



# **Copiar y sincronizar datos**

## **Cloud Manager 3.8**

NetApp  
March 25, 2024

# Tabla de contenidos

- Copiar y sincronizar datos ..... 1
- Información general de Cloud Sync ..... 1
- Manos a la obra ..... 4
- Tutoriales ..... 36
- Gestión de relaciones de sincronización ..... 42
- API de Cloud Sync ..... 47
- Preguntas técnicas frecuentes sobre Cloud Sync ..... 50

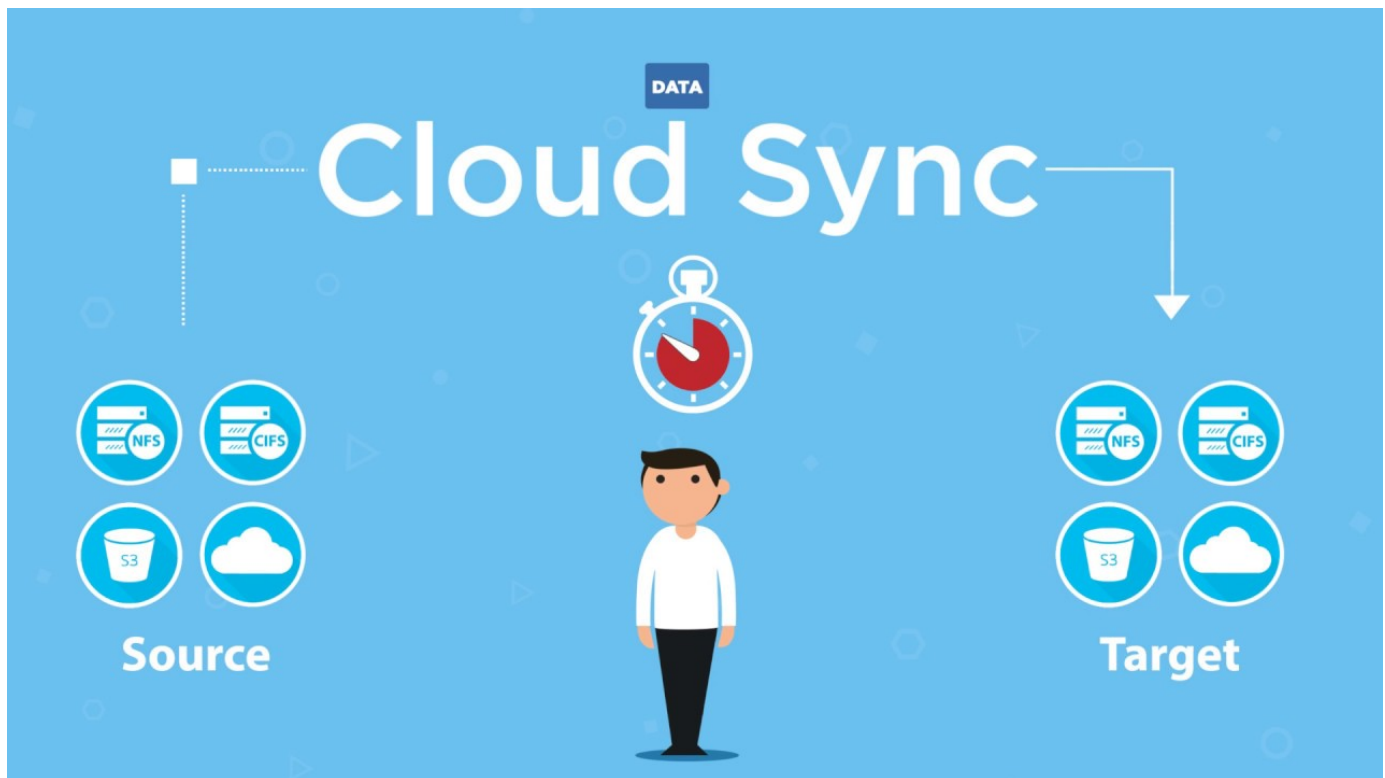
# Copiar y sincronizar datos

## Información general de Cloud Sync

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

### Funciones

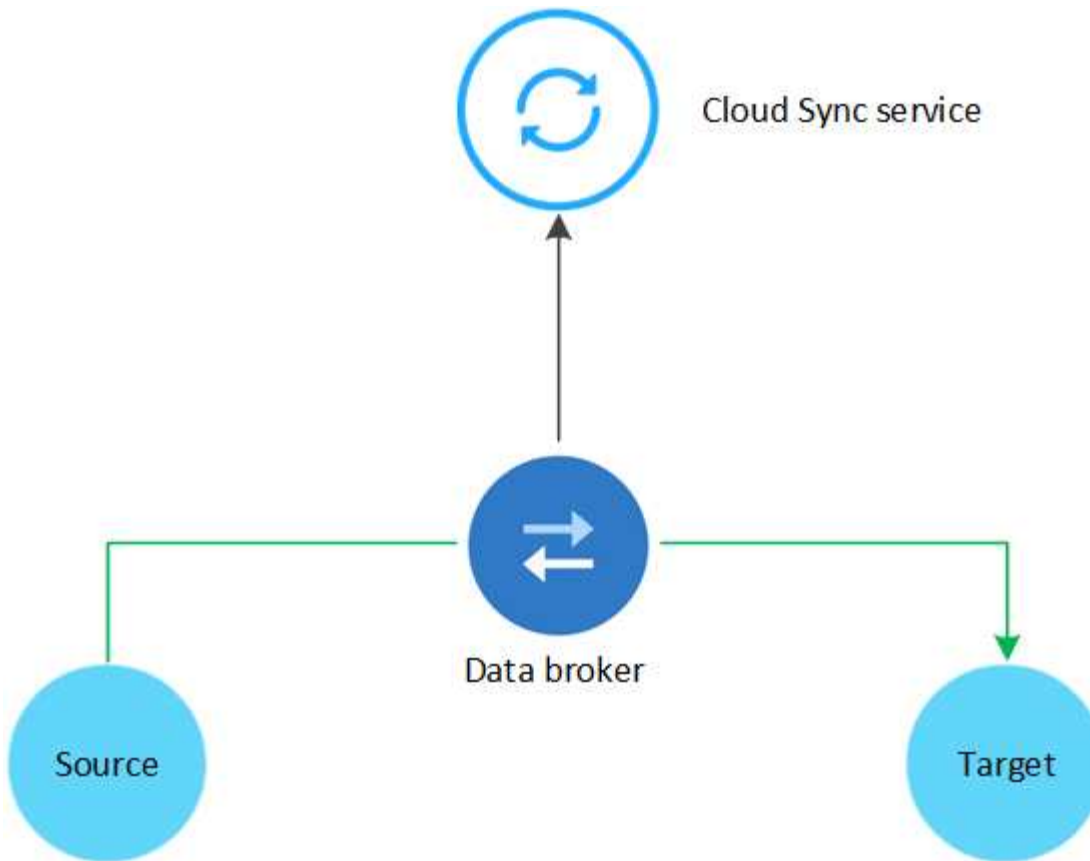
Vea el siguiente vídeo para obtener información general sobre Cloud Sync:



### Cómo funciona Cloud Sync

Cloud Sync es una plataforma de software como servicio (SaaS) que consta de un agente de datos, una interfaz basada en cloud disponible a través de Cloud Manager y un origen y un destino.

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



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

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

## Tipos de almacenamiento admitidos

Cloud Sync admite los siguientes tipos de almacenamiento:

- Cualquier servidor NFS
- Cualquier servidor SMB
- EFS DE AWS
- AWS S3
- Azure Blob
- Azure NetApp Files
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Google Cloud Storage
- Almacenamiento de objetos en cloud de IBM

- Clúster de ONTAP en las instalaciones
- Almacenamiento ONTAP S3
- StorageGRID

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

## Coste

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

### Cargos por recursos

Los cargos por recursos están relacionados con los costes de cómputo y almacenamiento para ejecutar el agente de datos en el cloud.

### Cargos por servicio

Hay dos formas de pagar las relaciones de sincronización después de que termine su prueba gratuita de 14 días. La primera opción es suscribirse a AWS o Azure, lo que permite pagar por horas o anualmente. La segunda opción consiste en comprar licencias directamente a NetApp. Lea las secciones siguientes para obtener más información.

## Suscripción a Marketplace

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

### Suscripciones por horas

Con una suscripción de pago por horas, el servicio Cloud Sync cobra por hora en función del número de relaciones de sincronización que cree.

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

### Suscripciones anuales

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

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

## De NetApp

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

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

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

## Términos de licencia

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

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

## Privacidad de datos

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

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

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

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

## Limitaciones

- Cloud Sync no es compatible con China.
- Además de China, el agente de datos de Cloud Sync no se ofrece en las siguientes regiones:
  - AWS GovCloud (EE. UU.)
  - Gobierno de Azure EE. UU
  - DoD de Azure US

## Manos a la obra

### Inicio rápido de Cloud Sync

Primeros pasos en el servicio Cloud Sync incluyen algunos pasos.



#### Prepare el origen y el destino

Compruebe que el origen y el destino son compatibles y están configurados. El requisito más importante es verificar la conectividad entre el agente de datos y las ubicaciones de origen y destino. ["Leer más"](#).

## 2

### Prepare una ubicación para el agente de datos de NetApp

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

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

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

## 3

### Cree su primera relación de sincronización

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

## 4

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

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

## Preparación del origen y del destino

Prepárese para sincronizar los datos mediante la verificación de que el origen y el destino son compatibles y la configuración.

### Relaciones de sincronización compatibles

Cloud Sync le permite sincronizar datos de un origen a un destino (esto se denomina *SYNC Relationship*). Debe comprender las relaciones admitidas antes de comenzar.

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



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

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

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

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

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

**Notas:**

1. Puede elegir un nivel de almacenamiento específico de Azure Blob cuando un contenedor Blob es el destino:
  - Almacenamiento en caliente
  - Almacenamiento en frío
2. puede elegir un tipo de almacenamiento S3 específico cuando AWS S3 es el destino:
  - Estándar (esta es la clase predeterminada)
  - Organización en niveles inteligente
  - Acceso Estándar-poco frecuente
  - Una Zona de acceso poco frecuente
  - Glaciar

- Glacier Deep Archive

## Redes para el origen y el destino

- El origen y el destino deben tener una conexión de red con el agente de datos.

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

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

## Requisitos de origen y objetivo

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

### requisitos de bloque de AWS S3

Asegúrese de que su bloque de AWS S3 cumpla con los siguientes requisitos.

## Ubicaciones de agentes de datos compatibles para AWS S3

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

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

## Regiones admitidas de AWS

Todas las regiones están soportadas excepto las regiones China y GovCloud (EE.UU.).

## Permisos necesarios para bloques de S3 en otras cuentas de AWS

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

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

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

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

ser el ARN de la función IAM creada por la plantilla.

