Instalar un agente de datos

NetApp Copy and Sync

NetApp
November 06, 2025

Tabla de contenidos

Instalar un agente de datos . . . 1
Cree un nuevo agente de datos en AWS para NetApp Copy and Sync . . . 1
Regiones de AWS compatibles . . . 1
Privilegios de root . . . 1
Requisitos de red . . . 1
Permisos necesarios para implementar el agente de datos en AWS . . . 1
Requisitos para usar su propio rol de IAM con el agente de datos de AWS . . . 1
Crear el agente de datos . . . 2
Detalles sobre la instancia del agente de datos . . . 4
Cree un nuevo agente de datos en Azure para NetApp Copy and Sync . . . 4
Regiones de Azure compatibles . . . 4
Privilegios de root . . . 4
Requisitos de red . . . 4
Permisos necesarios para implementar el agente de datos en Azure . . . 5
Método de autenticación . . . 7
Crear el agente de datos . . . 7
Detalles sobre la máquina virtual del agente de datos . . . 10
Cree un nuevo agente de datos en Google Cloud para NetApp Copy and Sync . . . 10
Regiones de Google Cloud compatibles . . . 11
Privilegios de root . . . 11
Requisitos de red . . . 11
Permisos necesarios para implementar el agente de datos en Google Cloud . . . 11
Permisos necesarios para la cuenta de servicio . . . 11
Crear el agente de datos . . . 12
Proporcionar permisos para usar buckets en otros proyectos de Google Cloud . . . 14
Detalles sobre la instancia de VM del agente de datos . . . 15
Instalar el agente de datos en un host Linux para NetApp Copy and Sync . . . 15
Requisitos del host Linux . . . 15
Privilegios de root . . . 16
Requisitos de red . . . 16
Habilitar el acceso a AWS . . . 16
Habilitar el acceso a Google Cloud . . . 17
Habilitar el acceso a Microsoft Azure . . . 17
Instalar el agente de datos . . . 17

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

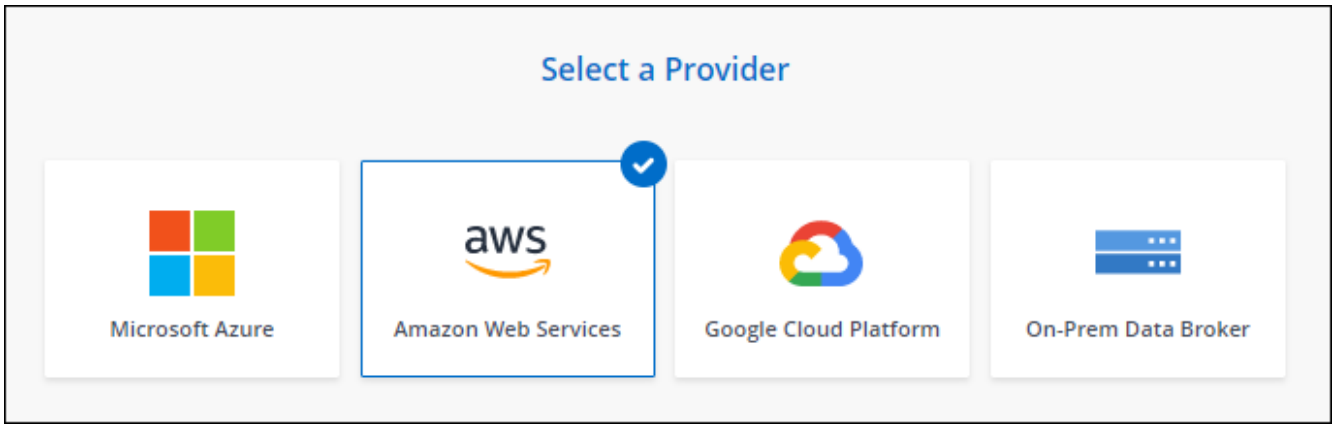
Hay algunas formas de crear un nuevo corredor de datos. Estos pasos describen cómo instalar un agente de datos en AWS al crear una relación de sincronización.

