



Documentación de Cloud Sync

Cloud Sync

NetApp
March 09, 2023

This PDF was generated from <https://docs.netapp.com/es-es/cloud-manager-sync/index.html> on March 09, 2023. Always check docs.netapp.com for the latest.

Tabla de Contenido

- Documentación de Cloud Sync 1
- Notas de la versión. 2
 - Novedades de Cloud Sync. 2
 - Limitaciones 19
- Manos a la obra 20
 - Información general de Cloud Sync 20
 - Inicio rápido de Cloud Sync 22
 - Relaciones de sincronización compatibles 23
 - Preparar el origen y el destino 31
 - Información general sobre redes para Cloud Sync 38
 - Instalar un agente de datos 41
- Utilice Cloud Sync 59
 - Sincronice datos entre un origen y un destino 59
 - Pago de las relaciones de sincronización después de que finalice su prueba gratuita 78
 - Gestión de relaciones de sincronización 80
 - Administrar grupos de agentes de datos 87
 - Creación y visualización de informes para ajustar la configuración 94
 - Desinstalar el Data broker 97
- API de Cloud Sync 99
 - Primeros pasos 99
 - Referencia de API 100
 - Uso de list API 100
- Conceptos 103
 - Información general sobre las licencias 103
 - Privacidad de datos 104
 - Preguntas técnicas frecuentes sobre Cloud Sync 104
- Conocimiento y apoyo 112
 - Regístrese para recibir soporte 112
 - Obtenga ayuda 116
- Avisos legales 122
 - Derechos de autor 122
 - Marcas comerciales 122
 - Estadounidenses 122
 - Política de privacidad 122
 - Código abierto 122

Documentación de Cloud Sync

Notas de la versión

Novedades de Cloud Sync

Descubra las novedades de Cloud Sync.

7 de marzo de 2023

Cifrado EBS para agentes de datos de AWS

Ahora puede cifrar volúmenes de agentes de datos de AWS mediante una clave KMS desde su cuenta.

["Obtenga más información sobre cómo crear un agente de datos en AWS".](#)

5 de febrero de 2023

Compatibilidad adicional para Azure Data Lake Storage Gen2, almacenamiento ONTAP S3 y NFS

Cloud Sync ahora admite relaciones de sincronización adicionales para el almacenamiento ONTAP S3 y NFS:

- Almacenamiento ONTAP S3 en NFS
- NFS a almacenamiento de ONTAP S3

Cloud Sync también ofrece compatibilidad adicional para el almacenamiento en lagos de datos Azure Gen2 como origen y destino para:

- Servidor NFS
- Servidor SMB
- Almacenamiento ONTAP S3
- StorageGRID
- Almacenamiento de objetos en cloud de IBM

["Obtenga más información sobre las relaciones de sincronización compatibles".](#)

Actualice al sistema operativo de Amazon Web Services Data broker

El sistema operativo para los agentes de datos de AWS se ha actualizado a Amazon Linux 2022.

["Obtenga más información acerca de la instancia de data broker en AWS".](#)

3 de enero de 2023

Muestra la configuración local de Data broker en la interfaz de usuario

Ahora existe una opción **Mostrar configuración** que permite a los usuarios ver la configuración local de cada Data broker en la interfaz de usuario.

["Obtenga más información sobre la administración de grupos de agentes de datos".](#)

Actualice a Azure y el sistema operativo de agentes de datos Google Cloud

El sistema operativo para los agentes de datos en Azure y Google Cloud se ha actualizado a Rocky Linux 9.0.

["Obtenga más información acerca de la instancia de data broker en Azure".](#)

["Obtenga más información acerca de la instancia de Data broker en Google Cloud".](#)

11 de diciembre de 2022

Filtrar directorios por nombre

Ahora hay disponible una nueva configuración de **excluir nombres de directorio** para las relaciones de sincronización. Los usuarios pueden filtrar un máximo de 15 nombres de directorio desde su sincronización. Los directorios .copy-fload, .snapshot, ~snapshot se excluyen de forma predeterminada.

["Obtenga más información acerca del valor excluir nombres de directorio".](#)

Compatibilidad adicional con Amazon S3 y ONTAP S3 Storage

Cloud Sync ahora admite relaciones de sincronización adicionales para AWS S3 y el almacenamiento de ONTAP S3:

- AWS S3 a almacenamiento ONTAP S3
- Almacenamiento ONTAP S3 en AWS S3

["Obtenga más información sobre las relaciones de sincronización compatibles".](#)

30 de octubre de 2022

Sincronización continua desde Microsoft Azure

La configuración de Continuous Sync ahora es compatible desde un bucket de almacenamiento de Azure de origen a un almacenamiento en cloud mediante un agente de datos de Azure.

Después de la sincronización inicial de datos, Cloud Sync escucha los cambios en el bloque de almacenamiento de Azure de origen y sincroniza constantemente los cambios en el destino a medida que se producen. Esta configuración está disponible cuando se sincroniza desde un bucket de almacenamiento de Azure con almacenamiento Azure Blob, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS y StorageGRID.

El agente de datos de Azure necesita un rol personalizado y los siguientes permisos para utilizar este ajuste:

```
'Microsoft.Storage/storageAccounts/read',  
'Microsoft.EventGrid/systemTopics/eventSubscriptions/write',  
'Microsoft.EventGrid/systemTopics/eventSubscriptions/read',  
'Microsoft.EventGrid/systemTopics/eventSubscriptions/delete',  
'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action',  
'Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes  
/action',  
'Microsoft.EventGrid/systemTopics/read',  
'Microsoft.EventGrid/systemTopics/write',  
'Microsoft.EventGrid/systemTopics/delete',  
'Microsoft.EventGrid/eventSubscriptions/write',  
'Microsoft.Storage/storageAccounts/write'
```

["Obtenga más información acerca de la configuración de sincronización continua".](#)

4 de septiembre de 2022

Compatibilidad adicional con Google Drive

- Cloud Sync ahora admite relaciones de sincronización adicionales para Google Drive:
 - Google Drive a servidores NFS
 - Google Drive a servidores SMB
- También puede generar informes para relaciones de sincronización que incluyan Google Drive.

["Obtenga más información acerca de los informes".](#)

Mejora de sincronización continua

Ahora puede activar la configuración de sincronización continua en los siguientes tipos de relaciones de sincronización:

- Bloque de S3 a un servidor NFS
- Google Cloud Storage en un servidor NFS

["Obtenga más información acerca de la configuración de sincronización continua".](#)

Notificaciones por correo electrónico

Ahora puede recibir notificaciones Cloud Sync por correo electrónico.

Para recibir las notificaciones por correo electrónico, deberá activar la configuración de **Notificaciones** en la relación de sincronización y, a continuación, configurar las alertas y notificaciones en BlueXP.

["Aprenda a configurar notificaciones".](#)

31 de julio de 2022

Unidad de Google

Ahora puede sincronizar datos de un servidor NFS o SMB en Google Drive. Tanto "My Drive" como "Shared Drives" son compatibles como destinos.

Antes de crear una relación de sincronización que incluya Google Drive, debe configurar una cuenta de servicio que tenga los permisos necesarios y una clave privada. ["Más información acerca de los requisitos de Google Drive"](#).

["Consulte la lista de relaciones de sincronización compatibles"](#).

Compatibilidad adicional con Azure Data Lake

Cloud Sync ahora admite relaciones de sincronización adicionales para el almacenamiento en lagos de datos de Azure Gen2:

- Amazon S3 a Azure Data Lake Storage Gen2
- Almacenamiento de objetos en cloud de IBM a Azure Data Lake Storage Gen2
- Almacenamiento de StorageGRID a Azure Data Lake Gen2

["Consulte la lista de relaciones de sincronización compatibles"](#).

Nuevas formas de configurar relaciones de sincronización

Hemos añadido formas adicionales de configurar relaciones de sincronización directamente desde el lienzo de BlueXP.

Arrastre y suelte

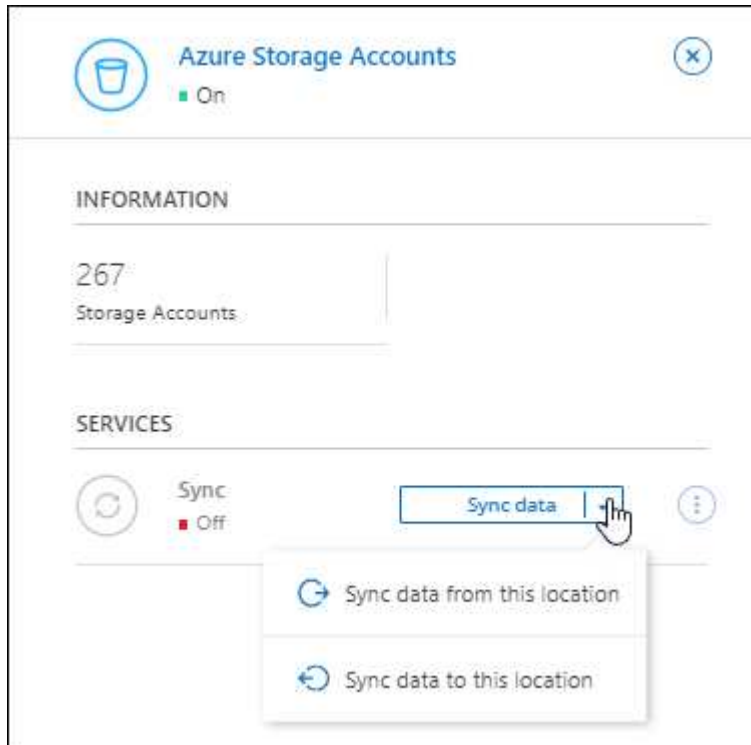
Ahora puede configurar una relación de sincronización desde el lienzo arrastrando y soltando un entorno de trabajo sobre otro.



Configuración del panel derecho

Ahora puede configurar una relación de sincronización para el almacenamiento de Azure Blob o para Google Cloud Storage seleccionando el entorno de trabajo en Canvas y seleccionando la opción de sincronización en

el panel derecho.



3 de julio de 2022

Compatibilidad con Azure Data Lake Storage Gen2

Ahora puede sincronizar datos de un servidor NFS o SMB en Azure Data Lake Storage Gen2.

Al crear una relación de sincronización que incluya el lago de datos de Azure, debe proporcionar a Cloud Sync la cadena de conexión de la cuenta de almacenamiento. Debe ser una cadena de conexión normal, no una firma de acceso compartido (SAS).

["Consulte la lista de relaciones de sincronización compatibles".](#)

Sincronización continua desde Google Cloud Storage

La configuración de Continuous Sync ahora es compatible con un bucket de Google Cloud Storage origen con un destino de almacenamiento en cloud.

Después de la sincronización inicial de datos, Cloud Sync escucha los cambios en el bucket de Google Cloud Storage de origen y sincroniza continuamente los cambios en el destino a medida que se producen. Esta configuración está disponible cuando se sincroniza un bucket de Google Cloud Storage con S3, Google Cloud Storage, un almacenamiento blob de Azure, StorageGRID o IBM Storage.

La cuenta de servicio asociada con el agente de datos necesita los siguientes permisos para utilizar esta configuración:


```
- pubsub.subscriptions.consume
- pubsub.subscriptions.create
- pubsub.subscriptions.delete
- pubsub.subscriptions.list
- pubsub.topics.attachSubscription
- pubsub.topics.create
- pubsub.topics.delete
- pubsub.topics.list
- pubsub.topics.setIamPolicy
- storage.buckets.update
```

["Obtenga más información acerca de la configuración de sincronización continua".](#)

Nueva compatibilidad regional con Google Cloud

El agente de datos de Cloud Sync ahora es compatible con las siguientes regiones de Google Cloud:

- Colón (EE. UU.-este 5)
- Dallas (EE.UU.-sur-1)
- Madrid (europa-sur-oeste)
- Milán (europa-west8)
- París (europa-West9)

Nuevo tipo de máquina de Google Cloud

El tipo de máquina predeterminado para el agente de datos en Google Cloud es ahora n2-standard-4.

6 de junio de 2022

Sincronización continua

Una nueva configuración le permite sincronizar continuamente cambios de un bloque de S3 de origen a un destino.

Después de la sincronización inicial de datos, Cloud Sync escucha los cambios en el bloque de S3 de origen y sincroniza constantemente 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 sincroniza desde un bloque de S3 con S3, Google Cloud Storage, un almacenamiento blob de Azure, StorageGRID o IBM Storage.

Tenga en cuenta que la función IAM asociada con el agente de datos necesitará los siguientes permisos para utilizar esta configuración:

```
"s3:GetBucketNotification",
"s3:PutBucketNotification"
```

Estos permisos se agregan automáticamente a los nuevos agentes de datos que cree.

["Obtenga más información acerca de la configuración de sincronización continua".](#)

Muestra todos los volúmenes ONTAP

Cuando crea una relación de sincronización, Cloud Sync ahora muestra todos los volúmenes en un sistema Cloud Volumes ONTAP de origen, un clúster ONTAP en las instalaciones o FSX para el sistema de archivos ONTAP.

Anteriormente, Cloud Sync solo mostraría los volúmenes que coincidía con el protocolo seleccionado. Ahora se muestran todos los volúmenes, pero los volúmenes que no coinciden con el protocolo seleccionado o que no tienen un recurso compartido o una exportación se atenúan y no se pueden seleccionar.

Copiando etiquetas a Azure Blob

Cuando crea una relación de sincronización en la que Azure Blob es el destino, Cloud Sync ahora le permite copiar etiquetas en el contenedor de Azure Blob:

- En la página **Ajustes**, puede utilizar el ajuste **Copiar para objetos** para copiar etiquetas del origen al contenedor de Azure Blob. Esto se suma a copiar metadatos.
- En la página **Etiquetas/metadatos**, puede especificar códigos de índice blob para establecer en los objetos que se copian en el contenedor de Azure Blob. Anteriormente, solo se podían especificar metadatos de relaciones.

Estas opciones son compatibles cuando Azure Blob es el destino y el origen es Azure Blob o un extremo compatible con S3 (S3, StorageGRID o IBM Cloud Object Storage).

1 de mayo de 2022

Tiempo de espera de sincronización

Ahora hay disponible un nuevo valor de tiempo de espera de sincronización* para las relaciones de sincronización. Esta configuración le permite definir si Cloud Sync debe cancelar una sincronización de datos si no se ha completado en el número de horas o días especificado.

["Más información sobre cómo cambiar la configuración de una relación de sincronización".](#)

Notificaciones

Ahora hay disponible una nueva configuración de **Notificaciones** para las relaciones de sincronización. Esta configuración 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.



["Más información sobre cómo cambiar la configuración de una relación de sincronización"](#).

3 de abril de 2022

Mejoras del grupo de agentes de datos

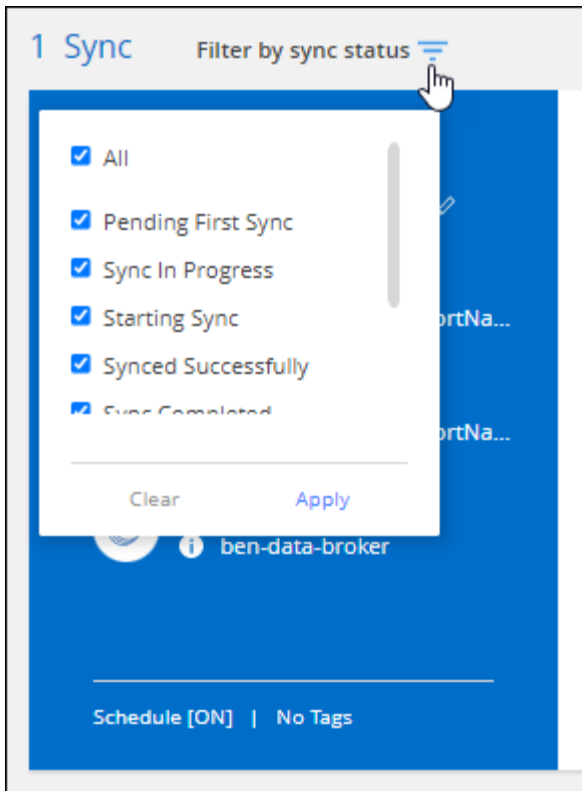
Hemos realizado varias mejoras en los grupos de agentes de datos:

- Ahora puede mover un agente de datos a un grupo nuevo o existente.
- Ahora puede actualizar la configuración del proxy de un agente de datos.
- Por último, también puede eliminar grupos de agentes de datos.

["Descubra cómo gestionar los grupos de agentes de datos"](#).

Filtro del tablero de a bordo

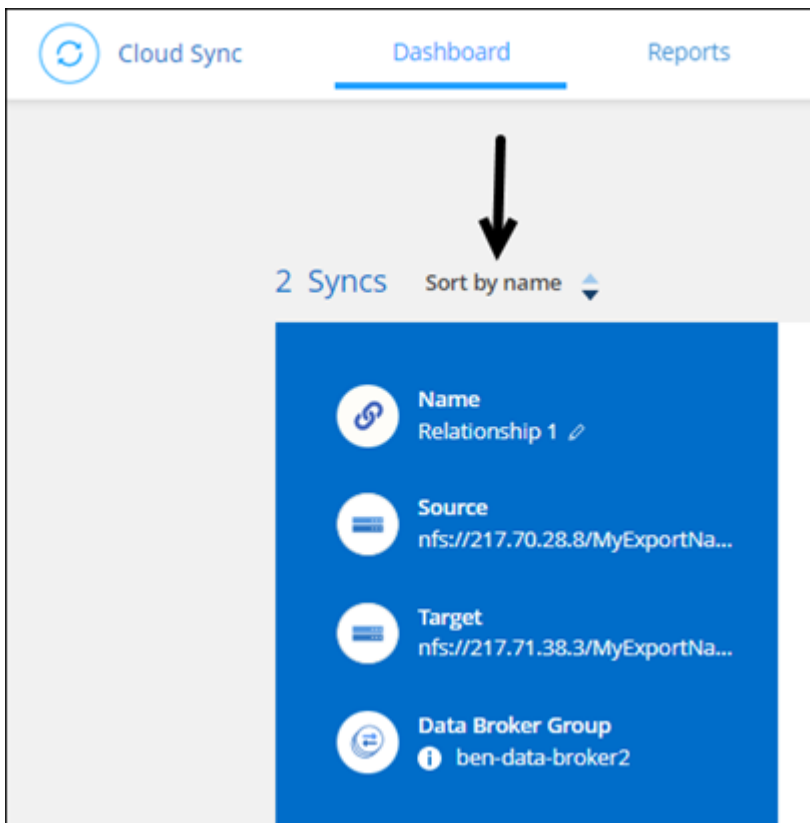
Ahora puede filtrar el contenido de la consola de sincronización para buscar fácilmente relaciones de sincronización que se ajusten a un estado determinado. Por ejemplo, puede filtrar las relaciones de sincronización que tengan un estado de error



3 de marzo de 2022

Ordenación en el tablero de a bordo

Ahora ordena el panel por nombre de relación de sincronización.



Mejora de la integración de Data Sense

En la versión anterior, presentamos la integración de Cloud Sync con Cloud Data Sense. En esta actualización, mejoramos la integración facilitando la creación de la relación de sincronización. 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.

The screenshot shows the 'Selected Data Sense Source' configuration screen. At the top, there is a progress bar with four steps: 1. Data Sense Integration (active), 2. Data Broker Group, 3. NFS Server, and 4. Directory. Below the progress bar, there is a 'How does it work?' link. The main content area displays the selected source details in a table-like format:

Azure NetApp Files	/cifs1 Source	1.1.1.1 Host	cifs Working Environment	\\1.1.1.1\\cifs1 Volume
--------------------	------------------	-----------------	-----------------------------	----------------------------

Below the table, there is a heading 'A few more things before we continue' and a section 'Define SMB Credentials:' with three input fields: 'User Name', 'Password', and 'Domain (Optional)'.

6 de febrero de 2022

Mejora a los grupos de agentes de datos

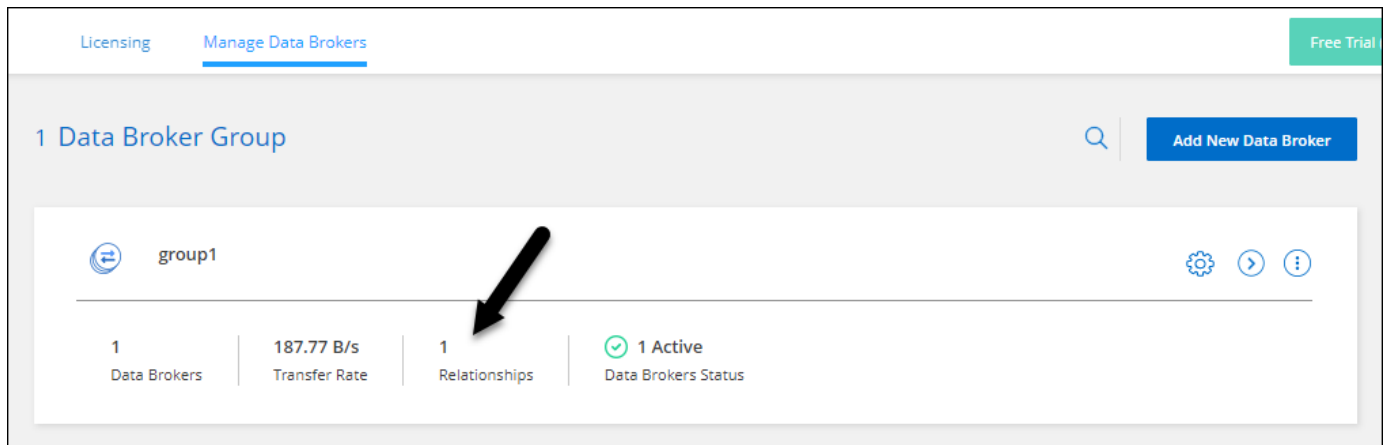
Hemos cambiado la forma en que interactúa con los agentes de datos haciendo hincapié en data broker groups.

Por ejemplo, cuando crea una nueva relación de sincronización, selecciona el intermediario de datos *group* que se va a utilizar con la relación, en lugar de un intermediario de datos específico.

The screenshot shows the 'Select a Data Broker Group' configuration screen. At the top, there is a progress bar with four steps: 1. SMB Server, 2. Data Broker Group (active), 3. Shares, and 4. Target SMB Server. Below the progress bar, there is a 'How does it work?' link. The main content area displays the selected group details in a table-like format:

group1	1 Data Brokers	928.43 B/s Transfer Rate	0 Relationships	1 Active Data Brokers Status
--------	-------------------	-----------------------------	--------------------	---------------------------------

En la pestaña **gestionar agentes de datos**, también se muestra el número de relaciones de sincronización que administra un grupo de Data broker.



Descargar informes en PDF

Ahora puede descargar el PDF de un informe.

["Obtenga más información acerca de los informes".](#)

2 de enero de 2022

Nuevas relaciones de sincronización de Box

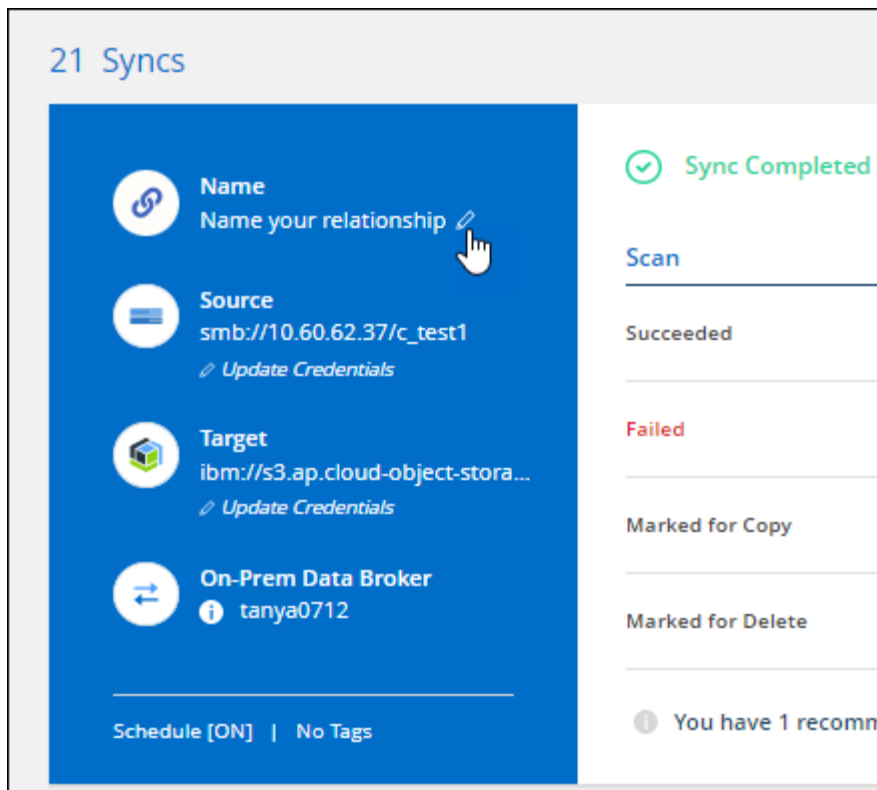
Se admiten dos nuevas relaciones de sincronización:

- Del buzón a Azure NetApp Files
- Box to Amazon FSX for ONTAP

["Consulte la lista de relaciones de sincronización compatibles".](#)

Nombres de las relaciones

Ahora puede proporcionar un nombre significativo a cada una de sus relaciones de sincronización para identificar más fácilmente el propósito de cada relación. Puede agregar el nombre al crear la relación y en cualquier momento después.



