Daten zwischen Quelle und Ziel synchronisieren

NetApp Copy and Sync

NetApp
December 16, 2025

Inhalt

Daten zwischen Quelle und Ziel synchronisieren

Bereiten Sie einen Datenbroker vor, um Daten zwischen Objektspeichern in NetApp Copy and Sync zu synchronisieren

Wenn Sie planen, Daten von Objektspeicher zu Objektspeicher (z. B. Amazon S3 zu Azure Blob) in NetApp Copy and Sync zu synchronisieren, müssen Sie die Datenbrokergruppe vorbereiten, bevor Sie die Synchronisierungsbeziehung erstellen.

Informationen zu diesem Vorgang

Um die Datenbrokergruppe vorzubereiten, müssen Sie die Konfiguration des Scanners ändern. Wenn Sie die Konfiguration nicht ändern, können bei dieser Synchronisierungsbeziehung Leistungsprobleme auftreten.

Bevor Sie beginnen

Die Datenbrokergruppe, die Sie zum Synchronisieren von Daten von Objektspeicher zu Objektspeicher verwenden, sollte nur diese Arten von Synchronisierungsbeziehungen verwalten. Wenn die Datenbrokergruppe eine andere Art von Synchronisierungsbeziehung verwaltet (z. B. NFS zu NFS oder Objektspeicher zu SMB), kann die Leistung dieser Synchronisierungsbeziehungen negativ beeinflusst werden.

Schritte

1. "Bei Copy and Sync anmelden" .
2. Wählen Sie unter „Kopieren und Synchronisieren“ die Option „Datenbroker verwalten“ aus.
3. Wählen 
4. Aktualisieren Sie die Scannerkonfiguration:
   a. Ändern Sie **Scanner-Parallelität** in **1**.
   b. Ändern Sie **Scanner-Prozesslimit** auf **1**.
5. Wählen Sie **Unify-Konfiguration**.

Ergebnis

Kopieren und Synchronisieren aktualisiert die Konfiguration der Datenbrokergruppe.

Wie geht es weiter?

Sie können jetzt die Synchronisierungsbeziehung zwischen Objektspeichern mithilfe der gerade konfigurierten Datenbrokergruppe erstellen.

Erstellen Sie Synchronisierungsbeziehungen in NetApp Copy and Sync

Wenn Sie eine Synchronisierungsbeziehung erstellen, NetApp Copy and Sync Dateien von der Quelle zum Ziel. Nach der ersten Kopie synchronisiert Copy and Sync alle geänderten Daten alle 24 Stunden.

Bevor Sie bestimmte Arten von Synchronisierungsbeziehungen erstellen können, müssen Sie zunächst ein System in der NetApp Console erstellen.

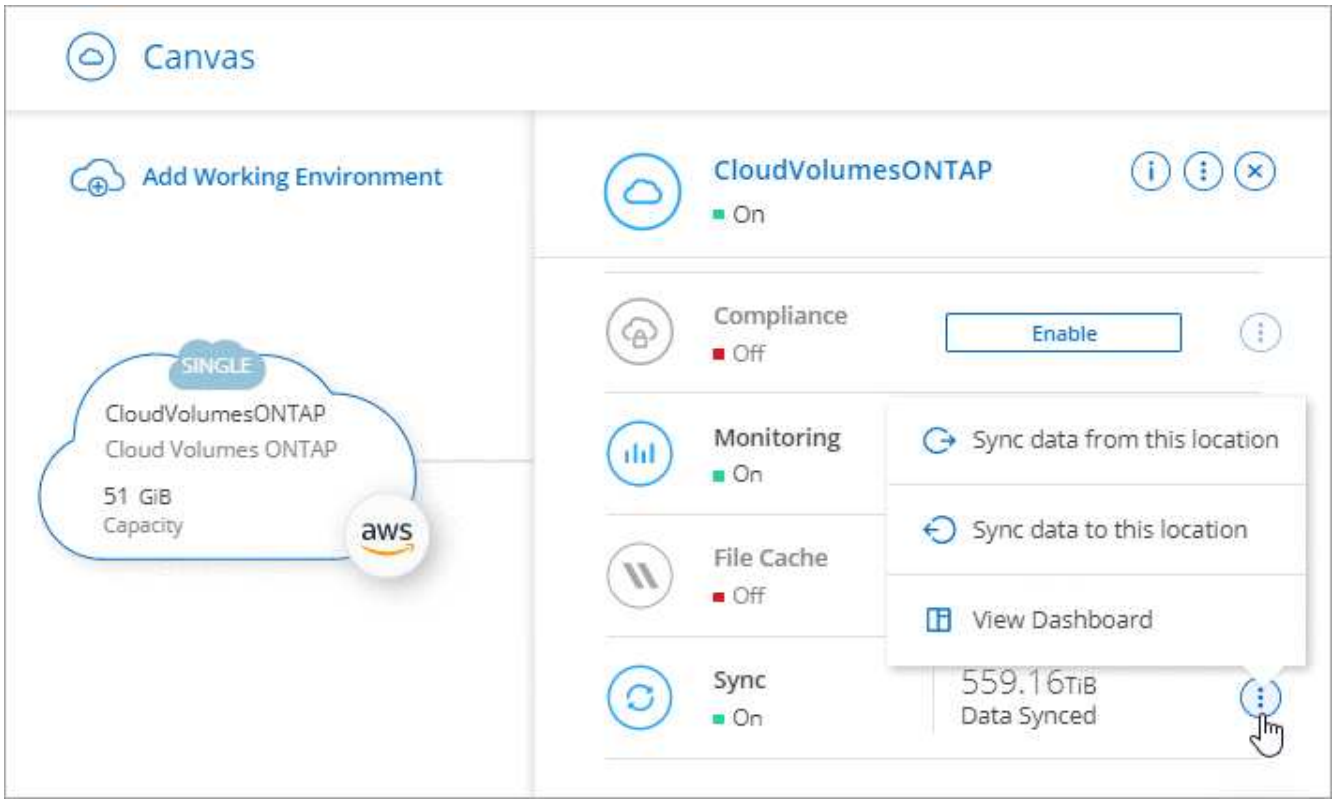
Erstellen Sie Synchronisierungsbeziehungen für bestimmte Systemtypen

Wenn Sie Synchronisierungsbeziehungen für eines der folgenden Elemente erstellen möchten, müssen Sie zuerst das System erstellen oder ermitteln:

- Amazon FSx für ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- On-Premise- ONTAP Cluster

Schritte

1. "Bei Copy and Sync anmelden" .
2. Erstellen oder entdecken Sie das System.
    - "Erstellen Sie ein Amazon FSx für ONTAP -System"
    - "Einrichten und Ermitteln von Azure NetApp Files"
    - "Starten von Cloud Volumes ONTAP in AWS"
    - "Starten von Cloud Volumes ONTAP in Azure"
    - "Starten von Cloud Volumes ONTAP in Google Cloud"
    - "Hinzufügen vorhandener Cloud Volumes ONTAP -Systeme"
    - "Erkennen von ONTAP Clustern"
3. Wählen Sie **Systemseite**.
4. Wählen Sie ein System aus, das einem der oben aufgeführten Typen entspricht.
5. Wählen Sie das Aktionsmenü neben „Synchronisieren“ aus.



6. Wählen Sie **Daten von diesem Ort synchronisieren** oder **Daten mit diesem Ort synchronisieren** und folgen Sie den Anweisungen zum Einrichten der Synchronisierungsbeziehung.

Erstellen anderer Arten von Synchronisierungsbeziehungen

Verwenden Sie diese Schritte, um Daten mit einem anderen unterstützten Speichertyp als Amazon FSx for ONTAP, Azure NetApp Files, Cloud Volumes ONTAP oder lokalen ONTAP Clustern zu synchronisieren oder von diesem zu übertragen. Die folgenden Schritte stellen ein Beispiel dar, das zeigt, wie eine Synchronisierungsbeziehung von einem NFS-Server zu einem S3-Bucket eingerichtet wird.

1. Wählen Sie in der NetApp Console*Synchronisieren* aus.
2. Wählen Sie auf der Seite **Synchronisierungsbeziehung definieren** eine Quelle und ein Ziel aus.

