



Utiliser Cloud Sync

Cloud Sync

NetApp
December 16, 2022

Table des matières

- Utiliser Cloud Sync 1
 - Synchronisation des données entre une source et une cible 1
 - Payer pour la synchronisation après la fin de votre essai gratuit. 20
 - Gestion des relations de synchronisation 22
 - Gérez les groupes de courtiers de données 29
 - Création et affichage de rapports pour ajuster votre configuration 36
 - Désinstallation du courtier de données 39

Utiliser Cloud Sync

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.

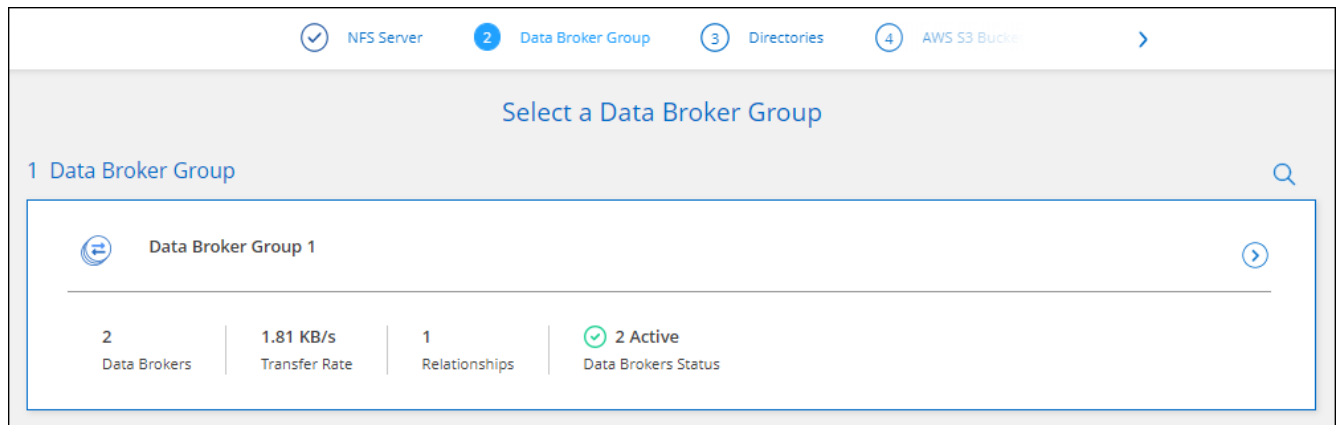


3. Sur la page **NFS Server**, entrez l'adresse IP ou le nom de domaine complet du serveur NFS que vous souhaitez synchroniser avec AWS.
4. Sur la page **Data Broker Group**, suivez les invites pour créer une machine virtuelle de courtier de données dans AWS, Azure ou Google Cloud Platform ou pour installer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



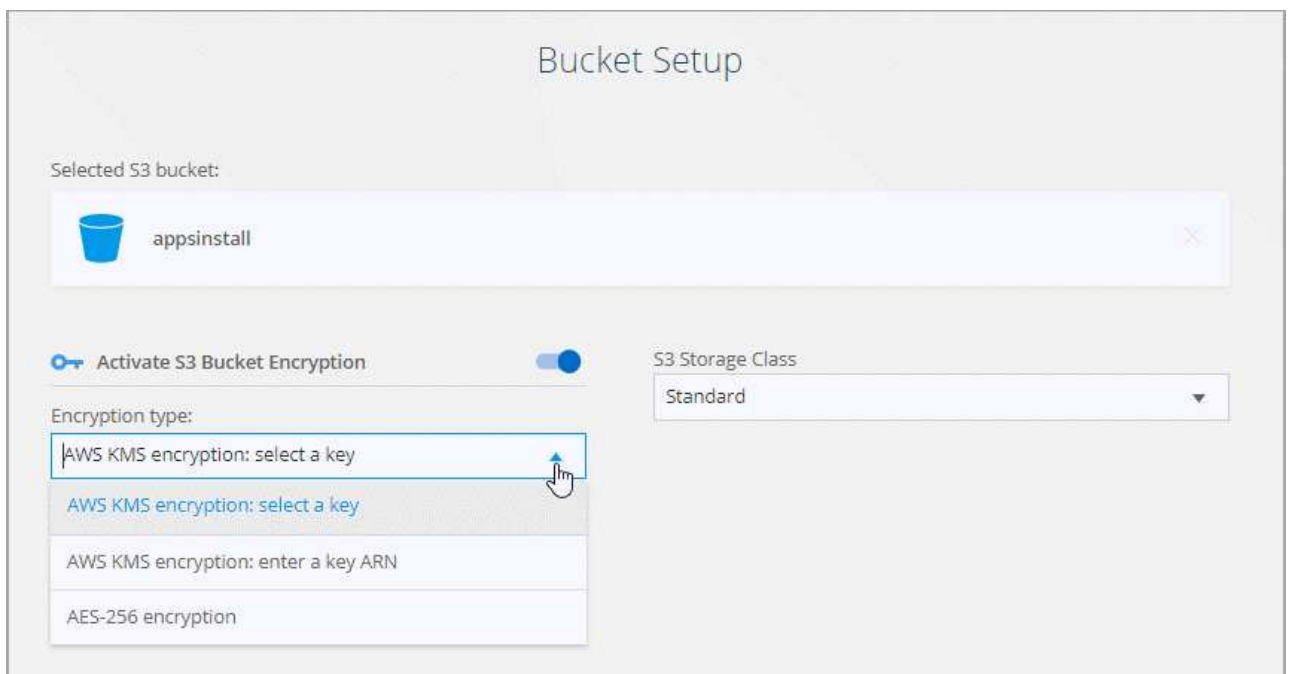
6. sur la page **répertoires**, sélectionnez un répertoire ou un sous-répertoire de niveau supérieur.

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 these 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 is a button '+ Add Relationship Tag' and at the bottom right is the text '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.

Sync Relationship

1 Data Sense Integration 2 Data Broker Group 3 NFS Server 4 Directory

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)

["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**.

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>

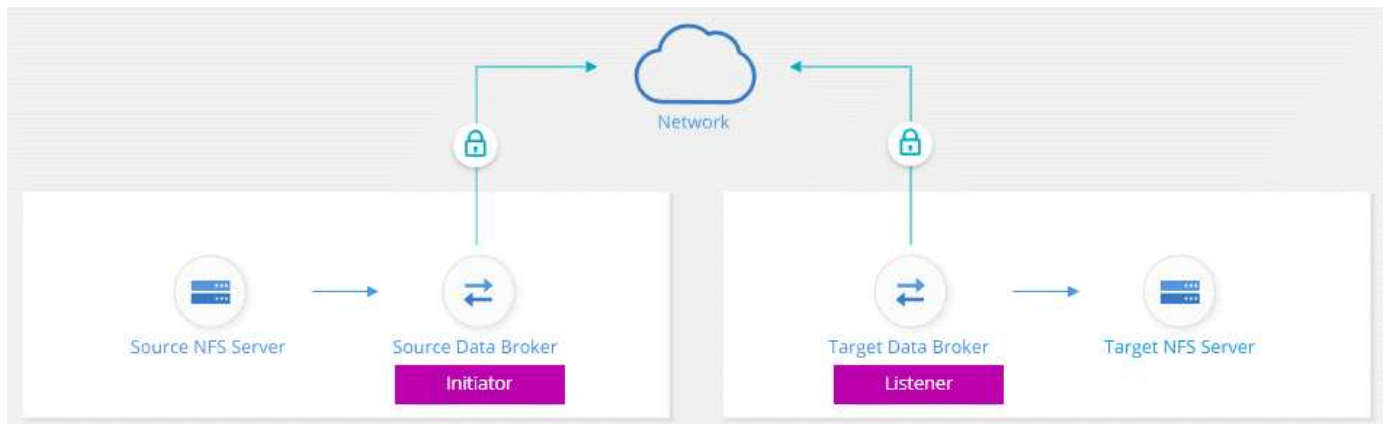
Synchronisation des données NFS à l'aide du chiffrement des données à la volée

