



Iniziare

NetApp Copy and Sync

NetApp
December 16, 2025

Sommario

Iniziare	1
Scopri di più su NetApp Copy and Sync	1
NetApp Console	1
Come funziona NetApp Copy and Sync	1
Tipi di archiviazione supportati	2
Costi	3
Avvio rapido per NetApp Copy and Sync	3
Relazioni di sincronizzazione supportate in NetApp Copy and Sync	4
Preparare l'origine e la destinazione in NetApp Copy and Sync	12
Networking	12
Directory di destinazione	12
Permessi per leggere le directory	12
Requisiti del bucket Amazon S3	13
Requisiti di archiviazione BLOB di Azure	14
Azure Data Lake Storage Gen2	16
Requisito Azure NetApp Files	16
Requisiti della scatola	17
Requisiti del bucket di Google Cloud Storage	17
Google Drive	18
Requisiti del server NFS	18
Requisiti ONTAP	18
Requisiti di archiviazione ONTAP S3	19
Requisiti del server SMB	19
Panoramica della rete per NetApp Copy and Sync	20
Posizione del broker di dati	20
Requisiti di rete	21
Endpoint di rete	21
Accedi a NetApp Copy and Sync	23
Installare un broker di dati	24
Crea un nuovo broker di dati in AWS per NetApp Copy and Sync	24
Crea un nuovo broker di dati in Azure per NetApp Copy and Sync	27
Crea un nuovo broker di dati in Google Cloud per NetApp Copy and Sync	33
Installa il broker di dati su un host Linux per NetApp Copy and Sync	38

Iniziare

Scopri di più su NetApp Copy and Sync

NetApp Copy and Sync offre un modo semplice, sicuro e automatizzato per migrare i tuoi dati verso qualsiasi destinazione, nel cloud o in sede. Che si tratti di un set di dati NAS basato su file (NFS o SMB), di un formato di oggetto Amazon Simple Storage Service (S3), di un dispositivo NetApp StorageGRID o di qualsiasi altro archivio di oggetti di un provider cloud, Copy and Sync può convertirlo e spostarlo per te.

NetApp Console

È possibile accedere a NetApp Copy and Sync tramite la NetApp Console.

NetApp Console offre una gestione centralizzata dei servizi di storage e dati NetApp in ambienti on-premise e cloud di livello aziendale. La console è necessaria per accedere e utilizzare i servizi dati NetApp. In quanto interfaccia di gestione, consente di gestire numerose risorse di archiviazione da un'unica interfaccia. Gli amministratori della console possono controllare l'accesso allo storage e ai servizi per tutti i sistemi all'interno dell'azienda.

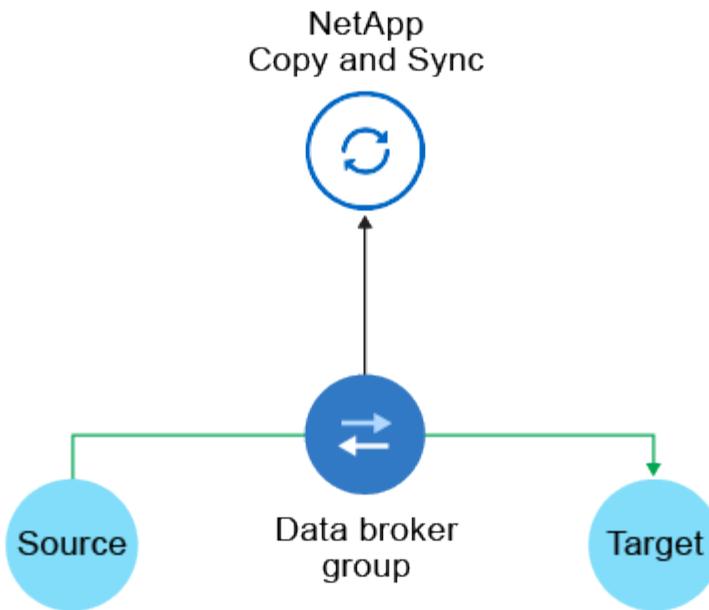
Per iniziare a utilizzare NetApp Console non è necessaria una licenza o un abbonamento e verranno addebitati costi solo quando sarà necessario distribuire gli agenti della console nel cloud per garantire la connettività ai sistemi di storage o ai servizi dati NetApp. Tuttavia, alcuni servizi dati NetApp accessibili dalla Console sono concessi in licenza o basati su abbonamento.

Scopri di più su ["NetApp Console"](#).

Come funziona NetApp Copy and Sync

NetApp Copy and Sync è una piattaforma software-as-a-service (SaaS) composta da un gruppo di broker di dati, un'interfaccia basata su cloud disponibile tramite la NetApp Console e un'origine e una destinazione.

L'immagine seguente mostra la relazione tra i componenti Copia e Sincronizzazione:



Il software del broker di dati NetApp sincronizza i dati da un'origine a una destinazione (questa è chiamata *relazione di sincronizzazione*). Puoi eseguire il broker di dati su AWS, Azure, Google Cloud Platform o in sede. Un gruppo di broker di dati, composto da uno o più broker di dati, necessita di una connessione Internet in uscita sulla porta 443 per poter comunicare con Copy and Sync e contattare alcuni altri servizi e repository. ["Visualizza l'elenco degli endpoint"](#).

Dopo la copia iniziale, Copia e sincronizzazione sincronizza tutti i dati modificati in base alla pianificazione impostata.

Tipi di archiviazione supportati

Copia e sincronizzazione supporta i seguenti tipi di archiviazione:

- Qualsiasi server NFS
- Qualsiasi server SMB
- Amazon EFS
- Amazon FSx per ONTAP
- Amazon S3
- Blob azzurro
- Azure Data Lake Storage Gen2
- Azure NetApp Files
- Box (disponibile in anteprima)
- Cloud Volumes ONTAP
- Google Cloud Storage
- Google Drive
- IBM Cloud Object Storage
- Cluster ONTAP on-premise
- Archiviazione ONTAP S3

- SFTP (utilizzando solo API)
- StorageGRID

["Visualizza le relazioni di sincronizzazione supportate"](#) .

Costi

L'utilizzo di Copia e sincronizzazione comporta due tipi di costi: costi delle risorse e costi del servizio.

Costi delle risorse

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

Spese di servizio

Al termine del periodo di prova gratuito di 14 giorni, è possibile pagare le relazioni di sincronizzazione in due modi. La prima opzione è quella di abbonarsi ad AWS o Azure, che consente di pagare su base oraria o annuale. La seconda opzione è quella di acquistare le licenze direttamente da NetApp.

["Scopri come funziona la concessione delle licenze"](#) .

Avvio rapido per NetApp Copy and Sync

Per iniziare a usare NetApp Copy and Sync sono necessari alcuni passaggi.

1

Accedi e configura la NetApp Console

Dovresti aver iniziato a usare la NetApp Console, che include l'accesso, la configurazione di un account e, possibilmente, la distribuzione di un agente Console e la creazione di sistemi.

Se si desidera creare relazioni di sincronizzazione per uno qualsiasi dei seguenti elementi, è necessario prima creare o individuare un sistema:

- Amazon FSx per ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Cluster ONTAP on-prem

Per Cloud Volumes ONTAP, cluster ONTAP on-prem e Amazon FSx for ONTAP è necessario un agente Console.

- ["Scopri come iniziare a utilizzare la NetApp Console"](#)
- ["Scopri di più sugli agenti della console"](#)

2

Prepara la tua sorgente e la tua destinazione

Verifica che la sorgente 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 di destinazione.

- ["Visualizza le relazioni supportate"](#)

- ["Preparare la sorgente e la destinazione"](#)

3

Preparare una posizione per il broker dati NetApp

Il software del broker di dati NetApp sincronizza i dati da un'origine a una destinazione (questa è chiamata *relazione di sincronizzazione*). Puoi eseguire il broker di dati su AWS, Azure, Google Cloud Platform o in sede. Un gruppo di broker di dati, composto da uno o più broker di dati, necessita di una connessione Internet in uscita sulla porta 443 per poter comunicare con NetApp Copy and Sync e contattare alcuni altri servizi e repository. ["Visualizza l'elenco degli endpoint"](#) .

