



Información general del producto

SnapManager for SAP

NetApp
April 19, 2024

This PDF was generated from <https://docs.netapp.com/es-es/snapmanager-sap/unix-administration/concept-create-backups-using-snapshot-copies.html> on April 19, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Información general del producto 1
 - Aspectos destacados de SnapManager 1
 - Crear backups usando copias de Snapshot 2
 - Por qué debe prune los archivos de registro de archivos 2
 - Consolidación de registros de archivo 2
 - Restauración total o parcial de bases de datos 3
 - Comprobar el estado del backup 3
 - Clones de backups de bases de datos 3
 - Realizar un seguimiento de los detalles y generar informes 4
 - Qué repositorios son 4
 - Qué perfiles son 5
 - Qué son los estados de operación de SnapManager 6
 - Cómo mantiene SnapManager la seguridad 8
 - Acceder a la ayuda en línea e imprimirla 9
 - Diseños generales de bases de datos y configuraciones de almacenamiento recomendados 9
 - Limitaciones al trabajar con SnapManager 14

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.

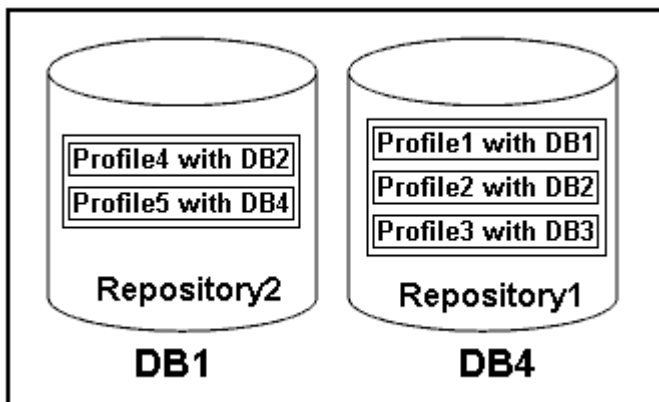
Qué perfiles son

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 Programación 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 1487 562">Error en la operación. SnapManager ha ejecutado automáticamente el proceso de anulación y ha limpiado la operación.</p> <div data-bbox="435 590 1487 716" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p data-bbox="553 604 1482 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.

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.