



Documentación de NetApp Copy and Sync

NetApp Copy and Sync

NetApp
December 16, 2025

This PDF was generated from <https://docs.netapp.com/es-es/data-services-copy-sync/index.html> on December 16, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Documentación de NetApp Copy and Sync	1
Notas de la versión	2
Novedades de NetApp Copy and Sync	2
6 de octubre de 2025	2
02 de febrero de 2025	2
27 de octubre de 2024	2
16 de septiembre de 2024	2
11 de agosto de 2024	2
14 de julio de 2024	3
02 de junio de 2024	3
08 de abril de 2024	3
11 de febrero de 2024	3
26 de noviembre de 2023	3
03 de septiembre de 2023	4
6 de agosto de 2023	4
9 de julio de 2023	4
11 de junio de 2023	5
08 de mayo de 2023	5
02 de abril de 2023	6
7 de marzo de 2023	6
05 de febrero de 2023	6
03 de enero de 2023	7
11 de diciembre de 2022	7
30 de octubre de 2022	7
04 de septiembre de 2022	8
31 de julio de 2022	9
03 de julio de 2022	10
6 de junio de 2022	11
1 de mayo de 2022	12
03 de abril de 2022	13
3 de marzo de 2022	14
06 de febrero de 2022	15
02 de enero de 2022	16
28 de noviembre de 2021	18
31 de octubre de 2021	18
4 de octubre de 2021	19
02 de septiembre de 2021	19
1 de agosto de 2021	19
7 de julio de 2021	21
7 de junio de 2021	21
02 de mayo de 2021	22
11 de abril de 2021	22
Limitaciones en NetApp Copy and Sync	23

Empezar	24
Obtenga más información sobre NetApp Copy and Sync	24
NetApp Console	24
Cómo funciona NetApp Copy and Sync	24
Tipos de almacenamiento admitidos	25
Costos	26
Inicio rápido para NetApp Copy and Sync	26
Relaciones de sincronización admitidas en NetApp Copy and Sync	27
Preparar el origen y el destino en NetApp Copy and Sync	35
Redes	35
Directorio de destino	35
Permisos para leer directorios	35
Requisitos del bucket de Amazon S3	36
Requisitos de almacenamiento de blobs de Azure	37
Almacenamiento de Azure Data Lake Gen2	39
Requisito de Azure NetApp Files	39
Requisitos de la caja	40
Requisitos del depósito de Google Cloud Storage	40
Google Drive	41
Requisitos del servidor NFS	41
Requisitos de ONTAP	42
Requisitos de almacenamiento de ONTAP S3	42
Requisitos del servidor SMB	42
Descripción general de redes para NetApp Copy and Sync	43
Ubicación del corredor de datos	43
Requisitos de red	44
Puntos finales de red	44
Inicie sesión en NetApp Copy and Sync	46
Instalar un agente de datos	47
Cree un nuevo agente de datos en AWS para NetApp Copy and Sync	47
Cree un nuevo agente de datos en Azure para NetApp Copy and Sync	50
Cree un nuevo agente de datos en Google Cloud para NetApp Copy and Sync	56
Instalar el agente de datos en un host Linux para NetApp Copy and Sync	61
Utilice NetApp Copy and Sync	66
Sincronizar datos entre un origen y un destino	66
Prepare un agente de datos para sincronizar datos entre el almacenamiento de objetos en NetApp Copy and Sync	66
Crear relaciones de sincronización en NetApp Copy and Sync	66
Copiar ACL de recursos compartidos SMB en NetApp Copy and Sync	75
Sincronice datos NFS mediante el cifrado de datos en tránsito en NetApp Copy and Sync	77
Configurar un grupo de intermediarios de datos para utilizar un almacén HashiCorp externo en NetApp Copy and Sync	81
Pague por las relaciones de sincronización después de que finalice su prueba gratuita de NetApp Copy and Sync	86
Suscribirse desde AWS	87

Suscribirse desde Azure	87
Compre licencias de NetApp y agréguelas a Copiar y sincronizar	88
Actualizar una licencia	88
Administración de relaciones de sincronización en NetApp Copy and Sync	89
Realizar una sincronización de datos inmediata	89
Acelerar el rendimiento de la sincronización	89
Actualizar credenciales	90
Configurar notificaciones	91
Cambiar la configuración de una relación de sincronización	91
Eliminar relaciones	95
Administrar grupos de intermediarios de datos en NetApp Copy and Sync	95
Cómo funcionan los grupos de corredores de datos	95
Recomendaciones de seguridad	96
Agregar un nuevo agente de datos a un grupo	96
Editar el nombre de un grupo	97
Configurar una configuración unificada	98
Mover corredores de datos entre grupos	99
Actualizar la configuración del proxy	99
Ver la configuración de un agente de datos	100
Abordar problemas con un corredor de datos	101
Eliminar un agente de datos de un grupo	102
Eliminar un grupo de corredores de datos	102
Cree y visualice informes para ajustar su configuración en NetApp Copy and Sync	103
Crear informes	103
Descargar informes	105
Ver errores del informe	106
Eliminar informes	106
Desinstalar el agente de datos para NetApp Copy and Sync	106
API de NetApp Copy and Sync	108
Empezar	108
Utilizar API de listas	109
Referencia de API	111
Conceptos	112
Descripción general de licencias para NetApp Copy and Sync	112
Suscripción al Marketplace	112
Licencias de NetApp	112
Privacidad de datos en NetApp Copy and Sync	113
Preguntas frecuentes técnicas NetApp Copy and Sync	113
Empezando	113
Fuentes y objetivos admitidos	115
Redes	116
Sincronización de datos	116
Seguridad	117
Permisos	118
Metadatos de almacenamiento de objetos	118

Actuación	119
Borrando cosas	120
Solución de problemas	120
Análisis profundo del corredor de datos	120
Conocimiento y apoyo	122
Regístrese para recibir asistencia	122
Descripción general del registro de soporte	122
Registrar la NetApp Console para obtener soporte de NetApp	122
Asociar credenciales NSS para la compatibilidad con Cloud Volumes ONTAP	124
Obtener ayuda	126
Obtenga soporte para un servicio de archivos de un proveedor de nube	126
Utilice opciones de autosuficiencia	126
Cree un caso con el soporte de NetApp	126
Gestione sus casos de soporte (Vista previa)	129
Avisos legales	132
Copyright	132
Marcas comerciales	132
Patentes	132
Política de privacidad	132
Código abierto	132

Documentación de NetApp Copy and Sync

Notas de la versión

Novedades de NetApp Copy and Sync

Descubra las novedades de NetApp Copy and Sync.

6 de octubre de 2025

La BlueXP copy and sync ahora es NetApp Copy and Sync

La BlueXP copy and sync ha cambiado de nombre a NetApp Copy and Sync.

BlueXP ahora es NetApp Console

La NetApp Console, construida sobre la base BlueXP mejorada y reestructurada, proporciona una gestión centralizada del almacenamiento de NetApp y de los NetApp Data Services en entornos locales y en la nube a nivel empresarial, brindando información en tiempo real, flujos de trabajo más rápidos y una administración simplificada, que es altamente segura y compatible.

Para obtener más detalles sobre lo que ha cambiado, consulte la ["Notas de la versión de la NetApp Console"](#).

02 de febrero de 2025

Nuevo soporte del sistema operativo para el agente de datos

El agente de datos ahora es compatible con hosts que ejecutan Red Hat Enterprise 9.4, Ubuntu 23.04 y Ubuntu 24.04.

["Ver los requisitos del host Linux"](#).

27 de octubre de 2024

Corrección de errores

Actualizamos NetApp Copy and Sync y el agente de datos para corregir algunos errores. La nueva versión del broker de datos es 1.0.56.

16 de septiembre de 2024

Corrección de errores

Actualizamos NetApp Copy and Sync y el agente de datos para corregir algunos errores. La nueva versión del broker de datos es 1.0.55.

11 de agosto de 2024

Corrección de errores

Actualizamos NetApp Copy and Sync y el agente de datos para corregir algunos errores. La nueva versión del broker de datos es 1.0.54.

14 de julio de 2024

Corrección de errores

Actualizamos Copy and Sync y el agente de datos para corregir algunos errores. La nueva versión del broker de datos es 1.0.53.

02 de junio de 2024

Corrección de errores

NetApp Copy and Sync se actualizó para corregir algunos errores. El agente de datos también se actualizó para aplicar actualizaciones de seguridad. La nueva versión del broker de datos es 1.0.52.

08 de abril de 2024

Compatibilidad con RHEL 8.9

El agente de datos ahora es compatible con hosts que ejecutan Red Hat Enterprise Linux 8.9.

["Ver los requisitos del host Linux"](#) .

11 de febrero de 2024

Filtrar directorios por expresiones regulares

Los usuarios ahora tienen la opción de filtrar directorios usando expresiones regulares.

["Obtenga más información sobre la función **Excluir directorios**."](#)

26 de noviembre de 2023

Compatibilidad de clases de almacenamiento en frío para Azure Blob

El nivel de almacenamiento en frío de Azure Blob ahora está disponible al crear una relación de sincronización.

["Obtenga más información sobre cómo crear una relación de sincronización."](#)

Compatibilidad con la región de Tel Aviv en los corredores de datos de AWS

Tel Aviv ahora es una región compatible al crear un agente de datos en AWS.

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

Actualización de la versión del nodo para corredores de datos

Todos los nuevos corredores de datos ahora utilizarán la versión de nodo 21.2.0. Los agentes de datos que no son compatibles con esta actualización, como CentOS 7.0 y Ubuntu Server 18.0, ya no funcionarán con NetApp Copy and Sync.

03 de septiembre de 2023

Excluir archivos mediante expresiones regulares

Los usuarios ahora tienen la opción de excluir archivos usando expresiones regulares.

["Obtenga más información sobre la función Excluir extensiones de archivo."](#)

Agregar claves S3 al crear un agente de datos de Azure

Los usuarios ahora pueden agregar claves de acceso y claves secretas de AWS S3 al crear un agente de datos de Azure.

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

6 de agosto de 2023

Utilice grupos de seguridad de Azure existentes al crear un agente de datos

Los usuarios ahora tienen la opción de usar grupos de seguridad de Azure existentes al crear un agente de datos.

La cuenta de servicio utilizada al crear el agente de datos debe tener estos permisos:

- "Microsoft.Network/networkSecurityGroups/securityRules/read"
- "Microsoft.Network/networkSecurityGroups/read"

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

Cifrar datos al sincronizar con Google Storage

Los usuarios ahora tienen la opción de especificar una clave de cifrado administrada por el cliente al crear una relación de sincronización con un depósito de Google Storage como destino. Puede ingresar su clave manualmente o elegirla de una lista de claves en una sola región.

La cuenta de servicio utilizada al crear el agente de datos debe tener estos permisos:

- cloudkms.cryptoKeys.lista
- lista de llaveros cloudkms

["Obtenga más información sobre los requisitos del depósito de Google Cloud Storage."](#)

9 de julio de 2023

Eliminar múltiples relaciones de sincronización a la vez

Los usuarios ahora pueden eliminar más de una relación de sincronización a la vez en la interfaz de usuario.

["Obtenga más información sobre cómo eliminar relaciones de sincronización."](#)

Copiar solo ACL

Los usuarios ahora tienen opciones adicionales para copiar información de ACL en relaciones CIF y NFS. Al

crear o administrar una relación de sincronización, puede copiar solo archivos, copiar solo información de ACL o copiar archivos e información de ACL.

["Obtenga más información sobre cómo copiar ACL."](#)

Actualizado a Node.js 20

Copiar y sincronizar se ha actualizado a Node.js 20. Se actualizarán todos los corredores de datos disponibles. No se pueden instalar sistemas operativos incompatibles con esta actualización y los sistemas existentes incompatibles pueden experimentar problemas de rendimiento.

11 de junio de 2023

Admite cancelación automática por minutos

Las sincronizaciones activas que no se hayan completado ahora se pueden cancelar después de quince minutos usando la función **Tiempo de espera de sincronización**.

["Obtenga más información sobre la configuración del tiempo de espera de sincronización"](#) .

Copiar metadatos de tiempo de acceso

En las relaciones que incluyen un sistema de archivos, la función **Copiar para objetos** ahora copia metadatos de tiempo de acceso.

["Obtenga más información sobre la configuración Copiar para objetos"](#) .

08 de mayo de 2023

Capacidades de enlace duro

Los usuarios ahora pueden incluir enlaces físicos para sincronizaciones que involucran relaciones NFS a NFS no seguras.

["Obtenga más información sobre la configuración de Tipos de archivo"](#) .

Capacidad de agregar certificados de usuario para intermediarios de datos en relaciones NFS seguras

Los usuarios ahora pueden configurar su propio certificado para el agente de datos de destino al crear una relación NFS segura. Necesitarán establecer un nombre de servidor y proporcionar una clave privada y un ID de certificado al hacerlo. Esta función está disponible para todos los corredores de datos.

Período de exclusión extendido para archivos modificados recientemente

Los usuarios ahora pueden excluir archivos que se modificaron hasta 365 días antes de la sincronización programada.

["Obtenga más información sobre la configuración de Archivos modificados recientemente"](#) .

Filtrar relaciones en la interfaz de usuario por ID de relación

Quienes utilizan la API RESTful ahora pueden filtrar relaciones utilizando identificadores de relación.

["Obtenga más información sobre el uso de la API RESTful con NetApp Copy and Sync"](#) .

["Obtenga más información sobre la configuración Excluir directorios"](#) .

02 de abril de 2023

Compatibilidad adicional con las relaciones de Azure Data Lake Storage Gen2

Ahora puede crear relaciones de sincronización con Azure Data Lake Storage Gen2 como origen y destino con lo siguiente:

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

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

Filtrar directorios por ruta completa

Además de filtrar directorios por nombre, ahora puedes filtrar directorios por su ruta completa.

["Obtenga más información sobre la configuración Excluir directorios"](#) .

7 de marzo de 2023

Cifrado EBS para corredores de datos de AWS

Ahora puede cifrar los volúmenes del agente de datos de AWS usando una clave KMS desde su cuenta.

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

05 de febrero de 2023

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

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

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

Cloud Sync también tiene soporte adicional para Azure Data Lake Storage Gen2 como origen y destino para:

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

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

Actualización al sistema operativo del agente de datos de Amazon Web Services

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

["Obtenga más información sobre la instancia del agente de datos en AWS"](#) .

03 de enero de 2023

Mostrar la configuración local del agente de datos en la interfaz de usuario

Ahora hay una opción **Mostrar configuración** que permite a los usuarios ver la configuración local de cada agente de datos en la interfaz de usuario.

["Obtenga más información sobre la gestión de grupos de intermediarios de datos"](#) .

Actualización al sistema operativo del agente de datos de Azure y Google Cloud

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

["Obtenga más información sobre la instancia del agente de datos en Azure"](#) .

["Obtenga más información sobre la instancia del agente de datos en Google Cloud"](#) .

11 de diciembre de 2022

Filtrar directorios por nombre

Ahora está disponible una nueva configuración **Excluir nombres de directorio** para las relaciones de sincronización. Los usuarios pueden filtrar un máximo de 15 nombres de directorio de su sincronización. Los directorios .copy-offload, .snapshot y ~snapshot están excluidos de forma predeterminada.

["Obtenga más información sobre la configuración Excluir nombres de directorio"](#) .

Compatibilidad adicional con almacenamiento Amazon S3 y ONTAP S3

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

- Almacenamiento de AWS S3 a 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 sincronización continua ahora es compatible desde un depósito de almacenamiento de Azure de origen a un almacenamiento en la nube mediante un agente de datos de Azure.

Después de la sincronización de datos inicial, Cloud Sync escucha los cambios en el depósito de almacenamiento de Azure de origen y sincroniza continuamente cualquier cambio con el destino a medida que se producen. Esta configuración está disponible al sincronizar desde un depósito de almacenamiento de Azure a Azure Blob Storage, 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 usar esta configuración:

```
'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 sobre la configuración de sincronización continua"](#) .

04 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 sobre los informes"](#) .

Mejora de la sincronización continua

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

- Depósito S3 a un servidor NFS
- Google Cloud Storage en un servidor NFS

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

Notificaciones por correo electrónico

Ahora puedes recibir notificaciones de Cloud Sync por correo electrónico.

Para recibir las notificaciones por correo electrónico, deberá habilitar la configuración **Notificaciones** en la relación de sincronización y luego configurar las configuraciones de Alertas y Notificaciones en la NetApp Console.

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

31 de julio de 2022

Google Drive

Ahora puedes sincronizar datos desde un servidor NFS o SMB a Google Drive. Se admiten como destinos tanto “Mi unidad” como “Unidades compartidas”.

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

["Ver la lista de relaciones de sincronización admitidas"](#) .

Compatibilidad adicional con Azure Data Lake

Cloud Sync ahora admite relaciones de sincronización adicionales para Azure Data Lake Storage Gen2:

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

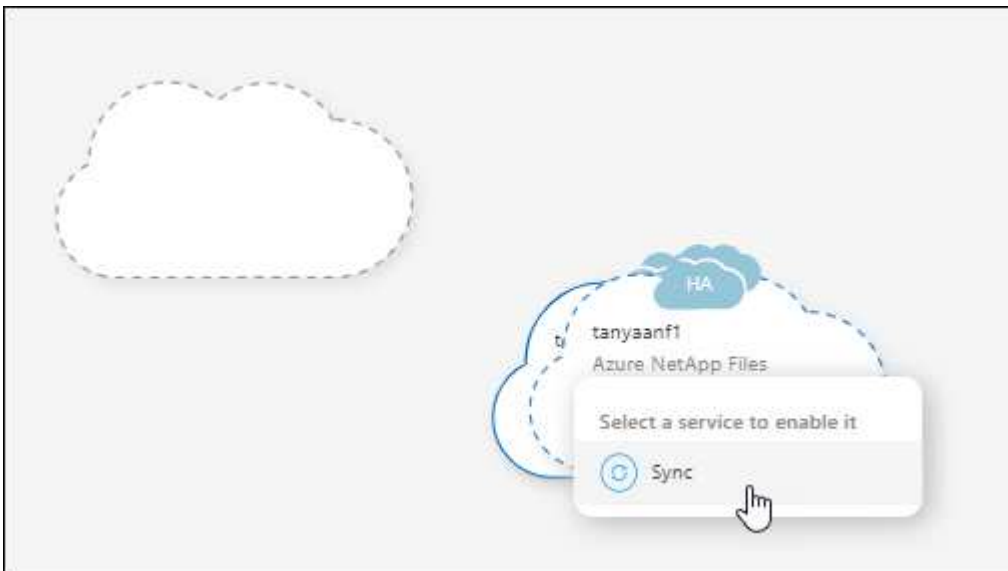
["Ver la lista de relaciones de sincronización admitidas"](#) .

Nuevas formas de establecer relaciones de sincronización

Hemos agregado formas adicionales de configurar relaciones de sincronización directamente desde la página Sistemas de la consola de NetApp .

Arrastrar y soltar

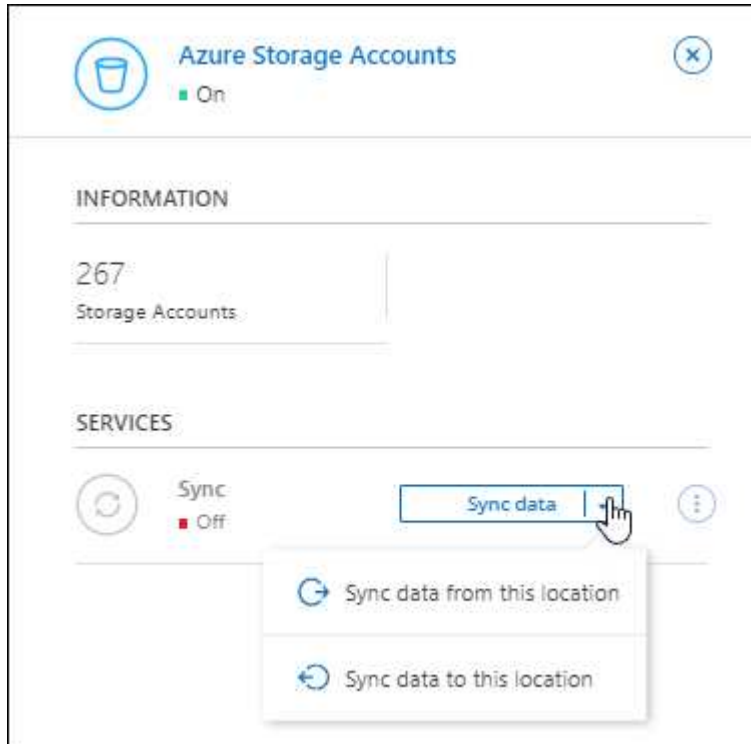
Ahora puede configurar una relación de sincronización desde la página Sistemas arrastrando y soltando un sistema sobre otro.



Configuración del panel derecho

Ahora puede configurar una relación de sincronización para Azure Blob Storage o para Google Cloud Storage

seleccionando el sistema en la página Sistemas y luego seleccionando la opción de sincronización en el panel derecho.



03 de julio de 2022

Compatibilidad con Azure Data Lake Storage Gen2

Ahora puede sincronizar datos desde un servidor NFS o un servidor SMB con Azure Data Lake Storage Gen2.

Al crear una relación de sincronización que incluya Azure Data Lake, 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).

["Ver la lista de relaciones de sincronización admitidas"](#) .

Sincronización continua desde Google Cloud Storage

La configuración de sincronización continua ahora es compatible desde un depósito de Google Cloud Storage de origen a un destino de almacenamiento en la nube.

Después de la sincronización de datos inicial, Cloud Sync escucha los cambios en el depósito de Google Cloud Storage de origen y sincroniza continuamente cualquier cambio con el destino a medida que se producen. Esta configuración está disponible al sincronizar desde un depósito de Google Cloud Storage a S3, Google Cloud Storage, Azure Blob Storage, StorageGRID o IBM Storage.

La cuenta de servicio asociada con su agente de datos necesita los siguientes permisos para usar 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 sobre la configuración de sincronización continua"](#) .

Nueva compatibilidad con regiones de Google Cloud

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

- Colón (us-east5)
- Dallas (us-south1)
- Madrid (europa-suroeste1)
- Milán (europa-oeste8)
- París (europa-oeste9)

Nuevo tipo de máquina de Google Cloud

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

6 de junio de 2022

Sincronización continua

Una nueva configuración le permite sincronizar continuamente los cambios desde un depósito S3 de origen a un destino.

Después de la sincronización de datos inicial, Cloud Sync escucha los cambios en el depósito S3 de origen y sincroniza continuamente cualquier cambio en el destino a medida que se producen. No es necesario volver a escanear la fuente a intervalos programados. Esta configuración solo está disponible cuando se sincroniza desde un bucket S3 a S3, Google Cloud Storage, Azure Blob Storage, StorageGRID o IBM Storage.

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

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

Estos permisos se agregan automáticamente a cualquier nuevo agente de datos que usted cree.

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

Mostrar todos los volúmenes de 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 local o un sistema de archivos FSx para ONTAP .

Anteriormente, Cloud Sync solo mostraba los volúmenes que coincidían con el protocolo seleccionado. Ahora se muestran todos los volúmenes, pero cualquier volumen que no coincida con el protocolo seleccionado o que no tenga un recurso compartido o exportación aparecerá en gris y no se podrá seleccionar.

Copiar etiquetas a Azure Blob

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

- En la página **Configuración**, puede usar la configuración **Copiar para objetos** para copiar etiquetas desde el origen al contenedor de blobs de Azure. Esto se suma a la copia de metadatos.
- En la página **Etiquetas/Metadatos**, puede especificar las etiquetas de índice de blob que se establecerán en los objetos que se copian al contenedor de blobs de Azure. Anteriormente, solo se podían especificar metadatos de relación.

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

1 de mayo de 2022

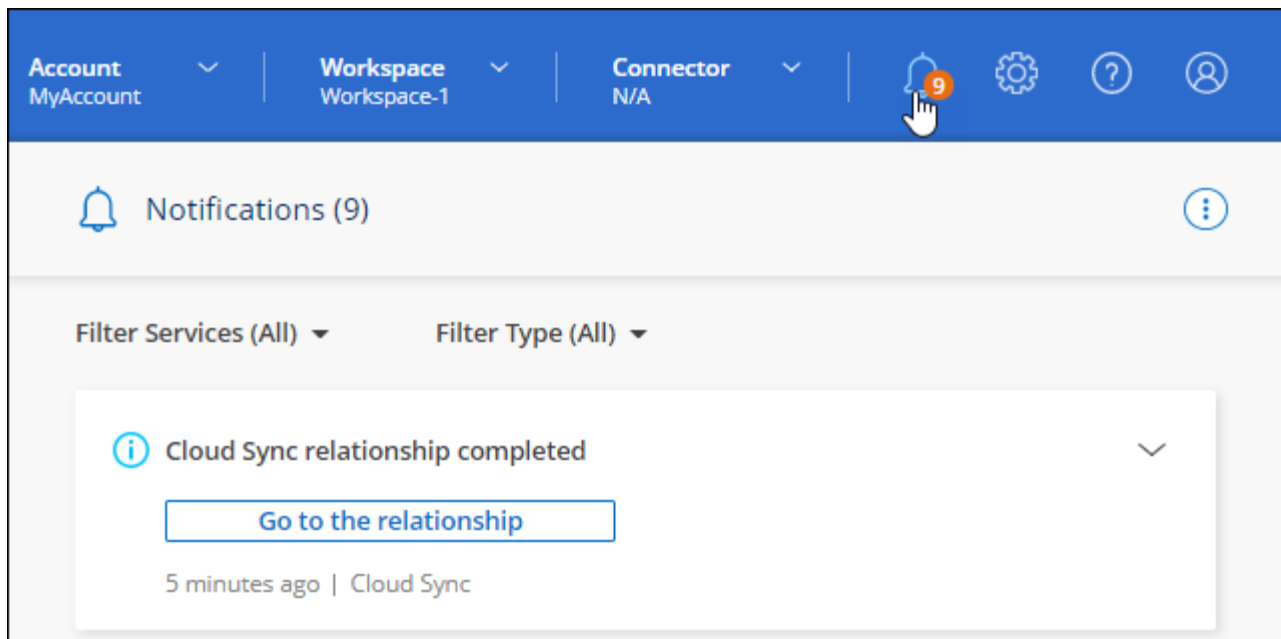
Tiempo de espera de sincronización

Ahora está disponible una nueva configuración 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 la sincronización no se completó en la cantidad de horas o días especificada.

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

Notificaciones

Ahora está 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 notificaciones de la consola de NetApp . Puede habilitar notificaciones para sincronizaciones de datos exitosas, fallidas y canceladas.



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

03 de abril de 2022

Mejoras en el grupo de intermediarios de datos

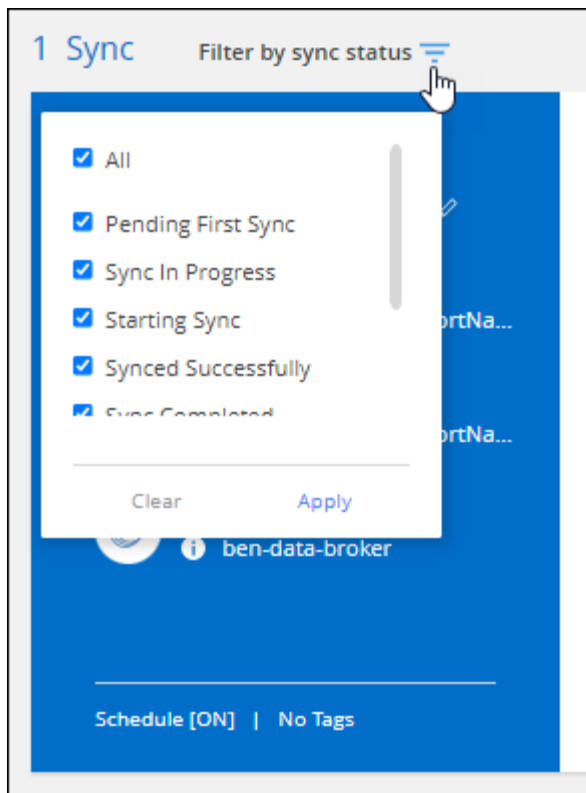
Realizamos varias mejoras en los grupos de corredores de datos:

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

["Aprenda a administrar grupos de intermediarios de datos"](#) .

Filtro del panel de control

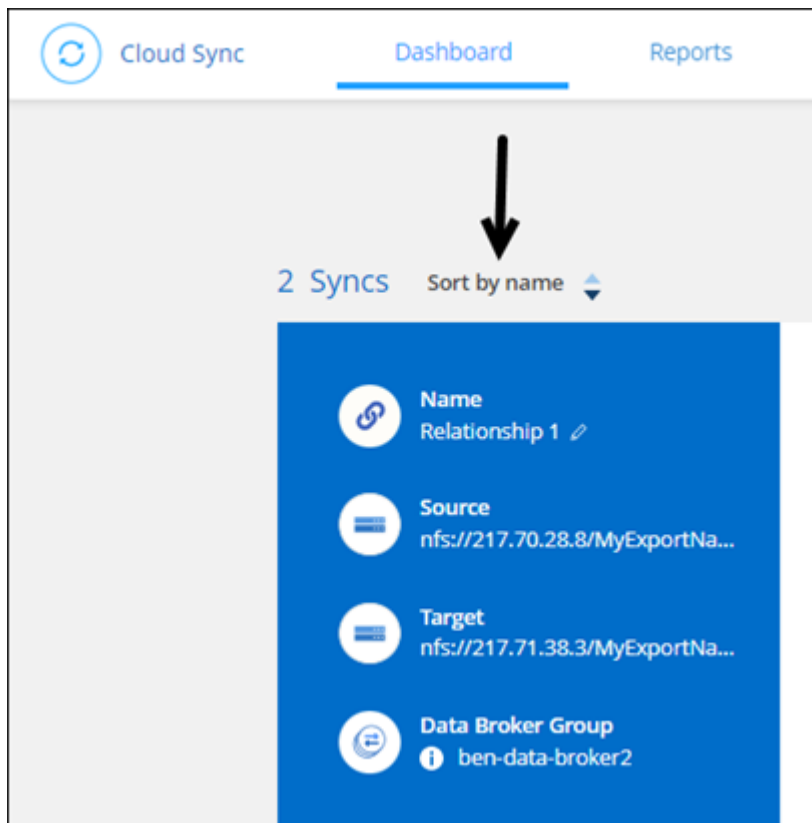
Ahora puedes filtrar el contenido del Panel de sincronización para encontrar más fácilmente relaciones de sincronización que coincidan con un estado determinado. Por ejemplo, puede filtrar las relaciones de sincronización que tienen un estado fallido.



3 de marzo de 2022

Ordenar en el panel de control

Ahora puede ordenar 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 al facilitar la creación de la relación de sincronización. Después de iniciar una sincronización de datos desde Cloud Data Sense, toda la información de origen se contiene en un solo paso y solo requiere que ingrese algunos detalles clave.

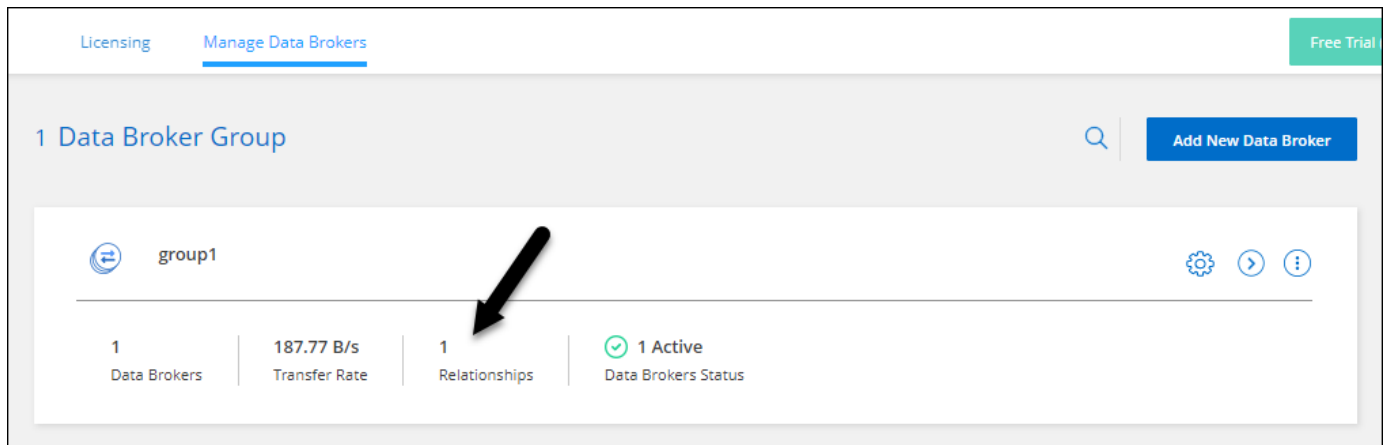
06 de febrero de 2022

Mejora de los grupos de intermediarios de datos

Cambiamos la forma en que interactúas con los corredores de datos al enfatizar los *grupos* de corredores de datos.

Por ejemplo, cuando crea una nueva relación de sincronización, selecciona el *grupo* de intermediarios de datos que se utilizará con la relación, en lugar de un intermediario de datos específico.

En la pestaña **Administrar agentes de datos**, también mostramos la cantidad de relaciones de sincronización que administra un grupo de agentes de datos.



Descargar informes en PDF

Ahora puedes descargar un informe en formato PDF.

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

02 de enero de 2022

Nuevas relaciones de sincronización de Box

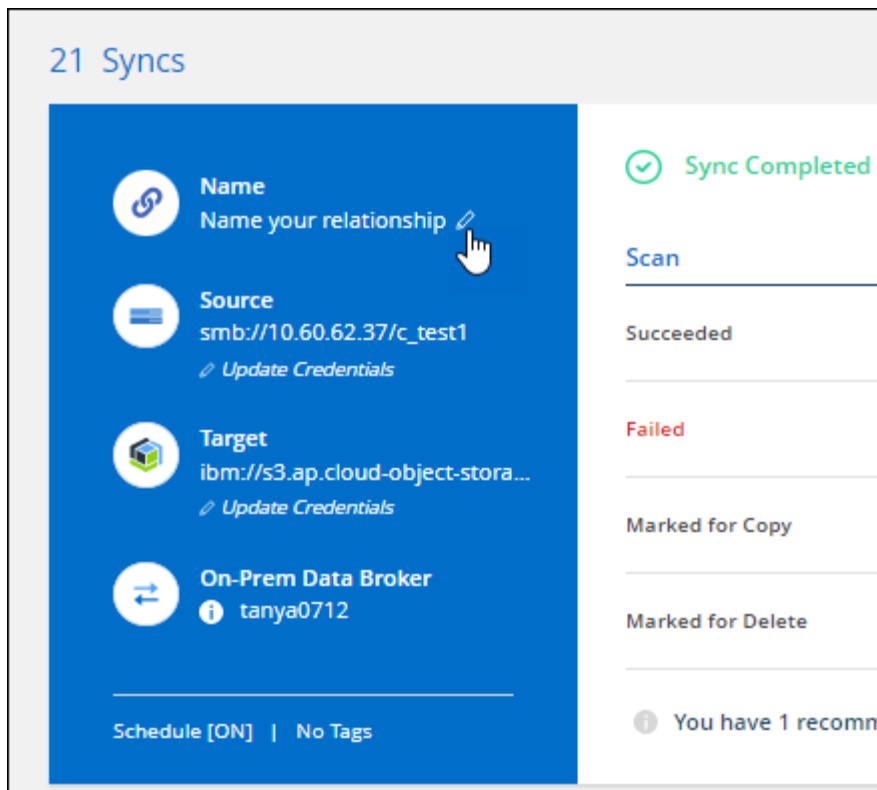
Se admiten dos nuevas relaciones de sincronización:

- Box a Azure NetApp Files
- Caja a Amazon FSx para ONTAP

["Ver la lista de relaciones de sincronización admitidas"](#) .

Nombres de 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 cuando crea la relación y en cualquier momento después.



Enlaces privados de S3

Al sincronizar datos hacia o desde Amazon S3, puede elegir si desea utilizar un enlace privado de S3. Cuando el agente de datos copia datos del origen al destino, lo hace a través del enlace privado.

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