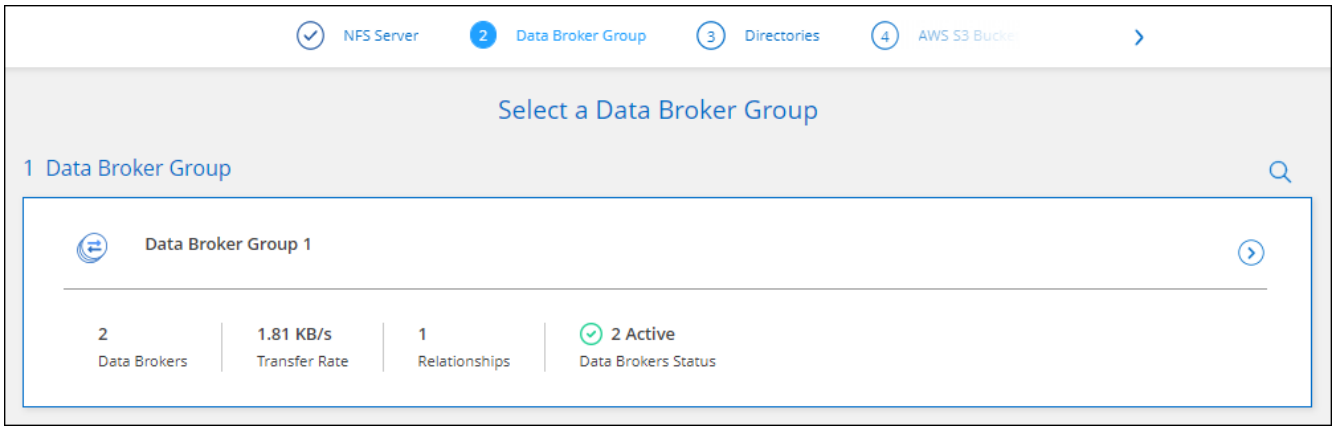
   Die folgenden Schritte bieten ein Beispiel für die Erstellung einer Synchronisierungsbeziehung von einem NFS-Server zu einem S3-Bucket.

3. Geben Sie auf der Seite **NFS-Server** die IP-Adresse oder den vollqualifizierten Domänennamen des NFS-Servers ein, den Sie mit AWS synchronisieren möchten.
4. Folgen Sie auf der Seite **Data Broker Group** den Anweisungen zum Erstellen einer virtuellen Data Broker-Maschine in AWS, Azure oder Google Cloud Platform oder zum Installieren der Data Broker-Software auf einem vorhandenen Linux-Host.

   Weitere Einzelheiten finden Sie auf den folgenden Seiten:

- "Erstellen Sie einen Datenbroker in AWS"
- "Erstellen eines Datenbrokers in Azure"
- "Erstellen Sie einen Datenbroker in Google Cloud"
- "Installieren des Datenbrokers auf einem Linux-Host"

5. Wählen Sie nach der Installation des Datenbrokers **Weiter**.

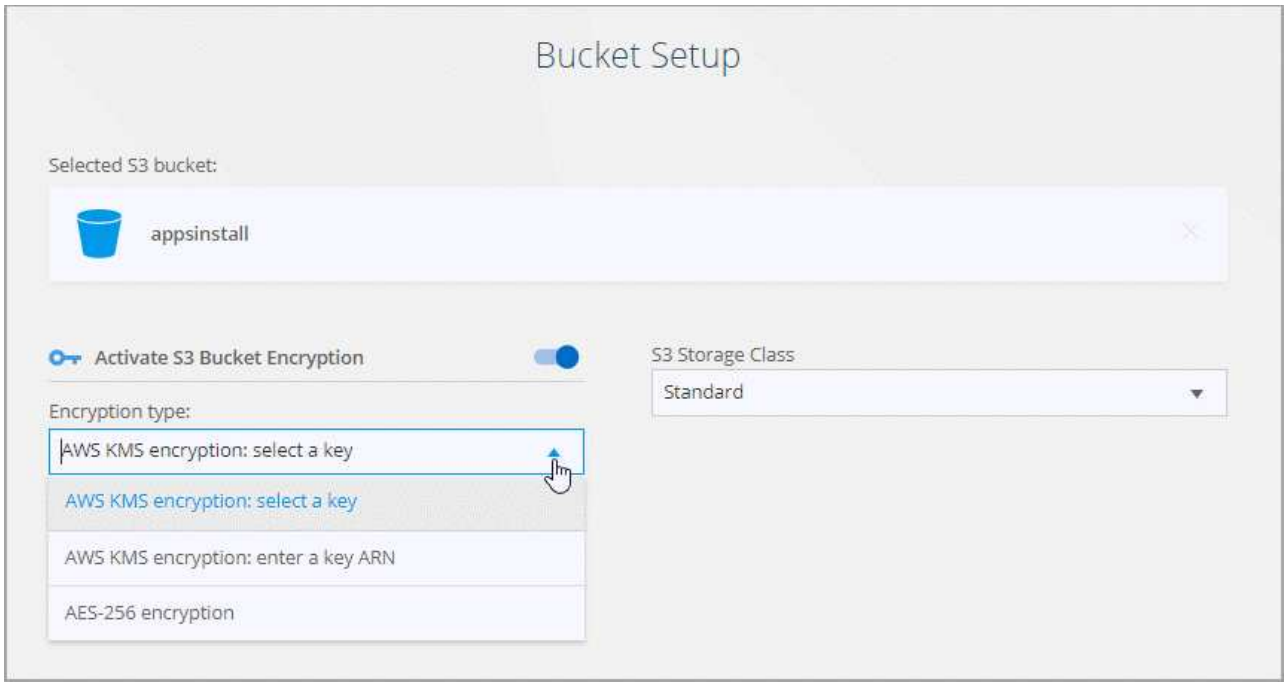


6. Wählen Sie auf der Seite **Verzeichnisse** ein Verzeichnis der obersten Ebene oder ein Unterverzeichnis aus.

   Wenn Copy and Sync die Exporte nicht abrufen kann, wählen Sie **Export manuell hinzufügen** und geben Sie den Namen eines NFS-Exports ein.

   Wenn Sie mehr als ein Verzeichnis auf dem NFS-Server synchronisieren möchten, müssen Sie anschließend zusätzliche Synchronisierungsbeziehungen erstellen.

7. Wählen Sie auf der Seite **AWS S3 Bucket** einen Bucket aus:
   - Führen Sie einen Drilldown durch, um einen vorhandenen Ordner im Bucket auszuwählen oder einen neuen Ordner auszuwählen, den Sie im Bucket erstellen.
   - Wählen Sie **Zur Liste hinzufügen**, um einen S3-Bucket auszuwählen, der nicht mit Ihrem AWS-Konto verknüpft ist. "Für den S3-Bucket müssen bestimmte Berechtigungen angewendet werden" .
8. Richten Sie auf der Seite **Bucket-Setup** den Bucket ein:
   - Wählen Sie, ob die S3-Bucket-Verschlüsselung aktiviert werden soll, und wählen Sie dann einen AWS KMS-Schlüssel aus, geben Sie die ARN eines KMS-Schlüssels ein oder wählen Sie die AES-256-Verschlüsselung aus.
   - Wählen Sie eine S3-Speicherklasse aus. "Anzeigen der unterstützten Speicherklassen" .



9. Definieren Sie auf der Seite **Einstellungen**, wie Quelldateien und -ordner am Zielspeicherort synchronisiert und verwaltet werden:

Zeitplan

Wählen Sie einen wiederkehrenden Zeitplan für zukünftige Synchronisierungen oder deaktivieren Sie den Synchronisierungszeitplan. Sie können eine Beziehung so planen, dass die Daten alle 1 Minute synchronisiert werden.

Synchronisierungs-Timeout

Legen Sie fest, ob Copy and Sync eine Datensynchronisierung abbrechen soll, wenn die Synchronisierung nicht innerhalb der angegebenen Anzahl von Minuten, Stunden oder Tagen abgeschlossen ist.

Benachrichtigungen

Ermöglicht Ihnen die Auswahl, ob Sie Kopier- und Synchronisierungsbenachrichtigungen im Benachrichtigungscenter der NetApp Konsole erhalten möchten. Sie können Benachrichtigungen für erfolgreiche, fehlgeschlagene und abgebrochene Datensynchronisierungen aktivieren.

