia, si los hay

Puede configurar lo siguiente:

- Servidor de correo para un repositorio
- Notificación por correo electrónico de un nuevo perfil
- Notificación por correo electrónico de un perfil existente
- Notificación por correo electrónico de resumen para varios perfiles en un repositorio



Es posible configurar las notificaciones por correo electrónico desde la interfaz de línea de comandos (CLI) y la interfaz gráfica de usuario (GUI).

## Configurar un servidor de correo para un repositorio

SnapManager permite especificar los detalles del servidor de correo desde los cuales se envían las alertas por correo electrónico.

### Acerca de esta tarea

SnapManager permite especificar el nombre de host o la dirección IP del servidor de correo electrónico del remitente y el número de puerto del servidor de correo electrónico para un nombre de la base de datos de repositorio que requiere la notificación por correo electrónico. Puede configurar el número de puerto del servidor de correo en un intervalo comprendido entre 0 y 65535; el valor predeterminado es 25. Si requiere autenticación para la dirección de correo electrónico, puede especificar el nombre de usuario y la contraseña.

Debe especificar el nombre o la dirección IP del servidor host que maneja la notificación por correo electrónico.

### Paso

1. Para configurar el servidor de correo para que envíe alertas por correo electrónico, escriba el siguiente comando: `smsap notification set -sender-email email_address-mailhost mailhost -mailport mailport [-authentication-username username-password password] -repository-port repo_port-database-name repo_service_name-host repo_host-login -username repo_username`

Las demás opciones para este comando son las siguientes:

`[-force]`

`[-quiet | -verbose]`

Para hacer lo siguiente...	Realice lo siguiente...
<b>Para especificar la dirección de correo electrónico del remitente.</b>	Especifique el <code>-sender-email</code> opción. En SnapManager 3.2 para SAP, puede incluir guión (-) al especificar el nombre de dominio de la dirección de correo electrónico. Por ejemplo, puede especificar la dirección de correo electrónico del remitente como <code>-sender-email user@org-corp.com</code> .
<b>Para especificar el nombre de host o la dirección IP del servidor de correo electrónico del remitente.</b>	Especifique el <code>-mailhost</code> opción.



Para hacer lo siguiente...	Realice lo siguiente...
<b>Especificar el número de puerto del servidor de correo electrónico para un nombre de base de datos de repositorio que requiere notificación por correo electrónico. Puede configurar el número de puerto del servidor de correo en un intervalo comprendido entre cero y 65535; el valor predeterminado es 25.</b>	Especifique el <code>-mailport</code> opción.
<b>Especifique el nombre de usuario y la contraseña si necesita autenticación para la dirección de correo electrónico.</b>	Especifique <code>-authentication</code> opción seguida del nombre de usuario y la contraseña.

En el siguiente ejemplo se configura el servidor de correo.

```
smsap notification set -sender-email admin1@org.com -mailhost
hostname.org.com -mailport 25 authentication -username admin1 -password
admin1 -repository -port 1521 -dbname SMSAPREPO -host hotspur -login
-username grabal21 -verbose
```

## Configurar la notificación por correo electrónico para un nuevo perfil

Cuando se crea un perfil nuevo, se puede configurar para recibir una notificación por correo electrónico al finalizar la operación de la base de datos.

### Lo que necesitará

- Debe configurar la dirección de correo electrónico desde la cual se envían las alertas.
- Debe usar una lista separada por comas para varias direcciones de correo electrónico.

Debe asegurarse de que no hay espacio entre la coma y la siguiente dirección de correo electrónico.

### Paso

1. Introduzca el siguiente comando:

```
smsap profile create -profile profile [-profile-password profile_password]
-repository-database repo_service_name -host repo_host -port repo_port -login
-username repo_username -database -dbname db_dbname -host db_host [-sid
db_sid] [-login-username db_username -password db_password -port db_port] [-
```

```
rman {-controlfile | {-login-username rman_username -password rman_password
-tnsname rman_tnsname} } ] -osaccount osaccount -osgroup osgroup [-retain [-
hourly [-count n] [-duration m]] [-daily [-count n] [-duration m]] [-weekly [-
count n] [-duration m]] [-monthly [-count n] [-duration m]]] [-comment
comment] [-snapname-pattern pattern] [-protect [-protection-policy policy_name
]] [-notification [-success-email email_address1,email_address2 -subject
subject_pattern] [-failure-email email_address1,email_address2 -subject
subject_pattern]]
```

Las demás opciones para este comando son las siguientes:

[-force]

[-quiet | -verbose]



SnapManager admite hasta 1000 caracteres para las direcciones de correo electrónico.

Cuando se crea un backup de archivos de datos y archivos de registro de archivos junto con el perfil (para crear backups de registros de archivos independientes) y se produce un error en la creación del backup de archivos de datos, la notificación por correo electrónico se envía con el backup de datos como nombre de la operación en lugar de un backup de datos y un backup de registros de archivos. Cuando la operación de backup de archivo de datos y archivo de registro de archivo se realiza correctamente, se muestra el resultado de la siguiente manera:

```
Profile Name      : PROF_31
Operation Name    : Data Backup and Archive Logs Backup
Database SID      : TENDB1
Database Host     : rep01.rtp.org.com
Start Date        : Fri Sep 23 13:37:21 EDT 2011
End Date          : Fri Sep 23 13:45:24 EDT 2011
Status            : SUCCESS
Error messages    :
```

En el siguiente ejemplo se muestra la notificación de correo electrónico configurada al crear un nuevo perfil:

```
smsap profile create -profile sales1 -profile-password sales1 -repository
-dbname repo2 -host 10.72.197.133 -port 1521 -login -username oba5
-database -dbname DB1 -host 10.72.197.142 -sid DB1 -osaccount oracle
-osgroup dba -notification -success -email admin1@org.com -subject
{profile}_{operation-name}_{db-sid}_{db-host}_{start-date}_{end-
date}_{status}
```

## Personalice el asunto del correo electrónico para un perfil nuevo

Puede personalizar el asunto del correo electrónico para el nuevo perfil cuando lo cree.

Puede personalizar el asunto del correo electrónico utilizando el patrón {profile}\_{operation-name}\_{db-sid}\_{db-host}\_{start-date}\_{end-date}\_{status} o bien introducir su propio texto.

Nombre de la variable	Descripción	Valor de ejemplo
<i>profile</i>	Nombre de perfil utilizado para la operación de base de datos	PROF1
<i>operation-name</i>	Nombre de la operación de base de datos	Backup, copia de seguridad de datos, copia de seguridad de registros de datos y archivos
<i>db-sid</i>	SID de la base de datos	DB1
<i>db-host</i>	Nombre del servidor host	Hosta
<i>start-date</i>	La hora de inicio de la operación de la base de datos en el formato mdd:hh:ss yyyy	Abril 27 21:00:45 PST 2012
<i>end-date</i>	Hora de finalización de la operación de la base de datos en el formato mdd:hh:ss yyyy	Abril 27 21:10:45 PST 2012
<i>status</i>	Estado de la operación de base de datos	Correcto

Si no se proporciona ningún valor para las variables, SnapManager muestra el siguiente mensaje de error: Missing value(s) -subject.

1. Introduzca el siguiente comando:

```
smsap profile create -profile profile [-profile-password profile_password]
-repository -dbname repo_service_name -host repo_host -portrepo port-login
-username repo_username -database -dbname db_dbname -host db_host [-sid
db_sid] [-login -username db_username -password db_password -port db_port] [-
rman {-controlfile | {-login-username rman_username -password rman_password
-tnsname rman_tnsname} } ] -osaccount osaccount -osgroup osgroup [-retain [-
hourly [-count n] [-duration m]] [-daily [-count n] [-duration m]] [-weekly [-
count n] [-duration m]] [-monthly [-count n] [-duration m]]] [-comment
comment] [-snapname-pattern pattern] [-protect [-protection-policy policy_name]]
[-notification [-success -email email_address1,email_address2 -subject
subject_pattern] [-failure -email email_address1,email_address2 -subject
subject_pattern]]
```

A continuación se muestra un ejemplo que muestra el patrón del asunto del correo electrónico:

```
smsap profile create -profile sales1 -profile-password admin1 -repository
-database repo2 -host 10.72.197.133 -port 1521 -login -username admin2
-database -dbname DB1 -host 10.72.197.142 -sid DB1
-osaccount oracle -osgroup dba -profile-notification -success -email
admin@org.com -subject {profile}_{operation-name}_{db-sid}_{db-
host}_{start-date}_{end-date}_{status}
```

## Configure la notificación por correo electrónico para un perfil existente

Al actualizar un perfil, puede configurar para recibir una notificación por correo electrónico al finalizar la operación de la base de datos.

### Lo que necesitará

- Debe configurar la dirección de correo electrónico desde la cual se envían las alertas.
- Debe introducir una sola dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas.

Puede usar una lista separada por comas para varias direcciones. Debe asegurarse de que no hay espacio entre la coma y la siguiente dirección de correo electrónico. Si lo desea, también puede añadir un asunto al correo electrónico.

### Paso

1. Introduzca el siguiente comando:

```
smsap profile update -profile profile [-profile-password profile_password] [-
database-database db_dbname -host db_host [-sid db_sid] [-login -username
db_username -password db_password -port db_port] [{-rman{-controlfile | {-
login -username rman_username -password rman_password -tnsname rman_tnsname}}]
| -remove-rman]-osaccount osaccount-osgroup osgroup [-retain [-hourly [-count
n] [-duration m]] [-daily [-count n] [-duration m]] [-weekly [-count n] [-
duration m]] [-monthly [-count n] [-duration m]]] [-comment comment][-
snapname-pattern pattern][[-protect [-protection-policy policy_name]]] [[-
noprotect]] [-notification [-success-email email_address1,email_address2
-subject subject_pattern] [-failure-email email_address1,email_address2
-subject subject_pattern]]
```

La opción Success se puede utilizar para recibir una notificación únicamente sobre las operaciones de base de datos correctas y la opción Failure para recibir una notificación solo sobre las operaciones de base de datos fallidas.

### Personalice el asunto del correo electrónico de un perfil existente

SnapManager le permite personalizar el patrón de asunto del correo electrónico para un perfil existente actualizando dicho perfil. Este patrón de asunto personalizado sólo es aplicable al perfil actualizado.

## Paso

1. Introduzca el siguiente comando:

```
smsap profile update -profile profile [-profile-password profile_password] [-  
database -dbname db_dbname -host db_host [-sid db_sid] [-login -username  
db_username -password db_password -port db_port]] [{"-rman{-controlfile | {-  
login -username rman_username -password rman_password -tnsname rman_tnsname}}}  
| -remove-rman]-osaccount osaccount -osgroup osgroup [-retain [-hourly [-count  
n] [-duration m]] [-daily [-count n] [-duration m]] [-weekly [-count n] [-  
duration m]] [-monthly [-count n] [-duration m]]] [-comment comment] [-  
snapname-pattern pattern][[-protect [-protection-policy policy_name]] | [-  
noprotect]] [-notification [-success-email email_address1,email_address2  
-subject subject_pattern] [-failure-email email_address1,email_address2  
-subject subject_pattern]]
```

En el siguiente ejemplo se muestra un patrón de asunto del correo electrónico:

```
smsap profile update -profile sales1 -profile-password sales1 -repository  
-dbname repo2 -host 10.72.197.133 -port 1521 -login -username admin2  
-database -dbname DB1 -host 10.72.197.142 -sid DB1  
-osaccount oracle -osgroup dba -profile-notification -success -email  
admin@org.com -subject {profile}_{operation-name}_{db-sid}_{db-  
host}_{start-date}_{end-date}_{status}
```

## Configurar la notificación de resumen por correo electrónico para varios perfiles

SnapManager permite configurar una notificación por correo electrónico de resumen para varios perfiles en una base de datos de repositorio.

### Acerca de esta tarea

Es posible configurar el host del servidor SnapManager como host de notificación desde el cual se envía el correo electrónico de notificación de resumen a los destinatarios. Si se cambian el nombre de host o la dirección IP del servidor SnapManager, también se puede actualizar el host de notificación.

Puede seleccionar cualquiera de las horas de programación en las que se requiera una notificación por correo electrónico:

- Hourly: Para recibir una notificación por correo electrónico cada hora
- Diario: Para recibir una notificación por correo electrónico diariamente
- Semanal: Para recibir una notificación por correo electrónico semanalmente
- Mensual: Recibir una notificación por correo electrónico mensualmente

Debe introducir una sola dirección de correo electrónico o una lista de direcciones de correo electrónico separadas por comas para recibir notificaciones de las operaciones realizadas mediante dichos perfiles.

Asegúrese de que no haya espacio entre la coma y la siguiente dirección de correo electrónico cuando introduzca varias direcciones de correo electrónico.

SnapManager le permite añadir un asunto de correo electrónico personalizado utilizando las siguientes variables:

- Nombre de perfil utilizado para la operación de base de datos.
- Nombre de la base de datos
- SID de la base de datos
- Nombre del servidor host
- Hora de inicio de la operación de la base de datos en el formato `yyyymmdd:hh:ss`
- Hora de finalización de la operación de la base de datos en el formato `yyyymmdd:hh:ss`
- Estado de la operación de base de datos

Si selecciona no agregar un asunto personalizado, SnapManager muestra un mensaje de error: `Missing value -subject`.

1. Introduzca el siguiente comando:

```
smsap notification update-summary-notification -repository -port repo_port
-dbname repo_service_name -host repo_host -login-username repo_username -email
email_address1,email_address2 -subject subject-pattern -frequency {-daily-time
daily_time | -hourly-time hourly_time | -monthly-time monthly_time -date {1
|2...|31} | -weekly-time weekly_time -day {1 |2 |3 |4 |5 |6 |7}} -profiles
profile1 profile2 -notification-host notification-host
```

Las demás opciones para este comando son las siguientes:

```
[-force] [-noprompt]
```

```
[-quiet | -verbose]
```

```
smsap notification update-summary-notification -repository -port 1521
-dbname repo2 -host 10.72.197.133 -login -username oba5 -email-address
admin@org.com -subject success -frequency -daily -time 19:30:45 -profiles
sales1 -notification-host wales
```

## Añada un nuevo perfil a las notificaciones por correo electrónico de resumen

Después de configurar una notificación por correo electrónico de resumen para la base de datos de repositorio, puede agregar un nuevo perfil a la notificación de resumen utilizando el comando `summary notification`.

### Paso

1. Introduzca el siguiente comando:

```
smsap profile create -profile profile_name [-profile-password profile_password] -repository-database repo_service_name -host repo_host -port repo_port -login-username repo_username -database -dbname db_dbname -host db_host [-siddb_sid] [-login-username db_username -password db_password -port db_port] [-rman {-controlfile | \{-login-username rman_username -password rman_password -tnsname rman_tnsname} } ] -osaccount osaccount -osgroup osgroup [-retain [-hourly-count n] [-duration m]] [-daily-count n] [-duration m]] [-weekly-count n] [-duration m]] [-monthly-count n] [-duration m]] [-comment comment] [-snapname-pattern pattern] [-protect [-protection-policy policy_name]] [-summary-notification]
```

Las demás opciones para este comando son las siguientes:

```
[-force]
```

```
[-quiet | -verbose]
```

## Agregue un perfil existente a las notificaciones de correo electrónico de resumen

SnapManager le permite añadir un perfil existente a una notificación de correo electrónico de resumen al actualizar dicho perfil.

### Paso

1. Introduzca el siguiente comando:

```
smsap profile update -profile profile_name [-profile-password profile_password] -repository-database repo_service_name -host repo_host -port repo_port -login-username repo_username -database -dbname db_dbname -host db_host [-siddb_sid] [-login-username db_username -password db_password -port db_port] [-rman {-controlfile | {-login-username rman_username -password rman_password -tnsname rman_tnsname} } ] -osaccount osaccount -osgroup osgroup [-retain [-hourly-count n] [-duration m]] [-daily-count n] [-duration m]] [-weekly-count n] [-duration m]] [-monthly-count n] [-duration m]] [-comment comment] [-snapname-pattern pattern] [-protect [-protection-policy policy_name]] [-summary-notification]
```

## Desactive la notificación por correo electrónico para varios perfiles

Después de activar la notificación de resumen por correo electrónico para varios perfiles, puede desactivarlos para que ya no reciban alertas por correo electrónico.

### Acercas de esta tarea

SnapManager permite deshabilitar la notificación de resumen por correo electrónico para esas operaciones de la base de datos ejecutadas por perfil. Desde la CLI de SnapManager, introduzca el `notification remove-summary-notification` comando para deshabilitar la notificación por correo electrónico de resumen de varios perfiles y el nombre de la base de datos del repositorio para la cual no se requiere la notificación por correo electrónico.

## Paso

1. Para deshabilitar la notificación de resumen de varios perfiles en una base de datos de repositorio, escriba el siguiente comando:

```
smsap notification remove-summary-notification -repository -port repo_port  
-dbname repo_service_name -host repo_host -login-username repo_username
```

En el siguiente ejemplo se muestra la desactivación de la notificación de resumen para varios perfiles en una base de datos de repositorio:

```
smsap notification remove-summary-notification -repository -port 1521  
-dbname repo2 -host 10.72.197.133 -login -username oba5
```

## Creación de archivos de especificación de tareas y secuencias de comandos para operaciones de SnapManager

SnapManager para SAP utiliza un archivo XML (lenguaje de marcado extensible) de la especificación de tareas que indica las tareas previas y las tareas posteriores para las operaciones de copia de seguridad, restauración y clonado. Es posible añadir los nombres de las tareas previas y las secuencias de comandos posteriores a las tareas en el archivo XML para que las tareas se realicen antes o después de las operaciones de backup, restauración y clonado.

En SnapManager (3.1 o anterior), puede ejecutar los scripts de tareas previas y posteriores a la tarea solo para la operación de clonado. En SnapManager (3.2 o posterior) para SAP, puede ejecutar las secuencias de comandos previas y posteriores a las tareas para las operaciones de backup, restauración y clonado.

En SnapManager (3.1 o anterior), la sección de especificación de tareas forma parte del archivo XML de especificación del clon. Desde SnapManager 3.2 para SAP, la sección de especificación de tareas es un archivo XML independiente.



SnapManager 3.3 o versiones posteriores no admiten el uso del archivo XML de especificación del clon creado en las versiones anteriores a SnapManager 3.2.

En SnapManager (3.2 o posterior) para SAP, debe asegurarse de que se cumplan las siguientes condiciones para efectuar correctamente las operaciones de SnapManager:

- Para las operaciones de copia de seguridad y restauración, utilice el archivo XML de especificación de tareas.
- Para la operación de clonado, proporcione dos archivos de especificación: Un archivo XML de especificación del clon y un archivo XML de especificación de tareas.

Si desea habilitar la actividad de tareas previas o posteriores a la tarea, también puede agregar el archivo



XML de especificación de tareas.

Puede crear el archivo de especificación de la tarea mediante la interfaz gráfica de usuario (GUI) de SnapManager, la interfaz de línea de comandos (CLI) o un editor de texto. Debe utilizar una extensión .xml para el archivo con el fin de habilitar las características de edición adecuadas. Puede guardar este archivo para usarlo para operaciones de backup, restauración y clonado futuras.

El archivo XML de especificación de tareas incluye dos secciones:

- La sección de tareas previas incluye scripts que se pueden ejecutar antes de las operaciones de backup, restauración y clonado.
- La sección tareas posteriores incluye scripts que se pueden ejecutar después de las operaciones de backup, restauración y clonado.

Los valores incluidos en las secciones de tareas previas y tareas posteriores deben cumplir las siguientes directrices:

- Nombre de la tarea: El nombre de la tarea debe coincidir con el nombre del script, que se muestra cuando se ejecuta el `plugin.sh -describe comando`.



Si hay un error de coincidencia, es posible que reciba el siguiente mensaje de error: `the file not found`.

- Nombre del parámetro: El nombre del parámetro debe ser una cadena que se puede utilizar como valor de variable de entorno.

La cadena debe coincidir con el nombre del parámetro en el script personalizado, que se muestra al ejecutar el `plugin.sh -describe comando`.

Puede crear el archivo de especificación según la estructura del siguiente archivo de especificación de tareas de ejemplo:

```

<task-specification>
  <pre-tasks>
<task>
  <name>name</name>
  <parameter>
    <name>name</name>
    <value>value</value>
  </parameter>
</task>
</pre-tasks>
<post-tasks>
  <task>
    <name>name</name>
    <parameter>
      <name>name</name>
      <value>value</value>
    </parameter>
  </task>
</post-tasks>
</task-specification>

```



El archivo XML de especificación de tareas no debe contener ninguna directiva.

En la interfaz gráfica de usuario de SnapManager, es posible establecer el valor del parámetro y guardar el archivo XML. Puede utilizar la página activación de tareas del asistente Crear copia de seguridad, del asistente Restaurar o recuperación y del asistente Crear copia de seguridad, para cargar el archivo XML de especificación de tareas existente y utilizar el archivo seleccionado para la actividad de tareas previas o posteriores a la tarea.

Una tarea se puede ejecutar varias veces, ya sea con combinaciones de parámetros y valores iguales o diferentes. Por ejemplo, puede utilizar una tarea Guardar para guardar varios archivos.



SnapManager utiliza las etiquetas XML que se proporcionan en el archivo de especificación de tareas para el procesamiento previo o la actividad de posprocesamiento para las operaciones de backup, restauración y clonado, independientemente de la extensión del archivo de especificación de la tarea.

## Crear scripts de tareas previas, tareas posteriores y directivas

SnapManager le permite crear los scripts para la actividad de procesamiento previo, la actividad de procesamiento posterior y las tareas de políticas de las operaciones de backup, restauración y clonado. Debe colocar los scripts en el directorio de instalación correcto para ejecutar la actividad de preprocesamiento, la actividad de posprocesamiento y las tareas de política de la operación de SnapManager.

### Acerca de esta tarea

## Contenido de secuencias de comandos de tareas previas y posteriores

Todos los scripts deben incluir lo siguiente:

- Operaciones específicas (comprobación, descripción y ejecución)
- (Opcional) variables de entorno predefinidas
- Código de manejo de errores específico (código de retorno (rc))



Debe incluir el código de gestión de errores correcto para validar el script.

Puede utilizar los scripts de tareas previas para muchos fines, por ejemplo, limpiar un espacio en disco antes de que se inicie la operación SnapManager. También puede utilizar los scripts posteriores a la tarea, por ejemplo, para calcular si SnapManager tiene espacio en disco suficiente para completar la operación.

## Contenido de secuencias de comandos de tareas de directiva

Puede ejecutar el script de directivas sin utilizar operaciones específicas como comprobar, describir y ejecutar. El script incluye las variables de entorno predefinidas (opcionales) y el código de gestión de errores específico.

El script de política se ejecuta antes de las operaciones de backup, restauración y clonado.

## Formato admitido

Se puede usar un archivo de script de shell con extensión .sh como script previo y posterior.

## Guía de instalación de script

El directorio en el que se instala la secuencia de comandos afecta al modo en que se utiliza. Es posible colocar los scripts en el directorio y ejecutar el script antes o después de que se lleve a cabo la operación de backup, restauración o clonado. Debe colocar el script en el directorio especificado en la tabla y utilizarlo de forma opcional al especificar la operación de backup, restauración o clonado.



Debe asegurarse de que el directorio plugins tenga el permiso ejecutable antes de utilizar los scripts para la operación SnapManager.

Actividad	Backup	Restaurar	Clonar
Preprocesamiento	<default_installation_directory>/plugins/backup/crear/pre	<default_installation_directory>/plugins/restore/create/pre	<default_installation_directory>/plugins/clone/create/pre
Procesamiento posterior	<default_installation_directory>/plugins/backup/creación/publicación	<default_installation_directory>/plugins/restore/create/post	<default_installation_directory>/plugins/clone/create/post
Basado en políticas	<default_installation_directory>/plugins/backup/creación/política	<default_installation_directory>/plugins/restore/create/policy	<default_installation_directory>/plugins/clone/create/policy

## Ubicación de secuencias de comandos de ejemplo

A continuación se muestran algunos ejemplos de los scripts de tareas previas y posteriores a las tareas para las operaciones de backup y clonado disponibles en la ruta de acceso del directorio de instalación:

- `<default_installation_directory>/plugins/ejemplos/backup/create/pre`
- `<default_installation_directory>/plugins/ejemplos/backup/creación/publicación`
- `<default_installation_directory>/plugins/ejemplos/clon/creación/previo`
- `<default_installation_directory>/plugins/ejemplos/clon/creación/publicación`

### Qué puede cambiar en el script

Si crea un nuevo script, sólo puede cambiar las operaciones describir y ejecutar. Cada script debe contener las siguientes variables: `context`, `timeout`, y `parameter`.

Las variables descritas en la función describir del script deben declararse al inicio del script. Puede añadir nuevos valores de parámetros en `parameter=()` y, a continuación, utilice los parámetros de la función `execute`.

### Guión de muestra

A continuación se muestra un script de ejemplo con un código de retorno especificado por el usuario para calcular el espacio en el host SnapManager:

```
#!/bin/bash
# $Id:
//depot/prod/capstan/main/src/plugins/unix/examples/backup/create/pre/disk
_space_estimate.sh#5 $
name="disk space estimation ($(basename $0))"
description="pre tasks for estimating the space on the target system"
context=
timeout="0"
parameter=()
EXIT=0
PRESERVE_DIR="/tmp/preserve/$(date +%Y%m%d%H%M%S)"
function _exit {
    rc=$1
    echo "Command complete."
    exit $rc
}
function usage {
    echo "usage: $(basename $0) { -check | -describe | -execute }"
    _exit 99
}
function describe {
    echo "SM_PI_NAME:$name"
    echo "SM_PI_DESCRIPTION:$description"
    echo "SM_PI_CONTEXT:$context"
```

```

echo "SM_PI_TIMEOUT:$timeout"
IFS=^
for entry in ${parameter[@]}; do
    echo "SM_PI_PARAMETER:$entry"
done
_exit 0
}
function check {
    _exit 0
}
function execute {
    echo "estimating the space on the target system"
    # Shell script to monitor or watch the disk space
    # It will display alert message, if the (free available) percentage
    # of space is >= 90%
    #
-----
    # Linux shell script to watch disk space (should work on other UNIX
oses )
    # set alert level 90% is default
    ALERT=90
    df -H | grep -vE '^Filesystem|tmpfs|cdrom' | awk '{ print $5 " " " $1
}' | while read output;
    do
        #echo $output
        usep=$(echo $output | awk '{ print $1}' | cut -d'%' -f1 )
        partition=$(echo $output | awk '{ print $2 }' )
        if [ $usep -ge $ALERT ]; then
            echo "Running out of space \"$partition ($usep%)\", on
$(hostname) as on $(date)" |
        fi
    done
    _exit 0
}
function preserve {
    [ $# -ne 2 ] && return 1
    file=$1
    save=$(echo ${2:0:1} | tr [a-z] [A-Z])
    [ "$save" == "Y" ] || return 0
    if [ ! -d "$PRESERVE_DIR" ] ; then
        mkdir -p "$PRESERVE_DIR"
        if [ $? -ne 0 ] ; then
            echo "could not create directory [$PRESERVE_DIR]"
            return 1
        fi
    fi
}

```

```

    if [ -e "$file" ] ; then
        mv "$file" "$PRESERVE_DIR/."
    fi
    return $?
}
case $(echo $1 | tr [A-Z] [a-z]) in
    -check)    check
                ;;
    -execute)  execute
                ;;
    -describe) describe
                ;;
    *)        echo "unknown option $1"
                usage
                ;;
esac

```

## Operaciones en scripts de tareas

Las secuencias de comandos de tareas previas o posteriores a las tareas que cree deben seguir una estructura de complemento SnapManager para SAP estándar.

Las secuencias de comandos de tareas previas y posteriores deben incluir las siguientes operaciones:

- comprobar
- describa
- ejecución

Si alguna de estas operaciones no se especifica en la secuencia de comandos de tareas previas o posteriores, la secuencia de comandos no será válida.

Cuando ejecute el `smsap plugin check` comando para las secuencias de comandos de tareas previas o posteriores, el estado devuelto de las secuencias de comandos muestra un error (porque el valor de estado devuelto no es cero).

Funcionamiento	Descripción
comprobar	El servidor SnapManager ejecuta el <code>plugin.sh -check</code> comando para garantizar que el sistema tenga permiso de ejecución en los scripts del plugin. También es posible incluir la comprobación de permisos de archivos en el sistema remoto.

Funcionamiento	Descripción
describe	<p>El servidor SnapManager ejecuta el <code>plugin.sh -describe</code> para obtener información acerca del script y hacer coincidir los elementos proporcionados por el archivo de especificación. El script de un plugin debe contener la siguiente información de descripción:</p> <ul style="list-style-type: none"> <li>• <code>SM_PI_NAME</code>: Nombre de script. Debe introducir un valor para este parámetro.</li> <li>• <code>SM_PI_DESCRIPTION</code>: Descripción del propósito del script. Debe introducir un valor para este parámetro.</li> <li>• <code>SM_PI_CONTEXT</code>: Contexto en el que se debe ejecutar la secuencia de comandos, por ejemplo, <code>root</code> u <code>orasisd</code>. Debe introducir un valor para este parámetro.</li> <li>• <code>SM_PI_TIMEOUT</code>: El tiempo máximo (en milisegundos) que SnapManager debe esperar a que el script complete el procesamiento y finalice la ejecución. Debe introducir un valor para este parámetro.</li> <li>• <code>SM_PI_PARAMETER</code>: Uno o varios parámetros personalizados necesarios para que la secuencia de comandos del plugin realice el procesamiento. Cada parámetro debe aparecer en una nueva línea de salida e incluir el nombre del parámetro y una descripción. Cuando el script finalice el procesamiento, una variable de entorno proporcionará al script el valor del parámetro.</li> </ul> <p>A continuación se muestra la salida de ejemplo de la secuencia de comandos <code>Followup_Activities</code>.</p> <pre style="background-color: #f0f0f0; padding: 10px;"> plugin.sh - describe  SM_PI_NAME:Followup_activities SM_PI_DESCRIPTION:this script contains follow-up activities to be executed after the clone create operation. SM_PI_CONTEXT:root SM_PI_TIMEOUT:60000 SM_PI_PARAMETER:SCHEMAOWNER:Name of the database schema owner. Command complete.</pre>
ejecución	<p>El servidor SnapManager ejecuta el <code>plugin.sh -execute</code> para iniciar la secuencia de comandos para ejecutar la secuencia de comandos.</p>

### Variables disponibles en los scripts de tareas para la operación de backup

SnapManager proporciona información de contexto en forma de variables de entorno relacionadas con la operación de backup que se realiza. Por ejemplo, el script puede recuperar el nombre del host original, el nombre de la política de retención y la etiqueta del backup.

En la siguiente tabla, se enumeran las variables de entorno que se pueden utilizar en los scripts:

<b>Variables</b>	<b>Descripción</b>	<b>Formato</b>
<i>SM_OPERATION_ID</i>	Especifica el ID de la operación actual	cadena
<i>SM_PROFILE_NAME</i>	Especifica el nombre del perfil utilizado	cadena
<i>SM_SID</i>	Especifica el identificador del sistema de la base de datos	cadena
<i>SM_HOST</i>	Especifica el nombre de host de la base de datos	cadena
<i>SM_OS_USER</i>	Especifica el propietario del sistema operativo (SO) de la base de datos	cadena
<i>SM_OS_GROUP</i>	Especifica el grupo del sistema operativo de la base de datos	cadena
<i>SM_BACKUP_TYPE</i>	Especifica el tipo de backup (en línea, sin conexión o automático)	cadena
<i>SM_BACKUP_LABEL</i>	Especifica la etiqueta del backup	cadena
<i>SM_BACKUP_ID</i>	Especifica el ID del backup	cadena
<i>SM_BACKUP_RETENTION</i>	Especifica el período de retención	cadena
<i>SM_BACKUP_PROFILE</i>	Especifica el perfil utilizado para esta copia de seguridad	cadena
<i>SM_ALLOW_DATABASE_SHUTDOWN</i>	Especifica si desea iniciar o cerrar la base de datos Si es necesario puede utilizar la opción -force de la interfaz de línea de comandos.	booleano
<i>SM_BACKUP_SCOPE</i>	Especifica el ámbito del backup (completo o parcial)	cadena
<i>SM_BACKUP_PROTECTION</i>	Especifica si la protección de backup está habilitada	booleano
<i>SM_TARGET_FILER_NAME</i>	Especifica el nombre del sistema de almacenamiento de destino  <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;">  Si se utiliza más de un sistema de almacenamiento, los nombres de los sistemas de almacenamiento deben separarse con comas. </div>	cadena



<b>Variables</b>	<b>Descripción</b>	<b>Formato</b>
<i>SM_TARGET_VOLUME_NAME</i>	<p>Especifica el nombre del volumen objetivo</p> <p> El nombre del volumen de destino debe estar precedido por el nombre del dispositivo de almacenamiento, por ejemplo, <i>SM_TARGET_FILER_NAME/SM_TARGET_VOLUME_NAME</i>.</p>	cadena
<i>SM_HOST_FILE_SYSTEM</i>	<p>Especifica el sistema de archivos del host</p>	cadena
<i>SM_SNAPSHOT_NAMES</i>	<p>Especifica la lista Snapshot</p> <p> El nombre de las copias de Snapshot debe prefijarse con el nombre del sistema de almacenamiento y el nombre del volumen. Los nombres de las copias Snapshot están separados por comas.</p>	matriz de cadenas
<i>SM_ARCHIVE_LOGS_DIRECTORY</i>	<p>Especifica el directorio de registros de archivos</p> <p> Si los registros de archivos se encuentran en más de un directorio, los nombres de esos directorios se separan con comas.</p>	matriz de cadenas
<i>SM_REDO_LOGS_DIRECTORY</i>	<p>Especifica el directorio redo logs</p> <p> Si los redo logs se encuentran en más de un directorio, los nombres de esos directorios se separan con comas.</p>	matriz de cadenas
<i>SM_CONTROL_FILES_DIRECTORY</i>	<p>Especifica el directorio de archivos de control</p> <p> Si los archivos de control se encuentran en más de un directorio, los nombres de esos directorios se separan con comas.</p>	matriz de cadenas
<i>SM_DATA_FILES_DIRECTORY</i>	<p>Especifica el directorio de archivos de datos</p> <p> Si los archivos de datos se encuentran en más de un directorio, los nombres de esos directorios se separan con comas.</p>	matriz de cadenas

<b>Variables</b>	<b>Descripción</b>	<b>Formato</b>
<i>user_defined</i>	Especifica parámetros adicionales definidos por el usuario. Los parámetros definidos por el usuario no están disponibles para los plugins que se usan como políticas.	definido por el usuario



### Variables disponibles en los scripts de tareas para la operación de restauración

SnapManager proporciona información de contexto en la forma de variables de entorno relacionadas con la operación de restauración que se está realizando. Por ejemplo, el script puede recuperar el nombre del host original y la etiqueta del backup que se restaura.

En la siguiente tabla, se enumeran las variables de entorno que se pueden utilizar en los scripts:

<b>Variables</b>	<b>Descripción</b>	<b>Formato</b>
<i>SM_OPERATION_ID</i>	Especifica el ID de la operación actual	cadena
<i>SM_PROFILE_NAME</i>	Especifica el nombre del perfil utilizado	cadena
<i>SM_HOST</i>	Especifica el nombre de host de la base de datos	cadena
<i>SM_OS_USER</i>	Especifica el propietario del sistema operativo (SO) de la base de datos	cadena
<i>SM_OS_GROUP</i>	Especifica el grupo del sistema operativo de la base de datos	cadena
<i>SM_BACKUP_TYPE</i>	Especifica el tipo de backup (en línea, sin conexión o automático)	cadena
<i>SM_BACKUP_LABEL</i>	Especifica la etiqueta de backup	cadena
<i>SM_BACKUP_ID</i>	Especifica el ID del backup	cadena
<i>SM_BACKUP_PROFILE</i>	Especifica el perfil utilizado para el backup	cadena
<i>SM_RECOVERY_TYPE</i>	Especifica la información de configuración de recuperación	cadena
<i>SM_VOLUME_RESTORE_MODE</i>	Especifica la configuración de restauración de volúmenes	cadena

<b>Variables</b>	<b>Descripción</b>	<b>Formato</b>
<i>SM_TARGET_FILER_NAME</i>	<p>Especifica el nombre del sistema de almacenamiento de destino</p> <p> Si se utiliza más de un sistema de almacenamiento, los nombres de los sistemas de almacenamiento deben separarse con comas.</p>	cadena
<i>SM_TARGET_VOLUME_NAME</i>	<p>Especifica el nombre del volumen objetivo</p> <p> El nombre del volumen de destino debe estar precedido por el nombre del dispositivo de almacenamiento, por ejemplo, SM_TARGET_FILER_NAME/SM_TARGET_VOLUME_NAME.</p>	cadena
<i>SM_HOST_FILE_SYSTEM</i>	<p>Especifica el sistema de archivos del host</p>	cadena
<i>SM_SNAPSHOT_NAMES</i>	<p>Especifica la lista Snapshot</p> <p> El nombre de las copias de Snapshot debe prefijarse con el nombre del sistema de almacenamiento y el nombre del volumen. Los nombres de las copias Snapshot están separados por comas.</p>	matriz de cadenas
<i>SM_ARCHIVE_LOGS_DIRECTORY</i>	<p>Especifica el directorio de registros de archivos</p> <p> Si los registros de archivos se encuentran en más de un directorio, los nombres de esos directorios se separan con comas.</p>	matriz de cadenas
<i>SM_REDO_LOGS_DIRECTORY</i>	<p>Especifica el directorio redo logs</p> <p> Si los redo logs se encuentran en más de un directorio, los nombres de esos directorios se separan con comas.</p>	matriz de cadenas

Variables	Descripción	Formato
<i>SM_CONTROL_FILES_DIRECTORY</i>	<p>Especifica el directorio de archivos de control</p> <p> Si los archivos de control se encuentran en más de un directorio, los nombres de esos directorios se separan con comas.</p>	matriz de cadenas
<i>SM_DATA_FILES_DIRECTORY</i>	<p>Especifica el directorio de archivos de datos</p> <p> Si los archivos de datos se encuentran en más de un directorio, los nombres de esos directorios se separan con comas.</p>	matriz de cadenas

### Variables disponibles en los scripts de tareas para la operación de clonado

SnapManager proporciona información de contexto en forma de variables de entorno relacionadas con la operación de clonado que se realiza. Por ejemplo, el script puede recuperar el nombre del host original, el nombre de la base de datos clonada y la etiqueta del backup.

En la siguiente tabla, se enumeran las variables de entorno que se pueden utilizar en los scripts:

Variables	Descripción	Formato
<i>SM_ORIGINAL_SID</i>	SID de la base de datos original	cadena
<i>SM_ORIGINAL_HOST</i>	Nombre de host asociado con la base de datos original	cadena
<i>SM_ORIGINAL_OS_USER</i>	Propietario del sistema operativo de la base de datos original	cadena
<i>SM_ORIGINAL_OS_GROUP</i>	Grupo del sistema operativo de la base de datos original	cadena
<i>SM_TARGET_SID</i>	SID de la base de datos del clon	cadena
<i>SM_TARGET_HOST</i>	Nombre del host asociado con la base de datos del clon	cadena
<i>SM_TARGET_OS_USER</i>	Propietario del sistema operativo de la base de datos clonada	cadena

<b>Variables</b>	<b>Descripción</b>	<b>Formato</b>
<i>SM_TARGET_OS_GROUP</i>	Grupo del sistema operativo de la base de datos clonada	cadena
<i>SM_TARGET_DB_PORT</i>	Puerto de la base de datos de destino	entero
<i>SM_TARGET_GLOBAL_DB_NAME</i>	Nombre de la base de datos global de la base de datos de destino	cadena
<i>SM_BACKUP_LABEL</i>	Etiqueta del backup utilizado para el clon	cadena

### **Error al manejar en scripts personalizados**

SnapManager procesa la secuencia de comandos personalizada según los códigos de retorno específicos. Por ejemplo, si el script personalizado devuelve el valor 0, 1, 2 o 3, SnapManager continúa con el proceso de clonado. El código de retorno también influye en el modo en que SnapManager procesa y devuelve la salida estándar de la ejecución de la secuencia de comandos.

<b>Código de retorno</b>	<b>Descripción</b>	<b>Continúe procesando la operación</b>
0	El script se ha completado correctamente.	Sí
1	El script se ha completado correctamente, con mensajes informativos.	Sí
2	La secuencia de comandos se ha completado, pero incluye advertencias	Sí
3	La secuencia de comandos falla, pero la operación continúa.	Sí
4 o >4	El script falla y la operación se detiene.	No

### **Ver scripts de plugins de muestra**

SnapManager incluye scripts que puede utilizar como ejemplos para crear sus propios scripts o como base para sus scripts personalizados.

#### **Acerca de esta tarea**

Puede encontrar los scripts de plugins de muestra en la siguiente ubicación:

- `<default_install_directory>/plugins/examples/backup/create`

- <default\_install\_directory>/plugins/examples/clone/create
- <default\_install\_directory>/plugins/unix/examples/backup/create/post

El directorio que contiene los scripts de plug-in de ejemplo incluye los siguientes subdirectorios:

- **policy:** Contiene secuencias de comandos que, cuando se configuran, siempre se ejecutan en la operación de clonación.
- **pre:** Contiene secuencias de comandos que, cuando se configuran, se ejecutan antes de la operación de clonación.
- **post:** Contiene secuencias de comandos que, cuando se configuran, se ejecutan después de la operación de clonación.

En la siguiente tabla se describen los scripts de ejemplo:

Nombre de script	Descripción	Tipo de script
validate_sid.sh	<p>Contiene comprobaciones adicionales al SID utilizado en el sistema de destino. La secuencia de comandos comprueba que el SID tenga las siguientes características:</p> <ul style="list-style-type: none"> <li>• Contiene tres caracteres alfanuméricos</li> <li>• Comienza con una letra</li> <li>• No incluye SIDS de SAP reservados</li> </ul>	Política
cleanup.sh	Borra el sistema de destino de modo que esté listo para almacenar el clon recién creado. Conserva o elimina archivos y directorios en función de la necesidad.	Pretask
sap_follow_up_activities.sh	Realiza tareas de seguimiento de las actividades descritas en <i>SAP System Copy Guide</i> y TR-3442, SAP con Oracle en UNIX y NFS y NetApp Storage. Por ejemplo, este script elimina o modifica las entradas de tabla del esquema SAP.	Postarea
os_db_authentication.sh	Adapta la autenticación del sistema operativo para el usuario OPS\$, como se recomienda en la nota SAP 316641. Este es un ejemplo de cómo procesar archivos SQL externos.	Postarea
Mirror_the_backup.sh	Refleja los volúmenes después de que la operación de backup se produzca en un entorno UNIX cuando se utiliza Data ONTAP en 7-Mode o Clustered Data ONTAP.	Postarea
Vault_the_backup_cDOT.sh	Almacena el backup después de que se produzca la operación de backup en un entorno UNIX cuando utiliza Clustered Data ONTAP.	Postarea

Los scripts suministrados con SnapManager utilizan el shell BASH de forma predeterminada. Debe asegurarse de que el soporte para el shell BASH está instalado en su sistema operativo antes de intentar ejecutar cualquiera de los scripts de ejemplo.

## Pasos

1. Para verificar que está utilizando el shell BASH, introduzca el siguiente comando en el símbolo del sistema:

```
bash
```

Si no ve un error, el shell BASH está funcionando correctamente.

De forma alternativa, puede introducir la `which-bash` en el símbolo del sistema.

