Empezar

NetApp Copy and Sync

NetApp
December 16, 2025

Tabla de contenidos

Empezar

Obtenga más información sobre NetApp Copy and Sync

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

NetApp Console

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

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

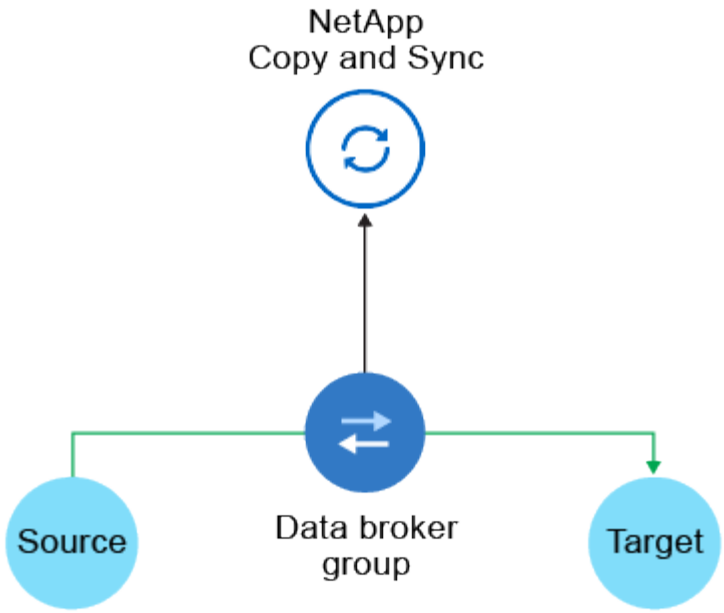
No necesita una licencia o suscripción para comenzar a usar NetApp Console y solo incurre en cargos cuando necesita implementar agentes de Console en su nube para garantizar la conectividad con sus sistemas de almacenamiento o servicios de datos de NetApp . Sin embargo, algunos servicios de datos de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

Obtenga más información sobre el "NetApp Console" .

Cómo funciona NetApp Copy and Sync

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

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



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

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

Tipos de almacenamiento admitidos

Copiar y sincronizar admite los siguientes tipos de almacenamiento:

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

- SFTP (solo usando API)
- StorageGRID

"Ver las relaciones de sincronización admitidas" .

Costos

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

Cargos por recursos

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

Cargos por servicio

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

"Aprenda cómo funcionan las licencias" .

Inicio rápido para NetApp Copy and Sync

Comenzar a utilizar NetApp Copy and Sync incluye algunos pasos.

1 Inicie sesión y configure la NetApp Console

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

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

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

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

- "Descubra cómo comenzar a utilizar la NetApp Console"
- "Obtenga más información sobre los agentes de consola"

2 Prepare su fuente y su destino

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

- "Ver relaciones compatibles"
- "Preparar la fuente y el destino"

3 Prepare una ubicación para el agente de datos de NetApp

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

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

- "Revisar la instalación de AWS"
- "Revisar la instalación de Azure"
- "Revisar la instalación de Google Cloud"
- "Revisar la instalación del host Linux"

4 Crea tu primera relación de sincronización

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

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

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

Relaciones de sincronización admitidas en NetApp Copy and Sync

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

Ubicación de la fuente	Ubicaciones de destino compatibles
Amazon EFS	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID
Amazon FSx para ONTAP	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID

Ubicación de la fuente	Ubicaciones de destino compatibles
Amazon S3	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Caja [1] • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID
Blob de Azure	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID

Ubicación de la fuente	Ubicaciones de destino compatibles
Almacenamiento de Azure Data Lake Gen2	• Azure NetApp Files • Cloud Volumes ONTAP • FSx para ONTAP • Almacenamiento de objetos en la nube de IBM • Servidor NFS • ONTAP • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID
Azure NetApp Files	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID
Caja [1]	• Amazon FSx para ONTAP • Amazon S3 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Servidor SMB • StorageGRID

Ubicación de la fuente	Ubicaciones de destino compatibles
Cloud Volumes ONTAP	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID
Almacenamiento en la nube de Google	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID
Google Drive	• Servidor NFS • Servidor SMB

Ubicación de la fuente	Ubicaciones de destino compatibles
Almacenamiento de objetos en la nube de IBM	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Caja [1] • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID
Servidor NFS	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Google Drive • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID

Ubicación de la fuente	Ubicaciones de destino compatibles
Clúster ONTAP local (NFS o SMB)	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Servidor SMB • StorageGRID
Almacenamiento ONTAP S3	• Amazon S3 • Almacenamiento de Azure Data Lake Gen2 • Almacenamiento en la nube de Google • Servidor NFS • Servidor SMB • StorageGRID • Almacenamiento ONTAP S3
SFTP [2]	S3

Ubicación de la fuente	Ubicaciones de destino compatibles
Servidor SMB	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Google Drive • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID
StorageGRID	• Amazon EFS • Amazon FSx para ONTAP • Amazon S3 • Blob de Azure • Almacenamiento de Azure Data Lake Gen2 • Azure NetApp Files • Caja [1] • Cloud Volumes ONTAP • Almacenamiento en la nube de Google • Almacenamiento de objetos en la nube de IBM • Servidor NFS • Clúster ONTAP local (NFS o SMB) • Almacenamiento ONTAP S3 • Servidor SMB • StorageGRID

Notas:

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

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

Preparar el origen y el destino en NetApp Copy and Sync

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

Redes

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

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

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

Directorio de destino

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

Permisos para leer directorios

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

Sistema Nacional de Archivos

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

Almacenamiento de objetos

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

SMB

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

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

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

Requisitos del bucket de Amazon S3

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

Ubicaciones de agentes de datos compatibles con Amazon S3

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

- "Aprenda a implementar el agente de datos de AWS"
- "Aprenda a instalar el agente de datos en un host Linux"

Regiones de AWS compatibles

Se admiten todas las regiones excepto la de China.

Permisos necesarios para los buckets S3 en otras cuentas de AWS

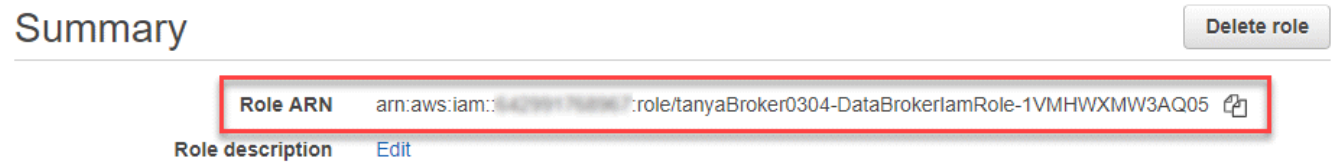
Al configurar una relación de sincronización, puede especificar un bucket S3 que resida en una cuenta de AWS que no esté asociada con un agente de datos.

