Guía del usuario del Agente para Linux

Arcserve® Unified Data Protection

Versión 10.0

arcserve®

Tabla de contenido

Ponerse en contacto con Soporte de Arcserve

El equipo de Soporte de Arcserve

Contacto con Soporte técnico

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 base de conocimiento 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.

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

Esta sección incluye los siguientes temas:

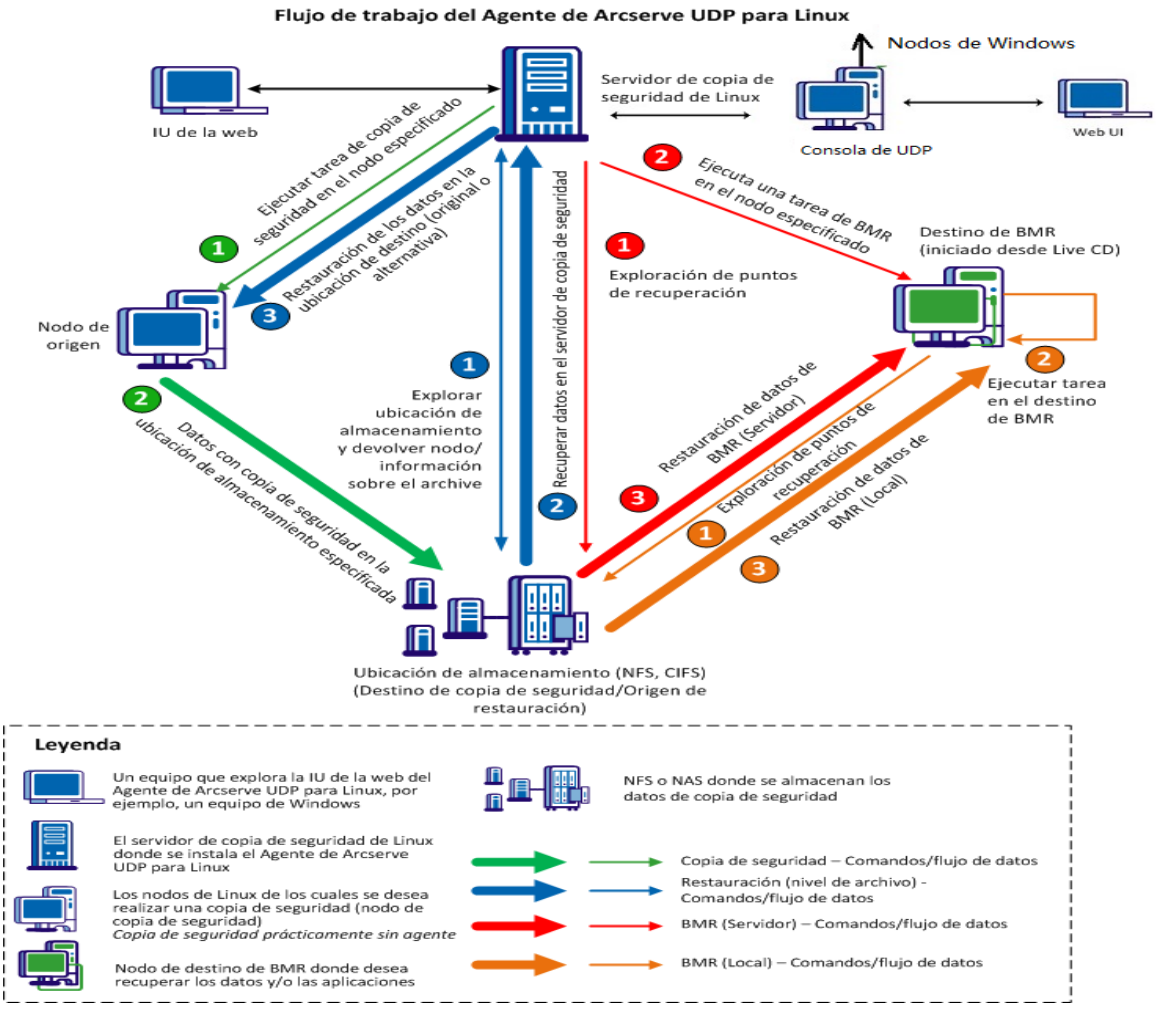
Introducción

Arcserve UDP 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. 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, lo que reduce el tamaño de cada copia de seguridad incremental (y de la ventana de copia de seguridad) y proporciona copias de seguridad más actualizadas. 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 mientras se realiza una copia de seguridad de los datos, Agente de Arcserve UDP (Linux) 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.

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
Nodos de Windows
Servidor de copia de seguridad de Linux
IU de la web
Consola de UDP
Web UI
Ejecutar tarea de copia de seguridad en el nodo especificado
Restauración de los datos en la ubicación de destino (original o alternativa)
Ejecuta una tarea de BMR en el nodo especificado
Destino de BMR (iniciado desde Live CD)
Exploración de puntos de recuperación
Nodo de origen
Explorar ubicación de almacenamiento y devolver nodo/ información sobre el archive
Recuperar datos en el servidor de copia de seguridad
Restauración de datos de BMR (Servidor)
Exploración de puntos de recuperación
Restauración de datos de BMR (Local)
Ejecutar tarea en el destino de BMR
Datos con copia de seguridad en la ubicación de almacenamiento especificada
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
NFS o NAS donde se almacenan los datos de copia de seguridad
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
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 incluye 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.

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

- Consideraciones sobre la instalación
- Instalación del Agente de Arcserve UDP (Linux)
- Instalación del Agente de Arcserve UDP (Linux) en la nube de AWS
- Verificación de la instalación

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 Arcserve UDP 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 NFS, verifique que el servidor NFS admite el *bloqueo*. También, verifique que el usuario raíz tenga 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.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.
- No se admite la instalación silenciosa o desatendida.

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.

Notas:

- Asegúrese de que el servidor de Linux tenga una memoria mínima de 2 GB. Para obtener más información sobre los requisitos del sistema para un servidor de Linux, consulte las Notas de la versión de Arcserve UDP 10.0.
- Utilice sudo para instalar el servidor de Linux en Microsoft Azure.
- Para el sistema de Debian/Ubuntu, no se permite al usuario raíz iniciar sesión en ssh de forma predeterminada. Para conceder a los usuarios no raíz permisos para iniciar sesión en la interfaz de usuario del servidor de copia de

seguridad de Linux, consulte Concesión de permisos de inicio de sesión a los usuarios no raíz.

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) en la carpeta raíz.

   Importante: Cuando se descarga el archivo 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. Ejecute el siguiente comando para iniciar la instalación:

   ./<linux_installation_file_name>.bin

   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.

   Notas:

   - Si se detecta un sistema operativo que no esté en inglés, se pedirá que seleccione el idioma aplicable antes de continuar con el proceso de instalación.
   - Para ser compatible con el idioma coreano cuando se actualiza una compilación, realice los pasos siguientes:
     a. Modifique el archivo de configuración siguiente en el servidor del Agente de Arcserve UDP (Linux): */opt/Arcserve/d2dserver/nls/nls.cfg*
     b. set D2D_LANG= ko_KR.
     c. Reinicie d2dserver utilizando el siguiente comando: *#/opt/Arcserve/d2dserver/bin/d2dserver restart*.
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/Arcserve/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)
- 8016 (servicio de reconstrucción completa instantánea)
- 8021 (servicio de copia de seguridad)

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 de Linux y los nodos de destino de la reconstrucción completa.

Nota: Para obtener más información sobre los puertos, consulte Puertos de comunicación utilizados por Arcserve UDP.

7. (Opcional) Para instalar el servidor de copia de seguridad de Linux en una máquina virtual de Amazon EC2 o Azure, realice los pasos siguientes para crear un usuario de D2D:

   Nota: Cuando el servidor se inicia, un mensaje le pedirá crear un usuario de D2D que se utilizará para iniciar sesión en la interfaz de usuario web del Agente de Arcserve UDP (Linux).

   a. Introduzca un nombre de usuario para crearlo.

   b. Establezca la contraseña y confírmela volviéndola a especificar.

c. Seleccione si se desea que la cuenta de usuario sea el usuario de inicio de sesión de forma predeterminada para la interfaz de usuario web del Agente de Arcserve UDP (Linux)

   Valor predeterminado: S (Sí)

d. Decida el número de errores consecutivos de inicio de sesión antes de que se bloquee la cuenta de usuario.

   Valor predeterminado: 3

Se ha instalado el Agente de Arcserve UDP (Linux) correctamente.

Instalación del Agente de Arcserve UDP (Linux) en la nube de AWS

En comparación con una instalación tradicional en un equipo de Linux, se puede iniciar una instancia del Agente de Arcserve UDP (Linux) directamente utilizando Amazon Machine Image (AMI) en la nube de AWS. Después de iniciar la instancia del Agente de Arcserve UDP (Linux), se puede abrir la interfaz de usuario desde cualquier equipo mediante un explorador web; se hace referencia al servidor como servidor de copia de seguridad.

Siga estos pasos:

1. Inicie sesión en la consola de gestión de EC2 con su cuenta y seleccione Launch Instance (Iniciar instancia).

   Aparacerá el asistente para iniciar la instancia mostrando 7 fichas.

2. En la primera ficha **Choose AMI**, seleccione la AMI del Agente de Arcserve UDP (Linux) en **Community AMIs** para el paso **Step 1: Choose an amazon Machine Image (AMI)** y haga clic en **Next: Choose an Instance Type**.

   Se puede buscar la AMI del Agente de Arcserve UDP (Linux) utilizando *Arcserve_Unified_Data_Protection_Agent_Linux* en las AMI de la comunidad.

   Nota: Seleccione una AMI del Agente de Arcserve UDP (Linux) con la última versión para iniciar la instancia.

   Aparece la segunda ficha **Choose Instance Type**.

3. Seleccione un tipo de instancia en función de los requisitos para completar el paso **Step 2: Choose an Instance Type** y haga clic en **Next: Configure Instance Details**.

   Nota: Compruebe que el tipo de instancia sea al menos t2.medium y que tenga una memoria mínima de 4 GB. Para obtener más información sobre los requisitos del sistema para un servidor de Linux, consulte las Notas de la versión de Arcserve UDP 10.0: Mejoras del Agente de Linux.

   Aparece la tercera ficha **Configure Instance**.

4. Seleccione los detalles para los campos relacionados con la red, la subred y la asignación automática de la dirección IP pública entre otros para completar el paso **Step 3: Configure Instance details** y, a continuación, haga clic en **Next: Add Storage**.

   Aparece la cuarta ficha **Add Storage**.

5. Asigne el almacenamiento a la instancia para completar el paso **Step 4: Add Storage** y haga clic en **Next: Add Tags**.

Nota: Se puede ajustar el tamaño del disco basándose en las necesidades de su empresa. Compruebe que el disco de la instancia de Linux tenga un tamaño mínimo de 40 GB.

Aparece la quinta ficha **Add Tags**.

5. Introduzca etiquetas para que la instancia de destino de la AMI pueda completar el paso **Step 5: Add tags** y haga clic en **Next: Configure Security Group**.

   Aparece la sexta ficha **Configure Security Groups**.

6. Realice los pasos siguientes para asignar los grupos de seguridad a la instancia de destino de la AMI para completar el paso **Step 6: Configure the security group** y, a continuación, haga clic en **Review and Launch**:

   Siga estos pasos:

   a. Cree un nuevo grupo de seguridad para SSH y para el Agente de Arcserve UDP (Linux).

   b. Compruebe que el puerto 22 está activado para el **Tipo** *SSH* y configure el **Origen** con el valor *Anytime* (En cualquier lugar).

   c. Compruebe que el puerto 8014 utilizado por Tomcat está activado para *Custom TCP Rule* (Regla TCP personalizada) - **Tipo** y configure el **Origen** con el valor *Anywhere* (En cualquier lugar).

   d. Compruebe que el puerto 8016 utilizado por d2ddss y que el puerto 8021 utilizado por cresvc estén activados para Custom TCP Rule - **Type** y configure **Source** de la regla con el valor Custom.

      Nota: Se puede especificar el origen personalizado con el formato CIDR para permitir que d2ddss y cresvc gestionen las instancias de Linux que se encuentran en la misma subred con el Agente de Arcserve UDP (Linux), pero que no están accesibles para otros equipos de Internet. Por ejemplo, si la subred CIDR es 102.31.16.0/20, también se puede especificar el origen en 102.31.16.0/20.

   Aparece la séptima ficha **Review**.

7. Verifique los detalles seleccionando o creando un par de clave para conectarse a la instancia para completar el paso **Step 7: Review Instance Launch** y, a continuación, haga clic en **Launch Instance**.

8. En la instancia iniciada del Agente de Arcserve UDP (Linux), establezca una nueva contraseña para udpuser como se muestra a continuación:

   ```
   #sudo /opt/Arcserve/d2dserver/bin/d2duser --action=passwd --username=udpuser
   ```

Nota: El nombre de usuario predeterminado de la interfaz de usuario de gestión del Agente de Arcserve UDP (Linux) es udpuser.

9. (Opcional) Si se desea cambiar a otro idioma, se puede modificar el archivo de configuración en el servidor del Agente de Arcserve UDP (Linux):

   /opt/Arcserve/d2dserver/nls/nls.cfg

   Y, a continuación, establezca D2D_LANG=$OTHER_LANGUAGE y reinicie d2dserver con el comando que se muestra a continuación:

   #/opt/Arcserve/d2dserver/bin/d2dserver restart

   Nota: El idioma predeterminado es el inglés para el Agente de Arcserve UDP (Linux).

   Ahora, el Agente de Arcserve UDP (Linux) está listo para poder ser utilizado en la nube de AWS y la dirección URL para buscar el servidor de copia de seguridad de Linux es https://$INSTANCE_IP:8014.

   El Agente de Arcserve UDP (Linux) se ha instalado correctamente en la nube de AWS.

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 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):

- Revisión de las consideraciones sobre la desinstalación
- Desinstalación de Agente de Arcserve UDP (Linux)
- Verificación de la desinstalación

Revisión de las consideraciones sobre la 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.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Desinstalación de Agente de Arcserve UDP (Linux)

Se puede desinstalar el Agente de Arcserve UDP (Linux) desde 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 Arcserve UDP para Linux está instalado con el comando siguiente:

   ```
   # cd /opt/Arcserve/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/Arcserve/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
- Actualización del Agente de Arcserve UDP (Linux)
- Verificación de la actualización

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, las bases de datos y los exploradores compatibles.

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 (por ejemplo, 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) en la carpeta raíz.

   Importante: Cuando se descarga el archivo 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. Ejecute el siguiente comando para iniciar la instalación:

   ```
   ./<nombre_archivo_instalación_Linux>.bin
   ```

   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.

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/Arcserve/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/Arcserve/d2dserver.bak`

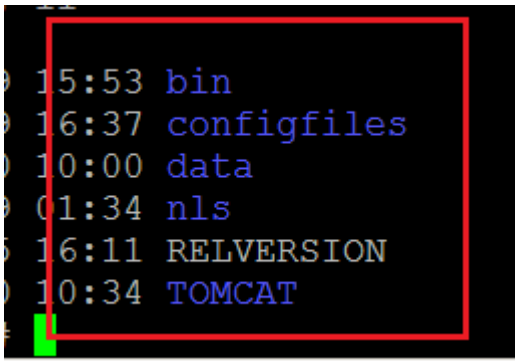
   El Agente de Arcserve UDP (Linux) se ha actualizado y verificado correctamente.

Cómo migrar el servidor de copia de seguridad de Linux de 32 bits a un servidor de 64 bits

A partir de la versión 6, el Agente de Arcserve UDP (Linux) no será compatible con un servidor de 32 bits para el servidor de copia de seguridad de Linux. Para utilizar el Agente de Arcserve UDP (Linux) versión 6, migre el servidor de Linux de 32 bits a un servidor de Linux de 64 bits.

Siga estos pasos:

1. Reserve los siguientes archivos y carpetas en la carpeta de instalación del Agente de Arcserve UDP (Linux):



   Una carpeta de instalación típica para el Agente de Arcserve UDP (Linux) versión 5 era /opt/CA/d2dserver/.

   Nota: Si la carpeta TOMCAT es una carpeta de gran tamaño, reserve solo la carpeta TOMCAT/conf.

2. Copie los archivos y carpetas reservados en alguna otra ubicación, como '/opt/d2dserver_32bit/'.
3. Empaquete los archivos y carpetas reservados en la ubicación siguiente:

   ```
   tar -czf UDP_LINUX_AGENT.tar.gz /ultraconservative
   ```

4. Copie el archivo empaquetado del SO Linux de 32 bits al SO Linux de 64 bits utilizando scp o ftp.
5. Cree una carpeta nueva en el servidor del SO de 64 bits utilizando el siguiente comando:

   ```
   mkdir -p /opt/CA/d2dserver
   ```

6. Extraiga el archivo empaquetado en el SO Linux de 64 bits utilizando el siguiente comando:

```
tar -xzf UDP_LINUX_AGENT.tar.gz
```

7. Copie los archivos y carpetas reservados a la ubicación siguiente:

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

   Por ejemplo: cp -Rp /opt/d2dserver_32bit/* /opt/CA/d2dserver

8. Ejecute el paquete de instalación del Agente de Arcserve UDP (Linux) versión 6.0 en el servidor de Linux de 64 bits.
9. El servidor de copia de seguridad de Linux se actualiza automáticamente.

   Nota: Si se cambia el nombre de host o la dirección IP, consulte Configuración de los valores de configuración del sistema cuando se cambia el nombre de host o la dirección IP.

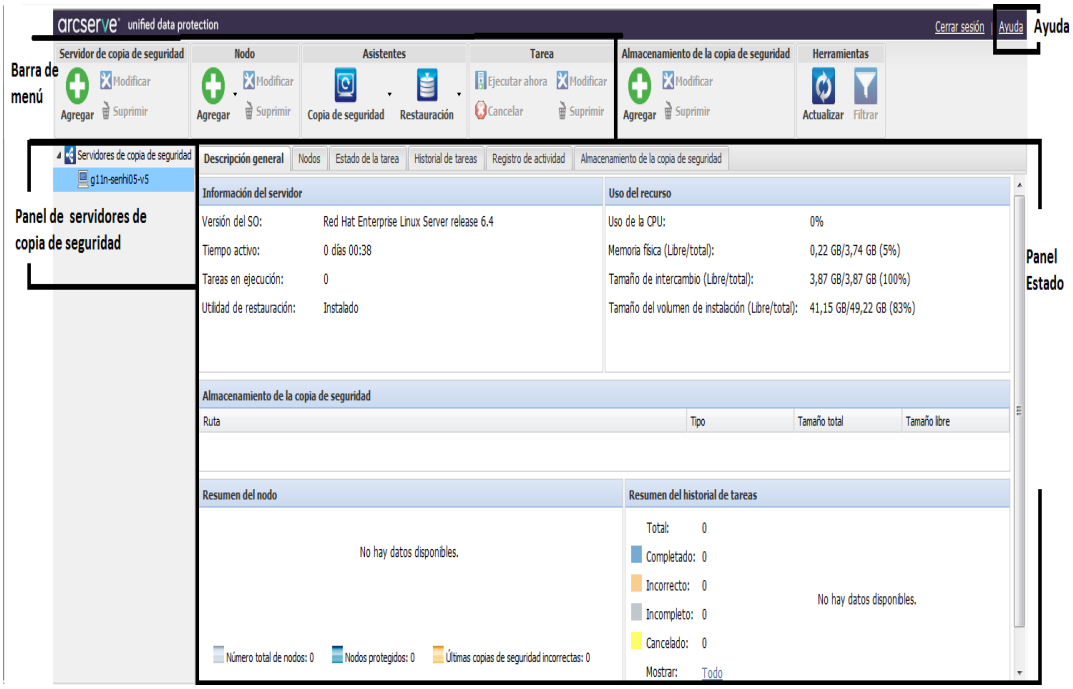
Capítulo 3: Interfaz de usuario

Esta sección incluye los siguientes temas:

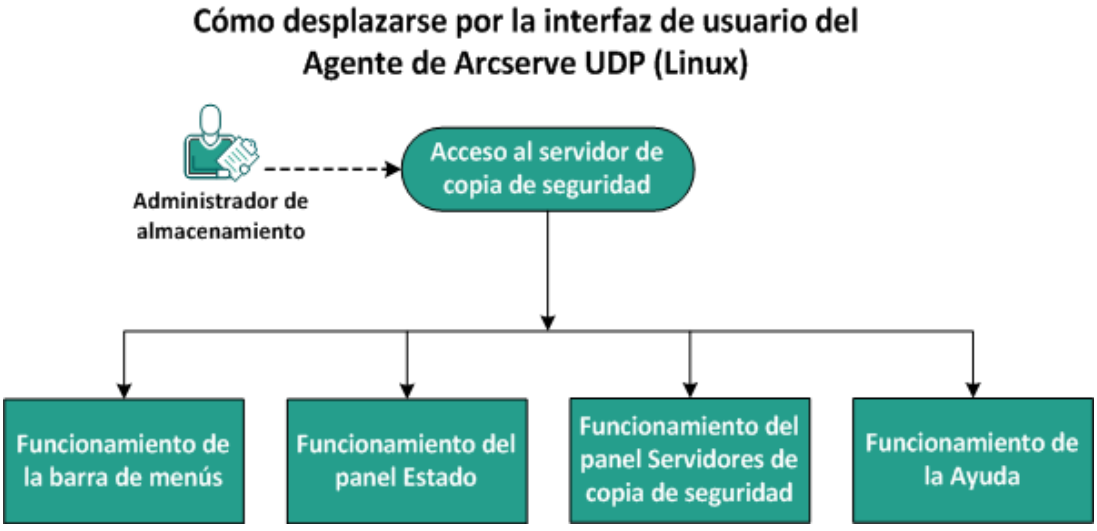
Cómo moverse por la interfaz de usuario del Agente de Arcserve UDP (Linux)

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
- Funcionamiento de la barra de menús
- Funcionamiento del panel Estado
- Funcionamiento del panel Servidores de copia de seguridad
- Funcionamiento de la Ayuda

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.

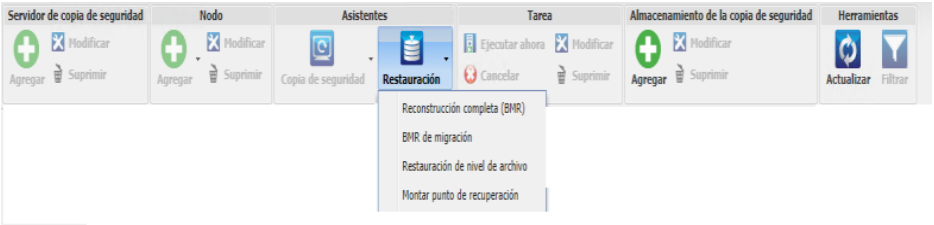
  Realizar la copia de seguridad de los nodos seleccionados

  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.

BMR de migración

Utilice esta opción para realizar la reconstrucción completa de migración.

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.

Montar punto de recuperación

Utilice esta opción para realizar un montaje de punto de recuperación. Un montaje de punto de recuperación puede compartir archivos en un punto de recuperación a través de NFS o WebDAV. Para acceder a estos archivos, monte la ubicación en el servidor de Linux.

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 una de las opciones siguientes: Recurso compartido de NFS, Recurso compartido de CIFS, Local o Servidor de puntos de recuperación.

Local es una ruta local en el servidor de copia de seguridad. Servidor de puntos de recuperación es el servidor de puntos de recuperación. El servidor de puntos de recuperación se instala cuando se instala Arcserve UDP. En el servidor de puntos de recuperación, se crean los almacenes de datos donde se almacenan los puntos de recuperación. Cuando se agrega un servidor de puntos de recuperación, también se debe especificar el almacén de datos.

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.

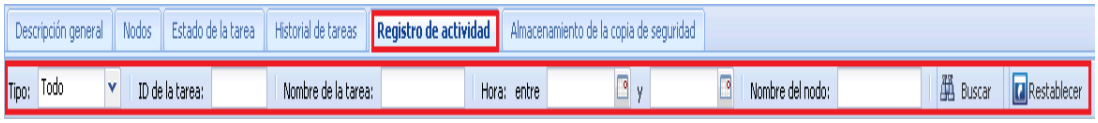
Actualizar

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.

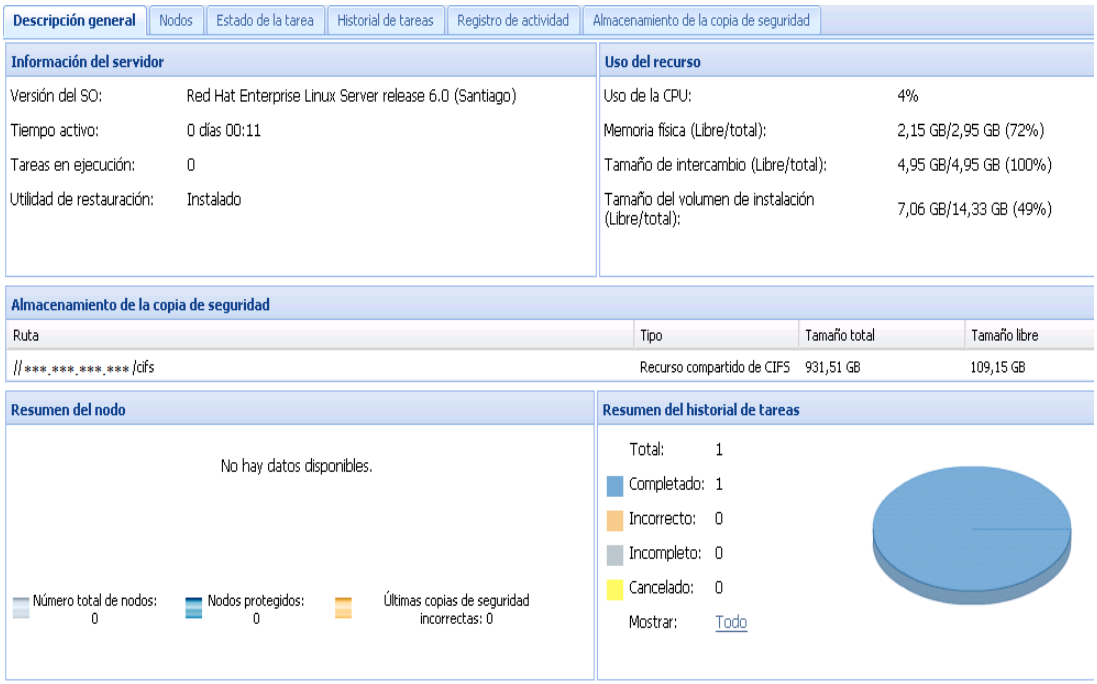
La siguiente pantalla muestra los filtros aplicados en el registro de actividad:



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.

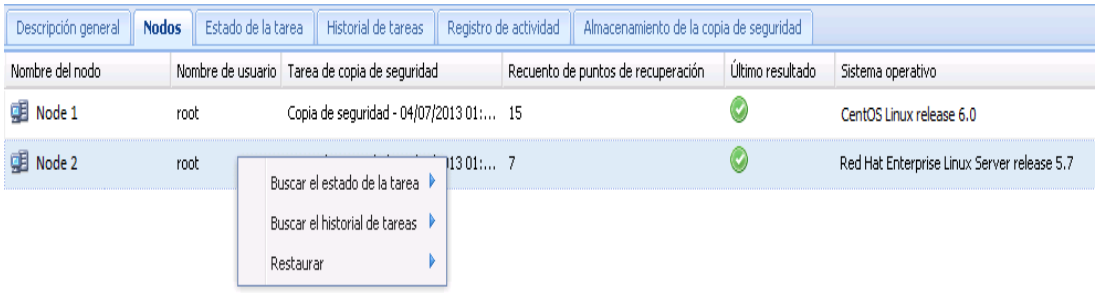
Los campos siguientes no son autoexplicativos:

- 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,

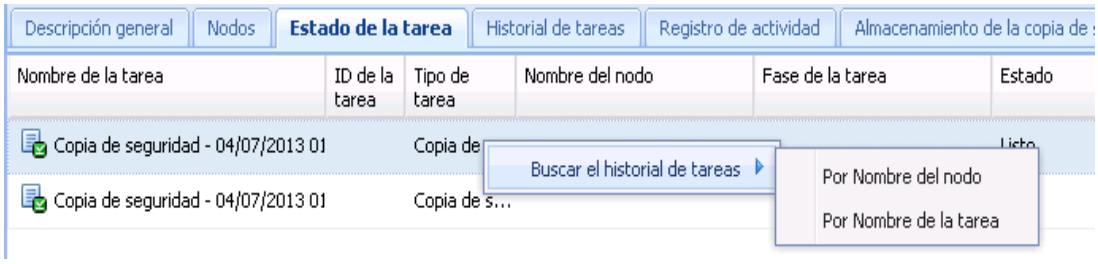
si se busca el estado de la tarea, a continuación se abrirá la ficha Estado de la tarea con el filtro de búsqueda aplicado en la ficha. La opción Restaurar permite realizar reconstrucciones completas o restauraciones de nivel de archivo. Se abre el Asistente de restauración y se muestra todos los puntos 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

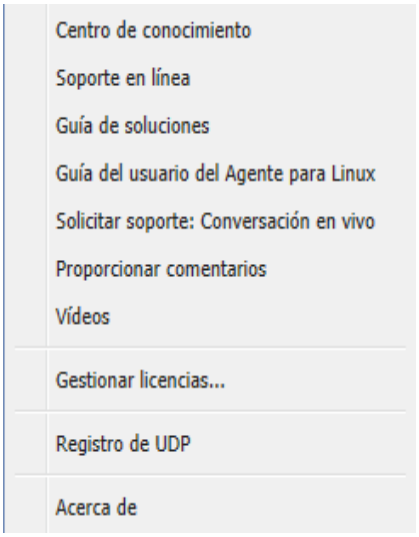
El panel Servidores de copia de seguridad muestra la lista de servidores de copia de seguridad que gestiona el servidor actual. Se pueden agregar servidores en la barra de menús y pueden gestionarse todos los servidores desde una interfaz. Si se han agregado varios servidores, el panel Estado mostrará 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 tareas siguientes en la lista desplegable Ayuda:



Las siguientes opciones están disponibles en la lista desplegable Ayuda:

Centro de conocimiento

Permite acceder a la biblioteca.

Soporte en línea

Permite acceder al sitio web de soporte de Arcserve.

Guía de soluciones

Permite acceder a la versión de HTML de la guía de soluciones del Agente de Arcserve Unified Data Protection para Linux.

Guía del usuario del Agente para Linux

Permite acceder a la versión de HTML de la guía del usuario.

Solicitar soporte: Conversación en vivo

Permite abrir una ventana de conversación en vivo y ponerse en contacto con un ejecutivo de soporte de Arcserve para una conversación en vivo.

Cómo proporcionar comentarios

Permite acceder al sitio web de soporte de Arcserve y proporcionar comentarios al equipo de desarrollo.

Vídeos

Permite acceder a tutoriales en línea y a vídeos relacionados con el Agente de Arcserve UDP (Linux).

Gestión de licencias

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

Programa de mejora del producto

Permite proporcionar sugerencias para mejorar el producto Arcserve.

Acerca de

Permite ver la información del producto (número de versión y de compilación) y acceder a las Notas de la versión del Agente de Arcserve Unified Data Protection para Linux.

Registro de Arcserve UDP

Después de instalar Arcserve UDP, se debe registrar el producto desde la consola. Este registro permite a Arcserve recopilar automáticamente los detalles y las estadísticas de uso de la consola.

Importante: Arcserve no recopila ninguna información crítica personal ni empresarial como, por ejemplo, el nombre del nodo, la dirección IP, las credenciales de inicio de sesión, el nombre del dominio y los nombres de red.

Si no se ha registrado la consola, se emitirá la notificación siguiente en la ficha **Mensajes** de la consola.