NetApp Copy and Sync ti guida attraverso il processo di installazione quando crei una relazione di sincronizzazione, a quel punto puoi distribuire un broker di dati nel cloud o scaricare uno script di installazione per il tuo host Linux.

- ["Revisione dell'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

Accedi a ["la NetApp Console"](#) , seleziona **Sincronizza**, quindi trascina e rilascia le selezioni per l'origine e la destinazione. Seguire le istruzioni per completare la configurazione. ["Saperne di più"](#) .

5

Paga le tue relazioni di sincronizzazione dopo la fine del periodo di prova gratuito

Abbonati ad AWS o Azure con pagamento in base al consumo o annuale. Oppure acquista le licenze direttamente da NetApp. Per configurarlo, basta andare alla pagina Impostazioni licenza in NetApp Copy and Sync . ["Saperne di più"](#) .

Relazioni di sincronizzazione supportate in NetApp Copy and Sync

NetApp Copy and Sync consente di sincronizzare i dati da un'origine a una destinazione. Questa è chiamata relazione di sincronizzazione. Prima di iniziare, dovresti comprendere le relazioni supportate.

Posizione della fonte	Posizioni di destinazione supportate
Amazon EFS	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx per ONTAP • Amazon S3 • Blob azzurro • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • server NFS • Cluster ONTAP locale (NFS o SMB) • server SMB • StorageGRID
Amazon FSx per ONTAP	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx per ONTAP • Amazon S3 • Blob azzurro • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • server NFS • Cluster ONTAP locale (NFS o SMB) • server SMB • StorageGRID

Posizione della fonte	Posizioni di destinazione supportate
Amazon S3	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx per ONTAP • Amazon S3 • Blob azzurro • Azure Data Lake Storage Gen2 • Azure NetApp Files • Casella ¹ • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • server NFS • Cluster ONTAP locale (NFS o SMB) • Archiviazione ONTAP S3 • server SMB • StorageGRID
Blob azzurro	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx per ONTAP • Amazon S3 • Blob azzurro • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • server NFS • Cluster ONTAP locale (NFS o SMB) • server SMB • StorageGRID

Posizione della fonte	Posizioni di destinazione supportate
Azure Data Lake Storage Gen2	<ul style="list-style-type: none"> • Azure NetApp Files • Cloud Volumes ONTAP • FSx per ONTAP • IBM Cloud Object Storage • server NFS • ONTAP in sede • Archiviazione ONTAP S3 • server SMB • StorageGRID
Azure NetApp Files	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx per ONTAP • Amazon S3 • Blob azzurro • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • server NFS • Cluster ONTAP locale (NFS o SMB) • server SMB • StorageGRID
Casella ¹	<ul style="list-style-type: none"> • Amazon FSx per ONTAP • Amazon S3 • Azure NetApp Files • Cloud Volumes ONTAP • IBM Cloud Object Storage • server NFS • server SMB • StorageGRID

Posizione della fonte	Posizioni di destinazione supportate
Cloud Volumes ONTAP	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx per ONTAP • Amazon S3 • Blob azzurro • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • server NFS • Cluster ONTAP locale (NFS o SMB) • server SMB • StorageGRID
Google Cloud Storage	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx per ONTAP • Amazon S3 • Blob azzurro • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • server NFS • Cluster ONTAP locale (NFS o SMB) • Archiviazione ONTAP S3 • server SMB • StorageGRID
Google Drive	<ul style="list-style-type: none"> • server NFS • server SMB

Posizione della fonte	Posizioni di destinazione supportate
IBM Cloud Object Storage	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx per ONTAP • Amazon S3 • Blob azzurro • Azure Data Lake Storage Gen2 • Azure NetApp Files • Casella ¹ • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • server NFS • Cluster ONTAP locale (NFS o SMB) • server SMB • StorageGRID
server NFS	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx per ONTAP • Amazon S3 • Blob azzurro • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • Google Drive • IBM Cloud Object Storage • server NFS • Cluster ONTAP locale (NFS o SMB) • Archiviazione ONTAP S3 • server SMB • StorageGRID

Posizione della fonte	Posizioni di destinazione supportate
Cluster ONTAP locale (NFS o SMB)	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx per ONTAP • Amazon S3 • Blob azzurro • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • server NFS • Cluster ONTAP locale (NFS o SMB) • server SMB • StorageGRID
Archiviazione ONTAP S3	<ul style="list-style-type: none"> • Amazon S3 • Azure Data Lake Storage Gen2 • Google Cloud Storage • server NFS • server SMB • StorageGRID • Archiviazione ONTAP S3
SFTP ²	S3

Posizione della fonte	Posizioni di destinazione supportate
server SMB	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx per ONTAP • Amazon S3 • Blob azzurro • Azure Data Lake Storage Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • Google Drive • IBM Cloud Object Storage • server NFS • Cluster ONTAP locale (NFS o SMB) • Archiviazione ONTAP S3 • server SMB • StorageGRID
StorageGRID	<ul style="list-style-type: none"> • Amazon EFS • Amazon FSx per ONTAP • Amazon S3 • Blob azzurro • Azure Data Lake Storage Gen2 • Azure NetApp Files • Casella ¹ • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • server NFS • Cluster ONTAP locale (NFS o SMB) • Archiviazione ONTAP S3 • server SMB • StorageGRID

Note:

1. Il supporto Box è disponibile in anteprima.
2. Le relazioni di sincronizzazione con questa origine/destinazione sono supportate solo tramite l'API Copia e sincronizzazione.

3. È possibile scegliere un livello di archiviazione BLOB di Azure specifico quando la destinazione è un contenitore BLOB:
 - Conservazione a caldo
 - Conservazione al fresco
4. È possibile scegliere una classe di archiviazione S3 specifica quando Amazon S3 è la destinazione:
 - Standard (questa è la classe predefinita)
 - Intelligent-Tiering
 - Accesso standard-non frequente
 - Una zona - Accesso poco frequente
 - Archivio Glacier Deep
 - Recupero flessibile del ghiacciaio
 - Recupero istantaneo del ghiacciaio
5. Puoi scegliere una classe di archiviazione specifica quando la destinazione è un bucket di Google Cloud Storage:
 - Standard
 - Nearline
 - Coldline
 - Archivio

Preparare l'origine e la destinazione in NetApp Copy and Sync

Verificare che l'origine e le destinazioni soddisfino i seguenti requisiti in NetApp Copy and Sync.

Networking

- L'origine e la destinazione devono disporre di una connessione di rete al gruppo del broker dati.
Ad esempio, se un server NFS si trova nel tuo data center e un broker di dati si trova in AWS, allora hai bisogno di una connessione di rete (VPN o Direct Connect) dalla tua rete alla VPC.
- NetApp consiglia di configurare l'origine, la destinazione e i broker di dati per utilizzare un servizio Network Time Protocol (NTP). La differenza di tempo tra i tre componenti non deve superare i 5 minuti.

Directory di destinazione

Quando si crea una relazione di sincronizzazione, Copia e sincronizzazione consente di selezionare una directory di destinazione esistente e quindi, facoltativamente, di creare una nuova cartella all'interno di tale directory. Assicuratevi quindi che la directory di destinazione preferita esista già.

Permessi per leggere le directory

Per visualizzare ogni directory o cartella in un'origine o in una destinazione, Copia e sincronizzazione necessita di autorizzazioni di lettura sulla directory o sulla cartella.

NFS

I permessi devono essere definiti sulla sorgente/destinazione con uid/gid su file e directory.

Archiviazione di oggetti

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

PMI

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



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



Quando si copiano dati SMB in Cloud Volumes ONTAP tramite Copia e sincronizzazione, la proprietà di file e cartelle dal sistema di origine non viene preservata. Questo comportamento si verifica perché Copy and Sync utilizza un client SMB Linux, che assegna la proprietà all'utente o all'account di servizio utilizzato per autenticare il trasferimento. Sebbene gli elenchi di controllo degli accessi possano essere conservati, le informazioni sulla proprietà e sull'audit possono differire da quelle del sistema di origine. Questo è un comportamento previsto.

