Inizia subito

BlueXP copy and sync

NetApp
September 23, 2024

Sommario

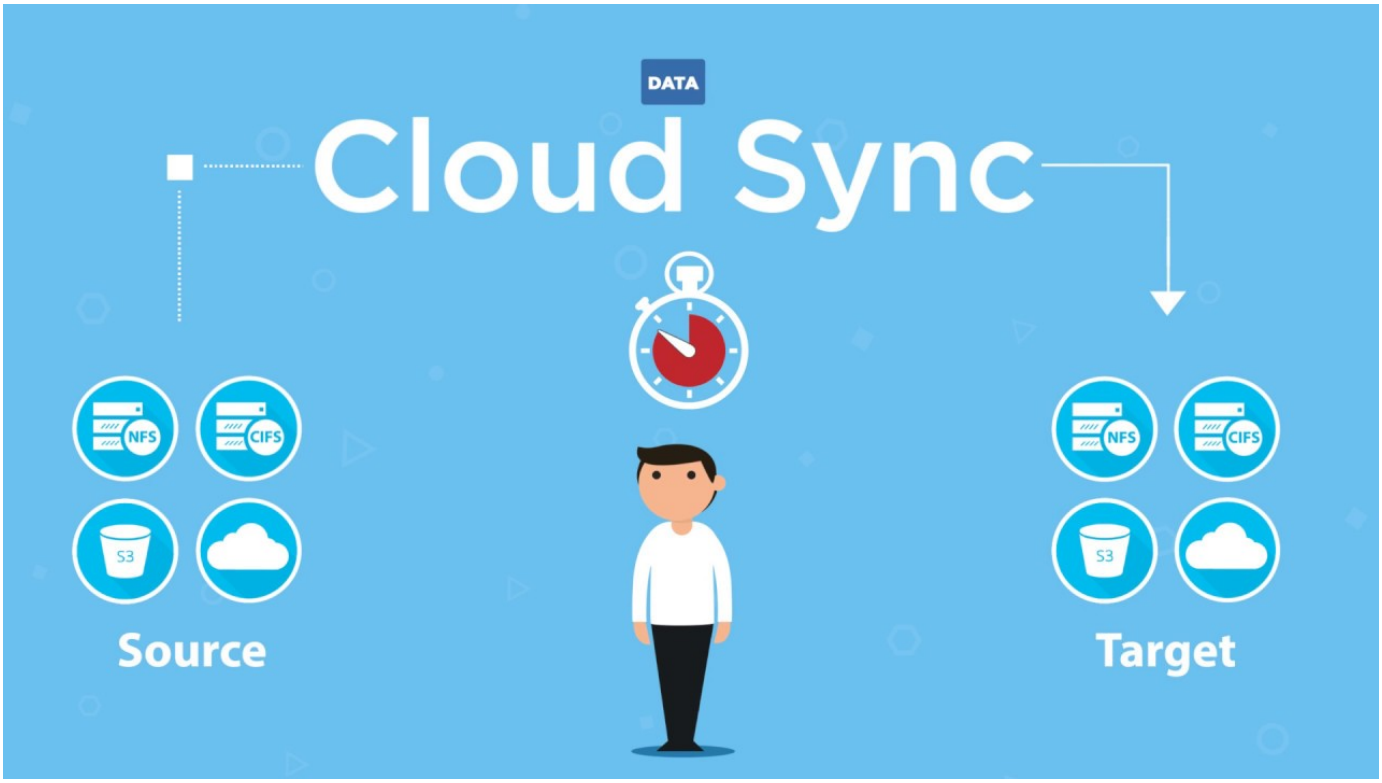
Inizia subito

Panoramica sulla copia e la sincronizzazione BlueXP

Il servizio di copia e sincronizzazione BlueXP di NetApp offre un modo semplice, sicuro e automatizzato per migrare i dati verso qualsiasi destinazione, nel cloud o on-premise. Sia che si tratti di un set di dati NAS basato su file (NFS o SMB), di un formato di oggetti Amazon Simple Storage Service (S3), di un'appliance NetApp StorageGRID® o di qualsiasi altro archivio di oggetti di provider cloud, BlueXP Copy and Sync può convertirlo e spostarlo per te.

Caratteristiche

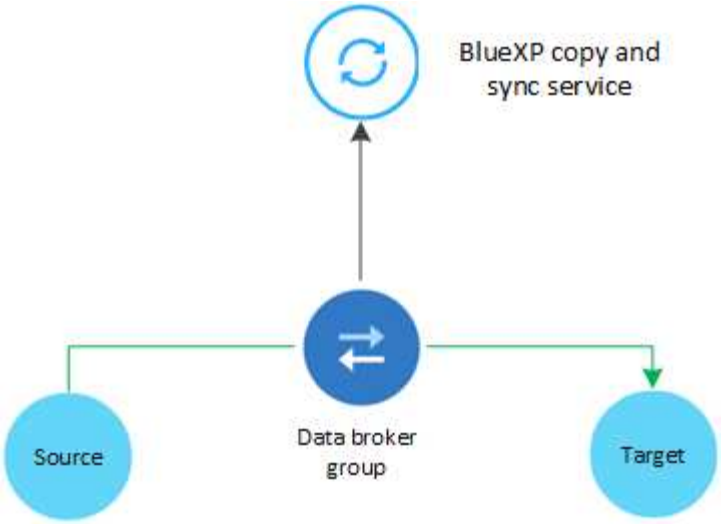
Guarda il seguente video per una panoramica della copia e della sincronizzazione di BlueXP:



Come funziona la copia e la sincronizzazione di BlueXP

BlueXP copy and Sync è una piattaforma software-as-a-service (SaaS) che consiste in un gruppo di broker di dati, un'interfaccia basata su cloud disponibile tramite BlueXP e un'origine e una destinazione.

La seguente immagine mostra la relazione tra i componenti di copia e sincronizzazione di BlueXP:



Il software NetApp data broker sincronizza i dati da un'origine a un'area di destinazione (chiamata *relazione di sincronizzazione*). Puoi eseguire il data broker in AWS, Azure, Google Cloud Platform o on-premise. Un gruppo di broker di dati, costituito da uno o più broker di dati, necessita di una connessione Internet in uscita sulla porta 443 in modo che possa comunicare con il servizio di copia e sincronizzazione BlueXP e contattare altri servizi e repository. "Visualizzare l'elenco degli endpoint".

Dopo la copia iniziale, il servizio sincronizza i dati modificati in base alla pianificazione impostata.

Tipi di storage supportati

BlueXP copy and Sync supporta i seguenti tipi di storage:

- Qualsiasi server NFS
- Qualsiasi server SMB
- Amazon EFS
- Amazon FSX per ONTAP
- Amazon S3
- Azure Blob
- Azure Data Lake Storage Gen2
- Azure NetApp Files
- Box (disponibile in anteprima)
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Storage Google Cloud
- Google Drive
- Storage a oggetti IBM Cloud
- Cluster ONTAP on-premise
- Storage ONTAP S3
- SFTP (solo tramite API)
- StorageGRID

"Visualizzare le relazioni di sincronizzazione supportate".

Costi

L'utilizzo della copia e della sincronizzazione di BlueXP comporta due tipi di costi: Costi delle risorse e costi del servizio.

Costi delle risorse

I costi delle risorse sono correlati ai costi di calcolo e storage per l'esecuzione di uno o più broker di dati nel cloud.

Costi del servizio

Esistono due modi per pagare le relazioni di sincronizzazione dopo la fine della prova gratuita di 14 giorni. La prima opzione consiste nell'effettuare l'iscrizione da AWS o Azure, che consente di pagare ogni ora o annualmente. La seconda opzione consiste nell'acquistare le licenze direttamente da NetApp.

"Scopri come funzionano le licenze".

Avvio rapido per la copia e la sincronizzazione BlueXP

La guida introduttiva al servizio di copia e sincronizzazione BlueXP include alcuni passaggi.

Accedere e configurare BlueXP

Dovresti aver iniziato a utilizzare BlueXP, che include l'accesso, la configurazione di un account e la distribuzione di un connettore e la creazione di ambienti di lavoro.

Se si desidera creare relazioni di sincronizzazione per uno dei seguenti elementi, è necessario innanzitutto creare o rilevare un ambiente di lavoro:

- Amazon FSX per ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Cluster ONTAP on-premise

È necessario un connettore per Cloud Volumes ONTAP, i cluster ONTAP on-premise e Amazon FSX per ONTAP.

