Déployez des données adaptées au cloud

Cloud Data Sense

NetApp
December 15, 2022

Table des matières

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.

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.

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".

Déployez des données adaptées au cloud

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

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

Terminaux	Objectif
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://user-feedback-store-prod.s3.us-west-2.amazonaws.com https://customer-data-production.s3.us-west-2.amazonaws.com	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
https://api.bluexp.netapp.com	Communication avec le service BlueXP, qui inclut les comptes NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Communication avec le site Web BlueXP pour l'authentification centralisée des utilisateurs.
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://dseasb33srnrn.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.

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.

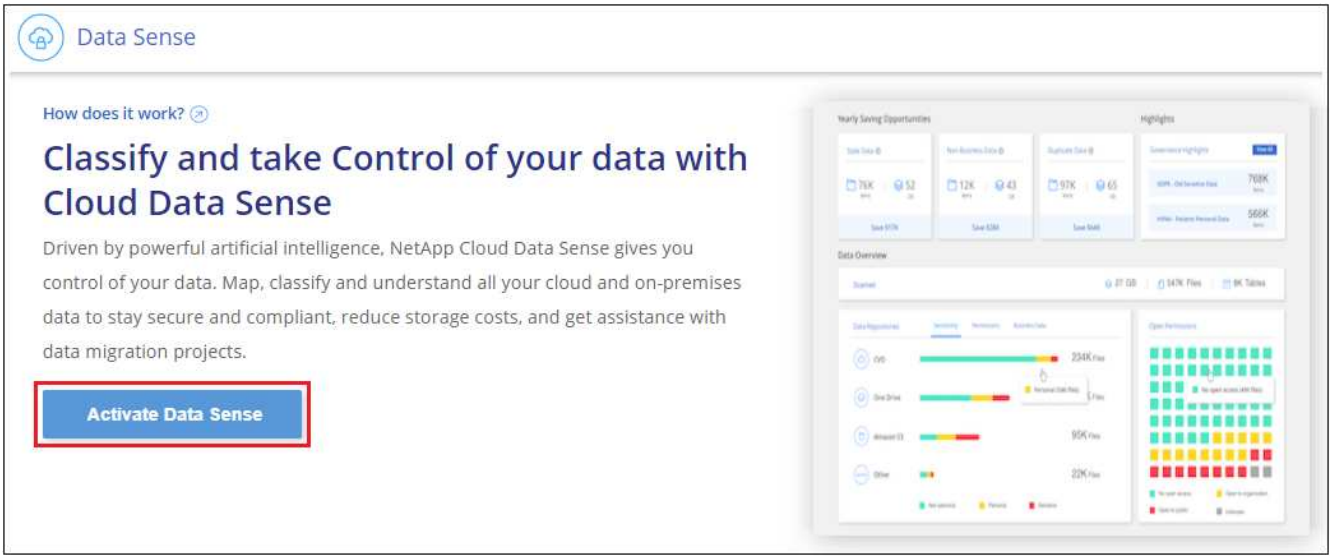
L'instance de détection de données utilise une adresse IP privée pour s'assurer que les données indexées ne sont pas accessibles à Internet. Par conséquent, le navigateur Web que vous utilisez pour accéder à BlueXP doit disposer d'une connexion à cette adresse IP privée. Cette connexion peut provenir 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

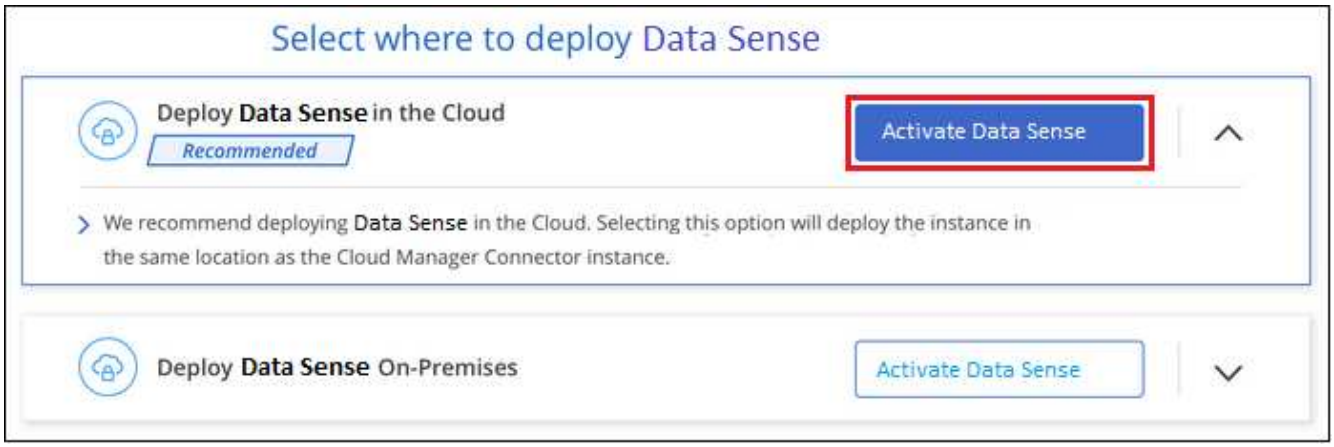
Voici la procédure à suivre pour déployer une instance de Cloud Data Sense dans le cloud.

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.

