



# Lernprogramme

## Cloud Manager 3.8

NetApp  
March 25, 2024

# Inhalt

- Lernprogramme ..... 1
  - Kopieren von ACLs zwischen SMB-Freigaben ..... 1
  - Synchronisierung von NFS-Daten mithilfe von Verschlüsselung bei der Übertragung ..... 3

# Lernprogramme

## Kopieren von ACLs zwischen SMB-Freigaben

Cloud Sync kann Zugriffssteuerungslisten (ACLs) zwischen einer SMB-Quell-Freigabe und einer SMB-Zielfreigabe kopieren. Bei Bedarf können Sie die ACLs manuell mithilfe von robocopy beibehalten.

### Wahlmöglichkeiten

- [um ACLs zwischen SMB-Servern zu kopieren](#), Richten Sie Cloud Sync so ein, dass ACLs automatisch kopiert werden
- [Kopieren Sie die ACLs manuell](#)

## Cloud Sync einrichten, um ACLs zwischen SMB-Servern zu kopieren

Kopieren Sie ACLs zwischen SMB-Servern, indem Sie eine Einstellung aktivieren, wenn Sie eine Beziehung erstellen oder nachdem Sie eine Beziehung erstellt haben.

Beachten Sie, dass diese Funktion für neue Synchronisierungsbeziehungen verfügbar ist, die nach der Version vom 23. Februar 2020 erstellt wurden. Wenn Sie möchten, um dieses Feature mit bestehenden Beziehungen vor diesem Datum erstellt verwenden, dann müssen Sie die Beziehung neu erstellen.

