Documentation sur les classifications BlueXP

BlueXP classification

NetApp
October 21, 2024

Sommaire

Documentation sur les classifications BlueXP

Notes de mise à jour

Nouveautés de la classification BlueXP

Découvrez les nouveautés de la classification BlueXP (Cloud Data Sense).

10 octobre 2024 (version 1.36)

Cette version de classification BlueXP inclut les mises à jour suivantes.

Prise en charge de RHEL 9.4

Cette version prend en charge Red Hat Enterprise Linux v9.4 en plus des versions précédemment prises en charge. Cela s'applique à toute installation manuelle sur site de la classification BlueXP , y compris les déploiements de sites invisibles.

Les systèmes d'exploitation suivants nécessitent l'utilisation du moteur de conteneur Podman et requièrent la classification BlueXP version 1.30 ou ultérieure : Red Hat Enterprise Linux version 8.8, 9.0, 9.1, 9.2, 9.3 et 9.4.

En savoir plus sur "Présentation des déploiements de classifications BlueXP".

Amélioration des performances de numérisation

Cette version offre des performances de numérisation améliorées.

2 septembre 2024 (version 1.35)

Cette version de classification BlueXP inclut la mise à jour suivante.

Analyser les données StorageGRID

La classification BlueXP peut maintenant analyser les données dans StorageGRID.

Pour plus de détails, reportez-vous à "Analyser les données StorageGRID".

5 août 2024 (version 1.34)

Cette version de classification BlueXP inclut la mise à jour suivante.

Passez de CentOS à Ubuntu

La classification BlueXP a mis à jour son système d'exploitation Linux pour Microsoft Azure et Google Cloud Platform (GCP) de CentOS 7.9 à Ubuntu 22.04.

Pour plus de détails sur le déploiement, reportez-vous à la section "Installez sur un hôte Linux avec accès Internet et préparez le système hôte Linux".

1er juillet 2024 (version 1.33)

Cette version inclut les mises à jour suivantes.

Ubuntu pris en charge

Cette version prend en charge la plate-forme Linux Ubuntu 24.04.

Les analyses de mappage rassemblent les métadonnées

Les métadonnées suivantes sont extraites des fichiers lors des analyses de mappage et sont affichées dans les tableaux de bord gouvernance, conformité et investigation :

- 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

Données supplémentaires dans les tableaux de bord

Cette version met à jour les données qui apparaissent dans les tableaux de bord gouvernance, conformité et investigation lors des analyses de mappage.

Pour plus de détails, voir "Quelle est la différence entre les analyses de cartographie et de classification"

5 juin 2024 (version 1.32)

Cette version inclut la mise à jour suivante.

Nouvelle colonne État de mappage de la page Configuration

Cette version affiche désormais une nouvelle colonne d'état de mappage dans la page Configuration. La nouvelle colonne vous permet d'identifier si le mappage est en cours d'exécution, en file d'attente, en pause ou plus.

Pour plus d'informations sur les États, reportez-vous à la section "Modifier les paramètres de numérisation".

15 mai 2024 (version 1.31)

La classification est disponible en tant que service principal dans BlueXP

La classification BlueXP est désormais disponible en tant que fonctionnalité clé dans BlueXP, sans frais supplémentaires pour un maximum de 500 To de données numérisées. Aucune licence de classification ou abonnement payant n'est nécessaire. Alors que nous nous concentrons sur la fonctionnalité de classification BlueXP lors de l'analyse des systèmes de stockage NetApp avec cette nouvelle version, certaines

fonctionnalités héritées ne seront disponibles que pour les clients qui avaient déjà payé pour une licence. L'utilisation de ces fonctions héritées expirera lorsque le contrat payé atteindra sa date de fin.

"En savoir plus sur les fonctionnalités obsolètes".

1er avril 2024 (version 1.30)

Prise en charge de la classification BlueXP RHEL v8.8 et v9.3

Cette version prend en charge Red Hat Enterprise Linux v8.8 et v9.3 en plus de la version 9.x précédemment prise en charge, qui nécessite Podman, plutôt que le moteur Docker. Cela s'applique à toute installation manuelle sur site de la classification BlueXP.

Les systèmes d'exploitation suivants nécessitent l'utilisation du moteur de conteneur Podman et requièrent la classification BlueXP version 1.30 ou supérieure : Red Hat Enterprise Linux version 8.8, 9.0, 9.1, 9.2 et 9.3.

En savoir plus sur "Présentation des déploiements de classifications BlueXP".

La classification BlueXP est prise en charge si vous installez le connecteur sur un hôte RHEL 8 ou 9 résidant sur site. Elle n'est pas prise en charge si l'hôte RHEL 8 ou 9 réside dans AWS, Azure ou Google Cloud.

Option d'activation de la collection de journaux d'audit supprimée

L'option permettant d'activer la collecte des journaux d'audit a été désactivée.

Vitesse de numérisation améliorée

Les performances de numérisation sur les nœuds de scanner secondaires ont été améliorées. Vous pouvez ajouter d'autres nœuds de scanner si vous avez besoin d'une puissance de traitement supplémentaire pour vos numérisations. Pour plus de détails, reportez-vous à "Installez la classification BlueXP sur un hôte disposant d'un accès Internet".

Mises à niveau automatiques

Si vous avez déployé la classification BlueXP sur un système disposant d'un accès Internet, le système est automatiquement mis à niveau. Auparavant, la mise à niveau s'est produite après un temps spécifique écoulé depuis la dernière activité de l'utilisateur. Avec cette version, la classification BlueXP est mise à niveau automatiquement si l'heure locale est comprise entre 1:00 AM et 5:00 AM. Si l'heure locale est en dehors de ces heures, la mise à niveau se produit après un délai spécifique écoulé depuis la dernière activité de l'utilisateur. Pour plus de détails, reportez-vous à "Installez sur un hôte Linux avec accès à Internet".

Si vous avez déployé la classification BlueXP sans accès à Internet, vous devez effectuer une mise à niveau manuelle. Pour plus de détails, reportez-vous à "Installez la classification BlueXP sur un hôte Linux sans accès Internet".

4 mars 2024 (version 1.29)

Vous pouvez maintenant exclure les données de numérisation qui résident dans certains répertoires de sources de données

Si vous souhaitez que la classification BlueXP exclut les données d'analyse qui résident dans certains répertoires de sources de données, vous pouvez ajouter ces noms de répertoires à un fichier de configuration traité par la classification BlueXP. Cette fonction vous permet d'éviter d'analyser des répertoires qui ne sont pas nécessaires ou qui pourraient renvoyer de faux résultats positifs pour les données personnelles.

"En savoir plus >>".

La prise en charge des instances extra-volumineuses est désormais qualifiée

Si vous avez besoin de la classification BlueXP pour analyser plus de 250 millions de fichiers, vous pouvez utiliser une très grande instance dans votre déploiement cloud ou votre installation sur site. Ce type de système peut analyser jusqu'à 500 millions de fichiers.

"En savoir plus >>".

10 janvier 2024 (version 1.27)

Les résultats de la page d'enquête affichent désormais la taille totale en plus du nombre total d'éléments

Les résultats filtrés de la page Investigation affichent désormais la taille totale des éléments en plus du nombre total de fichiers. Cela peut vous aider lors du déplacement de fichiers, de la suppression de fichiers, etc.

Configurer des ID de groupe supplémentaires comme « ouvert à l'entreprise »

Vous pouvez désormais configurer les ID de groupe dans NFS pour qu'ils soient considérés comme « ouverts à l'entreprise » directement dans la classification BlueXP si le groupe n'avait pas été défini initialement avec cette autorisation. Tous les fichiers et dossiers auxquels ces ID de groupe sont joints s'affichent comme « Ouvrir à l'organisation » dans la page Détails de l'enquête. Découvrez comment "Ajouter des ID de groupe supplémentaires comme « ouvert à l'organisation »".

14 décembre 2023 (version 1.26.6)

Cette version comprend quelques améliorations mineures.

La version a également supprimé les options suivantes :

- L'option permettant d'activer la collecte des journaux d'audit a été désactivée.
- Lors de l'enquête répertoires, l'option permettant de calculer le nombre de données d'informations personnelles identifiables (PII) par répertoires n'est pas disponible. Reportez-vous à la section "Examinez les données stockées dans votre organisation".
- L'option d'intégration des données à l'aide d'étiquettes Azure information protection (AIP) a été désactivée. Reportez-vous à la section "Organisez vos données privées".

6 novembre 2023 (version 1.26.3)

Les problèmes suivants ont été résolus dans cette version

- Correction d'une incohérence lors de la présentation du nombre de fichiers analysés par le système dans les tableaux de bord.
- Amélioration du comportement de numérisation en gérant et en signalant les fichiers et répertoires avec des caractères spéciaux dans le nom et les métadonnées.

4 octobre 2023 (version 1.26)

Prise en charge des installations sur site de la classification BlueXP sur RHEL version 9

Les versions 8 et 9 de Red Hat Enterprise Linux ne prennent pas en charge le moteur Docker requis pour l'installation de classification BlueXP. Nous prenons désormais en charge l'installation de classification BlueXP sur RHEL 9.0, 9.1 et 9.2 en utilisant Podman version 4 ou ultérieure comme infrastructure de conteneur. Si votre environnement requiert l'utilisation des dernières versions de RHEL, vous pouvez désormais installer la classification BlueXP (version 1.26 ou supérieure) lorsque vous utilisez Podman.

À l'heure actuelle, nous ne prenons pas en charge les installations de sites invisibles ou les environnements de numérisation distribués (à l'aide d'un scanner maître et distant) lors de l'utilisation de RHEL 9.x.

5 septembre 2023 (version 1.25)

Petits et moyens déploiements temporairement indisponibles

Lorsque vous déployez une instance de classification BlueXP dans AWS, l'option de sélectionner **Deploy > Configuration** et de choisir une instance de petite ou moyenne taille n'est pas disponible pour le moment. Vous pouvez toujours déployer l'instance à l'aide de la grande taille d'instance en sélectionnant **déployer > déployer**.

Appliquez des balises sur un maximum de 100,000 éléments à partir de la page Résultats d'enquête

Dans le passé, vous ne pouviez appliquer des balises qu'à une seule page à la fois dans la page Résultats d'enquête (20 éléments). Vous pouvez maintenant sélectionner **tous** éléments dans les pages Résultats d'enquête et appliquer des balises à tous les éléments - jusqu'à 100,000 éléments à la fois. "Découvrez comment".

Identifiez les fichiers dupliqués avec une taille de fichier minimale de 1 Mo

Classification BlueXP utilisée pour identifier les fichiers dupliqués uniquement lorsque les fichiers étaient de 50 Mo ou plus. Désormais, les fichiers dupliqués commençant par 1 Mo peuvent être identifiés. Vous pouvez utiliser les filtres de la page Investigation « taille du fichier » ainsi que « doublons » pour voir quels fichiers d'une certaine taille sont dupliqués dans votre environnement.

17 juillet 2023 (version 1.24)

Deux nouveaux types de données personnelles allemandes sont identifiés par la classification BlueXP

La classification BlueXP peut identifier et catégoriser les fichiers qui contiennent les types de données suivants :

- ID allemand (Personalausweisnummer)
- Numéro de sécurité sociale allemand (Sozialversicherungsnummer)

"Consultez tous les types de données personnelles que la classification BlueXP peut identifier dans vos données".

La classification BlueXP est entièrement prise en charge en mode restreint et en mode privé

La classification BlueXP est désormais entièrement prise en charge sur les sites sans accès Internet (mode privé) et avec un accès Internet sortant limité (mode restreint). "En savoir plus sur les modes de déploiement BlueXP pour Connector".

Possibilité d'ignorer les versions lors de la mise à niveau d'une installation en mode privé de la classification BlueXP

Vous pouvez maintenant effectuer la mise à niveau vers une version plus récente de la classification BlueXP, même s'il n'est pas séquentiel. Cela signifie que la limitation actuelle de la mise à niveau de la classification BlueXP par une version à la fois n'est plus nécessaire. Cette fonction est pertinente à partir de la version 1.24.

L'API de classification BlueXP est disponible

L'API de classification BlueXP vous permet d'effectuer des actions, de créer des requêtes et d'exporter des informations sur les données que vous analysez. La documentation interactive est disponible à l'aide de swagger. La documentation est divisée en plusieurs catégories, notamment Investigation, Compliance, Governance et Configuration. Chaque catégorie fait référence aux onglets de l'interface de classification BlueXP.

"En savoir plus sur les API de classification BlueXP".

6 juin 2023 (version 1.23)

Le japonais est désormais pris en charge lors de la recherche de noms de sujet de données

Les noms japonais peuvent maintenant être saisis lors de la recherche du nom d'un sujet en réponse à une demande d'accès de la personne concernée (DSAR, Data Subject Access Request). Vous pouvez générer un "Rapport de demande d'accès au sujet des données" avec les informations obtenues. Vous pouvez également entrer des noms japonais dans le "Filtre « sujet des données » dans la page enquête sur les données" pour identifier les fichiers contenant le nom du sujet.

Ubuntu est maintenant une distribution Linux prise en charge sur laquelle vous pouvez installer la classification BlueXP

Ubuntu 22.04 a été qualifié comme système d'exploitation pris en charge pour la classification BlueXP. Vous pouvez installer la classification BlueXP sur un hôte Ubuntu Linux de votre réseau ou sur un hôte Linux dans le cloud en utilisant la version 1.23 du programme d'installation. "Découvrez comment installer la classification BlueXP sur un hôte avec Ubuntu installé".

Red Hat Enterprise Linux 8.6 et 8.7 ne sont plus pris en charge par les nouvelles installations de classification BlueXP

Ces versions ne sont pas prises en charge par les nouveaux déploiements, car Red Hat ne prend plus en charge Docker, ce qui est un prérequis. Si vous disposez d'un ordinateur de classification BlueXP sous RHEL 8.6 ou 8.7, NetApp continuera à prendre en charge votre configuration.

La classification BlueXP peut être configurée en tant que collecteur FPolicy pour recevoir les événements FPolicy des systèmes ONTAP

Vous pouvez activer la collecte des journaux d'audit de l'accès aux fichiers sur votre système de classification BlueXP pour les événements d'accès aux fichiers détectés sur les volumes de vos environnements de travail. La classification BlueXP peut capturer les types d'événements FPolicy suivants et les utilisateurs qui ont effectué les actions sur vos fichiers : créer, lire, écrire, supprimer, renommer, Modifiez le propriétaire/les autorisations et modifiez SACL/DACL.

Les licences Data Sense BYOL sont désormais prises en charge sur les sites invisibles

Vous pouvez désormais charger votre licence Data Sense BYOL dans le portefeuille digital BlueXP situé dans un site invisible pour que vous soyez averti lorsque le niveau de licence est faible. "Découvrez comment

obtenir et télécharger votre licence Data Sense BYOL".

3 avril 2023 (version 1.22)

Nouveau rapport d'évaluation de découverte de données

Le rapport d'évaluation de la découverte de données fournit une analyse de haut niveau de votre environnement analysé afin de mettre en évidence les résultats du système et de montrer les points préoccupants et les étapes de correction potentielles. L'objectif de ce rapport est de sensibiliser les clients aux préoccupations liées à la gouvernance des données, à l'exposition aux risques en matière de sécurité des données et aux lacunes de conformité de leurs jeux de données. "Découvrez comment générer et utiliser le rapport d'évaluation de découverte de données".

Possibilité de déployer la classification BlueXP sur des instances plus petites dans le cloud

Lors du déploiement de la classification BlueXP à partir d'un connecteur BlueXP dans un environnement AWS, vous pouvez désormais choisir entre deux types d'instances plus petits que ceux disponibles avec l'instance par défaut. Si vous analysez un petit environnement, vous pouvez réduire vos coûts liés au cloud. Cependant, il existe des restrictions lors de l'utilisation de la plus petite instance. "Voir les types d'instances et les limites disponibles".

Un script autonome est désormais disponible pour qualifier votre système Linux avant l'installation de la classification BlueXP

Si vous souhaitez vérifier que votre système Linux répond à toutes les conditions préalables, indépendamment de l'installation de la classification BlueXP, vous pouvez télécharger un script distinct qui teste uniquement les prérequis. "Découvrez comment vérifier si votre hôte Linux est prêt à installer la classification BlueXP".

7 mars 2023 (version 1.21)

Nouvelle fonctionnalité permettant d'ajouter vos propres catégories personnalisées à partir de l'interface de classification BlueXP

La classification BlueXP vous permet désormais d'ajouter vos propres catégories personnalisées afin que la classification BlueXP identifie les fichiers qui s'intègrent dans ces catégories. La classification BlueXP en a beaucoup "catégories prédéfinies", cette fonction vous permet d'ajouter des catégories personnalisées pour identifier l'endroit où les informations propres à votre organisation se trouvent dans vos données.

"En savoir plus >>".

Vous pouvez désormais ajouter des mots-clés personnalisés à partir de l'interface de classification BlueXP

La classification BlueXP a eu la possibilité d'ajouter des mots-clés personnalisés que la classification BlueXP identifiera pendant un certain temps lors des analyses futures. Toutefois, vous avez dû vous connecter à l'hôte de classification BlueXP Linux et utiliser une interface de ligne de commande pour ajouter des mots-clés. Dans cette version, l'ajout de mots-clés personnalisés se fait dans l'interface de classification BlueXP, ce qui facilite considérablement l'ajout et la modification de ces mots-clés.

"En savoir plus sur l'ajout de mots-clés personnalisés à partir de l'interface de classification BlueXP".

Possibilité de disposer de fichiers de classification BlueXP NOT lors de la modification de l'« heure du dernier accès »

Par défaut, si la classification BlueXP ne dispose pas des autorisations d'écriture adéquates, le système ne scrutera pas les fichiers de vos volumes, car la classification BlueXP ne peut pas rétablir l'heure du dernier accès à l'horodatage d'origine. Cependant, si vous ne vous souciez pas de savoir si l'heure du dernier accès est réinitialisée à l'heure d'origine dans vos fichiers, vous pouvez remplacer ce comportement dans la page Configuration afin que la classification BlueXP analyse les volumes indépendamment des autorisations.

Grâce à cette fonctionnalité, et un nouveau filtre nommé « événement d'analyse » a été ajouté. Vous pouvez ainsi afficher les fichiers non classifiés, car la classification BlueXP n'a pas pu rétablir l'heure du dernier accès, ou les fichiers classés même si la classification BlueXP n'a pas pu rétablir l'heure du dernier accès.

"En savoir plus sur l'horodatage du dernier accès et les autorisations requises par la classification BlueXP".

Trois nouveaux types de données personnelles sont identifiés par la classification BlueXP

La classification BlueXP peut identifier et catégoriser les fichiers qui contiennent les types de données suivants :

- Numéro de carte d'identité Botswana (Omang)
- Botswana Numéro de passeport
- Carte d'identité nationale d'enregistrement de Singapour (NRIC)

"Consultez tous les types de données personnelles que la classification BlueXP peut identifier dans vos données".

Mise à jour des fonctionnalités des répertoires

- L'option « Rapport CSV léger » pour les rapports d'investigation de données inclut désormais des informations provenant des répertoires.
- Le filtre heure « dernier accès » affiche désormais l'heure du dernier accès pour les fichiers et les répertoires.

Améliorations apportées à l'installation

- Le programme d'installation de classification BlueXP pour les sites sans accès à Internet (sites invisibles) effectue désormais un pré-contrôle pour s'assurer que vos exigences système et réseau sont en place pour une installation réussie.
- Les fichiers journaux d'audit d'installation sont enregistrés maintenant ; ils sont écrits dans `/ops/netapp/install_logs`.

5 février 2023 (version 1.20)

Possibilité d'envoyer des e-mails de notification basés sur des règles à n'importe quelle adresse e-mail

Dans les versions précédentes de la classification BlueXP, vous pouviez envoyer des alertes par e-mail aux utilisateurs BlueXP de votre compte lorsque certaines stratégies stratégiques renvoient des résultats. Cette fonction vous permet d'obtenir des notifications pour protéger vos données lorsque vous n'êtes pas en ligne. Vous pouvez désormais envoyer des alertes par e-mail à partir de stratégies à tous les autres utilisateurs - jusqu'à 20 adresses e-mail - qui ne sont pas dans votre compte BlueXP.

"En savoir plus sur l'envoi d'alertes par e-mail basées sur les résultats des règles".

Vous pouvez désormais ajouter des modèles personnels à partir de l'interface de classification BlueXP

La classification BlueXP a eu la possibilité d'ajouter des « données personnelles » personnalisées que la classification BlueXP identifiera lors des analyses futures pendant un certain temps. Cependant, vous avez dû vous connecter à l'hôte de classification BlueXP Linux et utiliser une ligne de commande pour ajouter les modèles personnalisés. Dans cette version, l'ajout de modèles personnels à l'aide d'un regex se fait dans l'interface de classification de BlueXP, ce qui facilite considérablement l'ajout et la modification de ces modèles personnalisés.

"En savoir plus sur l'ajout de modèles personnalisés à partir de l'interface de classification BlueXP".

Possibilité de déplacer 15 millions de fichiers à l'aide de la classification BlueXP

Par le passé, vous pouviez déplacer jusqu'à 100,000 fichiers source vers n'importe quel partage NFS grâce à la classification BlueXP. Vous pouvez désormais déplacer jusqu'à 15 millions de fichiers à la fois. "En savoir plus sur le déplacement des fichiers source à l'aide de la classification BlueXP".

Possibilité de voir le nombre d'utilisateurs ayant accès aux fichiers SharePoint Online

Le filtre « nombre d'utilisateurs avec accès » prend désormais en charge les fichiers stockés dans les référentiels SharePoint Online. Auparavant, seuls les fichiers stockés sur des partages CIFS étaient pris en charge. Notez que les groupes SharePoint qui ne sont pas actifs basés sur un répertoire ne seront pas pris en compte dans ce filtre à l'heure actuelle.

Le nouvel état « réussite partielle » a été ajouté au panneau État de l'action

Le nouvel état « réussite partielle » indique qu'une action de classification BlueXP est terminée, que certains éléments ont échoué et que certains éléments ont réussi, par exemple, lorsque vous déplacez ou supprimez des fichiers 100. De plus, le statut « terminé » a été renommé « succès ». Par le passé, l'état « terminé » peut lister les actions qui ont réussi et qui ont échoué. Désormais, le statut « réussite » signifie que toutes les actions ont réussi sur tous les éléments. "Voir comment afficher le panneau Etat des actions".

9 janvier 2023 (version 1.19)

Possibilité d'afficher un graphique de fichiers contenant des données sensibles et qui sont trop permissives

Le tableau de bord gouvernance a ajouté une nouvelle zone données et autorisations larges_ qui fournit une carte thermique de fichiers contenant des données sensibles (y compris des données personnelles sensibles et sensibles) et qui sont trop permissives. Cela vous aide à déterminer les risques liés aux données sensibles. "En savoir plus >>".

Trois nouveaux filtres sont disponibles dans la page Data Investigation

De nouveaux filtres sont disponibles pour affiner les résultats affichés dans la page recherche de données :

- Le filtre « nombre d'utilisateurs avec accès » indique quels fichiers et dossiers sont ouverts à un certain nombre d'utilisateurs. Vous pouvez choisir une plage de nombres pour affiner les résultats, par exemple pour voir quels fichiers sont accessibles par 51-100 utilisateurs.
- Les filtres « heure créée », « heure découverte », « dernière modification » et « dernier accès » vous permettent désormais de créer une plage de dates personnalisée au lieu de sélectionner une plage de jours prédéfinie. Par exemple, vous pouvez rechercher des fichiers avec une "heure de création" "plus de 6 mois", ou avec une "date de dernière modification" dans les "10 derniers jours".