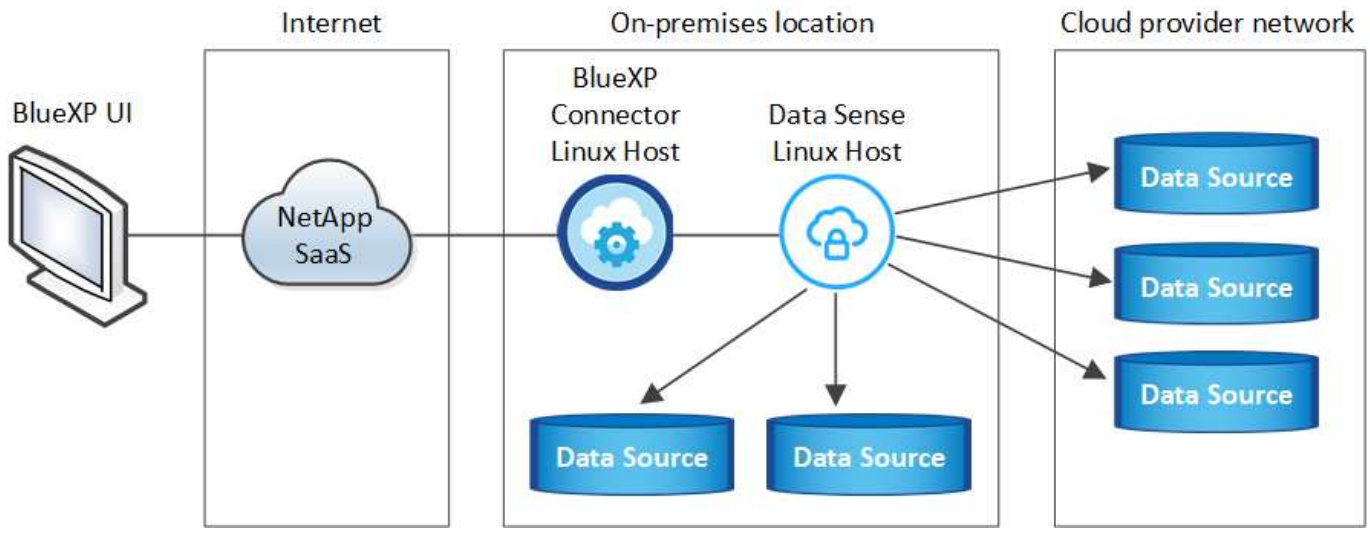
Vous pouvez également "Configurez les licences pour Cloud Data Sense" à ce moment-là. Vous ne serez facturé que lorsque la quantité de données dépasse 1 To.

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".

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.

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.

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
https://api.bluexp.netapp.com	Communication avec le service BlueXP, qui inclut les comptes NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Communication avec le site Web BlueXP pour l'authentification centralisée des utilisateurs.
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://dseasb33srnrn.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.

Terminaux	Objectif
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.

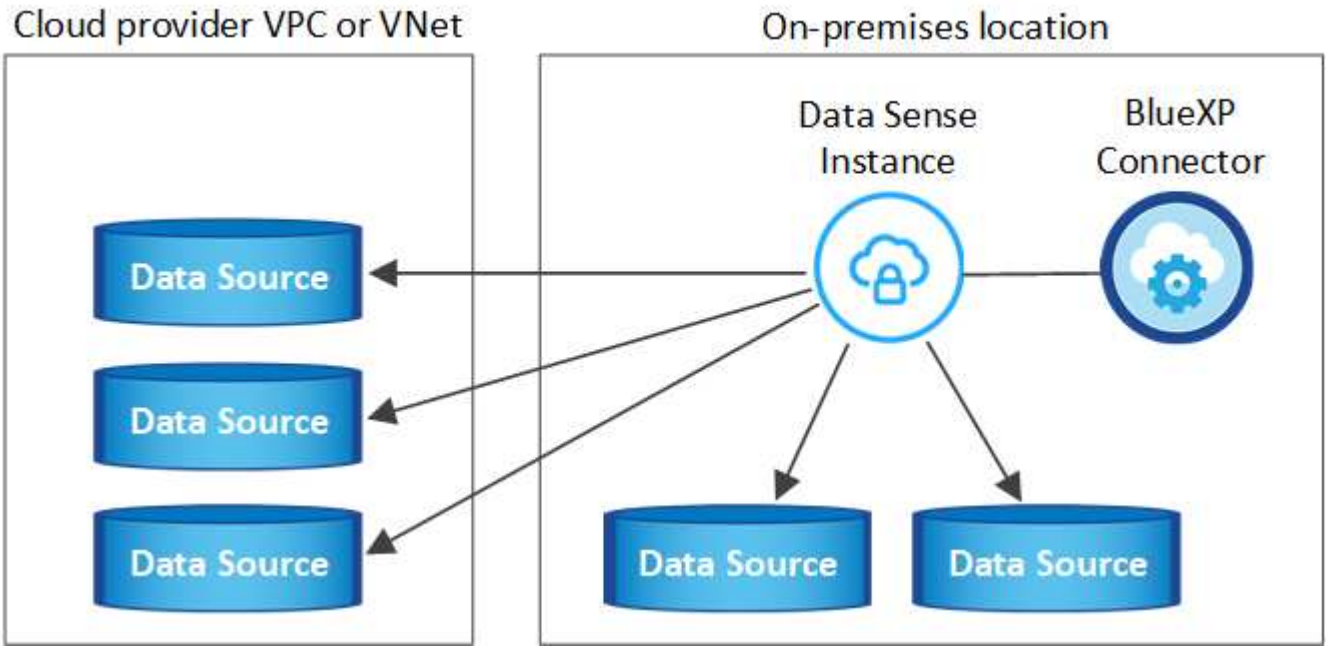
Type de connexion	Ports	Description
Connecteur <> cluster ONTAP (NAS)	443 (TCP)	BlueXP détecte les clusters ONTAP via HTTPS. Si vous utilisez des stratégies de pare-feu personnalisées, elles doivent répondre aux exigences suivantes : • L'hôte du connecteur doit autoriser l'accès HTTPS sortant via le port 443. Si le connecteur est dans le Cloud, toutes les communications sortantes sont autorisées par le groupe de sécurité prédéfini. • 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.
Cluster de détection des données <> ONTAP	• Pour NFS - 111 (TCP/UDP) et 2049 (TCP/UDP) • Pour CIFS - 139 (TCP/UDP) et 445 (TCP/UDP)	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. Assurez-vous que ces ports sont ouverts à l'instance de détection de données : • Pour NFS - 111 et 2049 • Pour CIFS : 139 et 445 Les règles d'exportation de volumes NFS doivent autoriser l'accès à partir de l'instance Data Sense.

