Información general del producto

SnapManager Oracle

NetApp
October 04, 2023

Tabla de contenidos

Información general del producto

SnapManager para Oracle automatiza y simplifica los procesos manuales asociados a operaciones como el backup, la recuperación y el clonado de bases de datos de Oracle, 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 se integra con tecnologías nativas de Oracle como Real Application Clusters (Oracle RAC), Automatic Storage Management (ASM) y Direct NFS en protocolos FC, iSCSI y NFS. De manera opcional, los backups creados mediante SnapManager se pueden catalogar con Oracle RMAN para conservar la información de backups; estos backups se pueden utilizar posteriormente en operaciones de restauración a nivel de bloque o recuperación a un momento específico de espacio de tabla.

Aspectos destacados de SnapManager

SnapManager integra perfectamente con las bases de datos Oracle en el host UNIX y es gracias a las tecnologías de copias Snapshot, SnapRestore y FlexClone de NetApp 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

  Es posible realizar un backup 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 sistemas de almacenamiento principales o secundarios

  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 Oracle 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 flash, debe asegurarse de especificar también la ubicación del registro de archivos en el parámetro archive_log_dest.

Consolidación de registros de archivo

SnapManager (3.2 o posterior) para Oracle consolida los backups de registros de archivos a fin de mantener una cantidad mínima de backups para los archivos de registro de archivos. SnapManager para Oracle 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.

Los administradores de bases de datos pueden usar SnapManager para restaurar la base de datos y usar otra herramienta para recuperar la información. Los administradores de bases de datos no tienen que usar SnapManager para ambas operaciones.

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

"Data ONTAP documentation: mysupport.netapp.com/documentation/productsatoz/index.html"

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, se registra el siguiente mensaje de error en el archivo sm_gui.log: [WARN]: SMO-01106: Se ha producido un error al consultar el repositorio: No se han producido más datos para leer desde el 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.

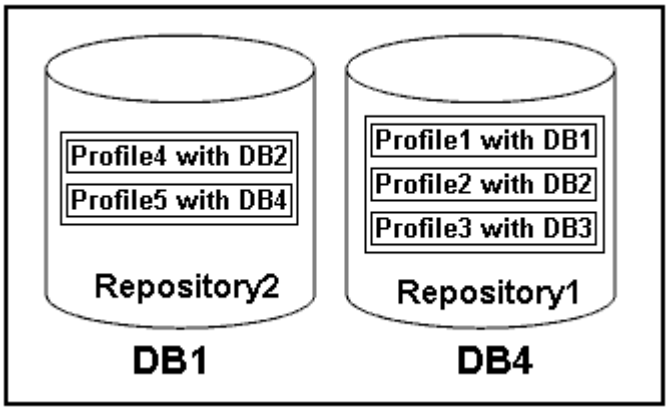
Qué perfiles son

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.

Información relacionada

Gestionar perfiles para backups eficientes

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.
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	Error en la operación. SnapManager ha ejecutado automáticamente el proceso de anulación y ha limpiado la operación. **Nota:** puede 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.

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.
- Se configuró una base de datos de Automatic Storage Management (ASM), pero no se está ejecutando la instancia de ASM.
- 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 SnapManager, desplácese a $ORACLE_HOME en el equipo de

destino y elimine el archivo sm_lock_TargetDBName. Después de eliminar el archivo, debe reiniciar SnapManager para Oracle Server.

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 debería añadirse a las credenciales de usuario mediante el comando smo credential set -host.
- 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 de sistema operativo, puede guardar los datos en la caché de credenciales de usuario de SnapManager mediante el comando smo credential set -host.

> El comando smo credential set -host recuerda las credenciales cuando la propiedad host.credentials.persists del archivo smo.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 verificación del sistema en Host1.

Acceso e impresión de la Ayuda en línea

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.

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.
- Incluyen el identificador del sistema de la base de datos en el archivo oratab.

  Incluir una entrada en el archivo oratab de cada base de datos que se gestionará. SnapManager utiliza el archivo oratab para determinar qué directorio raíz de Oracle usar.

- Para registrar backups de SnapManager en Oracle RMAN, debe crear perfiles habilitados para RMAN.

