SnapManager para Oracle usa Protection Manager para proteger un backup de base de datos

SnapManager Oracle

NetApp
October 04, 2023

This PDF was generated from https://docs.netapp.com/es-es/snapmanager-oracle/unix-administration/concept_details_of_the_target_database.html on October 04, 2023. Always check docs.netapp.com for the latest.

Tabla de contenidos

SnapManager para Oracle usa Protection Manager para proteger un backup de base de datos 1
Detalles de la base de datos de destino 1
Configuración y topología de almacenamiento principal y secundario 1
Programa de backup y estrategia de retención 5
Resumen de flujo de trabajo para backup de bases de datos local y secundario 6
Protección de la configuración y ejecución de backups 7
Restauración de base de datos desde backup 16

SnapManager para Oracle usa Protection Manager para proteger un backup de base de datos

Cuando SnapManager para Oracle y Protection Manager están instalados en un host UNIX y en el servidor respectivamente, proporcionan al administrador de la base de datos SnapManager la capacidad de configurar y ejecutar backups de bases de datos Oracle basados en normativas en el almacenamiento secundario, y restaurar, si es necesario, los datos de los que se ha realizado un backup del almacenamiento secundario al primario.

En el siguiente ejemplo, un administrador de bases de datos que utiliza SnapManager, crea un perfil para un backup local en el almacenamiento primario y otro perfil para un backup protegido en el almacenamiento secundario. A continuación, este administrador de base de datos trabaja con su administrador de almacenamiento en red, que utiliza la consola de Protection Manager, para configurar un backup basado en normativas de esa base de datos, desde el almacenamiento primario al secundario.

Detalles de la base de datos de destino

Este ejemplo de protección integrada de bases de datos describe la protección de una base de datos de nóminas. En el ejemplo se utilizan los datos siguientes.

El administrador de la base de datos (DBA) de TechCo, una empresa de 3000 personas con sede en Atlanta, debe crear una copia de seguridad coherente de la base de datos de nóminas de producción, PAYDB. La estrategia de protección para realizar la backup en el almacenamiento primario y secundario requiere que el administrador de almacenamiento y el administrador de bases de datos Oracle trabajen conjuntamente para realizar backups de la base de datos Oracle tanto de forma local en el almacenamiento primario como remota, en un almacenamiento secundario en una ubicación remota.

- **Información del perfil**

  Al crear un perfil en SnapManager, necesita los siguientes datos:

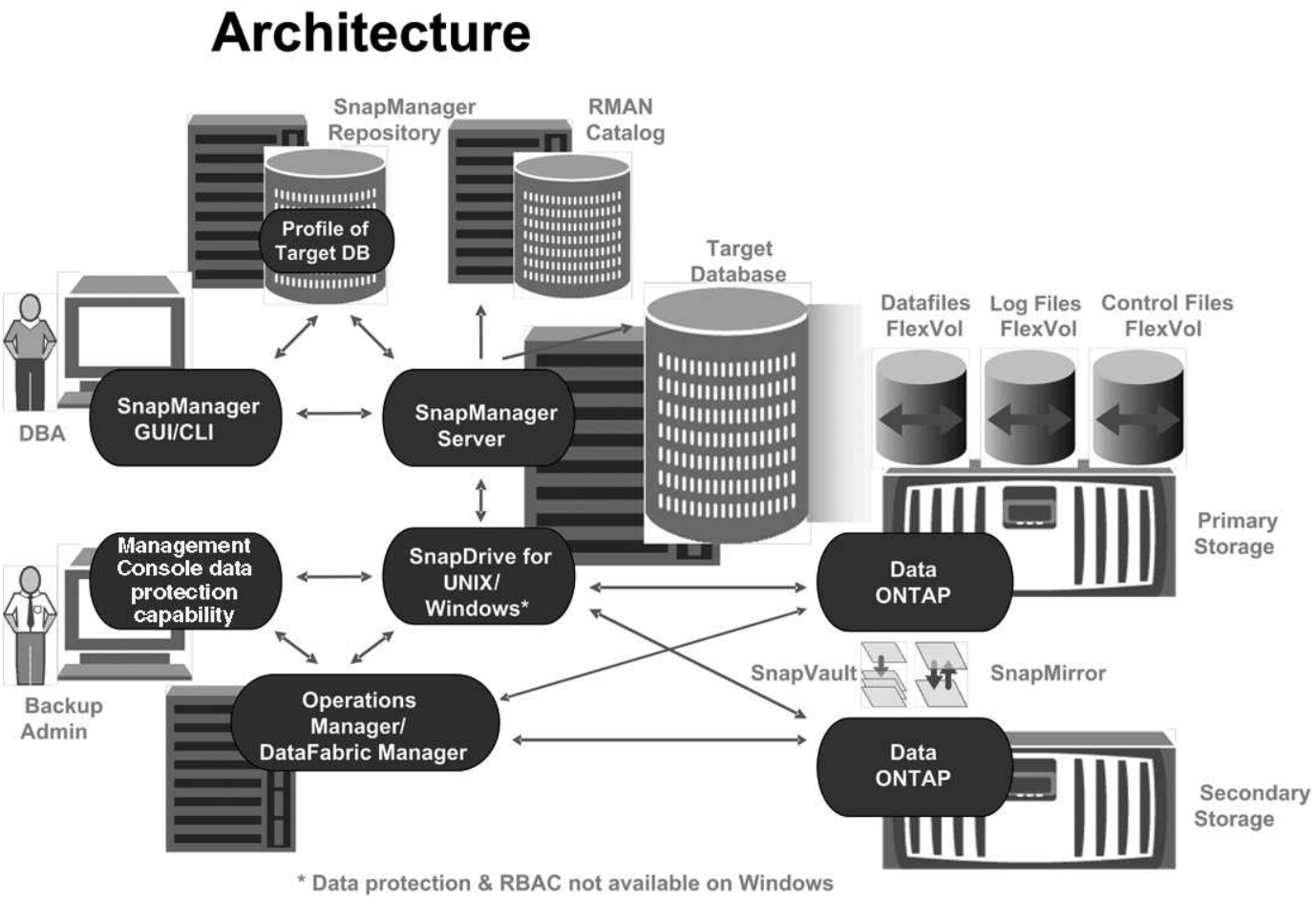
  - Nombre de la base de datos: PAYDB
  - Nombre del host: payroll.techco.com
  - ID de base de datos: Payroldb
  - Nombre del perfil: Payroll_prod
  - Modo de conexión: Autenticación de base de datos
  - Esquema de nomenclatura de Snapshot: smo_hostname_dbsid_smopirofile_scope_mode_smid (que se traduce a "smo_payroll.xyz.com_payrolldb_payroll_prod_f_h_x")

