



# **Manos a la obra**

## Cloud Sync

NetApp

February 20, 2023

This PDF was generated from <https://docs.netapp.com/es-es/cloud-manager-sync/concept-cloud-sync.html> on February 20, 2023. Always check docs.netapp.com for the latest.

# Tabla de Contenido

- Manos a la obra ..... 1
  - Información general de Cloud Sync ..... 1
  - Inicio rápido de Cloud Sync ..... 3
  - Relaciones de sincronización compatibles ..... 4
  - Preparar el origen y el destino ..... 12
  - Información general sobre redes para Cloud Sync ..... 19
  - Instalar un agente de datos ..... 22

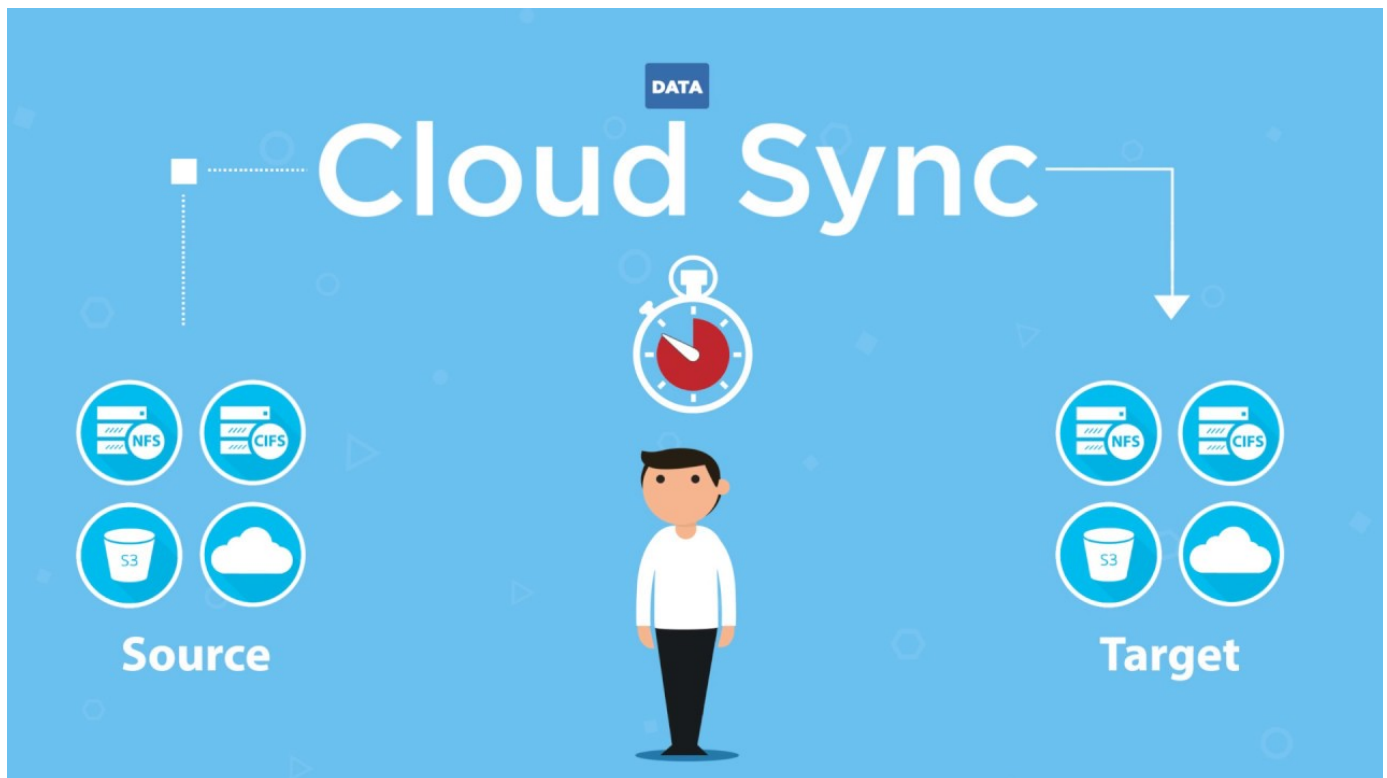
# Manos a la obra

## Información general de Cloud Sync

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

### Funciones

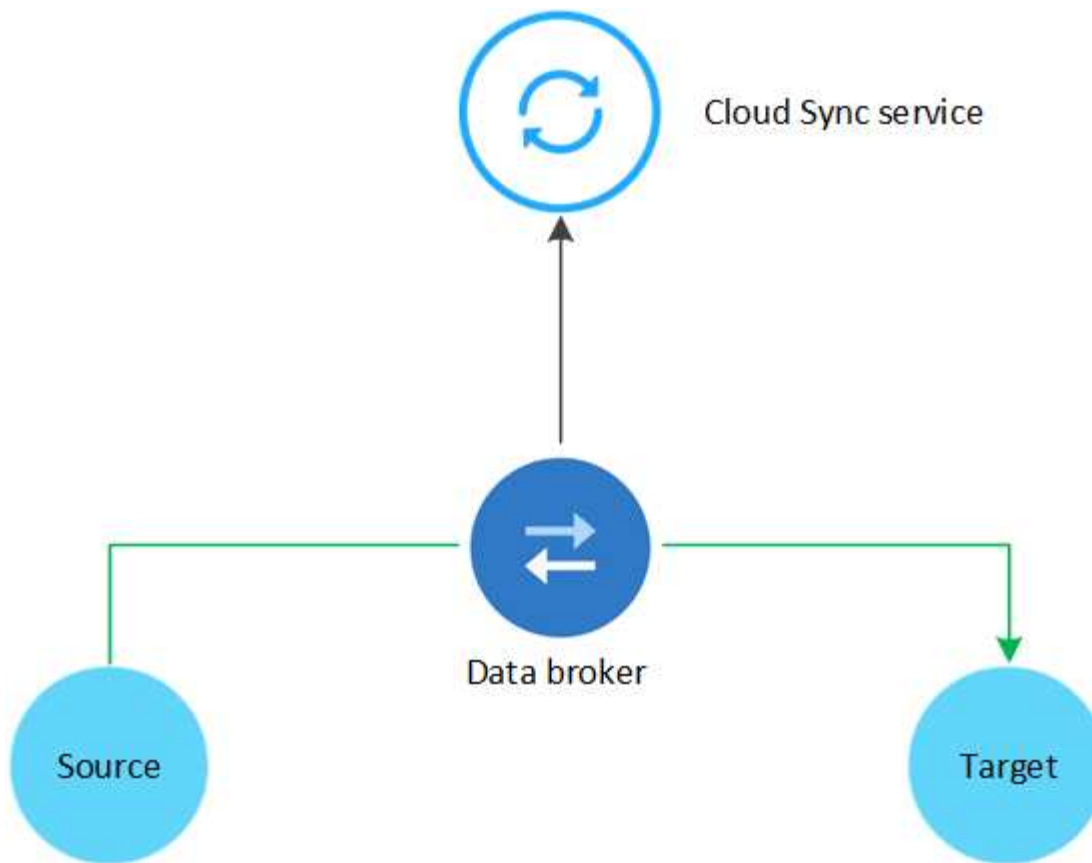
Vea el siguiente vídeo para obtener información general sobre Cloud Sync:



### Cómo funciona Cloud Sync

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

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



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

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

## Tipos de almacenamiento admitidos

Cloud Sync admite los siguientes tipos de almacenamiento:

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

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

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

## Externa

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

### Cargos por recursos

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

### Cargos por servicio

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

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

## Inicio rápido de Cloud Sync

Primeros pasos en el servicio Cloud Sync incluyen algunos pasos.



### Inicie sesión y configure BlueXP

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

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

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

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

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

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

2

### Prepare el origen y el destino

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

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

3

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

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

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

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

4

### Cree su primera relación de sincronización

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

