Sincronizar datos entre un origen y un destino

NetApp Copy and Sync

NetApp
December 16, 2025

Tabla de contenidos

Sincronizar datos entre un origen y un destino

Prepare un agente de datos para sincronizar datos entre el almacenamiento de objetos en NetApp Copy and Sync

Si planea sincronizar datos de un almacenamiento de objetos a otro (por ejemplo, Amazon S3 a Azure Blob) en NetApp Copy and Sync, entonces debe preparar el grupo de agentes de datos antes de crear la relación de sincronización.

Acerca de esta tarea

Para preparar el grupo de intermediarios de datos, deberá modificar la configuración del escáner. Si no modifica la configuración, es posible que observe problemas de rendimiento en esta relación de sincronización.

Antes de empezar

El grupo de intermediarios de datos que utiliza para sincronizar datos de un almacenamiento de objetos a otro solo debe administrar este tipo de relaciones de sincronización. Si el grupo de intermediarios de datos administra un tipo diferente de relación de sincronización (por ejemplo, NFS a NFS o almacenamiento de objetos a SMB), el rendimiento de esas relaciones de sincronización podría verse afectado negativamente.

Pasos

1. "Iniciar sesión en Copiar y sincronizar" .
2. En Copiar y sincronizar, seleccione **Administrar intermediarios de datos**.
3. Seleccionar 
4. Actualizar la configuración del escáner:
   a. Cambie **Concurrencia del escáner** a **1**.
   b. Cambie el **Límite de procesos del escáner** a **1**.
5. Seleccione **Unificar configuración**.

Resultado

Copiar y sincronizar actualiza la configuración del grupo de intermediarios de datos.

¿Que sigue?

Ahora puede crear la relación de sincronización entre el almacenamiento de objetos utilizando el grupo de intermediarios de datos que acaba de configurar.

Crear relaciones de sincronización en NetApp Copy and Sync

Cuando se crea una relación de sincronización, NetApp Copy and Sync copia archivos del origen al destino. Después de la copia inicial, Copiar y sincronizar sincroniza cualquier dato modificado cada 24 horas.

Antes de poder crear algunos tipos de relaciones de sincronización, primero deberá crear un sistema en la NetApp Console.

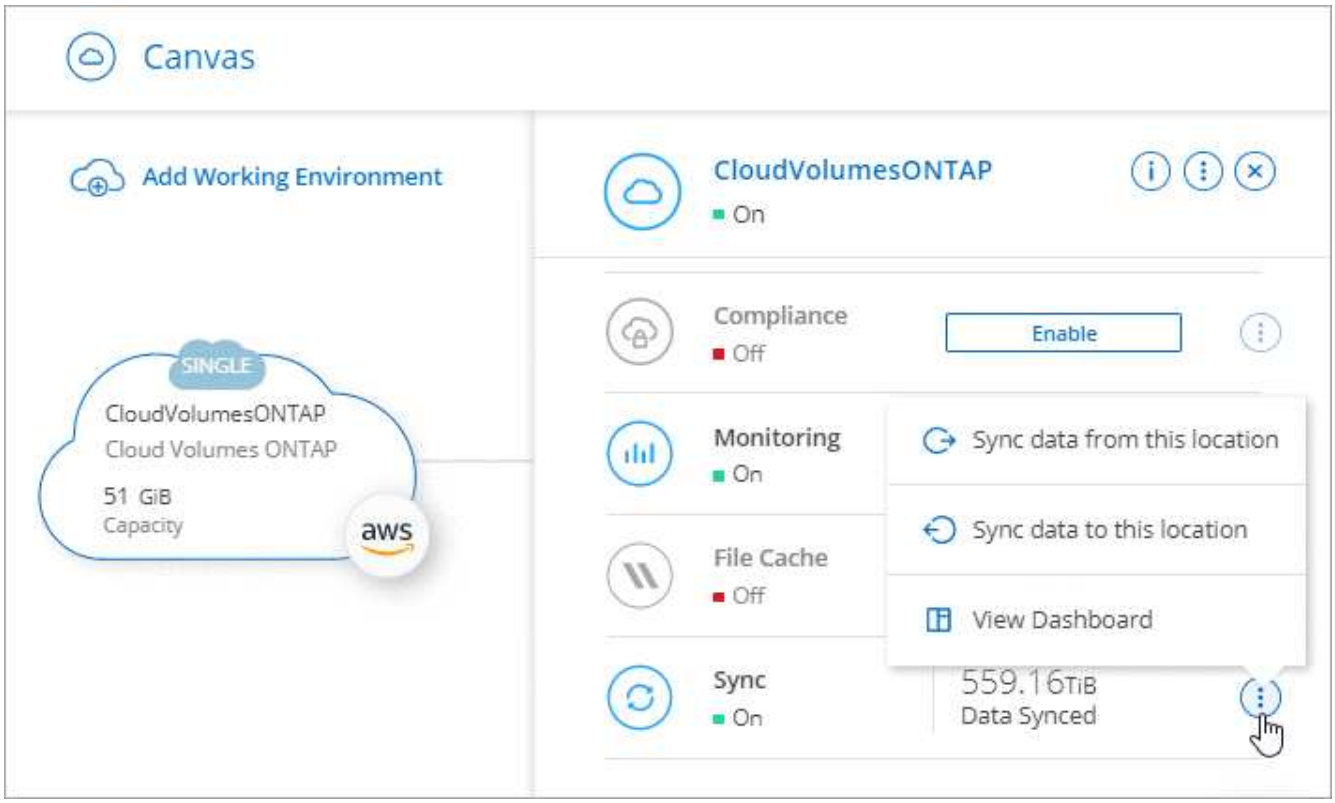
Crear relaciones de sincronización para tipos específicos de sistemas

Si desea crear relaciones de sincronización para cualquiera de los siguientes, primero debe crear o descubrir el sistema:

- Amazon FSx para ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Clústeres ONTAP locales

Pasos

1. "Iniciar sesión en Copiar y sincronizar" .
2. Crear o descubrir el sistema.
   - "Cree un sistema Amazon FSx para ONTAP"
   - "Configuración y detección de Azure NetApp Files"
   - "Lanzamiento de Cloud Volumes ONTAP en AWS"
   - "Lanzamiento de Cloud Volumes ONTAP en Azure"
   - "Lanzamiento de Cloud Volumes ONTAP en Google Cloud"
   - "Agregar sistemas Cloud Volumes ONTAP existentes"
   - "Descubriendo los clústeres de ONTAP"
3. Seleccione **Página de sistemas**.
4. Seleccione un sistema que coincida con cualquiera de los tipos enumerados anteriormente.
5. Seleccione el menú de acción junto a Sincronizar.



6. Seleccione **Sincronizar datos desde esta ubicación** o **Sincronizar datos con esta ubicación** y siga las instrucciones para configurar la relación de sincronización.