Configuración y topología de almacenamiento principal y secundario

En este ejemplo, TechCo Corporation ejecuta su base de datos de nóminas en un servidor de bases de datos que también es un host de SnapManager para Oracle y

almacena los datos de su base de datos de nóminas y los archivos de configuración en los sistemas de almacenamiento primario de la sede central de la empresa. El requisito corporativo es proteger la base de datos con backups diarios y semanales en un almacenamiento local, así como backups a sistemas de almacenamiento de un sitio de almacenamiento secundario situado a 50 kilómetros de distancia.

En la siguiente ilustración, se muestran los componentes de funcionalidades de protección de datos de SnapManager para Oracle y NetApp Management Console necesarios para admitir la protección de backup local y secundario.



Para gestionar la base de datos de nóminas y respaldar su protección de copia de seguridad local y secundaria como se muestra en el gráfico anterior, se utiliza la siguiente implementación.

- **SnapManager host**

  El host SnapManager, payroll.techco.com, se encuentra en la sede de la empresa y se ejecuta en un servidor UNIX, que también ejecuta el programa de base de datos que genera y mantiene la base de datos de nóminas.

  - **Conexiones**

    Para admitir la protección de backups locales y secundarios, el host SnapManager tiene conexiones de red a los siguientes componentes:

    - SnapManager para el cliente Oracle

        - Repositorio de SnapManager, que ejecuta el programa de bases de datos, SnapDrive para UNIX y SnapManager
        - Sistemas de almacenamiento primario
        - Sistemas de almacenamiento secundario
        - DataFabric Manager Server
    - **Productos instalados**

      El host SnapManager se instala con los siguientes productos para este ejemplo:

        - Servidor SnapManager
        - SnapDrive para UNIX
        - Utilidades de host
- **Sistemas de almacenamiento primario TechCo**

  La base de datos de nóminas, incluidos los archivos de datos asociados, los archivos de registro y los archivos de control, residen en los sistemas de almacenamiento principales. Estas se encuentran en la sede central de la empresa TechCo, junto con el host de SnapManager y la red que conecta el almacenamiento primario con el host de SnapManager. Las últimas transacciones y actualizaciones de la base de datos de nóminas se escriben en los sistemas de almacenamiento primarios. Las copias Snapshot, que proporcionan protección mediante backup local de la base de datos de nóminas, también residen en los sistemas de almacenamiento primarios.

    - **Conexiones**

      Para admitir la protección de backups secundarios, los sistemas de almacenamiento primario tienen conexiones de red a los siguientes componentes:

        - Host SnapManager que ejecuta el programa de bases de datos, SnapDrive para UNIX y SnapManager
        - Sistemas de almacenamiento secundario
        - DataFabric Manager Server
    - **Productos instalados**

      Para este ejemplo, deben habilitarse las siguientes licencias en estos sistemas:

        - Data ONTAP 7.3.1 o posterior
        - ONTAP primario de SnapVaultData
        - FlexVol (necesario para NFS)
        - SnapRestore
        - Protocolo NFS
- **Sistemas de almacenamiento secundario TechCo**

  Los sistemas de almacenamiento secundario, ubicados en un sitio de almacenamiento secundario conectado a la red, a 50 km de distancia, se utilizan para almacenar backups secundarios de la base de datos de nóminas.

    - **Conexiones**

Para admitir la protección de backup secundario, los sistemas de almacenamiento secundario tienen conexiones de red a los siguientes componentes:

    - Sistemas de almacenamiento primario
    - DataFabric Manager Server
  - **Productos instalados**

    Para este ejemplo, deben habilitarse las siguientes licencias en los sistemas de almacenamiento secundario:

    - Data ONTAP
    - SnapVaultData ONTAP secundario
    - SnapRestore
    - FlexVol (necesario para NFS)
    - Protocolo NFS
- **DataFabric Manager Server**

  DataFabric Manager Server, techco_dfm, se encuentra en la sede de la empresa en una ubicación accesible por el administrador de almacenamiento. DataFabric Manager Server, entre otras funciones, coordina las tareas de backup entre el almacenamiento principal y el secundario.

  - **Conexiones**

    Para admitir una protección de backup secundaria, DataFabric Manager Server mantiene conexiones de red con los siguientes componentes:

    - Consola de gestión de NetApp
    - Sistemas de almacenamiento primario
    - Sistemas de almacenamiento secundario
  - **Productos instalados**

    Para este ejemplo, DataFabric Manager Server cuenta con licencia para los siguientes productos de servidor:

    - DataFabric Manager
- **Repositorio de SnapManager**

  El repositorio de SnapManager, ubicado en un servidor dedicado, almacena datos sobre las operaciones realizadas por SnapManager, por ejemplo, el momento de realizar backups, los espacios de tablas y archivos de datos de los que se ha realizado backup, los sistemas de almacenamiento utilizados, los clones realizados y las copias Snapshot creadas. Cuando un administrador de base de datos intenta realizar una restauración completa o parcial, SnapManager consulta al repositorio para identificar los backups creados por SnapManager para Oracle para su restauración.