5

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

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

## Relaciones de sincronización compatibles

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

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



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

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

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

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

**Notas:**

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

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

## Preparar el origen y el destino

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

### Redes

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

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

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

### Directorio de destino

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

### Permisos para leer directorios

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

en el directorio o carpeta.

## NFS

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

## Almacenamiento de objetos

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

## SMB

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



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

## requisitos de bloque de Amazon S3

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

### Ubicaciones de agentes de datos compatibles para Amazon S3

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

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

### Regiones admitidas de AWS

Todas las regiones están soportadas excepto las regiones de China.

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

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

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

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


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

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

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

## Summary

[Delete role](#)

**Role ARN** `arn:aws:iam::142981742689:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05` 

[Role description](#) [Edit](#)

## requisitos de almacenamiento de Azure Blob

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

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

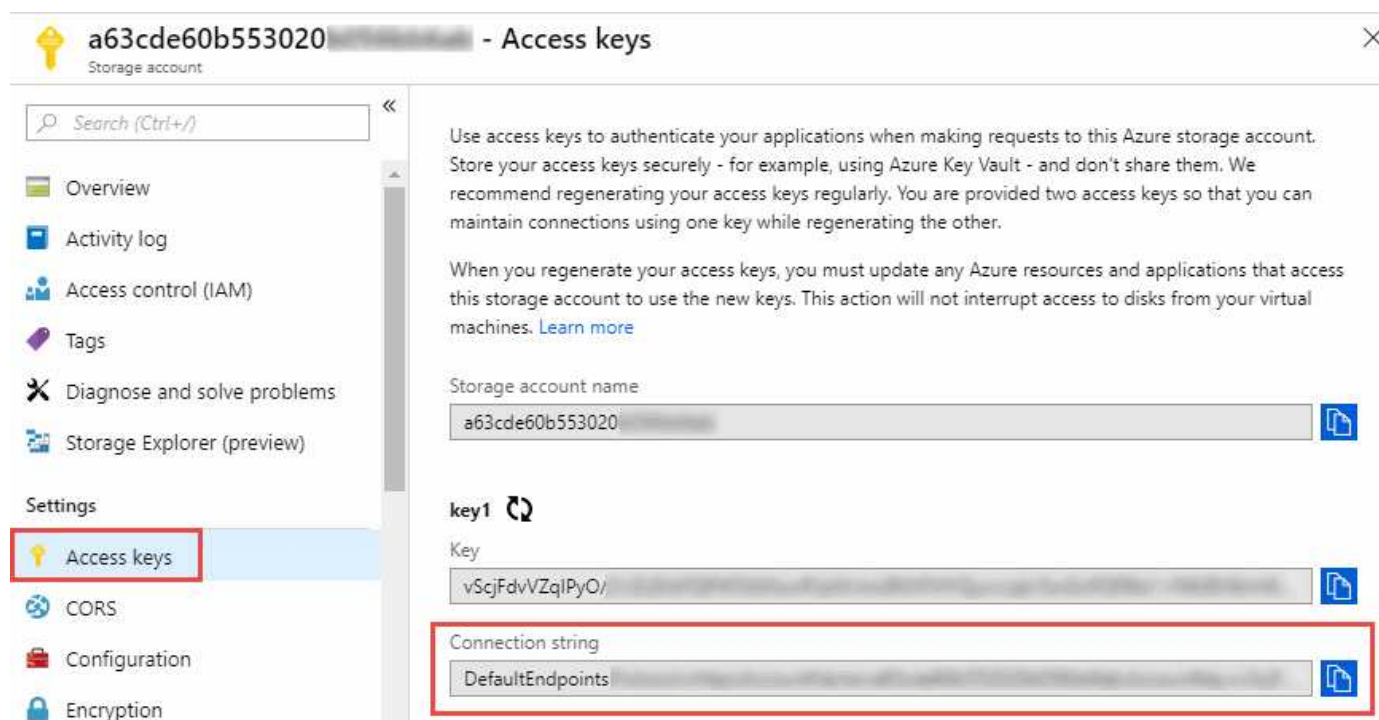
Un agente de datos puede residir en cualquier ubicación cuando una relación de sincronización incluye el almacenamiento de Azure Blob.