Enlaces privados S3

Al sincronizar datos con o desde Amazon S3, puede elegir si desea usar un enlace privado de S3. Cuando el agente de datos copia datos del origen al destino, pasa por el enlace privado.

Tenga en cuenta que la función IAM asociada con el agente de datos necesitará el siguiente permiso para utilizar esta función:

```
"ec2:DescribeVpcEndpoints"
```

Este permiso se agrega automáticamente a los nuevos agentes de datos que cree.

Recuperación instantánea de Glacier

Ahora puede elegir la clase de almacenamiento *Glacier Instant Retrieval* cuando Amazon S3 es el destino de una relación de sincronización.

ACL del almacenamiento de objetos para recursos compartidos de SMB

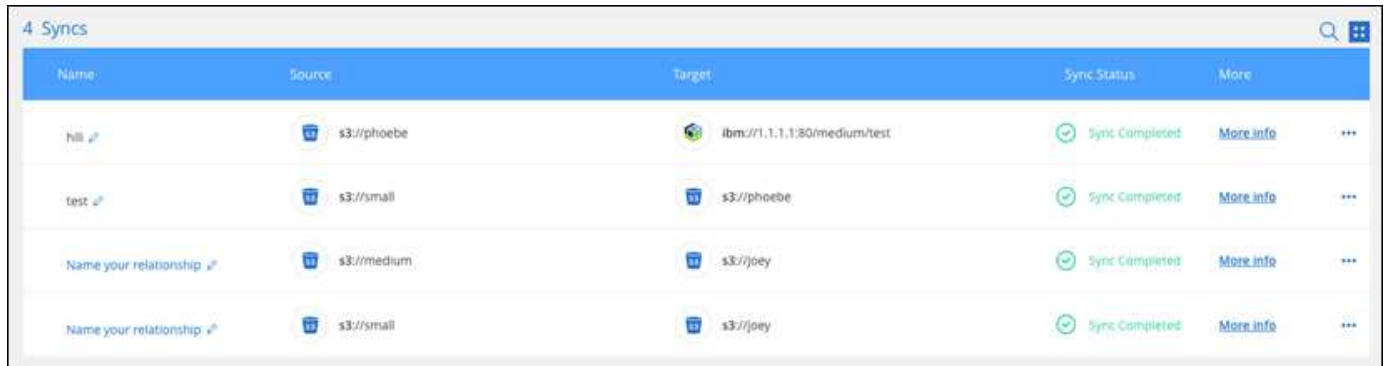
Cloud Sync ahora admite la copia de ACL de almacenamiento de objetos en recursos compartidos de SMB. Antes, solo admitía la copia de ACL de un recurso compartido de SMB a un almacenamiento de objetos.

SFTP a S3

Ahora es posible crear una relación de sincronización desde SFTP a Amazon S3 en la interfaz de usuario. Esta relación de sincronización se admitía previamente con la API únicamente.

Mejora de la vista de tabla

Hemos rediseñado la vista de tabla de la Consola para facilitar su uso. Si hace clic en **más información**, Cloud Sync filtra el panel para mostrar más información acerca de esa relación específica.



Name	Source	Target	Sync Status	More
hll	s3://phoebe	ibmc//1.1.1.1:80/medium/test	Sync Completed	More info
test	s3://small	s3://phoebe	Sync Completed	More info
Name your relationship	s3://medium	s3://joey	Sync Completed	More info
Name your relationship	s3://small	s3://joey	Sync Completed	More info

Apoyo para la región de Jarkarta

Cloud Sync ahora da soporte a la puesta en marcha de un agente de datos en la región del Pacífico asiático de AWS (Yakarta).

28 de noviembre de 2021

ACL de SMB para el almacenamiento de objetos

Ahora, Cloud Sync puede copiar listas de control de acceso (ACL) al configurar una relación de sincronización desde un recurso compartido de SMB de origen al almacenamiento de objetos (excepto ONTAP S3).

Cloud Sync no admite la copia de ACL de almacenamiento de objetos en recursos compartidos de SMB.

["Aprenda a copiar ACL de un recurso compartido de SMB"](#).

Actualice las licencias

Ahora puede actualizar las licencias de Cloud Sync que ha ampliado.

Si ha ampliado una licencia de Cloud Sync que ha comprado a NetApp, puede volver a añadir la licencia para actualizar la fecha de vencimiento.

["Aprenda a actualizar una licencia"](#).

Actualizar credenciales de Box

Ahora puede actualizar las credenciales de Box para una relación de sincronización existente.

["Aprenda a actualizar las credenciales"](#).

31 de octubre de 2021

Soporte de la caja

La compatibilidad con cajas ya está disponible en la interfaz de usuario de Cloud Sync como vista previa.

El cuadro puede ser el origen o el destino en varios tipos de relaciones de sincronización. ["Consulte la lista de](#)

[relaciones de sincronización compatibles](#)".

Configuración de fecha de creación

Cuando un servidor SMB es el origen, una nueva configuración de relación de sincronización denominada *Date Created* le permite sincronizar los archivos que se crearon después de una fecha específica, antes de una fecha específica o entre un intervalo de tiempo específico.

["Más información acerca de los ajustes de Cloud Sync"](#).

4 de octubre de 2021

Soporte adicional de Box

Cloud Sync ahora admite relaciones de sincronización adicionales para ["Caja"](#) Cuando se utiliza la API de Cloud Sync:

- Amazon S3 to Box
- Almacenamiento de objetos en cloud IBM a Box
- StorageGRID a caja
- Box to an NFS Server
- De un servidor SMB

["Aprenda a configurar una relación de sincronización con la API de"](#).

Informes para rutas SFTP

Ahora puede hacerlo ["cree un informe"](#) Para rutas SFTP.

2 de septiembre de 2021

Compatibilidad con FSX para ONTAP

Ahora puede sincronizar datos con o desde un sistema de archivos Amazon FSX para ONTAP.

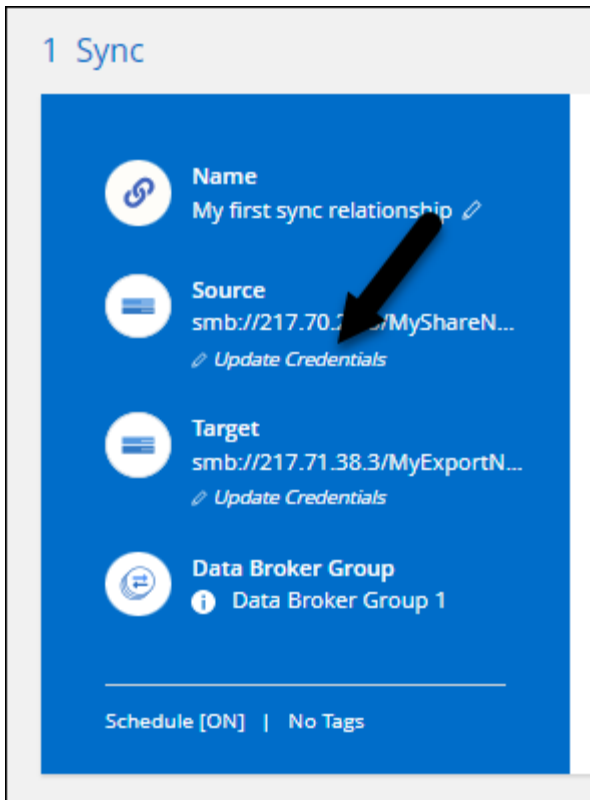
- ["Obtenga más información sobre Amazon FSX para ONTAP"](#)
- ["Consulte las relaciones de sincronización compatibles"](#)
- ["Aprenda a crear una relación de sincronización para Amazon FSX para ONTAP"](#)

1 de agosto de 2021

Actualizar las credenciales

Cloud Sync ahora le permite actualizar el agente de datos con las últimas credenciales del origen o destino en una relación de sincronización existente.

Esta mejora puede ayudar si sus políticas de seguridad requieren que actualice las credenciales de forma periódica. ["Aprenda a actualizar las credenciales"](#).



Etiquetas para destinos de almacenamiento de objetos

Al crear una relación de sincronización, ahora puede añadir etiquetas al destino de almacenamiento de objetos en una relación de sincronización.

Amazon S3, Azure Blob, Google Cloud Storage, IBM Cloud Object Storage y StorageGRID admiten la adición de etiquetas.

Soporte para Box

Cloud Sync ahora es compatible "Caja" Como origen en una relación de sincronización con Amazon S3, StorageGRID e IBM Cloud Object Storage cuando se usa la API de Cloud Sync.

["Aprenda a configurar una relación de sincronización con la API de".](#)

IP pública para agente de datos en Google Cloud

Al implementar un agente de datos en Google Cloud, ahora puede elegir si desea habilitar o deshabilitar una dirección IP pública para la instancia de la máquina virtual.

["Descubra cómo implementar un agente de datos en Google Cloud".](#)

Volumen de protocolo doble para Azure NetApp Files

Cuando elige el volumen de origen o de destino para Azure NetApp Files, Cloud Sync ahora muestra un volumen de doble protocolo independientemente del protocolo que elija para la relación de sincronización.

7 de julio de 2021

ONTAP S3 Storage y Google Cloud Storage

Cloud Sync ahora admite relaciones de sincronización entre el almacenamiento de ONTAP S3 y un bloque de Google Cloud Storage en la interfaz de usuario.

["Consulte la lista de relaciones de sincronización compatibles".](#)

Etiquetas de metadatos de objetos

Cloud Sync ahora puede copiar metadatos de objetos y etiquetas entre almacenamiento basado en objetos al crear una relación de sincronización y habilitar una configuración.

["Obtenga más información sobre el valor Copiar para objetos".](#)

Apoyo a HashiCorp Vaults

Ahora puede configurar el agente de datos para acceder a las credenciales desde un almacén HashiCorp externo mediante la autenticación con una cuenta de servicio de Google Cloud.

["Más información sobre el uso de un almacén de HashiCorp con un agente de datos".](#)

Defina etiquetas o metadatos para bloque de S3

Al configurar una relación de sincronización con un bloque de Amazon S3, el asistente de relación de sincronización ahora le permite definir las etiquetas o los metadatos que desea guardar en los objetos del bloque de S3 de destino.

La opción de etiquetado anteriormente formaba parte de la configuración de la relación de sincronización.

7 de junio de 2021

Clases de almacenamiento en Google Cloud

Cuando un bloque de Google Cloud Storage es el destino de una relación de sincronización, ahora puede elegir la clase de almacenamiento que desee utilizar. Cloud Sync admite las siguientes clases de almacenamiento:

- Estándar

- Nearline
- Coldline
- Archivado

2 de mayo de 2021

Errores en los informes

Ahora puede ver los errores encontrados en los informes y eliminar el último informe o todos los informes.

["Obtenga más información sobre la creación y visualización de informes para ajustar su configuración"](#).

Comparar atributos

Ahora hay disponible una nueva configuración de **Comparar por** para cada relación de sincronización.

Esta configuración avanzada le permite elegir si Cloud Sync debe comparar ciertos atributos al determinar si un archivo o directorio ha cambiado y debe volver a sincronizarse.

["Más información sobre cómo cambiar la configuración de una relación de sincronización"](#).

11 de abril de 2021

Se retira el servicio independiente de Cloud Sync

Se ha retirado el servicio independiente de Cloud Sync. Ahora debería acceder a Cloud Sync directamente desde BlueXP, donde están disponibles todas las mismas funciones.

Después de iniciar sesión en BlueXP, puede cambiar a la ficha Sincronizar en la parte superior y ver sus relaciones, como antes.

Cubos de Google Cloud en diferentes proyectos

Al configurar una relación de sincronización, puede elegir entre bloques de Google Cloud en diferentes proyectos si proporciona los permisos necesarios para la cuenta de servicio del agente de datos.

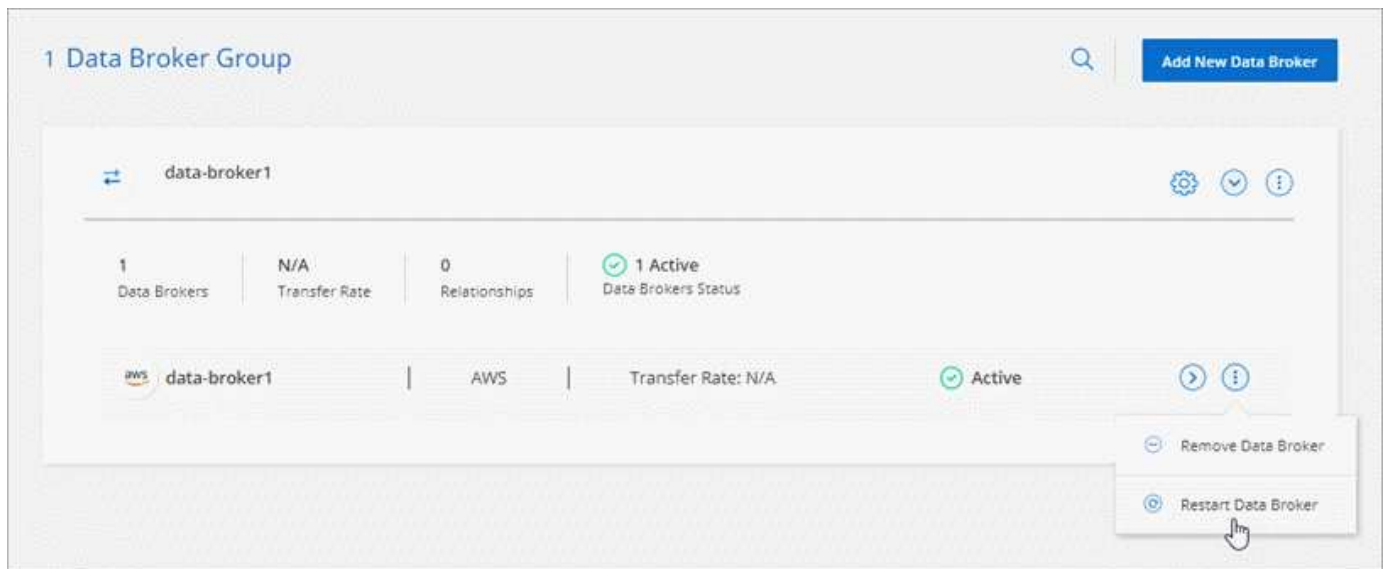
["Aprenda a configurar la cuenta de servicio"](#).

Metadatos entre Google Cloud Storage y S3

Cloud Sync ahora copia metadatos entre Google Cloud Storage y los proveedores S3 (AWS S3, StorageGRID y IBM Cloud Object Storage).

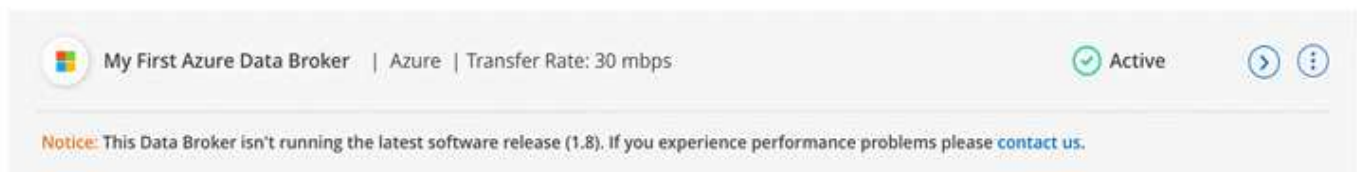
Reinicie los agentes de datos

Ahora puede reiniciar un agente de datos desde Cloud Sync.



Mensaje cuando no esté ejecutando la versión más reciente

Cloud Sync Now identifica cuándo un agente de datos no ejecuta la última versión del software. Este mensaje puede ayudarle a asegurarse de que recibe las últimas características y funcionalidades.



Limitaciones

Las limitaciones conocidas identifican plataformas, dispositivos o funciones que no son compatibles con esta versión del producto o cuya interoperabilidad con esta no es óptima. Revise estas limitaciones detenidamente.

Cloud Sync no se admite en las siguientes regiones:

- Regiones gubernamentales de AWS
- Regiones gubernamentales de Azure
- China

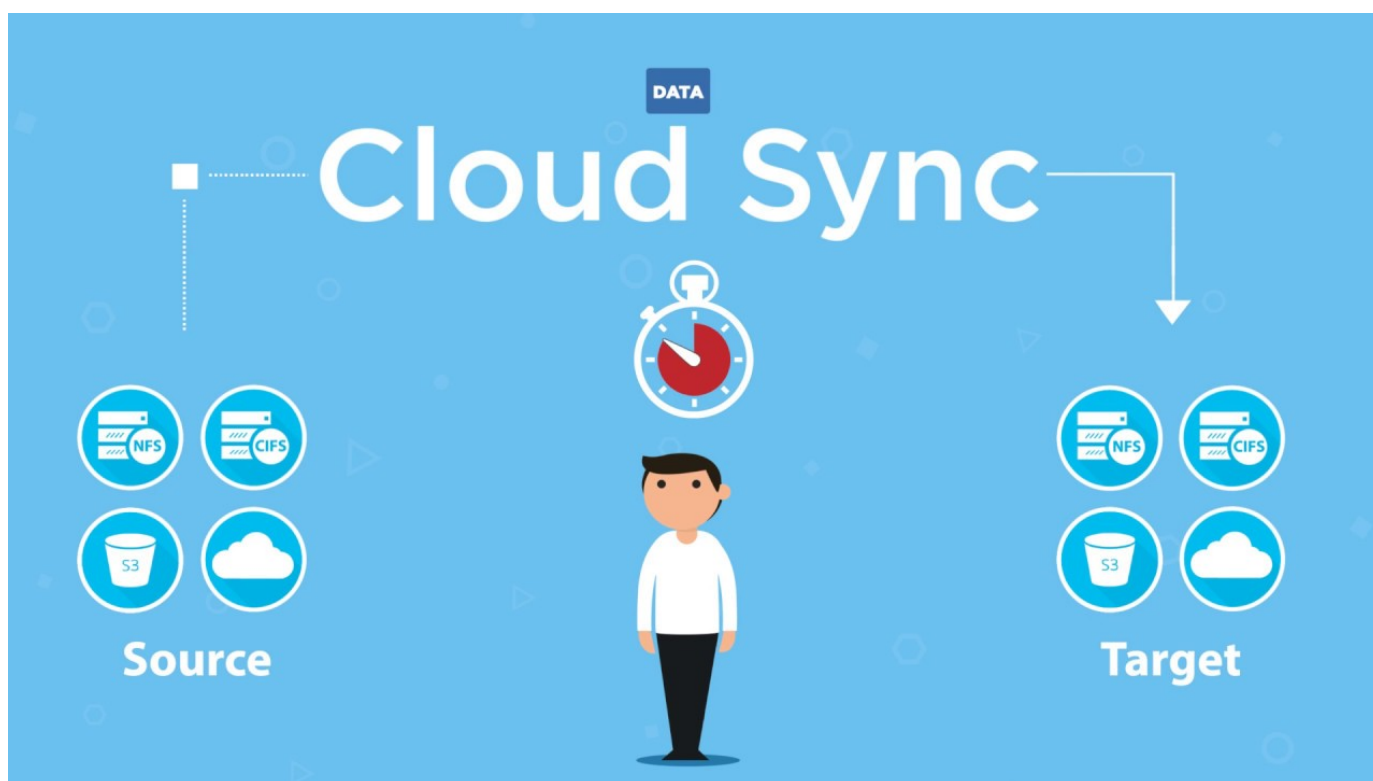
Manos a la obra

Información general de Cloud Sync

El servicio Cloud Sync de NetApp ofrece una forma sencilla, segura y automatizada de migrar sus datos a cualquier destino, tanto en el cloud como en las instalaciones. Tanto si se trata de un conjunto de datos NAS basado en archivos (NFS o SMB), un formato de objeto Amazon simple Storage Service (S3), un dispositivo StorageGRID® de NetApp o cualquier otro almacén de objetos de proveedores de cloud, Cloud Sync puede convertirlo y moverlo por usted.

Funciones

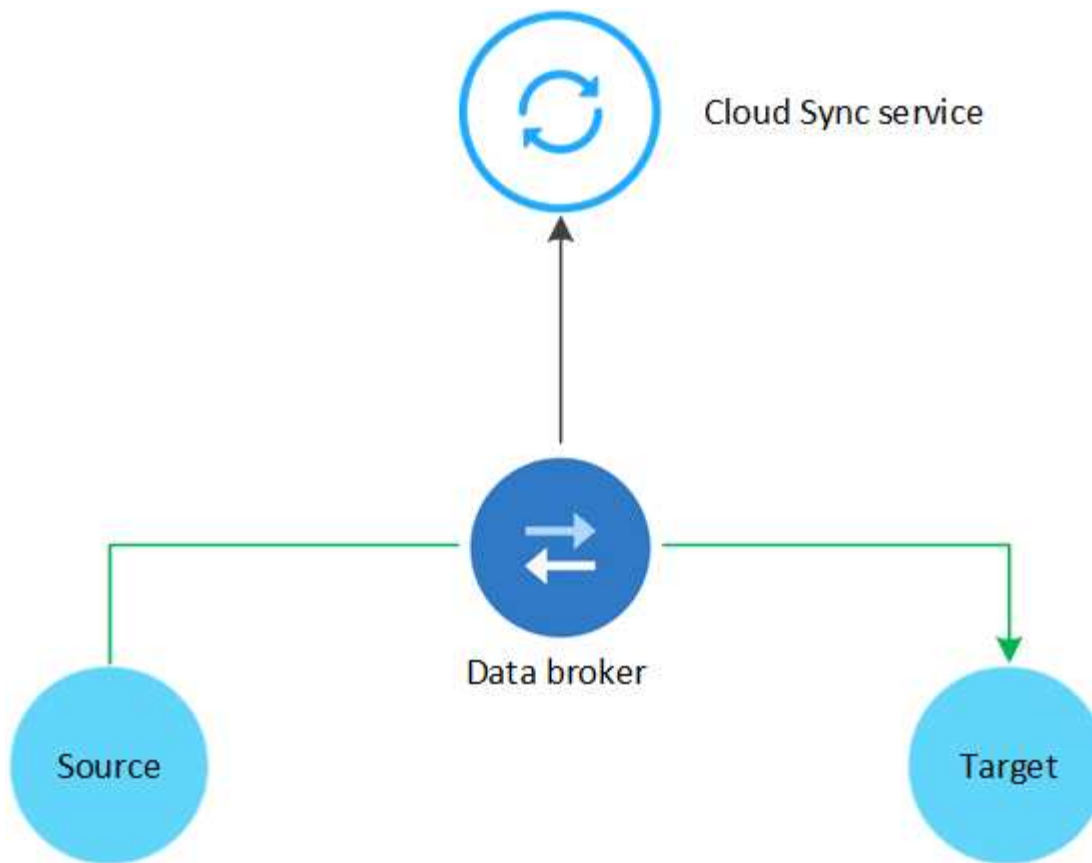
Vea el siguiente vídeo para obtener información general sobre Cloud Sync:



Cómo funciona Cloud Sync

Cloud Sync es una plataforma de software como servicio (SaaS) que consta de un grupo de agentes de datos, una interfaz basada en cloud disponible a través de BlueXP y una fuente y un destino.

En la siguiente imagen, se muestra la relación entre los componentes de Cloud Sync:



El software de agente de datos de NetApp sincroniza los datos de un origen con un destino (lo que se denomina *Sync Relationship*). Puede ejecutar el agente de datos en AWS, Azure, Google Cloud Platform o en sus instalaciones. Un grupo de agentes de datos, que consta de uno o más agentes de datos, necesita una conexión a Internet saliente a través del puerto 443 para poder comunicarse con el servicio Cloud Sync y ponerse en contacto con otros servicios y repositorios. ["Consulte la lista de extremos"](#).

Después de la copia inicial, el servicio sincroniza los datos modificados con la programación que se haya establecido.

Tipos de almacenamiento admitidos

Cloud Sync admite los siguientes tipos de almacenamiento:

- Cualquier servidor NFS
- Cualquier servidor SMB
- Amazon EFS
- Amazon FSX para ONTAP
- Amazon S3
- Azure Blob
- Azure Data Lake Storage Gen2
- Azure NetApp Files
- Cuadro (disponible como vista previa)
- Cloud Volumes Service

- Cloud Volumes ONTAP
- Google Cloud Storage
- Unidad de Google
- Almacenamiento de objetos en cloud de IBM
- Clúster de ONTAP en las instalaciones
- Almacenamiento ONTAP S3
- SFTP (solo con API)
- StorageGRID

["Consulte las relaciones de sincronización compatibles"](#).

Externa

Existen dos tipos de costes asociados con el uso de Cloud Sync: Cargos por recursos y cargos por servicios.

Cargos por recursos

Las cargas de recursos están relacionadas con los costes de computación y almacenamiento para ejecutar uno o más agentes de datos en el cloud.

