Commencez

BlueXP classification

NetApp
August 11, 2025

Sommaire

Commencez

Découvrez la classification BlueXP

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

À partir de la version 1.31, la classification BlueXP est disponible en tant que fonctionnalité clé de BlueXP . Il n'y a pas de frais supplémentaires. Aucune licence de classification ni aucun abonnement n'est requis. + si vous utilisez la version 1.30 ou antérieure, cette version est disponible jusqu'à expiration de votre abonnement. "Voir la liste des fonctions obsolètes".

Caractéristiques

La classification BlueXP utilise l'intelligence artificielle (IA), le traitement du langage naturel (NLP) et LE machine learning (ML) pour comprendre le contenu qu'il analyse afin d'extraire des entités et de répartir le contenu par catégorie. Ceci permet à la classification BlueXP de fournir les domaines de fonctionnalité suivants.

"En savoir plus sur les utilisations de la classification BlueXP".

Préservez la conformité

La classification BlueXP offre plusieurs outils qui vous aident dans vos efforts de conformité. Vous pouvez utiliser la classification BlueXP pour :

- Identifier les informations à caractère personnel
- Identifier une vaste portée des données personnelles sensibles, conformément aux réglementations en matière de confidentialité, RGPD, CCPA, PCI et HIPAA.
- Répondez aux demandes d'accès aux données (DSAR, Data Subject Access Requests) en fonction de votre nom ou de votre adresse e-mail.

Renforcez la sécurité

La classification BlueXP permet d'identifier les données potentiellement menacées d'accès à des fins criminelles. Vous pouvez utiliser la classification BlueXP pour :

- Identifiez tous les fichiers et répertoires (partages et dossiers) avec les autorisations ouvertes exposées à l'ensemble de votre organisation ou au public.
- Identifiez les données sensibles qui se trouvent en dehors de l'emplacement initial dédié.
- Respectez les règles de conservation des données.
- Utilisez *Policies* pour détecter automatiquement les nouveaux problèmes de sécurité afin que le personnel de sécurité puisse agir immédiatement.

Optimiser l'utilisation du stockage

La classification BlueXP fournit des outils qui vous aideront à maîtriser votre TCO. Vous pouvez utiliser la classification BlueXP pour :

- Amélioration de l'efficacité du stockage grâce à l'identification des données dupliquées ou non liées à l'activité.
- Réduisez les coûts du stockage en identifiant les données inactives que vous pouvez déplacer vers un stockage objet moins coûteux. "En savoir plus sur le Tiering des systèmes Cloud Volumes ONTAP". "En savoir plus sur le Tiering à partir des systèmes ONTAP sur site".

Environnements de travail et sources de données pris en charge

La classification BlueXP peut analyser et analyser les données structurées et non structurées à partir des types d'environnements de travail et de sources de données suivants :

Environnements de travail

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

Sources de données

- Partages de fichiers NetApp
- Bases de données :
  - Amazon Relational Database Service (Amazon RDS)
  - MongoDB
  - MySQL
  - Oracle
  - PostgreSQL
  - SAP HANA
  - Serveur SQL (MSSQL)

La classification BlueXP prend en charge les versions NFS 3.x, 4.0 et 4.1, ainsi que les versions CIFS 1.x, 2.0, 2.1 et 3.0.

Le coût

La classification BlueXP est gratuite. Aucune licence de classification ou abonnement payant n'est nécessaire.

Coûts d'infrastructure

- L'installation de la classification BlueXP dans le cloud nécessite le déploiement d'une instance cloud, ce qui entraîne des frais du fournisseur cloud où il est déployé. Voir type d'instance déployé pour chaque fournisseur cloud. L'installation de la classification BlueXP sur un système sur site est gratuit.
- Pour classification BlueXP, vous devez avoir déployé un connecteur BlueXP. Dans de nombreux cas, vous disposez déjà d'un connecteur en raison d'autres services et stockages que vous utilisez dans BlueXP. L'instance de connecteur entraîne des frais supplémentaires du fournisseur cloud sur lequel elle est déployée. Voir la "type d'instance déployé pour chaque fournisseur cloud". L'installation du connecteur sur un système sur site est gratuite.

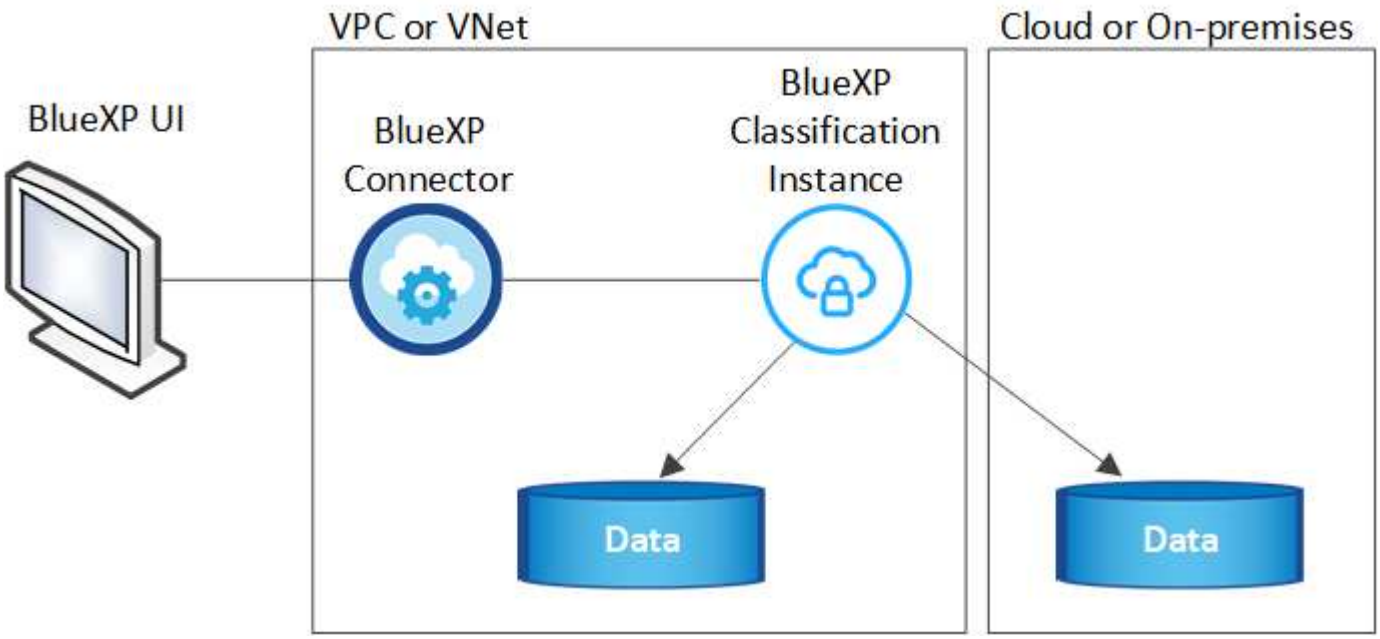
Coûts de transfert de données

Les coûts de transfert de données dépendent de votre configuration. Si l'instance de classification BlueXP et la source de données se trouvent dans la même zone de disponibilité et dans la même région, aucun coût de transfert de données n'est applicable. Mais si la source de données, comme un système Cloud Volumes ONTAP, se trouve dans une zone de disponibilité ou une région *différente*, les coûts de transfert des données vous seront facturés par votre fournisseur cloud. Consultez ces liens pour en savoir plus :

- "AWS : tarifs Amazon Elastic Compute Cloud (Amazon EC2)"
- "Microsoft Azure : détails de la tarification de la bande passante"
- "Google Cloud : tarification du service de transfert du stockage"

Instance de classification BlueXP

Lorsque vous déployez la classification BlueXP dans le cloud, BlueXP déploie l'instance dans le même sous-réseau que le connecteur. "En savoir plus sur les connecteurs."



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

- Dans AWS, la classification BlueXP s'exécute sur un "instance m6i.4xlarge" Avec un disque GP2 de 500 Gio. L'image du système d'exploitation est Amazon Linux 2. Lorsqu'elle est déployée dans AWS, vous pouvez choisir une instance de plus petite taille si vous analysez un petit volume de données.
- Dans Azure, la classification BlueXP s'exécute sur un avec un "Machine virtuelle standard_D16s_v3"disque de 500 Gio. L'image du système d'exploitation est Ubuntu 22.04.
- Dans GCP, la classification BlueXP s'exécute sur un avec un "n2-standard-16 VM"disque persistant standard de 500 Gio. L'image du système d'exploitation est Ubuntu 22.04.
- Dans les régions où l'instance par défaut n'est pas disponible, la classification BlueXP s'exécute sur une autre instance. "Voir les autres types d'instances".
- L'instance s'appelle *CloudCompliance* avec un hachage (UUID) généré concaténé. Par exemple : *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Chaque connecteur ne déploie qu'une seule instance de classification BlueXP.

Vous pouvez également déployer la classification BlueXP sur un hôte Linux sur site ou sur un hôte de votre fournisseur cloud préféré. Le logiciel fonctionne exactement de la même manière quelle que soit la méthode d'installation choisie. Les mises à niveau du logiciel de classification BlueXP sont automatisées tant que l'instance dispose d'un accès Internet.

L'instance doit rester en cours d'exécution en permanence, car la classification BlueXP analyse les données en continu.

Déployer sur différents types d'instances

Consultez les spécifications suivantes pour les types d'instances :

Taille du système	Caractéristiques	Limites
Très grand	32 processeurs, 128 Go de RAM, SSD de 1 Tio	Peut analyser jusqu'à 500 millions de fichiers.
Grand (par défaut)	16 processeurs, 64 Go de RAM, SSD de 500 Gio	Peut analyser jusqu'à 250 millions de fichiers.

Lorsque vous déployez la classification BlueXP dans Azure ou GCP, envoyez un e-mail à ng-contact-data-sense@netapp.com pour obtenir de l'aide si vous souhaitez utiliser un type d'instance plus petit.

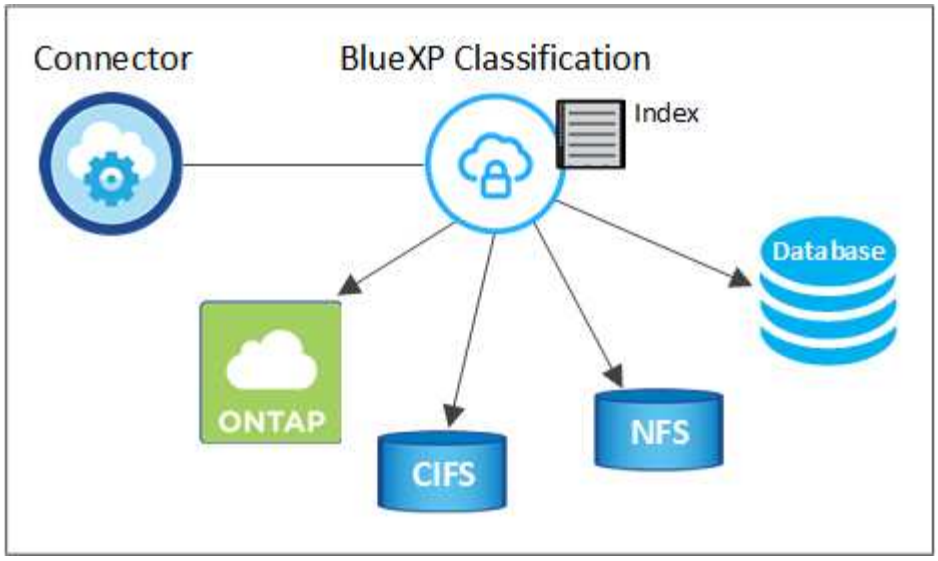
Fonctionnement de la numérisation de classification BlueXP

À un niveau élevé, la numérisation de classification BlueXP fonctionne comme suit :

1. Déployez une instance de classification BlueXP dans BlueXP.
2. Vous activez la cartographie de haut niveau (appelée *Mapping Only* scans) ou la numérisation de niveau profond (appelée *Map & Classify* scans) sur une ou plusieurs sources de données.
3. La classification BlueXP analyse les données à l'aide d'un processus d'apprentissage par l'IA.
4. Vous utilisez les tableaux de bord et les outils de génération de rapports fournis pour vous aider dans vos efforts de conformité et de gouvernance.

Une fois que vous avez activé la classification BlueXP et sélectionné les référentiels à analyser (il s'agit des volumes, des schémas de base de données ou d'autres données utilisateur), l'analyse des données commence immédiatement pour identifier les données personnelles et sensibles. Dans la plupart des cas, il est préférable de se concentrer sur l'analyse des données de production en direct plutôt que sur des sauvegardes, des miroirs ou des sites de reprise sur incident. Ensuite, la classification BlueXP mappe vos données d'entreprise, classe chaque fichier, puis identifie et extrait des entités et des modèles prédéfinis dans les données. Le résultat de l'analyse est un index des informations personnelles, des données personnelles sensibles, des catégories de données et des types de fichiers.

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



Après l'analyse initiale, la classification BlueXP analyse en continu vos données selon une séquence périodique pour détecter les modifications incrémentielles. C'est pourquoi il est important de maintenir l'instance en cours d'exécution.

Vous pouvez activer et désactiver les analyses au niveau du volume ou au niveau du schéma de base de données.

La BlueXP classification n'impose aucune limite à la quantité de données pouvant être analysée. Chaque connecteur prend en charge l'analyse et l'affichage de 500 Tio de données. Pour analyser plus de 500 Tio de données, "installer un autre connecteur" alors "déployer une autre instance de classification" . + L'interface utilisateur BlueXP affiche les données d'un seul connecteur. Pour obtenir des conseils sur l'affichage des données de plusieurs connecteurs, consultez "Utilisation de plusieurs connecteurs" .

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

Vous pouvez effectuer deux types d'acquisitions dans la classification BlueXP :

- **Les acquisitions cartographiques uniquement** ne fournissent qu'une vue d'ensemble de haut niveau de vos données et sont effectuées sur des sources de données sélectionnées. Les analyses de cartographie uniquement prennent moins de temps que les analyses de cartographie et de classification, car elles n'accèdent pas aux fichiers pour voir les données qu'ils contiennent. Vous pouvez commencer par identifier les domaines de recherche, puis effectuer une analyse carte et classification sur ces domaines.
- **Cartographiez et classifiez les acquisitions** fournissent une analyse de niveau profond de vos données.

Pour plus de détails sur les différences entre les analyses de mappage et de classification, voir "Quelle est la différence entre les acquisitions de mappage et de classification ?".

Informations catégorisées par la classification BlueXP

La classification BlueXP collecte, indexe et attribue des catégories aux données suivantes :

- **Métadonnées standard** à propos des fichiers : le type de fichier, sa taille, ses dates de création et de modification, etc.
- **Données personnelles** : informations personnelles identifiables (IIP) telles que les adresses électroniques, les numéros d'identification ou les numéros de carte de crédit, que la classification BlueXP

identifie en utilisant des mots, des chaînes et des modèles spécifiques dans les fichiers. "En savoir plus sur les données personnelles".

- **Données personnelles sensibles** : types particuliers d'informations personnelles sensibles (SPII), telles que les données de santé, l'origine ethnique ou les opinions politiques, tels que définis par le Règlement général sur la protection des données (RGPD) et d'autres réglementations sur la confidentialité. "En savoir plus sur les données personnelles sensibles".
- **Catégories**: La classification BlueXP prend les données qu'il a analysées et les divise en différents types de catégories. Les catégories sont des rubriques basées sur l'analyse par IA du contenu et des métadonnées de chaque fichier. "En savoir plus sur les catégories".
- **Types** : la classification BlueXP prend les données analysées et les répartit par type de fichier. "En savoir plus sur les types".
- **Reconnaissance des noms d'entités** : la classification BlueXP utilise l'IA pour extraire les noms naturels des personnes des documents. "Découvrez comment répondre aux demandes d'accès aux données".

Présentation du réseau

La classification BlueXP déploie un serveur ou un cluster unique, où que vous soyez, dans le cloud ou sur site. Les serveurs se connectent via des protocoles standard aux sources de données et indexent les résultats dans un cluster Elasticsearch, qui est également déployé sur les mêmes serveurs. Cela permet la prise en charge des environnements multicloud, cross-cloud, cloud privé et sur site.

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

Lorsque vous utilisez BlueXP en mode SaaS, la connexion à BlueXP est assurée via HTTPS et les données privées envoyées entre votre navigateur et l'instance de classification BlueXP sont sécurisées avec un chiffrement de bout en bout à l'aide de TLS 1.2, ce qui signifie que NetApp et des tiers ne peuvent pas les lire.

Les règles sortantes sont complètement ouvertes. Un accès à Internet est nécessaire pour installer et mettre à niveau le logiciel de classification BlueXP et pour envoyer des metrics d'utilisation.

Si vous avez des exigences de mise en réseau strictes, "Découvrez les terminaux que la classification BlueXP contacte".

Accéder à la BlueXP classification

Vous pouvez accéder au service de BlueXP classification via NetApp BlueXP.

Pour vous connecter à BlueXP, vous pouvez utiliser vos informations d'identification du site de support NetApp ou vous inscrire pour une connexion au cloud NetApp à l'aide de votre e-mail et d'un mot de passe. "En savoir plus sur la connexion à BlueXP".

Des tâches spécifiques nécessitent des rôles d'utilisateur BlueXP spécifiques. "En savoir plus sur les rôles d'accès BlueXP pour tous les services".

Avant de commencer

- "Vous devez ajouter un connecteur BlueXP ."
- "Comprendre quel style de déploiement de BlueXP classification convient à votre charge de travail."

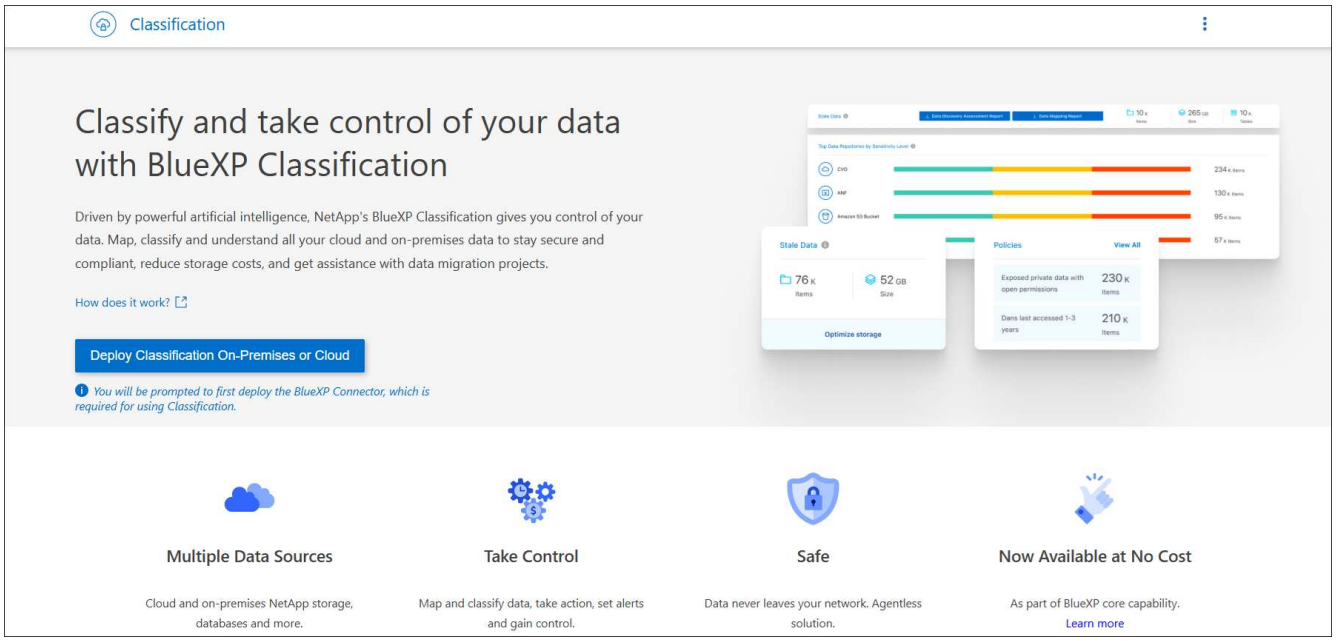
Étapes

1. Dans un navigateur Web, accédez à l' "Console BlueXP" .

La page de connexion NetApp BlueXP s'affiche.

2. Sign in à BlueXP.
3. Dans le menu de navigation de gauche de BlueXP , sélectionnez **Gouvernance** > **Classification**.
4. Si c'est la première fois que vous accédez à la BlueXP classification, la page de destination apparaît.

