Agente de Arcserve® Unified Data Protection para Linux

Guía del usuario

Versión 5.0

arcserve®

Contactar con Soporte de Arcserve

El equipo de Soporte de Arcserve ofrece un conjunto importante de recursos para resolver las incidencias técnicas y proporciona un fácil acceso a la información relevante del producto.

https://www.arcserve.com/support

Con Soporte de Arcserve:

- Se puede estar en contacto directo con la misma biblioteca de información que se comparte internamente por nuestros expertos de Soporte de Arcserve. Este sitio le proporciona el acceso a los documentos de nuestra base de conocimiento (KB). Desde aquí se pueden buscar fácilmente los artículos de la KB relacionados con el producto que contienen soluciones probadas para muchas de las principales incidencias y problemas comunes.
- Se puede utilizar nuestro vínculo Conversación en vivo para iniciar instantáneamente una conversación en tiempo real con el equipo de Soporte de Arcserve. Con la Conversación en vivo, se pueden obtener respuestas inmediatas a sus asuntos y preguntas, mientras todavía se mantiene acceso al producto.
- Se puede participar en la Comunidad global de usuarios de Arcserve para preguntar y responder a preguntas, compartir sugerencias y trucos, discutir prácticas recomendadas y participar en conversaciones con sus pares.
- Se puede abrir un ticket de soporte. Al abrir un ticket de soporte en línea se puede esperar una devolución de llamada de uno de nuestros expertos en el área del producto por el que está preguntando.
- Se puede acceder a otros recursos útiles adecuados para su producto de Arcserve.

Contenido

Capítulo 1: Funcionamiento del Agente de Arcserve UDP (Linux)

Esta sección contiene los siguientes temas:

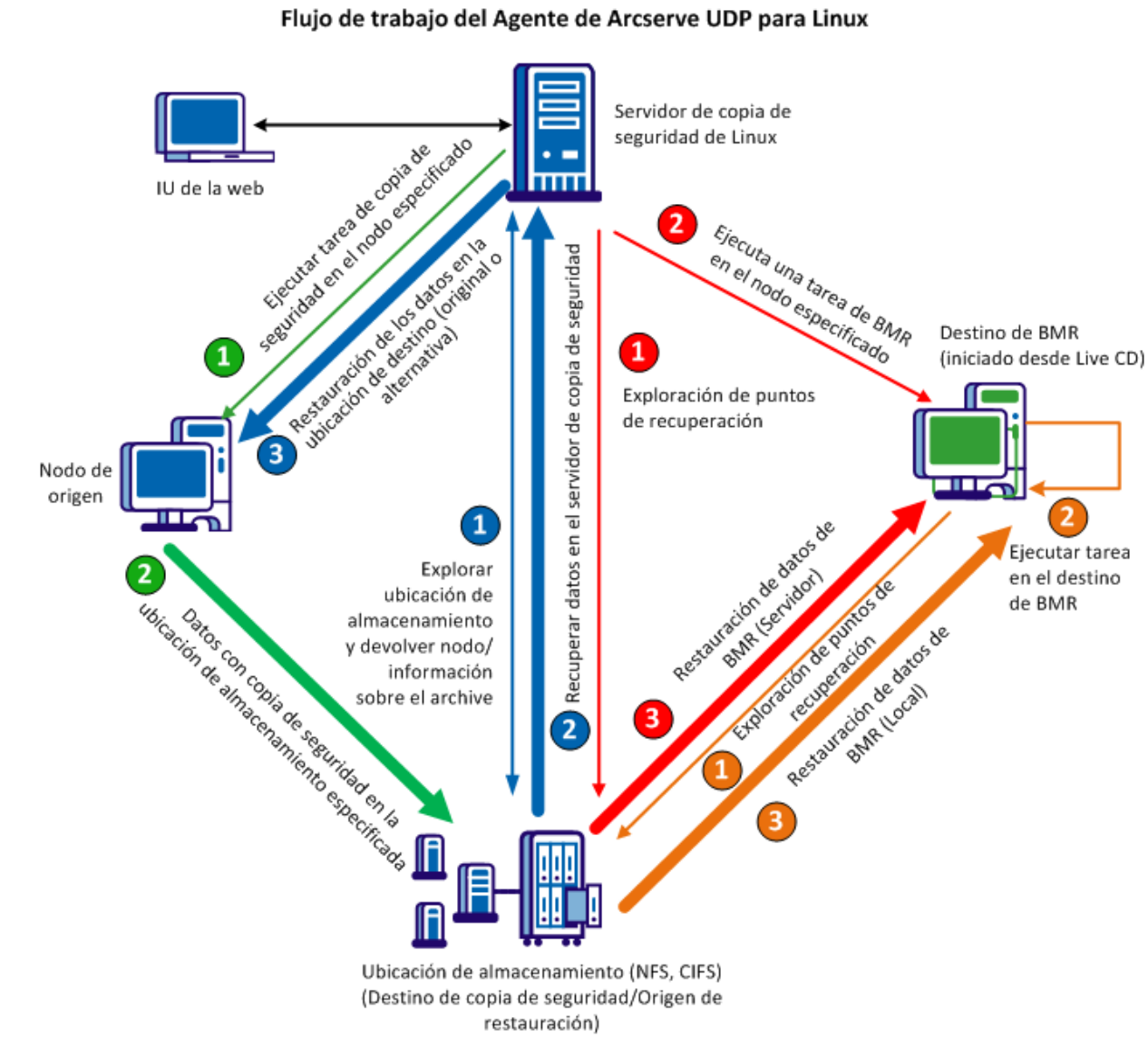
Introducción

Agente de Arcserve Unified Data Protection para Linux (Agente de Arcserve UDP (Linux)) es un producto de copia de seguridad basado en disco diseñado para los sistemas operativos de Linux. Proporciona una forma rápida, simple y fiable de proteger y recuperar información del negocio importante. El Agente de Arcserve UDP (Linux) realiza un seguimiento de los cambios de un nodo a nivel de bloque y, a continuación, realiza una copia de seguridad solamente de los bloques modificados en un proceso incremental. Como resultado, el Agente de Arcserve UDP (Linux) permite realizar copias de seguridad frecuentes, reduciendo el tamaño de cada copia de seguridad incremental (y de la ventana de copia de seguridad) y proporcionando copias de seguridad más actualizadas. El Agente de Arcserve UDP (Linux) también proporciona la capacidad para restaurar archivos o carpetas y realizar una reconstrucción completa (BMR) de una copia de seguridad única. Se puede almacenar la información de copia de seguridad en un uso compartido del sistema de archivos de red (NFS), del sistema de archivos de Internet comunes (CIFS) o en el nodo de origen de la copia de seguridad.

BMR es el proceso de restauración de un sistema informático *a partir de una reconstrucción completa*. La reconstrucción completa es un equipo sin ningún sistema operativo, controladores ni aplicaciones de software. La restauración incluye la instalación del sistema operativo, de las aplicaciones de software, controladores y, a continuación, la restauración de los datos y de los valores de configuración. La reconstrucción completa es posible porque cuando el Agente de Arcserve UDP (Linux) realiza una copia de seguridad de los datos, también captura información relacionada con el sistema operativo, las aplicaciones instaladas y los controladores, entre otros. Después de finalizar la reconstrucción completa, el nodo de destino tiene el mismo sistema operativo y datos que el nodo de producción.

El Agente de Arcserve UDP (Linux) utiliza un enfoque prácticamente sin agente para permitir la protección rápida y flexible de todos los clientes de Linux. La función elimina totalmente la necesidad de instalar manualmente los agentes en cada nodo del cliente, por esta razón se automatiza completamente la detección, configuración y protección de todos los clientes de Linux. Se puede instalar el Agente de Arcserve UDP (Linux) para ayudar a proteger todo el entorno de producción de Linux. El servidor donde se instala el Agente de Arcserve UDP (Linux) se conoce como servidor de copia de seguridad. Después de instalar el Agente de Arcserve UDP (Linux), se puede conectar al servidor de copia de seguridad en una red y se podrá abrir la interfaz de usuario mediante un explorador web.

El diagrama siguiente muestra el flujo global de operaciones del Agente de Arcserve UDP (Linux):


Flujo de trabajo del Agente de Arcserve UDP para Linux
IU de la web
Servidor de copia de seguridad de Linux
Ejecutar tarea de copia de seguridad en el nodo especificado
Restauración de los datos en la ubicación de destino (original o alternativa)
Nodo de origen
Explorar ubicación de almacenamiento y devolver nodo/ información sobre el archive
Recuperar datos en el servidor de copia de seguridad
Datos con copia de seguridad en la ubicación de almacenamiento especificada
Ejecuta una tarea de BMR en el nodo especificado
Exploración de puntos de recuperación
Destino de BMR (iniciado desde Live CD)
Restauración de datos de BMR (Servidor)
Exploración de puntos de recuperación
Restauración de datos de BMR (Local)
Ejecutar tarea en el destino de BMR
Ubicación de almacenamiento (NFS, CIFS) (Destino de copia de seguridad/Origen de restauración)
Leyenda
Un equipo que explora la IU de la web del Agente de Arcserve UDP para Linux, por ejemplo, un equipo de Windows
El servidor de copia de seguridad de Linux donde se instala el Agente de Arcserve UDP para Linux
Los nodos de Linux de los cuales se desea realizar una copia de seguridad (nodo de copia de seguridad)
Copia de seguridad prácticamente sin agente
Nodo de destino de BMR donde desea recuperar los datos y/o las aplicaciones
NFS o NAS donde se almacenan los datos de copia de seguridad
Copia de seguridad – Comandos/flujo de datos
Restauración (nivel de archivo) - Comandos/flujo de datos
BMR (Servidor) – Comandos/flujo de datos
BMR (Local) – Comandos/flujo de datos

Capítulo 2: Instalación/desinstalación del Agente de Arcserve UDP (Linux)

Esta sección contiene los siguientes temas:

Cómo instalar el Agente de Arcserve UDP (Linux)

Instale el Agente de Arcserve UDP (Linux) en un servidor de Linux para proteger y gestionar todos los nodos de origen de la copia de seguridad desde una IU. No es necesario instalar este software en los nodos de origen de la copia de seguridad.

El siguiente diagrama muestra el proceso para instalar el Agente de Arcserve UDP (Linux):

Realice estas tareas para instalar el Agente de Arcserve UDP (Linux):

- Instalación del Agente de Arcserve UDP (Linux) (en la página 16)
- Verificación de la instalación (en la página 19)
- Consideraciones sobre la instalación (en la página 16)

Consideraciones sobre la instalación

Tenga en cuenta los puntos siguientes antes de empezar la instalación:

- Cuando se realiza un protocolo Medio de ejecución anterior al inicio (PXE) basado en la reconstrucción completa, el servidor de Agente de Arcserve Unified Data Protection para Linux y los nodos de origen de producción tienen que estar en la misma subred. Si no están en la misma subred, asegúrese de que haya una puerta de enlace para enviar los paquetes de difusión de PXE a través de subredes.
- Si el destino de la copia de seguridad es un servidor de NFS, asegúrese de que el servidor de NFS admita el *bloqueo.* Verifique también que el usuario raíz disponga de acceso de escritura en los nodos de Linux.
- Para utilizar un servidor de NFS como destino de la copia de seguridad, instale el paquete de cliente de NFS en los nodos de Linux.
- Se instalan Perl y SSHD (Daemon de SSH) en el servidor de Linux y en los nodos de Linux de los que se desea realizar la copia de seguridad.
- No se admite la instalación silenciosa o desatendida.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Instalación del Agente de Arcserve UDP (Linux)

Instale el Agente de Arcserve UDP (Linux) en un servidor de copia de seguridad para gestionar operaciones de copia de seguridad y restauración. Después desinstalar el Agente de Arcserve UDP (Linux), se puede abrir la interfaz de usuario desde cualquier equipo mediante un explorador web y se hace referencia al servidor como servidor de copia de seguridad.

Al inicio de la instalación, el script de instalación verifica si algunas de las aplicaciones obligatorias se instalan en el servidor de Linux y si estas se están ejecutando.

Las siguientes aplicaciones obligatorias se requieren para que funcione el archivo de instalación:

- SSHD (Daemon de SSH)
- Perl

El archivo de instalación también verifica las siguientes aplicaciones opcionales al inicio de la instalación:

- rpc.statd: el servidor de NFS utiliza esta aplicación para implementar el bloqueo del archivo.
- mkisofs: el Agente de Arcserve UDP (Linux) utiliza esta aplicación para crear un Live CD.
- mount.nfs: el Agente de Arcserve UDP (Linux) utiliza esta aplicación para montar el servidor de NFS.
- mount.cifs: el Agente de Arcserve UDP (Linux) utiliza esta aplicación para montar el servidor de CIFS.
- ether-wake: el Agente de Arcserve UDP (Linux) utiliza esta aplicación para enviar la solicitud de Wake-on-LAN.

Nota: Asegúrese de que el servidor de copia de seguridad tenga una memoria mínima de 1 GB. Para obtener más información sobre los requisitos del sistema para un servidor de copia de seguridad, consulte las *Notas de la versión*.

Siga estos pasos:

1. Inicie sesión en el servidor de Linux como usuario raíz.
2. Descargue el paquete de instalación del Agente de Arcserve UDP (Linux) (archivo *.bin) y el archivo de paquete de utilidad de restauración en la carpeta raíz.

   Importante: Cuando se descargan los dos archivos del paquete de instalación en una carpeta local, la ruta completa de esta carpeta local no debe contener espacios en blanco. Además, debe incluir solamente los siguientes caracteres: a-z, A-Z, 0-9, - y _.
3. Proporcione los permisos de ejecución al paquete de instalación.

4. Realice uno de los siguientes pasos en función de la ubicación del paquete de instalación y el paquete de utilidad de restauración:

   - Si el paquete de instalación y el paquete de utilidad de restauración están en la misma carpeta, a continuación ejecute el siguiente comando para iniciar la instalación:

     ```
     ./<linux_installation_file_name>.bin
     ```

     Nota: Si se renombra el paquete de utilidad de restauración, el nombre del paquete deberá incluir los caracteres de utilidad de restauración para que el comando de instalación encuentre automáticamente el paquete de utilidad de restauración y lo instale. Si el nombre del paquete no tiene los caracteres de utilidad de restauración, se deberá proporcionar la ruta completa del paquete de utilidad de restauración.

     El paquete de instalación verifica la plataforma compatible y muestra un mensaje de confirmación.

     Si se detecta una plataforma no compatible, escriba Y y pulse Intro para confirmar la instalación de una plataforma no compatible.

   - Si el paquete de instalación y de utilidad de restauración están en carpetas diferentes, indique la ruta del paquete de utilidad de restauración en el primer parámetro:

     ```
     ./<linux_installation_file_name>.bin –-path=/<path_of_the
     restore-utility_package>
     ```

     El paquete de instalación verifica la plataforma compatible y muestra un mensaje de confirmación.

     Si se detecta una plataforma no compatible, escriba Y y pulse Intro para confirmar la instalación de una plataforma no compatible.

   Nota: Si se detecta un sistema operativo que no está en inglés, se pedirá que seleccione el idioma aplicable antes de continuar con el proceso de instalación.

5. Escriba Y y pulse Intro para confirmar la instalación.

   El paquete de instalación muestra la información del acuerdo de licencia.

6. Escriba Y y pulse Intro para aceptar el acuerdo de autorización.

   Se inicia el proceso de instalación del Agente de Arcserve UDP (Linux).

   Cuando la instalación del paquete de la utilidad de restauración se complete, aparecerá la información sobre la generación del Live CD.

   El Live CD se genera en la siguiente ubicación:

   ```
   /opt/CA/d2dserver/packages
   ```

   Nota: Si el Live CD para obtener la dirección IP del nodo de destino al llevar a cabo una reconstrucción completa (BMR).

Se instala el Agente de Arcserve UDP (Linux) y aparecerá la dirección URL para explorar el servidor de copia de seguridad.

Nota: Garantice que los puertos entrantes siguientes estén activados en el cortafuegos del servidor de copia de seguridad:

- Puerto TCP 22 (servidor de SSH)
- Puerto de transmisión 67 (servidor de arranque)
- 8014 (servicio web del agente)
- Protocolo de datagramas de usuario (UDP) puerto 69 (servidor de TFTP)

Garantice que el puerto entrante siguiente esté activado en el cortafuegos para los nodos del cliente de los cuales se desea realizar copia de seguridad:

- Puerto TCP 22 (servidor de SSH)

Asegúrese de que el puerto saliente necesario para NFS, CIFS o ambos destinos de copia de seguridad estén activados en el cortafuegos para el servidor de copia de seguridad y los nodos del cliente.

El Agente de Arcserve UDP (Linux) se ha instalado correctamente.

Verificación de la instalación

Verifique que la instalación finalice después de instalar el Agente de Arcserve UDP (Linux).

Siga estos pasos:

1. Abra un explorador web desde cualquier equipo de Windows.
2. Introduzca la dirección URL del servidor de copia de seguridad que aparece en la pantalla de instalación.

   Ejemplo: https://hostname:8014

   Se abrirá la página de inicio de sesión del Agente de Arcserve UDP (Linux).
3. Introduzca las credenciales de inicio de sesión raíz y haga clic en Iniciar sesión.

   Aparecerá la interfaz de usuario deL Agente de Arcserve UDP (Linux).

El Agente de Arcserve UDP (Linux) se instala y se verifica correctamente.

Cómo desinstalar el Agente de Arcserve UDP (Linux)

Desinstale el Agente de Arcserve UDP (Linux) del servidor de copia de seguridad de Linux para detener la protección de todos los nodos.

El diagrama de flujo siguiente muestra el proceso de desinstalación del Agente de Arcserve UDP (Linux):

Realice estas tareas para desinstalar el Agente de Arcserve UDP (Linux):

- Revise las consideraciones de desinstalación (en la página 20)
- Desinstalación del Agente de Arcserve UDP (Linux) (en la página 20)
- Verificación de la desinstalación (en la página 21)

Revise las consideraciones de desinstalación

Tenga en cuenta los puntos siguientes antes de empezar la desinstalación:

- Dispone de las credenciales de inicio de sesión raíz para el servidor de copia de seguridad.
- No tiene tareas en ejecución. Si se está ejecutando una tarea, no se puede desinstalar el Agente de Arcserve UDP (Linux).
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Desinstalación del Agente de Arcserve UDP (Linux)

Se puede desinstalar el Agente de Arcserve UDP (Linux) de la línea de comandos del servidor de copia de seguridad. El proceso de desinstalación elimina todos los archivos y los directorios que se crean durante la instalación del software.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Vaya a la carpeta *bin* donde se instala Agente de Arcserve Unified Data Protection para Linux con el comando siguiente:

   ```
   # cd /opt/CA/d2dserver/bin/
   ```

3. Ejecute el comando siguiente para desinstalar el Agente de Arcserve UDP (Linux):

   ```
   # ./d2duninstall
   ```

   Aparece un mensaje después de finalizar la desinstalación.

El Agente de Arcserve UDP (Linux) se desinstala del servidor.

Verificación de la desinstalación

Verifique que el Agente de Arcserve UDP (Linux) se elimina del servidor después de finalizar el proceso de desinstalación.

Vaya a la siguiente carpeta y verifique que el Agente de Arcserve UDP (Linux) se ha eliminado:

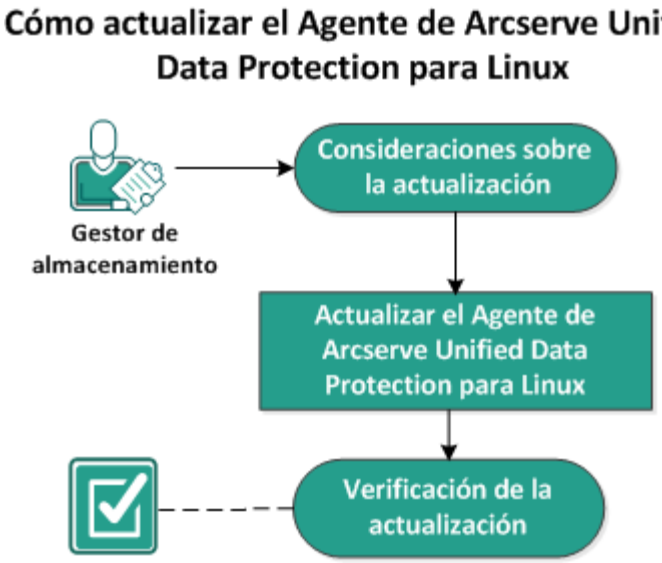
```
/opt/CA/d2dserver
```

Se ha verificado la desinstalación del Agente de Arcserve UDP (Linux). Se elimina el Agente de Arcserve UDP (Linux) del servidor de Linux.

Cómo actualizar el Agente de Arcserve UDP (Linux)

Actualice el Agente de Arcserve UDP (Linux) a la siguiente versión para poner a disposición de los usuarios las modificaciones y mejoras en las funciones y rendimiento del Agente de Arcserve UDP (Linux).

El siguiente diagrama muestra el proceso de actualización del Agente de Arcserve UDP (Linux):



Realice estas tareas para actualizar el Agente de Arcserve UDP (Linux):

- Consideraciones sobre la actualización (en la página 22)
- Actualización del Agente de Arcserve UDP (Linux) (en la página 23)
- Verificación de la actualización (en la página 25)

Consideraciones sobre la actualización

Tenga en cuenta los puntos siguientes antes de empezar la actualización:

- Garantice que se programa la actualización cuando no haya ninguna tarea de copia de seguridad en ejecución.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Actualización del Agente de Arcserve UDP (Linux)

Actualice el Agente de Arcserve UDP (Linux) a la siguiente versión para poner a disposición de los usuarios las modificaciones y mejoras en las funciones y rendimiento del Agente de Arcserve UDP (Linux).

Cuando se instala la actualización, el Agente de Arcserve UDP (Linux) intenta detectar una instalación existente.

- Si el Agente de Arcserve UDP (Linux) detecta una instalación existente, automáticamente se realiza el proceso de actualización. Todas las configuraciones existentes (p. ej. archivos de configuración, base de datos) se guardan y se actualizan.
- Si el Agente de Arcserve UDP (Linux) no detecta ninguna instalación existente, se realiza automáticamente una nueva instalación.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Descargue el paquete de instalación del Agente de Arcserve UDP (Linux) (archivo *.bin) y el archivo de paquete de utilidad de restauración en la carpeta raíz.

   Importante: Cuando se descargan los dos archivos del paquete de instalación en una carpeta local, la ruta completa de esta carpeta local no debe contener espacios en blanco. Además, debe incluir solamente los siguientes caracteres: a-z, A-Z, 0-9, - y _.
3. Proporcione los permisos de ejecución al paquete de instalación.

4. Realice uno de los siguientes pasos en función de la ubicación del paquete de instalación y el paquete de utilidad de restauración:

   - Si el paquete de instalación y el paquete de utilidad de restauración están en la misma carpeta, a continuación ejecute el siguiente comando para iniciar la instalación:

     ```
     ./<linux_installation_file_name>.bin
     ```

     Nota: Si se renombra el paquete de utilidad de restauración, el nombre del paquete deberá incluir los caracteres de utilidad de restauración para que el comando de instalación encuentre automáticamente el paquete de utilidad de restauración y lo instale. Si el nombre del paquete no tiene los caracteres de utilidad de restauración, se deberá proporcionar la ruta completa del paquete de utilidad de restauración.

     El paquete de instalación verifica la plataforma compatible y muestra un mensaje de confirmación.

     Si se detecta una plataforma no compatible, escriba Y y pulse Intro para confirmar la instalación de una plataforma no compatible.

   - Si el paquete de instalación y de utilidad de restauración están en carpetas diferentes, indique la ruta del paquete de utilidad de restauración en el primer parámetro:

     ```
     ./<linux_installation_file_name>.bin –-path=/<path_of_the
     restore-utility_package>
     ```

     El paquete de instalación verifica la plataforma compatible y muestra un mensaje de confirmación.

     Si se detecta una plataforma no compatible, escriba Y y pulse Intro para confirmar la instalación de una plataforma no compatible.

   El paquete de instalación detecta una instalación existente y se muestra un mensaje de confirmación para la actualización.

5. (Opcional) Escriba Y y pulse Intro para confirmar las dependencias de la aplicación.

   El paquete de instalación verifica las dependencias de la aplicación.

6. Escriba Y y pulse Intro para confirmar la instalación.

   El paquete de instalación muestra la información del acuerdo de licencia.

7. Escriba Y y pulse Intro para aceptar el acuerdo de autorización.

   Se inicia el proceso de instalación del Agente de Arcserve UDP (Linux).

   Cuando la instalación del paquete de la utilidad de restauración se complete, aparecerá la información sobre la generación del Live CD.

   El Live CD se genera en la siguiente ubicación:

   `/opt/CA/d2dserver/packages`

   Nota: Si el Live CD para obtener la dirección IP del nodo de destino al llevar a cabo una reconstrucción completa (BMR).

El Agente de Arcserve UDP (Linux) se ha actualizado correctamente.

Verificación de la actualización

Verifique que la actualización ha finalizado después de actualizar el Agente de Arcserve UDP (Linux) a la versión siguiente. El servidor de copia de seguridad almacena una copia de seguridad de los archivos de configuraciones existentes. Después de finalizar la verificación, suprima la copia de seguridad de los archivos de configuración existentes.

Siga estos pasos:

1. Abra un explorador web desde cualquier equipo de Windows.
2. Introduzca la dirección URL del servidor de copia de seguridad.

   Ejemplo: https://hostname:8014

   Se abrirá la página de inicio de sesión del Agente de Arcserve UDP (Linux).
3. Introduzca las credenciales de inicio de sesión raíz y haga clic en Iniciar sesión.

   Aparecerá la interfaz de usuario deL Agente de Arcserve UDP (Linux).
4. Verifique que el servidor de copia de seguridad funciona correctamente.
5. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
6. Vaya a la carpeta d2dserver.bak y suprima la carpeta.

   `/opt/CA/d2dserver.bak`

El Agente de Arcserve UDP (Linux) se ha actualizado y verificado correctamente.

Capítulo 3: Interfaz de usuario

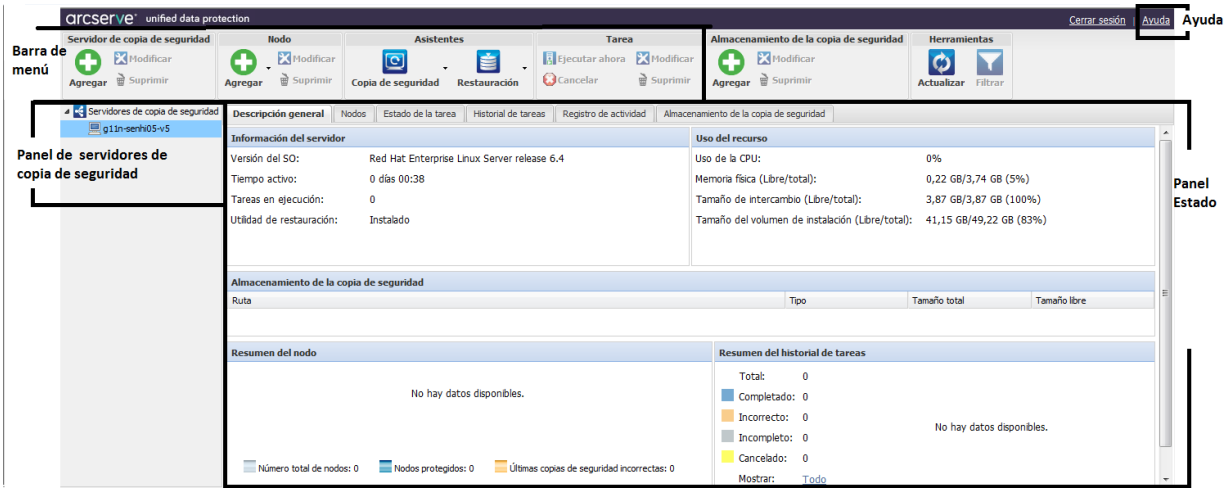
Esta sección contiene los siguientes temas:

Cómo moverse por la interfaz de usuario del Agente de Arcserve UDP (Linux) (en la página 27)

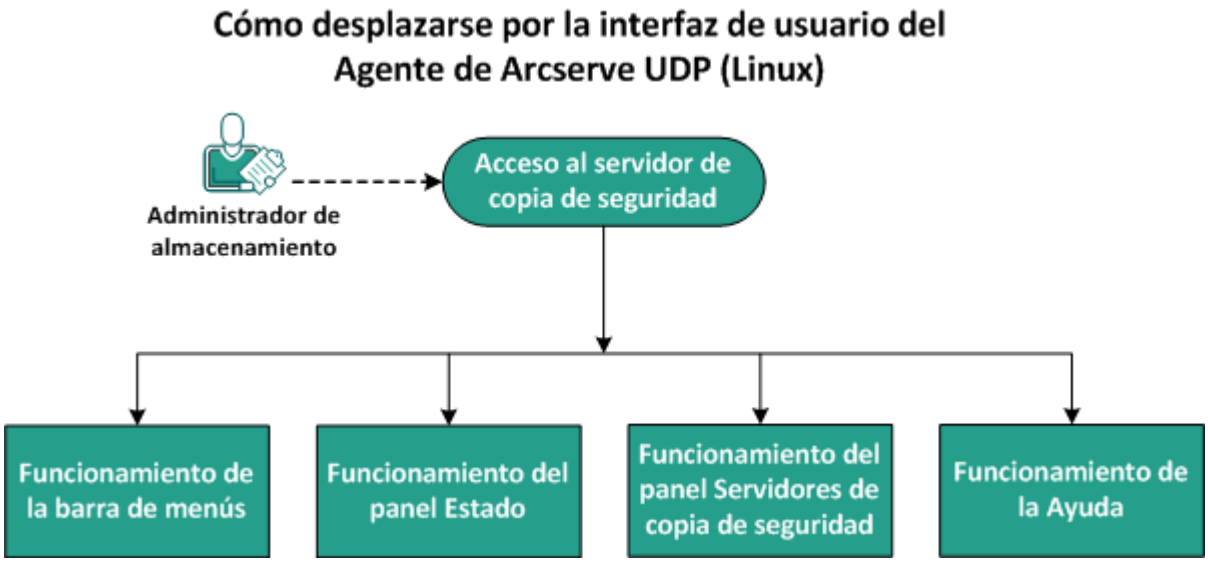
Cómo moverse por la interfaz de usuario del Agente de Arcserve UDP (Linux)

Antes de empezar a utilizar el Agente de Arcserve UDP (Linux), debe familiarizarse con la interfaz de usuario (IU). En la interfaz se pueden gestionar nodos, ubicaciones de almacenamiento de la copia de seguridad, tareas de copia de seguridad y de restauración, así como acceder a los temas de ayuda.

La interfaz de la página principal incluye cuatro áreas principales: barra de menús, panel Estado, panel Servidores de copia de seguridad y Ayuda.



El diagrama siguiente muestra el proceso para navegar por la interfaz del Agente de Arcserve UDP (Linux):



Realice estas tareas para familiarizarse con la interfaz del servidor de copia de seguridad:

- Acceso al servidor de copia de seguridad (en la página 29)
- Funcionamiento de la barra de menús (en la página 29)
- Funcionamiento del panel Estado (en la página 32)
- Funcionamiento del panel Servidores de copia de seguridad (en la página 36)
- Funcionamiento de la Ayuda (en la página 37)

Acceso al servidor de copia de seguridad

Como gestor del almacenamiento se puede acceder al servidor de copia de seguridad mediante la interfaz web. Inicie sesión con las credenciales raíz y no raíz para acceder al servidor de copia de seguridad. Utilice la dirección IP que se ha recibido durante la instalación del Agente de Arcserve UDP (Linux) para iniciar sesión en el servidor. Si se ha registrado el nombre de host del servidor, se podrá iniciar sesión en el servidor mediante el nombre de host.

Nota: Para obtener más información sobre el aprovisionamiento de permisos de inicio de sesión a los usuarios no raíz, consulte Concesión de permisos de inicio de sesión a los usuarios no raíz.

Siga estos pasos:

1. Abra un explorador web y escriba la dirección IP del servidor de copia de seguridad.

   Nota: De forma predeterminada, el servidor de copia de seguridad sigue el protocolo HTTPS y utiliza el puerto 8014.

2. Introduzca las credenciales de inicio de sesión y haga clic en Iniciar sesión.

   Se abre la interfaz del servidor de copia de seguridad.

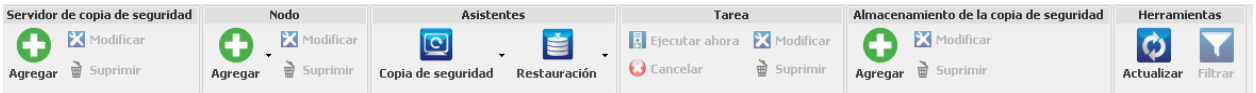
Se puede acceder correctamente al servidor de copia de seguridad.

Funcionamiento de la barra de menús

La barra de menús permite realizar las siguientes tareas:

- Gestionar servidores de copia de seguridad
- Gestionar nodos
- Gestionar tareas de copia de seguridad
- Gestionar tareas de restauración
- Gestionar ubicaciones de almacenamiento de copia de seguridad
- Filtrar búsquedas
- Actualizar páginas

La siguiente pantalla muestra la barra de menús:



La barra de menús incluye las siguientes opciones:

Servidor de copia de seguridad

Permite agregar, modificar y suprimir los servidores que tienen instalado el Agente de Arcserve UDP (Linux). Se puede instalar el Agente de Arcserve UDP (Linux) en varios servidores y estos se podrán gestionar desde una IU central. Los nodos que gestiona el servidor seleccionado aparecen en el panel Estado. Todos los servidores agregados se muestran en el panel Servidores de copia de seguridad. No se puede modificar ni suprimir el servidor central. Un servidor central es el primer servidor que se muestra en el panel Servidores de copia de seguridad. Se pueden modificar y suprimir otros servidores del panel Servidores de copia de seguridad. El botón Modificar permite actualizar solamente el número de puerto de los servidores.

Nodo

Permite agregar, modificar y suprimir los nodos de los cuales se desea realizar copia de seguridad. Los nodos son los equipos de los cuales se desea realizar copia de seguridad. Se pueden agregar varios nodos de los que se debe realizar copia de seguridad. También se puede detectar los nodos que están presentes en la red mediante un script. Se pueden agregar como máximo 200 nodos por cada servidor.

Si se suprime un nodo, el servidor de copia de seguridad borra toda la información acerca del nodo de la base de datos, incluyendo la información de la tarea de copia de seguridad. El servidor de copia de seguridad también suprime los controladores del nodo. Se puede tardar un poco de tiempo en suprimir completamente los controladores.

Asistentes

Permite iniciar el Asistente de copia de seguridad y el Asistente de restauración para ayudar a guiarse mediante el proceso de copia de seguridad y de restauración.

- El Asistente de copia de seguridad contiene una lista desplegable con tres opciones disponibles:

  Copia de seguridad

  Utilice esta opción si no se han agregado previamente nodos de los que se tiene que realizar copia de seguridad. Si se selecciona esta opción se inicia el Asistente de copia de seguridad y será posible agregar los nodos durante el proceso.

  Realizar la copia de seguridad de los nodos seleccionados

  Utilice esta opción si se han agregado previamente los nodos antes de iniciar el Asistente de copia de seguridad. Si se hace clic en Realizar copia de seguridad de los nodos seleccionados sin agregar ningún nodo o seleccionando los existentes, obtendrá un mensaje de error. Para evitar este error, seleccione el nodo en la ficha Nodos y, a continuación, seleccione Realizar la copia de seguridad de los nodos seleccionados.

Agregar nodos seleccionados a una tarea existente

Utilice esta opción si ya tiene una tarea de copia de seguridad existente y desea aplicar los mismos valores de configuración de copia de seguridad a los nuevos nodos. No es necesario configurar el Asistente de copia de seguridad.

- El Asistente de restauración contiene una lista desplegable con tres opciones disponibles:

  Reconstrucción completa (BMR)

  Utilice esta opción para realizar una reconstrucción completa. Se puede realizar una reconstrucción completa mediante la dirección IP o dirección MAC del equipo de reconstrucción completa que debe recuperarse.

  Restaurar un archivo

  Utilizar esta opción para realizar una restauración de nivel de archivo. Se pueden seleccionar los archivos específicos desde un punto de recuperación y restaurarlos.

Tarea

Permite gestionar las tareas que se han creado. Una tarea es una instancia de una operación de copia de seguridad o restauración. Después de crear una tarea de copia de seguridad para un nodo, no será necesario crear otra tarea para ejecutar una copia de seguridad para el mismo nodo la próxima vez. Sin embargo, es necesario crear una tarea de restauración cada vez que se desee realizar una reconstrucción completa.

Almacenamiento de copia de seguridad

Permite agregar y gestionar las ubicaciones de almacenamiento de la copia de seguridad. La ubicación de almacenamiento de la copia de seguridad puede ser un recurso compartido del sistema de archivos de red (NFS) o de un sistema de archivos de Internet comunes (CIFS) o local. Local es una ruta local en el servidor de copia de seguridad.

Cuando se agrega una ubicación de almacenamiento de copia de seguridad, se deben proporcionar las credenciales para la ubicación de almacenamiento de copia de seguridad seleccionada. Solamente se puede modificar el nombre de usuario y la contraseña del recurso compartido de CIFS. No se pueden modificar detalles del recurso compartido de NFS. Active la casilla de verificación Ejecutar script cuando el espacio libre sea menor de para ejecutar el script *backup_storage_alert.sh* cuando el espacio libre sea menor que el valor especificado. Este valor puede ser un porcentaje del espacio total en el destino de la copia de seguridad o una cantidad mínima de espacio (en MB) en el destino de la copia de seguridad. El script backup_storage_alert.sh se puede configurar para que envíe una alerta cuando el espacio libre disponible sea menor que el valor especificado.

Nota: Para obtener más información acerca de cómo configurar el script backup_storage_alert.sh, consulte *Cómo integrar y automatizar el Agente de Arcserve UDP (Linux) con el entorno de TI existente*.

Después de agregar una ubicación de almacenamiento de copia de seguridad, se podrá ver el tamaño total de los archivos y el espacio vacío en el panel Estado. Seleccione una ubicación de almacenamiento de la copia de seguridad para ver los puntos de recuperación y conjuntos de recuperación, así como el espacio que ha utilizado cada nodo de los que se ha realizado una copia de seguridad en la ubicación de almacenamiento de la copia de seguridad. Los almacenamientos de la copia de seguridad agregados aparecen también en la página Destino de copia de seguridad del Asistente de copia de seguridad y en la página Puntos de recuperación del Asistente de restauración.

Herramientas

El menú Herramientas incluye el botón Actualizar y el botón Filtro.

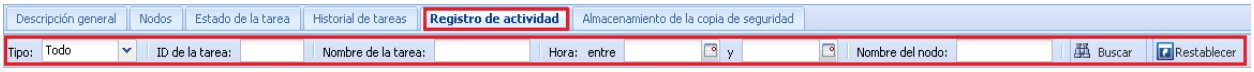
Actualizar

Permite actualizar el área de visualización seleccionada en el panel Estado, incluido el registro de actividad para ver los últimos mensajes de estado de copia de seguridad o restauración.

Filtro

Permite filtrar la información que se muestra en el panel Estado en función de la entrada. El botón Filtrar sirve de conmutador para que se puedan mostrar y ocultar filtros a través del mismo botón. Cuando se muestran los filtros, los campos de búsqueda se muestran en el panel Estado. Cuando se ocultan los filtros, los campos de búsqueda se eliminan del panel Estado.

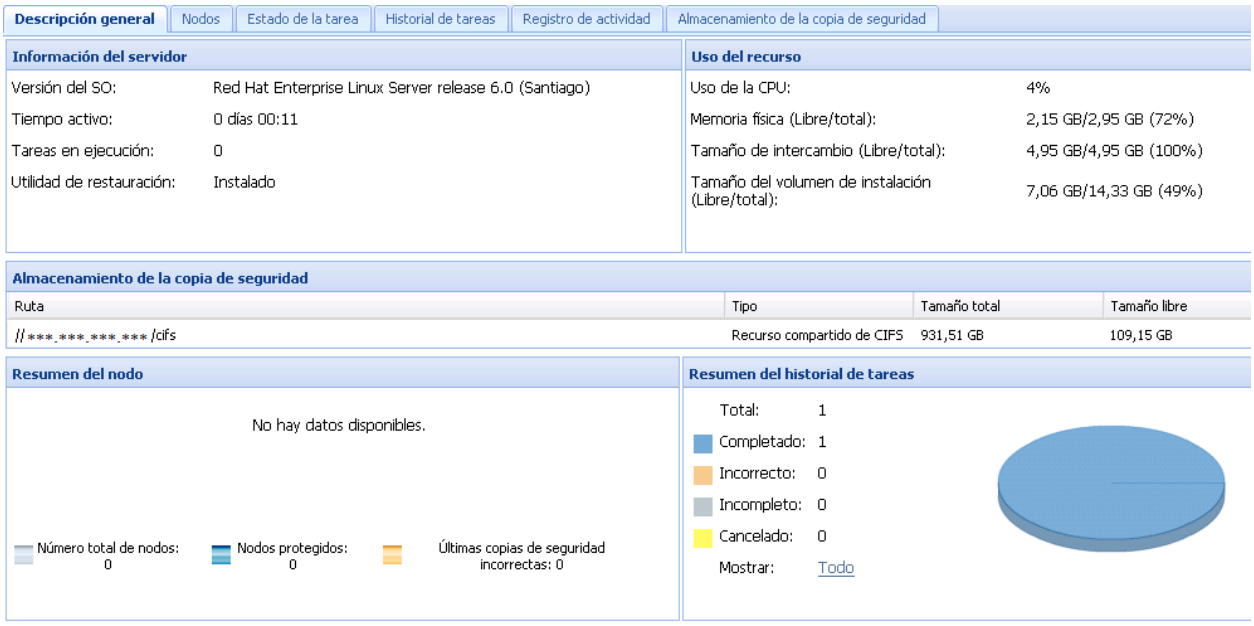
La siguiente pantalla muestra los filtros aplicados en el registro de actividad:



Funcionamiento del panel Estado

El panel Estado es el área que muestra toda la información en la IU. El panel Estado incluye seis fichas que permiten ver la información en función de la ficha seleccionada.

La siguiente pantalla muestra el panel Estado:



El panel Estado incluye las fichas siguientes:

Descripción general

Proporciona un resumen de los elementos siguientes:

Información del servidor

Aparece la versión del sistema operativo, el tiempo transcurrido desde el servidor iniciado y la información de la licencia para el Agente de Arcserve UDP (Linux). También aparece si la utilidad de restauración se instala en este servidor.

Uso del recurso:

Se muestra el uso de la CPU, la memoria física total y disponible y el tamaño de intercambio. También aparece el tamaño del volumen de instalación.

Almacenamiento de copia de seguridad

Muestra todas las ubicaciones de la sesión de copia de seguridad que se han agregado y el espacio disponible en cada ubicación. Esta información ayuda a planificar la ubicación de la copia de seguridad siguiente en función del espacio de almacenamiento disponible.

Resumen del nodo

Muestra una representación gráfica de los nodos que se protegen y de los nodos con las últimas copias de seguridad erróneas. Resumen del nodo incluye las categorías siguientes:

Número total de nodos muestra el número de nodos que se incluyen en el Agente de Arcserve UDP (Linux), sin tener en cuenta el estado de la copia de seguridad.

Nodos protegidos muestra el número de nodos con las copias de seguridad correctas más recientes y que deben protegerse en caso de que sea necesaria una recuperación.

Últimas copias de seguridad incorrectas muestra el número de nodos con las copias de seguridad incorrectas más recientes (erróneas, canceladas e incompletas). En función de la causa de la copia de seguridad errónea, algunos nodos pueden estar desprotegidos en caso de que sea necesaria una recuperación.

Resumen de historial de tareas

Aparece un gráfico de sectores que resume el historial de todas las tareas. El resumen no incluye las tareas en ejecución.

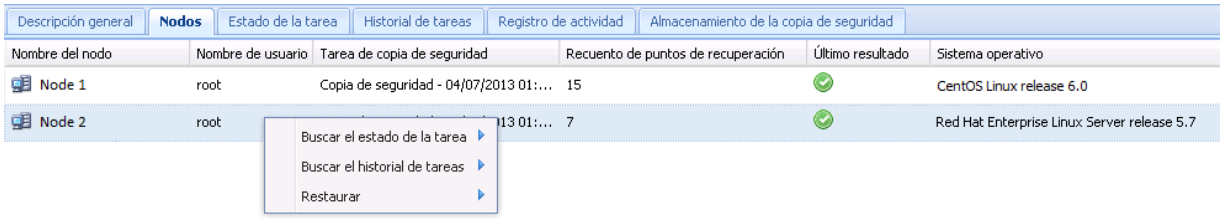
Los campos siguientes no son autoexplicativos:

Incompleto muestra el número de tareas que se han ejecutado correctamente con cambios menores. Por ejemplo, cuando se restauran archivos de Red Hat 6 en Red Hat 5, los archivos se restauran correctamente; sin embargo, faltan algunos atributos en los archivos restaurados.

Otros muestra el número de tareas canceladas.

Nodos

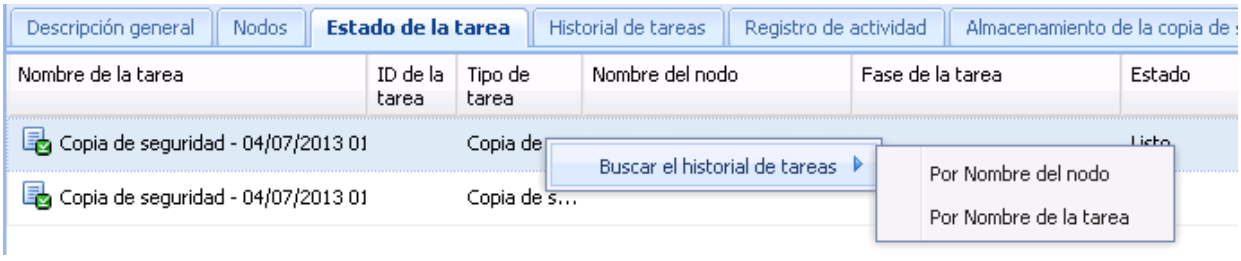
Muestra todos los nodos agregados al servidor de copia de seguridad. Se pueden aplicar filtros a la ficha Nodos para buscar los nodos obligatorios. La ficha Nodos también incluye un menú contextual. El menú contextual permite buscar el estado de la tarea o el historial de tareas del nodo seleccionado. El menú contextual también permite restaurar datos. Se puede filtrar el historial de tareas o el estado de la tarea usando el nombre de la tarea o el del nodo. Si se busca en el historial de tareas el nodo seleccionado, a continuación se abrirá la ficha Historial de tareas con el filtro de búsqueda aplicado en la ficha. De modo similar, si se busca el estado de la tarea, a continuación se abrirá la ficha Estado de la tarea con el filtro de búsqueda aplicado en la ficha. La opción Restaurar permite realizar reconstrucciones completas o restauraciones de nivel de archivo. Se abre el Asistente de restauración y se muestra todos los puntos de recuperación del nodo seleccionado.



Estado de tarea

Muestra la lista de tareas de copia de seguridad y de restauración que se crean, incluyendo el estado de cada tarea. Utilice esta ficha para ejecutar una tarea de copia de seguridad o de restauración y vuelva a ejecutar una tarea de copia de seguridad. Se puede ver el progreso de las tareas de copia de seguridad o de restauración que se ejecutan. Se pueden aplicar filtros a la ficha Estado de la tarea para buscar las tareas necesarias. La ficha Estado de la tarea también incluye un menú contextual. El menú contextual permite buscar el historial de tareas de la tarea seleccionada. Se puede filtrar el historial de tareas usando el nombre de la tarea o el del nodo. Si se busca el historial de tareas de la tarea seleccionada, la ficha Historial de tareas se abrirá a continuación con el filtro de búsqueda aplicado a la ficha.

La siguiente pantalla muestra el menú contextual en la ficha Estado de la tarea:



Historial de tarea

Aparece la lista de tareas de copia de seguridad y de restauración que se han ejecutado previamente. Se pueden aplicar filtros a la ficha Estado de la tarea para buscar el historial de tareas necesario. Cuando se selecciona una tarea, el estado de la tarea aparecerá al final de la página.

Registro de actividad

Aparece una lista de mensajes de procesamiento y mensajes de estado para las tareas de copia de seguridad y de restauración. Actualice el Registro de actividad para obtener los últimos mensajes para las tareas de copia de seguridad y de restauración recientes. Se pueden aplicar filtros a la ficha Registro de actividad para buscar registros de actividades obligatorios.

Almacenamiento de copia de seguridad

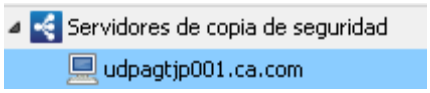
En la barra de menús aparecerá el destino de copia de seguridad que se ha agregado. Se puede ver el espacio de almacenamiento libre y gestionar el destino de copia de seguridad. Esta opción es útil si saber cuánto espacio libre hay disponible en cualquier destino de copia de seguridad particular para planificar la copia de seguridad. Cuando se agrega un almacenamiento de copia de seguridad, este destino aparecerá en el Asistente de copia de seguridad.

Funcionamiento del panel Servidores de copia de seguridad

El panel Servidores de copia de seguridad muestra la lista de servidores de copia de seguridad que gestiona el servidor actual. Se pueden agregar servidores en la barra de menús y pueden gestionarse todos los servidores desde una interfaz. Si se han agregado varios servidores, el panel Estado mostrará el estado del servidor seleccionado. Cada servidor puede gestionar, como mínimo, 200 nodos del cliente.

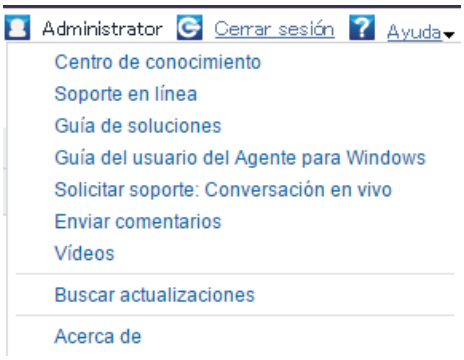
Normalmente, el primer servidor mostrado en el panel Servidores de copia de seguridad es el servidor de copia de seguridad central y otros servidores son servidores miembros. Si se gestionan varios servidores desde un servidor central, a continuación se deberá verificar que la versión del servidor central y los servidores miembros son idénticos.