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.

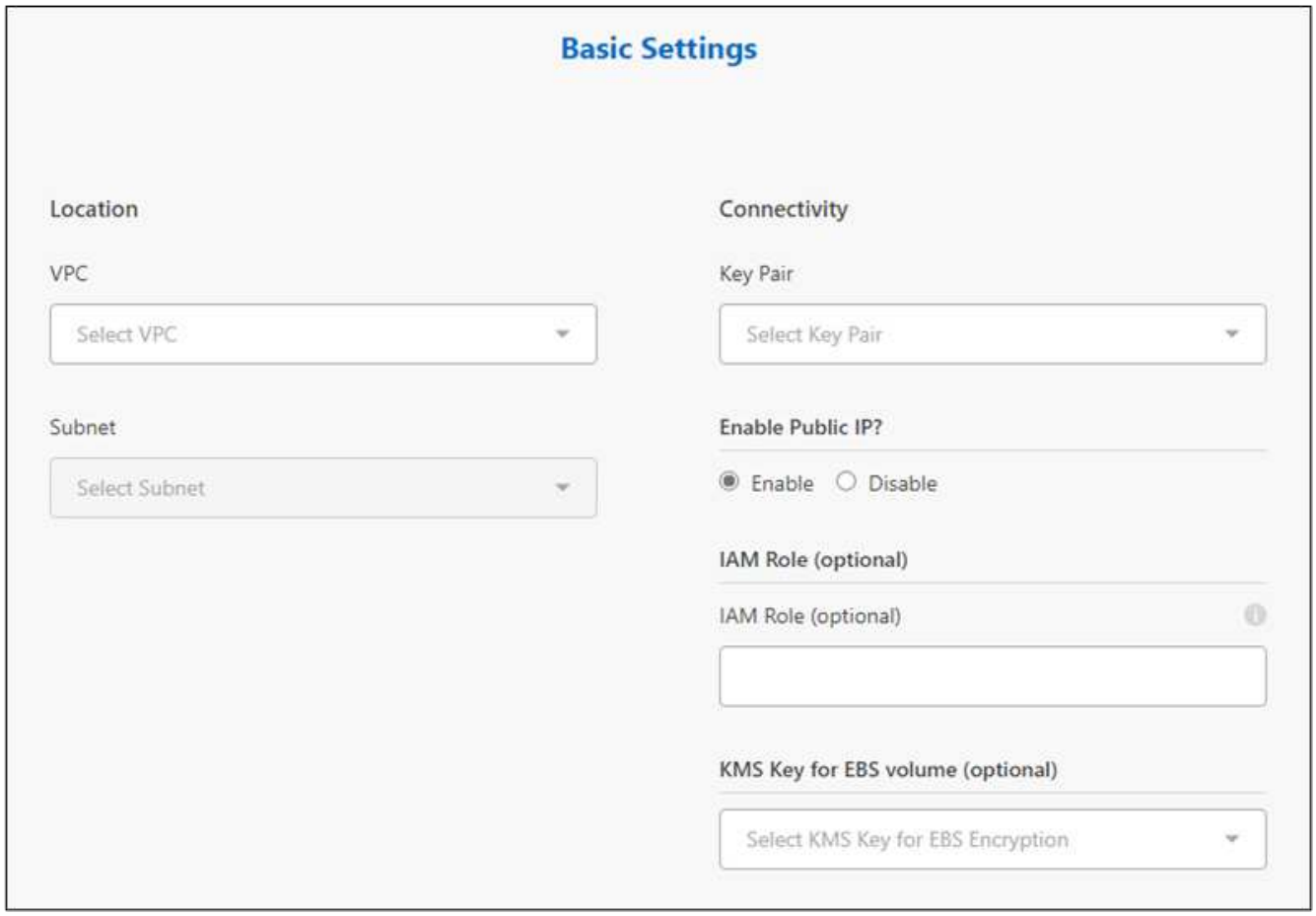
   El siguiente video muestra cómo iniciar la instancia del agente de datos utilizando una plantilla de CloudFormation:

   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

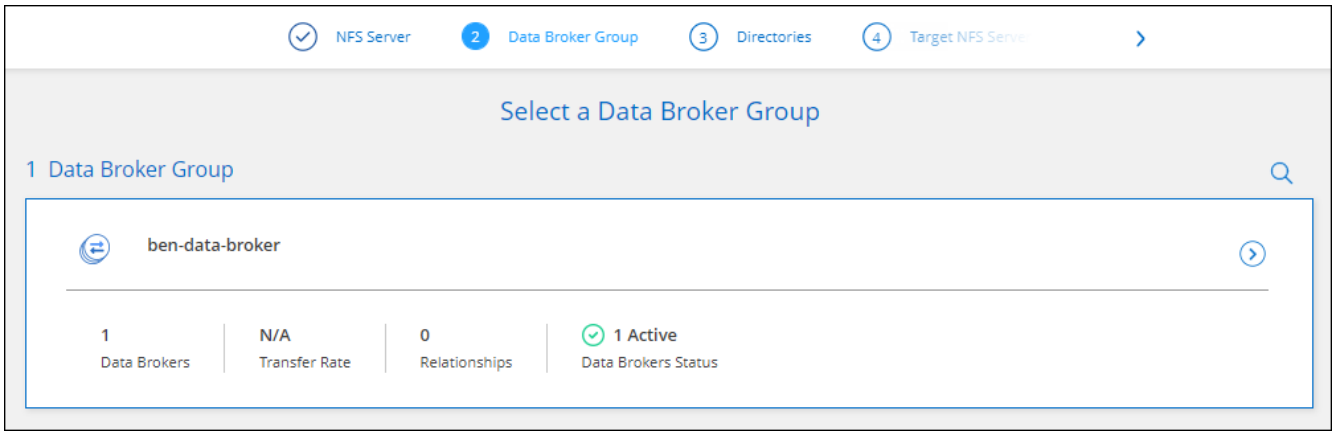
campo en blanco para que Copiar y sincronizar cree la función por usted. También tiene la opción de cifrar su agente de datos utilizando una clave KMS.

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

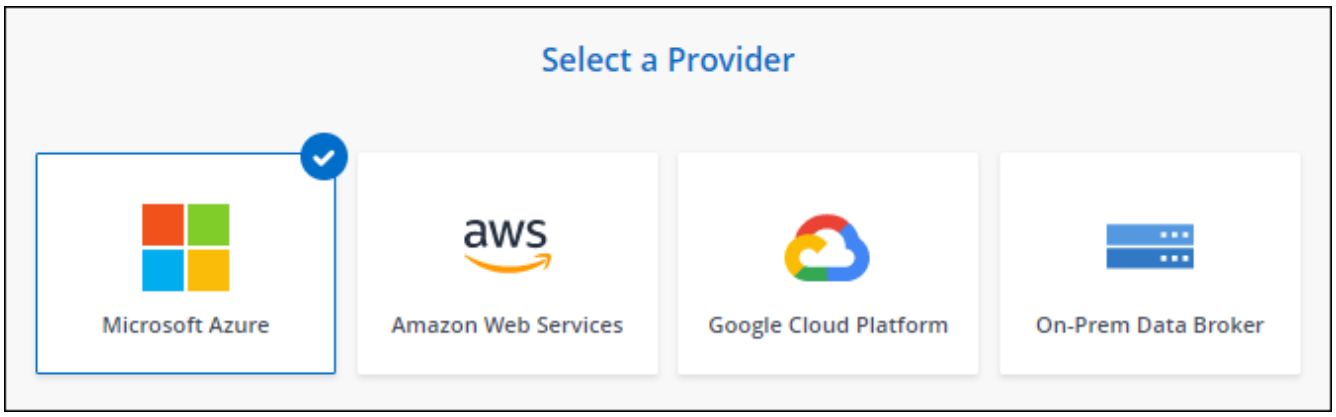
Hay algunas formas de crear un nuevo corredor de datos. Estos pasos describen cómo instalar un agente de datos en Azure cuando se crea una relación de sincronización.

