



# **Copiare e sincronizzare i dati**

## **Cloud Manager 3.8**

NetApp  
March 25, 2024

# Sommario

- Copiare e sincronizzare i dati ..... 1
  - Panoramica di Cloud Sync ..... 1
  - Inizia subito ..... 4
  - Tutorial ..... 36
  - Gestione delle relazioni di sincronizzazione ..... 42
  - API Cloud Sync ..... 47
  - Domande tecniche frequenti su Cloud Sync ..... 50

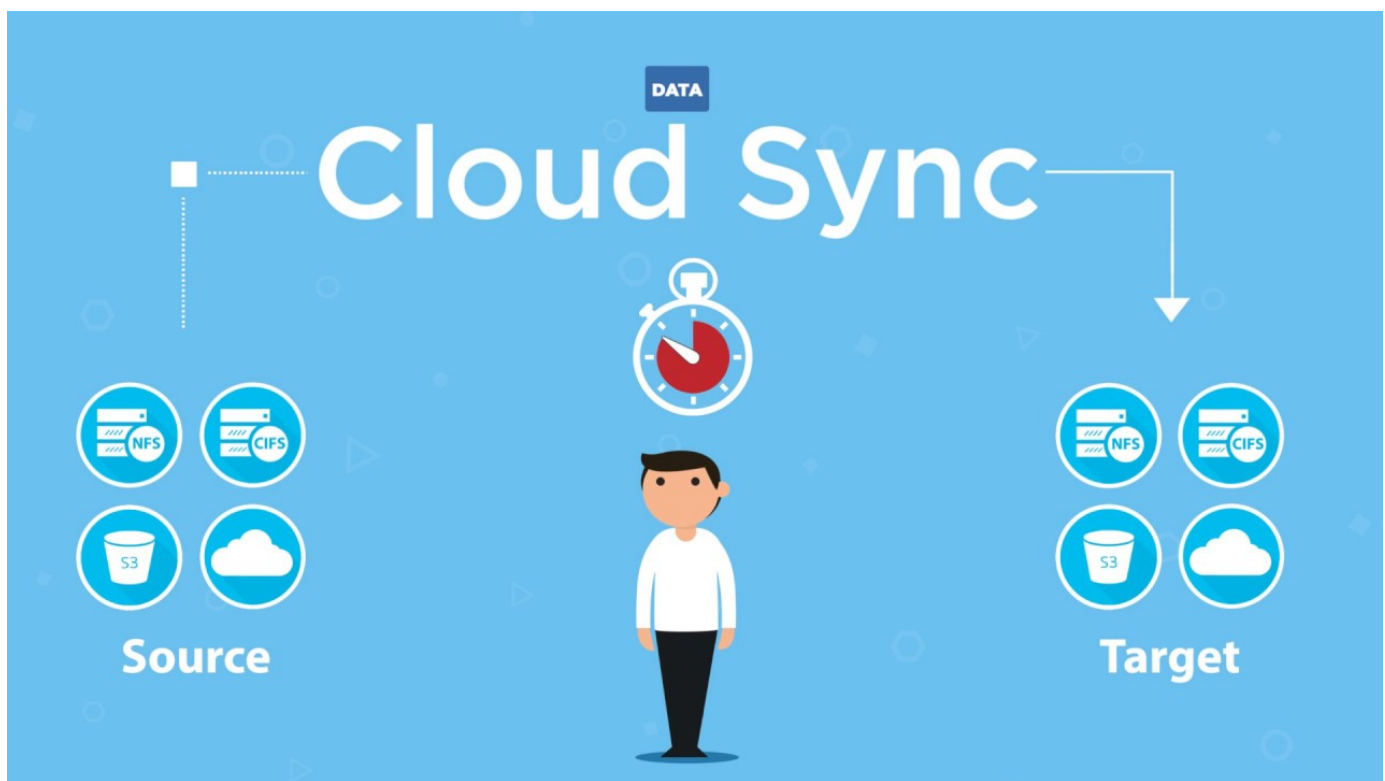
# Copiare e sincronizzare i dati

## Panoramica di Cloud Sync

Il servizio NetApp Cloud Sync offre un modo semplice, sicuro e automatizzato per migrare i dati a 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 del provider cloud, Cloud Sync può convertirlo e spostarlo per te.

### Caratteristiche

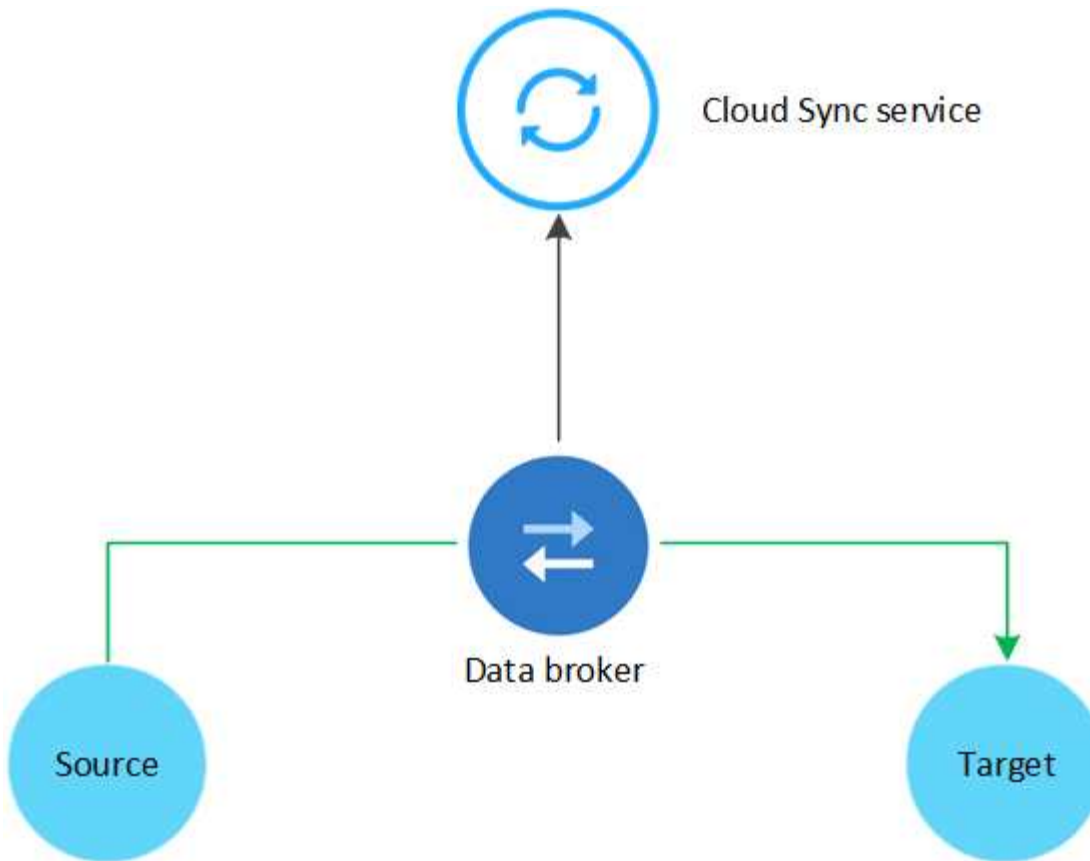
Guarda il seguente video per una panoramica di Cloud Sync:



### Come funziona Cloud Sync

Cloud Sync è una piattaforma software-as-a-service (SaaS) che comprende un broker di dati, un'interfaccia basata sul cloud disponibile tramite Cloud Manager e un'origine e un target.

La seguente immagine mostra la relazione tra i componenti di Cloud Sync:



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. Il broker di dati necessita di una connessione Internet in uscita sulla porta 443 in modo che possa comunicare con il servizio Cloud Sync 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

Cloud Sync supporta i seguenti tipi di storage:

- Qualsiasi server NFS
- Qualsiasi server SMB
- EFS AWS
- AWS S3
- Azure Blob
- Azure NetApp Files
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Storage Google Cloud
- Storage a oggetti IBM Cloud
- Cluster ONTAP on-premise
- Storage ONTAP S3

- [StorageGRID](#)

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

## Costo

L'utilizzo di Cloud Sync 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 del data broker 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. Per ulteriori informazioni, leggere le sezioni seguenti.

### Iscrizione al Marketplace

La sottoscrizione al servizio Cloud Sync di AWS o Azure consente di pagare a una tariffa oraria o annuale. ["Puoi iscriverti tramite AWS o Azure"](#), a seconda del luogo in cui si desidera essere fatturati.

### Abbonamenti orari

Con un abbonamento orario pay-as-you-go, il servizio Cloud Sync addebita ogni ora in base al numero di relazioni di sincronizzazione create.

- ["Visualizza i prezzi in Azure"](#)
- ["Visualizza i prezzi pay-as-you-go in AWS"](#)

### Abbonamenti annuali

Un abbonamento annuale fornisce una licenza per 20 relazioni di sincronizzazione che si paga in anticipo. Se superi le 20 relazioni di sincronizzazione e ti sei iscritto tramite Azure, pagherai per le relazioni aggiuntive entro l'ora.

["Visualizza i prezzi annuali in AWS"](#)

### Licenze di NetApp

Un altro modo per pagare anticipatamente le relazioni di sincronizzazione è acquistare le licenze direttamente da NetApp. Ogni licenza consente di creare fino a 20 relazioni di sincronizzazione.

È possibile utilizzare queste licenze con un abbonamento AWS o Azure. Ad esempio, se si dispone di 25 relazioni di sincronizzazione, è possibile pagare le prime 20 relazioni di sincronizzazione utilizzando una licenza e quindi pagare a consumo da AWS o Azure con le restanti 5 relazioni di sincronizzazione.

["Scopri come acquistare le licenze e aggiungerle a Cloud Sync"](#).

### Termini di licenza

I clienti che acquistano una licenza Bring Your Own (BYOL) al servizio Cloud Sync devono essere consapevoli delle limitazioni associate al diritto di licenza.

- I clienti hanno il diritto di sfruttare la licenza BYOL per un periodo non superiore a un anno dalla data di

consegna.

- I clienti hanno il diritto di sfruttare la licenza BYOL per stabilire e non superare un totale di 20 singole connessioni tra un'origine e una destinazione (ciascuna una "relazione di sincronizzazione").
- Il diritto di un cliente scade al termine del periodo di validità della licenza di un anno, indipendentemente dal fatto che il cliente abbia raggiunto la limitazione della relazione di sincronizzazione del 20.
- Nel caso in cui il cliente scelga di rinnovare la propria licenza, le relazioni di sincronizzazione inutilizzate associate alla concessione di licenza precedente NON vengono ripristinate al rinnovo della licenza.

## Privacy dei dati

NetApp non ha accesso alle credenziali fornite durante l'utilizzo del servizio Cloud Sync. Le credenziali vengono memorizzate direttamente sulla macchina del data broker, che risiede nella rete.

A seconda della configurazione scelta, Cloud Sync potrebbe richiedere le credenziali quando si crea una nuova relazione. Ad esempio, quando si imposta una relazione che include un server SMB o quando si implementa il data broker in AWS.

Queste credenziali vengono sempre salvate direttamente nel data broker stesso. Il data broker risiede su un computer della tua rete, sia esso on-premise che nel tuo account cloud. Le credenziali non vengono mai rese disponibili a NetApp.

Le credenziali vengono crittografate localmente sulla macchina del broker di dati utilizzando HashiCorp Vault.

## Limitazioni

- Cloud Sync non è supportato in Cina.
- Oltre alla Cina, il data broker Cloud Sync non è supportato nelle seguenti regioni:
  - AWS GovCloud (USA)
  - Azure US Gov
  - Azure US DOD

## Inizia subito

### Avvio rapido per Cloud Sync

La guida introduttiva al servizio Cloud Sync include alcuni passaggi.



#### 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 data broker e le posizioni di origine e destinazione. ["Scopri di più"](#).



#### 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. Il broker di dati necessita di una connessione Internet in uscita sulla porta 443 in modo che possa comunicare con il

servizio Cloud Sync e contattare altri servizi e repository. ["Visualizzare l'elenco degli endpoint"](#).

Cloud Sync ti guida attraverso il processo di installazione quando crei una relazione di sincronizzazione, a questo punto puoi implementare il 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 GCP"](#)
- ["Esaminare l'installazione dell'host Linux"](#)



### **Crea la tua prima relazione di sincronizzazione**

Accedere a ["Cloud Manager"](#), Fare clic su **Sync**, quindi trascinare le selezioni per l'origine e la destinazione. Seguire le istruzioni per completare la configurazione. ["Scopri di più"](#).



### **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. Per configurarla, accedere alla pagina Impostazioni di licenza di Cloud Sync. ["Scopri di più"](#).

## **Preparazione dell'origine e della destinazione**

Preparare la sincronizzazione dei dati verificando che l'origine e la destinazione siano supportate e configurate.

### **Relazioni di sincronizzazione supportate**

Cloud Sync consente di sincronizzare i dati da un'origine a una destinazione (chiamata *relazione di sincronizzazione*). Prima di iniziare, è necessario comprendere le relazioni supportate.