Crear otros tipos de relaciones de sincronización

Utilice estos pasos para sincronizar datos hacia o desde un tipo de almacenamiento compatible que no sea Amazon FSx para ONTAP, Azure NetApp Files, Cloud Volumes ONTAP o clústeres de ONTAP locales. Los pasos a continuación proporcionan un ejemplo que muestra cómo configurar una relación de sincronización desde un servidor NFS a un depósito S3.

1. En la NetApp Console, seleccione **Sincronizar**.
2. En la página **Definir relación de sincronización**, elija un origen y un destino.

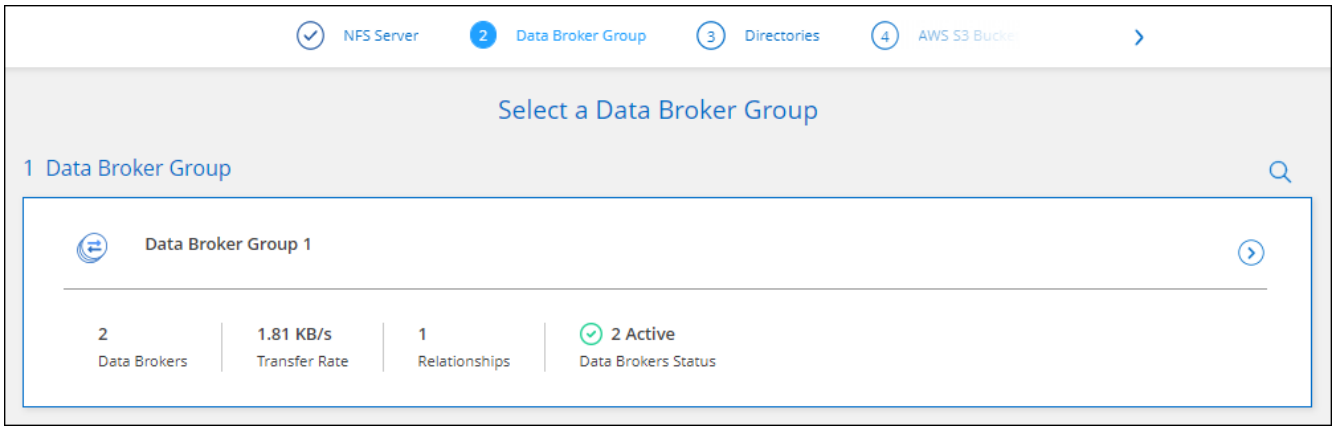
   Los siguientes pasos proporcionan un ejemplo de cómo crear una relación de sincronización desde un servidor NFS a un depósito S3.

3. En la página **Servidor NFS**, ingrese la dirección IP o el nombre de dominio completo del servidor NFS que desea sincronizar con AWS.
4. En la página **Grupo de agente de datos**, siga las instrucciones para crear una máquina virtual de agente de datos en AWS, Azure o Google Cloud Platform, o para instalar el software de agente de datos en un host Linux existente.

   Para más detalles, consulte las siguientes páginas:

- "Crear un agente de datos en AWS"
- "Crear un agente de datos en Azure"
- "Crear un agente de datos en Google Cloud"
- "Instalación del agente de datos en un host Linux"

5. Después de instalar el agente de datos, seleccione **Continuar**.

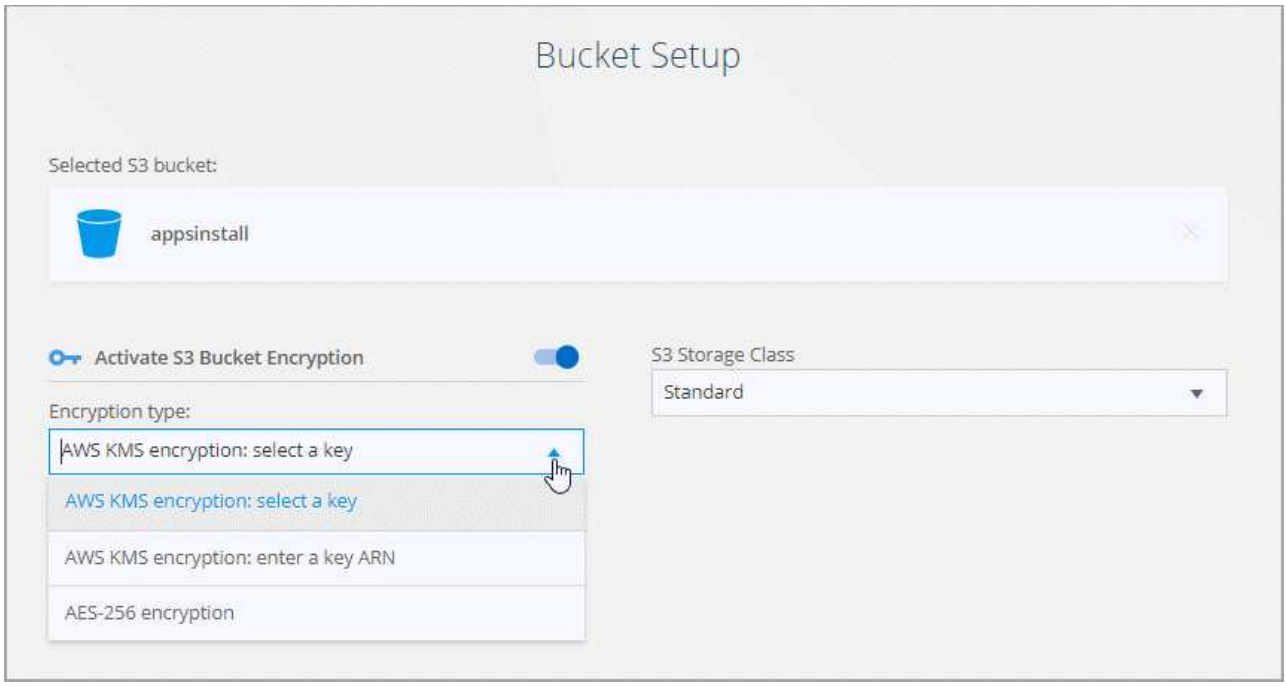


6. En la página **Directorios**, seleccione un directorio o subdirectorio de nivel superior.

   Si Copiar y sincronizar no puede recuperar las exportaciones, seleccione **Agregar exportación manualmente** e ingrese el nombre de una exportación NFS.

   Si desea sincronizar más de un directorio en el servidor NFS, deberá crear relaciones de sincronización adicionales una vez que haya terminado.

7. En la página **AWS S3 Bucket**, seleccione un bucket:
   - Desplácese hacia abajo para seleccionar una carpeta existente dentro del depósito o para seleccionar una nueva carpeta que cree dentro del depósito.
   - Seleccione **Agregar a la lista** para seleccionar un depósito S3 que no esté asociado con su cuenta de AWS. "Se deben aplicar permisos específicos al bucket S3" .
8. En la página **Configuración del depósito**, configure el depósito:
   - Elija si desea habilitar el cifrado del bucket S3 y luego seleccione una clave AWS KMS, ingrese el ARN de una clave KMS o seleccione el cifrado AES-256.
   - Seleccione una clase de almacenamiento S3. "Ver las clases de almacenamiento admitidas" .