Wiederholungsversuche

Definieren Sie, wie oft Copy and Sync erneut versuchen soll, eine Datei zu synchronisieren, bevor sie übersprungen wird.

Kontinuierliche Synchronisierung

Nach der ersten Datensynchronisierung überwacht Copy and Sync Änderungen am Quell-S3-Bucket oder Google Cloud Storage-Bucket und synchronisiert alle Änderungen kontinuierlich mit dem Ziel, sobald sie auftreten. Es ist nicht erforderlich, die Quelle in geplanten Intervallen erneut zu scannen.

Diese Einstellung ist nur verfügbar, wenn Sie eine Synchronisierungsbeziehung erstellen und wenn Sie Daten aus einem S3-Bucket oder Google Cloud Storage mit Azure Blob Storage, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS, S3 und StorageGRID **oder** von Azure Blob Storage mit Azure Blob Storage, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS und StorageGRID synchronisieren.

Wenn Sie diese Einstellung aktivieren, wirkt sich dies wie folgt auf andere Funktionen aus:

- Der Synchronisierungszeitplan ist deaktiviert.
- Die folgenden Einstellungen werden auf ihre Standardwerte zurückgesetzt: Synchronisierungszeitüberschreitung, Zuletzt geänderte Dateien und Änderungsdatum.
- Wenn S3 die Quelle ist, ist die Filterung nach Größe nur bei Kopierereignissen aktiv (nicht bei Löschereignissen).
- Nachdem die Beziehung erstellt wurde, können Sie sie nur beschleunigen oder löschen. Sie können Synchronisierungen nicht abbrechen, Einstellungen nicht ändern oder Berichte anzeigen.

  Es ist möglich, eine Continuous Sync-Beziehung mit einem externen Bucket zu erstellen. Führen Sie dazu die folgenden Schritte aus:

  i. Gehen Sie zur Google Cloud-Konsole für das Projekt des externen Buckets.
  ii. Gehen Sie zu **Cloud-Speicher > Einstellungen > Cloud-Speicher-Dienstkonto**.
  iii. Aktualisieren Sie die Datei local.json:

```
{
"protocols": {
    "gcp": {
        "storage-account-email": <storage account email>
}
}
}
```

  iv. Starten Sie den Datenbroker neu:
    A. sudo pm2 alles stoppen
    B. sudo pm2 starte alles
  v. Erstellen Sie eine Continuous Sync-Beziehung mit dem entsprechenden externen Bucket.

> Ein Datenbroker, der zum Erstellen einer kontinuierlichen Synchronisierungsbeziehung mit einem externen Bucket verwendet wird, kann keine weitere kontinuierliche Synchronisierungsbeziehung mit einem Bucket in seinem Projekt erstellen.

Vergleichen nach

Wählen Sie, ob Copy and Sync bestimmte Attribute vergleichen soll, wenn festgestellt wird, ob sich eine Datei oder ein Verzeichnis geändert hat und erneut synchronisiert werden soll.

Auch wenn Sie diese Attribute deaktivieren, vergleicht Copy and Sync die Quelle dennoch mit dem Ziel, indem es die Pfade, Dateigrößen und Dateinamen überprüft. Wenn es Änderungen gibt, werden diese Dateien und Verzeichnisse synchronisiert.

Sie können den Vergleich der folgenden Attribute durch Kopieren und Synchronisieren aktivieren oder deaktivieren:

- **mtime**: Die letzte Änderungszeit einer Datei. Dieses Attribut ist für Verzeichnisse nicht gültig.

- **uid**, **gid** und **mode**: Berechtigungsflags für Linux.

Kopieren für Objekte

Aktivieren Sie diese Option, um Metadaten und Tags des Objektspeichers zu kopieren. Wenn ein Benutzer die Metadaten der Quelle ändert, kopiert Copy and Sync dieses Objekt bei der nächsten Synchronisierung. Wenn ein Benutzer jedoch die Tags der Quelle ändert (und nicht die Daten selbst), kopiert Copy and Sync das Objekt bei der nächsten Synchronisierung nicht.

Sie können diese Option nicht mehr bearbeiten, nachdem Sie die Beziehung erstellt haben.

Das Kopieren von Tags wird mit Synchronisierungsbeziehungen unterstützt, die Azure Blob oder einen S3-kompatiblen Endpunkt (S3, StorageGRID oder IBM Cloud Object Storage) als Ziel enthalten.

Das Kopieren von Metadaten wird mit „Cloud-zu-Cloud“-Beziehungen zwischen den folgenden Endpunkten unterstützt:

- AWS S3
- Azure-Blob
- Google Cloud-Speicher
- IBM Cloud Object Storage
- StorageGRID

Kürzlich geänderte Dateien

Wählen Sie aus, ob Dateien ausgeschlossen werden sollen, die vor der geplanten Synchronisierung geändert wurden.

Dateien auf der Quelle löschen

Wählen Sie, ob Dateien vom Quellspeicherort gelöscht werden sollen, nachdem Copy and Sync die Dateien an den Zielspeicherort kopiert hat. Bei dieser Option besteht das Risiko eines Datenverlusts, da die Quelldateien nach dem Kopieren gelöscht werden.

Wenn Sie diese Option aktivieren, müssen Sie auch einen Parameter in der Datei local.json auf dem Datenbroker ändern. Öffnen Sie die Datei und aktualisieren Sie sie wie folgt:

```
{
"workers":{
"transferrer":{
"delete-on-source": true
}
}
}
```

Nach der Aktualisierung der Datei local.json sollten Sie einen Neustart durchführen: `pm2 restart all`.

Dateien auf dem Ziel löschen

Wählen Sie das Löschen von Dateien vom Zielspeicherort aus, wenn diese vom Quellspeicherort gelöscht wurden. Standardmäßig werden niemals Dateien vom Zielspeicherort gelöscht.

Dateitypen

Definieren Sie die Dateitypen, die bei jeder Synchronisierung berücksichtigt werden sollen: Dateien, Verzeichnisse, symbolische Links und Hardlinks.

Hardlinks sind nur für ungesicherte NFS-zu-NFS-Beziehungen verfügbar. Benutzer sind auf einen Scanvorgang und eine Scanner-Parallelität beschränkt und Scans müssen von einem Stammverzeichnis aus ausgeführt werden.

Dateierweiterungen ausschließen

Geben Sie den regulären Ausdruck oder die Dateierweiterungen an, die von der Synchronisierung ausgeschlossen werden sollen, indem Sie die Dateierweiterung eingeben und die Eingabetaste drücken. Geben Sie beispielsweise *log* oder *.log* ein, um *.log-Dateien auszuschließen. Bei mehreren Erweiterungen ist kein Trennzeichen erforderlich. Das folgende Video bietet eine kurze Demo:

Dateierweiterungen für eine Synchronisierungsbeziehung ausschließen

Regex oder reguläre Ausdrücke unterscheiden sich von Platzhaltern oder Glob-Ausdrücken. Diese Funktion funktioniert **nur** mit regulären Ausdrücken.

Verzeichnisse ausschließen

Geben Sie maximal 15 reguläre Ausdrücke oder Verzeichnisse an, die von der Synchronisierung ausgeschlossen werden sollen, indem Sie deren Namen oder den vollständigen Verzeichnispfad eingeben und die Eingabetaste drücken. Die Verzeichnisse .copy-offload, .snapshot und ~snapshot sind standardmäßig ausgeschlossen.

Regex oder reguläre Ausdrücke unterscheiden sich von Platzhaltern oder Glob-Ausdrücken. Diese Funktion funktioniert **nur** mit regulären Ausdrücken.

Dateigröße

Wählen Sie, ob alle Dateien unabhängig von ihrer Größe oder nur Dateien in einem bestimmten Größenbereich synchronisiert werden sollen.

Änderungsdatum

Wählen Sie alle Dateien unabhängig vom Datum der letzten Änderung, Dateien, die nach einem bestimmten Datum, vor einem bestimmten Datum oder innerhalb eines bestimmten Zeitraums geändert wurden.

