



Utilice Cloud Sync

Cloud Sync

NetApp

March 09, 2023

Tabla de Contenido

- Utilice Cloud Sync 1
 - Sincronice datos entre un origen y un destino 1
 - Pago de las relaciones de sincronización después de que finalice su prueba gratuita 20
 - Gestión de relaciones de sincronización 22
 - Administrar grupos de agentes de datos 29
 - Creación y visualización de informes para ajustar la configuración 36
 - Desinstalar el Data broker 39

Utilice Cloud Sync

Sincronice datos entre un origen y un destino

Creación de relaciones de sincronización

Al crear una relación de sincronización, el servicio Cloud Sync copia los archivos del origen al 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. Haga clic en **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, haga clic en **Sincronizar**.
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 Data broker, haga clic en **continuar**.



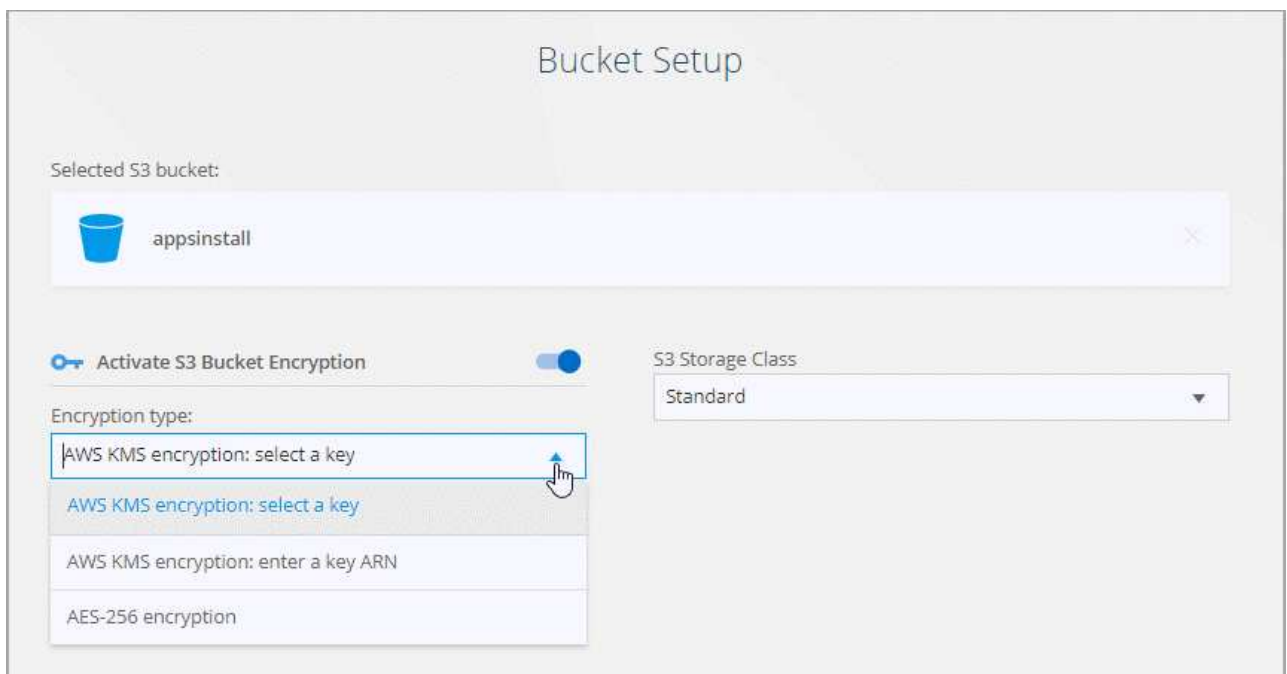
6. en la página **directorios**, seleccione un directorio o subdirectorio de nivel superior.

Si Cloud Sync no puede recuperar las exportaciones, haga clic en **Agregar exportación manualmente** e introduzca 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.
 - Haga clic en **Agregar a la lista** para seleccionar un bloque 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

Defina si Cloud Sync debe cancelar una sincronización de datos si la sincronización no se ha completado en el número de horas o días especificado.

Notificaciones

Le permite elegir si desea recibir notificaciones de Cloud Sync en el Centro de notificación 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

Defina el número de veces que Cloud Sync debe volver a intentar sincronizar un archivo antes de omitirlo.

Sincronización continua

Después de la sincronización inicial de datos, Cloud Sync escucha los cambios en el bloque de S3 de origen o en el bloque de almacenamiento en cloud de Google y sincroniza continuamente cualquier cambio 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.

Comparar por

Elija si Cloud Sync debe comparar ciertos atributos al determinar si un archivo o directorio ha cambiado y debe sincronizarse de nuevo.

Aunque desactive estos atributos, Cloud Sync seguirá comparando el origen con el destino comprobando las rutas de acceso, los tamaños de archivo y los nombres de archivo. Si hay cambios, sincroniza esos archivos y directorios.