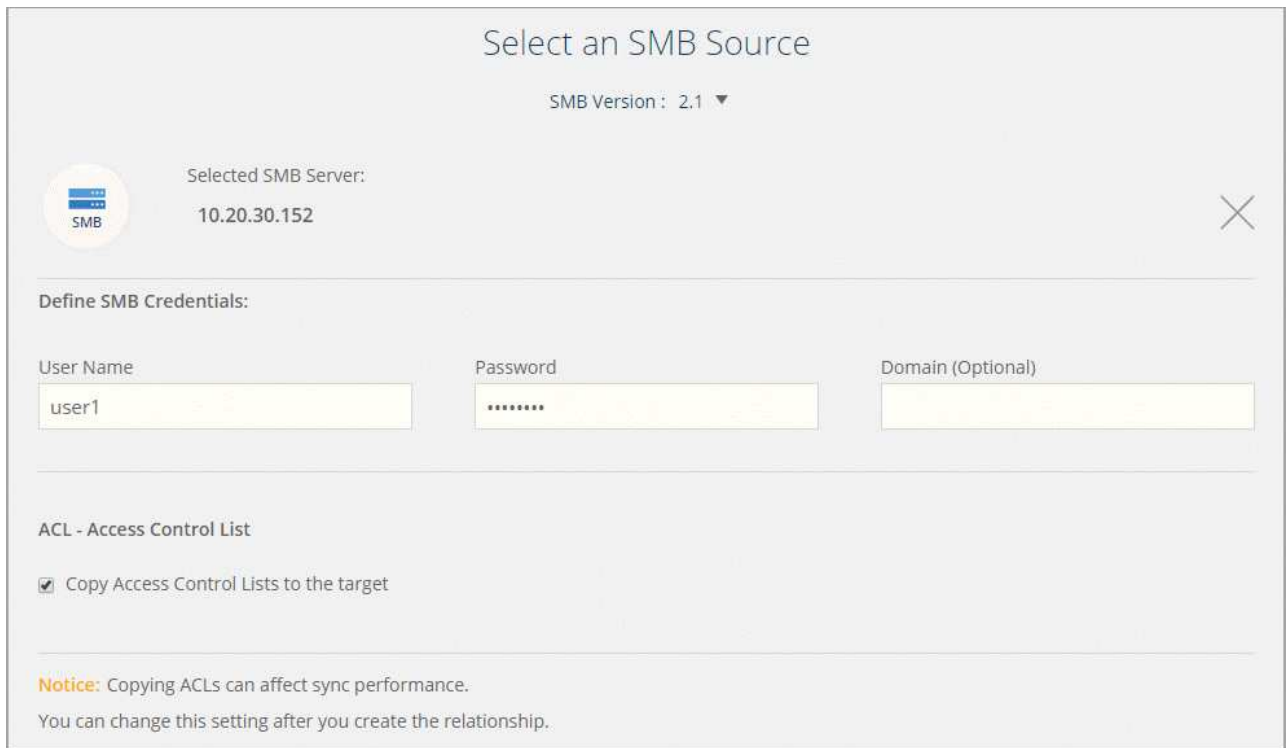
### Was Sie benötigen

- Eine neue Sync-Beziehung oder eine bestehende Sync-Beziehung, die nach dem Release des 23. Februar 2020 erstellt wurde.
- Jeder Typ von Daten-Broker.

Diese Funktion arbeitet mit jedem Datentyp Broker zusammen – AWS, Azure, Google Cloud Platform oder On-Premises-Daten-Broker. Der On-Premises-Daten-Broker kann ausgeführt werden "[Alle unterstützten Betriebssysteme](#)".

### Schritte für eine neue Beziehung

1. Klicken Sie in Cloud Sync auf **Neuen Sync erstellen**.
2. Ziehen Sie **SMB Server** an die Quelle und das Ziel und klicken Sie auf **Weiter**.
3. Auf der Seite **SMB Server**:
  - a. Geben Sie einen neuen SMB-Server ein oder wählen Sie einen vorhandenen Server aus und klicken Sie auf **Weiter**.
  - b. Geben Sie die Anmeldedaten für den SMB-Server ein.
  - c. Wählen Sie **Zugriffssteuerungslisten zum Ziel kopieren** und klicken Sie auf **Weiter**.



Select an SMB Source

SMB Version: 2.1 ▼

Selected SMB Server: 10.20.30.152

Define SMB Credentials:

User Name: user1 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. Befolgen Sie die übrigen Anweisungen, um die Synchronisierungsbeziehung zu erstellen.

#### Schritte für eine bestehende Beziehung

1. Zeigen Sie mit der Maus auf die Synchronisierungsbeziehung, und klicken Sie auf das Aktionsmenü.
2. Klicken Sie Auf **Einstellungen**.
3. Wählen Sie **Zugriffssteuerungslisten zum Ziel kopieren** aus.
4. Klicken Sie Auf **Einstellungen Speichern**.

#### Ergebnis

Beim Synchronisieren von Daten behält Cloud Sync die ACLs zwischen den Quell- und Ziel-SMB-Freigaben vor.

## Manuelles Kopieren von ACLs

Sie können ACLs manuell zwischen SMB-Freigaben beibehalten, indem Sie den Befehl Windows robocopy verwenden.

#### Schritte

1. Identifizieren Sie einen Windows-Host mit vollem Zugriff auf beide SMB-Freigaben.
2. Wenn einer der Endpunkte eine Authentifizierung erfordert, verwenden Sie den Befehl **net use**, um eine Verbindung zu den Endpunkten vom Windows-Host herzustellen.

Sie müssen diesen Schritt ausführen, bevor Sie Robocopy verwenden.