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

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

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

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



Requisitos de almacenamiento de blobs de Azure

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

Ubicaciones de agentes de datos compatibles con Azure Blob

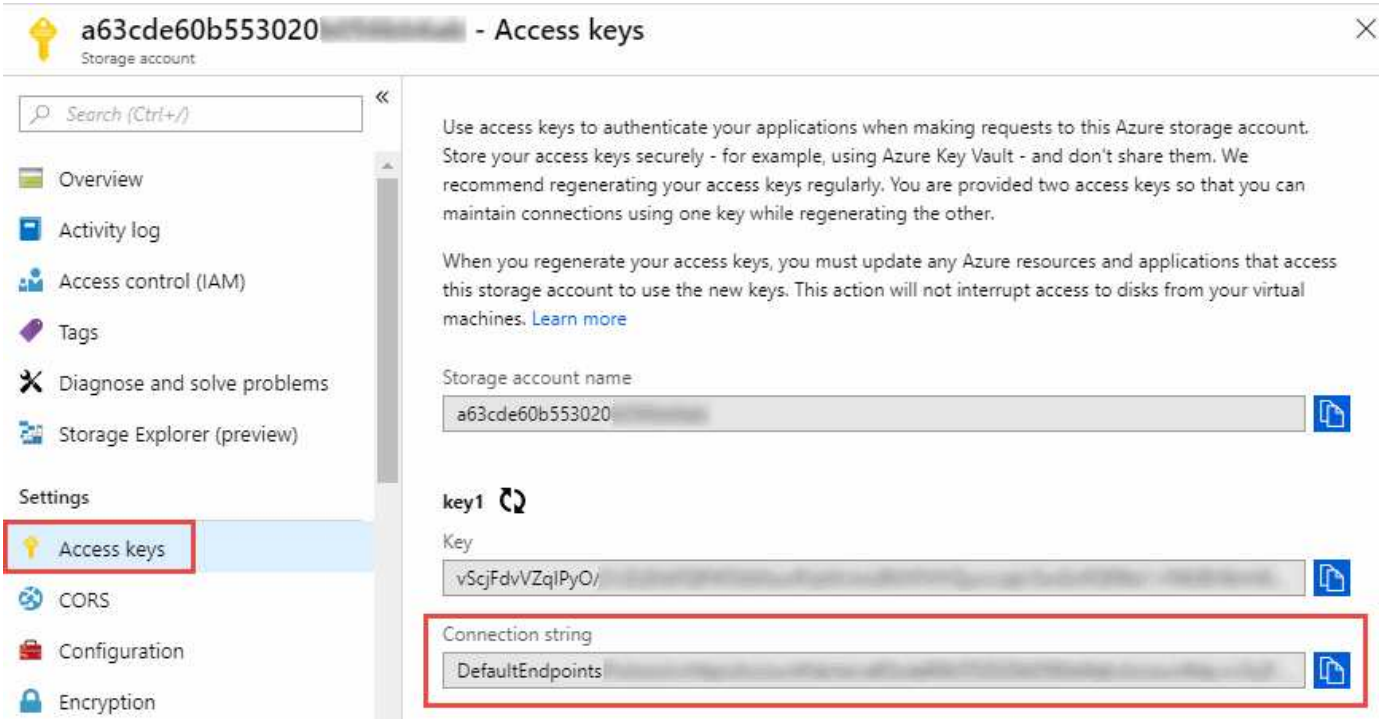
Un agente de datos puede residir en cualquier ubicación cuando una relación de sincronización incluye almacenamiento de blobs de Azure.

Regiones de Azure compatibles

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

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

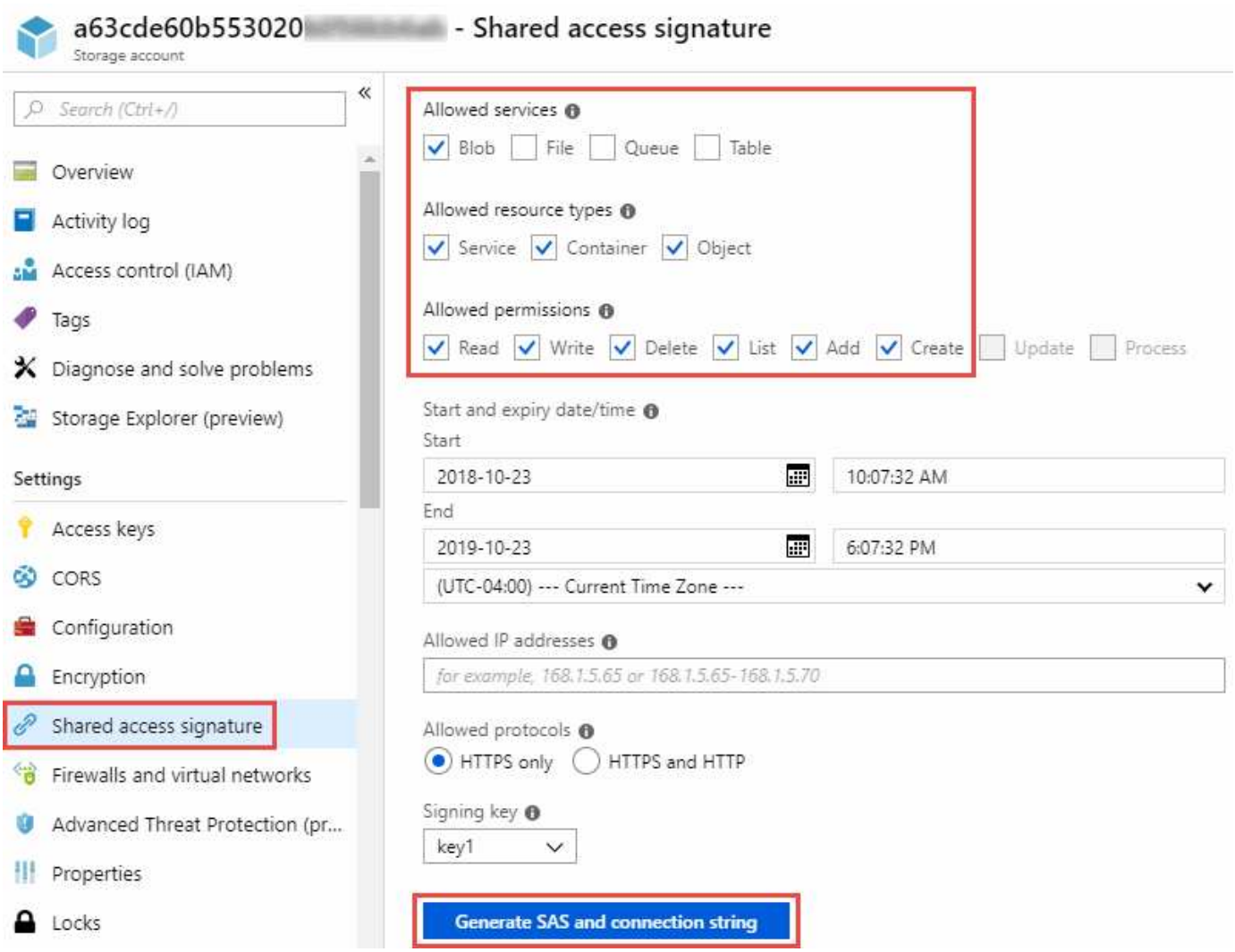
Al crear una relación de sincronización entre un contenedor de blobs de Azure y un servidor NFS o SMB, debe proporcionar Copiar y sincronizar con la cadena de conexión de la cuenta de almacenamiento:



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

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

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



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

Almacenamiento de Azure Data Lake Gen2

Al crear una relación de sincronización que incluya Azure Data Lake, debe proporcionar Copiar y sincronizar con la cadena de conexión de la cuenta de almacenamiento. Debe ser una cadena de conexión normal, no una firma de acceso compartido (SAS).

Requisito de Azure NetApp Files

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

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

"Obtenga más información sobre los niveles de servicio y el rendimiento de Azure NetApp Files" .

Requisitos de la caja

- Para crear una relación de sincronización que incluya Box, deberá proporcionar las siguientes credenciales:
  - ID de cliente
  - Secreto del cliente
  - Clave privada
  - ID de clave pública
  - Frase de contraseña
  - ID de empresa
- Si crea una relación de sincronización de Amazon S3 a Box, debe utilizar un grupo de agentes de datos que tenga una configuración unificada donde las siguientes configuraciones estén establecidas en 1:
  - Concurrencia del escáner
  - Límite de procesos del escáner
  - Concurrencia del transferente
  - Límite de procesos de transferencia

  "Aprenda a definir una configuración unificada para un grupo de agentes de datos" .

Requisitos del depósito de Google Cloud Storage

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

Ubicaciones de intermediarios de datos compatibles con Google Cloud Storage

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

- "Aprenda a implementar el agente de datos de Google Cloud"
- "Aprenda a instalar el agente de datos en un host Linux"

Regiones de Google Cloud compatibles

Se admiten todas las regiones.

Permisos para depósitos en otros proyectos de Google Cloud

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

Permisos para un destino SnapMirror

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

Cómo cifrar un depósito de Google Cloud

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

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

Google Drive

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

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

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

- "Crear la cuenta de servicio y las credenciales"
- "Delegar autoridad de todo el dominio a su cuenta de servicio"

Cuando edite el campo Ámbitos de OAuth, ingrese los siguientes ámbitos:

- \ https://www.googleapis.com/auth/drive
- \ https://www.googleapis.com/auth/drive.file

Requisitos del servidor NFS

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

  La versión deseada debe estar habilitada en el servidor.
- Si desea sincronizar datos NFS desde un sistema ONTAP , asegúrese de que el acceso a la lista de exportación NFS para una SVM esté habilitado (vserver nfs modify -vserver *svm_name* -showmount enabled).

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

Requisitos de ONTAP

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

Requisitos de almacenamiento de ONTAP S3

Cuando se configura una relación de sincronización que incluye "Almacenamiento ONTAP S3" , deberá proporcionar lo siguiente:

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

Requisitos del servidor SMB

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

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

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

Limitación de SMB para directorios y archivos ocultos

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

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

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

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

En el caso de los directorios, digamos que hay un directorio llamado "b" en el origen y un directorio llamado "B" en el destino. Cuando Copy and Sync intenta copiar el directorio llamado "b" al destino, Copy and Sync recibe un error que indica que el directorio ya existe. Como resultado, Copiar y sincronizar siempre falla al copiar el directorio llamado “b”.

