Sincronice datos entre un origen y un destino

BlueXP copy and sync

NetApp
April 08, 2024

Tabla de contenidos

Sincronice datos entre un origen y un destino

Creación de relaciones de sincronización

Cuando creas una relación de sincronización, el servicio de copia y sincronización de BlueXP copia los archivos del origen en el destino. Después de la copia inicial, el servicio sincroniza los datos modificados cada 24 horas.

Antes de crear algunos tipos de relaciones de sincronización, primero tendrá que crear un entorno de trabajo en BlueXP.

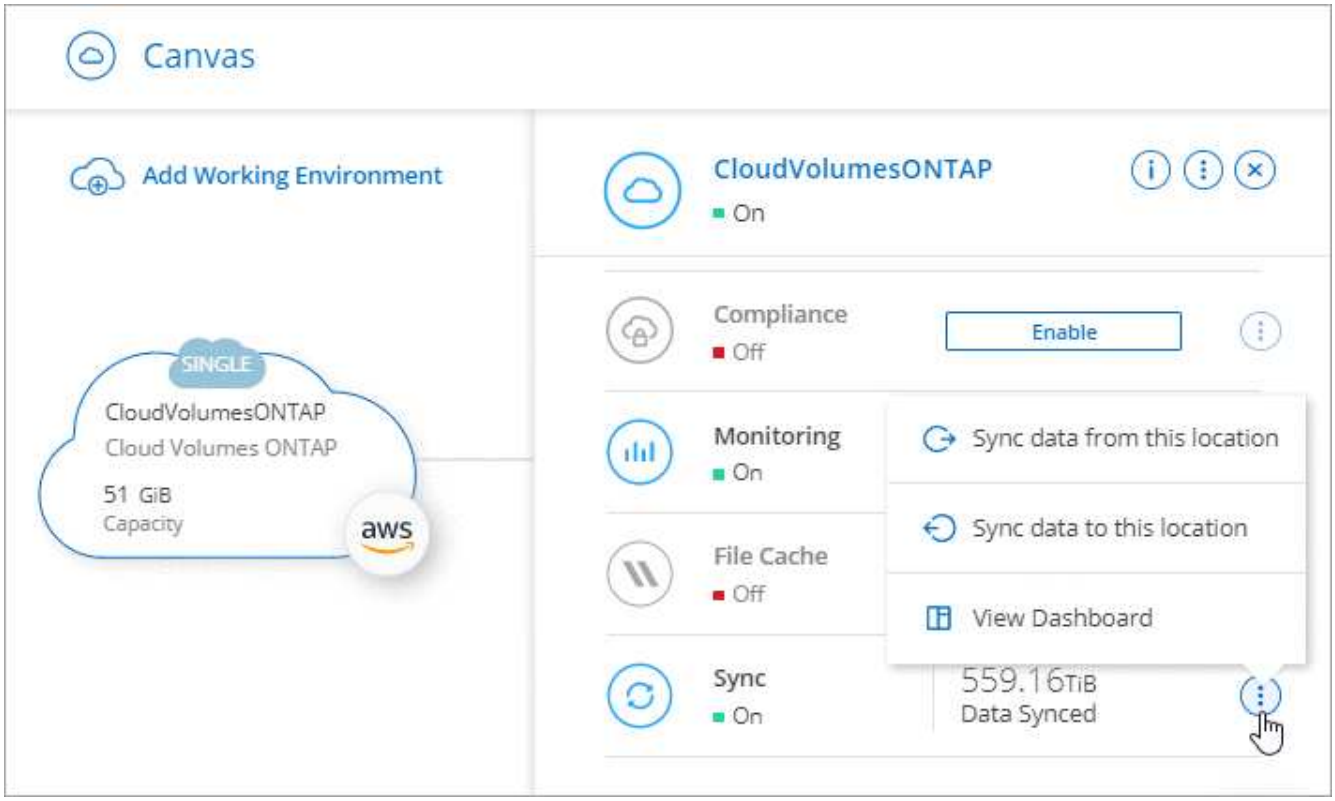
Crear relaciones de sincronización para tipos específicos de entornos de trabajo

Si desea crear relaciones de sincronización para cualquiera de las siguientes, primero debe crear o detectar el entorno de trabajo:

- Amazon FSX para ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Clústeres de ONTAP en las instalaciones

Pasos

1. Crear o detectar el entorno de trabajo.
    - "Cree un entorno de trabajo de Amazon FSX para ONTAP"
    - "Configuración y detección de Azure NetApp Files"
    - "Inicio de Cloud Volumes ONTAP en AWS"
    - "Inicio de Cloud Volumes ONTAP en Azure"
    - "Lanzamiento de Cloud Volumes ONTAP en Google Cloud"
    - "Añadiendo sistemas Cloud Volumes ONTAP existentes"
    - "Detección de clústeres de ONTAP"
2. Selecciona **Canvas**.
3. Seleccione un entorno de trabajo que coincida con cualquiera de los tipos indicados anteriormente.
4. Seleccione el menú de acción situado junto a Sincronizar.



5. Seleccione **Sincronizar datos de esta ubicación** o **Sincronizar datos a esta ubicación** y siga las indicaciones para configurar la relación de sincronización.

Cree otros tipos de relaciones de sincronización

Siga estos pasos para sincronizar datos en un tipo de almacenamiento compatible distinto de Amazon FSX para clústeres de ONTAP, Azure NetApp Files, Cloud Volumes ONTAP o ONTAP en las instalaciones. Los siguientes pasos proporcionan un ejemplo que muestra cómo configurar una relación de sincronización desde un servidor NFS a un bloque de S3.

