



# **Commencez**

## Cloud Data Sense

NetApp  
December 12, 2022

This PDF was generated from <https://docs.netapp.com/fr-fr/cloud-manager-data-sense/concept-cloud-compliance.html> on December 12, 2022. Always check docs.netapp.com for the latest.

# Table des matières

- Commencez ..... 1
  - Tout savoir sur le sens des données du cloud ..... 1
  - Déployez des données adaptées au cloud ..... 8
  - Activez la numérisation sur vos sources de données ..... 40
  - Intégrez Active Directory avec le sens des données dans le cloud ..... 85
  - Configurez les licences pour Cloud Data Sense ..... 88
  - Les questions les plus fréquemment posées à propos des données du cloud sont pertinentes ..... 94

# Commencez

## Tout savoir sur le sens des données du cloud

Cloud Data Sense est un service de gouvernance des données pour BlueXP (anciennement Cloud Manager) qui analyse vos sources de données sur site et dans le cloud de votre entreprise pour mapper et classer les données, et identifier des informations privées. Cela peut réduire les risques liés à la sécurité et à la conformité, diminuer les coûts de stockage et vous aider dans vos projets de migration des données.

["Découvrez les utilisations de Cloud Data Sense".](#)

### Caractéristiques

Cloud Data Sense utilise l'intelligence artificielle (IA), le traitement du langage naturel (NLP) et l'apprentissage machine (ML) pour comprendre le contenu qu'il analyse afin d'extraire les entités et de catégoriser le contenu en conséquence. Cela permet à Data Sense de fournir les domaines de fonctionnalité suivants.

#### Préservez la conformité

Data SENSE fournit plusieurs outils qui peuvent vous aider dans vos efforts de conformité. Vous pouvez utiliser Data Sense pour :

- Identifier les informations à caractère personnel
- Identifier une vaste portée des données personnelles sensibles, conformément aux réglementations en matière de confidentialité, RGPD, CCPA, PCI et HIPAA.
- Répondez aux demandes d'accès aux données (DSAR, Data Subject Access Requests) en fonction de votre nom ou de votre adresse e-mail.
- Identifiez si des identificateurs uniques de vos bases de données se trouvent dans des fichiers d'autres référentiels, en faisant simplement votre propre liste de « données personnelles » identifiées dans les analyses de détection de données.
- Notifier les utilisateurs BlueXP par courrier électronique lorsque des fichiers contiennent certains PII (vous définissez ce critère à l'aide de ["Stratégies"](#)) de sorte que vous puissiez décider d'un plan d'action.

#### Renforcez la sécurité

Le sens des données permet d'identifier les données susceptibles d'être consultées à des fins criminelles. Vous pouvez utiliser Data Sense pour :

- Identifiez tous les fichiers et répertoires (partages et dossiers) avec les autorisations ouvertes exposées à l'ensemble de votre organisation ou au public.
- Identifiez les données sensibles qui se trouvent en dehors de l'emplacement initial dédié.
- Respectez les règles de conservation des données.
- Utilisez *Politiques* pour avertir automatiquement le personnel de sécurité de nouveaux problèmes de sécurité afin qu'il puisse agir immédiatement.
- Ajoutez des balises personnalisées aux fichiers (par exemple, "doit être déplacé") et affectez un utilisateur BlueXP pour que cette personne puisse posséder des mises à jour des fichiers.

- Afficher et modifier "[Étiquettes Azure information protection \(AIP\)](#)" dans vos fichiers.

## Optimiser l'utilisation du stockage

Data Sense fournit des outils qui peuvent vous aider dans votre coût total de possession (TCO) du stockage. Vous pouvez utiliser Data Sense pour :

- Amélioration de l'efficacité du stockage grâce à l'identification des données dupliquées ou non liées à l'activité. Vous pouvez utiliser ces informations pour décider si vous voulez déplacer ou supprimer certains fichiers.
- Supprimez des fichiers qui semblent non sécurisés ou trop risqués pour l'éviter dans votre système de stockage, ou qui ont été identifiés en double. Vous pouvez utiliser *Politiques* pour supprimer automatiquement des fichiers qui correspondent à certains critères.
- Réduisez les coûts du stockage en identifiant les données inactives que vous pouvez déplacer vers un stockage objet moins coûteux. "[En savoir plus sur le Tiering](#)".

## Accélérez la migration des données

Data Sense peut être utilisé pour analyser les données sur site avant de les migrer vers le cloud public ou privé. Vous pouvez utiliser Data Sense pour :

- Permet d'afficher la taille des données et si l'une des données contient des informations sensibles avant de les déplacer.
- Filtrez les données source (en fonction de plus de 25 types de critères) pour pouvoir déplacer uniquement les fichiers requis vers la destination. Les données inutiles ne sont pas déplacées.
- Déplacez, copiez ou synchronisez uniquement les données requises dans le référentiel cloud de manière automatique et continue.

## Sources de données prises en charge

Cloud Data Sense peut analyser et analyser des données structurées et non structurées à partir de plusieurs types de sources de données :

### NetApp:

- Cloud Volumes ONTAP (déployé dans AWS, Azure ou GCP)
- Clusters ONTAP sur site
- StorageGRID
- Azure NetApp Files
- Amazon FSX pour ONTAP
- Cloud Volumes Service pour Google Cloud

### Non NetApp:

- Dell EMC Isilon
- Pure Storage
- Nutanix
- Tout autre fournisseur de stockage

## Cloud:

- Amazon S3
- Blob d'Azure
- Google Cloud Storage
- OneDrive
- SharePoint Online
- SharePoint sur site (SharePoint Server)
- Google Drive

## Bases de données:

- Amazon Relational Database Service (Amazon RDS)
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP HANA
- Serveur SQL (MSSQL)

Data Sense prend en charge les versions NFS 3.x, 4.0 et 4.1 et CIFS 1.x, 2.0, 2.1 et 3.0.

## Le coût

- Le coût d'utilisation des données du cloud SENSE dépend de la quantité de données que vous scannez. Les 1 premiers To de données analysés par Data Sense dans un espace de travail BlueXP sont gratuits. Cela inclut toutes les données issues de tous les environnements de travail et de toutes les sources de données. Un abonnement à AWS, Azure, GCP Marketplace ou une licence BYOL de NetApp est requis pour continuer l'analyse des données après ce point. Voir "[tarifs](#)" pour plus d'informations.

["Découvrez comment obtenir des licences Cloud Data Sense"](#).

- Pour installer Cloud Data dans le cloud, il faut déployer une instance cloud, ce qui entraîne des frais supplémentaires du fournisseur cloud chargé du déploiement. Voir [type d'instance déployé pour chaque fournisseur cloud](#). L'installation de Data Sense sur un système sur site est gratuite.
- Cloud Data sens requiert que vous ayez déployé un connecteur BlueXP. Dans de nombreux cas, vous disposez déjà d'un connecteur en raison d'autres services et stockages que vous utilisez dans BlueXP. L'instance de connecteur entraîne des frais supplémentaires du fournisseur cloud sur lequel elle est déployée. Voir la "[type d'instance déployé pour chaque fournisseur cloud](#)". L'installation du connecteur sur un système sur site est gratuite.

## Coûts de transfert de données

Les coûts de transfert de données dépendent de votre configuration. Si l'instance de Cloud Data SENSE et la source de données se trouvent dans la même zone de disponibilité et la même région, aucun coût de transfert de données n'est observé. Mais si la source de données, telle qu'un système Cloud Volumes ONTAP ou un compartiment S3, se trouve dans une *autre* zone ou région de disponibilité, vous serez facturé par votre fournisseur cloud pour les coûts de transfert de données. Consultez ces liens pour en savoir plus :

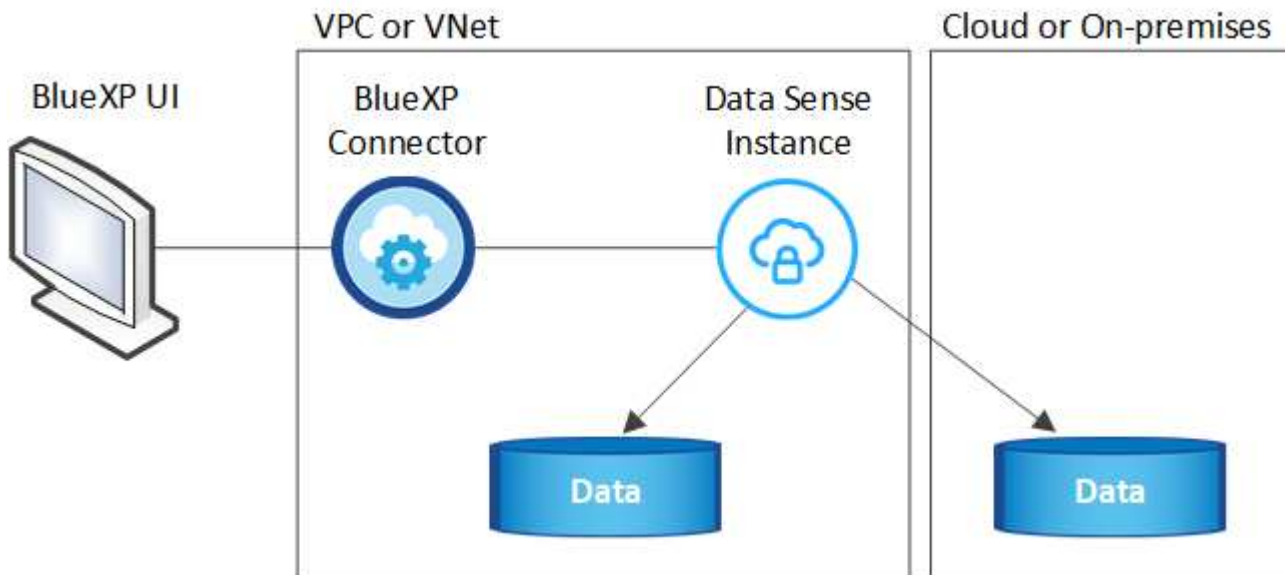
- ["AWS : tarification Amazon EC2"](#)
- ["Microsoft Azure : détails de la tarification de la bande passante"](#)
- ["Google Cloud : tarification du service de transfert du stockage"](#)

## Instance Cloud Data SENSE

Lorsque vous déployez Data Sense dans le cloud, BlueXP déploie l'instance dans le même sous-réseau que le connecteur. ["En savoir plus sur les connecteurs."](#)



Si le connecteur est installé sur site, il déploie l'instance Cloud Data Sense dans le même VPC ou VNet que le premier système Cloud Volumes ONTAP de la demande. Vous pouvez également installer Data Sense sur site.



Voici la liste des éléments suivants pour l'instance par défaut :

- Dans AWS, Cloud Data Sense s'exécute sur un ["m5.4xlarge instance"](#) Avec un disque GP2 de 500 Go. L'image du système d'exploitation est Amazon Linux 2 (Red Hat 7.3.1).

Dans les régions où m5.4xlarge n'est pas disponible, Data Sense s'exécute sur une instance m4.4xlarge au lieu de.

- Dans Azure, Cloud Data Sense s'exécute sur un ["Machine virtuelle standard\\_D16s\\_v3"](#) Avec un disque de 512 Go. L'image du système d'exploitation est CentOS 7.8.
- Dans GCP, Cloud Data Sense s'exécute sur un ["n2-standard-16 VM"](#) Avec disque persistant standard de 512 Go. L'image du système d'exploitation est CentOS 7.9.

Dans les régions où n2-standard-16 n'est pas disponible, Data Sense s'exécute sur une machine virtuelle n2d-standard-16 ou n1-standard-16.

- L'instance s'appelle *CloudCompliance* avec un hachage (UUID) généré concaténé. Par exemple : *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Une seule instance de détection des données est déployée par connecteur.
- Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance a accès à Internet.



L'instance doit rester en cours d'exécution à tout moment, car Cloud Data SENSE analyse en continu les données.

## Utilisation d'un type d'instance plus petit

Vous pouvez déployer Data Sense sur un système avec moins de processeurs et moins de RAM, mais il ya certaines limites quand l'utilisation de ces systèmes moins puissants.

Taille du système	Caractéristiques	Limites
Grand (par défaut)	16 PROCESSEURS, 64 GO DE RAM, 500 GO DE SSD	Aucune
Moyen	8 PROCESSEURS, 32 GO DE RAM, 200 GO DE SSD	Numérisation plus lente et numérisation jusqu'à 1 million de fichiers uniquement.
Petit	8 PROCESSEURS, 16 GO DE RAM, 100 GO DE SSD	Mêmes limites que « Moyen », plus la capacité d'identifier "noms des sujets de données" les fichiers internes sont désactivés.

Si vous souhaitez utiliser l'un de ces systèmes plus petits, envoyez un e-mail à l'adresse [ng-contact-data-sense@netapp.com](mailto:ng-contact-data-sense@netapp.com) pour obtenir de l'aide. Nous devons nous aider à déployer ces plus petites configurations cloud.

Pour déployer Data Sense sur site, il vous suffit d'utiliser un hôte Linux avec des spécifications moindres. Vous n'avez pas besoin de contacter NetApp pour obtenir de l'aide.

## Fonctionnement du Cloud Data Sense

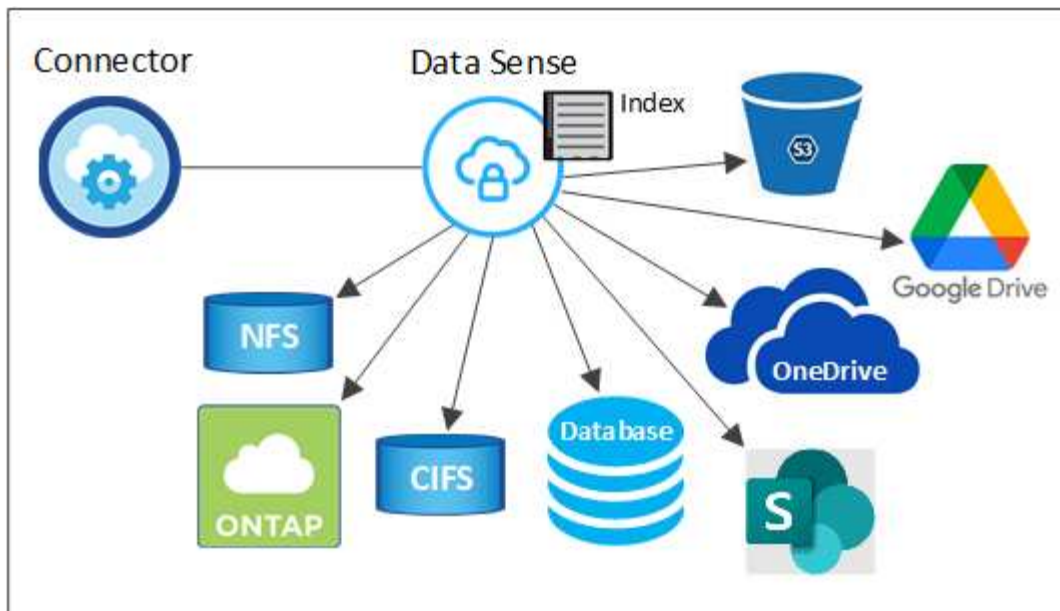
À un niveau élevé, Cloud Data sens fonctionne comme suit :

1. Vous déployez une instance de Data Sense dans BlueXP.
2. Vous activez la cartographie de haut niveau ou la numérisation de haut niveau sur une ou plusieurs sources de données.
3. La détection des données analyse les données à l'aide d'un processus d'IA.
4. Vous utilisez les tableaux de bord et les outils de génération de rapports fournis pour vous aider dans vos efforts de conformité et de gouvernance.

## Fonctionnement des acquisitions

Une fois que vous avez activé Cloud Data SENSE et sélectionné les volumes, compartiments, schémas de base de données ou données utilisateur OneDrive ou SharePoint que vous souhaitez analyser, l'analyse des données démarre immédiatement pour identifier les données personnelles et sensibles. Il mappe les données de votre organisation, classe chaque fichier et identifie et extrait des entités et des modèles prédéfinis dans les données. Le résultat de l'analyse est un index des informations personnelles, des données personnelles sensibles, des catégories de données et des types de fichiers.

Le Data Sense se connecte aux données comme n'importe quel autre client en montant les volumes NFS et CIFS. Les volumes NFS sont automatiquement accessibles en lecture seule, tandis que vous devez fournir des identifiants Active Directory pour analyser les volumes CIFS.



Après l'analyse initiale, Data Sense analyse en continu vos données pour détecter les modifications incrémentielles (c'est pourquoi il est important de maintenir l'instance en cours d'exécution).

Vous pouvez activer et désactiver les analyses au niveau du volume, au niveau du compartiment, au niveau du schéma de la base de données, au niveau utilisateur OneDrive et au niveau du site SharePoint.

### Quelle est la différence entre les acquisitions de mappage et de classification

Cloud Data SENSE vous permet d'exécuter une analyse générale « mapping » sur certaines sources de données. La cartographie ne fournit qu'une vue d'ensemble de haut niveau de vos données, tandis que Classification permet une analyse approfondie de vos données. Le mappage peut être effectué très rapidement sur vos sources de données car il n'accède pas aux fichiers pour voir les données à l'intérieur.

De nombreux utilisateurs apprécient cette fonctionnalité car ils souhaitent analyser rapidement leurs données afin d'identifier les sources de données qui nécessitent davantage de recherche. Ils ne peuvent ensuite activer des analyses de classification que sur les sources ou volumes de données requis.

Le tableau ci-dessous présente certaines des différences :

Fonction	Classement	Mappage
Vitesse de numérisation	Lentes	Rapides
Liste des types de fichiers et de la capacité utilisée	Oui.	Oui.
Nombre de fichiers et capacité utilisée	Oui.	Oui.
Âge et taille des fichiers	Oui.	Oui.
Exécution d'un "Rapport de mappage de données"	Oui.	Oui.
Page Data Investigation pour afficher les détails du fichier	Oui.	Non
Rechercher des noms dans les fichiers	Oui.	Non
Création "stratégies" fournissant des résultats de recherche personnalisés	Oui.	Non



Fonction	Classement	Mappage
Catégoriser les données à l'aide d'étiquettes AIP et de balises d'état	Oui.	Non
Copier, supprimer et déplacer des fichiers source	Oui.	Non
Possibilité d'exécuter d'autres rapports	Oui.	Non

## Informations fournies par Cloud Data Sense

Data Sense collecte, index et attribue des catégories à vos données (fichiers). Les données que les index Data Sense incluent les éléments suivants :

### Métadonnées standard

Cloud Data Sense collecte des métadonnées standard sur les fichiers : le type de fichier, sa taille, ses dates de création et de modification, etc.

### Données personnelles

Informations personnelles identifiables telles que les adresses électroniques, les numéros d'identification ou les numéros de carte de crédit. ["En savoir plus sur les données personnelles"](#).

### Données personnelles sensibles

Des types spéciaux d'informations sensibles, comme les données de santé, l'origine ethnique ou les opinions politiques, tels que définis par le RGPD et d'autres réglementations sur la confidentialité. ["En savoir plus sur les données personnelles sensibles"](#).

### Catégories

Cloud Data SENSE répartit les données analysées et les divise en différents types de catégories. Les catégories sont des rubriques basées sur l'analyse par IA du contenu et des métadonnées de chaque fichier. ["En savoir plus sur les catégories"](#).

### Types

Cloud Data SENSE affecte les données analysées et les divise par type de fichier. ["En savoir plus sur les types"](#).

### Reconnaissance de l'entité de nom

Cloud Data Sense utilise l'IA pour extraire les noms des personnes physiques des documents. ["Découvrez comment répondre aux demandes d'accès aux données"](#).

## Présentation du réseau

BlueXP déploie l'instance Cloud Data Sense avec un groupe de sécurité qui active les connexions HTTP entrantes à partir de l'instance de connecteur.

Si vous utilisez BlueXP en mode SaaS, la connexion à BlueXP est assurée par HTTPS. Les données privées envoyées entre votre navigateur et l'instance Data Sense sont sécurisées par un cryptage de bout en bout, ce qui signifie que NetApp et des tiers ne peuvent pas les lire.

Les règles sortantes sont complètement ouvertes. Un accès Internet est nécessaire pour installer et mettre à niveau le logiciel Data Sense et pour envoyer des mesures d'utilisation.

Si vous avez des exigences de mise en réseau strictes, ["Découvrez les terminaux hébergés dans le cloud Data et leurs contacts"](#).

## Accès des utilisateurs aux informations de conformité

Le rôle attribué à chaque utilisateur offre différentes fonctionnalités dans BlueXP et dans Cloud Data Sense :

- Un **Account Admin** peut gérer les paramètres de conformité et afficher les informations de conformité pour tous les environnements de travail.
- Un **Workspace Admin** peut gérer les paramètres de conformité et afficher les informations de conformité uniquement pour les systèmes auxquels ils disposent d'autorisations d'accès. Si un administrateur d'espace de travail ne peut pas accéder à un environnement de travail dans BlueXP, il ne peut pas voir d'informations de conformité pour l'environnement de travail dans l'onglet Data Sense.
- Les utilisateurs disposant du rôle **Compliance Viewer** peuvent uniquement afficher les informations de conformité et générer des rapports pour les systèmes auxquels ils sont autorisés à accéder. Ces utilisateurs ne peuvent pas activer/désactiver la lecture des volumes, compartiments ou schémas de base de données. Ces utilisateurs ne peuvent pas non plus copier, déplacer ou supprimer des fichiers.

"[En savoir plus sur les rôles BlueXP](#)" et comment "[ajoutez des utilisateurs avec des rôles spécifiques](#)".

## Déployez des données adaptées au cloud

### Déployez les données du cloud dans le cloud

Déployez ce sens en quelques étapes dans le cloud.

Notez que vous pouvez également "[Déployer Data Sense sur un hôte Linux avec accès à Internet](#)". Le type d'installation peut être une bonne option si vous préférez analyser les systèmes ONTAP sur site à l'aide d'une instance Data Sense également située sur site, mais ce n'est pas une exigence. Le logiciel fonctionne exactement de la même manière quelle que soit la méthode d'installation choisie.

### Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

#### Créer un connecteur

Si vous n'avez pas encore de connecteur, créez-en un maintenant. Voir "[Création d'un connecteur dans AWS](#)", "[Création d'un connecteur dans Azure](#)", ou "[Création d'un connecteur dans GCP](#)".

Vous pouvez également "[Déployez le connecteur sur site](#)" Sur un hôte Linux de votre réseau ou dans le cloud.

2

#### Passer en revue les prérequis

Assurez-vous que votre environnement est conforme aux conditions préalables. Cela inclut l'accès Internet sortant pour l'instance, la connectivité entre le connecteur et Cloud Data SENSE sur le port 443, etc. [Voir la liste complète](#).

La configuration par défaut requiert 16 vCPU pour l'instance de Cloud Data Sense. Voir "[plus de détails sur le type d'instance](#)".

### 3

#### Déployez des données adaptées au cloud

Lancez l'assistant d'installation pour déployer l'instance Cloud Data SENSE dans le cloud.

### 4

#### Abonnez-vous au service Cloud Data Sense

Les 1 premiers To de données scanners Cloud Data SENSE dans BlueXP sont gratuits. Un abonnement BlueXP via votre fournisseur cloud Marketplace, ou une licence BYOL auprès de NetApp, est nécessaire pour continuer à analyser les données après ce point.

#### Créer un connecteur

Si vous n'avez pas encore de connecteur, créez-en un chez votre fournisseur cloud. Voir "[Création d'un connecteur dans AWS](#)" ou "[Création d'un connecteur dans Azure](#)", ou "[Création d'un connecteur dans GCP](#)". Dans la plupart des cas, vous aurez probablement configuré un connecteur avant d'essayer d'activer le Cloud Data SENSE "[Les fonctionnalités BlueXP nécessitent un connecteur](#)", mais il y a des cas où vous devrez en configurer un maintenant.

Dans certains cas, vous devez utiliser un connecteur déployé dans un fournisseur de cloud spécifique :

- Pour l'analyse des données dans Cloud Volumes ONTAP dans AWS, Amazon FSX pour ONTAP ou dans des compartiments AWS S3, vous utilisez un connecteur dans AWS.
- Pour analyser les données dans Cloud Volumes ONTAP dans Azure ou dans Azure NetApp Files, vous utilisez un connecteur dans Azure.
  - Pour Azure NetApp Files, il doit être déployé dans la même région que les volumes que vous souhaitez analyser.
- Pour l'analyse des données dans Cloud Volumes ONTAP dans GCP, vous utilisez un connecteur dans GCP.

Vous pouvez analyser les systèmes ONTAP sur site, les partages de fichiers non NetApp, le stockage objet S3 générique, les bases de données, les dossiers OneDrive, les comptes SharePoint et les comptes Google Drive à l'aide de ces connecteurs cloud.

Notez que vous pouvez également "[Déployez le connecteur sur site](#)" Sur un hôte Linux de votre réseau ou dans le cloud. Certains utilisateurs qui prévoient d'installer Data Sense sur site peuvent également choisir d'installer le connecteur sur site.

Comme vous pouvez le voir, il peut y avoir des situations où vous devez utiliser "[Plusieurs connecteurs](#)".

#### Soutien de la région du gouvernement

Cloud Data Sense est pris en charge lorsque le connecteur est déployé dans une région gouvernementale (AWS GovCloud, Azure Government ou Azure DoD). Lorsqu'il est déployé de cette manière, Data SENSE présente les restrictions suivantes :

- Les comptes OneDrive, les comptes SharePoint et Google Drive ne peuvent pas être analysés.
- Impossible d'intégrer la fonctionnalité de label Microsoft Azure information protection (AIP).

#### Passer en revue les prérequis

Avant de déployer le cloud Data Sense dans le cloud, lisez les conditions suivantes pour vous assurer que

vous bénéficiez d'une configuration prise en charge.

### Activation de l'accès Internet sortant à partir du Cloud Data SENSE

Cloud Data Sense requiert un accès Internet sortant. Si votre réseau virtuel ou physique utilise un serveur proxy pour l'accès à Internet, assurez-vous que l'instance de détection de données dispose d'un accès Internet sortant pour contacter les points de terminaison suivants. Lorsque vous déployez Data Sense dans le cloud, il se trouve dans le même sous-réseau que le connecteur.

Consultez le tableau approprié ci-dessous selon que vous déployez Cloud Data Sense dans AWS, Azure ou GCP.

#### Terminaux requis pour les déploiements AWS:

Terminaux	Objectif
<a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a>	Communication avec le service BlueXP, qui inclut les comptes NetApp.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://auth0.com">https://auth0.com</a>	Communication avec le site Web BlueXP pour l'authentification centralisée des utilisateurs.
<a href="https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com">https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com</a> <a href="https://hub.docker.com">https://hub.docker.com</a> <a href="https://auth.docker.io">https://auth.docker.io</a> <a href="https://registry-1.docker.io">https://registry-1.docker.io</a> <a href="https://index.docker.io/">https://index.docker.io/</a> <a href="https://dseasb33srrn.cloudfront.net/">https://dseasb33srrn.cloudfront.net/</a> <a href="https://production.cloudflare.docker.com/">https://production.cloudflare.docker.com/</a>	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://user-feedback-store-prod.s3.us-west-2.amazonaws.com">https://user-feedback-store-prod.s3.us-west-2.amazonaws.com</a> <a href="https://customer-data-production.s3.us-west-2.amazonaws.com">https://customer-data-production.s3.us-west-2.amazonaws.com</a>	Cloud Data est raisonnable pour accéder aux manifestes et aux modèles, mais aussi pour envoyer des journaux et des metrics.

#### Terminaux requis pour les déploiements Azure et GCP :

Terminaux	Objectif
<a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a>	Communication avec le service BlueXP, qui inclut les comptes NetApp.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://auth0.com">https://auth0.com</a>	Communication avec le site Web BlueXP pour l'authentification centralisée des utilisateurs.
<a href="https://support.compliance.api.bluexp.netapp.com/">https://support.compliance.api.bluexp.netapp.com/</a> <a href="https://hub.docker.com">https://hub.docker.com</a> <a href="https://auth.docker.io">https://auth.docker.io</a> <a href="https://registry-1.docker.io">https://registry-1.docker.io</a> <a href="https://index.docker.io/">https://index.docker.io/</a> <a href="https://dseasb33srrn.cloudfront.net/">https://dseasb33srrn.cloudfront.net/</a> <a href="https://production.cloudflare.docker.com/">https://production.cloudflare.docker.com/</a>	Permet d'accéder aux images logicielles, aux manifestes, aux modèles et à l'envoi de journaux et de mesures.

Terminaux	Objectif
<a href="https://support.compliance.api.bluexp.netapp.com/">https://support.compliance.api.bluexp.netapp.com/</a>	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.

### Assurez-vous que BlueXP dispose des autorisations requises

Assurez-vous que BlueXP dispose d'autorisations pour déployer des ressources et créer des groupes de sécurité pour l'instance Cloud Data Sense. Vous trouverez les dernières autorisations BlueXP dans ["Règles fournies par NetApp"](#).

### Vérifiez les limites de vos CPU virtuels

Assurez-vous que la limite de vCPU de votre fournisseur de cloud permet de déployer une instance de 16 cœurs. Vous devez vérifier la limite de CPU virtuels pour la famille d'instances concernée dans la région où BlueXP est en cours d'exécution. ["Voir les types d'instances requis"](#).

Pour plus de détails sur les limites des CPU virtuels, consultez les liens suivants :

- ["Documentation AWS : quotas de service Amazon EC2"](#)
- ["Documentation Azure : quotas de vCPU de machine virtuelle"](#)
- ["Documentation Google Cloud : quotas de ressources"](#)

Notez que vous pouvez déployer Data Sense sur un système avec moins de processeurs et moins de RAM, mais il y a des limites lors de l'utilisation de ces systèmes. Voir ["Utilisation d'un type d'instance plus petit"](#) pour plus d'informations.

### Assurez-vous que le connecteur BlueXP peut accéder à Cloud Data SENSE

Assurez la connectivité entre le connecteur et l'instance Cloud Data SENSE. Le groupe de sécurité du connecteur doit autoriser le trafic entrant et sortant via le port 443 vers et depuis l'instance de détection des données. Cette connexion permet le déploiement de l'instance de détection des données et vous permet d'afficher des informations dans les onglets conformité et gouvernance. Cloud Data SENSE est pris en charge par les régions gouvernementales sur AWS et Azure.

Des règles de groupes de sécurité supplémentaires sont nécessaires pour les déploiements AWS et AWS GovCloud. Voir ["Règles pour le connecteur dans AWS"](#) pour plus d'informations.

Des règles de groupes de sécurité entrantes et sortantes supplémentaires sont nécessaires pour les déploiements d'Azure et d'Azure Government. Voir ["Règles pour le connecteur dans Azure"](#) pour plus d'informations.

### Assurez-vous de continuer d'exécuter le contrôle des données cloud

L'instance Cloud Data SENSE doit rester active pour analyser en continu vos données.

### Assurez la connectivité de votre navigateur Web au cloud Data Sense

Une fois Cloud Data SENSE activé, assurez-vous que les utilisateurs accèdent à l'interface BlueXP à partir d'un hôte connecté à l'instance Data Sense.

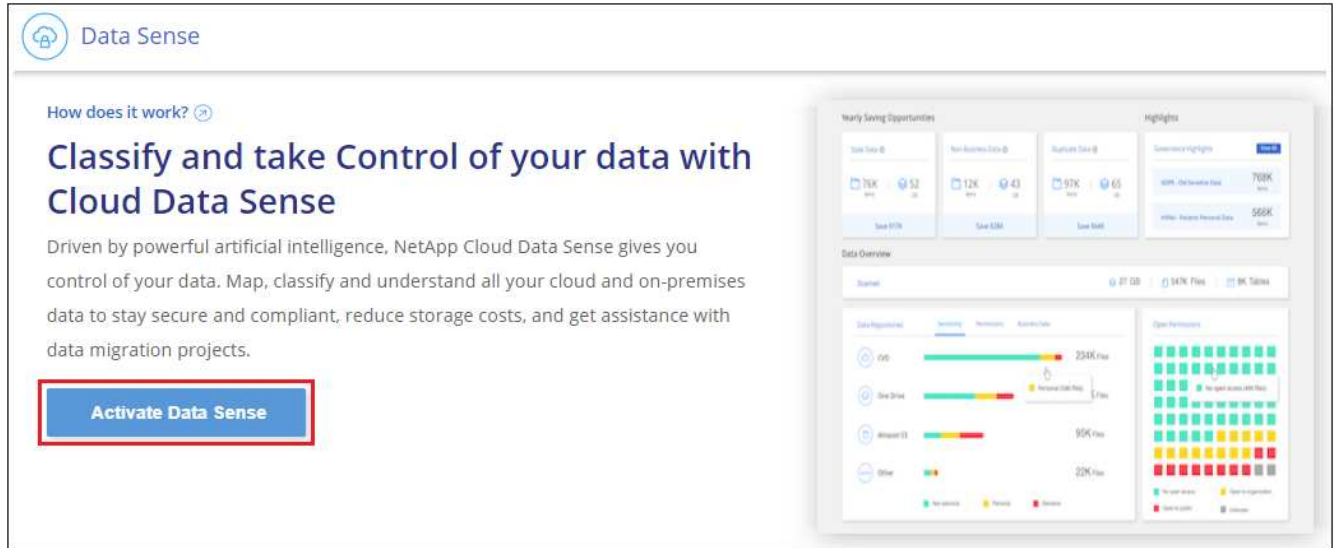
L'instance de détection de données utilise une adresse IP privée pour s'assurer que les données indexées ne sont pas accessibles à Internet. Par conséquent, le navigateur Web que vous utilisez pour accéder à BlueXP doit disposer d'une connexion à cette adresse IP privée. Cette connexion peut provenir d'une connexion directe avec votre fournisseur de cloud (par exemple, un VPN), ou d'un hôte situé dans le même réseau que l'instance Data Sense.

## Déployez votre sens des données dans le cloud

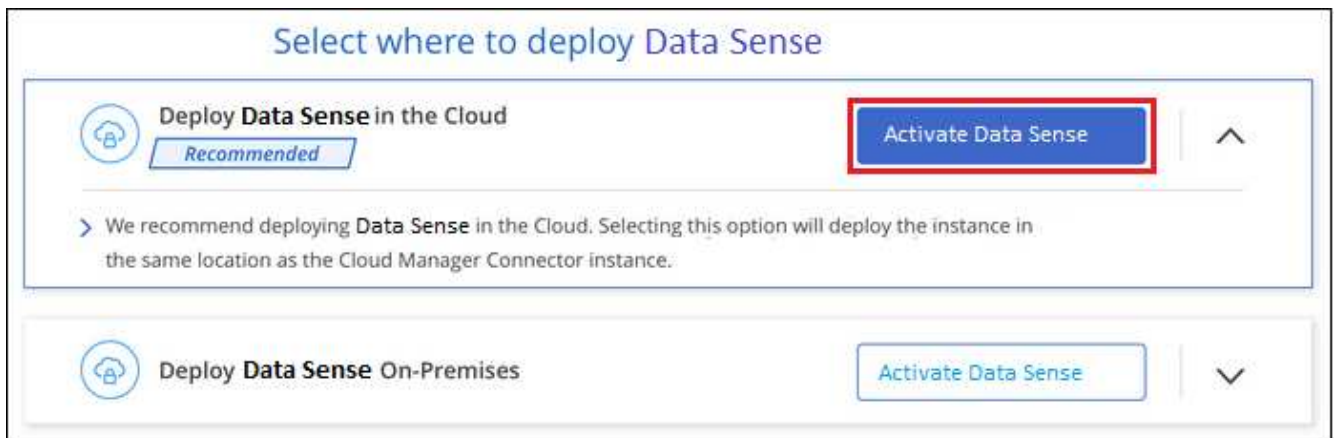
Voici la procédure à suivre pour déployer une instance de Cloud Data Sense dans le cloud.

### Étapes

1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**.
2. Cliquez sur **Activer détection de données**.



3. Cliquez sur **Activer Data Sense** pour démarrer l'assistant de déploiement du cloud.



4. L'assistant affiche la progression au fur et à mesure des étapes de déploiement. Il s'arrête et demande des commentaires s'il n'y a pas de problème.