La siguiente pantalla muestra el panel Servidores de copia de seguridad:



Funcionamiento de la Ayuda

El cuadro de diálogo Ayuda permite acceder a los temas de ayuda del Agente de Arcserve UDP (Linux). Puede realizar las siguientes tareas en la lista desplegable Ayuda:



Las siguientes opciones están disponibles en la lista desplegable Ayuda:

Centro de conocimiento

Permite acceder a la biblioteca.

Ayuda (HTML)

Permite acceder a la versión de HTML de la Guía del usuario del Agente de Arcserve UDP (Linux).

Guía del usuario

Permite acceder a la versión de PDF de la Guía del usuario del Agente de Arcserve UDP (Linux).

Acceso al Soporte técnico y a la comunidad

Permite acceder al sitio de soporte del Agente de Arcserve UDP (Linux) y a los sitios de comunidad de ARCserve. Se pueden realizar las siguientes tareas en Acceso al Soporte técnico y a la comunidad:

- Ver especificaciones de productos
- Acceder al sitio web oficial de ARCserve
- Enviar comentarios al equipo de desarrollo
- Leer sugerencias y comentarios de los expertos de ARCserve

- Hablar con un ejecutivo de soporte
- Suscribirse a fuentes RSS

Gestionar licencia

Permite acceder al cuadro de diálogo Gestión de licencias y gestionar todas las licencias desde una interfaz central.

Acerca de

Permite ver la información del producto (número de versión y de compilación) y acceder a las Notas de la versión de Arcserve UDP.

Capítulo 4: Utilización del Agente de Arcserve UDP (Linux)

Esta sección contiene los siguientes temas:

Cómo gestionar las licencias

Es necesario disponer de la licencia del Agente de Arcserve UDP (Linux) para tener acceso autorizado e ininterrumpido a los componentes relacionados. Además, si desea implementar Agente de Arcserve Unified Data Protection para Linux en ubicaciones remotas, puede autorizar estos sitios remotos para sacar provecho de los beneficios que el Agente de Arcserve UDP (Linux) proporciona.

El Agente de Arcserve UDP (Linux) funcionará durante un período de prueba de 30 días después de empezar a utilizarse. A continuación, aplique una clave de licencia adecuada para continuar utilizándolo. El Agente de Arcserve UDP (Linux) permite gestionar las licencias de todos los servidores de copia de seguridad de Linux desde una interfaz central.

El siguiente diagrama muestra el proceso de gestión de licencias:

Complete las siguientes tareas para gestionar las licencias:

- Acceso al gestor de licencias (en la página 40)
- Información general del cuadro de diálogo Gestión de licencias (en la página 41)
- Gestión de licencias (en la página 42)

Acceda al gestor de licencias.

Se debe acceder al cuadro de diálogo Gestión de licencias de la interfaz web del Agente de Arcserve UDP (Linux) para gestionar todas las licencias.

Siga estos pasos:

1. Inicie sesión en la interfaz web del Agente de Arcserve UDP (Linux).
2. En la página principal, haga clic en Ayuda, Gestionar licencia.

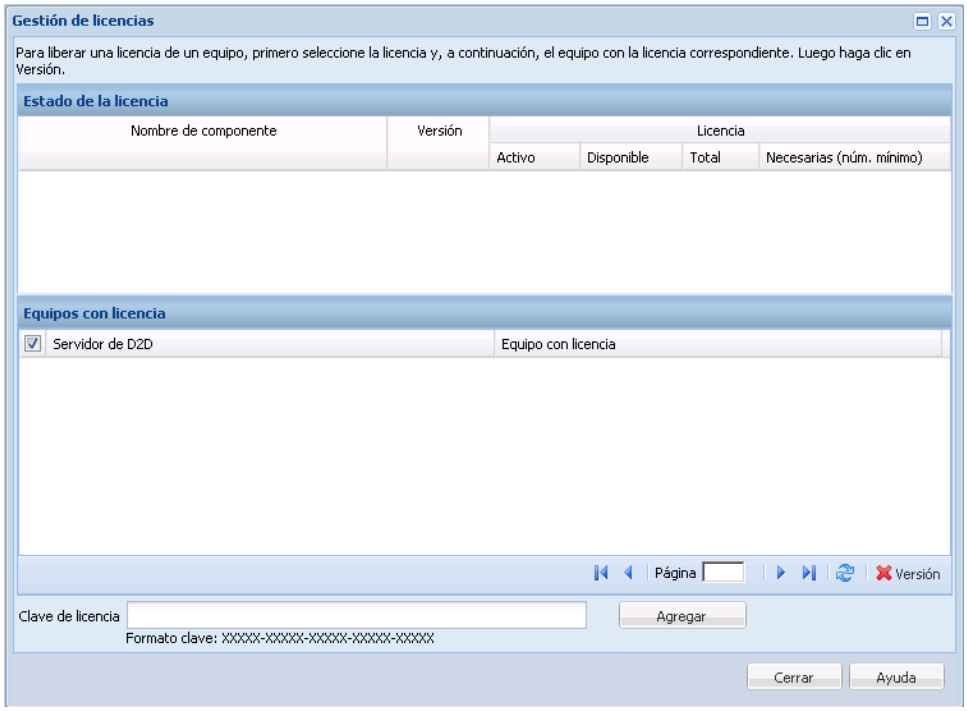
   Se abrirá el cuadro de diálogo Gestión de licencias.

Se accederá al gestor de licencias.

Información general del cuadro de diálogo Gestión de licencias

El cuadro de diálogo Gestión de licencias permite gestionar todas las licencias del Agente de Arcserve UDP (Linux). Se pueden gestionar las licencias de varios servidores de copia de seguridad de Linux desde una única interfaz.

La siguiente pantalla muestra el cuadro de diálogo Gestión de licencias:



El cuadro de diálogo Gestión de licencias se divide en dos secciones: Estado de la licencia y Equipos con licencia.

Estado de la licencia

Nombre de componente

Indica el nombre de la licencia.

Versión

Identifica el número de versión de la licencia.

Activo

Identifica el número de licencias que se están utilizando actualmente para realizar copia de seguridad de los nodos.

Disponible

Identifica el número de licencias que están todavía disponibles en la agrupación de licencias y que se pueden utilizar para realizar copia de seguridad de equipos de Linux.

Total

Identifica el número total de licencias que se han obtenido para realizar copia de seguridad del equipo. El total es la suma de licencias activas y disponibles.

Equipos con licencia

Servidor de copia de seguridad

Identifica el servidor de Linux donde se ha instalado el Agente de Arcserve UDP (Linux).

Equipos con licencia

Identifica los equipos de Linux para los cuales se ha aplicado una licencia de protección de dichos equipos.

Gestión de licencias

Se puede agregar y liberar licencias desde el cuadro de diálogo Gestión de licencias. La licencia agregada se muestra en el cuadro de diálogo Gestión de licencias. Si no se desea volver a realizar copia de seguridad de ningún equipo, se puede liberar la licencia de ese equipo.

Siga estos pasos:

- Para agregar una licencia, siga estos pasos:
  a. Compruebe la clave de licencia en el medio de instalación o en el certificado de licencia.
  b. Introduzca una clave de licencia en el campo Clave de licencia y haga clic en Agregar.
  c. Cierre y abra el cuadro de diálogo Gestión de licencias.

     La licencia se agrega y se muestra en el área Estado de la licencia.

- Para liberar una licencia, siga estos pasos:
  a. Seleccione la licencia en el área de Estado de la licencia.
  b. Seleccione el servidor de copia de seguridad en Equipos con licencia y haga clic en Liberar.
  c. Cierre y abra el cuadro de diálogo Gestión de licencias.

     La licencia se libera del equipo.

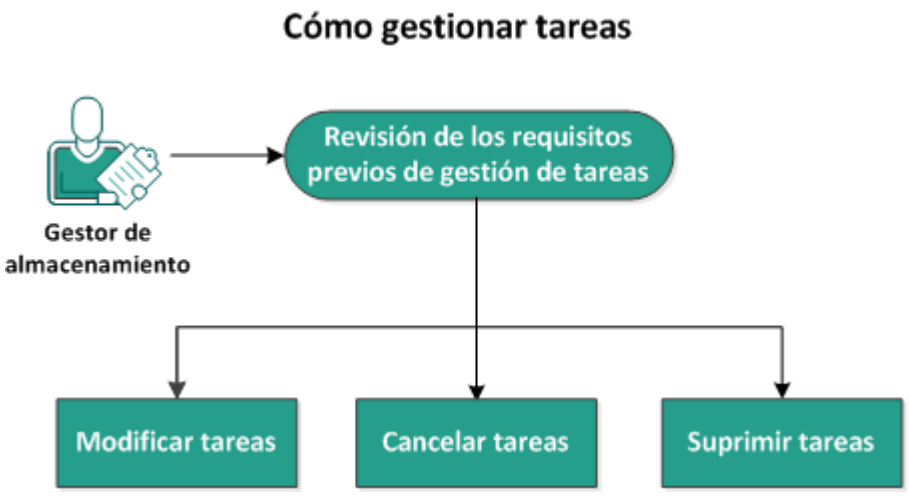
Las licencias se gestionan correctamente.

Cómo gestionar tareas

Después de crear una tarea de copia de seguridad o restauración, se pueden gestionar todas las tareas en el menú Tarea. La gestión de tareas incluye las siguientes tareas:

- Modificar una tarea
- Cancelación de una tarea
- Suprimir una tarea

El siguiente diagrama muestra el proceso de gestión de tareas:



Realice estas tareas para gestionar tareas:

- Revisión de los requisitos previos (en la página 44)
- Modificación de tareas (en la página 44)
- Cancelación de tareas (en la página 44)
- Supresión de tareas (en la página 45)

Revisión de los requisitos previos de gestión de tareas

Se deben tener los siguientes requisitos previos antes de gestionar tareas:

- Se debe disponer de una tarea existente válida para gestionar tareas.
- Se deben contar con los permisos adecuados para gestionar tareas.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Modificación de tareas

Se puede abrir cualquier tarea existente y modificar la configuración para la tarea de la interfaz web. Por ejemplo, si se desea cambiar el destino de la copia de seguridad para un equipo ya protegido, no se tendrá que crear una nueva tarea. Se puede abrir la tarea existente que protege el equipo y modificar solamente la sección de destino de la copia de seguridad. El resto de la configuración permanecerá sin modificaciones, excepto la configuración de destino de la copia de seguridad.

Siga estos pasos:

1. Seleccione una tarea en la ficha Estado de la tarea.
2. Haga clic en Modificar en el menú Tarea.

   Se abrirá el asistente para la tarea seleccionada.
3. Modifique la configuración en el asistente.
4. Haga clic en Enviar en la página Resumen del asistente.

   La tarea se envía y se ejecuta en función de la configuración.

La tarea se modifica correctamente.

Cancelación de tareas

Se puede cancelar una tarea en ejecución desde la interfaz web del Agente de Arcserve UDP (Linux).

Siga estos pasos:

1. Seleccione una tarea en la ficha Estado de la tarea.
2. Haga clic en Cancelar en el menú Tarea.

   Se abrirá el cuadro de diálogo Cancelar tarea.

3. Seleccione una de las siguientes opciones en la lista desplegable Cancelar tarea para:

   Nodo seleccionado

   Especifica que la tarea se cancela solamente para el nodo seleccionado.

   Todos los nodos protegidos por la tarea seleccionada

   Especifica que la tarea se cancela para todos los nodos que protege la tarea seleccionada.

4. Haga clic en Aceptar.

   Se cancela la tarea.

Supresión de tareas

Se puede suprimir una tarea cuando ya no se desee proteger o restaurar un equipo. Se puede suprimir también una tarea que protege un grupo de nodos. Cuando se suprime una tarea, los puntos de recuperación de los que se realizó previamente una copia de seguridad siguen estando disponibles en el destino de la copia de seguridad especificado. Se pueden utilizar estos puntos de recuperación para restaurar los datos.

En una tarea en ejecución, la opción Suprimir está inactiva. Se tendrá que cancelar la tarea en ejecución y, a continuación, suprimirla.

Siga estos pasos:

1. Seleccione una tarea en la ficha Estado de la tarea.
2. Haga clic en Suprimir en el menú Tarea.

   Se abrirá el cuadro de diálogo Eliminar tarea.

3. Seleccione una de las siguientes opciones en la lista desplegable Suprimir tarea para:

   Nodo seleccionado

   Especifica que la tarea se suprime solamente para el nodo seleccionado.

   Todos los nodos protegidos por la tarea seleccionada

   Especifica que la tarea se suprime para todos los nodos que protege la tarea seleccionada.

4. Haga clic en Aceptar.

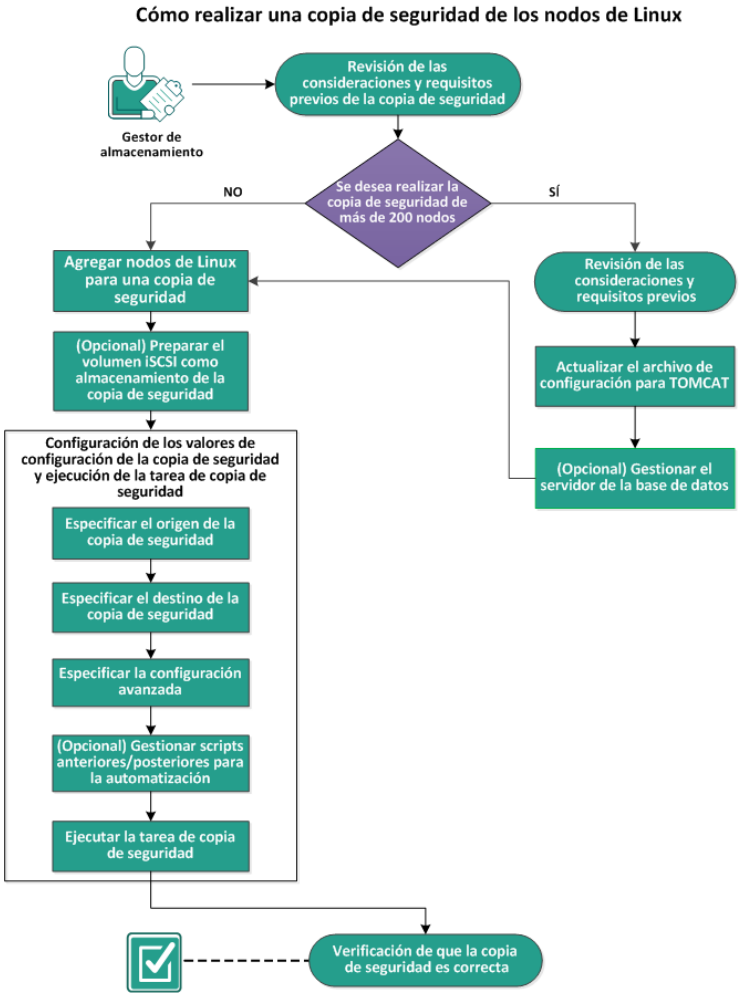
   Se suprime la tarea.

Cómo realizar una copia de seguridad de los nodos de Linux

El Agente de Arcserve UDP (Linux) permite realizar la copia de seguridad de los nodos de Linux y de los datos almacenados en él. Se puede realizar también la copia de seguridad del servidor de copia de seguridad como con cualquier otro nodo de Linux. El servidor de copia de seguridad puede realizar una copia de seguridad de un máximo de 200 nodos.

Cuando el Agente de Arcserve UDP (Linux) realiza una copia de seguridad de los datos, también captura información relacionada con el sistema operativo, las aplicaciones instaladas y los controladores, entre otros, desde el nodo de producción. Como resultado, cuando se restauran los datos de copia de seguridad, se puede realizar una reconstrucción completa o se pueden restaurar los archivos que necesite de forma específica.

El siguiente diagrama muestra cómo realizar una copia de seguridad de los nodos de Linux:



Realice estas tareas para realizar una copia de seguridad de un nodo de Linux:

- Revisión de las consideraciones y requisitos previos de la copia de seguridad (en la página 47)
- Se desea realizar la copia de seguridad de más de 200 nodos (en la página 49)
  - Revisión de las consideraciones y requisitos previos (en la página 50)
  - Actualización del archivo de configuración para TOMCAT. (en la página 51)
  - Gestión del servidor de la base de datos
- Adición de nodos de Linux para una copia de seguridad (en la página 52)
- (Opcional) Preparación del volumen iSCSI como almacenamiento de la copia de seguridad (en la página 55)
- Configuración de los valores de configuración de la copia de seguridad y ejecución de la tarea de copia de seguridad (en la página 57)
  - Especificación del origen de la copia de seguridad (en la página 57)
  - Cómo especificar el destino de copia de seguridad (en la página 60)
  - Especificación de la configuración avanzada (en la página 64)
    - (Opcional) Gestión de scripts anteriores/posteriores para la automatización (en la página 75)
  - Ejecución de la tarea de copia de seguridad (en la página 78)
- Verificación de que la copia de seguridad es correcta (en la página 78)

Revisión de las consideraciones y requisitos previos de la copia de seguridad

Verifique los requisitos siguientes antes de realizar una copia de seguridad:

- Tiene los requisitos de hardware y software que admite el nodo de la copia de seguridad.

  Nota: Para obtener más información sobre los requisitos de hardware y software admitidos, consulte las *Notas de la versión*.

- Tiene un destino válido para almacenar los datos de copia de seguridad.
- Tiene los nombres de usuario y las contraseñas de los nodos de los que desea realizar una copia de seguridad.
- La carpeta */tmp* del nodo de copia de seguridad tiene un mínimo de espacio de 300 MB. La carpeta */tmp* se utiliza para procesar la acumulación de bloques incrementales.
- Se instalan Perl y SSHD (Daemon de SSH) en los nodos de los que se desea realizar copia de seguridad.
- mount.nfs se ha instalado en los nodos de los que se desea realizar copia de seguridad.

- mount.cifs se ha instalado en los nodos de los que se desea realizar copia de seguridad.
- El nodo de copia de seguridad puede acceder al destino de la copia de seguridad y tiene permisos de escritura.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Para repetir una tarea de copia de seguridad, verifique que se ha realizado una copia de seguridad del nodo antes y de que dispone de una tarea de copia de seguridad válida.

Revise las siguientes consideraciones de copia de seguridad:

- Para optimizar la gestión de los puntos de recuperación, debería tener en cuenta las recomendaciones siguientes al programar la frecuencia de las copias de seguridad:
  - Para los sistemas que se protegen con copias de seguridad incrementales realizadas cada 15 minutos, debería programar una copia de seguridad completa todas las semanas (para actualizar la imagen base).
  - Para los sistemas que se protegen con copias de seguridad incrementales realizadas cada hora, debería programar una copia de seguridad completa cada mes (para actualizar la imagen base).

  Nota: Si le preocupa la cantidad de espacio utilizado para almacenar las imágenes de copia de seguridad, debería programar las copias de seguridad completas menos frecuentemente para consumir menos espacio de almacenamiento.

Disco admitido por el Agente de Arcserve UDP (Linux)

Hay varios tipos de disco compatibles con los discos de origen de copia de seguridad y los de copia de seguridad del Agente de Arcserve UDP (Linux). La matriz siguiente enumera los tipos de discos compatibles con cada función.

Compatibilidad con la copia de seguridad y la reconstrucción completa		
Tipo de disco (volumen)	**Como origen de copia de seguridad**	**Como destino de copia de seguridad**
Volumen montado (Partición de disco tradicional y LVM *2)	Sí	Sí
Volumen SIN FORMATO (Sin formato)	No	No
Intercambio	No	No aplicable
Disco GPT:		

Compatibilidad con la copia de seguridad y la reconstrucción completa		
■ Disco de datos (tabla de particiones GUID) de GPT	Sí	Sí
■ Disco de arranque (tabla de particiones GUI) de GPT	No	No aplicable
Disco de RAID *1:		
■ RAID de software (RAID-0 (secciones)	Sí	Sí
■ RAID de software (RAID-1 (reflejado)	Sí	Sí
■ Software RAID-5	Sí	Sí
■ Hardware RAID (incluye RAID incrustado)	Sí	Sí
Sistema de archivos:		
■ EXT2	Sí	Sí
■ EXT3	Sí	Sí
■ EXT4	Sí	Sí
■ Reiserfs versión 3	Sí	Sí
Volumen compartido:		
■ Volumen compartido de Windows	No	Sí
■ Volumen de recurso compartido de NFS 3.0 de Windows	No	Sí
■ Volumen de Linux compartido (Samba compartido)	No	Sí
■ Recurso compartido de NFS de Linux	No	Sí
Tipo de dispositivo:		
■ Disco extraíble (Ej. unidad de memoria, RDX)	Sí	Sí

*1	El Agente de Arcserve UDP (Linux) no es compatible con el RAID falso, también llamado RAID incrustado, proporcionado por el BIOS en la placa base.
	LVM (gestor de volumen lógico) no es compatible en SUSE Linux Enterprise Server (SLES) 10, pero se admite en SLES 10 SP1 a SP4. LVM incrustado no se admite.

Se desea realizar la copia de seguridad de más de 200 nodos

Un servidor de copia de seguridad puede gestionar un máximo de 200 nodos de forma predeterminada. Si se tienen más de 200 nodos de los que se debe realizar una copia de seguridad, se pueden configurar servidores de copia de seguridad miembros. A continuación, se utiliza un servidor de copia de seguridad central para gestionar todos los servidores miembros.

Si se tiene un servidor de copia de seguridad dedicado y se tienen más de 200 nodos que se deben gestionar, se pueden activar valores de configuración específicos y gestionar más de 200 nodos.

Revisión de las consideraciones y requisitos previos

Verifique los siguientes requisitos previos antes de realizar la copia de seguridad de más de 200 nodos de Linux:

- Se es compatible solamente con Linux de 64 bits para el servidor de copia de seguridad
- El servidor de copia de seguridad debe ser un servidor de dedicado. El Agente de Arcserve UDP (Linux) modifica los valores de configuración del sistema para cumplir el requisito de alta escalabilidad del servidor.
- El servidor debe cumplir los siguientes requisitos mínimos de hardware. Si se tiene un mayor número de nodos, las especificaciones de hardware deben ser mayores que los requisitos mínimos.
  - Memoria de 8 GB
  - Espacio libre en disco de 10 GB para la carpeta /opt

Revise las siguientes consideraciones:

- Cuando se activa el Agente de Arcserve UDP (Linux) para realizar una copia de seguridad de más de 200 nodos, el servidor utiliza una base de datos nueva (postgresql) para cumplir el requisito de alta escalabilidad. Toda la información relacionada con los nodos y tareas existentes en la base de datos antigua (sqlite) se migra a la base de datos nueva, excepto el historial de tareas y el registro de actividades. No se puede volver a la base de datos antigua (sqlite) después de la migración.
- Después de la migración, el resultado se muestra en un formato diferente para el comando d2djobhistory.
- Como práctica recomendada, una tarea de copia de seguridad debe realizar la copia de seguridad de menos de 1000 nodos.

Actualización del archivo de configuración para TOMCAT.

Cuando se actualiza al Agente de Arcserve UDP (Linux) desde la versión anterior como, por ejemplo, r16.5 SP1, actualice el archivo de configuración de TOMCAT para ser compatible con el requisito de alta escalabilidad del servidor de copia de seguridad. Esta actualización le permite realizar la copia de seguridad de más de 200 nodos utilizando un servidor de copia de seguridad.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Vaya a la carpeta bin:

   ```
   /opt/CA/d2dserver/bin
   ```

3. Verifique que no haya ninguna tarea en ejecución y, a continuación, detenga el servidor de copia de seguridad mediante el comando siguiente:

   ```
   d2dserver stop
   ```

   Si hay tareas en ejecución, espere la terminación de las tareas antes de detener el servidor de copia de seguridad.
4. Abra el archivo server.xml de la siguiente ubicación:

   ```
   /opt/CA/d2dserver/TOMCAT/conf/
   ```

5. Actualice los parámetros siguientes.

   Si se usa https, actualice los parámetros siguientes:

   ```
   <Connector port="8014" connectionTimeout="180000" protocol="HTTP/1.1"
   SSLEnabled="true" maxThreads="300"  acceptCount="200" scheme="https"
   secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

   Si se utiliza http, actualice los parámetros siguientes:

   ```
   <Connector connectionTimeout="180000" port="8014"
   maxThreads="300"  acceptCount="200" protocol="HTTP/1.1"/>
   ```

   El archivo de configuración de TOMCAT se ha actualizado correctamente.
6. Detenga el servidor de copia de seguridad.

   ```
   ./d2dserver stop
   ```

7. Ejecute el siguiente comando para iniciar el servidor de copia de seguridad:

   ```
   ./pgmgr init
   ```

   El comando verifica que todos los cambios necesarios se han completado e inicia el servidor de copia de seguridad.

```
[root@<Machine Name> bin]# ./d2dserver stop
Se ha detenido arcserve UDP Agent(Linux).
[root@<Machine Name> bin]# ./pgmgr init
El proceso de instalación se ha iniciado para la base de datos Postgresql. El re
gistro de depuración se coloca en la ubicación siguiente: /opt/CA/d2dserver/logs
/pginit.log.
La base de datos Postgresql se ha instalado correctamente.
Los datos se han migrado correctamente a la nueva base de datos.
Se ha iniciado arcserve UDP Agent(Linux).
```

El servidor de copia de seguridad y el servidor de la base de datos se han iniciado correctamente.

Gestión del servidor de la base de datos

El comando *d2dserver start* normalmente inicia el servidor de la base de datos junto con el servidor de copia de seguridad. Si no hay ninguna tarea en curso, el comando *d2dserver stop* normalmente para los dos servidores.

Si se desea iniciar y detener el servidor de la base de datos manualmente, se pueden ejecutar los comandos siguientes:

pgmgr start

Inicia el servidor de la base de datos.

pgmgr stop

Detiene el servidor de la base de datos.

pgmgr status

Muestra el estado del servidor de la base de datos. Muestra si el servidor de la base de datos se está ejecutando o si está detenido.

Nota: Si la base de datos está cargada de datos excesivos, la consola del Agente de Arcserve UDP (Linux) tardará demasiado tiempo en cargar datos para el historial de tareas y el registro de actividades. Para mejorar la consulta de dato, consulte Mejorar el rendimiento de las consultas para el historial de tareas y el registro de actividades.

Adición de nodos de Linux para una copia de seguridad

Agregue los nodos de Linux para que se pueda realizar copia de seguridad de los nodos en una ubicación de almacenamiento de la copia de seguridad. Los nodos de Linux son los equipos de los que se desea realizar copia de seguridad. Se pueden agregar nodos manualmente o se puede ejecutar un script para detectar y agregar nodos.

Siga estos pasos:

1. Introduzca la dirección URL del servidor de copia de seguridad en un explorador web para abrir la interfaz del usuario.

   Nota: Durante la instalación del Agente de Arcserve UDP (Linux), recibirá la dirección URL para acceder al servidor y gestionarlo.

2. Realice las tareas siguientes si desea detectar los nodos que utilizan un script:

   a. Haga clic en Agregar en el menú Nodo y seleccione Detección.

      Se abrirá el cuadro de diálogo Detección de nodos.

   b. Seleccione un script de la lista desplegable Script.

      Nota: Para obtener más información acerca de cómo crear el script de detección de nodos, consulte Detección de los nodos mediante un script en Cómo integrar y automatizar el Agente de Arcserve UDP (Linux) con el entorno de TI existente.

   c. Especifique la Programación y haga clic en Aceptar.

      El cuadro de diálogo Detección de nodos se cierra y empieza el proceso de detección de nodos. La ficha Registro de actividad se actualiza con un mensaje nuevo.

3. Realice las tareas siguientes si desea agregar los nodos manualmente:

   a. Haga clic en Agregar en el menú Nodo y seleccione Nombre del host/dirección IP.

      Se abrirá el cuadro de diálogo Agregar nodo.

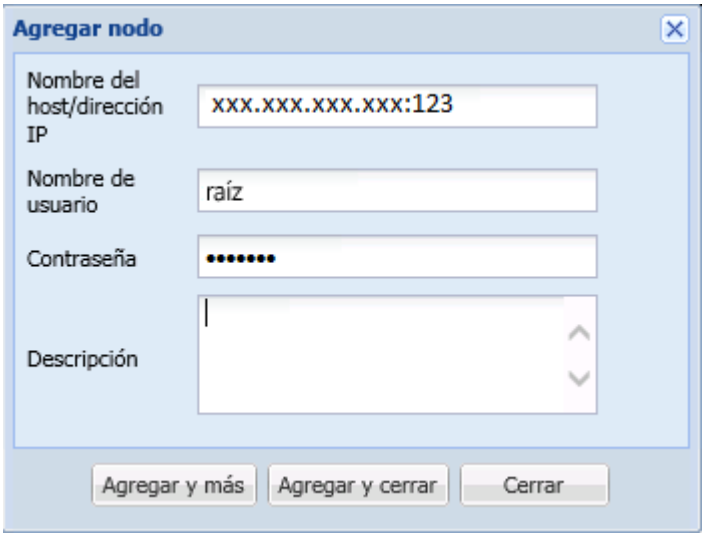
   b. Introduzca el nombre de host o la dirección IP del nodo de Linux, el nombre de usuario que tiene el permiso raíz y la contraseña.

      Nota: Si el puerto de ssh predeterminado del nodo se cambia, se puede agregar el nodo del modo siguiente:

      `<Nombre de IP>:Número de puerto`

      Ejemplo: xxx.xxx.xxx.xxx:123

      Donde xxx.xxx.xxx.xxx es la dirección IP y 123, el número de puerto.



   c. (Opcional) Introduzca una descripción para que el nodo le ayude a encontrar el nodo.

   d. Seleccione una de las opciones siguientes:

      Agregar y más

      Permite agregar varios nodos a la vez. Después de finalizar con la adición de nodos, haga clic en Agregar y cerrar o Cerrar para cerrar el cuadro de diálogo Agregar nodo.

      Agregar y cerrar

      Permite agregar un nodo y, a continuación, se cierra el cuadro de diálogo Agregar nodo.

      Cerrar

      Cierra el cuadro de diálogo sin agregar nodos.

4. Haga clic en la ficha Nodos y compruebe que aparecen nuevos nodos.

Se agregan nodos de Linux para la copia de seguridad.

(Opcional) Preparación del volumen iSCSI como almacenamiento de la copia de seguridad

Se pueden almacenar los puntos de recuperación en un volumen de una interfaz estándar de equipos pequeños de Internet (iSCSI). iSCSI se utiliza para gestionar la transferencia de datos y el almacenamiento en una red mediante la dirección IP estándar.

Verifique que tiene la última versión del software del iniciador de iSCSI instalado en el servidor de copia de seguridad. El software de iniciador en sistemas de RHEL se encuentra dentro del paquete de iscsi-iniciador-utils. El software de iniciador en sistemas de SLES se encuentra dentro del paquete de open-iscsi.

Siga estos pasos:

1. Inicie sesión en el entorno de shell del nodo de origen de copia de seguridad.
2. Ejecute uno de los siguientes comandos para iniciar el daemon del iniciador iSCSI.
   - Para los sistemas de RHEL:

     ```
     /etc/init.d/iscsid start
     ```

     El servicio en los sistemas de RHEL se denomina iscsid.
   - Para los sistemas de SLES:

     ```
     /etc/init.d/open-iscsi start
     ```

     El servicio en los sistemas de SLES se denomina open-iscsi.
3. Ejecute un script de detección para detectar el host de destino de iSCSI.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   El valor del puerto predeterminado del host de destino de iSCSI es 3260.

4. Tome nota del nombre completo de iSCSI (IQN) del host de destino de iSCSI que ha encontrado el script de detección antes de realizar el registro manual en el destino detectado.
5. Enumere el dispositivo de bloqueo disponible del nodo de origen de la copia de seguridad.

   ```
   #fdisk -l
   ```

6. Inicie sesión en el destino detectado.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p
   <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>  -l
   ```

   Se puede ver un dispositivo de bloqueo en el directorio /dev del nodo de origen de la copia de seguridad.
7. Ejecute el comando siguiente para obtener el nuevo nombre del dispositivo:

   ```
   #fdisk –l
   ```

   Se puede ver otro dispositivo denominado /dev/sd<x> en el nodo de origen de la copia de seguridad.

   Por ejemplo, tenga en cuenta que el nombre del dispositivo es /dev/sdc. Este nombre de dispositivo se utilizará para crear una partición y un sistema de archivos en los pasos siguientes.
8. Formatee y monte el volumen de iSCSI.
9. Cree una partición y un sistema de archivos en el nodo de origen de copia de seguridad mediante los comandos siguientes.

   ```
   # fdisk /dev/sdc
   ```

   Si solamente se ha creado una partición, utilice el comando siguiente para crear un sistema de archivos para la partición única:

   ```
   # mkfs.ext3 /dev/sdc1
   ```

10. Monte la partición nueva mediante los comandos siguientes:

    ```
    # mkdir /iscsi
    # mount /dev/sdc1 /iscsi
    ```

    La partición nueva se monta y el volumen de iSCSI ya estará listo para ser utilizado como almacenamiento de copia de seguridad en una tarea de copia de seguridad.
11. (Opcional) Agregue el registro siguiente a la carpeta /etc/fstab para que el volumen de iSCSI se conecte automáticamente al servidor de copia de seguridad después de reiniciar el servidor.

    ```
    /dev/sdc1 /iscsi ext3 _netdev 0 0
    ```

El volumen de iSCSI está preparado para ser utilizado como almacenamiento de la copia de seguridad.

Configuración de los valores de configuración de la copia de seguridad y ejecución de la tarea de copia de seguridad

Configure los valores de configuración de la copia de seguridad mediante el Asistente de copia de seguridad. Se puede realizar una copia de seguridad de los datos en una ubicación del sistema de archivos de red (NFS), en un almacenamiento adjunto de red (NAS), en un sistema de archivos de Internet comunes (CIFS) o en una ubicación local de origen. Una ubicación local de origen es una ubicación en el nodo de origen de copia de seguridad donde se almacenan los datos de copia de seguridad. Una tarea de copia de seguridad inicia el proceso de copia de seguridad. El Asistente de copia de seguridad crea la tarea de copia de seguridad y ejecuta la tarea. Cada vez que se realiza una copia de seguridad correcta, se creará un punto de recuperación. Un punto de recuperación es una copia en un momento dado del nodo de copia de seguridad.

Especificación del origen de la copia de seguridad

Especifique los nodos de origen de copia de seguridad en el Asistente de copia de seguridad para que se pueda realizar una copia de seguridad de los nodos en una ubicación deseada. La página Origen de la copia de seguridad del Asistente de copia de seguridad muestra el nodo del cual desea realizar una copia de seguridad. Utilice el botón Agregar en esta página a fin de agregar más nodos para la copia de seguridad.

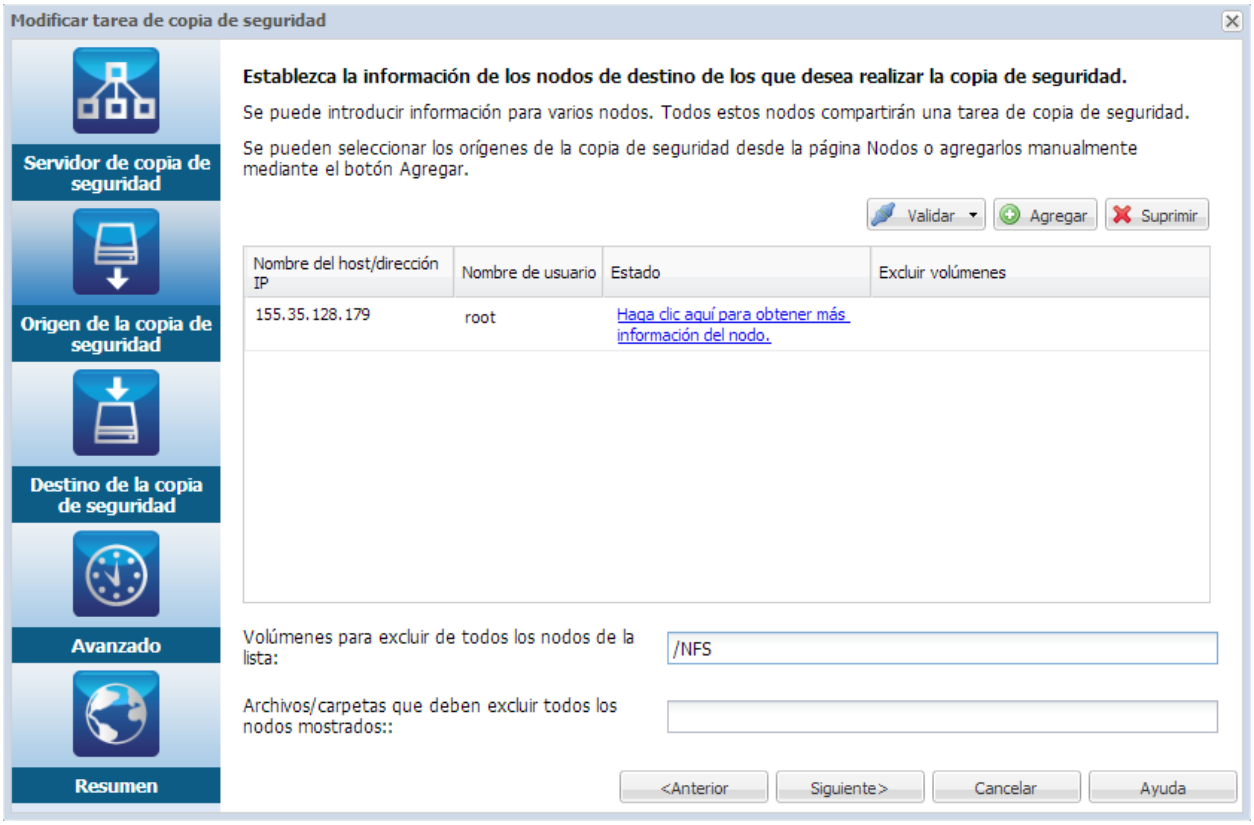
Nota: Si se abre el Asistente de copia de seguridad mediante el botón Realizar la copia de seguridad de los nodos seleccionados, aparecerán todos los nodos seleccionados en la página del asistente. Si se abre el Asistente de copia de seguridad mediante el botón Copia de seguridad, los nodos no aparecerán en la página del asistente. Es necesario agregar los nodos mediante el botón Agregar en la página del asistente.

Siga estos pasos:

1. Seleccione los nodos de los cuales desea realizar copia de seguridad en la ficha Nodos.
2. Haga clic en Copia de seguridad y seleccione la opción Realizar copia de seguridad de los nodos seleccionados en el menú Asistente.

   Se abrirá la página Servidor de copia de seguridad del Asistente de copia de seguridad. La página Servidor de copia de seguridad muestra el nombre del servidor.
3. Haga clic en Siguiente.

   Se abre la página Origen de la copia de seguridad. Los nodos previamente seleccionados se muestran en esta página.



4. (Opcional) Haga clic en Agregar en la página Origen de la copia de seguridad para agregar más nodos y proporcionar los detalles en el cuadro de diálogo Agregar nodo.

5. (Opcional) Haga clic en el icono Excluir volúmenes.

   Aparece el cuadro de diálogo Excluir valores de configuración del volumen que incluye todos los volúmenes del nodo.

6. (Opcional) Seleccione la casilla de verificación para los volúmenes de los que no desee realizar copia de seguridad y haga clic en Aceptar.

   Se cierra el cuadro de diálogo Excluir valores de configuración del volumen.

   Nota: Para excluir un volumen específico de todos los nodos de copia de seguridad, introduzca los nombres del punto de montaje del volumen en **Volúmenes para excluir de todos los nodos de la lista**. Si se excluye el volumen */* o el volumen */boot* de un nodo, no se podrá realizar ninguna reconstrucción completa del nodo.

7. (Opcional) Especifique los archivos/carpetas en **Archivos y carpetas para excluir de todos los nodos de la lista**.

   Los archivos/carpetas se deben especificar con un nombre de ruta absoluto y separarse con dos puntos (:). Los caracteres comodín como, por ejemplo, * y ? son compatibles y se deben utilizar después de la última barra diagonal del nombre de ruta absoluto. Si el nombre de los archivos/carpetas situado después de la última barra diagonal se encierra entre paréntesis, estos archivos/carpetas se excluirán recursivamente, de lo contrario los archivos/carpetas se excluirán directamente.

   Por ejemplo:

   ```
   /home/user/a/foo*:/home/user/b/(foo*)
   ```

   La primera parte (home/user/a/foo*) excluirá solamente archivos/carpetas que coinciden con foo* debajo de "/home/user/a", pero realizará la copia de seguridad de los subdirectorios. La segunda parte (/home/user/b/(foo*) excluirá todos los archivos/carpetas que coinciden con foo* debajo de "/home/user/b", incluyendo todas las subcarpetas.

   Notas:

   - Si muchos archivos/carpetas se excluyen de un volumen, se recomienda excluir el volumen relevante.
   - Si muchos archivos/carpetas se excluyen, la fase y el estado de la tarea se pueden quedar en "Realizando copia de seguridad del volumen" y en "Activo" durante mucho tiempo, cuando la tarea de copia de seguridad se inicia.
   - Si el valor de **Archivos y carpetas para excluir de todos los nodos de la lista** cambia, la tarea de copia de seguridad se convertirá en una copia de seguridad completa.

   Si se excluyen algunos archivos del sistema de la copia de seguridad, es posible que no se inicie el SO de Linux y la reconstrucción completa no funcionará correctamente. Estos archivos de sistema incluyen, pero sin limitarse a:

- Archivos y carpetas bajo /bin, /sbin, /usr, /etc, /lib, /lib64, /boot y /var.
- Las carpetas /proc, / sys, / dev y /tmp.

Si se excluyen los archivos del sistema, se recomienda verificar la función de la reconstrucción completa y confirme si el SO de Linux se inicia correctamente.

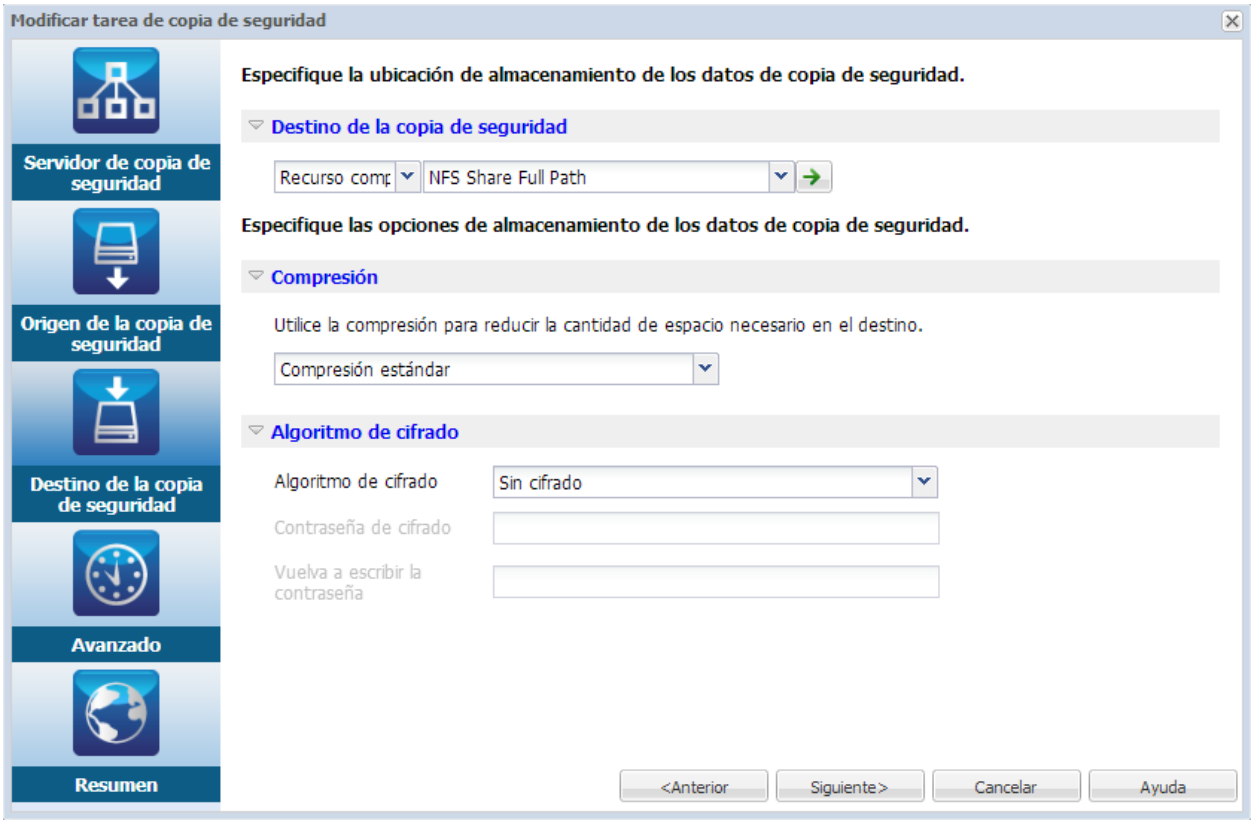
8. Haga clic en Siguiente.

   Se abre la página Destino de copia de seguridad.

Se especifica el origen de copia de seguridad.

Cómo especificar el destino de copia de seguridad

Especifique una ubicación para almacenar los datos de copia de seguridad (puntos de recuperación) en la página Destino de copia de seguridad del Asistente de copia de seguridad. El destino de copia de seguridad podría ser un recurso compartido de NFS, un recurso compartido de CIFS o un origen local. El origen local es el nodo de origen de copia de seguridad. Si el destino de la copia de seguridad es Origen local, a continuación los datos de copia de seguridad se crearán directamente en su propio disco local.



Si un disco físico incluye dos volúmenes lógicos, se puede especificar un volumen como el origen de la copia de seguridad y el otro volumen como el destino de la copia de seguridad.

Nota: Si se selecciona Origen local como el destino de la copia de seguridad, el servidor de copia de seguridad no podrá gestionar los puntos de recuperación. Para gestionar los conjuntos de recuperación, consulte Gestión de los conjuntos de recuperación en Cómo gestionar los valores de configuración del servidor de copia de seguridad.

Siga estos pasos:

1. Seleccione un destino en la lista desplegable Destino de copia de seguridad e introduzca la ruta completa de la ubicación de almacenamiento.

   - Si se ha seleccionado Recurso compartido de NFS, escriba los detalles Destino de copia de seguridad en el formato siguiente:
     `Dirección IP del uso compartido de NFS:/ruta completa de la ubicación de almacenamiento`

     Nota: Algunas versiones del NAS de dominio de datos no son compatibles con el mecanismo de bloqueo del archivo de NFS. Como resultado, estos recursos compartidos de NFS no se pueden utilizar como destino de la copia de seguridad. Para obtener más información acerca de esta incidencia, consulte la sección Incidencias de compatibilidad con el Agente de Arcserve UDP (Linux) en las Notas de la versión.

   - Si se ha seleccionado Recurso compartido de CIFS, escriba los detalles Destino de copia de seguridad en el formato siguiente:
     `//hostname/share_folder`

     Nota: El nombre de la carpeta compartida no puede contener espacios.

   - Si se ha seleccionado Origen local, deberá modificar algunos valores de configuración para que el servidor de copia de seguriad pueda gestionar los puntos de recuperación. Por ejemplo, se debe considerar que servidor-A sea el nombre del host del servidor de copia de seguridad y nodo-B el nombre del host del nodo de origen. Ahora, siga estos pasos para modificar la configuración de node-B:

     - Asegúrese de que el servidor de NFS esté en ejecución. Se puede ejecutar el comando siguiente para verificar el estado del servidor de NFS:

       estado del servicio nfs

     - Si el servidor de NFS no se está ejecutando, ejecute el comando siguiente para iniciar el servidor de NFS:

       inicio del servicio nfs

     - Si la carpeta de destino de la copia de seguridad en node-B es */backup/test*, agregue a continuación la línea siguiente a */etc/exports*:

       /backup/test server-A(rw,no_root_squash)

       Ejecute el siguiente comando:

       exportfs -a

     - En la interfaz de usuario del servidor de copia de seguridad, agregue *node-B:/backup/test* como ubicación de almacenamiento de la copia de seguridad. La ubicación de almacenamiento Origen local aparecerá en la lista desplegable Destino de la copia de seguridad.

2. Haga clic en el botón de flecha para validar la información Destino de copia de seguridad.

   Si el destino de copia de seguridad no es válido, aparecerá un mensaje de error.

3. Seleccione un nivel de compresión en la lista desplegable Compresión para especificar un tipo de compresión que se utiliza para la copia de seguridad.

   Las opciones disponibles para la Compresión son:

   Compresión estándar

   Especifica que esta opción proporciona un buen equilibrio entre el uso de la CPU y del espacio en disco. La compresión estándar es la configuración predeterminada.

   Compresión máxima

   Esta opción utiliza la mayor cantidad de CPU (velocidad más baja) pero también utiliza el menor espacio en disco para la imagen de copia de seguridad.

4. Seleccione un algoritmo en la lista desplegable Algoritmo de cifrado y escriba la contraseña de cifrado, si es necesario.

   a. Seleccione el tipo de algoritmo de cifrado que desea utilizar para las copias de seguridad.

      El cifrado de datos es la traducción de los datos a una forma que resulte ininteligible sin un mecanismo de descifrado. La protección de los datos del Agente de Arcserve UDP (Linux) utiliza algoritmos de cifrado seguros AES (estándar de cifrado avanzado) a fin de lograr la máxima seguridad y privacidad de los datos especificados.

      Las opciones de formato disponibles son Sin cifrado, AES-128, AES-192 y AES-256. (Para desactivar el cifrado, se debe seleccionar Sin cifrado).

      - Todas las copias de seguridad completas y sus copias de seguridad incrementales relacionadas deben utilizar el mismo algoritmo de cifrado.
      - Si el algoritmo de cifrado para una copia de seguridad incremental ha cambiado, se deberá realizar una copia de seguridad completa.

        Por ejemplo, si se cambia el formato del algoritmo y, a continuación, se ejecuta una copia de seguridad incremental, el tipo de copia de seguridad se convertirá automáticamente en una copia de seguridad completa.

   b. Cuando se selecciona un algoritmo de cifrado, se debe proporcionar, y confirmar, la contraseña de cifrado.

      - La contraseña de cifrado puede tener un máximo de 23 caracteres.
      - Una copia de seguridad completa y todas las copias de seguridad incrementales y de verificación relacionadas deben utilizar la misma contraseña para cifrar los datos.