### Regiones de Azure compatibles

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

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

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



**a63cde60b553020 - Access keys**

Storage account

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Storage Explorer (preview)

Settings

- Access keys**
- CORS
- Configuration
- Encryption

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

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

Storage account name: a63cde60b553020

**key1**

Key: vScjFdvVZqIPyO/

**Connection string**: DefaultEndpoints



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

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

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

**a63cde60b553020 - Shared access signature**

Storage account

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Storage Explorer (preview)

Settings

Access keys

CORS

Configuration

Encryption

**Shared access signature**

Firewalls and virtual networks

Advanced Threat Protection (pr...

Properties

Locks

**Allowed services**

☒ Blob ☐ File ☐ Queue ☐ Table

**Allowed resource types**

☒ Service ☒ Container ☒ Object

**Allowed permissions**

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

**Start and expiry date/time**

Start

2018-10-23 10:07:32 AM

End

2019-10-23 6:07:32 PM

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

**Allowed IP addresses**

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

**Allowed protocols**

☒ HTTPS only ☐ HTTPS and HTTP

**Signing key**

key1

**Generate SAS and connection string**



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

## Azure Data Lake Storage Gen2

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

## Requisito de Azure NetApp Files

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



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

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

## Requisitos de caja

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

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

## requisitos de bloque de almacenamiento en cloud de Google

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

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

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

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

### Regiones compatibles de Google Cloud

Se admiten todas las regiones.

## Permisos para bloques de otros proyectos de Google Cloud

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

## Permisos para un destino de SnapMirror

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

## Unidad de Google

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

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

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

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

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

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

## Requisitos del servidor NFS

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

La versión deseada debe estar activada en el servidor.

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



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

## Requisitos de ONTAP

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

## Requisitos de almacenamiento de S3 de ONTAP

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

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

## Requisitos del servidor SMB

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

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

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

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

## Limitación de SMB para directorios y archivos ocultos

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

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

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

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

"a" del origen.

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

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

## Información general sobre redes para Cloud Sync

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

### Ubicación de agente de datos

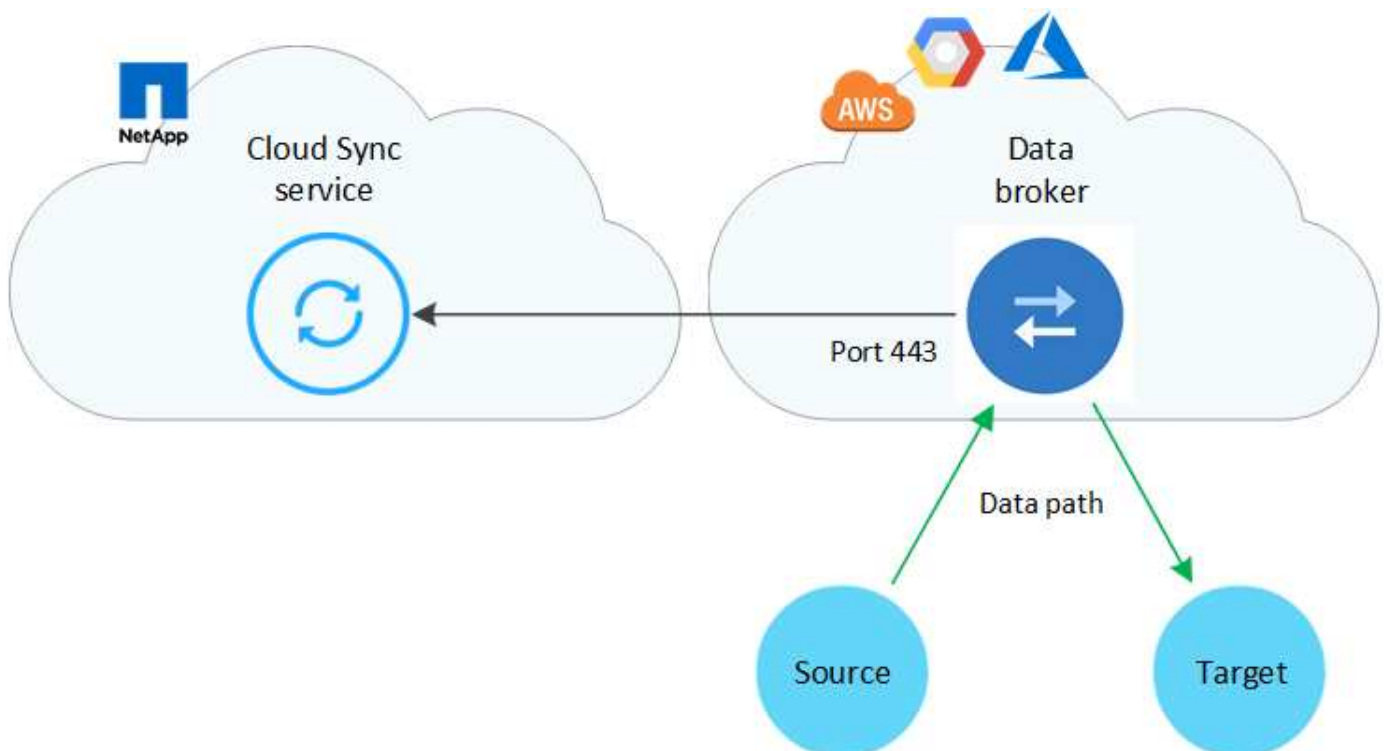
Un grupo de agentes de datos está compuesto por uno o más agentes de datos instalados en el cloud o en las instalaciones.