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

## Summary

Delete role

Role ARN `arn:aws:iam::143281744617:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05`

Role description [Edit](#)

### requisitos de almacenamiento de Azure Blob

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

### Ubicaciones de agentes de datos compatibles para Azure Blob

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

### Regiones de Azure compatibles

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

### Se requiere una cadena de conexión para relaciones que incluyen Azure Blob y. NFS/SMB

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

The screenshot shows the 'Access keys' page for an Azure storage account. The page title is 'a63cde60b553020 - Access keys'. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Storage Explorer (preview), Settings, Access keys (highlighted), CORS, Configuration, and Encryption. The main content area includes instructions on using access keys and a list of keys. The 'key1' section shows the 'Key' and 'Connection string' fields. The 'Connection string' field is highlighted with a red box and contains the value 'DefaultEndpoints'. The 'Storage account name' field contains 'a63cde60b553020'.

Si desea sincronizar datos entre dos contenedores de Azure Blob, la cadena de conexión debe incluir un

"firma de acceso compartido" (SAS). También tiene la opción de utilizar un SAS al sincronizar entre un contenedor Blob y un servidor NFS o SMB.

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

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

The screenshot displays the Azure portal interface for configuring a Shared Access Signature (SAS) for a storage account named 'a63cde60b553020'. The left-hand navigation pane includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Storage Explorer (preview), Settings, Access keys, CORS, Configuration, Encryption, Shared access signature (highlighted with a red box), Firewalls and virtual networks, Advanced Threat Protection (pr...), Properties, and Locks. The main content area is titled 'Shared access signature' and contains several sections: 'Allowed services' with checkboxes for Blob (checked), File, Queue, and Table; 'Allowed resource types' with checkboxes for Service (checked), Container (checked), and Object (checked); 'Allowed permissions' with checkboxes for Read (checked), Write (checked), Delete (checked), List (checked), Add (checked), Create (checked), Update, and Process; 'Start and expiry date/time' with fields for Start (2018-10-23 at 10:07:32 AM) and End (2019-10-23 at 6:07:32 PM); 'Allowed IP addresses' with a text input field; 'Allowed protocols' with radio buttons for HTTPS only (selected) and HTTPS and HTTP; and 'Signing key' with a dropdown menu showing 'key1'. A blue button labeled 'Generate SAS and connection string' is located at the bottom of the configuration area, also highlighted with a red box.

### Requisito de Azure NetApp Files

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



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

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



## Requisitos de bucket de Google Cloud Storage

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

## Ubicaciones de agentes de datos compatibles para Google Cloud Storage

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

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

## Regiones compatibles de GCP

Se admiten todas las regiones.

## Requisitos del servidor NFS

- El servidor NFS puede ser un sistema de NetApp o un sistema que no sea de NetApp.
- El servidor de archivos debe permitir que el host de Data broker acceda a las exportaciones.
- Se admiten las versiones 3, 4.0, 4.1 y 4.2 de NFS.

La versión deseada debe estar activada en el servidor.

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



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

## Requisitos de almacenamiento de S3 de ONTAP

ONTAP 9.7 admite Amazon simple Storage Service (Amazon S3) como vista previa pública. ["Obtenga más información sobre la compatibilidad de ONTAP para Amazon S3"](#).

Al configurar una relación de sincronización que incluya el almacenamiento de ONTAP S3, tendrá que proporcionar lo siguiente:

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

## Requisitos del servidor SMB

- El servidor SMB puede ser un sistema de NetApp o un sistema distinto de NetApp.
- El servidor de archivos debe permitir que el host de Data broker acceda a las exportaciones.
- Se admiten las versiones 1.0, 2.0, 2.1, 3.0 y 3.11 de SMB.
- Conceda el grupo "Administradores" con permisos "Control total" a las carpetas de origen y destino.

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

## Limitación de SMB para directorios y archivos ocultos

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

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

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

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

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

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

## Permisos para un destino de SnapMirror

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

## Información general sobre redes para Cloud Sync

La conexión de red para Cloud Sync incluye la conectividad entre el agente de datos y las ubicaciones de origen y destino, y una conexión de Internet saliente desde el agente de datos a través del puerto 443.

### Ubicación de agente de datos

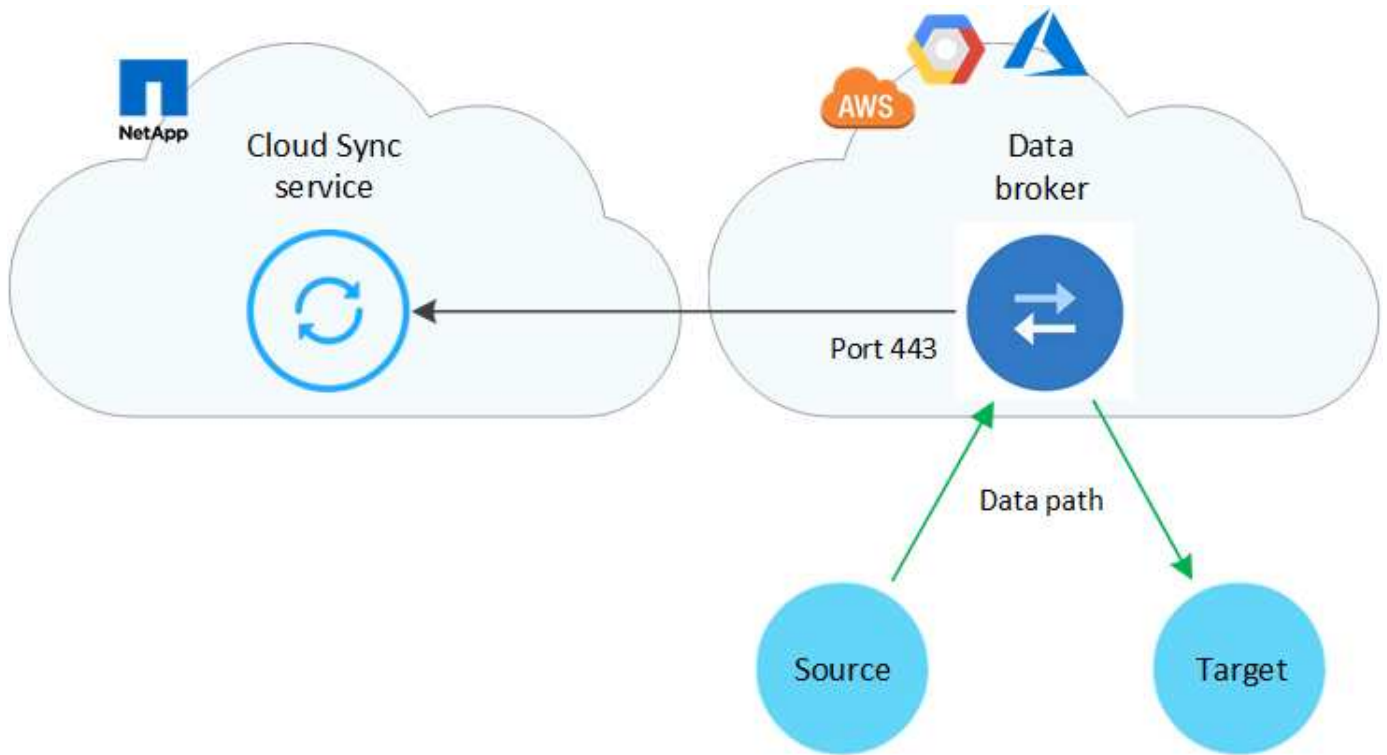
Puede instalar el agente de datos en el cloud o en sus instalaciones.

### Agente de datos en el cloud

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

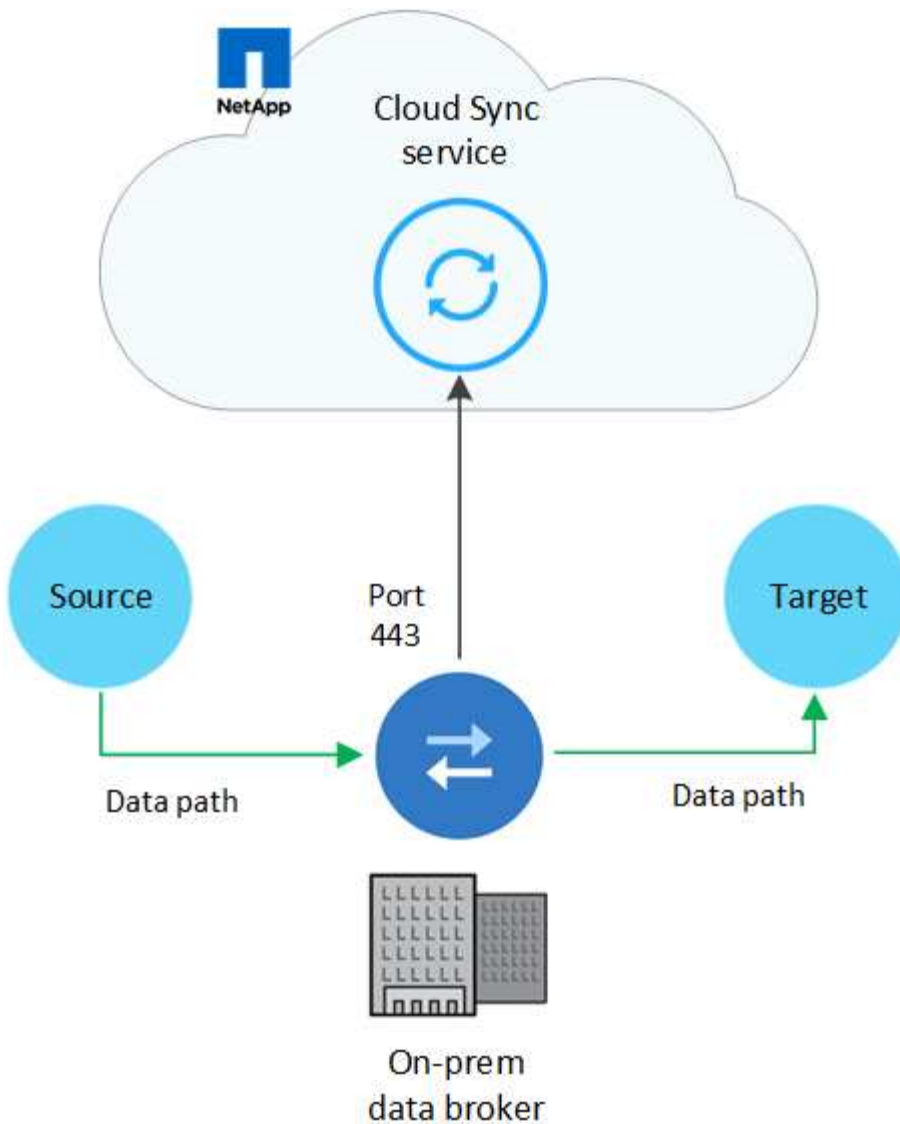


Cuando Cloud Sync implementa el agente de datos en AWS, Azure o GCP, crea un grupo de seguridad que permite las comunicaciones salientes necesarias.