9. En la página **Configuración**, defina cómo se sincronizan y mantienen los archivos y carpetas de origen en la ubicación de destino:

Cronograma

Elija una programación recurrente para sincronizaciones futuras o desactive la programación de sincronización. Puede programar una relación para sincronizar datos con una frecuencia de hasta 1 minuto.

Tiempo de espera de sincronización

Define si Copiar y sincronizar debe cancelar una sincronización de datos si la sincronización no se ha completado en la cantidad especificada de minutos, horas o días.

Notificaciones

Le permite elegir si desea recibir notificaciones de copia y sincronización en el Centro de notificaciones de la consola de NetApp . Puede habilitar notificaciones para sincronizaciones de datos exitosas, fallidas y canceladas.

Reintentos

Define la cantidad de veces que Copiar y sincronizar debe volver a intentar sincronizar un archivo antes de omitirlo.

Sincronización continua

Después de la sincronización de datos inicial, Copy and Sync escucha los cambios en el depósito S3 de origen o en el depósito de Google Cloud Storage y sincroniza continuamente cualquier cambio con el destino a medida que se produce. No es necesario volver a escanear la fuente a intervalos programados.

Esta configuración solo está disponible cuando se crea una relación de sincronización y cuando se sincronizan datos desde un bucket S3 o Google Cloud Storage con Azure Blob Storage, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS, S3 y StorageGRID **o** desde Azure Blob Storage con Azure Blob Storage, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS y StorageGRID.

Si habilita esta configuración, afectará otras funciones de la siguiente manera:

- La programación de sincronización está deshabilitada.
- Las siguientes configuraciones vuelven a sus valores predeterminados: Tiempo de espera de sincronización, Archivos modificados recientemente y Fecha de modificación.
- Si S3 es la fuente, el filtro por tamaño estará activo solo en eventos de copia (no en eventos de eliminación).
- Una vez creada la relación, solo puedes acelerarla o eliminarla. No puedes cancelar sincronizaciones, modificar configuraciones ni ver informes.

  Es posible crear una relación de sincronización continua con un depósito externo. Para ello siga estos pasos:

  i. Vaya a la consola de Google Cloud para el proyecto del depósito externo.

  ii. Vaya a **Almacenamiento en la nube > Configuración > Cuenta de servicio de almacenamiento en la nube**.

  iii. Actualice el archivo local.json:

  ```
  {
  "protocols": {
      "gcp": {
          "storage-account-email": <storage account email>
  }
  }
  }
  ```

  iv. Reiniciar el agente de datos:

  A. sudo pm2 detener todo

  B. sudo pm2 start all

  v. Cree una relación de sincronización continua con el depósito externo relevante.

  > Un agente de datos utilizado para crear una relación de sincronización continua con un depósito externo no podrá crear otra relación de sincronización continua con un depósito en su proyecto.

Comparar por

Elija si Copiar y sincronizar debe comparar ciertos atributos al determinar si un archivo o directorio ha cambiado y debe sincronizarse nuevamente.

Incluso si desmarca estos atributos, Copiar y sincronizar aún compara el origen con el destino verificando las rutas, los tamaños de archivo y los nombres de archivo. Si hay algún cambio, sincroniza esos archivos y directorios.

Puede elegir habilitar o deshabilitar Copiar y sincronizar comparando los siguientes atributos:

- **mtime**: La hora de la última modificación de un archivo. Este atributo no es válido para directorios.
- **uid**, **gid** y **mode**: Indicadores de permisos para Linux.

Copiar para objetos

Habilite esta opción para copiar metadatos y etiquetas de almacenamiento de objetos. Si un usuario cambia los metadatos en la fuente, Copiar y sincronizar copia este objeto en la próxima sincronización, pero si un usuario cambia las etiquetas en la fuente (y no los datos en sí), Copiar y sincronizar no copia el objeto en la próxima sincronización.

No puedes editar esta opción después de crear la relación.

La copia de etiquetas se admite con relaciones de sincronización que incluyen Azure Blob o un punto final compatible con S3 (S3, StorageGRID o IBM Cloud Object Storage) como destino.

La copia de metadatos es compatible con relaciones "de nube a nube" entre cualquiera de los siguientes puntos finales:

- AWS S3
- Blob de Azure
- Almacenamiento en la nube de Google
- Almacenamiento de objetos en la nube de IBM
- StorageGRID

Archivos modificados recientemente

Elija excluir archivos que se modificaron recientemente antes de la sincronización programada.

Eliminar archivos en la fuente

Elija eliminar archivos de la ubicación de origen después de que Copiar y sincronizar copie los archivos a la ubicación de destino. Esta opción incluye el riesgo de pérdida de datos porque los archivos de origen se eliminan después de copiarse.

Si habilita esta opción, también deberá cambiar un parámetro en el archivo local.json en el agente de datos. Abra el archivo y actualícelo de la siguiente manera:

```
{
"workers":{
"transferrer":{
"delete-on-source": true
}
}
}
```

Después de actualizar el archivo local.json, debes reiniciar: `pm2 restart all`.

Eliminar archivos en el destino

Elija eliminar archivos de la ubicación de destino, si se eliminaron de la fuente. El valor predeterminado es nunca eliminar archivos de la ubicación de destino.

Tipos de archivos

Define los tipos de archivos que se incluirán en cada sincronización: archivos, directorios, enlaces simbólicos y enlaces duros.

Los enlaces duros solo están disponibles para relaciones NFS a NFS no seguras. Los usuarios estarán limitados a un proceso de escáner y a una concurrencia de escáneres, y los escaneos deberán ejecutarse desde un directorio raíz.

Excluir extensiones de archivo

Especifique la expresión regular o las extensiones de archivo que desea excluir de la sincronización escribiendo la extensión del archivo y presionando **Enter**. Por ejemplo, escriba *log* o *.log* para excluir archivos *.log. No se requiere un separador para múltiples extensiones. El siguiente vídeo ofrece una breve demostración:

Excluir extensiones de archivo para una relación de sincronización

Las expresiones regulares o regex se diferencian de los comodines o expresiones glob. Esta función **sólo** funciona con expresiones regulares.

Excluir directorios

Especifique un máximo de 15 expresiones regulares o directorios para excluir de la sincronización escribiendo su nombre o la ruta completa del directorio y presionando **Enter**. Los directorios .copy-offload, .snapshot y ~snapshot están excluidos de forma predeterminada.

Las expresiones regulares o regex se diferencian de los comodines o expresiones glob. Esta función **sólo** funciona con expresiones regulares.

Tamaño del archivo

Elija sincronizar todos los archivos independientemente de su tamaño o solo los archivos que estén en un rango de tamaño específico.

Fecha de modificación

Elija todos los archivos independientemente de su última fecha de modificación, archivos modificados después de una fecha específica, antes de una fecha específica o entre un rango de tiempo.