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

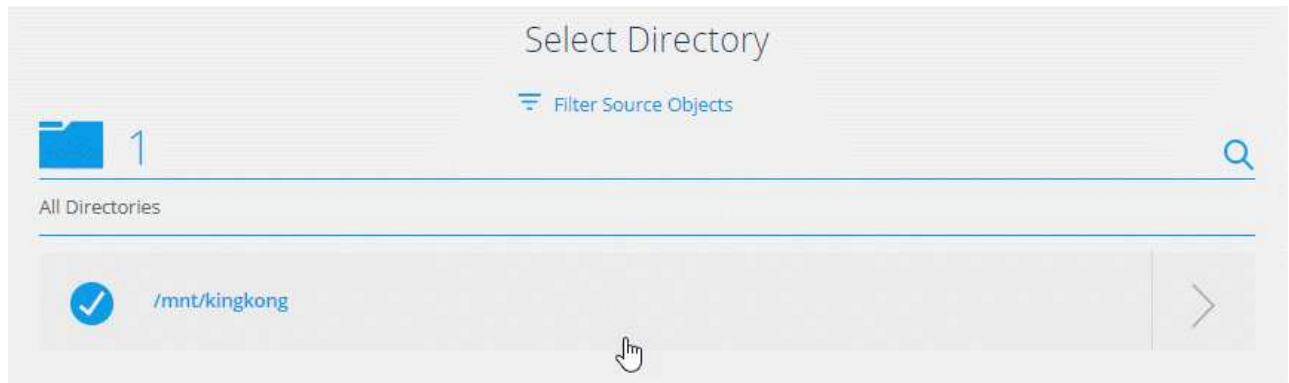
1. Cliquez sur **Créer une nouvelle synchronisation**.
2. Faites glisser **serveur NFS** vers les emplacements source et cible ou **Azure NetApp Files** vers les emplacements source et cible et sélectionnez **Oui** pour activer le cryptage des données en transit.
3. Suivez les invites pour créer la relation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