2. Busque el script en el siguiente directorio:

```
<installdir>/plugins/examples/clone/create
```

3. Abra el script en un editor de secuencia de comandos como `vi`.

---

## Guión de muestra

El siguiente script personalizado de muestra valida los nombres de SID de base de datos y evita que los nombres no válidos se usen en la base de datos clonada. Incluye tres operaciones (comprobación, descripción y ejecución), a las que se llama después de ejecutar el script. La secuencia de comandos también incluye el manejo de mensajes de error con los códigos 0, 4 y >4.

```
EXIT=0
name="Validate SID"
description="Validate SID used on the target system"
parameter=()

# reserved system IDs
INVALID_SIDS=("ADD" "ALL" "AND" "ANY" "ASC"
             "COM" "DBA" "END" "EPS" "FOR"
             "GID" "IBM" "INT" "KEY" "LOG"
             "MON" "NIX" "NOT" "OFF" "OMS"
             "RAW" "ROW" "SAP" "SET" "SGA"
             "SHG" "SID" "SQL" "SYS" "TMP"
             "UID" "USR" "VAR")

function _exit {
    rc=$1
    echo "Command complete."
    return $rc}

function usage {
    echo "usage: $(basename $0) { -check | -describe | -execute }"
    _exit 99}

function describe {
    echo "SM_PI_NAME:$name"
```

```

    echo "SM_PI_DESCRIPTION:$description"
    _exit 0}

function check {
    _exit 0}

function execute {
    IFS=\$ myEnv=$(env)
    for a in ${parameter[@]}; do
        key=$(echo ${$a} | awk -F':' '{ print $1 }')
        val=$(echo $myEnv | grep -i -w $key 2>/dev/null | awk -F=' ' '{
print $2 }')

        if [ -n "$val" ] ; then
            state="set to $val"
        else
            state="not set"
            #indicate a FATAL error, do not continue processing
            ((EXIT+=4))
        fi
        echo "parameter $key is $state"
    done

#####
# additional checks
# Use SnapManager environment variable of SM_TARGET_SID

    if [ -n "$SM_TARGET_SID" ] ; then
        if [ ${#SM_TARGET_SID} -ne 3 ] ; then
            echo "SID is defined as a 3 digit value, [$SM_TARGET_SID] is not
valid."
            EXIT=4
        else
            echo "${INVALID_SIDS[@]}" | grep -i -w $SM_TARGET_SID >/dev/null
2>&1

                if [ $? -eq 0 ] ; then
                    echo "The usage of SID [$SM_TARGET_SID] is not supported by
SAP."

                        ((EXIT+=4))
                    fi
                fi
            else
                echo "SM_TARGET_SID not set"
                EXIT=4
            fi
        _exit $EXIT}

```



```
# Include the 3 required operations for clone plugin
case $(echo "$1" | tr [A-Z] [a-z]) in
  -check )      check      ;;
  -describe )   describe   ;;
  -execute )    execute    ;;      * )
              echo "unknown option $1"  usage      ;;
esac
```

## Información relacionada

["SAP con Oracle en UNIX y NFS y almacenamiento de NetApp: TR-3442"](#)

## Crear scripts de tareas

Es posible crear los scripts de tareas previas, posteriores a tareas y de políticas para operaciones de backup, restauración y clonado, escribir el script e incluir las variables de entorno predefinidas en los parámetros. Es posible crear un nuevo script o modificar uno de los scripts de ejemplo de SnapManager.

### Lo que necesitará

Antes de comenzar a crear el script, asegúrese de lo siguiente:

- Es necesario estructurar el script de un modo determinado para que se ejecute en el contexto de una operación SnapManager.
- Debe crear el script en función de las operaciones esperadas, los parámetros de entrada disponibles y las convenciones de código de devolución.
- Debe incluir mensajes de registro y redirigir los mensajes a archivos de registro definidos por el usuario.
  - a. Cree la secuencia de comandos de la tarea personalizando la secuencia de comandos de ejemplo.

Realice lo siguiente:

- i. Busque un script de ejemplo en el siguiente directorio de instalación:

```
<default_install_directory>/plugins/examples/backup/create
```

```
<default_install_directory>/plugins/examples/clone/create
```

- i. Abra el script en el editor de secuencia de comandos.
  - ii. Guarde el script con un nombre diferente.
- b. Modifique las funciones, variables y parámetros según sea necesario.
  - c. Guarde el script en uno de los siguientes directorios:

### Secuencias de comandos de operaciones de copia de seguridad

- `<default_install_directory>/plugins/backup/create/pre`: Ejecuta el script antes de que se ejecute la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.

- `<default_install_directory>/plugins/backup/create/post`: Ejecuta el script después de que se realiza la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- `<default_install_directory>/plugins/backup/create/policy`: Siempre ejecuta el script antes de que se ejecute la operación de backup. SnapManager utiliza siempre este script para todos los backups del repositorio. **Restaurar secuencias de comandos de operación**
- `<default_install_directory>/plugins/restore/create/pre`: Ejecuta el script antes de que se ejecute la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- `<default_install_directory>/plugins/restore/create/post`: Ejecuta el script después de que se realiza la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- `<default_install_directory>/plugins/restore/create/policy`: Siempre ejecuta el script antes de que se ejecute la operación de backup. SnapManager utiliza siempre este script para todos los backups del repositorio. **Clonar secuencias de comandos**
- `<default_install_directory>/plugins/clone/create/pre`: Ejecuta el script antes de que se ejecute la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- `<default_install_directory>/plugins/clone/create/post`: Ejecuta el script después de que se produzca la operación de backup. Utilícelo de manera opcional al especificar la creación de backups.
- `<default_install_directory>/plugins/clone/create/policy`: Siempre ejecuta el script antes de que se ejecute la operación de backup. SnapManager utiliza siempre este script para todos los backups del repositorio.

## Almacenar los scripts de tareas

Debe almacenar los scripts de tareas previas, posteriores a tareas y de políticas en un directorio especificado en el servidor de destino donde se crearán los backups o clones. Para la operación de restauración, los scripts deben colocarse en el directorio especificado en el servidor de destino donde se desea restaurar el backup.

### Pasos

1. Cree el script.
2. Guarde el script en una de las siguientes ubicaciones:

#### Para la operación de copia de seguridad

Directorio	Descripción
<code>&lt;default_install_directory&gt;/plugins/backup/create/policy</code>	Los scripts de políticas se ejecutan antes de las operaciones de backup.
<code>&lt;default_install_directory&gt;/plugins/backup/create/pre</code>	Los scripts de preprocesamiento ejecutan el antes de las operaciones de backup.

Directorio	Descripción
<code>&lt;default_install_directory&gt;/plugins/backup/create/post</code>	Los scripts de procesamiento posterior se ejecutan después de las operaciones de backup.

#### Para la operación de restauración

Directorio	Descripción
<code>&lt;default_install_directory&gt;/plugins/restore/create/policy</code>	Los scripts de políticas se ejecutan antes de las operaciones de restauración.
<code>&lt;default_install_directory&gt;/plugins/restore/create/pre</code>	Las secuencias de comandos de preprocesamiento se ejecutan antes de las operaciones de restauración.
<code>&lt;default_install_directory&gt;/plugins/restore/create/post</code>	Los scripts posteriores al procesamiento se ejecutan después de las operaciones de restauración.

#### Para la operación de clonación

Directorio	Descripción
<code>&lt;default_install_directory&gt;/plugins/clone/create/policy</code>	Los scripts de políticas se ejecutan antes de las operaciones de clonado.
<code>&lt;default_install_directory&gt;/plugins/clone/create/pre</code>	Los scripts de procesamiento previo se ejecutan antes de las operaciones de clonado.
<code>&lt;default_install_directory&gt;/plugins/clone/create/post</code>	Los scripts de procesamiento posterior se ejecutan después de las operaciones de clonado.

## Compruebe la instalación de los scripts de plugins

SnapManager le permite instalar y utilizar scripts personalizados para realizar diversas operaciones. SnapManager proporciona plugins para las operaciones de backup, restauración y clonado, que puede usar para automatizar sus scripts personalizados antes y después de las operaciones de backup, restauración y clonado.

### Paso

1. Introduzca el siguiente comando:

```
smsap plugin check -osaccount os db user name
```

Si no proporciona el `-osaccount` opción, la verificación de la instalación del script de plugin tiene lugar para el usuario raíz en lugar de para el usuario especificado.

### ejemplo

El siguiente resultado indica que las secuencias de comandos `policy 1`, `pre-plugin1` y `pre-plugin2` se han instalado correctamente. Sin embargo, la secuencia de comandos `post-plugin1` no funciona.

```
        smsap plugin check
Checking plugin directory structure ...
<installdir>/plugins/clone/policy
    OK: 'policy1' is executable

<installdir>/plugins/clone/pre
    OK: 'pre-plugin1' is executable and returned status 0
    OK: 'pre-plugin2' is executable and returned status 0

<installdir>/plugins/clone/post
    ERROR: 'post-plugin1' is executable and returned status 3
Command complete.
```

## Cree un archivo de especificación de tarea

Puede crear los archivos de especificación de tareas mediante la interfaz gráfica de usuario (GUI), la interfaz de línea de comandos (CLI) o un editor de texto. Estos archivos se utilizan para realizar un procesamiento previo o la actividad de posprocesamiento de las operaciones de backup, restauración o clonado.

### Pasos

1. Cree un archivo de especificación de tareas mediante GUI, CLI o un editor de texto.

### ejemplo

Puede crear el archivo de especificación según la estructura del siguiente archivo de especificación de tareas de ejemplo:

```
<task-specification>
  <pre-tasks>
    <task>
      <name>name</name>
      <parameter>
        <name>name</name>
        <value>value</value>
      </parameter>
    </task>
  </pre-tasks>
  <post-tasks>
    <task>
      <name>name</name>
      <parameter>
        <name>name</name>
        <value>value</value>
      </parameter>
    </task>
  </post-tasks>
</task-specification>
```

2. Introduzca el nombre del script.
3. Introduzca el nombre del parámetro y el valor asignado al parámetro.
4. Guarde el archivo XML en el directorio de instalación correcto.

---

### Ejemplo de especificación de tarea

```

<task-specification>
  <pre-tasks>
    <task>
      <name>clone cleanup</name>
      <description>pre tasks for cleaning up the target
system</description>
    </task>
  </pre-tasks>
  <post-tasks>
    <task>
      <name>SystemCopy follow-up activities</name>
      <description>SystemCopy follow-up activities</description>
      <parameter>
        <name>SCHEMAOWNER</name>
        <value>SAMSR3</value>
      </parameter>
    </task>
    <task>
      <name>Oracle Users for OS based DB authentication</name>
      <description>Oracle Users for OS based DB
authentication</description>
      <parameter>
        <name>SCHEMAOWNER</name>
        <value>SAMSR3</value>
      </parameter>
      <parameter>
        <name>ORADBUSR_FILE</name>
        <value\>/mnt/sam/oradbusr.sql</value\>

      </parameter>
    </task>
  </post-tasks>
</task-specification>

```

## Realizar operaciones de backup, restauración y clonado mediante scripts previos y posteriores

Puede usar su propio script para iniciar una operación de backup, restauración o clonado. SnapManager muestra una página Task-abling en el asistente Backup Create, el asistente Restore or Recover o el asistente Clone Create, donde puede seleccionar el script y proporcionar valores a los parámetros que requiera el script.

### Lo que necesitará

- Instale los scripts de los plugins en la ubicación correcta de instalación de SnapManager.
- Compruebe que los plugins se han instalado correctamente mediante el comando.
- Asegúrese de que está utilizando el shell BASH.

## Acerca de esta tarea

En la interfaz de línea de comandos (CLI), enumere el nombre del script, seleccione los parámetros y configure los valores.

## Pasos

1. Para verificar que está utilizando el shell BASH, introduzca el siguiente comando en el símbolo del sistema:

```
bash
```

De forma alternativa, puede introducir la `which-bash` en el símbolo del sistema y utilice el resultado del comando como parámetro `start` del script.

El shell BASH funciona correctamente si no ve un error.

2. Para la operación de backup, introduzca el `-taskspec` Y proporcionar la ruta absoluta del archivo XML de especificación de tareas para realizar un preprocesamiento o una actividad de post-procesamiento antes o después de la operación de copia de seguridad:

```
smsap backup create -profile profile_name {[-full {-online | -offline | -auto}
[-retain {-hourly | [-daily | -weekly | -monthly | -unlimited]}] [-verify] | [-
data [[-files files [files]] | [-tablespaces tablespaces [-tablespaces]] [-
datalabel label] {-online | -offline | -auto} [-retain {-hourly | [-daily |
-weekly | -monthly | -unlimited]}] [-verify] | [-archivelogs [-label label] [-
comment comment] [-protect | -noprotect | -protectnow] [-backup-dest path1
[,path2]] [-exclude-dest path1 [,path2]]] [-prunelogs {-all | -untilSCN
untilSCN | -before {-date yyyy-MM-dd HH:mm:ss | -months | -days | -weeks |
-hours}} -prune-dest prune_dest1 [,prune_dest2]] [-taskspec taskspec] [-
include-with-online-backups | -no-include-with-online-backups]} -dump [-force]
[-quiet | -verbose]
```

Si se produce un error en la operación del plugin de backup, solo se muestran el nombre del plugin y el código de devolución. El script del plugin debe incluir mensajes de registro y redirigir los mensajes a los archivos de registro definidos por el usuario.

3. Para la operación de restauración de backup, introduzca el `-taskspec` Y proporcione la ruta absoluta del archivo XML de especificación de tareas para realizar un preprocesamiento o una actividad de post-procesamiento que se produzca antes o después de la operación de restauración:

```
smsap backup restore -profile profile_name {-label <label> | -id <id>} {-files
<files> | -tablespaces <tablespaces> | -complete | -controlfiles} [-recover {
-alllogs | -nologs | -until <until>}] [-restorespec <restorespec>] | -from
-secondary [-temp-volume <temp_volume>] [-copy-id id] [-taskspec <taskspec>]
[-verify] [-force] backup restore -fast [require | override | fallback | off]
[-preview] -dump [-quiet | -verbose]
```

Si se produce un error en la operación del plugin de restauración, solo se muestran el nombre del plugin y el código de devolución. El script del plugin debe incluir mensajes de registro y redirigir los mensajes a los

archivos de registro definidos por el usuario.

4. Para la operación de creación de clones, introduzca la opción `-taskspec` y proporcione la ruta absoluta del archivo XML de especificación de tareas para realizar un procesamiento previo o una actividad de procesamiento posterior que debe tener lugar antes o después de la operación de clonado:

```
smsap clone create -profile profile_name {-backup-label backup_name | -backup
-id <backup-id> | -current} -newsid new_sid -clonespec
full_path_to_clonespecfile [-reserve <yes, no, inherit> ] [-host <host>] [-
label <label>] [-comment <comment>] [-from-secondary [-copy-id <id>]] {-
taskspec <taskspec>} -dump [-quiet | -verbose]
```

Si se produce un error en la operación del plugin de clonado, solo se muestran el nombre del plugin y el código de devolución. El script del plugin debe incluir mensajes de registro y redirigir los mensajes a los archivos de registro definidos por el usuario.

### Ejemplo de creación de una copia de seguridad utilizando el archivo XML de especificación de tareas

```
smsap backup create -profile SALES1 -full -online -taskspec
sales1_taskspec.xml -force -verify
```

## Actualizar el nombre del sistema de almacenamiento y el nombre de host de la base de datos de destino asociados con un perfil

Con SnapManager 3.3 o versiones posteriores, es posible actualizar el nombre de host del sistema de almacenamiento o la dirección del sistema de almacenamiento, así como el nombre de host de la base de datos de destino asociado con un perfil de SnapManager.

### Actualice el nombre del sistema de almacenamiento asociado a un perfil

A partir de la versión 3.3 de SnapManager, es posible actualizar el nombre de host o la dirección IP de un sistema de almacenamiento asociado con un perfil.

#### Lo que necesitará

Debe asegurarse de lo siguiente:

- El perfil tiene al menos una copia de seguridad.

Si el perfil no tiene backup, no es necesario actualizar el nombre del sistema de almacenamiento para ese perfil.

#### Acerca de esta tarea



- No se está ejecutando ninguna operación para el perfil.

Puede actualizar el nombre o la dirección IP del sistema de almacenamiento mediante la interfaz de línea de comandos (CLI) de SnapManager. Mientras se actualiza el nombre del sistema de almacenamiento, se actualizan los metadatos almacenados únicamente en la base de datos del repositorio. Después de cambiar el nombre del sistema de almacenamiento, puede realizar todas las operaciones de SnapManager como antes.



No se puede cambiar el nombre del sistema de almacenamiento mediante la interfaz gráfica de usuario (GUI) de SnapManager.

Debe asegurarse de que haya copias Snapshot disponibles en el nuevo sistema de almacenamiento. SnapManager no verifica la existencia de las copias Snapshot en el sistema de almacenamiento.

Sin embargo, debe recordar lo siguiente al realizar la actualización y reversión del host después de cambiar el nombre del sistema de almacenamiento:

- Si va a realizar una actualización gradual del host después de cambiar el nombre del sistema de almacenamiento, debe actualizar el perfil con el nuevo nombre del sistema de almacenamiento.

Consulte *solución de problemas con los problemas de nombre del sistema de almacenamiento* para obtener información sobre cómo usar los comandos de la SnapDrive para cambiar el nombre del sistema de almacenamiento.

- Si va a revertir el host después de cambiar el nombre del sistema de almacenamiento, debe asegurarse de cambiar el nombre del sistema de almacenamiento a su nombre anterior para poder utilizar los perfiles, los backups y los clones del sistema de almacenamiento anterior para ejecutar operaciones de SnapManager.



Si SnapDrive no pudo identificar el sistema de almacenamiento y muestra mensajes de error, puede introducir el comando `ipmigrate` con los nombres de host anteriores y posteriores del sistema de almacenamiento. Para obtener información adicional sobre problemas de nombres del sistema de almacenamiento, consulte *Troubleshooting Storage system name ediciones*.

## Paso

1. Introduzca el siguiente comando:

```
smsap storage rename -profile profile -oldname old_storage_name -newname new_storage_name [quiet | -verbose]
```

Si desea...	Realice lo siguiente...
Actualice el nombre del sistema de almacenamiento asociado a un perfil	Especifique el <code>-profile</code> opción.
Actualice el nombre o la dirección IP del sistema de almacenamiento asociados a un perfil	Especifique las siguientes opciones y variables: <ul style="list-style-type: none"> <li>• <code>-oldname old_storage_name</code> Es el nombre de host o la dirección IP del sistema de almacenamiento.</li> <li>• <code>-newname new_storage_name</code> Es el nombre de host o la dirección IP del sistema de almacenamiento.</li> </ul>

En el ejemplo siguiente se muestra el nombre del sistema de almacenamiento que se está actualizando:

```
smsap storage rename -profile mjullian -oldname lech -newname hudson  
-verbose
```

## Ver una lista de los sistemas de almacenamiento asociados a un perfil

Puede ver una lista de los sistemas de almacenamiento asociados con un perfil en particular.

### Acerca de esta tarea

La lista muestra los nombres de los sistemas de almacenamiento asociados con el perfil en particular.



Si no hay backups disponibles para el perfil, no puede ver el nombre del sistema de almacenamiento asociado con el perfil.

### Paso

1. Para mostrar información sobre los sistemas de almacenamiento asociados con un perfil determinado, escriba este comando:

```
smsap storage list -profile profile [-quiet | -verbose]
```

### Ejemplo

```
smsap storage list -profile mjubllian
```

```
Sample Output:  
Storage Controllers  
-----  
STCO1110-RTP07OLD
```

## Actualice el nombre de host de la base de datos de destino asociado a un perfil

SnapManager (3.2 o posterior) para SAP permite actualizar el nombre de host de la base de datos de destino en el perfil de SnapManager.

### Lo que necesitará

- El directorio inicial del usuario local debe tener en cuenta las asignaciones de perfil a repositorio.
- Se deben cerrar las sesiones de la interfaz gráfica de usuario (GUI) de SnapManager.
- En un entorno RAC, los clones o backups montados disponibles en el host especificado en el perfil deben eliminarse y desmontarse.

### Acerca de esta tarea

Puede actualizar el perfil con el nuevo nombre de host únicamente mediante la CLI.

### Escenarios no admitidos para cambiar el nombre de host de la base de datos de destino en Profile

Las siguientes situaciones no son compatibles para cambiar el nombre de host de la base de datos de destino en el perfil:

- Cambiar el nombre de host de la base de datos de destino mediante la interfaz gráfica de usuario de SnapManager
- Reversión de la base de datos del repositorio después de actualizar el nombre de host de la base de datos de destino del perfil
- Actualizar varios perfiles para un nuevo nombre de host de base de datos de destino ejecutando un solo comando
- Cambiar el nombre de host de la base de datos de destino cuando se ejecuta cualquier operación de SnapManager
- Cambiar el nombre de host de la base de datos de destino si SnapManager se instala en Solaris y si los números de unidad lógica de base de datos (LUN) se crean mediante el sistema de archivos montado en host con la pila de SVM.



Después de actualizar el nombre de host de la base de datos de destino en el perfil, solo se cambia el nombre de host de la base de datos de destino. Se conservan todos los demás parámetros de configuración establecidos en el perfil.

Después de actualizar el nuevo nombre de host de la base de datos de destino en un perfil habilitado para la protección, se conservan el mismo conjunto de datos y las mismas políticas de protección para el perfil actualizado.

Después de cambiar el nombre de host del host objetivo, debe asegurarse de actualizar el nombre de host para todos los perfiles protegidos existentes antes de crear los nuevos perfiles protegidos. Para actualizar el nombre de host de un perfil, ejecute el `smsap profile update` comando.

Después de actualizar el nombre de host de la base de datos de destino, no se puede omitir o dividir el clon o desmontar el backup si el clon o el backup montado no están disponibles en el nuevo host. En tales situaciones, ejecutar las operaciones de SnapManager desde el host nuevo conlleva el fallo y las entradas obsoletas del host anterior. Para realizar operaciones de SnapManager, debe revertir al nombre de host anterior mediante el uso `profile update`.

1. Introduzca el siguiente comando:

```
smsap profile update -profile profile [-profile-password profile_password] [-
database-dbname db_dbname -host db_host [-sid db_sid] [-login-username
db_username -password db_password -port db_port] [{-rman{-controlfile | {-
login-username rman_username -password rman_password -tnsname rman_tnsname}}}
| -remove-rman]-osaccount osaccount -osgroup osgroup [-retain [-hourly [-count
```

```
n] [-duration m]] [-daily [-count n] [-duration m]] [-weekly [-count n] [-duration m]] [-monthly [-count n] [-duration m]]] [-comment comment][-snapname-pattern pattern][[-protect [-protection-policy policy_name]]] [[-noproduct]] [-summary-notification] [-notification [-success -email email_address1, email_address2 -subject subject_pattern] [-failure -email email_address1, email_address2 -subject subject_pattern]] [-separate-archivelog-backups-retain-archivelog-backups -hours hours | -days days | -weeks weeks | -months months [-protect [-protection-policy policy_name] | -noproduct] [-include-with-online-backups | -no-include-with-online-backups]] [-dump]
```

Las demás opciones para este comando son las siguientes:

```
[-force] [-noprompt]
```

```
[-quiet | -verbose]
```

Si desea...	Realice lo siguiente...
<b>Cambiar el nombre de host de la base de datos de destino</b>	Specify <code>-host <i>new_db_host</i></code>

2. Para ver el nombre de host de la base de datos de destino del perfil, escriba el siguiente comando:

```
smsap profile show
```

## Mantener el historial de operaciones de SnapManager

SnapManager para SAP le permite mantener el historial de operaciones de SnapManager asociadas con un único perfil o múltiples perfiles. Puede mantener el historial desde la interfaz de línea de comandos (CLI) de SnapManager o desde la interfaz gráfica de usuario (GUI). Puede ver el historial de las operaciones como un informe y utilizar el informe para fines de cumplimiento de auditoría.

Puede mantener el historial de las siguientes operaciones de SnapManager:

- Crear backup
- Verificación de backup
- Restauración de backup
- Clone create
- División de clones

La información del historial de las operaciones de SnapManager se mantiene en función de la retención. Puede configurar diferentes clases de retención para cada una de las operaciones de SnapManager admitidas.

A continuación se enumeran algunas clases de retención que puede asignar:

- Número de días

- Número de semanas
- Número de meses
- Cantidad de operaciones

Según la retención, SnapManager purga el historial automáticamente. También puede purgar manualmente el historial de las operaciones de SnapManager. Si elimina o destruye el perfil, se eliminará toda la información del historial asociada con el perfil.



Después de revertir el host, no se pueden ver los detalles del historial ni se pueden realizar operaciones relacionadas con el historial asociadas con el perfil que se haya configurado para el mantenimiento del historial.

## Configurar el historial de funcionamiento de SnapManager

SnapManager para SAP le permite mantener el historial de funcionamiento de SnapManager desde la interfaz de línea de comandos o la interfaz gráfica de usuario de SnapManager. Puede ver el historial de la operación SnapManager como un informe.

### Paso

1. Para configurar el historial de funcionamiento de SnapManager, introduzca el siguiente comando:

```
smsap history set -profile {-name, profile_name [profile_name1, profile_name2]
| -all -repository -login [-password repo_password] -username repo_username
-dbname repo_dbname -host repo_host -port repo_port} -operation {-operations
operation_name [-operation_name1, operation_name2] | -all} -retain {-count
retain_count | -daily retain_daily | -weekly retain_weekly | -monthly
retain_monthly} [-quiet | -verbose]
```

```
smsap
history set -profile -name PROFILE1 -operation -operations backup -retain
-daily 6 -verbose
```

```
smsap
history set -profile -name PROFILE1 -operation -all -retain -weekly 3
-verbose
```

## Consulte una lista del historial de operaciones de SnapManager

Puede ver el historial de todas las operaciones de SnapManager específicas o como un informe de acuerdo con la configuración de retención.

### Paso

1. Para ver una lista de operaciones de historial de SnapManager, introduzca el siguiente comando:

```
smsap history list -profile {-name, profile_name [profile_name1,profile_name2]
| -all -repository-login [-password repo_password] -username repo_username
-dbname repo_dbname -host repo_host -port repo_port} -operation {-operations
operation_name [operation_name1, operation_name2] | -all} [-delimiter
delimiter] [-quiet | -verbose]
```

## Ver el historial detallado de una operación específica asociada a un perfil

Es posible ver el historial detallado de una operación SnapManager específica asociada con un perfil.

### Paso

1. Para mostrar información detallada del historial de una operación de SnapManager específica asociada con un perfil, escriba el siguiente comando:

```
smsap history operation-show -profile profile_name {-label label | -id id} [-
quiet | -verbose]
```

## Eliminar historial de operaciones de SnapManager

Puede eliminar el historial de la operación SnapManager si ya no se necesitan los detalles del historial.

### Paso

1. Para eliminar el historial de operación de SnapManager, introduzca el siguiente comando:

```
smsap history purge -profile {-name, profile_name profile_name1,
profile_name2} | all-repository-login [-password repo_password] -username
repo_username -dbname repo_dbname -host repo_host -port repo_port} -operation
{-operations operation_name [operation_name1, operation_name2] | -all} [-quiet
| -verbose]
```

## Eliminar la configuración del historial asociada a un único perfil o a varios perfiles

SnapManager permite eliminar la configuración del historial de una operación SnapManager. Esta operación purga toda la información del historial asociada con un único perfil o múltiples perfiles.

### Paso

1. Para eliminar el historial de las operaciones de SnapManager asociadas con un único perfil o múltiples perfiles, escriba el siguiente comando:

```
smsap history remove -profile {-name, profile_name [profile_name1,
profile_name2] | all-repository-login [-password repo_password] -username
repo_username -dbname repo_dbname -host repo_host -port repo_port} -operation
{-operations operation_name [operation_name1, operation_name2] | -all} [-quiet
| -verbose]
```

## Ver detalles de configuración del historial de SnapManager

Puede ver la configuración del historial de un único perfil.

### Acerca de esta tarea

La operación del historial de SnapManager muestra la siguiente información para cada perfil:

- Nombre de la operación
- Clase de retención
- Recuento de retención

### Paso

1. Para mostrar la información sobre la operación del historial de SnapManager de un perfil específico, introduzca el siguiente comando:

```
smsap history show -profile profile_name
```

## Uso de BR\*Tools con SnapManager para SAP

Puede utilizar los comandos BR\*Tools de SAP con SnapManager para SAP. BR\*Tools es un paquete de programas SAP que contiene herramientas SAP para la administración de bases de datos Oracle, por ejemplo, BRARCHIVE, BRBACKUP, BRCONNECT, BRRECOVER, BRRESTORE, BRSPACE Y BRTOOLS.

Puede completar las siguientes tareas relacionadas con el uso de BR\*Tools y SnapManager para SAP:

- Deshabilitar el acceso del cliente a las copias Snapshot
- Especifique el perfil para las copias de seguridad BR\*Tools
- Crear copias de seguridad de la base de datos mediante BRBACKUP y BRARCHIVE
- Programar backups con transacciones SAP DB13
- Restaure una base de datos mediante BRRESTORE y BRRECOVER
- Realice copias de seguridad y restaure archivos con BR\*Tools
- Restaurar un backup en otro host

### Qué son las BR\*Tools

Encontrará información que necesitaría para utilizar SAP con los sistemas de almacenamiento.

Para obtener información general sobre el uso de BR\*Tools, incluida la sintaxis de comandos, consulte la documentación de SAP, como BR\*Tools para la administración de bases de datos Oracle en línea.

### Requisitos de perfil

El perfil de SnapManager para SAP debe nombrarse correctamente para trabajar con BR\*Tools. De forma predeterminada, BACKINT usa el perfil, que tiene el mismo nombre que el SID de SAP, del repositorio determinado por el ID de usuario que emite los comandos BR\*Tools.


Debe utilizar un nombre de perfil diferente si el SID de SAP no es único en su entorno. Para obtener más información, vea *uso del perfil para copias de seguridad* de BR\* Tools.

Usted debe tener un enlace del directorio BR\*Tools al `/opt/NetApp/smsap/bin/backint` Archivo instalado por SnapManager para SAP. Para obtener información acerca de cómo crear el vínculo, vea *integrar con SAP BR\* Tools*.

Los backups creados con versiones anteriores a BR\*Tools 7.00 no se pueden verificar. El tamaño de bloque del tablespace o del archivo de datos es necesario para completar la verificación; sin embargo, las versiones anteriores a BR\*Tools 7.00 no lo proporcionan.

### Acerca de la combinación de las interfaces BR\*Tools y SnapManager para SAP

Puede utilizar una combinación de BR\*Tools y la interfaz gráfica de usuario (GUI) de SnapManager for SAP o la interfaz de línea de comandos (CLI) para realizar las siguientes operaciones:

Funcionamiento	Interfaces que puede utilizar
Enumerar, restaurar, recuperar y eliminar copias de seguridad de la base de datos (copias de seguridad que incluyen archivos de datos, archivos de control o archivos redo log en línea) creadas con BRBACKUP	SnapManager para la CLI y GUI de SAP   BR*Tools puede enumerar y restaurar sólo las copias de seguridad creadas mediante BR*Tools.
Enumerar y eliminar copias de seguridad de otros conjuntos de archivos creados con BRBACKUP	SnapManager para la CLI y GUI de SAP
Clonar copias de seguridad de otros conjuntos de archivos creados con BRBACKUP	Se puede clonar un backup completo en línea o sin conexión utilizando el comando BRBACKUP mediante la SnapManager para la CLI o GUI de SAP.

### Opciones disponibles bajo BR\*Tools CLI con SnapManager para SAP

Las siguientes opciones están disponibles bajo la CLI de BR\*Tools:

Opción	Tareas que se pueden realizar
Gestión de instancias	Registrar todas las acciones en las tablas del sistema de archivos y de la base de datos y guardar también los registros y perfiles de copia de seguridad en los medios de copia de seguridad.
Gestión del espacio	Permite una gestión de volúmenes completa. Para utilizar las funciones proporcionadas en la administración de espacio, debe inicializar los volúmenes con BRBACKUP o BRARCHIVE para asegurarse de que incluyan una etiqueta específica de SAP.
Backup y copia de la base de datos	Crear un backup de una base de datos, realizar un registro de recuperación sin conexión (registro de archivo) y verificar backups.
Restauración y recuperación	Restaurar y recuperar backups.



Opción	Tareas que se pueden realizar
Estadísticas de la base de datos	Mantener las estadísticas de tablas e índices.

### Funciones similares disponibles bajo BR\*Tools GUI

Las siguientes operaciones están disponibles en la GUI de BR\*Tools:

Tipo de asistente	Tareas que se pueden realizar
Asistente para crear repositorio	Crear un repositorio en una base de datos.
Asistente de perfil	Crear un perfil en un repositorio.
Asistente Backup	Cree una copia de seguridad del perfil.
Asistente Restore and Recovery	Restaurar y recuperar una copia de seguridad de un perfil.
Asistente SnapManager Clone Delete	Eliminar el clon de un backup.
Asistente para la eliminación de copias de seguridad de SnapManager	Eliminar la copia de seguridad de un perfil.

### Acerca de la clonado de backups creados con BR\*Tools

Se puede clonar un backup completo en línea o sin conexión utilizando el comando BRBACKUP con la SnapManager para la CLI o GUI de SAP.

Para crear un clon de la copia de seguridad de la base de datos creada mediante el comando BRBACKUP, asegúrese de establecer el parámetro de configuración `brbackup.enable.cloneable.backups` en `true` en el archivo `smSAP.config` y, a continuación, reinicie SnapManager para el servidor SAP. Introduzca el siguiente comando: `brbackup.enable.cloneable.backups=true`

Para los backups online creados con el comando BRBACKUP, SnapManager para SAP le permite clonar el backup sin realizar ningún cambio desde la CLI o GUI de SnapManager para SAP.

Para los backups sin conexión creados con el comando BRBACKUP, SnapManager para SAP le permite clonar el backup desde la CLI o GUI de SnapManager para SAP después de realizar los siguientes pasos:

1. Agregue las siguientes variables de configuración en el archivo `smsap.config`.

Los valores de las variables que se muestran a continuación son valores predeterminados. Puede conservar estos valores si desea establecerlos en valores predeterminados.

- `brbackup.oracle.maxfiles=254`
- `brbackup.oracle.maxloghistory=1168`
- `brbackup.oracle.maxinstances=50`
- `brbackup.oracle.maxlogfiles=255`

- brbackup.oracle.maxlogmembers=3
  - brbackup.oracle.character\_set=UTF8
2. Para cambiar cualquiera de estos valores de parámetros de configuración predeterminados en el archivo smSAP.config, ejecute el siguiente comando desde el símbolo del sistema SQL:

```
alter database backup controlfile to trace as file
```

El archivo puede ser cualquier nombre definido por el usuario y se crea en el mismo directorio desde donde se llama a SQL\*Plus.

3. Abra el archivo para establecer estos valores en las variables de configuración correspondientes del archivo smSAP.config.
4. Reinicie el servidor SnapManager.

### **Acerca de la eliminación de copias de seguridad creadas con BR\*Tools**

BR\*Tools no elimina las copias de seguridad. Dado que los backups de SnapManager para SAP se basan en copias Snapshot, existe un límite para la cantidad de backups que puede retener. Es necesario garantizar que los backups se eliminen cuando ya no se necesiten.

En el sistema de almacenamiento NetApp, cada volumen puede tener un máximo de 255 copias snapshot. Si un volumen alcanza el límite, se producirá un error en los backups. Un backup realizado con BRBACKUP suele crear dos copias Snapshot de cada volumen afectado.

Para evitar llegar al máximo de la copia Snapshot de 255, puede gestionar los backups de las siguientes formas:

- Puede establecer las opciones retain en el perfil usado para las operaciones BR\*Tools.

A continuación, SnapManager para SAP elimina automáticamente los backups más antiguos, según sea necesario.

- Puede eliminar manualmente backups que ya no sean necesarios mediante la interfaz gráfica de usuario o la interfaz de línea de comandos de SnapManager para SAP.

### **Deshabilitar el acceso del cliente a las copias Snapshot**

En el caso de cualquier volumen del sistema de almacenamiento que utilice el protocolo NFS y contenga los datos de SAP de los que se realice un backup mediante BR\*Tools, debe deshabilitar el acceso del cliente a las copias Snapshot de ese volumen. Si el acceso de cliente está activado, BR\*Tools intentará crear copias de seguridad de los directorios .snapshot ocultos que contengan copias de seguridad anteriores.

Para deshabilitar el acceso de los clientes, utilice uno de los métodos siguientes.

- Con Data ONTAP: Con la interfaz de línea de comandos de Data ONTAP, introduzca el siguiente comando: vol options volume\_name nosinnapdir en donde volume\_name es el nombre del volumen que contiene datos de SAP, por ejemplo, /vol/falls\_sap\_cer9i\_data1
- Utilizando FilerView: Para desactivar el acceso mediante la interfaz gráfica de usuario de FilerView, ya se necesita una copia snapshot del volumen.
  - a. En el panel izquierdo de FilerView, seleccione **volumenes > instantáneas > gestionar**.

- b. En la página Manage Snapshots, haga clic en el nombre del volumen en la columna Volume.
- c. En la página Configurar instantáneas, desactive la casilla de verificación Directorio de instantáneas visible y haga clic en **aplicar**.

Para obtener más información acerca de cómo desactivar el acceso de los clientes a las copias snapshot, consulte el capítulo sobre la administración de instantáneas de la *Guía de recuperación y copia de seguridad en línea de protección de datos de Data ONTAP* correspondiente a su versión de Data ONTAP.

## Uso del perfil para copias de seguridad BR\*Tools

Cuando ejecuta un comando BR\*Tools que usa la interfaz BACKINT, SnapManager usa un perfil del repositorio. El repositorio está determinado por las credenciales SnapManager del usuario que ejecuta el comando BR\*Tools.

De forma predeterminada, SnapManager utiliza el perfil con el mismo nombre que el identificador de sistema de base de datos SAP.

### Acerca de la creación de credenciales para acceder al repositorio

Puede utilizar el `smsap credential set` Para establecer las credenciales del repositorio para el usuario BR\*Tools.

### Especificar un nombre de perfil de SnapManager diferente

Siempre que el identificador del sistema sea único para todos los hosts cuyos perfiles de SnapManager se encuentren en un repositorio determinado, el nombre del perfil predeterminado será suficiente. Puede crear el perfil de SnapManager y llamarlo mediante el valor identificador del sistema de la base de datos.

Sin embargo, si se utiliza el mismo identificador de sistema en distintos hosts, o si desea especificar más de un perfil SnapManager para utilizarlo con BR\*Tools en una instancia SAP determinada, deberá definir el nombre del perfil para los comandos BR\*Tools.

Las operaciones de base de datos programadas en la aplicación SAP se ejecutan como usuario. Las operaciones BR\*Tools programadas dentro de las aplicaciones SAP se ejecutan como `sidadm`. Estos usuarios deben tener acceso al repositorio y al perfil.

Para configurar las credenciales de un usuario, realice los siguientes pasos:

1. Inicie sesión como `sidadm`.
2. Introduzca el comando para establecer las credenciales del repositorio:

```
smsap credential set command
```

3. Sincronice los perfiles introduciendo el siguiente comando:

```
smsap profile sync
```

4. Establezca la contraseña de los perfiles detectados introduciendo el comando:

```
smsap credential set
```

## Acerca de la creación del archivo de parámetros de la utilidad de copia de seguridad

El comando BR\*Tools puede pasar opcionalmente un archivo de parámetros de utilidad de copia de seguridad (.utl Parameter) a la interfaz BACKINT. De forma predeterminada, el nombre de este archivo es `initSID.utl`, Donde SID es el identificador de sistema de la base de datos.

De manera predeterminada, BR\*Tools usa el archivo de parámetros especificado por `util_par_file` en la `initSID.sap file`. El archivo de parámetros de la utilidad de copia de seguridad se almacena normalmente en el mismo directorio que el `initSID.sap file`.

Agregar `profile_name = <profile>` para la `.utl` archivos y guardar. La `profile` Es el nombre del perfil SnapManager que desea utilizar para los comandos BR\*Tools.

En la siguiente tabla se enumeran los parámetros adicionales de la utilidad de copia de seguridad incluidos en la `.utl` archivos para operaciones como la retención de backups, la restauración rápida y la protección de datos:

Operaciones	Parámetros de la utilidad de copia de seguridad
Retención de backups	<ul style="list-style-type: none"><li>• Clave: Retener</li><li>• Valor: Ilimitado</li></ul>
horario	diario
semanal	mensual
Restauración rápida	<ul style="list-style-type: none"><li>• Tecla: Rápido</li><li>• Valor: Requerir</li></ul>
anular	respaldo
desactivado	Protección de datos
<ul style="list-style-type: none"><li>• Clave: Proteger</li><li>• Valor: sí</li></ul>	no

Operaciones	Parámetros de la utilidad de copia de seguridad
<p>se deja en blanco</p> <div style="border-left: 1px solid black; padding-left: 10px; margin-left: 20px;"> <p>Las diferentes opciones mencionadas para el parámetro Value son similares a las <code>-protect</code> opción que se utiliza en la interfaz de línea de comandos.</p> </div>	<p>Realice backups de datos del almacenamiento secundario en una ubicación definida según las preferencias de los usuarios</p>
<ul style="list-style-type: none"> <li>• Key: Preferred_backup_locations</li> <li>• Valor: Los nombres de nodos de protección de datos como una lista separada por comas.</li> <li>• Valor predeterminado: No se ha establecido ningún valor.</li> </ul> <div style="border-left: 1px solid black; padding-left: 10px; margin-left: 20px;"> <p>Para añadir un nombre de nodo de política de protección de datos, consulte <a href="#">Acerca de las descripciones de políticas de protección.</a></p> </div>	<p>Restaurar los datos del almacenamiento secundario a una ubicación preferida</p>

Operaciones	Parámetros de la utilidad de copia de seguridad
<ul style="list-style-type: none"> <li>• Key: Restore_from_Latter_backup_location</li> <li>• Valor: sí</li> </ul>	no * Valor predeterminado: sí

En la siguiente tabla se describen los diferentes parámetros de la utilidad de backup para estas operaciones:

Funcionamiento	Clave	Valor
Retención de backups	rápido=	respaldo
Restauración rápida	retener=	cada hora
Protección de datos	proteger=	no

### Adición del parámetro de utilidad de copia de seguridad al archivo de inicialización BR\*Tools

SAP crea un archivo de perfil de copia de seguridad denominado `initSID.sap` Para cada instancia de base de datos SAP en `$ORACLE_HOME/dbs/`. Puede usar este archivo para especificar el parámetro predeterminado de la utilidad de copia de seguridad (`.utl`) Archivo utilizado para comandos BR\*Tools.

1. Edite el `initSID.sap` archiva y localiza la línea que comienza con `util_par_file =`.
2. Anule el comentario de esta línea y agregue la ruta al archivo de parámetros de la utilidad de copia de seguridad que contiene el nombre del perfil, por ejemplo, `util_par_file = initSA1.utl`.
3. Si especifica un valor para `util_par_file`, asegúrese de que el archivo existe.

Si no se encuentra el archivo, los comandos BRBACKUP fallan porque intentan incluir ese archivo en una copia de seguridad.

Si se encuentra alguna de las siguientes condiciones de error, deberá utilizar el `-u` opción como nombre de perfil:

- Parameter files does not exist
- No profile\_name entry

Tanto `orasid` como `sidadm` necesitan tener acceso al perfil que se utilizaría para crear o gestionar copias de seguridad creadas con BR\*Tools.

### Especificar el nombre del archivo del parámetro de la utilidad de copia de seguridad en el comando BR\*Tools

Opcionalmente, puede especificar el archivo de parámetros de utilidad de copia de seguridad (`.utl` Parameter) en los comandos BR\*Tools con la opción `-r` . El valor de la línea de comandos anula el valor especificado en el archivo de inicialización SAP.

BR\*Tools busca el archivo de parámetros en `$ORACLE_HOME/dbs/` directorio. Si almacena el archivo en otra ubicación, debe proporcionar la ruta completa con la opción `-r`. Por ejemplo:

```
brbackup -r /opt/NetApp_fcp_price_10g_enterprise_inst_voll/dbs/initCER.utl ...
```

## Copias de seguridad de bases de datos creadas con BRBACKUP y BRARCHIVE

El comando BRBACKUP crea un respaldo de la base de datos SAP mediante copia Snapshot en el sistema de almacenamiento. Puede ejecutar el BRBACKUP Comando desde la interfaz de línea de comandos (CLI) del host SAP, la CLI de BR\*Tools o la interfaz gráfica de usuario (GUI). Para realizar una copia de seguridad de los archivos redo log sin conexión, puede utilizar la BRARCHIVE comando.

BRBACKUP realiza una copia de seguridad de los archivos de datos, archivos de control y archivos redo log en línea de la base de datos SAP. Debería realizar una copia de seguridad de los otros archivos de configuración de SAP, por ejemplo, archivos de registro de SAP, archivos del kernel y transportar solicitudes mediante BRBACKUP con la SAP\_DIR y restaurar mediante BRRESTORE.

Si el valor de `SQLNET.AUTHENTICATION_SERVICES` en la `sqlnet.ora` se establece en **NONE**, Asegúrese de que el usuario de la base de datos Oracle (sistema) tiene privilegios sysoper. El sistema es el usuario predeterminado que se crea durante la creación de la base de datos de Oracle. Para activar los privilegios SYSOPER, ejecute el siguiente comando:

```
grant sysoper to system;
```

Debe utilizar los comandos BR\*Tools o los comandos SnapManager para administrar los archivos de registro de archivos.