- "Scopri come iniziare a utilizzare BlueXP"
- "Scopri di più sui connettori"

Preparare l'origine e la destinazione

Verificare che l'origine e la destinazione siano supportate e configurate. Il requisito più importante è verificare la connettività tra il gruppo di broker di dati e le posizioni di origine e destinazione.

- "Visualizzare le relazioni supportate"
- "Preparare l'origine e la destinazione"

3 Preparare una posizione per il data broker di NetApp

Il software NetApp data broker sincronizza i dati da un'origine a un'area di destinazione (chiamata *relazione di sincronizzazione*). Puoi eseguire il data broker in AWS, Azure, Google Cloud Platform o on-premise. Un gruppo di broker di dati, costituito da uno o più broker di dati, necessita di una connessione Internet in uscita sulla porta 443 in modo che possa comunicare con il servizio di copia e sincronizzazione BlueXP e contattare altri servizi e repository. "Visualizzare l'elenco degli endpoint".

BlueXP copy and Sync ti guida attraverso il processo di installazione quando crei una relazione di sincronizzazione, a questo punto puoi implementare un data broker nel cloud o scaricare uno script di installazione per il tuo host Linux.

- "Esaminare l'installazione di AWS"
- "Esaminare l'installazione di Azure"
- "Esaminare l'installazione di Google Cloud"
- "Esaminare l'installazione dell'host Linux"

4 Crea la tua prima relazione di sincronizzazione

Accedere a. "BlueXP", Selezionare **Sync**, quindi trascinare le selezioni per l'origine e la destinazione. Seguire le istruzioni per completare la configurazione. "Scopri di più".

5 Paga le tue relazioni di sincronizzazione al termine della prova gratuita

Iscriviti ad AWS o Azure per pagare a consumo o per pagare annualmente. Oppure acquistare le licenze direttamente da NetApp. Basta andare alla pagina License Settings (Impostazioni di licenza) in BlueXP copy (Copia BlueXP) e sincronizzarla per configurarla. "Scopri di più".

Relazioni di sincronizzazione supportate

BlueXP copy and Sync consente di sincronizzare i dati da un'origine a una destinazione. Questa relazione viene chiamata relazione di sincronizzazione. Prima di iniziare, è necessario comprendere le relazioni supportate.

Posizione di origine	Posizioni di destinazione supportate
Amazon EFS	• Amazon EFS • Amazon FSX per ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise (NFS o SMB) • Server SMB • StorageGRID
Amazon FSX per ONTAP	• Amazon EFS • Amazon FSX per ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise (NFS o SMB) • Server SMB • StorageGRID

Posizione di origine	Posizioni di destinazione supportate
Amazon S3	• Amazon EFS • Amazon FSX per ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Casella [1] • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise (NFS o SMB) • Storage ONTAP S3 • Server SMB • StorageGRID
Azure Blob	• Amazon EFS • Amazon FSX per ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise (NFS o SMB) • Server SMB • StorageGRID

Posizione di origine	Posizioni di destinazione supportate
Azure Data Lake Storage Gen2	• Azure NetApp Files • Cloud Volumes ONTAP • FSX per ONTAP • Storage a oggetti IBM Cloud • Server NFS • ONTAP on-premise • Storage ONTAP S3 • Server SMB • StorageGRID
Azure NetApp Files	• Amazon EFS • Amazon FSX per ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise (NFS o SMB) • Server SMB • StorageGRID
Casella [1]	• Amazon FSX per ONTAP • Amazon S3 • Azure NetApp Files • Cloud Volumes ONTAP • Storage a oggetti IBM Cloud • Server NFS • Server SMB • StorageGRID

Posizione di origine	Posizioni di destinazione supportate
Cloud Volumes ONTAP	• Amazon EFS • Amazon FSX per ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise (NFS o SMB) • Server SMB • StorageGRID
Cloud Volumes Service	• Amazon EFS • Amazon FSX per ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise (NFS o SMB) • Server SMB • StorageGRID

Posizione di origine	Posizioni di destinazione supportate
Storage Google Cloud	• Amazon EFS • Amazon FSX per ONTAP • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise (NFS o SMB) • Storage ONTAP S3 • Server SMB • StorageGRID
Google Drive	• Server NFS • Server SMB
Storage a oggetti IBM Cloud	• Amazon EFS • Amazon FSX per ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Casella [1] • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise (NFS o SMB) • Server SMB • StorageGRID

Posizione di origine	Posizioni di destinazione supportate
Server NFS	• Amazon EFS • Amazon FSX per ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Google Drive • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise (NFS o SMB) • Storage ONTAP S3 • Server SMB • StorageGRID
Cluster ONTAP on-premise (NFS o SMB)	• Amazon EFS • Amazon FSX per ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise (NFS o SMB) • Server SMB • StorageGRID

Posizione di origine	Posizioni di destinazione supportate
Storage ONTAP S3	• Amazon S3 • Azure Data Lake Storage Gen2 • Storage Google Cloud • Server NFS • Server SMB • StorageGRID • Storage ONTAP S3
SFTP [2]	S3
Server SMB	• Amazon EFS • Amazon FSX per ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Google Drive • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise (NFS o SMB) • Storage ONTAP S3 • Server SMB • StorageGRID

Posizione di origine	Posizioni di destinazione supportate
StorageGRID	• Amazon EFS • Amazon FSX per ONTAP • Amazon S3 • Azure Blob • Azure Data Lake Storage Gen2 • Azure NetApp Files • Casella [1] • Cloud Volumes ONTAP • Cloud Volumes Service • Storage Google Cloud • Storage a oggetti IBM Cloud • Server NFS • Cluster ONTAP on-premise (NFS o SMB) • Storage ONTAP S3 • Server SMB • StorageGRID

Note:

1. Il supporto Box è disponibile come anteprima.
2. Le relazioni di sincronizzazione con questa origine/destinazione sono supportate utilizzando solo l'API di copia e sincronizzazione BlueXP.
3. È possibile scegliere un livello di storage Azure Blob specifico quando un container Blob è la destinazione:
    - Storage a caldo
    - Storage fresco
4. puoi scegliere una classe di storage S3 specifica quando Amazon S3 è la destinazione:
    - Standard (classe predefinita)
    - Tiering intelligente
    - Standard-infrequent Access (accesso standard-non frequente)
    - Accesso non frequente a una sola zona
    - Glacier Deep Archive
    - Recupero flessibile di Glacier
    - Glacier Instant Retrieval
5. È possibile scegliere una classe di storage specifica quando l'obiettivo è un bucket di storage Google Cloud:
    - Standard
    - Nearline

- Coldline
- Archiviare

Preparare l’origine e la destinazione

Verificare che la fonte e le destinazioni soddisfino i seguenti requisiti.

Networking

- L’origine e la destinazione devono disporre di una connessione di rete al gruppo di broker di dati.

  Ad esempio, se un server NFS si trova nel data center e un broker di dati si trova in AWS, è necessaria una connessione di rete (VPN o Direct Connect) dalla rete al VPC.

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

Directory di destinazione

Quando si crea una relazione di sincronizzazione, BlueXP copy and Sync consente di selezionare una directory di destinazione esistente e, se necessario, di creare una nuova cartella all’interno di tale directory. Quindi, assicurarsi che la directory di destinazione preferita esista già.

Permessi di lettura delle directory

Per visualizzare ogni directory o cartella in un’origine o destinazione, la copia e la sincronizzazione di BlueXP richiedono permessi di lettura per la directory o la cartella.

NFS

I permessi devono essere definiti sull’origine/destinazione con uid/gid su file e directory.

Storage a oggetti

- Per AWS e Google Cloud, un data broker deve disporre delle autorizzazioni per gli oggetti elenco (queste autorizzazioni vengono fornite per impostazione predefinita se si seguono le fasi di installazione del data broker).
- Per Azure, StorageGRID e IBM, le credenziali immesse durante l’impostazione di una relazione di sincronizzazione devono disporre delle autorizzazioni per gli oggetti elenco.

PMI

Le credenziali SMB immesse durante l’impostazione di una relazione di sincronizzazione devono disporre delle autorizzazioni per la cartella elenco.

Per impostazione predefinita, il data broker ignora le seguenti directory: .Snapshot, ~snapshot, .copy-offload

requisiti del bucket Amazon S3

Assicurati che il bucket Amazon S3 soddisfi i seguenti requisiti.

