



# **Installare un data broker**

## **BlueXP copy and sync**

NetApp

September 23, 2024

# Sommario

- Installare un data broker. . . . . 1
  - Crea un nuovo broker di dati in AWS . . . . . 1
  - Crea un nuovo broker di dati in Azure . . . . . 4
  - Crea un nuovo broker di dati in Google Cloud . . . . . 10
  - Installare il broker di dati su un host Linux . . . . . 14

# Installare un data broker

## Crea un nuovo broker di dati in AWS

Quando crei un nuovo gruppo di broker di dati, scegli Amazon Web Services per implementare il software di broker di dati su una nuova istanza EC2 in un VPC. BlueXP copy and Sync guida l'utente attraverso il processo di installazione, ma i requisiti e i passaggi sono ripetuti in questa pagina per aiutarti a prepararti all'installazione.

È inoltre possibile installare il data broker su un host Linux esistente nel cloud o on-premise. ["Scopri di più"](#).

### Regioni AWS supportate

Tutte le regioni sono supportate, ad eccezione delle regioni della Cina.

### Privilegi root

Il software del data broker viene eseguito automaticamente come root sull'host Linux. L'esecuzione come root è un requisito per le operazioni di data broker. Ad esempio, per montare condivisioni.

### Requisiti di rete

- Il broker di dati necessita di una connessione Internet in uscita in modo che possa eseguire il polling del servizio di copia e sincronizzazione BlueXP per le attività sulla porta 443.

Quando BlueXP copy and Sync implementa il data broker in AWS, crea un gruppo di sicurezza che abilita la comunicazione in uscita richiesta. Nota: È possibile configurare il data broker per l'utilizzo di un server proxy durante il processo di installazione.

Per limitare la connettività in uscita, vedere ["l'elenco degli endpoint a cui il data broker contatta"](#).

- NetApp consiglia di configurare l'origine, la destinazione e il data broker per utilizzare un servizio NTP (Network Time Protocol). La differenza di tempo tra i tre componenti non deve superare i 5 minuti.

### Autorizzazioni necessarie per implementare il data broker in AWS

L'account utente AWS utilizzato per implementare il data broker deve disporre delle autorizzazioni incluse in ["Questa policy fornita da NetApp"](#).

### requisiti per utilizzare il tuo ruolo IAM con il data broker AWS

Quando BlueXP copia e sincronizza implementa il data broker, crea un ruolo IAM per l'istanza del data broker. Se preferisci, puoi implementare il data broker utilizzando il tuo ruolo IAM. È possibile utilizzare questa opzione se l'organizzazione dispone di policy di sicurezza rigorose.

Il ruolo IAM deve soddisfare i seguenti requisiti:

- Il servizio EC2 deve essere autorizzato ad assumere il ruolo di IAM come entità attendibile.
- ["Le autorizzazioni definite in questo file JSON"](#) Deve essere associato al ruolo IAM in modo che il data broker possa funzionare correttamente.

Seguire i passaggi riportati di seguito per specificare il ruolo IAM durante l'implementazione del data broker.

## Creare il broker di dati

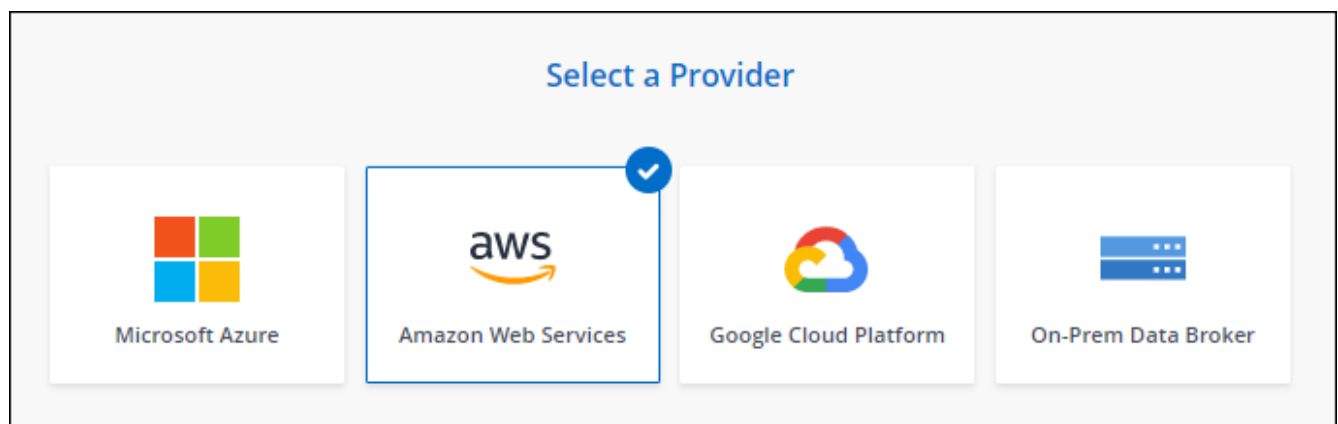
Esistono diversi modi per creare un nuovo data broker. Questi passaggi descrivono come installare un data broker in AWS quando si crea una relazione di sincronizzazione.