#### Agente de datos en sus instalaciones

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



### Requisitos de red

- El origen y el destino deben tener una conexión de red con el agente de datos.

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

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

### Extremos de red

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

## Extremos de Data broker

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

Puntos finales	Específico
olcentgbl.trafficmanager.net:443	Para ponerse en contacto con un repositorio para actualizar paquetes CentOS para el host de Data broker. Solo se puede contactar con este extremo si instala manualmente el agente de datos en un host CentOS.
rpm.nodesource.com:443 registry.npmjs.org:443 nodejs.org:443	Para ponerse en contacto con repositorios para actualizar los paquetes Node.js, npm y otros paquetes de terceros utilizados en desarrollo.
tgz.pm2.io:443	Para acceder a un repositorio para la actualización de Pm2, que es un paquete de terceros que se utiliza para supervisar Cloud Sync.
sqs.us-east-1.amazonaws.com:443 kinesis.us-east-1.amazonaws.com:443	Para ponerse en contacto con los servicios de AWS que Cloud Sync utiliza en las operaciones (poner en cola archivos, registrar acciones y entregar actualizaciones al agente de datos).
s3.region.amazonaws.com:443 por ejemplo: s3.us-east-2.amazonaws.com:443 <a href="https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region">https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region</a> ["Consulte la documentación de AWS para obtener una lista de extremos de S3"^]	Para ponerse en contacto con Amazon S3 cuando una relación de sincronización incluya un bloque de S3.
cf.cloudsync.netapp.com:443 repo.cloudsync.netapp.com:443	Para ponerse en contacto con el servicio Cloud Sync.
support.netapp.com:443	Para ponerse en contacto con el soporte de NetApp cuando use una licencia BYOL para relaciones de sincronización.
fedoraproject.org:443	Para instalar 7z en la máquina virtual Data Broker durante la instalación y las actualizaciones. Es necesario enviar mensajes de AutoSupport al soporte técnico de NetApp.

## Extremos del navegador web

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

logs.cloudsync.netapp.com:443

## Cómo instalar un agente de datos

### Instalar el agente de datos en AWS

Al crear una relación de sincronización, elija la opción AWS Data Broker para implementar el software de agente de datos en una nueva instancia de EC2 en un VPC. Cloud Sync le guía durante el proceso de instalación, pero en esta página se repiten los requisitos y los pasos que le ayudarán a preparar la instalación.

También tiene la opción de instalar el agente de datos en un host Linux existente en el cloud o en sus

instalaciones. ["Leer más"](#).

### Regiones admitidas de AWS

Todas las regiones están soportadas excepto las regiones China y GovCloud (EE.UU.).

### Requisitos de red

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

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

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

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

### Permisos necesarios para implementar el agente de datos en AWS

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

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

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

El rol del IAM debe cumplir los siguientes requisitos:

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

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

### Instalación del Data broker


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

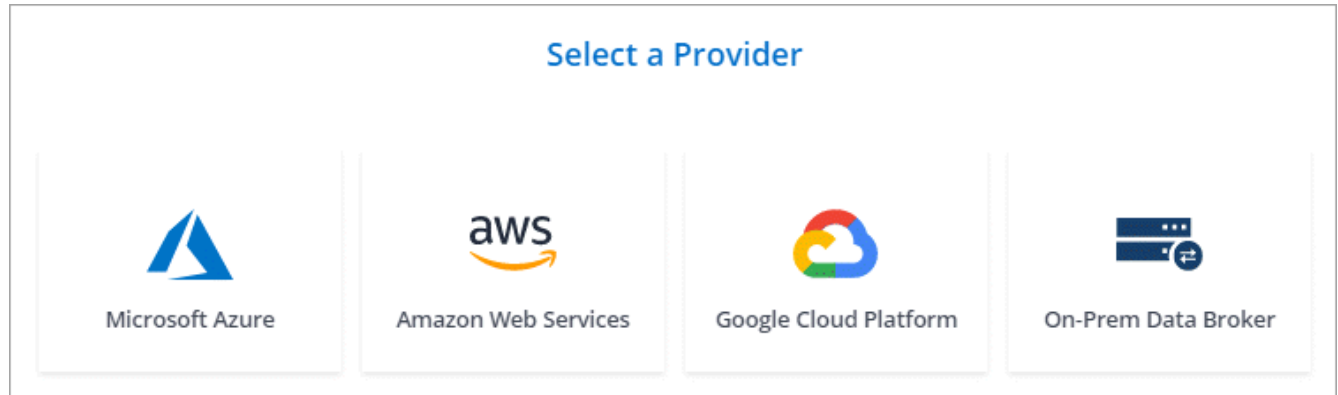
### Pasos

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

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

3. En la página **Data Broker**, haga clic en **Crear Data Broker** y, a continuación, seleccione **Amazon Web Services**.

Si ya tiene un agente de datos, tendrá que hacer clic en el  icono primero.



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

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

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

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

► [https://docs.netapp.com/es-es/occm38//media/video\\_cloud\\_sync.mp4](https://docs.netapp.com/es-es/occm38//media/video_cloud_sync.mp4) (video)

6. Si introdujo una clave de acceso de AWS, seleccione una ubicación para la instancia, seleccione un par de claves, elija si desea habilitar una dirección IP pública y, a continuación, seleccione un rol de IAM existente o deje el campo en blanco para que Cloud Sync cree el rol para usted.

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

### Basic Settings

<p><b>Location</b></p> <p>Region  <input type="text" value="US West   Oregon"/></p> <p>VPC  <input type="text" value="vpc-3c46c059 - 10.60.21.0/25"/></p> <p>Subnet  <input type="text" value="10.60.21.0/25"/></p>	<p><b>Connectivity</b></p> <p>Key Pair  <input type="text" value="newKey"/></p> <p>Enable Public IP?  <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>IAM Role (optional) <span style="float: right;">?</span>  <input type="text"/></p>
---	---

7. Después de que el Data broker esté disponible, haga clic en **continuar** en Cloud Sync.

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

Select a NetApp Data Broker

1 NetApp Data Brokers 🔍

<input checked="" type="checkbox"/>	name		<span style="color: green;">✔ Active</span>
	US West (Oregon) <small>Region</small>	10.60.21.0/25   vpc-3c46c059 <small>VPC</small>	10.60.21.5 <small>Private IP</small>
	us-west-2c <small>Availability Zone</small>	10.60.21.0/25   subnet-e7f526be <small>Subnet</small>	5f5002eecf378e000a560988 <small>Broker ID</small>
		i-0fc5c97e2f5f22c20 <small>Instance ID</small>	

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

### Resultado

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

### Instalar el agente de datos en Azure

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

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



## Regiones de Azure compatibles

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

## Requisitos de red

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

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

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

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

## Método de autenticación

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


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

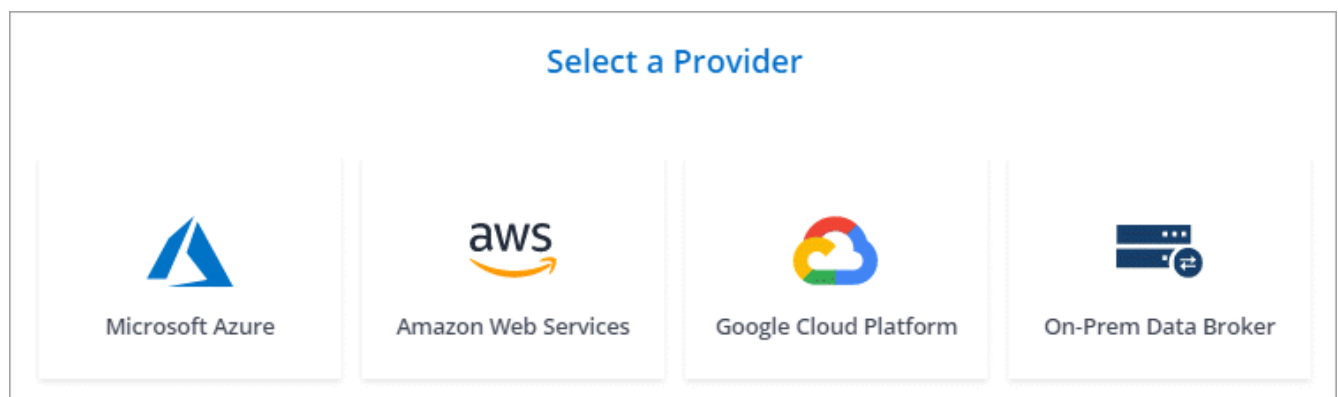
## Instalación del Data broker

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

## Pasos

1. Haga clic en **Crear nueva sincronización**.
2. En la página **definir relación de sincronización**, elija un origen y un destino y haga clic en **continuar**.  
Rellene las páginas hasta que llegue a la página **Data Broker**.
3. En la página **Data Broker**, haga clic en **Crear Data Broker** y, a continuación, seleccione **Microsoft Azure**.

Si ya tiene un agente de datos, tendrá que hacer clic en el  icono primero.



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

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

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

The screenshot shows the configuration page for a virtual machine in the Azure portal. It is divided into two main sections: **Location** and **Virtual Machine**.

**Location Section:**

- Subscription:** A dropdown menu showing "OCCM Dev".
- Azure Region:** A dropdown menu showing "West US 2".
- VNet:** A dropdown menu showing "Vnet1".
- Subnet:** A dropdown menu showing "Subnet1".

**Virtual Machine Section:**

- VM Name:** A text input field containing "netappdatabroker".
- User Name:** A text input field containing "databroker".
- Authentication Method:** Two radio buttons: "Password" (selected) and "Public Key".
- Enter Password:** A text input field with masked characters (dots).
- Resource Group:** Two radio buttons: "Generate a new group" (selected) and "Use an existing group".

- Haga clic en **continuar** y mantenga la página abierta hasta que finalice la implementación.

El proceso puede tardar hasta 7 minutos.

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

## Resultado

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

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

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

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

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

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

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

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

### Instalación del agente de datos en Google Cloud Platform

Al crear una relación de sincronización, elija la opción GCP Data Broker para implementar el software de broker de datos en una nueva instancia de máquina virtual en un VPC. Cloud Sync le guía durante el proceso de instalación, pero en esta página se repiten los requisitos y los pasos que le ayudarán a preparar la instalación.

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

#### Regiones compatibles de GCP

Se admiten todas las regiones.

#### Requisitos de red

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

Cuando Cloud Sync implementa el intermediario de datos en GCP, crea un grupo de seguridad que habilita la comunicación saliente necesaria.

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

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

## Permisos necesarios para desplegar el agente de datos en GCP

Asegúrese de que el usuario de GCP que despliega el intermediario de datos tiene los siguientes permisos:

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

## Permisos necesarios para la cuenta de servicio

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

- `logging.logEntries.create`
- `resourcemanager.projects.get`
- `storage.buckets.get`
- `storage.buckets.list`
- `storage.objects.*`

## Instalación del Data broker


Puede instalar un intermediario de datos en GCP cuando cree una relación de sincronización.