```
No se ha registrado la copia de Arcserve Unified Data Protection en el Programa de mejora del producto Arcserve. Registrar.
```

Siga estos pasos:

1. En la consola, haga clic en **Ayuda** y en **Programa de mejora del producto**.

   Se abrirá el cuadro de diálogo **Programa de mejora del producto de Arcserve**.

2. Seleccione la casilla de verificación **Participar en el programa de mejora del producto Arcserve**.
3. Especifique los siguientes detalles:

   Nombre

   Especifique el nombre.

   Empresa

   Especifique el nombre de la empresa.

   Número de teléfono

   Especifique el número de teléfono en el formato siguiente:

   Código del país - número de teléfono. Por ejemplo: 000-1122334455

   Dirección de correo electrónico

   Especifique la dirección de correo electrónico. Es un campo obligatorio. El correo electrónico de verificación se enviará a esta dirección de correo.

   Número de pedido

   Especifique el número de pedido. Se debe haber recibido este número en un correo electrónico al descargar Arcserve UDP.

4. Haga clic en **Enviar el correo electrónico de verificación**.

   El correo electrónico de verificación se envía a la dirección de correo electrónico que se ha mencionado en el cuadro de diálogo **Programa de mejora del producto de Arcserve**.

5. Inicie sesión en la cuenta de correo electrónico y abra el correo electrónico recibido.
6. Haga clic en el vínculo de verificación que aparece en él.

   Arcserve UDP se ha registrado correctamente.

   Después de que se haya registrado, se activa el botón Cancelar participación.

   Para cancelar el proceso de registro, haga clic en **Cancelar participación**.

   Si se desea actualizar la dirección de correo electrónico, se deberá volver a registrarse. Para registrarse de nuevo, siga el mismo proceso que se ha descrito en este tema.

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

Esta sección incluye 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 se desea implementar Arcserve UDP para Linux en ubicaciones remotas, se pueden 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
- Información general del cuadro de diálogo Gestión de licencias
- Gestión de licencias

Acceso 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.

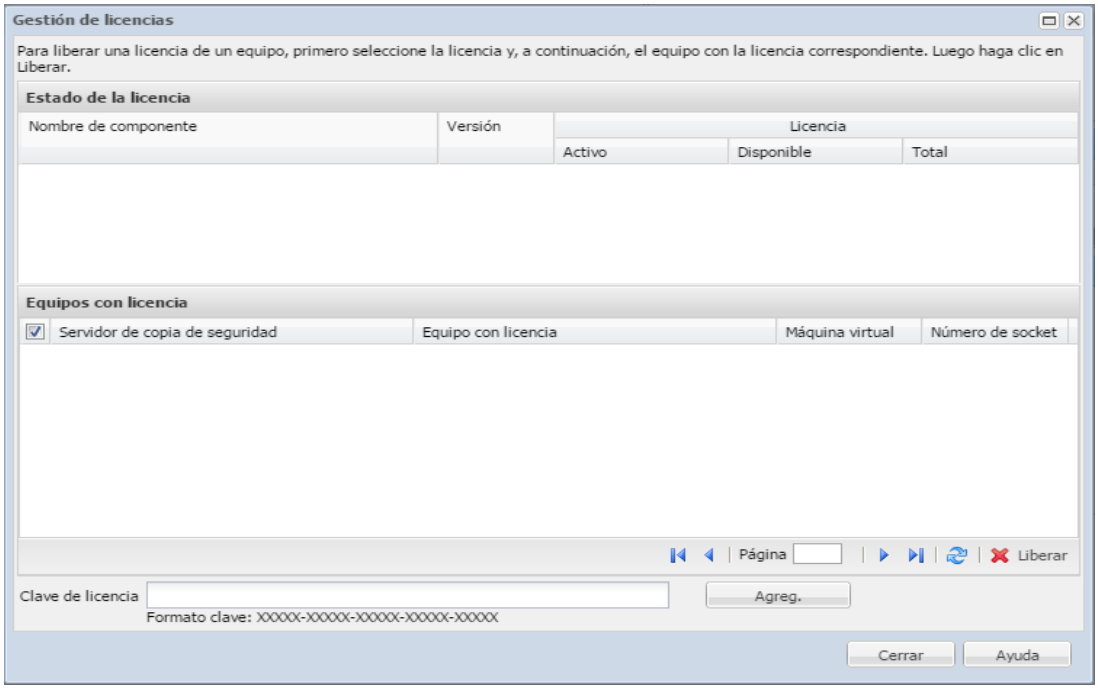
   Se abrirá el cuadro de diálogo Gestión de licencias.

   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 realizar la copia de seguridad de un equipo, se puede liberar la licencia de ese equipo.

Para agregar una licencia, siga estos pasos:

a. En el Portal de licencias de Arcserve genere la clave de licencia. Para obtener más detalles, consulte Cómo generar claves de licencia de Arcserve para agentes independientes.

b. Introduzca la clave de licencia en el campo Clave de licencia del cuadro de diálogo Gestión de licencias 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 Estado de la licencia del cuadro de diálogo Gestión de licencias.

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.

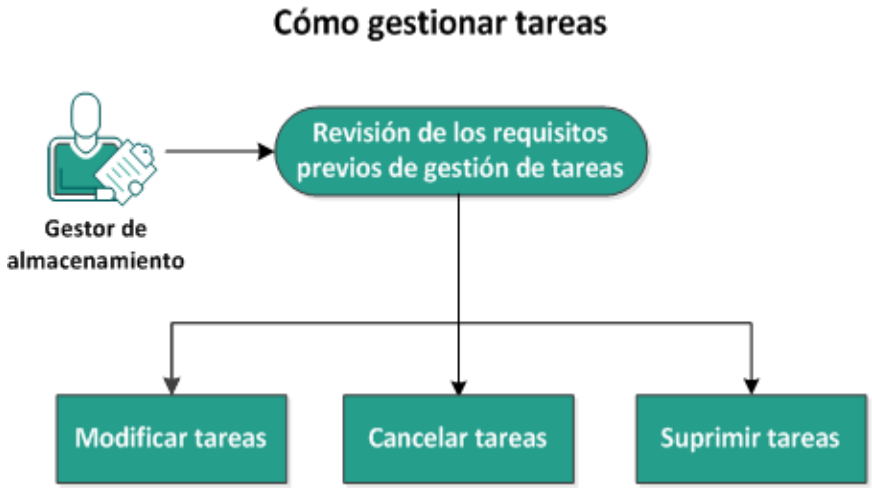
Las licencias se gestionan correctamente.

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
- Modificación de tareas
- Cancelación de tareas
- Supresión de tareas

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, las bases de datos y los exploradores compatibles.

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.

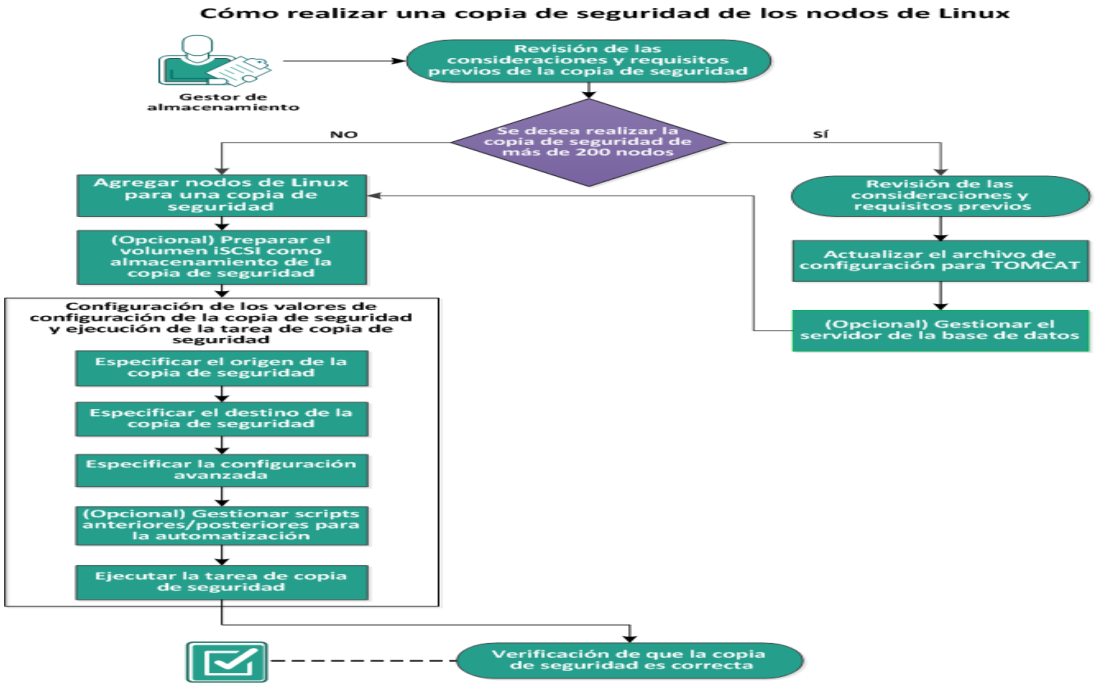
Cómo realizar una copia de seguridad de los nodos de Linux

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.

Nota: Si reinicia el nodo de origen de copia de seguridad, la siguiente copia de seguridad se convierte en una copia de seguridad de verificación (para la copia de seguridad de no deduplicación) o copia de seguridad completa (para la copia de seguridad de deduplicación).

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
- Se desea realizar la copia de seguridad de más de 200 nodos
  - Revisión de las consideraciones y los requisitos previos
  - Actualización del archivo de configuración de TOMCAT
  - Gestión del servidor de la base de datos
- Adición de nodos de Linux para una copia de seguridad
- (Opcional) Inscripción de la clave pública de Arcserve para el arranque seguro
- (Opcional) Preparación del volumen iSCSI 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
  - Especificación del origen de la copia de seguridad
  - Cómo especificar el destino de copia de seguridad
  - Especificación de la configuración avanzada
  - (Opcional) Gestión de scripts anteriores/posteriores para la automatización
  - Ejecución de la tarea de copia de seguridad
- Verificación de que la copia de seguridad es correcta

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 *Arcserve UDP 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.
- 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, las bases de datos y los exploradores compatibles.

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.

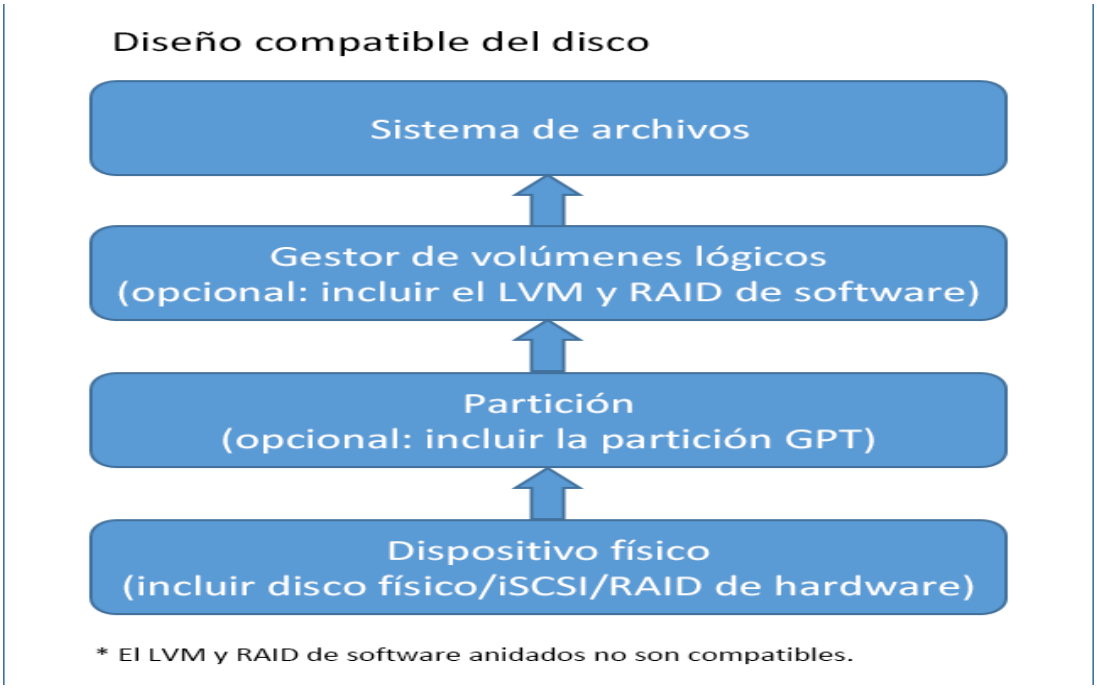
Revise las siguientes consideraciones de copia de seguridad:

- Para optimizar la gestión de los puntos de recuperación, debe tener en cuenta la recomendación siguiente 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).

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.

Diseño del disco compatible con el Agente de Arcserve UDP (Linux)

La siguiente ilustración muestra el diseño del disco compatible con el origen de copia de seguridad del Agente de Arcserve UDP (Linux):



Discos compatibles con 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
Volumen cifrado	No	No
Intercambio	No	No aplicable
Disco GPT:		
■ Disco de datos (tabla de particiones GUID) de GPT	Sí	Sí
■ Disco de arranque (tabla de particiones GUI) de GPT	Sí	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
■ XFS *3	Sí	Sí
■ Btrfs *4	Sí	Sí
Volumen compartido:		
■ Volumen compartido de Windows (Recurso compartido de CIFS)	No aplicable	Sí
■ Volumen de Linux compartido (Samba compartido)	No	Sí

■ Recurso compartido de NFS de Linux	No	Sí
Tipo de dispositivo:		
■ Disco extraíble (p. 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.	
*2	No se admite el LVM incrustado.	
*3	La restauración a nivel del archivo para una versión posterior de XFS no es compatible en un servidor de copia de seguridad de Linux que tenga una versión anterior de XFS. Por ejemplo, el realizar la restauración a nivel del archivo para XFS en RHEL7.X no admite RHEL6.x como servidor de copia de seguridad. Sin embargo, se puede utilizar el Live CD en su lugar como un servidor de copia de seguridad temporal para realizar la restauración a nivel del archivo. **Nota:** RedHat Enterprise Linux 8, CentOS 8 y Oracle Linux 8 tienen limitaciones que no son compatibles con la reconstrucción completa, la máquina virtual instantánea y la recuperación asegurada para el sistema de archivos XFS en la	

	compilación de Arcserve UDP 7.0 U1.
*4	La restauración a nivel de archivo para sistemas de archivos basados en btrfs (servidores SLES) no se admite en CentOS 8.0 y RHEL 8.0 LBS (servidor de copia de seguridad de Linux). No se admite la restauración a nivel del archivo en el equipo de origen (por ejemplo, instale el servidor de copia de seguridad de Linux en el equipo A, realice la copia de seguridad del equipo A, y, a continuación, ejecute la restauración desde el punto de recuperación en el equipo A). No se admite el filtro de archivo/carpeta. El proceso de limpieza/equilibrio del sistema de archivos se cancelará al principio de la copia de seguridad. Compatibilidad con BTRFS RAID: RAID-0 y RAID-1. Interfaz de usuario del filtro del volumen: Solo se muestra el volumen principal. No es una limitación, es el comportamiento esperado.

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 de TOMCAT

Cuando se actualiza el 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/Arcserve/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.

   ```
   /opt/Arcserve/d2dserver/TOMCAT/conf/
   ```

4. 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="TLSv1, TLSv1.1, TLSv1.2" 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.

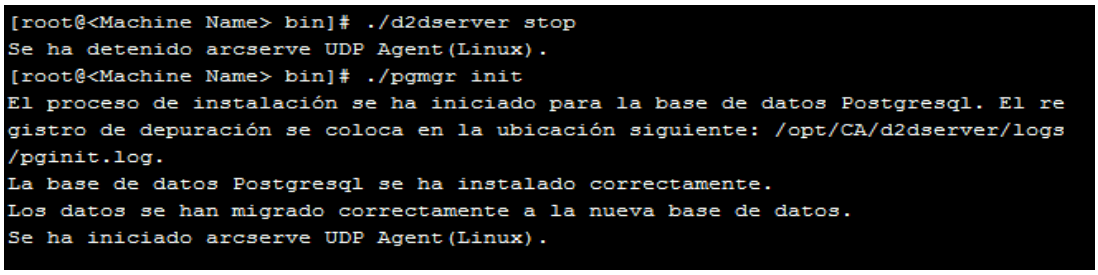
5. Detención del servidor de copia de seguridad.

   ```
   ./d2dserver stop
   ```

6. 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.



   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 contiene demasiados datos, la Consola del Agente de Arcserve UDP (Linux) tardará demasiado tiempo en cargar datos para el historial de tareas y el registro de actividad. Para mejorar la consulta de dato, consulte Mejora del rendimiento de las consultas para el historial de tareas y el registro de actividad.

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), ha recibido 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 sobre 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.

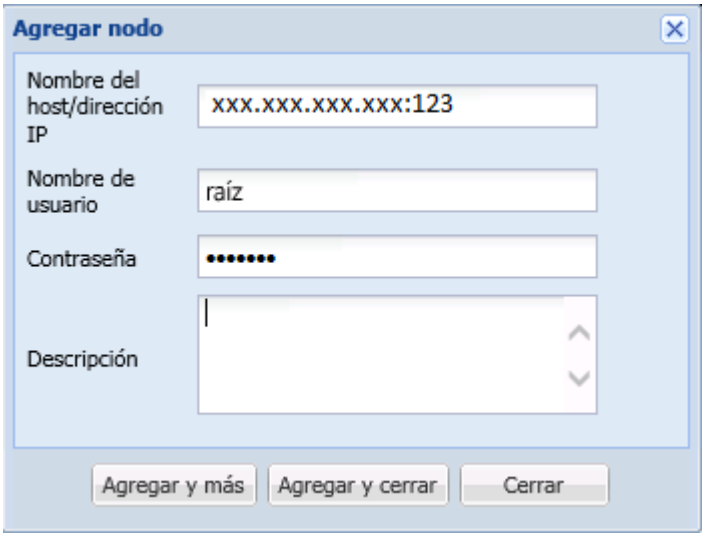
   b. Introduzca el nombre de host o la dirección IP del nodo de Linux, el nombre de usuario que tiene el permiso raíz y la contraseña.

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) Inscripción de la clave pública de Arcserve UDP para el arranque seguro

Cuando se está ejecutando en el arranque seguro, el nodo de origen de la copia de seguridad necesita una instalación manual de la clave pública de Arcserve para que el controlador de la copia de seguridad sea de confianza. Solo cuando se ha registrado la clave, la gestión de nodos y la función de la copia de seguridad funcionan correctamente. Este tema describe cómo inscribir la clave pública de Arcserve para el nodo con el arranque seguro activado.

Requisitos previos:

- Compruebe que dispone de derecho de acceso a la clave pública de Arcserve.
- Compruebe si su sistema tiene el paquete relacionado del archivo MokManager.efi o mmx64.efi que se encuentra en la siguiente carpeta:

  RedHat: carpeta /boot/efi/EFI/redhat

  CentOS: /boot/efi/EFI/centos

  Ubuntu: /boot/efi/EFI/ubuntu

  SLES: /boot/efi/EFI/SLES12

Siga estos pasos:

1. Inicie sesión en el entorno de shell del nodo de origen de copia de seguridad.
2. Busque la clave pública de Arcserve en la siguiente ubicación:

   `/tmp/arcserve_public_key_for_secureboot.der`
3. En el documento de la ejecución de la distribución de Linux para agregar la clave pública a la lista UEFI MOK, realice los pasos siguientes tal y como se explica en el ejemplo siguiente:
   a. Importe la certificación a MOK:

      mokutil [--root-pw] --import

      `/tmp/arcserve_public_key_for_secureboot.der`

      La opción --root-pw permite el uso del usuario root directamente. La contraseña root es necesaria para inscribir la clave después de reiniciar el sistema.

      Nota: En SLES15 SP2, utilice la siguiente clave pública al importar la certificación a MOK para las versiones de kernel de *linux-5.3.18-24.52* a *linux-5.14.21-150400.24.18*:

      `/tmp/arcserve_public_key_for_secureboot_v1.der`

b. Especifique una contraseña para la certificación cuando la opción --root-pw no esté disponible.

   Esta contraseña es necesaria para inscribir la clave después de reiniciar el sistema.

c. Verifique la lista de certificados que están preparados para inscribirse desde mokutil:

   mokutil --list-new>

   La lista debe tener una clave pública de Arcserve.

d. Reinicie el sistema.

   El sistema inicia la herramienta de gestión de claves de UEFI de shim.

   Nota: Si no se inicia la herramienta de gestión de claves de UEFI de shim, es posible que el sistema no tenga el archivo MokManager.efi.

e. Introduzca la contraseña que se ha especificado mientras se estaba importando la clave pública de Arcserve para inscribir la certificación a la lista MOK.

f. Compruebe si la clave recién importada aparece inscrita después de iniciar el sistema:

   mokutil --list-enrolled

   La lista debe tener una clave pública de Arcserve.

4. Agregue o vuelva a realizar la copia de seguridad del nodo para verificar que la clave pública Arcserve está inscrita correctamente.

   El nodo activado con el arranque seguro está preparado para ser protegido por el Agente de Arcserve UDP (Linux).

(Opcional) Inscripción de la clave pública de Arcserve UDP para el kernel de UEK6 de Oracle Linux activado con el arranque seguro

Esta sección proporciona información sobre cómo inscribir la clave pública de Arcserve para el kernel de UEK6 de Oracle Linux activado con el arranque seguro.

Requisitos previos:

- Compruebe que dispone de credenciales raíz.
- Compruebe que dispone de derecho de acceso a la clave pública de Arcserve.
- Compruebe que dispone de acceso al archivo de clave de la plataforma de Arcserve (PKCS12).
- Compruebe si el sistema tiene el paquete relacionado del archivo **mmx64.efi** que se encuentra en la siguiente carpeta:

  /boot/efi/EFI/redhat
- Instale los siguientes paquetes según sea necesario:
  - Oracle Linux 7.x
    - *sudo yum install kernel-uek-devel*
    - *sudo yum update*
    - *sudo yum-config-manager –enable ol7_optional_latest*
    - *sudo yum install keyutils mokutil pesign*
  - Oracle Linux 8.x
    - *sudo dnf install kernel-uek-devel*
    - *sudo dnf update*
    - *sudo dnf install keyutils mokutil pesign*

Siga estos pasos:

1. Inicie sesión en el entorno de shell del nodo de origen de copia de seguridad.
2. Localice la clave pública Arcserve en la ubicación siguiente:

   `/tmp/arcserve_public_key_for_secureboot.der`
3. Busque el archivo de clave de la plataforma de Arcserve (PKCS12) en la siguiente ubicación:

   `/tmp/arcserve_p12key_for_secureboot.p12`

4. En la documentación de Oracle Linux sobre cómo insertar el certificado del módulo en el kernel y sobre cómo firmar la imagen del kernel para el kernel de UEK6, siga estos pasos:

   a. Para cambiar al directorio donde existen los archivos de clave pública y de clave de la plataforma de Arcserve, ejecute el siguiente comando:

   ```
   # cd /tmp
   ```

   b. Para insertar el certificado del módulo en la imagen del kernel mediante la utilidad *insert-sys-cert*, ejecute el siguiente comando:

   ```
   # /usr/src/kernels/$(uname -r)/scripts/insert-sys-cert
   -s /boot/System.map-$(uname -r) -z /boot/vmlinuz-$(u-
   name -r) -c arcserve_public_key_for_secureboot.der
   ```

   c. Para configurar la base de datos de NSS, que está diseñada para almacenar el conjunto completo de claves, ejecute el siguiente comando:

   ```
   # certutil -d . -N

   Enter a password which will be used to encrypt your keys.
   The password should be at least 8 characters long,
   and should contain at least one non-alphabetic character.

   Enter new password:
   Re-enter password:
   ```

   Se le solicitará que introduzca una contraseña para la base de datos de NSS. Introduzca una contraseña para la base de datos, que se requiere al firmar el kernel.

   d. Agregue la versión de PKCS#12 de la clave de firma del kernel a la nueva base de datos. Primero se le solicitará la contraseña de la base de datos de NSS que se ha creado en el paso anterior y, a continuación, se le solicitará la contraseña, que se utilizará al exportar el archivo de clave PKCS#12 (cad2d es la contraseña utilizada para PKCS#12).

   # pk12util -d . -i arcserve_p12key_for_secureboot.p12

   ```
   Enter Password or Pin for "NSS Certificate DB":
   Enter password for PKCS12 file:
   pk12util: PKCS12 IMPORT SUCCESSFUL
   ```

   e. Firme la imagen del kernel mediante la utilidad pesign.

   ```
   # pesign -u 0 -i /boot/vmlinuz-$(uname -r) --remove-signature -o vmlinuz.unsigned
   # pesign -n . -c cert -i vmlinuz.unsigned -o vmlinuz.signed -s
   Enter Password or Pin for "NSS Certificate DB":

   # cp -bf vmlinuz.signed /boot/vmlinuz-$(uname -r)
   ```

5. Para actualizar la base de datos de MOK, siga estos pasos:
   a. Para importar la certificación a MOK, ejecute el siguiente comando:

      mokutil [--root-pw] --import

      /tmp/arcserve_public_key_for_secureboot.der

      La opción --root-pw permite el uso del usuario root directamente. La contraseña root es necesaria para inscribir la clave después de reiniciar el sistema.

   b. Especifique una contraseña para la certificación cuando la opción --root-pw no esté disponible.

      Esta contraseña es necesaria para inscribir la clave después de reiniciar el sistema.

   c. Verifique la lista de certificados que están preparados para inscribirse desde mokutil utilizando el siguiente comando:

      mokutil --list-new>

      La lista debe incluir la clave pública de Arcserve.

   d. Reinicie el sistema.

      El sistema inicia la herramienta de gestión de claves de UEFI de shim.

      Nota: Si no se inicia la herramienta de gestión de claves de UEFI de shim, es posible que el sistema no tenga el archivo *mmx64.efi*.

   e. Introduzca la contraseña que se ha especificado mientras se estaba importando la clave pública de Arcserve para inscribir la certificación a la lista MOK.
6. Para UEK R6, solo se confía en las claves que se enumeran en el conjunto de claves *builtin_trusted_keys* del kernel para la firma del módulo. Por esta razón, las claves de firma del módulo se agregan a la imagen del kernel como parte del proceso de firma de módulos. Ejecute el siguiente comando para validar que una clave es de confianza:

   # keyctl show %:.builtin_trusted_keys

   Conjunto de claves: *335047181 ---lswrv 0 0 keyring: .builtin_trusted_keys*

   1042239099 ---lswrv 0 0 _ asymmetric: Oracle CA Server: *58bd7ea9-c4fba3a4a62720d5d06f1e96053ddf4d*

   24285436 ---lswrv 0 0 _ asymmetric: Arcserve kernel module signing key: *fb4-c19dca60d31bb203499bf6cb384af6615699d*

   362335717 ---lswrv 0 0 _ asymmetric: Oracle America, Inc.: Ksplice Kernel Module Signing Key: *09010ebef5545fa7c54b626ef518e077b5b1ee4c*

448587676 ---lswrv 0 0 _ asymmetric: Oracle Linux Kernel Module Signing Key: *2bb352412969a3653f0eb6021763408ebb9bb5ab*

Notas:

- La lista debe incluir la clave pública de Arcserve.
- Si se instalan varios kernels de la versión de UEK, si se firma solo un kernel no se permitirá que los otros kernels inicien sesión. Por ejemplo, si se han instalado los kernels de UEK5 y UEK6, se ha importado una clave y se ha firmado el kernel de UEK6 mediante los pasos anteriores, se producirá un error en el arranque con el kernel de UEK5 en el arranque seguro.

El kernel de UEK6 de Oracle Linux activado con el arranque seguro está listo para la protección.

(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.

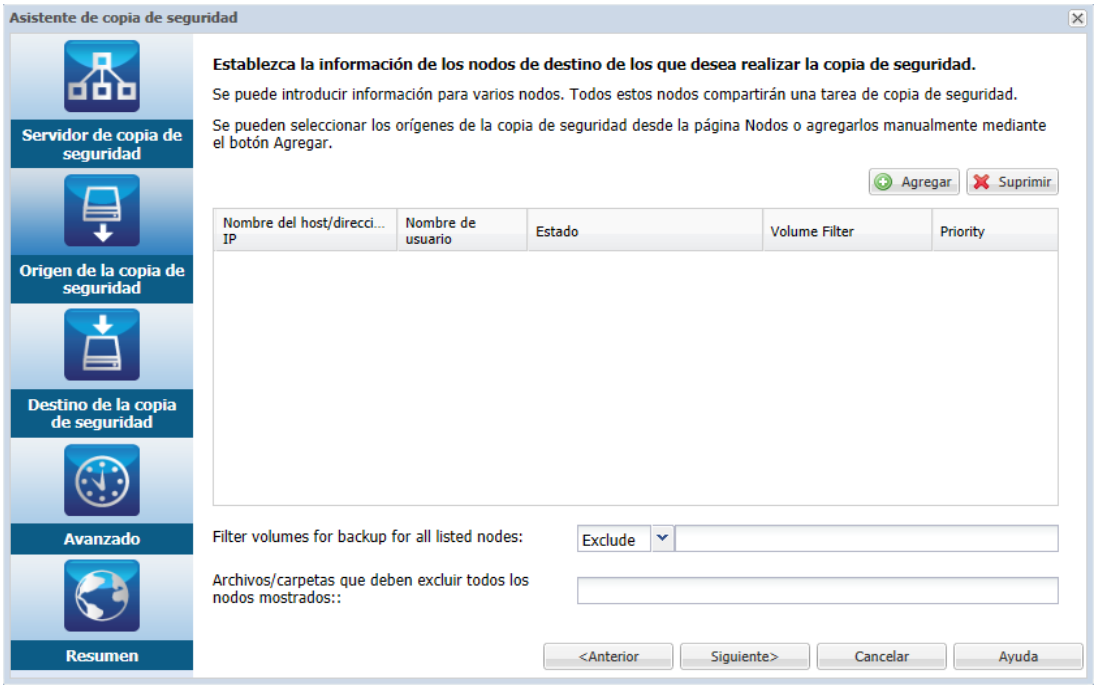
Nota: Si se abre el Asistente de copia de seguridad mediante el botón Realizar la copia de seguridad de los nodos seleccionados, aparecerán todos los nodos seleccionados en la página del asistente. Si se abre el Asistente de copia de seguridad mediante el botón Copia de seguridad, los nodos no aparecerán 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) Especifique los volúmenes en **Volúmenes para filtrar todos los nodos de la lista**.

   Seleccione Incluir o Excluir en la lista desplegable. Incluir especifica que se incluirán solo los volúmenes especificados para la copia de seguridad. No se realizará la copia de seguridad de cualquier volumen que no se haya especificado. Excluir especifica que los volúmenes se excluirán de la copia de seguridad.
6. (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.

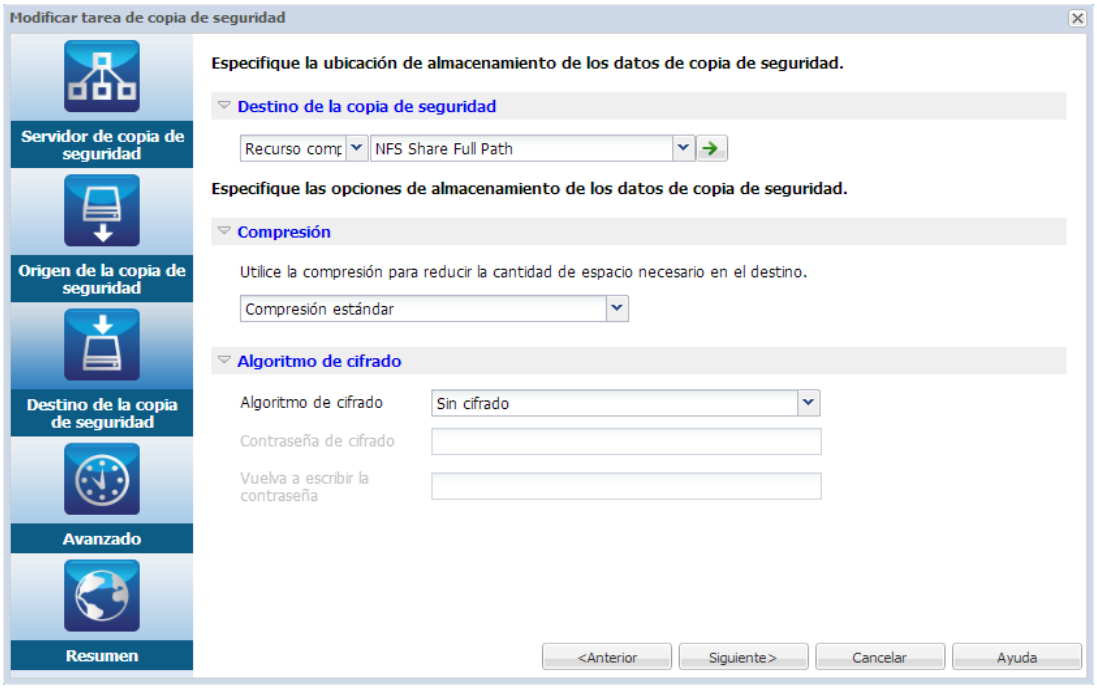
7. Haga clic en Siguiente.

   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

Se debe especificar una ubicación para almacenar los datos de la copia de seguridad (puntos de recuperación) en la página Destino de la 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 de Destino de la copia de seguridad en el formato siguiente:

```
Dirección_IP_recurso_compartido_NFS:/ruta_completa_ubi-
cación_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, especifique los detalles de Destino de copia de seguridad con el formato siguiente:

  ```
  //hostname/share_folder
  ```

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

- Si ha seleccionado Local, debe modificar algunos valores de configuración para que el servidor de copia de seguridad 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.

- Si se ha seleccionado Amazon S3, escriba los detalles del destino de la copia de seguridad en el formato siguiente:

  //ID_región_S3/Nombre_depósito_S3

  Notas:

  - //./ se puede utilizar como acceso directo para la cuenta global de la nube de Amazon. Por ejemplo, //./Nombre_depósito_global
  - //China/ puede utilizarse como acceso directo para cuenta China de la nube de Amazon. Por ejemplo, //China/Nombre_depósito_China
  - Si se desea exportar el depósito de Amazon S3 como un recurso compartido de CIFS, se puede hacer clic en la casilla de verificación Activar el acceso de cliente a CIFS. El puerto predeterminado es 8017.

    Esta función tiene el archivo de configuración siguiente:

    /opt/Arcserve/d2dserver/configfiles/ofs.cfg

    No modifique su contenido original. Se pueden agregar el siguiente contenido:

    - PROXY_HOST= (Si se desea utilizar el servidor proxy, introduzca el nombre del proxy aquí)
    - PROXY_USERNAME = (Nombre de usuario del servidor proxy)
    - PROXY_PASSWORD_ENC = (Contraseña del servidor proxy, debe estar cifrada)
    - PROXY_PORT = (Puerto del servidor proxy)
    - WRITE_THROUGHPUT = (Si se desea limitar el rendimiento de escritura, unidad: kB/s)
    - HTTPS = sí/no (el valor predeterminado es sí)
    - S3_STORAGE_CLASS = STANDARD/STANDARD_IA/REDUCED_REDUNDANCY (el valor predeterminado es STANDARD)
    - DEBUG_LEVEL = (nivel de registro de depuración: 0,1,2,3. 3 imprimirá la mayoría del registro)

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 datos a un formato ininteligible sin un mecanismo de descifrado. La protección de datos del Agente de Arcserve UDP (Linux) utiliza algoritmos de cifrado seguros AES (Advanced Encryption Standard) para 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.

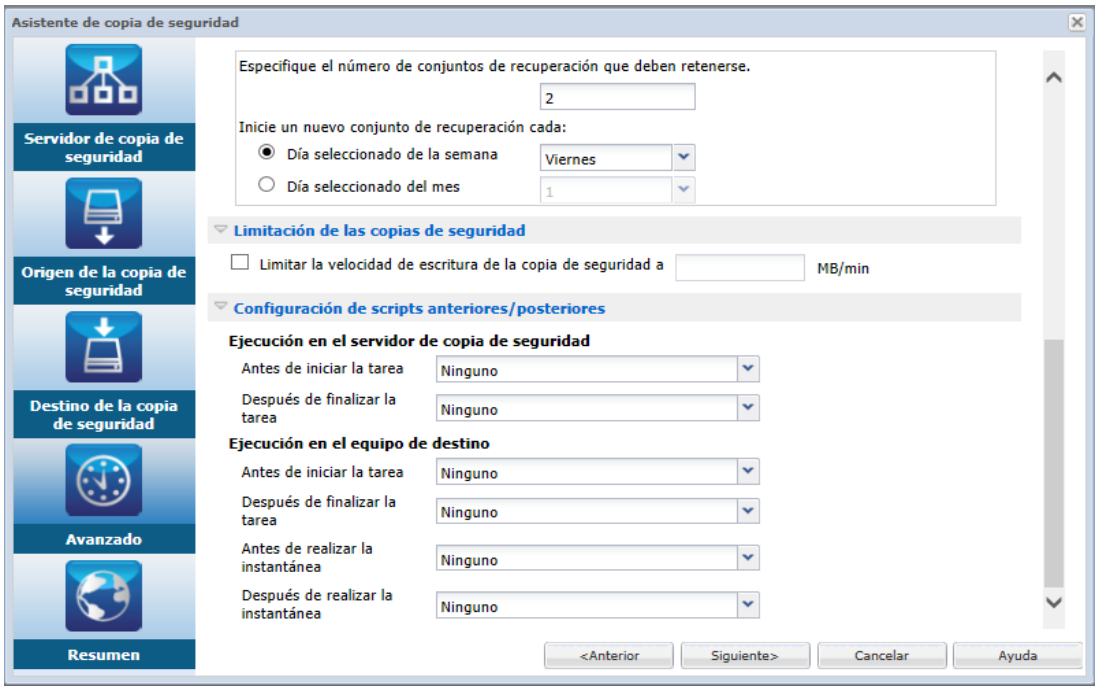
   Aparecerá la página Configuración avanzada.

   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.

  Importante: Establezca la misma zona horaria en el servidor de UDP y el servidor de copia de seguridad de Linux. Después de cambiar la zona horaria en ambos servidores, se debe reiniciar el servicio de gestión de UDP o el servidor de copia de seguridad de Linux para que se apliquen los cambios.

- 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:

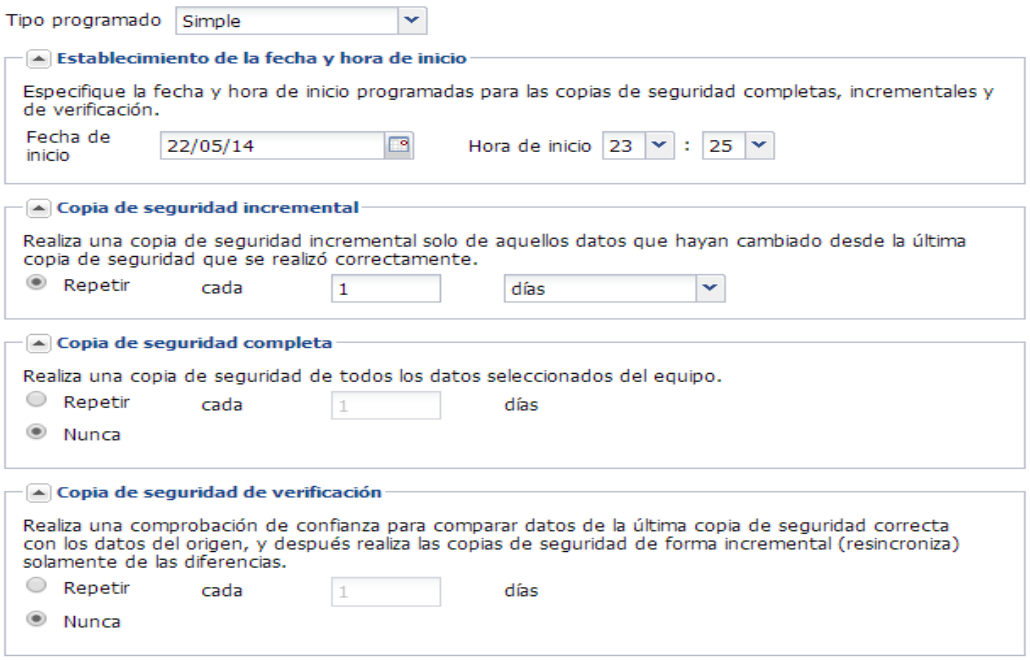
   Simple

   El tipo de programación **Simple** no está disponible cuando se crea una nueva programación. Sin embargo, si se modifica una tarea de copia de seguridad anterior que ya tiene una programación de tipo Simple, se puede configurar la programación 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.

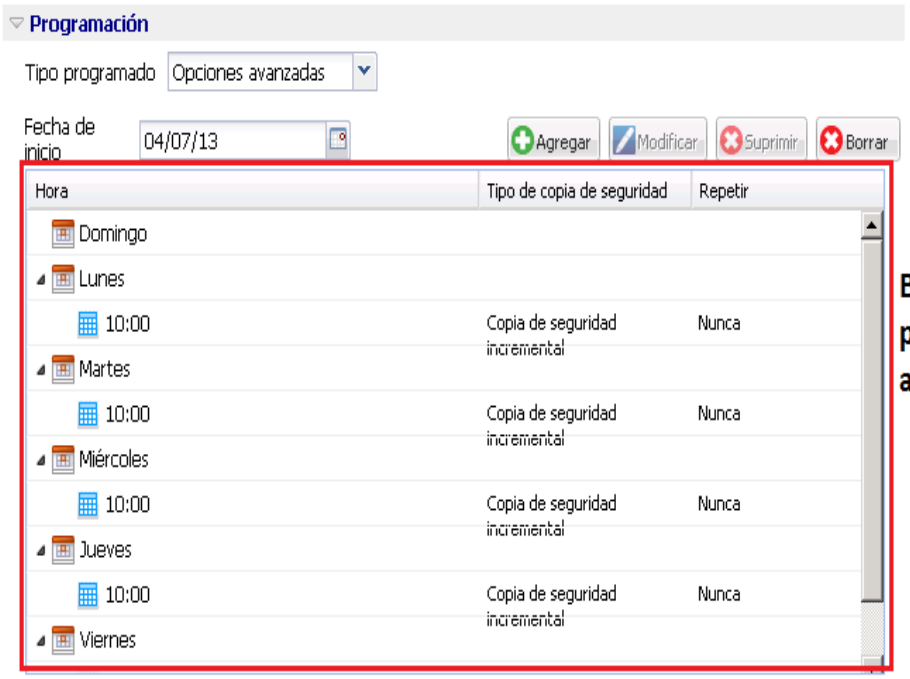
Por tanto, no se puede especificar una fecha y hora de inicio diferentes para distintos tipos de copia de seguridad.

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



Personalizada

Seleccione la opción Personalizada para especificar una programación de copia de seguridad para 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 o borrar una programación personalizada. Al hacer clic en Borrar, se suprimen todas las programaciones de copia de seguridad personalizadas de la bandeja de programaciones personalizadas.

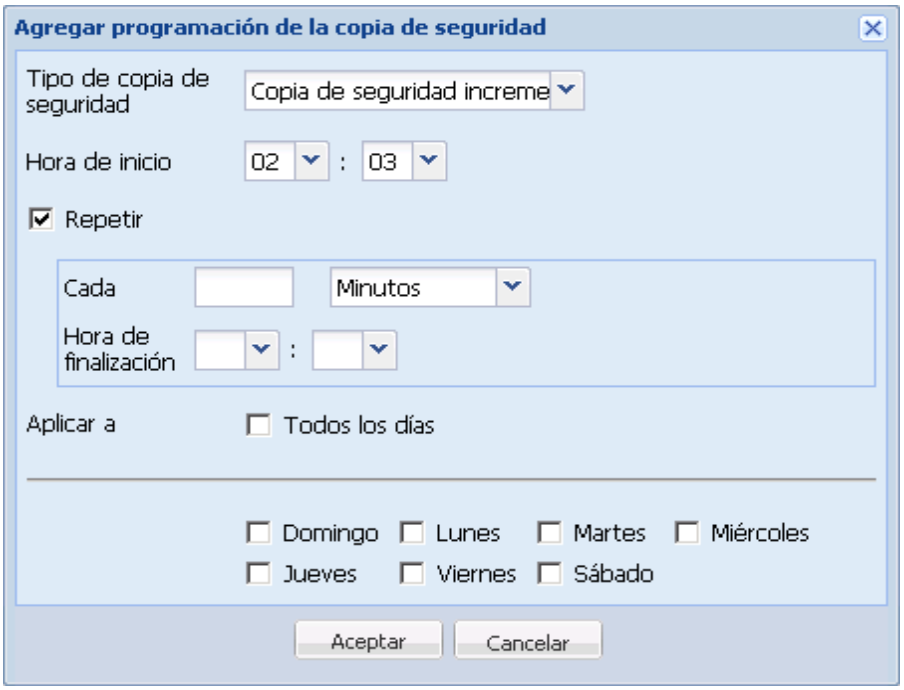


Bandeja de programación avanzada

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 programaciones personalizadas.

Ninguno

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 de 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 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/Arcserve/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 personalizada.

   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.

Esta sección incluye los siguientes temas:

- Información general de los tipos de copia de seguridad
- Información general de los conjuntos de recuperación

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. Arcserve UDP 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 se selecciona la opción Repetir, se debe 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 se selecciona la opción Repetir, se debe 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 del origen (es posible que sea por los cambios en el sistema desde la última copia de seguridad), Arcserve UDP para Linux 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 se selecciona la opción Repetir, se debe 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 estos. 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 en el 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 un 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 retener solamente un conjunto de recuperación, se necesitará espacio para al menos dos copias de seguridad completas.

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 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-target

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

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.