Type de connexion	Ports	Description
Détection de données <> Active Directory	389 (TCP ET UDP), 636 (TCP), 3268 (TCP) ET 3269 (TCP)	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. Vous devez disposer des informations pour Active Directory : • Adresse IP du serveur DNS ou adresses IP multiples • Nom d'utilisateur et mot de passe du 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)

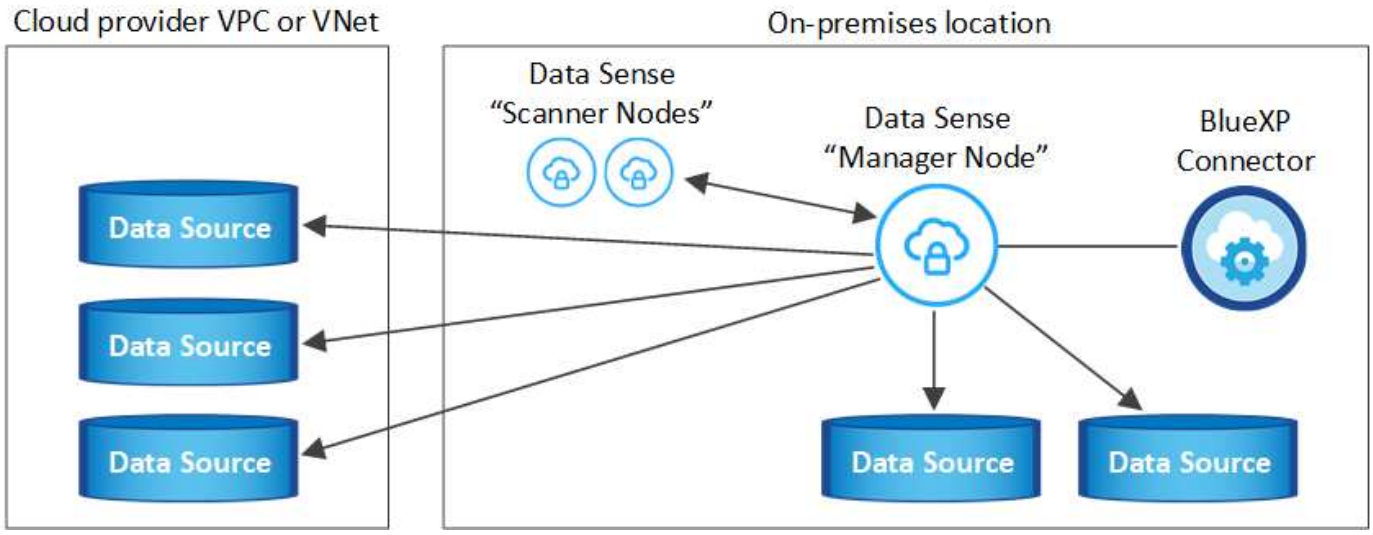
Si vous utilisez plusieurs hôtes Data Sense pour fournir une puissance de traitement supplémentaire pour analyser vos sources de données, vous devez activer des ports/protocoles supplémentaires. "Voir la configuration de port supplémentaire requise".

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

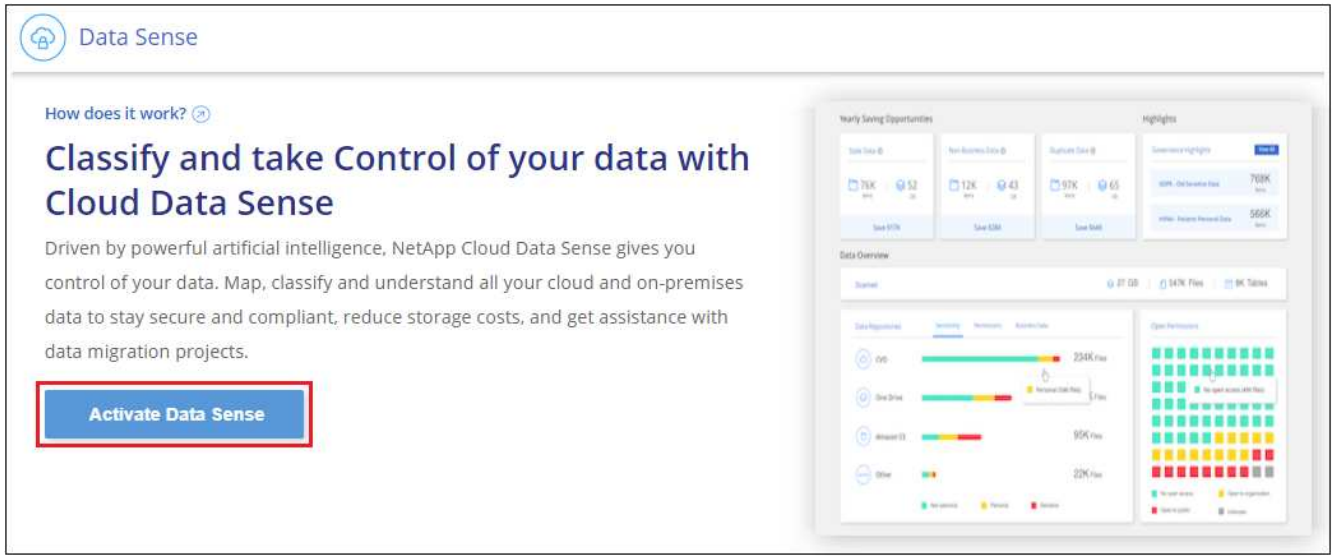
Suivez ces étapes pour installer le logiciel Data Sense sur un hôte sur site unique.