Posizioni dei data broker supportate per Amazon S3

Le relazioni di sincronizzazione che includono lo storage S3 richiedono un broker di dati implementato in AWS o on-premise. In entrambi i casi, BlueXP Copy and Sync richiede di associare il data broker a un account AWS durante l'installazione.

- "Scopri come implementare il data broker AWS"
- "Scopri come installare il data broker su un host Linux"

Regioni AWS supportate

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

Autorizzazioni richieste per i bucket S3 in altri account AWS

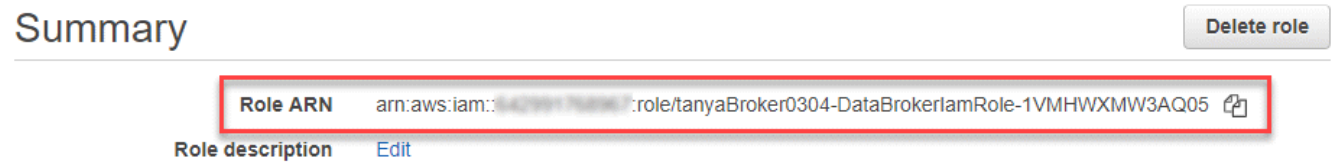
Quando si imposta una relazione di sincronizzazione, è possibile specificare un bucket S3 che risiede in un account AWS non associato a un data broker.

"Le autorizzazioni incluse in questo file JSON" Deve essere applicato al bucket S3 in modo che un broker di dati possa accedervi. Queste autorizzazioni consentono al broker di dati di copiare i dati da e verso il bucket e di elencare gli oggetti nel bucket.

Tenere presente quanto segue sulle autorizzazioni incluse nel file JSON:

1. *<BucketName>* è il nome del bucket che risiede nell'account AWS non associato a un data broker.
2. *<RoleARN>* deve essere sostituito con uno dei seguenti elementi:
   - Se un data broker è stato installato manualmente su un host Linux, *RoleARN* dovrebbe essere l'ARN dell'utente AWS per cui hai fornito le credenziali AWS durante l'implementazione di un data broker.
   - Se un broker di dati è stato implementato in AWS utilizzando il modello CloudFormation, *RoleARN* deve essere l'ARN del ruolo IAM creato dal modello.

     Per trovare il ruolo ARN, accedere alla console EC2, selezionare l'istanza del broker di dati, quindi selezionare il ruolo IAM dalla scheda Description (Descrizione). Viene visualizzata la pagina Summary (Riepilogo) nella console IAM che contiene il ruolo ARN.



requisiti di storage di Azure Blob

Assicurati che lo storage Azure Blob soddisfi i seguenti requisiti.

Posizioni dei data broker supportate per Azure Blob

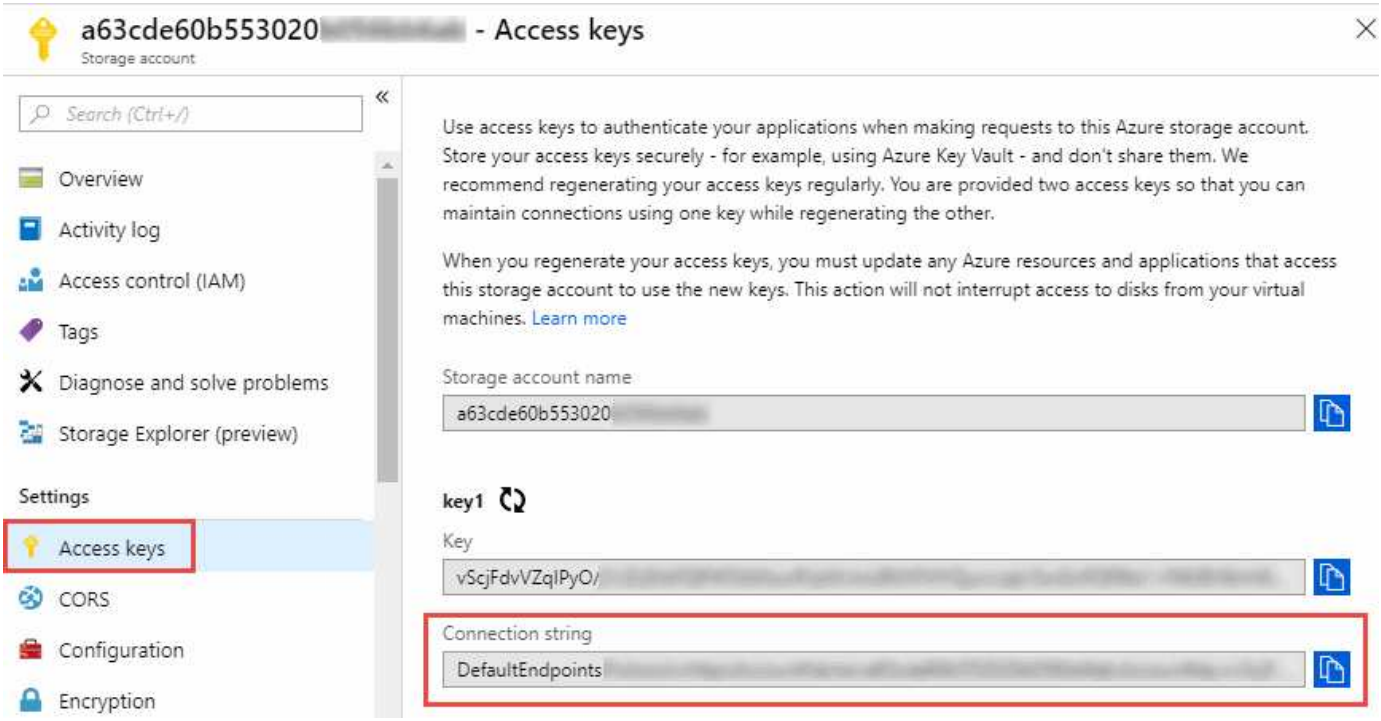
Un broker di dati può risiedere in qualsiasi posizione quando una relazione di sincronizzazione include lo storage Azure Blob.

Aree Azure supportate

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

Stringa di connessione per le relazioni che includono Azure Blob e NFS/SMB

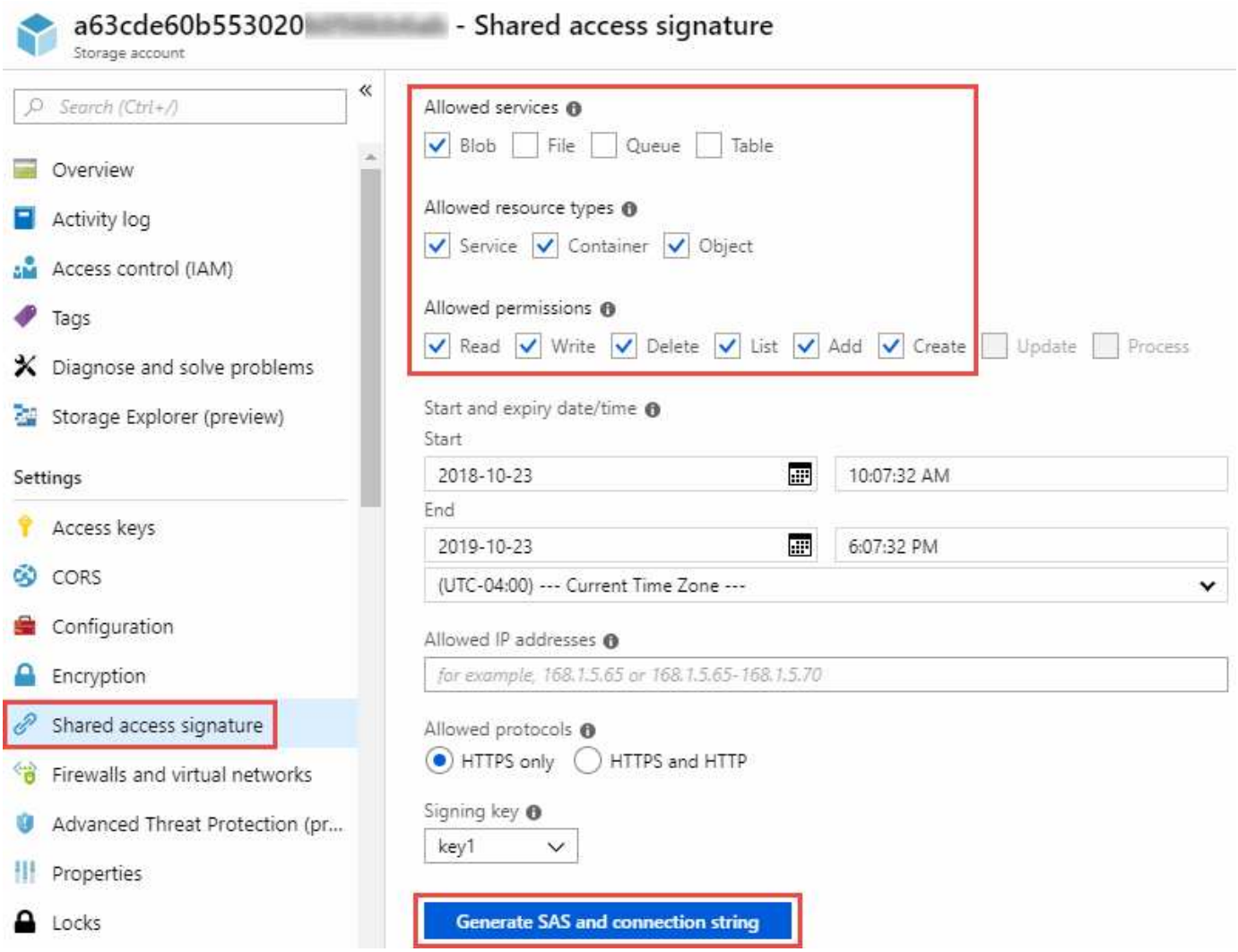
Quando si crea una relazione di sincronizzazione tra un container Azure Blob e un server NFS o SMB, è necessario fornire una copia BlueXP e la sincronizzazione con la stringa di connessione dell'account di storage:



Se si desidera sincronizzare i dati tra due contenitori Azure Blob, la stringa di connessione deve includere un "firma di accesso condivisa" (SAS). È inoltre possibile utilizzare un SAS durante la sincronizzazione tra un container Blob e un server NFS o SMB.

Il SAS deve consentire l'accesso al servizio Blob e a tutti i tipi di risorse (Servizio, container e oggetto). Il SAS deve includere anche le seguenti autorizzazioni:

- Per il contenitore Blob di origine: Read and List (lettura ed elenco)
- Per il contenitore Blob di destinazione: Lettura, scrittura, elenco, Aggiungi e Crea



Se si sceglie di implementare una relazione di sincronizzazione continua che include un container Azure Blob, è possibile utilizzare una stringa di connessione normale o una stringa di connessione SAS. Se si utilizza una stringa di connessione SAS, non deve essere impostata in modo che scada nel prossimo futuro.

Azure Data Lake Storage Gen2

Quando si crea una relazione di sincronizzazione che include Azure Data Lake, è necessario fornire una copia BlueXP e sincronizzarla con la stringa di connessione dell'account di storage. Deve essere una stringa di connessione regolare e non una firma di accesso condivisa (SAS).

Requisito Azure NetApp Files

Utilizzare il livello di servizio Premium o Ultra quando si sincronizzano i dati da o verso Azure NetApp Files. Se il livello di servizio del disco è Standard, potrebbero verificarsi errori e problemi di performance.

Se hai bisogno di aiuto per determinare il livello di servizio giusto, consulta un Solutions Architect. Le dimensioni del volume e il Tier del volume determinano il throughput che è possibile ottenere.

"Scopri di più sui livelli di servizio e sul throughput di Azure NetApp Files".

Requisiti della confezione

- Per creare una relazione di sincronizzazione che includa Box, devi fornire le seguenti credenziali:
  - ID client
  - Segreto del client
  - Chiave privata
  - ID chiave pubblica
  - Passphrase
  - ID aziendale
- Se crei una relazione di sincronizzazione da Amazon S3 a Box, devi utilizzare un gruppo di broker di dati con una configurazione unificata in cui le seguenti impostazioni sono impostate su 1:
  - Concorrenza scanner
  - Limiti dei processi dello scanner
  - Concorrenza del transferrer
  - Limiti dei processi di trasferimento

  "Scopri come definire una configurazione unificata per un gruppo di broker di dati".

requisiti del bucket di storage Google Cloud

Assicurati che il tuo bucket di storage Google Cloud soddisfi i seguenti requisiti.

Posizioni dei data broker supportate per Google Cloud Storage

Le relazioni di sincronizzazione che includono Google Cloud Storage richiedono un broker di dati implementato in Google Cloud o on-premise. BlueXP copy and Sync ti guida attraverso il processo di installazione del data broker quando crei una relazione di sincronizzazione.

- "Scopri come implementare il data broker di Google Cloud"
- "Scopri come installare il data broker su un host Linux"

Aree di Google Cloud supportate

Sono supportate tutte le regioni.

Permessi per bucket in altri progetti Google Cloud

Quando si imposta una relazione di sincronizzazione, è possibile scegliere tra i bucket di Google Cloud in diversi progetti, se si forniscono le autorizzazioni necessarie all'account di servizio del broker di dati. "Scopri come configurare l'account di servizio".

Autorizzazioni per una destinazione SnapMirror

Se l'origine di una relazione di sincronizzazione è una destinazione SnapMirror (di sola lettura), le autorizzazioni di "lettura/elenco" sono sufficienti per sincronizzare i dati dall'origine a una destinazione.

Crittografia di un bucket Google Cloud

Puoi crittografare un bucket Google Cloud di destinazione con una chiave KMS gestita dal cliente o la chiave predefinita gestita da Google. Se nel bucket è già stata aggiunta una crittografia KMS, verrà sovrascritta la crittografia predefinita gestita da Google.

Per aggiungere una chiave KMS gestita dal cliente, è necessario utilizzare un broker di dati con "correggere le autorizzazioni", e la chiave deve trovarsi nella stessa regione del bucket.

Google Drive

Quando si imposta una relazione di sincronizzazione che include Google Drive, è necessario fornire quanto segue:

- L'indirizzo e-mail di un utente che ha accesso alla posizione Google Drive in cui si desidera sincronizzare i dati
- L'indirizzo e-mail di un account di servizio Google Cloud che dispone delle autorizzazioni per accedere a Google Drive
- Chiave privata per l'account del servizio

Per configurare l'account di servizio, seguire le istruzioni nella documentazione di Google:

- "Creare l'account del servizio e le credenziali"
- "Delegare l'autorità a livello di dominio all'account di servizio"

Quando si modifica il campo OAuth Scopes (Scopes OAuth), immettere i seguenti ambiti:

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

Requisiti del server NFS

- Il server NFS può essere un sistema NetApp o un sistema non NetApp.
- Il file server deve consentire a un host del data broker di accedere alle esportazioni sulle porte richieste.
  - 111 TCP/UDP
  - 2049 TCP/UDP
  - 5555 TCP/UDP
- Sono supportate le versioni 3, 4.0, 4.1 e 4.2 di NFS.

  La versione desiderata deve essere abilitata sul server.
- Se si desidera sincronizzare i dati NFS da un sistema ONTAP, assicurarsi che sia abilitato l'accesso all'elenco di esportazione NFS per una SVM (vserver nfs modify -vserver *nome_svm* -showmount abilitato).

  L'impostazione predefinita per showmount è *enabled* a partire da ONTAP 9.2.

Requisiti ONTAP

Se la relazione di sincronizzazione include Cloud Volumes ONTAP o un cluster ONTAP on-premise ed è stato selezionato NFSv4 o successivo, sarà necessario attivare gli ACL NFSv4 sul sistema ONTAP. Questa operazione è necessaria per copiare gli ACL.

Requisiti di storage per ONTAP S3

Quando si imposta una relazione di sincronizzazione che include "Storage ONTAP S3", è necessario fornire quanto segue:

- L'indirizzo IP del LIF connesso a ONTAP S3
- La chiave di accesso e la chiave segreta che ONTAP è configurato per utilizzare

Requisiti dei server SMB

- Il server SMB può essere un sistema NetApp o un sistema non NetApp.
- È necessario fornire una copia BlueXP e la sincronizzazione con le credenziali che dispongono di autorizzazioni sul server SMB.
  - Per un server SMB di origine, sono necessarie le seguenti autorizzazioni: List and Read (elenco e lettura).

    I membri del gruppo Backup Operators sono supportati con un server SMB di origine.
  - Per un server SMB di destinazione, sono necessarie le seguenti autorizzazioni: List, Read e write.
- Il file server deve consentire a un host del data broker di accedere alle esportazioni sulle porte richieste.
  - 139 TCP
  - 445 TCP
  - 137-138 UDP
- Sono supportate le versioni SMB 1.0, 2.0, 2.1, 3.0 e 3.11.
- Assegnare al gruppo "Administrators" le autorizzazioni "controllo completo" alle cartelle di origine e di destinazione.