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**.

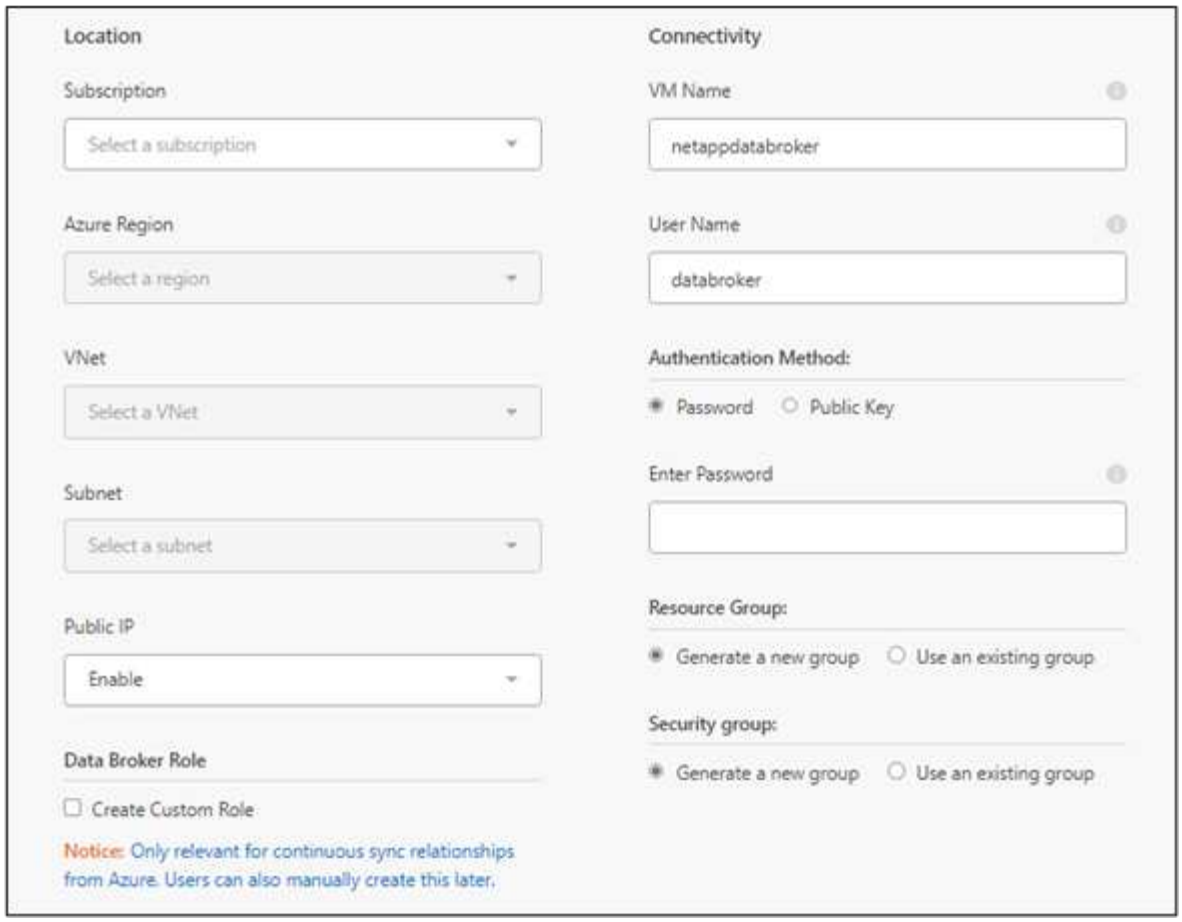
4. En la página **Grupo de agentes de datos**, seleccione **Crear agente de datos** y luego seleccione **Microsoft Azure**.



