



Daten zwischen Quelle und Ziel synchronisieren

Cloud Sync

NetApp
December 16, 2022

Inhaltsverzeichnis

- Daten zwischen Quelle und Ziel synchronisieren 1
 - Erstellung von Synchronisierungsbeziehungen 1
 - Kopieren von ACLs aus SMB-Freigaben 9
 - Synchronisierung von NFS-Daten mithilfe von Verschlüsselung bei der Übertragung 11
 - Einrichtung einer Datenvermittler-Gruppe zur Verwendung eines externen HashiCorp Vault 15

Daten zwischen Quelle und Ziel synchronisieren

Erstellung von Synchronisierungsbeziehungen

Wenn Sie eine Synchronisierungsbeziehung erstellen, kopiert der Cloud Sync-Dienst Dateien von der Quelle zum Ziel. Nach der ersten Kopie synchronisiert der Service alle 24 Stunden alle geänderten Daten.

Bevor Sie einige Arten von Synchronisierungsbeziehungen erstellen können, müssen Sie zunächst eine Arbeitsumgebung in BlueXP erstellen.

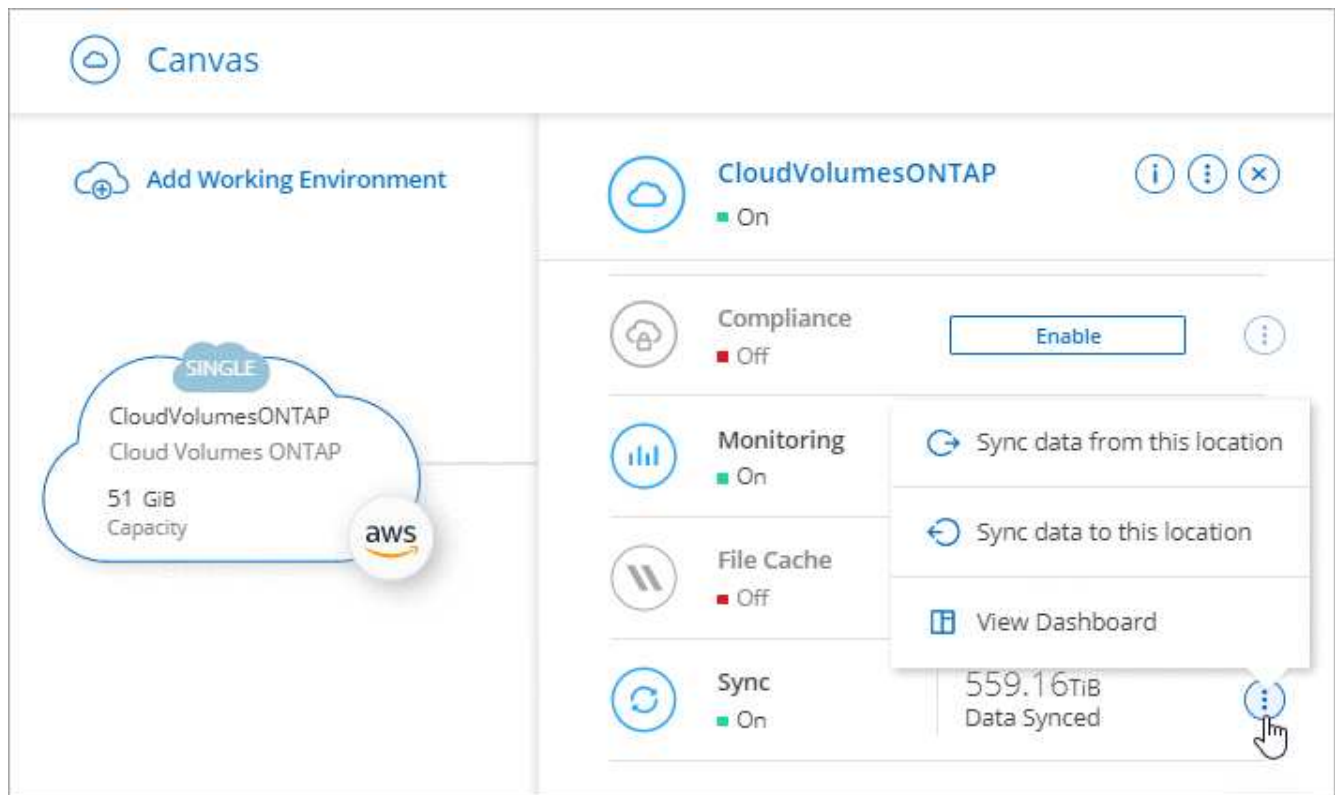
Erstellen von Synchronisierungsbeziehungen für bestimmte Arbeitsumgebungen

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

- Amazon FSX für ONTAP
- Azure NetApp Dateien
- Cloud Volumes ONTAP
- ONTAP-Cluster vor Ort

Schritte

1. Schaffen oder ermitteln Sie die Arbeitsumgebung.
 - ["Amazon FSX für ONTAP-Arbeitsumgebungen erstellen"](#)
 - ["Einrichtung und Erkennung von Azure NetApp Files"](#)
 - ["Starten von Cloud Volumes ONTAP in AWS"](#)
 - ["Starten von Cloud Volumes ONTAP in Azure"](#)
 - ["Cloud Volumes ONTAP in Google Cloud wird gestartet"](#)
 - ["Hinzufügen vorhandener Cloud Volumes ONTAP Systeme"](#)
 - ["Erkennung von ONTAP Clustern"](#)
2. Klicken Sie Auf **Leinwand**.
3. Wählen Sie eine Arbeitsumgebung aus, die einem der oben aufgeführten Typen entspricht.
4. Wählen Sie das Aktionsmenü neben Synchronisieren.