Requisiti del bucket Amazon S3

Assicurati che il tuo bucket Amazon S3 soddisfi i seguenti requisiti.

Posizioni dei broker di dati supportati per Amazon S3

Le relazioni di sincronizzazione che includono l'archiviazione S3 richiedono un broker di dati distribuito in AWS o presso la tua sede. In entrambi i casi, durante l'installazione, Copia e sincronizzazione richiede di associare il broker di dati a un account AWS.

- ["Scopri come distribuire il broker di dati AWS"](#)
- ["Scopri come installare il data broker su un host Linux"](#)

Regioni AWS supportate

Sono supportate tutte le regioni, ad eccezione 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 broker di dati.

["I permessi inclusi in questo file JSON"](#) deve essere applicato a quel bucket S3 affinché un broker di dati possa accedervi. Queste autorizzazioni consentono al broker di dati di copiare dati da e verso il bucket e di elencare gli oggetti nel bucket.

Si noti quanto segue in merito alle autorizzazioni incluse nel file JSON:

1. <BucketName> è il nome del bucket che risiede nell'account AWS non associato a un broker di dati.

2. <RoleARN> deve essere sostituito con uno dei seguenti:

- Se un broker di dati è stato installato manualmente su un host Linux, *RoleARN* dovrebbe essere l'ARN dell'utente AWS per il quale sono state fornite le credenziali AWS durante la distribuzione di un broker di dati.
- Se un broker di dati è stato distribuito in AWS utilizzando il modello CloudFormation, *RoleARN* dovrebbe essere l'ARN del ruolo IAM creato dal modello.

È possibile trovare l'ARN del ruolo accedendo alla console EC2, selezionando l'istanza del broker dati e quindi selezionando il ruolo IAM dalla scheda Descrizione. Dovresti quindi visualizzare la pagina Riepilogo nella console IAM che contiene l'ARN del ruolo.

Summary

[Delete role](#)

Role ARN	arn:aws:iam::123456789012:role/tanyaBroker0304-DataBrokeriamRole-1VMHWXMW3AQ05	
Role description	Edit	

Requisiti di archiviazione BLOB di Azure

Assicurati che l'archiviazione BLOB di Azure soddisfi i seguenti requisiti.

Posizioni dei broker di dati supportati per Azure Blob

Un broker di dati può risiedere in qualsiasi posizione quando una relazione di sincronizzazione include l'archiviazione BLOB di Azure.

Regioni di Azure supportate

Sono supportate tutte le regioni, ad eccezione di Cina, Governo degli Stati Uniti e Dipartimento della Difesa degli Stati Uniti.

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

Quando si crea una relazione di sincronizzazione tra un contenitore BLOB di Azure e un server NFS o SMB, è necessario fornire a Copia e Sincronizzazione la stringa di connessione dell'account di archiviazione:

a63cde60b553020 - Access keys

Storage account name: a63cde60b553020

key1

Key: vScjFdVZqIPyO/

Connection string: DefaultEndpoints

Se si desidera sincronizzare i dati tra due contenitori BLOB di Azure, la stringa di connessione deve includere un ["firma di accesso condiviso"](#) (SAS). È anche possibile utilizzare un SAS durante la sincronizzazione tra un contenitore BLOB e un server NFS o SMB.

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

- Per il contenitore Blob di origine: Leggi ed Elenca
- Per il contenitore Blob di destinazione: lettura, scrittura, elenco, aggiunta e creazione

The screenshot shows the Azure Storage account settings for 'a63cde60b553020'. The 'Shared access signature' tab is selected. The 'Allowed services' section has 'Blob' checked. The 'Allowed resource types' section has 'Service', 'Container', and 'Object' checked. The 'Allowed permissions' section has 'Read', 'Write', 'Delete', 'List', 'Add', and 'Create' checked. The 'Start and expiry date/time' section shows a start date of 2018-10-23 at 10:07:32 AM and an end date of 2019-10-23 at 6:07:32 PM. The 'Allowed IP addresses' section is empty. The 'Allowed protocols' section has 'HTTPS only' selected. The 'Signing key' dropdown is set to 'key1'. A red box highlights the 'Generate SAS and connection string' button at the bottom.

i Se si sceglie di implementare una relazione di sincronizzazione continua che include un contenitore BLOB di Azure, è possibile utilizzare una stringa di connessione normale o una stringa di connessione SAS. Se si utilizza una stringa di connessione SAS, non è necessario impostarla 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 Copia e Sincronizzazione con la stringa di connessione dell'account di archiviazione. Deve essere una stringa di connessione normale, non una firma di accesso condiviso (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 prestazioni.

i Se hai bisogno di aiuto per determinare il giusto livello di servizio, rivolgiti a un architetto di soluzioni. La dimensione e il livello del volume determinano la produttività ottenibile.

["Scopri di più sui livelli di servizio e sulla velocità effettiva Azure NetApp Files"](#).

Requisiti della scatola

- Per creare una relazione di sincronizzazione che includa Box, dovrà fornire le seguenti credenziali:
 - ID cliente
 - Segreto del cliente
 - Chiave privata
 - ID chiave pubblica
 - Frase segreta
 - ID aziendale
- Se si crea una relazione di sincronizzazione da Amazon S3 a Box, è necessario utilizzare un gruppo di broker di dati con una configurazione unificata in cui le seguenti impostazioni sono impostate su 1:
 - Concorrenza dello scanner
 - Limite dei processi dello scanner
 - Concorrenza del trasferente
 - Limite dei processi di trasferimento

["Scopri come definire una configurazione unificata per un gruppo di broker di dati"](#) .

Requisiti del bucket di Google Cloud Storage

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

Posizioni dei broker di dati supportati per Google Cloud Storage

Le relazioni di sincronizzazione che includono Google Cloud Storage richiedono un broker di dati distribuito in Google Cloud o in sede. Copia e sincronizzazione ti guida attraverso il processo di installazione del broker dati quando crei una relazione di sincronizzazione.

- ["Scopri come distribuire il broker di dati di Google Cloud"](#)
- ["Scopri come installare il data broker su un host Linux"](#)

Regioni Google Cloud supportate

Sono supportate tutte le regioni.

Autorizzazioni per i bucket in altri progetti Google Cloud

Quando si imposta una relazione di sincronizzazione, è possibile scegliere tra i bucket di Google Cloud in progetti diversi, 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 "lettura/elenco" sono sufficienti per sincronizzare i dati dall'origine a una destinazione.

Crittografia di un bucket Google Cloud

È possibile crittografare un bucket Google Cloud di destinazione con una chiave KMS gestita dal cliente o con la chiave predefinita gestita da Google. Se al bucket è già stata aggiunta una crittografia KMS, questa sovrascriverà la crittografia predefinita gestita da Google.

Per aggiungere una chiave KMS gestita dal cliente, sarà necessario utilizzare un broker di dati con "permessi corretti" e la chiave deve trovarsi nella stessa regione del bucket.

Google Drive

Quando imposta una relazione di sincronizzazione che include Google Drive, dovrà fornire quanto segue:

- L'indirizzo email di un utente che ha accesso alla posizione di Google Drive in cui desideri sincronizzare i dati
- L'indirizzo email di un account del servizio Google Cloud che dispone delle autorizzazioni per accedere a Google Drive
- Una chiave privata per l'account di servizio

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

- ["Creare l'account di servizio e le credenziali"](#)
- ["Delega l'autorità a livello di dominio al tuo account di servizio"](#)

Quando modifichi il campo Ambiti OAuth, immetti 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 broker di dati di accedere alle esportazioni tramite le porte richieste.
 - 111 TCP/UDP
 - 2049 TCP/UDP
 - 5555 TCP/UDP
- Sono supportate le versioni NFS 3, 4.0, 4.1 e 4.2.

La versione desiderata deve essere abilitata sul server.

- Se si desidera sincronizzare i dati NFS da un sistema ONTAP , assicurarsi che l'accesso all'elenco di esportazione NFS per una SVM sia abilitato (vserver nfs modify -vserver *svm_name* -showmount enabled).



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 locale e hai

selezionato NFSv4 o versione successiva, dovrà abilitare gli ACL NFSv4 sul sistema ONTAP . Ciò è necessario per copiare gli ACL.