  - **Conexiones**

    Para admitir la protección de backup secundario, los sistemas de almacenamiento secundario tienen conexiones de red a los siguientes componentes:

    - Host SnapManager

        - SnapManager para el cliente Oracle

- **Consola de gestión de NetApp**

  La consola de gestión de NetApp es la consola de interfaz gráfica de usuario que utiliza el administrador de almacenamiento para configurar programaciones, políticas, conjuntos de datos y asignaciones de pools de recursos con el fin de permitir el backup en sistemas de almacenamiento secundarios, a los que el administrador de almacenamiento puede acceder.

  - **Conexiones**

    Para admitir la protección de backups secundarios, NetApp Management Console tiene conexiones de red a los siguientes componentes:

    - Sistemas de almacenamiento primario
    - Sistemas de almacenamiento secundario
    - DataFabric Manager Server

- **SnapManager para el cliente Oracle**

  El cliente SnapManager para Oracle es la interfaz gráfica de usuario y la consola de línea de comandos que usa el administrador de bases de datos para la base de datos de nóminas de este ejemplo para configurar y realizar copias de seguridad locales y copias de seguridad en el almacenamiento secundario.

  - **Conexiones**

    Para admitir la protección de backups locales y secundarios, SnapManager para Oracle Client tiene conexiones de red a los siguientes componentes:

    - Host SnapManager
    - SnapManager Repository, ejecuta el programa de bases de datos, SnapDrive para UNIX y SnapManager
    - Host de base de datos (si está separado del host que ejecuta SnapManager)
    - DataFabric Manager Server

  - **Productos instalados**

    Para admitir la protección de copia de seguridad local y copia de seguridad secundaria, se debe instalar SnapManager para el software de cliente de Oracle en este componente.

Programa de backup y estrategia de retención

El administrador de bases de datos quiere asegurarse de que los backups estén disponibles en caso de pérdida de datos, en caso de siniestro y por motivos normativos. Esto requiere una política de retención de pensamiento detenidamente para las distintas bases de datos.

Para la base de datos de nóminas de producción, el DBA se adhiere a la siguiente estrategia de retención de TechCo:

Frecuencia de backup	Duración de la retención	El tiempo de los backups	Tipo de almacenamiento
Una vez al día	10 días	7 p. m.	Primario (local)
Una vez al día	10 días	7 p. m.	Secundario (archivado)
Una vez por semana	52 semanas	Sábados 1:00 a.m.	Secundario (archivado)

- **Ventajas de copia de seguridad local**

  El backup local diario proporciona protección de bases de datos, que es instantánea, utiliza cero ancho de banda de red, utiliza un mínimo de espacio de almacenamiento adicional, ofrece una restauración instantánea y ofrece funciones de backup y restauración de datos muy detalladas.

  Como los backups semanales finales de la base de datos de nóminas se conservan durante un mínimo de 52 semanas en un site de almacenamiento secundario, no es necesario conservar los backups diarios durante más de 10 días.

- **Ventajas de copia de seguridad protegida**

  Los backups diarios y semanales a un almacenamiento secundario en una ubicación remota garantizan que si los datos del site de almacenamiento principal presentan daños, la base de datos objetivo sigue estando protegida y podrá restaurarse a partir del almacenamiento secundario.

  Se realizan los backups diarios al almacenamiento secundario para protegerse frente a daños en el sistema de almacenamiento primario. Como los backups semanales finales de la base de datos de nóminas se conservan durante un mínimo de 52 semanas, no es necesario conservar los backups diarios durante más de 10 días.

Resumen de flujo de trabajo para backup de bases de datos local y secundario

En este ejemplo, el administrador de bases de datos (con SnapManager) y el administrador de almacenamiento (con la función de protección de datos Management Console de NetApp) coordinan las acciones para configurar los backups locales y secundarios (también conocidos como backup protegido) de la base de datos de destino.

La secuencia de acciones realizadas se resume de la siguiente manera:

- **Configuración del pool de recursos secundario**

  El administrador de almacenamiento usa la funcionalidad de protección de datos de NetApp Management Console para configurar un conjunto de recursos de sistemas de almacenamiento en el sitio secundario que puede usarse para almacenar el backup de base de datos de nóminas.

- **Programación de copia de seguridad secundaria**

  El administrador de almacenamiento usa la funcionalidad de protección de datos de NetApp Management Console para configurar programaciones de backup secundarias.

- **Configuración de la política de protección**

  El administrador de almacenamiento usa la funcionalidad de protección de datos de NetApp Management Console para configurar una normativa de protección de backup secundaria para la base de datos de destino. La política de protección incluye las programaciones y especifica el tipo base de protección para implementar la protección de backups (backup, reflejo o una combinación de ambos), y nombra políticas de retención para los datos primarios, secundarios y, en ocasiones, nodos de almacenamiento terciarios.

- **Asignación de políticas de protección y configuración de perfiles de base de datos**

  El DBA utiliza SnapManager para crear o editar un perfil de la base de datos de destino que admita una copia de seguridad secundaria. Al configurar el perfil, el DBA:

  - Permite la protección de backups en el almacenamiento secundario.
  - Asigna a este perfil la nueva política de protección, que se creó en la funcionalidad de protección de datos de NetApp Management Console y se recuperó de ella.