No debe utilizar la combinación de perfiles SnapManager y los comandos BR\*Tools para administrar las copias de seguridad del registro de archivo con respecto a las operaciones siguientes:

- Creación de copias de seguridad independientes de archivos de datos y archivos de registro de archivo mediante los comandos BRBACKUP y BRARCHIVE con el perfil SnapManager (creado con la opción para separar las copias de seguridad de registros de archivo)
- Eliminar archivos de registro de archivos mientras se crea el backup con el perfil SnapManager



SnapManager no muestra ningún mensaje de advertencia o error cuando utiliza una combinación de perfiles SnapManager para SAP y los comandos BR\*Tools para administrar los archivos de registro de archivos.

Debe crear un perfil sin usar la opción de separar las copias de seguridad de los registros de archivos y utilizar este perfil para las operaciones normales de BR\*Tools.

Para restaurar el backup, se puede utilizar BRRESTORE. Para los backups de la base de datos (los backups incluyen archivos de datos, archivos de control o archivos de registro de recuperación en línea) creados con el uso BRBACKUP con la `-m all` o `-m full` Opción, también puede restaurar el backup con la interfaz gráfica de línea de comandos o la interfaz gráfica de usuario de SnapManager.

Para obtener más información acerca de cómo SnapManager controla la copia de seguridad, consulte *copia de seguridad de bases de datos*.

Consulte la documentación de SAP para obtener las instrucciones y la sintaxis específicas de BRBACKUP y BRARCHIVE comandos. Antes de utilizar los comandos BRBACKUP y BRARCHIVE con un sistema de almacenamiento, asegúrese de que se cumplen las siguientes condiciones:

- Si el nombre del perfil SnapManager es diferente del identificador del sistema de la base de datos SAP, especifique el nombre del archivo de parámetros que contiene el nombre del perfil SnapManager.

Puede hacerlo de una de las siguientes maneras:

- Especifique el archivo de parámetros de la utilidad de copia de seguridad (`initSID.utl`) utilizando la opción `-r` con el `BRBACKUP` comando.
  - Especifique el archivo de parámetros en el archivo de inicialización (`initSID.sap`). Para obtener más información, vea *Specifying the profile for BR\*Tools backups*.
- Si se considera adecuado para su entorno, cree backups adicionales de sus datos SAP utilizando un medio diferente, como la cinta. Las copias Snapshot están diseñadas para realizar respaldos y restauraciones rápidos. Se almacenan en los mismos soportes físicos que los datos de los que se realiza el backup y no están pensados para la recuperación ante desastres a menos que se copien a otros dispositivos de almacenamiento.

## Programar backups con transacciones SAP DB13

Es necesario realizar varios pasos para permitir que las copias de seguridad de SnapManager para SAP funcionen desde la transacción DB13 del Calendario de planificación de DBA.

### Pasos

1. Cambie los permisos de `/oracle/SID/sapbackup` directorio para permitir el acceso de escritura por el identificador de usuario de `sidadm`.

Utilice el siguiente comando como `orasid`:

```
chmod 775 /oracle/SID/sapbackup
```

Esto permitirá a los miembros del `dba` grupo para escribir en ese directorio. El identificador de usuario `sidadm` es miembro de `dba` grupo.

2. Cambiar los permisos del archivo de credenciales de SnapManager para SAP `orasid` permitir `sidadm` acceso. Utilice el siguiente comando ejecutado por `orasid`:

Utilice el siguiente comando ejecutado por `orasid`:

```
chmod 660 /oracle/SID/.netapp/smsap/credentials
```

Siga las instrucciones de la sección 3.3, "Registro de sistemas en el repositorio" de TR-3582 "prácticas recomendadas de SnapManager para SAP" para registrar el identificador de usuario de `sidadm` en el repositorio de SnapManager para SAP.

## Restauración de bases de datos mediante BRRESTORE y BRRECOVER

Los comandos `BRRESTORE` y `BRRECOVER` sólo funcionan con las copias de seguridad creadas mediante `BRBACKUP`.

Consulte la documentación de SAP para obtener instrucciones y sintaxis específicas para los comandos `BRRESTORE` y `BRRECOVER`.



Si el nombre del perfil de SnapManager es diferente del identificador del sistema de la base de datos SAP, debe especificar el nombre del archivo de parámetros que contiene el nombre del perfil de SnapManager. Puede hacerlo de una de las siguientes maneras:

- Especifique el archivo de parámetros de la utilidad de copia de seguridad (`initSID.utl`) uso de la opción `-r` en `BRBACKUP` comando.
- Especifique el archivo de parámetros en el archivo de inicialización `BR*Tools` (`initSID.sap`).



Backups (archivos de datos, archivos de control o archivos de registro de recuperación en línea) que se crean mediante `BRBACKUP` puede restaurarse desde sistemas de almacenamiento secundario o terciario mediante el `smSAP restore` comando. Sin embargo, se recomienda realizar una copia de seguridad de los otros archivos de configuración de SAP, por ejemplo, archivos de registro de SAP, archivos de kernel y transportes de solicitudes mediante `BRBACKUP` con `SAP_DIR`` y restaure mediante `BRRESTORE`.

Puede anular las comprobaciones de una restauración rápida basada en volúmenes mediante `BRRESTORE` especificando `fast=override` en la `.utl` archivo (el mismo archivo en el que se especifica el nombre del perfil si es diferente del identificador del sistema de la base de datos).

## Copia de seguridad y restauración de archivos mediante BR\*Tools

Además de realizar copias de seguridad de archivos de base de datos, puede usar `BR*Tools` para realizar copias de seguridad y restaurar cualquier archivo, como los archivos del sistema SAP almacenados en el sistema de almacenamiento.

Siga la documentación de SAP `BR*Tools` para los comandos `BRBACKUP` y `BRRESTORE`. La siguiente información adicional es aplicable cuando utiliza SnapManager para SAP:

- Los archivos deben almacenarse en el sistema de almacenamiento.
- Asegúrese de que tiene permisos para los archivos de los que va a realizar la copia de seguridad. Por ejemplo, realizar backups de archivos del sistema SAP (`BRBACKUP backup_mode=sap_dir`) O archivos de sistema de Oracle (`BRBACKUP backup_mode=ora_dir`) requiere permiso `root` en el host. Utilizar el comando `su root` antes de ejecutar `BRBACKUP`.

## Restaurar un backup en otro host

Puede utilizar el comando `BRRESTORE` o `smSAP restore` para restaurar una copia de seguridad realizada con `BRBACKUP` en un host diferente. El nuevo host también debe ejecutar SnapManager para SAP.

### Hacer que el perfil SnapManager esté disponible

Para poder ejecutar `BRRESTORE`, debe hacer que el perfil SnapManager del host original esté disponible para el nuevo host. Complete los siguientes pasos:

- Configure la credencial para el repositorio: Utilice el `smSAP credential set` Comando para habilitar el nuevo host para acceder al repositorio de SnapManager usado para el backup original.
- Configure las credenciales para el perfil: Utilice el `smSAP credential set` Comando para habilitar el nuevo host para acceder al perfil de SnapManager usado para el backup original.

- Cargue el perfil en el host nuevo: Utilice el `smsap profile sync` Comando para cargar la información de perfil de SnapManager en el nuevo host.

## Ejecute BRRestORE

Configure el nuevo almacenamiento en el host nuevo con las mismas rutas que el almacenamiento original en el host original.

Utilice la `BRRESTORE` comando para restaurar el backup en el nuevo host. De forma predeterminada, los archivos se restauran en las ubicaciones de ruta de acceso originales. Puede especificar una ruta alternativa para los archivos restaurados con el `-m` opción de `BRRESTORE` comando. Consulte la documentación de SAP para obtener más información acerca de `BRRESTORE`.

## Restauración de un backup desde un almacenamiento secundario a otra ubicación

Puede utilizar el `BRRESTORE` o `smsap restore` comando para restaurar un backup secundario a otra ubicación. El nuevo host también debe ejecutar SnapManager.

Debe configurar el `preferred_backup_locations` y `restore_from_nearest_backup_location` parámetros en la `initSID.utl` archivo para restaurar la copia de seguridad secundaria a la ubicación deseada.

1. Edite el `initSID.utl` archivo.
2. Agregar `preferred_backup_locations` y `restore_from_nearest_backup_location` en el archivo.



La `PREFERRED_BACKUP_LOCATIONS` la variable de entorno anula el valor establecido para `preferred_backup_locations` Parámetro en el archivo `initSID.utl`.



- Si el valor para `preferred_backup_locations` no coincide con ningún nombre de nodo de política de protección y `restore_from_nearest_backup_location` se establece en **No**, la operación falla.
- Si existe el valor para `preferred_backup_locations` no está configurado o `restore_from_nearest_backup_location` se establece en **Yes**, la operación de restauración se puede realizar desde la ubicación de copia de seguridad más cercana.

## Referencia de comandos de SnapManager para SAP

La referencia del comando SnapManager incluye la sintaxis de uso, las opciones, los parámetros y los argumentos que debe proporcionar con los comandos, junto con ejemplos.

Los siguientes problemas se aplican al uso de comandos:

- Los comandos distinguen mayúsculas de minúsculas.
- SnapManager acepta hasta 200 caracteres y etiquetas de hasta 80 caracteres.
- Si el shell del host limita el número de caracteres que pueden aparecer en una línea de comandos, puede utilizar `cmdfile` comando.

- No utilice espacios en nombres de perfiles ni nombres de etiquetas.
- En la especificación del clon, no utilice espacios en la ubicación del clon.

SnapManager puede mostrar tres niveles de mensajes en la consola:

- Mensajes de error
- Mensajes de advertencia
- Mensajes informativos

Puede especificar cómo desea que se muestren los mensajes. Si no especifica nada, SnapManager solo muestra mensajes de error y advertencias en la consola. Para controlar la cantidad de salida que SnapManager muestra en la consola, utilice una de las siguientes opciones de línea de comandos:

- `-quiet`: Muestra sólo los mensajes de error en la consola.
- `-verbose`: Muestra mensajes de error, advertencia e informativos en la consola.



Independientemente del comportamiento predeterminado o del nivel de detalle especificado para la pantalla, SnapManager siempre escribe todos los tipos de mensaje en los archivos de registro.

## El comando `backint register-sld`

Si desea usar SAP BR\*Tools, puede ejecutar el comando `backint register-sld` con SnapManager for SAP para registrar la interfaz BACKINT en el Directorio de entorno del sistema (SLD). El proveedor de almacenamiento proporciona la interfaz BACKINT para que el sistema de almacenamiento funcione con los comandos BR\*Tools. SnapManager para SAP instala su archivo de interfaz BACKINT en `/opt/NetApp/smSAP/bin/`.

### Sintaxis

```
backint register-sld-host host_name-port port_id-username
username-password password-template template_ID
```

### Parámetros

- `-host host_name`

Especifica el nombre del host en el que se ejecuta SAP SLD.

- `-port port_id`

Especifica el ID del puerto en el que el SLD de SAP acepta peticiones HTTP. El ID debe ser numérico e inferior o igual a nueve dígitos.

- `-username username`

Especifica un nombre de usuario de SAP SLD válido y autorizado.

- **-password *password***

Especifica una contraseña de usuario de SAP SLD válida y autorizada. Esto es opcional. Si no define la contraseña mediante `-password`, se le pedirá que introduzca una contraseña en el siguiente formato:

`username@http://host:port`

Si no introduce la contraseña correcta, después de tres intentos, el comando falla y sale.

- **-template *template\_id***

Especifica el nombre del archivo XML de plantilla maestra, que se puede utilizar como base para el archivo personalizado.

### Comando de ejemplo

En el siguiente ejemplo, se muestra una correcta finalización del comando:

```
backint register-sld -host jack12 -port 50100
-username j2ee_admin -password user123 -template /u/template.xml
Operation Id [N96f4142a1442b31ee4636841babbc1d7 succeeded.
```

### El comando `msap_Server restart`

Este comando reinicia el servidor host SnapManager y se introduce como root.

#### Sintaxis

```
msap_server restart
[-quiet | -verbose]
```

#### Parámetros

- **-quiet**

Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

### Comando de ejemplo

En el ejemplo siguiente se reinicia el servidor host.

```
smsap_server restart
```

## El comando start smsap\_Server

Este comando inicia el servidor host que ejecuta SnapManager para software SAP.

### Sintaxis

```
smsap_server start  
[-quiet | -verbose]
```

### Parámetros

- **-quiet**

Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

### Comando de ejemplo

En el ejemplo siguiente se inicia el servidor host.

```
smsap_server start  
SMSAP-17100: SnapManager Server started on secure port 25204 with PID  
11250
```

## El comando smsap\_Server status

Puede ejecutar el `smsap_server status` Comando para ver el estado del servidor de host SnapManager.

### Sintaxis

```
smsap_server status  
[-quiet | -verbose]
```

## Parámetros

- **-quiet**

Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

---

## Ejemplo

En el siguiente ejemplo, se muestra el estado del servidor de host:

```
smsap_server status
SMSAP-17104: SnapManager Server version 3.3.1 is running on secure port
25204 with PID 11250
    and has 0 operations in progress.
```

## El comando smsap\_Server stop

Este comando detiene el servidor host de SnapManager y se introduce en la raíz.

### Sintaxis

```
smsap_server stop
[-quiet | -verbose]
```

## Parámetros

- **-quiet**

Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

---

## Comando de ejemplo

En el ejemplo siguiente se utiliza la `smsap_server` comando `stop`.

```
smsap_server stop
```

## El comando `smsap backup create`

Puede ejecutar el `backup create` comando para crear backups de bases de datos en uno o más sistemas de almacenamiento.

### Sintaxis



Antes de ejecutar este comando, debe crear un perfil de base de datos mediante el comando `profile create`.

```
smsap backup create
-profile profile_name
{[-full{-auto | -online | -offline} [-retain {-hourly | -daily | -weekly |
-monthly | -unlimited} [-verify] |
[-data [[-files files [files] |
[-tablespaces tablespaces [tablespaces] [-label label] {-auto | -online |
-offline}
[-retain {-hourly | -daily | -weekly | -monthly | -unlimited} [-verify |
[-archivelogs [-label label] [-comment comment]]}
[-protect | -noprotect | -protectnow]
[-backup-dest path1 [ , path2]]
[-exclude-dest path1 [ , path2]]
[-prunelogs {-all | -until-scن until-scن | -until-date yyyy-MM-
dd:HH:mm:ss] | -before {-months | -days | -weeks | -hours}}]
-prune-dest prune_dest1,[prune_dest2]]
[-taskspec taskspec]
[-dump-force
[-quiet | -verbose]]
```

### Parámetros

- **-profile *profile\_name***

Especifica el nombre del perfil relacionado con la base de datos de la que desea realizar backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-auto opción**

Si la base de datos está en estado montado o sin conexión, SnapManager realiza un backup sin conexión. Si la base de datos está en estado abierto o en línea, SnapManager realiza un backup en línea. Si utiliza la `-force` con la `-offline` Option, SnapManager fuerza un backup sin conexión incluso si la base de datos está en línea actualmente.

- **-online opción**

Especifica un backup de base de datos en línea.

Es posible crear un backup en línea de una base de datos de Real Application Clusters (RAC), siempre que el primario se encuentre en estado abierto o el primario se monte y una instancia se encuentre en estado abierto. Puede utilizar el `-force` opción para backups en línea si la instancia local está en estado de apagado o no hay ninguna instancia en estado abierto. La versión de Oracle debe ser 10.2.0.5; de lo contrario, la base de datos se bloqueará si existe alguna instancia en el RAC montada.

- Si la instancia local está en estado de cierre y al menos una instancia está en estado abierto, puede utilizar la `-force` opción para cambiar la instancia local al estado montado.
- Si ninguna instancia está en estado abierto, puede utilizar la opción `-force` para cambiar la instancia local al estado abierto.

- **-offline opción**

Especifica una copia de seguridad sin conexión mientras la base de datos está en estado de apagado. Si la base de datos está en estado abierto o montado, el backup genera errores. Si la `-force` Se utiliza la opción, SnapManager intenta modificar el estado de la base de datos para cerrar la base de datos para realizar un backup sin conexión.

- **-full opción**

Realiza un backup de toda la base de datos. Esto incluye todos los datos, registros archivados y archivos de control. Se realiza una copia de seguridad de los redo logs archivados y de los archivos de control, independientemente del tipo de copia de seguridad que realice. Si desea realizar un backup solo de una parte de la base de datos, use la `-files` opción o. `-tablespaces` opción.

- **-data opción**

Especifica los archivos de datos.

- **-files list**

Realiza un backup solo de los archivos de datos especificados, además de los archivos de registro y control archivados. Separe la lista de nombres de archivo con espacios. Si la base de datos se encuentra en estado abierto, SnapManager verifica que los espacios de tablas apropiados se encuentren en modo de backup en línea.

- **-tablespaces tablespaces**

Realiza un backup solo de los espacios de tablas de la base de datos especificados, además de los archivos de registro y control archivados. Separe los nombres de tablespace con espacios. Si la base de datos se encuentra en estado abierto, SnapManager verifica que los espacios de tablas apropiados se encuentren en modo de backup en línea.

- **-label label**



Especifica un nombre opcional para este backup. Este nombre debe ser único dentro del perfil. El nombre puede contener letras, números, guiones bajos (\_) y guiones (-). No puede comenzar con un guión. Si no se especifica una etiqueta, SnapManager crea una etiqueta predeterminada en el formato `scope_type_date`:

- El ámbito es F indicar un backup completo o P para indicar un backup parcial.
- El tipo es C para indicar una copia de seguridad sin conexión (en frío), H para indicar una copia de seguridad en línea (activa) o A para indicar una copia de seguridad automática, por ejemplo, `P_A_20081010060037IST`.
- Fecha es el año, el mes, el día y la hora de la copia de seguridad.

SnapManager se usa un reloj de 24 horas.

Por ejemplo, si realizó un backup completo con la base de datos sin conexión el 16 de enero de 2007, a las 5:45:16 Hora estándar del este, SnapManager crearía la etiqueta `F_C_20070116174516EST`.

#### • **-comment string**

Especifica un comentario opcional para describir esta copia de seguridad. La cadena debe escribirse entre comillas simples (').



Algunos vaciados despegan las comillas. En este caso, se debe incluir la comillas con una barra diagonal inversa (\). Por ejemplo, es posible que deba introducir la siguiente información: `\ ' this is a comment \'`.

#### • **-verify opción**

Verifica que los archivos de la copia de seguridad no están dañados ejecutando la utilidad `oracle dbv`.



Si especifica el `-verify` opción, la operación de backup no se completa hasta que se complete la operación de verificación.

#### • **-force opción**

Fuerza un cambio de estado si la base de datos no está en el estado correcto. Por ejemplo, SnapManager puede cambiar el estado de la base de datos de en línea a sin conexión, según el tipo de backup especificado y el estado en el que está la base de datos.

Con un backup de base de datos RAC en línea, utilice `-force` si la instancia local está en el estado de cierre o ninguna instancia está en el estado abierto.



La versión de Oracle debe ser 10.2.0.5; de lo contrario, la base de datos se bloqueará si existe alguna instancia en el RAC montada.

- Si la instancia local está en estado de cierre y al menos una instancia está en estado abierto, utilice la `-force` opción cambia la instancia local al estado montado.
- Si ninguna instancia está en estado abierto, utilice `-force` opción cambia la instancia local al estado abierto.

#### • **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y

advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

- **-protect | -noprotect | -protectnow**

Indica si el backup debe protegerse a un almacenamiento secundario. La opción `-noProtect` especifica que el backup no debe protegerse en el almacenamiento secundario. Solo se protegen los backups completos. Si se especifica ninguna de las dos opciones, SnapManager protege el backup como predeterminado si el backup es un backup completo y el perfil especifica una política de protección. La `-protectnow` Esta opción solo se aplica a Data ONTAP operando en 7-Mode. La opción especifica que el backup se proteja inmediatamente en el almacenamiento secundario.

- **-retain { -hourly | -daily | -weekly | -monthly | -unlimited}**

Especifica si el backup se debe retener por hora, día, semana, mes o ilimitada. Si la `-retain` no se especifica la opción, la clase de retención predeterminada es `-hourly` opción. Para retener los backups para siempre, utilice la `-unlimited` opción. La `-unlimited` opción hace que el backup no sea apto para su eliminación por parte de la política de retención.

- **-archivelogs opción**

Crea un backup de registro de archivos.

- **-backup-dest path1, [, [path2]]**

Especifica los destinos de registros de archivos que se incluirán en el backup para el backup de registros de archivos.

- **-exclude-dest path1, [, [path2]]**

Especifica los destinos de registro de archivos que se excluirán de la copia de seguridad.

- **-prunelogs {-all | -until-scununtil-scn | -until-date yyyy-MM-dd:HH:mm:ss | -before {-months | -days | -weeks | -hours}}**

Elimina los archivos de registro de archivos de los destinos de registro de archivos según las opciones proporcionadas al crear un backup. La `-all` la opción elimina todos los archivos de registro de archivos de los destinos de registro de archivos. La `-until-scn` La opción elimina los archivos de registro de archivos hasta que se especifique un número de cambio de sistema (SCN). La `-until-date` la opción elimina los archivos de registro de archivos hasta el periodo de tiempo especificado. La `-before` la opción elimina los archivos de registro de archivos antes del período de tiempo especificado (días, meses, semanas, horas).

- **-prune-dest prune\_dest1,prune\_dest2**

Elimina los archivos de registro de archivos de los destinos de registro de archivos mientras se crea el backup.

- **-taskspec taskspec**

Especifica el archivo XML de especificación de la tarea que se puede utilizar para la actividad de

preprocesamiento o la actividad de posprocesamiento de la operación de copia de seguridad. Se debe proporcionar la ruta completa del archivo XML al proporcionar la opción `-taskspec`.

- **-dump opción**

Recoge los archivos de volcado después de una operación de backup de base de datos con errores o realizada correctamente.

## Comando de ejemplo

El siguiente comando crea un backup completo en línea, crea un backup en el almacenamiento secundario y establece la política de retención en diaria:

```
smsap backup create -profile SALES1 -full -online
-label full_backup_sales_May -profile SALESDB -force -retain -daily
Operation Id [8abc01ec0e79356d010e793581f70001] succeeded.
```

## El comando `smsap backup delete`

Puede ejecutar el `backup delete` comando para quitar backups que no se quitan automáticamente, como los backups que se usaron para crear un clon o backups que generaron errores. Puede eliminar backups retenidos de forma ilimitada sin cambiar la clase de retención.

### Sintaxis

```
smsap backup delete
-profile profile_name
[-label label [-data | -archivelogs] | [-id guid | -all]]
-force
[-dump]
[-quiet | -verbose]
```

### Parámetros

- **-profile *profile\_name***

Especifica la base de datos asociada con el backup que desea quitar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id *guid***

Especifica la copia de seguridad con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el `smsap backup list` Comando para mostrar el GUID de cada backup.

- **-label *label***

Especifica el backup con la etiqueta especificada. Opcionalmente, especifique el alcance del backup como archivo de datos o registro de archivo.

- **-data**

Especifica los archivos de datos.

- **-archivelogs**

Especifica los archivos de registro de archivos.

- **-all**

Especifica todos los backups. Para eliminar solo los backups especificados, use la `-id` o `-label` opción.

- **-dump**

Recopila los archivos de volcado después de una operación de eliminación de backup realizada correctamente o con errores.

- **-force**

Fuerza la eliminación del backup. SnapManager elimina el backup incluso si hay problemas para liberar los recursos asociados con el backup. Por ejemplo, si el backup se catalogó con Oracle Recovery Manager (RMAN), pero la base de datos de RMAN ya no existe, incluido `-force` Elimina la copia de seguridad aunque no pueda conectarse con RMAN.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Ejemplo

En el ejemplo siguiente se elimina el backup:

```
smsap backup delete -profile SALES1 -label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

## El comando `smsap backup free`

Puede ejecutar el `backup free` Comando para liberar las copias Snapshot de los backups sin eliminar los metadatos de backup del repositorio.

### Sintaxis

```
smsap backup free
-profile profile_name
[-label label [-data | -archivelogs] | [-id guid | -all]]
-force
[-dump] [-quiet | -verbose]
```

### Parámetros

- **-profile *profile\_name***

Especifica el perfil asociado al backup que desea liberar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id *guid***

Especifica los recursos del backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el `smsap backup list` Comando para mostrar el GUID de cada backup. Incluya el `-verbose` Opción para mostrar los ID de backup.

- **-label *label***

Especifica el backup con la etiqueta especificada.

- **-data**

Especifica los archivos de datos.

- **-archivelogs**

Especifica los archivos de registro de archivos.

- **-all**

Especifica todos los backups. Para eliminar las copias de seguridad especificadas, utilice `-id` o `-label` opción.

- **-force**

Fuerza la eliminación de las copias snapshot.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Ejemplo

En el siguiente ejemplo se libera el backup:

```
smsap backup free -profile SALES1 -label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

## El comando smsap backup list

Puede ejecutar el `backup list` comando para mostrar información sobre los backups de un perfil, incluidos información sobre la clase de retención y el estado de protección.

### Sintaxis

```
smsap backup list
-profile profile_name
-delimiter character
[-data | -archivelogs | -all]
[-quiet | -verbose]]
```

### Parámetros

- **-profile *profile\_name***

Especifica el perfil para el que desea mostrar las copias de seguridad. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-delimiter *character***

Muestra cada fila en una línea diferente. Los atributos de la fila están separados por el carácter especificado.

- **-data**

Especifica los archivos de datos.

- **-archivelogs**

Especifica los archivos de registro de archivos.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola. Incluye el `-verbose` Opción para mostrar los ID de backup. ----

## Ejemplo

En el ejemplo siguiente se enumeran las copias de seguridad del perfil SALES1:

```
smsap backup list -profile SALES1 -verbose
Start Date          Status  Scope  Mode    Primary  Label      Retention
Protection
-----
-----
2007-08-10 14:31:27 SUCCESS FULL   ONLINE  EXISTS   backup1    DAILY
PROTECTED
2007-08-10 14:12:31 SUCCESS FULL   ONLINE  EXISTS   backup2    HOURLY
NOT PROTECTED
2007-08-10 10:52:06 SUCCESS FULL   ONLINE  EXISTS   backup3    HOURLY
PROTECTED
2007-08-05 12:08:37 SUCCESS FULL   ONLINE  EXISTS   backup4    UNLIMITED
NOT PROTECTED
2007-08-05 09:22:08 SUCCESS FULL   OFFLINE EXISTS   backup5    HOURLY
PROTECTED
2007-08-04 22:03:09 SUCCESS FULL   ONLINE  EXISTS   backup6    UNLIMITED
NOT REQUESTED
2007-07-30 18:31:05 SUCCESS FULL   OFFLINE EXISTS   backup7    HOURLY
PROTECTED
```

## El comando smsap backup Mount

Puede ejecutar el `backup mount` comando para montar una copia de seguridad para realizar una operación de recuperación con una herramienta externa.

## Sintaxis

```
smsap backup mount
-profile profile_name
[-label label [-data | -archivelogs] | [-id id]
[-host host
[-from-secondary {-copy-id _id_}]
[-dump]
[-quiet | -verbose]]
```

## Parámetros

- **-profile *profile\_name***

Especifica el perfil asociado con el backup que desea montar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id *guid***

Monta la copia de seguridad con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el `smsap backup list` Comando para mostrar el GUID de cada backup.

- **-label *label***

Monta la copia de seguridad con la etiqueta especificada.

- **-data**

Especifica los archivos de datos.

- **-archivelogs**

Especifica los archivos de registro de archivos.

- **-from-secondary -copy-id *id***

Monta el backup desde el almacenamiento secundario. Si no se especifica esta opción, SnapManager monta el backup desde el almacenamiento principal. Puede utilizar esta opción si se libera el backup.

Debe especificar el `-copy-id` siempre que especifique la `-from-secondary` opción. Si existe más de un backup en el sistema de almacenamiento secundario, el `-copy-id` la opción se utiliza para especificar qué copia de backup en el almacenamiento secundario se debe usar para montar el backup.



Si utiliza Data ONTAP operando en 7-Mode, debe especificar un valor válido para `-copy-id` opción. Sin embargo, si utiliza Clustered Data ONTAP, el `-copy-id` la opción no es necesaria.

- **-host *host***

Especifica el host en el que desea montar el backup.

- **-dump**



Recopila los archivos de volcado después de la operación de montaje correcta o con errores.

- **-quiet**

Muestra sólo mensajes de error en la consola. La configuración predeterminada es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.



Debe utilizar este comando sólo si utiliza una herramienta externa como Oracle Recovery Manager (RMAN). SnapManager se encarga automáticamente del montaje de los backups si se utiliza el `smsap backup restore` comando para restaurar el backup. Este comando muestra una lista, que muestra las rutas donde se han montado las copias Snapshot. Esta lista sólo se muestra cuando la `-verbose` se especifica la opción.

---

## Ejemplo

En el ejemplo siguiente se monta la copia de seguridad:

```
smsap backup mount -profile S10_BACKUP -label full_monthly_10 -verbose
SMSAP-13046 [INFO ]: Operation GUID 8abc013111b9088e0111b908a7560001
starting on Profile S10_BACKUP
SMSAP-08052 [INFO ]: Beginning to connect mount(s)
[/oracle/S10_mirrlogs, /oracle/S10_sapdata] from logical snapshot
SMSAP_S10_BACKUP_S10_F_C_1_8abc013111a450480111a45066210001.
SMSAP-08025 [INFO ]: Beginning to connect mount
/oracle/S10_mirrlogs from snapshot
SMSAP_S10_BACKUP_S10_F_C_1_8abc013111a450480111a45066210001_0 of
volume saplog_S10.
SMSAP-08027 [INFO ]: Finished connecting mount /oracle/S10_mirrlogs from
snapshot
SMSAP_S10_BACKUP_S10_F_C_1_8abc013111a450480111a45066210001_0 of
volume saplog_S10.
SMSAP-08025 [INFO ]: Beginning to connect mount /oracle/S10_sapdata
from snapshot
SMSAP_S10_BACKUP_S10_F_C_1_8abc013111a450480111a45066210001_0 of
volume sapdata_S10.
SMSAP-08027 [INFO ]: Finished connecting mount /oracle/S10_sapdata
from snapshot
SMSAP_S10_BACKUP_S10_F_C_1_8abc013111a450480111a45066210001_0 of
volume sapdata_S10.
SMSAP-08053 [INFO ]: Finished connecting mount(s)
[/oracle/S10_mirrlogs, /oracle/S10_sapdata] from logical snapshot
SMSAP_S10_BACKUP_S10_F_C_1_8abc013111a450480111a45066210001.
SMSAP-13037 [INFO ]: Successfully completed operation: Backup Mount
SMSAP-13048 [INFO ]: Operation Status: SUCCESS
SMSAP-13049 [INFO ]: Elapsed Time: 0:01:00.981
Operation Id [8abc013111b9088e0111b908a7560001] succeeded.
```

## El comando smsap backup restore

Puede ejecutar el `backup restore` comando para restaurar backups de una base de datos o parte de una base de datos y, opcionalmente, recuperar la información de la base de datos.

### Sintaxis

```

smsap backup restore
-profile profile_name
[-label label | -id id]
[-files files [files...] |
-tablespaces tablespaces [tablespaces...]] |
-complete | -controlfiles]
[-recover {-alllogs | -nologs | -until until} [-using-backup-controlfile]
]
[-restorespec restorespec | -from-secondary [-temp-volume temp_volume] [-
copy-id id]]
[-preview]
[-fast {-require | -override | -fallback | -off}]
[-recover-from-location path1 [, path2]] [-taskspec taskspec] [-dump]
[-force]
[-quiet | -verbose]

```

## Parámetros

- **-profile *profile\_name***

Especifica la base de datos que desea restaurar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-label *name***

Restaura el backup con la etiqueta especificada.

- **-id *guid***

Restaura el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando `smsap backup list` para mostrar el GUID de cada copia de seguridad.

- **Elija todos los archivos o especificados**

De manera opcional, puede utilizar una de las siguientes opciones:

- **-complete** Restaura todos los archivos de datos del backup.
- **-tablespaces *list***: Restaura sólo los tablespaces especificados a partir de la copia de seguridad.

Debe utilizar espacios para separar los nombres en la lista.

- **-files *list***: Restaura sólo los archivos de datos especificados desde la copia de seguridad.

Debe utilizar espacios para separar los nombres en la lista. Si la base de datos se está ejecutando, SnapManager garantiza que el tablespace que contiene los archivos esté sin conexión.

- **-controlfiles**

Restaura los archivos de control. SnapManager permite restaurar archivos de control junto con los

archivos de datos de los backups en una única operación. La `-controlfiles` esta opción es independiente de otros parámetros del ámbito de restauración como `-complete`, `-tablespaces`, y `-files`.

- **-recover**

Recupera la base de datos después de restaurarla. También debe especificar el punto en el que desea que SnapManager recupere la base de datos mediante una de las siguientes opciones:

- `-nologs`: Recupera la base de datos al momento de la copia de seguridad y no aplica ningún registro.

Este parámetro se puede usar para backups en línea o sin conexión.

- `-alllogs`: Recupera la base de datos a la última transacción o confirmación, y aplica todos los registros requeridos.
- `-until date`: Recupera la base de datos hasta la fecha y hora especificadas.

Debe utilizar el formato `year-month-date: Hour: Minute: Second (yyyy-mm-dd:hh:mm:ss)`. Para horas, utilice el formato de 12 o 24 horas, según la configuración de la base de datos.

- `-until scn`: Rolls reenvíe los archivos de datos hasta que alcance el número de cambio de sistema (SCN) especificado.
- `-using-backup-controlfile`: Recupera la base de datos utilizando el archivo de control de copia de seguridad.

- **-restorespec**

Permite restaurar los datos en un sistema de archivos activo y restaurar desde los datos especificados mediante la asignación de cada copia Snapshot original a su sistema de archivos activo. Si no especifica una opción, SnapManager restaura los datos desde las copias Snapshot en el almacenamiento principal. Es posible especificar una de las siguientes opciones:

- `-restorespec`: Especifica los datos que se van a restaurar y el formato de restauración.
- `-from-secondary`: Restaura los datos desde el almacenamiento secundario.

No puede utilizar esta opción si el backup existe en el almacenamiento principal; debe liberarse el backup principal antes de poder restaurar un backup desde el almacenamiento secundario. Si se utiliza un volumen temporal, se debe especificar el volumen con el `-temp-volume` opción.

Debe especificar el `-copy-id` siempre que especifique la `-from-secondary` opción. Si existe más de un backup en el sistema de almacenamiento secundario, el `-copy-id` la opción se utiliza para especificar qué copia de backup del almacenamiento secundario debe usarse en la operación de restauración.



Si utiliza Data ONTAP operando en 7-Mode, debe especificar un valor válido para `-copy-id` opción. Sin embargo, si utiliza Clustered Data ONTAP, el `-copy-id` la opción no es necesaria

Cuando se restaura a partir de un almacenamiento secundario, SnapManager intenta en primer lugar restaurar los datos directamente desde el sistema de almacenamiento secundario al sistema de almacenamiento primario (sin afectar el host). Si SnapManager no puede realizar este tipo de restauración (por ejemplo, si los archivos no forman parte del sistema de archivos), SnapManager

recuperará una restauración de copia de archivos del lado del host. SnapManager tiene dos métodos para realizar una restauración de copia de archivos en el lado del host desde secundario. El método que selecciona SnapManager se configura en la `smsap.config` archivo.

- Directo: SnapManager clona los datos en el almacenamiento secundario, monta los datos clonados del sistema de almacenamiento secundario en el host, y después copia los datos del clon en el entorno activo.

Esta es la directiva de acceso secundaria predeterminada.

- Indirecto: SnapManager copia primero los datos en un volumen temporal en el sistema de almacenamiento primario, monta los datos del volumen temporal en el host y, a continuación, copia los datos del volumen temporal en el entorno activo.

Esta política se debe utilizar solo si el host no tiene acceso directo al sistema de almacenamiento secundario. Las restauraciones mediante el método indirecto demorarán el doble de tiempo que la política de acceso secundario directo, ya que se realizan dos copias de los datos.

La decisión de utilizar el método directo o indirecto se controla mediante el valor del `restore.secondaryAccessPolicy` en la `smsap.config` archivo de configuración.

- **-preview**

Muestra la siguiente información:

- Qué mecanismo de restauración (restauración rápida, restauración de sistema de archivos en el lado del almacenamiento, restauración de archivos en el lado del almacenamiento o restauración de copias de archivos del lado del host) se utilizará para restaurar cada archivo
- Por qué no se utilizaron mecanismos más eficientes para restaurar cada archivo, al especificar el `-verbose` Opción Si está utilizando `-preview` debe conocer lo siguiente:
- La `-force` la opción no afecta al comando.
- La `-recover` la opción no afecta al comando.
- La `-fast` opción (`-require`, `-override`, `-fallback`, o `-off`) tiene un impacto significativo en la salida. Para obtener una vista previa de la operación de restauración, se debe montar la base de datos. Si desea obtener la vista previa de un plan de restauración y la base de datos no está montada actualmente, SnapManager monta la base de datos. Si no se puede montar la base de datos, el comando fallará y SnapManager devolverá la base de datos a su estado original.

La `-preview` la opción muestra hasta 20 archivos. Puede configurar el número máximo de archivos que se mostrarán en la `smsap.config` archivo.

- **-fast**

Permite elegir el proceso que se usará en la operación de restauración. Si se cumplen todas las condiciones obligatorias de restauración, es posible forzar a SnapManager para que use el proceso de restauración rápida basado en volúmenes en lugar de otros procesos de restauración. Si no se sabe que no puede realizarse una restauración de volumen, también puede usar este proceso para impedir que SnapManager realice comprobaciones de cumplimiento y la operación de restauración mediante el proceso de restauración rápido.

La `-fast` la opción incluye los siguientes parámetros:

- `-require`: Le permite forzar a SnapManager a realizar una restauración de volumen, si se cumplen todas las condiciones de elegibilidad para la restauración.

Si especifica el `-fast` opción, pero no se debe especificar ningún parámetro para `-fast`, SnapManager utiliza la `-require` parámetro como valor predeterminado.

- `-override`: Permite anular las comprobaciones de elegibilidad no obligatorias y realizar el proceso de restauración rápida basado en el volumen.
- `-fallback`: Permite restaurar la base de datos mediante cualquier método que SnapManager determine.

Si no especifica el `-fast` SnapManager utiliza la opción predeterminada `backup restore -fast fallback` opción.

- `-off`: Le permite evitar el tiempo necesario para realizar las comprobaciones de elegibilidad.

- **`-recover-from-location`**

Especifica la ubicación del registro de archivos externo de los archivos de registro de archivos. SnapManager toma los archivos de registro de archivos de la ubicación externa y los utiliza para el proceso de recuperación.

- **`-taskspec`**

Especifica el archivo XML de especificación de la tarea para la actividad de preprocesamiento o la actividad de posprocesamiento de la operación de restauración. Debe proporcionar la ruta de acceso completa del archivo XML de especificación de la tarea.

- **`-dump`**

Especifica recoger los archivos de volcado después de la operación de restauración.

- **`-force`**

Si es necesario, cambia el estado de la base de datos a uno más bajo que el estado actual. Para Real Application Clusters (RAC), debe incluir la `-force` Si SnapManager tiene que cambiar el estado de cualquier instancia de RAC a un estado inferior.

De forma predeterminada, SnapManager puede cambiar el estado de la base de datos a más alto durante una operación. Esta opción no es necesaria para que SnapManager cambie el estado de la base de datos a uno más alto.

- **`-quiet`**

Muestra sólo mensajes de error en la consola. La configuración predeterminada es mostrar mensajes de error y advertencia.

- **`-verbose`**

Muestra mensajes de error, advertencia e informativos en la consola. Puede usar esta opción para ver por qué no se pueden usar procesos de restauración más eficientes para restaurar el archivo.

## Ejemplo

En el siguiente ejemplo se restaura una base de datos junto con los archivos de control:

```
smsap backup restore -profile SALES1 -label full_backup_sales_May
-complete -controlfiles -force
```

## El comando smsap backup show

Puede utilizar el `backup show` comando para mostrar información detallada sobre un backup, incluidos el estado de protección, la clase de retención de backup y los backups en el almacenamiento principal y secundario.

### Sintaxis

```
smsap backup show
-profile profile_name
[-label label [-data | -archivelogs] | [-id id]
[-quiet | -verbose]
```

### Parámetros

- **-profile *profile\_name***

Especifica el perfil para el que se mostrarán las copias de seguridad. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-label *label***

Especifica la etiqueta del backup.

- **-data**

Especifica los archivos de datos.

- **-archivelogs**

Especifica los archivos de registro de archivos.

- **-id *id***

Especifica el ID del backup.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos de la consola, al igual que cualquier información de clonación y verificación.

---

### **Ejemplo**

El siguiente ejemplo muestra información detallada sobre el backup:



```
smsap backup show -profile SALES1 -label BTNFS -verbose
Backup id: 8abc013111a450480111a45066210001
Backup status: SUCCESS
Primary storage resources: EXISTS
Protection sate: PROTECTED
Retention class: DAILY
Backup scope: FULL
Backup mode: OFFLINE
Mount status: NOT MOUNTED
Backup label: BTNFS
Backup comment:

Backup start time: 2007-03-30 15:26:30
Backup end time: 2007-03-30 15:34:13
Verification status: OK
Backup Retention Policy: NORMAL
Backup database: hsd1
Checkpoint: 2700620
Tablespace: SYSAUX
Datafile: /mnt/ssys1/data/hsdb/sysaux01.dbf [ONLINE]
...
Control Files:
File: /mnt/ssys1/data/control03.ctl
...
Archive Logs:
File: /mnt/ssys1/data/archive_logs/2_131_626174106.dbf
...
Host: Host1
Filesystem: /mnt/ssys1/data
File: /mnt/ssys1/data/hsdb/SMSAPBakCtl_1175283005231_0
...
Volume: hs_data
Snapshot: SMSAP_HSDBR_hsd1_F_C_1_
8abc013111a450480111a45066210001_0
File: /mnt/ssys1/data/hsdb/SMSAPBakCtl_1175283005231_0
...
Protected copies on Secondary Storage:
  14448939 - manow
  88309228 - graffe
```

## El comando smsap backup unmount

Puede ejecutar el backup unmount comando para desmontar un backup.

## Sintaxis

```
smsap backup unmount
-profile profile_name
[-label label [-data | -archivelogs] | [-id id]
[-force]
[-dump] [-quiet | -verbose]
```

## Parámetros

- **-profile *profile\_name***

Especifica el perfil para el que desea desmontar un backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id *id***

Desmonta el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando `smsap backup list` para mostrar el GUID de cada copia de seguridad.

- **-label *label***

Desmonta el backup con la etiqueta especificada.

- **-data**

Especifica los archivos de datos.

- **-archivelogs**

Especifica los archivos de registro de archivos.

- **-dump**

Recoge los archivos de volcado después de una operación de desmontaje correcta o con errores.

- **-force**

Desmonta el backup incluso si hay problemas en la liberación de los recursos asociados con el backup. SnapManager intenta desmontar el backup y borrar todos los recursos asociados. El registro muestra la operación de desmontaje correcta, pero es posible que deba limpiar los recursos de forma manual si hay errores en el registro.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Ejemplo

A continuación se muestra un ejemplo de una operación de desmontaje:

```
# smsap backup unmount -label test -profile SALES1 -verbose
```

```
SMSAP-13046 [INFO ]: Operation GUID 8abc013111b909eb0111b90a02f50001
starting on Profile SALES1
SMSAP-08028 [INFO ]: Beginning to disconnect connected mount(s)
[/u/user1/mnt/_mnt_ssys1_logs_SMSAP_SALES1_hsdb1_F_C_1_8abc013111a45048011
1a45066210001,
 /u/user1/mnt/_mnt_ssys1_data_SMSAP_SALES1_hsdb1_F_C_1_8abc013111a45048011
1a45066210001].
SMSAP-08030 [INFO ]: Done disconnecting connected mount(s)
[/u/user1/mnt/_mnt_ssys1_logs_SMSAP_SALES1_hsdb1_F_C_1_8abc013111a45048011
1a45066210001,
 /u/user1//mnt/_mnt_ssys1_data_SMSAP_SALES1_hsdb1_F_C_1_8abc013111a4504801
11a45066210001].
SMSAP-13037 [INFO ]: Successfully completed operation: Backup Unmount
SMSAP-13048 [INFO ]: Operation Status: SUCCESS
SMSAP-13049 [INFO ]: Elapsed Time: 0:00:33.715
Operation Id [8abc013111b909eb0111b90a02f50001] succeeded.
```

## El comando smsap backup update

Puede ejecutar el `backup update` comando para actualizar la política de retención de backups.