  Se non si concede questa autorizzazione, il broker di dati potrebbe non disporre di autorizzazioni sufficienti per ottenere gli ACL in un file o in una directory. In questo caso, viene visualizzato il seguente errore: "Getxattr error 95"

Limitazione SMB per directory e file nascosti

Una limitazione SMB influisce sulle directory e sui file nascosti durante la sincronizzazione dei dati tra server SMB. Se una delle directory o dei file sul server SMB di origine è stata nascosta tramite Windows, l'attributo nascosto non viene copiato nel server SMB di destinazione.

Comportamento di sincronizzazione SMB dovuto a una limitazione di insensibilità ai casi

Il protocollo SMB non fa distinzione tra maiuscole e minuscole, il che significa che le lettere maiuscole e minuscole sono considerate uguali. Questo comportamento può causare errori di file sovrascritti e copia della directory, se una relazione di sincronizzazione include un server SMB e i dati sono già presenti sulla destinazione.

Ad esempio, supponiamo che vi sia un file denominato "a" sull'origine e un file denominato "A" sull'origine. Quando BlueXP copia e sincronizza il file denominato "a" nella destinazione, il file "A" viene sovrascritto dal file "a" della fonte.

Nel caso delle directory, supponiamo che sia presente una directory denominata "b" sull'origine e una directory denominata "B" sull'origine. Quando BlueXP copy and Sync tenta di copiare la directory denominata "b" nella destinazione, BlueXP copy and Sync riceve un errore che indica che la directory esiste già. Di conseguenza, la copia e la sincronizzazione di BlueXP non riescono sempre a copiare la directory denominata "b."

Il modo migliore per evitare questo limite è quello di garantire la sincronizzazione dei dati in una directory vuota.

Panoramica delle reti per la copia e la sincronizzazione di BlueXP

Il networking per la copia e la sincronizzazione BlueXP include la connettività tra il gruppo di broker di dati e le ubicazioni di origine e destinazione, e una connessione Internet in uscita da broker di dati sulla porta 443.

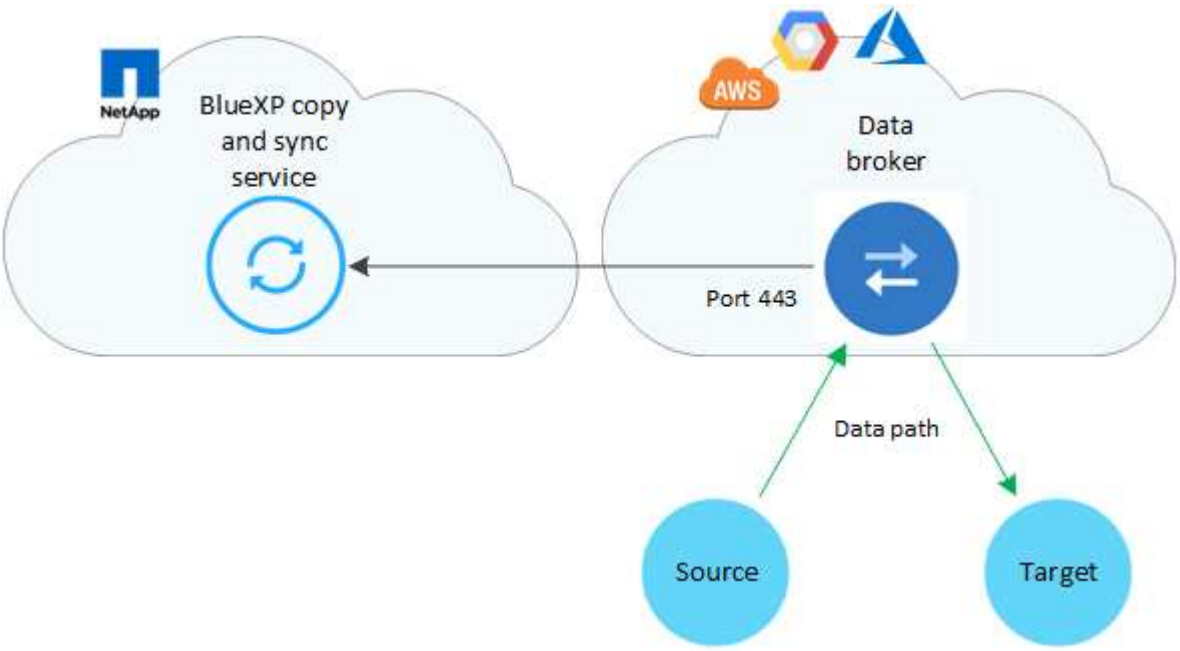
Posizione del data broker

Un gruppo di broker di dati è costituito da uno o più broker di dati installati nel cloud o on-premise.

Broker di dati nel cloud

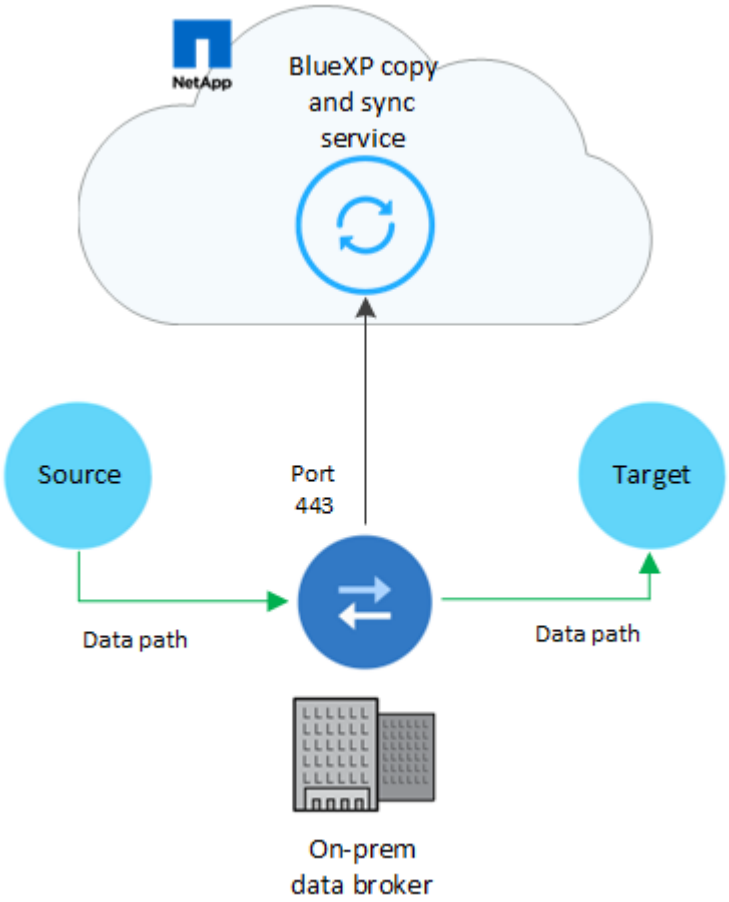
La seguente immagine mostra un broker di dati eseguito nel cloud, in AWS, Google Cloud o Azure. L'origine e la destinazione possono trovarsi in qualsiasi posizione, a condizione che vi sia una connessione al data broker. Ad esempio, è possibile che si disponga di una connessione VPN dal data center al cloud provider.

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



Broker di dati on-premise

La seguente immagine mostra il data broker in esecuzione on-premise in un data center. Anche in questo caso, l'origine e la destinazione possono trovarsi in qualsiasi posizione, a condizione che vi sia una connessione al data broker.



Requisiti di rete

- L'origine e la destinazione devono disporre di una connessione di rete al gruppo di broker di dati.

  Ad esempio, se un server NFS si trova nel data center e un broker di dati si trova in AWS, è necessaria una connessione di rete (VPN o Direct Connect) dalla rete al VPC.

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

Endpoint di rete

Il data broker di NetApp richiede l'accesso a Internet in uscita tramite la porta 443 per comunicare con il servizio di copia e sincronizzazione BlueXP e per contattare altri servizi e repository. Il browser Web locale richiede inoltre l'accesso agli endpoint per determinate azioni. Per limitare la connettività in uscita, fare riferimento al seguente elenco di endpoint durante la configurazione del firewall per il traffico in uscita.