    La asignación de la normativa de protección incluye automáticamente la base de datos de destino en un conjunto de datos parcialmente aprovisionado, pero no conforme con el conjunto de datos de la funcionalidad de protección de datos de la Consola de gestión de NetApp. Cuando está totalmente aprovisionado, la configuración del conjunto de datos permite realizar backups de la base de datos de destino en un almacenamiento secundario.

  El nombre del conjunto de datos utiliza esta sintaxis: smo_hostname_datasename, que se traduce en "smo_payroll.techco.com_paydb".

- **Aprovisionamiento de almacenamiento secundario y terciario**

  El administrador de almacenamiento usa la funcionalidad de protección de datos de Management Console de NetApp para asignar pools de recursos con el fin de aprovisionar los nodos de almacenamiento secundario y, en ocasiones, terciario (si la política de protección asignada especifica nodos de almacenamiento terciarios).

- **Backup en almacenamiento local**

  El administrador de bases de datos abre el perfil con la protección habilitada en SnapManager y crea un backup completo al almacenamiento local. El nuevo backup se muestra en SnapManager como programado para la protección, pero no protegido todavía.

- **Confirmación de copia de seguridad secundaria**

  Como el backup se basa en un perfil habilitado para la protección, el backup se transfiere al volumen secundario según la programación de la política de protección. El administrador de bases de datos utiliza SnapManager para confirmar la transferencia del backup a un almacenamiento secundario. Una vez que el backup se ha copiado al almacenamiento secundario, SnapManager cambia el estado de protección de backup de "no protegido" a "protegido".

Protección de la configuración y ejecución de backups

Es necesario configurar SnapManager y Protection Manager para admitir backups de bases de datos en el almacenamiento secundario. El administrador de la base de datos y el administrador de almacenamiento deben coordinar las acciones correspondientes.

Uso de SnapManager para Oracle para crear el perfil de base de datos para un backup local

Los administradores de bases de datos utilizan SnapManager para crear un perfil de base de datos que se utilizará para iniciar una copia de seguridad en el almacenamiento local en un sistema de almacenamiento primario. Los procesos de creación de perfiles y de creación de backups se realizan por completo en SnapManager; no implican Protection Manager.

Un perfil contiene información sobre la base de datos que se gestiona, incluidas sus credenciales, su configuración de backup y la configuración de protección para las copias de seguridad. Al crear un perfil, no es necesario especificar los detalles de la base de datos cada vez que se realiza una operación en esa base de datos, en su lugar sólo se proporciona el nombre del perfil. Un perfil sólo puede hacer referencia a una base de datos. Se puede hacer referencia a esa misma base de datos por más de un perfil.

1. Vaya al cliente de SnapManager para Oracle.
2. En el árbol repositorios SnapManager, haga clic con el botón secundario del ratón en el host que desee asociar a este perfil y seleccione **Crear perfil**.
3. En la página Información de configuración del perfil, introduzca la siguiente información y haga clic en **Siguiente**.
   - Nombre del perfil: Payroll_prod
   - Contraseña de perfil: Payroll123
   - Comentario: Base de datos de nóminas de producción
4. En la página Database Configuration Information (Información de configuración de la base de datos), introduzca la siguiente información y haga clic en **Next** (Siguiente).
   - Nombre de la base de datos: PAYDB
   - SID de base de datos: Payroldb
   - Host de la base de datos: Acepte el valor predeterminado

     Debido a que está creando un perfil a partir de un host en el árbol de repositorios, SnapManager muestra el nombre de host.
5. En la segunda página Información de configuración de la base de datos, acepte la siguiente información de la base de datos y haga clic en **Siguiente**:
   - Cuenta de host, que representa la cuenta de usuario de Oracle: oracle
   - Host Group, que representa al grupo Oracle: dba
6. En la página Información de conexión a la base de datos, seleccione **utilizar autenticación de base de datos** para permitir que los usuarios se autentiquen mediante la información de la base de datos.

   Para este ejemplo, introduzca la siguiente información y haga clic en **Siguiente**.

   - SYSDBA Privileged User Name, que representa al administrador de la base de datos del sistema que tiene privilegios administrativos: Sys
   - Contraseña (contraseña SYSDBA): oracle
   - Puerto para conectarse al host de la base de datos: 1521
7. En la página Información de configuración de RMAN, seleccione **no utilizar RMAN** y haga clic en **Siguiente**.

Oracle Recovery Manager (RMAN) es una herramienta de Oracle que ayuda a realizar el backup y la recuperación de bases de datos de Oracle mediante la detección a nivel de bloque.

8. En la página Snapshot Naming Information, especifique una convención de nomenclatura para las Snapshot asociadas con este perfil seleccionando variables. La única variable que se requiere es la variable **smid**, que crea un identificador de instantánea único.

   Para este ejemplo, haga lo siguiente:

   a. En la lista símbolo de variable, seleccione la variable **{usertext}** y haga clic en **Agregar**.
   b. Introduzca "payroll.techco.com_" como nombre de host y haga clic en **Aceptar**.
   c. Haga clic en **izquierda** hasta que el nombre de host aparezca justo después de "smo" en el cuadro Formato .
   d. Haga clic en **Siguiente**.

   La convención de nomenclatura de Snapshot de smo_hostname_smoprofile_dbsid_Scope_mode_smid se convierte en "smo_payroll.techco.com_payroll_prod2_payrolldb_f_a_x" (donde "f" indica un backup completo, la "a" indica el modo automático, y la "x" representa el SMID único).

9. En la página realizar operación, compruebe la información y haga clic en **Crear**.
10. Haga clic en **Detalles de operación** para ver información acerca de la operación de creación de perfiles e información de elegibilidad de restauración basada en volumen.