Ce dont vous avez besoin

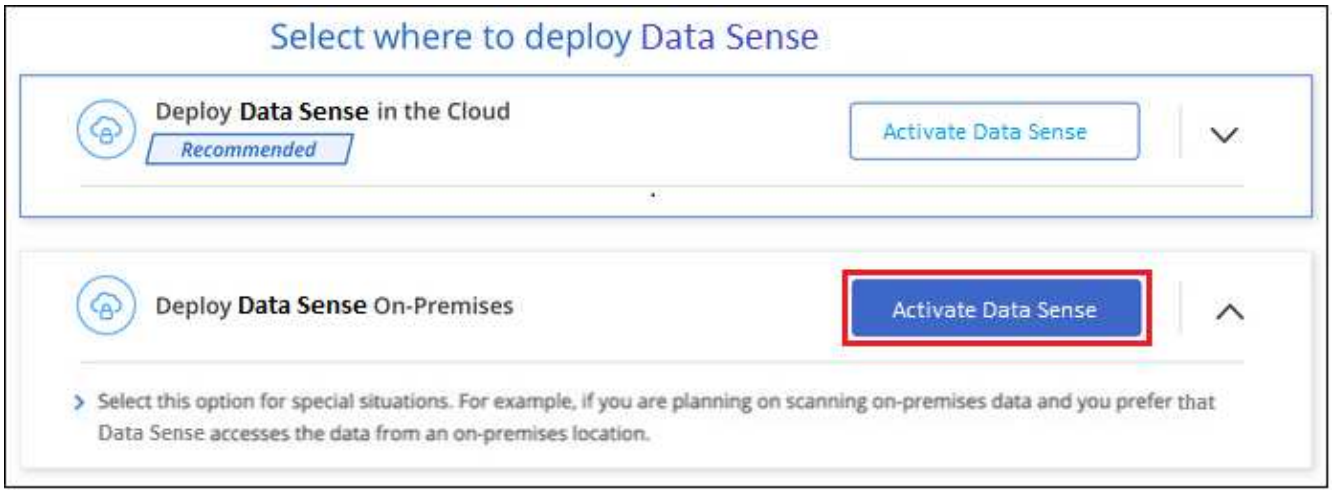
- Vérifiez que votre système Linux est conforme à la configuration requise pour l'hôte.
- (Facultatif) Vérifiez que le système est équipé des deux packages logiciels prérequis (Docker Engine et Python 3). Le programme d'installation installe ce logiciel s'il n'est pas déjà installé sur le système.
- 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 **DATASESNSE-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 :
a. Coller les informations copiées à partir de l'étape 6 : `sudo ./install.sh -a <account_id> -c <agent_id> -t <token>` 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. 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. 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.	Vous pouvez également créer l'ensemble de la commande à l'avance, en fournissant les paramètres d'hôte et de proxy nécessaires : `sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host> --manager-host <cm_host> --proxy-host <proxy_host> --proxy-port <proxy_port> --proxy-scheme <proxy_scheme> --proxy -user <proxy_user> --proxy-password <proxy_password> --cacert-folder-path <ca_cert_dir>`

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 "Configurez les licences pour Cloud Data Sense" à ce moment-là. Vous ne serez facturé que lorsque la quantité de données dépasse 1 To.

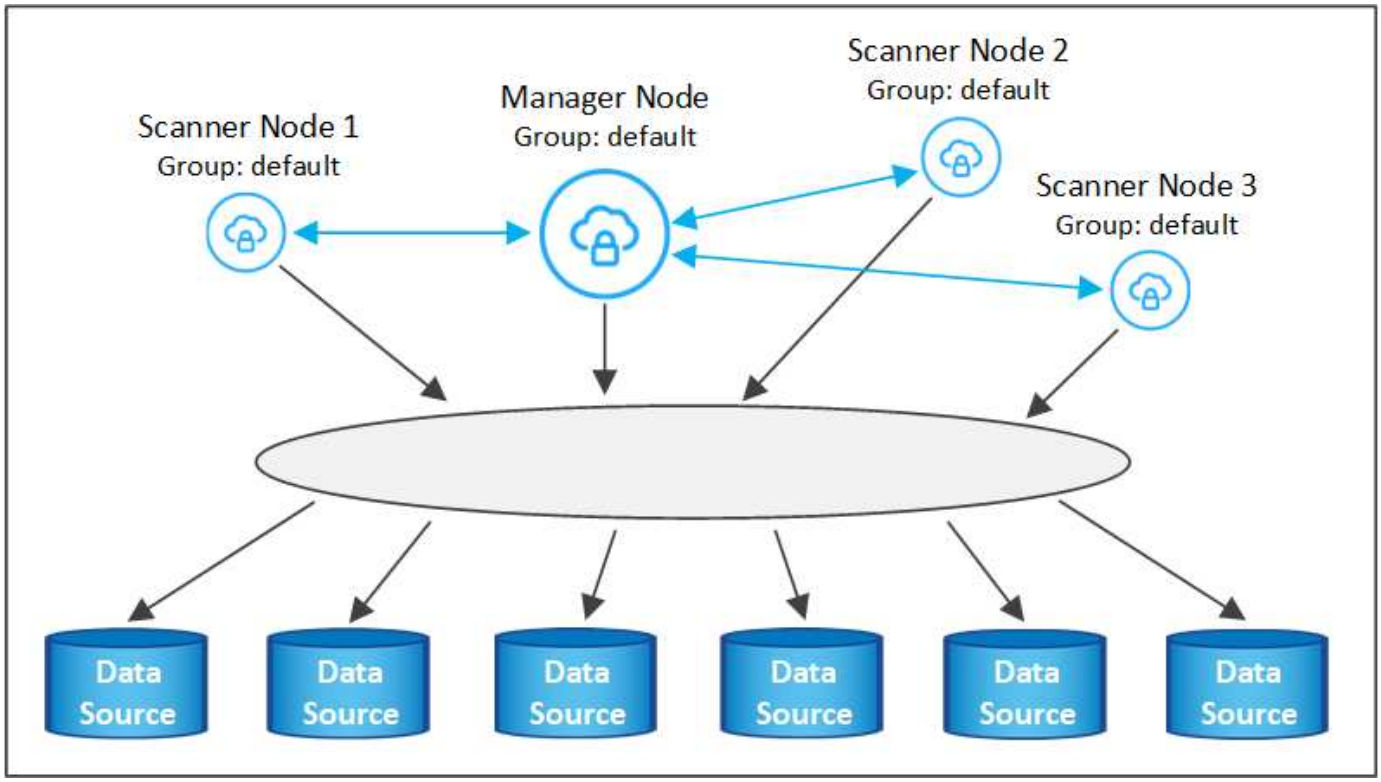
Ajoutez des nœuds de scanner à un déploiement existant