- Le filtre "chemin du fichier" vous permet maintenant de spécifier les chemins que vous souhaitez exclure des résultats de la requête filtrée. Si vous entrez des chemins pour inclure et exclure certaines données, la classification BlueXP recherche d'abord tous les fichiers des chemins inclus, puis supprime les fichiers des chemins exclus, puis affiche les résultats.

"Voir la liste de tous les filtres que vous pouvez utiliser pour examiner vos données".

La classification BlueXP peut identifier le numéro individuel japonais

La classification BlueXP peut identifier et catégoriser les fichiers qui contiennent le numéro individuel japonais (également appelé mon numéro). Cela inclut à la fois le numéro mon personnel et celui de l'entreprise. "Consultez tous les types de données personnelles que la classification BlueXP peut identifier dans vos données".

Limites connues

Les limitations connues identifient les fonctions qui ne sont pas prises en charge par cette version du produit ou qui ne sont pas compatibles avec lui. Examinez attentivement ces limites.

Options supprimées de la version de classification BlueXP

La version de décembre 2023 (version 1.26.6) a supprimé les options suivantes :

- L'option permettant d'activer la collecte des journaux d'audit a été désactivée.
- Lors de l'enquête répertoires, l'option permettant de calculer le nombre de données d'informations personnelles identifiables (PII) par répertoires n'est pas disponible.
- L'option d'intégration des données à l'aide d'étiquettes Azure information protection (AIP) a été désactivée.

Limites de l'analyse de classification BlueXP

La classification BlueXP analyse un seul partage sous un volume

Si vous avez plusieurs partages de fichiers sous un seul volume, la classification BlueXP analyse le partage avec la hiérarchie la plus élevée. Par exemple, si vous avez des partages comme les suivants :

- /A
- /A/B.
- /C
- /D/E.

Les données dans /A seront ensuite analysées. Les données dans /C et /D ne seront pas analysées.

Solution de contournement

Il existe une solution pour vous assurer que vous analysez les données de tous les partages de votre volume. Voici la procédure à suivre :

1. Dans l'environnement de travail, ajoutez le volume à scanner.
2. Une fois que la classification BlueXP a terminé l'analyse du volume, accédez à la page *Data Investigation* et créez un filtre pour voir quel partage est en cours d'analyse :

Vous allez filtrer les données par « Nom de l'environnement de travail » et « Type de répertoire = partage » pour voir quel partage est analysé.

3. Obtenez la liste complète des partages qui existent dans le volume pour voir quels partages ne sont pas analysés.
4. "Ajoutez les partages restants à un groupe de partages".

   Vous devrez ajouter tous les partages individuellement, par exemple :

   ```
   /C
   /D
   ```

5. Procédez comme suit pour chaque volume de l'environnement de travail qui a plusieurs partages.

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.

IMPORTANT

À partir de mai 2024 avec la version 1.31, la classification BlueXP est désormais disponible en tant que fonctionnalité clé dans BlueXP, sans frais supplémentaires. Aucune licence de classification ni aucun abonnement n'est requis. Nous avons également concentré la fonctionnalité de classification BlueXP sur les systèmes de stockage NetApp. Ainsi, certaines fonctionnalités inutilisées ou sous-utilisées ont été désapprouvées.

"Voir la liste des fonctions obsolètes".

Les utilisateurs qui utilisent des versions 1.30 ou antérieures héritées pourront continuer à utiliser cette version jusqu'à expiration de leur abonnement.

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

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

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 et CIFS 1.x, 2.0, 2.1 et 3.0.

Le coût

La classification BlueXP est désormais 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.

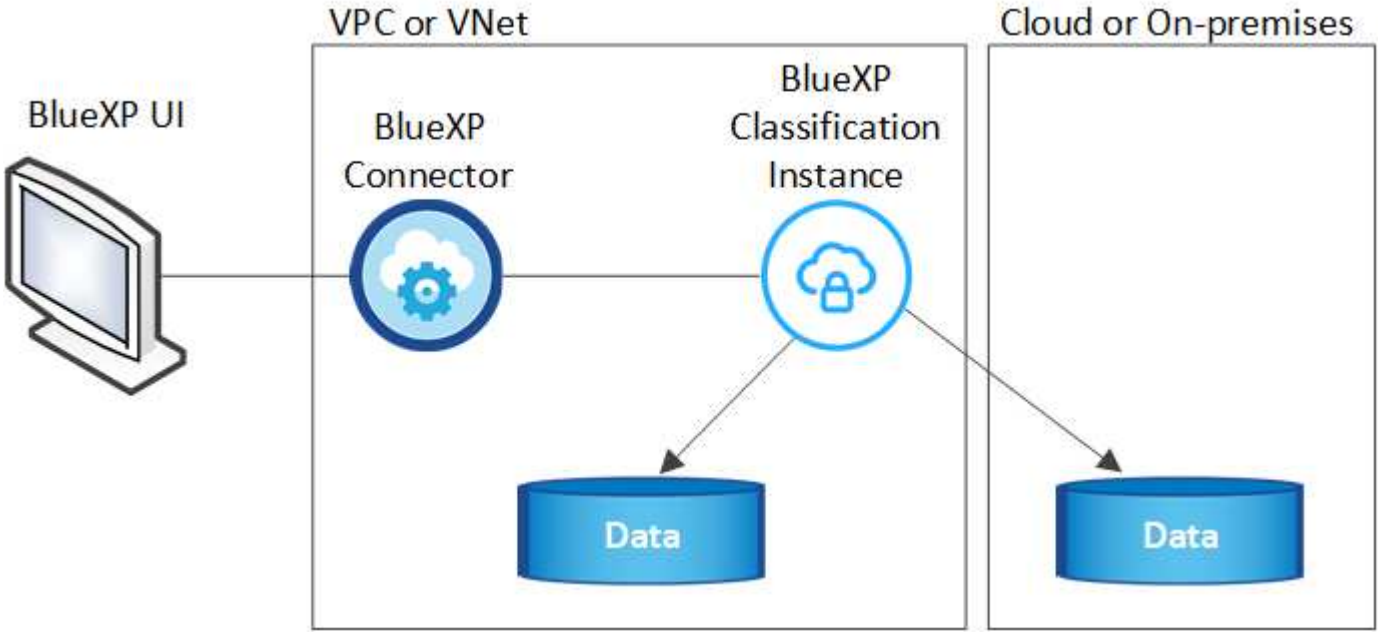
Coûts de transfert de données

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

Vous pouvez déployer la classification BlueXP sur un système avec moins de processeurs et moins de RAM.

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 classification BlueXP

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

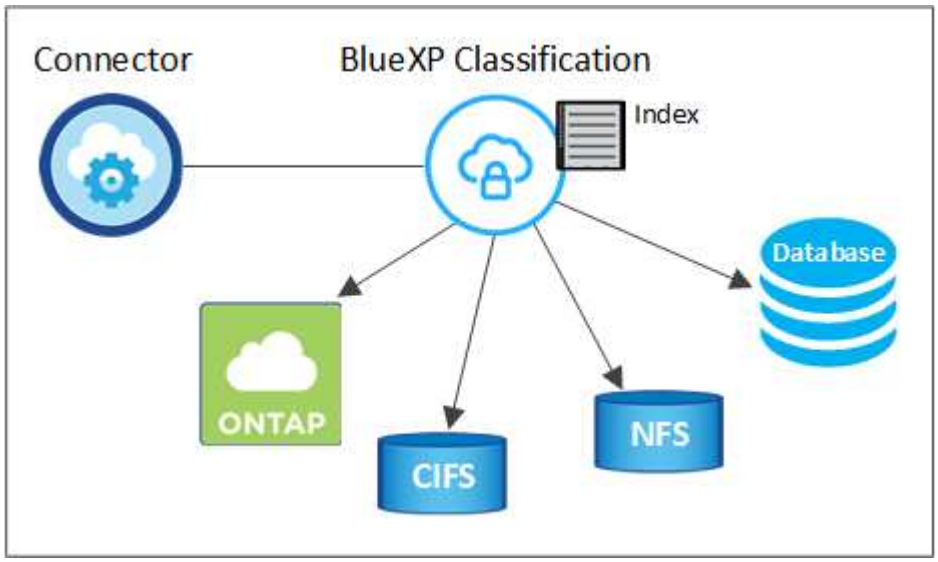
1. Déployez une instance de classification BlueXP dans BlueXP.
2. Vous activez la cartographie de haut niveau ou la numérisation de haut niveau sur une ou plusieurs sources de données.
3. La classification BlueXP analyse les données à l'aide d'un processus d'apprentissage par l'IA.
4. Vous utilisez les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

Fonctionnement des acquisitions

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 à séquence périodique pour détecter les modifications incrémentielles (c'est pourquoi il est important de maintenir l'instance en fonctionnement).

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

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

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

Le tableau ci-dessous présente certaines des différences :

Fonction	Classement	Mappage
Vitesse de numérisation	Lentes	Rapides
Tarifs	Libre	Libre
Puissance	Limité à 500 To	Limité à 500 To
Liste des types de fichiers et de la capacité utilisée	Oui.	Oui.
Nombre de fichiers et capacité utilisée	Oui.	Oui.

Fonction	Classement	Mappage
Âge et taille des fichiers	Oui.	Oui.
Exécution d'un "Rapport de mappage de données"	Oui.	Oui.
Page Data Investigation pour afficher les détails du fichier	Oui.	Non
Rechercher des noms dans les fichiers	Oui.	Non
Création "stratégies" fournissant des résultats de recherche personnalisés	Oui.	Non
Possibilité d'exécuter d'autres rapports	Oui.	Non
Possibilité de voir les métadonnées des fichiers*	Non	Oui.

*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.
Des règles prédéfinies	Oui.	Non
Règles personnalisées	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
Stratégies	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 d'analyses de mappage, la classification BlueXP peut analyser entre 100-150 Tibs de données par

jour.

- Lors des analyses de classification, la classification BlueXP peut analyser entre 15-40 Tibs de données par jour.

Informations catégorisées par la classification BlueXP

La classification BlueXP collecte, indexe et attribue des catégories à vos données (fichiers). Les données index par classification BlueXP sont les 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 (PII) telles que les adresses électroniques, les numéros d'identification ou les numéros de carte de crédit. "En savoir plus sur les données personnelles".
- **Données personnelles sensibles** : 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 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

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 desservie par 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. NetApp et des tiers ne peuvent donc 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".

Rôles d'utilisateur dans la classification BlueXP

Le rôle attribué à chaque utilisateur fournit des fonctionnalités différentes dans BlueXP et dans la classification BlueXP . Pour plus de détails, reportez-vous aux sections suivantes :

- "Rôles IAM BlueXP " (Lors de l'utilisation de BlueXP en mode standard)
- "Rôles de compte BlueXP " (Lors de l'utilisation de BlueXP en mode restreint ou privé)

Déployez la classification BlueXP

Quel déploiement de classification BlueXP devez-vous utiliser ?

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

La classification BlueXP peut être déployée de plusieurs manières :

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

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

Reportez-vous à la section "Vérifiez que votre hôte Linux est prêt à installer la classification BlueXP".

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

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

Notez que vous pouvez également "Installez la classification BlueXP sur un hôte Linux disposant d'un accès Internet". Ce type d'installation peut être une bonne option si vous préférez analyser les systèmes ONTAP sur site à l'aide d'une instance de classification BlueXP également située sur site, mais ce n'est pas une exigence. Le logiciel fonctionne exactement de la même manière quelle que soit la méthode d'installation choisie.

Démarrage rapide

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

1 Créer un connecteur

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

Vous pouvez également "Installer le connecteur sur site" Sur un hôte Linux de votre réseau ou sur un hôte Linux du cloud.

2 Passer en revue les prérequis

Assurez-vous que votre environnement est conforme aux conditions préalables. Notamment l'accès Internet

sortant pour l'instance, la connectivité entre le connecteur et la classification BlueXP via le port 443, etc. Voir la liste complète.

3 Déployez la classification BlueXP

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

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".

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 - nous ne

prenons actuellement pas en charge les proxys transparents.

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

Terminaux requis pour AWS

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

Terminaux requis pour Azure

Terminaux	Objectif
https://api.bluexp.netapp.com	Communication avec le service BlueXP, qui inclut les comptes NetApp.
https://netapp-cloud-account.auth0.com https://auth0.com	Communication avec le site Web BlueXP pour l'authentification centralisée des utilisateurs.
https://support.compliance.api.bluexp.netapp.com/ https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Permet d'accéder aux images logicielles, aux manifestes, aux modèles et à l'envoi de journaux et de mesures.
https://support.compliance.api.bluexp.netapp.com/	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.

Terminaux requis pour GCP

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

Terminaux	Objectif
https://support.compliance.api.bluexp.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 les ressources et créer des groupes de sécurité pour l'instance de classification BlueXP. Vous trouverez les dernières autorisations BlueXP dans "Règles fournies par NetApp".

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

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

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

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

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

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

Assurez la connectivité du navigateur web à la classification BlueXP

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

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

Vérifiez les limites de vos CPU virtuels

Assurez-vous que la limite de CPU virtuels de votre fournisseur cloud permet le déploiement d'une instance avec le nombre de cœurs nécessaire. Vous devez vérifier la limite de CPU virtuels pour la famille d'instances concernée dans la région où BlueXP est en cours d'exécution. "Voir les types d'instances requis".

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

- "Documentation AWS : quotas de service Amazon EC2"

- "Documentation Azure : quotas de vCPU de machine virtuelle"
- "Documentation Google Cloud : quotas de ressources"

Déployez la classification BlueXP dans le cloud

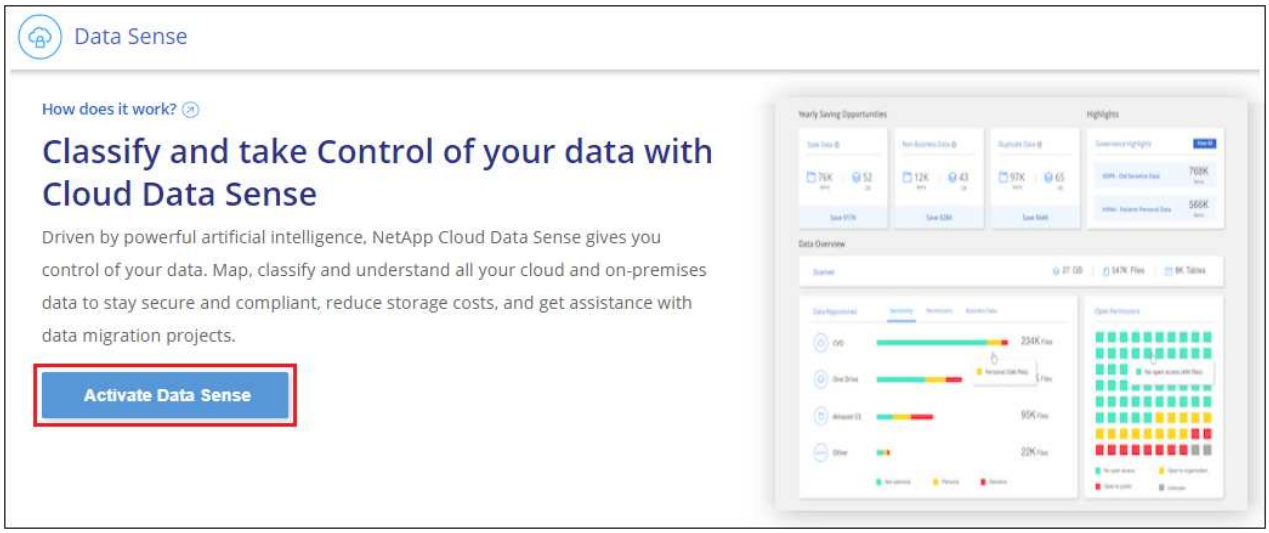
Suivez ces étapes pour déployer une instance de classification BlueXP dans le cloud. Le connecteur va déployer l'instance dans le cloud, puis installer le logiciel de classification BlueXP sur cette instance.

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, cliquez sur **gouvernance > Classification**.



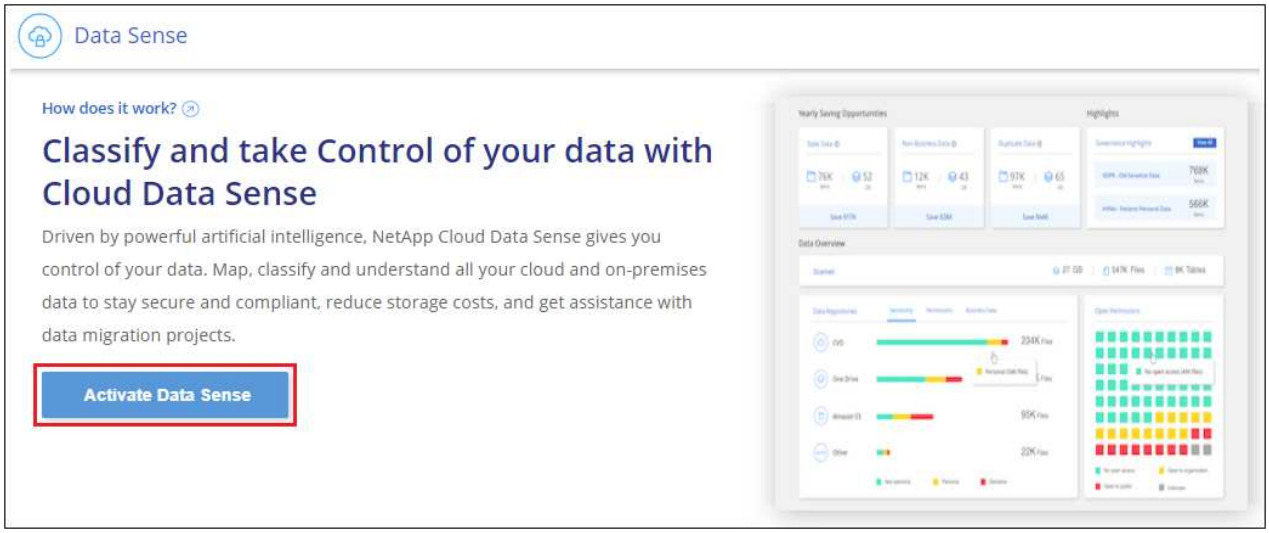
2. Cliquez sur **Activer détection de données**.
3. Sur la page *installation*, cliquez sur **déployer > déployer** pour utiliser la taille d'instance « grande » et lancer l'assistant de déploiement cloud.
4. L'assistant affiche la progression au fur et à mesure des étapes de déploiement. Il s'arrête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

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

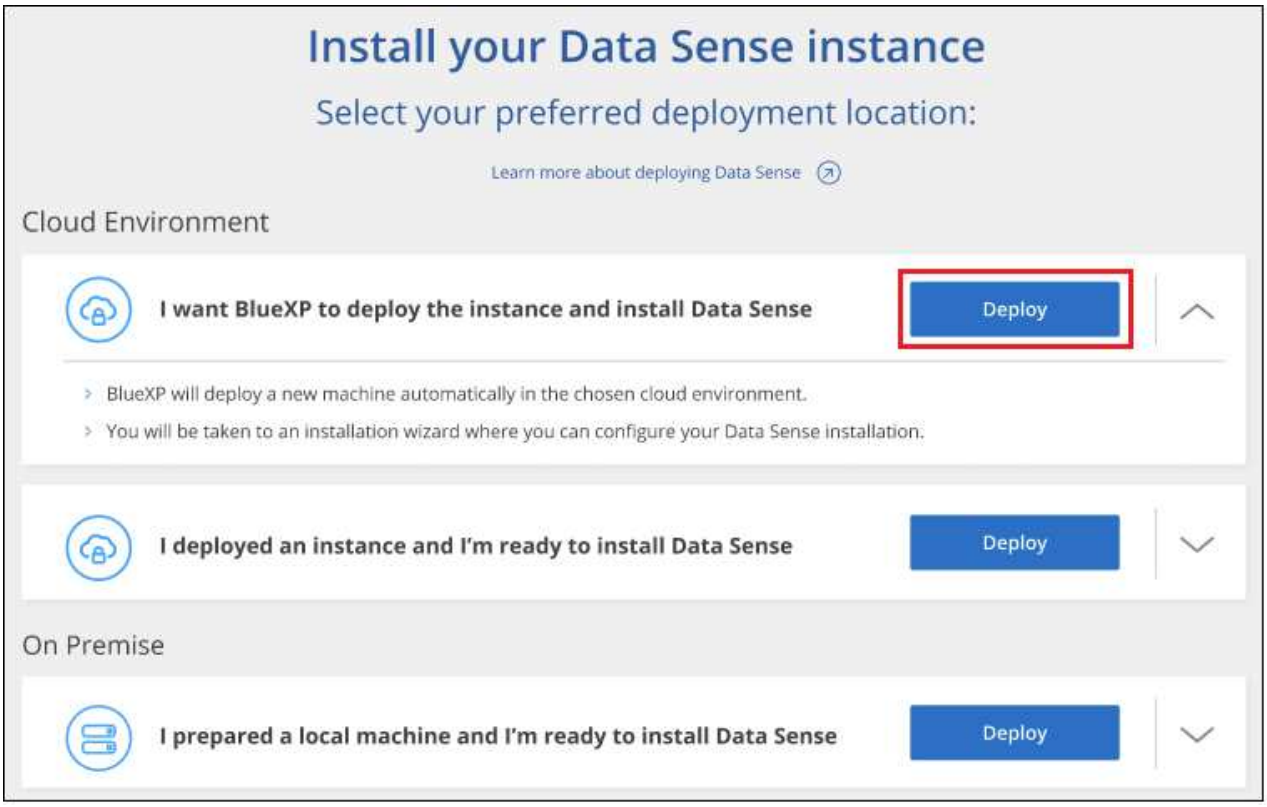
Déploiement dans Azure

Étapes

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



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



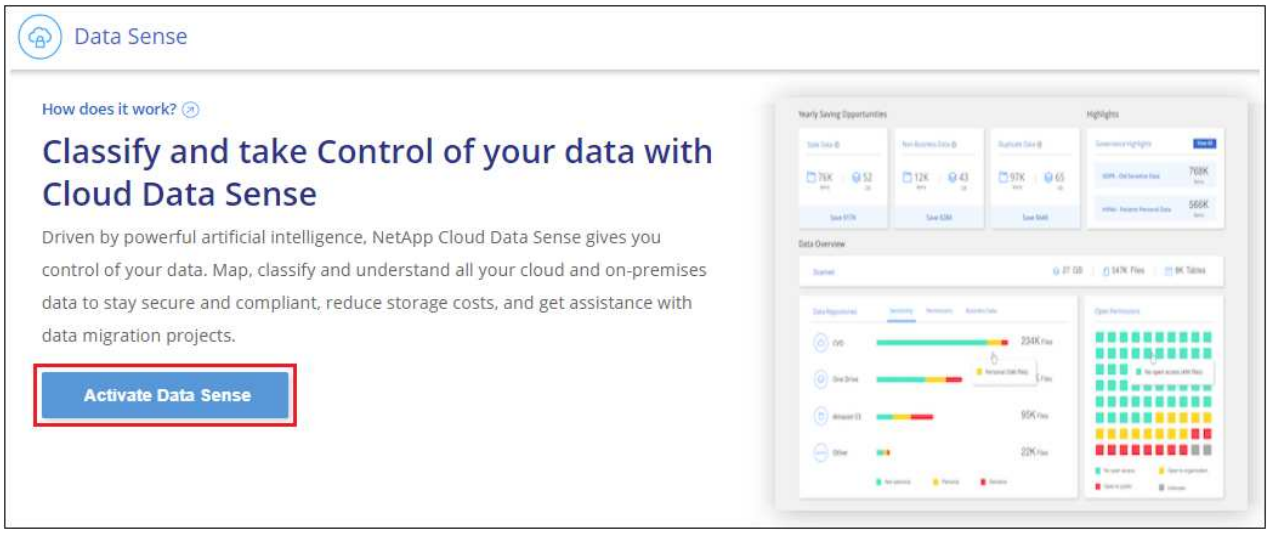
4. L'assistant affiche la progression au fur et à mesure des étapes de déploiement. Il s'arrête et vous invite à entrer s'il est en cours de problème.