Uso de Protection Manager para configurar un pool de recursos secundario

Para admitir el backup de la base de datos en el almacenamiento secundario, el administrador de almacenamiento usa Protection Manager para organizar los sistemas de almacenamiento secundario habilitados con la licencia secundaria de SnapVault en un conjunto de recursos para los backups.

Lo ideal es que los sistemas de almacenamiento de un conjunto de recursos sean intercambiables en cuanto a su aceptación como destinos para los backups. Por ejemplo, al desarrollar la estrategia de protección para la base de datos de nóminas, como administrador de almacenamiento, identificó los sistemas de almacenamiento secundarios con niveles de servicio y rendimiento similares que serían miembros adecuados del mismo conjunto de recursos.

Ya creó agregados de espacio no utilizado en sistemas de almacenamiento que piensa asignar a pools de recursos. De este modo se garantiza que haya espacio adecuado para contener las copias de seguridad.

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **datos** > **grupos de recursos**.

   Aparecerá la ventana Pools de recursos.

3. Haga clic en **Agregar**.

   Se iniciará el asistente Add Resource Pool.

4. Complete los pasos del asistente para crear el pool de recursos **paydb_backup_resource**.

   Utilice los siguientes ajustes:

- Nombre: Use **paydb-backup_resource**
- Umbrales de espacio (utilice los valores predeterminados):
  - Umbrales de utilización del espacio: Activado
  - Umbral casi completo (para el conjunto de recursos): 80%
  - Umbral completo (para el conjunto de recursos): 90%

Uso de Protection Manager para configurar las programaciones de backups secundarios

Para admitir el backup de la base de datos en el almacenamiento secundario, el administrador de almacenamiento usa Protection Manager para configurar una programación de backups.

Antes de configurar la programación para las copias de seguridad secundarias, el administrador de almacenamiento consulta al partner DBA la siguiente información:

- La programación que el administrador de bases de datos desea que se sigan los backups secundarios.

  En este caso, los backups únicos diarios se realizan a las 7 p. m. Y los backups una vez semanales se realizan el sábado a las 1:00

  a. Vaya a la Consola de gestión de NetApp de Protection Manager.
  b. En la barra de menús, haga clic en **políticas** > **Protección** > **programas**.

     Se muestra la pestaña Schedules de la ventana Protection Policies.

  c. Seleccione el horario diario **Diario a las 8:00 PM** en la lista de horarios.
  d. Haga clic en **Copiar**.

     En la lista se muestra un nuevo horario diario, **copia del diario a las 8:00 PM**. Ya está seleccionado.

  e. Haga clic en **Editar**.

     La hoja de propiedades Editar horario diario se abre a la ficha Programación.

  f. Cambie el nombre del programa a **nómina diaria a las 7 PM**, actualice la descripción y, a continuación, haga clic en **aplicar**.

     Se guardan los cambios.

  g. Haga clic en la ficha **Eventos diarios**.

     La hora actual de copia de seguridad diaria de la programación es de 8:00 p.m. aparece en pantalla.

  h. Haga clic en **Agregar** e introduzca **7:00 PM** en el nuevo campo Hora y, a continuación, haga clic en **aplicar**.

     La hora actual de copia de seguridad diaria del programa es ahora a las 7:00 p.m.

  i. Haga clic en **Aceptar** para guardar los cambios y salir de la hoja de propiedades.

     Su nuevo horario diario, **Payroll Daily a las 7 PM**, se muestra en la lista de horarios.

j. Seleccione el horario semanal **Domingo a las 8:00 PM más diariamente** en la lista de horarios.

k. Haga clic en **Copiar**.

   En la lista se muestra un nuevo horario semanal, **copia del domingo a las 8:00 PM más diario**. Ya está seleccionado.

l. Haga clic en **Editar**.

   La hoja de propiedades Editar horario semanal se abre a la ficha Programación.

m. Cambie el nombre del programa a **Payroll Saturday a la 1 AM PLUS Daily a las 7 PM** y actualice la descripción.

n. En la lista desplegable **Horario diario**, seleccione el horario diario que acaba de crear, **Payroll Daily a las 7 PM**.

   Seleccionar **nómina diaria a las 7 PM** significa que este programa define cuándo se producen las operaciones diarias cuando se aplica a una política el programa **nómina de sábado a la 1 AM más diario a las 7 PM**.

o. Haga clic en **Aceptar** para guardar los cambios y salir de la hoja de propiedades.

   Su nuevo horario semanal, **Payroll Saturday a la 1 AM más diariamente a las 7 PM**, se muestra en la lista de horarios.

Uso de Protection Manager para configurar una política de protección de backups secundarios

Después de configurar la programación de backup, el administrador de almacenamiento configura una normativa de almacenamiento de backup protegido en la que se incluirá dicha programación.

Antes de configurar la normativa de protección, el administrador de almacenamiento le ofrece al partner DBA la siguiente información:

- Duración de retención que se debe especificar para el almacenamiento secundario
- Tipo de protección del almacenamiento secundario requerida

La política de protección que se crea, puede listarse en SnapManager para Oracle por parte del socio de administrador de bases de datos y asignarse a un perfil de base de datos para la protección de los datos.

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **políticas** > **Protección** > **Descripción general**.

   Se muestra la pestaña Overview de la ventana Protection Policies.

3. Haga clic en **Agregar directiva** para iniciar el asistente Agregar directiva de protección.
4. Complete el asistente con los siguientes pasos:

   a. Especifique un nombre de política descriptivo.

      Para este ejemplo, introduzca **TechCo Payroll Data: Copia de seguridad** y una descripción y, a continuación, haga clic en **Siguiente**.

b. Seleccione una política base.