Posizione di origine	Posizioni di destinazione supportate
EFS AWS	<ul style="list-style-type: none"> <li>• EFS AWS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (NFS)</li> <li>• Cloud Volumes ONTAP (NFS)</li> <li>• Cloud Volumes Service (NFS)</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Storage Google Cloud</li> <li>• Server NFS</li> <li>• Cluster ONTAP on-premise</li> <li>• StorageGRID</li> </ul>
AWS S3	<ul style="list-style-type: none"> <li>• EFS AWS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Storage Google Cloud</li> <li>• Server NFS</li> <li>• Cluster ONTAP on-premise</li> <li>• Server SMB</li> <li>• StorageGRID</li> </ul>



Posizione di origine	Posizioni di destinazione supportate
Azure Blob	<ul style="list-style-type: none"> <li>• EFS AWS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Storage Google Cloud</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Server NFS</li> <li>• Cluster ONTAP on-premise</li> <li>• Server SMB</li> <li>• StorageGRID</li> </ul>
Azure NetApp Files (NFS)	<ul style="list-style-type: none"> <li>• EFS AWS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (NFS)</li> <li>• Cloud Volumes ONTAP (NFS)</li> <li>• Cloud Volumes Service (NFS)</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Storage Google Cloud</li> <li>• Server NFS</li> <li>• Cluster ONTAP on-premise</li> <li>• StorageGRID</li> </ul>
Azure NetApp Files (PMI)	<ul style="list-style-type: none"> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (PMI)</li> <li>• Cloud Volumes ONTAP (PMI)</li> <li>• Cloud Volumes Service (PMI)</li> <li>• Storage Google Cloud</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Cluster ONTAP on-premise</li> <li>• Server SMB</li> <li>• StorageGRID</li> </ul>

Posizione di origine	Posizioni di destinazione supportate
Cloud Volumes ONTAP (NFS)	<ul style="list-style-type: none"> <li>• EFS AWS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (NFS)</li> <li>• Cloud Volumes ONTAP (NFS)</li> <li>• Cloud Volumes Service (NFS)</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Storage Google Cloud</li> <li>• Server NFS</li> <li>• Cluster ONTAP on-premise</li> <li>• StorageGRID</li> </ul>
Cloud Volumes ONTAP (PMI)	<ul style="list-style-type: none"> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (PMI)</li> <li>• Cloud Volumes ONTAP (PMI)</li> <li>• Cloud Volumes Service (PMI)</li> <li>• Storage Google Cloud</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Cluster ONTAP on-premise</li> <li>• Server SMB</li> <li>• StorageGRID</li> </ul>
Cloud Volumes Service (NFS)	<ul style="list-style-type: none"> <li>• EFS AWS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (NFS)</li> <li>• Cloud Volumes ONTAP (NFS)</li> <li>• Cloud Volumes Service (NFS)</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Storage Google Cloud</li> <li>• Server NFS</li> <li>• Cluster ONTAP on-premise</li> <li>• StorageGRID</li> </ul>

Posizione di origine	Posizioni di destinazione supportate
Cloud Volumes Service (PMI)	<ul style="list-style-type: none"> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (PMI)</li> <li>• Cloud Volumes ONTAP (PMI)</li> <li>• Cloud Volumes Service (PMI)</li> <li>• Storage Google Cloud</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Cluster ONTAP on-premise</li> <li>• Server SMB</li> <li>• StorageGRID</li> </ul>
Storage Google Cloud	<ul style="list-style-type: none"> <li>• EFS AWS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Storage Google Cloud</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Server NFS</li> <li>• Cluster ONTAP on-premise</li> <li>• Server SMB</li> <li>• StorageGRID</li> </ul>
Storage a oggetti IBM Cloud	<ul style="list-style-type: none"> <li>• EFS AWS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Storage Google Cloud</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Server NFS</li> <li>• Cluster ONTAP on-premise</li> <li>• Server SMB</li> <li>• StorageGRID</li> </ul>

Posizione di origine	Posizioni di destinazione supportate
Server NFS	<ul style="list-style-type: none"> <li>• EFS AWS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (NFS)</li> <li>• Cloud Volumes ONTAP (NFS)</li> <li>• Cloud Volumes Service (NFS)</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Storage Google Cloud</li> <li>• Server NFS</li> <li>• Cluster ONTAP on-premise</li> <li>• StorageGRID</li> </ul>
Cluster ONTAP on-premise (NFS)	<ul style="list-style-type: none"> <li>• EFS AWS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (NFS)</li> <li>• Cloud Volumes ONTAP (NFS)</li> <li>• Cloud Volumes Service (NFS)</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Storage Google Cloud</li> <li>• Server NFS</li> <li>• Cluster ONTAP on-premise</li> <li>• StorageGRID</li> </ul>
Cluster ONTAP on-premise (SMB)	<ul style="list-style-type: none"> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (PMI)</li> <li>• Cloud Volumes ONTAP (PMI)</li> <li>• Cloud Volumes Service (PMI)</li> <li>• Storage Google Cloud</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Cluster ONTAP on-premise</li> <li>• Server SMB</li> <li>• StorageGRID</li> </ul>
Storage ONTAP S3	<ul style="list-style-type: none"> <li>• StorageGRID</li> </ul>

Posizione di origine	Posizioni di destinazione supportate
Server SMB	<ul style="list-style-type: none"> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files (PMI)</li> <li>• Cloud Volumes ONTAP (NFS)</li> <li>• Cloud Volumes Service (NFS)</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Storage Google Cloud</li> <li>• Cluster ONTAP on-premise</li> <li>• Server SMB</li> <li>• StorageGRID</li> </ul>
StorageGRID	<ul style="list-style-type: none"> <li>• EFS AWS</li> <li>• AWS S3</li> <li>• Azure Blob</li> <li>• Azure NetApp Files</li> <li>• Cloud Volumes ONTAP</li> <li>• Cloud Volumes Service</li> <li>• Storage a oggetti IBM Cloud</li> <li>• Storage Google Cloud</li> <li>• Server NFS</li> <li>• Cluster ONTAP on-premise</li> <li>• Storage ONTAP S3</li> <li>• Server SMB</li> <li>• StorageGRID</li> </ul>

**Note:**

1. È possibile scegliere un livello di storage Azure Blob specifico quando un container Blob è la destinazione:
  - Storage a caldo
  - Storage fresco
2. È possibile scegliere una classe di storage S3 specifica quando AWS S3 è la destinazione:
  - Standard (classe predefinita)
  - Tiering intelligente
  - Standard-infrequent Access (accesso standard-non frequente)
  - Accesso non frequente a una sola zona
  - Ghiacciaio
  - Glacier Deep Archive

## Networking per l'origine e la destinazione

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

Ad esempio, se un server NFS si trova nel data center e il data broker 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 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.

## Requisiti di origine e destinazione

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

### requisiti del bucket AWS S3

Assicurarsi che il bucket AWS S3 soddisfi i seguenti requisiti.

## Posizioni dei data broker supportate per AWS 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, Cloud 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 di quelle della Cina e di GovCloud (USA).

## 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 al data broker.

["Le autorizzazioni incluse in questo file JSON"](#) Deve essere applicato al bucket S3 in modo che il data broker 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 al data broker.
2. *<RoleARN>* deve essere sostituito con uno dei seguenti elementi:
  - Se il 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 del data broker.
  - Se il data broker è stato implementato in AWS utilizzando il modello CloudFormation, *RoleARN* dovrebbe 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 e fare clic sul ruolo IAM nella scheda Description (Descrizione). Viene visualizzata la pagina Summary (Riepilogo) nella console IAM che contiene il ruolo ARN.

**Role ARN** `arn:aws:iam::042991749898:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05` 

**Role description** [Edit](#)

### requisiti di storage di Azure Blob

Assicurati che lo storage Azure Blob soddisfi i seguenti requisiti.

### Posizioni dei data broker supportate per Azure Blob

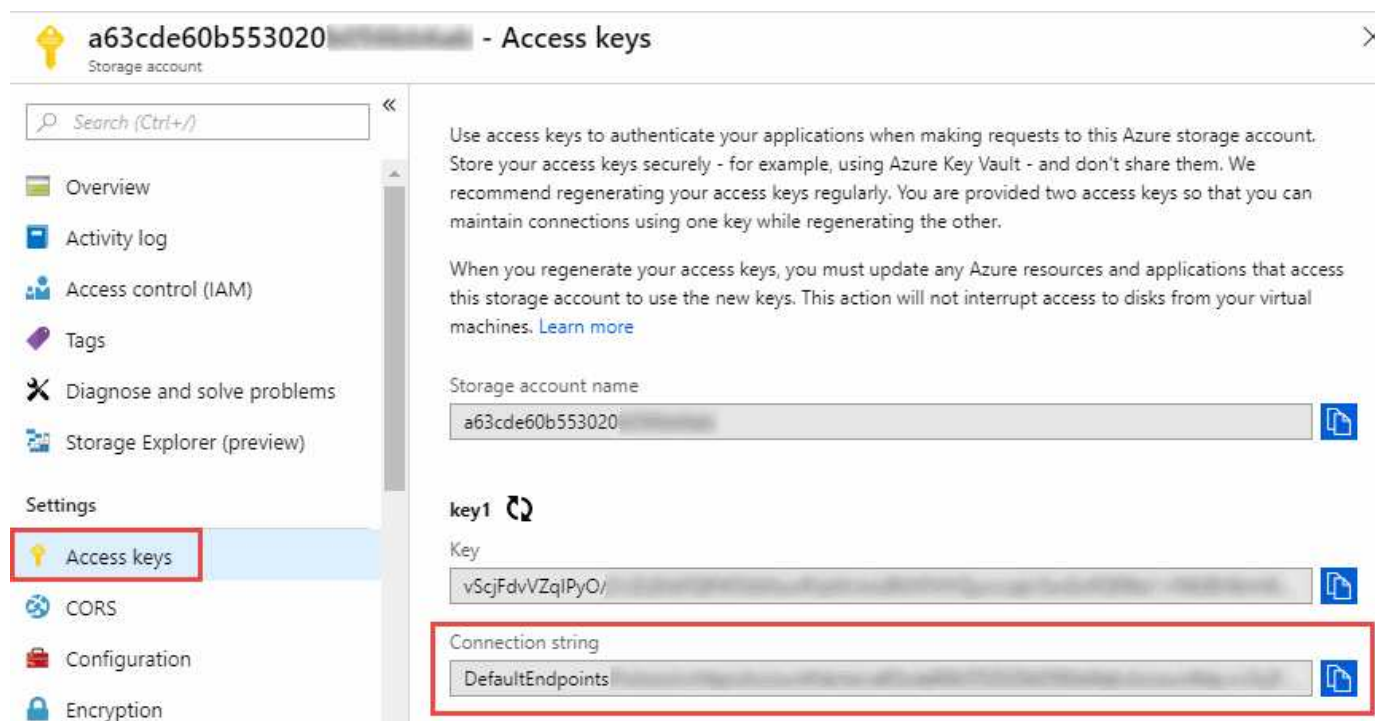
Il data broker può risiedere in qualsiasi posizione quando una relazione di sincronizzazione include lo storage Azure Blob.

### Aree Azure supportate

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

### Stringa di connessione richiesta 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 a Cloud Sync la stringa di connessione dell'account di storage:



**a63cde60b553020** - Access keys

Storage account

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Storage Explorer (preview)

Settings

- Access keys**
- CORS
- Configuration
- Encryption

Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to disks from your virtual machines. [Learn more](#)

Storage account name  
a63cde60b553020

**key1**

Key  
vScjFdvVZqIPyO/

Connection string  
DefaultEndpoints

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

### 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 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 GCP o on-premise. Cloud Sync ti guida nel processo di installazione del data broker quando crei una relazione di sincronizzazione.



- ["Scopri come implementare il data broker GCP"](#)
- ["Scopri come installare il data broker su un host Linux"](#)

## Regioni GCP supportate

Sono supportate tutte le regioni.

## Requisiti del server NFS

- Il server NFS può essere un sistema NetApp o un sistema non NetApp.
- Il file server deve consentire all'host del data broker di accedere alle esportazioni.
- 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 di storage per ONTAP S3

ONTAP 9.7 supporta Amazon Simple Storage Service (Amazon S3) come anteprima pubblica. ["Scopri di più sul supporto ONTAP per Amazon S3"](#).

Quando si imposta una relazione di sincronizzazione che include lo 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.
- Il file server deve consentire all'host del data broker di accedere alle esportazioni.
- 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 Cloud Sync copia il file denominato "a" nella destinazione, il file "A" viene sovrascritto dal file "a" proveniente dall'origine.

Nel caso delle directory, supponiamo che sia presente una directory denominata "b" sull'origine e una directory denominata "B" sull'origine. Quando Cloud Sync tenta di copiare la directory denominata "b" nella destinazione, Cloud Sync riceve un errore che indica che la directory esiste già. Di conseguenza, Cloud Sync non riesce 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.

### 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.

## Panoramica delle reti per Cloud Sync

Il networking per Cloud Sync include la connettività tra il broker di dati e le posizioni di origine e destinazione e una connessione Internet in uscita dal broker di dati sulla porta 443.

### Posizione del data broker

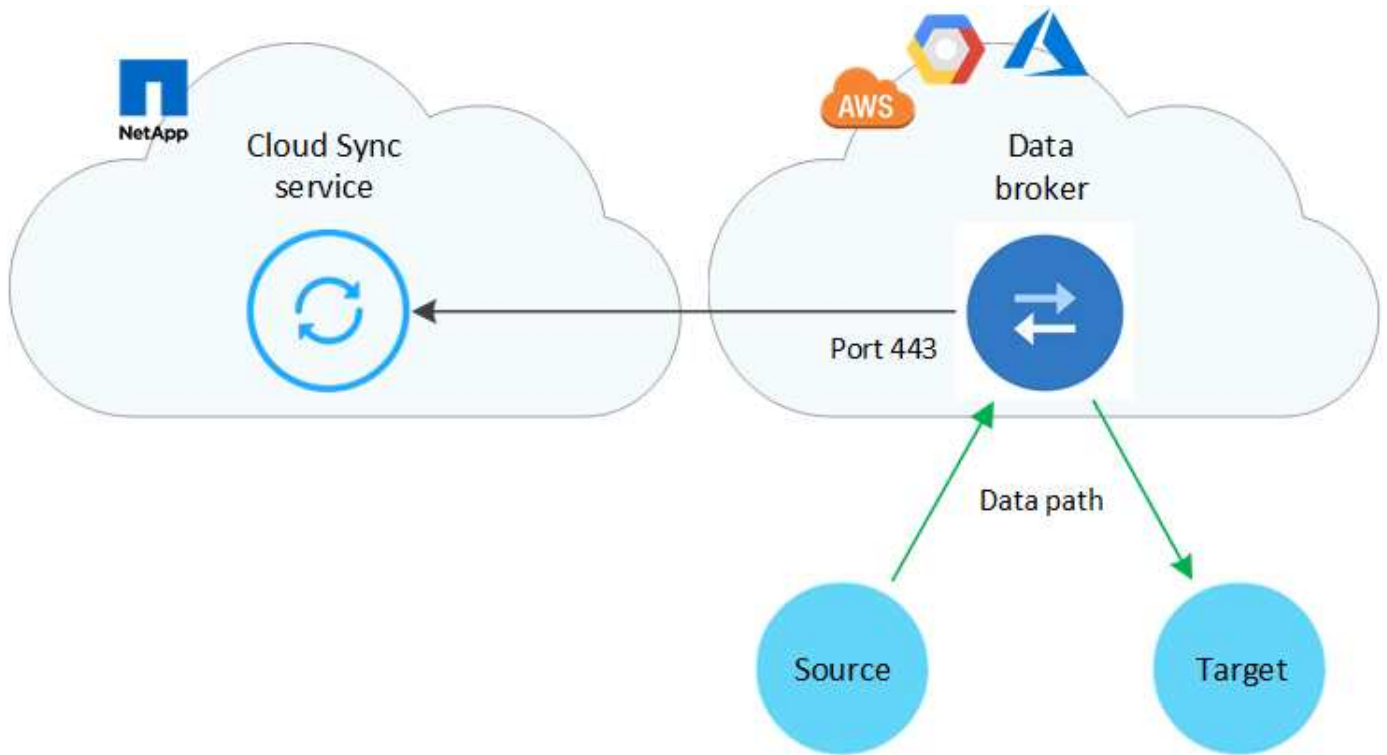
Puoi installare il data broker nel cloud o on-premise.

#### Broker di dati nel cloud

L'immagine seguente mostra il data broker in esecuzione nel cloud, in AWS, GCP 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.