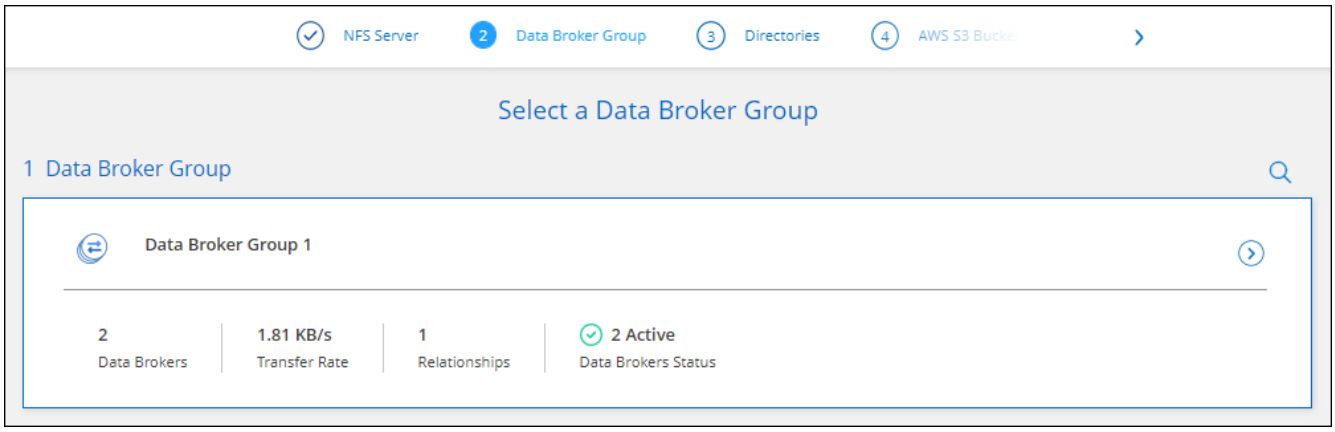
1. En BlueXP, selecciona **Sync**.
2. En la página **definir relación de sincronización**, elija un origen y un destino.

   En los siguientes pasos se proporciona un ejemplo de cómo crear una relación de sincronización desde un servidor NFS hasta un bloque de S3.

3. En la página **servidor NFS**, introduzca la dirección IP o el nombre de dominio completo del servidor NFS que desea sincronizar con AWS.
4. En la página **Data Broker Group**, siga las indicaciones para crear una máquina virtual de Data Broker en AWS, Azure o Google Cloud Platform, o para instalar el software de Data Broker en un host Linux existente.

   Para obtener más información, consulte las siguientes páginas:

   - "Crear un agente de datos en AWS"
   - "Cree un agente de datos en Azure"
   - "Crear un agente de datos en Google Cloud"
   - "Instalar el agente de datos en un host Linux"
5. Después de instalar el broker de datos, seleccione **Continuar**.

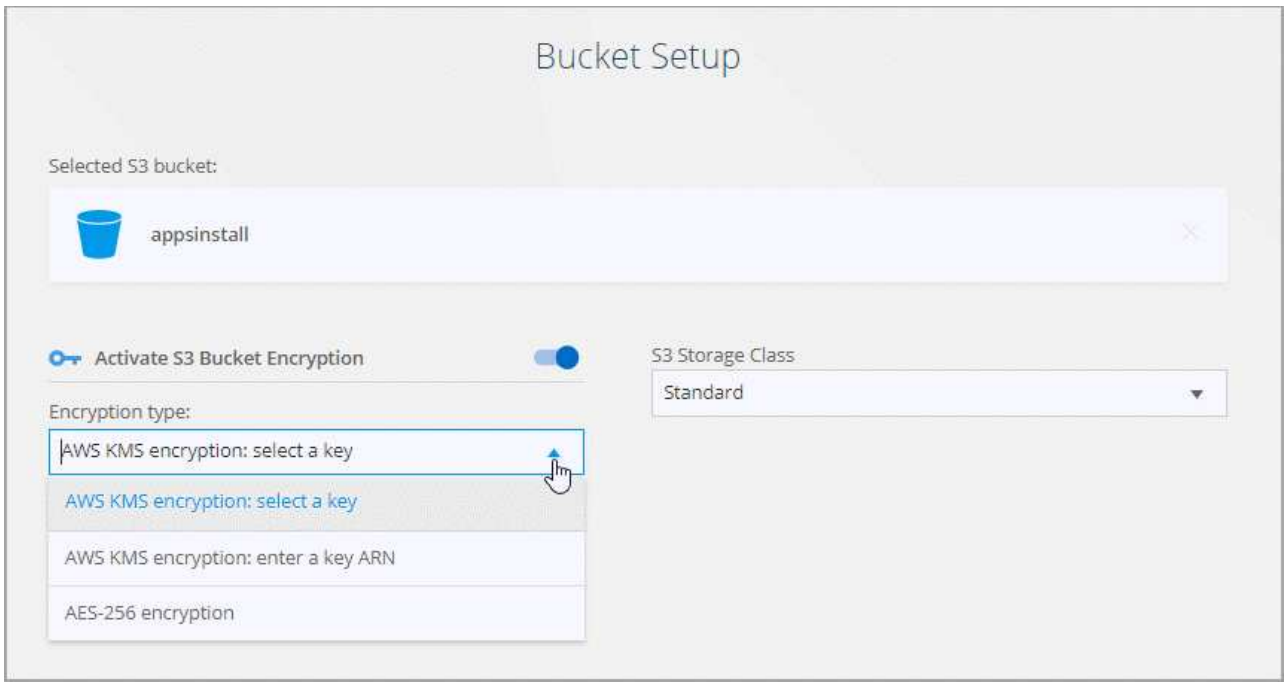


6. en la página **directorios**, seleccione un directorio o subdirectorio de nivel superior.

   Si la copia y sincronización de BlueXP no pueden recuperar las exportaciones, selecciona **Agregar exportación manualmente** e introduce el nombre de una exportación NFS.