Cargos por servicio

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, lo que permite pagar por horas o anualmente. La segunda opción consiste en comprar licencias directamente a NetApp.

["Descubra cómo funciona la licencia"](#).

Inicio rápido de Cloud Sync

Primeros pasos en el servicio Cloud Sync incluyen algunos pasos.



Inicie sesión y configure BlueXP

Debería haber comenzado con BlueXP, que incluye el inicio de sesión, la configuración de una cuenta y posiblemente la implementación de un conector y la creación de entornos de trabajo.

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

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

Se requiere un conector para Cloud Volumes ONTAP, clústeres de ONTAP en las instalaciones y Amazon FSX para ONTAP.

- ["Aprenda a comenzar con BlueXP"](#)

- ["Más información sobre conectores"](#)

2

Prepare el origen y el destino

Compruebe que el origen y el destino son compatibles y están configurados. El requisito más importante es verificar la conectividad entre el grupo de agentes de datos y las ubicaciones de origen y destino.

- ["Consulte las relaciones admitidas"](#)
- ["Preparar el origen y el destino"](#)

3

Prepare una ubicación para el agente de datos de NetApp

El software de agente de datos de NetApp sincroniza los datos de un origen con un destino (lo que se denomina *Sync Relationship*). Puede ejecutar el agente de datos en AWS, Azure, Google Cloud Platform o en sus instalaciones. Un grupo de agentes de datos, que consta de uno o más agentes de datos, necesita una conexión a Internet saliente a través del puerto 443 para poder comunicarse con el servicio Cloud Sync y ponerse en contacto con otros servicios y repositorios. ["Consulte la lista de extremos"](#).

Cloud Sync le guía por el proceso de instalación cuando crea una relación de sincronización, en cuyo momento puede implementar un agente de datos en el cloud o descargar un script de instalación para su propio host Linux.

- ["Revise la instalación de AWS"](#)
- ["Revise la instalación de Azure"](#)
- ["Revise la instalación de Google Cloud"](#)
- ["Revise la instalación del host Linux"](#)

4

Cree su primera relación de sincronización

Inicie sesión en ["BlueXP"](#), haga clic en **Sincronizar** y, a continuación, arrastre y suelte las selecciones para el origen y el destino. Siga las indicaciones para completar la configuración. ["Leer más"](#).

5

Pague por sus relaciones de sincronización una vez que finalice su prueba gratuita

Suscríbase a AWS o Azure para pagar según el uso o anualmente. O adquiera licencias directamente a NetApp. Sólo tiene que ir a la página Configuración de licencia de Cloud Sync para configurarlo. ["Leer más"](#).

Relaciones de sincronización compatibles

Cloud Sync le permite sincronizar datos de un origen en un destino. Esto se denomina relación de sincronización. Debe comprender las relaciones admitidas antes de comenzar.

Ubicación de origen	Ubicaciones de destino compatibles
Amazon EFS	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSX para ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID
Amazon FSX para ONTAP	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSX para ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID

Ubicación de origen	Ubicaciones de destino compatibles
Amazon S3	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSX para ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Caja hacia 1 • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID
Azure Blob	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSX para ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID
Azure Data Lake Storage Gen2	<ul style="list-style-type: none"> • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID

Ubicación de origen	Ubicaciones de destino compatibles
Azure NetApp Files	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSX para ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID
Caja hacia 1	<ul style="list-style-type: none"> • Amazon FSX para ONTAP • Amazon S3 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Servidor SMB • StorageGRID
Cloud Volumes ONTAP	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSX para ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID

Ubicación de origen	Ubicaciones de destino compatibles
Cloud Volumes Service	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSX para ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID
Google Cloud Storage	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSX para ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID
Unidad de Google	<ul style="list-style-type: none"> • Servidor NFS • Servidor SMB

Ubicación de origen	Ubicaciones de destino compatibles
Almacenamiento de objetos en cloud de IBM	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSX para ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Caja hacia 1 • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID
Servidor NFS	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSX para ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Unidad de Google • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID

Ubicación de origen	Ubicaciones de destino compatibles
Clúster de ONTAP en las instalaciones	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSX para ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Servidor SMB • StorageGRID
Almacenamiento ONTAP S3	<ul style="list-style-type: none"> • Amazon S3 • Azure Data Lake Storage Gen2 • Google Cloud Storage • Servidor NFS • Servidor SMB • StorageGRID • Almacenamiento ONTAP S3
SFTP HACIA LA SEGUNDA	S3

Ubicación de origen	Ubicaciones de destino compatibles
Servidor SMB	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSX para ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Unidad de Google • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID
StorageGRID	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSX para ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Caja hacia 1 • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • Almacenamiento de objetos en cloud de IBM • Servidor NFS • Clúster de ONTAP en las instalaciones • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID

Notas:

1. La compatibilidad con cajas está disponible como vista previa.

2. Las relaciones de sincronización con este origen/destino se admiten únicamente mediante la API de Cloud Sync.
3. Puede elegir un nivel de almacenamiento específico de Azure Blob cuando un contenedor Blob es el destino:
 - Almacenamiento en caliente
 - Almacenamiento en frío
4. puede elegir una clase de almacenamiento S3 específica cuando Amazon S3 es el destino:
 - Estándar (esta es la clase predeterminada)
 - Organización en niveles inteligente
 - Acceso Estándar-poco frecuente
 - Una Zona de acceso poco frecuente
 - Glacier Deep Archive
 - Recuperación de Glacier flexible
 - Recuperación instantánea de Glacier
5. Puede elegir una clase de almacenamiento específica cuando un bucket de Google Cloud Storage sea el objetivo:
 - Estándar
 - Nearline
 - Coldline
 - Archivado

Preparar el origen y el destino

Compruebe que el origen y los objetivos cumplen los siguientes requisitos.

Redes

- El origen y el destino deben tener una conexión de red con el grupo de Data broker.

Por ejemplo, si un servidor NFS se encuentra en su centro de datos y existe un agente de datos en AWS, necesitará una conexión de red (VPN o Direct Connect) desde su red hasta el VPC.

- NetApp recomienda configurar el origen, el destino y los agentes de datos para que utilicen un servicio de protocolo de tiempo de redes (NTP). La diferencia de tiempo entre los tres componentes no debe superar los 5 minutos.

Directorio de destino

Al crear una relación de sincronización, Cloud Sync le permite seleccionar un directorio de destino existente y, a continuación, crear opcionalmente una nueva carpeta dentro de ese directorio. Así que asegúrese de que su directorio de destino preferido ya existe.

Permisos para leer directorios

Para mostrar todos los directorios o carpetas de un origen o destino, Cloud Sync necesita permisos de lectura

en el directorio o carpeta.

NFS

Los permisos deben definirse en el origen/destino con uid/gid en archivos y directorios.

Almacenamiento de objetos

- Para AWS y Google Cloud, un agente de datos debe tener permisos de objeto de lista (estos permisos se proporcionan de forma predeterminada si sigue los pasos de instalación del agente de datos).
- Para Azure, StorageGRID e IBM, las credenciales introducidas al configurar una relación de sincronización deben tener permisos de objetos de lista.

SMB

Las credenciales de SMB que se introducen al configurar una relación de sincronización deben tener permisos de carpeta de lista.



El agente de datos ignora los siguientes directorios de forma predeterminada: .Snapshot, ~snapshot, .copy-fload

requisitos de bloque de Amazon S3

Asegúrese de que su bloque de Amazon S3 cumple los siguientes requisitos.

Ubicaciones de agentes de datos compatibles para Amazon S3

Las relaciones de sincronización que incluyen el almacenamiento S3 requieren un agente de datos implementado en AWS o en sus instalaciones. En cualquier caso, Cloud Sync le solicita que asocie el agente de datos con una cuenta de AWS durante la instalación.

- ["Descubra cómo implementar el agente de datos de AWS"](#)
- ["Descubra cómo instalar el agente de datos en un Linux host"](#)

Regiones admitidas de AWS

Todas las regiones están soportadas excepto las regiones de China.

Permisos necesarios para bloques de S3 en otras cuentas de AWS

Al configurar una relación de sincronización, puede especificar un bloque de S3 que resida en una cuenta de AWS que no esté asociado a un agente de datos.

["Los permisos incluidos en este archivo JSON"](#) Debe aplicarse a ese bloque de S3 para que un agente de datos pueda acceder a él. Estos permisos permiten al agente de datos copiar datos desde y hacia el bloque y enumerar los objetos del bloque.

Tenga en cuenta lo siguiente acerca de los permisos incluidos en el archivo JSON:


1. *<BucketName>* es el nombre del bloque que reside en la cuenta de AWS que no está asociado a un agente de datos.
2. *<RoleARN>* debe sustituirse por uno de los siguientes:
 - Si se instaló manualmente un agente de datos en un host Linux, *RoleARN* debería ser el ARN del usuario de AWS para el que proporcionó credenciales de AWS al implementar un agente de datos.

- Si se ha implementado un agente de datos en AWS mediante la plantilla CloudFormation, *RoleARN* debería ser el ARN de la función IAM creada por la plantilla.

Para encontrar el rol ARN, vaya a la consola EC2, seleccione la instancia de Data broker y haga clic en el rol IAM en la pestaña Descripción. A continuación, debería ver la página Resumen de la consola del IAM que contiene el rol ARN.

Summary

Delete role

Role ARN `arn:aws:iam::142281742600:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05` 

Role description [Edit](#)

requisitos de almacenamiento de Azure Blob

Asegúrese de que su almacenamiento de Azure Blob cumpla los siguientes requisitos.

Ubicaciones de agentes de datos compatibles para Azure Blob

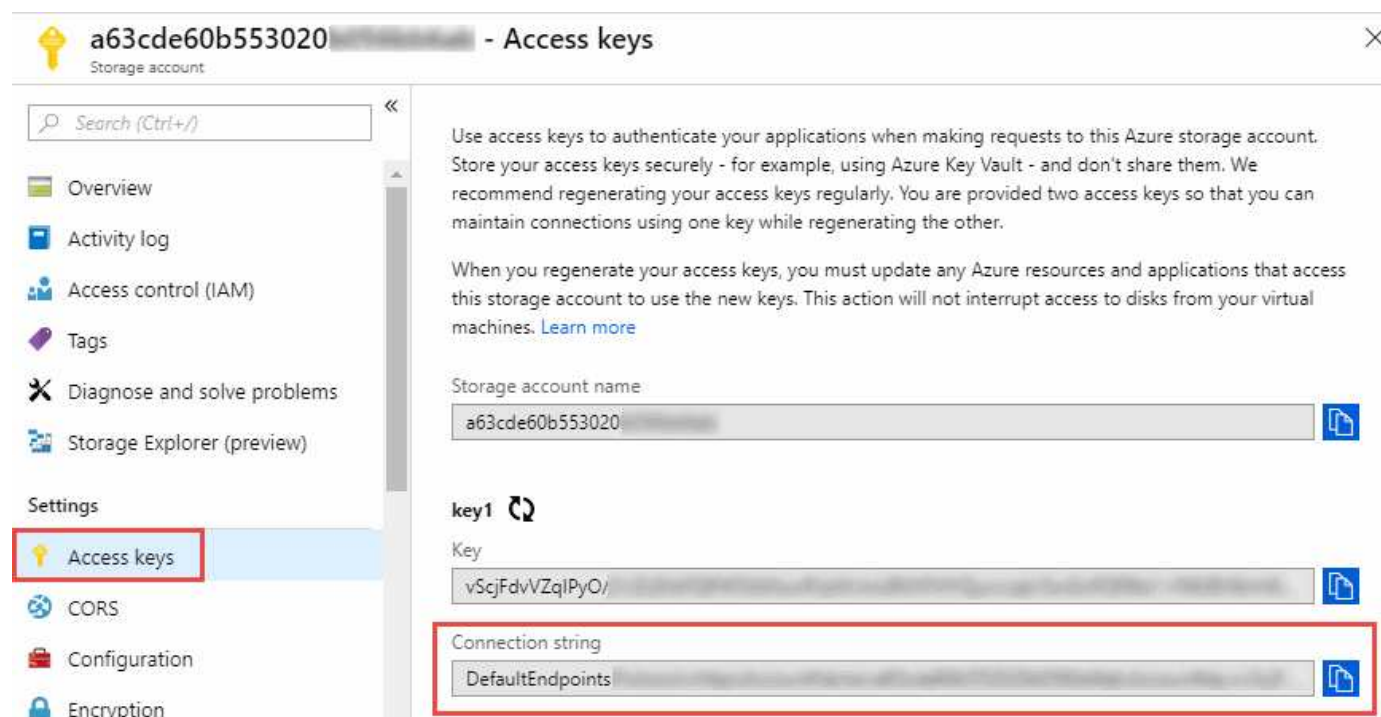
Un agente de datos puede residir en cualquier ubicación cuando una relación de sincronización incluye el almacenamiento de Azure Blob.

Regiones de Azure compatibles

Todas las regiones cuentan con el apoyo de las regiones de China, la gobernadora de los Estados Unidos y el Departamento de Defensa de los Estados Unidos.

Cadena de conexión para relaciones que incluyen Azure Blob y NFS/SMB

A la hora de crear una relación de sincronización entre un contenedor de Azure Blob y un servidor NFS o SMB, debe proporcionar a Cloud Sync la cadena de conexión de la cuenta de almacenamiento:





The screenshot shows the 'Access keys' page for an Azure storage account. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Storage Explorer (preview), Settings, Access keys (highlighted with a red box), CORS, Configuration, and Encryption. The main content area displays instructions on using access keys and provides fields for the storage account name, key1, and connection string. The 'key1' field is also highlighted with a red box. The 'Connection string' field is highlighted with a red box and contains the value 'DefaultEndpoints'.


Access keys


Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to disks from your virtual machines. [Learn more](#)

Storage account name: `a63cde60b553020` 

key1 

Key: `vScjFdvVZqIPyO/` 

Connection string: `DefaultEndpoints` 

Si desea sincronizar datos entre dos contenedores de Azure Blob, la cadena de conexión debe incluir un "firma de acceso compartido" (SAS). También tiene la opción de utilizar un SAS al sincronizar entre un contenedor Blob y un servidor NFS o SMB.

El SAS debe permitir el acceso al servicio Blob y todos los tipos de recursos (Servicio, contenedor y objeto). El SAS también debe incluir los siguientes permisos:

- Para el contenedor de fuente Blob: Leer y enumerar
- Para el contenedor de blob de destino: Leer, escribir, Lista, Agregar y Crear

a63cde60b553020 - Shared access signature

Storage account

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Storage Explorer (preview)

Settings

Access keys

CORS

Configuration

Encryption

Shared access signature

Firewalls and virtual networks

Advanced Threat Protection (pr...

Properties

Locks

Allowed services

☒ Blob ☐ File ☐ Queue ☐ Table

Allowed resource types

☒ Service ☒ Container ☒ Object

Allowed permissions

☒ Read ☒ Write ☒ Delete ☒ List ☒ Add ☒ Create ☐ Update ☐ Process

Start and expiry date/time

Start

2018-10-23 10:07:32 AM

End

2019-10-23 6:07:32 PM

(UTC-04:00) --- Current Time Zone ---

Allowed IP addresses

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols

☒ HTTPS only ☐ HTTPS and HTTP

Signing key

key1

Generate SAS and connection string



Si decide implementar una relación de sincronización continua que incluya un contenedor de Azure Blob, puede utilizar una cadena de conexión normal o una cadena de conexión SAS. Si utiliza una cadena de conexión SAS, no debe establecerse que caduque en un futuro próximo.

Azure Data Lake Storage Gen2

Al crear una relación de sincronización que incluya el lago de datos de Azure, debe proporcionar a Cloud Sync la cadena de conexión de la cuenta de almacenamiento. Debe ser una cadena de conexión normal, no una firma de acceso compartido (SAS).

Requisito de Azure NetApp Files

Utilice el nivel de servicio Premium o Ultra cuando sincronice datos con o desde Azure NetApp Files. Es posible que experimente errores y problemas de rendimiento si el nivel de servicio del disco es estándar.



Consulte a un arquitecto de soluciones si necesita ayuda para determinar el nivel de servicio adecuado. El tamaño del volumen y el nivel de volumen determinan el rendimiento que se puede obtener.

["Obtenga más información acerca de los niveles de servicio y el rendimiento de Azure NetApp Files".](#)

Requisitos de caja

- Para crear una relación de sincronización que incluya Box, deberá proporcionar las siguientes credenciales:
 - ID del cliente
 - Secreto de cliente
 - Clave privada
 - ID de clave pública
 - Frase de contraseña
 - ID de empresa
- Si crea una relación de sincronización de Amazon S3 a Box, debe utilizar un grupo de Data broker que tenga una configuración unificada en la que los siguientes ajustes se establezcan en 1:
 - Moneda del escáner
 - Límite de procesos de escáner
 - Moneda del transferir
 - Límite de procesos de transferir

["Aprenda a definir una configuración unificada para un grupo de intermediarios de datos".](#)

requisitos de bloque de almacenamiento en cloud de Google

Asegúrese de que su bloque de Google Cloud Storage cumpla con los siguientes requisitos.

Ubicaciones de agentes de datos compatibles para Google Cloud Storage

Las relaciones de sincronización que incluyen Google Cloud Storage requieren que se ponga en marcha un agente de datos en Google Cloud o en sus instalaciones. Cloud Sync le guía por el proceso de instalación de Data broker cuando crea una relación de sincronización.

- ["Descubra cómo implementar el agente de datos de Google Cloud"](#)
- ["Descubra cómo instalar el agente de datos en un Linux host"](#)

Regiones compatibles de Google Cloud

Se admiten todas las regiones.

Permisos para bloques de otros proyectos de Google Cloud

Al configurar una relación de sincronización, puede elegir entre bloques de Google Cloud en diferentes proyectos si proporciona los permisos necesarios para la cuenta de servicio del agente de datos. ["Aprenda a configurar la cuenta de servicio"](#).

Permisos para un destino de SnapMirror

Si el origen de una relación de sincronización es un destino de SnapMirror (que es de solo lectura), los permisos de "lectura/lista" son suficientes para sincronizar los datos del origen en un destino.

Unidad de Google

Al configurar una relación de sincronización que incluya Google Drive, tendrá que proporcionar lo siguiente:

- La dirección de correo electrónico de un usuario que tiene acceso a la ubicación de Google Drive donde desea sincronizar los datos
- La dirección de correo electrónico de una cuenta de servicio de Google Cloud que tenga permisos para acceder a Google Drive
- Clave privada para la cuenta de servicio

Para configurar la cuenta de servicio, siga las instrucciones de la documentación de Google:

- ["Cree la cuenta de servicio y las credenciales"](#)
- ["Delegue la autoridad en todo el dominio en su cuenta de servicio"](#)

Al editar el campo ámbitos OAuth Scopes, introduzca los siguientes ámbitos:

- <https://www.googleapis.com/auth/drive>
- <https://www.googleapis.com/auth/drive.file>

Requisitos del servidor NFS

- El servidor NFS puede ser un sistema de NetApp o un sistema que no sea de NetApp.
- El servidor de archivos debe permitir que un host de Data broker acceda a las exportaciones a través de los puertos necesarios.
 - 111 TCP/UDP
 - 2049 TCP/UDP
 - 5555 TCP/UDP
- Se admiten las versiones 3, 4.0, 4.1 y 4.2 de NFS.

La versión deseada debe estar activada en el servidor.

- Si desea sincronizar datos NFS desde un sistema ONTAP, asegúrese de que el acceso a la lista de exportación NFS de una SVM esté habilitado (`vserver nfs modify -vserver svm_name -showmount` habilitado).



La configuración predeterminada para showmount es *Enabled* a partir de ONTAP 9.2.

Requisitos de ONTAP

Si la relación de sincronización incluye Cloud Volumes ONTAP o un clúster de ONTAP en las instalaciones y ha seleccionado NFSv4 o posterior, deberá habilitar las ACL de NFSv4 en el sistema ONTAP. Esto es necesario para copiar las ACL.

Requisitos de almacenamiento de S3 de ONTAP

Al configurar una relación de sincronización que incluya ["Almacenamiento ONTAP S3"](#), deberá proporcionar lo siguiente:

- La dirección IP de la LIF conectada a ONTAP S3
- La clave de acceso y la clave secreta configurada por ONTAP para usar

Requisitos del servidor SMB

- El servidor SMB puede ser un sistema de NetApp o un sistema distinto de NetApp.
- Debe proporcionar a Cloud Sync credenciales con permisos en el servidor SMB.
 - Para un servidor SMB de origen, se requieren los siguientes permisos: List y Read.

Los miembros del grupo operadores de copia de seguridad son compatibles con un servidor SMB de origen.

- Para un servidor SMB de destino, se requieren los siguientes permisos: List, Read y Write.
- El servidor de archivos debe permitir que un host de Data broker acceda a las exportaciones a través de los puertos necesarios.
 - 139 TCP
 - 445 TCP
 - 137-138 UDP
- Se admiten las versiones 1.0, 2.0, 2.1, 3.0 y 3.11 de SMB.
- Conceda el grupo "Administradores" con permisos "Control total" a las carpetas de origen y destino.

Si no otorga este permiso, es posible que el agente de datos no tenga permisos suficientes para obtener las ACL en un archivo o directorio. Si esto ocurre, recibirá el siguiente error: "Getxattr error 95"

Limitación de SMB para directorios y archivos ocultos

Una limitación de SMB afecta a directorios y archivos ocultos al sincronizar datos entre servidores SMB. Si alguno de los directorios o archivos del servidor SMB de origen se ocultó a través de Windows, el atributo oculto no se copiará al servidor SMB de destino.

Comportamiento de sincronización de SMB por limitación de falta de sensibilidad en caso

El protocolo SMB no distingue mayúsculas y minúsculas, lo que significa que las letras mayúsculas y minúsculas se tratan como las mismas. Este comportamiento puede provocar errores de copia de directorio y archivos sobrescritos si una relación de sincronización incluye un servidor SMB y los datos ya existen en el destino.

Por ejemplo, digamos que hay un archivo llamado "a" en el origen y un archivo llamado "A" en el destino. Cuando Cloud Sync copia el archivo denominado "a" en el destino, el archivo "A" se sobrescribe con el archivo

"a" del origen.

En el caso de los directorios, digamos que hay un directorio llamado "b" en el origen y un directorio llamado "B" en el destino. Cuando Cloud Sync intenta copiar el directorio llamado "b" en el destino, Cloud Sync recibe un error que dice que el directorio ya existe. Como resultado, Cloud Sync siempre falla al copiar el directorio llamado "b".

La mejor manera de evitar esta limitación es asegurarse de que sincroniza los datos con un directorio vacío.

Información general sobre redes para Cloud Sync

Las redes para Cloud Sync incluyen la conectividad entre el grupo de agentes de datos y las ubicaciones de origen y destino, así como una conexión a Internet de salida de los agentes de datos a través del puerto 443.

Ubicación de agente de datos

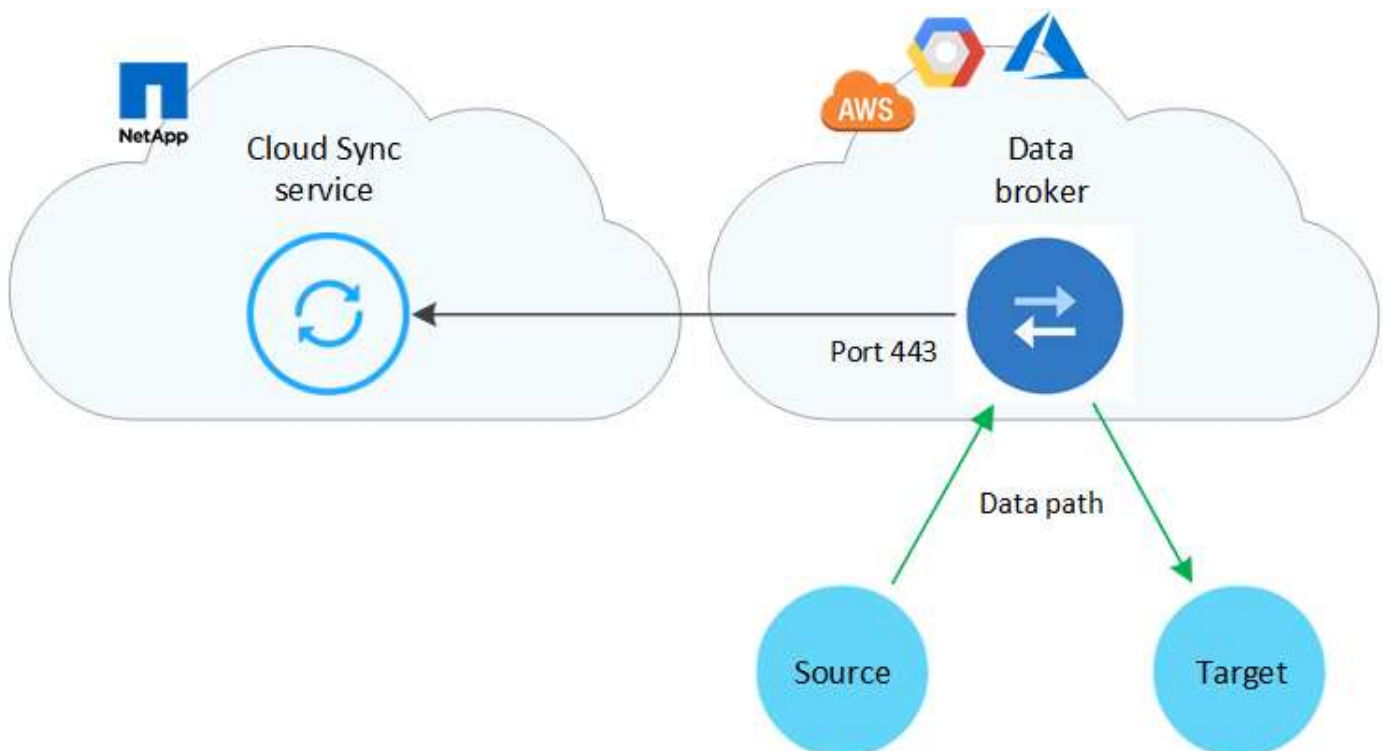
Un grupo de agentes de datos está compuesto por uno o más agentes de datos instalados en el cloud o en las instalaciones.