3. Von Cloud Sync aus: Erstellen Sie eine neue Beziehung zwischen Quell- und Ziel-SMB-Freigaben, oder synchronisieren Sie eine vorhandene Beziehung.
4. Führen Sie nach Abschluss der Datensynchronisierung den folgenden Befehl vom Windows-Host aus aus, um die ACLs und Besitzrechte zu synchronisieren:

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

Es sollten sowohl *Source* als auch *Target* mit dem UNC-Format angegeben werden. Beispiel:  
\\<Server>\<Freigabe>\<Pfad>

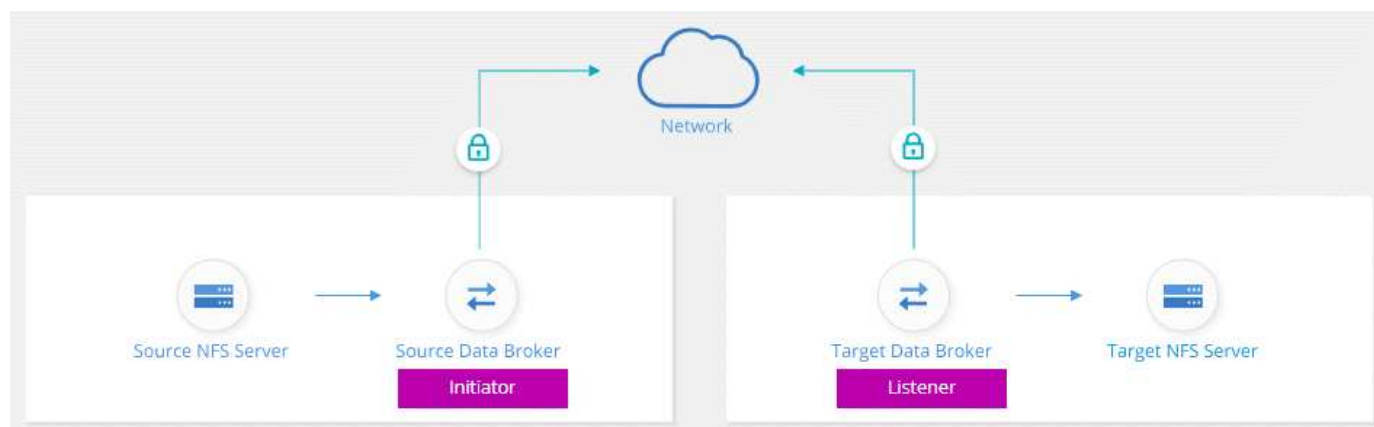
## Synchronisierung von NFS-Daten mithilfe von Verschlüsselung bei der Übertragung

Verfügt Ihr Unternehmen über strenge Sicherheitsrichtlinien, können Sie NFS-Daten mithilfe von Verschlüsselung der aktiven Daten synchronisieren. Diese Funktion wird von einem NFS-Server zu einem anderen NFS-Server und von Azure NetApp Files zu Azure NetApp Files unterstützt.

So könnten Sie beispielsweise Daten zwischen zwei NFS Servern synchronisieren, die sich in verschiedenen Netzwerken befinden. Alternativ müssen Daten über Azure NetApp Files sicher über Subnetze und Regionen hinweg übertragen werden.

### Funktionsweise der Datenverschlüsselung während des Flugs

Verschlüsselung von übertragenen Daten verschlüsselt NFS-Daten, wenn sie zwischen zwei Datenmaklern über das Netzwerk gesendet werden. Das folgende Bild zeigt eine Beziehung zwischen zwei NFS-Servern und zwei Datenmaklern:



Ein Datenvermittler fungiert als *Initiator*. Wenn es Zeit ist, Daten zu synchronisieren, sendet es eine Verbindungsanforderung an den anderen Daten-Broker, der *Listener* ist. Der Datenmanager wartet auf Anfragen am Port 443. Sie können bei Bedarf einen anderen Port verwenden, überprüfen jedoch, ob der Port nicht von einem anderen Dienst verwendet wird.

Wenn Sie beispielsweise Daten von einem lokalen NFS-Server mit einem Cloud-basierten NFS-Server synchronisieren, können Sie auswählen, welcher Daten-Broker die Verbindungsanforderungen abhört und welche sendet.

