Instalar un agente de datos

BlueXP copy and sync

NetApp
August 13, 2024

Tabla de contenidos

Instalar un agente de datos

Cree un nuevo agente de datos en AWS

Al crear un nuevo grupo de agentes de datos, elija Amazon Web Services para implementar el software de agente de datos en una nueva instancia de EC2 en un VPC. La copia y sincronización de BlueXP te guía por el proceso de instalación, pero los requisitos y los pasos se repiten en esta página para ayudarte a preparar la instalación.

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

Regiones admitidas de AWS

Todas las regiones están soportadas excepto las regiones de China.

Privilegios de usuario raíz

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

Requisitos de red

- El agente de datos necesita una conexión a Internet de salida para que pueda sondear el servicio de copia y sincronización de BlueXP para tareas a través del puerto 443.

  Cuando la copia y sincronización de BlueXP pone en marcha el agente de datos en AWS, crea un grupo de seguridad que permite la comunicación saliente necesaria. Tenga en cuenta que puede configurar el agente de datos para que utilice un servidor proxy durante el proceso de instalación.

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

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

Permisos necesarios para implementar el agente de datos en AWS

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

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

Cuando la copia y sincronización de BlueXP implementa el agente de datos, crea un rol de IAM para la instancia de agente de datos. Si lo prefiere, puede implementar el agente de datos con su propio rol de IAM. Puede usar esta opción si su organización tiene políticas de seguridad estrictas.

El rol del IAM debe cumplir los siguientes requisitos:

- Se debe permitir al servicio EC2 asumir el rol IAM como entidad de confianza.

- "Los permisos definidos en este archivo JSON" Se debe adjuntar a la función IAM para que el intermediario de datos pueda funcionar correctamente.

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

Cree el agente de datos

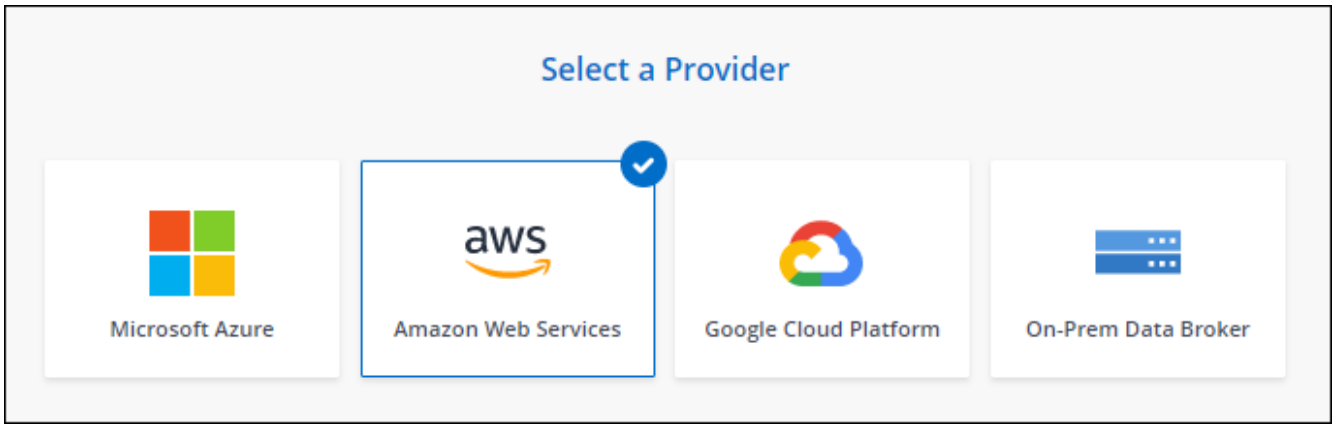
Hay varias formas de crear un nuevo agente de datos. Estos pasos describen cómo instalar un agente de datos en AWS al crear una relación de sincronización.

Pasos

1. Selecciona **Crear nueva sincronización**.
2. En la página **Definir relación de sincronización**, elige un origen y un destino y selecciona **Continuar**.

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

3. En la página **Data Broker Group**, selecciona **Crear Data Broker** y luego selecciona **Amazon Web Services**.



4. Introduzca un nombre para el broker de datos y seleccione **Continuar**.
5. Introduce una clave de acceso de AWS para que la copia y sincronización de BlueXP pueda crear el agente de datos en AWS en tu nombre.