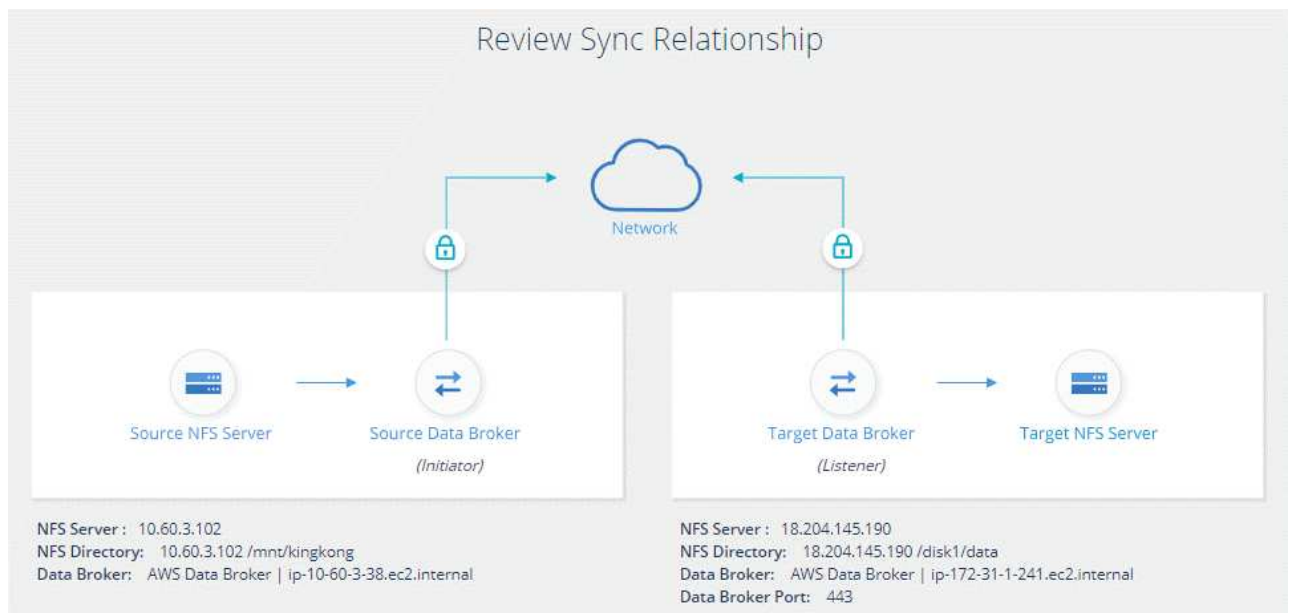


On-Prem Data Broker

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-integrations.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"
    }
  }
}
```

Payer pour la synchronisation après la fin de votre essai gratuit

Il existe deux façons de payer les relations de synchronisation après la fin de votre essai gratuit de 14 jours. La première option consiste à vous abonner à AWS ou Azure pour payer à votre gré ou à payer annuellement. La deuxième option consiste à acheter des licences directement auprès de NetApp.

Vous pouvez vous abonner à AWS Marketplace ou à Azure Marketplace. Vous ne pouvez pas vous abonner des deux.

Vous avez la possibilité d'utiliser les licences de NetApp avec un abonnement Marketplace. Par exemple, si vous disposez de 25 relations de synchronisation, vous pouvez payer les 20 premières relations de synchronisation à l'aide d'une licence, puis effectuer des opérations de paiement à la demande à partir d'AWS ou d'Azure avec les 5 autres relations de synchronisation.

["En savoir plus sur le fonctionnement des licences"](#).

Que dois-je payer immédiatement après 8217 la fin de mon essai gratuit ?

Vous ne pourrez pas créer de relations supplémentaires. Les relations existantes ne sont pas supprimées, mais vous ne pouvez pas y apporter de modifications tant que vous n'êtes pas abonné ou que vous n'avez pas saisi de licence.

abonnement d'AWS

AWS vous permet de payer à votre gré ou de payer chaque année.

Les étapes à payer en tant que vous-même

1. Cliquez sur **Sync > licences**.
2. Sélectionnez **AWS**
3. Cliquez sur **s'abonner**, puis sur **Continuer**.
4. Abonnez-vous à AWS Marketplace, puis connectez-vous au service Cloud Sync pour terminer l'enregistrement.

La vidéo suivante montre le processus :

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

Étapes à payer annuellement

1. ["Accédez à la page AWS Marketplace"](#).
2. Cliquez sur **Continuer pour s'inscrire**.
3. Sélectionnez vos options de contrat et cliquez sur **Créer contrat**.

abonnement d'Azure

Azure vous permet de payer à votre gré ou de payer chaque année.

Ce dont vous avez besoin

Un compte utilisateur Azure disposant des autorisations Contributeur ou Propriétaire dans l'abonnement correspondant.

Étapes

1. Cliquez sur **Sync > licences**.
2. Sélectionnez **Azure**.
3. Cliquez sur **s'abonner**, puis sur **Continuer**.
4. Dans le portail Azure, cliquez sur **Créer**, sélectionnez vos options et cliquez sur **s'abonner**.

Sélectionnez **mensuel** pour payer par heure, ou **annuel** pour payer une année avant.

5. Une fois le déploiement terminé, cliquez sur le nom de la ressource SaaS dans le menu contextuel de notification.
6. Cliquez sur **configurer le compte** pour revenir à Cloud Sync.

La vidéo suivante montre le processus :

► https://docs.netapp.com/fr-fr/cloud-manager-sync//media/video_cloud_sync_registering_azure.mp4

(video)

achat de licences de NetApp et leur ajout à Cloud Sync

Pour payer vos relations de synchronisation, vous devez acheter une ou plusieurs licences et les ajouter au service Cloud Sync.

Ce dont vous avez besoin

Vous devez disposer du numéro de série correspondant à votre licence, ainsi que du nom d'utilisateur et du mot de passe du compte sur le site de support NetApp auquel la licence est associée.

Étapes

1. Achetez une licence par [contacter NetApp](#).
2. Dans BlueXP, cliquez sur **Sync > licences**.
3. Cliquez sur **Ajouter une licence** et ajoutez les informations requises :
 - a. Saisissez le numéro de série.
 - b. Sélectionnez le compte sur le site de support NetApp associé à la licence que vous ajoutez :
 - Si votre compte a déjà été ajouté à BlueXP, sélectionnez-le dans la liste déroulante.
 - Si votre compte n'a pas encore été ajouté, cliquez sur **Ajouter des informations d'identification NSS**, entrez le nom d'utilisateur et le mot de passe, cliquez sur **Enregistrer**, puis sélectionnez-le dans la liste déroulante.
 - c. Cliquez sur **Ajouter**.

Mise à jour d'une licence

Si vous avez prolongé une licence Cloud Sync que vous avez achetée auprès de NetApp, la nouvelle date d'expiration ne sera pas automatiquement mise à jour dans Cloud Sync. Vous devez ajouter de nouveau la licence pour actualiser la date d'expiration.

Étapes

1. Dans BlueXP, cliquez sur **Sync > licences**.
2. Cliquez sur **Ajouter une licence** et ajoutez les informations requises :
 - a. Saisissez le numéro de série.
 - b. Sélectionnez le compte du site de support NetApp associé à la licence que vous ajoutez.
 - c. Cliquez sur **Ajouter**.

Résultat

Cloud Sync met à jour la licence existante avec la nouvelle date d'expiration.


Gestion des relations de synchronisation

Vous pouvez gérer les relations de synchronisation à tout moment en synchronisant immédiatement les données, en modifiant les horaires, etc.