```
"ec2:DescribeVpcEndpoints"
```

Este permiso se agrega automáticamente a cualquier nuevo corredor de datos que usted cree.

Recuperación instantánea de glaciares

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

ACL desde almacenamiento de objetos a recursos compartidos SMB

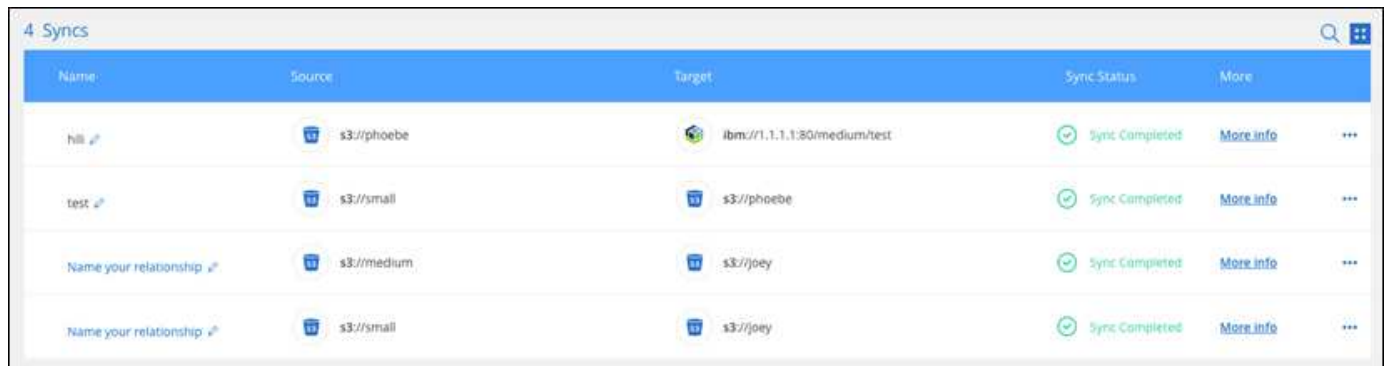
Cloud Sync ahora admite la copia de ACL desde el almacenamiento de objetos a recursos compartidos SMB. Anteriormente, solo admitíamos la copia de ACL desde un recurso compartido SMB al almacenamiento de objetos.

SFTP a S3

Ahora se admite la creación de una relación de sincronización de SFTP a Amazon S3 en la interfaz de usuario. Anteriormente esta relación de sincronización solo era compatible con la API.

Mejora de la vista de tabla

Rediseñamos la vista de tabla en el Tablero para facilitar su uso. Si selecciona **Más información**, Cloud Sync filtra el panel para mostrarle más información sobre 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 a la región de Jarkarta

Cloud Sync ahora admite la implementación del agente de datos en la región Asia Pacífico (Yakarta) de AWS.

28 de noviembre de 2021

ACL de SMB a almacenamiento de objetos

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

Cloud Sync no admite la copia de ACL desde el almacenamiento de objetos a recursos compartidos SMB.

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

Actualizar licencias

Ahora puedes actualizar las licencias de Cloud Sync que hayas extendido.

Si extendió una licencia de Cloud Sync que compró en NetApp, puede agregar la licencia nuevamente para actualizar la fecha de vencimiento.

["Aprenda cómo 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 caja

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

Box puede ser el origen o el destino de varios tipos de relaciones de sincronización. ["Ver la lista de relaciones de sincronización admitidas"](#) .

Configuración de fecha de creación

Cuando un servidor SMB es la fuente, una nueva configuración de relación de sincronización denominada *Fecha de creación* le permite sincronizar archivos que se crearon después de una fecha específica, antes de una fecha específica o entre un rango de tiempo específico.

["Obtenga más información sobre la configuración de Cloud Sync"](#) .

4 de octubre de 2021

Soporte de caja adicional

Cloud Sync ahora admite relaciones de sincronización adicionales para ["Caja"](#) al utilizar la API de Cloud Sync :

- De Amazon S3 a Box
- Almacenamiento de objetos en IBM Cloud para Box
- StorageGRID a Box
- Caja a un servidor NFS
- Caja a un servidor SMB

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

Informes para rutas SFTP

Ahora puedes ["crear un informe"](#) para rutas SFTP.

02 de septiembre de 2021

Compatibilidad con FSx para ONTAP

Ahora puede sincronizar datos hacia o desde un sistema de archivos de Amazon FSx para ONTAP .

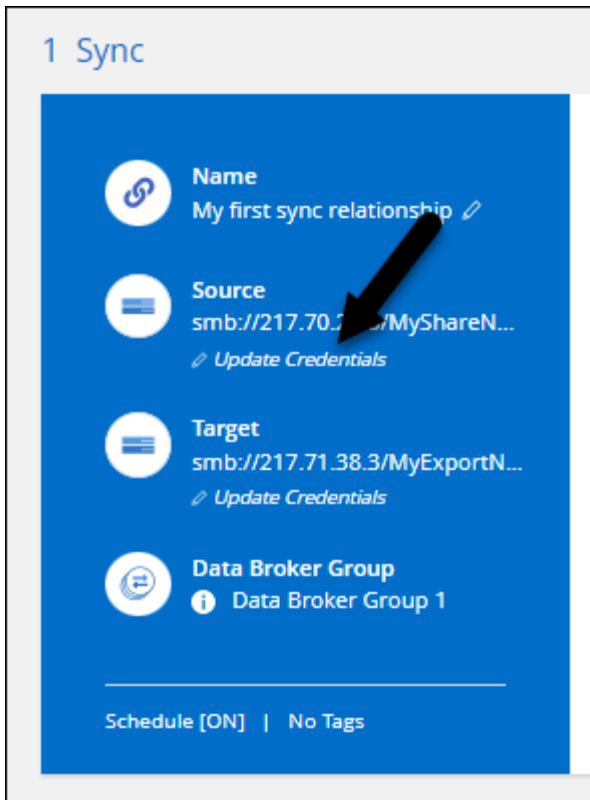
- ["Obtenga más información sobre Amazon FSx para ONTAP"](#)
- ["Ver relaciones de sincronización admitidas"](#)
- ["Aprenda a crear una relación de sincronización para Amazon FSx para ONTAP"](#)

1 de agosto de 2021

Actualizar credenciales

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

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



Etiquetas para objetivos de almacenamiento de objetos

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

La adición de etiquetas es compatible con Amazon S3, Azure Blob, Google Cloud Storage, IBM Cloud Object Storage y StorageGRID.

Soporte para Box

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

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

IP pública para el 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 máquina virtual.

["Aprenda a implementar un agente de datos en Google Cloud"](#) .

Volumen de protocolo dual para Azure NetApp Files

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

7 de julio de 2021

Almacenamiento ONTAP S3 y Google Cloud Storage

Cloud Sync ahora admite relaciones de sincronización entre ONTAP S3 Storage y un depósito de Google Cloud Storage desde la interfaz de usuario.

["Ver la lista de relaciones de sincronización admitidas"](#) .

Etiquetas de metadatos de objetos

Cloud Sync ahora puede copiar metadatos y etiquetas de objetos entre almacenamiento basado en objetos cuando crea una relación de sincronización y habilita una configuración.

["Obtenga más información sobre la configuración Copiar para objetos"](#) .

Soporte para bóvedas de HashiCorp

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

["Obtenga más información sobre el uso de HashiCorp Vault con un agente de datos"](#) .

Definir etiquetas o metadatos para el bucket S3

Al configurar una relación de sincronización con un bucket de Amazon S3, el asistente de relación de sincronización ahora le permite definir las etiquetas o los metadatos que desea guardar en los objetos en el bucket 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 depósito de Google Cloud Storage es el destino de una relación de sincronización, ahora puedes elegir la clase de almacenamiento que deseas usar. Cloud Sync admite las siguientes clases de almacenamiento:

- Estándar

- Cerca de línea
- Línea fría
- Archivo

02 de mayo de 2021

Errores en los informes

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

["Obtenga más información sobre cómo crear y visualizar informes para ajustar su configuración"](#) .

Comparar atributos

Ahora está disponible una nueva configuración **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 sincronizarse nuevamente.

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

11 de abril de 2021

El servicio independiente Cloud Sync se ha retirado

El servicio independiente Cloud Sync ha sido retirado. Ahora debería acceder a Cloud Sync directamente desde la NetApp Console, donde están disponibles las mismas características y funcionalidades.

Después de iniciar sesión en la NetApp Console, puede cambiar a la pestaña 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 depósitos de Google Cloud en diferentes proyectos, si proporciona los permisos necesarios a la cuenta de servicio del agente de datos.

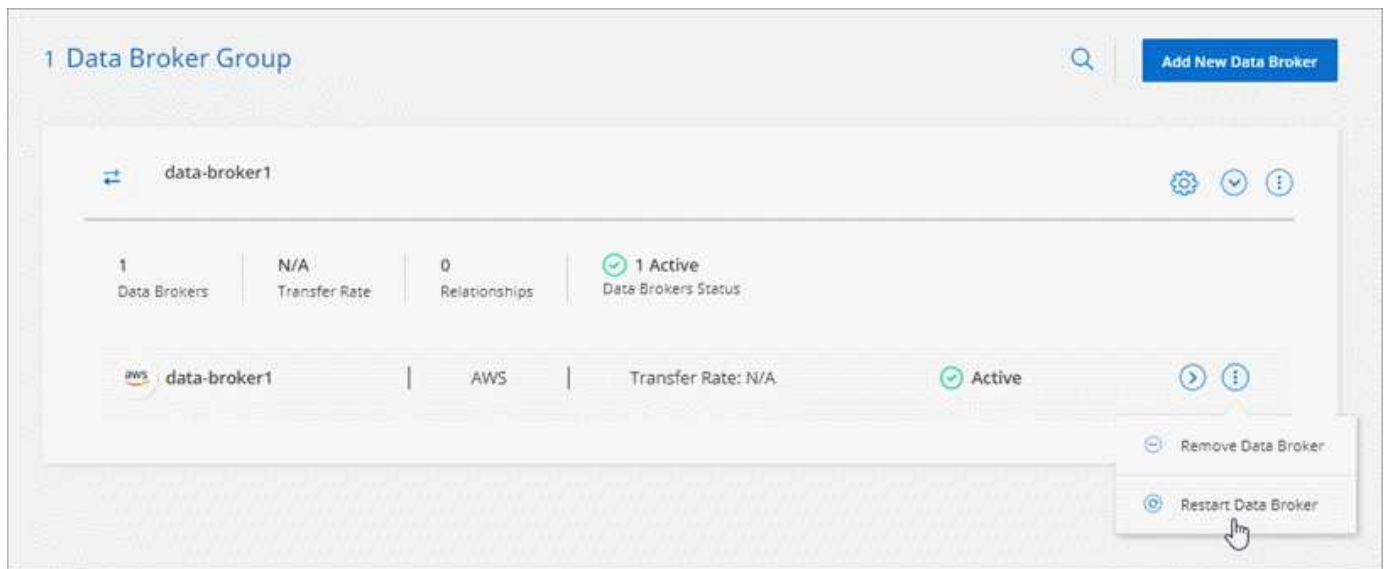
["Aprenda a configurar la cuenta de servicio"](#) .

Metadatos entre Google Cloud Storage y S3

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

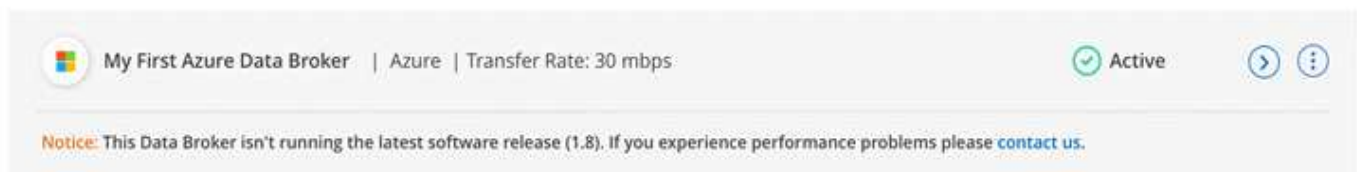
Reiniciar los corredores de datos

Ahora puedes reiniciar un agente de datos desde Cloud Sync.



Mensaje cuando no se ejecuta la última versión

Cloud Sync ahora identifica cuándo un agente de datos no está ejecutando la última versión de software. Este mensaje puede ayudarle a garantizar que obtenga las últimas características y funcionalidades.



Limitaciones en NetApp Copy and Sync

Las limitaciones conocidas identifican plataformas, dispositivos o funciones que no son compatibles con esta versión del producto o que no interoperan correctamente con él. Revise estas limitaciones cuidadosamente.

NetApp Copy and Sync no es compatible con las siguientes regiones:

- Regiones gubernamentales de AWS
- Regiones gubernamentales de Azure
- Porcelana

Empezar

Obtenga más información sobre NetApp Copy and Sync

NetApp Copy and Sync ofrece una forma sencilla, segura y automatizada de migrar sus datos a cualquier destino, en la nube o en sus instalaciones. Ya sea un conjunto de datos NAS basado en archivos (NFS o SMB), un formato de objeto de Amazon Simple Storage Service (S3), un dispositivo NetApp StorageGRID o cualquier otro almacén de objetos de un proveedor de nube, Copy and Sync puede convertirlo y moverlo por usted.

NetApp Console

Se puede acceder a NetApp Copy and Sync a través de la NetApp Console.

La NetApp Console proporciona una gestión centralizada de los servicios de datos y almacenamiento de NetApp en entornos locales y en la nube a nivel empresarial. La consola es necesaria para acceder y utilizar los servicios de datos de NetApp . Como interfaz de administración, le permite administrar muchos recursos de almacenamiento desde una sola interfaz. Los administradores de la consola pueden controlar el acceso al almacenamiento y los servicios para todos los sistemas dentro de la empresa.

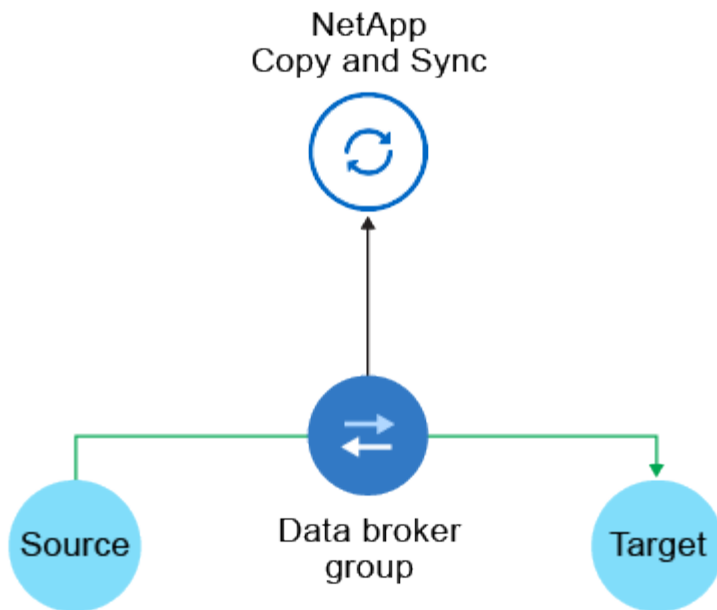
No necesita una licencia o suscripción para comenzar a usar NetApp Console y solo incurre en cargos cuando necesita implementar agentes de Console en su nube para garantizar la conectividad con sus sistemas de almacenamiento o servicios de datos de NetApp . Sin embargo, algunos servicios de datos de NetApp accesibles desde la consola requieren licencia o suscripción.

Obtenga más información sobre el ["NetApp Console"](#) .

Cómo funciona NetApp Copy and Sync

NetApp Copy and Sync es una plataforma de software como servicio (SaaS) que consta de un grupo de intermediarios de datos, una interfaz basada en la nube disponible a través de la NetApp Console y un origen y un destino.

La siguiente imagen muestra la relación entre los componentes Copiar y Sincronizar:



El software de intermediación de datos de NetApp sincroniza datos desde un origen a un destino (esto se denomina *relación de sincronización*). Puede ejecutar el agente de datos en AWS, Azure, Google Cloud Platform o en sus instalaciones. Un grupo de corredores de datos, que consta de uno o más corredores de datos, necesita una conexión a Internet saliente a través del puerto 443 para poder comunicarse con Copy and Sync y contactar a algunos otros servicios y repositorios. ["Ver la lista de puntos finales"](#) .

Después de la copia inicial, Copiar y sincronizar sincroniza todos los datos modificados según el cronograma que usted establezca.

Tipos de almacenamiento admitidos

Copiar y sincronizar admite los siguientes tipos de almacenamiento:

- Cualquier servidor NFS
- Cualquier servidor SMB
- Amazon EFS
- Amazon FSx para ONTAP
- Amazon S3
- Blob de Azure
- Almacenamiento de Azure Data Lake Gen2
- Azure NetApp Files
- Caja (disponible como vista previa)
- Cloud Volumes ONTAP
- Almacenamiento en la nube de Google
- Google Drive
- Almacenamiento de objetos en la nube de IBM
- Clúster ONTAP local
- Almacenamiento ONTAP S3

- SFTP (solo usando API)
- StorageGRID

["Ver las relaciones de sincronización admitidas"](#) .

Costos

Hay dos tipos de costos asociados con el uso de Copiar y sincronizar: cargos por recursos y cargos por servicio.

Cargos por recursos

Los cargos por recursos están relacionados con los costos de computación y almacenamiento para ejecutar uno o más corredores de datos en la nube.

Cargos por servicio

Hay dos formas de pagar las relaciones de sincronización una vez finalizada la prueba gratuita de 14 días. La primera opción es suscribirse desde AWS o Azure, lo que le permite pagar por hora o anualmente. La segunda opción es comprar licencias directamente de NetApp.

["Aprenda cómo funcionan las licencias"](#) .

Inicio rápido para NetApp Copy and Sync

Comenzar a utilizar NetApp Copy and Sync incluye algunos pasos.

1

Inicie sesión y configure la NetApp Console

Debería haber comenzado a utilizar la NetApp Console, lo que incluye iniciar sesión, configurar una cuenta y posiblemente implementar un agente de consola y crear sistemas.

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

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

Se requiere un agente de consola para Cloud Volumes ONTAP, clústeres ONTAP locales y Amazon FSx para ONTAP.

- ["Descubra cómo comenzar a utilizar la NetApp Console"](#)
- ["Obtenga más información sobre los agentes de consola"](#)

2

Prepare su fuente y su destino

Verifique que su origen y destino sean compatibles y estén configurados. El requisito más importante es verificar la conectividad entre el grupo de intermediarios de datos y las ubicaciones de origen y destino.

- ["Ver relaciones compatibles"](#)
- ["Preparar la fuente y el destino"](#)

3

Prepare una ubicación para el agente de datos de NetApp

El software de intermediación de datos de NetApp sincroniza datos desde un origen a un destino (esto se denomina *relación de sincronización*). Puede ejecutar el agente de datos en AWS, Azure, Google Cloud Platform o en sus instalaciones. Un grupo de corredores de datos, que consta de uno o más corredores de datos, necesita una conexión a Internet saliente a través del puerto 443 para poder comunicarse con NetApp Copy and Sync y contactar a algunos otros servicios y repositorios. ["Ver la lista de puntos finales"](#) .

NetApp Copy and Sync lo guía a través del proceso de instalación cuando crea una relación de sincronización, momento en el que puede implementar un agente de datos en la nube o descargar un script de instalación para su propio host Linux.

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

4

Crea tu primera relación de sincronización

Iniciar sesión en ["la NetApp Console"](#) , seleccione **Sincronizar** y luego arrastre y suelte sus selecciones para el origen y el destino. Siga las instrucciones para completar la configuración. ["Más información"](#) .

5

Pague por sus relaciones de sincronización después de que finalice su prueba gratuita

Suscríbete desde AWS o Azure para pagar por uso o pagar anualmente. O compre licencias directamente de NetApp. Simplemente vaya a la página de Configuración de licencia en NetApp Copy and Sync para configurarlo. ["Más información"](#) .

Relaciones de sincronización admitidas en NetApp Copy and Sync

NetApp Copy and Sync le permite sincronizar datos desde un origen a un destino. Esto se llama relación de sincronización. Debes comprender las relaciones admitidas antes de comenzar.

Ubicación de la fuente	Ubicaciones de destino compatibles
Amazon EFS	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID
Amazon FSx para ONTAP	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID

Ubicación de la fuente	Ubicaciones de destino compatibles
Amazon S3	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Caja ¹ • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID
Blob de Azure	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID

Ubicación de la fuente	Ubicaciones de destino compatibles
Almacenamiento de Azure Data Lake Gen2	<ul style="list-style-type: none"> • Azure NetApp Files • Cloud Volumes ONTAP • FSx para ONTAP • Almacenamiento de objetos en la nube de IBM • Servidor NFS • ONTAP • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID
Azure NetApp Files	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID
Caja ¹	<ul style="list-style-type: none"> • Amazon FSx para ONTAP • Amazon S3 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Servidor SMB • StorageGRID

Ubicación de la fuente	Ubicaciones de destino compatibles
Cloud Volumes ONTAP	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID
Almacenamiento en la nube de Google	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID
Google Drive	<ul style="list-style-type: none"> • Servidor NFS • Servidor SMB

Ubicación de la fuente	Ubicaciones de destino compatibles
Almacenamiento de objetos en la nube de IBM	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Caja ¹ • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID
Servidor NFS	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Google Drive • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID

Ubicación de la fuente	Ubicaciones de destino compatibles
Clúster ONTAP local (NFS o SMB)	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID
Almacenamiento ONTAP S3	<ul style="list-style-type: none"> • Amazon S3 • Almacenamiento de Azure Data Lake Gen2 • Almacenamiento en la nube de Google • Servidor NFS • Servidor SMB • StorageGRID • Almacenamiento ONTAP S3
SFTP ²	S3

Ubicación de la fuente	Ubicaciones de destino compatibles
Servidor SMB	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Google Drive • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID
StorageGRID	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Caja ¹ • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID

Notas:

1. El soporte de Box está disponible como vista previa.
2. Las relaciones de sincronización con esta fuente/destino se admiten únicamente mediante la API de copia y sincronización.

3. Puede elegir un nivel de almacenamiento de blobs de Azure específico cuando un contenedor de blobs es el destino:
 - Almacenamiento en caliente
 - Almacenamiento en frío
4. [[clases de almacenamiento]]Puede elegir una clase de almacenamiento S3 específica cuando Amazon S3 es el destino:
 - Estándar (esta es la clase predeterminada)
 - Niveles inteligentes
 - Acceso estándar poco frecuente
 - Una zona - Acceso poco frecuente
 - Archivo de Glaciar Deep
 - Recuperación flexible de glaciares
 - Recuperación instantánea de glaciares
5. Puedes elegir una clase de almacenamiento específica cuando un depósito de Google Cloud Storage es el destino:
 - Estándar
 - Cerca de línea
 - Línea fría
 - Archivo

Preparar el origen y el destino en NetApp Copy and Sync

Verifique que su origen y sus destinos cumplan con los siguientes requisitos en NetApp Copy and Sync.

Redes

- El origen y el destino deben tener una conexión de red al grupo de intermediarios de datos.

Por ejemplo, si un servidor NFS está en su centro de datos y un agente de datos está en AWS, entonces necesita una conexión de red (VPN o Conexión directa) desde su red a la VPC.

- NetApp recomienda configurar el origen, el destino y los intermediarios de datos para utilizar un servicio de Protocolo de tiempo de red (NTP). La diferencia de tiempo entre los tres componentes no debe exceder los 5 minutos.

Directorio de destino

Cuando crea una relación de sincronización, Copiar y sincronizar le permite seleccionar un directorio de destino existente y luego, opcionalmente, crear una nueva carpeta dentro de ese directorio. Así que asegúrese de que su directorio de destino preferido ya exista.

Permisos para leer directorios

Para mostrar cada directorio o carpeta en un origen o destino, Copiar y sincronizar necesita permisos de lectura en el directorio o carpeta.

Sistema Nacional de Archivos

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 objetos 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 que ingrese al configurar una relación de sincronización deben tener permisos de objeto de lista.

SMB

Las credenciales SMB que ingrese 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-offload



Al copiar datos de SMB en Cloud Volumes ONTAP mediante Copiar y sincronizar, no se conserva la propiedad de los archivos y las carpetas del sistema de origen. Este comportamiento se produce porque Copy and Sync utiliza un cliente SMB de Linux, que asigna propiedad al usuario o a la cuenta de servicio utilizada para autenticar la transferencia. Si bien se pueden conservar las listas de control de acceso, la información de propiedad y auditoría puede diferir del sistema de origen. Este es el comportamiento esperado.

Requisitos del bucket de Amazon S3

Asegúrese de que su bucket de Amazon S3 cumpla con los siguientes requisitos.

Ubicaciones de agentes de datos compatibles con Amazon S3

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

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

Regiones de AWS compatibles

Se admiten todas las regiones excepto la de China.

Permisos necesarios para los buckets S3 en otras cuentas de AWS

Al configurar una relación de sincronización, puede especificar un bucket S3 que resida en una cuenta de AWS que no esté asociada con un agente de datos.

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


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

1. *<BucketName>* es el nombre del depósito que reside en la cuenta de AWS que no está asociada con un agente de datos.
2. *<RoleARN>* debe reemplazarse por uno de los siguientes:
 - Si se instaló manualmente un agente de datos en un host Linux, *RoleARN* debe ser el ARN del usuario de AWS para el que proporcionó las credenciales de AWS al implementar un agente de datos.
 - Si se implementó un agente de datos en AWS mediante la plantilla CloudFormation, *RoleARN* debe ser el ARN del rol de IAM creado por la plantilla.

Puede encontrar el ARN del rol yendo a la consola EC2, seleccionando la instancia del agente de datos y luego seleccionando el rol IAM en la pestaña Descripción. Luego debería ver la página Resumen en la consola IAM que contiene el ARN del rol.