Requisiti di archiviazione ONTAP S3

Quando si imposta una relazione di sincronizzazione che include "[Archiviazione ONTAP S3](#)" , dovrà 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 del server SMB

- Il server SMB può essere un sistema NetApp o un sistema non NetApp .
 - È necessario fornire a Copia e sincronizzazione le credenziali che dispongono delle autorizzazioni sul server SMB.
 - Per un server SMB di origine, sono richieste le seguenti autorizzazioni: elenco e lettura.
- I membri del gruppo Backup Operators sono supportati con un server SMB di origine.
- Per un server SMB di destinazione sono richieste le seguenti autorizzazioni: elenco, lettura e scrittura.
- Il file server deve consentire a un host del broker di dati di accedere alle esportazioni tramite le 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.
 - Concedere al gruppo "Amministratori" i permessi di "Controllo completo" sulle 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 su un file o una directory. Se ciò si verifica, verrà visualizzato il seguente errore: "getxattr error 95"

Limitazione SMB per directory e file nascosti

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

Comportamento di sincronizzazione SMB dovuto alla limitazione della non distinzione tra maiuscole e minuscole

Il protocollo SMB non distingue tra maiuscole e minuscole, il che significa che le lettere maiuscole e minuscole vengono trattate come se fossero uguali. Questo comportamento può causare errori di sovrascrittura dei file e di copia delle directory, se una relazione di sincronizzazione include un server SMB e i dati sono già presenti sulla destinazione.

Ad esempio, supponiamo che ci sia un file denominato "a" sulla sorgente e un file denominato "A" sulla destinazione. Quando Copia e sincronizzazione copia il file denominato "a" nella destinazione, il file "A" viene

sovrascritto dal file "a" della sorgente.

Nel caso delle directory, supponiamo che ci sia una directory denominata "b" sulla sorgente e una directory denominata "B" sulla destinazione. Quando Copy and Sync tenta di copiare la directory denominata "b" nella destinazione, Copy and Sync riceve un errore che indica che la directory esiste già. Di conseguenza, Copia e sincronizzazione non riesce mai a copiare la directory denominata "b".

Il modo migliore per evitare questa limitazione è assicurarsi di sincronizzare i dati in una directory vuota.

Panoramica della rete per NetApp Copy and Sync

La rete per NetApp Copy and Sync include la connettività tra il gruppo di broker di dati e le posizioni di origine e di destinazione, nonché una connessione Internet in uscita dai broker di dati sulla porta 443.

Posizione del broker di dati

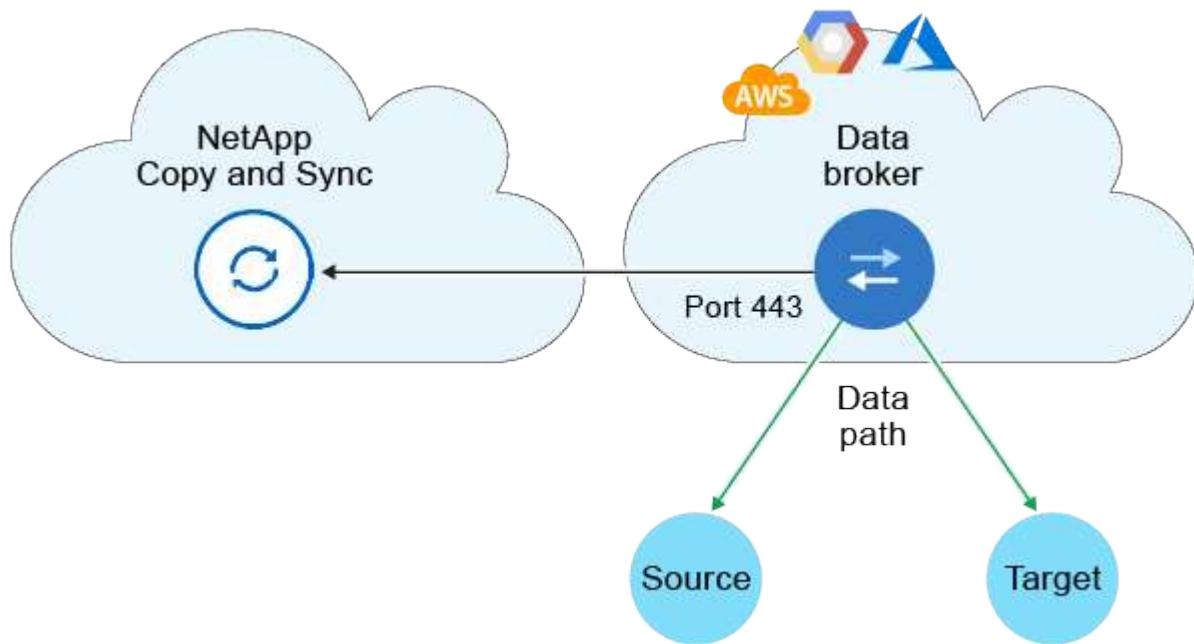
Un gruppo di broker di dati è costituito da uno o più broker di dati installati nel cloud o presso la tua sede.

Broker di dati nel cloud

L'immagine seguente mostra un broker di dati in esecuzione nel cloud, in AWS, Google Cloud o Azure. La sorgente e la destinazione possono trovarsi in qualsiasi posizione, purché ci sia una connessione al broker di dati. Ad esempio, potresti avere una connessione VPN dal tuo data center al tuo provider cloud.



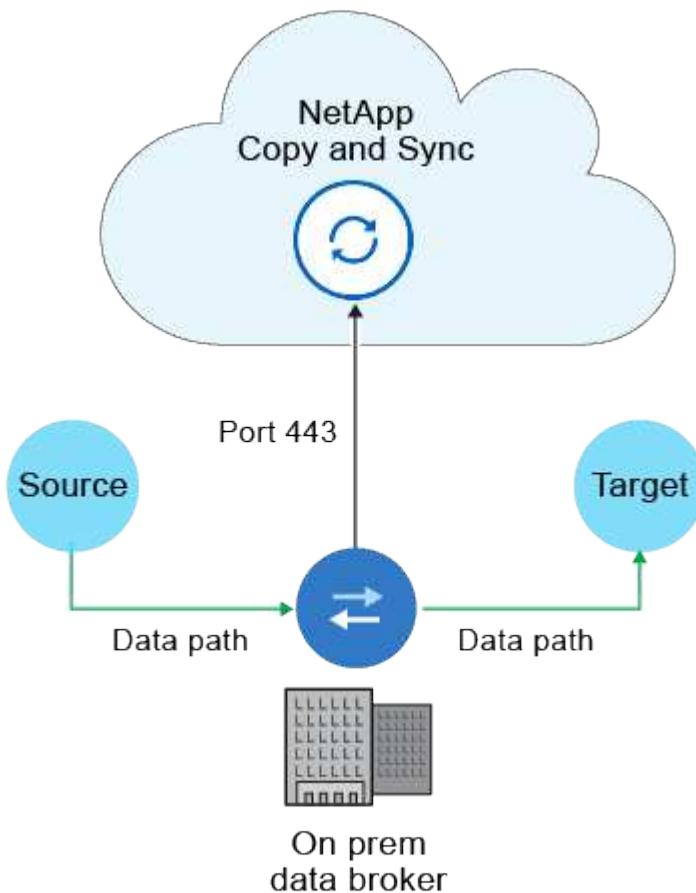
Quando Copy and Sync distribuisce il broker di dati in AWS, Azure o Google Cloud, crea un gruppo di sicurezza che abilita la comunicazione in uscita richiesta.



Broker di dati presso la tua sede

L'immagine seguente mostra il broker di dati in esecuzione in locale in un data center. Anche in questo caso, la sorgente e la destinazione possono trovarsi in qualsiasi posizione, purché ci sia una connessione al broker di

dati.



Requisiti di rete

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

Ad esempio, se un server NFS si trova nel tuo data center e un broker di dati si trova in AWS, allora hai bisogno di una connessione di rete (VPN o Direct Connect) dalla tua rete alla VPC.