5. Wählen Sie **Daten von diesem Standort** oder **Daten zu diesem Standort synchronisieren** und folgen Sie den Anweisungen, um die Synchronisierungsbeziehung einzurichten.

Erstellung anderer Arten von Synchronisierungsbeziehungen

Verwenden Sie diese Schritte, um Daten zu einem anderen unterstützten Storage-Typ als Amazon FSX für ONTAP, Azure NetApp Files, Cloud Volumes ONTAP oder On-Premises-ONTAP-Cluster zu synchronisieren. Die folgenden Schritte zeigen ein Beispiel, wie eine Synchronisierungsbeziehung von einem NFS-Server zu einem S3-Bucket eingerichtet wird.

1. Klicken Sie in BlueXP auf **Sync**.
2. Wählen Sie auf der Seite * Synchronisierungsbeziehung definieren* eine Quelle und ein Ziel aus.

Die folgenden Schritte zeigen ein Beispiel für das Erstellen einer Synchronisierungsbeziehung von einem NFS-Server zu einem S3-Bucket.



3. Geben Sie auf der Seite **NFS Server** die IP-Adresse oder den vollqualifizierten Domännennamen des NFS-Servers ein, den Sie mit AWS synchronisieren möchten.
4. Folgen Sie auf der Seite **Data Broker Group** den Aufforderungen zur Erstellung einer virtuellen Maschine für den Datenvermittler in AWS, Azure oder Google Cloud Platform oder zur Installation der Datenvermittler-Software auf einem vorhandenen Linux-Host.

Weitere Informationen finden Sie auf den folgenden Seiten:

- ["Erstellen eines Daten-Brokers in AWS"](#)
- ["Erstellen eines Daten-Brokers in Azure"](#)
- ["Erstellen Sie in Google Cloud einen Daten-Broker"](#)
- ["Installation des Data Brokers auf einem Linux-Host"](#)

5. Klicken Sie nach der Installation des Datenmaklers auf **Weiter**.



6. Wählen Sie auf der Seite **Directories** ein Verzeichnis oder Unterverzeichnis auf oberster Ebene aus.

Wenn Cloud Sync die Exporte nicht abrufen kann, klicken Sie auf **Export manuell hinzufügen** und geben Sie den Namen eines NFS-Exports ein.



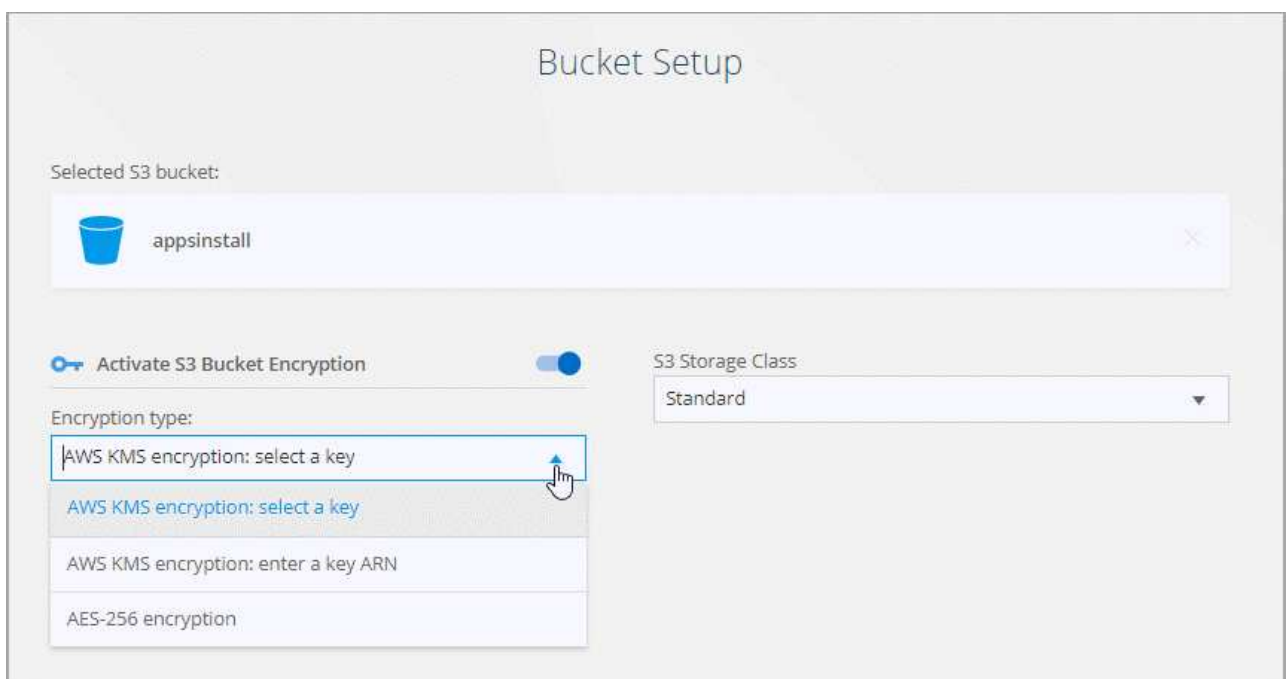
Wenn Sie mehr als ein Verzeichnis auf dem NFS-Server synchronisieren möchten, müssen Sie nach Abschluss der Synchronisierung weitere Synchronisierungsbeziehungen erstellen.