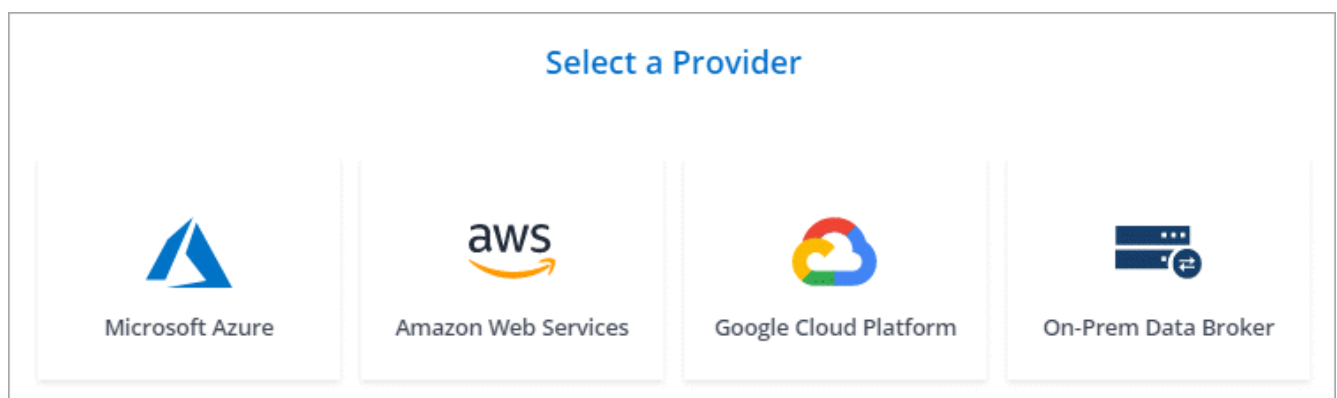
### Pasos

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

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

3. En la página **Data Broker**, haga clic en **Crear Data Broker** y seleccione **Google Cloud Platform**.

Si ya tiene un agente de datos, tendrá que hacer clic en el  icono primero.



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

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

- Seleccione un proyecto y una cuenta de servicio y, a continuación, elija una ubicación para el agente de datos.

### Basic Settings

<b>Project</b>	<b>Location</b>
Project <input type="text" value="OCCM-Dev"/>	Region <input type="text" value="us-west1"/>
Service Account <input type="text" value="test"/>	Zone <input type="text" value="us-west1-a"/>
Select a Service Account that includes <a href="#">these permissions</a>	VPC <input type="text" value="default"/>
	Subnet <input type="text" value="default"/>

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

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

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

## Resultado

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

## Instalar el agente de datos en un host Linux

Al crear una relación de sincronización, elija la opción de Data Broker en las instalaciones para instalar el software de agente de datos en un host Linux local o en un host Linux existente en el cloud. Cloud Sync le guía durante el proceso de instalación, pero en esta página se repiten los requisitos y los pasos que le ayudarán a preparar la instalación.

## Requisitos del host Linux

- **sistema operativo:**
  - CentOS 7.0, 7.7 y 8.0
  - Red Hat Enterprise Linux 7.7 y 8.0
  - Sistema operativo Ubuntu Server 18.04 LTS
  - SUSE Linux Enterprise Server 15 SP1

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

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

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

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

- **OpenSSL:** Debe estar instalado en el host Linux.

## Requisitos de red

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

## Habilitar el acceso a AWS

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

## Pasos

1. Cree una política de IAM mediante ["Esta política proporcionada por NetApp"](#). ["Consulte las instrucciones de AWS"](#).
2. Cree un usuario IAM con acceso mediante programación. ["Consulte las instrucciones de AWS"](#).

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

## Habilitar el acceso a Google Cloud

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

### Pasos

1. Cree una cuenta de servicio de GCP que tenga permisos de administrador de almacenamiento, si aún no tiene una.
2. Cree una clave de cuenta de servicio guardada en formato JSON. "[Vea las instrucciones de GCP](#)".

El archivo debe contener al menos las siguientes propiedades: "Project\_id", "private\_key" y "client\_email"



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

3. Guarde el archivo JSON en el host Linux.

## Habilitar el acceso a Microsoft Azure

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

### Instalación del Data broker

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

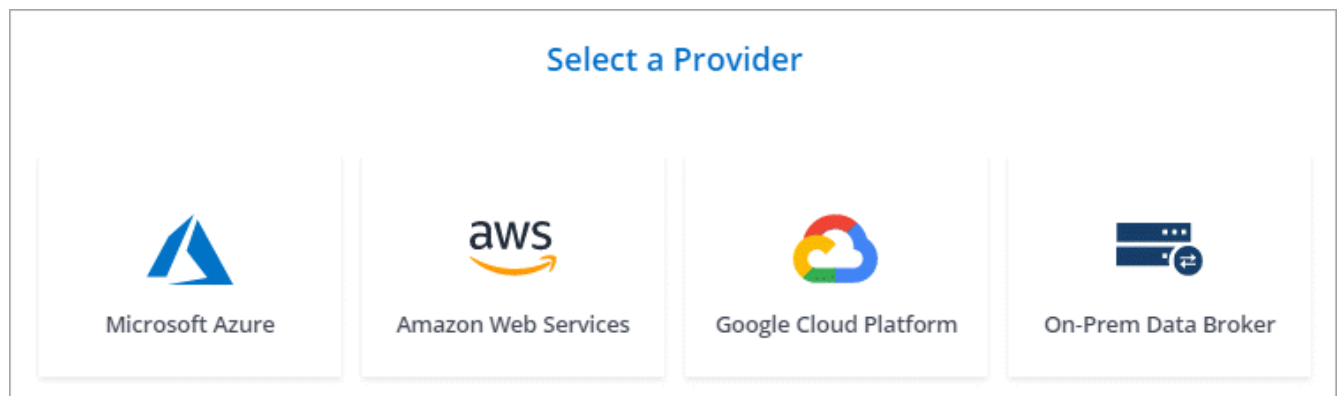
### Pasos

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

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

3. En la página **Data Broker**, haga clic en **Crear Data Broker** y, a continuación, seleccione **On-Prem Data Broker**.

Si ya tiene un agente de datos, tendrá que hacer clic en el icono primero.



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

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

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

5. En la página de instrucciones:

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

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

d. Descargue el instalador:

- Sin proxy:

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

- Usar servidor proxy:

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

- Utilice el servidor proxy con autenticación:

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

### URI

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

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



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

- Sin configuración de proxy:

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

- Configuración de proxy:

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



```
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port>
```

- Configuración del proxy con autenticación:

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

### Claves de AWS

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

### Archivo JSON

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

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

## Creación de una relación de sincronización

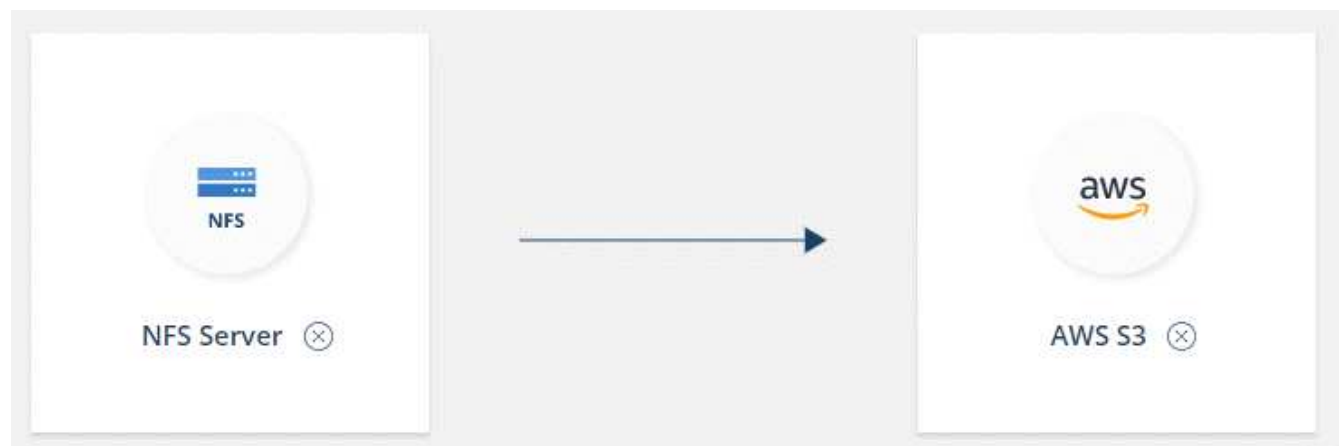
Al crear una relación de sincronización, el servicio Cloud Sync copia los archivos del origen al destino. Después de la copia inicial, el servicio sincroniza los datos modificados cada 24 horas.

Los siguientes pasos proporcionan un ejemplo que muestra cómo configurar una relación de sincronización desde un servidor NFS a un bloque de S3.

### Pasos

1. En Cloud Manager, haga clic en **sincronización**.
2. En la página **definir relación de sincronización**, elija un origen y un destino.

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



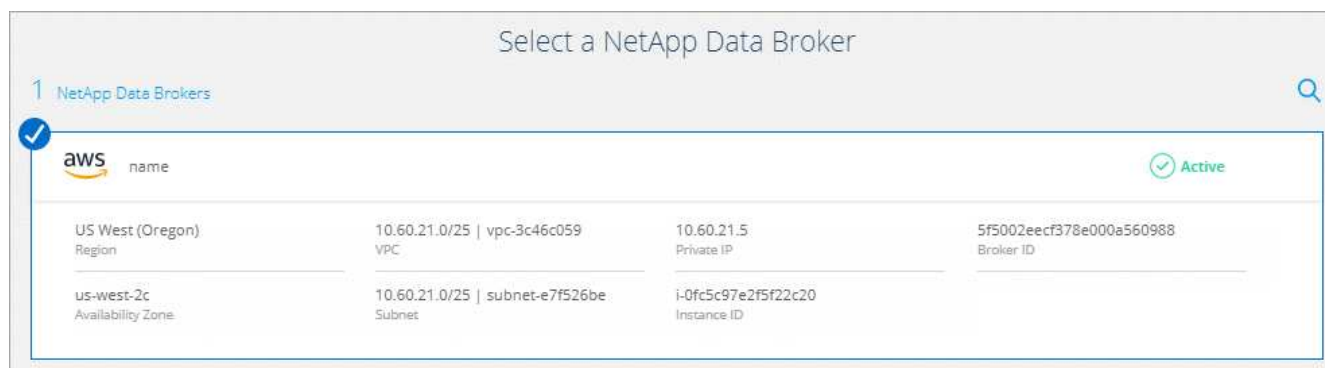
3. En la página **servidor NFS**, introduzca la dirección IP o el nombre de dominio completo del servidor NFS que desea sincronizar con AWS.
4. En la página **Data Broker**, siga las indicaciones para crear una máquina virtual de Data Broker en AWS, Azure o Google Cloud Platform, o para instalar el software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