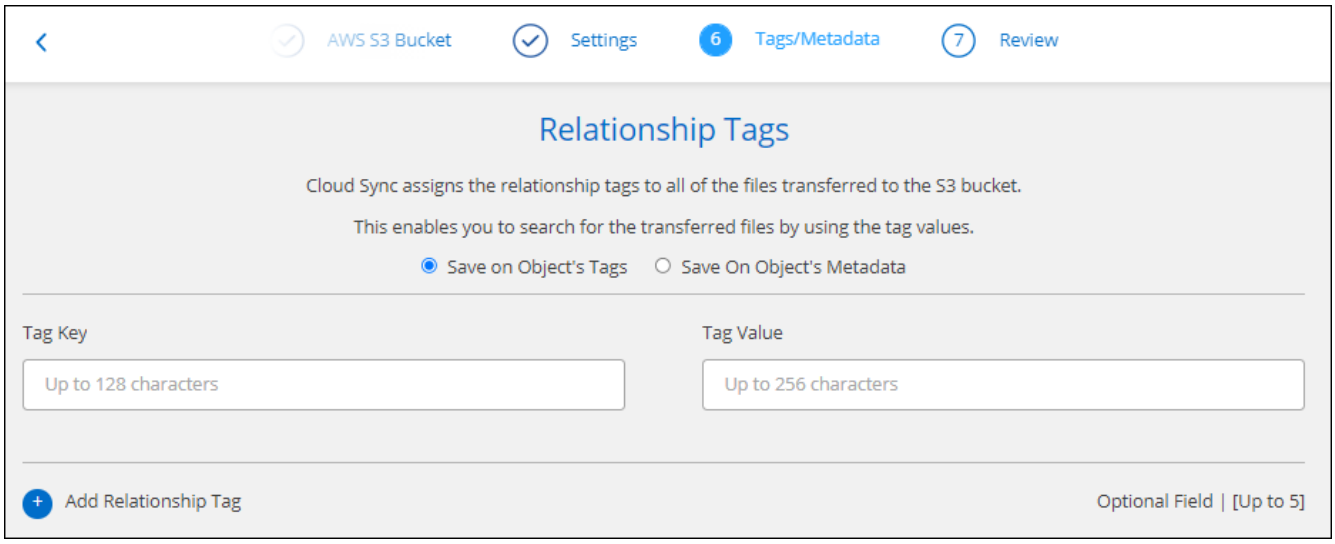
Erstellungsdatum

Wenn ein SMB-Server die Quelle ist, können Sie mit dieser Einstellung Dateien synchronisieren, die nach einem bestimmten Datum, vor einem bestimmten Datum oder innerhalb eines bestimmten Zeitraums erstellt wurden.

ACL – Zugriffskontrollliste

Kopieren Sie nur ACLs, nur Dateien oder ACLs und Dateien von einem SMB-Server, indem Sie beim Erstellen einer Beziehung oder nach dem Erstellen einer Beziehung eine Einstellung aktivieren.

10. Wählen Sie auf der Seite **Tags/Metadaten** aus, ob ein Schlüssel-Wert-Paar als Tag für alle in den S3-Bucket übertragenen Dateien gespeichert oder allen Dateien ein Schlüssel-Wert-Paar für Metadaten zugewiesen werden soll.



Dieselbe Funktion ist beim Synchronisieren von Daten mit StorageGRID und IBM Cloud Object Storage verfügbar. Für Azure und Google Cloud Storage ist nur die Metadatenoption verfügbar.

11. Überprüfen Sie die Details der Synchronisierungsbeziehung und wählen Sie dann **Beziehung erstellen**.

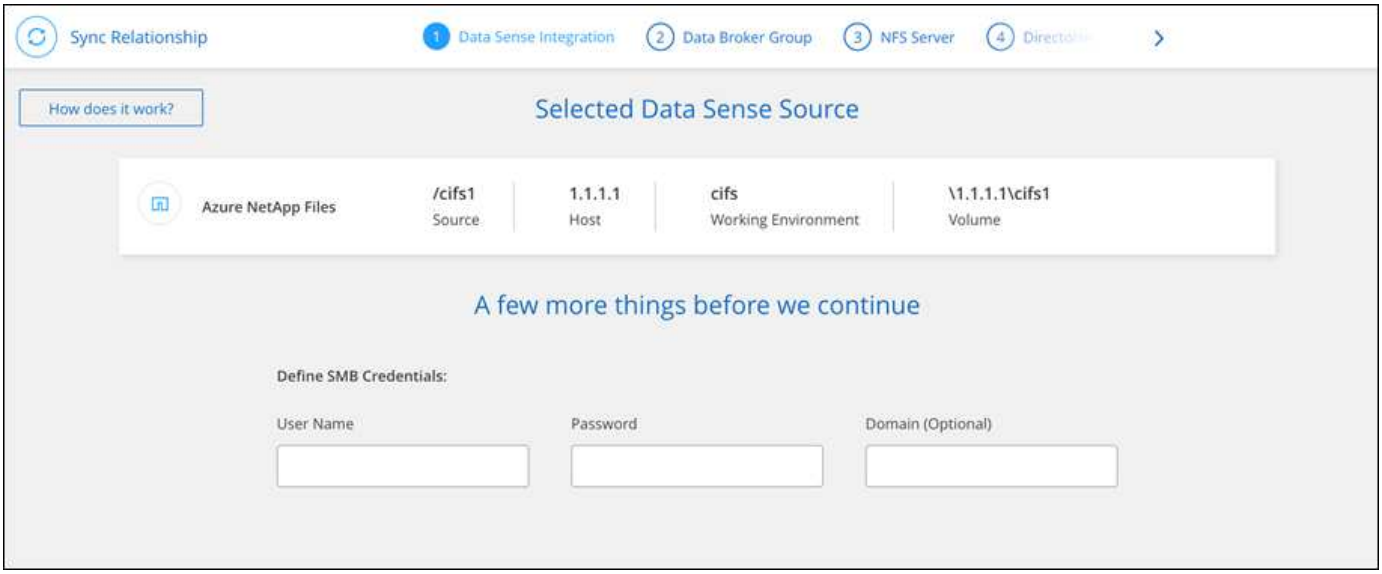
Ergebnis

„Kopieren und Synchronisieren“ startet die Synchronisierung der Daten zwischen Quelle und Ziel. Es stehen Synchronisierungsstatistiken zur Verfügung, die Aufschluss darüber geben, wie lange die Synchronisierung gedauert hat, ob sie angehalten wurde und wie viele Dateien kopiert, gescannt oder gelöscht wurden. Sie können dann Ihre "Synchronisierungsbeziehungen" , "Verwalten Sie Ihre Datenbroker" , oder "Erstellen Sie Berichte zur Optimierung Ihrer Leistung und Konfiguration" .

Erstellen Sie Synchronisierungsbeziehungen aus der NetApp Data Classification

Copy and Sync ist in die NetApp Data Classification integriert. Innerhalb von NetApp Data Classification können Sie die Quelldateien auswählen, die Sie mithilfe von „Kopieren und Synchronisieren“ mit einem Zielspeicherort synchronisieren möchten.

Nachdem Sie eine Datensynchronisierung von NetApp Data Classification initiiert haben, sind alle Quellinformationen in einem einzigen Schritt enthalten und Sie müssen nur einige wichtige Details eingeben. Anschließend wählen Sie den Zielort für die neue Synchronisierungsbeziehung.



"Erfahren Sie, wie Sie eine Synchronisierungsbeziehung von NetApp Data Classification starten" .

Kopieren von ACLs von SMB-Freigaben in NetApp Copy and Sync

NetApp Copy and Sync kann Zugriffskontrolllisten (ACLs) zwischen SMB-Freigaben und zwischen einer SMB-Freigabe und einem Objektspeicher kopieren (außer ONTAP S3). Bei Bedarf haben Sie auch die Möglichkeit, ACLs zwischen SMB-Freigaben manuell mithilfe von Robocopy beizubehalten.

Auswahlmöglichkeiten

- Richten Sie „Kopieren und Synchronisieren“ ein, um ACLs automatisch zu kopieren
- Manuelles Kopieren der ACLs zwischen SMB-Freigaben

Einrichten von „Kopieren und Synchronisieren“ zum Kopieren von ACLs

Kopieren Sie ACLs zwischen SMB-Freigaben und zwischen SMB-Freigaben und Objektspeicher, indem Sie beim Erstellen einer Beziehung oder danach eine Einstellung aktivieren.