### Fasi

1. Selezionare **Crea nuova sincronizzazione**.
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione e selezionare **continua**.

Completa i passaggi fino a raggiungere la pagina **Data Broker Group**.

3. Nella pagina **Data Broker Group**, selezionare **Create Data Broker**, quindi selezionare **Amazon Web Services**.



4. Immettere un nome per il data broker e selezionare **continua**.
5. Inserire una chiave di accesso AWS in modo che la copia e la sincronizzazione BlueXP possano creare il data broker in AWS per tuo conto.

Le chiavi non vengono salvate o utilizzate per altri scopi.

Se invece non si desidera fornire le chiavi di accesso, selezionare il collegamento in fondo alla pagina per utilizzare un modello CloudFormation. Quando si utilizza questa opzione, non è necessario fornire le credenziali perché si effettua l'accesso direttamente ad AWS.

il seguente video mostra come avviare l'istanza del data broker utilizzando un modello CloudFormation:

► [https://docs.netapp.com/it-it/bluexp-copy-sync//media/video\\_cloud\\_sync.mp4](https://docs.netapp.com/it-it/bluexp-copy-sync//media/video_cloud_sync.mp4) (video)

6. Se è stata inserita una chiave di accesso AWS, selezionare una posizione per l'istanza, selezionare una coppia di chiavi, scegliere se attivare un indirizzo IP pubblico e selezionare un ruolo IAM esistente oppure lasciare vuoto il campo in modo che BlueXP copy and Sync crei il ruolo per te. È inoltre possibile crittografare il data broker utilizzando una chiave KMS.

Se scegli il tuo ruolo IAM, è **necessario fornire le autorizzazioni necessarie**.

### Basic Settings

**Location**

VPC

Select VPC

Subnet

Select Subnet

**Connectivity**

Key Pair

Select Key Pair

**Enable Public IP?**

Enable  Disable

**IAM Role (optional)**

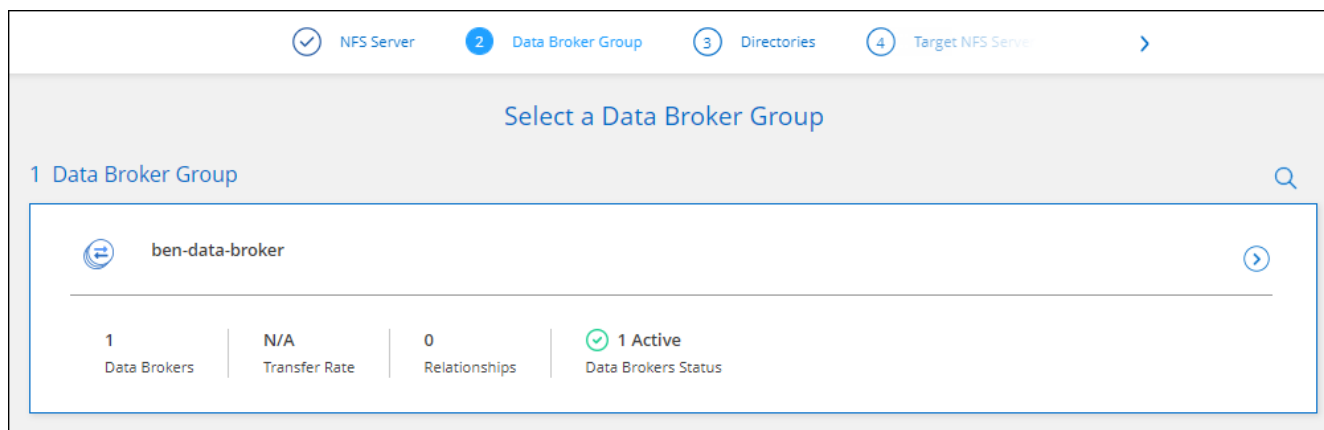
IAM Role (optional) ⓘ

**KMS Key for EBS volume (optional)**

Select KMS Key for EBS Encryption

7. Specificare una configurazione proxy, se è richiesto un proxy per l'accesso a Internet nel VPC.
8. Una volta disponibile il data broker, selezionare **Continue** (continua) in BlueXP copy and Sync (Copia e sincronizza BlueXP).

