



Déployez la classification BlueXP

BlueXP classification

NetApp
April 03, 2024

Sommaire

- Déployez la classification BlueXP 1
 - Quel déploiement de classification BlueXP devez-vous utiliser ? 1
 - Déployez la classification BlueXP dans le cloud à l'aide de BlueXP 1
 - Installez la classification BlueXP sur un hôte disposant d'un accès Internet 11
 - Installez la classification BlueXP sur un hôte Linux sans accès Internet 31
 - Vérifiez que votre hôte Linux est prêt à installer la classification BlueXP 43

Déployez la classification BlueXP

Quel déploiement de classification BlueXP devez-vous utiliser ?

Le classement BlueXP peut être déployé de différentes manières. Découvrez la méthode qui répond à vos besoins.

La classification BlueXP peut être déployée de plusieurs manières :

- ["Déployez dans le cloud à l'aide de BlueXP"](#). BlueXP déploie l'instance de classification BlueXP dans le même réseau de fournisseur cloud que le connecteur BlueXP.
- ["Installez sur un hôte Linux avec accès à Internet"](#). Installez la classification BlueXP sur un hôte Linux de votre réseau ou sur un hôte Linux dans le cloud disposant d'un accès Internet. Ce type d'installation peut être une bonne option si vous préférez analyser les systèmes ONTAP sur site à l'aide d'une instance de classification BlueXP également située sur site, mais ce n'est pas une exigence.
- ["Installation sur un hôte Linux dans un site sur site sans accès à Internet"](#). Également connu sous le nom de *private mode*. ce type d'installation, qui utilise un script d'installation, est bon pour vos sites sécurisés.

L'installation sur un hôte Linux avec accès à Internet et l'installation sur site sur un hôte Linux sans accès à Internet utilisent un script d'installation. Le script commence par vérifier si le système et l'environnement répondent aux conditions préalables. Si les conditions préalables sont remplies, l'installation démarre. Si vous souhaitez vérifier les prérequis indépendamment de l'installation de la classification BlueXP, vous pouvez télécharger un pack logiciel distinct qui teste uniquement les prérequis.

Reportez-vous à la section ["Vérifiez que votre hôte Linux est prêt à installer la classification BlueXP"](#).

Déployez la classification BlueXP dans le cloud à l'aide de BlueXP

Suivez ces étapes pour déployer la classification BlueXP dans le cloud. BlueXP déploie l'instance de classification BlueXP dans le même réseau de fournisseur cloud que le connecteur BlueXP.

Notez que vous pouvez également ["Installez la classification BlueXP sur un hôte Linux disposant d'un accès Internet"](#). Ce type d'installation peut être une bonne option si vous préférez analyser les systèmes ONTAP sur site à l'aide d'une instance de classification BlueXP 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 ["Installer le connecteur sur site"](#) Sur un hôte Linux de votre réseau ou sur un hôte Linux du cloud.

2

Passer en revue les prérequis

Assurez-vous que votre environnement est conforme aux conditions préalables. Notamment l'accès Internet sortant pour l'instance, la connectivité entre le connecteur et la classification BlueXP via le port 443, etc. [Voir la liste complète.](#)

3

Déployez la classification BlueXP

Lancez l'assistant d'installation pour déployer l'instance de classification BlueXP dans le cloud.

4

Abonnez-vous au service de classification BlueXP

Les 1 premiers To de données analysés par le système de classification BlueXP dans BlueXP sont gratuits pendant 30 jours. 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, un connecteur sera probablement configuré avant d'essayer d'activer la classification BlueXP, car la plupart ["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 :

- Lors de 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.
- Lorsque vous analysez des 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 ["Installer le connecteur sur site"](#) Sur un hôte Linux de votre réseau ou dans le cloud. Certains utilisateurs qui prévoient d'installer la classification BlueXP 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

La classification BlueXP est prise en charge lorsque le connecteur est déployé dans une région gouvernementale (AWS GovCloud, Azure Gov ou Azure DoD). Lorsqu'il est déployé de cette manière, la classification BlueXP 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).

["Voir plus d'informations sur le déploiement du connecteur dans une région gouvernementale"](#).

Passer en revue les prérequis

Vérifiez les conditions préalables suivantes afin de vous assurer que votre configuration est prise en charge avant de déployer la classification BlueXP dans le cloud. Lorsque vous déployez la classification BlueXP dans le cloud, elle se trouve dans le même sous-réseau que le connecteur.

Assurez un accès Internet sortant à partir de la classification BlueXP

La classification BlueXP nécessite un accès Internet sortant. Si votre réseau physique ou virtuel utilise un serveur proxy pour l'accès à Internet, assurez-vous que l'instance de classification BlueXP dispose d'un accès Internet sortant pour contacter les terminaux suivants. Le proxy doit être non transparent - nous ne prenons actuellement pas en charge les proxys transparents.

Consultez le tableau approprié ci-dessous selon que vous déployez ou non la classification BlueXP dans AWS, Azure ou GCP.

Terminaux requis pour 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.
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	Permet la classification BlueXP d'accéder aux manifestes et aux modèles, et de les télécharger, et d'envoyer des journaux et des metrics.

Terminaux requis pour Azure

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 requis pour 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.

Terminaux	Objectif
https://support.compliance.api.bluexp.netap p.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.netap p.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 des autorisations nécessaires pour déployer les ressources et créer des groupes de sécurité pour l'instance de classification BlueXP. Vous trouverez les dernières autorisations BlueXP dans ["Règles fournies par NetApp"](#).

Assurez-vous que le connecteur BlueXP peut accéder à la classification BlueXP

Assurez la connectivité entre le connecteur et l'instance de classification BlueXP. Le groupe de sécurité du connecteur doit autoriser le trafic entrant et sortant sur le port 443 vers et depuis l'instance de classification BlueXP. Cette connexion permet le déploiement de l'instance de classification BlueXP et vous permet d'afficher les informations des onglets conformité et gouvernance. La classification BlueXP est prise en charge dans les régions du gouvernement dans 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 pouvoir maintenir la classification BlueXP en cours d'exécution

L'instance de classification BlueXP doit continuer à analyser vos données en continu.

Assurez la connectivité du navigateur web à la classification BlueXP

Une fois la classification BlueXP activée, assurez-vous que les utilisateurs accèdent à l'interface BlueXP depuis un hôte qui dispose d'une connexion à l'instance de classification BlueXP.

L'instance de classification BlueXP 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 au sein du même réseau que l'instance de classification BlueXP.

Vérifiez les limites de vos CPU virtuels

Assurez-vous que la limite de CPU virtuels de votre fournisseur cloud permet le déploiement d'une instance avec le nombre de cœurs nécessaire. 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 la classification BlueXP sur une instance dans les environnements cloud AWS avec moins de processeurs et moins de RAM, mais que l'utilisation de ces systèmes est limitée. Voir ["Utilisation d'un type d'instance plus petit"](#) pour plus d'informations.

Déployez la classification BlueXP dans le cloud

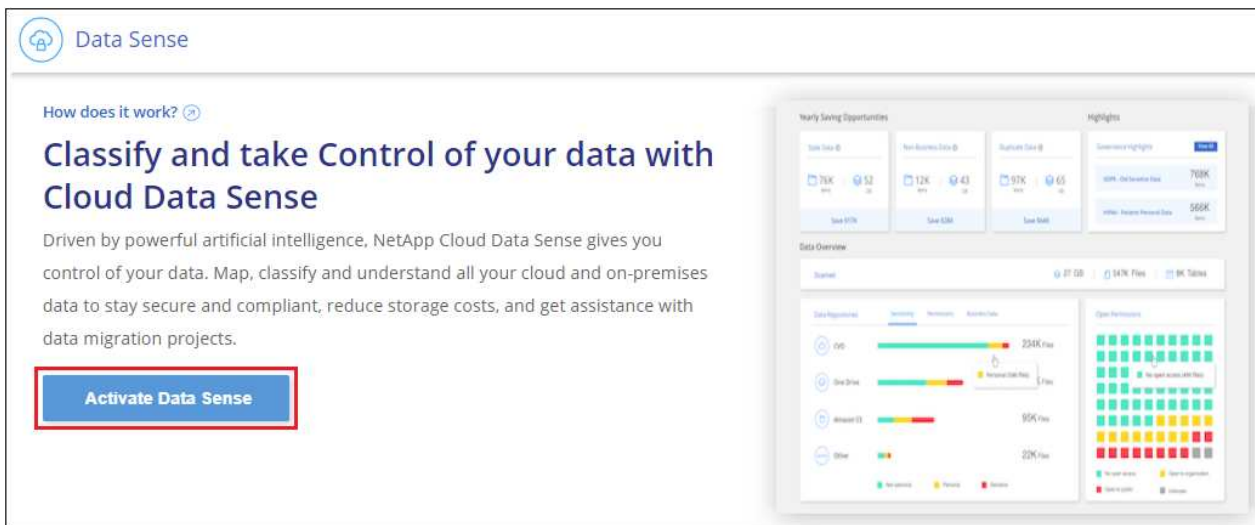
Suivez ces étapes pour déployer une instance de classification BlueXP dans le cloud. Le connecteur va déployer l'instance dans le cloud, puis installer le logiciel de classification BlueXP sur cette instance.

Notez que lors du déploiement de la classification BlueXP à partir d'un connecteur BlueXP dans un environnement AWS, vous pouvez sélectionner la taille d'instance par défaut ou choisir l'un des deux types d'instances les plus petits. ["Voir les types d'instances et les limites disponibles"](#). Dans les régions où le type d'instance par défaut n'est pas disponible, la classification BlueXP s'exécute sur un ["autre type d'instance"](#).

Déploiement dans AWS

Étapes

1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**.



2. Cliquez sur **Activer détection de données**.
3. Sur la page *installation*, cliquez sur **déployer > déployer** pour utiliser la taille d'instance « grande » et lancer l'assistant de déploiement cloud.
4. L'assistant affiche la progression au fur et à mesure des étapes de déploiement. Il s'arrête et vous invite à entrer s'il est en cours de problème.



5. Une fois l'instance déployée et la classification BlueXP installée, cliquez sur **Continuer à la configuration** pour accéder à la page *Configuration*.

Déploiement dans Azure

Étapes

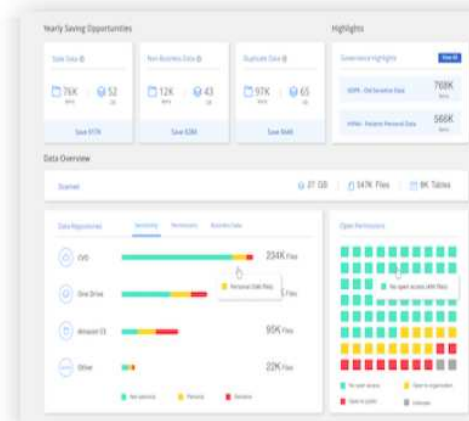
1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**.
2. Cliquez sur **Activer détection de données**.

How does it work? ⓘ

Classify and take Control of your data with Cloud Data Sense

Driven by powerful artificial intelligence, NetApp Cloud Data Sense gives you control of your data. Map, classify and understand all your cloud and on-premises data to stay secure and compliant, reduce storage costs, and get assistance with data migration projects.

Activate Data Sense



3. Cliquez sur **déployer** pour démarrer l'assistant de déploiement de cloud.

Install your Data Sense instance

Select your preferred deployment location:

[Learn more about deploying Data Sense ⓘ](#)

Cloud Environment

I want BlueXP to deploy the instance and install Data Sense

Deploy

- > BlueXP will deploy a new machine automatically in the chosen cloud environment.
- > You will be taken to an installation wizard where you can configure your Data Sense installation.

I deployed an instance and I'm ready to install Data Sense

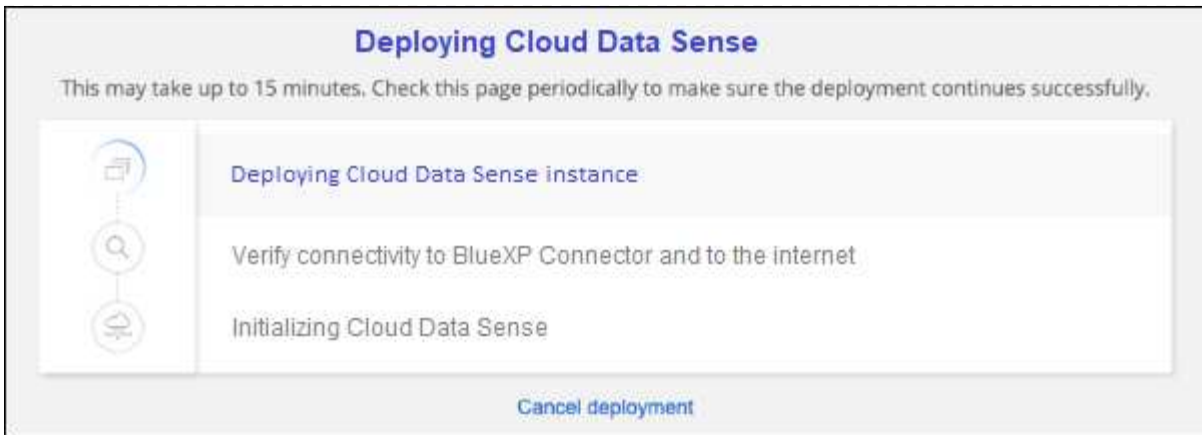
Deploy

On Premise

I prepared a local machine and I'm ready to install Data Sense

Deploy

4. L'assistant affiche la progression au fur et à mesure des étapes de déploiement. Il s'arrête et vous invite à entrer s'il est en cours de problème.