D2D_RECOVERYPOINT

Identifica el punto de recuperación creado por la tarea de copia de seguridad. Este valor solo es aplicable en el script posterior a la copia de seguridad.

D2D_RPSSCHEDULETYPE

Identifica el tipo de programación cuando se realiza la copia de seguridad en un almacén de datos en el servidor de puntos de recuperación. Los siguientes valores identifican la variable D2D_ RPSSCHEDULETYPE:

diariamente

Identifica la programación como una copia de seguridad diaria.

semanalmente

Identifica la programación como una copia de seguridad semanal.

mensualmente

Identifica la programación como una copia de seguridad mensual.

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/Arcserve/d2dserver/usr/prepost
```

Siga estos pasos:

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

   ```
   /opt/Arcserve/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.

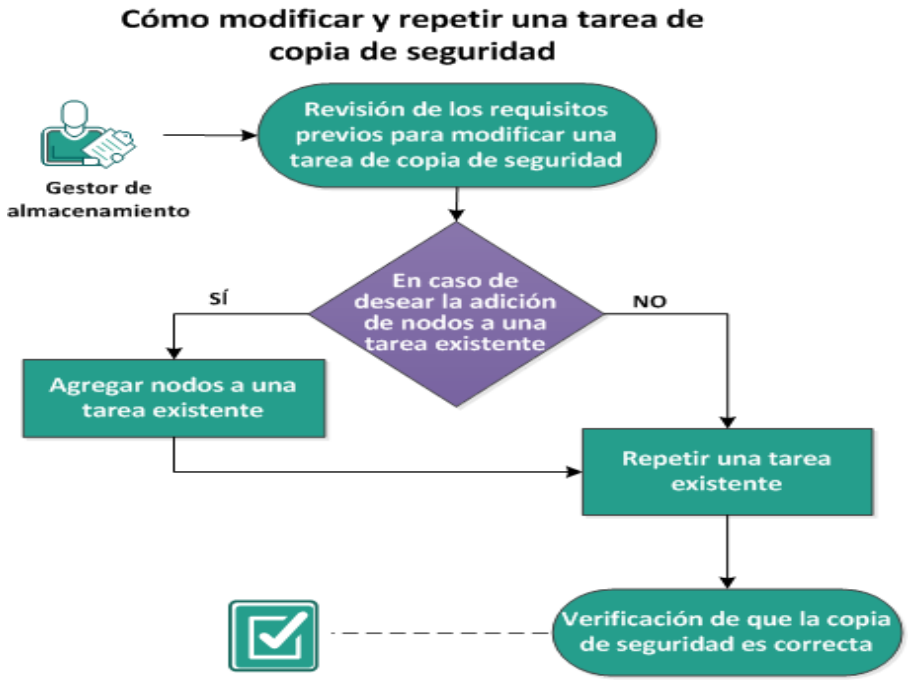
   Los datos de copia de seguridad se han verificado correctamente.

   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 caso de desear la adición de nodos a una tarea existente
- Adición de nodos a una tarea existente
- Repetición de una tarea existente
- Verificación de que la copia de seguridad es correcta

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, las bases de datos y los exploradores compatibles.

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, a continuación, 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, haga lo siguiente:

   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, a continuación, haga clic en **Modificar**.

Aparecerá el cuadro de diálogo Ejecutar tarea de copia de seguridad ahora.

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 la copia de seguridad es xxx.xxx.xxx.xxx:/Data, vaya al destino de la 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.

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

- Revisión de los requisitos previos
- Especificación del punto de recuperación para la copia de seguridad sin agente basada en host
- Especificación del punto de recuperación para la copia de seguridad basada en agentes
- Especificación de los detalles de la máquina de destino
- Especificación de la configuración avanzada
  - (Opcional) Gestión de scripts anteriores/posteriores para la automatización
- Creación y ejecución de la tarea de restauración
- Verificación de la restauración de archivos

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.
- Cuando el destino de la copia de seguridad de una tarea de copia de seguridad es un origen local, para realizar una tarea de restauración a nivel de archivo desde el destino es necesario exportar el destino local del origen a través de NFS o CIFS y también es necesario especificar que el punto de recuperación está disponible en el recurso compartido NFS o CIFS.
- Ha verificado que el servidor de copia de seguridad de Linux sea compatible con el sistema de archivos que desee restaurar.

  Por ejemplo, RedHat 7.x no es compatible con el sistema de archivos de *reiserfs.* Si el sistema operativo del servidor de copia de seguridad es RedHat 7.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 del Agente de Arcserve UDP (Linux) para realizar la restauración a nivel del archivo, ya que el Live CD es compatible con todos los tipos de sistemas de archivos.
- Se han instalado los paquetes siguientes en el servidor de copia de seguridad de Linux:
  - mdadm
  - kpartx
  - lvm2
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Especificación del punto de recuperación para la copia de seguridad sin agente basada en host

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.

Siga estos pasos:

1. Acceda al asistente de restauración de una de las formas siguientes:

   - Desde el Arcserve UDP:

   a. Haga clic en la ficha **recursos**.

   b. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos agregados en el panel central.

   c. En el panel central, seleccione el nodo y haga clic en **Acciones**.

   d. En el menú desplegable **Acciones**, haga clic en **Restaurar archivo**.

      Se abre 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.

   e. 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.**

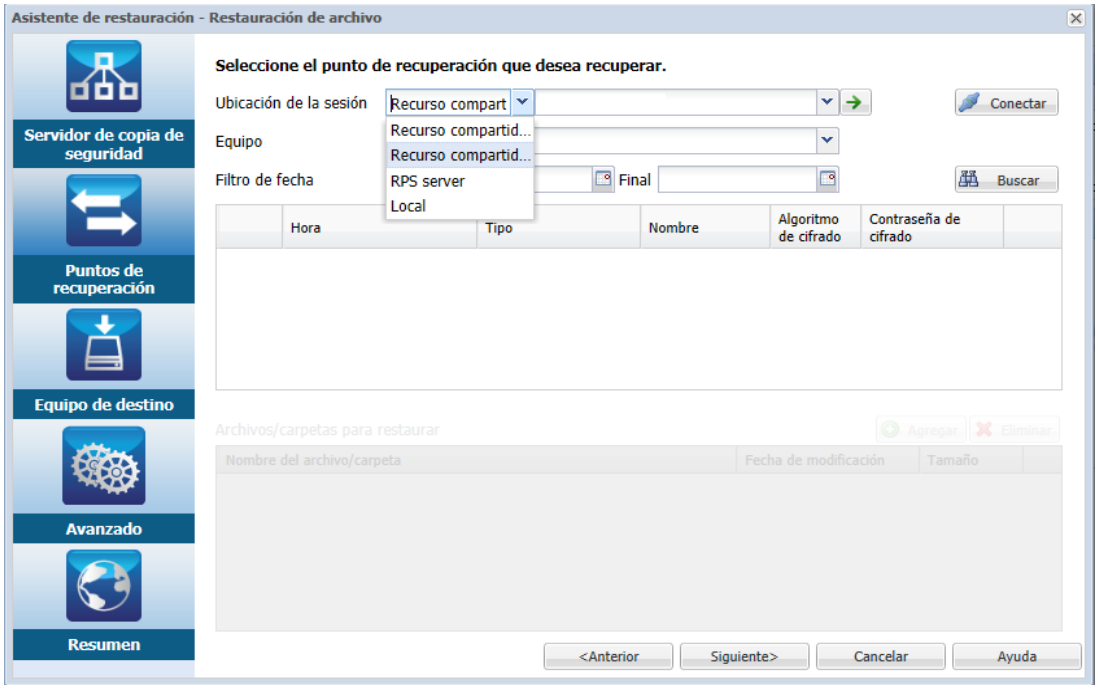
      Se puede ver el servidor de copia de seguridad en la página **Servidor de copia de seguridad** del **Asistente de restauración**.

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**.

   Importante: Si ha abierto el Asistente desde la Consola, los detalles del equipo y de la ubicación de la sesión se muestran automáticamente. Vaya al paso 5.



3. En la lista desplegable **Ubicación de la sesión**, seleccione **Recurso compartido de CIFS** o **RPS**.

   Nota: No se puede seleccionar Recurso compartido de NFS o Local para la restauración de sesiones de copia de seguridad sin agente basada en host.

4. Realice uno de los pasos siguientes en función de la ubicación de la sesión:

   Para el recurso compartido de CIFS:

   a. Especifique la ruta completa del recurso compartido de CIFS y haga clic en **Conectar**.

   b. Especifique el nombre de usuario y la contraseña para conectarse al recurso compartido de CIFS y haga clic en **Aceptar**.

   Para el servidor de puntos de recuperación:

a. Seleccione el servidor de puntos de recuperación y haga clic en Agregar.

   Aparece el cuadro de diálogo **Información del servidor de puntos de recuperación**.

a. Proporcione los detalles del servidor de puntos de recuperación y haga clic en Cargar.

b. Seleccione el almacén de datos de la lista desplegable y haga clic en **Sí**.

   El cuadro de diálogo **Información del servidor de puntos de recuperación** se cierra y aparece el Asistente.

c. Haga clic en **Conectar**.

   Se muestra la lista desplegable Equipo que incluye todos los equipos.

d. Seleccione el equipo de la lista desplegable.

   Todos los puntos de recuperación del equipo seleccionado se muestran debajo de la opción **Filtro de fecha.**

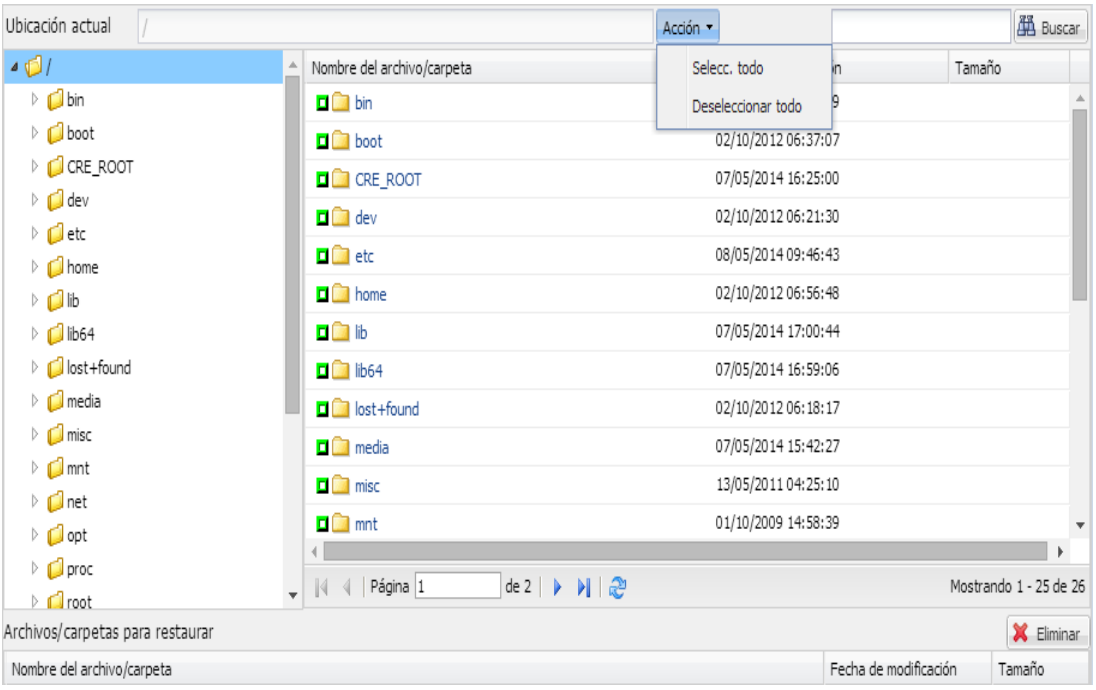
5. Aplique el filtro de fecha para que se muestren los puntos de recuperación que se han generado entre la fecha especificada y haga clic en **Buscar**.

   Valor predeterminado: Las dos últimas semanas.

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

6. 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>**.



Importante: Si aparece el mensaje de advertencia "Los archivos y las carpetas se muestran debajo del archivo del dispositivo. Para obtener más información, haga clic en Ayuda" en la Consola, consulte la siguiente nota para solucionar la incidencia.

Nota: En el caso de algunos diseños de disco complejos, el archivo de dispositivo muestra el sistema de archivos. Este cambio en el comportamiento de visualización del sistema de archivos no afecta a la función de restauración a nivel de archivo de la máquina virtual de Linux basada en el host. Se puede explorar el sistema de archivos del archivo de dispositivo. También, se puede utilizar la función de búsqueda para buscar un directorio o archivo específicos.

7. 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**.

8. Haga clic en **Siguiente**.

   Aparecerá la página **Equipo de destino**.

   Se especifica el punto de recuperación.

Especificación del punto de recuperación para la copia de seguridad basada en agentes

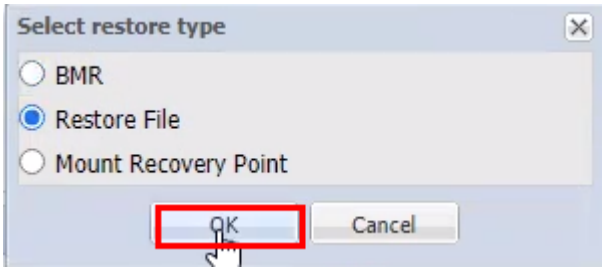
Cada vez que se realiza una copia de seguridad correcta, se creará un punto de recuperación. Especifique la información del punto de recuperación en el Asistente de restauración para que se puedan recuperar los datos exactos que desee. Se pueden restaurar archivos específicos o todos los archivos en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

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. Vaya a **recursos** > **Nodo** > **Todos los nodos**.

        Se muestran todos los nodos agregados en el panel central.
     c. Haga clic con el botón secundario en el nodo y, a continuación, haga clic en **Restaurar**.

        Se abre la interfaz web del Agente de Arcserve UDP (Linux) y se muestra el cuadro de diálogo Seleccionar tipo de restauración.
     d. En el cuadro de diálogo Seleccionar tipo de restauración, haga clic en la opción **Restaurar archivo** y, a continuación, haga clic en **Aceptar**.

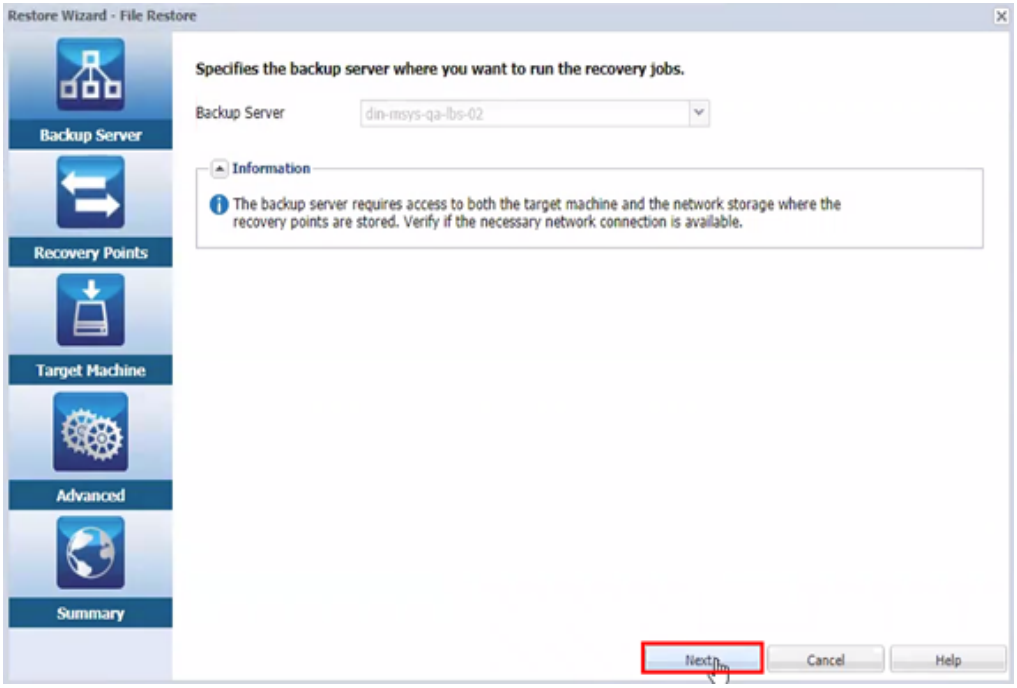
        Nota: Se inicia sesión automáticamente en el nodo del agente y el Asistente de restauración se abre desde el nodo del agente.
   - **Desde el Agente de Arcserve UDP (Linux):**
     a. Abra la interfaz web del Agente de Arcserve UDP (Linux).

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

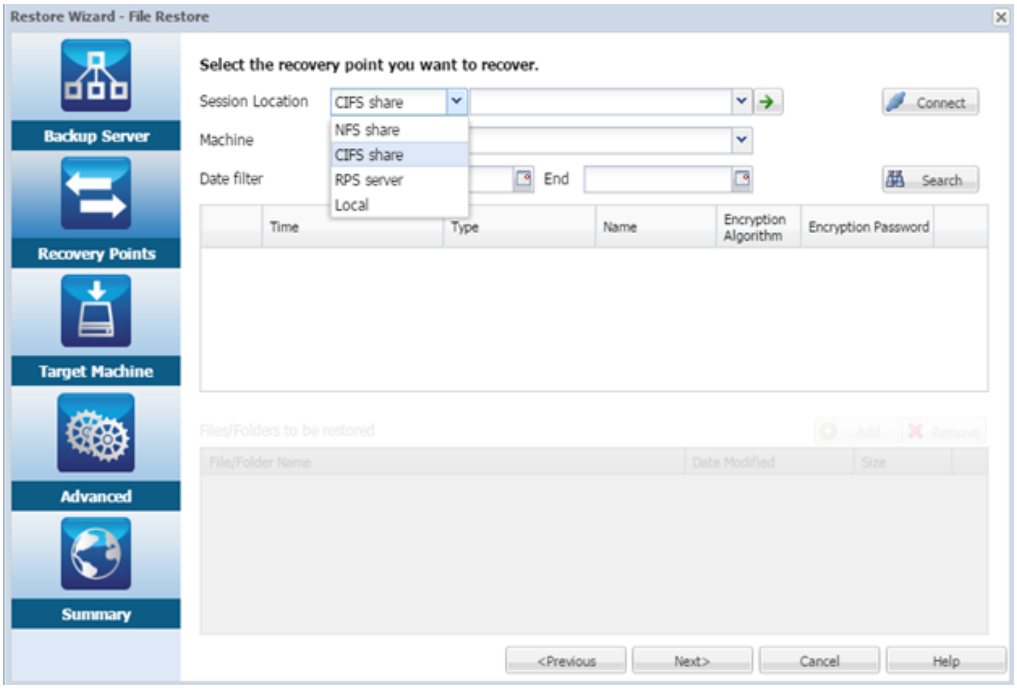
b. En el menú Asistente, haga clic en **Restaurar** y, a continuación, seleccione **Restaurar archivo**.

   Se abre el cuadro de diálogo Asistente de restauración - Restaurar archivo.

2. En la página Servidor de copia de seguridad del Asistente de restauración, se puede ver el servidor de copia de seguridad. No se puede seleccionar ninguna opción en la lista desplegable Servidor de copia de seguridad. Haga clic en **Siguiente**.



3. En la página Puntos de recuperación del Asistente de restauración, haga lo siguiente:



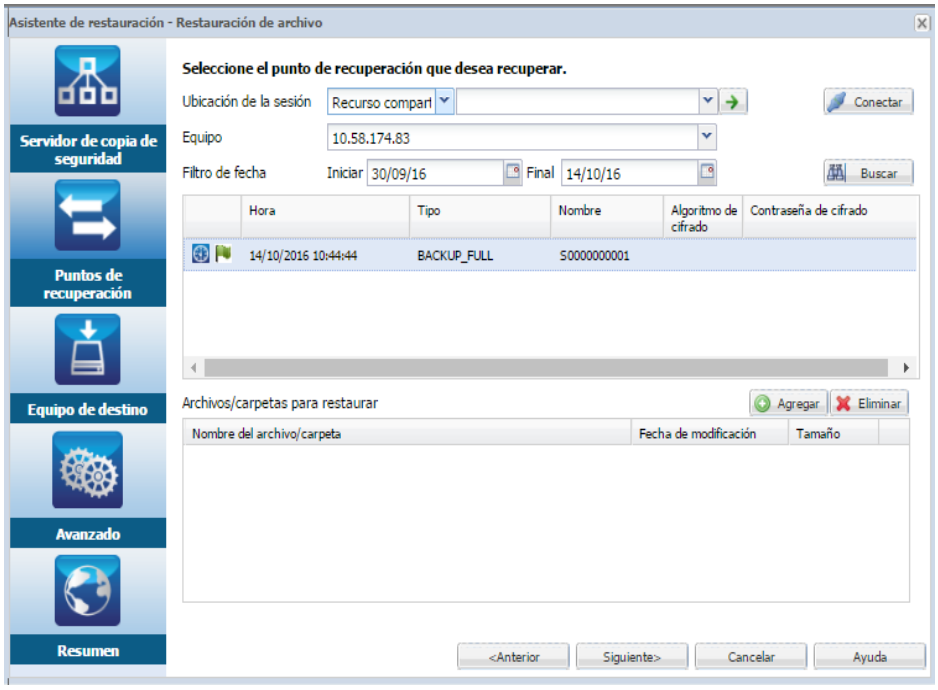
Importante: Si ha abierto el Asistente desde la Consola, los detalles del equipo y de la ubicación de la sesión se muestran automáticamente. Vaya al paso 4.

a. Seleccione **Recurso compartido de CIFS**, **Recurso compartido de NFS**, **Servidor de puntos de recuperación** o **Local** en la lista desplegable Ubicación de la sesión.

b. Si selecciona **Recurso compartido de CIFS, Recurso compartido de NFS o Local**, especifique la ruta completa del recurso compartido de CIFS, del recurso compartido de NFS o local y, a continuación, haga clic en **Conectar**.

   Se muestra la lista desplegable Equipo que incluye todos los equipos.

   Nota: Si se selecciona la opción **Recurso compartido de CIFS**, se deben especificar el nombre de usuario y la contraseña.



c. Si selecciona **Servidor de puntos de recuperación**, haga lo siguiente:

   1. Seleccione el servidor de puntos de recuperación en la lista desplegable y, a continuación, haga clic en **Agregar**.

      Aparece el cuadro de diálogo Información del servidor de puntos de recuperación.

   2. Proporcione los detalles del servidor de puntos de recuperación y, a continuación, haga clic en **Sí**.

   3. Seleccione el almacén de datos en la lista desplegable.

      El cuadro de diálogo Información del servidor de puntos de recuperación se cierra y aparece el Asistente.

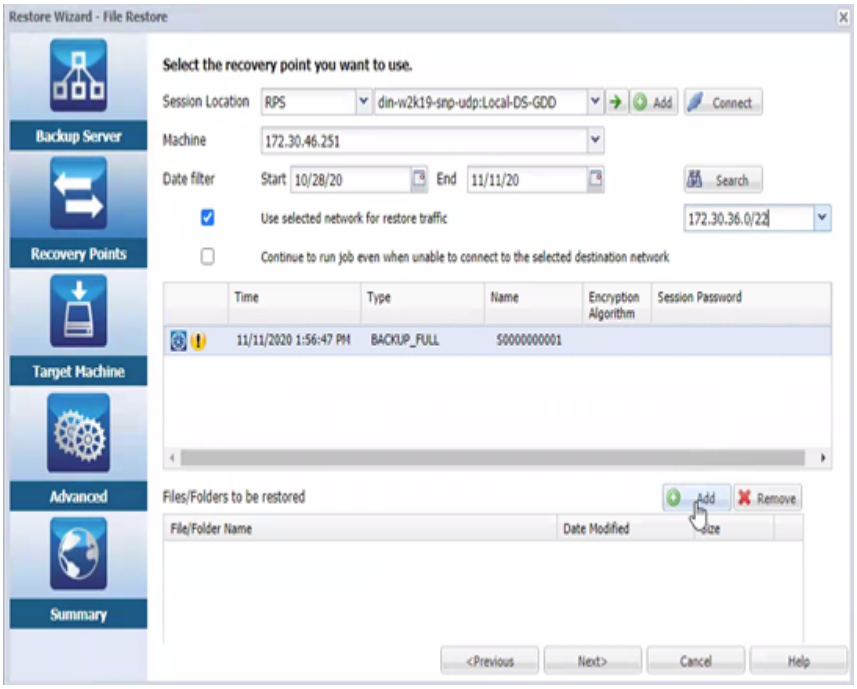
   4. Haga clic en **Conectar**.

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

   5. En la lista desplegable Equipo, seleccione el nodo que desea restaurar.

      Aparecen todos los puntos de recuperación del nodo selec-

cionado.



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

   Valor predeterminado: Las dos últimas semanas.

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

5. Para activar la comunicación entre el Agente de Linux y el servidor de puntos de recuperación, seleccione la casilla de verificación **Utilizar la red seleccionada para el tráfico de restauración** y, a continuación, seleccione la red en la lista desplegable.

   Nota: Si no se puede acceder a la red de copia de seguridad seleccionada y para continuar la tarea de copia de seguridad con la red disponible o con la red predeterminada, haga clic en la casilla de verificación **Continuar ejecutando la tarea incluso cuando no se pueda conectar con la red de copia de seguridad seleccionada**.

6. Seleccione el punto de recuperación que desee restaurar. Si se cifra el punto de recuperación, introduzca la contraseña de cifrado para restaurar datos.

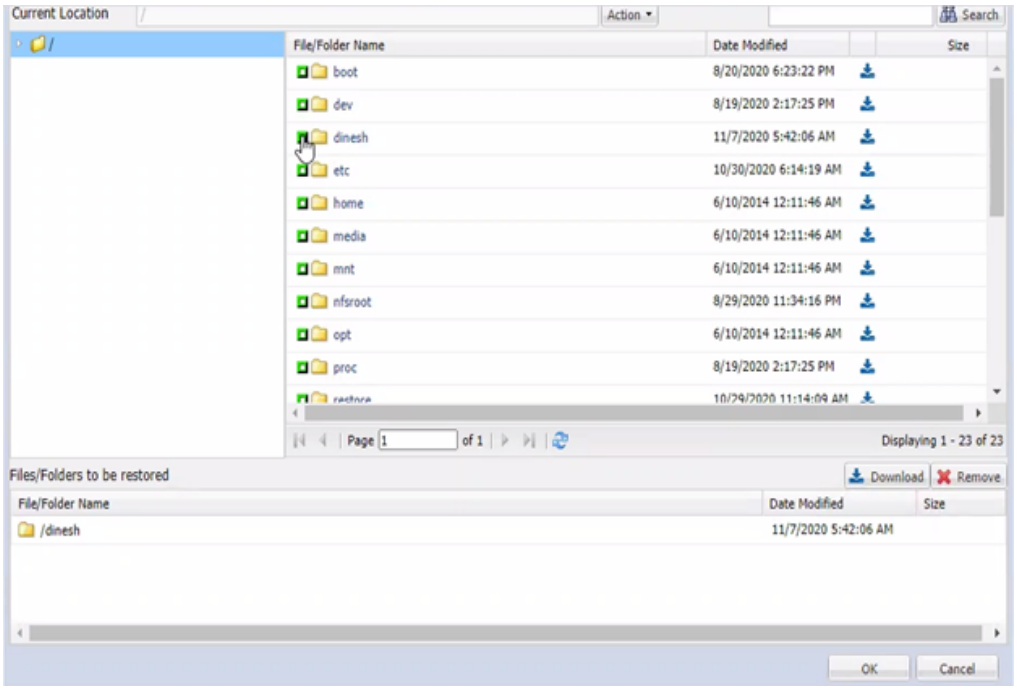
7. Para restaurar los archivos o carpetas, haga clic en **Agregar**.

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

Importante: Si aparece el mensaje de advertencia "Los archivos y las carpetas se muestran debajo del archivo del dispositivo. Para obtener más información, haga clic en Ayuda." en la Consola, consulte la siguiente nota para solucionar la incidencia.

Nota: En el caso de algunos diseños de disco complejos, el archivo de dispositivo muestra el sistema de archivos. Este cambio en el comportamiento de visualización del sistema de archivos no afecta a la función de restauración a nivel de archivo de la máquina virtual de Linux basada en el host. Se puede explorar el sistema de archivos del archivo de dispositivo. También, se puede utilizar la función de búsqueda para buscar un directorio o archivo específicos.

8. En el cuadro de diálogo Explorar-<nombre de nodo>, seleccione el archivo o carpeta que desea restaurar y, a continuación, 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.

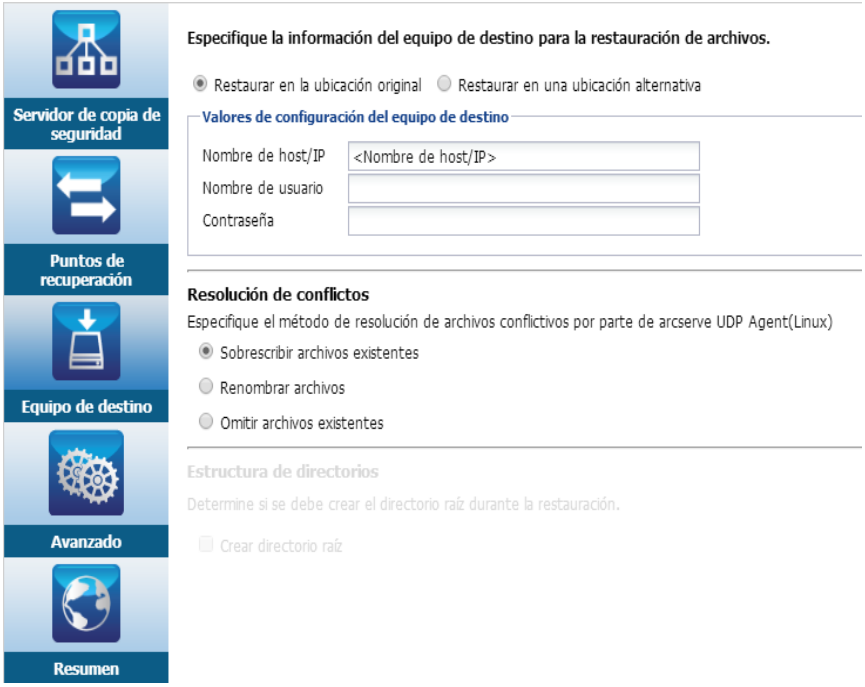
Se especifica el punto de recuperación.

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.

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

1. En la página Equipo de destino, seleccione **Restaurar en la ubicación original**.



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 restaura el archivo. Todos los datos se restaurarán en el nuevo archivo.

Omitir archivos existentes

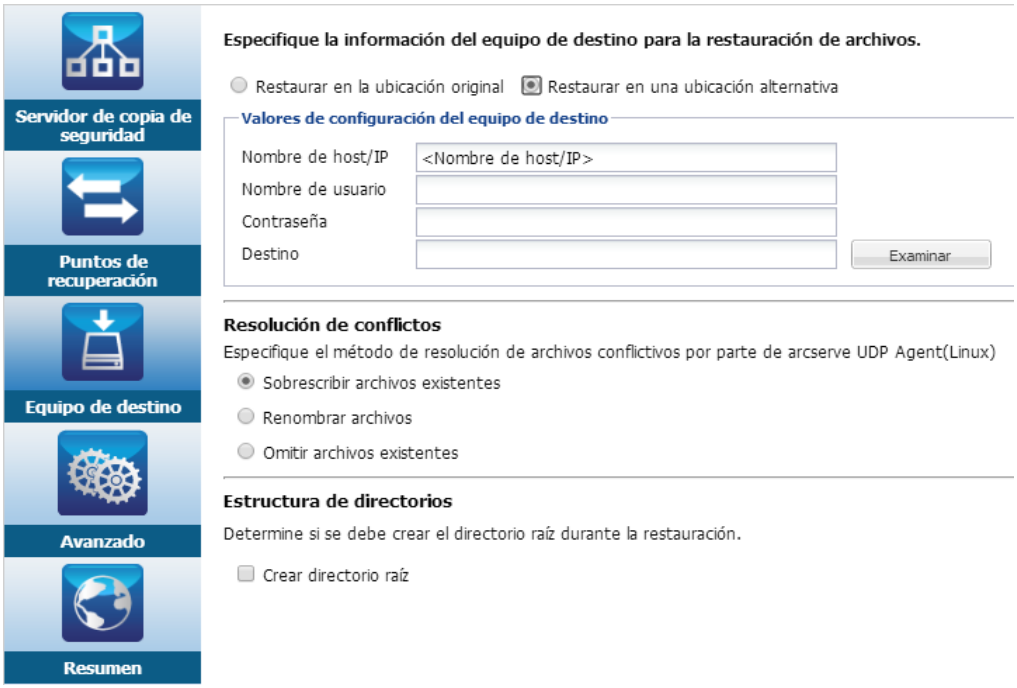
Especifica que existe el mismo archivo en el equipo de destino. A continuación, los archivos no se restauran desde el punto de recuperación.

4. (Opcional) Seleccione **Crear directorio raíz**.
5. Haga clic en **Siguiente**.

   Aparecerá la página Configuración avanzada.

Para restaurar en un nodo nuevo, siga estos pasos:

1. En la página Equipo de destino, seleccione **Restaurar en una ubicación alternativa**.



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, a continuación, 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 restaura 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/Arcserve/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*.

4. Haga clic en **Siguiente**.

   Aparecerá la página Resumen**.**

   Se especifica la configuración avanzada.

   Esta sección incluye los siguientes temas:

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

(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/Arcserve/d2dserver/usr/prepost

Siga estos pasos:

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

   `/opt/Arcserve/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.

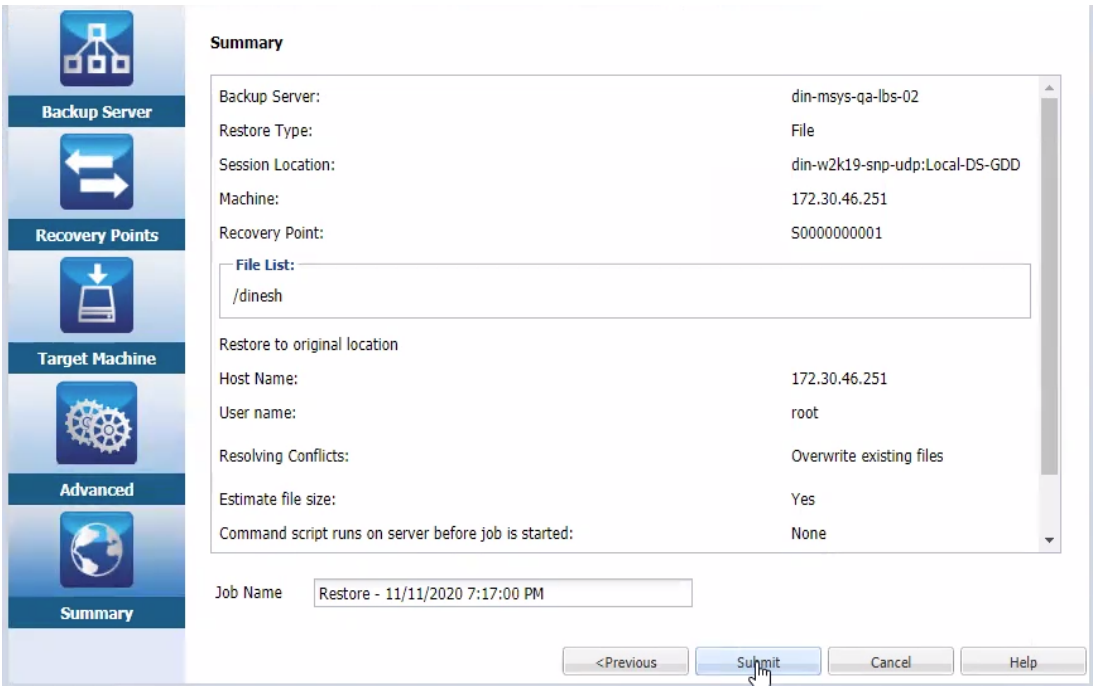
   Los scripts anteriores/posteriores se crean correctamente y se colocan en la carpeta prepost.

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, vuelva atrás y cambie la configuración de la restauración en el asistente.

Siga estos pasos:

1. En la página Resumen del Asistente de restauración, verifique los detalles de la restauración.



2. Realice uno de los procedimientos siguientes:
   - Si la información de resumen no es correcta, haga clic en **Anterior** para volver al cuadro de diálogo correspondiente para cambiar el valor de configuración incorrecto.
   - Si la información de resumen es correcta, introduzca un nombre de tarea y, a continuación, haga clic en **Enviar** para iniciar el proceso de restauración.

Nota: 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 página 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

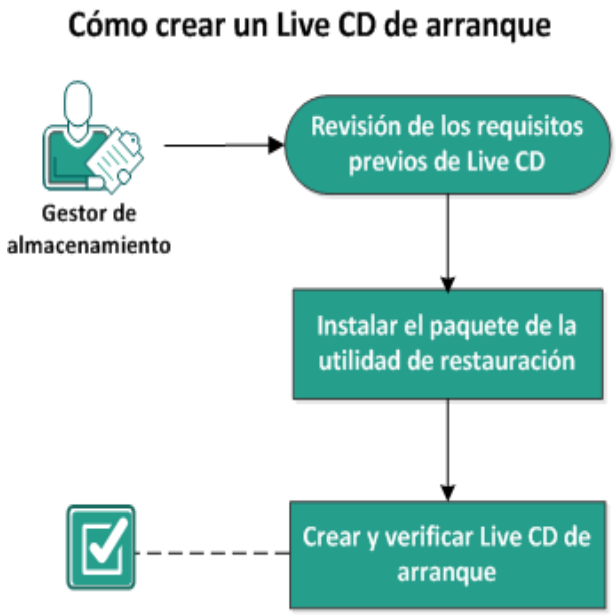
Como gestor de almacenamiento, puede crear un Live CD de arranque. Cuando se cree, este Live CD de arranque contendrá una imagen completa de solo lectura del sistema operativo del equipo. Además, se puede utilizar para ofrecer una funcionalidad temporal del sistema operativo. Este Live CD incluye toda 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 el 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/Arcserve/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
- Instalación del paquete de la utilidad de restauración
- Creación y verificación de Live CD de arranque
- Cómo utilizar el Live CD como un servidor de copia de seguridad de Linux

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, las bases de datos y los exploradores compatibles.

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/Arcserve/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 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 sistema operativo del equipo.

