Tutoriales

Cloud Manager 3.8

NetApp
March 25, 2024

Tabla de contenidos

Tutoriales

Copiar ACL entre recursos compartidos de SMB

Cloud Sync puede copiar listas de control de acceso (ACL) entre un recurso compartido de SMB de origen y un recurso compartido de SMB de destino. Si es necesario, puede conservar manualmente las ACL usted mismo mediante robocopy.

Opciones

- Configure Cloud Sync para que copie automáticamente las ACL
- Copie manualmente las ACL usted mismo

Configurar Cloud Sync para copiar ACL entre servidores SMB

Copiar ACL entre servidores de SMB habilitando una configuración cuando se crea una relación o después de crear una relación.

Tenga en cuenta que esta función está disponible para las nuevas relaciones de sincronización creadas después de la versión 23 de febrero de 2020. Si desea utilizar esta característica con relaciones existentes creadas antes de esa fecha, deberá volver a crear la relación.

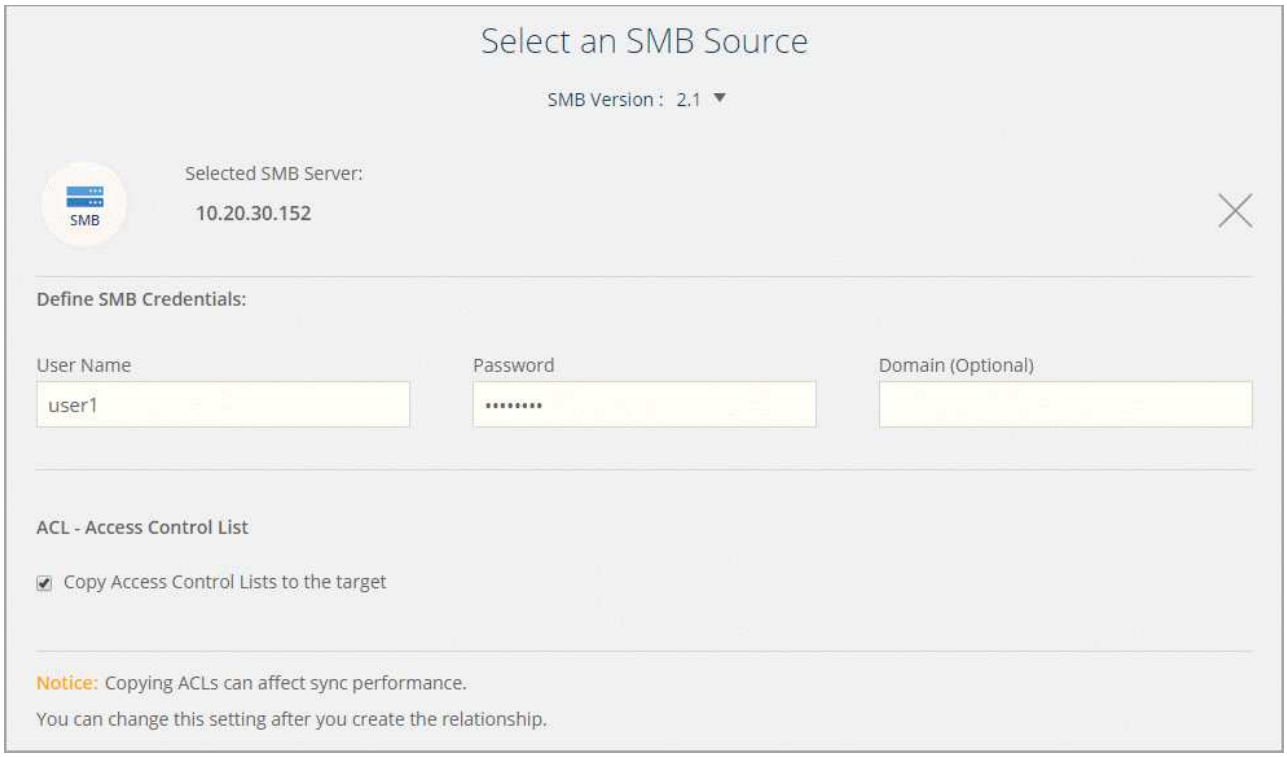
Lo que necesitará

- Una nueva relación de sincronización o una relación de sincronización existente creada después de la versión del 23 de febrero de 2020.
- Cualquier tipo de agente de datos.