Bevor Sie beginnen

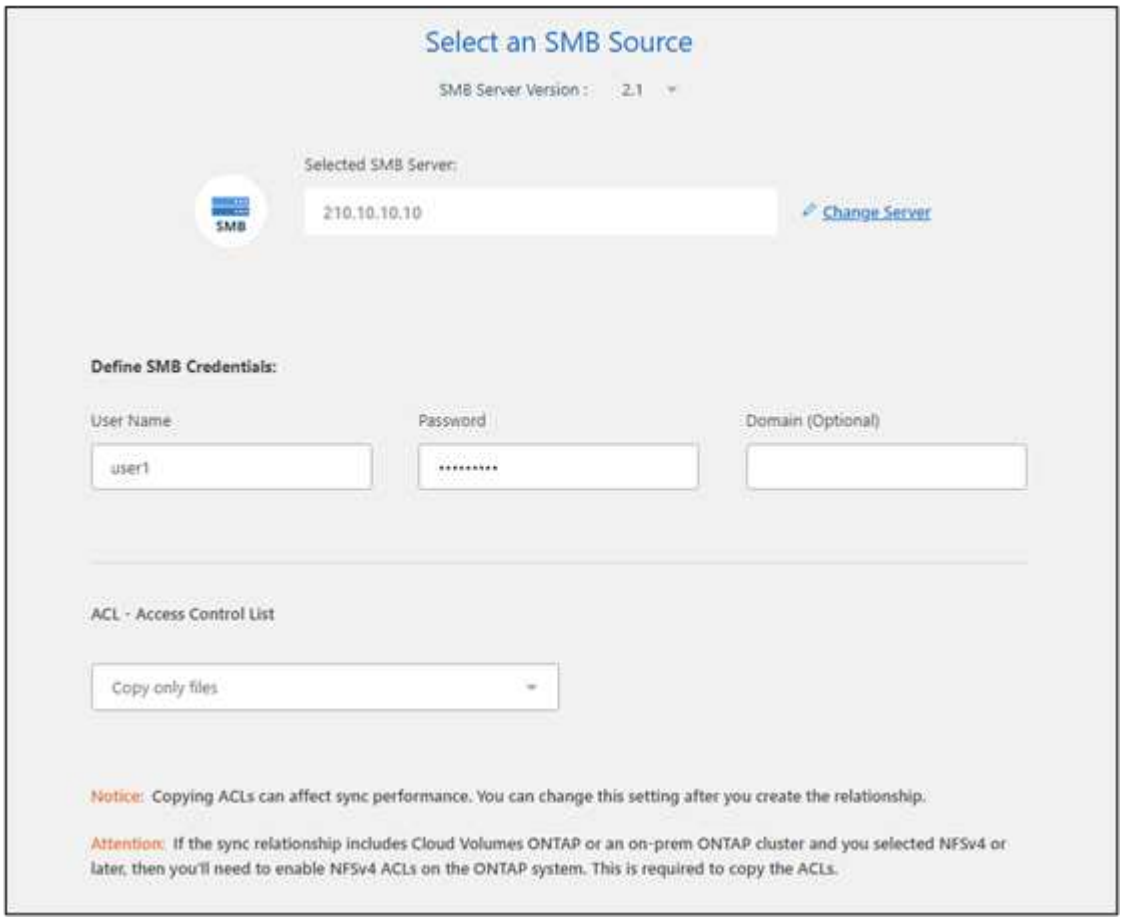
Diese Funktion funktioniert mit *jedem* Datenbrokertyp: AWS, Azure, Google Cloud Platform oder On-Premise-Datenbroker. Der On-Prem-Datenbroker kann ausgeführt werden"jedes unterstützte Betriebssystem" .

Schritte für eine neue Beziehung

1. "Bei Copy and Sync anmelden" .
2. Wählen Sie unter „Kopieren und Synchronisieren“ die Option „Neue Synchronisierung erstellen“ aus.
3. Ziehen Sie per Drag & Drop einen SMB-Server oder Objektspeicher als Quelle und einen SMB-Server oder Objektspeicher als Ziel und wählen Sie **Weiter**.
4. Auf der Seite **SMB-Server**:
   a. Geben Sie einen neuen SMB-Server ein oder wählen Sie einen vorhandenen Server aus und wählen Sie **Weiter**.

b. Geben Sie die Anmeldeinformationen für den SMB-Server ein.

c. Wählen Sie entweder **Nur Dateien kopieren**, **Nur ACL kopieren** oder **Dateien und ACL kopieren** und wählen Sie **Weiter**.



5. Folgen Sie den weiteren Anweisungen, um die Synchronisierungsbeziehung zu erstellen.

   Wenn Sie ACLs von SMB in den Objektspeicher kopieren, können Sie je nach Ziel wählen, ob die ACLs in die Tags des Objekts oder in die Metadaten des Objekts kopiert werden sollen. Für Azure und Google Cloud Storage ist nur die Metadatenoption verfügbar.

   Der folgende Screenshot zeigt ein Beispiel für den Schritt, in dem Sie diese Auswahl treffen können.

Schritte für eine bestehende Beziehung

1. Bewegen Sie den Mauszeiger über die Synchronisierungsbeziehung und wählen Sie das Aktionsmenü aus.
2. Wählen Sie **Einstellungen**.
3. Wählen Sie entweder **Nur Dateien kopieren**, **Nur ACL kopieren** oder **Dateien und ACL kopieren** und wählen Sie **Weiter**.
4. Wählen Sie **Einstellungen speichern**.

> Copy and Sync erhält die SMB-ACLs (Berechtigungen), kopiert aber nicht die Datei- oder Ordnerbesitzverhältnisse. Die Eigentumsverhältnisse werden bei der SMB-ACL-Übertragung nicht berücksichtigt.

Ergebnis

Beim Synchronisieren von Daten behält Copy and Sync die ACLs zwischen Quelle und Ziel bei.

Manuelles Kopieren von ACLs zwischen SMB-Freigaben

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

> Wenn Sie neben den Zugriffskontrolllisten (ACLs) auch die Eigentumsrechte (Besitzer und Gruppe) beibehalten müssen, können Sie Folgendes verwenden: `robocopy` Befehl. Verwendung der `/copyall` Flag-Kopien enthalten ACLs, Eigentümer- und Audit-Informationen.

Schritte

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

   Sie müssen diesen Schritt ausführen, bevor Sie Robocopy verwenden.
3. Erstellen Sie über „Kopieren und Synchronisieren“ eine neue Beziehung zwischen den Quell- und Ziel-SMB-Freigaben oder synchronisieren Sie eine vorhandene Beziehung.
4. Nachdem die Datensynchronisierung abgeschlossen ist, führen Sie den folgenden Befehl vom Windows-Host aus, um die ACLs und den Besitz zu synchronisieren:

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

   Sowohl *source* als auch *target* sollten im UNC-Format angegeben werden. Beispiel: \\<Server>\<Freigabe>\<Pfad>

Synchronisieren Sie NFS-Daten mithilfe der Data-in-Flight-Verschlüsselung in NetApp Copy and Sync

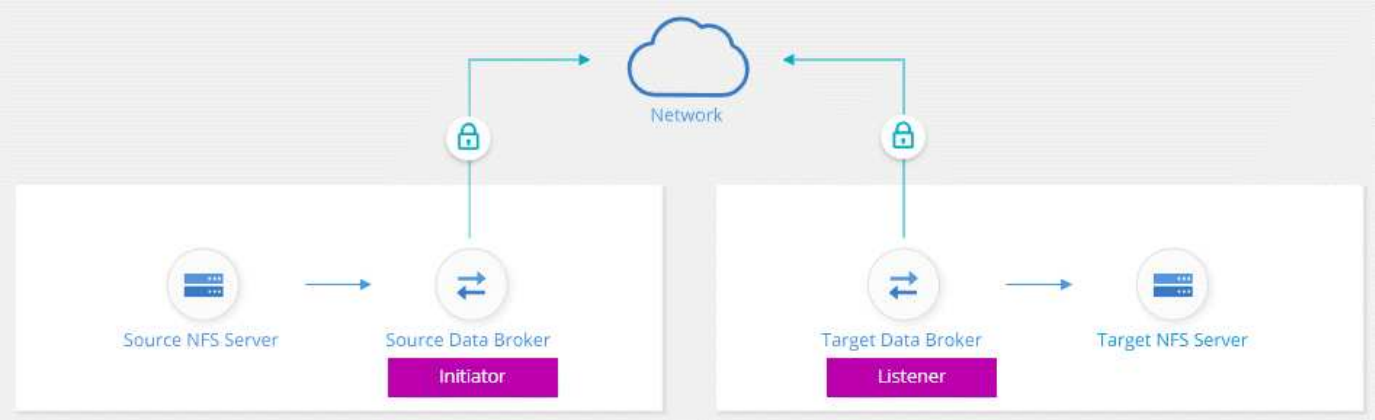
Wenn in Ihrem Unternehmen strenge Sicherheitsrichtlinien gelten, können Sie NFS-

Daten mithilfe der Data-in-Flight-Verschlüsselung in NetApp Copy and Sync synchronisieren. Diese Funktion wird von einem NFS-Server zu einem anderen NFS-Server und von Azure NetApp Files zu Azure NetApp Files unterstützt.