Siga estos pasos:

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

   ```
   # cd /opt/Arcserve/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/Arcserve/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 utilizar el Live CD como un servidor de copia de seguridad de Linux

Se puede utilizar el Live CD como un servidor de copia de seguridad de linux.

Siga estos pasos:

1. Cree un Live CD desde el servidor de copia de seguridad de Linux.

   Para crear el Live CD, realice lo siguiente desde la página principal

   - Haga clic en Restaurar, Reconstrucción completa (BMR).
   - En el Asistente de restauración - reconstrucción completa, haga clic en el vínculo **Haga clic aquí para descargar Live CD** y guarde como el Live CD.

2. Inicie una máquina física o virtual con el Live CD.

   Nota: Se recomienda tener 4 GB de memoria para este equipo.

   Cuando se inicia el equipo con Live CD, se puede ver el mensaje siguiente:

   Utilice la siguiente dirección URL para acceder a este Agente de Arcserve UDP (Linux) y gestionarlo: https://xxx.xxx.xxx.xxx:8014.

   xxx.xxx.xxx.xxx hace referencia a la dirección URL actual que el equipo está utilizando.

3. Introduzca la dirección URL *https://xxx.xxx.xxx.xxx:8014* en el explorador.

   Aparecerá la página de inicio del servidor de copia de seguridad de Linux.

4. Utilice las funciones del servidor de copia de seguridad de Linux para realizar una tarea.

   Por ejemplo: haga clic en Restaurar, Restaurar el archivo y, a continuación, busque la ubicación de la sesión de la copia de seguridad y realice la tarea de restauración a nivel del archivo.

Cómo crear un Live CD de arranque para incluir controladores personalizados para AlmaLinux 9.x

La función de Live CD personalizado permite crear un Live CD de arranque para AlmaLinux 9.0 para incluir los controladores personalizados.

Cuándo debe utilizarse el Live CD personalizado:

Utilice el Live CD personalizado cuando el Live CD predeterminado no pueda identificar los dispositivos de red y de almacenamiento debido a la falta de disponibilidad de un 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 Unified Data Protection para Linux bloquea 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/Arcserve/d2dserver/bin

Revisión de los requisitos previos

Verifique que se han realizado las siguientes tareas de los requisitos previos:

1. Se debe instalar UDP Linux 10.0 o versiones posteriores en LBS.
2. Los controladores de dispositivo (archivos *.ko o *.rpm) se deben preparar y almacenar en una carpeta dentro de LBS.

   Por ejemplo, almacene los controladores de dispositivo en la carpeta /tmp/drivers.

   Nota: Se debe proporcionar el controlador de dispositivo para que coincida con la versión del kernel del Live CD predeterminado de UDPLinux. Actualmente, las versiones del kernel y del sistema operativo para el Live CD de UDP son las siguientes:

   - Versión del SO: AlmaLinux 9.0
   - Versión de Kernel: 5.14.0-70.13.1.el9_0.x86_64
3. Para crear un Live CD personalizado dentro de LBS, se debe asignar suficiente espacio.

   Por ejemplo, si la ruta deseada para la salida del Live CD personalizado es /tmp/iso, el espacio de la ubicación de /tmp/iso debe ser mayor o igual que la suma total del tamaño predeterminado del Live CD, el tamaño total de los controladores del usuario y los archivos .rpm, y 500 MB.

Creación del Live CD personalizado

La función del Live CD personalizado permite iniciar un equipo de destino de reconstrucción completa y ejecutar una tarea de reconstrucción completa. Para crear un Live CD personalizado, se utilizan los siguientes archivos:

driverinlivecd

Script utilizado para remasterizar el Live CD predeterminado.

UDP_Agent_Linux-LiveCD.iso

Live CD predeterminado disponible para el Agente de UDP para Linux.

Siga estos pasos:

1. Vaya a la ubicación siguiente:

   /opt/Arcserve/d2dserver/bin

2. Ejecute el siguiente comando:

   driverinlivecd <ruta_completa_de_LiveCD_predeterminado> <ruta_donde_están_almacenados_los_controladores_de_dispositivo> <ruta_donde_se_debe_almacenar_LiveCD_personalizado>

   Ejemplo: ./driverinlivecd /opt/Arcserve/d2dserver/packages/UDP_Agent_Linux-LiveCD.iso /tmp/drivers /tmp/iso

   El script crea el Live CD personalizado en función de los controladores de dispositivo proporcionados y, a continuación, almacena el archivo de imagen ISO en la ubicación deseada.

   Ejemplo: */tmp/iso/ UDP_Agent_Linux-LiveCD.iso*

Verificación del Live CD personalizado

Esta sección proporciona información sobre cómo verificar el Live CD personalizado.

Siga estos pasos:

1. Inicie un nodo de destino con el Live CD personalizado resultante (UDP_ Agent_Linux-LiveCD.iso) creado en la ubicación deseada:

   /tmp/iso/

2. Abra el shell o la línea de comandos.
3. Para verificar si los archivos .rpm están incluidos en el Live CD personalizado, ejecute el siguiente comando:

   ls /user_rpms/

4. Para verificar si los archivos *.ko están incluidos en el Live CD personalizado, ejecute el siguiente comando:

   ls /lib/modules/5.14.0-70.13.1.el9_0.x86_64/kernel/drivers/users/

5. Compruebe la información de los controladores de dispositivos.

   Ejemplo: modinfo “driver_name”

   Si el resultado no es vacío o NULO, el resultado debe mostrar la información sobre el controlador de dispositivo cargado.

   El Live CD personalizado se ha verificado correctamente. Ahora, se puede realizar la tarea de reconstrucción completa para el nodo de origen deseado.

Notas:

- En el caso de los paquetes rpm, compruebe si los paquetes se pueden instalar simplemente utilizando las utilidades de rpm y no deben tener otras dependencias o paquetes pendientes.

  Por ejemplo, para comprobarlo, intente instalar el paquete rpm en la máquina virtual de AlmaLinux 9.0 (kernel: 5.14.0-70.13.1.el9_0.x86_64) antes de utilizar la función.

- Si los paquetes rpm contienen controladores de dispositivos (archivos *.ko), es posible que a veces los controladores no se carguen correctamente en el nodo de destino después de ejecutar el script *driverinlivecd* y crear el Live CD personalizado. En tales casos, extraiga los paquetes rpm para obtener los archivos .ko requeridos, que se deben cargar en el nodo de destino. Mientras se ejecuta el script *driverinlivecd*, guarde los archivos .ko directamente en la

ruta donde se almacenan los controladores de dispositivo en lugar de guardar el paquete rpm.

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.

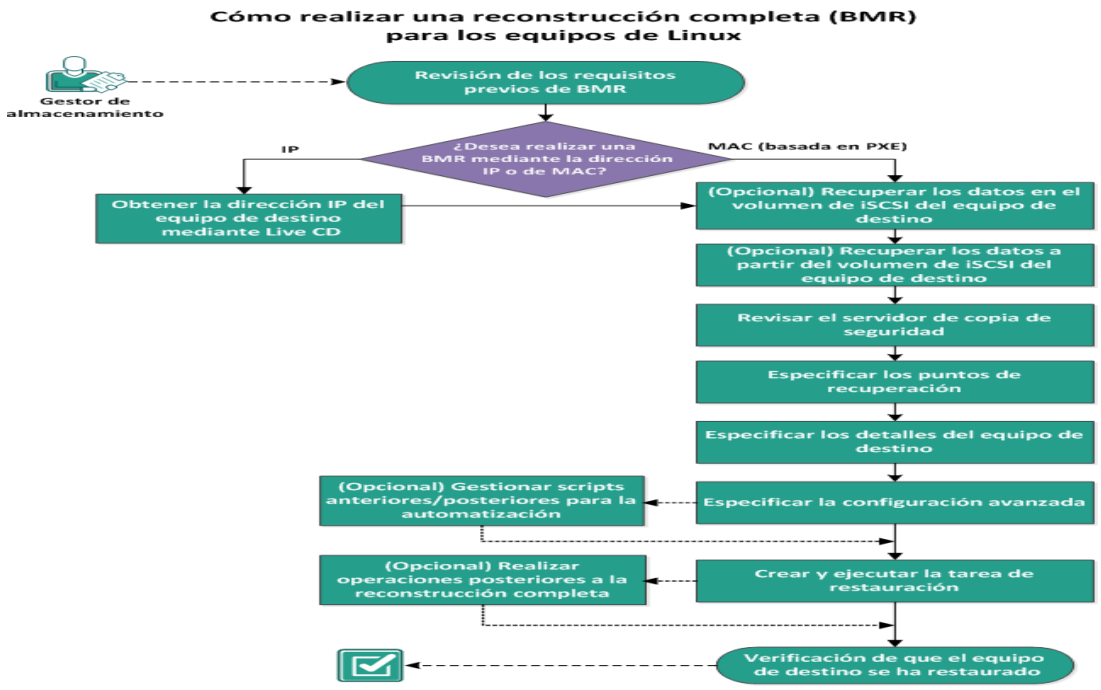
La reconstrucción completa es posible porque cuando se realiza una copia de seguridad de los datos, la copia de seguridad también captura la información relacionada con el sistema operativo, las aplicaciones instaladas y los controladores, entre otros.

Se puede realizar una reconstrucción completa mediante cualquiera de las siguientes opciones:

- Con la opción de la línea de comandos. Para obtener más información, consulte Creación de una plantilla de configuración utilizando la línea de comandos.
- Con la dirección IP o la dirección 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.

  Nota: La máquina puede arrancar. Solo se configura una tarjeta NIC.

El diagrama siguiente muestra el proceso para realizar una reconstrucción completa utilizando la dirección IP o MAC:



Complete las tareas siguientes para realizar una reconstrucción completa:

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

Creación de una plantilla de configuración utilizando la línea de comandos

Cree un archivo de configuración para que el comando d2dbmr pueda restaurar las máquinas virtuales basadas en los parámetros especificados en el archivo. El archivo d2dbmr recopila todas las especificaciones del archivo y realiza la restauración basándose en las especificaciones. El comando d2dbmr se utiliza para ejecutar la reconstrucción completa desde la línea de comandos.

Sintaxis

d2dbmr --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 hace referencia a la contraseña que se debe especificar.

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:

   ```
   d2dbmr --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.

   storage_location_type

   Especifica el tipo de ubicación de almacenamiento de la sesión. La ubicación de almacenamiento puede ser CIFS, NFS o RPS.

   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.

rps_server

Especifica el nombre del servidor de puntos de recuperación cuando **storage_location_type** es RPS.

rps_server_username

Especifica el nombre de usuario del servidor de puntos de recuperación cuando **storage_location_type** es RPS.

rps_server_password

Especifica la contraseña del servidor de puntos de recuperación cuando **storage_location_type** es RPS. La contraseña se cifra utilizando la utilidad de cifrado d2dutil.

rps_server_protocol

Especifica el protocolo del servidor de puntos de recuperación cuando **storage_location_type** es RPS.

rps_server_port

Especifica el puerto del servidor de puntos de recuperación cuando **storage_location_type** es RPS.

rps_server_datastore

Especifica el nombre del almacén de datos del servidor de puntos de recuperación cuando **storage_location_type** es RPS.

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'.

exclude_volumes

Especifica los volúmenes que se deben excluir para la máquina virtual de destino.

No excluya el volumen '/'. Utilice ':' para separar varios volúmenes.

include_volumes

Especifica los volúmenes que se deben incluir para la máquina virtual de destino.

Se deben incluir los siguientes volúmenes: / , /boot, /boot/efi, /home, /usr, /usr/local. Utilice ':' para separar varios volúmenes.

restore_target

Especifica la dirección IP/MAC del destino de la restauración.

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 IP estática.

guest_dns

Especifica la dirección de DNS 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.

enable_instant_restore

(Opcional) Especifica la activación de la restauración instantánea. Los valores son sí y no.

auto_restore_data

(Opcional) Especifica la restauración de datos automáticamente. Los valores son sí y no.

script_pre_job_server

(Opcional) Especifica el script que se debe poner en marcha antes de ejecutar la tarea en el servidor.

script_post_job_server

(Opcional) Especifica el script que se debe poner en marcha después de ejecutar la tarea en el servidor.

script_pre_job_client

(Opcional) Especifica el script que se debe poner en marcha antes de ejecutar la tarea en el cliente.

script_post_job_client

(Opcional) Especifica el script que se debe poner en marcha después de ejecutar la tarea en el cliente.

script_ready_to_use

(Opcional) Especifica el script que se debe ejecutar cuando el equipo de destino está listo para su uso y cuando el valor del parámetro **enable_instant_restore** es Sí.

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.

5. Envíe una tarea utilizando la plantilla d2dbmr con el comando siguiente:

   ./d2dbmr –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 disponible, el usuario volverá al entorno de shell inmediatamente después de enviar la tarea.

   Se envía la tarea de restauración.

Revisión de los requisitos previos de BMR

Tenga en cuenta los requisitos previos siguientes antes de realizar una reconstrucción completa:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado, si la hay, para la restauración.
- 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.
- Cuando el destino de la copia de seguridad de una tarea de copia de seguridad es un origen local, para realizar una tarea de restauración completa desde el destino es necesario exportar el destino local del origen a través de NFS o CIFS y también es necesario especificar que el punto de recuperación está disponible en el recurso compartido de NFS o CIFS.
- El punto de recuperación debe ser de la copia de seguridad basada en el agente de Linux.
- El nodo de destino y el nodo de origen deben tener las mismas configuraciones de firmware. Por ejemplo, si configura el nodo de origen con el firmware del BIOS, deberá configurar el nodo de destino solamente con el firmware del BIOS.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

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. Para obtener la dirección IP, se debe iniciar el equipo de reconstrucción completa utilizando el Live CD predeterminado, es decir, el Live CD del Agente de Arcserve UDP (Linux), o el Live CD basado en CentOS. 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 del 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>
```

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.

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 el Live CD del Agente de Arcserve UDP (Linux) o monte el archivo .iso del 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 del 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.

   ```
   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```
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 nodo 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 el Live CD del Agente de Arcserve UDP (Linux) o monte el archivo .iso del 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 del 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 discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>
   ```

   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
```

```
# mkdir /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 el Arcserve UDP:

   a. Haga clic en la ficha **recursos**.

   b. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos de agregados en el panel central.

   c. En el panel central, seleccione el nodo y haga clic en **Acciones**.

   d. Haga clic en **Restaurar** en el menú desplegable **Acciones**.

      Se abre 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.

   e. 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)**.

   Se abre la página **Servidor de copia de seguridad** del **Asistente de restauración - BMR**.

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**.

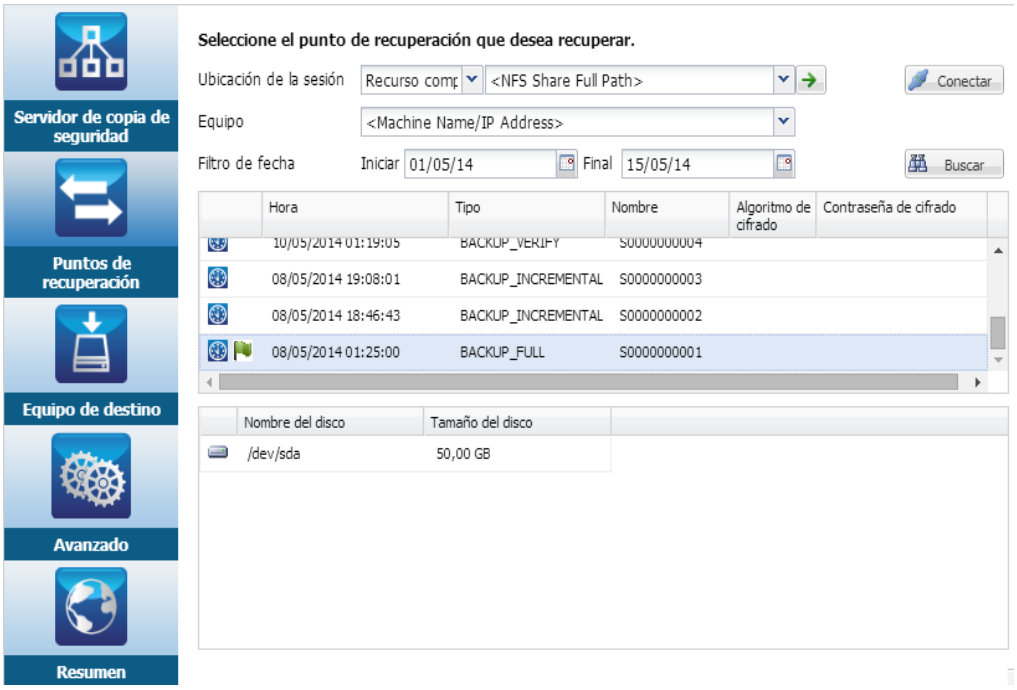
   e. Seleccione **Local** como la **Ubicación de la sesión** en la página **Puntos de recuperación** del **Asistente de reconstrucción completa**.

   - 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.

6. Aplique los valores de configuración del filtro del volumen para el punto de recuperación seleccionado y haga clic en **Aceptar**.

   Se muestran todos los volúmenes disponibles presentes en el nodo. Puede incluir o excluir volúmenes en función de los requisitos.

   Nota: No excluya los siguientes volúmenes: / , /boot, /boot/efi, /home, /usr, /usr/local.

7. Haga clic en **Siguiente**.

   Aparecerá la página **Equipo de destino**.

Se especifica el punto de recuperación.

Especificación de los detalles de la máquina 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 **Activar la reconstrucción completa instantánea** para poder utilizar el equipo de destino instantáneamente.

   Cuando se activa esta opción, el Agente de Arcserve UDP (Linux) primero recupera todos los datos necesarios requeridos para iniciar el equipo. Después de que se inicie el equipo de destino, se recuperarán los datos restantes. La conexión de red

debe estar disponible constantemente durante la reconstrucción completa instantánea.

Ejemplo: Si se tienen 100 GB de datos, se desea realizar una reconstrucción completa y *no* se selecciona esta opción, primero se recuperarán los 100 GB de datos y, a continuación, se podrá utilizar el equipo de destino. Sin embargo, solo se necesita alrededor de 1 GB de datos para iniciar el equipo. Cuando se activa esta opción, primero se recuperan los datos de 1 GB necesarios para poder iniciar y utilizar el equipo. Una vez iniciado el equipo, se recuperan automáticamente los 99 GB de datos restantes.

Nota: Los datos necesarios para iniciar el equipo dependen de la configuración del sistema operativo. También se puede pausar o reanudar la recuperación automática de los datos si la opción **No recuperar los datos automáticamente después de que se inicie el equipo** no está seleccionada.

5. (Opcional) Seleccione la opción **No recuperar los datos automáticamente después de que se inicie el equipo** para detener la recuperación automática de los datos cuando se inicia el equipo de destino.

   Cuando se selecciona la opción **Activar la reconstrucción completa instantánea**, el comportamiento predeterminado es primero recuperar los datos necesarios e iniciar el equipo. Después de iniciar el equipo, los datos restantes se recuperan automáticamente. Si se actualizan los datos de origen durante la recuperación, seleccionando esta opción se recuperarán los datos hasta el punto anterior a su actualización.

6. 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/Arcserve/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*.

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. (Opcional) Seleccione la opción **Reiniciar** para reiniciar automáticamente el nodo de destino después de finalizar la reconstrucción completa.
9. Haga clic en **Siguiente**.

   Aparecerá la página **Resumen**.

   Se especifica la configuración avanzada.

   Esta sección incluye los siguientes temas:

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

(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 una copia de seguridad completa.

backup.incremental

Identifica la tarea como una copia de seguridad incremental.

backup.verify

Identifica la tarea como una 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 después 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/Arcserve/d2dserver/usr/prepost
```

Siga estos pasos:

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

   ```
   /opt/Arcserve/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 la 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.

   Esta sección incluye los siguientes temas:

- (Opcional) Realización de operaciones posteriores a la reconstrucción completa

(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.

Siga estos pasos:

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.

Siga estos pasos:

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

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

# mount /dev/sdb1 /data

--- Volumen lógico ---

Nombre LV                /dev/VGTest/LVTest

Nombre VG                VGTest

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

Acceso de escritura a LV        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): pDisk /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

Command actione   extended

p   partición principal (1-4)

p

Número de partición (2-4): 1

Primer sector (16777216-33554431, valor pre-
determinado 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.

```
# vgchange -a y VGTest# 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 a LV        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 realizar una reconstrucción completa (BMR) para los equipos de Linux en la nube de AWS

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 utilizando la dirección IP de la instancia de destino de Linux en Amazon EC2. Si se arranca la instancia de Linux de destino mediante la AMI del Agente de Arcserve UDP (Linux), se podrá obtener la dirección IP privada de la instancia.

El proceso para realizar una reconstrucción completa para instancias de Linux en Amazon EC2 es casi el mismo con los equipos de Linux en el recurso local.

Complete las tareas siguientes para realizar una reconstrucción completa:

- Revisión de los requisitos previos de la reconstrucción completa
- Inicio de una instancia utilizando el CD Live del Agente de Arcserve UDP
- Revisión de la instancia del servidor de copia de seguridad
- Especificación de los puntos de recuperación
- Especificación de los detalles de la instancia de destino
- Especificación de la configuración avanzada
- Creación y ejecución de la tarea de restauración
- Verificación de que la instancia de destino se ha restaurado

Revisión de los requisitos previos de la reconstrucción completa

Antes de realizar una reconstrucción completa para las instancias de Linux en Amazon EC2, considere las siguientes opciones:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado para la restauración, si hay.
- Cuando el destino de la copia de seguridad de una tarea de copia de seguridad es un origen local, para realizar una tarea de restauración completa desde el destino es necesario exportar el destino local del origen a través de NFS o CIFS y también es necesario especificar que el punto de recuperación está disponible en el recurso compartido de NFS o CIFS.
- El punto de recuperación debe ser de la copia de seguridad basada en el agente de Linux.
- Tiene una instancia del Agente de Arcserve UDP para Linux en Amazon EC2.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Inicio de una instancia utilizando el CD Live del Agente de Arcserve UDP

Antes de realizar una reconstrucción completa para las instancias de Linux en Amazon EC2, se debe iniciar una instancia de destino de la reconstrucción completa utilizando el CD Live del Agente de Arcserve UDP. Cuando la instancia de destino de la reconstrucción completa esté lista, se podrá obtener la dirección IP de la instancia y realizar una tarea de reconstrucción completa con la dirección IP.

Siga estos pasos:

1. Inicie sesión en la consola de gestión de EC2 con su cuenta y seleccione **Launch Instance** (Iniciar instancia).
2. Seleccione una Amazon Machine Image (AMI) en Community AMIs (AMI de la comunidad).

   Se puede buscar la AMI del CD Live con *Arcserve_UDP_Agent_Linux-LiveCD* en Community AMIs.

   Notas:

   - Si la máquina virtual paralela (PVM, por sus siglas en inglés) es el nodo de origen de la copia de seguridad que se desea restaurar, seleccione "Arcserve_UDP_Agent_Linux-LiveCD-PVM-UDP$version AMI" para iniciar la instancia.
   - Si la máquina virtual de hardware (HVM. por sus siglas en inglés) u otro equipo de destino es el nodo de origen de la copia de seguridad que se desea restaurar, seleccione "Arcserve_UDP_Agent_Linux-LiveCD-HVM-UDP$version AMI" para iniciar la instancia.
   - Arcserve_UDP_Agent_Linux-LiveCD-PVM-UDP7.1 se aplica a UDP 8.0.
   - Arcserve_UDP_Agent_Linux-LiveCD-HVM-UDP7.2
   - Arcserve_UDP_Agent_Linux-LiveCD-HVM-UDP8.0
   - Arcserve_UDP_Agent_Linux-LiveCD-HVM-UDP8.1
   - Arcserve_UDP_Agent_Linux-LiveCD-HVM-UDP9.0
3. En el asistente para el inicio de la instancia, seleccione el tipo de instancia necesario.
4. Configure los detalles de la instancia mientras se inician otras instancias. Por ejemplo: incluya la red, la subred, asigne automáticamente la dirección IP pública, etc.

5. Agregue almacenamiento para la instancia utilizando los pasos siguientes:
    a. Obtenga la información del disco incluido el número de disco y el tamaño del disco del nodo de origen de la copia de seguridad que se desea restaurar. Se puede obtener la información del disco cuando se selecciona un punto de recuperación en el Asistente para la restauración para realizar una tarea de reconstrucción completa.
    b. Amplíe el tamaño del volumen raíz para que coincida con el tamaño del disco raíz del nodo de origen de la copia de seguridad. Se pueden agregar otros discos, si el nodo de origen de la copia de seguridad tiene más discos.
6. Agregue etiquetas para la instancia de destino de la reconstrucción completa.
7. Configure el grupo de seguridad para la instancia de destino de la reconstrucción completa utilizando los pasos siguientes:
    a. Cree un nuevo grupo de seguridad para el tipo SSH.
    b. Para que la instancia de destino de la reconstrucción completa sea más segura, seleccione el modo **Personalizado** para el origen que va a determinar el tráfico que debe llegar a la instancia de destino de la reconstrucción completa en la regla recién creada. Especifique el origen personalizado con el formato CIDR para que la instancia de destino de la reconstrucción completa pueda tener acceso al Agente de Arcserve UDP para el servidor de Linux, pero que no pueda tener acceso a los otros equipos de Internet.

        Por ejemplo, si la dirección IP del Agente de Arcserve UDP para el servidor de Linux es 172.31.X.X, especifique el origen como 172.31.0.0/16 o 172.0.0.0/8.
8. Revise los detalles de la instancia y, a continuación, haga clic en **Launch** (Iniciar).

    Se mostrará el cuadro de diálogo para **seleccionar un par de clave existente o crear un par de clave nuevo**.
9. En el cuadro de diálogo, seleccione la opción **Proceed without a key pair** (Continúe sin un par de clave) y haga clic en **Launch Instances** (Iniciar instancias).
10. Adquiera la dirección IP privada en la descripción de la instancia, cuando la instancia de destino de la reconstrucción completa esté lista para usar.

    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 de la instancia de destino de la reconstrucción completa.

Revisión de la instancia del servidor de copia de seguridad

Cuando se abre el **Asistente de restauración**, revise la instancia del 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 el Arcserve UDP:
   a. Haga clic en la ficha **recursos**.
   b. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos de agregados en el panel central.

   c. En el panel central, seleccione el nodo y haga clic en **Acciones**.
   d. Haga clic en **Restaurar** del menú desplegable **Acción**.

      Se abre 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.

   e. 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)**.

   Se abre la página **Servidor de copia de seguridad** del **Asistente de restauración - BMR**.

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

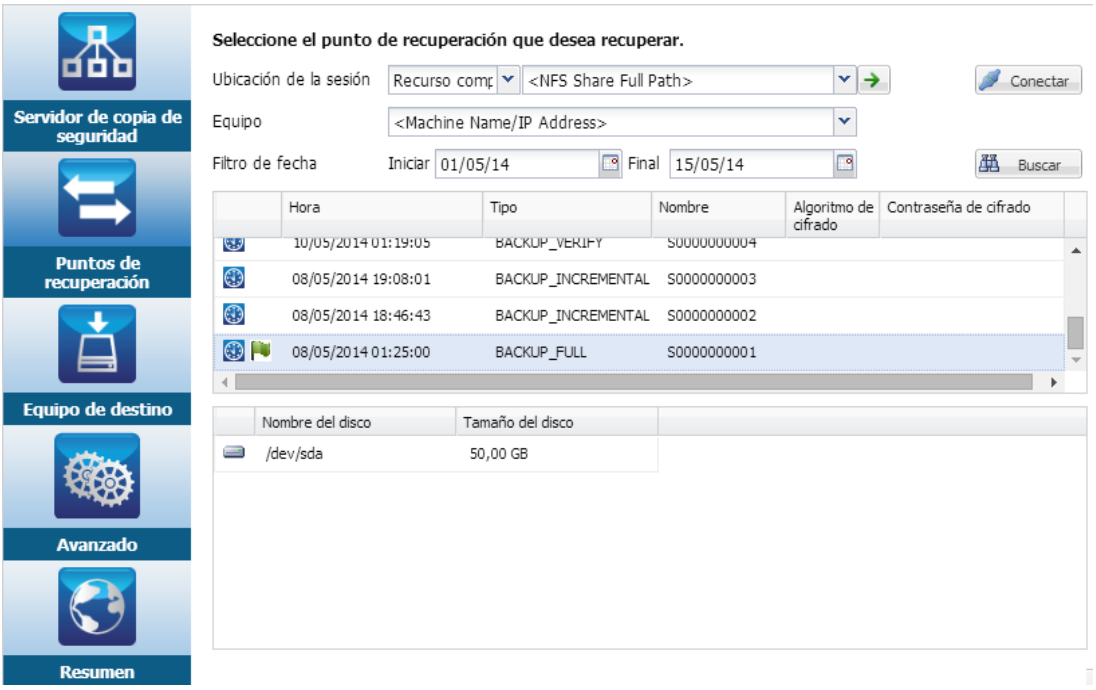
Cada vez que se realiza una copia de seguridad correcta, se creará un punto de recuperación. Especifique la información del punto de recuperación en el **Asistente de restauración** para que se puedan recuperar los datos exactos que desee. Se pueden restaurar archivos específicos o todos los archivos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



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**.

   Se abre la página de la **Instancia de destino de la reconstrucción completa**.

   Se especifica el punto de recuperación.

Especificación de los detalles de la instancia de destino

Especifique los detalles de la instancia de destino de la reconstrucción completa para restaurar datos en ese equipo. Una instancia de destino es un equipo de reconstrucción completa donde se realiza una reconstrucción completa. Se necesita la dirección IP de la instancia de destino de la reconstrucción completa que se ha registrado previamente en el inicio de este proceso.

Siga estos pasos:

1. Escriba la dirección IP de la instancia de destino de la reconstrucción completa en el campo **Dirección MAC/IP**.
2. Introduzca un nombre en el campo **Nombre del host**.

   La instancia de destino de la reconstrucción completa 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 **Activar la reconstrucción completa instantánea** para poder utilizar el equipo de destino instantáneamente.

   Cuando se activa esta opción, el Agente de Arcserve UDP (Linux) primero recupera todos los datos necesarios requeridos para iniciar el equipo. Después de que se inicie el equipo de destino, se recuperarán los datos restantes. La conexión de red debe estar disponible constantemente durante la reconstrucción completa instantánea.

Ejemplo: Si se tienen 100 GB de datos, se desea realizar una reconstrucción completa y *no* se selecciona esta opción, primero se recuperarán los 100 GB de datos y, a continuación, se podrá utilizar el equipo de destino. Sin embargo, solo se necesita alrededor de 1 GB de datos para iniciar el equipo. Cuando se activa esta opción, primero se recuperan los datos de 1 GB necesarios para poder iniciar y utilizar el equipo. Una vez iniciado el equipo, se recuperan automáticamente los 99 GB de datos restantes.

Nota: Los datos necesarios para iniciar el equipo dependen de la configuración del sistema operativo. También se puede pausar o reanudar la recuperación automática de los datos si la opción **No recuperar los datos automáticamente después de que se inicie el equipo** no está seleccionada.

5. (Opcional) Seleccione la opción **No recuperar los datos automáticamente después de que se inicie el equipo** para detener la recuperación automática de los datos cuando se inicia el equipo de destino.

   Cuando se selecciona la opción **Activar la reconstrucción completa instantánea**, el comportamiento predeterminado es primero recuperar los datos necesarios e iniciar el equipo. Después de iniciar el equipo, los datos restantes se recuperan automáticamente. Si se actualizan los datos de origen durante la recuperación, seleccionando esta opción se recuperarán los datos hasta el punto anterior a su actualización.

6. Haga clic en **Siguiente**.

   Aparecerá la página **Configuración avanzada**.

   Se han especificado los detalles de la instancia de destino de la reconstrucción completa.

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 la instancia de destino de la reconstrucción completa.

   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/Arcserve/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*.

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 la instancia de destino de la reconstrucción completa durante el proceso de recuperación.

7. (Opcional) Seleccione la opción **Reiniciar** para reiniciar automáticamente el nodo de destino después de finalizar la reconstrucción completa.
8. Haga clic en **Siguiente**.

   Aparecerá la página **Resumen**.

   Se especifica la configuración avanzada.

   Esta sección incluye los siguientes temas:

   - (Opcional) Gestión de scripts anteriores/posteriores para la automatización en la nube de AWS

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

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 una copia de seguridad completa.

   backup.incremental

   Identifica la tarea como una copia de seguridad incremental.

backup.verify

Identifica la tarea como una 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 la instancia de destino de la reconstrucción completa después de que se inicie la tarea.

post-job-target

Identifica el script que se ejecuta en la instancia de destino de la reconstrucción completa después de que se complete la tarea.

pre-snapshot

Identifica el script que se ejecuta en la instancia de destino de la reconstrucción completa antes de capturar la instantánea.

post-snapshot

Identifica el script que se ejecuta en la instancia de destino de la reconstrucción completa 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/Arcserve/d2dserver/usr/prepost
```

Siga estos pasos:

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

   ```
   /opt/Arcserve/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 la 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.

   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.

   Esta sección incluye los siguientes temas:

   - (Opcional) Realización de operaciones posteriores a la reconstrucción completa

(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:

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 la instancia de destino de la reconstrucción completa se reinicie correctamente después de la reconstrucción completa, se podrá ampliar 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.

Siga estos pasos:

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.

Siga estos pasos:

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

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

# mount /dev/sdb1 /data
```

```
--- Volumen lógico ---
Nombre LV                /dev/VGTest/LVTest
Nombre VG                VGTest
LV UUID                  udoBIx-XKBS-1Wky-3FVQ-mxMf-
FayO-tpfPl8
Acceso de escritura a LV        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): pDisk /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