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

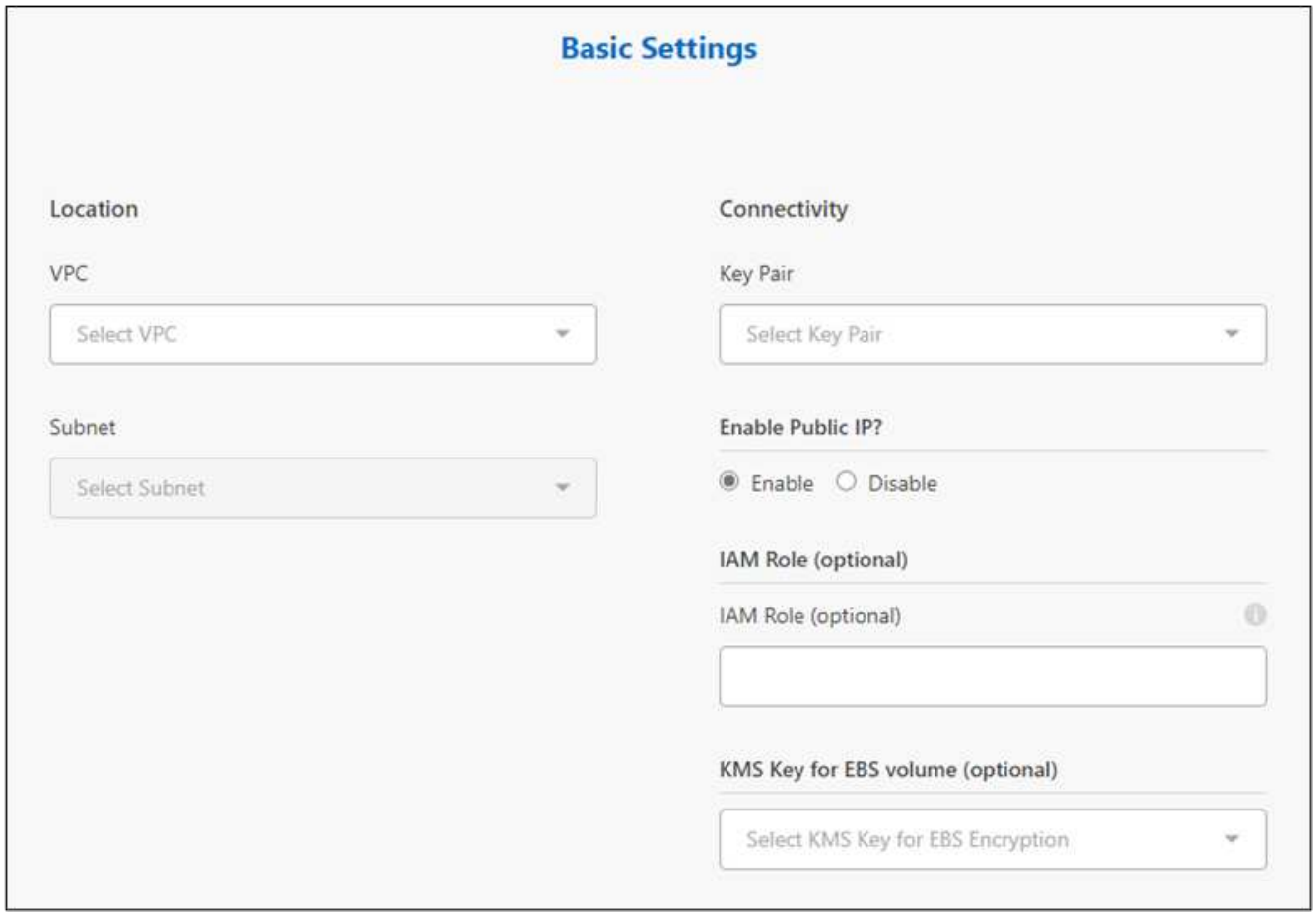
   Si prefiere no proporcionar claves de acceso, seleccione el enlace en la parte inferior de la página para usar una plantilla de CloudFormation en su lugar. Cuando usa esta opción, no necesita proporcionar credenciales, ya que inicia sesión directamente en AWS.