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

Descripción general de redes para NetApp Copy and Sync

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

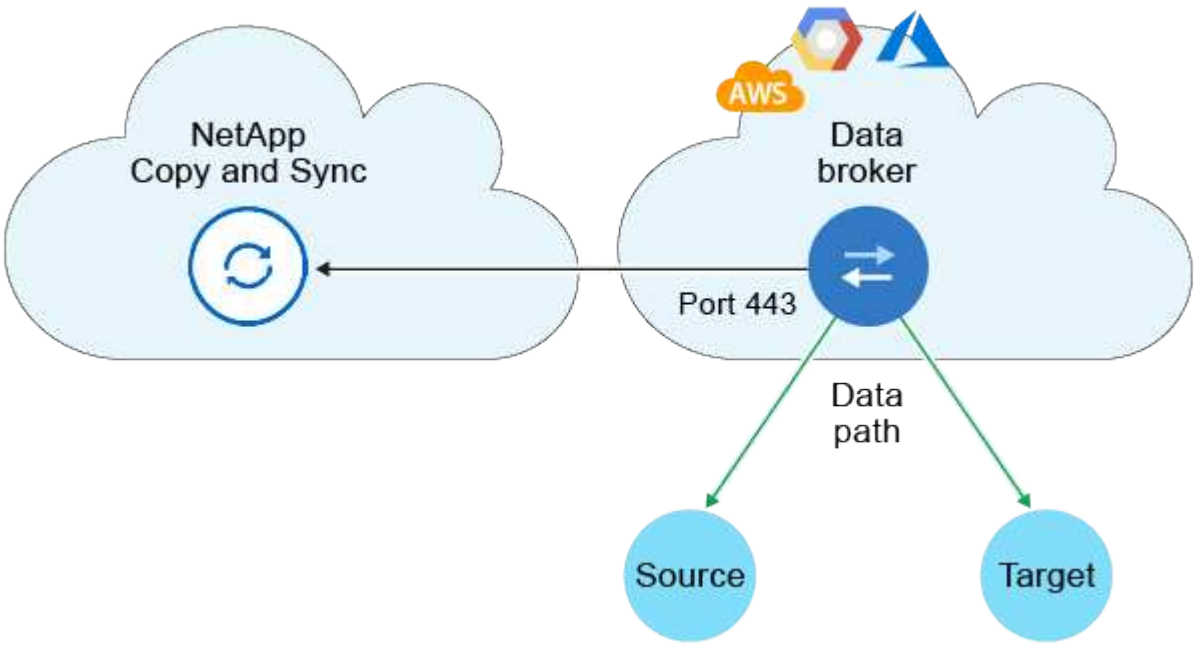
Ubicación del corredor de datos

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

Broker de datos en la nube

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

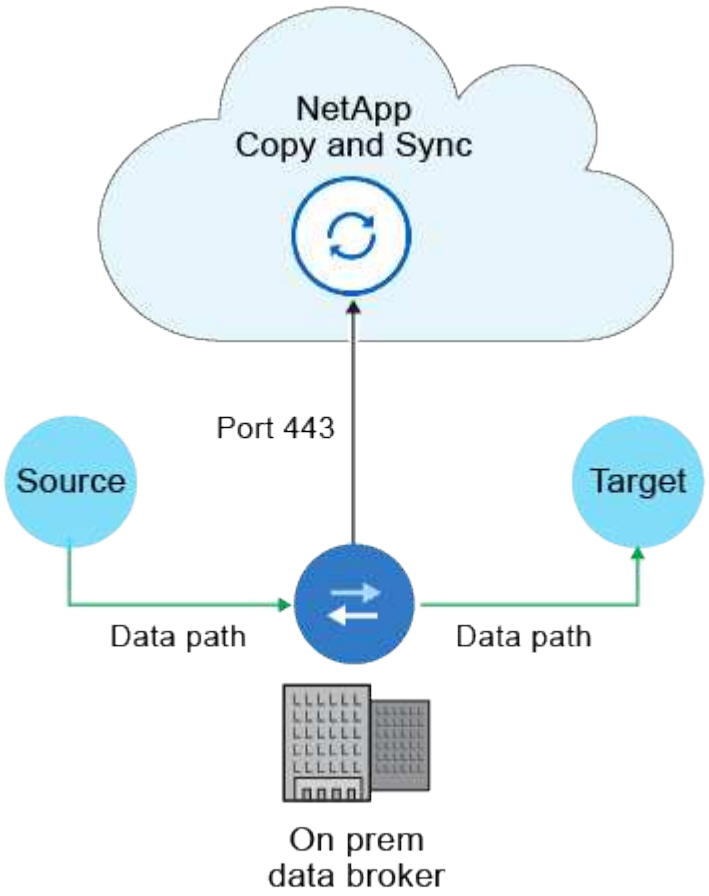
Cuando Copy and Sync implementa el agente de datos en AWS, Azure o Google Cloud, crea un grupo de seguridad que habilita la comunicación saliente requerida.



Corredor de datos en sus instalaciones

La siguiente imagen muestra el agente de datos ejecutándose localmente en un centro de datos. Nuevamente, la fuente y el destino pueden estar en cualquier ubicación, siempre que haya una conexión con

el agente de datos.



Requisitos de red

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

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

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

Puntos finales de red

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

Puntos finales del intermediario de datos

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

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

Puntos finales	Objetivo
\ https://sts.amazonaws.com \ https://sts.us-east-1.amazonaws.com	Para verificar las credenciales de AWS cuando el agente de datos se implementa en AWS o cuando se implementa en sus instalaciones y se proporcionan las credenciales de AWS. El agente de datos se comunica con este punto final durante la implementación, cuando se actualiza y cuando se reinicia.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com	Para ponerse en contacto con NetApp Data Classification cuando utiliza la clasificación para seleccionar los archivos de origen para una nueva relación de sincronización.
\ https://pubsub.googleapis.com	Si se crea una relación de sincronización continua desde una cuenta de almacenamiento de Google.
https://storage-account</ em>.queue.core.windows.net\ https://management.azure.com/subscriptions/ ${subscriptionId} /resourceGroups/${resourceGroup}/providers/Microsoft.EventGrid/* Donde storage-account es la cuenta de almacenamiento de origen del usuario, subscriptionid es el ID de suscripción de origen y resourceGroup es el grupo de recursos de origen.	Si se crea una relación de sincronización continua desde una cuenta de almacenamiento de Azure.

Puntos finales del navegador web

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

registros.cloudsync.netapp.com:443

Inicie sesión en NetApp Copy and Sync

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

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

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

Rol de NetApp Console obligatorio Rol de administrador de la organización. "Obtenga más información sobre los roles de acceso a la NetApp Console" .

Pasos

1. Abra un navegador web y vaya a "NetApp Console" .

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

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

Instalar un agente de datos

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

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

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

Regiones de AWS compatibles

Se admiten todas las regiones excepto la de China.

Privilegios de root

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

Requisitos de red

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

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

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

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

Permisos necesarios para implementar el agente de datos en AWS

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

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

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

El rol de IAM debe cumplir los siguientes requisitos:

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

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

Crear el agente de datos

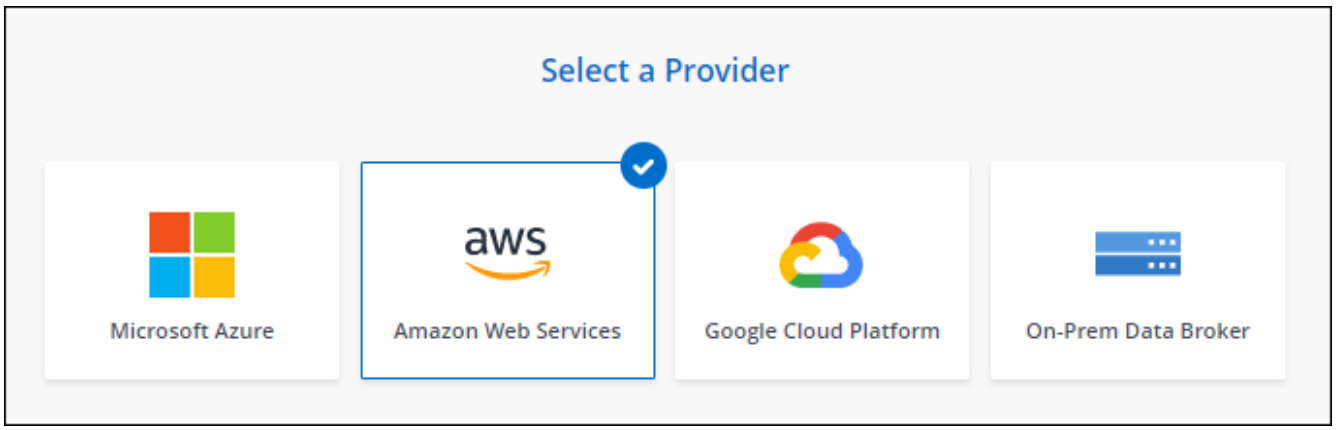
Hay algunas formas de crear un nuevo corredor de datos. Estos pasos describen cómo instalar un agente de datos en AWS al crear una relación de sincronización.