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

7. En la página **AWS S3 Bucket**, seleccione un bloque:
   - Examine para seleccionar una carpeta existente dentro del bloque o para seleccionar una carpeta nueva que cree dentro del bloque.
   - Seleccione **Agregar a la lista** para seleccionar un bucket de S3 que no esté asociado a su cuenta de AWS. "Los permisos específicos se deben aplicar al bloque de S3".
8. En la página **Configuración de bloque**, configure el cucharón:
   - Elija si desea habilitar el cifrado de bloque de S3 y, a continuación, seleccione una clave de AWS KMS, introduzca el ARN de una clave de KMS o seleccione el cifrado AES-256.
   - Seleccione una clase de almacenamiento S3. "Consulte las clases de almacenamiento compatibles".



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

Programación

Elija una programación recurrente para sincronizar en el futuro o desactive la programación de sincronización. Puede programar una relación para que se sincronice datos con una frecuencia de hasta cada 1 minuto.

Tiempo de espera de sincronización

Define si la copia y sincronización de BlueXP debe cancelar una sincronización de datos si la sincronización no se ha completado en el número especificado de minutos, horas o días.

Notificaciones

Te permite elegir si deseas recibir notificaciones de copia y sincronización de BlueXP en el centro de notificaciones de BlueXP. Es posible habilitar notificaciones para que la sincronización de los datos se haya realizado correctamente, que no se hayan podido sincronizar los datos y que se haya cancelado.

Reintentos

Define la cantidad de veces que la copia y sincronización de BlueXP deben volver a intentar sincronizar un archivo antes de omitirlo.

Sincronización continua

Tras la sincronización de datos inicial, la copia y sincronización de BlueXP escucha los cambios en el bloque de S3 de origen o en el bloque de Google Cloud Storage y sincroniza continuamente los cambios en el destino a medida que se producen. No es necesario volver a analizar el origen a intervalos programados.

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

Si activa esta configuración, afecta a otras funciones de la siguiente manera:

- Se deshabilitó la programación de sincronización.
- Los siguientes valores se revierten a sus valores predeterminados: Tiempo de espera de sincronización, Archivos modificados recientemente y Fecha de modificación.
- Si S3 es el origen, el filtro por tamaño solo estará activo en eventos de copia (no al eliminar eventos).
- Una vez creada la relación, solo se puede acelerar o eliminar. No puede cancelar la sincronización, modificar la configuración ni ver informes.

  Se puede crear una relación de sincronización continua con un bloque externo. Para hacerlo, siga estos pasos:

  i. Ve a la consola de Google Cloud para ver el proyecto del bucket 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. Reinicie el agente de datos:

   A. sudo pm2 pare todo

   B. sudo pm2 inicie todo

v. Cree una relación de sincronización continua con el bloque 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 la copia y sincronización de BlueXP deben comparar ciertos atributos al determinar si un archivo o directorio ha cambiado y debería volver a sincronizarse.

Incluso si desmarca estos atributos, la copia y sincronización de BlueXP sigue comparando el origen con el destino comprobando las rutas, los tamaños de los archivos y los nombres de los archivos. Si hay cambios, sincroniza esos archivos y directorios.

Puedes elegir habilitar o deshabilitar la copia y sincronización de BlueXP entre la comparación de los siguientes atributos:

- **Mtime**: La última hora de 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 etiquetas y metadatos de almacenamiento de objetos. Si un usuario cambia los metadatos en el origen, BlueXP copia y sincronización este objeto en la siguiente sincronización, pero si un usuario cambia las etiquetas del origen (y no los datos en sí), la copia y sincronización de BlueXP no copiará el objeto en la siguiente sincronización.

No se puede editar esta opción después de crear la relación.

Se admiten las relaciones de copia de etiquetas, entre las que se incluyen Azure Blob o un extremo compatible con S3 (S3, StorageGRID o IBM Cloud Object Storage) como destino.

Es compatible con las relaciones de "cloud a cloud" entre cualquiera de los siguientes extremos:

- AWS S3
- Azure Blob
- Google Cloud Storage

- Almacenamiento de objetos en cloud de IBM
- StorageGRID

Archivos modificados recientemente

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

Eliminar archivos en el origen

Elija eliminar los archivos de la ubicación de origen después de que BlueXP copie y sincronice los archivos en la ubicación de destino. Esta opción incluye el riesgo de pérdida de datos porque los archivos de origen se eliminan una vez copiados.

Si habilita esta opción, también debe cambiar un parámetro en el archivo local.json del agente de datos. Abra el archivo y actualícelo del siguiente modo:

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

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

Eliminar archivos en destino

Elija eliminar archivos de la ubicación de destino, si se eliminaron del origen. El valor predeterminado es no eliminar nunca los archivos de la ubicación de destino.

Tipos de archivo

Defina los tipos de archivo que se incluirán en cada sincronización: Archivos, directorios, enlaces simbólicos y enlaces físicos.

> Los enlaces físicos solo están disponibles para relaciones NFS no seguras con NFS. Los usuarios estarán limitados a un proceso de escáner y a una simultaneidad de escáner, y las exploraciones deben ejecutarse desde un directorio raíz.

Excluir extensiones de archivo

Especifique el regex o las extensiones de archivo que desea excluir de la sincronización escribiendo la extensión de archivo y pulsando **Intro**. Por ejemplo, escriba *log* o *.log* para excluir archivos *.log. No es necesario un separador para varias extensiones. El siguiente vídeo proporciona una breve demostración:

► https://docs.netapp.com/es-es/bluexp-copy-sync//media/video_file_extensions.mp4 *(video)*

> Regex, o expresiones regulares, difieren de comodines o expresiones glob. Esta función **Only** funciona con regex.