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:

- Varias bases de datos no pueden compartir el mismo grupo de discos de Automatic Storage Management (ASM).

- 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.

Definir el inicio de la base de datos con el archivo oratab

SnapManager utiliza el archivo oratab durante las operaciones para determinar el directorio inicial de la base de datos de Oracle. Una entrada de la base de datos de Oracle debe estar en el archivo oratab para que SnapManager funcione correctamente. El archivo oratab se crea durante la instalación del software de Oracle.

El archivo oratab 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	/etc/oratab
Solaris	/var/opt/oracle/oratab
IBM AIX	/etc/oratab

El archivo oratab de muestra 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)
smoclone:/u01/app/11.2.0/oracle:N
```

Después de instalar Oracle, debe asegurarse de que el archivo oratab resida en la ubicación especificada en la tabla anterior. Si el archivo oratab no reside en la ubicación correcta por cada sistema operativo, debe comunicarse 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 o en un entorno de ASM, se debe instalar y ejecutar el servidor SnapManager 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.

Requisitos para usar bases de datos de ASM con SnapManager

Debe conocer los requisitos para usar las bases de datos de gestión automática de almacenamiento (ASM) con SnapManager. Conocer estos requisitos puede ayudarle a evitar problemas con ASMLib, particiones y especificaciones de clonación, entre otras cosas.

- SnapManager (3.0.3 o posterior) utiliza el nuevo privilegio sysasm disponible con Oracle 11gR2 en lugar del privilegio sysdba para administrar una instancia de Oracle ASM.

  Si utiliza el privilegio sysdba para ejecutar comandos administrativos en la instancia de ASM, se muestra un mensaje de error. La base de datos utiliza el privilegio sysdba para acceder a los grupos de discos. Si se conecta a la instancia de ASM mediante el privilegio sysasm, tendrá acceso completo a todos los grupos de discos y funciones de administración de Oracle ASM disponibles.

  > Si utiliza Oracle 10gR2 y 11gR1, debe continuar utilizando el privilegio sysdba.

- SnapManager (3.0.3 o posterior) admite la copia de seguridad de bases de datos que se almacenan directamente en grupos de discos ASM cuando el grupo de discos también contiene un volumen de sistema automático de archivos de clúster (ACFS).

  Estos archivos están protegidos indirectamente por SnapManager y pueden restaurarse con el contenido restante de un grupo de discos de ASM, pero SnapManager (3.0.3 o posterior) no admite ACFS.

  > ACFS es una tecnología de gestión del almacenamiento del sistema de archivos escalable y multiplataforma disponible con Oracle 11gR2. ACFS amplía la funcionalidad ASM para admitir archivos de clientes que se mantienen fuera de la base de datos Oracle.

- SnapManager (3.0.3 o posterior) admite la copia de seguridad de archivos almacenados en grupos de discos ASM cuando el grupo de discos también contiene archivos de registro de cluster Oracle (OCR) o archivos de disco de votación; sin embargo, las operaciones de restauración requieren un método más lento, basado en host o de restauración instantánea de archivo parcial (PFSR).

  Es mejor tener discos OCR y de votación en grupos de discos que no contengan archivos de base de datos.

- Cada disco utilizado para ASM debe contener sólo una partición.
- La partición que aloja los datos de ASM debe estar correctamente alineada para evitar problemas graves de rendimiento.

Esto implica que la LUN debe ser del tipo correcto y la partición debe tener un desplazamiento que es un múltiplo de 4K bytes.

> Para obtener más información sobre cómo crear particiones alineadas con 4K, consulte el artículo 1010717 de Knowledge base.

- No se especifica la configuración de ASM como parte de la especificación del clon.