Pasos

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

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

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



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

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

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

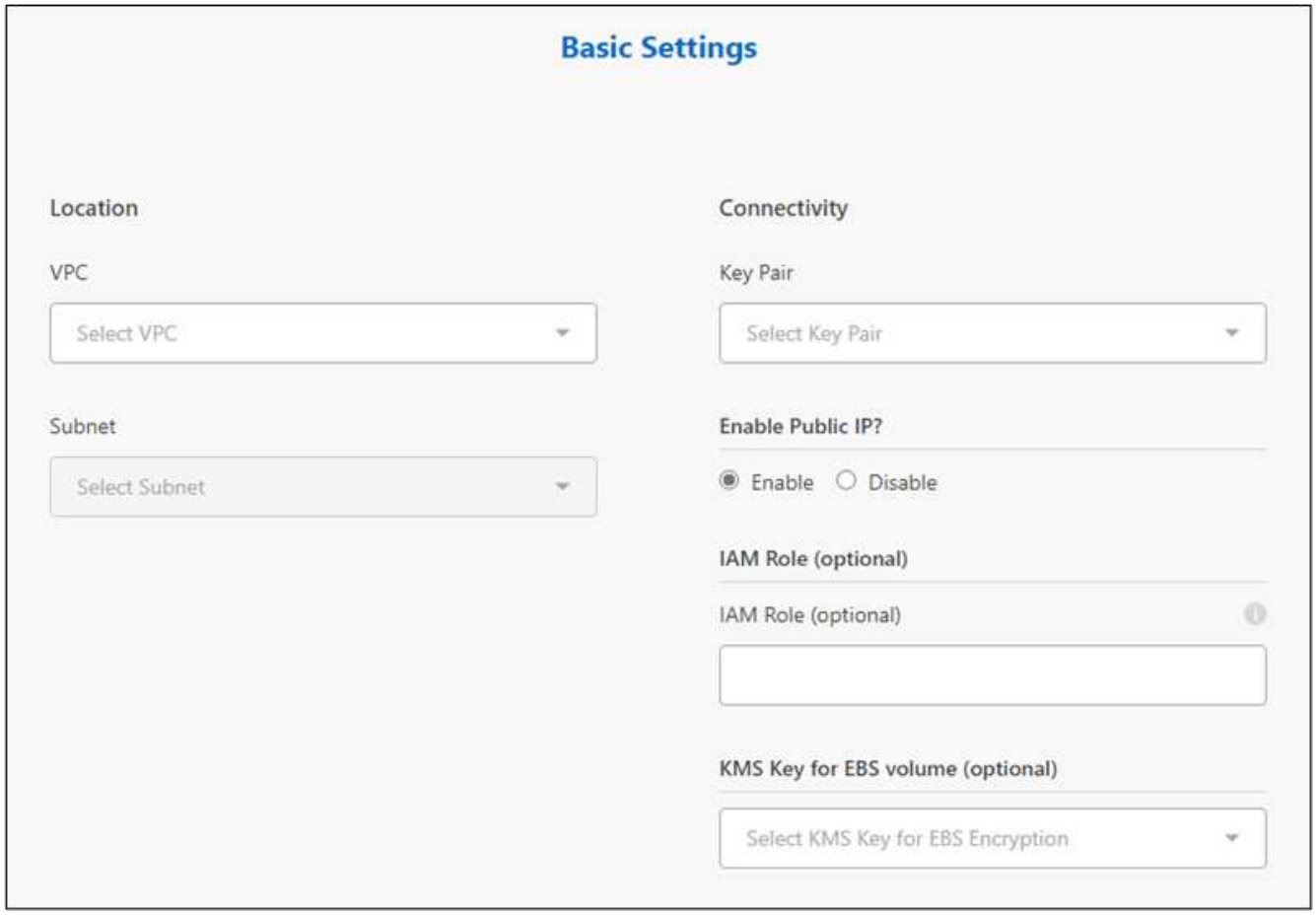
   El siguiente video muestra cómo iniciar la instancia del agente de datos utilizando una plantilla de

CloudFormation:

Iniciar un agente de datos desde una plantilla de AWS CloudFormation

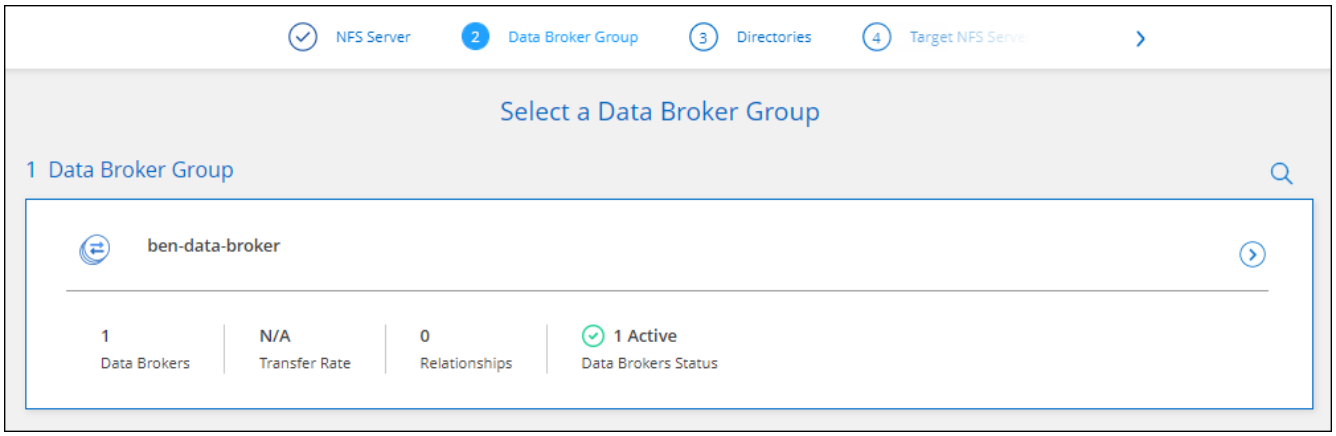
7. Si ingresó una clave de acceso de AWS, seleccione una ubicación para la instancia, seleccione un par de claves, elija si desea habilitar una dirección IP pública y seleccione una función de IAM existente, o deje el campo en blanco para que Copiar y sincronizar cree la función por usted. También tiene la opción de cifrar su agente de datos utilizando una clave KMS.