5. Lorsque l'instance est déployée, cliquez sur **Continuer la configuration** pour accéder à la page *Configuration*.

### Résultat

BlueXP déploie l'instance Cloud Data Sense dans votre fournisseur cloud.

### Et la suite

Dans la page Configuration, vous pouvez sélectionner les sources de données à numériser.

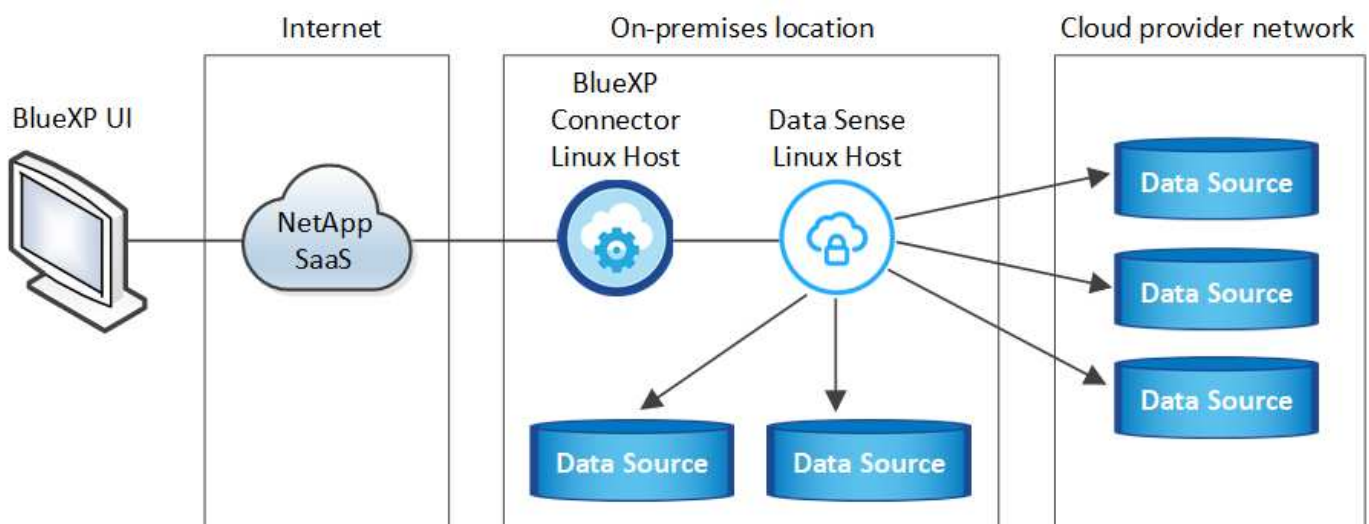
Vous pouvez également "[Configurer les licences pour Cloud Data Sense](#)" à ce moment-là. Vous ne serez facturé que lorsque la quantité de données dépasse 1 To.

## Déployez Cloud Data Sense sur un hôte Linux avec accès Internet

Suivez quelques étapes pour déployer Cloud Data Sense sur un hôte Linux de votre réseau ou dans le cloud, qui dispose d'un accès Internet.

L'installation sur site peut être une bonne option si vous préférez analyser les systèmes ONTAP sur site à l'aide d'une instance Data Sense également située sur site, mais ce n'est pas une exigence. Le logiciel fonctionne exactement de la même manière quelle que soit la méthode d'installation choisie.

Les installations sur site classiques comportent les composants et les connexions suivants.





Pour les très grandes configurations dans lesquelles vous numérisez des pétaoctets de données, vous pouvez inclure plusieurs hôtes pour bénéficier d'une puissance de traitement supplémentaire. Lorsque vous utilisez plusieurs systèmes hôtes, le système principal est appelé nœud Manager et les systèmes supplémentaires qui fournissent une puissance de traitement supplémentaire sont appelés nœuds de scanner.

Notez que vous pouvez également ["Déployer Data Sense dans un site sur site qui ne dispose pas d'un accès Internet"](#) pour des sites totalement sécurisés.

## Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

### Créer un connecteur

Si vous n'avez pas encore de connecteur, ["Déployez le connecteur sur site"](#) Sur un hôte Linux de votre réseau ou dans le cloud.

Vous pouvez également créer un connecteur avec votre fournisseur cloud. Voir ["Création d'un connecteur dans AWS"](#), ["Création d'un connecteur dans Azure"](#), ou ["Création d'un connecteur dans GCP"](#).

2

### Passer en revue les prérequis

Assurez-vous que votre environnement est conforme aux conditions préalables. Cela inclut l'accès Internet sortant pour l'instance, la connectivité entre le connecteur et Cloud Data SENSE sur le port 443, etc. [Voir la liste complète.](#)

Vous avez également besoin d'un système Linux qui répond à [exigences suivantes](#).

3

### Téléchargez et déployez Cloud Data Sense

Téléchargez le logiciel Cloud Data SENSE sur le site de support NetApp et copiez le fichier d'installation sur l'hôte Linux que vous prévoyez d'utiliser. Lancez ensuite l'assistant d'installation et suivez les invites pour déployer l'instance de détection de données.

4

### Abonnez-vous au service Cloud Data Sense

Les 1 premiers To de données scanners Cloud Data SENSE dans BlueXP sont gratuits. Un abonnement à votre fournisseur cloud Marketplace, ou une licence BYOL de NetApp, est nécessaire pour continuer l'analyse des données après ce point.

## Créer un connecteur

Un connecteur BlueXP est nécessaire avant de pouvoir installer et utiliser Data Sense. Dans la plupart des cas, vous aurez probablement configuré un connecteur avant d'essayer d'activer le cloud Data SENSE ["Les fonctionnalités BlueXP nécessitent un connecteur"](#), mais il y a des cas où vous devrez en configurer un maintenant.

Pour en créer un dans votre environnement de fournisseur cloud, consultez la section ["Création d'un connecteur dans AWS"](#), ["Création d'un connecteur dans Azure"](#), ou ["Création d'un connecteur dans GCP"](#).



Dans certains cas, vous devez utiliser un connecteur déployé dans un fournisseur de cloud spécifique :

- Pour l'analyse des données dans Cloud Volumes ONTAP dans AWS, Amazon FSX pour ONTAP ou dans des compartiments AWS S3, vous utilisez un connecteur dans AWS.
- Pour analyser les données dans Cloud Volumes ONTAP dans Azure ou dans Azure NetApp Files, vous utilisez un connecteur dans Azure.

Pour Azure NetApp Files, il doit être déployé dans la même région que les volumes que vous souhaitez analyser.

- Pour l'analyse des données dans Cloud Volumes ONTAP dans GCP, vous utilisez un connecteur dans GCP.

Vous pouvez analyser les systèmes ONTAP sur site, les partages de fichiers non NetApp, le stockage objet S3 générique, les bases de données, les dossiers OneDrive, les comptes SharePoint et les comptes Google Drive à l'aide de ces connecteurs cloud.

Notez que vous pouvez également ["Déployez le connecteur sur site"](#) Sur un hôte Linux de votre réseau ou dans le cloud. Certains utilisateurs qui prévoient d'installer Data Sense sur site peuvent également choisir d'installer le connecteur sur site.

Comme vous pouvez le voir, il peut y avoir des situations où vous devez utiliser ["Plusieurs connecteurs"](#).

Vous aurez besoin de l'adresse IP ou du nom d'hôte du système de connecteur lors de l'installation de Data Sense. Vous aurez ces informations si vous avez installé le connecteur sur votre site. Si le connecteur est déployé dans le cloud, vous pouvez trouver ces informations à partir de la console BlueXP : cliquez sur l'icône aide, sélectionnez **support** et cliquez sur **BlueXP Connector**.

## Préparez le système hôte Linux

Le logiciel de détection des données doit être exécuté sur un hôte qui répond à des exigences spécifiques du système d'exploitation, de la RAM, des exigences logicielles, etc. L'hôte Linux peut se trouver sur votre réseau ou dans le cloud. Data Sense n'est pas pris en charge sur un hôte partagé avec d'autres applications ; l'hôte doit être un hôte dédié.

- **Système d'exploitation** : Red Hat Enterprise Linux ou CentOS versions 8.0 à 8.6
  - La version 7.8 ou 7.9 peut être utilisée, mais la version du noyau Linux doit être 4.0 ou supérieure
  - Le système d'exploitation doit pouvoir installer le moteur docker
- **Disque** : SSD avec 500 Gio disponible sur /, ou
  - 100 Gio disponible sur /opt
  - 400 Gio disponible sur /var
  - 5 Gio sur /tmp
- **RAM** : 64 Go (la mémoire d'échange doit être désactivée sur l'hôte)
- **CPU** : 16 cœurs

Notez que vous pouvez déployer Data Sense sur un système avec moins de processeurs et moins de RAM, mais il y a des limites lors de l'utilisation de ces systèmes. Voir ["Utilisation d'un type d'instance plus petit"](#) pour plus d'informations.

- **Gestion des abonnements Red Hat** : un système Red Hat Enterprise Linux doit être enregistré auprès de la gestion des abonnements Red Hat. S'il n'est pas enregistré, le système ne peut pas accéder aux

référentiels pour mettre à jour les logiciels tiers requis au cours de l'installation.

- **Logiciel supplémentaire** : le logiciel suivant doit être installé sur l'hôte. S'il n'existe pas déjà sur l'hôte, le programme d'installation installe le logiciel pour vous :
  - Docker Engine version 19 ou ultérieure. "[Voir les instructions d'installation](#)".
  - Python 3 version 3.6 ou ultérieure. "[Voir les instructions d'installation](#)".
- **Firesund considérations**: Si vous prévoyez d'utiliser `firewalld`, Nous vous recommandons de l'activer avant d'installer Data Sense. Exécutez les commandes suivantes pour configurer `firewalld` Pour qu'il soit compatible avec Data Sense :

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --reload
```

Si vous prévoyez d'utiliser d'autres hôtes Data Sense, ajoutez ces règles à votre système principal à l'heure actuelle :

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7496/udp
firewall-cmd --permanent --add-port=7496/tcp
firewall-cmd --permanent --add-port=4789/udp
```

Si vous activez `firewalld` Après avoir installé Data Sense, vous devez redémarrer docker.



L'adresse IP du système hôte Data Sense ne peut pas être modifiée après l'installation.

## Vérifier les prérequis BlueXP et Data Sense

Consultez les conditions préalables suivantes pour vous assurer que votre configuration est prise en charge avant de déployer Cloud Data SENSE sur un système Linux.

### Activation de l'accès Internet sortant à partir du Cloud Data SENSE

Cloud Data Sense requiert un accès Internet sortant. Si votre réseau virtuel ou physique utilise un serveur proxy pour l'accès à Internet, assurez-vous que l'instance de détection de données dispose d'un accès Internet sortant pour contacter les points de terminaison suivants.

Terminaux	Objectif
<code>https://api.bluexp.netapp.com</code>	Communication avec le service BlueXP, qui inclut les comptes NetApp.
<code>https://netapp-cloud-account.auth0.com</code> <code>https://auth0.com</code>	Communication avec le site Web BlueXP pour l'authentification centralisée des utilisateurs.

Terminaux	Objectif
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srrn.cloudfront.net/ https://production.cloudflare.docker.com/	Permet d'accéder aux images logicielles, aux manifestes, aux modèles et à l'envoi de journaux et de mesures.
https://support.compliance.api.bluexp.netapp.com/	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://github.com/docker https://download.docker.com http://mirror.centos.org http://mirrorlist.centos.org http://mirror.centos.org/centos/7/extras/x86_64/Packages/container-selinux-2.107-3.el7.noarch.rpm	Fournit les packages requis pour l'installation.

### Assurez-vous que le connecteur BlueXP dispose des autorisations requises

Assurez-vous que le connecteur dispose d'autorisations pour déployer des ressources et créer des groupes de sécurité pour l'instance Cloud Data Sense. Vous trouverez les dernières autorisations BlueXP dans ["Règles fournies par NetApp"](#).

### Assurez-vous de continuer d'exécuter le contrôle des données cloud

Le serveur Cloud Data Sense doit rester activé pour analyser en continu vos données.

### Assurez la connectivité de votre navigateur Web au cloud Data Sense

Une fois Cloud Data SENSE activé, assurez-vous que les utilisateurs accèdent à l'interface BlueXP à partir d'un hôte connecté à l'instance Data Sense.

L'instance de détection de données utilise une adresse IP privée pour s'assurer que les données indexées ne sont pas accessibles à Internet. Par conséquent, le navigateur Web que vous utilisez pour accéder à BlueXP doit disposer d'une connexion à cette adresse IP privée. Cette connexion peut provenir d'une connexion directe avec votre fournisseur de cloud (par exemple, un VPN), ou d'un hôte situé dans le même réseau que l'instance Data Sense.

### Vérifiez que tous les ports requis sont activés

Vous devez vous assurer que tous les ports requis sont ouverts pour la communication entre le connecteur, Data Sense, Active Directory et vos sources de données.

Type de connexion	Ports	Description
Connecteur <> détection des données	8080 (TCP), 443 (TCP) et 80	Le groupe de sécurité du connecteur doit autoriser le trafic entrant et sortant via le port 443 vers et depuis l'instance de détection des données. Assurez-vous que le port 8080 est ouvert pour voir la progression de l'installation dans BlueXP.

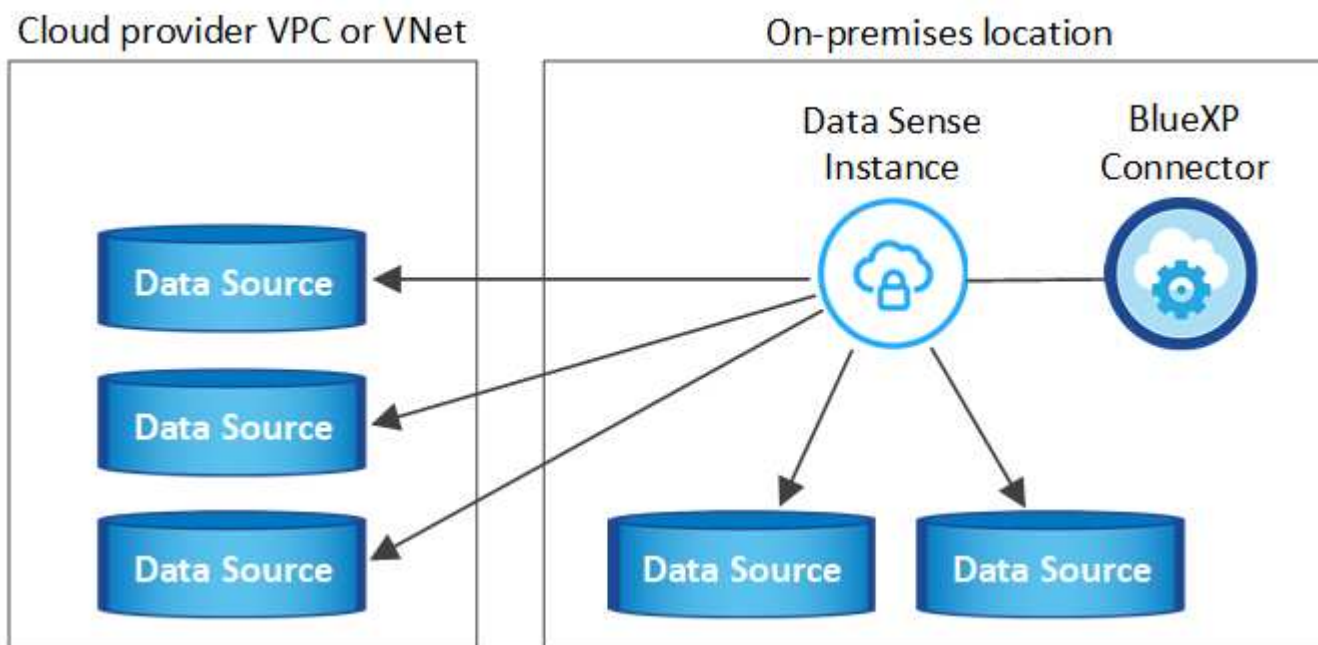
Type de connexion	Ports	Description
Connecteur <> cluster ONTAP (NAS)	443 (TCP)	<p>BlueXP détecte les clusters ONTAP via HTTPS. Si vous utilisez des stratégies de pare-feu personnalisées, elles doivent répondre aux exigences suivantes :</p> <ul style="list-style-type: none"> <li>• L'hôte du connecteur doit autoriser l'accès HTTPS sortant via le port 443. Si le connecteur est dans le Cloud, toutes les communications sortantes sont autorisées par le groupe de sécurité prédéfini.</li> <li>• Le cluster ONTAP doit autoriser l'accès HTTPS entrant via le port 443. La stratégie de pare-feu " mgmt " par défaut permet l'accès HTTPS entrant à partir de toutes les adresses IP. Si vous avez modifié cette stratégie par défaut ou si vous avez créé votre propre stratégie de pare-feu, vous devez associer le protocole HTTPS à cette politique et activer l'accès à partir de l'hôte du connecteur.</li> </ul>
Cluster de détection des données <> ONTAP	<ul style="list-style-type: none"> <li>• Pour NFS - 111 (TCP/UDP) et 2049 (TCP/UDP)</li> <li>• Pour CIFS - 139 (TCP/UDP) et 445 (TCP/UDP)</li> </ul>	<p>La détection des données requiert une connexion réseau à chaque sous-réseau Cloud Volumes ONTAP ou système ONTAP sur site. Les groupes de sécurité pour Cloud Volumes ONTAP doivent autoriser les connexions entrantes à partir de l'instance de détection de données.</p> <p>Assurez-vous que ces ports sont ouverts à l'instance de détection de données :</p> <ul style="list-style-type: none"> <li>• Pour NFS - 111 et 2049</li> <li>• Pour CIFS : 139 et 445</li> </ul> <p>Les règles d'exportation de volumes NFS doivent autoriser l'accès à partir de l'instance Data Sense.</p>

Type de connexion	Ports	Description
Détection de données <> Active Directory	389 (TCP ET UDP), 636 (TCP), 3268 (TCP) ET 3269 (TCP)	<p>Un Active Directory doit déjà être configuré pour les utilisateurs de votre entreprise. En outre, Data Sense nécessite des identifiants Active Directory pour analyser les volumes CIFS.</p> <p>Vous devez disposer des informations pour Active Directory :</p> <ul style="list-style-type: none"> <li>• Adresse IP du serveur DNS ou adresses IP multiples</li> <li>• Nom d'utilisateur et mot de passe du serveur</li> <li>• Nom de domaine (nom Active Directory)</li> <li>• Que vous utilisiez ou non le protocole LDAP sécurisé (LDAPS)</li> <li>• Port serveur LDAP (généralement 389 pour LDAP et 636 pour LDAP sécurisé)</li> </ul>

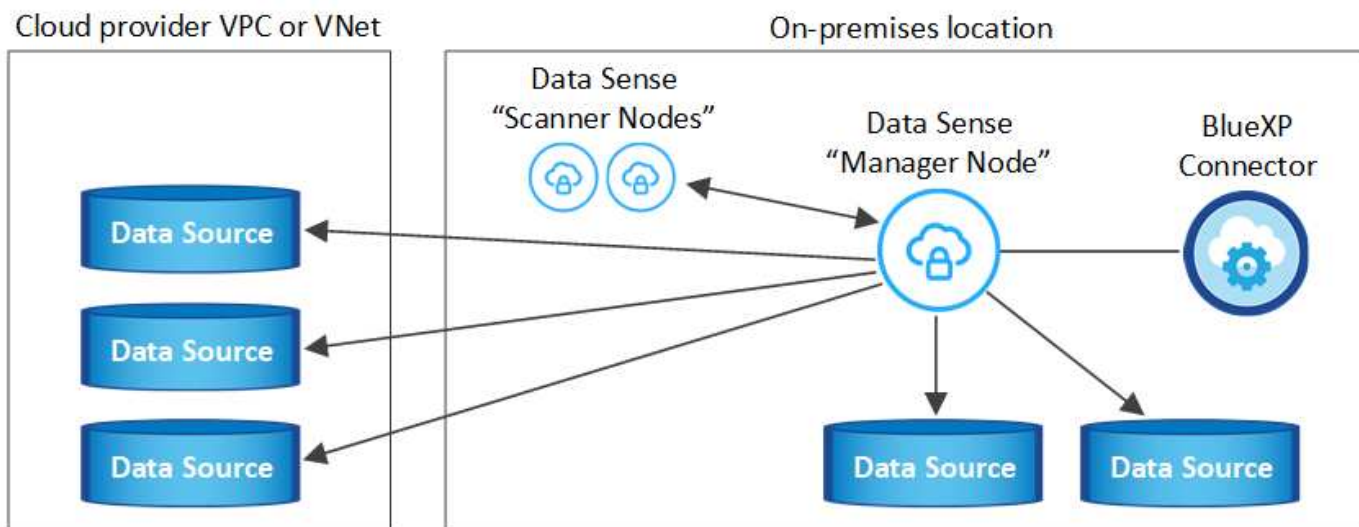
Si vous utilisez plusieurs hôtes Data Sense pour fournir une puissance de traitement supplémentaire pour analyser vos sources de données, vous devez activer des ports/protocoles supplémentaires. ["Voir la configuration de port supplémentaire requise"](#).

### Déployer des solutions Data Sense sur site

Pour les configurations standard, le logiciel est installé sur un système hôte unique. [Découvrez ces étapes ici](#).



Pour les très grandes configurations dans lesquelles vous numérisez des pétaoctets de données, vous pouvez inclure plusieurs hôtes pour bénéficier d'une puissance de traitement supplémentaire. [Découvrez ces étapes ici](#).



Voir [Préparation du système hôte Linux](#) et [Vérification des prérequis](#) Avant de déployer Cloud Data Sense, vous devez consulter la liste complète des exigences.

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.



Cloud Data Sense n'est actuellement pas en mesure d'analyser les compartiments S3, Azure NetApp Files ou FSX pour ONTAP lorsque le logiciel est installé sur site. Dans ce cas, vous devez déployer un connecteur et une instance de Data Sense dans le cloud et ["Basculer entre les connecteurs"](#) pour les différentes sources de données.

#### Installation à un seul hôte pour les configurations courantes

Suivez ces étapes pour installer le logiciel Data Sense sur un hôte sur site unique.

#### Ce dont vous avez besoin

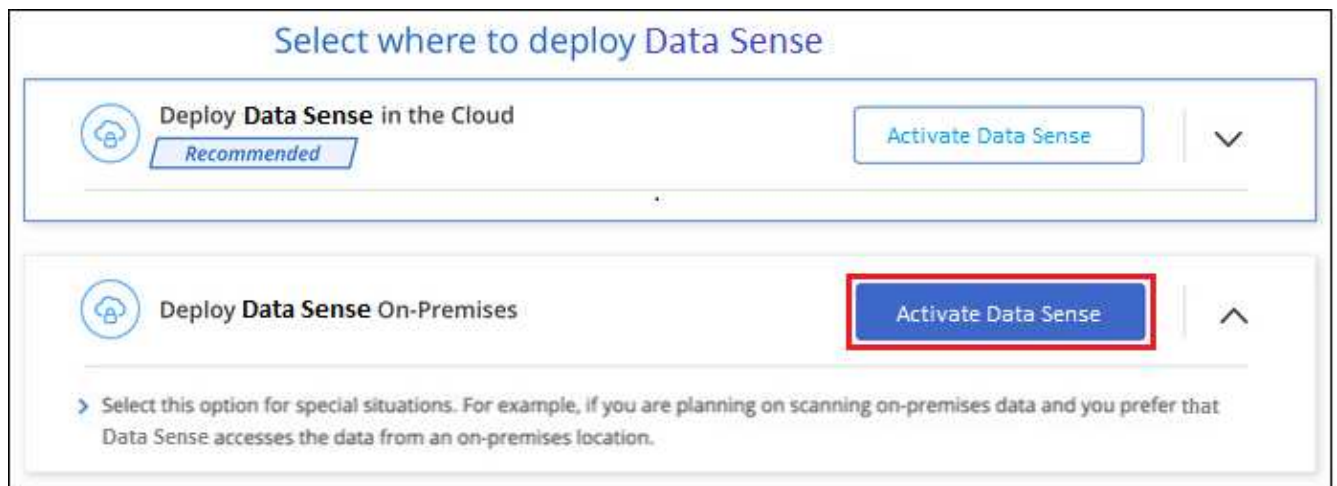
- Vérifiez que votre système Linux est conforme à la [configuration requise pour l'hôte](#).
- (Facultatif) Vérifiez que le système est équipé des deux packages logiciels prérequis (Docker Engine et Python 3). Le programme d'installation installe ce logiciel s'il n'est pas déjà installé sur le système.
- Assurez-vous que vous disposez des privilèges root sur le système Linux.
- Si vous utilisez un proxy et qu'il effectue une interception TLS, vous devez connaître le chemin d'accès sur le système Linux Data Sense où sont stockés les certificats CA TLS.
- Vérifiez que votre environnement hors ligne répond aux besoins [autorisations et connectivité](#).

#### Étapes

1. Téléchargez le logiciel Cloud Data SENSE sur le ["Site de support NetApp"](#). Le fichier que vous devez sélectionner est nommé **DATASENSE-INSTALLER-<version>.tar.gz**.
2. Copiez le fichier d'installation sur l'hôte Linux que vous envisagez d'utiliser (à l'aide de `scp` ou une autre méthode).
3. Dans BlueXP, sélectionnez **gouvernance > Classification**.
4. Cliquez sur **Activer détection de données**.



5. Cliquez sur **Activer Data Sense** pour démarrer l'assistant de déploiement sur site.



6. Dans la boîte de dialogue *Deploy Data Sense on local*, copiez la commande fournie et collez-la dans un fichier texte afin que vous puissiez l'utiliser ultérieurement, puis cliquez sur **Fermer**. Par exemple :

```
sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq
```

7. Décompressez le fichier d'installation sur la machine hôte, par exemple :

```
tar -xzf DATASENSE-INSTALLER-V1.16.1.tar.gz
```

8. Lorsque le programme d'installation vous le demande, vous pouvez entrer les valeurs requises dans une série d'invites, ou vous pouvez fournir les paramètres requis comme arguments de ligne de commande au programme d'installation.

Notez que le programme d'installation effectue une pré-vérification afin de s'assurer que vos exigences système et réseau sont en place pour une installation réussie.



Entrez les paramètres comme demandé :	Saisissez la commande complète :
<p>a. Coller les informations copiées à partir de l'étape 6 :</p> <pre>sudo ./install.sh -a &lt;account_id&gt; -c &lt;agent_id&gt; -t &lt;token&gt;</pre> <p>b. Entrez l'adresse IP ou le nom d'hôte de la machine hôte Data Sense afin qu'elle soit accessible par l'instance de connecteur.</p> <p>c. Entrez l'adresse IP ou le nom d'hôte de la machine hôte BlueXP Connector afin qu'elle soit accessible par l'instance Data Sense.</p> <p>d. Entrez les détails du proxy comme vous y êtes invité. Si votre connecteur BlueXP utilise déjà un proxy, il n'est pas nécessaire de saisir à nouveau ces informations ici car Data Sense utilisera automatiquement le proxy utilisé par le connecteur.</p>	<p>Vous pouvez également créer l'ensemble de la commande à l'avance, en fournissant les paramètres d'hôte et de proxy nécessaires :</p> <pre>sudo ./install.sh -a &lt;account_id&gt; -c &lt;agent_id&gt; -t &lt;token&gt; --host &lt;ds_host&gt; --manager-host &lt;cm_host&gt; --proxy-host &lt;proxy_host&gt; --proxy-port &lt;proxy_port&gt; --proxy-scheme &lt;proxy_scheme&gt; --proxy -user &lt;proxy_user&gt; --proxy-password &lt;proxy_password&gt; --cacert-folder-path &lt;ca_cert_dir&gt;</pre>

Valeurs variables :

- *Account\_ID* = ID du compte NetApp
- *Agent\_ID* = ID connecteur
- *token* = jeton utilisateur jwt
- *Ds\_host* = adresse IP ou nom d'hôte du système Data Sense Linux.
- *Cm\_host* = adresse IP ou nom d'hôte du système de connecteurs BlueXP.
- *Proxy\_host* = IP ou nom d'hôte du serveur proxy si l'hôte est derrière un serveur proxy.
- *Proxy\_port* = Port pour se connecter au serveur proxy (80 par défaut).
- *Proxy\_schéma* = schéma de connexion : https ou http (par défaut : http).
- *Proxy\_user* = utilisateur authentifié pour se connecter au serveur proxy, si une authentification de base est requise.
- *Proxy\_password* = Mot de passe pour le nom d'utilisateur que vous avez spécifié.
- *CA\_cert\_dir* = chemin sur le système Data Sense Linux contenant des bundles de certificat d'autorité de certification TLS supplémentaires. Requis uniquement si le proxy effectue une interception TLS.

## Résultat

Le programme d'installation de Cloud Data Sense installe des packages, installe docker, enregistre l'installation et installe Data Sense. L'installation peut prendre entre 10 et 20 minutes.

S'il y a une connectivité sur le port 8080 entre la machine hôte et l'instance de connecteur, vous verrez la progression de l'installation dans l'onglet détection de données de BlueXP.

## Et la suite

Dans la page Configuration, vous pouvez sélectionner les sources de données à numériser.

Vous pouvez également "[Configurer les licences pour Cloud Data Sense](#)" à ce moment-là. Vous ne serez facturé que lorsque la quantité de données dépasse 1 To.



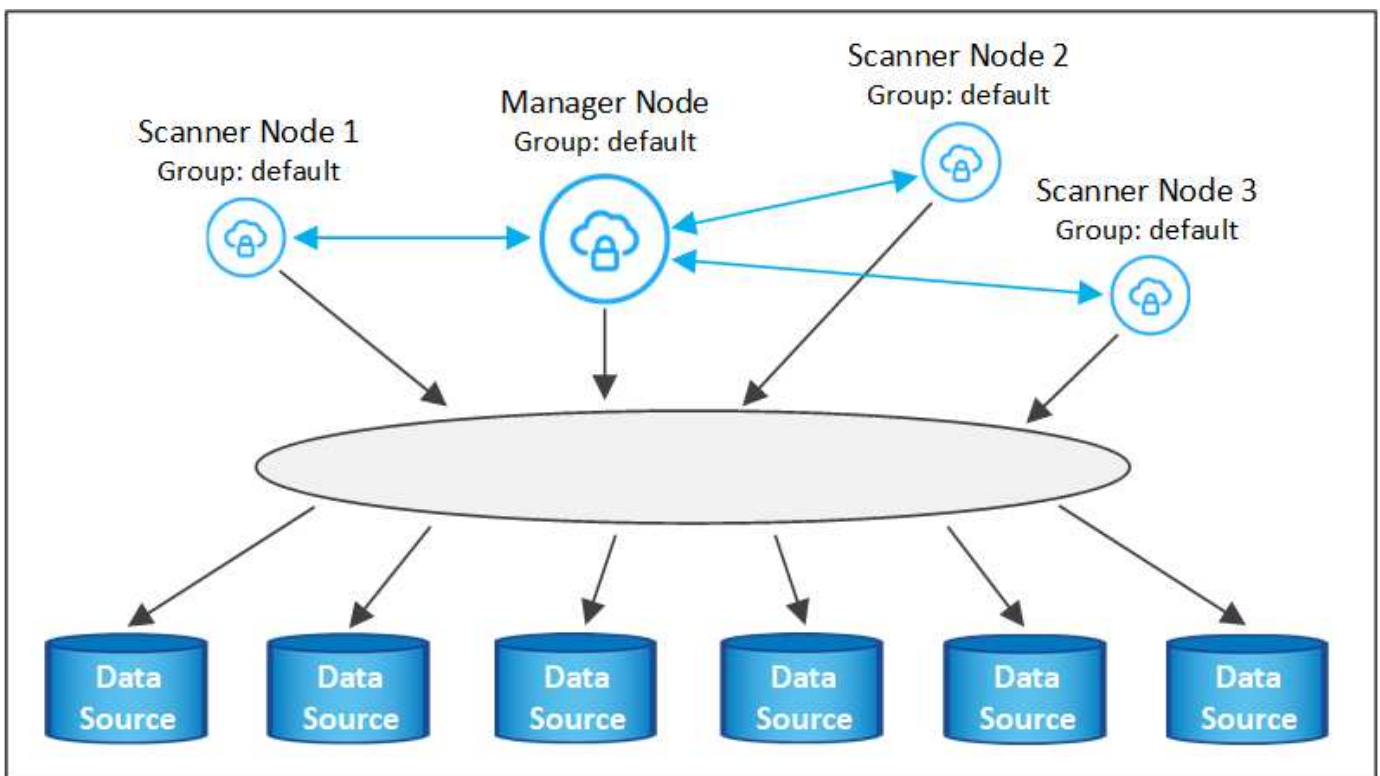
## Ajoutez des nœuds de scanner à un déploiement existant

Vous pouvez ajouter d'autres nœuds de numérisation si vous trouvez que vous avez besoin d'une puissance de traitement plus élevée pour numériser vos sources de données. Vous pouvez ajouter les nœuds du scanner immédiatement après avoir installé le nœud du gestionnaire, ou vous pouvez ajouter un nœud du scanner ultérieurement. Par exemple, si vous réalisez que la quantité de données de l'une de vos sources de données a doublé ou triplé au bout de 6 mois, vous pouvez ajouter un nouveau nœud du scanner pour faciliter l'analyse des données.

Il existe deux façons d'ajouter des nœuds de scanner supplémentaires :

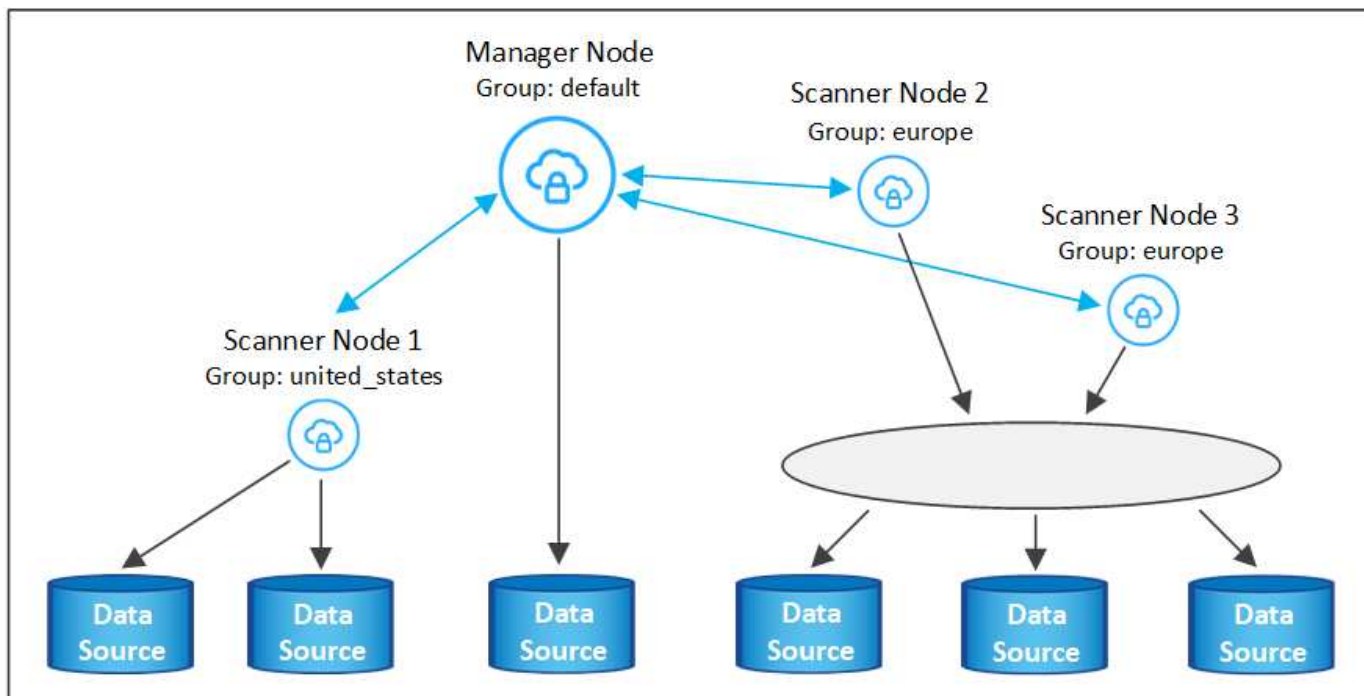
- ajoutez un nœud pour faciliter la numérisation de toutes les sources de données
- ajoutez un nœud pour faciliter l'analyse d'une source de données spécifique ou d'un groupe spécifique de sources de données

Par défaut, tous les nouveaux nœuds de scanner que vous ajoutez sont ajoutés au pool général de ressources de numérisation. Il s'agit du « groupe de scanner par défaut ». Dans l'image ci-dessous, il y a 1 nœud Manager et 3 nœuds de scanner dans le groupe « par défaut » qui sont tous des données de numérisation provenant des 6 sources de données.