Puede habilitar o deshabilitar Cloud Sync si compara 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 del origen, Cloud Sync copia este objeto en la siguiente sincronización, pero si un usuario cambia las etiquetas del origen (y no los datos en sí), Cloud Sync no copia 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 archivos de la ubicación de origen después de que Cloud Sync copie 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
    }
  }
}
```

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 van a incluir en cada sincronización: Archivos, directorios y enlaces simbólicos.

Excluir extensiones de archivo

Especifique 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/cloud-manager-sync//media/video_file_extensions.mp4 (video)

Excluir nombres de directorio

Especifique un máximo de 15 directorios para excluir de la sincronización escribiendo su nombre y pulsando **Intro**. Los directorios .copy-fload, .snapshot, ~snapshot se excluyen de forma predeterminada. Si desea incluirlas en su sincronización, póngase en contacto con nosotros.

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

Copiar ACL de un servidor SMB habilitando una configuración cuando se crea 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.

The screenshot shows the 'Relationship Tags' configuration page. At the top, there is a navigation bar with five items: a back arrow, 'AWS S3 Bucket' (checked), 'Settings' (checked), '6 Tags/Metadata' (active), and '7 Review'. The main heading is 'Relationship Tags'. Below it, a message states: 'Cloud Sync assigns the relationship tags to all of the files transferred to the S3 bucket. This enables you to search for the transferred files by using the tag values.' There are two radio button options: 'Save on Object's Tags' (selected) and 'Save On Object's Metadata'. Below these are two input fields: 'Tag Key' with a placeholder 'Up to 128 characters' and 'Tag Value' with a placeholder 'Up to 256 characters'. At the bottom left is a button with a plus icon and the text 'Add Relationship Tag'. At the bottom right is the text 'Optional Field | [Up to 5]'.



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

resultado

Cloud Sync inicia la sincronización de datos entre el origen y el destino.

Cree relaciones de sincronización desde Cloud Data Sense

Cloud Sync se integra con Cloud Data Sense. Desde detección de datos, puede seleccionar los archivos de origen que desea sincronizar con una ubicación de destino mediante Cloud Sync.

Después de iniciar una sincronización de datos desde Cloud Data Sense, toda la información de origen se encuentra en un único paso y solo requiere que introduzca unos cuantos detalles clave. A continuación, elija la ubicación de destino para la nueva relación de sincronización.

Source	Host	Working Environment	Volume
/cifs1	1.1.1.1	cifs	\1.1.1.1\cifs1

["Descubra cómo iniciar una relación de sincronización desde Cloud Data Sense"](#).

Copiar ACL de recursos compartidos de SMB

Cloud Sync 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 ONTAP S3). Si es necesario, también se dispone de la opción de conservar manualmente las ACL entre las unidades SMB mediante robocopy.

Opciones

- [Configure Cloud Sync para que copie automáticamente las ACL](#)
- [Copiar manualmente las ACL entre los recursos compartidos de SMB](#)

Configuración de Cloud Sync para copiar ACL

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.

Lo que necesitará

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 un servidor SMB o un almacenamiento de objetos como origen y un servidor SMB o almacenamiento de objetos como 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**.

Select an SMB Source

SMB Version : 2.1 ▼

Selected SMB Server:
10.20.30.152

Define SMB Credentials:

User Name: user1 Password: ***** Domain (Optional):

ACL - Access Control List

☒ Copy Access Control Lists to the target

Notice: Copying ACLs can affect sync performance.
You can change this setting after you create the relationship.

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 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 el origen y el destino.

Copia manual de 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. 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>

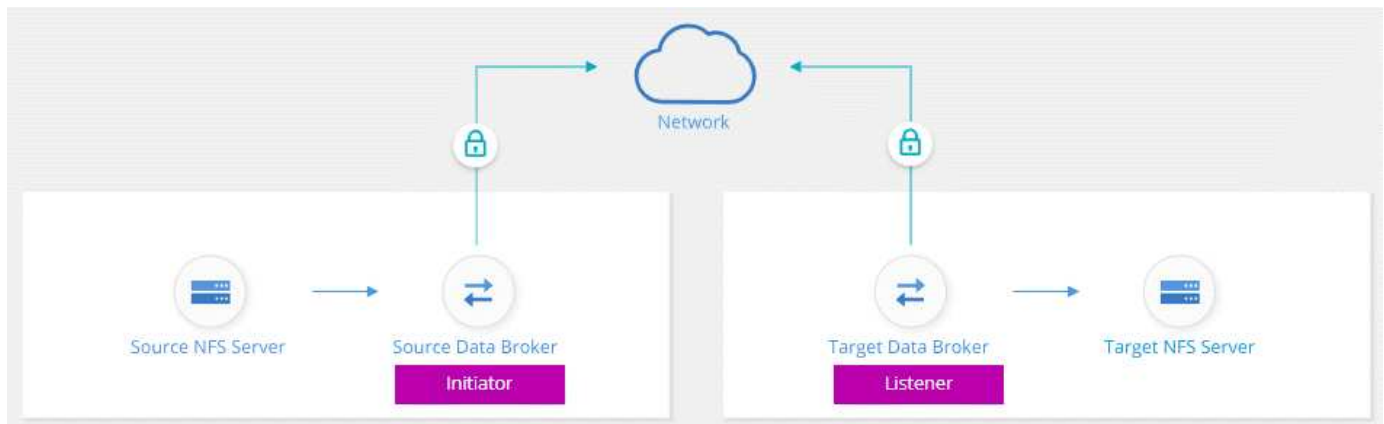
Sincronizando los datos NFS mediante el cifrado de datos en tránsito

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.

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

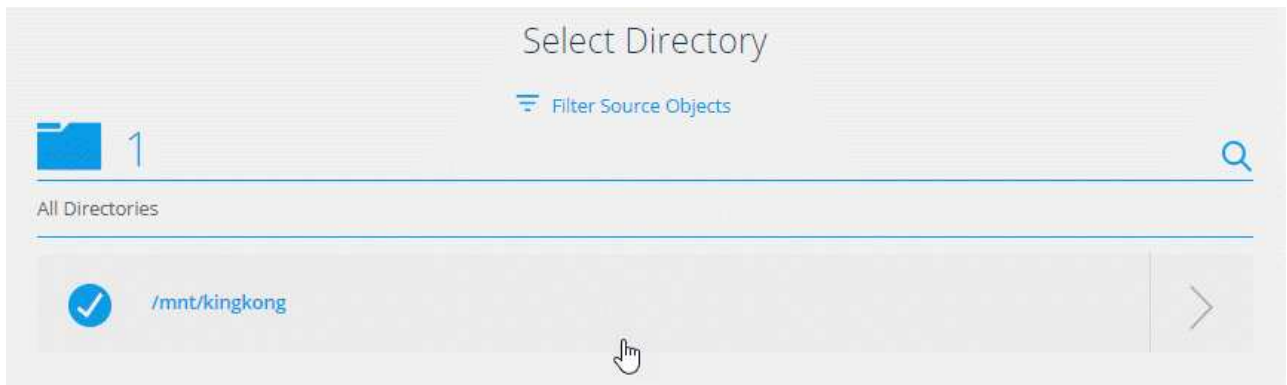
1. Haga clic en **Crear nueva sincronización**.
2. Arrastre y suelte **servidor NFS** a las ubicaciones de origen y destino o **Azure NetApp Files** a las ubicaciones de origen y destino y seleccione **Sí** para activar el cifrado de datos en vuelo.
3. Siga las indicaciones para crear la relación:
 -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


Select a Provider




Microsoft Azure



Amazon Web Services



Google Cloud Platform

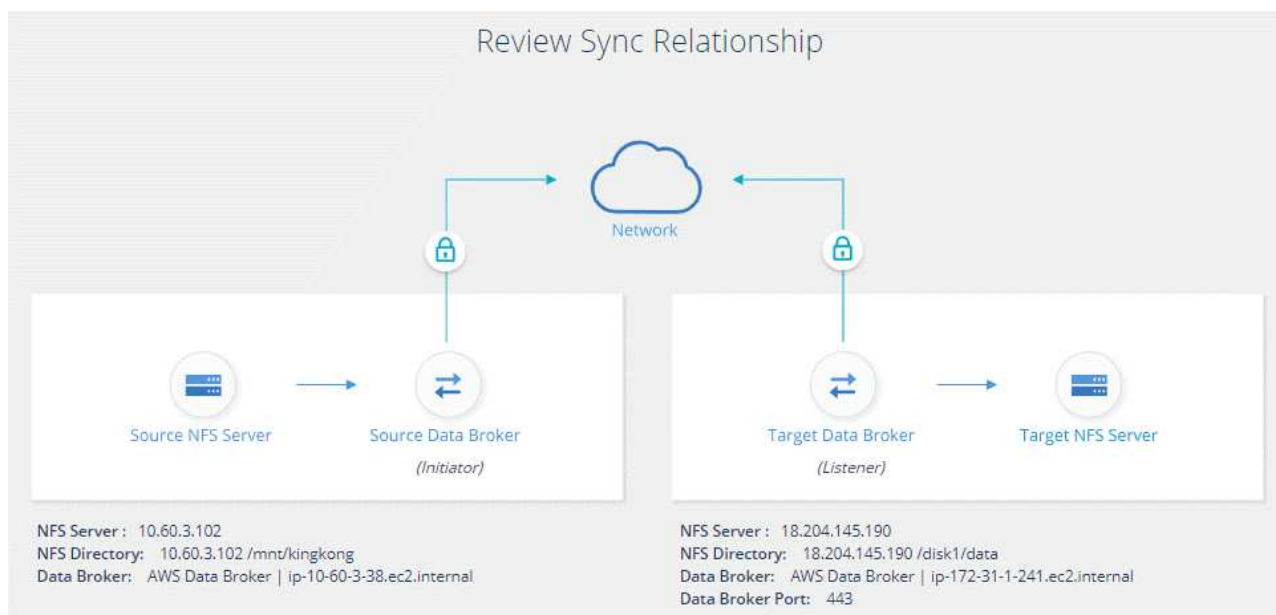


On-Prem Data Broker

Data Broker Name:

Port:

- 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.

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

Al crear una relación de sincronización que requiera credenciales de Amazon S3, Azure o Google Cloud, debe especificar dichas credenciales a través de la interfaz de usuario o la API de Cloud Sync. 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 a través de la API de Cloud Sync con relaciones sincronizadas que requieren las 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

Deberá proporcionar a Cloud Sync la URL de los secretos del 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/hb312vdsr2/S3Creds`

Como puede ver en el ejemplo, la ruta de acceso de prefijo es `/my-path/all-Secrets/`, el ID de solicitud es `hb312vdsr2` 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.

Coloque la relación mediante la API DE REST de Cloud Sync.

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": "5e6e111d578dtyuul555sa60",
  "source": {
    "protocol": "s3",
    "s3": {
      "provider": "sgws",
      "host": "1.1.1.1",
      "port": "443",
      "bucket": "my-source"
    }
  },
  "target": {
    "protocol": "s3",
    "s3": {
      "bucket": "my-target-bucket"
    }
  }
}
```

Pago de las relaciones de sincronización después de que finalice su prueba gratuita

Hay dos formas de pagar las relaciones de sincronización después de que termine su prueba gratuita de 14 días. La primera opción es suscribirse a AWS o Azure para pagar por uso o anualmente. La segunda opción consiste en comprar licencias directamente a NetApp.

Puede suscribirse desde el AWS Marketplace o desde Azure Marketplace. No puede suscribirse de ambos.

Puede utilizar licencias de NetApp con una suscripción a Marketplace. Por ejemplo, si tiene 25 relaciones de sincronización, puede pagar las primeras 20 relaciones de sincronización con una licencia y, a continuación, pagar por el uso desde AWS o Azure con las 5 relaciones de sincronización restantes.