   Si elige su propio rol de IAM,Necesitarás proporcionar los permisos necesarios .



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

   La siguiente imagen muestra una instancia implementada correctamente en AWS:



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

Resultado

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

Detalles sobre la instancia del agente de datos

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

Compatibilidad con Node.js

v21.2.0

Tipo de instancia

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

vCPU

4

RAM

16 GB

Sistema operativo

Amazon Linux 2023

Tamaño y tipo de disco

SSD GP2 de 10 GB

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

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

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

Regiones de Azure compatibles

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

Privilegios de root

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

Requisitos de red

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

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

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

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

Permisos necesarios para implementar el agente de datos en Azure

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Nota:

1. Los siguientes permisos solo son necesarios si planea habilitar el "Configuración de sincronización continua" en una relación de sincronización de Azure a otra ubicación de almacenamiento en la nube:
    - 'Microsoft.Storage/storageAccounts/read',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/write',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/leer',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/eliminar',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/acción',
    - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes/acción',
    - 'Microsoft.EventGrid/systemTopics/leer',
    - 'Microsoft.EventGrid/systemTopics/escritura',
    - 'Microsoft.EventGrid/systemTopics/eliminar',
    - 'Microsoft.EventGrid/eventSubscriptions/escritura',
    - 'Microsoft.Storage/storageAccounts/write'

    Además, el alcance asignable debe establecerse en el alcance de suscripción y **no** en el alcance del grupo de recursos si planea implementar sincronización continua en Azure.
2. Los siguientes permisos solo son necesarios si planea elegir su propia seguridad para la creación del agente de datos:
    - "Microsoft.Network/networkSecurityGroups/securityRules/read"
    - "Microsoft.Network/networkSecurityGroups/read"

Método de autenticación

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

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

Crear el agente de datos

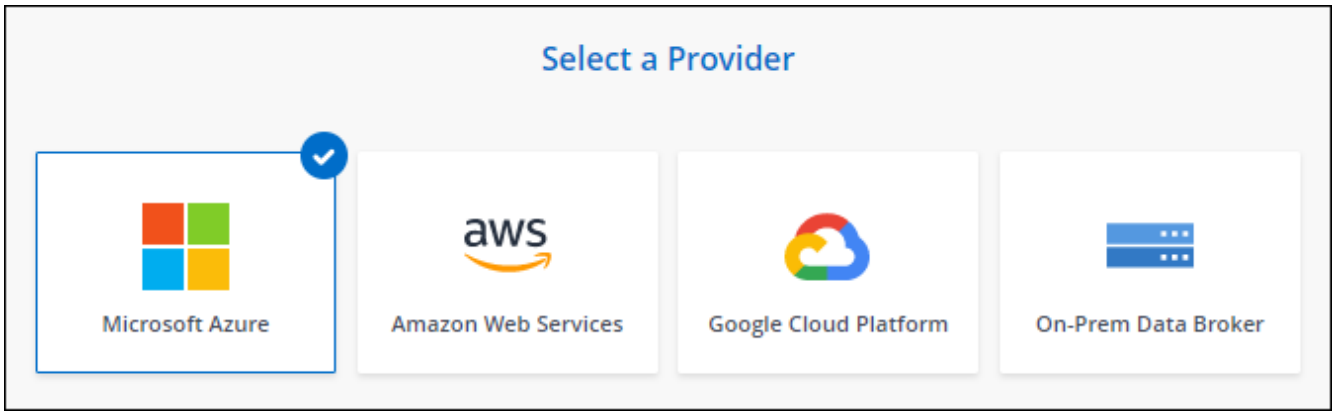
Hay algunas formas de crear un nuevo corredor de datos. Estos pasos describen cómo instalar un agente de datos en Azure cuando se crea una relación de sincronización.

Pasos

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

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

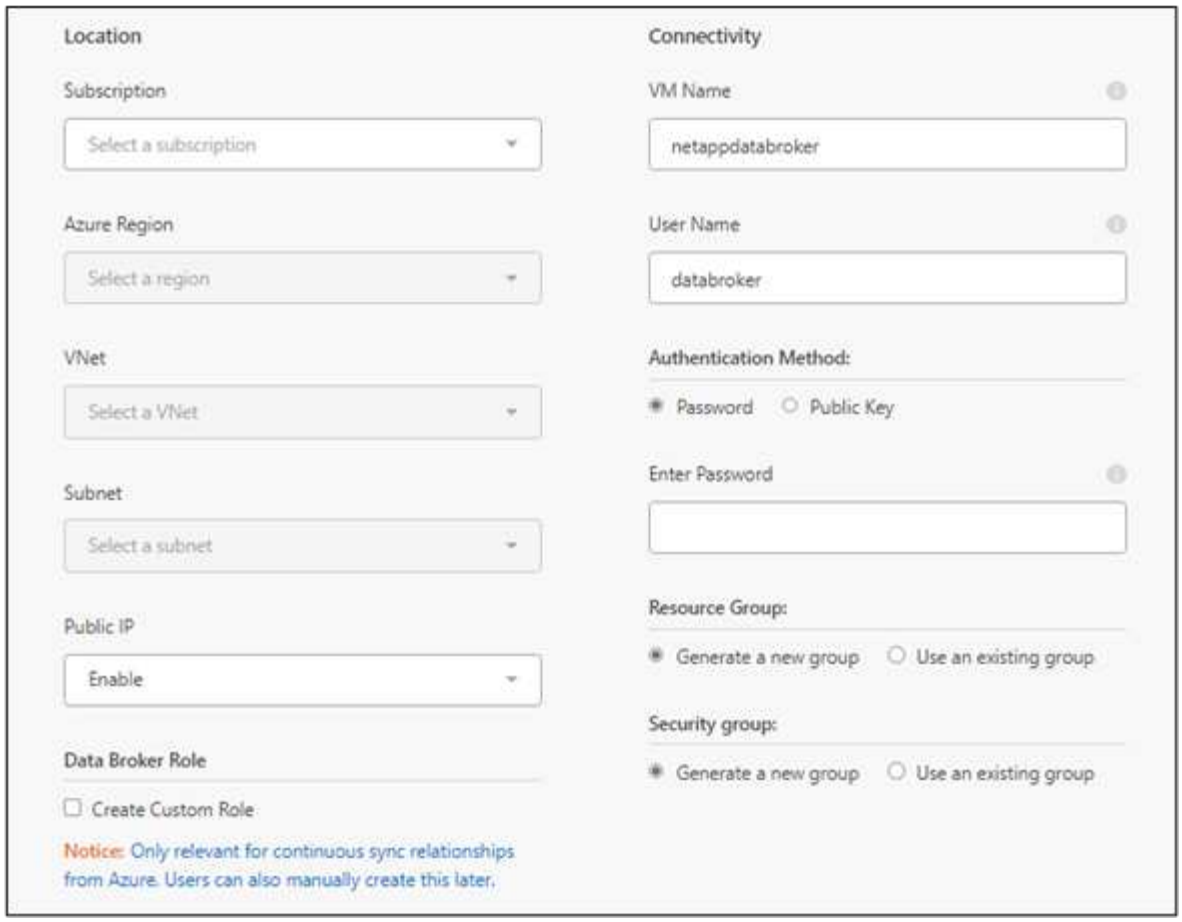
4. En la página **Grupo de agentes de datos**, seleccione **Crear agente de datos** y luego seleccione **Microsoft Azure**.