  Debe quitar manualmente la información de configuración de ASM en las especificaciones de clonado que se crearon con SnapManager 2.1 antes de actualizar el host a SnapManager (2.2 o posterior).

- SnapManager 3.1, 3.1p1 y 3.2 o posterior admiten ASMLib 2.1.4.
- SnapManager 3.1p4 o posterior admiten ASMLib 2.1.4, 2.1.7 y 2.1.8.

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
Red Hat Enterprise Linux 5x o 5 veces Oracle Enterprise Linux	Sí	No	No	ext3*
Red Hat Enterprise Linux 6xor 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***
Red Hat Enterprise Linux 5x o posterioresor Oracle Enterprise Linux 5 o posterior	Sí	No	Sí	ASM con ASMLib**

De NetApp	Partición única	Partición múltiple	Dispositivos sin partición	Sistema de archivos o dispositivos RAW
SUSE Linux Enterprise Server 10 SP4or SUSE Linux Enterprise Server 11	Sí	No	Sí	ASM con ASMLib**
SUSE Linux Enterprise Server 10 SP4 o posteror SUSE Linux Enterprise Server 11	Sí	No	No	ASM sin ASMLib**

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

Compatibilidad con ASMLib

SnapManager admite diferentes versiones de ASMLib, aunque hay varios factores que debe tener en cuenta al utilizar SnapManager con ASMLib.

SnapManager admite ASMLib 2.1.4, 2.1.7 y 2.1.8. Todas las operaciones de SnapManager se pueden realizar con ASMLib 2.1.4, 2.1.7 y 2.1.8.

Si actualizó desde ASMLib 2.1.4 a ASM 2.1.7, es posible usar los mismos perfiles y backups creados con ASMLib 2.1.4 para restaurar los backups y crear los clones.

Debe tener en cuenta lo siguiente al utilizar SnapManager con ASMLib:

- SnapManager 3.1 no admite ASMLib 2.1.7.

  SnapManager 3.1p4 o posterior admiten ASMLib 2.1.4, 2.1.7 y 2.1.8.

- Después de realizar una actualización sucesiva desde SnapManager 3.1 a 3.2, las copias de seguridad creadas mediante ASMLib 2.1.7 funcionan únicamente si el repositorio se revierte a SnapManager 3.1 y ASMLib 2.1.7 se degrada a ASMLib 2.1.4.
- Después de realizar una actualización sucesiva desde SnapManager 3.1 a 3.2, las copias de seguridad creadas con ASMLib 2.1.7 no funcionan si el repositorio se revierte a SnapManager 3.1 con ASMLib 2.1.7.

  La reversión se realiza correctamente, pero no se pueden utilizar los perfiles y las copias de seguridad.

Compatibilidad con bases de datos de ASM sin ASMLib

SnapManager admite ASM sin ASMLib, de forma predeterminada. El requisito básico es que se deban particionar los dispositivos que se usan para los grupos de discos ASM.

Cuando ASMLib no está instalado, los permisos de dispositivo relacionados con los grupos de discos de ASM cambian a root:disk cuando se realizan las siguientes operaciones:

- Reinicie el host
- Restaure una base de datos desde el almacenamiento principal mediante SnapRestore (VBSR) basada en volúmenes.
- Restaurar una base de datos desde el almacenamiento secundario

Puede establecer los permisos de dispositivo adecuados asignando true a la variable de configuración oracleasm.support.without.asmlib en smo.conf. Los dispositivos relacionados con los grupos de discos ASM se agregan o eliminan del archivo initasmdisks cada vez que se agregan o eliminan nuevos dispositivos del host. El archivo initasmdisks está ubicado en /etc/initasmdisks.

Por ejemplo, si establece oracleasm.support.without.asmlib=true y, a continuación, realiza un montaje de copia de seguridad, se agregan nuevos dispositivos a initasmdisks. Cuando se reinicia el host, los scripts de inicio mantienen los permisos y la propiedad del dispositivo.

El valor predeterminado para oracleasm.support.without.asmlib es FALSE.

Información relacionada

Dispositivos de partición compatibles

Scripts compatibles

Los scripts asmmain.sh y asmquerydisk.sh permiten cambiar el usuario, el grupo y el usuario de la cuadrícula, todos los cuales se utilizan para consultar los discos ASM. Los scripts siempre deben ejecutarse desde la raíz.

