



Synchronisation des données entre une source et une cible

Cloud Sync

NetApp
December 16, 2022

Table des matières

- Synchronisation des données entre une source et une cible. 1
 - Création de relations synchronisées 1
 - Copie des listes de contrôle d'accès à partir des partages SMB. 8
 - Synchronisation des données NFS à l'aide du chiffrement des données à la volée 11
 - Configuration d'un groupe de courtier de données pour utiliser un coffre-fort externe HashiCorp 14

Synchronisation des données entre une source et une cible

Création de relations synchronisées

Lorsque vous créez une relation de synchronisation, le service Cloud Sync copie les fichiers de la source vers la cible. Après la copie initiale, le service synchronise les données modifiées toutes les 24 heures.

Avant de pouvoir créer certains types de relations de synchronisation, vous devez d'abord créer un environnement de travail dans BlueXP.

Créer des relations de synchronisation pour des types spécifiques d'environnements de travail

Si vous souhaitez créer des relations de synchronisation pour l'un des éléments suivants, vous devez d'abord créer ou détecter l'environnement de travail :

- Amazon FSX pour ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Clusters ONTAP sur site

Étapes

1. Créer ou découvrir l'environnement de travail.
 - ["Créez un environnement de travail Amazon FSX pour ONTAP"](#)
 - ["Configuration et détection d'Azure NetApp Files"](#)
 - ["Lancement d'Cloud Volumes ONTAP dans AWS"](#)
 - ["Lancement d'Cloud Volumes ONTAP dans Azure"](#)
 - ["Lancement d'Cloud Volumes ONTAP dans Google Cloud"](#)
 - ["Ajout de systèmes Cloud Volumes ONTAP existants"](#)
 - ["Découverte des clusters ONTAP"](#)
2. Cliquez sur **Canvas**.
3. Sélectionnez un environnement de travail correspondant à l'un des types répertoriés ci-dessus.
4. Sélectionnez le menu d'action en regard de Synchroniser.



5. Sélectionnez **Synchroniser les données de cet emplacement** ou **Synchroniser les données à cet emplacement** et suivez les invites pour configurer la relation de synchronisation.

Créez d'autres types de relations de synchronisation

Procédez comme suit pour synchroniser des données depuis ou vers un type de stockage pris en charge autre que Amazon FSX pour les clusters ONTAP, Azure NetApp Files, Cloud Volumes ONTAP ou ONTAP sur site. Les étapes ci-dessous fournissent un exemple de configuration d'une relation de synchronisation à partir d'un serveur NFS vers un compartiment S3.

1. Dans BlueXP, cliquez sur **Sync**.
2. Sur la page **Define Sync Relationship**, choisissez une source et une cible.

Les étapes suivantes fournissent un exemple de création d'une relation de synchronisation entre un serveur NFS et un compartiment S3.



3. Sur la page **NFS Server**, entrez l'adresse IP ou le nom de domaine complet du serveur NFS que vous souhaitez synchroniser avec AWS.
4. Sur la page **Data Broker Group**, suivez les invites pour créer une machine virtuelle de courtier de données dans AWS, Azure ou Google Cloud Platform ou pour installer le logiciel de courtier de données sur un hôte Linux existant.

Pour plus de détails, reportez-vous aux pages suivantes :

- ["Créer un courtier en données dans AWS"](#)
 - ["Créer un courtier en données dans Azure"](#)
 - ["Créer un courtier en données dans Google Cloud"](#)
 - ["Installation du data broker sur un hôte Linux"](#)
5. Après avoir installé le courtier de données, cliquez sur **Continuer**.



6. sur la page **répertoires**, sélectionnez un répertoire ou un sous-répertoire de niveau supérieur.

Si Cloud Sync ne parvient pas à récupérer les exportations, cliquez sur **Ajouter une exportation manuelle** et entrez le nom d'une exportation NFS.



Si vous souhaitez synchroniser plusieurs répertoires sur le serveur NFS, vous devez créer des relations de synchronisation supplémentaires après avoir terminé.

7. Sur la page **AWS S3 Bucket**, sélectionnez un compartiment :
- Allez vers le bas pour sélectionner un dossier existant dans la rubrique ou pour sélectionner un nouveau dossier que vous créez dans la rubrique.
 - Cliquez sur **Ajouter à la liste** pour sélectionner un compartiment S3 qui n'est pas associé à votre compte AWS. "[Des autorisations spécifiques doivent être appliquées au compartiment S3](#)".
8. Sur la page **Configuration godet**, configurez le compartiment :
- Optez pour l'activation du chiffrement des compartiments S3, puis sélectionnez une clé KMS AWS, saisissez l'ARN d'une clé KMS ou sélectionnez le chiffrement AES-256.
 - Sélectionnez une classe de stockage S3. "[Afficher les classes de stockage prises en charge](#)".