- Un broker di dati necessita di una connessione Internet in uscita per poter interrogare Copy and Sync per le attività sulla porta 443.
- 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.

Endpoint di rete

Il broker di dati NetApp necessita di un accesso Internet in uscita sulla porta 443 per comunicare con Copy and Sync e per contattare alcuni altri servizi e repository. Anche il browser web locale richiede l'accesso agli endpoint per determinate azioni. Se è necessario limitare la connettività in uscita, fare riferimento al seguente elenco di endpoint durante la configurazione del firewall per il traffico in uscita.

Endpoint del broker di dati

Un broker di dati contatta i seguenti endpoint:

Punti finali	Scopo
\ https://olcentgbl.trafficmanager.net	Per contattare un repository per l'aggiornamento dei pacchetti CentOS per l'host del broker dati. Questo endpoint viene contattato solo se si installa manualmente il broker di dati 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 Copia e Sincronizzazione.
\ https://sqs.us-east-1.amazonaws.com \ https://kinesis.us-east-1.amazonaws.com	Per contattare i servizi AWS utilizzati da Copy and Sync per le operazioni (accodamento dei file, registrazione delle azioni e distribuzione degli aggiornamenti al broker di dati).
\ https://s3.region.amazonaws.com Ad esempio: s3.us-east-2.amazonaws.com:443 https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region ["Consultare la documentazione AWS per un elenco degli endpoint S3"]	Per contattare Amazon S3 quando una relazione di sincronizzazione include un bucket S3.
\ https://s3.amazonaws.com/	Quando si scaricano i log del broker di dati da Copia e sincronizzazione, il broker di dati comprime la propria directory dei log e carica i log 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 di archiviazione di origine dell'utente.	Per aprire il proxy all'indirizzo dell'account di archiviazione di Azure di un utente.
\ https://cf.cloudsync.netapp.com \ https://repo.cloudsync.netapp.com	Per contattare Copy and Sync.
\ https://support.netapp.com	Per contattare l'assistenza NetApp quando si utilizza una licenza BYOL per le relazioni di sincronizzazione.
\ https://fedoraproject.org	Per installare 7z sulla macchina virtuale del broker dati durante l'installazione e gli aggiornamenti. 7z è necessario per inviare messaggi AutoSupport al supporto tecnico NetApp .

Punti finali	Scopo
\ https://sts.amazonaws.com \ https://sts.us-east-1.amazonaws.com	Per verificare le credenziali AWS quando il broker di dati viene distribuito in AWS o quando viene distribuito nei tuoi locali e vengono fornite le credenziali AWS. Il broker di dati contatta questo endpoint durante la distribuzione, quando viene aggiornato e quando viene riavviato.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com	Per contattare NetApp Data Classification 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 archiviazione Google.
https://storage-account.queue.core.windows.net\ https://management.azure.com/subscriptions/ \${subscriptionId} /resourceGroups/\${resourceGroup}/providers/Microsoft.EventGrid/* Dove storage-account è l'account di archiviazione di origine dell'utente, subscriptionId è l'ID della sottoscrizione di origine e resourceGroup è il gruppo di risorse di origine.	Se si crea una relazione di sincronizzazione continua da un account di archiviazione di Azure.

Endpoint del browser Web

Il tuo browser web ha bisogno di accedere al seguente endpoint per scaricare i registri a scopo di risoluzione dei problemi:

logs.cloudsync.netapp.com:443

Accedi a NetApp Copy and Sync

Utilizzare la NetApp Console per accedere a NetApp Copy and Sync.

Per accedere alla Console, puoi utilizzare le credenziali del sito di supporto NetApp oppure registrarti per un accesso cloud NetApp utilizzando il tuo indirizzo email e una password. ["Scopri di più sull'accesso"](#) .

NetApp Copy and Sync utilizza la gestione dell'accesso alle identità per gestire l'accesso di ciascun utente ad azioni specifiche.

Ruolo NetApp Console obbligatorio Ruolo di amministratore dell'organizzazione. ["Scopri di più sui ruoli di accesso NetApp Console"](#) .

Passi

1. Apri un browser web e vai su "[NetApp Console](#)" .

Viene visualizzata la pagina di accesso NetApp Console .

2. Accedi alla Console.

3. Dal menu di navigazione a sinistra della Console, seleziona **Mobilità > Copia e sincronizza**.

Installare un broker di dati

Crea un nuovo broker di dati in AWS per NetApp Copy and Sync

Quando si crea un nuovo gruppo di broker di dati per NetApp Copy and Sync, scegliere Amazon Web Services per distribuire il software del broker di dati su una nuova istanza EC2 in una VPC. NetApp Copy and Sync ti guida attraverso il processo di installazione, ma i requisiti e i passaggi vengono ripetuti in questa pagina per aiutarti a preparare l'installazione.

Hai anche la possibilità di installare il data broker su un host Linux esistente nel cloud o nella tua sede. ["Saperne di più"](#) .

Regioni AWS supportate

Sono supportate tutte le regioni, ad eccezione della Cina.

Privilegi di root

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

Requisiti di rete

- Il broker di dati necessita di una connessione Internet in uscita per poter interrogare Copy and Sync per le attività sulla porta 443.

Quando Copy and Sync distribuisce il broker di dati in AWS, crea un gruppo di sicurezza che abilita la comunicazione in uscita richiesta. Si noti che è possibile configurare il broker di dati in modo che utilizzi un server proxy durante il processo di installazione.

Se è necessario limitare la connettività in uscita, vedere "[l'elenco degli endpoint contattati dal broker di dati](#)" .

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

Autorizzazioni necessarie per distribuire il broker di dati in AWS

L'account utente AWS utilizzato per distribuire il broker di dati deve disporre delle autorizzazioni incluse in ["questa politica fornita da NetApp"](#) .

Requisiti per utilizzare il proprio ruolo IAM con AWS Data Broker

Quando Copy and Sync distribuisce il broker di dati, crea un ruolo IAM per l'istanza del broker di dati. Se preferisci, puoi distribuire il data broker utilizzando il tuo ruolo IAM. Potresti utilizzare questa opzione se la tua organizzazione ha rigide politiche di sicurezza.

Il ruolo IAM deve soddisfare i seguenti requisiti:

- Al servizio EC2 deve essere consentito di assumere il ruolo IAM come entità attendibile.
- ["I permessi definiti in questo file JSON"](#) deve essere associato al ruolo IAM affinché il broker di dati possa funzionare correttamente.

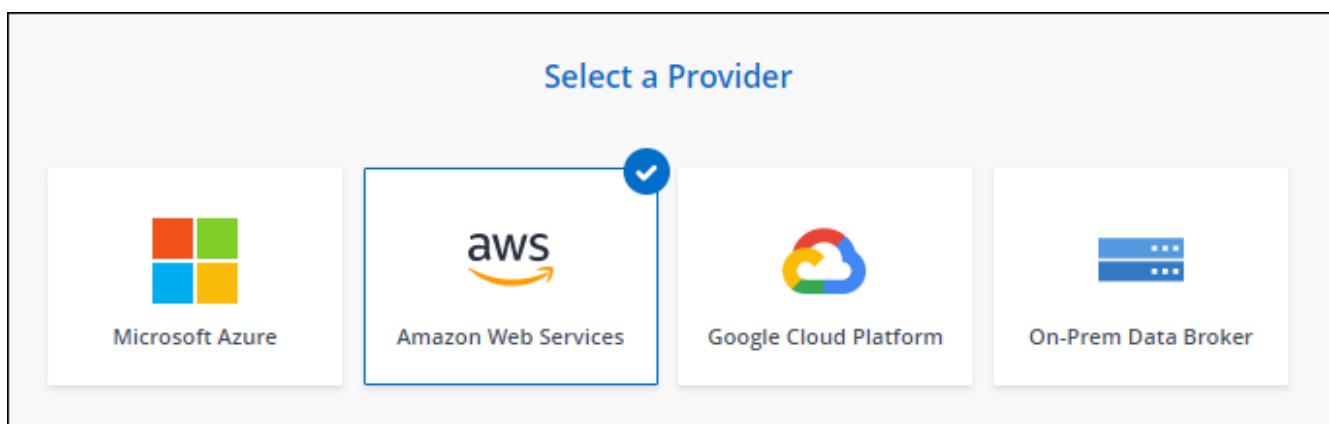
Per specificare il ruolo IAM durante la distribuzione del broker di dati, seguire i passaggi indicati di seguito.