5. Haga clic en Siguiente.

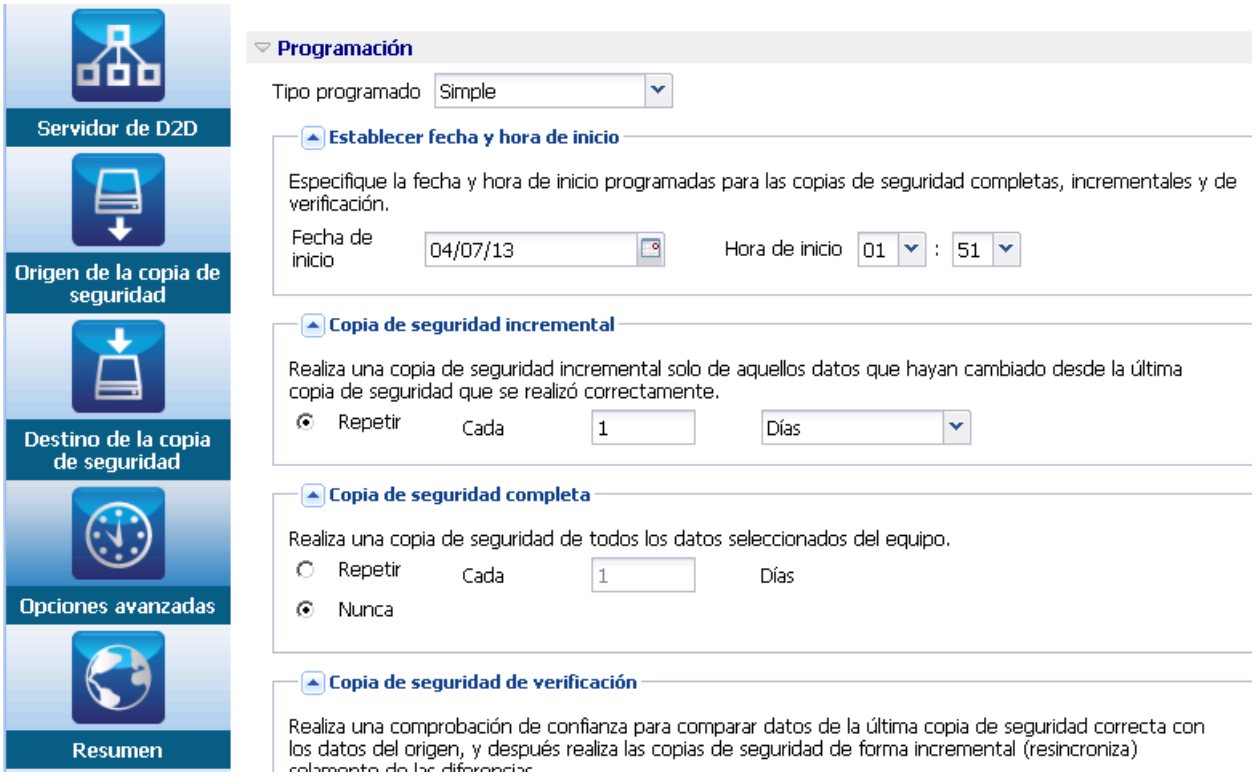
   Aparecerá la página Configuración avanzada.

Se especifica el destino de la copia de seguridad.

Especificación de la configuración avanzada

Especifique la programación de la copia de seguridad, la configuración de los conjuntos de recuperación y la configuración de la copia de seguridad anterior y posterior en la página Configuración avanzada.

El siguiente diagrama muestra la página Avanzado del Asistente de copia de seguridad. En este diagrama, se selecciona la opción Ninguno para el Tipo de programación.



Los siguientes valores de configuración están disponibles en la página Configuración avanzada:

- La configuración de la programación garantiza que la tarea de copia de seguridad se ejecute periódicamente en una hora especificada.
- La configuración de los conjuntos de recuperación garantiza el mantenimiento periódico de estos. Si el número de conjuntos de recuperación supera el número especificado, se suprimirá el conjunto de recuperación más antiguo para mantener el número especificado.
- La configuración de regulación de copias de seguridad permite activar y especificar la velocidad máxima (MB/min) a la cual se escriben las copias de seguridad.
- La configuración de scripts anteriores/posteriores define los scripts que se pueden ejecutar en el servidor de copia de seguridad y en el nodo de destino. Se pueden configurar los scripts para llevar a cabo acciones específicas antes del inicio de una tarea, durante su ejecución o después de la finalización de dicha tarea.

Para optimizar la gestión de los puntos de recuperación, debería tener en cuenta las recomendaciones siguientes al programar la frecuencia de las copias de seguridad:

- Para los sistemas que se protegen con copias de seguridad incrementales realizadas cada 15 minutos, debería programar una copia de seguridad completa todas las semanas (para actualizar la imagen base).
- Para los sistemas que se protegen con copias de seguridad incrementales realizadas cada hora, debería programar una copia de seguridad completa cada mes (para actualizar la imagen base).

Nota: Si le preocupa la cantidad de espacio utilizado para almacenar las imágenes de copia de seguridad, debería programar las copias de seguridad completas menos frecuentemente para consumir menos espacio de almacenamiento.

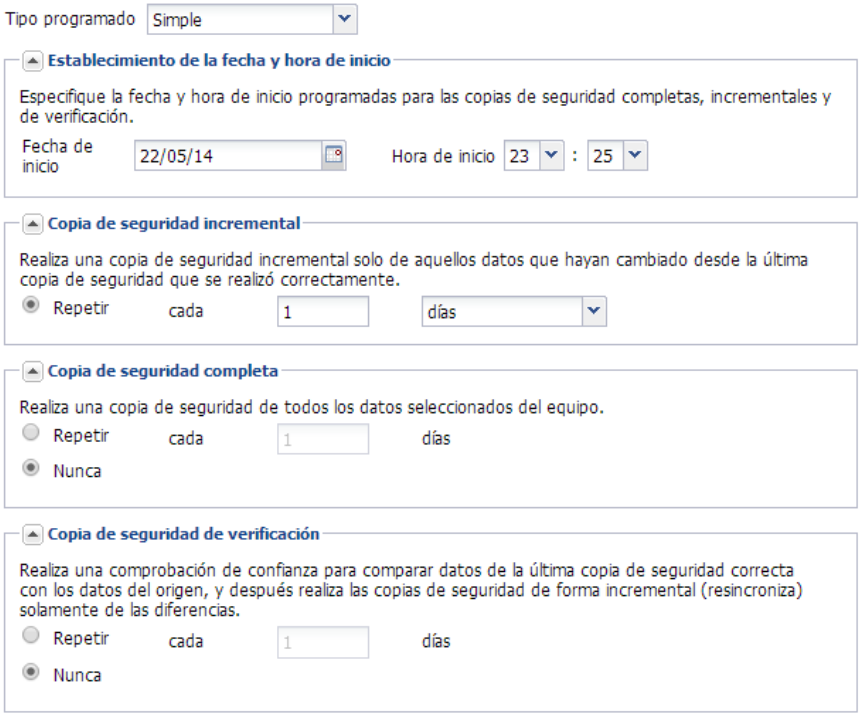
Siga estos pasos:

1. Establezca la fecha y la hora de inicio seleccionando una de las siguientes opciones de la lista desplegable Tipo programado:

   Simple

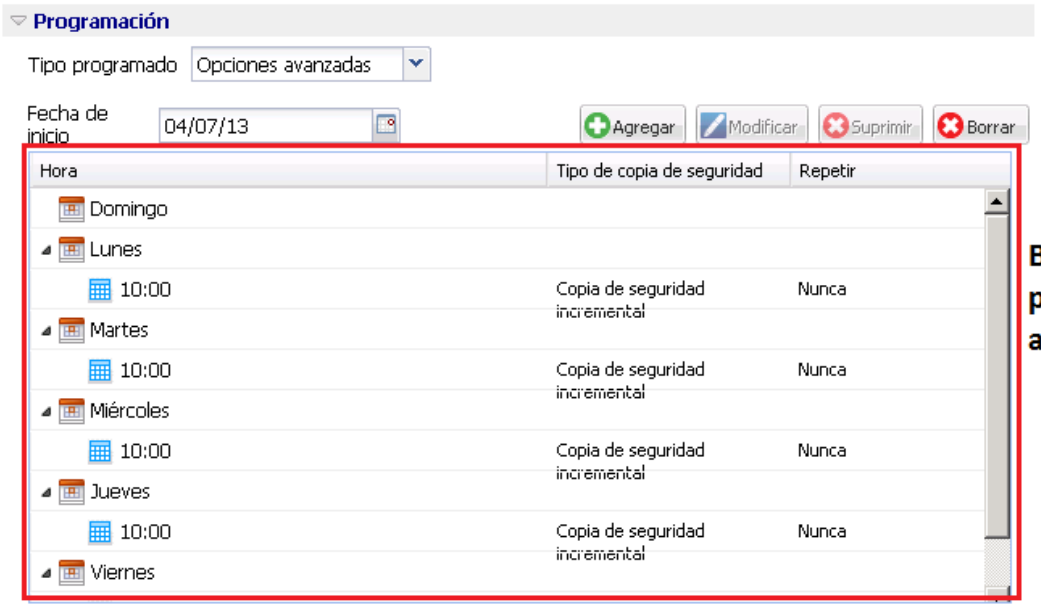
   Seleccione la opción Simple para programar la copia de seguridad incremental, la copia de seguridad completa y la copia de seguridad de verificación según la fecha de inicio y la hora de inicio especificadas. En cada tipo de copia de seguridad se puede especificar también la duración de repetición de una copia de seguridad o que nunca se repita una copia de seguridad. La fecha y la hora de inicio son fijas en todos los tipos de copia de seguridad. Por tanto, no se puede especificar una fecha y hora de inicio diferentes para distintos tipos de copia de seguridad.

   Nota: Para obtener más información acerca de los tipos de copia de seguridad, consulte *Funcionamiento de los tipos de copia de seguridad*.



Avanzadas

Seleccione la opción Avanzado para especificar varias programaciones de copia de seguridad cada día de la semana. Se puede especificar una fecha y hora de inicio diferentes para distintos tipos de copia de seguridad. Se puede agregar, modificar, suprimir y borrar la programación avanzada. Cuando se hace clic en Borrar, se suprimen todas las programaciones de copia de seguridad avanzadas de la bandeja de programación avanzada.

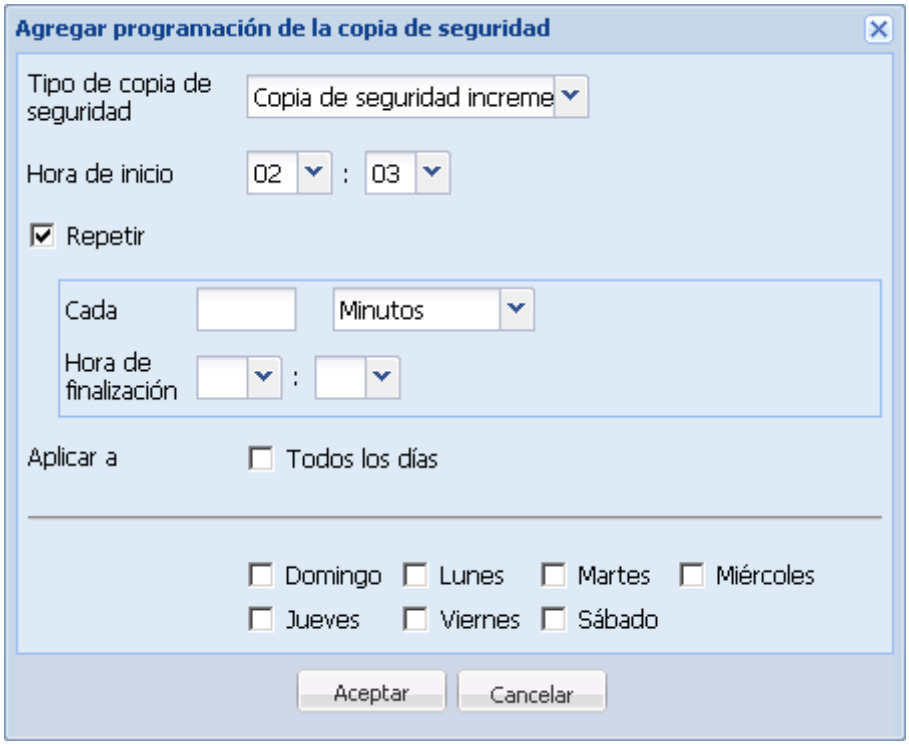


Bandeja de programación avanzada

Para agregar una programación de copia de seguridad, siga estos pasos:

a. Haga clic en Agregar.

Se abrirá el cuadro de diálogo Agregar programación de la copia de seguridad.



b. Especifique las opciones de programación de copia de seguridad y haga clic en Aceptar.

La programación de copia de seguridad especificada se muestra en la bandeja de programación avanzada.

None

Seleccione la opción Ninguno para crear la tarea de copia de seguridad y para almacenarla en la ficha Estado de la tarea. Esta opción no ejecutará la tarea debido a que no existe ninguna programación especificada. Cuando se envía la tarea, el estado de la tarea cambia a Listo. Cuando desee ejecutar la tarea, deberá seleccionar la tarea y hacer clic en Ejecutar ahora en el menú Tarea. Cada vez que desee ejecutar la tarea, esta deberá ejecutarse manualmente. Se puede escribir también esta tarea en un script para ejecutarla en su propia programación personalizada.

2. Especifique la configuración de los conjuntos de recuperación.

   Nota: Para obtener más información acerca de los conjuntos de recuperación, consulte *Funcionamiento de los conjuntos de recuperación*.

   Especifique el número de conjuntos de recuperación que deben retenerse.

   Especifica el número de conjuntos de recuperación retenidos.

   Inicie un nuevo conjunto de recuperación cada:

   Día seleccionado de la semana

   Especifica el día de la semana seleccionado para iniciar un nuevo conjunto de recuperación.

   Cada día seleccionado del mes

   Especifica el día del mes seleccionado para iniciar un nuevo conjunto de recuperación. Seleccione del 1 al 30, o bien el último día del mes.

   Nota: El servidor de copia de seguridad comprueba cada 15 minutos el número de conjuntos de recuperación en el almacenamiento de la copia de seguridad configurado y suprime cualquier conjunto de recuperación adicional de la ubicación de almacenamiento de la copia de seguridad.

3. Especifique el valor de regulación de la copia de seguridad.

   Se puede especificar la velocidad máxima de escritura (MB/min) para las copias de seguridad. Es posible regular la velocidad de la copia de seguridad para reducir el uso de la CPU o de la red. Sin embargo, la limitación de la velocidad de las copias de seguridad puede tener efectos adversos en la ventana de copia de seguridad. A medida que se reduzca la velocidad máxima de la copia de seguridad, aumentará la cantidad de tiempo necesario para realizar la copia de seguridad. En una tarea de copia de seguridad, la ficha Estado de la tarea muestra el promedio de velocidad de lectura y escritura de la tarea en curso y el límite de velocidad de regulación que se ha configurado.

   Nota: De forma predeterminada, la opción Regular copia de seguridad no aparece activada y no se controla la velocidad de la copia de seguridad.

4. Especifique la configuración de copia de seguridad anterior y posterior en Configuración de scripts anteriores/posteriores.

   Estos scripts ejecutan comandos de script para realizar acciones antes del inicio de la tarea o cuando esta se finalice.

   Nota: Los campos de configuración de scripts se rellenan solamente si ya se ha creado un archivo de script y se ha colocado en la siguiente ubicación.

   ```
   /opt/CA/d2dserver/usr/prepost
   ```

   Nota: Para obtener más información acerca de cómo crear los scripts anteriores/posteriores, consulte *Gestión de scripts anteriores/posteriores para la automatización*.

5. Haga clic en Siguiente.

   Aparecerá la página Resumen.

Se especifica la programación avanzada.

Nota: Si en un momento determinado existe más de un tipo de copia de seguridad programado para realizarse de manera simultánea, el tipo de copia de seguridad que se realizará depende de las prioridades siguientes:

- Prioridad 1 - Copia de seguridad completa
- Prioridad 2 - Copia de seguridad de verificación
- Prioridad 3 - Copia de seguridad incremental

Por ejemplo, si se programan tres tipos de copia de seguridad para que se ejecuten al mismo tiempo, el Agente de Arcserve UDP (Linux) realizará una copia de seguridad completa. Si no se ha programado una copia de seguridad completa, sino una copia de seguridad de verificación e incremental simultáneamente, el Agente de Arcserve UDP (Linux) realizará una copia de seguridad de verificación. Una copia de seguridad incremental programada sólo se realizará si no existe ningún conflicto con los otros tipos de copia de seguridad.

Información general de los tipos de copia de seguridad

Se pueden especificar los siguientes tipos de copia de seguridad en la página Configuración avanzada del Asistente de copia de seguridad:

Copia de seguridad incremental

Se realiza una copia de seguridad solo de los bloques que han cambiado desde la última copia de seguridad correcta. Las ventajas de la copia de seguridad incremental consisten en que se trata de una copia de seguridad rápida y que produce una imagen de copia de seguridad pequeña. Agente de Arcserve Unified Data Protection para Linux utiliza un controlador para monitorizar los bloques modificados en el nodo de origen desde la última copia de seguridad correcta.

Las opciones disponibles son Repetir y Nunca. Si selecciona la opción Repetir, debería especificar el período de tiempo transcurrido (en minutos, horas o días) entre los intentos de copia de seguridad.

Mínimo: 15 minutos

Valor predeterminado: 1 día

Copia de seguridad completa

Realiza una copia de seguridad de todo el nodo de origen. En función del tamaño del volumen del nodo de copia de seguridad, la copia de seguridad completa producirá una imagen de copia de seguridad de gran tamaño, con lo que normalmente se tardará más tiempo para finalizar. Las opciones disponibles son Repetir y Nunca.

Si selecciona la opción Repetir, debería especificar el período de tiempo transcurrido (en minutos, horas o días) entre los intentos de copia de seguridad.

Mínimo: 1 día

Valor predeterminado: Nunca (ninguna repetición programada)

Copia de seguridad de verificación

Comprobará que los datos protegidos sean válidos y estén completos mediante una comprobación de confianza de la imagen de copia de seguridad almacenada en el origen de copia de seguridad original. Si es necesario, volverá a sincronizar la imagen. Una copia de seguridad de verificación se fijará en la copia de seguridad más reciente de cada bloque individual y comparará el contenido y la información con la de origen. Esta comparación garantizará que los últimos bloques con copia de seguridad representan información correspondiente con la de origen. Si la imagen de copia de seguridad para un bloque no coincide con la de origen (es posible que sea por los cambios en el sistema desde la última copia de seguridad), CA ARCserve Dynamic Recovery actualizará (resincronizará) la copia de seguridad del bloque que no coincide. Se puede utilizar también una copia de seguridad de verificación (aunque poco frecuentemente) para obtener la garantía de copia de seguridad completa sin utilizar el espacio necesario para una copia de seguridad completa.

Ventajas: produce una pequeña imagen de copia de seguridad si se compara con la copia de seguridad completa porque solamente se realiza copia de seguridad de los bloques modificados (los bloques que no coinciden con la última copia de seguridad).

Desventajas: el tiempo durante el cual se realiza la copia de seguridad es considerable puesto que todos los bloques de origen se comparan con los bloques de la última copia de seguridad.

Las opciones disponibles son Repetir y Nunca. Si selecciona la opción Repetir, debería especificar el período de tiempo transcurrido (en minutos, horas o días) entre los intentos de copia de seguridad.

Mínimo: 1 día

Valor predeterminado: Nunca (ninguna repetición programada)

El tipo de copia de seguridad que se ejecuta depende de las siguientes situaciones:

- Si se ejecuta la tarea de copia de seguridad de los nodos seleccionados por primera vez, la primera copia de seguridad será siempre una copia de seguridad completa.
- Si se ejecuta la tarea de copia de seguridad de nuevo para el mismo conjunto de nodos y el destino de copia de seguridad también es el mismo, el tipo de copia de seguridad será una copia de seguridad incremental.
- Si se ejecuta la tarea de copia de seguridad para el mismo conjunto de nodos, pero el destino de copia de seguridad es distinto, el tipo de copia de seguridad será una copia de seguridad completa. Esto es porque el destino de copia de seguridad ha cambiado y se trata de la primera copia de seguridad para el nuevo destino. La primera copia de seguridad siempre es una copia de seguridad completa.
- Si se suprime el nodo y se agrega el mismo nodo de nuevo pero no se cambia el destino de copia de seguridad, la copia de seguridad será una Copia de seguridad de verificación. Esto es porque ya se ha realizado una copia de seguridad del nodo en las tareas de copia de seguridad anteriores. Cuando se suprime el nodo y se agrega de nuevo, la tarea de copia de seguridad verifica todos los bloques del nodo con la última imagen de copia de seguridad. Cuando la tarea de copia de seguridad determina que es el mismo nodo, a continuación realizará una copia de seguridad solamente de los bloques modificados. Si la tarea de copia de seguridad no encuentra ninguna imagen de copia de seguridad del nodo en el destino de copia de seguridad, el tipo de copia de seguridad será una Copia de seguridad completa.

Información general de los conjuntos de recuperación

Un conjunto de recuperación es una configuración de almacenamiento donde se realiza copia de seguridad de un grupo de puntos de recuperación y se almacena en un período especificado como un conjunto. Un conjunto de recuperación es una serie de copias de seguridad, empezando con una copia de seguridad completa y seguida, a continuación, por un número determinado de copias de seguridad incrementales, completas o de verificación. Especifique el número de conjuntos de recuperación que deben retenerse.

La configuración de los conjuntos de recuperación garantiza el mantenimiento periódico de los conjuntos de recuperación. Cuando el límite especificado se sobrepasa, el conjunto de recuperación más antiguo se suprimirá. Los siguientes valores definen los conjuntos de recuperación predeterminados, mínimos y máximos del Agente de Arcserve UDP (Linux):

Valor predeterminado: 2

Mínimo: 1

Número máximo de conjuntos de recuperación: 100

Número máximo de puntos de recuperación (incluida una copia de seguridad completa): 1344

Nota: Si se desea suprimir un conjunto de recuperación para guardar espacio de almacenamiento de copia de seguridad, reduzca el número de conjuntos retenidos y el servidor de copia de seguridad suprimirá automáticamente el conjunto de recuperación más antiguo. No intente suprimir el conjunto de recuperación manualmente.

Conjunto de ejemplo 1:

- Completa
- Incremental
- Incremental
- Verificar
- Incremental

Conjunto de ejemplo 2:

- Completa
- Incremental
- Completa
- Incremental

Se requiere una copia de seguridad completa para iniciar un nuevo conjunto de recuperación. La copia de seguridad que inicia el conjunto se convertirá automáticamente en una copia de seguridad completa, incluso si no hay ninguna copia de seguridad completa configurada o programada para que se lleve a cabo en ese momento. Después de cambiar la configuración del conjunto de recuperación (por ejemplo, cambiando el punto de partida del conjunto de recuperación de la primera copia de seguridad realizada el lunes a la primera copia de seguridad realizada el jueves), el punto de partida de los conjuntos de recuperación existentes no se cambiará.

Nota: No se cuenta ningún conjunto de recuperación incompleto al calcular un conjunto de recuperación existente. Un conjunto de recuperación se considera completo solamente cuando se crea la copia de seguridad inicial del siguiente conjunto de recuperación.

Ejemplo 1 - Retener 1 conjunto de recuperación:

- Especifique el valor del número de conjuntos de recuperación que deben retenerse como 1.

  El servidor de copia de seguridad siempre mantiene dos conjuntos para mantener un conjunto completo antes de iniciar el siguiente conjunto de recuperación.

Ejemplo 2 - Retener 2 conjuntos de recuperación:

- Especifique el valor del número de conjuntos de recuperación que deben retenerse como 2.

  El servidor de copia de seguridad suprime el primer conjunto de recuperación en el momento en que va a iniciarse el cuarto conjunto de recuperación. De esta manera se asegura que cuando la primera copia de seguridad se suprima y la cuarto se está iniciando, todavía habrá dos conjuntos de recuperación (el conjunto de recuperación 2 y el conjunto de recuperación 3) disponibles en disco.

  Nota: Aunque se seleccione el mantenimiento de un único conjunto de recuperación, se necesitará espacio para dos copias de seguridad completas, como mínimo.

Ejemplo 3 - Retener 3 conjuntos de recuperación:

- La hora de inicio de la copia de seguridad es a las 06:00, 20 de agosto de 2012.
- Una copia de seguridad incremental se ejecuta cada 12 horas.
- Un nuevo conjunto de recuperación se inicia en la última copia de seguridad realizada el viernes.
- Se desea retener 3 conjuntos de recuperación.

Con la configuración anterior, se ejecutará una copia de seguridad incremental a las 06:00 y a las 18:00 cada día. El primer conjunto de recuperación se crea cuando se realiza la primera copia de seguridad (debe ser una copia de seguridad completa). A continuación, la primera copia de seguridad completa se marca como la copia de seguridad de partida del conjunto de recuperación. Cuando la copia de seguridad programada a las 18:00 del viernes se ejecuta, se convertirá en una copia de seguridad completa y se marcará como la copia de seguridad de partida del conjunto de recuperación.

(Opcional) Gestión de scripts anteriores/posteriores para la automatización

Los scripts previos/posteriores permiten ejecutar su propia lógica empresarial en las etapas específicas de una tarea en ejecución. Se puede especificar cuando se ejecutan los scripts en **Configuración previa/posterior** de los scripts del **Asistente de copia de seguridad** y el **Asistente de restauración** en la interfaz de usuario. Los scripts se pueden ejecutar en el servidor de copia de seguridad en función de la configuración.

La gestión de scripts anteriores/posteriores constituye un proceso de dos partes que consta de la creación del script anterior/posterior y la colocación de dicho script en la carpeta prepost.

Creación de scripts anteriores/posteriores

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree un archivo de script mediante el uso de las variables de entorno en el lenguaje de generación de scripts preferido.

   Variables de entorno de scripts anteriores/posteriores

   Para crear un script, utilice las variables de entorno siguientes:

   D2D_JOBNAME

   Indica el nombre de la tarea.

   D2D_JOBID

   Identifica el ID de la tarea. El ID de la tarea es un número que se proporciona a la tarea cuando esta se ejecuta. Si se ejecuta la misma tarea de nuevo, obtendrá un nuevo número de tareas.

   D2D_TARGETNODE

   Identifica el nodo del cual se realiza copia de seguridad o que se restaura.

   D2D_JOBTYPE

   Identifica el tipo de tarea en ejecución. Los valores siguientes identifican la variable D2D_JOBTYPE:

   backup.full

   Identifica la tarea como copia de seguridad completa.

   backup.incremental

   Identifica la tarea como copia de seguridad incremental.

   backup.verify

   Identifica la tarea como copia de seguridad de verificación.

restore.bmr

Identifica la tarea como una reconstrucción completa. Esta tarea es de restauración.

restore.file

Identifica la tarea como una restauración de nivel de archivo. Esta tarea es de restauración.

D2D_SESSIONLOCATION

Identifica la ubicación donde se almacenan los puntos de recuperación.

D2D_PREPOST_OUTPUT

Identifica un archivo temporal. El contenido de la primera línea del archivo temporal aparecerá en el registro de actividades.

D2D_JOBSTAGE

Indica la etapa de la tarea. Los valores siguientes identifican la variable D2D_JOBSTAGE:

pre-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad antes de que se inicie la tarea.

post-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad después de que se complete la tarea.

pre-job-target

Identifica el script que se ejecuta en el equipo de destino antes de que se inicie la tarea.

post-job-target

Identifica el script que se ejecuta en el equipo de destino después de que se complete la tarea.

pre-snapshot

Identifica el script que se ejecuta en el equipo de destino antes de capturar la instantánea.

post-snapshot

Identifica el script que se ejecuta en el equipo de destino después de capturar la instantánea.

D2D_TARGETVOLUME

Identifica el volumen del cual se realiza copia de seguridad durante una tarea de copia de seguridad. Esta variable es aplicable para los scripts de instantáneas previas y posteriores para una tarea de copia de seguridad.

D2D_JOBRESULT

Identifica el resultado para un script de tarea de publicación. Los valores siguientes identifican la variable D2D_JOBRESULT:

success

Identifica el resultado como correcto.

fail

Identifica el resultado como incorrecto.

D2DSVR_HOME

Identifica la carpeta donde se instala el servidor de copia de seguridad. Esta variable es aplicable para los scripts que se ejecutan en el servidor de copia de seguridad.

El script se crea.

Nota: En todos los scripts, un valor de retorno de cero indica que se ha realizado correctamente, mientras que un valor de retorno distinto a cero indica que se han producido errores.

Colocación del script en la carpeta prepost y verificación

Todos los scripts previos/posteriores para un servidor de copia de seguridad se gestionan centralmente desde la carpeta prepost en la ubicación siguiente:

```
/opt/CA/d2dserver/usr/prepost
```

Siga estos pasos:

1. Coloque el archivo en la siguiente ubicación del servidor de copia de seguridad:

   ```
   /opt/CA/d2dserver/usr/prepost
   ```

2. Proporcione los permisos de ejecución al archivo de script.
3. Inicie sesión en la interfaz web del Agente de Arcserve UDP (Linux).
4. Abra el **Asistente de copia de seguridad** o el **Asistente de restauración** y vaya a la ficha **Configuración avanzada**.
5. Seleccione el archivo de script en la lista desplegable **Configuración de scripts anteriores/posteriores** y, a continuación, envíe la tarea.
6. Haga clic en **Registro de actividad** y verifique que el script se ejecute en la tarea de copia de seguridad especificada.

   El script se ejecuta.

Los scripts anteriores/posteriores se crean correctamente y se colocan en la carpeta prepost.

Ejecución de la tarea de copia de seguridad

Ejecute la tarea de copia de seguridad para que se cree un punto de recuperación. Se puede utilizar este punto de recuperación para restaurar datos.

En la página Resumen, revise el resumen de los detalles de la copia de seguridad y proporcione un nombre de tarea para distinguirlo de otras tareas.

Siga estos pasos:

1. Revise el resumen e introduzca un nombre de tarea.

   El campo Nombre de la tarea tiene un nombre predeterminado inicialmente. Se puede introducir el nombre de la tarea nuevo que elija pero no se puede dejar vacío este campo.

2. (Opcional) Seleccione Anterior para modificar los valores de configuración en las páginas del asistente.

3. Haga clic en Enviar.

   Se iniciará el proceso de copia de seguridad. En la ficha Estado de la tarea, la tarea se agregará y aparecerá el estado de copia de seguridad.

Se crea y se ejecuta la tarea de copia de seguridad.

Verificación de que la copia de seguridad es correcta

Después de finalizar la tarea de copia de seguridad, verifique que el punto de recuperación se cree en el destino especificado.

Siga estos pasos:

1. Vaya al destino especificado donde ha almacenado los datos de copia de seguridad.

2. Verifique que los datos de copia de seguridad estén presentes en el destino.

   Por ejemplo, si el nombre de tarea de copia de seguridad es *Demostración* y el destino de copia de seguridad es xxx.xxx.xxx.xxx:/Data, vaya al destino de copia de seguridad y compruebe que se genera un nuevo punto de recuperación.

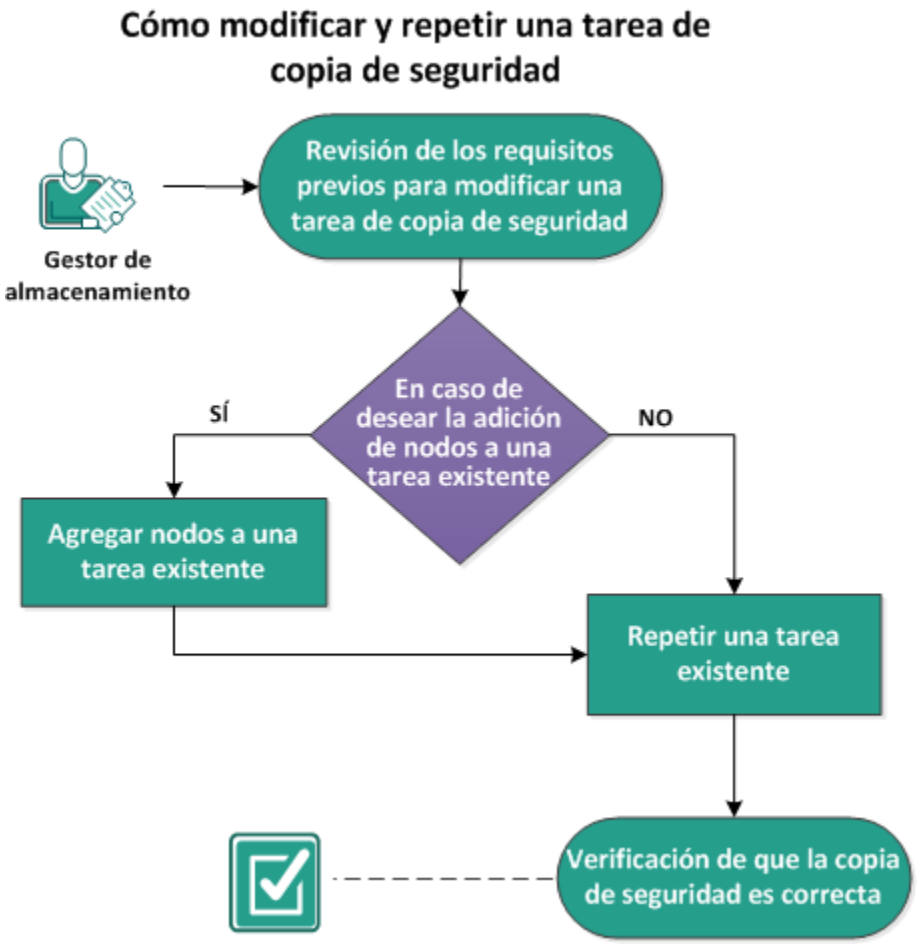
   Los datos de copia de seguridad se han verificado correctamente.

Se ha realizado una copia de seguridad de los nodos de Linux.

Cómo modificar y repetir una tarea de copia de seguridad

Si se ha creado ya una tarea para un nodo, se puede modificar y repetir la tarea varias veces. No es necesario crear otra tarea para proteger el mismo nodo. Si no se desea modificar la tarea, se puede ejecutar también la tarea sin realizar cambios. La modificación de una tarea incluye agregar un nodo a una tarea existente, configurar los valores de configuración de la tarea, o ambos.

El diagrama siguiente muestra el proceso para modificar y repetir una tarea de copia de seguridad:



Realice estas tareas para modificar y repetir una tarea de copia de seguridad:

- Revisión de los requisitos previos para modificar una tarea de copia de seguridad (en la página 80)
- En caso de desear la adición de nodos a una tarea existente (en la página 80)
- Adición de nodos a una tarea existente (en la página 80)
- Repetición de una tarea existente (en la página 81)
- Verificación de que la copia de seguridad es correcta (en la página 82)

Revisión de los requisitos previos para modificar una tarea de copia de seguridad

Verifique los requisitos siguientes antes de modificar y repetir una tarea de copia de seguridad:

- Dispone de una tarea de copia de seguridad válida.
- Ha agregado los nodos a Arcserve UDP.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

En caso de desear la adición de nodos a una tarea existente

Si ya se tiene una tarea de copia de seguridad y se desean proteger los nodos nuevos con los mismos valores de configuración de la copia de seguridad, se pueden agregar nodos a una tarea existente. Después de agregarlos, se pueden modificar también los valores de configuración de la copia de seguridad y ejecutar la tarea.

Adición de nodos a una tarea existente

Se pueden agregar nuevos nodos a una tarea de copia de seguridad existente y se podrá ejecutar la tarea. Todos los valores de configuración de la tarea seleccionada se aplican al nodo nuevo y no será necesario configurar ningún valor de configuración de copia de seguridad nuevo. Utilice esta opción si desea mantener los mismos valores de configuración de copia de seguridad para todos los nodos.

Siga estos pasos:

1. Seleccione todos los nodos nuevos en la ficha Nodos del panel Estado.
2. En el menú Asistente, haga clic en Copia de seguridad y seleccione Agregar nodos seleccionados a una tarea existente.

   Se abre el cuadro de diálogo Agregar nodos seleccionados a una tarea existente.
3. Seleccione una tarea de la lista desplegable Nombre de tarea y haga clic en Aceptar.

   El nodo se agrega a la tarea de copia de seguridad seleccionada y la columna Protegido en la ficha Nodos cambia a Sí.

Se agregan nodos a una tarea existente.

Repetición de una tarea de copia de seguridad existente

Repita la tarea de copia de seguridad para realizar otra copia de seguridad de los nodos especificados. Se crea un punto de recuperación después de cada copia de seguridad correcta. Si ya se ha realizado una copia de seguridad de un nodo, no será necesario crear otra tarea de copia de seguridad para realizar una copia de seguridad del nodo de nuevo. Todas las tareas anteriores aparecen en la ficha Estado de la tarea en el panel Estado.

Cuando se repite una tarea de copia de seguridad, especifique el tipo de tarea que desee repetir.

Nota: Si se actualiza cualquier información en la página Destino de copia de seguridad del Asistente de copia de seguridad antes de repetir una tarea, el tipo de trabajo cambiará automáticamente a *Copia de seguridad completa*.

Siga estos pasos:

1. Introduzca la dirección URL del Agente de Arcserve UDP (Linux) en un explorador web para abrir la interfaz de usuario.

   Nota: Durante la instalación del Agente de Arcserve UDP (Linux), recibirá la dirección URL para acceder al servidor y gestionarlo.
2. Haga clic en la ficha Estado de la tarea y seleccione la tarea que desee ejecutar.
3. Compruebe que el estado de la tarea seleccionada sea Finalizado o Listo.

   Finalizado implica que la tarea no está programada y Listo implica que sí.
4. Realice una de las acciones siguientes:
   - Para ejecutar la tarea sin ningún cambio,
     a. Haga clic en Ejecutar ahora en el menú Tarea.

        Aparecerá el cuadro de diálogo Ejecutar tarea de copia de seguridad ahora.
     b. Seleccione el tipo de copia de seguridad.

c. Seleccione una opción de la lista desplegable Ejecutar tarea para:

Nodo seleccionado

Especifica que la tarea de copia de seguridad se ejecuta solamente en el nodo seleccionado.

Todos los nodos protegidos por la tarea seleccionada

Especifica que la tarea de copia de seguridad se ejecuta en todos los nodos protegidos por la tarea seleccionada.

d. Haga clic en Aceptar.

Se cerrará el cuadro de diálogo Ejecutar tarea de copia de seguridad ahora. El estado de la tarea cambia a Activo en la ficha Estado de la tarea y se ejecuta la misma tarea de nuevo.

- Para modificar la tarea antes de ejecutarla, siga estos pasos:

a. Seleccione una tarea y haga clic en Modificar.

Se abrirá el Asistente de copia de seguridad.

b. Actualice el campo obligatorio en el Asistente de copia de seguridad.

c. Haga clic en Enviar.

La tarea se vuelve a ejecutar en función de la programación de tareas.

La tarea de copia de seguridad se repite correctamente.

Verificación de que la copia de seguridad es correcta

Después de finalizar la tarea de copia de seguridad, verifique que el punto de recuperación se cree en el destino especificado.

Siga estos pasos:

1. Vaya al destino especificado donde ha almacenado los datos de copia de seguridad.
2. Verifique que los datos de copia de seguridad estén presentes en el destino.

   Por ejemplo, si el nombre de tarea de copia de seguridad es *Demostración* y el destino de copia de seguridad es xxx.xxx.xxx.xxx:/Data, vaya al destino de copia de seguridad y compruebe que se genera un nuevo punto de recuperación.

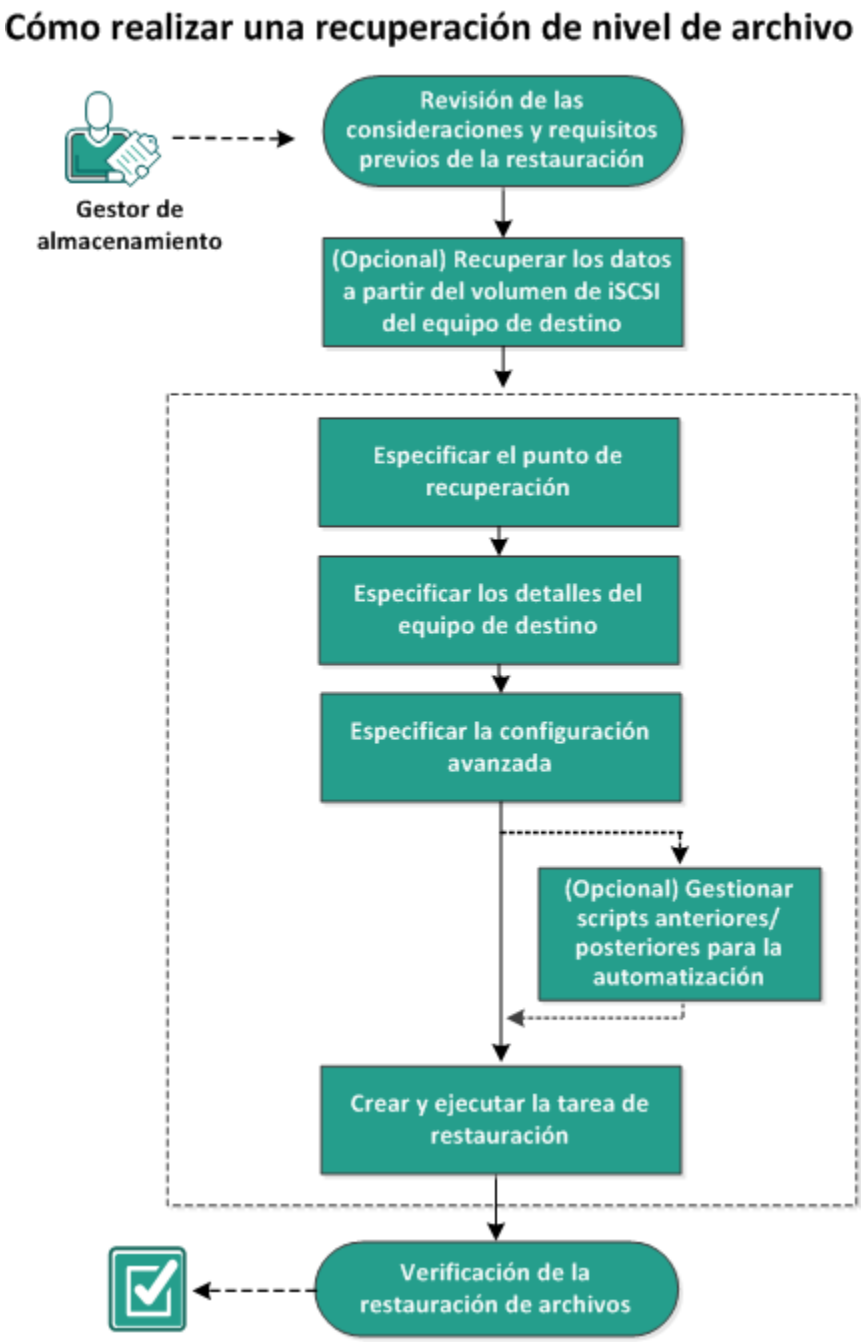
   Los datos de copia de seguridad se han verificado correctamente.

La tarea de copia de seguridad se modifica correctamente y se repite.

Cómo realizar una recuperación a nivel de archivo en nodos de Linux

Una recuperación de nivel de archivo restaura archivos y carpetas individuales desde un punto de recuperación. La restauración mínima consiste en restaurar un archivo del punto de recuperación. Esta opción es útil si se desea restaurar solo los archivos seleccionados y no todo el punto de recuperación.

El diagrama siguiente muestra el proceso para realizar una recuperación de nivel de archivo:



Realice estas tareas para realizar una recuperación de nivel de archivo:

- Revisión de los requisitos previos (en la página 85)
- (Opcional) Recuperación de los datos a partir del volumen de iSCSI del equipo de destino (en la página 86)
- Especificación del punto de recuperación (en la página 87)
- Especificación de los detalles del equipo de destino (en la página 91)
- Especificación de la configuración avanzada (en la página 95)
- (Opcional) Gestión de scripts anteriores/posteriores para la automatización (en la página 96)
- Creación y ejecución de la tarea de restauración (en la página 99)
- Verificación de la restauración de archivos (en la página 100)

Revisión de los requisitos previos

Tenga en cuenta las opciones siguientes antes de realizar una recuperación de nivel de archivo:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado, si hay.
- Tiene un nodo de destino válido para la recuperación de datos.
- Ha verificado que el servidor de copia de seguridad de Linux sea compatible con el sistema de archivos que desee restaurar.

  Por ejemplo, RedHat 5.x no es compatible con el sistema de archivos de *reiserfs.* Si el sistema operativo del servidor de copia de seguridad es RedHat 5.x y desea restaurar el sistema de archivos reiserfs, se deberá instalar el controlador del sistema de archivos para admitir reiserfs. También se puede utilizar el Live CD de Agente de Arcserve UDP (Linux) para realizar la restauración de nivel de archivo, ya que el Live CD es compatible con todos los tipos de sistema de archivos.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

(Opcional) Recuperación de los datos a partir del volumen de iSCSI del equipo de destino

Si se han almacenado sus datos en un volumen de destino de iSCSI, se puede conectar al volumen de iSCSI y recuperar datos. El volumen de iSCSI permite gestionar datos y transferirlos a una red.

Verifique que tiene la última versión del software del iniciador de iSCSI instalado en el servidor de copia de seguridad. El software de iniciador en sistemas de RHEL se encuentra dentro del paquete de iscsi-iniciador-utils. El software de iniciador en sistemas de SLES se encuentra dentro del paquete de open-iscsi.

Siga estos pasos:

1. Inicie sesión en el entorno de shell del servidor de copia de seguridad.
2. Ejecute uno de los siguientes comandos para iniciar el daemon del iniciador iSCSI.
   - Para los sistemas de RHEL:

     ```
     /etc/init.d/iscsid start
     ```

     El servicio en los sistemas de RHEL se denomina iscsid.
   - Para los sistemas de SLES:

     ```
     /etc/init.d/open-iscsi start
     ```

     El servicio en los sistemas de SLES se denomina open-iscsi.
3. Ejecute un script de detección para detectar el host de destino de iSCSI.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   El valor del puerto predeterminado del host de destino de iSCSI es 3260.
4. Tome nota del nombre completo de iSCSI (IQN) del host de destino de iSCSI que ha encontrado el script de detección antes de realizar el registro manual en el destino detectado.
5. Enumere el dispositivo de bloqueo disponible del servidor de copia de seguridad.