L'immagine seguente mostra un'istanza implementata correttamente in AWS:



9. Completare le pagine della procedura guidata per creare la nuova relazione di sincronizzazione.

### Risultato

Hai implementato un data broker in AWS e creato una nuova relazione di sincronizzazione. È possibile utilizzare questo gruppo di broker di dati con ulteriori relazioni di sincronizzazione.

## Dettagli sull'istanza del data broker

BlueXP copy and Sync crea un data broker in AWS utilizzando la seguente configurazione.

### Compatibilità Node.js

v21,2.0

### Tipo di istanza

m5n.xlarge se disponibile nella regione, altrimenti m5.xlarge

### VCPU

4

### RAM

16 GB

### Sistema operativo

Amazon Linux 2023

### Dimensione e tipo di disco

SSD GP2 DA 10 GB

## Crea un nuovo broker di dati in Azure

Quando si crea un nuovo gruppo di broker di dati, scegliere Microsoft Azure per implementare il software di broker di dati su una nuova macchina virtuale in una VNET. BlueXP copy and Sync guida l'utente attraverso il processo di installazione, ma i requisiti e i passaggi sono ripetuti in questa pagina per aiutarti a prepararti all'installazione.

È inoltre possibile installare il data broker su un host Linux esistente nel cloud o on-premise. ["Scopri di più"](#).

### Aree Azure supportate

Sono supportate tutte le regioni, ad eccezione di quelle della Cina, degli Stati Uniti e del DOD.

### Privilegi root

Il software del data broker viene eseguito automaticamente come root sull'host Linux. L'esecuzione come root è un requisito per le operazioni di data broker. Ad esempio, per montare condivisioni.

### Requisiti di rete

- Il broker di dati necessita di una connessione Internet in uscita in modo che possa eseguire il polling del servizio di copia e sincronizzazione BlueXP per le attività sulla porta 443.

Quando BlueXP copy and Sync implementa il data broker in Azure, crea un gruppo di sicurezza che abilita la comunicazione in uscita richiesta.

Per limitare la connettività in uscita, vedere ["l'elenco degli endpoint a cui il data broker contatta"](#).

- NetApp consiglia di configurare l'origine, la destinazione e il data broker per utilizzare un servizio NTP

(Network Time Protocol). La differenza di tempo tra i tre componenti non deve superare i 5 minuti.