   Sélectionnez **Déployer la classification sur site ou dans le cloud** pour commencer à déployer votre instance de classification. Pour plus d'informations, voir "Quel déploiement de classification BlueXP devez-vous utiliser ?"



   Sinon, le tableau de bord de BlueXP classification apparaît.

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, n'a pas de connectivité avec la couche SaaS BlueXP .

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.

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.

Déployez la classification BlueXP

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

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 :

- Lorsque vous analysez les données dans des compartiments Cloud Volumes ONTAP dans AWS ou Amazon FSX pour ONTAP, 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.

Ces connecteurs cloud permettent d'analyser les systèmes ONTAP sur site, les partages de fichiers NetApp et les bases de données.

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".

La BlueXP classification n'impose aucune limite à la quantité de données pouvant être analysée. Chaque connecteur prend en charge l'analyse et l'affichage de 500 Tio de données. Pour analyser plus de 500 Tio de données, "installer un autre connecteur" alors "déployer une autre instance de classification" . + L'interface utilisateur BlueXP affiche les données d'un seul connecteur. Pour obtenir des conseils sur l'affichage des données de plusieurs connecteurs, consultez "Utilisation de 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 :

"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. Les proxys transparents ne sont actuellement pas pris en charge.

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.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Permet d'accéder aux images logicielles, aux manifestes, aux modèles et à l'envoi de journaux et de mesures.
https://support.compliance.api.bluexp.netapp.com/	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.

Assurez-vous que BlueXP dispose des autorisations requises

Assurez-vous que BlueXP dispose des autorisations nécessaires pour déployer des ressources et créer des groupes de sécurité pour l'instance de BlueXP classification .

- "Autorisations Google Cloud"
- "Autorisations AWS"
- "Autorisations Azure"

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"

Déployez la classification BlueXP dans le cloud

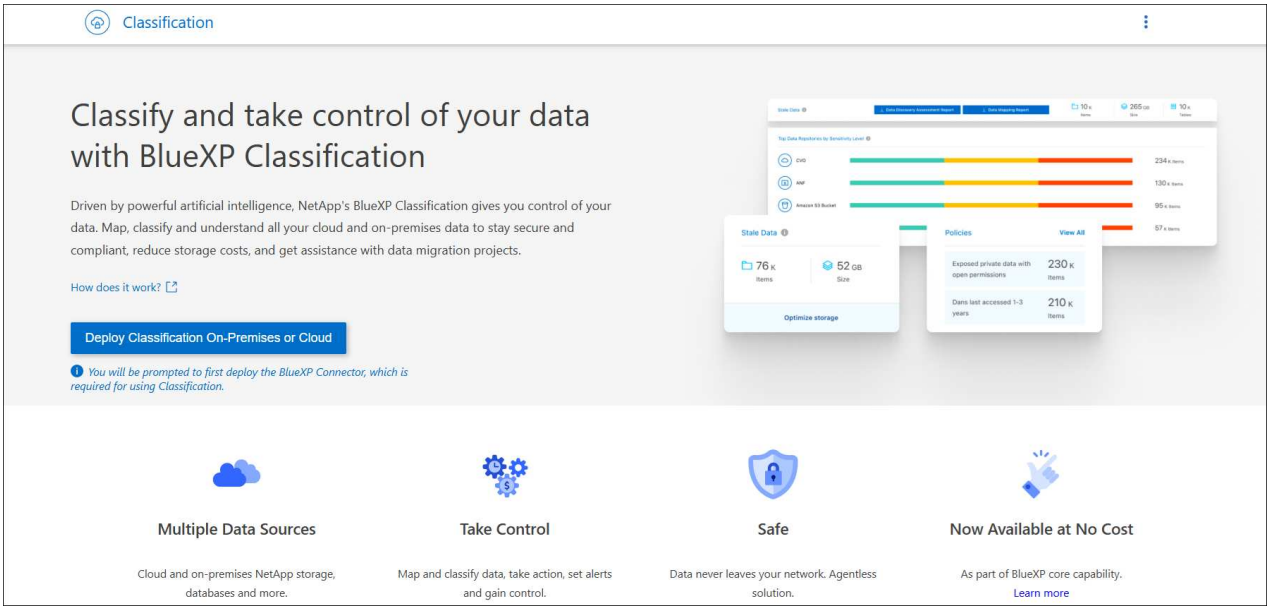
Suivez ces étapes pour déployer une instance de classification BlueXP dans le cloud. Le connecteur va déployer l'instance dans le cloud, puis installer le logiciel de classification BlueXP sur cette instance.

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 , sélectionnez **gouvernance > Classification**.
2. Sélectionnez **Déployer la classification sur site ou dans le cloud**.



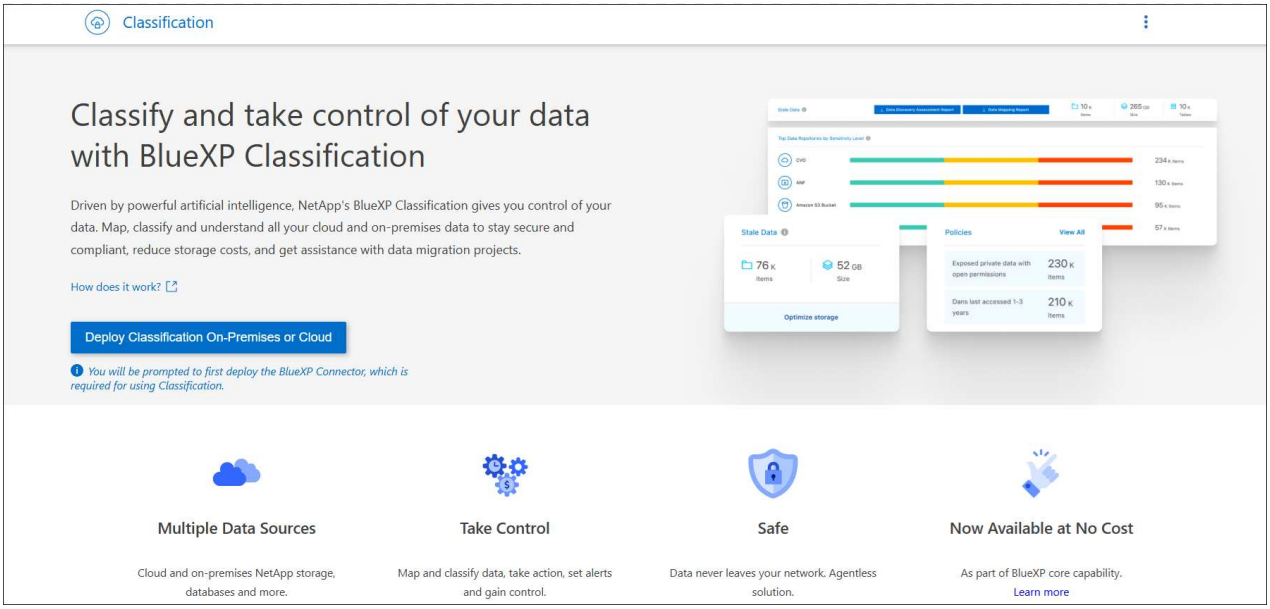
3. Depuis la page *Installation*, sélectionnez **Déployer > Déployer** pour utiliser la taille d'instance « Grande » et démarrer l'assistant de déploiement cloud.
4. L'assistant affiche la progression au fur et à mesure des étapes de déploiement. Il s'arrête et vous invite à entrer s'il est en cours de problème.

5. Lorsque l'instance est déployée et que la BlueXP classification est installée, sélectionnez **Continuer vers la configuration** pour accéder à la page *Configuration*.

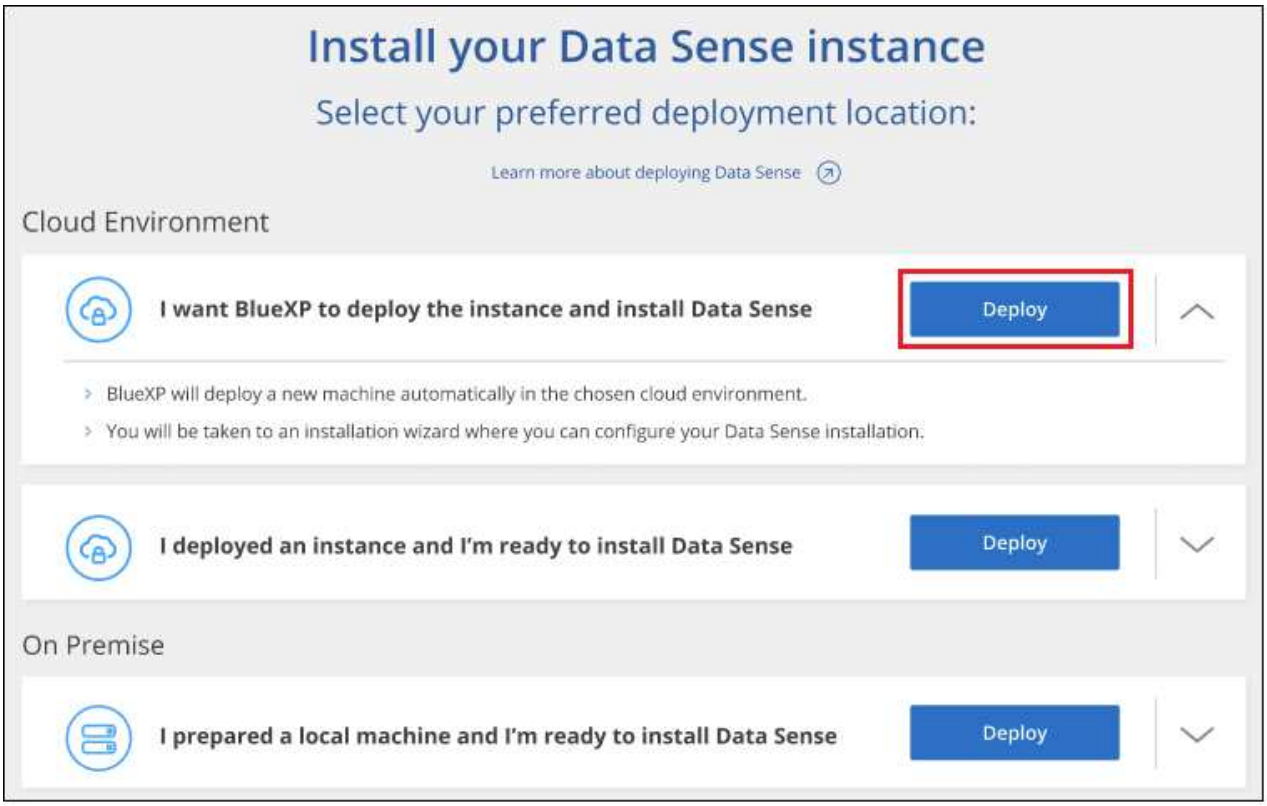
Déploiement dans Azure

Étapes

1. Dans le menu de navigation de gauche BlueXP , sélectionnez **gouvernance > Classification**.
2. Sélectionnez **Déployer la classification sur site ou dans le cloud**.



3. Sélectionnez **Déployer** pour démarrer l'assistant de déploiement cloud.



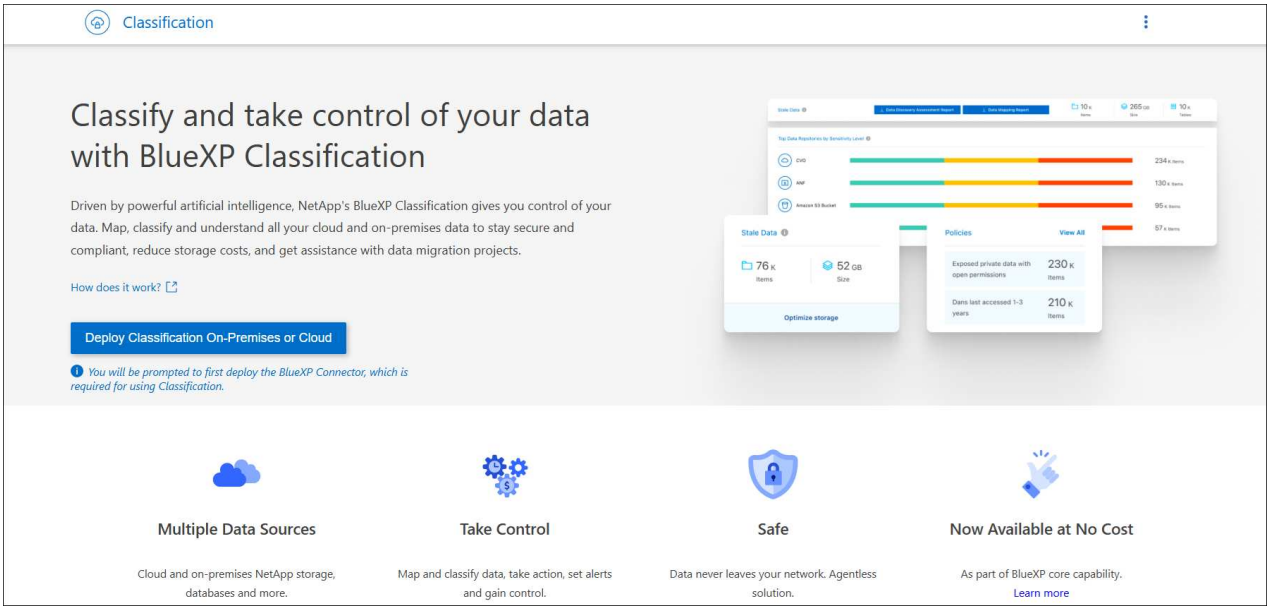
4. L'assistant affiche la progression au fur et à mesure des étapes de déploiement. Il s'arrête et vous invite à entrer s'il est en cours de problème.

5. Lorsque l'instance est déployée et que la BlueXP classification est installée, sélectionnez **Continuer vers la configuration** pour accéder à la page *Configuration*.

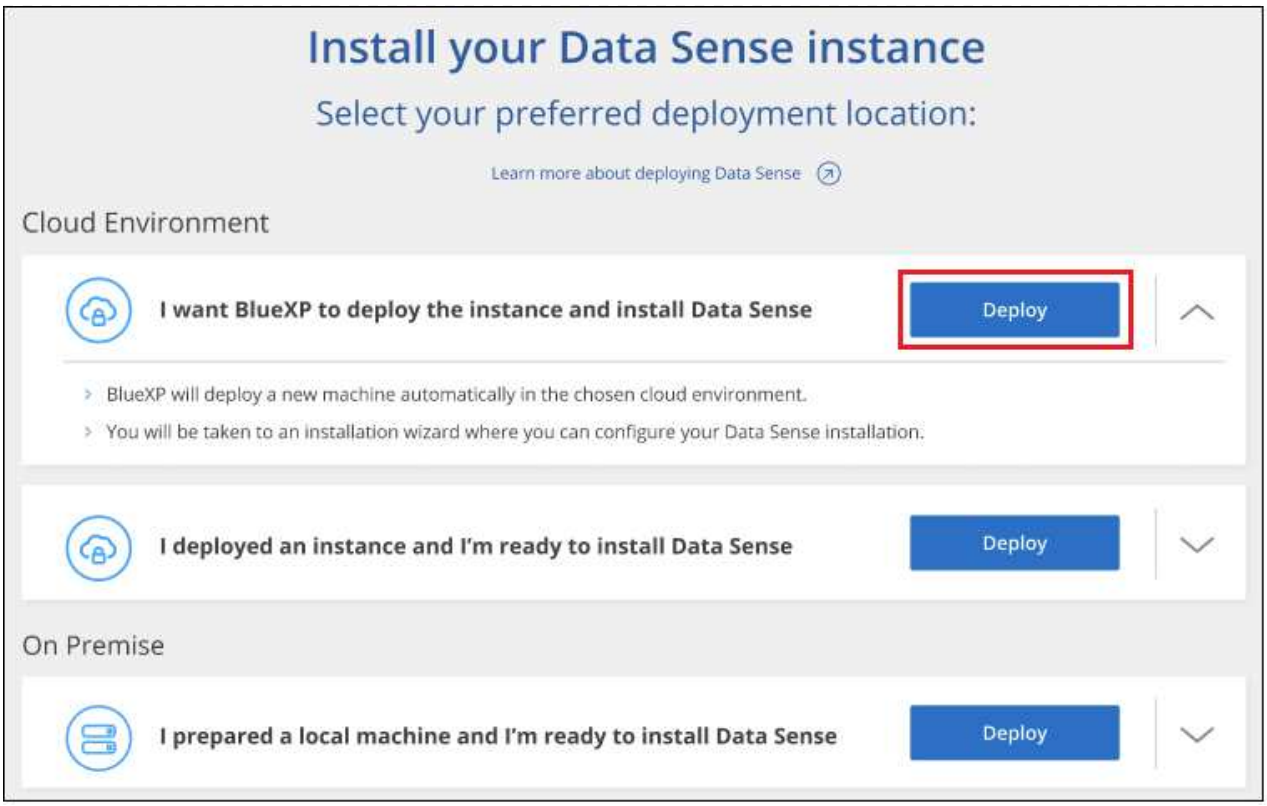
Déploiement dans Google Cloud

Étapes

1. Dans le menu de navigation de gauche BlueXP , sélectionnez **gouvernance > Classification**.
2. Sélectionnez **Déployer la classification sur site ou dans le cloud**.



3. Sélectionnez **Déployer** pour démarrer 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. Lorsque l'instance est déployée et que la BlueXP classification est installée, sélectionnez **Continuer vers 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.

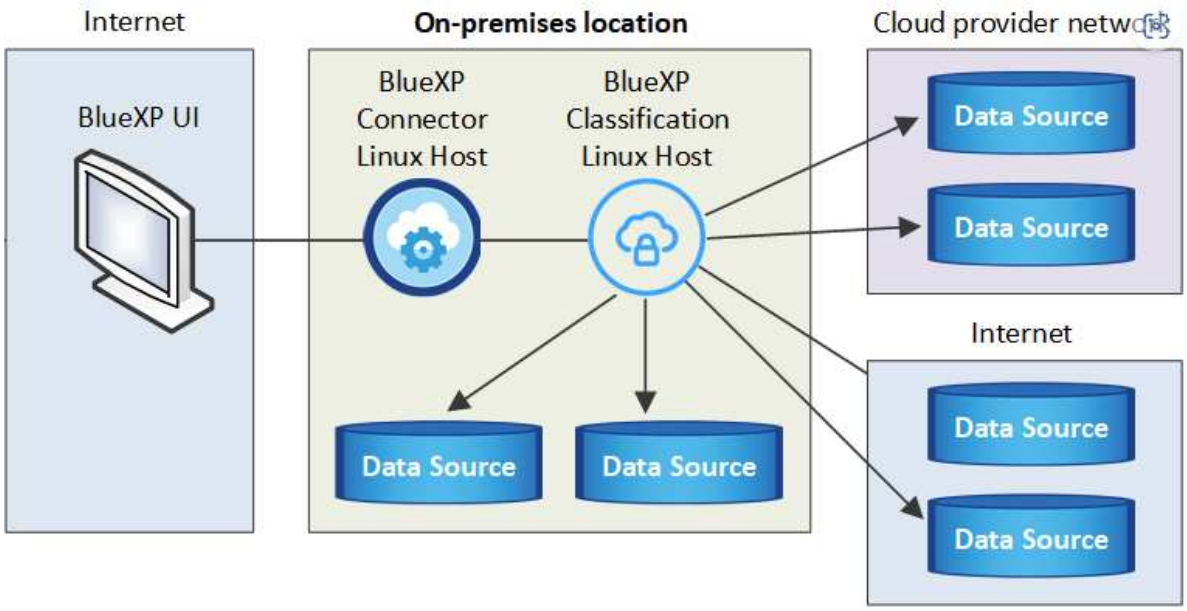
Installez la classification BlueXP sur un hôte disposant d'un accès Internet

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.