  Esta función funciona con *any* type de agente de datos: AWS, Azure, Google Cloud Platform o agente de datos en las instalaciones. Se puede ejecutar el agente de datos en las instalaciones "cualquier sistema operativo compatible".

Pasos para una nueva relación

1. En Cloud Sync, haga clic en **Crear nueva sincronización**.
2. Arrastre y suelte **SMB Server** al origen y al destino y haga clic en **continuar**.
3. En la página **SMB Server**:
   a. Introduzca un nuevo servidor SMB o seleccione un servidor existente y haga clic en **continuar**.
   b. Introduzca credenciales para el servidor SMB.
   c. Seleccione **Copiar listas de control de acceso al destino** y haga clic en **continuar**.



4. Siga el resto de las indicaciones para crear la relación de sincronización.

Pasos para una relación existente

1. Pase el ratón por la relación de sincronización y haga clic en el menú de acción.
2. Haga clic en **Configuración**.
3. Seleccione **Copiar listas de control de acceso al destino**.
4. Haga clic en **Guardar configuración**.

Resultado

Al sincronizar datos, Cloud Sync conserva las ACL entre los recursos compartidos de SMB de origen y de destino.

Copia manual de ACL

Se pueden conservar manualmente las ACL entre recursos compartidos de SMB mediante el comando Windows robocopy.

Pasos

1. Identifique un host Windows con acceso completo a ambos recursos compartidos SMB.
2. Si alguno de los extremos requiere autenticación, utilice el comando **net use** para conectarse a los extremos desde el host de Windows.

   Debe realizar este paso antes de utilizar robocopy.

3. En Cloud Sync, cree una nueva relación entre los recursos compartidos de SMB de origen y de destino, o sincronice una relación existente.
4. Una vez finalizada la sincronización de datos, ejecute el siguiente comando desde el host de Windows para sincronizar las ACL y la propiedad:

```
robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots
/UNILOG:”[logfilepath]
```

Se deben especificar tanto *source* como *target* con el formato UNC. Por ejemplo: \\<servidor>\<recurso compartido>\<ruta>

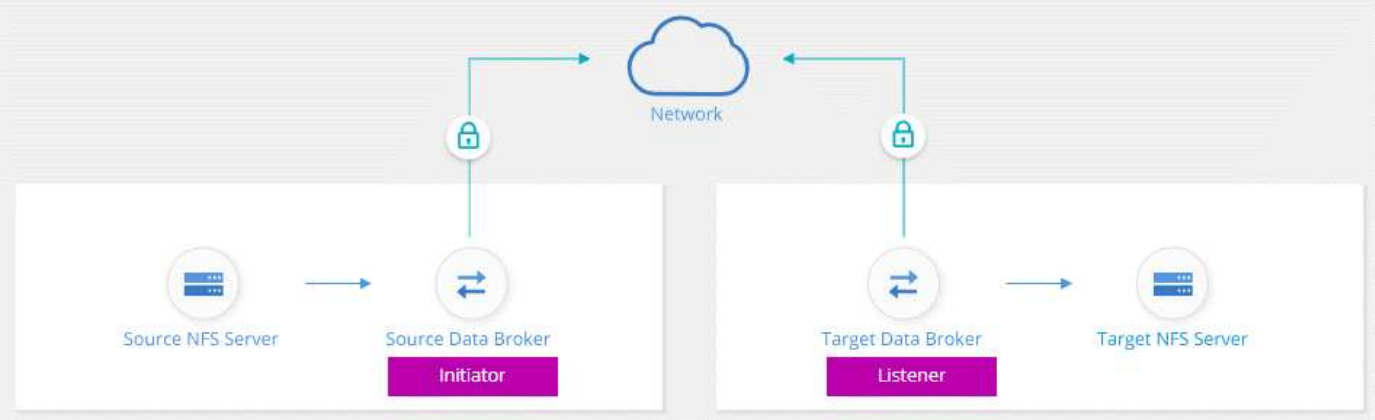
Sincronizando los datos NFS mediante el cifrado de datos en tránsito

Si su negocio tiene políticas de seguridad estrictas, puede sincronizar datos NFS mediante el cifrado de datos en tránsito. Esta función es compatible desde un servidor NFS a otro servidor NFS y de Azure NetApp Files a Azure NetApp Files.