9. dans la page **Settings**, définissez comment les fichiers et dossiers source sont synchronisés et conservés à l'emplacement cible :

Planification

Choisissez un programme récurrent pour les synchronisations ultérieures ou désactivez la planification de synchronisation. Vous pouvez planifier une relation pour synchroniser les données aussi souvent que toutes les 1 minute.

Délai d'expiration de la synchronisation

Définissez si Cloud Sync doit annuler une synchronisation de données si la synchronisation n'a pas été effectuée dans le nombre d'heures ou de jours spécifié.

Notifications

Vous permet de choisir de recevoir ou non des notifications Cloud Sync dans le Centre de notification de BlueXP. Vous pouvez activer des notifications pour la synchronisation des données avec succès, les échecs de synchronisation et les synchronisations de données annulées.

Tentatives

Définissez le nombre de tentatives de synchronisation d'un fichier par Cloud Sync avant de l'ignorer.

Synchronisation continue

Après la synchronisation initiale des données, Cloud Sync écoute les modifications apportées au compartiment S3 source ou au compartiment Google Cloud Storage, et synchronise en continu les modifications apportées à la cible au fur et à mesure de leur apparition. Il n'est pas nécessaire d'effectuer une nouvelle analyse de la source à intervalles réguliers.

Ce paramètre est disponible uniquement lors de la création d'une relation de synchronisation et lors de la synchronisation des données à partir d'un compartiment S3 ou de Google Cloud Storage vers le stockage Azure Blob, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS, S3, Et StorageGRID * ou* à partir d'Azure Blob Storage vers le stockage Azure Blob, CIFS, Google Cloud Storage, IBM Cloud Object Storage, NFS et StorageGRID.

Si vous activez ce paramètre, il affecte d'autres fonctions comme suit :

- La planification de synchronisation est désactivée.
- Les paramètres suivants sont rétablis à leurs valeurs par défaut : délai de synchronisation, fichiers récemment modifiés et Date de modification.
- Si S3 est la source, le filtre par taille sera actif uniquement lors des événements de copie (et non lors des événements de suppression).
- Une fois la relation créée, vous ne pouvez accélérer ou supprimer que la relation. Vous ne pouvez pas annuler les synchronisations, modifier les paramètres ou afficher les rapports.

Comparer par

Choisissez si Cloud Sync doit comparer certains attributs lorsqu'il détermine si un fichier ou un répertoire a été modifié et doit être à nouveau synchronisé.

Même si vous décochez ces attributs, Cloud Sync compare toujours la source à la cible en cochant les chemins, la taille des fichiers et les noms des fichiers. En cas de modifications, il synchronise ces fichiers et répertoires.

Vous pouvez choisir d'activer ou de désactiver Cloud Sync pour comparer les attributs suivants :

- **Mtime** : dernière heure modifiée pour un fichier. Cet attribut n'est pas valide pour les répertoires.
- **Uid, gid et mode** : indicateurs d'autorisation pour Linux.

Copier pour objets

Activez cette option pour copier les métadonnées et les balises de stockage objet. Si un utilisateur modifie les métadonnées sur la source, Cloud Sync copie cet objet dans la prochaine synchronisation, mais si un utilisateur modifie les balises de la source (et non les données en soi), Cloud Sync ne copie pas l'objet dans la prochaine synchronisation.

Vous ne pouvez pas modifier cette option après avoir créé la relation.

La copie des balises est prise en charge avec les relations de synchronisation incluant Azure Blob ou un terminal compatible avec S3 (S3, StorageGRID ou stockage objet dans le cloud IBM) comme cible.

La copie de métadonnées est prise en charge avec des relations « cloud à cloud » entre l'un des terminaux suivants :

- AWS S3
- Blob d'Azure
- Google Cloud Storage
- IBM Cloud Object Storage
- StorageGRID

Fichiers récemment modifiés

Choisissez d'exclure les fichiers récemment modifiés avant la synchronisation planifiée.

Supprimer des fichiers sur la source

Choisissez de supprimer des fichiers de l'emplacement source une fois que Cloud Sync a copié les fichiers vers l'emplacement cible. Cette option inclut le risque de perte de données car les fichiers source sont supprimés après leur copie.

Si vous activez cette option, vous devez également modifier un paramètre dans le fichier local.json du courtier de données. Ouvrez le fichier et mettez-le à jour comme suit :

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

Supprimer des fichiers sur la cible

Choisissez de supprimer des fichiers de l'emplacement cible, s'ils ont été supprimés de la source. La valeur par défaut est de ne jamais supprimer de fichiers de l'emplacement cible.

Types de fichiers

Définissez les types de fichiers à inclure dans chaque synchronisation : fichiers, répertoires et liens symboliques.