Para obtener más información, consulte las siguientes páginas:

- ["Instalar el agente de datos en AWS"](#)
- ["Instalar el agente de datos en Azure"](#)
- ["Instalación del agente de datos en GCP"](#)
- ["Instalar el agente de datos en un host Linux"](#)

5. Después de instalar el Data broker, haga clic en **continuar**.

La siguiente imagen muestra un agente de datos implementado correctamente en AWS:



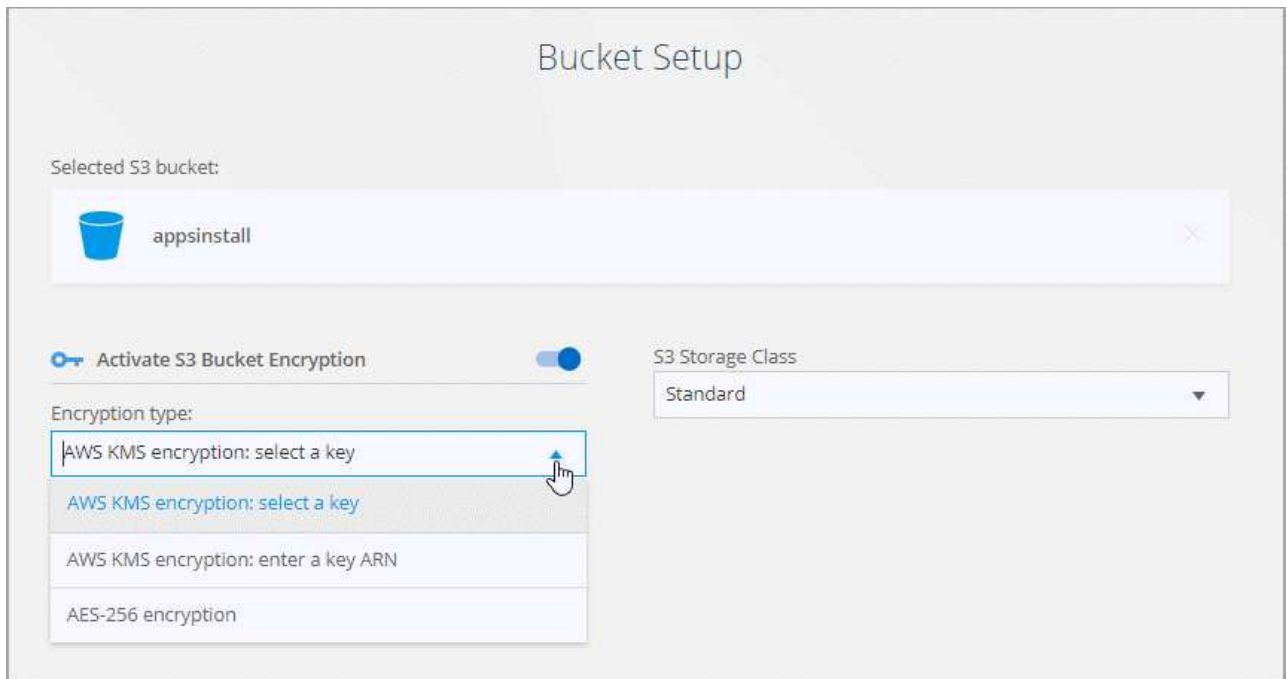
6. en la página **directorios**, seleccione un directorio o subdirectorio de nivel superior.

Si Cloud Sync no puede recuperar las exportaciones, haga clic en **Agregar exportación manualmente** e introduzca el nombre de una exportación NFS.



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

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



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

### Programación

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

### Reintentos

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

### Archivos modificados recientemente

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

### Eliminar archivos en el origen

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

Si habilita esta opción, también debe cambiar un parámetro en el archivo local.json del agente de datos. Abra el archivo y cambie el parámetro denominado *workers.transferrer.delete-on-source* a **TRUE**.

### Eliminar archivos en destino

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

### Etiquetado de objetos

Cuando AWS S3 es el destino de una relación de sincronización, Cloud Sync etiqueta objetos de S3 con metadatos relevantes para la operación de sincronización. Puede deshabilitar el etiquetado de objetos S3 si no se desea en el entorno. Cloud Sync no afecta si deshabilita el etiquetado: Cloud Sync solo almacena los metadatos de sincronización de una manera diferente.

## Tipos de archivo

Defina los tipos de archivo que se van a incluir en cada sincronización: Archivos, directorios y enlaces simbólicos.

## Excluir extensiones de archivo

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

► [https://docs.netapp.com/es-es/occm38//media/video\\_file\\_extensions.mp4](https://docs.netapp.com/es-es/occm38//media/video_file_extensions.mp4) (video)

## Tamaño de archivo

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

## Fecha de modificación

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

10. En la página **etiquetas de relación**, introduzca hasta 9 etiquetas de relación y, a continuación, haga clic en **continuar**.

El servicio Cloud Sync asigna las etiquetas a cada objeto que se sincroniza con el bloque de S3.

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

## resultado

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

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

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

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

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

### ¿Qué pasa si no 8217 pago inmediatamente después de que finalice mi prueba gratuita?

No podrá crear relaciones adicionales. Las relaciones existentes no se eliminan, pero no puede realizar ningún cambio hasta que se suscriba o introduzca una licencia.

## Suscribirse a AWS

AWS le permite pagar anualmente.

### De pago por uso

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

El siguiente vídeo muestra el proceso:

► [https://docs.netapp.com/es-es/occm38//media/video\\_cloud\\_sync\\_registering.mp4](https://docs.netapp.com/es-es/occm38//media/video_cloud_sync_registering.mp4) (video)

### Pasos a pagar anualmente

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

## suscribirse de Azure

Azure le permite pagar por uso o anualmente.

### Lo que necesitará

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

### Pasos

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

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

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

El siguiente vídeo muestra el proceso:

► [https://docs.netapp.com/es-es/occm38//media/video\\_cloud\\_sync\\_registering\\_azure.mp4](https://docs.netapp.com/es-es/occm38//media/video_cloud_sync_registering_azure.mp4) (video)

## Compra de licencias de NetApp y añadirlas a Cloud Sync

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

### Pasos

1. Adquiera una licencia por correo electrónico:ng-cloudsync-contact@netapp.com?Subject=Cloud%20Sync%20Service%20-%20BYOL%20Licencia%20Compra%20Solicite[Contacto con NetApp].
2. En Cloud Manager, haga clic en **sincronización > licencias**.
3. Haga clic en **Agregar licencia** y agregue la licencia.

## Tutoriales

### Copiar ACL entre recursos compartidos de SMB

Cloud Sync puede copiar listas de control de acceso (ACL) entre un recurso compartido de SMB de origen y un recurso compartido de SMB de destino. Si es necesario, puede conservar manualmente las ACL usted mismo mediante robocopy.

#### Opciones

- [Configure Cloud Sync para que copie automáticamente las ACL](#)
- [Copie manualmente las ACL usted mismo](#)

### Configurar Cloud Sync para copiar ACL entre servidores SMB

Copiar ACL entre servidores de SMB habilitando una configuración cuando se crea una relación o después de crear una relación.

Tenga en cuenta que esta función está disponible para las nuevas relaciones de sincronización creadas después de la versión 23 de febrero de 2020. Si desea utilizar esta característica con relaciones existentes creadas antes de esa fecha, deberá volver a crear la relación.

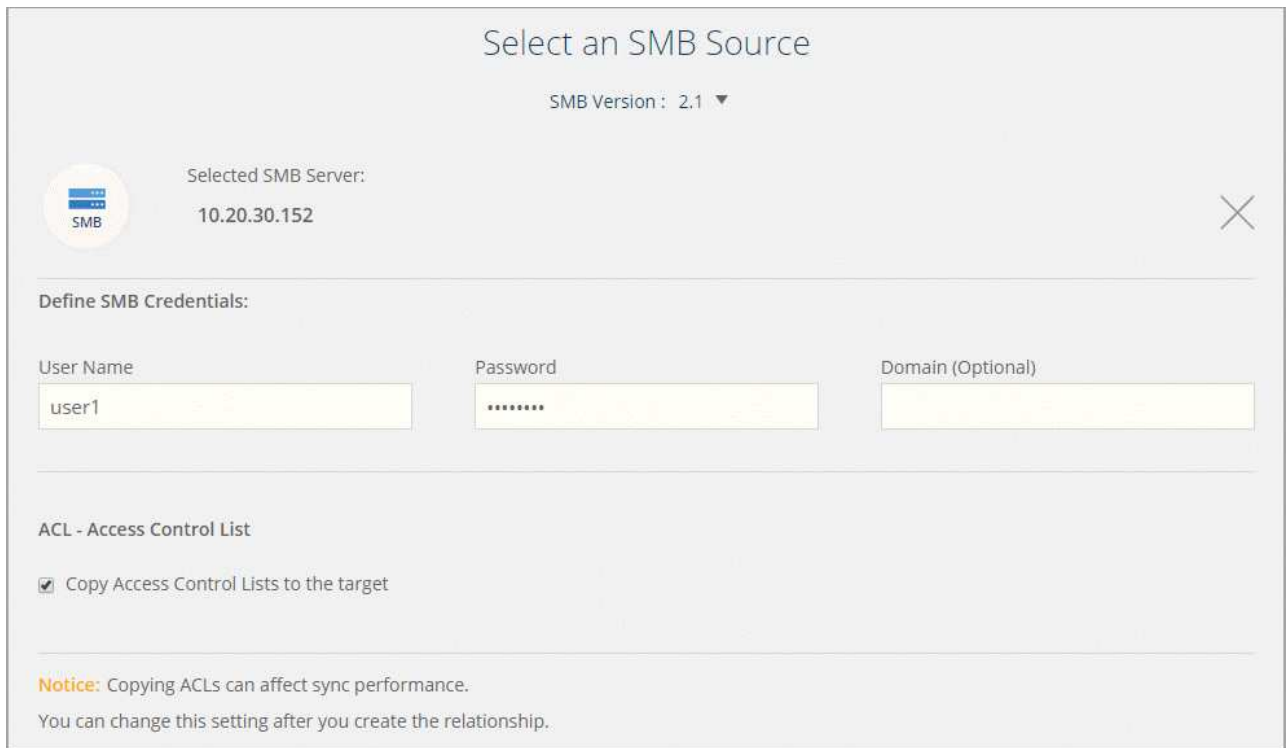
#### Lo que necesitará

- Una nueva relación de sincronización o una relación de sincronización existente creada después de la versión del 23 de febrero de 2020.
- Cualquier tipo de agente de datos.

Esta función funciona con *any* type de agente de datos: AWS, Azure, Google Cloud Platform o agente de datos en las instalaciones. Se puede ejecutar el agente de datos en las instalaciones "[cualquier sistema operativo compatible](#)".