El archivo asmmain.sh es el archivo de secuencia de comandos principal llamado desde cualquier operación que agregue o elimine dispositivos. La secuencia de comandos asmmain.sh llama internamente a otra secuencia de comandos, que debe ejecutarse desde la raíz que tiene las credenciales de la cuadrícula de oracle. Esta secuencia de comandos consulta los dispositivos del grupo de discos ASM y, a continuación, agrega esas entradas en el archivo initasmdisk con el permiso y la propiedad de los dispositivos. Puede cambiar los permisos y la propiedad de este archivo en función del entorno y del patrón regex que se utiliza para hacer coincidir sólo con /dev/mapper/*p1.

La secuencia de comandos asmquerydisk.sh se utiliza para consultar la lista de discos, que se utiliza para crear el grupo de discos ASM. Debe asignar valores a ORACLE_BASE, ORACLE_HOME y ORACLE_SID, según la configuración.

Los scripts están ubicados en /opt/NetApp/smo/plugins/examples/noasmlib. Sin embargo, estos scripts deben moverse a /opt/NetApp/smo/plugins/noasmlib antes de iniciar el servidor SnapManager para Oracle en el host.

Limitaciones de uso de scripts para admitir una base de datos ASM sin ASMLib

Debe tener en cuenta ciertas limitaciones al uso de scripts para admitir una base de datos ASM sin ASMLib.

- Las secuencias de comandos ofrecen una solución alternativa para cualquier versión del kernel, pero sólo si ASMLib no está instalado.
- Los permisos de los scripts deben definirse de forma que los usuarios root, Grid, oracle o equivalentes

puedan acceder a los scripts.

- Los scripts no admiten la restauración desde una ubicación secundaria.

Implementar y ejecutar los scripts

Es posible implementar y ejecutar los scripts asmmain.sh y asmquerydisk.sh para admitir bases de datos ASM sin ASMLib.

Estas secuencias de comandos no siguen la sintaxis de los scripts previos o posteriores y se llama al flujo de trabajo cuando los intitasmdiscos están habilitados. Puede cambiar cualquier cosa relacionada con la configuración en los scripts. Se recomienda verificar si todo lo contenido en los scripts funciona según lo esperado realizando una ejecución de secado rápida.

> Estas secuencias de comandos no afectan a su sistema en caso de fallos ni afectarán a su sistema. Estas secuencias de comandos se ejecutan para actualizar los discos relacionados con ASM para que tengan los permisos y la propiedad adecuados, de modo que los discos siempre estarán bajo control de instancia de ASM.

1. Cree los grupos de discos ASM con los discos con particiones.
2. Cree la base de datos Oracle en LOS GRUPOS de DISCOS.
3. Detenga el servidor SnapManager para Oracle.

   > En un entorno RAC, debe realizar este paso en todos los nodos de RAC.

4. Modifique smo.conf para incluir los siguientes parámetros:

   a. oracleasm.support.without.asmlib = true
   b. oracleasm.support.without.asmlib.owpropiedad = true
   c. oracleasm.support.without.asmlib.username = nombre de usuario del entorno de instancia de ASM
   d. oracleasm.support.without.asmlib.groupname = nombre de grupo del entorno de instancia de ASM

   Estas modificaciones establecen los permisos sólo para la ruta absoluta, lo que significa que en lugar del dispositivo de partición, los permisos se establecerán sólo para el dispositivo dm-*.

5. Modifique los scripts de los plugins disponibles en /opt/NetApp/smo/plugins/examples/noasmlib para incluir los ajustes de configuración en los scripts.
6. Copie las secuencias de comandos en /opt/NetApp/smo/plugins/noasmlib antes de iniciar el servidor SnapManager para Oracle en el host.
7. Desplácese hasta el directorio /opt/NetApp/smo y ejecute una ejecución en seco ejecutando el siguiente script: sh plugins/noasmlib/asmmain.sh

   Se crea el archivo etc/initasmdisks, que es el archivo principal que se utiliza.

   Puede confirmar que el archivo etc/initasmdisks contiene todos los dispositivos relacionados con la base de datos ASM configurada, como:

```
chown -R grid:oinstall /dev/mapper/360a98000316b61396c3f394645776863p1
         chmod 777 /dev/mapper/360a98000316b61396c3f394645776863p1
         chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714239p1
         chmod 777 /dev/mapper/360a980003754322f7a2b433469714239p1
         chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714241p1
         chmod 777 /dev/mapper/360a980003754322f7a2b433469714241p1
         chown -R grid:oinstall
/dev/mapper/360a980003754322f7a2b433469714243p1
         chmod 777 /dev/mapper/360a980003754322f7a2b433469714243p1
```

8. Inicie el servidor de SnapManager para Oracle.
9. Configure SnapDrive para UNIX añadiendo lo siguiente al archivo snapdrive.conf.disconnect-luns-before-vbsr=on
10. Reinicie el servidor de SnapDrive para UNIX.

> En un entorno RAC, es necesario realizar los pasos del 3 al 10 para todos los nodos RAC.

El archivo /etc/initasmdisks creado, debe ejecutarse desde uno de los scripts de inicio o desde un script que se acaba de definir en rc3.d. El archivo /etc/initasmdisks debe ejecutarse siempre antes de que se inicie el servicio oracleha.

Ejemplo

```
# ls -ltr *ohasd*
          lrwxrwxrwx 1 root root 17 Aug  7 02:34 S96ohasd ->
/etc/init.d/ohasd
          lrwxrwxrwx 1 root root 17 Aug  7 02:34 K15ohasd ->
/etc/init.d/ohasd
```

En el ejemplo siguiente, sh -x/etc/initasmdisks no estará disponible de forma predeterminada, y debe anexarlo como primera línea de la función `start_stack()` en un script ohasd:

```
start_stack()
{
sh -x /etc/initasmdisks
# see init.ohasd.sbs for a full rationale case $PLATFORM in Linux
}
```

Compatibilidad con bases de datos de ASM de Oracle RAC sin ASMLib

Si utiliza bases de datos Oracle RAC, los nodos RAC deben actualizarse con el archivo

initasmdisks cada vez que se realice una operación en el nodo RAC maestro.

Si no se requiere autenticación para iniciar sesión en los nodos RAC desde el nodo maestro, la asmmain.sh realiza una copia segura (SCP) de inimasmdisks en todos los nodos RAC. El archivo initasmdisks del nodo maestro se llamará cada vez que se produzca la restauración, y la secuencia de comandos asmmain.sh se puede actualizar para invocar la misma secuencia de comandos en todos los nodos RAC.

El archivo /etc/initasmdisks creado que debe ejecutarse desde una de las secuencias de comandos de inicio o desde una secuencia de comandos recientemente definida en rc3.d. El archivo /etc/initasmdisks debe ejecutarse siempre antes de que se inicie el servicio oracleha.

Compatibilidad con bases de datos ASM de Oracle 10g sin ASMLib

Si utiliza Oracle 10g, el comando asmcmd no está disponible para enumerar discos. Puede utilizar la consulta sql para obtener la lista de discos.

La secuencia de comandos disk_list.sql se incluye en las secuencias de comandos existentes proporcionadas en el directorio examples para admitir consultas sql. Al ejecutar el script theasmquerydisk.sh, el script disk_list.sql debe ejecutarse manualmente. Las líneas del script de ejemplo se añaden con comentarios en el archivo asmquerydisk.shl. Este archivo se puede colocar en la ubicación /home/grid u otra ubicación que desee.

Secuencias de comandos de ejemplo para admitir bases de datos ASM sin ASMLib

Los scripts de ejemplo están disponibles en el directorio plugins/examples/noasmlib del directorio de instalación de SnapManager para Oracle.

asmmain.sh

```
#!/bin/bash
griduser=grid
gridgroup=oinstall

# Run the script which takes the disklist from the asmcmd
# use appropriate user , here grid user is being used to run
# asmcmd command.
su -c "plugins/noasmlib/asmdiskquery.sh" -s /bin/sh grid
cat /home/grid/disklist

# Construct the final file as .bak file with propre inputs
awk -v guser=$griduser -v ggroup=$gridgroup '/^\/dev\/mapper/ { print
"chown -R "guser":"ggroup" "$1; print "chmod 777 " $1; }'
/home/grid/disklist > /etc/initasmdisks.bak