#### Agente de datos en el cloud

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

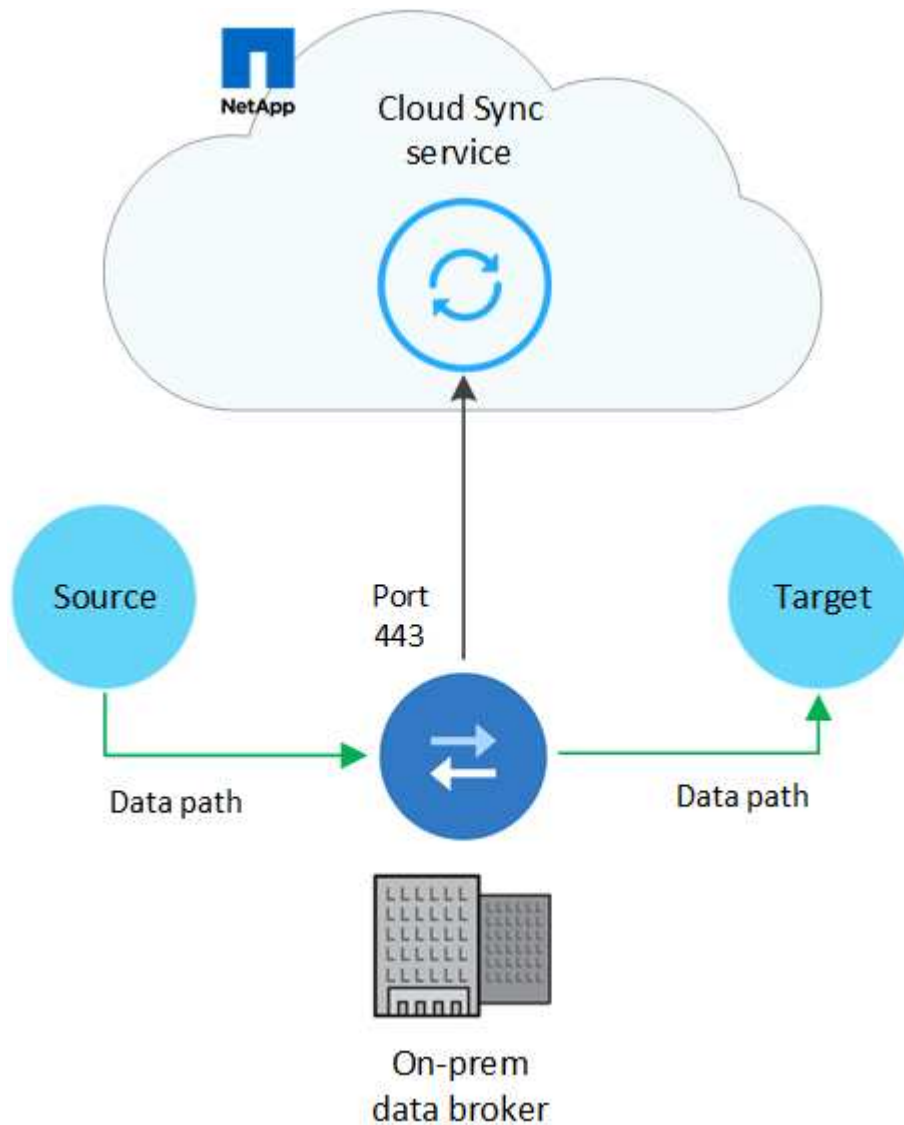


Cuando Cloud Sync implementa el agente de datos en AWS, Azure o Google Cloud, crea un grupo de seguridad que permite realizar las comunicaciones salientes necesarias.