#### Pasos para una nueva relación

1. En Cloud Sync, haga clic en **Crear nueva sincronización**.
2. Arrastre y suelte **SMB Server** al origen y al destino y haga clic en **continuar**.
3. En la página **SMB Server**:
  - a. Introduzca un nuevo servidor SMB o seleccione un servidor existente y haga clic en **continuar**.
  - b. Introduzca credenciales para el servidor SMB.
  - c. Seleccione **Copiar listas de control de acceso al destino** y haga clic en **continuar**.



Select an SMB Source

SMB Version: 2.1 ▼

Selected SMB Server: 10.20.30.152

Define SMB Credentials:

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

ACL - Access Control List

Copy Access Control Lists to the target

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

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

### Pasos para una relación existente

1. Pase el ratón por la relación de sincronización y haga clic en el menú de acción.
2. Haga clic en **Configuración**.
3. Seleccione **Copiar listas de control de acceso al destino**.
4. Haga clic en **Guardar configuración**.

### Resultado

Al sincronizar datos, Cloud Sync conserva las ACL entre los recursos compartidos de SMB de origen y de destino.

### Copia manual de ACL

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

### Pasos

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

Debe realizar este paso antes de utilizar robocopy.

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

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

Se deben especificar tanto *source* como *target* con el formato UNC. Por ejemplo: \\<servidor>\<recurso compartido>\<ruta>

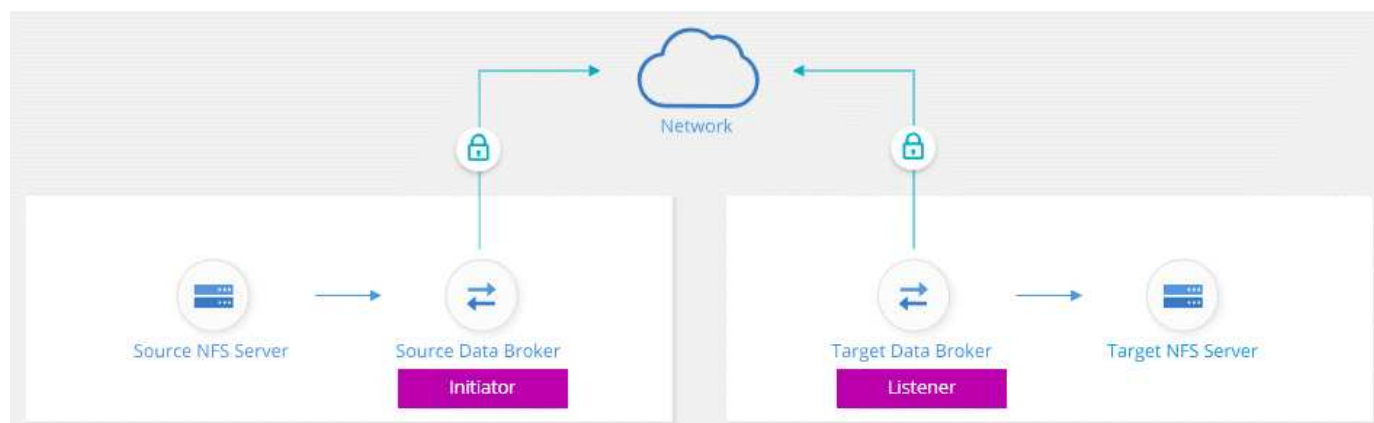
## Sincronizando los datos NFS mediante el cifrado de datos en tránsito

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

Por ejemplo, se recomienda sincronizar datos entre dos servidores NFS que se encuentran en redes diferentes. O puede que necesite transferir datos de Azure NetApp Files de manera segura en subredes o regiones.

### Cómo funciona el cifrado de datos en tiempo real

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



Un agente de datos funciona como el *initiator*. Cuando es hora de sincronizar datos, envía una solicitud de conexión al otro intermediario de datos, que es el *listener*. Ese agente de datos escucha las solicitudes en el puerto 443. Puede utilizar un puerto diferente, si es necesario, pero asegúrese de comprobar que el puerto no está en uso por otro servicio.

Por ejemplo, si sincroniza datos de un servidor NFS local con un servidor NFS basado en cloud, puede elegir el agente de datos que escucha las solicitudes de conexión y que las envía.

Así es como funciona el cifrado en tránsito:

1. Después de crear la relación de sincronización, el iniciador inicia una conexión cifrada con el otro agente de datos.
2. El agente de datos de origen cifra los datos del origen mediante TLS 1.3.
3. A continuación, envía los datos a través de la red al agente de datos de destino.
4. El agente de datos de destino descifra los datos antes de enviarlos al destino.



- Después de la copia inicial, el servicio sincroniza los datos modificados cada 24 horas. Si hay datos que sincronizar, el proceso comienza con el iniciador abriendo una conexión cifrada con el otro agente de datos.

Si prefiere sincronizar datos con mayor frecuencia, ["se puede cambiar la programación después de crear la relación"](#).

### Versiones NFS compatibles

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

### Lo que necesitará para comenzar

No olvide disponer de lo siguiente:

- Dos servidores NFS que cumplen ["requisitos de origen y objetivo"](#) O Azure NetApp Files en dos subredes o regiones.
- Las direcciones IP o los nombres de dominio completos de los servidores.
- Ubicaciones de red para dos agentes de datos.

Puede seleccionar un agente de datos existente pero debe funcionar como iniciador. El agente de datos del listener debe ser un agente de datos *new*.

Si aún no ha implementado un agente de datos, revise los requisitos de Data Broker. Debido a que tiene directivas de seguridad estrictas, asegúrese de revisar los requisitos de red, que incluyen tráfico saliente desde el puerto 443 y el ["puntos finales de internet"](#) que el agente de datos se pone en contacto con.

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

### Sincronizando los datos NFS mediante el cifrado de datos en tránsito

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

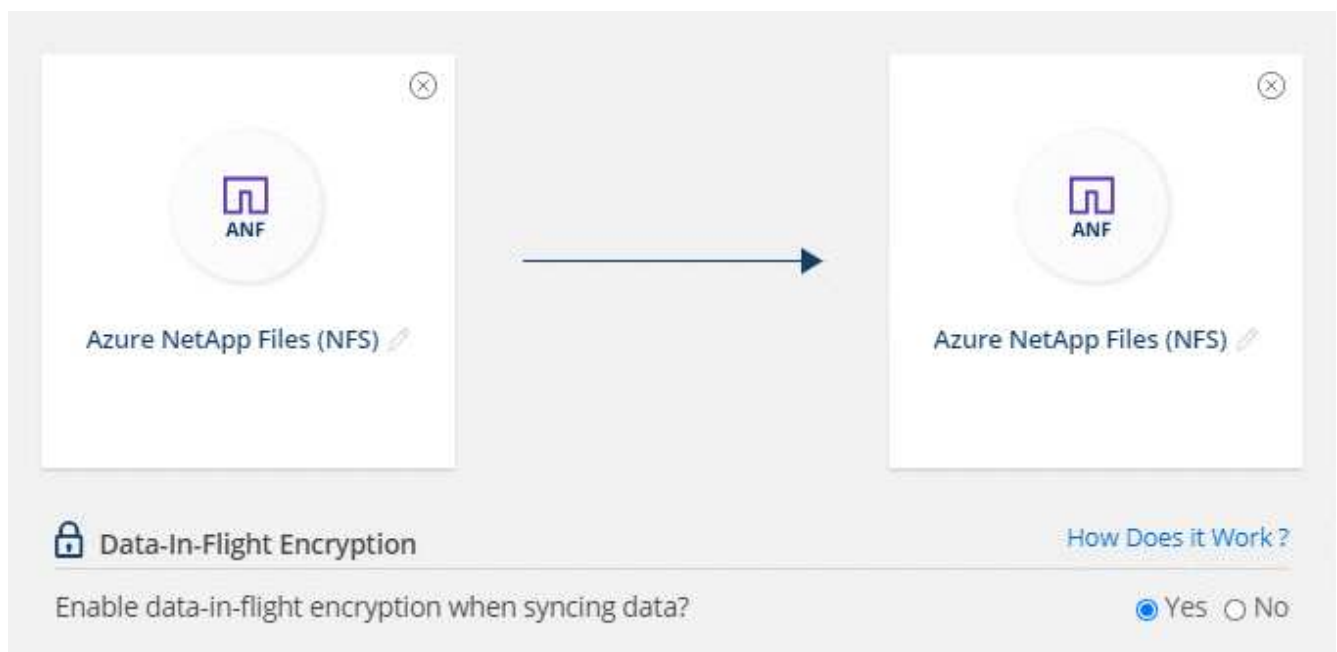
#### Pasos

- Haga clic en **Crear nueva sincronización**.
- Arrastre y suelte **servidor NFS** a las ubicaciones de origen y destino o **Azure NetApp Files** a las ubicaciones de origen y destino y seleccione **Sí** para activar el cifrado de datos en vuelo.

En la siguiente imagen se muestra lo que seleccionaría para sincronizar datos entre dos servidores NFS:



La siguiente imagen muestra lo que seleccionaría para sincronizar datos entre Azure NetApp Files:



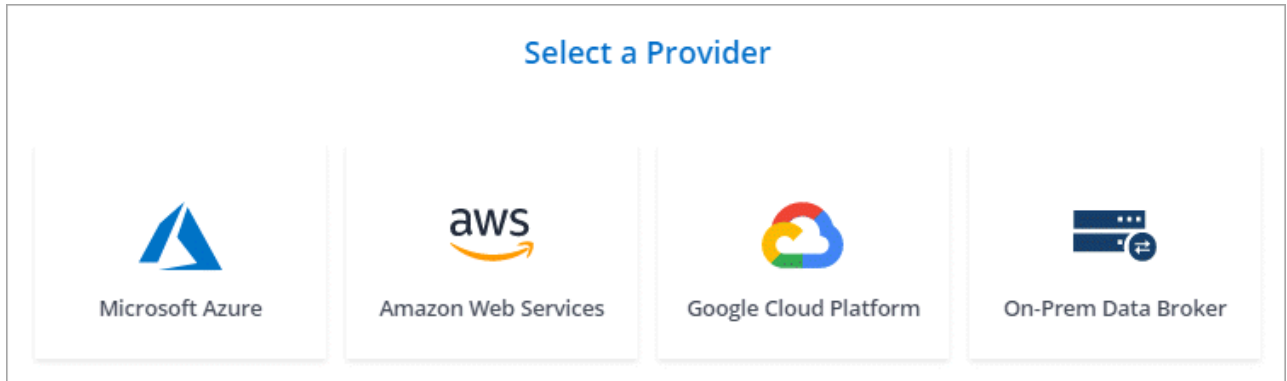
3. Siga las indicaciones para crear la relación:

- NFS Server/Azure NetApp Files:** Elija la versión NFS y, a continuación, especifique un nuevo origen NFS o seleccione un servidor existente.
- definir la funcionalidad de Data Broker:** Defina qué intermediario de datos *escucha* las solicitudes de conexión de un puerto y cuál *inicia* la conexión. Elija en función de sus requisitos de red.
- Data Broker:** Siga las indicaciones para agregar un nuevo intermediario de datos de origen o seleccionar un intermediario de datos existente.