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

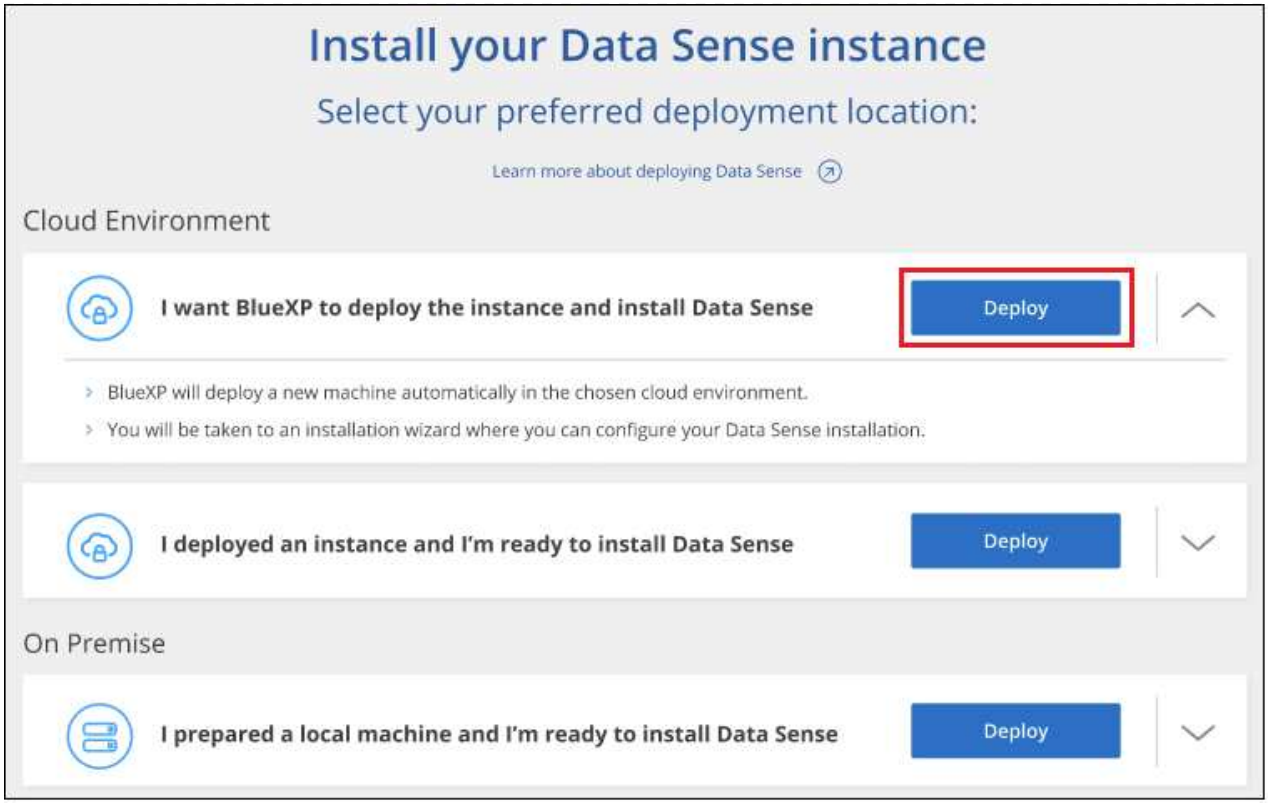
Déploiement dans Google Cloud

Étapes

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



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



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

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

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.

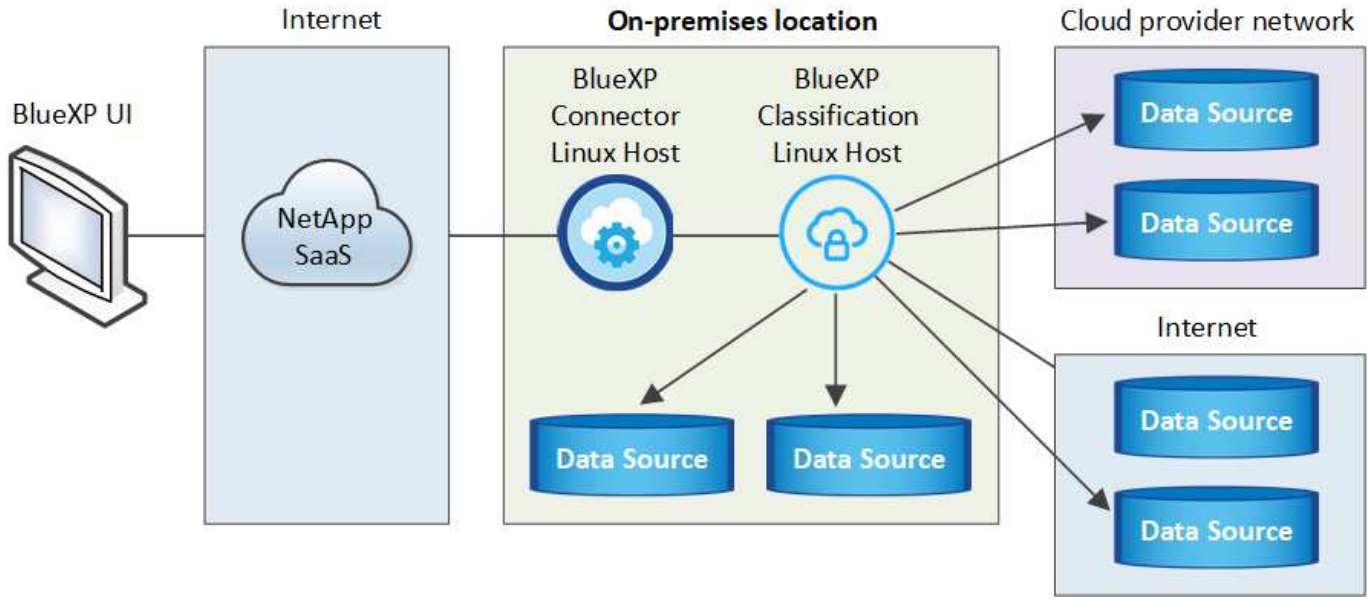
Installez la classification BlueXP sur un hôte disposant d'un accès Internet

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.

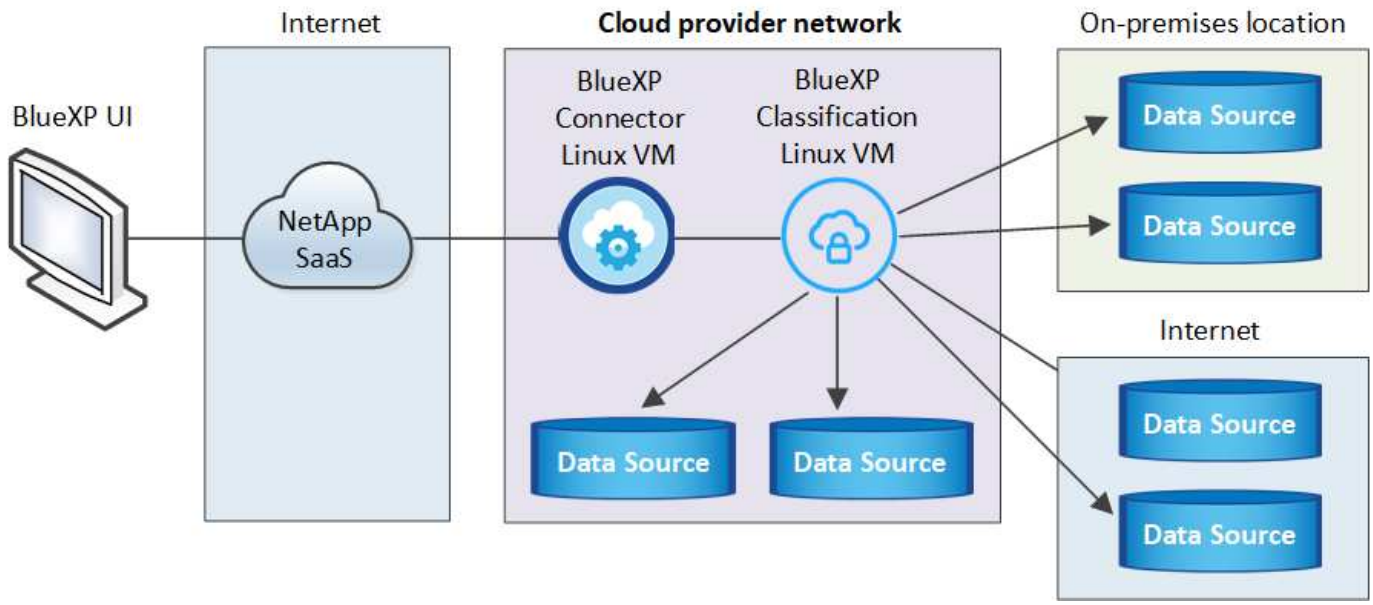
L'installation sur site peut être une bonne option si vous préférez analyser les systèmes ONTAP sur site à l'aide d'une instance de classification BlueXP également située sur site, mais ce n'est pas une exigence. Le logiciel fonctionne exactement de la même manière quelle que soit la méthode d'installation 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 configurations très volumineuses où vous allez analyser des pétaoctets de données, sur les versions 1.30 et antérieures, vous pouvez inclure plusieurs hôtes pour fournir une puissance de traitement supplémentaire. Lors de l'utilisation de plusieurs systèmes hôtes, le système principal est appelé le *Manager node*, et les systèmes supplémentaires qui fournissent une puissance de traitement supplémentaire sont appelés *scanner nodes*.

> 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" pour des sites totalement sécurisés.

> Pour les anciennes versions 1.30 et antérieures, pour ajouter des nœuds de scanner, reportez-vous à la section "Ajoutez des nœuds de scanner à un déploiement existant".

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 To SSD sur /, ou - 100 Gio disponible sur /opt - 895 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp
Grand	16 processeurs	64 GO DE RAM	500 Gio de SSD sur /, ou - 100 Gio disponible sur /opt - 395 Gio disponible sur /var/lib/docker ou pour Podman /var/lib/containers ou pour Podman /var/lib/containers - 5 Gio sur /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 version 8.8, 9.0, 9.1, 9.2, 9.3, 9.4

- **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.

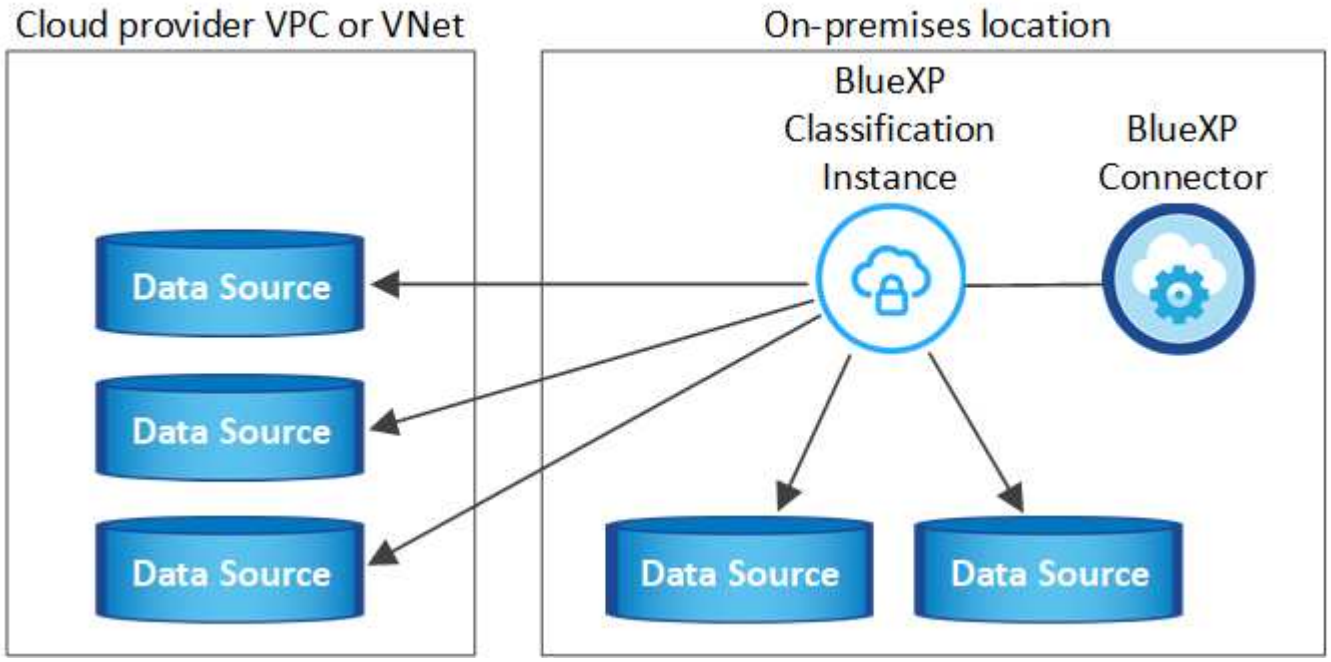
Type de connexion	Ports	Description
Classification de Connector <> BlueXP	8080 (TCP), 443 (TCP) et 80. 9000	Les règles de pare-feu ou de routage du connecteur doivent autoriser le trafic entrant et sortant via le port 443 vers et depuis l'instance de classification BlueXP. Assurez-vous que le port 8080 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.

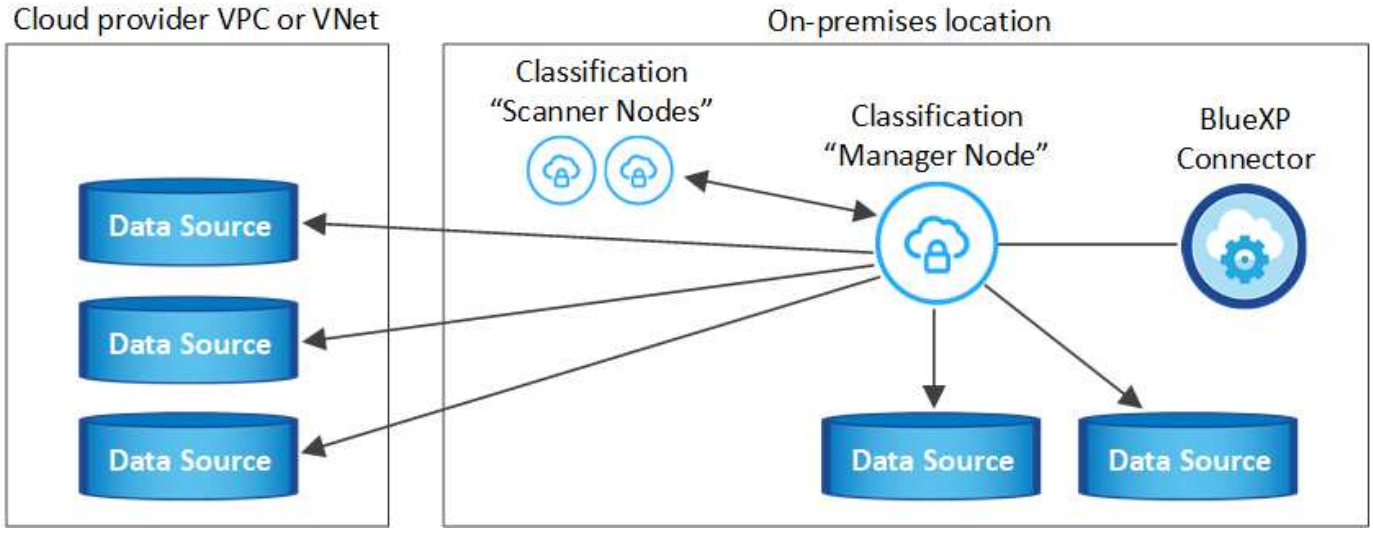
Type de connexion	Ports	Description
Classification BlueXP <> Active Directory	389 (TCP ET UDP), 636 (TCP), 3268 (TCP) ET 3269 (TCP)	Un Active Directory doit déjà être configuré pour les utilisateurs de votre entreprise. De plus, la classification BlueXP requiert des informations d'identification Active 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.



Pour les très grandes configurations dans lesquelles vous numérisez des pétaoctets de données, vous pouvez inclure plusieurs hôtes pour bénéficier d'une puissance de traitement supplémentaire. En savoir plus lien:task-Deploy-multi-host-install-dark-site.html> à propos de l'installation sur plusieurs hôtes pour de grandes configurations.



Voir Préparation du système hôte Linux et Vérification des prérequis Liste complète des exigences avant de déployer la classification BlueXP.

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

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

Installation à un seul hôte pour les configurations courantes

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

"Regardez cette vidéo" Pour voir comment installer la classification BlueXP.

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

Ce dont vous avez besoin

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

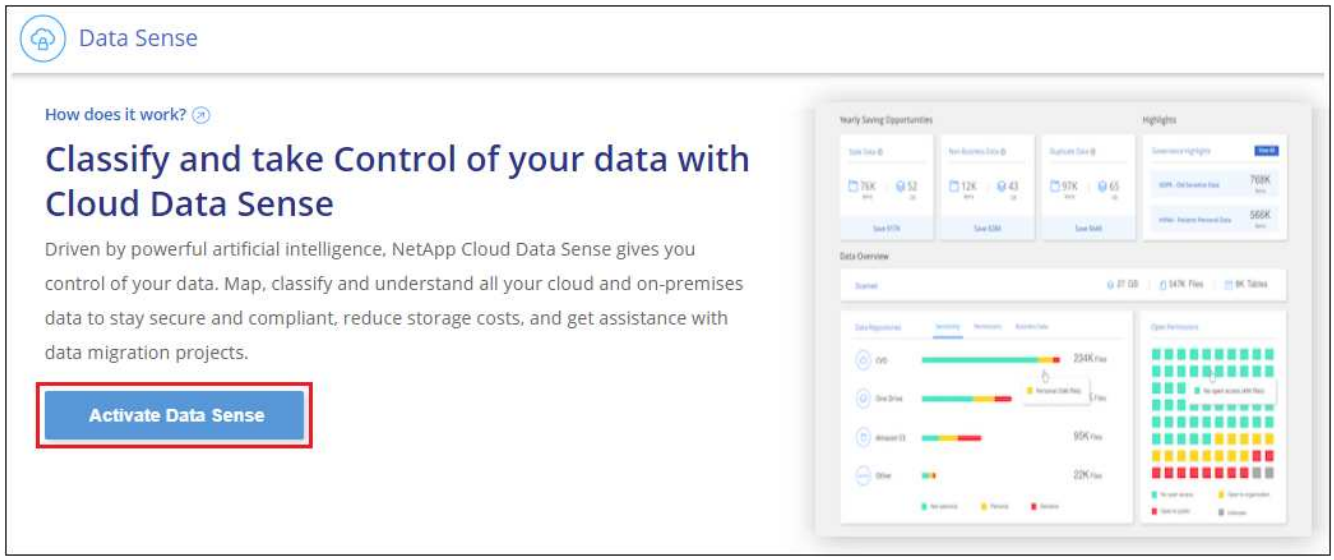
- L'utilisateur doit être un utilisateur local. Les utilisateurs du domaine ne sont pas pris en charge.
- Vérifiez que votre environnement hors ligne répond aux besoins autorisations et connectivité.

Étapes

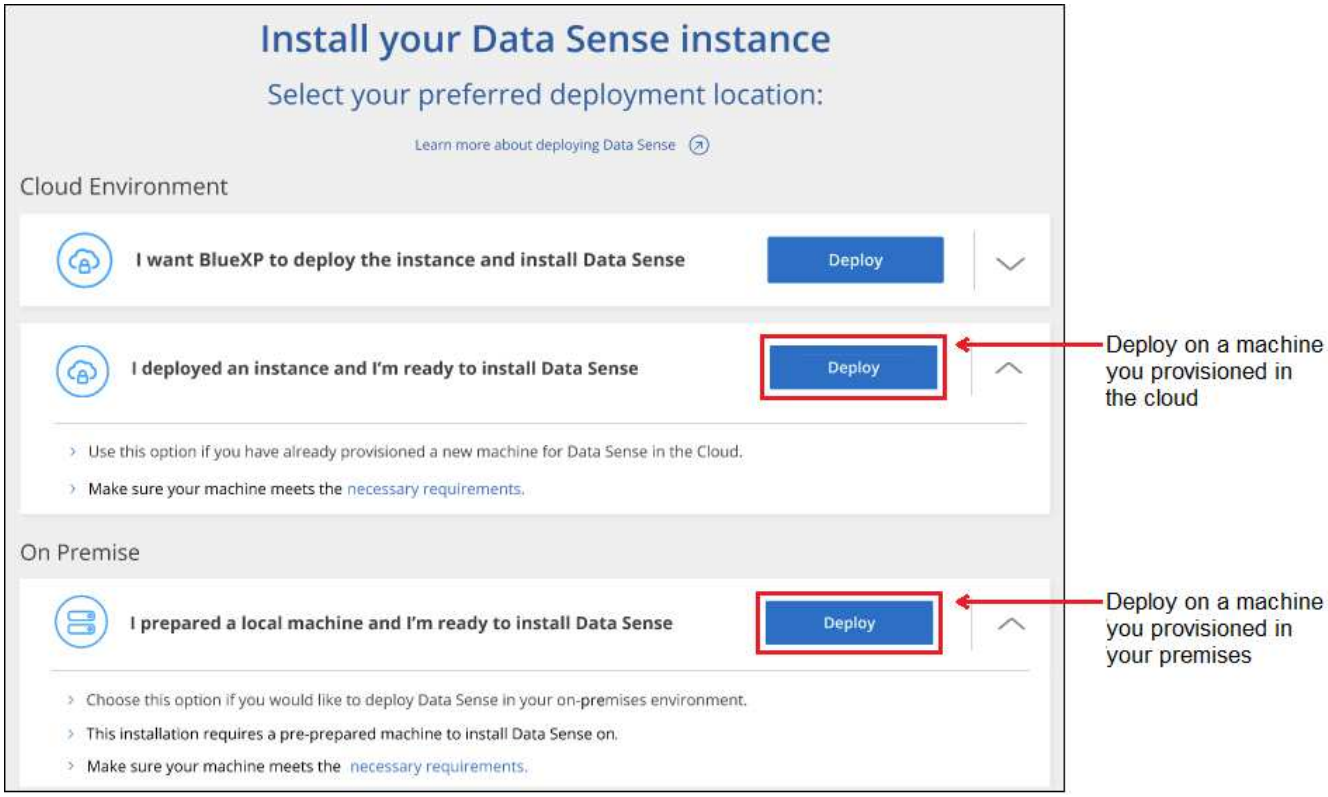
1. Téléchargez le logiciel de classification BlueXP depuis le "Site de support NetApp". Le fichier que vous devez sélectionner est nommé **DATASESNSE-INSTALLER-<version>.tar.gz**.
2. Copiez le fichier d'installation sur l'hôte Linux que vous envisagez d'utiliser (à l'aide de `scp` ou une autre méthode).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



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



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

   Notez que le programme d'installation effectue une pré-vérification afin de s'assurer que vos exigences système et réseau sont en place pour une installation réussie. "Regardez cette vidéo" pour comprendre les messages de pré-vérification et les implications.