Command actione   extended

p   partición principal (1-4)

p

Número de partición (2-4): 1

Primer sector (16777216-33554431, valor pre-
determinado 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.

```
# vgchange -a y VGTest# 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 a LV        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 la instancia de destino se ha restaurado

Después de finalizar la tarea de restauración, verifique que la instancia de destino se restaure con los datos relevantes.

Siga estos pasos:

1. Vaya a la instancia de destino de la reconstrucción completa que se ha restaurado.
2. Verifique que la instancia de destino de la reconstrucción completa tiene toda la información de la que se ha realizado la copia de seguridad.

   La instancia de destino se ha verificado correctamente.

   Nota: Cuando la instancia de destino de la reconstrucción completa está lista para su uso, se puede modificar el grupo de seguridad recién creado según las necesidades de su empresa.

   La reconstrucción completa se ha ejecutado correctamente en los equipos de Linux.

Cómo realizar una reconstrucción completa (BMR) para los equipos de Linux en la nube de Azure

Una reconstrucción completa restaura las aplicaciones de software y el sistema operativo y recupera todos los datos de copia de seguridad. 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 utilizando la dirección IP de la máquina virtual de destino de Linux en Microsoft Azure. El proceso para realizar una reconstrucción completa para instancias de Linux en Microsoft Azure es ligeramente diferente del proceso con los equipos de Linux en el recurso local.

Complete las tareas siguientes para realizar una reconstrucción completa:

- Revisión de los requisitos previos de la reconstrucción completa
- Creación de un nuevo equipo de Microsoft Azure como destino de la reconstrucción completa
- Revisión de la máquina virtual del servidor de copia de seguridad
- Especificación de los puntos de recuperación
- Especificación de los detalles de la máquina virtual de destino
- Especificación de la configuración avanzada
- Creación y ejecución de la tarea de restauración
- Verificación de que la instancia de destino se ha restaurado

Revisión de los requisitos previos de BMR

Antes de realizar una reconstrucción completa para las instancias de Linux en Microsoft Azure, considere las siguientes opciones:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado para la restauración, si hay.
- Cuando el destino de la copia de seguridad de una tarea de copia de seguridad es un origen local, para realizar una tarea de restauración completa desde el destino es necesario exportar el destino local del origen a través de NFS o CIFS y también es necesario especificar que el punto de recuperación está disponible en el recurso compartido de NFS o CIFS.
- El punto de recuperación debe ser de la copia de seguridad basada en el agente de Linux.
- Tiene una instancia del Agente de Arcserve UDP para Linux en Microsoft Azure.
- La reconstrucción completa en la máquina virtual de Linux de destino debe tener el mismo sistema de operación que el nodo de origen de Linux.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Creación de un nuevo equipo de Microsoft Azure como destino de la reconstrucción completa

Para la reconstrucción completa en Azure, el usuario puede realizar directamente una reconstrucción completa para la máquina virtual a una máquina virtual de Linux con el mismo sistema de Linux en Azure en lugar de iniciar el nodo de destino con el Live CD del Agente de Arcserve UDP.

En primer lugar, se debe crear una nueva máquina virtual en Azure como nodo de destino de la reconstrucción completa. Se deben comprobar los siguientes requisitos previos.

- Prepare una nueva máquina virtual con el mismo sistema de operación que la máquina virtual que desea realizar una reconstrucción completa.
- Configure el Tipo de autenticación como contraseña para la máquina virtual. Recuerde el nombre de usuario y la contraseña de la máquina virtual.
- Configure el Grupo de recursos como el grupo en el que el servidor de copia de seguridad de Linux realiza la reconstrucción completa. De lo contrario, se produce un error en la reconstrucción completa al crear la conexión SSH entre el servidor de copia de seguridad de Linux y la máquina virtual de destino.

Revisión de la máquina virtual del servidor de copia de seguridad

Para obtener más información, consulte Revisión del servidor de copia de seguridad.

Especificación de los puntos de recuperación

Para obtener más información, consulte Especificación de los puntos de recuperación.

Especificación de los detalles de la máquina virtual de destino

Especifique los detalles de la máquina virtual de destino de la reconstrucción completa para restaurar datos en ese equipo. Una máquina virtual de destino es un equipo de reconstrucción completa donde se realiza una reconstrucción completa. Se necesita la dirección IP, el nombre de usuario y la contraseña de la máquina virtual de destino de la reconstrucción completa que se ha registrado previamente en el inicio de este proceso.

Siga estos pasos:

1. En la pantalla del asistente para la reconstrucción completa de la restauración, especifique los siguientes detalles:
   - Escriba la dirección IP de la máquina virtual de destino de la reconstrucción completa en el campo Dirección IP.
   - Escriba el nombre de usuario y la contraseña de la máquina virtual de destino que se ha creado en Azure.
2. Para obtener información detallada de la máquina virtual:
   - Introduzca un nombre en el campo **Nombre del host**.

     La máquina virtual de destino de la reconstrucción completa utilizará este nombre como nombre del host después de que el proceso de restauración finalice.
   - Compruebe si la opción de DHCP está seleccionada de forma predeterminada como Configuración de la red.

     Nota: Solo DHCP está disponible en Azure. Se configura automáticamente la dirección IP.

     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.
3. (Opcional) Seleccione la opción **Activar la reconstrucción completa instantánea** para poder utilizar el equipo de destino instantáneamente.

   Cuando se activa esta opción, el Agente de Arcserve UDP (Linux) primero recupera todos los datos necesarios requeridos para iniciar el equipo. Después de que se

inicie el equipo de destino, se recuperarán los datos restantes. La conexión de red debe estar disponible constantemente durante la reconstrucción completa instantánea.

Ejemplo: Si se tienen 100 GB de datos, se desea realizar una reconstrucción completa y *no* se selecciona esta opción, primero se recuperarán los 100 GB de datos y, a continuación, se podrá utilizar el equipo de destino. Sin embargo, solo se necesita alrededor de 1 GB de datos para iniciar el equipo. Cuando se activa esta opción, primero se recuperan los datos de 1 GB necesarios para poder iniciar y utilizar el equipo. Una vez iniciado el equipo, se recuperan automáticamente los 99 GB de datos restantes.

Nota: Los datos necesarios para iniciar el equipo dependen de la configuración del sistema operativo. También se puede pausar o reanudar la recuperación automática de los datos si la opción **No recuperar los datos automáticamente después de que se inicie el equipo** no está seleccionada.

4. (Opcional) Seleccione la opción **No recuperar los datos automáticamente después de que se inicie el equipo** para detener la recuperación automática de los datos cuando se inicia el equipo de destino.

   Cuando se selecciona la opción **Activar la reconstrucción completa instantánea**, el comportamiento predeterminado es primero recuperar los datos necesarios e iniciar el equipo. Después de iniciar el equipo, los datos restantes se recuperan automáticamente. Si se actualizan los datos de origen durante la recuperación, seleccionando esta opción se recuperarán los datos hasta el punto anterior a su actualización.

5. Haga clic en **Siguiente**.

   Aparecerá la página **Configuración avanzada**.

   Se han especificado los detalles de la instancia de destino de la reconstrucción completa.

Especificación de la configuración avanzada

Para obtener más información, consulte Especificación de la configuración avanzada.

Creación y ejecución de la tarea de restauración

Para obtener más detalles, consulte Creación y ejecución de la tarea de restauración.

Verificación de que la máquina virtual de destino se ha restaurado

Para obtener más detalles, consulte Verificación de que el nodo de destino se ha restaurado.

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

Una reconstrucción completa de la migración es un proceso de dos partes donde primero se realiza la restauración de los datos en un equipo temporal y, a continuación, se restaurarán al equipo real. Una reconstrucción completa con la opción de reconstrucción completa instantánea activada permite recuperar datos en un equipo temporal. Se puede utilizar el equipo temporal hasta que el equipo real esté listo. Cuando se tiene el equipo real, una reconstrucción completa de la migración permite migrar los datos desde el equipo temporal al equipo real. Al realizar una reconstrucción completa de la migración, los datos que se crean en el equipo temporal se migrarán al equipo real.

Nota: Se puede realizar la reconstrucción completa de la migración con solo una copia de seguridad basada en el agente. Una copia de seguridad sin agente no es compatible con la reconstrucción completa de la migración.

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.

Nota: El equipo se puede iniciar. Solo se configura una tarjeta NIC.

Complete las tareas siguientes para realizar una reconstrucción completa de la migración:

- Revisión de los requisitos previos para la reconstrucción completa de migración
- Realización de una reconstrucción completa en el equipo temporal
- Realización de una reconstrucción completa de la migración
- Verificación de que la máquina de destino se ha restaurado

Revisión de los requisitos previos para la reconstrucción completa de migración

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

- 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.
- El punto de recuperación debe ser de la copia de seguridad basada en el agente de Linux.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Realización de una reconstrucción completa en el equipo temporal

Antes de realizar una reconstrucción completa de la migración, se deben restaurar los datos desde el origen a un equipo temporal. Para restaurar los datos temporalmente, se puede realizar una reconstrucción completa en el equipo temporal. Después de que el equipo temporal esté listo para ser utilizado, se puede continuar trabajando en el equipo temporal.

Cuando el equipo real esté listo, se puede realizar una reconstrucción completa de la migración desde el equipo temporal al equipo real.

Nota: Para obtener más información sobre cómo realizar una reconstrucción completa, consulte Cómo realizar una reconstrucción completa (BMR) para los equipos de Linux.

Siga estos pasos:

1. Acceda al asistente de restauración de una de las formas siguientes:

   - Desde el Arcserve UDP:

   a. Inicie sesión en el Arcserve UDP.

   b. Haga clic en la ficha **recursos**.

   c. Seleccione **Todos los nodos** en el panel izquierdo.

      Se muestran todos los nodos de 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**.

      Se abre 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.

b. Inicie sesión en el Agente de Arcserve UDP (Linux).

2. Haga clic en **Restaurar** en el menú **Asistente** y seleccione **Reconstrucción completa (BMR)**.

   Se abre la página **Servidor de copia de seguridad** del **Asistente de restauración - BMR**.

3. Proporcione todos los detalles en el **Asistente de restauración - Reconstrucción completa** y guarde el asistente.
4. Asegúrese de que se selecciona la casilla de verificación **Activar la reconstrucción completa instantánea** en la página **Equipo de destino** del asistente.
5. Asegúrese de que se selecciona la casilla de verificación **No recuperar los datos automáticamente después de que se inicie el equipo** en la página **Equipo de destino** del asistente.
6. Ejecute la tarea de reconstrucción completa.

   El equipo temporal se recupera utilizando la reconstrucción completa, con la opción de la reconstrucción completa instantánea activada. Se puede utilizar el equipo temporal hasta que el equipo real esté listo.

Realización de una reconstrucción completa de la migración

Cuando el equipo real esté listo, realice una reconstrucción completa de la migración. La reconstrucción completa de la migración restaura los datos originales de la sesión de copia de seguridad y los nuevos datos desde el equipo temporal al equipo real.

Siga estos pasos:

1. Haga clic en **Restaurar** en el menú **Asistente** y seleccione **Reconstrucción completa de la migración**.

   Aparece la página **Servidor de copia de seguridad** del **Asistente de restauración - Reconstrucción completa de la migración**.

2. Proporcione todos los detalles en el **Asistente de restauración - Reconstrucción completa de la migración**.

   Nota: Para obtener más información sobre cómo realizar una reconstrucción completa, consulte Cómo realizar una reconstrucción completa (BMR) para los equipos de Linux.

3. Asegúrese de que la siguiente información se proporciona en la página **Servidor de copia de seguridad** del asistente.

a. Seleccione la tarea de reconstrucción completa instantánea o la tarea de recuperación de la máquina virtual instantánea.

   Servidor local

   Especifica que el servidor de copia de seguridad se gestiona localmente. La tarea de reconstrucción completa para el equipo temporal se ejecuta en el servidor local.

   Servidor remoto

   Especifica que el servidor de copia de seguridad se gestiona remotamente. La tarea de reconstrucción completa para el equipo temporal se ejecuta en el servidor remoto. Se deben proporcionar los detalles del servidor remoto para conectarse al servidor remoto.

b. Seleccione la tarea de restauración en la lista desplegable Nombre de la tarea.

   La lista muestra la tarea de recuperación de la máquina virtual instantánea o la tarea de reconstrucción completa instantánea, que se encuentran en la fase de la tarea Listo para usar o Apagar, una vez que está preparada para usarse.

4. Guarde la tarea de reconstrucción completa.

   En la página principal, la **Fase de la tarea** en la ficha **Estado de la tarea** cambia a **Haga clic aquí para migrar datos**.

5. (Opcional) Inicie el equipo temporal mediante un Live CD cuando el tipo de tarea seleccionada sea la reconstrucción completa instantánea.
6. En la ficha **Estado de la tarea**, haga clic en **Haga clic aquí para migrar datos**.

   Comienza la migración de datos.

   Se ha realizado correctamente una reconstrucción completa de la migración.

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. Compruebe que el equipo de destino tiene toda la información del equipo temporal, incluidos los datos nuevos que haya creado en el equipo temporal.

   El equipo de destino se ha verificado correctamente.

   La reconstrucción completa de la migración se ha ejecutado correctamente en los equipos de Linux basados en agente.

Cómo realizar una reconstrucción completa (BMR) de la migración para los equipos de Linux desde Amazon EC2 al equipo local

Una reconstrucción completa de la migración es un proceso de dos partes donde primero se realiza la restauración de los datos en un equipo temporal y, a continuación, se restaurarán al equipo real. Una reconstrucción completa con la opción de reconstrucción completa instantánea activada permite recuperar datos en un equipo temporal. Se puede utilizar el equipo temporal hasta que el equipo real esté listo. Cuando se tiene el equipo real, una reconstrucción completa de la migración permite migrar los datos desde el equipo temporal al equipo real. Al realizar una reconstrucción completa de la migración, los datos que se crean en el equipo temporal se migrarán al equipo real.

Se puede producir localmente un problema en el servidor de Linux que puede necesitar tiempo de inactividad. A continuación, se puede utilizar la sesión de copia de seguridad para crear la máquina virtual instantánea en Amazon EC2 y utilizar el servidor para proporcionar servicios continuos. Cuando se haya solucionado el problema local, la reconstrucción completa de migración le ayudará a migrar todos los datos desde Amazon EC2 al recurso local, y se restaurará el servidor local para proporcionar de nuevo el servicio necesario.

Nota: Se puede realizar la reconstrucción completa de la migración con solo una copia de seguridad basada en el agente. Una copia de seguridad sin agente no es compatible con la reconstrucción completa de la migración.

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.

Nota: El equipo se puede iniciar. Solo se configura una tarjeta NIC.

Complete las tareas siguientes para realizar una reconstrucción completa de la migración:

- Revisión de los requisitos previos para la reconstrucción completa de migración
- Realización de una reconstrucción completa de la migración
- Verificación de que la máquina de destino se ha restaurado

Revisión de los requisitos previos para la reconstrucción completa de migración

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

- 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.
- El punto de recuperación debe ser de la copia de seguridad basada en el agente de Linux.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Realización de una migración de la reconstrucción completa desde Amazon EC2 al equipo local

Antes de realizar una reconstrucción completa de la migración desde Amazon EC2, se deben restaurar los datos desde el origen a una instancia de EC2. Para restaurar los datos temporalmente, se puede realizar una máquina virtual instantánea en la instancia de EC2. Después de que la instancia de EC2 esté lista para ser utilizada, se puede continuar trabajando en la instancia.

Cuando el equipo local real esté listo, se puede realizar una reconstrucción completa de la migración desde la instancia de Amazon EC2 al equipo local real.

Nota: Para obtener más información sobre cómo realizar una reconstrucción completa, consulte Cómo realizar una reconstrucción completa (BMR) para los equipos de Linux.

Siga estos pasos:

1. Acceda al asistente de restauración de una de las formas siguientes:

   - Desde el 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 de 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**.

      Se abre 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.

b. Inicie sesión en el Agente de Arcserve UDP (Linux).

2. Haga clic en **Restaurar** en el menú **Asistente** y seleccione **Reconstrucción completa de la migración**.

   Aparece la página **Servidor de copia de seguridad** del **Asistente de restauración - Reconstrucción completa de la migración**.

3. Realice los siguientes pasos y haga clic en **Siguiente**:

   a. Seleccione **Servidor remoto** como la ubicación del servidor.

   b. Especifique el servidor de copia de seguridad de Linux en Amazon EC2 para conectarse al servidor.

   c. Introduzca el nombre de host, el nombre de usuario, la contraseña, el protocolo y el puerto del servidor de copia de seguridad de Linux.

   d. Haga clic en **Actualizar** y seleccione la tarea de restauración en la lista desplegable **Nombre de la tarea**.

      La lista muestra la tarea de recuperación de la máquina virtual instantánea que se encuentra en la fase de la tarea **Listo para usar** o **Apagar**, una vez que está preparada para usarse.

   Aparece la sección Puntos de recuperación.

4. En la sección **Puntos de recuperación**, realice los pasos siguientes y haga clic en **Conectar**.

   - Especifique el **Servidor de puntos de recuperación** que se ha creado localmente.
   - Seleccione el almacén de datos correspondiente.

     El equipo se cargará automáticamente según la tarea de máquina virtual instantánea.
   - Seleccione la sesión y haga clic en **Siguiente**.

   Se le llevará automáticamente a la ficha **Equipo de destino**.

5. En la sección Equipo de destino, introduzca la dirección MAC/IP y haga clic en **Siguiente**.

   Nota: Se puede iniciar un equipo local con el Live CD para obtener la dirección MAC/IP.

   Se abre la sección Opciones avanzadas.

6. En la sección **Opciones avanzadas**, configure los Scripts anteriores/posteriores y, a continuación, haga clic en Siguiente.

   Aparecerá la sección **Resumen**.

7. Especifique el nombre de la tarea y haga clic en **Enviar**.

   Se realiza una tarea de reconstrucción completa en el equipo que se ha reiniciado con Live CD.

8. En la página principal del Agente de Linux, vaya a la ficha **Estado de la tarea** y haga clic en **Haga clic aquí para migrar los datos.**

   Se migran los datos de la máquina virtual de Amazon EC2 al equipo local.

   Se ha realizado correctamente una reconstrucción completa de la migración.

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. Compruebe que el equipo de destino tiene toda la información del equipo temporal, incluidos los datos nuevos que haya creado en el equipo temporal.

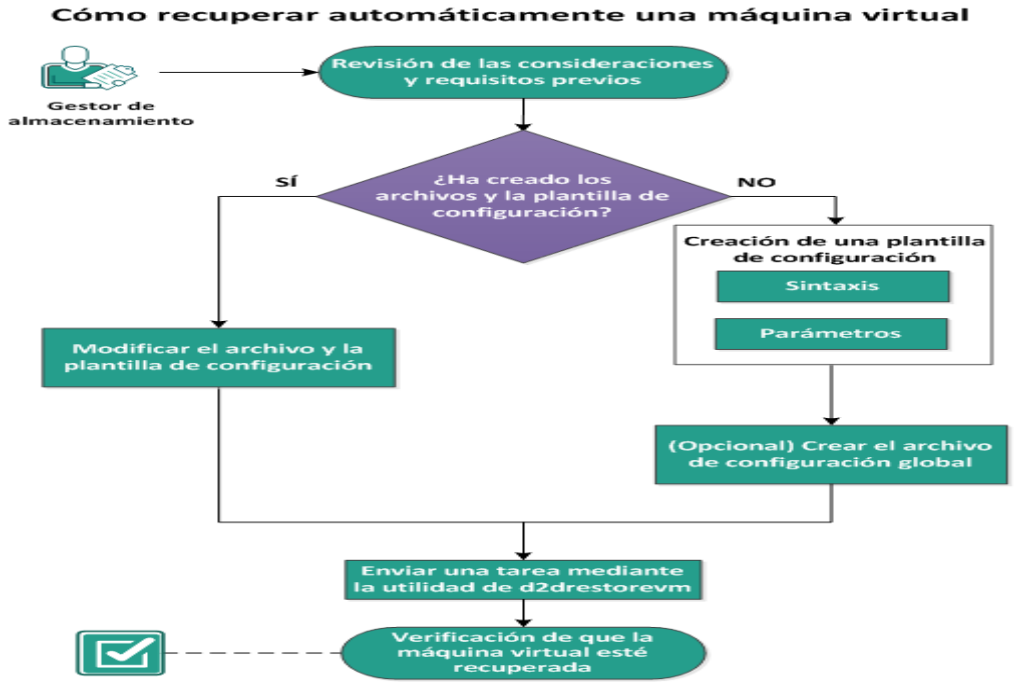
   El equipo de destino se ha verificado correctamente.

   La reconstrucción completa de la migración se ha ejecutado correctamente en los equipos de Linux basados en agente.

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 o una reconstrucción completa instantánea sin 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:



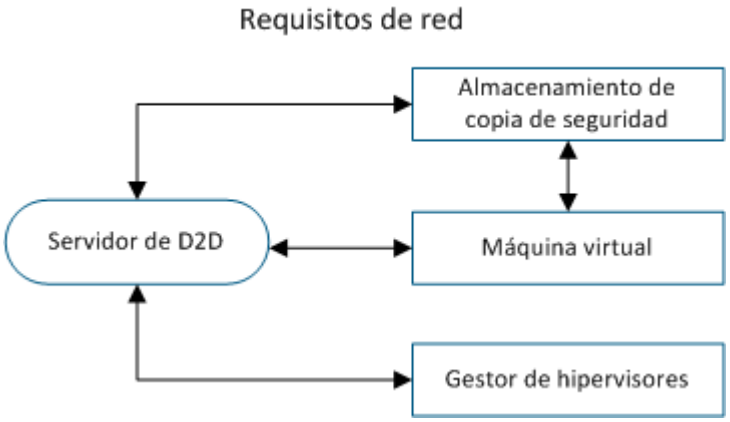
Realice estas tareas para recuperar automáticamente una máquina virtual:

- Revisión de las consideraciones y los requisitos previos
- Creación de una plantilla de configuración
- (Opcional) Creación del archivo de configuración global
- Modificación del archivo y de la plantilla de configuración
- Envío de una tarea mediante la utilidad de d2drestorevm
- Verificación de que la máquina virtual esté recuperada

Revisión de las consideraciones y requisitos previos

Revise los requisitos previos siguientes antes de restaurar la máquina virtual:

- Las versiones siguientes de los hipervisores admiten la reconstrucción completa o la máquina virtual instantánea mediante la utilidad d2drestorevm:
  - XenServer 6.0 y posterior (restaurar la máquina virtual mediante el método de la reconstrucción completa normal)
  - OVM 3.2 (restaurar la máquina virtual mediante el método de la reconstrucción completa normal)
  - VMware vCenter/ESX 5.0 o posterior (enviar la tarea de máquina virtual instantánea)
  - Windows Hyper-V Server 2012 o posterior (enviar la tarea de máquina virtual instantánea)
  - Nutanix AHV 5.5.3.1 o posterior (enviar la tarea de máquina virtual instantánea)
- 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 o en la máquina virtual de Oracle (OVM).
- 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.
- 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 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 al restaurar a Xen u OVM:

  `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, las bases de datos y los exploradores compatibles.

Revise las siguientes consideraciones antes de restaurar la máquina virtual:

- Se recomienda restaurar las sesiones de la versión anterior del Agente de Arcserve UDP (Linux) o de Arcserve UDP 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 para virtualización (PV) se pueden restaurar solamente en una máquina virtual de destino de PV de XenServer y OVM.
- 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 hace referencia a la contraseña que se debe especificar.

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 de hipervisores válidos son Xen y OVM.

   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.

vm_svr_password

Especifica la contraseña del hipervisor. La contraseña se cifra utilizando la utilidad de cifrado d2dutil.

vm_sub_server

Especifica el nombre del servidor ESX cuando se restaura a vCenter o especifica el nombre del clúster de Prism Element cuando se restaura a Prism Central.

vm_svr_protocol

Especifica el protocolo del hipervisor cuando se restaura a vCenter/ESX(i) o AHV.

vm_svr_port

Especifica el puerto del hipervisor cuando se restaura a vCenter/ESX(i) o AHV.

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.

vm_memory

Especifica la memoria de la máquina virtual en MB cuando se restaura a vCenter/ESX(i), Hyper-V o AHV.

vm_cpu_count

Especifica el recuento de CPU de la máquina virtual cuando se restaura a vCenter/ESX(i), Hyper-V o AHV.

vm_resource_pool

Especifica la agrupación de recursos del hipervisor cuando se restaura a vCenter/ESX(i) o AHV.

vm_datastore

Especifica el almacén de datos del hipervisor cuando se restaura a vCenter/ESX(i) o AHV.

storage_location_type

Especifica el tipo de ubicación de almacenamiento de la sesión. La ubicación de almacenamiento puede ser CIFS, NFS o RPS.

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.

rps_server

Especifica el nombre del servidor de puntos de recuperación cuando **storage_location_type** es RPS.

rps_server_username

Especifica el nombre de usuario del servidor de puntos de recuperación cuando **storage_location_type** es RPS.

rps_server_password

Especifica la contraseña del servidor de puntos de recuperación cuando **storage_location_type** es RPS. La contraseña se cifra utilizando la utilidad de cifrado d2dutil.

rps_server_protocol

Especifica el protocolo del servidor de puntos de recuperación cuando **storage_location_type** es RPS.

rps_server_port

Especifica el puerto del servidor de puntos de recuperación cuando **storage_location_type** es RPS.

rps_server_datastore

Especifica el nombre del almacén de datos del servidor de puntos de recuperación cuando **storage_location_type** es RPS.

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 IP estática.

guest_dns

Especifica la dirección de DNS 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.

enable_instant_restore

(Opcional) Especifica la activación de la restauración instantánea. Los valores son sí y no.

auto_restore_data

(Opcional) Especifica la restauración de datos automáticamente. Los valores son sí y no.

script_pre_job_server

(Opcional) Especifica el script que se debe poner en marcha antes de ejecutar la tarea en el servidor.

script_post_job_server

(Opcional) Especifica el script que se debe poner en marcha después de ejecutar la tarea en el servidor.

script_pre_job_client

(Opcional) Especifica el script que se debe poner en marcha antes de ejecutar la tarea en el cliente.

script_post_job_client

(Opcional) Especifica el script que se debe poner en marcha después de ejecutar la tarea en el cliente.

script_ready_to_use

(Opcional) Especifica el script que se debe ejecutar cuando el equipo de destino está listo para su uso y cuando el valor del parámetro **enable_instant_restore** es Sí.

force

Especifica si se debe forzar o no la restauración de la máquina virtual. Los valores son sí y no.

Valor predeterminado: no

exclude_volumes

Especifica los volúmenes que se deben excluir para la máquina virtual de destino.

No excluya el volumen '/'. Utilice ':' para separar varios volúmenes.

include_volumes

Especifica los volúmenes que se deben incluir para la máquina virtual de destino.

Se deben incluir los siguientes volúmenes: / , /boot, /boot/efi, /home, /usr, /usr/local. Utilice ':' para separar varios volúmenes.

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/Arcserve/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.

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 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/Arcserve/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/Arcserve/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 d2dres-torevm

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:

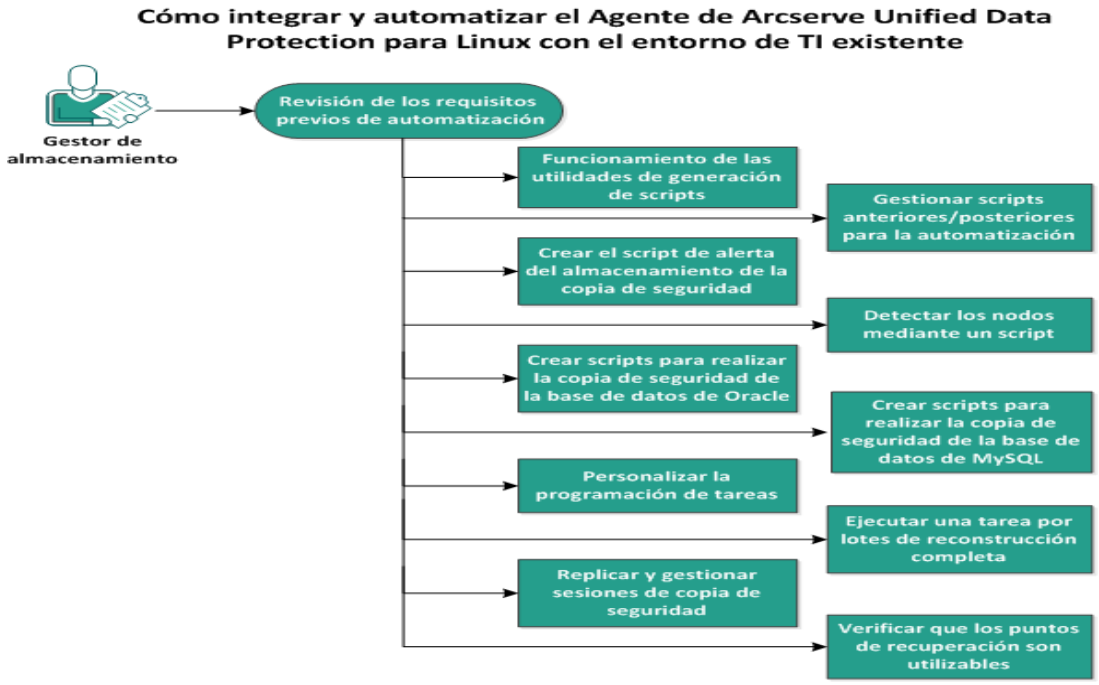
1. Vaya a la máquina virtual que se ha restaurado.
2. Verifique que la VM dispone de toda la información de la cual se ha realizado copia de seguridad.

   La máquina virtual se ha verificado correctamente.

Cómo integrar y automatizar el Arcserve UDP 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
- Funcionamiento de las utilidades de generación de scripts
- Gestión de scripts anteriores/posteriores para la automatización
- Creación del script de alerta del almacenamiento de la copia de seguridad
- Detección de los nodos mediante un script

- Creación de scripts para realizar la copia de seguridad de la base de datos de Oracle
- Creación de scripts para realizar la copia de seguridad de la base de datos de MySQL
- Utilización de scripts para realizar copias de seguridad y restauraciones de la base de datos de PostgreSQL
- Personalización de la programación de tareas
- Ejecución de una tarea por lotes de reconstrucción completa
- Replicación y gestión de sesiones de copia de seguridad
- Verificación de que los puntos de recuperación son utilizables

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, las bases de datos y los exploradores compatibles.

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/Arcserve/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 hace referencia a la contraseña que se debe especificar.

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/Arcserve/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, elcomando ./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=nombrenodo -- user=nombreusuario --password=contraseña --rootuser=cuentaroot --rootpwd=contraseñaroot --pwdfile=rutaarchivocontraseñas --description=descripción --attach=nombretarea –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=nombrenodo -- user=nombreusuario --
password=nuevacontraseña --rootuser=cuentaroot --rootpw-
d=nuevacontraseñaroot --pwdfile=rutaarchivocontraseñas -
-description=nuevadescripción
```

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 y 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 ámbito (intervalo) entre 192.168.1.100 y 192.168.1.254. Aquí no se debe mencionar el final del intervalo.

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. Cada entrada se separa por una coma.

--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 los 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 y 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 enviar una tarea de restauración de archivo:

   ```
   d2drestorefile --createtemplate=file
   ```

   Especifica la creación de una plantilla. Una vez creada la plantilla, se puede modificar. El comando d2drestorefile utiliza esta plantilla. Se pueden definir valores en esta plantilla. El comando d2drestorefile lee la plantilla y proporciona el resultado como se especifica en esta.

   ```
   d2drestorefile --template=restore_template [--wait]
   ```

   Especifica el envío de la tarea de restauración de archivo. Si se incluye el parámetro [--wait] en el comando, el mensaje de estado aparecerá solo después de que finalice la tarea de restauración.

5. Ejecute los comandos siguientes para gestionar las tareas:

   ```
   # ./d2djob
   ```

   Aparece una lista de comandos para facilitar la gestión de tareas. Mediante este comando, se pueden ejecutar, cancelar y suprimir tareas.

   ```
   # ./d2djob --delete=jobname
   ```

   Suprime la tarea especificada de la ficha Estado de la tarea.

   ```
   # ./d2djob --run=jobname --jobtype=1 --recoverysetstart --
   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.

El parámetro --recoverysetstart es opcional. Si se especifica esta opción, la copia de seguridad actual se convierte en una copia de seguridad completa y se marca como el primer punto de recuperación del conjunto de recuperación si el conjunto de recuperación no está disponible.

```
# ./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 --tar-
get=macaddress/ipaddress --hostname=hostname --netwo-
rk=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, no se debe proporcionar ningún valor para *--staticip, --subnet* ni *--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>
```

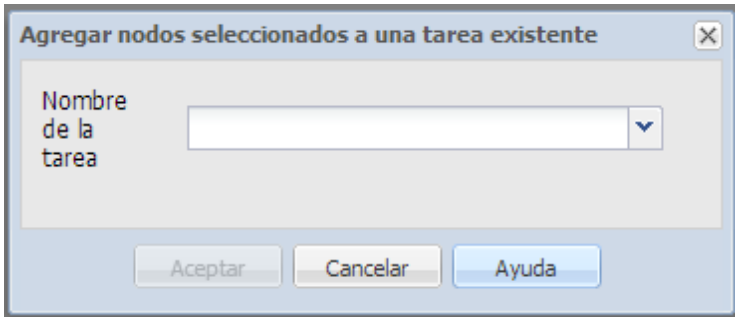
Exporta varias tareas del servidor de copia de seguridad a un archivo. Si desea tener configuraciones de copia de seguridad parecidas en varios servidores de copia de seguridad, se pueden exportar las tareas de copia de seguridad a un archivo y, a continuación, importar el archivo a otros servidores 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
```

6. 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-
   e=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-
e=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=r-
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.

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 --for-
mat=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 --for-
mat=column/csv/html
```

Muestra el historial de tareas reciente en función de los meses especificados.

```
# ./d2djobhistory --starttime=aaaammdd --endtime=aaaammdd -
-headers=nombre_columna1, nombre_columna2,...nombre_
columna_X --width=valor_ancho --format=column/csv/html
```

Muestra el historial de tareas reciente en función de la fecha de inicio y de finalización especificada.

```
# ./d2djobhistory --starttime=aaaammdd --endtime=aaaammdd -
-headers=nombre_columna1, nombre_columna2,...nombre_
columna_X --width=valor_ancho --format=column/csv/html
```

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.

D2D_RECOVERYPOINT

Identifica el punto de recuperación creado por la tarea de copia de seguridad. Este valor solo es aplicable en el script posterior a la copia de seguridad.

D2D_RPSSCHEDULETYPE

Identifica el tipo de programación cuando se realiza la copia de seguridad en un almacén de datos en el servidor de puntos de recuperación. Los siguientes valores identifican la variable D2D_ RPSSCHEDULETYPE:

diariamente

Identifica la programación como una copia de seguridad diaria.

semanalmente

Identifica la programación como una copia de seguridad semanal.

mensualmente

Identifica la programación como una copia de seguridad mensual.

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/Arcserve/d2dserver/usr/prepost
```

Siga estos pasos:

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

   ```
   /opt/Arcserve/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.

   Esta sección incluye los siguientes temas:

   - Ejemplo de creación de scripts definidos por el usuario

Ejemplo de creación de scripts definidos por el usuario

La variable de entorno D2D_JOBSTAGE, que tiene cuatro etapas diferentes, es muy importante para escribir el script. En la fase pre_share, se pueden hacer algunos preparativos o implementar el método de acceso. En la fase post_share, también se puede implementar el método de acceso y realizar algunas otras cosas. La diferencia entre las dos fases es que la ruta indicada de D2D_SHARE_PATH está disponible en la fase post_share. Las fases pre_cleanup y post_cleanup ofrecen la posibilidad de limpiar los recursos que se han asignado o romper las conexiones a la ruta compartida. La diferencia entre las dos fases es que la ruta indicada de D2D_SHARE_PATH está disponible en la fase pre_cleanup y no está disponible en la fase post_cleanup.

Notas:

- Se puede leer la contraseña que se establece para el usuario en la interfaz de usuario web en la entrada estándar.
- Los códigos se ejecutan mediante diferentes procesos en una fase diferente. Por tanto, si se desea compartir datos en una fase diferente, se tendrá que utilizar un recurso global como, por ejemplo, una base de datos o un archivo temporales.

Ejemplo: Creación de scripts definidos por el usuario

Nota: El script SFTP se utiliza como ejemplo en el directorio examples/sharerp.

```
#!/bin/bash
function pre_sftp_share()
{
local share_path=${D2D_SHARE_PATH}
local user_name=${D2D_SHARE_USER}
local pass_word=""

# Read pass word from standard input.
read -s pass_word

# Check user whether exist.
if grep $user_name /etc/passwd >/dev/null 2>&1; then
    return 1
fi
```

```
# Add new user.
useradd $user_name -d $share_path >/dev/null 2>&1
[ $? -ne 0 ] && return 2

# Set pass word for the user.
echo -e "$pass_word\n$pass_word"|passwd "$user_name" >/dev/null 2>&1
[ $? -ne 0 ] && return 3

return 0
}

function post_sftp_share()
{
return 0
}

function pre_sftp_cleanup()
{
return 0
}

function post_sftp_cleanup()
{
local user_name=${D2D_SHARE_USER}

# Delete the user.
userdel $user_name >/dev/null 2>&1

return 0
}

# Main
################################################################
ret=0
stage=${D2D_JOBSTAGE}
case $stage in
pre_share)
```

```
pre_sftp_share
ret=$?
;;

post_share)
post_sftp_share
ret=$?
;;

pre_cleanup)
pre_sftp_cleanup
ret=$?
;;

post_cleanup)
post_sftp_cleanup
ret=$?
;;
esac

exit $ret
```

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/Arcserve/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/Arcserve/d2dserver/examples/discovery
```

Se puede copiar el script de muestra en la ubicación siguiente y modificar el script por el requisito:

/opt/Arcserve/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/Arcserve/d2dserver/usr/discovery
   ```

3. Proporcione los permisos de ejecución necesarios al archivo de script.
4. Inicie sesión en la interfaz web del .
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

connect / as 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

connect / as 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/Arcserve/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 el Agente de Arcserve UDP (Linux).

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/Arcserve/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.

Esta sección incluye los siguientes temas:

- Realización de una reconstrucción completa de MySQL Server
- Realización de la recuperación de la base de datos de MySQL

Realización de una reconstrucción completa de MySQL Server

Una reconstrucción completa (BMR) 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 usando el Live CD del Agente de Arcserve UDP (Linux), se puede obtener la dirección IP del equipo de destino.

Si MySQL Server se corrompe, se puede restaurar el servidor entero a través de una reconstrucción completa.

Para restaurar MySQL Server, realice los siguientes 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.

   MySQL Server se ha recuperado correctamente.

Realización de la recuperación de la base de datos de MySQL

Cuando se pierde o se daña una base de datos de MySQL, se puede realizar una recuperación de nivel de archivo para restaurar la base de datos específica.

Siga estos pasos:

1. Inicie sesión en el servidor de destino como usuario raíz.
2. Detención del servicio de MySQL
3. Para restaurar en la ubicación original:
    1. Suprima archivos y directorios de la carpeta actual de la base de datos de MySQL
    2. Restaure la carpeta de la base de datos desde el punto de recuperación a la carpeta de la base de datos de MySQL.
4. Inicie el servicio de MySQL.

   La base de datos se ha recuperado correctamente.

Utilización de scripts para realizar copias de seguridad y restauraciones de la base de datos de PostgreSQL

Están disponibles los siguientes scripts para realizar la copia de seguridad de la base de datos de PostgreQL. Al ejecutar los scripts, no se tiene que detener la base de datos para realizar una copia de seguridad.

- **postgresql_backup_pre.sh:** Este script coloca la base de datos en modo de copia de seguridad.
- **postgresql_snapshot_post.sh:** Este script elimina la base de datos del modo de copia de seguridad.
- **postgresql_settings:** Se trata de un archivo de configuración donde es posible que sea necesario actualizar las variables de PostgreSQL.
- **postgresql_backup_post.sh:** Este script actualiza el registro sobre el estado de la copia de seguridad.

Requisitos previos

Antes de iniciar la copia de seguridad, asegúrese de realizar los siguientes pasos:

- El nivel de WAL se establece en archivo de archivado (o hot_standby)
- archive_mode está activado
- Se debe configurar archive_command para especificar la ubicación del archivo de archivado.

Nota: Para aplicar los valores de configuración, reinicie el servidor después de configurar estos valores en el archivo postgresql.conf.

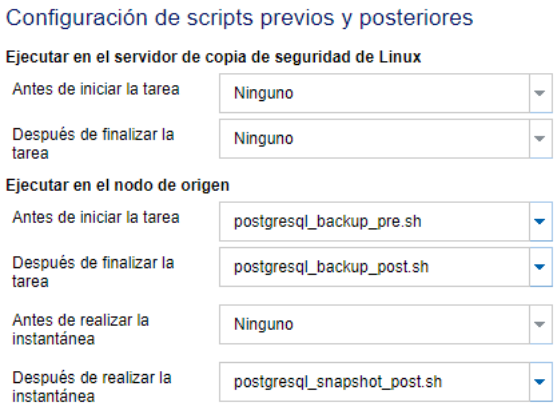
Los siguientes comandos sirven para comprobar el estado del modo de archivo de archivado después del reinicio:

- show archive_mode
- show archive_command
- show WAL level

Aplicación de scripts

Siga estos pasos:

1. Extraiga el archivo LinuxPostgres.zip que contiene los siguientes cuatro archivos: postgresql_backup_pre.sh, postgresql_snapshot_post.sh, postgresql_settings y postgresql_backup_post.sh
2. Copie los archivos de una instantánea o copia de seguridad previa/posterior en la siguiente ruta del servidor de copia de seguridad de Linux: /opt/Arcserve/d2dserver/usr/prepost.
3. Copie postgresql_settings en la ruta del origen /root/backup.
4. Asegúrese de comprobar postgresql_settings para todos los valores configurados con las variables y realice modificaciones en los cambios necesarios según su entorno.
5. Configure el plan desde la Consola de UDP y seleccione el nodo de PostgreSQL como origen.



6. Confirme el estado de la copia de seguridad. Para conocer el estado de la copia de seguridad de PostgreSQL, consulte el archivo arcserve_postgresql_backup_${DATE}.log. Este archivo de registro se creará en el directorio definido por el usuario. Para obtener más información sobre la configuración del directorio, consulte el archivo postgresql_settings.

Restauración de la base de datos de PostgreSQL

Siga estos pasos:

1. Detenga el servidor de la base de datos.
2. Para restaurar la ubicación original, realice los siguientes pasos:
   a. Suprima archivos y directorios de la carpeta /data actual.
   b. Realice una restauración de toda la carpeta /data.

3. Suprima los archivos de las siguientes carpetas después de la finalización de la restauración desde la carpeta /data:
   - pg_dynshmem/
   - pg_notify/
   - pg_serial/
   - pg_snapshots/
   - pg_stat_tmp/
   - pg_subtrans/
   - pg_internal.init
4. Vaya a la carpeta que se ha configurado para el archivado de WAL y realice los siguientes pasos:
   a. Suprima los archivos que se encuentran en el directorio pg_wal restaurado, que contiene la información relacionada con las transacciones que se han realizado durante la copia de seguridad.
   b. Ahora, copie los archivos desde la ubicación de archivo de archivado definida por el usuario en la carpeta de pg_wal, para la recuperación de datos y la consistencia de los datos en el momento.
5. Inicie el servidor de la base de datos.

Restauración en una ubicación alternativa en el mismo servidor

1. Detenga el servidor de la base de datos.
2. Ejecute PGDATA utilizando la configuración new_data_directory_path.
3. Inicialice la base de datos recientemente creada utliizando el comando initdb.
4. Suprima archivos y directorios de la carpeta /data actual.
5. Realice una restauración de toda la carpeta /data.
6. Suprima los archivos de las siguientes carpetas después de la finalización de la restauración desde la carpeta /data:
   - pg_dynshmem/
   - pg_notify/
   - pg_serial/
   - pg_snapshots/

- pg_stat_tmp/
- pg_subtrans/
- pg_internal.init

7. Vaya a la carpeta configurada para el archivado de WAL y, a continuación, realice los siguientes pasos:
   a. Suprima los archivos que se encuentran en el directorio pg_wal restaurado, que contiene la información relacionada con las transacciones que se han realizado durante la copia de seguridad.
   b. Ahora, copie los archivos desde la ubicación de archivo de archivado definida por el usuario en la carpeta de pg_wal, para la recuperación de datos y la consistencia de los datos en el momento.
8. Inicie el servidor de la base de datos.

   Nota: Asegúrese de que el inicio de la base de datos se realiza en la sesión en la que se ha actualizado PGDATA.

Limitaciones

Los scripts anteriores no ayudarán a realizar la copia de seguridad si la base de datos de PostgreSQL está configurada con un puerto no predeterminado. Los scripts solo funcionan con el número de puerto predeterminado 5432.

Como solución alternativa, utilice las recomendaciones siguientes para modificar de forma manual los scripts postgresql_backup_pre.sh y postgresql_snapshot_post.sh:

- postgresql_backup_pre.sh:

  Original: sudo -u ${USERNAME} -H -- psql -c "SELECT pg_start_backup ('Arcserve UDP backup - ${DATE} $(timestamp)', true)" >> ${LOG} 2>&1

  Modificado: sudo -u ${USERNAME} -H -- psql -p 5432 -c "SELECT pg_start_backup('Arcserve UDP backup - ${DATE} $(timestamp)', true)" >> ${LOG} 2>&1
- postgresql_snapshot_post.sh:

  Original: sudo -u ${USERNAME} -H -- psql -c "SELECT pg_stop_backup()" >> ${LOG} 2>&1

  Modificado: sudo -u ${USERNAME} -H -- psql -p 5432 -c "SELECT pg_stop_backup()" >> ${LOG} 2>&1

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 interfaz de usuario 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/Arcserve/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/Arcserve/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/Arcserve/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".

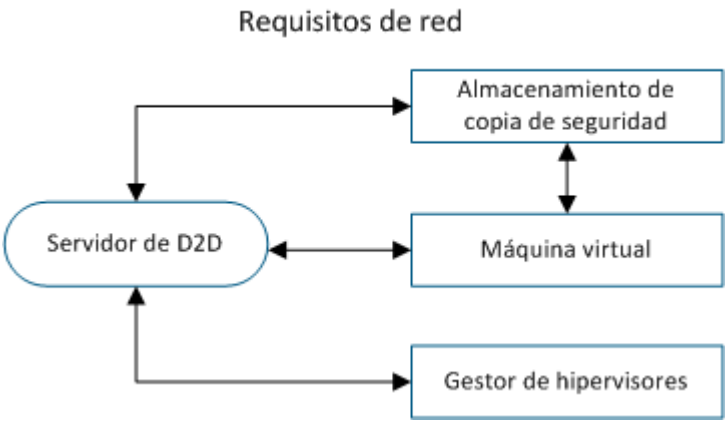
- Revise los requisitos de red.
- Identifique una red en la cual las máquinas virtuales estén conectadas.

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
- 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 d2d-verify.

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 siguientes tipos de hipervisores son válidos: xen u ovm.

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

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
- Configurar el historial de tareas y los valores de configuración de retención del registro de actividades
- Configurar los valores de configuración de retención del registro de depuración
- Configuración de la duración del tiempo de espera de la IU
- Cambio del número de puerto SSH del servidor de copia de seguridad
- Gestión de los conjuntos de recuperación
- Desactivación de los servicios de BOOTPD y TFTPD
- Mejora del rendimiento de consultas para el historial de tareas y el registro de actividades
- Omisión de la verificación del cliente de CIFS y NFS
- Omisión de la validación de CIFS y NFS en el servidor de copia de seguridad de Linux
- Configuración de la carpeta temporal predeterminada
- Configuración de la ruta de instantáneas para el nodo de copia de seguridad
- Configuración de la información de conexión del servidor Hyper-V para la máquina virtual instantánea

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, las bases de datos y los exploradores compatibles.

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/Arcserve/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/Arcserve/d2dserver/configfiles/server.cfg
   ```

   Nota: De forma predeterminada, se retienen el historial de tareas y los registros de actividad durante 90 días.