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

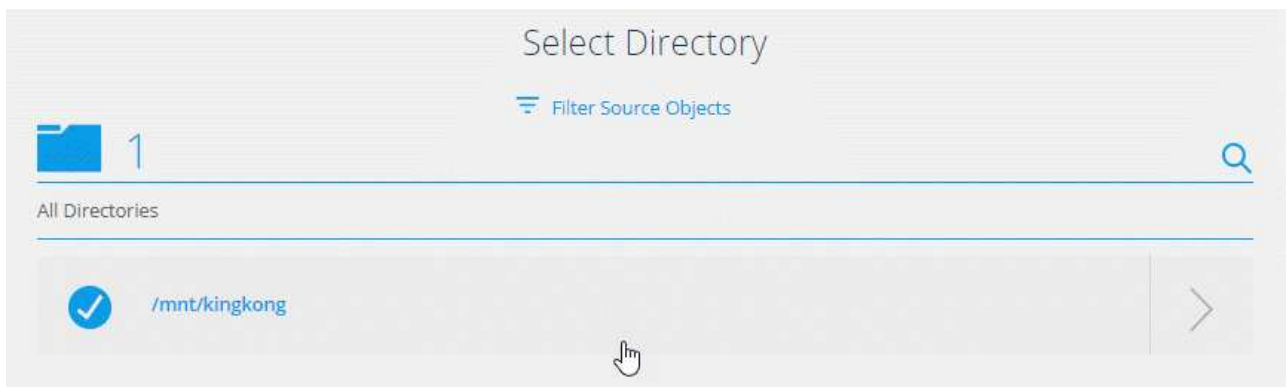
Si necesita un nuevo agente de datos, Cloud Sync le pedirá las instrucciones de instalación. Puede

desplegar el agente de datos en el cloud o descargar un script de instalación para su propio host Linux.



- d. **directorios:** Elija los directorios que desea sincronizar seleccionando todos los directorios, o taladrando y seleccionando un subdirectorio.

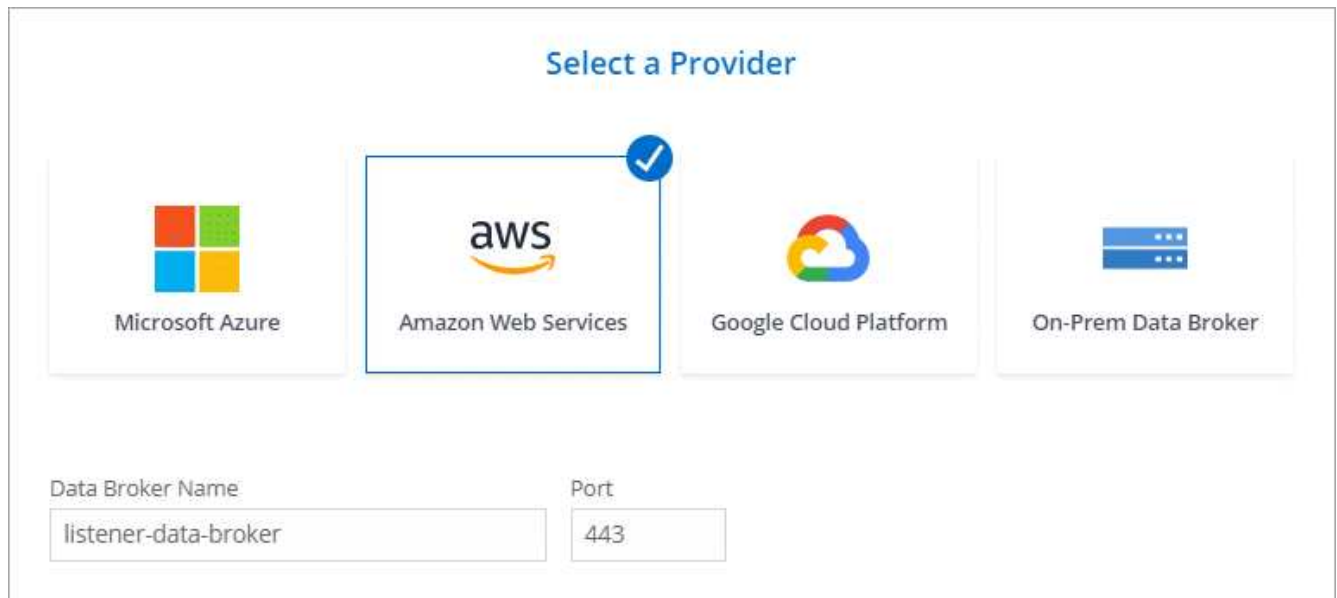
Haga clic en **Filtrar objetos de origen** para modificar la configuración que define cómo se sincronizan y mantienen los archivos y carpetas de origen en la ubicación de destino.



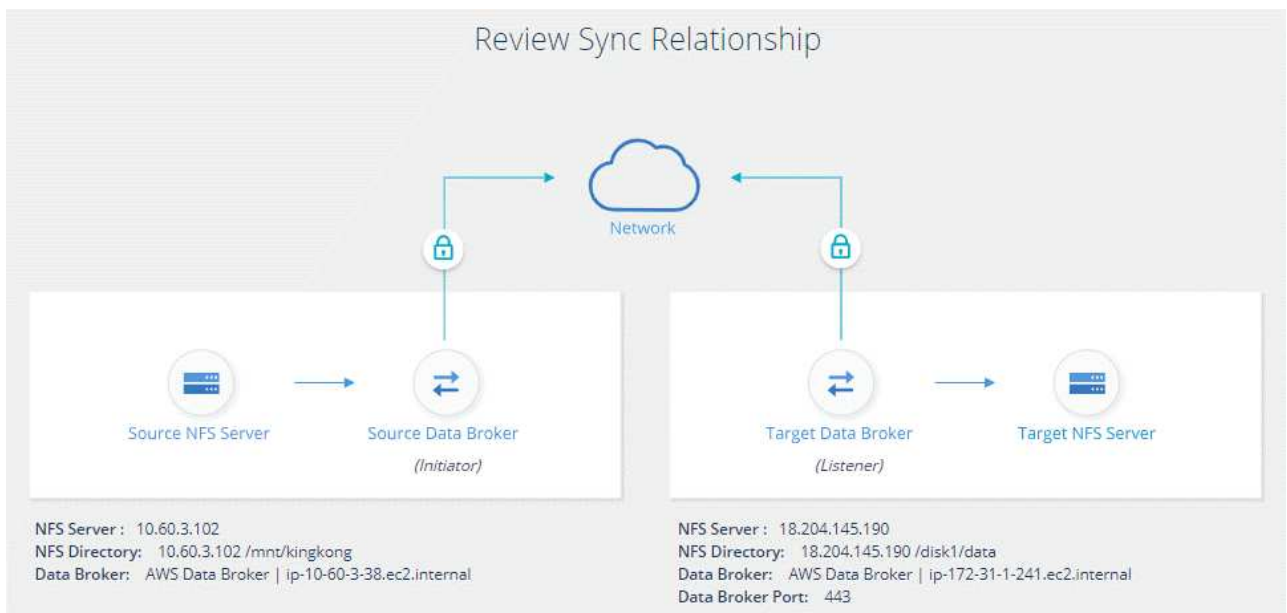
- e. **servidor NFS de destino/Azure NetApp Files de destino:** Elija la versión NFS y, a continuación, introduzca un destino NFS nuevo o seleccione un servidor existente.
- f. **Target Data Broker:** Siga las indicaciones para agregar un nuevo intermediario de datos de origen o seleccionar un intermediario de datos existente.

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

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



- directorios de destino:** Seleccione un directorio de nivel superior o examine para seleccionar un subdirectorio existente o crear una nueva carpeta dentro de una exportación.
- Configuración:** Defina cómo se sincronizan y mantienen los archivos y carpetas de origen en la ubicación de destino.
- Revisión:** Revise los detalles de la relación de sincronización y haga clic en **Crear relación**.



## Resultado

Cloud Sync comienza a crear la nueva relación de sincronización. Cuando haya terminado, haga clic en **Ver en Panel** para ver detalles sobre la nueva relación.

## Gestión de relaciones de sincronización

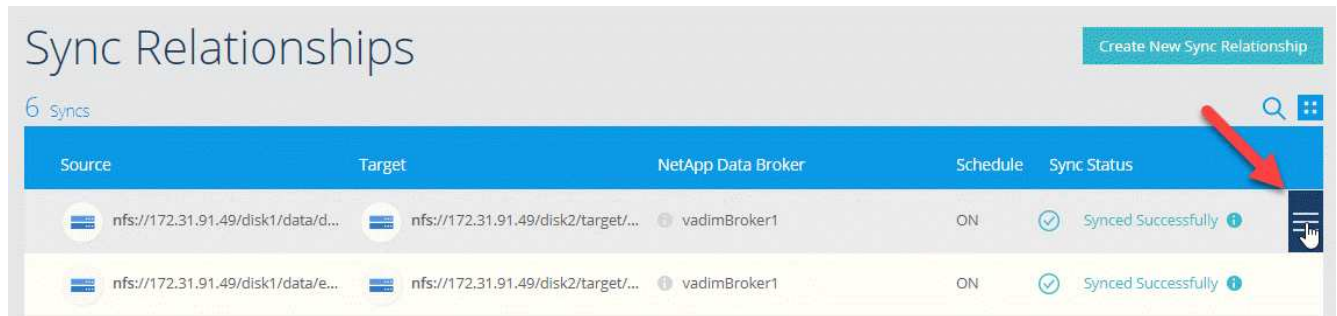
Puede gestionar las relaciones de sincronización en cualquier momento sincronizando de forma inmediata datos, cambiando programaciones y mucho más.

## Realizar una sincronización inmediata de datos

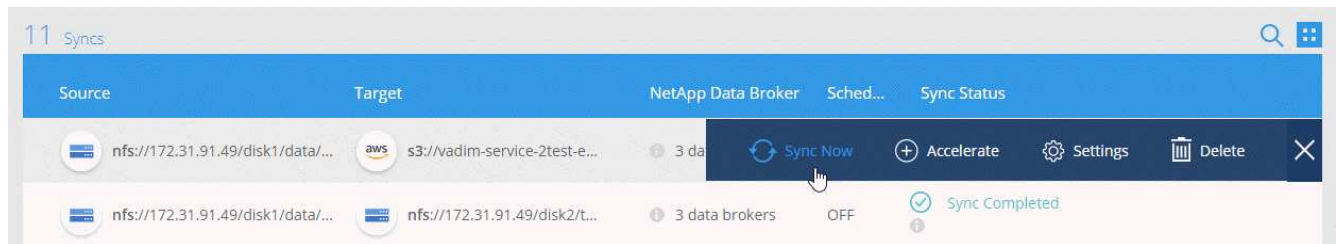
En lugar de esperar a la siguiente sincronización programada, puede pulsar un botón para sincronizar inmediatamente los datos entre la fuente y el destino.