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

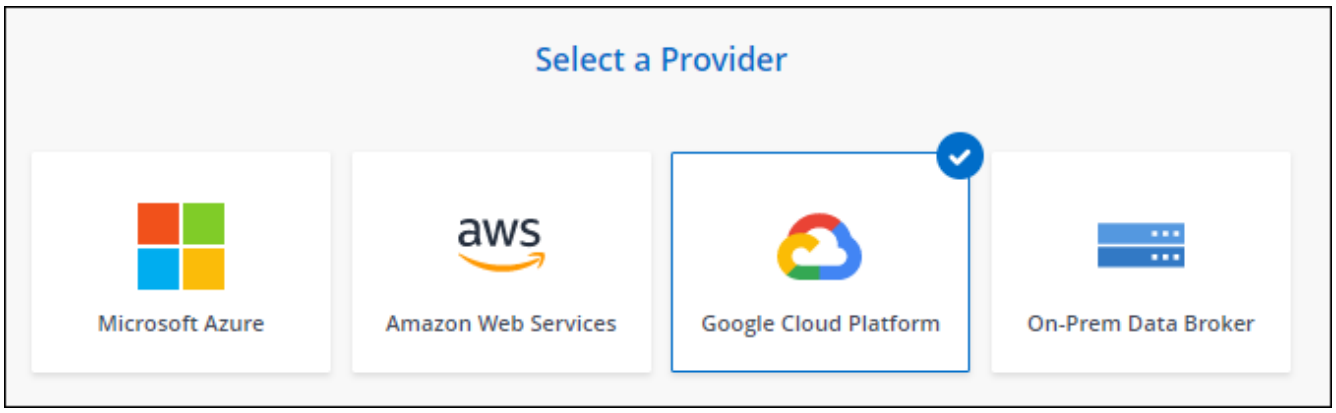
Hay algunas formas de crear un nuevo corredor de datos. Estos pasos describen cómo instalar un agente de datos en Google Cloud cuando se crea una relación de sincronización.

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**.