Beispielsweise möchten Sie möglicherweise Daten zwischen zwei NFS-Servern synchronisieren, die sich in unterschiedlichen Netzwerken befinden. Oder Sie müssen möglicherweise Daten auf Azure NetApp Files sicher über Subnetze oder Regionen hinweg übertragen.

So funktioniert die Data-in-Flight-Verschlüsselung

Die Data-in-Flight-Verschlüsselung verschlüsselt NFS-Daten, wenn sie über das Netzwerk zwischen zwei Datenbrokern gesendet werden. Das folgende Bild zeigt eine Beziehung zwischen zwei NFS-Servern und zwei Datenbrokern:



Ein Datenbroker fungiert als *Initiator*. Wenn es Zeit ist, Daten zu synchronisieren, sendet es eine Verbindungsanforderung an den anderen Datenbroker, der der *Listener* ist. Dieser Datenbroker lauscht auf Port 443 auf Anfragen. Sie können bei Bedarf einen anderen Port verwenden, achten Sie jedoch darauf, dass 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 Datenbroker auf die Verbindungsanforderungen wartet und welche diese sendet.

So funktioniert die Verschlüsselung während der Übertragung:

1. Nachdem Sie die Synchronisierungsbeziehung erstellt haben, startet der Initiator eine verschlüsselte Verbindung mit dem anderen Datenbroker.
2. Der Quelldatenbroker verschlüsselt Daten aus der Quelle mit TLS 1.3.
3. Anschließend sendet es die Daten über das Netzwerk an den Zieldatenbroker.
4. Der Zieldatenbroker entschlüsselt die Daten, bevor er sie an das Ziel sendet.
5. Nach der ersten Kopie synchronisiert Copy and Sync alle geänderten Daten alle 24 Stunden. Wenn Daten zu synchronisieren sind, beginnt der Prozess damit, dass der Initiator eine verschlüsselte Verbindung mit dem anderen Datenbroker öffnet.

   Wenn Sie Daten häufiger synchronisieren möchten,"Sie können den Zeitplan ändern, nachdem Sie die Beziehung erstellt haben" .

Unterstützte NFS-Versionen

- Für NFS-Server wird die Data-in-Flight-Verschlüsselung mit den NFS-Versionen 3, 4.0, 4.1 und 4.2 unterstützt.
- Für Azure NetApp Files wird die Data-in-Flight-Verschlüsselung mit den NFS-Versionen 3 und 4.1 unterstützt.

Proxyserver-Beschränkung

Wenn Sie eine verschlüsselte Synchronisierungsbeziehung erstellen, werden die verschlüsselten Daten über HTTPS gesendet und können nicht über einen Proxyserver weitergeleitet werden.

Was Sie für den Einstieg benötigen

Stellen Sie sicher, dass Sie Folgendes haben:

- Zwei NFS-Server, die sich treffen"Quell- und Zielanforderungen" oder Azure NetApp Files in zwei Subnetzen oder Regionen.
- Die IP-Adressen oder vollqualifizierten Domänennamen der Server.
- Netzwerkstandorte für zwei Datenbroker.

  Sie können einen vorhandenen Datenbroker auswählen, dieser muss jedoch als Initiator fungieren. Der Listener-Datenbroker muss ein *neuer* Datenbroker sein.

  Wenn Sie eine vorhandene Datenbrokergruppe verwenden möchten, darf die Gruppe nur einen Datenbroker haben. Mehrere Datenbroker in einer Gruppe werden bei verschlüsselten Synchronisierungsbeziehungen nicht unterstützt.

  Wenn Sie noch keinen Datenbroker bereitgestellt haben, überprüfen Sie die Anforderungen für den Datenbroker. Da Sie strenge Sicherheitsrichtlinien haben, sollten Sie unbedingt die Netzwerkanforderungen überprüfen, die den ausgehenden Datenverkehr von Port 443 und die"Internet-Endpunkte" die der Datenbroker kontaktiert.

  - "Überprüfen der AWS-Installation"
  - "Überprüfen der Azure-Installation"
  - "Überprüfen Sie die Google Cloud-Installation"
  - "Überprüfen der Linux-Hostinstallation"

Synchronisieren Sie NFS-Daten mithilfe der Data-in-Flight-Verschlüsselung

Erstellen Sie eine neue Synchronisierungsbeziehung zwischen zwei NFS-Servern oder zwischen Azure NetApp Files, aktivieren Sie die Option zur In-Flight-Verschlüsselung und folgen Sie den Anweisungen.

Schritte

1. "Bei Copy and Sync anmelden" .
2. Wählen Sie **Neue Synchronisierung erstellen**.
3. Ziehen Sie **NFS-Server** per Drag & Drop an die Quell- und Zielspeicherorte oder * Azure NetApp Files* an die Quell- und Zielspeicherorte und wählen Sie **Ja**, um die Data-in-Flight-Verschlüsselung zu aktivieren.
4. 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 vorhandenen Server aus.

b. **Funktionalität des Datenbrokers definieren**: Definieren Sie, welcher Datenbroker auf Verbindungsanfragen an einem Port *lauscht* und welcher die Verbindung *initiiert*. Treffen Sie Ihre Wahl basierend auf Ihren Netzwerkanforderungen.

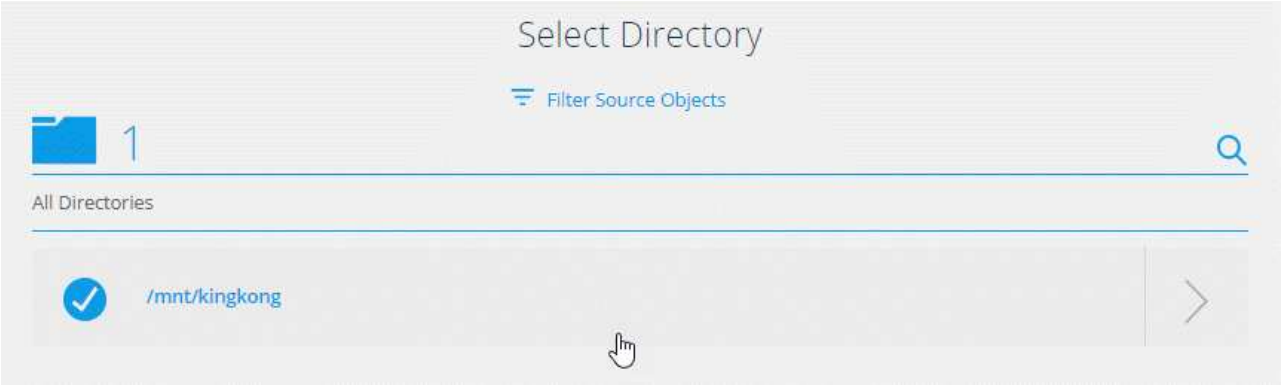
c. **Datenbroker**: Folgen Sie den Anweisungen, um einen neuen Quelldatenbroker hinzuzufügen, oder wählen Sie einen vorhandenen Datenbroker aus.