Synchronisez immédiatement les données

Au lieu d'attendre la synchronisation planifiée suivante, vous pouvez appuyer sur un bouton pour synchroniser immédiatement les données entre la source et la cible.

Étapes

1. Dans **Dashboard**, naviguez jusqu'à la relation de synchronisation et cliquez sur .
2. Cliquez sur **Synchroniser maintenant**, puis sur **Sync** pour confirmer.

Résultat

Cloud Sync démarre le processus de synchronisation des données pour la relation.

Accélération des performances de synchronisation

Accélérez les performances d'une relation de synchronisation en ajoutant un courtier de données supplémentaire au groupe qui gère la relation. Le courtier de données supplémentaire doit être un *New Data broker*.

Comment cela fonctionne


Si le groupe du courtier gère d'autres relations de synchronisation, le nouveau courtier de données que vous ajoutez au groupe accélère également les performances de ces relations de synchronisation.

Imaginons par exemple que vous ayez trois relations :

- La relation 1 est gérée par le groupe de courtiers de données A
- La relation 2 est gérée par le groupe de courtiers de données B
- La relation 3 est gérée par le groupe de courtiers de données A.

Vous voulez accélérer les performances de la relation 1 pour ajouter un nouveau courtier de données au groupe de courtier de données A. Dans la mesure où le groupe A gère également la relation de synchronisation 3, les performances de synchronisation de la relation sont également automatiquement accélérées.

Étapes

1. Assurez-vous qu'au moins un des courtiers de données existants dans la relation est en ligne.
2. Dans **Dashboard**, naviguez jusqu'à la relation de synchronisation et cliquez sur .
3. Cliquez sur **accélérer**.
4. Suivez les invites pour créer un nouveau courtier de données.

Résultat

Cloud Sync ajoute le nouveau courtier de données au groupe. Les performances de la prochaine synchronisation des données doivent être accélérées.

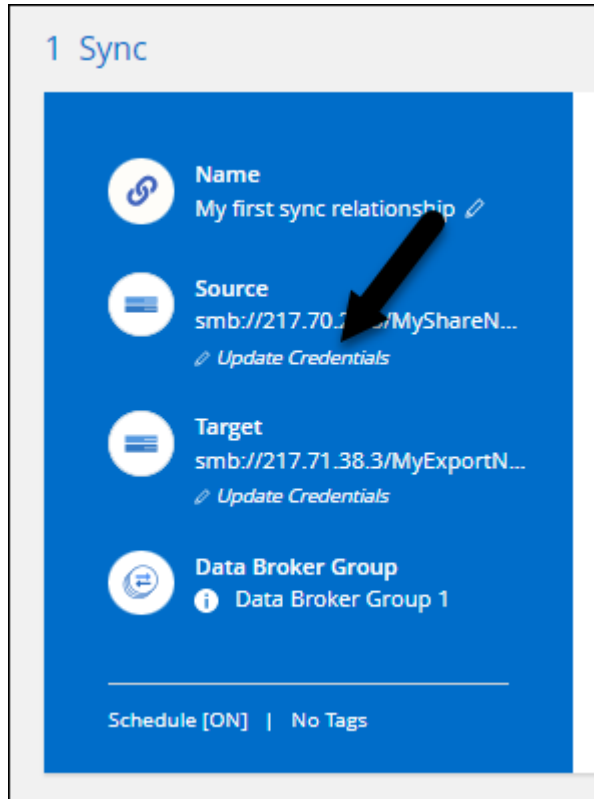
Mise à jour des identifiants

Vous pouvez mettre à jour le courtier de données avec les informations d'identification les plus récentes de la source ou de la cible dans une relation de synchronisation existante. La mise à jour des informations d'identification peut vous aider si vos stratégies de sécurité vous obligent à mettre à jour les informations d'identification de manière périodique.

La mise à jour des identifiants est prise en charge avec toute source ou cible pour laquelle Cloud Sync nécessite des identifiants pour : Azure Blob, Box, IBM Cloud Object Storage, StorageGRID, ONTAP S3 Storage, SFTP et les serveurs SMB.

Étapes

1. Dans le tableau de bord **Sync**, accédez à une relation de synchronisation qui nécessite des informations d'identification, puis cliquez sur **mettre à jour les informations d'identification**.



2. Entrez les informations d'identification et cliquez sur **Update**.

Remarque sur les serveurs SMB : si le domaine est nouveau, vous devez le spécifier lors de la mise à jour des informations d'identification. Si le domaine n'a pas changé, vous n'avez pas besoin de le saisir à nouveau.

Si vous avez entré un domaine lors de la création de la relation de synchronisation, mais que vous n'entrez pas de nouveau domaine lorsque vous mettez à jour les informations d'identification, Cloud Sync utilisera alors le domaine d'origine que vous avez fourni.

Résultat

Cloud Sync met à jour les identifiants du courtier en données. Le 10 courtier en données peut prendre jusqu'à ce que ses identifiants soient utilisés pour la synchronisation des données.


Configuration des notifications

Un paramètre **Notifications** pour chaque relation de synchronisation 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.



Vous pouvez également recevoir des notifications par e-mail.

Étapes


1. Modifiez les paramètres d'une relation de synchronisation :
 - a. Dans **Dashboard**, naviguez jusqu'à la relation de synchronisation et cliquez sur .
 - b. Cliquez sur **Paramètres**.
 - c. Activez **Notifications**.
 - d. Cliquez sur **Enregistrer les paramètres**.
2. Si vous souhaitez recevoir des notifications par e-mail, configurez les paramètres d'alerte et de notification :
 - a. Cliquez sur **Paramètres > Paramètres d'alertes et de notifications**.
 - b. Sélectionnez un ou plusieurs utilisateurs et choisissez le type de notification **Info**.
 - c. Cliquez sur **appliquer**.

Résultat

Vous recevrez maintenant des notifications Cloud Sync dans le Centre de notification de BlueXP, avec quelques notifications envoyées par e-mail, si vous avez configuré cette option.

Modification des paramètres d'une relation de synchronisation