Agente de datos en el cloud

La siguiente imagen muestra un agente de datos que se ejecuta en el cloud, ya sea en AWS, Google Cloud o Azure. El origen y el destino pueden encontrarse en cualquier ubicación, siempre que haya una conexión con el agente de datos. Por ejemplo, es posible que tenga una conexión VPN desde su centro de datos hacia su proveedor de cloud.

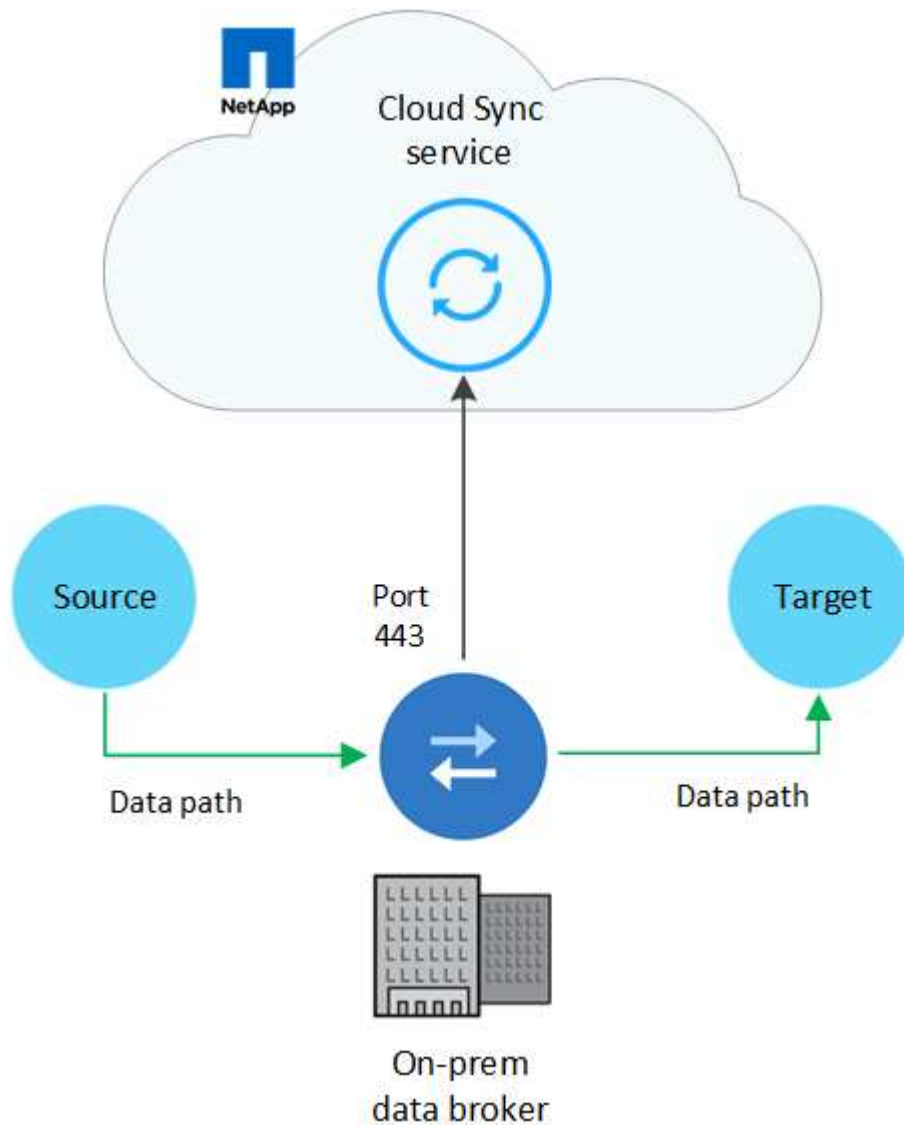


Cuando Cloud Sync implementa el agente de datos en AWS, Azure o Google Cloud, crea un grupo de seguridad que permite realizar las comunicaciones salientes necesarias.



Agente de datos en sus instalaciones

La siguiente imagen muestra el agente de datos que se ejecuta en las instalaciones, en un centro de datos. De nuevo, el origen y el destino pueden encontrarse en cualquier ubicación, siempre que haya una conexión con el agente de datos.



Requisitos de red

- El origen y el destino deben tener una conexión de red con el grupo de Data broker.

Por ejemplo, si un servidor NFS se encuentra en su centro de datos y existe un agente de datos en AWS, necesitará una conexión de red (VPN o Direct Connect) desde su red hasta el VPC.

- Un agente de datos necesita una conexión saliente a Internet para que pueda sondear el servicio Cloud Sync para tareas a través del puerto 443.
- NetApp recomienda configurar el origen, el destino y los agentes de datos para que utilicen un servicio de protocolo de tiempo de redes (NTP). La diferencia de tiempo entre los tres componentes no debe superar los 5 minutos.

Extremos de red

El agente de datos de NetApp requiere acceso saliente a Internet a través del puerto 443 para comunicarse con el servicio Cloud Sync y ponerse en contacto con algunos otros servicios y repositorios. El explorador web local también requiere acceder a extremos para determinadas acciones. Si necesita limitar la conectividad saliente, consulte la siguiente lista de puntos finales al configurar el firewall para el tráfico saliente.

Extremos de Data broker

Un agente de datos se pone en contacto con los siguientes extremos:

Puntos finales	Específico
https://olcentgbl.trafficmanager.net	Para ponerse en contacto con un repositorio para actualizar paquetes CentOS para el host de Data broker. Solo se puede contactar con este extremo si instala manualmente el agente de datos en un host CentOS.
https://rpm.nodesource.com https://registry.npmjs.org https://nodejs.org :	Para ponerse en contacto con repositorios para actualizar los paquetes Node.js, npm y otros paquetes de terceros utilizados en desarrollo.
https://tgz.pm2.io	Para acceder a un repositorio para la actualización de Pm2, que es un paquete de terceros que se utiliza para supervisar Cloud Sync.
https://sqs.us-east-1.amazonaws.com https://kinesis.us-east-1.amazonaws.com	Para ponerse en contacto con los servicios de AWS que Cloud Sync utiliza en las operaciones (poner en cola archivos, registrar acciones y entregar actualizaciones al agente de datos).
https://s3.region.amazonaws.com por ejemplo: s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region ["Consulte la documentación de AWS para obtener una lista de extremos de S3"]	Para ponerse en contacto con Amazon S3 cuando una relación de sincronización incluya un bloque de S3.
https://s3.amazonaws.com/	Cuando se descargan registros del agente de datos de Cloud Sync, el agente de datos cierra su directorio de registros y carga los registros en un bloque S3 predefinido en la región de US-East-1.
https://storage.googleapis.com/	Para ponerse en contacto con Google Cloud cuando una relación de sincronización utiliza un bloque de GCP.
https://storage-account.blob.core.windows.net ["Si se utiliza Azure Data Lake Gen2: https://storage-account.dfs.core.windows.net "] Donde <i>Storage-account</i> es la cuenta de almacenamiento de origen del usuario.	Para abrir el proxy en la dirección de la cuenta de almacenamiento de Azure de un usuario.
https://cf.cloudsync.netapp.com https://repo.cloudsync.netapp.com	Para ponerse en contacto con el servicio Cloud Sync.
https://support.netapp.com	Para ponerse en contacto con el soporte de NetApp cuando use una licencia BYOL para relaciones de sincronización.

Puntos finales	Específico
https://fedoraproject.org	Para instalar 7z en la máquina virtual Data Broker durante la instalación y las actualizaciones. Es necesario enviar mensajes de AutoSupport al soporte técnico de NetApp.
https://sts.amazonaws.com	Para verificar las credenciales de AWS cuando el agente de datos se implementa en AWS o cuando está implementado en sus instalaciones, y se proporcionan las credenciales de AWS. El agente de datos se pone en contacto con este extremo durante la implementación, cuando se actualiza y cuando se reinicia.
https://console.bluelxp.netapp.com/ https://netapp-cloud-account.auth0.com	Para ponerse en contacto con Cloud Data Sense cuando utilice Data Sense para seleccionar los archivos de origen de una nueva relación de sincronización.
https://pubsub.googleapis.com	Si crea una relación de sincronización continua desde una cuenta de almacenamiento de Google.
https://storage-account.queue.core.windows.net/ https://management.azure.com/subscriptions/{subscriptionId}/ResourceGroups/{ResourceGroup}/providers/Microsoft.EventGrid/* donde <i>Storage-account</i> es la cuenta de almacenamiento de origen del usuario, <i>subscriptionid</i> es el identificador de suscripción de origen y <i>ResourceGroup</i> es el grupo de recursos de origen.	Si se crea una relación de sincronización continua desde una cuenta de almacenamiento de Azure.

Extremos del navegador web

El explorador web necesita acceder al siguiente extremo para descargar los registros con fines de solución de problemas:

logs.cloudsync.netapp.com:443

Instalar un agente de datos

Crear un nuevo agente de datos en AWS

Al crear un nuevo grupo de agentes de datos, elija Amazon Web Services para implementar el software de agente de datos en una nueva instancia de EC2 en un VPC. Cloud Sync le guía durante el proceso de instalación, pero en esta página se repiten los requisitos y los pasos que le ayudarán a preparar la instalación.

También tiene la opción de instalar el agente de datos en un host Linux existente en el cloud o en sus instalaciones. "[Leer más](#)".

Regiones admitidas de AWS

Todas las regiones están soportadas excepto las regiones de China.

Privilegios de usuario raíz

El software de Data broker se ejecuta automáticamente como root en el host Linux. Ejecutar como root es un requisito para las operaciones de data broker. Por ejemplo, para montar recursos compartidos.

Requisitos de red

- El agente de datos necesita una conexión saliente a Internet para que pueda sondear el servicio Cloud Sync para las tareas a través del puerto 443.

Cuando Cloud Sync implementa el agente de datos en AWS, crea un grupo de seguridad que permite la comunicación saliente necesaria. Tenga en cuenta que puede configurar el agente de datos para que utilice un servidor proxy durante el proceso de instalación.

Si necesita limitar la conectividad saliente, consulte ["lista de puntos finales con los que se contacta el data broker"](#).

- NetApp recomienda configurar el origen, el destino y el intermediario de datos para utilizar un servicio de protocolo de tiempo de redes (NTP). La diferencia de tiempo entre los tres componentes no debe superar los 5 minutos.

Permisos necesarios para implementar el agente de datos en AWS

La cuenta de usuario de AWS que utiliza para implementar el el agente de datos debe tener los permisos incluidos en ["Esta política proporcionada por NetApp"](#).

requisitos para utilizar su propia función de IAM con el agente de datos de AWS

Cuando Cloud Sync implementa el Data broker, crea una función IAM para la instancia de Data broker. Si lo prefiere, puede implementar el agente de datos con su propio rol de IAM. Puede usar esta opción si su organización tiene políticas de seguridad estrictas.

El rol del IAM debe cumplir los siguientes requisitos:

- Se debe permitir al servicio EC2 asumir el rol IAM como entidad de confianza.
- ["Los permisos definidos en este archivo JSON"](#) Se debe adjuntar a la función IAM para que el intermediario de datos pueda funcionar correctamente.

Siga los pasos que se indican a continuación para especificar la función de IAM al implementar el agente de datos.

Creación del agente de datos

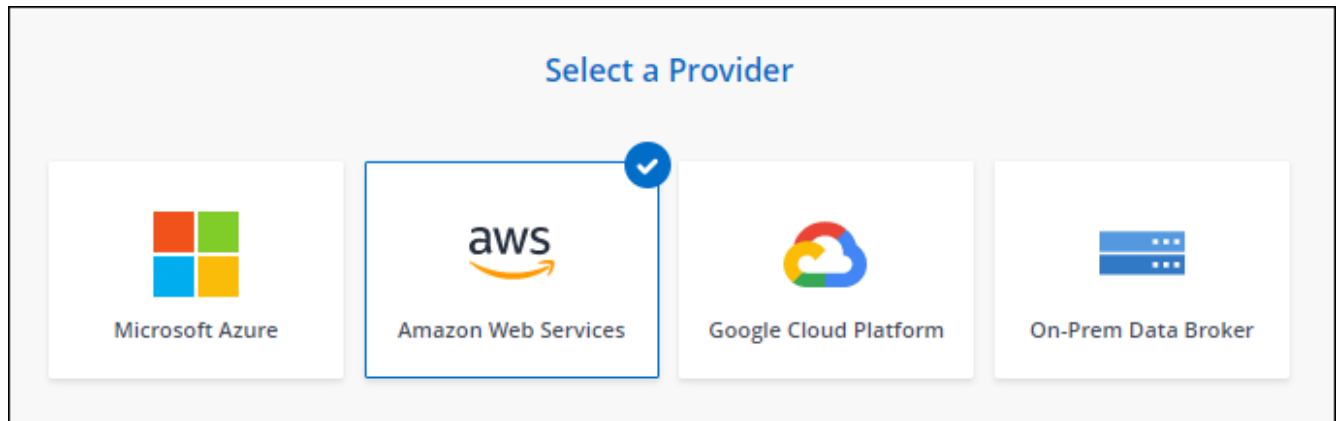
Hay varias formas de crear un nuevo agente de datos. Estos pasos describen cómo instalar un agente de datos en AWS al crear una relación de sincronización.

Pasos

1. Haga clic en **Crear nueva sincronización**.
2. En la página **definir relación de sincronización**, elija un origen y un destino y haga clic en **continuar**.

Complete los pasos hasta llegar a la página **Grupo de agentes de datos**.

3. En la página **Grupo de agentes de datos**, haga clic en **Crear agente de datos** y, a continuación, seleccione **Amazon Web Services**.



4. Introduzca un nombre para el Data broker y haga clic en **continuar**.
5. Introduzca una clave de acceso de AWS para que Cloud Sync pueda crear el agente de datos en AWS en su nombre.

Las teclas no se guardan ni utilizan para ningún otro propósito.

Si prefiere no proporcionar claves de acceso, haga clic en el vínculo situado en la parte inferior de la página para utilizar una plantilla CloudFormation en su lugar. Cuando usa esta opción, no necesita proporcionar credenciales, ya que inicia sesión directamente en AWS.

en el siguiente vídeo se muestra cómo iniciar la instancia de Data broker mediante una plantilla CloudFormation:

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

6. Si introdujo una clave de acceso de AWS, seleccione una ubicación para la instancia, seleccione un par de claves, elija si desea habilitar una dirección IP pública y seleccione un rol de IAM existente o deje el campo vacío para que Cloud Sync cree el rol para usted. También tiene la opción de cifrar el agente de datos con una clave KMS.

Si elige su propio rol de IAM, [deberá proporcionar los permisos necesarios](#).

Basic Settings

Location

VPC

Select VPC ▼

Subnet

Select Subnet ▼

Connectivity

Key Pair

Select Key Pair ▼

Enable Public IP?

☒ Enable ☐ Disable

IAM Role (optional)

IAM Role (optional) ⓘ

KMS Key for EBS volume (optional)

Select KMS Key for EBS Encryption ▼

7. Especifique una configuración de proxy, si se requiere un proxy para el acceso a Internet en el VPC.
8. Después de que el Data broker esté disponible, haga clic en **continuar** en Cloud Sync.

En la siguiente imagen se muestra una instancia implementada correctamente en AWS:

✓ NFS Server
2 Data Broker Group
 3 Directories
 4 Target NFS Server
 >

Select a Data Broker Group

1 Data Broker Group
🔍

ben-data-broker
➔

1	N/A	0	1 Active
Data Brokers	Transfer Rate	Relationships	Data Brokers Status

9. Complete las páginas del asistente para crear la nueva relación de sincronización.

Resultado

Ha implementado un agente de datos en AWS y creado una nueva relación de sincronización. Puede utilizar este grupo de Data broker con relaciones de sincronización adicionales.

Detalles sobre la instancia de Data broker

Cloud Sync crea un agente de datos en AWS utilizando la siguiente configuración.

Tipo de instancia

m5n.xlarge cuando esté disponible en la región, de lo contrario m5.xlarge

VCPU

4

RAM

16 GB

De NetApp

Amazon Linux 2022

Tamaño y tipo del disco

SSD GP2 DE 10 GB

Creación de un nuevo agente de datos en Azure

Al crear un nuevo grupo de agentes de datos, elija Microsoft Azure para implementar el software de Data broker en una nueva máquina virtual en un vnet. Cloud Sync le guía durante el proceso de instalación, pero en esta página se repiten los requisitos y los pasos que le ayudarán a preparar la instalación.

También tiene la opción de instalar el agente de datos en un host Linux existente en el cloud o en sus instalaciones. "[Leer más](#)".

Regiones de Azure compatibles

Todas las regiones cuentan con el apoyo de las regiones de China, la gobernadora de los Estados Unidos y el Departamento de Defensa de los Estados Unidos.

Privilegios de usuario raíz

El software de Data broker se ejecuta automáticamente como root en el host Linux. Ejecutar como root es un requisito para las operaciones de data broker. Por ejemplo, para montar recursos compartidos.

Requisitos de red

- El agente de datos necesita una conexión saliente a Internet para que pueda sondear el servicio Cloud Sync para las tareas a través del puerto 443.

Cuando Cloud Sync implementa el agente de datos en Azure, crea un grupo de seguridad que permite la comunicación saliente necesaria.

Si necesita limitar la conectividad saliente, consulte "[lista de puntos finales con los que se contacta el data broker](#)".

- NetApp recomienda configurar el origen, el destino y el intermediario de datos para utilizar un servicio de protocolo de tiempo de redes (NTP). La diferencia de tiempo entre los tres componentes no debe superar los 5 minutos.

Permisos necesarios para implementar el agente de datos en Azure

Asegúrese de que la cuenta de usuario de Azure que utilice para implementar el agente de datos tenga los siguientes permisos:

```
{
  "Name": "Azure Data Broker",
  "Actions": [
    "Microsoft.Resources/subscriptions/read",

    "Microsoft.Resources/deployments/operationstatuses/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/virtualNetworks/subnets/read",

    "Microsoft.Resources/subscriptions/resourceGroups/write",

    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/validate/action",

    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/disks/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/publicIPAddresses/delete",

    "Microsoft.Network/networkSecurityGroups/securityRules/delete",

    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Compute/disks/write",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/publicIPAddresses/read",

    "Microsoft.Network/virtualNetworks/subnets/join/action",
```



```

        "Microsoft.Network/publicIPAddresses/join/action",
        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Storage/storageAccounts/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/write",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/delete",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes
/action",

        "Microsoft.EventGrid/systemTopics/read",
        "Microsoft.EventGrid/systemTopics/write",
        "Microsoft.EventGrid/systemTopics/delete",
        "Microsoft.EventGrid/eventSubscriptions/write",
        "Microsoft.Storage/storageAccounts/write"

```

```

    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure Data Broker",
    "IsCustom": "true"
}

```

Nota:

1. Los siguientes permisos solo son necesarios si tiene pensado habilitar la configuración de sincronización continua en una relación de sincronización de Azure con otra ubicación de almacenamiento en cloud:
 - "Microsoft.Storage/storageAccounts/read",
 - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/Write',
 - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/read',
 - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/DELETE',
 - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action',
 - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes/action',
 - 'Microsoft.EventGrid/systemTopics/Read',
 - 'Microsoft.EventGrid/systemTopics/Write',
 - 'Microsoft.EventGrid/systemTopics/DELETE',
 - 'Microsoft.EventGrid/eventSubscriptions/Write',
 - 'Microsoft.almacenamiento/cuentas de almacenamiento/escritura'

Además, el ámbito asignable debe definirse en el ámbito de suscripción y el ámbito del grupo de recursos **no** si tiene previsto implementar Continuous Sync en Azure.

["Obtenga más información acerca de la configuración de sincronización continua"](#).

Método de autenticación

Al implementar el agente de datos, tendrá que elegir un método de autenticación para la máquina virtual: Una contraseña o un par de claves público-privadas SSH.

Para obtener ayuda sobre la creación de un par de claves, consulte ["Documentación de Azure: Cree y utilice una pareja de claves SSH público-privada para máquinas virtuales de Linux en Azure"](#).

Creación del agente de datos

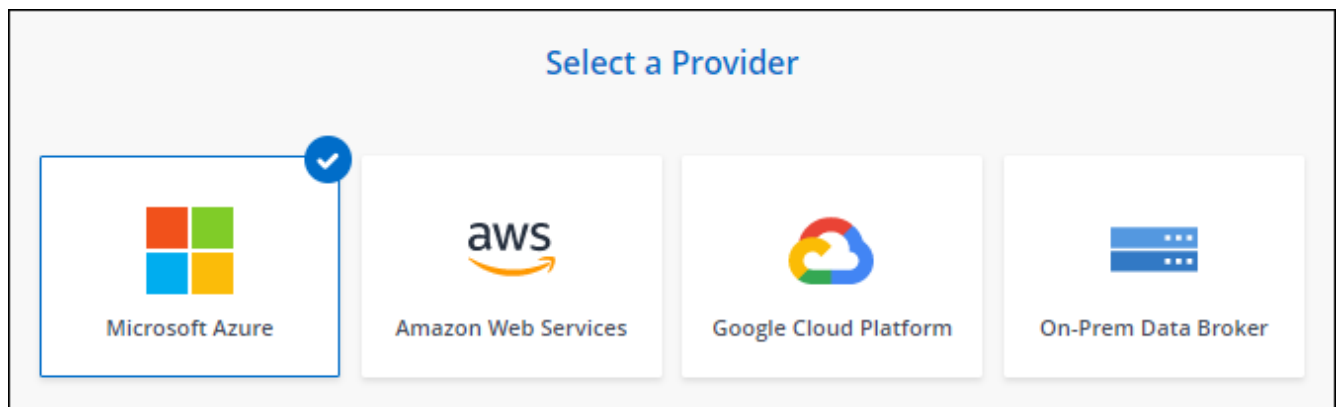
Hay varias formas de crear un nuevo agente de datos. Estos pasos describen cómo instalar un agente de datos en Azure al crear una relación de sincronización.

Pasos

1. Haga clic en **Crear nueva sincronización**.
2. En la página **definir relación de sincronización**, elija un origen y un destino y haga clic en **continuar**.

Complete los pasos hasta llegar a la página **Grupo de agentes de datos**.

3. En la página **Grupo de agentes de datos**, haga clic en **Crear agente de datos** y, a continuación, seleccione **Microsoft Azure**.



4. Introduzca un nombre para el Data broker y haga clic en **continuar**.
5. Si se le solicita, inicie sesión en su cuenta de Microsoft. Si no se le solicita, haga clic en **Iniciar sesión en Azure**.

El formulario es propiedad de Microsoft y está alojado en él. Sus credenciales no se proporcionan a NetApp.

6. Elija una ubicación para el agente de datos e introduzca detalles básicos sobre la máquina virtual.

Location	Virtual Machine
Subscription OCCM Dev ▼	VM Name netappdatabroker ⓘ
Azure Region West US 2 ▼	User Name databroker ⓘ
VNet Vnet1 ▼	Authentication Method: <input checked="" type="radio"/> Password <input type="radio"/> Public Key
Subnet Subnet1 ▼	Enter Password ⓘ
	Resource Group: <input checked="" type="radio"/> Generate a new group <input type="radio"/> Use an existing group



Si planea implementar una relación de sincronización continua, debe asignar una función personalizada a su agente de datos. También se puede realizar manualmente después de crear el broker.

7. Especifique una configuración de proxy, si se requiere un proxy para el acceso a Internet en la vnet.
8. Haga clic en **continuar** y mantenga la página abierta hasta que finalice la implementación.

El proceso puede tardar hasta 7 minutos.

9. En Cloud Sync, haga clic en **continuar** una vez que el Data broker esté disponible.
10. Complete las páginas del asistente para crear la nueva relación de sincronización.

Resultado

Ha puesto en marcha un agente de datos en Azure y creado una nueva relación de sincronización. Puede utilizar este Data broker con relaciones de sincronización adicionales.

¿obtiene un mensaje acerca de cómo se necesita el consentimiento de administrador?