Por ejemplo, se recomienda sincronizar datos entre dos servidores NFS que se encuentran en redes diferentes. O puede que necesite transferir datos de Azure NetApp Files de manera segura en subredes o regiones.

Cómo funciona el cifrado de datos en tiempo real

El cifrado en tiempo real de los datos cifra los datos NFS cuando se envían a través de la red entre dos gestores de datos. La siguiente imagen muestra una relación entre dos servidores NFS y dos agentes de datos:



Un agente de datos funciona como el *initiator*. Cuando es hora de sincronizar datos, envía una solicitud de conexión al otro intermediario de datos, que es el *listener*. Ese agente de datos escucha las solicitudes en el puerto 443. Puede utilizar un puerto diferente, si es necesario, pero asegúrese de comprobar que el puerto no está en uso por otro servicio.

Por ejemplo, si sincroniza datos de un servidor NFS local con un servidor NFS basado en cloud, puede elegir el agente de datos que escucha las solicitudes de conexión y que las envía.

Así es como funciona el cifrado en tránsito:

1. Después de crear la relación de sincronización, el iniciador inicia una conexión cifrada con el otro agente de datos.
2. El agente de datos de origen cifra los datos del origen mediante TLS 1.3.

3. A continuación, envía los datos a través de la red al agente de datos de destino.
4. El agente de datos de destino descifra los datos antes de enviarlos al destino.
5. Después de la copia inicial, el servicio sincroniza los datos modificados cada 24 horas. Si hay datos que sincronizar, el proceso comienza con el iniciador abriendo una conexión cifrada con el otro agente de datos.

   Si prefiere sincronizar datos con mayor frecuencia, "se puede cambiar la programación después de crear la relación".

Versiones NFS compatibles

- En los servidores NFS, el cifrado de datos en tránsito es compatible con las versiones 3, 4.0, 4.1 y 4.2 de NFS.
- En Azure NetApp Files, el cifrado de datos en tiempo real es compatible con las versiones 3 y 4.1 de NFS.

Lo que necesitará para comenzar

No olvide disponer de lo siguiente:

- Dos servidores NFS que cumplen "requisitos de origen y objetivo" O Azure NetApp Files en dos subredes o regiones.
- Las direcciones IP o los nombres de dominio completos de los servidores.
- Ubicaciones de red para dos agentes de datos.

  Puede seleccionar un agente de datos existente pero debe funcionar como iniciador. El agente de datos del listener debe ser un agente de datos *new*.

  Si aún no ha implementado un agente de datos, revise los requisitos de Data Broker. Debido a que tiene directivas de seguridad estrictas, asegúrese de revisar los requisitos de red, que incluyen tráfico saliente desde el puerto 443 y el "puntos finales de internet" que el agente de datos se pone en contacto con.

  - "Revise la instalación de AWS"
  - "Revise la instalación de Azure"
  - "Revise la instalación de GCP"
  - "Revise la instalación del host Linux"