Modifiez les paramètres qui définissent la façon dont les fichiers et dossiers source sont synchronisés et gérés à l'emplacement cible.

1. Dans **Dashboard**, naviguez jusqu'à la relation de synchronisation et cliquez sur .
2. Cliquez sur **Paramètres**.
3. Modifiez l'un des paramètres.

General

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

Files and Directories

Compare By	The following attributes (and size): uid, gid, mode, mtime	⌵
Recently Modified Files	Exclude files that are modified up to 30 Seconds before a scheduled sync	⌵
Delete Files On Source	Never delete files from the source location	⌵
Delete Files On Target	Never delete files from the target location	⌵
File Types	Include All: Files, Directories, Symbolic Links	⌵
Exclude File Extensions	None	⌵
File Size	All	⌵
Date Modified	All	⌵
Date Created	All	⌵
ACL - Access Control List	Inactive	⌵

Reset to defaults

Voici une brève description de chaque paramètre :

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.

Si vous souhaitez recevoir des notifications pour

Tentatives

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

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

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

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 copier 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.

4. Cliquez sur **Enregistrer les paramètres**.


Résultat

Cloud Sync modifie la relation de synchronisation avec les nouveaux paramètres.

Suppression de relations

Vous pouvez supprimer une relation de synchronisation si vous n'avez plus besoin de synchroniser les données entre la source et la cible. Cette action ne supprime pas le groupe du courtier de données (ou les instances individuelles du courtier de données) et ne supprime pas les données de la cible.

Étapes

1. Dans **Dashboard**, naviguez jusqu'à la relation de synchronisation et cliquez sur 
2. Cliquez sur **Supprimer**, puis cliquez à nouveau sur **Supprimer** pour confirmer.

Résultat

Cloud Sync supprime la relation de synchronisation.

Gérez les groupes de courtiers de données

Un groupe de courtier de données synchronise les données d'un emplacement source vers un emplacement cible. Au moins un courtier de données est requis dans un groupe pour chaque relation de synchronisation que vous créez. Gérer les groupes de courtiers de données en ajoutant un nouveau courtier de données à un groupe, en affichant des informations sur les groupes, etc.

Fonctionnement des groupes de courtiers de données

Un groupe de courtiers de données peut comprendre un ou plusieurs courtiers de données. Le regroupement de courtiers de données entre eux permet d'améliorer les performances des relations de synchronisation.

Les groupes peuvent gérer plusieurs relations

Un groupe de courtiers de données peut gérer une ou plusieurs relations synchronisées à la fois.

Imaginons par exemple que vous ayez trois relations :

- La relation 1 est gérée par le groupe de courtiers de données A
- La relation 2 est gérée par le groupe de courtiers de données B
- La relation 3 est gérée par le groupe de courtiers de données A.

Vous voulez accélérer les performances de la relation 1 pour ajouter un nouveau courtier de données au groupe de courtier de données A. Dans la mesure où le groupe A gère également la relation de synchronisation 3, les performances de synchronisation de la relation sont également automatiquement accélérées.

Nombre de courtiers de données dans un groupe

Dans de nombreux cas, un seul courtier de données peut répondre aux exigences de performance d'une relation de synchronisation. Si ce n'est pas le cas, vous pouvez accélérer les performances de synchronisation en ajoutant des courtiers de données supplémentaires au groupe. Mais vous devez d'abord vérifier d'autres facteurs qui peuvent avoir un impact sur les performances de synchronisation. ["En savoir plus sur la façon de déterminer si plusieurs courtiers de données sont nécessaires"](#).

Recommandations en matière de sécurité

Pour assurer la sécurité de votre courtier en données, NetApp recommande les éléments suivants :

- SSH ne doit pas autoriser X11 Forwarding
- SSH ne doit pas autoriser le transfert de connexion TCP
- SSH ne doit pas autoriser les tunnels
- SSH ne doit pas accepter les variables d'environnement client

Ces recommandations de sécurité peuvent aider à empêcher toute connexion non autorisée à la machine du courtier de données.

Ajouter un nouveau courtier de données à un groupe

Il existe plusieurs façons de créer un nouveau courtier de données :

- Lors de la création d'une nouvelle relation de synchronisation

["Découvrez comment créer un nouveau courtier de données lors de la création d'une relation de synchronisation"](#).

- Dans la page **gérer les courtiers de données** en cliquant sur **Ajouter un nouveau courtier de données** qui crée le courtier de données dans un nouveau groupe