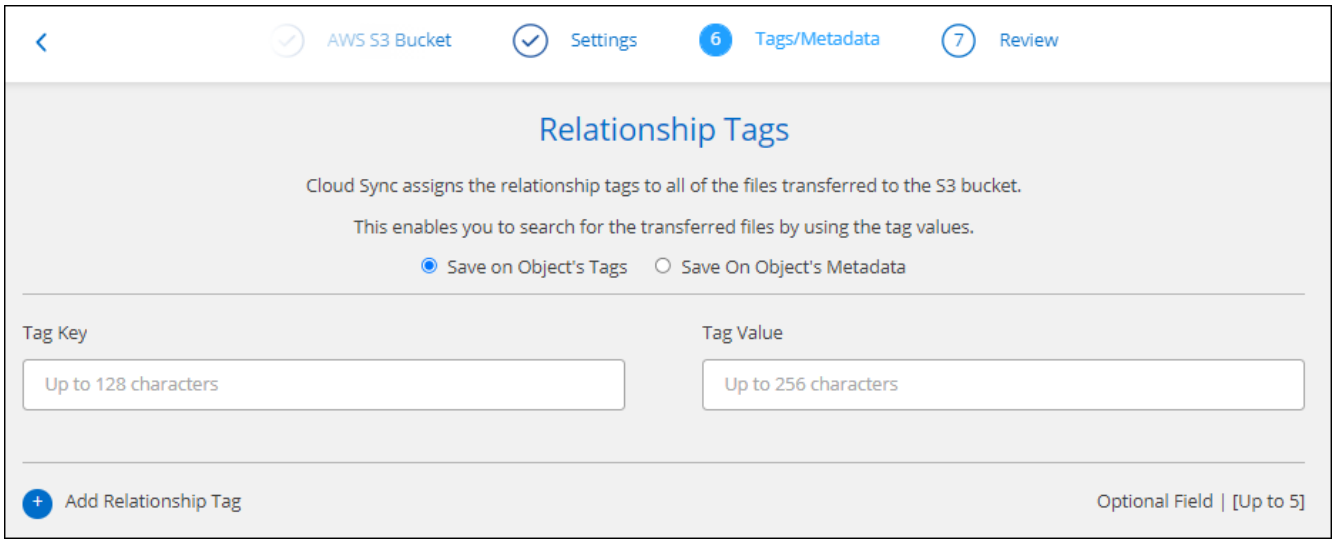
Fecha de creación

Cuando un servidor SMB es la fuente, esta configuración le permite sincronizar archivos que se crearon después de una fecha específica, antes de una fecha específica o entre un rango de tiempo específico.

ACL - Lista de control de acceso

Copie solo ACL, solo archivos o ACL y archivos desde un servidor SMB habilitando una configuración cuando crea una relación o después de crear una relación.

10. En la página **Etiquetas/Metadatos**, elija si desea guardar un par clave-valor como etiqueta en todos los archivos transferidos al bucket S3 o asignar un par clave-valor de metadatos en todos los archivos.



Esta misma función está disponible al sincronizar datos con StorageGRID e IBM Cloud Object Storage. Para Azure y Google Cloud Storage, solo está disponible la opción de metadatos.

11. Revise los detalles de la relación de sincronización y luego seleccione **Crear relación**.

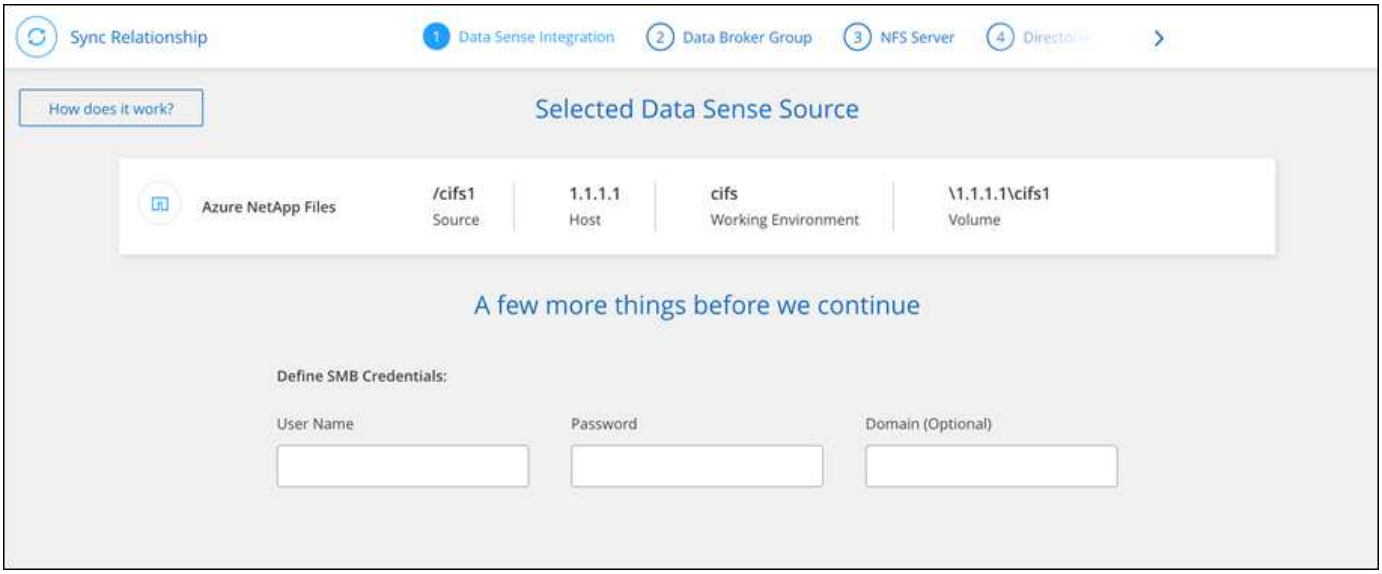
Resultado

Copiar y sincronizar comienza a sincronizar datos entre el origen y el destino. Están disponibles estadísticas de sincronización sobre cuánto tiempo tomó la sincronización, si se detuvo y cuántos archivos se copiaron, escanearon o eliminaron. Luego podrás administrar tu "relaciones de sincronización" , "Gestione sus corredores de datos" , o "Crea informes para optimizar tu rendimiento y configuración" .

Crear relaciones de sincronización desde NetApp Data Classification

Copy and Sync está integrado con NetApp Data Classification. Desde NetApp Data Classification, puede seleccionar los archivos de origen que desea sincronizar con una ubicación de destino mediante Copiar y sincronizar.

Después de iniciar una sincronización de datos desde NetApp Data Classification, toda la información de origen está contenida en un solo paso y solo requiere que ingrese algunos detalles clave. A continuación, elige la ubicación de destino para la nueva relación de sincronización.



"Aprenda a iniciar una relación de sincronización desde NetApp Data Classification" .

Copiar ACL de recursos compartidos SMB en NetApp Copy and Sync

NetApp Copy and Sync puede copiar listas de control de acceso (ACL) entre recursos compartidos SMB y entre un recurso compartido SMB y un almacenamiento de objetos (excepto ONTAP S3). Si es necesario, también tiene la opción de conservar manualmente las ACL entre recursos compartidos SMB mediante robocopy.