Si vous souhaitez analyser certaines sources de données par des nœuds de scanner qui sont physiquement plus proches des sources de données, vous pouvez définir un nœud de scanner, ou un groupe de nœuds de scanner, pour analyser une source de données spécifique ou un groupe de sources de données. Dans l'image ci-dessous, il y a 1 nœud Manager et 3 nœuds scanner.

- Le nœud Manager se trouve dans le groupe « par défaut » et il analyse 1 source de données
- Le nœud du scanner 1 se trouve dans le groupe États-unis et analyse 2 sources de données
- Les nœuds du scanner 2 et 3 se trouvent dans le groupe « europe » et partagent les tâches de numérisation pour 3 sources de données



Les groupes de lecteurs de détection de données peuvent être définis comme des zones géographiques distinctes où vos données sont stockées. Vous pouvez déployer plusieurs nœuds de scanner Data Sense dans le monde entier et choisir un groupe de scanner pour chaque nœud. De cette façon, chaque nœud du scanner analyse les données qui lui sont les plus proches. Plus le nœud du scanner est proche des données, mieux c'est, car il réduit la latence du réseau autant que possible lors de l'acquisition des données.

Vous pouvez choisir les groupes de scanner à ajouter à Data Sense et choisir leur nom. Data Sense ne fait pas valoir qu'un nœud mappé à un groupe de scanner nommé « europe » sera déployé en Europe.

Procédez comme suit pour installer d'autres nœuds du scanner Data Sense :

1. Préparez les systèmes hôtes Linux qui feront office de nœuds de scanner
2. Téléchargez le logiciel Data Sense sur ces systèmes Linux
3. Exécutez une commande sur le nœud Manager pour identifier les nœuds du scanner
4. Suivez les étapes de déploiement du logiciel sur les nœuds du scanner (et définissez éventuellement un « groupe de scanner » pour certains nœuds du scanner).
5. Si vous avez défini un scanner group, sur le nœud Manager :
  - a. Ouvrez le fichier « environnement\_de\_travail\_vers\_scanner\_groupe\_config.yml » et définissez les environnements de travail qui seront analysés par chaque groupe de scanner
  - b. Exécutez le script suivant pour enregistrer ces informations de mappage avec tous les nœuds du scanner : `update_we_scanner_group_from_config_file.sh`

### Ce dont vous avez besoin

- Vérifiez que tous vos systèmes Linux pour les nœuds du scanner sont conformes à la [configuration requise pour l'hôte](#).
- (Facultatif) Vérifiez que les deux packages logiciels prérequis sont installés sur les systèmes (Docker Engine et Python 3). Le programme d'installation installe ce logiciel s'il n'est pas déjà installé sur les systèmes.
- Assurez-vous que vous disposez des privilèges root sur les systèmes Linux.

- Vérifiez que votre environnement répond aux exigences requises [autorisations et connectivité](#).
- Vous devez disposer des adresses IP des hôtes du nœud scanner que vous ajoutez.
- Vous devez disposer de l'adresse IP du système hôte du nœud Data Sense Manager
- Vous devez disposer de l'adresse IP ou du nom d'hôte du système Connector, de votre ID de compte NetApp, de votre ID de client Connector et du jeton d'accès utilisateur. Si vous prévoyez d'utiliser des groupes de scanner, vous devrez connaître l'ID de l'environnement de travail pour chaque source de données de votre compte. Voir les *étapes préalables* ci-dessous pour obtenir ces informations.
- Les ports et protocoles suivants doivent être activés sur tous les hôtes :

Port	Protocoles	Description
2377	TCP	Communications de gestion du cluster
7946	TCP, UDP	Communication inter-nœuds
4789	UDP	Superposition du trafic réseau
50	ESP	Trafic du réseau de superposition IPSec chiffré (ESP)
111	TCP, UDP	Serveur NFS pour le partage de fichiers entre les hôtes (requis de chaque nœud de scanner vers le nœud gestionnaire)
2049	TCP, UDP	Serveur NFS pour le partage de fichiers entre les hôtes (requis de chaque nœud de scanner vers le nœud gestionnaire)

- Si vous utilisez `firewalld` Sur vos machines Data Sense, nous vous recommandons de l'activer avant d'installer Data Sense. Exécutez les commandes suivantes pour configurer `firewalld` Pour qu'il soit compatible avec Data Sense :

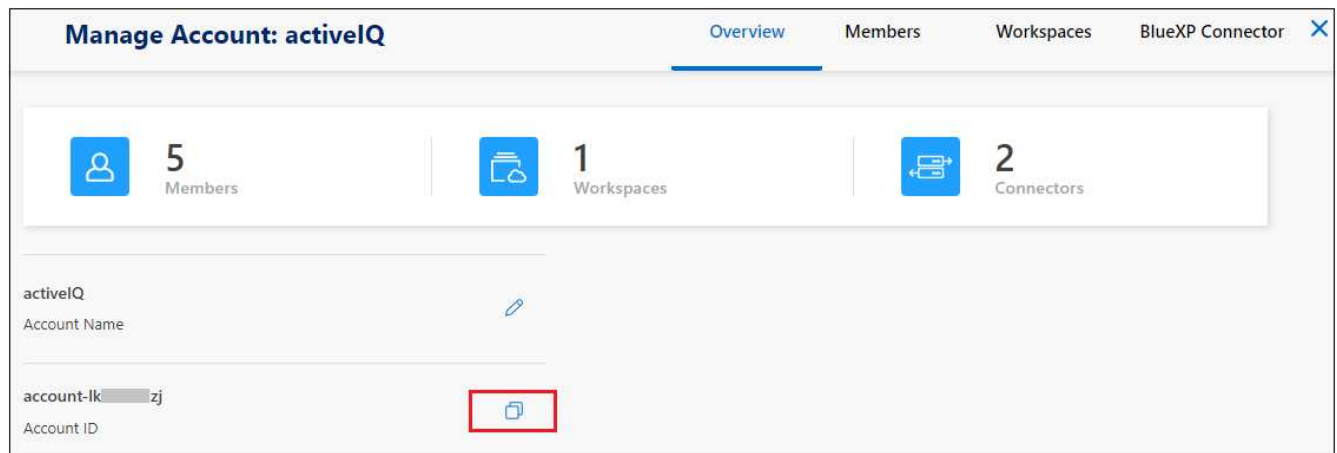
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7496/udp
firewall-cmd --permanent --add-port=7496/tcp
firewall-cmd --permanent --add-port=4789/udp
firewall-cmd --reload
```

Si vous activez `firewalld` Après avoir installé Data Sense, vous devez redémarrer docker.

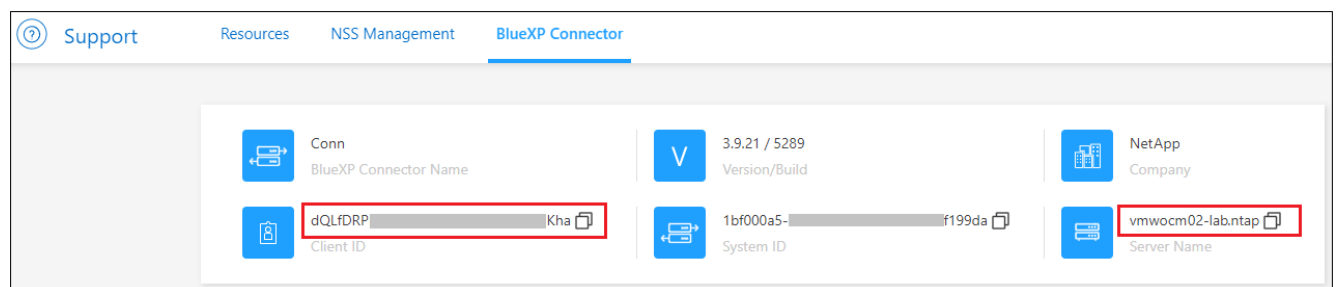
## Étapes préalables

Procédez comme suit pour obtenir l'ID de compte NetApp, l'ID client Connector, le nom du serveur Connector et le jeton d'accès utilisateur nécessaires à l'ajout de nœuds de scanner.

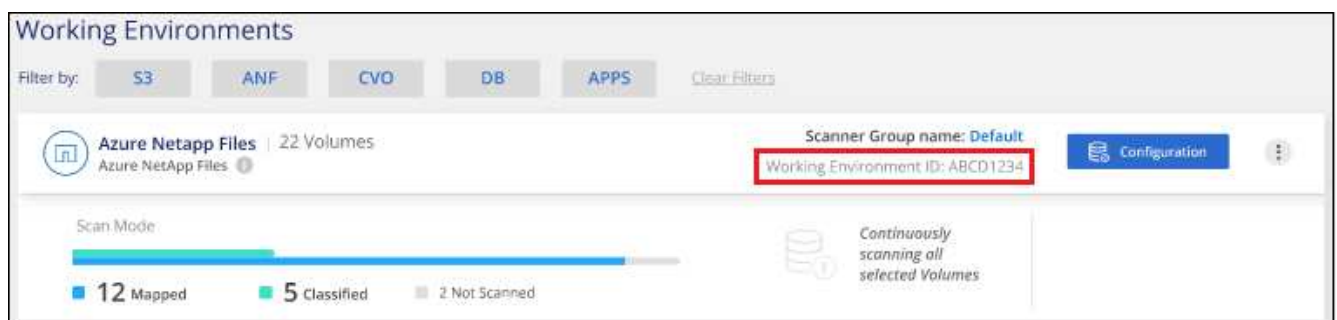
1. Dans la barre de menus BlueXP, cliquez sur **compte > gérer les comptes**.



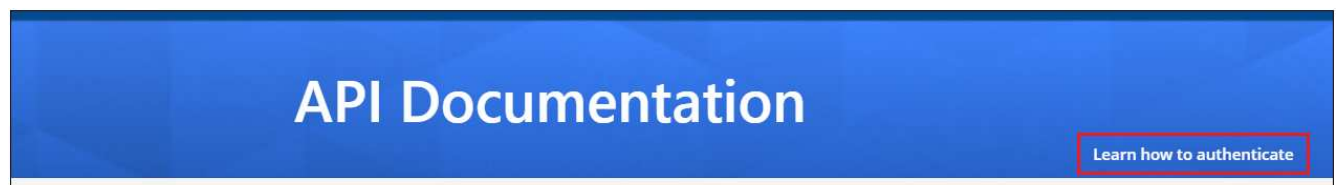
2. Copiez le *ID de compte*.
3. Dans la barre de menus BlueXP, cliquez sur **aide > support > connecteur BlueXP**.



4. Copiez le connecteur *ID client* et le *Nom du serveur*.
5. Si vous prévoyez d'utiliser des groupes de scanner, dans l'onglet Configuration de la détection de données, copiez l'ID de l'environnement de travail pour chaque environnement de travail que vous envisagez d'ajouter à un groupe de scanner.



6. Accédez au ["API Documentation Developer Hub"](#) Et cliquez sur **Apprenez à vous authentifier**.



7. Suivez les instructions d'authentification et copiez le *Access token* à partir de la réponse.

## Étapes

1. Sur le nœud Data Sense Manager, exécutez le script "add\_scanner\_node.sh". Par exemple, cette commande ajoute 2 nœuds de scanner :

```
sudo ./add_scanner_node.sh -a <account_id> -c <client_id> -m <cm_host> -h  
<ds_manager_ip> -n <node_private_ip_1,node_private_ip_2> -t <user_token>
```

Valeurs variables :

- *Account\_ID* = ID du compte NetApp
  - *Client\_ID* = ID client du connecteur
  - *Cm\_host* = adresse IP ou nom d'hôte du système de connecteurs
  - *Ds\_Manager\_ip* = adresse IP privée du système de nœuds Data Sense Manager
  - *Node\_private\_ip* = adresses IP des systèmes de nœuds du scanner de détection de données (plusieurs adresses IP du nœud du scanner sont séparées par une virgule)
  - *User\_token* = jeton d'accès utilisateur JWT
2. Avant la fin du script add\_scanner\_node, une boîte de dialogue affiche la commande d'installation requise pour les nœuds du scanner. Copiez la commande et enregistrez-la dans un fichier texte. Par exemple :

```
sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j
```

3. Sur **chaque hôte de nœud du scanner** :

- a. Copiez le fichier d'installation de Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) sur la machine hôte (à l'aide de `scp` ou une autre méthode).
- b. Décompressez le fichier d'installation.
- c. Collez et exécutez la commande que vous avez copiée à l'étape 2.
- d. Si vous souhaitez ajouter un nœud de scanner à un « scanner group », ajoutez le paramètre **-r <scanner\_group\_name>** à la commande. Sinon, le nœud du scanner est ajouté au groupe « défaut ».

Une fois l'installation terminée sur tous les nœuds du scanner et qu'ils ont été associés au nœud du gestionnaire, le script « Add\_scanner\_node.sh » se termine également. L'installation peut prendre entre 10 et 20 minutes.

4. Si vous avez ajouté des nœuds de scanner à un scanner group, revenez au nœud Manager et effectuez les 2 tâches suivantes :

  - a. Ouvrez le fichier « /opt/netapp/DataSense/working\_Environment\_to\_scanner\_group\_config.yml » et entrez le mappage pour lequel les groupes de lecteurs vont analyser des environnements de travail spécifiques. Vous devez avoir l'ID *Working Environment* pour chaque source de données. Par exemple, les entrées suivantes ajoutent 2 environnements de travail dans 2 groupes de scanner :

```
scanner group:  
  europe:  
    - "working_environment_id1"  
    - "working_environment_id2"  
  united_states:  
    - "working_environment_id3"  
    - "working_environment_id4"
```

Tout environnement de travail qui n'est pas ajouté à la liste est analysé par le groupe « par défaut ». Vous devez avoir au moins un gestionnaire ou un nœud de scanner dans le groupe « par défaut ».

- b. Exécutez le script suivant pour enregistrer ces informations de mappage avec tous les nœuds du scanner :

```
/opt/netapp/Datasense/tools/update_we_scanner_group_from_config_file.sh
```

## Résultat

Data Sense est configuré avec les nœuds Manager et scanner pour analyser toutes vos sources de données.

## Et la suite

Dans la page Configuration, vous pouvez sélectionner les sources de données que vous souhaitez numériser, si vous ne l'avez pas déjà fait. Si vous avez créé des groupes de scanner, chaque source de données est analysée par les nœuds du scanner dans le groupe correspondant. Vous pouvez voir le nom du groupe de lecteurs pour chaque environnement de travail dans la page Configuration.

Vous pouvez également "[Configurer les licences pour Cloud Data Sense](#)" à ce moment-là. Vous ne serez facturé que lorsque la quantité de données dépasse 1 To.

## Installation de plusieurs hôtes pour de grandes configurations

Pour les très grandes configurations où vous pourrez numériser plusieurs pétaoctets de données, vous pouvez inclure plusieurs hôtes pour fournir une puissance de traitement supplémentaire. Lors de l'utilisation de plusieurs systèmes hôtes, le système principal est appelé le *Manager node* et les systèmes supplémentaires qui fournissent une puissance de traitement supplémentaire sont appelés *scanner nodes*.

Procédez comme suit lors de l'installation du logiciel Data Sense sur plusieurs hôtes sur site.

## Ce dont vous avez besoin

- Vérifiez que tous vos systèmes Linux pour les nœuds Manager et scanner sont conformes à la [configuration requise pour l'hôte](#).
- (Facultatif) Vérifiez que les deux packages logiciels prérequis sont installés sur les systèmes (Docker Engine et Python 3). Le programme d'installation installe ce logiciel s'il n'est pas déjà installé sur les systèmes.
- Assurez-vous que vous disposez des privilèges root sur les systèmes Linux.
- Vérifiez que votre environnement répond aux exigences requises [autorisations et connectivité](#).
- Vous devez disposer des adresses IP des hôtes du nœud de scanner que vous prévoyez d'utiliser.
- Les ports et protocoles suivants doivent être activés sur tous les hôtes :

Port	Protocoles	Description
2377	TCP	Communications de gestion du cluster
7946	TCP, UDP	Communication inter-nœuds
4789	UDP	Superposition du trafic réseau
50	ESP	Trafic du réseau de superposition IPSec chiffré (ESP)
111	TCP, UDP	Serveur NFS pour le partage de fichiers entre les hôtes (requis de chaque nœud de scanner vers le nœud gestionnaire)
2049	TCP, UDP	Serveur NFS pour le partage de fichiers entre les hôtes (requis de chaque nœud de scanner vers le nœud gestionnaire)

## Étapes

1. Suivez les étapes 1 à 7 du [Installation avec un seul hôte](#) sur le nœud gestionnaire.
2. Comme indiqué à l'étape 8, lorsque le programme d'installation vous le demande, vous pouvez entrer les valeurs requises dans une série d'invites, ou vous pouvez fournir les paramètres requis comme arguments de ligne de commande au programme d'installation.

En plus des variables disponibles pour une installation à un seul hôte, une nouvelle option **-n <node\_ip>** est utilisée pour spécifier les adresses IP des nœuds du scanner. Plusieurs adresses IP de nœuds de scanner sont séparées par une virgule.

Par exemple, cette commande ajoute 3 nœuds de scanner :

```
sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host>
--manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --proxy-host
<proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy
-user <proxy_user> --proxy-password <proxy_password>
```

3. Avant la fin de l'installation du nœud Manager, une boîte de dialogue affiche la commande d'installation requise pour les nœuds du scanner. Copiez la commande et enregistrez-la dans un fichier texte. Par exemple :

```
sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212
```

4. Sur **chaque hôte de nœud du scanner** :

- a. Copiez le fichier d'installation de Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) sur la machine hôte (à l'aide de `scp` ou une autre méthode).
- b. Décompressez le fichier d'installation.
- c. Collez et exécutez la commande que vous avez copiée à l'étape 3.

Une fois l'installation terminée sur tous les nœuds du scanner et qu'ils ont été associés au nœud du gestionnaire, l'installation du nœud du gestionnaire se termine également.

## Résultat

Le programme d'installation de Cloud Data Sense termine l'installation des packages, de docker et enregistre l'installation. L'installation peut prendre entre 10 et 20 minutes.

## Et la suite

Dans la page Configuration, vous pouvez sélectionner les sources de données à numériser.

Vous pouvez également "[Configurer les licences pour Cloud Data Sense](#)" à ce moment-là. Vous ne serez facturé que lorsque la quantité de données dépasse 1 To.

## Déploiement des données cloud sur site sans accès Internet

Suivez quelques étapes pour déployer Cloud Data Sense sur un hôte dans un site sur site qui ne dispose pas d'un accès Internet. Ce type d'installation est parfait pour vos sites sécurisés.

Notez que vous pouvez également "[Déployer Data Sense dans un site sur site qui dispose d'un accès Internet](#)".



## Sources de données prises en charge

Lorsqu'il est installé de cette manière (parfois appelé site « hors ligne » ou « distant »), Data Sense peut uniquement analyser les données à partir de sources également locales sur site. A ce moment, Data Sense peut analyser les sources de données **locales** suivantes :

- Systèmes ONTAP sur site
- Schémas de base de données
- Comptes SharePoint sur site (SharePoint Server)
- Partages de fichiers CIFS ou NFS non NetApp
- Stockage objet qui utilise le protocole simple Storage Service (S3)

Dans les cas particuliers où vous avez besoin d'une installation BlueXP très sécurisée, mais que vous souhaitez également numériser des données locales à partir de comptes OneDrive ou de comptes SharePoint Online, vous pouvez utiliser le programme d'installation hors ligne Data Sense et fournir un accès Internet à quelques points de terminaison sélectionnés. Voir [Exigences spéciales relatives à SharePoint et OneDrive](#) pour plus d'informations.

L'analyse des comptes Cloud Volumes ONTAP, Azure NetApp Files, FSX pour ONTAP, AWS S3 ou Google Drive n'est pas prise en charge lorsque Data SENSE est déployé sur un site sombre.

## Limites

La plupart des fonctions de détection de données fonctionnent lorsqu'elles sont déployées sur un site sans accès à Internet. Toutefois, certaines fonctionnalités nécessitant un accès à Internet ne sont pas prises en charge, par exemple :

- Gestion des étiquettes Microsoft Azure information protection (AIP)
- Envoi d'alertes par e-mail aux utilisateurs BlueXP lorsque certaines stratégies critiques renvoient des résultats
- Définition des rôles BlueXP pour différents utilisateurs (par exemple, Account Admin ou Compliance Viewer)
- Copie et synchronisation des fichiers source à l'aide de Cloud Sync
- Réception des commentaires de l'utilisateur
- Mises à niveau logicielles automatisées depuis BlueXP

Le connecteur BlueXP et Data Sense nécessitent tous deux des mises à niveau manuelles régulières pour activer de nouvelles fonctionnalités. Vous pouvez voir la version de détection de données au bas des pages de l'interface utilisateur de détection de données. Vérifier le ["Notes de version de Cloud Data Sense"](#) pour voir les nouvelles fonctionnalités dans chaque version et si vous voulez ou non ces fonctionnalités. Vous pouvez ensuite suivre les étapes à [Mettez à niveau votre logiciel Data Sense](#).

## Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.



### Installez le connecteur BlueXP



Si aucun connecteur n'est déjà installé sur votre site hors ligne sur site, "[Déployer le connecteur](#)" Sur un hôte Linux.

2

### Passer en revue les prérequis Data Sense

Assurez-vous que votre système Linux est conforme au [configuration requise pour l'hôte](#), que tous les logiciels requis sont installés, et que votre environnement hors ligne répond aux exigences [autorisations et connectivité](#).

3

### Téléchargez et déployez Data Sense

Téléchargez le logiciel Cloud Data SENSE sur le site de support NetApp et copiez le fichier d'installation sur l'hôte Linux que vous prévoyez d'utiliser. Lancez ensuite l'assistant d'installation et suivez les invites pour déployer l'instance Cloud Data Sense.

4

### Abonnez-vous au service Cloud Data Sense

Les 1 premiers To de données scanners Cloud Data SENSE dans BlueXP sont gratuits. Une licence NetApp BYOL est requise pour continuer l'analyse des données après ce point.

## Installez le connecteur BlueXP

Si vous n'avez pas encore de connecteur BlueXP installé sur votre site hors ligne, "[Déployer le connecteur](#)" Sur un hôte Linux de votre site hors ligne.

## Préparez le système hôte Linux

Le logiciel de détection des données doit être exécuté sur un hôte qui répond à des exigences spécifiques du système d'exploitation, de la RAM, des exigences logicielles, etc. Data Sense n'est pas pris en charge sur un hôte partagé avec d'autres applications ; l'hôte doit être un hôte dédié.

- **Système d'exploitation** : Red Hat Enterprise Linux ou CentOS versions 8.0 à 8.6
  - La version 7.8 ou 7.9 peut être utilisée, mais la version du noyau Linux doit être 4.0 ou supérieure
  - Le système d'exploitation doit pouvoir installer le moteur Docker
- **Disque** : SSD avec 500 Gio disponible sur /, ou
  - 100 Gio disponible sur /opt
  - 400 Gio disponible sur /var
  - 5 Gio sur /tmp
- **RAM** : 64 Go (la mémoire d'échange doit être désactivée sur l'hôte)
- **CPU** : 16 cœurs

Notez que vous pouvez déployer Data Sense sur un système avec moins de processeurs et moins de RAM, mais il y a des limites lors de l'utilisation de ces systèmes. Voir "[Utilisation d'un type d'instance plus petit](#)" pour plus d'informations.

- **Logiciel supplémentaire**: Vous devez installer le logiciel suivant sur l'hôte avant d'installer Data Sense:
  - Docker Engine version 19 ou ultérieure. "[Voir les instructions d'installation](#)".
  - Python 3 version 3.6 ou ultérieure. "[Voir les instructions d'installation](#)".

- **Firesund considérations:** Si vous prévoyez d'utiliser `firewalld`, Nous vous recommandons de l'activer avant d'installer Data Sense. Exécutez les commandes suivantes pour configurer `firewalld` Pour qu'il soit compatible avec Data Sense :

```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-service=mysql
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=555/tcp
firewall-cmd --permanent --add-port=3306/tcp
firewall-cmd --reload
```

Si vous activez `firewalld` Après avoir installé Data Sense, vous devez redémarrer docker.



L'adresse IP du système hôte Data Sense ne peut pas être modifiée après l'installation.

## Vérifier les prérequis BlueXP et Data Sense

Avant de déployer Cloud Data, lisez les conditions préalables suivantes pour vérifier que la configuration est prise en charge.

- Assurez-vous que le connecteur dispose d'autorisations pour déployer des ressources et créer des groupes de sécurité pour l'instance Cloud Data Sense. Vous trouverez les dernières autorisations BlueXP dans ["Règles fournies par NetApp"](#).
- Assurez-vous de continuer d'exécuter le contrôle des données cloud. L'instance Cloud Data SENSE doit rester active pour analyser en continu vos données.
- Assurez la connectivité de votre navigateur Web au cloud Data Sense. Une fois Cloud Data SENSE activé, assurez-vous que les utilisateurs accèdent à l'interface BlueXP à partir d'un hôte connecté à l'instance Data Sense.

L'instance de détection de données utilise une adresse IP privée pour s'assurer que les données indexées ne sont pas accessibles aux autres. Par conséquent, le navigateur Web que vous utilisez pour accéder à BlueXP doit disposer d'une connexion à cette adresse IP privée. Cette connexion peut provenir d'un hôte qui se trouve dans le même réseau que l'instance Data Sense.

## Vérifiez que tous les ports requis sont activés

Vous devez vous assurer que tous les ports requis sont ouverts pour la communication entre le connecteur, Data Sense, Active Directory et vos sources de données.

Type de connexion	Ports	Description
Connecteur <> détection des données	8080 (TCP), 443 (TCP) et 80	Le groupe de sécurité du connecteur doit autoriser le trafic entrant et sortant via le port 443 vers et depuis l'instance de détection des données. Assurez-vous que le port 8080 est ouvert pour voir la progression de l'installation dans BlueXP.
Connecteur <> cluster ONTAP (NAS)	443 (TCP)	<p>BlueXP détecte les clusters ONTAP via HTTPS. Si vous utilisez des stratégies de pare-feu personnalisées, elles doivent répondre aux exigences suivantes :</p> <ul style="list-style-type: none"> <li>• L'hôte du connecteur doit autoriser l'accès HTTPS sortant via le port 443. Si le connecteur est dans le Cloud, toutes les communications sortantes sont autorisées par le groupe de sécurité prédéfini.</li> <li>• Le cluster ONTAP doit autoriser l'accès HTTPS entrant via le port 443. La stratégie de pare-feu " mgmt " par défaut permet l'accès HTTPS entrant à partir de toutes les adresses IP. Si vous avez modifié cette stratégie par défaut ou si vous avez créé votre propre stratégie de pare-feu, vous devez associer le protocole HTTPS à cette politique et activer l'accès à partir de l'hôte du connecteur.</li> </ul>
Cluster de détection des données <> ONTAP	<ul style="list-style-type: none"> <li>• Pour NFS - 111 (TCP/UDP) et 2049 (TCP/UDP)</li> <li>• Pour CIFS - 139 (TCP/UDP) et 445 (TCP/UDP)</li> </ul>	<p>La détection des données requiert une connexion réseau à chaque sous-réseau Cloud Volumes ONTAP ou système ONTAP sur site. Les groupes de sécurité pour Cloud Volumes ONTAP doivent autoriser les connexions entrantes à partir de l'instance de détection de données.</p> <p>Assurez-vous que ces ports sont ouverts à l'instance de détection de données :</p> <ul style="list-style-type: none"> <li>• Pour NFS - 111 et 2049</li> <li>• Pour CIFS : 139 et 445</li> </ul> <p>Les règles d'exportation de volumes NFS doivent autoriser l'accès à partir de l'instance Data Sense.</p>

Type de connexion	Ports	Description
Détection de données <> Active Directory	389 (TCP ET UDP), 636 (TCP), 3268 (TCP) ET 3269 (TCP)	<p>Un Active Directory doit déjà être configuré pour les utilisateurs de votre entreprise. En outre, Data Sense nécessite des identifiants Active Directory pour analyser les volumes CIFS.</p> <p>Vous devez disposer des informations pour Active Directory :</p> <ul style="list-style-type: none"> <li>• Adresse IP du serveur DNS ou adresses IP multiples</li> <li>• Nom d'utilisateur et mot de passe du serveur</li> <li>• Nom de domaine (nom Active Directory)</li> <li>• Que vous utilisiez ou non le protocole LDAP sécurisé (LDAPS)</li> <li>• Port serveur LDAP (généralement 389 pour LDAP et 636 pour LDAP sécurisé)</li> </ul>

Si vous utilisez plusieurs hôtes Data Sense pour fournir une puissance de traitement supplémentaire pour analyser vos sources de données, vous devez activer des ports/protocoles supplémentaires. "[Voir la configuration de port supplémentaire requise](#)".

### Exigences spéciales relatives à SharePoint et OneDrive

Lorsque BlueXP et Data Sense sont déployés sur un site sans accès à Internet, vous pouvez analyser les fichiers dans les comptes SharePoint Online et OneDrive en fournissant un accès Internet à quelques points de terminaison sélectionnés.

Les comptes sur site SharePoint installés localement peuvent être analysés sans accès à Internet.

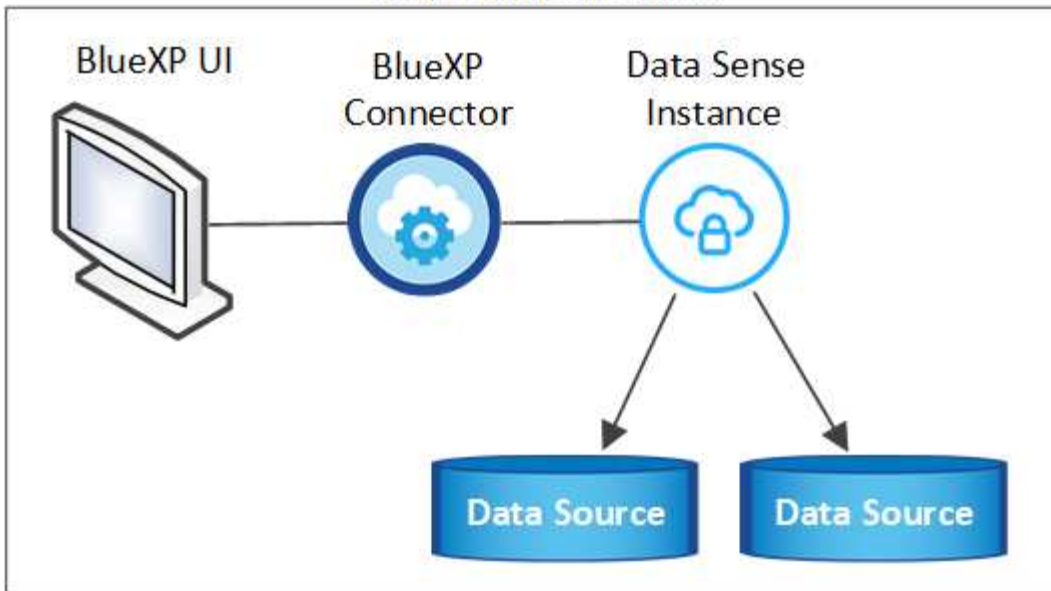
Terminaux	Objectif
\login.microsoft.com \graph.microsoft.com	Communication avec les serveurs Microsoft pour se connecter au service en ligne sélectionné.
https://api.bluexp.netapp.com	Communication avec le service BlueXP, qui inclut les comptes NetApp.

L'accès à *api.bluexp.netapp.com* n'est nécessaire que lors des connexions initiales à ces services externes.

### Déployer un sens des données

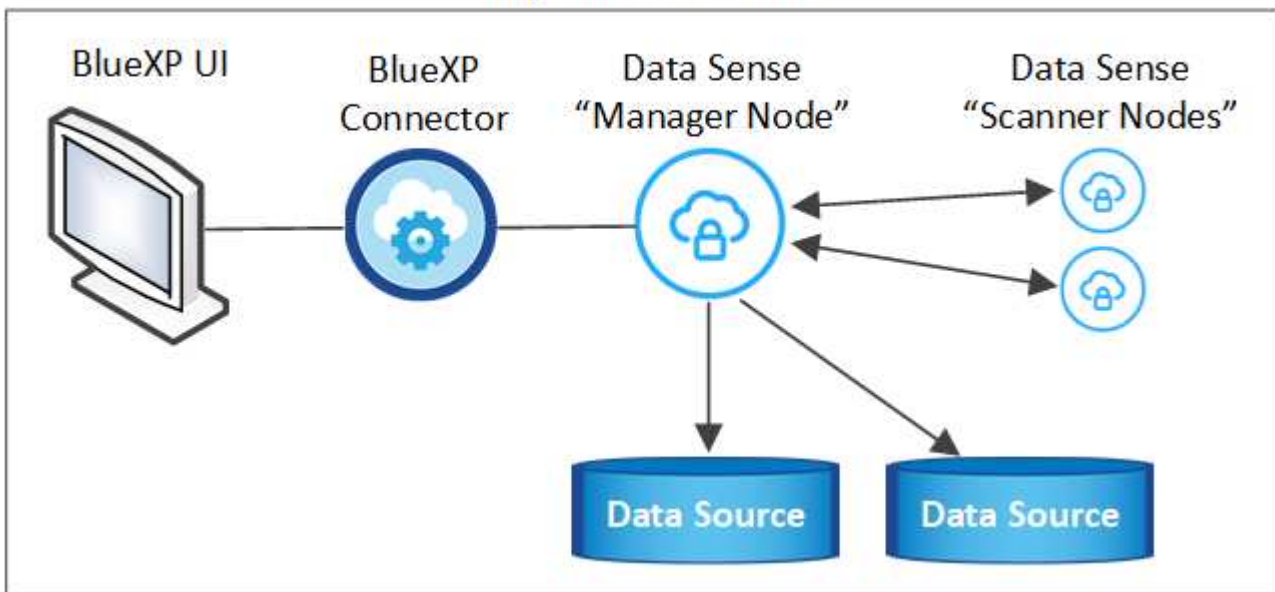
Pour les configurations standard, le logiciel est installé sur un système hôte unique. "[Découvrez ces étapes ici](#)".

### On-premises location



Pour les très grandes configurations dans lesquelles vous numérisez des pétaoctets de données, vous pouvez inclure plusieurs hôtes pour bénéficier d'une puissance de traitement supplémentaire. ["Découvrez ces étapes ici"](#).

### On-premises location



#### Installation à un seul hôte pour les configurations courantes

Procédez comme suit lors de l'installation du logiciel Data Sense sur un hôte sur site unique dans un environnement hors ligne.

#### Ce dont vous avez besoin

- Vérifiez que votre système Linux est conforme à la [configuration requise pour l'hôte](#).
- Vérifiez que vous avez installé les deux modules de prérequis logiciels (Docker Engine et Python 3).
- Assurez-vous que vous disposez des privilèges root sur le système Linux.

- Vérifiez que votre environnement hors ligne répond aux besoins [autorisations et connectivité](#).

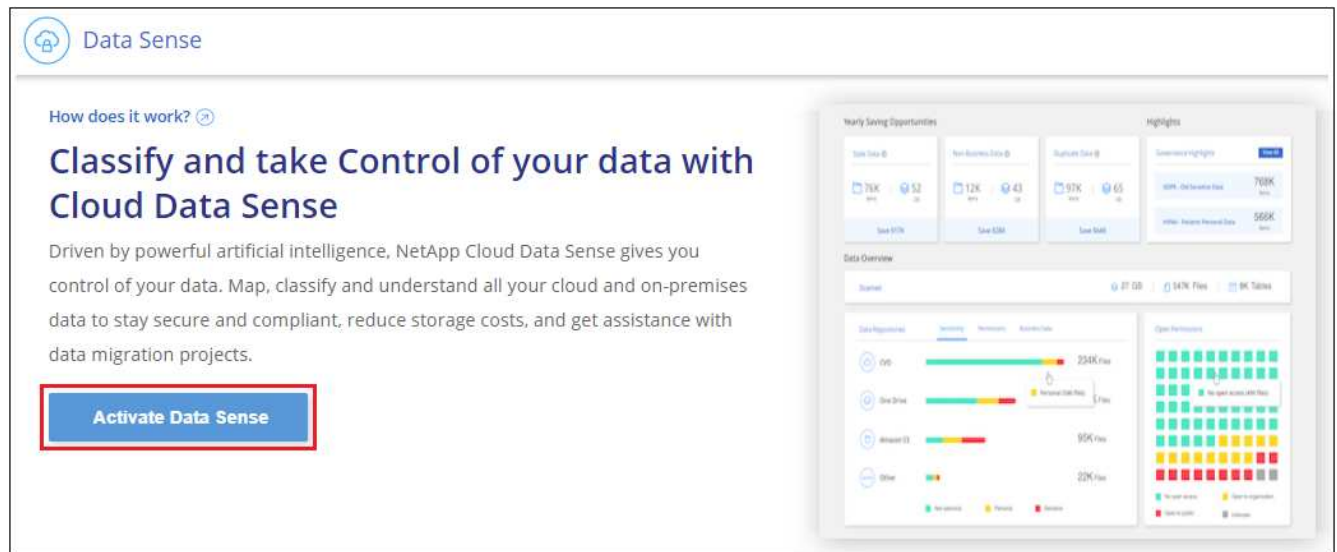
## Étapes

1. Sur un système configuré sur Internet, téléchargez le logiciel Cloud Data Sense à partir du "[Site de support NetApp](#)". Le fichier que vous devez sélectionner est nommé **DataSense-Offline-bundle-<version>.tar.gz**.
2. Copiez le pack d'installation sur l'hôte Linux que vous envisagez d'utiliser sur le site sombre.
3. Décompressez le programme d'installation sur la machine hôte, par exemple :

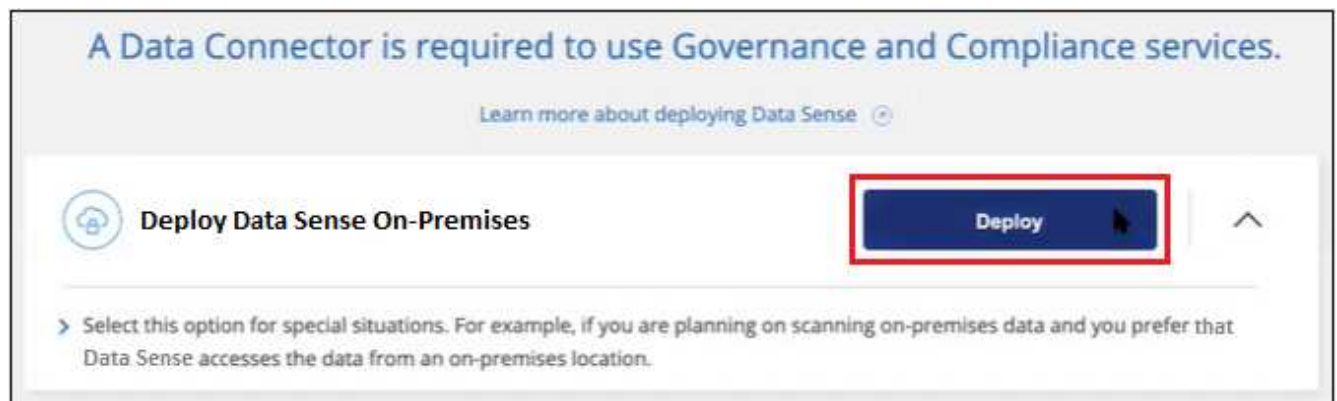
```
tar -xzf DataSense-offline-bundle-v1.16.1.tar.gz
```

Ceci extrait le logiciel requis et le fichier d'installation réel **DATASENSE-INSTALLER-V1.16.1.tar.gz**.

4. Lancez BlueXP et sélectionnez **gouvernance > Classification**.
5. Cliquez sur **Activer détection de données**.



6. Cliquez sur **déployer** pour démarrer l'assistant de déploiement sur site.



7. Dans la boîte de dialogue *Deploy Data Sense on local*, copiez la commande fournie et collez-la dans un fichier texte afin que vous puissiez l'utiliser ultérieurement, puis cliquez sur **Fermer**. Par exemple :