Creare il broker di dati

Esistono diversi modi per creare un nuovo broker di dati. Questi passaggi descrivono come installare un broker di dati in AWS durante la creazione di una relazione di sincronizzazione.

Passi

1. ["Accedi a Copia e Sincronizza"](#) .
 2. Seleziona **Crea nuova sincronizzazione**.
 3. Nella pagina **Definisci relazione di sincronizzazione**, scegli un'origine e una destinazione e seleziona **Continua**.
- Completa i passaggi fino a raggiungere la pagina **Data Broker Group**.
4. Nella pagina **Gruppo Data Broker**, seleziona **Crea Data Broker** e poi seleziona **Amazon Web Services**.



5. Inserisci un nome per il broker di dati e seleziona **Continua**.
6. Inserisci una chiave di accesso AWS in modo che Copy and Sync possa creare il broker di dati in AWS per tuo conto.

Le chiavi non vengono salvate né utilizzate per altri scopi.

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

Il seguente video mostra come avviare l'istanza del broker dati utilizzando un modello CloudFormation:

Avviare un broker di dati da un modello AWS CloudFormation

7. Se hai immesso una chiave di accesso AWS, seleziona una posizione per l'istanza, seleziona una coppia di chiavi, scegli se abilitare un indirizzo IP pubblico e seleziona un ruolo IAM esistente oppure lascia il campo vuoto in modo che Copia e sincronizzazione crei il ruolo per te. Hai anche la possibilità di crittografare il tuo data broker utilizzando una chiave KMS.

Se scegli il tuo ruolo IAM, [dovrai fornire le autorizzazioni richieste](#).

Basic Settings

Location	Connectivity
VPC	Key Pair
Select VPC	Select Key Pair
Subnet	Enable Public IP?
Select Subnet	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IAM Role (optional)	
IAM Role (optional)	
Select KMS Key for EBS Encryption	
KMS Key for EBS volume (optional)	

8. Specificare una configurazione proxy, se è necessario un proxy per l'accesso a Internet nella VPC.
9. Una volta che il broker di dati è disponibile, seleziona **Continua** in Copia e sincronizza.

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

1 Data Broker Group

1 Data Brokers	N/A Transfer Rate	0 Relationships	1 Active Data Brokers Status
----------------	-------------------	-----------------	------------------------------

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

Risultato

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

Dettagli sull'istanza del broker di dati

Copia e sincronizzazione crea un broker di dati in AWS utilizzando la seguente configurazione.

Compatibilità con Node.js

v21.2.0

Tipo di istanza

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

vCPU

4

Memoria RAM

16 GB

Sistema operativo

Amazon Linux 2023

Dimensioni e tipo di disco

SSD GP2 da 10 GB

Crea un nuovo broker di dati in Azure per NetApp Copy and Sync

Quando si crea un nuovo gruppo di broker di dati per NetApp Copy and Sync, scegliere Microsoft Azure per distribuire il software del broker di dati su una nuova macchina virtuale in una rete virtuale. NetApp Copy and Sync ti guida attraverso il processo di installazione, ma i requisiti e i passaggi vengono ripetuti in questa pagina per aiutarti a preparare l'installazione.

Hai anche la possibilità di installare il data broker su un host Linux esistente nel cloud o nella tua sede. ["Saperne di più"](#).

Regioni di Azure supportate

Sono supportate tutte le regioni, ad eccezione di Cina, Governo degli Stati Uniti e Dipartimento della Difesa degli Stati Uniti.

Privilegi di root

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

Requisiti di rete

- Il broker di dati necessita di una connessione Internet in uscita per poter interrogare il servizio Copia e sincronizzazione per le attività sulla porta 443.

Quando Copy and Sync distribuisce il broker di dati in Azure, crea un gruppo di sicurezza che abilita la comunicazione in uscita richiesta.

Se è necessario limitare la connettività in uscita, vedere ["l'elenco degli endpoint contattati dal broker di dati"](#).

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

Autorizzazioni necessarie per distribuire il broker di dati in Azure

Assicurarsi che l'account utente di Azure utilizzato per distribuire il broker dati 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/agreements/read"
"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/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 abilitare "[Impostazione di sincronizzazione continua](#)" su una relazione di sincronizzazione da Azure a un'altra posizione di archiviazione cloud:

- 'Microsoft.Storage/storageAccounts/read',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/write',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/read',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/delete',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action',
- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes/action',
- 'Microsoft.EventGrid/systemTopics/read',
- 'Microsoft.EventGrid/systemTopics/write',
- 'Microsoft.EventGrid/systemTopics/delete',
- 'Microsoft.EventGrid/eventSubscriptions/write',
- 'Microsoft.Storage/storageAccounts/write'

Inoltre, l'ambito assegnabile deve essere impostato sull'ambito della sottoscrizione e **non** sull'ambito del gruppo di risorse se si prevede di 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 distribuisci il broker di dati, dovrà scegliere un metodo di autenticazione per la macchina virtuale: una password o una coppia di chiavi pubblica-privata SSH.

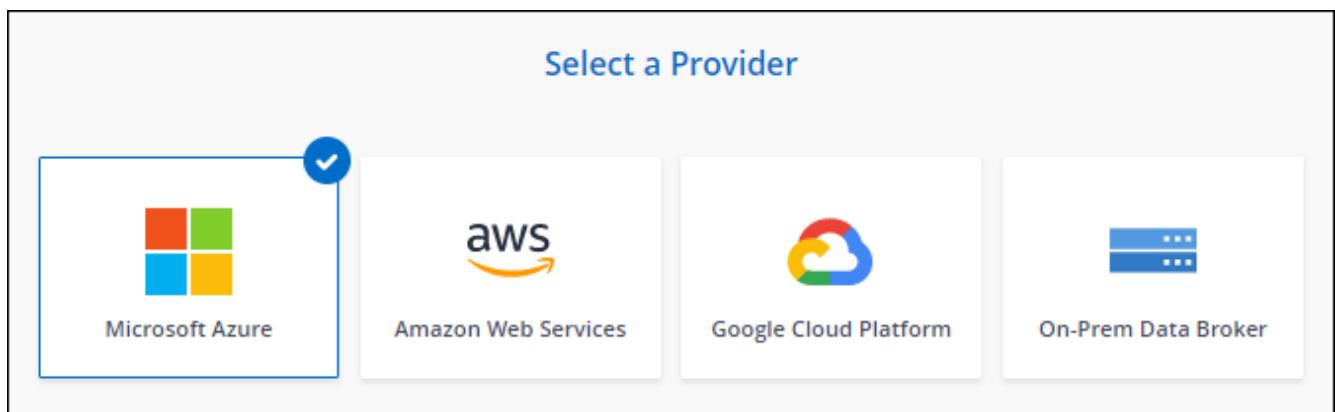
Per assistenza nella creazione di una coppia di chiavi, fare riferimento a "[Documentazione di Azure: creare e utilizzare una coppia di chiavi pubblica-privata SSH per le VM Linux in Azure](#)" .

Creare il broker di dati

Esistono diversi modi per creare un nuovo broker di dati. In questa procedura viene descritto come installare un broker di dati in Azure quando si crea una relazione di sincronizzazione.

Passi

1. "Accedi a Copia e Sincronizza".
 2. Seleziona **Crea nuova sincronizzazione**.
 3. Nella pagina **Definisci relazione di sincronizzazione**, scegli un'origine e una destinazione e seleziona **Continua**.
- Completa i passaggi fino a raggiungere la pagina **Data Broker Group**.
4. Nella pagina **Gruppo Data Broker**, seleziona **Crea Data Broker** e poi seleziona **Microsoft Azure**.



5. Inserisci un nome per il broker di dati e seleziona **Continua**.
 6. Se richiesto, accedi al tuo account Microsoft. Se non ti viene richiesto, seleziona **Accedi ad Azure**.
Il modulo è di proprietà e ospitato da Microsoft. Le tue credenziali non vengono fornite a NetApp.
7. Selezionare una posizione per il broker di dati e immettere i dettagli di base sulla macchina virtuale.