Summary

[Delete role](#)

Role ARN `arn:aws:iam::542991777600:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05` 

Role description [Edit](#)

Requisitos de almacenamiento de blobs de Azure

Asegúrese de que su almacenamiento de blobs de Azure cumpla con los siguientes requisitos.

Ubicaciones de agentes de datos compatibles con Azure Blob


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

Regiones de Azure compatibles

Se admiten todas las regiones, excepto las de China, Gobierno de EE. UU. y Departamento de Defensa de EE. UU.

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

Al crear una relación de sincronización entre un contenedor de blobs de Azure y un servidor NFS o SMB, debe proporcionar Copiar y sincronizar con la cadena de conexión de la cuenta de almacenamiento:

 **a63cde60b553020** - Access keys

Storage account

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Storage Explorer (preview)

Settings

Access keys

CORS

Configuration

Encryption

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 blobs de Azure, 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 a todos los tipos de recursos (servicio, contenedor y objeto). El SAS también debe incluir los siguientes permisos:

- Para el contenedor Blob de origen: Leer y Listar
- Para el contenedor Blob de destino: Leer, Escribir, Listar, Agregar y Crear

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 elige implementar una relación de sincronización continua que incluya un contenedor de blobs de Azure, puede usar una cadena de conexión normal o una cadena de conexión SAS. Si se utiliza una cadena de conexión SAS, no debe configurarse para que caduque en el futuro cercano.

Almacenamiento de Azure Data Lake Gen2

Al crear una relación de sincronización que incluya Azure Data Lake, debe proporcionar Copiar y sincronizar con 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 hacia o desde Azure NetApp Files. Es posible que experimente fallas y problemas de rendimiento si el nivel de servicio del disco es Estándar.



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

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

Requisitos de la caja

- Para crear una relación de sincronización que incluya Box, deberá proporcionar las siguientes credenciales:
 - ID de cliente
 - Secreto del 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 agentes de datos que tenga una configuración unificada donde las siguientes configuraciones estén establecidas en 1:
 - Concurrencia del escáner
 - Límite de procesos del escáner
 - Concurrencia del transferente
 - Límite de procesos de transferencia

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

Requisitos del depósito de Google Cloud Storage

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

Ubicaciones de intermediarios de datos compatibles con Google Cloud Storage

Las relaciones de sincronización que incluyen Google Cloud Storage requieren un agente de datos implementado en Google Cloud o en sus instalaciones. Copiar y sincronizar lo guía a través del proceso de instalación del agente de datos cuando crea una relación de sincronización.

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

Regiones de Google Cloud compatibles

Se admiten todas las regiones.

Permisos para depósitos en otros proyectos de Google Cloud

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

Permisos para un destino SnapMirror

Si la fuente de una relación de sincronización es un destino SnapMirror (que es de solo lectura), los permisos de "lectura/lista" son suficientes para sincronizar datos desde la fuente a un destino.

Cómo cifrar un depósito de Google Cloud

Puedes cifrar un depósito de Google Cloud de destino con una clave KMS administrada por el cliente o con la clave predeterminada administrada por Google. Si el depósito ya tiene un cifrado KMS agregado, anulará el cifrado predeterminado administrado por Google.

Para agregar una clave KMS administrada por el cliente, deberá utilizar un agente de datos con la "[permisos correctos](#)", y la clave debe estar en la misma región que el depósito.

Google Drive

Cuando configure una relación de sincronización que incluya Google Drive, deberá proporcionar lo siguiente:

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

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

- "[Crear la cuenta de servicio y las credenciales](#)"
- "[Delegar autoridad de todo el dominio a su cuenta de servicio](#)"

Cuando edite el campo Ámbitos de OAuth, ingrese 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 NetApp o un sistema que no sea NetApp .
- El servidor de archivos debe permitir que un host de agente de datos acceda a las exportaciones a través de los puertos requeridos.
 - 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 habilitada en el servidor.

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



La configuración predeterminada para showmount está *habilitada* a partir de ONTAP 9.2.

Requisitos de ONTAP

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

Requisitos de almacenamiento de ONTAP S3

Cuando se configura una relación de sincronización que incluye ["Almacenamiento ONTAP S3"](#) , deberá proporcionar lo siguiente:

- La dirección IP del LIF que está conectado a ONTAP S3
- La clave de acceso y la clave secreta que ONTAP está configurado para usar

Requisitos del servidor SMB

- El servidor SMB puede ser un sistema NetApp o un sistema que no sea NetApp .
- Debe proporcionar Copiar y sincronizar con credenciales que tengan permisos en el servidor SMB.
 - Para un servidor SMB de origen, se requieren los siguientes permisos: lista y lectura.

Los miembros del grupo Operadores de respaldo reciben soporte de un servidor SMB de origen.
 - Para un servidor SMB de destino, se requieren los siguientes permisos: lista, lectura y escritura.
- El servidor de archivos debe permitir que un host de agente de datos acceda a las exportaciones a través de los puertos requeridos.
 - 139 TCP
 - 445 TCP
 - 137-138 UDP
- Se admiten las versiones 1.0, 2.0, 2.1, 3.0 y 3.11 de SMB.
- Otorgue al grupo "Administradores" permisos de "Control total" sobre las carpetas de origen y de destino.

Si no concede 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 los directorios y archivos ocultos al sincronizar datos entre servidores SMB. Si alguno de los directorios o archivos en el servidor SMB de origen se ocultó a través de Windows, el atributo oculto no se copia al servidor SMB de destino.

Comportamiento de sincronización SMB debido a la limitación de no distinguir entre mayúsculas y minúsculas

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

Por ejemplo, digamos que hay un archivo llamado "a" en el origen y un archivo llamado "A" en el destino. Cuando Copiar y sincronizar copia el archivo llamado "a" al 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 Copy and Sync intenta copiar el directorio llamado "b" al destino, Copy and Sync recibe un error que indica que el directorio ya existe. Como resultado, Copiar y sincronizar siempre falla al copiar el directorio llamado "b".

La mejor manera de evitar esta limitación es asegurarse de sincronizar los datos en un directorio vacío.

Descripción general de redes para NetApp Copy and Sync

La red para NetApp Copy and Sync incluye conectividad entre el grupo de agentes de datos y las ubicaciones de origen y destino, y una conexión a Internet saliente desde los agentes de datos a través del puerto 443.

Ubicación del corredor de datos

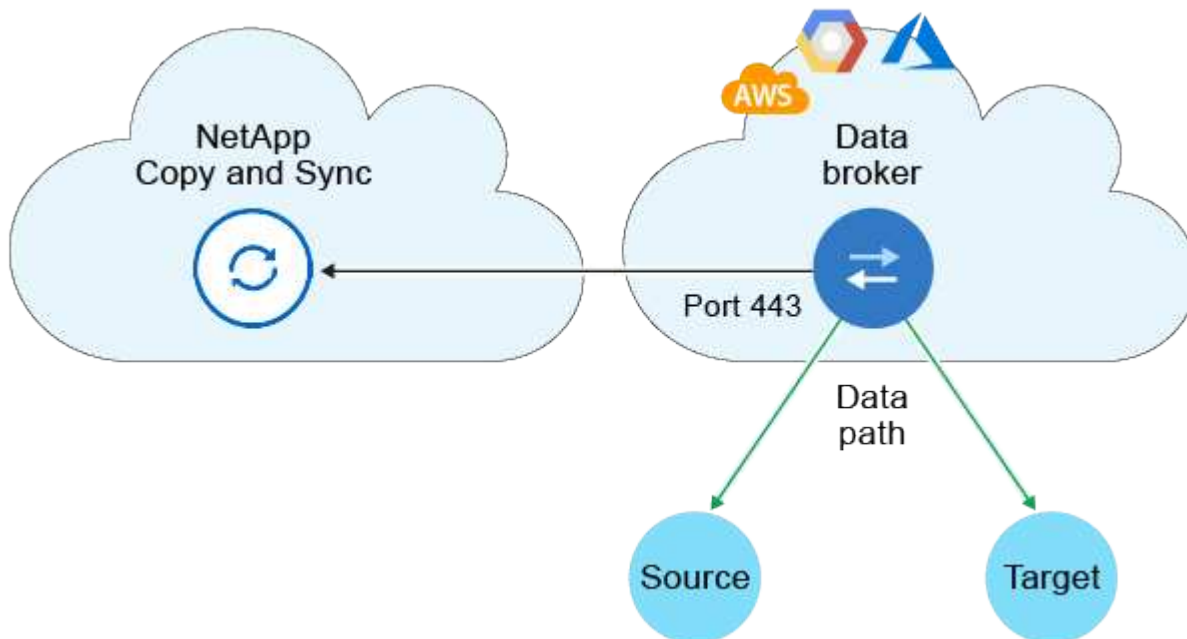
Un grupo de corredores de datos consta de uno o más corredores de datos instalados en la nube o en sus instalaciones.

Broker de datos en la nube

La siguiente imagen muestra un agente de datos ejecutándose en la nube, ya sea en AWS, Google Cloud o Azure. El origen y el destino pueden estar 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 a su proveedor de nube.



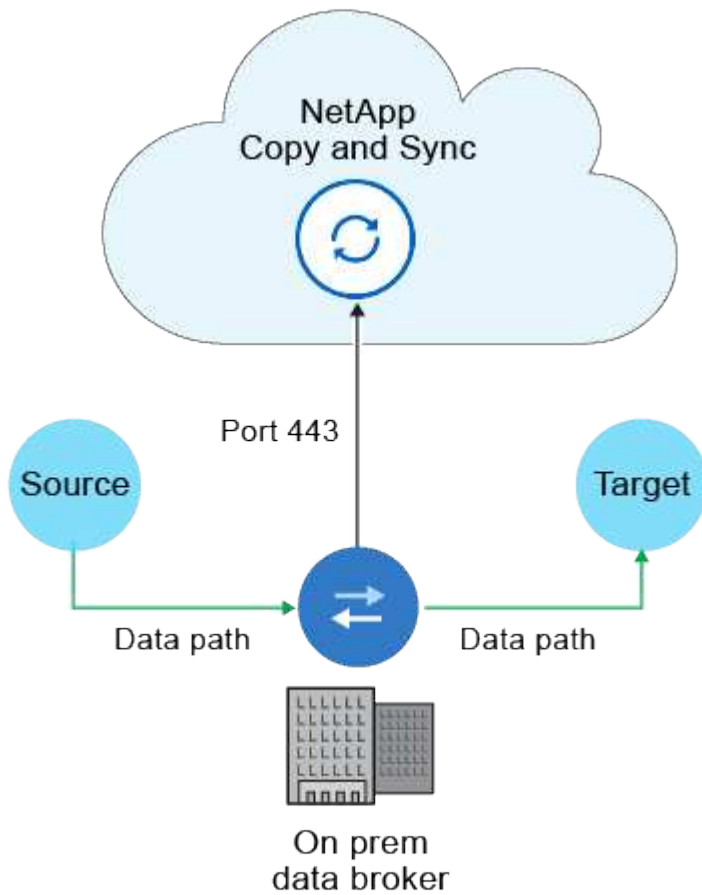
Cuando Copy and Sync implementa el agente de datos en AWS, Azure o Google Cloud, crea un grupo de seguridad que habilita la comunicación saliente requerida.



Corredor de datos en sus instalaciones

La siguiente imagen muestra el agente de datos ejecutándose localmente en un centro de datos. Nuevamente, la fuente y el destino pueden estar 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 al grupo de intermediarios de datos.

Por ejemplo, si un servidor NFS está en su centro de datos y un agente de datos está en AWS, entonces necesita una conexión de red (VPN o Conexión directa) desde su red a la VPC.

- Un agente de datos necesita una conexión a Internet saliente para poder sondear Copy and Sync en busca de tareas a través del puerto 443.
- NetApp recomienda configurar los intermediarios de origen, destino y datos para utilizar un servicio de Protocolo de tiempo de red (NTP). La diferencia de tiempo entre los tres componentes no debe exceder los 5 minutos.

Puntos finales de red

El agente de datos de NetApp requiere acceso a Internet saliente a través del puerto 443 para comunicarse con Copy and Sync y para contactar con algunos otros servicios y repositorios. Su navegador web local también requiere acceso a los puntos finales para determinadas acciones. Si necesita limitar la conectividad saliente, consulte la siguiente lista de puntos finales al configurar su firewall para el tráfico saliente.

Puntos finales del intermediario de datos

Un corredor de datos se pone en contacto con los siguientes puntos finales:

Puntos finales	Objetivo
\ https://olcentgbl.trafficmanager.net	Para ponerse en contacto con un repositorio para actualizar los paquetes de CentOS para el host del agente de datos. Solo se contacta con este punto final 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 los repositorios para actualizar Node.js, npm y otros paquetes de terceros utilizados en el desarrollo.
\ https://tgz.pm2.io	Para acceder a un repositorio para actualizar PM2, que es un paquete de terceros utilizado para monitorear Copiar y Sincronizar.
\ https://sqs.us-east-1.amazonaws.com \ https://kinesis.us-east-1.amazonaws.com	Para ponerse en contacto con los servicios de AWS que Copy and Sync utiliza para las operaciones (poner en cola archivos, registrar acciones y enviar actualizaciones al agente de datos).
\ https://s3.region.amazonaws.com Por ejemplo: s3.us-east-2.amazonaws.com:443 https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region ["Consulte la documentación de AWS para obtener una lista de puntos finales de S3"]	Para ponerse en contacto con Amazon S3 cuando una relación de sincronización incluye un bucket S3.
\ https://s3.amazonaws.com/	Cuando descarga registros del agente de datos desde Copy and Sync, el agente de datos comprime su directorio de registros y carga los registros en un depósito S3 predefinido en la región us-east-1.
\ https://storage.googleapis.com/	Para ponerse en contacto con Google Cloud cuando una relación de sincronización utiliza un depósito de GCP.
https://storage-account.blob.core.windows.net Si utiliza Azure Data Lake Gen2: https://storage-account.dfs.core.windows.net Donde storage-account 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 contactar con Copiar y Sincronizar.
\ https://support.netapp.com	Para ponerse en contacto con el soporte de NetApp cuando se utiliza una licencia BYOL para relaciones de sincronización.
\ https://fedoraproject.org	Para instalar 7z en la máquina virtual del agente de datos durante la instalación y las actualizaciones. Se necesita 7z para enviar mensajes de AutoSupport al soporte técnico de NetApp .

Puntos finales	Objetivo
\ https://sts.amazonaws.com \ https://sts.us-east-1.amazonaws.com	Para verificar las credenciales de AWS cuando el agente de datos se implementa en AWS o cuando se implementa en sus instalaciones y se proporcionan las credenciales de AWS. El agente de datos se comunica con este punto final durante la implementación, cuando se actualiza y cuando se reinicia.
\ https://api.blueexp.netapp.com \ https://netapp-cloud-account.auth0.com	Para ponerse en contacto con NetApp Data Classification cuando utiliza la clasificación para seleccionar los archivos de origen para una nueva relación de sincronización.
\ https://pubsub.googleapis.com	Si se 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 storage-account es la cuenta de almacenamiento de origen del usuario, subscriptionid es el ID de suscripción de origen y resourceGroup es el grupo de recursos de origen.	Si se crea una relación de sincronización continua desde una cuenta de almacenamiento de Azure.

Puntos finales del navegador web

Su navegador web necesita acceso al siguiente punto final para descargar registros con fines de resolución de problemas:

registros.cloudsync.netapp.com:443

Inicie sesión en NetApp Copy and Sync

Utilice la NetApp Console para iniciar sesión en NetApp Copy and Sync.

Para iniciar sesión en la consola, puede usar sus credenciales del sitio de soporte de NetApp o puede registrarse para iniciar sesión en la nube de NetApp usando su correo electrónico y una contraseña. ["Obtenga más información sobre cómo iniciar sesión"](#) .

NetApp Copy and Sync utiliza la gestión de acceso de identidad para controlar el acceso que tiene cada usuario a acciones específicas.

Rol de NetApp Console obligatorio Rol de administrador de la organización. ["Obtenga más información sobre los roles de acceso a la NetApp Console"](#) .

Pasos

1. Abra un navegador web y vaya a ["NetApp Console"](#) .

Aparece la página de inicio de sesión de la NetApp Console .

2. Inicie sesión en la consola.
3. Desde la navegación izquierda de la consola, seleccione **Movilidad > Copiar y sincronizar**.

Instalar un agente de datos

Cree un nuevo agente de datos en AWS para NetApp Copy and Sync

Cuando crea un nuevo grupo de agente de datos para NetApp Copy and Sync, elija Amazon Web Services para implementar el software del agente de datos en una nueva instancia EC2 en una VPC. NetApp Copy and Sync lo guía a través del proceso de instalación, pero los requisitos y pasos se repiten en esta página para ayudarlo a prepararse para la instalación.

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

Regiones de AWS compatibles

Se admiten todas las regiones excepto la de China.

Privilegios de root

El software del intermediario de datos se ejecuta automáticamente como root en el host Linux. Ejecutarse como root es un requisito para las operaciones del agente de datos. Por ejemplo, para montar acciones.

Requisitos de red

- El agente de datos necesita una conexión a Internet saliente para poder sondear Copy and Sync en busca de tareas a través del puerto 443.

Cuando Copy and Sync implementa el agente de datos en AWS, crea un grupo de seguridad que habilita la comunicación saliente requerida. Tenga en cuenta que puede configurar el agente de datos para utilizar un servidor proxy durante el proceso de instalación.

Si necesita limitar la conectividad saliente, consulte ["la lista de puntos finales con los que se pone en contacto el agente de datos"](#) .

- NetApp recomienda configurar el origen, el destino y el agente de datos para utilizar un servicio de Protocolo de tiempo de red (NTP). La diferencia de tiempo entre los tres componentes no debe exceder los 5 minutos.

Permisos necesarios para implementar el agente de datos en AWS

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

Requisitos para usar su propio rol de IAM con el agente de datos de AWS

Cuando Copy and Sync implementa el agente de datos, crea una función de IAM para la instancia del agente de datos. Puede implementar el agente de datos utilizando su propio rol de IAM, si lo prefiere. Puede utilizar esta opción si su organización tiene políticas de seguridad estrictas.

El rol de IAM debe cumplir los siguientes requisitos:

- Se debe permitir que el servicio EC2 asuma el rol de IAM como entidad confiable.
- "Los permisos definidos en este archivo JSON" debe estar asociado al rol IAM para que el agente de datos pueda funcionar correctamente.

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

Crear el agente de datos

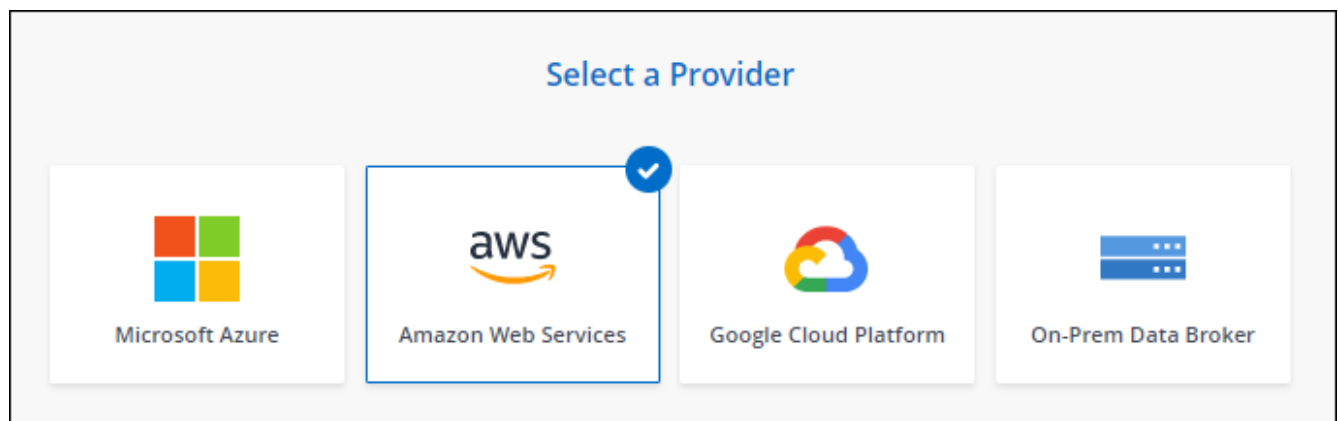
Hay algunas formas de crear un nuevo corredor de datos. Estos pasos describen cómo instalar un agente de datos en AWS al crear una relación de sincronización.

Pasos

1. "Iniciar sesión en Copiar y sincronizar" .
2. Seleccione **Crear nueva sincronización**.
3. En la página **Definir relación de sincronización**, elija un origen y un destino y seleccione **Continuar**.

Complete los pasos hasta llegar a la página **Data Broker Group**.

4. En la página **Grupo de agente de datos**, seleccione **Crear agente de datos** y luego seleccione **Amazon Web Services**.



5. Ingrese un nombre para el agente de datos y seleccione **Continuar**.
6. Ingrese una clave de acceso de AWS para que Copy and Sync pueda crear el agente de datos en AWS en su nombre.

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

Si prefiere no proporcionar claves de acceso, seleccione el enlace en la parte inferior de la página para utilizar una plantilla de CloudFormation en su lugar. Cuando utiliza esta opción, no necesita proporcionar credenciales porque está iniciando sesión directamente en AWS.

El siguiente video muestra cómo iniciar la instancia del agente de datos utilizando una plantilla de

CloudFormation:

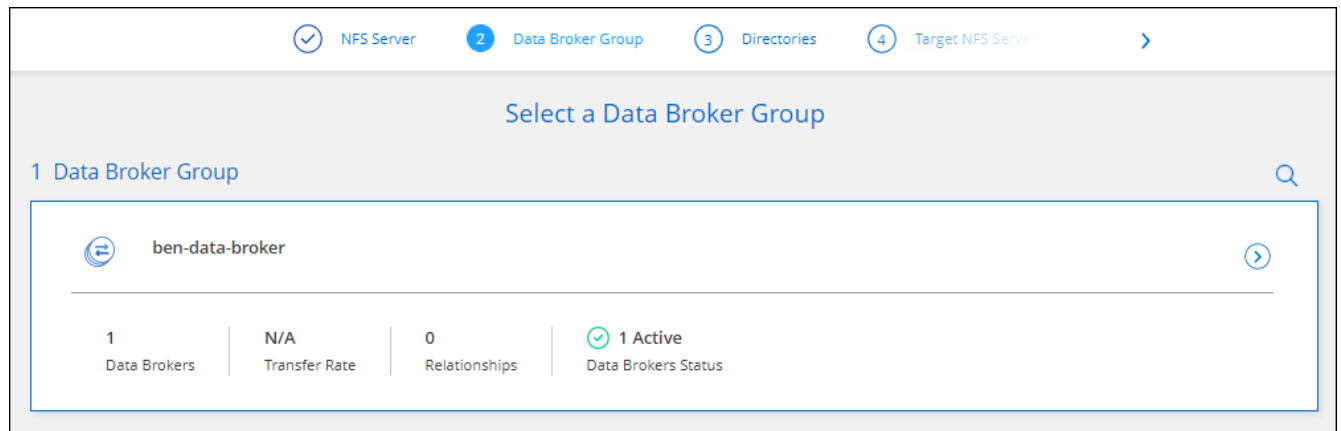
Iniciar un agente de datos desde una plantilla de AWS CloudFormation

7. Si ingresó 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 una función de IAM existente, o deje el campo en blanco para que Copiar y sincronizar cree la función por usted. También tiene la opción de cifrar su agente de datos utilizando una clave KMS.

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

8. Especifique una configuración de proxy, si se requiere un proxy para el acceso a Internet en la VPC.
9. Una vez que el agente de datos esté disponible, seleccione **Continuar** en Copiar y sincronizar.

La siguiente imagen muestra una instancia implementada correctamente en AWS:



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

Resultado

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

Detalles sobre la instancia del agente de datos

Copiar y sincronizar crea un agente de datos en AWS utilizando la siguiente configuración.

Compatibilidad con Node.js

v21.2.0

Tipo de instancia

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

vCPU

4

RAM

16 GB

Sistema operativo

Amazon Linux 2023

Tamaño y tipo de disco

SSD GP2 de 10 GB

Cree un nuevo agente de datos en Azure para NetApp Copy and Sync

Cuando crea un nuevo grupo de agentes de datos para NetApp Copy and Sync, elija Microsoft Azure para implementar el software del agente de datos en una nueva máquina virtual en una VNet. NetApp Copy and Sync lo guía a través del proceso de instalación, pero los requisitos y pasos se repiten en esta página para ayudarlo a prepararse para la instalación.

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

Regiones de Azure compatibles

Se admiten todas las regiones, excepto las de China, Gobierno de EE. UU. y Departamento de Defensa de EE. UU.

Privilegios de root

El software del intermediario de datos se ejecuta automáticamente como root en el host Linux. Ejecutarse como root es un requisito para las operaciones del agente de datos. Por ejemplo, para montar acciones.

Requisitos de red

- El agente de datos necesita una conexión a Internet saliente para poder sondear el servicio de copia y sincronización en busca de tareas a través del puerto 443.

Cuando Copy and Sync implementa el agente de datos en Azure, crea un grupo de seguridad que habilita la comunicación saliente requerida.

Si necesita limitar la conectividad saliente, consulte [la lista de puntos finales con los que se pone en contacto el agente de datos](#).

- NetApp recomienda configurar el origen, el destino y el agente de datos para utilizar un servicio de Protocolo de tiempo de red (NTP). La diferencia de tiempo entre los tres componentes no debe exceder los 5 minutos.

Permisos necesarios para implementar el agente de datos en Azure

Asegúrese de que la cuenta de usuario de Azure que utiliza 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"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write"