Exclure les extensions de fichier

Spécifiez les extensions de fichier à exclure de la synchronisation en tapant l'extension de fichier et en appuyant sur **entrée**. Par exemple, tapez *log* ou *.log* pour exclure les fichiers *.log. Un séparateur n'est pas nécessaire pour les extensions multiples. La vidéo suivante présente une courte démonstration :

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

Exclure les noms de répertoire

Spécifiez un maximum de 15 répertoires à exclure de la synchronisation en saisissant leur nom et en appuyant sur **entrée**. Les répertoires .copy-Offload, .snapshot, ~snapshot sont exclus par défaut. Si vous souhaitez les inclure dans votre synchronisation, veuillez nous contacter.

Taille du fichier

Choisissez de synchroniser tous les fichiers, quelle que soit leur taille ou uniquement les fichiers qui se trouvent dans une plage de taille spécifique.

Date de modification

Choisissez tous les fichiers quelle que soit leur date de dernière modification, les fichiers modifiés après une date spécifique, avant une date spécifique ou entre une plage de temps.

Date de création

Lorsqu'un serveur SMB est source, ce paramètre vous permet de synchroniser les fichiers créés après une date spécifique, avant une date spécifique ou entre une plage horaire spécifique.

ACL - liste de contrôle d'accès

Copiez les ACL depuis un serveur SMB en activant un paramètre lors de la création d'une relation ou après la création d'une relation.

10. Sur la page **Tags/Metadata**, choisissez d'enregistrer une paire clé-valeur en tant qu'étiquette sur tous les fichiers transférés dans le compartiment S3 ou d'attribuer une paire clé-valeur de métadonnées sur tous les fichiers.

The screenshot shows the 'Relationship Tags' configuration page. At the top, there's a navigation bar with 'AWS S3 Bucket', 'Settings', '6 Tags/Metadata', and '7 Review'. The main heading is 'Relationship Tags'. Below it, a message states: '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.' There are two radio buttons: 'Save on Object's Tags' (selected) and 'Save On Object's Metadata'. Below this, there are two input fields: 'Tag Key' with a placeholder 'Up to 128 characters' and 'Tag Value' with a placeholder 'Up to 256 characters'. At the bottom left, there's a '+ Add Relationship Tag' button. At the bottom right, it says 'Optional Field | [Up to 5]'.



Cette même fonctionnalité est disponible lors de la synchronisation de données sur StorageGRID et IBM Cloud Object Storage. Pour Azure et Google Cloud Storage, seule l'option de métadonnées est disponible.

11. Vérifiez les détails de la relation de synchronisation, puis cliquez sur **Créer une relation**.

Résultat

Cloud Sync démarre la synchronisation des données entre la source et la cible.

Créez des relations synchronisées à partir du cloud Data Sense

Cloud Sync est intégré au sens des données dans le cloud. Dans Data Sense, vous pouvez sélectionner les fichiers source à synchroniser vers un emplacement cible à l'aide de Cloud Sync.

Une fois la synchronisation des données effectuée à partir du cloud Data SENSE, toutes les informations source le sont en une seule étape et vous devez saisir quelques informations clés. Choisissez ensuite l'emplacement cible de la nouvelle relation de synchronisation.

["Découvrez comment établir une relation synchrone à partir du Cloud Data SENSE"](#).

Copie des listes de contrôle d'accès à partir des partages SMB

Cloud Sync peut copier les listes de contrôle d'accès (ACL) entre les partages SMB et entre un partage SMB et le stockage objet (à l'exception de ONTAP S3). Si nécessaire, vous avez également la possibilité de conserver manuellement des listes de contrôle d'accès entre les partages SMB à l'aide de robocopy.

Choix

- [Configurez Cloud Sync pour copier automatiquement les ACL](#)
- [Copiez manuellement les listes de contrôle d'accès entre les partages SMB](#)