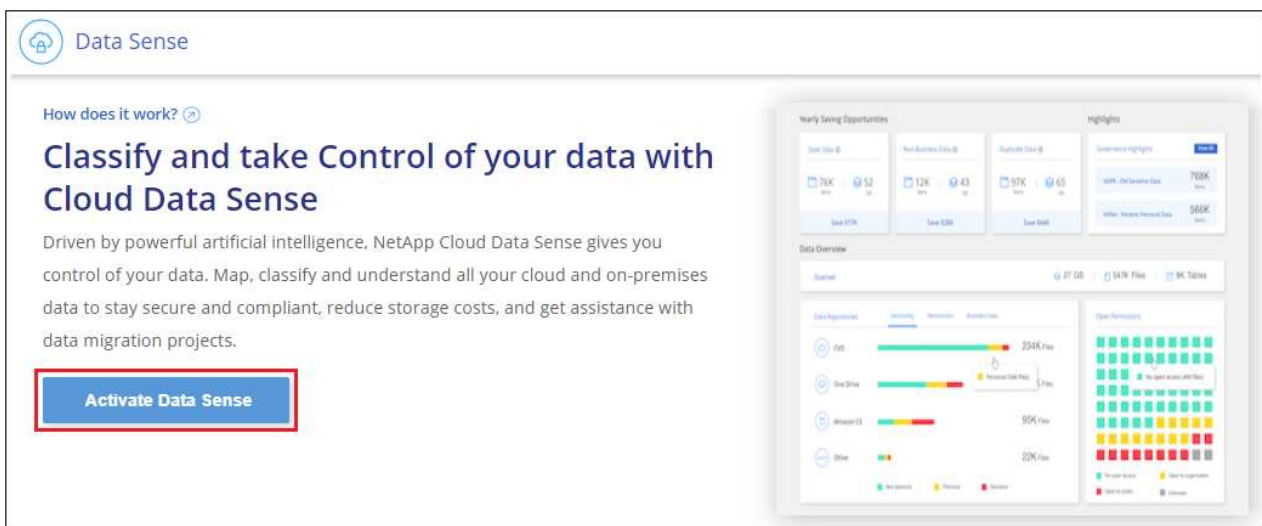


5. Une fois l'instance déployée et la classification BlueXP installée, cliquez sur **Continuer à la configuration** pour accéder à la page *Configuration*.

Déploiement dans Google 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 **déployer** pour démarrer l'assistant de déploiement de cloud.

Install your Data Sense instance

Select your preferred deployment location:

[Learn more about deploying Data Sense](#) 

Cloud Environment




I want BlueXP to deploy the instance and install Data Sense

Deploy

^

> BlueXP will deploy a new machine automatically in the chosen cloud environment.

> You will be taken to an installation wizard where you can configure your Data Sense installation.




I deployed an instance and I'm ready to install Data Sense

Deploy

v

On Premise



I prepared a local machine and I'm ready to install Data Sense

Deploy

v

4. L'assistant affiche la progression au fur et à mesure des étapes de déploiement. Il s'arrête et vous invite à entrer s'il est en cours de problème.

Deploying Cloud Data Sense

This may take up to 15 minutes. Check this page periodically to make sure the deployment continues successfully.



Deploying Cloud Data Sense instance

Verify connectivity to BlueXP Connector and to the internet

Initializing Cloud Data Sense

[Cancel deployment](#)

5. Une fois l'instance déployée et la classification BlueXP installée, cliquez sur **Continuer à la configuration** pour accéder à la page *Configuration*.

Résultat

BlueXP déploie l'instance de classification BlueXP dans votre fournisseur cloud.

Les mises à niveau vers le connecteur BlueXP et le logiciel de classification BlueXP sont automatisées tant que les instances disposent d'une connectivité Internet.

Et la suite

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

Vous pouvez également ["Configurez les licences pour la classification BlueXP"](#) à ce moment-là. Vous ne serez facturé que lorsque votre essai gratuit de 30 jours se terminera.

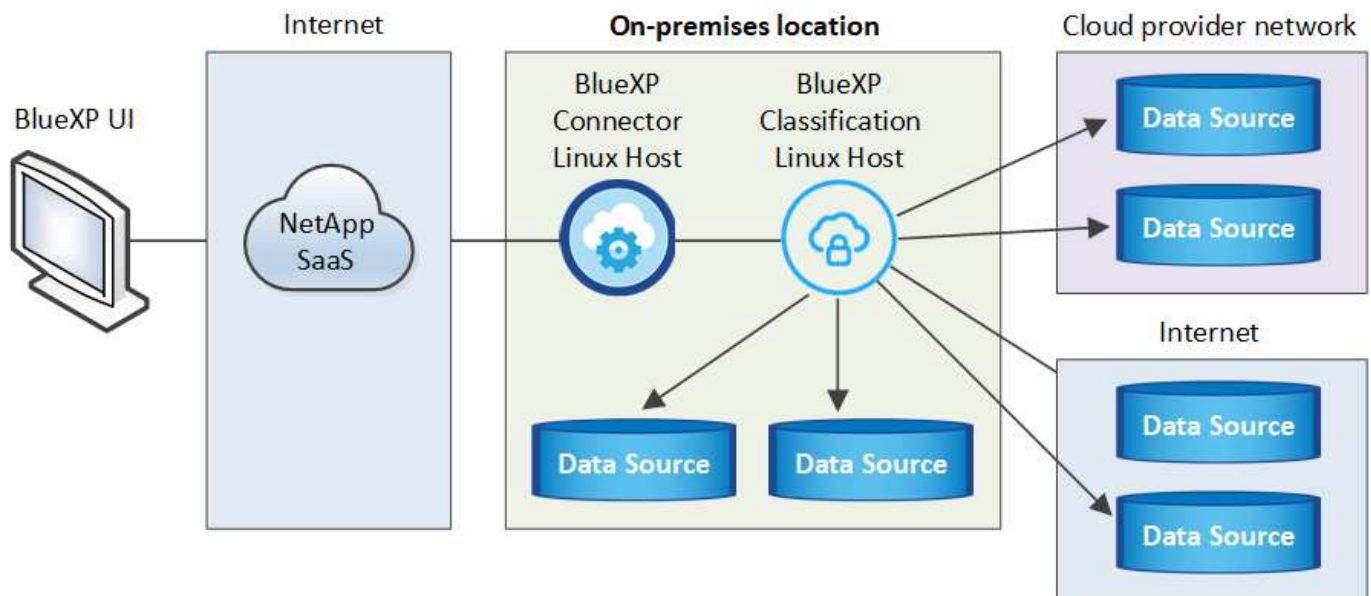
Installez la classification BlueXP sur un hôte disposant d'un accès Internet

Procédez en quelques étapes pour installer la classification BlueXP sur un hôte Linux de votre réseau ou sur un hôte Linux dans le cloud disposant d'un accès Internet. Dans le cadre de cette installation, vous devrez déployer l'hôte Linux manuellement sur votre réseau ou dans le cloud.

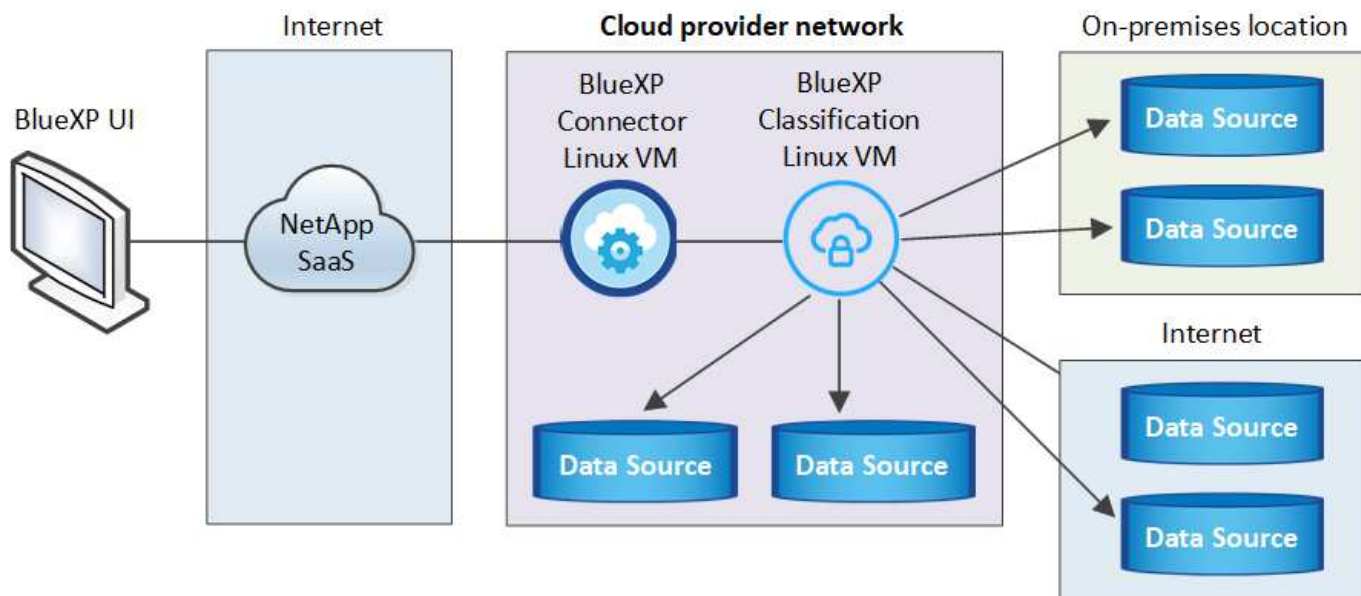
L'installation sur site peut être une bonne option si vous préférez analyser les systèmes ONTAP sur site à l'aide d'une instance de classification BlueXP également située sur site, mais ce n'est pas une exigence. Le logiciel fonctionne exactement de la même manière quelle que soit la méthode d'installation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

Le script d'installation de la classification BlueXP commence par vérifier si le système et l'environnement répondent aux prérequis requis. Si les conditions préalables sont toutes remplies, l'installation démarre. Si vous souhaitez vérifier les prérequis indépendamment de l'installation de la classification BlueXP, vous pouvez télécharger un pack logiciel distinct qui teste uniquement les prérequis. ["Découvrez comment vérifier si votre hôte Linux est prêt à installer la classification BlueXP"](#).

L'installation typique sur un hôte Linux *dans vos locaux* comporte les composants et les connexions suivants.



L'installation typique sur un hôte Linux *dans le cloud* comporte 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. 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*.

Notez que vous pouvez également "[Installer la classification BlueXP sur un 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 sur un hôte Linux 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. Notamment l'accès Internet sortant pour l'instance, la connectivité entre le connecteur et la classification BlueXP via 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 la classification BlueXP

Téléchargez le logiciel de classification Cloud BlueXP depuis le site de support NetApp et copiez le fichier d'installation sur l'hôte Linux que vous souhaitez utiliser. Lancez ensuite l'assistant d'installation et suivez les

invites pour déployer l'instance de classification BlueXP.



Abonnez-vous au service de classification BlueXP

Les 1 premiers To de données analysés par le système de classification BlueXP dans BlueXP sont gratuits pendant 30 jours. 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 requis avant de pouvoir installer et utiliser la classification BlueXP. Dans la plupart des cas, vous aurez probablement configuré un connecteur avant d'essayer d'activer la classification BlueXP, car la plupart ["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 :

- Lors de 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.
- Lorsque vous analysez des 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 sur un hôte Linux du cloud. Certains utilisateurs qui prévoient d'installer la classification BlueXP 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 pour installer la classification BlueXP. 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 classification BlueXP doit s'exécuter sur un hôte répondant à des exigences spécifiques en termes de système d'exploitation, de RAM, de logiciels, etc. L'hôte Linux peut se trouver sur votre réseau ou dans le cloud.

Assurez-vous de pouvoir maintenir la classification BlueXP en cours d'exécution. La machine de classification

BlueXP doit continuer à analyser vos données en continu.

- La classification BlueXP n'est pas prise en charge sur un hôte partagé avec d'autres applications : l'hôte doit être un hôte dédié.
- Lors de la création du système hôte sur site, vous pouvez choisir entre trois tailles de système selon la taille du dataset que vous prévoyez d'analyser par la classification BlueXP.