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 :

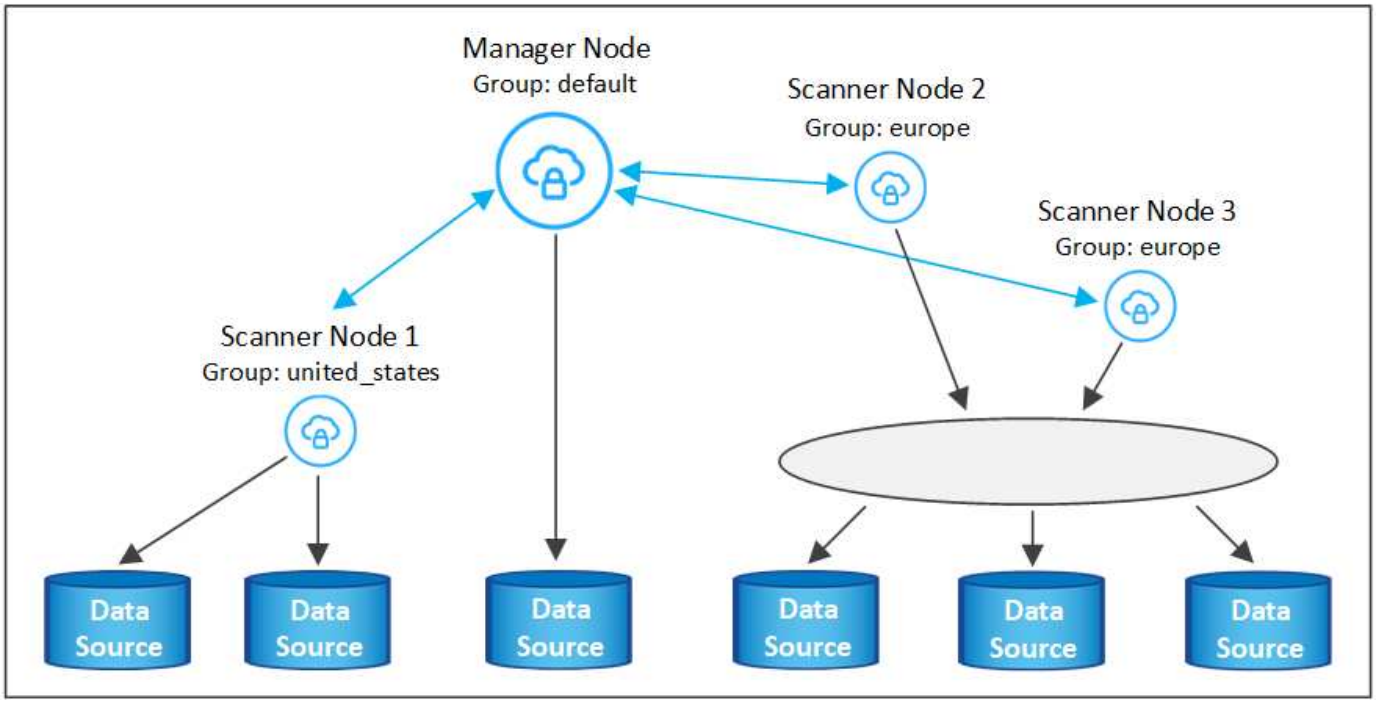
- ajoutez un nœud pour faciliter la numérisation de toutes les sources de données
- ajoutez un nœud pour faciliter l'analyse d'une source de données spécifique ou d'un groupe spécifique de sources de données

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 :