## Agente de datos en sus instalaciones

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



## Requisitos de red

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

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

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

## Extremos de red

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

### Extremos de Data broker

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

Puntos finales	Específico
<a href="https://olcentgbl.trafficmanager.net">https://olcentgbl.trafficmanager.net</a>	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.
<a href="https://rpm.nodesource.com">https://rpm.nodesource.com</a> <a href="https://registry.npmjs.org">https://registry.npmjs.org</a> <a href="https://nodejs.org">https://nodejs.org</a> :	Para ponerse en contacto con repositorios para actualizar los paquetes Node.js, npm y otros paquetes de terceros utilizados en desarrollo.
<a href="https://tgz.pm2.io">https://tgz.pm2.io</a>	Para acceder a un repositorio para la actualización de Pm2, que es un paquete de terceros que se utiliza para supervisar Cloud Sync.
<a href="https://sqs.us-east-1.amazonaws.com">https://sqs.us-east-1.amazonaws.com</a> <a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	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).
<a href="https://s3.region.amazonaws.com">https://s3.region.amazonaws.com</a> por ejemplo: <a href="https://s3.us-east-2.amazonaws.com">s3.us-east-2.amazonaws.com</a> :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.
<a href="https://s3.amazonaws.com/">https://s3.amazonaws.com/</a>	Cuando se descargan registros del agente de datos de Cloud Sync, el agente de datos cierra su directorio de registros y carga los registros en un bloque S3 predefinido en la región de US-East-1.
<a href="https://storage.googleapis.com/">https://storage.googleapis.com/</a>	Para ponerse en contacto con Google Cloud cuando una relación de sincronización utiliza un bloque de GCP.
<a href="https://storage-account.blob.core.windows.net">https://storage-account.blob.core.windows.net</a> ["Si se utiliza Azure Data Lake Gen2: <a href="https://storage-account.dfs.core.windows.net">https://storage-account.dfs.core.windows.net</a> "] Donde <i>Storage-account</i> es la cuenta de almacenamiento de origen del usuario.	Para abrir el proxy en la dirección de la cuenta de almacenamiento de Azure de un usuario.
<a href="https://cf.cloudsync.netapp.com">https://cf.cloudsync.netapp.com</a> <a href="https://repo.cloudsync.netapp.com">https://repo.cloudsync.netapp.com</a>	Para ponerse en contacto con el servicio Cloud Sync.
<a href="https://support.netapp.com">https://support.netapp.com</a>	Para ponerse en contacto con el soporte de NetApp cuando use una licencia BYOL para relaciones de sincronización.

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

### Extremos del navegador web

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

[logs.cloudsync.netapp.com:443](https://logs.cloudsync.netapp.com:443)

## Instalar un agente de datos

### Crear un nuevo agente de datos en AWS

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

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

### Regiones admitidas de AWS

Todas las regiones están soportadas excepto las regiones de China.



## Privilegios de usuario raíz

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

## Requisitos de red

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

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

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

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

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

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

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

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

El rol del IAM debe cumplir los siguientes requisitos:

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

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

## Creación del agente de datos

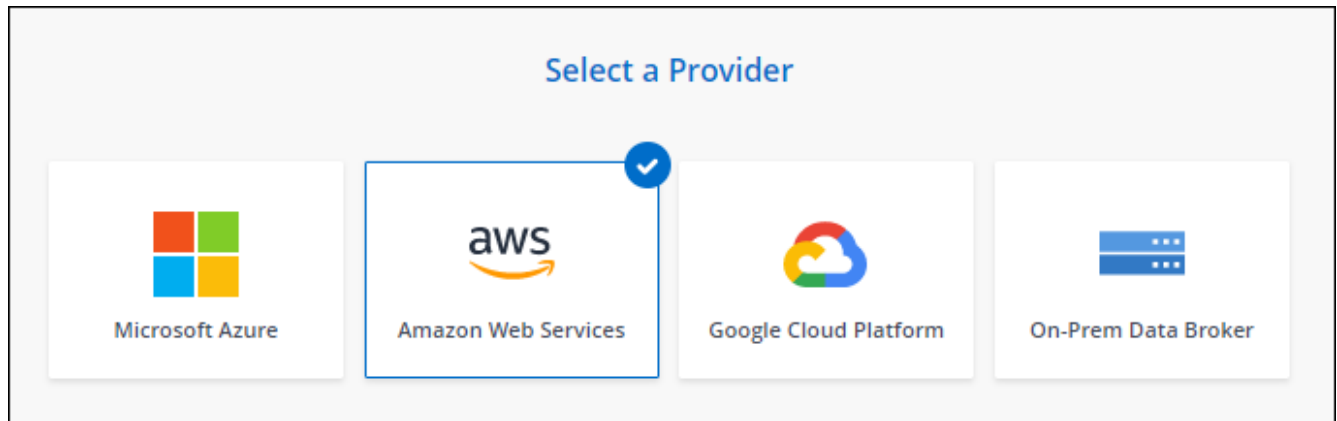
Hay varias formas de crear un nuevo agente de datos. Estos pasos describen cómo instalar un agente de datos en AWS al crear una relación de sincronización.