Si Microsoft le notifica que se requiere la aprobación del administrador porque Cloud Sync necesita permiso para acceder a los recursos de la organización en su nombre, dispone de dos opciones:

1. Pida a su administrador de AD que le proporcione los siguientes permisos:

En Azure, vaya a **Centros de administración > Azure AD > usuarios y grupos > Configuración de usuario** y active **los usuarios pueden dar su consentimiento a las aplicaciones que acceden a los datos de la empresa en su nombre**.

2. Pida a su administrador de AD que consiente en su nombre **CloudSync-AzureDataBrokerCreator** utilizando la siguiente URL (éste es el punto final del consentimiento de administración):

`https://login.microsoftonline.com/{FILL AQUÍ su ID DE INQUILINO}/v2.0/adminconsent?client_id=8ee4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read`

Como se muestra en la URL, nuestra URL de aplicación es `https://cloudsync.netapp.com` y el ID de cliente de aplicación es `8ee4ca3a-bafa-4831-97cc-5a38923cab85`.

Información sobre el equipo virtual de Data broker

Cloud Sync crea un agente de datos en Azure utilizando la siguiente configuración.

Tipo de máquina virtual

Estándar DS4 v2

VCPU

8

RAM

28 GB

De NetApp

Rocky Linux 9.0

Tamaño y tipo del disco

SSD Premium de 64 GB

Creación de un nuevo agente de datos en Google Cloud

Al crear un nuevo grupo de agentes de datos, elija Google Cloud Platform para implementar el software de agente de datos en una nueva instancia de máquina virtual en Google Cloud VPC. Cloud Sync le guía durante el proceso de instalación, pero en esta página se repiten los requisitos y los pasos que le ayudarán a preparar la instalación.

También tiene la opción de instalar el agente de datos en un host Linux existente en el cloud o en sus instalaciones. "[Leer más](#)".

Regiones compatibles de Google Cloud

Se admiten todas las regiones.

Privilegios de usuario raíz

El software de Data broker se ejecuta automáticamente como root en el host Linux. Ejecutar como root es un requisito para las operaciones de data broker. Por ejemplo, para montar recursos compartidos.

Requisitos de red

- El agente de datos necesita una conexión saliente a Internet para que pueda sondear el servicio Cloud Sync para las tareas a través del puerto 443.

Cuando Cloud Sync implementa el agente de datos en Google Cloud, crea un grupo de seguridad que permite la comunicación saliente necesaria.

Si necesita limitar la conectividad saliente, consulte "[lista de puntos finales con los que se contacta el data broker](#)".

- NetApp recomienda configurar el origen, el destino y el intermediario de datos para utilizar un servicio de protocolo de tiempo de redes (NTP). La diferencia de tiempo entre los tres componentes no debe superar los 5 minutos.

Permisos necesarios para implementar el agente de datos en Google Cloud

Asegúrese de que el usuario de Google Cloud que implementa el agente de datos tiene los siguientes permisos:

```
- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list
```

Permisos necesarios para la cuenta de servicio

Al implementar el agente de datos, debe seleccionar una cuenta de servicio que tenga los siguientes permisos:

- `logging.logEntries.create`
- `resourceManager.projects.get`
- `storage.buckets.get`
- `storage.buckets.list`
- `storage.objects.create`
- `storage.objects.delete`
- `storage.objects.get`
- `storage.objects.getIamPolicy`
- `storage.objects.list`
- `storage.objects.setIamPolicy`
- `storage.objects.update`
- `iam.serviceAccounts.signJwt`
- `pubsub.subscriptions.consume`
- `pubsub.subscriptions.create`
- `pubsub.subscriptions.delete`
- `pubsub.subscriptions.list`
- `pubsub.topics.attachSubscription`
- `pubsub.topics.create`
- `pubsub.topics.delete`
- `pubsub.topics.list`
- `pubsub.topics.setIamPolicy`
- `storage.buckets.update`

Notas:

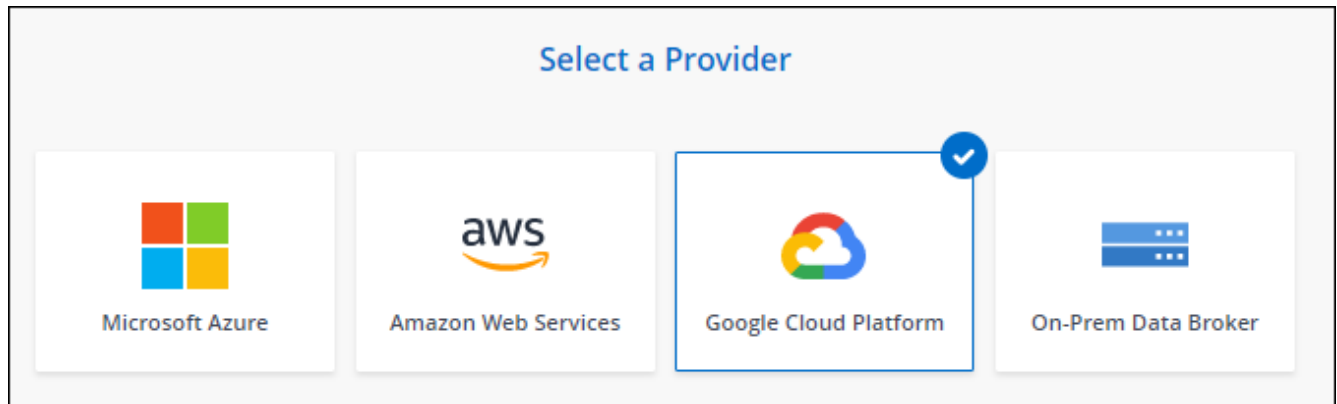
1. El "permiso `iam.serviceAccounts.signJwt`" es requerido sólo si usted está planeando establecer el corredor de datos para usar un almacén externo de HashiCorp.
2. Los permisos "`pubsub.*`" y "`Storage.buckets.update`" sólo son necesarios si tiene previsto habilitar la configuración de sincronización continua en una relación de sincronización desde Google Cloud Storage a otra ubicación de almacenamiento en la nube. ["Obtenga más información acerca de la opción Continuous Sync \(sincronización continua\)"](#).

Creación del agente de datos

Hay varias formas de crear un nuevo agente de datos. Estos pasos describen cómo instalar un agente de datos en Google Cloud al crear una relación de sincronización.

Pasos

1. Haga clic en **Crear nueva sincronización**.
2. En la página **definir relación de sincronización**, elija un origen y un destino y haga clic en **continuar**.
Complete los pasos hasta llegar a la página **Grupo de agentes de datos**.
3. En la página **Grupo de agentes de datos**, haga clic en **Crear agente de datos** y seleccione **Google Cloud Platform**.



4. Introduzca un nombre para el Data broker y haga clic en **continuar**.
5. Si se le solicita, inicie sesión con su cuenta de Google.

El formulario es propiedad de Google y está alojado en él. Sus credenciales no se proporcionan a NetApp.

6. Seleccione un proyecto y una cuenta de servicio y, a continuación, elija una ubicación para el agente de datos, incluyendo si desea habilitar o deshabilitar una dirección IP pública.

Si no habilita una dirección IP pública, tendrá que definir un servidor proxy en el siguiente paso.

7. Especifique una configuración de proxy, si se requiere un proxy para el acceso a Internet en el VPC.

Si se necesita un proxy para el acceso a Internet, el proxy debe estar en Google Cloud y utilizar la misma cuenta de servicio que el agente de datos.

8. Una vez que el Data broker esté disponible, haga clic en **continuar** en Cloud Sync.

La puesta en marcha de la instancia tarda entre 5 y 10 minutos, aproximadamente. Puede supervisar el progreso desde el servicio Cloud Sync, que se actualiza automáticamente cuando la instancia está disponible.

9. Complete las páginas del asistente para crear la nueva relación de sincronización.

Resultado

Ha puesto en marcha un agente de datos en Google Cloud y creado una nueva relación de sincronización. Puede utilizar este Data broker con relaciones de sincronización adicionales.

Proporciona permisos para utilizar bloques en otros proyectos de Google Cloud

Al crear una relación de sincronización y elegir Google Cloud Storage como origen o destino, Cloud Sync le permite elegir entre los bloques que la cuenta de servicio del agente de datos tiene permisos para utilizar. De forma predeterminada, incluye los bloques que se encuentran en el proyecto *same* como la cuenta de servicio de Data broker. Pero puede seleccionar cubos de proyectos *other* si proporciona los permisos necesarios.

Pasos

1. Abra la consola de Google Cloud Platform y cargue el servicio Cloud Storage.
2. Haga clic en el nombre del bloque que desea utilizar como origen o destino en una relación de sincronización.
3. Haga clic en **permisos**.
4. Haga clic en **Agregar**.
5. Introduzca el nombre de la cuenta de servicio del agente de datos.
6. Seleccione una función que proporcione [los mismos permisos que se muestran anteriormente](#).
7. Haga clic en **Guardar**.

Resultado

Al configurar una relación de sincronización, ahora puede elegir ese bloque como origen o destino en la relación de sincronización.

Detalles sobre la instancia de VM de Data broker

Cloud Sync crea un agente de datos en Google Cloud utilizando la siguiente configuración.

Tipo de máquina

n2-estándar-4

VCPU

4

RAM

15 GB

De NetApp

Rocky Linux 9.0

Tamaño y tipo del disco

Disco duro de 20 GB, estándar pd

Instalar el agente de datos en un host Linux

Cuando crea un nuevo grupo de agentes de datos, elija la opción On-Prem Data Broker para instalar el software de agente de datos en un host Linux local o en un host Linux existente en el cloud. Cloud Sync le guía durante el proceso de instalación, pero en esta página se repiten los requisitos y los pasos que le ayudarán a preparar la instalación.

Requisitos del host Linux

- **sistema operativo:**

- CentOS 8.0 y 8.5

CentOS Stream no es compatible.

- Red Hat Enterprise Linux 8.0 y 8.5
- Rocky Linux 9
- Sistema operativo Ubuntu Server 20.04 LTS
- SUSE Linux Enterprise Server 15 SP1

El comando `yum update` debe ejecutarse en el host antes de instalar el agente de datos.

Debe registrarse un sistema Red Hat Enterprise Linux con Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software necesario de terceros durante la instalación.

- **RAM:** 16 GB
- **CPU:** 4 núcleos
- **espacio libre en disco:** 10 GB
- **SELinux:** Le recomendamos que desactive la función "SELinux" en el host.

SELinux aplica una política que bloquea las actualizaciones de software de Data broker y puede bloquear el intermediario de datos de los extremos de contacto necesarios para un funcionamiento normal.

Privilegios de usuario raíz

El software de Data broker se ejecuta automáticamente como root en el host Linux. Ejecutar como root es un requisito para las operaciones de data broker. Por ejemplo, para montar recursos compartidos.

Requisitos de red

- El host Linux debe tener una conexión con el origen y el destino.
- El servidor de archivos debe permitir que el host Linux acceda a las exportaciones.

- El puerto 443 debe estar abierto en el host Linux para el tráfico saliente a AWS (el agente de datos se comunica constantemente con el servicio Amazon SQS).
- NetApp recomienda configurar el origen, el destino y el intermediario de datos para utilizar un servicio de protocolo de tiempo de redes (NTP). La diferencia de tiempo entre los tres componentes no debe superar los 5 minutos.

Habilitar el acceso a AWS

Si planea utilizar el agente de datos con una relación de sincronización que incluya un bloque de S3, debe preparar el host Linux para el acceso a AWS. Cuando instale el agente de datos, necesitará proporcionar claves AWS para un usuario de AWS que tenga acceso al mismo mediante programación y permisos específicos.

Pasos

1. Cree una política de IAM mediante ["Esta política proporcionada por NetApp"](#)

["Consulte las instrucciones de AWS"](#)

2. Cree un usuario IAM con acceso mediante programación.

["Consulte las instrucciones de AWS"](#)

Asegúrese de copiar las claves de AWS porque debe especificarlas al instalar el software de Data broker.

Habilitar el acceso a Google Cloud

Si tiene pensado utilizar el agente de datos con una relación de sincronización que incluya un bucket de Google Cloud Storage, debería preparar el host Linux para el acceso a Google Cloud. Al instalar el Data Broker, deberá proporcionar una clave para una cuenta de servicio que tenga permisos específicos.

Pasos

1. Cree una cuenta de servicio de Google Cloud que tenga permisos de administrador de almacenamiento, si todavía no dispone de una.
2. Cree una clave de cuenta de servicio guardada en formato JSON.

["Vea las instrucciones de Google Cloud"](#)

El archivo debe contener al menos las siguientes propiedades: "Project_id", "private_key" y "client_email"



Al crear una clave, el archivo se genera y descarga en el equipo.

3. Guarde el archivo JSON en el host Linux.

Habilitar el acceso a Microsoft Azure

El acceso a Azure se define por relación proporcionando una cuenta de almacenamiento y una cadena de conexión en el asistente de relaciones de sincronización.

Instalación del Data broker

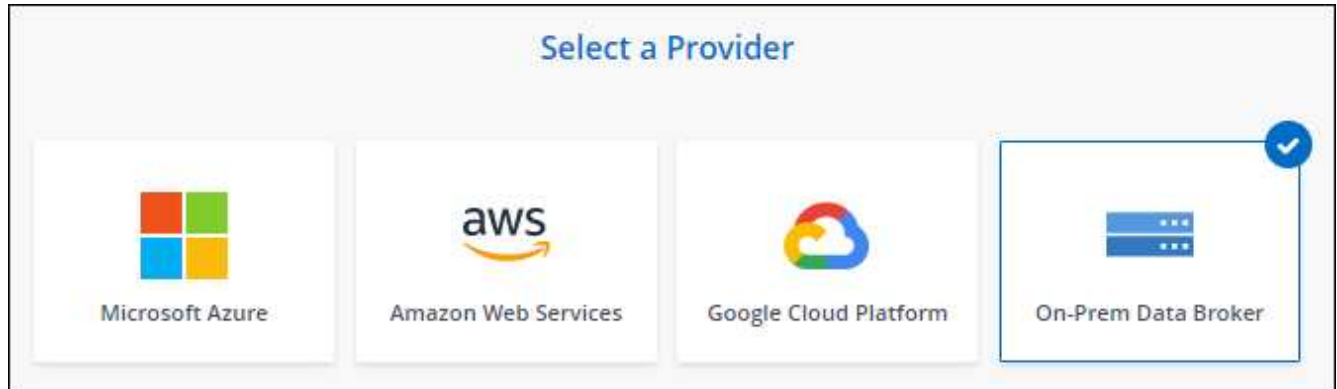
Puede instalar un agente de datos en un host Linux al crear una relación de sincronización.

Pasos

1. Haga clic en **Crear nueva sincronización**.
2. En la página **definir relación de sincronización**, elija un origen y un destino y haga clic en **continuar**.

Complete los pasos hasta llegar a la página **Grupo de agentes de datos**.

3. En la página **Grupo de agentes de datos**, haga clic en **Crear agente de datos** y, a continuación, seleccione **Corredor de datos en las instalaciones**.



Aunque la opción se etiqueta **on-Prem Data Broker**, se aplica a un host Linux en sus instalaciones o en la nube.

4. Introduzca un nombre para el Data broker y haga clic en **continuar**.

La página de instrucciones se carga en breve. Tendrá que seguir estas instrucciones; incluyen un enlace único para descargar el instalador.

5. En la página de instrucciones:

- a. Seleccione si desea activar el acceso a **AWS**, **Google Cloud** o ambos.
- b. Seleccione una opción de instalación: **sin proxy**, **usar servidor proxy** o **usar servidor proxy con autenticación**.
- c. Utilice los comandos para descargar e instalar el Data broker.

En los siguientes pasos se ofrecen detalles sobre cada posible opción de instalación. Siga la página de instrucciones para obtener el comando exacto según la opción de instalación.

- d. Descargue el instalador:

- Sin proxy:

```
curl <URI> -o data_broker_installer.sh
```

- Usar servidor proxy:

```
curl <URI> -o data_broker_installer.sh -x <proxy_host>:<proxy_port>
```

- Utilice el servidor proxy con autenticación:

```
curl <URI> -o data_broker_installer.sh -x  
<proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>
```

URI

Cloud Sync muestra el URI del archivo de instalación en la página de instrucciones, que se carga cuando sigue los mensajes para implementar el agente de datos en las instalaciones. Ese URI no se repite aquí porque el enlace se genera dinámicamente y sólo se puede usar una vez. [Siga estos pasos para obtener el URI de Cloud Sync.](#)

e. Cambie a superusuario, haga ejecutable el instalador e instale el software:



Cada uno de los comandos enumerados a continuación incluye parámetros para el acceso a AWS y el acceso a Google Cloud. Siga la página de instrucciones para obtener el comando exacto según la opción de instalación.

- Sin configuración de proxy:

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file>
```

- Configuración de proxy:

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port>
```

- Configuración del proxy con autenticación:

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port> -u
<proxy_username> -w <proxy_password>
```

Claves de AWS

Estas son las claves para el usuario que debería prepararon [siga estos pasos](#). Las claves de AWS se almacenan en el agente de datos, que se ejecuta en la red local o en el cloud. NetApp no utiliza las claves fuera del agente de datos.

Archivo JSON

Este es el archivo JSON que contiene una cuenta de servicio clave que usted debe haber preparado [siga estos pasos](#).

6. Una vez que el Data broker esté disponible, haga clic en **continuar** en Cloud Sync.
7. Complete las páginas del asistente para crear la nueva relación de sincronización.

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.



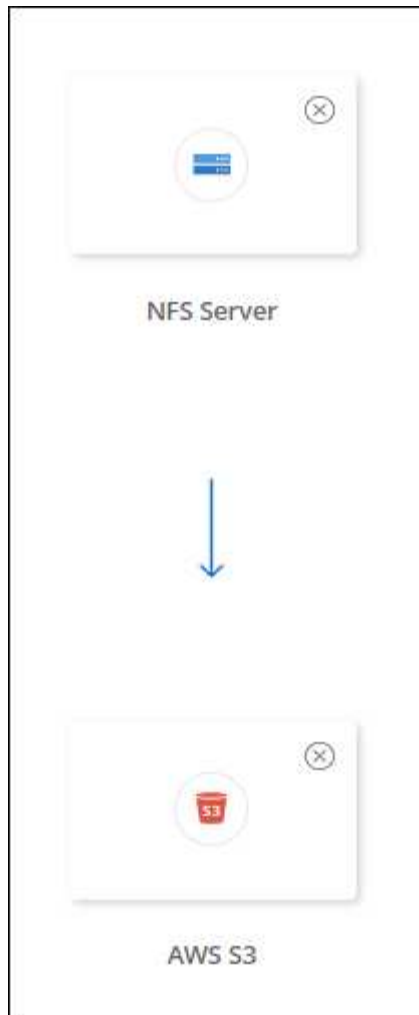
5. Seleccione **Sincronizar datos de esta ubicación** o **Sincronizar datos a esta ubicación** y siga las indicaciones para configurar la relación de sincronización.

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.

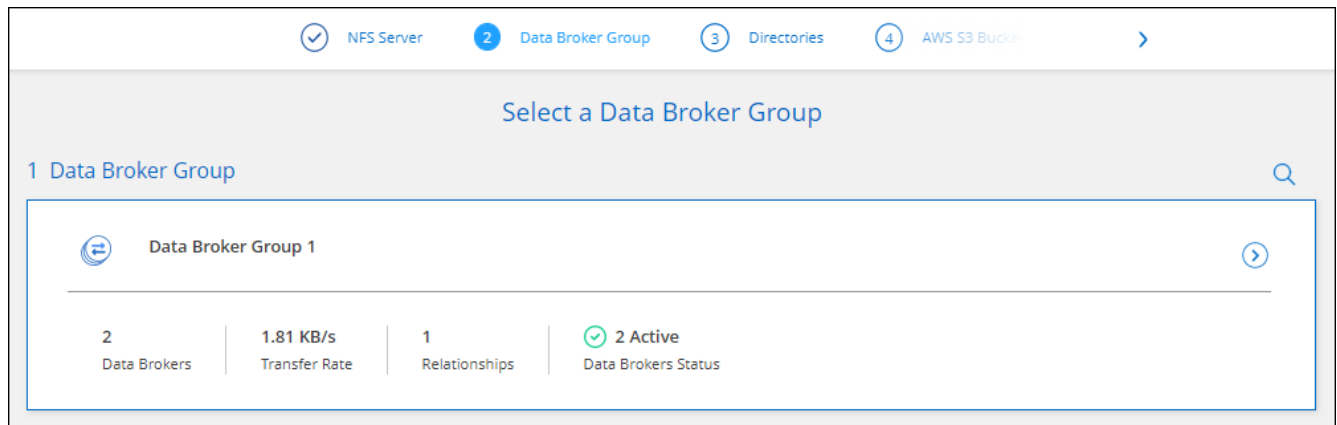


3. En la página **servidor NFS**, introduzca la dirección IP o el nombre de dominio completo del servidor NFS que desea sincronizar con AWS.
4. En la página **Data Broker Group**, siga las indicaciones para crear una máquina virtual de Data Broker en AWS, Azure o Google Cloud Platform, o para instalar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



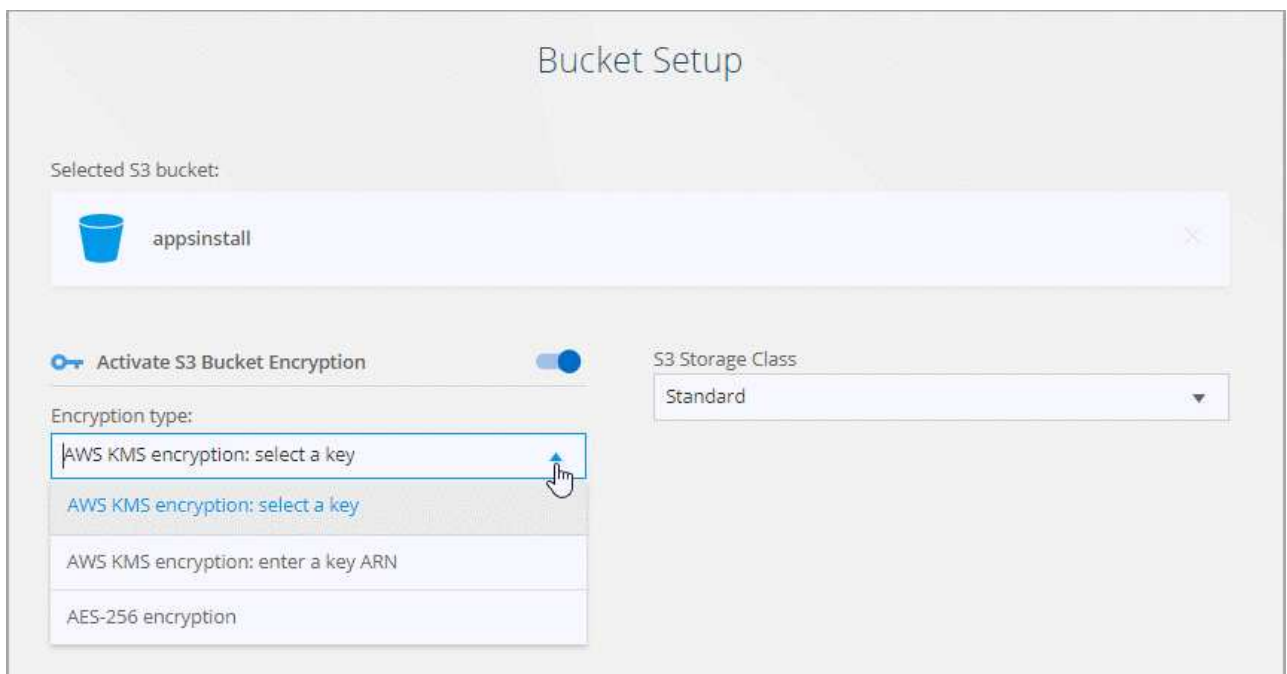
6. en la página **directorios**, seleccione un directorio o subdirectorio de nivel superior.

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>

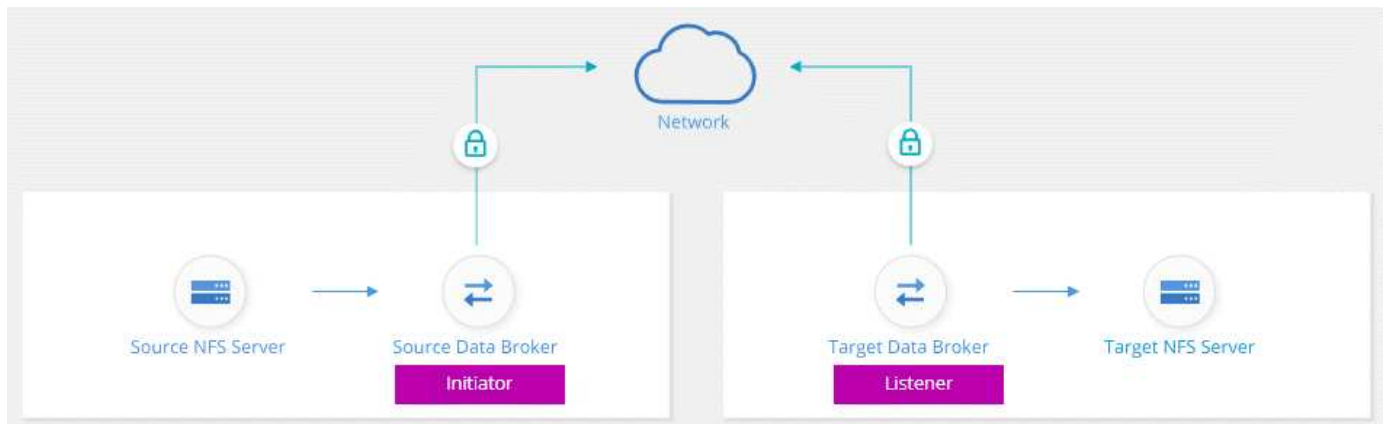
Sincronizando los datos NFS mediante el cifrado de datos en tránsito

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

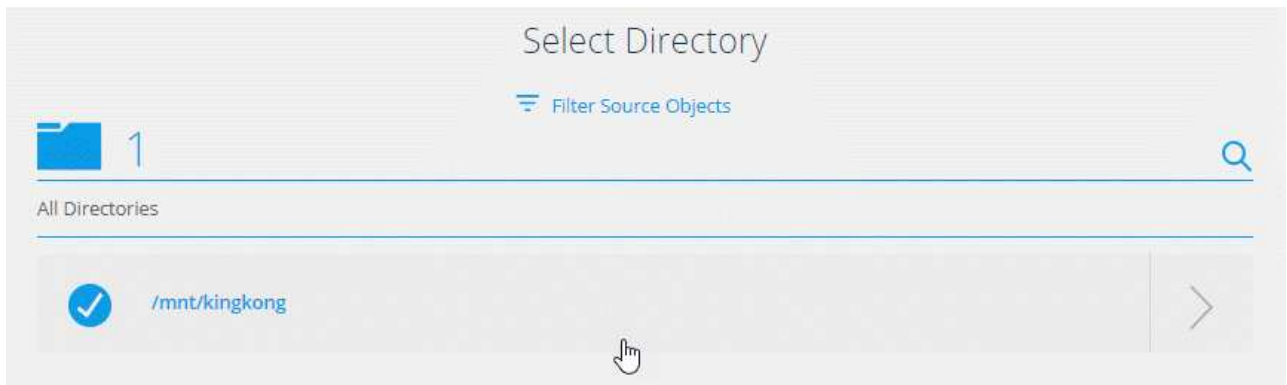
1. Haga clic en **Crear nueva sincronización**.
2. Arrastre y suelte **servidor NFS** a las ubicaciones de origen y destino o **Azure NetApp Files** a las ubicaciones de origen y destino y seleccione **Sí** para activar el cifrado de datos en vuelo.
3. Siga las indicaciones para crear la relación:
 -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

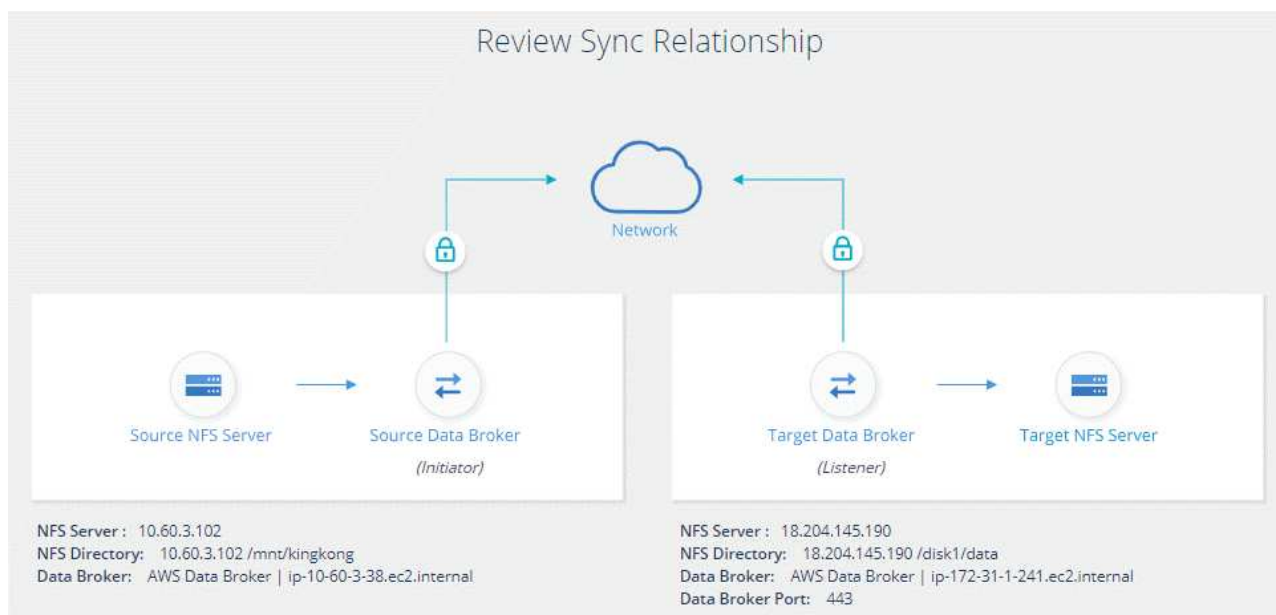


On-Prem Data Broker

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 eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ikp..."`

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. Suscríbese 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

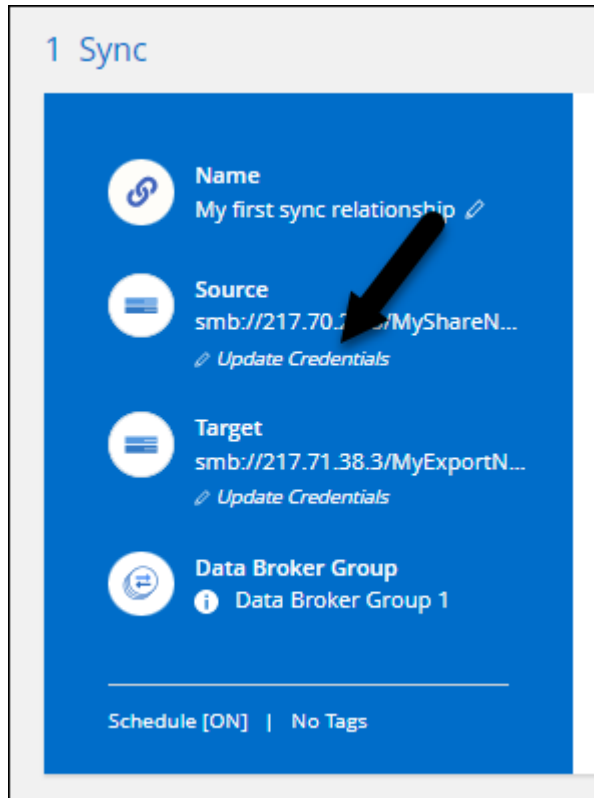
Puede actualizar el agente de datos con las credenciales más recientes del origen o destino en una relación de sincronización existente. La actualización de las credenciales puede ayudar si las políticas de seguridad requieren que actualice las credenciales de forma periódica.

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.

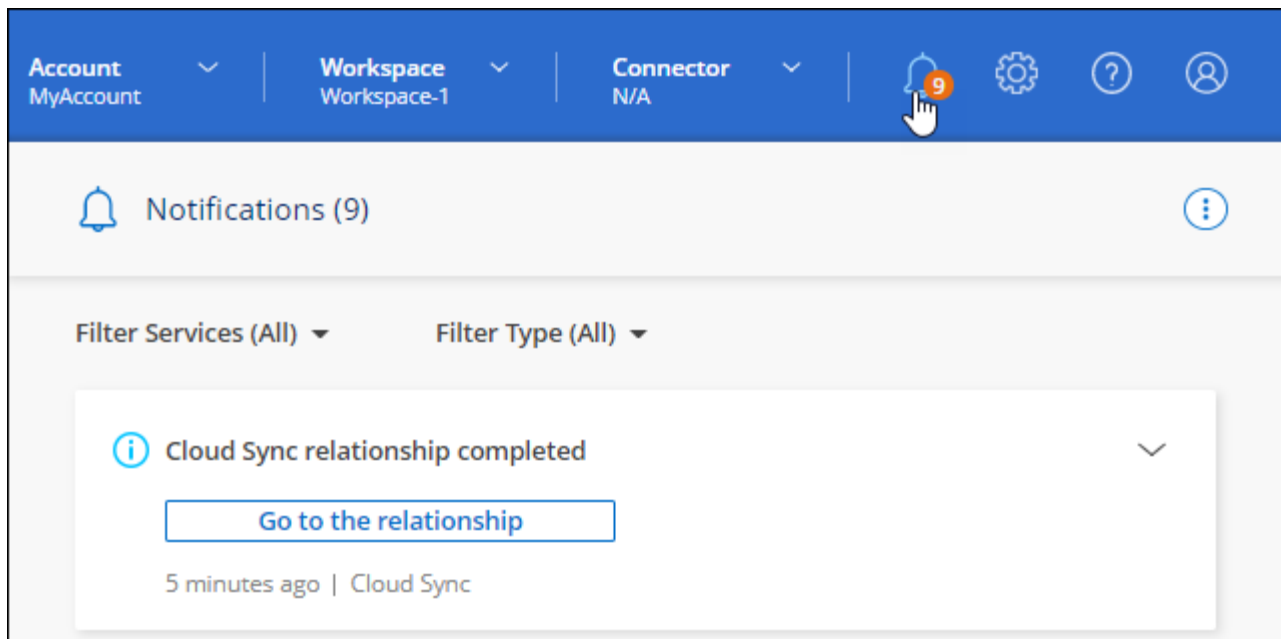
Si introdujo un dominio al crear la relación de sincronización, pero no introduce un dominio nuevo al actualizar las credenciales, Cloud Sync seguirá utilizando el dominio original que ha proporcionado.

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

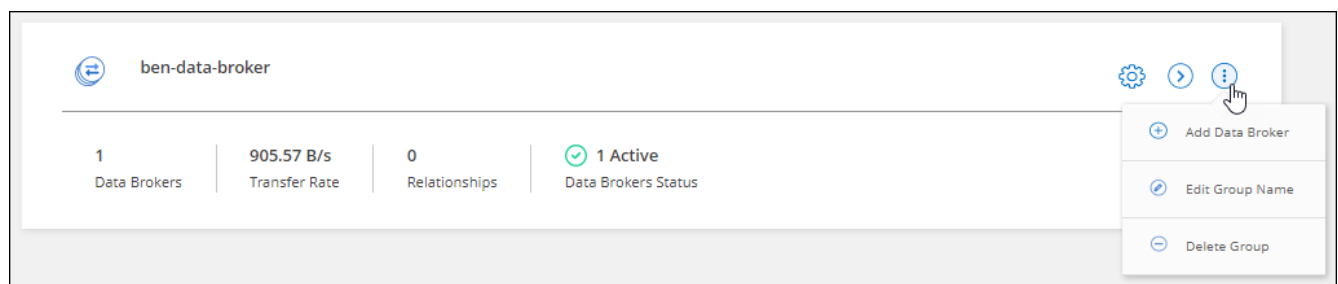
1. Haga clic en **Sincronizar > gestionar agentes de datos**.
2. Haga clic en **Agregar nuevo agente de datos**.
3. Siga las indicaciones para crear el Data broker.

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"](#)

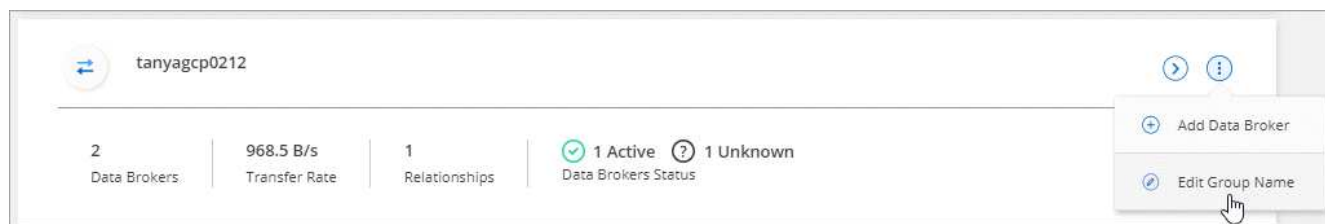
- "Instalar el agente de datos en un host Linux"

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.

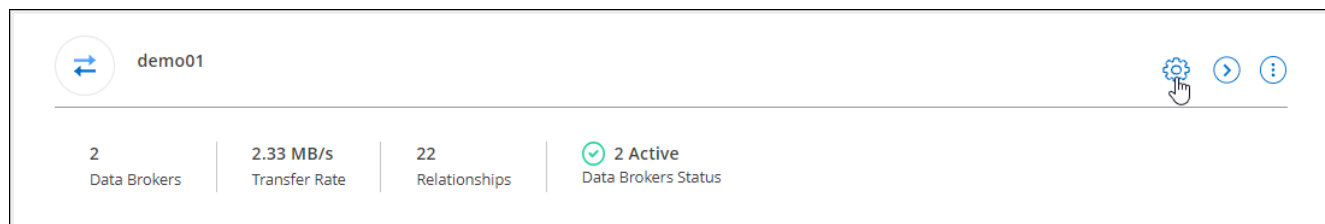
Configuración unificada

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.

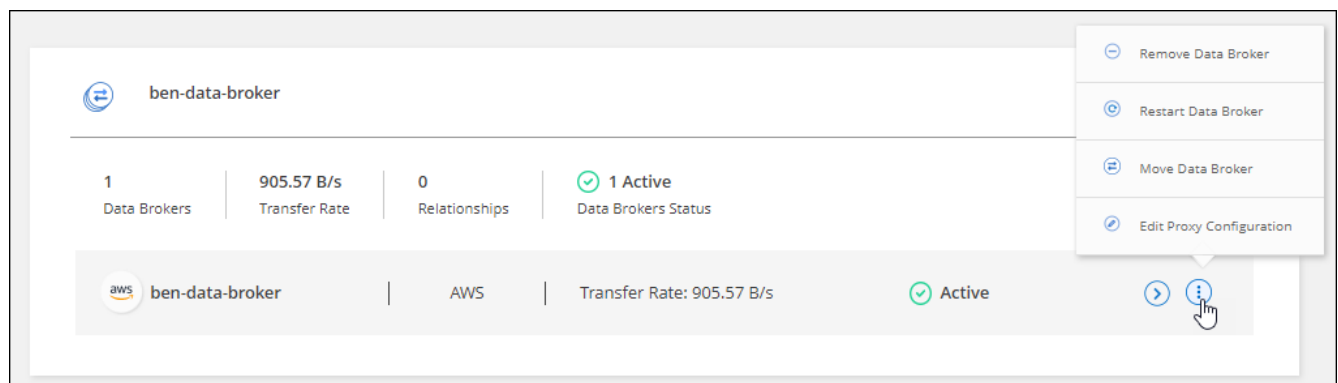
Por ejemplo, si un agente de datos ya no gestiona una relación de sincronización, puede moverla fácilmente a otro grupo que esté gestionando las relaciones de sincronización.

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 an information 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.

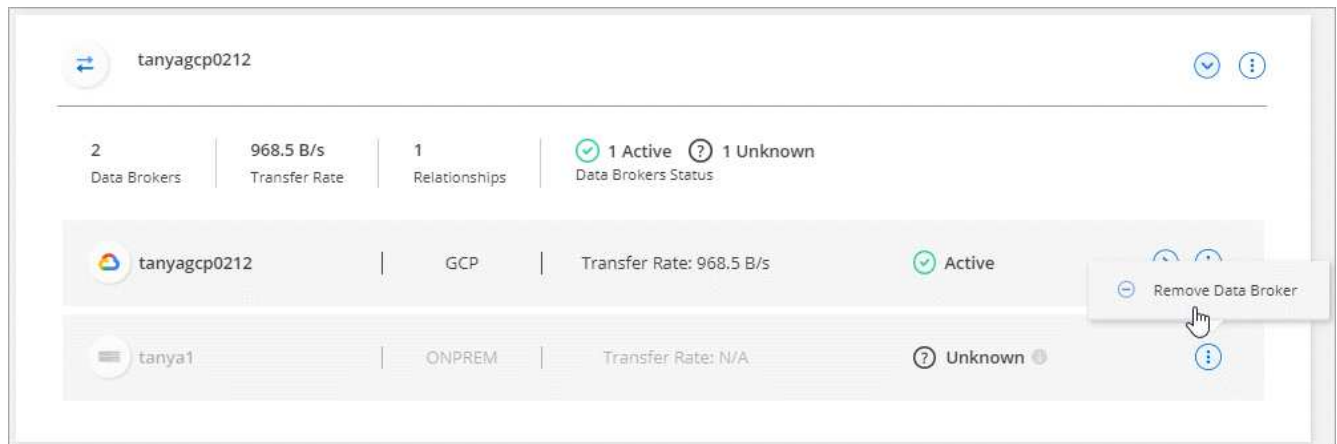
Esta acción solo elimina el agente de datos de los registros de Cloud Sync. Deberá eliminar manualmente el agente de datos y los recursos de cloud adicionales usted mismo.

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.

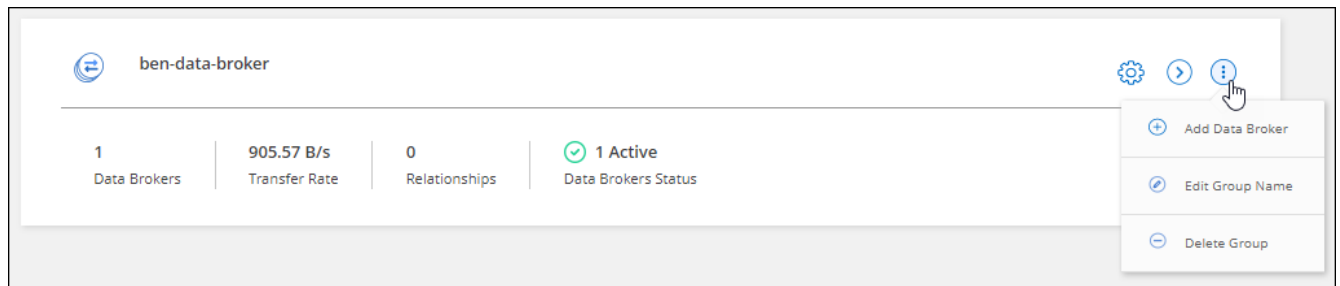
Eliminar un grupo de Data broker

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

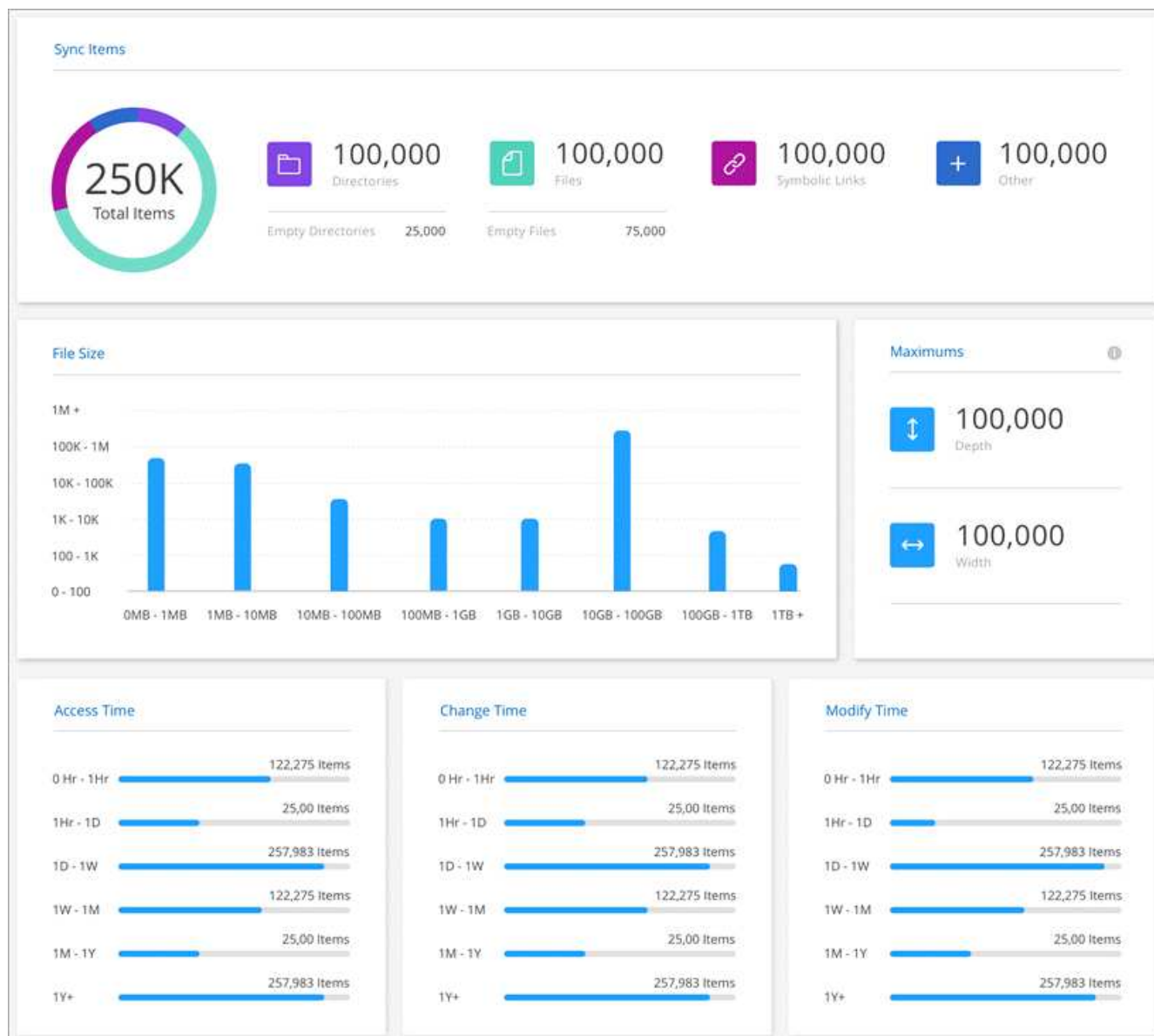
1. Haga clic en **Sincronizar > Informes**.

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

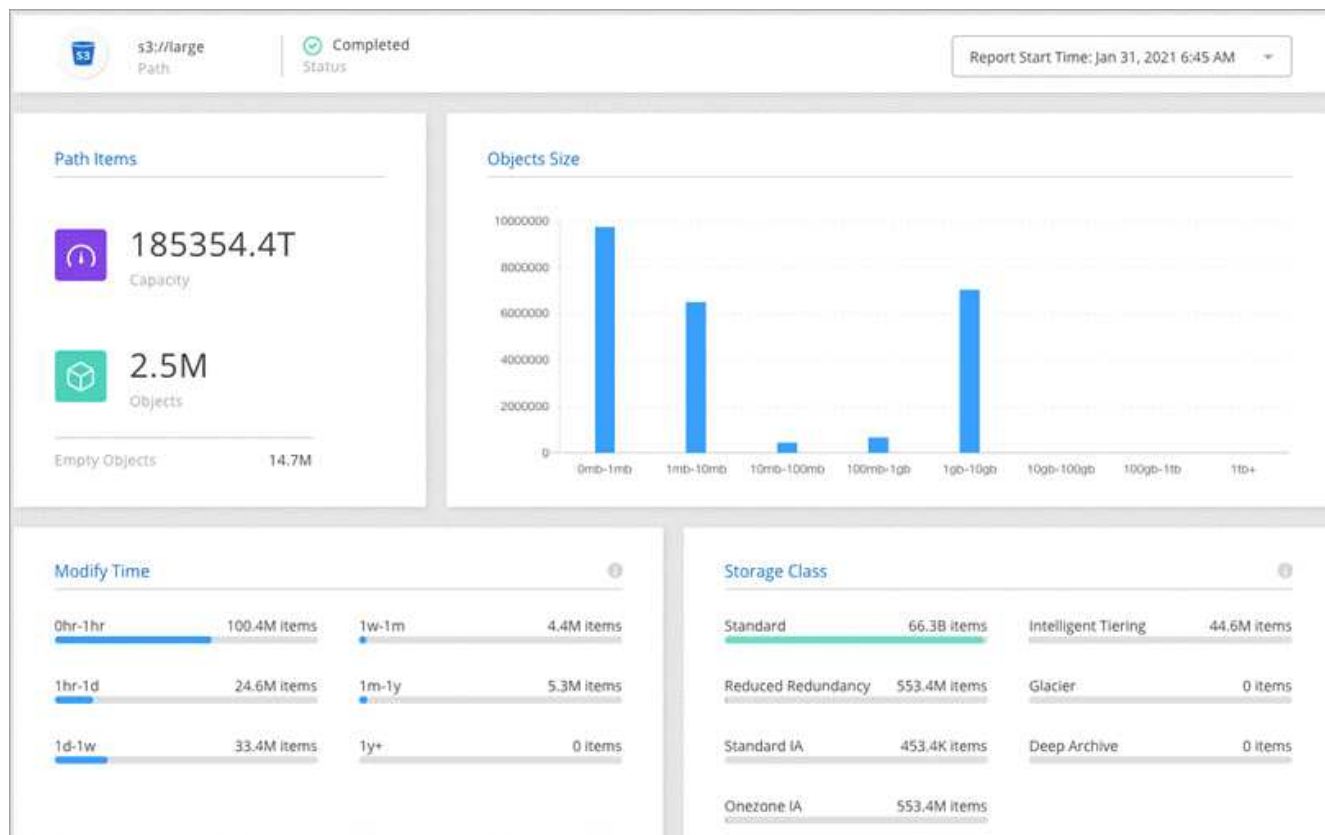
2. En la columna **acciones de Informes**, vaya a una ruta de acceso específica y haga clic en **Crear**, o haga clic en el menú de acciones y seleccione **Crear nuevo**.

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.

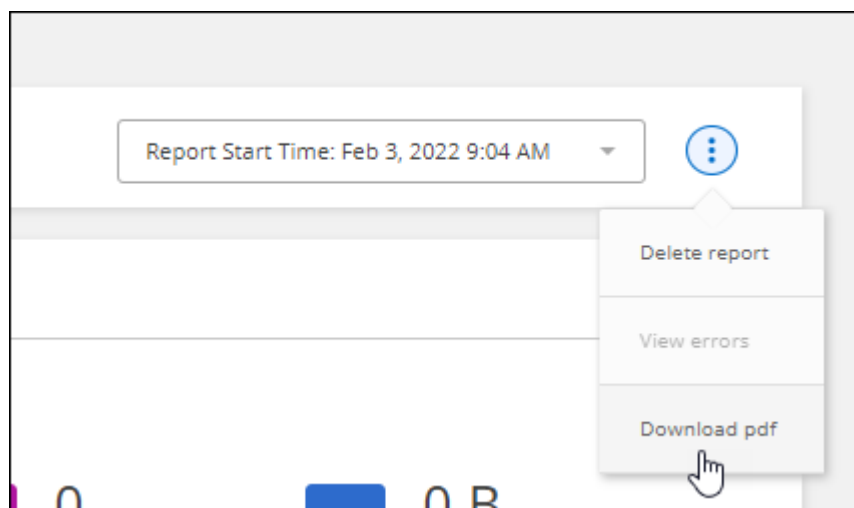


Descargando informes

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

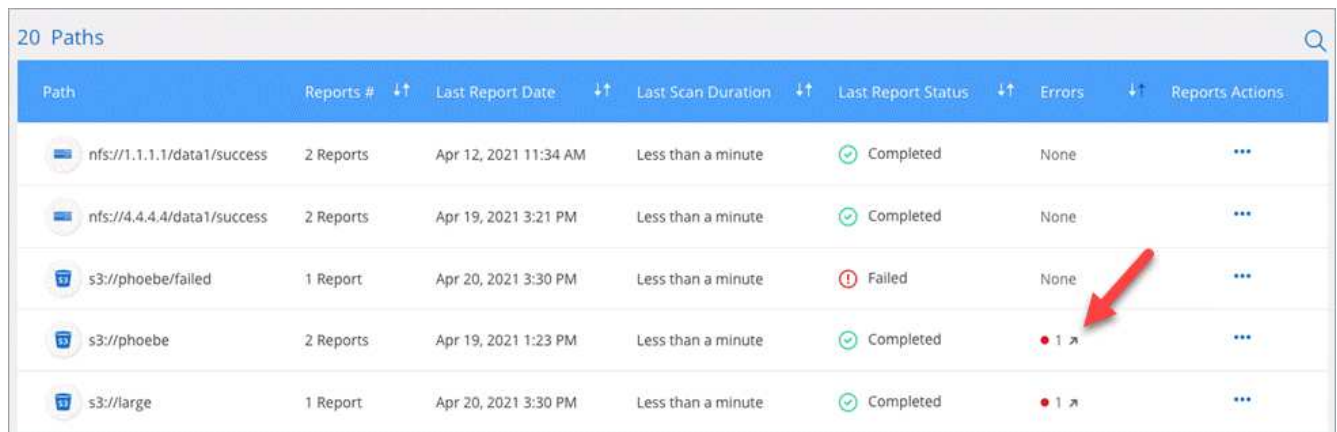
La tabla de rutas de acceso identifica si hay algún error en el informe más reciente. Un error identifica un problema que Cloud Sync enfrentó al analizar la ruta.

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.

API de Cloud Sync

Las funcionalidades Cloud Sync que están disponibles en la interfaz de usuario web también están disponibles mediante la API RESTful.

Primeros pasos

Para comenzar con la API de Cloud Sync, necesita obtener un token de usuario y su ID de cuenta de BlueXP. Deberá agregar el token y el ID de cuenta al encabezado de autorización cuando realice llamadas a la API.

Pasos

1. Obtenga un token de usuario de BlueXP de NetApp.