Entrez les paramètres comme demandé :	Saisissez la commande complète :
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 est parfait pour vos sites sécurisés.

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

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

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

> 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.

1 Installez le connecteur BlueXP

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

2 Examinez les conditions préalables à la classification BlueXP

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

3 Téléchargez et déployez la classification BlueXP

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

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 To SSD sur /, ou - 100 Gio disponible sur /opt - 895 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp

Taille du système	CPU	RAM (la mémoire d'échange doit être désactivée)	Disque
Grand	16 processeurs	64 GO DE RAM	500 Gio de SSD sur /, ou - 100 Gio disponible sur /opt - 395 Gio disponible sur /var/lib/docker ou pour Podman /var/lib/containers ou pour Podman /var/lib/containers - 5 Gio sur /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 version 8.8, 9.0, 9.1, 9.2, 9.3, 9.4
- **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.

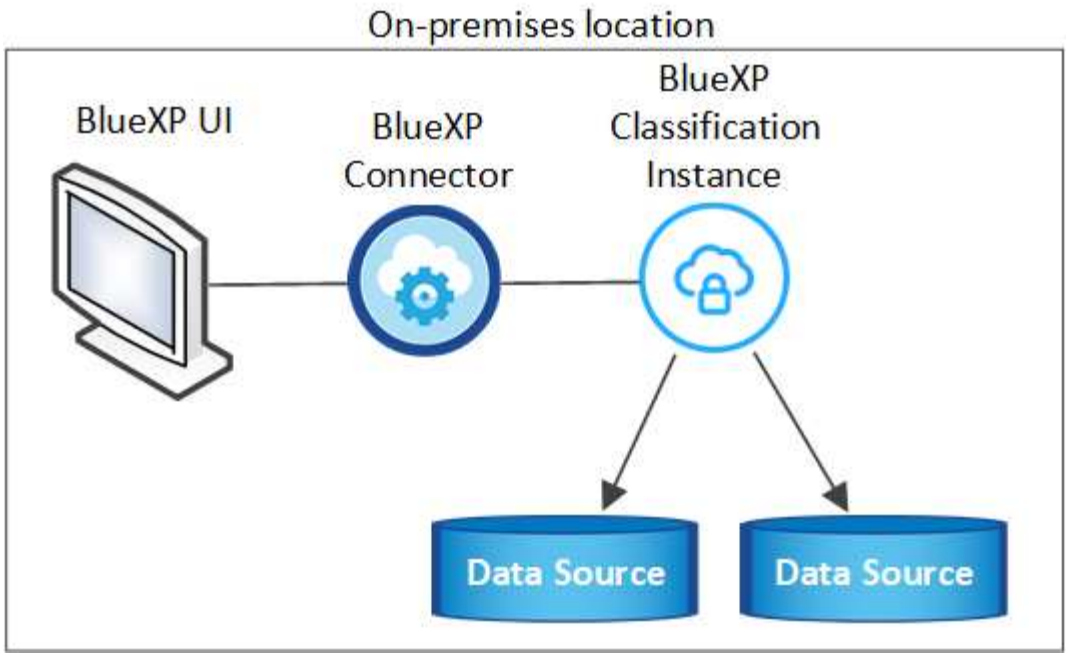
Type de connexion	Ports	Description
Classification de Connector <> BlueXP	8080 (TCP), 6000 (TCP), 443 (TCP) ET 80. 9000	Le groupe de sécurité du connecteur doit autoriser le trafic entrant et sortant sur les ports 6000 et 443 vers et depuis l'instance de classification BlueXP. • Le port 6000 est requis 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.

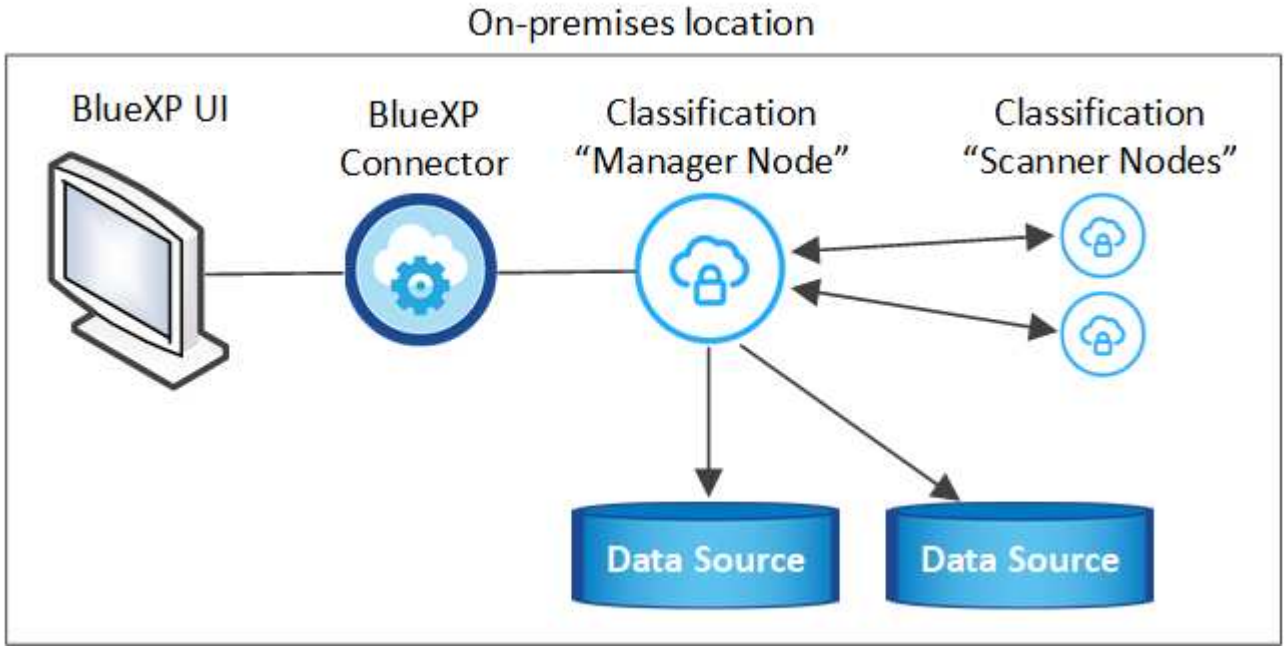
Type de connexion	Ports	Description
Classification BlueXP <> cluster ONTAP	• Pour NFS - 111 (TCP/UDP) et 2049 (TCP/UDP) • Pour CIFS - 139 (TCP/UDP) et 445 (TCP/UDP)	La classification BlueXP nécessite une connexion réseau à chaque sous-réseau Cloud Volumes ONTAP ou système ONTAP sur site. Les groupes 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.

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

Installez la classification BlueXP sur l'hôte Linux sur site

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





Installation à un seul hôte pour les configurations courantes

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

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

Ce dont vous avez besoin

- Vérifiez que votre système Linux est conforme à la configuration requise pour l'hôte.
- Vérifiez que vous avez installé les deux packages logiciels prérequis (Docker Engine ou Podman et Python 3).

- Assurez-vous que vous disposez des privilèges root sur le système Linux.
- Vérifiez que votre environnement hors ligne répond aux besoins autorisations et connectivité.

Étapes

1. Sur un système configuré en ligne, téléchargez le logiciel de classification BlueXP depuis le "Site de support NetApp". Le fichier que vous devez sélectionner est nommé **DataSense-Offline-bundle-<version>.tar.gz**.
2. Copiez l'ensemble d'installation sur l'hôte Linux que vous prévoyez d'utiliser en mode privé.
3. Décompressez le programme d'installation sur la machine hôte, par exemple :

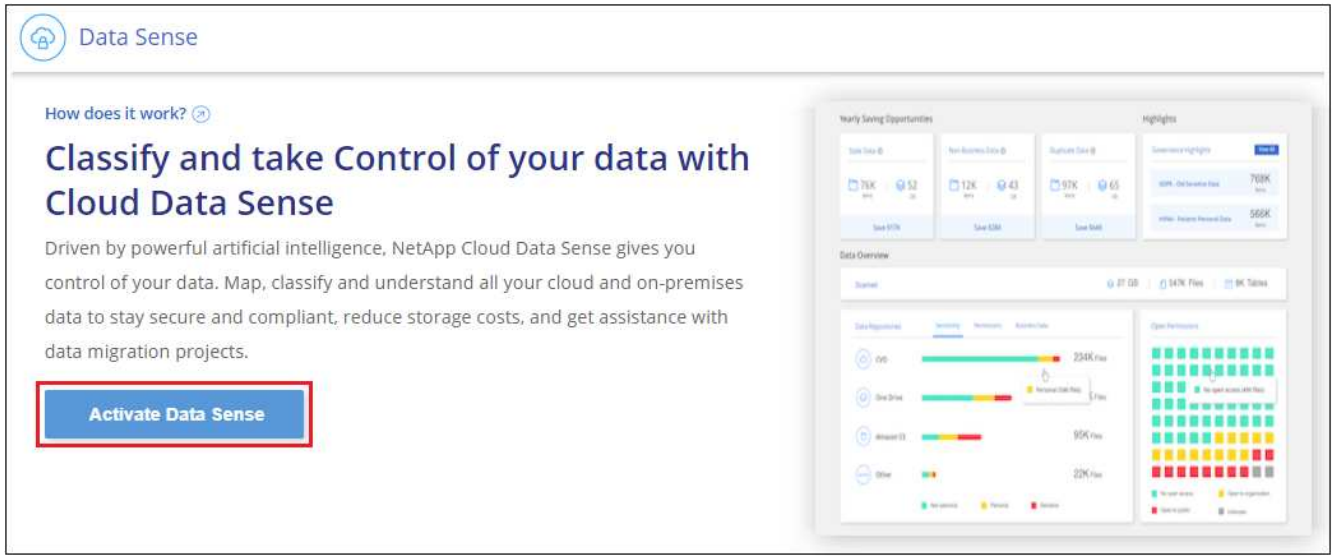
```
tar -xzf DataSense-offline-bundle-v1.25.0.tar.gz
```

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

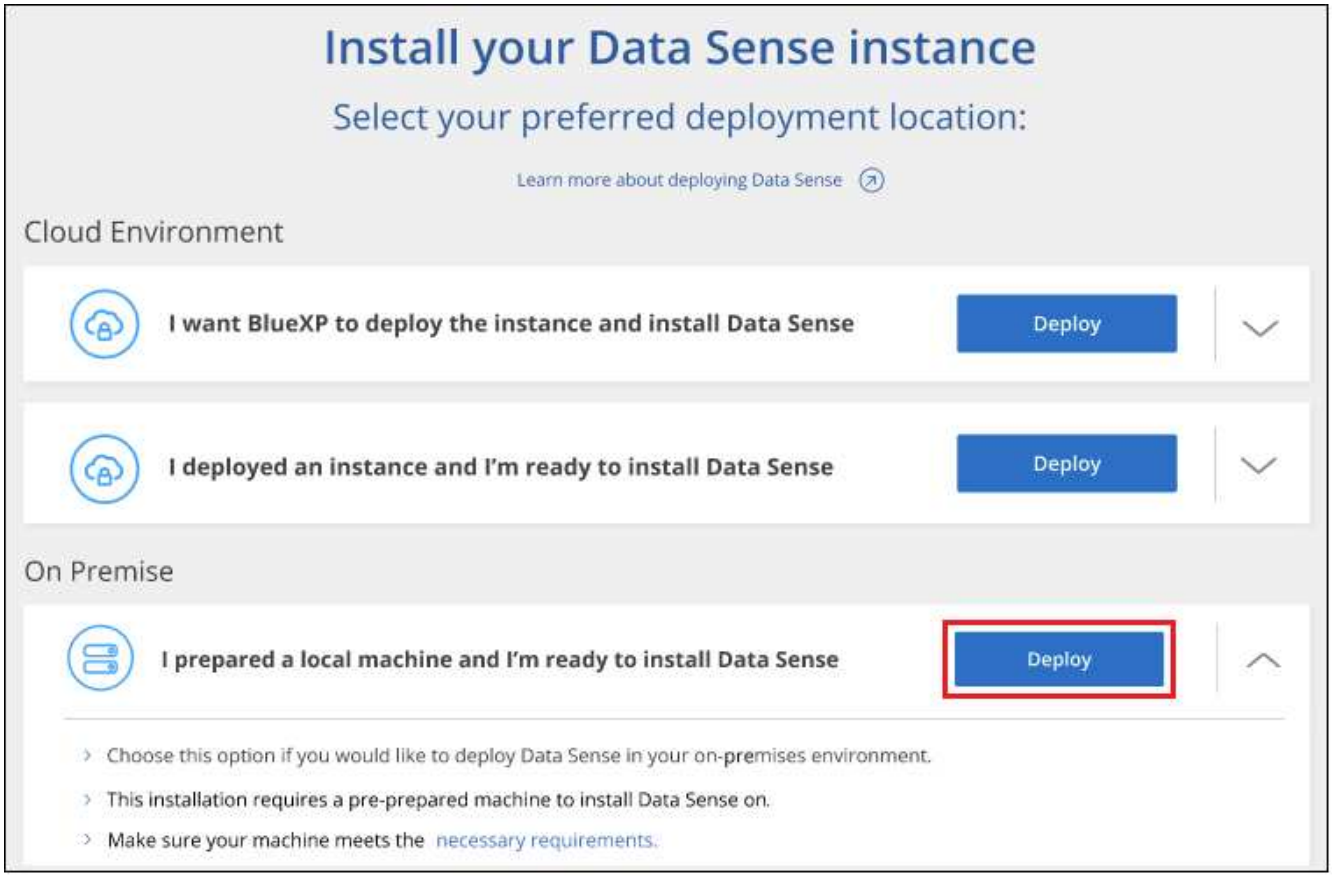
4. Décompressez le fichier d'installation sur la machine hôte, par exemple :

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

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



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



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

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

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

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

Mise en route

Vous effectuerez les tâches suivantes.

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

Créer un connecteur

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

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

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

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

Vérifiez les besoins de l'hôte

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

- La classification BlueXP n'est pas prise en charge sur un hôte partagé avec d'autres applications : l'hôte doit être un hôte dédié.
- Lors de la création du système hôte sur site, vous pouvez choisir 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 To SSD sur /, ou - 100 Gio disponible sur /opt - 895 Gio disponible sur /var/lib/docker - 5 Gio sur /tmp
Grand	16 processeurs	64 GO DE RAM	500 Gio de SSD sur /, ou - 100 Gio disponible sur /opt - 395 Gio disponible sur /var/lib/docker ou pour Podman /var/lib/containers ou pour Podman /var/lib/containers - 5 Gio sur /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 version 8.8, 9.0, 9.1, 9.2, 9.3, 9.4
- **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.

Ce dont vous avez besoin

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

Étapes

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

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

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

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

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

5. Le script vous demande l'adresse IP de la machine hôte de classification BlueXP.
   - Entrez l'adresse IP ou le nom d'hôte.

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

Résultat

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

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

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

Activez la numérisation sur vos sources de données

Analysez les volumes Azure NetApp Files avec la classification BlueXP

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

Démarrage rapide

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

1 Découvrez les systèmes Azure NetApp Files que vous souhaitez analyser

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

2 Déployez l'instance de classification BlueXP

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

3 Activez la classification BlueXP et sélectionnez les volumes à analyser

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

4 Vérifiez l'accès aux volumes

Une fois la classification BlueXP activée, assurez-vous qu'elle peut accéder à tous les volumes.

- L'instance de classification BlueXP nécessite une connexion réseau à chaque sous-réseau Azure NetApp Files.
- 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.
- Les règles d'exportation des volumes NFS doivent autoriser l'accès à partir de l'instance de classification BlueXP.
- La classification BlueXP requiert des informations d'identification Active Directory pour analyser les volumes CIFS.

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

5 Gérer les volumes à analyser

Sélectionnez ou désélectionnez les volumes à analyser ; la classification BlueXP démarre ou arrête leur analyse.

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.

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 sur vos volumes Azure NetApp Files.

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

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

     Voir Activer et désactiver les analyses de conformité sur les volumes pour plus de détails.
3. 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.

- 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.

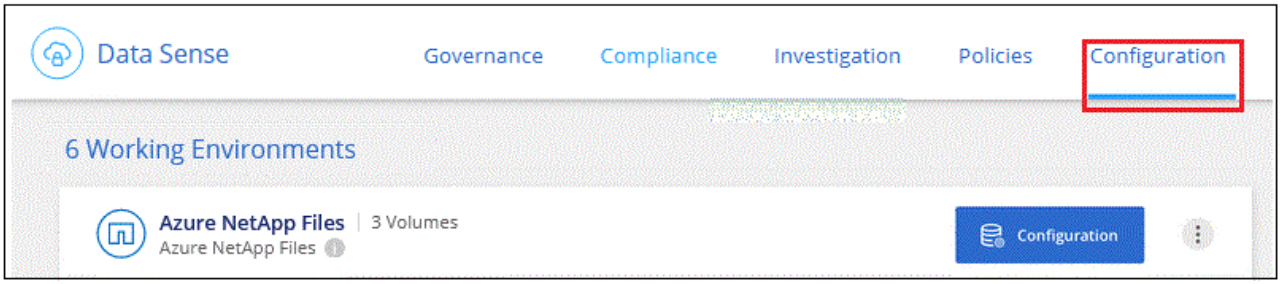
Étapes

1. Assurez-vous qu'il existe une connexion réseau entre l'instance de classification BlueXP et chaque réseau incluant des volumes pour Azure NetApp Files.

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

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, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.

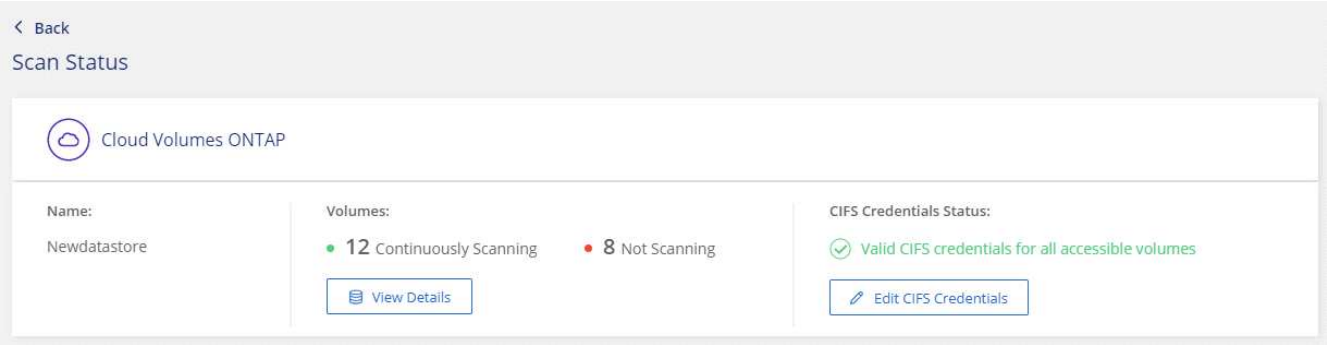


   b. Pour chaque environnement de travail, cliquez sur **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe dont la classification BlueXP a besoin pour accéder aux volumes CIFS du système.

      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.

      Si vous souhaitez vous assurer que les « dernières heures d'accès » de vos fichiers restent inchangées par les analyses de classification BlueXP, nous recommandons à l'utilisateur de disposer des autorisations d'écriture d'attributs dans CIFS ou d'autorisations d'écriture dans NFS. Si possible, nous vous recommandons de faire en sorte que l'utilisateur configuré Active Directory fasse partie d'un groupe parent de l'organisation qui dispose des autorisations pour tous les fichiers.

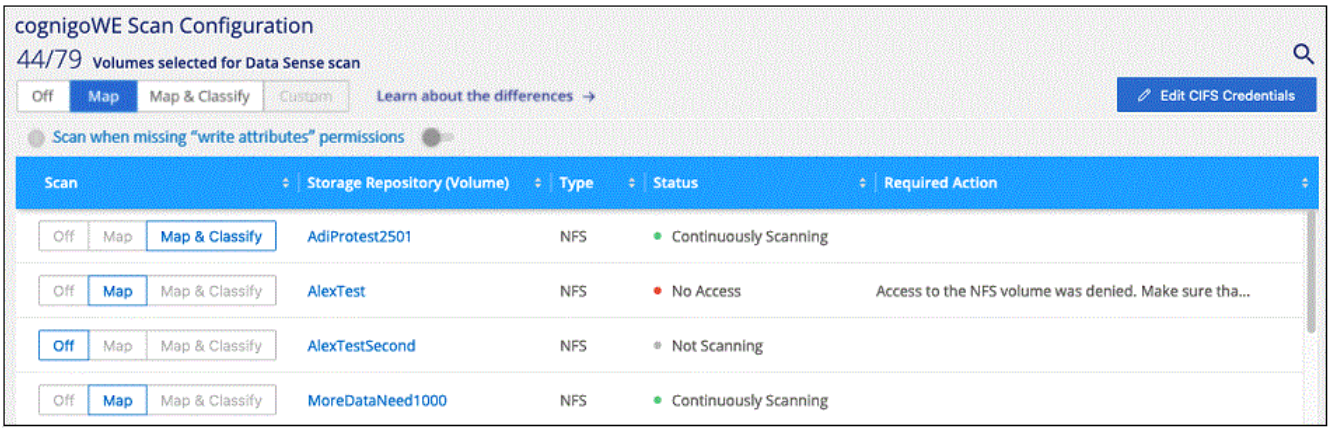
      Une fois les informations d'identification saisies, un message indiquant que tous les volumes CIFS ont été authentifiés avec succès s'affiche.



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

corriger les erreurs éventuelles.

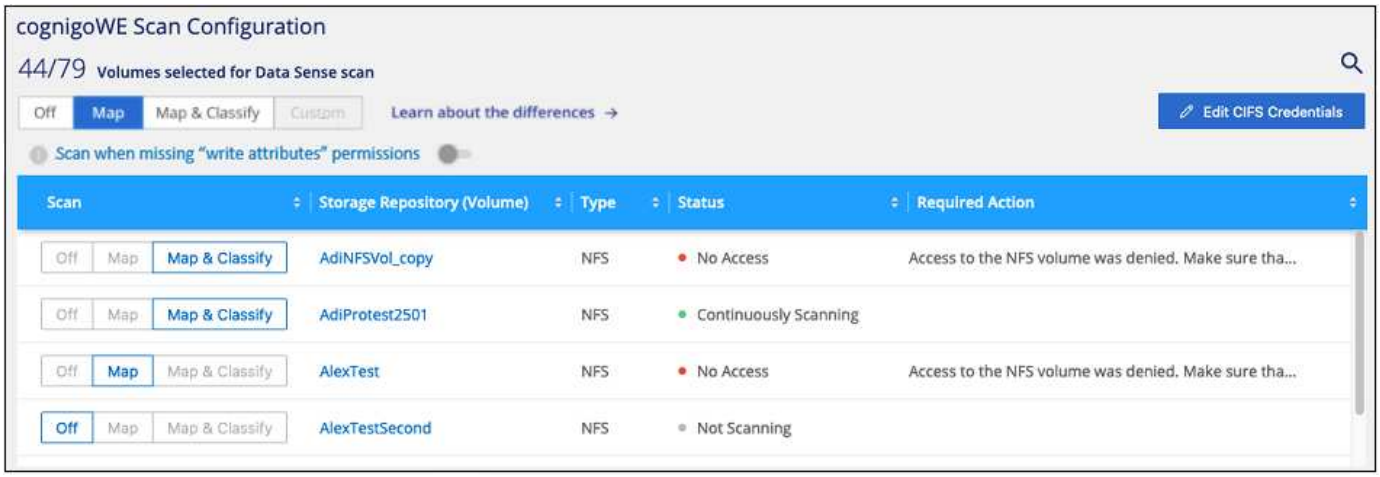
Par exemple, l'image suivante montre quatre volumes, dont l'un ne peut pas être scanné dans la classification BlueXP en raison de problèmes de connectivité réseau entre l'instance de classification BlueXP et le volume.