Endpoint del data broker

Un broker di dati contatta i seguenti endpoint:

Endpoint	Scopo
https://olcentgbl.trafficmanager.net	Per contattare un repository per l'aggiornamento dei pacchetti CentOS per l'host del data broker. Questo endpoint viene contattato solo se si installa manualmente il data broker su un host CentOS.
https://rpm.nodesource.com https://registry.npmjs.org https://nodejs.org:	Per contattare i repository per l'aggiornamento di Node.js, npm e altri pacchetti di terze parti utilizzati nello sviluppo.
https://tgz.pm2.io	Per accedere a un repository per l'aggiornamento di PM2, un pacchetto di terze parti utilizzato per monitorare la copia e la sincronizzazione di BlueXP.
https://sqs.us-east-1.amazonaws.com https://kinesis.us-east-1.amazonaws.com	Per contattare i servizi AWS utilizzati da BlueXP copy e Sync per le operazioni (accodamento dei file, registrazione delle azioni e distribuzione degli aggiornamenti al data broker).
https://s3.*region*.amazonaws.com ad esempio: s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region["Per un elenco degli endpoint S3, consultare la documentazione di AWS"^]	Per contattare Amazon S3 quando una relazione di sincronizzazione include un bucket S3.
https://s3.amazonaws.com/	Quando si scaricano i registri del broker di dati da BlueXP copy e Sync, il broker di dati esegue la zip della directory dei registri e carica i registri in un bucket S3 predefinito nella regione US-East-1.
https://storage.googleapis.com/	Per contattare Google Cloud quando una relazione di sincronizzazione utilizza un bucket GCP.
https://storage-account.blob.core.windows.netSe si utilizza Azure Data Lake Gen2:https://storage-account.dfs.core.windows.net[]Dove storage-account è l’account storage di origine dell’utente.	Per aprire il proxy all'indirizzo dell'account di storage Azure di un utente.
https://cf.cloudsync.netapp.com https://repo.cloudsync.netapp.com	Per contattare il servizio di copia e sincronizzazione BlueXP.
https://support.netapp.com	Per contattare il supporto NetApp quando si utilizza una licenza BYOL per le relazioni di sincronizzazione.
https://fedoraproject.org	Per installare 7z sulla macchina virtuale del data broker durante l'installazione e gli aggiornamenti. 7z è necessario per inviare messaggi AutoSupport al supporto tecnico NetApp.

Endpoint	Scopo
https://sts.amazonaws.com https://sts.us-east-1.amazonaws.com	Per verificare le credenziali AWS quando il data broker viene implementato in AWS o quando viene implementato in sede e vengono fornite le credenziali AWS. Il data broker contatta questo endpoint durante l'implementazione, quando viene aggiornato e quando viene riavviato.
https://console.bluexp.netapp.com/ https://netapp-cloud-account.auth0.com	Per contattare la classificazione BlueXP quando si utilizza la classificazione per selezionare i file di origine per una nuova relazione di sincronizzazione.
https://pubsub.googleapis.com	Se si crea una relazione di sincronizzazione continua da un account di storage Google.
https://storage-account.queue.core.windows.nethttps://management.azure.com/subscriptions/${subscriptionId}/resourceGroups/{resourceGroup}/provider/Microsoft.EventGrid/* dove storage-account è l’account storage di origine dell’utente, subscriptionid è l’ID dell’abbonamento di origine e resourceGroup è il gruppo di risorse di origine.	Se si crea una relazione di sincronizzazione continua da un account di storage Azure.

Endpoint del browser Web

Il browser Web deve accedere al seguente endpoint per scaricare i registri a scopo di risoluzione dei problemi:

logs.cloudsync.netapp.com:443

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

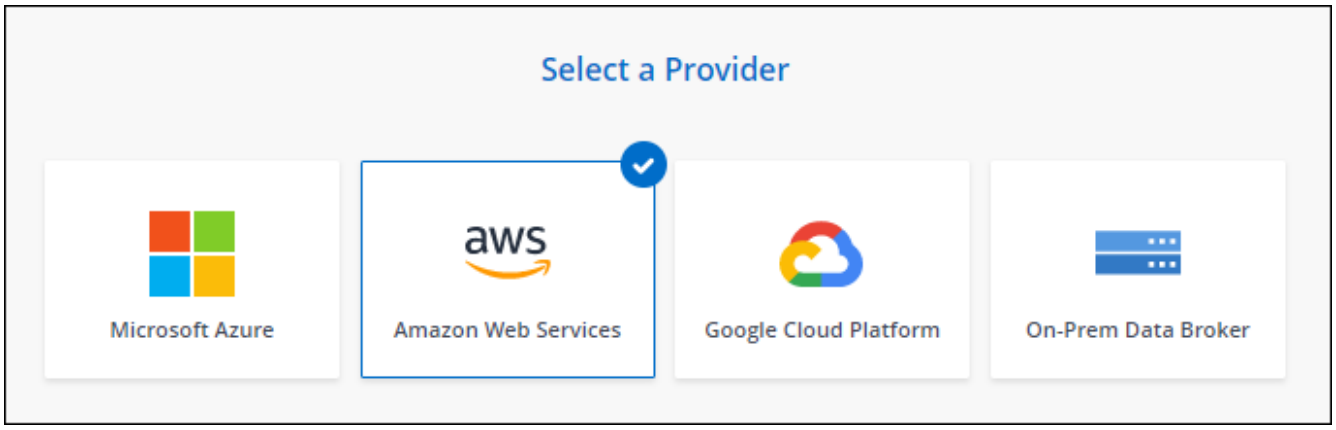
Esistono diversi modi per creare un nuovo data broker. Questi passaggi descrivono come installare un data broker in AWS quando si crea una relazione di sincronizzazione.

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.

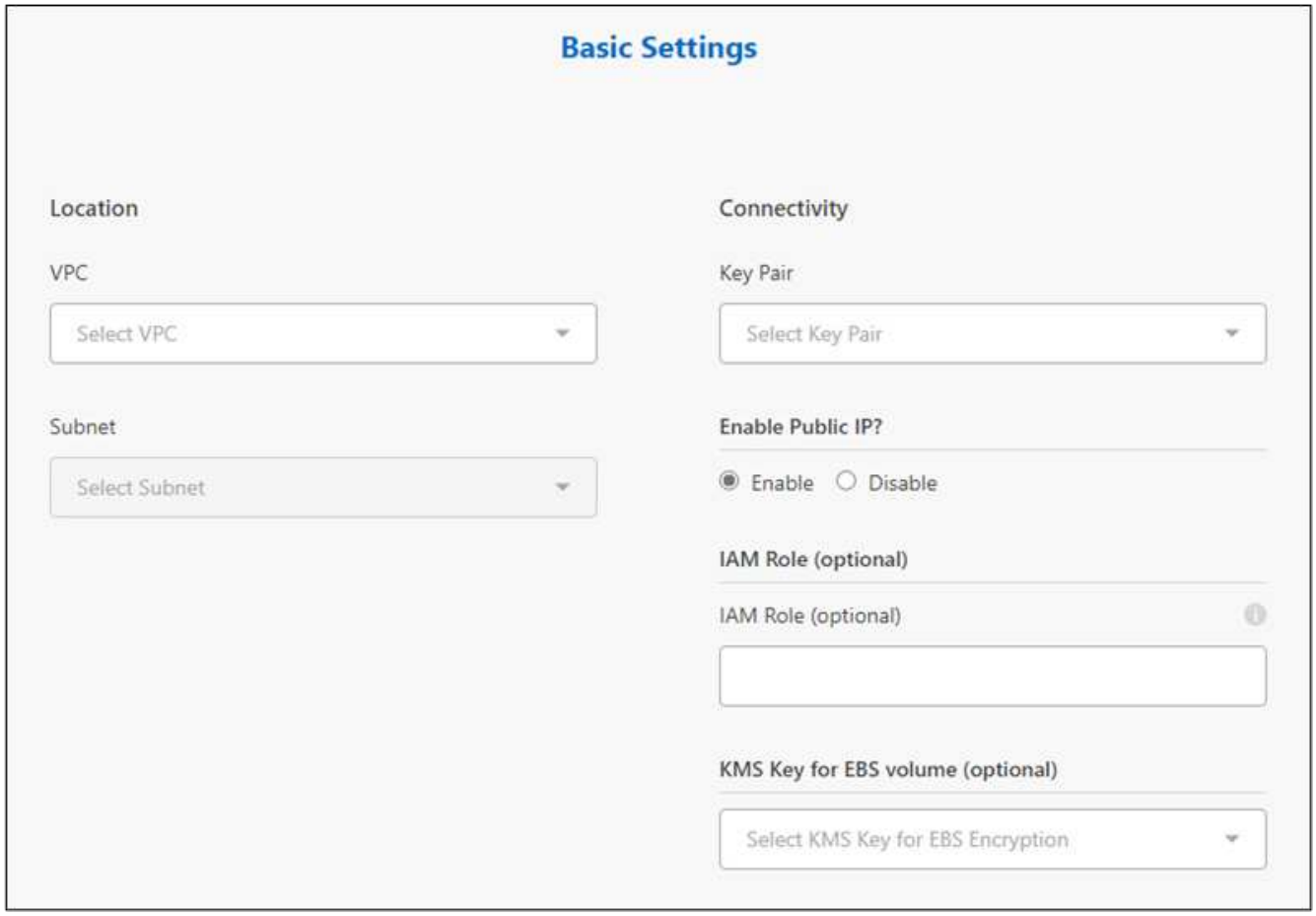
   Se invece non si desidera fornire le chiavi di accesso, selezionare il collegamento in fondo alla pagina per utilizzare un modello CloudFormation. Quando si utilizza questa opzione, non è necessario fornire le credenziali perché si effettua l'accesso direttamente ad AWS.