Funktionsweise der Verschlüsselung auf der Übertragungsstrecke:

1. Nachdem Sie die Synchronisierungsbeziehung erstellt haben, startet der Initiator eine verschlüsselte Verbindung mit dem anderen Daten-Broker.
2. Der Quell-Datenvermittler verschlüsselt Daten aus der Quelle mithilfe von TLS 1.3.

3. Die Daten werden dann über das Netzwerk an den Ziel-Data-Broker gesendet.
4. Der Zieldatenbroker entschlüsselt die Daten, bevor sie an das Ziel gesendet werden.
5. Nach der ersten Kopie synchronisiert der Service alle 24 Stunden alle geänderten Daten. Wenn Daten zu synchronisieren sind, beginnt der Prozess mit dem Öffnen einer verschlüsselten Verbindung mit dem anderen Daten-Broker durch den Initiator.

Falls Sie Daten häufiger synchronisieren möchten, ["Sie können den Zeitplan nach dem Erstellen der Beziehung ändern"](#).

## Unterstützte NFS-Versionen

- Bei NFS-Servern wird die Verschlüsselung der aktiven Daten mit NFS Version 3, 4.0, 4.1 und 4.2 unterstützt.
- Für Azure NetApp Files wird die Verschlüsselung von aktiven Daten mit NFS Version 3 und 4.1 unterstützt.

## Was Sie benötigen, um zu beginnen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

- Zwei NFS-Server, die erfüllen ["Quell- und Zielforderungen"](#) Oder Azure NetApp Files in zwei Subnetzen oder Regionen.
- Die IP-Adressen oder vollqualifizierte Domain-Namen der Server.
- Netzwerkstandorte für zwei Datenvermittler.

Sie können einen vorhandenen Daten-Broker auswählen, der jedoch als Initiator fungieren muss. Der Listener-Daten-Broker muss ein *New* Daten-Broker sein.

Wenn Sie noch keinen Data Broker implementiert haben, überprüfen Sie die Anforderungen des Data Brokers. Da Sie über strenge Sicherheitsrichtlinien verfügen, überprüfen Sie unbedingt die Netzwerkanforderungen, einschließlich des ausgehenden Datenverkehrs von Port 443 und dem ["internetendpunkte"](#) Dass sich der Daten-Broker mit diesen in Verbindung setzt.

- ["Überprüfen Sie die AWS-Installation"](#)
- ["Überprüfen Sie die Azure Installation"](#)
- ["Überprüfen Sie die GCP-Installation"](#)
- ["Überprüfen Sie die Installation des Linux-Hosts"](#)

## Synchronisierung von NFS-Daten mithilfe von Verschlüsselung bei der Übertragung

Erstellen Sie eine neue Synchronisierungsbeziehung zwischen zwei NFS-Servern oder zwischen Azure NetApp Files, aktivieren Sie die Option für die Verschlüsselung während des Fluges, und befolgen Sie die Anweisungen.