Excluir directorios

Especifique un máximo de 15 regex o directorios para excluir de la sincronización escribiendo su nombre o directorio de ruta completa y pulsando **Intro**. Los directorios .copy-fload, .snapshot, ~snapshot se excluyen de forma predeterminada.

> Regex, o expresiones regulares, difieren de comodines o expresiones glob. Esta función **Only** funciona con regex.

Tamaño de archivo

Elija sincronizar todos los archivos independientemente de su tamaño o sólo los archivos que se encuentren en un rango de tamaño específico.

Fecha de modificación

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

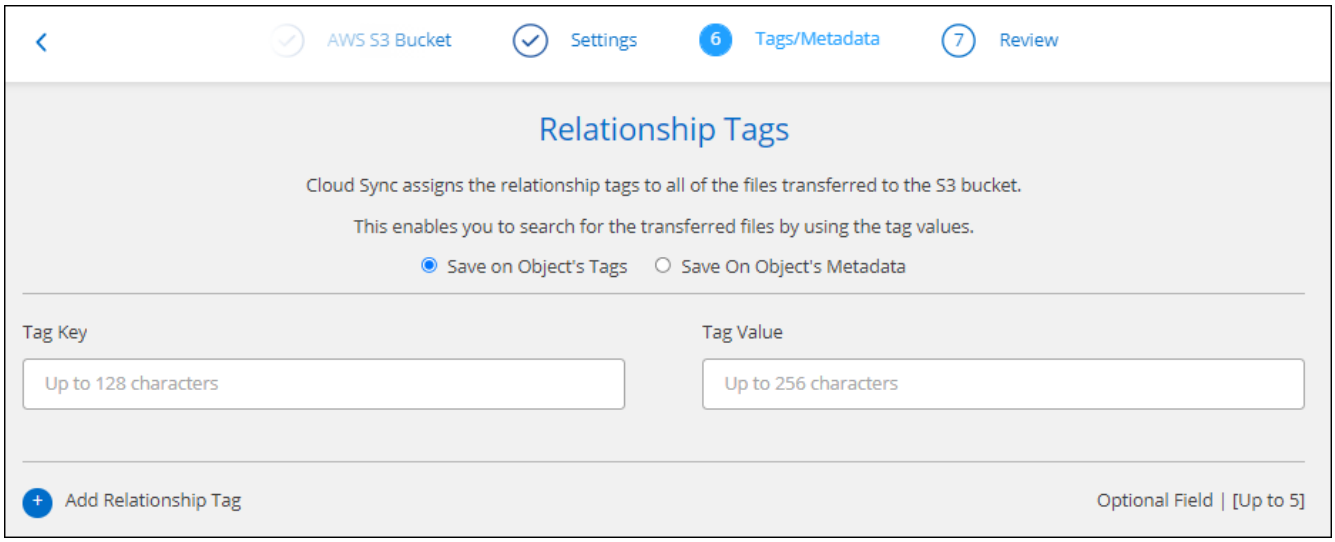
Fecha de creación

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

ACL - Lista de control de acceso

Copie sólo ACL, archivos o ACL y archivos de un servidor SMB mediante la activación de una configuración al crear una relación o después de crear una relación.

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



> Esta misma función está disponible cuando se sincroniza datos con StorageGRID o el almacenamiento de objetos en el cloud de IBM. Para Azure y Google Cloud Storage, solo está disponible la opción de metadatos.

11. Revisa los detalles de la relación de sincronización y luego selecciona **Crear relación**.

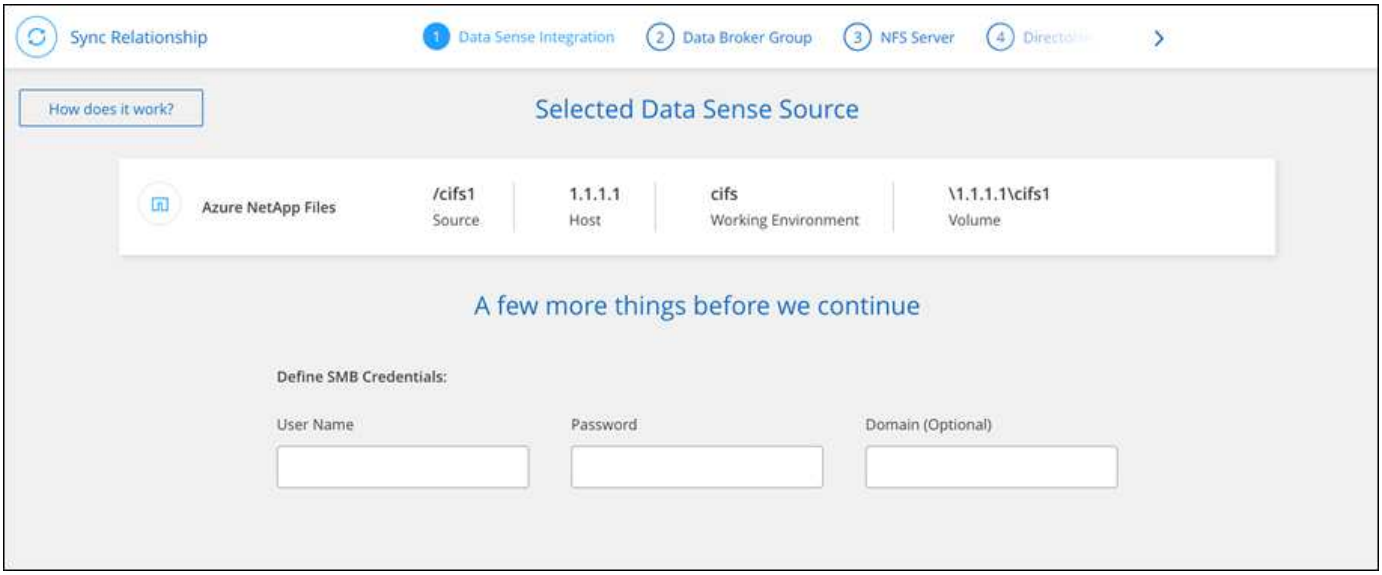
resultado

La copia y la sincronización de BlueXP comienzan a sincronizar datos entre el origen y el destino.