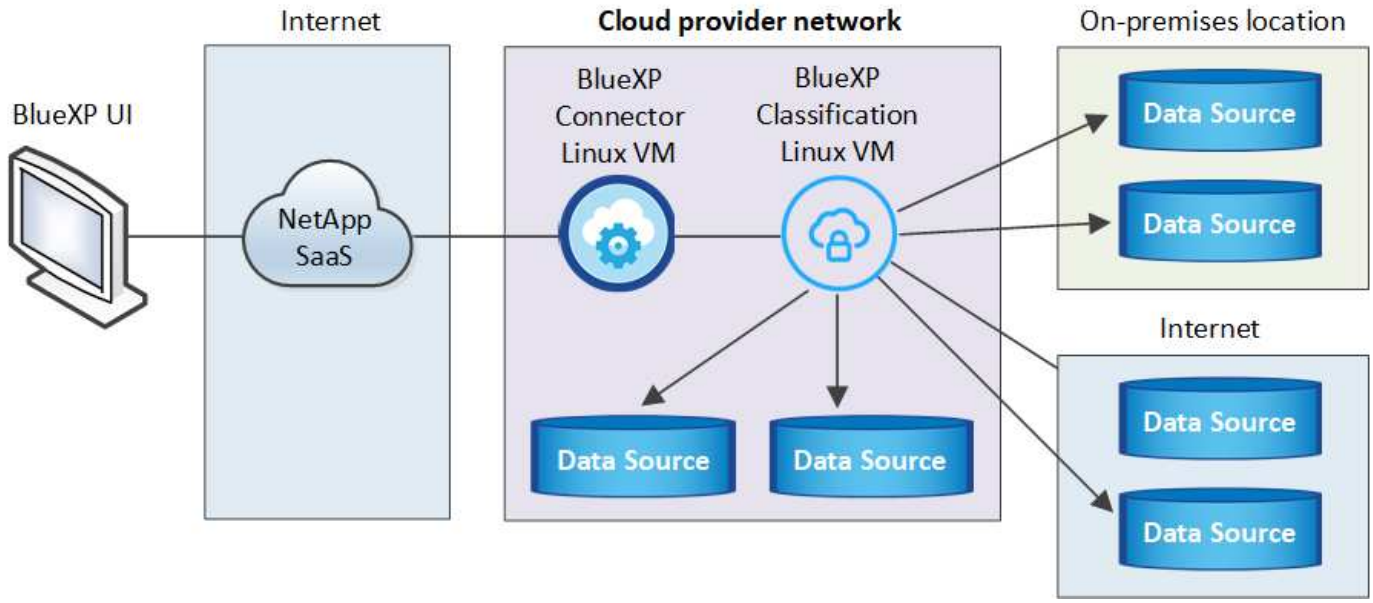
L'installation sur site peut être une bonne option si vous préférez analyser les systèmes ONTAP sur site à l'aide d'une instance de classification BlueXP également située sur site, mais ce n'est pas une exigence. Le logiciel fonctionne exactement de la même manière quelle que soit la méthode d'installation 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 versions héritées 1.30 et antérieures, si vous devez installer la classification BlueXP sur plusieurs hôtes, reportez-vous à la section "Installez la classification BlueXP sur plusieurs hôtes sans accès Internet".

Vous pouvez également "Installez la classification BlueXP sur un site qui ne dispose pas d'un accès Internet".

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.

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 :

- Lorsque vous analysez les données dans Cloud Volumes ONTAP dans AWS ou Amazon FSX pour ONTAP, 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.

Les systèmes ONTAP sur site, les partages de fichiers NetApp et les comptes de base de données peuvent être analysés 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.

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 parmi ces tailles de système, en fonction de la taille du dataset sur lequel vous prévoyez d'effectuer l'analyse de classification BlueXP.

Taille du système	CPU	RAM (la mémoire d'échange doit être désactivée)	Disque
Très grand	32 processeurs	128 GO DE RAM	• 1 Tio SSD sur / ou 100 Gio disponible sur /opt • 895 Gio disponible sur /var/lib/docker • 5 Gio sur /tmp • **Pour Podman, 5 Go sur /tmp** • **Pour Podman, 30 Go sur /var/tmp**
Grand	16 processeurs	64 GO DE RAM	• 500 Gio de SSD sur /, ou 100 Gio disponible pour /opt • 395 Gio disponible sur /var/lib/docker ou pour Podman /var/lib/containers ou pour Podman /var/lib/containers • 5 Gio sur /tmp • **Pour Podman, 5 Go sur /tmp** • **Pour Podman, 30 Go sur /var/tmp**

- 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 Amazon Elastic Compute Cloud (Amazon 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------`
/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

        - Ubuntu 22.04 (requiert la classification BlueXP version 1.23 ou supérieure)
        - Ubuntu 24.04 (nécessite 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 versions 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 et 9.6.
    - Les extensions vectorielles avancées (AVX2) doivent être activées sur le système hôte.
- **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".
        - Podman version 4 ou supérieure. Pour installer Podman, entrez (`sudo yum install podman 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.
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.

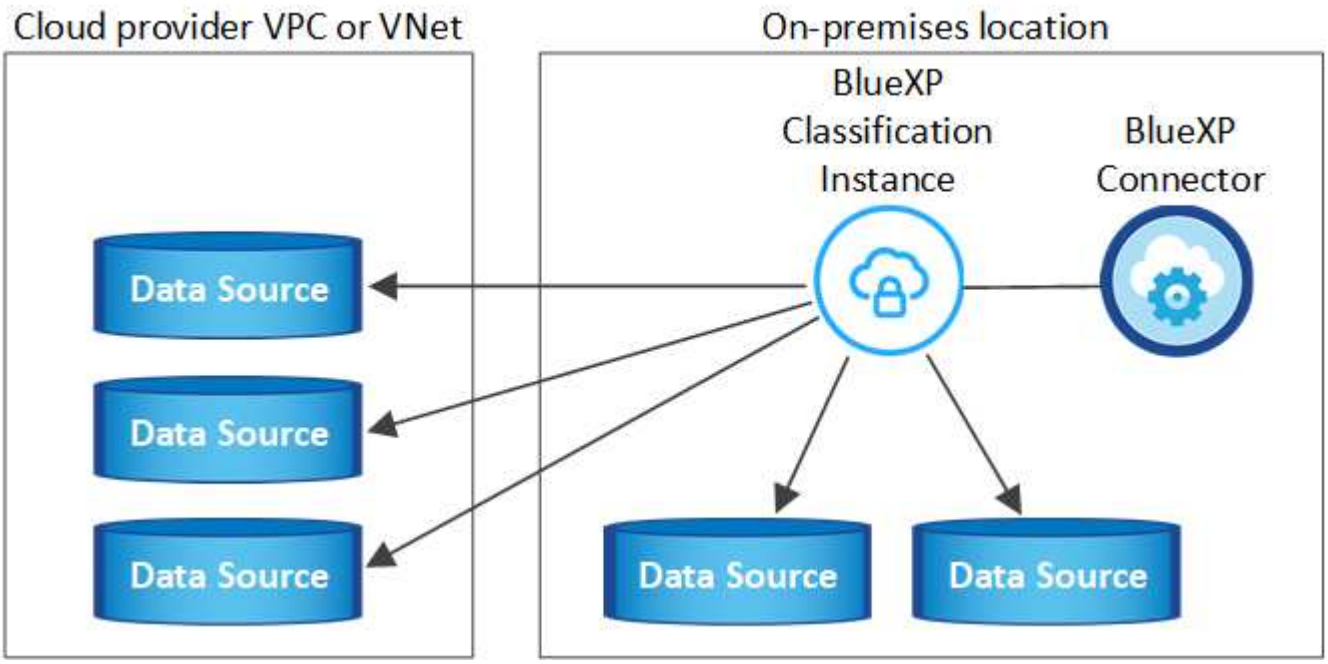
Type de connexion	Ports	Description
Classification de Connector <> BlueXP	8080 (TCP), 443 (TCP) et 80. 9000	Les règles de pare-feu ou de routage du connecteur doivent autoriser le trafic entrant et sortant via le port 443 vers et depuis l’instance de classification BlueXP. Assurez-vous que le port 8080 est ouvert pour voir la progression de l’installation dans BlueXP. Si un pare-feu est utilisé sur l’hôte Linux, le port 9000 est requis pour les processus internes d’un serveur Ubuntu.

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

Type de connexion	Ports	Description
Classification BlueXP <> Active Directory	389 (TCP ET UDP), 636 (TCP), 3268 (TCP) ET 3269 (TCP)	Un Active Directory doit déjà être configuré pour les utilisateurs de votre entreprise. De plus, la classification BlueXP requiert des informations d'identification Active Directory pour analyser les volumes CIFS. Vous devez disposer des informations pour Active Directory : • Adresse IP du serveur DNS ou adresses IP multiples • Nom d'utilisateur et mot de passe du serveur • Nom de domaine (nom Active Directory) • Que vous utilisiez ou non le protocole LDAP sécurisé (LDAPS) • Port serveur LDAP (généralement 389 pour LDAP et 636 pour LDAP sécurisé)

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.



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 savoir 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".

Avant de commencer

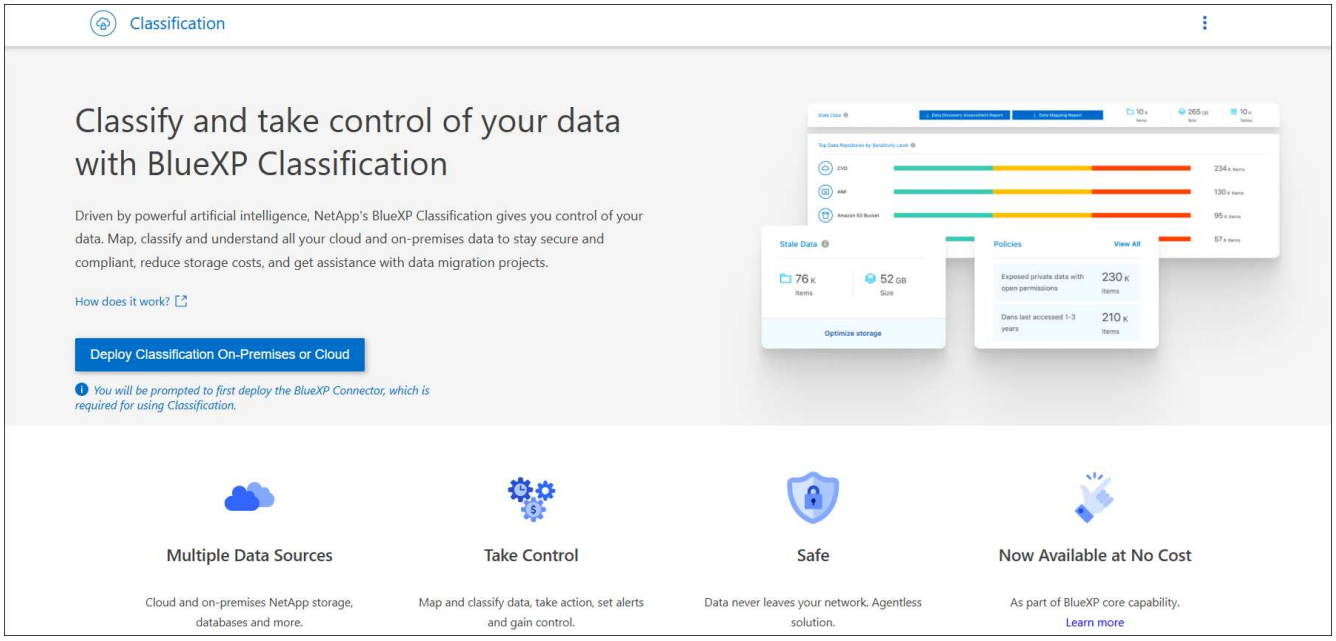
- Vérifiez que votre système Linux est conforme à la configuration requise pour l'hôte.
- Vérifiez que le système dispose des deux packages logiciels prérequis installés (Docker Engine ou Podman et Python 3).
- Assurez-vous que vous disposez des privilèges root sur le système Linux.
- Si vous utilisez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

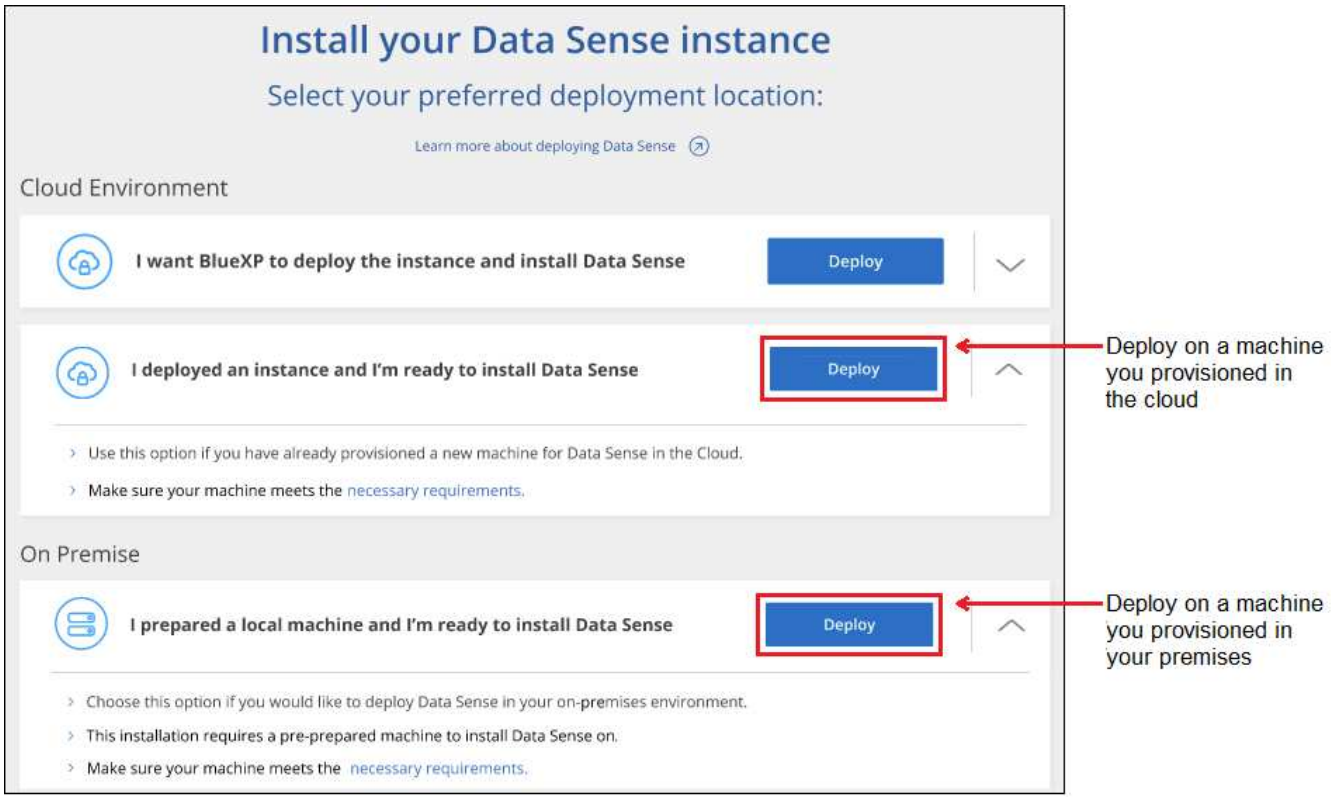
1. Téléchargez le logiciel de classification BlueXP depuis le "Site de support NetApp". Le fichier que vous devez sélectionner est nommé **DATASESNSE-INSTALLER-<version>.tar.gz**.
2. Copiez le fichier d'installation sur l'hôte Linux que vous envisagez d'utiliser (à l'aide de `scp` ou une autre méthode).
3. 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. Sélectionnez **Déployer la classification sur site ou dans le cloud**.



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 pour s'assurer que votre système et vos exigences 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 :
a. Collez la commande que vous avez copiée à partir de l'étape 7 : `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token>` Si vous installez sur une instance cloud (pas sur site), ajoutez `--manual-cloud-install <cloud_provider>`. 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. 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. 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.	Vous pouvez également créer l'ensemble de la commande à l'avance, en fournissant les paramètres d'hôte et de proxy nécessaires : `sudo ./install.sh -a <account_id> -c <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>`

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.

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, qui utilise un script d'installation, n'a pas de connectivité avec la couche SaaS BlueXP .

"Découvrez les différents modes de déploiement pour le connecteur BlueXP et la classification BlueXP".

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".

Pour les versions héritées 1.30 et antérieures, si vous devez installer la classification BlueXP sur plusieurs hôtes, reportez-vous à la section "Installez la classification BlueXP sur plusieurs hôtes sans accès Internet".

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

Il n'est actuellement pas possible de prendre en charge l'analyse des comptes Cloud Volumes ONTAP, Azure NetApp Files ou FSX pour ONTAP 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 :

- 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
- 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.

Installez le connecteur BlueXP

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

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.

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.

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 parmi ces tailles de système, en fonction de la taille du dataset sur lequel vous prévoyez d'effectuer l'analyse de classification BlueXP.

Taille du système	CPU	RAM (la mémoire d'échange doit être désactivée)	Disque
Très grand	32 processeurs	128 GO DE RAM	• 1 Tio SSD sur / ou 100 Gio disponible sur /opt • 895 Gio disponible sur /var/lib/docker • 5 Gio sur /tmp • **Pour Podman, 5 Go sur /tmp** • **Pour Podman, 30 Go sur /var/tmp**
Grand	16 processeurs	64 GO DE RAM	• 500 Gio de SSD sur /, ou 100 Gio disponible pour /opt • 395 Gio disponible sur /var/lib/docker ou pour Podman /var/lib/containers ou pour Podman /var/lib/containers • 5 Gio sur /tmp • **Pour Podman, 5 Go sur /tmp** • **Pour Podman, 30 Go sur /var/tmp**

- 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 Amazon Elastic Compute Cloud (Amazon 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------`
/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

        - Ubuntu 22.04 (requiert la classification BlueXP version 1.23 ou supérieure)
        - Ubuntu 24.04 (nécessite 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 versions 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 et 9.6.
    - Les extensions vectorielles avancées (AVX2) doivent être activées sur le système hôte.
- **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".
        - Podman version 4 ou supérieure. Pour installer Podman, entrez (`sudo yum install podman 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

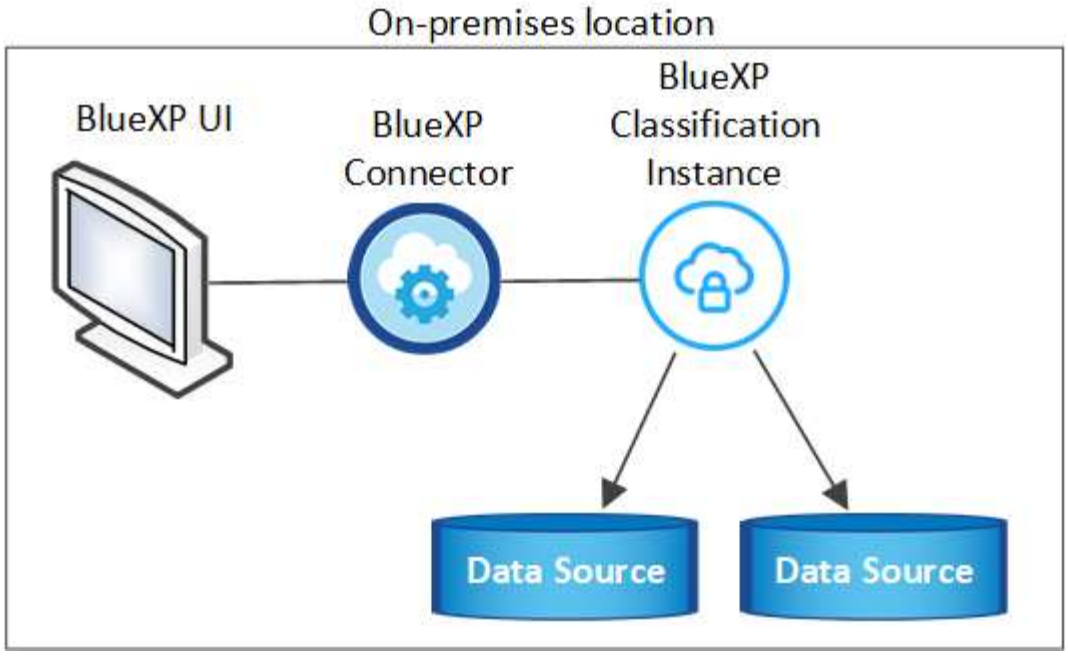
Vous devez vous assurer que tous les ports requis sont ouverts pour la communication entre le connecteur, la classification BlueXP, Active Directory et vos sources de données.