### Pasos

1. En **Consola de sincronización**, pase el ratón sobre la relación de sincronización y haga clic en el menú de acciones.



2. Haga clic en **Sincronizar ahora** y, a continuación, en **Sincronizar** para confirmar.



### Resultado

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

## Acelerando el rendimiento de la sincronización

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

### Cómo funciona

Si los agentes de datos existentes en la relación se utilizan en otras relaciones de sincronización, Cloud Sync agrega automáticamente el nuevo agente de datos a dichas relaciones.

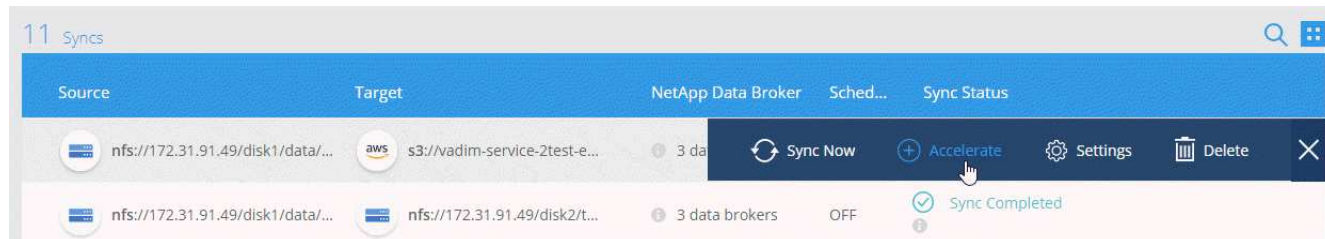
Por ejemplo, digamos que usted tiene tres relaciones:

- La relación 1 utiliza el agente DE datos A
- La relación 2 utiliza Data broker B
- La relación 3 utiliza Data broker A

Desea acelerar el rendimiento de la relación 1 para agregar un nuevo agente de datos a dicha relación (agente de datos C). Debido a que el agente DE datos A también se utiliza en la relación 3, el nuevo agente de datos también se agrega automáticamente a la relación 3.

### Pasos

1. Asegúrese de que al menos uno de los agentes de datos existentes en la relación esté en línea.
2. Pase el ratón por la relación de sincronización y haga clic en el menú de acción.
3. Haga clic en **acelerar**.



4. Siga las indicaciones para crear un nuevo Data broker.

### Resultado

Cloud Sync agrega el nuevo agente de datos a las relaciones de sincronización. Es necesario acelerar el rendimiento de la siguiente sincronización de datos.

### Cambiar la configuración de una relación de sincronización

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

1. Pase el ratón por la relación de sincronización y haga clic en el menú de acción.
2. Haga clic en **Configuración**.
3. Modifique cualquiera de los ajustes.

**General**

Schedule	ON   Every 1 Day	▼
Retries	Retry 3 times before skipping file	▼

**Files and Directories**

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	▼
Object Tagging	Allow Cloud Sync to tag S3 objects	▼
File Types	Include All: Files, Directories, Symbolic Links	▼
Exclude File Extensions	None	▼
File Size	All	▼
Date Modified	All	▼

[Reset to defaults](#)

aquí hay una breve descripción de cada configuración:

### Programación

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

### Reintentos

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

### Archivos modificados recientemente

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

### Eliminar archivos en el origen

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

Si habilita esta opción, también debe cambiar un parámetro en el archivo local.json del agente de datos. Abra el archivo y cambie el parámetro denominado *workers.transferrer.delete-on-source* a **TRUE**.

### Eliminar archivos en destino

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

### Etiquetado de objetos

Cuando AWS S3 es el destino de una relación de sincronización, Cloud Sync etiqueta objetos de S3 con metadatos relevantes para la operación de sincronización. Puede deshabilitar el etiquetado de objetos S3 si no se desea en el entorno. Cloud Sync no afecta si deshabilita el etiquetado: Cloud Sync solo almacena los metadatos de sincronización de una manera diferente.

### Tipos de archivo

Defina los tipos de archivo que se van a incluir en cada sincronización: Archivos, directorios y enlaces simbólicos.

### Excluir extensiones de archivo

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

► [https://docs.netapp.com/es-es/occm38//media/video\\_file\\_extensions.mp4](https://docs.netapp.com/es-es/occm38//media/video_file_extensions.mp4) (video)

### Tamaño de archivo

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

### Fecha de modificación

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

### Copiar listas de control de acceso en el destino

Opción de copiar listas de control de acceso (ACL) entre los recursos compartidos de SMB de origen y los recursos compartidos de SMB de destino. Tenga en cuenta que esta opción solo está disponible para relaciones de sincronización creadas después de la versión 23 de febrero de 2020.

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

### Resultado

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

## Eliminar relaciones

Puede eliminar una relación de sincronización si ya no necesita sincronizar datos entre el origen y el destino. Esta acción no elimina la instancia de Data broker y no elimina los datos del destino.

### Pasos

1. Pase el ratón por la relación de sincronización y haga clic en el menú de acción.
2. Haga clic en **Eliminar** y, a continuación, vuelva a hacer clic en **Eliminar** para confirmar.



## Resultado

Cloud Sync elimina la relación de sincronización.

# API de Cloud Sync

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

## Primeros pasos

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

### Pasos

1. Obtenga un token de usuario de Cloud Central de NetApp.

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

2. Obtenga su ID de cuenta de Cloud Central.

```
GET https://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 identificador de usuario y el ID de cuenta en el encabezado de autorización de cada llamada de API.

### ejemplo

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

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

## ¿Qué debo hacer cuando caduca el token?

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

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

## Referencia de API

Es posible acceder a la documentación para cada API de Cloud Sync en "[Cloud Central de NetApp](#)".

## Uso de list API

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

### Pasos

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

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

### ejemplo

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

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

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

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

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

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

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

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

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

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

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

## Preguntas técnicas frecuentes sobre Cloud Sync

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

### Primeros pasos

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

#### ¿Cómo funciona Cloud Sync?

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

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

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

establecido.

## ¿Cómo funciona la prueba gratuita de 14 días?

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

## ¿Cuánto cuesta Cloud Sync?

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

### **cargos por servicio**

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

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

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

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

### **gastos de recursos**

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

## ¿Cómo se factura Cloud Sync?

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

## ¿Puedo usar Cloud Sync fuera del cloud?

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

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

- Para la sincronización en las instalaciones, hay un bloque de Amazon S3 privado disponible a través de StorageGRID de NetApp.
- El agente de datos necesita una conexión a Internet para comunicarse con el servicio Cloud Sync.
- Si no adquiere una licencia directamente a NetApp, necesitará una cuenta de AWS o Azure para la facturación del servicio de PAYGO Cloud Sync.

## ¿Cómo puedo acceder a Cloud Sync?

Cloud Sync está disponible en Cloud Manager en la ficha **sincronización**.

## Orígenes y objetivos compatibles

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

### ¿Qué orígenes y destinos es compatible con Cloud Sync?

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

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

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

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

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

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

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

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

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

- Almacenamiento en caliente
- Almacenamiento en frío

## Redes

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

### ¿Cuáles son los requisitos de red de Cloud Sync?

El entorno de Cloud Sync requiere que el agente de datos esté conectado al origen y al destino a través del protocolo seleccionado (NFS, SMB, EFS) o de la API de almacenamiento de objetos (Amazon S3, Azure Blob, IBM Cloud Object Storage).

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

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

## ¿Existen limitaciones de red relacionadas con la conectividad de Data broker?

Los agentes de datos requieren acceso a Internet. No ofrecemos compatibilidad con un servidor proxy cuando implantamos el agente de datos en Azure o Google Cloud Platform.

## Sincronización de datos

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

### ¿con qué frecuencia se produce la sincronización?

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

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

### ¿Cuál es el programa de sincronización mínimo?

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

### ¿vuelve a intentar el agente de datos cuando un archivo no se puede sincronizar? ¿o se agote el tiempo de espera?

El agente de datos no se agotó cuando un único archivo no se transfiere. En su lugar, el agente de datos reintenta 3 veces antes de omitir el archivo. El valor de reintento se puede configurar en la configuración de una relación de sincronización.

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

### ¿y si tengo un conjunto de datos muy grande?

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

## Seguridad

Las siguientes preguntas están relacionadas con la seguridad.

### ¿es Cloud Sync seguro?

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

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

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

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

Cualquiera de estos métodos establece una conexión segura entre los servidores NAS locales y un agente de datos Cloud Sync.

### ¿los datos están cifrados por Cloud Sync?

- Cloud Sync admite el cifrado de datos en tiempo real entre los servidores NFS de origen y de destino. ["Leer más"](#).
- SMB no es compatible con el cifrado.
- Cuando un bloque de Amazon S3 es el destino de una relación de sincronización, puede elegir si habilitar el cifrado de datos mediante el cifrado AWS KMS o el cifrado AES-256.

## Permisos

Las siguientes preguntas se refieren a los permisos de datos.

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

Es posible configurar Cloud Sync para que se conserven las listas de control de acceso (ACL) entre un recurso compartido de SMB de origen y un recurso compartido de SMB de destino. También puede copiar manualmente las ACL usted mismo. ["Aprenda a copiar ACL entre recursos compartidos de SMB"](#).

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

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

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

## Rendimiento

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

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

La relación de sincronización muestra el rendimiento del adaptador de red del agente de datos. Si aceleró el rendimiento de sincronización mediante el uso de varios agentes de datos, el rendimiento será la suma de todo el tráfico. Este rendimiento se actualiza cada 20 segundos.

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

El agente de datos puede sincronizar 4 archivos a la vez. Si tiene archivos muy grandes (varios TB cada uno), puede tardar mucho tiempo en completar el proceso de transferencia y el rendimiento puede verse afectado.

Limitar el número de transferencias simultáneas puede ser de ayuda. [Mailto:ng-cloudsync-](mailto:ng-cloudsync-)



support@netapp.com[Contacte con nosotros para obtener ayuda].

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

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

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

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

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

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

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

### **¿Cuántos agentes de datos son necesarios?**

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

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

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

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

## **Eliminar cosas**

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

### **¿Qué sucede si elimino mi relación con Cloud Sync?**

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

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

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

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

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

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

## **Resolución de problemas**

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

## **Análisis en profundidad de los agentes de datos**

La siguiente pregunta se refiere al agente de datos.

### **¿puede explicar la arquitectura del agente de datos?**

Claro. Estos son los puntos más importantes:

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

## Información de copyright

Copyright © 2024 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.