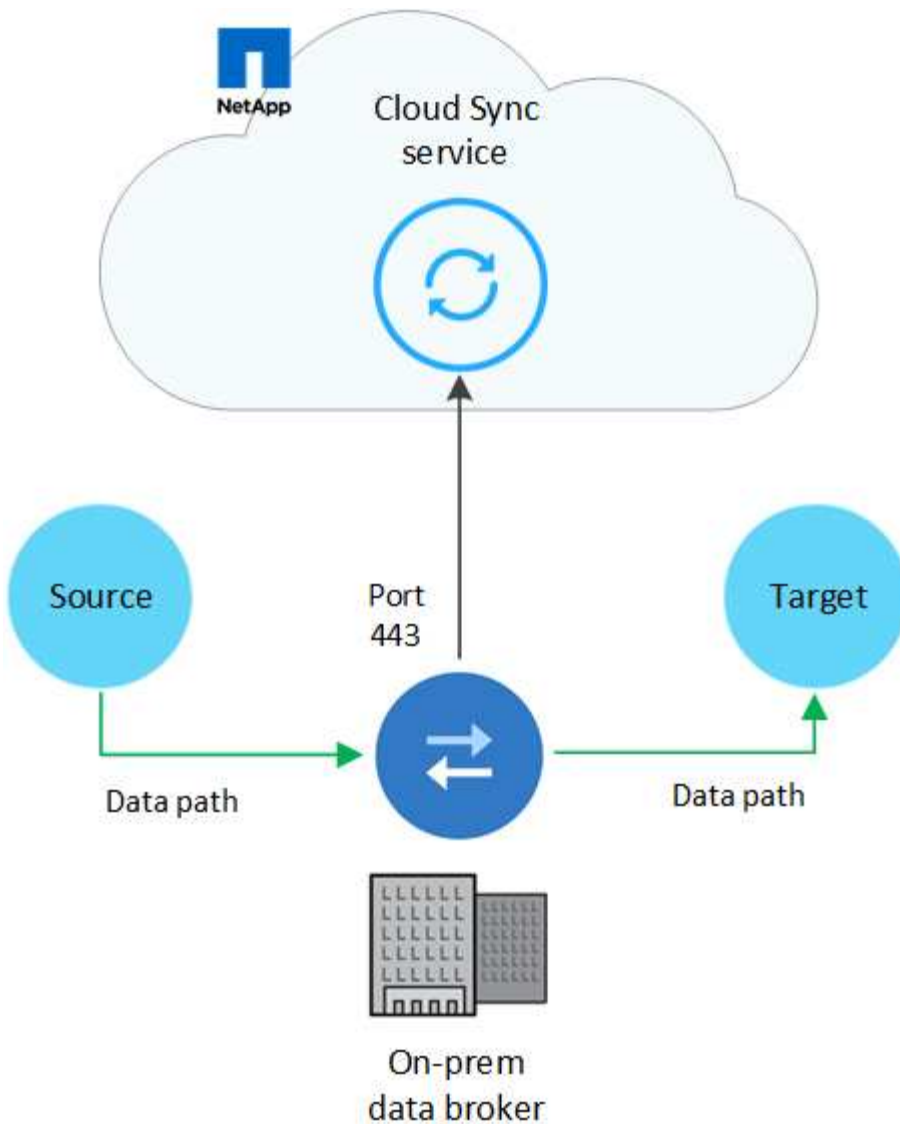


Quando Cloud Sync implementa il data broker in AWS, Azure o GCP, crea un gruppo di sicurezza che abilita la comunicazione in uscita richiesta.



#### 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 data broker.

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

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

## Endpoint di rete

Il data broker NetApp richiede l'accesso a Internet in uscita tramite la porta 443 per comunicare con il servizio Cloud Sync 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

Il data broker contatta i seguenti endpoint:

Endpoint	Scopo
olcentgbl.trafficmanager.net:443	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.
rpm.nodesource.com:443 registry.npmjs.org:443 nodejs.org:443	Per contattare i repository per l'aggiornamento di Node.js, npm e altri pacchetti di terze parti utilizzati nello sviluppo.
tgz.pm2.io:443	Per accedere a un repository per l'aggiornamento di PM2, un pacchetto di terze parti utilizzato per monitorare Cloud Sync.
sqs.us-east-1.amazonaws.com:443 kinesis.us-east-1.amazonaws.com:443	Per contattare i servizi AWS utilizzati da Cloud Sync per le operazioni (accodamento di file, registrazione di azioni e invio di aggiornamenti al data broker).
s3.region.amazonaws.com:443 ad esempio: s3.us-east-2.amazonaws.com:443 <a href="https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region">https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region</a> ["Per un elenco degli endpoint S3, consultare la documentazione di AWS"]	Per contattare Amazon S3 quando una relazione di sincronizzazione include un bucket S3.
cf.cloudsync.netapp.com:443 repo.cloudsync.netapp.com:443	Per contattare il servizio Cloud Sync.
support.netapp.com:443	Per contattare il supporto NetApp quando si utilizza una licenza BYOL per le relazioni di sincronizzazione.
fedoraproject.org:443	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 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

## Come installare un data broker

### Installazione del data broker in AWS

Quando si crea una relazione di sincronizzazione, scegliere l'opzione AWS Data Broker per implementare il software del data broker su una nuova istanza EC2 in un VPC. Cloud Sync guida l'utente attraverso il processo di installazione, ma i requisiti e i passaggi vengono ripetuti in questa pagina per facilitare la preparazione 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 di quelle della Cina e di GovCloud (USA).

## Requisiti di rete

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

Quando Cloud 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 Cloud Sync 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.

## Installazione del data broker


È possibile installare un data broker in AWS quando si crea una relazione di sincronizzazione.

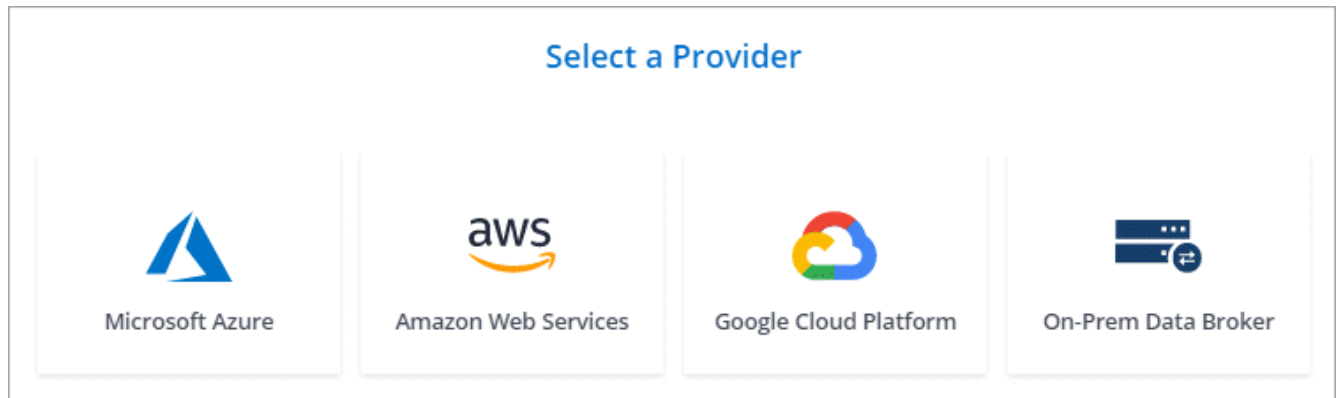
## Fasi

1. Fare clic su **Create New Sync** (Crea nuova sincronizzazione).
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione e fare clic su **continua**.

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

3. Nella pagina **Data Broker**, fare clic su **Create Data Broker**, quindi selezionare **Amazon Web Services**.

Se disponi già di un data broker, dovrai fare clic su  prima icona.



4. Immettere un nome per il broker di dati e fare clic su **continua**.
5. Immettere una chiave di accesso AWS in modo che Cloud Sync possa creare il data broker in AWS per conto dell'utente.

Le chiavi non vengono salvate o utilizzate per altri scopi.

Se invece non si desidera fornire le chiavi di accesso, fare clic sul 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/occm38//media/video\\_cloud\\_sync.mp4](https://docs.netapp.com/it-it/occm38//media/video_cloud_sync.mp4) (video)

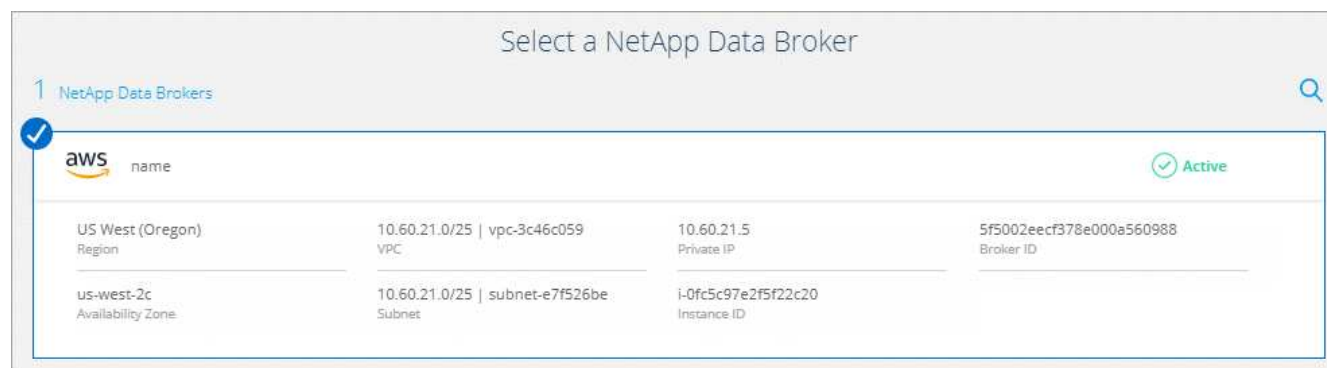
6. Se è stata immessa una chiave di accesso AWS, selezionare una posizione per l'istanza, selezionare una coppia di chiavi, scegliere se attivare un indirizzo IP pubblico, quindi selezionare un ruolo IAM esistente oppure lasciare vuoto il campo in modo che Cloud Sync crei il ruolo.

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

The image shows a 'Basic Settings' form with two columns. The left column has 'Location' with fields for 'Region' (US West | Oregon), 'VPC' (vpc-3c46c059 - 10.60.21.0/25), and 'Subnet' (10.60.21.0/25). The right column has 'Connectivity' with a 'Key Pair' field (newKey), an 'Enable Public IP?' section with 'Enable' selected, and an 'IAM Role (optional)' field with an information icon.

7. Una volta che il data broker è disponibile, fare clic su **Continue** (continua) in Cloud Sync.

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



8. 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. Puoi utilizzare questo data broker con ulteriori relazioni di sincronizzazione.

### Installazione del data broker in Azure

Quando si crea una relazione di sincronizzazione, scegliere l'opzione Azure Data Broker per implementare il software del data broker su una nuova macchina virtuale in una VNET. Cloud Sync guida l'utente attraverso il processo di installazione, ma i requisiti e i passaggi vengono ripetuti in questa pagina per facilitare la preparazione 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.

### Requisiti di rete

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

Quando Cloud 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.

### Metodo di autenticazione

Quando si implementa il data broker, è necessario scegliere un metodo di autenticazione: 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"](#).



## Installazione del data broker

È possibile installare un data broker in Azure quando si crea una relazione di sincronizzazione.

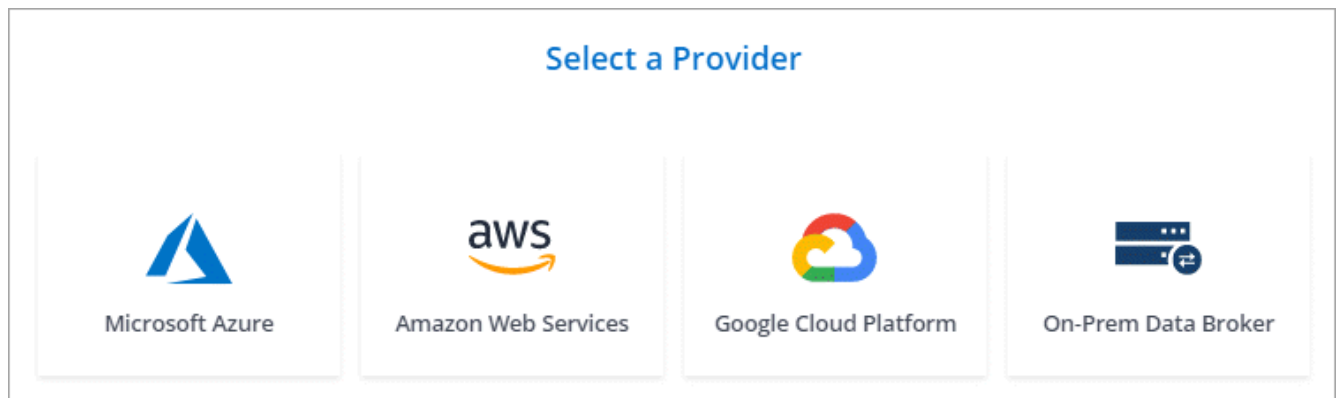
### Fasi

1. Fare clic su **Create New Sync** (Crea nuova sincronizzazione).
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione e fare clic su **continua**.

Completa le pagine fino a raggiungere la pagina **Data Broker**.

3. Nella pagina **Data Broker**, fare clic su **Create Data Broker**, quindi selezionare **Microsoft Azure**.

Se disponi già di un data broker, dovrai fare clic su  prima icona.



4. Immettere un nome per il broker di dati e fare clic su **continua**.
5. Se richiesto, accedere all'account Microsoft. Se non viene richiesto, fare clic su **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.

<u>Location</u>	<u>Virtual Machine</u>
Subscription OCCM Dev ▼	VM Name netappdatabroker ⓘ
Azure Region West US 2 ▼	User Name databroker ⓘ
VNet Vnet1 ▼	Authentication Method: <input checked="" type="radio"/> Password <input type="radio"/> Public Key
Subnet Subnet1 ▼	Enter Password ⓘ .....
	Resource Group: <input checked="" type="radio"/> Generate a new group <input type="radio"/> Use an existing group

7. Fare clic su **Continue** (continua) e mantenere aperta la pagina fino al completamento dell'implementazione.

Il processo può richiedere fino a 7 minuti.

8. In Cloud Sync, fare clic su **Continue** una volta che il data broker è disponibile.
9. 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 Cloud Sync ha bisogno dell'autorizzazione per accedere alle risorse dell'organizzazione per conto dell'utente, sono disponibili due opzioni:

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

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

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

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

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

### Installazione del data broker in Google Cloud Platform

Quando si crea una relazione di sincronizzazione, scegliere l'opzione GCP Data Broker per implementare il software del data broker su una nuova istanza di macchina virtuale in un VPC. Cloud Sync guida l'utente attraverso il processo di installazione, ma i requisiti e i passaggi vengono ripetuti in questa pagina per facilitare la preparazione all'installazione.

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

#### Regioni GCP supportate

Sono supportate tutte le regioni.

#### Requisiti di rete

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

Quando Cloud Sync implementa il data broker in GCP, 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 GCP

Assicurarsi che l'utente GCP 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.*`

## Installazione del data broker

È possibile installare un data broker in GCP quando si crea una relazione di sincronizzazione.