Taille du système	CPU	RAM (la mémoire d'échange doit être désactivée)	Disque
Très grand	32 processeurs	128 GO DE RAM	1 To SSD sur /, ou - 100 Gio disponible sur /opt - 895 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp
Grand	16 processeurs	64 GO DE RAM	500 Gio de SSD sur /, ou - 100 Gio disponible sur /opt - 395 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp
Moyen	8 processeurs	32 GO DE RAM	200 Gio de SSD sur /, ou - 50 Gio disponible sur /opt - 145 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp
Petit	8 processeurs	16 GO DE RAM	100 Gio de SSD sur /, ou - 50 Gio disponible sur /opt - 45 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp

Notez qu'il existe des limites lors de l'utilisation des systèmes plus petits. Voir ["Utilisation d'un type d'instance plus petit"](#) pour plus d'informations.

- Lors du déploiement d'une instance de calcul dans le cloud pour votre installation de classification BlueXP, nous vous recommandons de opter pour un système qui répond à la configuration requise pour les « grands » systèmes ci-dessus :
 - **Type d'instance AWS EC2**: Nous recommandons "m6i.4xlarge". ["Consultez la section autres types d'instances AWS"](#).
 - **Taille de VM Azure**: Nous recommandons "Standard_D16s_v3". ["Consultez la section autres types d'instances Azure"](#).
 - **Type de machine GCP**: Nous recommandons "n2-standard-16". ["Voir autres types d'instances GCP"](#).
- **Autorisations de dossier UNIX** : les autorisations UNIX minimales suivantes sont requises :

Dossier	Autorisations minimales
/tmp	rwxrwxrwt
/opt	rwxr-xr-x
/var/lib/docker	rwx-----

Dossier	Autorisations minimales
/usr/lib/systemd/system	rwxr-xr-x

- **Système d'exploitation :**

- Les systèmes d'exploitation suivants nécessitent l'utilisation du moteur de mise en conteneurs Docker :
 - Red Hat Enterprise Linux version 7.8 et 7.9
 - CentOS versions 7.8 et 7.9
 - Ubuntu 22.04 (requiert la classification BlueXP version 1.23 ou supérieure)
- Les systèmes d'exploitation suivants nécessitent l'utilisation du moteur de conteneur Podman et requièrent la classification BlueXP version 1.30 ou supérieure :
 - Red Hat Enterprise Linux version 8.8, 9.0, 9.1, 9.2 et 9.3

Notez que les fonctionnalités suivantes ne sont actuellement pas prises en charge lors de l'utilisation de RHEL 8.x et RHEL 9.x :

- Installation dans un site sombre
- Numérisation distribuée ; utilisation d'un nœud de scanner maître et de nœuds de scanner distants

- **Gestion des abonnements Red Hat :** l'hôte 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 pendant l'installation.

- **Logiciels supplémentaires :** vous devez installer les logiciels suivants sur l'hôte avant d'installer la classification BlueXP :

- En fonction du système d'exploitation que vous utilisez, vous devrez installer l'un des moteurs de mise en conteneurs :

- Docker Engine version 19.3.1 ou supérieure. ["Voir les instructions d'installation"](#).

["Regardez cette vidéo"](#) Pour une démonstration rapide de l'installation de Docker sur CentOS.

- Podman version 4 ou supérieure. Pour installer Podman, mettez à jour vos packages système (`sudo yum update -y`), puis installez Podman (`sudo yum install netavark -y`).

- Python version 3.6 ou supérieure. ["Voir les instructions d'installation"](#).

- **Considérations NTP :** NetApp recommande de configurer le système de classification BlueXP pour utiliser un service NTP (Network Time Protocol). L'heure doit être synchronisée entre le système de classification BlueXP et le système BlueXP Connector.
- **Firesund considérations:** Si vous prévoyez d'utiliser `firewalld`, Nous vous recommandons de l'activer avant d'installer la classification BlueXP. Exécutez les commandes suivantes pour configurer `firewalld` Pour qu'il soit compatible avec la classification BlueXP :

```
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 des hôtes de classification BlueXP supplémentaires comme nœuds d'analyse, ajoutez ces règles à votre système principal à ce moment :

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

+

Notez que vous devez redémarrer Docker ou Podman chaque fois que vous activez ou mettez à jour `firewalld` paramètres.



L'adresse IP du système hôte de classification BlueXP ne peut pas être modifiée après l'installation.

Assurez un accès Internet sortant à partir de la classification BlueXP

La classification BlueXP nécessite un accès Internet sortant. Si votre réseau physique ou virtuel utilise un serveur proxy pour l'accès à Internet, assurez-vous que l'instance de classification BlueXP dispose d'un accès Internet sortant pour contacter les terminaux 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.
https://github.com/docker https://download.docker.com	Fournit les packages prérequis pour l'installation de docker.

Terminaux	Objectif
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 des packages prérequis pour l'installation de CentOS.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Fournit les packages prérequis pour l'installation d'Ubuntu.

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, la classification BlueXP, Active Directory et vos sources de données.

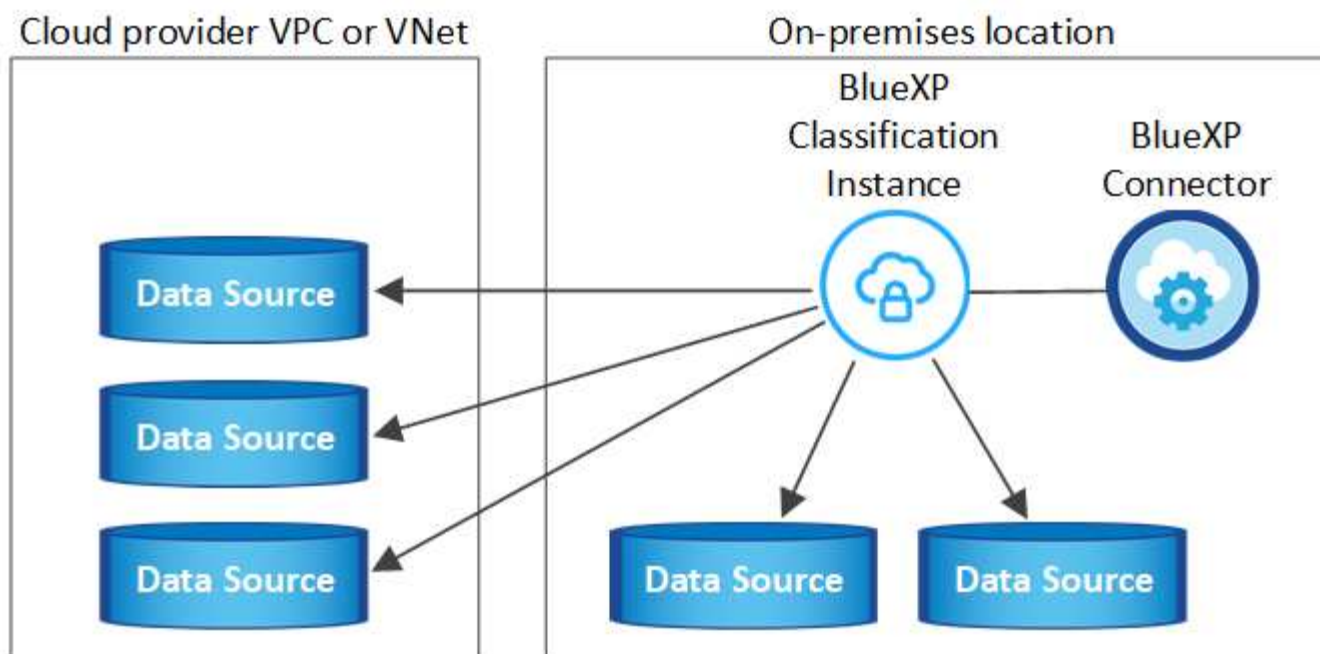
Type de connexion	Ports	Description
Classification de Connector <> BlueXP	8080 (TCP), 443 (TCP) et 80	Les règles de pare-feu ou de routage du connecteur doivent autoriser le trafic entrant et sortant via le port 443 vers et depuis l'instance de classification BlueXP. Assurez-vous que le port 8080 est 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"> • 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 pare-feu ou les règles de routage prédéfinies. • 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.

Type de connexion	Ports	Description
Classification BlueXP <> cluster ONTAP	<ul style="list-style-type: none"> • Pour NFS - 111 (TCP/UDP) et 2049 (TCP/UDP) • Pour CIFS - 139 (TCP/UDP) et 445 (TCP/UDP) 	<p>La classification BlueXP nécessite une connexion réseau à chaque sous-réseau Cloud Volumes ONTAP ou système ONTAP sur site. Les pare-feu ou les règles de routage pour Cloud Volumes ONTAP doivent autoriser les connexions entrantes à partir de l'instance de classification BlueXP.</p> <p>Assurez-vous que les ports suivants sont ouverts pour l'instance de classification BlueXP :</p> <ul style="list-style-type: none"> • Pour NFS - 111 et 2049 • Pour CIFS : 139 et 445 <p>Les règles d'exportation des volumes NFS doivent autoriser l'accès à partir de l'instance de classification BlueXP.</p>
Classification BlueXP <> 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. De plus, la classification BlueXP requiert des informations d'identification Active Directory pour analyser les volumes CIFS.</p> <p>Vous devez disposer des informations pour Active Directory :</p> <ul style="list-style-type: none"> • 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)

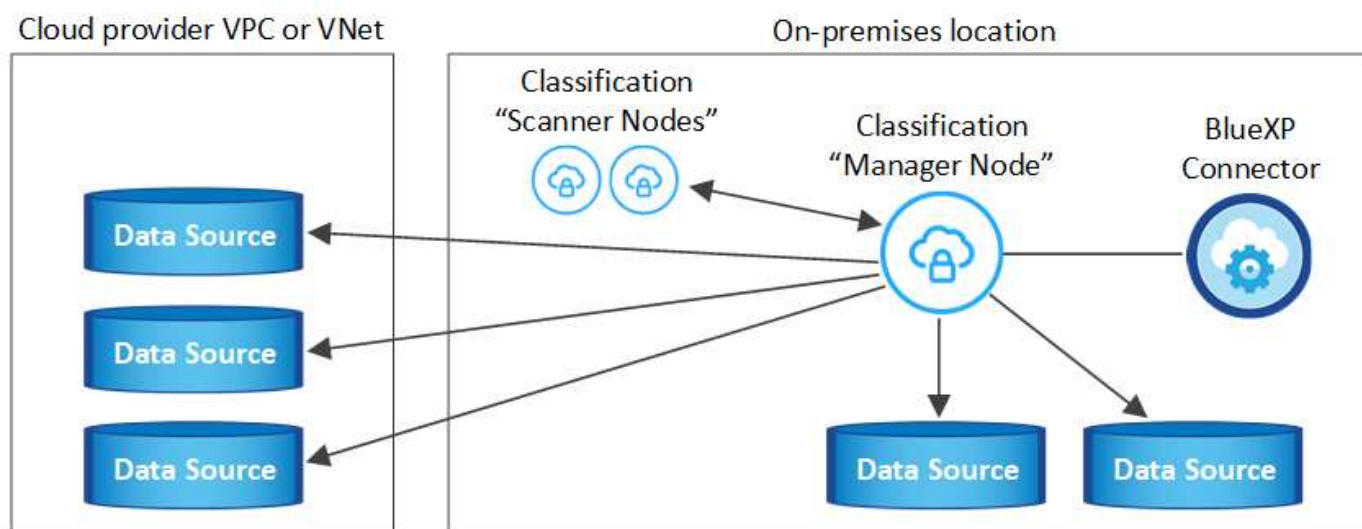
Si vous utilisez plusieurs hôtes de classification BlueXP pour augmenter la puissance de traitement afin d'analyser vos sources de données, vous devez activer des ports/protocoles supplémentaires. ["Voir la configuration de port supplémentaire requise"](#).

Installez la classification BlueXP sur l'hôte Linux

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](#) Liste complète des exigences avant de déployer la classification BlueXP.

Les mises à niveau du logiciel de classification BlueXP sont automatisées tant que l'instance dispose d'une connectivité Internet.



La classification BlueXP est actuellement incapable d'analyser les compartiments S3, Azure NetApp Files ou FSX pour ONTAP lorsque le logiciel est installé sur site. Dans ce cas, vous devrez déployer un connecteur et une instance séparés de la classification BlueXP dans le cloud et "[Basculer entre les connecteurs](#)" pour les différentes sources de données.

Installation à un seul hôte pour les configurations courantes

Étudiez la configuration requise et suivez les étapes ci-dessous lors de l'installation du logiciel de classification BlueXP sur un hôte sur site unique.

["Regardez cette vidéo"](#) Pour voir comment installer la classification BlueXP.

Notez que toutes les activités d'installation sont consignées lors de l'installation de la classification BlueXP. Si vous rencontrez des problèmes lors de l'installation, vous pouvez afficher le contenu du journal d'audit d'installation. Il est écrit dans `/opt/netapp/install_logs/`. ["Pour en savoir plus, cliquez ici"](#).

Ce dont vous avez besoin

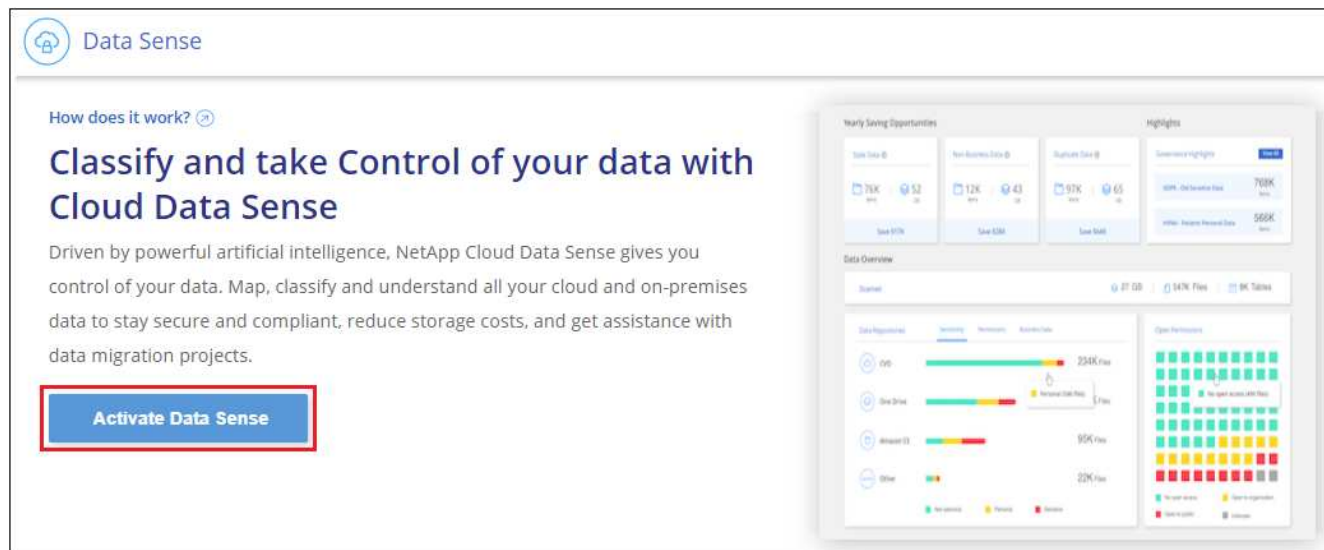
- Vérifiez que votre système Linux est conforme à la [configuration requise pour l'hôte](#).
- Vérifiez que le système dispose des deux packages logiciels prérequis installés (Docker Engine ou Podman et Python 3).
- Assurez-vous que vous disposez des privilèges root sur le système Linux.
- Si vous utilisez un proxy pour accéder à Internet :
 - Vous aurez besoin des informations du serveur proxy (adresse IP ou nom d'hôte, port de connexion, schéma de connexion : https ou http, nom d'utilisateur et mot de passe).
 - Si le proxy effectue l'interception TLS, vous devez connaître le chemin d'accès au système de classification BlueXP Linux où sont stockés les certificats TLS CA.
 - Le proxy doit être non transparent - nous ne prenons actuellement pas en charge les proxys transparents.
 - L'utilisateur doit être un utilisateur local. Les utilisateurs du domaine ne sont pas pris en charge.
- Vérifiez que votre environnement hors ligne répond aux besoins [autorisations et connectivité](#).

Étapes

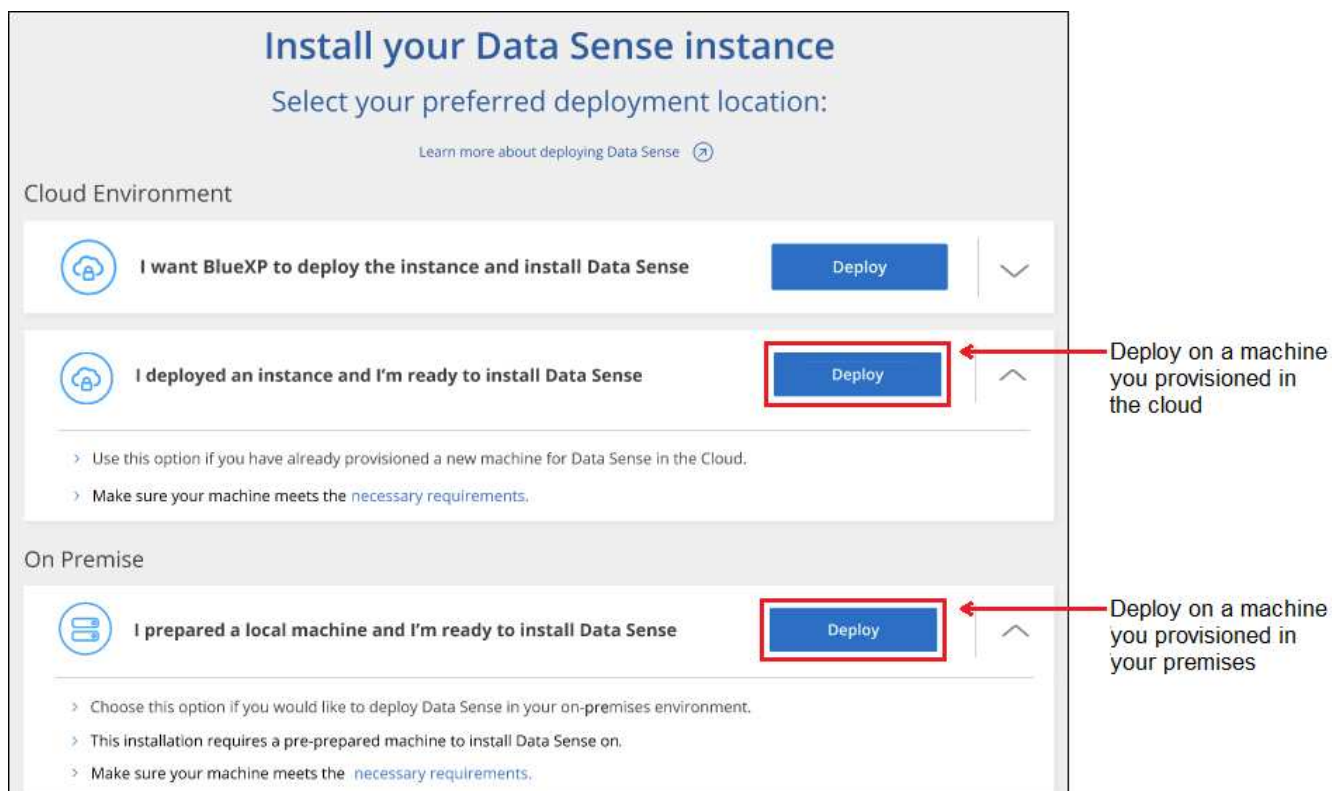
1. Téléchargez le logiciel de classification BlueXP depuis le ["Site de support NetApp"](#). Le fichier que vous devez sélectionner est nommé **DATASENSE-INSTALLER-<version>.tar.gz**.
2. Copiez le fichier d'installation sur l'hôte Linux que vous envisagez d'utiliser (à l'aide de `scp` ou une autre méthode).
3. Décompressez le fichier d'installation sur la machine hôte, par exemple :