Configuration de Cloud Sync pour copier les ACL

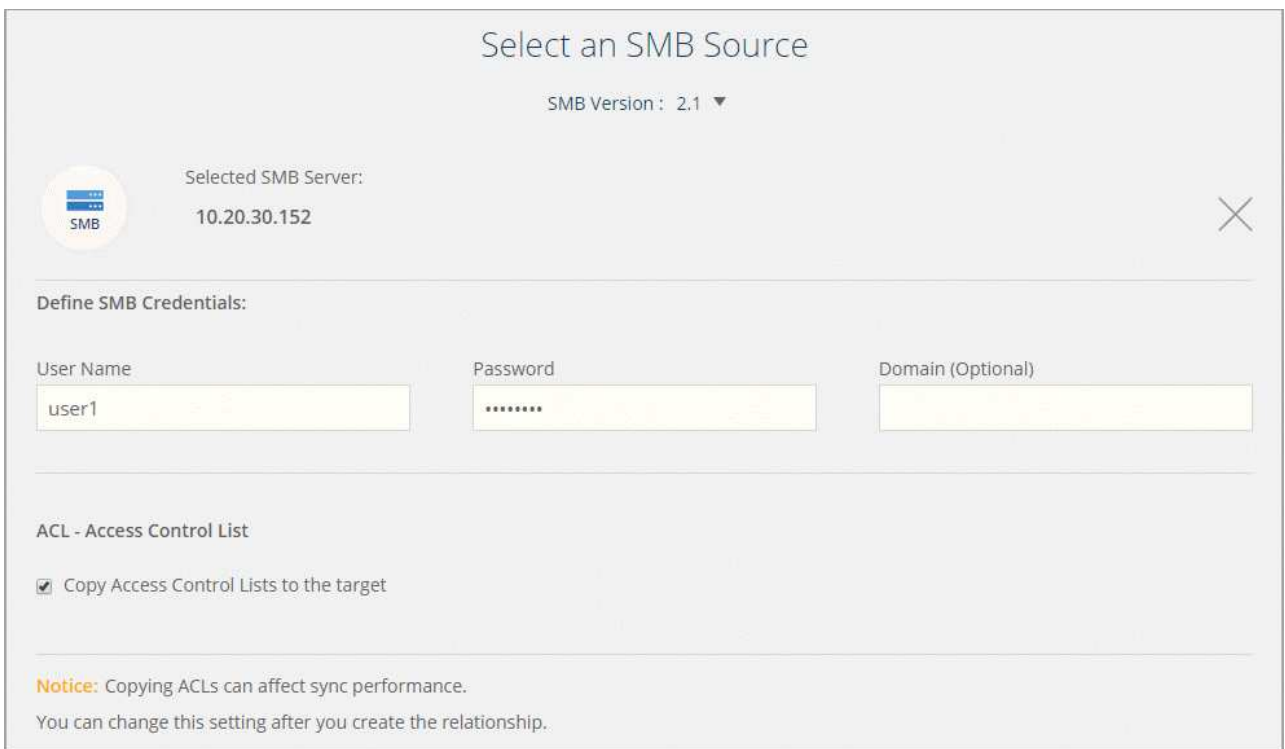
Copie de listes de contrôle d'accès entre les partages SMB et entre les partages SMB et le stockage objet en activant un paramètre lors de la création d'une relation ou après la création d'une relation.

Ce dont vous avez besoin

Cette fonctionnalité fonctionne avec *tout* type de courtier en données : AWS, Azure, Google Cloud Platform ou comme courtier en données sur site. Le courtier en données sur site peut être exécuté "[tout système d'exploitation pris en charge](#)".

Étapes d'une nouvelle relation

1. Dans Cloud Sync, cliquez sur **Créer une nouvelle synchronisation**.
2. Faites glisser un serveur SMB ou un stockage objet en tant que source et un serveur SMB ou un stockage objet en tant que cible, puis cliquez sur **Continuer**.
3. Sur la page **SMB Server** :
 - a. Entrez un nouveau serveur SMB ou sélectionnez un serveur existant et cliquez sur **Continuer**.
 - b. Saisissez les informations d'identification du serveur SMB.
 - c. Sélectionnez **Copier les listes de contrôle d'accès vers la cible** et cliquez sur **Continuer**.



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. Suivez les autres invites pour créer la relation de synchronisation.

Lorsque vous copiez des listes de contrôle d'accès depuis SMB vers le stockage objet, vous pouvez choisir de copier ces listes de contrôle d'accès vers les balises de l'objet ou sur les métadonnées de l'objet, en fonction de la cible. Pour Azure et Google Cloud Storage, seule l'option de métadonnées est disponible.

La capture d'écran suivante montre un exemple de l'étape où vous pouvez faire ce choix.

Étapes d'une relation existante

1. Survolez la relation de synchronisation et cliquez sur le menu d'action.
2. Cliquez sur **Paramètres**.
3. Sélectionnez **Copier les listes de contrôle d'accès vers la cible**.
4. Cliquez sur **Enregistrer les paramètres**.

Résultat

Lors de la synchronisation des données, Cloud Sync préserve les ACL entre la source et la cible.

Copie manuelle des listes de contrôle d'accès entre partages SMB

Vous pouvez conserver manuellement les listes de contrôle d'accès entre les partages SMB à l'aide de la commande Windows robocopy.

Étapes

1. Identifiez un hôte Windows qui dispose d'un accès complet aux deux partages SMB.
2. Si l'un des noeuds finaux nécessite une authentification, utilisez la commande **net use** pour vous connecter aux noeuds finaux à partir de l'hôte Windows.

Vous devez effectuer cette étape avant d'utiliser Robocopy.