### Sintaxis

```
smsap backup update
-profile profile_name
[-label label [-data | -archivelogs] | [-id guid]
[-retain {-hourly | -daily | -weekly | -monthly | -unlimited}]
[-comment comment_text]
[-quiet | -verbose]
```

### Parámetros

- **-profile *profile\_name***

Especifica el perfil para el que se actualizarán las copias de seguridad. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id *guid***

Verifica el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando `smsap backup list` para mostrar el GUID de cada copia de seguridad.

- **-label *label***

Especifica la etiqueta de backup y el alcance del backup como archivo de datos o registro de archivos.

- **-data**

Especifica los archivos de datos.

- **-archivelogs**

Especifica los archivos de registro de archivos.

- **-comment *comment\_text***

Introduzca texto (hasta 200 caracteres) acerca de la actualización de copia de seguridad. Puede incluir espacios.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

- **-retain {-hourly | -daily | -weekly | -monthly | -unlimited}**

Especifica si el backup se debe retener por hora, día, semana, mes o ilimitada. Si `-retain` no se especifica, la clase de retención predeterminada es `-hourly`. Para retener los backups para siempre, utilice la `-unlimited` opción. La `-unlimited` la opción hace que la copia de seguridad no sea elegible para su eliminación.

---

## Ejemplo

En el ejemplo siguiente se actualiza el backup para establecer la política de retención en Unlimited:

```
smsap backup update -profile SALES1 -label full_backup_sales_May
-retain -unlimited -comment save_forever_monthly_backup
```

## El comando `smsap backup verify`

Puede ejecutar el `backup verify` Comando para ver si el backup tiene un formato válido para Oracle.

### Sintaxis

```
smsap backup verify
-profile profile_name
[-label backup_name- | [-id _guid]
[-retain {-hourly | -daily | -weekly | -monthly | -unlimited}] [-force]
[-dump] [-quiet | -verbose]
```

### Parámetros

- **-profile *profile\_name***

Especifica el perfil para el que desea verificar un backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id *guid***

Verifica el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando `smsap backup list` para mostrar el GUID de cada copia de seguridad.

- **-label *label\_name***

Verifica el backup con la etiqueta especificada.

- **-dump**

Recopila los archivos de volcado después de la operación de verificación de backup realizada correctamente o con errores.

- **-force**

Fuerza a la base de datos al estado necesario para realizar la operación de verificación.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Ejemplo

A continuación se muestra un ejemplo de verificación del backup:

```
smsap backup verify -profile SALES1 -label full_backup_sales_May -quiet
```

```
DBVERIFY - Verification starting : FILE =  
+SMSAP_1_1161675083835/smsmsap/datafile/data.277.582482539 ...
```

## El comando smsap clone create

Puede ejecutar el `clone create` comando para crear el clon de una base de datos con backup. Es posible clonar un backup del almacenamiento primario o secundario.

### Sintaxis

```
smsap clone create  
-profile profile_name  
[-backup-id backup_guid | -backup-label backup_label_name | -current]  
-newsid new_sid  
[-host target_host]  
[-label clone_label  
[-comment string]  
-clonespec full_path_to_clonespec_file  
[-asminstance -asmusername asminstance_username -asmpassword  
asminstance_password]  
[-syspassword syspassword] [-reserve {yes | no | inherit}  
[-from-secondary {-copy-id id]  
[-no-resetlogs | -recover-from-location path1 [, path2]] [-taskspec  
taskspec] [-dump  
[-quiet | -verbose]]
```

### Parámetros

- **-profile *name***

Especifica la base de datos que desea clonar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-backup-id *guid***

Clona el backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Puede utilizar el comando `list-verbose` de `smsap backup` para mostrar el GUID de cada copia de seguridad.

- **-backup-label *backup\_label\_name***

Especifica que se clone el backup con el nombre de etiqueta especificado.

- **-current**

Especifica la creación de backup y clonado a partir del estado actual de la base de datos.



Si la base de datos se encuentra en el modo noarchivelog, SnapManager creará un backup sin conexión.

- **-newsid *new\_sid***

Especifica un nuevo identificador exclusivo del sistema de Oracle para la base de datos clonada. El valor identificador del sistema es un máximo de ocho caracteres. Oracle no permite la ejecución simultánea de dos bases de datos con el mismo identificador de sistema en el mismo host.

- **-host *target\_host***

Especifica el host en el que se debe crear el clon.

- **-label *clone\_label***

Especifica una etiqueta para el clon.

- **-comment *string***

Especifica un comentario opcional para describir este clon. La cadena debe escribirse entre comillas simples.



Algunos vaciados eliminan las comillas. Si esto es cierto para el shell, debe escapar de las comillas con una barra invertida (\). Por ejemplo, es posible que deba introducir: \  
is a comment\'

- **-clonespec *full\_path\_to\_clonespec\_file***

Especifica la ruta de acceso al archivo XML de especificación del clon. Puede ser un nombre de ruta relativo o absoluto.

- **-asminstance**

Especifica las credenciales que se utilizan para iniciar sesión en la instancia de ASM.

- **-asmusername *asminstance\_username***

Especifica el nombre de usuario que se utiliza para iniciar sesión en la instancia de ASM.

- **-asmpassword *asminstance\_password***

Especifica la contraseña que se utiliza para iniciar sesión en la instancia de ASM.

- **-syspassword *syspassword***

Especifica la contraseña para el usuario con privilegios sys.



Debe proporcionar la contraseña para el usuario con privilegios sys si las credenciales de la base de datos proporcionadas no son las mismas para el usuario con privilegios sys.

- **-reserve**

Ajuste de `-reserve` la opción de "sí" garantiza que la reserva de espacio de garantía de volumen esté activada para los volúmenes de clones nuevos. Ajuste de `-reserve` la opción a no garantiza que la reserva de espacio de garantía de volumen esté desactivada para los volúmenes clonados nuevos. Ajuste de `-reserve` opción a **inherit** Garantiza que el clon nuevo herede las características de reserva de espacio de la copia Snapshot principal. El valor predeterminado es **no**.

En la siguiente tabla se describen los métodos de clonado y su efecto en la operación de creación de clon y su `-reserve` opción. Una LUN se puede clonar mediante cualquiera de estos métodos.

Método de clonación	Descripción	Resultado
Clonado de LUN	Se crea un nuevo LUN clon en el mismo volumen.	Cuando la <code>-reserve</code> La opción para una LUN está establecida en Sí, se reserva espacio para todo el tamaño de LUN dentro del volumen.
Clonado de volúmenes	Se crea un nuevo FlexClone y la LUN clonada existe dentro del nuevo volumen clonado. Utiliza la tecnología FlexClone.	Cuando la <code>-reserve</code> opción para un volumen se establece en yes, se reserva espacio para todo el tamaño del volumen dentro del agregado.

- **-from-secondary [-copy-id copy\_id]**

Especifica que SnapManager debe clonar una copia de un backup que se protegió en el almacenamiento secundario. Si no se especifica esta opción, SnapManager clona la copia desde el almacenamiento principal.

Debe especificar el `-copy-id` siempre que especifique la `-from-secondary` opción. Si existe más de un backup en el sistema de almacenamiento secundario, la opción `-copy-id` se utiliza para especificar qué copia de backup en el almacenamiento secundario se debe usar para clonar.



Si utiliza Data ONTAP operando en 7-Mode, debe especificar un valor válido para `-copy-id` opción. Sin embargo, si utiliza Clustered Data ONTAP, el `-copy-id` la opción no es necesaria.

- **-no-resetlogs**

Especifica omitir la recuperación de la base de datos, ejecutar la utilidad DBNEWID y no abrir la base de datos con los registros de nuevo mientras se crea el clon.

- **-recover-from-location**

Especifica la ubicación del registro de archivos externo de los backups de registros de archivos donde



SnapManager toma los archivos de registro de archivos de la ubicación externa y los utiliza para la clonado.

- **-taskspec**

Especifica el archivo XML de especificación de la tarea para la actividad de procesamiento previo o la actividad de procesamiento posterior de la operación de clonado. Debe proporcionar la ruta de acceso completa del archivo XML de especificación de la tarea.

- **-dump**

Especifica recoger los archivos de volcado después de la operación de creación de clones.

- **-quiet**

Muestra sólo mensajes de error en la consola. La configuración predeterminada es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Ejemplo

En el ejemplo siguiente se clona el backup mediante una especificación de clon que se crea para este clon:

```
smsap clone create -profile SALES1 -backup-label full_backup_sales_May
-newsid
CLONE -label sales1_clone -clonespec
/opt/<path>/smsap/clonespecs/sales1_clonespec.xml
```

```
Operation Id [8abc01ec0e794e3f010e794e6e9b0001] succeeded.
```

---

## El comando `smsap clone delete`

Puede ejecutar el `clone delete` comando para eliminar un clon. No es posible eliminar un clon si utiliza algún operación.

### Sintaxis

```
smsap clone delete
-profile profile_name
[-id guid | -label clone_name]
[-login
[-username db_username -password db_password -port db_port]
[-asminstance -asmusername asminstance_username -asmpassword
asminstance_password]]
[-syspassword _syspassword_] -force
[-dump] [-quiet | -verbose]
```

## Parámetros

- **-profile *profile\_name***

Especifica el nombre del perfil que contiene el clon que se va a eliminar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-force**

Elimina el clon incluso si hay recursos asociados con el clon.

- **-id *guid***

Especifica el GUID del clon que se va a eliminar. SnapManager genera el GUID cuando se crea un clon. Puede utilizar el `smsap clone list` Comando para mostrar el GUID de cada clon.

- **-label *name***

Especifica la etiqueta del clon que se va a eliminar.

- **-asminstance**

Especifica las credenciales que se utilizan para iniciar sesión en la instancia de Automatic Storage Management (ASM).

- **-asmusername *asminstance\_username***

Especifica el nombre de usuario utilizado para iniciar sesión en la instancia de ASM.

- **-asmpassword *asminstance\_password***

Especifica la contraseña utilizada para iniciar sesión en la instancia de ASM.

- **-syspassword *syspassword***

Especifica la contraseña para el usuario con privilegios sys.



Debe proporcionar la contraseña para el usuario con privilegios sys si las credenciales de la base de datos proporcionadas no son las mismas para el usuario con privilegios sys.

- **-login**

Permite introducir los detalles de inicio de sesión de la base de datos.

- **-username *db\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos.

- **-password *db\_password***

Especifica la contraseña necesaria para acceder a la base de datos.

- **-port *db\_port***

Especifica el número de puerto TCP utilizado para acceder a la base de datos que describe el perfil.

- **-dump**

Especifica que se recopilen los archivos de volcado después de la operación de eliminación de clones.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Ejemplo

En el ejemplo siguiente se elimina el clon:

```
smsap clone delete -profile SALES1 -label SALES_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

---

## El comando `smsap clone list`

Este comando enumera los clones de la base de datos para un perfil determinado.

### Sintaxis

```
smsap clone list
-profile profile_name
-delimiter character
[-quiet | -verbose
```

## Parámetros

- **-profile *profile\_name***

Especifica la lista de clones asociados con el perfil. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-delimiter *character***

Cuando se especifica este parámetro, el comando enumera los atributos de cada fila separados por el carácter especificado.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Comando de ejemplo

En el siguiente ejemplo se enumeran los clones de base de datos del perfil SALES1.

```
smsap clone list -profile SALES1 -verbose
```

```
ID Status SID Host Label Comment
-----
8ab...01 SUCCESS hsdhc server1 back1clone test comment
```

## El comando smsap clone show

Puede ejecutar el `clone show` comando para mostrar información sobre los clones de la base de datos del perfil especificado.

## Sintaxis

```
smsap clone show
-profile profile_name
[-id guid | -label clone_name]
[-quiet | -verbose]
```

## Parámetros

- **-profile *profile\_name***

Especifica la lista de clones asociados con el perfil. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id *guid***

Muestra información sobre el clon con el GUID especificado. SnapManager genera el GUID cuando se crea un clon. Puede utilizar el `smsap clone show` Comando para mostrar el GUID de cada clon.

- **-label *label\_name***

Muestra información sobre el clon con la etiqueta especificada.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Ejemplo

En el siguiente ejemplo se muestra información sobre el clon:

```
smsap clone show -profile SALES1 -label full_backup_sales_May -verbose
```

---

En la siguiente salida se muestra información sobre un clon de un backup en el almacenamiento primario:

```
Clone id: 8abc013111b916e30111b916ffb40001
Clone status: SUCCESS
Clone SID: hsdbc
Clone label: hsdbc
Clone comment: null
Clone start time: 2007-04-03 16:15:50
Clone end time: 2007-04-03 16:18:17
Clone host: Host1
Filesystem: /mnt/ssys1/data_clone
File: /mnt/ssys1/data_clone/hsdb/sysaux01.dbf
File: /mnt/ssys1/data_clone/hsdb/undotbs01.dbf
File: /mnt/ssys1/data_clone/hsdb/users01.dbf
File: /mnt/ssys1/data_clone/hsdb/system01.dbf
File: /mnt/ssys1/data_clone/hsdb/undotbs02.dbf
Backup id: 8abc013111a450480111a45066210001
Backup label: full_backup_sales_May
Backup SID: hsdb1
Backup comment:
Backup start time: 2007-03-30 15:26:30
Backup end time: 2007-03-30 15:34:13
Backup host: server1
```

---

En el siguiente resultado, se muestra información sobre un clon de un backup protegido en el almacenamiento secundario:

```
clone show -label clone_CLSTEST -profile
TEST_USER_NFSTEST_DIRMAC
Clone id:8abc01ec16514aec0116514af52f0001
Clone status: SUCCESS
Clone SID: CLSTEST
Clone label: clone_CLSTEST
Clone comment:comment_for_clone_CLSTEST
Clone start time: 2007-11-18 00:46:10
Clone end time: 2007-11-18 00:47:54
Clone host: dirmac
Filesystem: /ant/fish/bt_dirmac_nfs_clone
File: /ant/fish/bt_dirmac_nfs_clone/datafiles/sysaux01.dbf
File: /ant/fish/bt_dirmac_nfs_clone/datafiles/system01.dbf
File: /ant/fish/bt_dirmac_nfs_clone/datafiles/undotbs01.dbf
File: /ant/fish/bt_dirmac_nfs_clone/datafiles/users01.dbf
Backup id: 8abc01ec16514883011651488b580001
Backup label:full_backup
Backup SID: NFSTEST
Backup comment:
Backup start time: 2007-11-18 00:43:32
Backup end time: 2007-11-18 00:45:30
Backup host: dirmac
Storage System: fish (Secondary storage)
Volume: bt_dirmac_nfs
Snapshot:smsap_user_nfstest_b_nfstest_f_c_1_8abc01ec16511d6a0116511d735900
01_0
File: /ant/fish/bt_dirmac_nfs/archlogs/1_14_638851420.dbf
File: /ant/fish/bt_dirmac_nfs/datafiles/sysaux01.dbf
File: /ant/fish/bt_dirmac_nfs/datafiles/undotbs01.dbf
File: /ant/fish/bt_dirmac_nfs/archlogs/1_13_638851420.dbf
File: /ant/fish/bt_dirmac_nfs/archlogs_2/1_16_638851420.dbf
File: /ant/fish/bt_dirmac_nfs/datafiles/users01.dbf
File: /ant/fish/bt_dirmac_nfs/controlfiles/SMSAPBakCtl_1195361899651_2
File: /ant/fish/bt_dirmac_nfs/datafiles/system01.dbf
```

## El comando smsap clone template

Este comando permite crear una plantilla de especificación de clon.

### Sintaxis

```
smsap clone template
-profile name
[-backup-id guid | -backup-label backup_name]
[-quiet | -verbose]
```

## Parámetros

- **-profile *name***

Especifica la base de datos que desea crear una especificación de clon de. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-backup-id *guid***

Crea una especificación de clon a partir del backup con el GUID especificado. SnapManager genera el GUID cuando se crea un backup. Utilice el comando `smsap backup list` para mostrar el GUID de cada copia de seguridad.

- **-backup-label *backup\_label\_name***

Crea una especificación de clonado a partir del backup con la etiqueta de backup especificada.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Comando de ejemplo

En el siguiente ejemplo, se crea una plantilla de especificación de clon a partir del backup con la etiqueta `full_backup_sales_May`. Una vez completado el comando `smsap clone template`, la plantilla de especificación del clon estará completa.

```
smsap clone template -profile SALES1 -backup-label full_backup_sales_May
Operation Id [8abc01ec0e79004b010e79006da60001] succeeded.
```

## El comando `smsap clone update`

Este comando actualiza información acerca del clon. Puede actualizar el comentario.



## Sintaxis

```
smsap clone update
-profile profile_name
[-label label | -id id]
-comment comment_text [-quiet | -verbose]
```

## Parámetros

- **-profile *profile\_name***

Especifica el nombre del perfil que contiene el clon que desea actualizar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-id *id***

Especifica el ID del clon. SnapManager genera el ID cuando crea un clon. Utilice la `smsap clone list` Comando para mostrar el ID de cada clon.

- **-label *label***

Especifica la etiqueta del clon.

- **-comment**

Muestra el comentario introducido en la creación del clon. Este es un parámetro opcional.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Comando de ejemplo

En el siguiente ejemplo se actualiza el comentario del clon.

```
smsap clone update -profile anson.pcrac5
-label clone_pcrac51_20080820141624EDT -comment See updated clone
```

## El comando `smsap clone split-delete`

Este comando permite eliminar una entrada de ciclo de operaciones de división de clones de una base de datos del repositorio.

### Sintaxis

```
smsap clone split-delete
-profile profile [-host hostname]
[-label split-label | -id split-id]
[-quiet | -verbose]
```

### Parámetros

- **-profile *profile***

Especifica el nombre del perfil del clon.

- **-host *hostname***

Especifica el nombre de host en el que existe el clon.

- **-label *split-label***

Especifica el nombre de etiqueta generado por el proceso de inicio de división de clones.

- **-id *split-id***

Especifica el ID único generado por el proceso de inicio de división de clones.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## El comando `smsap clone split-estimation`

Este comando permite ver la cantidad de división de clones del almacenamiento consumido.

### Sintaxis

```
smsap clone split-estimate
-profile profile
[-host hostname]
[-label clone-label | -id clone-id]
[-quiet | -verbose]
```

## Parámetros

- **-profile *profile***

Especifica el nombre del perfil del clon.

- **-host *hostname***

Especifica el nombre de host en el que existe el clon.

- **-label *clone-label***

Especifica el nombre de etiqueta generado por el proceso de clonado.

- **-id *clone-id***

Especifica el ID único generado por el proceso de clonado.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## El comando `smsap clone split`

Puede ejecutar el `clone split` comando para dividir un clon. El clon de división se independiza del clon original. SnapManager genera un nuevo perfil después de la operación de división de clones y se puede usar este perfil para gestionar el clon dividido.

## Sintaxis

```

smsap clone split
-profile clone-profile
[-host hostname]
{-label clone-label | -id clone-id} [-split-label split-operation_label]
[-comment comment]
-new-profile new-profile-name [-profile-password new-profile_password]
-repository -dbname repo_service_name
-host repo_host
-port repo_port
-login -username repo_username
-database -dbname db_dbname
-host db_host [-sid db_sid] [-login -username db_username -password
db_password
-port db_port]
[-rman {{-controlfile | {-login -username rman_username
-password rman_password} -tnsname rman_tnsname}}]
-osaccount osaccount
-osgroup osgroup
[-retain
[-hourly [-count n] [-duration m]]
[-daily [-count n] [-duration m]]
[-weekly [-count n] [-duration m]]
[-monthly [-count n] [-duration m]] ]
[-profile-comment profile-comment]
[-snapname-pattern pattern]
[-protect [-protection-policy policy_name]] | [-noprotect]]
[-summary-notification
[-notification
[-success -email email_address1,email_address2
-subject subject-pattern]
[failure -email email_address1,email_address2
-subject subject-pattern] ]
[-separate-archivelog-backups
-retain-archivelog-backups -hours hours |
-days days |
-weeks weeks |
-months months
[-protect [-protection-policy policy_name | -noprotect]
[-include-with-online-backups | -no-include-with-online-backups]]
[-dump]
[-quiet | -verbose]

```

## Parámetros

- **-profile *clone-profile***

Especifica el nombre del perfil a partir del cual se crea el clon.

- **-host *hostname***

Especifica el nombre de host en el que existe el clon.

- **label *clone-label***

Especifica el nombre de etiqueta generado por la operación de clonado.

- **-id *clone-id***

Especifica el ID único generado por la operación de clonado.

- **-split-label *split-operation\_label***

Especifica el nombre de etiqueta generado por la operación de clonado.

- **-new-profile *new-profile\_name***

Especifica el nuevo nombre de perfil que generará SnapManager después de una operación de división correcta.

- **-profile-password *new-profile\_password***

Especifica la contraseña del perfil.

- **-repository**

Especifica los detalles de la base de datos para el repositorio.

- **-dbname *repo\_service\_name***

Especifica el nombre de la base de datos que almacena el repositorio. Es posible usar el nombre global o el identificador del sistema.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del equipo host en el que reside la base de datos del repositorio.

- **-port *repo\_port***

Especifica el número de puerto del protocolo de control de transmisión (TCP) que se utiliza para acceder al host en el que reside la base de datos del repositorio.

- **-login**

Especifica los detalles de inicio de sesión del repositorio. Esto es opcional. Si no se especifica, SnapManager toma de forma predeterminada el modo de conexión de autenticación del sistema operativo.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder al host en el que reside la base de datos del repositorio.

- **-database**

Especifica los detalles de la base de datos que se realizará un backup, se restaurará o se clonará.

- **-dbname *db\_dbname***

Especifica el nombre de la base de datos que describe el perfil. Es posible usar el nombre global o el identificador del sistema.

- **-host *db\_host***

Especifica el nombre o la dirección IP del equipo host en el que reside la base de datos.

- **-sid *db\_sid***

Especifica el identificador del sistema de la base de datos que describe el perfil. De forma predeterminada, SnapManager utiliza el nombre de la base de datos como identificador del sistema. Si el identificador del sistema es diferente del nombre de la base de datos, debe especificarlo mediante el `-sid` opción.

- **-login**

Especifica los detalles de inicio de sesión de la base de datos.

- **-username *db\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos que describe el perfil.

- **-password *db\_password***

Especifica la contraseña necesaria para acceder a la base de datos que describe el perfil.

- **-osaccount *osaccount***

Especifica el nombre de la cuenta de usuario de la base de datos Oracle. SnapManager utiliza esta cuenta para realizar operaciones de Oracle como el inicio y el apagado. Normalmente es el usuario propietario del software Oracle en el host, por ejemplo, `orasid`.

- **-osgroup *osgroup***

Especifica el nombre del grupo de base de datos Oracle asociado a la cuenta `orasid`.



La `-osaccount` y `-osgroup` Las variables son necesarias para UNIX, pero no se permiten para las bases de datos que se ejecutan en Windows.

- **-retain [-hourly [-count *n*] [-duration *m*]] [-daily [-count *n*] [-duration *m*]] [-weekly [-count *n*] [-duration *m*]] [-monthly [-count *n*] [-duration *m*]]**

Especifica la política de retención para un backup.

Para cada clase de retención, se puede especificar el recuento de retención o la duración de la retención, o bien tanto. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora, días por día). Por ejemplo, si especifica solo una duración de retención de 7 para backups diarios, SnapManager no limitará la cantidad de backups diarios del perfil (ya que el número de retención es 0), pero SnapManager

eliminará automáticamente los backups diarios creados hace más de 7 días.

- **-profile-comment *profile-comment***

Especifica el comentario de un perfil que describe el dominio del perfil.

- **-snapname-pattern *pattern***

Especifica el patrón de nomenclatura para las copias Snapshot. También puede incluir texto personalizado, por ejemplo, HOPS para operaciones altamente disponibles, en todos los nombres de copias Snapshot. Puede cambiar el patrón de nomenclatura de las copias Snapshot al crear un perfil o después de crear el perfil. El patrón actualizado se aplica solo a las copias snapshot que aún no se han creado. Las copias Snapshot que existen conservan el patrón Snapname anterior. Puede utilizar varias variables en el texto del patrón.

- **-protect -protection-policy *policy\_name***

Especifica si el backup debe protegerse en el almacenamiento secundario.



Si `-protect` se especifica sin `-protection-policy`, entonces el conjunto de datos no tendrá una política de protección. Si `-protect` se especifica y `-protection-policy` no se establece cuando se crea el perfil y, a continuación, puede establecerlo más adelante `smsap profile update` o bien lo establezca el administrador de almacenamiento mediante la consola de Protection Manager.

- **-summary-notification**

Especifica los detalles para configurar la notificación de resumen por correo electrónico para varios perfiles en una base de datos de repositorio. SnapManager genera este correo electrónico.

- **-notification**

Especifica los detalles para configurar la notificación por correo electrónico para el nuevo perfil. SnapManager genera este correo electrónico. La notificación por correo electrónico permite al administrador de la base de datos recibir correos electrónicos sobre el estado correcto o con errores de la operación de base de datos que se realiza mediante este perfil.

- **-success**

Especifica que la notificación de correo electrónico está habilitada para un perfil para cuando la operación de SnapManager se realiza correctamente.

- **-email *email address 1 email address 2***

Especifica la dirección de correo electrónico del destinatario.

- **-subject *subject-pattern***

Especifica el asunto del correo electrónico.

- **-failure**

Especifica que la notificación por correo electrónico está habilitada para un perfil para cuando se produce un error en la operación de SnapManager.

- **-separate-archivelog-backups**

Especifica que el backup de registros de archivos está separado del backup del archivo de datos. Se trata de un parámetro opcional que puede proporcionar al crear el perfil. Después de separar los backups con esta opción, es posible crear backup solo de archivos de datos o backup de solo registros de archivos.

- **-retain-archivelog-backups -hours *hours* | -days *days* | -weeks *weeks* | -months *months***

Especifica que los backups de los registros de archivos se retendrán según la duración de la retención de los registros de archivo (horaria, diaria, semanal o mensual).

- **protect [-protection-policy *policy\_name*] | -noprotect**

Especifica que los archivos de registro de archivos están protegidos en función de la política de protección del registro de archivos.

Especifica que los archivos de registro de archivos no están protegidos mediante el `-noprotect` opción.

- **-include-with-online-backups | -no-include-with-online-backups**

Especifica que el backup de registros de archivos se incluye junto con el backup de la base de datos en línea.

Especifica que no se incluyen los backups de registros de archivos junto con el backup de la base de datos en línea.

- **-dump**

Especifica que los archivos de volcado no se recopilan después de la operación de creación de perfiles correcta.

- **-quiet**

Muestra sólo mensajes de error en la consola. La configuración predeterminada muestra mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## El comando `msap clone split-result`

### Sintaxis

Este comando permite ver el resultado del proceso de división de clones.



```
smsap clone split-result
-profile profile
[-host hostname]
[-label split-label | -id split-id]
[-quiet | -verbose]
```

## Parámetros

- **-profile *profile***

Especifica el nombre del perfil del clon.

- **-host *hostname***

Especifica el nombre de host en el que existe el clon.

- **-label *split-label***

Especifica el nombre de etiqueta generado por el proceso de inicio de división de clones.

- **-id *split-id***

Especifica un ID único generado por el proceso de inicio de división de clones.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## El comando `smsap clone split-stop`

Este comando detiene el proceso de división de clones en ejecución.

### Sintaxis

```
smsap clone split-stop
-profile profile
[-host hostname]
[-label split-label | -id split-id]
[-quiet | -verbose]
```

## Parámetros

- **-profile *profile***

Especifica el nombre del perfil del clon.

- **-host *hostname***

Especifica el nombre de host en el que existe el clon.

- **-label *split-label***

Especifica el nombre de etiqueta generado por el proceso de clonado.

- **-id *split-id***

Especifica el ID único generado por el proceso de clonado.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## El comando `smsap clone split-status`

Este comando le permite conocer el progreso de la ejecución del proceso de división.

### Sintaxis

```
smsap clone split-status
-profile profile
[-host hostname]
[-label split-label | -id split-id]
[-quiet | -verbose]
```

### Parámetros

- **-profile *profile***

Especifica el nombre del perfil del clon.

- **-host *hostname***

Especifica el nombre de host en el que existe el clon.

- **-label *split-label***

Especifica el nombre de etiqueta generado por el proceso de clonado.

- **-id *split-id***

Especifica el ID único generado por el proceso de clonado.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## El comando `smsap clone detach`

Después de dividir un volumen clonado de su volumen principal en Data ONTAP, se puede ejecutar el comando `clone detach` desde SnapManager para hacer saber a SnapManager que el volumen ya no es un clon.

### Sintaxis

```
smsap clone detach -profile profile_name -label clone_label
```

### Parámetros

- **-profile *profile\_name***

Especifica el nombre del perfil a partir del cual se crea el clon.

- **-label *clone\_label***

Especifica el nombre generado por la operación de clonado.

### Ejemplo

El siguiente comando desvincula el clon:

```
smsap clone detach -profile SALES1 -label sales1_clone
```

## El comando `scmcmdfile`

Puede utilizar el `cmdfile` comando para ejecutar cualquier comando si el shell del host limita el número de caracteres que pueden aparecer en una línea de comandos.

### Sintaxis

```
smsap cmdfile
-file file_name
[-quiet | -verbose]
```

Puede incluir el comando en un archivo de texto y utilizar `smsap cmdfile` comando para ejecutar el comando. Sólo puede agregar un comando en un archivo de texto. No debe incluir `smsap` en la sintaxis del comando.



La `smsap cmdfile` el comando sustituye al `smsap pfile` comando. La `smsap cmdfile` no es compatible con `smsap pfile` comando.

## Parámetros

- **-file *file\_name***

Especifica la ruta de acceso al archivo de texto que contiene el comando que desea ejecutar.

- **-quiet**

Especifica que sólo se muestran mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Especifica que los mensajes de error, advertencia e informativos se muestran en la consola.

## Ejemplo

En este ejemplo se crea un perfil incluyendo `profile create` comando en `command.txt` situado en `/tmp`. A continuación, puede ejecutar el `smsap cmdfile` comando.

El archivo de texto contiene la siguiente información:

```
profile create -profile SALES1 -repository -dbname SNAPMGR
-login -username server1_user -password ontap -port 1521 -host server1
-database -dbname SMSMSAP -sid SMSMSAP -login -username sys -password
oracle -port 1521
-host Host2 -osaccount oracle -osgroup db2
```

Ahora puede crear el perfil ejecutando `smsap cmdfile` con el `command.txt` archivo:

```
smsap cmdfile -file /tmp/command.txt
```

## El comando `smsap credential clear`

Este comando borra la caché de las credenciales de usuario de todos los recursos protegidos.

### Sintaxis

```
smsap credential clear  
[-quiet | -verbose]
```

### Parámetros

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

### Comando de ejemplo

En este ejemplo se borran todas las credenciales del usuario que ejecuta el comando.

```
smsap credential clear -verbose
```

```
SMSAP-20024 [INFO ]: Cleared credentials for user "user1".
```

## El comando `smsap credential delete`

Este comando elimina las credenciales de usuario de un recurso protegido en particular.

### Sintaxis

```
smsap credential delete
[-host -name host_name
-username username] |
[-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port] |
[-profile
-name profile_name]
[-quiet | -verbose]
```

## Parámetros

- **-host *hostname***

Especifica el nombre del servidor host en el que se ejecuta SnapManager.

La `-host` el parámetro incluye las siguientes opciones:

- `-name host_name`: Especifica el nombre del host para el que se eliminará la contraseña.
- `-username user_name`: Especifica el nombre de usuario en el host.

- **-repository -dbname**

Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

La `-repository` el parámetro incluye las siguientes opciones:

- `-dbname repo_service_name`: Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.
- `-host repo_host`: Especifica el nombre o la dirección IP del servidor host en el que se ejecuta la base de datos de repositorio.
- `-login-username repo_username`: Especifica el nombre de usuario necesario para tener acceso a la base de datos que almacena el repositorio.
- `-port repo_port`: Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-profile -name *profile\_name***

Especifica el perfil con el que está asociada la base de datos.

La `-profile` el parámetro incluye la siguiente opción:

- `-name profilename`: Especifica el nombre del perfil para el que se eliminará la contraseña.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y

advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

### Comando de ejemplo

En este ejemplo se eliminan las credenciales del perfil.

```
smsap credential delete -profile -name user1 -verbose
```

```
SMSAP-20022 [INFO ]: Deleted credentials and repository mapping  
for profile "user1" in user credentials for "user1".
```

En este ejemplo, se eliminan las credenciales del repositorio.

```
smsap credential delete -repository -dbname SMSAPREPO -host Host2  
-login -username user1 -port 1521
```

```
SMSAP-20023 [INFO ]: Deleted repository credentials for  
"user1@SMSAPREPO/wasp:1521"  
and associated profile mappings in user credentials for "user1".
```

En este ejemplo, se eliminan las credenciales del host.

```
smsap credential delete -host -name Host2
```

```
SMSAP-20033 [INFO ]: Deleted host credentials for "Host2" in user  
credentials for "user1".
```

---

### El comando smsap credential list

Este comando enumera todas las credenciales de un usuario.

#### Sintaxis

```
smsap credential list
[-quiet | -verbose]
```

## Parámetros

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Comando de ejemplo

Este ejemplo muestra todas las credenciales del usuario que ejecuta el comando.

```
smsap credential list
```

```
Credential cache for OS user "user1":
Repositories:
Host1_test_user@SMSAPREPO/hotspur:1521
Host2_test_user@SMSAPREPO/hotspur:1521
user1_1@SMSAPREPO/hotspur:1521
Profiles:
HSDBR (Repository: user1_2_1@SMSAPREPO/hotspur:1521)
PBCASM (Repository: user1_2_1@SMSAPREPO/hotspur:1521)
HSDB (Repository: Host1_test_user@SMSAPREPO/hotspur:1521) [PASSWORD NOT
SET]
Hosts:
Host2
Host5
Host4
Host1
```

## El comando smsap credential set

Este comando permite establecer las credenciales para que los usuarios accedan a recursos seguros, como hosts, repositorios y perfiles de bases de datos. La contraseña del host es la contraseña del usuario en el host donde se ejecuta SnapManager. La



contraseña del repositorio es la contraseña del usuario de Oracle que contiene el esquema del repositorio de SnapManager. La contraseña del perfil es una contraseña compuesta por la persona que crea el perfil. Para las opciones del host y del repositorio, si es opcional `-password` no se incluye la opción, se le pedirá que introduzca una contraseña del tipo especificado en los argumentos de comando.

## Sintaxis

```
smsap credential set
[-host
-name host_name
-username username]
[-password password] ] |
[-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username] [-password repo_password] ]
-port repo_port |
[-profile
-name profile_name]
[-password password] ]
[-quiet | -verbose]
```

## Parámetros

- **-host *hostname***

Especifica el nombre o la dirección IP del servidor host en el que se ejecuta SnapManager.

La `-host` el parámetro incluye las siguientes opciones:

- `-name host_name`: Especifica el nombre del host para el que se establecerá la contraseña.
- `-username user_name`: Especifica el nombre de usuario en el host.
- `-password password` Especifica la contraseña del usuario en el host.

- **-repository -dbname**

Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

La `-repository` el parámetro incluye las siguientes opciones:

- `-dbname repo_service_name`: Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.
- `-host repo_host`: Especifica el nombre o la dirección IP del servidor host en el que se ejecuta la base de datos de repositorio.
- `-login-username repo_username`: Especifica el nombre de usuario necesario para tener acceso a la base de datos que almacena el repositorio.

- `-password password`: Especifica la contraseña necesaria para tener acceso a la base de datos que almacena el repositorio.
- `-port repo_port`: Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **`-profile -name profile_name`**

Especifica el perfil con el que está asociada la base de datos.

La `-profile` el parámetro incluye la siguiente opción:

- `-name profilename`: Especifica el nombre del perfil para el que se establecerá la contraseña.
- `-password password`: Especifica la contraseña necesaria para acceder al perfil.

- **`-quiet`**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **`-verbose`**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Ejemplo de comando para configurar las credenciales del repositorio

En el ejemplo siguiente se establecen credenciales para un repositorio.

```
smsap credential set -repository -dbname SMSAPREPO -host hotspur -port
1527 -login -username chris
Password for chris@hotspur:1527/SMSAPREPO : *****
Confirm password for chris@hotspur:1527/SMSAPREPO : *****
```

```
SMSAP-12345 [INFO ]: Updating credential cache for OS user "admin1"
SMSAP-12345 [INFO ]: Set repository credential for user "user1" on
rep01@Host2.
Operation Id [Nff8080810da9018f010da901a0170001] succeeded.
```

---

## Ejemplo de comando para configurar las credenciales del host

Dado que las credenciales de host representan una credencial real del sistema operativo, deben incluir el nombre de usuario además de la contraseña.

```
smsap credential set -host -name bismarck -username avida
Password for avida@bismarck : *****
Confirm password for avida@bismarck : *****
```

## El comando smsap history list

Este comando le permite ver una lista de detalles del historial de la operación SnapManager.

### Sintaxis

```
smsap history list
-profile {-name profile_name [profile_name1, profile_name2] | -all
-repository -login [-password repo_password] -username repo_username
-host repo_host
-dbname repo_dbname
-port repo_port}
-operation {-operations operation_name [operation_name1, operation_name2]
| -all}
[-delimiter character] [-quiet | -verbose]
```

### Parámetros

- **-profile *profile***

Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-repository**

Las opciones que siguen -repository especifican los detalles de la base de datos que almacena el perfil.

- **-dbname *repo\_dbname***

Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

Inicia los detalles de inicio de sesión en el repositorio.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port *repo\_port***

Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-operation** {-operations *operation\_name* [*operation\_name1*, *operation\_name2*] | -all}

Especifica la operación SnapManager para la que se configura el historial.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Comando de ejemplo

```
smsap history list -profile -name PROFILE1 -operation -operations backup  
-verbose
```

---

## El comando smsap history operation-show

Este comando le permite ver el historial de una operación de SnapManager específica asociada con un perfil.

### Sintaxis

```
smsap history operation-show  
-profile profile {-label label | -id id} [-quiet | -verbose]
```

### Parámetros

- **-profile *profile***

Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-label *label* | -id *id***

Especifica el ID o la etiqueta de la operación de SnapManager para la que desea ver el historial.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Comando de ejemplo

```
smsap history operation-show -profile PROFILE1 -label backup1 -verbose
```

---

## El comando `smsap history purge`

Este comando le permite eliminar el historial de operaciones de SnapManager.

### Sintaxis

```
smsap history purge
-profile {-name profile_name [profile_name1, profile_name2] | -all
-repository -login [-password repo_password] -username repo_username
-host repo_host
-dbname repo_dbname
-port repo_port}
-operation {-operations operation_name [operation_name1, operation_name2]
| -all}
[-quiet | -verbose]
```

### Parámetros

- **-profile *profile***

Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-repository**

Las opciones que siguen `-repository` especifican los detalles de la base de datos que almacena el perfil.

- **-dbname *repo\_dbname***

Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

Inicia los detalles de inicio de sesión en el repositorio.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port *repo\_port***

Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-operation {-operations *operation\_name* [*operation\_name1*, *operation\_name2*] | -all**

Especifica la operación SnapManager para la que se configura el historial.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Comando de ejemplo

```
smsap history purge -profile -name PROFILE1 -operation -operations backup  
-verbose
```

---

## Comando smsap history remove

Este comando permite quitar el historial de operaciones de SnapManager asociadas con un único perfil, varios perfiles o todos los perfiles bajo un repositorio.

### Sintaxis

```
smsap history remove
-profile {-name profile_name [profile_name1, profile_name2] | -all
-repository -login [-password repo_password] -username repo_username
-host repo_host
-dbname repo_dbname
-port repo_port}
-operation {-operations operation_name [operation_name1, operation_name2] |
-all}
[-quiet | -verbose]
```

## Parámetros

- **-profile profile**

Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-repository**

Las opciones que siguen -repository especifican los detalles de la base de datos que almacena el perfil.

- **-dbname repo\_dbname**

Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

- **-host repo\_host**

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

Inicia los detalles de inicio de sesión en el repositorio.

- **-username repo\_username**

Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port repo\_port**

Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-operation {-operations operation\_name [operation\_name1, operation\_name2] | -all**

Especifica la operación SnapManager para la que se configura el historial.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y

advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Comando de ejemplo

```
smsap history purge -profile -name PROFILE1 -operation -operations backup  
-verbose
```

---

## El comando smsap history set

Puede ejecutar el `history set` comando para configurar las operaciones para las que desea ver el historial.

### Sintaxis

```
smsap history set  
-profile {-name profile_name [profile_name1, profile_name2] | -all  
-repository -login [password repo_password] -username repo_username  
-host repo_host  
-dbname repo_dbname  
-port repo_port}  
-operation {-operations operation_name [operation_name1, operation_name2]  
| -all}  
-retain  
{-count retain_count | -daily daily_count | -monthly monthly_count |  
-weekly weekly_count}  
[-quiet | -verbose]
```

### Parámetros

- **-profile *profile***

Especifica el nombre del perfil. El nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-repository**

Especifica los detalles de la base de datos que almacena el perfil.

- **-dbname *repo\_dbname***



Especifica el nombre de la base de datos que almacena el perfil. Es posible usar el nombre global o el identificador del sistema.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del host donde reside la base de datos del repositorio.

- **-login**

Especifica los detalles de inicio de sesión del repositorio.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-port *repo\_port***

Especifica el número de puerto del Protocolo de control de transmisión (TCP) que se utiliza para acceder a la base de datos del repositorio.

- **-operation {-operations *operation\_name* [*operation\_name1*, *operation\_name2*] | -all**

Especifica las operaciones de SnapManager para las que se desea configurar el historial.

- **-retain {-count *retain\_count* | -daily *daily\_count* | -monthly *monthly\_count* | -weekly *weekly\_count*}**

Especifica la clase de retención de las operaciones de creación de backup, verificación de backup, restauración y recuperación, y creación y división de clones. La clase de retención se establece en función del número de recuento de operaciones, el número de días, semanas o meses.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Comando de ejemplo

El siguiente ejemplo muestra información sobre la operación de backup:

```
smsap history set -profile -name PROFILE1 -operation -operations backup
-retain -daily 6
-verbose
```

## El comando `smsap history show`

Este comando le permite ver información detallada del historial de un perfil en concreto.

### Sintaxis

```
smsap history show
-profile profile
```

### Parámetros

- **`-profile profile`**

Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **`-quiet`**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **`-verbose`**

Muestra mensajes de error, advertencia e informativos en la consola.

---

### Comando de ejemplo

```
smsap history show -profile -name PROFILE1
-verbose
```

## El comando `smsap help`

Puede ejecutar el `help` Comando para mostrar información acerca de los comandos de la SnapManager y sus opciones. Si no proporciona un nombre de comando, se muestra una lista de comandos válidos. Si proporciona un nombre de comando, muestra la sintaxis de ese comando.

### Sintaxis

```
smsap help  
[backup|cmdfile|clone|credential|help|operation|profile|protection-policy  
|repository|system|version|plugin|diag|history|schedule|notification|storage|get]  
[-quiet | -verbose]]
```

## Parámetros

A continuación se muestran algunos nombres de comandos que puede utilizar con este comando:

- backup
- clone
- cmdfile
- credential
- diag
- get
- notification
- help
- history
- operation
- plugin
- profile
- protection policy
- repository
- schedule
- storage
- system
- version

## El comando `remove-summary-notification` de `smsap`

Este comando deshabilita la notificación de resumen de varios perfiles en una base de datos de repositorio.

## Sintaxis

```
smsap notification remove-summary-notification
-repository
-dbname repo_service_name
-port repo_port
-host repo_host
-login -username repo_username
[-quiet | -verbose]
```

## Parámetros

- **-repository**

Las opciones siguientes `-repository` especifique los detalles de la base de datos para el repositorio.

- **-port *repo\_port***

Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-dbname *repo\_service\_name***

Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login *repo\_username***

Especifica el nombre de inicio de sesión necesario para acceder a la base de datos que almacena el repositorio.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

En el siguiente ejemplo se deshabilita la notificación de resumen de varios perfiles en una base de datos de repositorio.