Opciones

- Configurar Copiar y sincronizar para copiar ACL automáticamente
- Copiar manualmente las ACL entre recursos compartidos SMB

Configurar Copiar y sincronizar para copiar ACL

Copie las ACL entre recursos compartidos SMB y entre recursos compartidos SMB y almacenamiento de objetos habilitando una configuración cuando crea una relación o después de crear una relación.

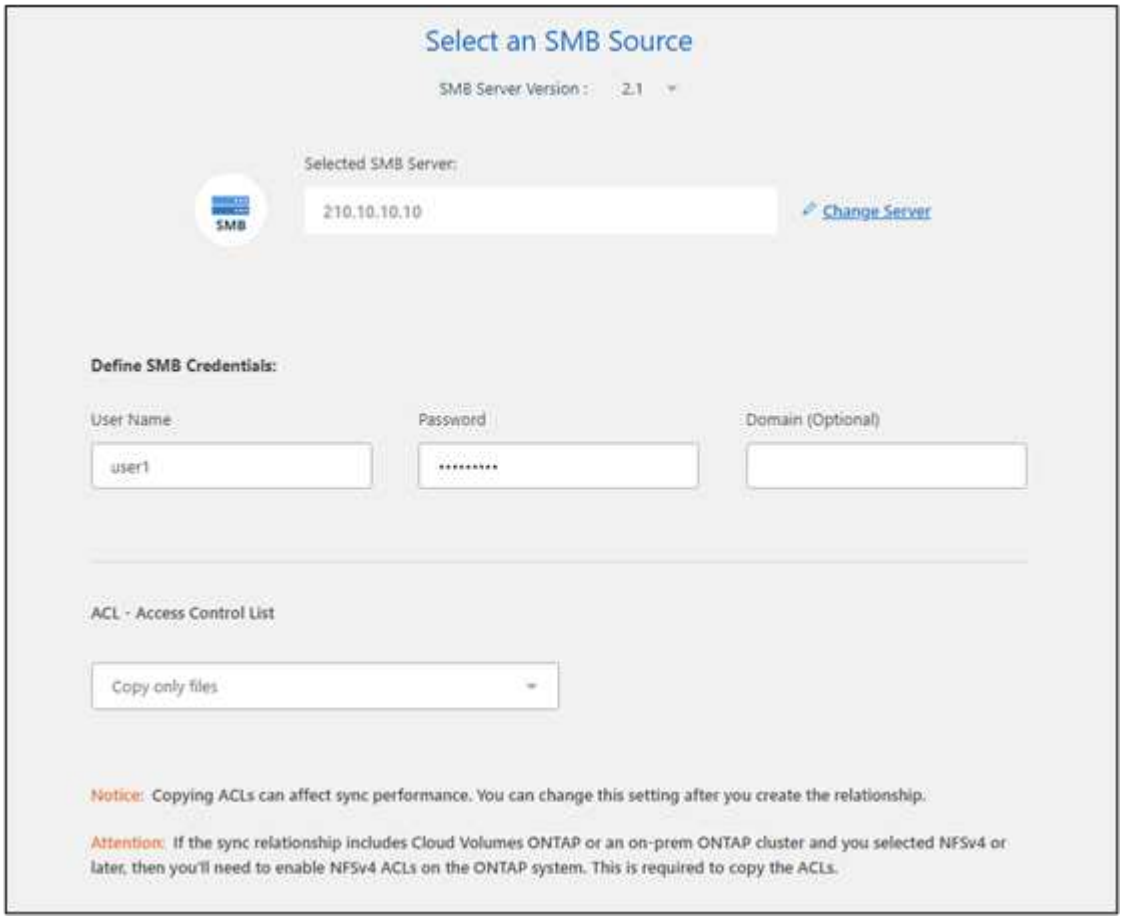
Antes de empezar

Esta función funciona con *cualquier* tipo de agente de datos: AWS, Azure, Google Cloud Platform o agente de datos local. El agente de datos local puede ejecutarse"cualquier sistema operativo compatible" .

Pasos para una nueva relación

1. "Iniciar sesión en Copiar y sincronizar" .
2. Desde Copiar y sincronizar, seleccione **Crear nueva sincronización**.
3. Arrastre y suelte un servidor SMB o un almacenamiento de objetos como origen y un servidor SMB o un almacenamiento de objetos como destino, y seleccione **Continuar**.
4. En la página **Servidor SMB**:
   a. Ingrese un nuevo servidor SMB o seleccione un servidor existente y seleccione **Continuar**.
   b. Introduzca las credenciales para el servidor SMB.

c. Elija entre **Copiar solo archivos**, **Copiar solo ACL** o **Copiar archivos y ACL** y seleccione **Continuar**.



5. Siga las instrucciones restantes para crear la relación de sincronización.

   Al copiar ACL desde SMB al almacenamiento de objetos, puede elegir copiar las ACL en las etiquetas del objeto o en los metadatos del objeto, según el destino. Para Azure y Google Cloud Storage, solo está disponible la opción de metadatos.

   La siguiente captura de pantalla muestra un ejemplo del paso en el que puede realizar esta elección.

Pasos para una relación existente

1. Coloque el cursor sobre la relación de sincronización y seleccione el menú de acciones.
2. Seleccione **Configuración**.
3. Elija entre **Copiar solo archivos**, **Copiar solo ACL** o **Copiar archivos y ACL** y seleccione **Continuar**.
4. Seleccione **Guardar configuración**.

Copiar y sincronizar conserva las ACL (permisos) de SMB, pero no copia la propiedad de archivos o carpetas. La propiedad no está incluida en la operación de transferencia de ACL SMB.

Resultado

Al sincronizar datos, Copiar y sincronizar conserva las ACL entre el origen y el destino.

Copiar manualmente las ACL entre recursos compartidos SMB

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

Si necesita conservar la propiedad (propietario y grupo) además de las ACL, puede utilizar el `robocopy` dominio. Usando el `/copyall` Las copias de bandera incluyen ACL, propiedad e información de auditoría.

Pasos

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

   Debes realizar este paso antes de utilizar robocopy.