```

```
"Microsoft.Network/networkSecurityGroups/securityRules/read",  
"Microsoft.Network/networkSecurityGroups/read",
```

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

Nota:

1. Los siguientes permisos solo son necesarios si planea habilitar el ["Configuración de sincronización continua"](#) en una relación de sincronización de Azure a otra ubicación de almacenamiento en la nube:

- 'Microsoft.Storage/storageAccounts/read',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/write',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/leer',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/eliminar',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/acción',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes/acción',
- 'Microsoft.EventGrid/systemTopics/leer',
- 'Microsoft.EventGrid/systemTopics/escritura',
- 'Microsoft.EventGrid/systemTopics/eliminar',
- 'Microsoft.EventGrid/eventSubscriptions/escritura',
- 'Microsoft.Storage/storageAccounts/write'

Además, el alcance asignable debe establecerse en el alcance de suscripción y **no** en el alcance del grupo de recursos si planea implementar sincronización continua en Azure.

2. Los siguientes permisos solo son necesarios si planea elegir su propia seguridad para la creación del agente de datos:

- "Microsoft.Network/networkSecurityGroups/securityRules/read"
- "Microsoft.Network/networkSecurityGroups/read"

Método de autenticación

Al implementar el agente de datos, deberá elegir un método de autenticación para la máquina virtual: una contraseña o un par de claves pública-privada SSH.

Para obtener ayuda con la creación de un par de claves, consulte ["Documentación de Azure: Crear y usar un par de claves públicas y privadas SSH para máquinas virtuales Linux en Azure"](#) .

Crear el agente de datos

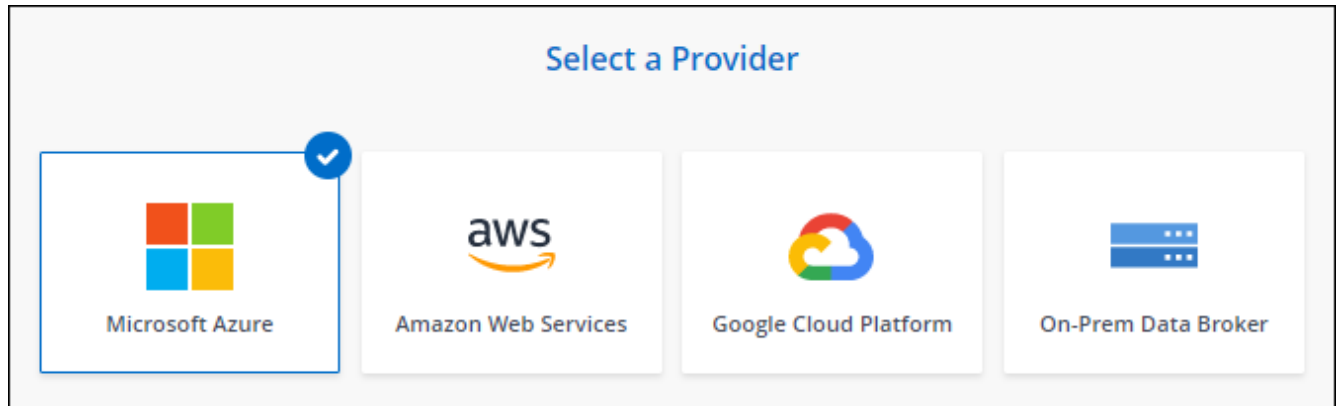
Hay algunas formas de crear un nuevo corredor de datos. Estos pasos describen cómo instalar un agente de datos en Azure cuando se crea una relación de sincronización.

Pasos

1. "Iniciar sesión en Copiar y sincronizar" .
2. Seleccione **Crear nueva sincronización**.
3. En la página **Definir relación de sincronización**, elija un origen y un destino y seleccione **Continuar**.

Complete los pasos hasta llegar a la página **Data Broker Group**.

4. En la página **Grupo de agentes de datos**, seleccione **Crear agente de datos** y luego seleccione **Microsoft Azure**.



5. Ingrese un nombre para el agente de datos y seleccione **Continuar**.
6. Si se le solicita, inicie sesión en su cuenta Microsoft. Si no se le solicita, seleccione **Iniciar sesión en Azure**.

El formulario es propiedad de Microsoft y está alojado por esta empresa. Sus credenciales no se proporcionan a NetApp.

7. Seleccione una ubicación para el agente de datos e ingrese detalles básicos sobre la máquina virtual.

Location	Connectivity
Subscription <div>Select a subscription</div>	VM Name <div>netappdatabroker</div>
Azure Region <div>Select a region</div>	User Name <div>databroker</div>
VNet <div>Select a VNet</div>	Authentication Method: <input checked="" type="radio"/> Password <input type="radio"/> Public Key
Subnet <div>Select a subnet</div>	Enter Password <div></div>
Public IP <div>Enable</div>	Resource Group: <input checked="" type="radio"/> Generate a new group <input type="radio"/> Use an existing group
Data Broker Role <input type="checkbox"/> Create Custom Role <i>Notice: Only relevant for continuous sync relationships from Azure. Users can also manually create this later.</i>	Security 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 un rol personalizado a su agente de datos. Esto también se puede hacer manualmente después de crear el bróker.

8. Especifique una configuración de proxy, si se requiere un proxy para el acceso a Internet en la red virtual.
9. Seleccione **Continuar**. Si desea agregar permisos S3 a su agente de datos, ingrese sus claves secretas y de acceso de AWS.
10. Seleccione **Continuar** y mantenga la página abierta hasta que se complete la implementación.

El proceso puede tardar hasta 7 minutos.

11. En Copiar y sincronizar, seleccione **Continuar** una vez que el agente de datos esté disponible.
12. Complete las páginas del asistente para crear la nueva relación de sincronización.

Resultado

Ha implementado un agente de datos en Azure y ha creado una nueva relación de sincronización. Puede utilizar este agente de datos con relaciones de sincronización adicionales.

¿Recibes un mensaje sobre la necesidad de consentimiento del administrador?

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

1. Pídale a su administrador de AD que le proporcione el siguiente permiso:

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

2. Pídale a su administrador de AD que dé su consentimiento en su nombre para **CloudSync-AzureDataBrokerCreator** mediante la siguiente URL (este es el punto final de consentimiento del administrador):

\ [https://login.microsoftonline.com/ {RELLENE 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](https://login.microsoftonline.com/{RELLENE 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, la URL de nuestra aplicación es \ <https://cloudsync.netapp.com> y el ID del cliente de la aplicación es 8ee4ca3a-bafa-4831-97cc-5a38923cab85.

Detalles sobre la máquina virtual del agente de datos

Copiar y sincronizar crea un agente de datos en Azure mediante la siguiente configuración.

Compatibilidad con Node.js

v21.2.0

Tipo de VM

Estándar DS4 v2

vCPU

8

RAM

28 GB

Sistema operativo

Rocky Linux 9.0

Tamaño y tipo de disco

SSD premium de 64 GB

Cree un nuevo agente de datos en Google Cloud para NetApp Copy and Sync

Cuando crea un nuevo grupo de agente de datos para NetApp Copy and Sync, elija Google Cloud Platform para implementar el software del agente de datos en una nueva

instancia de máquina virtual en una VPC de Google Cloud. NetApp Copy and Sync lo guía a través del proceso de instalación, pero los requisitos y pasos se repiten en esta página para ayudarlo a prepararse para la instalación.

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

Regiones de Google Cloud compatibles

Se admiten todas las regiones.

Privilegios de root

El software del intermediario de datos se ejecuta automáticamente como root en el host Linux. Ejecutarse como root es un requisito para las operaciones del agente de datos. Por ejemplo, para montar acciones.

Requisitos de red

- El agente de datos necesita una conexión a Internet saliente para poder sondear Copy and Sync en busca de tareas a través del puerto 443.

Cuando Copy and Sync implementa el agente de datos en Google Cloud, crea un grupo de seguridad que habilita la comunicación saliente requerida.

Si necesita limitar la conectividad saliente, consulte ["la lista de puntos finales con los que se pone en contacto el agente de datos"](#) .

- NetApp recomienda configurar el origen, el destino y el agente de datos para utilizar un servicio de Protocolo de tiempo de red (NTP). La diferencia de tiempo entre los tres componentes no debe exceder 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 tenga 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
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

Notas:

1. El permiso "iam.serviceAccounts.signJwt" solo es necesario si planea configurar el agente de datos para utilizar una bóveda externa de HashiCorp.
2. Los permisos "pubsub.*" y "storage.buckets.update" solo son necesarios si planea habilitar la configuración de sincronización continua en una relación de sincronización de Google Cloud Storage a otra ubicación de almacenamiento en la nube. ["Obtenga más información sobre la opción Sincronización continua"](#) .
3. Los permisos "cloudkms.cryptoKeys.list" y "cloudkms.keyRings.list" solo son necesarios si planea usar una clave KMS administrada por el cliente en un depósito de Google Cloud Storage de destino.

Crear el agente de datos

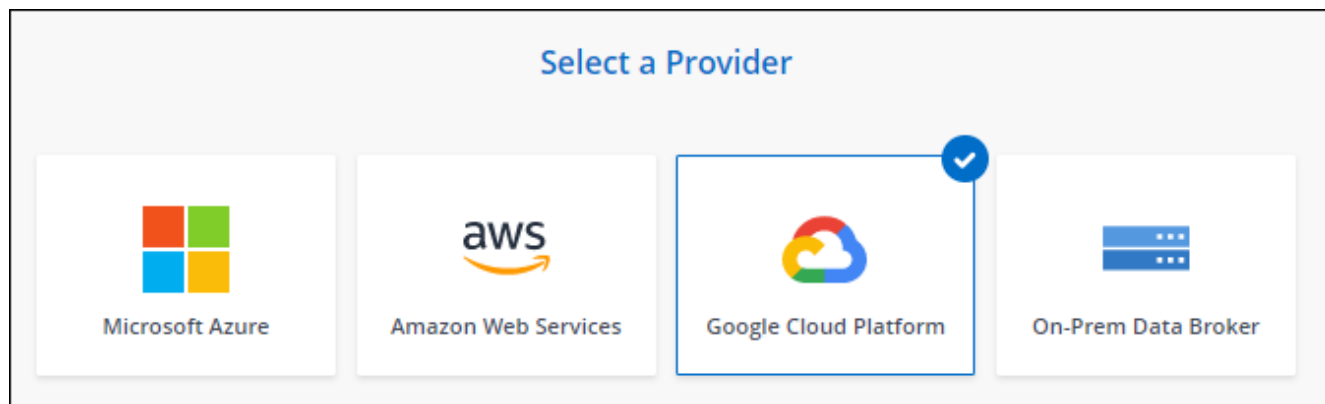
Hay algunas formas de crear un nuevo corredor de datos. Estos pasos describen cómo instalar un agente de datos en Google Cloud cuando se crea una relación de sincronización.

Pasos

1. ["Iniciar sesión en Copiar y sincronizar"](#) .
2. Seleccione **Crear nueva sincronización**.
3. En la página **Definir relación de sincronización**, elija un origen y un destino y seleccione **Continuar**.

Complete los pasos hasta llegar a la página **Data Broker Group**.

4. En la página **Grupo de corredores de datos**, seleccione **Crear corredor de datos** y luego seleccione **Google Cloud Platform**.



5. Ingrese un nombre para el agente de datos y seleccione **Continuar**.
6. Si se le solicita, inicie sesión con su cuenta de Google.

El formulario es propiedad de Google y está alojado por esta empresa. Sus credenciales no se proporcionan a NetApp.

7. Seleccione un proyecto y una cuenta de servicio y luego elija una ubicación para el agente de datos, incluso si desea habilitar o deshabilitar una dirección IP pública.

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

Basic Settings

Project Project <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">OCCM-Dev ▼</div> Service Account <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">test ▼</div> Select a Service Account that includes these permissions	Location Region <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">us-west1 ▼</div> Zone <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">us-west1-a ▼</div> VPC <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">default ▼</div> Subnet <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">default ▼</div> Public IP <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">Enable ▼</div>
--	---

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

Si se requiere un proxy para acceder a Internet, entonces el proxy debe estar en Google Cloud y usar la misma cuenta de servicio que el agente de datos.

9. Una vez que el agente de datos esté disponible, seleccione **Continuar** en Copiar y sincronizar.

La instancia tarda aproximadamente entre 5 y 10 minutos en implementarse. Puede supervisar el progreso desde Copiar y sincronizar, que se actualiza automáticamente cuando la instancia está disponible.

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

Resultado

Implementó un agente de datos en Google Cloud y creó una nueva relación de sincronización. Puede utilizar este agente de datos con relaciones de sincronización adicionales.

Proporcionar permisos para usar buckets en otros proyectos de Google Cloud

Cuando crea una relación de sincronización y elige Google Cloud Storage como origen o destino, Copiar y sincronizar le permite elegir entre los depósitos que la cuenta de servicio del agente de datos tiene permisos para usar. De forma predeterminada, esto incluye los depósitos que están en el *mismo* proyecto que la cuenta de servicio del agente de datos. Pero puedes elegir depósitos de *otros* proyectos si proporcionas los permisos necesarios.

Pasos

1. Abra la consola de Google Cloud Platform y cargue el servicio Cloud Storage.
2. Seleccione el nombre del depósito que desea utilizar como origen o destino en una relación de sincronización.
3. Seleccione **Permisos**.
4. Seleccione **Agregar**.
5. Introduzca el nombre de la cuenta de servicio del agente de datos.
6. Seleccione un rol que proporcionelos mismos permisos que se muestran arriba .
7. Seleccione **Guardar**.

Resultado

Cuando configura una relación de sincronización, ahora puede elegir ese depósito como origen o destino en la relación de sincronización.

Detalles sobre la instancia de VM del agente de datos

Copiar y sincronizar crea un agente de datos en Google Cloud utilizando la siguiente configuración.

Compatibilidad con Node.js

v21.2.0

Tipo de máquina

n2-estándar-4

vCPU

4

RAM

15 GB

Sistema operativo

Rocky Linux 9,0

Tamaño y tipo de disco

Disco duro pd estándar de 20 GB

Instalar el agente de datos en un host Linux para NetApp Copy and Sync

Cuando cree un nuevo grupo de agentes de datos para NetApp Copy and Sync, elija la opción Agente de datos local para instalar el software del agente de datos en un host Linux local o en un host Linux existente en la nube. NetApp Copy and Sync lo guía a través del proceso de instalación, pero los requisitos y pasos se repiten en esta página para ayudarlo a prepararse para la instalación.

Requisitos del host Linux

- **Compatibilidad con Node.js:** v21.2.0
- **Sistema operativo:**

- CentOS 8.0 y 8.5

CentOS Stream no es compatible.

- Red Hat Enterprise Linux 8.5, 8.8, 8.9 y 9.4
- Rocky Linux 9
- Servidor Ubuntu 20.04 LTS, 23.04 LTS y 24.04 LTS
- Servidor empresarial SUSE Linux 15 SP1

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

Un sistema Red Hat Enterprise Linux debe estar registrado en Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software de terceros requerido durante la instalación.

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

SELinux aplica una política que bloquea las actualizaciones del software del agente de datos y puede impedir que el agente de datos se comuniquen con los puntos finales necesarios para el funcionamiento normal.

Privilegios de root

El software del intermediario de datos se ejecuta automáticamente como root en el host Linux. Ejecutarse como root es un requisito para las operaciones del agente de datos. Por ejemplo, para montar acciones.

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 agente de datos para utilizar un servicio de Protocolo de tiempo de red (NTP). La diferencia de tiempo entre los tres componentes no debe exceder los 5 minutos.

Habilitar el acceso a AWS

Si planea utilizar el agente de datos con una relación de sincronización que incluye un bucket S3, entonces debe preparar el host Linux para el acceso a AWS. Cuando instale el agente de datos, deberá proporcionar claves de AWS para un usuario de AWS que tenga acceso programático y permisos específicos.

Pasos

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

["Ver instrucciones de AWS"](#)

2. Cree un usuario de IAM que tenga acceso programático.

["Ver instrucciones de AWS"](#)

Asegúrese de copiar las claves de AWS porque deberá especificarlas cuando instale el software del agente de datos.

Habilitar el acceso a Google Cloud

Si planea utilizar el agente de datos con una relación de sincronización que incluye un depósito de Google Cloud Storage, entonces debe preparar el host Linux para el acceso a Google Cloud. Cuando instale el agente de datos, 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 aún no tiene una.
2. Crea una clave de cuenta de servicio guardada en formato JSON.

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

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



Cuando creas una clave, el archivo se genera y se descarga en tu máquina.

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 sincronización de relaciones.

Instalar el agente de datos

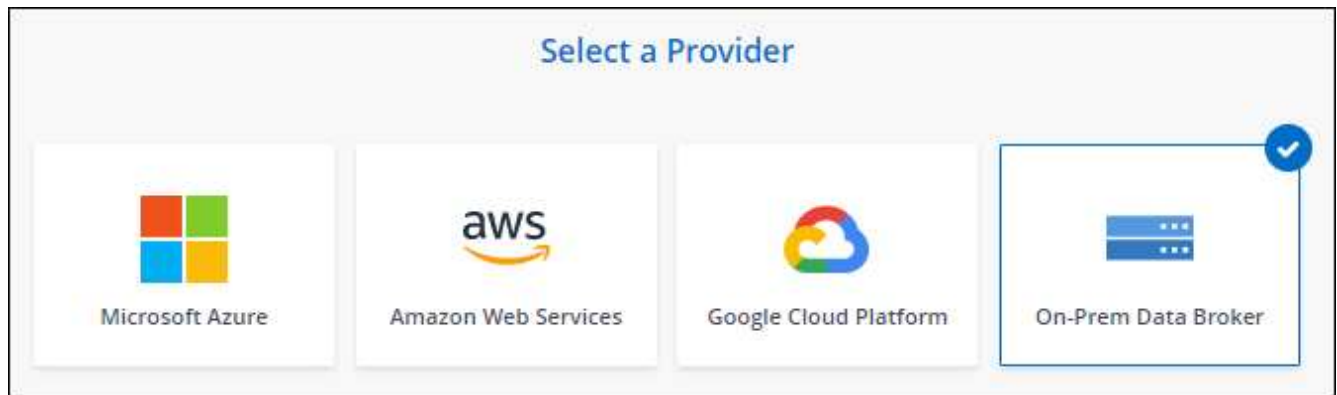
Puede instalar un agente de datos en un host Linux cuando crea una relación de sincronización.

Pasos

1. ["Iniciar sesión en Copiar y sincronizar"](#) .
2. Seleccione **Crear nueva sincronización**.
3. En la página **Definir relación de sincronización**, elija un origen y un destino y seleccione **Continuar**.

Complete los pasos hasta llegar a la página **Data Broker Group**.

4. En la página **Grupo de agente de datos**, seleccione **Crear agente de datos** y luego seleccione **Agente de datos local**.



Aunque la opción está etiquetada como **On-Prem Data Broker**, se aplica a un host Linux en sus instalaciones o en la nube.

5. Ingrese un nombre para el agente de datos y seleccione **Continuar**.

La página de instrucciones se cargará en breve. Necesitará seguir estas instrucciones; incluyen un enlace único para descargar el instalador.

6. En la página de instrucciones:

- Seleccione si desea habilitar el acceso a **AWS**, **Google Cloud** o ambos.
- Seleccione una opción de instalación: **Sin proxy**, **Usar servidor proxy** o **Usar servidor proxy con autenticación**.



El usuario debe ser un usuario local. Los usuarios del dominio no son compatibles.

- Utilice los comandos para descargar e instalar el agente de datos.

Los siguientes pasos proporcionan detalles sobre cada posible opción de instalación. Siga la página de instrucciones para obtener el comando exacto según su opción de instalación.

- Descargar el instalador:

- Sin proxy:

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

- Utilice el servidor proxy:

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

- Utilice un servidor proxy con autenticación:

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

URI

Copiar y sincronizar muestra la URI del archivo de instalación en la página de instrucciones, que se carga cuando sigue las indicaciones para implementar el agente de datos local. Esa URI no se repite aquí porque el enlace se genera dinámicamente y solo se puede usar una vez.

[Siga estos pasos para obtener la URI de Copiar y sincronizar](#).

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



Cada comando enumerado a continuación incluye parámetros para el acceso a AWS y al acceso a Google Cloud. Siga la página de instrucciones para obtener el comando exacto según su 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 de 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 debes tener preparadas [siguiendo estos pasos](#) . Las claves de AWS se almacenan en el agente de datos, que se ejecuta en su red local o en la nube. NetApp no utiliza las claves fuera del agente de datos.

archivo JSON

Este es el archivo JSON que contiene una clave de cuenta de servicio que debería tener preparadas [siguiendo estos pasos](#) .

7. Una vez que el agente de datos esté disponible, seleccione **Continuar** en Copiar y sincronizar.
8. Complete las páginas del asistente para crear la nueva relación de sincronización.

Utilice NetApp Copy and Sync

Sincronizar datos entre un origen y un destino

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

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


Acerca de esta tarea

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

Antes de empezar

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

Pasos

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

Resultado

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

¿Que sigue?

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

Crear relaciones de sincronización en NetApp Copy and Sync

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

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

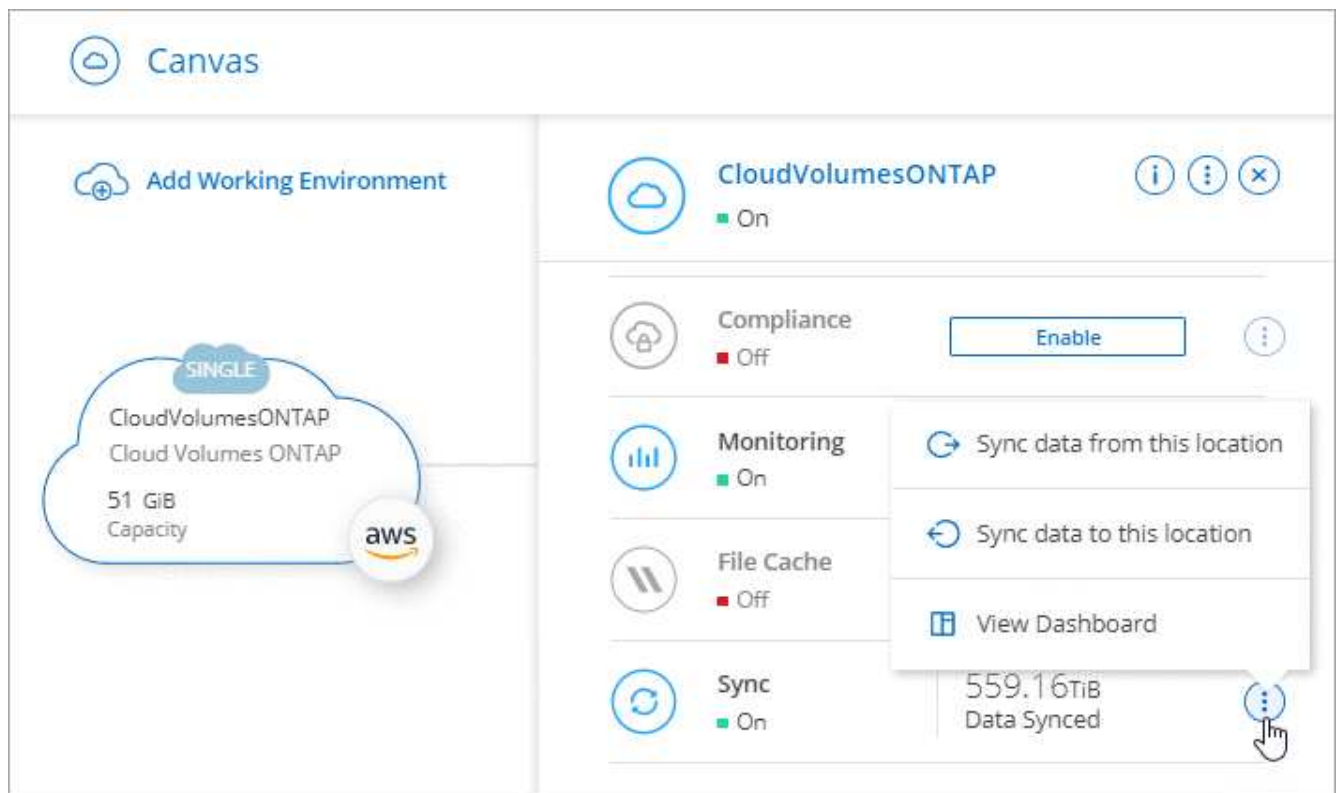
Crear relaciones de sincronización para tipos específicos de sistemas

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

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

Pasos

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



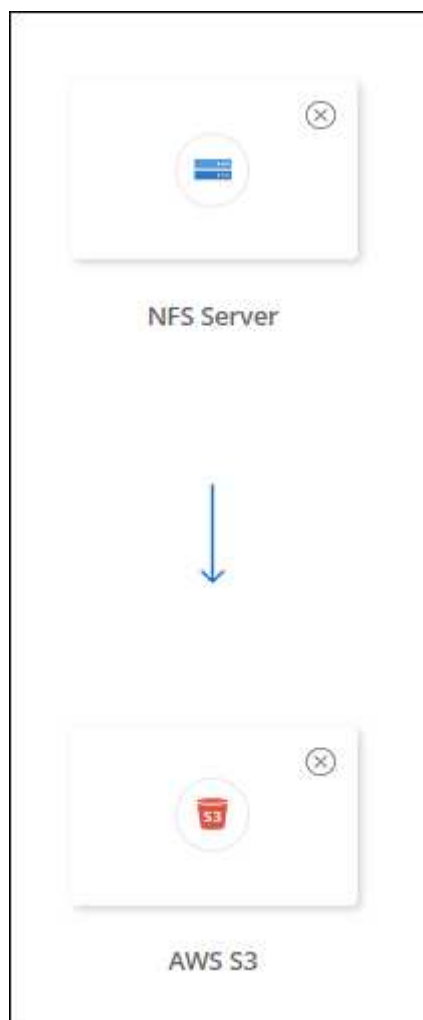
6. Seleccione **Sincronizar datos desde esta ubicación** o **Sincronizar datos con esta ubicación** y siga las instrucciones para configurar la relación de sincronización.