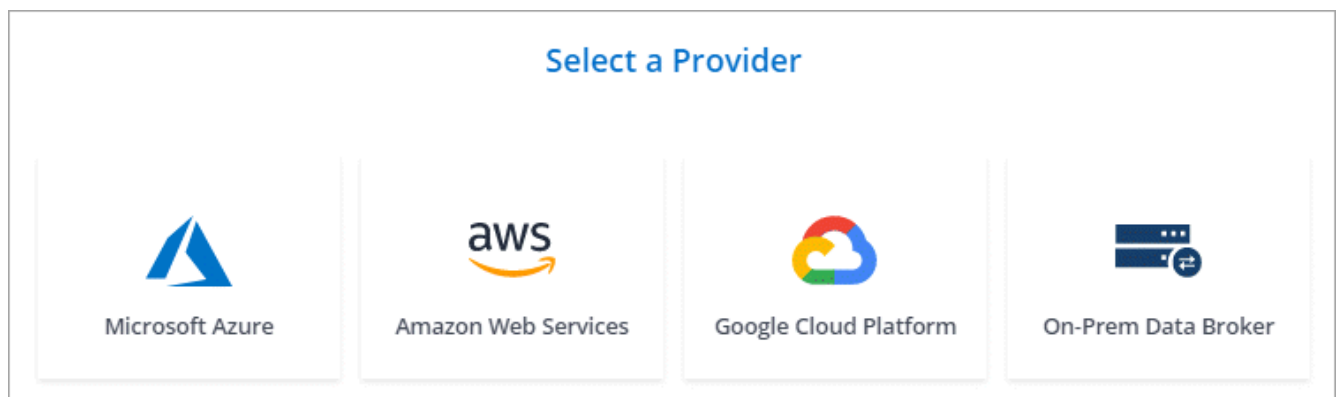
### Fasi

1. Fare clic su **Create New Sync** (Crea nuova sincronizzazione).
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione e fare clic su **continua**.

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

3. Nella pagina **Data Broker**, fare clic su **Create Data Broker**, quindi selezionare **Google Cloud Platform**.

Se disponi già di un data broker, dovrai fare clic su  prima icona.



4. Immettere un nome per il broker di dati e fare clic su **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.

### Basic Settings

<b>Project</b>	<b>Location</b>
Project <input type="text" value="OCCM-Dev"/>	Region <input type="text" value="us-west1"/>
Service Account <input type="text" value="test"/>	Zone <input type="text" value="us-west1-a"/>
Select a Service Account that includes <a href="#">these permissions</a>	VPC <input type="text" value="default"/>
	Subnet <input type="text" value="default"/>

7. Una volta che il data broker è disponibile, fare clic su **Continue** (continua) in Cloud Sync.

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

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

### Risultato

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

### Installazione del data broker su un host Linux

Quando crei una relazione di sincronizzazione, scegli l'opzione on-Prem Data Broker per installare il software data broker su un host Linux on-premise o su un host Linux esistente nel cloud. Cloud Sync guida l'utente attraverso il processo di installazione, ma i requisiti e i passaggi vengono ripetuti in questa pagina per facilitare la preparazione all'installazione.

#### Requisiti degli host Linux

- **Sistema operativo:**

- CentOS 7.0, 7.7 e 8.0
- Red Hat Enterprise Linux 7.7 e 8.0
- Ubuntu Server 18.04 LTS
- SUSE Linux Enterprise Server 15 SP1

Il comando `yum update all` 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.

- **OpenSSL:** OpenSSL deve essere installato sull'host Linux.

#### 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.

#### Abilitazione dell'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.

#### Abilitazione dell'accesso a Google Cloud

Se si prevede di utilizzare il data broker con una relazione di sincronizzazione che include un bucket di storage Google Cloud, è necessario preparare l'host Linux per l'accesso GCP. 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 GCP con autorizzazioni Storage Admin, se non ne hai già uno.
2. Creare una chiave dell'account di servizio salvata in formato JSON. "[Visualizzare le istruzioni GCP](#)".

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.

### Abilitazione dell'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 data broker

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

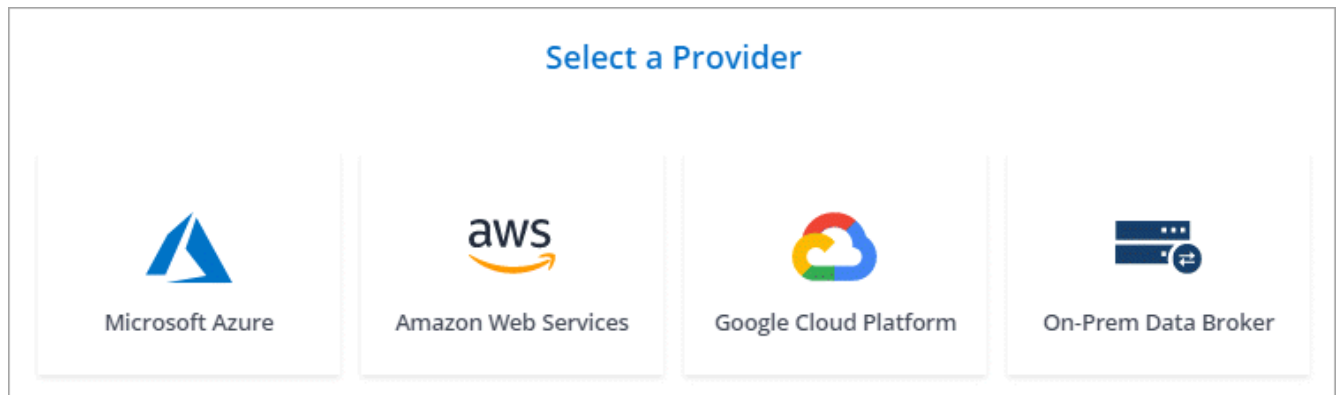
### Fasi

1. Fare clic su **Create New Sync** (Crea nuova sincronizzazione).
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione e fare clic su **continua**.

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

3. Nella pagina **Data Broker**, fare clic su **Create Data Broker**, quindi selezionare **on-Prem Data Broker**.

Se disponi già di un data broker, dovrai fare clic su  prima icona.



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 broker di dati e fare clic su **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**.
- 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

Cloud Sync visualizza l'URI del file di installazione nella pagina delle istruzioni, che viene caricato quando si seguono le istruzioni per implementare il Data Broker on-Prem. 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 da Cloud Sync, 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 GCP. 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 aver preparato [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

Si tratta del file JSON che contiene una chiave dell'account di servizio che si dovrebbe preparare [seguire questa procedura](#).

6. Una volta che il data broker è disponibile, fare clic su **Continue** (continua) in Cloud Sync.
7. Completare le pagine della procedura guidata per creare la nuova relazione di sincronizzazione.

## Creazione di una relazione di sincronizzazione

Quando si crea una relazione di sincronizzazione, il servizio Cloud Sync copia i file dall'origine alla destinazione. Dopo la copia iniziale, il servizio sincronizza tutti i dati modificati ogni 24 ore.

I passaggi riportati di seguito forniscono un esempio che mostra come impostare una relazione di sincronizzazione da un server NFS a un bucket S3.

### Fasi

1. In Cloud Manager, fare clic su **Sync**.
2. Nella pagina **Definisci relazione di sincronizzazione**, scegliere un'origine e una destinazione.

I passaggi seguenti forniscono un esempio di come creare una relazione di sincronizzazione da un server NFS a un bucket S3.



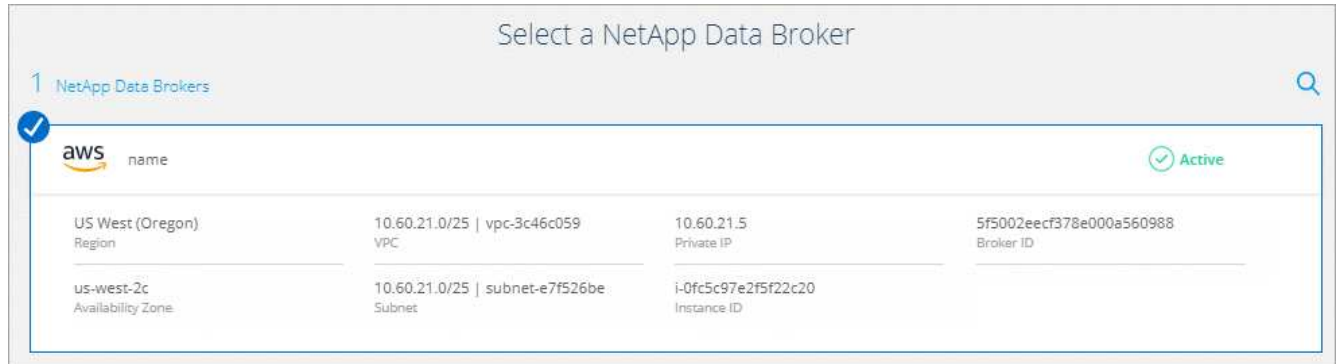
3. Nella pagina **NFS Server**, inserire l'indirizzo IP o il nome di dominio completo del server NFS che si desidera sincronizzare con AWS.
4. Nella pagina **Data Broker**, seguire le istruzioni per creare una macchina virtuale per il data broker in AWS, Azure o Google Cloud Platform, oppure per installare il software per il data broker su un host Linux esistente.

Per ulteriori informazioni, consultare le seguenti pagine:

- "Installazione del data broker in AWS"
- "Installazione del data broker in Azure"
- "Installazione del data broker in GCP"
- "Installazione del data broker su un host Linux"

5. Dopo aver installato il data broker, fare clic su **Continue** (continua).

La seguente immagine mostra un data broker implementato correttamente in AWS:



6. nella pagina **Directory**, selezionare una directory o una sottodirectory di livello superiore.

Se Cloud Sync non riesce a recuperare le esportazioni, fare clic su **Aggiungi esportazione manualmente** e immettere il nome di un'esportazione NFS.



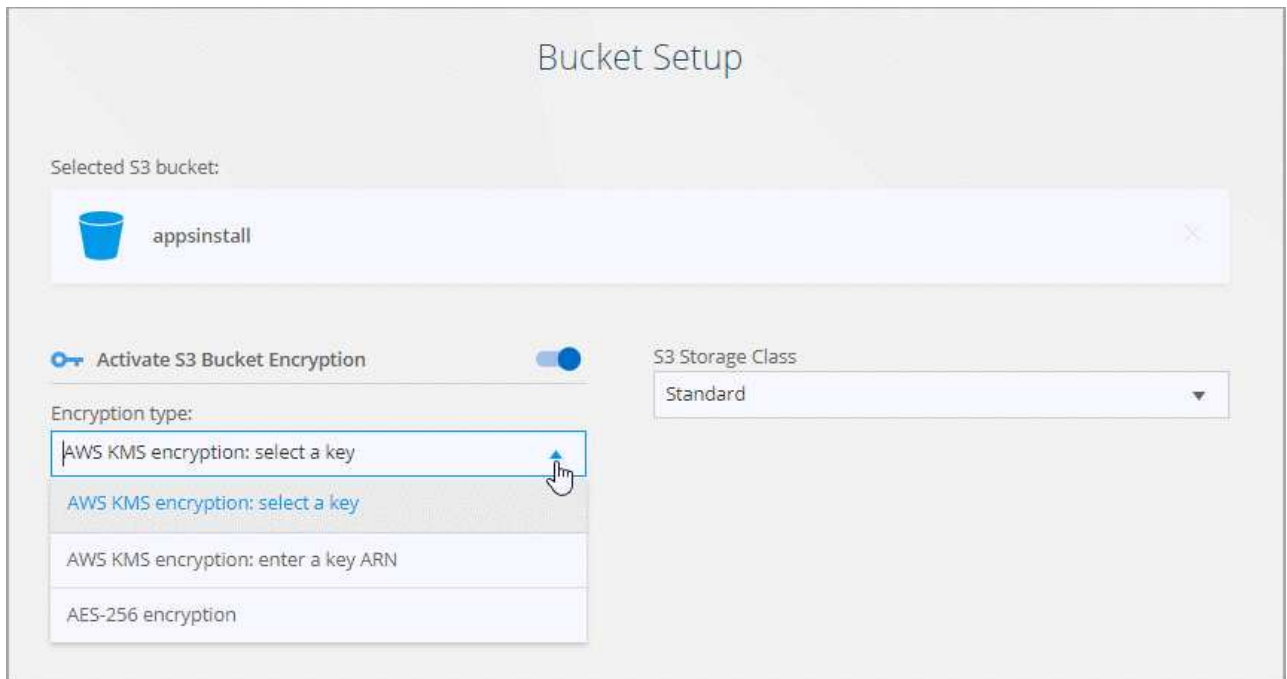
Se si desidera sincronizzare più di una directory sul server NFS, è necessario creare ulteriori relazioni di sincronizzazione al termine dell'operazione.

7. Nella pagina **bucket AWS S3**, selezionare un bucket:

- Eseguire il drill-down per selezionare una cartella esistente all'interno del bucket o per selezionare una nuova cartella creata all'interno del bucket.
- Fare clic su **Aggiungi all'elenco** per selezionare un bucket S3 non associato all'account AWS. "[Al bucket S3 devono essere applicate autorizzazioni specifiche](#)".

8. Nella pagina **Bucket Setup**, impostare il bucket:

- Scegliere se attivare la crittografia del bucket S3, quindi selezionare una chiave AWS KMS, immettere l'ARN di una chiave KMS o selezionare la crittografia AES-256.
- Selezionare una classe di storage S3. "[Visualizzare le classi di storage supportate](#)".



9. Nella pagina **Impostazioni**, definire la modalità di sincronizzazione e gestione dei file e delle cartelle di origine nella posizione di destinazione:

#### **Pianificazione**

Scegliere una pianificazione ricorrente per le sincronizzazioni future o disattivare la pianificazione della sincronizzazione. È possibile pianificare una relazione per sincronizzare i dati ogni 1 minuto.

#### **Tentativi**

Definire il numero di tentativi di sincronizzazione di un file da parte di Cloud Sync prima di ignorarlo.

#### **File modificati di recente**

Scegliere di escludere i file modificati di recente prima della sincronizzazione pianificata.

#### **Elimina file in origine**

Scegliere di eliminare i file dalla posizione di origine dopo che Cloud Sync copia i file nella posizione di destinazione. Questa opzione include il rischio di perdita dei dati perché i file di origine vengono cancellati dopo la copia.

Se si attiva questa opzione, è necessario modificare anche un parametro nel file `local.json` sul data broker. Aprire il file e modificare il parametro denominato `workers.transferrer.delete-on-source` in **true**.

#### **Eliminare i file di destinazione**

Scegliere di eliminare i file dalla posizione di destinazione, se sono stati eliminati dall'origine. Per impostazione predefinita, non elimina mai i file dalla posizione di destinazione.