["Obtenga más información sobre cómo funcionan las licencias".](#)

Si usted no paga inmediatamente después de que su prueba gratuita termina, usted no podrá crear ninguna relación adicional. Las relaciones existentes no se eliminan, pero no puede realizar ningún cambio hasta que se suscriba o introduzca una licencia.

Las licencias se deben administrar a través de Cloud Sync o del sitio web correspondiente y **no** a través de una cartera digital.

Suscribirse a AWS

AWS le permite pagar anualmente.

De pago por uso

1. Haga clic en **Sincronizar > licencias**.
2. Seleccione **AWS**
3. Haga clic en **Suscribirse** y, a continuación, en **continuar**.
4. Suscríbase desde el mercado de AWS y, a continuación, vuelva a iniciar sesión en el servicio Cloud Sync para completar el registro.

El siguiente vídeo muestra el proceso:

► https://docs.netapp.com/es-es/cloud-manager-sync//media/video_cloud_sync_registering.mp4 (video)

Pasos a pagar anualmente

1. ["Vaya a la página AWS Marketplace"](#).
2. Haga clic en **continuar para suscribirse**.
3. Seleccione sus opciones de contrato y haga clic en **Crear contrato**.

suscribirse de Azure

Azure le permite pagar por uso o anualmente.

Lo que necesitará

Cuenta de usuario de Azure con permisos de colaborador o propietario en la suscripción correspondiente.

Pasos

1. Haga clic en **Sincronizar > licencias**.
2. Seleccione **Azure**.
3. Haga clic en **Suscribirse** y, a continuación, en **continuar**.
4. En el portal de Azure, haga clic en **Crear**, seleccione sus opciones y haga clic en **Suscribirse**.

Seleccione **Mensual** para pagar por hora, o **Anual** para pagar por un año antes de la fecha.

5. Una vez completada la implementación, haga clic en el nombre del recurso SaaS en la ventana emergente de notificaciones.
6. Haga clic en **Configurar cuenta** para volver a Cloud Sync.

El siguiente vídeo muestra el proceso:

► https://docs.netapp.com/es-es/cloud-manager-sync//media/video_cloud_sync_registering_azure.mp4

(video)

Compra de licencias de NetApp y añadirlas a Cloud Sync

Para pagar por adelantado sus relaciones de sincronización, debe adquirir una o más licencias y añadirlas al servicio de Cloud Sync.

Lo que necesitará

Necesitará el número de serie de su licencia, así como el nombre de usuario y la contraseña de la cuenta del sitio de soporte de NetApp con la que está asociada la licencia.

Pasos

1. Adquiera una licencia por correo electrónico:ng-cloudsync-contact@netapp.com?Subject=Cloud%20Sync%20Service%20-%20BYOL%20Licencia%20Compra%20Solicite[Contacto con NetApp].
2. En BlueXP, haga clic en **Sincronizar > licencias**.
3. Haga clic en **Agregar licencia** y agregue la información necesaria:
 - a. Introduzca el número de serie.
 - b. Seleccione la cuenta del sitio de soporte de NetApp asociada con la licencia que va a añadir:
 - Si su cuenta ya se ha añadido a BlueXP, selecciónela en la lista desplegable.
 - Si aún no se ha agregado su cuenta, haga clic en **Agregar credenciales de NSS**, introduzca el nombre de usuario y la contraseña, haga clic en **Registro** y, a continuación, selecciónela en la lista desplegable.
 - c. Haga clic en **Agregar**.

Actualizar una licencia

Si ha ampliado una licencia de Cloud Sync que ha comprado a NetApp, la nueva fecha de caducidad no se actualizará automáticamente en Cloud Sync. Debe volver a agregar la licencia para actualizar la fecha de caducidad. Las licencias se deben administrar a través de Cloud Sync o del sitio web correspondiente y **no** a través de una cartera digital.

Pasos

1. En BlueXP, haga clic en **Sincronizar > licencias**.
2. Haga clic en **Agregar licencia** y agregue la información necesaria:
 - a. Introduzca el número de serie.
 - b. Seleccione la cuenta del sitio de soporte de NetApp asociada con la licencia que va a añadir.
 - c. Haga clic en **Agregar**.

Resultado

Cloud Sync actualiza la licencia existente con la nueva fecha de caducidad.


Gestión de relaciones de sincronización

Puede gestionar las relaciones de sincronización en cualquier momento sincronizando de forma inmediata datos, cambiando programaciones y mucho más.

Realice una sincronización inmediata de datos

En lugar de esperar a la siguiente sincronización programada, puede pulsar un botón para sincronizar inmediatamente los datos entre la fuente y el destino.

Pasos

1. Desde **Dashboard**, desplácese hasta la relación de sincronización y haga clic en 
2. Haga clic en **Sincronizar ahora** y, a continuación, en **Sincronizar** para confirmar.

Resultado

Cloud Sync inicia el proceso de sincronización de datos para la relación.

Acelerando el rendimiento de la sincronización

Acelere el rendimiento de una relación de sincronización añadiendo un agente de datos adicional al grupo que administra la relación. El agente de datos adicional debe ser un intermediario de datos *new*.

Cómo funciona


Si el grupo de Data broker administra otras relaciones de sincronización, el nuevo Data broker que agregue al grupo también acelera el rendimiento de esas relaciones de sincronización.

Por ejemplo, digamos que usted tiene tres relaciones:

- La relación 1 está administrada por el grupo De Data broker A
- La relación 2 es administrada por el grupo de Data broker B
- La relación 3 está administrada por el grupo de Data broker A

Desea acelerar el rendimiento de la relación 1 para agregar un nuevo agente de datos al grupo de intermediarios de datos A. Dado que el grupo A también gestiona la relación de sincronización 3, el rendimiento de sincronización de la relación se acelera automáticamente.

Pasos

1. Asegúrese de que al menos uno de los agentes de datos existentes en la relación esté en línea.
2. Desde **Dashboard**, desplácese hasta la relación de sincronización y haga clic en 
3. Haga clic en **acelerar**.
4. Siga las indicaciones para crear un nuevo Data broker.

Resultado

Cloud Sync agrega el nuevo agente de datos al grupo. Es necesario acelerar el rendimiento de la siguiente sincronización de datos.

Actualizando credenciales

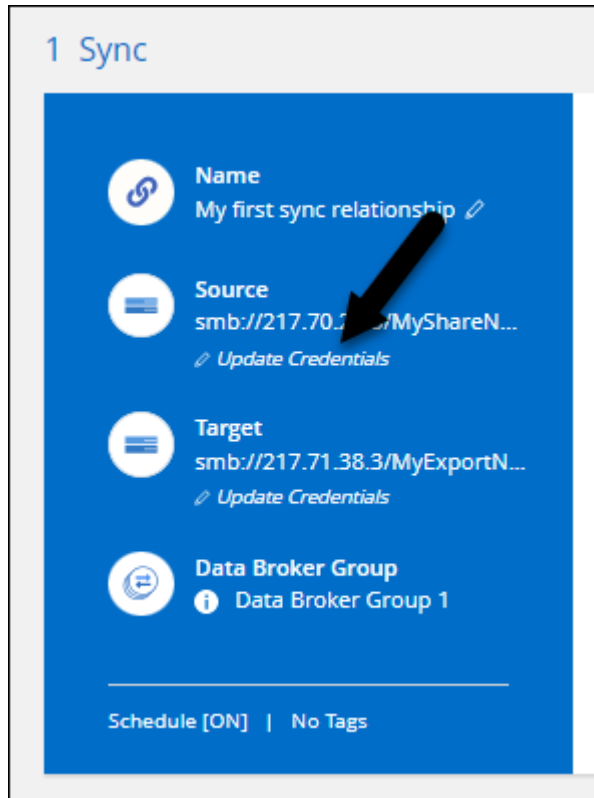
Puede actualizar el agente de datos con las credenciales más recientes del origen o destino en una relación de sincronización existente. La actualización de las credenciales puede ayudar si las políticas de seguridad requieren que actualice las credenciales de forma periódica.

Las credenciales para actualizar son compatibles con cualquier origen o destino que Cloud Sync requiera credenciales para: Azure Blob, Box, IBM Cloud Object Storage, StorageGRID, ONTAP S3 Storage, SFTP y

servidores SMB.

Pasos

1. En **Consola de sincronización**, vaya a una relación de sincronización que requiere credenciales y, a continuación, haga clic en **Actualizar credenciales**.



2. Introduzca las credenciales y haga clic en **Actualizar**.

Una nota sobre los servidores SMB: Si el dominio es nuevo, deberá especificarlo al actualizar las credenciales. Si el dominio no ha cambiado, no es necesario volver a introducirlo.