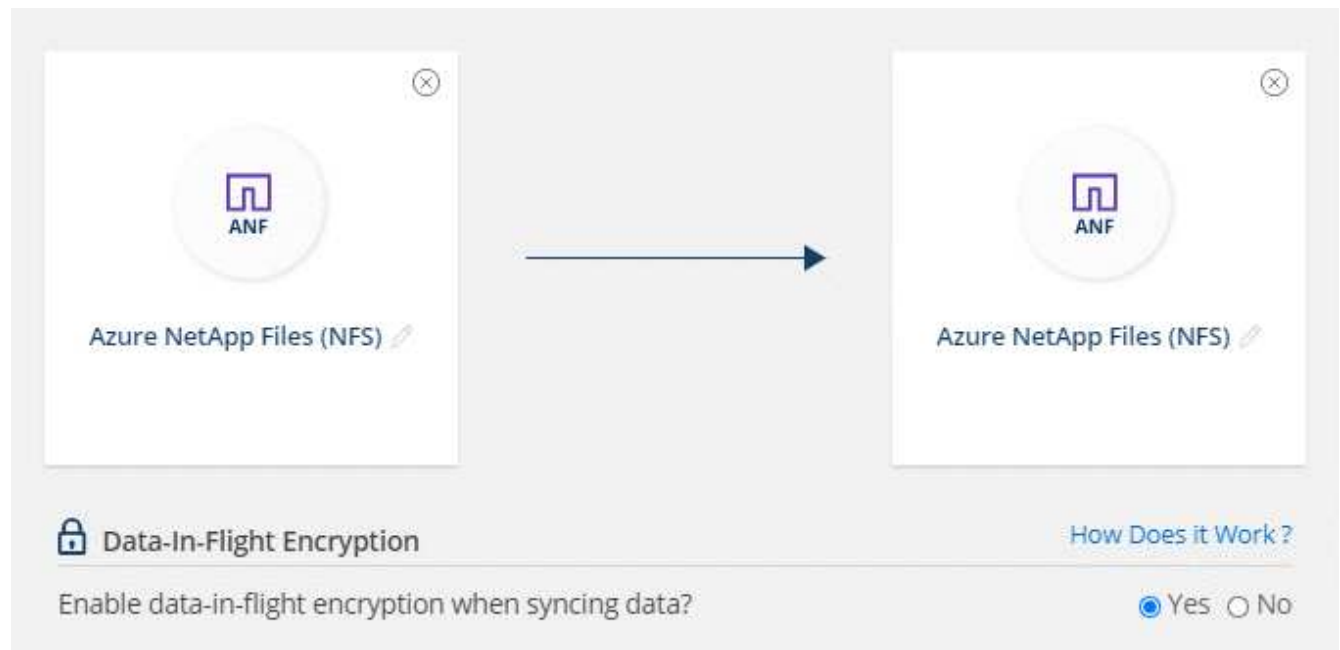
### Schritte

1. Klicken Sie Auf **Neuen Sync Erstellen**.
2. Ziehen Sie **NFS-Server** an den Quell- und Zielspeicherort oder **Azure NetApp Files** an den Quell- und Zielstandorten und wählen Sie **Ja** aus, um die Verschlüsselung von Daten während der Übertragung zu aktivieren.

Das folgende Bild zeigt, was Sie für die Synchronisierung von Daten zwischen zwei NFS-Servern auswählen würden:



Das folgende Bild zeigt, was Sie für die Synchronisierung von Daten zwischen Azure NetApp Files auswählen würden:



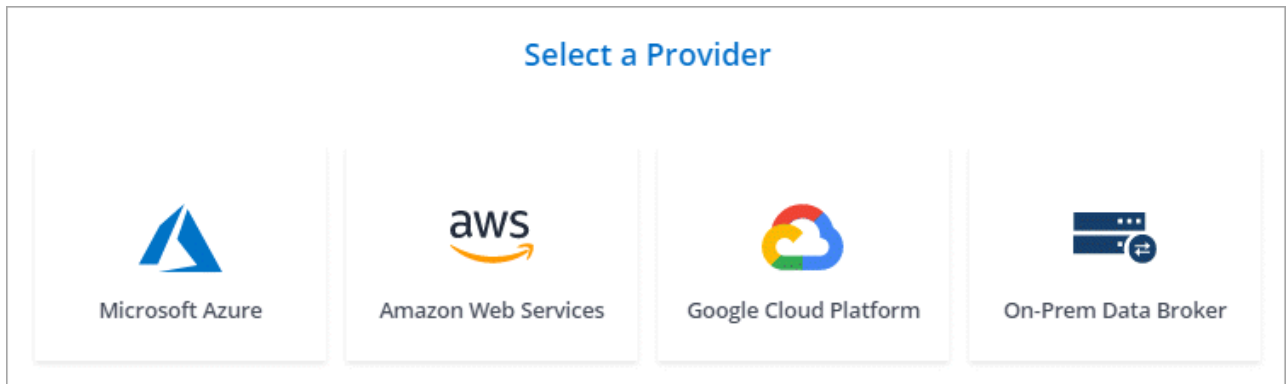
3. Folgen Sie den Anweisungen, um die Beziehung zu erstellen:

- a. **NFS Server/Azure NetApp Files:** Wählen Sie die NFS-Version und geben Sie dann eine neue NFS-Quelle an oder wählen Sie einen bestehenden Server aus.
- b. **Definieren der Data Broker-Funktionalität:** Legen Sie fest, welcher Datenbroker *hört* nach Verbindungsanfragen an einem Port ab und welcher die Verbindung initiiert. Treffen Sie Ihre Wahl auf der Grundlage Ihrer Netzwerkanforderungen.

- c. **Data Broker:** Folgen Sie den Aufforderungen, um einen neuen Quell-Daten-Broker hinzuzufügen oder einen vorhandenen Datenmakler auszuwählen.

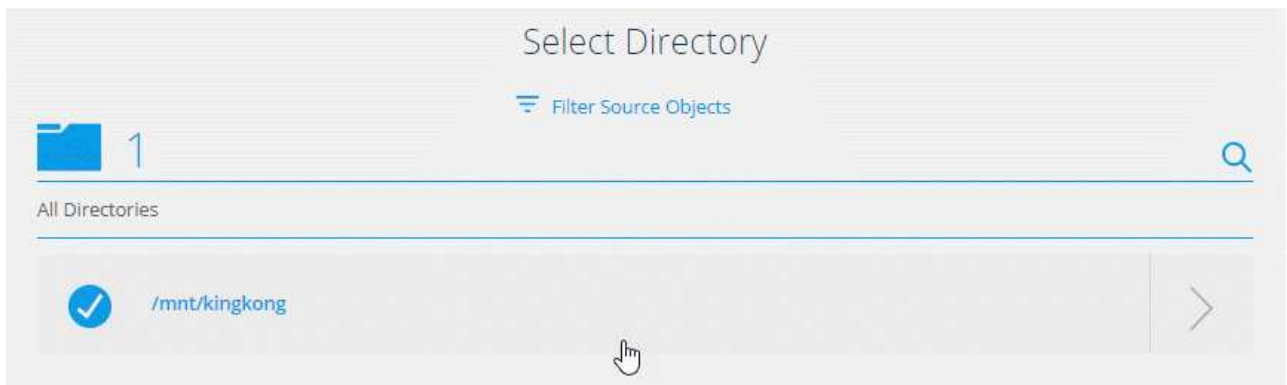
Wenn der Quelldaten-Broker als Listener fungiert, muss er ein neuer Daten-Broker sein.

Wenn Sie einen neuen Daten-Broker benötigen, werden Sie von Cloud Sync aufgefordert, die Installationsanweisungen einzugeben. Sie können den Data Broker in der Cloud bereitstellen oder ein Installationskript für Ihren eigenen Linux-Host herunterladen.



- d. **Directories:** Wählen Sie die Verzeichnisse aus, die Sie synchronisieren möchten, indem Sie alle Verzeichnisse auswählen oder indem Sie nach unten bohren und ein Unterverzeichnis auswählen.

Klicken Sie auf **Quellobjekte filtern**, um Einstellungen zu ändern, die festlegen, wie Quelldateien und Ordner synchronisiert und am Zielspeicherort verwaltet werden.




- e. **Ziel-NFS-Server/Ziel-Azure NetApp Files:** Wählen Sie die NFS-Version und geben Sie dann ein neues NFS-Ziel ein oder wählen Sie einen vorhandenen Server aus.
- f. **Target Data Broker:** Befolgen Sie die Aufforderungen, um einen neuen Quell-Daten-Broker hinzuzufügen oder einen vorhandenen Daten-Broker auszuwählen.