7. Wählen Sie auf der Seite **AWS S3 Bucket** einen Bucket aus:

- Drill-down zum Auswählen eines vorhandenen Ordners innerhalb des Buckets oder zum Auswählen eines neuen Ordners, den Sie innerhalb des Buckets erstellen.
- Klicken Sie auf **zur Liste hinzufügen**, um einen S3-Bucket auszuwählen, der nicht mit Ihrem AWS-Konto verknüpft ist. ["Spezifische Berechtigungen müssen auf den S3-Bucket angewendet werden"](#).

8. Richten Sie auf der Seite **Bucket Setup** den Bucket ein:

- Legen Sie fest, ob die S3-Bucket-Verschlüsselung aktiviert und dann einen AWS KMS-Schlüssel ausgewählt werden soll, den ARN eines KMS-Schlüssels eingeben oder die AES-256-Verschlüsselung auswählen soll.
- Wählen Sie eine S3-Storage-Klasse aus. ["Zeigen Sie die unterstützten Speicherklassen an"](#).



9. legen Sie auf der Seite **Settings** fest, wie Quelldateien und Ordner synchronisiert und am Zielspeicherort verwaltet werden:

Zeitplan

Wählen Sie einen wiederkehrenden Zeitplan für zukünftige Synchronisierungen aus oder deaktivieren Sie den Synchronisationsplan. Sie können eine Beziehung planen, um Daten bis zu alle 1 Minute zu synchronisieren.

Sync Timeout

Legen Sie fest, ob Cloud Sync eine Datensynchronisation abbrechen soll, wenn die Synchronisierung in der angegebenen Anzahl an Stunden oder Tagen nicht abgeschlossen ist.

Benachrichtigungen

Ermöglicht Ihnen die Auswahl, ob Sie Cloud Sync Benachrichtigungen im Benachrichtigungscenter von BlueXP erhalten möchten. Benachrichtigungen für erfolgreiche Datensynchronisation, fehlerhafte Datensynchronisation und stornierte Datensynchronisierungen sind möglich.

Wiederholungen

Legen Sie fest, wie oft Cloud Sync versuchen soll, eine Datei zu synchronisieren, bevor Sie sie überspringen.

Kontinuierliche Synchronisierung

Nach der ersten Datensynchronisierung überwacht Cloud Sync Änderungen am S3-Quell-Bucket oder Google Cloud Storage Bucket und synchronisiert kontinuierlich alle Änderungen am Zielspeicherort. Es ist nicht erforderlich, die Quelle in geplanten Intervallen erneut zu scannen.

Diese Einstellung ist nur verfügbar, wenn eine Synchronisierungsbeziehung erstellt wird und wenn Daten von einem S3-Bucket oder Google Cloud Storage zu Azure Blob Storage, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS, S3, Und StorageGRID * oder* von Azure Blob Storage auf Azure Blob Storage, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS und StorageGRID.

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

- Der Synchronisierungszeitplan ist deaktiviert.
- Die folgenden Einstellungen werden auf die Standardwerte zurückgesetzt: Sync Timeout, kürzlich geänderte Dateien und Änderungsdatum.
- Wenn S3 die Quelle ist, ist der Filter nach Größe nur für kopierende Ereignisse aktiv (nicht bei Löschereignissen).
- Nachdem die Beziehung erstellt wurde, können Sie die Beziehung nur beschleunigen oder löschen. Sie können die Synchronisierung nicht abbrechen, Einstellungen ändern oder Berichte anzeigen.

Vergleich Von

Wählen Sie aus, ob Cloud Sync bestimmte Attribute vergleichen soll, wenn Sie feststellen, ob sich eine Datei oder ein Verzeichnis geändert hat und erneut synchronisiert werden soll.

Selbst wenn Sie diese Attribute deaktivieren, vergleicht Cloud Sync die Quelle immer noch mit dem Ziel, indem es die Pfade, Dateigrößen und Dateinamen überprüft. Falls Änderungen vorliegen, werden diese Dateien und Verzeichnisse synchronisiert.