Crear otros tipos de relaciones de sincronización

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

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

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

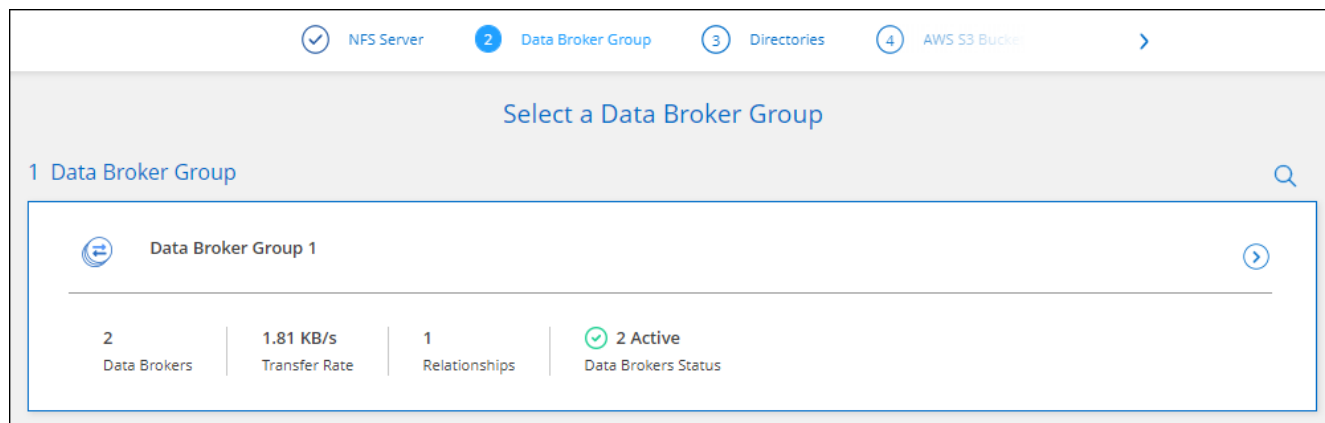


3. En la página **Servidor NFS**, ingrese la dirección IP o el nombre de dominio completo del servidor NFS que desea sincronizar con AWS.
4. En la página **Grupo de agente de datos**, siga las instrucciones para crear una máquina virtual de agente de datos en AWS, Azure o Google Cloud Platform, o para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

Para más detalles, consulte las siguientes páginas:

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

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



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

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



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

7. En la página **AWS S3 Bucket**, seleccione un bucket:

- Desplácese hacia abajo para seleccionar una carpeta existente dentro del depósito o para seleccionar una nueva carpeta que cree dentro del depósito.
- Seleccione **Agregar a la lista** para seleccionar un depósito S3 que no esté asociado con su cuenta de AWS. ["Se deben aplicar permisos específicos al bucket S3"](#) .

8. En la página **Configuración del depósito**, configure el depósito:

- Elija si desea habilitar el cifrado del bucket S3 y luego seleccione una clave AWS KMS, ingrese el ARN de una clave KMS o seleccione el cifrado AES-256.
- Seleccione una clase de almacenamiento S3. ["Ver las clases de almacenamiento admitidas"](#) .

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

Cronograma

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

Tiempo de espera de sincronización

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

Notificaciones

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

Reintentos

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

Sincronización continua

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

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

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

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

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

- Vaya a la consola de Google Cloud para el proyecto del depósito externo.
- Vaya a **Almacenamiento en la nube > Configuración > Cuenta de servicio de almacenamiento en la nube**.
- Actualice el archivo local.json:

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

- Reiniciar el agente de datos:
 - sudo pm2 detener todo
 - sudo pm2 start all
- Cree una relación de sincronización continua con el depósito externo relevante.



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

Comparar por

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

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

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

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

Copiar para objetos

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

No puedes editar esta opción después de crear la relación.

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

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

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

Archivos modificados recientemente

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

Eliminar archivos en la fuente

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

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

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

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

Eliminar archivos en el destino

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

Tipos de archivos

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



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

Excluir extensiones de archivo

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

Excluir extensiones de archivo para una relación de sincronización



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

Excluir directorios

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



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

Tamaño del archivo

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

Fecha de modificación

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

Fecha de creación

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

ACL - Lista de control de acceso

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

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



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

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

Resultado

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

Crear relaciones de sincronización desde NetApp Data Classification

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

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

Sync Relationship

1 Data Sense Integration 2 Data Broker Group 3 NFS Server 4 Directories

How does it work?

Selected Data Sense Source

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

A few more things before we continue

Define SMB Credentials:

User Name Password Domain (Optional)

["Aprenda a iniciar una relación de sincronización desde NetApp Data Classification"](#) .

Copiar ACL de recursos compartidos SMB en NetApp Copy and Sync

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

Opciones

- [Configurar Copiar y sincronizar para copiar ACL automáticamente](#)
- [Copiar manualmente las ACL entre recursos compartidos SMB](#)

Configurar Copiar y sincronizar para copiar ACL

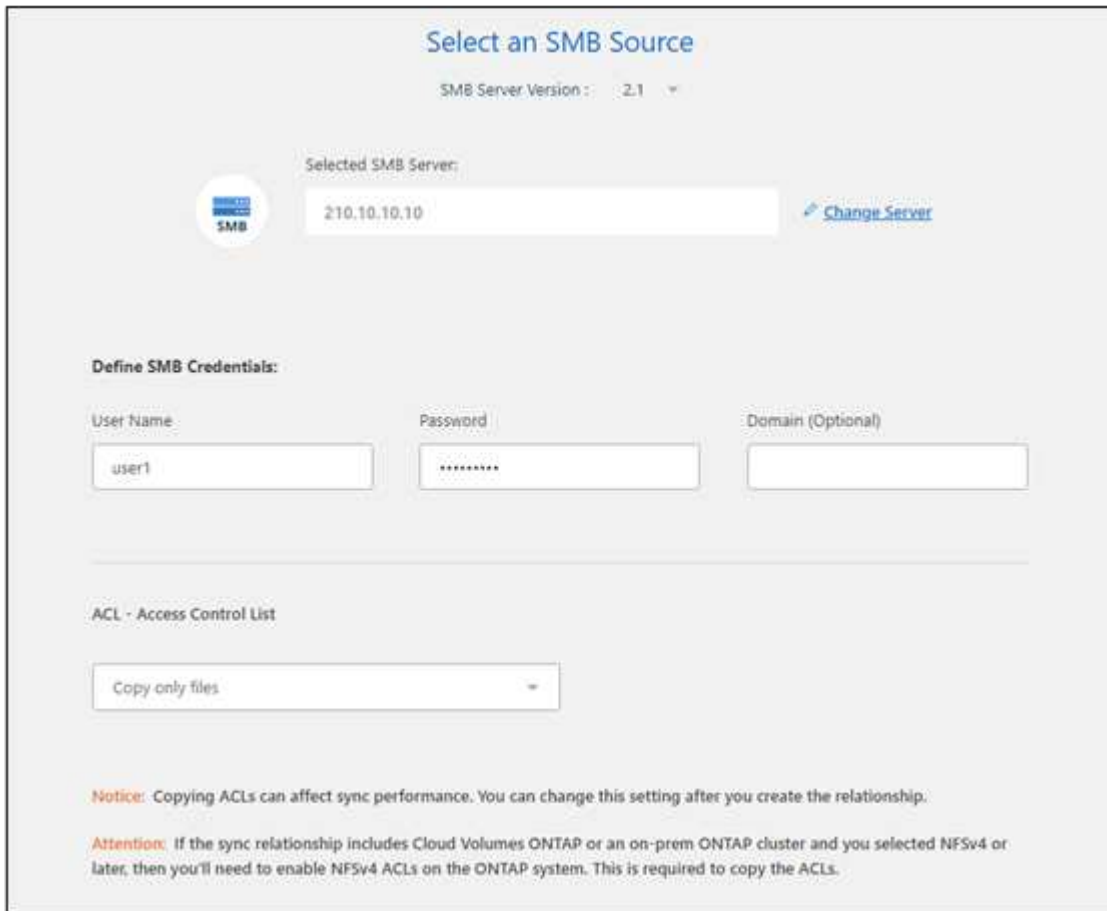
Copie las ACL entre recursos compartidos SMB y entre recursos compartidos SMB y almacenamiento de objetos habilitando una configuración cuando crea una relación o después de crear una relación.

Antes de empezar

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

Pasos para una nueva relación

1. ["Iniciar sesión en Copiar y sincronizar"](#) .
2. Desde Copiar y sincronizar, seleccione **Crear nueva sincronización**.
3. Arrastre y suelte un servidor SMB o un almacenamiento de objetos como origen y un servidor SMB o un almacenamiento de objetos como destino, y seleccione **Continuar**.
4. En la página **Servidor SMB**:
 - a. Ingrese un nuevo servidor SMB o seleccione un servidor existente y seleccione **Continuar**.
 - b. Introduzca las credenciales para el servidor SMB.
 - c. Elija entre **Copiar solo archivos**, **Copiar solo ACL** o **Copiar archivos y ACL** y seleccione **Continuar**.



Select an SMB Source

SMB Server Version : 2.1

Selected SMB Server:

210.10.10.10 [Change Server](#)

Define SMB Credentials:

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

ACL - Access Control List

Copy only files

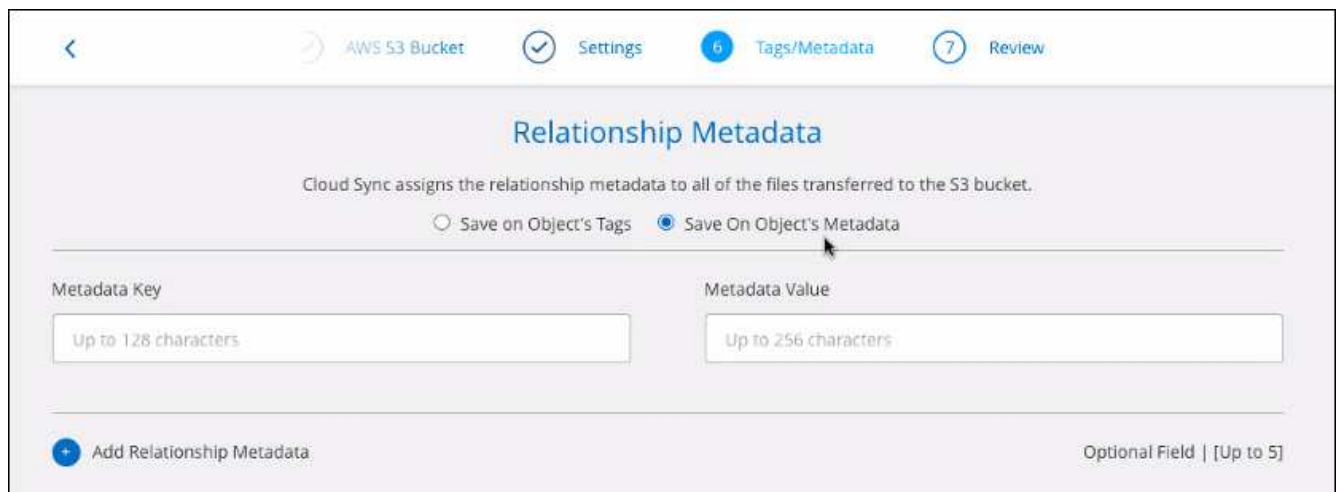
Notice: Copying ACLs can affect sync performance. You can change this setting after you create the relationship.

Attention: If the sync relationship includes Cloud Volumes ONTAP or an on-prem ONTAP cluster and you selected NFSv4 or later, then you'll need to enable NFSv4 ACLs on the ONTAP system. This is required to copy the ACLs.

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

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

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



< AWS S3 Bucket Settings **6 Tags/Metadata** 7 Review

Relationship Metadata

Cloud Sync assigns the relationship metadata to all of the files transferred to the S3 bucket.

☐ Save on Object's Tags ☒ Save On Object's Metadata

Metadata Key: Up to 128 characters Metadata Value: Up to 256 characters

+ Add Relationship Metadata Optional Field | [Up to 5]

Pasos para una relación existente

1. Coloque el cursor sobre la relación de sincronización y seleccione el menú de acciones.

2. Seleccione **Configuración**.
3. Elija entre **Copiar solo archivos**, **Copiar solo ACL** o **Copiar archivos y ACL** y seleccione **Continuar**.
4. Seleccione **Guardar configuración**.



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

Resultado

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

Copiar manualmente las ACL entre recursos compartidos SMB

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



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

Pasos

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

Debes realizar este paso antes de utilizar robocopy.

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

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

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

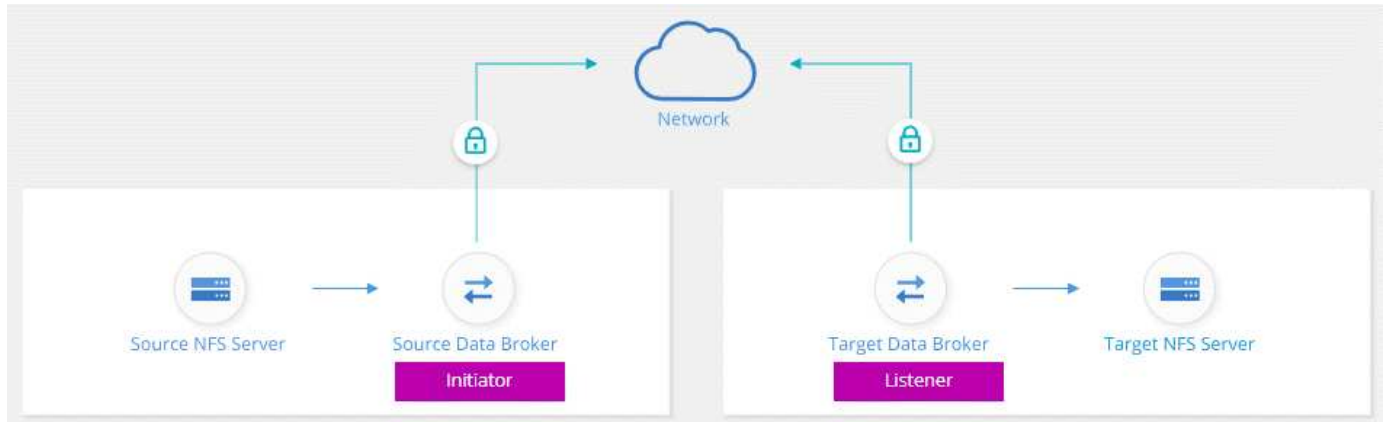
Sincronice datos NFS mediante el cifrado de datos en tránsito en NetApp Copy and Sync

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

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

Cómo funciona el cifrado de datos en tránsito

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



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

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

Así es como funciona el cifrado en vuelo:

1. Después de crear la relación de sincronización, el iniciador inicia una conexión cifrada con el otro agente de datos.
2. El agente de datos de origen cifra los datos de la fuente mediante TLS 1.3.
3. Luego envía los datos a través de la red al agente de datos de destino.
4. El agente de datos de destino descifra los datos antes de enviarlos al destino.
5. Después de la copia inicial, Copiar y sincronizar sincroniza los datos modificados cada 24 horas. Si hay datos para sincronizar, el proceso comienza cuando el iniciador abre una conexión cifrada con el otro agente de datos.

Si prefiere sincronizar datos con más frecuencia, ["Puedes cambiar el horario después de crear la relación"](#).

Versiones de NFS compatibles

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

Limitación del servidor proxy

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

Lo que necesitarás para empezar

Asegúrese de tener lo siguiente:

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

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

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

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

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

Sincronizar datos NFS mediante cifrado de datos en tránsito

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

Pasos

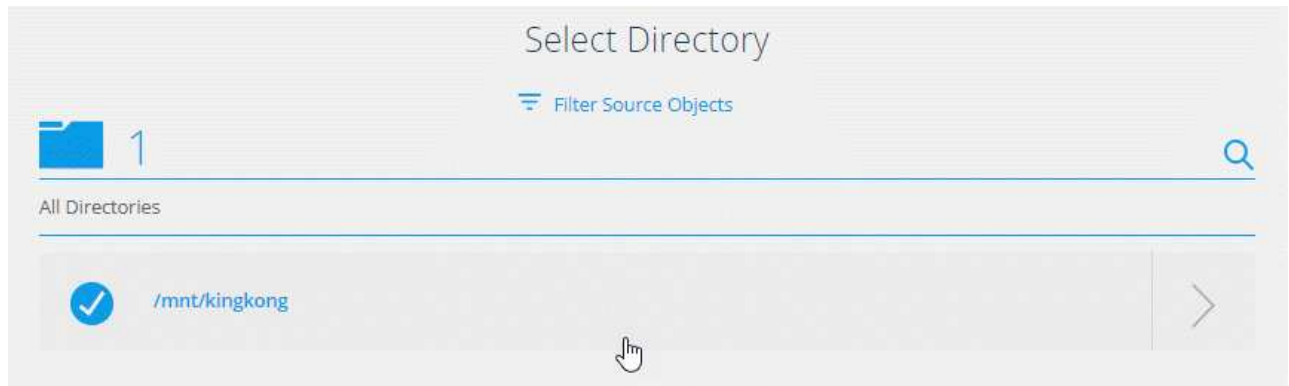
1. ["Iniciar sesión en Copiar y sincronizar"](#) .
2. Seleccione **Crear nueva sincronización**.
3. Arrastre y suelte **Servidor NFS** en las ubicaciones de origen y destino o *** Azure NetApp Files*** en las ubicaciones de origen y destino y seleccione **Sí** para habilitar el cifrado de datos en tránsito.
4. Siga las instrucciones para crear la relación:
 - a. **Servidor NFS/* Azure NetApp Files***: elija la versión de NFS y luego especifique una nueva fuente de NFS o seleccione un servidor existente.
 - b. **Definir la funcionalidad del agente de datos**: define qué agente de datos *escucha* las solicitudes de conexión en un puerto y cuál *inicia* la conexión. Haga su elección en función de sus necesidades de red.
 - c. **Agente de datos**: siga las instrucciones para agregar un nuevo agente de datos de origen o seleccionar un agente de datos existente.

Tenga en cuenta lo siguiente:

- Si desea utilizar un grupo de corredores de datos existente, el grupo debe tener solo un corredor de datos. No se admiten varios corredores de datos en un grupo con relaciones de sincronización cifradas.
- Si el agente de datos de origen actúa como oyente, entonces debe ser un nuevo agente de datos.

- Si necesita un nuevo agente de datos, Copiar y sincronizar le solicitará las instrucciones de instalación. Puede implementar el agente de datos en la nube o descargar un script de instalación para su propio host Linux.
- d. **Directorios:** elija los directorios que desea sincronizar seleccionando todos los directorios o explorando y seleccionando un subdirectorio.

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



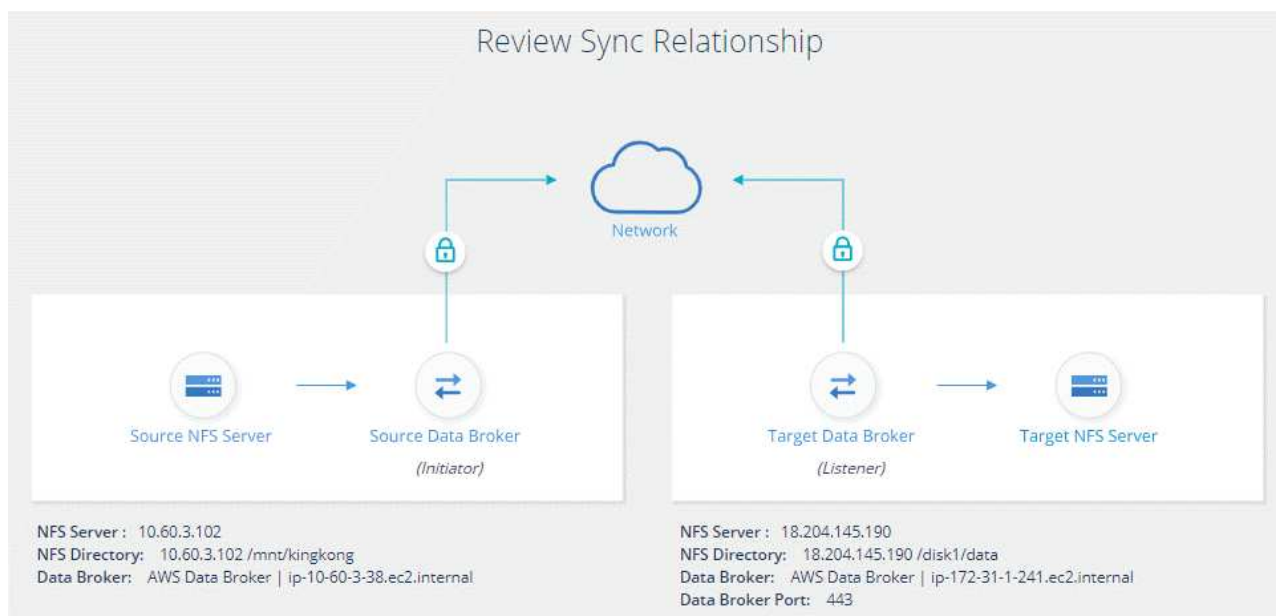
- e. **Servidor NFS de destino/* Azure NetApp Files de destino*:** elija la versión de NFS y luego ingrese un nuevo destino NFS o seleccione un servidor existente.
- f. **Agente de datos de destino:** siga las instrucciones para agregar un nuevo agente de datos de origen o seleccionar un agente de datos existente.

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

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

- a. **Directorios de destino:** seleccione un directorio de nivel superior o profundice para seleccionar un subdirectorio existente o para crear una nueva carpeta dentro de una exportación.
- b. **Configuración:** Define cómo se sincronizan y mantienen los archivos y carpetas de origen en la ubicación de destino.

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



Resultado

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

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

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

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

1

Preparar la bóveda

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

2

Preparar el grupo de intermediarios de datos

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

3

Crear una relación de sincronización usando la API

Ahora que todo está configurado, puedes enviar una llamada API para crear una relación de sincronización

que use tu bóveda para obtener los secretos.

Preparar la bóveda

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

La URL debe configurarse de la siguiente manera:

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

Camino

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

ID de solicitud

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

Protocolo de punto final

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

Creds

La URL debe terminar con *Creds*.

Ejemplos

Los siguientes ejemplos muestran URL a secretos.

Ejemplo de URL completa y ruta para las credenciales de origen

\ <http://example.vault.com:8200/my-path/all-secrets/hb312vdsr2/S3Creds>

Como puede ver en el ejemplo, la ruta del prefijo es */my-path/all-secrets/*, el ID de solicitud es *hb312vdsr2* y el punto final de origen es S3.

Ejemplo de URL completa y ruta para credenciales de destino

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

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

Preparar el grupo de intermediarios de datos

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

Pasos

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

activado

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

URL

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

camino

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

Rechazar no autorizado

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

método de autenticación

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

nombre del rol

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

Secretid y rootid

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

Espacio de nombres

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

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

Ejemplo de autenticación de roles de AWS


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

Ejemplo de autenticación gcp-iam

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

Configurar permisos al usar la autenticación gcp-iam

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

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

["Obtenga más información sobre los requisitos de permisos de GCP para el agente de datos"](#) .

Creación de una nueva relación de sincronización utilizando secretos del almacén

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

Publique la relación utilizando la API REST Copiar y sincronizar.

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

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

Ejemplo

Ejemplo para la solicitud POST:

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

Pague por las relaciones de sincronización después de que finalice su prueba gratuita de NetApp Copy and Sync

Hay dos formas de pagar las relaciones de sincronización después de que finalice su prueba gratuita de 14 días para NetApp Copy and Sync. La primera opción es suscribirse desde AWS o Azure con pago por uso o pago anual. La segunda opción es comprar licencias directamente de NetApp.

Puede suscribirse desde AWS Marketplace o desde Azure Marketplace. No puedes suscribirte desde ambos.

Tiene la opción de utilizar licencias de NetApp con una suscripción al Marketplace. Por ejemplo, si tiene 25 relaciones de sincronización, puede pagar las primeras 20 relaciones de sincronización usando una licencia y luego pagar por uso desde AWS o Azure con las 5 relaciones de sincronización restantes.

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

Si no paga inmediatamente después de que finalice su prueba gratuita, no podrá crear ninguna relación adicional. Las relaciones existentes no se eliminan, pero no podrás realizar ningún cambio en ellas hasta que te suscribas o ingreses una licencia.

Las licencias deben administrarse a través de NetApp Copy and Sync o el sitio web correspondiente y **no** a través de las suscripciones de la NetApp Console .

Suscribirse desde AWS

AWS le permite pagar según su uso o pagar anualmente.

Pasos para pagar por uso

1. Desde el menú de navegación de la NetApp Console , seleccione **Movilidad > Copiar y sincronizar**.
2. Seleccione **Licencia**.
3. Seleccione **AWS**.
4. Seleccione **Suscribirse** y luego seleccione **Continuar**.
5. Suscríbete desde AWS Marketplace y luego vuelve a iniciar sesión en Copiar y sincronizar para completar el registro.

El siguiente vídeo muestra el proceso:

[Suscríbete a Copiar y sincronizar desde AWS Marketplace](#)

Pasos para pagar anualmente

1. ["Vaya a la página de AWS Marketplace"](#) .
2. Seleccione **Continuar con la suscripción**.
3. Seleccione sus opciones de contrato y luego seleccione **Crear contrato**.

Suscribirse desde Azure

Azure le permite pagar por uso o pagar anualmente.

Lo que necesitarás

Una cuenta de usuario de Azure que tenga permisos de colaborador o propietario en la suscripción correspondiente.

Pasos

1. Desde el menú de navegación de la NetApp Console , seleccione **Movilidad > Copiar y sincronizar**.
2. Seleccione **Licencia**.
3. Seleccione **Azure**.
4. Seleccione **Suscribirse** y luego seleccione **Continuar**.
5. En el portal de Azure, seleccione **Crear**, seleccione sus opciones y luego seleccione **Suscribirse**.

Seleccione **Mensual** para pagar por hora, o **Anual** para pagar un año por adelantado.

6. Cuando se complete la implementación, seleccione el nombre del recurso SaaS en la ventana emergente de notificación.
7. Seleccione **Configurar cuenta** para volver a Copiar y sincronizar.

El siguiente vídeo muestra el proceso:

[Suscríbete a Copiar y sincronizar desde Azure Marketplace](#)

Compre licencias de NetApp y agréguelas a Copiar y sincronizar

Para pagar sus relaciones de sincronización por adelantado, debe comprar una o más licencias y agregarlas a Copiar y sincronizar.

Lo que necesitarás

Necesitará el número de serie de su licencia y 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. Compre una licencia enviando un correo electrónico a: [ng-cloudsync-contact@netapp.com?subject=Cloud%20Sync%20Service%20-%20BYOL%20License%20Purchase%20Request\[contacting NetApp\]](mailto:ng-cloudsync-contact@netapp.com?subject=Cloud%20Sync%20Service%20-%20BYOL%20License%20Purchase%20Request[contacting%20NetApp]).
2. "Iniciar sesión en Copiar y sincronizar" .
3. Seleccione **Licencia**.
4. Seleccione **Agregar licencia** y agregue la información requerida:
 - a. Introduzca el número de serie.
 - b. Seleccione la cuenta del sitio de soporte de NetApp que está asociada con la licencia que está agregando:
 - Si su cuenta ya se agregó a la NetApp Console, selecciónela de la lista desplegable.
 - Si aún no ha agregado su cuenta, seleccione **Agregar credenciales NSS**, ingrese el nombre de usuario y la contraseña, seleccione **Registrar** y luego selecciónelo de la lista desplegable.
 - c. Seleccione **Agregar**.

Actualizar una licencia

Si extendió una licencia de Copiar y sincronizar que compró en NetApp, la nueva fecha de vencimiento no se actualizará automáticamente en Copiar y sincronizar. Debe agregar la licencia nuevamente para actualizar la fecha de vencimiento. Las licencias deben administrarse a través de Copy and Sync o el sitio web correspondiente y **no** a través de las suscripciones de la NetApp Console .

Pasos

1. Desde el menú de navegación de la NetApp Console , seleccione **Movilidad > Copiar y sincronizar**.
2. Seleccione **Licencia**.
3. Seleccione **Agregar licencia** y agregue la información requerida:
 - a. Introduzca el número de serie.
 - b. Seleccione la cuenta del sitio de soporte de NetApp que está asociada con la licencia que está agregando.
 - c. Seleccione **Agregar**.