## Autorizzazioni necessarie per implementare il data broker in Azure

Assicurarsi che l'account utente Azure utilizzato per implementare il data broker disponga delle seguenti autorizzazioni:

```
{
  "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. Le seguenti autorizzazioni sono necessarie solo se si prevede di attivare ["Impostazione sincronizzazione continua"](#) Su una relazione di sincronizzazione da Azure a un'altra posizione di cloud storage:
  - "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"

Inoltre, l'ambito assegnabile deve essere impostato sull'ambito della sottoscrizione e sull'ambito del gruppo di risorse **NOF** se si intende implementare la sincronizzazione continua in Azure.

2. Le seguenti autorizzazioni sono necessarie solo se si intende scegliere una propria sicurezza per la creazione del broker di dati:

- "Microsoft.Network/networkSecurityGroups/securityRules/read"
- "Microsoft.Network/networkSecurityGroups/read"

## Metodo di autenticazione

Quando si implementa il data broker, è necessario scegliere un metodo di autenticazione per la macchina virtuale: Una password o una coppia di chiavi SSH pubblico-privato.

Per informazioni sulla creazione di una coppia di chiavi, fare riferimento a ["Documentazione di Azure: Creare e utilizzare una coppia di chiavi SSH pubblico-privato per macchine virtuali Linux in Azure"](#).

## Creare il broker di dati

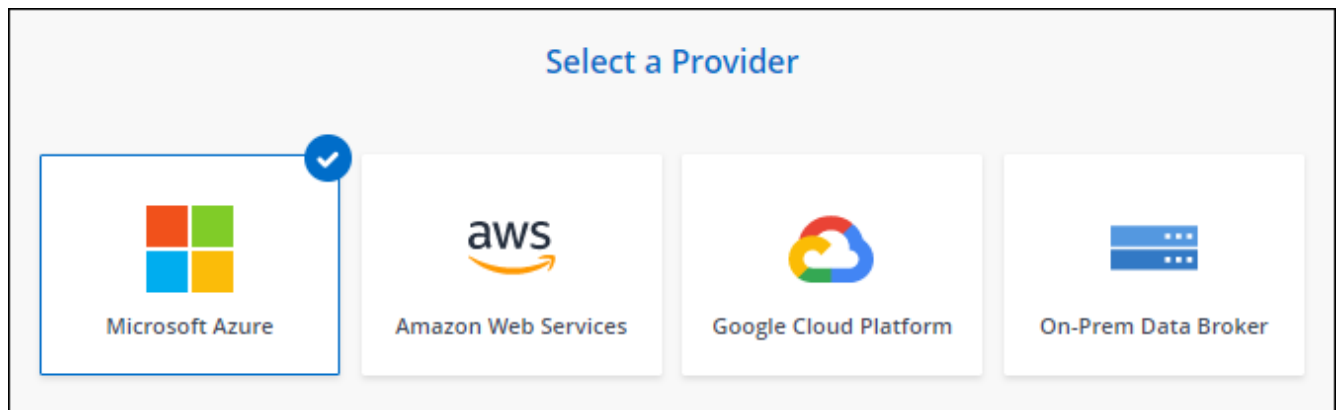
Esistono diversi modi per creare un nuovo data broker. Questi passaggi descrivono come installare un data broker in Azure quando si crea una relazione di sincronizzazione.

### Fasi

1. Selezionare **Crea nuova sincronizzazione**.
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione e selezionare **continua**.

Completa i passaggi fino a raggiungere la pagina **Data Broker Group**.

3. Nella pagina **Data Broker Group**, selezionare **Create Data Broker**, quindi selezionare **Microsoft Azure**.



4. Immettere un nome per il data broker e selezionare **continua**.
5. Se richiesto, accedere all'account Microsoft. Se non viene richiesto, selezionare **Accedi ad Azure**.

Il modulo è di proprietà e ospitato da Microsoft. Le tue credenziali non vengono fornite a NetApp.

6. Scegliere una posizione per il data broker e inserire i dettagli di base sulla macchina virtuale.

Location	Connectivity
<b>Subscription</b> <input type="text" value="Select a subscription"/>	<b>VM Name</b> <input type="text" value="netappdatabroker"/>
<b>Azure Region</b> <input type="text" value="Select a region"/>	<b>User Name</b> <input type="text" value="databroker"/>
<b>VNet</b> <input type="text" value="Select a VNet"/>	<b>Authentication Method:</b> <input checked="" type="radio"/> Password <input type="radio"/> Public Key
<b>Subnet</b> <input type="text" value="Select a subnet"/>	<b>Enter Password</b> <input type="text"/>
<b>Public IP</b> <input type="text" value="Enable"/>	<b>Resource Group:</b> <input checked="" type="radio"/> Generate a new group <input type="radio"/> Use an existing group
<b>Data Broker Role</b> <input type="checkbox"/> Create Custom Role <small><b>Notice:</b> Only relevant for continuous sync relationships from Azure. Users can also manually create this later.</small>	<b>Security group:</b> <input checked="" type="radio"/> Generate a new group <input type="radio"/> Use an existing group



Se si prevede di implementare una relazione di sincronizzazione continua, è necessario assegnare un ruolo personalizzato al proprio data broker. Questa operazione può essere eseguita anche manualmente dopo la creazione del broker.

7. Specificare una configurazione proxy, se è richiesto un proxy per l'accesso a Internet in VNET.

8. Selezionare **continua**. Per aggiungere permessi S3 al tuo broker di dati, inserisci l'accesso ad AWS e le chiavi segrete.
9. Selezionare **continua** e mantenere aperta la pagina fino al completamento dell'implementazione.

Il processo può richiedere fino a 7 minuti.

10. In BlueXP copy and Sync (Copia e sincronizzazione BlueXP), selezionare **Continue** (continua) una volta che il data broker è disponibile.