#### **Tagging degli oggetti**

Quando AWS S3 è la destinazione in una relazione di sincronizzazione, Cloud Sync contrassegna gli oggetti S3 con metadati rilevanti per l'operazione di sincronizzazione. È possibile disattivare la tagging degli oggetti S3, se non si desidera, nell'ambiente in uso. La disattivazione del tagging non ha alcun impatto su Cloud Sync: Cloud Sync memorizza i metadati di sincronizzazione in un modo diverso.

## Tipi di file

Definire i tipi di file da includere in ogni sincronizzazione: File, directory e collegamenti simbolici.

## Escludi estensioni file

Specificare le estensioni dei file da escludere dalla sincronizzazione digitando l'estensione del file e premendo **Invio**. Ad esempio, digitare *log* o *.log* per escludere i file \*.log. Non è necessario un separatore per più interni. Il seguente video fornisce una breve demo:

► [https://docs.netapp.com/it-it/occm38//media/video\\_file\\_extensions.mp4](https://docs.netapp.com/it-it/occm38//media/video_file_extensions.mp4) (video)

## Dimensione del file

Scegliere di sincronizzare tutti i file indipendentemente dalle dimensioni o solo i file che si trovano in un intervallo di dimensioni specifico.

## Data di modifica

Scegliere tutti i file indipendentemente dalla data dell'ultima modifica, i file modificati dopo una data specifica, prima di una data specifica o tra un intervallo di tempo.

10. Nella pagina **Relationship Tags**, inserire fino a 9 tag di relazione, quindi fare clic su **Continue**.

Il servizio Cloud Sync assegna i tag a ciascun oggetto sincronizzato con il bucket S3.

11. Esaminare i dettagli della relazione di sincronizzazione, quindi fare clic su **Crea relazione**.

## Risultato

Cloud Sync avvia la sincronizzazione dei dati tra l'origine e la destinazione.

## Pagamento delle relazioni di sincronizzazione al termine della prova gratuita

Esistono due modi per pagare le relazioni di sincronizzazione dopo la fine della prova gratuita di 14 giorni. La prima opzione consiste nell'abbonarsi ad AWS o Azure per il pagamento a consumo o per il pagamento annuale. La seconda opzione consiste nell'acquistare le licenze direttamente da NetApp.

È possibile utilizzare le licenze di NetApp con un abbonamento AWS o Azure. Ad esempio, se si dispone di 25 relazioni di sincronizzazione, è possibile pagare le prime 20 relazioni di sincronizzazione utilizzando una licenza e quindi pagare a consumo da AWS o Azure con le restanti 5 relazioni di sincronizzazione.

["Scopri di più sul funzionamento delle licenze"](#).

### Cosa succede se non pago 8217 immediatamente dopo la fine della prova gratuita?

Non sarà possibile creare relazioni aggiuntive. Le relazioni esistenti non vengono eliminate, ma non è possibile apportare modifiche fino a quando non si sottoscrive o si inserisce una licenza.

## sottoscrizione da AWS

AWS ti consente di pagare a consumo o di pagare annualmente.

## Procedura per il pagamento a consumo

1. Fare clic su **Sync > Licensing**.

2. Selezionare **AWS**
3. Fare clic su **Iscriviti**, quindi su **continua**.
4. Iscriviti al marketplace AWS, quindi accedi nuovamente al servizio Cloud Sync per completare la registrazione.

Il seguente video mostra il processo:

► [https://docs.netapp.com/it-it/occm38//media/video\\_cloud\\_sync\\_registering.mp4](https://docs.netapp.com/it-it/occm38//media/video_cloud_sync_registering.mp4) (video)

### Passi da pagare annualmente

1. "Accedere alla pagina [AWS Marketplace](#)".
2. Fare clic su **continua per iscriversi**.
3. Selezionare le opzioni del contratto e fare clic su **Crea contratto**.

### sottoscrizione a Azure

Azure ti consente di pagare in base alle tue esigenze o di pagare ogni anno.

### Di cosa hai bisogno

Un account utente Azure che dispone delle autorizzazioni Contributor o Owner nell'abbonamento pertinente.

### Fasi

1. Fare clic su **Sync > Licensing**.
2. Selezionare **Azure**.
3. Fare clic su **Iscriviti**, quindi su **continua**.
4. Nel portale Azure, fare clic su **Create**, selezionare le opzioni e fare clic su **Subscribe**.

Seleziona **mensile** per pagare in base all'ora o **annuale** per pagare in anticipo un anno.

5. Una volta completata l'implementazione, fare clic sul nome della risorsa SaaS nella finestra a comparsa di notifica.
6. Fare clic su **Configura account** per tornare a Cloud Sync.

Il seguente video mostra il processo:

► [https://docs.netapp.com/it-it/occm38//media/video\\_cloud\\_sync\\_registering\\_azure.mp4](https://docs.netapp.com/it-it/occm38//media/video_cloud_sync_registering_azure.mp4) (video)

### Acquisto di licenze NetApp e aggiunta a Cloud Sync

Per pagare anticipatamente le relazioni di sincronizzazione, è necessario acquistare una o più licenze e aggiungerle al servizio Cloud Sync.

### Fasi

1. Acquista una licenza inviando un messaggio di posta:ng-cloudsync-contact@netapp.com?subject=Cloud%20Sync%20Service%20-%20BYOL%20License%20Purchase%20Request[come contattare NetApp].
2. In Cloud Manager, fare clic su **Sync > Licensing**.
3. Fare clic su **Add License** (Aggiungi licenza) e aggiungere la licenza.

# Tutorial

## Copia degli ACL tra le condivisioni SMB

Cloud Sync può copiare gli elenchi di controllo degli accessi (ACL) tra una condivisione SMB di origine e una condivisione SMB di destinazione. Se necessario, è possibile conservare manualmente gli ACL utilizzando robocopy.

### Scelte

- [Impostare Cloud Sync per la copia automatica degli ACL](#)
- [Copiare manualmente gli ACL](#)

## Configurazione di Cloud Sync per copiare gli ACL tra server SMB

Copiare gli ACL tra server SMB attivando un'impostazione quando si crea una relazione o dopo la creazione di una relazione.

Questa funzionalità è disponibile per le nuove relazioni di sincronizzazione create dopo la release 23 febbraio 2020. Se si desidera utilizzare questa funzione con le relazioni esistenti create prima di tale data, sarà necessario ricreare la relazione.

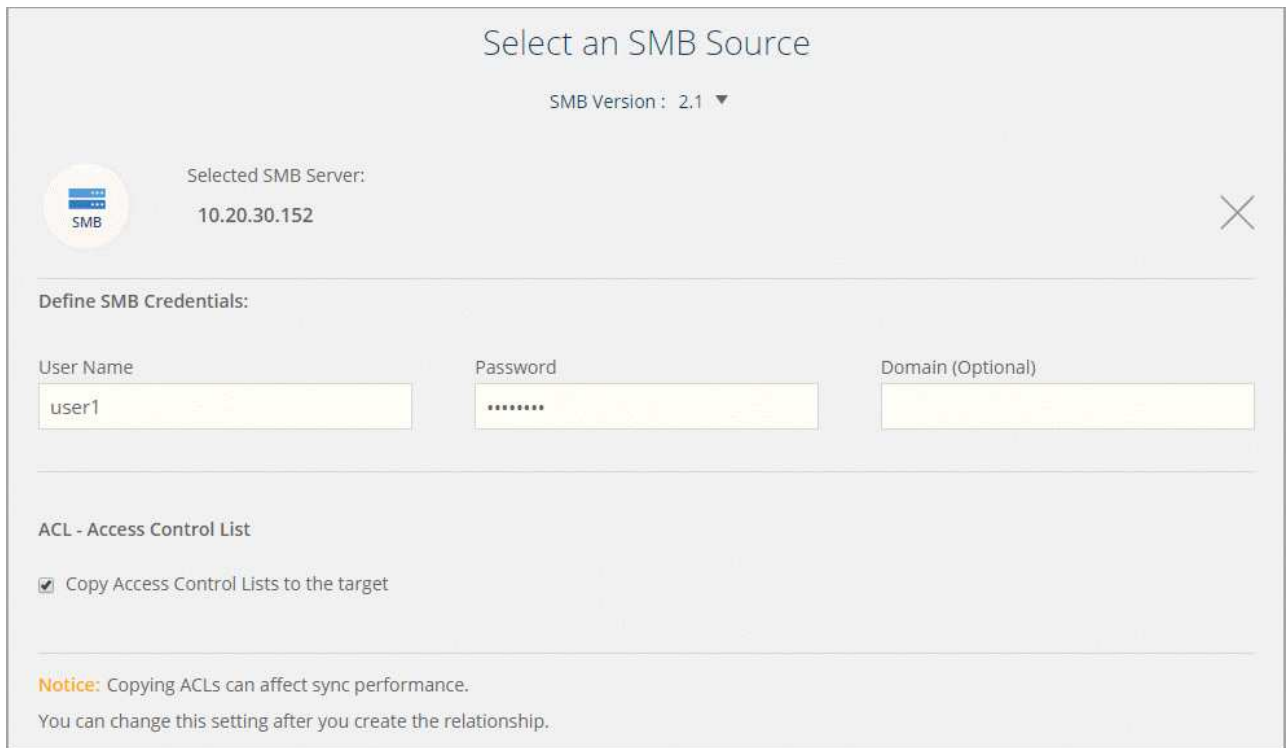
### Di cosa hai bisogno

- Una nuova relazione di sincronizzazione o una relazione di sincronizzazione esistente creata dopo la release del 23 febbraio 2020.
- Qualsiasi tipo di broker di dati.

Questa funzionalità funziona con *qualsiasi* tipo di data broker: AWS, Azure, Google Cloud Platform o data broker on-premise. Il data broker on-premise può essere eseguito "[qualsiasi sistema operativo supportato](#)".

### Passaggi per una nuova relazione

1. Da Cloud Sync, fare clic su **Crea nuova sincronizzazione**.
2. Trascinare **SMB Server** nell'origine e nella destinazione e fare clic su **Continue** (continua).
3. Nella pagina **SMB Server**:
  - a. Immettere un nuovo server SMB o selezionare un server esistente e fare clic su **continua**.
  - b. Immettere le credenziali per il server SMB.
  - c. Selezionare **Copy Access Control Lists to the target** (Copia elenchi di controllo degli accessi nella destinazione) e fare clic su **Continue** (continua).



Select an SMB Source

SMB Version: 2.1 ▼

Selected SMB Server:  
10.20.30.152

Define SMB Credentials:

User Name: user1 Password: Password Domain (Optional):

ACL - Access Control List

Copy Access Control Lists to the target

**Notice:** Copying ACLs can affect sync performance.  
You can change this setting after you create the relationship.

4. Seguire le istruzioni rimanenti per creare la relazione di sincronizzazione.

### Passaggi per una relazione esistente

1. Passare il mouse sulla relazione di sincronizzazione e fare clic sul menu delle azioni.
2. Fare clic su **Impostazioni**.
3. Selezionare **Copy Access Control Lists to the target** (Copia elenchi di controllo degli accessi nella destinazione).
4. Fare clic su **Save Settings** (Salva impostazioni).

### Risultato

Durante la sincronizzazione dei dati, Cloud Sync preserva gli ACL tra le condivisioni SMB di origine e di destinazione.

### Copia manuale degli ACL

È possibile conservare manualmente gli ACL tra le condivisioni SMB utilizzando il comando Windows robocopy.

### Fasi

1. Identificare un host Windows con accesso completo a entrambe le condivisioni SMB.
2. Se uno degli endpoint richiede l'autenticazione, utilizzare il comando **net use** per connettersi agli endpoint dall'host Windows.

Eseguire questa procedura prima di utilizzare robocopy.

3. Da Cloud Sync, creare una nuova relazione tra le condivisioni SMB di origine e di destinazione o sincronizzare una relazione esistente.
4. Una volta completata la sincronizzazione dei dati, eseguire il seguente comando dall'host Windows per sincronizzare gli ACL e la proprietà:

```
robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots  
/UNILOG:"[logfilepath]
```

È necessario specificare sia *source* che *target* utilizzando il formato UNC. Ad esempio:  
<server>/<share>/<path>

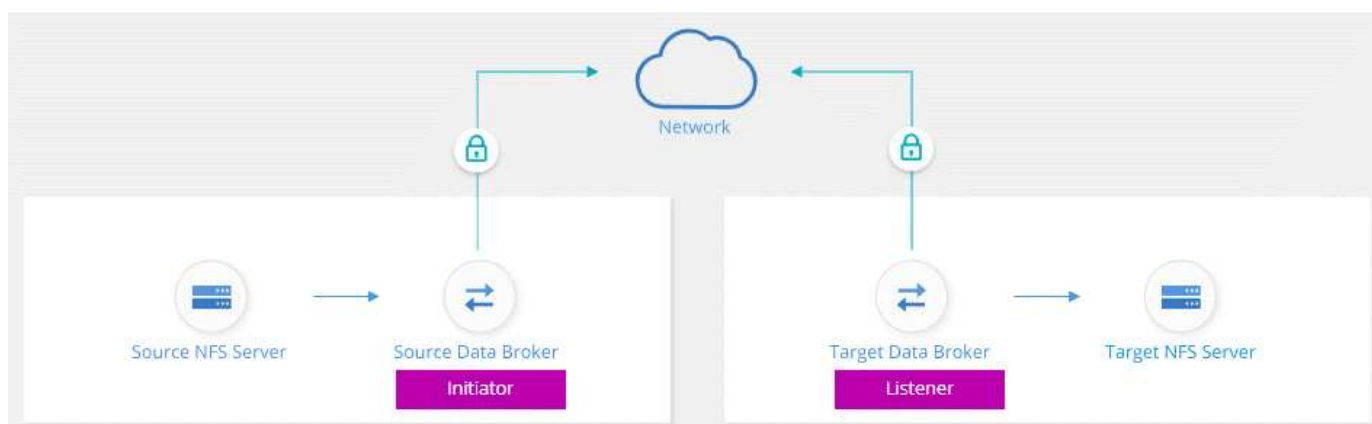
## Sincronizzazione dei dati NFS con crittografia data-in-flight

Se la tua azienda ha policy di sicurezza rigorose, puoi sincronizzare i dati NFS utilizzando la crittografia data-in-flight. Questa funzionalità è supportata da un server NFS a un altro server NFS e da Azure NetApp Files a Azure NetApp Files.

Ad esempio, è possibile sincronizzare i dati tra due server NFS che si trovano in reti diverse. In alternativa, potrebbe essere necessario trasferire in modo sicuro i dati su Azure NetApp Files tra sottoreti o regioni.

### Come funziona la crittografia dei dati in volo

La crittografia Data-in-flight crittografa i dati NFS quando vengono inviati in rete tra due broker di dati. La seguente immagine mostra una relazione tra due server NFS e due broker di dati:



Un data broker funziona come *initiator*. Quando è il momento di sincronizzare i dati, invia una richiesta di connessione all'altro data broker, che è il *listener*. Il data broker ascolta le richieste sulla porta 443. Se necessario, è possibile utilizzare un'altra porta, ma assicurarsi che la porta non sia utilizzata da un altro servizio.