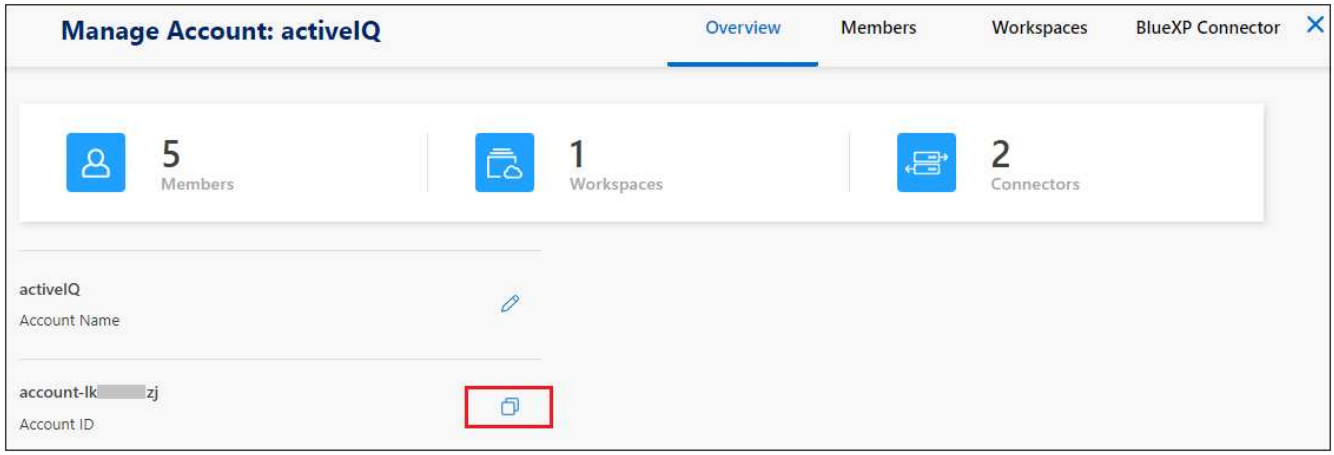
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7496/udp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

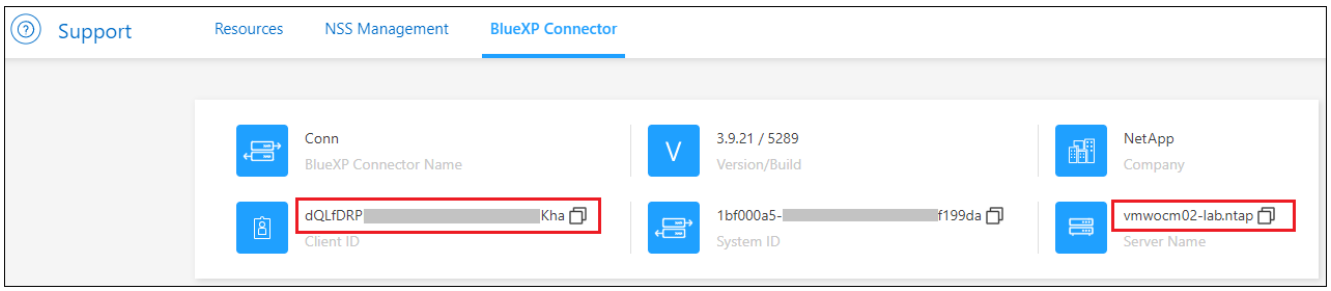
Étapes préalables

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.

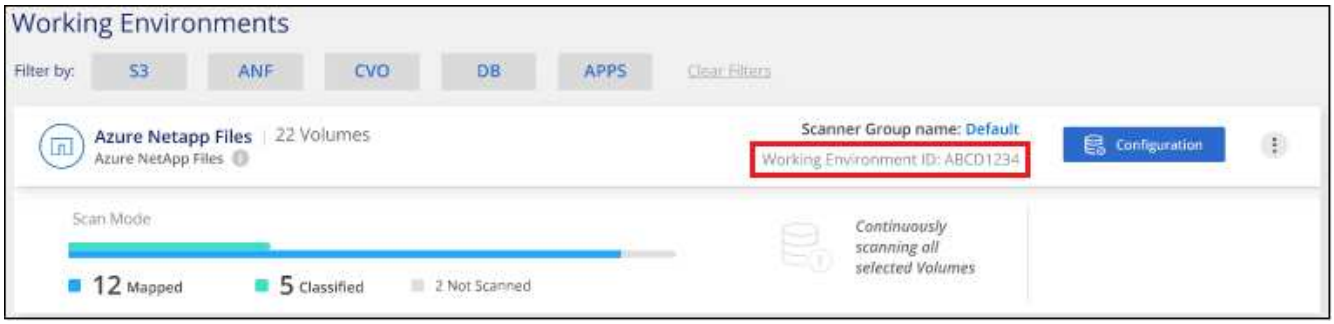
1. Dans la barre de menus BlueXP, cliquez sur **compte > gérer les comptes**.



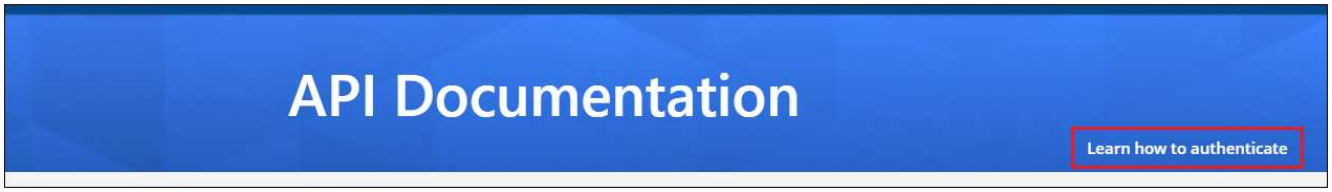
2. Copiez le *ID de compte*.
3. Dans la barre de menus BlueXP, cliquez sur **aide > support > connecteur BlueXP**.



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 (**DATASENNSE-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/Datase/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 "Configurez 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)

Port	Protocoles	Description
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 (**DATASENNSE-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 "Configurez 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.

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.

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.