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

   ► https://docs.netapp.com/es-es/bluexp-copy-sync//media/video_cloud_sync.mp4 *(video)*

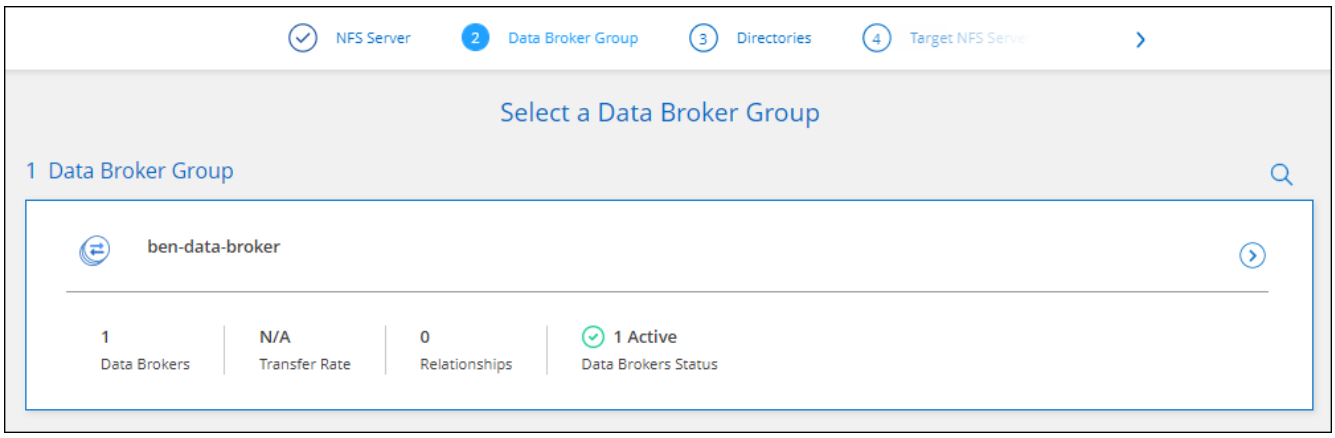
6. Si introdujo una clave de acceso de AWS, seleccione una ubicación para la instancia, seleccione un par de claves, elija si desea habilitar una dirección IP pública y seleccionar un rol de IAM existente o deje el campo en blanco para que la copia y sincronización de BlueXP creen el rol para usted. También tiene la opción de cifrar el agente de datos con una clave KMS.

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



7. Especifique una configuración de proxy, si se requiere un proxy para el acceso a Internet en el VPC.
8. Una vez que el agente de datos esté disponible, selecciona **Continuar** en la copia y sincronización de BlueXP.

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



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

Resultado

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

Detalles sobre la instancia de Data broker

La copia y sincronización de BlueXP crea un agente de datos en AWS mediante 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

De NetApp
Amazon Linux 2023

Tamaño y tipo del disco
SSD GP2 DE 10 GB

Cree un nuevo agente de datos en Azure

Al crear un nuevo grupo de agentes de datos, elija Microsoft Azure para implementar el software de Data broker en una nueva máquina virtual en un vnet. La copia y sincronización de BlueXP te guía por el proceso de instalación, pero los requisitos y los pasos se repiten en esta página para ayudarte a preparar la instalación.

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

Regiones de Azure compatibles

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

Privilegios de usuario raíz

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

Requisitos de red

- El agente de datos necesita una conexión a Internet de salida para que pueda sondear el servicio de copia y sincronización de BlueXP para tareas a través del puerto 443.

  Cuando la copia y sincronización de BlueXP pone en marcha el agente de datos en Azure, crea un grupo de seguridad que permite la comunicación saliente necesaria.

  Si necesita limitar la conectividad saliente, consulte "lista de puntos finales con los que se contacta el data

broker".