# move the bak file to the actual file.
mv /etc/initasmdisks.bak /etc/initasmdisks

# Set full full permission for this file to be called while rebooting and
restore
```

```
chmod 777 /etc/initasmdisks

# If the /etc/initasmdisks needs to be updated in all the RAC nodes
# or /etc/initasmdisks script has to be executed in the RAC nodes, then
the following
# section needs to be uncommented and used.
#
# Note: To do scp or running scripts in remote RAC node via ssh, it needs
password less login
# for root user with ssh keys shared between the two nodes.
#
# The following 2 lines are used for updating the file in the RAC nodes:
# scp /etc/initasmdisks root@racnode1:/etc/initasmdisks
# scp /etc/initasmdisks root@racnode2:/etc/initasmdisks
#
# In order to execute the /etc/initasmdisks in other RAC nodes
# The following must be added to the master RAC node /etc/initasmdisks
file
# from the asmmain.sh script itself. The above scp transfer will make sure
# the permissions and mode for the disk list contents are transferred to
the other RAC nodes
# so now appending any command in the /etc/initasmsdisks will be retained
only in the master RAC node.
# The following lines will add entries to the /etc/initasmsdisks file in
master RAC node only. When this script is executed
#  master RAC node, /etc/initasmdisks in all the RAC nodes will be
executed.
# echo 'ssh racnode1 /etc/initasmdisks' >> /etc/initasmdisks
# echo 'ssh racnode2 /etc/initasmdisks' >> /etc/initasmdisks
```

asmquerydisk.sh

```
#!/bin/bash
export  ORACLE_BASE=/u01/app/oracle
export ORACLE_HOME=/u01/app/grid/product/11.2.0.3/grid
export ORACLE_SID=+ASM
export  PATH=$ORACLE_HOME/bin:$PATH

# Get the Disk List and save this in a file called dglist.
asmcmd lsdsk  > /home/grid/disklist

# In oracle 10g the above used command 'asmcmd' is not available so use
SQL
# query can be used to take the disk list. Need to uncomment the following
# line and comment the above incase oracle 10g is being in use.
# The disk_list.sql script is availbe in this noasmlib examples folder
itself
# which can be modified as per customer needs.
# sqlplus "/as sysdba" @/home/grid/disk_list.sql > /home/grid/disklist
```

disk_list.sql