### Pasos

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

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

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



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

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

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

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

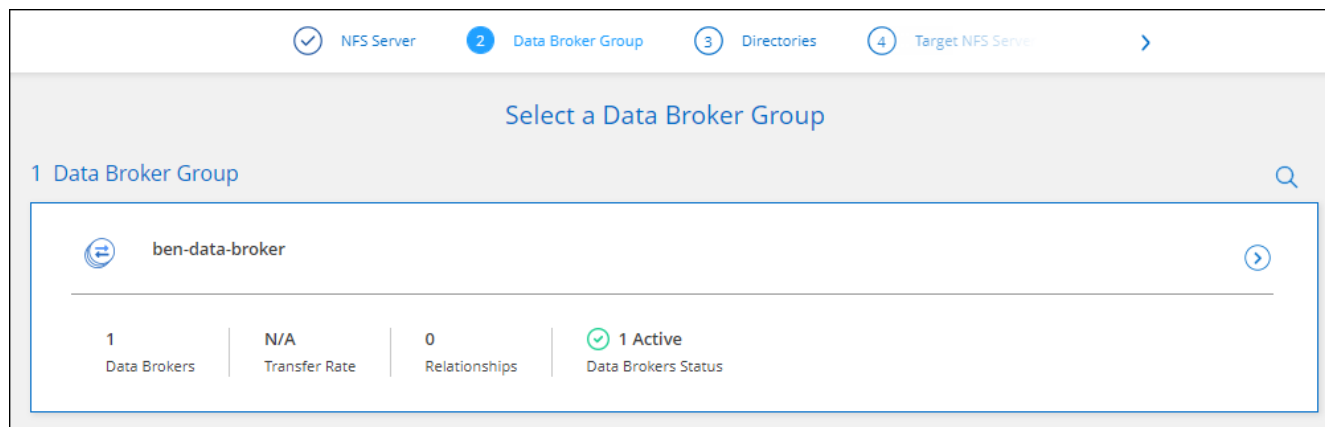
► [https://docs.netapp.com/es-es/cloud-manager-sync//media/video\\_cloud\\_sync.mp4](https://docs.netapp.com/es-es/cloud-manager-sync//media/video_cloud_sync.mp4) (video)

- 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](#).

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

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



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

## Resultado

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

## Detalles sobre la instancia de Data broker

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

### Tipo de instancia

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

### VCPU

4

### RAM

16 GB

### De NetApp

Amazon Linux 2022

### Tamaño y tipo del disco

SSD GP2 DE 10 GB

## Creación de un nuevo agente de datos en Azure

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

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

instalaciones. ["Leer más"](#).

## Regiones de Azure compatibles

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

## Privilegios de usuario raíz

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

## Requisitos de red

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

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

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

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

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

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

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

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

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

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

    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Compute/virtualMachines/read",
```

```

        "Microsoft.Compute/virtualMachines/delete",
        "Microsoft.Compute/disks/delete",
        "Microsoft.Network/networkInterfaces/delete",
        "Microsoft.Network/publicIPAddresses/delete",