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

Permisos necesarios para implementar el agente de datos en Azure

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

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

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

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

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

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Resources/deployments/cancel/action",
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/publicIPAddresses/delete",

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

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

```
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/publicIPAddresses/read",

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

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

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

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

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

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

"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 activar el "Ajuste de sincronización continua" En una relación de sincronización de Azure con otra ubicación de almacenamiento en cloud:

- "Microsoft.Storage/storageAccounts/read",
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/Write',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/read',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/DELETE',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes/action',
- 'Microsoft.EventGrid/systemTopics/Read',
- 'Microsoft.EventGrid/systemTopics/Write',
- 'Microsoft.EventGrid/systemTopics/DELETE',
- 'Microsoft.EventGrid/eventSubscriptions/Write',
- 'Microsoft.almacenamiento/cuentas de almacenamiento/escritura'

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

2. Los siguientes permisos solo son necesarios si planea elegir su propia seguridad para la creación de Data Broker:
   - «Microsoft.Network/networkSecurityGroups/securityRules/read"
   - «Microsoft.Network/networkSecurityGroups/read"

Método de autenticación

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

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

Cree el agente de datos

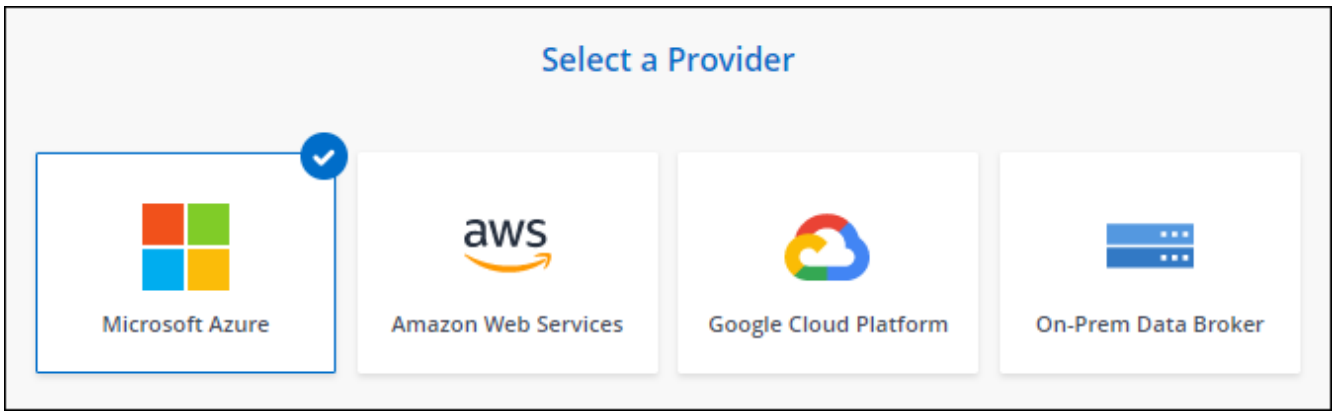
Hay varias formas de crear un nuevo agente de datos. Estos pasos describen cómo instalar un agente de datos en Azure al crear una relación de sincronización.

Pasos

1. Selecciona **Crear nueva sincronización**.