   ```
   #fdisk -l
   ```
6. Inicie sesión en el destino detectado.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p
   <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>  -l
   ```

   Se puede ver un dispositivo de bloqueo en el directorio /dev del servidor de copia de seguridad.

7. Ejecute el comando siguiente para obtener el nuevo nombre del dispositivo:

   ```
   #fdisk –l
   ```

   Se puede ver otro dispositivo denominado /dev/sd<x> en el servidor de copia de seguridad.

   Por ejemplo, tenga en cuenta que el nombre del dispositivo es /dev/sdc. Este nombre de dispositivo se utilizará para crear una partición y un sistema de archivos en los pasos siguientes.

8. Monte el volumen de iSCSI mediante los comandos siguientes:

   ```
   # mkdir /iscsi
   ```

   ```
   # mount /dev/sdc1 /iscsi
   ```

   Nota: Cuando se especifica la ubicación de la sesión en el asistente de restauración, será necesario seleccionar Local e introducir la ruta /iscsi.

   Ejemplo: <path>/iscsi

9. (Opcional) Agregue el registro siguiente al archivo /etc/fstab para que el volumen de iSCSI se conecte automáticamente al servidor de copia de seguridad después de reiniciar el servidor.

   ```
   /dev/sdc1 /iscsi ext3 _netdev 0 0
   ```

El servidor de copia de seguridad se puede conectar ahora al volumen de iSCSI y podrá recuperar datos del volumen de iSCSI.

Especificación del punto de recuperación

Cada vez que se realiza una copia de seguridad correcta, se creará un punto de recuperación. Especifique la información del punto de recuperación en el **Asistente de restauración** para que se puedan recuperar los datos exactos que desee. Se pueden restaurar archivos específicos o todos los archivos en función de sus requisitos.

Nota: Si se ha seleccionado **Origen local** como el destino de la copia de seguridad, el servidor de copia de seguridad no se puede conectar al origen local directamente. Para acceder al origen local, tiene que realizar configuraciones adicionales.

Para restaurar los archivos desde Origen local, siga estos pasos:

a. Comparta el destino de copia de seguridad (Origen local) y asegúrese de que el servidor de copia de seguridad se pueda conectar al destino de copia de seguridad.

b. Agregue el destino compartido al servidor de copia de seguridad como la ubicación de almacenamiento de copia de seguridad.

Ahora, Origen local se comporta como una ubicación de almacenamiento de copia de seguridad de NFS. Además, se pueden restaurar archivos desde el recurso compartido.

Siga estos pasos:

1. Acceda al asistente de restauración de una de las formas siguientes:
   - Desde Arcserve UDP:
     a. Inicie sesión en Arcserve UDP
     b. Haga clic en la ficha **recursos**.
     c. Seleccione **Todos los nodos** en el panel izquierdo.

        Se muestran todos los nodos agregados en el panel central.
     d. En el panel central, seleccione el nodo y haga clic en **Acciones**.
     e. Haga clic en **Restaurar** en el menú desplegable **Acciones**.

        Aparecerá la interfaz web del Agente de Arcserve UDP (Linux). Se muestra el cuadro de diálogo de selección del tipo de restauración en la interfaz de usuario del agente.
     f. Seleccione el tipo de restauración y haga clic en **Aceptar**.

        Nota: Se inicia sesión automáticamente en el nodo del agente y el **Asistente de restauración** se abre desde el nodo del agente.

- Desde el Agente de Arcserve UDP (Linux):

  a. Abra la interfaz web del Agente de Arcserve UDP (Linux).

  Nota: Durante la instalación del Agente de Arcserve UDP (Linux), recibirá la dirección URL para acceder al servidor y gestionarlo. Inicie sesión en el Agente de Arcserve UDP (Linux).

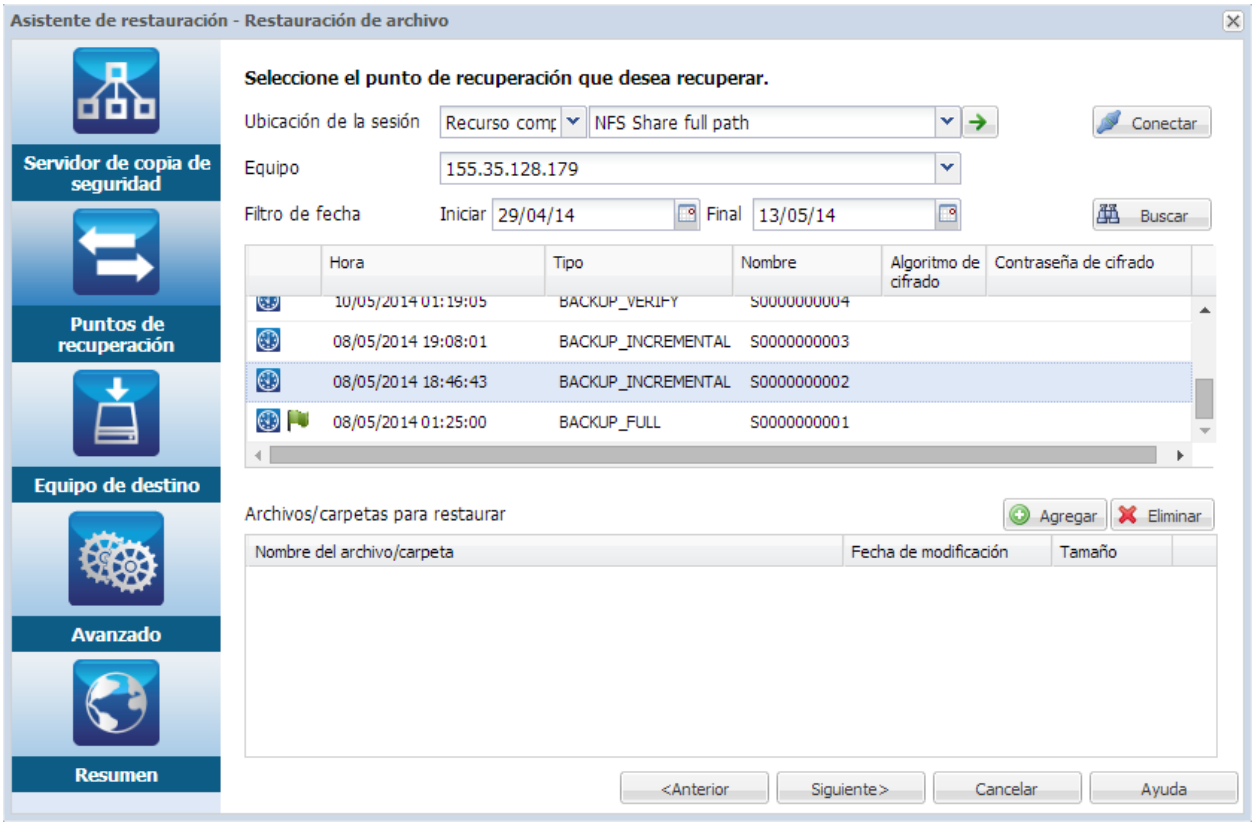
  b. Haga clic en **Restaurar** en el menú **Asistente** y seleccione **Archivo de restauración**.

  Se abre **Asistente de restauración - Restauración de archivo.**

Se puede ver el servidor de copia de seguridad en la página **Servidor de copia de seguridad** del **Asistente de restauración**. No se puede seleccionar ninguna opción en la lista desplegable **Servidor de copia de seguridad**.

2. Haga clic en **Siguiente**.

   Aparece la página **Puntos de recuperación** del **Asistente de restauración**. El punto de recuperación reciente se selecciona.



3. Seleccione una sesión en la lista desplegable **Ubicación de la sesión**, si se desea restaurar otra sesión, e introduzca la ruta completa del recurso compartido.

   Por ejemplo, tenga en cuenta la ubicación de la sesión como un recurso compartido de NFS, xxx.xxx.xxx.xxx como la dirección IP del recurso compartido de NFS y el nombre de la carpeta debe ser *Datos.* Introducirá xxx.xxx.xxx.xxx:/Data como ubicación compartida de NFS.

   Nota: Si los datos de la copia de seguridad se almacenan en Origen local, deberá convertirse primero el nodo de origen en un servidor de NFS y, a continuación, compartir la ubicación de la sesión.

4. Haga clic en **Conectar**.

   Todos los nodos de los cuales se ha realizado copia de seguridad en esta ubicación aparecen en la lista desplegable **Equipo.**

5. Seleccione el nodo que desee restaurar en la lista desplegable **Equipo.**

   Aparecen todos los puntos de recuperación del nodo seleccionado.

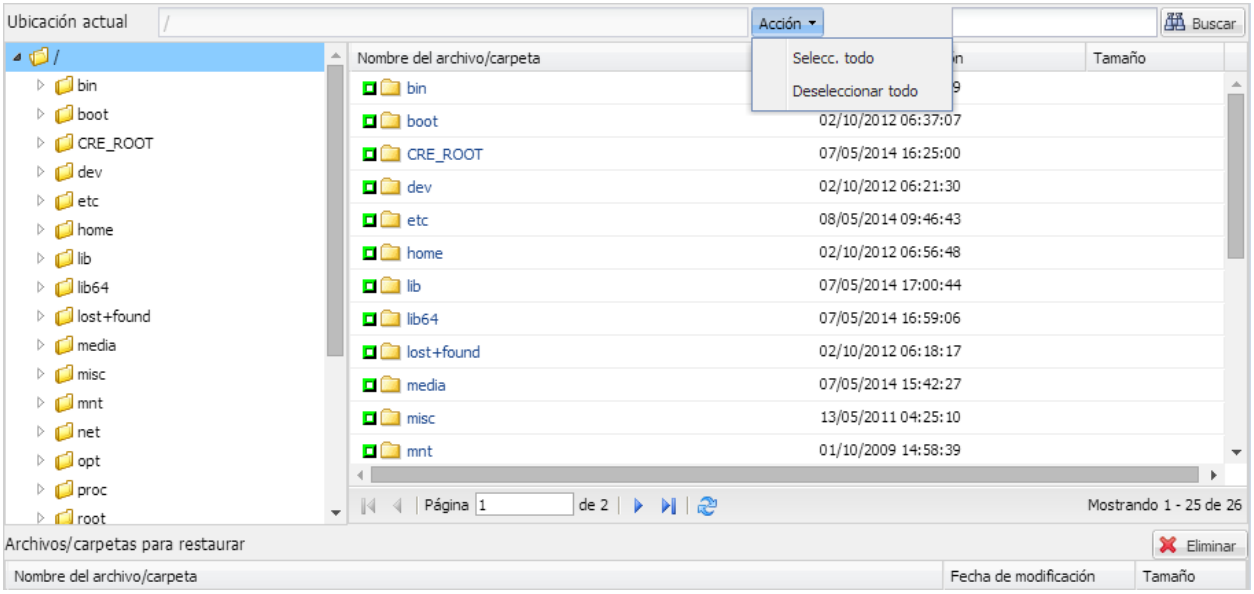
6. Aplique el filtro de fecha para que se muestren los puntos de recuperación que se han generado entre la fecha especificada y haga clic en **Buscar**.

   Valor predeterminado: Las dos últimas semanas.

   Se muestran todos los puntos de recuperación disponibles entre las fechas especificadas.

7. Seleccione el punto de recuperación que desee restaurar y haga clic en **Agregar**. Si se cifra el punto de recuperación, introduzca la contraseña de cifrado para restaurar datos.

   Aparece el cuadro de diálogo **Examinar <nombre de nodo>**.



8. Seleccione los archivos y las carpetas que desee restaurar y haga clic en **Aceptar**.

   Nota: Si desea ubicar un archivo o una carpeta mediante el campo **Buscar**, asegúrese de que se selecciona la carpeta superior en la jerarquía. La búsqueda se realiza en todas las carpetas secundarias de la carpeta seleccionada.

   El cuadro de diálogo **Examinar <nombre de nodo>** se cierra y vuelve a la página **Puntos de recuperación**. Los archivos y carpetas que se han seleccionado aparecen en **Archivos/carpetas para restaurar**.

9. Haga clic en **Siguiente**.

   Aparecerá la página **Equipo de destino**.

Se especifica el punto de recuperación.

Especificación de los detalles del equipo de destino

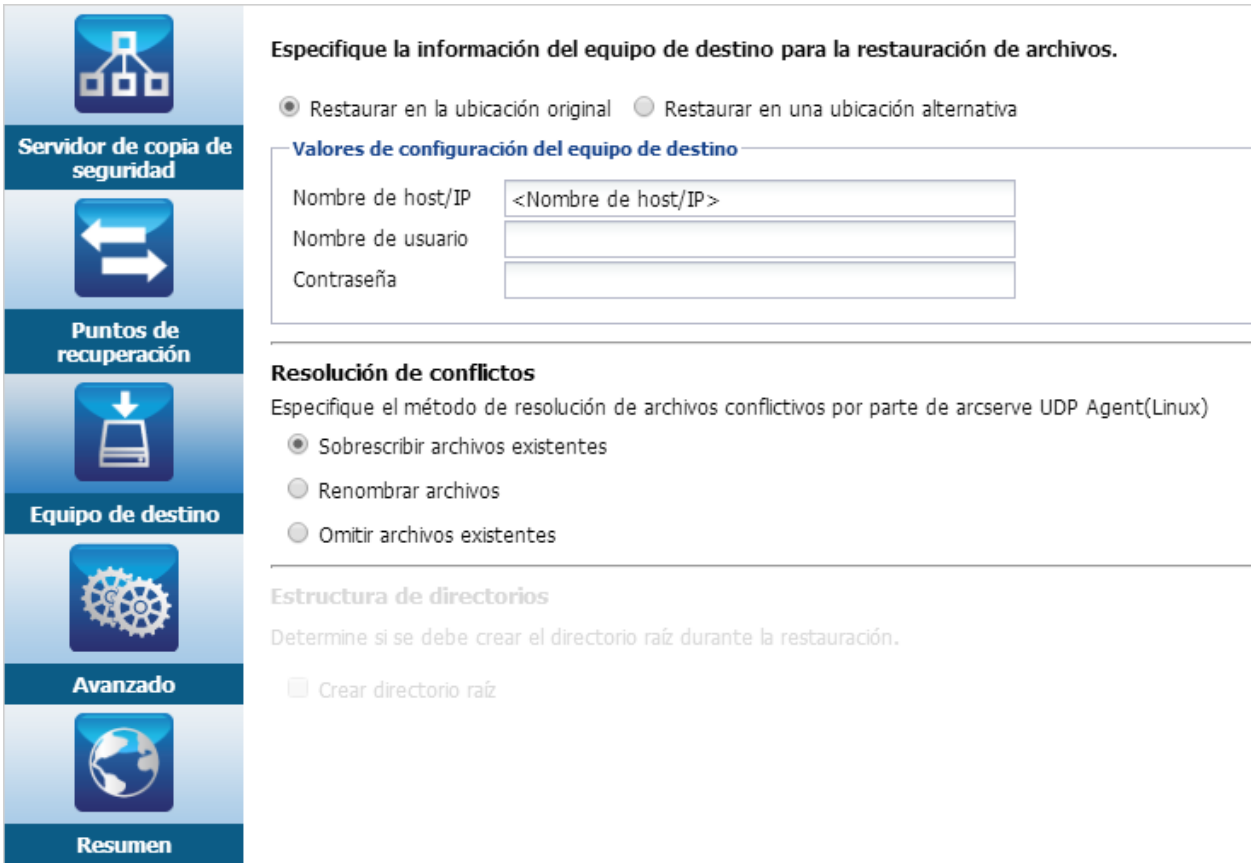
Especifique los detalles del nodo de destino para restaurar los datos en el nodo. Se pueden restaurar los archivos o las carpetas que se han seleccionado en el nodo de origen o en un nodo nuevo.

Siga estos pasos:

- Para realizar una restauración en el nodo del cual se ha realizado la copia de seguridad de los datos, siga los pasos siguientes:

  1. Seleccione **Restaurar en la ubicación original** de la página **Equipo de destino.**

     El campo **Nombre de host** en **Valores de configuración del equipo de destino** se rellena con el nombre del nodo de origen.



2. Introduzca el nombre de usuario y la contraseña del nodo.
3. Seleccione una de las opciones siguientes para resolver los archivos en conflicto:

   Sobrescribir archivos existentes

   Especifica si existe el archivo en el equipo de destino. A continuación, el archivo de copia de seguridad del punto de recuperación reemplazará el archivo existente.

   Cambiar el nombre de los archivos

   Especifica que, si el archivo existe en el equipo de destino, se creará a continuación un nuevo archivo con el mismo nombre de archivo y con la extensión de archivo *.d2dduplicate<x>.* <x> especifica el número de veces que se ha restaurado el archivo. Todos los datos se restaurarán en el nuevo archivo.

   Omitir archivos existentes

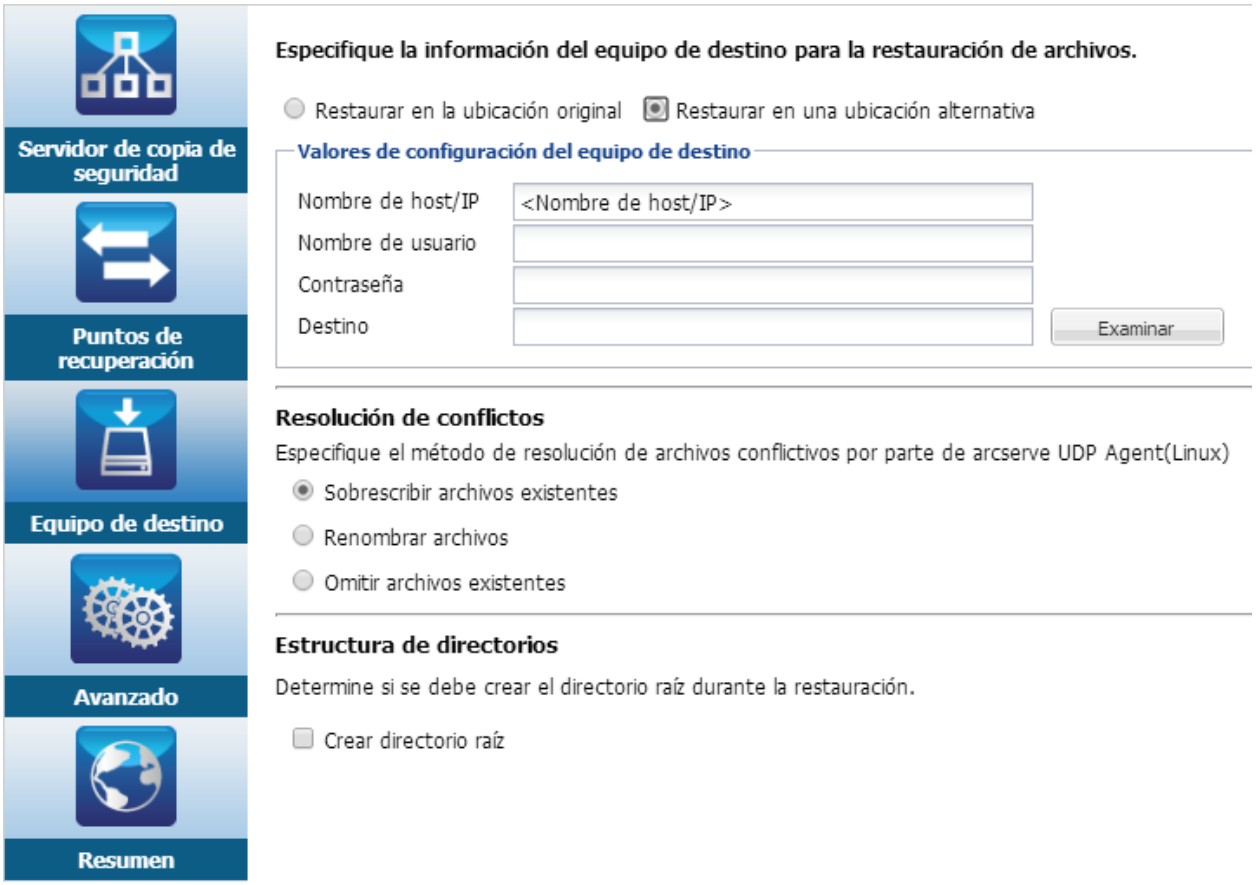
   Especifica que existe el mismo archivo en el equipo de destino. A continuación, los archivos no se restauran desde el punto de recuperación.

4. Haga clic en **Siguiente**.

   Aparecerá la página **Configuración avanzada**.

- Para restaurar en un nodo nuevo, siga estos pasos:

  1. Seleccione **Restaurar en una ubicación alternativa** desde la página **Equipo de destino.**



  2. Introduzca el nombre de host o la dirección IP del nodo de destino.
  3. Introduzca el nombre de usuario y la contraseña del nodo.
  4. Introduzca la ruta donde se restauran los datos o haga clic en **Examinar** para seleccionar la carpeta donde se restauran los datos y haga clic en **Aceptar.**

5. Seleccione una de las opciones siguientes para resolver los archivos en conflicto:

   Sobrescribir archivos existentes

   Especifica si existe el archivo en el equipo de destino. A continuación, el archivo de copia de seguridad del punto de recuperación reemplazará el archivo existente.

   Cambiar el nombre de los archivos

   Especifica que, si el archivo existe en el equipo de destino, se creará a continuación un nuevo archivo con el mismo nombre de archivo y con la extensión de archivo *.d2dduplicate<x>.* <x> especifica el número de veces que se ha restaurado el archivo. Todos los datos se restaurarán en el nuevo archivo.

   Omitir archivos existentes

   Especifica que existe el mismo archivo en el equipo de destino. Como consecuencia, los archivos no se restauran desde el punto de recuperación.

6. (Opcional) Seleccione **Crear directorio raíz**.
7. Haga clic en **Siguiente**.

   Aparecerá la página **Configuración avanzada**.

Se especifican los detalles del equipo de destino.

Especificación de la configuración avanzada

Especifique la configuración avanzada para realizar una recuperación programada de los datos. La recuperación programada asegura que los datos se recuperen en la hora especificada incluso en su ausencia.

Siga estos pasos:

1. Establezca la fecha y la hora de inicio seleccionando una de las opciones siguientes:

   Ejecutar ahora

   Inicia la tarea de restauración de nivel de archivo tan pronto como se envíe la tarea.

   Establecer fecha y hora de inicio

   Inicia la tarea de restauración de nivel de archivo a la hora especificada después de haber enviado la tarea.

2. (Opcional) Seleccione la **Estimación del tamaño del archivo**.
3. (Opcional) Seleccione un script de la opción **Configuración de scripts anteriores/posteriores**.

   Estos scripts ejecutan comandos de script para realizar acciones antes del inicio de la tarea o cuando esta se finalice.

   Nota: Los campos **Configuración de scripts previos y posteriores** se rellenan solamente si ya se ha creado un archivo de script y se ha colocado en la siguiente ubicación:

   ```
   /opt/CA/d2dserver/usr/prepost
   ```

   Nota: Para obtener más información acerca de cómo crear los scripts anteriores/posteriores, consulte *Gestión de scripts anteriores/posteriores para la automatización* (en la página 158).
4. Haga clic en **Siguiente**.

   Aparecerá la página **Resumen**.

Se especifica la configuración avanzada.

(Opcional) Gestión de scripts anteriores/posteriores para la automatización

Los scripts previos/posteriores permiten ejecutar su propia lógica empresarial en las etapas específicas de una tarea en ejecución. Se puede especificar cuando se ejecutan los scripts en **Configuración previa/posterior** de los scripts del **Asistente de copia de seguridad** y el **Asistente de restauración** en la interfaz de usuario. Los scripts se pueden ejecutar en el servidor de copia de seguridad en función de la configuración.

La gestión de scripts anteriores/posteriores constituye un proceso de dos partes que consta de la creación del script anterior/posterior y la colocación de dicho script en la carpeta prepost.

Creación de scripts anteriores/posteriores

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree un archivo de script mediante el uso de las variables de entorno en el lenguaje de generación de scripts preferido.

   Variables de entorno de scripts anteriores/posteriores

   Para crear un script, utilice las variables de entorno siguientes:

   D2D_JOBNAME

   Indica el nombre de la tarea.

D2D_JOBID

Identifica el ID de la tarea. El ID de la tarea es un número que se proporciona a la tarea cuando esta se ejecuta. Si se ejecuta la misma tarea de nuevo, obtendrá un nuevo número de tareas.

D2D_TARGETNODE

Identifica el nodo del cual se realiza copia de seguridad o que se restaura.

D2D_JOBTYPE

Identifica el tipo de tarea en ejecución. Los valores siguientes identifican la variable D2D_JOBTYPE:

backup.full

Identifica la tarea como copia de seguridad completa.

backup.incremental

Identifica la tarea como copia de seguridad incremental.

backup.verify

Identifica la tarea como copia de seguridad de verificación.

restore.bmr

Identifica la tarea como una reconstrucción completa. Esta tarea es de restauración.

restore.file

Identifica la tarea como una restauración de nivel de archivo. Esta tarea es de restauración.

D2D_SESSIONLOCATION

Identifica la ubicación donde se almacenan los puntos de recuperación.

D2D_PREPOST_OUTPUT

Identifica un archivo temporal. El contenido de la primera línea del archivo temporal aparecerá en el registro de actividades.

D2D_JOBSTAGE

Indica la etapa de la tarea. Los valores siguientes identifican la variable D2D_JOBSTAGE:

pre-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad antes de que se inicie la tarea.

post-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad después de que se complete la tarea.

pre-job-target

Identifica el script que se ejecuta en el equipo de destino antes de que se inicie la tarea.

post-job-target

Identifica el script que se ejecuta en el equipo de destino después de que se complete la tarea.

pre-snapshot

Identifica el script que se ejecuta en el equipo de destino antes de capturar la instantánea.

post-snapshot

Identifica el script que se ejecuta en el equipo de destino después de capturar la instantánea.

D2D_TARGETVOLUME

Identifica el volumen del cual se realiza copia de seguridad durante una tarea de copia de seguridad. Esta variable es aplicable para los scripts de instantáneas previas y posteriores para una tarea de copia de seguridad.

D2D_JOBRESULT

Identifica el resultado para un script de tarea de publicación. Los valores siguientes identifican la variable D2D_JOBRESULT:

success

Identifica el resultado como correcto.

fail

Identifica el resultado como incorrecto.

D2DSVR_HOME

Identifica la carpeta donde se instala el servidor de copia de seguridad. Esta variable es aplicable para los scripts que se ejecutan en el servidor de copia de seguridad.

El script se crea.

Nota: En todos los scripts, un valor de retorno de cero indica que se ha realizado correctamente, mientras que un valor de retorno distinto a cero indica que se han producido errores.

Colocación del script en la carpeta prepost y verificación

Todos los scripts previos/posteriores para un servidor de copia de seguridad se gestionan centralmente desde la carpeta prepost en la ubicación siguiente:

`/opt/CA/d2dserver/usr/prepost`

Siga estos pasos:

1. Coloque el archivo en la siguiente ubicación del servidor de copia de seguridad:

   `/opt/CA/d2dserver/usr/prepost`

2. Proporcione los permisos de ejecución al archivo de script.
3. Inicie sesión en la interfaz web del Agente de Arcserve UDP (Linux).
4. Abra el **Asistente de copia de seguridad** o el **Asistente de restauración** y vaya a la ficha **Configuración avanzada**.
5. Seleccione el archivo de script en la lista desplegable **Configuración de scripts anteriores/posteriores** y, a continuación, envíe la tarea.
6. Haga clic en **Registro de actividad** y verifique que el script se ejecute en la tarea de copia de seguridad especificada.

   El script se ejecuta.

Los scripts anteriores/posteriores se crean correctamente y se colocan en la carpeta prepost.

Creación y ejecución de la tarea de restauración

Cree y ejecute la tarea de restauración de modo que se pueda iniciar la recuperación de nivel de archivo. Verifique la información del punto de recuperación antes de restaurar los archivos. Si es necesario, se puede volver atrás y cambiar la configuración de restauración en el asistente.

Siga estos pasos:

1. Verifique los detalles de restauración en la página **Resumen** del **Asistente de restauración**.
2. (Opcional) Seleccione **Anterior** para modificar la información que se ha introducido en cualquiera de las páginas del **Asistente de restauración**.

3. Introduzca un nombre de la tarea y haga clic en **Enviar**.

   El campo **Nombre de la tarea** tiene un nombre predeterminado inicialmente. Se puede introducir el nombre de la tarea nuevo que elija pero no se puede dejar vacío este campo.

   Se cierra el **Asistente de restauración**. Se puede ver el estado de la tarea en la ficha **Estado de la tarea**.

Se ha creado y ejecutado la tarea de restauración correctamente.

Verificación de la restauración de archivos

Después de la finalización de la tarea de restauración, verifique que todos los archivos se restauren en el nodo de destino. Compruebe las fichas **Historial de tareas** y **Registro de actividad** en el panel **Estado** para controlar el progreso del proceso de restauración.

Siga estos pasos:

1. Vaya al equipo de destino en el que se han restaurado los datos.
2. Compruebe que los datos obligatorios del punto de recuperación se hayan restaurado.

   Los archivos se han verificado correctamente.

La recuperación de nivel de archivo se ha realizado correctamente.

Cómo crear un Live CD de arranque

Como gestor de almacenamiento, puede crear un Live CD de arranque. Cuando se cree, este Live CD de arranque contendrá una imagen completa de solo lectura del sistema operativo del equipo. Además, se puede utilizar para ofrecer una funcionalidad temporal del sistema operativo. Este Live CD incluye toda la configuración del sistema y los archivos del sistema operativo; además, se puede utilizar para desempeñar las siguientes funciones:

- Se puede utilizar el Agente de Arcserve UDP (Linux) sin instalar realmente el producto. Esto permite probar y evaluar el producto sin instalarlo, o bien realizar algunos cambios en la unidad de disco duro existente del equipo.
- Se puede instalar el Agente de Arcserve UDP (Linux) (en varios servidores) utilizando solamente un paquete de configuración. Sin Live CD, se deberán instalar dos archivos independientes (el archivo .bin y el paquete de utilidad de restauración) para instalar el Agente de Arcserve UDP (Linux). El paquete de utilidad de restauración se incluye en el mismo paquete de instalación de Live CD.
- Se puede realizar una reconstrucción completa (BMR). Se puede utilizar este Live CD para obtener la dirección IP del equipo de destino, que se requiere durante la reconstrucción completa.

La carpeta bin contiene los scripts que se pueden ejecutar desde la línea de comandos para crear un Live CD de arranque. La carpeta bin se encuentra en la ruta siguiente:

```
# /opt/CA/d2dserver/bin
```

El diagrama siguiente muestra el proceso para crear un Live CD de arranque:

En la lista siguiente se describe cada tarea para crear un Live CD de arranque:

- Revisión de los requisitos previos de Live CD (en la página 102)
- Instalación del paquete de la utilidad de restauración (en la página 102)
- Creación y verificación de Live CD de arranque (en la página 103)

Revisión de los requisitos previos de Live CD

Se deben tener en cuenta los requisitos previos siguientes antes de crear un Live CD:

- Dispone de las credenciales de inicio de sesión raíz para iniciar sesión en el servidor de copia de seguridad.
- Ha leído las Notas de la versión para comprender las funciones de un Live CD.
- Dispone del conocimiento de generación de scripts de Linux.
- Ha instalado la herramienta *mkisofs* en el servidor de copia de seguridad. El servidor de copia de seguridad utiliza la herramienta mkisofs para crear el archivo Live CD.iso.
- Como mínimo, dispone de una memoria gratis en su equipo de 1024 MB para iniciar y ejecutar Live CD.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Instalación del paquete de la utilidad de restauración

Se debe instalar el paquete de la utilidad de restauración para realizar cualquier operación de restauración. Si no se instala el paquete de la utilidad de restauración, no se podrá realizar ninguna restauración de nivel de archivos o de reconstrucción completa. Se puede instalar el paquete de la utilidad de restauración durante la instalación del Agente de Arcserve UDP (Linux). También se puede descargar e instalar el paquete de la utilidad de restauración en cualquier momento posterior a la instalación del Agente de Arcserve UDP (Linux).

Después de instalar el paquete de la utilidad de restauración, se podrá crear un Live CD.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Vaya a la carpeta bin mediante el siguiente comando:

   ```
   # cd /opt/CA/d2dserver/bin
   ```

3. Ejecute el comando siguiente para instalar el paquete de la utilidad de restauración:

   ```
   # ./configutility
   ```

   Se muestra un mensaje en el que se pide indicar la ruta del paquete de utilidad de restauración.

4. Indique la ruta completa donde se ha descargado el paquete de utilidad de restauración.

   Comenzará la instalación.

Se instala el paquete de la utilidad de restauración.

Creación y verificación de Live CD de arranque

Live CD crea el entorno del servidor de copia de seguridad sin instalar el software. Live CD facilita el proceso de reconstrucción completa utilizando una dirección IP en una red privada.

Live CD es un sistema operativo de equipo de arranque total que se ejecuta en la memoria del equipo, en lugar de cargarse desde el disco duro. Live CD permite experimentar y evaluar un sistema operativo sin instalarlo o cambiar el que ya existe en el equipo.

Siga estos pasos:

1. Vaya a la carpeta bin mediante el siguiente comando:

   ```
   # cd /opt/CA/d2dserver/bin
   ```

2. Ejecute el comando siguiente para crear un Live CD:

   ```
   # ./makelivecd
   ```

3. Vaya a la siguiente ubicación y compruebe que se haya creado el archivo LiveCD.iso:

   /opt/CA/d2dserver/packages

Se ha creado y verificado correctamente el Live CD de arranque. Si se desea utilizar el Live CD en una red virtual, se puede montar directamente el archivo LiveCD.iso en la máquina virtual. Si se desea utilizar el Live CD en un equipo físico, a continuación se debe grabar la imagen LiveCD.iso en un archivo multimedia (CD o DVD) y, después, utilizar el archivo multimedia para iniciar el equipo.

Cómo crear un Live CD de CentOS

Como gestor de almacenamiento, se puede crear un Live CD de CentOS. Live CD de CentOS es un entorno informático en memoria de CentOS. La finalidad de este Live CD es proporcionar a los usuarios la capacidad para experimentar la funcionalidad de CentOS sin instalarlo. Live CD se ejecuta en memoria, sin impacto en el disco duro. Los cambios que realiza en el entorno de tiempo de ejecución de Live CD se pierden después de reiniciar el equipo.

Este Live CD incluye toda la configuración del sistema y los archivos del sistema operativo; además, se puede utilizar para desempeñar las siguientes funciones:

- Se puede utilizar el Agente de Arcserve UDP (Linux) sin instalar realmente el producto. Esto permite probar y evaluar el producto sin instalarlo, o bien realizar algunos cambios en la unidad de disco duro existente del equipo.
- Se puede realizar una reconstrucción completa (BMR). Se puede utilizar este Live CD para obtener la dirección IP del equipo de destino, que se requiere durante la reconstrucción completa.

Cuándo debe utilizarse LiveCD de CentOS:

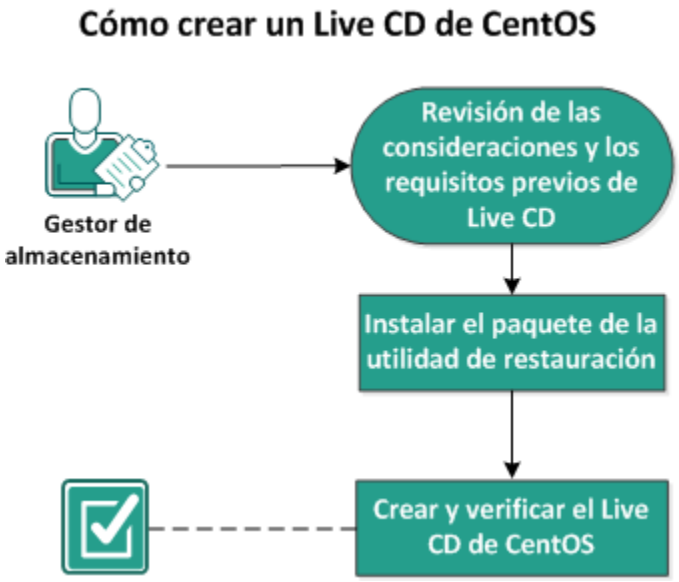
Cuando un LiveCD predeterminado no pueda identificar el dispositivo de almacenamiento ni el dispositivo de red puesto que falta el controlador de dispositivo.

Nota: Los puntos de recuperación para restaurar no incluyen los controladores de dispositivo para el sistema de almacenamiento del equipo de BMR de destino. Como resultado, el Agente de Arcserve UDP (Linux) bloqueará cualquier intento de realización de una tarea de reconstrucción completa en una primera etapa.

La carpeta bin contiene los scripts que se pueden ejecutar desde la línea de comandos para crear un Live CD de arranque. La carpeta bin se encuentra en la ruta siguiente:

```
# /opt/CA/d2dserver/bin
```

El diagrama siguiente muestra el proceso de creación de un Live CD de CentOS:



Realice las tareas siguientes para crear un Live CD basado en CentOS.

- Revisión de las consideraciones y los requisitos previos de Live CD (en la página 105)
- Instalación del paquete de la utilidad de restauración (en la página 107)
- Creación y verificación de Live CD de CentOS (en la página 107)

Revisión de las consideraciones y los requisitos previos de Live CD

Antes de crear un Live CD de CentOS, revise la tabla siguiente que compara un Live CD predeterminado con Live CD de CentOS:

Parámetros	Live CD predeterminado	Live CD de CentOS
Medios de instalación del servidor de copia de seguridad	Compatibles	No compatibles
IU de escritorio	No compatible. Los usuarios deben utilizar un explorador en un equipo Windows para explorar la interfaz de usuario web del servidor de copia de seguridad.	Compatible. Live CD de CentOS incluye un explorador. Los usuarios no necesitan ningún explorador adicional para explorar la interfaz de usuario web del servidor de copia de seguridad.
Tamaño de imagen	Aproximadamente 400 MB. La imagen se puede grabar en un CD.	Más de 800 MB. La imagen se puede grabar en un DVD.

Parámetros	Live CD predeterminado	Live CD de CentOS
Controlador de dispositivos adicional para Live CD	No compatible	Compatibles
BMR local **(Recuperación del equipo sin necesidad de instalar otro servidor de copia de seguridad)**	Compatibles	Compatibles
Imagen de inicio de PXE	Compatibles	No compatible
Eliminación de CD/ISO del equipo de destino de BMR después de iniciar el equipo	Compatibles	No compatible. Se deberá montar DVD/ISO en el equipo de destino de BMR durante todo el proceso de recuperación, hasta que BMR finalice la tarea y el equipo se reinicie.
Entorno del sistema operativo de Live CD en inglés	Sí	Sí. El escritorio de la interfaz de usuario también está en inglés
El idioma localizado para la interfaz de usuario web del servidor de copia de seguridad	Sí	Sí
Compatibilidad con el tipo de nodo	Admite el equipo físico, servidor ESX de VMWare, RHEV, OVM y la máquina virtual de Citrix	Solamente admite el equipo físico y la máquina virtual del servidor ESX de VMware

Tenga en cuenta los siguientes requisitos previos antes de crear Live CD de CentOS:

- Verifique que se hayan instalado los siguientes paquetes de software en el servidor de copia de seguridad:
  - genisoimage
  - squashfs-tools
- Solamente se puede iniciar Live CD de CentOS desde un equipo físico y una máquina virtual del servidor ESX. No admite otras soluciones de virtualización.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Instalación del paquete de la utilidad de restauración

Se debe instalar el paquete de la utilidad de restauración para realizar cualquier operación de restauración. Si no se instala el paquete de la utilidad de restauración, no se podrá realizar ninguna restauración de nivel de archivos o de reconstrucción completa. Se puede instalar el paquete de la utilidad de restauración durante la instalación del Agente de Arcserve UDP (Linux). También se puede descargar e instalar el paquete de la utilidad de restauración en cualquier momento posterior a la instalación del Agente de Arcserve UDP (Linux).

Después de instalar el paquete de la utilidad de restauración, se podrá crear un Live CD.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Vaya a la carpeta bin mediante el siguiente comando:

   ```
   # cd /opt/CA/d2dserver/bin
   ```

3. Ejecute el comando siguiente para instalar el paquete de la utilidad de restauración:

   ```
   # ./configutility
   ```

   Se muestra un mensaje en el que se pide indicar la ruta del paquete de utilidad de restauración.

4. Indique la ruta completa donde se ha descargado el paquete de utilidad de restauración.

   Comenzará la instalación.

Se instala el paquete de la utilidad de restauración.

Creación y verificación de Live CD de CentOS

Se puede utilizar este Live CD para iniciar un equipo de destino de BMR y, a continuación, ejecutar la tarea de reconstrucción completa. Los archivos siguientes se utilizan para crear un Live CD de CentOS:

makelivecd.centos

Script utilizado para remasterizar Live CD de CentOS.

CentOS-6.X-i386-LiveCD.iso

Imagen ISO de Live CD de CentOS. La imagen se puede descargar del sitio web de CentOS.

El punto de recuperación que se restaura no contiene ningún controlador de dispositivo para el sistema de almacenamiento del equipo de reconstrucción completa de destino. El Agente de Arcserve UDP (Linux) bloquea la tarea de reconstrucción completa en una primera etapa.

Siga estos pasos:

1. Prepare los controladores de dispositivo (archivos *.ko y *.rpm) para CentOS y almacénelos en una carpeta.

   Ejemplo: Almacene los controladores del dispositivo en la carpeta /tmp/drivers.

   Nota: Se debe proporcionar el controlador del dispositivo para que coincida con la versión de kernel de Live CD de CentOS.

2. Acceda al sitio web de CentOS y descargue CentOS 6.0 de 32 bits o un Live CD posterior a la carpeta /tmp del servidor de copia de seguridad.

   El archivo CentOS-6.X-i386-LiveCD.iso se ha descargado.

   Importante: Si se utiliza Live CD de CentOS 6.5 para restaurar desde ubicaciones de red, instale manualmente mount.nfs o mount.cifs en el servidor de Live CD.

3. Vaya a la carpeta de la papelera de reciclaje (/opt/CA/d2dserver/bin) y ejecute el comando siguiente:

   ```
   makelivecd.centos <full_path_to_CentOS_live_cd>
   <path_where_device_drivers_are_stored>
   ```

   Ejemplo: makelivecd.centos <full_path_to_CentOS_live_cd> /tmp/drivers

   El script crea un Live CD de Agente de Arcserve Unified Data Protection para Linux de CentOS y almacena el archivo de imagen ISO en la ubicación siguiente:

   ```
   /opt/CA/d2dserver/packages/CentOS-LiveCD-for-D2D.iso
   ```

4. Vaya a la carpeta de paquetes y compruebe que el archivo CentOS-LiveCD-for-D2D.iso se incluye en la carpeta.

   Live CD de CentOS se ha creado y verificado.

Se ha creado un Live CD de CentOS correctamente.

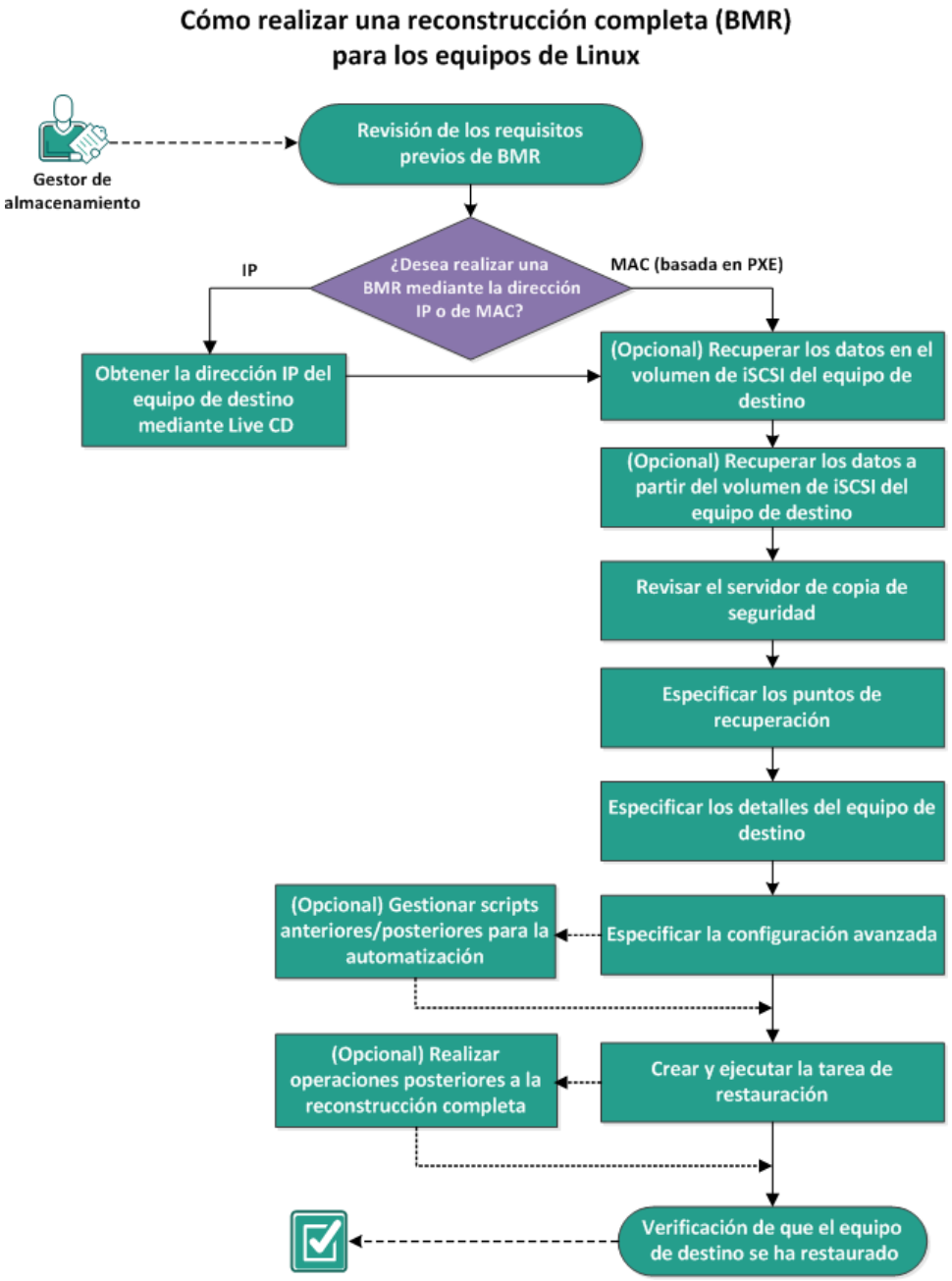
Cómo realizar una reconstrucción completa (BMR) para los equipos de Linux

Una reconstrucción completa restaura las aplicaciones de software y el sistema operativo y recupera todos los datos de copia de seguridad. BMR es el proceso de restauración de un sistema informático *a partir de una reconstrucción completa*. La reconstrucción completa es un equipo sin ningún sistema operativo, controladores ni aplicaciones de software. Después de finalizar la restauración, el equipo de destino se reinicia automáticamente en el mismo entorno operativo que el nodo de origen de la copia de seguridad y se restaurarán todos los datos.

La reconstrucción completa es posible porque cuando se realiza una copia de seguridad de los datos, la copia de seguridad también captura la información relacionada con el sistema operativo, las aplicaciones instaladas y los controladores, entre otros.

Se puede realizar una reconstrucción completa mediante la dirección IP o la dirección de control de acceso a medios (MAC) del equipo de destino. Si se inicia el equipo de destino mediante el Live CD del Agente de Arcserve UDP (Linux), se podrá obtener la dirección IP del equipo de destino.

El diagrama siguiente muestra el proceso para realizar una reconstrucción completa:



Complete las tareas siguientes para realizar una reconstrucción completa:

- Revisión de los requisitos previos de BMR (en la página 111)
- Obtención de la dirección IP del equipo de destino mediante Live CD (en la página 112)
- (Opcional) Recuperación de los datos en el volumen de iSCSI del equipo de destino (en la página 113)
- (Opcional) Recuperación de los datos a partir del volumen de iSCSI del equipo de destino (en la página 114)
- Revisión del servidor de copia de seguridad (en la página 116)
- Especificación de los puntos de recuperación (en la página 117)
- Especificación de los detalles del equipo de destino (en la página 120)
- Especificación de la configuración avanzada (en la página 120)
- (Opcional) Gestión de scripts anteriores/posteriores para la automatización (en la página 122)
- Creación y ejecución de la tarea de restauración (en la página 125)
- (Opcional) Realización de operaciones posteriores a la reconstrucción completa (en la página 126)
- Verificación de que el equipo de destino se ha restaurado (en la página 133)

Revisión de los requisitos previos de BMR

Tenga en cuenta las opciones siguientes antes de realizar una reconstrucción completa:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado para la restauración, si hay.
- Tiene un equipo de destino válido para la reconstrucción completa.
- Se ha creado el Live CD del Agente de Arcserve UDP (Linux).
- Si desea realizar una reconstrucción completa mediante la dirección IP, se deberá obtener la dirección IP del equipo de destino mediante Live CD.
- Si desea realizar una reconstrucción completa de PXE mediante la dirección MAC, se debe disponer de la dirección MAC del equipo de destino.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Obtención de la dirección IP del equipo de destino mediante Live CD

Antes de realizar una reconstrucción completa mediante la dirección IP, es necesario obtener la dirección IP del equipo de destino. Un equipo de reconstrucción completa no tiene ninguna dirección IP al principio. De este modo, se debe iniciar el equipo de reconstrucción completa utilizando el Live CD predeterminado, que es el Live CD del Agente de Arcserve UDP (Linux), o el Live CD basado en CentOS para obtener la dirección IP. Después de obtener la dirección IP del equipo de destino, se puede configurar la IP estática de dicho equipo.

Siga estos pasos:

1. Inserte el Live CD o monte el archivo .iso del Live CD en la unidad de CD-ROM del nodo de destino.
2. Inicie el equipo de destino desde el CD-ROM.

   El equipo de destino se inicia en el entorno de Live CD del Agente de Arcserve UDP (Linux). En la pantalla, aparece la dirección IP del equipo de destino.
3. Para configurar la IP estática del equipo de destino utilizando el Live CD predeterminado, siga estos pasos:
   a. En la pantalla del equipo de destino, pulse Intro para introducir el entorno de la shell.
   b. Ejecute el siguiente comando para configurar la IP estática:

      ```
      ifconfig <nombre de la NIC>  <dirección IP estática> netmask <máscara de red>
      ```

      ```
      route add default  gw  <dirección IP de la puerta de enlace> <nombre de la NIC>
      ```

Nota: El nombre de la tarjeta de interfaz de red (NIC) dependerá del hardware. Por ejemplo, los nombres de NIC habituales son eth0 o em0.

4. Para configurar la IP estática del equipo de destino utilizando el Live CD basado en CentOS, siga estos pasos:

   a. Abra una ventana de terminal en el equipo de destino haciendo clic en Aplicaciones, Herramientas del sistema, Terminal.

   b. Ejecute los siguientes comandos:

      ```
      sudo ifconfig <nombre de la NIC>  <dirección IP estática> netmask <máscara de red>
      ```

      ```
      sudo route add default  gw  <dirección IP de la puerta de enlace> <nombre de la NIC>
      ```

   Se configura la IP estática.

Se obtiene la dirección IP del equipo de destino.

Importante: Mantenga un registro de esta dirección IP puesto que se utilizará en el **Asistente de restauración** cuando se deban especificar los detalles del equipo de destino.

(Opcional) Recuperación de los datos en el volumen de iSCSI del equipo de destino

Se puede integrar el volumen de iSCSI en el equipo de destino y convertir este volumen en una parte del equipo de destino. A continuación se pueden restaurar datos en el volumen de iSCSI del equipo de destino. Si hace esto, se podrán gestionar datos y transferirlos a una red.

Importante: Cuando se integre el volumen de iSCSI con el equipo de destino, perderá todos los datos existentes del volumen de iSCSI.

Siga estos pasos:

1. Inserte Live CD del Agente de Arcserve UDP (Linux) o monte el archivo .iso de Live CD del Agente de Arcserve UDP (Linux) en la unidad de CD-ROM del equipo de destino.
2. Inicie el equipo de destino desde el CD-ROM.

   El equipo de destino se inicia en el entorno de Live CD del Agente de Arcserve UDP (Linux). En la pantalla, aparece la dirección IP del equipo de destino.

3. Introduzca el entorno de shell del equipo de destino.
4. Ejecute el comando siguiente para iniciar el daemon de iniciador iSCSI:

   ```
   /etc/init.d/iscsid start
   ```

5. Ejecute un script de detección para detectar el host de destino de iSCSI.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   El valor del puerto predeterminado del host de destino de iSCSI es 3260.
6. Tome nota del nombre completo de iSCSI (IQN) del host de destino de iSCSI que ha encontrado el script de detección antes de realizar el registro manual en el destino detectado.
7. Enumere el dispositivo de bloqueo disponible del nodo de destino.

   ```
   #fdisk -l
   ```

8. Inicie sesión en el destino detectado.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p
   <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l
   ```

   Se puede ver un dispositivo de bloqueo en el directorio /dev del nodo de destino.
9. Ejecute el comando siguiente para obtener el nuevo nombre del dispositivo:

   ```
   #fdisk –l
   ```

   Se puede ver otro dispositivo llamado /dev/sd<x> en el nodo de destino.

El volumen iSCSI se integra con el volumen de destino.

(Opcional) Recuperación de los datos a partir del volumen de iSCSI del equipo de destino

Si se han almacenado sus datos en un volumen de destino de iSCSI, se puede conectar al volumen de iSCSI y recuperar datos. El volumen de iSCSI permite gestionar datos y transferirlos a una red.

Siga estos pasos:

1. Inserte Live CD del Agente de Arcserve UDP (Linux) o monte el archivo .iso de Live CD del Agente de Arcserve UDP (Linux) en la unidad de CD-ROM del equipo de destino.
2. Inicie el equipo de destino desde el CD-ROM.

   El equipo de destino se inicia en el entorno de Live CD del Agente de Arcserve UDP (Linux). En la pantalla, aparece la dirección IP del equipo de destino.

3. Introduzca el entorno de shell del equipo de destino.
4. Ejecute el comando siguiente para iniciar el daemon de iniciador iSCSI:

   ```
   /etc/init.d/iscsid start
   ```

5. Ejecute un script de detección para detectar el host de destino de iSCSI.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   El valor del puerto predeterminado del host de destino de iSCSI es 3260.
6. Tome nota del nombre completo de iSCSI (IQN) del host de destino de iSCSI que ha encontrado el script de detección antes de realizar el registro manual en el destino detectado.
7. Enumere el dispositivo de bloqueo disponible del nodo de destino.

   ```
   #fdisk -l
   ```

8. Inicie sesión en el destino detectado.

   ```
   iscsiadm -m node -T <iSCSI Target IQN name> -p
   <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l
   ```

   Se puede ver un dispositivo de bloqueo en el directorio /dev del nodo de destino.
9. Ejecute el comando siguiente para obtener el nuevo nombre del dispositivo:

   ```
   #fdisk –l
   ```

   Se puede ver otro dispositivo llamado /dev/sd<x> en el nodo de destino.