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/Arcserve/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>`

   Ejemplo:

   El valor debe estar en minutos. El límite máximo para el valor de tiempo de espera de la IU es 60.

   `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 pre-determinada (SSH) para conectarse a los nodos. Si desea cambiar el puerto pre-determinado 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/Arcserve/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/Arcserve/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/Arcserve/d2dserver/configfiles/server.env
   ```

   Nota: Si el archivo server.env no está presente, créelo.
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/Arcserve/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/Arcserve/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:

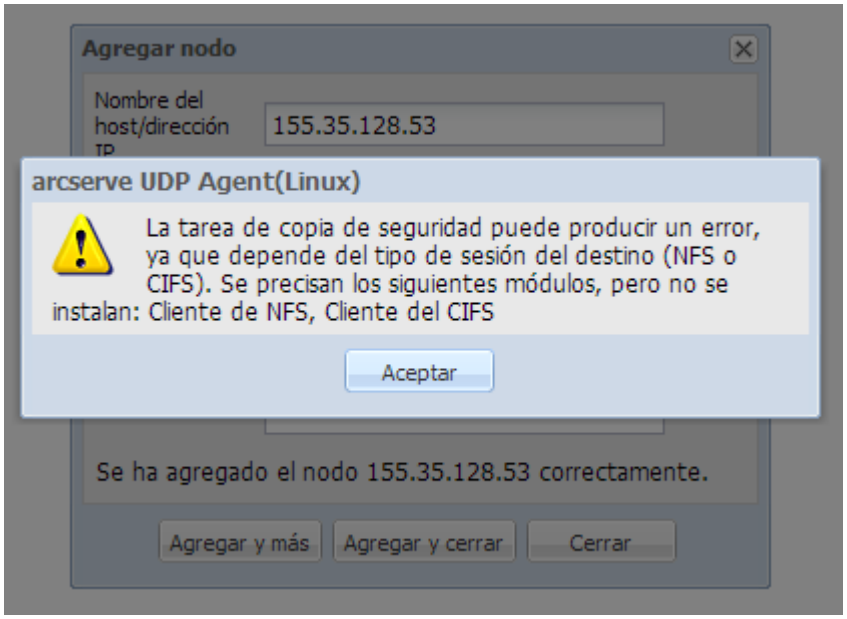
     ```
     skip_getting_activity_log_count=true
     ```

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 módulo 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/Arcserve/d2dserver/configfiles/server.cfg`

3. Agregue el siguiente parámetro:

   `skip_client_check=nfs,cifs`

   El ejemplo proporcionado omite la verificación de los módulos NFS y CIFS en el nodo de destino. Cuando se proporcionan los dos módulos, la verificación se omite para ambos. Cuando solo se proporciona un módulo, la verificación se omite solo para ese módulo.

4. Guarde el archivo server.cfg.

   La verificación se omite para los módulos CIFS y NFS.

Omisión de la validación de CIFS y NFS en el servidor de copia de seguridad de Linux

Cuando se agrega o modifica el almacenamiento de la copia de seguridad, el servidor de copia de seguridad valida si CIFS o NFS es accesible en el servidor de copia de seguridad de Linux. Si se desea omitir esta validación en el servidor de copia de seguridad de Linux, se puede configurar el archivo server.env.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra el archivo server.env:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.env
   ```

   Nota: Si el archivo no está presente, cree el archivo server.env.
3. Agregue la siguiente línea en el archivo server.env:

   ```
   export skip_validate_backup_storage_on_server=true
   ```
4. Reinicie el servidor de copia de seguridad.

Configuración de la carpeta temporal predeterminada

Cuando se realizan copias de seguridad de nodos de Linux, se usa la carpeta predeterminada **/tmp** para almacenar los registros de depuración, los registros de datos temporales de la instantánea y los registros binarios necesarios. La carpeta /tmp debe disponer de suficiente espacio libre y de los permisos necesarios para ejecutar los archivos binarios. Para cambiar la ruta predeterminada en los nodos de Linux, se puede configurar el archivo server.env y especificar las nuevas rutas.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra el archivo server.env:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.env
   ```

   Nota: Si el archivo no está presente, cree el archivo server.env.

3. Para configurar la ruta de ejecución del Agente de nodo de Linux, agregue la línea siguiente en el archivo server.env:

   ```
   export TARGET_BOOTSTRAP_DIR=<ruta>
   ```

   Ejemplo: Para implementar el Agente de Linux en la ruta **/d2dagent** introduzca la siguiente línea:

   ```
   export TARGET_BOOTSTRAP_DIR=/d2dagent
   ```

   Nota: De forma predeterminada, se implementa el Agente y se ejecuta en la carpeta /tmp.

4. Para configurar la ruta del almacén de los datos temporales de la instantánea y del registro de depuración del nodo de Linux, agregue la línea siguiente en el archivo server.env:

   ```
   export TARGET_ WORK_DIR=<ruta>
   ```

   Ejemplo: Para configurar los registros de depuración y los datos temporales de la instantánea en la ruta **/d2dagentlogs**, introduzca la línea siguiente:

   ```
   export TARGET_WORK_DIR=/d2dagentlogs
   ```

   Nota: De forma predeterminada, se implementa el Agente y se ejecuta en la carpeta /tmp.

5. Reinicie el servidor de copia de seguridad.

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

Se configura la carpeta temporal predeterminada.

Configuración de la ruta de instantáneas para el nodo de copia de seguridad

Cuando se realizan copias de seguridad de nodos de Linux, se usa la carpeta predeterminada **/tmp** para almacenar el archivo de instantáneas del disco. La carpeta **/tmp** debe tener suficiente espacio libre. Para cambiar la ruta de instantáneas en los nodos de Linux, puede configurar un archivo específico para nodos e indicar la nueva ruta.

Siga estos pasos:

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

   `/opt/Arcserve/d2dserver/configfiles/node`

   Nota: Si la carpeta no está presente, créela.

   La carpeta **nodo** contiene el archivo <nombre_nodo>.cfg. Cada nodo cuenta con su propio archivo .cfg.

3. Para configurar la ruta de instantáneas del nodo de Linux, agregue la línea siguiente en el archivo <nombre_nodo>.cfg específico:

   `target_snapshot_dir=<ruta>`

   Nota: Si el archivo <nombre_nodo>.cfg no está presente, créelo.

   Ejemplo: Si el nombre del nodo es **d2dbackupnode** y desea almacenar la instantánea en la ruta **/d2dsnapshot**, abra el archivo .cfg siguiente:

   `/opt/Arcserve/d2dserver/configfiles/node/d2dbackupnode.cfg`

   Agregue la línea siguiente:

   `target_snapshot_dir=/d2dsnapshot`

   Se ha configurado la carpeta de instantáneas en el nodo de destino.

Configuración de la información de conexión del servidor Hyper-V para la máquina virtual instantánea

Cuando se envían tareas de la máquina virtual instantánea para nodos de Linux, el servidor de copia de seguridad intenta detectar automáticamente el servidor Hyper-V. Sin embargo, si se produce un error en el proceso, se puede realizar una verificación para asegurarse de que se está utilizando la información correcta de la conexión al servidor Hyper-V.

La máquina virtual instantánea de Linux es compatible con Hyper-V con SMB 2.0 o posterior para evitar las vulnerabilidades de SMB 1.0.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Vaya a la siguiente carpeta de Hyper-V:

   `/opt/Arcserve/d2dserver/configfiles/hyperv`

   Nota: Si la carpeta no está presente, créela. La carpeta de Hyper-V contiene el archivo <nombre_servidor_hyperv_en_mayúsculas>.cfg. Cada servidor Hyper-V cuenta con su propio archivo .cfg.
3. Para configurar la información de conexión de Hyper-V, agregue las línea siguientes en el archivo <nombre_servidor_hyperv_en_mayúsculas>.cfg específico:

   protocol=<HTTP|HTTPS>

   port=<número>

   Nota: Si el archivo <nombre_servidor_hyperv_en_mayúsculas>.cfg no está presente, créelo.

   Para el protocolo y número de puerto, acceda al servidor Hyper-V mediante la siguiente línea de comandos:

   winrm enumerate winrm/Config/Listener

   Por ejemplo, si el nombre del servidor Hyper-V de destino es la máquina virtual instantánea de Hyper-V y WinRM en el servidor Hyper-V está configurado como HTTPS en escucha en el puerto 5986, abra el archivo .cfg siguiente:

   /opt/Arcserve/d2dserver/configfiles/hyperv/IVM-HYPERV.cfg

   Agregue las líneas siguientes:

   protocol=HTTPS

port=5986

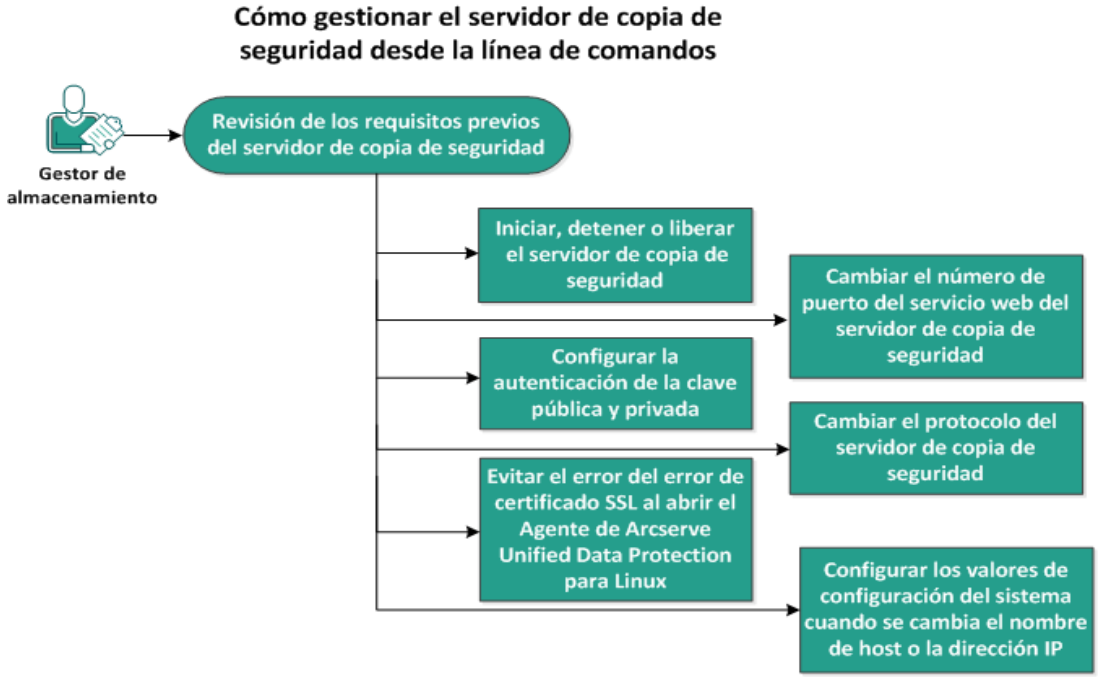
La información de conexión del servidor Hyper-V está configurada.

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
- Inicio, detención o liberación del servidor de copia de seguridad
- Cambio del número de puerto del servicio web del servidor de copia de seguridad
- Configuración de la autenticación de la clave pública y privada
- Cambio del protocolo del servidor de copia de seguridad

- Evitación del error de certificado SSL al abrir el Agente de Arcserve UDP (Linux)
- Configuración de los valores de configuración del sistema cuando se cambia el nombre de host o la dirección IP

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, las bases de datos y los exploradores compatibles.

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/Arcserve/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/Arcserve/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 y así acceder a dichos 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/Arcserve/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" clien-
   tAuth="false" sslProtocol="TLS" keys-
   toreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

3. Ejecute el siguiente comando para reiniciar el servidor de copia de seguridad:

   ```
   /opt/Arcserve/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.
- Cuando se utiliza la autenticación de sudo, consulte Cómo configurar cuentas de usuario de Sudo para los nodos de Linux para obtener la configuración específica.
- Se requerirá un plan para agregar un nodo de Linux para la autenticación de clave SSH, que tiene un conjunto de cambios relacionados con la configuración tanto en el servidor de copia de seguridad de Linux como en la máquina virtual de origen.

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
   ```

   Nota: Se puede generar una clave pública o privada para Rhel/alma/rocky/orel 9.X y Debian 12.X mediante el siguiente comando:

   ```
   ssh-keygen -t ecdsa -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/Arcserve/d2dserver/configfiles/server_pub.key
   ```

4. Copie el archivo de clave pública en la ubicación siguiente:

   ```
   /opt/Arcserve/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/Arcserve/d2dserver/configfiles/key.pass
   ```

6. Cambie el permiso para el archivo key.pass mediante el comando siguiente:

   ```
   chmod 600 /opt/Arcserve/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:

   ```
   /<directorio_principal_usuario>/.ssh/authorized_keys
   ```

   Ejemplo: Para un backup_admin, user_home es */home/backup_admin*

   Ejemplo: /home/backup_admin/.ssh/authorized_keys

9. (Opcional) Ejecute el siguiente comando en el nodo si SELinux bloquea la autenticación:

   ```
   restorecon /<directorio_principal_usuario>/.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/Arcserve/d2dserver/TOMCAT/conf/server.xml
   ```

2. Busque la siguiente cadena en el archivo server.xml:

   ```
   <!--<Connector connectionTimeout="180000" port="8014" pro-
   tocol="HTTP/1.1"/>-->
   ```

3. 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 eliminar los caracteres de cadena **<!--** y **-->**:

   ```
   <Connector connectionTimeout="180000" port="8014" pro-
   tocol="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" clien-
   tAuth="false" sslProtocol="TLS" keys-
   toreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

5. Agregue 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" SSLE-
   nabled="true" maxThreads="150" scheme="https" secure="true"
   clientAuth="false" sslProtocol="TLS" keys-
   toreFile="${catalina.home}/conf/server.keystore" keys-
   torePass="LinuxD2D"/>-->
   ```

6. Ejecute el siguiente comando para reiniciar el servidor de copia de seguridad:

   ```
   /opt/Arcserve/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 I 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 Certificate.

5. En la ficha General, haga clic en Install Certificate.

   Se abrirá el Asistente para importación de certificados.

6. Haga clic en Siguiente.
7. En la página Certificate Store, seleccione Place all certificates in the following store y, a continuación, haga clic en Browse.
8. Seleccione Trusted Root Certification Authorities y haga clic en OK.

   Se abre la página Certificate Store del asistente para la importación de certificados.

9. Haga clic en Siguiente y, a continuación, haga clic en Finalizar.

   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/Arcserve/d2dserver/bin/setenv

/opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2-
dserver/data/ARCserveLinuxD2D.db "update D2DServer set
Name='New_Hostname' where IsLocal=1"

/opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2-
dserver/data/License.db "update LicensedMachine set Ser-
verName ='Nuevo_nombrehost' where ServerName ='Nombrehost_
anterior'"
```

3. Cambie el nombre del archivo keystore:

   ```
   mv /opt/Arcserve/d2dserver/TOMCAT/conf/server.keystore
   /opt/Arcserve/d2dserver/TOMCAT/conf/server.keystore.old
   ```

4. Cree un archivo keystore mediante el comando keytool de Java.

   ```
   keytool -genkey -alias tomcat -keyalg RSA -keypass <YOUR_
   VALUE> -storepass <YOUR_VALUE> -keystore /op-
   t/Arcserve/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 RSA -keypass LinuxD2D -
   storepass LinuxD2D -keystore /op-
   t/Arcserve/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" clien-
   tAuth="false" sslProtocol="TLS" keys-
   toreFile="${catalina.home}/conf/server.keystore"
   keystorePass="YOUR_VALUE"/>
   ```

   Ejemplo:

   ```
   <Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
   maxThreads="150" scheme="https" secure="true" clien-
   tAuth="false" sslProtocol="TLS" keys-
   toreFile="${catalina.home}/conf/server.keystore"
   keystorePass="LinuxD2D"/>
   ```

6. Reinicie el servidor de copia de seguridad central.

   ```
   /opt/Arcserve/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/Arcserve/d2dserver/bin/setenv

/opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2-
dserver/data/ARCserveLinuxD2D.db "update D2DServer set
Name='New_Hostname' where IsLocal=1"
```

3. Cambie el nombre del archivo keystore:

```
mv /opt/Arcserve/d2dserver/TOMCAT/conf/server.keystore
/opt/Arcserve/d2dserver/TOMCAT/conf/

server.keystore.old
```

4. Cree un archivo keystore mediante el comando keytool de Java.

```
keytool -genkey -alias tomcat -keyalg RSA -keypass LinuxD2D -
storepass LinuxD2D -keystore /opt/Arcserve/d2-
dserver/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 RSA -keypass LinuxD2D -
storepass LinuxD2D -keystore /op-
t/Arcserve/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" clien-
tAuth="false" sslProtocol="TLS" keys-
toreFile="${catalina.home}/conf/server.keystore"
keystorePass="YOUR_VALUE"/>
```

Ejemplo:

```
<Connector port="8014" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true" clien-
tAuth="false" sslProtocol="TLS" keys-
toreFile="${catalina.home}/conf/server.keystore"
keystorePass="LinuxD2D"/>
```

6. Reinicie el servidor de copia de seguridad miembro.

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

7. Inicie sesión en la interfaz web de Arcserve UDP 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/Arcserve/d2dserver/bin/setenv
    ```

    ```
    /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2-
    dserver/data/License.db "update LicensedMachine set Ser-
    verName ='Nuevo_nombrehost' where ServerName ='Nombrehost_
    anterior'"
    ```

    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/Arcserve/d2dserver/bin/setenv
   ```

   ```
   /opt/Arcserve/d2dserver/bin/d2drp --storagepath=Backup Destination --node=Nuevo_nombrehost
   ```

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dserver/data/ARCserveLinuxD2D.db "update TargetMachine set Name='New_Hostname' where Name='Old_Hostname'"
   ```

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dserver/data/ARCserveLinuxD2D.db "update JobQueue set TargetName='New_Hostname' where JobType in (1,3,4,5) and TargetName='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/Arcserve/d2dserver/bin/d2drp --storagepath=<punto_montaje> --node=Nuevo_NombreHost
   ```

   Nota: Si se utiliza el recurso compartido Local, el comando será:

   ```
   /opt/Arcserve/d2dserver/bin/d2drp --storagepath=<ruta_local> --node=Nuevo_NombreHost
   ```
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/Arcserve/d2dserver/sbin/sqlite3 /opt/Arcserve/d2dserver/data/License.db "update LicensedMachine set MachineName ='Nuevo_nombrehost' where MachineName ='Nombrehost_anterior'"
   ```

El nombre de host se configura para realizar una copia de seguridad sin ningún error.

Cuando la máquina virtual LBS se clona en un entorno virtual

Cuando se clona la máquina virtual LBS en un entorno virtual, contiene el mismo UUID que la plantilla clonada. Por lo tanto, se le pedirá que vuelva a generar el UUID.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad de Linux como usuario raíz.
2. Abra el símbolo del sistema sqlite.

   ```
   /opt/Arcserve/d2dserver/sbin/sqlite3 /op-
   t/Arcserve/d2dserver/data/ARCserveLinuxD2D.db
   ```

3. Obtenga el UUID de la base de datos de sqlite.

   ```
   sqlite> select uuid from D2DServer;

   702ab046-3b70-493d-a2e2-ef3ff3b4dc52
   ```

4. Suprima el UUID existente de la base de datos de sqlite.

   ```
   sqlite> delete from D2DServer where UUID="702ab046-3b70-493d-
   a2e2-ef3ff3b4dc52";
   ```

5. Reinicie los servicios de UDP para volver a generar un nuevo UUID.

   ```
   opt/Arcserve/d2dserver/bin # ./d2dserver restart
   ```

Cómo agregar un usuario a la Consola del servidor de copia de seguridad de Linux mediante la línea de comandos

La utilización del Agente de Arcserve UDP para Linux mediante la línea de comandos permite crear un usuario que puede actuar como el reemplazo del usuario raíz en el servidor de Linux. Se puede utilizar el comando d2duser en la línea de comandos para agregar un usuario que puede actuar cuando el usuario raíz está desactivado.

El usuario raíz está desactivado debido a varios motivos. Por ejemplo, cuando se crea la máquina virtual en EC2 AWS, de forma predeterminada la raíz está desactivada.

- Revisión de los requisitos previos
- Adición de un usuario a la Consola del servidor de copia de seguridad de Linux mediante la línea de comandos

Revisión de los requisitos previos

Antes de agregar al usuario, tenga en cuenta el siguiente requisito previo o consideración:

- Dispone de las credenciales de inicio de sesión raíz para el servidor de copia de seguridad.
- Solo el usuario raíz puede ejecutar la línea de comandos: d2duser.

Adición de un usuario a la Consola del servidor de copia de seguridad de Linux mediante la línea de comandos

Se puede utilizar el comando d2duser en la línea de comandos para agregar un usuario que puede actuar como sustituto del usuario raíz cuando sea necesario.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario root.
2. Vaya a /opt/Arcserve/d2dserver/configfiles y abra el archivo: server.cfg.

   Nota: Si no existe un archivo con ese nombre, cree un nuevo archivo con el mismo nombre y agregue el siguiente contenido al archivo:

   ui_login_use_udp_user= true|false

   Permite la creación del usuario que actúa como el usuario predeterminado en ausencia del usuario raíz cuando se inicia sesión en el servidor. Se puede seleccionar **true** para esta opción.

   ui_login_user_password_min_length = 6

   Permite decidir la longitud mínima de la contraseña. Se puede cambiar el valor predeterminado 6, si es necesario.

   login_failure_time_to_lock_user = 9

   Permite decidir el número de errores consecutivos de inicio de sesión después del cual la cuenta de usuario se bloquea. Se puede cambiar el valor predeterminado 9, si es necesario.
3. Vaya a */opt/Arcserve/d2dserver/bin* y busque la línea de comandos d2duser.
4. Introduzca./d2duser para ver el uso de esta línea de comandos:

   ```
   d2duser --action=<add|delete|lock|unlock|passwd> --user-
   name=<nombreusuario>
   ```

5. Introduzca los siguientes detalles en la línea de comandos d2duser:

   d2duser --action=add --username=arcserve

   Permite agregar un usuario con el nombre arcserve. Cuando se pulsa Intro, se le pedirá que introduzca una contraseña y, a continuación, deberá volverla a introducir para confirmarla.

   d2duser --action=delete --username=arcserve

   Permite suprimir el usuario arcserve.

d2duser --action=lock --username=arcserve

Permite bloquear el usuario arcserve.

d2duser --action=unlock --username=arcserve

Permite desbloquear el usuario arcserve.

d2duser --action=passwd --username=arcserve

Permite cambiar la contraseña del usuario arcserve.

d2duser --action=list

Permite ver la lista de todos los usuarios.

6. En el navegador, abra la página de la consola del servidor de copia de seguridad de Linux.
7. Compruebe si el usuario predeterminado mostrado es el que se acaba de agregar.
8. Inicie sesión con ese nombre de usuario y contraseña.

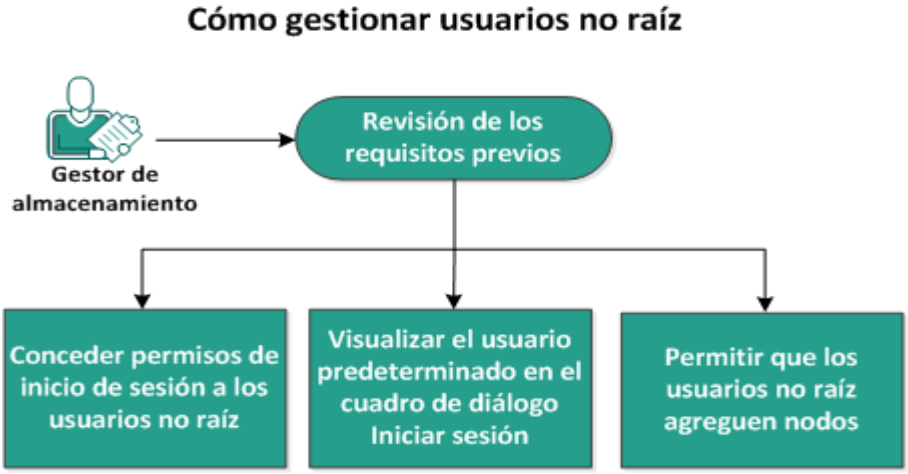
   El inicio de sesión correcto confirma que se ha creado el usuario.

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
- Concesión de permisos de inicio de sesión a los usuarios no raíz
- Visualización del usuario predeterminado en el cuadro de diálogo Iniciar sesión
- Permiso para que los usuarios no raíz agreguen nodos

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, las bases de datos y los exploradores compatibles.

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/Arcserve/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 del 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/Arcserve/d2dserver/configfiles/server.cfg`

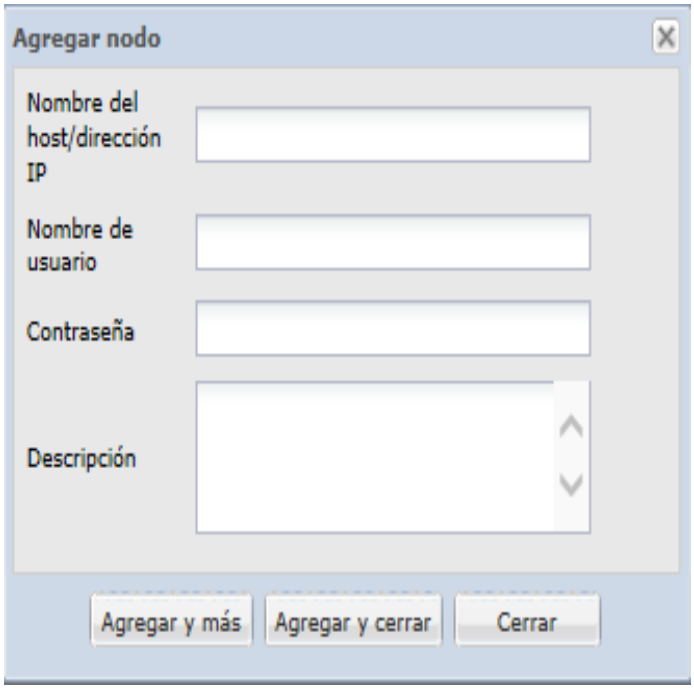
   Nota: Si el archivo server.cfg no está presente, créelo.
3. Agregue el siguiente código en el archivo server.cfg: show_default_user_when_login=false|true
4. Inicie sesión en la interfaz web del Agente de Arcserve UDP (Linux).
   - Si se ha agregado el comando *allow_login_users,* el cuadro de diálogo 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/Arcserve/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 configurar la cuenta de usuario sudo para los nodos de Linux

Puede utilizarse Sudo para configurar que cuentas de usuario normales realicen tareas de copia de seguridad y restauración. Para las cuentas de sudo, todas las configuraciones están relacionadas con nodos de Linux. Cuando la cuenta de sudo está configurada correctamente, puede utilizarla de un modo similar a una cuenta raíz normal en todas las interfaces de usuario. Mediante la cuenta de sudo, se pueden realizar tareas como agregar nodos, realizar copias de seguridad de nodos o restaurar archivos. Configure la cuenta de sudo según el documento de distribución de Linux específico.

Realice estas tareas para gestionar los usuarios sudo:

- Revise de los requisitos previos
- Modificación de la configuración de sudo predeterminada en SUSE
- Configuración de sudo en Debian
- Configuración de sudo en Ubuntu
- Configuración de sudo para la autorización sin contraseña al utilizar la autenticación de clave pública SSH
- Configuración de sudo para solo permitir el proceso del agente de la copia de seguridad

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 del nodo de Linux.
- Se ha configurado correctamente el permiso de sudo para el usuario deseado.
  - Compruebe que el usuario sudo puede ejecutar al menos estos programas: d2d_ea e ln. Por ejemplo, si el nombre de usuario es backupadmin, el ejemplo de configuración de sudo es el siguiente: *backupadmin ALL=(ALL) /usr/bin/d2d_ea,/usr/bin/ln*.
  - Compruebe si el usuario sudo puede conservar al menos las siguientes variables de entorno:

HOSTNAME	USERNAME	LANG	LC_ADDRESS
LC_CTYPE	LC_COLLATE	LC_ IDENTIFICATION	LC_ MEASUREMENT
LC_MESSAGES	LC_MONETARY	LC_NAME	LC_NUMERIC
LC_TIME	IDIOMA LC_ALL	SSH_ CONNECTION	CRE_ROOT_PATH
CRE_LOG_BASE_ DIR	TARGET_BOOTSTRAP_ DIR	TARGET_WORK_ DIR	jobID

    Por ejemplo, si el nombre de usuario es backupadmin, a continuación se muestran ejemplos de la configuración de sudo:

    Valores predeterminados: backupadmin env_keep += "HOSTNAME USERNAME LANG LC_ADDRESS LC_CTYPE"

    Valores predeterminados: backupadmin env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT"

    Valores predeterminados: backupadmin env_keep += "LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC LC_TIME LC_ALL LANGUAGE"

    Valores predeterminados: backupadmin env_keep += "SSH_ CONNECTION CRE_LOG_BASE_DIR jobID TARGET_BOOTSTRAP_DIR CRE_ROOT_PATH TARGET_WORK_DIR"

- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Modificación de la configuración de sudo predeterminada en SUSE

De forma predeterminada, SUSE requiere contraseña raíz en lugar de la contraseña de usuario para la autorización. Una autenticación de Sudo no funciona en el servidor de copia de seguridad de Linux porque el servidor de copia de seguridad utiliza las credenciales de usuario para la autorización. Se puede modificar la configuración predeterminada de sudo para autorizar el uso de las credenciales de usuario.

Siga estos pasos:

1. Inicie sesión en el nodo de Linux como usuario raíz.
2. Abra el archivo **/etc/sudoer** o ejecute el comando *visudo*.
3. Escriba un comentario en los valores de configuración, tal y como se muestra en el ejemplo siguiente:

   Ejemplo:

   ```
   #Defaults targetpw # pedir la contraseña del usuario de destino (raíz)

   #ALL ALL=(ALL) ALL # ¡ADVERTENCIA! Use esta opción solo con valores predeterminados de targetpw.
   ```

4. Compruebe que la línea de comandos de sudo ahora requiere una contraseña de usuario en lugar de la contraseña raíz para la autorización.

   Se ha modificado correctamente la configuración predeterminada de sudo.

Configuración de sudo en Debian

De forma predeterminada, la cuenta root no está activada para iniciar la sesión en Debian. Como resultado, se requiere una autenticación de sudo cuando se agrega Debian Linux como un nodo de Linux.

Siga estos pasos:

1. Inicie sesión en el nodo de Linux y cambie a root utilizando el comando *su*.
2. Si sudo no está instalado, instale el paquete de sudo mediante el comando siguiente:

   ```
   apt-get install sudo
   ```

3. Agregue un usuario ya existente con id=user a group=sudo:

   Ejemplo:

   ```
   adduser user sudo
   ```

   O cree un nuevo usuario con sudo

   ```
   adduser user
   ```

   ```
   adduser user sudo
   ```

4. Inicie sesión en el shell del usuario y escriba el siguiente comando para comprobar que el usuario está autorizado:

   ```
   sudo -v
   ```

   Se ha configurado correctamente sudo en Debian.

   Nota: Para Debian 12.x, después de realizar los pasos anteriores, abra el archivo **/etc/sudoers** desde la raíz, comente la línea siguiente en el archivo *sudoers* y, a continuación, guarde el archivo *sudoers*:

   ```
   Defaults use_pty
   ```

Configuración de sudo en Ubuntu

Esta sección proporciona información sobre cómo configurar el archivo *sudoers* en Ubuntu 22.

Para configurar, siga estos pasos:

1. Inicie sesión en el nodo de Linux como usuario raíz.
2. Cree un nuevo usuario sudo utilizando el siguiente comando:

   ```
   adduser user
   ```

3. Abra el archivo **/etc/sudoers** desde la raíz y agregue marcas de comentario a la línea siguiente en el archivo *sudoers*.

   ```
   Defaults use_pty
   ```

4. Guarde el archivo *sudoers*.

Se ha configurado correctamente sudo en Ubuntu 22.

Configuración de sudo para la autorización sin contraseña al utilizar la autenticación de clave pública SSH

Cuando se utiliza la autenticación de clave pública SSH, el servidor de copia de seguridad de Linux no guarda las credenciales del usuario. Se puede configurar Sudo para permitir la autorización sin necesidad de especificar una contraseña.

Siga estos pasos:

1. Inicie sesión en el nodo de Linux como usuario raíz.
2. Abrir el archivo **/etc/sudoer** o ejecute *visudo* para editar el archivo de configuración.
3. Vaya a la línea de configuración del usuario especificado y agregue la opción 'NOPASSWD'.

   Por ejemplo, si el nombre de usuario es backupadmin, agregue la opción 'NOPASSWD' como se muestra en el ejemplo siguiente:

   Ejemplo: backupadmin ALL=(ALL) NOPASSWD: /usr/bin/d2d_ea,/user/bin/ln
4. Inicie sesión en el shell del usuario y escriba el siguiente comando para verificar que la autorización no requiere ninguna contraseña:

   ```
   sudo -v
   ```

   Se ha configurado correctamente Sudo para la autorización sin contraseña cuando se utiliza la configuración de clave pública SSH.

Configuración de sudo para solo permitir el proceso del agente de la copia de seguridad

Cuando solo se permite al usuario utilizar los comandos limitados en sudo, se requiere realizar la instalación manual del programa del agente de copia de seguridad. Para que las tareas de copia de seguridad se ejecuten, es necesario tener el permiso de sudo para el proceso de *d2d_ea*.

Siga estos pasos:

1. Inicie sesión en el nodo de Linux como usuario raíz.
2. Abrir el archivo **/etc/sudoer** o ejecute *visudo* para editar el archivo de configuración.
3. Vaya a la línea de configuración del usuario especificado y agregue '/ usr/bin/d2d_ea' al elemento de configuración de los comandos permitidos.

   Por ejemplo, si el nombre de usuario es backupadmin, agregue '/usr/bin/d2d_ea' como se muestra en el ejemplo siguiente:

   Ejemplo: backupadmin ALL=(ALL) /usr/bin/d2d_ea
4. Determine si el nodo de origen de la copia de seguridad es de 32 o 64 bits y busque el archivo binario correcto en el servidor del agente de la copia de seguridad:
5. Copie el archivo binario determinado del paso 4 en el nodo de origen de la copia de seguridad como d2d_ea y, a continuación, colóquelo en '/ usr/bin/d2d_ea'.

   ```
   Para 32 bits: /opt/Arcserve/d2dserver/sbin/ea.32
   ```

   ```
   Para 64 bits: /opt/Arcserve/d2dserver/sbin/ea.64
   ```
6. Ejecute el siguiente comando para verificar el permiso de ejecución:

   ```
   chmod +x /usr/bin/d2d_ea
   ```

   Se ha configurado correctamente sudo para permitir solo el proceso del agente de la copia de seguridad.