2. En la página **Definir relación de sincronización**, elige un origen y un destino y selecciona **Continuar**.

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

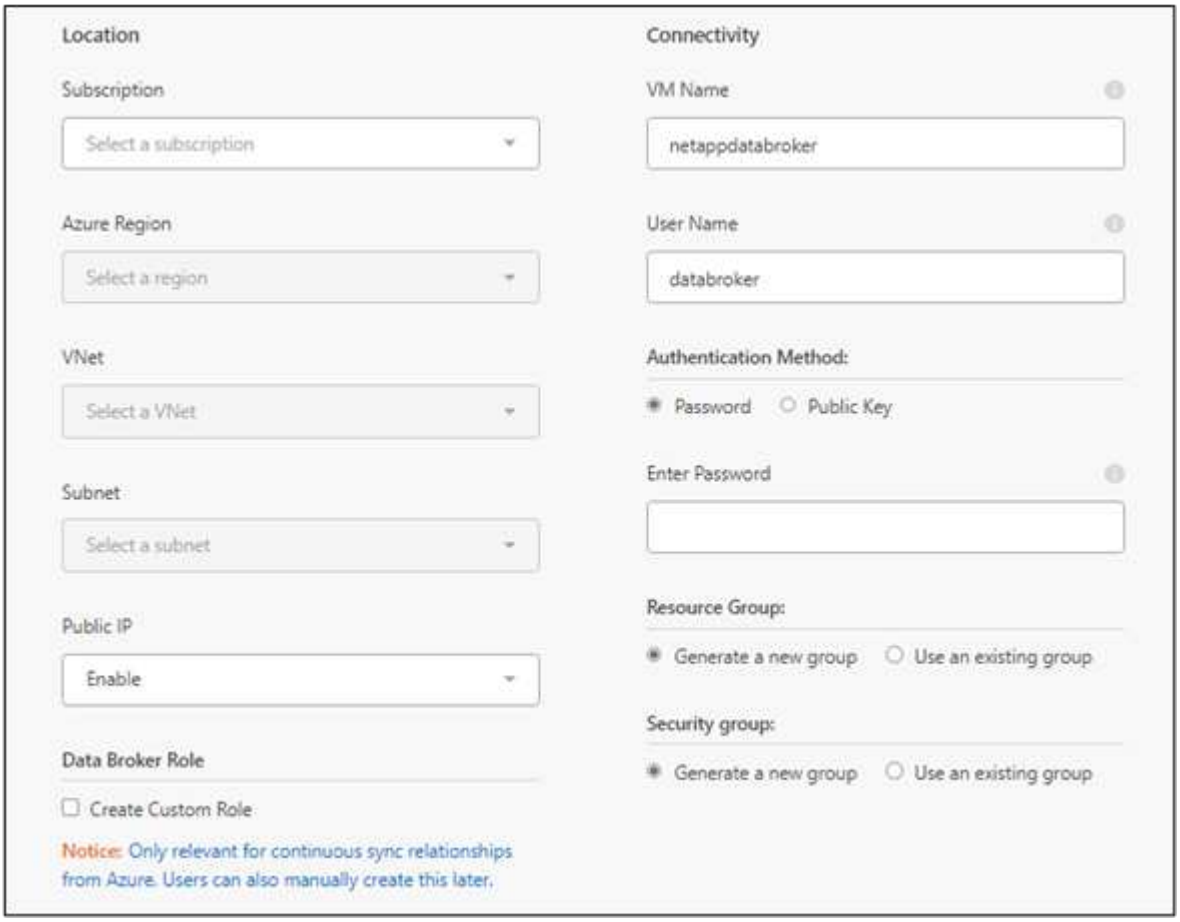
3. En la página **Data Broker Group**, selecciona **Crear Data Broker** y luego selecciona **Microsoft Azure**.



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

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

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



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

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

   El proceso puede tardar hasta 7 minutos.

10. En la copia y sincronización de BlueXP, selecciona **Continuar** una vez que el agente de datos esté disponible.
11. Complete las páginas del asistente para crear la nueva relación de sincronización.

Resultado

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

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

Si Microsoft te notifica que se requiere aprobación de administrador porque la copia y sincronización de BlueXP necesitan permiso para acceder a los recursos de tu organización en tu nombre, tienes dos opciones:

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

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

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

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

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

Información sobre el equipo virtual de Data broker

La copia y sincronización de BlueXP crea un agente de datos en Azure con la siguiente configuración.

Compatibilidad con Node.js

v21,2.0

Tipo de máquina virtual

Estándar DS4 v2

VCPU
8

RAM
28 GB

De NetApp
Rocky Linux 9.0

Tamaño y tipo del disco
SSD Premium de 64 GB

Cree un nuevo agente de datos en Google Cloud

Al crear un nuevo grupo de agentes de datos, elija Google Cloud Platform para implementar el software de agente de datos en una nueva instancia de máquina virtual en Google Cloud VPC. La copia y sincronización de BlueXP te guía por el proceso de instalación, pero los requisitos y los pasos se repiten en esta página para ayudarte a preparar la instalación.

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

Regiones compatibles de Google Cloud

Se admiten todas las regiones.

Privilegios de usuario raíz

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

Requisitos de red

- El agente de datos necesita una conexión a Internet de salida para que pueda sondear el servicio de copia y sincronización de BlueXP para tareas a través del puerto 443.