```
POST https://netapp-cloud-account.auth0.com/oauth/token
Header: Content-Type: application/json
Body:
{
  "username": "<user_email>",
  "scope": "profile",
  "audience": "https://api.cloud.netapp.com",
  "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",
  "grant_type": "password",
  "password": "<user_password>"
}
```



Si utiliza una cuenta de correo electrónico personal sin ID de cliente, puede utilizar el ID de cliente predeterminado "QC3AgHk6qdbmC7Yyr82ApBwaaJLwRrNO".

1. Obtenga su ID de cuenta de BlueXp.

```
GET https://api.cloudsync.netapp.com/api/accounts
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
```

Esta API devolverá una respuesta como la siguiente:

```
[
  {
    "accountId": "account-JeL97Ry3",
    "name": "Test"
  }
]
```

2. Agregue el identificador de usuario y el ID de cuenta en el encabezado de autorización de cada llamada de API.

ejemplo

El siguiente ejemplo muestra una llamada de API para crear un agente de datos en Microsoft Azure. Simplemente debería reemplazar `<user_token>` y `<accountId>` por el token y el ID que ha obtenido en los pasos anteriores.

```
POST https://api.cloudsync.netapp.com/api/data-brokers
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
Body: { "name": "databroker1", "type": "AZURE" }
```

¿Qué debo hacer cuando caduca el token?

El token de usuario de NetApp BlueXp tiene una fecha de vencimiento. Para actualizar el token, debe volver a llamar a la API desde el paso 1.

La respuesta de la API incluye un campo "expires_in" que indica cuándo caduca el token.

Referencia de API

Es posible acceder a la documentación para cada API de Cloud Sync en <https://api.cloudsync.netapp.com/docs>.

Uso de list API

Las API de la lista son API asíncronas, por lo que el resultado no devuelve de inmediato (por ejemplo: GET /data-brokers/{id}/list-nfs-export-folders y GET /data-brokers/{id}/list-s3-buckets). La única respuesta del servidor es el estado HTTP 202. Para obtener el resultado real, debe usar el GET /messages/client API.

Pasos

1. Llame a la API de lista que desea utilizar.
2. Utilice la GET /messages/client API para ver el resultado de la operación.
3. Utilice la misma API anexándola con el ID que acaba de recibir: GET `http://api.cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>`

Tenga en cuenta que el ID cambia cada vez que llama al GET /messages/client API.

ejemplo

Al llamar al list-s3-buckets API, los resultados no se devuelven inmediatamente:

```
GET http://api.cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

El resultado es el código de estado HTTP 202, lo que significa que el mensaje fue aceptado, pero aún no se ha procesado.

Para obtener el resultado de la operación, debe usar la siguiente API:

```
GET http://api.cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

El resultado es una matriz con un objeto que incluye un campo ID. El campo Id. Representa el último mensaje enviado por el servidor. Por ejemplo:

```
[
  {
    "header": {
      "requestId": "init",
      "clientId": "init",
      "agentId": "init"
    },
    "payload": {
      "init": {}
    },
    "id": "5801"
  }
]
```

Ahora haría la siguiente llamada a la API mediante el ID que acaba de recibir:

```
GET
http://api.cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

El resultado es un conjunto de mensajes. Dentro de cada mensaje hay un objeto de carga, que consiste en el nombre de la operación (como clave) y su resultado (como valor). Por ejemplo:

```
[
  {
    "payload": {
      "list-s3-buckets": [
        {
          "tags": [
            {
              "Value": "100$",
              "Key": "price"
            }
          ],
          "region": {
            "displayName": "US West (Oregon)",
            "name": "us-west-2"
          },
          "name": "small"
        }
      ]
    },
    "header": {
      "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",
      "clientId": "5beb032f548e6e35f4ed1ba9",
      "agentId": "5bed61f4489fb04e34a9aac6"
    },
    "id": "5802"
  }
]
```


Conceptos

Información general sobre las licencias

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.

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

Suscripción a Marketplace

Al suscribirse al servicio de Cloud Sync de AWS o Azure, usted podrá pagar por horas o pagar anualmente. ["Puede suscribirse a través de AWS o Azure"](#), en función de dónde desee facturar.

Suscripción cada hora

Con una suscripción de pago por horas por uso, se factura por horas en función del número de relaciones de sincronización que se haya creado.

- ["Ver los precios en Azure"](#)
- ["Vea los precios de pago por uso en AWS"](#)

Suscripción anual

Una suscripción anual proporciona una licencia para 20 relaciones de sincronización que usted paga por adelantado. Si va por encima de 20 relaciones de sincronización y se ha suscrito a AWS, pagará por las relaciones adicionales por horas.

["Ver precios anuales en AWS"](#)

De NetApp

Otra forma de pagar por las relaciones de sincronización es mediante la compra de licencias directamente a NetApp. Cada licencia permite crear hasta 20 relaciones de sincronización.

Puede usar estas licencias con una suscripción a AWS o Azure. 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.

["Aprenda a comprar licencias y a añadirlas a cloud Sincr"](#).

Términos de licencia

Los clientes que adquieran una licencia propia (BYOL) para el servicio Cloud Sync deben conocer las limitaciones asociadas con el derecho de la licencia.

- Los clientes tienen derecho a aprovechar la licencia BYOL por un período que no supere un año a partir de la fecha de entrega.

- Los clientes tienen derecho a aprovechar la licencia BYOL para establecer y no superar un total de 20 conexiones individuales entre un origen y un destino (cada una de ellas una “relación de sincronización”).
- El derecho de un cliente expira al finalizar el plazo de un año para la licencia, independientemente de si el cliente ha alcanzado la limitación de relación de sincronización de 20.
- En el caso de que el Cliente decida renovar su licencia, las relaciones de sincronización no utilizadas asociadas a la concesión de licencia anterior NO se reviertan a la renovación de la licencia.

Privacidad de datos

NetApp no tiene acceso a ninguna credencial que proporcione mientras utiliza el servicio Cloud Sync. Las credenciales se almacenan directamente en el equipo de Data broker, que reside en la red.

Según la configuración seleccionada, Cloud Sync puede pedirle credenciales cuando cree una nueva relación. Por ejemplo, cuando se configura una relación que incluye un servidor SMB o cuando se implementa el agente de datos en AWS.

Estas credenciales siempre se guardan directamente en el propio agente de datos. El agente de datos reside en un equipo de su red, ya sea en las instalaciones o en su cuenta de cloud. NetApp nunca pone a disposición de estas credenciales.

Las credenciales se cifran localmente en la máquina de corredores de datos utilizando HashiCorp Vault.

Preguntas técnicas frecuentes sobre Cloud Sync

Estas preguntas frecuentes pueden ayudar si sólo está buscando una respuesta rápida a una pregunta.

Primeros pasos

Las siguientes preguntas tratan sobre los primeros pasos con Cloud Sync.

¿Cómo funciona Cloud Sync?

Cloud Sync utiliza el software de intermediarios de datos de NetApp para sincronizar los datos de un origen con un destino (esto se denomina *Sync Relationship*).

Un grupo de Data broker controla las relaciones de sincronización entre sus orígenes y destinos. Después de configurar una relación de sincronización, Cloud Sync analiza su sistema de origen y lo divide en varios flujos de replicación para enviar los datos de destino seleccionados.

Después de la copia inicial, el servicio sincroniza los datos modificados con la programación que se haya establecido.

¿Cómo funciona la prueba gratuita de 14 días?

La prueba gratuita de 14 días se inicia cuando se inscriba en el servicio Cloud Sync. No está sujeto a los cargos por NetApp relacionados con las relaciones con Cloud Sync que cree durante 14 días. Sin embargo, sigue siendo aplicable todo coste por recursos para los agentes de datos que realice la puesta en marcha.

¿Cuánto cuesta Cloud Sync?

Hay dos tipos de costos asociados con el uso de Cloud Sync: Cargos por servicios y cargos por recursos.

cargos por servicio

Para los precios de pago por uso, los cargos del servicio Cloud Sync se cobran por hora según el número de relaciones de sincronización que cree.

- ["Vea los precios de pago por uso en AWS"](#)
- ["Ver precios anuales en AWS"](#)
- ["Ver los precios en Azure"](#)

Las licencias de Cloud Sync también están disponibles a través de su representante de NetApp. Cada licencia activa 20 relaciones de sincronización durante 12 meses.

["Más información sobre las licencias"](#).



Las relaciones de Cloud Sync son gratuitas para Cloud Volumes Service y Azure NetApp Files.

gastos de recursos

Las cargas de recursos están relacionadas con los costes de informática y almacenamiento para ejecutar el agente de datos en el cloud.

¿Cómo se factura Cloud Sync?

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, lo que le permite pagar por uso o anualmente. La segunda opción consiste en comprar licencias directamente a NetApp.

¿Puedo usar Cloud Sync fuera del cloud?

Sí, puede usar Cloud Sync en una arquitectura que no sea de cloud. El origen y el destino pueden residir en las instalaciones, por lo que puede hacerlo el software de agente de datos.

Tenga en cuenta los siguientes puntos clave sobre el uso de Cloud Sync fuera del cloud:

- Un grupo de Data broker necesita una conexión a Internet para comunicarse con el servicio Cloud Sync.
- Si no adquiere una licencia directamente a NetApp, necesitará una cuenta de AWS o Azure para la facturación del servicio de PAYGO Cloud Sync.

¿Cómo puedo acceder a Cloud Sync?

Cloud Sync está disponible en el sitio web de BlueXP en la ficha **Sync**.

¿Qué es un grupo de agentes de datos?

Cada agente de datos pertenece a un grupo de Data broker. La agrupación conjunta de gestores de datos ayuda a mejorar el rendimiento de las relaciones de sincronización.

Orígenes y objetivos compatibles

Las siguientes preguntas relacionadas con el origen y los destinos que se admiten en una relación de sincronización.

¿Qué orígenes y destinos es compatible con Cloud Sync?

Cloud Sync admite muchos tipos distintos de relaciones de sincronización. ["Vea toda la lista"](#).

¿Qué versiones de NFS y SMB es compatible Cloud Sync?

Cloud Sync admite NFS versión 3 y posteriores, y SMB versión 1 y posteriores.

["Más información sobre los requisitos de sincronización"](#).

Cuando Amazon S3 es el objetivo, ¿se pueden organizar los datos en niveles en un tipo de almacenamiento S3 específico?

Sí, puede elegir una clase de almacenamiento S3 específica cuando AWS S3 es el destino:

- Estándar (esta es la clase predeterminada)
- Organización en niveles inteligente
- Acceso Estándar-poco frecuente
- Una Zona de acceso poco frecuente
- Glacier Deep Archive
- Recuperación de Glacier flexible
- Recuperación instantánea de Glacier

¿Qué pasa con los niveles de almacenamiento para el almacenamiento de Azure Blob?

Puede elegir un nivel de almacenamiento específico de Azure Blob cuando un contenedor Blob es el destino:

- Almacenamiento en caliente
- Almacenamiento en frío

¿Admite niveles de almacenamiento de Google Cloud?

Sí, puede elegir una clase de almacenamiento específica cuando un bucket de Google Cloud Storage es el destino:

- Estándar
- Nearline
- Coldline
- Archivado

Redes

Las siguientes preguntas hacen referencia a los requisitos de red de Cloud Sync.

¿Cuáles son los requisitos de red de Cloud Sync?

El entorno de Cloud Sync requiere que un grupo de intermediarios de datos esté conectado con el origen y el destino a través del protocolo o la API de almacenamiento de objetos seleccionados (Amazon S3, Azure Blob, IBM Cloud Object Storage).

Además, un grupo de agentes de datos necesita una conexión a Internet saliente a través del puerto 443 para que pueda comunicarse con el servicio Cloud Sync y ponerse en contacto con otros servicios y repositorios.

Si quiere más información, ["revise los requisitos de red"](#).

¿Puedo utilizar un servidor proxy con el agente de datos?

Sí.

Cloud Sync admite servidores proxy con o sin autenticación básica. Si especifica un servidor proxy al implementar un agente de datos, todo el tráfico HTTP y HTTPS del agente de datos se enrutará a través del proxy. Tenga en cuenta que el tráfico no HTTP como NFS o SMB no se puede enrutar a través de un servidor proxy.

La única limitación del servidor proxy se produce cuando se utiliza el cifrado de datos en tránsito con una relación de sincronización de NFS o Azure NetApp Files. Los datos cifrados se envían a través de HTTPS y no se pueden enrutar a través de un servidor proxy.

Sincronización de datos

Las siguientes preguntas se refieren a cómo funciona la sincronización de datos.

¿con qué frecuencia se produce la sincronización?

La programación predeterminada se define para la sincronización diaria. Después de la sincronización inicial, puede:

- Modifique la programación de sincronización con el número de días, horas o minutos que desee
- Deshabilite la programación de sincronización
- Eliminar la programación de sincronización (no se perderán datos; solo se eliminará la relación de sincronización)

¿Cuál es el programa de sincronización mínimo?

Puede programar una relación para que se sincronice datos con una frecuencia de hasta cada 1 minuto.

¿Vuelve a intentar el grupo de Data broker cuando un archivo no se puede sincronizar? ¿o se agota el tiempo de espera?

Un grupo de Data broker no se agotó cuando un solo archivo no se transfiere. En su lugar, el grupo de agentes de datos reintenta 3 veces antes de omitir el archivo. El valor de reintento se puede configurar en la configuración de una relación de sincronización.

["Aprenda a cambiar la configuración de una relación de sincronización"](#).

¿y si tengo un conjunto de datos muy grande?

Si un único directorio contiene 600,000 archivos o más, [contact US](#) para que podamos ayudarle a configurar el grupo de Data broker para manejar la carga útil. Es posible que necesitemos agregar memoria adicional al grupo de intermediarios de datos.

Tenga en cuenta que no hay límite en el número total de archivos del punto de montaje. La memoria adicional es necesaria para directorios grandes con 600,000 archivos o más, independientemente de su nivel en la jerarquía (directorio superior o subdirectorio).

Seguridad

Las siguientes preguntas están relacionadas con la seguridad.

¿es Cloud Sync seguro?

Sí. Toda la conectividad de redes del servicio Cloud Sync se realiza mediante "[Amazon simple Queue Service \(SQS\)](#)".

Toda la comunicación entre el grupo de agentes de datos y Amazon S3, Azure Blob, Google Cloud Storage y IBM Cloud Object Storage se realiza mediante el protocolo HTTPS.

Si utiliza Cloud Sync con sistemas en las instalaciones (origen o destino), puede ver algunas opciones de conectividad recomendadas:

- Una conexión de AWS Direct Connect, Azure ExpressRoute o Google Cloud Interconnect, que no es enrutada por Internet (y solo puede comunicarse con las redes cloud que especifique).
- Una conexión VPN entre el dispositivo de puerta de enlace local y el redes cloud
- Para obtener una transferencia de datos más segura con bloques S3, almacenamiento de Azure Blob o Google Cloud Storage, se puede establecer un Amazon Private S3 Endpoint, extremos de servicio de red virtual de Azure o Google Private Access.

Cualquiera de estos métodos establece una conexión segura entre los servidores NAS locales y el grupo de agentes de datos Cloud Sync.

¿los datos están cifrados por Cloud Sync?

- Cloud Sync admite el cifrado de datos en tiempo real entre los servidores NFS de origen y de destino. ["Leer más"](#).
- Para SMB, Cloud Sync admite datos SMB 3.0 y 3.11 que haya cifrado en el servidor. Cloud Sync copia los datos cifrados desde el origen al destino donde permanecen cifrados los datos.

Cloud Sync no puede cifrar los propios datos de SMB.

- Cuando un bloque de Amazon S3 es el destino de una relación de sincronización, puede elegir si habilitar el cifrado de datos mediante el cifrado AWS KMS o el cifrado AES-256.

Permisos

Las siguientes preguntas se refieren a los permisos de datos.

¿los permisos de datos del SMB se sincronizan con la ubicación de destino?

Es posible configurar Cloud Sync para que se conserven las listas de control de acceso (ACL) entre un recurso compartido de SMB de origen y un recurso compartido de SMB de destino, así como desde un recurso compartido de SMB de origen al almacenamiento de objetos (excepto ONTAP S3).



Cloud Sync no admite la copia de ACL de almacenamiento de objetos en recursos compartidos de SMB.

["Aprenda a copiar ACL entre recursos compartidos de SMB".](#)

¿los permisos de datos NFS se sincronizan con la ubicación de destino?

Cloud Sync copia automáticamente los permisos de NFS entre servidores NFS de la siguiente forma:

- NFS versión 3: Cloud Sync copia los permisos y el propietario del grupo de usuarios.
- NFS versión 4: Cloud Sync copia las ACL.

Metadatos de almacenamiento de objetos

Cloud Sync copia los metadatos de almacenamiento de objetos del origen al destino para los siguientes tipos de relaciones de sincronización:

- Amazon S3 → Amazon S3 esta 1 de
- Amazon S3 → StorageGRID
- StorageGRID → Amazon S3
- StorageGRID → StorageGRID
- StorageGRID → Google Cloud Storage
- Google Cloud Storage → StorageGRID versión 1
- Google Cloud Storage → IBM Cloud Object Storage este 1
- Google Cloud Storage → Amazon S3 esta 1
- Amazon S3 → Google Cloud Storage
- IBM Cloud Object Storage → Google Cloud Storage
- StorageGRID → almacenamiento de objetos en cloud de IBM
- Almacenamiento de objetos en cloud de IBM → StorageGRID
- Almacenamiento de objetos en cloud de IBM → almacenamiento de objetos en cloud de IBM

Hacia 1 para estas relaciones de sincronización, debe hacerlo ["Active la opción Copiar para objetos cuando cree la relación de sincronización"](#).

Rendimiento

Las siguientes preguntas están relacionadas con el rendimiento de Cloud Sync.

¿Qué representa el indicador de progreso de una relación de sincronización?

La relación de sincronización muestra el rendimiento del adaptador de red del grupo de Data broker. Si aceleró el rendimiento de sincronización mediante el uso de varios agentes de datos, el rendimiento será la

suma de todo el tráfico. Este rendimiento se actualiza cada 20 segundos.

Estoy experimentando problemas de rendimiento. ¿podemos limitar el número de transferencias simultáneas?

Si tiene archivos muy grandes (múltiples TIBs cada uno), puede tardar mucho tiempo en completar el proceso de transferencia y el rendimiento puede verse afectado.

Limitar el número de transferencias simultáneas puede ser de ayuda. [Mailto:ng-cloudsync-support@netapp.com](mailto:ng-cloudsync-support@netapp.com)[Contacte con nosotros para obtener ayuda].

¿por qué estoy experimentando un bajo rendimiento con Azure NetApp Files?

Al sincronizar datos con o desde Azure NetApp Files, es posible que experimente errores y problemas de rendimiento si el nivel de servicio del disco es estándar.

Cambie el nivel de servicio a Premium o Ultra para mejorar el rendimiento de la sincronización.

["Obtenga más información acerca de los niveles de servicio y el rendimiento de Azure NetApp Files"](#).

¿por qué estoy experimentando un bajo rendimiento con Cloud Volumes Service para AWS?

Al sincronizar datos con un volumen de cloud o desde este, es posible que experimente errores y problemas de rendimiento si el nivel de rendimiento del volumen de cloud es estándar.

Cambie el nivel de servicio a Premium o Extreme para mejorar el rendimiento de la sincronización.

¿Cuántos agentes de datos son necesarios en un grupo?

Al crear una nueva relación, comienza con un solo agente de datos de un grupo (a menos que haya seleccionado un agente de datos existente que pertenezca a una relación de sincronización acelerada). En muchos casos, un único agente de datos puede satisfacer los requisitos de rendimiento de una relación de sincronización. Si no lo hace, puede acelerar el rendimiento de la sincronización añadiendo agentes de datos adicionales al grupo. Pero primero debe comprobar otros factores que pueden afectar al rendimiento de la sincronización.

El rendimiento de la transferencia de datos puede afectar múltiples factores. El rendimiento general de la sincronización puede verse afectado debido al ancho de banda de la red, la latencia y la topología de la red, así como las especificaciones del equipo virtual del agente de datos y el rendimiento del sistema de almacenamiento. Por ejemplo, un solo intermediario de datos de un grupo puede alcanzar los 100 MB/s, mientras que el rendimiento de disco en el destino sólo puede permitir 64 MB/s. Como resultado, el grupo de agentes de datos sigue intentando copiar los datos, pero el destino no puede satisfacer el rendimiento del grupo de agentes de datos.

Por lo tanto, asegúrese de comprobar el rendimiento de la red y del disco en el destino.

A continuación, puede plantearse acelerar el rendimiento de sincronización añadiendo agentes de datos adicionales a un grupo para compartir la carga de dicha relación. ["Descubra cómo acelerar el rendimiento de la sincronización"](#).