Resultado

Copiar y sincronizar actualiza la licencia existente con la nueva fecha de vencimiento.


Administración de relaciones de sincronización en NetApp Copy and Sync

Puede administrar las relaciones de sincronización en NetApp Copy and Sync en cualquier momento sincronizando datos de inmediato, cambiando programaciones y más.

Realizar una sincronización de datos inmediata

En lugar de esperar a la próxima sincronización programada, puede sincronizar inmediatamente los datos entre el origen y el destino.

Pasos

1. "Iniciar sesión en Copiar y sincronizar" .
2. Desde el **Panel de Control**, navegue hasta la relación de sincronización y seleccione .
3. Seleccione **Sincronizar ahora** y luego seleccione **Sincronizar** para confirmar.

Resultado

Copiar y sincronizar inicia el proceso de sincronización de datos para la relación.

Acelerar el rendimiento de la sincronización

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

Cómo funciona


Si el grupo de agentes de datos administra otras relaciones de sincronización, el nuevo agente de datos que agregue al grupo también acelera el rendimiento de esas relaciones de sincronización.

Por ejemplo, digamos que tienes tres relaciones:

- La relación 1 está gestionada por el grupo de corredores de datos A
- La relación 2 está gestionada por el grupo de corredores de datos B
- La relación 3 está gestionada por el grupo de corredores de datos A

Desea acelerar el rendimiento de la relación 1, por lo que agrega un nuevo agente de datos al grupo de agentes de datos A. Debido a que el grupo A también administra la relación de sincronización 3, el rendimiento de sincronización de la relación también se acelera automáticamente.

Pasos

1. Asegúrese de que al menos uno de los corredores de datos existentes en la relación esté en línea.
2. Desde el **Panel de Control**, navegue hasta la relación de sincronización y seleccione .
3. Seleccione **Acelerar**.
4. Siga las instrucciones para crear un nuevo agente de datos.

Resultado

Copiar y sincronizar agrega el nuevo agente de datos al grupo. Se debe acelerar el rendimiento de la próxima

sincronización de datos.

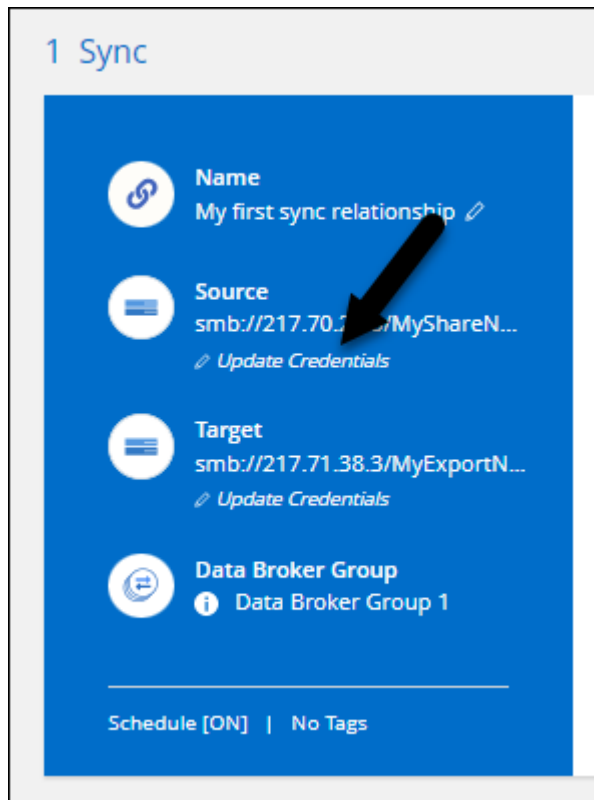
Actualizar credenciales

Puede actualizar el agente de datos con las últimas credenciales del origen o el destino en una relación de sincronización existente. Actualizar las credenciales puede ayudar si sus políticas de seguridad requieren que actualice las credenciales periódicamente.

La actualización de credenciales es compatible con cualquier origen o destino para el que Copy and Sync requiera credenciales: Azure Blob, Box, IBM Cloud Object Storage, StorageGRID, ONTAP S3 Storage, SFTP y servidores SMB.

Pasos

1. Desde el **Panel de sincronización**, vaya a una relación de sincronización que requiera credenciales y luego seleccione **Actualizar credenciales**.



2. Ingrese las credenciales y seleccione **Actualizar**.

Una nota sobre los servidores SMB: si el dominio es nuevo, deberá especificarlo cuando actualice las credenciales. Si el dominio no ha cambiado, no es necesario ingresarlo nuevamente.

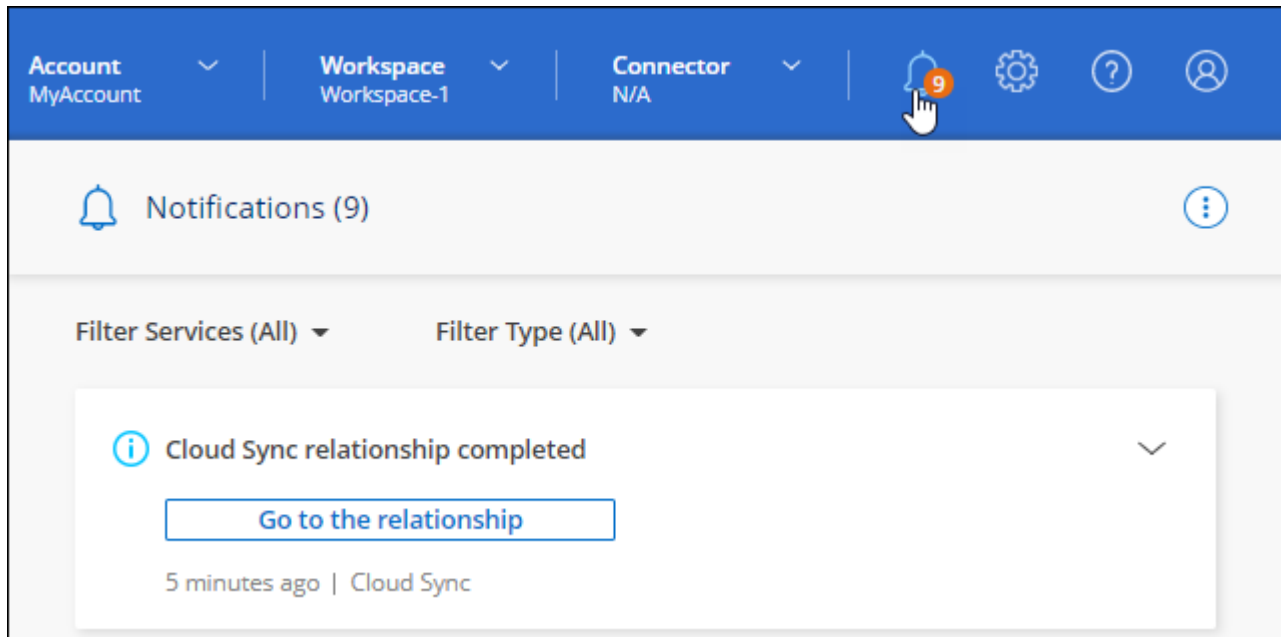
Si ingresó un dominio cuando creó la relación de sincronización, pero no ingresa un nuevo dominio cuando actualiza las credenciales, Copiar y sincronizar seguirá usando el dominio original que proporcionó.

Resultado

Copiar y sincronizar actualiza las credenciales en el agente de datos. Pueden pasar hasta 10 minutos hasta que el agente de datos comience a utilizar las credenciales actualizadas para las sincronizaciones de datos.


Configurar notificaciones

Una configuración de **Notificaciones** para cada relación de sincronización le permite elegir si desea recibir notificaciones de Copiar y Sincronizar en el Centro de notificaciones de la Consola de NetApp . Puede habilitar notificaciones para sincronizaciones de datos exitosas, fallidas y canceladas.



Además, también podrás recibir notificaciones por correo electrónico.

Pasos


1. Modificar la configuración de una relación de sincronización:
 - a. Desde el **Panel de Control**, navegue hasta la relación de sincronización y seleccione .
 - b. Seleccione **Configuración**.
 - c. Habilitar **Notificaciones**.
 - d. Seleccione **Guardar configuración**.
2. Si desea recibir notificaciones por correo electrónico, configure los ajustes de alertas y notificaciones:
 - a. Seleccione **Configuración > Configuración de alertas y notificaciones**.
 - b. Seleccione un usuario o varios usuarios y elija el tipo de notificación **Info**.
 - c. Seleccione **Aplicar**.

Resultado

Ahora recibirá notificaciones de Copiar y Sincronizar en el Centro de notificaciones de la Consola de NetApp , y algunas notificaciones llegarán por correo electrónico, si configuró esa opción.

Cambiar la configuración de una relación de sincronización

Modifique las configuraciones que definen cómo se sincronizan y mantienen los archivos y carpetas de origen en la ubicación de destino.

1. Desde el **Panel de Control**, navegue hasta la relación de sincronización y seleccione .


2. Seleccione **Configuración**.
3. Modificar cualquiera de las configuraciones.

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:

Cronograma

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

Tiempo de espera de sincronización

Define si Copiar y sincronizar debe cancelar una sincronización de datos si la sincronización no se ha

completado en la cantidad especificada de minutos, horas o días.

Notificaciones

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

Si deseas recibir notificaciones de

Reintentos

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

Comparar por

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

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

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

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

Copiar para objetos

No puedes editar esta opción después de crear la relación.

Archivos modificados recientemente

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

Eliminar archivos en la fuente

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

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

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

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

Eliminar archivos en el destino

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

Tipos de archivos

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



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

Excluir extensiones de archivo

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

[Excluir extensiones de archivo para una relación de sincronización](#)



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

Excluir directorios

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



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

Tamaño del archivo

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

Fecha de modificación

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

Fecha de creación

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

ACL - Lista de control de acceso

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

4. Seleccione **Guardar configuración**.

Resultado


Copiar y sincronizar modifica la relación de sincronización con la nueva 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 corredores de datos (ni las instancias individuales de corredores de datos) y no elimina datos del destino.

Opción 1: Eliminar una sola relación de sincronización

Pasos


1. Desde el **Panel de Control**, navegue hasta la relación de sincronización y seleccione .
2. Seleccione **Eliminar** y luego seleccione **Eliminar** nuevamente para confirmar.

Resultado

Copiar y sincronizar elimina la relación de sincronización.

Opción 2: Eliminar múltiples relaciones de sincronización

Pasos

1. Desde el **Panel de Control**, navegue hasta el botón "Crear nueva sincronización" y seleccione .
2. Seleccione las relaciones de sincronización que desea eliminar, seleccione **Eliminar** y luego seleccione **Eliminar** nuevamente para confirmar.

Resultado

Copiar y sincronizar elimina las relaciones de sincronización.

Administrar grupos de intermediarios de datos en NetApp Copy and Sync

Un grupo de intermediarios de datos en NetApp Copy and Sync sincroniza datos desde una ubicación de origen a una ubicación de destino. Se requiere al menos un agente de datos en un grupo para cada relación de sincronización que cree. Administre grupos de corredores de datos agregando un nuevo corredor de datos a un grupo, viendo información sobre los grupos y más.

Cómo funcionan los grupos de corredores de datos

Un grupo de corredores de datos puede incluir uno o más corredores de datos. Agrupar corredores de datos puede ayudar a mejorar el rendimiento de las relaciones de sincronización.

Los grupos pueden gestionar varias relaciones

Un grupo de corredores de datos puede administrar una o más relaciones de sincronización a la vez.

Por ejemplo, digamos que tienes tres relaciones:

- La relación 1 está gestionada por el grupo de corredores de datos A

- La relación 2 está gestionada por el grupo de corredores de datos B
- La relación 3 está gestionada por el grupo de corredores de datos A

Desea acelerar el rendimiento de la relación 1, por lo que agrega un nuevo agente de datos al grupo de agentes de datos A. Debido a que el grupo A también administra la relación de sincronización 3, el rendimiento de sincronización de la relación también se acelera automáticamente.

Número de corredores de datos en un grupo

En muchos casos, un único agente de datos puede satisfacer los requisitos de rendimiento para una relación de sincronización. Si no es así, puede acelerar el rendimiento de la sincronización agregando agentes de datos adicionales al grupo. Pero primero debes comprobar otros factores que pueden afectar el rendimiento de la sincronización. ["Obtenga más información sobre cómo determinar cuándo se requieren varios corredores de datos"](#) .

Recomendaciones de seguridad

Para garantizar la seguridad de su máquina de agente de datos, NetApp recomienda lo siguiente:

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

Estas recomendaciones de seguridad pueden ayudar a prevenir conexiones no autorizadas a la máquina del agente de datos.

Agregar un nuevo agente de datos a un grupo

Hay varias formas de crear un nuevo corredor de datos:

- Al crear una nueva relación de sincronización

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

- Desde la página **Administrar corredores de datos**, seleccione **Agregar nuevo corredor de datos**, lo que crea el corredor de datos en un nuevo grupo
- Desde la página **Administrar corredores de datos** creando un nuevo corredor de datos en un grupo existente

Antes de empezar

- No se pueden agregar corredores de datos a un grupo que administra 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 local 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 local en ese grupo. No se puede crear un agente de datos de Azure o 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 nuevo grupo

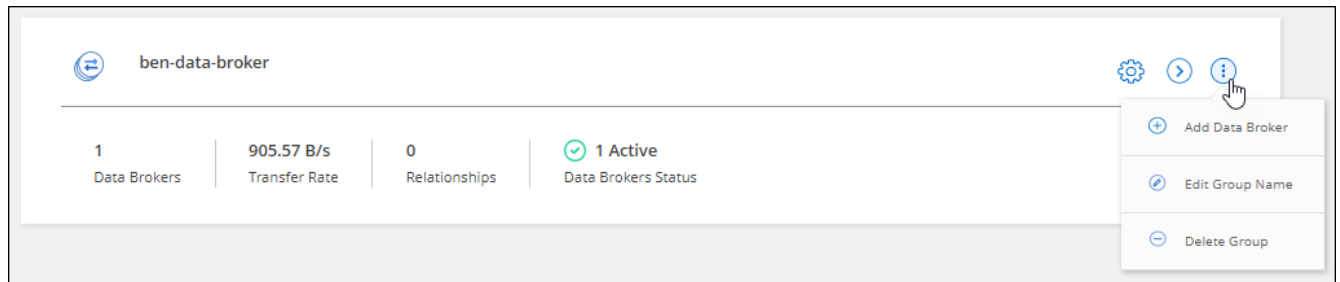
1. ["Iniciar sesión en Copiar y sincronizar"](#) .
2. Seleccione **Sincronizar > Administrar agentes de datos**.
3. Seleccione **Agregar nuevo agente de datos**.
4. Siga las instrucciones para crear el agente de datos.

Para obtener ayuda, consulte las siguientes páginas:

- ["Crear un agente de datos en AWS"](#)
- ["Crear un agente de datos en Azure"](#)
- ["Crear un agente de datos en Google Cloud"](#)
- ["Instalación del agente de datos en un host Linux"](#)

Pasos para crear un agente de datos en un grupo existente

1. ["Iniciar sesión en Copiar y sincronizar"](#) .
2. Seleccione **Sincronizar > Administrar agentes de datos**.
3. Seleccione el menú de acciones y seleccione **Agregar agente de datos**.



4. Siga las instrucciones para crear el agente de datos en el grupo.

Para obtener ayuda, consulte las siguientes páginas:

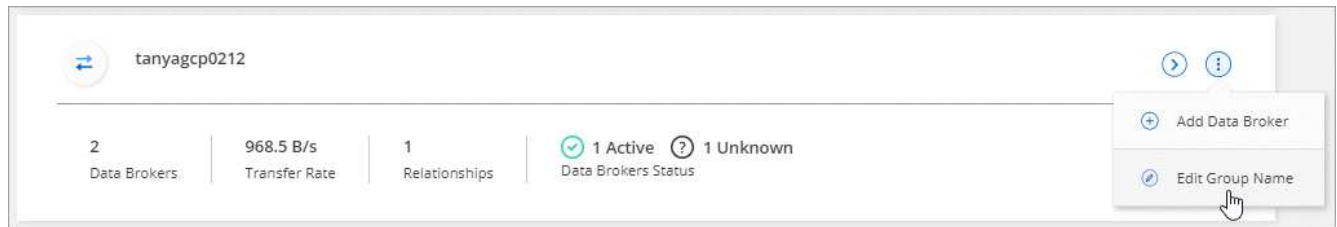
- ["Crear un agente de datos en AWS"](#)
- ["Crear un agente de datos en Azure"](#)
- ["Crear un agente de datos en Google Cloud"](#)
- ["Instalación del agente de datos en un host Linux"](#)

Editar el nombre de un grupo

Cambie el nombre de un grupo de corredores de datos en cualquier momento.

Pasos

1. ["Iniciar sesión en Copiar y sincronizar"](#) .
2. Seleccione **Sincronizar > Administrar agentes de datos**.
3. Seleccione el menú de acciones y seleccione **Editar nombre del grupo**.



4. Introduzca un nuevo nombre y seleccione **Guardar**.

Resultado

Copiar y sincronizar actualiza el nombre del grupo de intermediarios de datos.

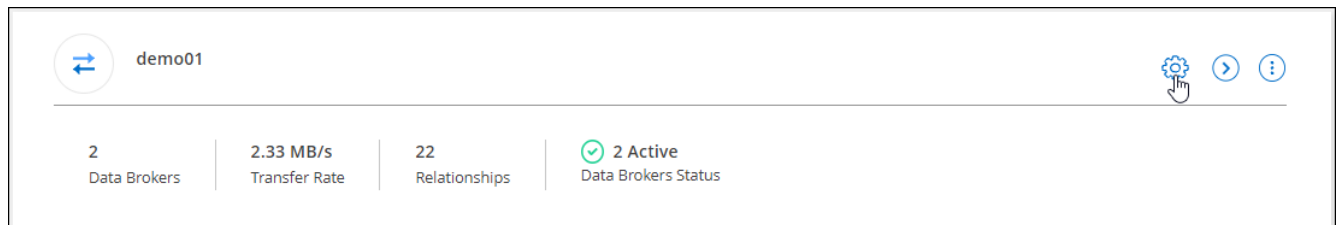
Configurar una configuración unificada

Si una relación de sincronización encuentra errores durante el proceso de sincronización, unificar la simultaneidad del grupo de intermediarios de datos puede ayudar a disminuir la cantidad de errores de sincronización. Tenga en cuenta que los cambios en la configuración del grupo pueden afectar el rendimiento al ralentizar la transferencia.

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

Pasos

1. "Iniciar sesión en Copiar y sincronizar" .
2. Seleccione **Administrar corredores de datos**.
3. Seleccione el icono de Configuración para un grupo de corredores de datos.



4. Cambie la configuración según sea necesario y luego seleccione **Unificar configuración**.

Tenga en cuenta lo siguiente:

- Puede seleccionar qué configuraciones desea cambiar (no es necesario que cambie las cuatro a la vez).
- Después de enviar una nueva configuración a un agente de datos, este se reinicia automáticamente y utiliza la nueva configuración.
- Puede tomar hasta un minuto hasta que este cambio se realice y sea visible en la interfaz Copiar y sincronizar.
- Si un agente de datos no se está ejecutando, su configuración no cambiará porque Copiar y sincronizar no puede comunicarse con él. La configuración cambiará después de que se reinicie el agente de datos.
- Después de establecer una configuración unificada, cualquier nuevo agente de datos utilizará automáticamente la nueva configuración.

Mover corredores de datos entre grupos


Mueva un agente de datos de un grupo a otro si necesita acelerar el rendimiento del grupo de agentes de datos de destino.

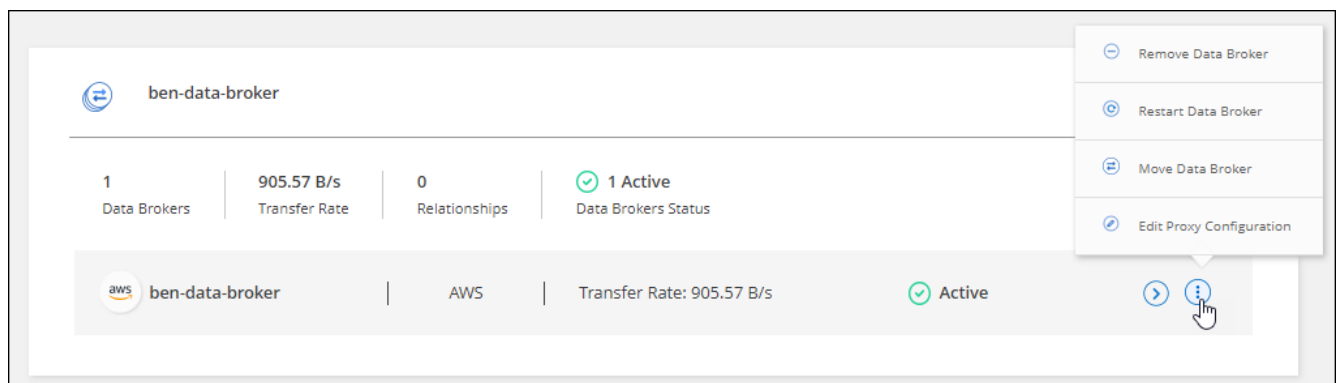
Por ejemplo, si un agente de datos ya no administra una relación de sincronización, puede moverlo fácilmente a otro grupo que sí administre relaciones de sincronización.

Limitaciones

- Si un grupo de agentes de datos administra una relación de sincronización y solo hay un agente de datos en el grupo, no podrá mover ese agente de datos a otro grupo.
- No se puede mover un agente de datos hacia o desde un grupo que administra relaciones de sincronización cifradas.
- No se puede mover un agente de datos que se esté implementando actualmente.

Pasos

1. "Iniciar sesión en Copiar y sincronizar" .
2. Seleccione **Sincronizar > Administrar agentes de datos**.
3. Seleccionar  para ampliar la lista de corredores de datos en un grupo.
4. Seleccione el menú de acciones para un agente de datos y seleccione **Mover agente de datos**.



5. Cree un nuevo grupo de corredores de datos o seleccione un grupo de corredores de datos existente.
6. Seleccione **Mover**.

Resultado


Copiar y sincronizar mueve el agente de datos a un grupo de agentes de datos nuevo o existente. Si no hay otros intermediarios de datos en el grupo anterior, Copiar y sincronizar lo elimina.

Actualizar 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. "Iniciar sesión en Copiar y sincronizar" .
2. Seleccione **Sincronizar > Administrar agentes de datos**.
- 3.

Seleccionar  para ampliar la lista de corredores de datos en un grupo.

4. Seleccione el menú de acciones para un agente de datos y seleccione **Editar configuración de proxy**.
5. Especifique detalles sobre el proxy: nombre de host, número de puerto, nombre de usuario y contraseña.
6. Seleccione **Actualizar**.

Resultado

Copiar y sincronizar actualiza el agente de datos para utilizar la configuración de proxy para el acceso a Internet.

Ver la configuración de un agente de datos

Es posible que desee ver detalles sobre un agente de datos para identificar cosas como su nombre de host, dirección IP, CPU y RAM disponibles, y más.



Copy and Sync proporciona los siguientes detalles sobre un agente de datos:

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



El escáner escanea el origen y el destino y decide qué se debe copiar. El transferente es quien realiza la copia propiamente dicha. El personal de NetApp puede usar estos detalles de configuración para sugerir acciones que puedan optimizar el rendimiento.

Pasos

1. "Iniciar sesión en Copiar y sincronizar" .
2. Seleccione **Sincronizar > Administrar agentes de datos**.
3. Seleccionar  para ampliar la lista de corredores de datos en un grupo.
4. Seleccionar  para ver detalles sobre un corredor de datos.

tanyagcp0212

2 Data Brokers

968.5 B/s Transfer Rate

1 Relationships

1 Active
 1 Unknown
 Data Brokers Status

	tanyagcp0212	GCP	Transfer Rate: 968.5 B/s	Active		
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		

Abordar problemas con un corredor de datos

Copiar y sincronizar muestra un estado para cada agente de datos que puede ayudarle a solucionar problemas.

Pasos

1. ["Iniciar sesión en Copiar y sincronizar"](#) .
2. Identifique cualquier corredor de datos que tenga un estado de "Desconocido" o "Fallido".

tanyagcp0212

2 Data Brokers

968.5 B/s Transfer Rate

1 Relationships

1 Active
 1 Unknown
 Data Brokers Status

tanyagcp0212	GCP	Transfer Rate: 968.5 B/s	Active		
tanya1	ONPREM	Transfer Rate: N/A	Unknown		

3. Pase el cursor sobre el Icono para ver el motivo del fallo.
4. Corrija el problema.

Por ejemplo, es posible que necesite simplemente reiniciar el agente de datos si está fuera de línea, o es posible que necesite eliminar el agente de datos si falló la implementación inicial.


Eliminar un agente de datos de un grupo

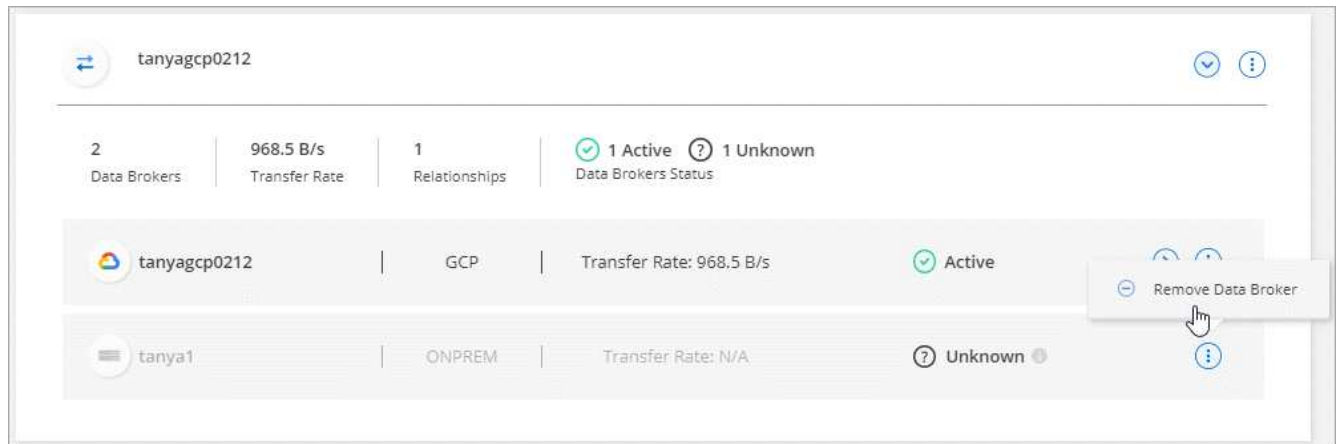
Puedes eliminar un agente de datos de un grupo si ya no es necesario o si la implementación inicial falló. Esta acción solo elimina el intermediario de datos de los registros de Copiar y sincronizar. Necesitará eliminar manualmente el agente de datos y cualquier recurso en la nube adicional.

Cosas que debes saber

- Copiar y sincronizar elimina un grupo cuando se quita el último agente de datos del grupo.
- No se puede eliminar el último agente de datos de un grupo si existe una relación que utiliza ese grupo.

Pasos

1. "Iniciar sesión en Copiar y sincronizar" .
2. Seleccione **Sincronizar > Administrar agentes de datos**.
3. Seleccionar  para ampliar la lista de corredores de datos en un grupo.
4. Seleccione el menú de acciones para un agente de datos y seleccione **Eliminar agente de datos**.



5. Seleccione **Eliminar agente de datos**.

Resultado

Copiar y sincronizar elimina el agente de datos del grupo.