- À partir de la page **gérer les courtiers de données** en créant un nouveau courtier de données dans un groupe existant

Avant de commencer

- Vous ne pouvez pas ajouter de courtiers de données à un groupe qui gère une relation de synchronisation chiffrée.
- Si vous souhaitez créer un courtier en données au sein d'un groupe existant, le courtier en données doit être un courtier en données sur site ou le même type de courtier.

Par exemple, si un groupe inclut un courtier en données AWS, vous pouvez créer un courtier en données AWS ou un courtier en données sur site dans ce groupe. Vous ne pouvez pas créer de courtier en données Azure ou de courtier en données Google Cloud, car ils ne sont pas le même type de courtier.

Étapes pour créer un courtier de données dans un nouveau groupe

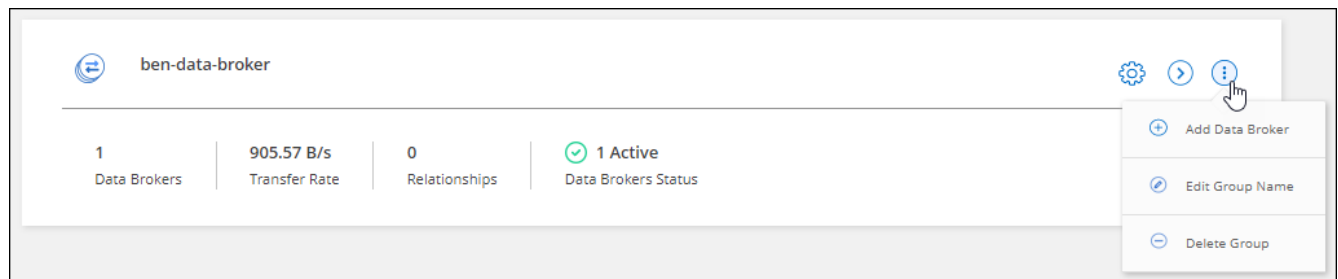
1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur **Ajouter un nouveau courtier de données**.
3. Suivez les invites pour créer le courtier de données.

Pour obtenir de l'aide, 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"](#)

Étapes pour créer un courtier de données dans un groupe existant

1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur le menu d'action et sélectionnez **Ajouter un courtier de données**.



3. Suivez les invites pour créer le courtier de données dans le groupe.

Pour obtenir de l'aide, reportez-vous aux pages suivantes :

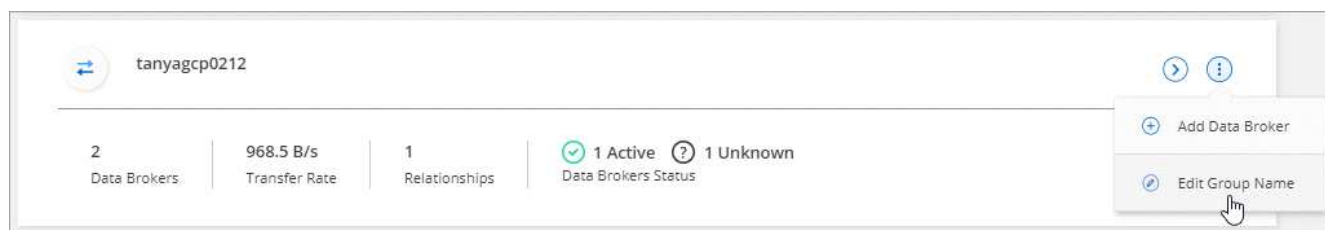
- ["Créer un courtier en données dans AWS"](#)
- ["Créer un courtier en données dans Azure"](#)
- ["Créer un courtier en données dans Google Cloud"](#)
- ["Installation du data broker sur un hôte Linux"](#)

Modifier le nom d'un groupe

Modifier le nom d'un groupe de courtiers de données à tout moment.

Étapes

1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur le menu d'action et sélectionnez **Modifier le nom du groupe**.



3. Entrez un nouveau nom et cliquez sur **Enregistrer**.

Résultat

Cloud Sync met à jour le nom du groupe de courtiers de données.

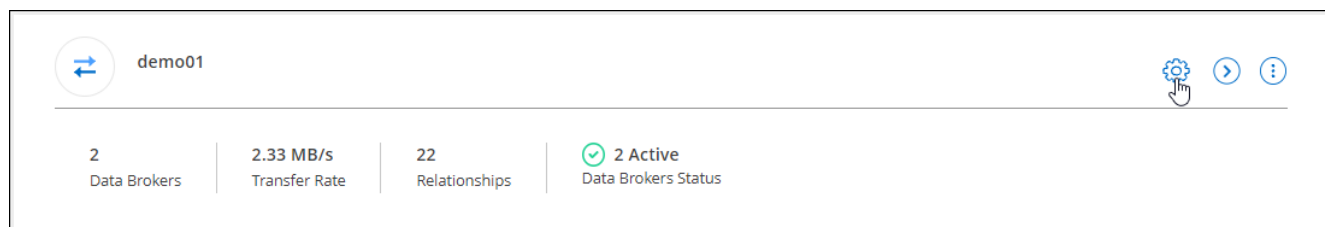
Configurez une configuration unifiée

Si une relation de synchronisation rencontre des erreurs lors du processus de synchronisation, l'unification de la simultanéité du groupe de courtiers de données peut aider à diminuer le nombre d'erreurs de synchronisation. Notez que les modifications apportées à la configuration du groupe peuvent affecter les performances en ralentissant le transfert.

Nous ne recommandons pas de modifier par vous-même la configuration. Consultez NetApp pour savoir quand modifier la configuration et comment la modifier.

Étapes

1. Cliquez sur **gérer les courtiers de données**.
2. Cliquez sur l'icône Paramètres d'un groupe de courtiers de données.



3. Modifiez les paramètres selon vos besoins, puis cliquez sur **Unify Configuration**.

Notez ce qui suit :

- Vous pouvez choisir les paramètres à modifier, mais vous n'avez pas besoin de les modifier simultanément.
- Une fois qu'une nouvelle configuration est envoyée à un courtier de données, le courtier redémarre automatiquement et utilise la nouvelle configuration.
- Un délai peut s'effectuer jusqu'à ce que cette modification soit visible dans l'interface de Cloud Sync.
- Si un courtier de données n'est pas en cours d'exécution, sa configuration ne change pas, car Cloud Sync ne peut pas communiquer avec lui. La configuration change après le redémarrage du courtier de données.
- Une fois la configuration unifiée définie, tous les nouveaux courtiers de données utilisent automatiquement la nouvelle configuration.

Déplacez les courtiers de données d'un groupe à l'autre


Déplacez un courtier de données d'un groupe à un autre si vous avez besoin d'accélérer les performances du groupe de courtiers de données cible.

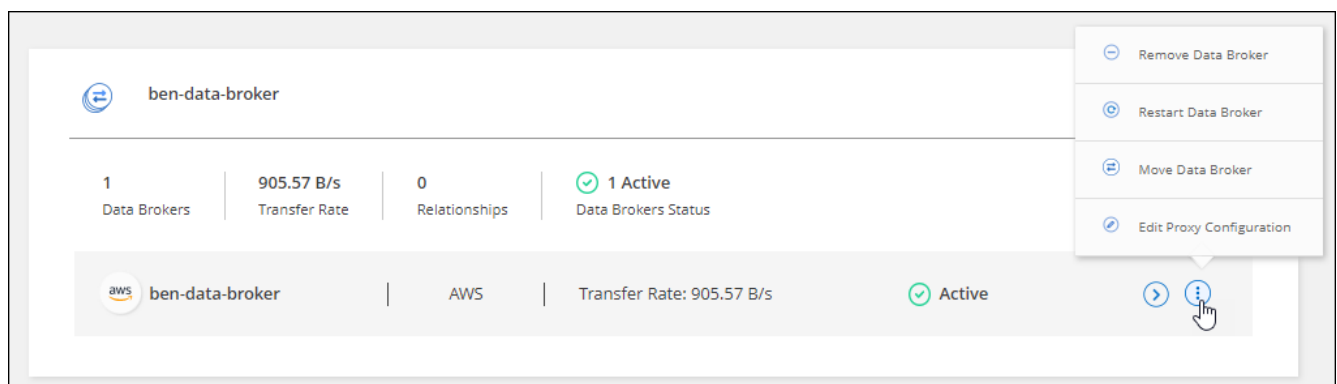
Par exemple, si un courtier de données ne gère plus une relation synchrone, vous pouvez facilement la déplacer vers un autre groupe gérant les relations de synchronisation.

Limites

- Si un groupe de courtiers de données gère une relation de synchronisation et qu'il n'y a qu'un seul courtier de données dans le groupe, vous ne pouvez pas transférer ce courtier de données vers un autre groupe.
- Vous ne pouvez pas déplacer un courtier de données vers ou depuis un groupe qui gère les relations de synchronisation chiffrées.
- Vous ne pouvez pas déplacer un courtier en données actuellement déployé.

Étapes

1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur  pour développer la liste des courtiers de données d'un groupe.
3. Cliquez sur le menu d'action d'un courtier de données et sélectionnez **déplacer le courtier de données**.



4. Créez un nouveau groupe de courtiers de données ou sélectionnez un groupe de courtiers de données existant.