Sincronizando los datos NFS mediante el cifrado de datos en tránsito

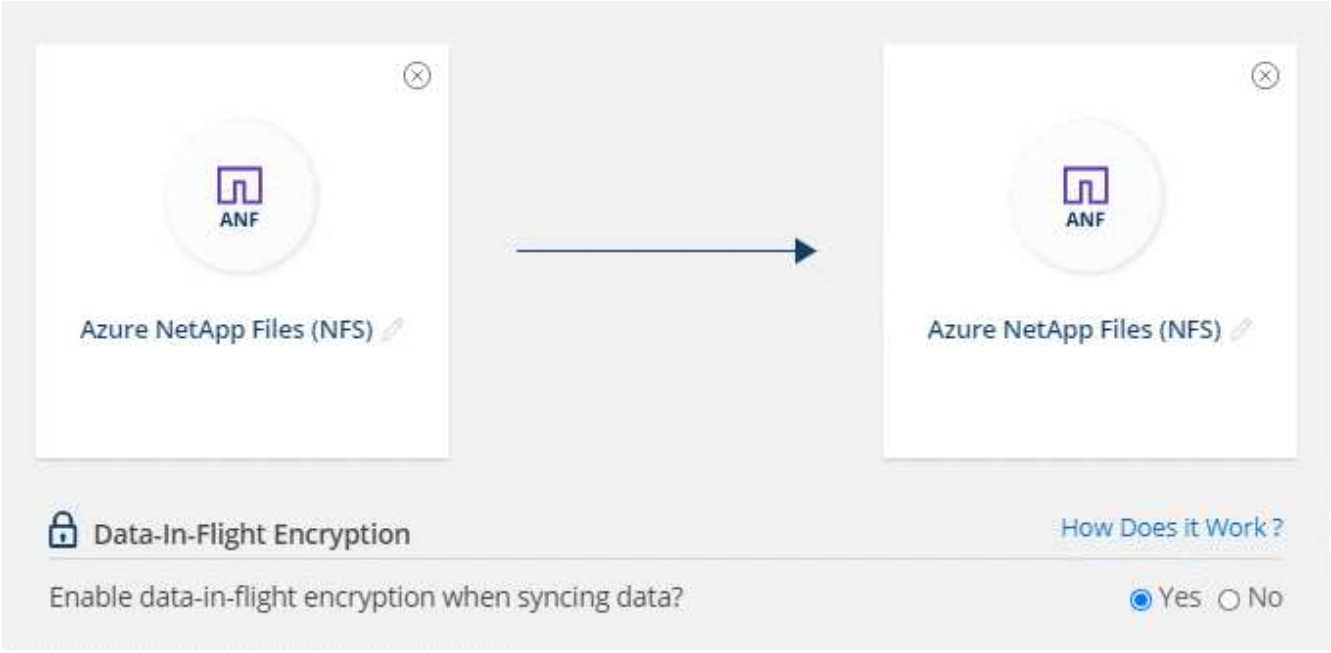
Cree una nueva relación de sincronización entre dos servidores NFS o entre Azure NetApp Files, habilite la opción de cifrado en curso y siga las indicaciones.

Pasos

1. Haga clic en **Crear nueva sincronización**.
2. Arrastre y suelte **servidor NFS** a las ubicaciones de origen y destino o **Azure NetApp Files** a las ubicaciones de origen y destino y seleccione **Sí** para activar el cifrado de datos en vuelo.

   En la siguiente imagen se muestra lo que seleccionaría para sincronizar datos entre dos servidores NFS:

La siguiente imagen muestra lo que seleccionaría para sincronizar datos entre Azure NetApp Files:



3. Siga las indicaciones para crear la relación:

   a. **NFS Server/Azure NetApp Files**: Elija la versión NFS y, a continuación, especifique un nuevo origen NFS o seleccione un servidor existente.

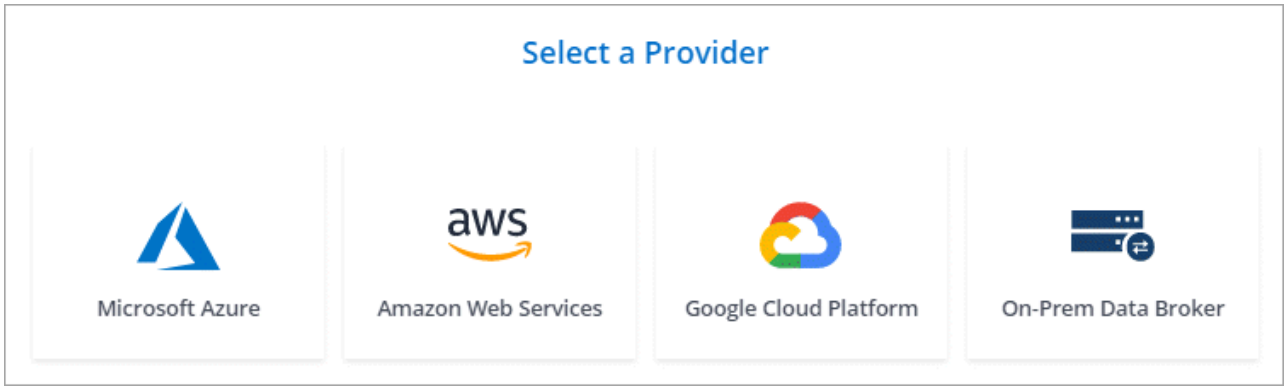
   b. **definir la funcionalidad de Data Broker**: Defina qué intermediario de datos *escucha* las solicitudes de conexión de un puerto y cuál *inicia* la conexión. Elija en función de sus requisitos de red.

   c. **Data Broker**: Siga las indicaciones para agregar un nuevo intermediario de datos de origen o seleccionar un intermediario de datos existente.