   Para este ejemplo, seleccione **copia de seguridad** y haga clic en **Siguiente**.

c. En la hoja de propiedades de la directiva del nodo de datos principal, acepte la configuración predeterminada y haga clic en **Siguiente**.

   > En este ejemplo, se aplica la programación de backup local configurada en SnapManager. Se ignora cualquier programación de backup local especificada con este método.

d. En la hoja de propiedades de conexión de datos primarios a copia de seguridad, seleccione una programación de copia de seguridad.

   Para este ejemplo, seleccione **Payroll Saturday a la 1 AM más diariamente a las 7 PM** como su programa de copia de seguridad y, a continuación, haga clic en **Next**.

   En este ejemplo, la programación seleccionada incluye tanto las programaciones semanales como diarias que se configuraron anteriormente.

e. En la hoja de propiedades Backup policy, especifique el nombre del nodo de backup y los tiempos de retención de los backups Daily, Weekly o Monthly.

   Para este ejemplo, especifique una retención de backup diaria de 10 días y una retención de backup semanal de 52 semanas. Después de completar cada hoja de propiedades, haga clic en **Siguiente**.

Una vez completadas todas las hojas de propiedades, el asistente para agregar directivas de protección muestra una hoja de resumen de la directiva de protección que desea crear.

5. Haga clic en **Finalizar** para guardar los cambios.

La política de protección de **TechCo Payroll Data: Backup** se incluye entre las demás políticas configuradas para Protection Manager.

El socio DBA puede ahora usar SnapManager para Oracle para enumerar y asignar esta política al crear el perfil de base de datos para proteger los datos.

Utilice SnapManager para Oracle para crear el perfil de base de datos y asignar una política de protección

Debe crear un perfil en SnapManager para Oracle, habilitar la protección en el perfil y asignar una política de protección para crear un backup protegido.

Un perfil contiene información sobre la base de datos que se gestiona, incluidas sus credenciales, su configuración de backup y la configuración de protección para backups. Después de crear un perfil, no es necesario especificar los detalles de la base de datos cada vez que se realiza una operación. Un perfil sólo puede hacer referencia a una base de datos, pero es posible hacer referencia a esa misma base de datos mediante más de un perfil.

1. Vaya al cliente de SnapManager para Oracle.
2. En el árbol repositorios, haga clic con el botón secundario del ratón en el host y seleccione **Crear perfil**.
3. En la página Información de configuración del perfil, introduzca los detalles del perfil y haga clic en **Siguiente**.

Puede introducir la siguiente información:

- Nombre del perfil: Payroll_prod2
- Contraseña de perfil: Payroll123
- Comentario: Base de datos de nóminas de producción

4. En las páginas Database Configuration Information (Información de configuración de la base de datos), introduzca los detalles de la base de datos y haga clic en **Next** (Siguiente).

   Puede introducir la siguiente información:

   - Nombre de la base de datos: PAYDB
   - SID de base de datos: Payroldb
   - Host de la base de datos: Acepte el valor predeterminado. Debido a que está creando un perfil a partir de un host en el árbol de repositorios, SnapManager muestra el nombre de host.
   - Cuenta de host, que representa la cuenta de usuario de Oracle: oracle
   - Host Group, que representa al grupo Oracle: dba

5. En la página Información de conexión a la base de datos, haga clic en **usar autenticación de base de datos** para permitir que los usuarios autentiquen mediante información de la base de datos.
6. Introduzca los detalles de conexión de la base de datos y haga clic en **Siguiente**.

   Puede introducir la siguiente información:

   - SYSDBA Privileged User Name, que representa al administrador de la base de datos del sistema que tiene privilegios administrativos: Sys
   - Contraseña (contraseña SYSDBA): oracle
   - Puerto para conectarse al host de la base de datos: 1521

7. En la página Información de configuración de RMAN, haga clic en **no utilizar RMAN** y haga clic en **Siguiente**.

   Oracle Recovery Manager (RMAN) es una herramienta de Oracle que ayuda a realizar el backup y la recuperación de bases de datos de Oracle mediante la detección a nivel de bloque.

8. En la página Snapshot Naming Information, especifique una convención de nomenclatura para las Snapshot asociadas con este perfil seleccionando variables.

   La variable smid crea un identificador de instantánea único.

   Realice lo siguiente:

   a. En la lista símbolo de variable, seleccione texto de usuario y haga clic en **Agregar**.
   b. Introduzca payroll.techco.com_ como nombre de host y haga clic en **Aceptar**.
   c. Haga clic en **izquierda** hasta que el nombre de host aparezca justo después de smo en el cuadro Formato .
   d. Haga clic en **Siguiente**.

   La convención de nomenclatura de Snapshot de smo_hostname_smoprofile_dbsid_Scope_mode_smid se convierte en "smo_payroll.techco.com_payroll_prod2_payrolldb_f_a_x" (donde "f" indica un backup completo, "a" indica el modo automático, y "x" representa el SMID único).

9. Seleccione **Directiva de protección de Protection Manager**.

   La normativa de protección de Protection Manager le permite seleccionar una directiva de protección configurada mediante la Consola de gestión de NetApp.

10. Seleccione **TechCo Payroll Data: Backup** como política de protección de las políticas de protección recuperadas de NetApp Management Console y haga clic en **Siguiente**.
11. En la página realizar operación, compruebe la información y haga clic en **Crear**.
12. Haga clic en **Detalles de operación** para ver información acerca de la operación de creación de perfiles e información de elegibilidad de restauración basada en volumen.
    - La asignación de una normativa de protección de la consola de gestión de NetApp al perfil de la base de datos crea automáticamente un conjunto de datos no conforme, visible para el operador de la consola de gestión de NetApp, con el nombre de convención smo_<hostname>_<profilename>, o en este ejemplo: smo_payroll.tech.com_PAYDB.
    - Si el perfil no es apto para la restauración de volumen (también llamado "restauración rápida"), se produce lo siguiente:
      - La ficha **resultados** indica que la creación del perfil se ha realizado correctamente y que se han producido advertencias durante la operación.
      - La ficha **Detalles de operación** incluye un registro DE ADVERTENCIA, que indica que el perfil no es elegible para una restauración rápida y explica por qué.