Type de connexion	Ports	Description
Classification de Connector <> BlueXP	8080 (TCP), 6000 (TCP), 443 (TCP) ET 80. 9000	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. • 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. • Si un pare-feu est utilisé sur l'hôte Linux, le port 9000 est requis pour les processus internes d'un serveur Ubuntu.
Connecteur <> cluster ONTAP (NAS)	443 (TCP)	BlueXP détecte les clusters ONTAP via HTTPS. Si vous utilisez des stratégies de pare-feu personnalisées, elles doivent répondre aux exigences suivantes : • L'hôte du connecteur doit autoriser l'accès HTTPS sortant via le port 443. Si le connecteur est dans le Cloud, toutes les communications sortantes sont autorisées par le groupe de sécurité prédéfini. • Le cluster ONTAP doit autoriser l'accès HTTPS entrant via le port 443. La stratégie de pare-feu " mgmt " par défaut permet l'accès HTTPS entrant à partir de toutes les adresses IP. Si vous avez modifié cette stratégie par défaut ou si vous avez créé votre propre stratégie de pare-feu, vous devez associer le protocole HTTPS à cette politique et activer l'accès à partir de l'hôte du connecteur.

Type de connexion	Ports	Description
Classification BlueXP <> cluster ONTAP	• Pour NFS - 111 (TCP/UDP) et 2049 (TCP/UDP) • Pour CIFS - 139 (TCP/UDP) et 445 (TCP/UDP)	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. Assurez-vous que les ports suivants sont ouverts pour l'instance de classification BlueXP : • Pour NFS - 111 et 2049 • Pour CIFS : 139 et 445 Les règles d'exportation des volumes NFS doivent autoriser l'accès à partir de l'instance de classification BlueXP.
Classification BlueXP <> Active Directory	389 (TCP ET UDP), 636 (TCP), 3268 (TCP) ET 3269 (TCP)	Un Active Directory doit déjà être configuré pour les utilisateurs de votre entreprise. De plus, la classification BlueXP requiert des informations d'identification Active Directory pour analyser les volumes CIFS. Vous devez disposer des informations pour Active Directory : • Adresse IP du serveur DNS ou adresses IP multiples • Nom d'utilisateur et mot de passe du serveur • Nom de domaine (nom Active Directory) • Que vous utilisiez ou non le protocole LDAP sécurisé (LDAPS) • Port serveur LDAP (généralement 389 pour LDAP et 636 pour LDAP sécurisé)
Si un pare-feu est utilisé sur un hôte Linux	9000	Nécessaire pour les processus internes au sein d'un serveur Ubuntu.

Installez la classification BlueXP sur l'hôte Linux sur site

Pour les configurations standard, le logiciel est installé sur un système hôte unique.



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".

Avant de commencer

- 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 :

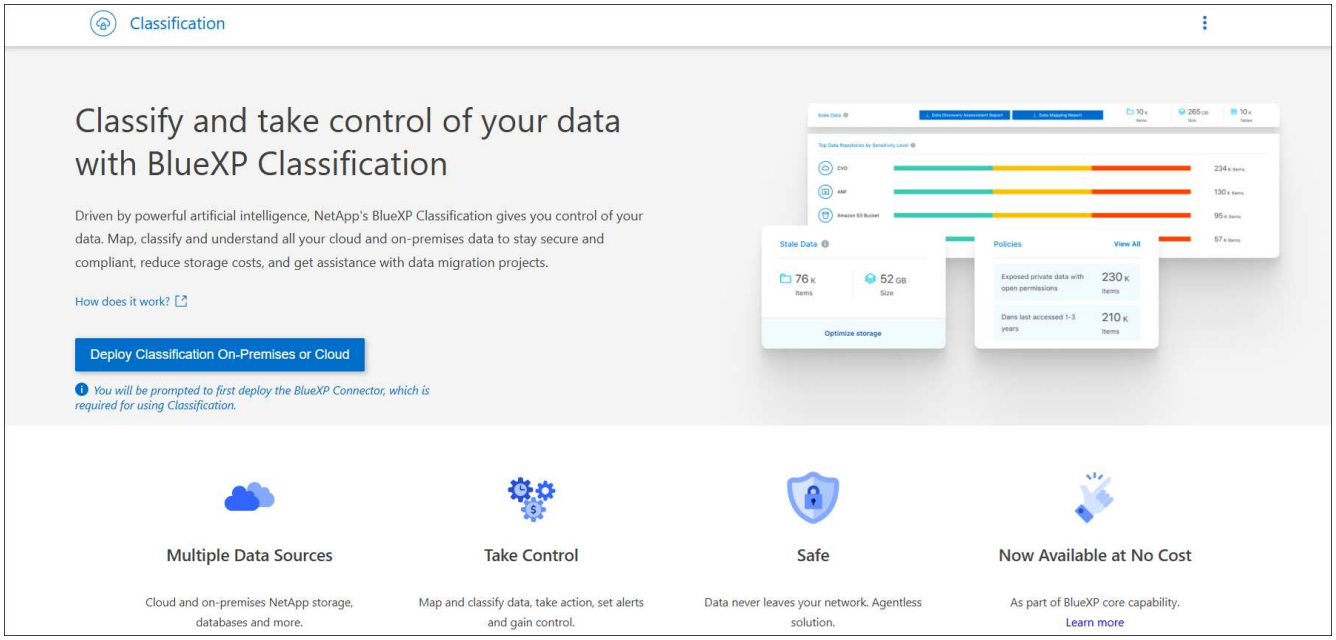
   ```
   tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
   ```

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

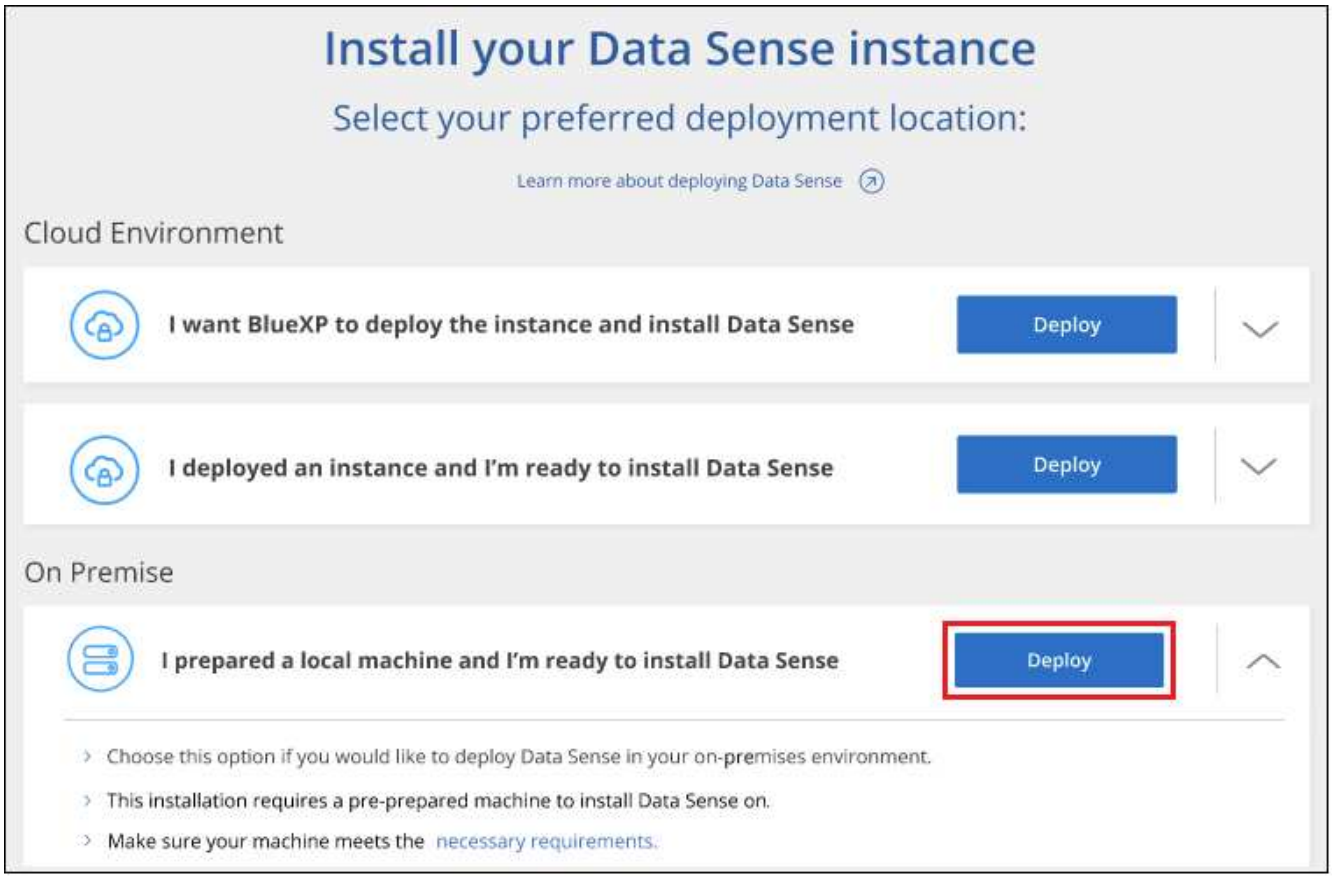
4. Décompressez le fichier d'installation sur la machine hôte, par exemple :

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

5. Lancez BlueXP et sélectionnez **gouvernance > Classification**.
6. Sélectionnez **Déployer la classification sur site ou dans le cloud**.



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 :
a. Collez les informations que vous avez copiées à partir de l'étape 8 : `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --darksite` 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. 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.	Vous pouvez également créer la commande entière à l'avance, en fournissant les paramètres d'hôte nécessaires : `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> --no-proxy --darksite`

   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.

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

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 le bundle logiciel sur l'hôte Linux où la classification BlueXP est installée sur le site invisible.
3. 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.

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, exécutez éventuellement un script sur l'hôte pour vérifier que toutes les conditions préalables sont

en place pour l'installation de la classification BlueXP . 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 parmi ces tailles de système, en fonction de la taille du dataset sur lequel vous prévoyez d'effectuer l'analyse de classification BlueXP.

Taille du système	CPU	RAM (la mémoire d'échange doit être désactivée)	Disque
Très grand	32 processeurs	128 GO DE RAM	• 1 Tio SSD sur / ou 100 Gio disponible sur /opt • 895 Gio disponible sur /var/lib/docker • 5 Gio sur /tmp • **Pour Podman, 5 Go sur /tmp** • **Pour Podman, 30 Go sur /var/tmp**
Grand	16 processeurs	64 GO DE RAM	• 500 Gio de SSD sur /, ou 100 Gio disponible pour /opt • 395 Gio disponible sur /var/lib/docker ou pour Podman /var/lib/containers ou pour Podman /var/lib/containers • 5 Gio sur /tmp • **Pour Podman, 5 Go sur /tmp** • **Pour Podman, 30 Go sur /var/tmp**

- 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 Amazon Elastic Compute Cloud (Amazon 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------`
/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

        - Ubuntu 22.04 (requiert la classification BlueXP version 1.23 ou supérieure)
        - Ubuntu 24.04 (nécessite 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 versions 8.8, 8.10, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5 et 9.6.
    - Les extensions vectorielles avancées (AVX2) doivent être activées sur le système hôte.
- **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".
        - Podman version 4 ou supérieure. Pour installer Podman, entrez (`sudo yum install podman 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://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.
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. 9000	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. Si un pare-feu est utilisé sur l'hôte Linux, le port 9000 est requis pour les processus internes d'un serveur Ubuntu.
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.

Avant de commencer

- 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.

Activez la numérisation sur vos sources de données

Analyser les sources de données avec la classification BlueXP

La classification BlueXP scrute les données des référentiels (les volumes, les schémas de base de données ou autres données utilisateur) que vous sélectionnez pour identifier les données personnelles et sensibles. La classification BlueXP mappe ensuite vos données d'entreprise, classe chaque fichier et identifie des modèles prédéfinis dans les données. Le résultat de l'analyse est un index des informations personnelles, des données personnelles sensibles, des catégories de données et des types de fichiers.

Après l'analyse initiale, la classification BlueXP analyse en continu vos données selon une séquence périodique pour détecter les modifications incrémentielles. C'est pourquoi il est important de maintenir l'instance en cours d'exécution.

Vous pouvez activer et désactiver les analyses au niveau du volume ou au niveau du schéma de la base de données.

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

Vous pouvez effectuer deux types d'acquisitions dans la classification BlueXP :

- **Les acquisitions cartographiques uniquement** ne fournissent qu'une vue d'ensemble de haut niveau de vos données et sont effectuées sur des sources de données sélectionnées. Les analyses de mappage uniquement prennent moins de temps que les analyses de mappage et de classification car elles n'accèdent pas aux fichiers pour voir les données qu'elles contiennent. Vous pouvez commencer par identifier les domaines de recherche, puis effectuer une analyse carte et classification sur ces domaines.
- **Cartographiez et classifiez les acquisitions** fournissent une analyse de niveau profond de vos données.

Le tableau ci-dessous présente certaines des différences :

Fonction	Cartographiez et classez les analyses	Analyses de mappage uniquement
Vitesse de numérisation	Lentes	Rapides
Tarifs	Libre	Libre
Puissance	Limité à 500 Tio*	Limité à 500 Tio*
Liste des types de fichiers et de la capacité utilisée	Oui.	Oui.
Nombre de fichiers et capacité utilisée	Oui.	Oui.
Âge et taille des fichiers	Oui.	Oui.
Possibilité d'exécuter un "Rapport de mappage de données"	Oui.	Oui.
Page Data Investigation pour afficher les détails du fichier	Oui.	Non
Rechercher des noms dans les fichiers	Oui.	Non

Fonction	Cartographiez et classez les analyses	Analyses de mappage uniquement
Créer "recherches enregistrées" qui fournit des résultats de recherche personnalisés	Oui.	Non
Possibilité d'exécuter d'autres rapports	Oui.	Non
Possibilité de voir les métadonnées des fichiers*	Non	Oui.

{astérisque} include::_include/connector-limit.adoc[]

*Les métadonnées suivantes sont extraites des fichiers lors des analyses de mappage :

- Environnement de travail
- Type d'environnement de travail
- Référentiel de stockage
- Type de fichier
- Capacité utilisée
- Nombre de fichiers
- Taille du fichier
- Création de fichier
- Dernier accès au fichier
- Dernier fichier modifié
- Heure de découverte du fichier
- Extraction des autorisations

Différences entre les tableaux de bord de gouvernance :

Fonction	Cartographiez et classez	Carte
Les données obsolètes	Oui.	Oui.
Données non commerciales	Oui.	Oui.
Fichiers dupliqués	Oui.	Oui.
Recherches enregistrées prédéfinies	Oui.	Non
Recherches enregistrées par défaut	Oui.	Oui.
Rapport DDA	Oui.	Oui.
Rapport de mappage	Oui.	Oui.
Détection du niveau de sensibilité	Oui.	Non
Données sensibles avec autorisations étendues	Oui.	Non
Ouvrez les autorisations	Oui.	Oui.
Âge des données	Oui.	Oui.
Taille des données	Oui.	Oui.
Catégories	Oui.	Non
Types de fichiers	Oui.	Oui.

Différences du tableau de bord de conformité :

Fonction	Cartographiez et classez	Carte
Informations personnelles	Oui.	Non
Informations personnelles sensibles	Oui.	Non
Rapport sur l’évaluation des risques en matière de confidentialité	Oui.	Non
Rapport HIPAA	Oui.	Non
Rapport PCI DSS	Oui.	Non

Différences entre les filtres d'investigation :

Fonction	Cartographiez et classez	Carte
Recherches enregistrées	Oui.	Oui.
Type d'environnement de travail	Oui.	Oui.
Environnement de travail	Oui.	Oui.
Référentiel de stockage	Oui.	Oui.
Type de fichier	Oui.	Oui.
Taille du fichier	Oui.	Oui.
Heure de création	Oui.	Oui.
Heure découverte	Oui.	Oui.
Dernière modification	Oui.	Oui.
Dernier accès	Oui.	Oui.
Ouvrez les autorisations	Oui.	Oui.
Chemin du répertoire de fichiers	Oui.	Oui.
Catégorie	Oui.	Non
Niveau de sensibilité	Oui.	Non
Nombre d'identificateurs	Oui.	Non
Données personnelles	Oui.	Non
Données personnelles sensibles	Oui.	Non
Sujet des données	Oui.	Non
Doublons	Oui.	Oui.
Statut de classification	Oui.	Le statut est toujours « informations limitées »
Événement d'analyse d'acquisition	Oui.	Oui.
Hachage de fichier	Oui.	Oui.
Nombre d'utilisateurs ayant accès	Oui.	Oui.
Autorisations utilisateur/groupe	Oui.	Oui.
Propriétaire du fichier	Oui.	Oui.
Type de répertoire	Oui.	Oui.

La rapidité avec laquelle la classification BlueXP analyse les données

La vitesse de analyse est affectée par la latence du réseau, la latence des disques, la bande passante réseau, la taille de l'environnement et la taille de la distribution de fichiers.

- Lors de l'exécution d'acquisitions de mappage uniquement, la classification BlueXP peut analyser entre

100-150 Tibs de données par jour.

- Lors d'analyses de cartes et de classifications, la classification BlueXP peut analyser entre 15-40 000 Tibs de données par jour.

Analysez les volumes Azure NetApp Files avec la classification BlueXP

Suivez ces étapes pour commencer à utiliser la classification BlueXP pour Azure NetApp Files.

Découvrez le système Azure NetApp Files que vous souhaitez analyser

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

"Découvrez comment découvrir le système Azure NetApp Files dans BlueXP".

Déployez l'instance de classification BlueXP

"Déployez la classification BlueXP" si aucune instance n'est déjà déployée.

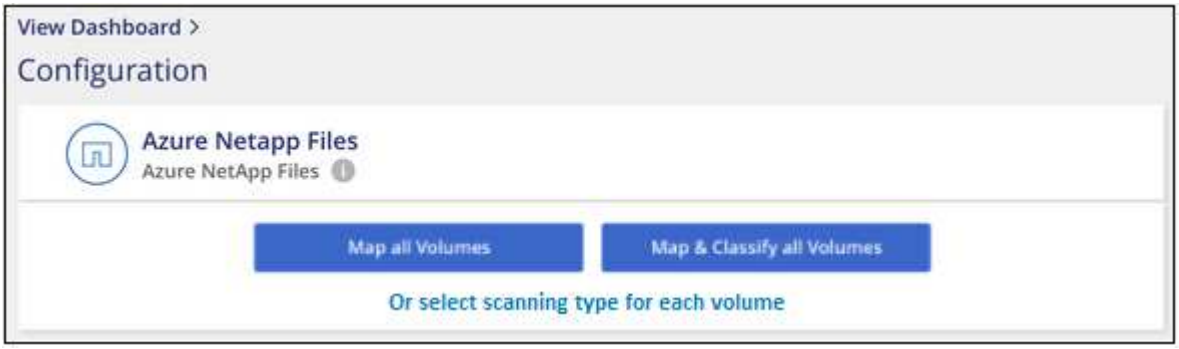
La classification BlueXP doit être déployée dans le cloud lors de l'analyse des volumes Azure NetApp Files et doit être déployée dans la même région que les volumes à analyser.

Remarque : le déploiement de la classification BlueXP dans un emplacement sur site n'est actuellement pas pris en charge lors de l'analyse des volumes Azure NetApp Files.

Activez la classification BlueXP dans vos environnements de travail

Vous pouvez activer la classification BlueXP sur vos volumes Azure NetApp Files.

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



3. Sélectionnez le mode de numérisation des volumes dans chaque environnement de travail. "En savoir plus sur les acquisitions de mappage et de classification":
   - Pour mapper tous les volumes, sélectionnez **Mapper tous les volumes**.
   - Pour mapper et classer tous les volumes, sélectionnez **Mapper et classer tous les volumes**.
   - Pour personnaliser le balayage de chaque volume, sélectionnez **ou sélectionnez le type de balayage pour chaque volume**, puis choisissez les volumes à mapper et/ou classer.

     Voir Activer et désactiver les analyses de conformité sur les volumes pour plus de détails.

4. Dans la boîte de dialogue de confirmation, sélectionnez **Approve** pour que la classification BlueXP commence à analyser vos volumes.

Résultat

La classification BlueXP démarre l'analyse des volumes sélectionnés dans l'environnement de travail. Les résultats seront disponibles dans le tableau de bord de conformité dès que les analyses initiales seront terminées par la classification BlueXP. Le temps nécessaire dépend de la quantité de données—il peut être de quelques minutes ou heures. Vous pouvez suivre la progression de l'acquisition initiale en accédant au menu **Configuration** puis en sélectionnant la **Configuration de l'environnement de travail**. La progression de chaque acquisition est affichée sous la forme d'une barre de progression. Vous pouvez également passer le curseur de la souris sur la barre de progression pour voir le nombre de fichiers analysés par rapport au nombre total de fichiers dans le volume.