3. Desde Copiar y sincronizar, cree una nueva relación entre los recursos compartidos SMB de origen y destino o sincronice una relación existente.
4. Una vez completada 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]
   ```

   Tanto *source* como *target* deben especificarse utilizando el formato UNC. Por ejemplo: \\<servidor>\<recurso compartido>\<ruta>

Sincronice datos NFS mediante el cifrado de datos en tránsito en NetApp Copy and Sync

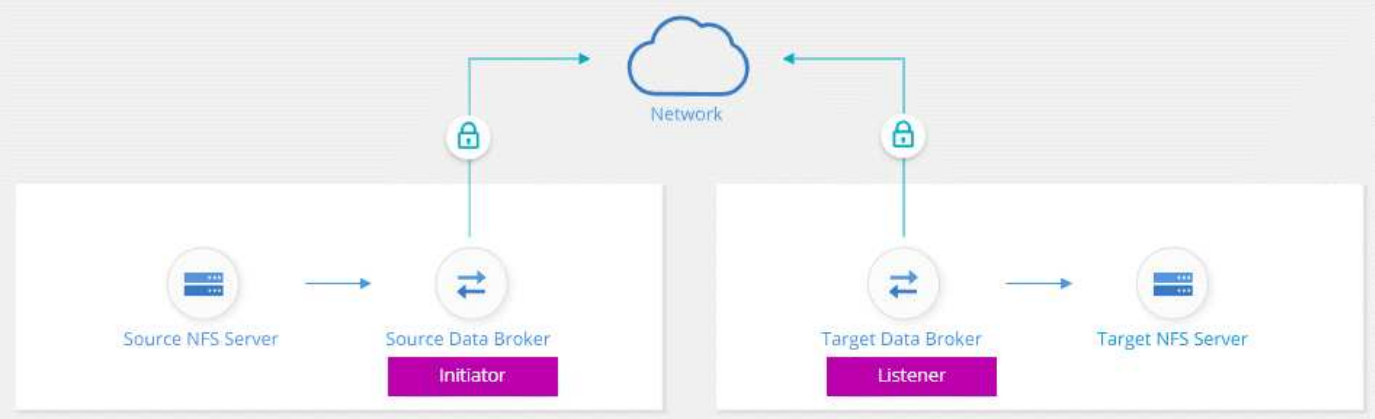
Si su empresa tiene políticas de seguridad estrictas, puede sincronizar datos NFS mediante el cifrado de datos en tránsito en NetApp Copy and Sync. Esta característica es compatible desde un servidor NFS a otro servidor NFS y desde Azure NetApp Files a

Azure NetApp Files.

Por ejemplo, es posible que desee sincronizar datos entre dos servidores NFS que estén en redes diferentes. O tal vez necesite transferir datos de forma segura en Azure NetApp Files entre subredes o regiones.

Cómo funciona el cifrado de datos en tránsito

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



Un agente de datos funciona como *iniciador*. Cuando llega el momento de sincronizar datos, envía una solicitud de conexión al otro agente de datos, que es el *listener*. Ese agente de datos escucha solicitudes en el puerto 443. Puede utilizar un puerto diferente, si es necesario, pero asegúrese de verificar que el puerto no esté siendo utilizado por otro servicio.

Por ejemplo, si sincroniza datos desde un servidor NFS local a un servidor NFS basado en la nube, puede elegir qué agente de datos escucha las solicitudes de conexión y cuál las envía.

Así es como funciona el cifrado en vuelo:

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 de la fuente mediante TLS 1.3.
3. Luego 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, Copiar y sincronizar sincroniza los datos modificados cada 24 horas. Si hay datos para sincronizar, el proceso comienza cuando el iniciador abre una conexión cifrada con el otro agente de datos.

   Si prefiere sincronizar datos con más frecuencia,"Puedes cambiar el horario después de crear la relación" .

Versiones de NFS compatibles

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

Limitación del servidor proxy

Si crea una relación de sincronización cifrada, los datos cifrados se envían a través de HTTPS y no se pueden enrutar a través de un servidor proxy.

Lo que necesitarás para empezar

Asegúrese de tener lo siguiente:

- Dos servidores NFS que se encuentran"Requisitos de origen y destino" o Azure NetApp Files en dos subredes o regiones.
- Las direcciones IP o nombres de dominio completos de los servidores.
- Ubicaciones de red para dos corredores de datos.

  Puede seleccionar un agente de datos existente, pero debe funcionar como iniciador. El agente de datos del oyente debe ser un agente de datos *nuevo*.

  Si desea utilizar un grupo de corredores de datos existente, el grupo debe tener solo un corredor de datos. No se admiten varios corredores de datos en un grupo con relaciones de sincronización cifradas.

  Si aún no ha implementado un agente de datos, revise los requisitos del agente de datos. Debido a que tiene políticas de seguridad estrictas, asegúrese de revisar los requisitos de red, que incluyen el tráfico saliente desde el puerto 443 y el"puntos finales de Internet" que el corredor de datos contacta.

  - "Revisar la instalación de AWS"
  - "Revisar la instalación de Azure"
  - "Revisar la instalación de Google Cloud"
  - "Revisar la instalación del host Linux"

Sincronizar datos NFS mediante 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 tránsito y siga las indicaciones.

Pasos

1. "Iniciar sesión en Copiar y sincronizar" .
2. Seleccione **Crear nueva sincronización**.
3. Arrastre y suelte **Servidor NFS** en las ubicaciones de origen y destino o * Azure NetApp Files* en las ubicaciones de origen y destino y seleccione **Sí** para habilitar el cifrado de datos en tránsito.
4. Siga las instrucciones para crear la relación:

   a. **Servidor NFS**/* Azure NetApp Files*: elija la versión de NFS y luego especifique una nueva fuente de NFS o seleccione un servidor existente.

   b. **Definir la funcionalidad del agente de datos**: define qué agente de datos *escucha* las solicitudes de conexión en un puerto y cuál *inicia* la conexión. Haga su elección en función de sus necesidades de red.

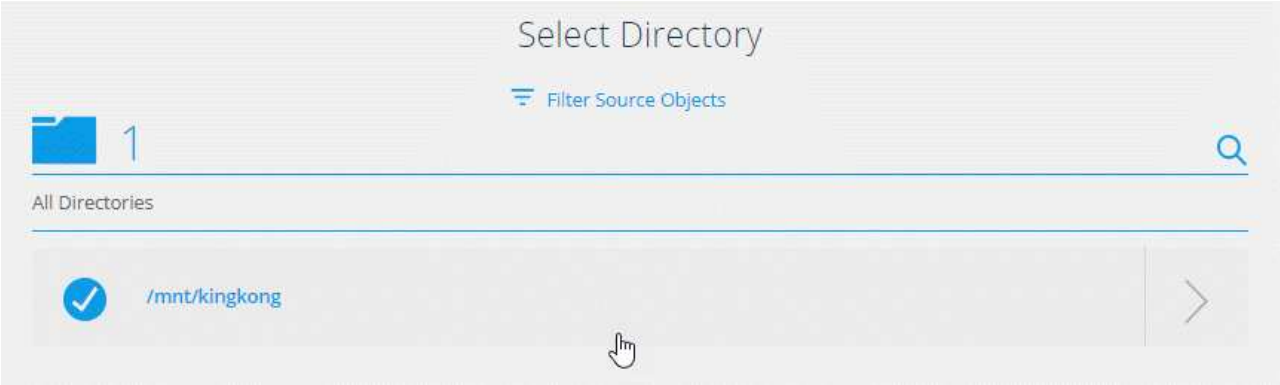
   c. **Agente de datos**: siga las instrucciones para agregar un nuevo agente de datos de origen o seleccionar un agente de datos existente.

      Tenga en cuenta lo siguiente:

- Si desea utilizar un grupo de corredores de datos existente, el grupo debe tener solo un corredor de datos. No se admiten varios corredores de datos en un grupo con relaciones de sincronización cifradas.
- Si el agente de datos de origen actúa como oyente, entonces debe ser un nuevo agente de datos.
- Si necesita un nuevo agente de datos, Copiar y sincronizar le solicitará las instrucciones de instalación. Puede implementar el agente de datos en la nube o descargar un script de instalación para su propio host Linux.

d. **Directorios**: elija los directorios que desea sincronizar seleccionando todos los directorios o explorando y seleccionando un subdirectorio.

   Seleccione **Filtrar objetos de origen** para modificar las configuraciones que definen cómo se sincronizan y mantienen los archivos y carpetas de origen en la ubicación de destino.

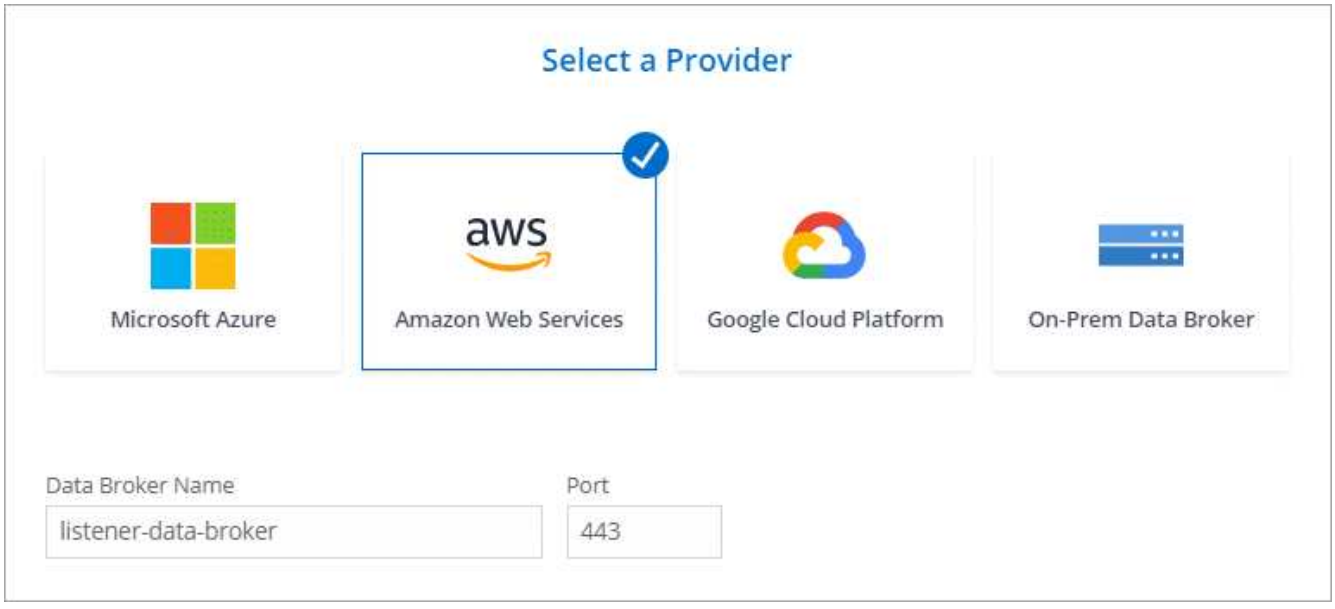


e. **Servidor NFS de destino**/* Azure NetApp Files de destino*: elija la versión de NFS y luego ingrese un nuevo destino NFS o seleccione un servidor existente.

f. **Agente de datos de destino**: siga las instrucciones para agregar un nuevo agente de datos de origen o seleccionar un agente de datos existente.

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

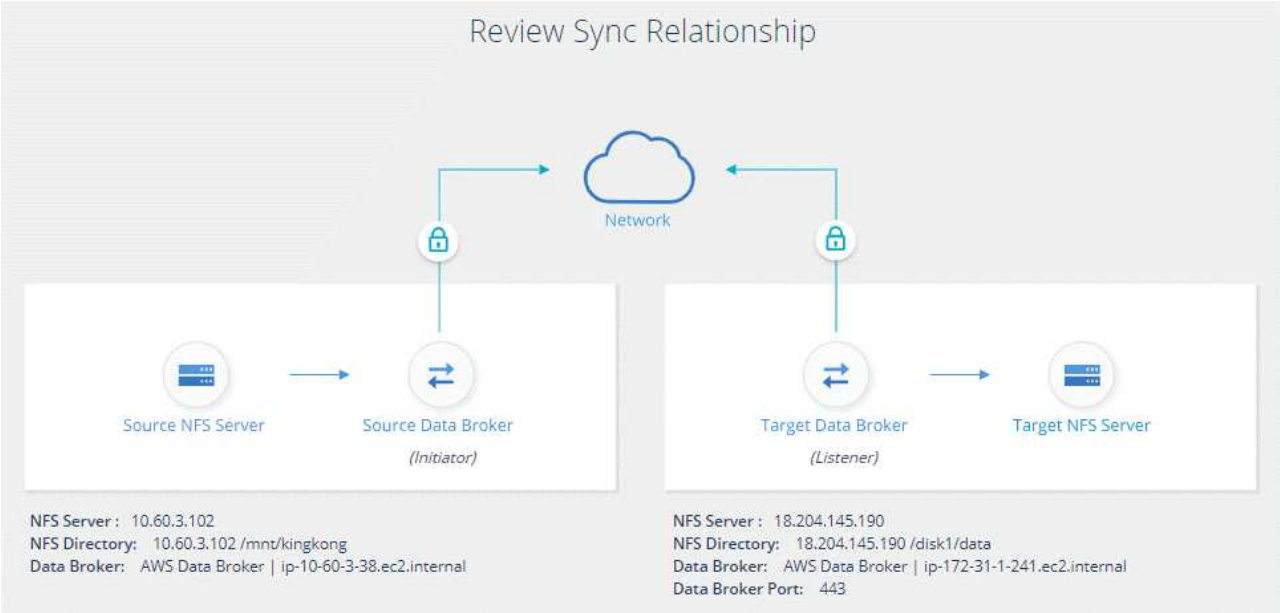
   A continuación se muestra un ejemplo del mensaje que aparece cuando el agente de datos de destino funciona como oyente. Tenga en cuenta la opción para especificar el puerto.



a. **Directorios de destino**: seleccione un directorio de nivel superior o profundice para seleccionar un subdirectorio existente o para crear una nueva carpeta dentro de una exportación.

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

c. **Revisar**: revise los detalles de la relación de sincronización y luego seleccione **Crear relación**.



Resultado

Copiar y sincronizar comienza a crear la nueva relación de sincronización. Cuando haya terminado, seleccione **Ver en el panel** para ver detalles sobre la nueva relación.

Configurar un grupo de intermediarios de datos para utilizar un almacén HashiCorp externo en NetApp Copy and Sync

Cuando crea una relación de sincronización que requiere credenciales de Amazon S3, Azure o Google Cloud, debe especificar esas credenciales a través de la interfaz de usuario o API de NetApp Copy and Sync . Una alternativa es configurar el grupo de intermediarios de datos para acceder a las credenciales (o *secretos*) directamente desde un almacén externo de HashiCorp.

Esta función es compatible con la API de copia y sincronización con relaciones de sincronización que requieren credenciales de Amazon S3, Azure o Google Cloud.

1 Preparar la bóveda

Prepare la bóveda para proporcionar credenciales al grupo de agentes de datos configurando las URL. Las URL de los secretos en la bóveda deben terminar con *Creds*.

2 Preparar el grupo de intermediarios de datos

Prepare el grupo de agentes de datos para obtener credenciales del almacén externo modificando el archivo

de configuración local para cada agente de datos del grupo.

3 Crear una relación de sincronización usando la API

Ahora que todo está configurado, puedes enviar una llamada API para crear una relación de sincronización que use tu bóveda para obtener los secretos.

Preparar la bóveda

Necesitarás proporcionar Copiar y sincronizar con la URL de los secretos en tu bóveda. Prepare la bóveda configurando esas URL. Debe configurar URL para las credenciales para cada origen y destino en las relaciones de sincronización que planea crear.

La URL debe configurarse de la siguiente manera:

```
/<path>/<requestid>/<endpoint-protocol>Creds
```

Camino

La ruta del prefijo al secreto. Este puede ser cualquier valor que sea exclusivo para usted.

ID de solicitud

Un ID de solicitud que necesita generar. Necesitará proporcionar la ID en uno de los encabezados de la solicitud POST de API cuando cree la relación de sincronización.

Protocolo de punto final

Uno de los siguientes protocolos, según se define "En la documentación de la relación posterior v2" :S3, AZURE o GCP (cada uno debe estar en mayúsculas).

Creds

La URL debe terminar con *Creds*.

Ejemplos

Los siguientes ejemplos muestran URL a secretos.

Ejemplo de URL completa y ruta para las credenciales de origen

\ http://example.vault.com:8200/my-path/all-secrets/hb312vdasr2/S3Creds

Como puede ver en el ejemplo, la ruta del prefijo es */my-path/all-secrets/*, el ID de solicitud es *hb312vdasr2* y el punto final de origen es S3.

Ejemplo de URL completa y ruta para credenciales de destino

\ http://example.vault.com:8200/my-path/all-secrets/n32hcbnejk2/AZURECreds

La ruta del prefijo es */my-path/all-secrets/*, el ID de solicitud es *n32hcbnejk2* y el punto final de destino es Azure.

Preparar el grupo de intermediarios de datos

Prepare el grupo de agentes de datos para obtener credenciales del almacén externo modificando el archivo de configuración local para cada agente de datos del grupo.

Pasos

1. SSH a un agente de datos del grupo.
2. Edite el archivo local.json que reside en /opt/netapp/databroker/config.
3. Establezca habilitar en **verdadero** y configure los campos de parámetros de configuración en *external-integrations.hashicorp* de la siguiente manera:

   activado
   - Valores válidos: verdadero/falso
   - Tipo: Booleano
   - Valor predeterminado: falso
   - Verdadero: El corredor de datos obtiene secretos de su propia bóveda externa de HashiCorp
   - Falso: El agente de datos almacena las credenciales en su bóveda local

   URL
   - Tipo: cadena
   - Valor: La URL de su bóveda externa

   camino
   - Tipo: cadena
   - Valor: Prefijo de ruta al secreto con sus credenciales

   Rechazar no autorizado
   - Determina si desea que el agente de datos rechace el almacén externo no autorizado
   - Tipo: Booleano
   - Predeterminado: falso

   método de autenticación
   - El método de autenticación que debe utilizar el agente de datos para acceder a las credenciales de la bóveda externa
   - Tipo: cadena
   - Valores válidos: “aws-iam” / “role-app” / "gcp-iam"

   nombre del rol
   - Tipo: cadena
   - Su nombre de rol (en caso de que utilice aws-iam o gcp-iam)

   Secretid y rootid
   - Tipo: cadena (en caso de que utilice app-role)

   Espacio de nombres
   - Tipo: cadena
   - Su espacio de nombres (encabezado X-Vault-Namespace si es necesario)

4. Repita estos pasos para cualquier otro agente de datos del grupo.

Ejemplo de autenticación de roles de AWS