   Por ejemplo, tenga en cuenta que el nombre del dispositivo es /dev/sdc. Este nombre de dispositivo se utilizará para crear una partición y un sistema de archivos en los pasos siguientes.
10. Monte el volumen de iSCSI mediante los comandos siguientes:

    ```
    # mkdir /iscsi
    ```

    ```
    # mount /dev/sdc1 /iscsi
    ```

    Nota: Cuando se especifica la ubicación de la sesión en el asistente de restauración, será necesario seleccionar Local e introducir la ruta /iscsi.

    Ejemplo: <path>/iscsi

El equipo de destino se puede conectar ahora al volumen de iSCSI y podrá recuperar datos del volumen de iSCSI.

Revisión del servidor de copia de seguridad

Cuando se abre el **Asistente de restauración**, revise el servidor de copia de seguridad donde se desea realizar la operación de restauración.

Siga estos pasos:

1. Acceda al asistente de restauración de una de las formas siguientes:
   - Desde Arcserve UDP:
     a. Inicie sesión en Arcserve UDP
     b. Haga clic en la ficha **recursos**.
     c. Seleccione **Todos los nodos** en el panel izquierdo.

        Se muestran todos los nodos agregados en el panel central.
     d. En el panel central, seleccione el nodo y haga clic en **Acciones**.
     e. Haga clic en **Restaurar** en el menú desplegable **Acciones**.

        Aparecerá la interfaz web del Agente de Arcserve UDP (Linux). Se muestra el cuadro de diálogo de selección del tipo de restauración en la interfaz de usuario del agente.
     f. Seleccione el tipo de restauración y haga clic en **Aceptar**.

        Nota: Se inicia sesión automáticamente en el nodo del agente y el **Asistente de restauración** se abre desde el nodo del agente.
   - Desde el Agente de Arcserve UDP (Linux):
     a. Abra la interfaz web del Agente de Arcserve UDP (Linux).

        Nota: Durante la instalación del Agente de Arcserve UDP (Linux), recibirá la dirección URL para acceder al servidor y gestionarlo. Inicie sesión en el Agente de Arcserve UDP (Linux).
     b. Haga clic en **Restaurar** en el menú **Asistente** y seleccione **Reconstrucción completa (BMR)**.

   Aparece la página **Servidor de copia de seguridad** del **Asistente de restauración - Restauración completa**.
2. Seleccione el servidor en la lista desplegable **Servidor de copia de seguridad** de la página **Servidor de copia de seguridad**.

   No se puede seleccionar ninguna opción en la lista desplegable **Servidor de copia de seguridad**.
3. Haga clic en **Siguiente**.

   Aparece la página **Puntos de recuperación** del **Asistente de restauración - Reconstrucción completa (BMR)**.

Se especifica el servidor de copia de seguridad.

Especificación de los puntos de recuperación

Cada vez que se realiza una copia de seguridad correcta, se creará un punto de recuperación. Especifique la información del punto de recuperación en el **Asistente de restauración** para que se puedan recuperar los datos exactos que desee. Se pueden restaurar archivos específicos o todos los archivos en función de sus requisitos.

Importante: Para realizar una reconstrucción completa de un punto de recuperación, el volumen de raíz y el volumen de inicio deberán estar presentes en el punto de recuperación.

Siga estos pasos:

1. Realice uno de los pasos siguientes en función del almacenamiento de la copia de seguridad.

   - Realice los pasos siguientes para acceder a los puntos de recuperación si los puntos de recuperación se almacenan en un dispositivo móvil:

     a. Inicie el equipo de destino mediante Live CD.

     b. Inicie sesión en la interfaz web del Agente de Arcserve UDP (Linux) desde el Live CD.

     c. Abra el **Asistente de reconstrucción completa**.

     d. Vaya a la página **Puntos de recuperación**.

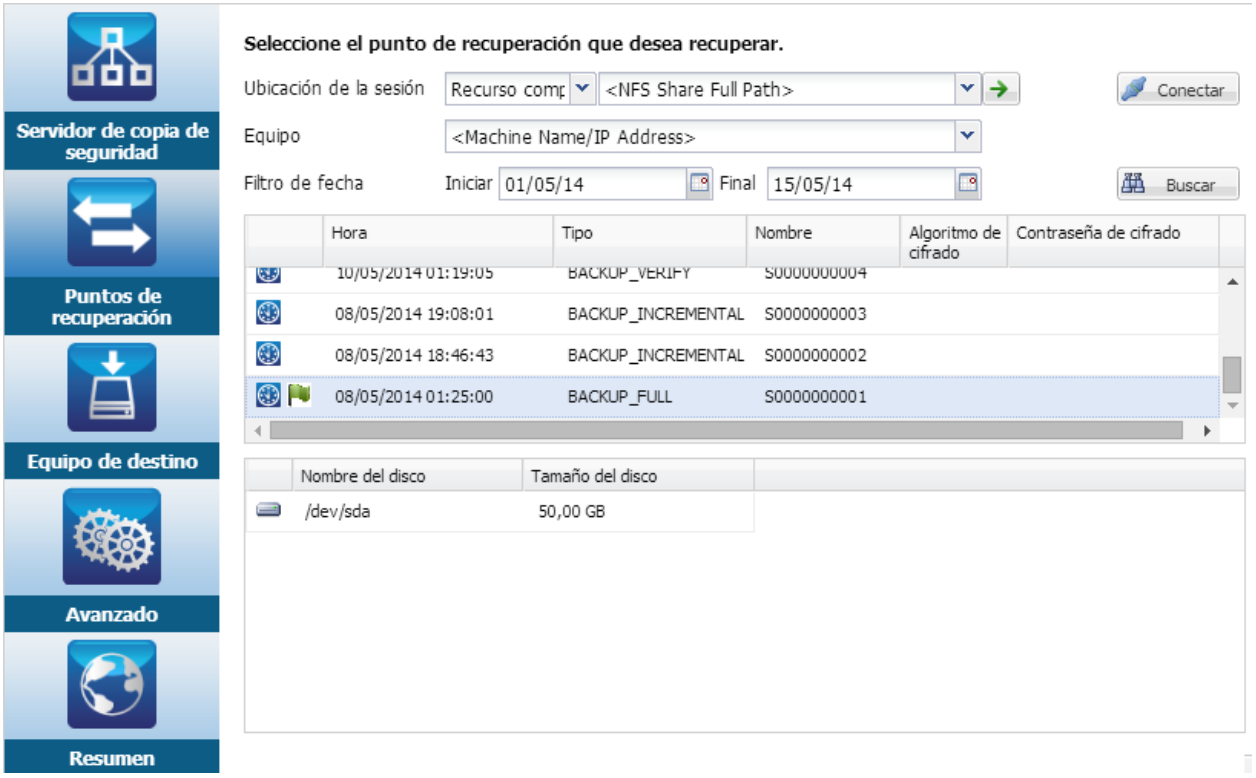
     e. Seleccione **Local** como la **Ubicación de la sesión** en la página **Puntos de recuperación** del **Asistente de reconstrucción completa**.

   - Realice los pasos siguientes si la ubicación de la sesión es un recurso compartido de NFS o de CIFS:

     a. Seleccione una sesión en la lista desplegable **Ubicación de la sesión** e introduzca la ruta completa del recurso compartido.

     Por ejemplo, tenga en cuenta la ubicación de la sesión como un recurso compartido de NFS, xxx.xxx.xxx.xxx como la dirección IP del recurso compartido de NFS y el nombre de la carpeta debe ser *Datos.* Introducirá xxx.xxx.xxx.xxx:/Data como ubicación compartida de NFS.

   Nota: Si los datos de la copia de seguridad se almacenan en Origen local, deberá convertirse primero el nodo de origen en un servidor de NFS y, a continuación, compartir la ubicación de la sesión.



2. Haga clic en **Conectar**.

   Todos los nodos de los cuales se ha realizado copia de seguridad en esta ubicación aparecen en la lista desplegable **Equipo.**

3. Seleccione el nodo que desee restaurar en la lista desplegable **Equipo.**

   Aparecen todos los puntos de recuperación del nodo seleccionado.

4. Aplique el filtro de fecha para que se muestren los puntos de recuperación que se han generado entre la fecha especificada y haga clic en **Buscar**.

   Valor predeterminado: Las dos últimas semanas.

   Se muestran todos los puntos de recuperación disponibles entre las fechas especificadas.

5. Seleccione el punto de recuperación que desee restaurar y haga clic en **Siguiente**.

   Aparecerá la página **Equipo de destino**.

Se especifica el punto de recuperación.

Especificación de los detalles del equipo de destino

Especifique los detalles del equipo de destino para que los datos se restauren en el equipo. Un equipo de destino es un equipo de reconstrucción completa donde se realizará una reconstrucción completa. Si se realiza una restauración mediante la dirección IP, será necesaria la dirección IP del equipo de destino que se ha registrado previamente al inicio de este proceso. Si se realiza una restauración mediante una dirección de control de acceso a medios (MAC), será necesaria la dirección de MAC del equipo de destino.

Siga estos pasos:

1. Introduzca la dirección MAC o la dirección IP del equipo de destino en el campo Dirección MAC/IP.
2. Introduzca un nombre en el campo Nombre del host.

   El equipo de destino utilizará este nombre como nombre del host después de que el proceso de restauración finalice.
3. Seleccione una de las opciones siguientes como red:

   DHCP

   Se configura la dirección IP automáticamente. Se trata de la opción predeterminada. Utilice esta opción si dispone de un servidor de protocolo de configuración dinámica de host (DHCP) para realizar la restauración con la red de DHCP.

   IP estática

   Se configura la dirección IP manualmente. Si se selecciona esta opción, introduzca la **Dirección IP**, la **Máscara de subred** y la **Puerta de enlace predeterminada** del equipo de destino.

   Importante: Asegúrese de que ningún otro equipo utilice la IP estática en la red durante el proceso de restauración.
4. (Opcional) Seleccione la opción **Reiniciar** para reiniciar automáticamente el nodo de destino después de finalizar la reconstrucción completa.
5. Haga clic en **Siguiente**.

   Aparecerá la página **Configuración avanzada**.

Se especifican los detalles del equipo de destino.

Especificación de la configuración avanzada

Especifique la configuración avanzada para realizar una reconstrucción completa programada de los datos. La reconstrucción completa programada garantiza que los datos se recuperen en la hora especificada incluso en su ausencia.

Siga estos pasos:

1. Establezca la fecha y la hora de inicio seleccionando una de las opciones siguientes:

   Ejecutar ahora

   Inicia la tarea de restauración en cuanto se envía la tarea.

   Establecer fecha y hora de inicio

   Inicia la tarea de restauración en la hora especificada después de haber enviado la tarea.

2. (Opcional) Seleccione un script de la opción **Configuración de scripts anteriores/posteriores** para el servidor de copia de seguridad y para el equipo de destino.

   Estos scripts ejecutan comandos de script para realizar acciones antes del inicio de la tarea o cuando esta se finalice.

   Nota: Los campos **Configuración de scripts previos y posteriores** se rellenan solamente si ya se ha creado un archivo de script y se ha colocado en la siguiente ubicación:

   ```
   /opt/CA/d2dserver/usr/prepost
   ```

   Nota: Para obtener más información acerca de cómo crear los scripts anteriores/posteriores, consulte *Gestión de scripts anteriores/posteriores para la automatización* (en la página 158).

3. (Opcional) Seleccione **Mostrar más valores de configuración** para mostrar más valores de configuración para la reconstrucción completa.

4. (Opcional) Restablezca la contraseña del nombre de usuario especificado para el equipo de destino recuperado.

5. (Opcional) Introduzca la ruta completa de la ubicación de almacenamiento de copia de seguridad de los puntos de recuperación en **Acceso local del punto de recuperación**.

6. (Opcional) Introduzca el nombre completo del disco en el campo **Discos** para excluir la participación de los discos en el equipo de destino durante el proceso de recuperación.

7. (Opcional) Seleccione **Activar Wake-on-LAN** si está realizando una reconstrucción completa del protocolo Medio de ejecución anterior al inicio (PXE).

   Nota: La opción **Activar Wake-on-LAN** es aplicable solamente para equipos físicos. Se debe garantizar que se haya activado la configuración de Wake-on-LAN en la configuración de BIOS del equipo físico.

8. Haga clic en **Siguiente**.

   Aparecerá la página **Resumen**.

Se especifica la configuración avanzada.

(Opcional) Gestión de scripts anteriores/posteriores para la automatización

Los scripts previos/posteriores permiten ejecutar su propia lógica empresarial en las etapas específicas de una tarea en ejecución. Se puede especificar cuando se ejecutan los scripts en **Configuración previa/posterior** de los scripts del **Asistente de copia de seguridad** y el **Asistente de restauración** en la interfaz de usuario. Los scripts se pueden ejecutar en el servidor de copia de seguridad en función de la configuración.

La gestión de scripts anteriores/posteriores constituye un proceso de dos partes que consta de la creación del script anterior/posterior y la colocación de dicho script en la carpeta prepost.

Creación de scripts anteriores/posteriores

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree un archivo de script mediante el uso de las variables de entorno en el lenguaje de generación de scripts preferido.

   Variables de entorno de scripts anteriores/posteriores

   Para crear un script, utilice las variables de entorno siguientes:

   D2D_JOBNAME

   Indica el nombre de la tarea.

   D2D_JOBID

   Identifica el ID de la tarea. El ID de la tarea es un número que se proporciona a la tarea cuando esta se ejecuta. Si se ejecuta la misma tarea de nuevo, obtendrá un nuevo número de tareas.

   D2D_TARGETNODE

   Identifica el nodo del cual se realiza copia de seguridad o que se restaura.

   D2D_JOBTYPE

   Identifica el tipo de tarea en ejecución. Los valores siguientes identifican la variable D2D_JOBTYPE:

   backup.full

   Identifica la tarea como copia de seguridad completa.

   backup.incremental

   Identifica la tarea como copia de seguridad incremental.

   backup.verify

   Identifica la tarea como copia de seguridad de verificación.

restore.bmr

Identifica la tarea como una reconstrucción completa. Esta tarea es de restauración.

restore.file

Identifica la tarea como una restauración de nivel de archivo. Esta tarea es de restauración.

D2D_SESSIONLOCATION

Identifica la ubicación donde se almacenan los puntos de recuperación.

D2D_PREPOST_OUTPUT

Identifica un archivo temporal. El contenido de la primera línea del archivo temporal aparecerá en el registro de actividades.

D2D_JOBSTAGE

Indica la etapa de la tarea. Los valores siguientes identifican la variable D2D_JOBSTAGE:

pre-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad antes de que se inicie la tarea.

post-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad después de que se complete la tarea.

pre-job-target

Identifica el script que se ejecuta en el equipo de destino antes de que se inicie la tarea.

post-job-target

Identifica el script que se ejecuta en el equipo de destino después de que se complete la tarea.

pre-snapshot

Identifica el script que se ejecuta en el equipo de destino antes de capturar la instantánea.

post-snapshot

Identifica el script que se ejecuta en el equipo de destino después de capturar la instantánea.

D2D_TARGETVOLUME

Identifica el volumen del cual se realiza copia de seguridad durante una tarea de copia de seguridad. Esta variable es aplicable para los scripts de instantáneas previas y posteriores para una tarea de copia de seguridad.

D2D_JOBRESULT

Identifica el resultado para un script de tarea de publicación. Los valores siguientes identifican la variable D2D_JOBRESULT:

success

Identifica el resultado como correcto.

fail

Identifica el resultado como incorrecto.

D2DSVR_HOME

Identifica la carpeta donde se instala el servidor de copia de seguridad. Esta variable es aplicable para los scripts que se ejecutan en el servidor de copia de seguridad.

El script se crea.

Nota: En todos los scripts, un valor de retorno de cero indica que se ha realizado correctamente, mientras que un valor de retorno distinto a cero indica que se han producido errores.

Colocación del script en la carpeta prepost y verificación

Todos los scripts previos/posteriores para un servidor de copia de seguridad se gestionan centralmente desde la carpeta prepost en la ubicación siguiente:

```
/opt/CA/d2dserver/usr/prepost
```

Siga estos pasos:

1. Coloque el archivo en la siguiente ubicación del servidor de copia de seguridad:

   ```
   /opt/CA/d2dserver/usr/prepost
   ```

2. Proporcione los permisos de ejecución al archivo de script.
3. Inicie sesión en la interfaz web del Agente de Arcserve UDP (Linux).
4. Abra el **Asistente de copia de seguridad** o el **Asistente de restauración** y vaya a la ficha **Configuración avanzada**.
5. Seleccione el archivo de script en la lista desplegable **Configuración de scripts anteriores/posteriores** y, a continuación, envíe la tarea.
6. Haga clic en **Registro de actividad** y verifique que el script se ejecute en la tarea de copia de seguridad especificada.

   El script se ejecuta.

Los scripts anteriores/posteriores se crean correctamente y se colocan en la carpeta prepost.

Creación y ejecución de la tarea de restauración

Cree y ejecute la tarea de restauración para que se pueda iniciar el proceso de reconstrucción completa. Antes de realizar una reconstrucción completa, verifique la información del punto de recuperación. Si es necesario, se puede volver y cambiar los valores de configuración de restauración.

Siga estos pasos:

1. Verifique los detalles de restauración en la página **Resumen** del **Asistente de restauración**.
2. (Opcional) Seleccione **Anterior** para modificar la configuración de restauración en cualquiera de las páginas del **Asistente de restauración**.
3. Introduzca un nombre de la tarea y haga clic en **Enviar**.

   El campo **Nombre de la tarea** tiene un nombre predeterminado inicialmente. Se puede introducir el nombre de la tarea nuevo que elija pero no se puede dejar vacío este campo.

   Se cierra el **Asistente de restauración**. Se puede ver la tarea en la ficha **Estado de la tarea.** Si se utiliza la dirección IP para la reconstrucción completa, el equipo de destino se reiniciará automáticamente en el mismo sistema operativo que el origen de la copia de seguridad después de que el proceso de BMR finalice.

   Si se utiliza la dirección de MAC para la reconstrucción completa, el estado en la ficha **Estado de la tarea** se cambia a *Esperando el inicio del nodo de destino*.
4. (Opcional) Para realizar el proceso de BMR mediante la dirección de MAC, inicie el equipo de destino cuando vea el mensaje *Esperando el inicio del nodo de destino* en la ficha **Estado de la tarea.**

   Nota: Si el equipo de destino se inicia antes de enviar la tarea de restauración, se deberá reiniciar el equipo de destino. Asegúrese de que se configure BIOS para realizar un inicio desde la red.

   El estado en la columna **Estado de la tarea** cambia a **Restaurando el volumen**. Esto indica que la restauración está en curso. Después de finalizar la tarea de restauración, el equipo de destino se reiniciará automáticamente con el mismo sistema operativo que el origen de copia de seguridad.

Se ha creado y ejecutado la tarea de restauración correctamente.

(Opcional) Realización de operaciones posteriores a la reconstrucción completa

Los temas siguientes son valores de configuración opcionales que es posible que deba ejecutar después de una reconstrucción completa:

Configuración de X Windows

Cuando se realiza una reconstrucción completa en un hardware distinto, X Windows del sistema operativo restaurado no funcionará correctamente y el nodo de destino mostrará un cuadro de diálogo de error. El cuadro de diálogo de error aparece porque la configuración de visualización ha cambiado. Para resolver este error, siga las instrucciones en el cuadro de diálogo de error para configurar la tarjeta gráfica. Después de esto, se podrá ver X Windows y la IU de escritorio.

Configure el nombre del dominio completamente calificado del sistema (FQDN)

Cuando se necesita un FQDN, se deberá configurar el FQDN. El proceso de reconstrucción completa no configura el FQDN automáticamente.

Número máximo de caracteres para FQDN: 63

Siga estos pasos para configurar el FQDN:

1. Edite el archivo */etc/hosts* y proporcione la dirección IP, el nombre FQDN y el nombre del servidor.

   ```
   #vi /etc/hosts

   ip_of_system  servername.domainname.com  servername
   ```

2. Reinicie el servicio de red.

   ```
   #/etc/init.d/network restart
   ```

3. Verifique el nombre de host y el nombre de FQDN.

   ```
   #hostname

   servername

   #hostname -f

   servername.domainname.com
   ```

Se configura el FQDN.

Extensión del volumen de datos después de una reconstrucción completa en discos distintos

Cuando se realiza una reconstrucción completa en un disco mayor que el disco del nodo original, habrá una parte de espacio en disco que no se utiliza. La operación de reconstrucción completa no procesa automáticamente el espacio en disco sin utilizar. Se puede formatear el espacio en disco a una partición separada o cambiar de tamaño la partición existente con el espacio en disco sin utilizar. El volumen que se desea cambiar de tamaño debe estar sin utilizar, de modo que se debe evitar cambiar de tamaño un volumen del sistema. En esta sección, nos centraremos en cómo extender un volumen de datos con el espacio en disco sin utilizar.

Nota: Para evitar la pérdida de datos, cambie de tamaño los volúmenes inmediatamente después del proceso de reconstrucción completa. Se puede realizar también una copia de seguridad del nodo antes de iniciar la tarea de cambio de tamaño del volumen.

Cuando el equipo de destino se reinicie correctamente después de la reconstrucción completa, se podrá extender el volumen de datos.

Volumen de partición sin formato

Por ejemplo, se restaura un disco de 2 GB de la sesión en otro de 16 GB denominado */dev/sdb* con solamente una partición. La partición sin formato */dev/sdb1* se monta directamente en el directorio */data*.

Este ejemplo se utiliza para explicar el procedimiento de extensión del volumen de partición sin formato.

Lleve a cabo los pasos siguientes:

1. Compruebe el estado del volumen /dev/sdb1.

```
# df –h /dev/sdb1
/dev/sdb1             2.0G   40M  1.9G   3% /data
```

2. Desmonte el volumen /dev/sdb1.

   ```
   # umount /data
   ```

3. Cambie de tamaño /dev/sdb1 para ocupar el espacio en disco entero mediante el comando fdisk.

   Para realizar esta operación, primero suprima la partición existente y, a continuación, vuélvala a crear con el mismo número de sector de inicio. El mismo número de sector de inicio es responsable de evitar la pérdida de datos.

   ```
   # fdisk -u /dev/sdb

   Comando (m para obtener ayuda): p

   Disk /dev/sdb: 17,1 GB - 17179869184 bytes

   255 cabezales, 63 sectores/pista, 2088 cilindros, 33554432 sectores totales

   Unidades = sectores de 1 * 512 = 512 bytes

   Arranque del
   dispositivo      Inicio         Final      Bloques   ID  Sistema

   /dev/sdb1              63     4192964     2096451   83  Linux

   Command (m for help): d

   Partición seleccionada 1

   Comando (m para obtener ayuda): n

   Acción de comando

   e   extendido

   p   partición principal (1-4)

   p

   Número de partición (1-4): 1

   Primer sector (63-33554431, valor predeterminado 63):

   Mediante el valor predeterminado 63

   Último sector o +size o +sizeM o +sizeK (63-33554431, valor predeterminado
   33554431):

   Mediante el valor predeterminado 33554431

   Comando (m para obtener ayuda): p

   Disk /dev/sdb: 17,1 GB - 17179869184 bytes

   255 cabezales, 63 sectores/pista, 2088 cilindros, 33554432 sectores totales

   Unidades = sectores de 1 * 512 = 512 bytes
   ```

```
Arranque del
dispositivo      Inicio         Final      Bloques   ID  Sistema

/dev/sdb1              63    33554431    16777184+  83  Linux

Comando (m para obtener ayuda): w
```

La partición cambia al mismo número de sector de inicio que la partición original y el número de sector final es 33554431.

4. Cambie de tamaño el volumen mediante el comando resize2fs. Si es necesario, ejecute primero el comando e2fsck.

```
# e2fsck -f /dev/sdb1

# resize2fs /dev/sdb1
```

5. Monte el volumen en el punto de montaje y compruebe el estado del volumen de nuevo.

```
# mount /dev/sdb1 /data

# df –h /dev/sdb1

/dev/sdb1              16G   43M   16G   1% /data
```

El volumen se extiende a 16 GB y está listo para el uso.

Volumen de LVM:

Por ejemplo, se restaura un disco de 8 GB de la sesión en otro de 16 GB denominado */dev/sdc* con una partición solamente. La partición sin formato */dev/sdc1* se utiliza como único volumen físico del /volumen lógico de LVM *dev/mapper/VGTest-LVTest* cuyo punto de montaje es */lvm*.

Este ejemplo se utiliza para explicar el procedimiento de extensión del volumen de LVM.

Lleve a cabo los pasos siguientes:

1. Compruebe el estado del volumen /dev/mapper/VGTest-LVTest.

```
# lvdisplay –m /dev/mapper/VGTest-LVTest

--- Volumen lógico ---

Nombre LV                /dev/VGTest/LVTest

Nombre VG                VGTest

LV UUID                  udoBIx-XKBS-1Wky-3FVQ-mxMf-FayO-tpfPl8

Acceso de escritura        lectura/escritura
```

```
Estado de LV              disponible
# open                 1
Tamaño de LV               7.88 GB
LE actual             2018
Segmentos               1
Adjudicación             heredada
Lectura anticipada de sectores     0
Dispositivo de bloques           253:2
--Segmentos---
Extensión lógica 0 a 2017:
Tipo                lineal
Volumen físico     /dev/sdc1
Extensiones físicas    0 a 2017
```

El volumen físico es */dev/sdc1*, el grupo del volumen es *VGTest* y el volumen lógico es */dev/VGTest/LVTest o /dev/mapper/VGTest-LVTest.*

2. Desmonte el volumen /dev/mapper/VGTest-LVTest.

```
# umount /lvm
```

3. Desactive el grupo del volumen en el cual se encuentra el volumen físico /dev/sdc1.

```
# vgchange -a n VGTest
```

4. Cree una partición para ocupar el espacio en disco sin utilizar mediante el comando fdisk.

```
# fdisk -u /dev/sdc
Comando (m para obtener ayuda): p
Disk /dev/sdc: 17,1 GB, 17179869184 bytes
255 cabezales, 63 sectores/pista, 2088 cilindros, 33554432 sectores totales
Unidades = sectores de 1 * 512 = 512 bytes
```

```
Arranque del
dispositivo      Inicio         Final      Bloques   ID  Sistema

/dev/sdc1              63    16777215     8388576+  83  Linux

Comando (m para obtener ayuda): n

Acción de comando

e   extendido

p   partición principal (1-4)

p

Número de partición (1-4): 2

Primer sector (16777216-33554431, valor predeterminado 16777216):

Mediante el valor predeterminado 16777216

Último sector o +size o +sizeM o +sizeK (16777216-33554431, valor
predeterminado 33554431):

Mediante el valor predeterminado 33554431

Comando (m para obtener ayuda): p

Disk /dev/sdc: 17,1 GB, 17179869184 bytes

255 cabezales, 63 sectores/pista, 2088 cilindros, 33554432 sectores totales

Unidades = sectores de 1 * 512 = 512 bytes

Arranque del
dispositivo      Inicio         Final      Bloques   ID  Sistema

/dev/sdc1              63    16777215     8388576+  83  Linux

/dev/sdc2        16777216    33554431     8388608   83  Linux

Comando (m para obtener ayuda): w
```

Se crea la partición /dev/sdc2.

5. Cree un nuevo volumen físico.

   ```
   # pvcreate /dev/sdc2
   ```

6. Extienda el tamaño del grupo del volumen.

   ```
   # vgextend VGTest /dev/sdc2
   ```

7. Active el grupo del volumen que ya se ha desactivado.

   ```
   # vgchange -a y VGTest
   ```

8. Extienda el tamaño del volumen lógico mediante el comando lvextend.

   ```
   # lvextend -L +8G /dev/VGTest/LVTest
   ```

9. Cambie de tamaño el volumen mediante el comando resize2fs. Si es necesario, ejecute primero el comando e2fsck.

   ```
   # e2fsck -f /dev/mapper/VGTest-LVTest
   ```

   ```
   # resize2fs /dev/mapper/VGTest-LVTest
   ```

10. Monte el volumen en el punto de montaje y compruebe el estado del volumen de nuevo.

    ```
    # mount /dev/mapper/VGTest-LVTest /lvm
    ```

    ```
    # lvdisplay -m /dev/mapper/VGTest-LVTest
    ```

    ```
    ---Volumen lógico---
    ```

    ```
    Nombre LV                /dev/VGTest/LVTest
    ```

    ```
    Nombre VG                VGTest
    ```

    ```
    LV UUID                GTP0a1-kUL7-WUL8-bpbM-9eTR-SVzl-WgA11h
    ```

    ```
    Acceso de escritura        lectura/escritura
    ```

    ```
    Estado de LV              disponible
    ```

    ```
    # open                 0
    ```

    ```
    Tamaño de LV                15.88 GB
    ```

    ```
    LE actual             4066
    ```

    ```
    Segmentos               2
    ```

    ```
    Adjudicación             heredada
    ```

    ```
    Lectura anticipada de sectores     0
    ```

    ```
    Dispositivo de bloques           253:2
    ```

    ```
    --- Segmentos ---
    ```

    ```
    Extensión lógica 0 a 2046:
    ```

    ```
    Tipo                lineal
    ```

    ```
    Volumen físico     /dev/sdc1
    ```

    ```
    Extensiones físicas    0 a 2046
    ```

    ```
    Extensión lógica 2047 a 4065:
    ```

    ```
    Tipo                lineal
    ```

    ```
    Volumen físico     /dev/sdc2
    ```

    ```
    Extensiones físicas    0 a 2018
    ```

    El volumen LVM se extiende a 16 GB y está listo para el uso.

Verificación de que el nodo de destino se ha restaurado

Después de finalizar la tarea de restauración, verifique que el nodo de destino se restaure con los datos relevantes.

Siga estos pasos:

1. Vaya al equipo de destino que se ha restaurado.
2. Verifique que el equipo de destino tiene toda la información de copia de seguridad.

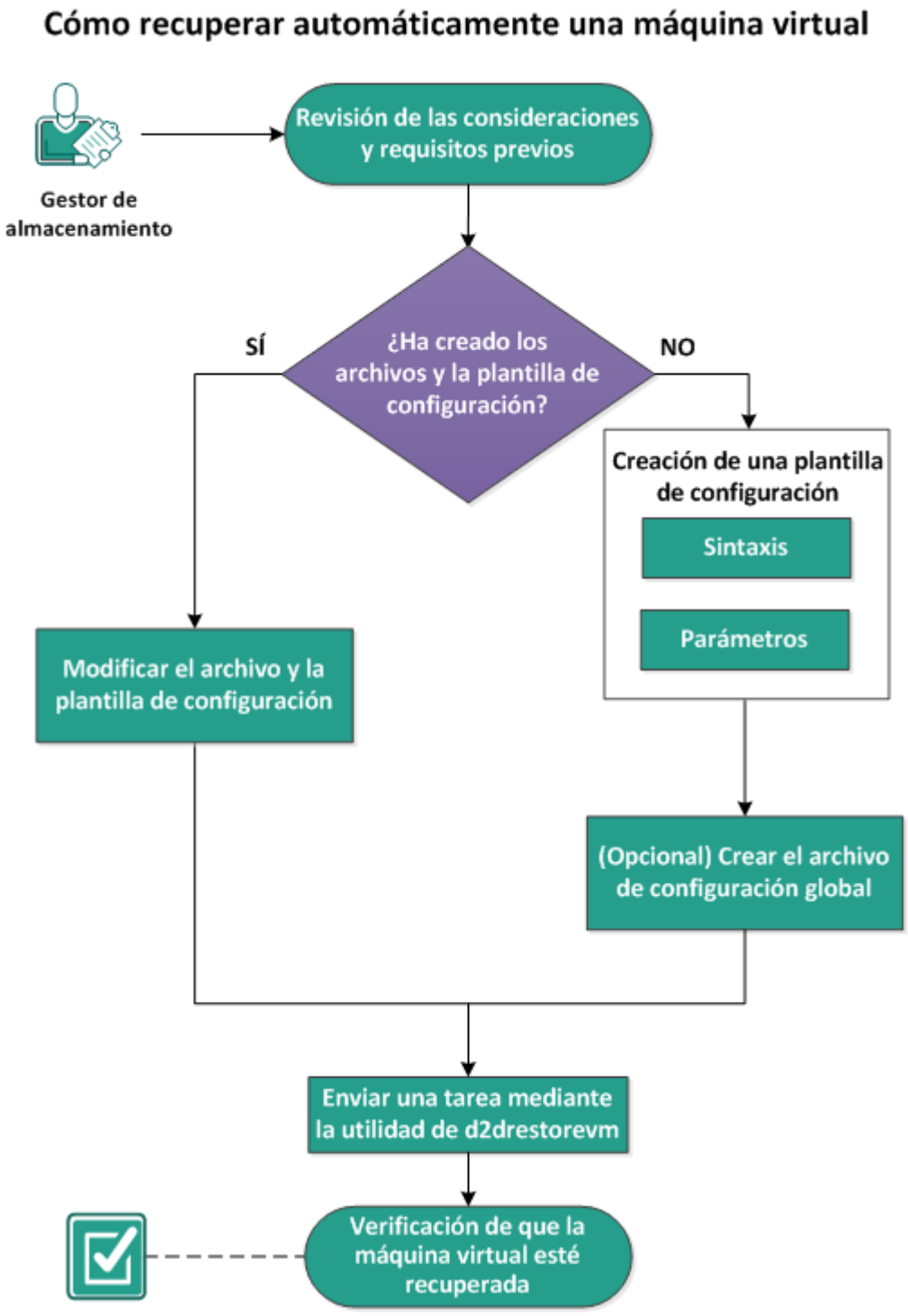
   El equipo de destino se ha verificado correctamente.

La reconstrucción completa se ha ejecutado correctamente en los equipos de Linux.

Cómo recuperar automáticamente una máquina virtual

Se puede recuperar una máquina virtual desde la línea de comandos del servidor de copia de seguridad mediante la utilidad d2drestorevm. La utilidad de d2drestorevm automatiza el proceso de realización de una reconstrucción completa sin la necesidad de iniciar manualmente la máquina virtual mediante Live CD.

El diagrama siguiente muestra el proceso de recuperación de una máquina virtual desde la línea de comandos a través de la utilidad de d2drestorevm:



Realice estas tareas para recuperar automáticamente una máquina virtual:

- Revisión de las consideraciones y requisitos previos (en la página 135)
- Creación de una plantilla de configuración (en la página 138)
- (Opcional) Creación del archivo de configuración global (en la página 142)
- Modificación del archivo y de la plantilla de configuración (en la página 143)
- Envío de una tarea mediante la utilidad de d2drestorevm (en la página 144)
- Verificación de que la máquina virtual esté recuperada (en la página 144)

Revisión de las consideraciones y requisitos previos

Revise los requisitos previos siguientes antes de restaurar la máquina virtual:

- Las versiones siguientes de hipervisores admiten BMR mediante la utilidad de d2drestorevm:
  - XenServer 6.0 y posteriores
  - RHEV 3.0 y posteriores
  - OVM 3.2
- La opción de restauración de la máquina virtual se puede realizar solamente desde la línea de comandos. Esta opción no está disponible en la interfaz de usuario.
- Se puede utilizar la interfaz de usuario para controlar el estado de la tarea y los registros de actividades. Se puede utilizar la interfaz de usuario para pausar, suprimir y repetir la tarea de restauración de la máquina virtual. Sin embargo, no se puede modificar la tarea de restauración de la máquina virtual.
- Antes de restaurar una máquina virtual, se tiene que configurar manualmente la máquina virtual en Xen, la máquina virtual de Oracle (OVM) o la virtualización de Red Hat Enterprise (RHEV).
- Al restaurar a las máquinas virtuales de OVM y Xen, será necesario instalar el servidor de NFS y ejecutarlo en el servidor de copia de seguridad. Verifique que el cortafuegos no esté bloqueando el servicio de NFS y que el hipervisor tenga los accesos y los permisos correctos para utilizar el servicio de NFS en el servidor de copia de seguridad.

- Cuando se restaura a RHEV, la versión Perl interpreter 5.10.0 y posteriores, junto con los módulos siguientes, se deberán instalar en el servidor de copia de seguridad:

  `XML::Simple`

  `URI::Escape`

  `WWW::Curl`

  `File::Copy`

  `File::Temp`

  Los módulos se pueden instalar con el gestor de paquetes del sistema. También se puede utilizar el gestor de paquetes de Perl y CPAN para instalar los módulos.

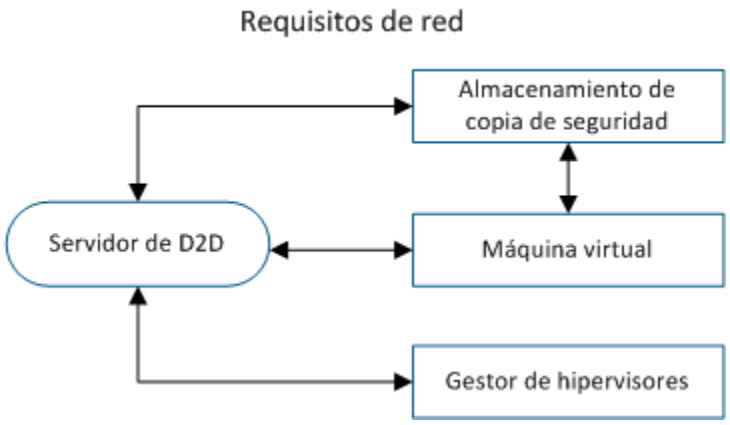
  Ejemplo: Instale "XML::Simple" mediante CPAN

  ```
  # perl -MCPAN -e "install XML::Simple"
  ```

  Ejecute el siguiente comando para verificar la instalación:

  ```
  # perldoc -l " XML::Simple"
  ```

- Para realizar una restauración correcta de la máquina virtual, tanto el hipervisor como la máquina virtual de destino deben tener una conexión de red válida con el servidor de copia de seguridad. El siguiente diagrama ilustra el requisito de redes.



El servidor de copia de seguridad intentará detectar automáticamente y configurar un NIC virtual para la máquina virtual. Sin embargo, a veces es posible que una red válida no se seleccione para el NIC. El parámetro vm_network permite especificar la red a la cual se debe conectar el NIC. Las consideraciones siguientes se refieren a distintas plataformas virtuales:

- Después de una instalación en XenServer, la red predeterminada se mostrará como Red 0 en XenCenter, que no es la red real. Cualquier red con el nombre "Red general asociada con xxx" aparecerá como "Red 0" en XenCenter. En tales casos, renombre la red predeterminada y utilice el valor nuevo para el parámetro vm_network.
- En RHEV, cuando el parámetro vm_network no se especifica, la red rhevm predeterminada tendrá una prioridad más alta.
- En OVM, se recomienda establecer manualmente el parámetro vm_network cuando haya más de una red disponible.

- Cuando se utiliza el recurso compartido de CIFS como ubicación de la copia de seguridad (sesión), tenga en cuenta los puntos siguientes:
  - Utilice el carácter / en lugar de \.
  - Los parámetros storage_username y storage_password son necesarios para verificar las credenciales para los recursos compartidos de CIFS.
- Como mínimo, se deberá especificar uno de los parámetros siguientes para que d2drestorevm funcione:

  `vm_name`

  `vm_uuid`

  Si se proporcionan los dos parámetros, estos deberán pertenecer a la misma máquina virtual. Si los parámetros pertenecen a distintas máquinas virtuales, se obtendrá un error.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Revise las siguientes consideraciones antes de restaurar la máquina virtual:

- Se recomienda restaurar las sesiones de la versión anterior de Agente de Arcserve UDP (Linux) o Agente de Arcserve Unified Data Protection para Linux en las máquinas virtuales originales.
- Cuando se restaura una máquina virtual en un XenServer PV y la máquina virtual restaurada muestra una pantalla en blanco aunque el SSH y otros servicios estén activos, verifique que el parámetro 'console='kernel esté correctamente establecido en los argumentos de inicio.
- Las sesiones de paravirtualización (PV) se pueden restaurar solamente en una máquina virtual de destino de PV de XenServer y OVM.
- Se pueden restaurar las sesiones de no PV en las VM de destino de no PV, como XenServer HVM, OVM HVM y RHEV.
- HVM de la serie RHEL 6 y sus derivados (RHEL 6, CentOS 6, y Oracle Linux6) se puede restaurar a la máquina virtual de PV.

Creación de una plantilla de configuración

Cree un archivo de configuración para que el comando d2drestorevm pueda restaurar las máquinas virtuales basadas en los parámetros especificados en el archivo. El archivo d2drestorevm recopila todas las especificaciones del archivo y realiza la restauración basándose en las especificaciones.

Sintaxis

```
d2drestorevm --createtemplate=[save path]
```

La utilidad d2dutil --encrypt cifra la contraseña y proporciona una contraseña cifrada. Se debe utilizar esta utilidad para cifrar todas las contraseñas. Si se utiliza el parámetro --pwdfile=pwdfilepath, se deberá cifrar la contraseña. Se puede utilizar la utilidad de acuerdo con los métodos siguientes:

Método 1

```
echo "string" | d2dutil --encrypt
```

string es la contraseña que se especifica.

Método 2

Escriba el comando "d2dutil –encrypt" y, a continuación, especifique la contraseña. Pulse Intro y verá el resultado en su pantalla. Si se elige este método, la contraseña introducida no se registra en la pantalla.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree la plantilla de configuración utilizando el comando siguiente:

   ```
   d2drestorevm --createtemplate=[save path]
   ```

   [save path] indica la ubicación donde se crea la plantilla de configuración.
3. Abra la plantilla de configuración y actualice los parámetros siguientes en la plantilla de configuración:

   job_name

   Especifica el nombre de la tarea de restauración.

   vm_type

   Especifica el tipo del hipervisor donde se restaura la máquina virtual. Los tipos válidos de hipervisores son xen, ovm y rhev.

   vm_server

   Especifica la dirección del servidor de hipervisor. La dirección puede ser el nombre de host o la dirección IP.

   vm_svr_username

   Especifica el nombre de usuario del hipervisor. El nombre de usuario se debe introducir con el formato siguiente para RHEV:

   ```
   [nombreusuario]@[dominio]
   ```

   El nombre de usuario se debe introducir con el formato siguiente para OVM y Xen:

   ```
   [nombreusuario]
   ```

   vm_svr_password

   Especifica la contraseña del hipervisor. La contraseña se cifra utilizando la utilidad de cifrado d2dutil.

vm_name

Especifica el nombre de la máquina virtual de destino que se muestra en el hipervisor.

Importante: El parámetro vm_name no debe contener caracteres especiales excepto espacios en blanco y debe incluir solamente los caracteres siguientes: a-z, A-Z, 0-9, - y _.

vm_uuid

Especifica el uuid de la máquina virtual de destino.

vm_network

(Opcional) Especifica el nombre de red que se desea utilizar. Si no se proporciona el nombre de red, a continuación la red predeterminada se selecciona automáticamente.

storage_location

Especifica la ubicación del servidor de almacenamiento de la sesión. La ubicación de almacenamiento puede ser CIFS o NFS.

storage_username

Especifica el nombre de usuario cuando se utiliza CIFS como la ubicación de almacenamiento.

storage_password

Especifica la contraseña cuando se utiliza CIFS como la ubicación de almacenamiento. La contraseña se cifra utilizando la utilidad de cifrado d2dutil.

encryption_password

Especifica la contraseña de cifrado de la sesión. La contraseña se cifra utilizando la utilidad de cifrado d2dutil.

source_node

Especifica el nombre de nodo del origen cuyo punto de recuperación se utiliza para restaurar.

recovery_point

Especifica la sesión que se desea restaurar. Normalmente, una sesión de recuperación tiene el formato siguiente: S00000000X, dónde X es un valor numérico. Si se desea restaurar la sesión más reciente, especifique la palabra clave 'last'.

guest_hostname

Especifica el nombre de host que se desea proporcionar después de restaurar la máquina virtual.

guest_network

Especifica el tipo de red que se desea configurar. La red puede ser dhcp o estática.

guest_ip

Especifica la dirección IP cuando se especifica la dirección IP estática.

guest_netmask

Especifica la máscara de red cuando se especifica la dirección IP estática.

guest_gateway

Especifica la dirección de la puerta de enlace cuando se especifica la dirección IP estática.

guest_reboot

(Opcional) Especifica si la máquina virtual de destino se debe reiniciar o no después de restaurar la máquina virtual. Los valores son sí y no.

Valor predeterminado: no

guest_reset_username

(Opcional) Especifica que se debe restablecer la contraseña al valor proporcionado en el parámetro guest_reset_password.

guest_reset_password

(Opcional) Especifica que se debe restablecer la contraseña al valor especificado. La contraseña se cifra utilizando la utilidad de cifrado d2dutil.

force

Especifica si se debe forzar o no la restauración de la máquina virtual. Los valores son sí y no.

Valor predeterminado: no

4. Guarde y cierre la plantilla de configuración.

La plantilla de configuración se ha creado correctamente.

(Opcional) Creación del archivo de configuración global

El archivo de configuración global (vm.cfg) tiene parámetros y valores relacionados con las ubicaciones de almacenamiento donde se crean los discos virtuales de VM. Los valores para las ubicaciones de almacenamiento se detectan automáticamente durante el proceso de restauración. El archivo vm.cfg anula los valores relacionados con las ubicaciones de almacenamiento y otros parámetros. Si desea especificar su propia ubicación de almacenamiento en lugar del valor que se detecta automáticamente, se puede utilizar el archivo vm.cfg.

El archivo de configuración global se encuentra en la ubicación siguiente:

```
/opt/CA/d2dserver/configfiles/vm.cfg
```

Los parámetros siguientes se pueden configurar en el archivo vm.cfg:

Parámetros generales

D2D_VM_PORT

Permite especificar un puerto personalizado para comunicarse con el servidor del hipervisor.

- Para OVM, el comando d2drestorevm requiere la interfaz de OVM CLI y el puerto predeterminado es 10000.
- Para XenServer, el comando d2drestorevm se comunica con el servidor mediante SSH y el puerto predeterminado será 22.
- Para RHEV, el comando d2drestorevm utiliza la API de transferencia de estado representacional (REST) para comunicarse con el servidor mediante HTTPS.

Parámetros específicos de OVM

OVM_ISO_REPOSITORY

Permite establecer manualmente el repositorio para cargar el Live CD del Agente de Arcserve UDP (Linux).

OVM_ISO_UPLOAD_SERVER

Permite especificar manualmente el servidor del repositorio para cargar el Live CD del Agente de Arcserve UDP (Linux).

OVM_DISK_REPOSITORY

Permite utilizar el repositorio de OVM específico para crear discos virtuales.

Nota: La utilidad de d2drestorevm utiliza el ID para los parámetros específicos de OVM.

Parámetros específicos de RHEV

RHEV_DISK_STORAGE_DOMAIN

Permite utilizar el dominio de almacenamiento específico de RHEV para crear discos virtuales. La utilidad de d2drestorevm utiliza el nombre de archivo léxico para los parámetros específicos de RHEV.

Parámetros específicos de Xen

XEN_DISK_SR

Permite utilizar el dominio de almacenamiento específico de Xen para crear discos virtuales. La utilidad de d2drestorevm utiliza el nombre de archivo léxico para los parámetros específicos de Xen.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad.
2. Cree el archivo de configuración global y cambie el nombre a vm.cfg.
3. Abra el archivo de configuración global y actualice los parámetros en el archivo.
4. Guarde y cierre el archivo.
5. Coloque el archivo en la carpeta configfiles:

   `/opt/CA/d2dserver/configfiles/vm.cfg`

El archivo de configuración global se ha creado correctamente.

Modificación del archivo y de la plantilla de configuración

Si ya se dispone de la plantilla de configuración y del archivo de configuración global, se pueden modificar los archivos y restaurar otra máquina virtual. No es necesario crear más plantillas de configuración y archivos cada vez que se restaura una máquina virtual. Cuando se envía la tarea, se agrega una tarea nueva en la interfaz de usuario web. Se pueden ver los registros de actividades en la interfaz de usuario web.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.

2. Abra la plantilla de configuración en la ubicación donde ha guardado el archivo y modifique los parámetros si es necesario.
3. Guarde y cierre la plantilla de configuración.
4. (Opcional) Abra el archivo de configuración global en la ubicación siguiente y modifique los parámetros si es necesario:

   ```
   /opt/CA/d2dserver/configfiles/vm.cfg
   ```

5. Guarde y cierre el archivo de configuración global.

El archivo y la plantilla de configuración se han modificado correctamente.

Envío de una tarea mediante la utilidad de d2drestorevm

Ejecute el comando de d2drestorevm para restaurar la máquina virtual. El comando verifica la máquina virtual de destino y envía una tarea de restauración. La tarea de restauración se puede ver en la interfaz de usuario web. Si no se cumple algún requisito durante el proceso de restauración, obtendrá un error. Se puede ver el registro de actividades en la interfaz de usuario web.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Envíe la tarea de restauración para la máquina virtual mediante el comando siguiente:

   ```
   d2drestorevm --template=cfg_file_path [--wait]
   ```

   Nota: El conmutador --wait permite volver al entorno de shell después de finalizar la tarea de restauración. Si el conmutador --wait no está presente, el usuario volverá al entorno de shell inmediatamente después de enviar la tarea.

Se envía la tarea de restauración.

Verificación de que la máquina virtual esté recuperada

Después de finalizar la tarea de restauración, verifique que el nodo de destino se restaure con los datos relevantes.