3. Dans Cloud Sync, créez une nouvelle relation entre les partages SMB source et cible ou synchronisez une relation existante.
4. Une fois la synchronisation des données terminée, exécutez la commande suivante à partir de l'hôte Windows pour synchroniser les ACL et la propriété :

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

Source et *target* doivent être spécifiés à l'aide du format UNC. Par exemple :

\\<serveur>\<partage>\<chemin>

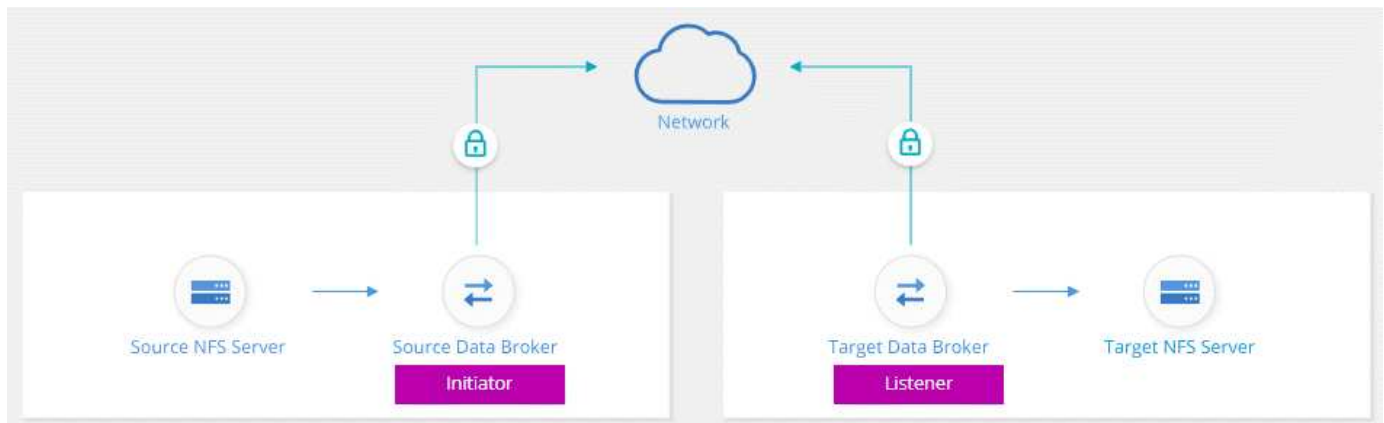
Synchronisation des données NFS à l'aide du chiffrement des données à la volée

Si votre entreprise dispose de règles de sécurité strictes, vous pouvez synchroniser les données NFS à l'aide du chiffrement des données à la volée. Cette fonctionnalité est prise en charge d'un serveur NFS vers un autre serveur NFS et de Azure NetApp Files vers Azure NetApp Files.

Par exemple, vous pouvez synchroniser des données entre deux serveurs NFS situés sur des réseaux différents. Ou bien vous devrez peut-être transférer des données sur Azure NetApp Files de manière sécurisée entre plusieurs sous-réseaux ou régions.

Fonctionnement du chiffrement des données en vol.

Le chiffrement des données à la volée crypte les données NFS lorsqu'elles sont transmises sur le réseau entre deux courtiers de données. L'image suivante montre une relation entre deux serveurs NFS et deux courtiers de données :



Un courtier de données fonctionne comme *initiator*. Lorsqu'il est temps de synchroniser des données, il envoie une demande de connexion à l'autre courtier de données, qui est le *listener*. Ce courtier de données écoute les demandes sur le port 443. Vous pouvez utiliser un autre port, si nécessaire, mais assurez-vous que le port n'est pas utilisé par un autre service.

Par exemple, si vous synchronisez des données d'un serveur NFS sur site vers un serveur NFS basé sur le cloud, vous pouvez choisir le courtier de données qui écoute les demandes de connexion et qui les envoie.

Voici le fonctionnement du chiffrement à la volée :

1. Après avoir créé la relation de synchronisation, l'initiateur démarre une connexion chiffrée avec l'autre courtier de données.
2. Le courtier de données source crypte les données à partir de la source à l'aide de TLS 1.3.
3. Il envoie ensuite les données via le réseau au data broker cible.
4. Le courtier de données cible décrypte les données avant de les envoyer à la cible.
5. Après la copie initiale, le service synchronise les données modifiées toutes les 24 heures. S'il y a des données à synchroniser, le processus commence par l'initiateur qui ouvre une connexion chiffrée avec l'autre courtier de données.

Si vous préférez synchroniser les données plus fréquemment, ["vous pouvez modifier le planning après avoir créé la relation"](#).

Versions NFS prises en charge

- Pour les serveurs NFS, le chiffrement des données à la volée est pris en charge avec les versions 3, 4.0, 4.1 et 4.2 de NFS.
- Pour Azure NetApp Files, le chiffrement des données à la volée est pris en charge avec les versions 3 et 4.1 de NFS.

Limitation du serveur proxy

Si vous créez une relation de synchronisation chiffrée, les données cryptées sont envoyées via HTTPS et ne sont pas routables via un serveur proxy.

Ce dont vous avez besoin pour commencer

Assurez-vous d'avoir les éléments suivants :

- Deux serveurs NFS qui sont équipés ["exigences source et cible"](#) Ou Azure NetApp Files dans deux sous-réseaux ou régions.
- Les adresses IP ou noms de domaine complets des serveurs.
- Emplacements réseau pour deux courtiers de données.