Uso de Protection Manager para aprovisionar el nuevo conjunto de datos

Una vez creado el conjunto de datos smo_paydb, el administrador de almacenamiento usa Protection Manager para asignar recursos del sistema de almacenamiento a fin de aprovisionar el nodo de backup del conjunto de datos.

Antes de aprovisionar el conjunto de datos recién creado, el administrador de almacenamiento consulta al partner DBA el nombre del conjunto de datos especificado en el perfil.

En este caso, el nombre del conjunto de datos es smo_payroll.tech.com_PAYDB.

1. Vaya a la Consola de gestión de NetApp de Protection Manager.
2. En la barra de menús, haga clic en **datos** > **conjuntos de datos** > **Descripción general**.

   La pestaña Datasets de la ventana Datasets muestra una lista de conjuntos de datos que incluye el conjunto de datos que acaba de crear mediante SnapManager.

3. Localice y seleccione el conjunto de datos **smo_payroll.tech.com_PAYDB**.

   Al seleccionar este conjunto de datos, el área del gráfico muestra el conjunto de datos smo_paydb con su nodo de copia de seguridad sin aprovisionar. Su estado de conformidad se Marca como no conforme.

4. Con el conjunto de datos smo_paydb todavía resaltado, haga clic en **Editar**.

   La consola de gestión de NetApp de Protection Manager muestra la ventana Editar conjunto de datos para el conjunto de datos **smo_payroll.tech.com_PAYDB**. El panel de navegación de la ventana muestra las opciones de configuración del nodo principal del conjunto de datos, la conexión de backup y el nodo de backup.

5. En el panel de navegación, busque las opciones del nodo de copia de seguridad del conjunto de datos y

seleccione **agrupaciones de aprovisionamiento/recursos**.

La ventana Edit Dataset muestra una configuración de la política de aprovisionamiento predeterminada y una lista de pools de recursos disponibles.

6. Para este ejemplo, seleccione el pool de recursos **paydb_backup_resource** y haga clic en **>**.

   El pool de recursos seleccionado aparece en el campo "Pools de recursos para este nodo".

7. Haga clic en **Finalizar** para guardar los cambios.

Protection Manager aprovisiona automáticamente el nodo de copia de seguridad secundario con recursos del pool de recursos paydb_backup_resource.

Uso de SnapManager para Oracle para crear un backup protegido

Al crear un backup para este ejemplo, el administrador de bases de datos selecciona la creación de un backup completo, define las opciones de backup y selecciona la protección para el almacenamiento secundario. Si bien el backup se realiza inicialmente en el almacenamiento local, ya que este backup se basa en un perfil con protección habilitada, el backup se transfiere luego al almacenamiento secundario según la programación de la política de protección definida en Protection Manager.

1. Vaya al cliente de SnapManager para Oracle.
2. En el árbol del repositorio de SnapManager, haga clic con el botón derecho del ratón en el perfil que contiene la base de datos de la que desea realizar la copia de seguridad y seleccione **copia de seguridad**.

   Se iniciará el Asistente para copia de seguridad de SnapManager para Oracle.

3. Introduzca Production_Payroll como etiqueta.
4. Introduzca la nómina de producción Jan 19 backup como comentario.
5. Seleccione **Auto** como el tipo de copia de seguridad que desea crear.

   Esto permite a SnapManager determinar si se debe realizar un backup en línea o sin conexión.

6. Seleccione **Diario** o **Semanal** como la frecuencia de la copia de seguridad.
7. Para confirmar que la copia de seguridad tiene un formato válido para Oracle, marque la casilla junto a **verificar copia de seguridad**.

   Esta operación utiliza Oracle DBVerify para comprobar el formato de bloque y la estructura.

8. Para forzar el estado de la base de datos al modo apropiado (por ejemplo, de abierto a montado), seleccione **permitir inicio o cierre de la base de datos, si es necesario**, y haga clic en **Siguiente**.
9. En la página Database, Tablespaces o Datafiles to Backup, seleccione **Full Backup** y haga clic en **Next**.
10. Para proteger la copia de seguridad en almacenamiento secundario, seleccione **proteger la copia de seguridad** y haga clic en **Siguiente**.
11. En la página realizar operación, compruebe la información suministrada y haga clic en **copia de seguridad**.
12. En la página Progress, consulte el progreso y los resultados de la creación de backup.

13. Para ver los detalles de la operación, haga clic en **Detalles de la operación**.

Usar SnapManager para Oracle para confirmar la protección del backup

Con SnapManager para Oracle, se puede ver una lista de backups asociados a un perfil, determinar si los backups estaban habilitados para la protección y ver la clase de retención (diaria o semanal, en este ejemplo).

Al principio, el nuevo backup en este ejemplo se muestra como programado para la protección, pero no está protegido aún (en la interfaz gráfica de usuario de SnapManager y en el resultado del comando backup show). Una vez que el administrador de almacenamiento garantiza que el backup se haya copiado al almacenamiento secundario, SnapManager cambia el estado de protección de backup de "no protegido" a "protegido" en la interfaz gráfica de usuario y con el comando backup list.

1. Vaya al cliente de SnapManager para Oracle.
2. En el árbol del repositorio de SnapManager, expanda el perfil para mostrar sus copias de seguridad.
3. Haga clic en la ficha **copias de seguridad/clones**.
4. En el panel Informes, seleccione **Detalles de copia de seguridad**.
5. Consulte la columna Protection y asegúrese de que el estado sea "Protected".