Crea relaciones de sincronización a partir de la clasificación de BlueXP

La copia y sincronización de BlueXP están integradas con la clasificación de BlueXP. Desde dentro de la clasificación de BlueXP, puedes seleccionar los archivos de origen que deseas sincronizar con una ubicación de destino mediante la copia y sincronización de BlueXP.

Tras iniciar una sincronización de datos de la clasificación de BlueXP, toda la información de fuente se contiene en un solo paso y solo requiere que introduzca algunos detalles clave. A continuación, elija la ubicación de destino para la nueva relación de sincronización.



"Descubre cómo iniciar una relación de sincronización desde la clasificación de BlueXP".

Copiar ACL de recursos compartidos de SMB

La copia y sincronización de BlueXP puede copiar listas de control de acceso (ACL) entre recursos compartidos de SMB y entre un recurso compartido de SMB y el almacenamiento de objetos (excepto para ONTAP S3). Si es necesario, también se dispone de la opción de conservar manualmente las ACL entre las unidades SMB mediante robocopy.

Opciones

- Configura la copia y sincronización de BlueXP para copiar automáticamente las ACL
- Copiar manualmente las ACL entre los recursos compartidos de SMB

Configura la copia y sincronización de BlueXP para copiar listas de control de acceso

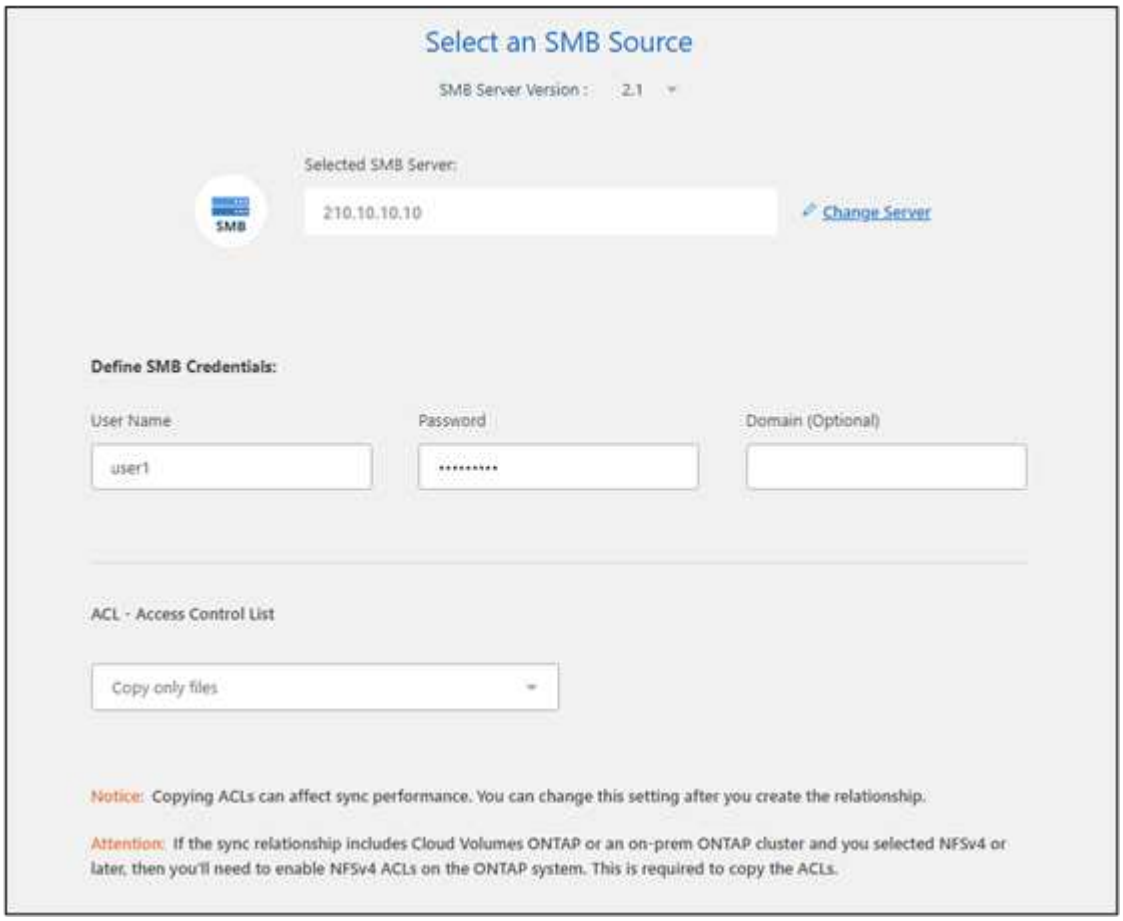
Copiar ACL entre recursos compartidos de SMB y entre recursos compartidos de SMB y el almacenamiento de objetos. Para ello, se habilita una configuración cuando se crea una relación o después de crear una relación.