```
tar -xzf DATASENSE-INSTALLER-V1.25.0.tar.gz
```

4. Dans BlueXP, sélectionnez **gouvernance > Classification**.
5. Cliquez sur **Activer détection de données**.



6. Selon que vous installez la classification BlueXP sur une instance préparée dans le cloud ou sur une instance préparée dans votre environnement sur site, cliquez sur le bouton **Deploy** approprié pour démarrer l'installation de la classification BlueXP.



7. La boîte de dialogue *Deploy Data Sense on local* s'affiche. Copiez la commande fournie (par exemple : `sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq`) et collez-le dans un fichier texte pour pouvoir l'utiliser ultérieurement. Cliquez ensuite sur **Fermer** pour fermer la boîte de dialogue.
8. Sur la machine hôte, entrez la commande que vous avez copiée, puis suivez une série d'invites, ou vous pouvez fournir la commande complète incluant tous les paramètres requis comme arguments de ligne de commande.

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. "[Regardez cette vidéo](#)" pour comprendre les

messages de pré-vérification et les implications.

Entrez les paramètres comme demandé :	Saisissez la commande complète :
<p>a. Collez la commande que vous avez copiée à partir de l'étape 7 :</p> <pre>sudo ./install.sh -a <account_id> -c <client_id> -t <user_token></pre> <p>Si vous installez sur une instance cloud (pas sur site), ajoutez <code>--manual-cloud-install <cloud_provider></code>.</p> <p>b. Entrez l'adresse IP ou le nom d'hôte de la machine hôte de classification BlueXP afin qu'elle soit accessible par le système de connecteurs.</p> <p>c. Entrez l'adresse IP ou le nom d'hôte de la machine hôte du connecteur BlueXP afin que le système de classification BlueXP puisse y accéder.</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 la classification BlueXP 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 <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --manual-cloud-install <cloud_provider> --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></pre>

Valeurs variables :

- *Account_ID* = ID du compte NetApp
- *Client_ID* = connecteur client ID (ajoutez le suffixe "clients" à l'ID client s'il n'y en a pas déjà)
- *User_token* = jeton d'accès utilisateur JWT
- *Ds_host* = adresse IP ou nom d'hôte du système de classification BlueXP Linux.
- *Cm_host* = adresse IP ou nom d'hôte du système de connecteurs BlueXP.
- *Cloud_Provider* = lors de l'installation sur une instance cloud, entrez « AWS », « Azure » ou « GCP » en fonction du fournisseur de cloud.
- *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. L'utilisateur doit être un utilisateur local - les utilisateurs de domaine ne sont pas pris en charge.
- *Proxy_password* = Mot de passe pour le nom d'utilisateur que vous avez spécifié.
- *Ca_cert_dir* = chemin du système de classification BlueXP Linux contenant des bundles de certificats TLS CA supplémentaires. Requis uniquement si le proxy effectue une interception TLS.

Résultat

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

En cas de connectivité sur le port 8080 entre la machine hôte et l'instance de connecteur, vous verrez la progression de l'installation dans l'onglet de classification BlueXP.

Et la suite

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

Vous pouvez également "[Configurer les licences pour la classification BlueXP](#)" à ce moment-là. Vous ne serez facturé que lorsque votre essai gratuit de 30 jours se terminera.

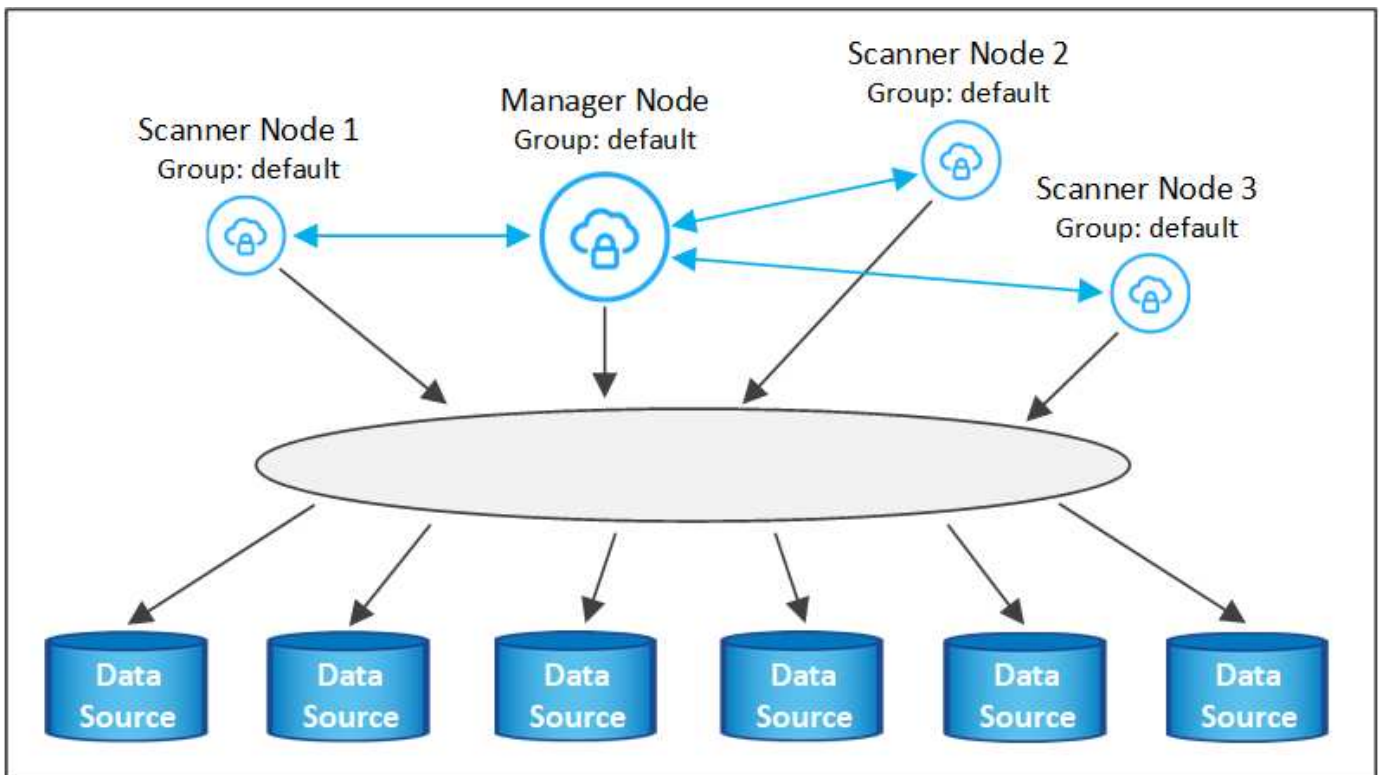
Ajoutez des nœuds de scanner à un déploiement existant

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 :

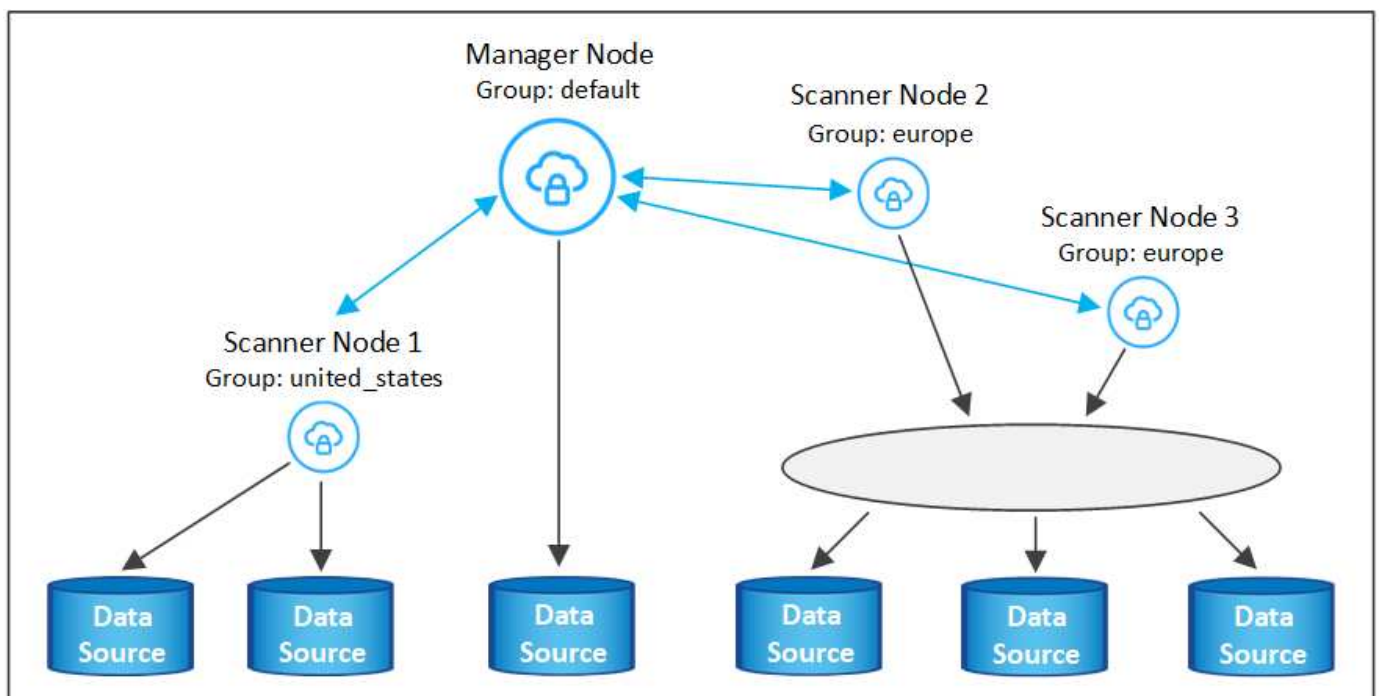
- ajoutez un nœud pour faciliter la numérisation de toutes les sources de données
- ajout d'un nœud pour faciliter l'analyse d'une source de données spécifique ou d'un groupe spécifique de sources de données (généralement basé sur l'emplacement)

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 d'analyse de classification BlueXP peuvent être définis comme des zones géographiques distinctes où vos données sont stockées. Vous pouvez déployer plusieurs nœuds d'analyse de classification BlueXP à travers le monde 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 la classification BlueXP et choisir leur nom. La classification BlueXP n'applique pas qu'un nœud mappé à un groupe de scanner nommé « europe » soit déployé en Europe.

Pour installer d'autres nœuds d'analyse de classification BlueXP, procédez comme suit :

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](#).
- Vérifier que les deux logiciels prérequis sont installés sur les systèmes (Docker Engine ou Podman et Python 3).
- 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 BlueXP classification 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 **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)

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)

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

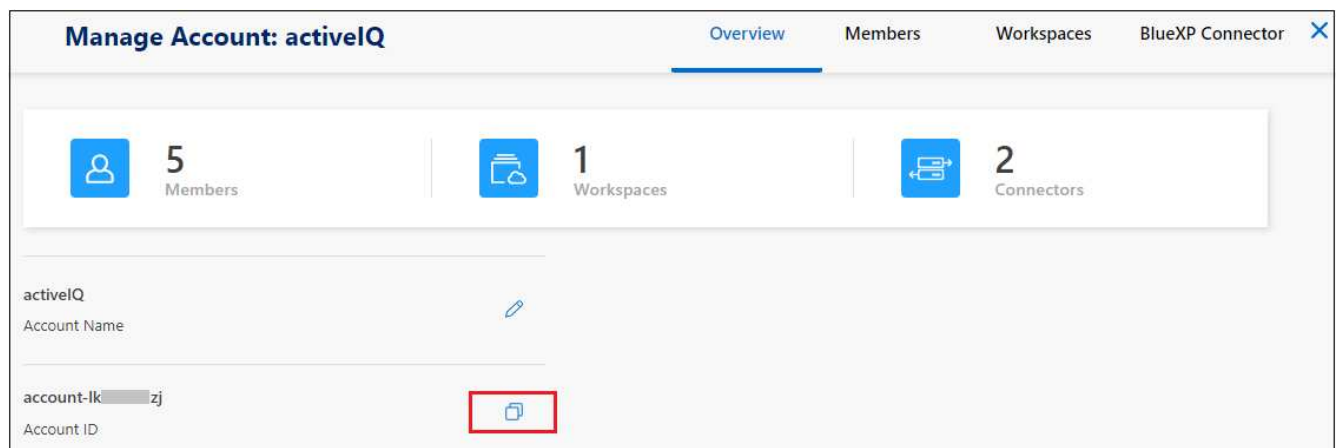
```
firewall-cmd --permanent --add-service=http
firewall-cmd --permanent --add-service=https
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=443/tcp
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
firewall-cmd --reload
```

Notez que vous devez redémarrer Docker ou Podman chaque fois que vous activez ou mettez à jour `firewalld` paramètres.

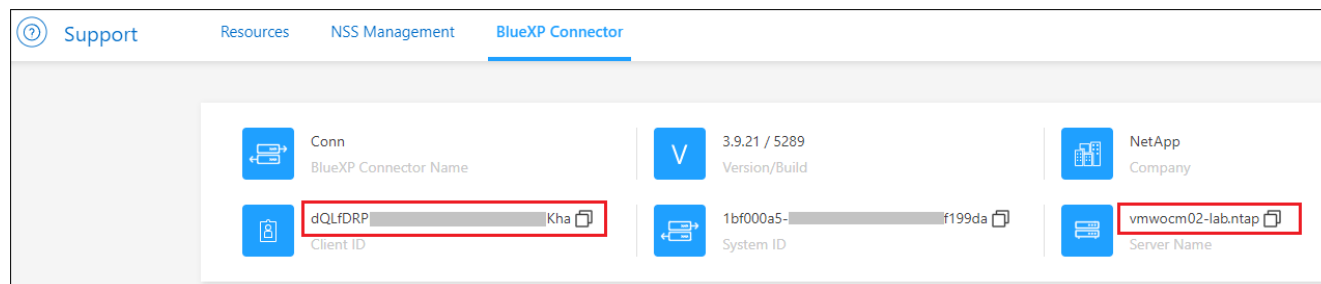
Étapes préalables

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.

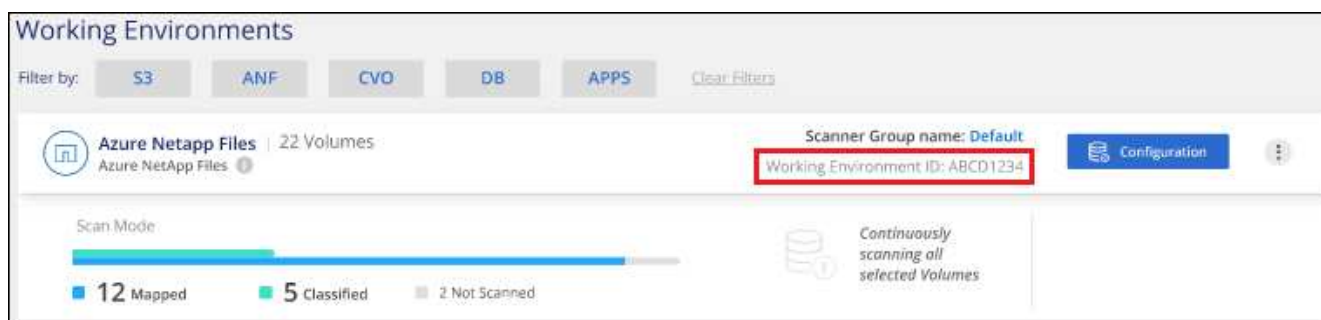
1. Dans la barre de menus BlueXP, cliquez sur **compte > gérer les comptes**.



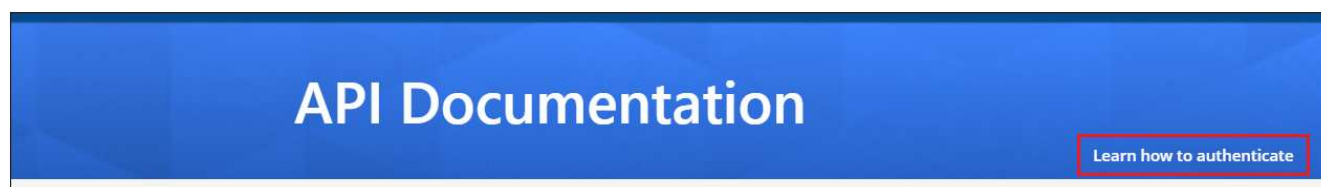
2. Copiez le *ID de compte*.
3. Dans la barre de menus BlueXP, cliquez sur **aide > support > connecteur BlueXP**.



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 classification BlueXP, copiez l'ID d'environnement de travail de chaque environnement de travail que vous prévoyez 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, en utilisant le nom d'utilisateur et le mot de passe de l'administrateur du compte dans les paramètres "nom d'utilisateur" et "mot de passe".
8. Copiez ensuite le *jeton d'accès* de la réponse.

Étapes

1. Sur le nœud du gestionnaire de classification BlueXP, 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* = connecteur client ID (ajoutez le suffixe "clients" à l'ID client que vous avez copié dans les étapes préalables)
- *Cm_host* = adresse IP ou nom d'hôte du système de connecteurs
- *Ds_Manager_ip* = adresse IP privée du système de nœuds BlueXP classification Manager

- *Node_private_ip* = adresses IP des systèmes de nœuds du scanner de classification BlueXP (les adresses IP de plusieurs nœuds 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 (par exemple : `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j`) et enregistrez-le dans un fichier texte.
 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/config/custom_configuration/working_Environment_to_scanner_group_config.yml` » et entrez le mappage pour lequel les groupes de scanner 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 au groupe de scanner « `europe` » et 2 au groupe de scanner « `united_States` » :