```
{
          “external-integrations”: {
                  “hashicorp”: {
                          “enabled”: true,
                          “url”: “https://example.vault.com:8200”,
                          “path”: ““my-path/all-secrets”,
                          “reject-unauthorized”: false,
                          “auth-method”: “aws-role”,
                          “aws-role”: {
                                “role-name”: “my-role”
                          }
                  }
        }
}
```

Ejemplo de autenticación gcp-iam

```
{
"external-integrations": {
    "hashicorp": {
      "enabled": true,
      "url": http://ip-10-20-30-55.ec2.internal:8200,
      "path": "v1/secret",
      "namespace": "",
      "reject-unauthorized": true,
      "auth-method": "gcp-iam",
      "aws-iam": {
        "role-name": ""
      },
      "app-role": {
        "root_id": "",
        "secret_id": ""
      },
"gcp-iam": {
          "role-name": "my-iam-role"
      }
    }
  }
}
```

Configurar permisos al usar la autenticación gcp-iam

Si utiliza el método de autenticación *gcp-iam*, el agente de datos debe tener el siguiente permiso de GCP:

```
- iam.serviceAccounts.signJwt
```

"Obtenga más información sobre los requisitos de permisos de GCP para el agente de datos" .

Creación de una nueva relación de sincronización utilizando secretos del almacén

Ahora que todo está configurado, puedes enviar una llamada API para crear una relación de sincronización que use tu bóveda para obtener los secretos.

Publique la relación utilizando la API REST Copiar y sincronizar.

```
Headers:
Authorization: Bearer <user-token>
Content-Type: application/json
x-account-id: <accountid>
x-netapp-external-request-id-src: request ID as part of path for source
credentials
x-netapp-external-request-id-trg: request ID as part of path for target
credentials
Body: post relationship v2 body
```

- Para obtener un token de usuario y el ID de su cuenta de NetApp Console ,"Consulte esta página en la documentación" .
- Para construir un cuerpo para tu relación posterior, "Consulte la llamada API de relaciones-v2" .

Ejemplo

Ejemplo para la solicitud POST:

```
url: https://api.cloudsync.netapp.com/api/relationships-v2
headers:
"x-account-id": "CS-SasdW"
"x-netapp-external-request-id-src": "hb312vdasr2"
"Content-Type": "application/json"
"Authorization": "Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik…"
Body:
{
"dataBrokerId": "5e6e111d578dtyuu1555sa60",
"source": {
        "protocol": "s3",
        "s3": {
                "provider": "sgws",
                "host": "1.1.1.1",
                "port": "443",
                "bucket": "my-source"
     },
"target": {
        "protocol": "s3",
        "s3": {
                "bucket": "my-target-bucket"
        }
    }
}
```

Información de copyright

Información de la marca comercial