```
sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite
```

8. Décompressez le fichier d'installation sur la machine hôte, par exemple :

```
tar -xzf DATASENSE-INSTALLER-V1.16.1.tar.gz
```

9. Lorsque le programme d'installation vous le demande, vous pouvez entrer les valeurs requises dans une série d'invites, ou vous pouvez fournir les paramètres requis comme arguments de ligne de commande au programme d'installation :

Notez que le programme d'installation effectue une pré-vérification afin de s'assurer que vos exigences système et réseau sont en place pour une installation réussie.

Entrez les paramètres comme demandé :	Saisissez la commande complète :
<p>a. Coller les informations copiées à partir de l'étape 7 :</p> <pre>sudo ./install.sh -a &lt;account_id&gt; -c &lt;agent_id&gt; -t &lt;token&gt; --darksite</pre> <p>b. Entrez l'adresse IP ou le nom d'hôte de la machine hôte Data Sense afin qu'elle soit accessible par l'instance de connecteur.</p> <p>c. Entrez l'adresse IP ou le nom d'hôte de la machine hôte BlueXP Connector afin qu'elle soit accessible par l'instance Data Sense.</p>	<p>Vous pouvez également créer la commande entière à l'avance, en fournissant les paramètres d'hôte nécessaires :</p> <pre>sudo ./install.sh -a &lt;account_id&gt; -c &lt;agent_id&gt; -t &lt;token&gt; --host &lt;ds_host&gt; --manager-host &lt;cm_host&gt; --no-proxy --darksite</pre>

Valeurs variables :

- *Account\_ID* = ID du compte NetApp
- *Agent\_ID* = ID connecteur
- *token* = jeton utilisateur jwt
- *Ds\_host* = adresse IP ou nom d'hôte du système Data Sense Linux.
- *Cm\_host* = adresse IP ou nom d'hôte du système de connecteurs BlueXP.

## Résultat

Le programme d'installation de Data Sense installe les packages, enregistre l'installation et installe Data Sense. L'installation peut prendre entre 10 et 20 minutes.

S'il y a une connectivité sur le port 8080 entre la machine hôte et l'instance de connecteur, vous verrez la progression de l'installation dans l'onglet détection de données de BlueXP.

## Et la suite

Dans la page Configuration, vous pouvez sélectionner local ["Clusters ONTAP sur site"](#) et ["les bases de données"](#) que vous voulez numériser.

Vous pouvez également ["Configurer les licences BYOL pour Cloud Data Sense"](#) À partir de la page du porte-monnaie numérique. Vous ne serez facturé que lorsque la quantité de données dépasse 1 To.

## Installation de plusieurs hôtes pour de grandes configurations

Pour les très grandes configurations dans lesquelles vous numérisez des pétaoctets de données, vous pouvez inclure plusieurs hôtes pour bénéficier d'une puissance de traitement supplémentaire. Lors de l'utilisation de plusieurs systèmes hôtes, le système principal est appelé le *Manager node* et les systèmes supplémentaires qui fournissent une puissance de traitement supplémentaire sont appelés *scanner nodes*.

Procédez comme suit lors de l'installation du logiciel Data Sense sur plusieurs hôtes sur site dans un environnement hors ligne.

### Ce dont vous avez besoin

- Vérifiez que tous vos systèmes Linux pour les nœuds Manager et scanner sont conformes à la [configuration requise pour l'hôte](#).
- Vérifiez que vous avez installé les deux modules de prérequis logiciels (Docker Engine et Python 3).
- Assurez-vous que vous disposez des privilèges root sur les systèmes Linux.
- Vérifiez que votre environnement hors ligne répond aux besoins [autorisations et connectivité](#).
- Vous devez disposer des adresses IP des hôtes du nœud de scanner que vous prévoyez d'utiliser.
- Les ports et protocoles suivants doivent être activés sur tous les hôtes :

Port	Protocoles	Description
2377	TCP	Communications de gestion du cluster
7946	TCP, UDP	Communication inter-nœuds
4789	UDP	Superposition du trafic réseau
50	ESP	Trafic du réseau de superposition IPSec chiffré (ESP)
111	TCP, UDP	Serveur NFS pour le partage de fichiers entre les hôtes (requis de chaque nœud de scanner vers le nœud gestionnaire)
2049	TCP, UDP	Serveur NFS pour le partage de fichiers entre les hôtes (requis de chaque nœud de scanner vers le nœud gestionnaire)

### Étapes

1. Suivez les étapes 1 à 8 du "[Installation avec un seul hôte](#)" sur le nœud gestionnaire.
2. Comme indiqué à l'étape 9, lorsque le programme d'installation vous le demande, vous pouvez entrer les valeurs requises dans une série d'invites, ou vous pouvez fournir les paramètres requis comme arguments de ligne de commande au programme d'installation.

En plus des variables disponibles pour une installation à un seul hôte, une nouvelle option **-n <node\_ip>** est utilisée pour spécifier les adresses IP des nœuds du scanner. Plusieurs adresses IP de nœud sont séparées par une virgule.

Par exemple, cette commande ajoute 3 nœuds de scanner :

```
sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host>
--manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --no-proxy
--darksite
```

3. Avant la fin de l'installation du nœud Manager, une boîte de dialogue affiche la commande d'installation requise pour les nœuds du scanner. Copiez la commande et enregistrez-la dans un fichier texte. Par exemple :



```
sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212
```

#### 4. Sur **chaque hôte de nœud du scanner** :

- Copiez le fichier d'installation de Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) sur l'ordinateur hôte.
- Décompressez le fichier d'installation.
- Collez et exécutez la commande que vous avez copiée à l'étape 3.

Une fois l'installation terminée sur tous les nœuds du scanner et qu'ils ont été associés au nœud du gestionnaire, l'installation du nœud du gestionnaire se termine également.

### Résultat

Le programme d'installation de Cloud Data Sense termine l'installation des packages et enregistre l'installation. L'installation peut prendre entre 15 et 25 minutes.

### Et la suite

Dans la page Configuration, vous pouvez sélectionner local ["Clusters ONTAP sur site"](#) et locales ["les bases de données"](#) que vous voulez numériser.

Vous pouvez également ["Configurez les licences BYOL pour Cloud Data Sense"](#) À partir de la page du porte-monnaie numérique. Vous ne serez facturé que lorsque la quantité de données dépasse 1 To.

### Mettre à niveau le logiciel Data Sense

Le logiciel Data Sense étant mis à jour régulièrement avec de nouvelles fonctionnalités, vous devez rechercher régulièrement de nouvelles versions afin de vous assurer que vous utilisez les derniers logiciels et fonctionnalités. Vous devrez mettre à niveau le logiciel Data Sense manuellement car il n'y a pas de connexion Internet pour effectuer la mise à niveau automatiquement.

### Avant de commencer

- Le logiciel Data Sense peut être mis à niveau une version majeure à la fois. Par exemple, si la version 1.15.x est installée, vous ne pouvez effectuer la mise à niveau que vers la version 1.16.x. Si vous êtes quelques versions principales derrière, vous devrez mettre à niveau le logiciel à plusieurs reprises.
- Vérifiez que votre logiciel On-site Connector a été mis à niveau vers la dernière version disponible. ["Reportez-vous aux étapes de mise à niveau du connecteur"](#).

### Étapes

- Sur un système configuré sur Internet, téléchargez le logiciel Cloud Data Sense à partir du ["Site de support NetApp"](#). Le fichier que vous devez sélectionner est nommé **DataSense-Offline-bundle-<version>.tar.gz**.
- Copiez le pack logiciel sur l'hôte Linux où Data Sense est installé sur le site sombre.
- Décompressez le pack logiciel sur la machine hôte, par exemple :

```
tar -xvf DataSense-offline-bundle-v1.16.1.tar.gz
```

Ceci extrait le fichier d'installation **DATASENSE-INSTALLER-V1.16.1.tar.gz**.

- Décompressez le fichier d'installation sur la machine hôte, par exemple :

```
tar -xzf DATASENSE-INSTALLER-V1.16.1.tar.gz
```

Ceci extrait le script de mise à niveau **start\_darksite\_upgrade.sh** et tout logiciel tiers requis.

5. Exécutez le script de mise à niveau sur la machine hôte, par exemple :