Siga estos pasos:

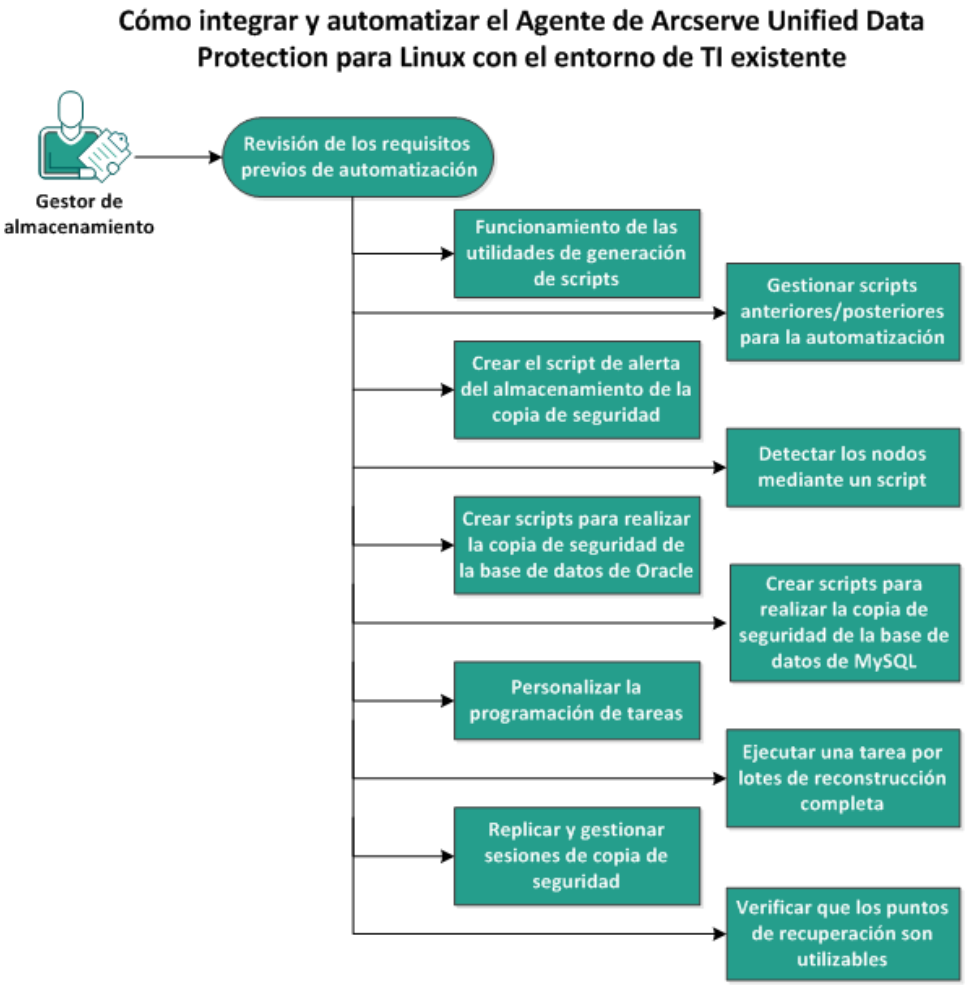
1. Vaya a la máquina virtual que se ha restaurado.
2. Verifique que la VM dispone de toda la información de la cual se ha realizado copia de seguridad.

   La máquina virtual se ha verificado correctamente.

Cómo integrar y automatizar Agente de Arcserve Unified Data Protection para Linux con el entorno de TI existente

Como gestor de almacenamiento se pueden crear scripts y automatizar tareas para integrar el Agente de Arcserve UDP (Linux) con el entorno de TI existente. Los scripts reducen la intervención manual y reducen la dependencia en la interfaz web del servidor de copia de seguridad para realizar cualquier tarea. El Agente de Arcserve UDP (Linux) también proporciona la interfaz y las utilidades para realizar la administración de tareas, gestión de nodos y las tareas de gestión del registro de actividad.

El diagrama siguiente muestra el proceso para integrar y automatizar el Agente de Arcserve UDP (Linux) con el entorno de TI existente:



Realice las tareas siguientes para automatizar y gestionar el Agente de Arcserve UDP (Linux):

Revisión de los requisitos previos de automatización

Tenga en cuenta los siguientes requisitos previos antes de automatizar y gestionar el Agente de Arcserve UDP (Linux):

- Dispone de las credenciales de inicio de sesión raíz para el servidor de copia de seguridad.
- Dispone del conocimiento de generación de scripts de Linux.
- Comprende mejor el funcionamiento de la interfaz web del Agente de Arcserve UDP (Linux).
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Funcionamiento de las utilidades de generación de scripts

El Agente de Arcserve UDP (Linux) proporciona algunas utilidades de generación de scripts para ayudar a crear el script de automatización. Estas utilidades solo se utilizan para la generación de scripts de modo que el resultado sea una generación de scripts descriptiva. Las utilidades se utilizan para gestionar nodos, tareas, replicar destinos de la copia de seguridad, así como gestionar registros de actividad.

Todas las utilidades se encuentran en la carpeta *bin* en la siguiente ubicación:

```
/opt/CA/d2dserver/bin
```

La utilidad d2dutil --encrypt cifra la contraseña y proporciona una contraseña cifrada. Se debe utilizar esta utilidad para cifrar todas las contraseñas. Si se utiliza el parámetro --pwdfile=pwdfilepath, se deberá cifrar la contraseña. Se puede utilizar la utilidad de acuerdo con los métodos siguientes:

Método 1

```
echo "string" | d2dutil --encrypt
```

string es la contraseña que se especifica.

Método 2

Escriba el comando "d2dutil –encrypt" y, a continuación, especifique la contraseña. Pulse Intro y verá el resultado en su pantalla. Si se elige este método, la contraseña introducida no se registra en la pantalla.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Vaya a la carpeta *bin* mediante el siguiente comando:

   ```
   # cd/opt/CA/d2dserver/bin
   ```

3. Ejecute los comandos siguientes para gestionar los nodos:

   `# ./d2dnode`

   Muestra una lista de comandos disponibles para facilitar la gestión de todos los nodos de Linux relacionados. Mediante este comando, se pueden agregar, suprimir, modificar e importar nodos. Se pueden agregar también nodos mediante las credenciales no raíz.

   Nota: Se pueden utilizar todos los parámetros del comando d2dnode cuando el servidor de copia de seguridad es un Agente de Linux independiente. Cuando la consola de UDP gestiona el servidor de copia de seguridad, el comando d2dnode le permite realizar solamente los parámetros list, add, modifiy e import. Los parámetros list, add, modify e import actualizarán el nodo en la consola de UDP. Por ejemplo, el comando ./d2dnode --list enumerará todos los nodos de Linux que se han agregado a la consola de UDP.

   `# ./d2dnode --list enumera todos los nodos que gestiona el servidor de copia de seguridad.`

   `# ./d2dnode -–add=nodename/ip -–user=username -–password=password -–description="the description of that node" --attach=jobname --force`

   Agrega al servidor de copia de seguridad el nodo específico. Si se trata de un usuario raíz, utilice este comando para agregar nodos.

   Nota: Si se cambia el número de puerto del nodo, se deberá especificar el número de puerto nuevo en el parámetro --add como se muestra en el ejemplo siguiente.

   Ejemplo: # ./d2dnode -–add=nodename/ip:new_port -–user=username -–password=password -–description="the description of that node" --attach=jobname --force

   --attach=jobname

   Agrega un nuevo nodo a una tarea de copia de seguridad existente.

   --force

   Agrega el nodo de forma forzosa incluso si otro servidor de copia de seguridad lo gestiona. Si se elimina el parámetro *force*, entonces no se agregará el nodo a este servidor si lo gestiona otro servidor de copia de seguridad.

```
# ./d2dnode --add=nodename --user=username --password=password
--rootuser=rootaccount --rootpwd=rootpassword --pwdfile=pwdfilepath
--description=description --attach=jobname –force
```

Agrega al servidor de copia de seguridad el nodo específico. Si se trata de un usuario no raíz, utilice este comando para agregar nodos.

Nota: Si se cambia el número de puerto del nodo, se deberá especificar el número de puerto nuevo en el parámetro --add como se muestra en el ejemplo siguiente.

Ejemplo: # ./d2dnode --add=nodename/ip:new_port --user=username --password=password --rootuser=rootaccount --rootpwd=rootpassword --pwdfile=pwdfilepath --description=description --attach=jobname –force

--user=username

Especifica el nombre de usuario del usuario no raíz.

--password=password

Especifica la contraseña del usuario no raíz. Si se proporciona el parámetro --pwdfile=pwdfilepath, no se tiene que especificar este parámetro.

--rootuser=rootaccount

Especifica el nombre de usuario del usuario raíz.

--rootpwd=rootpassword

Especifica la contraseña del usuario raíz. Si se proporciona el parámetro --pwdfile=pwdfilepath, no se tiene que especificar este parámetro.

--pwdfile=pwdfilepath

(Opcional) Especifica la contraseña del usuario raíz y del usuario no raíz. Este parámetro es opcional y se utiliza si se han almacenado las contraseñas del usuario raíz y los usuarios no raíz en un archivo independiente. El archivo de contraseña incluye los parámetros siguientes: -- password=password y --rootpwd=rootpassword. Para mayor seguridad, la contraseña se deberá cifrar mediante la utilidad -encrypt de d2dutil. Después de cifrar la contraseña, reemplace la contraseña anterior por la contraseña cifrada en el parámetro --pwdfile.

```
# ./d2dnode --node=nodename --attach=jobname
```

Agrega el nodo especificado a una tarea de copia de seguridad existente.

```
# ./d2dnode --modify=nodename/ip --user=username --password=newpassword
--description=newdescription
```

Modifica el nombre del usuario, la contraseña o la descripción del nodo agregado. Si se trata de un usuario raíz, utilice este comando para modificar los nodos.

```
# ./d2dnode --modify=nodename --user=username --password=newpassword
--rootuser=rootaccount --rootpwd=newrootpassword --pwdfile=pwdfilepath
--description=newdescription
```

Modifica el nombre del usuario, la contraseña o la descripción del nodo agregado. Si se trata de un usuario no raíz, utilice este comando para modificar los nodos.

--user=username

Especifica el nombre de usuario del usuario no raíz.

--password=newpassword

Especifica la nueva contraseña del usuario no raíz.

--rootuser=rootaccount

Especifica el nombre de usuario del usuario raíz.

--rootpwd=newrootpassword

Especifica la nueva contraseña del usuario raíz.

--pwdfile=pwdfilepath

(Opcional) Especifica la contraseña del usuario raíz y del usuario no raíz. Este parámetro es opcional y se utiliza si se han almacenado las contraseñas del usuario raíz y los usuarios no raíz en un archivo independiente. El archivo de contraseña incluye los parámetros siguientes:--password=newpassword and --rootpwd=newrootpassword.

```
# ./d2dnode --delete=nodename1,nodename2,nodename3
```

Suprime los nodos especificados del servidor de copia de seguridad. Para suprimir varios nodos, utilice la coma (,) como delimitador.

```
# ./d2dnode --import=network --help
```

Importa nodos desde la red. Cuando se importan nodos, se obtienen las opciones siguientes para configurarlas:

--netlist

Especifica la lista de direcciones IP de IP v4. Para varias entradas, la lista debe estar compuesta por entradas separadas con comas.

Ejemplo

192.168.1.100: Importa el nodo que tiene la dirección IP 192.168.1.100.

192.168.1.100-150: Importa todos los nodos que pertenecen al intervalo entre 192.168.1.100 y 192.168.100.150.

192.168.1.100-: Importa todos los nodos que pertenecen al intervalo entre 192.168.1.100 y 192.168.1.254. No se debe mencionar el intervalo final.

192.168.1.100-150,192.168.100.200-250: Importa varios nodos que pertenecen a dos intervalos diferentes. El primer intervalo entre 192.168.1.100 y 192.168.1.150, y el segundo intervalo entre 192.168.100.200 y 192.168.100.250. Un coma separa cada entrada.

--joblist

Especifica la lista de nombres de tareas. Un nombre de tarea no debe incluir un coma. Después de importar correctamente un nodo, el nodo se agrega a la tarea. Para varias tareas, la lista debe estar compuesta por entradas separadas por comas.

Ejemplo: -- joblist=jobA,jobB,jobC

En este ejemplo, una coma separa cada entrada de tarea.

Nota: Solo la versión independiente del Agente de Arcserve UDP (Linux) es compatible con esta opción.

--user

Especifica el nombre de usuario que se debe importar y agregar los nodos.

--password

Especifica la contraseña para importar y agregar nodos.

--rootuser

Especifica el nombre de usuario del usuario raíz. Si se agrega un usuario que no es el usuario raíz, utilice este parámetro para especificar las credenciales del usuario raíz.

--rootpwd

Especifica la contraseña del usuario raíz. Si se agrega un usuario que no es el usuario raíz, utilice este parámetro para especificar las credenciales del usuario raíz.

--pwdfile

(Opcional) Especifica la contraseña del usuario raíz y del usuario no raíz. Este parámetro es opcional y se utiliza si se han almacenado las contraseñas del usuario raíz y los usuarios no raíz en un archivo independiente. El archivo de contraseña incluye los parámetros siguientes:--password=newpassword and --rootpwd=newrootpassword.

--prefix

Especifica el prefijo proporcionado a un nombre de host. Utilice este parámetro para filtrar nodos que incluyen el prefijo en el nombre de host.

--blacklistfile

Especifica un archivo que incluye una lista de nombres de host de nodos que no se desean agregar al servidor de copia de seguridad. Se debe proporcionar un nodo por línea en el archivo.

--force

Agrega el nodo de forma forzosa incluso si otro servidor de copia de seguridad lo gestiona. Si se elimina el parámetro *force*, entonces no se agregará el nodo a este servidor si lo gestiona otro servidor de copia de seguridad.

--verbose

Muestra más información acerca del proceso de importación de nodos. Utilice este parámetro con el fin de generar scripts de depuración o automatización.

--help

Muestra la pantalla de ayuda.

Notas:

- La función de importación utiliza el servidor SSH para detectar si un nodo es un nodo de Linux. Si el servidor SSH utiliza un puerto que no es el predeterminado, configure el servidor para usar el puerto no predeterminado. Para obtener más información sobre cómo configurar el número de puerto SSH, consulte Cambio del número de puerto SSH del servidor de copia de seguridad.
- Cuando no se proporciona la contraseña, se utiliza el método de autenticación de clave SSH.

4. Ejecute los comandos siguientes para gestionar las tareas:

```
# ./d2djob
```

Aparece una lista de comandos para facilitar la gestión de tareas. Mediante este comando, se podrán ejecutar, cancelar y suprimir tareas.

```
# ./d2djob -—delete=jobname
```

Suprime la tarea especificada de la ficha Estado de la tarea.

```
# ./d2djob -—run=jobname -—jobtype=1 -—wait
```

Ejecuta la tarea especificada. El parámetro --jobtype es opcional. El comando d2djob identifica automáticamente el tipo de trabajo del nombre de tarea que se especifica. Si el comando identifica una tarea de restauración, esta se inicia. Si el comando identifica una tarea de copia de seguridad y no se proporciona ningún valor para el parámetro --jobtype, se iniciará una tarea de copia de seguridad incremental. La copia de seguridad incremental es el tipo de tarea predeterminada.

Si se desea especificar el tipo de tarea para una tarea de copia de seguridad, los valores son 0, 1 y 2, donde 0 indica una tarea de copia de seguridad completa; 1 indica una tarea de copia de seguridad incremental y 2 indica una tarea de copia de seguridad de verificación.

```
# ./d2djob -—cancel=jobname -—wait
```

Cancela una tarea que está en curso.

Si se incluye --wait en el comando, el estado de la tarea aparecerá después de que la tarea se cancele. Si no se incluye --wait en el comando, el mensaje de estado se muestra inmediatamente después de enviar la solicitud de cancelación.

```
# ./d2djob --newrestore=restoreJobName --target=macaddress/ipaddress
--hostname=hostname --network=dhcp/staticip --staticip=ipaddress
--subnet=subnetMask --gateway=gateway --runnow --wait
```

Ejecuta una tarea de restauración para un nuevo equipo de destino basado en una tarea de restauración existente. Este comando permite utilizar la misma configuración de restauración que la tarea de restauración existente; solamente los detalles del equipo de destino son diferentes. Si se utiliza este comando, no se tienen que crear varias tareas de restauración para equipos de destino diferentes.

Se debe proporcionar un valor para *--newrestore*, *--target*, *--hostname* y *--network*.

Si el valor para *--network* es staticip, a continuación se debe proporcionar un valor para *--staticip*, *--subnet* y *--gateway*. Si el valor para *--network* es dhcp, a continuación no se tiene que proporcionar ningún valor para *--staticip, --subnet* y *--gateway*.

Si se incluye --runnow en el comando, la tarea se ejecutará inmediatamente después de que se envíe la tarea, sin tener en cuenta la programación de tareas.

Si se incluye el parámetro --wait en el comando, el mensaje de estado aparecerá después de que la tarea finalice. Si no se incluye --wait en el comando, el mensaje de estado se muestra inmediatamente después de enviar la tarea.

```
# ./d2djob <--export=nombretarea1,nombretarea2,nombretarea3>
<--file=rutaarchivo>
```

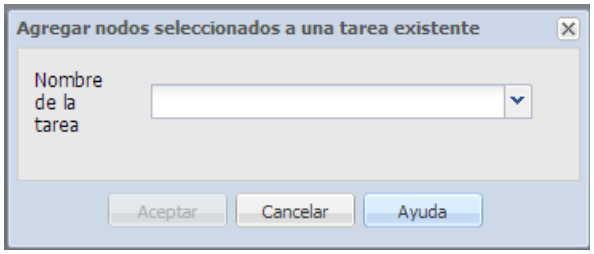
Exporta varias tareas del servidor de copia de seguridad a un archivo. Si desea tener configuraciones de copia de seguridad parecidas en varios servidores de copia de seguridad, se pueden exportar las tareas de copia de seguridad a un archivo y, a continuación, importar el archivo a otros servidores de copia de seguridad.

Nota: Si el servidor de copia de seguridad de Linux se gestiona mediante la consola de Arcserve UDP, la función de exportación no es compatible.

```
# ./d2djob <--import=rutaarchivo>
```

Importa el archivo que contiene la información de la tarea de copia de seguridad a un servidor de copia de seguridad. Se puede importar también el archivo a Arcserve UDP, si Arcserve UDP gestiona el servidor de copia de seguridad.

Si la tarea de copia de seguridad se importa a un servidor de copia de seguridad, se podrá seleccionar la tarea en el cuadro de diálogo siguiente:



Se puede utilizar también la siguiente utilidad de la línea de comandos para agregar nodos a esta tarea:

```
./d2dnode –attach=jobname
```

5. Ejecute los siguientes comandos para crear o actualizar el archivo de configuración de los puntos de recuperación. El Agente de Arcserve UDP (Linux) utiliza el archivo de configuración para gestionar y mostrar los puntos de recuperación de la IU.

```
# ./d2drp
```

Crea o actualiza los archivos de configuración de los puntos de recuperación en función de los detalles de los puntos de recuperación. Mediante este comando se pueden crear o actualizar los archivos de configuración.

```
# ./d2drp --build -–storagepath=/backupdestination –-node=node_name
```

Verifica todos los puntos de recuperación que pertenecen a *node_name* y actualizan todos los archivos de configuración de los puntos de recuperación. Si los archivos de configuración de los puntos de recuperación no están presentes, este comando creará los archivos automáticamente. El parámetro --build crea los archivos de configuración de los puntos de recuperación.

```
# ./d2drp --build –-storagepath=/backupdestination –-node=node_name
–-rp=recovery_point
```

Verifica el nombre de la sesión especificado y actualiza todos los archivos de configuración de los puntos de recuperación. Si los archivos de configuración de los puntos de recuperación no están presentes, este comando creará los archivos automáticamente. Especifique la palabra clave "last" para que el parámetro --rp obtenga el punto de recuperación más reciente.

```
# ./d2drp  --show --storagepath=path --node=nodeName --rp=recovery_point
--user=username --password=password
```

Muestra información del sistema para el punto de recuperación especificado.

--rp=recovery_point

Seleccione el punto de recuperación al cual se desee acceder. Especifique la palabra clave "last" para obtener el punto de recuperación más reciente.

--user=username

Especifica el nombre del usuario para acceder a la ubicación de almacenamiento o al destino de la copia de seguridad.

--password=password

Especifica la contraseña para acceder a la ubicación de almacenamiento o al destino de la copia de seguridad.

Nota: d2drp no admite el recurso compartido de NFS o de CIFS para el parámetro --build. Si desea utilizar el recurso compartido de NFS o de CIFS, deberá montar primero el recurso compartido al host local y, a continuación, utilice el punto de montaje como ruta de almacenamiento.

6. Ejecute el comando siguiente para registrar el servidor de copia de seguridad en Arcserve UDP. Cuando se registra el servidor de copia de seguridad con Arcserve UDP, se puede gestionar el servidor de copia de seguridad desde Arcserve UDP. También se pueden importar a Arcserve UDP nodos y tareas que se gestionaban previamente mediante el servidor de copia de seguridad.

   ```
   # ./d2dreg <--reg=nombreservidor> <--user=nombreusuario> <--port=puerto>
   <--protocol=http/https> [--password=contraseña]
   ```

   Registra el servidor de copia de seguridad en Arcserve UDP para que el servidor de copia de seguridad se pueda gestionar desde la consola de Arcserve UDP.

   Nota: El comando d2dreg utiliza el nombre de host del servidor de copia de seguridad para identificar el servidor. Si la consola de Arcserve UDP no se puede conectar al servidor de copia de seguridad mediante el nombre de host, cambie el nombre de host en la Dirección IP en el cuadro de diálogo **Actualizar nodo**.

7. Ejecute los comandos siguientes para gestionar los registros de actividades:

   ```
   # ./d2dlog
   ```

   Aparece el formato que ayuda a obtener los registros de actividades para el ID de la tarea especificada en el formato determinado.

   ```
   # ./d2dlog -—show=jobid -—format=text/html
   ```

   Se muestra el registro de actividades de la tarea especificada. El valor de formato es opcional porque el valor predeterminado es texto.

8. Ejecute los comandos siguientes para gestionar el historial de tareas:

   ```
   # ./d2djobhistory
   ```

   Muestra el historial de tareas en función de los filtros que se especifican. Se puede filtrar el historial de tareas por días, semanas, meses y fecha de inicio y finalización.

```
# ./d2djobhistory --day=n --headers=column_name1,column_name2,...column_name_n
--width=width_value --format=column/csv/html
```

Muestra el historial de tareas reciente en función de los días especificados.

--headers=column_name1,column_name2,...column_name_n

(Opcional) Especifica las columnas que se desean ver en el historial de tareas. Este parámetro es opcional. Las columnas predeterminadas son ServerName, TargetName, JobName, JobID, JobType, DestinationLocation, EncryptionAlgoName, CompressLevel, ExecuteTime, FinishTime, Throughput, WriteThroughput, WriteData, ProcessedData y Status.

--width=width_value

(Opcional) Especifica el número de caracteres que se desean mostrar para cada columna. Este parámetro es opcional. Cada columna tiene su propia anchura predeterminada. Se puede actualizar el valor de anchura para cada columna, donde cada valor de anchura se separa con una coma (,).

--format=column/csv/html

Especifica el formato de apariencia del historial de tareas. Los formatos disponibles son columna, csv y html. Se puede especificar solamente un formato a la vez.

```
# ./d2djobhistory --week=n
--headers=column_name1,column_name2,...column_name_n --width=width_value
--format=column/csv/html
```

Muestra el historial de tareas reciente en función de las semanas especificadas.

```
# ./d2djobhistory --month=n
--headers=column_name1,column_name2,...column_name_n --width=width_value
--format=column/csv/html
```

Muestra el historial de tareas reciente en función de los meses especificados.

```
# ./d2djobhistory --starttime=yyyymmdd --endtime=yyyymmdd
--headers=column_name1,column_name2,...column_name_n --width=width_value
--format=column/csv/html
```

Muestra el historial de tareas reciente en función de la fecha de inicio y de finalización especificada.

Las utilidades de generación de scripts se han utilizado para gestionar correctamente nodos, tareas y registros de actividades.

Gestión de scripts anteriores/posteriores para la automatización

Los scripts previos/posteriores permiten ejecutar su propia lógica empresarial en las etapas específicas de una tarea en ejecución. Se puede especificar cuando se ejecutan los scripts en **Configuración previa/posterior** de los scripts del **Asistente de copia de seguridad** y el **Asistente de restauración** en la consola. Los scripts se pueden ejecutar en el servidor de copia de seguridad en función de la configuración.

La gestión de scripts anteriores/posteriores constituye un proceso de dos partes que consta de la creación del script anterior/posterior y la colocación de dicho script en la carpeta prepost.

Creación de scripts anteriores/posteriores

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree un archivo de script mediante el uso de las variables de entorno en el lenguaje de generación de scripts preferido.

   Variables de entorno de scripts anteriores/posteriores

   Para crear un script, utilice las variables de entorno siguientes:

   D2D_JOBNAME

   Indica el nombre de la tarea.

   D2D_JOBID

   Identifica el ID de la tarea. El ID de la tarea es un número que se proporciona a la tarea cuando esta se ejecuta. Si se ejecuta la misma tarea de nuevo, obtendrá un nuevo número de tareas.

   D2D_TARGETNODE

   Identifica el nodo del cual se realiza copia de seguridad o que se restaura.

   D2D_JOBTYPE

   Identifica el tipo de tarea en ejecución. Los valores siguientes identifican la variable D2D_JOBTYPE:

   backup.full

   Identifica la tarea como copia de seguridad completa.

   backup.incremental

   Identifica la tarea como copia de seguridad incremental.

   backup.verify

   Identifica la tarea como copia de seguridad de verificación.

restore.bmr

Identifica la tarea como reconstrucción completa. Esta tarea es de restauración.

restore.file

Identifica la tarea como una restauración de nivel de archivo. Esta tarea es de restauración.

D2D_SESSIONLOCATION

Identifica la ubicación donde se almacenan los puntos de recuperación.

D2D_PREPOST_OUTPUT

Identifica un archivo temporal. El contenido de la primera línea del archivo temporal aparecerá en el registro de actividades.

D2D_JOBSTAGE

Indica la etapa de la tarea. Los valores siguientes identifican la variable D2D_JOBSTAGE:

pre-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad antes de que se inicie la tarea.

post-job-server

Identifica el script que se ejecuta en el servidor de copia de seguridad después de que se complete la tarea.

pre-job-target

Identifica el script que se ejecuta en el equipo de destino antes de que se inicie la tarea.

post-job-target

Identifica el script que se ejecuta en el equipo de destino después de que se complete la tarea.

pre-snapshot

Identifica el script que se ejecuta en el equipo de destino antes de capturar la instantánea.

post-snapshot

Identifica el script que se ejecuta en el equipo de destino después de capturar la instantánea.

D2D_TARGETVOLUME

Identifica el volumen del cual se realiza copia de seguridad durante una tarea de copia de seguridad. Esta variable es aplicable para los scripts de instantáneas previas y posteriores para una tarea de copia de seguridad.

D2D_JOBRESULT

Identifica el resultado para un script de tarea de publicación. Los valores siguientes identifican la variable D2D_JOBRESULT:

success

Identifica el resultado como correcto.

fail

Identifica el resultado como incorrecto.

D2DSVR_HOME

Identifica la carpeta donde se instala el servidor de copia de seguridad. Esta variable es aplicable para los scripts que se ejecutan en el servidor de copia de seguridad.

El script se crea.

Nota: En todos los scripts, un valor de retorno de cero indica que se ha realizado correctamente, mientras que un valor de retorno distinto a cero indica que se han producido errores.

Colocación del script en la carpeta prepost y verificación

Todos los scripts previos/posteriores para un servidor de copia de seguridad se gestionan centralmente desde la carpeta prepost en la ubicación siguiente:

```
/opt/CA/d2dserver/usr/prepost
```

Siga estos pasos:

1. Coloque el archivo en la siguiente ubicación del servidor de copia de seguridad:

   ```
   /opt/CA/d2dserver/usr/prepost
   ```

2. Proporcione los permisos de ejecución al archivo de script.
3. Inicie sesión en la interfaz web del Agente de Arcserve UDP (Linux).
4. Abra el **Asistente de copia de seguridad** o el **Asistente de restauración** y vaya a la ficha **Configuración avanzada**.
5. Seleccione el archivo de script en la lista desplegable **Configuración de scripts anteriores/posteriores** y, a continuación, envíe la tarea.
6. Haga clic en **Registro de actividad** y verifique que el script se ejecute en la tarea de copia de seguridad especificada.

   El script se ejecuta.

Los scripts anteriores/posteriores se crean correctamente y se colocan en la carpeta prepost.

Creación del script de alerta del almacenamiento de la copia de seguridad

Cree el script de alerta del almacenamiento de la copia de seguridad para que se pueda ejecutar cuando el espacio de almacenamiento de la copia de seguridad sea menor que el valor especificado. Cuando se agrega una ubicación de almacenamiento de la copia de seguridad a la IU, se tendrá la opción de activar la casilla de verificación Ejecutar script cuando el espacio libre sea menor de. Cuando se activa la casilla de verificación, el Agente de Arcserve UDP (Linux) controla el espacio de almacenamiento disponible cada 15 minutos. Cada vez que el espacio de almacenamiento es menor que el valor especificado, el Agente de Arcserve UDP (Linux) ejecuta el script *backup_storage_alert.sh.* Se puede configurar el script *backup_storage_alert.sh* para realizar cualquier tarea cuando el espacio de almacenamiento de la copia de seguridad es menor.

Ejemplo 1: se puede configurar el script para enviar automáticamente una alerta de correo electrónico con objeto de advertir de la disminución del espacio de almacenamiento.

Ejemplo 2: se puede configurar el script para suprimir automáticamente algunos datos del espacio de almacenamiento de la copia de seguridad cuando dicho espacio es menor que el valor especificado.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree el script *backup_storage_alert.sh* usando las siguientes variables:

   backupstoragename

   Define el nombre de la ubicación de almacenamiento de la copia de seguridad. Por ejemplo, NFS o CIFS.

   freesize

   Define el espacio libre disponible en la ubicación de almacenamiento de la copia de seguridad.
3. Coloque el script en la siguiente ubicación:

   `/opt/CA/d2dserver/usr/alert/backup_storage_alert.sh`

Se creará el script backup_storage_alert.sh.

Detección de los nodos mediante un script

El Agente de Arcserve UDP (Linux) proporciona la capacidad para ejecutar un script que detecta los nodos de la red. Se puede crear un script para detectar nodos en la red y colocarlo en la carpeta de *detección* en la siguiente ubicación.

Se puede configurar la detección de nodos de la interfaz web y establecer la frecuencia de ejecución del script. En el script se pueden especificar las utilidades para detectar nodos de la red. Después de que el script detecte un nodo, utilice el comando *d2dnode* para agregar el nodo al Agente de Arcserve UDP (Linux). Se podrá acceder a un registro de actividad cada vez que se ejecuta el script.

Nota: En todos los scripts, un valor de retorno de cero indica que se ha realizado correctamente, mientras que un valor de retorno distinto a cero indica que se han producido errores.

Si desea imprimir algo en el Registro de actividad en cuanto al script de detección de nodos, se podrá utilizar la siguiente variable de entorno especial:

```
echo "print something into activity log" > "$D2D_DISCOVER_OUTPUT"
```

Un script de muestra se coloca en la carpeta de *detección* en la ubicación siguiente que puede detectar los nodos de Linux en una subred.

```
/opt/CA/d2dserver/examples/discovery
```

Se puede copiar el script de muestra en la ubicación siguiente y modificar el script por el requisito:

```
/opt/CA/d2dserver/usr/discovery
```

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree un script de detección de nodos y colóquelo en la carpeta de *detección* en la ubicación siguiente:

   ```
   /opt/CA/d2dserver/usr/discovery
   ```
3. Proporcione los permisos de ejecución necesarios al archivo de script.
4. Inicie sesión en la interfaz web.
5. Configure los valores de configuración de detección de nodos en el menú Nodo para ejecutar el script.
6. Haga clic en Registro de actividad y verifique que el script está ejecutándose.

   El registro de actividad muestra una lista de todos los nodos detectados.

Los nodos se detectan correctamente mediante el script.

Creación de scripts para realizar la copia de seguridad de la base de datos de Oracle

Se pueden crear scripts que se utilizan para realizar copia de seguridad de la base de datos de Oracle. No se tiene que detener la base de datos para realizar una copia de seguridad. Verifique que la base de datos esté en el modo de registro de archivado. Si no está en el modo de registro de archivado, cambie la base de datos al modo de registro de archivado antes de realizar la copia de seguridad de la base de datos. Cree los dos scripts siguientes para realizar copia de seguridad de la base de datos de Oracle:

- **pre-db-backup-mode.sh**: este script se prepara y mantiene toda la base de datos en el modo de copia de seguridad.
- **post-db-backup-mode.sh**: este script elimina la base de datos del modo de copia de seguridad.

Se puede especificar que los scripts se ejecuten en los nodos de la base de datos de Oracle en Configuración de scripts anteriores/posteriores del Asistente de copia de seguridad.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree el script *pre-db-backup-mode.sh* utilizando el siguiente código:

```
#!/bin/bash

orauser="oracle"

orasid="orcl"

su - ${orauser}   << BOF 2>&1

export ORACLE_SID=$orasid

sqlplus /nolog << EOF 2>&1

conéctese / como sysdba

alter database begin backup;

exit;

EOF

BOF
```

Nota: Especifique el valor para las variables *orauser* y *orasid* tal y como se definen en la base de datos de Oracle.

3. Cree el script *post-db-backup-mode.sh* utilizando el siguiente código:

```
#!/bin/bash

orauser="oracle"

orasid="orcl"

su - ${orauser}   << BOF 2>&1

export ORACLE_SID=$orasid

sqlplus /nolog << EOF 2>&1

conéctese / como sysdba

alter database end backup;

exit;

EOF

BOF
```

   Nota: Especifique el valor para las variables *orauser* y *orasid* tal y como se definen en la base de datos de Oracle.

4. Proporcione permisos de ejecución en ambos scripts.
5. Coloque los dos scripts en la siguiente ubicación:

   ```
   /opt/CA/d2dserver/usr/prepost/
   ```

6. Inicie sesión en la interfaz web del Agente de Arcserve UDP (Linux).
7. Abra el Asistente de copia de seguridad y vaya a la ficha Configuración avanzada.
8. En la opción Configuración de scripts anteriores/posteriores, seleccione el archivo de script *pre-db-backup-mode.sh* de la lista desplegable Antes de realizar la instantánea.
9. En la opción Configuración de scripts anteriores/posteriores, seleccione el archivo de script *post-db-backup-mode.sh* de la lista desplegable Después de realizar la instantánea.
10. Para enviar la tarea.

    Se envía la tarea de copia de seguridad.

Los scripts se crean para realizar copia de seguridad de la base de datos de Oracle.

Nota: El Agente de Arcserve UDP (Linux) admite la instantánea de nivel de volumen. Para garantizar la coherencia en los datos, todos los archivos de datos de la base de datos deben estar en un volumen.

Para restaurar la base de datos Oracle, consulte Cómo restaurar una base de datos de Oracle mediante Agente de Arcserve UDP (Linux) (en la página 212).

Creación de scripts para realizar la copia de seguridad de la base de datos de MySQL

Se pueden crear scripts que se utilizan para realizar copia de seguridad de la base de datos de MySQL. No se tiene que detener la base de datos para realizar una copia de seguridad. Cree los dos scripts siguientes para realizar copia de seguridad de la base de datos de MySQL:

- **pre-db-backup-mode.sh**: este script cierra todas las tablas abiertas y bloquea todas las tablas en todas las bases de datos con un bloqueo de lectura global.
- **post-db-backup-mode.sh**: este script libera todos los bloqueos.

Se puede especificar que los scripts se ejecuten en los nodos de la base de datos de MySQL en Configuración de scripts anteriores/posteriores del Asistente de copia de seguridad.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree el script *pre-db-backup-mode.sh* utilizando el siguiente código:

```
#!/bin/bash

dbuser=root

dbpwd=rootpwd

lock_mysqldb(){

  (

    echo "flush tables with read lock;"

    sleep 5

  ) | mysql -u$dbuser -p$dbpwd ${ARGUMENTS}

}

lock_mysqldb &

PID="/tmp/mysql-plock.$!"

touch ${PID}
```

Nota: Especifique el valor para las variables *dbuserr* y *bpwd* tal y como se definen en la base de datos de MySQL.

3. Cree el script *post-db-backup-mode.sh* utilizando el siguiente código:

```
#!/bin/bash
killcids(){
pid="$1"
cids=`ps -ef|grep ${pid}|awk '{if('$pid'==$3){print $2}}'`
for cid in ${cids}
do
  echo ${cid}
  kill -TERM ${cid}
done
echo -e "\n"
}
mysql_lock_pid=`ls /tmp/mysql-plock.* | awk -F . '{print $2}'`
[ "$mysql_lock_pid" != "" ] && killcids ${mysql_lock_pid}
rm -fr /tmp/mysql-plock.*
```

4. Proporcione permisos de ejecución en ambos scripts.
5. Coloque los dos scripts en la siguiente ubicación:

   ```
   /opt/CA/d2dserver/usr/prepost/
   ```

6. Inicie sesión en la interfaz web del Agente de Arcserve UDP (Linux).
7. Abra el Asistente de copia de seguridad y vaya a la ficha Configuración avanzada.
8. En la opción Configuración de scripts anteriores/posteriores, seleccione el archivo de script *pre-db-backup-mode.sh* de la lista desplegable Antes de realizar la instantánea.
9. En la opción Configuración de scripts anteriores/posteriores, seleccione el archivo de script *post-db-backup-mode.sh* de la lista desplegable Después de realizar la instantánea.
10. Para enviar la tarea.

    Se envía la tarea de copia de seguridad.

Los scripts se crean para realizar copia de seguridad de la base de datos de MySQL.

Nota: El Agente de Arcserve UDP (Linux) admite la instantánea de nivel de volumen. Para garantizar la coherencia en los datos, todos los archivos de datos de la base de datos deben estar en un volumen.

Personalización de la programación de tareas

El Agente de Arcserve UDP (Linux) proporciona la capacidad para definir su propia programación mediante un script para ejecutar una tarea. Si desea ejecutar una tarea periódicamente y no se puede programar mediante la IU web, se podrá crear un script para definir la programación. Por ejemplo, en el caso de desear ejecutar una copia de seguridad a las 22:00 el último sábado de todos los meses. No se puede definir la programación mediante la interfaz web, pero se puede crear un script para definir la programación.

Se puede enviar una tarea de copia de seguridad sin especificar la programación (mediante la opción Ninguna de la página Configuración avanzada). Utilice el programador Linux Cron para definir la programación personalizada y ejecutar el comando *d2djob* para ejecutar la tarea.

Nota: El procedimiento siguiente asume que se ha enviado una tarea de copia de seguridad sin especificar ninguna programación y, además, se desea ejecutar una copia de seguridad a las 22:00 el último sábado de cada mes.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree un archivo de script e introduzca el comando siguiente para ejecutar una copia de seguridad a las 22:00 el último sábado de cada mes:

   ```
   #!/bin/bash

   LAST_SAT=$(cal | awk '$7!=""{t=$7} END {print t}')

   TODAY=$(date +%d)

   if [ "$LAST_SAT" = "$TODAY" ]; then

               source /opt/CA/d2dserver/bin/setenv

              d2djob --run=your_job_name   --jobtype=your_job_type      #run your
       backup job here

   fi
   ```

   Nota: Se deben proporcionar al archivo los permisos de ejecución necesarios.
3. Vaya a la carpeta crontab y agregue el comando siguiente al crontab del sistema (/etc/crontab):

   ```
   00 22 * * Saturday root runjob.sh
   ```

   Cron ejecuta el script de runjob.sh a las 22:00 todos los sábados. En runjob.sh, primero comprueba si hoy es el último sábado del mes. En caso afirmativo, se utiliza d2djob para ejecutar la tarea de copia de seguridad.

La programación de la tarea se personaliza para ejecutar una copia de seguridad a las 22:00 el último sábado de todos los meses.

Ejecución de una tarea por lotes de reconstrucción completa

Si se desea realizar una reconstrucción completa en varios equipos, así como instalar el mismo entorno operativo en todos los equipos, se puede realizar una reconstrucción completa por lotes. No se tiene que crear una tarea para cada tarea de reconstrucción completa. Se puede ahorrar tiempo y el esfuerzo; además, se puede reducir el riesgo de que se produzca cualquier error al configurar los equipos de reconstrucción completa.

Nota: Se debe contar con un punto de recuperación válido del equipo de origen que desea restaurar. Si no se cuenta con un punto de recuperación válido, se debe realizar primero la copia de seguridad del equipo de origen y, a continuación, enviar una tarea de restauración.

Primero defina toda la configuración de reconstrucción completa en una tarea de reconstrucción completa de plantilla y, a continuación, cambie la dirección del equipo de destino (IP o MAC), el nombre del host y la configuración de red mediante el siguiente comando:

```
d2djob
```

Siga estos pasos:

1. Cree una tarea de reconstrucción completa denominada PLANTILLA-BMR y ejecute la tarea para un equipo de los diversos equipos.

   Nota: Se puede asignar cualquier nombre a la tarea de reconstrucción completa. Se debe proporcionar el mismo nombre de la tarea en el script de reconstrucción completa por lotes.

2. Inicie sesión en el servidor de copia de seguridad como usuario raíz.

3. Cree un script de reconstrucción completa por lotes basado en la tarea PLANTILLA-BMR con el fin de enviar automáticamente varias tareas de reconstrucción completa. Utilice el siguiente script para crear un script de reconstrucción completa por lotes:

   ```
   #!/bin/sh
   prename=lab-server
   serverList[0]="<MAC_Address>"
   serverList[1]=" <MAC_Address>"
   serverList[2]=" <MAC_Address>"
   .
   .
   .
   serverList[300]=" <MAC_Address>"
   for((i=0;i<${#serverList[@]};i=i+1))
   do
   ./d2djob --newrestore="BMR-TEMPLATE" --target=${serverList[i]}
   --hostname=$prename$i --network=dhcp
   done
   ```

4. Ejecute el script de reconstrucción completa por lotes.

   Se ejecuta el script. Se crean varias tareas de reconstrucción completa en la IU.

Se ejecuta una tarea de reconstrucción completa por lotes.

Replicación y gestión de sesiones de copia de seguridad

Se puede crear un script para replicar sesiones de copia de seguridad con objeto de que se puedan recuperar datos cuando los datos de copia de seguridad originales estén dañados. Las sesiones de copia de seguridad incluyen todos los puntos de recuperación de los que se realizaron copia de seguridad. Se pueden proteger las sesiones de copia de seguridad replicando sesiones de copia de seguridad en un destino de replicación.

Una vez que se hayan replicado las sesiones de copia de seguridad, se podrá gestionar a continuación el destino de replicación agregando el destino a la interfaz del Agente de Arcserve UDP (Linux).

El proceso de replicar y gestionar sesiones de copia de seguridad consta de tres fases. Incluye las siguientes tres fases:

- Replicación de sesiones de copia de seguridad en el destino de replicación
- Creación o actualización de los archivos de configuración de los puntos de recuperación para poder gestionarlos y mostrarse en la interfaz web del Agente de Arcserve UDP (Linux)
- Adición del destino de replicación a la interfaz web del Agente de Arcserve UDP (Linux)

Replicación de las sesiones de copia de seguridad

Se puede aprovechar la función Configuración de scripts anteriores/posteriores en el Asistente de copia de seguridad para replicar las sesiones de copia de seguridad al destino de replicación. Se puede seleccionar cualquier opción —como el protocolo de transferencia de archivos (FTP), de copia segura (SCP) o el comando cp— para replicar la sesión de copia de seguridad.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree un script anterior/posterior para replicar las sesiones de copia de seguridad.
3. Coloque el script en la siguiente ubicación:

   `/opt/CA/d2dserver/usr/prepost`
4. Inicie sesión en la interfaz web del Agente de Arcserve UDP (Linux).
5. Abra al Asistente de copia de seguridad y vaya a la página Avanzado.
6. En la opción Configuración de scripts anteriores/posteriores de Ejecución en el servidor de copia de seguridad, seleccione el script de replicación en la lista desplegable Después de finalizar la tarea.
7. Para enviar la tarea.

La sesión de copia de seguridad se replica en el destino de la copia de seguridad.

Creación o actualización de los archivos de configuración de los puntos de recuperación

Después de replicar las sesiones de copia de seguridad, cree y configure el archivo de configuración de los puntos de recuperación. Este archivo se utiliza para identificar los puntos de recuperación al realizar la operación de restauración desde la interfaz del Agente de Arcserve UDP (Linux).

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Vaya a la ubicación siguiente:

   ```
   /opt/CA/d2dserver/bin
   ```

3. Introduzca el siguiente comando para crear o actualizar el archivo de configuración de los puntos de recuperación:

   ```
   ./d2drp --storagepath=/backupdestination --node=node_name
   --session=session_name
   ```

   Si proporciona solamente la información de *--storagepath* y *--node,* a continuación el comando actualizará todas las sesiones de copia de seguridad para el nodo seleccionado. Si proporciona la información de *--session,* a continuación el comando actualizará la información de la sesión específica.

   Nota: Para obtener más información acerca del comando d2drp, consulte *Funcionamiento de las utilidades de generación de scripts*.

El archivo de configuración de los puntos de recuperación se crea o actualiza en función del estado del archivo.

Adición del destino de replicación

Agregue el destino de replicación a la interfaz del Agente de Arcserve UDP (Linux) para gestionar el destino. Después de agregar el destino de replicación, se puede ver el espacio libre disponible en ese destino y gestionar los datos de la manera correspondiente.

Siga estos pasos:

1. Inicie sesión en el destino de replicación.
2. Cree un archivo denominado Configuración e introduzca el siguiente código siguiente en el archivo de configuración:

   ```
   RecoverySetLimit=n
   ```

   n indica el número de conjuntos de recuperación que se desea retener en el destino de replicación.

3. Coloque el archivo en la carpeta de nodo del destino de replicación.

   Por ejemplo, /backup_destination/node_name/Settings

4. Inicie sesión en la interfaz web del Agente de Arcserve UDP (Linux).
5. Agregue el destino de replicación en el menú Almacenamiento de la copia de seguridad.

El destino de replicación se agrega a la interfaz web del Agente de Arcserve UDP (Linux).

Las sesiones de copia de seguridad se replican y gestionan correctamente.

Verificación de que los puntos de recuperación son utilizables

La utilidad d2dverify ayuda a verificar que los puntos de recuperación son utilizables desde varias sesiones de copia de seguridad. Normalmente, las tareas de copia de seguridad se ejecutan cada día y cuando se dispone de varios puntos de recuperación es posible que no esté seguro de si los puntos de recuperación son utilizables para la recuperación de datos durante un error del sistema. Para evitar estas situaciones, se pueden realizar tareas de BMR para verificar periódicamente si las copias de seguridad son utilizables. La utilidad d2dverify ayuda a automatizar la tarea de verificación de usabilidad de los puntos de recuperación.

Después de configurar los parámetros obligatorios, la utilidad d2dverify envía la tarea de BMR y recupera los datos en la máquina virtual especificada. A continuación, d2dverify inicia la máquina virtual y ejecuta un script para verificar si las aplicaciones en la máquina virtual funcionan correctamente. Se puede crear también una programación para ejecutar la utilidad d2dverify periódicamente mediante utilidades del sistema como Linux Cron. Por ejemplo, se puede ejecutar la utilidad d2dverify después de la última copia de seguridad de un conjunto de recuperación. En tal caso, d2dverify verifica todos los puntos de recuperación en el conjunto de recuperación.

Nota: Para obtener más información sobre la programación de una tarea mediante el programador Linux Cron, consulte Personalización de la programación de tareas.

La utilidad d2dverify se puede utilizar también en los escenarios siguientes:

- Se puede utilizar la utilidad d2dverify para migrar las copias de seguridad de varios equipos físicos a máquinas virtuales.
- Después de recuperar un hipervisor, se puede utilizar la utilidad d2dverify para restaurar todas las máquinas virtuales en el nuevo hipervisor.

Tenga en cuenta los siguientes requisitos previos antes de utilizar la utilidad d2dverify:

- Identifique los nodos de origen cuya copia de seguridad se desea verificar.
- Identifique un hipervisor en el cual se crearán máquinas virtuales.
- Cree máquinas virtuales para cada nodo que se desee verificar. Asigne el nombre de la máquina virtual en el formato siguiente:

  `verify_<nombre del nodo>`

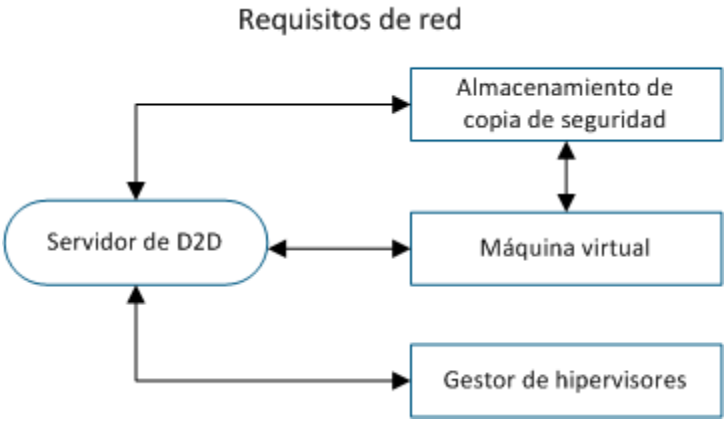
  Nota: No es necesario adjuntar los discos duros virtuales para estas máquinas virtuales. Es posible que no se adjunte una red virtual a estas máquinas virtuales si se especifican los parámetros de "vm_network".
- Revise los requisitos de red.
- Identifique una red en la cual las máquinas virtuales estén conectadas.

  Nota: La utilidad d2dverify solo admite la red de IP estática.

Importante: Si la base de datos dispone de información sobre la cuenta del nodo relacionada con un usuario no raíz, d2dverify restablecerá la contraseña del usuario no raíz a CAd2d@2013 para la máquina virtual de destino.

Requisitos de red:

Cuando se utiliza d2dverify, se recomienda guardar las máquinas virtuales de destino en una red virtual aislada para evitar cualquier conflicto con el entorno de producción. En tales casos, las máquinas virtuales de destino se deberán conectar al servidor de copia de seguridad y al almacenamiento de copia de seguridad.



Compatibilidad con el hipervisor:

d2dverify depende de la utilidad d2drestorevm para realizar la restauración. d2dverify admite las versiones siguientes de hipervisores:

- XenServer 6.0 y anteriores
- RHEV 3.0 y anteriores
- OVM 3.2

Argumentos:

--template

Identifica la plantilla que incluye los parámetros para ejecutar la utilidad d2dverify.

--createtemplate

Crea una plantilla vacía que incluye los parámetros para ejecutar la utilidad d2dverify.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Cree la plantilla que use la utilidad d2dverify mediante el comando siguiente:

   ```
   d2dverify --createtemplate=file_path
   ```

3. Abra la plantilla y actualice los parámetros siguientes:

   node_list

   Especifica una lista de nodos o unos criterios de consulta que buscan la información en la base de datos del servidor de copia de seguridad. Cada nodo está separado por una coma, como Node1,Node2,Node3.

   Notes: Si el número de puerto de ssh no es el puerto predeterminado 22, el formato para especificar cada nodo será: Node1:new_port,Node2:new_port,Node3:new_port. El nombre de la máquina virtual se asigna como verify_<nombre del nodo>, donde el nombre de nodo no incluirá el número de puerto.