   Beachten Sie Folgendes:

   - Wenn Sie eine vorhandene Datenbrokergruppe verwenden möchten, darf die Gruppe nur einen Datenbroker haben. Mehrere Datenbroker in einer Gruppe werden bei verschlüsselten Synchronisierungsbeziehungen nicht unterstützt.
   - Wenn der Quelldatenbroker als Listener fungiert, muss es sich um einen neuen Datenbroker handeln.
   - Wenn Sie einen neuen Datenbroker benötigen, werden Sie von Copy and Sync mit den Installationsanweisungen aufgefordert. Sie können den Datenbroker in der Cloud bereitstellen oder ein Installationsskript für Ihren eigenen Linux-Host herunterladen.

d. **Verzeichnisse**: Wählen Sie die Verzeichnisse aus, die Sie synchronisieren möchten, indem Sie alle Verzeichnisse auswählen oder indem Sie einen Drilldown durchführen und ein Unterverzeichnis auswählen.

   Wählen Sie **Quellobjekte filtern**, um Einstellungen zu ändern, die definieren, wie Quelldateien und -ordner synchronisiert und am Zielspeicherort verwaltet werden.

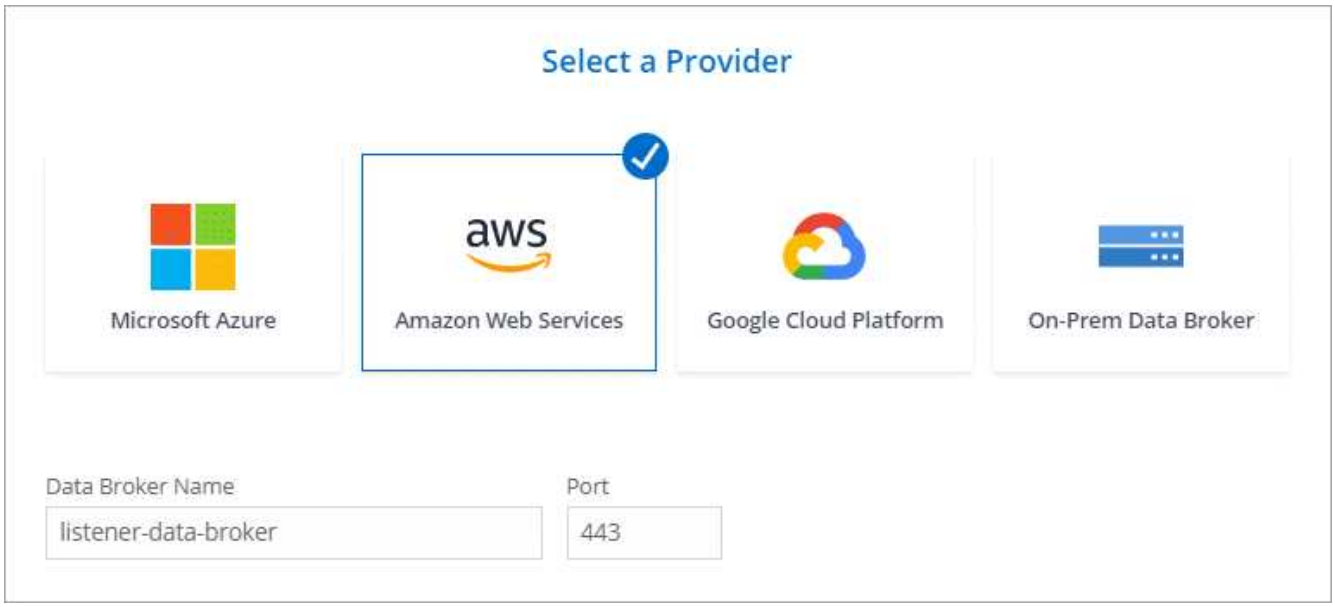


e. **Ziel-NFS-Server/Ziel Azure NetApp Files**: Wählen Sie die NFS-Version und geben Sie dann ein neues NFS-Ziel ein oder wählen Sie einen vorhandenen Server aus.

f. **Zieldatenbroker**: Folgen Sie den Anweisungen, um einen neuen Quelldatenbroker hinzuzufügen, oder wählen Sie einen vorhandenen Datenbroker aus.

   Wenn der Zieldatenbroker als Listener fungiert, muss es sich um einen neuen Datenbroker handeln.

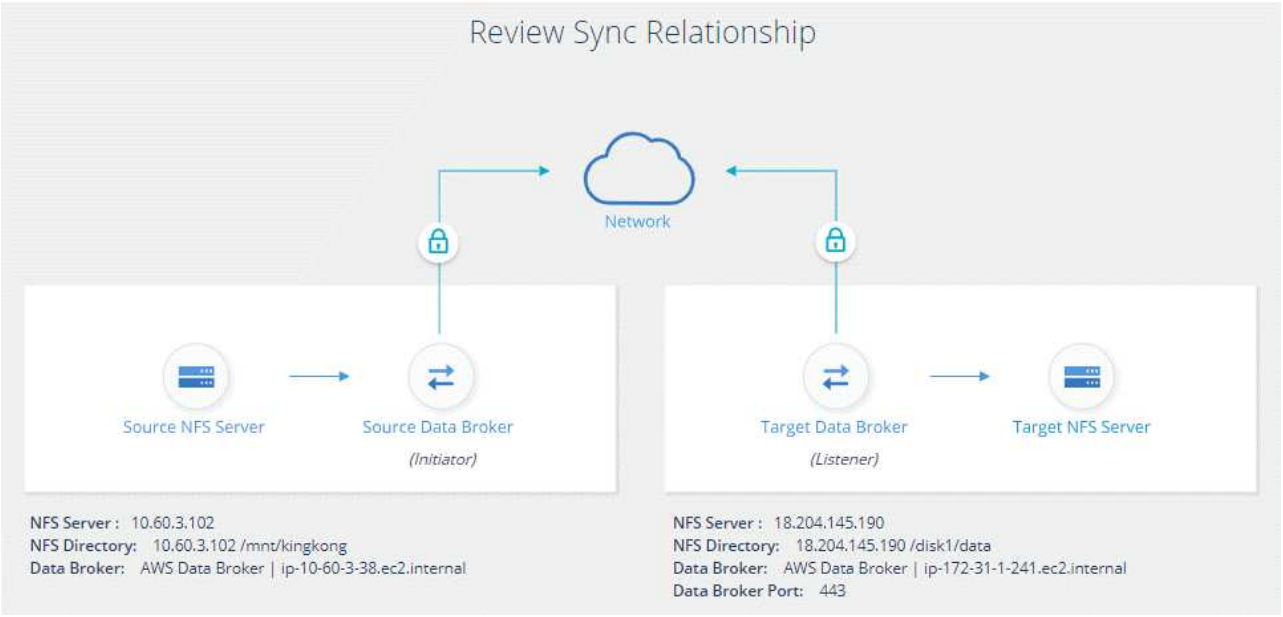
   Hier ist ein Beispiel für die Eingabeaufforderung, wenn der Zieldatenbroker als Listener fungiert. Beachten Sie die Option zur Angabe des Ports.



a. **Zielverzeichnisse**: Wählen Sie ein Verzeichnis der obersten Ebene aus oder navigieren Sie zu einem vorhandenen Unterverzeichnis oder erstellen Sie einen neuen Ordner innerhalb eines Exports.

b. **Einstellungen**: Definieren Sie, wie Quelldateien und -ordner am Zielspeicherort synchronisiert und verwaltet werden.

c. **Überprüfen**: Überprüfen Sie die Details der Synchronisierungsbeziehung und wählen Sie dann **Beziehung erstellen**.



Ergebnis

„Kopieren und Synchronisieren“ beginnt mit der Erstellung der neuen Synchronisierungsbeziehung. Wenn Sie fertig sind, wählen Sie **Im Dashboard anzeigen**, um Details zur neuen Beziehung anzuzeigen.

Richten Sie eine Datenbrokergruppe ein, um einen externen HashiCorp Vault in NetApp Copy and Sync zu verwenden

Wenn Sie eine Synchronisierungsbeziehung erstellen, die Amazon S3-, Azure- oder Google Cloud-Anmeldeinformationen erfordert, müssen Sie diese Anmeldeinformationen über die NetApp Copy and Sync -Benutzeroberfläche oder API angeben. Eine Alternative besteht darin, die Datenbrokergruppe so einzurichten, dass sie direkt von einem externen HashiCorp-Tresor auf die Anmeldeinformationen (oder *Geheimnisse*) zugreift.