```
start_darksite_upgrade.sh
```

### Résultat

Le logiciel Data Sense est mis à niveau sur votre hôte. La mise à jour peut prendre entre 5 et 10 minutes.

Notez qu'aucune mise à niveau n'est requise sur les nœuds du scanner si vous avez déployé Data Sense sur plusieurs systèmes hôtes pour analyser des configurations très volumineuses.

Vous pouvez vérifier que le logiciel a été mis à jour en vérifiant la version au bas des pages de l'interface utilisateur de détection de données.

## Activez la numérisation sur vos sources de données

### Mise en route de Cloud Data Sense pour Cloud Volumes ONTAP et ONTAP sur site

Procédez comme suit pour commencer à analyser les volumes ONTAP Cloud Volumes ONTAP et sur site à l'aide de Cloud Data SENSE.

#### Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

#### Découvrez les sources de données que vous souhaitez analyser

Avant de pouvoir numériser des volumes, vous devez ajouter les systèmes en tant qu'environnements de travail dans BlueXP :

- Pour les systèmes Cloud Volumes ONTAP, ces environnements de travail devraient déjà être disponibles dans BlueXP
- Pour les systèmes ONTAP sur site, ["BlueXP doit découvrir les clusters ONTAP"](#)

2

#### Déployez l'instance Cloud Data SENSE

["Déployez des données adaptées au cloud"](#) si aucune instance n'est déjà déployée.

3

#### Activez Cloud Data SENSE et sélectionnez les volumes à analyser

Cliquez sur **Data Sense**, sélectionnez l'onglet **Configuration** et activez les analyses de conformité pour les volumes dans des environnements de travail spécifiques.

## 4

### Vérifiez l'accès aux volumes

Lorsque Cloud Data SENSE est activé, assurez-vous qu'il peut accéder à tous les volumes.

- L'instance Cloud Data Sense doit être connectée réseau à chaque sous-réseau Cloud Volumes ONTAP ou système ONTAP sur site.
- Les groupes de sécurité pour Cloud Volumes ONTAP doivent autoriser les connexions entrantes à partir de l'instance de détection de données.
- Assurez-vous que ces ports sont ouverts à l'instance de détection de données :
  - Pour NFS – ports 111 et 2049.
  - Pour CIFS – ports 139 et 445.
- Les règles d'exportation de volumes NFS doivent autoriser l'accès à partir de l'instance Data Sense.
- La détection de données a besoin des identifiants Active Directory pour analyser les volumes CIFS.

Cliquez sur **Compliance > Configuration > Modifier les informations d'identification CIFS** et fournissez les informations d'identification.

## 5

### Gérer les volumes à analyser

Sélectionnez ou désélectionnez les volumes que vous souhaitez scanner et Cloud Data SENSE démarre ou arrête l'acquisition.

#### Recherche des sources de données que vous souhaitez analyser

Si les sources de données que vous souhaitez numériser ne se trouvent pas déjà dans votre environnement BlueXP, vous pouvez les ajouter au canevas pour le moment.

Vos systèmes Cloud Volumes ONTAP devraient déjà être disponibles dans la zone de travail de BlueXP. Dont vous avez besoin avec les systèmes ONTAP sur site "[BlueXP découvre ces clusters](#)".

#### Déploiement de l'instance Cloud Data Sense

Déployez Cloud Data si aucune instance n'est déjà déployée.

Si vous numérisez des systèmes Cloud Volumes ONTAP et ONTAP sur site accessibles via Internet, vous pouvez "[Déployez les données du cloud dans le cloud](#)" ou "[dans un emplacement sur site avec accès à internet](#)".

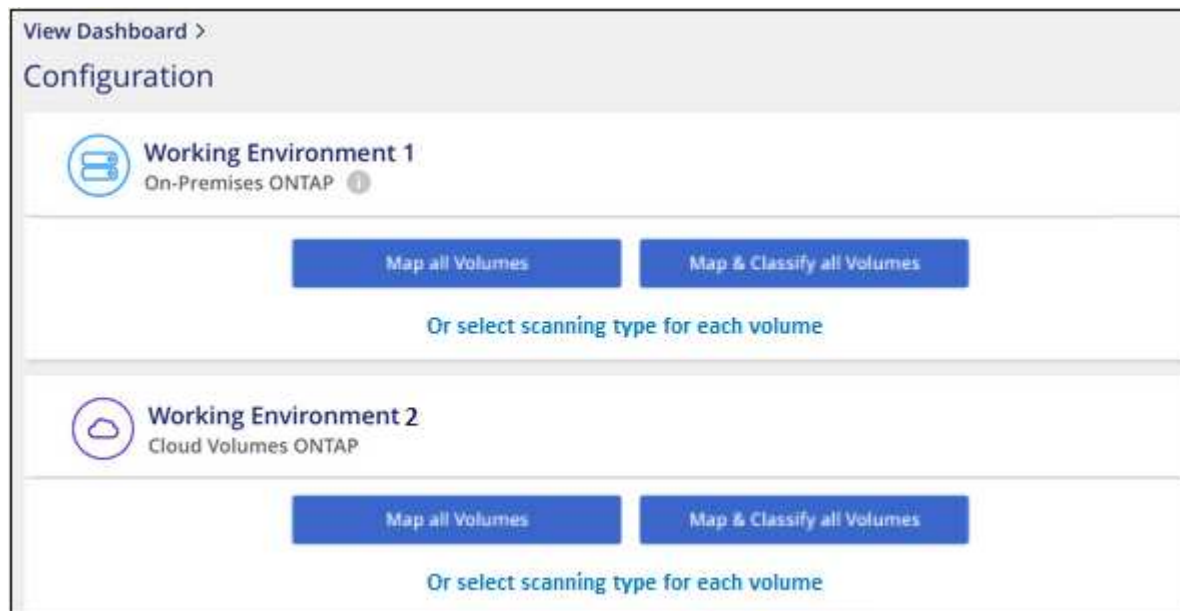
Si vous numérisez des systèmes ONTAP sur site qui ont été installés sur un site sombre et ne disposant pas d'accès à Internet, vous devez le faire "[Déployez les données cloud sur site qui ne disposent pas d'un accès Internet](#)". Cela nécessite également que le connecteur BlueXP soit déployé dans le même emplacement sur site.

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

#### Activation des données cloud dans vos environnements de travail

Vous pouvez activer Cloud Data Sense sur les systèmes Cloud Volumes ONTAP dans n'importe quel fournisseur cloud pris en charge et dans des clusters ONTAP sur site.

1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.



2. Sélectionnez le mode de numérisation des volumes dans chaque environnement de travail. ["En savoir plus sur les acquisitions de mappage et de classification"](#):

- Pour mapper tous les volumes, cliquez sur **mapper tous les volumes**.
- Pour mapper et classer tous les volumes, cliquez sur **cartographier et classer tous les volumes**.
- Pour personnaliser la numérisation de chaque volume, cliquez sur **ou sélectionnez le type de numérisation pour chaque volume**, puis choisissez les volumes que vous souhaitez mapper et/ou classer.

Voir [Activation et désactivation des analyses de conformité sur les volumes](#) pour plus d'informations.

3. Dans la boîte de dialogue de confirmation, cliquez sur **approuver** pour que Data Sense commence à analyser vos volumes.

## Résultat

Cloud Data SENSE commence à analyser les volumes que vous avez sélectionnés dans l'environnement de travail. Les résultats seront disponibles dans le tableau de bord de conformité dès que Cloud Data SENSE aura terminé les analyses initiales. Le temps nécessaire dépend de la quantité de données—il peut être de quelques minutes ou heures.

## Vérifier que le sens des données cloud a accès aux volumes

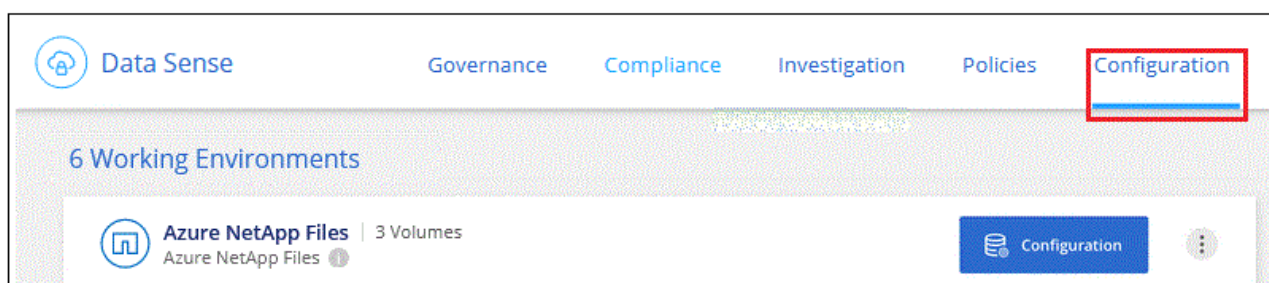
Assurez-vous que Cloud Data est capable d'accéder aux volumes en vérifiant vos groupes de sécurité et vos règles d'exportation. Vous devez fournir un « logique de données » avec des identifiants CIFS pour pouvoir accéder aux volumes CIFS.

## Étapes

1. Assurez-vous qu'il existe une connexion réseau entre l'instance Cloud Data Sense et chaque réseau incluant des volumes pour les clusters Cloud Volumes ONTAP ou ONTAP sur site.
2. Assurez-vous que le groupe de sécurité pour Cloud Volumes ONTAP autorise le trafic entrant à partir de l'instance de détection de données.

Vous pouvez soit ouvrir le groupe de sécurité pour le trafic à partir de l'adresse IP de l'instance de détection de données, soit ouvrir le groupe de sécurité pour tout le trafic à partir du réseau virtuel.

3. Assurez-vous que les ports suivants sont ouverts à l'instance de détection de données :
  - Pour NFS – ports 111 et 2049.
  - Pour CIFS – ports 139 et 445.
4. Assurez-vous que les règles d'exportation de volume NFS incluent l'adresse IP de l'instance Data Sense afin qu'elle puisse accéder aux données sur chaque volume.
5. Si vous utilisez le protocole CIFS, fournissez Data Sense avec des identifiants Active Directory afin qu'il puisse analyser les volumes CIFS.
  - a. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.

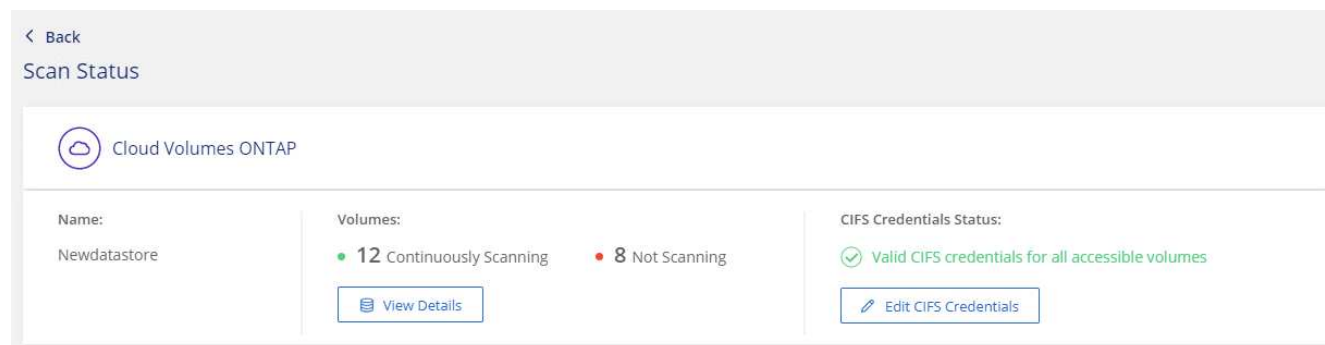


- b. Pour chaque environnement de travail, cliquez sur **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe dont Data Sense a besoin pour accéder aux volumes CIFS sur le système.

Les informations d'identification peuvent être en lecture seule, mais fournir des informations d'identification admin garantit que Data Sense peut lire toutes les données qui requièrent des autorisations élevées. Les identifiants sont stockés sur l'instance Cloud Data Sense.

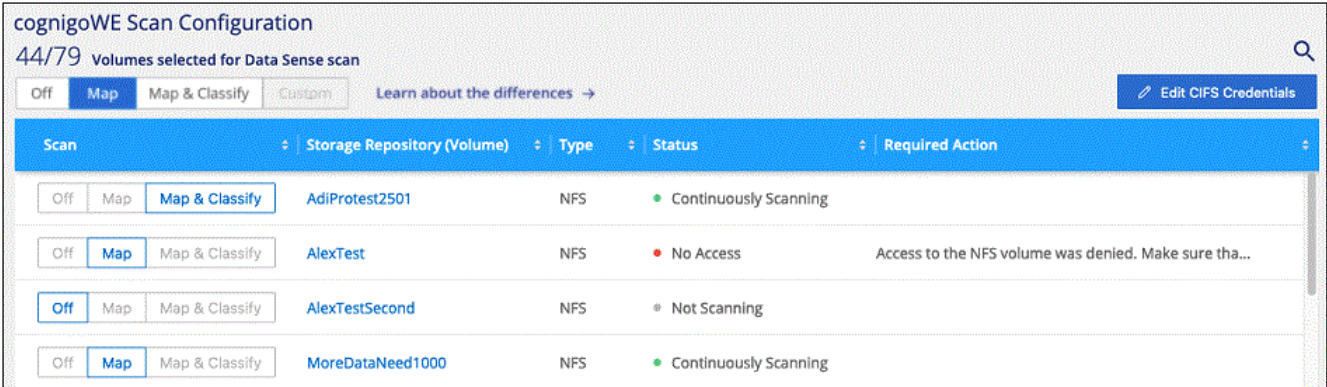
Si vous voulez vous assurer que vos fichiers "dernières heures d'accès" sont inchangés par les analyses de classification de détection de données, nous recommandons à l'utilisateur de disposer de l'autorisation Write Attributes. Si possible, nous vous recommandons de faire en sorte que l'utilisateur configuré Active Directory fasse partie d'un groupe parent de l'organisation qui dispose des autorisations pour tous les fichiers.

Une fois les informations d'identification saisies, un message indiquant que tous les volumes CIFS ont été authentifiés avec succès s'affiche.



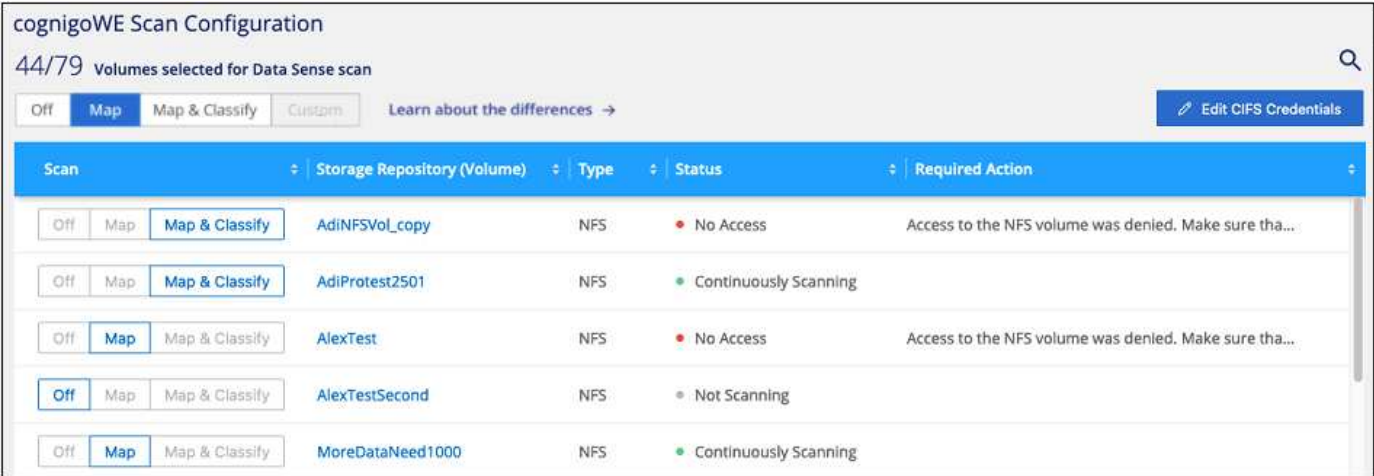
6. Sur la page *Configuration*, cliquez sur **View Details** pour vérifier l'état de chaque volume CIFS et NFS et corriger les erreurs éventuelles.

L'image suivante montre par exemple quatre volumes dont l'un des types de données cloud n'est pas capable de se scanner en raison de problèmes de connectivité réseau entre l'instance Data Sense et le volume.



Activation et désactivation des analyses de conformité sur les volumes

Vous pouvez démarrer ou arrêter des analyses de mappage uniquement, ou des analyses de mappage et de classification, dans un environnement de travail à tout moment à partir de la page Configuration. Vous pouvez également passer des acquisitions avec mappage uniquement à des acquisitions avec mappage et classification, et inversement. Nous vous recommandons de scanner tous les volumes.



À :	Procédez comme suit :
Activez les acquisitions avec mappage uniquement sur un volume	Dans la zone du volume, cliquez sur <b>Map</b>
Activer la numérisation complète sur un volume	Dans la zone de volume, cliquez sur <b>carte et classement</b>
Désactiver la numérisation sur un volume	Dans la zone du volume, cliquez sur <b>Off</b>
Activez les analyses de mappage uniquement sur tous les volumes	Dans la zone d'en-tête, cliquez sur <b>carte</b>
Activez l'analyse complète sur tous les volumes	Dans la zone d'en-tête, cliquez sur <b>carte et classement</b>
Désactiver l'analyse de tous les volumes	Dans la zone d'en-tête, cliquez sur <b>Off</b>





Les nouveaux volumes ajoutés à l'environnement de travail sont automatiquement analysés uniquement lorsque vous avez défini le paramètre **Map** ou **Map & Classify** dans la zone d'entête. Lorsque vous sélectionnez **personnalisé** ou **Désactivé** dans la zone de titre, vous devez activer le mappage et/ou la numérisation complète sur chaque nouveau volume que vous ajoutez à l'environnement de travail.

## Analyse des volumes de protection des données

Par défaut, les volumes DP ne sont pas analysés parce qu'ils ne sont pas exposés en externe et que Cloud Data SENSE ne peut pas y accéder. Il s'agit des volumes de destination des opérations SnapMirror depuis un système ONTAP sur site ou à partir d'un système Cloud Volumes ONTAP.

Initialement, la liste de volumes identifie ces volumes comme *Type DP* avec *Status Not Scanning* et la *Required action Enable Access to DP volumes*.

**'Working Environment Name' Configuration**

22/28 Volumes selected for compliance scan

**Enable Access to DP Volumes** [Edit CIFS Credentials](#)

Off **Map** Map & Classify Custom [Learn about the differences](#) →

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off <b>Map</b> Map & Classify	VolumeName1	DP	Not Scanning	Enable access to DP Volumes ⓘ
Off <b>Map</b> Map & Classify	VolumeName2	NFS	Continuously Scanning	
Off <b>Map</b> Map & Classify	VolumeName3	CIFS	Not Scanning	

## Étapes

Pour analyser ces volumes de protection des données :

1. Cliquez sur **Activer l'accès aux volumes DP** en haut de la page.
2. Vérifiez le message de confirmation et cliquez à nouveau sur **Activer l'accès aux volumes DP**.
  - Les volumes initialement créés en tant que volumes NFS dans le système ONTAP source sont activés.
  - Pour les volumes initialement créés en tant que volumes CIFS dans le système ONTAP source, vous devez entrer des identifiants CIFS pour scanner ces volumes DP. Si vous avez déjà saisi les informations d'identification Active Directory afin que Cloud Data SENSE puisse analyser des volumes CIFS, vous pouvez utiliser ces informations d'identification ou spécifier un autre ensemble d'informations d'identification Admin.

**Provide Active Directory Credentials**

☒ Use existing CIFS Scanning Credentials (user1@domain2) ☐ Use Custom Credentials

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for **Data Sense**. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

**Enable Access to DP Volumes** Cancel

**Provide Active Directory Credentials**

☐ Use existing CIFS Scanning Credentials (user1@domain2) ☒ Use Custom Credentials

Username ⓘ Password

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for **Data Sense**. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

**Enable Access to DP Volumes** Cancel

3. Activez chaque volume DP que vous souhaitez analyser [de la même façon que vous avez activé d'autres volumes](#).

## Résultat

Une fois activée, Cloud Data Sense crée un partage NFS à partir de chaque volume DP activé pour l'analyse. Les règles d'exportation de partage autorisent uniquement l'accès à partir de l'instance de détection de données.

**Remarque :** si vous ne aviez pas de volumes de protection des données CIFS lorsque vous avez activé l'accès initial aux volumes DP, puis en ajoutant d'autres, le bouton **Activer l'accès à CIFS DP** s'affiche en haut de la page Configuration. Cliquez sur ce bouton et ajoutez des identifiants CIFS pour permettre l'accès à ces volumes CIFS DP.



Les identifiants Active Directory sont uniquement enregistrés dans la machine virtuelle de stockage du premier volume CIFS DP, de sorte que tous les volumes DP de ce SVM soient analysés. Les volumes résidant sur d'autres SVM ne seront pas enregistrés pour les identifiants Active Directory, de sorte que ces volumes DP ne seront pas analysés.

## Mise en route de Cloud Data Sense for Azure NetApp Files

Suivez ces quelques étapes pour commencer à utiliser Cloud Data Sense for Azure NetApp Files.

### Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

#### Découvrez les systèmes Azure NetApp Files que vous souhaitez analyser

Avant de pouvoir analyser des volumes Azure NetApp Files, ["BlueXP doit être configuré pour détecter la configuration"](#).

2

#### Déployez l'instance Cloud Data SENSE

["Déployez Cloud Data Sense dans BlueXP"](#) si aucune instance n'est déjà déployée.

3

#### Activez Cloud Data SENSE et sélectionnez les volumes à analyser

Cliquez sur **Compliance**, sélectionnez l'onglet **Configuration** et activez les analyses de conformité pour les volumes dans des environnements de travail spécifiques.

4

#### Vérifiez l'accès aux volumes

Lorsque Cloud Data SENSE est activé, assurez-vous qu'il peut accéder à tous les volumes.

- L'instance Cloud Data SENSE doit disposer d'une connexion réseau à chaque sous-réseau Azure NetApp Files.
- Assurez-vous que ces ports sont ouverts à l'instance de détection de données :



- Pour NFS – ports 111 et 2049.
- Pour CIFS – ports 139 et 445.
- Les règles d'exportation de volumes NFS doivent autoriser l'accès à partir de l'instance Data Sense.
- La détection de données a besoin des identifiants Active Directory pour analyser les volumes CIFS.

Cliquez sur **Compliance > Configuration > Modifier les informations d'identification CIFS** et fournissez les informations d'identification.

## 5

### Gérer les volumes à analyser

Sélectionnez ou désélectionnez les volumes que vous souhaitez scanner et Cloud Data SENSE démarre ou arrête l'acquisition.

#### Détection du système Azure NetApp Files que vous souhaitez numériser

Si le système Azure NetApp Files que vous voulez numériser n'est pas déjà dans BlueXP comme environnement de travail, vous pouvez l'ajouter au canevas pour le moment.

["Découvrez comment découvrir le système Azure NetApp Files dans BlueXP".](#)

#### Déploiement de l'instance Cloud Data Sense

["Déployez des données adaptées au cloud"](#) si aucune instance n'est déjà déployée.

Il est nécessaire de déployer Data Sense dans le cloud lors de l'analyse des volumes Azure NetApp Files, et il doit être déployé dans la même région que les volumes que vous souhaitez analyser.

**Remarque :** le déploiement de Cloud Data Sense dans un emplacement sur site n'est pas pris en charge actuellement lors de l'analyse de volumes Azure NetApp Files.

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

#### Activation des données cloud dans vos environnements de travail

Vous pouvez activer Cloud Data SENSE sur vos volumes Azure NetApp Files.

1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.



2. Sélectionnez le mode de numérisation des volumes dans chaque environnement de travail. ["En savoir plus sur les acquisitions de mappage et de classification"](#):

- Pour mapper tous les volumes, cliquez sur **mapper tous les volumes**.
- Pour mapper et classer tous les volumes, cliquez sur **cartographier et classer tous les volumes**.
- Pour personnaliser la numérisation de chaque volume, cliquez sur **ou sélectionnez le type de numérisation pour chaque volume**, puis choisissez les volumes que vous souhaitez mapper et/ou classer.

Voir [Activation et désactivation des analyses de conformité sur les volumes](#) pour plus d'informations.

3. Dans la boîte de dialogue de confirmation, cliquez sur **approuver** pour que Data Sense commence à analyser vos volumes.

## Résultat

Cloud Data SENSE commence à analyser les volumes que vous avez sélectionnés dans l'environnement de travail. Les résultats seront disponibles dans le tableau de bord de conformité dès que Cloud Data SENSE aura terminé les analyses initiales. Le temps nécessaire dépend de la quantité de données—il peut être de quelques minutes ou heures.

## Vérifier que le sens des données cloud a accès aux volumes

Assurez-vous que Cloud Data est capable d'accéder aux volumes en vérifiant vos groupes de sécurité et vos règles d'exportation. Vous devez fournir un « logique de données » avec des identifiants CIFS pour pouvoir accéder aux volumes CIFS.

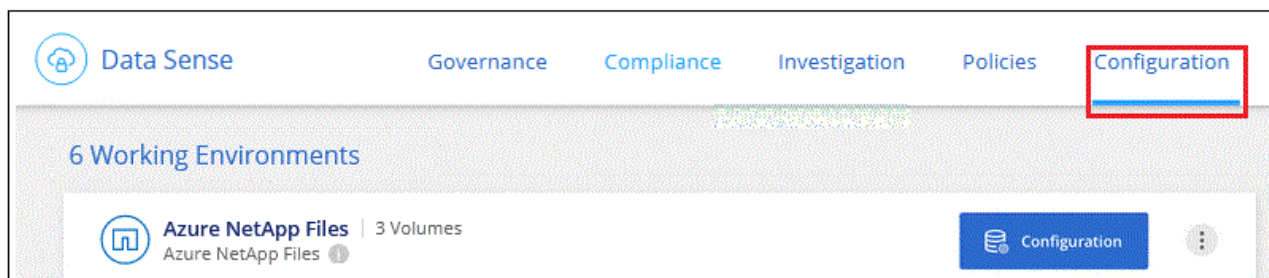
## Étapes

1. Vérifiez qu'il existe une connexion réseau entre l'instance Cloud Data Sense et chaque réseau incluant des volumes pour Azure NetApp Files.



Pour Azure NetApp Files, Cloud Data SENSE ne peut analyser que les volumes se trouvant dans la même région que BlueXP.

2. Assurez-vous que les ports suivants sont ouverts à l'instance de détection de données :
  - Pour NFS – ports 111 et 2049.
  - Pour CIFS – ports 139 et 445.
3. Assurez-vous que les règles d'exportation de volume NFS incluent l'adresse IP de l'instance Data Sense afin qu'elle puisse accéder aux données sur chaque volume.
4. Si vous utilisez le protocole CIFS, fournissez Data Sense avec des identifiants Active Directory afin qu'il puisse analyser les volumes CIFS.
  - a. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.

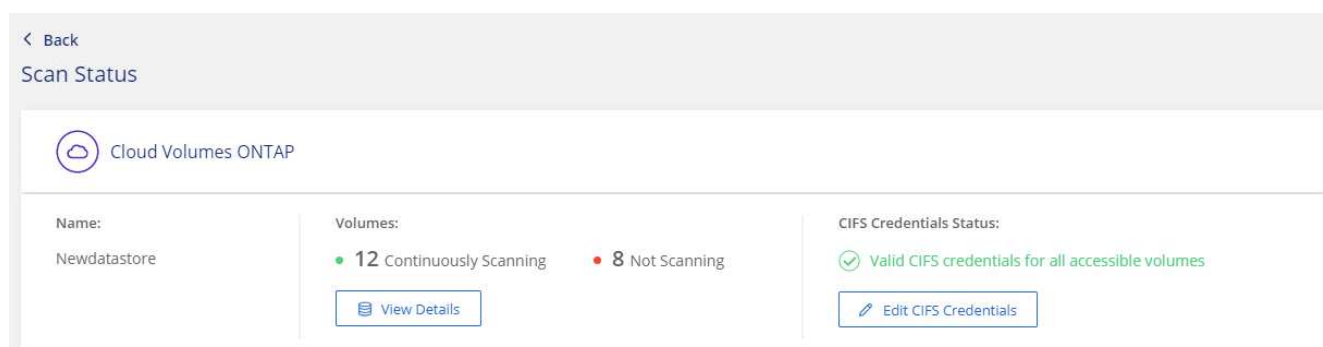


- b. Pour chaque environnement de travail, cliquez sur **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe dont Data Sense a besoin pour accéder aux volumes CIFS sur le système.

Les informations d'identification peuvent être en lecture seule, mais fournir des informations d'identification admin garantit que Data Sense peut lire toutes les données qui requièrent des autorisations élevées. Les identifiants sont stockés sur l'instance Cloud Data Sense.

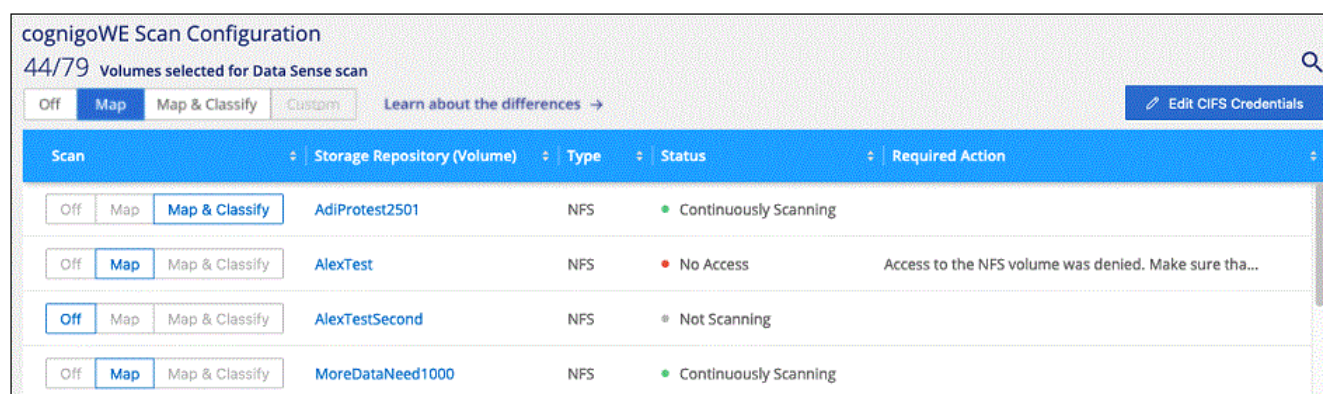
Si vous voulez vous assurer que vos fichiers “dernières heures d'accès” sont inchangés par les analyses de classification de détection de données, nous recommandons à l'utilisateur de disposer de l'autorisation Write Attributes. Si possible, nous vous recommandons de faire en sorte que l'utilisateur configuré Active Directory fasse partie d'un groupe parent de l'organisation qui dispose des autorisations pour tous les fichiers.

Une fois les informations d'identification saisies, un message indiquant que tous les volumes CIFS ont été authentifiés avec succès s'affiche.



5. Sur la page *Configuration*, cliquez sur **View Details** pour vérifier l'état de chaque volume CIFS et NFS et corriger les erreurs éventuelles.

L'image suivante montre par exemple quatre volumes dont l'un des types de données cloud n'est pas capable de se scanner en raison de problèmes de connectivité réseau entre l'instance Data Sense et le volume.



## Activation et désactivation des analyses de conformité sur les volumes

Vous pouvez démarrer ou arrêter des analyses de mappage uniquement, ou des analyses de mappage et de classification, dans un environnement de travail à tout moment à partir de la page Configuration. Vous pouvez également passer des acquisitions avec mappage uniquement à des acquisitions avec mappage et classification, et inversement. Nous vous recommandons de scanner tous les volumes.

cognigoWE Scan Configuration
44/79 Volumes selected for Data Sense scan

Off

Map

Map & Classify

Custom

Learn about the differences →

Edit CIFS Credentials

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map <b>Map &amp; Classify</b>	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
Off Map <b>Map &amp; Classify</b>	AdiProtest2501	NFS	Continuously Scanning	
Off <b>Map</b> Map & Classify	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<b>Off</b> Map Map & Classify	AlexTestSecond	NFS	Not Scanning	
Off <b>Map</b> Map & Classify	MoreDataNeed1000	NFS	Continuously Scanning	

À :	Procédez comme suit :
Activez les acquisitions avec mappage uniquement sur un volume	Dans la zone du volume, cliquez sur <b>Map</b>
Activer la numérisation complète sur un volume	Dans la zone de volume, cliquez sur <b>carte et classement</b>
Désactiver la numérisation sur un volume	Dans la zone du volume, cliquez sur <b>Off</b>
Activez les analyses de mappage uniquement sur tous les volumes	Dans la zone d'en-tête, cliquez sur <b>carte</b>
Activez l'analyse complète sur tous les volumes	Dans la zone d'en-tête, cliquez sur <b>carte et classement</b>
Désactiver l'analyse de tous les volumes	Dans la zone d'en-tête, cliquez sur <b>Off</b>



Les nouveaux volumes ajoutés à l'environnement de travail sont automatiquement analysés uniquement lorsque vous avez défini le paramètre **Map** ou **Map & Classify** dans la zone d'en-tête. Lorsque vous sélectionnez **personnalisé** ou **Désactivé** dans la zone de titre, vous devez activer le mappage et/ou la numérisation complète sur chaque nouveau volume que vous ajoutez à l'environnement de travail.

## Lancez-vous avec Cloud Data Sense for Amazon FSX pour ONTAP

Suivez quelques étapes pour commencer l'analyse d'Amazon FSX pour les volumes ONTAP avec Cloud Data Sense.

### Avant de commencer

- Vous avez besoin d'un connecteur actif dans AWS pour déployer et gérer Data Sense.
- Le groupe de sécurité que vous avez sélectionné lors de la création de l'environnement de travail doit autoriser le trafic à partir de l'instance Cloud Data SENSE. Vous pouvez trouver le groupe de sécurité associé à l'aide de l'ENI connecté au système de fichiers FSX pour ONTAP et le modifier à l'aide de la console de gestion AWS.

["Groupes de sécurité AWS pour les instances Linux"](#)

["Groupes de sécurité AWS pour les instances Windows"](#)

["Interfaces réseau flexibles AWS \(ENI\)"](#)

## Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler vers le bas pour obtenir plus de détails.

1

### Découvrez le FSX pour les systèmes de fichiers ONTAP que vous souhaitez analyser

Avant de pouvoir analyser FSX pour des volumes ONTAP, "[Vous devez disposer d'un environnement de travail FSX avec des volumes configurés](#)".

2

### Déployez l'instance Cloud Data SENSE

"[Déployez Cloud Data Sense dans BlueXP](#)" si aucune instance n'est déjà déployée.

3

### Activez Cloud Data SENSE et sélectionnez les volumes à analyser

Cliquez sur **Data Sense**, sélectionnez l'onglet **Configuration** et activez les analyses de conformité pour les volumes dans des environnements de travail spécifiques.

4

### Vérifiez l'accès aux volumes

Lorsque Cloud Data SENSE est activé, assurez-vous qu'il peut accéder à tous les volumes.

- L'instance Cloud Data SENSE doit disposer d'une connexion réseau à chaque sous-réseau FSX pour ONTAP.
- Assurez-vous que les ports suivants sont ouverts à l'instance de détection de données :
  - Pour NFS – ports 111 et 2049.
  - Pour CIFS – ports 139 et 445.
- Les règles d'exportation de volumes NFS doivent autoriser l'accès à partir de l'instance Data Sense.
- La détection de données a besoin des identifiants Active Directory pour analyser les volumes CIFS. + cliquez sur **conformité > Configuration > Modifier les informations d'identification CIFS** et fournissez les informations d'identification.

5

### Gérer les volumes à analyser

Sélectionnez ou désélectionnez les volumes que vous souhaitez analyser et Cloud Data SENSE démarre ou arrête l'acquisition.

## Détection du système de fichiers FSX pour ONTAP que vous souhaitez numériser

Si le système de fichiers FSX pour ONTAP que vous souhaitez numériser n'est pas déjà dans BlueXP comme environnement de travail, vous pouvez l'ajouter au canevas à ce moment.

["Découvrez comment découvrir ou créer le système de fichiers FSX pour ONTAP dans BlueXP"](#).

## Déploiement de l'instance Cloud Data Sense

"Déployez des données adaptées au cloud" si aucune instance n'est déjà déployée.

Vous devez déployer Data Sense dans le même réseau AWS que le connecteur pour AWS et les volumes FSX que vous souhaitez analyser.

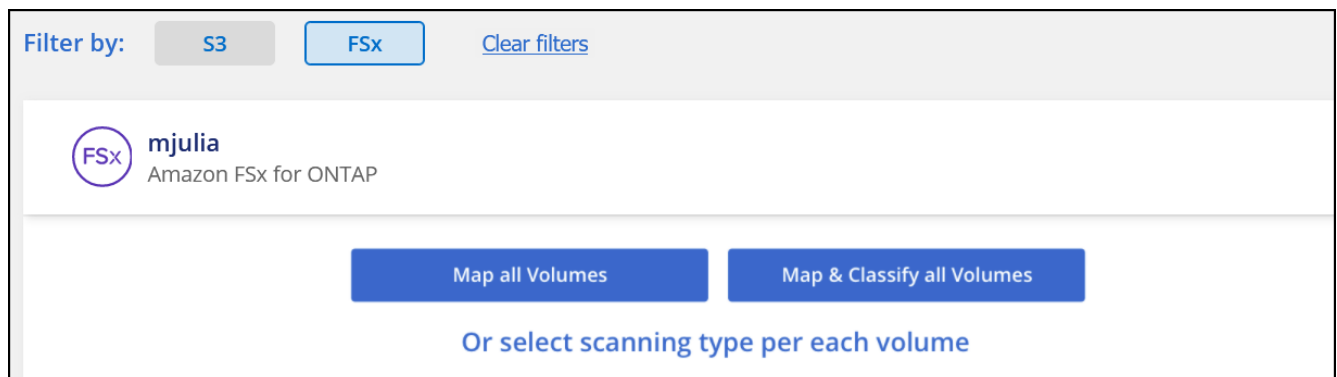
**Remarque :** le déploiement de Cloud Data SENSE dans un emplacement sur site n'est pas pris en charge actuellement lors de l'analyse de volumes FSX.

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

## Activation des données cloud dans vos environnements de travail

Vous pouvez activer Cloud Data Sense pour FSX pour les volumes ONTAP.

1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.



2. Sélectionnez le mode de numérisation des volumes dans chaque environnement de travail. ["En savoir plus sur les acquisitions de mappage et de classification"](#):
  - Pour mapper tous les volumes, cliquez sur **mapper tous les volumes**.
  - Pour mapper et classer tous les volumes, cliquez sur **cartographier et classer tous les volumes**.
  - Pour personnaliser la numérisation de chaque volume, cliquez sur **ou sélectionnez le type de numérisation pour chaque volume**, puis choisissez les volumes que vous souhaitez mapper et/ou classer.

Voir [Activation et désactivation des analyses de conformité sur les volumes](#) pour plus d'informations.

3. Dans la boîte de dialogue de confirmation, cliquez sur **approuver** pour que Data Sense commence à analyser vos volumes.

## Résultat

Cloud Data SENSE commence à analyser les volumes que vous avez sélectionnés dans l'environnement de travail. Les résultats seront disponibles dans le tableau de bord de conformité dès que Cloud Data SENSE aura terminé les analyses initiales. Le temps nécessaire dépend de la quantité de données—il peut être de quelques minutes ou heures.

## Vérifier que le sens des données cloud a accès aux volumes

Assurez-vous que Cloud Data peut détecter l'accès aux volumes en vérifiant vos groupes de sécurité et vos



règles de mise en réseau et d'exportation.

Vous devez fournir un « logique de données » avec des identifiants CIFS pour pouvoir accéder aux volumes CIFS.

## Étapes

1. Sur la page *Configuration*, cliquez sur **Afficher les détails** pour vérifier l'état et corriger les erreurs.

Par exemple, l'image suivante montre qu'un volume Cloud Data SENSE ne peut pas se scanner en raison de problèmes de connectivité réseau entre l'instance Data Sense et le volume.

Scan	Storage Repository (Volume)	Type	Status	Required Action
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map &amp; Classify"/>	jrmclone	NFS	<span style="color: red;">●</span> No Access	Check network connectivity between the Data Sense ...

2. Vérifiez qu'il existe une connexion réseau entre l'instance Cloud Data Sense et chaque réseau incluant des volumes pour FSX pour ONTAP.



Pour FSX pour ONTAP, Cloud Data SENSE ne peut analyser les volumes que dans la même région que BlueXP.

3. Assurez-vous que les ports suivants sont ouverts à l'instance de détection de données.
  - Pour NFS – ports 111 et 2049.
  - Pour CIFS – ports 139 et 445.
4. Assurez-vous que les règles d'exportation de volume NFS incluent l'adresse IP de l'instance Data Sense afin qu'elle puisse accéder aux données sur chaque volume.
5. Si vous utilisez le protocole CIFS, fournissez Data Sense avec des identifiants Active Directory afin qu'il puisse analyser les volumes CIFS.
  - a. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.
  - b. Pour chaque environnement de travail, cliquez sur **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe dont Data Sense a besoin pour accéder aux volumes CIFS sur le système.

Les informations d'identification peuvent être en lecture seule, mais fournir des informations d'identification admin garantit que Data Sense peut lire toutes les données qui requièrent des autorisations élevées. Les identifiants sont stockés sur l'instance Cloud Data Sense.

Si vous voulez vous assurer que vos fichiers “dernières heures d'accès” sont inchangés par les analyses de classification de détection de données, nous recommandons à l'utilisateur de disposer de l'autorisation Write Attributes. Si possible, nous vous recommandons de faire en sorte que l'utilisateur configuré Active Directory fasse partie d'un groupe parent de l'organisation qui dispose des autorisations pour tous les fichiers.

Une fois les informations d'identification saisies, un message indiquant que tous les volumes CIFS ont été authentifiés avec succès s'affiche.

## Activation et désactivation des analyses de conformité sur les volumes

Vous pouvez démarrer ou arrêter des analyses de mappage uniquement, ou des analyses de mappage et de

classification, dans un environnement de travail à tout moment à partir de la page Configuration. Vous pouvez également passer des acquisitions avec mappage uniquement à des acquisitions avec mappage et classification, et inversement. Nous vous recommandons de scanner tous les volumes.

cognigoWE Scan Configuration

44/79 Volumes selected for Data Sense scan

OffMapMap & ClassifyCustom

Learn about the differences →

Edit CIFS Credentials

Scan	Storage Repository (Volume)	Type	Status	Required Action
<div>OffMapMap &amp; Classify</div>	AdiNFSVol_copy	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<div>OffMapMap &amp; Classify</div>	AdiProtest2501	NFS	Continuously Scanning	
<div>OffMapMap &amp; Classify</div>	AlexTest	NFS	No Access	Access to the NFS volume was denied. Make sure tha...
<div>OffMapMap &amp; Classify</div>	AlexTestSecond	NFS	Not Scanning	
<div>OffMapMap &amp; Classify</div>	MoreDataNeed1000	NFS	Continuously Scanning	

À :	Procédez comme suit :
Activez les acquisitions avec mappage uniquement sur un volume	Dans la zone du volume, cliquez sur <b>Map</b>
Activer la numérisation complète sur un volume	Dans la zone de volume, cliquez sur <b>carte et classement</b>
Désactiver la numérisation sur un volume	Dans la zone du volume, cliquez sur <b>Off</b>
Activez les analyses de mappage uniquement sur tous les volumes	Dans la zone d'en-tête, cliquez sur <b>carte</b>
Activez l'analyse complète sur tous les volumes	Dans la zone d'en-tête, cliquez sur <b>carte et classement</b>
Désactiver l'analyse de tous les volumes	Dans la zone d'en-tête, cliquez sur <b>Off</b>



Les nouveaux volumes ajoutés à l'environnement de travail sont automatiquement analysés uniquement lorsque vous avez défini le paramètre **Map** ou **Map & Classify** dans la zone d'en-tête. Lorsque vous sélectionnez **personnalisé** ou **Désactivé** dans la zone de titre, vous devez activer le mappage et/ou la numérisation complète sur chaque nouveau volume que vous ajoutez à l'environnement de travail.

Analyse des volumes de protection des données

Par défaut, les volumes DP ne sont pas analysés parce qu'ils ne sont pas exposés en externe et que Cloud Data SENSE ne peut pas y accéder. Il s'agit des volumes de destination pour les opérations SnapMirror à partir d'un système de fichiers FSX pour ONTAP.

Initialement, la liste de volumes identifie ces volumes comme *Type DP* avec *Status Not Scanning* et la *Requited action Enable Access to DP volumes*.



**'Working Environment Name' Configuration**

22/28 Volumes selected for compliance scan

**Enable Access to DP Volumes** [Edit CIFS Credentials](#)

Off **Map** Map & Classify Custom [Learn about the differences](#) →

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off <b>Map</b> Map & Classify	VolumeName1	DP	Not Scanning	Enable access to DP Volumes ⓘ
Off <b>Map</b> Map & Classify	VolumeName2	NFS	Continuously Scanning	
Off <b>Map</b> Map & Classify	VolumeName3	CIFS	Not Scanning	

## Étapes

Pour analyser ces volumes de protection des données :

1. Cliquez sur **Activer l'accès aux volumes DP** en haut de la page.
2. Vérifiez le message de confirmation et cliquez à nouveau sur **Activer l'accès aux volumes DP**.
  - Les volumes initialement créés en tant que volumes NFS dans le système de fichiers FSX source pour ONTAP sont activés.
  - Les volumes initialement créés en tant que volumes CIFS dans le système de fichiers FSX source pour ONTAP nécessitent que vous saisiez des informations d'identification CIFS pour scanner ces volumes DP. Si vous avez déjà saisi les informations d'identification Active Directory afin que Cloud Data SENSE puisse analyser des volumes CIFS, vous pouvez utiliser ces informations d'identification ou spécifier un autre ensemble d'informations d'identification Admin.

**Provide Active Directory Credentials**

☒ Use existing CIFS Scanning Credentials (user1@domain2) ☐ Use Custom Credentials

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

**Enable Access to DP Volumes** Cancel

**Provide Active Directory Credentials**

☐ Use existing CIFS Scanning Credentials (user1@domain2) ☒ Use Custom Credentials

Username ⓘ Password ⓘ

Active Directory Domain ⓘ DNS IP Address ⓘ

DP Volumes, created from a SnapMirror relationship, do not allow external access by default. Continuing will create NFS shares from DP Volumes which have been activated for Data Sense. The shares' export policies will allow access only from the Cloud Data Sense instance. [Learn More](#)

**Enable Access to DP Volumes** Cancel

3. Activez chaque volume DP que vous souhaitez analyser [de la même façon que vous avez activé d'autres volumes](#).

## Résultat

Une fois activée, Cloud Data Sense crée un partage NFS à partir de chaque volume DP activé pour l'analyse. Les règles d'exportation de partage autorisent uniquement l'accès à partir de l'instance de détection de données.

**Remarque :** si vous ne aviez pas de volumes de protection des données CIFS lorsque vous avez activé l'accès initial aux volumes DP, puis en ajoutant d'autres, le bouton **Activer l'accès à CIFS DP** s'affiche en haut de la page Configuration. Cliquez sur ce bouton et ajoutez des identifiants CIFS pour permettre l'accès à ces volumes CIFS DP.



Les identifiants Active Directory sont uniquement enregistrés dans la machine virtuelle de stockage du premier volume CIFS DP, de sorte que tous les volumes DP de ce SVM soient analysés. Les volumes résidant sur d'autres SVM ne seront pas enregistrés pour les identifiants Active Directory, de sorte que ces volumes DP ne seront pas analysés.

## Mise en route de Cloud Data Sense pour Amazon S3

Cloud Data Sense peut analyser vos compartiments Amazon S3 pour identifier les données personnelles et sensibles qui résident dans le stockage objet S3. Cloud Data Sense peut scanner n'importe quel compartiment du compte, indépendamment de sa création pour une solution NetApp.

### Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

#### Configurez les exigences S3 dans votre environnement cloud

Assurez-vous que votre environnement cloud répond aux exigences du Cloud Data SENSE, notamment la préparation d'un rôle IAM et la configuration de la connectivité depuis Data Sense vers S3. [Voir la liste complète.](#)

2

#### Déployez l'instance Cloud Data SENSE

"[Déployez des données adaptées au cloud](#)" si aucune instance n'est déjà déployée.

3

#### Activation de Data Sense dans votre environnement de travail S3

Sélectionnez l'environnement de travail Amazon S3, cliquez sur **Activer** et sélectionnez un rôle IAM qui inclut les autorisations requises.

4

#### Sélectionnez les compartiments à numériser

Sélectionnez les compartiments que vous souhaitez analyser et Cloud Data SENSE commence à les analyser.

### Vérification des prérequis S3

Les exigences suivantes sont spécifiques à l'analyse des compartiments S3.

#### Configurez un rôle IAM pour l'instance Cloud Data Sense

Cloud Data SENSE a besoin d'autorisations pour se connecter aux compartiments S3 de votre compte et pour les analyser. Configurez un rôle IAM qui inclut les autorisations répertoriées ci-dessous. BlueXP vous invite à sélectionner un rôle IAM lorsque vous activez Data Sense dans l'environnement de travail Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

### Connectivité entre le maillage Cloud Data Sense et Amazon S3

Cloud Data SENSE a besoin d'une connexion à Amazon S3. Pour assurer cette connexion, le meilleur moyen consiste à utiliser un terminal VPC pour le service S3. Pour obtenir des instructions, reportez-vous à la section ["Documentation AWS : création d'un terminal de passerelle"](#).

Lorsque vous créez le point de terminaison VPC, veillez à sélectionner la région, le VPC et la table de routage correspondant à l'instance Cloud Data Sense. Vous devez également modifier le groupe de sécurité pour ajouter une règle HTTPS sortante qui active le trafic vers le terminal S3. Dans le cas contraire, Data Sense ne peut pas se connecter au service S3.

Si vous rencontrez des problèmes, reportez-vous à la section ["Centre de connaissances du support AWS : pourquoi ne puis-je pas me connecter à un compartiment S3 à l'aide d'un terminal VPC de passerelle ?"](#)

Une alternative consiste à fournir la connexion à l'aide d'une passerelle NAT.



Vous ne pouvez pas utiliser de proxy pour accéder à S3 sur Internet.

### Déploiement de l'instance Cloud Data Sense

["Déployez Cloud Data Sense dans BlueXP"](#) si aucune instance n'est déjà déployée.

Vous devez déployer l'instance à l'aide d'un connecteur déployé dans AWS. BlueXP détecte automatiquement les compartiments S3 dans ce compte AWS et les affiche dans un environnement de travail Amazon S3.

**Remarque :** le déploiement de Cloud Data SENSE dans un emplacement sur site n'est pas pris en charge actuellement lors de l'analyse des compartiments S3.

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

### Activation de Data Sense dans votre environnement de travail S3

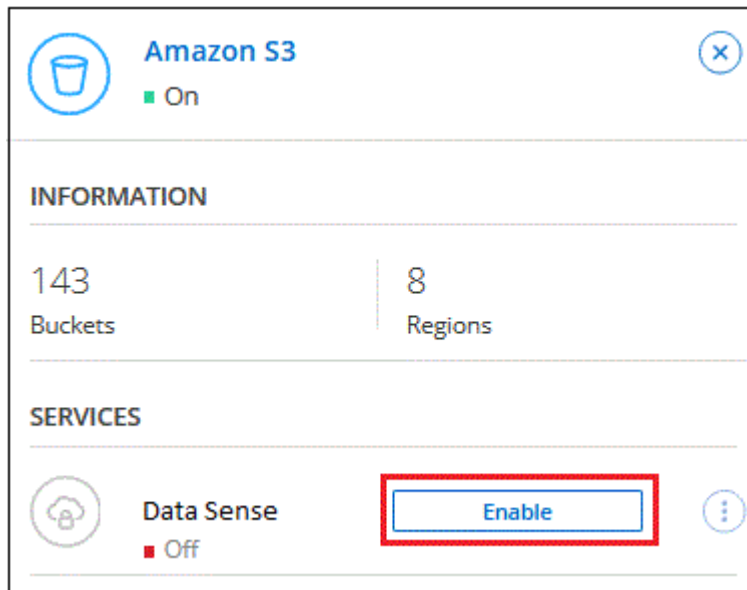
Activez Cloud Data SENSE sur Amazon S3 après avoir vérifié les prérequis.

#### Étapes

1. Dans le menu de navigation de gauche de BlueXP, cliquez sur **stockage > Canvas**.
2. Sélectionnez l'environnement de travail Amazon S3.



3. Dans le volet de détection de données situé à droite, cliquez sur **Activer**.



4. Attribuez un rôle IAM à l'instance Cloud Data SENSE qui dispose de [les autorisations requises](#).

### Assign an AWS IAM Role for Cloud Data Sense

To enable **Cloud Data Sense** on Amazon S3 buckets, select an existing IAM Role. Make sure that your AWS IAM Role has the permission defined in the [Policy Requirements](#).

Select IAM Role

occm

**VPC Endpoint for Amazon S3 Required**

A VPC endpoint to the Amazon S3 service is required so **Data Sense** can securely scan the data.

Alternatively, ensure that the **Data Sense** instance has direct access to the internet via a NAT Gateway or Internet Gateway.

**Free for the 1st TB**

Over 1 TB you pay only for what you use. [Learn more about pricing.](#)

**Enable**

Cancel

5. Cliquez sur **Activer**.



Vous pouvez également activer les analyses de conformité pour un environnement de travail à partir de la page Configuration en cliquant sur Et en sélectionnant **Activer détection de données**.

## Résultat

BlueXP affecte le rôle IAM à l'instance.

## Activation et désactivation des analyses de conformité dans les compartiments S3

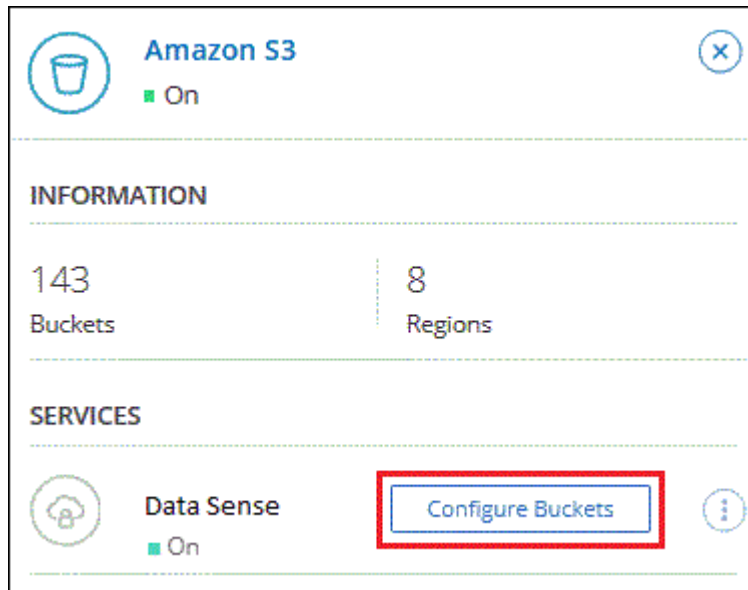
Une fois que BlueXP a activé Cloud Data Sense sur Amazon S3, l'étape suivante consiste à configurer les compartiments que vous souhaitez numériser.

Lorsque BlueXP est exécuté dans le compte AWS doté des compartiments S3 que vous souhaitez analyser, il détecte ces compartiments et les affiche dans un environnement de travail Amazon S3.

Cloud Data Sense peut également être [Analysez les compartiments S3 qui se trouvent dans différents comptes AWS](#).

## Étapes

1. Sélectionnez l'environnement de travail Amazon S3.
2. Dans le volet de droite, cliquez sur **configurer les rubriques**.



3. Activez les analyses de mappage uniquement ou les analyses de mappage et de classification sur vos compartiments.

Amazon S3 Configuration			
15/28 Buckets in Scan Scope.			
Scan	Bucket Name	Status	Required Action
Off Map <b>Map &amp; Classify</b>	BucketName1	● Not Scanning	Add Credentials
Off <b>Map</b> Map & Classify	BucketName2	● Continuously Scanning	
<b>Off</b> Map Map & Classify	BucketName3	● Not Scanning	

À :	Procédez comme suit :
Activez les acquisitions avec mappage uniquement sur un compartiment	Cliquez sur <b>carte</b>
Activer les acquisitions complètes sur un compartiment	Cliquez sur <b>carte et classement</b>
Désactiver l'acquisition sur un godet	Cliquez sur <b>Off</b>

## Résultat

Cloud Data Sense commence l'analyse des compartiments S3 que vous avez activés. En cas d'erreur, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

## Analyse des compartiments à partir de comptes AWS supplémentaires

Pour scanner les compartiments S3 qui se trouvent dans un autre compte AWS, vous devez attribuer un rôle à partir de ce compte pour accéder à l'instance Cloud Data Sense existante.

## Étapes

1. Accédez au compte AWS cible où vous voulez analyser les compartiments S3 et créer un rôle IAM en







sélectionnant **un autre compte AWS**.

## Create role




### Select type of trusted entity

 <b>AWS service</b> EC2, Lambda and others	 <b>Another AWS account</b> Belonging to you or 3rd party	 <b>Web identity</b> Cognito or any OpenID provider	 <b>SAML 2.0 federation</b> Your corporate directory
--	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

### Specify accounts that can use this role

Account ID\*

- Options
- ☐ Require external ID (Best practice when a third party will assume this role)
  - ☐ Require MFA 

Assurez-vous de faire ce qui suit :

- Entrez l'ID du compte sur lequel réside l'instance Cloud Data SENSE.
- Modifiez la durée \* maximale de la session CLI/API\* de 1 heure à 12 heures et enregistrez cette modification.
- Joignez la politique IAM de détection des données cloud. Assurez-vous qu'il dispose des autorisations requises.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

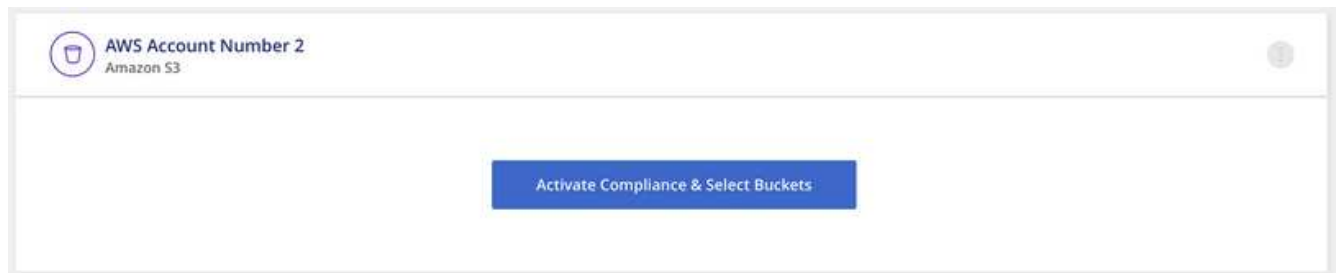
2. Accédez au compte AWS source sur lequel réside l'instance Data Sense et sélectionnez le rôle IAM associé à l'instance.
  - a. Modifiez la durée \* maximale de la session CLI/API\* de 1 heure à 12 heures et enregistrez cette modification.
  - b. Cliquez sur **attacher des stratégies**, puis sur **Créer une stratégie**.

- c. Créez une stratégie qui inclut l'action « sts:AssumeRole » et spécifiez l'ARN du rôle que vous avez créé dans le compte cible.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-ID>:role/<ADDITIONAL_ROLE_NAME>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:policy/*",
        "arn:aws:iam::*:role/*"
      ]
    }
  ]
}
```

Le compte d'instance Cloud Data SENSE a désormais accès au compte AWS supplémentaire.