11. Completare le pagine della procedura guidata per creare la nuova relazione di sincronizzazione.

## Risultato

Hai implementato un data broker in Azure e creato una nuova relazione di sincronizzazione. Puoi utilizzare questo data broker con ulteriori relazioni di sincronizzazione.

### Viene visualizzato un messaggio che richiede il consenso dell'amministratore?

Se Microsoft notifica che è richiesta l'approvazione dell'amministratore perché la copia e la sincronizzazione di BlueXP richiedono l'autorizzazione per accedere alle risorse dell'organizzazione per conto dell'utente, sono disponibili due opzioni:

1. Chiedi all'amministratore di ad di fornirti le seguenti autorizzazioni:

In Azure, accedere a **Admin Center > Azure ad > utenti e gruppi > Impostazioni utente e abilitare gli utenti possono autorizzare le applicazioni ad accedere ai dati aziendali per loro conto**.

2. Chiedi al tuo amministratore di ad di acconsentire a **CloudSync-AzureDataBrokerCreator** utilizzando il seguente URL (questo è l'endpoint di consenso dell'amministratore):

[https://login.microsoftonline.com/{FILL QUI IL tuo ID TENANT}/v2.0/adminassenso?client\\_id=8e4ca3a-bafa-4831-97cc-5a38923cab85&redirect\\_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/USER\\_IMPERSONATIONhttps://graph.microsoft.com/User.Read](https://login.microsoftonline.com/{FILL QUI IL tuo ID TENANT}/v2.0/adminassenso?client_id=8e4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/USER_IMPERSONATIONhttps://graph.microsoft.com/User.Read)

Come mostrato nell'URL, l'URL dell'applicazione è <https://cloudsync.netapp.com> e l'ID del client dell'applicazione è 8ee4ca3a-bafa-4831-97cc-5a38923cab85.

## Dettagli sulla VM del data broker

BlueXP copy and Sync crea un data broker in Azure utilizzando la seguente configurazione.

### Compatibilità Node.js

v21,2.0

### Tipo di macchina virtuale

DS4 v2 standard

### VCPU

8

## RAM

28 GB

## Sistema operativo

Rocky Linux 9.0

## Dimensione e tipo di disco

SSD Premium da 64 GB

# Crea un nuovo broker di dati in Google Cloud

Quando crei un nuovo gruppo di broker di dati, scegli Google Cloud Platform per implementare il software di broker di dati su una nuova istanza di macchina virtuale in un VPC Google Cloud. BlueXP copy and Sync guida l'utente attraverso il processo di installazione, ma i requisiti e i passaggi sono ripetuti in questa pagina per aiutarti a prepararti all'installazione.

È inoltre possibile installare il data broker su un host Linux esistente nel cloud o on-premise. ["Scopri di più"](#).

## Aree di Google Cloud supportate

Sono supportate tutte le regioni.

## Privilegi root

Il software del data broker viene eseguito automaticamente come root sull'host Linux. L'esecuzione come root è un requisito per le operazioni di data broker. Ad esempio, per montare condivisioni.

## Requisiti di rete

- Il broker di dati necessita di una connessione Internet in uscita in modo che possa eseguire il polling del servizio di copia e sincronizzazione BlueXP per le attività sulla porta 443.

Quando BlueXP copy and Sync implementa il broker di dati in Google Cloud, crea un gruppo di sicurezza che abilita la comunicazione in uscita richiesta.

Per limitare la connettività in uscita, vedere ["l'elenco degli endpoint a cui il data broker contatta"](#).

- NetApp consiglia di configurare l'origine, la destinazione e il data broker per utilizzare un servizio NTP (Network Time Protocol). La differenza di tempo tra i tre componenti non deve superare i 5 minuti.

## Autorizzazioni necessarie per implementare il data broker in Google Cloud

Assicurarsi che l'utente di Google Cloud che implementa il data broker disponga delle seguenti autorizzazioni:

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

## Autorizzazioni richieste per l'account del servizio

Quando si implementa il data broker, è necessario selezionare un account di servizio che disponga delle seguenti autorizzazioni:

- `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`