Vous pouvez sélectionner un courtier de données existant, mais il doit fonctionner comme initiateur. Le courtier de données de l'écouteur doit être un courtier de données *New*.

Si vous souhaitez utiliser un groupe de courtiers de données existant, le groupe ne doit avoir qu'un seul courtier de données. Plusieurs courtiers de données d'un groupe ne sont pas pris en charge avec des relations de synchronisation chiffrées.

Si vous n'avez pas encore déployé de courtier de données, consultez les exigences du courtier de données. Comme vous disposez de règles de sécurité strictes, passez en revue les exigences de mise en réseau, notamment le trafic sortant à partir du port 443 et du ["terminaux internet"](#) que le courtier de données contacte.

- ["Consultez l'installation d'AWS"](#)
- ["Vérifiez l'installation d'Azure"](#)
- ["Consultez l'installation de Google Cloud"](#)
- ["Vérifiez l'installation de l'hôte Linux"](#)

Synchronisation des données NFS à l'aide du chiffrement des données à la volée

Créez une nouvelle relation de synchronisation entre deux serveurs NFS ou entre Azure NetApp Files, activez l'option de chiffrement à la volée et suivez les invites.

Étapes

1. Cliquez sur **Créer une nouvelle synchronisation**.
2. Faites glisser **serveur NFS** vers les emplacements source et cible ou **Azure NetApp Files** vers les emplacements source et cible et sélectionnez **Oui** pour activer le cryptage des données en transit.
3. Suivez les invites pour créer la relation :
 - a. **NFS Server/Azure NetApp Files** : Choisissez la version NFS, puis spécifiez une nouvelle source NFS

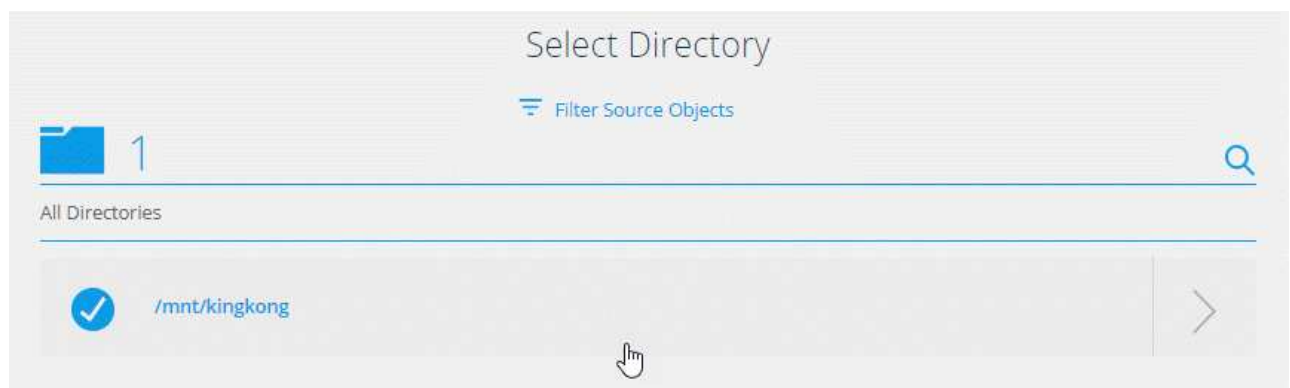
ou sélectionnez un serveur existant.

- b. **Définir la fonctionnalité de Data Broker** : définissez le courtier de données *écoute* pour les demandes de connexion sur un port et lequel *lance* la connexion. Faites votre choix en fonction de vos besoins en matière de mise en réseau.
- c. **Data Broker** : suivez les invites pour ajouter un nouveau courtier de données source ou sélectionner un courtier de données existant.

Notez ce qui suit :

- Si vous souhaitez utiliser un groupe de courtiers de données existant, le groupe ne doit avoir qu'un seul courtier de données. Plusieurs courtiers de données d'un groupe ne sont pas pris en charge avec des relations de synchronisation chiffrées.
 - Si le courtier de données source agit en tant qu'auditeur, il doit alors être un nouveau courtier de données.
 - Si vous avez besoin d'un nouveau courtier de données, Cloud Sync vous invite à suivre les instructions d'installation. Vous pouvez déployer le data broker dans le cloud ou télécharger un script d'installation pour votre propre hôte Linux.
- d. **Répertoires** : Choisissez les répertoires que vous souhaitez synchroniser en sélectionnant tous les répertoires ou en descendant et en sélectionnant un sous-répertoire.

Cliquez sur **Filtrer les objets source** pour modifier les paramètres qui définissent la synchronisation et la gestion des fichiers et dossiers source à l'emplacement cible.




- e. **Serveur NFS cible/Azure NetApp Files cible** : Choisissez la version NFS, puis entrez une nouvelle cible NFS ou sélectionnez un serveur existant.
- f. **Courtier de données cible** : suivez les invites pour ajouter un nouveau courtier de données source ou sélectionner un courtier de données existant.