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



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

8. Specificare una configurazione proxy, se è necessario un proxy per l'accesso a Internet nella rete virtuale.
 9. Selezionare **Continua**. Se desideri aggiungere autorizzazioni S3 al tuo data broker, inserisci le tue chiavi di accesso e segrete AWS.
 10. Selezionare **Continua** e tenere aperta la pagina fino al completamento della distribuzione.
- Il processo può durare fino a 7 minuti.
11. In Copia e sincronizzazione, seleziona **Continua** una volta che il broker di dati è disponibile.
 12. Completare le pagine della procedura guidata per creare la nuova relazione di sincronizzazione.

Risultato

Hai distribuito un broker di dati in Azure e creato una nuova relazione di sincronizzazione. È possibile utilizzare questo broker di dati con relazioni di sincronizzazione aggiuntive.

Ricevi un messaggio che richiede il consenso dell'amministratore?

Se Microsoft ti avvisa che è necessaria l'approvazione dell'amministratore perché Copia e sincronizzazione necessita dell'autorizzazione per accedere alle risorse della tua organizzazione per tuo conto, hai due opzioni:

1. Chiedi all'amministratore AD di fornirti la seguente autorizzazione:

In Azure, vai su **Centro di amministrazione > Azure AD > Utenti e gruppi > Impostazioni utente** e abilita **Gli utenti possono consentire alle app di accedere ai dati aziendali per loro conto**.

2. Chiedi all'amministratore di AD di fornire il consenso per tuo conto a **CloudSync-AzureDataBrokerCreator** utilizzando il seguente URL (questo è l'endpoint del consenso dell'amministratore):

```
\ https://login.microsoftonline.com/ {INSERISCI QUI IL TUO ID  
TENANT}/v2.0/adminconsent?client_id=8ee4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri=  
https://cloudsync.netapp.com&scope=https://management.azure.com/user\_impersonationhttps://graph.microsoft.com/User.Read
```

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

Dettagli sulla VM del broker di dati

Copia e sincronizzazione crea un broker di dati in Azure utilizzando la seguente configurazione.

Compatibilità con Node.js

v21.2.0

Tipo VM

Standard DS4 v2

vCPU

8

Memoria RAM

28 GB

Sistema operativo

Rocky Linux 9,0

Dimensioni e tipo di disco

SSD Premium da 64 GB

Crea un nuovo broker di dati in Google Cloud per NetApp Copy and Sync

Quando crei un nuovo gruppo di broker di dati per NetApp Copy and Sync, scegli Google Cloud Platform per distribuire il software del broker di dati su una nuova istanza di macchina virtuale in una VPC di Google Cloud. NetApp Copy and Sync ti guida

attraverso il processo di installazione, ma i requisiti e i passaggi vengono ripetuti in questa pagina per aiutarti a preparare l'installazione.

Hai anche la possibilità di installare il data broker su un host Linux esistente nel cloud o nella tua sede. ["Saperne di più"](#) .

Regioni Google Cloud supportate

Sono supportate tutte le regioni.

Privilegi di root

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

Requisiti di rete

- Il broker di dati necessita di una connessione Internet in uscita per poter interrogare Copy and Sync per le attività sulla porta 443.

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

Se è necessario limitare la connettività in uscita, vedere ["l'elenco degli endpoint contattati dal broker di dati"](#)

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

Autorizzazioni necessarie per distribuire il broker di dati in Google Cloud

Assicurarsi che l'utente di Google Cloud che distribuisce il broker di dati 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 di servizio

Quando si distribuisce il broker di dati, 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 richiesta solo se si prevede di configurare il broker di dati per utilizzare un vault HashiCorp esterno.
2. Le autorizzazioni "pubsub.*" e "storage.buckets.update" sono necessarie solo se si prevede di abilitare l'impostazione Sincronizzazione continua su una relazione di sincronizzazione da Google Cloud Storage a un'altra posizione di archiviazione cloud. ["Scopri di più sull'opzione Sincronizzazione continua"](#).
3. Le autorizzazioni "cloudkms.cryptoKeys.list" e "cloudkms.keyRings.list" sono necessarie 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

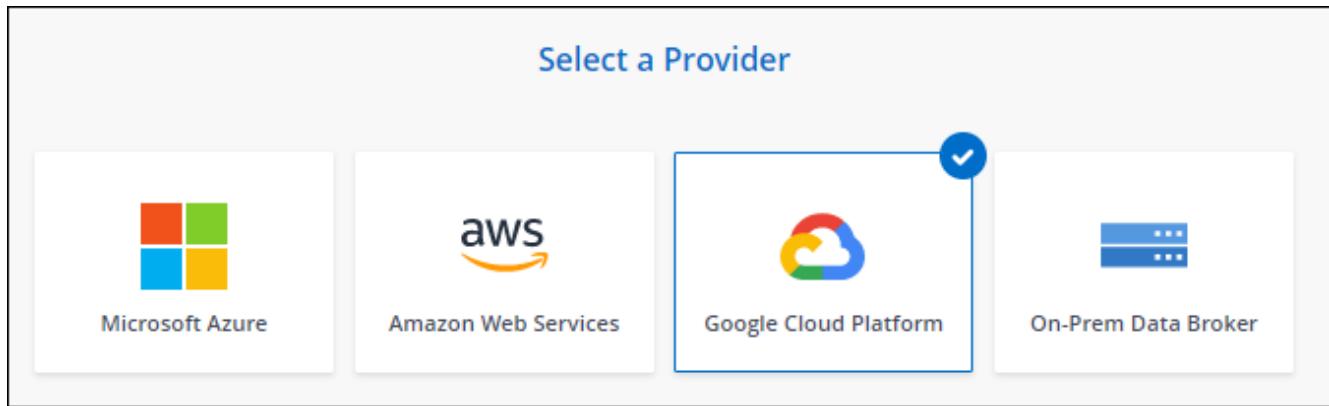
Esistono diversi modi per creare un nuovo broker di dati. Questi passaggi descrivono come installare un broker di dati in Google Cloud quando si crea una relazione di sincronizzazione.

Passi

1. ["Accedi a Copia e Sincronizza"](#).
2. Seleziona **Creare nuova sincronizzazione**.
3. Nella pagina **Definisci relazione di sincronizzazione**, scegli un'origine e una destinazione e seleziona **Continua**.

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

4. Nella pagina **Gruppo Data Broker**, seleziona **Crea Data Broker** e poi seleziona **Google Cloud Platform**.



5. Inserisci un nome per il broker di dati e seleziona **Continua**.

6. Se richiesto, accedi con il tuo account Google.

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

7. Seleziona un progetto e un account di servizio, quindi scegli una posizione per il broker di dati, specificando se desideri abilitare o disabilitare un indirizzo IP pubblico.

Se non si abilita un indirizzo IP pubblico, nel passaggio successivo sarà necessario definire un server proxy.

A screenshot of the "Basic Settings" configuration page. It includes fields for "Project" (selected "OCCM-Dev"), "Location" (selected "us-west1"), "Service Account" (selected "test"), "Zone" (selected "us-west1-a"), "VPC" (selected "default"), "Subnet" (selected "default"), and "Public IP" (selected "Enable"). There is also a note: "Select a Service Account that includes [these permissions](#)".

Basic Settings	
Project	Location
Project	Region
OCCM-Dev	us-west1
Service Account	Zone
test	us-west1-a
Select a Service Account that includes these permissions	VPC
	default
	Subnet
	default
	Public IP
	Enable

8. Specificare una configurazione proxy, se è necessario un proxy per l'accesso a Internet nella 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 broker di dati.

9. Una volta che il broker di dati è disponibile, seleziona **Continua** in Copia e sincronizza.

L'implementazione dell'istanza richiede circa 5-10 minuti. È possibile monitorare l'avanzamento tramite Copia e sincronizzazione, che si aggiorna automaticamente quando l'istanza è disponibile.