Note:

1. L'autorizzazione "iam.serviceAccounts.signJwt" è necessaria solo se si intende configurare il data broker per l'utilizzo di un vault HashiCorp esterno.
2. Le autorizzazioni "pubsub.\*" e "storage.bucket.update" sono necessarie solo se si intende attivare l'impostazione di Continuous Sync su una relazione di sincronizzazione tra Google Cloud Storage e un'altra posizione di cloud storage. ["Scopri di più sull'opzione Continuous Sync"](#).

3. Le autorizzazioni "cloudkms.cryptKeys.list" e "cloudkms.keyrings.list" sono richieste solo se si prevede di utilizzare una chiave KMS gestita dal cliente su un bucket Google Cloud Storage di destinazione.

## Creare il broker di dati

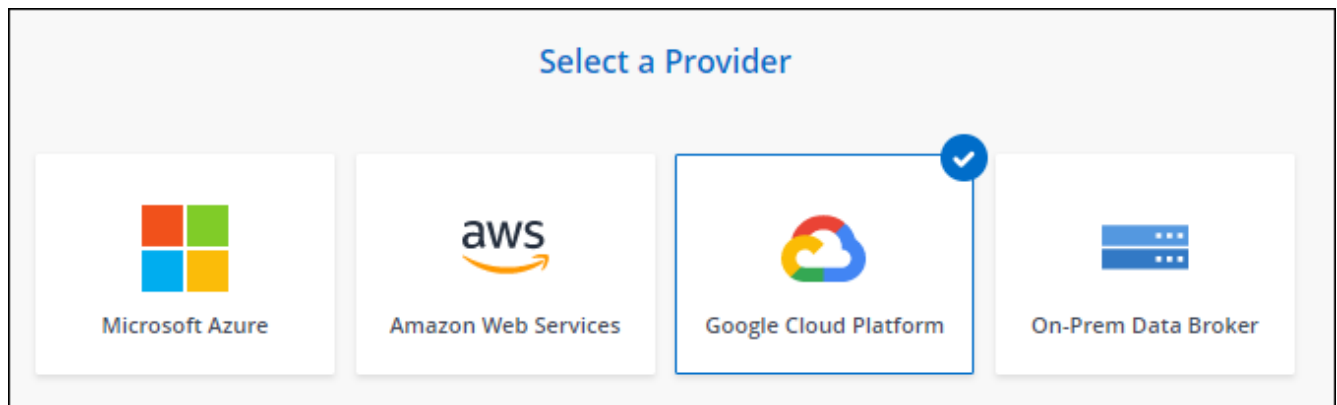
Esistono diversi modi per creare un nuovo data broker. Questi passaggi descrivono come installare un data broker in Google Cloud quando si crea una relazione di sincronizzazione.

### Fasi

1. Selezionare **Crea nuova sincronizzazione**.
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione e selezionare **continua**.

Completa i passaggi fino a raggiungere la pagina **Data Broker Group**.

3. Nella pagina **Data Broker Group**, selezionare **Create Data Broker**, quindi **Google Cloud Platform**.



4. Immettere un nome per il data broker e selezionare **continua**.
5. Se richiesto, accedere con l'account Google.

Il modulo è di proprietà e ospitato da Google. Le tue credenziali non vengono fornite a NetApp.

6. Selezionare un account di progetto e servizio, quindi scegliere una posizione per il data broker, ad esempio se si desidera attivare o disattivare un indirizzo IP pubblico.

Se non si attiva un indirizzo IP pubblico, sarà necessario definire un server proxy nella fase successiva.

### Basic Settings

<p><b>Project</b></p> <p>Project</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">OCCM-Dev ▼</div> <p>Service Account</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">test ▼</div> <p>Select a Service Account that includes <a href="#">these permissions</a></p>	<p><b>Location</b></p> <p>Region</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">us-west1 ▼</div> <p>Zone</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">us-west1-a ▼</div> <p>VPC</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">default ▼</div> <p>Subnet</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">default ▼</div> <p>Public IP</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 10px;">Enable ▼</div>
---	---

7. Specificare una configurazione proxy, se è richiesto un proxy per l'accesso a Internet nel VPC.

Se è necessario un proxy per l'accesso a Internet, il proxy deve trovarsi in Google Cloud e utilizzare lo stesso account di servizio del data broker.

8. Una volta che il data broker è disponibile, selezionare **Continue** (continua) in BlueXP copy and Sync (Copia e sincronizza BlueXP).

L'implementazione dell'istanza richiede da 5 a 10 minuti circa. È possibile monitorare l'avanzamento del servizio di copia e sincronizzazione BlueXP, che si aggiorna automaticamente quando l'istanza è disponibile.

9. Completare le pagine della procedura guidata per creare la nuova relazione di sincronizzazione.

#### Risultato

Hai implementato un data broker in Google Cloud e creato una nuova relazione di sincronizzazione. Puoi utilizzare questo data broker con ulteriori relazioni di sincronizzazione.

### Fornisci autorizzazioni per l'utilizzo dei bucket in altri progetti Google Cloud

Quando crei una relazione di sincronizzazione e scegli Google Cloud Storage come origine o destinazione, BlueXP Copy and Sync ti consente di scegliere tra i bucket che l'account di servizio del broker di dati dispone delle autorizzazioni per l'utilizzo. Per impostazione predefinita, sono inclusi i bucket che si trovano nel *stesso* progetto dell'account di servizio del broker di dati. Tuttavia, è possibile scegliere i bucket di *altri* progetti se si forniscono le autorizzazioni necessarie.

## Fasi

1. Aprire la console di Google Cloud Platform e caricare il servizio Cloud Storage.