Ad esempio, se si sincronizzano i dati da un server NFS on-premise a un server NFS basato sul cloud, è possibile scegliere quale broker di dati ascoltare le richieste di connessione e quale inviarle.

Ecco come funziona la crittografia in-flight:

1. Dopo aver creato la relazione di sincronizzazione, l'iniziatore avvia una connessione crittografata con l'altro data broker.
2. Il broker dei dati di origine crittografa i dati dall'origine utilizzando TLS 1.3.
3. Quindi, invia i dati in rete al data broker di destinazione.
4. Il broker di dati di destinazione decrta i dati prima di inviarli alla destinazione.
5. Dopo la copia iniziale, il servizio sincronizza tutti i dati modificati ogni 24 ore. Se sono presenti dati da sincronizzare, il processo inizia con l'iniziatore che apre una connessione crittografata con l'altro data



broker.

Se preferisci sincronizzare i dati più frequentemente, ["è possibile modificare la pianificazione dopo aver creato la relazione"](#).

## Versioni NFS supportate

- Per i server NFS, la crittografia data-in-flight è supportata con le versioni NFS 3, 4.0, 4.1 e 4.2.
- Per Azure NetApp Files, la crittografia data-in-flight è supportata con NFS versioni 3 e 4.1.

## Cosa ti serve per iniziare

Assicurarsi di disporre di quanto segue:

- Due server NFS che si incontrano ["requisiti di origine e destinazione"](#) O Azure NetApp Files in due sottoreti o regioni.
- Gli indirizzi IP o i nomi di dominio completi dei server.
- Posizioni di rete per due broker di dati.

È possibile selezionare un data broker esistente, ma deve funzionare come iniziatore. Il data broker listener deve essere un *new* data broker.

Se non hai ancora implementato un data broker, esamina i requisiti del data broker. Poiché si dispone di policy di sicurezza rigorose, assicurarsi di esaminare i requisiti di rete, che includono il traffico in uscita dalla porta 443 e da ["endpoint internet"](#) che il data broker contatta.

- ["Esaminare l'installazione di AWS"](#)
- ["Esaminare l'installazione di Azure"](#)
- ["Esaminare l'installazione di GCP"](#)
- ["Esaminare l'installazione dell'host Linux"](#)

## Sincronizzazione dei dati NFS con crittografia data-in-flight

Creare una nuova relazione di sincronizzazione tra due server NFS o tra Azure NetApp Files, attivare l'opzione di crittografia in-flight e seguire le istruzioni.

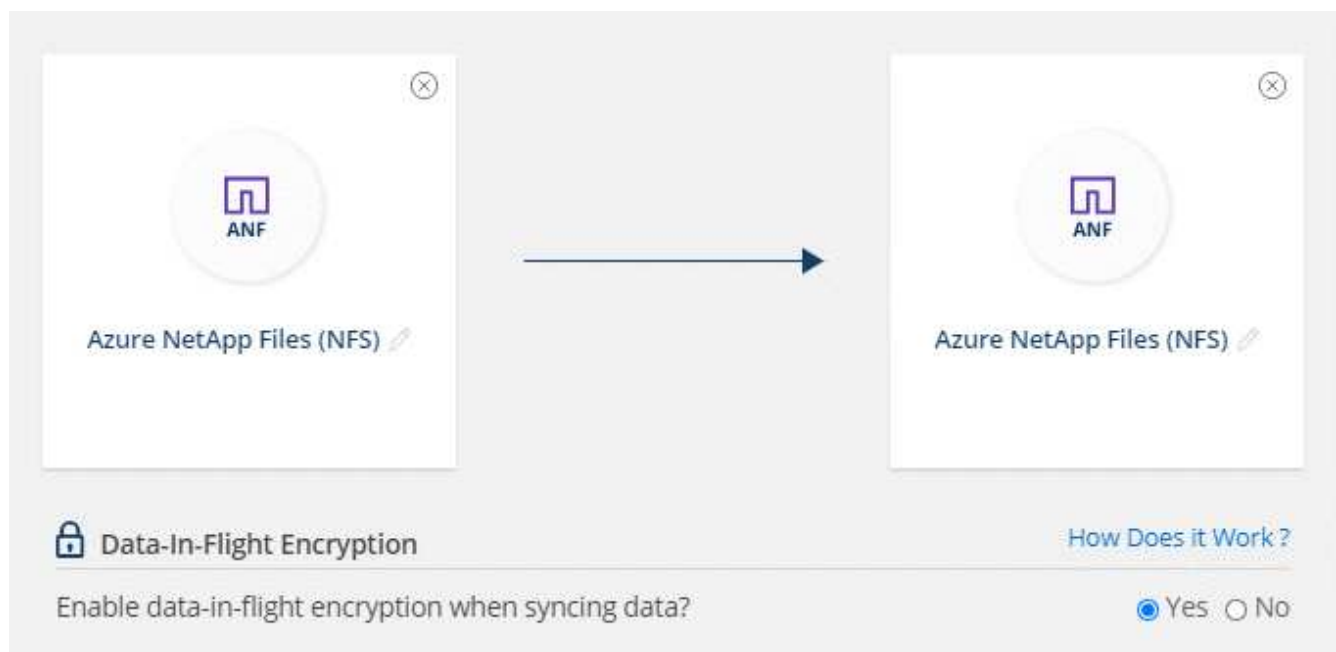
### Fasi

1. Fare clic su **Create New Sync** (Crea nuova sincronizzazione).
2. Trascinare **server NFS** nelle posizioni di origine e destinazione o **Azure NetApp Files** nelle posizioni di origine e destinazione e selezionare **Si** per attivare la crittografia dei dati in volo.

La seguente immagine mostra ciò che si desidera selezionare per sincronizzare i dati tra due server NFS:



La seguente immagine mostra ciò che si desidera selezionare per sincronizzare i dati tra Azure NetApp Files:

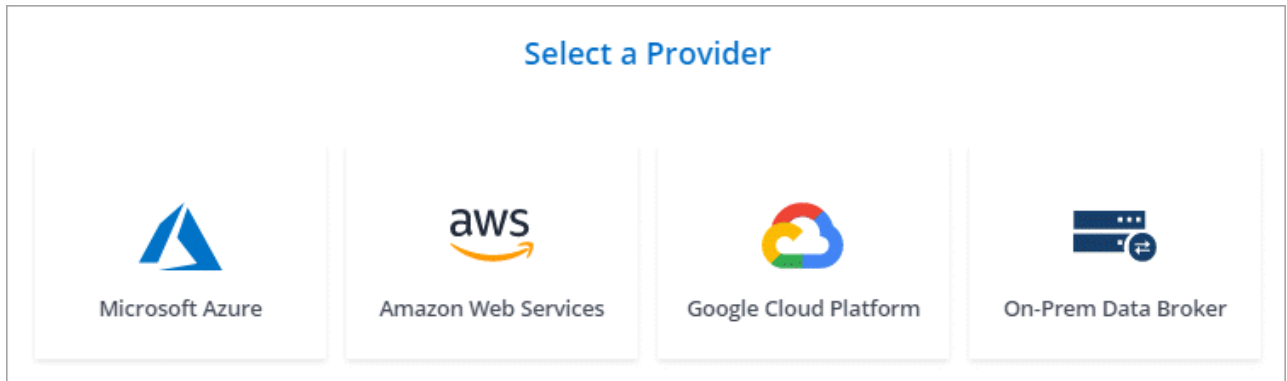


3. Seguire le istruzioni per creare la relazione:

- a. **Server NFS/Azure NetApp Files:** Scegliere la versione di NFS e specificare una nuova origine NFS oppure selezionare un server esistente.
- b. **Definisci funzionalità Data Broker:** Definire quale broker di dati *ascolta* per le richieste di connessione su una porta e quale *avvia* la connessione. Scegli la tua scelta in base ai tuoi requisiti di rete.
- c. **Data Broker:** Seguire le istruzioni per aggiungere un nuovo data broker di origine o selezionare un data broker esistente.

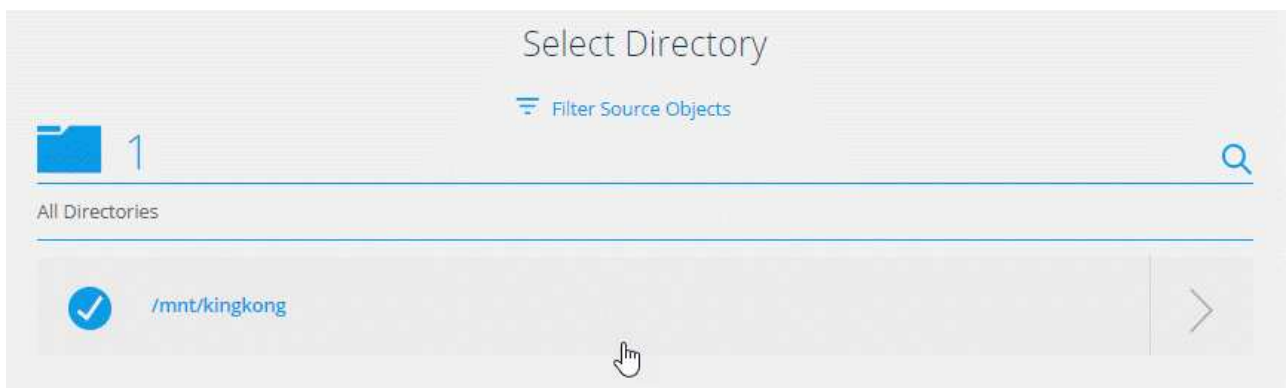
Se il broker di dati di origine agisce come listener, deve essere un nuovo broker di dati.

Se è necessario un nuovo data broker, Cloud Sync richiede le istruzioni per l'installazione. Puoi implementare il data broker nel cloud o scaricare uno script di installazione per il tuo host Linux.



- d. **Directory:** Scegliere le directory che si desidera sincronizzare selezionando tutte le directory oppure eseguendo il drill-down e selezionando una sottodirectory.

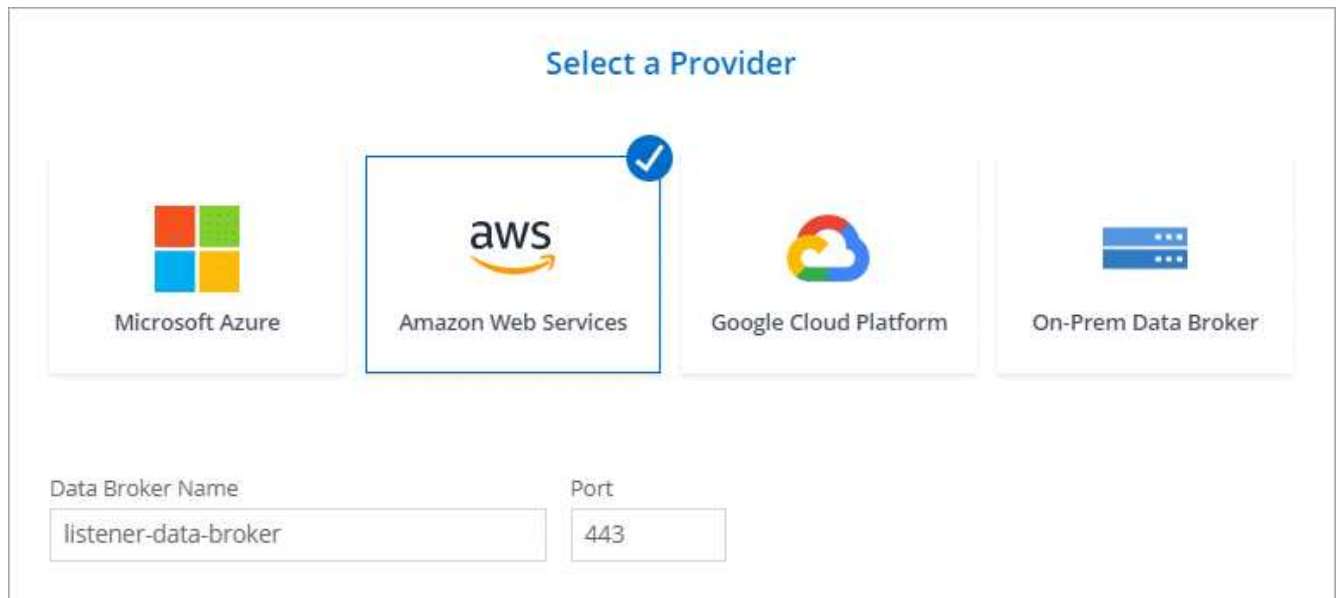
Fare clic su **Filter Source Objects** (Filtra oggetti origine) per modificare le impostazioni che definiscono la modalità di sincronizzazione e gestione dei file e delle cartelle di origine nella posizione di destinazione.



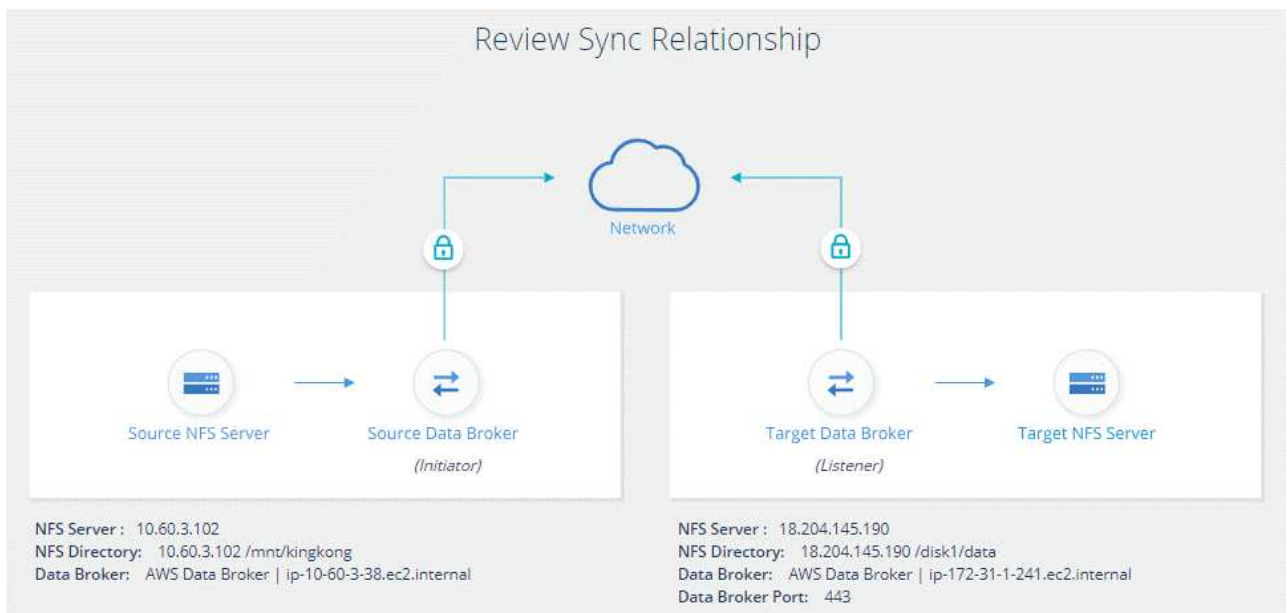
- e. **Server NFS di destinazione/Azure NetApp Files di destinazione:** Scegliere la versione di NFS, quindi inserire una nuova destinazione NFS o selezionare un server esistente.
- f. **Target Data Broker:** Seguire le istruzioni per aggiungere un nuovo broker di dati di origine o selezionare un broker di dati esistente.