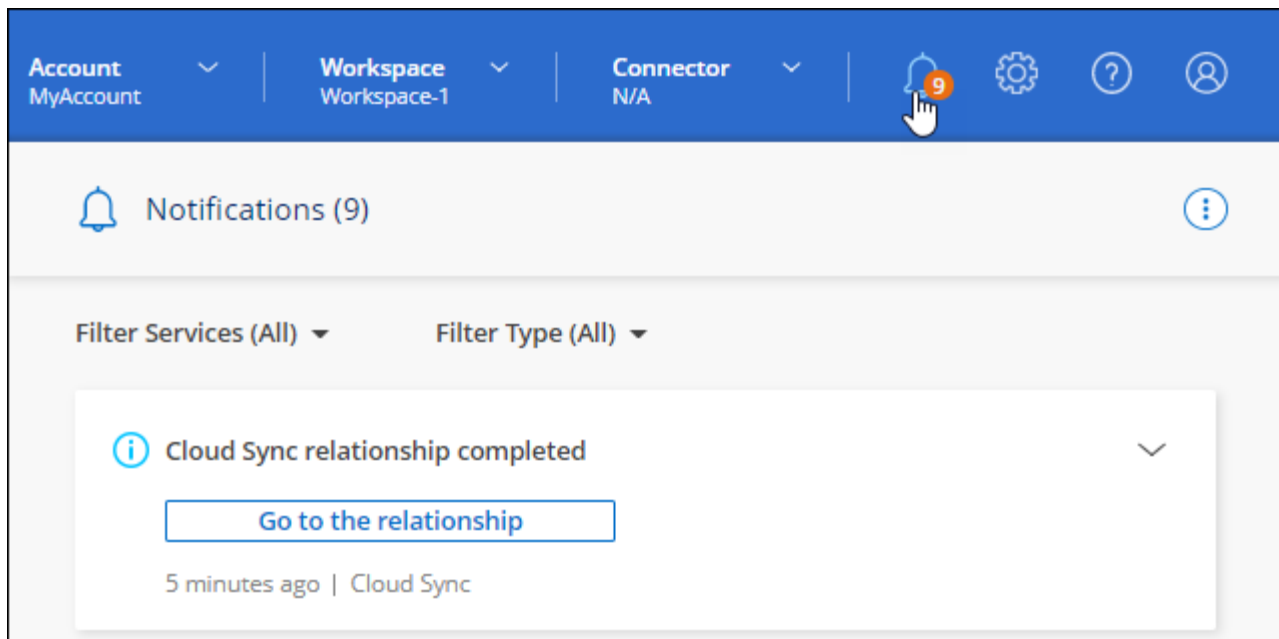
Si introdujo un dominio al crear la relación de sincronización, pero no introduce un dominio nuevo al actualizar las credenciales, Cloud Sync seguirá utilizando el dominio original que ha proporcionado.

Resultado

Cloud Sync actualiza las credenciales del agente de datos. Puede tardar hasta 10 que el agente de datos comience a usar las credenciales actualizadas para sincronizar los datos.


Configuración de notificaciones

Una configuración de **Notificaciones** para cada relación de sincronización permite elegir si desea recibir notificaciones de Cloud Sync en el Centro de notificación 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.



Además, también puede recibir notificaciones por correo electrónico.

Pasos


1. Modifique la configuración de una relación de sincronización:
 - a. Desde **Dashboard**, desplácese hasta la relación de sincronización y haga clic en .
 - b. Haga clic en **Configuración**.
 - c. Activar **Notificaciones**.
 - d. Haga clic en **Guardar configuración**.
2. Si desea recibir notificaciones por correo electrónico, configure los ajustes de alerta y notificaciones:
 - a. Haga clic en **Configuración > Configuración de alertas y notificaciones**.
 - b. Seleccione un usuario o varios usuarios y elija el tipo de notificación **Info**.
 - c. Haga clic en **aplicar**.

Resultado

Ahora recibirá notificaciones de Cloud Sync en el Centro de notificaciones de BlueXP, con unas notificaciones que llegan por correo electrónico, si configuró esta opción.

Cambiar la configuración de una relación de sincronización

Modifique la configuración que define cómo se sincronizan y mantienen los archivos y carpetas de origen en la ubicación de destino.

1. Desde **Dashboard**, desplácese hasta la relación de sincronización y haga clic en .
2. Haga clic en **Configuración**.
3. Modifique cualquiera de los ajustes.

General

Schedule

ON | Every 1 Day

Retries

Retry 3 times before skipping file

Files and Directories

Compare By

The following attributes (and size): uid, gid, mode, mtime

Recently Modified Files

Exclude files that are modified up to 30 Seconds before a scheduled sync

Delete Files On Source

Never delete files from the source location

Delete Files On Target

Never delete files from the target location

File Types

Include All: Files, Directories, Symbolic Links

Exclude File Extensions

None

File Size

All

Date Modified

All

Date Created

All

ACL - Access Control List

Inactive

Reset to defaults

aquí hay una breve descripción de cada configuración:

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

Defina si Cloud Sync debe cancelar una sincronización de datos si la sincronización no se ha completado en el número de horas o días especificado.

Notificaciones

Le permite elegir si desea recibir notificaciones de Cloud Sync en el Centro de notificación 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.

Si desea recibir notificaciones para

Reintentos

Defina el número de veces que Cloud Sync debe volver a intentar sincronizar un archivo antes de omitirlo.

Comparar por

Elija si Cloud Sync debe comparar ciertos atributos al determinar si un archivo o directorio ha cambiado y debe sincronizarse de nuevo.

Aunque desactive estos atributos, Cloud Sync seguirá comparando el origen con el destino comprobando las rutas de acceso, los tamaños de archivo y los nombres de archivo. Si hay cambios, sincroniza esos archivos y directorios.

Puede habilitar o deshabilitar Cloud Sync si compara 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