  Cuando la copia y sincronización de BlueXP pone en marcha el agente de datos en Google Cloud, crea un grupo de seguridad que permite establecer la comunicación saliente necesaria.

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

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

Permisos necesarios para implementar el agente de datos en Google Cloud

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

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

Permisos necesarios para la cuenta de servicio

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

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

Notas:

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

3. Los permisos «cloudkms.cryptoKeys.list» y «cloudkms.keyrings.list» solo son necesarios si planea utilizar una clave KMS gestionada por el cliente en un depósito de Google Cloud Storage de destino.

Cree el agente de datos

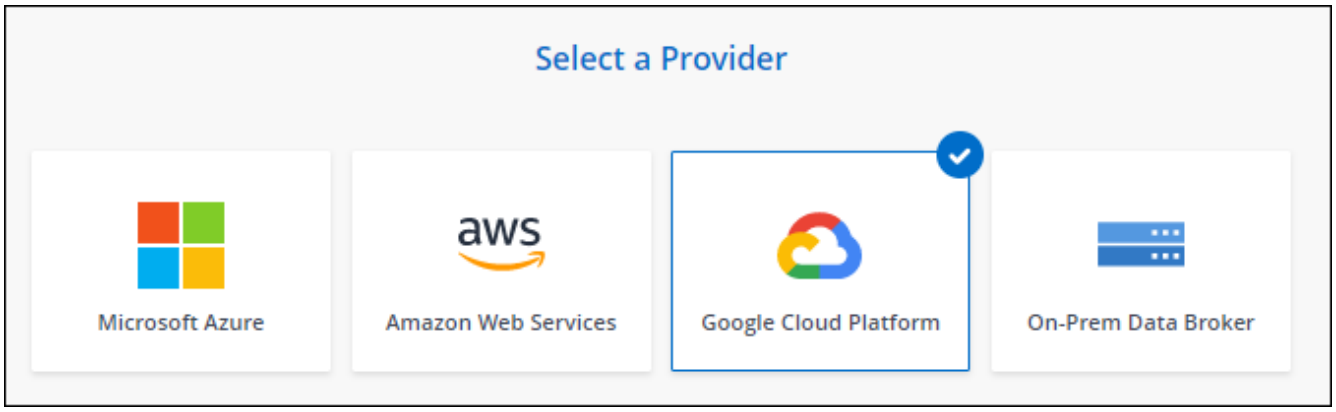
Hay varias formas de crear un nuevo agente de datos. Estos pasos describen cómo instalar un agente de datos en Google Cloud al crear una relación de sincronización.

Pasos

1. Selecciona **Crear nueva sincronización**.
2. En la página **Definir relación de sincronización**, elige un origen y un destino y selecciona **Continuar**.

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

3. En la página **Data Broker Group**, selecciona **Crear Data Broker** y luego selecciona **Google Cloud Platform**.

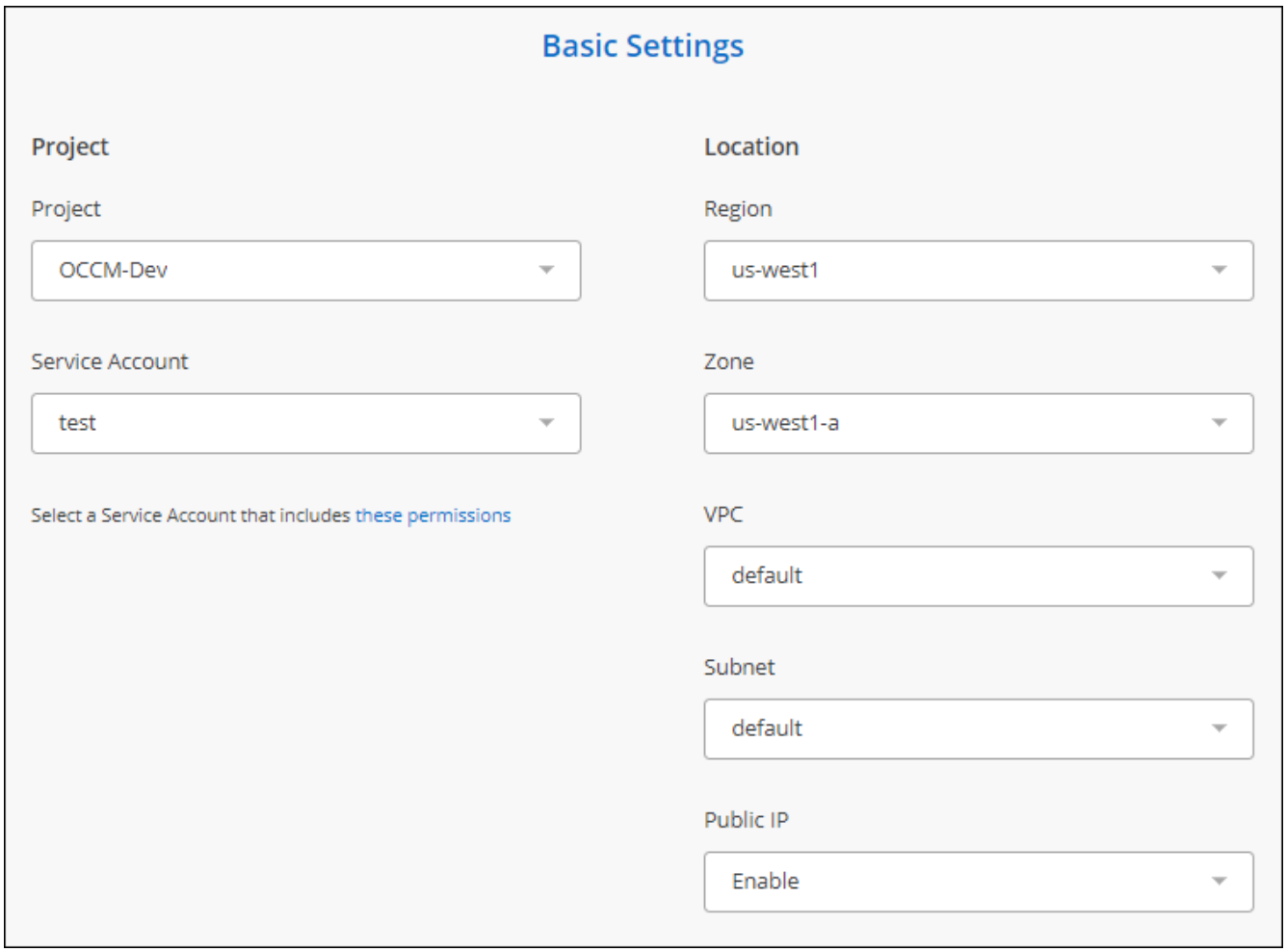


4. Introduzca un nombre para el broker de datos y seleccione **Continuar**.
5. Si se le solicita, inicie sesión con su cuenta de Google.

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

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

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



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

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

8. Una vez que el agente de datos esté disponible, selecciona **Continuar** en la copia y sincronización de BlueXP.

   La puesta en marcha de la instancia tarda entre 5 y 10 minutos, aproximadamente. Puede supervisar el progreso en el servicio de copia y sincronización de BlueXP, que se actualiza automáticamente cuando la instancia esté disponible.

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

Resultado

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

Proporcionar permisos para usar buckets en otros proyectos de Google Cloud

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

Pasos

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

Resultado