      Si el agente de datos de origen actúa como oyente, debe ser un nuevo agente de datos.

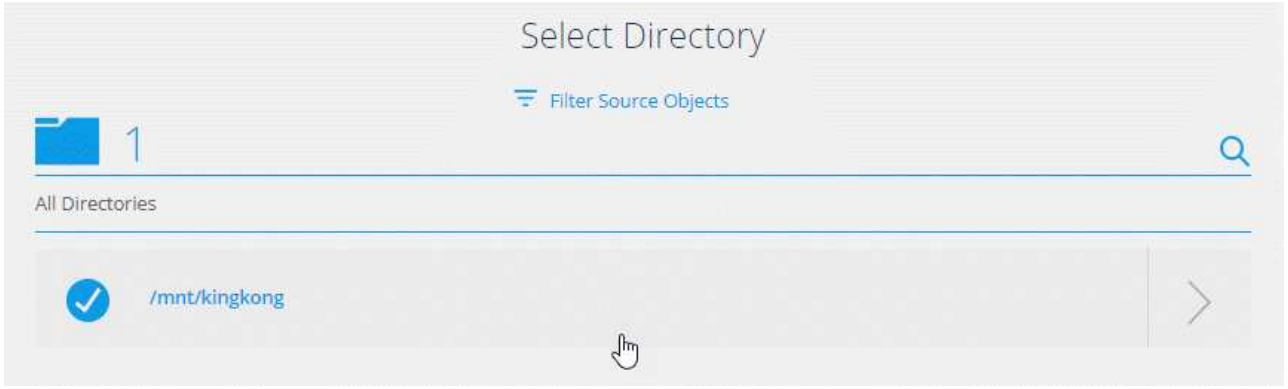
      Si necesita un nuevo agente de datos, Cloud Sync le pedirá las instrucciones de instalación. Puede

desplegar el agente de datos en el cloud o descargar un script de instalación para su propio host Linux.



d. **directorios**: Elija los directorios que desea sincronizar seleccionando todos los directorios, o taladrando y seleccionando un subdirectorio.

   Haga clic en **Filtrar objetos de origen** para modificar la configuración que define cómo se sincronizan y mantienen los archivos y carpetas de origen en la ubicación de destino.