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

Risultato

Hai distribuito un data broker in Google Cloud e creato una nuova relazione di sincronizzazione. È possibile utilizzare questo broker di dati con relazioni di sincronizzazione aggiuntive.

Fornire autorizzazioni per utilizzare i bucket in altri progetti Google Cloud

Quando crei una relazione di sincronizzazione e scegli Google Cloud Storage come origine o destinazione, Copia e sincronizzazione ti consente di scegliere tra i bucket che l'account di servizio del broker di dati è autorizzato a utilizzare. Per impostazione predefinita, sono inclusi i bucket che si trovano nello stesso progetto dell'account del servizio Data Broker. Ma puoi scegliere bucket da *altri* progetti se fornisci le autorizzazioni richieste.

Passi

1. Apri la console di Google Cloud Platform e carica il servizio Cloud Storage.
2. Seleziona il nome del bucket che desideri utilizzare come origine o destinazione in una relazione di sincronizzazione.
3. Selezionare **Autorizzazioni**.
4. Selezionare **Aggiungi**.
5. Immettere il nome dell'account di servizio del broker di dati.
6. Seleziona un ruolo che forniscagli stessi permessi mostrati sopra .
7. Seleziona **Salva**.

Risultato

Quando imposta una relazione di sincronizzazione, ora puoi scegliere quel bucket come origine o destinazione nella relazione di sincronizzazione.

Dettagli sull'istanza VM del broker dati

Copia e sincronizzazione crea un broker di dati in Google Cloud utilizzando la seguente configurazione.

Compatibilità con Node.js

v21.2.0

Tipo di macchina

n2-standard-4

vCPU

4

Memoria RAM

15 GB

Sistema operativo

Rocky Linux 9,0

Dimensioni e tipo di disco

HDD da 20 GB pd-standard

Installa il broker di dati su un host Linux per NetApp Copy and Sync

Quando si crea un nuovo gruppo di broker di dati per NetApp Copy and Sync, scegliere l'opzione On-Prem Data Broker per installare il software del broker di dati su un host Linux locale o su un host Linux esistente nel cloud. NetApp Copy and Sync ti guida attraverso il processo di installazione, ma i requisiti e i passaggi vengono ripetuti in questa pagina per aiutarti a preparare l'installazione.

Requisiti host Linux

- **Compatibilità con 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, 8.9 e 9.4

- Rocky Linux 9

- Ubuntu Server 20.04 LTS, 23.04 LTS e 24.04 LTS

- SUSE Linux Enterprise Server 15 SP1

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

Un sistema Red Hat Enterprise Linux deve essere registrato presso 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 disabilitare SELinux sull'host.

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

Privilegi di root

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

Requisiti di rete

- L'host Linux deve avere una connessione con la sorgente e la 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 broker di dati comunica costantemente con il servizio Amazon SQS).
- NetApp consiglia di configurare l'origine, la destinazione e il broker di dati per utilizzare un servizio Network Time Protocol (NTP). La differenza di tempo tra i tre componenti non deve superare i 5 minuti.

Abilita l'accesso ad AWS

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

Passi

1. Creare una policy IAM utilizzando "[questa politica fornita da NetApp](#)"

["Visualizza le istruzioni AWS"](#)

2. Creare un utente IAM con accesso programmatico.

["Visualizza le istruzioni AWS"](#)

Assicurati di copiare le chiavi AWS perché dovrà specificarle quando installi il software del broker di dati.

Abilita l'accesso a Google Cloud

Se si prevede di utilizzare il broker di dati con una relazione di sincronizzazione che include un bucket di Google Cloud Storage, è necessario preparare l'host Linux per l'accesso a Google Cloud. Quando installi il broker di dati, dovrà fornire una chiave per un account di servizio che abbia autorizzazioni specifiche.

Passi

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

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

Il file dovrebbe contenere almeno le seguenti proprietà: "project_id", "private_key" e "client_email"



Quando crei una chiave, il file viene generato e scaricato sul tuo computer.

3. Salvare il file JSON sull'host Linux.

Abilita l'accesso a Microsoft Azure

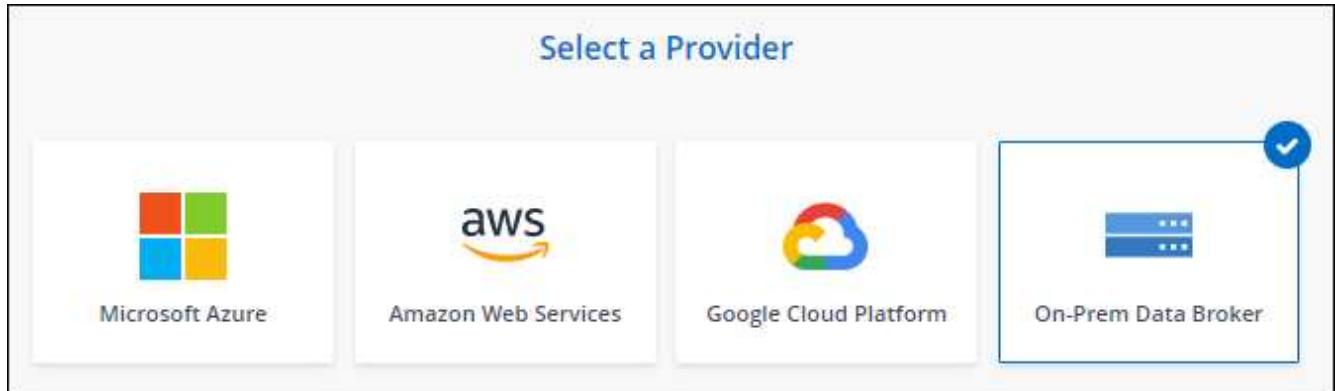
L'accesso ad Azure viene definito per relazione fornendo un account di archiviazione e una stringa di connessione nella procedura guidata Relazione di sincronizzazione.

Installa il broker di dati

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

Passi

1. ["Accedi a Copia e Sincronizza"](#).
2. Seleziona **Crea nuova sincronizzazione**.
3. Nella pagina **Definisci relazione di sincronizzazione**, scegli un'origine e una destinazione e seleziona **Continua**.
Completa i passaggi fino a raggiungere la pagina **Data Broker Group**.
4. Nella pagina **Gruppo Data Broker**, seleziona **Crea Data Broker** e poi seleziona **Data Broker locale**.



Anche se l'opzione è etichettata **On-Prem Data Broker**, si applica a un host Linux in sede o nel cloud.

5. Inserisci un nome per il broker di dati e seleziona **Continua**.

La pagina delle istruzioni verrà caricata tra poco. Dovrai seguire queste istruzioni: includono un collegamento univoco per scaricare il programma di installazione.

6. Nella pagina delle istruzioni:

- Seleziona se abilitare l'accesso ad **AWS**, **Google Cloud** o entrambi.
- Seleziona 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.

- Utilizzare i comandi per scaricare e installare il broker di dati.

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

- Scarica il programma di installazione:

- Nessun proxy:

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

- Utilizza il server proxy:

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

- Utilizza un server proxy con autenticazione:

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

URI

Copia e sincronizzazione visualizza l'URI del file di installazione nella pagina delle istruzioni, che viene caricata quando si seguono le istruzioni per distribuire On-Prem Data Broker. L'URI non viene ripetuto qui perché il collegamento viene generato dinamicamente e può essere utilizzato una sola volta. [Segui questi passaggi per ottenere l'URI da Copia e sincronizzazione](#) .

- Passare a superutente, rendere eseguibile il programma di installazione e installare il software:



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

- 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 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 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>
```

Chiavi AWS

Queste sono le chiavi per l'utente che dovrà aver preparato [seguendo questi passaggi](#) . Le chiavi AWS vengono archiviate sul data broker, che viene eseguito nella rete locale o nel cloud. NetApp non utilizza le chiavi al di fuori del broker di dati.

file JSON

Questo è il file JSON che contiene una chiave dell'account di servizio che avresti dovuto preparare [seguendo questi passaggi](#) .

- Una volta che il broker di dati è disponibile, seleziona **Continua** in Copia e sincronizza.

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

Informazioni sul copyright

Copyright © 2025 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 COMMERCIALITÀ 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 CONSEGUENZIALE (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.