```
smsap notification remove-summary-notification -repository -port 1521
-dbname repo2 -host 10.72.197.133 -login -username oba5
```

## El comando `smsap notification update-summary-notification`

Puede ejecutar el comando `notification update-summary-notification` para habilitar la notificación de resumen para una base de datos de repositorio.

### Sintaxis

```
smsap notification update-summary-notification
-repository
-port repo_port
-dbname repo_service_name
-host repo_host
-login -username repo_username
-email email-address1,email-address2
-subject subject-pattern
-frequency
[-daily -time daily_time |
-hourly -time hourly_time |
-monthly -time monthly_time -date [1|2|3|...|31] |
-weekly -time weekly_time -day [1|2|3|4|5|6|7]]
-profiles profile1,profile2 -notification-host notification-host
[-quiet | -verbose]
```

### Parámetros

- **-repository**

Especifica los detalles de la base de datos del repositorio.

- **-port *repo\_port***

Especifica el número de puerto TCP utilizado para acceder a la base de datos del repositorio.

- **-dbname *repo\_service\_name***

Especifica el nombre de la base de datos del repositorio. Es posible usar el nombre global o el identificador del sistema.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del host en el que reside la base de datos del repositorio.

- **-login**

Especifica los detalles de inicio de sesión del repositorio. Esto es opcional. Si no se especifica, SnapManager toma de forma predeterminada el modo de conexión de autenticación del sistema operativo.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-email** *email-address1,e-mail-address2*

Especifica las direcciones de correo electrónico de los destinatarios.

- **-subject** *subject-pattern*

Especifica el patrón del asunto del correo electrónico.

- **-frequency** { **-daily** --time *daily\_time* | **-hourly** --time *hourly\_time* | **-monthly** --time *monthly\_time* -date {1|2|3...|31 } | **-weekly** --time *weekly\_time* -day {1|2|3|4|5|6|7 } }

Especifica el tipo de programación y la hora de la programación en el momento en que desea recibir la notificación por correo electrónico.

- **-profiles** *profile1, profile2*

Especifica los nombres de perfil que requieren notificación por correo electrónico.

- **-notification-host** *notification-host*

Especifica el host del servidor SnapManager desde el cual se envía el correo electrónico de notificación de resumen a los destinatarios. Puede proporcionar un nombre de host o una dirección IP para el host de notificación. También es posible actualizar la dirección IP del host o el nombre de host.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Ejemplo

En el siguiente ejemplo se habilita la notificación de resumen para una base de datos de repositorio:

```
smsap notification update-summary-notification -repository -port 1521
-dbname repo2 -host 10.72.197.133 -login -username oba5 -email
admin@org.com -subject success -frequency -daily -time 19:30:45 -profiles
sales1
```

## El comando `smsap notification Set`

Puede utilizar el `notification set` para configurar el servidor de correo.

### Sintaxis

```
smsap notification set
-sender-email email_address
-mailhost mailhost
-mailport mailport
[-authentication
-username username
-password password]
-repository
-dbname repo_service_name
-port repo_port]
-host repo_host
-login -username repo_username
[-quiet | -verbose]
```

### Parámetros

- **-sender-email *email\_address***

Especifica la dirección de correo electrónico del remitente desde la cual se envían las alertas por correo electrónico. En SnapManager 3.2 para SAP, puede incluir un guión (-) al especificar el nombre de dominio de la dirección de correo electrónico. Por ejemplo, puede especificar la dirección de correo electrónico del remitente como `-sender-email07lbfmdatacenter@continental-corporation.com`.

- **-mailhost *mailhost***

Especifica el nombre o la dirección IP del servidor host que gestiona las notificaciones por correo electrónico.

- **-mailport *mailport***

Especifica el número de puerto del servidor de correo.

- **-authentication -username *username* -password *password***

Especifica los detalles de autenticación de la dirección de correo electrónico. Debe especificar el nombre de usuario y la contraseña.

- **-repository**

Especifica los detalles de la base de datos del repositorio.

- **-port *repo\_port***

Especifica el número de puerto del Protocolo de control de transmisión (TCP) que se utiliza para acceder a

la base de datos del repositorio.

- **-dbname *repo\_service\_name***

Especifica el nombre de la base de datos del repositorio. Es posible usar el nombre global o el identificador del sistema.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del host donde reside la base de datos del repositorio.

- **-login**

Especifica los detalles de inicio de sesión del repositorio. Esto es opcional. Si no se especifica, SnapManager toma de forma predeterminada el modo de conexión de autenticación del sistema operativo.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Ejemplo

En el siguiente ejemplo, se configura el servidor de correo:

```
smsap notification set -sender-email admin@org.com -mailhost
hostname.org.com -mailport 25 authentication -username davis -password
davis -repository -port 1521 -dbname SMSAPREPO -host hotspur
-login -username grabal21 -verbose
```

---

## El comando dump de operación smsap

Puede ejecutar el `operation` Comando dump para crear un archivo JAR que contenga información de diagnóstico acerca de una operación.

### Sintaxis



```
smsap operation dump
-profile profile_name
[-label label_name | -id guid
[-quiet | -verbose]]
```

## Parámetros

- **-profile *profile\_name***

Especifica el perfil para el que desea crear los archivos de volcado. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-label *label\_name***

Crea archivos de volcado para la operación y asigna la etiqueta especificada.

- **-id *guid***

Crea archivos de volcado para la operación con el GUID especificado. SnapManager genera el GUID cuando se inicia la operación.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Ejemplo

En el siguiente ejemplo se crea el archivo de volcado para la copia de seguridad:

```
smsap operation dump -profile SALES1
-id 8abc01ec0e78f3e2010e78f3fdd00001
```

```
Dump file created
Path:/userhomedirectory/.netapp/smsap/3.3/smsap_dump_8abc01ec0e78f3e2010e7
8f3fdd00001.jar
```

## El comando `smsap operation list`

Este comando muestra la información resumida de todas las operaciones registradas en un perfil especificado.

### Sintaxis

```
smsap operation list
-profile profile_name
[-delimiter character]
[-quiet | -verbose]]
```

### Parámetros

- **-profile *profile\_name***

Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-delimiter *character***

(Opcional) cuando se especifica este parámetro, el comando enumera cada fila en una línea independiente y los atributos de esa fila están separados por el carácter especificado.

- **-quiet**

(Opcional) sólo muestra mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

(Opcional) muestra mensajes de error, advertencia e informativos en la consola.

### Comando de ejemplo

En el siguiente ejemplo, se muestra la información de resumen de todas las operaciones registradas con el perfil especificado.

```
smsap operation list -profile myprofile
```

```

Start Date Status Operation ID Type Host
-----
-----
2007-07-16 16:03:57 SUCCESS 8abc01c813d0a1530113d0a15c5f0005 Profile
Create Host3
2007-07-16 16:04:55 FAILED 8abc01c813d0a2370113d0a241230001 Backup Host3
2007-07-16 16:50:56 SUCCESS 8abc01c813d0cc580113d0cc60ad0001 Profile
Update Host3
2007-07-30 15:44:30 SUCCESS 8abc01c81418a88e011418a8973e0001 Remove Backup
Host3
2007-08-10 14:31:27 SUCCESS 8abc01c814510ba20114510bac320001 Backup Host3
2007-08-10 14:34:43 SUCCESS 8abc01c814510e9f0114510ea98f0001 Mount Host3
2007-08-10 14:51:59 SUCCESS 8abc01c814511e6e0114511e78d40001 Unmount Host3

```

## Comando smsap operation show

Puede ejecutar el comando `operation show` para mostrar la información de resumen de todas las operaciones realizadas en el perfil especificado. La salida muestra el usuario cliente (el usuario del PC cliente) y el usuario efectivo (el usuario de SnapManager que es válido en el host seleccionado).

### Sintaxis

```

smsap operation show
-profile profile_name
[-label label | -id id] [-quiet | -verbose]

```

### Parámetros

- **-profile *profile\_name***

Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-label *label***

Especifica la etiqueta de la operación.

- **-id *id***

Especifica el identificador de la operación.

- **-quiet**

Opcional: Muestra solo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de

error y advertencia.

- **-verbose**

Opcional: Muestra mensajes de error, advertencia e informativos en la consola.

---

## Ejemplo

La siguiente línea de comandos muestra información detallada sobre una operación:

```
smsap operation show -id 8ac861781d0ac992011d0ac999680001 -profile CER
```

#### Operation Attempted

Operation ID: 8ac861781d0ac992011d0ac999680001  
Type:Backup  
For profile: CER  
With Force: No  
Label: 081017180043  
Comments: BRBACKUP

#### Operation Runtime Information

Status: SUCCESS  
Start date: 2008-10-16 18:01:00 IST  
End date: 2008-10-17 18:01:26 IST  
Client user: oracle  
Effective user: oracle  
By schedule: none

#### Host

Host Run upon: lnx225-248.lab.eng.org.com  
Process ID: 29096  
SnapManager version: 3.3

#### Repository

Connection: krishna@smsaprep/10.72.225.155:1521  
Repository version: 62

#### Error messages

The operation did not generate any error messages.

#### Resources in use

##### Snapshots:

f270-225-

57:/vol/f270\_lnx225\_248\_10gr2\_sap\_oracle\_cer:smsap\_cer\_cer1\_f\_c\_2\_8ac86178  
1d0ac992011d0ac999680001\_0

##### Storage components:

/sapbackup/backCER1.log (File)  
/sapbackup/bdzbalta.anf (File)  
/sapreorg/spaceCER1.log (File)  
/mnt/oracle/CER (File System)

...

## El comando smsap password reset

Puede ejecutar el comando de restablecimiento de contraseña para restablecer la contraseña de un perfil.

### Sintaxis

```
smsap password reset
-profile profile [-profile-password profile_password]
[-repository-hostadmin-password repository_hostadmin_password]
[-quiet | -verbose]
```

## Parámetros

- **-profile *profile***

Especifica el nombre del perfil para el que desea restablecer la contraseña.

- **-profile-password *profile\_password***

Especifica la nueva contraseña para el perfil.

- **-repository-hostadmin-password *admin\_password***

Especifica la credencial de usuario autorizado con privilegios raíz para la base de datos del repositorio.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## El comando smsap plugin check

SnapManager le permite instalar y utilizar scripts personalizados para diversas operaciones. SnapManager ofrece plugins de backup, restauración y clonado para automatizar scripts personalizados antes y después de las operaciones de backup, restauración y clonado. Antes de utilizar el plugin de backup, restauración y clonado, puede ejecutar el comando plugin check para comprobar la instalación de los scripts de los plugins. Los scripts personalizados se almacenan en tres directorios: Política (para scripts que siempre deben ejecutarse antes de que se realice el backup, la restauración o la operación de clonado), el previo (para scripts de procesamiento previo) y el posterior (para scripts de procesamiento posterior).

## Sintaxis

```
smsap plugin check
-osaccount os_db_user_name
```

## Parámetro

- **-osaccount**

Especifica el nombre de usuario de la base de datos del sistema operativo (SO). Si no se introduce la opción `-osaccount`, SnapManager comprueba los scripts del plugin como usuario raíz en lugar de como usuario específico.

## Ejemplo

El ejemplo siguiente muestra que el comando `plugin check` encontró el script personalizado de la directiva 1 almacenado en el directorio de directivas como ejecutable. El ejemplo también muestra que los otros dos scripts personalizados almacenados en el directorio previo no devuelven mensajes de error (mostrados con un estado de 0); sin embargo, el cuarto script personalizado (`post-plugin1`), que se encuentra en el directorio `post`, contiene errores (mostrados con un estado de 3).

```
smsap plugin check
Checking plugin directory structure ...
<installdir>/plugins/clone/policy
OK: 'policy1' is executable
<installdir>/plugins/clone/pre
OK: 'pre-plugin1' is executable and returned status 0
OK: 'pre-plugin2' is executable and returned status 0
<installdir>/plugins/clone/post
ERROR: 'post-plugin1' is executable and returned status 3
<installdir>/plugins/backup/policy
OK: 'policy1' is executable
<installdir>/plugins/backup/pre
OK: 'pre-plugin1' is executable and returned status 0
OK: 'pre-plugin2' is executable and returned status 0
<installdir>/plugins/backup/post
ERROR: 'post-plugin1' is executable and returned status 3
<installdir>/plugins/restore/policy
OK: 'policy1' is executable
<installdir>/plugins/restore/pre
OK: 'pre-plugin1' is executable and returned status 0
OK: 'pre-plugin2' is executable and returned status 0
<installdir>/plugins/restore/post
ERROR: 'post-plugin1' is executable and returned status 3
Command complete.
```

## El comando `smsap profile create`

Puede ejecutar el `profile create` comando para crear un perfil de una base de datos

en un repositorio. Debe montar la base de datos antes de ejecutar este comando.

### **Sintaxis**



```

smsap profile create
-profile profile [-profile-password profile_password]
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login -username repo_username
-database
-dbname db_dbname
-host db_host
[-sid db_sid]
[-login
[-username db_username -password db_password -port db_port]
[-asminstance -asmusername asminstance_username -asmpassword
asminstance_password]
[-rman {-controlfile | {-login
-username rman_username -password rman_password\}
-tnsname rman_tnsname}}]
[-osaccount osaccount] [-osgroup osgroup]
[-retain
[-hourly [-count n] [-duration m]]
[-daily [-count n] [-duration m]]
[-weekly [-count n] [-duration m]]
[-monthly [-count n] [-duration m]]]
-comment comment
-snapname-pattern pattern
[-protect \[-protection-policy policy]
[-summary-notification]
[-notification
[-success
-email email_address1,email_address2
-subject subject_pattern]
[-failure
-email email_address1,email_address2
-subject subject_pattern]
[-separate-archivelog-backups -retain-archivelog-backups -hours hours |
-days days |
-weeks weeks |
-months months
[-protect [-protection-policy policy_name | -noprotect
[-include-with-online-backups | -no-include-with-online-backups]]
[-dump]
[-quiet | -verbose]

```

## Parámetros

- **-profile *profile***

Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-profile-password *profile\_password***

Especifique la contraseña del perfil.

- **-repository**

Las opciones siguientes `-repository` especifique los detalles de la base de datos que almacena el perfil.

- **-dbname *repo\_service\_name***

Especifica el nombre de la base de datos que almacena el perfil. Utilice el nombre global o el SID.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-sid *db\_sid***

Especifica el identificador del sistema de la base de datos que describe el perfil. De forma predeterminada, SnapManager utiliza el nombre de la base de datos como identificador del sistema. Si el identificador del sistema es diferente del nombre de la base de datos, se debe especificar con el `-sid` opción.

Por ejemplo, si utiliza Real Application Clusters (RAC) de Oracle, debe especificar el identificador del sistema de la instancia de RAC en el nodo de RAC desde el cual se ejecuta SnapManager.

- **-login**

Especifica los detalles de inicio de sesión del repositorio.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-port *repo\_port***

Especifica el número de puerto TCP utilizado para acceder a la base de datos del repositorio.

- **-database**

Especifica los detalles de la base de datos que describe el perfil. Esta es la base de datos que se realizará un backup, se restaurará o se clonará.

- **-dbname *db\_dbname***

Especifica el nombre de la base de datos que describe el perfil. Es posible usar el nombre global o el

identificador del sistema.

- **-host *db\_host db\_host***

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos.

- **-asminstance**

Especifica las credenciales que se utilizan para iniciar sesión en la instancia de Automatic Storage Management (ASM).

- **-asmusername *asminstance\_username***

Especifica el nombre de usuario utilizado para iniciar sesión en la instancia de ASM.

- **-asmpassword *asminstance\_password***

Especifica la contraseña utilizada para iniciar sesión en la instancia de ASM.

- **-login**

Especifica los detalles de inicio de sesión de la base de datos.

- **-username *db\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos que describe el perfil.

- **-password *db\_password***

Especifica la contraseña necesaria para acceder a la base de datos que describe el perfil.

- **-port *db\_port***

Especifica el número de puerto TCP utilizado para acceder a la base de datos que describe el perfil.

- **-osaccount *osaccount***

Especifica el nombre de la cuenta de usuario de la base de datos Oracle. SnapManager utiliza esta cuenta para realizar operaciones de Oracle como el inicio y el apagado. Generalmente, es el usuario propietario del software de Oracle en el host, por ejemplo, `orasid`.

- **-osgroup *osgroup***

Especifica el nombre del grupo de base de datos Oracle asociado con `orasid` cuenta.

- **-retain [-hourly [-count *n*] [-duration *m*]] [-daily [-count *n*] [-duration *m*]] [-weekly [-count *n*] [-duration *m*]] [-monthly [-count *n*] [-duration *m*]]**

Especifica la política de retención para un backup donde se cuenta un número de retención o ambos, junto con una duración de retención para una clase de retención (por hora, día, semana, mes).

Para cada clase de retención, se puede especificar un recuento de retención o una duración de retención. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora, días por día). Por ejemplo, si el usuario especifica solo una duración de retención de 7 para backups diarios, SnapManager no

limitará la cantidad de backups diarios del perfil (ya que el número de retención es 0), pero SnapManager eliminará automáticamente los backups diarios creados hace más de 7 días.

- **-comment *comment***

Especifica el comentario de un perfil que describe el dominio del perfil.

- **-snapname-pattern *pattern***

Especifica el patrón de nomenclatura para las copias Snapshot. También puede incluir texto personalizado, por ejemplo, HOPS para operaciones altamente disponibles, en todos los nombres de copias Snapshot. Puede cambiar el patrón de nomenclatura de las copias Snapshot al crear un perfil o después de crear el perfil. El patrón actualizado se aplica solo a las copias snapshot que aún no se han creado. Las copias Snapshot que existen conservan el patrón Snapname anterior. Puede utilizar varias variables en el texto del patrón.

- **-protect -protection-policy *policy***

Indica si el backup debe protegerse a un almacenamiento secundario.



Si `-protect` se especifica sin `-protection-policy`, entonces el conjunto de datos no tendrá una política de protección. Si `-protect` se especifica y `-protection-policy` no se establece cuando se crea el perfil y, a continuación, se puede establecer más adelante `smsap profile update` o bien configurado por el administrador de almacenamiento mediante la consola de Protection Manager.

- **-summary-notification**

Especifica que la notificación de resumen por correo electrónico está activada para el nuevo perfil.

- **-notification -success-email *e-mail\_address1,e-mail\_address2* -subject *subject\_pattern***

Especifica que la notificación de correo electrónico está habilitada para el nuevo perfil de forma que los destinatarios reciban correos electrónicos cuando la operación de SnapManager se realice correctamente. Debe introducir una única dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas por correo electrónico y un patrón de asunto del nuevo perfil.

También se puede incluir texto de asunto personalizado para el nuevo perfil. Puede cambiar el texto del asunto cuando cree un perfil o después de que se haya creado el perfil. El asunto actualizado sólo se aplica a los correos electrónicos que no se envían. Puede usar varias variables para el asunto del correo electrónico.

- **-notification -failure -email *e-mail\_address1,e-mail\_address2* -subject *subject\_pattern***

Especifica que la habilitación de la notificación por correo electrónico está habilitada para el nuevo perfil, de modo que los destinatarios reciban los correos electrónicos cuando falle la operación de SnapManager. Debe introducir una única dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas por correo electrónico y un patrón de asunto del nuevo perfil.

También se puede incluir texto de asunto personalizado para el nuevo perfil. Puede cambiar el texto del asunto cuando cree un perfil o después de que se haya creado el perfil. El asunto actualizado sólo se aplica a los correos electrónicos que no se envían. Puede usar varias variables para el asunto del correo

electrónico.

- **-separate-archivelog-backups**

Especifica que el backup de registros de archivos está separado del backup del archivo de datos. Este es un parámetro opcional que puede proporcionar al crear el perfil. Después de separar el backup con esta opción, es posible tomar el backup solo de los archivos de datos o el backup de solo los registros de archivos.

- **-retain-archivelog-backups -hours *hours* | -days *days* | -weeks *weeks* | -months *months***

Especifica que los backups de los registros de archivos se retendrán según la duración de la retención del registro de archivos (hora, día, semana, mensual).

- **protect [-protection-policy *policy\_name* | -noprotect**

Especifica la protección de los archivos de registro de archivos en función de la política de protección del registro de archivos.

La opción -noProtect especifica no proteger los archivos de registro de archivos.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

- **-include-with-online-backups**

Especifica que el backup de registros de archivos se incluye junto con el backup de la base de datos en línea.

- **-no-include-with-online-backups**

Especifica que no se incluyen los backups de registros de archivos junto con el backup de la base de datos en línea.

- **-dump**

Especifica que los archivos de volcado se recopilan después de la operación de creación de perfiles correcta.

---

## Ejemplo

El siguiente ejemplo muestra la creación de un perfil con una política de retención de horas y notificaciones por correo electrónico:

```
smsap profile create -profile test_rbac -profile-password netapp
-repository -dbname SMSAPREP -host hostname.org.com -port 1521 -login
-username smsaprep -database -dbname RACB -host saal -sid racb1 -login
-username sys -password netapp -port 1521 -rman -controlfile -retain
-hourly -count 30 -verbose
Operation Id [8abc01ec0e78ebda010e78ebe6a40005] succeeded.
```

## El comando `smsap profile delete`

Puede ejecutar el `profile delete` comando para eliminar un perfil de la base de datos.

### Sintaxis

```
smsap profile delete
-profile profile
[-quiet | -verbose]
```

### Parámetros

- **-profile *profile***

Especifica el perfil que se va a eliminar.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

### Ejemplo

En el siguiente ejemplo se elimina el perfil:

```
smsap profile delete -profile SALES1
Operation Id [Ncaf00af0242b3e8dba5c68a57a5ae932] succeeded.
```

## El comando `smsap profile destroy`

Este comando elimina la división de clones (base de datos) junto con el perfil que genera SnapManager durante el proceso de división de clones.

### Sintaxis

```
smsap profile destroy
-profile profile
[-host hostname]
[-quiet | -verbose]
```

### Parámetros

- **-profile *profile***

Especifica el perfil que genera SnapManager después de un proceso de división de clones correcto.

- **-host *hostname***

Especifica el nombre de host en el que existe el clon dividido.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

### Comando de ejemplo

En el ejemplo siguiente se elimina el perfil denominado SALES1.

```
smsap profile destroy -profile SALES1
```

## El comando `smsap profile dump`

Puede ejecutar el `profile dump` comando para crear el `.jar` archivo que contiene información de diagnóstico acerca de un perfil.

## Sintaxis

```
smsap profile dump
-profile profile_name
[-quiet | -verbose]
```

## Parámetros

- **-profile *profile\_name***

Especifica el perfil para el que desea crear los archivos de volcado. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola. ----

## Ejemplo

En el siguiente ejemplo se crea un volcado para el perfil SALES1:

```
smsap profile dump -profile SALES1
Dump file created
Path:/userhomedirectory/.netapp/smsap/3.3.0/smsap_dump_SALES1_hostname.jar
```

## El comando smsap profile list

Este comando muestra una lista de los perfiles actuales.

## Sintaxis

```
smsap profile list
[-quiet | -verbose]
```

## Parámetros

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.



- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Comando de ejemplo

En el siguiente ejemplo se muestran los perfiles existentes con sus detalles.

```
smsap profile list -verbose
Profile name: FGTER
Repository:
  Database name: SMSAPREPO
  SID: SMSAPREPO
  Host: hotspur
  Port: 1521
  Username: swagrahn
  Password: *****
Profile name: TEST_RBAC
Repository:
  Database name: smsaprep
  SID: smsaprep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smsapsaal
  Password: *****
Profile name: TEST_RBAC_DP_PROTECT
Repository:
  Database name: smsaprep
  SID: smsaprep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smsapsaal
  Password: *****
Profile name: TEST_HOSTCREDEN_OFF
Repository:
  Database name: smsaprep
  SID: smsaprep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smsapsaal
  Password: *****
Profile name: SMK_PRF
Repository:
  Database name: smsaprep
  SID: smsaprep
```

```
Host: elbe.rtp.org.com
Port: 1521
Username: smsapsaal
Password: *****
Profile name: FGLEX
Repository:
  Database name: SMSAPREPO
  SID: SMSAPREPO
  Host: hotspur
  Port: 1521
  Username: swagrahn
  Password: *****
```

## El comando `smsap profile show`

Puede ejecutar el `profile show` comando para mostrar la información de un perfil.

### Sintaxis

```
smsap profile show
-profile profile_name
[-quiet | -verbose]
```

### Parámetros

- **-profile *profile\_name***

Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

### Ejemplo

En el siguiente ejemplo se muestran los detalles del perfil:

```
smsap profile show -profile TEST_RBAC_DP_PROTECT
Profile name: TEST_RBAC_DP_PROTECT
Comment:
Target database:
  Database name: racb
  SID: racb1
  Host: saal
  Port: 1521
  Username: sys
  Password: *****
Repository:
  Database name: smsaprep
  SID: smsaprep
  Host: elbe.rtp.org.com
  Port: 1521
  Username: smsapsaal
  Password: *****
RMAN:
  Use RMAN via control file
Oracle user account: oracle
Oracle user group: dba
Snapshot Naming:
  Pattern: smsap_{profile}_{db-sid}_{scope}_{mode}_{smid}
  Example:
smsap_test_rbac_dp_protect_racb1_f_h_1_8abc01e915a55ac50115a55acc8d0001_0
Protection:
  Dataset: smsap_saal_racb
  Protection policy: Back up
  Conformance status: CONFORMANT
Local backups to retain:
  Hourly: 4 copies
  Daily: 7 day(s)
  Weekly: 4 week(s)
  Monthly: 12 month(s)
```

## El comando smsap profile Sync

Este comando carga las asignaciones de perfil a repositorio para ese repositorio en un archivo del directorio inicial en el host local.

### Sintaxis

```
smsap profile sync
-repository
-dbname repo_service_name
-host repo_host
-port repo_port
-login
-username repo_username          [-quiet | -verbose]
```

## Parámetros

- **-repository**

Las opciones que siguen a -repository especifican los detalles de la base de datos para el repositorio.

- **-dbname *repo\_service\_name***

Especifica la base de datos del repositorio para el perfil que se va a sincronizar.

- **-host**

Especifica el host de la base de datos.

- **-port**

Especifica el puerto para el host.

- **-login**

Especifica el proceso de inicio de sesión para el usuario host.

- **-username**

Especifica el nombre de usuario para el host.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Comando de ejemplo

En el siguiente ejemplo se muestra el resultado del comando para sincronizar las asignaciones de perfil a repositorio de la base de datos.

```
smsap profile sync -repository -dbname smrepo -host Host2 -port 1521
-login -username user2
SMSAP-12345 [INFO ]: Loading profile mappings for repository
"user2@Host2:smrepo" into cache for OS User "admin".
Operation Id [Nff8080810da9018f010da901a0170001] succeeded.
```

## Comando smsap profile update

Puede ejecutar el `profile update` comando para actualizar la información de un perfil existente.

### Sintaxis

```

smsap profile update
-profile profile
[-new-profile new_profile_name]
[-profile-password profile_password]
[-database
-dbname db_dbname
-host db_host
[-sid db_sid]
[-login
[-username db_username -password db_password -port db_port]
[-asminstance -asmusername asminstance_username -asmpassword
asminstance_password]
[{-rman {-controlfile | {{-login
-username rman_username
-password rman_password }
[-tnsname tnsname}}}] |
-remove-rman]
-osaccount osaccount
-osgroup osgroup
[-retain
[-hourly [-count n] [-duration m]]
[-daily [-count n] [-duration m]
[-weekly [-count n] [-duration m]
[-monthly [-count n] [-duration m]]]
-comment comment
-snapname-pattern pattern
[-protect [-protection-policy policy_name] | [-noprotect]
[-summary-notification]
[-notification
[-success
-email email_address1,email_address2
-subject subject_pattern]
[-failure
-email email_address1,email_address2
-subject subject_pattern
[-separate-archivelog-backups
-retain-archivelog-backups
-hours hours |
-days days |
-weeks weeks |
-months months
[-protect [-protection-policy policy_name] | [-noprotect]
[-include-with-online-backups | -no-include-with-online-backups]]
[-dump]
[-quiet | -verbose]]

```

## Parámetros

Si se ha establecido una política de protección en el perfil, no podrá cambiar la política con SnapManager. Debe cambiar la política con la consola de Protection Manager.

- **-profile *profile***

Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-profile-password *profile\_password***

Especifica la contraseña del perfil.

- **-new-profile *new\_profile\_name***

Especifica el nuevo nombre que puede proporcionar para un perfil.

- **-database**

Especifica los detalles de la base de datos que describe el perfil. Esta es la base de datos de la que se realizará un backup, se restaurará, etc.

- **-dbname *db\_dbname***

Especifica el nombre de la base de datos que describe el perfil. Es posible usar el nombre global o el identificador del sistema.

- **-host *db\_host***

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos.

- **-sid *db\_sid***

Especifica el identificador del sistema de la base de datos que describe el perfil. De forma predeterminada, SnapManager utiliza el nombre de la base de datos como identificador del sistema. Si el identificador del sistema es diferente del nombre de la base de datos, debe especificarlo mediante el `-sid` opción.

Por ejemplo, si utiliza Real Application Clusters (RAC) de Oracle, debe especificar el identificador de sistema SID de la instancia de RAC en el nodo RAC desde el cual se ejecuta SnapManager.

- **-login**

Especifica los detalles de inicio de sesión del repositorio.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos del repositorio.

- **-port *repo\_port***

Especifica el número de puerto TCP necesario para acceder a la base de datos del repositorio.

- **-database**

Especifica los detalles de la base de datos que describe el perfil. Esta es la base de datos que se realizará un backup, se restaurará o se clonará.

- **-dbname *db\_dbname***

Especifica el nombre de la base de datos que describe el perfil. Es posible usar el nombre global o el identificador del sistema.

- **-host *db\_host***

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos.

- **-login**

Especifica los detalles de inicio de sesión de la base de datos.

- **-username *db\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos que describe el perfil.

- **-password *db\_password***

Especifica la contraseña necesaria para acceder a la base de datos que describe el perfil.

- **-port *db\_port***

Especifica el número de puerto TCP necesario para acceder a la base de datos que describe el perfil.

- **-asminstance**

Especifica las credenciales que se utilizan para iniciar sesión en la instancia de Automatic Storage Management (ASM).

- **-asmusername *asminstance\_username***

Especifica el nombre de usuario utilizado para iniciar sesión en la instancia de ASM.

- **-asmpassword *asminstance\_password***

Especifica la contraseña utilizada para iniciar sesión en la instancia de ASM.

- **-osaccount *osaccount***

Especifica el nombre de la cuenta de usuario de la base de datos Oracle. SnapManager utiliza esta cuenta para realizar operaciones de Oracle como el inicio y el apagado. Normalmente es el usuario propietario del software Oracle en el host, por ejemplo, orasid.

- **-osgroup *osgroup***

Especifica el nombre del grupo de base de datos Oracle asociado a la cuenta orasid.

- **-retain [-hourly [-count *n*] [-duration *m*]] [-daily [-count *n*] [-duration *m*]] [-weekly [-count *n*] [-duration *m*]] [-monthly [-count *n*] [-duration *m*]]**



Especifica la clase de retención (por hora, por día, por semana o por mes) para una copia de seguridad.

Para cada clase de retención, se puede especificar un recuento de retención, una duración de retención o ambas. La duración se encuentra en unidades de la clase (por ejemplo, horas por hora o días por día). Por ejemplo, si el usuario especifica solo una duración de retención de 7 para backups diarios, SnapManager no limitará la cantidad de backups diarios del perfil (ya que el número de retención es 0), pero SnapManager eliminará automáticamente los backups diarios creados hace más de 7 días.

- **-comment *comment***

Especifica el comentario de un perfil.

- **-snapname-pattern *pattern***

Especifica el patrón de nomenclatura para las copias Snapshot. También puede incluir texto personalizado, por ejemplo, HOPS para operaciones altamente disponibles, en todos los nombres de copias Snapshot. Puede cambiar el patrón de nomenclatura de las copias Snapshot al crear un perfil o después de crear el perfil. El patrón actualizado se aplica solo a las copias snapshot que aún no se han producido. Las copias Snapshot que existen conservan el patrón Snapname anterior. Puede utilizar varias variables en el texto del patrón.

- **-protect [-protection-policy *policy\_name*] | [-noprotect]**

Indica si el backup debe protegerse a un almacenamiento secundario o no.



Si `-protect` se especifica sin `-protection-policy`, entonces el conjunto de datos no tendrá una política de protección. Si `-protect` se especifica y `-protection-policy` no se establece cuando se crea el perfil y, a continuación, se puede establecer más adelante `smsap profile update` o bien, el administrador de almacenamiento lo establece mediante la consola de Protection Manager .

La `-noprotect` la opción especifica no proteger el perfil en el almacenamiento secundario.

- **-summary-notification**

Especifica que la notificación de resumen por correo electrónico está activada para el perfil existente.

- **-notification [-success-email *e-mail\_address1,e-mail address2* -subject *subject\_pattern*]**

Habilita la notificación de correo electrónico para el perfil existente de forma que los destinatarios reciban los correos electrónicos cuando la operación SnapManager se realice correctamente. Debe introducir una única dirección de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas por correo electrónico y un patrón de asunto del correo electrónico para el perfil existente.

Puede cambiar el texto del asunto al actualizar el perfil o incluir texto de asunto personalizado. El asunto actualizado sólo se aplica a los correos electrónicos que no se envían. Puede usar varias variables para el asunto del correo electrónico.

- **-notification [-failure -email *e-mail\_address1,e-mail address2* -subject *subject\_pattern*]**

Habilita la notificación de correo electrónico para el perfil existente de modo que los destinatarios reciban los correos electrónicos cuando falle la operación de SnapManager. Debe introducir una única dirección

de correo electrónico o varias direcciones de correo electrónico a las que se enviarán las alertas por correo electrónico y un patrón de asunto del correo electrónico para el perfil existente.

Puede cambiar el texto del asunto al actualizar el perfil o incluir texto de asunto personalizado. El asunto actualizado sólo se aplica a los correos electrónicos que no se envían. Puede usar varias variables para el asunto del correo electrónico.

- **-separate-archivelog-backups**

Separa el backup de registros de archivos del backup de archivo de datos. Este es un parámetro opcional que puede proporcionar al crear el perfil. Después de separar los backups se separan con esta opción, es posible crear un backup de solo los archivos de datos o un backup de solo los registros de archivos.

- **-retain-archivelog-backups -hours *hours* | -days *days* | -weeks *weeks* | -months *months***

Especifica que los backups de los registros de archivos se retendrán según la duración de la retención del registro de archivos (hora, día, semana, mensual).

- **-protect [-protection-policy *policy\_name*] | -noprotect**

Especifica que los archivos de registro de archivos están protegidos en función de la política de protección del registro de archivos.

Especifica que los archivos de registro de archivos no están protegidos mediante el `-noprotect` opción.

- **-include-with-online-backups | -no-include-with-online-backups**

Especifica que el backup de registros de archivos se incluye junto con el backup de la base de datos en línea.

Especifica que no se incluyen los backups de registros de archivos junto con el backup de la base de datos en línea.

- **-dump**

Especifica que los archivos de volcado se recopilan después de la operación de creación de perfiles correcta.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Ejemplo

En el ejemplo siguiente se cambia la información de inicio de sesión de la base de datos descrita por el perfil y se configura la notificación por correo electrónico para este perfil:

```
smsap profile update -profile SALES1 -database -dbname SALESDB
-sid SALESDB -login -username admin2 -password d4jPe7bw -port 1521
-host server1 -profile-notification -success -e-mail Preston.Davis@org.com
-subject success
Operation Id [8abc01ec0e78ec33010e78ec3b410001] succeeded.
```

## El comando smsap profile verify

Puede ejecutar el comando `profile verify` para verificar la configuración del perfil. Debe montar la base de datos antes de ejecutar este comando.

### Sintaxis

```
smsap profile verify
-profile profile_name
[-quiet | -verbose]
```

### Parámetros

- **-profile**

Especifica el perfil que se va a verificar. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

### Ejemplo

En el siguiente ejemplo se verifica el perfil:

```
smsap profile verify -profile profileA -verbose
[ INFO] SMSAP-13505: SnapDrive environment verification passed.
[ INFO] SMSAP-13507: JDBC verification for "OS authenticated:
CER/hostA.rtp.com" passed.
[ INFO] SMSAP-13506: SQLPlus verification for database SID "CER" passed.
Environment: [ORACLE_HOME=/u02/app/oracle/product/11.2.0.2]
[ INFO] SMSAP-07431: Saving starting state of the database: CER(OPEN).
[ INFO] SMSAP-07431: Saving starting state of the database: CER(OPEN).
[ INFO] SD-00016: Discovering storage resources for
```

```
/vol/hostA_sap_datavol_CER.  
[ INFO] SD-00017: Finished storage discovery for /vol/  
hostA_sap_datavol_CER.  
[ INFO] SD-00016: Discovering storage resources for  
/vol/hostA_sap_datavol_CER.  
[ INFO] SD-00017: Finished storage discovery for /vol/  
hostA_sap_datavol_CER.  
[ INFO] SD-00016: Discovering storage resources for  
/vol/hostA_sap_cntrlvol_CER.  
[ INFO] SD-00017: Finished storage discovery for  
/vol/hostA_sap_cntrlvol_CER.  
[ INFO] SD-00016: Discovering storage resources for  
/vol/hostA_sap_redovol_CER.  
[ INFO] SD-00017: Finished storage discovery for  
/vol/hostA_sap_redovol_CER.  
[ INFO] SD-00016: Discovering storage resources for  
/vol/hostA_sap_archivevol_CER.  
[ INFO] SD-00017: Finished storage discovery for  
/vol/hostA_sap_archivevol_CER.  
[ INFO] SD-00040: Beginning to discover filesystem(s) upon host volume  
group hostA-3_SdDg.  
[ INFO] SD-00041: Finished discovering filesystem(s) upon host volume  
group hostA-3_SdDg.  
[ INFO] SD-00040: Beginning to discover filesystem(s) upon host volume  
group hostA-2_SdDg.  
[ INFO] SD-00041: Finished discovering filesystem(s) upon host volume  
group hostA-2_SdDg.  
[ INFO] SD-00040: Beginning to discover filesystem(s) upon host volume  
group hostA_s_SdDg.  
[ INFO] SD-00041: Finished discovering filesystem(s) upon host volume  
group hostA_s_SdDg.  
[ INFO] SD-00040: Beginning to discover filesystem(s) upon host volume  
group hostA-1_SdDg.  
[ INFO] SD-00041: Finished discovering filesystem(s) upon host volume  
group hostA-1_SdDg.  
[ WARN] SMSAP-05071: Database profile profileA is not eligible for fast  
restore: Restore Plan:  
Preview:
```

The following components will be restored completely via: host side  
file copy restore

```
/vol/hostA_sap_datavol_CER/CER/sapdata1/oradata/CER/sysaux01.dbf  
/vol/hostA_sap_datavol_CER/CER/sapdata1/oradata/CER/system01.dbf  
/vol/hostA_sap_datavol_CER/CER/sapdata1/oradata/CER/undotbs01.dbf  
/vol/hostA_sap_datavol_CER/CER/sapdata1/oradata/CER/users01.dbf
```

## Analysis:

The following reasons prevent certain components from being restored completely via: storage side file system restore

- \* Files in file system /vol/hostA\_sap\_datavol\_CER not part of the restore scope will be reverted.

- \* File systems in volume group hostA-1\_SdDg not part of the restore scope will be reverted: [/vol/hostA\_sap\_datavol\_CER]

Components not in restore scope:

```
/vol/hostA_sap_datavol_CER/CER/sapdata1/cfgtoollogs/catbundle/catbundle_PS  
U_CER_APPLY_2011Dec15_00_52_21.log
```

```
/vol/hostA_sap_datavol_CER/CER/sapdata1/cfgtoollogs/catbundle/catbundle_PS  
U_CER_GENERATE_2011Dec15_00_52_16.log
```

Components to restore:

```
/vol/hostA_sap_datavol_CER/CER/sapdata1/oradata/CER/sysaux01.dbf  
/vol/hostA_sap_datavol_CER/CER/sapdata1/oradata/CER/system01.dbf  
/vol/hostA_sap_datavol_CER/CER/sapdata1/oradata/CER/undotbs01.dbf  
/vol/hostA_sap_datavol_CER/CER/sapdata1/oradata/CER/users01.dbf
```

\* Reasons denoted with an asterisk (\*) are overridable.

```
[ INFO] SMSAP-07433: Returning the database to its initial state: CER  
(OPEN).
```

```
[ INFO] SMSAP-13048: Profile Verify Operation Status: SUCCESS
```

```
[ INFO] SMSAP-13049: Elapsed Time: 0:01:17.857
```

```
Operation Id [Nab0240e8200dae6f17ecf21060bc6de8] succeeded.
```

## El comando smsap protection-policy

Puede ejecutar el `protection-policy` comando para enumerar las directivas de protección que se pueden aplicar a un perfil. La directiva de protección se puede aplicar cuando se crea un perfil nuevo o se actualiza un perfil existente. También puede establecer la política de protección del perfil mediante la consola de Protection Manager.

### Sintaxis

```
smsap protection-policy list
```



Protection Manager y SnapDrive se deben instalar en el servidor para que pueda utilizar este comando.

## Parámetros

- **list**

Muestra la lista de directivas de protección que se pueden establecer en un perfil.

## Ejemplo

En el siguiente ejemplo, se enumeran las políticas de protección que se pueden configurar en un perfil:

```
smsap protection-policy list
```

```
Back up  
Back up, then mirror  
Chain of two mirrors  
DR Back up  
DR Back up, then mirror  
DR Mirror  
DR Mirror and back up  
DR Mirror and mirror  
DR Mirror, then back up  
DR Mirror, then mirror  
Local backups only  
Mirror  
Mirror and back up  
Mirror to two destinations  
Mirror, then back up  
No protection  
Partial-volume Mirror  
Remote backups only
```

## El comando smsap repository create

### Sintaxis

Este comando crea un repositorio en el que se almacenan perfiles de base de datos y credenciales asociadas. Este comando también comprueba si el tamaño de los bloques es adecuado.

```
smsap repository create
-repository
-port repo_port
-dbname repo_service_name
-host repo_host
-login -username repo_username
[-force] [-noprompt]
[-quiet | -verbose]
```

## Parámetros

- **-repository**

Las opciones siguientes *-repository* especifique los detalles de la base de datos para el repositorio

- **-port *repo\_port***

Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-dbname *repo\_service\_name***

Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

Inicia los detalles de inicio de sesión en el repositorio.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-force**

Se intenta forzar la creación del repositorio. Con esta opción, SnapManager se solicita que se realice un backup del repositorio antes de crear el repositorio.

- **-noprompt**

No muestra el símbolo del sistema de realizar un backup del repositorio antes de crearlo si utiliza la *-force* opción. Con el *-noprompt* la opción garantiza que el mensaje no aparezca, lo que facilita la creación de repositorios con un script.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y

advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Ejemplo de comando

El siguiente ejemplo crea un repositorio en la base de datos SMSAPREPO en el hotspur del host.

```
smsap repository create -repository -port 1521 -dbname SMSAPREPO -host
hotspur -login -username grabal21 -verbose
SMSAP-09202 [INFO ]: Creating new schema as grabal21 on
jdbc:oracle:thin:@//hotspur:1521/SMSAPREPO.
SMSAP-09205 [INFO ]: Schema generation complete.
SMSAP-09209 [INFO ]: Performing repository version INSERT.
SMSAP-09210 [INFO ]: Repository created with version: 30
SMSAP-13037 [INFO ]: Successfully completed operation: Repository Create
SMSAP-13049 [INFO ]: Elapsed Time: 0:00:08.844
```

## El comando smsap repository delete

Este comando elimina un repositorio utilizado para almacenar perfiles de base de datos y credenciales asociadas. Sólo puede eliminar un repositorio si no hay perfiles en el repositorio.

### Sintaxis

```
smsap repository delete
-repository
-port repo_port
-database repo_service_name
-host repo_host
-login -username repo_username
[-force] [-noprompt]
[-quiet | -verbose]
```

### Parámetros

- **-repository**

Las opciones siguientes `-repository` especifique los detalles de la base de datos para el repositorio.

- **-port *repo\_port***

Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el



repositorio.

- **-dbname *repo\_service\_name***

Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

Inicia los detalles de inicio de sesión en el repositorio.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-force**

Se intenta forzar la eliminación del repositorio, incluso si hay operaciones incompletas. SnapManager emite un aviso si existen operaciones incompletas, en las que se pregunta si está seguro de que se desea eliminar el repositorio.

- **-noprompt**

No se le solicita antes de eliminar el repositorio. Con el `-noprompt` la opción garantiza que el mensaje no aparezca, lo que facilita la eliminación de repositorios mediante una secuencia de comandos.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Ejemplo de comando

En el ejemplo siguiente se elimina el repositorio de la base de datos SALESDB.

```
smsap repository delete -repository -dbname SALESDB  
-host server1 -login -username admin -port 1527 -force -verbose
```

## El comando `smsap repository`

Este comando permite revertir o revertir una versión superior de SnapManager a la versión original de la que se actualizó.

## Sintaxis

```
smsap repository rollback
-repository
-dbname repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
-rollbackhost host_with_target_database
[-force]
[-quiet | -verbose]
```

## Parámetros

- **-repository**

Las opciones que siguen a **-repository** especifican los detalles de la base de datos para el repositorio.

- **-dbname *repo\_service\_name***

Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

Inicia los detalles de inicio de sesión en el repositorio.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-rollbackhost *host\_with\_target\_database***

Especifica el nombre del host que se va a revertir de una versión superior de SnapManager a la versión anterior original.

- **-port *repo\_port***

Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-force**

Intenta forzar la actualización del repositorio. SnapManager le solicita que realice una copia de seguridad del repositorio actual antes de la actualización.

- **-noprompt**

No muestra el mensaje antes de actualizar la base de datos del repositorio. El uso de la opción `-noprompt` garantiza que no aparezca la petición de datos, lo que facilita la actualización de repositorios mediante una secuencia de comandos.

- **`-quiet`**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **`-verbose`**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Comando de ejemplo

En el ejemplo siguiente se actualiza el repositorio de la base de datos SALESDB.