- Par défaut, si la classification BlueXP ne dispose pas d'autorisations d'attributs d'écriture dans CIFS ou d'autorisations d'écriture dans NFS, le système ne analyse pas les fichiers de vos volumes. En effet, la classification BlueXP ne peut pas rétablir l'heure du dernier accès à l'heure d'origine. Si vous ne vous souciez pas de réinitialiser l'heure du dernier accès, cliquez sur **ou sélectionnez le type de numérisation pour chaque volume**. La page résultante dispose d'un paramètre que vous pouvez activer afin que la classification BlueXP analyse les volumes indépendamment des autorisations.
- La classification BlueXP analyse un seul partage de fichiers sous un volume. Si vous avez plusieurs partages dans vos volumes, vous devrez analyser ces autres partages séparément en tant que groupe de partages. "Pour en savoir plus sur cette limitation de classification BlueXP, consultez".

Vérifiez que la classification BlueXP a accès aux volumes

Assurez-vous que la classification BlueXP peut accéder aux volumes en vérifiant votre réseau, vos groupes de sécurité et vos règles d'exportation. Vous devez fournir une classification BlueXP avec des informations d'identification CIFS pour pouvoir accéder aux volumes CIFS.

Pour Azure NetApp Files, la classification BlueXP ne peut analyser que les volumes situés dans la même région que BlueXP.

Étapes

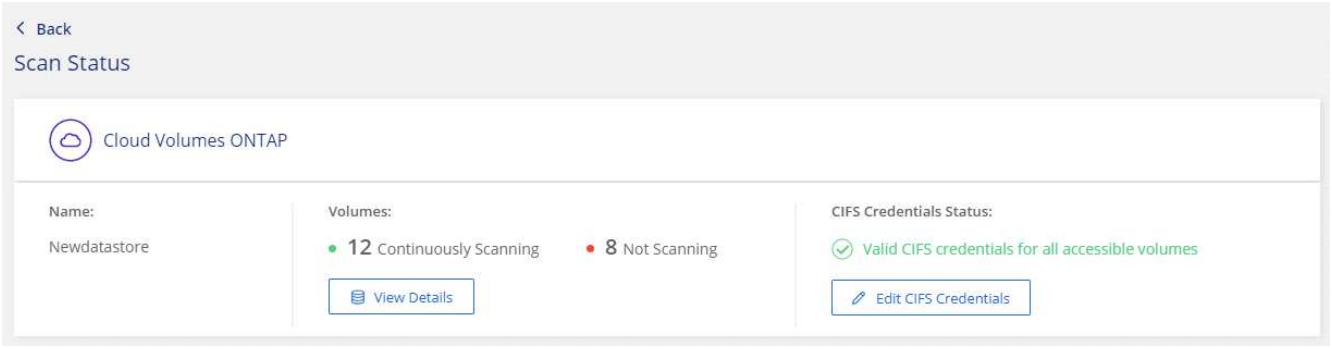
1. Assurez-vous qu'il existe une connexion réseau entre l'instance de classification BlueXP et chaque réseau incluant des volumes pour Azure NetApp Files.
2. Assurez-vous que les ports suivants sont ouverts pour l'instance de classification BlueXP :
   - Pour NFS – ports 111 et 2049.
   - Pour CIFS – ports 139 et 445.
3. Assurez-vous que les règles d'exportation du volume NFS incluent l'adresse IP de l'instance de classification BlueXP afin qu'elle puisse accéder aux données de chaque volume.
4. Si vous utilisez CIFS, fournissez la classification BlueXP avec les informations d'identification Active Directory pour qu'il puisse analyser les volumes CIFS.
   a. Dans le menu de navigation de gauche BlueXP , sélectionnez **gouvernance > Classification**.
5. Dans le menu BlueXP Classification, sélectionnez **Configuration**.

a. Pour chaque environnement de travail, sélectionnez **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe dont la classification BlueXP a besoin pour accéder aux volumes CIFS du système.

   Les identifiants peuvent être en lecture seule, mais il est possible de fournir des identifiants d'administrateur pour que la classification BlueXP puisse lire toutes les données qui nécessitent des autorisations élevées. Les identifiants sont stockés sur l'instance de classification BlueXP.

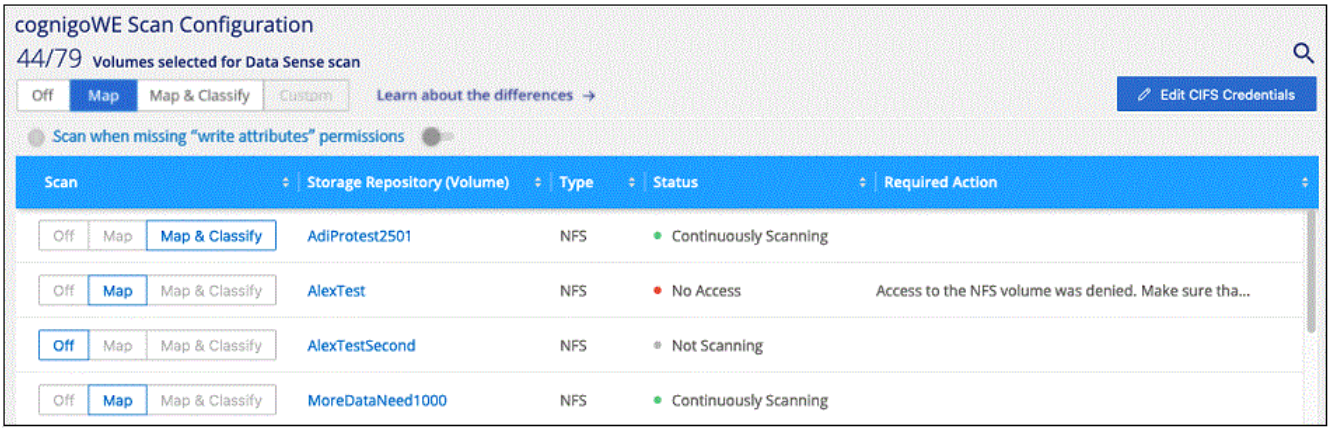
   Pour garantir que les analyses de BlueXP classification ne modifient pas les « derniers accès » de vos fichiers, il est recommandé que l'utilisateur dispose des autorisations d'écriture sur les attributs dans CIFS ou NFS. Si possible, configurez l'utilisateur Active Directory comme membre d'un groupe parent de l'organisation disposant d'autorisations sur tous les fichiers.

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



6. Sur la page Configuration, sélectionnez **Afficher les détails** pour vérifier l'état de chaque volume CIFS et NFS et corriger les erreurs éventuelles.

   Par exemple, l'image suivante montre quatre volumes, dont l'un ne peut pas être scanné dans la classification BlueXP en raison de problèmes de connectivité réseau entre l'instance de classification BlueXP et le volume.

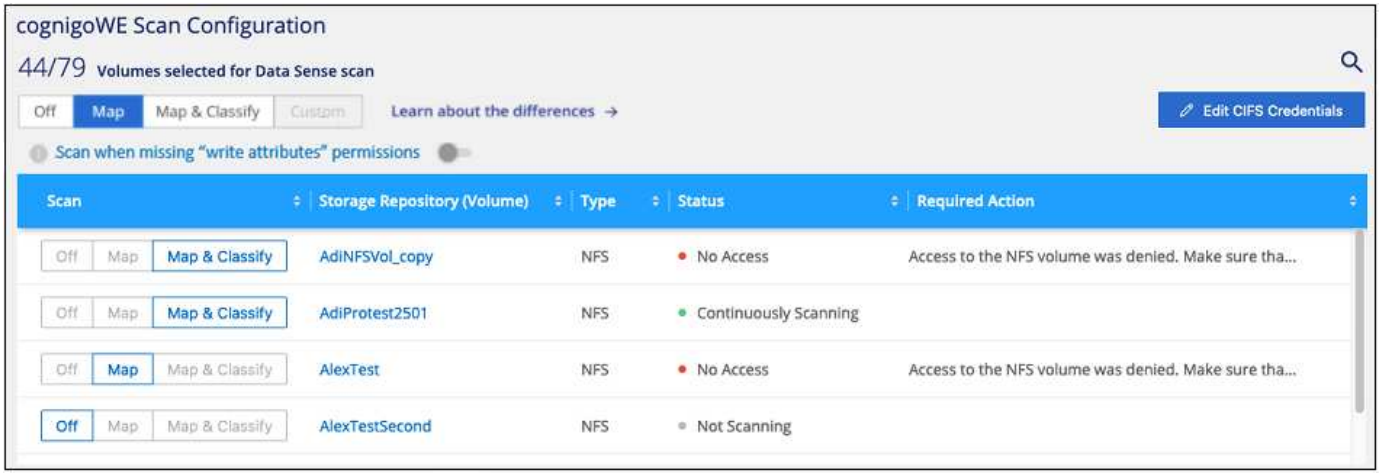


Activer et désactiver les analyses de conformité sur les volumes

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

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

Le commutateur en haut de la page pour **Scan en cas d'autorisations d'écriture d'attributs manquantes** est désactivé par défaut. Cela signifie que si la classification BlueXP ne dispose pas d'autorisations d'attributs d'écriture dans CIFS ou d'autorisations d'écriture dans NFS, le système ne analyse pas les fichiers car la classification BlueXP ne peut pas rétablir l'heure du dernier accès à l'horodatage d'origine. Si vous ne vous souciez pas de la réinitialisation de l'heure du dernier accès, activez le commutateur et tous les fichiers sont analysés, quelles que soient les autorisations. "En savoir plus >>".



Étapes

1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Effectuez l'une des opérations suivantes :
   - Pour activer les acquisitions de mappage uniquement sur un volume, dans la zone de volume,

sélectionnez **Map**. Pour activer sur tous les volumes, dans la zone d'en-tête, sélectionnez **carte**.

- Pour activer la numérisation complète sur un volume, dans la zone de volume, sélectionnez **carte et classement**. Pour activer sur tous les volumes, dans la zone d'en-tête, sélectionnez **carte et classement**.
- Pour désactiver la numérisation sur un volume, dans la zone de volume, sélectionnez **Désactivé**. Pour désactiver la numérisation sur tous les volumes, dans la zone Cap, sélectionnez **Désactivé**.

Analysez les volumes Amazon FSX pour ONTAP avec la classification BlueXP

Suivez ces étapes pour commencer à analyser le volume Amazon FSX pour ONTAP avec la classification BlueXP.

Avant de commencer

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

  "Groupes de sécurité AWS pour les instances Linux"

  "Groupes de sécurité AWS pour les instances Windows"

  "Interfaces réseau flexibles AWS (ENI)"

- Assurez-vous que les ports suivants sont ouverts pour l'instance de classification BlueXP :
  - Pour NFS – ports 111 et 2049.
  - Pour CIFS – ports 139 et 445.

Déployez l'instance de classification BlueXP

"Déployez la classification BlueXP" si aucune instance n'est déjà déployée.

Vous devez déployer la classification BlueXP dans le même réseau AWS que le connecteur pour AWS et les volumes FSX que vous souhaitez analyser.

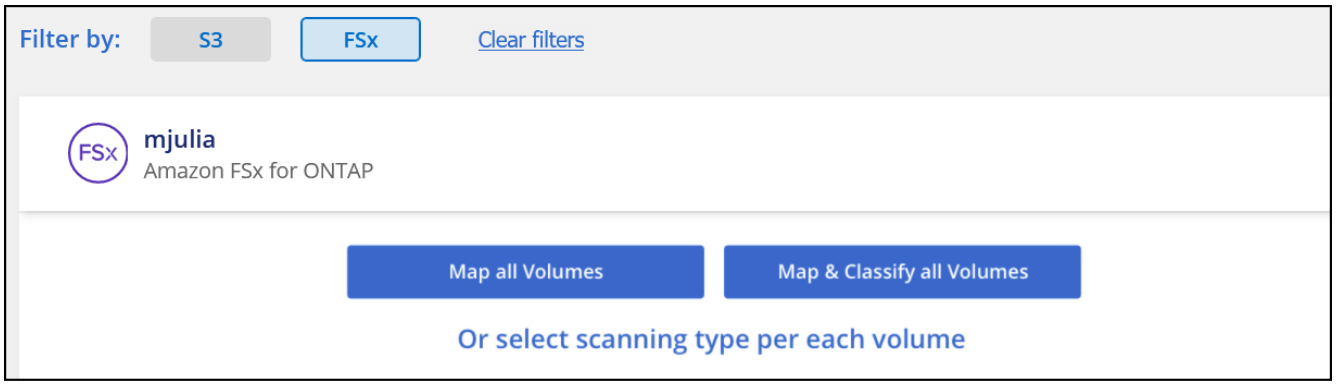
Remarque : le déploiement de la classification BlueXP dans un emplacement sur site n'est actuellement pas pris en charge lors de l'analyse des volumes FSX.

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

Activez la classification BlueXP dans vos environnements de travail

Vous pouvez activer la classification BlueXP pour les volumes FSX pour ONTAP.

1. Dans le menu de navigation de gauche BlueXP , sélectionnez **gouvernance > Classification**.
2. Dans le menu BlueXP Classification, sélectionnez **Configuration**.



3. Sélectionnez le mode de numérisation des volumes dans chaque environnement de travail. "En savoir plus sur les acquisitions de mappage et de classification":
   - Pour mapper tous les volumes, cliquez sur **mapper tous les volumes**.
   - Pour mapper et classer tous les volumes, cliquez sur **cartographier et classer tous les volumes**.
   - Pour personnaliser la numérisation de chaque volume, cliquez sur **ou sélectionnez le type de numérisation pour chaque volume**, puis choisissez les volumes que vous souhaitez mapper et/ou classer.
4. Dans la boîte de dialogue de confirmation, cliquez sur **Approve** pour que la classification BlueXP commence à analyser vos volumes.

Résultat

La classification BlueXP démarre l'analyse des volumes sélectionnés dans l'environnement de travail. Les résultats seront disponibles dans le tableau de bord de conformité dès que les analyses initiales seront terminées par la classification BlueXP. Le temps nécessaire dépend de la quantité de données—il peut être de quelques minutes ou heures. Vous pouvez suivre la progression de l'acquisition initiale en accédant au menu **Configuration** puis en sélectionnant la **Configuration de l'environnement de travail**. La progression de chaque acquisition est affichée sous la forme d'une barre de progression. Vous pouvez également passer le curseur de la souris sur la barre de progression pour voir le nombre de fichiers analysés par rapport au nombre total de fichiers dans le volume.

- Par défaut, si la classification BlueXP ne dispose pas d'autorisations d'attributs d'écriture dans CIFS ou d'autorisations d'écriture dans NFS, le système ne analyse pas les fichiers de vos volumes. En effet, la classification BlueXP ne peut pas rétablir l'heure du dernier accès à l'heure d'origine. Si vous ne vous souciez pas de réinitialiser l'heure du dernier accès, cliquez sur **ou sélectionnez le type de numérisation pour chaque volume**. La page résultante dispose d'un paramètre que vous pouvez activer afin que la classification BlueXP analyse les volumes indépendamment des autorisations.
- La classification BlueXP analyse un seul partage de fichiers sous un volume. Si vous avez plusieurs partages dans vos volumes, vous devrez analyser ces autres partages séparément en tant que groupe de partages. "Pour en savoir plus sur cette limitation de classification BlueXP, consultez".

Vérifiez que la classification BlueXP a accès aux volumes

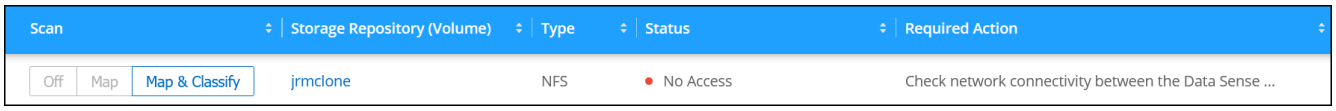
Assurez-vous que la classification BlueXP peut accéder aux volumes en vérifiant votre réseau, vos groupes de sécurité et vos règles d'exportation.

Vous devez fournir une classification BlueXP avec des informations d'identification CIFS pour pouvoir accéder aux volumes CIFS.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Sur la page Configuration, sélectionnez **Afficher les détails** pour vérifier l'état et corriger les erreurs éventuelles.

   Par exemple, l'image suivante montre qu'une classification de volume BlueXP ne peut pas analyser en raison de problèmes de connectivité réseau entre l'instance de classification BlueXP et le volume.



3. Assurez-vous qu'il existe une connexion réseau entre l'instance de classification BlueXP et chaque réseau incluant des volumes pour FSX pour ONTAP.

   Dans le cas de FSX pour ONTAP, la classification BlueXP ne peut analyser les volumes que dans la même région que BlueXP.

4. Assurez-vous que les règles d'exportation des volumes NFS incluent l'adresse IP de l'instance de classification BlueXP afin qu'elle puisse accéder aux données de chaque volume.
5. Si vous utilisez CIFS, fournissez la classification BlueXP avec les informations d'identification Active Directory pour qu'il puisse analyser les volumes CIFS.

   a. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
   b. Pour chaque environnement de travail, sélectionnez **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe dont la classification BlueXP a besoin pour accéder aux volumes CIFS du système.

      Les identifiants peuvent être en lecture seule, mais il est possible de fournir des identifiants d'administrateur pour que la classification BlueXP puisse lire toutes les données qui nécessitent des autorisations élevées. Les identifiants sont stockés sur l'instance de classification BlueXP.

      Pour garantir que les analyses de BlueXP classification ne modifient pas les « derniers accès » de vos fichiers, il est recommandé que l'utilisateur dispose des autorisations d'écriture sur les attributs dans CIFS ou NFS. Si possible, configurez l'utilisateur Active Directory comme membre d'un groupe parent de l'organisation disposant d'autorisations sur tous les fichiers.

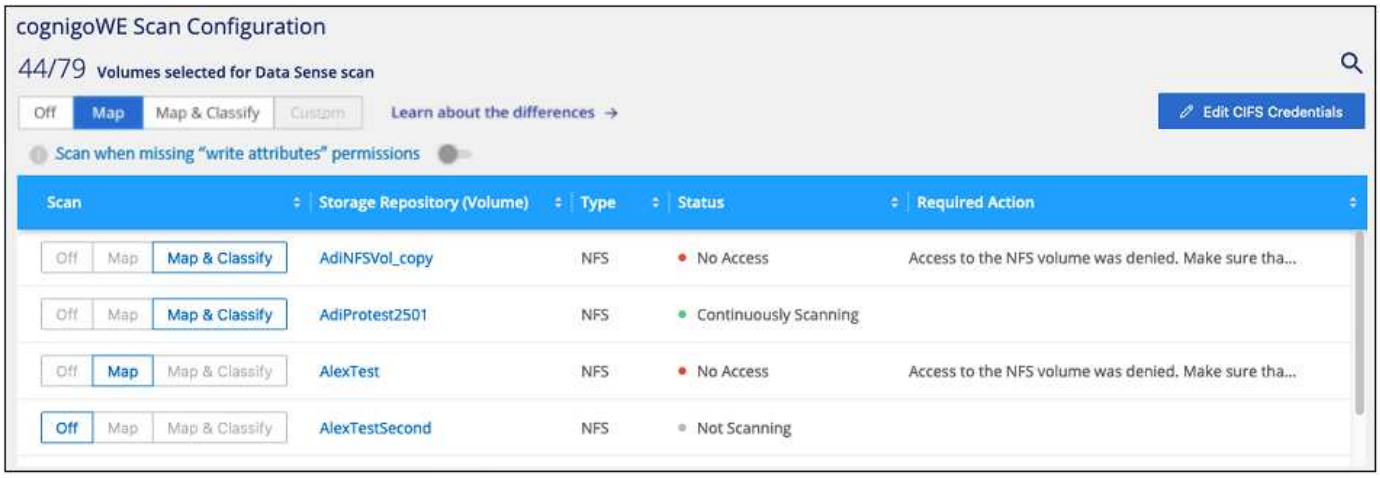
   Une fois les informations d'identification saisies, un message indiquant que tous les volumes CIFS ont été authentifiés avec succès s'affiche.

Activer et désactiver les analyses de conformité sur les volumes

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

Le commutateur en haut de la page pour **Scan en cas d'autorisations d'écriture d'attributs manquantes** est désactivé par défaut. Cela signifie que si la classification BlueXP ne dispose pas d'autorisations d'attributs d'écriture dans CIFS ou d'autorisations d'écriture dans NFS, le système ne analyse pas les fichiers car la classification BlueXP ne peut pas rétablir l'heure du dernier accès à l'horodatage d'origine. Si vous ne vous souciez pas de la réinitialisation de l'heure du dernier accès, activez le commutateur et tous les fichiers sont

analysés, quelles que soient les autorisations. "En savoir plus >>".