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.

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 >>".



À :	Procédez comme suit :
Activez les acquisitions avec mappage uniquement sur un volume	Dans la zone du volume, cliquez sur **Map**

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

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 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)"

Démarrage rapide

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

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

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

2 Déployez l'instance de classification BlueXP

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

3 **Activez la classification BlueXP et sélectionnez les volumes à analyser**

Sélectionnez l'onglet **Configuration** et activez les analyses de conformité pour les volumes dans des environnements de travail spécifiques.

4 **Vérifiez l'accès aux volumes**

Une fois la classification BlueXP activée, assurez-vous qu'elle peut accéder à tous les volumes.

- L'instance de classification BlueXP nécessite une connexion réseau à chaque sous-réseau FSX pour ONTAP.
- 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.
- Les règles d'exportation des volumes NFS doivent autoriser l'accès à partir de l'instance de classification BlueXP.
- La classification BlueXP requiert des informations d'identification Active Directory pour analyser les volumes CIFS. + cliquez sur **conformité** > **Configuration** > **Modifier les informations d'identification CIFS** et fournissez les informations d'identification.

5 **Gérer les volumes à analyser**

Sélectionnez ou désélectionnez les volumes à analyser ; la classification BlueXP démarre ou arrête leur analyse.

Identifiez le système de fichiers FSX pour ONTAP que vous souhaitez analyser

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

"Découvrez comment découvrir ou créer le système de fichiers FSX pour ONTAP dans BlueXP".

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.

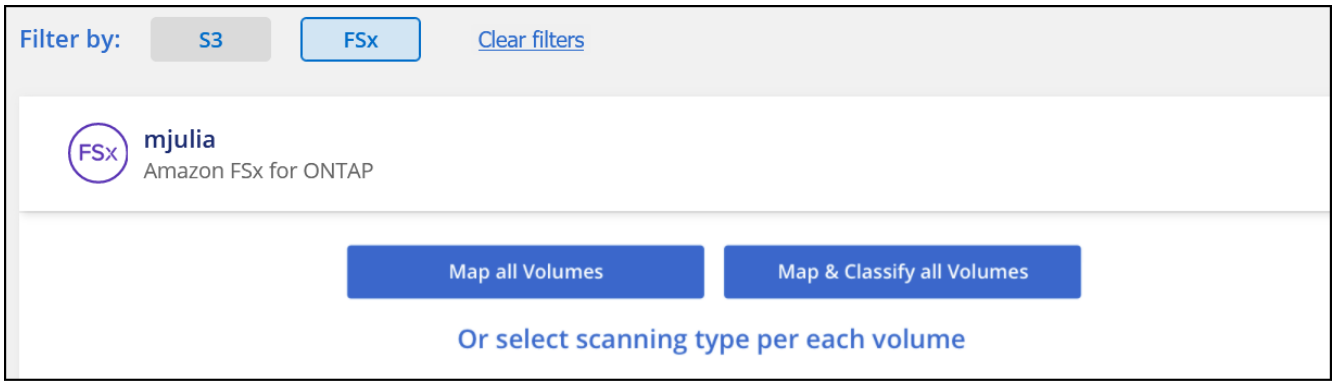
Remarque : le déploiement de la classification BlueXP dans un emplacement sur site n'est actuellement pas pris en charge lors de l'analyse des volumes FSX.

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, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.



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

     Voir Activation et désactivation des analyses de conformité sur les volumes pour plus de détails.

3. 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.

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

   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.

Scan	Storage Repository (Volume)	Type	Status	Required Action
Off Map Map & Classify	jrmclone	NFS	No Access	Check network connectivity between the Data Sense ...

2. 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.

3. 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.
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 de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.

   b. Pour chaque environnement de travail, cliquez sur **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe dont 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.

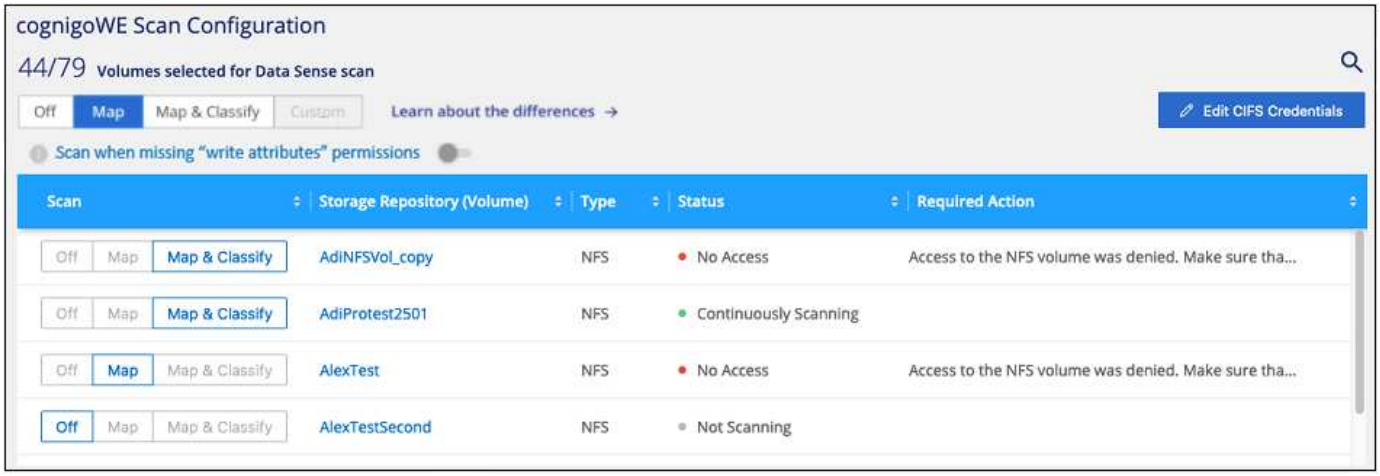
      Si vous souhaitez vous assurer que les « dernières heures d'accès » de vos fichiers restent inchangées par les analyses de classification BlueXP, nous recommandons à l'utilisateur de disposer des autorisations d'écriture d'attributs dans CIFS ou d'autorisations d'écriture dans NFS. Si possible, nous vous recommandons de faire en sorte que l'utilisateur configuré Active Directory fasse partie d'un groupe parent de l'organisation qui dispose des autorisations pour tous les fichiers.

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

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 >>".



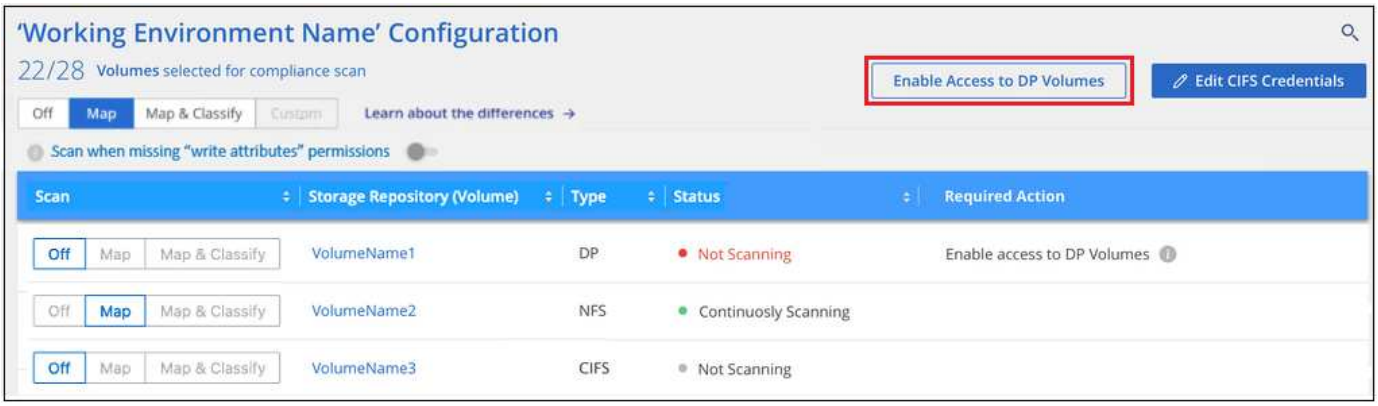
À :	Procédez comme suit :
Activez les acquisitions avec mappage uniquement sur un volume	Dans la zone du volume, cliquez sur **Map**
Activer la numérisation complète sur un volume	Dans la zone de volume, cliquez sur **carte et classement**
Désactiver la numérisation sur un volume	Dans la zone du volume,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

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.

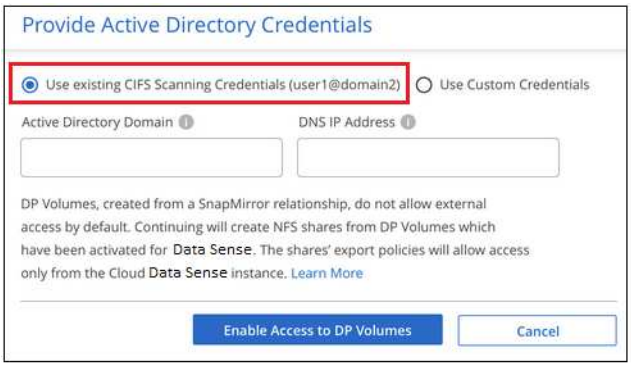
Initialement, la liste de volumes identifie ces volumes comme *Type* **DP** avec *Status* **Not Scanning** et la *Requited action* **Enable Access to DP volumes**.

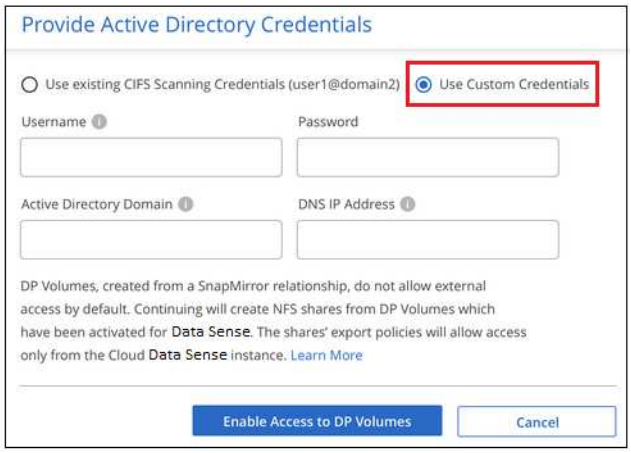


Étapes

Pour analyser ces volumes de protection des données :

1. Cliquez sur **Activer l'accès aux volumes DP** en haut de la page.
2. Vérifiez le message de confirmation et cliquez à nouveau sur **Activer l'accès aux volumes DP**.
   - Les volumes initialement créés en tant que volumes NFS dans le système de fichiers FSX source pour ONTAP sont activés.
   - Les volumes initialement créés en tant que volumes CIFS dans le système de fichiers FSX source pour ONTAP nécessitent que vous saisiez des informations d'identification CIFS pour scanner ces volumes DP. Si vous avez déjà saisi 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.





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

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.

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

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

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.

Démarrage rapide

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

1 Découvrez les sources de données que vous souhaitez analyser

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

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

2 Déployez l'instance de classification BlueXP

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

3 Activez la classification BlueXP et sélectionnez les volumes à analyser

Sélectionnez l'onglet **Configuration** et activez les analyses de conformité pour les volumes dans des environnements de travail spécifiques.

4 Vérifiez l'accès aux volumes

Une fois la classification BlueXP activée, assurez-vous qu'elle peut accéder à tous les volumes.

- L'instance de 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 - ports 111 et 2049.
  - Pour CIFS : ports 139 et 445.
- Les règles d'exportation des volumes NFS doivent autoriser l'accès à partir de l'instance de classification BlueXP.
- La classification BlueXP requiert des informations d'identification Active Directory pour analyser les volumes CIFS.

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

5 **Gérer les volumes à analyser**

Sélectionnez ou désélectionnez les volumes à analyser ; la classification BlueXP démarre ou arrête leur analyse.

Découvrez les sources de données que vous souhaitez analyser

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

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

Déployez l'instance de classification BlueXP

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

Si vous numérisez des systèmes Cloud Volumes ONTAP et ONTAP sur site accessibles via Internet, vous pouvez "Déployez la classification BlueXP dans le cloud" ou "dans un emplacement sur site avec accès à internet".

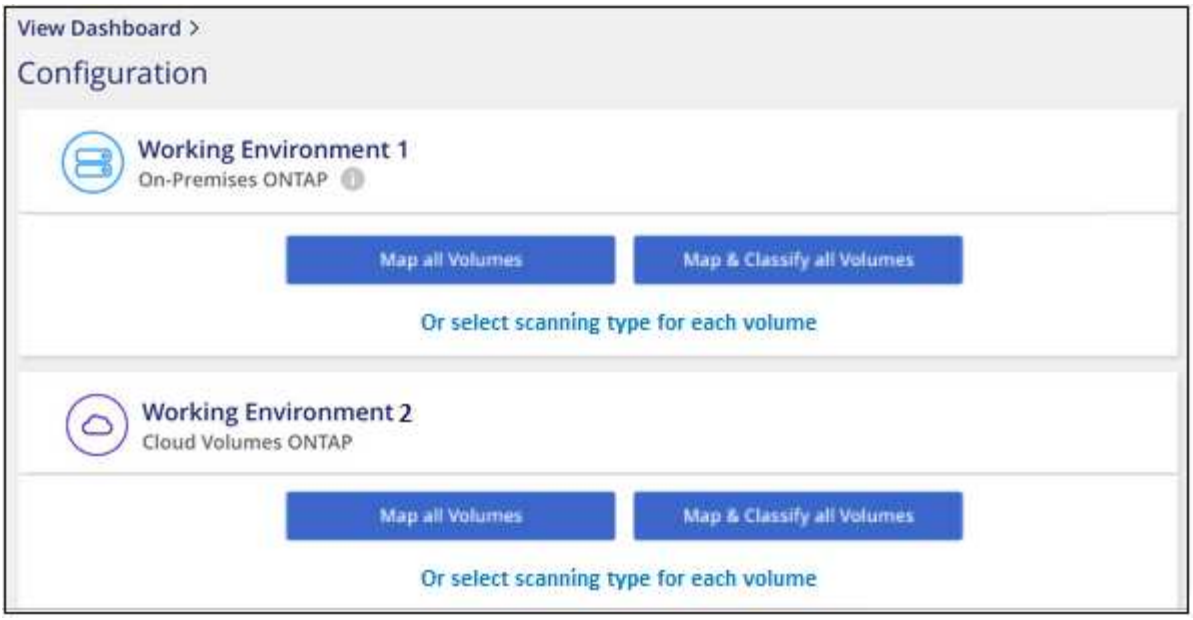
Si vous numérisez des systèmes ONTAP sur site qui ont été installés sur un site sombre et ne disposant pas d'accès à Internet, vous devez le faire "Déployez la classification BlueXP sur le même emplacement sur site qui n'a pas d'accès Internet". Cela nécessite également que le connecteur BlueXP soit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

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 sur les systèmes Cloud Volumes ONTAP de n'importe quel fournisseur cloud pris en charge et sur les clusters ONTAP sur site.

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



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

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

3. 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.

- 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.

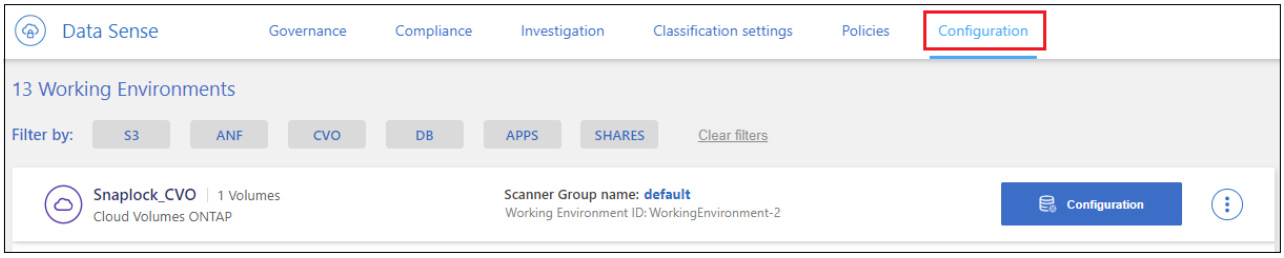
Étapes

1. 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 ports suivants sont ouverts pour l'instance de classification BlueXP :
   - Pour NFS - ports 111 et 2049.
   - Pour CIFS : ports 139 et 445.
4. 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.
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 de navigation de gauche BlueXP, cliquez sur **gouvernance > Classification**, puis sélectionnez l'onglet **Configuration**.

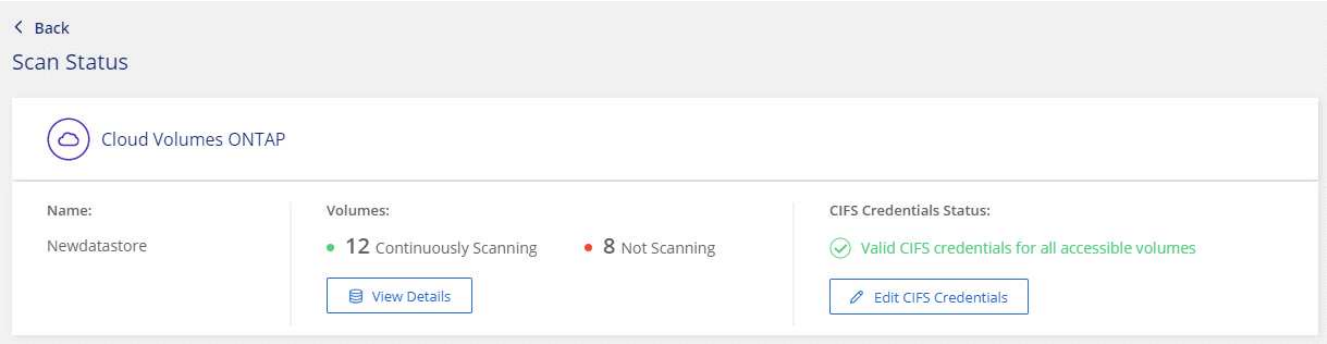
   

   b. Pour chaque environnement de travail, cliquez sur **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe dont la classification BlueXP a besoin pour accéder aux volumes CIFS du système.

   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.

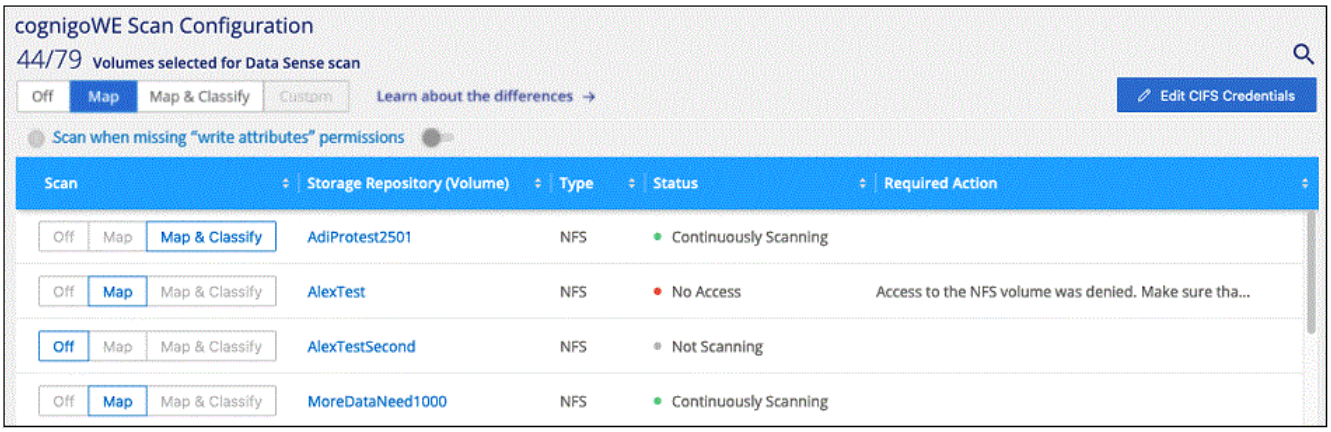
   Si vous souhaitez vous assurer que les « dernières heures d'accès » de vos fichiers restent inchangées par les analyses de classification BlueXP, nous recommandons à l'utilisateur de disposer des autorisations d'écriture d'attributs dans CIFS ou d'autorisations d'écriture dans NFS. Si possible, nous vous recommandons de faire en sorte que l'utilisateur configuré Active Directory fasse partie d'un groupe parent de l'organisation qui dispose des autorisations pour tous les fichiers.

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



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

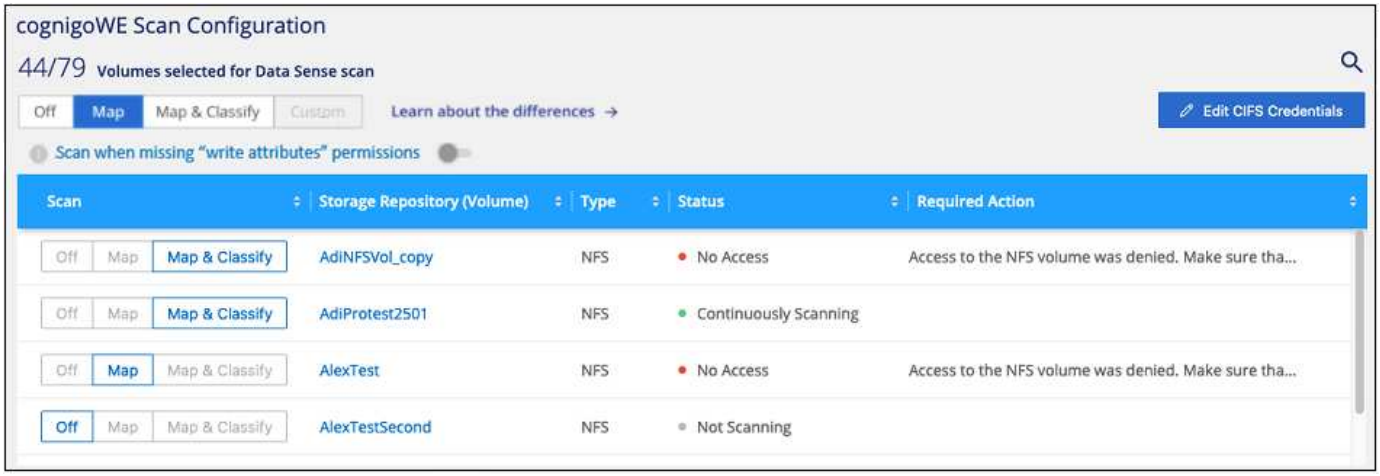
   Par exemple, l'image suivante montre quatre volumes, dont l'un ne peut pas être scanné dans la classification BlueXP en raison de problèmes de connectivité réseau entre l'instance de classification BlueXP et le volume.



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.

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 >>".