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

Archivos modificados recientemente

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

Eliminar archivos en el origen

Elija eliminar archivos de la ubicación de origen después de que Cloud Sync copie 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
    }
  }
}
```

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 van a incluir en cada sincronización: Archivos, directorios y enlaces simbólicos.

Excluir extensiones de archivo

Especifique 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/cloud-manager-sync//media/video_file_extensions.mp4 (video)

Excluir nombres de directorio

Especifique un máximo de 15 directorios para excluir de la sincronización escribiendo su nombre y pulsando **Intro**. Los directorios .copy-fload, .snapshot, ~snapshot se excluyen de forma predeterminada. Si desea incluirlas en su sincronización, póngase en contacto con nosotros.

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

Copiar ACL de un servidor SMB habilitando una configuración cuando se crea una relación o después de crear una relación.

4. Haga clic en **Guardar configuración**.


Resultado

Cloud Sync modifica la relación de sincronización con las nuevas opciones de configuración.

Eliminar relaciones

Puede eliminar una relación de sincronización si ya no necesita sincronizar datos entre el origen y el destino. Esta acción no elimina el grupo de Data broker (o las instancias individuales de data broker) y no elimina los datos del destino.

Pasos

1. Desde **Dashboard**, desplácese hasta la relación de sincronización y haga clic en 
2. Haga clic en **Eliminar** y, a continuación, vuelva a hacer clic en **Eliminar** para confirmar.

Resultado

Cloud Sync elimina la relación de sincronización.

Administrar grupos de agentes de datos

Un grupo de agentes de datos sincroniza los datos de una ubicación de origen con una ubicación de destino. Se necesita al menos un agente de datos en un grupo para cada relación de sincronización que cree. Administrar grupos de agentes de datos agregando un nuevo agente de datos a un grupo, visualizando información acerca de los grupos y mucho más.

Cómo funcionan los grupos de agentes de datos

Un grupo de agentes de datos puede incluir uno o más agentes de datos. La agrupación conjunta de agentes de datos puede ayudar a mejorar el rendimiento de las relaciones de sincronización.

Los grupos pueden gestionar varias relaciones

Un grupo de Data broker puede gestionar una o más relaciones de sincronización a la vez.

Por ejemplo, digamos que usted tiene tres relaciones:

- La relación 1 está administrada por el grupo De Data broker A
- La relación 2 es administrada por el grupo de Data broker B
- La relación 3 está administrada por el grupo de Data broker A

Desea acelerar el rendimiento de la relación 1 para agregar un nuevo agente de datos al grupo de intermediarios de datos A. Dado que el grupo A también gestiona la relación de sincronización 3, el rendimiento de sincronización de la relación se acelera automáticamente.

Número de agentes de datos en un grupo

En muchos casos, un único agente de datos puede satisfacer los requisitos de rendimiento de una relación de sincronización. De lo contrario, puede acelerar el rendimiento de sincronización añadiendo agentes de datos adicionales al grupo. Pero primero debe comprobar otros factores que pueden afectar al rendimiento de la sincronización. ["Obtenga más información sobre cómo determinar cuándo es necesario el uso de varios agentes de datos son obligatorios"](#).

Recomendaciones de seguridad

Para garantizar la seguridad del equipo de intermediarios de datos, NetApp recomienda lo siguiente:

- SSH no debe permitir el reenvío X11
- SSH no debe permitir el reenvío de conexión TCP
- SSH no debe permitir túneles
- SSH no debe aceptar variables de entorno del cliente

Estas recomendaciones de seguridad pueden ayudar a evitar conexiones no autorizadas al equipo de intermediarios de datos.

Agregar un nuevo agente de datos a un grupo

Hay varias formas de crear un nuevo Data broker:

- Al crear una nueva relación de sincronización

["Aprenda a crear un nuevo agente de datos al crear una relación de sincronización"](#).

- En la página **gestionar agentes de datos**, haga clic en **Agregar nuevo Data Broker** que crea el agente de datos en un nuevo grupo
- Desde la página **gestionar agentes de datos** creando un nuevo agente de datos en un grupo existente

Antes de empezar

- No puede agregar gestores de datos a un grupo que gestione una relación de sincronización cifrada.