Sie können festlegen, dass Cloud Sync aktiviert oder deaktiviert wird, indem Sie die folgenden Attribute vergleichen:

- **Mtime:** Die letzte geänderte Zeit für eine Datei. Dieses Attribut ist für Verzeichnisse nicht gültig.
- **Uid, gid und Mode:** Berechtigungsflaggen für Linux.

Für Objekte kopieren

Aktivieren Sie diese Option zum Kopieren von Objekt-Storage-Metadaten und -Tags. Wenn ein Benutzer die Metadaten an der Quelle ändert, kopiert Cloud Sync dieses Objekt im nächsten Sync. Wenn ein Benutzer jedoch die Tags auf der Quelle ändert (und nicht die Daten selbst), kopiert Cloud Sync das Objekt nicht im nächsten Sync.

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

Das Kopieren von Tags wird in Synchronisierungsbeziehungen unterstützt, einschließlich Azure Blob oder einem S3-kompatiblen Endpunkt (S3, StorageGRID oder IBM Cloud Objekt-Storage) als Ziel.

Das Kopieren von Metadaten wird durch „Cloud-to-Cloud“-Beziehungen zwischen folgenden Endpunkten unterstützt:

- AWS S3
- Azure Blob
- Google Cloud Storage
- IBM Cloud Objekt-Storage
- StorageGRID

Kürzlich geänderte Dateien

Wählen Sie diese Option aus, um Dateien auszuschließen, die vor der geplanten Synchronisierung zuletzt geändert wurden.

Dateien auf Quelle löschen

Wählen Sie diese Option aus, um Dateien vom Quellspeicherort zu löschen, nachdem Cloud Sync die Dateien auf den Zielspeicherort kopiert hat. Diese Option schließt das Risiko eines Datenverlusts ein, da die Quelldateien nach dem Kopieren gelöscht werden.

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

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

Dateien auf Ziel löschen

Wählen Sie diese Option aus, um Dateien vom Zielspeicherort zu löschen, wenn sie aus der Quelle gelöscht wurden. Standardmäßig werden keine Dateien vom Zielspeicherort gelöscht.

Dateitypen

Definieren Sie die Dateitypen, die in jede Synchronisierung einbezogen werden sollen: Dateien, Verzeichnisse und symbolische Links.

Dateierweiterungen ausschließen

Geben Sie Dateierweiterungen an, die vom Sync ausgeschlossen werden sollen, indem Sie die Dateierweiterung eingeben und **Enter** drücken. Geben Sie beispielsweise *log* oder *.log* ein, um *.log-Dateien auszuschließen. Für mehrere Erweiterungen ist kein Trennzeichen erforderlich. Das folgende Video enthält eine kurze Demo:

► https://docs.netapp.com/de-de/cloud-manager-sync//media/video_file_extensions.mp4 (video)

Verzeichnisnamen Ausschließen

Geben Sie maximal 15 Verzeichnisse an, die von der Synchronisierung ausgeschlossen werden sollen, indem Sie ihren Namen eingeben und **Enter** drücken. Die Verzeichnisse .Copy-Offload, .Snapshot, ~Snapshot sind standardmäßig ausgeschlossen. Wenn Sie diese in Ihre Synchronisierung aufnehmen möchten, kontaktieren Sie uns.

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 letzten Änderungsdatum aus, Dateien, die nach einem bestimmten Datum, vor einem bestimmten Datum oder zwischen einem bestimmten Zeitraum 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 zwischen einem bestimmten Zeitraum erstellt wurden.

ACL – Access Control List

Kopieren Sie ACLs von einem SMB-Server, indem Sie eine Einstellung aktivieren, wenn Sie eine Beziehung erstellen oder nachdem Sie eine Beziehung erstellt haben.

10. Wählen Sie auf der Seite **Tags/Metadaten**, ob ein Key-Value-Paar als Tag auf allen Dateien gespeichert werden soll, die auf den S3-Bucket übertragen werden, oder um ein Metadaten-Key-Value-Paar auf allen Dateien zuzuweisen.

<
AWS S3 Bucket
Settings
6 Tags/Metadata
7 Review

Relationship Tags

Cloud Sync assigns the relationship tags to all of the files transferred to the S3 bucket.

This enables you to search for the transferred files by using the tag values.

☒ Save on Object's Tags
☐ Save On Object's Metadata

Tag Key
Up to 128 characters

Tag Value
Up to 256 characters

+ Add Relationship Tag
Optional Field | [Up to 5]



Diese Funktion ist auch zur Synchronisierung 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 klicken Sie dann auf **Beziehung erstellen**.

Ergebnis

Cloud Sync beginnt mit der Synchronisierung von Daten zwischen Quelle und Ziel.

Synchronisierungsbeziehungen aus Cloud-Daten Sense erstellen

Cloud Sync ist in Cloud Data Sense integriert. Aus Data Sense können Sie die Quelldateien auswählen, die Sie mit Cloud Sync an einem Zielspeicherort synchronisieren möchten.

Nachdem Sie eine Datensynchronisierung aus Cloud Data Sense initiiert haben, sind alle Quellinformationen in einem einzigen Schritt enthalten und müssen nur einige wichtige Details eingeben. Anschließend wählen Sie den Zielspeicherort für die neue Synchronisierungsbeziehung aus.