```
smsap repository rollback -repository -dbname SALESDB
-host server1 -login -username admin -port 1521 -rollbackhost hostA
```

---

## El comando `msap repository rollingupgrade`

Este comando realiza la actualización en un solo host o de varios hosts y las bases de datos de destino asociadas desde una versión inferior de SnapManager a una versión posterior. El host actualizado solo se gestiona con la versión superior de SnapManager.

### Sintaxis

```
smsap repository rollingupgrade
-repository
-database repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
-upgradehost host_with_target_database
[-force [-noprompt]
[-quiet | -verbose]
```

### Parámetros

- **`-repository`**

Las opciones que siguen a `-repository` especifican los detalles de la base de datos para el repositorio.

- **-dbname *repo\_service\_name***

Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

Inicia los detalles de inicio de sesión en el repositorio.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-upgradehost *host\_with\_target\_database***

Especifica el nombre del host que se actualizará de una versión inferior de SnapManager a una versión superior.

- **-port *repo\_port***

Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-force**

Intenta forzar la actualización del repositorio. SnapManager le solicita que realice una copia de seguridad del repositorio actual antes de la actualización.

- **-noprompt**

No muestra el mensaje antes de actualizar la base de datos del repositorio. Con el `-noprompt` la opción garantiza que no aparezca el mensaje, lo que facilita la actualización de repositorios mediante una secuencia de comandos.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

---

## Comando de ejemplo

En el ejemplo siguiente se actualiza el repositorio de la base de datos SALESDB.

```
smsap repository rollinguupgrade -repository -dbname SALESDB
-host server1 -login -username admin -port 1521 -upgradehost hostA
```

## El comando `smsap repository show`

Este comando muestra información sobre el repositorio.

### Sintaxis

```
smsap repository show
-repository
-database repo_service_name
-host repo_host
-port repo_port
-login -username repo_username
[-quiet | -verbose]
```

### Parámetros

- **-repository**

Las opciones siguientes `-repository` especifica los detalles de la base de datos para el repositorio.

- **-dbname *repo\_service\_name***

Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

Inicia los detalles de inicio de sesión en el repositorio.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port *repo\_port***

Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Ejemplo de comando

En el siguiente ejemplo se muestran detalles sobre el repositorio de la base de datos SALESDB.

```
smsap repository show -repository -dbname SALESDB -host server1
-port 1521 -login -username admin
Repository Definition:
User Name: admin
Host Name: server1
Database Name: SALESDB
Database Port: 1521
Version: 28
Hosts that have run operations using this repository: 2
server2
server3
Profiles defined in this repository: 2
GSF5A
GSF3A
Incomplete Operations: 0
```

## El comando smsap repository update

Este comando actualiza el repositorio que almacena perfiles de base de datos y las credenciales asociadas al actualizar SnapManager. Cada vez que instale una nueva versión de SnapManager, debe ejecutar el comando de actualización del repositorio para poder utilizar la nueva versión. Puede utilizar este comando solo si no hay comandos incompletos en el repositorio.

### Sintaxis

```
smsap repository update
-repository
-database repo_service_name
-host repo_host
-login -username repo_username
-port repo_port
[-force] [-noprompt]
[-quiet | -verbose]
```

## Parámetros

- **-repository**

Las opciones siguientes `-repository` especifique los detalles de la base de datos para el repositorio.

- **-dbname *repo\_service\_name***

Especifica el nombre de la base de datos que almacena el repositorio. Utilice el nombre global o el SID.

- **-host *repo\_host***

Especifica el nombre o la dirección IP del equipo host en el que se ejecuta la base de datos del repositorio.

- **-login**

Inicia los detalles de inicio de sesión en el repositorio.

- **-username *repo\_username***

Especifica el nombre de usuario necesario para acceder a la base de datos que almacena el repositorio.

- **-port *repo\_port***

Especifica el número de puerto TCP utilizado para acceder a la base de datos que almacena el repositorio.

- **-force**

Intenta forzar la actualización del repositorio. SnapManager le solicita que realice una copia de seguridad del repositorio actual antes de la actualización.

- **-noprompt**

No muestra el mensaje antes de actualizar la base de datos del repositorio. Con el `-noprompt` la opción garantiza que no aparezca el mensaje, lo que facilita la actualización de repositorios mediante una secuencia de comandos.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Comando de ejemplo

En el ejemplo siguiente se actualiza el repositorio de la base de datos SALESDB.

```
smsap repository update -repository -dbname SALESDB
-host server1 -login -username admin -port 1521
```

## El comando smsap schedule create

Es posible utilizar el comando schedule create para programar la creación de un backup en un momento específico.

### Sintaxis

```
smsap schedule create -profile <em>profile_name</em>
[-full{-auto | -online | -offline}
[-retain <em>-hourly</em>| <em>-daily</em> | <em>-weekly</em> | <em>-
monthly</em> | <em>-unlimited</em> [-verify]] |
-data [[-files <em>files</em> [<em>files</em>] |
-tablespaces <em>tablespaces</em> [<em>tablespaces</em>] {-auto | -online
| -offline}
[-retain <em>-hourly</em> | -daily | <em>-weekly</em> | <em>-monthly</em>
| <em>-unlimited</em>] [-verify]] |
[-archivelogs]}
[-label <em>label</em>]
[-comment <em>comment</em>]
[-protect | -noprotect | -protectnow] [-backup-dest <em>path1</em> [ ,
<em>path2</em>]
[-exclude-dest <em>path1</em> [ , <em>path2</em>]] [-prunelogs {-all |
-until-scn <em>until-scn</em> | -until -date <em>yyyy-MM-
dd:HH:mm:ss</em>] | -before {-months | -days | -weeks | -hours}}
-prune-dest <em>prune_dest1</em>, [<em>prune_dest2</em>]]-schedule-name
<em>schedule_name</em>
[-schedule-comment <em>schedule_comment</em>] -interval {<em>-hourly</em>
| <em>-daily</em> | <em>-weekly</em> | <em>-monthly</em> | <em>-
onetimeonly</em>}
-cronstring <em>cron_string</em>-start-time {<em>start_time < yyyy-MM-dd
HH:mm</em>>}
-runasuser <em>runasuser</em>
[-taskspec <em>taskspec</em>]-force
[-quiet | -verbose]
```

### Parámetros

- **-profile *profile\_name***

Especifica el nombre del perfil relacionado con la base de datos para la que desea programar el backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.



- **-auto opción**

Si la base de datos está en estado montado o sin conexión, SnapManager realiza un backup sin conexión. Si la base de datos está en estado abierto o en línea, SnapManager realiza un backup en línea. Si utiliza la `-force` con la `-offline` Option, SnapManager fuerza un backup sin conexión incluso si la base de datos está en línea actualmente.

- **-online opción**

Especifica un backup de base de datos en línea.

Es posible crear un backup en línea de una base de datos de Real Application Clusters (RAC), siempre que el primario se encuentre en estado abierto o montado y una instancia esté en estado abierto. Puede utilizar el `-force` opción para backups en línea si la instancia local está en estado de apagado o no hay ninguna instancia abierta.

- Si la instancia local está en estado de apagado y al menos una instancia está abierta, puede utilizar la opción `-force` para cambiar la instancia local a montada.
- Si ninguna instancia está en estado abierto, puede utilizar `-force` opción para cambiar la instancia local a abierta.

- **-offline opción**

Especifica un backup sin conexión mientras la base de datos está en estado de apagado. Si la base de datos está en estado abierto o montado, el backup genera errores. Si la `-force` Se utiliza la opción, SnapManager intenta modificar el estado de la base de datos para cerrar la base de datos para realizar un backup sin conexión.

- **-full opción**

Realiza un backup de toda la base de datos. Esto incluye todos los datos, registros archivados y archivos de control. Se realiza una copia de seguridad de los redo logs archivados y de los archivos de control, independientemente del tipo de copia de seguridad que realice. Si desea realizar un backup solo de una parte de la base de datos, use la `-files` opción o. `-tablespaces` opción.

- **-files list**

Realiza un backup solo de los archivos de datos especificados, además de los archivos de registro y control archivados. Separe la lista de nombres de archivo con espacios. Si la base de datos está en estado abierto, SnapManager verifica que los espacios de tablas apropiados se encuentren en modo de backup en línea.

- **-tablespaces tablespaces**

Realiza un backup solo de los espacios de tablas de la base de datos especificados, además de los archivos de registro y control archivados. Separe los nombres de tablespace con espacios. Si la base de datos está en estado abierto, SnapManager verifica que los espacios de tablas apropiados se encuentren en modo de backup en línea.

- **-label name**

Especifica un nombre opcional para este backup. Este nombre debe ser único dentro del perfil. El nombre puede contener letras, números, guiones bajos (`_`) y guiones (`-`). No puede comenzar con un guión.

Si no se especifica una etiqueta, SnapManager crea una etiqueta predeterminada en el formato `scope_type_date`:

- El ámbito es F indicar un backup completo o P para indicar un backup parcial.
- El tipo es C para indicar una copia de seguridad sin conexión (en frío), H para indicar una copia de seguridad en línea (activa) o A para indicar una copia de seguridad automática, por ejemplo, `P_A_20081010060037IST`.
- Fecha es el año, el mes, el día y la hora de la copia de seguridad.

SnapManager se usa un reloj de 24 horas.

Por ejemplo, si realizó un backup completo con la base de datos sin conexión el 16 de enero de 2007, a las 5:45:16 Hora estándar del este, SnapManager crearía la etiqueta `F_C_20070116174516EST`.

#### • **-comment string**

Especifica un comentario opcional para describir esta copia de seguridad. La cadena debe escribirse entre comillas simples (').



Algunos vaciados pelan entre comillas. Si esto es cierto para el shell, debe incluir la comillas con una barra diagonal inversa (\). Por ejemplo, es posible que deba introducir: `\ ' this is a comment\ '`.

#### • **-verify opción**

Verifica que los archivos de la copia de seguridad no están dañados ejecutando la utilidad oracle dbv.



Si especifica el `-verify` opción, la operación de backup no se completa hasta que se complete la operación de verificación.

#### • **-force opción**

Fuerza un cambio de estado si la base de datos no está en el estado correcto. Por ejemplo, SnapManager puede cambiar el estado de la base de datos de en línea a sin conexión, según el tipo de backup especificado y el estado en el que está la base de datos.

Con un backup de base de datos RAC en línea, utilice `-force` si la instancia local está en estado de cierre o no hay ninguna instancia abierta.



La versión de Oracle debe ser 10.2.0.5; de lo contrario, la base de datos se bloqueará si existe alguna instancia en el RAC montada.

- Si la instancia local está en estado de apagado y al menos una instancia está abierta, puede cambiar la instancia local a montada mediante `-force` opción.
- Si no hay ninguna instancia abierta, puede cambiar la instancia local a abierta mediante `-force` opción.

#### • **-protect | -noprotect | -protectnow**

Indica si el backup debe protegerse a un almacenamiento secundario. La `-noprotect` la opción especifica que el backup no debe protegerse en el almacenamiento secundario. Solo se protegen los backups completos. Si se especifica ninguna de las dos opciones, SnapManager protege el backup como

predeterminado si el backup es un backup completo y el perfil especifica una política de protección. La `-protectnow` Esta opción solo se aplica a Data ONTAP operando en 7-Mode. La opción especifica que el backup se proteja inmediatamente en el almacenamiento secundario.

- **`-retain { -hourly | -daily | -weekly | -monthly | -unlimited}`**

Especifica si el backup se debe retener por hora, día, semana, mes o ilimitada. Si `-retain` no se especifica la opción, la clase de retención predeterminada es `-hourly`. Para retener los backups para siempre, utilice la `-unlimited` opción. La `-unlimited` opción hace que el backup no sea apto para su eliminación por parte de la política de retención.

- **`-archivelogs`**

Especifica la creación de un backup de registro de archivos.

- **`-backup-dest path1, [, [path2]]`**

Especifica los destinos de registros de archivos para el backup de registros de archivos.

- **`-exclude-dest path1, [, [path2]]`**

Especifica los destinos de registro de archivos que se excluirán de la copia de seguridad.

- **`-prunelogs {-all | -until-scnuntil-scn | -until-dateyyyy-MM-dd:HH:mm:ss | -before {-months | -days | -weeks | -hours}}`**

Especifica si se eliminarán los archivos de registro de archivos de los destinos de registro de archivos en función de las opciones proporcionadas al crear un backup. La `-all` option elimina todos los archivos de registro de archivos de los destinos de registro de archivos. La `-until-scn` La opción elimina los archivos de registro de archivos hasta que se especifique un número de cambio de sistema (SCN). La `-until-date` la opción elimina los archivos de registro de archivos hasta el periodo de tiempo especificado. La `-before` la opción elimina los archivos de registro de archivos antes del periodo de tiempo especificado (días, meses, semanas, horas).

- **`-schedule-name schedule_name`**

Especifica el nombre que se proporcionará para la programación.

- **`-schedule-comment schedule_comment`**

Especifica un comentario opcional que se va a describir acerca de la programación del backup.

- **`-interval { -hourly | -daily | -weekly | -monthly | -onetimeonly}`**

Especifica el intervalo de tiempo mediante el cual se crean los backups. Se puede programar el backup cada hora, día, semana, mes o solo una vez.

- **`-cronstring cron_string`**

Especifica la programación del backup mediante cronstring. Las expresiones cron se utilizan para configurar instancias de CronTrigger. Las expresiones cron son cadenas que se componen de las siguientes subexpresiones:

- 1 se refiere a segundos.

- 2 se refiere a minutos.
- 3 se refiere a horas.
- 4 se refiere a un día en un mes.
- 5 se refiere al mes.
- 6 se refiere a un día en una semana.
- 7 se refiere al año (opcional).

- **-start-time *yyyy-MM-dd HH:mm***

Especifica la hora de inicio de la operación programada. La hora de inicio de la programación debe incluirse en el formato *aaaa-MM-dd HH:mm*.

- **-runasuser *runasuser***

Especifica si se cambia el usuario (usuario raíz o usuario de Oracle) de la operación de backup programada mientras se programa el backup.

- **-taskspec *taskspec***

Especifica el archivo XML de especificación de la tarea que se puede utilizar para la actividad de preprocesamiento o la actividad de posprocesamiento de la operación de copia de seguridad. Se debe proporcionar la ruta completa del archivo XML con el `-taskspec` opción.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## El comando `smsap schedule delete`

Este comando elimina una programación de backup cuando ya no es necesaria.

### Sintaxis

```

smsap schedule delete -profile profile_name
-schedule-name schedule_name[-quiet | -verbose]

```

### Parámetros

- **-profile *profile\_name***

Especifica el nombre del perfil relacionado con la base de datos que desea eliminar una programación de backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-schedule-name *schedule\_name***

Especifica el nombre de programación que se proporcionó al crear una programación de backups.

## El comando `smsap schedule list`

Este comando, enumera las operaciones programadas asociadas con un perfil.

### Sintaxis

```
smsap schedule list -profile profile_name
[-quiet | -verbose]
```

### Parámetros

- **-profile *profile\_name***

Especifica el nombre del perfil relacionado con la base de datos, mediante el cual puede ver una lista de operaciones programadas. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

## El comando `smsap schedule resume`

Este comando reanuda la programación de backup suspendida.

### Sintaxis

```
smsap schedule resume -profile profile_name
-schedule-name schedule_name[-quiet | -verbose]
```

### Parámetros

- **-profile *profile\_name***

Especifica el nombre del perfil relacionado con la base de datos que desea reanudar la programación de backups suspendida. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-schedule-name *schedule\_name***

Especifica el nombre de programación que se proporcionó al crear una programación de backups.

## El comando `smsap schedule suspend`

Este comando suspende una programación de backup hasta que se reanuda la programación de backup.

## Sintaxis

```
smsap schedule suspend -profile profile_name
-schedule-name schedule_name [-quiet | -verbose]
```

## Parámetros

- **-profile *profile\_name***

Especifica el nombre del perfil relacionado con la base de datos que desea suspender una programación de backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-schedule-name *schedule\_name***

Especifica el nombre de programación que se proporcionó al crear una programación de backups.

## El comando `smsap schedule update`

Este comando actualiza la programación de una copia de seguridad.

## Sintaxis

```
smsap schedule update -profile profile_name
-schedule-name schedule_name [-schedule-comment
schedule_comment]
-interval {-hourly | -daily | -weekly | -
monthly | -onetimeonly}
-cronstring cron_string -start-time {start_time < yyyy-MM-dd
HH:mm>}
-runasuser runasuser [-taskspec taskspec] -force
[-quiet | -verbose]
```

## Parámetros

- **-profile *profile\_name***

Especifica el nombre del perfil relacionado con la base de datos que desea programar el backup. El perfil contiene el identificador de la base de datos y otra información de la base de datos.

- **-schedule-name *schedule\_name***

Especifica el nombre que se proporcionará para la programación.

- **-schedule-comment *schedule\_comment***

Especifica un comentario opcional que se va a describir acerca de la programación del backup.

- **-interval { *-hourly* | *-daily* | *-weekly* | *-monthly* | *-onetimeonly* }**

Indica el intervalo de tiempo mediante el cual se crean los backups. Se puede programar el backup cada hora, día, semana, mes o una sola vez.

- **-cronstring *cron\_string***

Especifica la programación del backup mediante cronstring. Las expresiones cron se utilizan para configurar instancias de CronTrigger. Las expresiones cron son cadenas que se componen de siete subexpresiones:

- 1 se refiere a segundos
- 2 se refiere a minutos
- 3 se refiere a horas
- 4 se refiere a un día en un mes
- 5 se refiere al mes
- 6 se refiere a un día en una semana
- 7 se refiere al año (opcional)

- **-start-time *yyyy-MM-dd HH:mm***

Especifica la hora de inicio de la operación de programación. La hora de inicio de la programación debe incluirse en el formato *aaaa-MM-dd HH:mm*.

- **-runasuser *runasuser***

Especifica si se va a cambiar el usuario de la operación de backup programada mientras se programa el backup.

- **-taskspec *taskspec***

Especifica el archivo XML de especificación de la tarea que se puede utilizar para la actividad de preprocesamiento o la actividad de posprocesamiento de la operación de copia de seguridad. Debe proporcionarse la ruta completa del archivo XML, que proporciona la opción `-taskspec` .

## El comando `smsap Storage list`

Puede ejecutar el `storage list` comando para mostrar la lista de sistemas de almacenamiento asociados con un perfil determinado.

### Sintaxis

```
smsap storage list  
-profile profile
```

### Parámetros

- **-profile *profile***

Especifica el nombre del perfil. El nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

## Ejemplo

En el siguiente ejemplo se muestran los sistemas de almacenamiento asociados al perfil mjullian:

```
smsap storage list -profile mjullian
```

```
Sample Output:  
Storage Controllers  
-----  
FAS3020-RTP07OLD
```

## El comando smsap Storage rename

Este comando actualiza el nombre o la dirección IP del sistema de almacenamiento.

### Sintaxis

```
smsap storage rename  
-profile profile -oldname old_storage_name -newname new_storage_name  
[-quiet | -verbose]
```

### Parámetros

- **-profile *profile***

Especifica el nombre del perfil. Este nombre puede tener hasta 30 caracteres y debe ser único dentro del host.

- **-oldname *old\_storage\_name***

Especifica la dirección IP o el nombre del sistema de almacenamiento antes de cambiar el nombre del sistema de almacenamiento. Debe introducir la dirección IP o el nombre del sistema de almacenamiento que se muestra al ejecutar el `smsap storage list` comando.

- **-newname *new\_storage\_name***

Especifica la dirección IP o el nombre del sistema de almacenamiento después de cambiar el nombre del sistema de almacenamiento.

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**



Muestra mensajes de error, advertencia e informativos en la consola.

## Ejemplo

En el ejemplo siguiente se utiliza la `smsap storage rename` comando para cambiar el nombre del sistema de almacenamiento:

```
smsap storage rename -profile mjullian -oldname lech -newname hudson  
-verbose
```

## El comando `smsap system dump`

Puede ejecutar el `system dump` Comando para crear un archivo JAR que contenga información de diagnóstico acerca del entorno del servidor.

### Sintaxis

```
smsap system dump  
[-quiet | -verbose]
```

### Parámetros

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

### Ejemplo del comando `system dump`

En el ejemplo siguiente se utiliza el comando `smsap system dump` para crear un archivo JAR:

```
smsap system dump  
Path:/userhomedirectory/.netapp/smsap/3.3.0/smsap_dump_hostname.jar
```

## El comando `smsap system verify`

Este comando confirma que todos los componentes del entorno necesario para ejecutar SnapManager están configurados correctamente.

## Sintaxis

```
smsap system verify  
[-quiet | -verbose]
```

## Parámetros

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra mensajes de error, advertencia e informativos en la consola.

## Ejemplo del comando system verify

En el ejemplo siguiente se utiliza la `smsap system verify` comando.

```
smsap system verify  
SMSAP-13505 [INFO ]: Snapdrive verify passed.  
SMSAP-13037 [INFO ]: Successfully completed operation: System Verify  
SMSAP-13049 [INFO ]: Elapsed Time: 0:00:00.559  
Operation Id [N4f4e910004b36cfecee74c710de02e44] succeeded.
```

## El comando smsap version

Puede ejecutar el `version` Comando para determinar la versión de SnapManager que se ejecuta en el host local.

## Sintaxis

```
smsap version  
[-quiet | -verbose]
```

## Parámetros

- **-quiet**

Muestra sólo mensajes de error en la consola. El valor predeterminado es mostrar mensajes de error y advertencia.

- **-verbose**

Muestra la fecha de creación y el contenido de cada perfil. También muestra mensajes de error,

advertencia e informativos en la consola.

## Ejemplo del comando version

En el siguiente ejemplo, se muestra la versión de SnapManager:

```
smsap version
SnapManager for SAP Version: 3.3.1
```

## Resolución de problemas de SnapManager

Puede encontrar información sobre algunos de los problemas más comunes que se pueden producir y el modo en que puede resolverlos.


La siguiente tabla describe los problemas comunes y las posibles soluciones:



Pregunta basada en cuestiones	Posible solución
¿Se están ejecutando la base de datos de destino y el listener?	Ejecute el <code>lsnrctl status</code> comando. Asegúrese de que la instancia de base de datos está registrada en el listener.
¿El almacenamiento está visible?	Ejecute el <code>snapdrive storage show -all</code> comando.
¿Es el almacenamiento editable?	Edite un archivo en el punto de montaje que acaba de crear. Utilice la <code>touch filename</code> comando. Si se crea el archivo, se puede escribir en el almacenamiento. Debe asegurarse de que el usuario pueda escribir el almacenamiento SnapManager como (por ejemplo, como raíz en UNIX).
¿Se ejecuta el servidor SnapManager?	Ejecución <code>smsap_server status</code> e intente iniciar el servidor utilizando <code>smsap_server start</code> comando.  Para poder utilizar la interfaz gráfica de usuario (GUI) o la interfaz de línea de comandos (CLI) para iniciar comandos de la SnapManager relacionados con los perfiles, el servidor debe estar en ejecución. Puede crear o actualizar repositorios sin iniciar el servidor, pero para ejecutar todas las demás operaciones de SnapManager, el servidor debe estar en ejecución.  Para iniciar el servidor SnapManager, introduzca el siguiente comando: <code>smsap_server start.</code>
¿Son todos los componentes necesarios para ejecutar la configuración correcta de SnapManager?	Ejecute el <code>smsap system verify</code> Comando para verificar que SnapDrive está configurado correctamente.

<b>Pregunta basada en cuestiones</b>	<b>Posible solución</b>
¿ Tiene la versión correcta de SnapManager?	Utilice la <code>smsap version</code> Comando para comprobar la versión de SnapManager.
¿ Ha consultado los archivos de registro de SnapManager para determinar si los mensajes de error pueden ayudar a aislar el problema?	<p>SnapManager registra todas las entradas de registro en un conjunto de archivos de registro giratorios. Los archivos de registro se encuentran en <code>/var/log/smsap</code>.</p> <p>Los archivos de registro se encuentran en <code>C:\program_files\NetApp\SnapManager for SAP\logs</code>.</p> <p>También puede ser útil consultar los registros en la siguiente ubicación:</p> <p><code>/usr_home/.netapp/smsap/3.3.0/log/</code></p> <p>Cada registro de operaciones se escribe en su propio archivo de registro del formulario <code>smsap_of_date_time.log</code>.</p>
Si tiene registros de archivos almacenados en un sistema de almacenamiento que no ejecuta Data ONTAP, ¿ los ha excluido de tener en cuenta para backup con SnapManager?	<p>La <code>smsap.config</code> file permite excluir determinados archivos de registro de archivos. Para UNIX, los archivos se encuentran en la siguiente ubicación: <code>/opt/NetApp/smsap/properties/smsap.config</code></p> <p>Utilice el formato mencionado en el archivo para excluir los registros de archivo locales. Para obtener información adicional, consulte el tema "Configuración de propiedades de configuración".</p> <p>También puede excluir los destinos del registro de archivos mientras crea un backup desde la interfaz de línea de comandos de SnapManager. Para obtener información adicional, consulte el tema «"creación de copias de seguridad de bases de datos"».</p> <p>También puede excluir los destinos del registro de archivos al crear un backup desde la interfaz gráfica de usuario de SnapManager.</p>
¿ Tiene una licencia de FlexClone si utiliza SnapManager con bases de datos de NFS?	<p>Se requiere una licencia de FlexClone para aprovechar al máximo SnapManager con las bases de datos NFS. SnapManager utiliza la función FlexClone para realizar estas tareas:</p> <ul style="list-style-type: none"> <li>• Montar backups de bases de datos NFS</li> <li>• Verificar backups de bases de datos NFS</li> <li>• Clonar bases de datos NFS</li> </ul>



Pregunta basada en cuestiones	Posible solución
¿No ha podido conectarse al repositorio?	<p>Si se produce un error en la conexión con un repositorio, ejecute el <code>lsnrctl status</code> en la base de datos del repositorio y compruebe los nombres de servicio activos. Cuando SnapManager se conecta a la base de datos del repositorio, utiliza el nombre de servicio de la base de datos. Dependiendo de cómo esté configurado el listener, este puede ser el nombre corto del servicio o el nombre completo del servicio. Cuando SnapManager se conecta a una base de datos para una operación de backup, restauración u otra, utiliza el nombre de host y el SID. Si el repositorio no se inicializa correctamente porque no se puede acceder a él actualmente, recibe un mensaje de error que le pregunta si desea quitar el repositorio. Es posible quitar el repositorio de la vista actual para poder realizar operaciones en otros repositorios.</p> <p>Además, compruebe si la instancia del repositorio está en ejecución ejecutando el <code>ps -eaf grep instance - name</code> comando.</p>
¿El sistema puede resolver el nombre de host?	<p>Compruebe si el nombre de host especificado está en una subred diferente. Si recibe un mensaje de error que SnapManager no puede resolver el nombre de host, añada el nombre de host en el archivo de host. Añada el nombre de host al archivo ubicado en <code>/etc/hosts</code>:</p> <p><b>xxx.xxx.xxx.xxx hostname IP address</b></p>
¿Se ejecuta SnapDrive?	<p>Compruebe si el daemon SnapDrive se está ejecutando:</p> <p><b>-snapdrived status</b></p> <p>Si el daemon no se está ejecutando, aparece un mensaje que indica que hay un error de conexión.</p>
¿A qué sistemas de almacenamiento se ha configurado para acceder mediante SnapDrive?	<p>Ejecute el comando:</p> <p><b>-snapdrive config list</b></p>

Pregunta basada en cuestiones	Posible solución
<p>¿Cómo se puede mejorar el rendimiento de la interfaz gráfica de usuario de SnapManager?</p>	<ul style="list-style-type: none"> <li>• Asegúrese de tener credenciales de usuario válidas para el repositorio, el host de perfiles y el perfil.</li> </ul> <p>Si la credencial no es válida, borre las credenciales de usuario para el repositorio, el host del perfil y el perfil. Restablezca las mismas credenciales de usuario que haya establecido antes para el repositorio, el host del perfil y el perfil. Para obtener información adicional acerca de cómo volver a configurar las credenciales de usuario, consulte "Configuración de credenciales después de borrar la caché de credenciales".</p> <ul style="list-style-type: none"> <li>• Cierre los perfiles no utilizados.</li> </ul> <p>Si el número de perfiles que ha abierto es mayor, el rendimiento de la interfaz gráfica de usuario de SnapManager se ralentiza.</p> <ul style="list-style-type: none"> <li>• Compruebe si ha activado <b>Abrir al inicio</b> en la ventana Preferencias del usuario en el menú <b>Admin</b> desde la GUI de SnapManager.</li> </ul> <p>Si esto está activado, la configuración del usuario (<code>user.config</code>) file available at <code>/root/.netapp/smsap/3.3.0/gui/state</code> is displayed as <code>openOnStartup=PROFILE</code>.</p> <p>Debido a que <b>Abrir al inicio</b> está activado, debe buscar perfiles abiertos recientemente desde la GUI de SnapManager, utilizando <code>lastOpenProfiles</code> en la configuración del usuario (<code>user.config</code>) archivo: <code>lastOpenProfiles=PROFILE1,PROFILE2,PROFILE3,...</code></p> <p>Puede eliminar los nombres de perfil que aparecen y mantener siempre un número mínimo de perfiles abiertos.</p> <ul style="list-style-type: none"> <li>• El perfil protegido tarda más tiempo en actualizarse que el perfil que no está protegido.</li> </ul> <p>El perfil protegido se actualiza en un intervalo de tiempo, según el valor especificado en <code>protectionStatusRefreshRate</code> parámetro de la configuración de usuario (<code>user.config</code>) archivo.</p> <p>Puede aumentar el valor desde el valor predeterminado (300 segundos) para que los perfiles protegidos se actualicen sólo después del intervalo de tiempo especificado.</p> <ul style="list-style-type: none"> <li>• Antes de instalar la nueva versión de SnapManager en el entorno basado en UNIX, elimine las entradas del cliente de SnapManager disponibles en la siguiente ubicación:</li> </ul> <p><code>/root/.netapp</code></p>

Pregunta basada en cuestiones	Posible solución
<p>La interfaz gráfica de usuario de SnapManager tarda más tiempo en actualizarse cuando se SnapManager inician y se ejecutan simultáneamente en segundo plano. Al hacer clic con el botón derecho en el backup (que ya se ha eliminado pero se sigue mostrando en la interfaz gráfica de usuario de SnapManager), las opciones de backup para ese backup no se habilitan en la ventana Backup o Clone.</p>	<p>Debe esperar hasta que se actualice la interfaz gráfica de usuario de SnapManager y, a continuación, comprobar el estado de backup.</p>
<p>¿Qué haría si la base de datos de Oracle no está configurada en inglés?</p>	<p>Posibilidad de error en las operaciones de SnapManager si el idioma de una base de datos de Oracle no está configurado en inglés. Defina el idioma de la base de datos Oracle en inglés:</p> <ol style="list-style-type: none"> <li>1. Añada lo siguiente bajo los comentarios iniciales de <code>/etc/init.d/smsap_server</code> <ul style="list-style-type: none"> <li>◦ <code>NLS_Lang=American_America</code></li> <li>◦ <code>Exportar NLS_Lang</code></li> </ul> </li> <li>2. Reinicie el servidor SnapManager con el siguiente comando: <code>smsap_server restart</code></li> </ol> <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p> Si los scripts de inicio de sesión como <code>.bash_profile</code>, <code>.bashrc</code>, y <code>.cshrc</code> Para el usuario de Oracle está establecido en <b>NLS_LANG</b>, debe editar la secuencia de comandos para que no se sobrescriba <b>NLS_LANG</b>.</p> </div>

Pregunta basada en cuestiones	Posible solución
<p>¿Qué se haría si se produce un error en la operación de programación de backups si la base de datos del repositorio apunta a más de una IP y cada IP tiene un nombre de host diferente?</p>	<ol style="list-style-type: none"> <li>1. Detenga el servidor SnapManager.</li> <li>2. Elimine los archivos de programación del directorio de repositorios de los hosts en los que desea activar la programación de backup.</li> </ol> <p>Los nombres de los archivos de programación pueden tener los siguientes formatos:</p> <ul style="list-style-type: none"> <li>◦ repository#repo_username#repository_database_name#repository_host#repo_port</li> <li>◦ repository-repo_usernamerepository_database_name-repository_host-repo_port</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>Asegúrese de eliminar el archivo de programación en el formato que coincida con los detalles del repositorio.</p> </div> <ol style="list-style-type: none"> <li>3. Reinicie el servidor SnapManager.</li> <li>4. Abra otros perfiles en el mismo repositorio de la interfaz gráfica de usuario de SnapManager para asegurarse de que no se pierda ninguna información de programación de dichos perfiles.</li> </ol>
<p>¿Qué haría si la operación de SnapManager presenta un error de bloqueo del archivo de credenciales?</p>	<p>SnapManager bloquea el archivo de credenciales antes de la actualización y lo desbloquea después de la actualización. cuando se ejecutan varias operaciones a la vez, una de las operaciones puede bloquear el archivo de credenciales para actualizarlo. Si otra operación intenta acceder al archivo de credenciales bloqueadas al mismo tiempo, la operación genera un error de bloqueo de archivo.</p> <p>Configure los siguientes parámetros en el archivo smsap.config en función de la frecuencia de las operaciones simultáneas:</p> <ul style="list-style-type: none"> <li>• fileLock.retryInterval = 100 milisegundos</li> <li>• fileLock.timeout = 5000 milisegundos</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>Los valores asignados a los parámetros deben ser en milisegundos.</p> </div>



Pregunta basada en cuestiones	Posible solución
<p>¿Qué haría si el estado intermedio de la operación de verificación de backup muestra un error en la pestaña Monitor aunque todavía esté en ejecución la operación de verificación de backup?</p>	<p>El mensaje de error se registra en el archivo <code>sm_gui.log</code>. Debe buscar en el archivo de registro para determinar los nuevos valores de <code>operation.heartbeatInterval</code> and <code>operation.heartbeatThreshold</code> que resolverán este problema.</p> <ol style="list-style-type: none"> <li>Añada los siguientes parámetros en el archivo <code>smsap.config</code>: <ul style="list-style-type: none"> <li><code>operation.heartbeatInterval = 5000</code></li> <li><code>operation.heartbeatThreshold = 5000</code> el valor predeterminado asignado por SnapManager es 5000.</li> </ul> </li> <li>Asigne nuevos valores a estos parámetros.</li> </ol> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin: 10px 0;">  Los valores asignados a los parámetros deben ser en milisegundos. </div> <ol style="list-style-type: none"> <li>Reinicie el servidor SnapManager y vuelva a realizar la operación.</li> </ol>
<p>¿Qué se debe hacer cuando se encuentra un problema de espacio en montón?</p>	<p>Cuando encuentre un problema de espacio en montón durante las operaciones de SnapManager para SAP, debe realizar los siguientes pasos:</p> <ol style="list-style-type: none"> <li>Vaya al directorio de instalación de SnapManager para SAP.</li> <li>Abra el <code>launchjava</code> de la <code>installationdirectory/bin/launchjava</code> ruta.</li> <li>Aumente el valor de <code>java -Xmx160m</code> Parámetro Java heap-space.</li> </ol> <p>Por ejemplo, puede aumentar el valor predeterminado de 160 m a 200 m.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin: 10px 0;">  Si ha aumentado el valor del parámetro Java heap-space en las versiones anteriores de SnapManager para SAP, debe conservar ese valor. </div>
<p>¿Qué haría si no pudiera utilizar los backups protegidos para restaurar o clonar?</p>	<p>Este problema se observa si utiliza SnapManager 3.3.1 con Clustered Data ONTAP y se ha actualizado a SnapManager 3.4. Los backups se protegieron mediante secuencias de comandos posteriores en SnapManager 3.3.1. A partir de SnapManager 3.4, los backups se protegen con las políticas <code>SnapManager_CDOT_Mirror</code> o <code>SnapManager_CDOT_Vault</code> que se seleccionan al crear un perfil. Después de actualizar a SnapManager 3.4, es posible que siga utilizando los perfiles antiguos y, por lo tanto, los backups se protejan con scripts de backup, Pero no puede usarlos para restaurar o clonar mediante SnapManager.</p> <p>Debe actualizar el perfil y seleccionar la política <code>SnapManager_CDOT_Mirror</code> o <code>SnapManager_CDOT_Vault</code> y eliminar el script posterior que se utilizó para la protección de datos en SnapManager 3.3.1.</p>

Pregunta basada en cuestiones	Posible solución
¿Qué haría si los backups programados no se protegerían (SnapVault)?	Después de actualizar a SnapManager 3.4 y actualizar el perfil para utilizar la política de protección de <i>SnapManager_CDOT_Vault</i> , debe eliminar las programaciones de backup antiguas y crear nuevas programaciones para especificar la etiqueta de SnapVault mientras crea la programación.

## Volcar archivos

Los archivos de volcado son archivos de registro comprimidos que contienen información acerca de SnapManager y su entorno. Los diferentes tipos de archivos de registro creados son operación, perfil y archivo de volcado del sistema.

Puede utilizar el comando `dump` o la ficha **Create Diagnostics** de la interfaz gráfica de usuario (GUI) para recopilar información sobre una operación, un perfil o el entorno. Un volcado del sistema no requiere un perfil; sin embargo, los volcados de perfil y operación requieren perfiles.

SnapManager incluye la siguiente información de diagnóstico en el archivo de volcado:

- Los pasos realizados
- El tiempo que tarda cada paso en completarse
- El resultado de cada paso
- Error, si hay alguno, que ocurrió durante la operación



Los archivos de registro o los archivos de volcado de SnapManager permiten permisos de lectura y escritura sólo para los usuarios raíz y los demás usuarios que pertenecen al grupo de usuarios raíz.

SnapManager también incluye la siguiente información en el archivo:

- Arquitectura y versión del sistema operativo
- Variables de entorno
- Versión de Java
- Arquitectura y versión de SnapManager
- Preferencias de SnapManager
- Mensajes de SnapManager
- propiedades `log4j`
- Arquitectura y versión de SnapDrive
- Archivos de registro de SnapDrive
- Versión de Oracle
- Detalles del inventario local de Oracle OPatch
- Detalles del inventario local de OPatch de la instancia de Automatic Storage Management (ASM)
- Versión del sistema de almacenamiento
- Archivo `oratab` de Oracle

- Estado del listener de Oracle
- Archivos de configuración de red de Oracle (`listener.ora` y `tnsnames.ora`)
- Versión de Oracle de la base de datos del repositorio
- Tipo de base de datos de destino (clústeres de aplicaciones reales (RAC) o en soporte)
- Función de base de datos de destino (primaria, física en espera o lógica en espera)
- Configuración de Oracle Recovery Manager (RMAN) de la base de datos de destino (sin integración de RMAN, RMAN con archivos de control o RMAN con archivo de catálogo)
- Versión de la instancia de ASM de la base de datos de destino
- Versión de Oracle de la base de datos de destino
- Identificador del sistema (SID) de la base de datos de destino
- Nombre del servicio de base de datos del repositorio
- Instancias de base de datos instaladas en el host
- Descriptor perfil
- Memoria compartida máxima
- Intercambio información de espacio
- Información de la memoria
- Versión del kernel
- FSTAB
- Protocolo que utiliza SnapDrive
- Entorno multivía
- RAC
- Gestor de volúmenes admitido
- Versión de Operations Manager
- Sistema de archivos compatible
- Versión de utilidades de host
- Versiones de interfaz BACKINT
- Versión de la herramienta BR
- Nivel de parche
- Salida del `system verify` comando
- Salida del `sdconfcheck` comando

Los archivos de volcado de SnapManager también contienen el archivo de recopilador de datos de SnapDrive y el archivo de registro de alertas de Oracle. Puede recopilar el archivo de registro de alertas de Oracle mediante el `smsap operation volcado` y `smsap profile dump` comandos.



El volcado del sistema no contiene registros de alertas de Oracle; sin embargo, los volcados de alerta y de operación contienen los registros de alerta.

Aunque no se esté ejecutando el servidor host SnapManager, puede acceder a la información de volcado mediante la interfaz de línea de comandos (CLI) o la interfaz gráfica de usuario.

Si se encuentra con un problema que no se puede resolver, puede enviar estos archivos a los servicios globales de NetApp.

### Crear archivos de volcado en el nivel de las operaciones

Puede utilizar el `smsap operation` El comando `dump` con el nombre o el ID de la operación ha fallado para obtener información de registro sobre una operación particular. Es posible especificar niveles de registro diferentes para recopilar información sobre una operación, un perfil, un host o un entorno específicos.

#### Paso

1. Introduzca el siguiente comando:

```
smsap operation dump -id guid
```



El comando `smsap operation dump` proporciona un superconjunto de la información proporcionada por el `smsap profile dump` comando, que a su vez proporciona un superconjunto de la información proporcionada por el comando `smsap system dump`.

Ubicación del archivo de volcado:

```
Path: /<user-home>  
/.netapp/smsap/3.3.0/smsap_dump_8abc01c814649ebd0114649ec69d0001.jar
```

### Cree archivos de volcado a nivel de perfil

Puede encontrar información de registro sobre un perfil determinado mediante `smsap profile dump` comando con el nombre del perfil.

#### Paso

1. Introduzca el siguiente comando:

```
smsap profile dump -profile profile_name
```

Ubicación del archivo de volcado:

```
Path: /<user-home>  
/.netapp/smsap/3.3.0/smsap_dump_8abc01c814649ebd0114649ec69d0001.jar
```



Si encuentra un error al crear un perfil, utilice `smsap system dump` comando. Una vez que haya creado correctamente un perfil, utilice `smsap operation dump` y `smsap profile dump` comandos.

## Crear archivos de volcado en el nivel del sistema

Puede utilizar el `smsap system dump` Comando para obtener información sobre el host y el entorno de SnapManager. Es posible especificar niveles de registro diferentes para recoger información sobre una operación, un perfil o un host y un entorno específicos.

### Paso

1. Introduzca el siguiente comando:

```
smsap system dump
```

Volcado resultante

```
Path: /<user-home>/ .netapp/smsap/3.3.0/smsap_dump_server_host.jar
```

### Cómo localizar archivos de volcado

El archivo de volcado se encuentra en el sistema cliente para facilitar el acceso. Estos archivos son útiles si necesita solucionar un problema relacionado con el perfil, el sistema o cualquier operación.

El archivo de volcado se encuentra en el directorio principal del usuario en el sistema cliente.

- Si utiliza la interfaz gráfica de usuario (GUI), el archivo de volcado se encuentra en:

```
user_home/Application Data/NetApp/smsap/3.3.0/smsap_dump  
dump_file_type_name  
server_host.jar
```

- Si utiliza la interfaz de línea de comandos (CLI), el archivo de volcado se encuentra en:

```
user_home/.netapp/smsap/3.3.0/smsap_dump_dump_file_type_name  
server_host.jar
```

El archivo dump contiene el resultado del comando dump. El nombre del archivo depende de la información proporcionada. En la siguiente tabla se muestran los tipos de operaciones de volcado y los nombres de archivo resultantes:

Tipo de operación de volcado	Nombre de archivo resultante
Comando de volcado de la operación con ID de operación	<code>smsap_dump_ operation-id.jar</code>

Tipo de operación de volcado	Nombre de archivo resultante
Comando de volcado de la operación sin ID de operación	<p>smsap operation dump -profile <i>VH1</i> -verbose Se muestra la siguiente salida:</p> <pre data-bbox="410 296 1482 636"> smsap operation dump -profile VH1 -verbose [ INFO] SMSAP-13048: Dump Operation Status: SUCCESS [ INFO] SMSAP-13049: Elapsed Time: 0:00:01.404 Dump file created. Path: /oracle/VH1/&lt;path&gt;/smsap/3.3.0/smsap_dump_VH1_kaw.rtp.foo.com.jar </pre>
Comando system dump	smsap_dump_ <i>host-name</i> .jar
Comando de volcado de perfil	smsap_dump_ <i>profile-name</i> _ <i>host-name</i> .jar

### Cómo recopilar archivos de volcado

Puede incluir `-dump` En el comando SnapManager para recoger los archivos de volcado después de una operación SnapManager correcta o con errores.

Es posible recoger archivos de volcado para las siguientes operaciones de SnapManager:

- Creación de perfiles
- Actualizando perfiles
- Crear backups
- Verificación de backups
- Eliminar backups
- Liberando backups
- Montar backups
- Desmontaje de backups
- Restaurar backups
- Crear clones
- Eliminar clones
- Dividir clones



Al crear un perfil, puede recopilar archivos de volcado sólo si la operación se realiza correctamente. Si se produce un error al crear un perfil, debe utilizar `smsap system dump` comando. Para perfiles correctos, puede utilizar `smsap operation dump` y `smsap profile dump` comandos para recoger los archivos de volcado.

## ejemplo

```
smsap backup create -profile targetdb1_prof1 -auto -full -online -dump
```

## Recopilación de información de registro adicional para facilitar la depuración

Si necesita registros adicionales para depurar una operación de SnapManager con errores, debe configurar una variable de entorno externa `Server.log.level`. Esta variable anula el nivel de registro predeterminado y vuelca todos los mensajes de registro del archivo de registro. Por ejemplo, puede cambiar el nivel de registro a `DEBUG`, lo que registra mensajes adicionales y puede ayudar en la depuración de problemas.

Los registros de SnapManager se pueden encontrar en las siguientes ubicaciones:

- `/var/log/smsap`

Para anular el nivel de registro predeterminado, debe realizar los siguientes pasos:

1. Cree un `platform.override` Archivo de texto en el directorio de instalación de SnapManager.
2. Añada el `server.log.level` en la `platform.override` archivo de texto.
3. Asignar un valor (*TRACE*, *DEBUG*, *INFO*, *WARN*, *ERROR*, *FATAL*, o *PROGRESO*) al `server.log.level` parámetro.

Por ejemplo, para cambiar el nivel de registro a *ERROR*, establezca el valor de `server.log.level` Para *ERROR*.