3. Accédez à la page **Amazon S3 Configuration** et le nouveau compte AWS s'affiche. Notez que la synchronisation de l'environnement de travail du nouveau compte peut prendre quelques minutes avec Cloud Data Sense.



4. Cliquez sur **Activer la détection des données et sélectionnez les rubriques** et sélectionnez les rubriques que vous souhaitez numériser.

## Résultat

Cloud Data Sense commence l'analyse des nouveaux compartiments S3 que vous avez activés.



## Analyse des schémas de base de données

Suivez quelques étapes pour commencer à scanner vos schémas de base de données à l'aide de Cloud Data Sense.

### Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

#### Vérifiez les prérequis de la base de données

Assurez-vous que votre base de données est prise en charge et que vous disposez des informations nécessaires pour vous connecter à la base de données.

2

#### Déployez l'instance Cloud Data SENSE

"[Déployez des données adaptées au cloud](#)" si aucune instance n'est déjà déployée.

3

#### Ajoutez le serveur de base de données

Ajoutez le serveur de base de données auquel vous souhaitez accéder.

4

#### Sélectionnez les schémas

Sélectionnez les schémas à numériser.

### Vérification des prérequis

Avant d'activer le Cloud Data sens, lisez les conditions préalables suivantes pour vérifier que la configuration est prise en charge.

#### Bases de données prises en charge

Cloud Data SENSE peut scanner des schémas à partir des bases de données suivantes :

- Amazon Relational Database Service (Amazon RDS)
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- SAP HANA
- Serveur SQL (MSSQL)



La fonction de collecte de statistiques **doit être activée** dans la base de données.

## Configuration requise pour les bases de données

Toutes les bases de données connectée à l'instance Cloud Data SENSE peuvent être analysées, quel que soit l'endroit où elles sont hébergées. Pour vous connecter à la base de données, il vous suffit de disposer des informations suivantes :

- Adresse IP ou nom d'hôte
- Port
- Nom du service (uniquement pour l'accès aux bases de données Oracle)
- Références permettant l'accès en lecture aux schémas

Lorsque vous choisissez un nom d'utilisateur et un mot de passe, il est important de choisir un nom qui dispose des autorisations de lecture complètes pour tous les schémas et tables que vous souhaitez numériser. Nous vous recommandons de créer un utilisateur dédié pour le système Cloud Data SENSE avec toutes les autorisations requises.

**Remarque :** pour MongoDB, un rôle d'administrateur en lecture seule est requis.

## Déploiement de l'instance Cloud Data Sense

Déployez Cloud Data si aucune instance n'est déjà déployée.

Si vous numérisez des schémas de base de données accessibles via Internet, vous pouvez "[Déployez les données du cloud dans le cloud](#)" ou "[Déployer Data Sense dans un emplacement sur site avec accès Internet](#)".

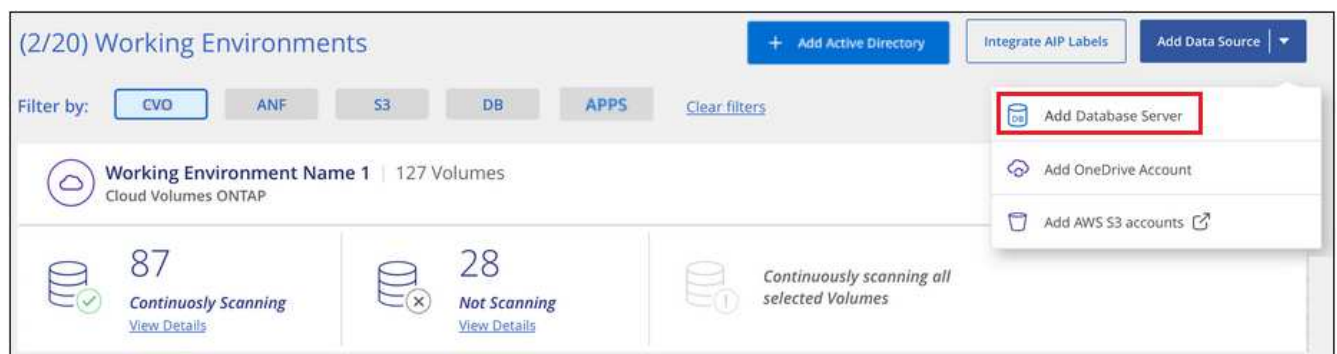
Si vous numérisez des schémas de base de données qui ont été installés sur un site sombre sans accès à Internet, vous devez le faire "[Déployez les données cloud sur site qui ne disposent pas d'un accès Internet](#)". Cela nécessite également que le connecteur BlueXP soit déployé dans le même emplacement sur site.

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

## Ajout du serveur de base de données

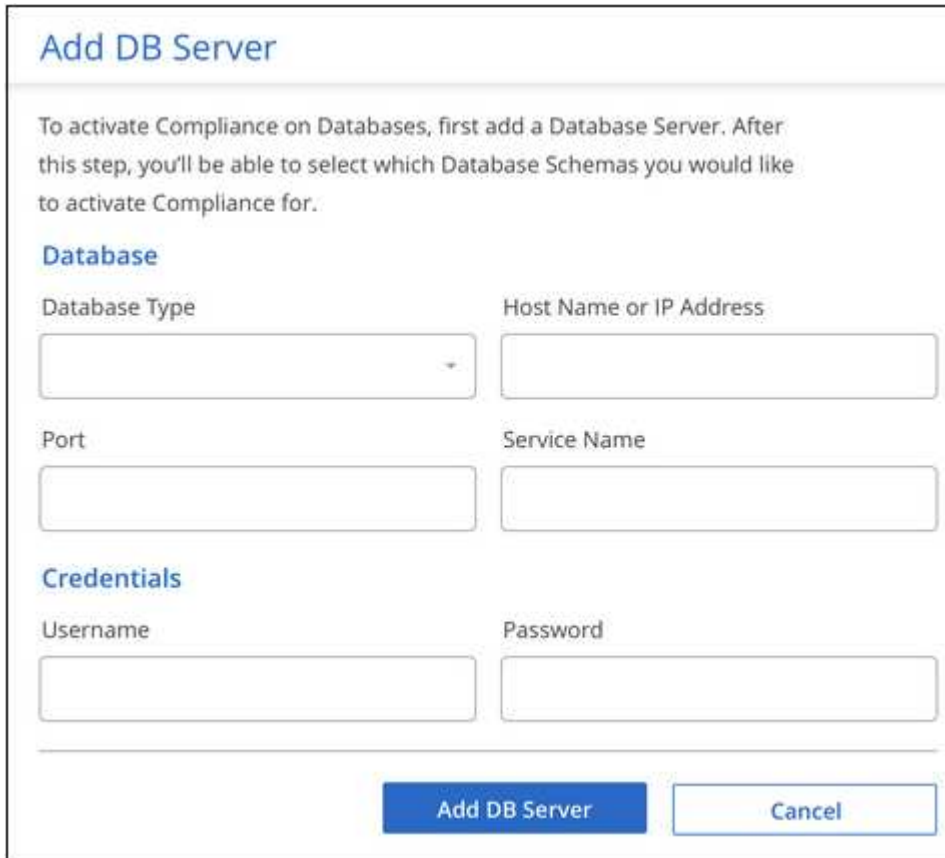
Ajoutez le serveur de base de données où se trouvent les schémas.

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données** > **Ajouter un serveur de base de données**.



2. Entrez les informations requises pour identifier le serveur de base de données.
  - a. Sélectionnez le type de base de données.

- b. Entrez le port et le nom d'hôte ou l'adresse IP pour vous connecter à la base de données.
- c. Pour les bases de données Oracle, entrez le nom du service.
- d. Entrez les identifiants afin que Cloud Data SENSE puisse accéder au serveur.
- e. Cliquez sur **Ajouter serveur DB**.



**Add DB Server**

To activate Compliance on Databases, first add a Database Server. After this step, you'll be able to select which Database Schemas you would like to activate Compliance for.

**Database**

Database Type:

Host Name or IP Address:

Port:

Service Name:

**Credentials**

Username:

Password:

**Add DB Server** **Cancel**

La base de données est ajoutée à la liste des environnements de travail.

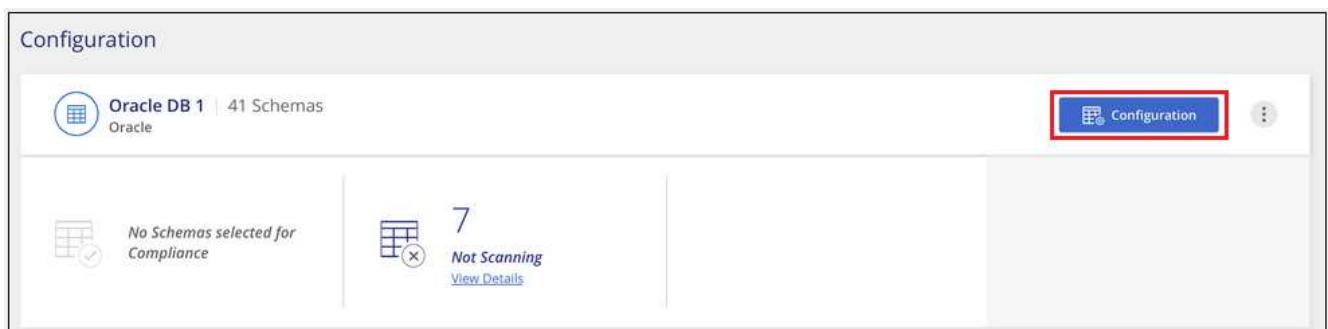
### Activation et désactivation des analyses de conformité sur les schémas de base de données

Vous pouvez arrêter ou démarrer la numérisation complète de vos schémas à tout moment.




Il n'existe pas d'option permettant de sélectionner des analyses de mappage uniquement pour les schémas de base de données.

1. Dans la page *Configuration*, cliquez sur le bouton **Configuration** de la base de données à configurer.



2. Sélectionnez les schémas à numériser en déplaçant le curseur vers la droite.

'Working Environment Name' Configuration			
28/28 Schemas selected for compliance scan		 <a href="#">Edit Credentials</a>	
Scan	Schema Name	Status	Required Action
<input checked="" type="checkbox"/>	DB1 - SchemaName1	<span>Not Scanning</span>	<a href="#">Add Credentials</a> ⓘ
<input checked="" type="checkbox"/>	DB1 - SchemaName2	<span>Continuously Scanning</span>	
<input checked="" type="checkbox"/>	DB1 - SchemaName3	<span>Continuously Scanning</span>	
<input checked="" type="checkbox"/>	DB1 - SchemaName4	<span>Continuously Scanning</span>	

## Résultat

Cloud Data SENSE commence à analyser les schémas de base de données que vous avez activés. S'il y a des erreurs, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

## En analysant les comptes OneDrive

Procédez comme suit pour lancer la numérisation des fichiers dans les dossiers OneDrive de votre utilisateur avec Cloud Data Sense.

### Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

#### Vérifiez les prérequis OneDrive

Assurez-vous que vous disposez des informations d'identification Admin pour vous connecter au compte OneDrive.

2

#### Déployez l'instance Cloud Data SENSE

"[Déployez des données adaptées au cloud](#)" si aucune instance n'est déjà déployée.

3

#### Ajoutez le compte OneDrive

À l'aide des informations d'identification utilisateur Admin, connectez-vous au compte OneDrive auquel vous souhaitez accéder afin qu'il soit ajouté en tant que nouvel environnement de travail.

4

#### Ajoutez les utilisateurs et sélectionnez le type de numérisation

Ajoutez la liste des utilisateurs du compte OneDrive que vous souhaitez numériser et sélectionnez le type de numérisation. Vous pouvez ajouter jusqu'à 100 utilisateurs à la fois.

## Vérification des exigences OneDrive

Avant d'activer le Cloud Data sens, lisez les conditions préalables suivantes pour vérifier que la configuration est prise en charge.

- Vous devez disposer des informations d'identification d'administrateur pour le compte OneDrive entreprise qui permet d'accéder en lecture aux fichiers de l'utilisateur.
- Vous aurez besoin d'une liste séparée en ligne des adresses e-mail pour tous les utilisateurs dont vous souhaitez numériser les dossiers OneDrive.

## Déploiement de l'instance Cloud Data Sense

Déployez Cloud Data si aucune instance n'est déjà déployée.

Il peut y avoir un sens des données "déploiement dans le cloud" ou "dans un emplacement sur site avec accès à internet".

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

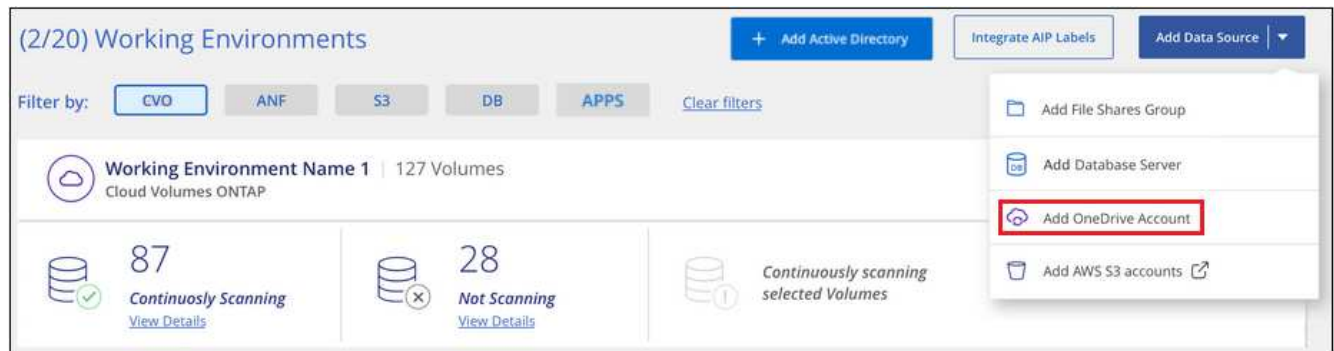
Il est également possible de détecter des données "déploiement dans un emplacement sur site qui ne dispose pas d'un accès internet". Cependant, vous devez fournir un accès Internet à quelques points de terminaison sélectionnés pour analyser vos fichiers OneDrive locaux. "Voir la liste des points finaux requis ici".

## Ajout du compte OneDrive

Ajoutez le compte OneDrive où résident les fichiers utilisateur.

### Étapes

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données > Ajouter un compte OneDrive**.



2. Dans la boîte de dialogue Ajouter un compte OneDrive, cliquez sur **connexion à OneDrive**.
3. Dans la page Microsoft qui s'affiche, sélectionnez le compte OneDrive et entrez l'utilisateur et le mot de passe d'administration requis, puis cliquez sur **Accept** pour permettre à Cloud Data SENSE de lire les données de ce compte.

Le compte OneDrive est ajouté à la liste des environnements de travail.

## Ajout d'utilisateurs OneDrive aux analyses de conformité

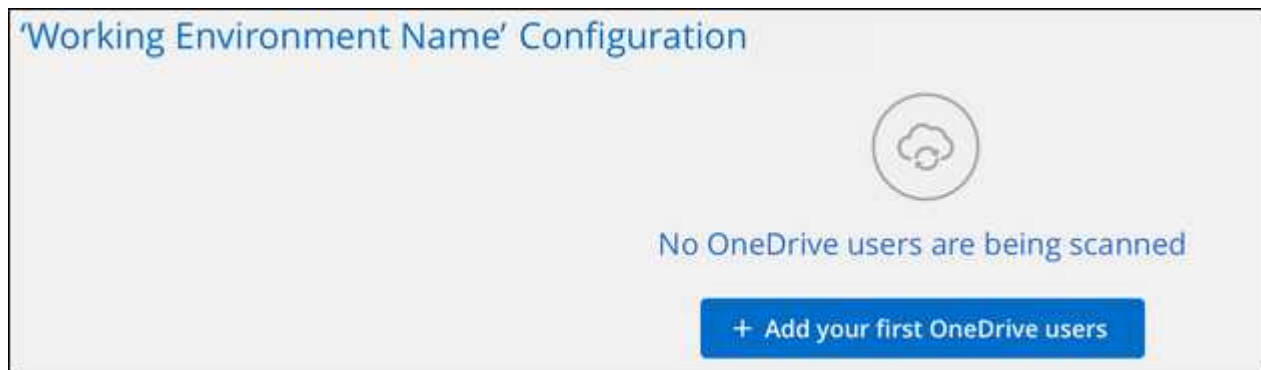
Vous pouvez ajouter des utilisateurs OneDrive individuels ou tous vos utilisateurs OneDrive, de sorte que leurs fichiers soient analysés par Cloud Data Sense.

## Étapes

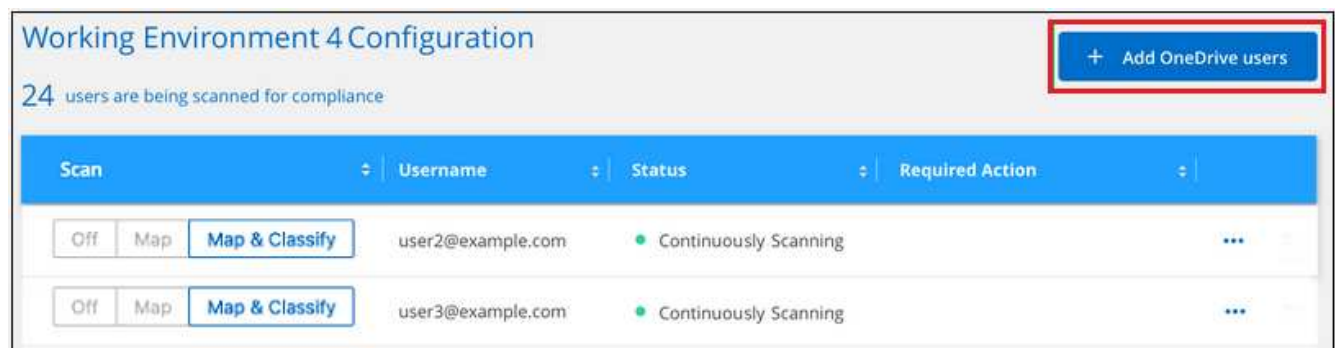
1. Dans la page *Configuration*, cliquez sur le bouton **Configuration** du compte OneDrive.



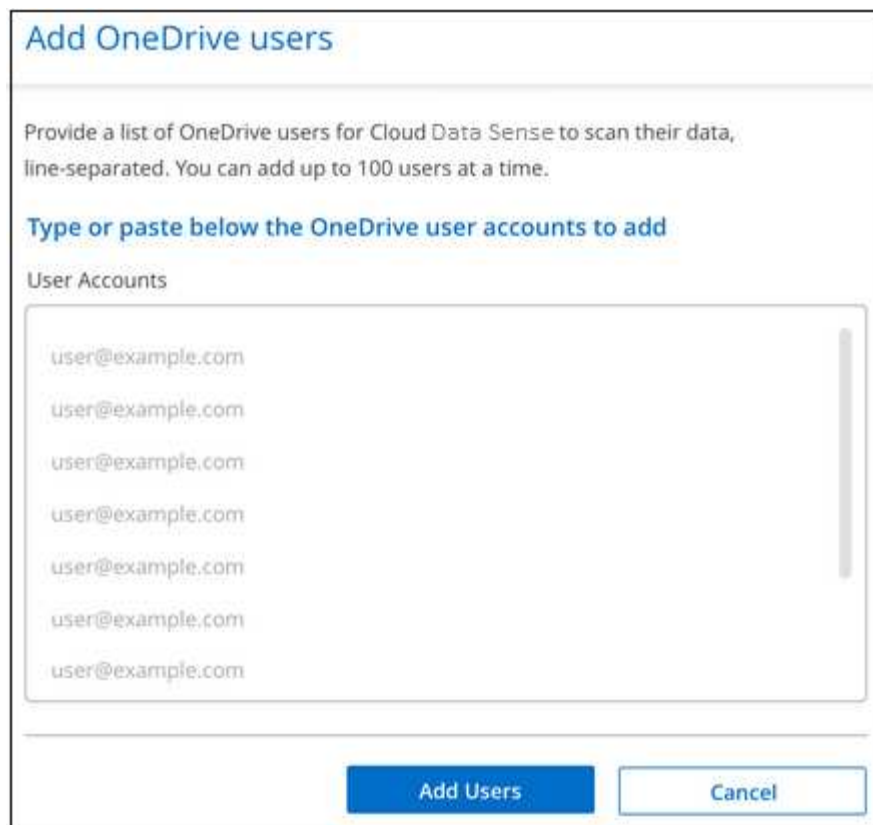
2. S'il s'agit de la première fois que vous ajoutez des utilisateurs pour ce compte OneDrive, cliquez sur **Ajouter vos premiers utilisateurs OneDrive**.



Si vous ajoutez des utilisateurs supplémentaires à partir d'un compte OneDrive, cliquez sur **Ajouter des utilisateurs OneDrive**.



3. Ajoutez les adresses e-mail des utilisateurs dont vous souhaitez numériser les fichiers - une adresse e-mail par ligne (jusqu'à 100 par session) - et cliquez sur **Ajouter utilisateurs**.



**Add OneDrive users**

Provide a list of OneDrive users for Cloud Data Sense to scan their data, line-separated. You can add up to 100 users at a time.

Type or paste below the OneDrive user accounts to add

User Accounts

user@example.com  
user@example.com  
user@example.com  
user@example.com  
user@example.com  
user@example.com  
user@example.com

Add Users Cancel

Une boîte de dialogue de confirmation affiche le nombre d'utilisateurs ajoutés.

Si la boîte de dialogue répertorie tous les utilisateurs qui n'ont pas pu être ajoutés, capturez ces informations pour résoudre le problème. Dans certains cas, vous pouvez ajouter à nouveau l'utilisateur avec une adresse e-mail corrigée.

4. Activez les analyses de mappage uniquement, ou les analyses de mappage et de classification, sur les fichiers utilisateur.

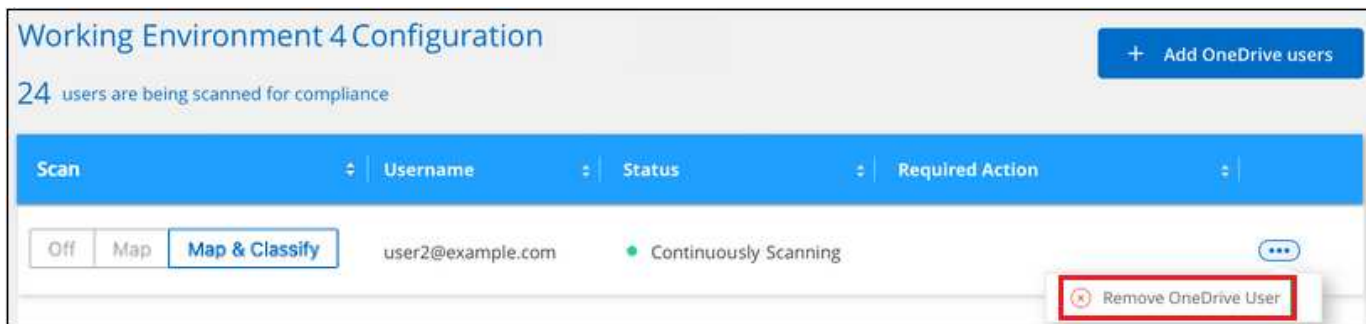
À :	Procédez comme suit :
Activer les analyses de mappage uniquement sur les fichiers utilisateur	Cliquez sur <b>carte</b>
Activer les analyses complètes sur les fichiers utilisateur	Cliquez sur <b>carte et classement</b>
Désactiver la numérisation sur les fichiers utilisateur	Cliquez sur <b>Off</b>

## Résultat

Cloud Data SENSE commence à analyser les fichiers pour les utilisateurs que vous avez ajoutés, et les résultats sont affichés dans le tableau de bord et à d'autres emplacements.

## Suppression d'un utilisateur OneDrive des analyses de conformité

Si des utilisateurs quittent l'entreprise ou si leur adresse e-mail change, vous pouvez supprimer à tout moment les utilisateurs OneDrive de faire analyser leurs fichiers. Il vous suffit de cliquer sur **Supprimer l'utilisateur OneDrive** dans la page de configuration.



Notez que vous pouvez "[Supprimez l'ensemble du compte OneDrive de Data Sense](#)" Si vous ne souhaitez plus numériser de données utilisateur à partir du compte OneDrive.

## Analyse des comptes SharePoint

Suivez quelques étapes pour commencer à analyser les fichiers de vos comptes sur site SharePoint Online et SharePoint avec Cloud Data Sense.

### Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

#### Consultez les prérequis pour SharePoint

Assurez-vous que vous disposez des informations d'identification Admin pour vous connecter au compte SharePoint et que vous disposez des URL des sites SharePoint que vous souhaitez analyser.

2

#### Déployez l'instance Cloud Data SENSE

"[Déployez des données adaptées au cloud](#)" si aucune instance n'est déjà déployée.

3

#### Connectez-vous au compte SharePoint

À l'aide des informations d'identification utilisateur Admin, connectez-vous au compte SharePoint auquel vous souhaitez accéder afin qu'il soit ajouté en tant que nouvelle source de données/environnement de travail.

4

#### Ajoutez les URL du site SharePoint à analyser

Ajoutez la liste des URL du site SharePoint que vous souhaitez analyser dans le compte SharePoint et sélectionnez le type de numérisation. Vous pouvez ajouter jusqu'à 100 URL à la fois.

### Révision des exigences SharePoint

Lisez les conditions préalables suivantes pour vous assurer que vous êtes prêt à activer Cloud Data SENSE sur un compte SharePoint.

- Vous devez disposer des informations d'identification d'administrateur pour le compte SharePoint qui fournissent un accès en lecture à tous les sites SharePoint.



- Pour les solutions SharePoint sur site, vous aurez également besoin de l'URL de SharePoint Server.
- Vous aurez besoin d'une liste séparée en plusieurs lignes des URL du site SharePoint pour toutes les données que vous souhaitez analyser.

## Déploiement de l'instance Cloud Data Sense

Déployez Cloud Data si aucune instance n'est déjà déployée.

- Pour SharePoint Online, il est possible de détecter les données "déploiement dans le cloud" ou "installé dans un emplacement sur site avec accès à internet".

Il est également possible de détecter des données "déploiement dans un emplacement sur site qui ne dispose pas d'un accès internet". Cependant, vous devrez fournir un accès Internet à quelques points de terminaison sélectionnés pour analyser vos fichiers SharePoint Online. "Voir la liste des points finaux requis ici".

- Dans le cas d'une solution SharePoint sur site, Data Sense peut être installé "dans un emplacement sur site avec accès à internet" ou "dans un emplacement sur site qui ne dispose pas d'un accès internet".

Lorsque Data SENSE est installé sur un site sans accès à Internet, le connecteur BlueXP doit également être installé sur ce même site sans accès à Internet. "En savoir plus >>".

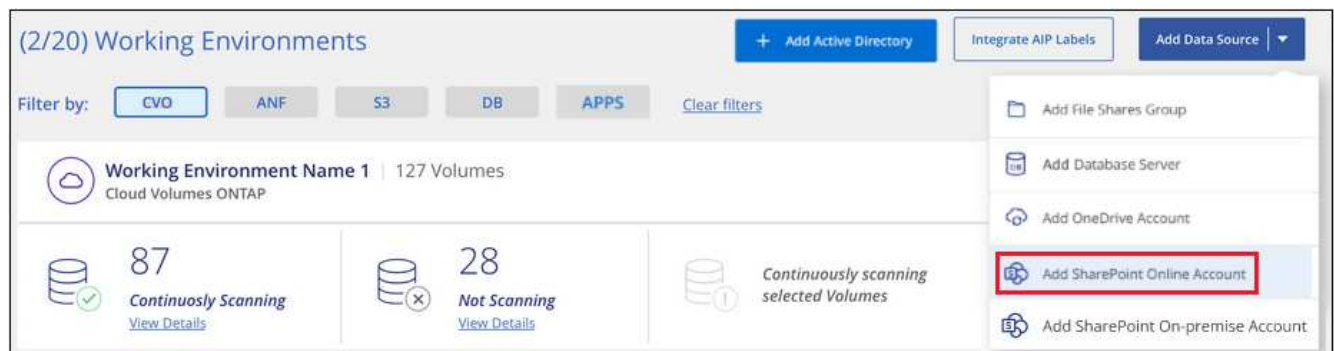
Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

## Ajout d'un compte SharePoint Online

Ajoutez le compte SharePoint Online où se trouvent les fichiers utilisateur.

### Étapes

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données >** **Ajouter un compte SharePoint en ligne**.



2. Dans la boîte de dialogue Ajouter un compte SharePoint en ligne, cliquez sur **se connecter à SharePoint**.
3. Dans la page Microsoft qui s'affiche, sélectionnez le compte SharePoint et entrez l'utilisateur et le mot de passe d'administration requis, puis cliquez sur **Accept** pour permettre à Cloud Data SENSE de lire les données de ce compte.

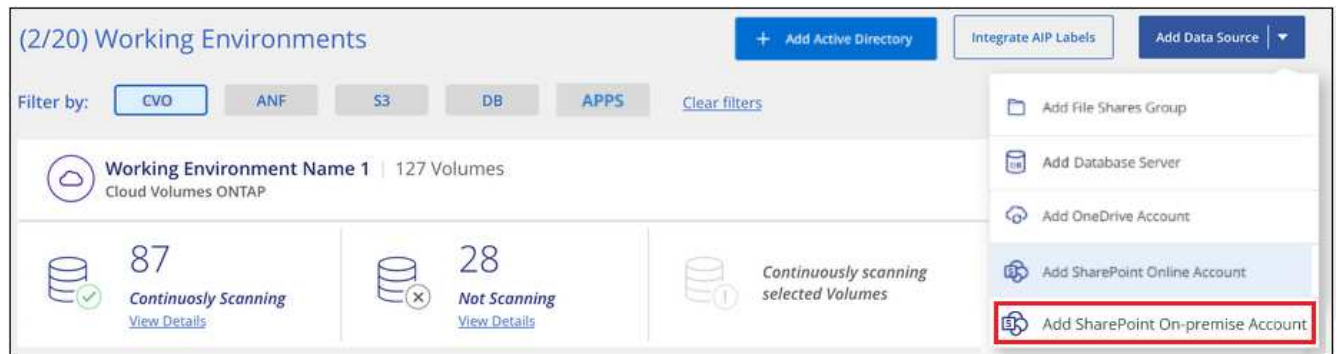
Le compte SharePoint Online est ajouté à la liste des environnements de travail.

## Ajout d'un compte SharePoint sur site

Ajoutez le compte SharePoint sur site où résident les fichiers utilisateur.

## Étapes

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données** > **Ajouter un compte SharePoint sur site**.



2. Dans la boîte de dialogue se connecter à SharePoint On-Premise Server, entrez les informations suivantes :
  - Admin user au format « domain/user » ou « user@domain », et le mot de passe admin
  - URL du serveur SharePoint

3. Cliquez sur **connexion**.

Le compte sur site SharePoint est ajouté à la liste des environnements de travail.

## Ajout de sites SharePoint aux analyses de conformité

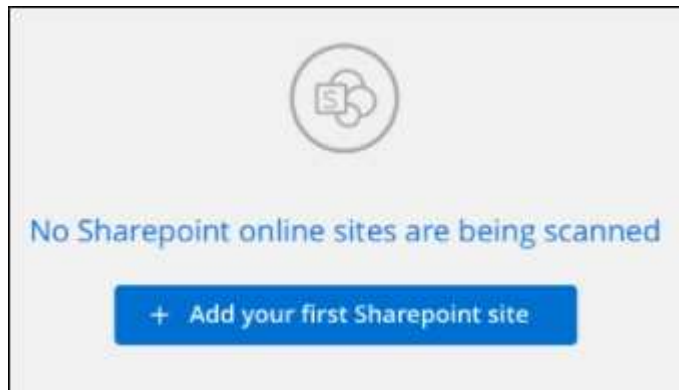
Vous pouvez ajouter des sites SharePoint individuels ou tous les sites SharePoint du compte, de sorte que les fichiers associés soient analysés par Cloud Data Sense. Les étapes sont identiques lors de l'ajout de sites SharePoint Online ou SharePoint sur site.

## Étapes

1. Dans la page *Configuration*, cliquez sur le bouton **Configuration** du compte SharePoint.



2. Si c'est la première fois que vous ajoutez des sites pour ce compte SharePoint, cliquez sur **Ajouter votre premier site SharePoint**.



Si vous ajoutez des utilisateurs supplémentaires à partir d'un compte SharePoint, cliquez sur **Ajouter des sites SharePoint**.



3. Ajoutez les URL des sites dont vous voulez numériser les fichiers - une URL par ligne (jusqu'à 100 maximum par session) - et cliquez sur **Ajouter des sites**.

Une boîte de dialogue de confirmation affiche le nombre de sites ajoutés.

Si la boîte de dialogue répertorie des sites qui n'ont pas pu être ajoutés, capturez ces informations pour résoudre le problème. Dans certains cas, vous pouvez ajouter à nouveau le site avec une URL corrigée.

4. Activez les analyses de mappage uniquement, ou les analyses de mappage et de classification, sur les fichiers des sites SharePoint.

À :	Procédez comme suit :
Activer les analyses de mappage uniquement sur les fichiers	Cliquez sur <b>carte</b>
Activez les analyses complètes sur les fichiers	Cliquez sur <b>carte et classement</b>
Désactiver la numérisation sur les fichiers	Cliquez sur <b>Off</b>

## Résultat

Cloud Data SENSE commence à analyser les fichiers des sites SharePoint que vous avez ajoutés, et les résultats sont affichés dans le tableau de bord et à d'autres emplacements.

## Suppression d'un site SharePoint des analyses de conformité

Si vous supprimez un site SharePoint à l'avenir ou décidez de ne pas analyser les fichiers d'un site SharePoint, vous pouvez supprimer chaque site SharePoint de la façon dont ses fichiers sont analysés à tout moment. Il vous suffit de cliquer sur **Supprimer le site SharePoint** dans la page Configuration.

Scan	Site URL	Status	Required Action
Off Map <b>Map &amp; Classify</b>	Site URL	Continuously Scanning	...
Off Map <b>Map &amp; Classify</b>	Site URL	Continuously Scanning	<b>Remove SharePoint Site</b>

Notez que vous pouvez "[Supprimez tout le compte SharePoint de Data Sense](#)" Si vous ne souhaitez plus analyser les données utilisateur du compte SharePoint.

## Numérisation de comptes Google Drive

Procédez comme suit pour lancer la numérisation des fichiers utilisateur dans vos comptes Google Drive avec Cloud Data Sense.

### Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

#### Consultez les conditions préalables à Google Drive

Assurez-vous que vous disposez des informations d'identification Admin pour vous connecter au compte Google Drive.

2

#### Déployez des données adaptées au cloud

"[Déployez des données adaptées au cloud](#)" si aucune instance n'est déjà déployée.

3

#### Connectez-vous au compte Google Drive

À l'aide des informations d'identification utilisateur Admin, connectez-vous au compte Google Drive auquel vous souhaitez accéder afin qu'il soit ajouté en tant que nouvelle source de données.

4

#### Sélectionnez le type de numérisation des fichiers utilisateur

Sélectionnez le type de numérisation que vous souhaitez effectuer sur les fichiers utilisateur : mappage ou mappage et classification.

### Vérification de la configuration requise pour Google Drive

Consultez les conditions préalables suivantes pour vous assurer que vous êtes prêt à activer Cloud Data SENSE sur un compte Google Drive.