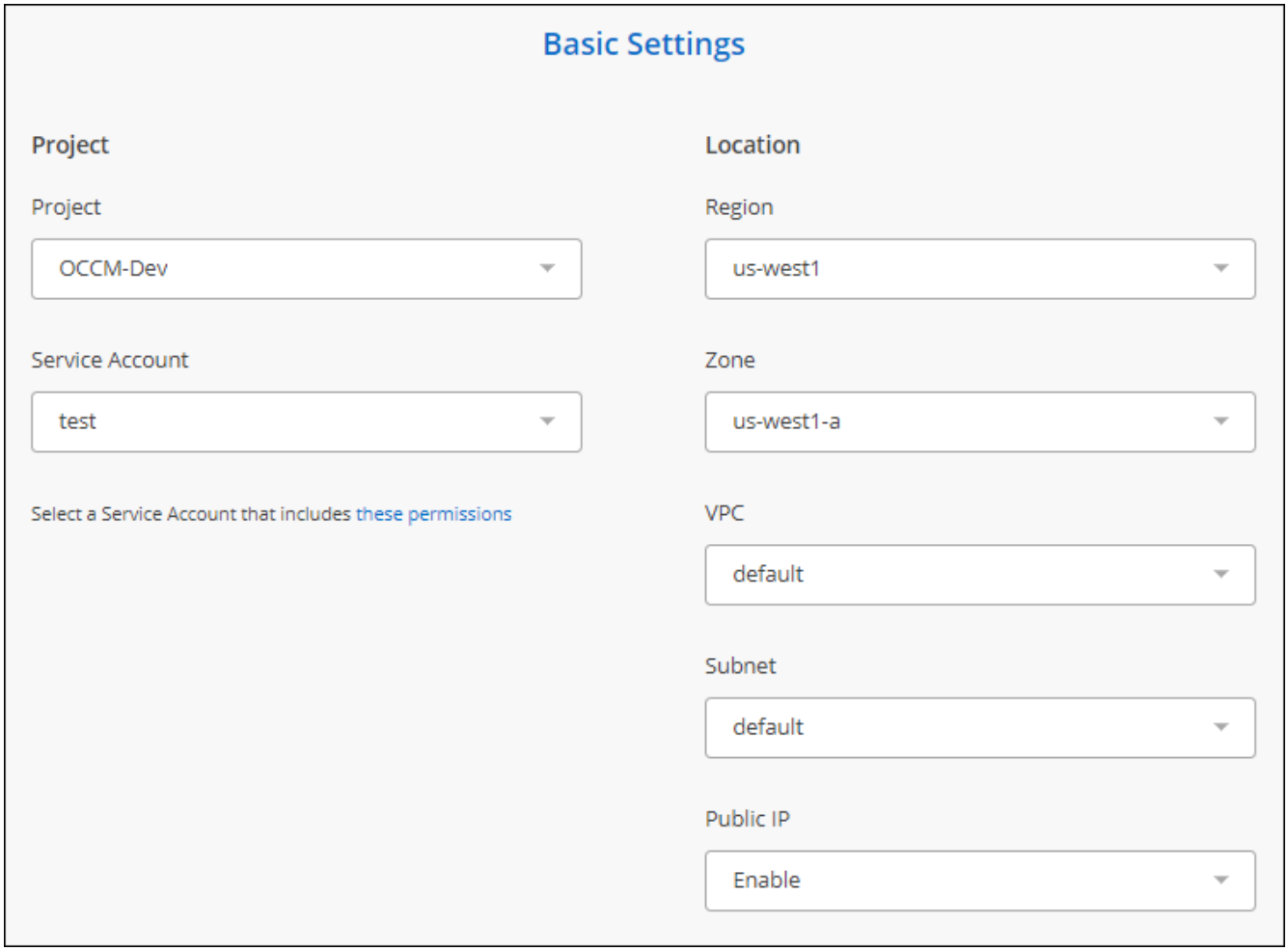


5. Ingrese un nombre para el agente de datos y seleccione **Continuar**.
6. Si se le solicita, inicie sesión con su cuenta de Google.

   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

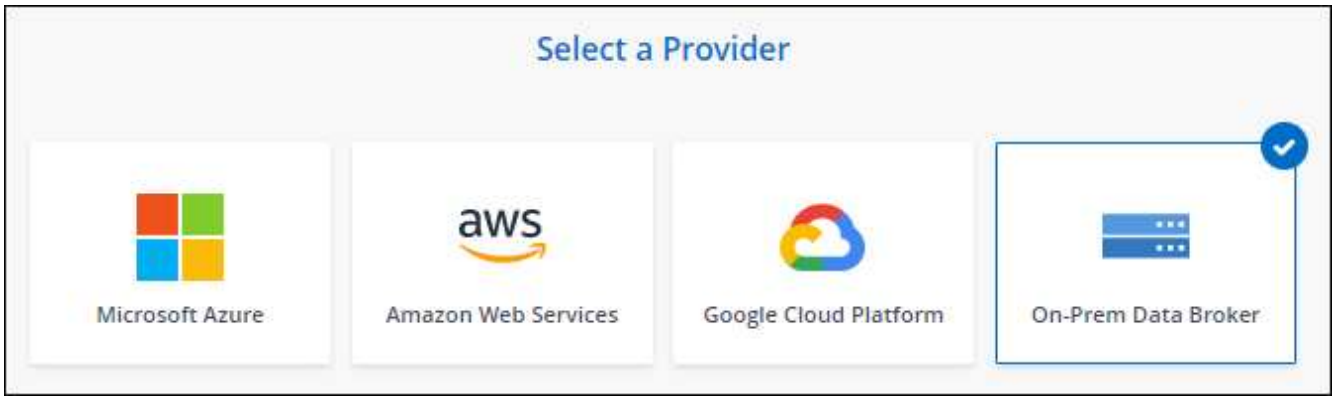
Puede instalar un agente de datos en un host Linux cuando crea una relación de sincronización.

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.