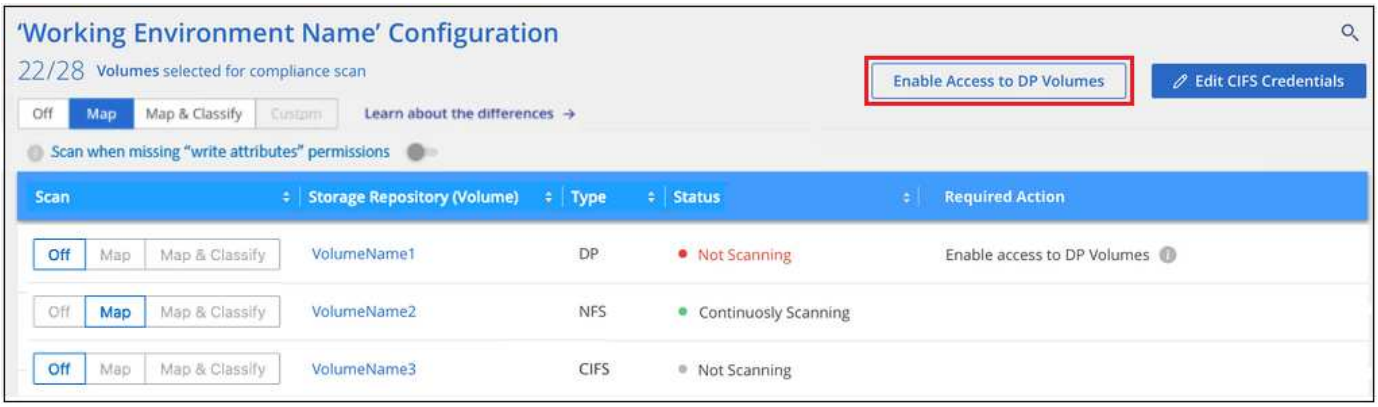
1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Dans la page Configuration, recherchez l'environnement de travail avec les volumes à analyser.
3. Effectuez l'une des opérations suivantes :
   - Pour activer les acquisitions de mappage uniquement sur un volume, dans la zone de volume, sélectionnez **Map**. Ou, pour activer sur tous les volumes, dans la zone d'en-tête, sélectionnez **carte**. Pour activer la numérisation complète sur un volume, dans la zone de volume, sélectionnez **carte et classement**. Ou, pour activer sur tous les volumes, dans la zone d'en-tête, sélectionnez **carte et classement**.
   - Pour désactiver la numérisation sur un volume, dans la zone de volume, sélectionnez **Désactivé**. Pour désactiver la numérisation sur tous les volumes, dans la zone Cap, sélectionnez **Désactivé**.

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

Analysez les volumes de protection des données

Par défaut, les volumes de protection des données (DP) ne sont pas analysés, car ils ne sont pas exposés en externe et la classification BlueXP ne peut pas y accéder. Il s'agit des volumes de destination pour les opérations SnapMirror à partir d'un système de fichiers FSX pour ONTAP.

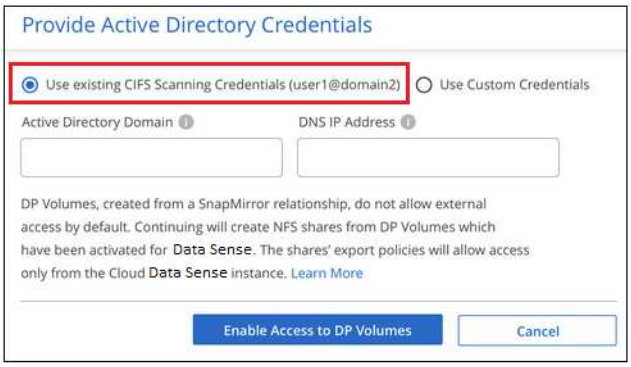
Initialement, la liste de volumes identifie ces volumes comme *Type* **DP** avec *Status* **Not Scanning** et la *Requited action* **Enable Access to DP volumes**.

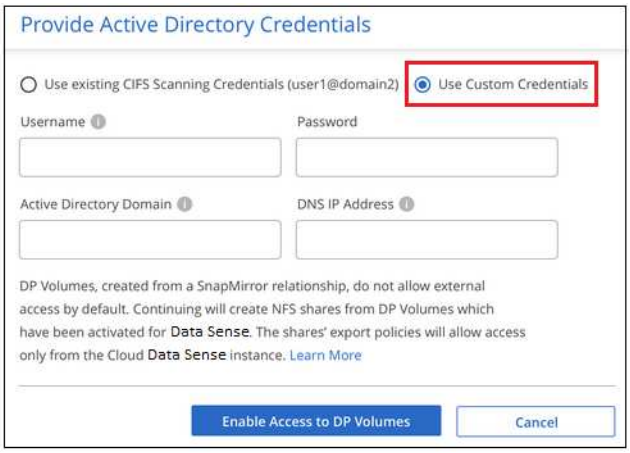


Étapes

Pour analyser ces volumes de protection des données :

1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Sélectionnez **Activer l'accès aux volumes DP** en haut de la page.
3. Consultez le message de confirmation et sélectionnez de nouveau **Activer l'accès aux volumes DP**.
   - Les volumes initialement créés en tant que volumes NFS dans le système de fichiers FSX source pour ONTAP sont activés.
   - Les volumes initialement créés en tant que volumes CIFS dans le système de fichiers FSX source pour ONTAP nécessitent que vous saisiez des informations d'identification CIFS pour scanner ces volumes DP. Si vous avez déjà saisi des informations d'identification Active Directory pour que la classification BlueXP puisse analyser les volumes CIFS, vous pouvez utiliser ces informations d'identification ou spécifier un autre ensemble d'informations d'identification d'administration.





4. Activez chaque volume DP que vous souhaitez analyser.

Résultat

Une fois activé, la classification BlueXP crée un partage NFS à partir de chaque volume DP activé pour l'analyse. Les règles d'exportation de partage autorisent uniquement l'accès à partir de l'instance de classification BlueXP.

Si vous n'aviez pas de volumes de protection de données CIFS lorsque vous avez activé l'accès aux volumes DP pour la première fois, puis ajoutez-en certains, le bouton **Activer l'accès à CIFS DP** s'affiche en haut de la page Configuration. Cliquez sur ce bouton et ajoutez des informations d'identification CIFS pour activer l'accès à ces volumes CIFS DP.

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

Analysez les volumes ONTAP Cloud Volumes ONTAP et sur site avec la classification BlueXP

Procédez en quelques étapes pour commencer l'analyse de vos volumes ONTAP Cloud Volumes ONTAP et sur site à l'aide de la classification BlueXP.

Prérequis

Avant d'activer la classification BlueXP , assurez-vous de disposer d'une configuration prise en charge.

- Si vous scannez des systèmes Cloud Volumes ONTAP et ONTAP sur site accessibles via Internet, vous pouvez "Déployez la classification BlueXP dans le cloud" ou "dans un emplacement sur site avec accès à internet".
- Si vous analysez des systèmes ONTAP sur site qui ont été installés dans un site invisible sans accès à Internet, vous devez "Déployez la classification BlueXP sur le même emplacement sur site qui n'a pas d'accès Internet". Cela nécessite également que le connecteur BlueXP soit déployé dans le même emplacement sur site.

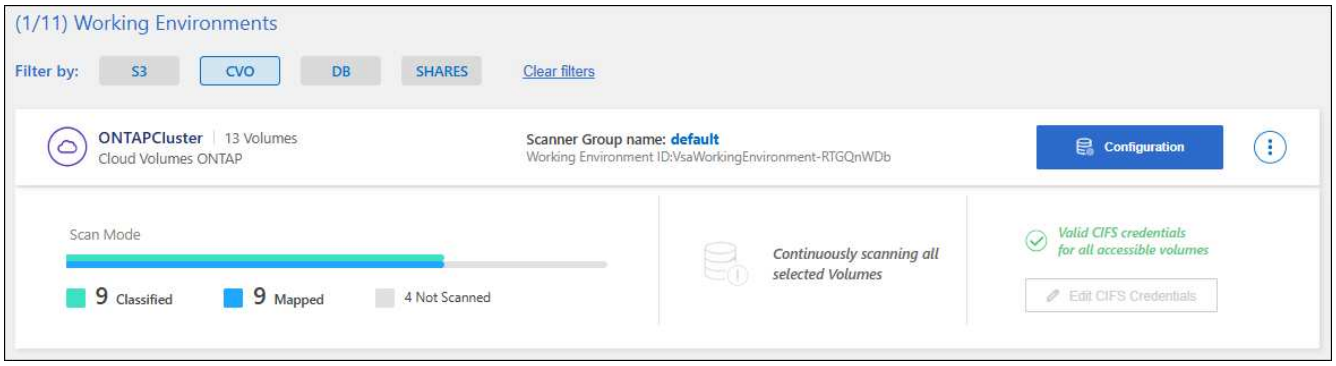
Activez la numérisation de classification BlueXP dans vos environnements de travail

Vous pouvez activer l'analyse de classification BlueXP sur les systèmes Cloud Volumes ONTAP de n'importe quel fournisseur cloud pris en charge et sur les clusters ONTAP sur site.

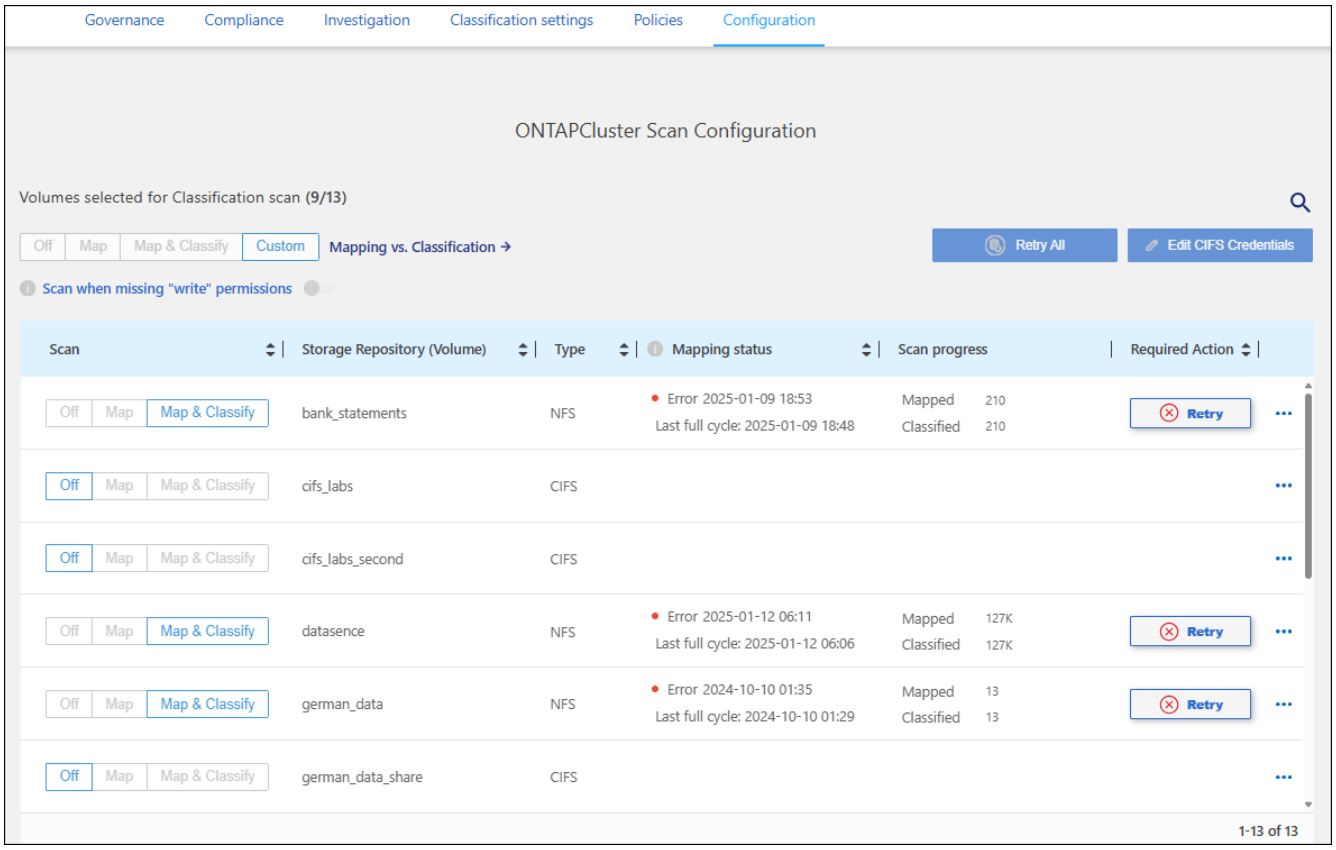
Étapes

1. Dans le menu de navigation de gauche BlueXP , sélectionnez **gouvernance > Classification**.
2. Dans le menu BlueXP Classification, sélectionnez **Configuration**.

   La page Configuration affiche plusieurs environnements de travail.



3. Choisissez un environnement de travail et sélectionnez **Configuration**.



4. Si vous ne vous souciez pas de la réinitialisation de l'heure du dernier accès, ACTIVEZ l'option **Scan en cas d'autorisations d'écriture d'attributs manquantes** et tous les fichiers sont analysés, quelles que soient les autorisations.

   Le commutateur en haut de la page pour **Scan en cas d'autorisations d'écriture d'attributs manquantes** est désactivé par défaut. Cela signifie que si la classification BlueXP ne dispose pas d'autorisations d'attributs d'écriture dans CIFS ou d'autorisations d'écriture dans NFS, le système ne classe pas les fichiers car la classification BlueXP ne peut pas rétablir l'heure du dernier accès à l'horodatage d'origine. "En savoir plus >>".

5. Sélectionnez le mode de numérisation des volumes dans chaque environnement de travail. "En savoir plus sur les acquisitions de mappage et de classification":
   - Pour mapper tous les volumes, sélectionnez **Map**.
   - Pour mapper et classer tous les volumes, sélectionnez **Map & Classify**.
   - Pour personnaliser le balayage de chaque volume, sélectionnez **personnalisé**, puis choisissez les volumes à mapper et/ou classer.
6. Dans la boîte de dialogue de confirmation, sélectionnez **Approve** pour que la classification BlueXP commence à analyser vos volumes.

Résultat

La classification BlueXP démarre l'analyse des volumes sélectionnés dans l'environnement de travail. Les résultats commencent à apparaître dans le tableau de bord de conformité dès que la classification BlueXP démarre l'analyse. Le temps nécessaire pour effectuer cette opération dépend de la quantité de données, qui peut prendre quelques minutes ou quelques heures.

La classification BlueXP analyse un seul partage de fichiers sous un volume. Si vous avez plusieurs partages dans vos volumes, vous devrez analyser ces autres partages séparément en tant que groupe de partages. "Pour en savoir plus sur cette limitation de classification BlueXP, consultez".

Vérifiez que la classification BlueXP a accès aux volumes

Assurez-vous que la classification BlueXP peut accéder aux volumes en vérifiant votre réseau, vos groupes de sécurité et vos règles d'exportation. Vous devez fournir une classification BlueXP avec des informations d'identification CIFS pour pouvoir accéder aux volumes CIFS.

Étapes

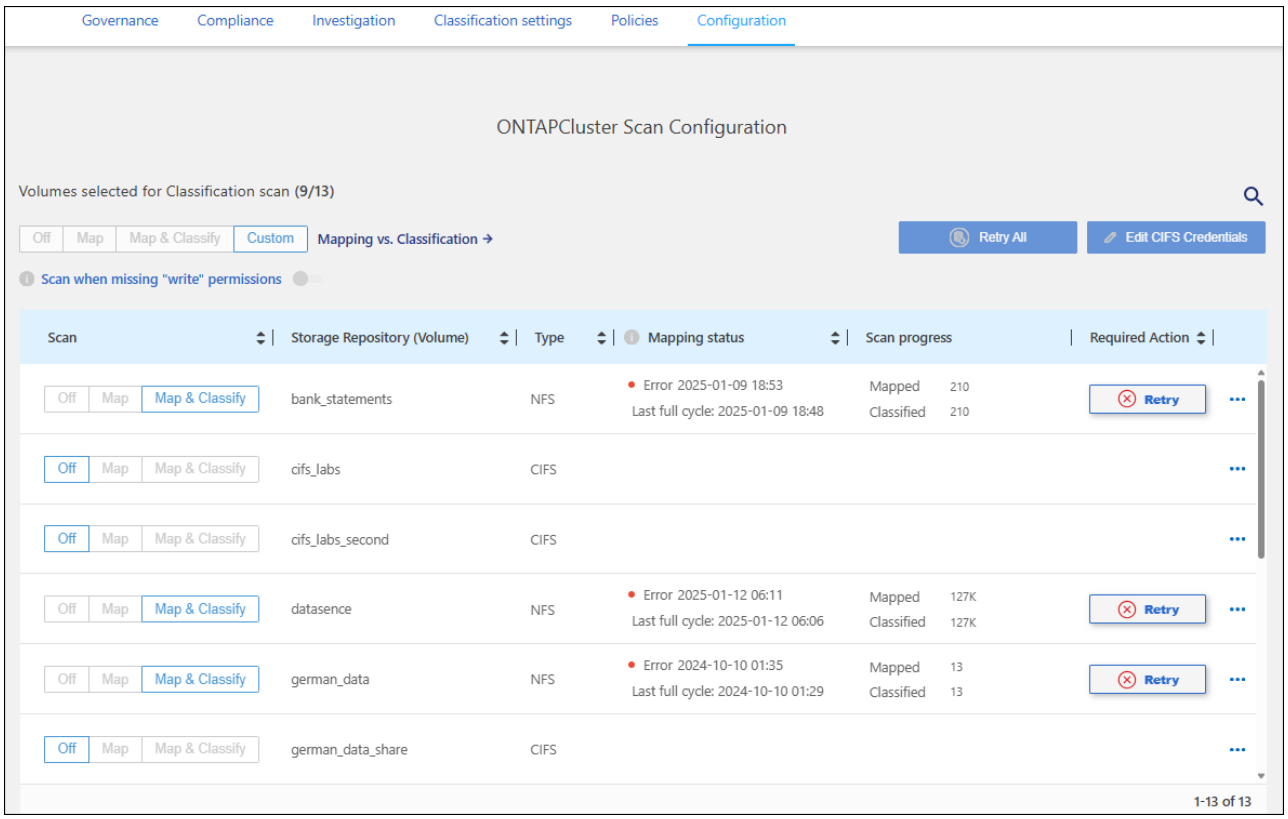
1. Assurez-vous qu'il existe une connexion réseau entre l'instance de classification BlueXP et chaque réseau, incluant des volumes pour les clusters Cloud Volumes ONTAP ou ONTAP sur site.
2. Assurez-vous que le groupe de sécurité pour Cloud Volumes ONTAP autorise le trafic entrant à partir de l'instance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

   Vous pouvez soit ouvrir le groupe de sécurité pour le trafic à partir de l'adresse IP de l'instance de classification BlueXP, soit ouvrir le groupe de sécurité pour tout le trafic depuis l'intérieur du réseau virtuel.

3. Assurez-vous que les règles d'exportation du volume NFS incluent l'adresse IP de l'instance de classification BlueXP afin qu'elle puisse accéder aux données de chaque volume.
4. Si vous utilisez CIFS, fournissez la classification BlueXP avec les informations d'identification Active Directory pour qu'il puisse analyser les volumes CIFS.

   a. Dans le menu de navigation de gauche BlueXP , sélectionnez **gouvernance > Classification**.

   b. Dans le menu BlueXP Classification, sélectionnez **Configuration**.



c. Pour chaque environnement de travail, sélectionnez **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe dont la classification BlueXP a besoin pour accéder aux volumes CIFS du système.

   Les identifiants peuvent être en lecture seule, mais il est possible de fournir des identifiants d'administrateur pour que la classification BlueXP puisse lire toutes les données qui nécessitent des autorisations élevées. Les identifiants sont stockés sur l'instance de classification BlueXP.

   Pour garantir que les analyses de BlueXP classification ne modifient pas les « derniers accès » de vos fichiers, il est recommandé que l'utilisateur dispose des autorisations d'écriture sur les attributs dans CIFS ou NFS. Si possible, configurez l'utilisateur Active Directory comme membre d'un groupe parent de l'organisation disposant d'autorisations sur tous les fichiers.