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

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

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



Si planea implementar una relación de sincronización continua, debe asignar un rol personalizado a su agente de datos. Esto también se puede hacer manualmente después de crear el bróker.

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

    El proceso puede tardar hasta 7 minutos.

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

Resultado

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

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

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

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

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

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

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

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

Detalles sobre la máquina virtual del agente de datos

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

Compatibilidad con Node.js
v21.2.0

Tipo de VM
Estándar DS4 v2

vCPU
8

RAM
28 GB

Sistema operativo
Rocky Linux 9,0

Tamaño y tipo de disco
SSD premium de 64 GB

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

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

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

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

Regiones de Google Cloud compatibles

Se admiten todas las regiones.

Privilegios de root

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

Requisitos de red

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

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

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

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

Permisos necesarios para implementar el agente de datos en Google Cloud

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

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

Permisos necesarios para la cuenta de servicio

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

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

Notas:

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

Crear el agente de datos

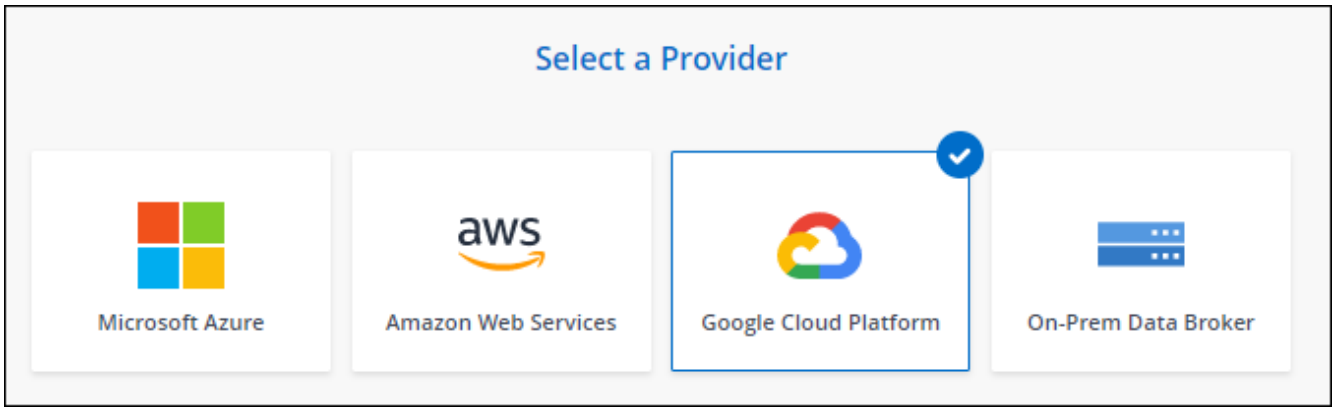
Hay algunas formas de crear un nuevo corredor de datos. Estos pasos describen cómo instalar un agente de datos en Google Cloud cuando se crea una relación de sincronización.