Wenn der Ziel-Data-Broker als Listener fungiert, muss er ein neuer Daten-Broker sein.


Dies ist ein Beispiel für die Eingabeaufforderung, wenn der Zieldatenbroker als Listener fungiert. Beachten Sie die Option zur Angabe des Ports.




### Select a Provider




Microsoft Azure



Amazon Web Services



Google Cloud Platform

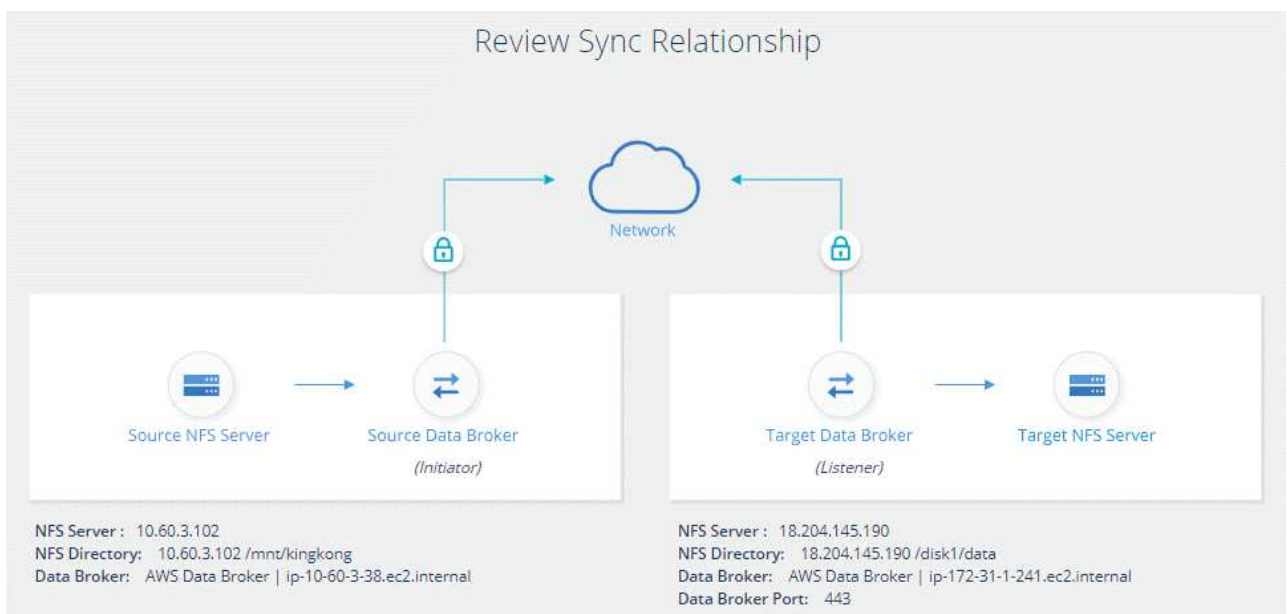


On-Prem Data Broker

Data Broker Name:

Port:

- a. **Zielverzeichnisse:** Wählen Sie ein Verzeichnis der obersten Ebene aus, oder gehen Sie nach unten, um ein vorhandenes Unterverzeichnis auszuwählen oder einen neuen Ordner in einem Export zu erstellen.
- b. **Einstellungen:** Legen Sie fest, wie Quelldateien und Ordner im Zielverzeichnis synchronisiert und verwaltet werden.
- c. **Review:** Überprüfen Sie die Details der Synchronisierungsbeziehung und klicken Sie dann auf **Beziehung erstellen**.



## Ergebnis

Cloud Sync beginnt mit der Erstellung der neuen Synchronisierungsbeziehung. Klicken Sie anschließend auf **Anzeigen in Dashboard**, um Details zur neuen Beziehung anzuzeigen.

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.