Sync Relationship
1 Data Sense Integration
2 Data Broker Group
3 NFS Server
4 Directories
>

How does it work?

Selected Data Sense Source

Azure NetApp Files
/cifs1 Source
1.1.1.1 Host
cifs Working Environment
\\1.1.1.1\cifs1 Volume

A few more things before we continue

Define SMB Credentials:

User Name
Password
Domain (Optional)

["Starten Sie eine Synchronisierungsbeziehung mit Cloud Data Sense"](#).

Kopieren von ACLs aus SMB-Freigaben

Cloud Sync kann Zugriffssteuerungslisten (ACLs) zwischen SMB-Freigaben und zwischen SMB-Freigaben und Objekt-Storage kopieren (außer ONTAP S3). Bei Bedarf haben Sie auch die Möglichkeit, ACLs mithilfe von robocopy manuell zwischen SMB-Freigaben beizubehalten.

Wahlmöglichkeiten

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

Einrichten von Cloud Sync zum Kopieren von ACLs

Kopieren Sie ACLs zwischen SMB-Freigaben und zwischen SMB-Freigaben und Objekt-Storage. Aktivieren Sie dazu eine Einstellung beim Erstellen einer Beziehung oder nach dem Erstellen einer Beziehung.

Was Sie benötigen

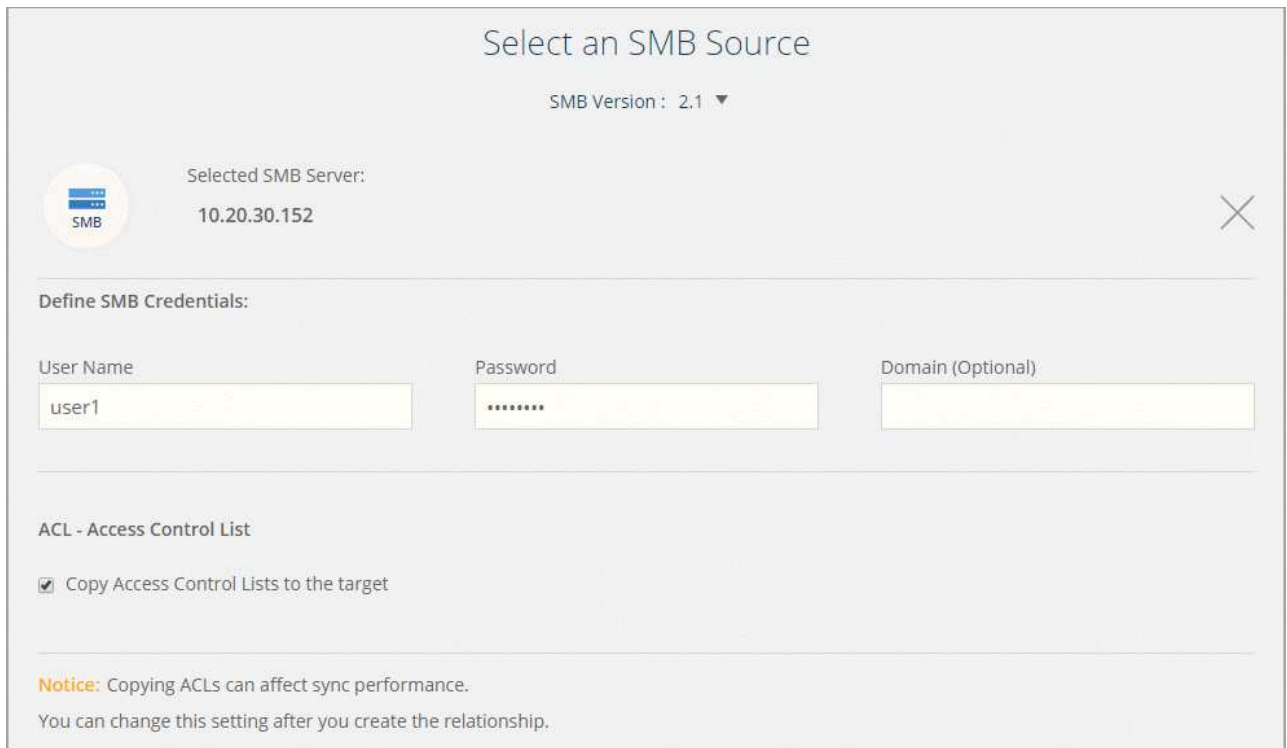
Diese Funktion arbeitet mit jedem Datentyp Broker zusammen – AWS, Azure, Google Cloud Platform oder On-Premises-Daten-Broker. Der On-Premises-Daten-Broker kann ausgeführt werden ["Alle unterstützten Betriebssysteme"](#).

Schritte für eine neue Beziehung

1. Klicken Sie in Cloud Sync auf **Neuen Sync erstellen**.
2. Ziehen Sie einen SMB-Server oder Objekt-Storage als Quelle und einen SMB-Server oder Objekt-Storage als 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	Password	Domain (Optional)
<input type="text" value="user1"/>	<input type="password" value="*****"/>	<input type="text"/>

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.