5. Cliquez sur **déplacer**.


Résultat

Cloud Sync déplace le courtier en données vers un groupe de courtiers de données nouveau ou existant. S'il n'y a pas d'autres courtiers de données dans le groupe précédent, Cloud Sync le supprime.

Mettre à jour la configuration du proxy

Mettez à jour la configuration du proxy pour un courtier de données en ajoutant des détails sur une nouvelle configuration de proxy ou en modifiant la configuration de proxy existante.

Étapes

1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur  pour développer la liste des courtiers de données d'un groupe.
3. Cliquez sur le menu d'action d'un courtier de données et sélectionnez **Modifier la configuration du proxy**.
4. Spécifiez des détails sur le proxy : nom d'hôte, numéro de port, nom d'utilisateur et mot de passe.
5. Cliquez sur **mettre à jour**.

Résultat

Cloud Sync met à jour le courtier de données pour utiliser la configuration proxy pour l'accès à Internet.

Afficher la configuration d'un courtier de données

Vous pouvez consulter des détails sur un courtier de données pour identifier des éléments tels que son nom d'hôte, son adresse IP, son CPU et sa mémoire vive disponibles, etc.



Cloud Sync fournit les informations suivantes concernant un courtier en données :

- Informations de base : ID d'instance, nom d'hôte, etc
- Réseau : région, réseau, sous-réseau, IP privée, etc
- Logiciel : distribution Linux, version de courtier de données, etc
- Matériel : processeur et RAM
- Configuration : détails sur les deux types de processus principaux du courtier de données : scanner et transfert



Le scanner numérise la source et la cible et décide de ce qui doit être copié. Le transfert effectue la copie réelle. L'équipe NetApp peut utiliser ces détails de configuration pour suggérer des actions permettant d'optimiser les performances.

Étapes

1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur  pour développer la liste des courtiers de données d'un groupe.
3. Cliquez sur  pour afficher les détails d'un courtier de données.

tanyagcp0212

2 Data Brokers | 968.5 B/s Transfer Rate | 1 Relationships | 1 Active 1 Unknown Data Brokers Status

	tanyagcp0212	GCP	Transfer Rate: 968.5 B/s	Active
Information	5fc766b3d3e3664b9e116... Broker ID	288871247573080556 Instance ID	tanyagcp0212-mnx-data-... Host Name	cloudsync-dev-214020 Project ID
Network	us-east1-b Region	default Network	255.255.240.0 Subnet	10.142.0.37 Private IP
Software	linux Linux Distribution & Version	1.5.4 Vault Version	14.15.1 Node Version	1.3.0.18650-73f960d-integ Data Broker Version
Hardware	4 Available CPUs	62.22 MB Available RAM		
Configuration	50 Scanner Concurrency	4 Scanner CPUs	50 Transferer Concurrency	4 Transferer CPUs

Résoudre les problèmes avec un courtier de données

Cloud Sync affiche un statut pour chaque courtier de données qui peut vous aider à résoudre les problèmes.

Étapes

1. Identifiez tous les courtiers de données dont l'état est « Inconnu » ou « en échec ».

tanyagcp0212

2 Data Brokers | 968.5 B/s Transfer Rate | 1 Relationships | 1 Active 1 Unknown Data Brokers Status

	tanyagcp0212	GCP	Transfer Rate: 968.5 B/s	Active
tanya1	ONPREM	Transfer Rate: N/A	Unknown	

2. Placez le pointeur de la souris sur le **i** pour voir la raison de l'échec.
3. Corrigez le problème.

Par exemple, vous devrez peut-être redémarrer le courtier en données si celui-ci est hors ligne, ou supprimer le courtier en données si le déploiement initial a échoué.

Supprimer un courtier de données d'un groupe


Vous pouvez supprimer un courtier de données d'un groupe s'il n'est plus nécessaire ou si le déploiement

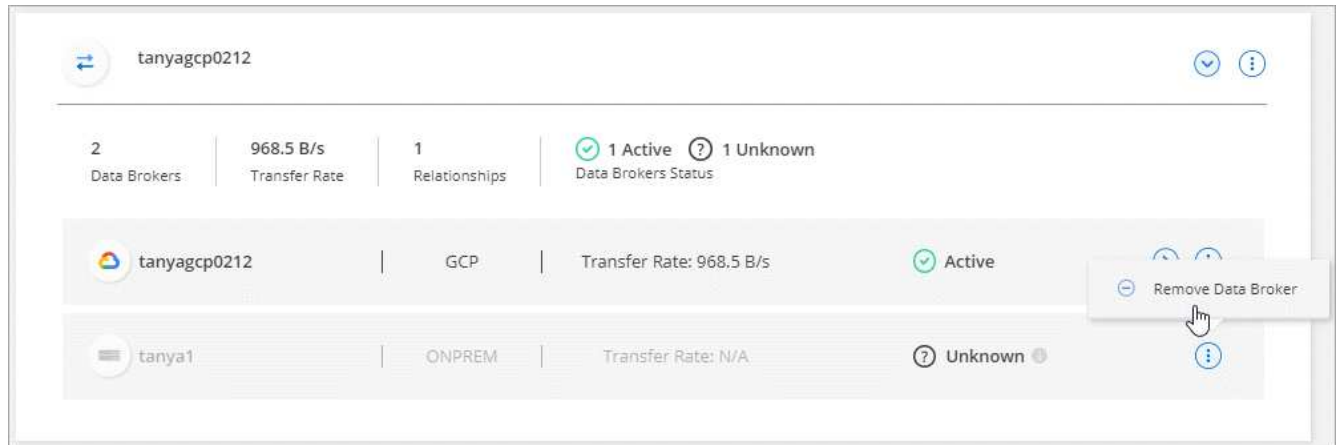
initial a échoué. Cette action supprime uniquement le courtier en données des enregistrements de Cloud Sync. Vous devrez supprimer manuellement le courtier en données et toutes les ressources cloud supplémentaires.

Ce que vous devez savoir

- Cloud Sync supprime un groupe lorsque vous supprimez le dernier courtier de données du groupe.
- Vous ne pouvez pas supprimer le dernier courtier de données d'un groupe s'il existe une relation utilisant ce groupe.

Étapes

1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur  pour développer la liste des courtiers de données d'un groupe.
3. Cliquez sur le menu d'action d'un courtier de données et sélectionnez **Supprimer le courtier de données**.



4. Cliquez sur **Supprimer le courtier de données**.

Résultat

Cloud Sync supprime le courtier de données du groupe.

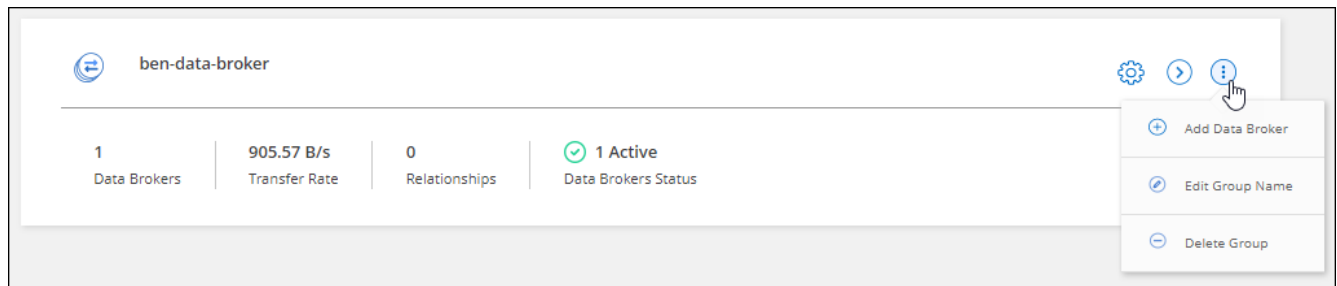
Supprimer un groupe de courtier de données

Si un groupe de courtiers de données ne gère plus de relations de synchronisation, vous pouvez supprimer le groupe, qui supprime tous les courtiers de données de Cloud Sync.