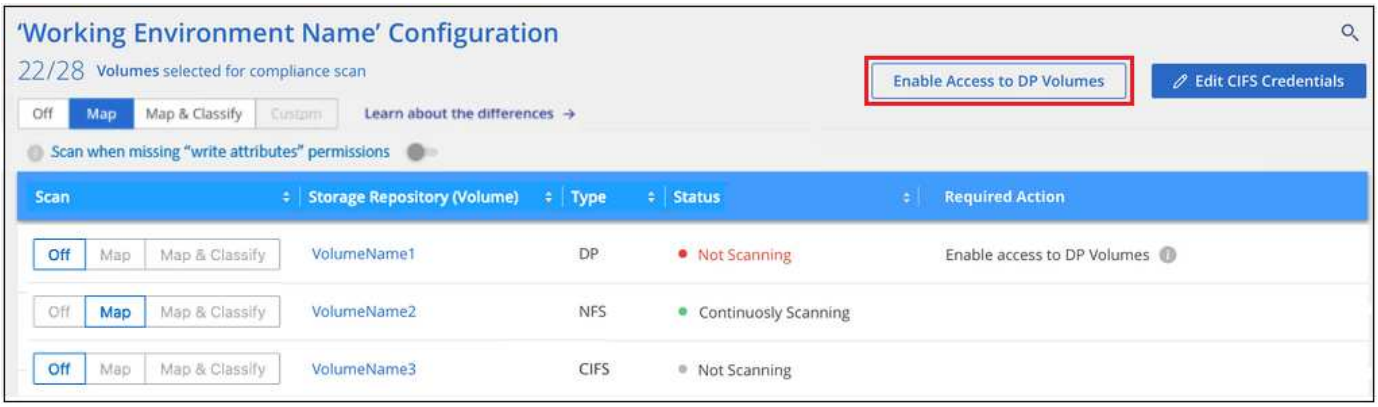
À :	Procédez comme suit :
Activez les acquisitions avec mappage uniquement sur un volume	Dans la zone du volume, cliquez sur **Map**
Activer la numérisation complète sur un volume	Dans la zone de volume, cliquez sur **carte et classement**
Désactiver la numérisation sur un volume	Dans la zone du volume,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

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 des opérations SnapMirror depuis un système ONTAP sur site ou à partir d'un système Cloud Volumes ONTAP.

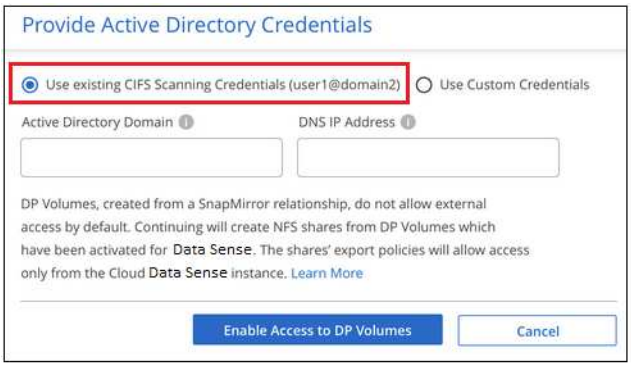
Initialement, la liste de volumes identifie ces volumes comme *Type* **DP** avec *Status* **Not Scanning** et la *Requited action* **Enable Access to DP volumes**.

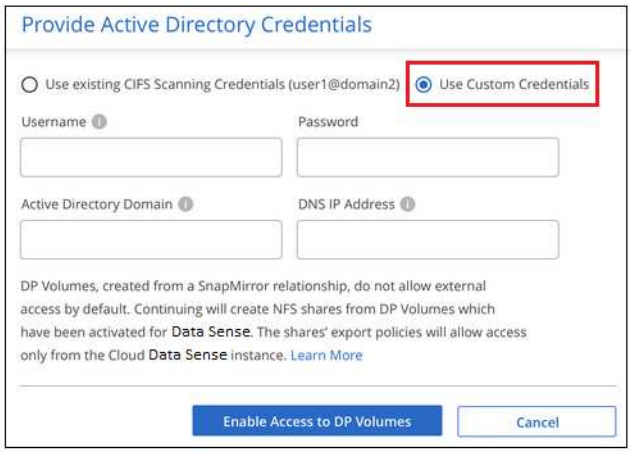


Étapes

Pour analyser ces volumes de protection des données :

1. Cliquez sur **Activer l'accès aux volumes DP** en haut de la page.
2. Vérifiez le message de confirmation et cliquez à nouveau sur **Activer l'accès aux volumes DP**.
   - Les volumes initialement créés en tant que volumes NFS dans le système ONTAP source sont activés.
   - Pour les volumes initialement créés en tant que volumes CIFS dans le système ONTAP source, vous devez entrer des identifiants CIFS pour scanner ces volumes DP. Si vous avez déjà saisi 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.





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

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.

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

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

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.

Démarrage rapide

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

1. **Vérifiez les prérequis de la base de données**

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

2. **Déployez l'instance de classification BlueXP**

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

3. **Ajoutez le serveur de base de données**

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

4. **Sélectionnez les schémas**

Sélectionnez les schémas à numériser.

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".

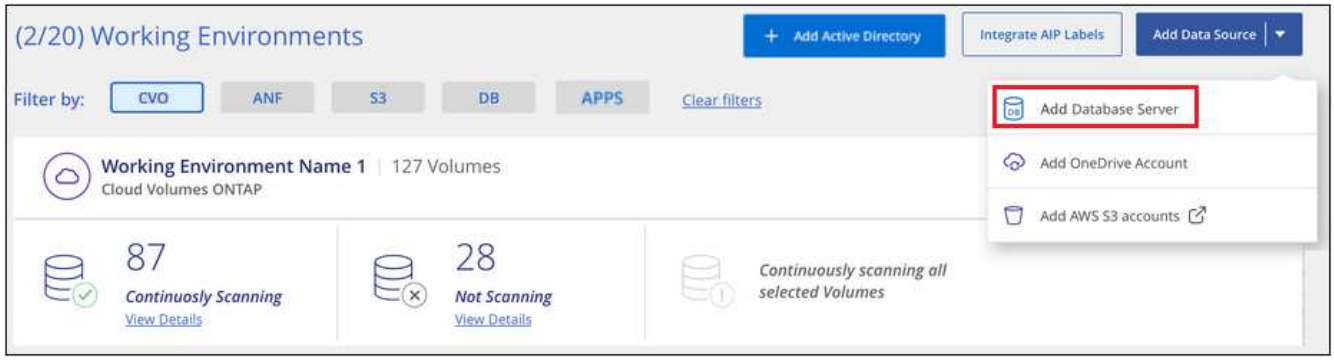
Si vous numérisez des schémas de base de données qui ont été installés sur un site sombre sans accès à Internet, vous devez le faire "Déployez la classification BlueXP sur le même emplacement sur site qui n'a pas d'accès Internet". Cela nécessite également que le connecteur BlueXP soit déployé dans le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

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

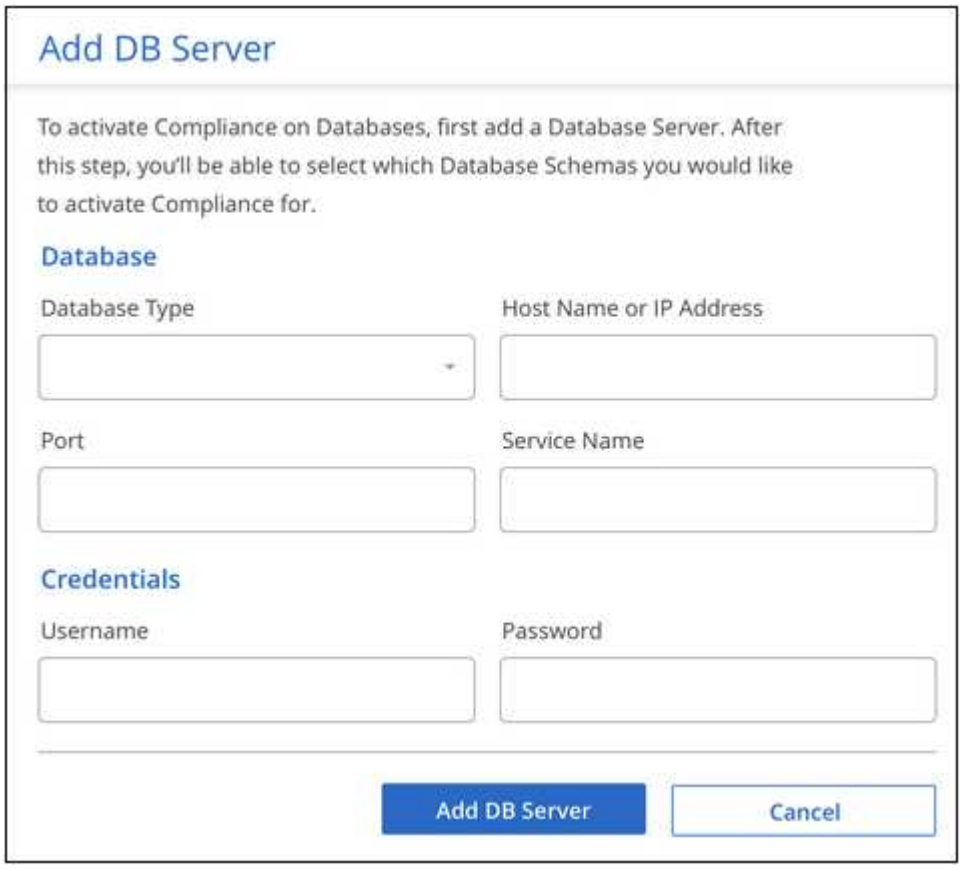
Ajoutez le serveur de base de données

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

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



2. Entrez les informations requises pour identifier le serveur de base de données.
   a. Sélectionnez le type de base de données.
   b. Entrez le port et le nom d'hôte ou l'adresse IP pour vous connecter à la base de données.
   c. Pour les bases de données Oracle, entrez le nom du service.
   d. Entrez les identifiants 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.

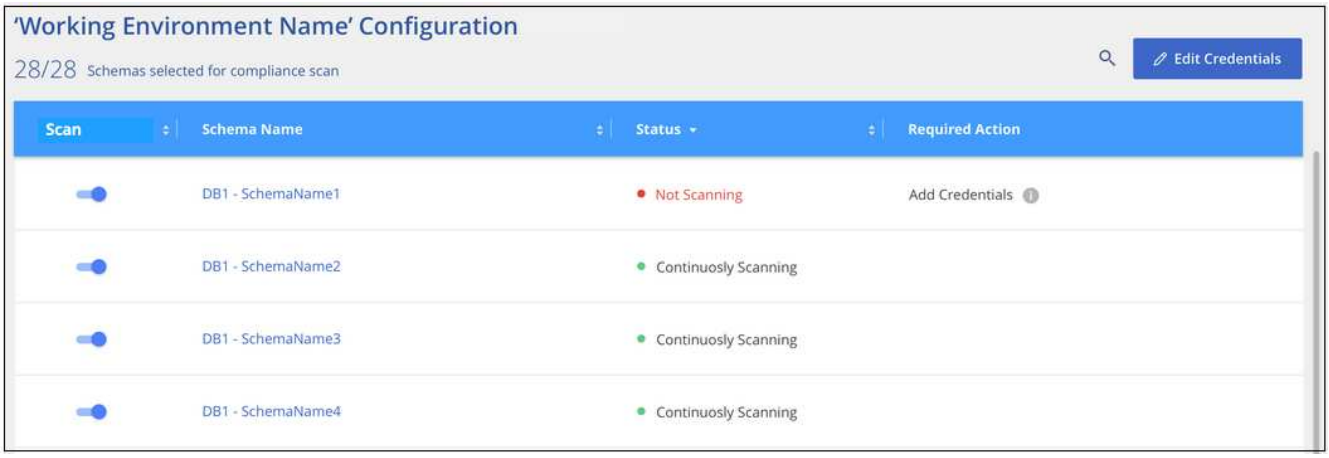
Activer et désactiver les analyses de conformité sur les schémas de base de données

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

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



Résultat

La classification BlueXP commence à analyser les schémas de base de données que vous avez activés. En cas d'erreur, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

Notez que 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

Procédez en quelques étapes pour commencer l'analyse des partages de fichiers NFS ou CIFS à partir de Google Cloud NetApp volumes et d'anciens systèmes NetApp 7-mode. Ces partages de fichiers peuvent résider 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.

Démarrage rapide

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

Vérifiez les conditions préalables au partage de fichiers

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

Déployez l'instance de classification BlueXP

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

Créez un groupe pour conserver les partages de fichiers

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

Ajoutez les partages de fichiers au groupe

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

Vérifiez les exigences en matière de partage de fichiers

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.

  Notez que la classification BlueXP ne peut pas extraire les autorisations, ni l'heure du dernier accès des systèmes 7-mode. En outre, en raison d'un problème connu entre certaines versions de Linux et certains partages CIFS sur les systèmes 7-mode, vous devez configurer le partage pour qu'il n'utilise que SMB v1 avec l'authentification NTLM activée.

- Il doit y avoir une connectivité réseau entre l'instance de classification BlueXP et les partages.
- 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.
- Vous pouvez ajouter un partage DFS (Distributed File System) en tant que partage CIFS standard. Cependant, la classification BlueXP n'ayant pas connaissance du fait que le partage repose sur plusieurs serveurs/volumes combinés en tant que partage CIFS unique, vous pouvez recevoir des erreurs d'autorisation ou de connectivité sur le partage lorsque le message ne s'applique qu'à l'un des dossiers/partages situés sur un autre serveur/volume.
- 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.

  Si vous souhaitez vous assurer que les « dernières heures d'accès » de vos fichiers restent inchangées par les analyses de classification BlueXP, nous recommandons à l'utilisateur de disposer des autorisations d'écriture d'attributs dans CIFS ou d'autorisations d'écriture dans NFS. 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.

- Vous aurez besoin de la liste des partages que vous souhaitez ajouter au format `<host_name>:/<share_path>`. Vous pouvez entrer les partages individuellement ou fournir une liste séparée par des lignes des partages de fichiers que vous souhaitez scanner.

Déployez l'instance de classification BlueXP

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

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

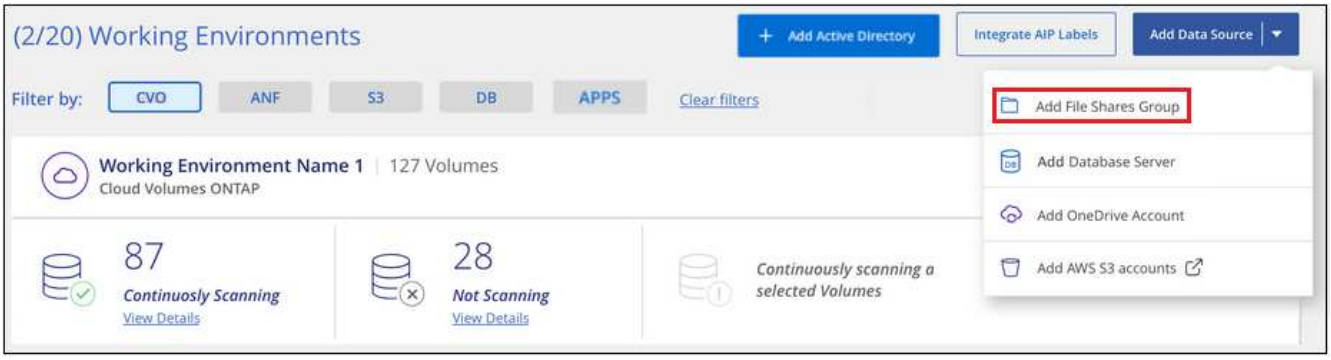
Créez le groupe pour les partages de fichiers

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

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

Étapes

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



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

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

Ajouter des partages de fichiers à un groupe

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

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

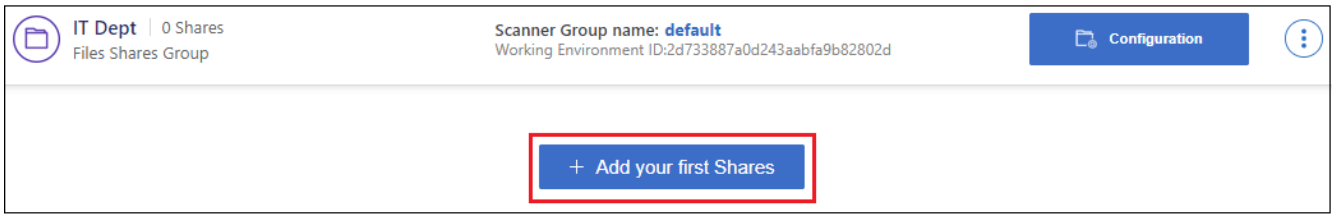
Lorsque vous ajoutez à la fois des partages NFS et CIFS au sein d'un seul groupe, vous devez recommencer le processus à deux reprises, après avoir ajouté des partages NFS, puis à nouveau en ajoutant les partages

CIFS.

Étapes

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

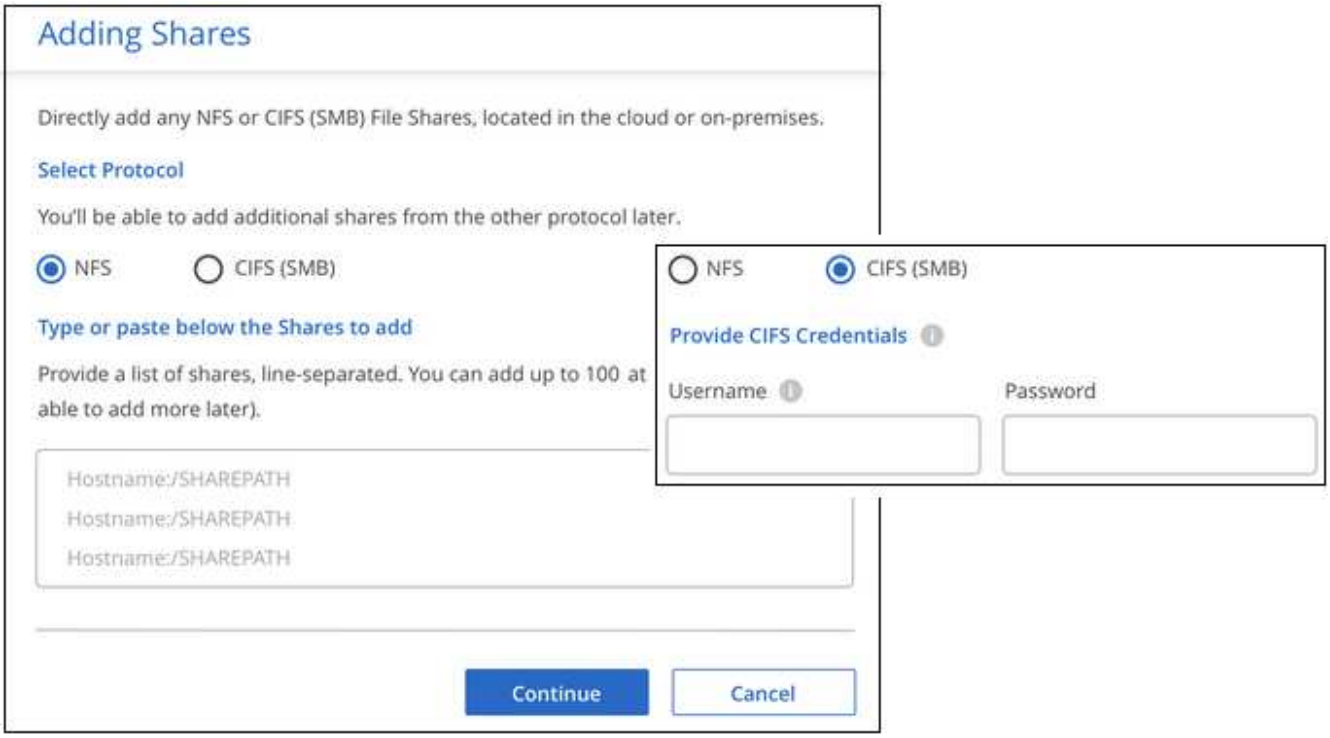
2. Si c'est la première fois que vous ajoutez des partages de fichiers pour ce groupe de partages de fichiers, cliquez sur **Ajouter vos premiers partages**.



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

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

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



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

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

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

À :	Procédez comme suit :
Activez les analyses de mappage uniquement sur les partages de fichiers	Cliquez sur **carte**
Activez les analyses complètes sur les partages de fichiers	Cliquez sur **carte et classement**
Désactiver l'analyse sur les partages de fichiers	Cliquez sur **Off**

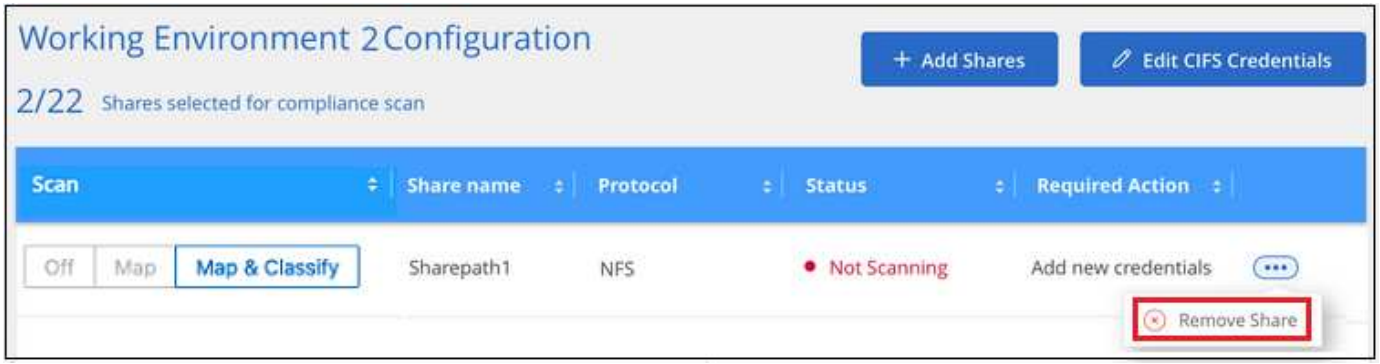
Le commutateur en haut de la page pour **Scan en cas d'autorisations d'écriture d'attributs manquantes** est désactivé par défaut. Cela signifie que si la classification BlueXP ne dispose pas d'autorisations d'attributs d'écriture dans CIFS ou d'autorisations d'écriture dans NFS, le système ne analyse 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 >>".

Résultat

La classification BlueXP commence à analyser les fichiers des partages de fichiers que vous avez ajoutés. Les résultats s'affichent dans le tableau de bord et à d'autres emplacements.

Supprimez un partage de fichiers des analyses de conformité

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



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 .

Démarrage rapide

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

1 **Consultez les conditions préalables de StorageGRID**

Vous devez disposer de l'URL du noeud final pour vous connecter au service StorageGRID.

Vous devez disposer de la clé d'accès et de la clé secrète de StorageGRID pour que la classification BlueXP puisse accéder aux compartiments.

2 **Déployez l'instance de classification BlueXP**

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

3 **Ajoutez le service StorageGRID**

Ajoutez le service StorageGRID à la classification BlueXP .

4 **Sélectionnez les compartiments à numériser**

Sélectionnez les compartiments que vous souhaitez analyser et la classification BlueXP commencera à les analyser.

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.