Wenn Sie ACLs zwischen SMB und Objekt-Storage kopieren, können Sie je nach Ziel die ACLs in die Tags des Objekts oder in die Metadaten des Objekts kopieren. Für Azure und Google Cloud Storage ist nur die Metadatenoption verfügbar.

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

<
>
AWS S3 Bucket
✓ Settings
6 Tags/Metadata
7 Review

Relationship Metadata

Cloud Sync assigns the relationship metadata to all of the files transferred to the S3 bucket.

☐ Save on Object's Tags
 ☒ Save On Object's Metadata

Metadata Key	Metadata Value
<input type="text" value="Up to 128 characters"/>	<input type="text" value="Up to 256 characters"/>

+ Add Relationship Metadata Optional Field | [Up to 5]

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 Quelle und Ziel bei.

Manuelles Kopieren von ACLs zwischen SMB-Freigaben

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>

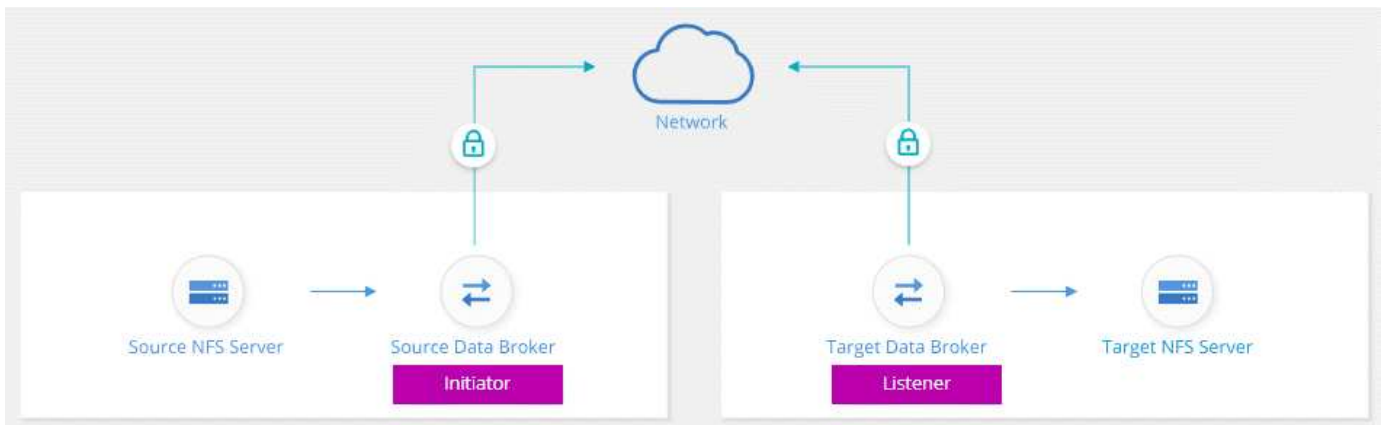
Synchronisierung von NFS-Daten mithilfe von Verschlüsselung bei der Übertragung

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.

Proxy-Serverbegrenzung

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

Was Sie benötigen, um zu beginnen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

- Zwei NFS-Server, die erfüllen "[Quell- und Zielerfordernungen](#)" 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 eine vorhandene Datenvermittler-Gruppe verwenden möchten, muss die Gruppe nur einen Daten-Broker haben. Mehrere Datenmakler in einer Gruppe werden nicht mit verschlüsselten Synchronisierungsbeziehungen unterstützt.

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](#)"
- "[Lesen Sie die Google Cloud 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

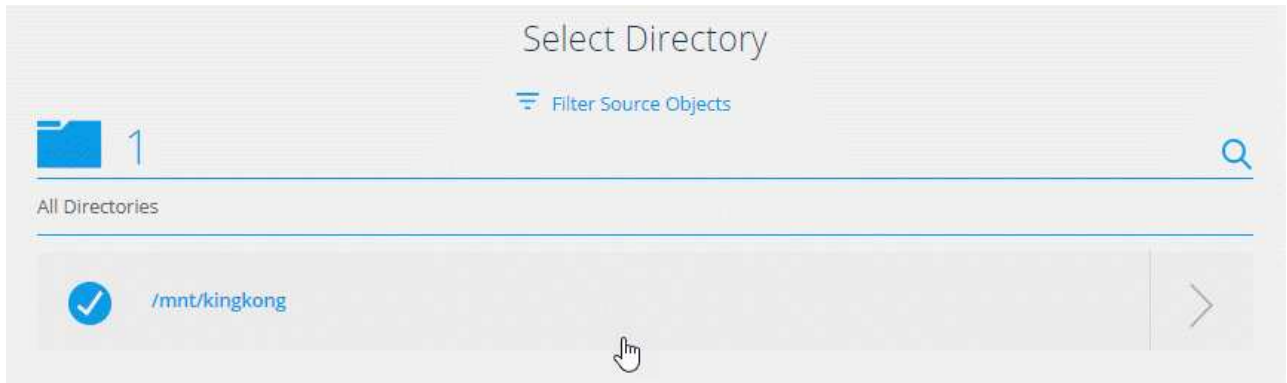
1. Klicken Sie Auf **Neuen Sync Erstellen**.
2. Ziehen Sie **NFS-Server** an den Quell- und Zielspeicherort oder **Azure NetApp Files** an den Quell- und Zielstandorten und wählen Sie **Ja** aus, um die Verschlüsselung von Daten während der Übertragung zu aktivieren.
3. Folgen Sie den Anweisungen, um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