- Vous devez disposer des informations d'identification Admin pour le compte Google Drive qui fournissent un accès en lecture aux fichiers de l'utilisateur

## Restrictions actuelles

Les fonctions suivantes de détection de données ne sont pas prises en charge actuellement avec les fichiers Google Drive :

- Lorsque vous affichez des fichiers dans la page recherche de données, les actions de la barre de boutons ne sont pas actives. Vous ne pouvez copier, déplacer, supprimer, etc. Aucun fichier.
- Les autorisations ne peuvent pas être identifiées dans les fichiers de Google Drive. Aucune information d'autorisation n'est donc affichée dans la page Investigation.

## Déployer des solutions Cloud Data est logique

Déployez Cloud Data si aucune instance n'est déjà déployée.

Il peut y avoir un sens des données "déploiement dans le cloud" ou "dans un emplacement sur site avec accès à internet".

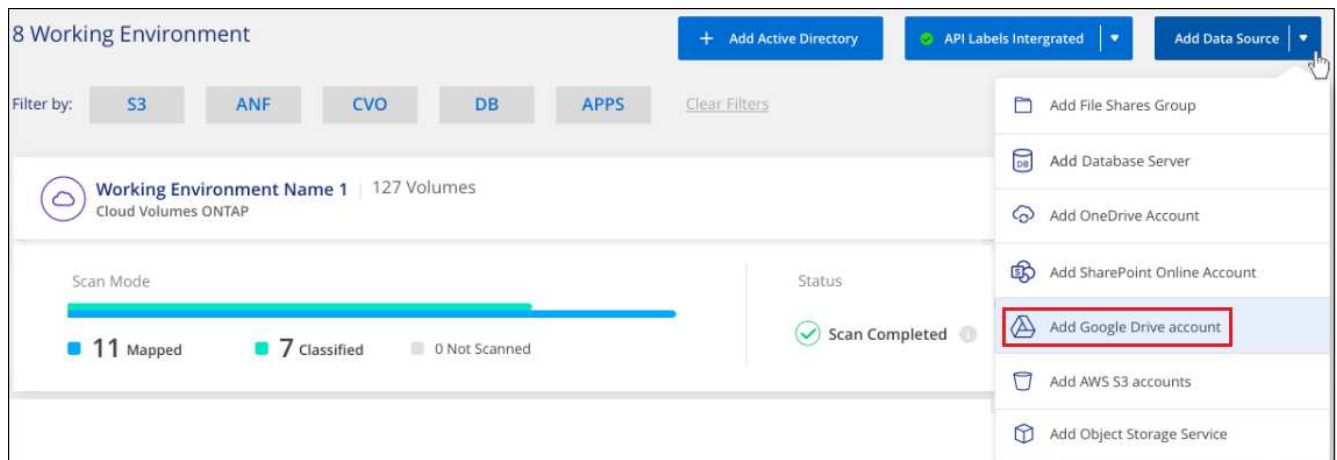
Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

## Ajout du compte Google Drive

Ajoutez le compte Google Drive où résident les fichiers utilisateur. Si vous souhaitez analyser des fichiers de plusieurs utilisateurs, vous devez exécuter cette étape pour chaque utilisateur.

### Étapes

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données > Ajouter un compte Google Drive**.



2. Dans la boîte de dialogue Ajouter un compte Google Drive, cliquez sur **Connectez-vous à Google Drive**.
3. Sur la page Google qui s'affiche, sélectionnez le compte Google Drive et entrez l'utilisateur et le mot de passe d'administration requis, puis cliquez sur **Accept** pour permettre à Cloud Data SENSE de lire les données de ce compte.

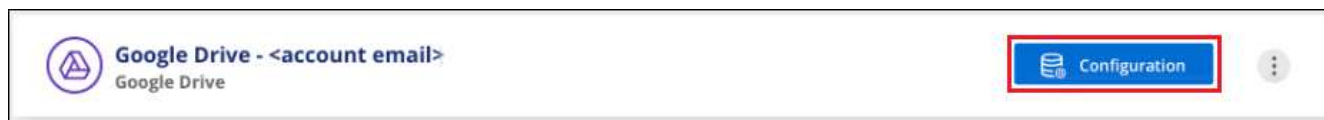
Le compte Google Drive est ajouté à la liste des environnements de travail.

## Sélection du type de numérisation des données utilisateur

Sélectionnez le type d'analyse que Cloud Data SENSE effectuera sur les données de l'utilisateur.

### Étapes

1. Dans la page *Configuration*, cliquez sur le bouton **Configuration** du compte Google Drive.



2. Activez les analyses de mappage uniquement, ou les analyses de mappage et de classification, sur les fichiers du compte Google Drive.



À :	Procédez comme suit :
Activer les analyses de mappage uniquement sur les fichiers	Cliquez sur <b>carte</b>
Activez les analyses complètes sur les fichiers	Cliquez sur <b>carte et classement</b>
Désactiver la numérisation sur les fichiers	Cliquez sur <b>Off</b>

## Résultat

Cloud Data SENSE commence à analyser les fichiers du compte Google Drive que vous avez ajouté et les résultats sont affichés dans le tableau de bord et à d'autres emplacements.

## Suppression d'un compte Google Drive des analyses de conformité

Étant donné que les fichiers Google Drive d'un seul utilisateur font partie d'un seul compte Google Drive, si vous voulez arrêter de numériser des fichiers à partir du compte Google Drive d'un utilisateur, alors vous devriez "[Supprimez le compte Google Drive de Data Sense](#)".

## Analyse des partages de fichiers

Procédez comme suit pour lancer l'analyse des partages de fichiers NFS ou CIFS non NetApp directement avec Cloud Data SENSE. Ces partages de fichiers peuvent résider sur site ou dans le cloud.

## Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.



### Vérifiez les conditions préalables au partage de fichiers

Pour les partages CIFS (SMB), assurez-vous que vous disposez des identifiants pour accéder aux partages.



**2**

## Déployez l'instance Cloud Data SENSE

"[Déployez des données adaptées au cloud](#)" si aucune instance n'est déjà déployée.

**3**

## Créez un groupe pour conserver les partages de fichiers

Le groupe est un conteneur pour les partages de fichiers que vous souhaitez analyser et il est utilisé comme nom d'environnement de travail pour ces partages de fichiers.

**4**

## Ajoutez les partages de fichiers et sélectionnez les partages à analyser

Ajoutez la liste des partages de fichiers que vous souhaitez numériser et sélectionnez le type de numérisation. Vous pouvez ajouter jusqu'à 100 partages de fichiers à la fois.

### Vérification des exigences relatives au partage de fichiers

Avant d'activer le Cloud Data sens, lisez les conditions préalables suivantes pour vérifier que la configuration est prise en charge.

- Ils peuvent être hébergés partout, y compris dans le cloud ou sur site. Il s'agit de partages de fichiers qui résident sur des systèmes de stockage non NetApp.
- Il faut une connectivité réseau entre l'instance Data Sense et les partages.
- Assurez-vous que ces ports sont ouverts à l'instance de détection de données :
  - Pour NFS – ports 111 et 2049.
  - Pour CIFS – ports 139 et 445.
- Vous aurez besoin de la liste des partages que vous souhaitez ajouter au format `<host_name>:/<share_path>`. Vous pouvez entrer les partages individuellement ou fournir une liste séparée par des lignes des partages de fichiers que vous souhaitez scanner.
- Pour les partages CIFS (SMB), assurez-vous que vous disposez des identifiants Active Directory qui fournissent un accès en lecture aux partages. Les identifiants d'administrateur sont à privilégier dans le cas où Cloud Data SENSE doit analyser toutes les données qui exigent des autorisations élevées.

Si vous voulez vous assurer que vos fichiers "dernières heures d'accès" sont inchangés par les analyses de classification de détection de données, nous recommandons à l'utilisateur de disposer de l'autorisation Write Attributes. Si possible, nous vous recommandons de faire en sorte que l'utilisateur configuré Active Directory fasse partie d'un groupe parent de l'organisation qui dispose des autorisations pour tous les fichiers.

### Déploiement de l'instance Cloud Data Sense

Déployez Cloud Data si aucune instance n'est déjà déployée.

Si vous scannez des partages de fichiers NFS ou CIFS non NetApp accessibles via Internet, vous pouvez "[Déployez les données du cloud dans le cloud](#)" ou "[Déployer Data Sense dans un emplacement sur site avec accès Internet](#)".

Si vous scannez des partages de fichiers NFS ou CIFS non NetApp installés dans un site sombre qui n'offrent pas d'accès à Internet, vous devez le faire "[Déployez les données cloud sur site qui ne disposent pas d'un accès Internet](#)". Cela nécessite également que le connecteur BlueXP soit déployé dans le même emplacement

sur site.

Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

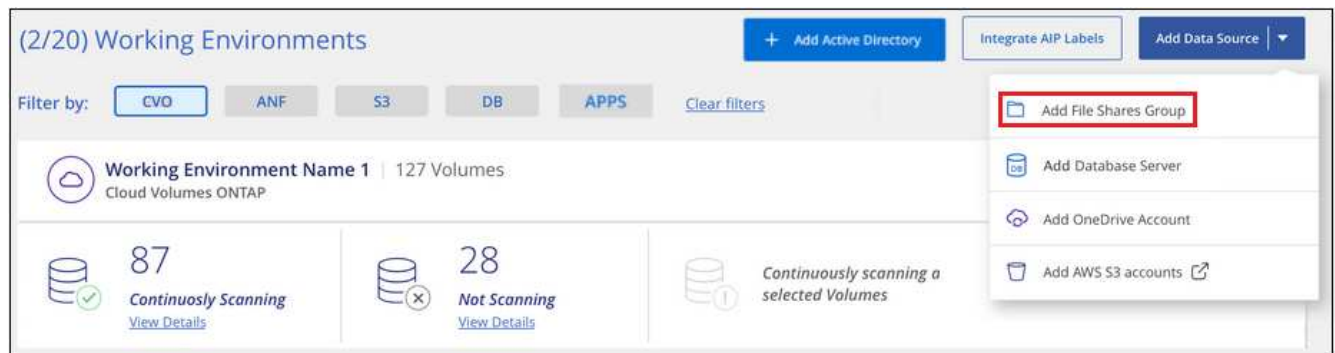
## Création du groupe pour les partages de fichiers

Vous devez ajouter un « groupe » de partages de fichiers avant de pouvoir ajouter vos partages de fichiers. Le groupe est un conteneur pour les partages de fichiers que vous souhaitez analyser et le nom du groupe est utilisé comme nom d'environnement de travail pour ces partages de fichiers.

Vous pouvez mélanger des partages NFS et CIFS dans le même groupe, mais tous les partages de fichiers CIFS d'un groupe doivent utiliser les mêmes informations d'identification Active Directory. Si vous prévoyez d'ajouter des partages CIFS qui utilisent des identifiants différents, vous devez créer un groupe distinct pour chaque ensemble unique d'informations d'identification.

### Étapes

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données > Ajouter un groupe de partages de fichiers**.



2. Dans la boîte de dialogue Ajouter un groupe de partages de fichiers, entrez le nom du groupe de partages et cliquez sur **Continuer**.

Le nouveau groupe de partages de fichiers est ajouté à la liste des environnements de travail.

## Ajout de partages de fichiers à un groupe

Vous ajoutez des partages de fichiers au groupe de partages de fichiers afin que les fichiers de ces partages soient analysés par Cloud Data Sense. Vous ajoutez les partages au format `<host_name>:/<share_path>`.

Vous pouvez ajouter des partages de fichiers individuels, ou vous pouvez fournir une liste séparée par des lignes des partages de fichiers que vous souhaitez analyser. Vous pouvez ajouter jusqu'à 100 partages à la fois.

Lorsque vous ajoutez à la fois des partages NFS et CIFS au sein d'un seul groupe, vous devez recommencer le processus à deux reprises, après avoir ajouté des partages NFS, puis à nouveau en ajoutant les partages CIFS.

### Étapes

1. Dans la page *Working Environments*, cliquez sur le bouton **Configuration** pour le groupe de partages de fichiers.



2. Si c'est la première fois que vous ajoutez des partages de fichiers pour ce groupe de partages de fichiers, cliquez sur **Ajouter vos premiers partages**.



Si vous ajoutez des partages de fichiers à un groupe existant, cliquez sur **Ajouter des partages**.



3. Sélectionnez le protocole pour les partages de fichiers que vous ajoutez, ajoutez les partages de fichiers que vous souhaitez analyser - un partage de fichiers par ligne - et cliquez sur **Continuer**.

Lors de l'ajout de partages CIFS (SMB), vous devez entrer les identifiants Active Directory qui fournissent un accès en lecture aux partages. Les identifiants d'administrateur sont privilégiés.

Une boîte de dialogue de confirmation affiche le nombre de partages ajoutés.

Si la boîte de dialogue répertorie tous les partages qui n’ont pas pu être ajoutés, capturez ces informations pour résoudre le problème. Dans certains cas, vous pouvez ajouter à nouveau le partage avec un nom d’hôte ou un nom de partage corrigé.

4. Activez les analyses de mappage uniquement, ou les analyses de mappage et de classification, sur chaque partage de fichiers.

À :	Procédez comme suit :
Activez les analyses de mappage uniquement sur les partages de fichiers	Cliquez sur <b>carte</b>
Activez les analyses complètes sur les partages de fichiers	Cliquez sur <b>carte et classement</b>
Désactiver l’analyse sur les partages de fichiers	Cliquez sur <b>Off</b>

### Résultat

Cloud Data Sense commence à analyser les fichiers dans les partages de fichiers que vous avez ajoutés, et les résultats sont affichés dans le Tableau de bord et à d’autres emplacements.

### Suppression d’un partage de fichiers des analyses de conformité

Si vous n’avez plus besoin d’analyser certains partages de fichiers, vous pouvez supprimer chaque partage de fichiers de l’analyse de leurs fichiers à tout moment. Il vous suffit de cliquer sur **Supprimer le partage** dans la page Configuration.



## Analyse du stockage objet à l'aide du protocole S3

Suivez quelques étapes pour commencer à analyser les données dans le stockage objet directement avec Cloud Data Sense. La fonction Data Sense peut analyser les données depuis n'importe quel service de stockage objet utilisant le protocole simple Storage Service (S3). Notamment NetApp StorageGRID, IBM Cloud Object Store, Azure Blob (via MiniO), Linode, B2 Cloud Storage, Amazon S3, et bien plus encore.

### Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

#### Examiner les prérequis en matière de stockage objet

Vous devez disposer de l'URL du terminal pour vous connecter au service de stockage objet.

Vous devez disposer de la clé d'accès et de la clé secrète du fournisseur de stockage objet pour que le Cloud Data SENSE puisse accéder aux compartiments.

2

#### Déployez l'instance Cloud Data SENSE

"[Déployez des données adaptées au cloud](#)" si aucune instance n'est déjà déployée.

3

#### Ajoutez le service de stockage objet

Ajoutez le service de stockage objet au sens des données dans le cloud.

4

#### Sélectionnez les compartiments à numériser

Sélectionnez les compartiments que vous souhaitez analyser et Cloud Data SENSE commence à les analyser.

### Examen des besoins en stockage objet

Avant d'activer le Cloud Data sens, lisez les conditions préalables suivantes pour vérifier que la configuration est prise en charge.

- Vous devez disposer de l'URL du terminal pour vous connecter au service de stockage objet.

- Vous devez disposer de la clé d'accès et de la clé secrète du fournisseur de stockage objet afin que Data Sense puisse accéder aux compartiments.
- La prise en charge d'Azure Blob requiert que vous utilisiez le "[Service MiniO](#)".

## Déploiement de l'instance Cloud Data Sense

Déployez Cloud Data si aucune instance n'est déjà déployée.

Si vous analysant des données à partir du stockage objet S3 accessible via Internet, vous pouvez "[Déployez les données du cloud dans le cloud](#)" ou "[Déployer Data Sense dans un emplacement sur site avec accès Internet](#)".

Si vous analysant les données à partir du stockage objet S3 qui a été installé dans un site sombre mais qui n'a pas d'accès à Internet, vous devez "[Déployez les données cloud sur site qui ne disposent pas d'un accès Internet](#)". Cela nécessite également que le connecteur BlueXP soit déployé dans le même emplacement sur site.

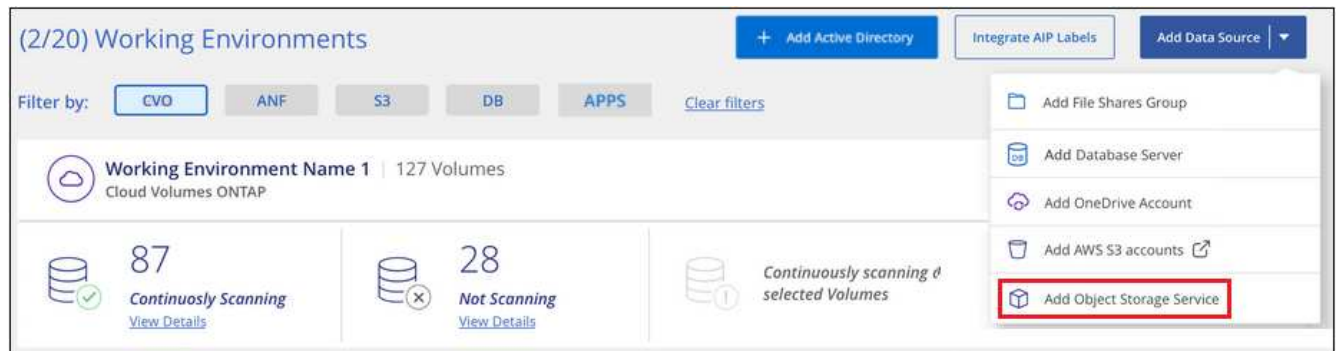
Les mises à niveau du logiciel Data Sense sont automatisées tant que l'instance est connectée à Internet.

## Ajout du service de stockage objet au sens Cloud Data

Ajoutez le service de stockage objet.

### Étapes

1. Dans la page Configuration des environnements de travail, cliquez sur **Ajouter une source de données > Ajouter un service de stockage d'objet**.



2. Dans la boîte de dialogue Ajouter un service de stockage objet, entrez les détails du service de stockage objet et cliquez sur **Continuer**.
  - a. Entrez le nom que vous souhaitez utiliser pour l'environnement de travail. Ce nom doit correspondre au nom du service de stockage objet auquel vous vous connectez.
  - b. Entrez l'URL du point final pour accéder au service de stockage d'objets.
  - c. Entrez la clé d'accès et la clé secrète pour que le cloud Data SENSE puisse accéder aux compartiments du stockage objet.

### Add Object Storage Service

Cloud Data Sense can scan data from any Object Storage service which uses the S3 protocol. This includes NetApp StorageGRID, IBM Object Store, and more.

To continue, enter the following information. In the next steps you'll need to select the buckets you want to scan.

Name the Working Environment	Endpoint URL
<input type="text" value="object_myIBM"/>	<input type="text" value="http://my.endpoint.com"/>
Access Key	Secret Key
<input type="text" value="AJUKD0574NDJG86795"/>	<input type="text" value="....."/>

## Résultat

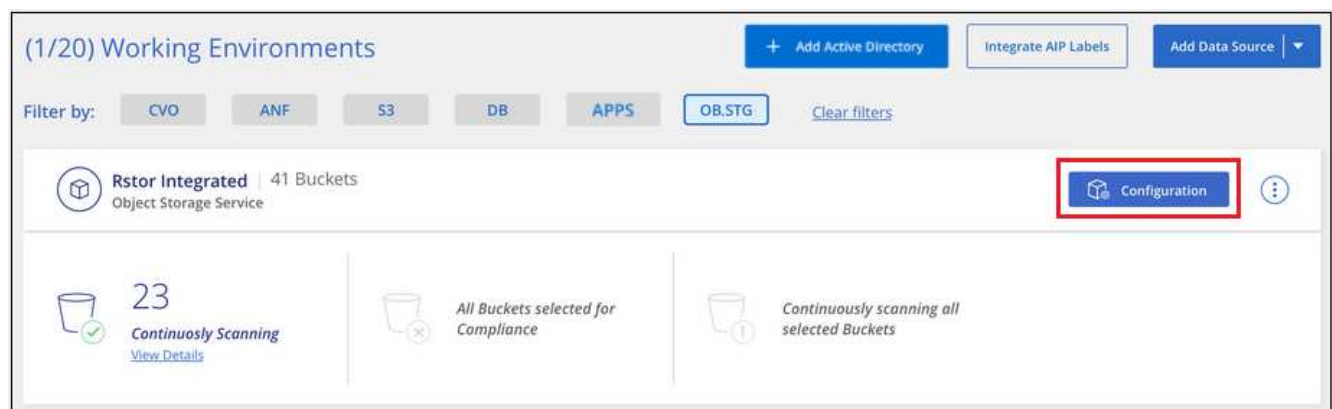
Le nouveau service de stockage objet est ajouté à la liste des environnements de travail.

## Activation et désactivation des analyses de conformité dans les compartiments de stockage objet

Une fois que vous avez activé le contrôle des données dans le cloud sur votre service de stockage objet, l'étape suivante consiste à configurer les compartiments à analyser. Data Sense détecte ces compartiments et les affiche dans l'environnement de travail que vous avez créé.

## Étapes

1. Dans la page Configuration, cliquez sur **Configuration** dans l'environnement de travail Object Storage Service.



2. Activez les analyses de mappage uniquement ou les analyses de mappage et de classification sur vos compartiments.



Rstor Integrated Configuration			
3/55 Buckets selected for Compliance scan			
Scan	Storage Repository (Bucket) ↓↑	Status ↓↑	Required Action ↓↑
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map &amp; Classify"/>	logs-759995470648-us-east-1	● Not Scanning	
<input type="button" value="Off"/> <input type="button" value="Map"/> <input type="button" value="Map &amp; Classify"/>	logs-759995470648-us-west-2	● Not Scanning	
<input type="button" value="Off"/> <input checked="" type="button" value="Map"/> <input type="button" value="Map &amp; Classify"/>	carstock	● Continuously Scanning	

À :	Procédez comme suit :
Activez les acquisitions avec mappage uniquement sur un compartiment	Cliquez sur <b>carte</b>
Activer les acquisitions complètes sur un compartiment	Cliquez sur <b>carte et classement</b>
Désactiver l'acquisition sur un godet	Cliquez sur <b>Off</b>

## Résultat

Cloud Data Sense commence l'analyse des compartiments que vous avez activés. En cas d'erreur, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

# Intégrez Active Directory avec le sens des données dans le cloud

Vous pouvez intégrer Active Directory global avec Cloud Data Sense pour améliorer les résultats de Data SENSE rapports sur les propriétaires de fichiers et quels utilisateurs et groupes ont accès à vos fichiers.

Lorsque vous configurez certaines sources de données (répertoriées ci-dessous), vous devez entrer les informations d'identification Active Directory pour que Data Sense puisse analyser les volumes CIFS. Cette intégration fournit des informations sur le propriétaire des fichiers et les autorisations des données qui résident dans ces sources. L'Active Directory saisi pour ces sources de données peut être différent des informations d'identification Active Directory globales que vous saisissez ici. Data Sense recherche dans tous les répertoires actifs intégrés les détails de l'utilisateur et de l'autorisation.

Cette intégration fournit des informations supplémentaires aux emplacements suivants dans Data Sense :

- Vous pouvez utiliser le « propriétaire de fichier » **"filtre"** Et voir les résultats dans les métadonnées du fichier dans le volet Investigation. Au lieu du propriétaire du fichier contenant le SID (identificateur de sécurité), il est renseigné avec le nom d'utilisateur réel.
- Vous pouvez voir **"autorisations complètes sur les fichiers"** Pour chaque fichier et répertoire lorsque vous cliquez sur le bouton « Afficher toutes les autorisations ».
- Dans le **"Tableau de bord gouvernance"**, Le panneau Ouvrir les autorisations affiche un niveau de détail plus élevé sur vos données.



Les SID des utilisateurs locaux et les SID des domaines inconnus ne sont pas traduits par le nom d'utilisateur réel.

## Sources de données prises en charge

Une intégration d'Active Directory avec Cloud Data SENSE peut identifier les données à partir de ces sources :

- Systèmes ONTAP sur site
- Cloud Volumes ONTAP
- Azure NetApp Files
- FSX pour ONTAP
- Partages de fichiers CIFS non NetApp (et non partages de fichiers NFS)

L'identification des informations d'utilisateur et d'autorisation à partir des schémas de base de données, des comptes OneDrive, des comptes SharePoint, des comptes Google Drive, des comptes Amazon S3 n'est pas prise en charge. Ou du stockage objet qui utilise le protocole simple Storage Service (S3).

## Connexion à votre serveur Active Directory

Une fois que vous avez déployé Data Sense et activé l'analyse sur vos sources de données, vous pouvez intégrer Data Sense à votre Active Directory. Il est possible d'accéder à Active Directory à l'aide d'une adresse IP de serveur DNS ou d'une adresse IP de serveur LDAP.

Les informations d'identification Active Directory peuvent être en lecture seule, mais fournir des informations d'identification d'administrateur garantit que Data Sense peut lire toutes les données qui requièrent des autorisations élevées. Les identifiants sont stockés sur l'instance Cloud Data Sense.

Pour les volumes/partages de fichiers CIFS, si vous voulez vous assurer que les « dernières heures d'accès » de vos fichiers ne sont pas modifiées par les analyses de classification de détection de données, nous recommandons à l'utilisateur de disposer des droits Write Attributes. Si possible, nous vous recommandons de faire en sorte que l'utilisateur configuré Active Directory fasse partie d'un groupe parent de l'organisation qui dispose des autorisations pour tous les fichiers.

### De formation

- Un Active Directory doit déjà être configuré pour les utilisateurs de votre entreprise.
- Vous devez disposer des informations pour Active Directory :
  - Adresse IP du serveur DNS, ou adresses IP multiples

ou

Adresse IP du serveur LDAP, ou adresses IP multiples

- Nom d'utilisateur et mot de passe pour accéder au serveur
  - Nom de domaine (nom Active Directory)
  - Que vous utilisiez ou non le protocole LDAP sécurisé (LDAPS)
  - Port serveur LDAP (généralement 389 pour LDAP et 636 pour LDAP sécurisé)
- Les ports suivants doivent être ouverts pour les communications sortantes par l'instance de détection de données :

Protocole	Port	Destination	Objectif
TCP ET UDP	389	Active Directory	LDAP
TCP	636	Active Directory	LDAP sur SSL
TCP	3268	Active Directory	Catalogue global
TCP	3269	Active Directory	Catalogue global sur SSL

## Étapes

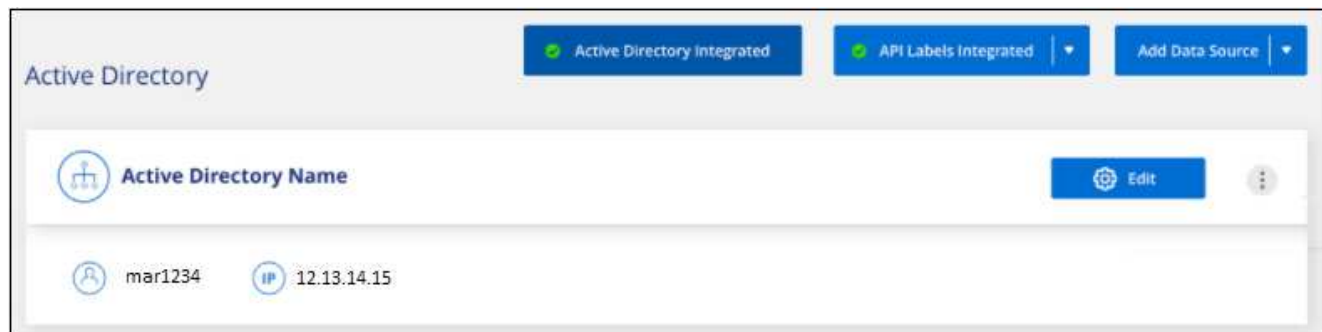
1. Dans la page Configuration de la détection des données du Cloud, cliquez sur **Ajouter Active Directory**.



2. Dans la boîte de dialogue connexion à Active Directory, entrez les détails d'Active Directory et cliquez sur **connexion**.


Si nécessaire, vous pouvez ajouter plusieurs adresses IP en cliquant sur **Ajouter IP**.

Data Sense s'intègre à Active Directory et une nouvelle section est ajoutée à la page Configuration.



## Gestion de votre intégration à Active Directory

Si vous devez modifier des valeurs dans votre intégration Active Directory, cliquez sur le bouton **Modifier** et apportez les modifications nécessaires.

Vous pouvez également supprimer l'intégration si vous n'en avez plus besoin en cliquant sur le bouton . Puis **Supprimer Active Directory**.

## Configurez les licences pour Cloud Data Sense

Les 1 premiers To de données que Cloud Data Sense scanne dans un espace de travail BlueXP sont gratuits. Une licence BYOL de NetApp, ou un abonnement depuis le marché de votre fournisseur cloud, est nécessaire pour continuer l'analyse des données après ce point.

Quelques remarques avant de lire plus loin :

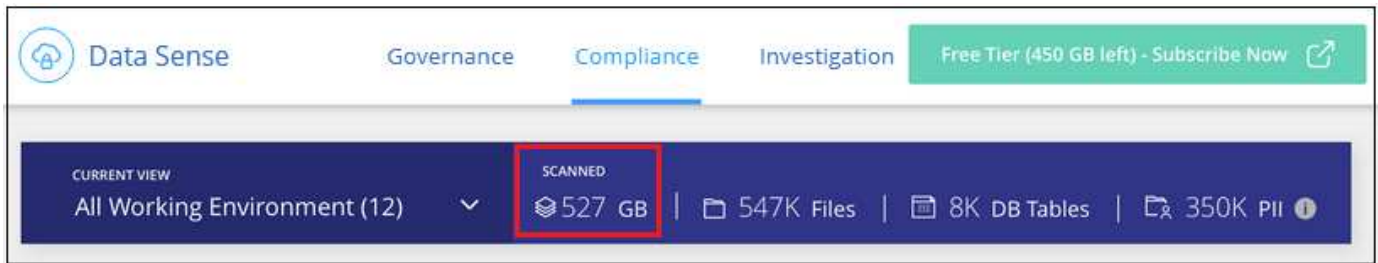
- Si vous vous êtes déjà abonné à l'abonnement BlueXP Pay-as-Go (PAYGO) dans le marché de votre fournisseur de services cloud, vous êtes également automatiquement abonné à Cloud Data SENSE. Vous n'aurez pas besoin de vous abonner à nouveau.
- La licence BYOL (Bring Your Own License) Cloud Data SENSE est une licence *flottante* que vous pouvez utiliser dans tous les environnements de travail et les sources de données de l'espace de travail que vous prévoyez d'analyser. Un abonnement actif s'affiche dans le porte-monnaie numérique.

["En savoir plus sur les licences et les coûts associés à Cloud Data Sense"](#).

## Utiliser un abonnement Cloud Data Sense PAYGO

Les abonnements avec paiement à l'utilisation sur le marché de votre fournisseur cloud vous permettent d'obtenir une licence pour l'utilisation de systèmes Cloud Volumes ONTAP et de nombreux services de données cloud, comme ceux de Cloud Data Sense.

Vous pouvez vous abonner à tout moment et vous ne serez facturé que lorsque la quantité de données dépasse 1 To. Vous pouvez toujours voir la quantité totale de données analysées à partir du tableau de bord de détection de données. Et le bouton *Subscribe Now* permet de vous abonner facilement lorsque vous êtes prêt.



## Étapes

Ces étapes doivent être effectuées par un utilisateur qui a le rôle *Account Admin*.

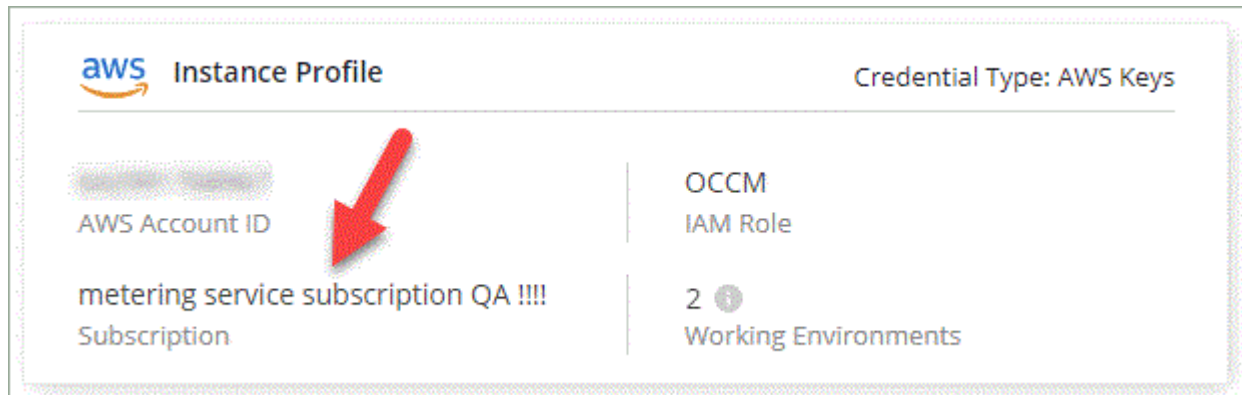
1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.



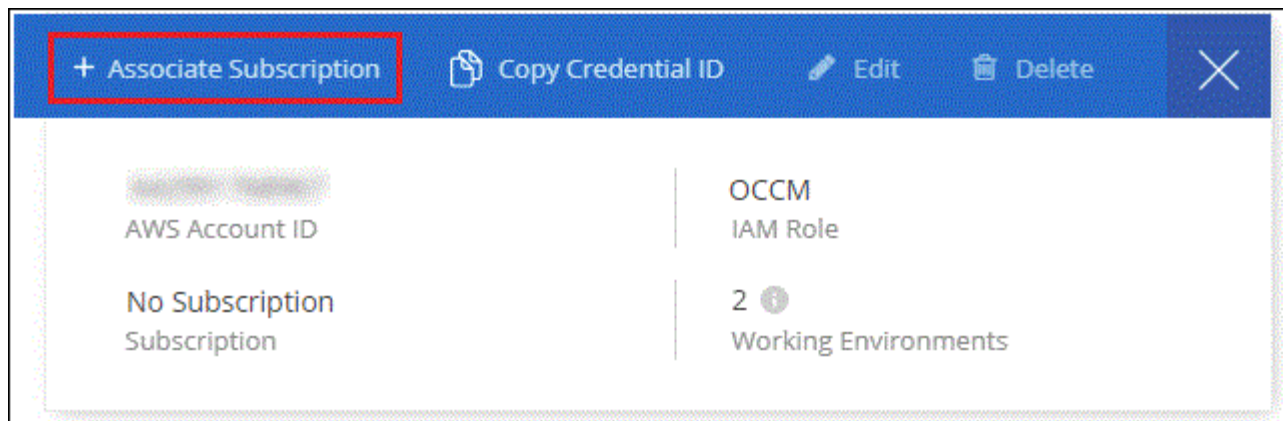
2. Recherchez les identifiants du profil d'instance AWS, de l'identité de service géré Azure ou de Google Project.

L'abonnement doit être ajouté au profil d'instance, à l'identité du service géré ou à Google Project. La charge ne fonctionnera pas autrement.

Si vous disposez déjà d'un abonnement BlueXP (indiqué ci-dessous pour AWS), vous êtes tous ensemble - il n'y a rien d'autre à faire.



3. Si vous n'avez pas encore d'abonnement, passez le curseur sur les informations d'identification, cliquez sur le menu d'action et cliquez sur **associer l'abonnement**.



4. Sélectionnez un abonnement existant et cliquez sur **associé**, ou cliquez sur **Ajouter un abonnement** et suivez les étapes.