Si le courtier de données cible agit en tant qu'auditeur, il doit alors être un nouveau courtier de données.

Voici un exemple d'invite lorsque le courtier de données cible fonctionne comme écouteur. Notez l'option permettant de spécifier le port.


Select a Provider




Microsoft Azure



Amazon Web Services



Google Cloud Platform

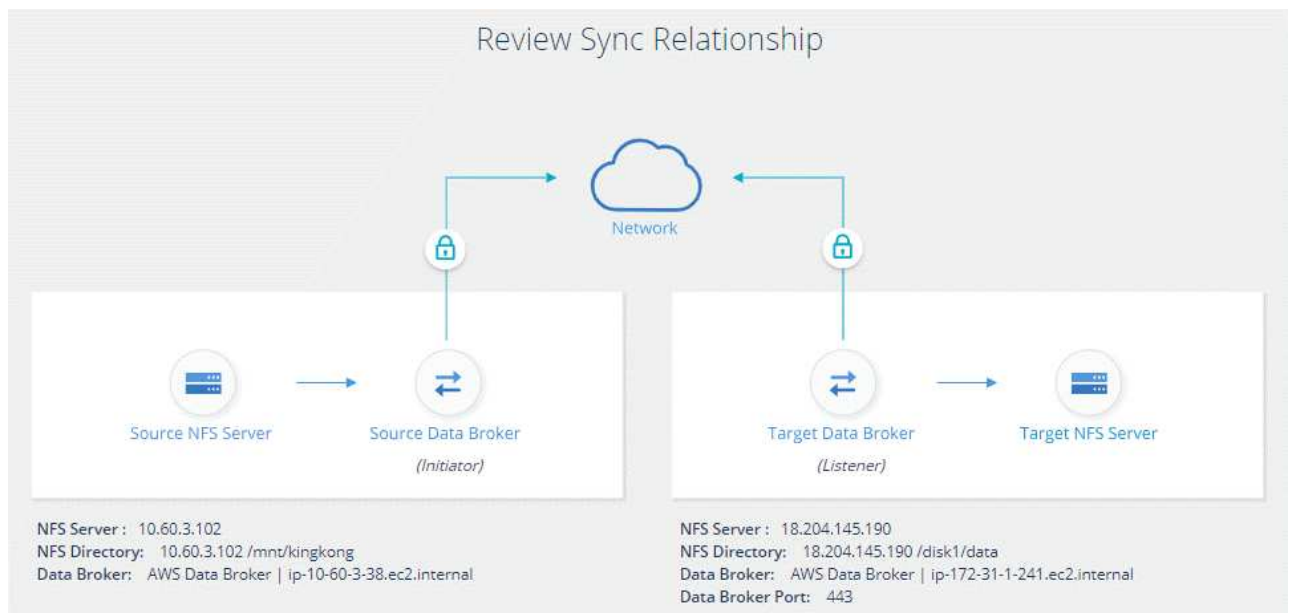


On-Prem Data Broker

Data Broker Name

Port

- a. **Répertoires cibles** : sélectionnez un répertoire de niveau supérieur ou accédez à la recherche pour sélectionner un sous-répertoire existant ou créer un nouveau dossier à l'intérieur d'une exportation.
- b. **Paramètres** : définissez comment les fichiers et dossiers source sont synchronisés et gérés à l'emplacement cible.
- c. **Revue** : consultez les détails de la relation de synchronisation, puis cliquez sur **Créer une relation**.



Résultat

Cloud Sync commence à créer la nouvelle relation de synchronisation. Lorsque vous avez terminé, cliquez sur **Afficher dans le tableau de bord** pour afficher les détails de la nouvelle relation.

Configuration d'un groupe de courtier de données pour utiliser un coffre-fort externe HashiCorp

Lorsque vous créez une relation de synchronisation qui requiert des identifiants Amazon S3, Azure ou Google

Cloud, vous devez spécifier ces identifiants via l'interface ou l'API utilisateur de Cloud Sync. Une alternative consiste à configurer le groupe de courtiers de données pour accéder aux informations d'identification (ou *secrets*) directement à partir d'un coffre-fort externe HashiCorp.

Cette fonctionnalité est prise en charge par le biais de l'API Cloud Sync avec des relations synchronisées qui requièrent des identifiants Amazon S3, Azure ou Google Cloud.

1

Préparez le coffre-fort

Préparez le coffre-fort pour fournir les informations d'identification au groupe de courtiers de données en configurant les URL. Les URL des secrets dans le coffre-fort doivent se terminer par *creds*.

2

Préparer le groupe de courtiers de données

Préparez le groupe de courtier de données pour extraire les informations d'identification du coffre-fort externe en modifiant le fichier de configuration local de chaque courtier de données du groupe.