Eliminar cosas

Las siguientes preguntas tratan de eliminar relaciones de sincronización y datos de orígenes y destinos.

¿Qué sucede si elimino mi relación con Cloud Sync?

Al eliminar una relación se detienen todos los datos futuros y se termina el pago. Todos los datos que se sincronizaron con el destino siguen siendo tal cual.

¿Qué ocurre si se elimina algo de mi servidor de origen? ¿se ha eliminado del objetivo también?

De forma predeterminada, si tiene una relación de sincronización activa, el elemento eliminado en el servidor de origen no se eliminará del destino durante la siguiente sincronización. Pero hay una opción en la configuración de sincronización para cada relación, donde puede definir que Cloud Sync eliminará los archivos de la ubicación de destino si se eliminaron del origen.

["Aprenda a cambiar la configuración de una relación de sincronización".](#)

¿Qué sucede si elimino algo de mi destino? ¿se ha eliminado de mi fuente también?

Si se elimina un elemento del destino, no se eliminará del origen. La relación es unidireccional, desde la fuente hasta el objetivo. En el siguiente ciclo de sincronización, Cloud Sync compara el origen con el destino, identifica que falta el elemento y Cloud Sync lo copia de nuevo del origen al destino.

Resolución de problemas

["Base de conocimientos de NetApp: Preguntas frecuentes de Cloud Sync: Soporte y solución de problemas"](#)

Análisis en profundidad de los agentes de datos

La siguiente pregunta se refiere al agente de datos.

¿puede explicar la arquitectura del agente de datos?

Claro. Estos son los puntos más importantes:

- Data broker es una aplicación node.js que se ejecuta en un host Linux.
- Cloud Sync implementa el agente de datos de la siguiente manera:
 - AWS: Desde una plantilla AWS CloudFormation
 - Azure: Desde Azure Resource Manager
 - Google: De Google Cloud Deployment Manager
 - Si utiliza su propio host Linux, debe instalar manualmente el software
- El software Data broker se actualiza automáticamente a la última versión.
- El agente de datos utiliza AWS SQS como un canal de comunicación fiable y seguro, y para el control y la supervisión. SQS también proporciona una capa de persistencia.
- Puede agregar agentes de datos adicionales a un grupo para aumentar la velocidad de transferencia y agregar una alta disponibilidad. Hay resiliencia de servicios si un agente de datos falla.

Conocimiento y apoyo

Regístrese para recibir soporte

Antes de poder abrir un caso de soporte con el soporte técnico de NetApp, debe añadir una cuenta del sitio de soporte de NetApp (NSS) a BlueXP y, a continuación, registrarse para recibir soporte.

Soporte para soluciones de proveedores cloud

Para obtener asistencia técnica sobre las siguientes soluciones de proveedores de nube que ha integrado en BlueXP, consulte "obtención de ayuda" en la documentación de BlueXP para ese producto.

- ["Amazon FSX para ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Cloud Volumes Service para Google Cloud"](#)

Información general del registro de soporte

Existen dos formas de registro para activar el derecho de asistencia:

- Registro de la suscripción al soporte de ID de cuenta de BlueXP (número de serie de 20 dígitos xxxx960xxxxx que se encuentra en la página Recursos de asistencia técnica de BlueXP).

Esto sirve como su ID de suscripción de soporte único para cualquier servicio dentro de BlueXP. Debe registrarse cada suscripción de asistencia técnica a nivel de cuenta de BlueXP.

- Registrar los números de serie de Cloud Volumes ONTAP asociados con una suscripción en el mercado de su proveedor de cloud (estos son números de serie de 20 dígitos 909201xxxxxxxx).

Estos números de serie se denominan comúnmente *PAYGO serial Numbers* y son generados por BlueXP en el momento de la implementación de Cloud Volumes ONTAP.

El registro de ambos tipos de números de serie permite funcionalidades, como abrir tickets de soporte y la generación automática de casos.

La forma de registrarse depende de si es un cliente o partner nuevo o existente.

- Cliente o partner existente

Como cliente o partner de NetApp, puede usar su cuenta de SSO del sitio de soporte de NetApp (NSS) para realizar estos registros anteriormente. En el Panel de soporte, BlueXP proporciona una página **NSS Management** en la que puede agregar su cuenta NSS. Una vez que agregue su cuenta NSS, BlueXP registra automáticamente estos números de serie.

[Aprenda a añadir su cuenta de NSS.](#)

- Nuevo en NetApp

Si es totalmente nuevo en NetApp, debe completar un registro una vez del número de serie de su ID de cuenta de BlueXP en el sitio de registro de soporte de NetApp. Una vez completado este registro y cree una nueva cuenta de NSS, puede utilizar esta cuenta en BlueXP para registrarse automáticamente en el futuro.

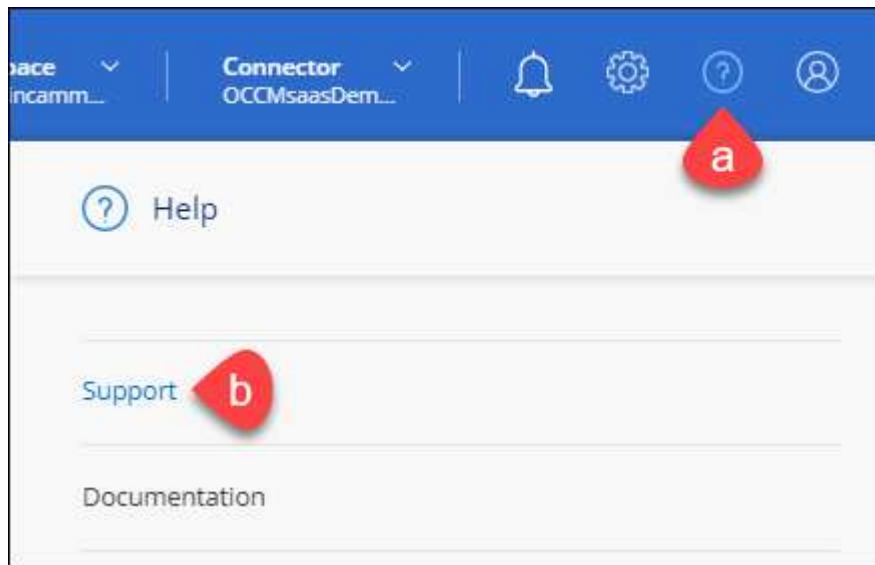
Agregue una cuenta NSS a BlueXP

La consola de soporte le permite añadir y gestionar sus cuentas de la página de soporte de NetApp para utilizarlas con BlueXP.

- Si tiene una cuenta de nivel de cliente, puede añadir una o varias cuentas de NSS.
- Si tiene una cuenta de partner o distribuidor, puede añadir una o varias cuentas de NSS, pero no se podrán añadir junto con las cuentas de nivel de cliente.

Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda y seleccione **Soporte**.



2. Haga clic en **Administración de NSS > Agregar cuenta de NSS**.
3. Cuando se le pregunte, haga clic en **continuar** para que se le redirija a una página de inicio de sesión de Microsoft.

NetApp utiliza Microsoft Azure Active Directory como proveedor de identidades para servicios de autenticación específicos para soporte y licencias.

4. En la página de inicio de sesión, proporcione su dirección de correo electrónico registrada en el sitio de soporte de NetApp y contraseña para realizar el proceso de autenticación.

Estas acciones permiten a BlueXP utilizar su cuenta NSS para cosas como descargas de licencias, verificación de actualizaciones de software y futuros registros de soporte.

Tenga en cuenta lo siguiente:

- La cuenta NSS debe ser una cuenta de nivel de cliente (no una cuenta de invitado o temporal). Puede tener varias cuentas de NSS en el nivel del cliente.
- Sólo puede haber una cuenta NSS si esa cuenta es una cuenta de nivel de partner. Si intenta agregar cuentas de NSS de nivel de cliente y existe una cuenta de nivel de partner, obtendrá el siguiente mensaje de error:

"El tipo de cliente NSS no está permitido para esta cuenta, ya que ya hay usuarios NSS de tipo diferente."

Lo mismo sucede si tiene cuentas de NSS de nivel de cliente preexistentes e intenta añadir una cuenta de nivel de partner.

- Después de iniciar sesión correctamente, NetApp almacenará el nombre de usuario de NSS.

Se trata de un ID generado por el sistema que se asigna a su correo electrónico. En la página **NSS Management**, puede mostrar su correo electrónico desde **...** de windows

- Si alguna vez necesita actualizar sus tokens de credenciales de inicio de sesión, también hay una opción **Actualizar credenciales** en la **...** de windows

Con esta opción se le solicita que vuelva a iniciar sesión. Tenga en cuenta que el token de estas cuentas caduca después de 90 días. Se enviará una notificación para avisarle de ello.

Regístrese en NetApp

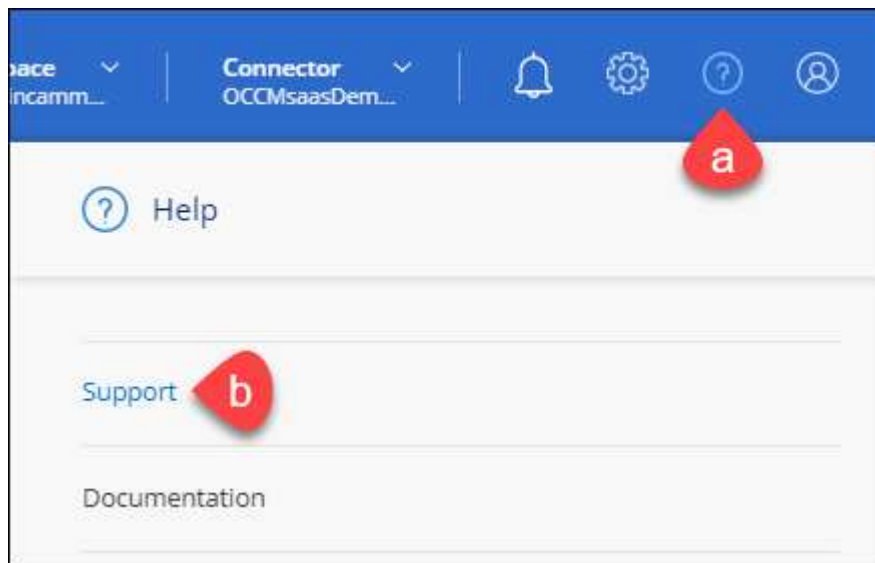
La forma de registrarse para recibir soporte de NetApp depende de si ya tiene una cuenta del sitio de soporte de NetApp (NSS).

Cliente existente con una cuenta de NSS

Si es cliente de NetApp con una cuenta de NSS, solo tiene que registrarse para recibir soporte a través de BlueXP.

Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda y seleccione **Soporte**.



2. Si aún no lo ha hecho, agregue su cuenta NSS a BlueXP.
3. En la página **Recursos**, haga clic en **Registrar para asistencia**.



96044890544097618700
Account serial number



Not Registered
Support Registration

[Register for Support](#)

Cliente existente pero no cuenta NSS

Si ya es cliente de NetApp con licencias y números de serie existentes pero *no* cuenta de NSS, solo tiene que crear una cuenta de NSS.

Pasos

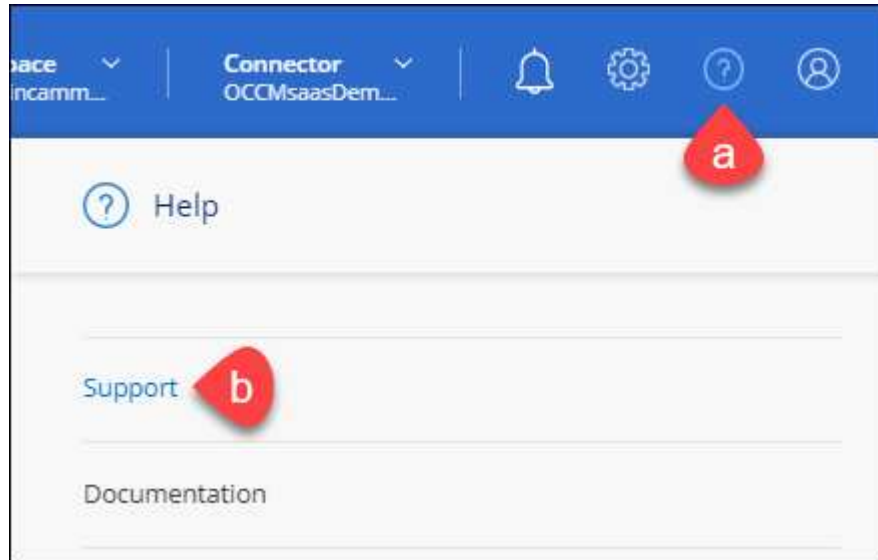
1. Complete el para crear una cuenta en la página de soporte de NetApp "[Formulario de registro de usuarios del sitio de soporte de NetApp](#)"
 - a. Asegúrese de seleccionar el nivel de usuario adecuado, que normalmente es **Cliente/Usuario final de NetApp**.
 - b. Asegúrese de copiar el número de serie de la cuenta BlueXP (960xxxx) utilizado anteriormente para el campo de número de serie. Esto agilizará el procesamiento de la cuenta.

Totalmente nuevo en NetApp

Si es totalmente nuevo en NetApp y no tiene una cuenta de NSS, siga cada paso que se indica a continuación.

Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda y seleccione **Soporte**.



2. Busque el número de serie de su ID de cuenta en la página Support Registration.



96044890544097618700
Account serial number



Not Registered
Support Registration

Go to [NSS Management](#) tab to add an NSS account

3. Vaya a. "[Sitio de registro de soporte de NetApp](#)" Y seleccione **no soy un cliente registrado de NetApp**.
4. Rellene los campos obligatorios (aquellos con asteriscos rojos).

5. En el campo **línea de productos**, seleccione **Cloud Manager** y, a continuación, seleccione el proveedor de facturación correspondiente.
6. Copie el número de serie de su cuenta desde el paso 2 anterior, complete la comprobación de seguridad y confirme que ha leído la Política de privacidad de datos global de NetApp.

Se envía inmediatamente un correo electrónico al buzón de correo para finalizar esta transacción segura. Asegúrese de comprobar sus carpetas de spam si el correo electrónico de validación no llega en pocos minutos.

7. Confirme la acción desde el correo electrónico.

Confirmar envía su solicitud a NetApp y recomienda que cree una cuenta en la página de soporte de NetApp.

8. Complete el para crear una cuenta en la página de soporte de NetApp "[Formulario de registro de usuarios del sitio de soporte de NetApp](#)"
 - a. Asegúrese de seleccionar el nivel de usuario adecuado, que normalmente es **Cliente/Usuario final de NetApp**.
 - b. Asegúrese de copiar el número de serie de la cuenta (960xxxx) utilizado anteriormente para el campo de número de serie. Esto agilizará el procesamiento de la cuenta.

Después de terminar

NetApp debería ponerse en contacto con usted durante este proceso. Este es un ejercicio de incorporación puntual para nuevos usuarios.

Una vez que tenga su cuenta de la página de soporte de NetApp, podrá navegar a BlueXP para añadir esta cuenta de NSS para futuros registros.

Obtenga ayuda

NetApp ofrece soporte para BlueXP y sus servicios cloud de diversas maneras. Hay disponibles amplias opciones de auto soporte gratuito las 24 horas del día, los 7 días de la semana, como artículos de la base de conocimiento (KB) y un foro de la comunidad. Su registro de soporte incluye soporte técnico remoto a través de tickets web.

Utilice opciones de soporte automático

Estas opciones están disponibles de forma gratuita, las 24 horas del día, los 7 días de la semana:

- "[Base de conocimientos](#)"

Busque en la base de conocimientos de BlueXP para encontrar artículos útiles para resolver problemas.

- "[Comunidades](#)"

Únase a la comunidad de BlueXP para seguir los debates en curso o crear otros nuevos.

- Documentación

La documentación de BlueXP que está viendo actualmente.

- Correo:ng-cloudmanager-feedback@netapp.com[correo electrónico de comentarios]

Cree un caso con el soporte de NetApp

Además de las opciones de autosoporte anteriores, puede trabajar con un especialista de soporte de NetApp para resolver cualquier problema después de activar el soporte de.

Antes de empezar

Para utilizar la capacidad **Crear un caso**, primero debe realizar un registro único del número de serie de su ID de cuenta de BlueXP (p. ej. 960xxxx) con NetApp. ["Aprenda a registrarse para obtener soporte"](#).

Pasos

1. En BlueXP, haga clic en **Ayuda > Soporte**.
 2. En la página **Recursos**, elija una de las opciones disponibles en Soporte técnico:
 - a. Haga clic en **Llame a nosotros** si desea hablar con alguien en el teléfono. Se le dirigirá a una página de netapp.com que enumera los números de teléfono a los que puede llamar.
 - b. Haga clic en **Crear un caso** para abrir una incidencia con un especialista en soporte de NetApp:
 - **Cuenta del sitio de soporte de NetApp:** Seleccione la cuenta de NSS correspondiente asociada con la persona que abre el caso de soporte. Esta persona será el contacto principal con NetApp para contactar con ella, además de los correos electrónicos adicionales que se proporcionan a continuación.
- Si no ve su cuenta NSS, puede ir a la pestaña **NSS Management** de la sección Soporte de BlueXP para agregarla allí.
- **Servicio:** Seleccione el servicio con el que está asociado el problema. Por ejemplo, cuando BlueXP es específico de un problema de soporte técnico con flujos de trabajo o funcionalidades dentro del servicio.
 - **Entorno de trabajo:** Si se aplica al almacenamiento, seleccione **Cloud Volumes ONTAP** o **On-Prem** y, a continuación, el entorno de trabajo asociado.


La lista de entornos de trabajo se encuentra dentro del ámbito de la cuenta BlueXP, el área de trabajo y el conector que ha seleccionado en el banner superior del servicio.

- **Prioridad de caso:** Elija la prioridad para el caso, que puede ser Baja, Media, Alta o crítica.

Para obtener más información sobre estas prioridades, pase el ratón sobre el icono de información situado junto al nombre del campo.


- **Descripción del problema:** Proporcione una descripción detallada del problema, incluidos los mensajes de error aplicables o los pasos de solución de problemas que haya realizado.
- **Direcciones de correo electrónico adicionales:** Introduzca direcciones de correo electrónico adicionales si desea que alguien más conozca este problema.

Create a Case


TESTCLOUD2NTAP 


NetApp Support Site Account


Service

Cloud Manager 

Working Environment


Select... 

Case Priority 


Low- General Guidance 

Issue Description

Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.

Additional Email Addresses (Optional) 

Attachment (Optional) Coming Soon

No files selected 

Después de terminar

Aparecerá una ventana emergente con el número de caso de soporte. Un especialista de soporte de NetApp revisará su caso y le pondrá en contacto con usted próximamente.

Para obtener un historial de sus casos de soporte, puede hacer clic en **Configuración > línea de tiempo** y buscar acciones denominadas "Crear caso de soporte". Un botón situado en el extremo derecho le permite ampliar la acción para ver los detalles.

Es posible que se encuentre el siguiente mensaje de error al intentar crear un caso:

"No está autorizado a crear un caso en el servicio seleccionado"

Este error podría significar que la cuenta NSS y la compañía de registro con la que está asociada no es la misma compañía de registro para el número de serie de la cuenta de BlueXP (es decir, 960xxxx) o el número de serie del entorno de trabajo. Puede consultar su lista de cuentas NSS en la parte superior del formulario **Crear un caso** para encontrar la coincidencia correcta, o puede buscar ayuda mediante una de las siguientes opciones:

- Usar el chat en el producto
- Envíe un caso no técnico en <https://mysupport.netapp.com/site/help>

Gestione sus casos de soporte (vista previa)

Puede ver y gestionar los casos de soporte activos y resueltos directamente desde BlueXP. Es posible gestionar los casos asociados con su cuenta de NSS y con su empresa.

La gestión de casos está disponible como vista previa. Tenemos pensado perfeccionar esta experiencia y añadir mejoras en próximos lanzamientos. Envíenos sus comentarios mediante el chat en el producto.

Tenga en cuenta lo siguiente:

- La consola de gestión de casos en la parte superior de la página ofrece dos vistas:
 - La vista de la izquierda muestra el total de casos abiertos en los últimos 3 meses por la cuenta de usuario NSS que ha proporcionado.
 - La vista de la derecha muestra el total de casos abiertos en los últimos 3 meses a nivel de su compañía en función de su cuenta NSS de usuario.

Los resultados de la tabla reflejan los casos relacionados con la vista seleccionada.

- Puede agregar o quitar columnas de interés y filtrar el contenido de columnas como prioridad y estado. Otras columnas proporcionan funciones de clasificación.

Consulte los pasos a continuación para obtener más información.

- En el nivel por caso, ofrecemos la posibilidad de actualizar las notas de un caso o cerrar un caso que no esté ya en estado cerrado o pendiente de cierre.

Pasos

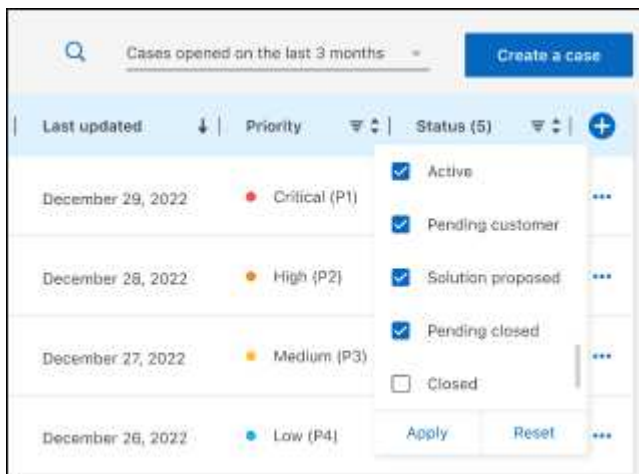
1. En BlueXP, haga clic en **Ayuda > Soporte**.
2. Haga clic en **Administración de casos** y si se le solicita, agregue su cuenta NSS a BlueXP.


La página **Administración de casos** muestra casos abiertos relacionados con la cuenta NSS asociada con su cuenta de usuario de BlueXP. Esta es la misma cuenta NSS que aparece en la parte superior de la página **NSS Management**.

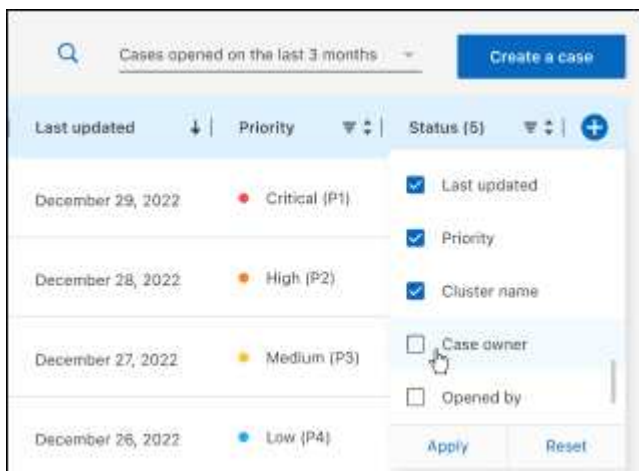
3. Si lo desea, puede modificar la información que se muestra en la tabla:
 - En **casos de la organización**, haga clic en **Ver** para ver todos los casos asociados con su empresa.
 - Modifique el rango de fechas eligiendo un rango de fechas exacto o eligiendo un marco de tiempo diferente.



- Filtre el contenido de las columnas.

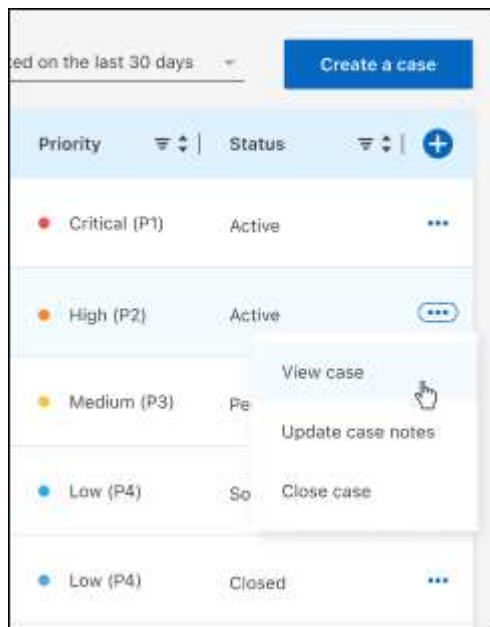


- Cambie las columnas que aparecen en la tabla haciendo clic en  y, a continuación, seleccione las columnas que desea mostrar.



4. Gestione un caso existente haciendo clic en ... y seleccione una de las opciones disponibles:

- **Ver caso:** Ver todos los detalles sobre un caso específico.
- **Actualizar notas de caso:** Proporcione detalles adicionales sobre su problema.
- **Cerrar caso:** Proporcione detalles sobre por qué cierra el caso y haga clic en **Cerrar caso**.



Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

<http://www.netapp.com/us/legal/copyright.aspx>

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

<https://www.netapp.com/us/media/patents-page.pdf>

Política de privacidad

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

["Aviso sobre Cloud Sync"](#)

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.