- Si desea crear un agente de datos en un grupo existente, el agente de datos debe ser un agente de datos en las instalaciones o el mismo tipo de agente de datos.

Por ejemplo, si un grupo incluye un agente de datos de AWS, puede crear un agente de datos de AWS o un agente de datos en las instalaciones de ese grupo. No se puede crear un agente de datos de Azure ni un agente de datos de Google Cloud porque no son el mismo tipo de agente de datos.

Pasos para crear un agente de datos en un grupo nuevo

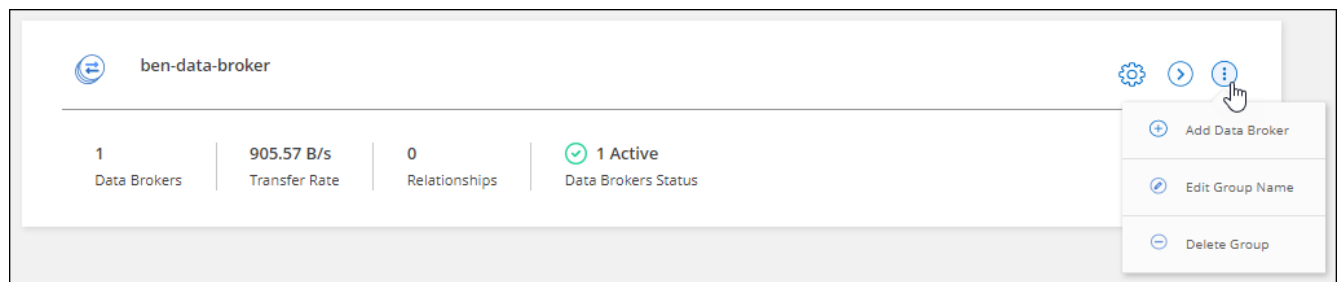
1. Haga clic en **Sincronizar > gestionar agentes de datos**.
2. Haga clic en **Agregar nuevo agente de datos**.
3. Siga las indicaciones para crear el Data broker.

Para obtener ayuda, 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"](#)

Pasos para crear un agente de datos en un grupo existente

1. Haga clic en **Sincronizar > gestionar agentes de datos**.
2. Haga clic en el menú de acción y seleccione **Agregar agente de datos**.



3. Siga las instrucciones para crear el Data broker en el grupo.

Para obtener ayuda, 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"](#)

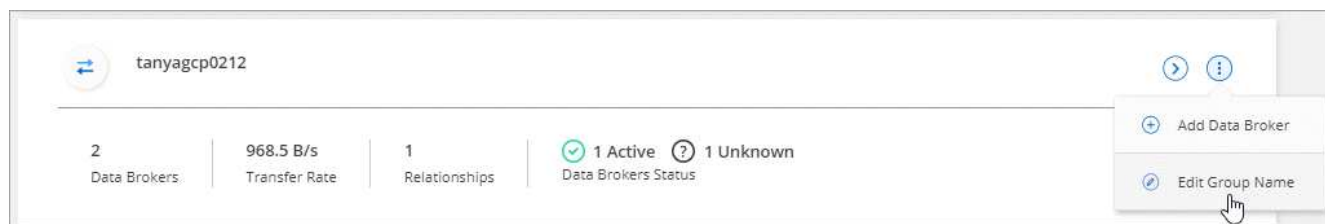
- "Instalar el agente de datos en un host Linux"

Edite el nombre de un grupo

Cambie el nombre de un grupo de Data broker en cualquier momento.

Pasos

1. Haga clic en **Sincronizar > gestionar agentes de datos**.
2. Haga clic en el menú de acción y seleccione **Editar nombre de grupo**.



3. Introduzca un nuevo nombre y haga clic en **Guardar**.

Resultado

Cloud Sync actualiza el nombre del grupo de agentes de datos.

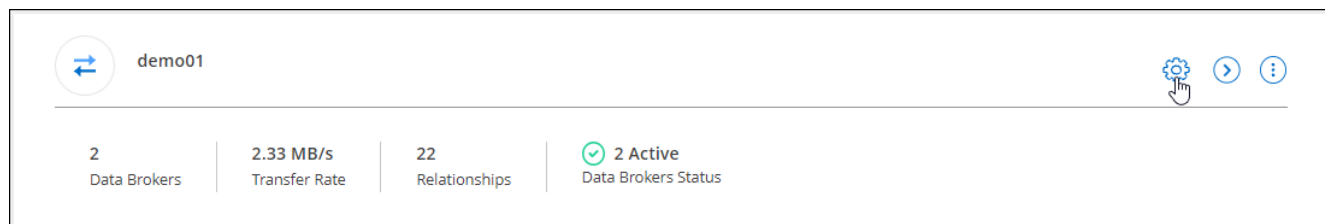
Configuración unificada

Si una relación de sincronización detecta errores durante el proceso de sincronización, la unificación de la concurrencia del grupo de Data broker puede ayudar a reducir el número de errores de sincronización. Tenga en cuenta que los cambios en la configuración del grupo pueden afectar al rendimiento ralentizando la transferencia.

No recomendamos cambiar la configuración por su cuenta. Debe consultar con NetApp para saber cuándo cambiar la configuración y cómo modificarla.

Pasos

1. Haga clic en **gestionar agentes de datos**.
2. Haga clic en el icono Configuración de un grupo de Data broker.



3. Cambie la configuración según sea necesario y, a continuación, haga clic en **Unify Configuration**.

Tenga en cuenta lo siguiente:

- Puede seleccionar y elegir los ajustes que desea cambiar: No es necesario cambiar los cuatro a la vez.
- Después de enviar una nueva configuración a un agente de datos, el Data broker se reinicia automáticamente y utiliza la nueva configuración.

- Puede tardar hasta que este cambio se realice y sea visible en la interfaz de Cloud Sync.
- Si un agente de datos no se está ejecutando, su configuración no cambiará porque Cloud Sync no se puede comunicar con él. La configuración cambiará después de reiniciar el Data broker.
- Una vez establecida una configuración unificada, los nuevos agentes de datos utilizarán automáticamente la nueva configuración.

Mueva los agentes de datos entre grupos


Si necesita acelerar el rendimiento del grupo de intermediarios de datos de destino, mueva un agente de datos de un grupo a otro.

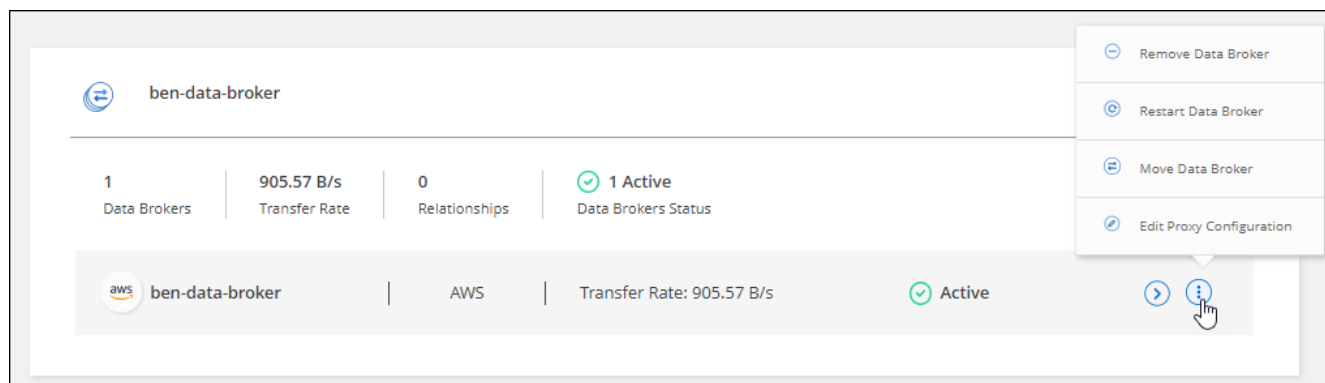
Por ejemplo, si un agente de datos ya no gestiona una relación de sincronización, puede moverla fácilmente a otro grupo que esté gestionando las relaciones de sincronización.

Limitaciones

- Si un grupo de Data broker gestiona una relación de sincronización y sólo hay un agente de datos en el grupo, no podrá mover dicho agente de datos a otro grupo.
- No se puede mover un agente de datos a un grupo que gestione relaciones de sincronización cifradas ni desde él.
- No puede mover un agente de datos que se esté implementando actualmente.

Pasos

1. Haga clic en **Sincronizar > gestionar agentes de datos**.
2. Haga clic en  para ampliar la lista de agentes de datos de un grupo.
3. Haga clic en el menú de acción de un agente de datos y seleccione **mover agente de datos**.



4. Cree un nuevo grupo de Data broker o seleccione un grupo de Data broker existente.
5. Haga clic en **mover**.


Resultado

Cloud Sync traslada el agente de datos a un grupo de agente de datos nuevo o existente. Si no hay otros agentes de datos en el grupo anterior, Cloud Sync lo elimina.

Actualice la configuración del proxy

Actualice la configuración de proxy de un agente de datos agregando detalles sobre una nueva configuración de proxy o editando la configuración de proxy existente.

Pasos