Diese Funktion wird durch die Copy and Sync-API mit Synchronisierungsbeziehungen unterstützt, die Amazon S3-, Azure- oder Google Cloud-Anmeldeinformationen erfordern.

1 Bereiten Sie den Tresor vor

Bereiten Sie den Tresor vor, um der Datenbrokergruppe Anmeldeinformationen bereitzustellen, indem Sie die URLs einrichten. Die URLs zu den Geheimnissen im Tresor müssen mit *Creds* enden.

2 Vorbereiten der Datenbrokergruppe

Bereiten Sie die Datenbrokergruppe darauf vor, Anmeldeinformationen aus dem externen Tresor abzurufen, indem Sie die lokale Konfigurationsdatei für jeden Datenbroker in der Gruppe ändern.

3 Erstellen einer Synchronisierungsbeziehung mithilfe der API

Nachdem nun alles eingerichtet ist, können Sie einen API-Aufruf senden, um eine Synchronisierungsbeziehung zu erstellen, die Ihren Tresor zum Abrufen der Geheimnisse verwendet.

Bereiten Sie den Tresor vor

Sie müssen Copy and Sync die URL zu den Geheimnissen in Ihrem Tresor bereitstellen. Bereiten Sie den Tresor vor, indem Sie diese URLs einrichten. Sie müssen URLs zu den Anmeldeinformationen für jede Quelle und jedes Ziel in den Synchronisierungsbeziehungen einrichten, die Sie erstellen möchten.

Die URL muss wie folgt aufgebaut sein:

```
/<path>/<requestid>/<endpoint-protocol>Creds
```

Weg
: Der Präfixpfad zum Geheimnis. Dies kann jeder für Sie eindeutige Wert sein.

Anforderungs-ID
: Eine Anforderungs-ID, die Sie generieren müssen. Sie müssen die ID in einem der Header in der API-POST-Anforderung angeben, wenn Sie die Synchronisierungsbeziehung erstellen.

Endpunktprotokoll
: Eines der folgenden Protokolle, wie definiert "in der Post-Relationship-V2-Dokumentation" : S3, AZURE oder GCP (jeweils in Großbuchstaben).

Credits

Die URL muss mit *Creds* enden.

Beispiele

Die folgenden Beispiele zeigen URLs zu Geheimnissen.

Beispiel für die vollständige URL und den Pfad für Quellanmeldeinformationen

http://example.vault.com:8200/my-path/all-secrets/hb312vdasr2/S3Creds

Wie Sie im Beispiel sehen können, lautet der Präfixpfad */my-path/all-secrets/*, die Anforderungs-ID ist *hb312vdasr2* und der Quellendpunkt ist S3.

Beispiel für die vollständige URL und den Pfad für Zielanmeldeinformationen

http://example.vault.com:8200/my-path/all-secrets/n32hcbnejk2/AZURECreds

Der Präfixpfad ist */my-path/all-secrets/*, die Anforderungs-ID ist *n32hcbnejk2* und der Zielendpunkt ist Azure.

Vorbereiten der Datenbrokergruppe

Bereiten Sie die Datenbrokergruppe darauf vor, Anmeldeinformationen aus dem externen Tresor abzurufen, indem Sie die lokale Konfigurationsdatei für jeden Datenbroker in der Gruppe ändern.

Schritte

1. Stellen Sie eine SSH-Verbindung zu einem Datenbroker in der Gruppe her.
2. Bearbeiten Sie die Datei local.json, die sich in /opt/netapp/databroker/config befindet.
3. Setzen Sie „enable“ auf **true** und legen Sie die Konfigurationsparameterfelder unter *external-integrations.hashicorp* wie folgt fest:

   ermöglicht
   - Gültige Werte: true/false
   - Typ: Boolean
   - Standardwert: false
   - Richtig: Der Datenbroker erhält Geheimnisse aus Ihrem eigenen externen HashiCorp Vault
   - Falsch: Der Datenbroker speichert Anmeldeinformationen in seinem lokalen Tresor

   URL
   - Typ: Zeichenfolge
   - Wert: Die URL zu Ihrem externen Tresor

   Weg
   - Typ: Zeichenfolge
   - Wert: Präfixieren Sie den Pfad zum Geheimnis mit Ihren Anmeldeinformationen

   Ablehnen – nicht autorisiert
   - Legt fest, ob der Datenbroker nicht autorisierte externe Tresore ablehnen soll
   - Typ: Boolean

- Standard: false

Authentifizierungsmethode

- Die Authentifizierungsmethode, die der Datenbroker für den Zugriff auf Anmeldeinformationen aus dem externen Tresor verwenden soll
- Typ: Zeichenfolge
- Gültige Werte: „aws-iam“ / „role-app“ / „gcp-iam“

Rollenname

- Typ: Zeichenfolge
- Ihr Rollenname (falls Sie aws-iam oder gcp-iam verwenden)

Geheim-ID und Root-ID

- Typ: Zeichenfolge (falls Sie die App-Rolle verwenden)

Namensraum

- Typ: Zeichenfolge
- Ihr Namespace (X-Vault-Namespace-Header, falls erforderlich)

4. Wiederholen Sie diese Schritte für alle anderen Datenbroker in der Gruppe.

Beispiel für die AWS-Rollenauthentifizierung

```
{
        "external-integrations": {
                "hashicorp": {
                        "enabled": true,
                        "url": "https://example.vault.com:8200",
                        "path": ""my-path/all-secrets",
                        "reject-unauthorized": false,
                        "auth-method": "aws-role",
                        "aws-role": {
                                "role-name": "my-role"
                        }
                }
        }
}
```

Beispiel für die GCP-IAM-Authentifizierung

```
{
"external-integrations": {
    "hashicorp": {
      "enabled": true,
      "url": http://ip-10-20-30-55.ec2.internal:8200,
      "path": "v1/secret",
      "namespace": "",
      "reject-unauthorized": true,
      "auth-method": "gcp-iam",
      "aws-iam": {
        "role-name": ""
      },
      "app-role": {
        "root_id": "",
        "secret_id": ""
      },
"gcp-iam": {
          "role-name": "my-iam-role"
      }
    }
  }
}
```

Richten Sie Berechtigungen ein, wenn Sie die GCP-IAM-Authentifizierung verwenden

Wenn Sie die Authentifizierungsmethode *gcp-iam* verwenden, muss der Datenbroker über die folgende GCP-Berechtigung verfügen:

```
- iam.serviceAccounts.signJwt
```

"Erfahren Sie mehr über die GCP-Berechtigungsanforderungen für den Datenbroker" .

Erstellen einer neuen Synchronisierungsbeziehung mithilfe von Geheimnissen aus dem Tresor

Nachdem nun alles eingerichtet ist, können Sie einen API-Aufruf senden, um eine Synchronisierungsbeziehung zu erstellen, die Ihren Tresor zum Abrufen der Geheimnisse verwendet.

Veröffentlichen Sie die Beziehung mithilfe der Copy and Sync REST-API.

```
Headers:
Authorization: Bearer <user-token>
Content-Type: application/json
x-account-id: <accountid>
x-netapp-external-request-id-src: request ID as part of path for source
credentials
x-netapp-external-request-id-trg: request ID as part of path for target
credentials
Body: post relationship v2 body
```

- Um ein Benutzertoken und Ihre NetApp Console -Konto-ID zu erhalten,"siehe diese Seite in der Dokumentation" .
- Um einen Körper für Ihre Post-Beziehung aufzubauen, "siehe den API-Aufruf „relationships-v2“" .

Beispiel

Beispiel für die POST-Anfrage:

```
url: https://api.cloudsync.netapp.com/api/relationships-v2
headers:
"x-account-id": "CS-SasdW"
"x-netapp-external-request-id-src": "hb312vdasr2"
"Content-Type": "application/json"
"Authorization": "Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik…"
Body:
{
"dataBrokerId": "5e6e111d578dtyuu1555sa60",
"source": {
        "protocol": "s3",
        "s3": {
                "provider": "sgws",
                "host": "1.1.1.1",
                "port": "443",
                "bucket": "my-source"
     },
"target": {
        "protocol": "s3",
        "s3": {
                "bucket": "my-target-bucket"
        }
    }
}
```