   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 *(video)*

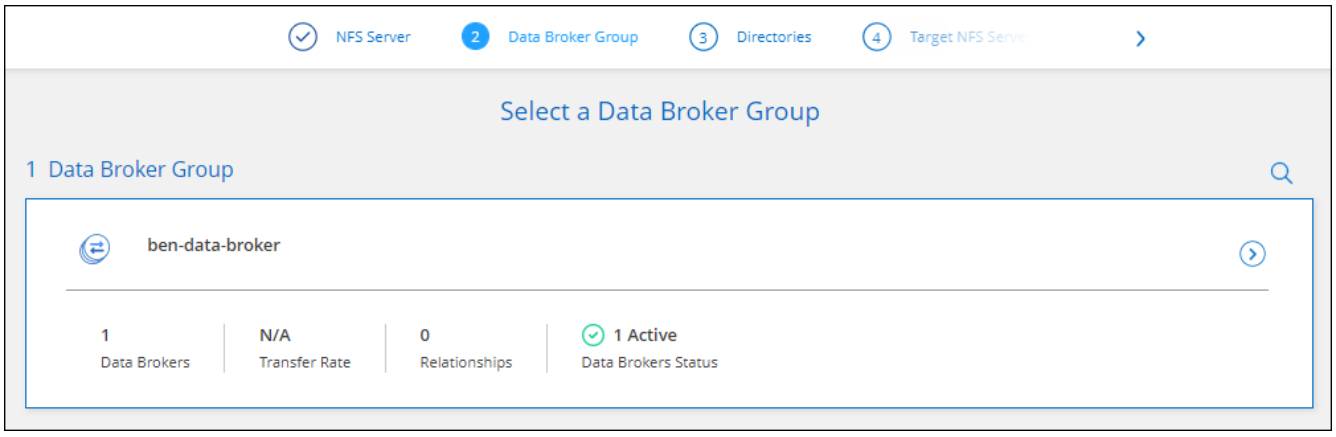
6. Se è stata inserita una chiave di accesso AWS, selezionare una posizione per l'istanza, selezionare una coppia di chiavi, scegliere se attivare un indirizzo IP pubblico e selezionare un ruolo IAM esistente oppure lasciare vuoto il campo in modo che BlueXP copy and Sync crei il ruolo per te. È inoltre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

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



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

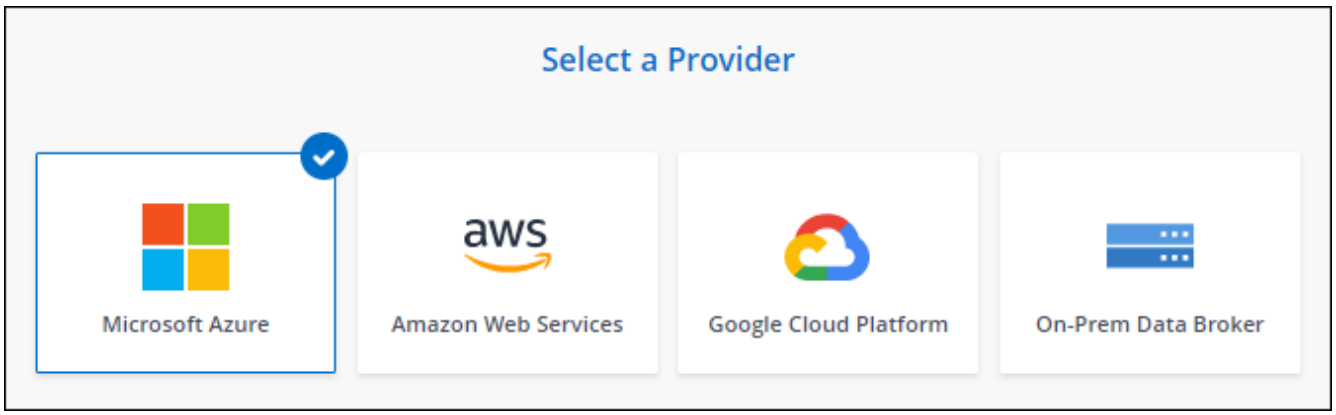
Esistono diversi modi per creare un nuovo data broker. Questi passaggi descrivono come installare un data broker in Azure quando si crea una relazione di sincronizzazione.

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**.

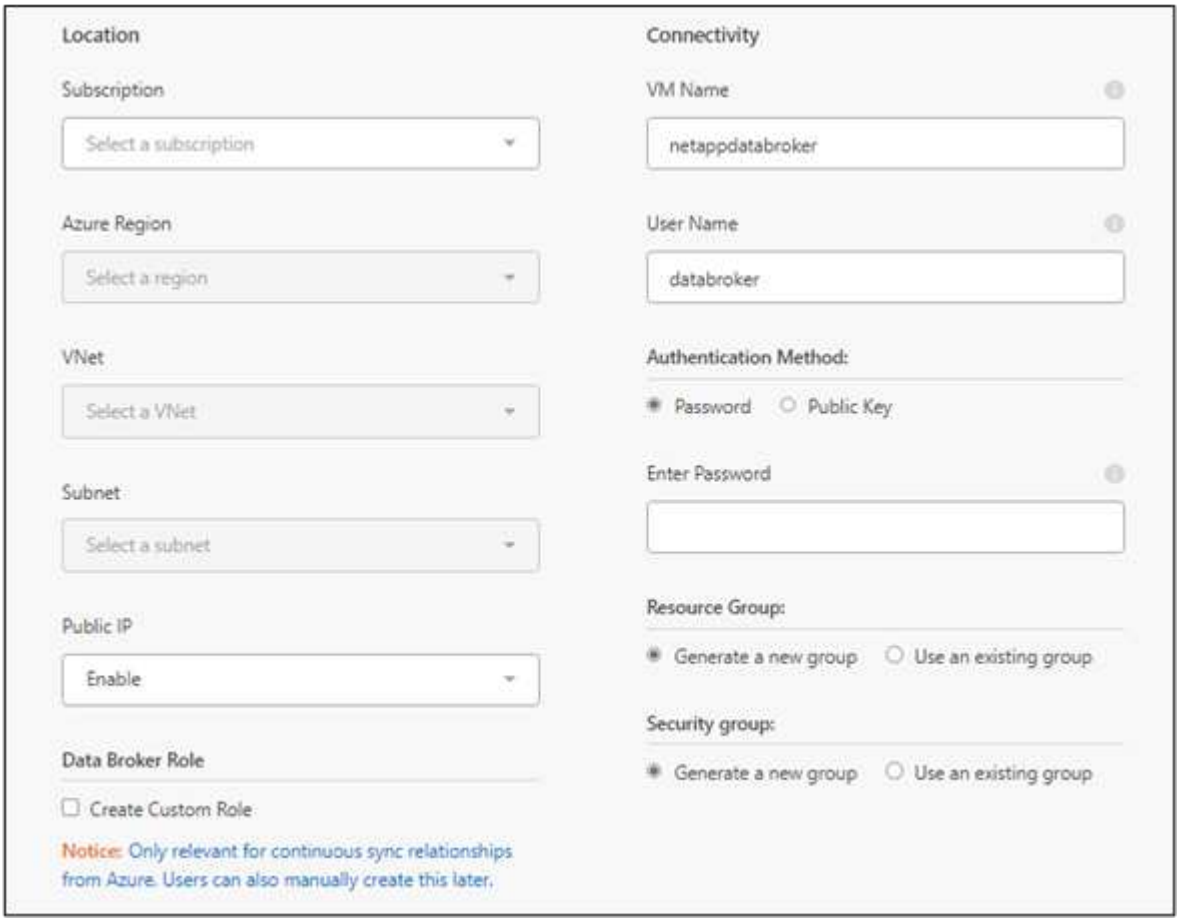
3. Nella pagina **Data Broker Group**, selezionare **Create Data Broker**, quindi selezionare **Microsoft Azure**.