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

Detalles sobre la instancia de VM de Data broker

La copia y sincronización de BlueXP crea un agente de datos en Google Cloud mediante la siguiente configuración.

Compatibilidad con Node.js

v21,2.0

Tipo de máquina

n2-estándar-4

VCPU

4

RAM

15 GB

De NetApp

Rocky Linux 9.0

Tamaño y tipo del disco

Disco duro de 20 GB, estándar pd

Instale el agente de datos en un host Linux

Cuando crea un nuevo grupo de agentes de datos, elija la opción On-Prem Data Broker para instalar el software de agente de datos en un host Linux local o en un host Linux existente en el cloud. La copia y sincronización de BlueXP te guía por el proceso de instalación, pero los requisitos y los pasos se repiten en esta página para ayudarte a preparar la instalación.

Requisitos del host Linux

- **Compatibilidad 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 y 8,9
  - Rocky Linux 9
  - Sistema operativo Ubuntu Server 20.04 LTS
  - SUSE Linux Enterprise Server 15 SP1

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

  Debe registrarse un sistema Red Hat Enterprise Linux con Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software necesario de terceros durante la instalación.
- **RAM**: 16 GB
- **CPU**: 4 núcleos
- **espacio libre en disco**: 10 GB
- **SELinux**: Le recomendamos que desactive la función "SELinux" en el host.

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

Privilegios de usuario raíz

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

Requisitos de red

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

Permita el acceso a AWS

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

Pasos

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

   "Consulte las instrucciones de AWS"

2. Cree un usuario IAM con acceso mediante programación.

   "Consulte las instrucciones de AWS"

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

Habilitar el acceso a Google Cloud

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

Pasos

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

   "Vea las instrucciones de Google Cloud"

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

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

3. Guarde el archivo JSON en el host Linux.

Permita el acceso a Microsoft Azure

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

Instale el agente de datos

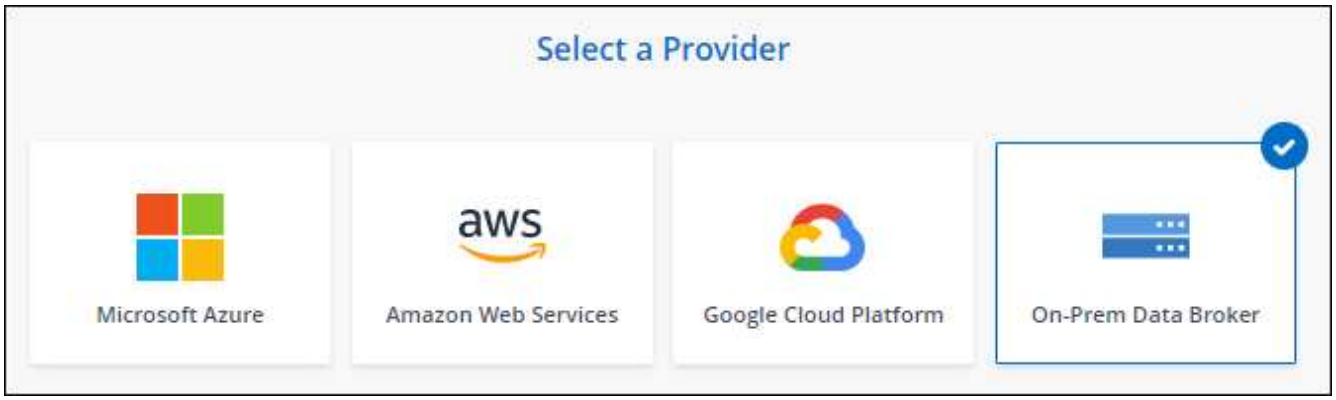
Puede instalar un agente de datos en un host Linux al crear una relación de sincronización.

Pasos

1. Selecciona **Crear nueva sincronización**.