   Ejemplo: Node1:222,Node2:333,Node4:333

   La lista siguiente es un ejemplo de los criterios de consulta:

   [node=prefix]

   Busca el nombre del nodo que contiene el prefijo definido.

   [desc=prefix]

   Busca la descripción del nodo que contiene el prefijo definido.

   guest_ip_list =

   Especifica la lista de direcciones IP que se aplica a cada nodo de destino respectivamente. Cada dirección IP se separa por una coma, como IP1,IP2,IP3. Si solamente hay una dirección IP disponible pero existen varios nodos en el parámetro node_list, el cuarto segmento de la dirección IP aumentará en uno para cada nodo. La utilidad d2dverify comprueba si se ha utilizado una dirección IP. En caso afirmativo, la dirección IP se omite.

   Por ejemplo, si se tienen tres nodos, Nodo 1, Nodo 2 y Nodo 3 y una dirección IP, xxx.xxx.xxx.xx6, la dirección IP se aplicará tal y como se muestra en la lista siguiente:

   Nodo 1: xxx.xxx.xxx.xx6

   Nodo 2: xxx.xxx.xxx.xx7

   Nodo 3: xxx.xxx.xxx.xx8

vm_type

Especifica el tipo de hipervisor. Los tres tipos siguientes de hipervisores son válidos: xen, ovm o rhev.

vm_server

Especifica el nombre de host o la dirección IP del gestor de hipervisores.

vm_svr_username

Especifica el nombre de usuario del gestor de hipervisores.

vm_svr_password

Especifica la contraseña del gestor de hipervisores. La contraseña se deberá cifrar mediante la utilidad d2dutil --encrypt.

El comando siguiente se utiliza para cifrar la contraseña:

```
echo "password" | d2dutil --encrypt
```

vm_network

Especifica la red virtual que utiliza la máquina virtual de destino. Se recomienda especificar este parámetro cuando la máquina virtual de destino se conecta a varias redes virtuales.

guest_gateway

Especifica la puerta de enlace de la red que utiliza el sistema operativo (SO) invitado de la máquina virtual de destino.

guest_netmask

Especifica la máscara de red que utiliza el SO invitado de la máquina virtual de destino.

guest_username

Especifica el nombre del usuario que se utiliza para conectarse a la máquina virtual recuperada. La contraseña se restablece a la contraseña especificada en el parámetro guest_password. El parámetro guest_username se ignora cuando se utiliza la utilidad d2dverify para consultar información de la base de datos del servidor de copia de seguridad. En tales casos, la contraseña de invitado de la máquina virtual se restablece a la contraseña del nodo almacenada en la base de datos.

guest_password

Especifica la contraseña para el parámetro guest_username. La contraseña se deberá cifrar mediante la utilidad d2dutil --encrypt. El parámetro guest_password se ignora cuando se utiliza la utilidad d2dverify para consultar información de la base de datos del servidor de copia de seguridad.

storage_location

Especifica la ruta de red de la ubicación de almacenamiento de copia de seguridad. No es necesario especificar la ubicación de almacenamiento si los nodos en el parámetro node_list están en la base de datos del servidor de copia de seguridad. Si la ubicación de almacenamiento es un recurso compartido de CIFS, utilice el formato siguiente para especificar la ubicación:

```
//hostname/path
```

storage_username

Especifica el nombre de usuario para acceder a la ubicación de almacenamiento de copia de seguridad. Este parámetro no es necesario para un recurso compartido de NFS.

Para un usuario de dominio de Windows, utilice el formato siguiente para especificar la ubicación:

```
domain_name/username
```

storage_password

Especifica la contraseña para acceder a la ubicación de almacenamiento de copia de seguridad. La contraseña se deberá cifrar mediante la utilidad d2dutil --encrypt. Este parámetro no es necesario para un recurso compartido de NFS.

recovery_point = last

Especifica la sesión que se desea restaurar. Normalmente, una sesión de recuperación tiene el formato siguiente: S00000000X, dónde X es un valor numérico. S00000000X es el nombre de la carpeta de los puntos de recuperación. Si se desea restaurar la sesión más reciente, especifique la palabra clave 'last'.

encryption_password

Especifica la contraseña de cifrado para el punto de recuperación. La contraseña se deberá cifrar mediante la utilidad d2dutil --encrypt.

script

Especifica el script que se desea ejecutar. El script se ejecuta en el equipo de destino después de una recuperación correcta. Si este parámetro no se proporciona, la utilidad d2dverify ejecutará el comando ls /proc en el equipo de destino.

email_to_address

Especifica la dirección de correo electrónico de los destinatarios que recibirán informes en un correo electrónico. Se puede especificar más de una dirección de correo electrónico, utilizando siempre la coma para separarlas.

email_subject

Especifica la línea de asunto del correo electrónico.

report_format

Especifica el formato del informe para recibir un correo electrónico. El formato podría ser texto (.txt) o html.

Valor predeterminado: html

node_not_in_db

Especifica los nodos de los parámetros node_list que no están en la base de datos del servidor de copia de seguridad. Se deben especificar los parámetros relacionados con storage_*.

Valor: yes

stop_vm_after_recovery

Especifica que el destino máquina virtual se debe detener después de una correcta recuperación y verificación. Los valores para este parámetro son yes y no.

Valor predeterminado: yes

4. Guarde y cierre la plantilla.
5. Ejecute la utilidad d2dverify mediante el comando siguiente:

```
d2dverify --template=file_path
```

Nota: Se produce un error en la utilidad d2dverify si se agregan los nodos en el parámetro node_list mediante la clave pública/privada. Para resolver esta incidencia, configure la variable de entorno export D2D_SSH_IGNORE_PWD=yes en el entorno de shell donde se ejecuta la utilidad d2dverify.

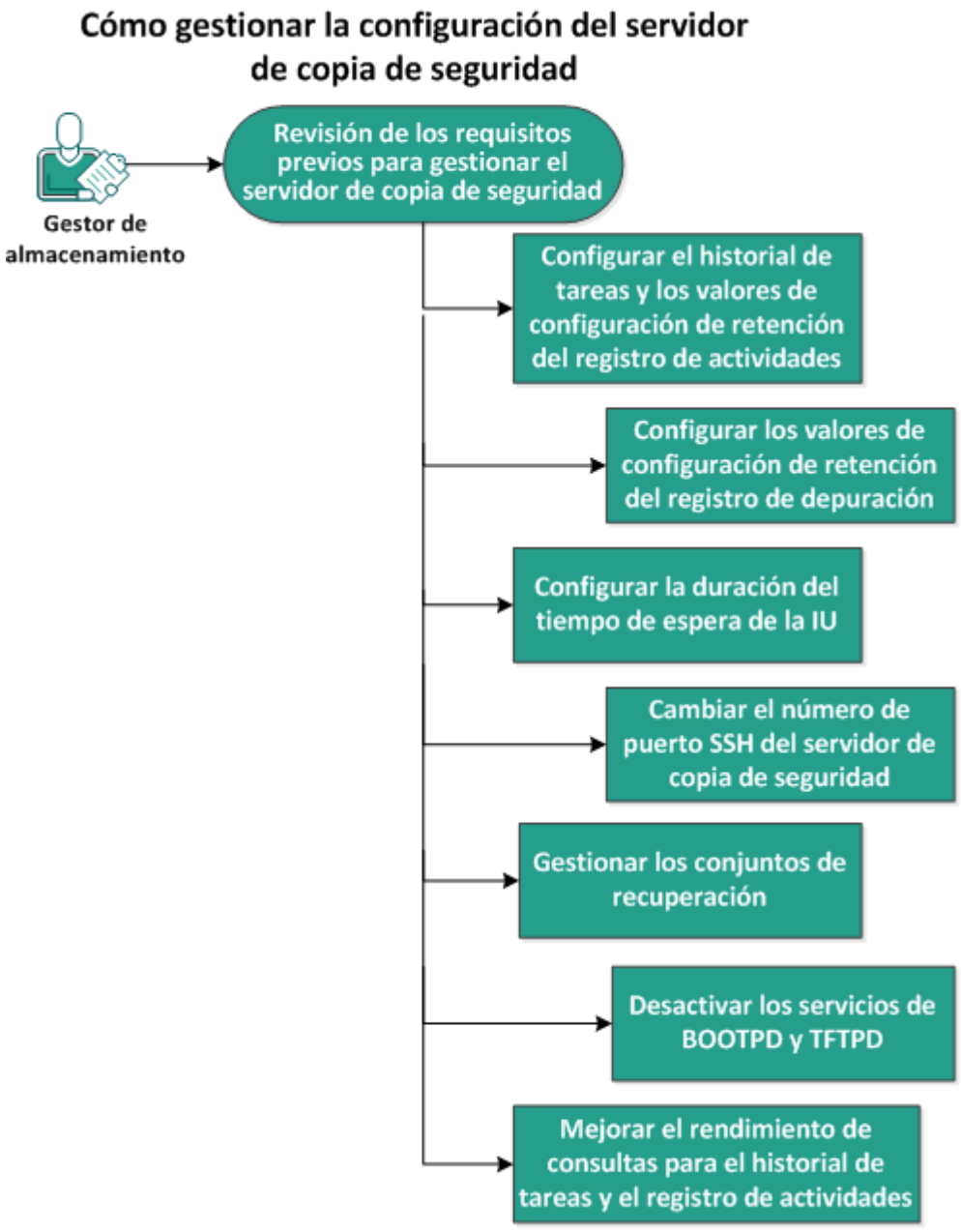
La usabilidad de los puntos de recuperación se ha verificado correctamente.

Cómo gestionar la configuración del servidor de copia de seguridad

Realice las tareas siguientes para gestionar el servidor de copia de seguridad:

- Configurar la duración para conservar el historial de tareas y los registros de actividades
- Configurar la duración para conservar los registros de depuración
- Cambiar el número de puerto de la shell segura (SSH) del servidor de copia de seguridad

El siguiente diagrama muestra el proceso de gestión del servidor de copia de seguridad:



Realice las tareas siguientes para gestionar los valores de configuración del servidor de copia de seguridad:

- Revisar los requisitos previos para gestionar el servidor de copia de seguridad (en la página 181)
- Configurar el historial de tareas y los valores de configuración de retención del registro de actividades (en la página 181)
- Configurar los valores de configuración de retención del registro de depuración (en la página 182)
- Configuración de la duración del tiempo de espera de la IU (en la página 183)
- Cambio del número de puerto SSH del servidor de copia de seguridad (en la página 183)
- Gestión de los conjuntos de recuperación (en la página 184)
- Desactivación de los servicios de BOOTPD y TFTPD (en la página 185)
- Mejora del rendimiento de consultas para el historial de tareas y el registro de actividades (en la página 185)
- Omisión de la verificación del cliente de CIFS y NFS (en la página 186)

Revisar los requisitos previos para gestionar el servidor de copia de seguridad

Tenga en cuenta los requisitos previos siguientes antes de gestionar el servidor de copia de seguridad:

- Dispone de las credenciales de inicio de sesión raíz para el servidor de copia de seguridad.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Configurar el historial de tareas y los valores de configuración de retención del registro de actividades

Se debe configurar la duración para conservar el historial de tareas y los registros de actividades. Si desea conservar los registros de actividades y el historial de tareas durante más tiempo, debe configurar el archivo del servidor.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra el archivo server.cfg:

   ```
   /opt/CA/d2dserver/configfiles/server.cfg
   ```

   Nota: Si el archivo no está presente, cree el archivo server.cfg.

3. Agregue la siguiente línea en el archivo server.cfg:

   ```
   job_history_activity_log_keep_day=<number of days>
   ```

   Ejemplo: Para conservar el historial de tareas y el registro de actividad durante 30 días, introduzca la siguiente línea:

   ```
   job_history_activity_log_keep_day=30
   ```

   Nota: De forma predeterminada, se retienen el historial de tareas y los registros de actividad durante 90 días.

Se retiene el historial de tareas y el registro de actividad durante el período especificado.

Configurar los valores de configuración de retención del registro de depuración

Se puede configurar la duración para conservar los registros de depuración. Si desea conservar los registros de depuración y el historial de tareas durante más tiempo, debe configurar el archivo del servidor.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra el archivo server.cfg:

   ```
   /opt/CA/d2dserver/configfiles/server.cfg
   ```

   Nota: Si el archivo no está presente, cree el archivo server.cfg.
3. Agregue la siguiente línea en el archivo server.cfg:

   ```
   d2d_log_keep_day =<number of days>
   ```

   Ejemplo: Para retener el registro de depuración durante 30 días, introduzca la siguiente línea:

   ```
   d2d_log_keep_day =30
   ```

   Nota: De forma predeterminada, los registros de depuración se retienen durante 90 días.

El registro de depuración del Agente de Arcserve UDP (Linux) se retiene durante el período especificado.

Configuración de la duración del tiempo de espera de la IU

Se puede configurar el archivo de configuración de Webserver para que se cierre la sesión de la IU cuando esté inactiva. Después de configurar el archivo, si no se realiza actividad en la IU durante el período especificado, se cerrará sesión automáticamente. Se puede volver a iniciar sesión y reanudar la actividad.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra el archivo server.cfg de la siguiente ubicación:

   `/opt/CA/d2dserver/configfiles/server.cfg`

   Nota: Si el archivo server.cfg no está presente, créelo.
3. Agregue la siguiente línea en el archivo server.cfg:

   `ui_timeout=<value>`

   El valor debe estar en minutos. El límite máximo para el valor de tiempo de espera de IU es 60.

   Ejemplo:

   `ui_timeout=40`

   El ejemplo indica que si el servidor de copia de seguridad no detecta actividad en la IU durante 40 minutos, se cerrará la sesión del usuario.
4. Actualice el explorador web para implementar los cambios.

Se configurará la duración del tiempo de espera de la IU.

Cambio del número de puerto SSH del servidor de copia de seguridad

El servidor de copia de seguridad usa el puerto 22 de la shell segura predeterminada (SSH) para conectarse a los nodos. Si desea cambiar el puerto predeterminado a un puerto diferente, se puede configurar el archivo server.env para especificar el puerto nuevo.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.

2. Abra el archivo server.env.

   `/opt/CA/d2dserver/configfiles/server.env`

   Nota: Si el archivo no está presente, cree el archivo server.env.

3. Agregue la línea siguiente en el archivo server.env y guarde el archivo:

   `export D2D_SSH_PORT=new_port_number`

   new_port_number debe ser un valor numérico.

4. Reinicie el servidor de copia de seguridad.

   Después de configurar el archivo server.env, todas las tareas, excepto la tarea de BMR, utilizan el número de puerto nuevo para conectarse al nodo de destino. La tarea de BMR usa el puerto predeterminado.

El número de puerto de SSH del servidor de copia de seguridad se ha modificado correctamente.

Gestión de los conjuntos de recuperación

La gestión de los conjuntos de recuperación incluye la supresión de los conjuntos de recuperación. Se deberían gestionar los conjuntos de recuperación regularmente para ser consciente del espacio libre disponible. Para ello, se puede planear un almacenamiento de los conjuntos de recuperación. Hay dos formas para gestionar los conjuntos de recuperación:

- **Método 1:** Gestionar mediante un almacenamiento de copia de seguridad especializado. En este método, el almacenamiento de copia de seguridad gestiona los conjuntos de recuperación cada 15 minutos. Se pueden gestionar solamente los almacenamientos de copia de seguridad a los cuales tiene acceso el servidor de copia de seguridad. Si se elige el origen local como el destino de la copia de seguridad, tendrá que compartir la carpeta local.
- **Método 2:** Gestionar mediante una tarea de copia de seguridad. En este método, la tarea de copia de seguridad gestiona los conjuntos de recuperación. Los conjuntos de recuperación se gestionan después de finalizar la tarea de copia de seguridad. Se pueden gestionar los conjuntos de recuperación que se almacenan en el local de origen.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra el archivo server.cfg.

   `/opt/CA/d2dserver/configfiles/server.cfg`

   Nota: Si el archivo no está presente, cree el archivo server.cfg.

3. Agregue la línea siguiente en el archivo server.cfg y guarde el archivo:

   `manage_recoveryset_local=0 o 1`

El valor 0 indica que el archivo utiliza el método 1.

El valor 1 indica que el archivo utiliza el método 2.

4. Reinicie el servidor de copia de seguridad.

Los conjuntos de recuperación se gestionan en la línea de comandos del servidor de copia de seguridad.

Desactivación de los servicios de BOOTPD y TFTPD

Se pueden desactivar los servicios de BOOTPD y TFTPD si no se requiere la función de BMR de PXE.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra el archivo server.env.

   `/opt/CA/d2dserver/configfiles/server.env`
3. Actualice el parámetro siguiente en el archivo server.env y guarde el archivo:

   `export D2D_DISABLE_PXE_SERVICE=yes`
4. Reinicie el servidor de copia de seguridad

   `/opt/CA/d2dserver/bin/d2dserver restart`

Los servicios de BOOTPD y TFTPD se han desactivado correctamente.

Mejora del rendimiento de consultas para el historial de tareas y el registro de actividades

Si se tiene un archivo de base de datos mayor, la consulta del historial de tareas y del registro de actividades llevará mucho más tiempo. Se puede mejorar el tiempo de consulta para el historial de tareas y el registro de actividades mediante los conmutadores específicos y obtener el resultado en un tiempo breve.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra el archivo server.cfg:

   `/opt/CA/d2dserver/configfiles/server.cfg`

   Nota: Si el archivo no está presente, cree el archivo server.cfg.

3. Agregue las siguientes líneas en el archivo server.cfg:
   - Para mejorar el rendimiento de consultas del historial de tareas, agregue la línea siguiente:

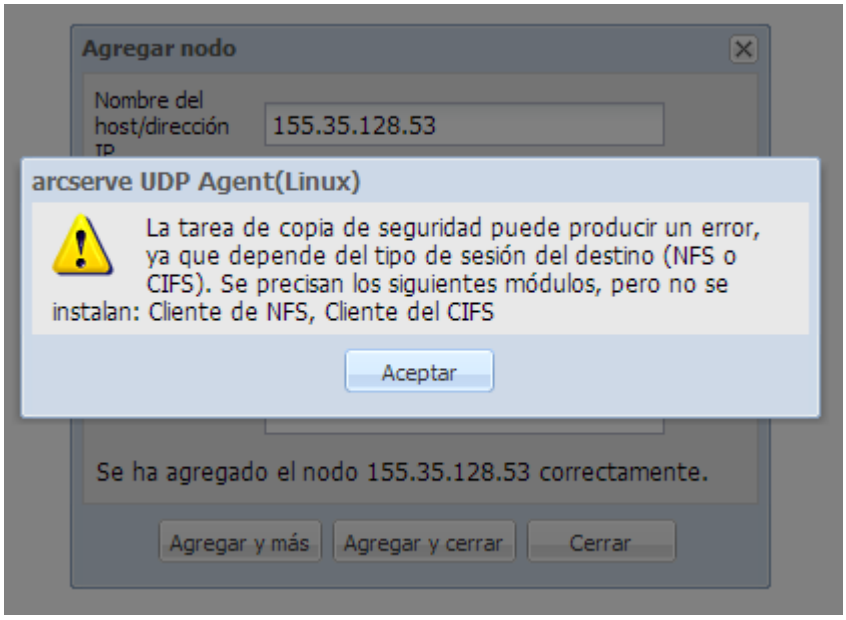
     ```
     skip_getting_job_history_count=true
     ```
   - Para mejorar el rendimiento de consultas del registro de actividades, agregue la línea siguiente:

     ```
     skip_getting_activity_log_count=true
     ```
4. Guarde el archivo server.cfg.

El tiempo de consulta para el historial de tareas y el registro de actividades se ha optimizado correctamente.

Omisión de la verificación del cliente de CIFS y NFS

Cuando se agrega o se modifica un nodo, el servidor de copia de seguridad verifica los módulos CIFS y NFS en el nodo de destino. Si uno de los módulos no está instalado, se abrirá un cuadro de diálogo de advertencia. Se puede ocultar este cuadro de diálogo configurando el archivo server.cfg.



Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad.
2. Abra el archivo server.cfg:

   `/opt/CA/d2dserver/configfiles/server.cfg`
3. Agregue el siguiente parámetro:

   `skip_client_check=cliente 1,cliente 2`

   Ejemplo:

   `skip_client_check=nfs,cifs`

   El ejemplo proporcionado omite la verificación de los paquetes de NFS y de CIFS en el nodo de destino. Cuando se proporcionan los dos clientes, la verificación se omite para los dos clientes. Cuando solo se proporciona un cliente, la verificación se omite para solamente ese cliente.
4. Guarde el archivo server.cfg.

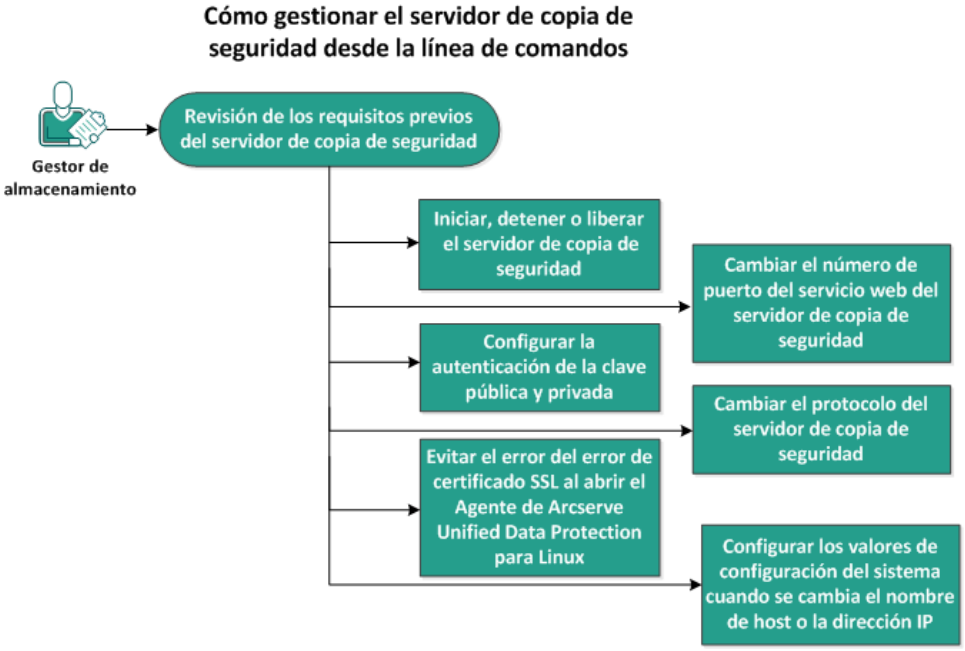
La verificación se omite para los clientes de CIFS y NFS.

Cómo gestionar el servidor de copia de seguridad de Linux desde la línea de comandos

El servidor de copia de seguridad de Linux realiza todas las tareas de procesamiento del Agente de Arcserve UDP (Linux). Para un correcto funcionamiento del Agente de Arcserve UDP (Linux), debe asegurarse de que el servidor de copia de seguridad se esté ejecutando. Se puede iniciar sesión en el servidor de copia de seguridad y gestionar el servidor mediante algunos comandos.

Por ejemplo, si desea acceder a la interfaz web del Agente de Arcserve UDP (Linux), se debe garantizar que el servidor web esté en ejecución. Se puede verificar el estado de ejecución del servidor web desde el servidor de copia de seguridad y garantizar el correcto funcionamiento del Agente de Arcserve UDP (Linux).

El diagrama siguiente muestra el proceso para gestionar el servidor de copia de seguridad desde la línea de comandos:



Realice las tareas siguientes para gestionar el servidor de copia de seguridad:

- Revisión de los requisitos previos del servidor de copia de seguridad (en la página 189)
- Inicio, detención o liberación del servidor de copia de seguridad (en la página 189)
- Cambio del número de puerto del servicio web del servidor de copia de seguridad (en la página 190)
- Configuración de la autenticación de la clave pública y privada (en la página 191)
- Cambio del protocolo del servidor de copia de seguridad (en la página 192)
- Evitación del error de certificado SSL al abrir el Agente de Arcserve UDP (Linux) (en la página 193)
- Configuración de los valores de configuración del sistema cuando se cambia el nombre de host o la dirección IP (en la página 195)

Revisión de los requisitos previos del servidor de copia de seguridad

Tenga en cuenta los requisitos previos siguientes antes de gestionar el servidor de copia de seguridad:

- Dispone de las credenciales de inicio de sesión raíz para el servidor de copia de seguridad.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Inicio, detención o liberación del servidor de copia de seguridad

Gestione el servidor de copia de seguridad para saber el estado de ejecución del servidor de copia de seguridad. Se puede verificar si se ha detenido el servidor de copia de seguridad o si se está ejecutando todavía y, a continuación, gestionar el servidor. El Agente de Arcserve UDP (Linux) admite las funciones siguientes de la línea de comandos:

- Inicio del servidor de copia de seguridad
- Detención del servidor de copia de seguridad
- Liberación del servidor de copia de seguridad

Siga estos pasos:

1. Vaya a la carpeta bin mediante el siguiente comando:

   ```
   # cd/opt/CA/d2dserver/bin
   ```

   Obtenga acceso a la carpeta bin.

2. Desde la carpeta bin, ejecute los siguientes comandos en función de la tarea que se desee realizar en el servidor:

   Nota: Si el comando no es correcto, aparecerá un mensaje de error explicando el motivo.

   ```
   # ./d2dserver start
   ```

   Inicia el servidor de copia de seguridad.

   Si es correcto, aparecerá un mensaje informando de que el servidor se ha iniciado.

`# ./d2dserver stop`

Detiene el servidor de copia de seguridad.

Si es correcto, aparecerá un mensaje informando de que el servidor se ha detenido

`# ./d2dserver restart`

Reinicia el servidor de copia de seguridad.

Si es correcto, aparecerá un mensaje informando de que el servidor se ha reiniciado.

`# ./d2dserver status`

Muestra el estado del servidor de copia de seguridad.

`# /opt/CA/d2dserver/bin/d2dreg --release`

Libera los servidores de copia de seguridad restantes que el servidor principal gestiona.

Por ejemplo, si el servidor de copia de seguridad A gestiona otros dos servidores (el servidor de copia de seguridad B y el servidor de copia de seguridad C), cuando se desinstala el servidor de copia de seguridad A no se podrá acceder al servidor de copia de seguridad B ni al servidor de copia de seguridad C. Se pueden liberar el servidor de copia de seguridad B y el servidor de copia de seguridad C mediante este script; además, se podrá acceder a estos servidores.

El servidor de copia de seguridad se ha gestionado correctamente desde la línea de comandos.

Cambio del número de puerto del servicio web del servidor de copia de seguridad

El Agente de Arcserve UDP (Linux) utiliza el puerto 8014 de forma predeterminada. Si otra aplicación utiliza el número de puerto 8014, el Agente de Arcserve UDP (Linux) no funcionará correctamente. En estas circunstancias, se debe cambiar el número de puerto predeterminado del Agente de Arcserve UDP (Linux) a un número de puerto diferente.

Siga estos pasos:

1. Abra el archivo server.xml de la siguiente ubicación:

   `/opt/CA/d2dserver/TOMCAT/conf/server.xml`

2. Busque la siguiente cadena en el archivo y cambie el número de puerto 8014 al número de puerto deseado:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

3. Ejecute el siguiente comando para reiniciar el servidor de copia de seguridad:

   ```
   /opt/CA/d2dserver/bin/d2dserver restart
   ```

El número de puerto predeterminado se cambia al número de puerto deseado.

Configuración de la autenticación de la clave pública y privada

La clave pública y la clave privada permiten conectarse de forma segura a los nodos cuando no se proporciona la contraseña. Cada vez que el servidor de copia de seguridad crea una conexión SSH con los nodos, el servidor de copia de seguridad verifica la clave pública y privada para los nodos respectivos. Si las claves no coinciden, aparecerá un mensaje de error.

Nota:

- Solamente se admiten los usuarios que tienen permisos raíz para utilizar la autenticación de clave pública y privada. No es necesario tener el nombre de usuario como raíz. Los usuarios no raíz no se admiten para el uso de la autenticación de clave pública y privada. Los usuarios no raíz deben proporcionar la autenticación del nombre de usuario y contraseña.
- La autenticación de clave pública y privada se aplica cuando no se proporciona la contraseña. El nombre del usuario todavía es obligatorio y debe coincidir con el propietario de la clave.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Genere una clave pública/privada mediante el comando de ssh-keygen siguiente:

   ```
   ssh-keygen -t rsa -f server
   ```

   Se generan dos archivos, concretamente server.pub y server.
3. Copie el archivo de clave pública server.pub en la ubicación siguiente:

   ```
   /opt/CA/d2dserver/configfiles/server_pub.key
   ```

4. Copie el archivo de clave pública en la ubicación siguiente:

   ```
   /opt/CA/d2dserver/configfiles/server_pri.key
   ```

5. (Opcional) Ejecute el comando siguiente si se ha proporcionado la frase de contraseña al generar las claves públicas y privadas:

   ```
   echo "passphrase" | d2dutil encrypt > /opt/CA/d2dserver/configfiles/key.pass
   ```

6. Cambie el permiso para el archivo key.pass mediante el comando siguiente:

   ```
   chmod 600 /opt/CA/d2dserver/configfiles/key.pass
   ```

7. Inicie sesión en el nodo de origen.

8. Copie el contenido del archivo server_pub.key en el servidor de copia de seguridad a la ubicación siguiente en el nodo:

   ```
   /root/.ssh/authorized_keys
   ```

La clave privada y la clave pública están correctamente configuradas. Se puede conectar a los nodos de origen mediante la clave pública y privada.

Cambio del protocolo del servidor de copia de seguridad

Se instala el Agente de Arcserve UDP (Linux) con el protocolo HTTPS. Se puede cambiar el protocolo si no se desea transferir datos cifrados. Se recomienda utilizar HTTPS, ya que todos los datos transferidos con este protocolo se cifran. Sin embargo, los datos transferidos con HTTP no se cifran.

Siga estos pasos:

1. Abra el archivo server.xml de la siguiente ubicación:

   ```
   /opt/CA/d2dserver/TOMCAT/conf/server.xml
   ```

2. Busque la siguiente cadena en el archivo server.xml:

   ```
   <!--<Connector connectionTimeout="180000" port="8014" protocol="HTTP/1.1"/>-->
   ```

3. Elimine los caracteres **<!--** y **-->**tal y como se muestra en el siguiente ejemplo:

   Ejemplo: la siguiente cadena es el resultado deseado después de eliminar los caracteres de cadena **<!--** y **-->:**

   ```
   <Connector connectionTimeout="180000" port="8014" protocol="HTTP/1.1"/>
   ```

4. Busque la siguiente cadena en el archivo server.xml:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

5. Elimine los caracteres de cadena **<!--** y **-->**tal y como se muestra en el siguiente ejemplo:

   Ejemplo: la siguiente cadena es el resultado deseado después de agregar los caracteres de cadena **<!--** y **-->:**

   ```
   <!--<Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true" clientAuth="false"
   sslProtocol="TLS" keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>-->
   ```

6. Ejecute el siguiente comando para reiniciar el servidor de copia de seguridad:

   ```
   /opt/CA/d2dserver/bin/d2dserver restart
   ```

El protocolo del servidor de copia de seguridad se cambia de HTTPS a HTTP.

Evitación del error de certificado SSL al abrir el Agente de Arcserve UDP (Linux)

Configure el certificado SSL personalizado para no obtener el error de certificado al abrir la interfaz web del Agente de Arcserve UDP (Linux). Una vez que se configura el certificado SSL, no se volverá a obtener el error de certificado.

Siga estos pasos:

- Utilice el certificado que genera el Agente de Arcserve UDP (Linux) para el explorador Firefox.

  1. Abra el Agente de Arcserve UDP (Linux) en Firefox.
  2. Haga clic en Understand the Risks y, a continuación, haga clic en Add Exception.

     Aparece el cuadro de diálogo Add Security Exception.
  3. Haga clic en View para revisar el certificado.

     Se abrirá el cuadro de diálogo Certificate Viewer.
  4. Revise los detalles de certificado y haga clic en Close.

     No es necesario realizar ninguna acción en el cuadro de diálogo Certificate Viewer.
  5. En el cuadro de diálogo Add Security Exception, seleccione la casilla de verificación Permanently store this exception.
  6. Haga clic en Confirm Security Exception.

     Se agregará el certificado.

- Use el certificado que ha generado el Agente de Arcserve UDP (Linux) para los exploradores Internet Explorer (IE) o Chrome.

  1. Abra el Agente de Arcserve UDP (Linux) en IE o Chrome.
  2. Haga clic en Continue to this website (not recommended).

     La barra de dirección se muestra en rojo y aparece un mensaje Certificate Error en la barra de estado de seguridad.
  3. Seleccione Certificate Error.

     Aparece el cuadro de diálogo Untrusted Certificate.
  4. Haga clic en View certificates.

     Se abrirá el cuadro de diálogo Certificado.
  5. En la ficha General, haga clic en Install Certificate.

     Se abrirá el Asistente para importación de certificados.
  6. Haga clic en Next.
  7. En la página Certificate Store, seleccione Place all certificates in the following store y, a continuación, haga clic en Browse.

     Se abrirá el cuadro de diálogo Seleccionar el almacén de certificados.
  8. Seleccione Trusted Root Certification Authorities y haga clic en Aceptar.

     Se abre la página Certificate Store del asistente para importación de certificados.
  9. Haga clic en Next y, a continuación, haga clic en Finish.

     Se abrirá el cuadro de diálogo Security Warning.
  10. Haga clic en Sí.
  11. Reinicie IE o Chrome.

      Se agregará el certificado.

      Nota: Después de agregar el certificado, el explorador de Chrome todavía mostrará el icono de error para el certificado SSL en la barra de direcciones. Esto es un recordatorio sobre las autoridades de certificación que no identifican el certificado pero según Chrome el certificado es de confianza y todos los datos que se transfieren a la red se cifran.

- Realice los pasos siguientes para usar un certificado firmado:

  1. Use el certificado firmado por una autoridad de certificación.
  2. Importe el certificado firmado mediante el comando keytool.

     Se agregará el certificado.

Se resuelve el error de certificado ssl.

Configuración de los valores de configuración del sistema cuando se cambia el nombre de host o la dirección IP

Si se modifica el nombre de host o la dirección IP del servidor de copia de seguridad o del nodo del cliente (nodo de copia de seguridad), deberá configurar los valores de configuración del sistema. Configure los valores de configuración del sistema para garantizar los elementos siguientes:

- Para garantizar que la comunicación entre el servidor central y el servidor miembro es óptima. Un servidor miembro es un servidor de copia de seguridad que se gestiona desde el servidor de copia de seguridad central. Para gestionar el servidor miembro desde la IU del servidor central, se debe agregar el servidor miembro a la IU del servidor central.
- Para garantizar que después de modificar el nombre de host o la dirección IP del nodo del cliente se puede realizar una copia de seguridad del nodo del cliente sin ningún error.

Cuando se modifica el nombre de host del servidor de copia de seguridad central

Cuando se modifica el nombre de host del servidor de copia de seguridad central, se debe configurar el servidor de modo que se pueda utilizar el Agente de Arcserve UDP (Linux) sin ningún problema.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad central como usuario raíz.
2. Para actualizar el nombre de host y la información de la licencia, introduzca los comandos siguientes:

   ```
   source /opt/CA/d2dserver/bin/setenv
   ```

   ```
   /opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/ARCserveLinuxD2D.db
   "update D2DServer set Name='New_Hostname' where IsLocal=1"
   ```

   ```
   /opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/License.db "update
   LicensedMachine set ServerName ='New_Hostname' where ServerName ='Old_Hostname'"
   ```

3. Cambie el nombre del archivo keystore:

   ```
   mv /opt/CA/d2dserver/TOMCAT/conf/server.keystore
   /opt/CA/d2dserver/TOMCAT/conf/server.keystore.old
   ```

4. Cree un archivo keystore mediante el comando keytool de Java.

   ```
   keytool -genkey -alias tomcat -keyalg DSA -keypass <YOUR_VALUE> -storepass
   <YOUR_VALUE> -keystore /opt/CA/d2dserver/TOMCAT/conf/server.keystore -validity
   3600 -dname "CN=<New Hostname>"
   ```

   Nota: Actualice el campo YOUR_VALUE según los requisitos. Normalmente, el valor es la contraseña.

   Ejemplo:

   ```
   keytool -genkey -alias tomcat -keyalg DSA -keypass LinuxD2D -storepass LinuxD2D
   -keystore /opt/CA/d2dserver/TOMCAT/conf/server.keystore -validity 3600 -dname
   "CN=New Hostname"
   ```

5. Abra el archivo de configuración de TOMCAT server.xml y cambie el valor de keystoreFile y el valor de keystorePass de acuerdo con el archivo keystore que se acaba de crear:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="YOUR_VALUE"/>
   ```

   Ejemplo:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

6. Reinicie el servidor de copia de seguridad central.

```
/opt/CA/d2dserver/bin/d2dserver restart
```

El servidor de copia de seguridad central está configurado.

Cuando se cambia el nombre de host o la dirección IP del servidor miembro

Cuando se cambia el nombre de host o la dirección IP del servidor de copia de seguridad miembro, configure el servidor miembro para gestionarlo desde el servidor central. Si no se configura el servidor miembro, aparecerá un error al intentar gestionarlo desde el servidor central. Un servidor miembro es un servidor que se ha agregado a la interfaz web del servidor de copia de seguridad central.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad central como usuario raíz:
2. Para cambiar el nombre de host, introduzca los comandos siguientes:

   ```
   source /opt/CA/d2dserver/bin/setenv
   ```

   ```
   /opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/ARCserveLinuxD2D.db
   "update D2DServer set Name='New_Hostname' where IsLocal=1"
   ```

3. Cambie el nombre del archivo keystore:

   ```
   mv /opt/CA/d2dserver/TOMCAT/conf/server.keystore
   /opt/CA/d2dserver/TOMCAT/conf/server.keystore.old
   ```

4. Cree un archivo keystore mediante el comando keytool de Java.

   ```
   keytool -genkey -alias tomcat -keyalg DSA -keypass <YOUR_VALUE> -storepass
   <YOUR_VALUE> -keystore /opt/CA/d2dserver/TOMCAT/conf/server.keystore -validity
   3600 -dname "CN=<New Hostname>"
   ```

   Nota: Actualice el campo YOUR_VALUE según los requisitos. Normalmente, el valor es la contraseña.

   Ejemplo:

   ```
   keytool -genkey -alias tomcat -keyalg DSA -keypass LinuxD2D -storepass LinuxD2D
   -keystore /opt/CA/d2dserver/TOMCAT/conf/server.keystore -validity 3600 -dname
   "CN=New Hostname"
   ```

5. Abra el archivo de configuración de TOMCAT server.xml y cambie el valor de keystoreFile y el valor de keystorePass según el archivo keystore.

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="YOUR_VALUE"/>
   ```

   Ejemplo:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
   scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
   keystoreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

6. Reinicie el servidor de copia de seguridad miembro.

   ```
   /opt/CA/d2dserver/bin/d2dserver restart
   ```

7. Inicie sesión en la interfaz web de Agente de Arcserve Unified Data Protection para Linux central.

8. En el panel Servidores de copia de seguridad, seleccione el servidor de nombre de host anterior.

9. En el menú Servidor de copia de seguridad, haga clic en Suprimir.

10. En el cuadro de diálogo Suprimir, seleccione Aceptar.

    El servidor del nombre de host antiguo se suprime.

11. En el menú Servidor de copia de seguridad, haga clic en Agregar.

    Aparecerá el cuadro de diálogo Agregar servidor.

12. Introduzca los detalles del nuevo nombre de host en el cuadro de diálogo y haga clic en Aceptar.

    El cuadro de diálogo Agregar servidor y el servidor miembro con el nuevo nombre de host se agrega a la IU.

13. Inicie sesión en el servidor de copia de seguridad central que gestiona el servidor de copia de seguridad miembro.

14. Para actualizar la información de la licencia, introduzca los comandos siguientes:

    ```
    source /opt/CA/d2dserver/bin/setenv
    ```

    ```
    /opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/License.db "update
    LicensedMachine set ServerName ='New_Hostname' where ServerName ='Old_Hostname'"
    ```

El servidor de copia de seguridad miembro está configurado.

Cuando se cambia el nombre de host o la dirección IP del nodo del cliente

Si se modifica el nombre de host o la dirección IP de un nodo, se puede configurar el nombre de host o la dirección IP en los valores de configuración del sistema para que se pueda realizar una copia de seguridad del nodo sin ningún error.

Siga estos pasos:

1. Inicie sesión en el destino de copia de seguridad.
2. Encuentre la carpeta denominada "**Old_Hostname"** en el destino de copia de seguridad de este nodo y renómbrela a "**New_Hostname**".

   Por ejemplo, tenga en cuenta que el nombre de host antiguo para node1 es First_Node. El destino de copia de seguridad para node1 es //Backup_Destination/LinuxBackup. Después de la primera copia de seguridad correcta, se creará una carpeta denominada First_Node en //Backup_Destination/LinuxBackup. Ahora, se ha modificado el nombre de host antiguo a Second_Node. Busque la carpeta First_Node en //Backup_Destination/LinuxBackup y renómbrela a Second_Node.
3. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
4. Para actualizar el nombre de host, introduzca los comandos siguientes:

   ```
   source /opt/CA/d2dserver/bin/setenv
   ```

   ```
   /opt/CA/d2dserver/bin/d2drp --storagepath=Backup Destination
   --node=New_Hostname
   ```

   ```
   /opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/ARCserveLinuxD2D.db
   "update JobQueue set TargetName='New_Hostname' where JobType in (1,3,4,5) and
   TargetName='Old_Hostname'"
   ```

   ```
   /opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/ARCserveLinuxD2D.db
   "update TargetMachine set Name='New_Hostname' where Name='Old_Hostname'"
   ```

   Nota: Si se utiliza un recurso compartido de NFS o de CIFS como destino de copia de seguridad, se debería montar en un recurso compartido local.

   Ejemplo: Si su punto de montaje es /mnt/backup_destination.

   ```
   /opt/CA/d2dserver/bin/d2drp --storagepath=<mount point>
   --node=New_Hostname
   ```

   Nota: Si se utiliza el recurso compartido Local, el comando será:

   ```
   /opt/CA/d2dserver/bin/d2drp --storagepath=<local path> --node=New_Hostname
   ```

5. Inicie sesión en el servidor de copia de seguridad central como usuario raíz.
6. Para actualizar la información de la licencia, introduzca el comando siguiente:

```
/opt/CA/d2dserver/sbin/sqlite3 /opt/CA/d2dserver/data/License.db "update
LicensedMachine set MachineName ='New_Hostname' where MachineName
='Old_Hostname'"
```

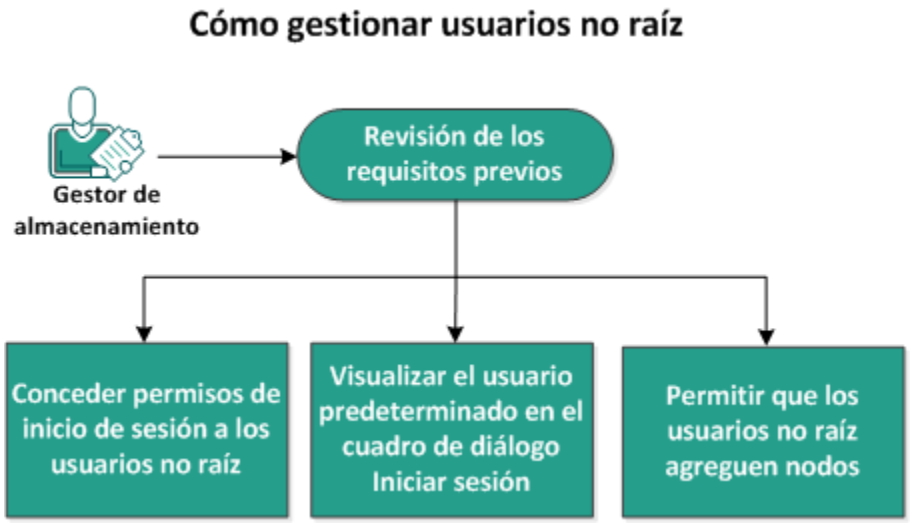
El nombre de host se configura para realizar una copia de seguridad sin ningún error.

Cómo gestionar usuarios no raíz

Se pueden gestionar todos los usuarios no raíz que acceden al Agente de Arcserve UDP (Linux) y se pueden definir los permisos de los usuarios no raíz con objeto de limitar el nivel de acceso del Agente de Arcserve UDP (Linux). Se pueden gestionar los usuarios no raíz modificando el archivo de configuración de Webserver (archivo server.cfg).

Nota: Si su nodo de origen de copia de seguridad se ha configurado con pam_wheel, utilice la opción use_uid para configurar pam_wheel. Para obtener más información sobre pam_wheel, consulte la página de pam_wheel.

El siguiente diagrama ilustra el proceso de gestión de los usuarios no raíz:



Realice estas tareas para gestionar los usuarios no raíz:

- Revisión de los requisitos previos (en la página 201)
- Concesión de permisos de inicio de sesión a los usuarios no raíz (en la página 201)
- Visualización del usuario predeterminado en el cuadro de diálogo Iniciar sesión (en la página 202)
- Permiso para que los usuarios no raíz agreguen nodos (en la página 203)

Revisión de los requisitos previos

Tenga en cuenta los requisitos previos siguientes antes de gestionar los usuarios no raíz:

- Dispone de las credenciales de inicio de sesión raíz para el servidor de copia de seguridad.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Concesión de permisos de inicio de sesión a los usuarios no raíz

Un usuario raíz puede conceder permisos a usuarios no raíz para que inicien sesión en el servidor de copia de seguridad. Si los usuarios no raíz obtienen los permisos para iniciar sesión en el servidor de copia de seguridad, pueden utilizar el Agente de Arcserve UDP (Linux) con objeto de llevar a cabo todas las tareas de recuperación y protección de datos.

Nota: Para conceder permisos de inicio de sesión a los usuarios no raíz, inicie sesión en el servidor de copia de seguridad como usuario raíz mediante la conexión SSH.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra el archivo server.cfg de la siguiente ubicación:

   ```
   /opt/CA/d2dserver/configfiles/server.cfg
   ```

   Nota: Si el archivo server.cfg no está presente, créelo.
3. Agregue el siguiente código en el archivo server.cfg:

   ```
   allow_login_users=user1 user2
   ```

   Nota: Utilice espacios en blanco para distinguir varios usuarios.

   Se agregará el código.
4. Verifique que el usuario no raíz pueda iniciar sesión en el servidor de copia de seguridad mediante la conexión SSH.

Los permisos de inicio de sesión se conceden a los no usuarios para que accedan al servidor de copia de seguridad.

Visualización del usuario predeterminado en el cuadro de diálogo Iniciar sesión

Se pueden gestionar los usuarios y cambiar el nombre que se muestra en el cuadro de diálogo para iniciar sesión de Agente de Arcserve UDP (Linux). El usuario predeterminado que se muestra en el cuadro de diálogo Iniciar sesión es usuario raíz. Si no se dispone de usuarios raíz que acceden al producto, se puede cambiar el nombre predeterminado a cualquier nombre de usuario no raíz. Se puede conseguir modificando el archivo server.cfg que se encuentra en el servidor de copia de seguridad.

Nota: Para modificar el archivo server.cfg, inicie sesión en el servidor de copia de seguridad como usuario raíz mediante la conexión SSH.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra el archivo server.cfg de la siguiente ubicación:

   `/opt/CA/d2dserver/configfiles/server.cfg`

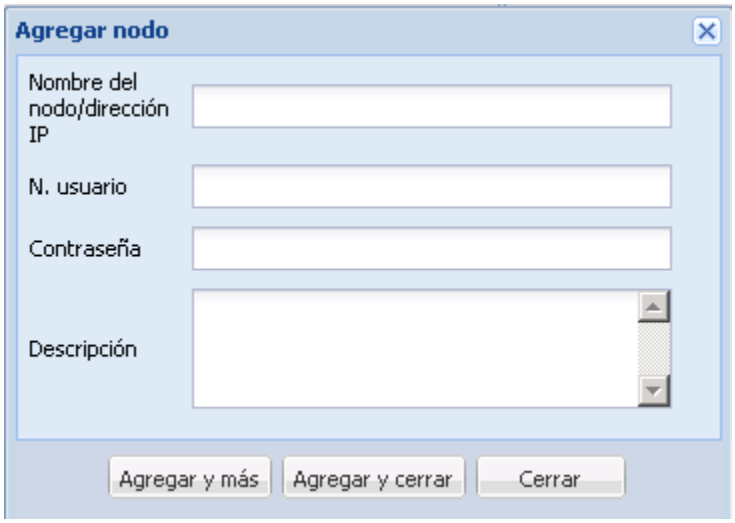
   Nota: Si el archivo server.cfg no está presente, créelo.
3. Agregue el siguiente código en el archivo server.cfg:
   show_default_user_when_login=false|true
4. Inicie sesión en la interfaz web del Agente de Arcserve UDP (Linux).
   - Si se ha agregado el comando *allow_login_users,* el cuadro de diálogo Iniciar sesión mostrará el primer usuario agregado en el comando *allow_login_users.*
   - Si no se ha agregado el comando *allow_login_users,* el cuadro de diálogo Iniciar sesión mostrará el usuario raíz.

El usuario predeterminado se mostrará en el cuadro de diálogo Iniciar sesión del Agente de Arcserve UDP (Linux).

Permiso para que los usuarios no raíz agreguen nodos

Si el servidor SSH desactiva el inicio de sesión de los usuarios raíz, se puede permitir que el usuario no raíz inicie sesión para agregar nodos. Cuando se activan las credenciales de inicio de sesión de usuarios no raíz, el cuadro de diálogo Agregar nodo cambiará y se mostrará la opción Credenciales raíz.

Nota: Si se cambia la credencial de nodo del cliente desde un usuario a un usuario no raíz, es recomendable borrar la carpeta */tmp* en el nodo del cliente antes de ejecutar la tarea de copia de seguridad.



Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra el archivo server.cfg de la siguiente ubicación:

   `/opt/CA/d2dserver/configfiles/server.cfg`

   Nota: Si el archivo server.cfg no está presente, créelo.
3. Agregue la siguiente línea en el archivo server.cfg para activar la función de usuario no raíz:

   `enable_non_root_user=true`

   Se activará la función de usuario no raíz.

4. (Opcional) Agregue la siguiente línea en el archivo server.cfg para desactivar la función de usuario no raíz:

   ```
   enable_non_root_user=false
   ```

   Se desactivará la función de usuario no raíz.

Los usuarios no raíz podrán agregar nodos.