```
scanner_groups:
  europe:
    working_environments:
      - "working_environment_id1"
      - "working_environment_id2"
  united_states:
    working_environments:
      - "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

La classification BlueXP est configurée avec des 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.

The screenshot shows the 'Working Environments' section. At the top, there are filter buttons for 'S3', 'ANF', 'CVO', 'DB', and 'APPS', along with a 'Clear Filters' link. Below this, a card for 'Azure Netapp Files' is displayed, showing '22 Volumes'. A 'Scanner Group name: Default' is indicated, and a 'Working Environment ID: ABCD1234' is highlighted with a red box. A 'Configuration' button is visible. A progress bar for 'Scan Mode' shows '12 Mapped' (blue), '5 Classified' (green), and '2 Not Scanned' (grey). A note states 'Continuously scanning all selected Volumes'.

Vous pouvez également afficher la liste de tous les groupes de scanner, ainsi que l'adresse IP et l'état de chaque nœud de scanner du groupe, en bas de la page Configuration.

The screenshot shows the 'Scanner Groups' page. At the top, there is a search bar. Below it, three scanner groups are listed: 'Scanner Group: Default', 'Scanner Group: United_States', and 'Scanner Group: Europe'. Each group has a 'Scanner nodes' link with a green checkmark icon. The 'Default' and 'United_States' groups each show '2 Scanner nodes'. Below each group, a table lists the scanner nodes with columns: 'Scanner node host name', 'IP', 'Last active time', 'Status', and 'Error'. The 'Status' column shows 'Active' for all nodes. The 'Europe' group is partially visible at the bottom.