2. Selezionare il nome del bucket che si desidera utilizzare come origine o destinazione in una relazione di sincronizzazione.
3. Selezionare **Permissions**.
4. Selezionare **Aggiungi**.
5. Immettere il nome dell'account di servizio del broker di dati.
6. Selezionare un ruolo che fornisce [le stesse autorizzazioni illustrate in precedenza](#).
7. Selezionare **Salva**.

## Risultato

Quando si imposta una relazione di sincronizzazione, è ora possibile scegliere tale bucket come origine o destinazione nella relazione di sincronizzazione.

## Dettagli sull'istanza di VM del data broker

BlueXP copy and Sync crea un data broker in Google Cloud utilizzando la seguente configurazione.

### Compatibilità Node.js

v21,2.0

### Tipo di macchina

n2-standard-4

### VCPU

4

### RAM

15 GB

### Sistema operativo

Rocky Linux 9.0

### Dimensione e tipo di disco

HDD da 20 GB pd-standard

## Installare il broker di dati su un host Linux

Quando crei un nuovo gruppo di broker di dati, scegli l'opzione on-Prem Data Broker per installare il software di broker di dati su un host Linux on-premise o su un host Linux esistente nel cloud. BlueXP copy and Sync guida l'utente attraverso il processo di installazione, ma i requisiti e i passaggi sono ripetuti in questa pagina per aiutarti a prepararti all'installazione.

### Requisiti degli host Linux

- **Compatibilità Node.js:** v21,2.0



- **Sistema operativo:**

- CentOS 8.0 e 8.5

CentOS Stream non è supportato.

- Red Hat Enterprise Linux 8,5, 8,8 e 8,9
- Rocky Linux 9
- Ubuntu Server 20.04 LTS
- SUSE Linux Enterprise Server 15 SP1

Il comando `yum update` deve essere eseguito sull'host prima di installare il data broker.

Un sistema Red Hat Enterprise Linux deve essere registrato con Red Hat Subscription Management. Se non è registrato, il sistema non può accedere ai repository per aggiornare il software di terze parti richiesto durante l'installazione.

- **RAM:** 16 GB
- **CPU:** 4 core
- **Spazio libero su disco:** 10 GB
- **SELinux:** Si consiglia di disattivarlo "[SELinux](#)" sull'host.

SELinux applica una policy che blocca gli aggiornamenti del software del data broker e impedisce al data broker di contattare gli endpoint necessari per il normale funzionamento.

## Privilegi root

Il software del data broker viene eseguito automaticamente come root sull'host Linux. L'esecuzione come root è un requisito per le operazioni di data broker. Ad esempio, per montare condivisioni.

## Requisiti di rete

- L'host Linux deve disporre di una connessione all'origine e alla destinazione.
- Il file server deve consentire all'host Linux di accedere alle esportazioni.
- La porta 443 deve essere aperta sull'host Linux per il traffico in uscita verso AWS (il data broker comunica costantemente con il servizio Amazon SQS).
- NetApp consiglia di configurare l'origine, la destinazione e il data broker per utilizzare un servizio NTP (Network Time Protocol). La differenza di tempo tra i tre componenti non deve superare i 5 minuti.

## Consenti l'accesso ad AWS

Se si prevede di utilizzare il data broker con una relazione di sincronizzazione che include un bucket S3, è necessario preparare l'host Linux per l'accesso AWS. Quando si installa il data broker, è necessario fornire le chiavi AWS per un utente AWS che dispone di un accesso programmatico e di autorizzazioni specifiche.

### Fasi

1. Creare un criterio IAM utilizzando "[Questa policy fornita da NetApp](#)"

["Visualizzare le istruzioni AWS"](#)

2. Creare un utente IAM con accesso programmatico.

["Visualizzare le istruzioni AWS"](#)

Assicurarsi di copiare le chiavi AWS perché è necessario specificarle quando si installa il software data broker.

## Abilita l'accesso a Google Cloud

Se intendi utilizzare il data broker con una relazione di sincronizzazione che include un bucket di storage Google Cloud, devi preparare l'host Linux per l'accesso a Google Cloud. Quando si installa il data broker, è necessario fornire una chiave per un account di servizio che dispone di autorizzazioni specifiche.