Beachten Sie Folgendes:

- Wenn Sie eine vorhandene Datenvermittler-Gruppe verwenden möchten, muss die Gruppe nur einen Daten-Broker haben. Mehrere Datenmakler in einer Gruppe werden nicht mit verschlüsselten Synchronisierungsbeziehungen unterstützt.

- 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 Installationsskript 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.



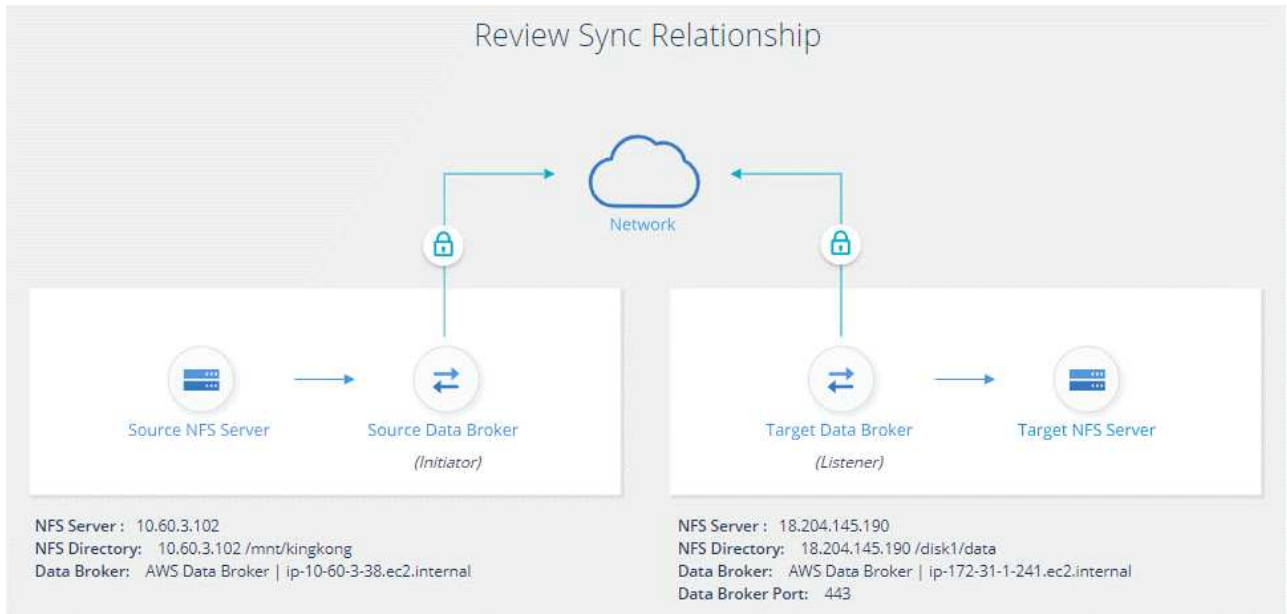
- e. **Ziel-NFS-Server/Ziel-Azure NetApp Files:** Wählen Sie die NFS-Version und geben Sie dann ein neues NFS-Ziel ein oder wählen Sie einen vorhandenen Server aus.
- f. **Target Data Broker:** Befolgen Sie die Aufforderungen, um einen neuen Quell-Daten-Broker hinzuzufügen oder einen vorhandenen Daten-Broker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

- 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.

Einrichtung einer Datenvermittler-Gruppe zur Verwendung eines externen HashiCorp Vault

Wenn Sie eine Synchronisierungsbeziehung erstellen, die Amazon S3, Azure oder Google Cloud Zugangsdaten erfordert, müssen Sie diese Anmeldedaten über die Cloud Sync Benutzeroberfläche oder die API angeben. Alternativ kann die Gruppe für den Datenvermittler eingerichtet werden, um direkt von einem externen HashiCorp Vault auf die Anmeldeinformationen (oder *Secrets*) zuzugreifen.

Diese Funktion wird durch die Cloud Sync-API für Synchronisierungsbeziehungen unterstützt, für die Amazon S3, Azure oder Google Cloud Anmeldedaten erforderlich sind.

1

Bereiten Sie den Tresor vor

Bereiten Sie den Tresor so vor, dass er die Anmeldeinformationen der Datenmaklergruppe durch Einrichten der URLs bereitstellen kann. Die URLs zu den Geheimnissen im Tresor müssen mit *Creds* enden.

2

Bereiten Sie die Gruppe des Datenmakers vor

Bereiten Sie die Datenvermittler-Gruppe so vor, dass sie Anmeldeinformationen aus dem externen Tresor abrufen kann, indem Sie die lokale Konfigurationsdatei für jeden Daten-Broker in der Gruppe ändern.