Antes de empezar

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

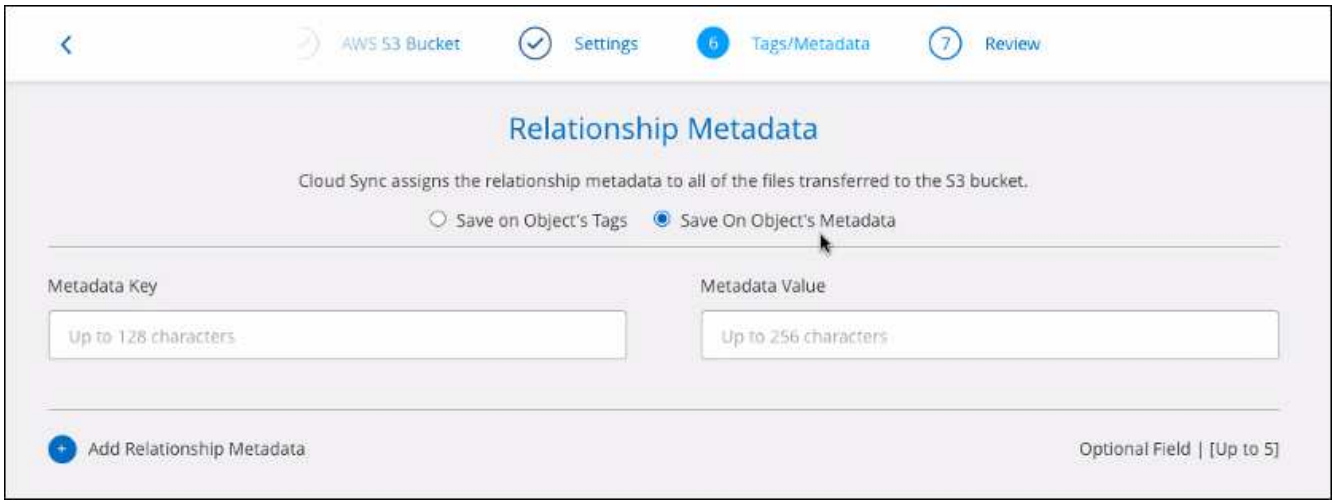
1. Desde la copia y sincronización de BlueXP, selecciona **Crear nueva sincronización**.
2. Arrastre y suelte un servidor SMB o almacenamiento de objetos como origen y un servidor SMB o almacenamiento de objetos como destino, y seleccione **Continuar**.
3. En la página **SMB Server**:
   a. Ingrese un nuevo servidor SMB o seleccione un servidor existente y seleccione **Continuar**.
   b. Introduzca credenciales para el servidor SMB.
   c. Elija * Copiar solo archivos *, * Copiar solo ACL * o * Copiar archivos y ACL * y seleccione * Continuar *.



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

   Cuando se copian ACL de SMB para el almacenamiento de objetos, se puede optar por 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 elegir esta opción.



Pasos para una relación existente

1. Pase el ratón sobre la relación de sincronización y seleccione el menú de acción.
2. Selecciona **Ajustes**.
3. Elija * Copiar solo archivos *, * Copiar solo ACL * o * Copiar archivos y ACL * y seleccione * Continuar *.
4. Selecciona **Guardar configuración**.

Resultado

Al sincronizar los datos, la copia y sincronización de BlueXP conserva las listas de control de acceso entre el origen y el destino.

Copie manualmente las ACL entre recursos compartidos de SMB

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. Desde la copia y sincronización de BlueXP, cree una nueva relación entre los recursos compartidos de SMB de origen y 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>

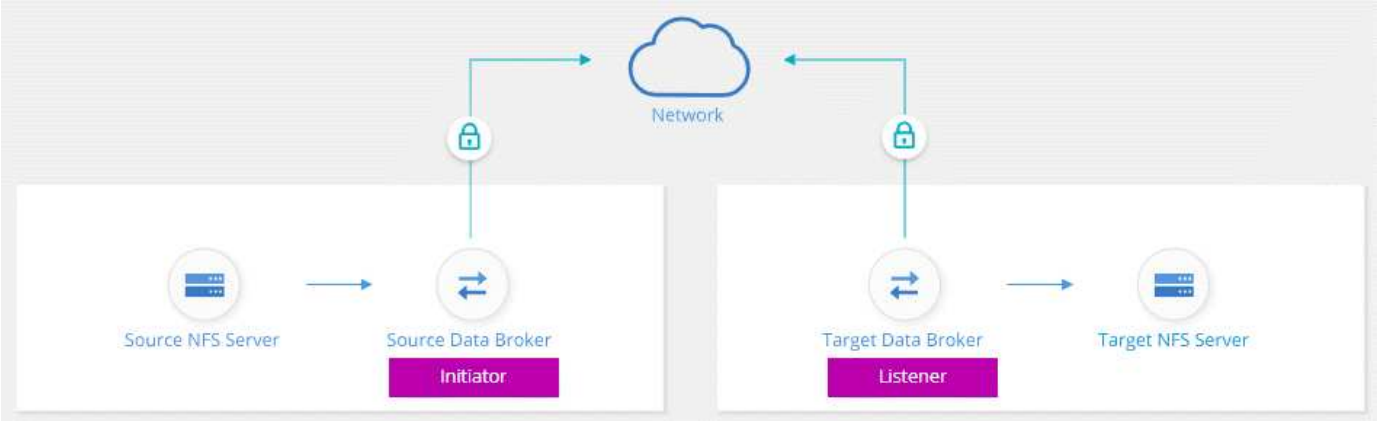
Sincronizando los datos NFS mediante el cifrado de datos en tránsito

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.

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 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 desea utilizar un grupo de Data broker existente, el grupo debe tener sólo un agente de datos. No se admiten varios gestores de datos en un grupo con relaciones de sincronización cifradas.

  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 Google Cloud"
  - "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. Selecciona **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.
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.