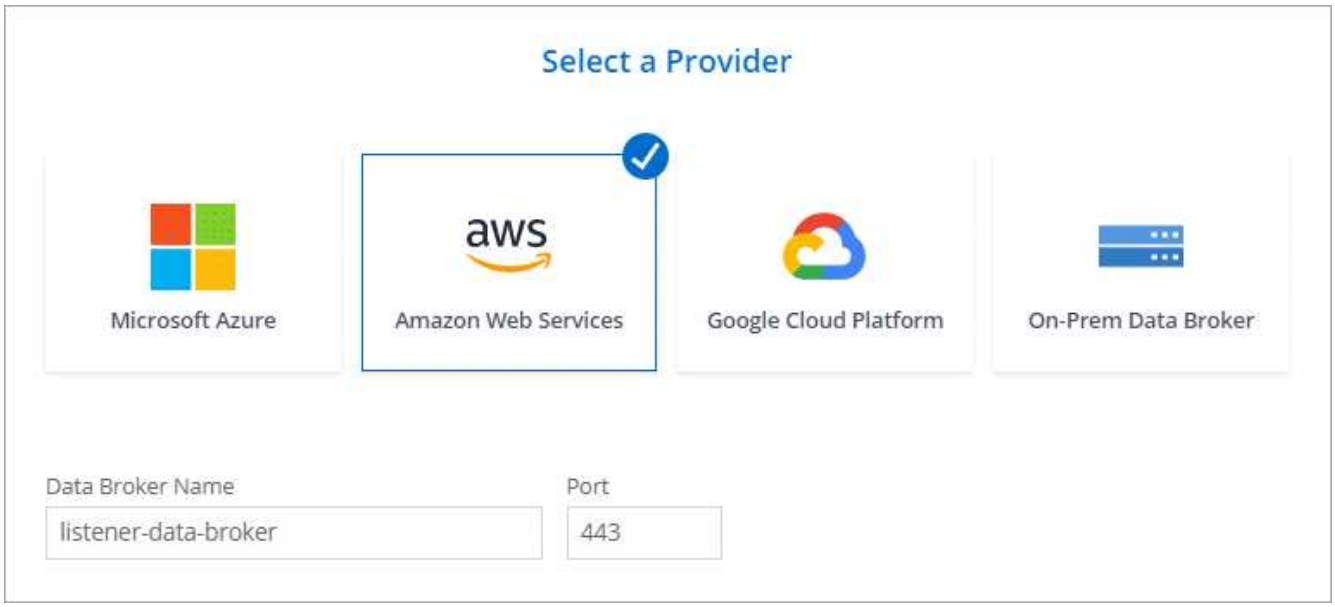


e. **servidor NFS de destino/Azure NetApp Files de destino**: Elija la versión NFS y, a continuación, introduzca un destino NFS nuevo o seleccione un servidor existente.

f. **Target Data Broker**: Siga las indicaciones para agregar un nuevo intermediario de datos de origen o seleccionar un intermediario de datos existente.

   Si el agente de datos de destino actúa como oyente, debe ser un nuevo agente de datos.

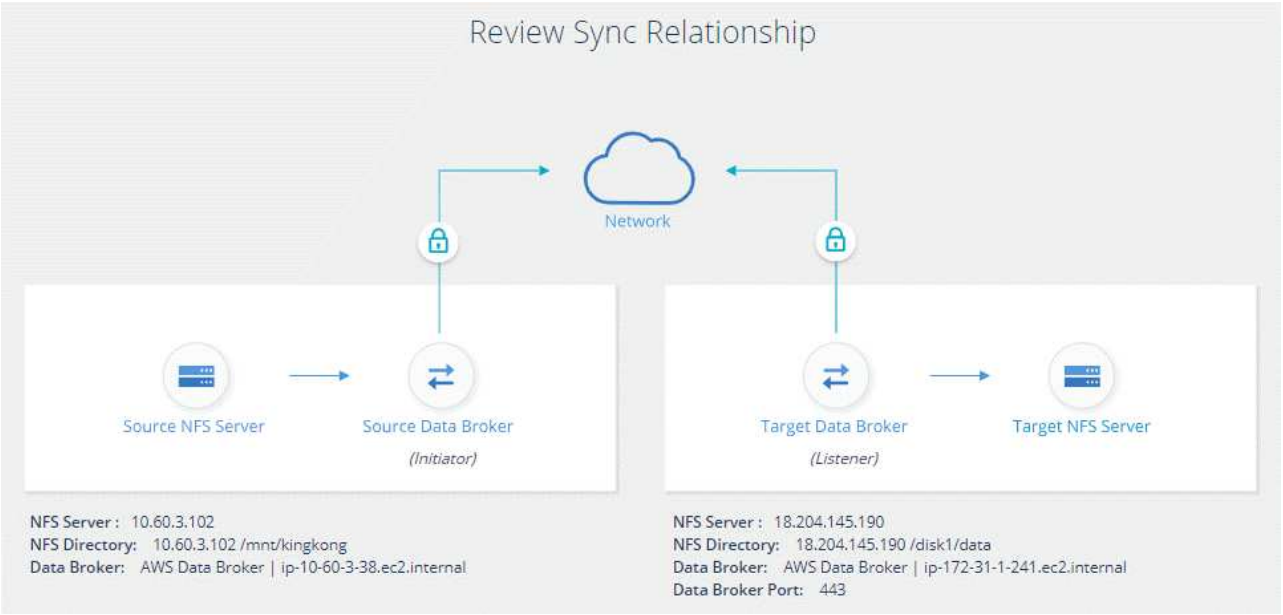
   A continuación se muestra un ejemplo del mensaje en el que el agente de datos de destino funciona como el listener. Observe la opción para especificar el puerto.



a. **directorios de destino**: Seleccione un directorio de nivel superior o examine para seleccionar un subdirectorio existente o crear una nueva carpeta dentro de una exportación.

b. **Configuración**: Defina cómo se sincronizan y mantienen los archivos y carpetas de origen en la ubicación de destino.

c. **Revisión**: Revise los detalles de la relación de sincronización y haga clic en **Crear relación**.



Resultado

Cloud Sync comienza a crear la nueva relación de sincronización. Cuando haya terminado, haga clic en **Ver en Panel** para ver detalles sobre la nueva relación.

Información de copyright

Información de la marca comercial