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

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

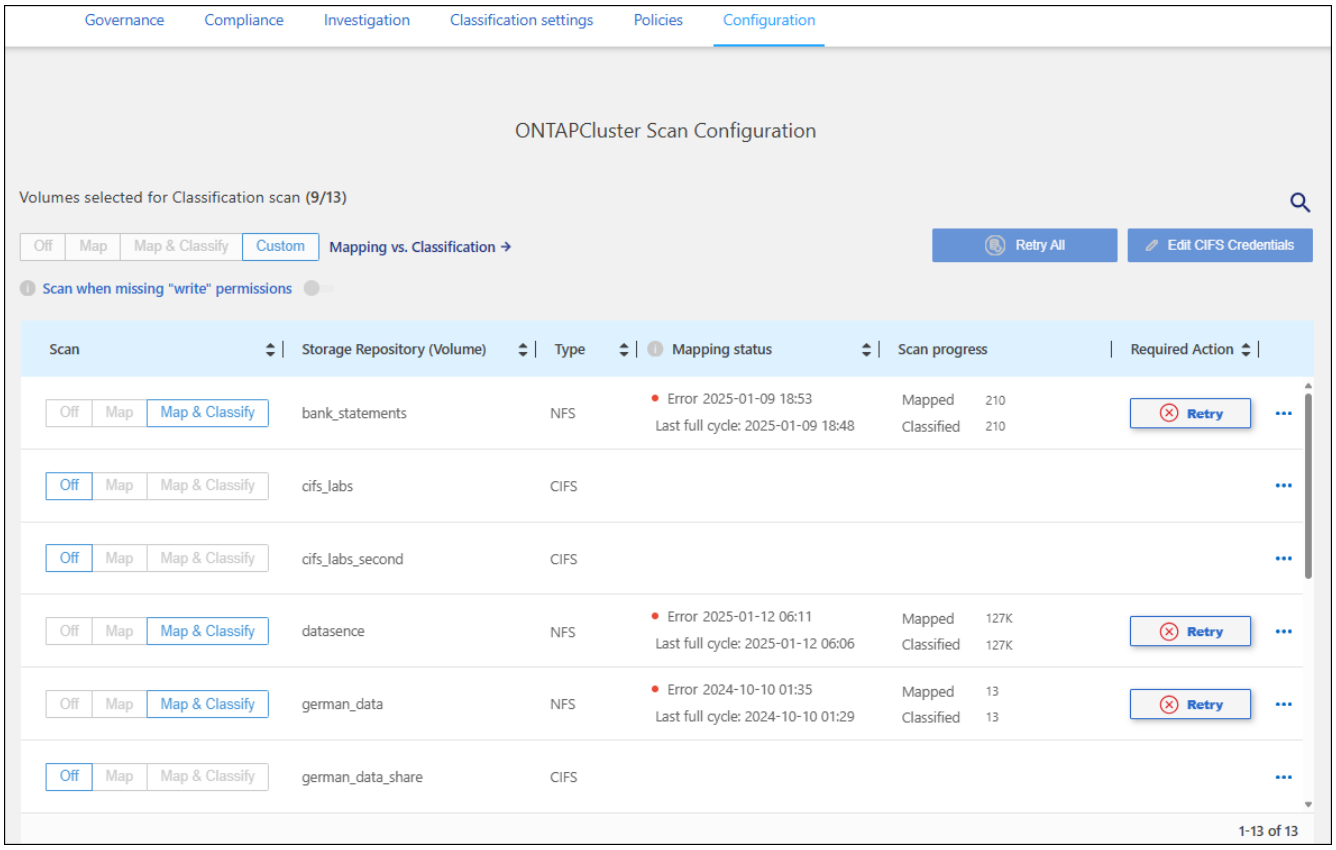
Désactivez les analyses de conformité sur les volumes

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

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

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Sélectionnez le bouton **Configuration** de l'environnement de travail que vous souhaitez modifier.



3. Effectuez l'une des opérations suivantes :
   - Pour désactiver la numérisation sur un volume, dans la zone de volume, sélectionnez **Désactivé**.
   - Pour désactiver la numérisation sur tous les volumes, dans la zone Cap, sélectionnez **Désactivé**.

Analyser les schémas de base de données avec la classification BlueXP

Procédez en quelques étapes pour commencer à analyser vos schémas de base de données avec la classification BlueXP.

Passer en revue les prérequis

Vérifiez les conditions préalables suivantes pour vous assurer que votre configuration est prise en charge avant d'activer la classification BlueXP.

Bases de données prises en charge

La classification BlueXP peut analyser les schémas à partir des bases de données suivantes :

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

- Serveur SQL (MSSQL)

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

Configuration requise pour les bases de données

N'importe quelle base de données connectée à l'instance de classification BlueXP peut être analysée, quel que soit son emplacement d'hébergement. Pour vous connecter à la base de données, il vous suffit de disposer des informations suivantes :

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

  Lors du choix d'un nom d'utilisateur et d'un mot de passe, il est important de choisir celui qui dispose des autorisations de lecture complètes pour tous les schémas et tables que vous souhaitez numériser. Nous vous recommandons de créer un utilisateur dédié pour le système de classification BlueXP avec toutes les autorisations requises.

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

Déployez l'instance de classification BlueXP

Déployez la classification BlueXP si aucune instance n'est déjà déployée.

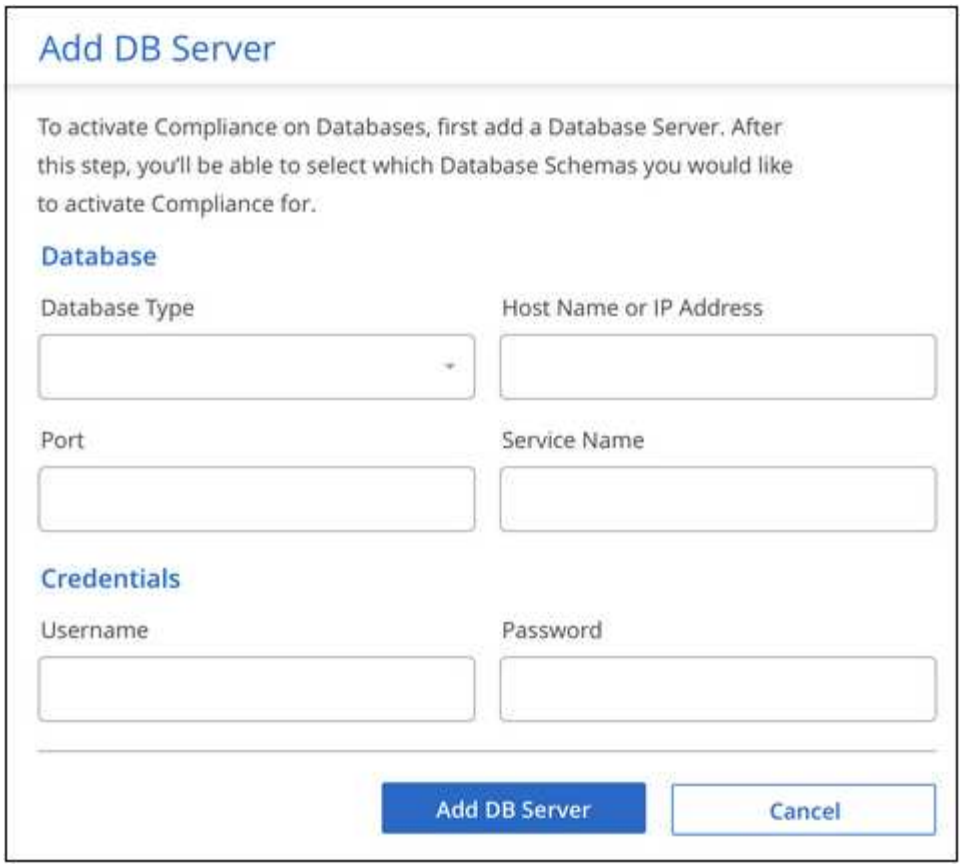
Si vous numérisez des schémas de base de données accessibles via Internet, vous pouvez "Déployez la classification BlueXP dans le cloud" ou "Déployez la classification BlueXP dans un emplacement sur site disposant d'un accès Internet".

Si vous numérisez des schémas de base de données qui ont été installés sur un site sombre sans accès à Internet, vous devez le faire "Déployez la classification BlueXP sur le même emplacement sur site qui n'a pas d'accès Internet". Cela nécessite également que le connecteur BlueXP soit déployé dans le même emplacement sur site.

Ajoutez le serveur de base de données

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

1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Sur la page Configuration, sélectionnez **Ajouter un environnement de travail** > **Ajouter un serveur de base de données**.
3. Entrez les informations requises pour identifier le serveur de base de données.
   a. Sélectionnez le type de base de données.
   b. Entrez le port et le nom d'hôte ou l'adresse IP pour vous connecter à la base de données.
   c. Pour les bases de données Oracle, entrez le nom du service.
   d. Entrez les identifiants pour que la classification BlueXP puisse accéder au serveur.
   e. Cliquez sur **Ajouter serveur DB**.



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

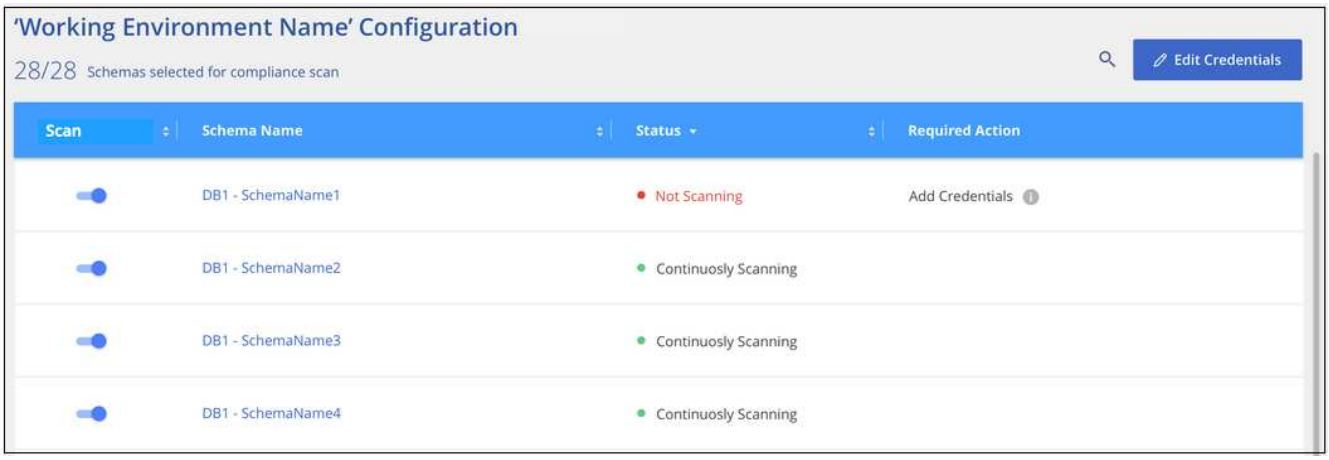
Activer et désactiver les analyses de conformité sur les schémas de base de données

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

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

1. Dans la page Configuration, sélectionnez le bouton **Configuration** de la base de données que vous souhaitez configurer.

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



Résultat

La classification BlueXP commence à analyser les schémas de base de données que vous avez activés. Vous pouvez suivre la progression de l'acquisition initiale en accédant au menu **Configuration** puis en sélectionnant la **Configuration de l'environnement de travail**. La progression de chaque acquisition est affichée sous la forme d'une barre de progression. Vous pouvez également passer le curseur de la souris sur la barre de progression pour voir le nombre de fichiers analysés par rapport au nombre total de fichiers dans le volume. En cas d'erreur, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

La classification BlueXP analyse vos bases de données une fois par jour. Les bases de données ne sont pas continuellement analysées comme d'autres sources de données.

Analysez les partages de fichiers avec la classification BlueXP

Pour analyser les partages de fichiers, vous devez d'abord créer un groupe de partages de fichiers dans la BlueXP classification. Les groupes de partages de fichiers sont destinés aux partages NFS ou CIFS (SMB) hébergés sur site ou dans le cloud.

L'analyse des données à partir de partages de fichiers non NetApp n'est pas prise en charge dans la version principale de classification BlueXP.

Prérequis

Vérifiez les conditions préalables suivantes pour vous assurer que votre configuration est prise en charge avant d'activer la classification BlueXP.

- Ils peuvent être hébergés partout, y compris dans le cloud ou sur site. Les partages CIFS d'anciens systèmes de stockage NetApp 7-mode peuvent être analysés en tant que partages de fichiers.
  - La BlueXP classification ne peut pas extraire les autorisations ou la « dernière heure d'accès » des systèmes 7-Mode.
  - En raison d'un problème connu entre certaines versions Linux et les partages CIFS sur les systèmes 7-Mode, vous devez configurer le partage pour utiliser uniquement SMBv1 avec l'authentification NTLM activée.
- Il doit y avoir une connectivité réseau entre l'instance de classification BlueXP et les partages.
- Vous pouvez ajouter un partage DFS (Distributed File System) en tant que partage CIFS standard. Étant donné que la BlueXP classification ne sait pas que le partage est basé sur plusieurs serveurs/volumes combinés en un seul partage CIFS, vous risquez de recevoir des erreurs d'autorisation ou de connectivité

concernant le partage lorsque le message s'applique réellement uniquement à l'un des dossiers/partages situés sur un serveur/volume différent.

- Pour les partages CIFS (SMB), assurez-vous que vous disposez des identifiants Active Directory qui fournissent un accès en lecture aux partages. Les identifiants d'administration sont préférés si la classification BlueXP doit analyser les données nécessitant des autorisations élevées.

  Pour garantir que les analyses de BlueXP classification ne modifient pas les « derniers accès » de vos fichiers, il est recommandé que l'utilisateur dispose des autorisations d'écriture sur les attributs dans CIFS ou NFS. Si possible, configurez l'utilisateur Active Directory comme membre d'un groupe parent de l'organisation disposant d'autorisations sur tous les fichiers.

- Tous les partages de fichiers CIFS d'un groupe doivent utiliser les mêmes informations d'identification Active Directory.
- Vous pouvez combiner des partages NFS et CIFS (via Kerberos ou NTLM). Vous devez ajouter les partages au groupe séparément. Autrement dit, vous devez effectuer cette procédure deux fois, une fois par protocole.
  - Vous ne pouvez pas créer un groupe de partage de fichiers qui mélange les types d'authentification CIFS (Kerberos et NTLM).
- Si vous utilisez CIFS avec l'authentification Kerberos, assurez-vous que l'adresse IP fournie est accessible au service de BlueXP classification . Les partages de fichiers ne peuvent pas être ajoutés si l'adresse IP est inaccessible.

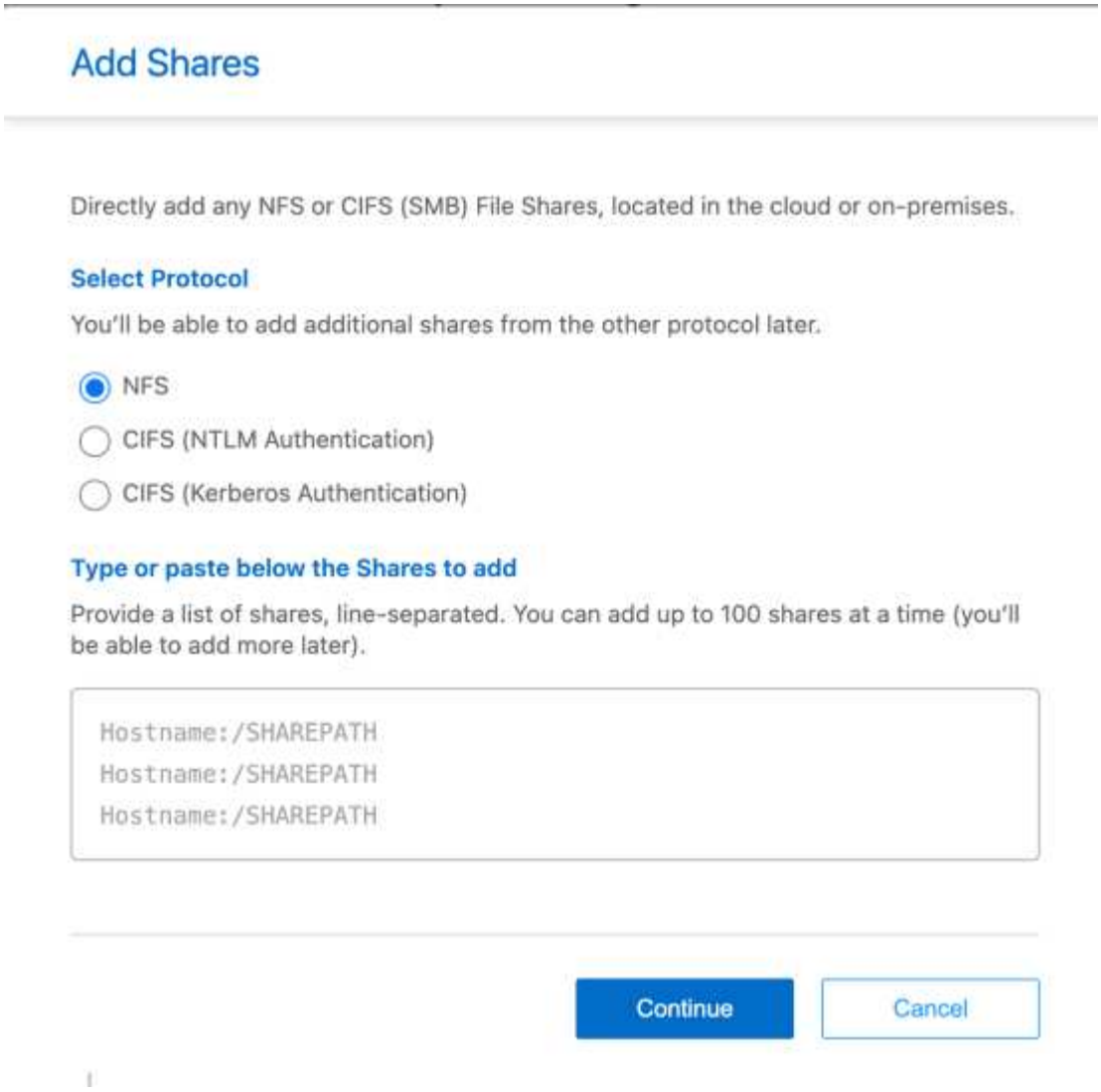
Créer un groupe de partage de fichiers

Lorsque vous ajoutez des partages de fichiers au groupe, vous devez utiliser le format `<host_name>:/<share_path>` .

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

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Sur la page Configuration, sélectionnez **Ajouter un environnement de travail** > **Ajouter un groupe de partages de fichiers**.
3. Dans la boîte de dialogue Ajouter un groupe de partages de fichiers, saisissez le nom du groupe de partages, puis sélectionnez **Continuer**.
4. Sélectionnez le protocole des partages de fichiers que vous ajoutez.



Si vous ajoutez des partages CIFS avec l'authentification NTLM, saisissez les informations d'identification Active Directory pour accéder aux volumes CIFS. Bien que les informations d'identification en lecture seule soient prises en charge, il est recommandé de fournir un accès complet avec les informations d'identification d'administrateur. Sélectionnez Enregistrer.

1. Ajoutez les partages de fichiers que vous souhaitez analyser (un partage de fichiers par ligne). Sélectionnez ensuite **Continuer**.
2. Une boîte de dialogue de confirmation affiche le nombre de partages ajoutés.

   Si la boîte de dialogue répertorie tous les partages qui n'ont pas pu être ajoutés, capturez ces informations pour résoudre le problème. Si le problème concerne une convention de nommage, vous pouvez rajouter le partage avec un nom corrigé.

3. Configurer l'analyse sur le volume :
   - Pour activer les analyses de mappage uniquement sur les partages de fichiers, sélectionnez **Map**.
   - Pour activer les analyses complètes sur les partages de fichiers, sélectionnez **Map & Classify**.
   - Pour désactiver la numérisation sur les partages de fichiers, sélectionnez **Désactivé**.

Le commutateur en haut de la page pour **Scan en cas d'autorisations d'écriture d'attributs manquantes** est désactivé par défaut. Cela signifie que si la BlueXP classification ne dispose pas des autorisations d'écriture d'attributs dans CIFS ou NFS, le système n'analysera pas les fichiers, car BlueXP classification ne peut pas rétablir l'horodatage d'origine pour l'heure du dernier accès. + Si vous activez l'option **Analyser en cas d'absence d'autorisations d'écriture d'attributs**, l'analyse réinitialise l'heure du dernier accès et analyse tous les fichiers, quelles que soient les autorisations. + Pour en savoir plus sur l'horodatage du dernier accès, consultez xref:./"Métadonnées collectées à partir de sources de données dans la classification BlueXP " .