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.



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

   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

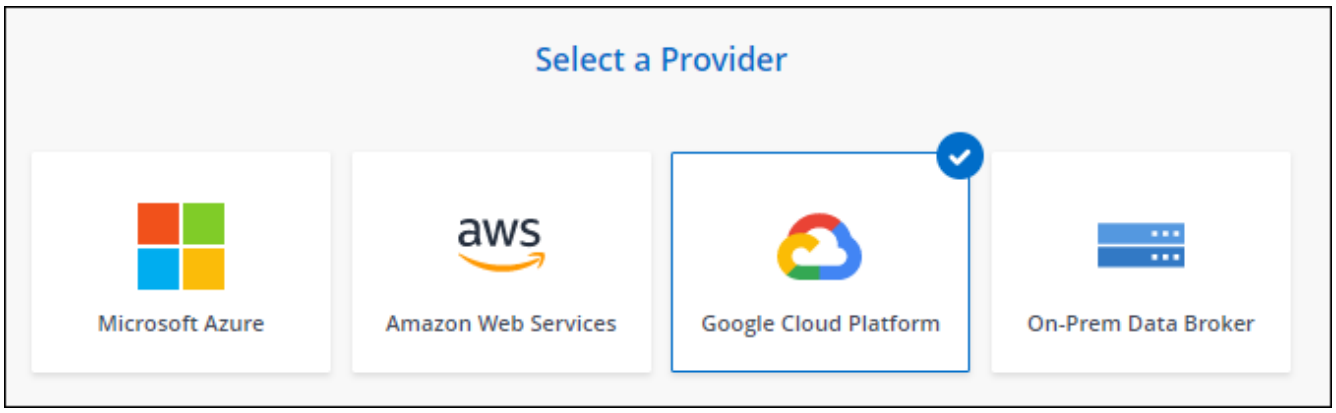
Esistono diversi modi per creare un nuovo data broker. Questi passaggi descrivono come installare un data broker in Google Cloud quando si crea una relazione di sincronizzazione.

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**.

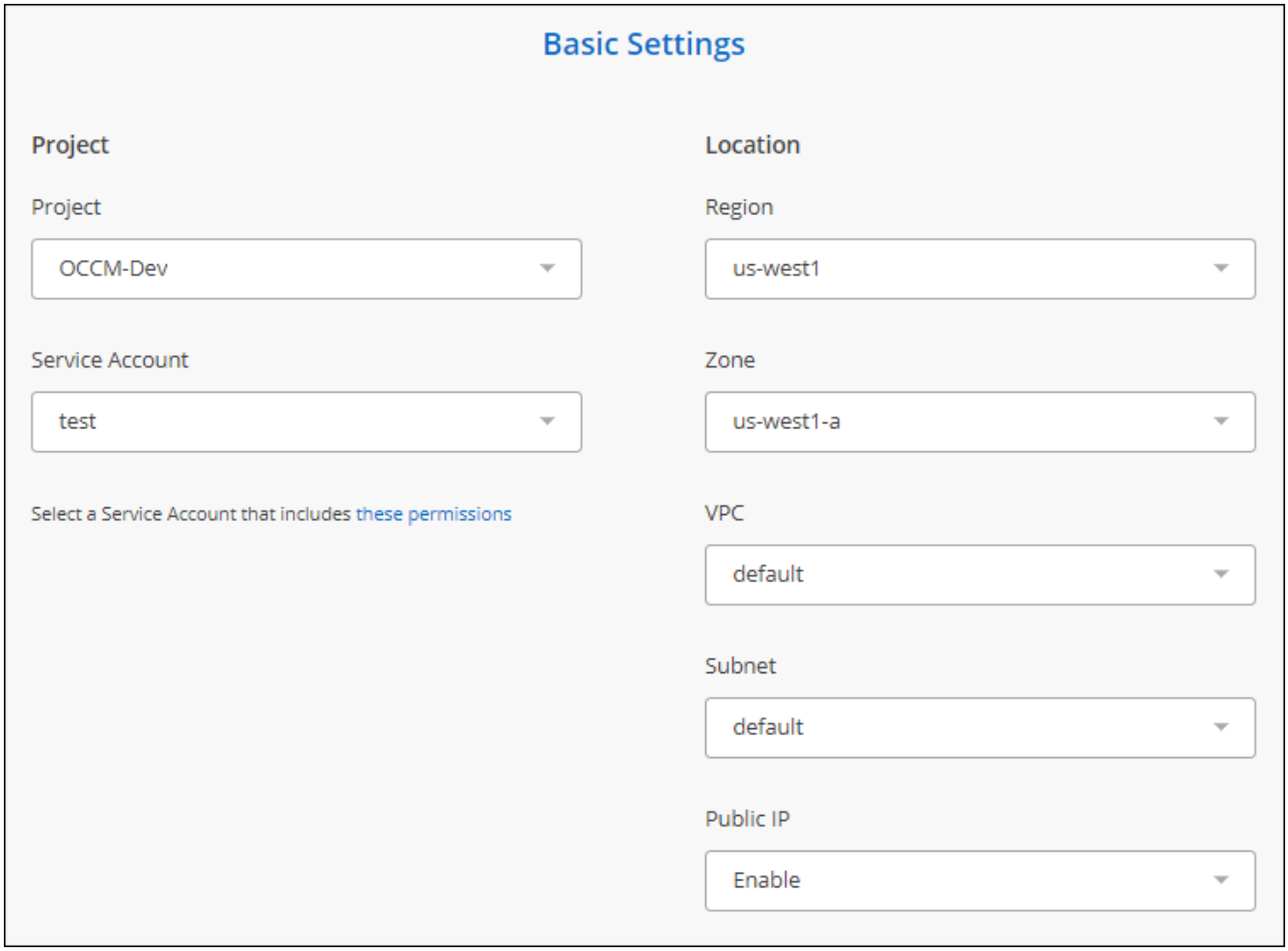


4. Immettere un nome per il data broker e selezionare **continua**.
5. Se richiesto, accedere con l'account Google.

   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.



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

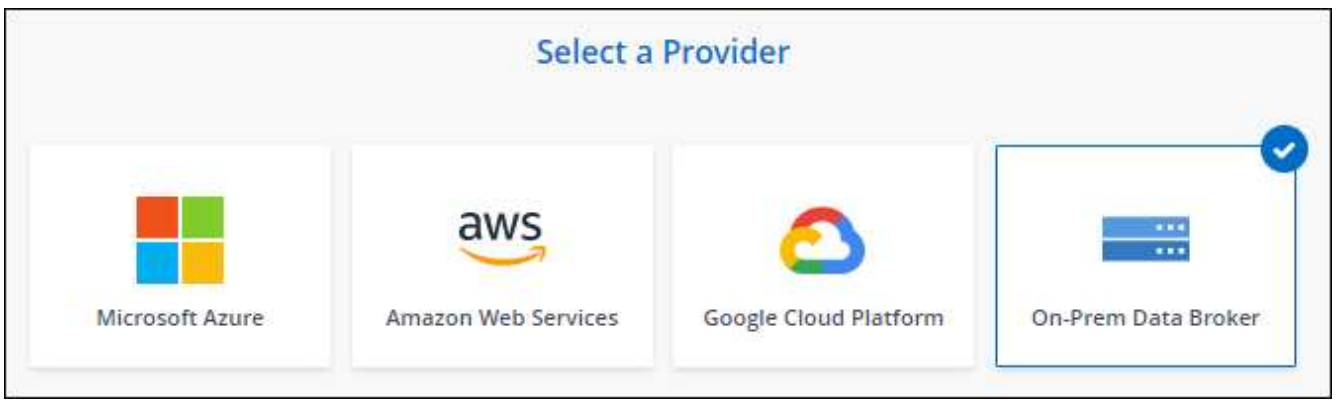
È possibile installare un data broker su un host Linux quando si crea una relazione di sincronizzazione.

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.