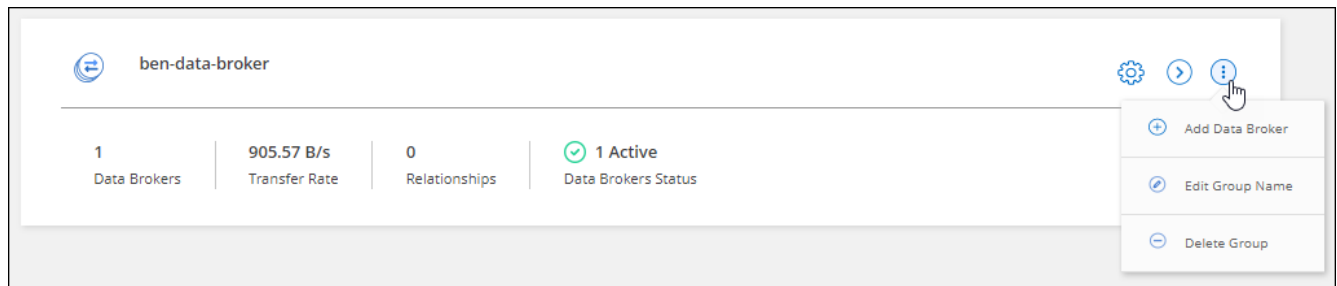
Eliminar un grupo de corredores de datos

Si un grupo de corredores de datos ya no administra ninguna relación de sincronización, puede eliminar el grupo, lo que elimina todos los corredores de datos de Copiar y sincronizar.

Los corredores de datos que Copy and Sync elimina solo se eliminan de los registros de Copy and Sync. Necesitará eliminar manualmente la instancia del agente de datos de su proveedor de nube y cualquier recurso de nube adicional.

Pasos

1. "Iniciar sesión en Copiar y sincronizar" .
2. Seleccione **Sincronizar > Administrar agentes de datos**.
3. Seleccione el menú de acciones y seleccione **Eliminar grupo**.



4. Para confirmar, ingrese el nombre del grupo y seleccione **Eliminar grupo**.

Resultado

Copiar y sincronizar elimina los intermediarios de datos y elimina el grupo.

Cree y visualice informes para ajustar su configuración en NetApp Copy and Sync

Cree y visualice informes en NetApp Copy and Sync para obtener información que pueda 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 detallados sobre una ruta en una relación de sincronización. Incluirá cuántos directorios, archivos y enlaces simbólicos hay, la distribución del tamaño de los archivos, qué tan profundos y anchos son los directorios, el tiempo de modificación y el tiempo de acceso. Esto difiere de las estadísticas de sincronización, que están disponibles en el panel de control después ["creando y completando con éxito una sincronización"](#).

Crear informes

Cada vez que se crea un informe, Copiar y sincronizar escanea la ruta y luego compila los detalles en un informe.

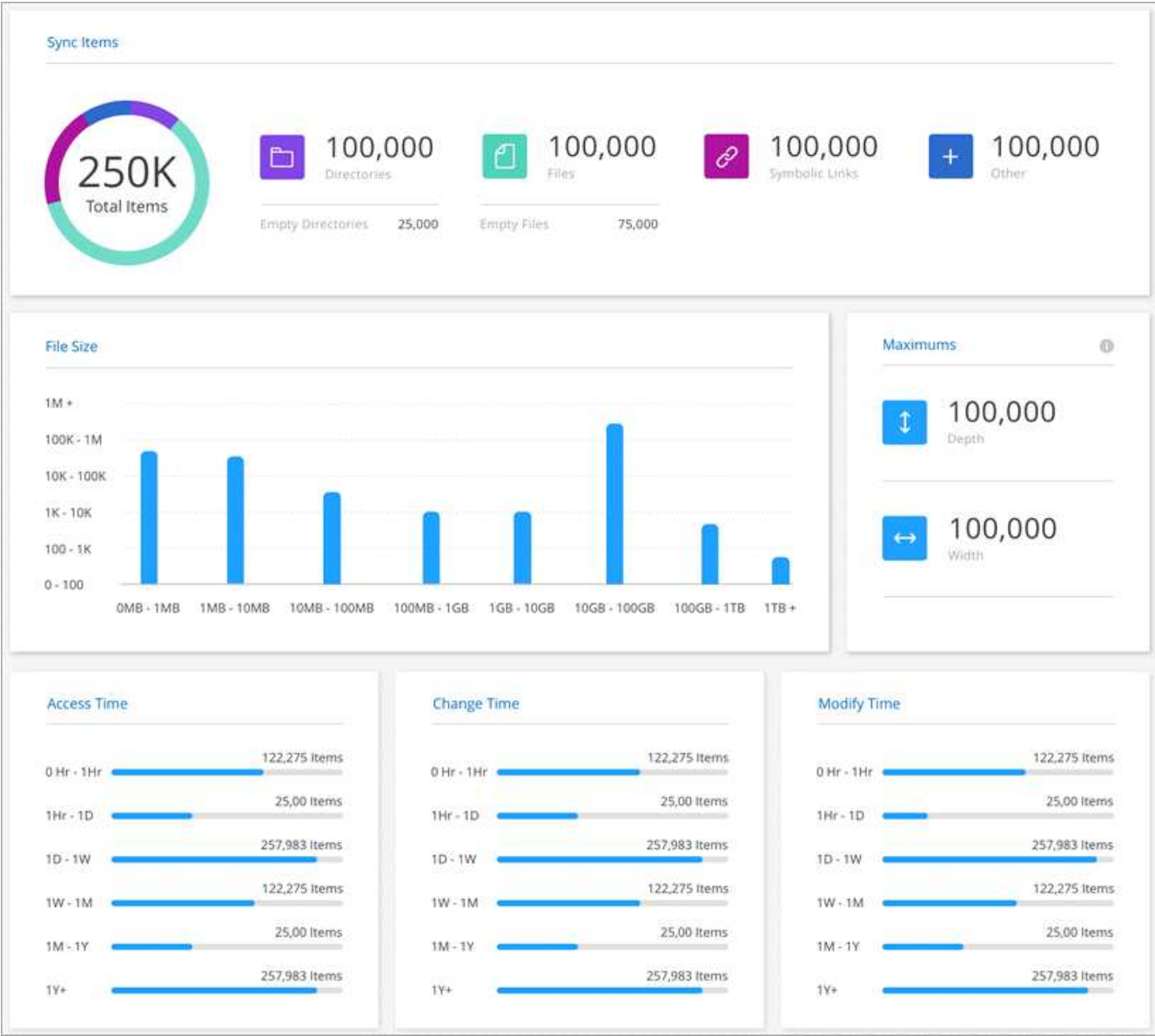
Pasos

1. ["Iniciar sesión en Copiar y sincronizar"](#).
2. Seleccione **Sincronizar > Informes**.

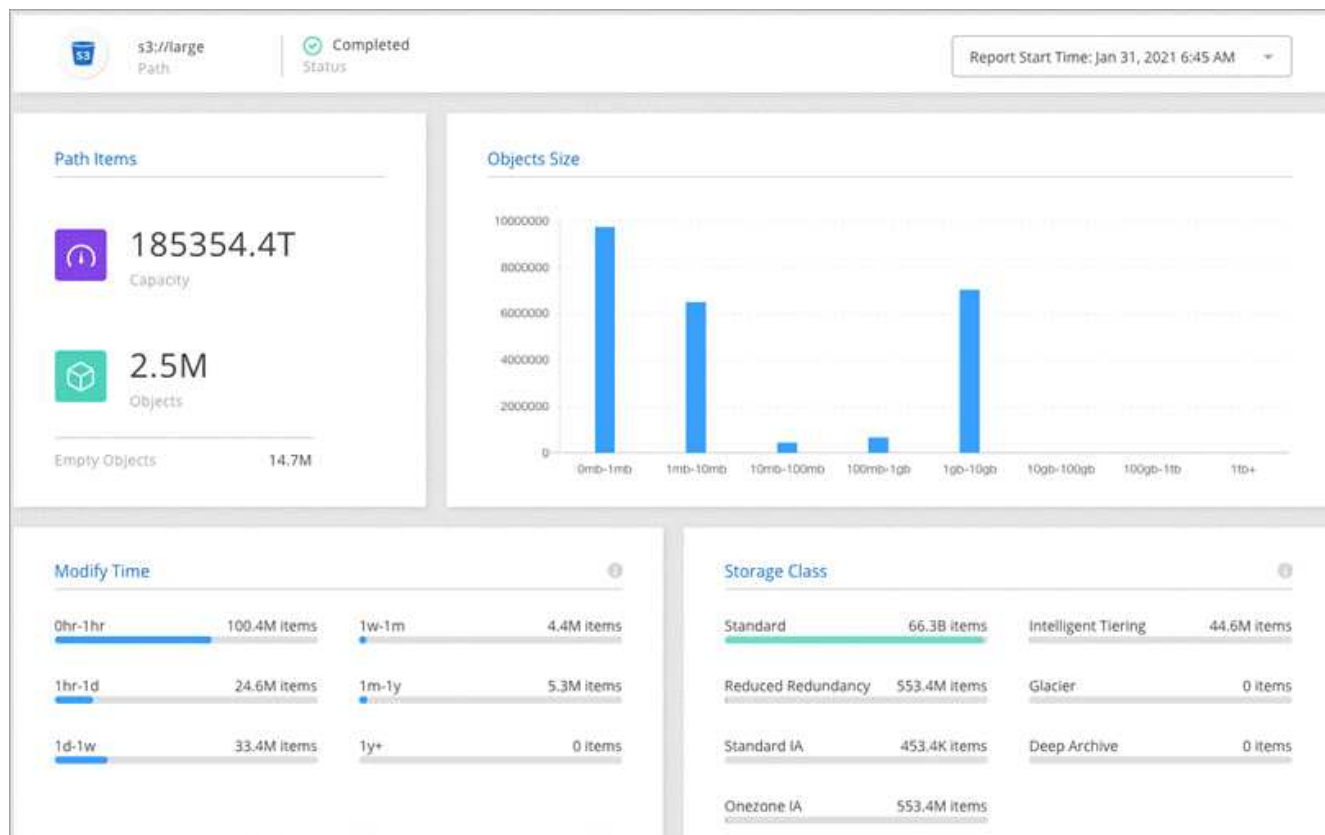
Las rutas (de origen o de destino) en cada una de sus relaciones de sincronización se muestran en una tabla.

3. En la columna **Acciones de informes**, vaya a una ruta específica y seleccione **Crear**, o seleccione el menú de acciones y seleccione **Crear nuevo**.
4. Cuando el informe esté listo, seleccione el menú de acciones y seleccione **Ver**.

A continuación se muestra un informe de muestra para una ruta del sistema de archivos.



Y aquí hay un informe de muestra para el almacenamiento de objetos.

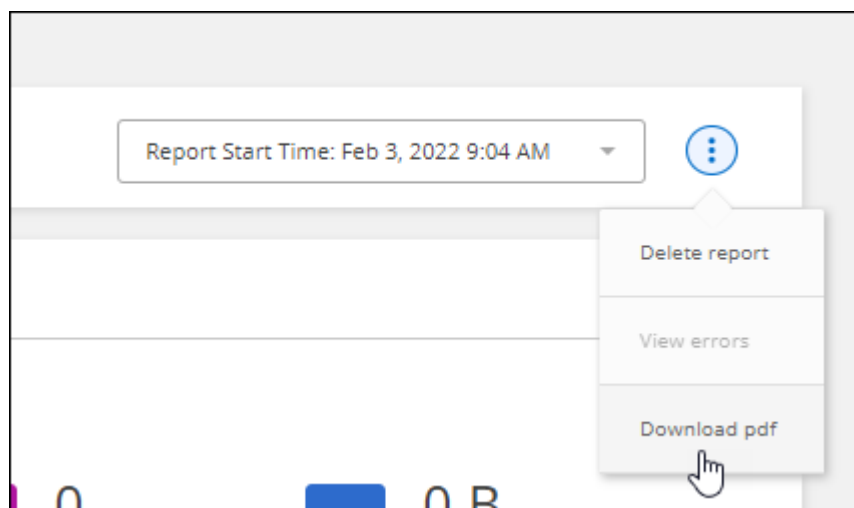


Descargar informes

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

Pasos

1. "Iniciar sesión en Copiar y sincronizar".
2. Seleccione **Sincronizar > Informes**.
3. En la columna **Acciones de informes**, seleccione el menú de acciones y seleccione **Ver**.
4. En la parte superior derecha del informe, seleccione el menú de acciones y seleccione **Descargar pdf**.



Ver errores del informe

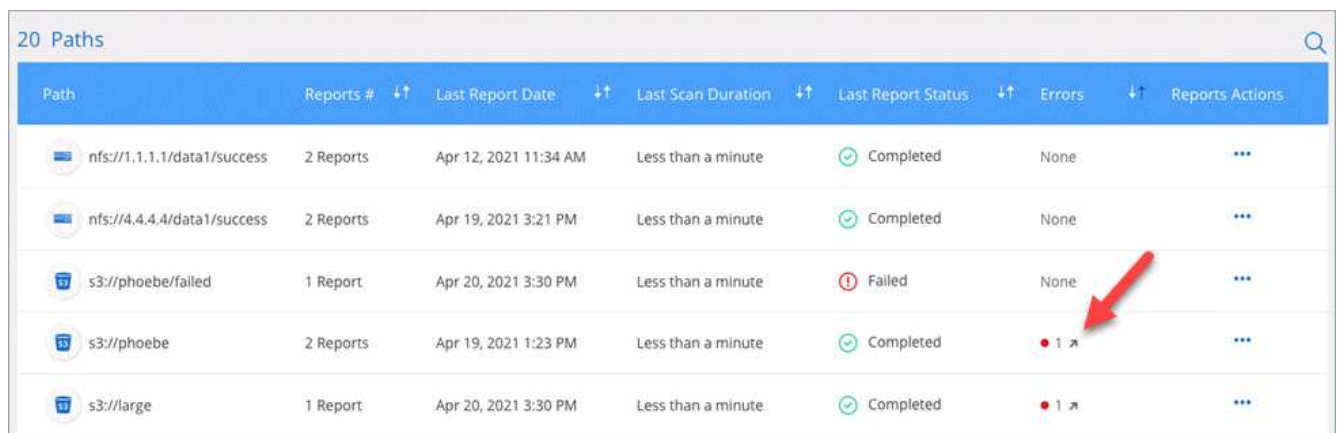
La tabla Rutas identifica si hay errores presentes en el informe más reciente. Un error identifica un problema que Copy and Sync enfrentó al escanear la ruta.

Por ejemplo, un informe podría contener errores de permiso denegado. Este tipo de error puede afectar la capacidad de Copy and Sync de escanear todo el conjunto de archivos y directorios.

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

Pasos

1. "Iniciar sesión en Copiar y sincronizar" .
2. Seleccione **Sincronizar > Informes**.
3. En la columna **Errores**, identifique si hay errores presentes en un informe.
4. Si hay errores, seleccione la flecha 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	...

5. 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

Es posible que elimines un informe que contenga un error que hayas corregido o que esté relacionado con una relación de sincronización que hayas eliminado.

Pasos

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

Desinstalar el agente de datos para NetApp Copy and Sync

Si es necesario, ejecute un script de desinstalación para eliminar el agente de datos y los paquetes y directorios que se crearon para NetApp Copy and Sync cuando se instaló el agente de datos.

Pasos

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

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

4. Presione 'y' para confirmar la desinstalación.

API de NetApp Copy and Sync

Las capacidades de NetApp Copy and Sync que están disponibles a través de la interfaz de usuario web también están disponibles a través de la API RESTful.

Empezar

Para comenzar a utilizar la API de copia y sincronización, debe obtener un token de usuario y su ID de cuenta de NetApp Console . Necesitará agregar el token y el ID de la cuenta al encabezado de Autorización cuando realice llamadas API.

Pasos

1. Obtenga un token de usuario desde la NetApp Console.

```
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".

2. Obtenga su ID de cuenta de NetApp Console .

```
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"
  }
]
```

3. Agregue el token de usuario y el ID de cuenta en el encabezado de Autorización de cada llamada API.

Ejemplo

El siguiente ejemplo muestra una llamada API para crear un agente de datos en Microsoft Azure. Simplemente reemplazarías <user_token> y <accountId> con el token y el ID que obtuviste 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" }
```

¿Que sigue?

El token de usuario de NetApp Console tiene una fecha de vencimiento. Para actualizar el token, debes llamar nuevamente a la API desde el paso 1.

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

Utilizar API de listas

Las API de lista son API asincrónicas, por lo que el resultado no se devuelve inmediatamente (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, debes utilizar el GET /messages/client API.

Pasos

1. Llame a la API de lista que desea utilizar.
2. Utilice el GET /messages/client API para ver el resultado de la operación.
3. Utilice la misma API agregándole 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

Cuando llamas al list-s3-buckets API, no se devuelve un resultado 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 fue

procesado.

Para obtener el resultado de la operación, debe utilizar 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 que envió el servidor. Por ejemplo:

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

Ahora deberá realizar la siguiente llamada API utilizando 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 una serie de mensajes. Dentro de cada mensaje hay un objeto de carga útil, que consta del 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"
  }
]
```

Referencia de API

La documentación para cada API de copia y sincronización está disponible en <https://api.cloudsync.netapp.com/docs>.

Conceptos

Descripción general de licencias para NetApp Copy and Sync

Hay dos formas de pagar las relaciones de NetApp Copy and Sync una vez finalizada la prueba gratuita de 14 días. La primera opción es suscribirse desde AWS o Azure con pago por uso o pago anual. La segunda opción es comprar licencias directamente de NetApp.

Las licencias deben administrarse a través de NetApp Copy and Sync o el sitio web correspondiente y **no** a través de la NetApp Console.

Suscripción al Marketplace

Suscribirse a Copy and Sync desde AWS o Azure le permite pagar una tarifa por hora o anualmente. ["Puede suscribirse a través de AWS o Azure"](#), dependiendo de dónde desea que se le facture.



Copy and Sync solo admite suscripciones de Marketplace de **AWS** y **Azure**. Las suscripciones de Google Cloud Marketplace no son compatibles con Copiar y sincronizar.

Suscripción por horas

Con una suscripción de pago por hora, se le cobrará por hora según la cantidad de relaciones de sincronización que cree.

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

Suscripción anual

Una suscripción anual proporciona una licencia para 20 relaciones de sincronización que debes pagar por adelantado. Si supera las 20 relaciones de sincronización y se ha suscrito a través de AWS, pagará las relaciones adicionales por hora.

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

Licencias de NetApp

Otra forma de pagar las relaciones de sincronización por adelantado es comprando licencias directamente de NetApp. Cada licencia le permite crear hasta 20 relaciones de sincronización.

Puede utilizar estas licencias con una suscripción de AWS o Azure. Por ejemplo, si tiene 25 relaciones de sincronización, puede pagar las primeras 20 relaciones de sincronización usando una licencia y luego pagar por uso desde AWS o Azure con las 5 relaciones de sincronización restantes.

["Descubra cómo comprar licencias y agregarlas a NetApp Copy and Sync"](#).

Términos de licencia

Los clientes que adquieran una licencia BYOL (Traiga su propia licencia) para copiar y sincronizar deben tener en cuenta las limitaciones asociadas con el derecho a la licencia.

- Los clientes tienen derecho a utilizar la licencia BYOL por un plazo que no exceda 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 una fuente y un destino (cada una una “relación de sincronización”).
- El derecho de un cliente vence al concluir el plazo de licencia de un año, independientemente de si el Cliente ha alcanzado el límite de relación de sincronización de 20.
- En el caso de que el Cliente elija renovar su licencia, las relaciones de sincronización no utilizadas asociadas a la concesión de licencia anterior NO se transfieren a la renovación de la licencia.

Privacidad de datos en NetApp Copy and Sync

NetApp no tiene acceso a ninguna credencial que proporcione al usar NetApp Copy and Sync. Las credenciales se almacenan directamente en la máquina del agente de datos, que reside en su red.

Según la configuración que elija, Copiar y sincronizar podría solicitarle credenciales cuando cree una nueva relación. Por ejemplo, al configurar una relación que incluye un servidor SMB o al implementar el agente de datos en AWS.

Estas credenciales siempre se guardan directamente en el propio agente de datos. El agente de datos reside en una máquina de su red, ya sea en sus instalaciones o en su cuenta en la nube. Las credenciales nunca están disponibles para NetApp.

Las credenciales se cifran localmente en la máquina del agente de datos mediante HashiCorp Vault.

Preguntas frecuentes técnicas NetApp Copy and Sync

Estas preguntas frecuentes pueden ayudarte si simplemente buscas una respuesta rápida a una pregunta.

Empezando

Las siguientes preguntas están relacionadas con cómo comenzar a utilizar NetApp Copy and Sync.

¿Cómo funciona NetApp Copy and Sync ?

Copy and Sync utiliza el software de agente de datos de NetApp para sincronizar datos desde un origen a un destino (esto se denomina *relación de sincronización*).

Un grupo de intermediarios de datos controla las relaciones de sincronización entre sus fuentes y destinos. Después de configurar una relación de sincronización, Copy and Sync analiza su sistema de origen y lo divide en múltiples flujos de replicación para enviarlos a los datos de destino seleccionados.

Después de la copia inicial, Copiar y sincronizar sincroniza todos los datos modificados según el cronograma que usted establezca.

¿Cómo funciona la prueba gratuita de 14 días?

La prueba gratuita de 14 días comienza cuando te registras en Copy and Sync. No estará sujeto a los cargos de NetApp por las relaciones de copia y sincronización que cree durante 14 días. Sin embargo, aún se aplican todos los cargos por recursos para cualquier agente de datos que implemente.

¿Cuanto cuesta copiar y sincronizar?

Hay dos tipos de costos asociados con el uso de Copiar y sincronizar: cargos por servicio y cargos por recursos.

Cargos por servicio

En el modelo de pago por uso, los cargos por servicio de copia y sincronización se cobran por hora y en función de la cantidad de relaciones de sincronización que usted cree.

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

Las licencias de copia y sincronización también están disponibles a través de su representante de NetApp . Cada licencia permite 20 relaciones de sincronización durante 12 meses.

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



Las relaciones de copia y sincronización son gratuitas para Azure NetApp Files.

Cargos por recursos

Los cargos por recursos están relacionados con los costos de computación y almacenamiento para ejecutar el agente de datos en la nube.

¿Cómo se factura Copy and Sync y cómo administro mi suscripción?

Hay dos formas de pagar las relaciones de sincronización una vez finalizada la prueba gratuita de 14 días. La primera opción es suscribirse desde AWS o Azure, lo que le permite pagar por uso o pagar anualmente. La segunda opción es comprar licencias directamente de NetApp. En cada caso, su suscripción se administrará a través del mercado de su proveedor y **no** a través de la interfaz de usuario Copiar y sincronizar.

¿Puedo usar Copiar y Sincronizar fuera de la nube?

Sí, puedes usar Copiar y Sincronizar en una arquitectura que no sea en la nube. La fuente y el destino pueden residir localmente, al igual que el software del intermediario de datos.

Tenga en cuenta los siguientes puntos clave sobre el uso de Copiar y sincronizar fuera de la nube:

- Un grupo de corredores de datos necesita una conexión a Internet para comunicarse con Copy and Sync.
- Si no compra una licencia directamente de NetApp, necesitará una cuenta de AWS o Azure para la facturación de PAYGO Copy and Sync.

¿Cómo accedo a Copiar y sincronizar?

Copiar y sincronizar está disponible desde la NetApp Console. Desde la navegación izquierda de la consola,

seleccione **Movilidad > Copiar y sincronizar**.

¿Qué es un grupo de corredores de datos?

Cada corredor de datos pertenece a un grupo de corredores de datos. La agrupación de corredores de datos ayuda a mejorar el rendimiento de las relaciones de sincronización.

Fuentes y objetivos admitidos

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

¿Qué fuentes y destinos admite Copy and Sync?

Copiar y sincronizar admite muchos tipos diferentes de relaciones de sincronización. ["Ver la lista completa"](#) .

¿Qué versiones de NFS y SMB admite Copy and Sync?

Copy and Sync admite NFS versión 3 y posteriores, y SMB versión 1 y posteriores.

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

Cuando Amazon S3 es el objetivo, ¿se pueden organizar los datos en niveles de una clase de almacenamiento S3 específica?

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

- Estándar (esta es la clase predeterminada)
- Niveles inteligentes
- Acceso estándar poco frecuente
- Una zona - Acceso poco frecuente
- Archivo de Glaciar Deep
- Recuperación flexible de glaciares
- Recuperación instantánea de glaciares

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

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

- Almacenamiento en caliente
- Almacenamiento en frío

¿Es compatible con los niveles de almacenamiento de Google Cloud?

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

- Estándar
- Cerca de línea

- Línea fría
- Archivo

Redes

Las siguientes preguntas se relacionan con los requisitos de red para copiar y sincronizar.

¿Cuáles son los requisitos de red para copiar y sincronizar?

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

Además, un grupo de corredores de datos necesita una conexión a Internet saliente a través del puerto 443 para poder comunicarse con Copy and Sync y contactar a algunos otros servicios y repositorios.

Para más detalles, ["revisar los requisitos de red"](#) .

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

Sí.

Copy and 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 enruta a través del proxy. Tenga en cuenta que el tráfico que no sea HTTP, como NFS o SMB, no se puede enrutar a través de un servidor proxy.

La única limitación del servidor proxy es cuando se usa 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 relacionan con cómo funciona la sincronización de datos.

¿Con qué frecuencia se produce la sincronización?

El cronograma predeterminado está configurado para la sincronización diaria. Después de la sincronización inicial, puedes:

- Modifique la programación de sincronización según la cantidad deseada de días, horas o minutos.
- Deshabilitar la programación de sincronización
- Eliminar la programación de sincronización (no se perderán datos; solo se eliminará la relación de sincronización)

¿Cuál es el cronograma mínimo de sincronización?

Puede programar una relación para sincronizar datos con una frecuencia de hasta 1 minuto.

¿El grupo del agente de datos vuelve a intentarlo cuando un archivo no se puede sincronizar? ¿O se agota el tiempo?

Un grupo de intermediarios de datos no expira cuando no se puede transferir un solo archivo. En lugar de ello, el grupo de intermediarios de datos vuelve a intentarlo tres 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"](#) .

¿Qué pasa si tengo un conjunto de datos muy grande?

Si un solo directorio contiene 600.000 archivos o más, ["Contáctanos"](#) para que podamos ayudarle a configurar el grupo de intermediarios de datos 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 para la cantidad total de archivos en el 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 seguro copiar y sincronizar?

Sí. Toda la conectividad de red de Copia y Sincronización se realiza mediante ["Servicio de cola simple de Amazon \(SQS\)"](#) .

Toda la comunicación entre el grupo de intermediarios de datos y Amazon S3, Azure Blob, Google Cloud Storage e IBM Cloud Object Storage se realiza a través del protocolo HTTPS.

Si utiliza Copiar y sincronizar con sistemas locales (de origen o destino), aquí le presentamos algunas opciones de conectividad recomendadas:

- Una conexión de AWS Direct Connect, Azure ExpressRoute o Google Cloud Interconnect, que no está enrutada a través de Internet (y solo puede comunicarse con las redes en la nube que usted especifique)
- Una conexión VPN entre su dispositivo de puerta de enlace local y sus redes en la nube
- Para una transferencia de datos más segura con buckets S3, almacenamiento de blobs de Azure o Google Cloud Storage, se puede establecer un punto de conexión S3 privado de Amazon, puntos de conexión de servicio de red virtual de Azure o acceso privado de Google.

Cualquiera de estos métodos establece una conexión segura entre sus servidores NAS locales y un grupo de agentes de datos de copia y sincronización.

¿Los datos están encriptados por Copiar y Sincronizar?

- Copy and Sync admite el cifrado de datos en tránsito entre servidores NFS de origen y destino. ["Más información"](#) .
- Para SMB, Copy and Sync admite datos SMB 3.0 y 3.11 que haya cifrado en el lado del servidor. Copiar y sincronizar copia los datos cifrados del origen al destino, donde los datos permanecen cifrados.

Copiar y sincronizar no puede cifrar datos SMB por sí solo.

- Cuando un bucket de Amazon S3 es el destino de una relación de sincronización, puede elegir si desea habilitar el cifrado de datos mediante el cifrado de AWS KMS o el cifrado AES-256.
- Cuando un depósito de Google Storage es el destino de una relación de sincronización, puedes elegir si deseas utilizar la clave de cifrado predeterminada administrada por Google o tu propia clave KMS.

Permisos

Las siguientes preguntas se relacionan con los permisos de datos.

¿Los permisos de datos SMB están sincronizados con la ubicación de destino?

Puede configurar Copiar y sincronizar para conservar las listas de control de acceso (ACL) entre un recurso compartido SMB de origen y un recurso compartido SMB de destino, y desde un recurso compartido SMB de origen hasta el almacenamiento de objetos (excepto ONTAP S3).



Copiar y sincronizar no admite la copia de ACL desde el almacenamiento de objetos a recursos compartidos SMB.

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



Copy Sync copia las ACL (permisos) de SMB, pero no copia la propiedad de archivos o carpetas. El atributo de propiedad no está incluido en la operación de copia de ACL SMB. Si necesita conservar la propiedad al copiar datos entre recursos compartidos SMB, utilice `robocopy` para copiar manualmente la información de seguridad. Por ejemplo, el `/copyall`. Las copias de bandera incluyen ACL, propietario y datos de auditoría.

¿Los permisos de datos NFS están sincronizados con la ubicación de destino?

Copiar y sincronizar copia automáticamente los permisos NFS entre servidores NFS de la siguiente manera:

- NFS versión 3: Copiar y sincronizar copia los permisos y el propietario del grupo de usuarios.
- Versión 4 de NFS: Copiar y sincronizar copia las ACL.

Metadatos de almacenamiento de objetos

¿Qué tipos de relaciones de sincronización preservan los metadatos del almacenamiento de objetos?

Copiar y sincronizar copia metadatos de almacenamiento de objetos del origen al destino para los siguientes tipos de relaciones de sincronización:

- Amazon S3 → Amazon S3 ¹
- Amazon S3 → StorageGRID
- StorageGRID → Amazon S3
- StorageGRID → StorageGRID
- StorageGRID → Almacenamiento en la nube de Google
- Almacenamiento en la nube de Google → StorageGRID ¹
- Almacenamiento en la nube de Google → Almacenamiento de objetos en la nube de IBM ¹
- Almacenamiento en la nube de Google → Amazon S3 ¹

- Amazon S3 → Almacenamiento en la nube de Google
- Almacenamiento de objetos en IBM Cloud → Almacenamiento en Google Cloud
- StorageGRID → Almacenamiento de objetos en la nube de IBM
- Almacenamiento de objetos en IBM Cloud → StorageGRID
- Almacenamiento de objetos en IBM Cloud → Almacenamiento de objetos en IBM Cloud

¹ Para estas relaciones de sincronización, necesitas ["Habilite la configuración Copiar para objetos cuando cree la relación de sincronización"](#) .

¿Qué tipos de metadatos se replican durante las sincronizaciones donde NFS o SMB son la fuente?

Los metadatos como el ID de usuario, la hora de modificación, la hora de acceso y el GID se replican de forma predeterminada. Los usuarios pueden optar por replicar ACL desde CIF marcándolo como obligatorio al crear una relación de sincronización.

Actuación

Las siguientes preguntas se relacionan con el rendimiento de Copiar y sincronizar.

¿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 intermediarios de datos. Si acelera el rendimiento de sincronización mediante el uso de múltiples intermediarios de datos, entonces el rendimiento es 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 (varios TiB cada uno), puede llevar mucho tiempo completar el proceso de transferencia y el rendimiento podría verse afectado.

Limitar el número de transferencias simultáneas puede ayudar. ["Contáctanos para obtener ayuda"](#) .

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

Al sincroniza datos hacia o desde Azure NetApp Files, es posible que experimente fallas 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 sobre los niveles de servicio y el rendimiento de Azure NetApp Files"](#) .

¿Cuántos corredores de datos se requieren en un grupo?

Cuando crea una nueva relación, comienza con un solo agente de datos en 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 para una relación de sincronización. Si no es así, puede acelerar el rendimiento de la sincronización agregando agentes de datos adicionales al grupo. Pero primero debes comprobar otros factores que pueden afectar el rendimiento de la sincronización.

Existen múltiples factores que pueden afectar el rendimiento de la transferencia de datos. El rendimiento general de sincronización puede verse afectado debido al ancho de banda de la red, la latencia y la topología

de la red, así como también por las especificaciones de la máquina virtual del agente de datos y el rendimiento del sistema de almacenamiento. Por ejemplo, un solo agente de datos en un grupo puede alcanzar 100 MB/s, mientras que el rendimiento del disco en el destino podría permitir solo 64 MB/s. Como resultado, el grupo de corredores de datos sigue intentando copiar los datos, pero el objetivo no puede alcanzar el rendimiento del grupo de corredores de datos.

Por lo tanto, asegúrese de verificar el rendimiento de su red y el rendimiento del disco en el destino.

Luego, puede considerar acelerar el rendimiento de la sincronización agregando intermediarios de datos adicionales a un grupo para compartir la carga de esa relación. "[Aprenda a acelerar el rendimiento de la sincronización](#)".

Borrando cosas

Las siguientes preguntas se relacionan con la eliminación de relaciones de sincronización y datos de orígenes y destinos.

¿Qué sucede si elimino mi relación de Copiar y Sincronizar?

Eliminar una relación detiene todas las sincronizaciones de datos futuras y finaliza el pago. Todos los datos que se sincronizaron con el destino permanecen tal como están.

¿Qué sucede si borro algo de mi servidor de origen? ¿Se elimina también del objetivo?

De forma predeterminada, si tiene una relación de sincronización activa, el elemento eliminado en el servidor de origen no se elimina del destino durante la próxima sincronización. Pero hay una opción en la configuración de sincronización para cada relación, donde puedes definir que Copiar y Sincronizar eliminará los archivos en la ubicación de destino si se eliminaron de la fuente.

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

¿Qué pasa si borro algo de mi objetivo? ¿Se elimina también de mi fuente?

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

Solución de problemas

"[Base de conocimientos de NetApp : Preguntas frecuentes sobre copia y sincronización: Soporte y solución de problemas](#)"

Análisis profundo del corredor de datos

La siguiente pregunta se relaciona con el corredor de datos.

¿Puedes explicar la arquitectura del broker de datos?

Seguro. A continuación los puntos más importantes:

- El agente de datos es una aplicación node.js que se ejecuta en un host Linux.
- Copiar y sincronizar implementa el agente de datos de la siguiente manera:
 - AWS: desde una plantilla de AWS CloudFormation

- Azure: desde Azure Resource Manager
- Google: Desde Google Cloud Deployment Manager
- Si utiliza su propio host Linux, deberá instalar manualmente el software
- El software del broker de datos se actualiza automáticamente a la última versión.
- El broker de datos utiliza AWS SQS como canal de comunicación confiable y seguro y para control y monitoreo. SQS también proporciona una capa de persistencia.
- Puede agregar corredores de datos adicionales a un grupo para aumentar la velocidad de transferencia y agregar alta disponibilidad. Existe resiliencia del servicio si falla un agente de datos.

Conocimiento y apoyo

Regístrese para recibir asistencia

Es necesario registrarse para recibir soporte técnico específico para la NetApp Console y sus soluciones de almacenamiento y servicios de datos. También es necesario registrarse para obtener soporte técnico para habilitar flujos de trabajo clave para los sistemas Cloud Volumes ONTAP .

Registrarse para recibir soporte no habilita el soporte de NetApp para un servicio de archivos de un proveedor de nube. Para obtener asistencia técnica relacionada con un servicio de archivos de un proveedor de nube, su infraestructura o cualquier solución que utilice el servicio, consulte "Obtener ayuda" en la documentación de ese producto.

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

Descripción general del registro de soporte

Existen dos formas de registro para activar el derecho a recibir ayuda:

- Registrar el número de serie de su cuenta de la NetApp Console (su número de serie 960xxxxxxx de 20 dígitos ubicado en la página Recursos de soporte en la consola).

Esto sirve como su ID de suscripción de soporte único para cualquier servicio dentro de la Consola. Cada cuenta de consola debe estar registrada.

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

Estos números de serie se conocen comúnmente como *números de serie PAYGO* y son generados por la NetApp Console en el momento de la implementación de Cloud Volumes ONTAP .

El registro de ambos tipos de números de serie permite funciones como la apertura de tickets de soporte y la generación automática de casos. El registro se completa agregando cuentas del sitio de soporte de NetApp (NSS) a la consola como se describe a continuación.

Registrar la NetApp Console para obtener soporte de NetApp

Para registrarse para recibir soporte y activar el derecho a soporte, un usuario de su cuenta de NetApp Console debe asociar una cuenta del sitio de soporte de NetApp con su inicio de sesión de consola. La forma de registrarse para el soporte de NetApp depende de si ya tiene una cuenta del sitio de soporte de NetApp (NSS).

Cliente existente con una cuenta NSS

Si es cliente de NetApp con una cuenta NSS, simplemente necesita registrarse para recibir soporte a través de la consola.

Pasos

1. Seleccione **Administración > Credenciales**.
2. Seleccione **Credenciales de usuario**.
3. Seleccione **Agregar credenciales NSS** y siga las instrucciones de autenticación del Sitio de soporte de NetApp (NSS).
4. Para confirmar que el proceso de registro fue exitoso, seleccione el ícono de Ayuda y seleccione **Soporte**.

La página **Recursos** debería mostrar que su cuenta de consola está registrada para recibir soporte.

Tenga en cuenta que otros usuarios de la consola no verán este mismo estado de registro de soporte si no han asociado una cuenta del sitio de soporte de NetApp con su inicio de sesión. Sin embargo, eso no significa que su cuenta no esté registrada para recibir soporte. Siempre que un usuario de la organización haya seguido estos pasos, su cuenta quedará registrada.

Soy cliente actual pero no tengo cuenta NSS

Si es un cliente existente de NetApp con licencias y números de serie existentes pero *no* una cuenta NSS, debe crear una cuenta NSS y asociarla con su inicio de sesión de la consola.

Pasos

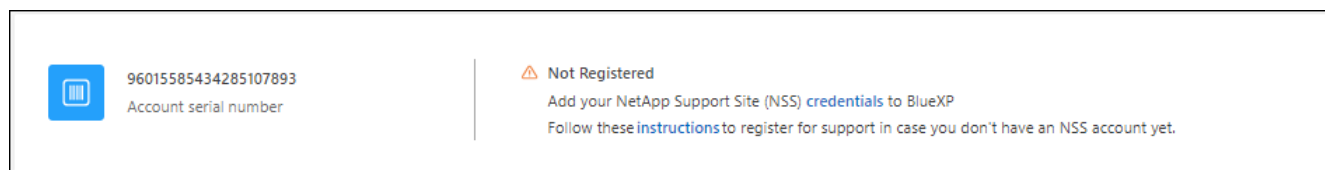
1. Cree una cuenta en el sitio de soporte de NetApp completando el "[Formulario de registro de usuario del sitio de soporte de NetApp](#)"
 - a. Asegúrese de seleccionar el nivel de usuario apropiado, que normalmente es **Cliente de NetApp /Usuario final**.
 - b. Asegúrese de copiar el número de serie de la cuenta de la consola (960xxxx) utilizado anteriormente para el campo de número de serie. Esto acelerará el procesamiento de la cuenta.
2. Asocie su nueva cuenta NSS con su inicio de sesión de la consola completando los pasos a continuación [Cliente existente con una cuenta NSS](#).

Completamente nuevo en NetApp

Si es nuevo en NetApp y no tiene una cuenta NSS, siga cada paso a continuación.

Pasos

1. En la parte superior derecha de la Consola, seleccione el ícono Ayuda y seleccione **Soporte**.
2. Localice el número de serie de su ID de cuenta en la página de Registro de soporte.



3. Navegar a "[Sitio de registro de soporte de NetApp](#)" y seleccione ***No soy un cliente registrado de NetApp ***.
4. Llene los campos obligatorios (aquellos con asteriscos rojos).
5. En el campo **Línea de productos**, seleccione **Administrador de nube** y luego seleccione su proveedor de facturación correspondiente.
6. Copie el número de serie de su cuenta del paso 2 anterior, complete la verificación de seguridad y luego confirme que leyó la Política de privacidad de datos global de NetApp.

Se envía inmediatamente un correo electrónico al buzón proporcionado para finalizar esta transacción segura. Asegúrese de revisar sus carpetas de correo no deseado si el correo electrónico de validación no llega en unos minutos.

7. Confirme la acción desde el correo electrónico.

Al confirmar, se envía su solicitud a NetApp y se recomienda que cree una cuenta en el sitio de soporte de NetApp .

8. Cree una cuenta en el sitio de soporte de NetApp completando el ["Formulario de registro de usuario del sitio de soporte de NetApp"](#)

- a. Asegúrese de seleccionar el nivel de usuario apropiado, que normalmente es **Cliente de NetApp /Usuario final**.
- b. Asegúrese de copiar el número de serie de la cuenta (960xxxx) utilizado anteriormente para el campo de número de serie. Esto acelerará el procesamiento.

Después de terminar

NetApp debería comunicarse con usted durante este proceso. Este es un ejercicio de incorporación único para nuevos usuarios.

Una vez que tenga su cuenta del sitio de soporte de NetApp , asocie la cuenta con su inicio de sesión de consola completando los pasos a continuación.[Cliente existente con una cuenta NSS](#) .

Asociar credenciales NSS para la compatibilidad con Cloud Volumes ONTAP

Es necesario asociar las credenciales del sitio de soporte de NetApp con su cuenta de consola para habilitar los siguientes flujos de trabajo clave para Cloud Volumes ONTAP:

- Registro de sistemas Cloud Volumes ONTAP de pago por uso para obtener soporte

Es necesario proporcionar su cuenta NSS para activar el soporte para su sistema y obtener acceso a los recursos de soporte técnico de NetApp .

- Implementación de Cloud Volumes ONTAP cuando trae su propia licencia (BYOL)

Es necesario proporcionar su cuenta NSS para que la consola pueda cargar su clave de licencia y habilitar la suscripción por el período que compró. Esto incluye actualizaciones automáticas para renovaciones de plazos.

- Actualización del software Cloud Volumes ONTAP a la última versión

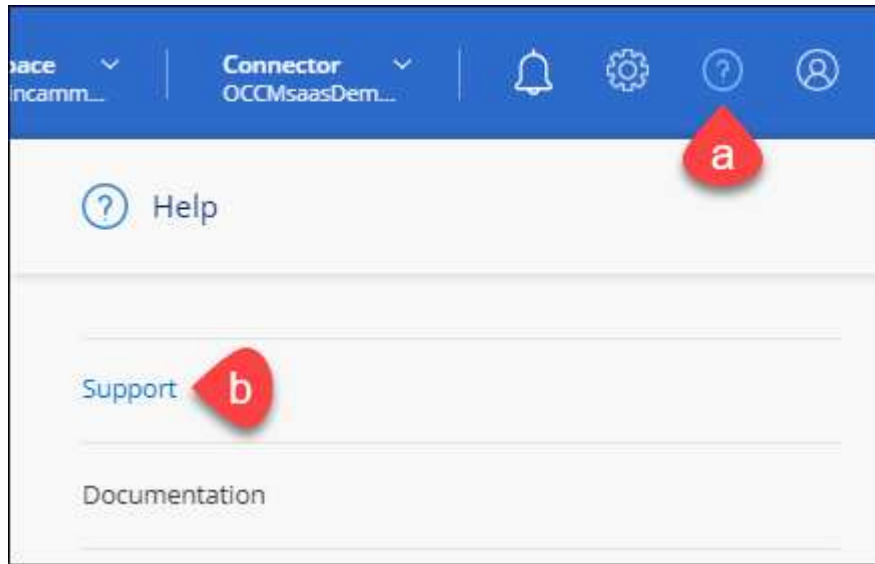
La asociación de credenciales NSS con su cuenta de NetApp Console es diferente a la asociación de una cuenta NSS con un inicio de sesión de usuario de consola.

Estas credenciales de NSS están asociadas con su ID de cuenta de consola específica. Los usuarios que pertenecen a la organización de la Consola pueden acceder a estas credenciales desde **Soporte > Administración de NSS**.

- Si tiene una cuenta de nivel de cliente, puede agregar una o más cuentas NSS.
- Si tiene una cuenta de socio o revendedor, puede agregar una o más cuentas NSS, pero no se pueden agregar junto con cuentas de nivel de cliente.

Pasos

1. En la parte superior derecha de la Consola, seleccione el ícono Ayuda y seleccione **Soporte**.



2. Seleccione **Administración de NSS > Agregar cuenta NSS**.
3. Cuando se le solicite, seleccione **Continuar** para ser redirigido a una página de inicio de sesión de Microsoft.

NetApp utiliza Microsoft Entra ID como proveedor de identidad para servicios de autenticación específicos de soporte y licencias.

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

Estas acciones permiten que la consola utilice 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 NSS a nivel de cliente.
- Solo puede haber una cuenta NSS si esa cuenta es una cuenta de nivel de socio. Si intenta agregar cuentas NSS de nivel de cliente y existe una cuenta de nivel de socio, recibirá el siguiente mensaje de error:

"El tipo de cliente NSS no está permitido para esta cuenta porque ya hay usuarios NSS de otro tipo".

Lo mismo ocurre si tiene cuentas NSS de nivel de cliente preexistentes e intenta agregar una cuenta de nivel de socio.

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

Esta es una identificación generada por el sistema que se asigna a su correo electrónico. En la página **Administración de NSS**, puede mostrar su correo electrónico desde el **...** menú.

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

Al utilizar esta opción se le solicitará que inicie sesión nuevamente. Tenga en cuenta que el token de

estas cuentas caduca después de 90 días. Se publicará una notificación para avisarle de esto.

Obtener ayuda

NetApp ofrece soporte para BlueXP y sus servicios en la nube de diversas maneras. Disponemos de amplias opciones de autoasistencia gratuitas las 24 horas, los 7 días de la semana, como artículos de la base de conocimientos (KB) y un foro comunitario. Su registro de soporte incluye soporte técnico remoto mediante tickets web.

Obtenga soporte para un servicio de archivos de un proveedor de nube

Para obtener asistencia técnica relacionada con un servicio de archivos de un proveedor de nube, su infraestructura o cualquier solución que utilice el servicio, consulte "Obtener ayuda" en la documentación de BlueXP para ese producto.

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

Para recibir soporte técnico específico para BlueXP y sus soluciones y servicios de almacenamiento, utilice las opciones de soporte que se describen a continuación.

Utilice opciones de autosuficiencia

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

- Documentación

La documentación de BlueXP que estás viendo actualmente.

- ["Base de conocimientos"](#)

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

- ["Comunidades"](#)

Únase a la comunidad BlueXP para seguir las discusiones en curso o crear otras nuevas.

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.

Antes de empezar

- Para utilizar la función **Crear un caso**, primero debe asociar sus credenciales del sitio de soporte de NetApp con su inicio de sesión de BlueXP. ["Aprenda a administrar las credenciales asociadas con su inicio de sesión de BlueXP"](#).
- Si está abriendo un caso para un sistema ONTAP que tiene un número de serie, entonces su cuenta NSS debe estar asociada con el número de serie de ese sistema.

Pasos

1. En BlueXP, seleccione **Ayuda > Soporte**.
2. En la página **Recursos**, elija una de las opciones disponibles en Soporte técnico:
 - a. Seleccione **Llámenos** si desea hablar con alguien por teléfono. Serás dirigido a una página en netapp.com que enumera los números de teléfono a los que puedes llamar.
 - b. Seleccione **Crear un caso** para abrir un ticket con un especialista de soporte de NetApp :
 - **Servicio:** Seleccione el servicio con el que está asociado el problema. Por ejemplo, BlueXP cuando es específico para un problema de soporte técnico con flujos de trabajo o funcionalidad dentro del servicio.
 - **Entorno de trabajo:** si corresponde al almacenamiento, seleccione * Cloud Volumes ONTAP* o **On-Prem** y luego el entorno de trabajo asociado.

La lista de entornos de trabajo está dentro del alcance de la organización (o cuenta), el proyecto (o espacio de trabajo) y el conector de BlueXP que haya seleccionado en el banner superior del servicio.

- **Prioridad del caso:** elija la prioridad del caso, que puede ser Baja, Media, Alta o Crítica.

Para obtener más detalles sobre estas prioridades, pase el mouse sobre el ícono de información junto al nombre del campo.

- **Descripción del problema:** proporcione una descripción detallada de su problema, incluidos los mensajes de error aplicables o los pasos de solución de problemas que realizó.
- **Direcciones de correo electrónico adicionales:** Ingrese direcciones de correo electrónico adicionales si desea informar a otra persona sobre este problema.
- **Adjunto (opcional):** cargue hasta cinco archivos adjuntos, uno a la vez.

Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.

ntapitdemo
NetApp Support Site Account

Service

Select

Working Enviroment

Select

Case Priority

Low - General guidance

Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional)

Type here

Attachment (Optional)

No files selected

Upload

Después de terminar

Aparecerá una ventana emergente con su número de caso de soporte. Un especialista de soporte de NetApp revisará su caso y se comunicará con usted pronto.

Para obtener un historial de sus casos de soporte, puede seleccionar **Configuración > Cronología** y buscar acciones llamadas "crear caso de soporte". Un botón en el extremo derecho le permite ampliar la acción para ver detalles.

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

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

Este error podría significar que la cuenta NSS y la empresa registrada con la que está asociada no son la misma empresa registrada para el número de serie de la cuenta BlueXP (es decir, 960xxxx) o el número de serie del entorno de trabajo. Puede buscar ayuda utilizando una de las siguientes opciones:

- Utilice el chat dentro del producto
- Envíe un caso no técnico a <https://mysupport.netapp.com/site/help>

Gestione sus casos de soporte (Vista previa)

Puede ver y administrar casos de soporte activos y resueltos directamente desde BlueXP. Podrás gestionar los casos asociados a tu cuenta NSS y a tu empresa.

La gestión de casos está disponible como vista previa. Planeamos perfeccionar esta experiencia y agregar mejoras en próximas versiones. Envíenos sus comentarios mediante el chat del producto.

Tenga en cuenta lo siguiente:

- El panel 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 usted proporcionó.
 - La vista de la derecha muestra el total de casos abiertos en los últimos 3 meses a nivel de su empresa en función de su cuenta de usuario NSS.

Los resultados en la tabla reflejan los casos relacionados con la vista que usted seleccionó.

- Puede agregar o eliminar columnas de interés y puede filtrar el contenido de columnas como Prioridad y Estado. Otras columnas sólo proporcionan capacidades de clasificación.

Vea los pasos a continuación para obtener más detalles.

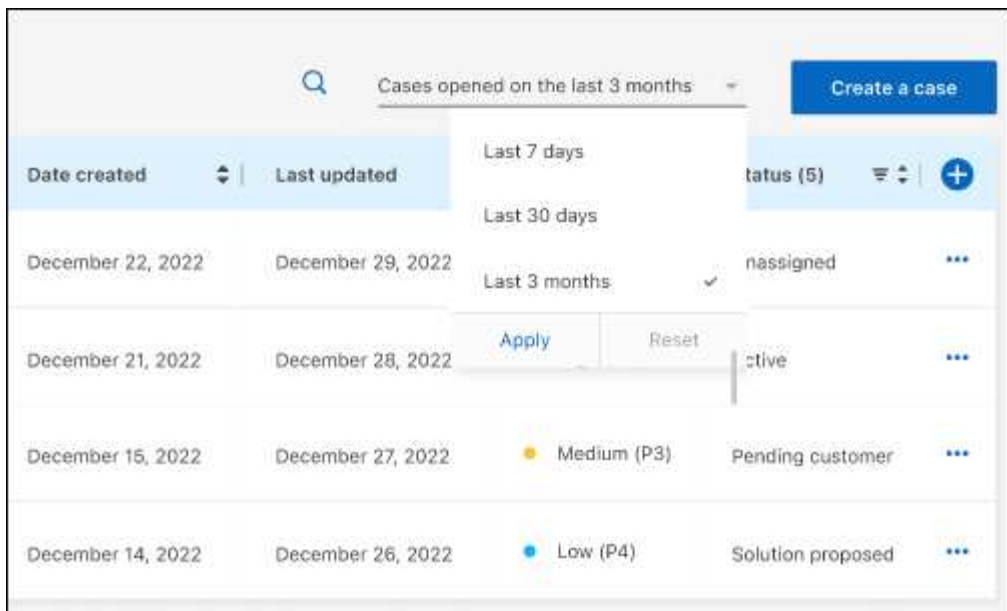
- A nivel de caso, ofrecemos la posibilidad de actualizar notas de caso o cerrar un caso que aún no esté en estado Cerrado o Pendiente de cierre.

Pasos

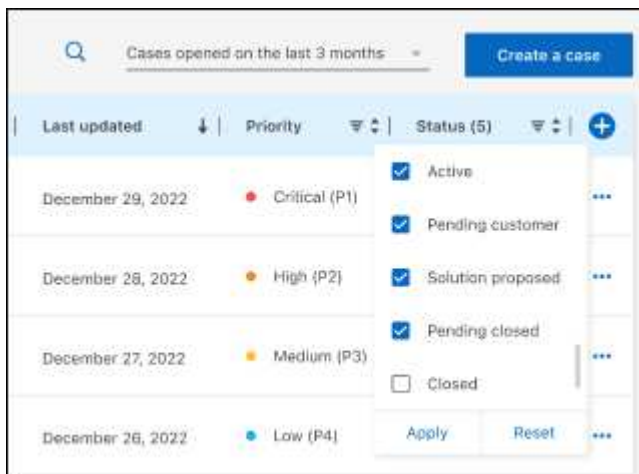
1. En BlueXP, seleccione **Ayuda > Soporte**.
2. Seleccione **Administración de casos** y, si se le solicita, agregue su cuenta NSS a BlueXP.


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

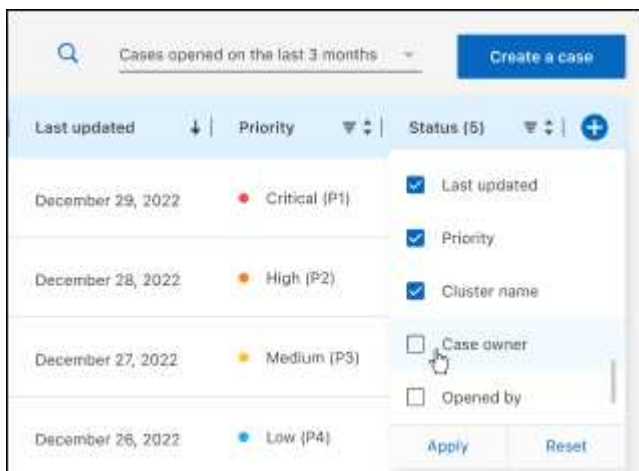
3. Modifique opcionalmente la información que se muestra en la tabla:
 - En **Casos de la organización**, seleccione **Ver** para ver todos los casos asociados a su empresa.
 - Modifique el rango de fechas eligiendo un rango de fechas exacto o eligiendo un período de tiempo diferente.



- Filtrar el contenido de las columnas.



- Cambie las columnas que aparecen en la tabla seleccionando  y luego elegir las columnas que desea mostrar.

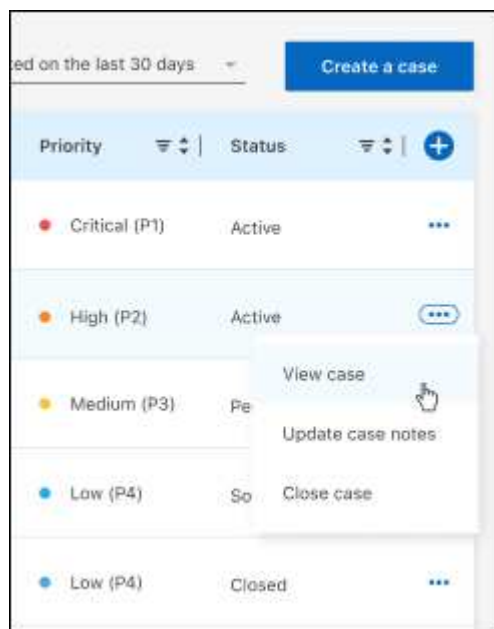


4. Gestionar un caso existente seleccionando... y seleccionando una de las opciones disponibles:

- **Ver caso:** Ver detalles completos sobre un caso específico.
- **Actualizar notas del caso:** proporcione detalles adicionales sobre su problema o seleccione **Cargar archivos** para adjuntar hasta un máximo de cinco archivos.

Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.

- **Cerrar caso:** proporcione detalles sobre el motivo por el cual está cerrando el caso y seleccione **Cerrar caso**.



Avisos legales

Los avisos legales proporcionan acceso a declaraciones de derechos de autor, marcas comerciales, patentes y más.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

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. Otros nombres de empresas y productos pueden ser marcas comerciales de sus respectivos propietarios.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patentes

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

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Política de privacidad

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Código abierto

Los archivos de aviso proporcionan información sobre derechos de autor y licencias de terceros utilizados en el software de NetApp .

["Aviso para NetApp Copy and Sync"](#)

Información de copyright

Copyright © 2025 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 INTERRUPTIÓN 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.