1. Haga clic en **Sincronizar > gestionar agentes de datos**.
2. Haga clic en  para ampliar la lista de agentes de datos de un grupo.
3. Haga clic en el menú de acción de un agente de datos y seleccione **Editar configuración de proxy**.
4. Especifique detalles sobre el proxy: Nombre de host, número de puerto, nombre de usuario y contraseña.
5. Haga clic en **Actualizar**.

Resultado

Cloud Sync actualiza el agente de datos para utilizar la configuración de proxy para el acceso a Internet.

Ver la configuración de un agente de datos

Puede que desee ver detalles sobre un agente de datos para identificar elementos como su nombre de host, dirección IP, CPU y RAM disponibles, entre otros.



Cloud Sync ofrece los siguientes detalles acerca de un agente de datos:

- Información básica: ID de instancia, nombre de host, etc.
- Red: Región, red, subred, IP privada, etc.
- Software: Distribución Linux, versión de data broker, etc.
- Hardware: CPU y RAM
- Configuración: Detalles acerca de los dos tipos de procesos principales del agente de datos: Escáner y transferir



El escáner escanea el origen y el destino y decide qué se debe copiar. El transferir realiza la copia real. Es posible que el personal de NetApp utilice estos detalles de configuración para sugerir acciones que puedan optimizar el rendimiento.

Pasos

1. Haga clic en **Sincronizar > gestionar agentes de datos**.
2. Haga clic en  para ampliar la lista de agentes de datos de un grupo.
3. Haga clic en  para ver detalles sobre un data broker.

The screenshot shows the Cloud Sync interface for a data broker group named 'tanyagcp0212'. At the top, there are summary statistics: 2 Data Brokers, 968.5 B/s Transfer Rate, 1 Relationships, and Data Brokers Status showing 1 Active and 1 Unknown. Below this is a detailed view of the 'tanyagcp0212' group, which is currently 'Active' with a transfer rate of 968.5 B/s. The detailed view includes a table with the following information:

Category	Item 1	Item 2	Item 3	Item 4
Information	5fc766b3d3e3664b9e116... Broker ID	288871247573080556 Instance ID	tanyagcp0212-mnx-data-... Host Name	cloudsync-dev-214020 Project ID
Network	us-east1-b Region	default Network	255.255.240.0 Subnet	10.142.0.37 Private IP
Software	linux Linux Distribution & Version	1.5.4 Vault Version	14.15.1 Node Version	1.3.0.18650-73f960d-integ Data Broker Version
Hardware	4 Available CPUs	62.22 MB Available RAM		
Configuration	50 Scanner Concurrency	4 Scanner CPUs	50 Transferer Concurrency	4 Transferer CPUs

Solución de problemas con un agente de datos

Cloud Sync muestra un estado para cada agente de datos que puede ayudarle a solucionar problemas.

Pasos

1. Identifique los agentes de datos con el estado "Unknown" o "Failed".

The screenshot shows the Cloud Sync interface with two data broker groups. The first group, 'tanyagcp0212', is 'Active' with a transfer rate of 968.5 B/s. The second group, 'tanya1', is 'Unknown' with a transfer rate of N/A. The 'Unknown' status is highlighted with a red circle and a question mark icon.

2. Pase el ratón sobre para ver el motivo del fallo.
3. Corrija el problema.

Por ejemplo, es posible que tenga que reiniciar simplemente el agente de datos si está desconectado o puede que necesite eliminar el agente de datos si la implementación inicial ha fallado.

Quitar un agente de datos de un grupo


Puede quitar un agente de datos de un grupo si ya no es necesario o si la implementación inicial ha fallado.

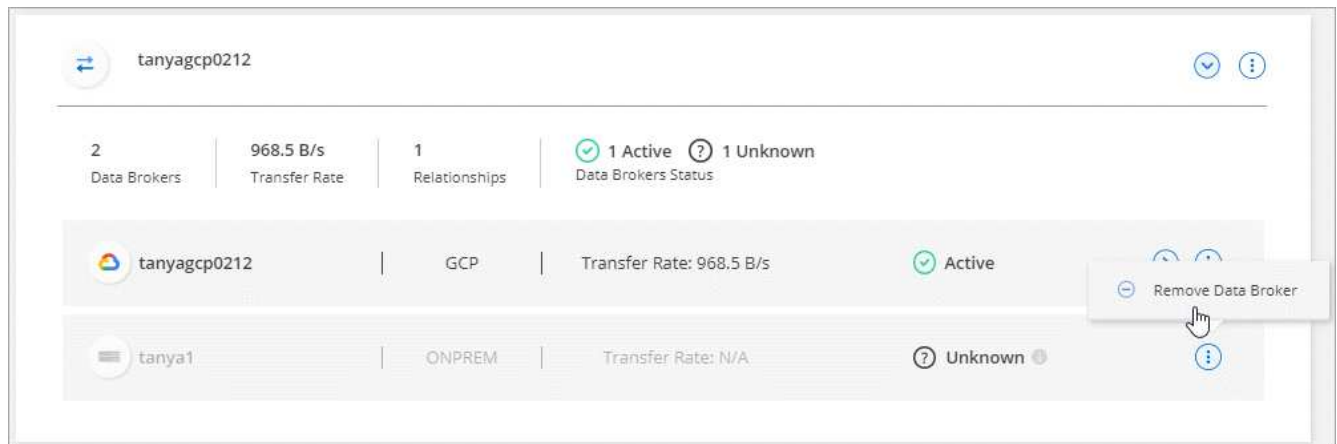
Esta acción solo elimina el agente de datos de los registros de Cloud Sync. Deberá eliminar manualmente el agente de datos y los recursos de cloud adicionales usted mismo.

Cosas que usted debe saber

- Cloud Sync elimina un grupo cuando elimina el último intermediario de datos del grupo.
- No se puede eliminar el último agente de datos de un grupo si existe una relación utilizando ese grupo.

Pasos

1. Haga clic en **Sincronizar > gestionar agentes de datos**.
2. Haga clic en  para ampliar la lista de agentes de datos de un grupo.
3. Haga clic en el menú de acción de un agente de datos y seleccione **Quitar agente de datos**.



4. Haga clic en **Quitar Data Broker**.

Resultado

Cloud Sync quita el agente de datos del grupo.

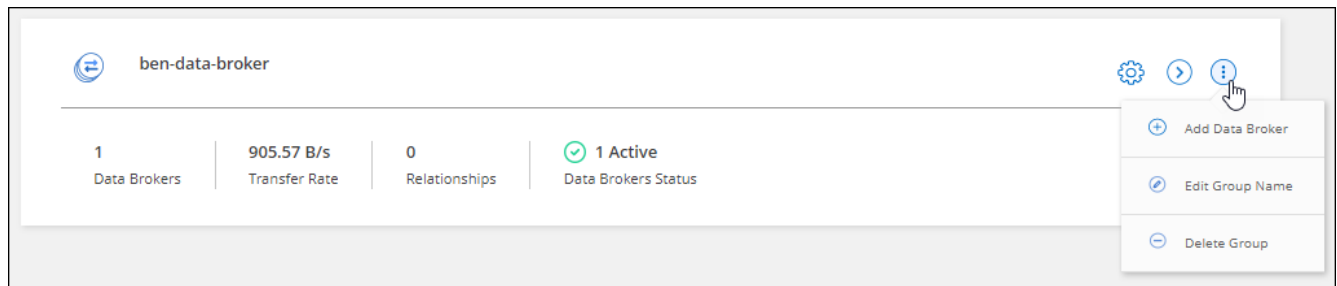
Eliminar un grupo de Data broker

Si un grupo de agentes de datos ya no gestiona ninguna relación de sincronización, puede eliminar el grupo, que elimina todos los agentes de datos de Cloud Sync.