Scanner node host name	IP	Last active time	Status	Error
ip-172-...us-west-2.compute	172-...	23/09/2022 14:32	Active	
ip-172-...us-west-2.compute	172-...	23/09/2022 14:32	Active	

C'est possible "[Configurez les licences pour la classification BlueXP](#)" à ce moment-là. Vous ne serez facturé que lorsque votre essai gratuit de 30 jours se terminera.

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*.

Suivez ces étapes lors de l'installation simultanée du logiciel de classification BlueXP sur plusieurs hôtes sur site. Notez que vous ne pouvez pas utiliser de « groupes de scanner » lors du déploiement de plusieurs hôtes de cette façon.

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 les deux packages logiciels prérequis sont installés sur les systèmes (Docker ou Podman Engine et Python 3).
- 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 <client_id> -t <user_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 (par exemple, `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`) et enregistrez-le dans un fichier texte.

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 classification BlueXP termine l'installation des packages 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 la classification BlueXP"](#) à ce moment-là. Vous ne serez facturé que lorsque votre essai gratuit de 30 jours se terminera.

Installez la classification BlueXP sur un hôte Linux sans accès Internet

Suivez ces étapes pour installer la classification BlueXP sur un hôte Linux d'un site sur site qui ne dispose pas d'un accès à Internet, également appelé *mode privé*. Ce type d'installation est parfait pour vos sites sécurisés.

["Découvrez les différents modes de déploiement pour le connecteur BlueXP et la classification BlueXP"](#).

Notez que vous pouvez également ["Déployez la classification BlueXP dans un site sur site disposant d'un accès Internet"](#).

Le script d'installation de la classification BlueXP commence par vérifier si le système et l'environnement répondent aux prérequis requis. Si les conditions préalables sont toutes remplies, l'installation démarre. Si vous souhaitez vérifier les prérequis indépendamment de l'installation de la classification BlueXP, vous pouvez télécharger un pack logiciel distinct qui teste uniquement les prérequis. ["Découvrez comment vérifier si votre hôte Linux est prêt à installer la classification BlueXP"](#).

Sources de données prises en charge

Lorsqu'il est installé en mode privé (parfois appelé site « hors ligne » ou « invisible »), la classification BlueXP ne peut analyser les données qu'à partir de sources de données également locales sur le site. À ce stade, la classification BlueXP 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)

Aucune prise en charge n'est actuellement prise en charge pour l'analyse de Cloud Volumes ONTAP, Azure NetApp Files, FSX pour ONTAP, AWS S3 ou Google Drive, Comptes OneDrive ou SharePoint Online lorsque la classification BlueXP est déployée en mode privé.

Limites

La plupart des fonctionnalités de classification BlueXP fonctionnent lorsqu'elles sont déployées dans un site sans accès 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 la copie et de la synchronisation BlueXP
- Réception des commentaires de l'utilisateur
- Mises à niveau logicielles automatisées depuis BlueXP

Le connecteur BlueXP et la classification BlueXP nécessitent toutes deux des mises à niveau manuelles périodiques pour activer de nouvelles fonctionnalités. La version de classification BlueXP est visible en bas des pages de l'interface de classification BlueXP. Vérifier le ["Notes de version de la classification BlueXP"](#) 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 le connecteur BlueXP"](#) et [Mettez à niveau votre logiciel de classification BlueXP](#).

Démarrage rapide

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

1

Installez le connecteur BlueXP

Si aucun connecteur n'est déjà installé en mode privé, ["Déployer le connecteur"](#) Sur un hôte Linux.

2

Examinez les conditions préalables à la classification BlueXP

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 la classification BlueXP

Téléchargez le logiciel de classification BlueXP depuis 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 classification BlueXP.

4

Abonnez-vous au service de classification BlueXP

Les 1 premiers To de données analysés par le système de classification BlueXP dans BlueXP sont gratuits pendant 30 jours. Une licence NetApp BYOL est requise pour continuer l'analyse des données après ce point.

Installez le connecteur BlueXP

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

Préparez le système hôte Linux

Le logiciel de classification BlueXP doit s'exécuter sur un hôte répondant à des exigences spécifiques en termes de système d'exploitation, de RAM, de logiciels, etc.

- La classification BlueXP n'est pas prise en charge sur un hôte partagé avec d'autres applications : l'hôte doit être un hôte dédié.
- Lors de la création du système hôte sur site, vous pouvez choisir entre trois tailles de système selon la taille du dataset que vous prévoyez d'analyser par la classification BlueXP.

Taille du système	CPU	RAM (la mémoire d'échange doit être désactivée)	Disque
Très grand	32 processeurs	128 GO DE RAM	1 To SSD sur /, ou - 100 Gio disponible sur /opt - 895 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp
Grand	16 processeurs	64 GO DE RAM	500 Gio de SSD sur /, ou - 100 Gio disponible sur /opt - 395 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp
Moyen	8 processeurs	32 GO DE RAM	200 Gio de SSD sur /, ou - 50 Gio disponible sur /opt - 145 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp
Petit	8 processeurs	16 GO DE RAM	100 Gio de SSD sur /, ou - 50 Gio disponible sur /opt - 45 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp

Notez qu'il existe des limites lors de l'utilisation des systèmes plus petits. Voir "[Utilisation d'un type d'instance plus petit](#)" pour plus d'informations.

- Lors du déploiement d'une instance de calcul dans le cloud pour votre installation de classification BlueXP, nous vous recommandons de opter pour un système qui répond à la configuration requise pour les « grands » systèmes ci-dessus :
 - **Type d'instance AWS EC2:** Nous recommandons "m6i.4xlarge". "[Consultez la section autres types d'instances AWS](#)".

- **Taille de VM Azure:** Nous recommandons "Standard_D16s_v3". ["Consultez la section autres types d'instances Azure"](#).
- **Type de machine GCP:** Nous recommandons "n2-standard-16". ["Voir autres types d'instances GCP"](#).

- **Autorisations de dossier UNIX :** les autorisations UNIX minimales suivantes sont requises :

Dossier	Autorisations minimales
/tmp	rw-rw-rwt
/opt	rw-r-xr-x
/var/lib/docker	rw-----
/usr/lib/systemd/system	rw-r-xr-x

- **Système d'exploitation :**

- Les systèmes d'exploitation suivants nécessitent l'utilisation du moteur de mise en conteneurs Docker :
 - Red Hat Enterprise Linux version 7.8 et 7.9
 - CentOS versions 7.8 et 7.9
 - Ubuntu 22.04 (requiert la classification BlueXP version 1.23 ou supérieure)
- Les systèmes d'exploitation suivants nécessitent l'utilisation du moteur de conteneur Podman et requièrent la classification BlueXP version 1.30 ou supérieure :
 - Red Hat Enterprise Linux version 8.8, 9.0, 9.1, 9.2 et 9.3

Notez que les fonctionnalités suivantes ne sont actuellement pas prises en charge lors de l'utilisation de RHEL 8.x et RHEL 9.x :

- Installation dans un site sombre
- Numérisation distribuée ; utilisation d'un nœud de scanner maître et de nœuds de scanner distants

- **Gestion des abonnements Red Hat :** l'hôte 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 pendant l'installation.
- **Logiciels supplémentaires :** vous devez installer les logiciels suivants sur l'hôte avant d'installer la classification BlueXP :
 - En fonction du système d'exploitation que vous utilisez, vous devrez installer l'un des moteurs de mise en conteneurs :
 - Docker Engine version 19.3.1 ou supérieure. ["Voir les instructions d'installation"](#).
 - ["Regardez cette vidéo"](#) Pour une démonstration rapide de l'installation de Docker sur CentOS.
 - Podman version 4 ou supérieure. Pour installer Podman, mettez à jour vos packages système (`sudo yum update -y`), puis installez Podman (`sudo yum install netavark -y`).
- Python version 3.6 ou supérieure. ["Voir les instructions d'installation"](#).
 - **Considérations NTP :** NetApp recommande de configurer le système de classification BlueXP pour utiliser un service NTP (Network Time Protocol). L'heure doit être synchronisée entre le système de classification BlueXP et le système BlueXP Connector.
 - **Firesund considérations:** Si vous prévoyez d'utiliser `firewalld`, Nous vous recommandons de

l'activer avant d'installer la classification BlueXP. Exécutez les commandes suivantes pour configurer `firewalld` Pour qu'il soit compatible avec la classification BlueXP :

```
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
```

Notez que vous devez redémarrer Docker ou Podman chaque fois que vous activez ou mettez à jour `firewalld` paramètres.



L'adresse IP du système hôte de classification BlueXP ne peut pas être modifiée après l'installation.

Vérifiez les conditions préalables à la classification BlueXP et BlueXP

Vérifiez les conditions préalables suivantes afin de vous assurer que votre configuration est prise en charge avant de déployer la classification BlueXP.

- Assurez-vous que le connecteur dispose des autorisations nécessaires pour déployer les ressources et créer des groupes de sécurité pour l'instance de classification BlueXP. Vous trouverez les dernières autorisations BlueXP dans ["Règles fournies par NetApp"](#).
- Assurez-vous de pouvoir maintenir la classification BlueXP en cours d'exécution. L'instance de classification BlueXP doit continuer à analyser vos données en continu.
- Assurez la connectivité du navigateur web à la classification BlueXP. Une fois la classification BlueXP activée, assurez-vous que les utilisateurs accèdent à l'interface BlueXP depuis un hôte qui dispose d'une connexion à l'instance de classification BlueXP.

L'instance de classification BlueXP 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 situé dans le même réseau que l'instance de classification BlueXP.

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, la classification BlueXP, Active Directory et vos sources de données.

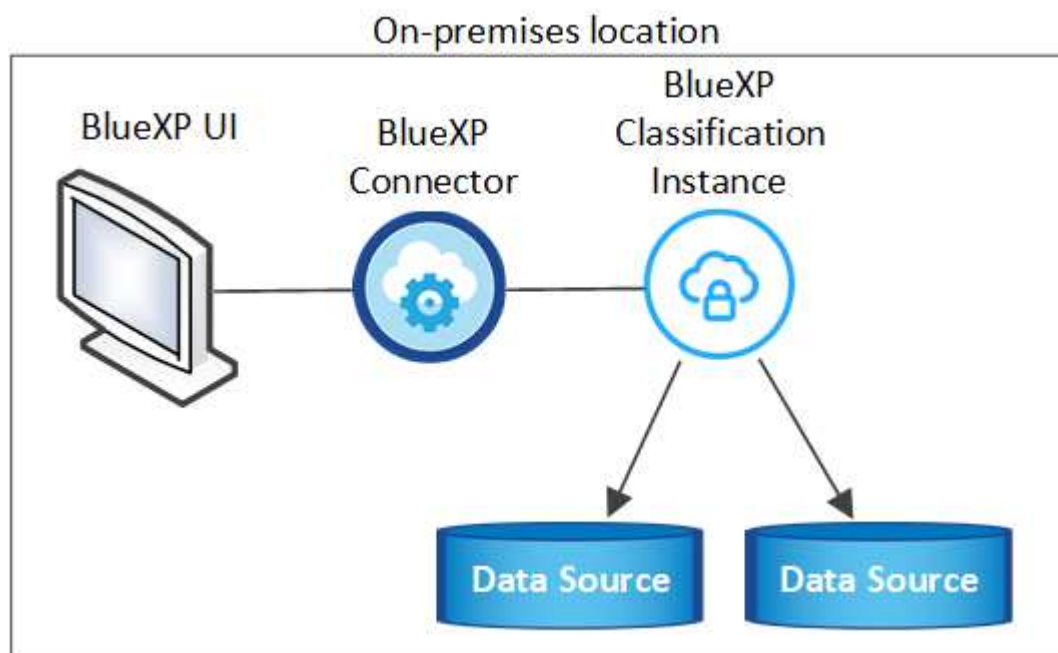
Type de connexion	Ports	Description
Classification de Connector <> BlueXP	8080 (TCP), 6000 (TCP), 443 (TCP) ET 80	<p>Le groupe de sécurité du connecteur doit autoriser le trafic entrant et sortant sur les ports 6000 et 443 vers et depuis l'instance de classification BlueXP.</p> <ul style="list-style-type: none"> • Le port 6000 est requis pour que la licence BYOL de classification BlueXP fonctionne sur un site invisible. • Le port 8080 doit être ouvert pour que vous puissiez 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"> • 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.
Classification BlueXP <> cluster ONTAP	<ul style="list-style-type: none"> • Pour NFS - 111 (TCP/UDP) et 2049 (TCP/UDP) • Pour CIFS - 139 (TCP/UDP) et 445 (TCP/UDP) 	<p>La classification BlueXP nécessite 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 classification BlueXP.</p> <p>Assurez-vous que les ports suivants sont ouverts pour l'instance de classification BlueXP :</p> <ul style="list-style-type: none"> • Pour NFS - 111 et 2049 • Pour CIFS : 139 et 445 <p>Les règles d'exportation des volumes NFS doivent autoriser l'accès à partir de l'instance de classification BlueXP.</p>

Type de connexion	Ports	Description
Classification BlueXP <> 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. De plus, la classification BlueXP requiert des informations d'identification Active Directory pour analyser les volumes CIFS.</p> <p>Vous devez disposer des informations pour Active Directory :</p> <ul style="list-style-type: none"> • 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 de classification BlueXP pour augmenter la puissance de traitement afin d'analyser vos sources de données, vous devez activer des ports/protocoles supplémentaires. ["Voir la configuration de port supplémentaire requise"](#).