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)	BlueXP détecte les clusters ONTAP via HTTPS. Si vous utilisez des stratégies de pare-feu personnalisées, elles doivent répondre aux exigences suivantes : • 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. • 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.
Cluster de détection des données <> ONTAP	• Pour NFS - 111 (TCP/UDP) et 2049 (TCP/UDP) • Pour CIFS - 139 (TCP/UDP) et 445 (TCP/UDP)	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. Assurez-vous que ces ports sont ouverts à l'instance de détection de données : • Pour NFS - 111 et 2049 • Pour CIFS : 139 et 445 Les règles d'exportation de volumes NFS doivent autoriser l'accès à partir de l'instance Data Sense.

Type de connexion	Ports	Description
Détection de données <> Active Directory	389 (TCP ET UDP), 636 (TCP), 3268 (TCP) ET 3269 (TCP)	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. Vous devez disposer des informations pour Active Directory : • Adresse IP du serveur DNS ou adresses IP multiples • Nom d'utilisateur et mot de passe du 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)

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.

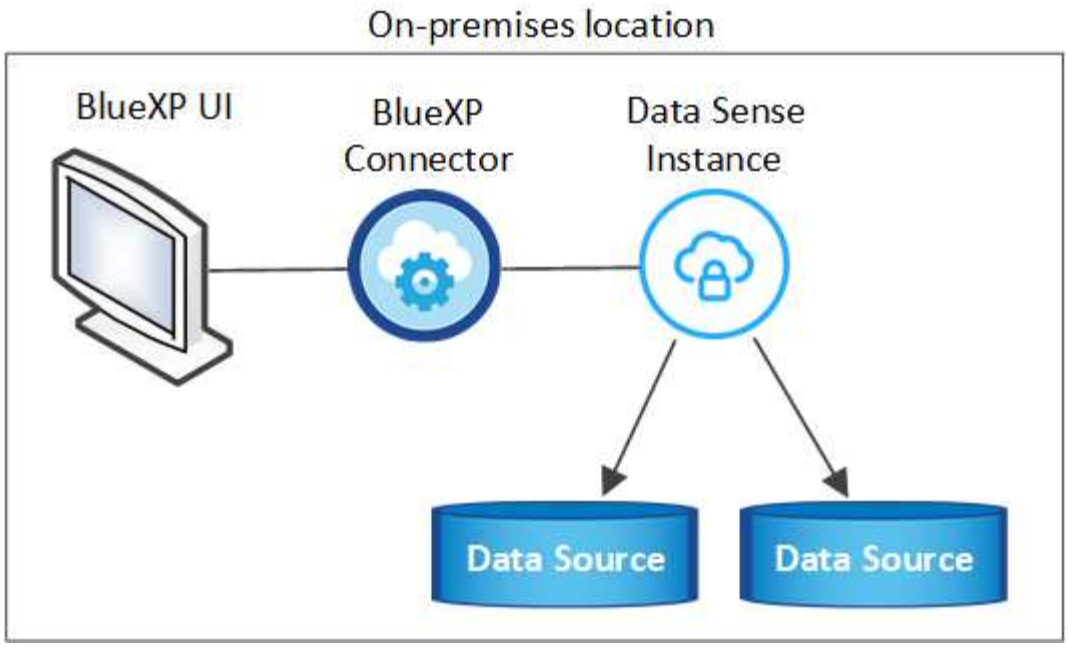
Les comptes sur site SharePoint installés localement peuvent être analysés sans accès à Internet.

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.

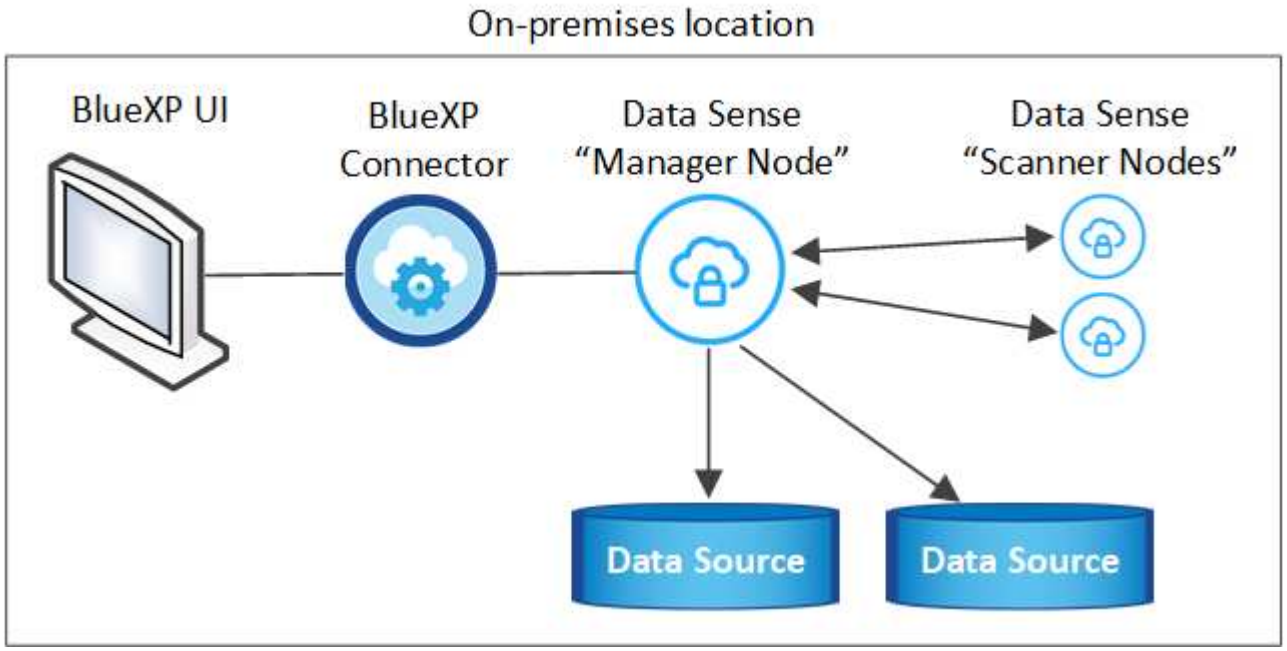
L'accès à *api.bluexp.netapp.com* n'est nécessaire que lors des connexions initiales à ces services externes.