Los agentes de datos que Cloud Sync elimina solo se eliminan de los registros de Cloud Sync. Deberá eliminar manualmente la instancia de agente de datos de su proveedor de cloud y los recursos adicionales de cloud.

Pasos

1. Haga clic en **Sincronizar > gestionar agentes de datos**.
2. Haga clic en el menú de acción y seleccione **Eliminar grupo**.



3. Para confirmar, introduzca el nombre del grupo y haga clic en **Eliminar grupo**.

Resultado

Cloud Sync elimina los intermediarios de datos y elimina el grupo.

Creación y visualización de informes para ajustar la configuración

Cree y vea informes para obtener información que puede usar con la ayuda del personal de NetApp para ajustar la configuración de un agente de datos y mejorar el rendimiento.

Cada informe proporciona detalles en profundidad sobre una ruta en una relación de sincronización. Por ejemplo, el informe de un sistema de archivos muestra cuántos directorios y archivos hay, la distribución del tamaño de los archivos, la profundidad y el ancho de los directorios y mucho más.

Crear informes

Cada vez que se crea un informe, Cloud Sync analiza la ruta y compila los detalles en un informe.

Pasos

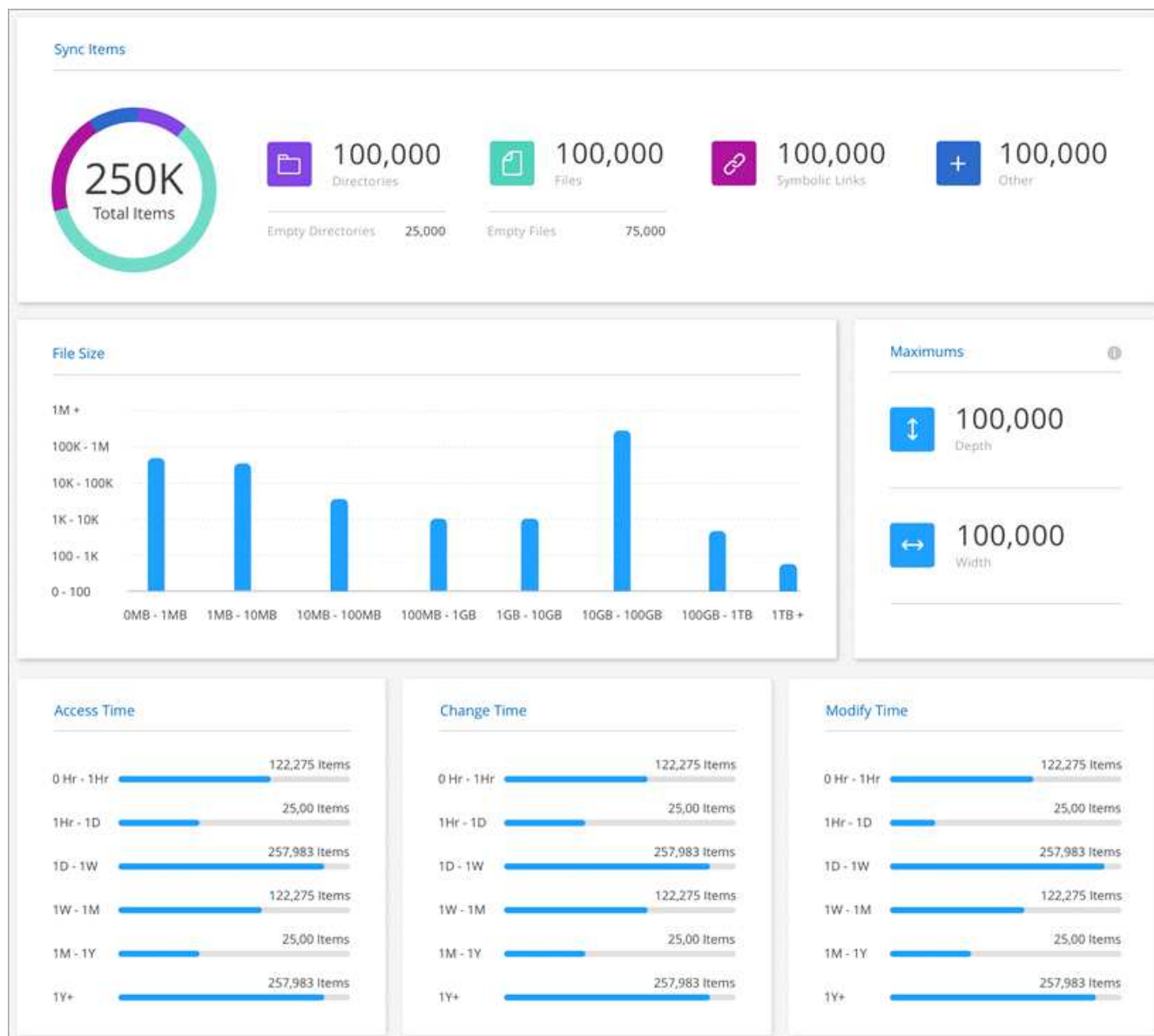
1. Haga clic en **Sincronizar > Informes**.

Las rutas (origen o destino) de cada una de las relaciones de sincronización se muestran en una tabla.

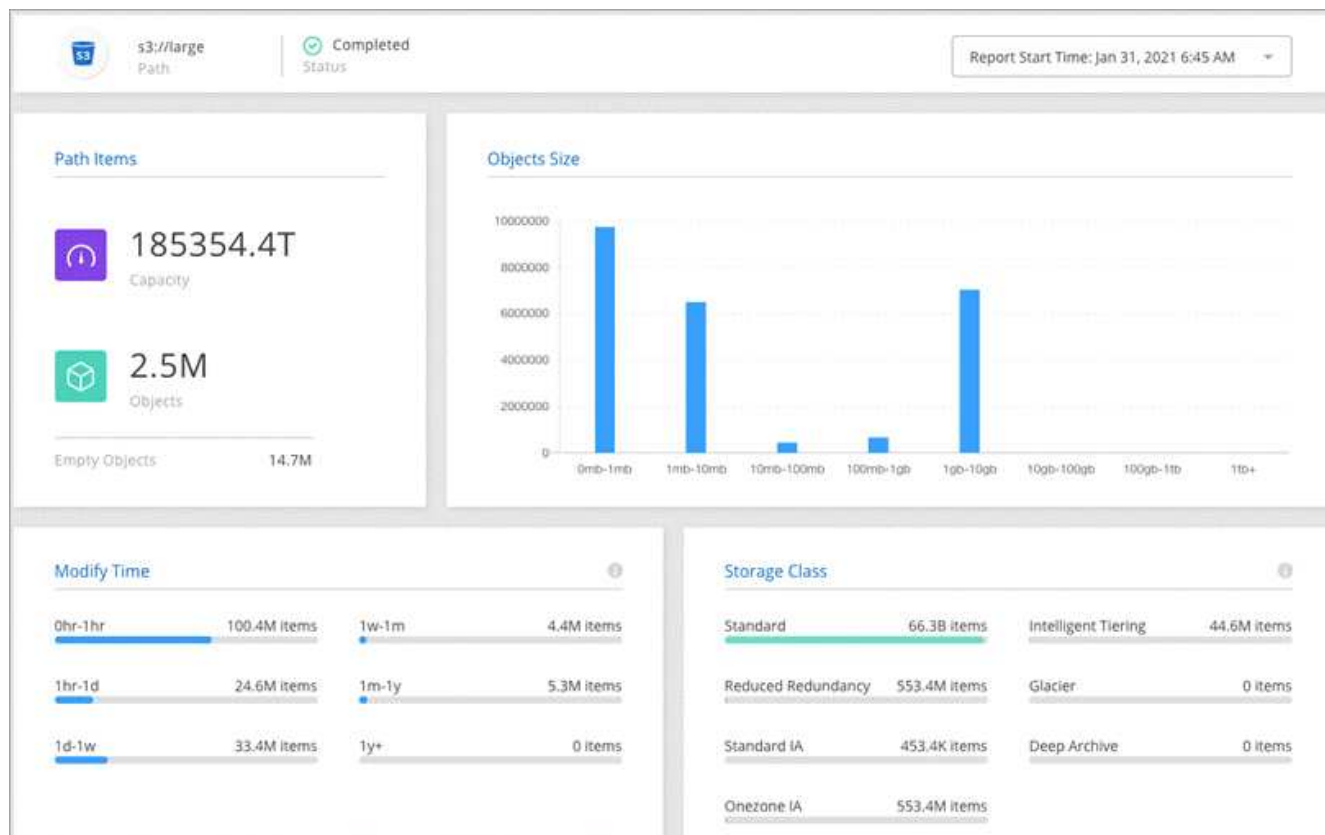
2. En la columna **acciones de Informes**, vaya a una ruta de acceso específica y haga clic en **Crear**, o haga clic en el menú de acciones y seleccione **Crear nuevo**.

3. Cuando el informe esté listo, haga clic en el menú de acciones y seleccione **Ver**.

Aquí tiene un informe de ejemplo para una ruta de acceso al sistema de archivos.



Y aquí tiene un informe de ejemplo para el almacenamiento de objetos.

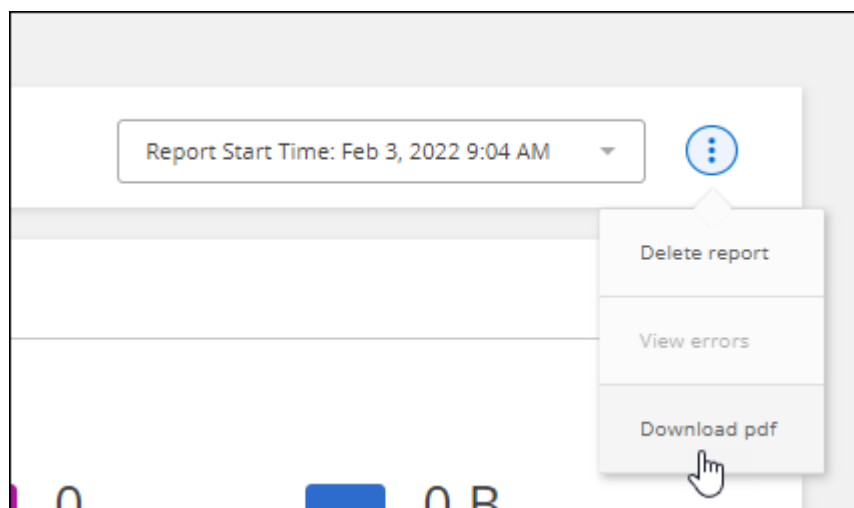


Descargando informes

Puede descargar un informe en PDF para poder verlo sin conexión o compartirlo.

Pasos

1. Haga clic en **Sincronizar > Informes**.
2. En la columna **acciones de informes**, haga clic en el menú de acciones y seleccione **Ver**.
3. En la parte superior derecha del informe, haga clic en el menú de acción y seleccione **Descargar pdf**.



Ver errores de informe

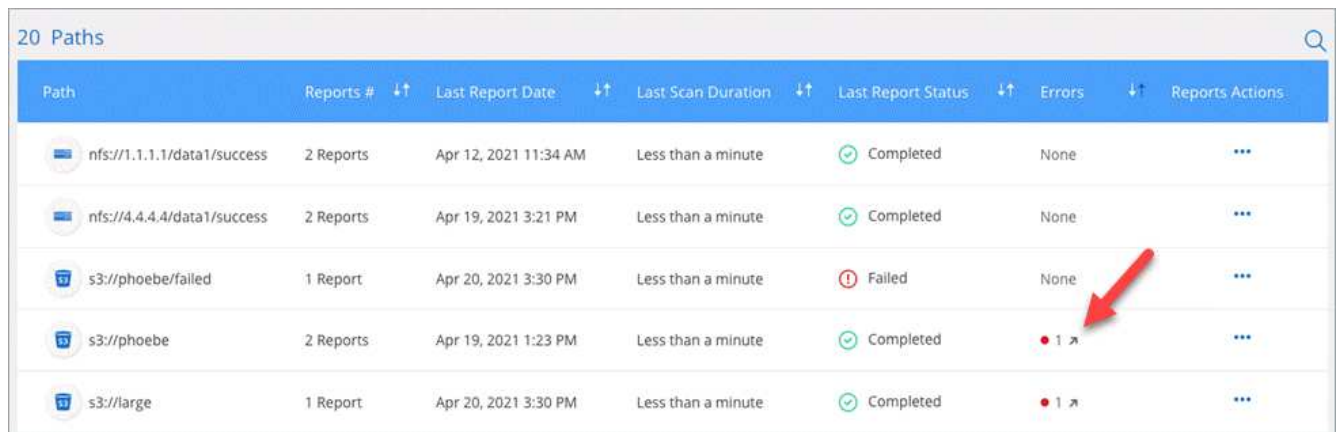
La tabla de rutas de acceso identifica si hay algún error en el informe más reciente. Un error identifica un problema que Cloud Sync enfrentó al analizar la ruta.

Por ejemplo, un informe puede contener errores de permiso denegado. Este tipo de error puede afectar a la capacidad de Cloud Sync para analizar todo el conjunto de archivos y directorios.

Después de ver la lista de errores, puede abordar los problemas y volver a ejecutar el informe.

Pasos

1. Haga clic en **Sincronizar > Informes**.
2. En la columna **errores**, identifique si hay algún error presente en un informe.
3. Si hay errores, haga clic en la flecha situada junto al número de errores.



Path	Reports #	Last Report Date	Last Scan Duration	Last Report Status	Errors	Reports Actions
nfs://1.1.1.1/data1/success	2 Reports	Apr 12, 2021 11:34 AM	Less than a minute	Completed	None	...
nfs://4.4.4.4/data1/success	2 Reports	Apr 19, 2021 3:21 PM	Less than a minute	Completed	None	...
s3://phoebe/failed	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Failed	None	...
s3://phoebe	2 Reports	Apr 19, 2021 1:23 PM	Less than a minute	Completed	1	...
s3://large	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Completed	1	...

4. Utilice la información del error para corregir el problema.

Después de resolver el problema, el error no debería aparecer la próxima vez que ejecute el informe.

Eliminar informes

Puede eliminar un informe que contenía un error corregido o si el informe está relacionado con una relación de sincronización que ha eliminado.

Pasos

1. Haga clic en **Sincronizar > Informes**.
2. En la columna **acciones de Informes**, haga clic en el menú de acciones de una ruta y seleccione **Eliminar último informe** o **Eliminar todos los informes**.
3. Confirme que desea eliminar el informe o los informes.

Desinstalar el Data broker

Si es necesario, ejecute una secuencia de comandos de desinstalación para eliminar el agente de datos y los paquetes y directorios que se crearon cuando se instaló el agente de datos.

Pasos

1. Inicie sesión en el host de Data broker.
2. Cambiar al directorio de Data broker: `/opt/netapp/databroker`
3. Ejecute los siguientes comandos:

```
chmod +x uninstaller-DataBroker.sh  
./uninstaller-DataBroker.sh
```

4. Pulse 'y' para confirmar la desinstalación.

Información de copyright

Copyright © 2023 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.