Pasos

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

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

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

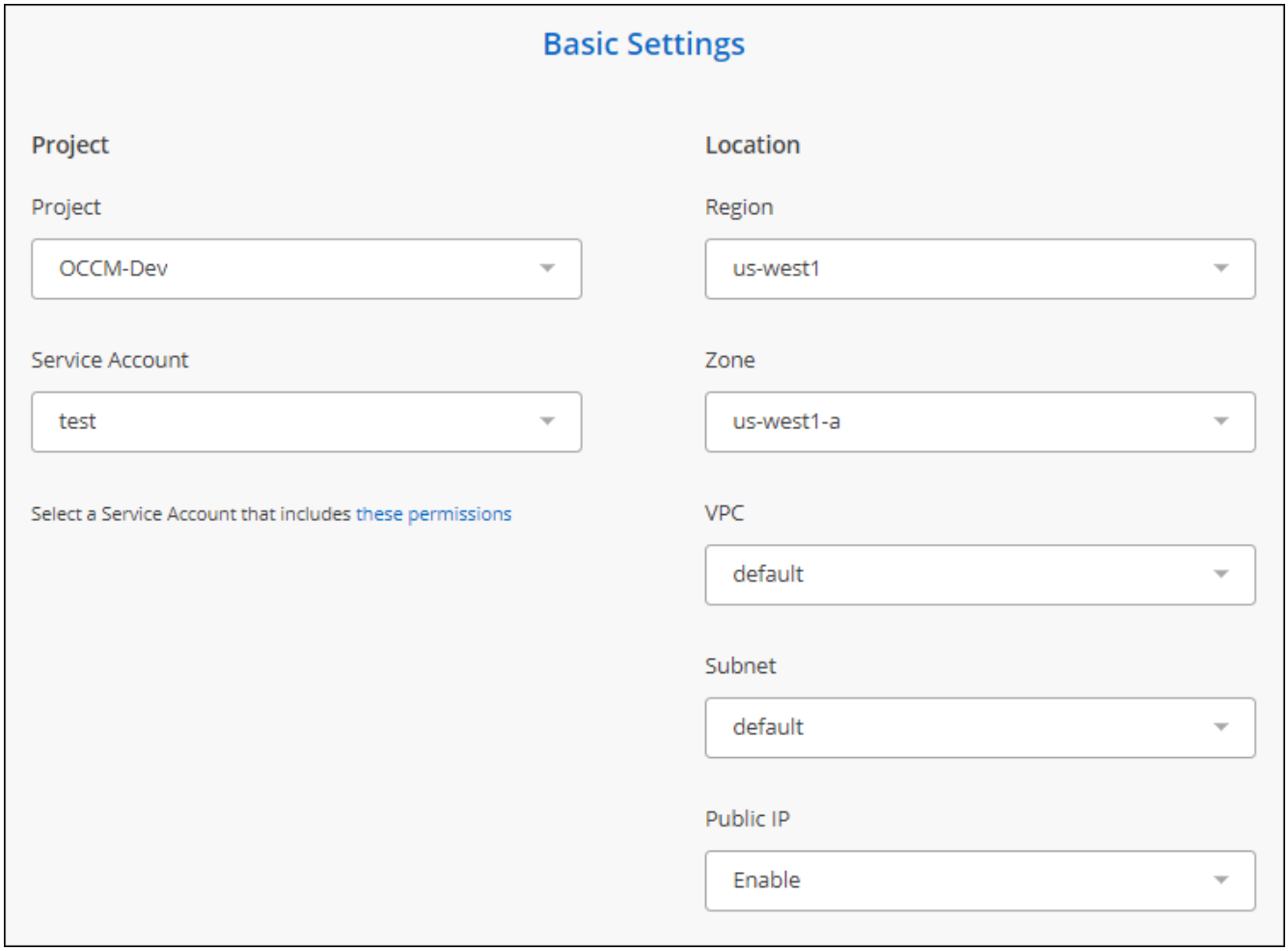


5. Ingrese un nombre para el agente de datos y seleccione **Continuar**.
6. Si se le solicita, inicie sesión con su cuenta de Google.

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

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

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



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

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

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

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

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

Resultado

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

Proporcionar permisos para usar buckets en otros proyectos de Google Cloud

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

Pasos

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

Resultado

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

Detalles sobre la instancia de VM del agente de datos

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

Compatibilidad con Node.js
v21.2.0

Tipo de máquina
n2-estándar-4

vCPU
4

RAM
15 GB

Sistema operativo
Rocky Linux 9,0

Tamaño y tipo de disco
Disco duro pd estándar de 20 GB

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

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

Requisitos del host Linux

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

- CentOS 8.0 y 8.5

  CentOS Stream no es compatible.

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

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

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

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

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

Privilegios de root

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

Requisitos de red

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

Habilitar el acceso a AWS

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

Pasos

1. Cree una política de IAM usando "Esta política proporcionada por NetApp"

   "Ver instrucciones de AWS"

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

   "Ver instrucciones de AWS"

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

Habilitar el acceso a Google Cloud

Si planea utilizar el agente de datos con una relación de sincronización que incluye un depósito de Google Cloud Storage, entonces debe preparar el host Linux para el acceso a Google Cloud. Cuando instale el agente de datos, deberá proporcionar una clave para una cuenta de servicio que tenga permisos específicos.

Pasos

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

   "Ver las instrucciones de Google Cloud"

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

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

3. Guarde el archivo JSON en el host Linux.

Habilitar el acceso a Microsoft Azure

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

Instalar el agente de datos

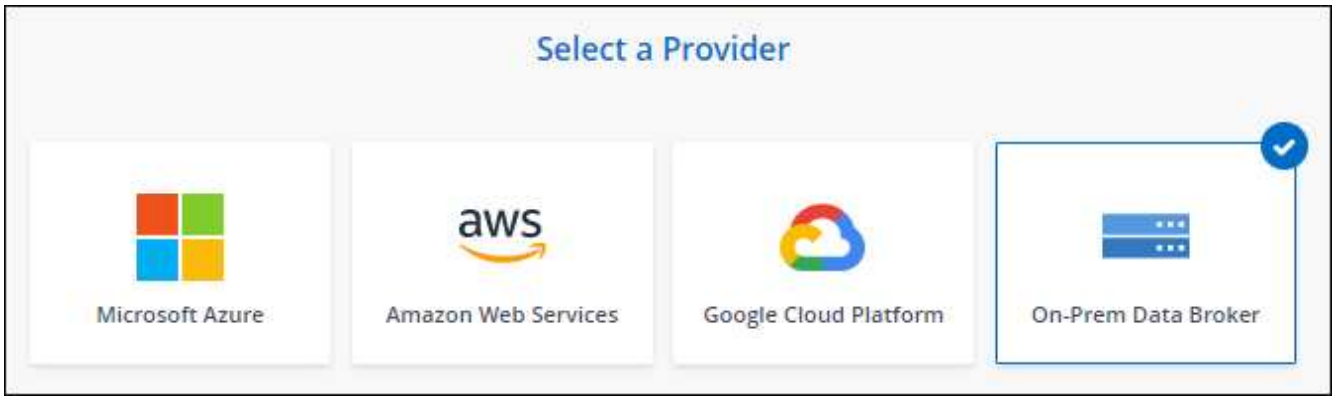
Puede instalar un agente de datos en un host Linux cuando crea una relación de sincronización.

Pasos

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

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

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



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

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

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

6. En la página de instrucciones:
   a. Seleccione si desea habilitar 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**.

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

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

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

   d. Descargar el instalador:
      - Sin proxy:

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

      - Utilice el servidor proxy:

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

      - Utilice un servidor proxy con autenticación:

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

        URI

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

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

> Cada comando enumerado a continuación incluye parámetros para el acceso a AWS y al acceso a Google Cloud. Siga la página de instrucciones para obtener el comando exacto según su opción de instalación.

- Sin configuración de proxy:

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

- Configuración de proxy:

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

- Configuración de proxy con autenticación:

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

Claves de AWS

Estas son las claves para el usuario que debes tener preparadassiguiendo estos pasos . Las claves de AWS se almacenan en el agente de datos, que se ejecuta en su red local o en la nube. NetApp no utiliza las claves fuera del agente de datos.

archivo JSON

Este es el archivo JSON que contiene una clave de cuenta de servicio que debería tener preparadasiguiendo estos pasos .

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