Installez la classification BlueXP sur l'hôte Linux sur site

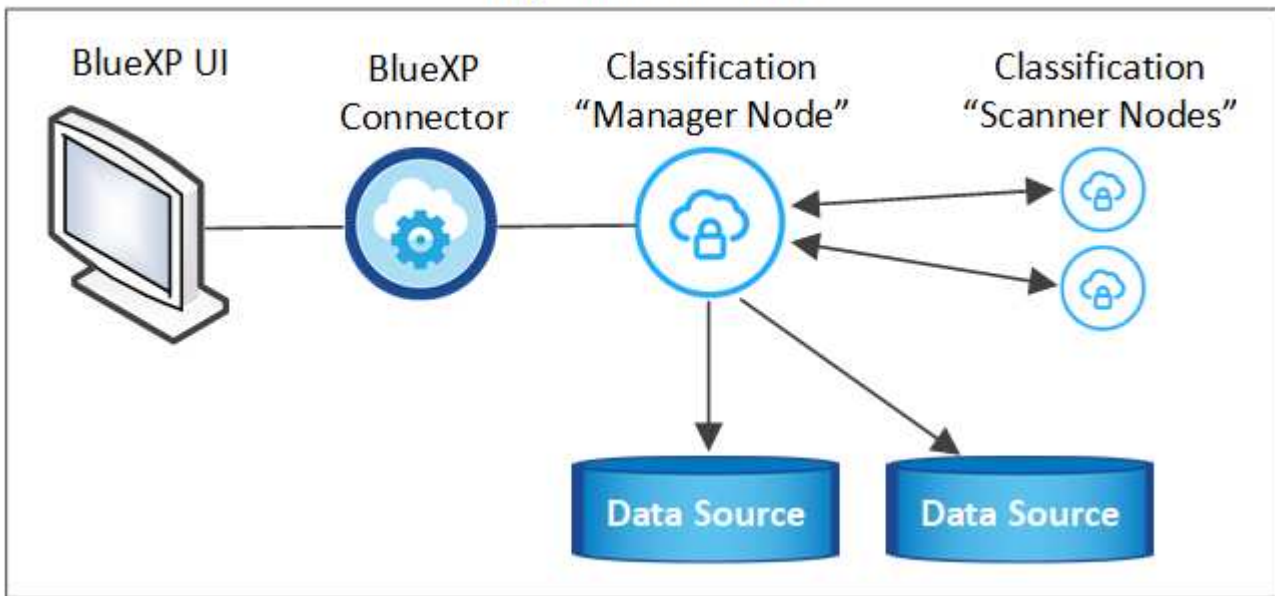
Pour les configurations standard, le logiciel est installé sur un système hôte unique. ["Découvrez ces étapes ici"](#).



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](#)".

On-premises location



Installation à un seul hôte pour les configurations courantes

Suivez ces étapes lors de l'installation du logiciel de classification BlueXP sur un hôte sur site unique dans un environnement hors ligne.

Notez que toutes les activités d'installation sont consignées lors de l'installation de la classification BlueXP. Si vous rencontrez des problèmes lors de l'installation, vous pouvez afficher le contenu du journal d'audit d'installation. Il est écrit dans `/opt/netapp/install_logs/`. ["Pour en savoir plus, cliquez ici"](#).

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 packages logiciels prérequis (Docker Engine ou Podman 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 en ligne, téléchargez le logiciel de classification BlueXP depuis le ["Site de support NetApp"](#). Le fichier que vous devez sélectionner est nommé **DataSense-Offline-bundle-`<version>`.tar.gz**.
2. Copiez l'ensemble d'installation sur l'hôte Linux que vous prévoyez d'utiliser en mode privé.
3. Décompressez le programme d'installation sur la machine hôte, par exemple :

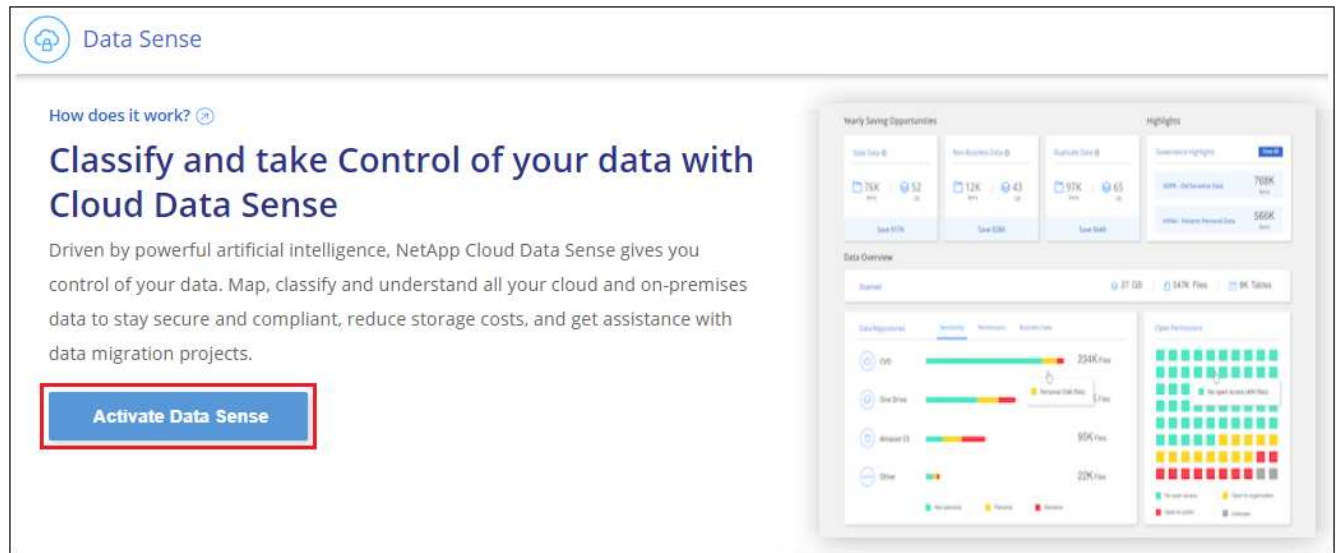
```
tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
```

Ceci extrait le logiciel requis et le fichier d'installation réel **cc_onsite_installer.tar.gz**.

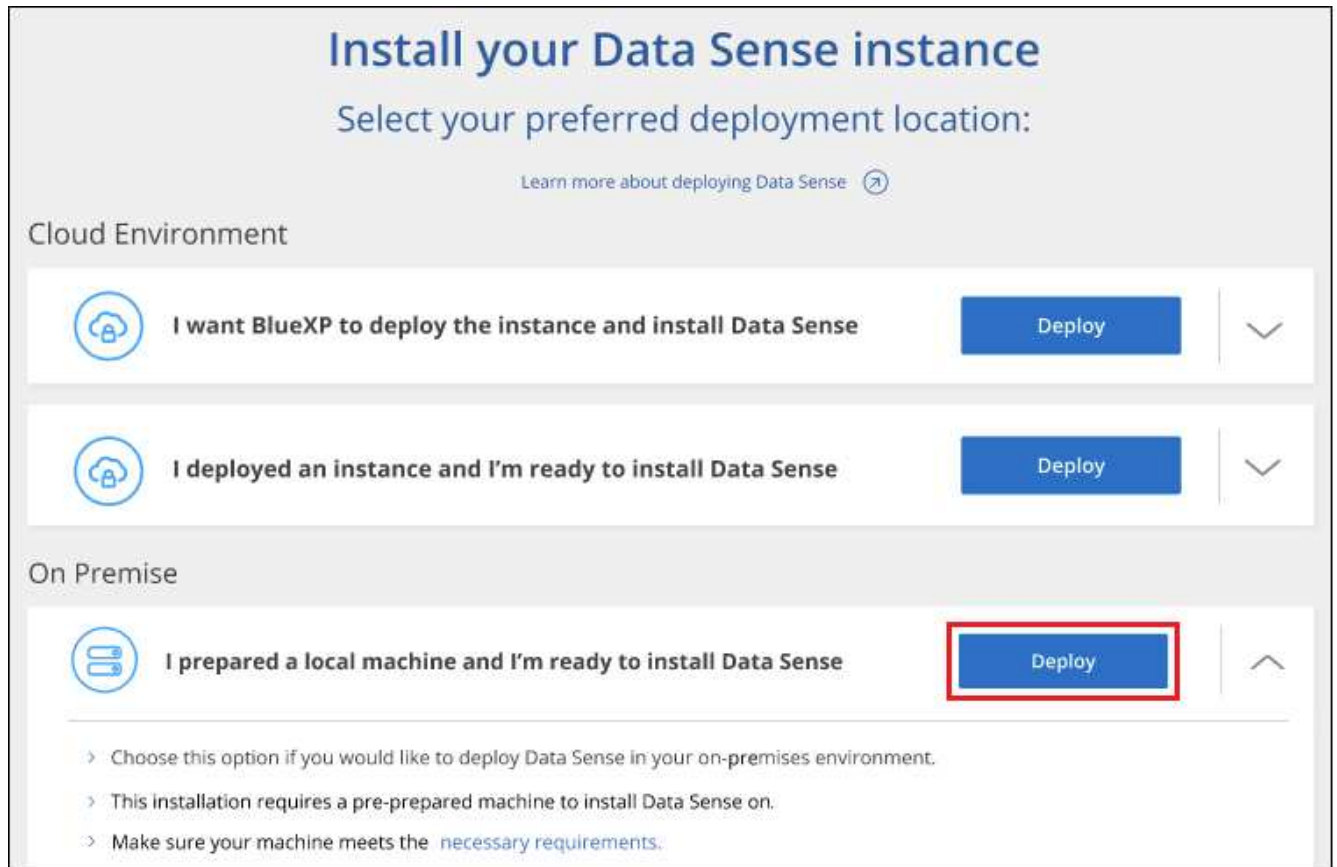
4. Décompressez le fichier d'installation sur la machine hôte, par exemple :


```
tar -xzf cc_onprem_installer.tar.gz
```

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



7. Cliquez sur **Deploy** pour démarrer l'installation sur site.



8. La boîte de dialogue *Deploy Data Sense on local* s'affiche. Copiez la commande fournie (par exemple :

`sudo ./install.sh -a 12345 -c 27AG75 -t 2198qq --darksite`) et collez-le dans un fichier texte pour pouvoir l'utiliser ultérieurement. Cliquez ensuite sur **Fermer** pour fermer la boîte de dialogue.

9. Sur la machine hôte, entrez la commande que vous avez copiée, puis suivez une série d'invites, ou vous pouvez fournir la commande complète incluant tous les paramètres requis comme arguments de ligne de commande.

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. Collez les informations que vous avez copiées à partir de l'étape 8 :</p> <pre>sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --darksite</pre> <p>b. Entrez l'adresse IP ou le nom d'hôte de la machine hôte de classification BlueXP afin qu'elle soit accessible par le système de connecteurs.</p> <p>c. Entrez l'adresse IP ou le nom d'hôte de la machine hôte du connecteur BlueXP afin que le système de classification BlueXP puisse y accéder.</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 <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite</pre>

Valeurs variables :

- *Account_ID* = ID du compte NetApp
- *Client_ID* = connecteur client ID (ajoutez le suffixe "clients" à l'ID client s'il n'y en a pas déjà)
- *User_token* = jeton d'accès utilisateur JWT
- *Ds_host* = adresse IP ou nom d'hôte du système de classification BlueXP.
- *Cm_host* = adresse IP ou nom d'hôte du système de connecteurs BlueXP.

Résultat

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

En cas de connectivité sur le port 8080 entre la machine hôte et l'instance de connecteur, vous verrez la progression de l'installation dans l'onglet de classification 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 la classification BlueXP"](#) À partir de la page du portefeuille digital BlueXP pour le moment. Vous ne serez facturé que lorsque votre essai gratuit de 30 jours se terminera.

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*.

Suivez ces étapes lors de l'installation du logiciel de classification BlueXP 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 packages logiciels prérequis (Docker Engine ou Podman 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 <client_id> -t <user_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 (par exemple : `sudo ./node_install.sh`

-m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212) et enregistrez-le dans un fichier texte.

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

- Copiez le fichier d'installation de Data Sense (**cc_onsite_installer.tar.gz**) sur la machine 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 classification BlueXP 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 la classification BlueXP"](#) À partir de la page du portefeuille digital BlueXP pour le moment. Vous ne serez facturé que lorsque votre essai gratuit de 30 jours se terminera.