La vidéo suivante montre comment associer un "AWS Marketplace" Abonnement à un abonnement AWS :

► [https://docs.netapp.com/fr-fr/cloud-manager-data-sense//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/fr-fr/cloud-manager-data-sense//media/video_subscribing_aws.mp4) (video)

La vidéo suivante montre comment associer un "Azure Marketplace" Abonnement à un abonnement Azure :

► [https://docs.netapp.com/fr-fr/cloud-manager-data-sense//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/fr-fr/cloud-manager-data-sense//media/video_subscribing_azure.mp4) (video)

La vidéo suivante montre comment associer un "Marketplace GCP" Abonnement à un abonnement GCP :

► [https://docs.netapp.com/fr-fr/cloud-manager-data-sense//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/fr-fr/cloud-manager-data-sense//media/video_subscribing_gcp.mp4) (video)

## Utilisez une licence BYOL Cloud Data Sense

Modèle BYOL de 1, 2 ou 3 ans avec les licences Bring Your Own. La licence BYOL **Cloud Data Sense** est une licence *flottante* où la capacité totale est partagée entre **tous** de vos environnements de travail et de vos sources de données, facilitant ainsi le renouvellement et la licence initiale.

Si vous ne disposez pas de licence Cloud Data Sense, contactez-nous pour en acheter un :

- Mailto:ng-contact-data-sense@netapp.com?subject=Licensing[Envoyer un e-mail pour acheter une licence].
- Cliquez sur l'icône de chat dans le coin inférieur droit de BlueXP pour demander une licence.

Si vous disposez d'une licence non attribuée pour Cloud Volumes ONTAP de nœud que vous ne pourrez pas utiliser, vous pouvez la convertir en licence Cloud Data Sense avec la même équivalence en dollars et la même date d'expiration. "[Cliquez ici pour plus d'informations](#)".

Utilisez la page porte-monnaie numérique de BlueXP pour gérer les licences BYOL Cloud Data Sense. Vous pouvez ajouter de nouvelles licences et mettre à jour des licences existantes.

## Procurez-vous votre fichier de licence Cloud Data Sense

Une fois que vous avez acheté votre licence Cloud Data Sense, vous activez la licence dans BlueXP en saisissant le numéro de série Cloud Data Sense et le compte NSS, ou en téléchargeant le fichier de licence NLF. Les étapes ci-dessous montrent comment obtenir le fichier de licence NLF si vous prévoyez d'utiliser cette méthode.

Si vous avez déployé Cloud Data SENSE sur un hôte d'un site sur site qui n'a pas accès à Internet, vous devez obtenir le fichier de licence d'un système connecté à Internet. L'activation de la licence à l'aide du numéro de série et du compte NSS n'est pas disponible pour les installations sur site sombre.

### Étapes

1. Connectez-vous au "[Site de support NetApp](#)" Et cliquez sur **systèmes > licences logicielles**.
2. Entrez le numéro de série de la licence Cloud Data Sense.

Serial #	Cluster SN	License Name	License Key	Host ID	Value	End Date
4810		SUBS-CLD-DAT-SENSE-TB-2Y	<a href="#">Get NetApp License File</a>		100	12/31/9998

3. Sous **License Key**, cliquez sur **Get NetApp License File**.
4. Saisissez votre identifiant de compte BlueXP (il s'agit d'un identifiant de locataire sur le site d'assistance) et cliquez sur **Submit** pour télécharger le fichier de licence.

**Get License**

SERIAL NUMBER: 4810

LICENSE: SUBS-CLD-DAT-SENSE-TB-2Y

SALES ORDER: 3005

TENANT ID:

Example: account-xxxxxxxx

[Cancel](#) [Submit](#)

Vous pouvez trouver votre identifiant de compte BlueXP en sélectionnant le menu déroulant **compte** en haut de BlueXP, puis en cliquant sur **gérer compte** en regard de votre compte. Votre ID de compte se trouve dans l'onglet vue d'ensemble.

### Ajoutez des licences BYOL Cloud Data Sense à votre compte

Après avoir acheté une licence Cloud Data Sense pour votre compte BlueXP, vous devez ajouter la licence à BlueXP pour utiliser le service Data Sense.

### Étapes

1. Dans le menu BlueXP, cliquez sur **gouvernance > porte-monnaie numérique**, puis sélectionnez l'onglet **licences de services de données**.
2. Cliquez sur **Ajouter une licence**.
3. Dans la boîte de dialogue *Add License*, entrez les informations de licence et cliquez sur **Add License**:



- Si vous disposez du numéro de série de la licence Data Sense et connaissez votre compte NSS, sélectionnez l'option **entrer le numéro de série** et saisissez ces informations.

Si votre compte sur le site de support NetApp n'est pas disponible dans la liste déroulante, "[Ajoutez le compte NSS à BlueXP](#)".

- Si vous disposez du fichier de licence de détection de données (requis lorsqu'il est installé sur un site sombre), sélectionnez l'option **Télécharger le fichier de licence** et suivez les invites pour joindre le fichier.

**Add License**

A license must be installed with an active subscription. The license enables you to use the Cloud Manager service for a certain period of time and for a maximum amount of space.

☒ Enter Serial Number    ☐ Upload License File

Serial Number

NetApp Support Site Account

**Add License**    Cancel

---

☐ Enter Serial Number    ☒ Upload License File

To install a license, follow these instructions:

- 1 Obtain the license file from the "System > Software Licenses" tab at [NetApp Support Site](#). You will need to provide your cloud service serial number and Cloud Manager Account ID.
- 2 Click Upload File and then select the file.

Upload License File  
 **Upload**

**Add License**    Cancel

## Résultat

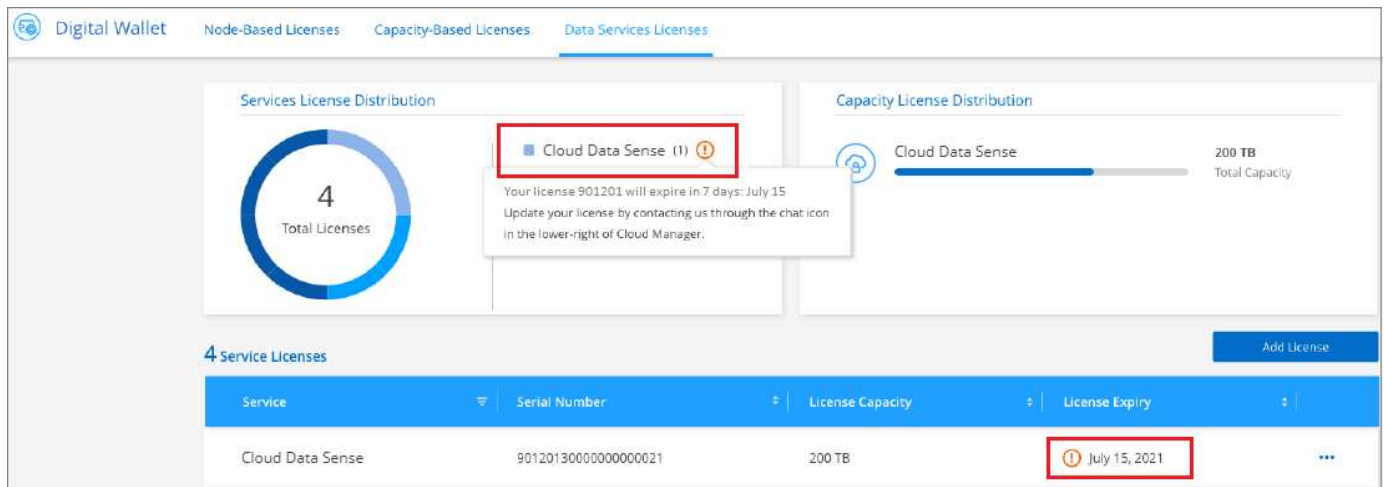
BlueXP ajoute la licence pour que votre service Cloud Data Sense soit actif.

## Mise à jour d'une licence BYOL Cloud Data Sense

Si la durée de votre licence approche de la date d'expiration ou si votre capacité sous licence atteint la limite, vous serez informé dans Cloud Data Sense.



Cet état apparaît également dans le porte-monnaie numérique.



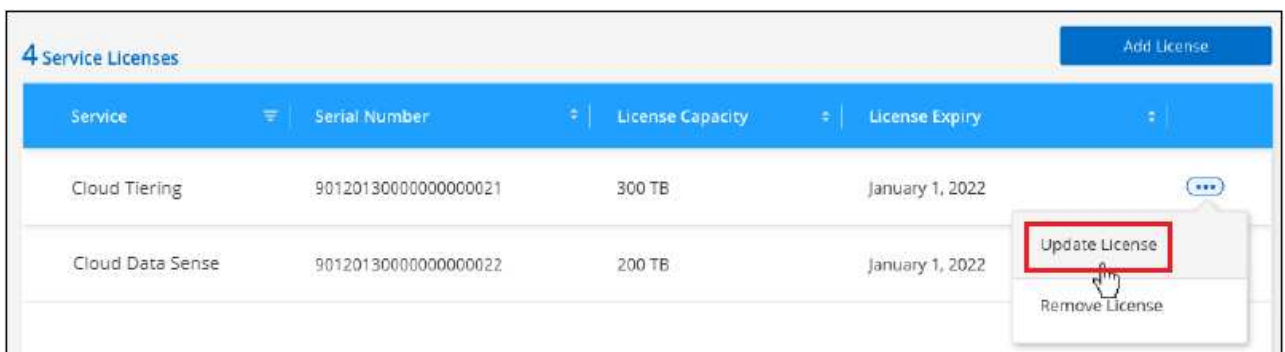
Vous pouvez mettre à jour votre licence Cloud Data Sense avant son expiration afin que vous puissiez accéder à vos données scannées sans interruption.

## Étapes

1. Cliquez sur l'icône de chat dans le coin inférieur droit de BlueXP pour demander une extension à votre terme ou une capacité supplémentaire à votre licence Cloud Data Sense pour le numéro de série particulier. Vous pouvez aussi [envoyer un e-mail pour demander une mise à jour de votre licence](#).

Une fois que vous avez payé la licence et qu'elle est enregistrée sur le site de support NetApp, BlueXP met automatiquement à jour la licence dans Digital Wallet et la page des licences des services de données reflétera la modification dans 5 à 10 minutes.

2. Si BlueXP ne peut pas mettre à jour automatiquement la licence (par exemple, lorsqu'elle est installée sur un site sombre), vous devrez charger manuellement le fichier de licence.
  - a. C'est possible [Procurez-vous le fichier de licence sur le site de support NetApp](#).
  - b. Sur la page porte-monnaie numérique de l'onglet *Data Services Licenses*, cliquez sur **...** Pour le numéro de série de service que vous mettez à jour, cliquez sur **mettre à jour la licence**.



- c. Dans la page *Update License*, téléchargez le fichier de licence et cliquez sur **Update License**.

## Résultat

BlueXP met à jour la licence pour que votre service Cloud Data Sense reste actif.

## Considérations relatives aux licences BYOL

Lors de l'utilisation d'une licence BYOL Cloud Data Sense, BlueXP affiche un avertissement dans l'interface utilisateur Data Sense et dans l'interface utilisateur de Digital Wallet lorsque la taille de toutes les données que

vous numérisez approche de la limite de capacité ou presque de la date d'expiration de la licence. Vous recevez ces avertissements :

- Lorsque la quantité de données que vous scannez atteint 80 % de la capacité sous licence, et une fois de plus que vous avez atteint la limite
- 30 jours avant l'expiration d'une licence, et encore une fois à l'expiration de celle-ci

Utilisez l'icône de chat en bas à droite de l'interface BlueXP pour renouveler votre licence lorsque vous voyez ces avertissements.

Si votre licence expire, Data Sense continue à fonctionner, mais l'accès aux tableaux de bord est bloqué afin que vous ne puissiez pas afficher les informations concernant vos données numérisées. Seule la page *Configuration* est disponible au cas où vous souhaitez réduire le nombre de volumes analysés afin d'augmenter votre capacité de stockage sous la limite de licence.

Une fois que vous renouvelez votre licence BYOL, BlueXP met automatiquement à jour la licence dans le porte-monnaie numérique et offre un accès complet à tous les tableaux de bord. Si BlueXP ne parvient pas à accéder au fichier de licence via la connexion Internet sécurisée (par exemple, lorsqu'il est installé sur un site sombre), vous pouvez obtenir le fichier vous-même et le télécharger manuellement vers BlueXP. Pour obtenir des instructions, reportez-vous à la section [Comment mettre à jour une licence Cloud Data Sense](#).



Si le compte que vous utilisez possède à la fois une licence BYOL et un abonnement PAYGO, Data Sense *ne* pas passer à l'abonnement PAYGO lorsque la licence BYOL expire. Vous devez renouveler la licence BYOL.

## Les questions les plus fréquemment posées à propos des données du cloud sont pertinentes

Cette FAQ peut vous aider si vous cherchez simplement une réponse rapide à une question.

### Service cloud Data Sense

Les questions suivantes présentent une compréhension générale du sens des données du cloud.

#### Qu'est-ce que les données cloud sont sensé ?

Cloud Data Sense est une offre cloud qui utilise la technologie d'intelligence artificielle (IA) pour vous aider à comprendre le contexte des données et à identifier les données sensibles dans vos systèmes de stockage. Les systèmes peuvent être des environnements de travail que vous avez ajoutés à BlueXP Canvas et de nombreux types de sources de données que Data Sense peut accéder sur vos réseaux. ["Voir la liste complète ci-dessous"](#).

Cloud Data SENSE fournit des paramètres prédéfinis (par exemple, des types d'informations sensibles et des catégories) pour respecter les nouvelles réglementations en matière de conformité des données concernant la confidentialité et la sensibilité des données, notamment le RGPD, la loi CCPA, HIPAA.

#### Comment fonctionne Cloud Data Sense ?

Cloud Data Sense déploie une autre couche d'intelligence artificielle avec votre système et vos systèmes de stockage BlueXP. Il analyse ensuite les données sur des volumes, des compartiments, des bases de données, ainsi que d'autres comptes de stockage, et indexe les informations exploitables concernant les données. Data

Sense exploite à la fois l'intelligence artificielle et le traitement du langage naturel, contrairement aux solutions alternatives habituellement développées autour d'expressions régulières et de la mise en correspondance de modèles. Cloud Data Sense utilise l'IA pour comprendre les données de façon contextuelle et assurer une détection et une classification précises. Elle est axée sur l'IA, car elle est conçue pour répondre aux besoins de types et d'évolutivité des données modernes. Il comprend également le contexte des données afin d'assurer une découverte et une classification solides et précises.

["Découvrez le fonctionnement de Cloud Data SENSE".](#)

### **Quelles sont les utilisations courantes du Cloud Data Sense ?**

- Identifier les informations à caractère personnel
- Localiser et créer facilement des rapports sur des données spécifiques en réponse à des sujets de données, conformément aux exigences du RGPD, de la loi CCPA, de l'HIPAA et d'autres réglementations en matière de confidentialité des données.
- Respectez les nouvelles réglementations sur la confidentialité des données, ainsi que celles à venir.
- Respectez les réglementations en matière de conformité et de confidentialité des données.
- Migrer les données des systèmes existants vers le cloud.
- Respectez les règles de conservation des données.

["Pour en savoir plus sur les utilisations de Cloud Data Sense".](#)

### **Qu'en est-il de l'architecture de données cloud SENSE ?**

Cloud Data Sense déploie un seul serveur ou un seul cluster, où que vous choisissiez, dans le cloud ou sur site. Les serveurs se connectent via des protocoles standard aux sources de données et indexent les résultats dans un cluster Elasticsearch, qui est également déployé sur les mêmes serveurs. Cette prise en charge permet la prise en charge d'environnements multcloud, interclouds, clouds privés et sur site.

### **Quels sont les fournisseurs de cloud pris en charge ?**

Cloud Data Sense fonctionne dans le cadre de BlueXP et prend en charge AWS, Azure et GCP. Votre entreprise peut ainsi bénéficier d'une visibilité unifiée sur la confidentialité des données entre les différents fournisseurs de cloud.

### **Cloud Data SENSE propose-t-il une API REST qui est compatible avec des outils tiers ?**

BlueXP prend en charge les fonctionnalités d'API REST pour ses services. Si BlueXP n'est pas le point de gestion préféré, il est également possible d'utiliser des services comme Cloud Data Sense via une API REST. Chaque action utilisateur dispose d'une API REST qui peut être intégrée à des systèmes tiers.

### **Est-il logique que les données cloud soient disponibles sur tous les marchés ?**

Oui, BlueXP et Cloud Data Sense sont disponibles sur les marchés AWS, Azure et GCP.

## **Analyse et analyse des données détecter les clouds**

Les questions suivantes concernent les performances d'analyse de Cloud Data Sense et l'analytique disponible pour les utilisateurs.

## Quelle est la fréquence d'analyse de mes données par Cloud Data SENSE ?

Comme les données changent fréquemment, Cloud Data SENSE analyse vos données en continu, sans aucune incidence sur vos données. Alors que l'analyse initiale de vos données peut prendre plus de temps, les analyses suivantes ne scannent que les modifications incrémentielles, ce qui réduit les temps d'analyse du système.

["Découvrez le fonctionnement des acquisitions"](#).

L'analyse des données a un impact négligeable sur vos systèmes de stockage et sur vos données. Cependant, si vous êtes préoccupé par un impact même très faible, vous pouvez configurer Data Sense pour effectuer des acquisitions « lentes ». ["Découvrez comment réduire la vitesse de numérisation"](#).

## Puis-je rechercher des données à l'aide du logiciel Cloud Data SENSE ?

Cloud Data Sense offre une fonctionnalité de recherche complète qui permet de rechercher facilement un fichier ou une pièce de données spécifique dans toutes les sources connectées. Le sens des données permet aux utilisateurs d'effectuer des recherches plus approfondies que ce que les métadonnées reflètent. Il s'agit d'un service indépendant de la langue qui peut également lire les fichiers et analyser une multitude de types de données sensibles, tels que les noms et les ID. Par exemple, les utilisateurs peuvent effectuer des recherches dans des magasins de données structurés et non structurés pour trouver des données qui peuvent s'être divulguées des bases de données aux fichiers des utilisateurs, en violation de la stratégie de l'entreprise. Les recherches peuvent être enregistrées ultérieurement et des règles peuvent être créées pour rechercher et prendre des mesures sur les résultats à une fréquence définie.

Une fois les fichiers qui vous intéressent trouvés, les caractéristiques peuvent être listées, y compris les balises, le compte de l'environnement de travail, le compartiment, le chemin du fichier, catégorie (à partir de la classification), taille du fichier, dernière modification, statut d'autorisation, doublons, niveau de sensibilité, données personnelles, types de données sensibles dans le fichier, propriétaire, type de fichier, taille de fichier, heure de création, hachage de fichier, si les données ont été attribuées à une personne demandant son attention, et plus encore. Les filtres peuvent être appliqués aux caractéristiques de tramage qui ne sont pas pertinentes. Data Sense possède également des contrôles RBAC permettant de déplacer ou de supprimer des fichiers, si les autorisations appropriées sont présentes. Si les autorisations appropriées ne sont pas présentes, les tâches peuvent être affectées à une personne de l'entreprise qui dispose des autorisations appropriées.

## Quels types d'analyses Cloud Data SENSE apporte-t-il ?

Les sources de données peuvent être représentées visuellement, et les relations définies et représentées graphiquement. Par exemple, les administrateurs peuvent visualiser toutes les données obsolètes, dupliquées et non liées à l'activité dans l'ensemble des sources de données de l'entreprise (systèmes sur site, bases de données, partages de fichiers, magasins S3, OneDrive, etc.). Elles peuvent ensuite copier, déplacer, supprimer et gérer des données afin d'optimiser les coûts de stockage et de réduire les risques. Les utilisateurs peuvent réduire les risques en voyant les données sensibles et créer des tâches de gestion des autorisations pour une protection renforcée des données. Data Sense classe également tous les différents types de données, afin que les administrateurs puissent analyser des données par type et voir les actions qui ont été effectuées sur les données et quand.

## Cloud Data SENSE propose-t-il des rapports ?

Oui. Les informations offertes par Cloud Data SENSE peuvent être pertinentes pour les autres parties prenantes de votre entreprise. Nous vous permettons donc de générer des rapports pour partager les informations exploitables. Les rapports suivants sont disponibles pour Data Sense :

## Rapport d'évaluation des risques pour la confidentialité

Fournit des informations sur la confidentialité à partir de vos données et un score de risque lié à la confidentialité. ["En savoir plus >>"](#).

## Rapport de demande d'accès au sujet des données

Vous permet d'extraire un rapport de tous les fichiers contenant des informations concernant le nom spécifique ou l'identifiant personnel d'un sujet de données. ["En savoir plus >>"](#).

## Rapport PCI DSS

Vous aide à identifier la distribution des informations de carte de crédit dans vos dossiers. ["En savoir plus >>"](#).

## Rapport HIPAA

Vous aide à identifier la distribution de l'information sur la santé dans vos dossiers. ["En savoir plus >>"](#).

## Rapport de mappage de données

Fournit des informations sur la taille et le nombre de fichiers dans vos environnements de travail. Cela inclut la capacité d'utilisation, l'âge des données, la taille des données et les types de fichiers. ["En savoir plus >>"](#).

## Rapports sur un type d'information spécifique

Des rapports sont disponibles, incluant des détails sur les fichiers identifiés qui contiennent des données personnelles et des données personnelles sensibles. Vous pouvez également voir les fichiers dérépartis par catégorie et par type de fichier. ["En savoir plus >>"](#).

## Les performances d'acquisition varient-elles ?

Les performances de l'analyse peuvent varier en fonction de la bande passante réseau et de la taille moyenne des fichiers dans votre environnement. Elle peut également dépendre des caractéristiques de taille du système hôte (dans le cloud ou sur site). Voir ["Instance Cloud Data SENSE"](#) et ["Déployer des solutions Cloud Data est logique"](#) pour en savoir plus.

Lors de l'ajout initial de nouvelles sources de données, vous pouvez également choisir d'effectuer uniquement une analyse de « mappage » au lieu d'une analyse de « classification » complète. Le mappage peut être effectué très rapidement sur vos sources de données car il n'accède pas aux fichiers pour voir les données à l'intérieur. ["Voir la différence entre une acquisition de cartographie et une acquisition de classification"](#).

## Gestion et confidentialité des données cloud SENSE

Les questions suivantes fournissent des informations sur la façon de gérer les paramètres de détection et de confidentialité des données dans le cloud.

### Comment activer le sens des données du cloud ?

Il vous faut tout d'abord déployer une instance de Cloud Data Sense dans BlueXP ou sur un système sur site. Une fois l'instance en cours d'exécution, vous pouvez activer le service sur les environnements de travail existants, les bases de données et d'autres sources de données à partir de l'onglet **Data Sense** ou en sélectionnant un environnement de travail spécifique.

["Découvrez comment démarrer"](#).



L'activation de Cloud Data Sense sur une source de données entraîne une analyse initiale immédiate. Les résultats de l'analyse s'affichent peu de temps après.

## Comment désactiver la détection des données dans le cloud ?

Vous pouvez désactiver Cloud Data Sense lors de l'analyse d'un environnement de travail, d'une base de données, d'un groupe de partage de fichiers, d'un compte OneDrive ou d'un compte SharePoint individuel à partir de la page Data Sense Configuration.

["En savoir plus >>".](#)



Pour supprimer complètement l'instance Cloud Data SENSE, vous pouvez supprimer manuellement l'instance Data Sense du portail de votre fournisseur cloud ou sur site.

## Puis-je personnaliser le service en fonction des besoins de mon entreprise ?

Cloud Data Sense fournit des informations prêtes à l'emploi pour vos données. Ces informations peuvent être extraites et utilisées en fonction des besoins de votre entreprise.

En outre, Data Sense offre de nombreuses façons d'ajouter une liste personnalisée de « données personnelles » que Data Sense identifiera dans les analyses, ce qui vous donne une idée complète de l'emplacement des données potentiellement sensibles dans les fichiers *All* de votre entreprise.

- Vous pouvez ajouter des identificateurs uniques basés sur des colonnes spécifiques dans les bases de données que vous scannez — nous appelons cela **Data Fusion**.
- Vous pouvez ajouter des mots-clés personnalisés à partir d'un fichier texte.
- Vous pouvez ajouter des répétitions personnalisées à l'aide d'une expression régulière (regex).

["En savoir plus >>".](#)

## Est-il possible de limiter les informations SENSE relatives aux données cloud à des utilisateurs spécifiques ?

Oui, Cloud Data SENSE est entièrement intégré à BlueXP. Les utilisateurs de BlueXP ne peuvent voir que les informations pour les environnements de travail qu'ils peuvent afficher en fonction de leurs privilèges d'espace de travail.

En outre, si vous souhaitez autoriser certains utilisateurs à simplement afficher les résultats d'analyse de détection de données sans pouvoir gérer les paramètres de détection de données, vous pouvez attribuer à ces utilisateurs le rôle Cloud Compliance Viewer.

["En savoir plus >>".](#)

## Quelqu'un peut-il accéder aux données privées envoyées entre mon navigateur et Data Sense ?

Non Les données privées envoyées entre votre navigateur et l'instance Data Sense sont sécurisées par un cryptage de bout en bout, ce qui signifie que NetApp et des tiers ne peuvent pas les lire. NetApp Data Sense ne partagera aucune donnée ou aucun résultat sauf si vous en faites la demande et que vous approuvez les accès.

## Que se passe-t-il si le Tiering des données est activé sur vos volumes ONTAP ?

Vous pouvez activer la détection des données cloud sur les systèmes ONTAP qui transfèrent les données inactives vers le stockage objet. Lorsque le Tiering est activé, Data Sense analyse toutes les données (sur des disques et les données inactives hiérarchisées vers le stockage objet).

L'analyse de conformité ne chauffe pas les données inactives : elles restent inactives et hiérarchisées vers le



stockage objet.

### **Cloud Data SENSE peut-il envoyer des notifications à mon entreprise ?**

Oui. En association avec la fonction stratégies, vous pouvez envoyer des alertes par e-mail aux utilisateurs BlueXP (tous les jours, toutes les semaines ou tous les mois) lorsqu'une police renvoie des résultats afin de recevoir des notifications pour protéger vos données. En savoir plus sur ["Stratégies"](#).

Vous pouvez également télécharger des rapports de statut à partir de la page gouvernance et de la page Investigation que vous pouvez partager en interne dans votre organisation.

### **Cloud Data Sense peut-il fonctionner avec les étiquettes AIP que j'ai intégrées dans mes fichiers ?**

Oui. Vous pouvez gérer les étiquettes AIP dans les fichiers que Cloud Data SENSE analyse si vous vous êtes abonné ["Protection des informations Azure \(AIP\)"](#). Vous pouvez afficher les libellés déjà affectés aux fichiers, ajouter des libellés aux fichiers et modifier les libellés existants.

["En savoir plus >>"](#).

## **Types de systèmes source et de types de données**

Les questions suivantes se rapportent aux types de stockage pouvant être analysés et aux types de données analysées.

### **Quelles sources de données peuvent être analysées à l'aide de Data Sense ?**

Cloud Data SENSE peut analyser les données à partir d'environnements de travail que vous avez ajoutés à BlueXP Canvas et à partir de nombreux types de sources de données structurées et non structurées auxquelles Data Sense peut accéder sur vos réseaux.

#### **Environnements de travail:**

- Cloud Volumes ONTAP (déployé dans AWS, Azure ou GCP)
- Clusters ONTAP sur site
- Azure NetApp Files
- Amazon FSX pour ONTAP
- Amazon S3

#### **Sources de données:**

- Partages de fichiers non NetApp
- Stockage objet (qui utilise le protocole S3)
- Bases de données (Amazon RDS, MongoDB, MySQL, Oracle, PostgreSQL, SAP HANA ET SQL SERVER)
- Comptes OneDrive
- SharePoint Online et des comptes sur site
- Comptes Google Drive

Data Sense prend en charge les versions NFS 3.x, 4.0 et 4.1 et CIFS 1.x, 2.0, 2.1 et 3.0.

## Y a-t-il des restrictions lorsqu'elles sont déployées dans une région gouvernementale?

Cloud Data Sense est pris en charge lorsque le connecteur est déployé dans une région gouvernementale (AWS GovCloud, Azure Government ou Azure DoD). Lorsqu'il est déployé de cette manière, Data SENSE présente les restrictions suivantes :

- Les comptes OneDrive, les comptes SharePoint et Google Drive ne peuvent pas être analysés.
- Impossible d'intégrer la fonctionnalité de label Microsoft Azure information protection (AIP).

## Quelles sources de données puis-je analyser si j'installe Data SENSE sur un site sans accès à Internet ?

Data Sense peut analyser uniquement les données à partir de sources locales vers le site. À l'heure actuelle, Data Sense peut analyser les sources de données locales suivantes dans un site « sombre » :

- Systèmes ONTAP sur site
- Schémas de base de données
- Comptes SharePoint sur site (SharePoint Server)
- Partages de fichiers CIFS ou NFS non NetApp
- Stockage objet qui utilise le protocole simple Storage Service (S3)

## Quels types de fichiers sont pris en charge ?

Cloud Data SENSE analyse tous les fichiers pour chaque catégorie et métadonnées, et affiche tous les types de fichiers dans la section types de fichiers du tableau de bord.

Lorsque Data SENSE détecte des informations à caractère personnel (PII) ou lorsqu'il effectue une recherche DSAR, seuls les formats de fichier suivants sont pris en charge :

.CSV, .DCM, .DICOM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX, Docs, Sheets, and Slides

## Quels types de données et de métadonnées Cloud Data détecte-t-il ?

Cloud Data SENSE vous permet d'exécuter une analyse « mapping » générale ou une analyse « complète » des sources de données. La cartographie ne fournit qu'une vue d'ensemble de haut niveau de vos données, tandis que Classification permet une analyse approfondie de vos données. Le mappage peut être effectué très rapidement sur vos sources de données car il n'accède pas aux fichiers pour voir les données à l'intérieur.

- Acquisition de mappage de données.

L'analyse des métadonnées uniquement. Ce qui est utile pour la gestion et la gouvernance globales des données, la définition rapide des projets, les gros domaines et la définition des priorités. Le mappage de données est basé sur les métadonnées et est considéré comme une acquisition **FAST**.

Après une acquisition rapide, vous pouvez générer un rapport de mappage de données. Ce rapport présente les données stockées dans vos sources de données d'entreprise et vous aide à prendre les bonnes décisions en matière d'utilisation des ressources, de migration, de sauvegarde, de sécurité et de conformité.

- Analyse de classification des données (approfondie).

Analyse de la détection de données à l'aide de protocoles standard et d'autorisations en lecture seule dans

l'ensemble de vos environnements. Les fichiers sélectionnés sont ouverts et analysés afin de détecter toute donnée sensible concernant l'entreprise, des informations privées et des problèmes liés aux attaques par ransomware.

Après une analyse complète, vous pouvez appliquer de nombreuses fonctions de détection de données supplémentaires à vos données, telles que la consultation et le raffinage des données dans la page recherche de données, la recherche de noms dans des fichiers, la copie, le déplacement et la suppression de fichiers source, etc.

## Licences et coût

Les questions suivantes se rapportent aux licences et aux coûts pour utiliser Cloud Data SENSE.

### Quel est le coût des données cloud ?

Le coût d'utilisation des données du cloud SENSE dépend de la quantité de données que vous scannez. Les 1 premiers To de données analysés par Data Sense dans un espace de travail BlueXP sont gratuits. Une fois cette limite atteinte, vous aurez besoin de l'une des options suivantes pour poursuivre l'analyse des données sur 1 To :

- Un abonnement à la liste BlueXP Marketplace de votre fournisseur cloud, ou
- Modèle BYOL (Bring Your Own License) de NetApp

Voir ["tarifs"](#) pour plus d'informations.

### Que se passe-t-il si la limite de capacité BYOL est atteinte ?

Si vous atteignez une limite de capacité BYOL, Data Sense continue à fonctionner, mais l'accès aux tableaux de bord est bloqué de sorte que vous ne puissiez pas afficher les informations concernant vos données numérisées. Seule la page de configuration est disponible au cas où vous souhaitez réduire le nombre de volumes analysés afin d'augmenter votre capacité de stockage sous la limite de licence. Vous devez renouveler votre licence BYOL pour rétablir l'accès complet à Data Sense.

## Déploiement de connecteurs

Les questions suivantes concernent le connecteur BlueXP.

### Quel est le connecteur ?

Il s'agit d'un logiciel exécuté sur une instance de calcul dans votre compte cloud ou sur site, permettant ainsi à BlueXP de gérer les ressources cloud de manière sécurisée. Vous devez déployer un connecteur pour utiliser le Cloud Data SENSE.

### Où le connecteur doit-il être installé ?

- Pour l'analyse des données dans Cloud Volumes ONTAP dans AWS, Amazon FSX pour ONTAP ou dans des compartiments AWS S3, vous utilisez un connecteur dans AWS.
- Pour analyser les données dans Cloud Volumes ONTAP dans Azure ou dans Azure NetApp Files, vous utilisez un connecteur dans Azure.
- Pour l'analyse des données dans Cloud Volumes ONTAP dans GCP, vous utilisez un connecteur dans GCP.
- Lors de l'analyse des données dans des systèmes ONTAP sur site, des partages de fichiers non NetApp,

un stockage objet S3 générique, des bases de données, des dossiers OneDrive, des comptes SharePoint et des comptes Google Drive, vous pouvez utiliser un connecteur dans tous ces emplacements cloud.

Donc, si vous disposez de données à plusieurs de ces emplacements, vous devrez peut-être les utiliser ["Plusieurs connecteurs"](#).

### **Puis-je déployer le connecteur sur mon propre hôte ?**

Oui. C'est possible ["Déployez le connecteur sur site"](#) Sur un hôte Linux de votre réseau ou dans le cloud. Si vous envisagez de déployer Data Sense sur site, vous pouvez aussi installer le connecteur sur site, mais ce n'est pas obligatoire.

### **Qu'en est-il des sites sécurisés sans accès à Internet ?**

Oui, cela est également pris en charge. C'est possible ["Déployez le connecteur sur un hôte Linux sur site qui n'a pas accès à Internet"](#). Vous pouvez ensuite détecter les clusters ONTAP sur site et d'autres sources de données locales et analyser les données à l'aide de Data Sense.

## **Le déploiement du sens des données**

Les questions suivantes se rapportent à l'instance séparée de détection de données.

### **Quels sont les modèles de déploiement pris en charge par Cloud Data ?**

BlueXP permet à l'utilisateur d'effectuer des analyses et des rapports sur des systèmes pratiquement n'importe où, y compris sur site, dans le cloud et dans les environnements hybrides. Cloud Data SENSE est généralement déployé à l'aide d'un modèle SaaS dans lequel le service est activé via l'interface BlueXP, et ne nécessite aucune installation matérielle ou logicielle. Même en ce mode de déploiement cliquer-exécuter, il est possible de gérer les données, que les datastores soient sur site ou dans le cloud public.

### **Quel type d'instance ou de machine virtuelle est requis pour le contrôle de données dans le cloud ?**

Quand ["déploiement dans le cloud"](#):

- Dans AWS, Cloud Data SENSE s'exécute sur une instance m5.4xlarge avec un disque GP2 de 500 Go.
- Dans Azure, Cloud Data Sense s'exécute sur une machine virtuelle standard\_D16s\_v3 avec un disque de 512 Go.
- Dans GCP, Cloud Data Sense s'exécute sur une machine virtuelle n2-standard-16 avec un disque persistant standard de 512 Go.

Notez que vous pouvez déployer Data Sense sur un système avec moins de processeurs et moins de RAM, mais il y a des limites lors de l'utilisation de ces systèmes. Voir ["Utilisation d'un type d'instance plus petit"](#) pour plus d'informations.

["Découvrez le fonctionnement de Cloud Data SENSE"](#).

### **Puis-je déployer l'analyse des données sur mon propre hôte ?**

Oui. Vous pouvez installer le logiciel Data Sense sur un hôte Linux qui a accès à Internet dans votre réseau ou dans le cloud. Tout fonctionne de la même façon et vous continuez à gérer votre configuration de numérisation et vos résultats via BlueXP. Voir ["Déploiement de Cloud Data SENSE sur site"](#) pour connaître la configuration système requise et les détails de l'installation.

### **Qu'en est-il des sites sécurisés sans accès à Internet ?**

Oui, cela est également pris en charge. C'est possible "[Déployer Data Sense dans un site sur site qui ne dispose pas d'un accès Internet](#)" pour des sites totalement sécurisés.

## 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.