Restauración de base de datos desde backup

Si el contenido activo de la base de datos de nóminas se pierde o destruye accidentalmente, SnapManager y la función de protección de datos de la consola de gestión de NetApp permiten la restauración de esos datos desde un backup local o un almacenamiento secundario.

Uso de SnapManager para Oracle para restaurar un backup local en el almacenamiento primario

Es posible restaurar backups locales que estén en el almacenamiento principal. Todo el proceso se realiza mediante SnapManager para Oracle.

También puede obtener una vista previa de la información acerca de un proceso de restauración de copia de seguridad. Puede que desee hacer esto para ver información acerca de la elegibilidad de restauración de un backup. SnapManager analiza los datos de un backup para determinar si puede completarse el proceso de restauración usando la restauración basada en volúmenes o el método de restauración basada en archivos.

La vista previa de la restauración muestra la siguiente información:

- Qué mecanismo de restauración (restauración rápida, restauración de sistema de archivos en el lado del almacenamiento, restauración de archivos en el lado del almacenamiento o restauración de copias de archivos del lado del host) se utilizará para restaurar cada archivo.
- Por qué no se utilizaron mecanismos más eficientes para restaurar cada archivo.

En la vista previa del plan de restauración, SnapManager no restaura nada. La vista previa muestra información de hasta 20 archivos.

Si desea obtener una vista previa de una restauración de archivos de datos pero la base de datos no está

montada, SnapManager monta la base de datos. Si no se puede montar la base de datos, la operación genera un error y SnapManager devuelve la base de datos a su estado original.

1. En el árbol del repositorio, haga clic con el botón derecho del ratón en la copia de seguridad que desea restaurar y seleccione **Restaurar**.
2. En la página de bienvenida del Asistente para restauración y recuperación, haga clic en **Siguiente**.
3. En la página Restore Configuration Information, seleccione **Complete Datafile/Tablespace Restore with Control Files**.
4. Haga clic en **permitir cierre de la base de datos si es necesario**.

   SnapManager cambia el estado de la base de datos, si es necesario. Por ejemplo, si la base de datos está sin conexión y debe estar en línea, SnapManager la fuerza a la conexión.

5. En la página Información de configuración de recuperación, haga clic en **todos los registros**.

   SnapManager restaura y recupera la base de datos a la última transacción y aplica todos los registros requeridos.

6. En la página Restore Source Location Configuration (Restaurar configuración de ubicación de origen), consulte la información sobre la copia de seguridad en primaria y haga clic en **Next** (Siguiente).

   Si el backup solo se realiza en el almacenamiento primario, SnapManager restaura el backup desde el almacenamiento primario.

7. En la página Volume Restore Configuration Information (Información de configuración de la restauración de volumen), seleccione **intentar la restauración de volumen** para intentar el método de restauración de volumen.
8. Haga clic en **Volver a restauración basada en archivos**.

   Así, SnapManager puede utilizar el método de restauración basada en archivos si no se puede utilizar el método de restauración de volumen.

9. Haga clic en **Vista previa** para ver las comprobaciones de elegibilidad para obtener una rápida restauración e información sobre comprobaciones obligatorias y anulables.
10. En la página realizar operación, compruebe la información introducida y haga clic en **Restaurar**.
11. Para ver detalles sobre el proceso, haga clic en **Detalles de la operación**.

Uso de SnapManager para Oracle para restaurar backups desde almacenamiento secundario

Los administradores pueden restaurar backups protegidos a partir de almacenamiento secundario y elegir cómo desean copiar los datos de nuevo en el almacenamiento primario.

Antes de intentar restaurar el backup, compruebe las propiedades del backup y asegúrese de que el backup se libere en el sistema de almacenamiento principal y esté protegido en el almacenamiento secundario.

1. En el árbol del repositorio de SnapManager para Oracle, haga clic con el botón derecho del ratón en la copia de seguridad que desea restaurar y seleccione **Restaurar**.
2. En la página de bienvenida del Asistente para restauración y recuperación, haga clic en **Siguiente**.

3. En la página Restore Configuration Information, haga clic en **Complete Datafile/Tablespace Restore with Control Files**.
4. Haga clic en **permitir cierre de la base de datos si es necesario** y, a continuación, haga clic en **Siguiente**.

   SnapManager cambia el estado de la base de datos, si es necesario. Por ejemplo, si la base de datos está sin conexión y debe estar en línea, SnapManager la fuerza a la conexión.

5. En la página Información de configuración de recuperación, haga clic en **todos los registros**. A continuación, haga clic en **Siguiente**.

   SnapManager restaura y recupera la base de datos a la última transacción y aplica todos los registros requeridos.

6. En la página Restore Source Location Configuration (Restaurar configuración de ubicación de origen), seleccione el ID del origen de copia de seguridad protegida y haga clic en **Next** (Siguiente).
7. En la página Información de configuración de la restauración de volumen, haga clic en **intentar la restauración de volumen** para intentar la restauración de volumen.
8. Haga clic en **Volver a restauración basada en archivos**.

   Esto permite a SnapManager utilizar el método de restauración basada en archivos si no se puede completar el método de restauración de volúmenes.

9. Para ver las comprobaciones de elegibilidad para obtener una rápida restauración e información sobre comprobaciones obligatorias y anulables, haga clic en **Vista previa**.
10. En la página realizar operación, compruebe la información que ha proporcionado y haga clic en **Restaurar**.
11. Para ver detalles sobre el proceso, haga clic en **Detalles de la operación**.

Información de copyright

Copyright © 2023 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.