3

Créez une relation de synchronisation à l'aide de l'API

Maintenant que tout est configuré, vous pouvez envoyer un appel API pour créer une relation de synchronisation qui utilise votre coffre-fort pour obtenir les secrets.

Préparation du coffre-fort

Vous devrez fournir à Cloud Sync l'URL des secrets de votre coffre-fort. Préparez le coffre-fort en configurant ces URL. Vous devez configurer des URL pour les identifiants de chaque source et cible dans les relations de synchronisation que vous prévoyez de créer.

L'URL doit être configurée comme suit :

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

Chemin

Chemin du préfixe vers le secret. Tous ces atouts peuvent être uniques à votre entreprise.

ID de la demande

ID de demande que vous devez générer. Vous devrez fournir l'ID dans l'un des en-têtes de la demande POST API lorsque vous créez la relation de synchronisation.

Protocole de terminal

L'un des protocoles suivants, tel que défini "[dans la documentation post-relation v2](#)": S3, AZURE ou GCP (chacun doit être en majuscules).

Creds

L'URL doit se terminer par *creds*.

Exemples

Les exemples suivants montrent des URL vers des secrets.

Exemple pour l'URL complète et le chemin d'accès pour les informations d'identification source

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

Comme vous pouvez le voir dans l'exemple, le chemin du préfixe est */mon-chemin/tous-secrets/*, l'ID de la demande est *hb312vdsr2* et le noeud final source est *S3*.

Exemple pour l'URL complète et le chemin des informations d'identification de la cible

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

Le chemin du préfixe est */my-path/all-secrets/*, l'ID de la demande est *n32hcbnejk2*, et le noeud final cible est *Azure*.

Préparation du groupe de courtiers de données

Préparez le groupe de courtier de données pour extraire les informations d'identification du coffre-fort externe en modifiant le fichier de configuration local de chaque courtier de données du groupe.

Étapes

1. SSH vers un courtier de données dans le groupe.
2. Modifiez le fichier `local.json` qui se trouve dans `/opt/netapp/Dataroker/config`.
3. Définissez l'option `enable` sur **true** et définissez les champs des paramètres de configuration sous *external-intégrations.haschicorp* comme suit :

activé

- Valeurs valides : vrai/faux
- Type : booléen
- Valeur par défaut : FALSE
- Vrai: Le courtier de données obtient des secrets de votre propre coffre-fort externe HashiCorp
- FALSE : le courtier de données stocke les informations d'identification dans son coffre-fort local

url

- Type : chaîne
- Valeur : l'URL de votre coffre-fort externe

chemin

- Type : chaîne
- Valeur : chemin du préfixe vers le secret avec vos informations d'identification

Rejet non autorisé

- Détermine si vous souhaitez que le courtier de données rejette le coffre-fort externe non autorisé
- Type : booléen
- Par défaut : FALSE

méthode-auth

- Méthode d'authentification que le courtier de données doit utiliser pour accéder aux informations d'identification à partir du coffre-fort externe
- Type : chaîne

- Valeurs valides : "aws-iam" / "Role-app" / "gcp-iam"

nom-rôle

- Type : chaîne
- Nom du rôle (si vous utilisez aws-iam ou gcp-iam)

Secretid et rotide

- Type : chaîne (si vous utilisez APP-role)

Espace de noms

- Type : chaîne
- Votre espace de noms (en-tête X-Vault-namespace, le cas échéant)

4. Répétez ces étapes pour tous les autres courtiers de données du groupe.

Exemple d'authentification aws-role

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

Exemple d'authentification gcp-iam

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

Configuration des autorisations lors de l'utilisation de l'authentification gcp-iam

Si vous utilisez la méthode d'authentification *gcp-iam*, le courtier de données doit disposer de l'autorisation GCP suivante :

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

["En savoir plus sur les exigences d'autorisation GCP pour le courtier de données".](#)

Création d'une nouvelle relation de synchronisation à l'aide des secrets du coffre-fort

Maintenant que tout est configuré, vous pouvez envoyer un appel API pour créer une relation de synchronisation qui utilise votre coffre-fort pour obtenir les secrets.

Publiez la relation à l'aide de l'API REST de Cloud Sync.

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

- Pour obtenir un jeton utilisateur et votre identifiant de compte BlueXP, ["reportez-vous à cette page dans la documentation"](#).
- Pour créer un corps pour votre relation post, ["Reportez-vous à l'appel de l'API relations-v2"](#).

Exemple

Exemple pour la demande POST :

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": "5e6e111d578dtyuul555sa60",
  "source": {
    "protocol": "s3",
    "s3": {
      "provider": "sgws",
      "host": "1.1.1.1",
      "port": "443",
      "bucket": "my-source"
    }
  },
  "target": {
    "protocol": "s3",
    "s3": {
      "bucket": "my-target-bucket"
    }
  }
}
```

Informations sur le copyright

Copyright © 2022 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.