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

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

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

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

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

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

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

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

```

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

Nota:

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

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

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

## Método de autenticación

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

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

## Creación del agente de datos

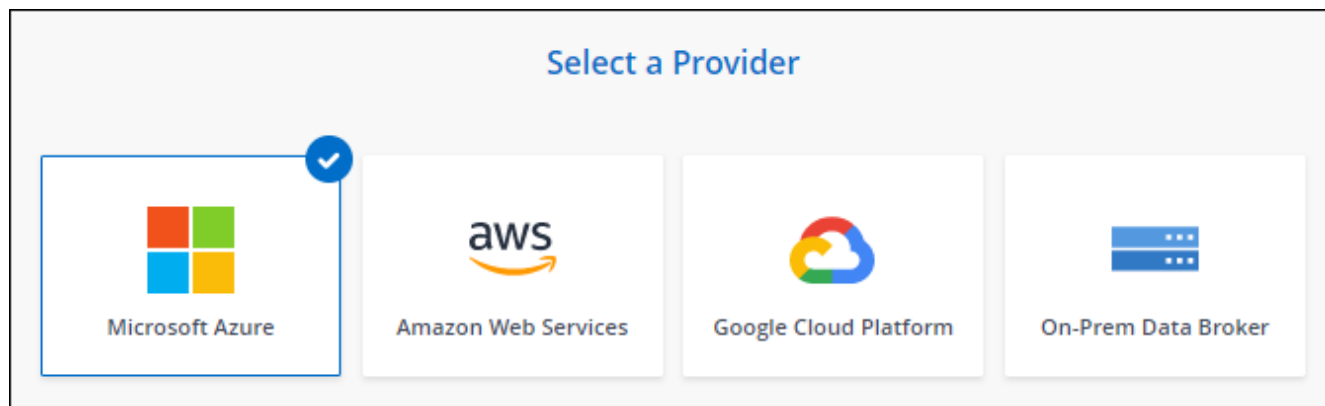
Hay varias formas de crear un nuevo agente de datos. Estos pasos describen cómo instalar un agente de datos en Azure al crear una relación de sincronización.

### Pasos

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

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

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



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

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

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

The image shows a configuration form with two main sections: 'Location' and 'Virtual Machine'. The 'Location' section has four dropdown menus: 'Subscription' (OCCM Dev), 'Azure Region' (West US 2), 'VNet' (Vnet1), and 'Subnet' (Subnet1). The 'Virtual Machine' section has a text input for 'VM Name' (netappdatabroker), a text input for 'User Name' (databroker), a radio button selection for 'Authentication Method' (Password is selected), a password input field for 'Enter Password' (masked with dots), and a radio button selection for 'Resource Group' (Generate a new group is selected).

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

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

El proceso puede tardar hasta 7 minutos.

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

## Resultado

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

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

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

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

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

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

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

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

## Información sobre el equipo virtual de Data broker

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

### Tipo de máquina virtual

Estándar DS4 v2

### VCPU

8

### RAM

28 GB

### De NetApp

Rocky Linux 9.0



## Tamaño y tipo del disco

SSD Premium de 64 GB

## Creación de un nuevo agente de datos en Google Cloud

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

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

### Regiones compatibles de Google Cloud

Se admiten todas las regiones.

### Privilegios de usuario raíz

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

### Requisitos de red

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

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

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

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

### Permisos necesarios para implementar el agente de datos en Google Cloud

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

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

## Permisos necesarios para la cuenta de servicio

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

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

### Notas:

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

## Creación del agente de datos

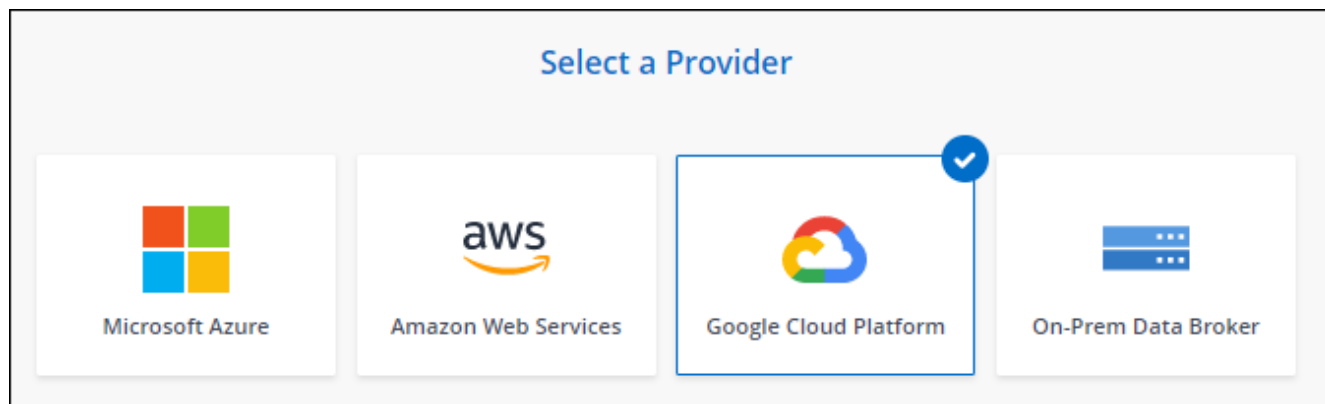
Hay varias formas de crear un nuevo agente de datos. Estos pasos describen cómo instalar un agente de datos en Google Cloud al crear una relación de sincronización.

### Pasos

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

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

3. En la página **Grupo de agentes de datos**, haga clic en **Crear agente de datos** y seleccione **Google Cloud Platform**.

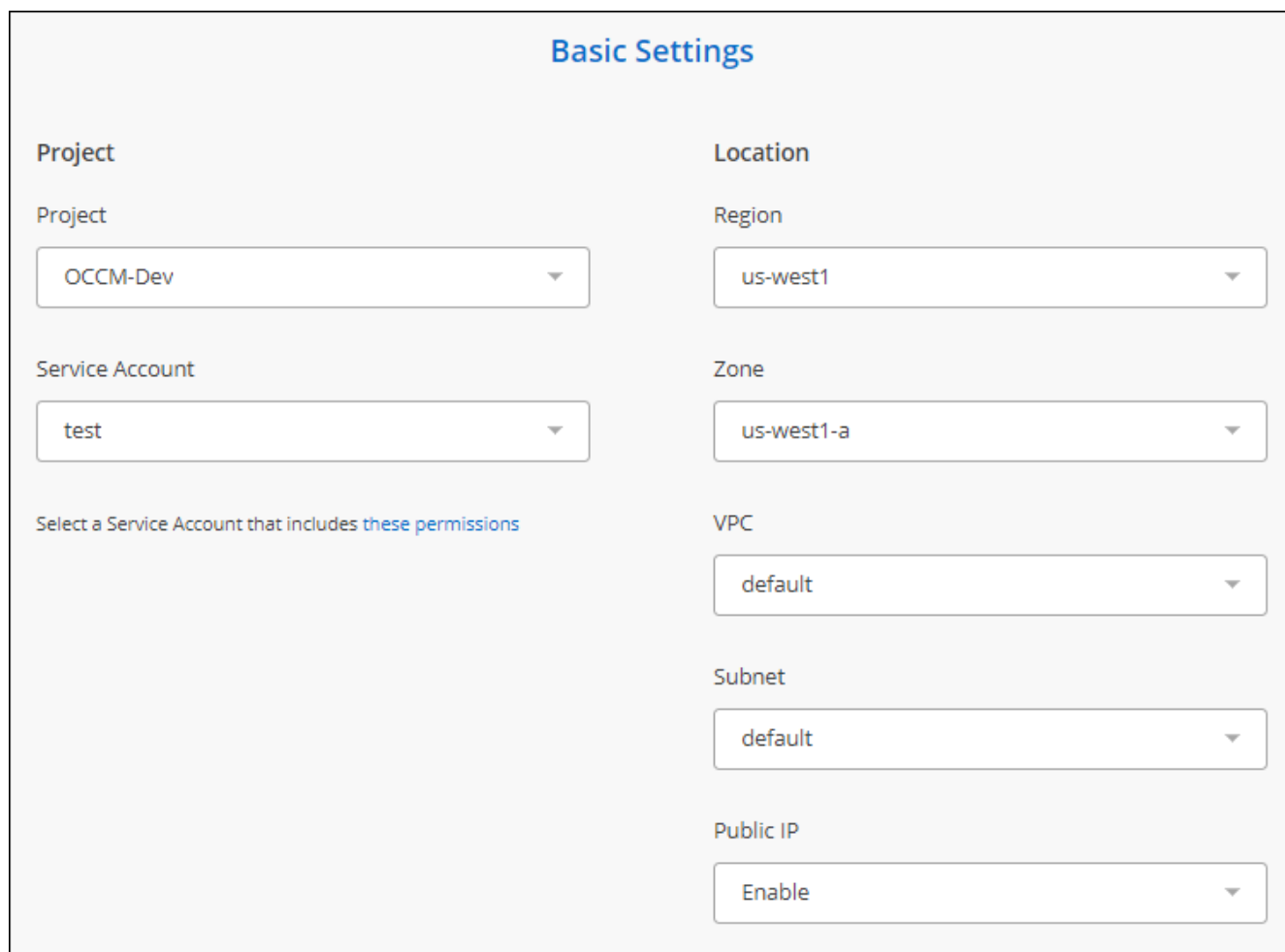


4. Introduzca un nombre para el Data broker y haga clic en **continuar**.
5. Si se le solicita, inicie sesión con su cuenta de Google.

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

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

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

The image shows a 'Basic Settings' form with two columns. The left column has 'Project' (OCCM-Dev) and 'Service Account' (test). Below these is a note: 'Select a Service Account that includes [these permissions](#)'. The right column has 'Location' (Region: us-west1, Zone: us-west1-a), 'VPC' (default), 'Subnet' (default), and 'Public IP' (Enable). All fields are dropdown menus.