Déployer un sens des données

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



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".



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.

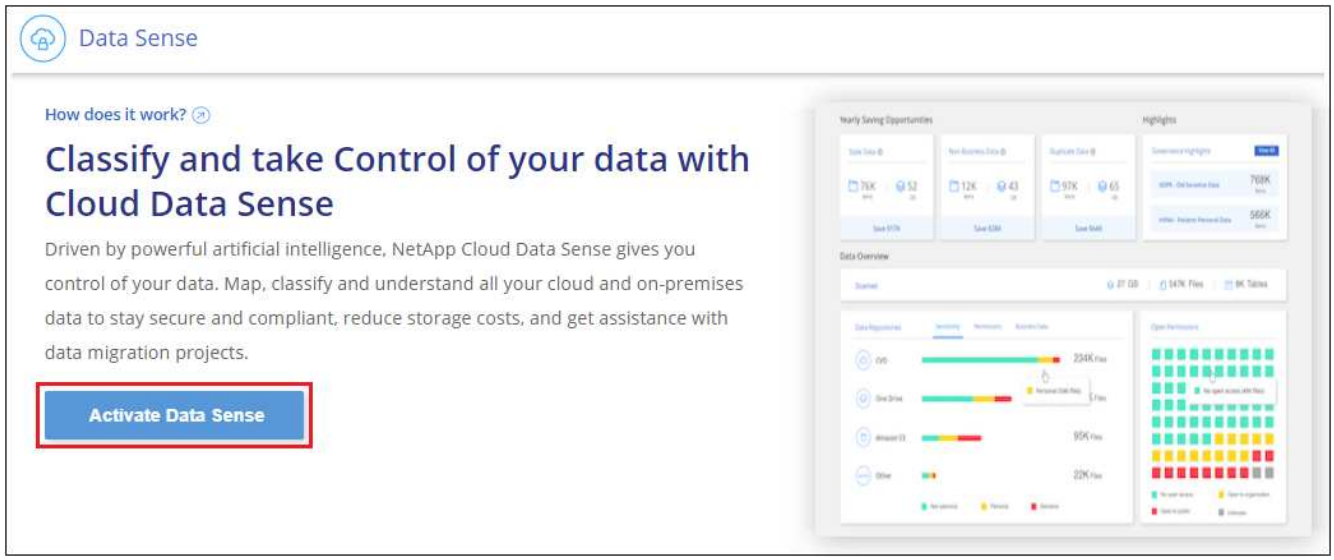
Étapes

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 :

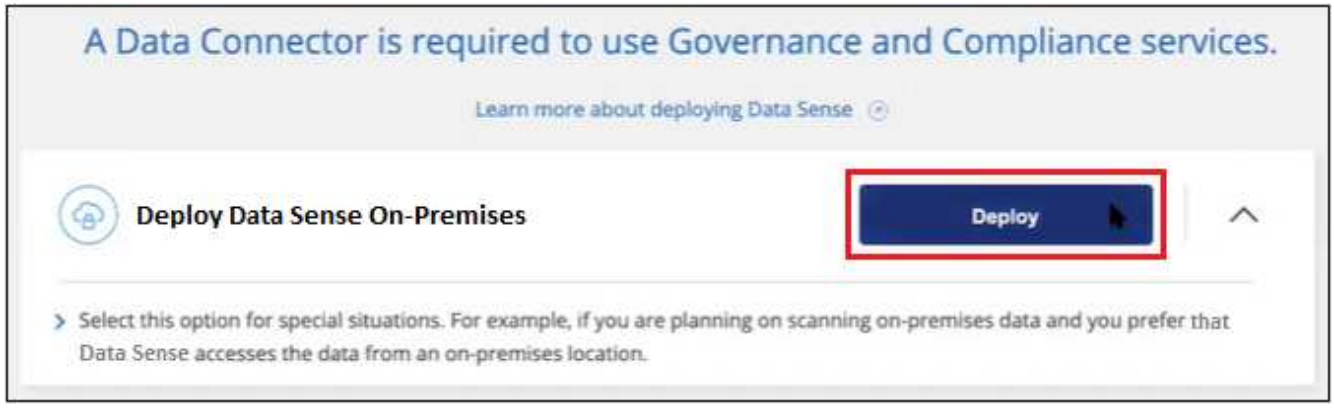
```
tar -xzf DataSense-offline-bundle-v1.16.1.tar.gz
```

   Ceci extrait le logiciel requis et le fichier d'installation réel **DATASENNSE-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 :
a. Coller les informations copiées à partir de l'étape 7 : `sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --darksite` 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. 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.	Vous pouvez également créer la commande entière à l'avance, en fournissant les paramètres d'hôte nécessaires : `sudo ./install.sh -a <account_id> -c <agent_id> -t <token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite`

   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 "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.

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** :
   a. Copiez le fichier d'installation de Data Sense (**DATASENSE-INSTALLER-<version>.tar.gz**) sur l'ordinateur hôte.
   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 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

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 logiciel sur l'hôte Linux où Data Sense est installé sur le site sombre.
3. 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 **DATASESNSE-INSTALLER-V1.16.1.tar.gz**.

4. 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.