Nota: Si se cambia la contraseña para el usuario raíz o el usuario no raíz y, a continuación, se modifica el nodo, deberá volver a introducir tanto la contraseña raíz como la contraseña no raíz en los campos respectivos del cuadro de diálogo Modificar nodo.

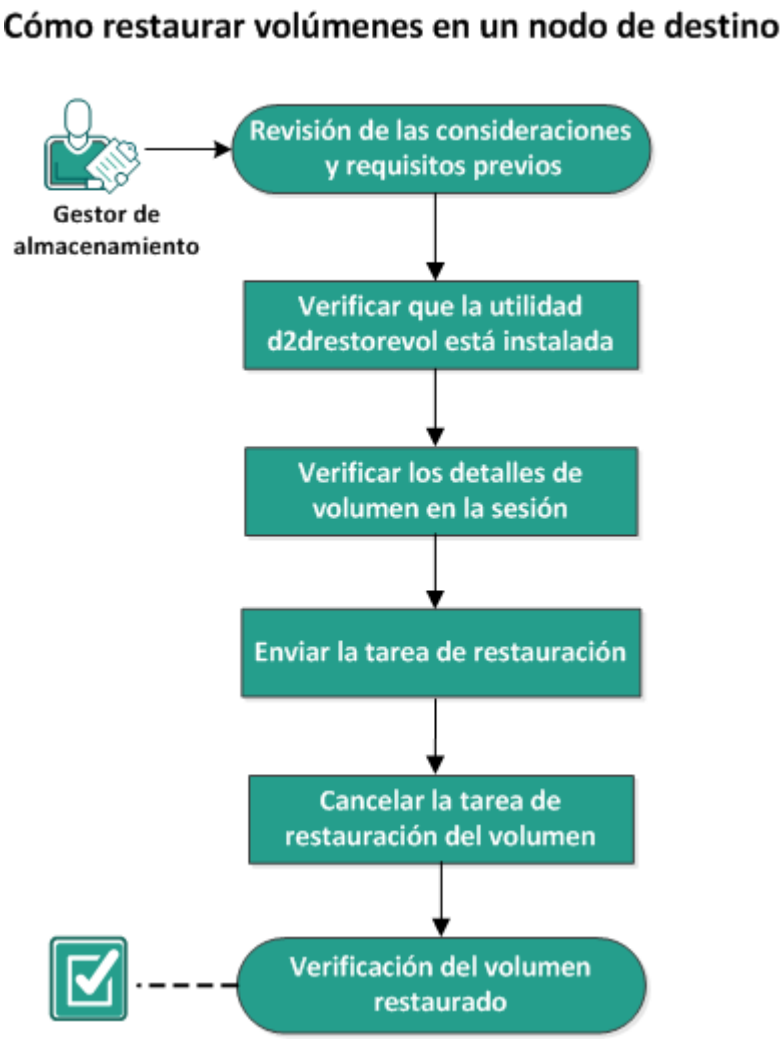
Nota: Los usuarios no raíz no pueden gestionar nodos mediante el comando *d2dnode* de la línea de comandos.

Cómo restaurar volúmenes en un nodo de destino

Se pueden restaurar volúmenes individuales en el nodo de destino sin realizar una reconstrucción completa. El nodo de destino puede ser un servidor de copia de seguridad o un nodo protegido.

El restaurar volúmenes individuales utiliza menos recursos y proporciona un rendimiento mejor.

El siguiente diagrama muestra el proceso de restauración de volúmenes:



Realice las tareas siguientes para restaurar los volúmenes:

- Revisión de las consideraciones y requisitos previos (en la página 206)
- Verificación de que la utilidad d2drestorevol está instalada (en la página 206)
- Verificación de los detalles de volumen en la sesión (en la página 208)
- Envío de la tarea de restauración (en la página 209)
- Cancelación de la tarea de restauración del volumen (en la página 211)
- Verificación del volumen restaurado (en la página 211)

Revisión de las consideraciones y requisitos previos

Revise los siguientes requisitos previos antes de restaurar volúmenes:

- Tiene una sesión de copia de seguridad válida para realizar una restauración.
- Se deberá acceder a las sesiones de copia de seguridad localmente en el nodo de destino. Si la ubicación de la sesión está en el volumen local del nodo de destino, utilice la ruta exacta del directorio como la ubicación de la sesión. Si la ubicación de la sesión está en un recurso compartido de la red, primero monte el recurso compartido de la red en un punto de montaje local y, a continuación, utilice la ruta del punto de montaje como la ubicación de la sesión.
- Los volúmenes de destino que se desean restaurar se deben desmontar mediante el comando umount:

  `Por ejemplo: umount /dev/sda2`
- El volumen de destino debe ser igual o mayor que el volumen de origen.
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Revise las siguientes consideraciones antes de restaurar los volúmenes:

- Cuando se restaura, se borrará cualquier dato existente en el volumen de destino. Realice una copia de seguridad de sus datos existentes en el volumen de destino antes de llevar a cabo la restauración.

Verificación de que la utilidad d2drestorevol está instalada

La utilidad d2drestorevol restaura el volumen en el nodo de destino. El nodo de destino puede ser un servidor de copia de seguridad o cualquier otro nodo de Linux (cliente). Si la utilidad restorevol no se instala en el nodo de destino, se debe instalar manualmente.

Restauración en un servidor de copia de seguridad

Si el nodo de destino es un servidor de copia de seguridad, la utilidad ya se ha instalado con el paquete de instalación. Verifique si la utilidad está presente en la carpeta *bin*.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad.
2. Verifique que la utilidad se encuentra en la ubicación siguiente:

   `/opt/CA/d2dserver/bin/d2drestorevol`

   La utilidad está instalada y verificada.

Restauración en un cliente

Un nodo del cliente no tendrá la utilidad instalada. Se tiene que instalar manualmente en el cliente.

Importante: La utilidad se debe descargar del servidor de copia de seguridad tal y como se describe en los pasos siguientes. Si se copia manualmente la utilidad desde un servidor de copia de seguridad a un cliente, es posible que la utilidad no funcione correctamente.

Siga estos pasos:

1. Inicie sesión en el cliente.
2. Encuentre la ruta de descarga de la utilidad d2drestorevol en la línea de comandos.

   ```
   http[s]://[dirección-servidor-copia-seguridad]:[puerto]/d2drestorevol
   ```

3. Descargue el script mediante una herramienta de la línea de comandos como, por ejemplo, wget.

   ```
   wget http://192.168.1.1:8014/d2drestorevol –O d2drestorevol
   ```

   Nota: Si el servidor utiliza el protocolo HTTPS, es posible que se tenga que incluir el parámetro '--no-check-certificate'.

   ```
   wget https://192.168.1.1:8014/d2drestorevol -O d2drestorevol
   --no-check-certificate
   ```

4. Proporcione el permiso de ejecución a la utilidad mediante el comando siguiente:

   ```
   chmod +x d2drestorevol
   ```

   Se proporciona el permiso.

La utilidad d2drestorevol se ha instalado y verificado.

Verificación de los detalles de volumen en la sesión

Verifique los detalles del volumen de la sesión que se desea restaurar. Se pueden ver el volumen de origen, el sistema de archivos, el tamaño del archivo y la información de montaje en el resultado.

Siga estos pasos:

1. Inicie sesión en el nodo de destino.
2. Utilice el siguiente comando para verificar la información del volumen:

   ```
   d2drestorevol --command=info --storage-path=<ruta_local> --node=<nombre_nodo>
   --rp=<punto_recuperación>
   ```

   --command=info

   Especifica que se mostrarán los detalles del volumen de la sesión.

   --storage-path

   Especifica la ruta determinada en el tema Requisitos previos. Para obtener más información, consulte Revisión de los requisitos previos y consideraciones.

   --node

   Especifica el nodo de origen del cual se ha realizado la copia de seguridad.

   --rp

   Especifica el punto de recuperación o sesión de recuperación que se desea restaurar. Normalmente, un punto de recuperación tiene el formato siguiente: S00000000X, donde X es un valor numérico.

   Se muestra el resultado.

Los detalles del volumen se han verificado.

Envío de la tarea de restauración

Envíe la tarea de restauración del volumen para empezar a restaurar el volumen en el nodo de destino.

Siga estos pasos:

1. Inicie sesión en el nodo de destino.
2. Envíe la tarea de restauración mediante el comando siguiente:

```
d2drestorevol --command=restore  --storage-path=<ruta_local>
--node=<nombre_nodo> --rp=<punto_recuperación>
--source-volume=<volumen_origen> --target-volume=<volumen_destino>
[--encryption-password=<contraseña_cifrada>] [--mount-target=<punto_montaje>
[--quick-recovery]]
```

--command=restore

Especifica que se ha enviado la tarea de restauración del volumen.

--storage-path

Especifica la ruta determinada en el tema Requisitos previos. Para obtener más información, consulte Revisión de los requisitos previos y consideraciones.

--node

Especifica el nodo de origen del cual se ha realizado la copia de seguridad.

--rp

Especifica el punto de recuperación o sesión de recuperación que se desea restaurar. Normalmente, un punto de recuperación tiene el formato siguiente: S00000000X, donde X es un valor numérico.

--encryption-password

Especifica la contraseña de la sesión. Esta opción se requiere si la sesión está cifrada. Si la sesión está cifrada pero esta opción no está presente, se le pedirá que introduzca la contraseña desde la terminal.

--source-volume

Especifica el volumen de origen. Se puede obtener el volumen de origen mediante el parámetro *command=info* tal y como se describe en el tema Verificación de los detalles del volumen en la sesión, o el volumen de origen puede ser el punto de montaje del sistema de origen.

--target-volume

Especifica la ruta del archivo de dispositivos del nodo de destino.

Por ejemplo: /dev/sda2

--mount-target

Especifica el punto de montaje donde el volumen restaurado se debe montar.

Ejemplo: /mnt/volrestore

--quick-recovery

Cuando se utiliza junto con --mount-target, el volumen de destino se montará lo más pronto posible. Se pueden utilizar los datos en el volumen de destino mientras los datos se están restaurando.

Después de que finalice la tarea de restauración, el proceso de restauración abandona automáticamente y se puede continuar utilizando los datos sin ninguna interrupción.

Nota: Cuando una tarea de restauración de volumen y una tarea de copia de seguridad se ejecutan al mismo tiempo, entonces:

- Si se utiliza --quick-recovery, la tarea (restauración de volumen o copia de seguridad) que se inicia más tarde no se ejecuta.
- Si no se utiliza --quick-recovery, la tarea de copia de seguridad realizará la copia de seguridad solamente de aquellos volúmenes que no se están restaurando.

La tarea de restauración se envía y se abre una pantalla que muestra el progreso. Si se desea enviar otras tareas, se puede esperar a que la tarea actual se complete o pulsar Q para salir de la pantalla y, a continuación, enviar una tarea nueva.

3. (Opcional) Utilice el comando siguiente para revisar el progreso de la tarea de restauración del volumen:

```
d2drestorevol --command=monitor
```

Los detalles de progreso como el nombre del volumen, el tiempo transcurrido, el progreso, la velocidad, el estado y el tiempo restante se muestran en una pantalla.

La pantalla se cierra cuando se completa la tarea. También se puede pulsar Q para salir manualmente de la pantalla. El salir manualmente de la pantalla no interrumpe la tarea de restauración en ejecución.

Se envía la tarea de restauración del volumen.

Cancelación de la tarea de restauración del volumen

Se puede cancelar la tarea de restauración del volumen desde la línea de comandos del nodo de destino. Utilice el comando siguiente para cancelar la tarea de restauración del volumen.

```
d2drestorevol --command=cancel --target-volume=<volumen_destino>
```

--command=cancel

Especifica que la tarea de restauración del volumen se ha cancelado.

--target-volume

Especifica la ruta del archivo de dispositivos del nodo de destino. El valor debe ser idéntico al valor utilizado para enviar la tarea de restauración.

Importante: El cancelar una tarea de restauración del volumen hará inutilizable el volumen de destino. En tales casos se puede volver a intentar la realización de la tarea de restauración del volumen o se pueden restaurar los datos perdidos, si se tiene una copia de seguridad.

Verificación del volumen restaurado

Verifique los datos cuando se restaura el volumen.

Siga estos pasos:

1. Inicie sesión en el nodo de destino.
2. Revise la pantalla de progreso para verificar el estado de terminación.
3. (Opcional) Revise el archivo *d2drestvol_activity_[volumen destino].log* para ver todos los registros de la tarea de restauración.
4. Monte el volumen restaurado y verifique que los datos se han restaurado.

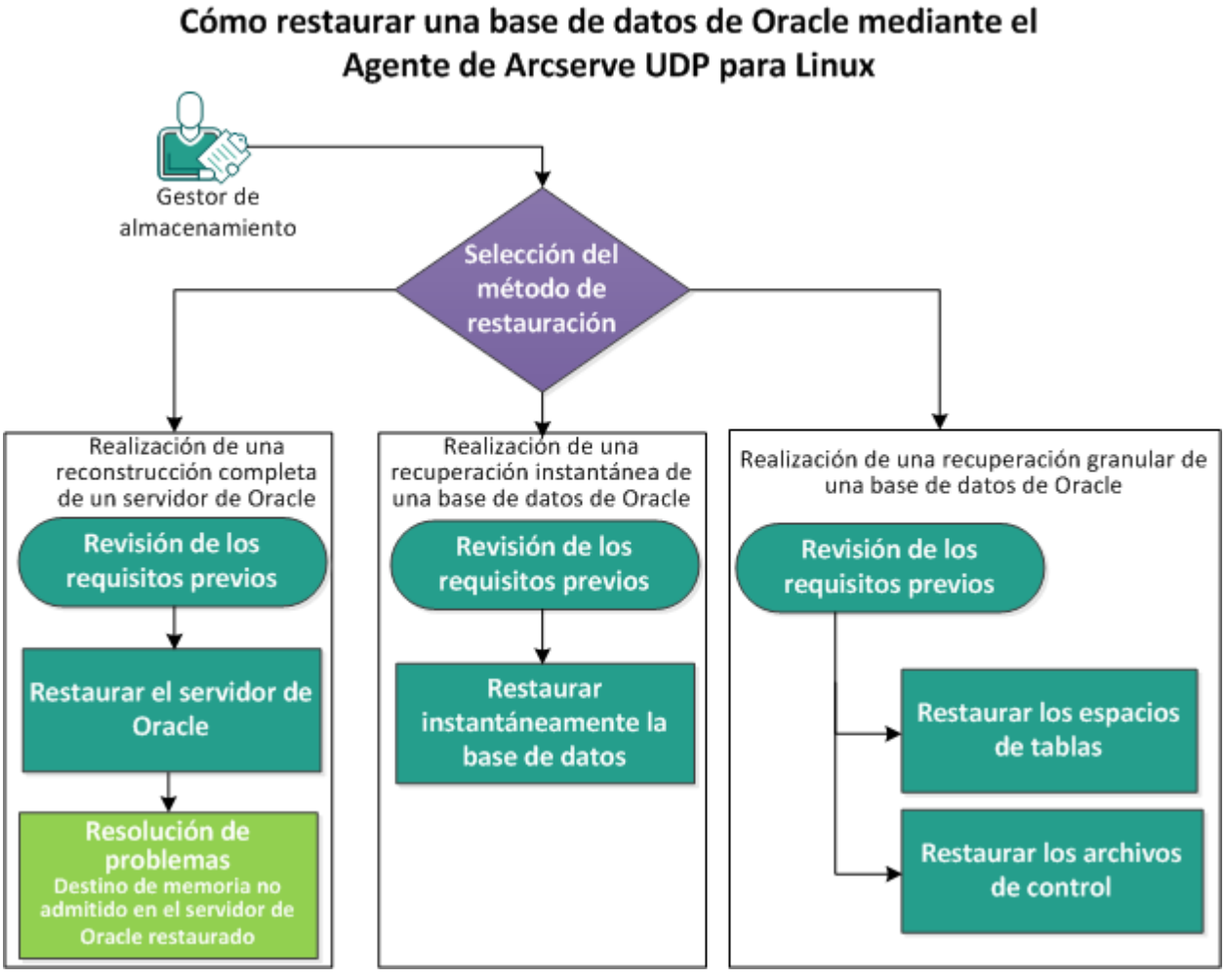
   La tarea de restauración del volumen se ha verificado.

El volumen se ha restaurado correctamente.

Cómo restaurar una base de datos de Oracle mediante el Agente de Arcserve UDP (Linux)

Se puede restaurar toda la base de datos de Oracle o restaurar archivos específicos de la base de datos. Se puede realizar también una reconstrucción completa (BMR) de un servidor de Oracle cuando el servidor de origen no funciona correctamente. Si se ha perdido la base de datos y desea que esté disponible inmediatamente, podrá realizar una recuperación instantánea. Lea los requisitos previos para cada tipo de restauración antes de empezar el proceso de restauración.

El diagrama siguiente ilustra el proceso de restauración de la base de datos de Oracle mediante el Agente de Arcserve UDP (Linux):



Realice los pasos siguientes para restaurar una base de datos de Oracle mediante el Agente de Arcserve UDP (Linux):

- Realización de una reconstrucción completa de un servidor de Oracle (en la página 213)
- Realización de una recuperación instantánea de una base de datos de Oracle (en la página 215)
- Realización de una recuperación granular de una base de datos de Oracle (en la página 218)

Realización de una reconstrucción completa de un servidor de Oracle

Una reconstrucción completa restaura las aplicaciones de software y el sistema operativo y recupera todos los datos de copia de seguridad. BMR es el proceso de restauración de un sistema informático a partir de una reconstrucción completa. La reconstrucción completa es un equipo sin ningún sistema operativo, controladores ni aplicaciones de software. Después de finalizar la restauración, el equipo de destino se reinicia automáticamente en el mismo entorno operativo que el nodo de origen de la copia de seguridad y se restaurarán todos los datos.

Se puede realizar una reconstrucción completa mediante la dirección IP o la dirección de control de acceso a medios (MAC) del equipo de destino. Si se inicia el equipo de destino mediante el Live CD del Agente de Arcserve UDP (Linux), se podrá obtener la dirección IP del equipo de destino.

Revisión de los requisitos previos

Revise los requisitos previos siguientes antes de restaurar la base de datos de Oracle:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado para la restauración, si hay.
- Tiene un equipo de destino válido para la reconstrucción completa.
- Se ha creado el Live CD del Agente de Arcserve UDP (Linux) (Linux).
- Si desea realizar una reconstrucción completa mediante la dirección IP, se deberá obtener la dirección IP del equipo de destino mediante Live CD.
- Si desea realizar una reconstrucción completa de PXE mediante la dirección MAC, se debe disponer de la dirección MAC del equipo de destino.
- La base de datos de Oracle almacena todos los archivos relacionados con la base de datos (archivos de datos, registros de rehacer, registros de archivado, pfile, spfile, copias de seguridad) en ext2, ext3, ext4 y ReiserFS. La base de datos no reconoce el Sistema de Archivo de Clúster Oracle (OCFS/OCFS2), los discos sin formato ni los sistemas de archivos de Gestión de almacenamiento automático (ASM).
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Restauración del servidor de Oracle

Si el servidor de Oracle se corrompe, se puede restaurar el servidor entero a través de una reconstrucción completa.

Siga estos pasos:

1. Inicie sesión en la consola del servidor de copia de seguridad de Linux como usuario raíz.
2. Realice una reconstrucción completa mediante el asistente de restauración. Para obtener más información sobre el proceso de restauración, consulte Cómo realizar una reconstrucción completa (BMR) para los equipos de Linux.
3. Después de finalizar la tarea de reconstrucción completa, inicie sesión en el equipo de destino y verifique que se ha restaurado la base de datos.

El servidor de Oracle se ha recuperado correctamente.

Destino de memoria no admitido en el servidor de Oracle restaurado

Síntoma:

He realizado una reconstrucción completa de un servidor de Oracle. El tamaño de memoria del equipo de destino es menor que el servidor de Oracle de origen y la base de datos de Oracle utiliza AMM (Gestión de memoria automática). Después de la reconstrucción completa, siempre que inicio la instancia de la base de datos de Oracle, obtengo el error siguiente:

SQL> startup

ORA-00845: MEMORY_TARGET not supported on this system

Solución:

Para resolver este error, aumente el tamaño del sistema de archivos virtuales de memoria compartida.

Siga estos pasos:

1. Inicie sesión en el servidor de destino como usuario raíz.
2. Abra el símbolo del sistema y verifique el tamaño del sistema de archivos virtuales de memoria compartida.

   ```
   # df -k /dev/shm
   Filesystem           1K-blocks      Used Available Use% Mounted on
   tmpfs                   510324        88    510236   1% /dev/shm
   ```

3. Introduzca el comando siguiente y especifique el tamaño obligatorio de la memoria compartida:

   ```
   # mount -o remount,size=1200m /dev/shm
   ```

4. Vaya a la carpeta /etc/fstab y actualice el valor de configuración de tmpfs:

   ```
   tmpfs /dev/shm tmpfs size=1200m 0 0
   ```

Nota: El tamaño del sistema de archivos virtuales de memoria compartida debería tener el tamaño suficiente para alojar los
valores MEMORY_TARGET y MEMORY_MAX_TARGET . Para obtener más información sobre las variables, consulte la documentación de Oracle.

Realización de una recuperación instantánea de una base de datos de Oracle

Se puede recuperar instantáneamente una base de datos de Oracle sin realizar una reconstrucción completa. Se puede recuperar la base de datos mediante comandos específicos de la línea de comandos.

Revisión de los requisitos previos

Revise los requisitos previos siguientes antes de restaurar la base de datos de Oracle:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado para la restauración, si hay.
- Se deberá acceder a las sesiones de copia de seguridad localmente en el nodo de destino. Si la ubicación de la sesión está en el volumen local del nodo de destino, utilice la ruta exacta del directorio como la ubicación de la sesión. Si la ubicación de la sesión está en un recurso compartido de la red, primero monte el recurso compartido de la red en un punto de montaje local y, a continuación, utilice la ruta del punto de montaje como la ubicación de la sesión.
- Los volúmenes de destino que desee restaurar no pueden ser un volumen raíz y deben estar desmontados a través del comando umount.

  Por ejemplo: umount /dev/sda1
- El volumen de destino debe ser igual o mayor que el volumen de origen.
- La base de datos de Oracle almacena todos los archivos relacionados con la base de datos (archivos de datos, registros de rehacer, registros de archivado, pfile, spfile, copias de seguridad) en ext2, ext3, ext4 y ReiserFS. La base de datos no reconoce el Sistema de Archivo de Clúster Oracle (OCFS/OCFS2), los discos sin formato ni los sistemas de archivos de Gestión de almacenamiento automático (ASM).
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Restauración instantánea de la base de datos

Cuando se recupera la base de datos de manera instantánea, la base de datos estará disponible para su uso inmediato. Sin embargo, el proceso de recuperación se ejecuta en el servidor backend y todos los archivos estarán disponibles solamente después de la recuperación total de la base de datos.

Nota: Para obtener más información sobre la restauración de volúmenes, consulte Cómo restaurar volúmenes en un nodo de destino.

Siga estos pasos:

1. Inicie sesión en el servidor de destino como usuario raíz.
2. Abra un símbolo del sistema como usuario raíz.
3. Verifique que el volumen de destino /dev/sdb1 no esté montado.
   `# df | grep 'target_volume'`

   Por ejemplo: # df | grep '/dev/sdb1'
4. Monte el recurso compartido de NFS remoto a la ruta local.
   `#mount <ruta_sesión_nfs>:/nfs  <ubicación_sesión-en_local>`

   Por ejemplo: #mount xxx.xxx.xxx.xxx:/nfs /CRE_ROOT
5. Introduzca el siguiente comando para iniciar la tarea de restauración:
   ```
   #. /d2drestorevol --command=restore --storage-path=<ubicación_sesión_en_local>
   --node=<servidor_oracle> --rp=last
   --source-volume=<punto_montaje_para_volumen_datos_oracle>
   --target-volume=<nombre_volumen_destino_restauración>
   --mount-target=<punto_montaje_para_volumen_datos_oracle> --quick-recovery
   ```

   Ejemplo: #. /d2drestorevol --command=restore --storage-path=/CRE_ROOT --node=rh63-v2 --rp=last --source-volume=/opt/oracle --target-volume=/dev/sdb1 --mount-target=/opt/oracle --quick-recovery

   Se puede iniciar la base de datos de Oracle inmediatamente después de iniciar la tarea de restauración. No es necesario esperar que finalice la recuperación de la base de datos.
6. Abra otro símbolo del sistema e inicie sesión con el nombre de usuario y la contraseña de Oracle.
   ```
   $sqlplus / as sysdba
   SQL>startup;
   ```

   La base de datos Oracle se abre y se podrán realizar las operaciones habituales en relación con la base de datos, como: la consulta, inserción, supresión, actualización de datos, entre otros.

La base de datos Oracle se ha recuperado de manera instantánea.

Realización de una recuperación granular de una base de datos de Oracle

Se pueden restaurar archivos específicos relacionados con la base de datos de Oracle. Estos archivos pueden ser archivos de control o archivos de datos de espacios de tablas.

Revisión de los requisitos previos

Revise los requisitos previos siguientes antes de restaurar la base de datos de Oracle:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado, si hay.
- Tiene un nodo de destino válido para la recuperación de datos.
- Ha verificado que el servidor de copia de seguridad de Linux sea compatible con el sistema de archivos que desee restaurar.
- La base de datos de Oracle almacena todos los archivos relacionados con la base de datos (archivos de datos, registros de rehacer, registros de archivado, pfile, spfile, copias de seguridad) en ext2, ext3, ext4 y ReiserFS. La base de datos no reconoce el Sistema de Archivo de Clúster Oracle (OCFS/OCFS2), los discos sin formato ni los sistemas de archivos de Gestión de almacenamiento automático (ASM).
- Revise la matriz de compatibilidad que proporciona los sistemas operativos, bases de datos y exploradores.

Restauración de los espacios de tablas

Si un espacio de tabla de base de datos se pierde o se corrompe, este se podrá restaurar a través de una recuperación de nivel de archivos. Si la recuperación de nivel de archivos es correcta, se deberá recuperar el espacio de tablas manualmente.

Siga estos pasos:

1. Inicie sesión en el servidor de destino como usuario raíz.
2. Asegúrese de que la base de datos esté disponible.

3. Seleccione el espacio de tablas necesario fuera de conexión.

   Ejemplo: Tenga en cuenta que el nombre del espacio de tablas es MYTEST_DB. Introduzca el comando siguiente para capturar el espacio de tablas fuera de conexión:

   ```
   $ sqlplus "/ as sysdba"
   SQL> alter tablespace MYTEST_DB offline;
   ```

4. Enumere todos los archivos de datos para el espacio de tablas denominado MYTEST_DB.

   ```
   SQL> select file_name, tablespace_name from dba_data_files where
   tablespace_name='MYTEST_DB';

   FILE_NAME

   ------------------------------------------------------------------------------
   ---

   TABLESPACE_NAME

   ------------------------------

   /opt/oracle/oradata/lynx/MYTEST_DATA01.dbf

   MYTEST_DB
   ```

5. Restaure los archivos de datos de los espacios de tablas mediante el Asistente de restauración. Para obtener más información sobre el proceso de restauración, consulte Cómo realizar una recuperación a nivel de archivo en nodos de Linux.

6. Especifique la información siguiente acerca del Asistente de restauración y envíe la tarea:

   a. Cuando se seleccionan los archivos y carpetas, introduzca el nombre del archivo de datos obligatorio del espacio de tablas y realice la búsqueda.

      Ejemplo: Introduzca MYTEST_DATA01.dbf del espacio de tablas MYTEST_DB y realice la búsqueda.

   b. En la página Equipo de destino, introduzca la información siguiente:

      - Seleccione Restaurar en la ubicación original.
      - Introduzca el nombre de host o la dirección IP del servidor de Oracle de destino.
      - Introduzca el nombre de usuario raíz y la contraseña del servidor de Oracle de destino.
      - Seleccione Sobrescribir archivos existentes para la opción Resolución de conflictos.

7. Después de la restauración del archivo de datos, recupere el espacio de tablas de la base de datos de Oracle.

```
SQL>recover tablespace MYTEST_DB;
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
Auto
```

8. Establezca el espacio de tablas especificado en línea.

```
SQL>alter tablespace MYTEST_DB online;
```

El espacio de tablas se ha recuperado correctamente.

Restauración de archivos de control

Si los archivos de control de la base de datos se pierden o se corrompen, estos podrán restaurarse a través de una recuperación de nivel de archivos. Si la recuperación de nivel de archivos es correcta, se deberán recuperar los archivos de control de la base de datos manualmente.

Siga estos pasos:

1. Inicie sesión en el servidor de destino como usuario raíz.
2. Cierre la instancia de Oracle.

```
SQL>shutdown abort
```

3. Inicie la base de datos en el estado nomount.

```
SQL>startup nomount
```

4. Muestre la ruta para todos los archivos de control.

```
SQL> show parameter control_files;
NAME                                 TYPE        VALUE
------------------------------------ -----------
------------------------------
control_files               string    /opt/oracle/oradata/lynx/control01.ctl,
/opt/oracle/flash_recovery_area/lynx/control02.ctl
```

5. Restaure los archivos de control mediante el Asistente de restauración. Para obtener más información sobre el proceso de restauración, consulte Cómo realizar una recuperación a nivel de archivo en nodos de Linux.

6. Especifique la información siguiente acerca del Asistente de restauración y envíe la tarea:

   a. Cuando se seleccionan los archivos y carpetas, introduzca el nombre obligatorio del archivo de control y realice la búsqueda. Repita este paso hasta que todos los archivos de control estén seleccionados.

      Por ejemplo: introduzca control01.ctl y realice la búsqueda.

   b. En la página Equipo de destino, introduzca la información siguiente:

      - Seleccione Restaurar en la ubicación original.
      - Introduzca el nombre de host o la dirección IP del servidor de Oracle de destino.
      - Introduzca el nombre de usuario raíz y la contraseña del servidor de Oracle de destino.
      - Seleccione Sobrescribir archivos existentes para la opción Resolución de conflictos.

7. Después de restaurar todos los archivos de control, monte la base de datos y ábrala.

   ```
   $sqlplus / as sysdba
   SQL>alter database mount;
   ```

8. Recupere la base de datos con el comando RECOVER y agregue la cláusula USING BACKUP CONTROLFILE.

   ```
   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE
   ```

9. Aplique los registros archivados solicitados.

   Nota: Si falta el registro archivado obligatorio, esto implica que un registro de rehacer necesario se encuentra en los registros de rehacer en línea. Esto ocurre porque se encuentran cambios no archivados en los registros en línea cuando se produce un error en la instancia. Se puede especificar la ruta completa de un archivo de registro de rehacer en línea. A continuación, pulse Intro (es posible que tenga que intentar realizar este proceso unas cuantas veces hasta localizar el registro correcto).

   Ejemplo:

   ```
   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE
   ORA-00279: change 1035184 generated at 27/05/14 18:12:49 needed for thread 1
   ORA-00289: suggestion :
   /opt/oracle/flash_recovery_area/LYNX/archivelog/2014_05_27/o1_mf_1_6_%u_.arc
   ORA-00280: change 1035184 for thread 1 is in sequence #6
   Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
   /opt/oracle/oradata/lynx/redo03.log
   Log applied.
   La recuperación de medios se ha completado.
   ```

10. Abra la base de datos con la cláusula RESETLOGS después de finalizar el proceso de recuperación.

    ```
    SQL>alter database open resetlogs;
    ```

Los archivos de control se han recuperado correctamente.

Capítulo 5: Solución de problemas

Esta sección contiene los siguientes temas:

Se produce un error en el Agente de Arcserve UDP (Linux) al instalarlo en servidores compatibles

Válido en CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, Suse Linux Enterprise Server (SLES) 11.x y el servidor de Oracle Linux 6.x

Síntoma

Cuando instalo el Agente de Arcserve UDP (Linux), se produce un error de instalación con los siguientes mensajes de advertencia de Linux:

```
mkisofs         Crear imagen de Live CD

mount.nfs               Montar el sistema de archivos del recurso compartido de NFS
como destino de la copia de seguridad y como origen de restauración.

mount.cifs              Montar el sistema de archivos del recurso compartido de CIFS
como destino de la copia de seguridad y como origen de restauración.

Los siguientes procesos deben estar en ejecución

Procesos inactivos              Función afectada

rpc.statd               La función de bloqueo del archivo de NFS no funciona,
```

Solución

Al inicio de la instalación, el Agente de Arcserve UDP (Linux) verifica si el SO de Linux cumple el requisito del servidor de copia de seguridad. Si el SO de Linux no cumple los requisitos mínimos, el Agente de Arcserve UDP (Linux) mostrará un mensaje de advertencia para informar de este problema. El mensaje incluye la lista de todos los paquetes que se requieren para el servidor de copia de seguridad.

Para solucionar este problema de instalación del Agente de Arcserve UDP (Linux), realice los pasos siguientes:

1. Instale los siguientes paquetes usando el comando *yum:*
   - genisoimage
   - nfs-utils
   - cifs-utils

2. Ejecute los dos comandos siguientes:

   ```
   service rpcbind start
   ```

   ```
   inicio del servicio nfs
   ```

3. Ejecute el siguiente comando para verificar si se está ejecutando *rpc.statd*:

   ```
   ps -ef|grep rpc.statd
   ```

4. Reinstale el Agente de Arcserve UDP (Linux).

El Agente de Arcserve UDP (Linux) se ha instalado correctamente.

El Agente de Arcserve UDP (Linux) muestra un error de tiempo de espera excedido en la operación

Válido en CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, Suse Linux Enterprise Server (SLES) 11.x y el servidor de Oracle Linux 6.x

Síntoma

Obtengo el mensaje de error siguiente:

Se ha agotado el tiempo de espera de la operación. Se ha superado la cantidad máxima de tiempo para completar la operación. Inténtelo de nuevo más tarde.

Obtengo este mensaje cuando realizo una restauración de nivel de archivo y exploro puntos de recuperación que tienen más de 1000 puntos de recuperación incrementales.

Solución

El valor del tiempo de espera predeterminado es de 3 minutos. Se puede solucionar el problema aumentando el valor del tiempo de espera.

Realice los pasos siguientes para aumentar el valor del tiempo de espera:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Agregue la siguiente variable de entorno del sistema:

   ```
   D2D_WEBSVR_TIMEOUT
   ```

   El valor para la variable de entorno es un número. El número debe ser mayor que 3. La unidad para el valor es el minuto.

3. Reinicie el servidor de copia de seguridad.

El valor del tiempo de espera ha aumentado correctamente.

Se produce un error en todas las tareas programadas cuando la hora del sistema se cambia a un valor ya transferido

Válido en CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, Suse Linux Enterprise Server (SLES) 11.x y el servidor de Oracle Linux 6.x

Síntoma

Cuando cambio la hora del sistema a un valor ya transferido, todas mis tareas programadas quedan afectadas. Las tareas programadas producen un error al ejecutarse después de cambiar la hora del sistema a una hora anterior.

Solución

Después de cambiar la hora del sistema, reinicie el servicio de BACKUP.

Siga estos pasos para reiniciar el servicio de BACKUP:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Vaya a la carpeta bin

   ```
   /opt/CA/d2dserver/bin/
   ```

3. Reinicie el servidor de copia de seguridad utilizando el siguiente comando:

   ```
   d2dserver restart
   ```

   El servidor de copia de seguridad se reinicia.

Todas las tareas programadas se ejecutan de acuerdo con lo programado.

Se produce un error en el Agente de Arcserve UDP (Linux) al montar dispositivos de RAID del software de Linux

Válido en CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, Suse Linux Enterprise Server (SLES) 11.x y el servidor de Oracle Linux 6.x

Síntoma

A veces se produce un error en el proceso de reconstrucción completa (BMR) al montar dispositivos RAID de software de Linux después de que el equipo de destino se reinicie.

Solución

Para resolver este problema, reinicie el equipo de destino.

Un equipo paravirtual (PVM) muestra una pantalla negra en la ventana del cliente del entorno de red virtual (VNC) mediante Live CD

Válido en PVM en el servidor de la máquina virtual de Oracle

Síntoma

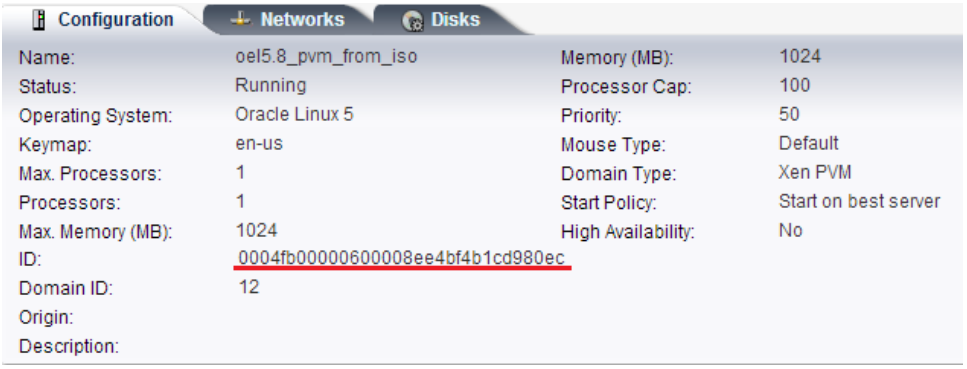
En un servidor de la máquina virtual de Oracle, cuando inicio el equipo paravirtual (PVM) mediante Live CD, veo una pantalla negra en la ventana del cliente de VNC.

Solución

Para resolver esta incidencia, inicie sesión en la consola de Live CD desde el back-end.

Siga estos pasos:

1. Inicie la máquina virtual mediante Live CD.
2. Tome nota del ID de la máquina virtual a la cual se puede acceder desde el gestor de la máquina virtual de Oracle.



3. Inicie sesión en el servidor de la máquina virtual de Oracle en el cual se ejecuta la máquina virtual mediante la shell segura (SSH).
4. Ejecute el comando *xm console $ID* como aparece en el diagrama siguiente:

```
[root@                ~]# xm console 0004fb00000600008ee4bf4b1cd980ec
```

5. (Opcional) Pulse Intro cuando se solicite confirmar la operación.
6. La consola de PVM de Xen que se reinicia al abrir Live CD.
7. Configure la red.
8. Salga de la consola pulsando ctrl+] o ctrl+5.

La incidencia se resuelve.

Cómo ajustar la secuencia de arranque de disco después de una tarea de BMR en un servidor de máquina virtual de Oracle

Válido en el servidor de la máquina virtual de Oracle

Síntoma

Cuando realizo una tarea de BMR en un nodo de destino en un servidor de la máquina virtual de Oracle, obtengo el mensaje de advertencia siguiente en el registro de actividades:

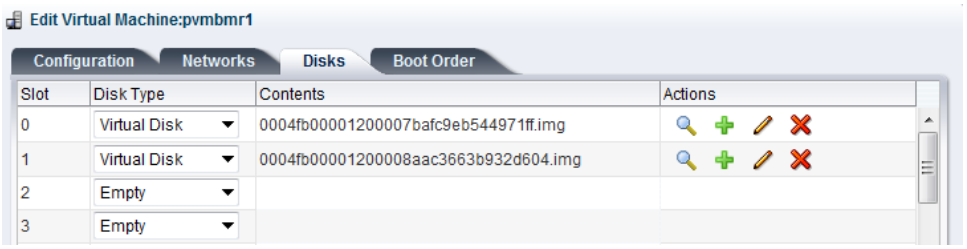
`El volumen de inicio se restaura en el disco /dev/xxx. Ajuste la secuencia de arranque de disco en BIOS para iniciar /dev/xxx.`

Solución

Para evitar este problema, intercambie la secuencia de arranque de disco del nodo de destino de BMR.

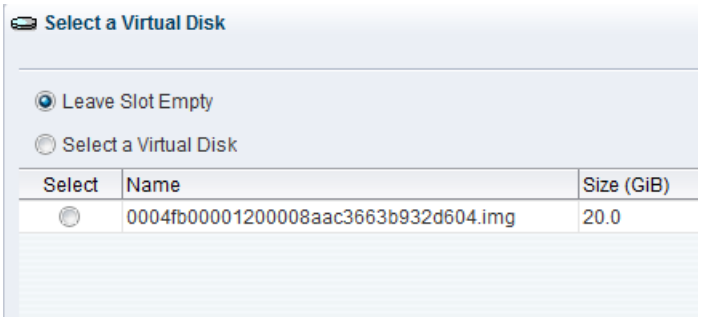
Siga estos pasos:

1. Edite el nodo de destino de BMR desde el Gestor de la máquina virtual de Oracle y haga clic en la ficha Disks.

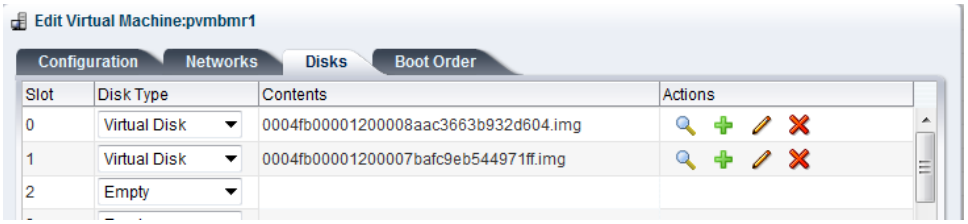


2. Seleccione Slot N como el disco de arranque.
3. Haga una nota del nombre de disco y el número de ranura N.

   Utilizará el nombre de disco y el número de ranura en los pasos posteriores.
4. En la columna Actions, seleccione el botón Virtual Machine Disk.
5. Seleccione la opción Leave Slot Empty y haga clic en Save.



6. Seleccione Slot 0 Disk y tome nota del nombre de disco.
7. En la columna Actions, seleccione el botón Virtual Machine Disk.
8. Seleccione la opción Leave Slot Empty y haga clic en Save.
9. Adjunte la imagen de disco de arranque seleccionada a Slot 0 y la Imagen Slot 0 Disk a Slot N.



10. Inicie el nodo de destino de BMR.

La secuencia de arranque del disco se ha ajustado correctamente.

Se produce un error en la tarea de copia de seguridad al recopilar la información relacionada con BMR o se produce un error en la tarea de BMR al crear un diseño de disco

Válido en el servidor de máquina virtual de Oracle para HVM con el volumen de LVM

Síntoma

Cuando realizo una tarea de copia de seguridad para un HVM con volúmenes de LVM en un servidor de máquina virtual de Oracle, se produce un error en la tarea de copia de seguridad al recopilar la información relacionada con BMR. También, cuando realizo una tarea de BMR para un HVM con volúmenes de LVM en un servidor de máquina virtual de Oracle, se produce un error en la tarea de BMR al crear el diseño de disco.

Solución

Para resolver esta incidencia, desactive los controladores de PV para el nodo de origen de copia de seguridad.

Siga estos pasos:

1. Abra la ventana Símbolo del sistema en el nodo de origen de copia de seguridad e introduzca el siguiente comando:

   ```
   sfdisk –s
   ```

2. Verifique si el mismo disco se muestra dos veces en el resultado.

   Por ejemplo, xvdX y hdX son el mismo disco. Verifique si estos dos discos se muestran en el resultado.

3. En caso afirmativo, realice los pasos siguientes:

   a. Agregue la línea siguiente al archivo */etc/modprobe.d/blacklist* en el nodo de origen de copia de seguridad:

      ```
      blacklist xen_vbd
      ```

   b. Reinicie el nodo de origen de copia de seguridad y vuelva a ejecutar la tarea de copia de seguridad.

      Se ejecuta la tarea de copia de seguridad.

4. En caso negativo, póngase en contacto con el equipo de Soporte de CA.

La incidencia se resuelve.

El rendimiento de la lectura de la copia de seguridad es menor cuando el nodo de la copia de seguridad es RHEL, CentOS u Oracle Linux 5.x en un servidor Xen de PVM

Válido en Red Hat Enterprise Linux (RHEL), CentOS, Suse Linux Enterprise Server (SLES) 11.x y el servidor de Oracle Linux 6.x en una máquina virtual paralela de Xen

Síntoma

Cuando realizo una copia de seguridad de RHEL, CentOS, SLES, o de un servidor de Oracle Linux 6.x en un PVM de Xen, el valor de rendimiento de lectura de la copia de seguridad será menor.

Solución

Para resolver esta incidencia, configure el programador de entrada/salida de disco (E/S) de la máquina virtual.

Siga estos pasos:

1. Abra la ventana Símbolo del sistema en el nodo de origen de la copia de seguridad.
2. Ejecute el comando siguiente para identificar el número de discos de los que dispone la máquina virtual:

   ```
   ls /dev/xvd*
   ```
3. Ejecute el comando siguiente para identificar el algoritmo del programador de E/S de los discos:

   ```
   cat /sys/block/xvda/queue/scheduler
   ```

   Aparece el resultado siguiente en la máquina virtual:

   ```
   [noop] anticipatory deadline cfq
   ```
4. Ejecute el comando siguiente para cambiar el programador de E/S a cfq:

   ```
   echo "cfq" > /sys/block/xvda/queue/scheduler
   ```
5. Verifique de nuevo el programador de E/S.

   Aparece el resultado siguiente en la máquina virtual:

   ```
   noop anticipatory deadline [cfq]
   ```
6. Cambie el programador de E/S para todos los discos.
7. Vuelva a ejecutar la tarea de copia de seguridad

La tarea de copia de seguridad se ejecuta con un rendimiento óptimo de lectura de la copia de seguridad.

Cómo restaurar la versión anterior del servidor de copia de seguridad

Válido en Red Hat Enterprise Linux (RHEL) 6.x y en CentOS 6.x para el servidor de copia de seguridad

Síntoma

He intentado actualizar el servidor de copia de seguridad pero se ha producido un error durante la actualización. El servidor de copia de seguridad no funciona como se esperaba. Ahora deseo restaurar la versión anterior del servidor de copia de seguridad.

Solución

Cuando se actualiza a una versión nueva, el servidor de copia de seguridad crea una carpeta de copia de seguridad que contiene todos los archivos de configuración viejos y los archivos de base de datos de la versión que se ha instalado previamente. La carpeta se genera en la ubicación siguiente:

```
/opt/CA/d2dserver.bak
```

Siga estos pasos:

1. Desinstale el servidor de copia de seguridad existente utilizando el siguiente comando:

   ```
   /opt/CA/d2dserver/bin/d2duninstall
   ```

2. Instale la versión que se ha instalado previamente del servidor de copia de seguridad.
3. Detenga el servidor de copia de seguridad utilizando el siguiente comando:

   ```
   /opt/CA/d2dserver/bin/d2dserver stop
   ```

4. Copie los archivos de configuración viejos y los archivos de base de datos en la carpeta de d2dserver mediante el comando siguiente:

   ```
   cp –Rpf /opt/CA/d2dserver.bak/* /opt/CA/d2dserver/
   ```

5. Inicie el servidor de copia de seguridad utilizando el siguiente comando:

   ```
   /opt/CA/d2dserver/bin/d2dserver start
   ```

La versión instalada previamente del servidor de copia de seguridad se ha restaurado correctamente.

SLES 10.X no se inicia correctamente después de una reconstrucción completa

Válido en SUSE Linux Enterprise Server (SLES) 10.X para BMR en equipos de destino viejos

Síntoma:

Cuando realizo una reconstrucción completa mediante los puntos de recuperación de SLES 10.x en un equipo de destino viejo, la reconstrucción completa será correcta pero el equipo de destino no se iniciará correctamente. También, en el caso de tener puntos de recuperación de un equipo de origen viejo de SLES 10.x si intento realizar una reconstrucción completa, esta será correcta pero el equipo de destino no se iniciará correctamente.

En ambos casos, obtendré el siguiente mensaje de error:

```
Ningún sistema operativo
```

Solución:

Modifique el MBR del disco de arranque en un entorno de Live CD y reinicie el equipo de destino.

Siga estos pasos:

1. Inicie sesión en el equipo de destino mediante un Live CD y busque el disco de arranque.

   Ejemplo: /dev/sda

2. Ejecute el siguiente comando:

   ```
   echo -en "\\x90\\x90"|dd of=/dev/sda seek=156  bs=1
   ```

3. Reinicie el equipo de destino y verifique si el equipo de destino se reinicia correctamente.

El equipo de destino de SLES 10.x se inicia correctamente después de una reconstrucción completa.

Las tareas de d2drestorevm y d2dverify producen un error en el servidor de la máquina virtual de Oracle

Válido en el servidor de la máquina virtual de Oracle

Síntoma

Cuando inicio las tareas de d2drestorevm y d2dverify en un servidor de la máquina virtual de Oracle, se producirá un error en todas las tareas. Obtengo el mensaje de error siguiente en el registro de actividades:

```
Se ha producido un error al importar la imagen ISO al hipervisor. Para
obtener más información, compruebe la consola de gestión del
hipervisor o el registro de depuración.
```

Solución

Verifique si el servidor de la máquina virtual de Oracle responde.

Siga estos pasos:

1. Inicie sesión en la consola del servidor de la máquina virtual de Oracle y vaya a la ficha Tareas.
2. Localice todas las tareas que estén en el estado En curso y, a continuación, anúlelas.
3. Inicie de nuevo la tarea de d2drestorevm o d2dverify.

   Si se produce un error en la tarea de d2drestorevm o d2dverify de nuevo y aparece el mismo mensaje de error, inicie sesión en la consola del servidor de la máquina virtual de Oracle y compruebe si hay tareas cuyo estado sea En curso. Si hay tareas cuyo estado sea En curso, reinicie el servidor de la máquina virtual de Oracle.

Las tareas de d2drestorevm y d2dverify se ejecutan correctamente.

Error en el inicio de la máquina virtual de ESXi después de la reconstrucción completa de una máquina física

Síntoma:

Realizo una reconstrucción completa mediante los puntos de recuperación de una máquina física a una máquina virtual de ESXi. El equipo físico utiliza un BIOS más antiguo. La reconstrucción completa es correcta pero la máquina virtual ESXi no se inicia correctamente.

Solución:

Modifique el tipo de controlador de SCSI de la máquina virtual ESXi de destino y envíe la tarea de reconstrucción completa de nuevo.

Siga estos pasos:

1. Inicie sesión en el servidor de ESX.
2. Haga clic con el botón secundario del ratón en la máquina virtual ESXi de destino y seleccione Editar configuración.
3. En la ficha Hardware, seleccione el controlador de SCSI 0 y haga clic en el botón Cambiar tipo.

   Aparece el cuadro de diálogo Change SCSI Controller Type (Cambiar el tipo de controlador de SCSI).
4. Seleccione LSI Logic SAS y guarde la configuración.
5. Envíe una tarea de reconstrucción completa a esta máquina virtual.

La máquina virtual se inicia correctamente después de la tarea de reconstrucción completa.