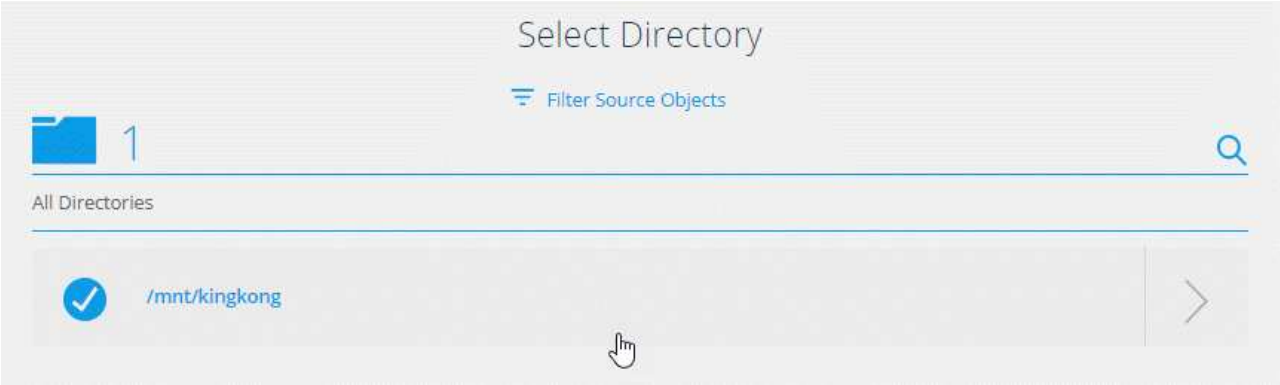
c. **Data Broker**: Siga las indicaciones para agregar un nuevo intermediario de datos de origen o seleccionar un intermediario de datos existente.

   Tenga en cuenta lo siguiente:

   - Si desea utilizar un grupo de Data broker existente, el grupo debe tener sólo un agente de datos. No se admiten varios gestores de datos en un grupo con relaciones de sincronización cifradas.
   - Si el agente de datos de origen actúa como oyente, debe ser un nuevo agente de datos.
   - Si necesitas un nuevo agente de datos, la copia y sincronización de BlueXP te indica 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.

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

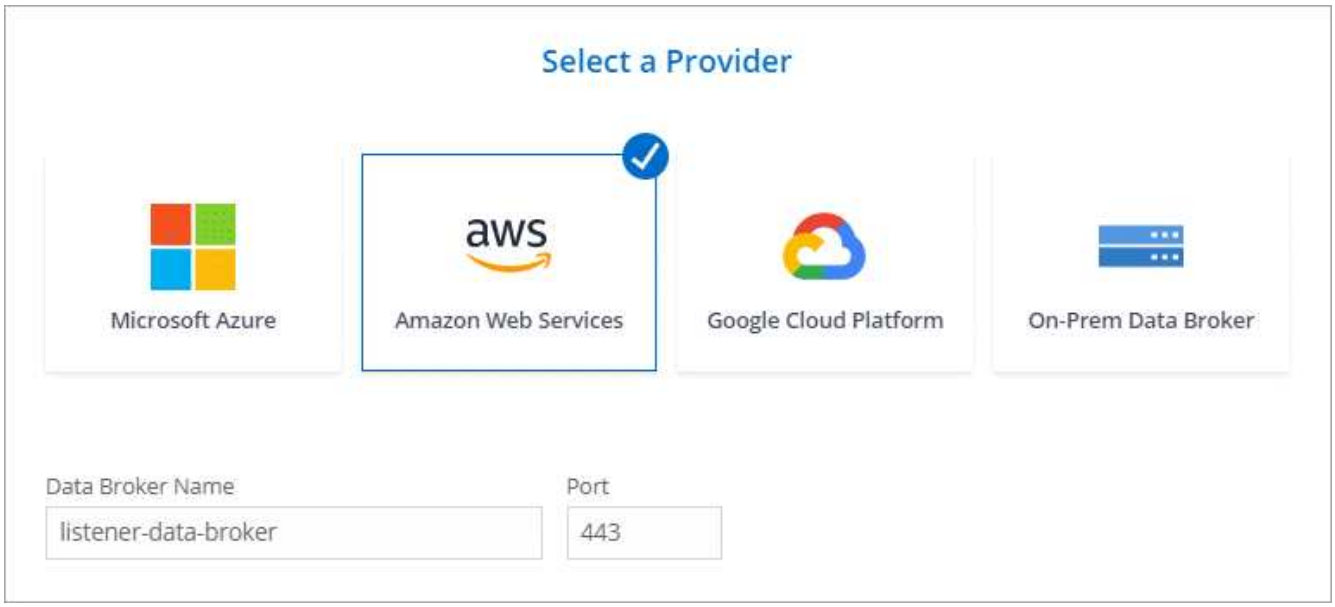


e. **servidor NFS de destino/Azure NetApp Files de destino**: Elija la versión NFS y, a continuación, introduzca un destino NFS nuevo o seleccione un servidor existente.

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.

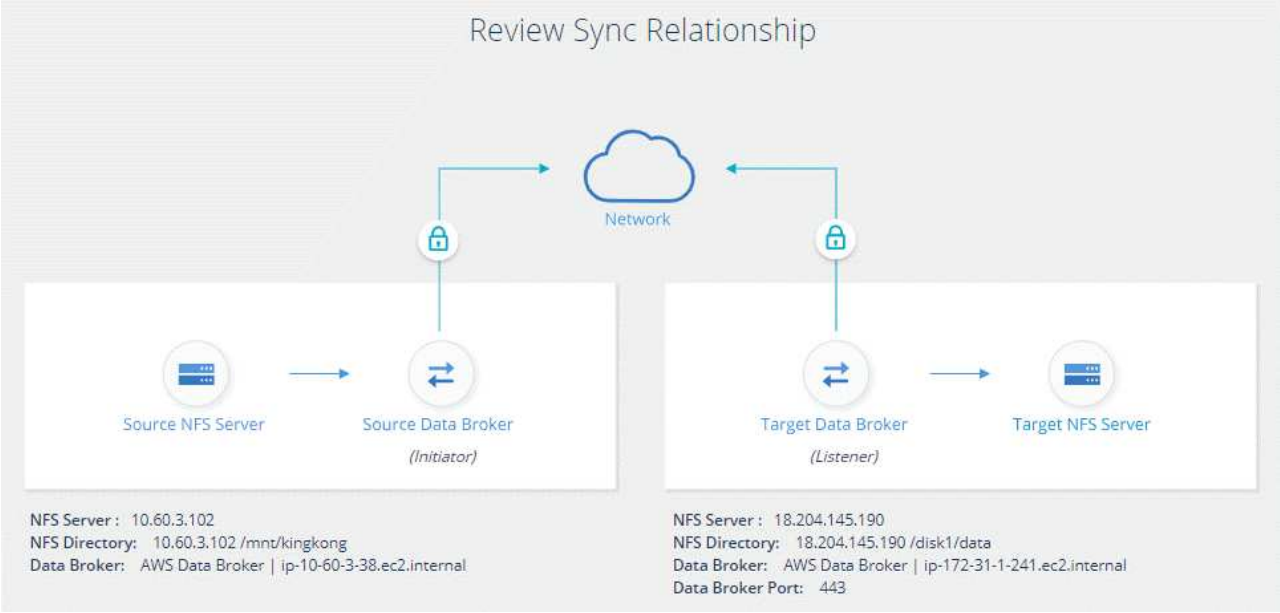
   A continuación se muestra un ejemplo del mensaje en el que el agente de datos de destino funciona como el listener. Observe la opción para especificar el puerto.