Se il data broker di destinazione agisce come listener, deve essere un nuovo data broker.

Ecco un esempio del prompt quando il broker di dati di destinazione funziona come listener. Notare l'opzione per specificare la porta.



- Directory di destinazione:** Selezionare una directory di primo livello oppure eseguire il drill-down per selezionare una sottodirectory esistente o per creare una nuova cartella all'interno di un'esportazione.
- Impostazioni:** Consente di definire la modalità di sincronizzazione e gestione dei file e delle cartelle di origine nella posizione di destinazione.
- Revisione:** Esaminare i dettagli della relazione di sincronizzazione, quindi fare clic su **Crea relazione**.



## Risultato

Cloud Sync inizia a creare la nuova relazione di sincronizzazione. Al termine, fare clic su **View in Dashboard** (Visualizza in Dashboard) per visualizzare i dettagli sulla nuova relazione.

## Gestione delle relazioni di sincronizzazione

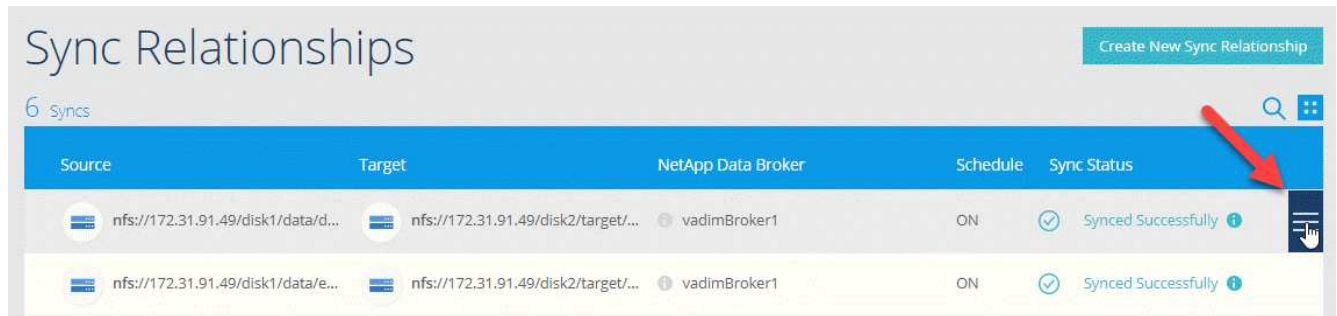
Puoi gestire le relazioni di sincronizzazione in qualsiasi momento sincronizzando immediatamente i dati, modificando le pianificazioni e molto altro ancora.

## Esecuzione di una sincronizzazione dei dati immediata

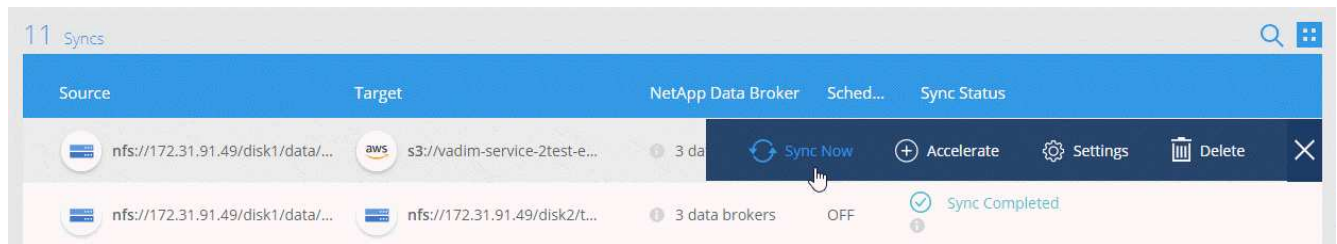
Invece di attendere la successiva sincronizzazione pianificata, è possibile premere un pulsante per sincronizzare immediatamente i dati tra l'origine e la destinazione.

### Fasi

1. Dalla dashboard di sincronizzazione, passare il mouse sulla relazione di sincronizzazione e fare clic sul menu delle azioni.



2. Fare clic su **Sincronizza ora**, quindi su **Sincronizza** per confermare.



### Risultato

Cloud Sync avvia il processo di sincronizzazione dei dati per la relazione.

## Accelerazione delle performance di sincronizzazione

Accelera le performance di una relazione di sincronizzazione aggiungendo un broker di dati aggiuntivo alla relazione. Il data broker aggiuntivo deve essere un *new* data broker.

### Come funziona

Se i data broker esistenti nella relazione vengono utilizzati in altre relazioni di sincronizzazione, Cloud Sync aggiunge automaticamente anche il nuovo data broker a tali relazioni.

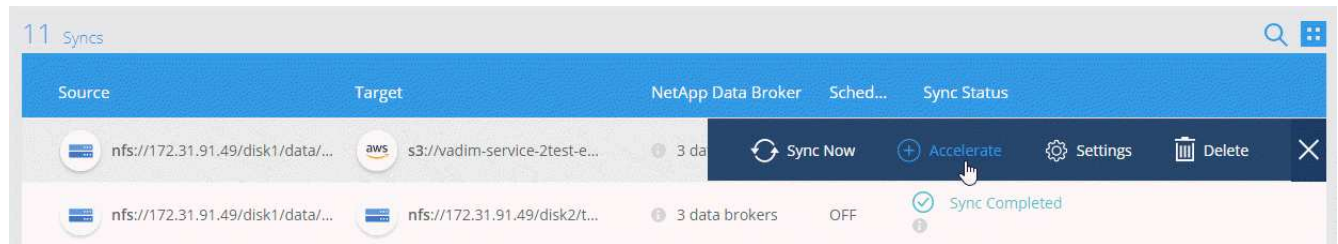
Ad esempio, supponiamo di avere tre relazioni:

- La relazione 1 utilizza il broker di dati A.
- La relazione 2 utilizza il data broker B.
- La relazione 3 utilizza il data broker A.

Si desidera accelerare le performance della relazione 1 in modo da aggiungere un nuovo data broker a tale relazione (data broker C). Poiché il broker di dati A viene utilizzato anche nella relazione 3, anche il nuovo broker di dati viene aggiunto automaticamente alla relazione 3.

### Fasi

1. Assicurarsi che almeno uno dei broker di dati esistenti nella relazione sia online.
2. Passare il mouse sulla relazione di sincronizzazione e fare clic sul menu delle azioni.
3. Fare clic su **Accelerate** (accelera).



4. Seguire le istruzioni per creare un nuovo data broker.

### Risultato

Cloud Sync aggiunge il nuovo data broker alle relazioni di sincronizzazione. Le performance della successiva sincronizzazione dei dati dovrebbero essere accelerate.

### Modifica delle impostazioni per una relazione di sincronizzazione

Modificare le impostazioni che definiscono la modalità di sincronizzazione e gestione dei file e delle cartelle di origine nella posizione di destinazione.

1. Passare il mouse sulla relazione di sincronizzazione e fare clic sul menu delle azioni.
2. Fare clic su **Impostazioni**.
3. Modificare le impostazioni.

**General**

Schedule	ON   Every 1 Day	▼
Retries	Retry 3 times before skipping file	▼

**Files and Directories**

Recently Modified Files	Exclude files that are modified up to 30 Seconds before a scheduled sync	▼
Delete Files On Source	Never delete files from the source location	▼
Delete Files On Target	Never delete files from the target location	▼
Object Tagging	Allow Cloud Sync to tag S3 objects	▼
File Types	Include All: Files, Directories, Symbolic Links	▼
Exclude File Extensions	None	▼
File Size	All	▼
Date Modified	All	▼

[Reset to defaults](#)

Ecco una breve descrizione di ciascuna impostazione:

### Pianificazione

Scegliere una pianificazione ricorrente per le sincronizzazioni future o disattivare la pianificazione della sincronizzazione. È possibile pianificare una relazione per sincronizzare i dati ogni 1 minuto.

### Tentativi

Definire il numero di tentativi di sincronizzazione di un file da parte di Cloud Sync prima di ignorarlo.

### File modificati di recente

Scegliere di escludere i file modificati di recente prima della sincronizzazione pianificata.

### Elimina file in origine

Scegliere di eliminare i file dalla posizione di origine dopo che Cloud Sync copia i file nella posizione di destinazione. Questa opzione include il rischio di perdita dei dati perché i file di origine vengono cancellati dopo la copia.

Se si attiva questa opzione, è necessario modificare anche un parametro nel file `local.json` sul data broker. Aprire il file e modificare il parametro denominato `workers.transferrer.delete-on-source` in **true**.

## Eliminare i file di destinazione

Scegliere di eliminare i file dalla posizione di destinazione, se sono stati eliminati dall'origine. Per impostazione predefinita, non elimina mai i file dalla posizione di destinazione.

## Tagging degli oggetti

Quando AWS S3 è la destinazione in una relazione di sincronizzazione, Cloud Sync contrassegna gli oggetti S3 con metadati rilevanti per l'operazione di sincronizzazione. È possibile disattivare la tagging degli oggetti S3, se non si desidera, nell'ambiente in uso. La disattivazione del tagging non ha alcun impatto su Cloud Sync: Cloud Sync memorizza i metadati di sincronizzazione in un modo diverso.

## Tipi di file

Definire i tipi di file da includere in ogni sincronizzazione: File, directory e collegamenti simbolici.

## Escludi estensioni file

Specificare le estensioni dei file da escludere dalla sincronizzazione digitando l'estensione del file e premendo **Invio**. Ad esempio, digitare *log* o *.log* per escludere i file \*.log. Non è necessario un separatore per più interni. Il seguente video fornisce una breve demo:

► [https://docs.netapp.com/it-it/occm38//media/video\\_file\\_extensions.mp4](https://docs.netapp.com/it-it/occm38//media/video_file_extensions.mp4) (video)

## Dimensione del file

Scegliere di sincronizzare tutti i file indipendentemente dalle dimensioni o solo i file che si trovano in un intervallo di dimensioni specifico.

## Data di modifica

Scegliere tutti i file indipendentemente dalla data dell'ultima modifica, i file modificati dopo una data specifica, prima di una data specifica o tra un intervallo di tempo.

## Copia gli elenchi di controllo degli accessi nella destinazione

Scegliere di copiare gli elenchi di controllo degli accessi (ACL) tra le condivisioni SMB di origine e le condivisioni SMB di destinazione. Si noti che questa opzione è disponibile solo per le relazioni di sincronizzazione create dopo la release del 23 febbraio 2020.

4. Fare clic su **Save Settings** (Salva impostazioni).

## Risultato

Cloud Sync modifica la relazione di sincronizzazione con le nuove impostazioni.

## Eliminazione delle relazioni

È possibile eliminare una relazione di sincronizzazione, se non è più necessario sincronizzare i dati tra l'origine e la destinazione. Questa azione non elimina l'istanza del broker di dati e non elimina i dati dalla destinazione.

## Fasi

1. Passare il mouse sulla relazione di sincronizzazione e fare clic sul menu delle azioni.
2. Fare clic su **Delete** (Elimina), quindi fare nuovamente clic su **Delete** (Elimina) per confermare.

## Risultato

Cloud Sync elimina la relazione di sincronizzazione.



# API Cloud Sync

Le funzionalità di Cloud Sync disponibili tramite l'interfaccia utente Web sono disponibili anche tramite le API RESTful.

## Per iniziare

Per iniziare a utilizzare le API di Cloud Sync, è necessario ottenere un token utente e l'ID account di Cloud Central. Quando si effettua una chiamata API, è necessario aggiungere il token e l'ID dell'account all'intestazione Authorization (autorizzazione).

### Fasi

1. Ottieni un token utente da NetApp Cloud Central.

```
POST https://netapp-cloud-account.auth0.com/oauth/token
Header: Content-Type: application/json
Body:
{
  "username": "<user_email>",
  "scope": "profile",
  "audience": "https://api.cloud.netapp.com",
  "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",
  "grant_type": "password",
  "password": "<user_password>"
}
```

2. Ottieni il tuo ID account Cloud Central.

```
GET https://cloudsync.netapp.com/api/accounts
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
```

Questa API restituirà una risposta come la seguente:

```
[
  {
    "accountId": "account-JeL97Ry3",
    "name": "Test"
  }
]
```

3. Aggiungere il token utente e l'ID account nell'intestazione Authorization di ogni chiamata API.

### Esempio

Nell'esempio seguente viene illustrata una chiamata API per creare un data broker in Microsoft Azure. È sufficiente sostituire <user\_token> e <accountId> con il token e l'ID ottenuti nei passaggi precedenti.

```
POST https://cloudsync.netapp.com/api/data-brokers
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
Body: { "name": "databroker1", "type": "AZURE" }
```

## Cosa devo fare quando il token scade?

Il token utente di NetApp Cloud Central ha una data di scadenza. Per aggiornare il token, è necessario richiamare nuovamente l'API dal passaggio 1.

La risposta API include un campo "expires\_in" che indica la scadenza del token.

## Riferimento API

La documentazione per ogni API Cloud Sync è disponibile all'indirizzo "[NetApp Cloud Central](#)".

## Utilizzo delle API di elenco

Le API di elenco sono API asincrone, pertanto il risultato non viene restituito immediatamente (ad esempio: GET /data-brokers/{id}/list-nfs-export-folders e GET /data-brokers/{id}/list-s3-buckets). L'unica risposta dal server è lo stato HTTP 202. Per ottenere il risultato effettivo, è necessario utilizzare GET /messages/client API.

### Fasi

1. Chiamare l'API dell'elenco che si desidera utilizzare.
2. Utilizzare GET /messages/client API per visualizzare il risultato dell'operazione.
3. Utilizzare la stessa API aggiungendo l'ID appena ricevuto: GET  
`http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>`

Tenere presente che l'ID cambia ogni volta che si chiama GET /messages/client API.