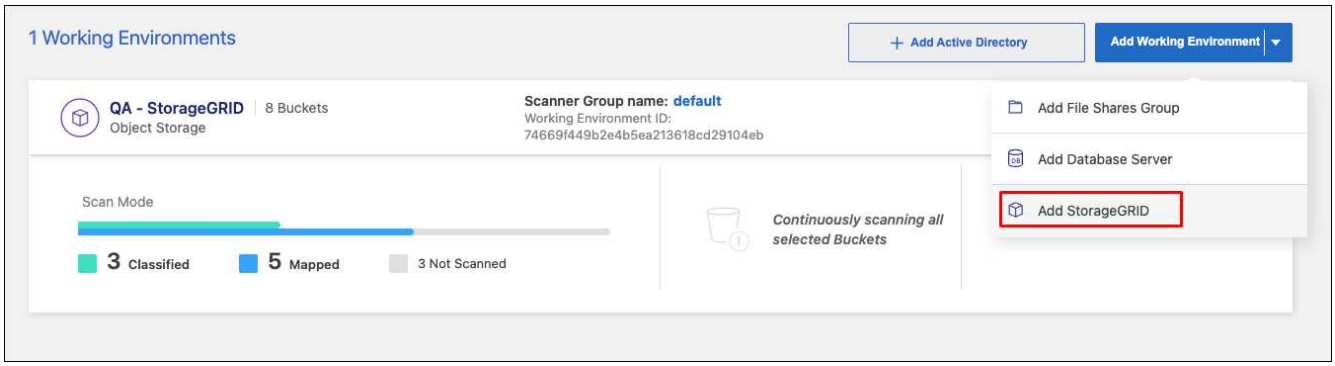
Les mises à niveau vers le logiciel de classification BlueXP sont automatisées tant que l'instance dispose d'une connectivité Internet.

Ajoutez le service StorageGRID à la classification BlueXP

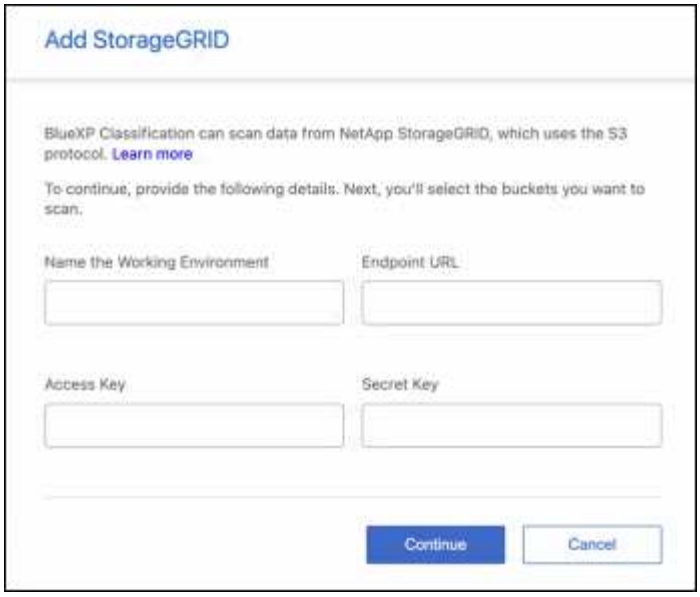
Ajoutez le service StorageGRID.

Étapes

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



2. 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

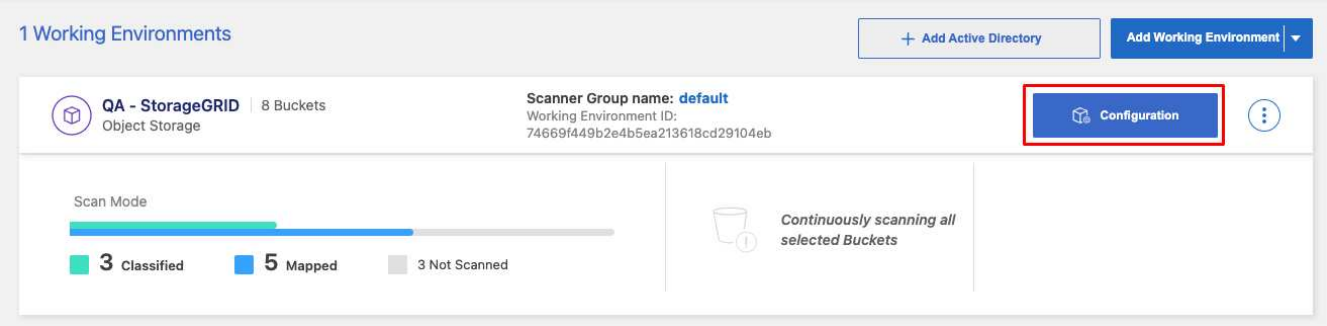
StorageGRID est ajouté à la liste des environnements de travail.

Activer et désactiver les analyses de conformité sur les compartiments StorageGRID

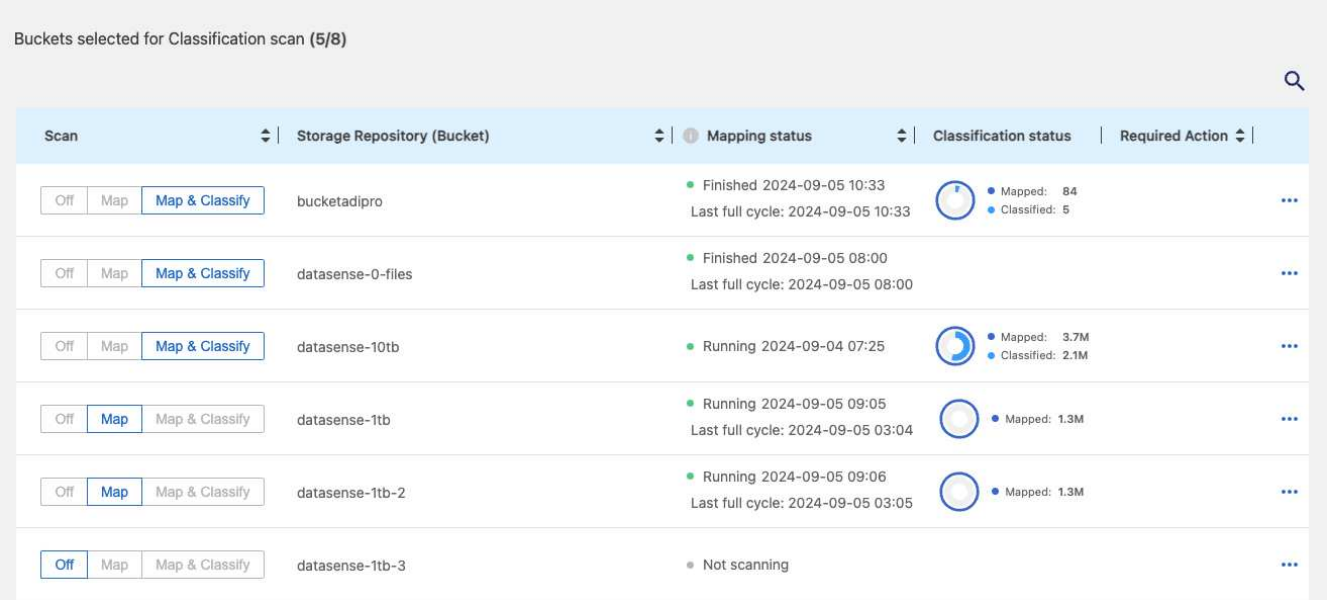
Après avoir activé la classification BlueXP sur StorageGRID, l'étape suivante consiste à configurer les compartiments que vous souhaitez analyser. La classification BlueXP détecte ces compartiments et les affiche dans l'environnement de travail que vous avez créé.

Étapes

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



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



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

Résultat

La classification BlueXP commence à analyser les compartiments que vous avez activés. En cas d'erreur, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

Intégrez 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 de fichier » "filtre" Et voir les résultats dans les métadonnées du fichier dans le volet Investigation. Au lieu du propriétaire du fichier contenant le SID (identificateur de sécurité), il est renseigné avec le nom d'utilisateur réel.
- Vous pouvez voir "autorisations complètes sur les fichiers" Pour chaque fichier et répertoire lorsque vous

cliquez sur le bouton « Afficher toutes les autorisations ».

- Dans le "Tableau de bord gouvernance", Le panneau Ouvrir les autorisations affiche un niveau de détail plus élevé sur vos données.

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

Sources de données prises en charge

Une intégration d'Active Directory avec 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)

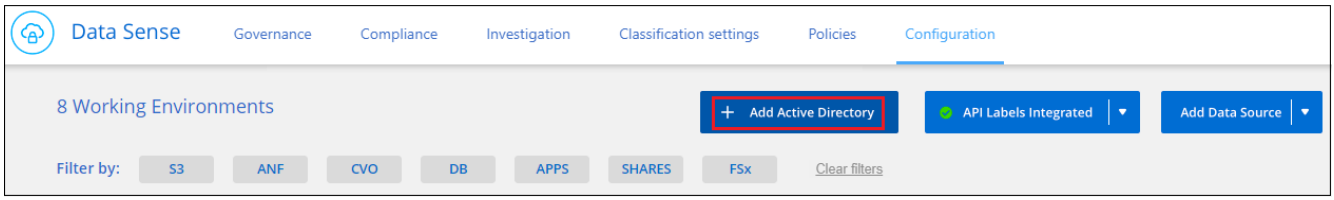
- Que vous utilisiez ou non le protocole LDAP sécurisé (LDAPS)
- Port serveur LDAP (généralement 389 pour LDAP et 636 pour LDAP sécurisé)

- 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

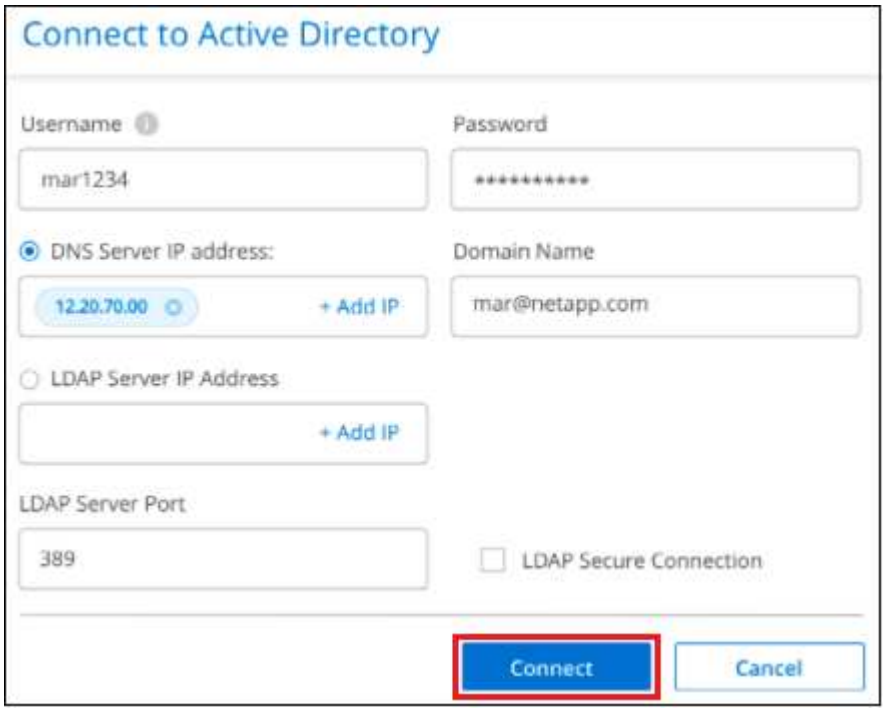
Étapes

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

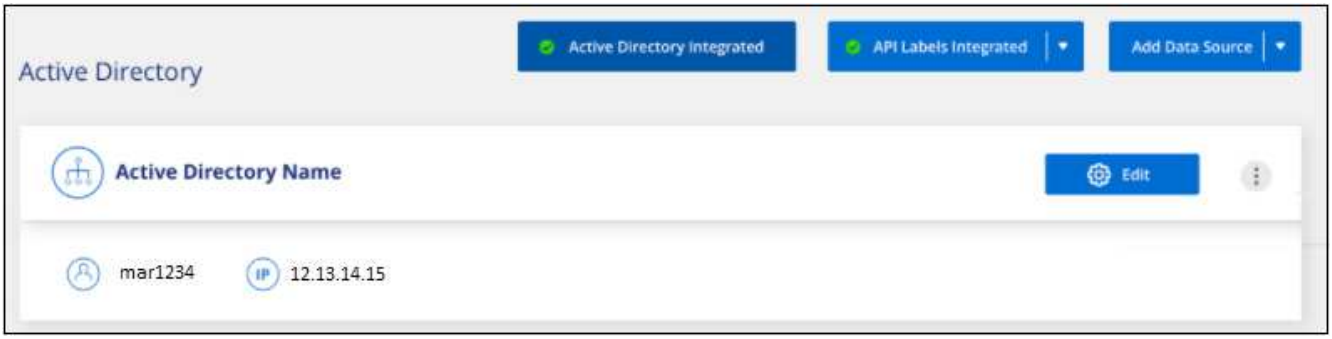


2. Dans la boîte de dialogue connexion à Active Directory, entrez les détails d'Active Directory et cliquez sur **connexion**.

   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 si vous n'en avez plus besoin en cliquant sur le bouton Puis **Supprimer Active Directory**.

Forum aux questions sur la classification BlueXP

Cette FAQ peut vous aider si vous cherchez juste une réponse rapide à une question.

Service de classification BlueXP

Les questions suivantes présentent des généralités sur la classification BlueXP.

Qu'est-ce que la classification BlueXP ?

La classification BlueXP est une offre cloud qui utilise la technologie basée sur l'intelligence artificielle (IA) pour vous aider à comprendre le contexte des données et à identifier les données sensibles dans vos systèmes de stockage. Les systèmes peuvent être des environnements de travail que vous avez ajoutés à BlueXP Canvas et de nombreux types de sources de données auxquels la classification BlueXP peut accéder via vos réseaux. "Voir la liste complète ci-dessous".

La classification BlueXP fournit des paramètres prédéfinis (tels que les types et catégories d'informations sensibles) pour répondre aux nouvelles réglementations de conformité en matière de confidentialité et de sensibilité des données, notamment le RGPD, la CCPA et l'HIPAA.

Fonctionnement de la classification BlueXP

La classification BlueXP déploie une autre couche d'intelligence artificielle en parallèle avec votre système et vos systèmes de stockage BlueXP. Il analyse ensuite les données sur des volumes, des compartiments, des bases de données, ainsi que d'autres comptes de stockage, et indexe les informations exploitables concernant les données. La classification BlueXP exploite à la fois l'intelligence artificielle et le traitement du langage naturel, contrairement aux autres solutions généralement construites autour d'expressions régulières et de la mise en correspondance de modèles.

La classification BlueXP utilise l'IA pour fournir une compréhension contextuelle des données pour une détection et une classification précises. Elle est axée sur l'IA, car elle est conçue pour répondre aux besoins de types et d'évolutivité des données modernes. Il comprend également le contexte des données afin d'assurer une découverte et une classification solides et précises.

"Découvrez le fonctionnement de la classification BlueXP".

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

Qu'en est-il de l'architecture de la classification BlueXP ?

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. Cette prise en charge permet la prise en charge d'environnements multicloud, interclouds, clouds privés et sur site.

Quels sont les fournisseurs de cloud pris en charge ?

La classification BlueXP fonctionne avec BlueXP et prend en charge AWS, Azure et GCP. Votre entreprise peut ainsi bénéficier d'une visibilité unifiée sur la confidentialité des données entre les différents fournisseurs de cloud.

La classification BlueXP utilise-t-elle une API REST et des outils tiers ?

Non, la classification BlueXP ne dispose pas d'API REST.

La classification BlueXP est-elle disponible sur les marchés ?

Oui, la classification BlueXP et BlueXP est disponible sur les marchés AWS, Azure et GCP.

Analyse de classification et analytique BlueXP

Les questions suivantes se rapportent aux performances de l'analyse de classification BlueXP et aux analyses disponibles pour les utilisateurs.

À quelle fréquence la classification BlueXP analyse-t-elle mes données ?

L'analyse initiale de vos données peut prendre un peu de temps, mais les analyses suivantes ne permettent qu'd'examiner les modifications incrémentielles, ce qui réduit les temps d'analyse du système. La classification BlueXP analyse vos données de manière continue selon une séquence périodique, six référentiels à la fois, de sorte que toutes les données modifiées soient classifiées très rapidement.

"Découvrez le fonctionnement des acquisitions".

Notez que la classification BlueXP analyse les bases de données une seule fois par jour. Les bases de données ne sont pas continuellement analysées comme d'autres sources de données.

L'analyse des données a un impact négligeable sur vos systèmes de stockage et sur vos données. Toutefois, si vous êtes préoccupé, même par un très faible impact, vous pouvez configurer la classification BlueXP pour effectuer des analyses « lentes ». "Découvrez comment réduire la vitesse de numérisation".

Puis-je effectuer des recherches dans mes données à l'aide de la classification BlueXP ?

Les fonctionnalités de recherche étendues de la classification BlueXP facilitent la recherche d'un fichier ou d'un élément de données spécifique dans l'ensemble des sources connectées. La classification BlueXP permet aux utilisateurs d'effectuer des recherches plus approfondies que les métadonnées ne reflètent. Il s'agit d'un service indépendant de la langue qui peut également lire les fichiers et analyser une multitude de types de données sensibles, tels que les noms et les ID. Par exemple, les utilisateurs peuvent effectuer des recherches dans des magasins de données structurés et non structurées pour trouver des données qui

peuvent s'être divulguées des bases de données aux fichiers des utilisateurs, en violation de la stratégie de l'entreprise. Les recherches peuvent être enregistrées ultérieurement et des règles peuvent être créées pour rechercher et prendre des mesures sur les résultats à une fréquence définie.

Une fois les fichiers qui vous intéressent trouvés, les caractéristiques peuvent être listées, y compris les balises, le compte de l'environnement de travail, le compartiment, le chemin du fichier, catégorie (à partir de la classification), taille du fichier, dernière modification, statut d'autorisation, doublons, niveau de sensibilité, données personnelles, types de données sensibles dans le fichier, propriétaire, type de fichier, taille de fichier, heure de création, hachage de fichier, si les données ont été attribuées à une personne demandant son attention, et plus encore. Les filtres peuvent être appliqués aux caractéristiques de tramage qui ne sont pas pertinentes. La classification BlueXP dispose également de contrôles RBAC pour permettre le déplacement ou la suppression de fichiers si les autorisations appropriées sont présentes. Si les autorisations appropriées ne sont pas présentes, les tâches peuvent être affectées à une personne de l'entreprise qui dispose des autorisations appropriées.

La classification BlueXP propose-t-elle des rapports ?

Oui. Les informations offertes par la classification BlueXP peuvent être pertinentes pour les autres parties prenantes de votre entreprise. Nous vous aidons à générer des rapports pour partager les informations exploitables. Les rapports suivants sont disponibles pour la classification BlueXP :

Rapport d'évaluation des risques pour la confidentialité

Fournit des informations sur la confidentialité à partir de vos données et un score de risque lié à la confidentialité. "En savoir plus >>".

Rapport de demande d'accès au sujet des données

Vous permet d'extraire un rapport de tous les fichiers contenant des informations concernant le nom spécifique ou l'identifiant personnel d'un sujet de données. "En savoir plus >>".

Rapport PCI DSS

Vous aide à identifier la distribution des informations de carte de crédit dans vos dossiers. "En savoir plus >>".

Rapport HIPAA

Vous aide à identifier la distribution de l'information sur la santé dans vos dossiers. "En savoir plus >>".

Rapport de mappage de données

Fournit des informations sur la taille et le nombre de fichiers dans vos environnements de travail. Cela inclut la capacité d'utilisation, l'âge des données, la taille des données et les types de fichiers. "En savoir plus >>".

Rapport d'évaluation de la découverte des données

Fournit une analyse de haut niveau de l'environnement analysé afin de mettre en évidence les résultats du système et de montrer les points préoccupants et les étapes de correction potentielles. "Mode apprentissage".

Rapports sur un type d'information spécifique

Des rapports sont disponibles, incluant des détails sur les fichiers identifiés qui contiennent des données personnelles et des données personnelles sensibles. Vous pouvez également voir les fichiers dérépartis par catégorie et par type de fichier. "En savoir plus >>".

Les performances d'acquisition varient-t-elles ?

Les performances de l'analyse peuvent varier en fonction de la bande passante réseau et de la taille moyenne des fichiers dans votre environnement. Elle peut également dépendre des caractéristiques de taille du système hôte (dans le cloud ou sur site). Voir "Instance de classification BlueXP" et "Classification BlueXP : déploiement" pour en savoir plus.

Lors de l'ajout initial de nouvelles sources de données, vous pouvez également choisir d'effectuer uniquement une analyse de « mappage » au lieu d'une analyse de « classification » complète. Le mappage peut être effectué très rapidement sur vos sources de données car il n'accède pas aux fichiers pour voir les données à l'intérieur. "Voir la différence entre une acquisition de cartographie et une acquisition de classification".

Gestion de la classification et confidentialité BlueXP

Les questions suivantes expliquent comment gérer les paramètres de classification et de confidentialité BlueXP.

Comment activer la classification BlueXP ?

Vous devez tout d'abord déployer une instance de classification BlueXP dans BlueXP ou dans un système sur site. Une fois l'instance en cours d'exécution, vous pouvez activer le service sur les environnements de travail, les bases de données et d'autres sources de données existants à partir de l'onglet **Configuration** ou en sélectionnant un environnement de travail spécifique.

"Découvrez comment démarrer".

> L'activation de la classification BlueXP sur une source de données entraîne une analyse initiale immédiate. Les résultats de l'analyse s'affichent peu de temps après.

Comment désactiver la classification BlueXP ?

Vous pouvez désactiver la classification BlueXP pour empêcher l'analyse d'un environnement de travail, d'une base de données ou d'un groupe de partage de fichiers individuels à partir de la page Configuration de la classification BlueXP.

"En savoir plus >>".

> Pour supprimer complètement l'instance de classification BlueXP, vous pouvez supprimer manuellement l'instance de classification BlueXP du portail de votre fournisseur cloud ou de l'emplacement sur site.

Puis-je personnaliser le service en fonction des besoins de mon entreprise ?

La classification BlueXP fournit des informations exploitables sur vos données. Ces informations peuvent être extraites et utilisées en fonction des besoins de votre entreprise.

En outre, la classification BlueXP offre de nombreuses façons d'ajouter une liste personnalisée de « données personnelles » que la classification BlueXP identifiera lors des analyses, ce qui vous donne une vue d'ensemble de l'emplacement des données potentiellement sensibles dans *tous* les fichiers de votre entreprise.

- Vous pouvez ajouter des identificateurs uniques basés sur des colonnes spécifiques dans les bases de données que vous scannez — nous appelons cela **Data Fusion**.

- Vous pouvez ajouter des mots-clés personnalisés à partir d'un fichier texte.
- Vous pouvez ajouter des répétitions personnalisées à l'aide d'une expression régulière (regex).

"En savoir plus >>".

Puis-je demander au service d'exclure les données d'analyse de certains répertoires ?

Oui. Si vous souhaitez que la classification BlueXP exclut les données d'analyse qui résident dans certains répertoires de sources de données, vous pouvez fournir cette liste au moteur de classification. Une fois cette modification appliquée, la classification BlueXP exclut les données d'analyse des répertoires spécifiés.

"En savoir plus >>".

Les copies Snapshot résidant sur les volumes ONTAP sont-elles analysées ?

Non La classification BlueXP ne analyse pas les snapshots, car le contenu est identique au contenu du volume.

Que se passe-t-il si le Tiering des données est activé sur vos volumes ONTAP ?

Lorsque la classification BlueXP analyse les volumes pour lesquels les données inactives sont envoyées vers le stockage objet, il analyse toutes les données, c'est-à-dire les données qui se trouvent sur des disques locaux et les données inactives envoyées vers le stockage objet. C'est également le cas pour les produits non-NetApp qui implémentent la hiérarchisation.