Erstellen einer Synchronisierungsbeziehung mit der API

Jetzt, da alles eingerichtet ist, können Sie einen API-Aufruf senden, um eine Synchronisierungsbeziehung zu erstellen, die Ihren Tresor verwendet, um die Geheimnisse zu erhalten.

Vorbereiten des Tresors

Sie müssen Cloud Sync mit der URL zu den Geheimnissen in Ihrem Tresor zur Verfügung stellen. Bereiten Sie den Tresor vor, indem Sie diese URLs einrichten. In den Synchronisierungsbeziehungen, die Sie erstellen möchten, müssen Sie URLs für die Anmeldeinformationen für jede Quelle und jedes Ziel einrichten.

Die URL muss wie folgt eingerichtet werden:

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

Pfad

Der Präfixpfad zum Geheimnis. Dabei kann es sich um jeden einzigartigen Wert handeln.

Anforderung-ID

Eine Anfrage-ID, die Sie generieren müssen. Beim Erstellen der Synchronisierungsbeziehung müssen Sie die ID in einem der Kopfzeilen in der API-POST-Anfrage angeben.

Endpoint-Protokoll

Eines der folgenden Protokolle, wie definiert ["In der Post-Beziehung v2-Dokumentation"](#): S3, AZURE oder GCP (jede muss Großbuchstaben enthalten).

Creds

Die URL muss mit *Creds* enden.

Beispiele

In den folgenden Beispielen werden URLs zu Secrets angezeigt.

Beispiel für die vollständige URL und den Pfad für die Quellenanmeldeinformationen

```
http://example.vault.com:8200/my-path/all-secrets/hb312vdsr2/S3Creds
```

Wie Sie im Beispiel sehen können, lautet der Präfixpfad */my-path/all-Secrets/*, die Anfragestellnummer lautet *hb312vdsr2* 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 Anfrage-ID lautet *n32hcbnejk2* und der Zielpunkt ist Azure.

Vorbereiten der Gruppe des Datenmaklers

Bereiten Sie die Datenvermittler-Gruppe so vor, dass sie Anmeldeinformationen aus dem externen Tresor abrufen kann, indem Sie die lokale Konfigurationsdatei für jeden Daten-Broker in der Gruppe ändern.

Schritte

1. SSH zu einem Daten-Broker in der Gruppe.

2. Bearbeiten Sie die Datei `local.json`, die sich in `/opt/netapp/datroker/config` befindet.
3. Stellen Sie `enable` auf **true** ein und setzen Sie die config Parameter Felder unter *External-integrationen.Haschicorp* wie folgt ein:

Aktiviert

- Gültige Werte: True/false
- Typ: Boolesch
- Standardwert: False
- Wahr: Der Datenvermittler erhält Geheimnisse von Ihrem eigenen externen HashiCorp Vault
- False: Der Datenmanager speichert die Zugangsdaten in seinem lokalen Tresor

url

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

Pfad

- Typ: Zeichenfolge
- Wert: Präfixpfad zum Geheimnis mit Ihren Anmeldeinformationen

Ablehnen – nicht autorisiert

- Legt fest, ob der Datenvermittler nicht autorisierte externe Tresore ablehnen soll
- Typ: Boolesch
- Standard: False

Auth-Methode

- Die Authentifizierungsmethode, die der Datenmanager für den Zugriff auf Anmeldeinformationen aus dem externen Tresor verwenden sollte
- Typ: Zeichenfolge
- Gültige Werte: „Aws-iam“ / „Role-App“ / „gcp-iam“

Rollenname

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

Secretid & rootid

- Typ: String (falls Sie App-Rolle verwenden)

Namespace

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

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

Beispiel für die Authentifizierung der AWS-Rolle

```
{
  "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"
      }
    }
  }
}
```

Einrichten von Berechtigungen bei Verwendung der gcp-iam-Authentifizierung

Wenn Sie die *gcp-iam*-Authentifizierungsmethode verwenden, muss der Daten-Broker die folgende GCP-Berechtigung haben:

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

["Erfahren Sie mehr über die GCP-Berechtigungsanforderungen für den Daten-Broker"](#).

Erstellen einer neuen Synchronisierungsbeziehung unter Verwendung von Secrets aus dem Tresor

Jetzt, da alles eingerichtet ist, können Sie einen API-Aufruf senden, um eine Synchronisierungsbeziehung zu erstellen, die Ihren Tresor verwendet, um die Geheimnisse zu erhalten.

Posten Sie die Beziehung mit der Cloud 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 Benutzer-Token und Ihre BlueXP-Konto-ID zu erhalten, ["Lesen Sie diese Seite in der Dokumentation"](#).
- Um einen Körper für Ihre Post-Beziehung aufzubauen, ["Siehe den Relationships-v2-API-Aufruf"](#).

Beispiel

Beispiel für DIE POST-Anforderung:

```
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"
    }
  }
}
```

Copyright-Informationen

Copyright © 2022 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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.