Les courtiers de données supprimés par Cloud Sync ne sont supprimés que des enregistrements de Cloud Sync. Vous devrez supprimer manuellement l'instance de courtier en données de votre fournisseur de cloud, ainsi que toutes les ressources cloud supplémentaires.

Étapes

1. Cliquez sur **Sync > gérer les courtiers de données**.
2. Cliquez sur le menu d'action et sélectionnez **Supprimer le groupe**.



3. Pour confirmer, entrez le nom du groupe et cliquez sur **Supprimer le groupe**.

Résultat

Cloud Sync supprime les courtiers de données et supprime le groupe.

Création et affichage de rapports pour ajuster votre configuration

Créez et consultez des rapports pour obtenir des informations utiles avec l'aide du personnel NetApp afin de régler la configuration d'un courtier de données et d'améliorer les performances.

Chaque rapport fournit des détails détaillés sur un chemin dans une relation de synchronisation. Par exemple, le rapport d'un système de fichiers indique le nombre de répertoires et de fichiers qu'il y a, la répartition de la taille du fichier, la profondeur et la largeur des répertoires, et plus encore.

Création de rapports

Chaque fois que vous créez un rapport, Cloud Sync analyse le chemin, puis compile les informations dans un rapport.

Étapes

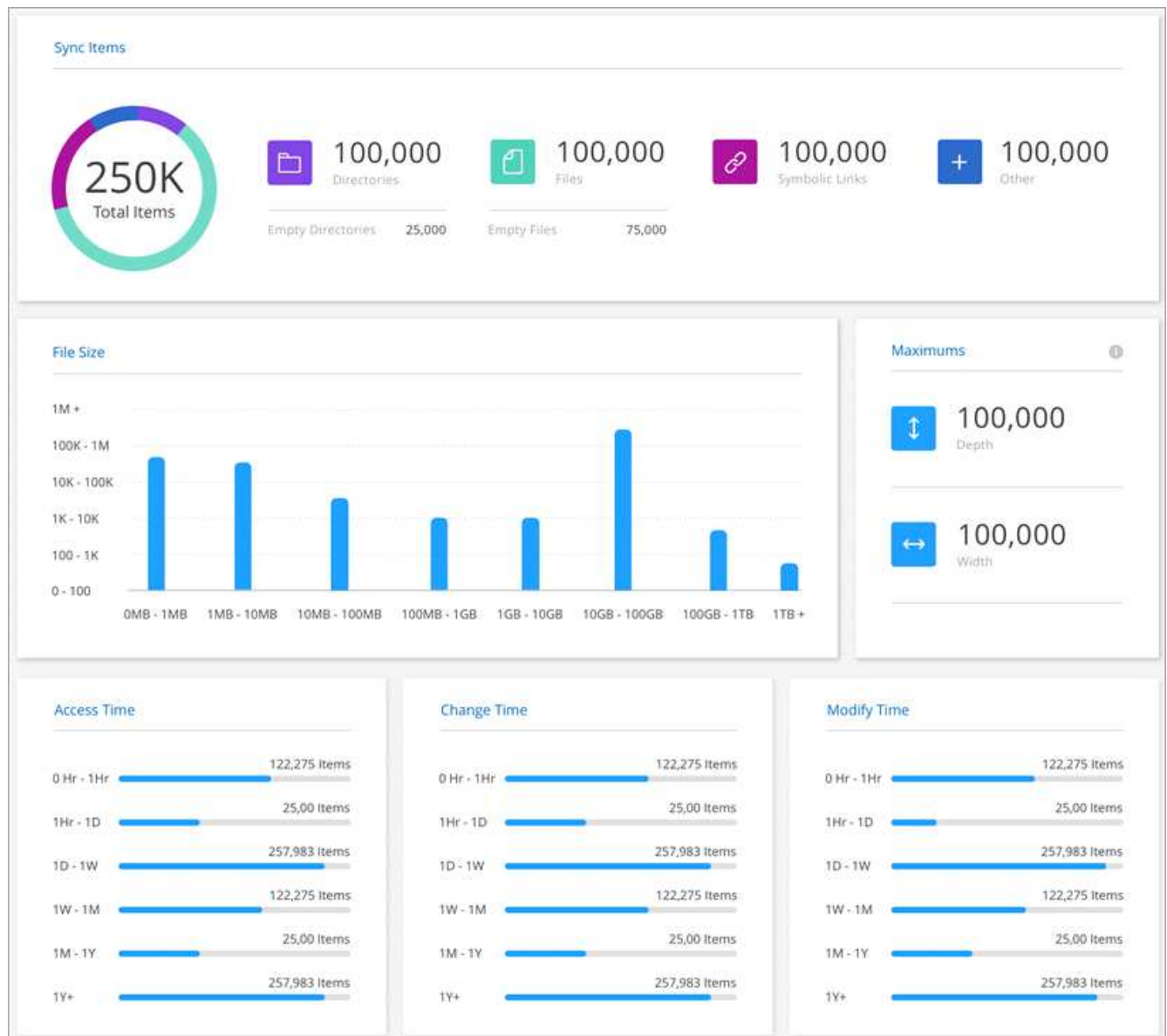
1. Cliquez sur **Sync > Rapports**.

Les chemins (source ou cible) de chacune de vos relations de synchronisation s'affichent dans une table.

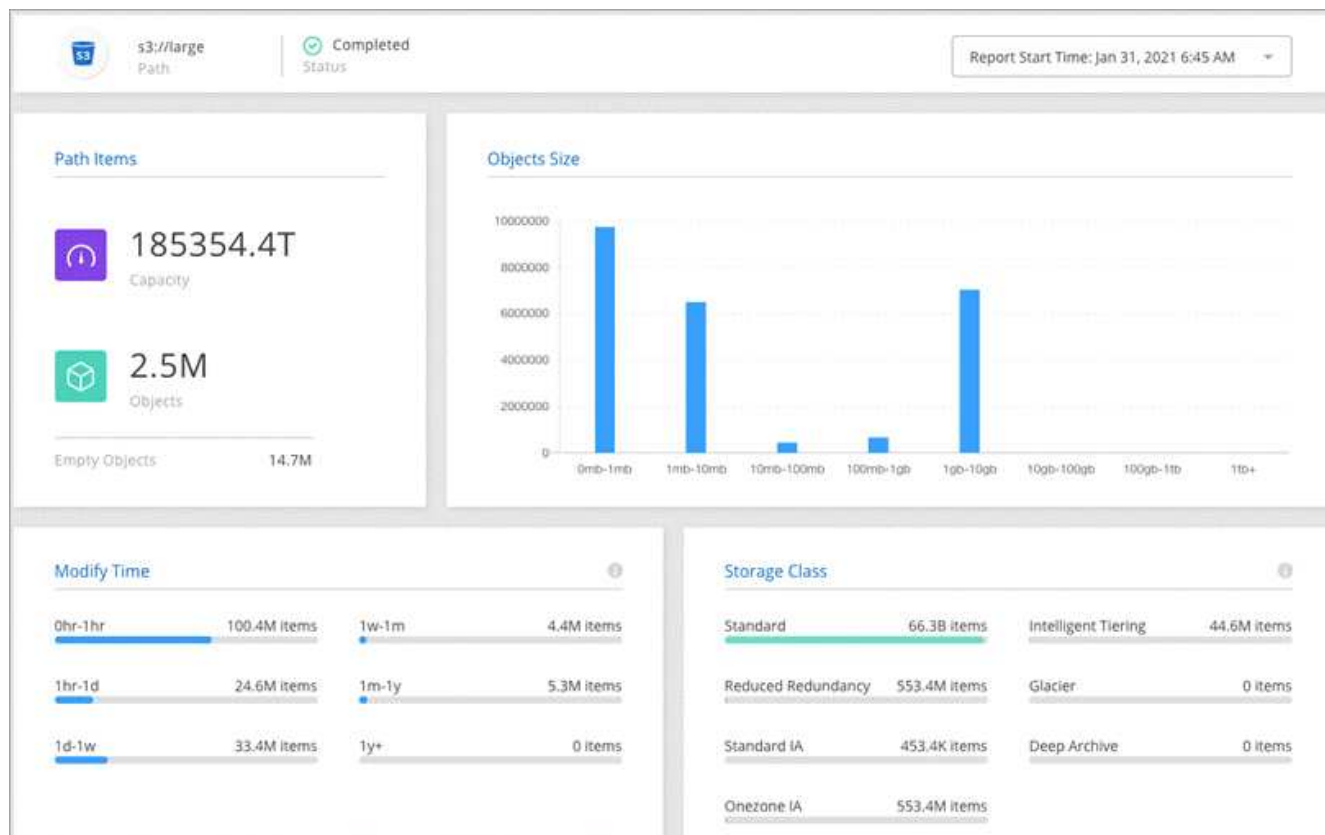
2. Dans la colonne **Rapports actions**, allez à un chemin spécifique et cliquez sur **Créer**, ou cliquez sur le menu d'action et sélectionnez **Créer nouveau**.

3. Lorsque le rapport est prêt, cliquez sur le menu d'action et sélectionnez **Affichage**.

Voici un exemple de rapport pour un chemin de système de fichiers.



Et voici un exemple de rapport sur le stockage objet.

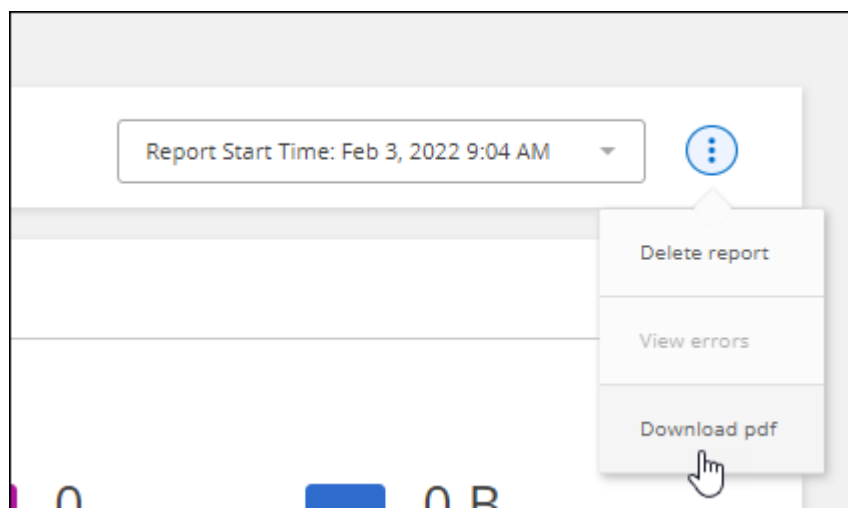


Téléchargement de rapports

Vous pouvez télécharger un rapport au format PDF pour le visualiser hors ligne ou le partager.

Étapes

1. Cliquez sur **Sync > Rapports**.
2. Dans la colonne **Rapports actions**, cliquez sur le menu d'action et sélectionnez **Affichage**.
3. Dans le coin supérieur droit du rapport, cliquez sur le menu d'action et sélectionnez **Télécharger PDF**.



Affichage des erreurs de rapport

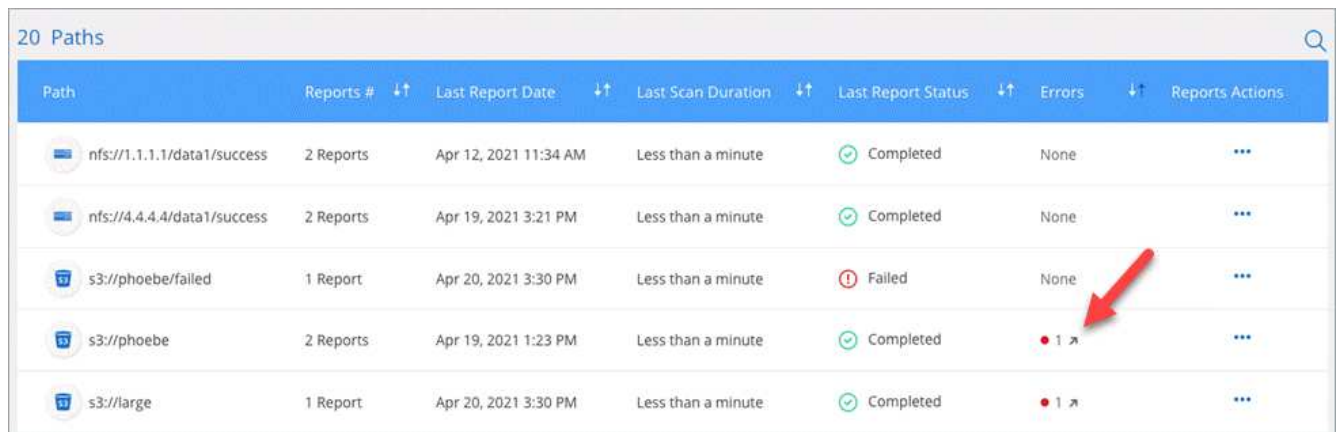
Le tableau chemins identifie si des erreurs sont présentes dans le rapport le plus récent. Une erreur identifie un problème rencontré par Cloud Sync lors de la numérisation du chemin.

Par exemple, un rapport peut contenir des erreurs d'autorisation refusée. Ce type d'erreur peut affecter la capacité de Cloud Sync à analyser l'ensemble des fichiers et des répertoires.

Après avoir vu la liste des erreurs, vous pouvez résoudre les problèmes et exécuter à nouveau le rapport.

Étapes

1. Cliquez sur **Sync > Rapports**.
2. Dans la colonne **erreurs**, identifiez si des erreurs sont présentes dans un rapport.
3. Si des erreurs sont présentes, cliquez sur la flèche en regard du nombre d'erreurs.



Path	Reports #	Last Report Date	Last Scan Duration	Last Report Status	Errors	Reports Actions
nfs://1.1.1.1/data1/success	2 Reports	Apr 12, 2021 11:34 AM	Less than a minute	Completed	None	...
nfs://4.4.4.4/data1/success	2 Reports	Apr 19, 2021 3:21 PM	Less than a minute	Completed	None	...
s3://phoebe/failed	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Failed	None	...
s3://phoebe	2 Reports	Apr 19, 2021 1:23 PM	Less than a minute	Completed	1	...
s3://large	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Completed	1	...

4. Utilisez les informations de l'erreur pour corriger le problème.

Après avoir résolu le problème, l'erreur ne devrait pas apparaître lors de la prochaine exécution du rapport.

Suppression de rapports

Vous pouvez supprimer un rapport contenant une erreur que vous avez corrigée ou si le rapport est associé à une relation de synchronisation que vous avez supprimée.

Étapes

1. Cliquez sur **Sync > Rapports**.
2. Dans la colonne **Rapports actions**, cliquez sur le menu d'action d'un chemin et sélectionnez **Supprimer le dernier rapport** ou **Supprimer tous les rapports**.
3. Confirmez que vous souhaitez supprimer le ou les rapports.

Désinstallation du courtier de données

Si nécessaire, exécutez un script de désinstallation pour supprimer le courtier de données et les packages et répertoires créés lors de l'installation du courtier de données.

Étapes

1. Connectez-vous à l'hôte du courtier de données.

2. Accédez au répertoire du courtier de données : `/opt/netapp/databroker`

3. Exécutez les commandes suivantes :

```
chmod +x uninstaller-DataBroker.sh  
./uninstaller-DataBroker.sh
```

4. Appuyez sur 'y' pour confirmer la désinstallation.

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.