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

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

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

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

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

## Resultado

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

## Proporciona permisos para utilizar bloques en otros proyectos de Google Cloud

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

## Pasos

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

## Resultado

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

## Detalles sobre la instancia de VM de Data broker

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

### Tipo de máquina

n2-estándar-4

### VCPU

4

### RAM

15 GB

## De NetApp

Rocky Linux 9.0

## Tamaño y tipo del disco

Disco duro de 20 GB, estándar pd

## Instalar el agente de datos en un host Linux

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

### Requisitos del host Linux

- **sistema operativo:**

- CentOS 7.0, 7.7 y 8.0

CentOS Stream no es compatible.

- Red Hat Enterprise Linux 7.7 y 8.0
- Sistema operativo Ubuntu Server 20.04 LTS
- SUSE Linux Enterprise Server 15 SP1

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

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

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

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

### Privilegios de usuario raíz

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

### Requisitos de red

- El host Linux debe tener una conexión con el origen y el destino.
- El servidor de archivos debe permitir que el host Linux acceda a las exportaciones.
- El puerto 443 debe estar abierto en el host Linux para el tráfico saliente a AWS (el agente de datos se

comunica constantemente con el servicio Amazon SQS).

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

## Habilitar el acceso a AWS

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

### Pasos

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

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

2. Cree un usuario IAM con acceso mediante programación.

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

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

## Habilitar el acceso a Google Cloud

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

### Pasos

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

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

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



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

3. Guarde el archivo JSON en el host Linux.

## Habilitar el acceso a Microsoft Azure

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

## Instalación del Data broker

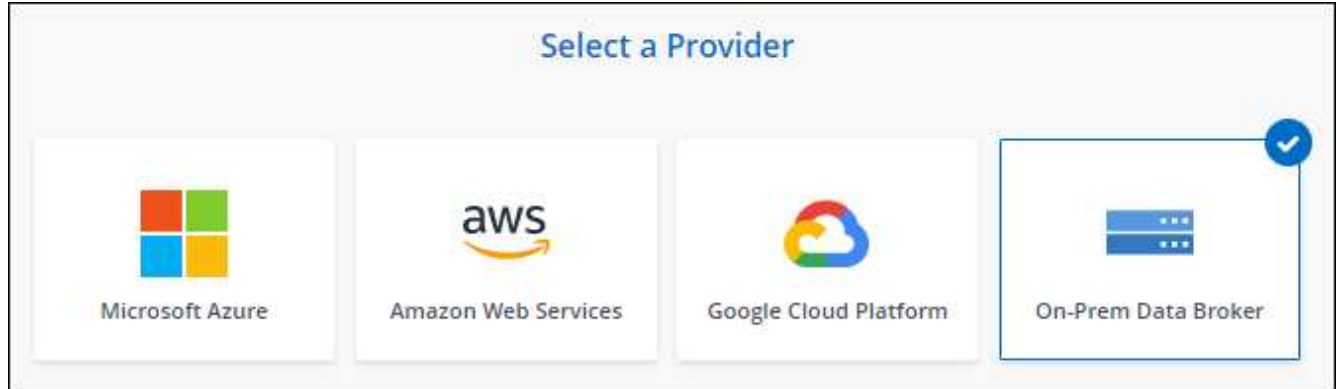
Puede instalar un agente de datos en un host Linux al crear una relación de sincronización.

### Pasos

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

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

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



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

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

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

5. En la página de instrucciones:

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

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

- d. Descargue el instalador:

- Sin proxy:

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

- Usar servidor proxy:

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

- Utilice el servidor proxy con autenticación:

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

## URI

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

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



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

- Sin configuración de proxy:

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

- Configuración de proxy:

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

- Configuración del proxy con autenticación:

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

## Claves de AWS

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

## Archivo JSON

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

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



## Información de copyright

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

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

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

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

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

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

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

## Información de la marca comercial

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