```
server.log.level=ERROR
```

4. Reinicie el servidor SnapManager.



Si no se requiere la información del registro adicional, puede eliminar el `server.log.level` desde el `platform.override` archivo de texto.

SnapManager gestiona el volumen de archivos de registro del servidor según los valores definidos por el usuario de los siguientes parámetros en la `smsap.config` archivo:

- `log.max_log_files`
- `log.max_log_file_size`
- `log.max_rolling_operation_factory_logs`

## Solucionar problemas de clones

Puede encontrar información sobre eso que puede ocurrir durante las operaciones de clonado y cómo puede resolverla.

Síntoma	Explicación	Solución alternativa
Se produce un error en la operación de clonado cuando el destino de archivo se establece en <i>USE_DB_RECOVERY_FILE_DEST</i> .	Cuando el destino de archivado hace referencia a <i>USE_DB_RECOVERY_FILE_DEST</i> , el área de recuperación flash (FRA) gestiona activamente el registro de archivos. SnapManager no utiliza la ubicación de la FRA durante las operaciones de clonado o restauración y, por lo tanto, fallan las operaciones.	Cambie el destino de archivado por la ubicación del registro de archivos real en lugar de la ubicación del FRA.



Síntoma	Explicación	Solución alternativa
<p>Se produce un error en la operación de clonado con el siguiente mensaje de error:</p> <pre>Cannot perform operation: Clone Create. Root cause: ORACLE-00001: Error executing SQL: [ALTER DATABASE OPEN RESETLOGS;]. The command returned: ORA- 01195: online backup of file 1 needs more recovery to be consistent.</pre>	<p>Este problema ocurre si Oracle listener no puede conectarse a la base de datos.</p>	<p>Si utiliza la interfaz gráfica de usuario de SnapManager para clonar un backup, realice las siguientes acciones:</p> <ol style="list-style-type: none"> <li>1. En el árbol del repositorio, haga clic en <b>repositorio &gt; Host &gt; Perfil</b> para visualizar las copias de seguridad.</li> <li>2. Haga clic con el botón derecho del ratón en la copia de seguridad que desea clonar y seleccione <b>Clonar</b>.</li> <li>3. En la página Clone Initialization, introduzca los valores obligatorios y seleccione el método de especificación del clon.</li> <li>4. En la página Clone Specification, seleccione <b>parámetros</b>.</li> <li>5. Haga clic en la ficha <b>parámetro</b>.</li> <li>6. En el campo <b>Nombre de parámetro</b>, introduzca el nombre como <i>local_listener</i> Y haga clic en <b>Aceptar</b>.</li> <li>7. Active la casilla de verificación <b>Anular valor predeterminado</b> de la fila local_listener.</li> <li>8. Haga clic en cualquier parámetro y, a continuación, haga doble clic en el parámetro local_listener e introduzca el siguiente valor: <b>(ADDRESS= (PROTOCOL= TCP) (HOST=&lt;your_host_name&gt;) (PORT=&lt;port#&gt;))</b></li> <li>9. Haga clic en <b>Guardar en archivo</b>.</li> <li>10. Haga clic en <b>Siguiente</b> y continúe con el asistente de creación de clones.</li> </ol> <p>Si está utilizando CLI para clonar una copia de seguridad, debe incluir la siguiente información en la etiqueta <b>&lt;parameters&gt;</b> del archivo de especificación del clon:</p>


Síntoma	Explicación	Solución alternativa
Se produce un error en la operación de clonado con un mensaje de error que indica que el punto de montaje que está usando ya está en uso.	SnapManager no permite montar un clon en un punto de montaje existente. Por lo tanto, un clon incompleto no eliminaba el punto de montaje.	Especifique otro punto de montaje para que lo utilice el clon, o desmonte el punto de montaje problemático.
Se produce un error en la operación de clonado con un mensaje de error acerca de los archivos de datos que no tienen la extensión .dbf.	Algunas versiones de la utilidad Oracle NID no funcionan con archivos de datos a menos que los archivos utilicen una extensión .dbf.	<ul style="list-style-type: none"> <li>• Cambie el nombre del archivo de datos para darle una extensión .dbf.</li> <li>• Repita la operación de backup.</li> <li>• Clone el backup nuevo.</li> </ul>
Se produce un error en la operación de clonado debido a requisitos no cumplidos.	Está intentando crear un clon; sin embargo, no se cumplieron algunos de los requisitos previos.	Proceda como se describe en <i>creando un clon</i> para cumplir con los requisitos previos.
SnapManager no logra generar un nuevo perfil después de la operación de división de clones y el usuario no sabe si se crea el nuevo perfil.	SnapManager no puede preguntar si no se crea un nuevo perfil después de la operación de división de clones. Dado que no se muestra el mensaje, puede suponer que se crea el perfil.	Desde la interfaz de línea de comandos (CLI) de la SnapManager, introduzca el <code>clone split-result</code> comando para ver el resultado detallado de la operación de división de clones
SnapManager para SAP no puede clonar bases de datos físicas de Oracle 10gR2 (10.2.0.5) en espera de Oracle Data Guard.	SnapManager para SAP no deshabilita el modo de recuperación gestionado mientras se realiza un backup sin conexión de las bases de datos físicas en espera de Oracle 10gR2 (10.2.0.5) creadas con los servicios de Oracle Data Guard. Debido a este problema, el backup sin conexión realizado no es coherente. Cuando SnapManager para SAP intenta clonar el backup sin conexión, ni siquiera intenta realizar una recuperación en la base de datos clonada. Debido a que el backup no es coherente, la base de datos clonada requiere una recuperación y, por lo tanto, SAP no puede crear el clon correctamente.	Actualización de la base de datos Oracle a Oracle 11gR1 (parche 11.1.0.7).

Síntoma	Explicación	Solución alternativa
La clonado de un backup en un host remoto se produce un error con el siguiente mensaje <code>Error: Access is denied.</code>	Durante el montaje, si la dirección IP del host se proporciona al comando de montaje Snap, se podría producir un error en la operación de clonado. Este problema ocurre si el host en el que reside la base de datos está en el grupo de trabajo mientras el host remoto está en el dominio o viceversa.	Debe asegurarse de que tanto el host remoto como el host en el que reside la base de datos están en el dominio y no en el grupo de trabajo.

## Solución de problemas de la interfaz gráfica de usuario


Es posible encontrar información sobre algunos problemas de la interfaz gráfica de usuario (GUI) conocidos comunes que pueden ser de ayuda para resolverlos.

Problema	Explicación	Solución alternativa
Al acceder a la interfaz gráfica de usuario de SnapManager para realizar una operación, se puede mostrar el siguiente mensaje de error: <code>SMSAP-20111 : Authentication failed for user on host.</code>	Este problema se produce si se cambia la contraseña del usuario en el host en el que se ejecuta el servidor SnapManager. después de cambiar la contraseña, la caché de credenciales creada para el usuario que inició la GUI deja de ser válida. La interfaz gráfica de usuario de SnapManager sigue utilizando las credenciales de la caché para autenticar y, por lo tanto, la autenticación falla.	Debe realizar una de las siguientes tareas: <ul style="list-style-type: none"> <li>• Elimine las credenciales del usuario cuya contraseña se modificó y añada las nuevas credenciales en la caché ejecutando los siguientes comandos: <ol style="list-style-type: none"> <li>a. <code>smsap credential delete</code></li> <li>b. <code>smsap credential set</code></li> </ol> </li> <li>• Ejecute el para borrar toda la caché <code>smsap credential clear</code> command. Vuelva a abrir la GUI y establezca las credenciales, si se le solicita.</li> </ul>
Se muestra una advertencia de seguridad mientras se utiliza Java Web Start para acceder a la GUI de SnapManager.	Al acceder a la GUI de SnapManager mediante Java Web Start, se muestra una advertencia de seguridad. este problema se produce porque los tarros JNLP son autofirmados y la versión Java utilizada por SnapManager no permite los tarros autofirmados en un nivel de seguridad alto.	Cambie la configuración de seguridad a medio en el panel de control de Java o agregue la dirección URL de la GUI de SnapManager a la lista de excepciones.

Problema	Explicación	Solución alternativa
<p>La interfaz gráfica de usuario de inicio web de SnapManager muestra la versión incorrecta.</p>	<p>Después de cambiar a SnapManager de una versión posterior a una versión anterior al iniciar la GUI de inicio web, se inicia la versión posterior de la GUI de inicio web de SnapManager.</p>	<p>También debe borrar la caché realizando los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. Inicie la consola.</li> <li>2. Introduzca lo siguiente: <b>javaws -viewer</b></li> <li>3. En la pantalla del visor de caché Java, haga clic con el botón derecho del ratón en la aplicación SnapManager y seleccione <b>Eliminar</b>.</li> </ol>
<p>Al reiniciar la GUI e intentar comprobar las copias de seguridad de un perfil determinado, sólo verá los nombres de los perfiles.</p>	<p>SnapManager no muestra ninguna información sobre un perfil hasta que lo abre.</p>	<p>Siga estos pasos:</p> <ol style="list-style-type: none"> <li>1. Haga clic con el botón derecho del ratón en el perfil y seleccione <b>Abrir</b> en el menú.</li> </ol> <p>SnapManager muestra el cuadro de diálogo autenticación de perfiles.</p> <ol style="list-style-type: none"> <li>2. Introduzca el nombre de usuario y la contraseña del host.</li> </ol> <p>SnapManager muestra la lista de backups.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Sólo es necesario autenticar el perfil una vez, siempre que las credenciales sean válidas y permanezcan en la caché.</p> </div>
<p>Al abrir el primer repositorio en la interfaz gráfica de usuario, se muestra un mensaje de error similar al siguiente: <code>The Profile name XXXX clashes with previously loaded repository.</code></p>	<p>Los perfiles con el mismo nombre no pueden existir en un repositorio. Además, solo es posible abrir un repositorio a la vez.</p>	<p>Haga referencia a los perfiles en conflicto de dos usuarios distintos del sistema operativo o cambie el nombre del perfil emitiendo una sentencia SQL para el repositorio:</p> <pre><b>UPDATE SMSAP_33_PROFILE SET NAME = 'NEW_NAME' WHERE NAME = 'OLD_NAME'</b></pre>

Problema	Explicación	Solución alternativa
<p>Se muestra un mensaje de error similar al siguiente: SMSAP-01092: Unable to initialize repository repol@ does not exist:repolSMSAP-11006: Cannot resolve host does not exist</p>	<p>El repositorio es inaccesible, quizás porque ya no existe. La GUI inicializa la lista de repositorios desde el archivo de credenciales.</p>	<p>El mensaje de error le pregunta si desea eliminar este repositorio para que no se intente cargarlo en el futuro. Si no necesita acceder a este repositorio, haga clic en <b>Eliminar</b> para eliminarlo de la vista GUI. Esto elimina la referencia al repositorio en el archivo de credenciales y la interfaz gráfica de usuario no intenta volver a cargar el repositorio.</p>
<p>La creación de perfiles falla porque las credenciales de host no se autentican en las plataformas SUSE Linux Enterprise Server 10 y SUSE Linux Enterprise Server 11.</p>	<p>SnapManager utiliza el módulo de autenticación conectable (PAM) para autenticar usuarios. En las plataformas SUSE Linux Enterprise Server versiones 10 y 11, no existe snapmanager de forma predeterminada, en la <code>/etc/pam.d</code> directorio que proporciona los detalles de autenticación necesarios. De este modo, se producen errores en las credenciales del host.</p>	<p>Para iniciar sesión correctamente en el host de las plataformas SUSE Linux Enterprise Server 10 y 11, realice los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. Cree un snapmanager entrada de archivo <code>/etc/pam.d/</code>.</li> <li>2. Añada el siguiente contenido al snapmanager archivo ubicado en <code>/etc/pam.d/snapmanager</code>: <div data-bbox="1094 1050 1487 1472" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre> #%PAM-1.0 auth    include common-auth account include common-account password include common-password session include common-session </pre> </div> </li> <li>3. Guarde el archivo y vuelva a intentar la operación de creación de perfiles.</li> </ol>

Problema	Explicación	Solución alternativa
<p>SnapManager tarda más tiempo en cargar la estructura del árbol de la base de datos y da como resultado un mensaje de error de tiempo de espera que se muestra en la interfaz gráfica de usuario de SnapManager.</p>	<p>Cuando se intenta realizar una operación de backup parcial desde la interfaz gráfica de usuario de SnapManager, SnapManager intenta cargar las credenciales para todos los perfiles y, si hay entradas no válidas, SnapManager intenta validar la entrada y esto provoca que se muestre un mensaje de error de tiempo de espera.</p>	<p>Elimine las credenciales del host, el repositorio y el perfil que no se utilicen en <code>credential delete</code>. Desde la interfaz de línea de comandos (CLI) de la SnapManager.</p>
<p>SnapManager no logra generar un nuevo perfil después de la operación de división de clones y no sabe si se crea el nuevo perfil.</p>	<p>SnapManager no puede preguntar si no se crea un nuevo perfil después de la operación de división de clones. Dado que no se muestra ningún mensaje para la operación fallida, puede suponer que se crea el perfil.</p>	<p>Para saber si se crea un nuevo perfil para la operación de división de clones, realice los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. Haga clic en la ficha <b>Monitor</b>, haga clic con el botón derecho del ratón en la entrada de la operación de división de clones y seleccione <b>Propiedades</b>.</li> <li>2. En la ventana Propiedades del perfil, haga clic en la ficha <b>registros</b> para ver la operación de división de clones y los registros de creación de perfiles.</li> </ol>
<p>Los scripts personalizados para el procesamiento previo o posterior a la actividad que se realizan antes o después de las operaciones de backup, restauración o clonado no se pueden ver en la interfaz gráfica de usuario de SnapManager.</p>	<p>Cuando se añaden scripts personalizados en la ubicación del backup, la restauración o la clonado de scripts después de iniciar el asistente respectivo, los scripts personalizados no se muestran en la lista Available Scripts.</p>	<p>Reinicie el servidor host SnapManager y, a continuación, abra la interfaz gráfica de usuario de SnapManager.</p>
<p>No se puede utilizar el archivo XML de especificación del clon creado en SnapManager (3.1 o anterior) para la operación de clonado.</p>	<p>Desde SnapManager 3.2 para SAP, la sección de especificación de tareas (especificación de tareas) se proporciona como un archivo XML de especificación de tareas independiente.</p>	<p>Si utiliza SnapManager 3.2 para SAP, debe eliminar la sección de especificación de tareas del XML de especificación del clon o crear un archivo XML de especificación del clon nuevo. SnapManager 3.3 o posterior no admite el archivo XML de especificación del clon creado en SnapManager 3.2 o versiones anteriores.</p>

Problema	Explicación	Solución alternativa
<p>La operación de SnapManager en la interfaz gráfica de usuario no continúa después de borrar las credenciales de usuario mediante el <code>smsap credential clear</code>. Desde la CLI de SnapManager o haciendo clic en <b>Admin &gt; credenciales &gt; Clear &gt; caché</b> desde la GUI de SnapManager.</p>	<p>Se borran las credenciales establecidas para los repositorios, hosts y perfiles. SnapManager verifica las credenciales de usuario antes de iniciar cualquier operación. cuando las credenciales de usuario no son válidas, SnapManager no puede autenticarse. Cuando se elimina un host o un perfil del repositorio, las credenciales del usuario siguen estando disponibles en la caché. Estas entradas de credenciales innecesarias ralentizan las operaciones de SnapManager de la interfaz gráfica de usuario.</p>	<p>Reinicie la interfaz gráfica de usuario de SnapManager en función de cómo se borre la caché.</p> <ul style="list-style-type: none"> <li>• Si borró la caché de credenciales de la interfaz gráfica de usuario de SnapManager, no es necesario salir de la interfaz gráfica de usuario de SnapManager.</li> <li>• Si borró la caché de credenciales de la interfaz gráfica de línea de comandos de SnapManager, debe reiniciar la interfaz gráfica de usuario de SnapManager.</li> <li>• Si ha eliminado manualmente el archivo de credenciales cifrado, deberá reiniciar la interfaz gráfica de usuario de SnapManager.</li> </ul> <p></p> <p>Configure las credenciales que haya otorgado para el repositorio, el host del perfil y el perfil. Desde la GUI de SnapManager, si no hay ningún repositorio asignado en el árbol de repositorios, realice los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. Haga clic en <b>tareas &gt; Agregar repositorio existente</b></li> <li>2. Haga clic con el botón derecho del ratón en el repositorio, haga clic en <b>Abrir</b> e introduzca las credenciales de usuario en la ventana <b>autenticación de credenciales de repositorio</b>.</li> </ol> <p>Haga clic con el botón derecho del ratón en el host bajo el <span style="float: right;">389</span> repositorio, haga clic en <b>Abrir</b> e</p>

Problema	Explicación	Solución alternativa
Mensaje de error Unable to list the protection policies for the following reason: Protection Manager is temporarily unavailable Aparece al seleccionar <b>Ninguno</b> en el menú desplegable <b>Directiva de protección de Protection Manager</b> de la ventana Propiedades del perfil y la página de configuración de directivas del Asistente para crear perfiles.	Protection Manager no se configuró con SnapManager o Protection Manager no está en ejecución.	No es necesario realizar ninguna acción.
No se puede abrir la GUI de SnapManager mediante la GUI de inicio web de Java debido a la fortaleza del cifrado de capa de sockets seguros (SSL) más débil del explorador.	SnapManager no admite cifrados SSL de más de 128 bits.	Actualice la versión del navegador y compruebe la intensidad del cifrado.

## Resolución de problemas de SnapDrive

Puede que tenga algunos problemas comunes al utilizar SnapManager con productos de SnapDrive.

En primer lugar, debe determinar si el problema está relacionado con SnapManager para SAP o SnapDrive. Si el problema es un error de SnapDrive, SnapManager para SAP muestra un mensaje de error similar al siguiente:

```
SMSAP-12111: Error executing snapdrive command "<snapdrive command>":
<snapdrive error>
```

A continuación se muestra un ejemplo de un mensaje de error de SnapDrive en el que SMSAP-12111 Es el número de error SnapManager. La 0001-770 El esquema de numeración representa los errores de SnapDrive para UNIX.



```

SMSAP-12111: Error executing snapdrive command
"/usr/sbin/snapdrive snap restore -file
/mnt/pathname/ar_anzio_name_10gR2_arracl1/data/undotbs02.dbf -snapname
pathname.company.com:
/vol/ar_anzio_name_10gR2_arracl1:
TEST_ARRAC1_YORKTOW_arracl12_F_C_0_8abc01b20f9ec03d010f9ec06bee0001_0":
0001-770
Admin error: Inconsistent number of files returned when listing contents
of
/vol/ar_anzio_name_10gR2_arracl1/.snapshot/
TEST_ARRAC1_YORKTOW_arracl12_F_C_0_8abc01b20f9ec03d010f9ec06bee0001_0/data
on filer pathname.

```

A continuación, se muestran los mensajes de error más comunes de SnapDrive para UNIX relacionados con la detección de LUN, los problemas de configuración y el espacio. Si recibe alguno de estos errores, consulte el capítulo solución de problemas de la *Guía de instalación y administración de SnapDrive*.

Síntoma	Explicación
0001-136 Admin error: Unable to log on to filer: <filer> Please set user name and/or password for <filer>	Configuración inicial de SnapDrive
0001-382 Admin error: Multipathing rescan failed	Error de detección de LUN
0001-462 Admin error: Failed to unconfigure multipathing for <LUN>: spd5: cannot stop device. Device busy.	Error de detección de LUN
0001-476 Admin error: Unable to discover the device associated with ... 0001-710 Admin error: OS refresh of LUN failed ...	Error de detección de LUN
0001-680 Admin error: Host OS requires an update to internal data to allow LUN creation or connection. Use 'snapdrive config prepare luns' or update this information manually...	Error de detección de LUN
0001-817 Admin error: Failed to create volume clone ... : FlexClone not licensed	Configuración inicial de SnapDrive
0001-878 Admin error: HBA assistant not found. Commands involving LUNs should fail.	Error de detección de LUN

## Solucionar problemas de cambio de nombre del sistema de almacenamiento

Puede enfrentarse a problemas al cambiar el nombre de un sistema de almacenamiento

o después de haber cambiado correctamente el nombre del sistema de almacenamiento.

Cuando intenta cambiar el nombre del sistema de almacenamiento, es posible que la operación falle con el siguiente mensaje de error: SMSAP-05085 No storage controller "fas3020-rtp07New" is found to be associated with the profile

Debe introducir la dirección IP o el nombre del sistema de almacenamiento que aparece cuando ejecuta el `smsap storage list` comando.

Después de cambiar el nombre del sistema de almacenamiento, es posible que se produzca un error en las operaciones de SnapManager si SnapManager no reconoce el sistema de almacenamiento. Para resolver este problema, debe realizar algunos pasos adicionales en el host del servidor de DataFabric Manager y en el host del servidor SnapManager.

Realice los siguientes pasos en el host del servidor de DataFabric Manager:

1. Elimine la dirección IP y el host del sistema de almacenamiento anterior en el archivo de host ubicado en `/etc/hosts` En el host de DataFabric Manager Server.
2. Añada la nueva dirección IP y el host del nuevo sistema de almacenamiento en el archivo de host ubicado en `/etc/hosts` En el host de DataFabric Manager Server.
3. Cambie el nombre del host de almacenamiento introduciendo el comando siguiente:

```
dfm host rename -a old_host_name new_host_name
```

4. Configure la nueva dirección IP en el host introduciendo el comando siguiente:

```
dfm host set old_host_name_or_objId hostPrimaryAddress =  
new_storage_controller_ip_address
```



Este paso debe realizarse solo si se especificó la dirección IP como nombre del nuevo sistema de almacenamiento.

5. Actualice el nuevo nombre del sistema de almacenamiento en el host del servidor de DataFabric Manager. Para ello, introduzca el siguiente comando:

```
dfm host diag old_storage_name
```

Es posible verificar que el nombre de la controladora de almacenamiento anterior se reemplaza por un nuevo nombre de la controladora de almacenamiento con el siguiente comando:

```
dfm host discover new_storage_name
```

Realice los siguientes pasos como usuario raíz en el host del servidor SnapManager.



Cuando se introduce el nuevo nombre de controladora de almacenamiento, se debe utilizar el nombre de alias del sistema y no el nombre de dominio completo (FQDN).

1. Elimine el nombre del sistema de almacenamiento anterior introduciendo el siguiente comando:

```
snapdrive config delete old_storage_name
```



Si no elimina el nombre de sistema de almacenamiento anterior, todas las operaciones de SnapManager fallarán.

2. Elimine la dirección IP y el host del sistema de almacenamiento anterior en el archivo de host ubicado en `etc/hosts` en el host de la base de datos de destino.
3. Añada la nueva dirección IP y el host del nuevo sistema de almacenamiento en el archivo de host ubicado en `/etc/hosts` en el host de la base de datos de destino.
4. Añada el nombre del nuevo sistema de almacenamiento introduciendo el comando siguiente:

```
snapdrive config set root new_storage_name
```

5. Para asignar los nombres de los sistemas de almacenamiento anteriores y posteriores, introduzca el siguiente comando:

```
snapdrive config migrate set old_storage_namenew_storage_name
```

6. Elimine la ruta de gestión del sistema de almacenamiento anterior introduciendo el comando siguiente:

```
snapdrive config delete -mgmpath old_storage_name
```

7. Añada la ruta de gestión del nuevo sistema de almacenamiento introduciendo el comando siguiente:

```
snapdrive config set -mgmpath new_storage_name
```

8. Actualice el conjunto de datos tanto para los archivos de datos como los archivos de registro de archivos con el nuevo nombre del sistema de almacenamiento introduciendo el siguiente comando:

```
snapdrive dataset changehostname -dn dataset_name -oldname old_storage_name  
-newname new_storage_name
```

9. Actualice el perfil del nuevo nombre del sistema de almacenamiento introduciendo el comando siguiente:

```
smsap storage rename -profile profile_name -oldname old_storage_name -newname  
new_storage_name
```

10. Compruebe el sistema de almacenamiento asociado con el perfil introduciendo el comando siguiente:

```
smsap storage list -profile profile_name
```

## Resolución de problemas conocidos

Es necesario conocer algunos problemas conocidos que se pueden producir al utilizar SnapManager y cómo solucionar sus problemas.

### SnapManager para SAP no identifica el perfil como un perfil de modo de clúster

Si el nombre del perfil de Cluster-Mode no está presente en la `cmode_profiles.config` Archivo en el directorio de instalación de SnapManager para SAP, el siguiente mensaje de error podría activarse:

```
Please configure DFM server using snapdrive config set -dfm user_name  
appliance_name.
```

Además, al actualizar SnapManager para SAP, si elimina la `/opt/NetApp/smsap/*` y, a continuación, la `cmode_profiles.config` El archivo que tiene los nombres de perfil de Cluster-Mode también se elimina. Este problema también activa el mismo mensaje de error.

## Solución

Actualice el perfil: **`smsap profile update-profile <profile_name>`**



Si se instala SnapManager para SAP en la `/opt/NetApp/smsap/` ruta, entonces la ubicación del archivo será `/opt/NetApp/smsap/cmode_profile/cmode_profiles.config`.

## El servidor no se inicia

Al iniciar el servidor, es posible que aparezca un mensaje de error similar al siguiente:

```
SMSAP-01104: Error invoking command: SMSAP-17107: SnapManager Server failed to start on port 8074 because of the following errors: java.net.BindException: Address already in use
```

Esto puede deberse a que los puertos de escucha SnapManager (27314 y 27315, de forma predeterminada) están actualmente en uso en otra aplicación.

Este error también puede ocurrir si `smsap_server` El comando ya está en ejecución, pero SnapManager no detecta el proceso existente.

## Solución

Es posible volver a configurar SnapManager o la otra aplicación para utilizar diferentes puertos.

Para volver a configurar SnapManager, edite el siguiente archivo:

```
/opt/NTAP/smsap/properties/smsap.config
```

Asigne los siguientes valores:

- `SMSAP Server.Port=27314`
- `SMSAP Server.rmiRegistry.Port=27315`
- `remote.registry.ocijdbc.port= 27315`

El archivo `remote.registry.ocijdbc.Port` debe ser el mismo que `Server.rmiRegistry.Port`.

Para iniciar el servidor SnapManager, introduzca el siguiente comando: **`smsap_server start`**



Si el servidor ya se está ejecutando, aparecerá un mensaje de error.

Si el servidor ya está en ejecución, realice los siguientes pasos:

1. Detenga el servidor introduciendo el siguiente comando: **`smsap_server stop`**
2. Reinicie el servidor introduciendo el siguiente comando: **`smsap_server start`**

## Terminando una operación SnapManager en ejecución actualmente

Si el servidor SnapManager se bloquea y no puede ejecutar ninguna operación correctamente, puede finalizar SnapManager y sus operaciones.

### Solución

SnapManager funciona tanto con SnapManager como con Protection Manager. Debe realizar los siguientes pasos para enumerar los diferentes procesos en ejecución y detener el último proceso en ejecución.

1. Enumerar todos los procesos de SnapDrive que se están ejecutando: `ps`

**ps**

Ejemplo:

**ps | rep snapdrive**

2. Detenga el proceso o los procesos de SnapDrive: `kill <pid>`

*pid* es la lista de procesos que ha encontrado utilizando `ps` comando.



No se detienen todos los procesos de SnapDrive. Se recomienda finalizar solo el último proceso en ejecución.

3. Si una de las operaciones implica restaurar un backup protegido desde un almacenamiento secundario, abra la consola de Protection Manager y realice lo siguiente:
  - a. En el menú sistema, seleccione **trabajos**.
  - b. Seleccione **Restaurar**.
  - c. Compruebe el nombre del conjunto de datos que coincide con el del perfil de SnapManager.
  - d. Haga clic con el botón derecho del ratón y seleccione **Cancelar**.
4. Enumerar los procesos de SnapManager:
  - a. Inicie sesión como usuario root.
  - b. Enumerar los procesos mediante el comando `ps`.

Ejemplo: **ps | grep java**

5. Finalice el proceso SnapManager: `kill <pid>`

## No se puede eliminar ni liberar la última copia de seguridad protegida

Cuando se crea el primer backup para un perfil en el almacenamiento secundario, SnapManager envía toda la información sobre el backup a Protection Manager. Para backups posteriores relacionados con este perfil, SnapManager solo envía la información modificada. Si se elimina el último backup protegido, SnapManager pierde la capacidad para identificar las diferencias entre los backups y debe buscar una forma de volver a establecer la base de estas relaciones. Por lo tanto, al intentar eliminar la última copia de seguridad protegida se muestra un mensaje de error.

### Solución

Puede eliminar el perfil o sólo la copia de seguridad del perfil.

Para eliminar el perfil, realice los siguientes pasos:

1. Eliminar las copias de seguridad del perfil.
2. Actualice el perfil y desactive la protección en el perfil.

De esta forma se elimina el conjunto de datos.

3. Elimine la última copia de seguridad protegida.
4. Elimine el perfil.

Para eliminar solamente el backup, realice los siguientes pasos:

1. Cree otra copia de seguridad del perfil.
2. Transferir esa copia de backup a almacenamiento secundario.
3. Elimine la copia de seguridad anterior.

### **No se pueden gestionar los nombres de destino de los archivos de registro de archivos si los nombres de destino forman parte de otros nombres de destino**

Al crear una copia de seguridad del registro de archivos, si el usuario excluye un destino que forme parte de otros nombres de destino, también se excluirán los demás nombres de destino.

Por ejemplo, supongamos que hay tres destinos disponibles para ser excluidos: `/dest`, `/dest1`, y `/dest2`. Al crear la copia de seguridad del archivo de registro de archivos, si excluye `/dest` mediante el comando

```
smsap backup create -profile almsamp1 -data -online -archivelogs -exclude  
-dest /dest
```

, SnapManager para SAP excluye todos los destinos que comiencen con `/dest`.

### **Solución**

- Agregue un separador de ruta después de que los destinos estén configurados en `v$archive_dest`. Por ejemplo, cambie el `/dest` para `/dest/`.
- Al crear una copia de seguridad, incluya destinos en lugar de excluir cualquier destino.

### **La restauración de archivos de control multiplexados en Automatic Storage Management (ASM) y almacenamiento no ASM falla**

Cuando los archivos de control se multiplexan en almacenamiento ASM y no ASM, la operación de copia de seguridad se realiza correctamente. Sin embargo, cuando intenta restaurar archivos de control de ese backup exitoso, se produce un error en la operación de restauración.

### **Error en la operación de clonado de SnapManager**

Al clonar un backup en SnapManager, es posible que DataFabric Manager Server no detecte volúmenes y muestre el siguiente mensaje de error:

```
SMSAP-13032: Cannot perform operation: Clone Create. Root cause: SMSAP-11007:
```

```
Error cloning from snapshot: FLOW-11019: Failure in ExecuteConnectionSteps: SD-00018: Error discovering storage for /mnt/datafile_clone3: SD-10016: Error executing snapdrive command "/usr/sbin/snapdrive storage show -fs /mnt/datafile_clone3": 0002-719 Warning: Could not check SD.Storage.Read access on volume filer:/vol/SnapManager_20091122235002515_vol1 for user user-vm5\oracle on Operations Manager servers x.x.x.x
```

Reason: Invalid resource specified. Unable to find its Id on Operations Manager server 10.x.x.x

Esto sucede si el sistema de almacenamiento tiene un gran número de volúmenes.

## Solución

Debe realizar una de las siguientes acciones:

- Desde el servidor Data Fabric Manager, ejecute

```
dfm host discover storage_system
```

También puede añadir el comando en un archivo de script del shell y programar una tarea en DataFabric Manager Server para ejecutar el script a intervalos frecuentes.

- Aumente el valor de *dfm-rbac-retries* en la *Snapdrive.conf* archivo.

SnapDrive usa el valor del intervalo de actualización predeterminado y la cantidad predeterminada de reintentos. El valor predeterminado de *dfm-rbac-retry-sleep-secs* es 15 segundos y *dfm-rbac-retries* es 12 iteraciones.



El intervalo de actualización de Operations Manager depende del número de sistemas de almacenamiento, del número de objetos de almacenamiento del sistema de almacenamiento y de la carga sobre DataFabric Manager Server.

Como recomendación, lleve a cabo lo siguiente:

1. Desde DataFabric Manager Server, ejecute manualmente el siguiente comando para todos los sistemas de almacenamiento secundario asociados con el conjunto de datos:

```
dfm host discover storage_system
```

2. Duplique el tiempo necesario para realizar la operación de detección del host y asigne ese valor *dfm-rbac-retry-sleep-secs*.

Por ejemplo, si la operación tardó 11 segundos, puede establecer el valor de *dfm-rbac-retry-sleep-secs* a 22 (11\*2).

## El tamaño de la base de datos del repositorio crece con el tiempo y no con el número de backups

El tamaño de la base de datos del repositorio crece con el tiempo debido a que las operaciones SnapManager insertan o eliminan datos dentro del esquema en las tablas de la base de datos del repositorio, lo que da como resultado un uso elevado del espacio de índice.

## Solución

Debe supervisar y reconstruir los índices de acuerdo con las directrices de Oracle para controlar el espacio consumido por el esquema del repositorio.

### **No se puede acceder a la interfaz gráfica de usuario de SnapManager y se produce un error en las operaciones de SnapManager cuando la base de datos del repositorio está inactiva**

Se produce un error en las operaciones de SnapManager y no se puede acceder a la interfaz gráfica de usuario cuando la base de datos del repositorio está inactiva.

En la siguiente tabla, se enumeran las diferentes acciones que se pueden realizar y sus excepciones:

<b>Operaciones</b>	<b>Excepciones</b>
Abrir un repositorio cerrado	El siguiente mensaje de error ha iniciado sesión <code>sm_gui.log</code> : [WARN ]: SMSAP-01106: Error occurred while querying the repository: Closed Connection <code>java.sql.SQLException: Closed Connection.</code>
Para actualizar un repositorio abierto, pulse F5	Se muestra una excepción de repositorio en la GUI y también registra una <code>NullPointerException</code> en la <code>sm_gui.log</code> archivo.
Actualizar el servidor host	Se registra una <code>NullPointerException</code> en <code>sumo_gui.log</code> archivo.
Creación de un nuevo perfil	Aparecerá <code>NullPointerException</code> en la ventana Profile Configuration.
Actualizar un perfil	Se ha iniciado sesión la siguiente excepción SQL <code>sm_gui.log</code> : [WARN ]: SMSAP-01106: Error occurred while querying the repository: Closed Connection.
Obtener acceso a un backup	El siguiente mensaje de error ha iniciado sesión <code>sm_gui.log</code> : Failed to lazily initialize a collection.
Ver las propiedades de clon	El siguiente mensaje de error ha iniciado sesión <code>sm_gui.log</code> y. <code>sumo_gui.log</code> : Failed to lazily initialize a collection.

### **Solución**

Debe asegurarse de que se ejecute la base de datos del repositorio cuando se desea acceder a la interfaz gráfica de usuario o realizar cualquier operación de SnapManager.

### **No se pueden crear los archivos temporales para la base de datos clonada**

Cuando los archivos de espacio de tabla temporales de la base de datos de destino se colocan en puntos de montaje diferentes del punto de montaje de los archivos de datos, la operación de creación de clonado se realiza correctamente, pero SnapManager no puede crear archivos temporales para la base de datos clonada.

### **Solución**

Debe realizar una de las siguientes acciones:



- Asegúrese de que la base de datos de destino esté diseñada para que los archivos temporales se coloquen en el mismo punto de montaje que los archivos de datos.
- Crear manualmente o añadir archivos temporales en la base de datos clonada.

### No se puede migrar el protocolo de NFSv3 a NFSv4

Puede migrar el protocolo de NFSv3 a NFSv4 mediante la habilitación de `enable-migrate-nfs-version` en la `snapdrive.conf` archivo. Durante la migración, SnapDrive considera únicamente la versión del protocolo, independientemente de las opciones de los puntos de montaje como `rw`, `largefiles`, `nosuid`, y así sucesivamente.

Sin embargo, después de migrar el protocolo a NFSv4, cuando restaura el backup creado mediante NFSv3, se produce lo siguiente:

- Si se habilitan NFSv3 y NFSv4 en el nivel de almacenamiento, la operación de restauración se realiza correctamente, pero se monta con las opciones de punto de montaje que estaban disponibles durante el backup.
- Si solo se habilita NFSv4 en el nivel de almacenamiento, la operación de restauración se realiza correctamente y solo se conserva la versión del protocolo (NFSv4).

Sin embargo, las otras opciones de punto de montaje como `rw`, `largefiles`, `nosuid`, y así sucesivamente no se retienen.

### Solución

Primero debe apagar manualmente la base de datos, desmontar los puntos de montaje de la base de datos y montarlos con las opciones disponibles antes de la restauración.

### Se produce un error en el backup de la base de datos Data Guard en espera

Si se configura alguna ubicación de registro de archivos con el nombre de servicio de la base de datos primaria, se produce un error en el backup de la base de datos en espera de Data Guard.

### Solución

En la GUI, debe desactivar **especificar la ubicación del registro de archivo externo** correspondiente al nombre de servicio de la base de datos primaria.

### Se produce un error en el montaje de un volumen FlexClone en un entorno NFS

Cuando SnapManager crea un FlexClone de un volumen en un entorno NFS, se añade una entrada en la `/etc/exports` archivo. El clon o el backup no se pueden montar en un host de SnapManager con un mensaje de error.