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**: Revisa los detalles de la relación de sincronización y luego selecciona **Crear relación**.



Resultado

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

Configuración de un grupo de corredores de datos para usar un almacén externo de HashiCorp

Cuando creas una relación de sincronización que requiera credenciales de Amazon S3,

Azure o Google Cloud, tienes que especificar esas credenciales a través de la interfaz de usuario o la API de copia y sincronización de BlueXP. Una alternativa es establecer el grupo de corredores de datos para acceder a las credenciales (o *Secrets*) directamente desde un almacén externo de HashiCorp.

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

1. **Prepare el almacén**

Prepare el almacén para proporcionar credenciales al grupo de Data broker configurando las direcciones URL. Las direcciones URL de los secretos del almacén deben terminar con *creds*.

2. **Preparar el grupo de Data broker**

Prepare el grupo de Data broker para recuperar credenciales del almacén externo modificando el archivo de configuración local de cada agente de datos del grupo.

3. **Cree una relación de sincronización con la API de**

Ahora que todo está configurado, puede enviar una llamada a la API para crear una relación de sincronización que utilice su almacén para obtener los secretos.

Preparación del almacén

Tendrás que proporcionar copia y sincronización de BlueXP con la URL de los secretos de tu almacén. Prepare el almacén configurando esas URL. Debe configurar URL para las credenciales de cada origen y destino en las relaciones de sincronización que desea crear.

La dirección URL debe configurarse de la siguiente manera:

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

Ruta

La ruta del prefijo al secreto. Puede ser cualquier valor que sea exclusivo de usted.

ID de solicitud

Un ID de solicitud que debe generar. Deberá proporcionar el ID en uno de los encabezados de la solicitud POST de API al crear la relación de sincronización.

Protocolo de extremo

Uno de los siguientes protocolos, tal como se ha definido "en la documentación de post relationship v2": S3, AZURE o GCP (cada UNO debe estar en mayúscula).

Credos

La dirección URL debe terminar con *creds*.

Ejemplos

En los ejemplos siguientes se muestran las direcciones URL de los secretos.

Ejemplo de la URL completa y la ruta de acceso para las credenciales de origen

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

Como puede ver en el ejemplo, la ruta de acceso de prefijo es */my-path/all-Secrets/*, el ID de solicitud es *hb312vdasr2* y el extremo de origen es S3.

Ejemplo de la URL completa y la ruta para las 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 la solicitud es *n32hcbnejk2* y el extremo de destino es Azure.

Preparación del grupo de Data broker

Prepare el grupo de Data broker para recuperar credenciales del almacén externo modificando el archivo de configuración local de 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/database roker/config.
3. Establezca enable en **true** y establezca los campos de parámetros config en *external-integraciones.hashicorp* de la siguiente forma:

   activado
   - Valores válidos: TRUE/FALSE
   - Tipo: Booleano
   - Valor predeterminado: FALSE
   - Verdadero: El agente de datos obtiene secretos de su propio almacén externo HashiCorp
   - False: El agente de datos almacena credenciales en su almacén local

   url
   - Tipo: Cadena
   - Valor: La URL de su almacén externo

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

   Rechazar no autorizado
   - Determina si desea que el agente de datos rechace los casos no autorizados almacén externo
   - Tipo: Booleano
   - Valor predeterminado: False

   método de autenticación
   - El método de autenticación que debe utilizar el agente de datos para acceder a las credenciales desde el almacén externo
   - Tipo: Cadena

- Valores válidos: “aws-iam” / “role-app” / “gcp-iam”

nombre-rol

- Tipo: Cadena
- Nombre de su puesto (en caso de que use aws-iam o gcp-iam)

Secretilado y roótida

- 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 corredores de datos del grupo.

Ejemplo de autenticación de rol 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"
      }
    }
  }
}
```

Configuración de permisos cuando se utiliza la autenticación gcp-iam

Si está utilizando el método de autenticación *gcp-iam*, el intermediario de datos debe tener el siguiente permiso de GCP:

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

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

Crear una nueva relación de sincronización mediante secretos del almacén

Ahora que todo está configurado, puede enviar una llamada a la API para crear una relación de sincronización que utilice su almacén para obtener los secretos.

Publica la relación mediante la API de REST DE copia y sincronización de BlueXP.

```
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 su ID de cuenta de BlueXP, "consulte esta página en la documentación".
- Para crear un cuerpo para su relación de post, "Consulte la llamada a la API Relationships-v2".

Ejemplo

Ejemplo de 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"
        }
    }
}
```