Résultat

La BlueXP classification commence à analyser les fichiers des partages ajoutés. Vous pouvez Suivre la progression de l'acquisition et afficher les résultats de l'analyse dans le **Tableau de bord**.

Si l'analyse ne se termine pas correctement pour une configuration CIFS avec authentification Kerberos, vérifiez l'onglet **Configuration** pour les erreurs.

Modifier un groupe de partage de fichiers

Après avoir créé un groupe de partages de fichiers, vous pouvez modifier le protocole CIFS ou ajouter et supprimer des partages de fichiers.

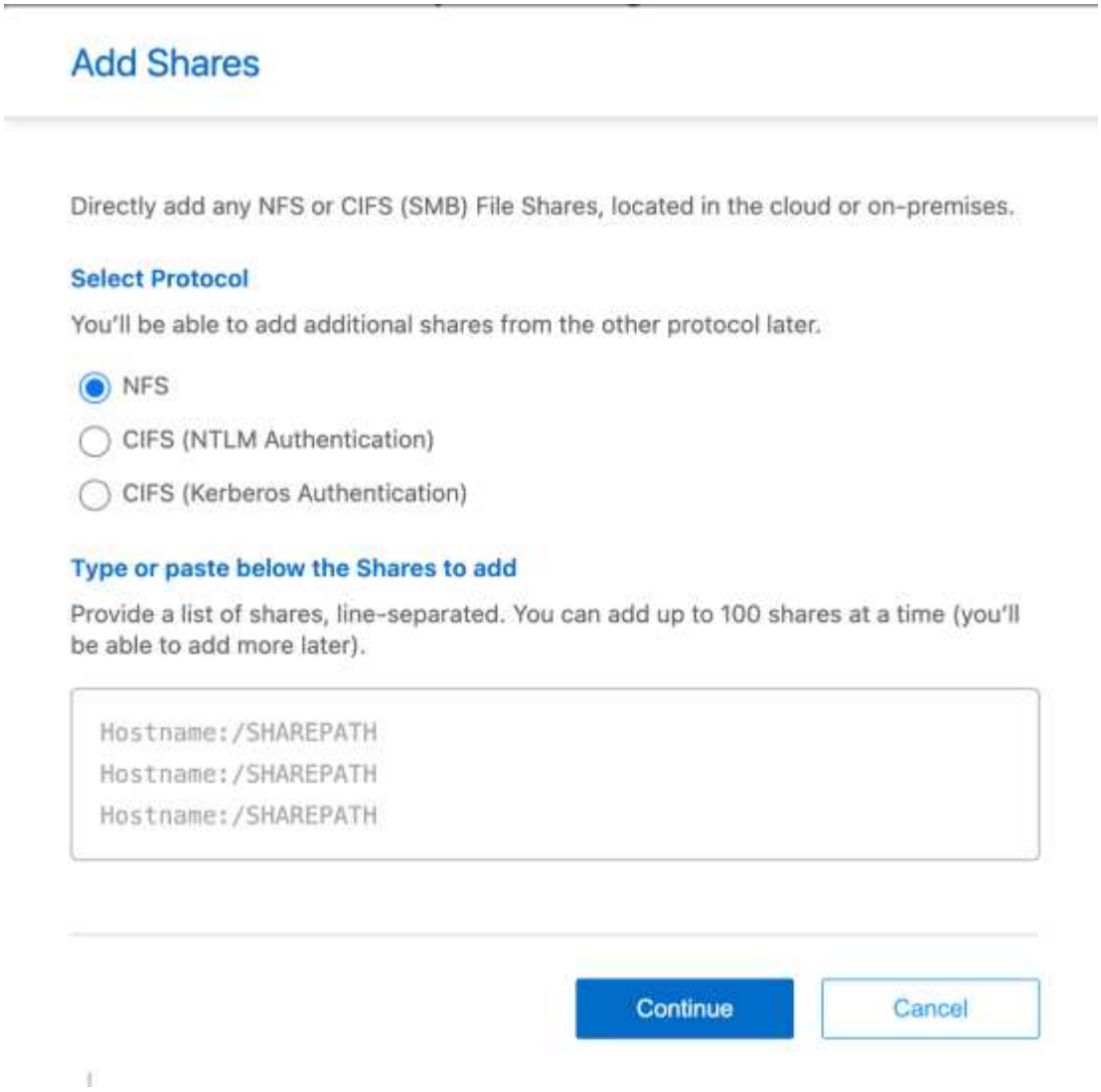
Modifier la configuration du protocole CIFS

1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Depuis la page Configuration, sélectionnez le groupe de partages de fichiers que vous souhaitez modifier.
3. Sélectionnez **Modifier les informations d'identification CIFS**.

4. Choisissez la méthode d'authentification : **NTLM** ou **Kerberos**.
5. Saisissez le **Nom d'utilisateur** et le **Mot de passe** Active Directory.
6. Sélectionnez **Enregistrer** pour terminer le processus.

Ajouter des partages de fichiers aux analyses de conformité

1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Depuis la page Configuration, sélectionnez le groupe de partages de fichiers que vous souhaitez modifier.
3. Sélectionnez **+ Ajouter des partages**.
4. Sélectionnez le protocole des partages de fichiers que vous ajoutez.



Si vous ajoutez des partages de fichiers à un protocole que vous avez déjà configuré, aucune modification n'est requise.

Si vous ajoutez des partages de fichiers avec un deuxième protocole, assurez-vous d'avoir correctement configuré l'authentification comme détaillé dans le "prérequis" .

5. Ajoutez les partages de fichiers que vous souhaitez analyser (un partage de fichiers par ligne) en utilisant le format `<host_name>:/<share_path>` .
6. Sélectionnez **Continuer** pour terminer l'ajout des partages de fichiers.

Supprimez un partage de fichiers des analyses de conformité

1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Sélectionnez l'environnement de travail à partir duquel vous souhaitez supprimer les partages de fichiers.
3. Sélectionnez **Configuration**.
4. Dans la page Configuration, sélectionnez les actions ••• du partage de fichiers à supprimer.
5. Dans le menu actions, sélectionnez **Supprimer le partage**.

Suivre la progression de l'acquisition

Vous pouvez suivre la progression de l'acquisition initiale.

1. Sélectionnez le menu **Configuration**.
2. Sélectionnez la **Configuration de l'environnement de travail**.

   La progression de chaque acquisition s'affiche sous la forme d'une barre de progression.

3. Passez le curseur sur la barre de progression pour voir le nombre de fichiers analysés par rapport au nombre total de fichiers dans le volume.

Analysez les données StorageGRID avec la classification BlueXP

Procédez en quelques étapes pour commencer à numériser des données directement dans StorageGRID avec la classification BlueXP .

Vérifiez les conditions requises pour le StorageGRID

Vérifiez les conditions préalables suivantes pour vous assurer que votre configuration est prise en charge avant d'activer la classification BlueXP.

- Vous devez disposer de l'URL du terminal pour vous connecter au service de stockage objet.
- Vous devez disposer de la clé d'accès et de la clé secrète de StorageGRID pour que la classification BlueXP puisse accéder aux compartiments.

Déployez l'instance de classification BlueXP

Déployez la classification BlueXP si aucune instance n'est déjà déployée.

Si vous numérisez des données à partir de StorageGRID accessibles via Internet, vous pouvez "Déployez la classification BlueXP dans le cloud" ou "Déployez la classification BlueXP dans un emplacement sur site disposant d'un accès Internet".

Si vous analysez des données à partir de StorageGRID qui a été installé dans un site sombre qui n'a pas d'accès à Internet, vous devez "Déployez la classification BlueXP sur le même emplacement sur site qui n'a pas d'accès Internet". Cela nécessite également que le connecteur BlueXP soit déployé dans le même emplacement sur site.

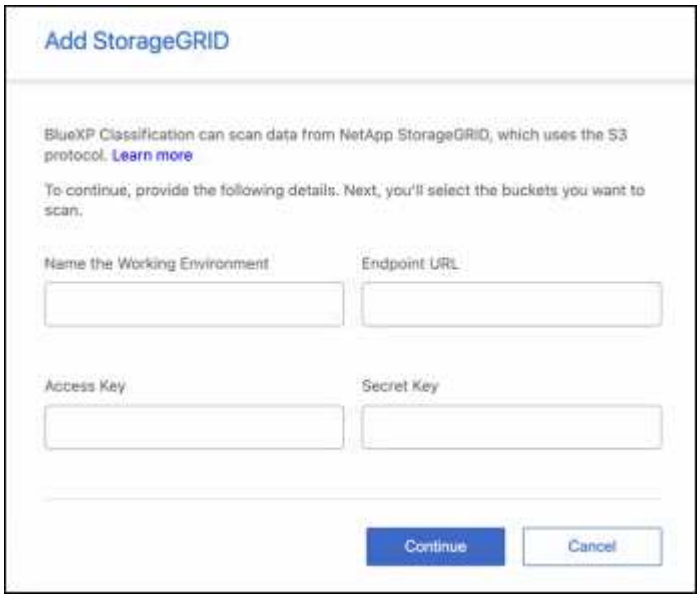
Ajoutez le service StorageGRID à la classification BlueXP

Ajoutez le service StorageGRID.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez l'option **Configuration**.
2. Sur la page Configuration, sélectionnez **Ajouter un environnement de travail** > **Ajouter StorageGRID**.
3. Dans la boîte de dialogue Ajouter un service StorageGRID, entrez les détails du service StorageGRID et cliquez sur **Continuer**.
   a. Entrez le nom que vous souhaitez utiliser pour l'environnement de travail. Ce nom doit correspondre au nom du service StorageGRID auquel vous vous connectez.
   b. Entrez l'URL du point final pour accéder au service de stockage d'objets.

c. Entrez la clé d'accès et la clé secrète pour que la classification BlueXP puisse accéder aux compartiments dans StorageGRID.



Résultat

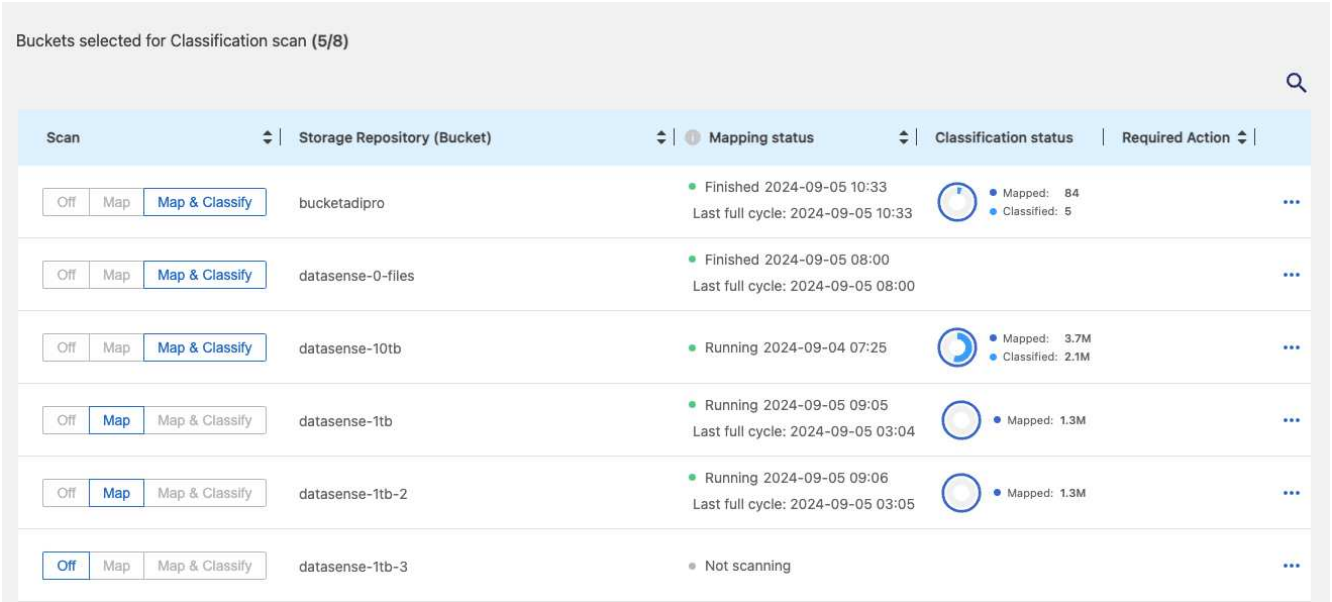
StorageGRID est ajouté à la liste des environnements de travail.

Activer et désactiver les analyses de conformité sur les compartiments StorageGRID

Après avoir activé la classification BlueXP sur StorageGRID, l'étape suivante consiste à configurer les compartiments que vous souhaitez analyser. La classification BlueXP détecte ces compartiments et les affiche dans l'environnement de travail que vous avez créé.

Étapes

1. Dans la page Configuration, recherchez l'environnement de travail StorageGRID.
2. Dans la mosaïque de l'environnement de travail StorageGRID, sélectionnez **Configuration**.



3. Effectuez l'une des étapes suivantes pour activer ou désactiver la numérisation :
    - Pour activer les acquisitions de mappage uniquement sur un compartiment, sélectionnez **Map**.
    - Pour activer les acquisitions complètes sur un compartiment, sélectionnez **Map & Classify**.
    - Pour désactiver la numérisation sur un compartiment, sélectionnez **Désactivé**.

Résultat

La classification BlueXP commence à analyser les compartiments que vous avez activés. Vous pouvez suivre la progression de l'acquisition initiale en accédant au menu **Configuration** puis en sélectionnant la **Configuration de l'environnement de travail**. La progression de chaque acquisition est affichée sous la forme d'une barre de progression. Vous pouvez également passer le curseur de la souris sur la barre de progression pour voir le nombre de fichiers analysés par rapport au nombre total de fichiers dans le volume. En cas d'erreur, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

Intégrez votre Active Directory avec la classification BlueXP

Vous pouvez intégrer un Active Directory global avec la classification BlueXP pour améliorer les résultats des rapports de classification BlueXP sur les propriétaires de fichiers et les utilisateurs et groupes qui ont accès à vos fichiers.

Lorsque vous configurez certaines sources de données (répertoriées ci-dessous), vous devez entrer les informations d'identification Active Directory pour que la classification BlueXP analyse les volumes CIFS. Cette intégration permet la classification BlueXP avec le propriétaire de fichier et les détails d'autorisations pour les données qui résident dans ces sources de données. L'Active Directory saisi pour ces sources de données peut différer des informations d'identification Active Directory globales que vous entrez ici. La classification BlueXP recherche les détails des utilisateurs et des autorisations dans tous les Active Directory intégrés.

Cette intégration fournit des informations supplémentaires aux emplacements suivants de la classification BlueXP :

- Vous pouvez utiliser le « propriétaire du fichier » "filtre" et afficher les résultats dans les métadonnées du fichier dans le volet Investigation. Au lieu du propriétaire du fichier contenant le SID (identificateur de sécurité), il est renseigné avec le nom d'utilisateur réel.

  Vous pouvez également afficher plus de détails sur le propriétaire du fichier : nom du compte, adresse e-mail et nom du compte SAM, ou afficher les éléments appartenant à cet utilisateur.

- Vous pouvez voir "autorisations complètes sur les fichiers" pour chaque fichier et répertoire lorsque vous cliquez sur le bouton « Afficher toutes les autorisations ».
- Dans le "Tableau de bord gouvernance", Le panneau Ouvrir les autorisations affiche un niveau de détail plus élevé sur vos données.

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

Sources de données prises en charge

Une intégration d'Active Directory avec la classification BlueXP permet d'identifier les données à partir des sources de données suivantes :

- Systèmes ONTAP sur site

- Cloud Volumes ONTAP
- Azure NetApp Files
- FSX pour ONTAP
- Comptes OneDrive et comptes SharePoint (pour anciennes versions 1.30 et antérieures)

Il n'est pas possible de prendre en charge l'identification des informations d'utilisateur et d'autorisation à partir des schémas de base de données, des comptes Google Drive, des comptes Amazon S3 ou du stockage objet qui utilise le protocole simple Storage Service (S3).

Connectez-vous à votre serveur Active Directory

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

Les identifiants Active Directory peuvent être en lecture seule, mais la fourniture d'identifiants d'administration permet à la classification BlueXP de lire toutes les données nécessitant des autorisations élevées. Les identifiants sont stockés sur l'instance de classification BlueXP.

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

De formation

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

    ou

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

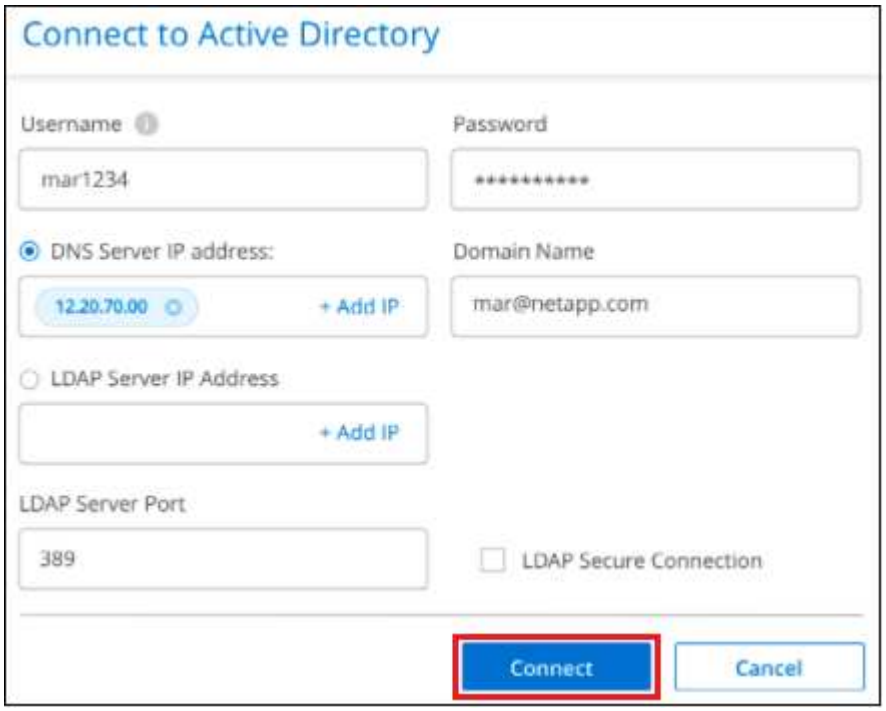
Protocole	Port	Destination	Objectif
TCP ET UDP	389	Active Directory	LDAP
TCP	636	Active Directory	LDAP sur SSL
TCP	3268	Active Directory	Catalogue global
TCP	3269	Active Directory	Catalogue global sur SSL

Étapes

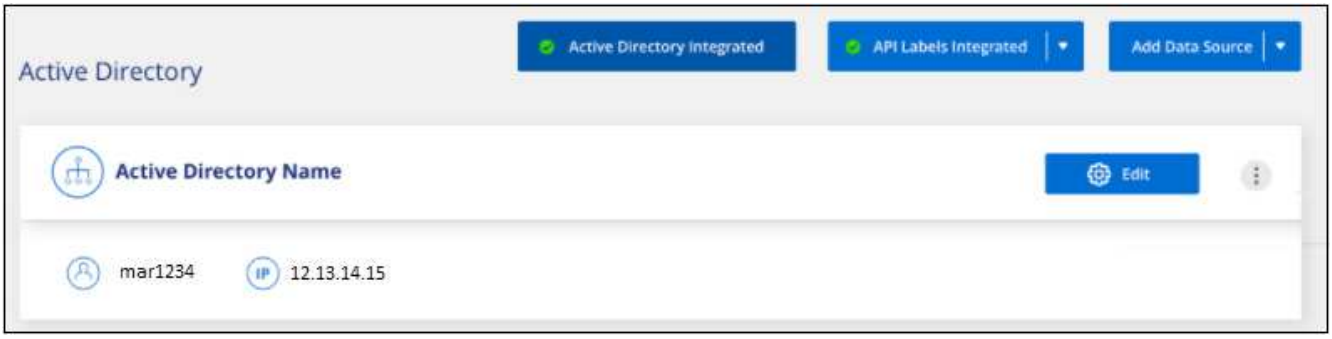
1. Sur la page Configuration de la classification BlueXP, cliquez sur **Ajouter Active Directory**.

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

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



   La classification BlueXP s'intègre à Active Directory. Une nouvelle section est ajoutée à la page Configuration.



Gérez votre intégration Active Directory

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

Vous pouvez également supprimer l'intégration en sélectionnant le bouton puis **Supprimer Active Directory**.