Mettez à niveau le logiciel de classification BlueXP

Étant donné que le logiciel de classification BlueXP est régulièrement mis à jour avec les nouvelles fonctionnalités, il est conseillé de passer régulièrement en revue les nouvelles versions afin de vérifier que vous utilisez les logiciels et les fonctionnalités les plus récents. Vous devrez mettre à niveau le logiciel de classification BlueXP manuellement, car aucune connexion Internet ne permet d'effectuer la mise à niveau automatiquement.

Avant de commencer

- Nous vous recommandons de mettre à niveau votre logiciel BlueXP Connector vers la dernière version disponible. ["Reportez-vous aux étapes de mise à niveau du connecteur"](#).
- À partir de la classification BlueXP version 1.24, vous pouvez effectuer des mises à niveau vers n'importe quelle version future du logiciel.

Si votre logiciel de classification BlueXP exécute une version antérieure à 1.24, vous ne pouvez mettre à niveau qu'une seule version majeure à la fois. Par exemple, si la version 1.21.x est installée, vous ne pouvez mettre à niveau que vers la version 1.22.x. Si vous êtes quelques versions principales derrière, vous devrez mettre à niveau le logiciel à plusieurs reprises.

Étapes

- Sur un système configuré en ligne, téléchargez le logiciel de classification BlueXP depuis le ["Site de support NetApp"](#). Le fichier que vous devez sélectionner est nommé **DataSense-Offline-bundle-
<version>.tar.gz**.
- Copiez le bundle logiciel sur l'hôte Linux où la classification BlueXP est installée sur le site invisible.
- Décompressez le pack logiciel sur la machine hôte, par exemple :

```
tar -xvf DataSense-offline-bundle-v1.25.0.tar.gz
```

Ceci extrait le fichier d'installation **cc_onsite_installer.tar.gz**.

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

```
tar -xzf cc_onprem_installer.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 de classification BlueXP 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 d'analyse si vous avez déployé la classification BlueXP sur plusieurs systèmes hôtes pour l'analyse de très grandes configurations.

Pour vérifier que le logiciel a été mis à jour, vérifiez la version en bas des pages de l'interface de classification BlueXP.

Vérifiez que votre hôte Linux est prêt à installer la classification BlueXP

Avant d'installer manuellement la classification BlueXP sur un hôte Linux, vous pouvez exécuter un script sur l'hôte pour vérifier que toutes les conditions préalables requises pour l'installation de la classification BlueXP sont en place. Vous pouvez exécuter ce script sur un hôte Linux de votre réseau ou sur un hôte Linux du cloud. L'hôte peut être connecté à Internet, ou l'hôte peut résider sur un site qui n'a pas accès à Internet (un *site sombre*).

Il existe également un script de test prérequis qui fait partie du script d'installation de la classification BlueXP. Le script décrit ici est spécialement conçu pour les utilisateurs qui souhaitent vérifier l'hôte Linux indépendamment de l'exécution du script d'installation de classification BlueXP.

Mise en route

Vous effectuerez les tâches suivantes.

1. Si vous ne l'avez pas déjà installé, installez un connecteur BlueXP. Vous pouvez exécuter le script de test sans avoir installé de connecteur, mais le script vérifie la connectivité entre le connecteur et la machine hôte de classification BlueXP. Il est donc recommandé de disposer d'un connecteur.
2. Préparer le porteur et vérifier qu'il répond à toutes les exigences.
3. Activez l'accès Internet sortant à partir de la machine hôte de classification BlueXP.
4. Vérifiez que tous les ports requis sont activés sur tous les systèmes.

5. Téléchargez et exécutez le script de test requis.

Créer un connecteur

Un connecteur BlueXP est requis avant de pouvoir installer et utiliser la classification BlueXP. Vous pouvez cependant exécuter le script `Prerequisites` sans connecteur.

C'est possible "[Installer le connecteur sur site](#)" Sur un hôte Linux de votre réseau ou sur un hôte Linux du cloud. Certains utilisateurs qui prévoient d'installer la classification BlueXP sur site peuvent également choisir d'installer le connecteur sur site.

Pour créer un connecteur dans l'environnement de votre fournisseur de cloud, reportez-vous à la section "[Création d'un connecteur dans AWS](#)", "[Création d'un connecteur dans Azure](#)", ou "[Création d'un connecteur dans GCP](#)".

Vous aurez besoin de l'adresse IP ou du nom d'hôte du système de connecteur lors de l'exécution du script `Prerequisites`. 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**.

Vérifiez les besoins de l'hôte

Le logiciel de classification BlueXP doit s'exécuter sur un hôte répondant à des exigences spécifiques en termes de système d'exploitation, de RAM, de logiciels, etc.

- La classification BlueXP n'est pas prise en charge sur un hôte partagé avec d'autres applications : l'hôte doit être un hôte dédié.
- Lors de la création du système hôte sur site, vous pouvez choisir entre trois tailles de système selon la taille du dataset que vous prévoyez d'analyser par la classification BlueXP.

Taille du système	CPU	RAM (la mémoire d'échange doit être désactivée)	Disque
Très grand	32 processeurs	128 GO DE RAM	1 To SSD sur /, ou - 100 Gio disponible sur /opt - 895 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp
Grand	16 processeurs	64 GO DE RAM	500 Gio de SSD sur /, ou - 100 Gio disponible sur /opt - 395 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp
Moyen	8 processeurs	32 GO DE RAM	200 Gio de SSD sur /, ou - 50 Gio disponible sur /opt - 145 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp

Taille du système	CPU	RAM (la mémoire d'échange doit être désactivée)	Disque
Petit	8 processeurs	16 GO DE RAM	100 Gio de SSD sur /, ou - 50 Gio disponible sur /opt - 45 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp

Notez qu'il existe des limites lors de l'utilisation des systèmes plus petits. Voir ["Utilisation d'un type d'instance plus petit"](#) pour plus d'informations.

- Lors du déploiement d'une instance de calcul dans le cloud pour votre installation de classification BlueXP, nous vous recommandons de opter pour un système qui répond à la configuration requise pour les « grands » systèmes ci-dessus :
 - **Type d'instance AWS EC2:** Nous recommandons "m6i.4xlarge". ["Consultez la section autres types d'instances AWS"](#).
 - **Taille de VM Azure:** Nous recommandons "Standard_D16s_v3". ["Consultez la section autres types d'instances Azure"](#).
 - **Type de machine GCP:** Nous recommandons "n2-standard-16". ["Voir autres types d'instances GCP"](#).
- **Autorisations de dossier UNIX :** les autorisations UNIX minimales suivantes sont requises :

Dossier	Autorisations minimales
/tmp	rw-rw-rwt
/opt	rw-r-xr-x
/var/lib/docker	rw-----
/usr/lib/systemd/system	rw-r-xr-x

- **Système d'exploitation :**
 - Les systèmes d'exploitation suivants nécessitent l'utilisation du moteur de mise en conteneurs Docker :
 - Red Hat Enterprise Linux version 7.8 et 7.9
 - CentOS versions 7.8 et 7.9
 - Ubuntu 22.04 (requiert la classification BlueXP version 1.23 ou supérieure)
 - Les systèmes d'exploitation suivants nécessitent l'utilisation du moteur de conteneur Podman et requièrent la classification BlueXP version 1.30 ou supérieure :
 - Red Hat Enterprise Linux version 8.8, 9.0, 9.1, 9.2 et 9.3

Notez que les fonctionnalités suivantes ne sont actuellement pas prises en charge lors de l'utilisation de RHEL 8.x et RHEL 9.x :

- Installation dans un site sombre
 - Numérisation distribuée ; utilisation d'un nœud de scanner maître et de nœuds de scanner distants
- **Gestion des abonnements Red Hat :** l'hôte 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 pendant l'installation.

- **Logiciels supplémentaires** : vous devez installer les logiciels suivants sur l'hôte avant d'installer la classification BlueXP :
 - En fonction du système d'exploitation que vous utilisez, vous devrez installer l'un des moteurs de mise en conteneurs :
 - Docker Engine version 19.3.1 ou supérieure. ["Voir les instructions d'installation"](#).
 - ["Regardez cette vidéo"](#) Pour une démonstration rapide de l'installation de Docker sur CentOS.
 - Podman version 4 ou supérieure. Pour installer Podman, mettez à jour vos packages système (`sudo yum update -y`), puis installez Podman (`sudo yum install netavark -y`).
- Python version 3.6 ou supérieure. ["Voir les instructions d'installation"](#).
 - **Considérations NTP** : NetApp recommande de configurer le système de classification BlueXP pour utiliser un service NTP (Network Time Protocol). L'heure doit être synchronisée entre le système de classification BlueXP et le système BlueXP Connector.
 - **Firesund considérations**: Si vous prévoyez d'utiliser `firewalld`, Nous vous recommandons de l'activer avant d'installer la classification BlueXP. Exécutez les commandes suivantes pour configurer `firewalld` Pour qu'il soit compatible avec la classification BlueXP :

```
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 des hôtes de classification BlueXP supplémentaires comme nœuds d'analyse (dans un modèle distribué), ajoutez ces règles à votre système principal à ce stade :

```
firewall-cmd --permanent --add-port=2377/tcp
firewall-cmd --permanent --add-port=7946/udp
firewall-cmd --permanent --add-port=7946/tcp
firewall-cmd --permanent --add-port=4789/udp
```

+

Notez que vous devez redémarrer Docker ou Podman chaque fois que vous activez ou mettez à jour `firewalld` paramètres.

Assurez un accès Internet sortant à partir de la classification BlueXP

La classification BlueXP nécessite un accès Internet sortant. Si votre réseau physique ou virtuel utilise un serveur proxy pour l'accès à Internet, assurez-vous que l'instance de classification BlueXP dispose d'un accès Internet sortant pour contacter les terminaux suivants.



Cette section n'est pas requise pour les systèmes hôtes installés sur des sites sans connexion Internet.

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://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	Fournit les packages prérequis pour l'installation de docker.
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 des packages prérequis pour l'installation de CentOS.
http://packages.ubuntu.com/ http://archive.ubuntu.com	Fournit les packages prérequis pour l'installation d'Ubuntu.

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, la classification BlueXP, Active Directory et vos sources de données.

Type de connexion	Ports	Description
Classification de Connector <> BlueXP	8080 (TCP), 443 (TCP) et 80	Les règles de pare-feu ou de routage du connecteur doivent autoriser le trafic entrant et sortant via le port 443 vers et depuis l'instance de classification BlueXP. 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, 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 pare-feu ou les règles de routage prédéfinies.

Exécutez le script BlueXP classification Prerequisites

Procédez comme suit pour exécuter le script BlueXP classification Prerequisites.

["Regardez cette vidéo"](#) Pour savoir comment exécuter le script Prerequisites et interpréter les résultats.

Ce dont vous avez besoin

- Vérifiez que votre système Linux est conforme à la [configuration requise pour l'hôte](#).
- Vérifiez que le système dispose des deux packages logiciels prérequis installés (Docker Engine ou Podman et Python 3).
- Assurez-vous que vous disposez des privilèges root sur le système Linux.

Étapes

1. Téléchargez le script BlueXP classification Prerequisites depuis le "[Site de support NetApp](#)". Le fichier que vous devez sélectionner est nommé **standalone-pre-tester-<version>**.
2. Copiez le fichier sur l'hôte Linux que vous souhaitez utiliser (à l'aide de `scp` ou une autre méthode).
3. Attribuez des autorisations pour exécuter le script.

```
chmod +x standalone-pre-requisite-tester-v1.25.0
```

4. Exécutez le script à l'aide de la commande suivante.

```
./standalone-pre-requisite-tester-v1.25.0 <--darksite>
```

Ajoutez l'option "`--darksite`" uniquement si vous exécutez le script sur un hôte qui n'a pas accès à Internet. Certains tests préalables sont ignorés lorsque l'hôte n'est pas connecté à Internet.

5. Le script vous demande l'adresse IP de la machine hôte de classification BlueXP.
 - Entrez l'adresse IP ou le nom d'hôte.
6. Le script vous demande si BlueXP Connector est installé.
 - Entrez **N** si vous n'avez pas de connecteur installé.
 - Entrez **y** si vous avez un connecteur installé. Puis entrez l'adresse IP ou le nom d'hôte du connecteur BlueXP afin que le script de test puisse tester cette connectivité.
7. Le script exécute une variété de tests sur le système et affiche les résultats au fur et à mesure qu'il progresse. Une fois terminé, il écrit un journal de la session dans un fichier nommé `prerequisites-test-<timestamp>.log` dans le répertoire `/opt/netapp/install_logs`.

Résultat

Si tous les tests prérequis ont été correctement exécutés, vous pouvez installer la classification BlueXP sur l'hôte lorsque vous êtes prêt.

Si des problèmes ont été découverts, ils sont classés comme « recommandés » ou « obligatoires » pour être résolus. Les problèmes recommandés sont généralement des éléments qui ralentiraient l'analyse de classification BlueXP et les tâches de catégorisation. Ces éléments n'ont pas besoin d'être corrigés, mais vous pouvez les corriger.

Si vous rencontrez des problèmes « obligatoires », vous devez résoudre les problèmes et exécuter à nouveau le script de test prérequis.

Informations sur le copyright

Copyright © 2024 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.