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 los requisitos previos
- Verificación de que la utilidad d2drestorevol está instalada
- Verificación de los detalles de volumen en la sesión
- Envío de la tarea de restauración
- Cancelación de la tarea de restauración del volumen
- Verificación del volumen restaurado

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.
- La restauración del volúmenes es compatible con la sesión generada por planes o tareas basados en agentes de Linux.
- 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. Si se realiza la copia de seguridad de la sesión en un almacén de datos de puntos de recuperación, primero debe buscar la ruta compartida en los detalles del almacén de datos. A continuación, monte la ruta compartida en un punto de montaje local y 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, las bases de datos y los exploradores compatibles.

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/Arcserve/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 archivo server.cfg no está presente, créelo.

```
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. Si los puntos de recuperación están en una carpeta compartida o local, 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.

3. Si los puntos de recuperación están en un almacén de datos del servidor de puntos de recuperación, utilice el siguiente comando para verificar la información del volumen:

   ```
   d2drestorevol: comando = info--storage-path = <ruta_servidor_
   puntos_recuperación>: nodo = "<nombre_nodo> [UUID_number]"--
   rp = <punto_recuperación>: rps-host = <nombre_host>: rps-user
   = <nombre_usuario>: rps-nombre = <contraseña_servidor_puntos_
   recuperación>: rps-protocolo = <protocolo_seguridad_Inter-
   net>: rps-port = <número_puerto>: rps-deduplicación
   ```

   El comando siguiente es un ejemplo de un almacén de datos activado para la deduplicación:

```
d2drestorevol --command=info --storage-path=/root/rpsshare --
node="xx.xx.xx.xx[11111aa-22bb-33cc-yyyy-4c4c4c4c]" --rp=V-
VStore/S0000000001 --rps-host=machine_name --rps-use-
r=administrator --rps-pw******** --rps-protocol=https --rps-
port=8014 --rps-dedup
```

--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 con el siguiente formato:

<nombre de nodo>[<uuid>]

--rp

Especifica el punto de recuperación o la sesión de recuperación que se desea restaurar a partir de un almacén de datos del servidor de puntos de recuperación. Por lo general, se debe especificar una sesión de punto de recuperación desde un almacén de datos del servidor de puntos de recuperación en el formato siguiente:

VStore/S00000000X ("X" hace referencia a un valor numérico)

-- rps-host

Especifica el nombre de host del servidor de puntos de recuperación donde se almacena la sesión de recuperación.

-- rps-user

Especifica el nombre de usuario para acceder al host del servidor de puntos de recuperación.

-- rps-pw

Especifica la contraseña para acceder al host del servidor de puntos de recuperación.

-- rps-protocol

Especifica el protocolo para el host del servidor de puntos de recuperación. El protocolo puede ser http o https.

-- rps-port

Especifica el número de puerto del host del servidor de puntos de recuperación.

-- rps-dedup

Especifica el almacén de datos que tiene activada la deduplicación. Este parámetro es necesario solo cuando el almacén de datos tiene activada la deduplicación.

-- ds-share-folder

Especifica la ruta compartida del almacén de datos. Este parámetro es necesario solo cuando el almacén de datos tiene desactivada la deduplicación.

-- ds-user

Especifica el nombre de usuario para acceder a la ruta compartida del almacén de datos.

-- ds-user-pw

Especifica el nombre de usuario para acceder a la ruta compartida del almacén de datos.

-- ds-pw

Especifica la contraseña de cifrado de datos si el almacén de datos también tiene activado el cifrado.

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. Si los puntos de recuperación se encuentran en una carpeta local o red compartida, 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-volu-
me=<volumen_destino> [--encryption-passwor-
d=<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. Si los puntos de recuperación se encuentran en un almacén de datos de puntos de recuperación, 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 con el siguiente formato:

<nombre de nodo>[<uuid>]

--rp

Especifica el punto de recuperación o sesión de recuperación que se desea restaurar desde el almacén de datos en un servidor de puntos de recuperación. Por lo general, se debe especificar una sesión de punto de recuperación desde un almacén de datos del servidor de puntos de recuperación en el formato siguiente:

VStore/S00000000X ("X" hace referencia a un valor numérico)

--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

-- rps-host

Especifica el nombre de host del servidor de puntos de recuperación donde se almacenan las sesiones de recuperación.

-- rps-user

Especifica el nombre de usuario para acceder al host del servidor de puntos de recuperación.

-- rps-pw

Especifica la contraseña para acceder al host del servidor de puntos de recuperación.

-- rps-protocol

Especifica el protocolo para el host del servidor de puntos de recuperación. El protocolo puede ser http o https.

-- rps-port

Especifica el número de puerto del host del servidor de puntos de recuperación.

-- rps-dedup

Especifica que el almacén de datos tiene activada la deduplicación. Este parámetro es necesario solo cuando el almacén de datos tiene activada la deduplicación.

-- ds-share-folder

Especifica la ruta compartida del almacén de datos. Este parámetro es necesario solo cuando el almacén de datos tiene desactivada la deduplicación.

-- ds-user

Especifica el nombre de usuario para acceder a la ruta compartida del almacén de datos.

-- ds-user-pw

Especifica la contraseña para acceder a la ruta compartida del almacén de datos.

-- ds-pw

Especifica la contraseña de cifrado de datos si el almacén de datos también tiene activado el cifrado.

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.

4. (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.

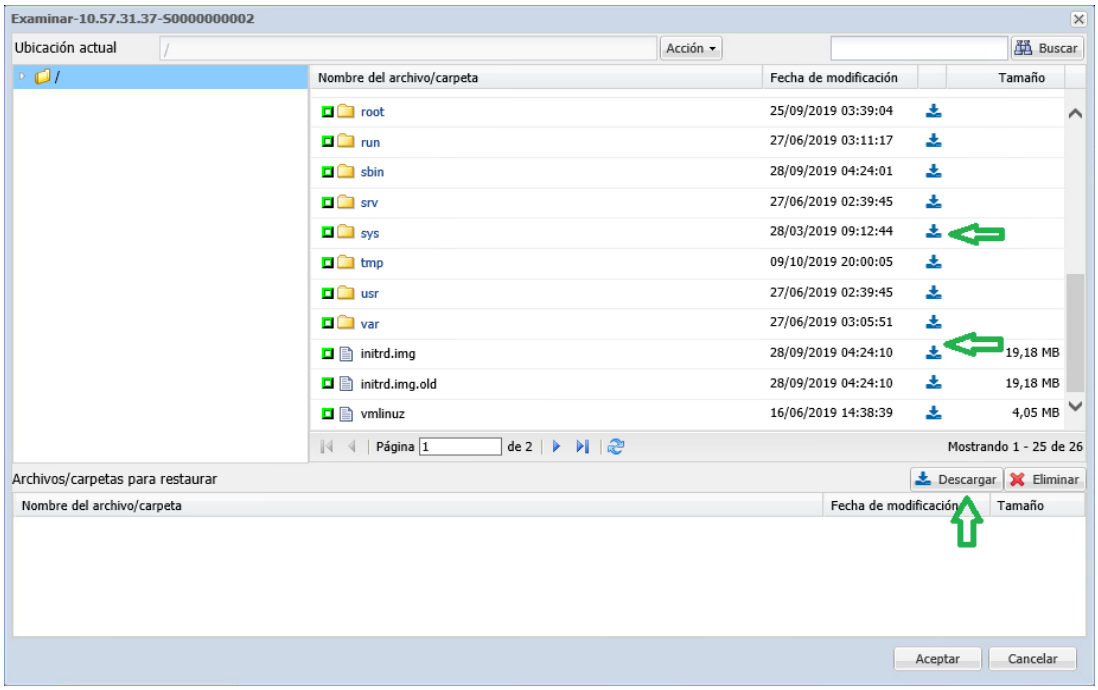
Cómo descargar archivos o carpetas sin restaurar para nodos de Linux

[[[Undefined variable Variables.AUDP]]] permite descargar un archivo o una carpeta completa sin tener que enviarlos a la restauración. En el Asistente de restauración, la pantalla Examen de puntos de recuperación permite descargar directamente cualquier archivo o carpeta completa con todos los archivos. El descargar antes de restaurar puede ayudar a realizar una comprobación rápida de los archivos para evitar que se restauren los archivos no deseados.

Un solo archivo se descarga directamente en el mismo formato, mientras que una carpeta se descarga como un archivo ZIP. El archivo ZIP tiene el siguiente formato de nombre:

[nombredenodo]_[IDsesión]_[marcatiempo].zip

Para descargar, basta con que llegue a la pantalla Examen de puntos de recuperación en el Asistente de restauración. La captura de pantalla que se muestra a continuación muestra cómo se debe realizar la descarga de un archivo o carpeta para los nodos de Linux:

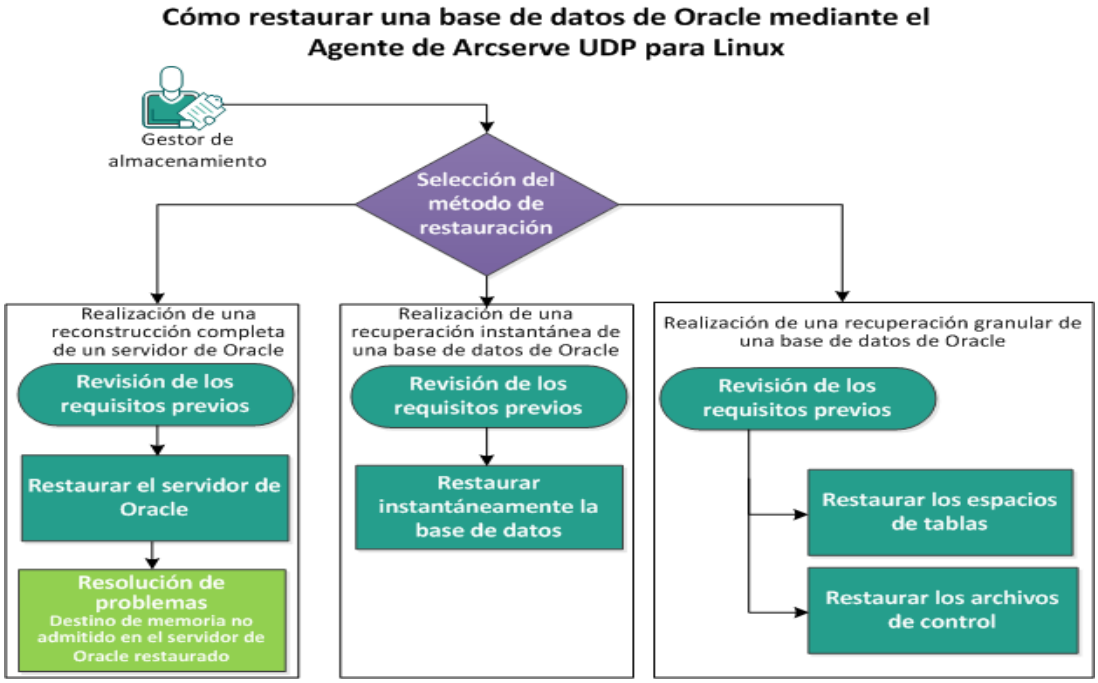


Para abrir los archivos descargados, utilice herramientas como WinZip, WinRAR, 7-Zip, etc.

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 utilizando 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
- Realización de una recuperación instantánea de una base de datos de Oracle
- Realización de una recuperación granular de una base de datos de Oracle

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.

Esta sección incluye los siguientes temas:

- Revise de los requisitos previos
- Restauración del servidor de Oracle
- Destino de memoria no admitido en el servidor de Oracle restaurado

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.
- Revise los sistemas de archivos compatibles para las copias de seguridad basadas en el Agente de UDP para Linux. La gestión de almacenamiento automática (ASM), el sistema de archivos del clúster de Oracle (OCFS / OCFS2) y los sistemas de archivos ACFS no son compatibles con las copias de seguridad basadas en el Agente de UDP para Linux. Para proteger los datos en estos sistemas de archivos, utilice las copias de seguridad de Oracle RMAN de UDP.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

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 base de datos de Oracle se produce 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.

Esta sección incluye los siguientes temas:

- Revise de los requisitos previos
- Restauración instantánea de la base de datos

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.
- Revise los sistemas de archivos compatibles para las copias de seguridad basadas en el Agente de UDP para Linux. La gestión de almacenamiento automática (ASM), el sistema de archivos del clúster de Oracle (OCFS / OCFS2) y los sistemas de archivos ACFS no son compatibles con las copias de seguridad basadas en el Agente de UDP para Linux. Para proteger los datos en estos sistemas de archivos, utilice las copias de seguridad de Oracle RMAN de UDP.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

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-
   h=<ubicación_sesión_en_local> --node=<servidor_oracle> --
   rp=last --source-volume=<punto_montaje_para_volumen_datos_ora-
   cle> --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-e=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;
```

Ejemplo: #. /d2drestorevol --command=restore --storage-path=/CRE_ROOT --node-e=rh63-v2 --rp=last --source-volume=/opt/oracle --target-volume=/dev/sdb1 --mount-target=/opt/oracle --quick-recovery

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.

Esta sección incluye los siguientes temas:

- Revise de los requisitos previos
- Restauración de los espacios de tablas
- Restauración de archivos de control

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.
- Revise los sistemas de archivos compatibles para las copias de seguridad basadas en el Agente de UDP para Linux. La gestión de almacenamiento automática (ASM), el sistema de archivos del clúster de Oracle (OCFS / OCFS2) y los sistemas de archivos ACFS no son compatibles con las copias de seguridad basadas en el Agente de UDP para Linux. Para proteger los datos en estos sistemas de archivos, utilice las copias de seguridad de Oracle RMAN de UDP.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