```
# su - oracle
-bash-4.1$ cat disk_list.sql
select path from v$asm_disk;
exit
-bash-4.1$
```

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=nombre de host
  - rw=nombre de host, 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	nombre_host_orabin	Sí	Encendido
Archivos de datos	oradata_sid	Sí	Apagado
Archivos de datos temporales	oratemp_sid	Sí	Apagado
Archivos de control	Oracntrl01_sid (multiplexado) Oracntrl02_sid (multiplexado)	Sí	Apagado
Rehacer registros	Oralog01_sid (multiplexado) Oralog02_sid (multiplexado)	Sí	Apagado
Registros de archivo	oraarch_sid	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	nombre_host_orabin	Sí	Encendido
Archivos de datos	oradata_dbname	Sí	Apagado
Archivos de datos temporales	oratemp_dbname	Sí	Apagado

Tipos de archivo	Nombres de volúmenes	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Archivos de control	Oracntrl01_dbname (Multiplexado) Oracntrl02_dbname (Multiplexado)	Sí	Apagado
Rehacer registros	Oralog01_dbname (Multiplexado) Oralog02_dbname (Multiplexado)	Sí	Apagado
Registros de archivo	oraarch_dbname	Sí	Apagado
Archivos de cluster	oracrs_clustername	Sí	Encendido

Instancia única de una base de datos de Automatic Storage Management (ASM)

Tipos de archivo	Nombres de volúmenes	Nombres de LUN	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Binarios de Oracle	nombre_host_orabin	nombre_host de orabin	Sí	Encendido
Archivos de datos	oradata_sid	oradata_sidlun	Sí	Apagado
Archivos de datos temporales	oratemp_sid	OraTemp_sidlun	Sí	Apagado
Archivos de control	Oracntrl01_sid (multiplexado) Oracntrl02_sid (multiplexado)	Oracntrl01_sidlun (Multiplexado) Oracntrl02_sidlun (Multiplexado)	Sí	Apagado
Rehacer registros	Oralog01_dbname (Multiplexado) Oralog02_dbname (Multiplexado)	Oralog01_dbnamelun (multiplexado) Oralog02_dbnamelun (multiplexado)	Sí	Apagado
Registros de archivo	oraarch_sid	Oraarch_sidlun	Sí	Apagado

Bases de datos RAC ASM

Tipos de archivo	Nombres de volúmenes	Nombres de LUN	Volumen dedicado para los tipos de archivo	Copias snapshot automáticas
Binarios de Oracle	nombre_host_orabin	nombre_host de orabin	Sí	Encendido
Archivos de datos	oradata_sid	oradata_sidlun	Sí	Apagado
Archivos de datos temporales	oratemp_sid	OraTemp_sidlun	Sí	Apagado
Archivos de control	Oracntrl01_sid (multiplexado) Oracntrl02_sid (multiplexado)	Oracntrl01_sidlun (Multiplexado) Oracntrl02_sidlun (Multiplexado)	Sí	Apagado
Rehacer registros	Oralog01_dbname (Multiplexado) Oralog02_dbname (Multiplexado)	Oralog01_dbnamelun (multiplexado) Oralog02_dbnamelun (multiplexado)	Sí	Apagado
Registros de archivo	oraarch_sid	Oraarch_sidlun	Sí	Apagado
Archivos de cluster	oracrs_clustername	oracrs_clusternamelun	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 o en un grupo de discos ASM 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

- SnapManager se puede configurar para catalogar backups de bases de datos con RMAN.

  Si se utiliza un catálogo de recuperación de RMAN, el catálogo de recuperación debe estar en una base de datos diferente a la base de datos de la que se realiza el backup.

- 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

- Se puede producir un error en la creación de backups si se ejecutan operaciones de SnapManager simultáneamente en el mismo host en una base de datos de ASM diferente.
- 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.
- Cuando se ejecuta una operación de backup o clonado simultáneamente en las bases de datos de RAC 10gR2 y 11gR2 en ASM, se produce un error en una de las operaciones de creación de clonado o backup.

  Este error se debe a una limitación conocida de Oracle.

- 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.

- En un entorno ASM, si los archivos de registro de clúster de Oracle (OCR) y de disco de votación coexisten en un grupo de discos que tiene archivos de datos, la operación de vista previa de restauración rápida muestra la estructura de directorio incorrecta para el disco de OCR y de votación.

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 clonado 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 la opción -resetlogs.

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 la operación de creación de perfiles que se generan desde la interfaz gráfica de usuario de SnapManager no tienen opciones de configuración del historial.

  No se puede utilizar el comando profile create para configurar las opciones de retención del historial desde la interfaz de línea de comandos 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 establecer la opción override-vbsr-snapmirror-check en 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: mysupport.netapp.com"

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 Oracle no admite la migración de un Vserver, que no es compatible con Clustered Data ONTAP
- SnapManager para Oracle 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 las versiones 10gR2, 11gR1, 11gR2 y 12*c*_, pero no es compatible con Oracle 10gR1 como repositorio o base de datos de destino.
- SnapManager no admite el uso de una dirección IP DE EXPLORACIÓN en lugar de un nombre de host.

  SCAN IP es una nueva función de Oracle 11gR2.

- SnapManager no es compatible con Oracle Cluster File System (OCFS).
- Oracle 11g en un entorno de NFS directo (dNFS) permite configuraciones de punto de montaje adicionales en el archivo Naranfstab, como varias rutas para el equilibrio de carga.

  SnapManager no modifica el archivo anorfstab. Debe agregar manualmente todas las propiedades adicionales que desee que utilice la base de datos clonada en el archivo oranfstab.

- 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: support.netapp.com/NOW/products/interoperability"

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 12*c*, debe actualizar a SnapManager 3.3.1 o posterior.

  > La base de datos Oracle 12*c* 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 12*c* 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.

- Los dispositivos sin formato respaldados por un gestor de volúmenes lógicos no son compatibles con la protección de los datos de Oracle.

  El almacenamiento de dispositivos sin procesar y los grupos de discos de gestión automática de almacenamiento (ASM) se deben aprovisionar directamente en los dispositivos físicos. En algunos casos, se requiere la partición.

- Un entorno Linux sin gestión de volúmenes lógicos requiere una partición.