### Esempio

Quando si chiama list-s3-buckets API, un risultato non viene restituito immediatamente:

```
GET http://cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Il risultato è il codice di stato HTTP 202, che significa che il messaggio è stato accettato, ma non è stato ancora elaborato.

Per ottenere il risultato dell'operazione, è necessario utilizzare la seguente API:

```
GET http://cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Il risultato è una matrice con un oggetto che include un campo ID. Il campo ID rappresenta l'ultimo messaggio inviato dal server. Ad esempio:

```
[
  {
    "header": {
      "requestId": "init",
      "clientId": "init",
      "agentId": "init"
    },
    "payload": {
      "init": {}
    },
    "id": "5801"
  }
]
```

A questo punto, effettuare la seguente chiamata API utilizzando l'ID appena ricevuto:

```
GET http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Il risultato è una serie di messaggi. All'interno di ogni messaggio è presente un oggetto payload, che consiste nel nome dell'operazione (come chiave) e nel relativo risultato (come valore). Ad esempio:

```
[
  {
    "payload": {
      "list-s3-buckets": [
        {
          "tags": [
            {
              "Value": "100$",
              "Key": "price"
            }
          ],
          "region": {
            "displayName": "US West (Oregon)",
            "name": "us-west-2"
          },
          "name": "small"
        }
      ]
    },
    "header": {
      "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",
      "clientId": "5beb032f548e6e35f4ed1ba9",
      "agentId": "5bed61f4489fb04e34a9aac6"
    },
    "id": "5802"
  }
]
```

## Domande tecniche frequenti su Cloud Sync

Queste FAQ possono essere utili se stai cercando una risposta rapida a una domanda.

### Per iniziare

Le seguenti domande si riferiscono alla guida introduttiva di Cloud Sync.

#### Come funziona Cloud Sync?

Cloud Sync utilizza il software per il broker dei dati NetApp per sincronizzare i dati da un'origine a una destinazione (questa è denominata *relazione di sincronizzazione*).

Il data broker controlla le relazioni di sincronizzazione tra le origini e le destinazioni. Dopo aver impostato una relazione di sincronizzazione, Cloud Sync analizza il sistema di origine e lo suddivide in più flussi di replica per eseguire il push sui dati di destinazione selezionati.

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

## Come funziona la prova gratuita di 14 giorni?

La prova gratuita di 14 giorni inizia quando ti iscrivi al servizio Cloud Sync. Non sei soggetto ai costi di NetApp per le relazioni Cloud Sync che crei per 14 giorni. Tuttavia, tutti i costi relativi alle risorse per qualsiasi broker di dati implementato sono ancora validi.

## Quanto costa Cloud Sync?

L'utilizzo di Cloud Sync comporta due tipi di costi: Costi di servizio e costi delle risorse.

### Costi di servizio

Per i prezzi pay-as-you-go, i costi del servizio Cloud Sync sono orari, in base al numero di relazioni di sincronizzazione create.

- ["Visualizza i prezzi pay-as-you-go in AWS"](#)
- ["Visualizza i prezzi annuali in AWS"](#)
- ["Visualizza i prezzi in Azure"](#)

Le licenze Cloud Sync sono disponibili anche presso il vostro rappresentante NetApp. Ogni licenza consente 20 relazioni di sincronizzazione per 12 mesi.

["Scopri di più sulle licenze"](#).

### Costi delle risorse

I costi delle risorse sono correlati ai costi di calcolo e storage per l'esecuzione del data broker nel cloud.

## Come viene fatturato Cloud Sync?

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

## Posso utilizzare Cloud Sync al di fuori del cloud?

Sì, puoi utilizzare Cloud Sync in un'architettura non cloud. L'origine e la destinazione possono risiedere on-premise e così anche il broker di dati.

Nota i seguenti punti chiave sull'utilizzo di Cloud Sync al di fuori del cloud:

- Per la sincronizzazione on-premise, NetApp StorageGRID mette a disposizione un bucket Amazon S3 privato.
- Il data broker ha bisogno di una connessione a Internet per comunicare con il servizio Cloud Sync.
- Se non acquisti una licenza direttamente da NetApp, dovrai disporre di un account AWS o Azure per la fatturazione del servizio PAYGO Cloud Sync.

## Come si accede a Cloud Sync?

Cloud Sync è disponibile in Gestione cloud nella scheda **sincronizzazione**.

## Fonti e destinazioni supportate

Le seguenti domande relative all'origine e alle destinazioni supportate in una relazione di sincronizzazione.

### Quali fonti e destinazioni supporta Cloud Sync?

Cloud Sync supporta diversi tipi di relazioni di sincronizzazione. "[Visualizzare l'intero elenco](#)".

### Quali versioni di NFS e SMB sono supportate da Cloud Sync?

Cloud Sync supporta NFS versione 3 e successive e SMB versione 1 e successive.

"[Scopri di più sui requisiti di sincronizzazione](#)".

### Quando Amazon S3 è la destinazione, è possibile eseguire il tiering dei dati in base a una classe di storage S3 specifica?

Sì, è possibile scegliere una classe di storage S3 specifica quando AWS S3 è la destinazione:

- Standard (classe predefinita)
- Tiering intelligente
- Standard-infrequent Access (accesso standard-non frequente)
- Accesso non frequente a una sola zona
- Ghiacciaio
- Glacier Deep Archive

### E i Tier di storage per lo storage Azure Blob?

È possibile scegliere un livello di storage Azure Blob specifico quando un container Blob è la destinazione:

- Storage a caldo
- Storage fresco

## Networking

Le seguenti domande si riferiscono ai requisiti di rete per Cloud Sync.

### Quali sono i requisiti di rete per Cloud Sync?

L'ambiente Cloud Sync richiede che il data broker sia connesso all'origine e alla destinazione attraverso il protocollo selezionato (NFS, SMB, EFS) o l'API dello storage a oggetti (Amazon S3, Azure Blob, IBM Cloud Object Storage).

Inoltre, il broker di dati necessita di una connessione Internet in uscita sulla porta 443 in modo che possa comunicare con il servizio Cloud Sync e contattare altri servizi e repository.

Per ulteriori informazioni, "[esaminare i requisiti di rete](#)".

### Esistono limitazioni di rete relative alla connettività del data broker?

I broker di dati richiedono l'accesso a Internet. Non supportiamo un server proxy durante l'implementazione del data broker in Azure o in Google Cloud Platform.

## Sincronizzazione dei dati

Le seguenti domande si riferiscono al funzionamento della sincronizzazione dei dati.

### Con quale frequenza si verifica la sincronizzazione?

La pianificazione predefinita è impostata per la sincronizzazione giornaliera. Dopo la sincronizzazione iniziale, è possibile:

- Modificare la pianificazione di sincronizzazione in base al numero di giorni, ore o minuti desiderato
- Disattivare la pianificazione della sincronizzazione
- Eliminare la pianificazione di sincronizzazione (nessun dato andrà perso; verrà rimossa solo la relazione di sincronizzazione)

### Qual è la pianificazione minima di sincronizzazione?

È possibile pianificare una relazione per sincronizzare i dati ogni 1 minuto.

### Il broker di dati riprova quando un file non riesce a sincronizzarsi? O il timeout?

Il data broker non esegue il timeout quando un singolo file non riesce a trasferire. Invece, il data broker tenta di nuovo 3 volte prima di saltare il file. Il valore di RETRY è configurabile nelle impostazioni per una relazione di sincronizzazione.

["Scopri come modificare le impostazioni per una relazione di sincronizzazione"](#).

### E se si dispone di un set di dati molto grande?

Se una singola directory contiene almeno 600,000 file, [contattaci](#) per aiutarti a configurare il data broker in modo da gestire il payload. Potrebbe essere necessario aggiungere ulteriore memoria alla macchina del broker di dati.

## Sicurezza

Le seguenti domande relative alla sicurezza.

### Cloud Sync è sicuro?

Sì. Tutta la connettività di rete del servizio Cloud Sync viene eseguita utilizzando ["Amazon Simple Queue Service \(SQS\)"](#).

Tutte le comunicazioni tra il data broker e Amazon S3, Azure Blob, Google Cloud Storage e IBM Cloud Object Storage vengono effettuate tramite il protocollo HTTPS.

Se utilizzi Cloud Sync con sistemi on-premise (di origine o di destinazione), ecco alcune opzioni di connettività consigliate:

- Una connessione AWS Direct Connect, Azure ExpressRoute o Google Cloud Interconnect, non instradata su Internet (e in grado di comunicare solo con le reti cloud specificate)
- Una connessione VPN tra il dispositivo gateway on-premise e le reti cloud
- Per un trasferimento dei dati estremamente sicuro con i bucket S3, lo storage Azure Blob o Google Cloud Storage, è possibile stabilire un endpoint Amazon Private S3 Endpoint, un endpoint del servizio Azure Virtual Network o un accesso privato a Google.

Uno qualsiasi di questi metodi stabilisce una connessione sicura tra i server NAS on-premise e un data broker Cloud Sync.

### **I dati sono crittografati da Cloud Sync?**

- Cloud Sync supporta la crittografia data-in-flight tra server NFS di origine e di destinazione. ["Scopri di più"](#).
- La crittografia non è supportata con SMB.
- Quando un bucket Amazon S3 è la destinazione di una relazione di sincronizzazione, puoi scegliere se attivare la crittografia dei dati utilizzando la crittografia AWS KMS o AES-256.

## **Permessi**

Le seguenti domande si riferiscono alle autorizzazioni per i dati.

### **Le autorizzazioni dei dati SMB sono sincronizzate con la posizione di destinazione?**

È possibile impostare Cloud Sync in modo da conservare gli elenchi di controllo degli accessi (ACL) tra una condivisione SMB di origine e una condivisione SMB di destinazione. In alternativa, è possibile copiare manualmente gli ACL. ["Scopri come copiare gli ACL tra le condivisioni SMB"](#).

### **Le autorizzazioni dei dati NFS sono sincronizzate con la posizione di destinazione?**

Cloud Sync copia automaticamente le autorizzazioni NFS tra i server NFS come segue:

- NFS versione 3: Cloud Sync copia i permessi e il proprietario del gruppo di utenti.
- NFS versione 4: Cloud Sync copia gli ACL.

## **Performance**

Le seguenti domande si riferiscono alle performance di Cloud Sync.

### **Cosa rappresenta l'indicatore di avanzamento di una relazione di sincronizzazione?**

La relazione di sincronizzazione mostra il throughput della scheda di rete del data broker. Se le prestazioni di sincronizzazione sono state accelerate utilizzando più broker di dati, il throughput è la somma di tutto il traffico. Questo throughput viene aggiornato ogni 20 secondi.

### **Sto riscontrando problemi di performance. Possiamo limitare il numero di trasferimenti simultanei?**

Il data broker può sincronizzare 4 file alla volta. Se si dispone di file di grandi dimensioni (più TB ciascuno), il completamento del processo di trasferimento può richiedere molto tempo e le prestazioni potrebbero risentirne.

Limitare il numero di trasferimenti simultanei può essere di aiuto. [Mailto:ng-cloudsync-support@netapp.com](mailto:ng-cloudsync-support@netapp.com)[Contattaci per ricevere assistenza].

### **Perché si riscontrano prestazioni ridotte con Azure NetApp Files?**

Quando si sincronizzano i dati con o da Azure NetApp Files, potrebbero verificarsi errori e problemi di performance se il livello di servizio del disco è standard.

Impostare il livello di servizio su Premium o Ultra per migliorare le prestazioni di sincronizzazione.



["Scopri di più sui livelli di servizio e sul throughput di Azure NetApp Files"](#).

## **Perché si riscontrano prestazioni ridotte con Cloud Volumes Service per AWS?**

Quando sincronizzi i dati da o verso un volume cloud, potresti riscontrare guasti e problemi di performance se il livello di performance per il volume cloud è Standard.

Impostare il livello di servizio su Premium o Extreme per migliorare le prestazioni di sincronizzazione.

## **Quanti broker di dati sono richiesti?**

Quando si crea una nuova relazione, si inizia con un singolo data broker (a meno che non sia stato selezionato un data broker esistente che appartiene a una relazione di sincronizzazione accelerata). In molti casi, un singolo data broker può soddisfare i requisiti di performance per una relazione di sincronizzazione. In caso contrario, puoi accelerare le performance di sincronizzazione aggiungendo ulteriori broker di dati. Tuttavia, è necessario prima controllare altri fattori che possono influire sulle prestazioni di sincronizzazione.

Diversi fattori possono influire sulle performance di trasferimento dei dati. Le performance di sincronizzazione complessive potrebbero risentire della larghezza di banda, della latenza e della topologia di rete, delle specifiche delle macchine virtuali del data broker e delle performance del sistema storage. Ad esempio, un singolo broker di dati in una relazione di sincronizzazione può raggiungere 100 MB/s, mentre il throughput del disco sulla destinazione potrebbe consentire solo 64 MB/s. Di conseguenza, il data broker continua a cercare di copiare i dati, ma la destinazione non può soddisfare le performance del data broker.

Pertanto, verificare le prestazioni della rete e il throughput del disco sulla destinazione.

Quindi, puoi prendere in considerazione l'accelerazione delle performance di sincronizzazione aggiungendo un ulteriore broker di dati per condividere il carico di tale relazione. ["Scopri come accelerare le performance di sincronizzazione"](#).

## **Eliminare le cose**

Le seguenti domande si riferiscono all'eliminazione di relazioni di sincronizzazione e dati da origini e destinazioni.

### **Cosa succede se si elimina la relazione Cloud Sync?**

L'eliminazione di una relazione interrompe tutte le future sincronizzazioni dei dati e termina il pagamento. Tutti i dati sincronizzati con la destinazione rimangono invariati.

### **Cosa succede se si elimina qualcosa dal server di origine? Viene rimosso anche dalla destinazione?**

Per impostazione predefinita, se si dispone di una relazione di sincronizzazione attiva, l'elemento eliminato sul server di origine non viene eliminato dalla destinazione durante la sincronizzazione successiva. Tuttavia, nelle impostazioni di sincronizzazione per ciascuna relazione è disponibile un'opzione in cui è possibile definire che Cloud Sync elimini i file nella posizione di destinazione se sono stati eliminati dall'origine.

["Scopri come modificare le impostazioni per una relazione di sincronizzazione"](#).

### **Cosa succede se si elimina qualcosa dalla destinazione? Viene rimosso anche dalla fonte?**

Se un elemento viene eliminato dalla destinazione, non verrà rimosso dall'origine. La relazione è unidirezionale, dall'origine alla destinazione. Al successivo ciclo di sincronizzazione, Cloud Sync confronta l'origine con la destinazione, identifica l'elemento mancante e Cloud Sync lo copia di nuovo dall'origine alla destinazione.

## Risoluzione dei problemi

["Knowledge base di NetApp: Domande frequenti su Cloud Sync: Supporto e risoluzione dei problemi"](#)

### Analisi approfondita del data broker

La seguente domanda si riferisce al data broker.

#### Puoi spiegare l'architettura del data broker?

Certo. Ecco i punti più importanti:

- Il data broker è un'applicazione node.js in esecuzione su un host Linux.
- Cloud Sync implementa il data broker come segue:
  - AWS: Da un modello AWS CloudFormation
  - Azure: Da Azure Resource Manager
  - Google: Da Google Cloud Deployment Manager
  - Se si utilizza il proprio host Linux, è necessario installare manualmente il software
- Il software data broker si aggiorna automaticamente alla versione più recente.
- Il data broker utilizza AWS SQS come canale di comunicazione affidabile e sicuro e per il controllo e il monitoraggio. SQS fornisce anche un layer di persistenza.
- È possibile aggiungere ulteriori broker di dati a una relazione per aumentare la velocità di trasferimento e aggiungere alta disponibilità. In caso di guasto di un broker di dati, esiste una resilienza del servizio.

## Informazioni sul copyright

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

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

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E 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.