```
El mensaje de error es: 0001-034 Command error: mount failed: mount:
filer1:/vol/SnapManager_20090914112850837_vol14 on /opt/NTAPsmsap/mnt/-
ora_data02-20090914112850735_1 - WARNING unknown option "zone=vol14" nfs mount:
filer1:/vol/SnapManager_20090914112850837_vol14: Permission denied.
```

Al mismo tiempo, se genera el siguiente mensaje en la consola del sistema de almacenamiento: Mon Sep 14 23:58:37 PDT [filer1: export.auto.update.disabled: warning]: /etc/exports was not updated for vol14 when the vol clone create command was run. Please either

manually update `/etc/exports` or copy `/etc/exports.new` to it.

Es posible que este mensaje no se capture en los mensajes de AutoSupport.



Es posible que tenga problemas similares al clonar volúmenes de FlexVol en NFS. Puede seguir los mismos pasos para habilitar el `nfs.export.auto-update` opción.

### Qué hacer

1. Ajuste la `nfs.export.auto-update` opción `on` así que la `/etc/exports` el archivo se actualiza automáticamente.

**options nfs.export.auto-update on**



En la configuración de par de alta disponibilidad, asegúrese de establecer la opción de exportaciones NFS en `on` para los dos sistemas de almacenamiento.

## Se produce un error en la ejecución de varias operaciones paralelas en SnapManager

Cuando se ejecutan varias operaciones en paralelo en bases de datos independientes que residen en el mismo sistema de almacenamiento, el `igroup` para LUN asociadas con ambas bases de datos puede eliminarse debido a una de las operaciones. Más adelante, si la otra operación intenta utilizar el `igroup` eliminado, SnapManager muestra un mensaje de error.

Por ejemplo, si ejecuta las operaciones de eliminación de backup y creación de backup en bases de datos diferentes casi al mismo tiempo, la operación de creación de backup generará errores. Los siguientes pasos secuenciales muestran lo que ocurre cuando se ejecutan operaciones de eliminación de backup y creación de backup en distintas bases de datos casi al mismo tiempo.

1. Ejecute el `backup delete` comando.
2. Ejecute el `backup create` comando.
3. La `backup create` El comando identifica el `igroup` ya existente y utiliza el mismo `igroup` para asignar la LUN.
4. La `backup delete` El comando elimina la LUN de backup, que se ha asignado al mismo `igroup`.
5. La `backup delete` A continuación, el comando elimina el `igroup` porque no hay ninguna LUN asociada con el `igroup`.
6. La `backup create` el comando crea el backup e intenta asignar al `igroup` que no existe y, por lo tanto, la operación genera un error.

### Qué hacer

Debe crear un `igroup` para cada sistema de almacenamiento utilizado por la base de datos y utilizar el siguiente comando para actualizar SDU con la información del `igroup`:

**snapdrive igroup add**

## Dónde obtener más información

Puede encontrar información sobre las tareas básicas relacionadas con la instalación y el uso de SnapManager.

Documentar	Descripción
Página de descripción de SnapManager	Esta página proporciona información sobre SnapManager, los punteros a la documentación en línea y un enlace a la página de descarga de SnapManager, desde la cual se puede descargar el software.
<i>Guía de configuración DE SAN Data ONTAP para 7-Mode</i>	Este documento está disponible en " <a href="#">Soporte de NetApp</a> ".  Se trata de un documento dinámico online que contiene la información más actualizada sobre los requisitos para configurar un sistema en un entorno SAN. Contiene información detallada sobre sistemas de almacenamiento y plataformas de host, problemas de cableado, problemas de switch y configuraciones.
Matriz de compatibilidad de SnapManager y SnapDrive	Este documento está disponible en la sección interoperabilidad de " <a href="#">Herramienta de matriz de interoperabilidad</a> ".  Se trata de un documento dinámico online que contiene la información más actualizada específica de SnapManager y sus requisitos de plataforma.
Notas de la versión de SnapManager	Este documento incluye SnapManager. También puede descargar una copia desde " <a href="#">Soporte de NetApp</a> ".  Contiene información de última hora que necesita para poner la configuración en funcionamiento sin problemas.
Documentación sobre la conexión para host y los kits de soporte de NetApp	" <a href="#">Soporte de NetApp</a> ".
Información del sistema operativo y de la base de datos del host	Estos documentos proporcionan información acerca del sistema operativo del host y el software de la base de datos.

## Clasificación de mensajes de error

Puede determinar la causa de un error si conoce las clasificaciones de mensajes.

En la siguiente tabla, se proporciona información acerca de los rangos numéricos de los diferentes tipos de mensajes que puede ver con SnapManager:

<b>Grupo</b>	<b>Rango</b>	<b>Uso</b>
ENTORNO ORACLE	1000-1999	Se utiliza para registrar el estado o los problemas con el entorno operativo de SnapManager. Este grupo incluye mensajes sobre los sistemas con los que SnapManager interactúa, por ejemplo, con el host, el sistema de almacenamiento, la base de datos, etc.
BACKUP	2000-2999	Asociados con el proceso de backup de la base de datos.
RESTAURAR	3000-3999	Asociados con el proceso de restauración de bases de datos.
CLONAR	4000-4999	Asociados con el proceso de clonado de base de datos.
PERFIL	5000-5999	Se utiliza para administrar perfiles.
GESTIONE	6000-6999	Se utiliza para gestionar backups.
INTERFAZ DE BASES DE DATOS VIRTUALES	7000-7999	Asociado con la interfaz de base de datos virtual.
INTERFAZ DE ALMACENAMIENTO VIRTUAL	8000-8999	Asociado con la interfaz de almacenamiento virtual.
REPOSITORIO	9000-9999	Asociado con la interfaz del repositorio.
MÉTRICAS	10000-10999	Asociados con el tamaño del backup de base de datos, tiempo transcurrido para realizar el backup, tiempo para restaurar la base de datos, número de veces que se clona una base de datos, etc.
INTERFAZ DE HOST VIRTUAL	11000-11999	Asociado con la interfaz del host virtual. Esta es la interfaz para el sistema operativo del host.
EJECUCIÓN	12000-12999	Asociado al paquete de ejecución, incluidas las llamadas al sistema operativo de desove y procesamiento.
PROCESO	13000-13999	Asociado con el componente de proceso de SnapManager.
SERVICIOS PÚBLICOS	14000-14999	Asociados con las utilidades de SnapManager, el contexto global, etc.
VOLCADO/DIAGNÓSTICO	15000-15999	Asociados con operaciones de volcado o diagnóstico.

Grupo	Rango	Uso
AYUDA	16000-16999	Asociado con ayuda.
SERVIDOR	17000-17999	Se utiliza en la administración del servidor SnapManager.
API	18000-18999	Asociado con la API.
RETROCESO	19000-19999	Asociado con BACKINT.
AUTOR	20000-20999	Asociado con la autorización de credenciales.

## Mensajes de error

Es posible encontrar información sobre los mensajes de error asociados a diferentes operaciones de SnapManager.

### Mensajes de error más comunes

En la siguiente tabla se enumeran algunos de los errores más comunes e importantes asociados con SnapManager para SAP:

Mensaje de error	Explicación	Resolución
SD-10038: File system is not writable.	El proceso de SnapManager no tiene acceso de escritura al sistema de archivos.	Debe asegurarse de que el proceso de SnapManager tenga acceso de escritura al sistema de archivos. Después de corregir esto, es posible que deba tomar otra instantánea.
SMSAP-05075: Unable to create Profile. You must configure the DP/XDP relationship properly or choose the correct protection policy per the underlying relationship.	Los volúmenes subyacentes no están en una relación de SnapVault ni de SnapMirror.	Debe configurar una relación de protección de datos entre los volúmenes de origen y de destino, e inicializar la relación.
[SMSAP-05503] You have specified the same name to the profile. Specify a different name to rename the profile.	Los perfiles con nombres idénticos no pueden existir en un repositorio.	Introduzca un nombre de perfil que no esté en uso.

Mensaje de error	Explicación	Resolución
SMSAP-05505: Unable to update dataset metadata.	Es posible que el conjunto de datos se haya eliminado o no exista.	Antes de actualizar los metadatos del conjunto de datos, compruebe que el conjunto de datos existe mediante la consola de gestión de NetApp.
SMSAP-05506: You cannot update the profile since there are operation(s) running on the profile. You must wait until the operation(s) complete and then update the profile	El perfil no se puede actualizar cuando hay operaciones de backup, restauración y clonado en curso.	Actualice el perfil una vez completada la operación actual.
SMSAP-05509: Invalid archivelog primary retention duration - Specify a positive integer value.	La duración de la retención de los backups de registros de archivos no puede ser negativa.	Especifique un valor positivo para la duración de la retención de los backups de registros de archivos.
SMSAP-07463: This backup restore requires the database to be in required state. Failed to bring the database to the required state.	La base de datos no está en el estado requerido para una operación de backup.	Compruebe que la base de datos esté en estado relevante antes de crear una copia de backup. El estado de la base de datos que se va a restaurar depende del tipo de proceso de restauración que se desee realizar y del tipo de archivos que se incluirán.
SMSAP-09315: After performing repository upgrade or update operation, you might not receive the summary notification for notifications set in previous version unless you update the summary notification with the notification host details.	Los ajustes de notificación no se configuran para el repositorio después de una actualización gradual.	Después de una actualización gradual, actualice la configuración de notificación de resumen para recibir notificaciones.

Mensaje de error	Explicación	Resolución
SMSAP-02076: Label name should not contain any special characters other than underscore.	El nombre de la etiqueta contiene caracteres especiales distintos del guión bajo.	El nombre de la etiqueta debe ser único dentro del perfil. El nombre puede contener letras, números, un guión bajo (_) y un guión (-) (pero no puede comenzar con un guión). Asegúrese de que las etiquetas no contengan caracteres especiales excepto el guion bajo.
SMSAP-06308: Exception when attempting to start schedule: java.lang.NullPointerException	Se configura el nombre de dominio completo (FQDN) del host de perfil en lugar del nombre de host del sistema y no se puede resolver el FQDN del host de perfil.	Asegúrese de usar el nombre de host del sistema y no el FQDN.
Failure in ExecuteRestoreSteps: ORACLE-10003: Error executing SQL "DROP DISKGROUP;control diskgroup name; INCLUDING CONTENTS" against Oracle database +ASM1: ORA-15039: diskgroup not dropped ORA-15027: active use of diskgroup; "control diskgroup name;" precludes its dismount	La operación para restaurar un backup con archivos de control no puede soltar el grupo de discos de control. Este problema ocurre si hay archivos de control de copia de seguridad obsoletos en el grupo de discos de control.	Identifique los archivos de control de copia de seguridad obsoletos y elimínelos manualmente.
RMAN-06004: ORACLE error from recovery catalog database: ORA-01424: missing or illegal character following the escape character	La operación de creación de backup no se pudo quitar la copia de backup del catálogo cuando SnapManager está integrada con RMAN.	Compruebe si hay secuencias de comandos externas utilizadas para eliminar las copias de seguridad de RMAN. Ejecute el <b>CROSSCHECK BACKUP</b> Comando en RMAN para actualizar el repositorio de RMAN y el <b>resync catalog</b> comando para sincronizar el archivo de control de la base de datos de destino con el catálogo de recuperación.
[DEBUG]: Exception while pruning backup. java.lang.IllegalStateException: [Assertion failed] - this state invariant must be true	Se crean múltiples copias de Snapshot para un solo ID de operación.	Eliminar las copias Snapshot manualmente y utilizar scripts para eliminar las entradas del repositorio.

Mensaje de error	Explicación	Resolución
La hora y la hora del sistema que muestra SnapManager en los archivos de registro no coinciden o no están sincronizados.	Java 7 aún no admite un cambio de zona horaria.	Aplique el <code>tzupdater</code> Parche suministrado por Oracle.
DISC-00001: Unable to discover storage: The following identifier does not exist or is not of the expected type: ASM File	Los archivos de datos o de control o los redo logs se multiplexan en una base de datos ASM.	Extraiga el multiplexado de Oracle.
0001-DS-10021: Unable to set protection policy of dataset <dataset-name> to <new-protection-policy> because the protection policy is already set to <old-protection-policy>. Please use Protection Manager to change the protection policy	Una vez establecida la política de protección de un conjunto de datos, SnapManager no le permitirá cambiar la política de protección, ya que puede requerir volver a alinear las relaciones de base y provocar la pérdida de backups existentes en el almacenamiento secundario.	Actualice la política de protección mediante la consola de gestión de Protection Manager, que proporciona más opciones para migrar de una política de protección a otra.
0001-SD-10028: SnapDrive Error (id:2618 code:102) Unable to discover the device associated with "lun_path". If multipathing in use, possible multipathing configuration error. Please verify configuration and retry.	El host no puede detectar las LUN creadas en los sistemas de almacenamiento.	Asegúrese de que el protocolo de transporte está correctamente instalado y configurado. Asegúrese de que SnapDrive pueda crear y detectar una LUN en el sistema de almacenamiento.
0001-SD-10028: SnapDrive Error (id:2836 code:110) Failed to acquire dataset lock on volume "storage name":"temp_volume_name"	Se intentó restaurar con el método de almacenamiento indirecto y el volumen temporal especificado no existe en el almacenamiento primario.	Cree un volumen temporal en el almacenamiento primario. O bien, especifique el nombre correcto del volumen si ya se ha creado un volumen temporal.



Mensaje de error	Explicación	Resolución
<p>0001-SMSAP-02016: There may have been external tables in the database not backed up as part of this backup operation (since the database was not OPEN during this backup ALL_EXTERNAL_LOCATIONS could not be queried to determine whether or not external tables exist).</p>	<p>SnapManager no realiza copias de seguridad de tablas externas (por ejemplo, tablas que no están almacenadas en archivos .dbf). Este problema se produce porque la base de datos no estaba abierta durante el backup, SnapManager no puede determinar si se están utilizando tablas externas.</p>	<p>Puede haber tablas externas en la base de datos que no se incluyeron en un backup como parte de esta operación (porque la base de datos no estaba abierta durante el backup).</p>
<p>0001-SMSAP-11027: Cannot clone or mount snapshots from secondary storage because the snapshots are busy. Try cloning or mounting from an older backup.</p>	<p>Intentó crear una clonación o montar copias Snapshot a partir del almacenamiento secundario del backup protegido más reciente.</p>	<p>Clone o monte desde un backup anterior.</p>
<p>0001-SMSAP-12346: Cannot list protection policies because Protection Manager product is not installed or SnapDrive is not configured to use it. Please install Protection Manager and/or configure SnapDrive..</p>	<p>Se intentó enumerar las políticas de protección en un sistema donde SnapDrive no se configuró para usar Protection Manager.</p>	<p>Instale Protection Manager y configure SnapDrive para que use Protection Manager.</p>
<p>0001-SMSAP-13032: Cannot perform operation: Backup Delete. Root cause: 0001-SMSAP-02039: Unable to delete backup of dataset: SD-10028: SnapDrive Error (id:2406 code:102) Failed to delete backup id: "backup_id" for dataset, error(23410):Snapshot "snapshot_name" on volume "volume_name" is busy.</p>	<p>Intentó liberar o eliminar el backup protegido más reciente o un backup que contiene copias de Snapshot que son bases de referencia en una relación de mirroring.</p>	<p>Libere o elimine el backup protegido.</p>

Mensaje de error	Explicación	Resolución
<pre>0002-332 Admin error: Could not check SD.SnapShot.Clone access on volume "volume_name" for user username on Operations Manager server(s) "dfm_server". Reason: Invalid resource specified. Unable to find its ID on Operations Manager server "dfm_server"</pre>	<p>No se han configurado los privilegios de acceso adecuados y los roles.</p>	<p>Defina los privilegios de acceso o los roles para los usuarios que intentan ejecutar el comando.</p>
<pre>[WARN] FLOW-11011: Operation aborted [ERROR] FLOW-11008: Operation failed: Java heap space.</pre>	<p>Hay más archivos de registro de archivos en la base de datos que el máximo permitido.</p>	<ol style="list-style-type: none"> <li>1. Desplácese hasta el directorio de instalación de SnapManager.</li> <li>2. Abra el launch-java archivo.</li> <li>3. Aumente el valor de java -Xmx160m Parámetro Java heap space . Por ejemplo, puede modificar el valor del valor predeterminado de 160 m a 200 m. java -Xmx200m.</li> </ol>
<pre>SD-10028: SnapDrive Error (id:2868 code:102) Could not locate remote snapshot or remote qtree.</pre>	<p>SnapManager muestra los backups como protegidos aunque el trabajo de protección de Protection Manager solo se haya realizado correctamente parcialmente. Esta condición ocurre cuando la conformidad del conjunto de datos está en curso (cuando las Snapshot básicas se están reflejando).</p>	<p>Realizar un nuevo backup tras el conjunto de datos conforme a las exigencias.</p>
<pre>SMSAP-21019: The archive log pruning failed for the destination: "/mnt/destination_name/" with the reason: "ORACLE- 00101: Error executing RMAN command: [DELETE NOPROMPT ARCHIVELOG '/mnt/destination_name/']</pre>	<p>La eliminación del registro de archivo falla en uno de los destinos. En este caso, SnapManager continúa depurando los archivos de registro de archivos de los otros destinos. Si algún archivo se elimina manualmente del sistema de archivos activo, RMAN no puede hacer una copia de los archivos de registro de archivos de ese destino.</p>	<p>Conéctese a RMAN desde el host SnapManager. Ejecute RMAN <b>CROSSCHECK ARCHIVELOG ALL</b> y vuelva a realizar la operación de eliminación en los archivos log de archivos.</p>

Mensaje de error	Explicación	Resolución
<p>SMSAP-13032: Cannot perform operation: Archive log Prune. Root cause: RMAN Exception: ORACLE-00101: Error executing RMAN command.</p>	<p>Los archivos de registro de archivos se eliminan manualmente de los destinos de registro de archivos.</p>	<p>Conéctese a RMAN desde el host SnapManager. Ejecute RMAN <b>CROSSCHECK ARCHIVELOG ALL</b> y vuelva a realizar la operación de eliminación en los archivos log de archivos.</p>
<p>Unable to parse shell output: (java.util.regex.Matcher[pattern=Command complete.region=0,18 lastmatch=]) does not match (name:backup_script)</p> <p>Unable to parse shell output: (java.util.regex.Matcher[pattern=Command complete.region=0,25 lastmatch=]) does not match (description:backup script)</p> <p>Unable to parse shell output: (java.util.regex.Matcher[pattern=Command complete.region=0,9 lastmatch=]) does not match (timeout:0)</p>	<p>Las variables de entorno no se definen correctamente en los scripts previos o posteriores a las tareas.</p>	<p>Compruebe si las secuencias de comandos previas o posteriores a las tareas siguen la estructura del complemento SnapManager estándar. Para obtener información adicional sobre el uso de las variables de entorno en el script, consulte <a href="#">Operaciones en scripts de tareas</a>.</p>
<p>ORA-01450: maximum key length (6398) exceeded.</p>	<p>Cuando se realiza una actualización de SnapManager 3.2 para SAP a SnapManager 3.3 para SAP, la operación de actualización genera este mensaje de error. Este problema puede ocurrir debido a uno de los siguientes motivos:</p> <ul style="list-style-type: none"> <li>• El tamaño de bloque del tablespace en el que existe el repositorio es inferior a 8k.</li> <li>• La <code>nls_length_semantics</code> el parámetro se establece en <code>char</code>.</li> </ul>	<p>Debe asignar los valores a los siguientes parámetros:</p> <ul style="list-style-type: none"> <li>• <code>block_size=8192</code></li> <li>• <code>nls_length=byte</code></li> </ul> <p>Después de modificar los valores de los parámetros, debe reiniciar la base de datos.</p> <p>Para obtener más información, consulte el artículo 2017632 de la base de conocimientos.</p>

## Mensajes de error asociados con el proceso de copia de seguridad de la base de datos (serie 2000)

En la siguiente tabla se enumeran los errores comunes asociados al proceso de copia de seguridad de la base de datos:

Mensaje de error	Explicación	Resolución
SMSAP-02066: You cannot delete or free the archive log backup "data-logs" as the backup is associated with data backup "data-logs".	La copia de seguridad del registro de archivos se realiza junto con la copia de seguridad de los archivos de datos y se intentó eliminar el backup del registro de archivos.	Utilice la <i>-force</i> opción para eliminar o liberar el backup.
SMSAP-02067: You cannot delete, or free the archive log backup "data-logs" as the backup is associated with data backup "data-logs" and is within the assigned retention duration.	El backup de registros de archivos se asocia con el backup de la base de datos y se encuentra dentro del período de retención, y se intentó eliminar el backup de registros de archivos.	Utilice la <i>-force</i> opción para eliminar o liberar el backup.
SMSAP-07142: Archived Logs excluded due to exclusion pattern <exclusion> pattern.	Se excluyen algunos archivos de registro de archivos durante la operación de creación de perfiles o creación de copias de seguridad.	No se requiere ninguna acción.
SMSAP-07155: <count> archived log files do not exist in the active file system. These archived log files will not be included in the backup.	Los archivos de registro de archivos no existen en el sistema de archivos activo durante la operación de creación de perfiles o de creación de backup. Estos archivos de registro archivados no se incluyen en la copia de seguridad.	No se requiere ninguna acción.
SMSAP-07148: Archived log files are not available.	No se crean archivos de registro de archivos para la base de datos actual durante la operación de creación de perfiles o creación de backups.	No se requiere ninguna acción.
SMSAP-07150: Archived log files are not found.	Faltan todos los archivos de registro de archivos del sistema de archivos o se excluyen durante la operación de creación de perfiles o creación de copia de seguridad.	No se requiere ninguna acción.

Mensaje de error	Explicación	Resolución
SMSAP-13032: Cannot perform operation: Backup Create. Root cause: ORACLE-20001: Error trying to change state to OPEN for database instance dfcln1: ORACLE-20004: Expecting to be able to open the database without the RESETLOGS option, but oracle is reporting that the database needs to be opened with the RESETLOGS option. To keep from unexpectedly resetting the logs, the process will not continue. Please ensure that the database can be opened without the RESETLOGS option and try again.	Se intenta realizar una copia de seguridad de la base de datos clonada que se creó con la opción -no-resetlogs. La base de datos clonada no es una base de datos completa. Sin embargo, es posible realizar operaciones de SnapManager, como crear perfiles y backups, dividir clones, etc. con la base de datos clonada, pero se produce un error en las operaciones de SnapManager debido a que la base de datos clonada no se configura como una base de datos completa.	Recuperar la base de datos clonada o convertir la base de datos a una base de datos de Data Guard en espera.

## Errores de protección de datos

En la siguiente tabla se muestran los errores comunes asociados con la protección de datos:


Mensaje de error	Explicación	Resolución
Backup protection is requested but the database profile does not have a protection policy. Please update the protection policy in the database profile or do not use the 'protect' option when creating backups.	Se intenta crear un backup con protección en el almacenamiento secundario; sin embargo, el perfil asociado a este backup no tiene una política de protección especificada.	Edite el perfil y seleccione una política de protección. Vuelva a crear el backup.
Cannot delete profile because data protection is enabled but the Protection Manager is temporarily unavailable. Please try again later.	Se intenta eliminar un perfil que tiene la protección habilitada; sin embargo, Protection Manager no está disponible.	Asegúrese de que los backups adecuados se almacenen en el almacenamiento primario o secundario. Desactive la protección en el perfil. Cuando Protection Manager esté disponible de nuevo, vuelva al perfil y elimínelo.

Mensaje de error	Explicación	Resolución
<p>Cannot list protection policies because Protection Manager is temporarily unavailable. Please try again later.</p>	<p>Al configurar el perfil de backup, debe habilitar la protección en el backup para que el backup se almacene en el almacenamiento secundario. Sin embargo, SnapManager no puede recuperar las políticas de protección de la consola de gestión de Protection Manager.</p>	<p>Desactive la protección en el perfil temporalmente. Continúe creando un nuevo perfil o actualizando un perfil existente. Cuando Protection Manager esté disponible de nuevo, vuelva al perfil.</p>
<p>Cannot list protection policies because Protection Manager product is not installed or SnapDrive is not configured to use it. Please install Protection Manager and/or configure SnapDrive.</p>	<p>Al configurar el perfil de backup, debe habilitar la protección en el backup para que el backup se almacene en el almacenamiento secundario. Sin embargo, SnapManager no puede recuperar las políticas de protección de la Consola de gestión de Protection Manager. Protection Manager no está instalado o SnapDrive no está configurado.</p>	<p>Instale Protection Manager. Configure SnapDrive.</p> <p>Vuelva al perfil, vuelva a activar la protección y seleccione las políticas de protección disponibles en la consola de gestión de Protection Manager.</p>
<p>Cannot set protection policy because Protection Manager is temporarily unavailable. Please try again later.</p>	<p>Al configurar el perfil de backup, debe habilitar la protección en el backup para que el backup se almacene en el almacenamiento secundario. Sin embargo, SnapManager no puede recuperar las políticas de protección de la Consola de gestión de Protection Manager.</p>	<p>Desactive la protección en el perfil temporalmente. Continúe creando o actualizando el perfil. Cuando la Consola de administración de Protection Manager esté disponible, vuelva al perfil.</p>
<p>Creating new dataset &lt;dataset_name&gt; for database &lt;dbname&gt; on host &lt;host&gt;.</p>	<p>Ha intentado crear un perfil de copia de seguridad. SnapManager crea un conjunto de datos para este perfil.</p>	<p>No es necesario realizar ninguna acción.</p>
<p>Data protection is not available because Protection Manager is not installed.</p>	<p>Al configurar el perfil de backup, se intentó habilitar la protección en el backup para que el backup se almacenara en el almacenamiento secundario. Sin embargo, SnapManager no puede acceder a las políticas de protección desde la consola de gestión de Protection Manager. Protection Manager no está instalado.</p>	<p>Instale Protection Manager.</p>

Mensaje de error	Explicación	Resolución
Deleted dataset <dataset_name> for this database.	Ha eliminado un perfil. SnapManager eliminará el conjunto de datos asociado.	No es necesario realizar ninguna acción.
Deleting profile with protection enabled and Protection Manager is no longer configured. Deleting profile from SnapManager but not cleaning up dataset in Protection Manager.	Se intentó eliminar un perfil que tiene la protección habilitada; sin embargo, Protection Manager ya no está instalado o ya no está configurado o ha caducado. SnapManager eliminará el perfil, pero no el conjunto de datos del perfil de la consola de gestión de Protection Manager.	Vuelva a instalar o vuelva a configurar Protection Manager. Vuelva al perfil y elimínelo.
Invalid retention class. Use "smsap help backup" to see a list of available retention classes.	Al configurar la directiva de retención, intentó utilizar una clase de retención no válida.	Cree una lista de clases de retención válidas introduciendo este comando: <b>smsap help backup</b>  Actualice la directiva de retención con una de las clases disponibles.
Specified protection policy is not available. Use "smsap protection-policy list" to see a list of available protection policies.	Al configurar el perfil, debe habilitar la protección e introducir una política de protección que no esté disponible.	Identifique las políticas de protección disponibles con el siguiente comando: <b>smsap protection-policy list</b>
Using existing dataset <dataset_name> for database <dbname> on host <host> since the dataset already existed.	Intentó crear un perfil; sin embargo, el conjunto de datos para el mismo perfil de base de datos ya existe.	Compruebe las opciones del perfil existente y asegúrese de que coinciden con lo que necesita en el nuevo perfil.
Using existing dataset <dataset_name> for RAC database <dbname> since profile <profile_name> for the same RAC database already exists for instance <SID> on host <hostname>.	Intentó crear un perfil para una base de datos RAC; sin embargo, el conjunto de datos para el mismo perfil de base de datos RAC ya existe.	Compruebe las opciones del perfil existente y asegúrese de que coinciden con lo que necesita en el nuevo perfil.

Mensaje de error	Explicación	Resolución
<p>The dataset &lt;dataset_name&gt; with protection policy &lt;existing_policy_name&gt; already exists for this database. You have specified protection policy &lt;new_policy_name&gt;. The dataset's protection policy will be changed to &lt;new_policy_name&gt;. You can change the protection policy by updating the profile.</p>	<p>Ha intentado crear un perfil con la protección activada y una política de protección seleccionada. Sin embargo, el conjunto de datos para el mismo perfil de base de datos ya existe, pero tiene una política de protección diferente. SnapManager usará la política recién especificada para el conjunto de datos existente.</p>	<p>Revise esta política de protección y determine si esta es la política que desea usar para el conjunto de datos. Si no es así, edite el perfil y cambie la directiva.</p>
<p>Protection Manager deletes the local backups created by SnapManager for SAP</p>	<p>La consola de gestión de Protection Manager elimina o libera los backups locales creados por SnapManager de acuerdo con la política de retención definida en Protection Manager. La clase de retención establecida para los backups locales no se considera mientras se eliminan o liberan los backups locales. cuando los backups locales se transfieren a un sistema de almacenamiento secundario, no se considera la clase de retención establecida para los backups locales en el sistema de almacenamiento primario. La clase de retención especificada en el programa de transferencia se asigna a la copia de seguridad remota.</p>	<p>Ejecute el <code>dfpm dataset fix_smsap</code> Comando del servidor de Protection Manager cada vez que se crea un nuevo conjunto de datos. ahora los backups no se eliminan de acuerdo con la normativa de retención definida en la consola de gestión de Protection Manager.</p>



Mensaje de error	Explicación	Resolución
<p>You have selected to disable protection for this profile. This could potentially delete the associated dataset in Protection Manager and destroy the replication relationships created for that dataset. You will also not be able to perform SnapManager operations such as restoring or cloning the secondary or tertiary backups for this profile. Do you wish to continue (Y/N)?</p>	<p>Intentó deshabilitar la protección para un perfil protegido al actualizar el perfil desde la interfaz gráfica de usuario o la interfaz de línea de comandos de SnapManager. Puede desactivar la protección para el perfil mediante <code>-noprotect</code> Opción de la CLI de SnapManager o desactive la casilla de verificación <b>Directiva de protección de Protection Manager</b> de la ventana Propiedades de directivas de la GUI de SnapManager. Cuando se deshabilita la protección para el perfil, SnapManager para SAP elimina el conjunto de datos de la consola de gestión de Protection Manager, que cancela el registro de todas las copias de backup secundarias y terciarias asociadas con ese conjunto de datos.</p> <p>Tras eliminar un conjunto de datos, todas las copias de backup secundarias y terciarias se huérfanas. Ni Protection Manager ni SnapManager para SAP tienen la capacidad de acceder a esas copias de backup. Ya no es posible restaurar las copias de backup mediante SnapManager para SAP.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Se muestra el mismo mensaje de advertencia incluso cuando el perfil no está protegido.</p> </div>	<p>Este es un problema conocido en SnapManager para SAP y el comportamiento esperado dentro de Protection Manager al destruir un conjunto de datos. No existe ninguna solución alternativa. Los backups huérfanos deben gestionarse manualmente.</p>

## Mensajes de error asociados con el proceso de restauración (serie 3000)

En la siguiente tabla se muestran los errores comunes asociados con el proceso de restauración:

<b>Mensaje de error</b>	<b>Explicación</b>	<b>Resolución</b>
<p>SMSAP-03031:Restore specification is required to restore backup &lt;variable&gt; because the storage resources for the backup has already been freed.</p>	<p>Intentó restaurar una copia de seguridad que tiene liberados sus recursos de almacenamiento sin especificar una especificación de restauración.</p>	<p>Especifique una especificación de restauración.</p>
<p>SMSAP-03032:Restore specification must contain mappings for the files to restore because the storage resources for the backup has already been freed. The files that need mappings are: &lt;variable&gt; from Snapshots: &lt;variable&gt;</p>	<p>Intentó restaurar una copia de seguridad que tiene liberados sus recursos de almacenamiento junto con una especificación de restauración que no contiene la asignación de todos los archivos que se van a restaurar.</p>	<p>Corrija el archivo de especificación de restauración de modo que las asignaciones coincidan con los archivos que se van a restaurar.</p>

Mensaje de error	Explicación	Resolución
<p>ORACLE-30028: Unable to dump log file &lt;filename&gt;. The file may be missing/inaccessible/corrupted. This log file will not be used for recovery.</p>	<p>Los archivos redo log en línea o los archivos archive log no se pueden utilizar para la recuperación.este error se produce debido a los siguientes motivos:</p> <ul style="list-style-type: none"> <li>• Los archivos redo log en línea o los archivos archive log mencionados en el mensaje de error no tienen números de cambio suficientes para solicitar la recuperación. Esto ocurre cuando la base de datos está en línea sin ninguna transacción. Los archivos redo log o archive log no tienen ningún número de cambio válido que se pueda aplicar para la recuperación.</li> <li>• El archivo redo log en línea o el archivo archive log mencionado en el mensaje de error no tiene suficientes privilegios de acceso para Oracle.</li> <li>• El archivo redo log en línea o el archivo de registro archivado mencionado en el mensaje de error están dañados y Oracle no puede leerlos.</li> <li>• El archivo redo log en línea o el archivo de registro archivado mencionado en el mensaje de error no se encuentra en la ruta de acceso mencionada.</li> </ul>	<p>Si el archivo mencionado en el mensaje de error es un archivo de registro archivado y si ha proporcionado manualmente para la recuperación, asegúrese de que el archivo tiene permisos de acceso completo a Oracle.incluso si el archivo tiene permisos completos, y el mensaje continúa, el archivo de registro de archivo no tiene ningún número de cambio que se aplicará para la recuperación, y este mensaje puede ignorarse.</p>
<p>SMSAP-03038: Cannot restore from secondary because the storage resources still exist on primary. Please restore from primary instead.</p>	<p>Intentó restaurar desde el almacenamiento secundario, pero existen copias Snapshot en el almacenamiento primario.</p>	<p>Restaura siempre desde el principal si el backup no se ha liberado.</p>

Mensaje de error	Explicación	Resolución
SMSAP-03054: Mounting backup archbkpl to feed archivelogs. DS-10001: Connecting mountpoints. [ERROR] FLOW-11019: Failure in ExecuteConnectionSteps: SD-10028: SnapDrive Error (id:2618 code:305). The following files could not be deleted. The corresponding volumes might be read-only. Retry the command with older snapshots.[ERROR] FLOW-11010: Operation transitioning to abort due to prior failure.	Durante la recuperación, SnapManager intenta montar el backup más reciente del sistema secundario para alimentar los archivos de registro de archivos desde el secundario. Sin embargo, si hay otros backups, la recuperación puede tener éxito. Sin embargo, si no hay otros backups, es posible que se produzca un error en la recuperación.	No elimine los backups más recientes del almacenamiento primario, por lo que SnapManager puede utilizar el backup principal para la recuperación.

## Mensajes de error asociados con el proceso de clonación (serie 4000)

En la siguiente tabla se muestran los errores comunes asociados con el proceso de clonación:

Mensaje de error	Explicación	Resolución
SMSAP-04133: Dump destination must not exist	Se está utilizando SnapManager para crear nuevos clones; sin embargo, los destinos de volcado que usará el nuevo clon ya existen. SnapManager no puede crear un clon si existen destinos de volcado.	Quite o cambie el nombre de los destinos de volcado antiguos antes de crear un clon.
SMSAP-04908: Not a FlexClone.	El clon es un clon LUN. Esto se aplica tanto a Data ONTAP 8.1 7-Mode como a Clustered Data ONTAP.	SnapManager admite la división de clones únicamente en la tecnología FlexClone.
SMSAP-04904: No clone split operation running with <i>split-idsplit_id</i>	El ID de la operación no es válido o no hay ninguna operación de división de clones en curso.	Proporcione un ID de división o una etiqueta de división válidos para el estado de división de clones, resultados y operaciones de detención.
SMSAP-04906: Stop clone split operation failed with <i>split-idsplit_id</i>	Se ha completado la operación de división.	Compruebe si el proceso de división está en curso utilizando <b>clone split-status 0</b> . <b>clone split-result</b> comando.

Mensaje de error	Explicación	Resolución
SMSAP-13032:Cannot perform operation: Clone Create. Root cause: ORACLE-00001: Error executing SQL: [ALTER DATABASE OPEN RESETLOGS;]. The command returned: ORA-38856: cannot mark instance UNNAMED_INSTANCE_2 (redo thread 2) as enabled.	Se produce un error en la creación del clon cuando se crea desde la base de datos en espera con la siguiente configuración: <ul style="list-style-type: none"> <li>• La base de datos primaria es una configuración de RAC y la base de datos en espera es independiente.</li> <li>• El modo de espera se crea mediante RMAN para realizar una copia de seguridad de los archivos de datos.</li> </ul>	Añada el <code>_no_recovery_through_reset_logs=TRUE</code> parámetro en el archivo de especificación del clon antes de crear el clon. Consulte la documentación de Oracle (ID 334899.1) para obtener información adicional. Asegúrese de tener el nombre de usuario y la contraseña de Oracle metalink.
[INFO] Operation failed. Syntax errors in clone specification: [error: cvc-complex-type.2.4c: Expected elements 'value@http://www.example.com default@http://www.example.com' before the end of the content in element parameter@http://www.example.com]	No ha especificado un valor para un parámetro en el archivo de especificación del clon.	Debe proporcionar un valor para el parámetro o eliminar ese parámetro si no es necesario en el archivo de especificación del clon.

## Mensajes de error asociados con el proceso de gestión de perfiles (serie 5000)

En la siguiente tabla se muestran los errores comunes asociados con el proceso de clonación:

Mensaje de error	Explicación	Resolución
SMSAP-20600: Profile "profile1" not found in repository "repo_name". Please run "profile sync" to update your profile-to-repository mappings.	La operación de volcado no se puede realizar cuando se produce un error al crear el perfil.	Uso <code>smsapsystem dump</code> .

## Mensajes de error asociados con la liberación de recursos de backup (series de backups 6000)

En la siguiente tabla se muestran los errores comunes asociados con las tareas de backup:

Mensaje de error	Explicación	Resolución
SMSAP-06030: Cannot remove backup because it is in use: <variable>	Se intentó realizar la operación de backup libre con comandos, cuando el backup se monta o se Marca que se retiene de forma ilimitada.	Desmonte el backup o cambie la política de retención ilimitada. Si hay clones, elimínelos.
SMSAP-06045: Cannot free backup <variable> because the storage resources for the backup have already been freed	Se intentó realizar la operación de backup libre con comandos, cuando ya se ha liberado el backup.	No se puede liberar la copia de seguridad si ya se ha liberado.
SMSAP-06047: Only successful backups can be freed. The status of backup <ID> is <status>.	Se intentó realizar la operación de backup libre con comandos, cuando el estado del backup no es correcto.	Vuelva a intentarlo después de realizar el backup correctamente.
SMSAP-13082: Cannot perform operation <variable> on backup <ID> because the storage resources for the backup have been freed.	Con comandos, se intentó montar un backup con los recursos de almacenamiento liberados.	No se pueden montar, clonar, verificar ni ejecutar restauraciones backint en un backup que tenga liberados los recursos de almacenamiento.

## Errores de interfaz de almacenamiento virtual (serie 8000 de interfaz de almacenamiento virtual)

La siguiente tabla muestra los errores comunes asociados con las tareas de interfaz de almacenamiento virtual:

Mensaje de error	Explicación	Resolución
SMSAP-08017 Error discovering storage for /.	SnapManager intentó localizar recursos de almacenamiento, pero encontró archivos de datos, archivos de control o registros en el root/ directorio. Estos archivos deben residir en un subdirectorio. El sistema de archivos raíz puede ser un disco duro en su equipo local. SnapDrive no puede hacer copias snapshot en esta ubicación y SnapManager no puede realizar operaciones con estos archivos.	<p>Compruebe si los archivos de datos, los archivos de control o los registros de recuperación están en la root directorio. Si es así, muévelos a sus ubicaciones correctas o vuelva a crear archivos de control o redo logs en sus ubicaciones correctas. El punto de montaje básico es siempre</p> <ul style="list-style-type: none"> <li>• /oracle/&lt;SID&gt; En entornos basados en UNIX</li> <li>• [drive:]\oracle\&lt;SID&gt; En entornos basados en Windows</li> </ul> <p>SAP utiliza cuatro grupos de redo log con dos miembros:</p> <ul style="list-style-type: none"> <li>• Un miembro se almacena en origlog{A}</li> </ul>

## Mensajes de error asociados con el proceso de actualización gradual (serie 9000)

En la siguiente tabla se muestran los errores comunes asociados con el proceso de actualización gradual:

Mensaje de error	Explicación	Resolución
SMSAP-09234:Following hosts does not exist in the old repository. <hostnames>.	Intentó realizar una actualización gradual de un host, que no existe en la versión de repositorio anterior.	Compruebe si el host existe en el repositorio anterior mediante el repository show-repository Comando desde la versión anterior de la interfaz de línea de comandos de SnapManager.
SMSAP-09255:Following hosts does not exist in the new repository. <hostnames>.	Intentó realizar la reversión de un host, que no existe en la versión del nuevo repositorio.	Compruebe si el host existe en el nuevo repositorio mediante el repository show-repository Comando desde la versión posterior de la CLI de SnapManager.
SMSAP-09256:Rollback not supported, since there exists new profiles <profilenames>.for the specified hosts <hostnames>.	Intentó revertir un host que contiene nuevos perfiles existentes en el repositorio. Sin embargo, estos perfiles no existían en el host de la versión anterior de SnapManager.	Elimine nuevos perfiles en la versión posterior o actualizada de SnapManager antes de la reversión.

<b>Mensaje de error</b>	<b>Explicación</b>	<b>Resolución</b>
SMSAP-09257:Rollback not supported, since the backups <backupid> are mounted in the new hosts.	Intentó revertir una versión posterior del host SnapManager que tiene backups montados. Estos backups no se montan en la versión anterior del host SnapManager.	Desmonte los backups en la versión posterior del host SnapManager y, a continuación, realice la reversión.
SMSAP-09258:Rollback not supported, since the backups <backupid> are unmounted in the new hosts.	Ha intentado revertir una versión posterior del host SnapManager que tiene backups que se están desdesmontan.	Monte los backups en la versión posterior del host SnapManager y, a continuación, ejecute la reversión.
SMSAP-09298:Cannot update this repository since it already has other hosts in the higher version. Please perform rollingupgrade for all hosts instead.	Realizó una actualización gradual en un solo host y, después, actualizó el repositorio para ese host.	Realice una actualización gradual en todos los hosts.
SMSAP-09297: Error occurred while enabling constraints. The repository might be in inconsistent state. It is recommended to restore the backup of repository you have taken before the current operation.	Se intentó realizar una operación de reversión o actualización sucesiva si la base de datos del repositorio queda en estado incoherente.	Restaurar el repositorio del que se ha hecho backup anteriormente.

## Ejecución de operaciones (serie 12,000)

En la siguiente tabla se muestran los errores comunes asociados a las operaciones:

<b>Mensaje de error</b>	<b>Explicación</b>	<b>Resolución</b>
SMSAP-12347 [ERROR]: SnapManager server not running on host <host> and port <port>. Please run this command on a host running the SnapManager server.	Al configurar el perfil, debe introducir información sobre el host y el puerto. Sin embargo, SnapManager no puede realizar estas operaciones porque el servidor SnapManager no está en ejecución en el host y el puerto especificados.	Introduzca el comando en un host que ejecuta el servidor SnapManager. Puede comprobar el puerto con el <code>lsnrctl status</code> y vea el puerto en el que se ejecuta la base de datos. Si es necesario, cambie el puerto del comando backup.



## Ejecución de componentes de proceso (serie 13,000)

En la siguiente tabla se muestran los errores comunes asociados con el componente de proceso de SnapManager:

Mensaje de error	Explicación	Resolución
SMSAP-13083: Snapname pattern with value "x" contains characters other than letters, numbers, underscore, dash, and curly braces.	Al crear un perfil, ha personalizado el patrón de Snapname; sin embargo, ha incluido caracteres especiales que no están permitidos.	Quite caracteres especiales que no sean letras, números, guion bajo, guion y corchetes.
SMSAP-13084: Snapname pattern with value "x" does not contain the same number of left and right braces.	Al crear un perfil, ha personalizado el patrón de Snapname; sin embargo, las llaves izquierda y derecha no coinciden.	Introduzca los corchetes de apertura y cierre coincidentes en el patrón de Snapname.
SMSAP-13085: Snapname pattern with value "x" contains an invalid variable name of "y".	Al crear un perfil, ha personalizado el patrón de Snapname; sin embargo, ha incluido una variable que no está permitida.	Elimine la variable ofensor. Para ver una lista de variables aceptables, consulte <a href="#">Nomenclatura de copias Snapshot</a> .
SMSAP-13086 Snapname pattern with value "x" must contain variable "smid".	Al crear un perfil, ha personalizado el patrón de Snapname; sin embargo, ha omitido el requerido <i>smid</i> variable.	Inserte el necesario <i>smid</i> variable.
SMSAP-13902: Clone Split Start failed.	Puede haber varios motivos para este error: <ul style="list-style-type: none"> <li>• No hay espacio en el volumen.</li> <li>• SnapDrive no está en ejecución.</li> <li>• El clon puede ser un clon de la LUN.</li> <li>• El volumen de FlexVol tiene copias snapshot restringidas.</li> </ul>	Compruebe el espacio disponible en el volumen mediante el <b>clone split-estimate</b> comando. Confirmar que el volumen FlexVol no tiene copias snapshot restringidas.
SMSAP-13904: Clone Split Result failed.	Esto podría deberse a un fallo en el SnapDrive o el sistema de almacenamiento.	Intente trabajar con un clon nuevo.

Mensaje de error	Explicación	Resolución
SMSAP-13906: Split operation already running for clone label <i>clone-label</i> or ID <i>clone-id</i> .	Intenta dividir un clon que ya está dividido.	El clon ya está dividido y se eliminarán los metadatos relacionados con los clones.
SMSAP-13907: Split operation already running for clone label <i>clone-label</i> or ID <i>clone-id</i> .	Está intentando dividir un clon que está en proceso de división.	Debe esperar hasta que finalice la operación de división.

## Mensajes de error asociados con utilidades de SnapManager (serie 14,000)

En la siguiente tabla se muestran los errores comunes asociados con las utilidades de SnapManager:

Mensaje de error	Explicación	Resolución
SMSAP-14501: Mail ID cannot be blank.	No ha introducido la dirección de correo electrónico.	Introduzca una dirección de correo electrónico válida.
SMSAP-14502: Mail subject cannot be blank.	No ha introducido el asunto del correo electrónico.	Introduzca el asunto del correo electrónico que corresponda.
SMSAP-14506: Mail server field cannot be blank.	No se introdujo el nombre de host ni la dirección IP del servidor de correo electrónico.	Introduzca el nombre de host o la dirección IP del servidor de correo válido.
SMSAP-14507: Mail Port field cannot be blank.	No ha introducido el número de puerto de correo electrónico.	Introduzca el número de puerto del servidor de correo electrónico.
SMSAP-14508: From Mail ID cannot be blank.	No ha introducido la dirección de correo electrónico del remitente.	Introduzca una dirección de correo electrónico del remitente válida.
SMSAP-14509: Username cannot be blank.	Habilitó la autenticación y no proporcionó el nombre de usuario.	Introduzca el nombre de usuario de autenticación por correo electrónico.
SMSAP-14510: Password cannot be blank. Please enter the password.	Habilitó la autenticación y no proporcionó la contraseña.	Introduzca la contraseña de autenticación por correo electrónico.
SMSAP-14550: Email status <success/failure>.	El número de puerto, el servidor de correo o la dirección de correo electrónico del receptor no son válidos.	Proporcione los valores adecuados durante la configuración del correo electrónico.

<b>Mensaje de error</b>	<b>Explicación</b>	<b>Resolución</b>
SMSAP-14559: Sending email notification failed: <error>.	Esto podría deberse a un número de puerto no válido, a un servidor de correo no válido o a una dirección de correo del destinatario no válida.	Proporcione los valores adecuados durante la configuración del correo electrónico.
SMSAP-14560: Notification failed: Notification configuration is not available.	Error en el envío de notificaciones porque la configuración de notificación no está disponible.	Agregar configuración de notificación.
SMSAP-14565: Invalid time format. Please enter time format in HH:mm.	Introdujo la hora en un formato incorrecto.	Introduzca la hora en el formato: hh:mm.
SMSAP-14566: Invalid date value. Valid date range is 1-31.	La fecha configurada es incorrecta.	La fecha debe estar entre 1 y 31.
SMSAP-14567: Invalid day value. Valid day range is 1-7.	El día configurado es incorrecto.	Introduzca el intervalo de días del 1 al 7.
SMSAP-14569: Server failed to start Summary Notification schedule.	El servidor SnapManager se cerró por motivos desconocidos.	Inicie el servidor SnapManager.
SMSAP-14570: Summary Notification not available.	No ha configurado la notificación de resumen.	Configure la notificación de resumen.
SMSAP-14571: Both profile and summary notification cannot be enable.	Ha seleccionado las opciones de notificación de perfil y resumen.	Habilite la notificación de perfil o la notificación de resumen.
SMSAP-14572: Provide success or failure option for notification.	No ha habilitado las opciones de éxito o fallo.	Debe seleccionar Success o Failure Option o both.

## **Mensajes de error comunes de SnapDrive para UNIX**

En la siguiente tabla se muestran los errores comunes relacionados con SnapDrive para UNIX:

Mensaje de error	Explicación
0001-136 Admin error: Unable to log on to filer: <filer> Please set user name and/or password for <filer>	Error de configuración inicial
0001-382 Admin error: Multipathing rescan failed	Error de detección de LUN
0001-462 Admin error: Failed to unconfigure multipathing for <LUN>: spd5: cannot stop device. Device busy.	Error de detección de LUN
0001-476 Admin error: Unable to discover the device associated with...	Error de detección de LUN
0001-680 Admin error: Host OS requires an update to internal data to allow LUN creation or connection. Use 'snapdrive config prepare luns' or update this information manually...	Error de detección de LUN
0001-710 Admin error: OS refresh of LUN failed..	Error de detección de LUN
0001-817 Admin error: Failed to create volume clone... : FlexClone not licensed	Error de configuración inicial
0001-817 Admin error: Failed to create volume clone... : Request failed as space cannot be guaranteed for the clone.	Problema de espacio
0001-878 Admin error: HBA assistant not found. Commands involving LUNs should fail.	Error de detección de LUN
SMSAP-12111: Error executing snapdrive command "<snapdrive command>": <snapdrive error>	Error genérico de SnapDrive para UNIX

## Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.