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 05/27/2014
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.
```

10. Recuperación de medios completa.
11. Abra la base de datos con la cláusula RESETLOGS después de finalizar el proceso de recuperación.

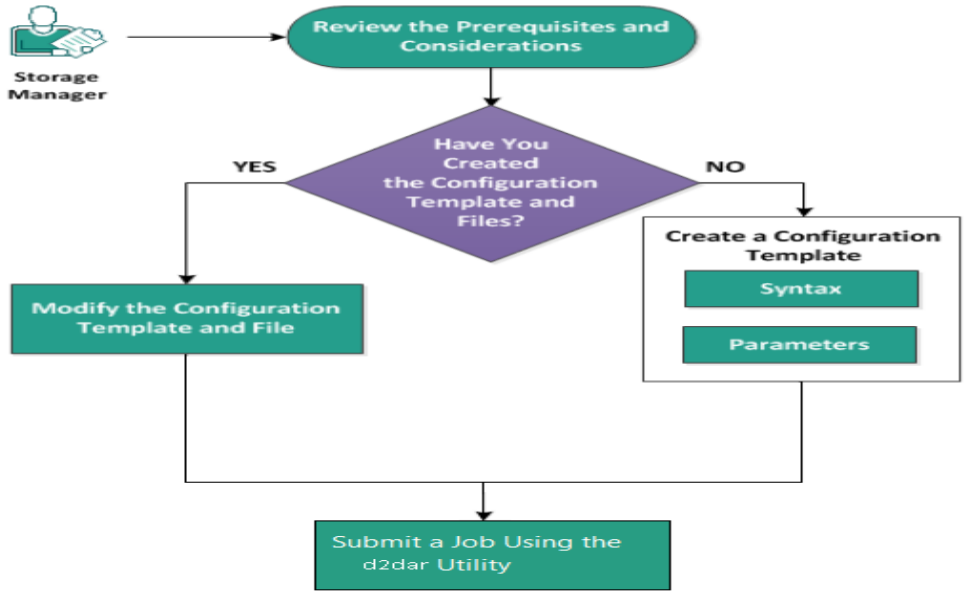
```
SQL> alter database open resetlogs;
```

Los archivos de control se han recuperado correctamente.

Cómo ejecutar la prueba de recuperación asegurada desde la línea de comandos

Se puede ejecutar una prueba de recuperación asegurada desde la línea de comandos del servidor de copia de seguridad mediante la utilidad d2dar. La utilidad d2dar automatiza el proceso de realización de una prueba de recuperación asegurada para las sesiones especificadas de las que se ha realizado una copia de seguridad.

El diagrama siguiente muestra el proceso para ejecutar una prueba de recuperación asegurada desde la línea de comandos mediante la utilidad d2dar:



Realice las tareas siguientes para ejecutar la prueba de recuperación asegurada:

- Revisión de las consideraciones y los requisitos previos
- Creación de una plantilla de configuración
- Modificación del archivo y de la plantilla de configuración
- Envío de una tarea mediante la utilidad d2dar

Revisión de las consideraciones y requisitos previos

Antes de llevar a cabo la prueba de recuperación asegurada, se deben revisar las consideraciones siguientes:

- Las siguientes versiones de hipervisores son compatibles con la recuperación asegurada mediante la utilidad d2dar:
  - VMware vCenter/ESX(i) 5.0 o posterior
  - Windows Hyper-V Server 2012 o posterior

    Nota: Para saber más sobre las máquinas virtuales de Linux compatibles en Hyper-V, haga clic en este vínculo.
- La prueba de recuperación asegurada únicamente se puede llevar a cabo desde la línea de comandos. Esta opción no está disponible en la interfaz de usuario.

Creación de una plantilla de configuración

Se puede crear un archivo de configuración para que el comando d2dar ejecute la tarea de prueba de recuperación asegurada en función de los parámetros especificados en el archivo.

Sintaxis

d2dar –createtemplate=<ruta_archivo_cfg>

La utilidad *d2dutil --encrypt* cifra la contraseña y proporciona una contraseña cifrada. Se debe utilizar esta utilidad para cifrar todas las contraseñas.

Método 1

echo 'string' | ./d2dutil --encrypt

string hace referencia a la contraseña que se debe especificar.

Método 2

Escriba el comando *d2dutil –encrypt* y especifique la contraseña. Pulse **Intro**. Se muestra el resultado en 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 root.
2. Vaya a la carpeta bin donde está instalado el Agente de Arcserve Unified Data Protection para Linux con el comando siguiente:

   #cd /opt/Arcserve/d2dserver/bin
3. Cree la plantilla de configuración utilizando el comando siguiente:

   #./d2dar --createtemplate=<ruta_archivo_cfg>

   <cfg_file_path> indica la ubicación de creación de la plantilla de configuración.
4. Abra la plantilla de configuración y actualice los parámetros siguientes en la plantilla de configuración:

   job_name

   Especifica el nombre de la tarea de recuperación asegurada.

   vm_name_prefix

   Especifica el prefijo para la máquina virtual que se crea para la tarea de recuperación asegurada. El nombre de la máquina virtual de recu-

peración asegurada es vm_name_prefix + nombre del nodo + marca de tiempo.

vm_type

Especifica el tipo de hipervisor en el que se lleva a cabo la prueba de recuperación asegurada. Los tipos válidos de hipervisores son Hyper-V, ESX y AHV.

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.

vm_svr_password

Especifica la contraseña del hipervisor. La contraseña se cifra utilizando la utilidad de cifrado d2dutil.

vm_svr_protocol

Especifica el protocolo del hipervisor cuando se realiza la recuperación asegurada en vCenter/ESX(i) o AHV.

vm_svr_port

Especifica el puerto del hipervisor cuando se realiza la recuperación asegurada en vCenter/ESX(i) o AHV.

vm_sub_server

Especifica el nombre del servidor ESX cuando se realiza la recuperación asegurada en vCenter o especifica el nombre del clúster de Prism Element cuando se realiza la recuperación asegurada en Prism Central.

vm_datastore

Especifica la ubicación de almacenamiento para la máquina virtual utilizada por la prueba de recuperación asegurada. Cuando se realiza la prueba de recuperación asegurada en vCenter/ESXI(i), la ubicación es el almacén de datos en el servidor ESX(i). La ubicación debe ser una ruta local en el servidor de Hyper-V cuando se realiza la recuperación asegurada en Hyper-V. La ubicación es storage_container en el clúster de AHV cuando se realiza la recuperación asegurada en AHV.

vm_resource_pool

Especifica el nombre de la agrupación de recursos cuando se realiza la recuperación asegurada en vCenter/ESXI(i).

tiempo de espera

Especifica el tiempo requerido para la tarea de recuperación asegurada durante el reinicio hasta que la máquina virtual está lista para su uso. El tiempo se muestra en segundos.

vm_memory

Especifica el tamaño de la memoria de la máquina virtual. El tamaño se debe especificar en MB y debe ser múltiplo de 4.

vm_cpu_count

Especifica el número de CPU de la máquina virtual.

run_after_backup

Especifica si esta tarea de recuperación asegurada se ejecutará una única vez o todas las veces para la tarea de copia de seguridad definida por el parámetro backup_job_name. Si se establece este parámetro en **no**, la tarea de recuperación asegurada se ejecuta inmediatamente para la tarea de copia de seguridad especificada; si se establece en **yes**, la tarea de recuperación asegurada se ejecuta cada vez que la tarea de copia de seguridad especificada ha finalizado.

Valor predeterminado: no

backup_job_name

Especifica el nombre de la tarea de copia de seguridad de los nodos para realizar la tarea de recuperación asegurada.

storage_type

Especifica el tipo de almacenamiento para la sesión de la que se ha realizado una copia de seguridad. Los tipos de almacenamiento válidos son cifs, nfs y rps.

storage_location

Especifica la ubicación de NFS o CIFS.

storage_username

Especifica el nombre de usuario de la ubicación de CIFS.

storage_password

Especifica la contraseña para la ubicación de CIFS. La contraseña se cifra utilizando la utilidad de cifrado d2dutil.

rps_protocol

Especifica el protocolo del servidor de puntos de recuperación cuando se realiza la tarea de recuperación asegurada para las sesiones del servidor de puntos de recuperación.

rps_hostname

Especifica el nombre de host del servidor de puntos de recuperación. La dirección puede ser el nombre de host o la dirección IP.

rps_username

Muestra el nombre de usuario del servidor de puntos de recuperación.

rps_password

Especifica la contraseña del servidor de puntos de recuperación. La contraseña se cifra utilizando la utilidad de cifrado d2dutil.

rps_port

Especifica el puerto del servidor de puntos de recuperación.

Valor predeterminado: 8014.

rps_datastore

Muestra el nombre del almacén de datos del servidor de puntos de recuperación.

encryption_password

Especifica la contraseña cifrada de la sesión. La contraseña se cifra utilizando la utilidad de cifrado d2dutil.

node_name_list

Especifica el nombre o nombres de los nodos donde se ejecuta la prueba de recuperación asegurada. Los nombres se deben separar mediante punto y coma (;). Si no se especifica un nombre o si se deja vacío, la prueba de recuperación asegurada se ejecuta en todos los nodos con el mismo nombre de tarea de copia de seguridad o que se encuentran en la misma ubicación.

recovery_point_date_filter

Especifica la fecha del punto de recuperación. La prueba de recuperación asegurada se ejecuta para el último punto de recuperación anterior a la fecha especificada. Si no se especifica la fecha o si se deja vacío, la prueba de recuperación asegurada se ejecuta para la última sesión de la que se ha realizado una copia de seguridad.

gateway_vm_network

Especifica la red de la máquina virtual para el servidor de puerta de enlace. La máquina virtual y el servidor de copia de seguridad se encuentran en la misma red.

gateway_guest_network

Especifica el tipo de dirección IP de red para el servidor de puerta de enlace. La red puede ser dhcp o una red estática.

gateway_guest_ip

Especifica la dirección IP para el servidor de puerta de enlace si se ha proporcionado la dirección IP estática.

gateway_guest_netmask

Especifica la máscara de red para el servidor de puerta de enlace si se ha proporcionado la dirección IP estática.

gateway_guest_gateway

Especifica la puerta de enlace para el servidor de puerta de enlace si se ha proporcionado la dirección IP estática.

script_post_job_server

(Opcional) Especifica el script que se debe ejecutar una vez que ha finalizado la tarea en el servidor de copia de seguridad.

script_ready_to_use

(Opcional) Especifica el script que se debe ejecutar cuando el equipo de destino está listo para utilizarse en la máquina virtual de recuperación asegurada.

run_script_ready_to_use_timeout

Especifica el tiempo requerido para ejecutar el script listo para su uso especificado por script_ready_to_use. El tiempo se muestra en segundos.

Nota: Los parámetros sobre información relacionada con la sesión *storage_type, storage_location, storage_username, storage_password, rps_protocol, rps_hostname, rps_username, rps_password, rps_port y rps_datastore* solo se requieren cuando no se especifica el parámetro *backup_job_name*.

5. Haga clic en **Guardar** y cierre la plantilla de configuración.

   La plantilla de configuración se ha creado correctamente.

Modificación del archivo y de la plantilla de configuración

Si ya se dispone del archivo de plantilla de configuración, se puede modificar el archivo y ejecutar la prueba de recuperación asegurada con una configuración diferente. No es necesario crear otra plantilla de configuración. Cuando se envía la tarea, se agrega una tarea nueva a la interfaz web. Se pueden consultar los registros de actividad en la interfaz web.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario root.
2. Abra la plantilla de configuración desde la ubicación donde ha guardado el archivo y modifique los parámetros en función de sus necesidades.
3. Haga clic en **Guardar** y cierre la plantilla de configuración.
4. Haga clic en **Guardar** y cierre el archivo de configuración global.

La plantilla de configuración se ha modificado correctamente.

Envío de una tarea mediante la utilidad d2dar

Se puede utilizar el comando d2dar para ejecutar la prueba de recuperación asegurada para las sesiones de las que se ha realizado una copia de seguridad. Tras su envío, se puede consultar la tarea desde la interfaz web. Si no se cumple alguno de los requisitos durante el proceso de recuperación asegurada, se muestra un error. Se puede consultar el registro de actividad en la interfaz web.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario root.
2. Envíe la tarea de recuperación asegurada mediante el comando siguiente:

   #./d2dar --template=cfg_file_path

Cómo montar un punto de recuperación

Un punto de recuperación montado puede compartir archivos en un punto de recuperación a través de NFS o WebDAV y se puede acceder a estos archivos mediante el montaje de la ubicación en el servidor de Linux.

Realice las tareas siguientes para montar un punto de recuperación:

- Revisión de los requisitos previos
- Especifique el punto de recuperación para montar.
- Especifique los valores de configuración para el montaje del punto de recuperación.
- Creación y ejecución de la tarea de montaje del punto de recuperación
- Monte el recurso compartido de NFS o de WebDAV en el servidor de Linux.

Revisión de los requisitos previos

Antes de montar un punto de recuperación, se deben tener en cuenta los requisitos previos siguientes:

- Dispone de un punto de recuperación válido y de la contraseña de cifrado, si hay.
- Si desea montar el punto de recuperación mediante WebDAV, asegúrese de que se ha instalado el paquete davfs2 en el servidor de Linux.
- Revise la Matriz de compatibilidad que proporciona los sistemas operativos, las bases de datos y los exploradores compatibles.

Especifique el punto de recuperación para montar.

Cada vez que se realiza una copia de seguridad, 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.

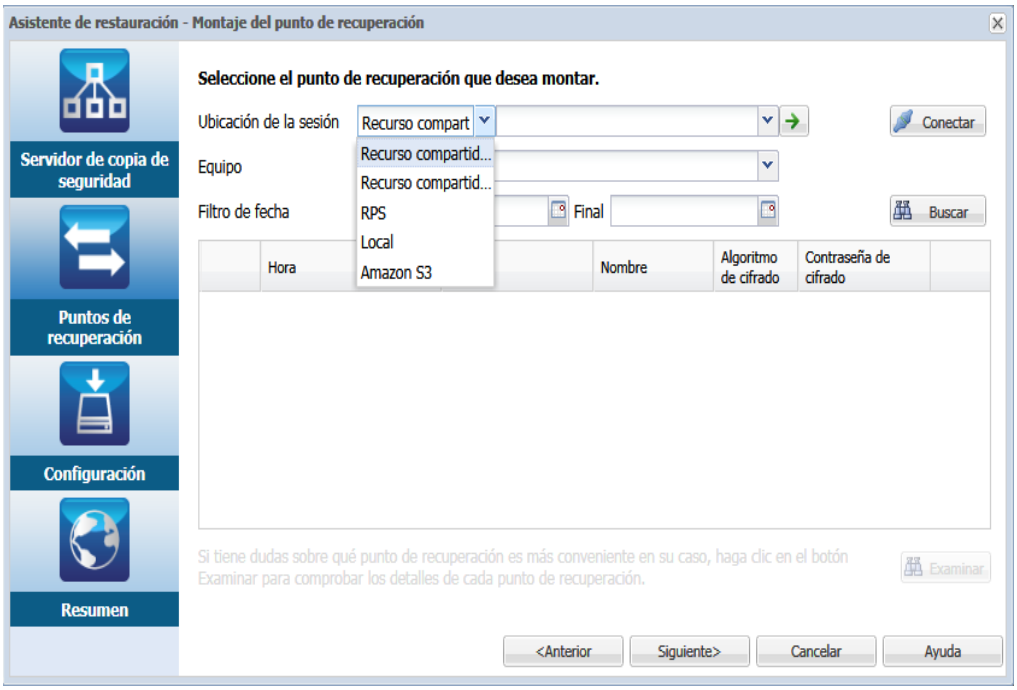
Siga estos pasos:

1. Abra la interfaz web del Agente de Arcserve UDP para Linux.
2. En el menú del **Asistente**, haga clic en **Restaurar** y seleccione **Montar punto de recuperación**.

   Se abre **Asistente de restauración – Montar punto de recuperación**.

   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**.
3. Haga clic en **Siguiente**.

   Aparece la página **Puntos de recuperación** del **Asistente de restauración.**



4. En la lista desplegable Ubicación de la sesión, seleccione **Recurso compartido de CIFS, Recurso compartido de NFS, RPS o Local**.
5. Realice uno de los pasos siguientes en función de la ubicación de la sesión:

Para Recurso compartido de CIFS, Recurso compartido de NFS o Local

Especifique la ruta completa del recurso compartido de CIFS, el recurso compartido de NFS o el recurso local y haga clic en **Conectar**.

Se muestra la lista desplegable **Equipo** que incluye todos los equipos.

Nota: Si se selecciona la opción Recurso compartido de CIFS, se deben especificar el nombre de usuario y la contraseña.

Para el servidor de puntos de recuperación:

a. Seleccione el servidor de puntos de recuperación y haga clic en **Agregar**.

   Aparece el cuadro de diálogo **Información del servidor de puntos de recuperación**.

b. Proporcione los detalles del servidor de puntos de recuperación y haga clic en el botón **Cargar**.

c. Seleccione el almacén de datos de la lista desplegable y haga clic en **Sí**.

   El cuadro de diálogo Información del servidor de puntos de recuperación se cierra y aparece el Asistente.

d. Haga clic en **Conectar**.

   Se muestra la lista desplegable Equipo que incluye todos los equipos.

e. Seleccione el equipo de la lista desplegable.

   Todos los puntos de recuperación del equipo seleccionado aparecen debajo de la opción **Filtro de fecha**.

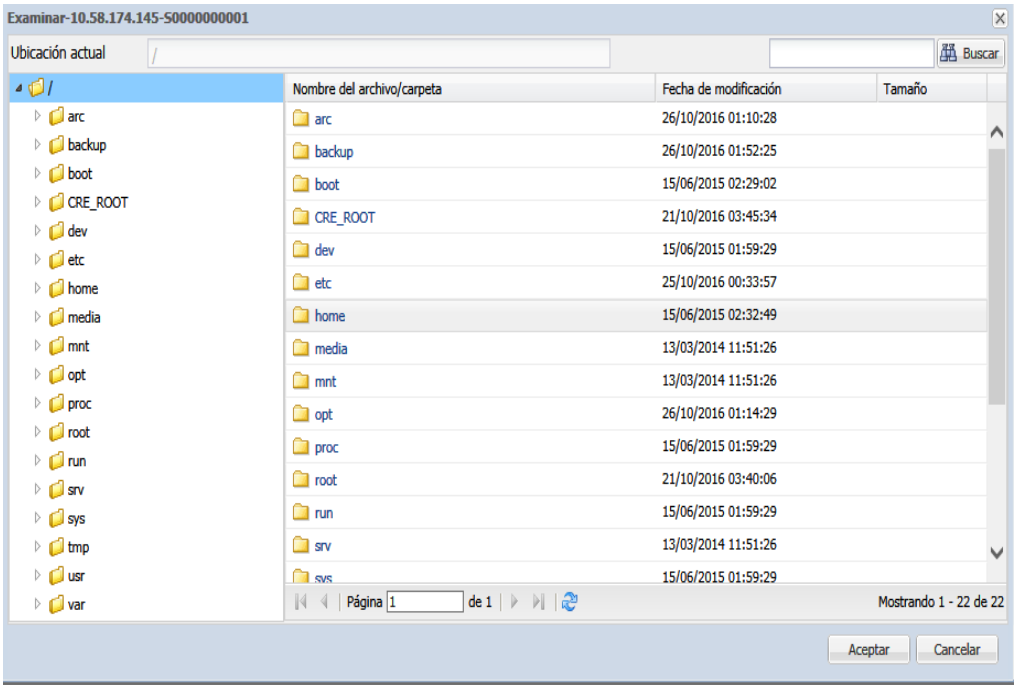
6. Aplique el filtro de fecha para que se muestren los puntos de recuperación que se han generado entre la fecha especificada y haga clic en **Buscar**.

   Valor predeterminado: Las dos últimas semanas.

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

7. Haga clic en Examinar para ver el punto de recuperación.

   Se abre el cuadro de diálogo **Examinar - <nombre nodo> - <número sesión>**.



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.

8. Haga clic en **Aceptar**.

   El cuadro de diálogo **Examinar - <nombre nodo> - <número sesión>** se cierra y se le redirige a la página Puntos de recuperación.

9. Haga clic en **Siguiente**.

   Se abre **Configuración** para las páginas de montaje de los puntos de recuperación.

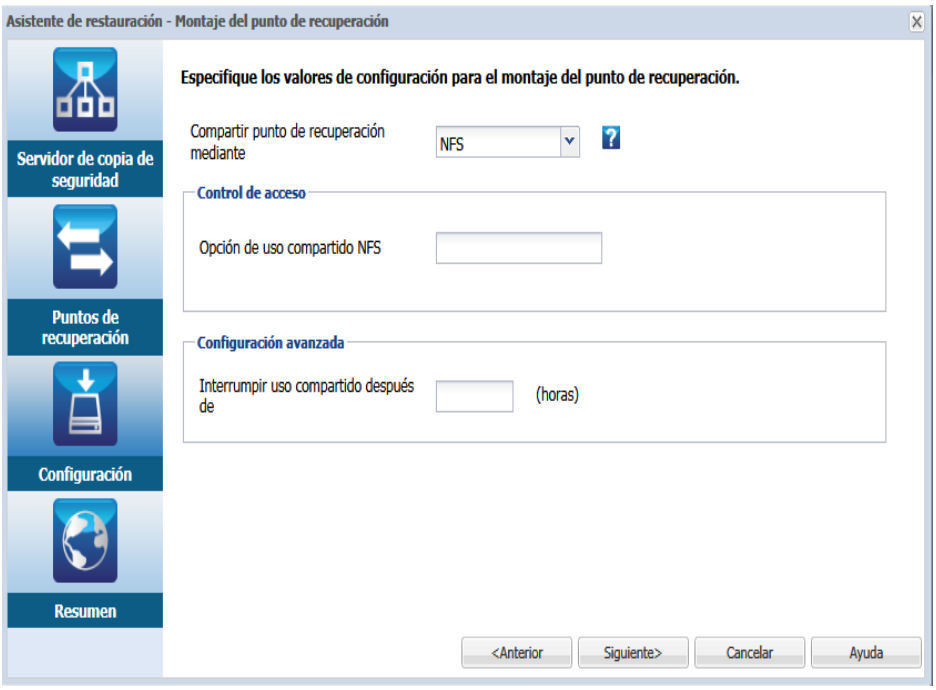
Especificación de los valores de configuración para el montaje del punto de recuperación

Se deben especificar valores de configuración para el montaje del punto de recuperación en función del método de compartición deseado.

Siga estos pasos:

1. Para montar el punto de recuperación a través de NFS, siga los pasos siguientes:
   a. Seleccione **NFS** de la lista desplegable de métodos de compartición.

      Los archivos del punto de recuperación se compartirán a través de NFS. Además, se puede montar el recurso compartido de NFS en cualquier equipo que tenga acceso al servidor de copia de seguridad de Linux.



   b. (Opcional) Introduzca la **opción de compartición NFS** en función de los requisitos.

      Consulte la página principal para las exportaciones, los candidatos y el formato válido. Deje este campo vacío si no necesita disponer de control de acceso.

   c. Introduzca el tiempo, en **horas**, tras el cual ya no se podrá acceder al recurso compartido.

Si se introduce 0 para este campo, se podrá acceder al recurso compartido de forma indefinida.

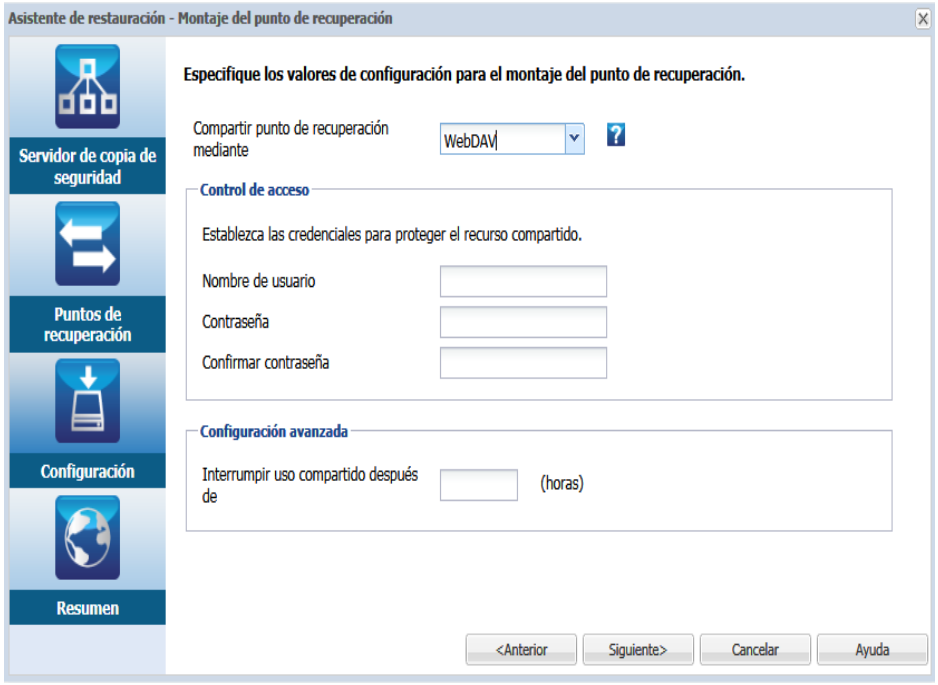
d. Haga clic en **Siguiente**.

Se abre la página Resumen para la tarea de montaje del punto de recuperación.

2. Para montar el punto de recuperación a través de WebDAV, siga los pasos siguientes:

a. Seleccione **WebDAV** de la lista desplegable de métodos de compartición.

Los archivos del punto de recuperación se compartirán a través de WebDAV. Además, se puede montar el recurso compartido de WebDAV mediante mount.davfs. Se recomienda utilizar este método recomendado cuando se requiera acceso al recurso compartido a través de Internet.



b. Introduzca el **nombre de usuario** y la **contraseña**, y vuelva a escribir la contraseña en el campo **Confirm your password (Confirmar contraseña)** para Access Control (Control de acceso).

Recuerde el nombre de usuario y la contraseña, ya que serán necesarios para acceder al punto de recuperación montado.

c. Introduzca el tiempo, en **horas**, tras el cual ya no se podrá acceder al recurso compartido.

   Si se introduce 0 para este campo, se podrá acceder al recurso compartido de forma indefinida.

   Si el tiempo alcanza la hora u horas especificadas, se interrumpirá el acceso al punto de recuperación montado.

d. Haga clic en **Siguiente**.

   Se abre la página Resumen para la tarea de montaje del punto de recuperación.

Creación y ejecución de la tarea de montaje del punto de recuperación

Para poder acceder a los archivos del punto de recuperación especificado, se debe crear y ejecutar primero la tarea de montaje del punto de recuperación. Antes de enviar la tarea, se debe verificar la información relativa a la configuración. Si es necesario, se puede volver al paso anterior y modificar los valores de configuración del asistente.

Siga estos pasos:

1. En la página **Resumen**, verifique los detalles del montaje del punto de recuperación.
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**.

   La tarea de montaje del punto de recuperación se ha creado y ejecutado correctamente.

Montaje del recurso compartido de NFS o de WebDAV en el servidor de Linux

Cuando el valor del campo **Fase de la tarea** de la ficha **Estado de la tarea** se establece en **Sharing recovery Point (Compartiendo punto de recuperación)**, ya se puede acceder al punto de recuperación montado.

Siga estos pasos:

1. Obtenga el **ID o el nombre de la tarea** de montaje del punto de recuperación en la ficha **Estado de la tarea**.
2. En la página **Registro de actividad**, filtre los registros de actividad para el punto de recuperación montado por **ID o nombre de la tarea** mediante las herramientas de **filtro**.

Tipo	ID de la tarea	Nombre de la tarea	Hora	Nombre del nodo	Mensaje
	2	Montar punto de recuperación-26/10/2016 11:56:12	26/10/2016 18:56:23	10.58.174.145	El punto de recuperación se ha compartido correctamente.
	2	Montar punto de recuperación-26/10/2016 11:56:12	26/10/2016 18:56:23	10.58.174.145	El uso compartido del punto de recuperación continuará todavía durante 1 horas.
	2	Montar punto de recuperación-26/10/2016 11:56:12	26/10/2016 18:56:23	10.58.174.145	Los informes de script: Acceda al directorio compartido mediante el recurso compartido NFS: 10.58.174.145:/opt/Arcserve/d2dserver/tmp/d2d_share_path2
	2	Montar punto de recuperación-26/10/2016 11:56:12	26/10/2016 18:56:23	10.58.174.145	El script de la tarea de montaje del punto de recuperación NFS se ha ejecutado correctamente en la fase post_share.
	2	Montar punto de recuperación-26/10/2016 11:56:12	26/10/2016 18:56:16	10.58.174.145	El script de la tarea de montaje del punto de recuperación NFS se ha ejecutado correctamente en la fase pre_share.
	2	Montar punto de recuperación-26/10/2016 11:56:12	26/10/2016 18:56:16	10.58.174.145	El punto de recuperación es: 10.58.174.145[f6219225-6597-ce49-6c87-81c717ea6ec3]/S0000000001.
	2	Montar punto de recuperación-26/10/2016 11:56:12	26/10/2016 18:56:16	10.58.174.145	La ubicación de la sesión de copia de seguridad es el Arcserve UDP Recovery Point Server [arcw2016svp1], almacén de datos [DS1].
	2	Montar punto de recuperación-26/10/2016 11:56:12	26/10/2016 18:56:16	10.58.174.145	El nombre de la tarea de montaje del punto de recuperación es Montar punto de recuperación-26/10/2016 11:56:12.
	2	Montar punto de recuperación-26/10/2016 11:56:12	26/10/2016 18:56:16	10.58.174.145	La tarea de montaje del punto de recuperación se ha iniciado correctamente.

3. Obtenga el directorio compartido para el punto de recuperación montado que aparece en el registro de actividad.

   Formato del directorio cuando se realiza el montaje a través de NFS:

   < servidord2d >:/opt/Arcserve/d2dserver/tmp/d2d_share_path<idtarea>

   Se puede acceder a los archivos del punto de recuperación montando el directorio.

   Ejemplo:

   mount *< servidord2d >:/opt/Arcserve/d2dserver/tmp/d2d_share_path<idtarea> /mnt*

   Formato del directorio cuando se realiza el montaje a través de WebDAV:

   https://<servidord2d>:8014/share/<nombre usuario>/

   Se puede acceder a los archivos del punto de recuperación mediante el explorador web o mediante el montaje del directorio.

   Ejemplo:

mount.dafs https://<servidord2d>:8014/share/<nombre usuario>/ /mnt

4. Introduzca el nombre de usuario y la contraseña introducidos para el envío de la tarea de montaje del punto de recuperación.

Esta sección incluye los siguientes temas:

- Instalación del paquete davfs en el servidor Linux

Instalación del paquete davfs en el servidor Linux

Se puede instalar el paquete davfs en el servidor Linux.

- Para Red Hat Linux, CentOS Linux u Oracle Linux

  Siga estos pasos:

  1. Obtenga los paquetes adicionales para Enterprise Linux (EPEL) para el servidor Linux con la versión coincidente de http://-fedoraproject.org/wiki/EPEL#How_can_I_use_these_extra_packa-ges.3F.
  2. Copie el paquete EPEL descargado en el servidor Linux de destino.
  3. Instale el paquete EPEL mediante el comando siguiente.

     # yum install <ruta_paquete>/epel-release-<información_versión>.rpm
  4. Instale el paquete davfs2 mediante el comando siguiente.

     # yum install davfs2

- Para SuSE Linux 12 SP1

  Siga estos pasos:

  1. Inicie sesión en el servidor Linux.
  2. Instale el paquete davfs2 mediante el comando siguiente.

     # zypper addrepo

     # zypper refresh

     # zypper install davfs2

  Para obtener más información, consulte el siguiente vínculo.

Cómo activar la compatibilidad para los kernels más recientes de RHEL, OEL (kernel de RHEL), Debian, SUSE y Ubuntu

RHEL, OEL (kernel de RHEL), Debian, SUSE y Ubuntu actualizan sus kernels regularmente, lo que da como resultado que los controladores enviados con la versión estén desactualizados. Además, el proceso de actualización automática del kernel elimina la necesidad de compilar y enviar manualmente un nuevo paquete del controlador mediante CFT para cada nuevo kernel. Aunque la desactivación del proceso automático de actualización del kernel de estos sistemas ayuda, Arcserve también es compatible con los kernels actualizados cuando sea necesario.

Importante: A pesar de hacer todo lo posible para admitir los kernels más recientes de RHEL, OEL (kernel de RHEL), Debian, SUSE y Ubuntu, es posible que los cambios importantes del kernel puedan retrasar o cancelar los controladores correspondientes.

Como gestor de almacenamiento, puede revisar los siguientes escenarios para activar el uso del Agente de Arcserve UDP (Linux) con los kernels más recientes de RHEL, OEL (kernel de RHEL), Debian, SUSE y Ubuntu:

- Si el servidor del Agente de Arcserve UDP (Linux) tiene una conexión activa a Internet, se descargan y se implementan de forma desatendida los controladores actualizados. Se puede utilizar el software sin esfuerzos adicionales.
- Si el servidor del Agente de Arcserve UDP (Linux) no tiene acceso a Internet, se puede descargar e implementar manualmente el paquete del controlador actualizado.
- Si tiene varios servidores del Agente de Arcserve UDP (Linux), se puede implementar el paquete del controlador actualizado en un servidor y, a continuación, se puede configurar el otro servidor para utilizarlo como un servidor de almacenamiento intermedio.

Realice los pasos siguientes para implementar el paquete del controlador actualizado:

- Revise de los requisitos previos
- Implementación manual del paquete del controlador de los kernels actualizados de RHEL, OEL (kernel de RHEL), Debian, SUSE y Ubuntu

- (Opcional) Utilización del servidor de almacenamiento intermedio para la actualización de controladores
- (Opcional) Configuración del servidor proxy HTTP

Revisión de los requisitos previos

Tenga en cuenta los siguientes requisitos previos:

- Debe disponer de las credenciales de inicio de sesión raíz para iniciar sesión en el servidor de copia de seguridad.
- Debe disponer de curl o wget instalado en el servidor de copia de seguridad.
- Debe disponer de gpg instalado en el servidor de copia de seguridad.

Implementación manual del paquete del controlador de los kernels actualizados de RHEL, OEL (kernel de RHEL), Debian, SUSE y Ubuntu

Cuando el servidor del Agente de Arcserve UDP (Linux) tiene acceso a Internet, todavía se pueden actualizar los controladores descargando e implementando de forma manual.

Siga estos pasos:

1. Descargue el paquete del controlador y el archivo de firma. Para obtener el vínculo de descarga, póngase en contacto con Soporte de Arcserve.

   Nota: Coloque el archivo de firma descargado y el paquete del controlador con el formato *.tar.gz en la ubicación de la carpeta de destino. No extraiga los archivos.

2. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
3. Vaya a la ubicación que contiene el paquete descargado e inicie la implementación usando los siguientes comandos:

   # source /opt/Arcserve/d2dserver/bin/setenv

   # /opt/Arcserve/d2dserver/bin/d2dupgradetool deploy <carpeta que contiene el paquete descargado>

   El paquete del controlador actualizado se ha implementado correctamente.

(Opcional) Utilización del servidor de almacenamiento intermedio para la actualización de controladores

Si se tienen varios servidores del Agente de Arcserve de UDP (Linux) que deben admitir los kernels más recientes de RHEL, OEL (kernel de RHEL), Debian, SUSE y Ubuntu, se pueden configurar para usar uno como el servidor de almacenamiento intermedio. Asegúrese de que el servidor de almacenamiento intermedio ya tenga implementado el controlador actualizado utilizando la conexión a Internet activa o que sigue las instrucciones de la tarea Implementación manual del paquete del controlador de los kernels actualizados de RHEL, OEL (kernel de RHEL), Debian, SUSE y Ubuntu. Se puede configurar cada servidor de copia de seguridad que necesite el paquete actualizado del controlador de RHEL, OEL (kernel de RHEL), Debian, SUSE y Ubuntu.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra y edite el archivo de configuración:

   # /opt/Arcserve/d2dserver/configfiles/auto_upgrade.cfg
3. Edite los siguientes elementos de configuración:

   scheme=<http o https>

   host=<dirección del servidor de almacenamiento intermedio>

   port=<puerto del servidor del Agente, normalmente 8014>

   La actualización automatizada del paquete de controladores se ha configurado correctamente.

(Opcional) Configuración del servidor proxy HTTP

Se puede configurar el servidor proxy para el Agente de Arcserve UDP (Linux) para tener acceso a la conexión a Internet.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra y edite el archivo de configuración:

   # /opt/Arcserve/d2dserver/configfiles/auto_upgrade.cfg
3. Edite los siguientes elementos de configuración:

   # /opt/Arcserve/d2dserver/configfiles/auto_upgrade.cfg

   http_proxy=<dirección del servidor proxy>

   proxy_user=<nombreusuario>

   proxy_password=<contraseña>

   El servidor proxy se ha configurado correctamente.

Cómo desactivar el bit SUID mientras se ejecuta la tarea de restauración de archivos

Mientras se ejecuta la tarea de restauración de archivos con las credenciales de usuario sudo (no raíz) del nodo de destino, el bit SUID se establece para que el binario de d2dtar aproveche su uso. Este binario de d2dtar se ejecuta en el nodo de destino durante la tarea de restauración de archivos. En algunos entornos, el uso del bit SUID está desactivado para la seguridad de los datos. Esta sección proporciona información sobre cómo desactivar el bit SUID para el binario de d2dtar.

Esta sección incluye los siguientes temas:

Revisión de los requisitos previos

Tenga en cuenta los siguientes requisitos previos:

- Dispone de las credenciales de inicio de sesión raíz para iniciar sesión en el servidor de copia de seguridad de Linux.
- Tiene las credenciales de inicio de sesión raíz del nodo de destino para modificar *sudoers*.

Configuración de los valores en el servidor de copia de seguridad de Linux

Esta sección proporciona información sobre cómo configurar los valores de configuración en el servidor de copia de seguridad de Linux.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad de Linux utilizando las credenciales raíz.
2. Vaya al archivo */opt/Arcserve/d2dserver/configfiles/server.env* y, a continuación, agregue la línea siguiente:

   "export FLR_DISABLE_SUID=1"

   Nota: Si el archivo *server.env* no existe en */opt/Arcserve/d2dserver/configfiles*, cree el archivo *server.env* y, a continuación, agregue la línea anterior al archivo *server.env*.
3. Para reiniciar d2dserver, ejecute el siguiente comando:

   # /opt/Arcserve/d2dserver/bin/d2dserver restart

Configuración de sudo para autorizar el binario de d2dtar en el nodo de destino

Esta sección proporciona información sobre cómo configurar sudo para autorizar el binario de d2dtar en el nodo de destino.

Siga estos pasos:

1. Inicie sesión en el nodo de destino utilizando las credenciales raíz.
2. Para editar el archivo de configuración, abra el archivo */etc/sudoer* con el comando *visudo*.
3. Añada la línea siguiente:

   <sudo-user> ALL=(ALL) NOPASSWD: /home/<usuario-sudo->/.d2drestorefile/d2dtar.64,/tmp/d2dtar.64

   Ejemplo: Si udplinux es un usuario sudo, añada la siguiente línea al archivo /etc/sudoers:

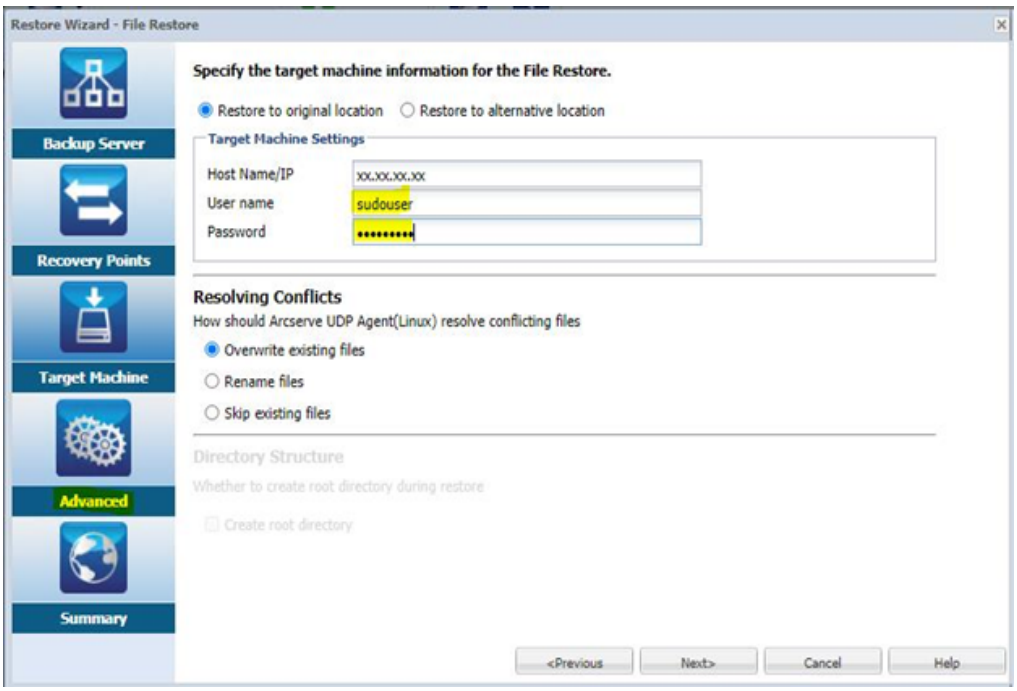
   udplinux ALL=(ALL) NOPASSWD: /home/udplinux/.d2drestorefile/d2dtar.64,/tmp/d2dtar.64

Ejecución de la tarea de restauración de archivos mediante las credenciales de usuario sudo del nodo de destino

Esta sección proporciona información sobre cómo ejecutar la tarea de restauración de archivos mediante las credenciales de usuario sudo.

Siga estos pasos:

1. Abra el asistente de restauración de archivos y, a continuación, complete los detalles según sea necesario.
2. En la página Opciones avanzadas, en Valores de configuración del equipo de destino, proporcione las credenciales de usuario sudo y, a continuación, ejecute la tarea de restauración de archivos.



El bit SUID se desactiva para el binario de d2dtar en el nodo de destino mientras se está ejecutando la tarea de restauración de archivos.

Capítulo 5: Solución de problemas

Esta sección incluye 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 SP3/SP4 y Oracle Linux Server 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 origen de restauración

mount.cifs             Montar el sistema de archivos del
recurso compartido de CIFS como destino de la copia de segu-
ridad y como origen de restauración

Los siguientes procesos deben estar en ejecución

Procesos inactivos                              Función afec-
tada

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. Vuelva a instalar el Agente de Arcserve UDP (Linux).

   Se ha instalado el Agente de Arcserve UDP (Linux) 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 SP3/SP4 y Oracle Linux Server 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.

El Agente de Arcserve UDP para la copia de seguridad de Linux puede producir un error al cambiar de una copia de seguridad sin agente a una copia de seguridad basada en el agente.

Síntoma

Cuando ya se ha realizado una copia de seguridad de la máquina virtual de Linux mediante la copia de seguridad sin agente de UDP (mediante el proxy de Windows) y se cambia a la copia de seguridad basada en el Agente de UDP (Linux), se puede producir un error en la tarea de copia de seguridad.

Solución

Como solución alternativa, antes de cambiar de la copia de seguridad sin agente a la copia de seguridad basada en el agente, haga lo siguiente:

1. Abra la máquina virtual de Linux de destino, vaya a la carpeta ***/tmp*** o a la ruta configurada como el directorio de trabajo.
2. Compruebe si existe el archivo *checkmachine.output.txt*. En caso afirmativo, suprima el archivo.
3. Vuelva a ejecutar la tarea de copia de seguridad de Linux.

La copia de seguridad de Linux se lleva a cabo 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 SP3/SP4 y Oracle Linux Server 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/Arcserve/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 RAID del software de Linux

Válido en CentOS 6.x, Red Hat Enterprise Linux (RHEL) 6.x, SUSE Linux Enterprise Server (SLES) 11.x SP3/SP4 y Oracle Linux Server 6.x

Síntoma

A veces se produce un error en el proceso de reconstrucción completa (BMR) al montar dispositivos RAID del software de Linux después de que el equipo de destino se reinicie.

Solución

Para solucionar este problema, reinicie el equipo de destino.

Se produce un error en el Agente de Arcserve UDP (Linux) al descargar e implementar los controladores actualizados de Ubuntu en SLES 11 y RHEL 6

Es válido en algunas de las versiones obsoletas de SUSE Linux Enterprise Server (SLES) 11 y de Red Hat Enterprise Linux (RHEL) 6

Síntoma

Cuando deseo realizar la copia de seguridad del nodo de Ubuntu que tiene la versión actualizada del kernel, se produce un error en la tarea de copia de seguridad y el mensaje en el registro de actividades se refiere a un error en la descarga y en la implementación de los controladores de Ubuntu.

Solución

Actualice los paquetes del sistema y compruebe si tiene la versión más reciente de curl o wget.

Siga estos pasos:

1. Reinicie el equipo de destino.
2. Ejecute el siguiente comando:

   En SUSE: zypper update wget curl

   En RHEL: yum update wget curl
3. Vuelva a ejecutar la tarea de copia de seguridad errónea en el nodo de Ubuntu.

El controlador de Ubuntu se ha actualizado correctamente.

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

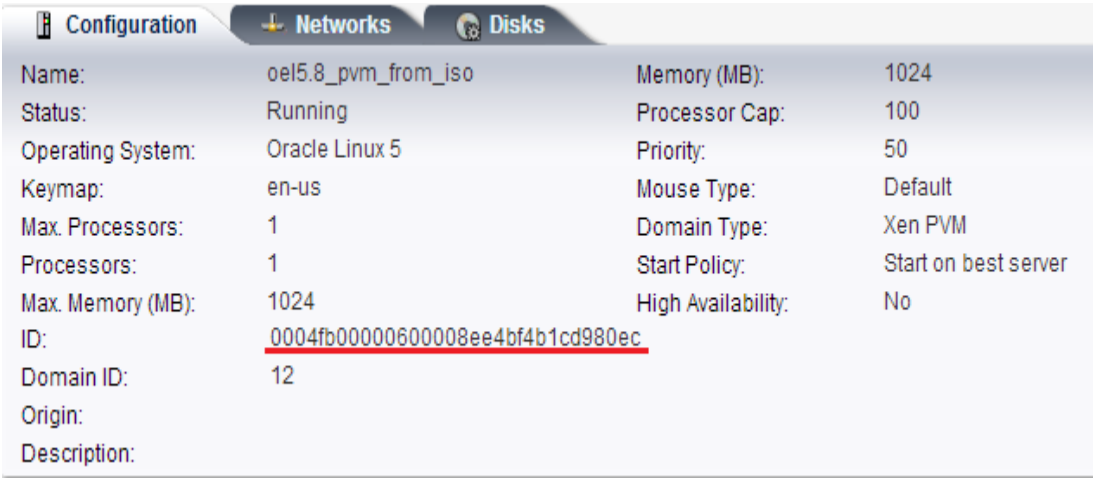
En un servidor de la máquina virtual de Oracle, cuando inicio el equipo paravirtual (PVM) mediante Live CD, veo una pantalla negra en la ventana del cliente de VNC.

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.

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 Arcserve.

   La incidencia se resuelve.

Se produce un error en la tarea de copia de seguridad en RHEL7.0 porque el servidor de copia de seguridad de Linux y el servidor de puntos de recuperación están en Windows Server 2019

Síntoma

Se produce un error en las tareas de copia de seguridad cuando se instala el servidor de puntos de recuperación en Windows Server 2019 y RHEL7.0 en el Agente de Linux, que utiliza el protocolo SMB1 mientras se monta CIFS y está desactivado en Windows Server 2019.

Solución

Para realizar la tarea de copia de seguridad correctamente, se debe activar el protocolo SMB1 en Windows Server 2019.

Siga estos pasos:

1. Para activar el protocolo SMB1 en Windows Server 2019, ejecute el siguiente comando:

   Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

2. Reinicie el servidor.

Se ejecuta la tarea de copia de seguridad correctamente.

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:

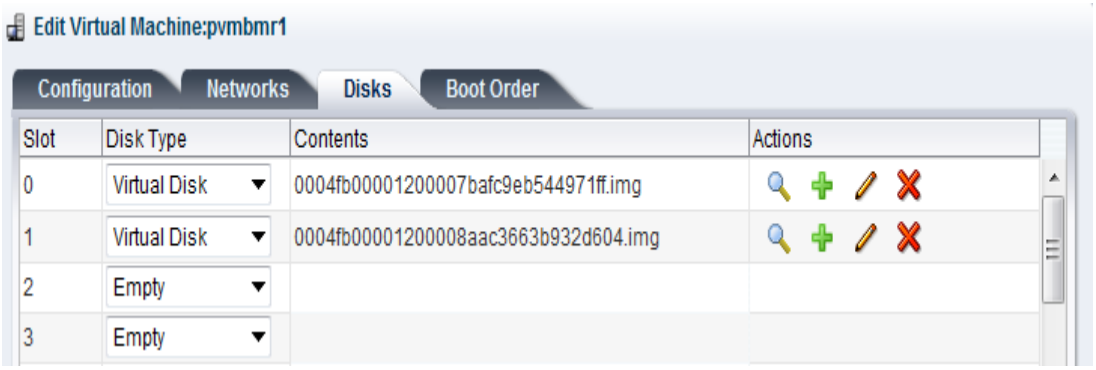
```
El volumen de inicio se restaura en el disco /dev/xxx. Ajuste la secuencia de arranque de disco en BIOS para iniciar /dev/xxx.
```

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.

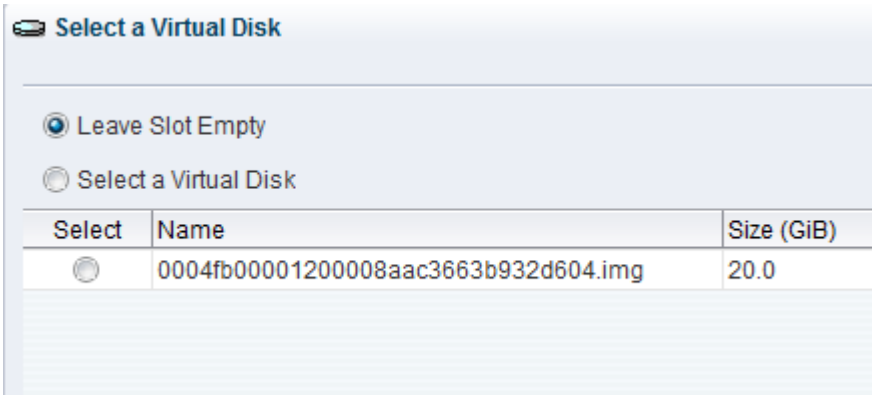


2. Seleccione Slot N como el disco de arranque.
3. Haga una nota del nombre de disco y el número de ranura N.

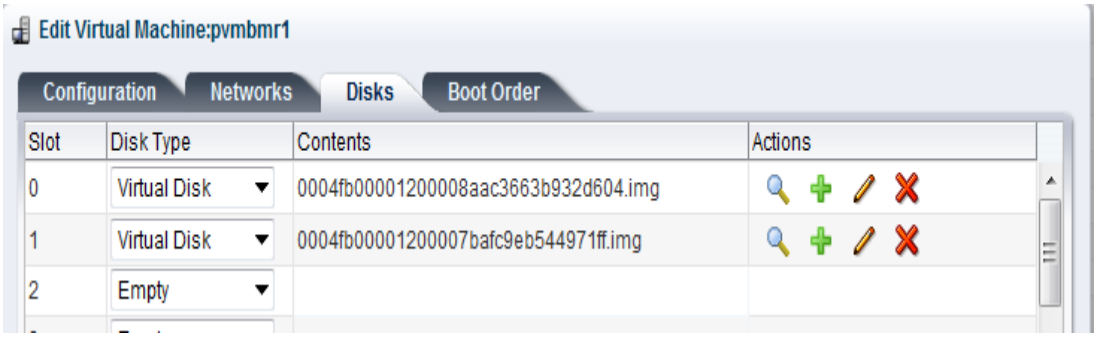
   Utilizará el nombre de disco y el número de ranura en los pasos posteriores.

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.

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/Arcserve/d2dserver.bak
```

Siga estos pasos:

1. Desinstale el servidor de copia de seguridad existente utilizando el siguiente comando:

   ```
   /opt/Arcserve/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/Arcserve/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/Arcserve/d2dserver.bak/* /opt/Arcserve/d2-
   dserver/
   ```

5. Inicie el servidor de copia de seguridad utilizando el siguiente comando:

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver start
   ```

   La versión instalada previamente del servidor de copia de seguridad se ha restaurado correctamente.

Cómo realizar copias de seguridad de las instancias de EC2 de Debian 9.X en la nube de AWS

Síntoma

Cuando la copia de seguridad se ejecuta para las instancias de EC2 de Debian 9.X en la nube de AWS, se produce un error en la tarea de copia de seguridad y no se muestra ningún error específico.

Solución

Cuando se crean las instancias de Debian 9.X en la nube de AWS y se agregan para proteger, es posible que si no dispone de los módulos de Perl se pueda producir el error. Para solucionar este problema, instale los paquetes utilizando los siguientes comandos:

sudo apt update

sudo apt install apt-file

sudo apt-file update

Se produce un error en el nodo de destino al iniciarse después de realizar la tarea de reconstrucción completa de migración para los nodos de Debian 10.8, 10.10 y 10.11

Síntoma

Cuando se realiza la tarea de reconstrucción completa de migración con la máquina virtual instantánea, se produce un error en el nodo de destino al iniciarse y, a continuación, se muestra el siguiente mensaje de error y se introduce el shell de recuperación *initramfs*:

Error de corrupción del sistema de archivos raíz

Solución

Como solución alternativa, haga lo siguiente:

1. Para comprobar y reparar el volumen de arranque, ejecute el siguiente comando fsck:

   (initramfs) fsck -yf /dev/sdX

2. Para salir del shell de rescate *initramfs*, ejecute el siguiente comando:

   (initramfs) exit

El nodo de destino se inicia correctamente.

Se produce un error en la máquina virtual al iniciar la tarea de máquina virtual instantánea o de recuperación asegurada en el servidor ESXi

Síntoma

Cuando se realiza una tarea de máquina virtual instantánea o de recuperación asegurada en el servidor de ESXi utilizando la sesión de la copia de seguridad sin agente y el nodo de origen también está en el servidor ESXi, la máquina virtual no se inicia en el sistema correctamente.

Solución

Es posible que la máquina virtual necesite la inserción de controladores. Se puede establecer una variable de entorno para activar.

Siga estos pasos:

1. Inicie sesión en el servidor de copia de seguridad como usuario raíz.
2. Abra el siguiente archivo server.env:

   ```
   /opt/Arcserve/d2dserver/configfiles/server.env
   ```

3. Actualice el parámetro siguiente en el archivo server.env y guarde el archivo:

   ```
   export HBBU_VM_RESTORE_DISABLE=1
   ```

4. Reinicie el servidor de copia de seguridad utilizando el siguiente comando:

   ```
   /opt/Arcserve/d2dserver/bin/d2dserver restart
   ```

La máquina virtual no se inicia cuando se utiliza el adaptador de red e1000e en el nodo de ESXi

Síntoma

Cuando se realiza una tarea de máquina virtual instantánea mediante el adaptador de red e1000e en el nodo de ESXi, es posible que la máquina virtual no se inicie en el sistema correctamente.

Solución

Se puede ejecutar una tarea de máquina virtual instantánea utilizando el resto de los controladores de interfaz de red (NIC) disponibles, pero no con el NIC de e1000e.

Se produce un error al iniciar la máquina virtual instantánea en Hyper-V para los nodos de origen de Debian 10.x

Síntoma

Si selecciona la opción **Servidor con GUI** mientras se instala cualquiera de estos nodos de origen como, por ejemplo, Debian 10.x en ESXI y realiza la tarea de máquina virtual instantánea a Hyper-V, es posible que el nodo de destino que se genera en Hyper-V no se inicie correctamente. Aunque los registros muestran que la tarea de máquina virtual instantánea se ha realizado correctamente, se produce un error al iniciarse correctamente.

Solución

Una vez que se haya creado el nodo de destino en la plataforma Hyper-V y que el estado o los registros de la tarea de máquina virtual instantánea a Hyper-V hayan finalizado correctamente, reinicie el nodo de destino manualmente. Después del reinicio, el nodo de destino abre la interfaz gráfica de usuario esperada.

Se produce un error al iniciar la máquina virtual instantánea en Hyper-V para el nodo de origen de RHEL 8.0/8.0

Síntoma

Si selecciona la opción **Servidor con GUI** mientras se instala RHEL 8.0 en ESXI y realiza la tarea de máquina virtual instantánea a Hyper-V, el nodo de destino que se

genera en Hyper-V no se inicia correctamente. Aunque los registros muestran que la tarea de máquina virtual instantánea se ha realizado correctamente, se produce un error al iniciarse.

Nota: Este problema está relacionado con Redhat 8.0 en la plataforma Hyper-V. Para obtener más información sobre este problema de Redhat 8.0, consulte el portal de Redhat.

A diferencia de la serie RHEL 7.x, cuando se selecciona la opción **Servidor con GUI** para la instalación de RHEL 8.0, los siguientes controladores no se instalan de forma predeterminada:

- xorg-x11-drv-fbdev
- xorg-x11-drv-vesa
- xorg-x11-drv-vmware

Solución 1

Como solución alternativa, siga estos pasos:

1. Después de instalar el nodo de origen de RHEL 8.0 en ESXI, instale los siguientes paquetes en el nodo:

   yum install xorg-x11-drv-fbdev xorg-x11-drv-vesa xorg-x11-drv-vmware -y
2. Realice una copia de seguridad.
3. Utilice la misma sesión de copia de seguridad del servidor de puntos de recuperación y ejecute la tarea de máquina virtual instantánea a Hyper-V.

Solución 2

Utilice esta solución alternativa cuando no se haya realizado la copia de seguridad después de instalar los siguientes controladores:

- xorg-x11-drv-fbdev
- xorg-x11-drv-vesa
- xorg-x11-drv-vmware

Como solución alternativa, siga estos pasos:

1. Después de realizar la tarea de máquina virtual instantánea a Hyper-V para la instancia de RHEL 8.0 presente en ESXI o después de instalar RHEL 8.0 en Hyper-V, obtenga la dirección IP en la ficha **Red** de Hyper-V.

   Nota: En este estado, la interfaz gráfica de usuario no está disponible en el nodo de la máquina virtual instantánea.

2. Conecte la máquina virtual a través de la aplicación SSH (como Putty) utilizando la dirección IP.
3. Instale los siguientes paquetes en el nodo.

   yum install xorg-x11-drv-fbdev xorg-x11-drv-vesa xorg-x11-drv-vmware -y
4. Reinicie el nodo.

Las tareas basadas en el Agente de Linux producen errores ocasionalmente

Síntoma

A veces, cuando se agregan más de 200 nodos de Linux en un plan, se producen errores en las tareas basadas en el Agente de Linux ocasionalmente y se muestra el error siguiente:

Se ha producido un error al conectar con el servidor de licencia.

Solución

Como solución alternativa, reduzca el número de tareas simultáneas. Por ejemplo, si el número de tareas simultáneas se establece en 48, se debe reducir a 30 y comprobar si se ha solucionado el error. La configuración de tareas simultáneas depende de los recursos del entorno como la E/S de disco, la memoria, la CPU en el servidor de la Consola de UDP y LBS. Se debe establecer el número de tareas simultáneas según cada entorno. Además, es posible que se deban agregar más nodos de LBS para dividir los planes para reducir la carga.

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 hiper-
visor. 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 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.

Error al montar CIFS en el servidor o en el nodo de destino

Síntoma

Cuando intento generar una copia de seguridad o restaurar usando CIFS, este sistema no puede realizar un montaje en el servidor o en el nodo de destino.

Solución

Se deben satisfacer algunos requisitos al montar CIFS en un equipo de Linux.

Siga estos pasos:

1. Utilice el comando mount en el servidor o en el nodo de destino para verificar el error.
2. Verifique que, al usar una ruta compartida exportada de un sistema que no sea de Windows, esta coincida con la ruta original en lo que respecta a las minúsculas y las mayúsculas.
3. Si el comando mount devuelve un error, compruebe si el tiempo del servidor o del nodo de destino está sincronizado con el servidor CIFS.
4. Si no encuentra el error, agregue algunas opciones al comando mount para intentarlo de nuevo.

   Por ejemplo, agregue “sec=ntlm” cuando reciba el error de permiso denegado.

5. Al diagnosticar el error, siga estos pasos:

   Para el error relacionado con el montaje de CIFS en el servidor

   1. Abra el archivo server.env de la siguiente ubicación:

      /opt/Arcserve/d2dserver/configfiles/server.env

   2. Agregue todas las opciones al archivo mediante el siguiente comando:

      export D2D_MOUNTOPTION=<options>

   c. Guarde el archivo y reinicie el servicio.

   Para el error relacionado con el montaje de CIFS en el nodo de destino

   1. Abra el archivo .bashrc en la ruta principal del usuario.

      Ejemplo: La ubicación de un usuario es */home/user/* y de la raíz es */root/*.

   2. Agregue todas las opciones al archivo mediante el siguiente comando:

      export D2D_MOUNTOPTION=<options>

   c. Guarde el archivo.

Nota: El archivo .bashrc es el archivo recomendado aquí, pero también se pueden modificar otros archivos como, por ejemplo, /etc/profile, /etc/bashrc y así sucesivamente.

6. Verifique que, al usar una ruta compartida exportada de un sistema que no sea de Windows, esta coincida con la ruta original en lo que respecta a las minúsculas y las mayúsculas.

Error de restauración a nivel del archivo en una máquina virtual de Linux basada en el host debido a un sistema de archivos no compatible

Síntoma

Cuando realizo una restauración de nivel de archivo en una máquina virtual de Linux basada en el host, el asistente de restauración muestra el mensaje de error siguiente:

No compatible: sistema de archivos reiserfs

El error se produce porque se está intentando restaurar un sistema de archivos no compatible.

Solución

Se pueden restaurar máquinas virtuales de Linux basadas en host mediante alguna de las formas siguientes:

- Se puede utilizar el Live CD del 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. Se trata de una solución práctica, aunque temporal. Se puede restaurar mediante un Live CD si no se restaura este nodo con frecuencia.
- Otro método permanente es instalar el controlador del sistema de archivos correcto para admitir reiserfs o activar el controlador correspondiente que ya esté instalado en el servidor de copia de seguridad.

No se puede restaurar el volumen del sistema de SUSE15 con el sistema de archivos XFS

Síntoma

Cuando se realiza una tarea de restauración utilizando el punto de recuperación de SUSE15 con el sistema de archivos XFS, se produce un error en la tarea de restauración porque no se ha montado el volumen del sistema y aparecerá el siguiente mensaje de advertencia en el registro de actividad: *Se ha producido un error al montar el volumen del sistema. Es posible que el sistema no se inicie después de la restauración.*

Solución

Cree un CentOS 7.5 Live CD y utilice este Live CD para realizar la reconstrucción completa instantánea con el comando sudo apt install apt-file.

Se ha producido un error al acceder a la dirección URL del punto de recuperación de montaje compartido por WebDAV

Síntoma

Al realizar la tarea de punto de recuperación de montaje compartida con WebDAV y a la que acceden varios usuarios que utilizan el mismo servidor de copia de seguridad de Linux, solo el acceso a la primera dirección URL se realiza correctamente y se produce un error en las direcciones URL restantes.
Este error se produce porque Arcserve no admite el acceso a las direcciones URL compartidas por varios usuarios desde el mismo explorador.

Solución

Utilice diferentes exploradores para acceder a las direcciones URL o borre las cookies e inténtelo de nuevo.

Se produce un error en la implementación de los controladores de Ubuntu utilizando el comando d2dupgradetool en Ubuntu 20.04 LBS

Síntoma

Al descargar el archivo de archivado de los controladores y los archivos de firma, el comando curl produce el siguiente error:

cURL error 35: error:1414D172:SSL routines:tls12_check_peer_sigalg:wrong signature type

Solución

Actualice OpenSSL 1.1.1f a OpenSSL 1.1.1g en Ubuntu 20.04 LBS.