### Fasi

1. Creare un account di servizio Google Cloud con autorizzazioni Storage Admin, se non ne hai già uno.
2. Creare una chiave dell'account di servizio salvata in formato JSON.

["Visualizza le istruzioni di Google Cloud"](#)

Il file deve contenere almeno le seguenti proprietà: "Project\_id", "private\_key" e "client\_email"



Quando si crea una chiave, il file viene generato e scaricato sul computer.

3. Salvare il file JSON nell'host Linux.

## Abilita l'accesso a Microsoft Azure

L'accesso ad Azure viene definito in base alla relazione fornendo un account di storage e una stringa di connessione nella procedura guidata delle relazioni di sincronizzazione.

## Installazione del broker di dati

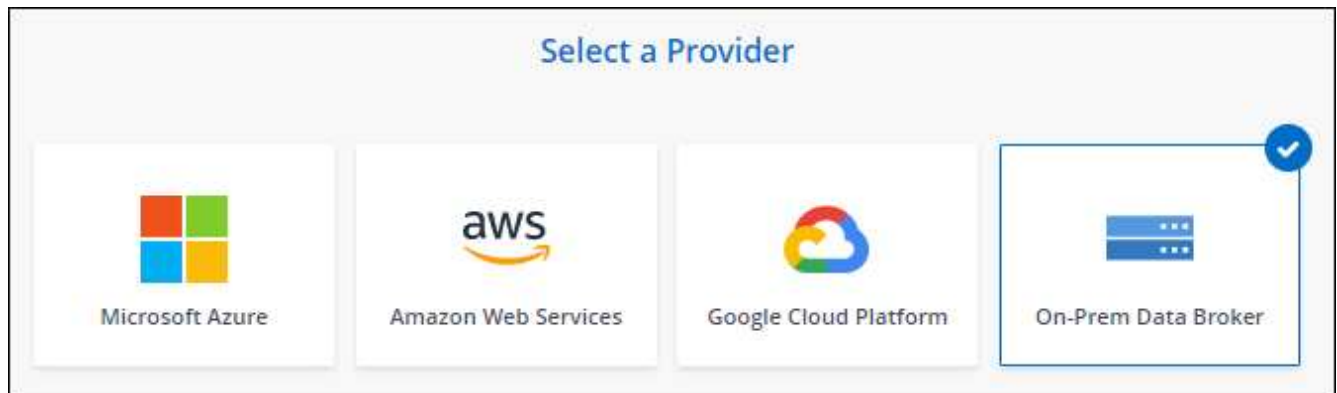
È possibile installare un data broker su un host Linux quando si crea una relazione di sincronizzazione.

### Fasi

1. Selezionare **Crea nuova sincronizzazione**.
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione e selezionare **continua**.

Completa i passaggi fino a raggiungere la pagina **Data Broker Group**.

3. Nella pagina **Data Broker Group**, selezionare **Create Data Broker**, quindi **on-Prem Data Broker**.



Anche se l'opzione è denominata **on-Prem Data Broker**, si applica a un host Linux on-premise o nel cloud.

4. Immettere un nome per il data broker e selezionare **continua**.

La pagina delle istruzioni viene caricata a breve. È necessario seguire queste istruzioni, che includono un link univoco per scaricare il programma di installazione.

5. Nella pagina delle istruzioni:

- a. Selezionare se attivare l'accesso a **AWS**, **Google Cloud** o entrambi.
- b. Selezionare un'opzione di installazione: **Nessun proxy**, **Usa server proxy** o **Usa server proxy con autenticazione**.



L'utente deve essere un utente locale. Gli utenti di dominio non sono supportati.

- c. Utilizzare i comandi per scaricare e installare il data broker.

I seguenti passaggi forniscono dettagli su ciascuna opzione di installazione possibile. Seguire la pagina delle istruzioni per ottenere il comando esatto in base all'opzione di installazione.

- d. Scaricare il programma di installazione:

- Nessun proxy:

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

- USA server proxy:

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

- USA server proxy con autenticazione:

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

### URI

BlueXP copy and Sync visualizza l'URI del file di installazione nella pagina delle istruzioni, che viene caricato quando si seguono le istruzioni per implementare on-Prem Data Broker. L'URI non viene ripetuto in questo caso perché il collegamento viene generato dinamicamente e può essere utilizzato una sola volta. [Per ottenere l'URI dalla copia e dalla sincronizzazione BlueXP, procedere come segue.](#)

e. Passare a superuser, rendere eseguibile il programma di installazione e installare il software:



Ciascun comando elencato di seguito include i parametri per l'accesso AWS e Google Cloud. Seguire la pagina delle istruzioni per ottenere il comando esatto in base all'opzione di installazione.

- Nessuna configurazione 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>
```

- Configurazione del 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>
```

- Configurazione del proxy con autenticazione:

```
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>
```

### Tasti AWS

Queste sono le chiavi per l'utente che si dovrebbe preparare [seguire questa procedura](#). Le chiavi AWS vengono memorizzate nel data broker, che viene eseguito nella rete on-premise o cloud. NetApp non utilizza le chiavi esterne al data broker.

### File JSON

Questo è il file JSON che contiene una chiave di account di servizio che si dovrebbe preparare [seguire questa procedura](#).

6. Una volta che il data broker è disponibile, selezionare **Continue** (continua) in BlueXP copy and Sync (Copia e sincronizza BlueXP).
7. Completare le pagine della procedura guidata per creare la nuova relazione di sincronizzazione.

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.