2. En la página **Definir relación de sincronización**, elige un origen y un destino y selecciona **Continuar**.

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

3. En la página **Data Broker Group**, selecciona **Create Data Broker** y luego selecciona **On-Prem Data Broker**.



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

4. Introduzca un nombre para el broker de datos y seleccione **Continuar**.

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

5. En la página de instrucciones:
   a. Seleccione si desea activar el acceso a **AWS**, **Google Cloud** o ambos.
   b. Seleccione una opción de instalación: **sin proxy**, **usar servidor proxy** o **usar servidor proxy con autenticación**.

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

   c. Utilice los comandos para descargar e instalar el Data broker.

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

   d. Descargue el instalador:
      - Sin proxy:

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

      - Usar servidor proxy:

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

      - Utilice el servidor proxy con autenticación:

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

        URI

        La copia y sincronización de BlueXP muestra el URI del archivo de instalación en la página de instrucciones, que se carga cuando sigue las instrucciones para implementar el agente de datos en las instalaciones. Ese URI no se repite aquí porque el enlace se genera dinámicamente y sólo se puede usar una vez. Sigue estos pasos para obtener el URI de copia y sincronización de BlueXP.

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

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

- Sin configuración de proxy:

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

- Configuración de proxy:

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

- Configuración del proxy con autenticación:

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

Claves de AWS

Estas son las claves para el usuario que debes haber preparado siga estos pasos. Las claves de AWS se almacenan en el agente de datos, que se ejecuta en la red local o en el cloud. NetApp no utiliza las claves fuera del agente de datos.

Archivo JSON

Este es el archivo JSON que contiene una clave de cuenta de servicio que debe haber preparado siga estos pasos.

6. Una vez que el agente de datos esté disponible, selecciona **Continuar** en la copia y sincronización de BlueXP.
7. Complete las páginas del asistente para crear la nueva relación de sincronización.