L'analyse ne chauffe pas les données inactives, elles restent inactives et restent dans le stockage objet.

Types de systèmes source et de types de données

Les questions suivantes se rapportent aux types de stockage pouvant être analysés et aux types de données analysées.

Quelles sources de données peuvent être analysées avec la classification BlueXP ?

La classification BlueXP peut analyser les données à partir des environnements de travail que vous avez ajoutés à BlueXP Canvas et de nombreux types de sources de données structurées et non structurées auxquels la classification BlueXP peut accéder sur vos réseaux.

Voir "Environnements de travail et sources de données pris en charge".

Y a-t-il des restrictions lorsqu'elles sont déployées dans une région gouvernementale?

La classification BlueXP est prise en charge lorsque le connecteur est déployé dans une région gouvernementale (AWS GovCloud, Azure Gov ou Azure DoD), également appelée « mode restreint ». Lorsqu'il est déployé de cette manière, la classification BlueXP présente les restrictions suivantes :

> **REMARQUE** ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP.

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

Quelles sources de données puis-je analyser si j'installe la classification BlueXP dans un site sans accès à Internet ?

La classification BlueXP ne peut analyser les données qu'à partir de sources de données locales. À ce stade, la classification BlueXP peut analyser les sources de données locales suivantes en « mode privé », également appelé site « invisible » :

- Systèmes ONTAP sur site
- Schémas de base de données
- Stockage objet qui utilise le protocole simple Storage Service (S3)

Voir "Environnements de travail et sources de données pris en charge".

Quels types de fichiers sont pris en charge ?

La classification BlueXP analyse tous les fichiers pour rechercher des informations par catégorie et par métadonnées, et affiche tous les types de fichiers dans la section types de fichiers du tableau de bord.

Lorsque la classification BlueXP détecte des informations à caractère personnel (PII) ou lorsqu'elle effectue une recherche DSAR, seuls les formats de fichier suivants sont pris en charge :

```
.CSV, .DCM, .DICOM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX,
Docs, Sheets, and Slides
```

Quels types de données et de métadonnées sont capturés par la classification BlueXP ?

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

- **Analyse de mappage des données** : la classification BlueXP analyse uniquement les métadonnées. Ce qui est utile pour la gestion et la gouvernance globales des données, la définition rapide des projets, les gros domaines et la définition des priorités. Le mappage de données est basé sur les métadonnées et est considéré comme une acquisition **FAST**.

  Après une acquisition rapide, vous pouvez générer un rapport de mappage de données. Ce rapport présente les données stockées dans vos sources de données d'entreprise et vous aide à prendre les bonnes décisions en matière d'utilisation des ressources, de migration, de sauvegarde, de sécurité et de conformité.

- **Analyse de classification des données (approfondie)** : analyse de classification BlueXP à l'aide de protocoles standard et d'autorisations en lecture seule dans vos environnements. Les fichiers sélectionnés sont ouverts et analysés afin de détecter toute donnée sensible concernant l'entreprise, des informations privées et des problèmes liés aux attaques par ransomware.

  Après une analyse complète, vous pouvez appliquer de nombreuses fonctionnalités de classification BlueXP supplémentaires à vos données, telles que l'affichage et le raffinage des données dans la page Data Investigation, la recherche de noms dans les fichiers, la copie, le déplacement et la suppression des fichiers source, etc.

La classification BlueXP capture des métadonnées telles que le nom du fichier, les autorisations, l'heure de création, le dernier accès et la dernière modification. Cela inclut toutes les métadonnées qui apparaissent dans

la page Détails de l'investigation de données et dans les rapports d'investigation de données.

La classification BlueXP permet d'identifier de nombreux types de données privées, telles que des informations personnelles (PII) et des informations personnelles sensibles. Pour plus d'informations sur les données privées, reportez-vous à la section "Catégories de données privées analysés par le système de classification BlueXP".

Puis-je limiter les informations de classification BlueXP à des utilisateurs spécifiques ?

Oui, la classification BlueXP est entièrement intégrée avec BlueXP. Les utilisateurs de BlueXP ne peuvent voir les informations relatives aux environnements de travail qu'ils peuvent afficher en fonction de leurs autorisations.

De plus, si vous souhaitez autoriser certains utilisateurs à afficher simplement les résultats d'analyse de classification BlueXP sans avoir la possibilité de gérer les paramètres de classification BlueXP , vous pouvez attribuer à ces utilisateurs le rôle **Visualiseur de classification** (lors de l'utilisation de BlueXP en mode standard) ou le rôle **Visualiseur de conformité** (lors de l'utilisation de BlueXP en mode restreint).

"En savoir plus >>".

Est-il possible d'accéder aux données privées envoyées entre mon navigateur et la classification BlueXP ?

Non Les données privées envoyées entre votre navigateur et l'instance de classification BlueXP sont sécurisées via un chiffrement de bout en bout avec TLS 1.2. Ainsi, NetApp et les tiers ne peuvent pas les lire. La classification BlueXP ne partage aucune donnée ou résultat avec NetApp que si vous demandez et approuvez l'accès.

Les données analysées restent dans votre environnement.

Comment les données sensibles sont-elles gérées ?

NetApp n'a pas accès aux données sensibles et ne les affiche pas dans l'interface utilisateur. Les données sensibles sont masquées. Par exemple, les quatre derniers chiffres sont affichés pour les informations de carte de crédit.

Où sont stockées les données ?

Les résultats d'analyse sont stockés dans Elasticsearch dans votre instance de classification BlueXP.

Comment accéder aux données ?

La classification BlueXP accède aux données stockées dans Elasticsearch via des appels API qui exigent une authentification et chiffrées à l'aide de AES-128. L'accès à Elasticsearch nécessite directement un accès racine.

Licences et coût

La question suivante concerne les licences et les coûts d'utilisation de la classification BlueXP.

Combien coûte la classification BlueXP ?

La classification BlueXP est une fonctionnalité clé de BlueXP qui n'est pas facturée.

Déploiement de connecteurs

Les questions suivantes concernent le connecteur BlueXP.

Quel est le connecteur ?

Il s'agit d'un logiciel exécuté sur une instance de calcul dans votre compte cloud ou sur site, permettant ainsi à BlueXP de gérer les ressources cloud de manière sécurisée. Vous devez déployer un connecteur pour utiliser la classification BlueXP.

Où le connecteur doit-il être installé ?

- Lorsque vous analysez les données dans Cloud Volumes ONTAP dans AWS ou Amazon FSX pour ONTAP, vous utilisez un connecteur dans AWS.
- Pour analyser les données dans Cloud Volumes ONTAP dans Azure ou dans Azure NetApp Files, vous utilisez un connecteur dans Azure.
- Pour l'analyse des données dans Cloud Volumes ONTAP dans GCP, vous utilisez un connecteur dans GCP.
- Lors de l'analyse des données dans des systèmes ONTAP sur site, des partages de fichiers NetApp ou des bases de données, vous pouvez utiliser un connecteur dans l'un de ces emplacements cloud.

Donc, si vous disposez de données à plusieurs de ces emplacements, vous devrez peut-être les utiliser "Plusieurs connecteurs".

La classification BlueXP requiert-elle l'accès aux identifiants ?

La classification BlueXP elle-même ne récupère pas les identifiants du stockage. Elles sont plutôt stockées dans le connecteur BlueXP.

La classification BlueXP utilise les identifiants du plan de données, par exemple les identifiants CIFS pour monter les partages avant l'analyse.

Puis-je déployer le connecteur sur mon propre hôte ?

Oui. C'est possible "Déployez le connecteur sur site" Sur un hôte Linux de votre réseau ou sur un hôte du cloud. Si vous prévoyez de déployer la classification BlueXP sur site, vous pouvez également installer le connecteur sur site, mais ce n'est pas obligatoire.

La communication entre le service et le connecteur utilise-t-elle HTTP ?

Oui, la classification BlueXP communique avec le connecteur BlueXP via HTTP.

Qu'en est-il des sites sécurisés sans accès à Internet ?

Oui, cela est également pris en charge. C'est possible "Déployez le connecteur sur un hôte Linux sur site qui ne dispose pas d'un accès Internet". "Il s'agit également du « mode privé »". Vous pourrez ensuite détecter les clusters ONTAP sur site et d'autres sources de données locales, puis analyser les données à l'aide de la classification BlueXP.

Le déploiement de la classification BlueXP

Les questions suivantes concernent l'instance de classification BlueXP séparée.

Quels modèles de déploiement la classification BlueXP prend-elle en charge ?

BlueXP permet à l'utilisateur d'effectuer des analyses et des rapports sur des systèmes pratiquement n'importe où, y compris sur site, dans le cloud et dans les environnements hybrides. La classification BlueXP est généralement déployée à l'aide d'un modèle SaaS, dans lequel le service est activé via l'interface BlueXP et ne nécessite aucune installation matérielle ou logicielle. Même en ce mode de déploiement cliquer-exécuter, il est possible de gérer les données, que les datastores soient sur site ou dans le cloud public.

Quel type d'instance ou de machine virtuelle est requis pour la classification BlueXP ?

Quand "déploiement dans le cloud":

- Dans AWS, le classement BlueXP s'exécute sur une instance m6i.4xlarge avec un disque GP2 de 500 Gio. Vous pouvez sélectionner un type d'instance plus petit pendant le déploiement.
- Dans Azure, la classification BlueXP s'exécute sur une VM Standard_D16s_v3 avec un disque de 500 Gio.
- Dans GCP, la classification BlueXP s'exécute sur une machine virtuelle n2-standard-16 avec un disque persistant standard de 500 Gio.

"Découvrez le fonctionnement de la classification BlueXP".

Puis-je déployer la classification BlueXP sur mon propre hôte ?

Oui. Vous pouvez installer le logiciel de classification BlueXP sur un hôte Linux disposant d'un accès Internet sur votre réseau ou dans le cloud. Tout fonctionne de la même façon et vous continuez à gérer votre configuration de numérisation et vos résultats via BlueXP. Voir "Déploiement de la classification BlueXP sur site" pour connaître la configuration système requise et les détails de l'installation.

Qu'en est-il des sites sécurisés sans accès à Internet ?

Oui, cela est également pris en charge. C'est possible "Déployez la classification BlueXP sur un site qui ne dispose pas d'un accès Internet" pour des sites totalement sécurisés.

Utilisez la classification BlueXP

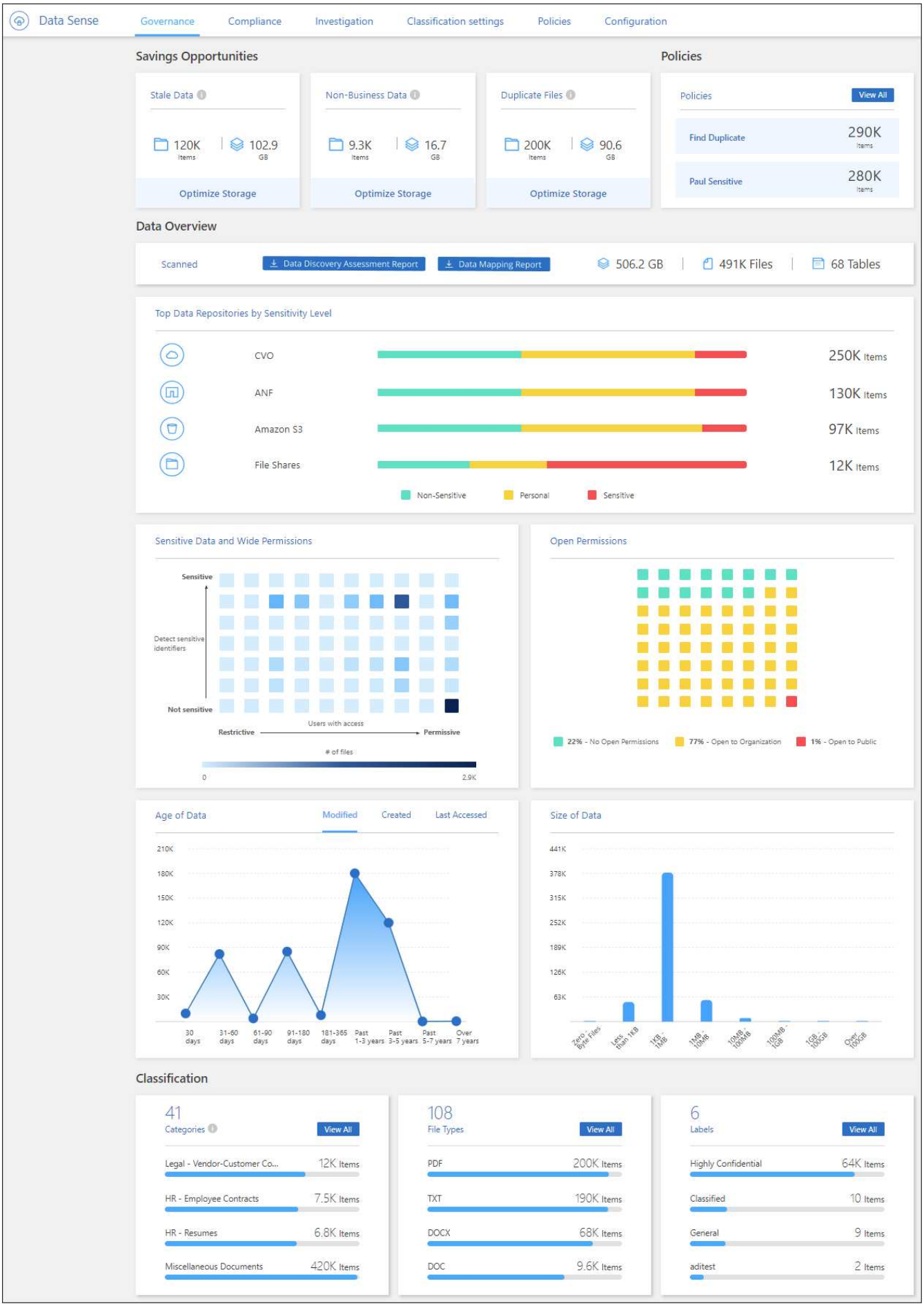
Afficher les détails de gouvernance sur les données stockées dans votre organisation

Maîtrisez les coûts liés aux données stockées sur les ressources de stockage de votre entreprise. La classification BlueXP identifie la quantité de données obsolètes, de données non stratégiques, de fichiers en double et de fichiers très volumineux présents dans vos systèmes. Vous pouvez ainsi décider de supprimer ou de déplacer certains fichiers vers un stockage objet moins coûteux.

En outre, si vous prévoyez de migrer des données depuis des emplacements sur site vers le cloud, vous pouvez afficher la taille des données et voir si elles contiennent des informations sensibles avant de les déplacer.

Tableau de bord gouvernance

Le tableau de bord de gouvernance fournit des informations vous permettant d'améliorer votre efficacité et de contrôler les coûts liés aux données stockées sur vos ressources de stockage.


Data Sense
Governance
Compliance
Investigation
Classification settings
Policies
Configuration
Savings Opportunities
Stale Data
120K Items
102.9 GB
Optimize Storage
Non-Business Data
9.3K Items
16.7 GB
Optimize Storage
Duplicate Files
200K Items
90.6 GB
Optimize Storage
Policies
Policies
View All
Find Duplicate
290K Items
Paul Sensitive
280K Items
Data Overview
Scanned
Data Discovery Assessment Report
Data Mapping Report
506.2 GB
491K Files
68 Tables
Top Data Repositories by Sensitivity Level
CVO
250K Items
ANF
130K Items
Amazon S3
97K Items
File Shares
12K Items
Non-Sensitive
Personal
Sensitive
Sensitive Data and Wide Permissions
Sensitive
Detect sensitive identifiers
Not sensitive
Users with access
Restrictive
Permissive
# of files
0
2.9K
Open Permissions
22% - No Open Permissions
77% - Open to Organization
1% - Open to Public
Age of Data
Modified
Created
Last Accessed
210K
180K
150K
120K
90K
60K
30K
30 days
31-60 days
61-90 days
91-180 days
181-365 days
Past 1-3 years
Past 3-5 years
Past 5-7 years
Over 7 years
Size of Data
441K
378K
315K
252K
189K
126K
63K
Zero Byte Files
Less than 1KB
1KB - 1MB
1MB - 10MB
10MB - 100MB
100MB - 1GB
1GB - 10GB
Over 10GB
Classification
41
Categories
View All
Legal - Vendor-Customer Co...
12K Items
HR - Employee Contracts
7.5K Items
HR - Resumes
6.8K Items
Miscellaneous Documents
420K Items
108
File Types
View All
PDF
200K Items
TXT
190K Items
DOCX
68K Items
DOC
9.6K Items
6
Labels
View All
Highly Confidential
64K Items
Classified
10 Items
General
9 Items
aditest
2 Items

Enregistrer les opportunités

Vous pouvez étudier les éléments de la zone *Saving Opportunities* pour voir s'il y a des données que vous devez supprimer ou mettre en Tier vers un stockage objet moins coûteux. Cliquez sur chaque élément pour afficher les résultats filtrés dans la page Investigation.

- **Données obsolètes** - données qui ont été modifiées pour la dernière fois il y a 3 ans.
- **Données non commerciales** - données considérées comme non liées à l'entreprise, en fonction de leur catégorie ou de leur type de fichier. Les points suivants sont notamment :
  - Données applicatives
  - Audio
  - Exécutables
  - Images
  - Journaux
  - Vidéos
  - Divers (catégorie « autre » générale)
- **Dupliquer les fichiers** - fichiers qui sont dupliqués à d'autres emplacements dans les sources de données que vous numérisez. "Voir quels types de fichiers dupliqués sont affichés".

> Si l'une de vos sources de données implémente le Tiering des données, les anciennes données qui résident déjà dans le stockage objet peuvent être identifiées dans la catégorie *données obsolètes*.

Règles avec le plus grand nombre de résultats

Dans la zone *Policies*, les politiques avec le plus grand nombre de résultats apparaissent en haut de la liste. Cliquez sur le nom d'une police pour afficher les résultats dans la page Investigation. Cliquez sur **Afficher tout** pour afficher la liste de toutes les stratégies disponibles.

Cliquez sur "ici" Pour en savoir plus sur les politiques.

Présentation des données

La section *Data Overview* fournit un aperçu rapide de toutes les données en cours d'acquisition. Cliquez sur le bouton pour télécharger un rapport de mappage de données complet incluant la capacité d'utilisation, l'âge des données, la taille des données et les types de fichiers pour tous vos environnements de travail et toutes vos sources de données. Voir Rapport de mappage de données pour plus d'informations sur ce rapport.

Principaux référentiels de données répertoriés par sensibilité des données

La zone *Top Data Repositories by Sensitivity Level* répertorie les quatre principaux référentiels de données (environnements de travail et sources de données) qui contiennent les éléments les plus sensibles. Le graphique à barres de chaque environnement de travail est divisé en :

- Données non sensibles
- Données personnelles
- Données personnelles sensibles

Vous pouvez placer votre curseur sur chaque section pour voir le nombre total d'éléments dans chaque

catégorie.

Cliquez sur chaque zone pour afficher les résultats filtrés dans la page Investigation afin que vous puissiez approfondir votre recherche.

Données répertoriées par type d'autorisations ouvertes

La zone *Ouvrir autorisations* affiche le pourcentage pour chaque type d'autorisations existant pour tous les fichiers en cours d'analyse. Le graphique montre les types d'autorisations suivants :

- Aucune autorisation ouverte
- Ouvert à l'organisation
- Ouvert au public
- Accès inconnu

Vous pouvez placer votre curseur sur chaque section pour voir le nombre total de fichiers dans chaque catégorie. Cliquez sur chaque zone pour afficher les résultats filtrés dans la page Investigation afin que vous puissiez approfondir votre recherche.

Age des données et taille des données graphiques

Vous pouvez étudier les éléments des graphiques *Age* et *Size* afin de voir s'il y a des données que vous devez supprimer ou placer dans un stockage objet moins coûteux.

Vous pouvez placer votre curseur sur un point des graphiques pour afficher des détails sur l'âge ou la taille des données de cette catégorie. Cliquez pour afficher tous les fichiers filtrés en fonction de l'âge ou de la plage de tailles.

- **Age of Data Graph** - catégorise les données en fonction de l'heure de création, de la dernière fois où il a été accédé ou de la dernière fois qu'il a été modifié.
- **Taille du graphique de données** - classe les données en fonction de leur taille.

> Si l'une de vos sources de données implémente le Tiering des données, les anciennes données qui résident déjà dans le stockage objet peuvent être identifiées dans le graphique *Age of Data*.

Classification des données la plus identifiée

La zone *Classification* fournit une liste des plus identifiés "Catégories" et "Types de fichiers" dans vos données numérisées.

Catégories

Les catégories peuvent vous aider à comprendre ce qui se passe avec vos données en vous montrant les types d'informations dont vous disposez. Par exemple, une catégorie telle que « CV » ou « contrats employés » peut inclure des données sensibles. Lorsque vous examinez les résultats, vous pouvez constater que les contrats d'employés sont stockés dans un emplacement non sécurisé. Vous pouvez ensuite corriger ce problème.

Voir "Affichage des fichiers par catégories" pour en savoir plus.

Types de fichiers

La vérification de vos types de fichiers peut vous aider à contrôler vos données sensibles car il se peut que certains types de fichiers ne soient pas stockés correctement.

Voir "Affichage des types de fichiers" pour en savoir plus.

Rapport de mappage de données

Le rapport de mappage de données offre une vue d'ensemble des données stockées dans les sources de données de votre entreprise pour vous aider à prendre des décisions concernant la migration, la sauvegarde, la sécurité et les processus de conformité. Le rapport répertorie d'abord une vue d'ensemble qui résume l'ensemble de vos environnements de travail et sources de données, puis fournit une analyse pour chaque environnement de travail.

Le rapport contient les informations suivantes :

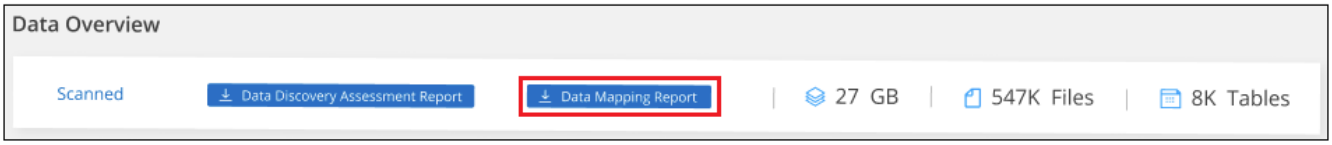
Catégorie	Description
Capacité d'utilisation	Pour tous les environnements de travail : indique le nombre de fichiers et la capacité utilisée pour chaque environnement de travail. Pour les environnements de travail uniques : répertorie les fichiers qui utilisent la capacité la plus élevée.
Âge des données	Fournit trois graphiques pour la date de création, la dernière modification ou le dernier accès aux fichiers. Répertorie le nombre de fichiers et leur capacité utilisée, en fonction de certaines plages de dates.
Taille des données	Répertorie le nombre de fichiers qui existent dans certaines plages de tailles dans vos environnements de travail.
Types de fichiers	Indique le nombre total de fichiers et la capacité utilisée pour chaque type de fichier stocké dans vos environnements de travail.

Générez le rapport de mappage de données

Ce rapport est généré à partir de l'onglet gouvernance de la classification BlueXP.

Étapes

1. Dans le menu BlueXP, cliquez sur **gouvernance > Classification**.
2. Cliquez sur **gouvernance**, puis sur le bouton **Rapport de mappage des données**.



Résultat

La classification BlueXP génère un rapport au format .PDF que vous pouvez examiner et envoyer à d'autres groupes si nécessaire.

Si la taille du rapport est supérieure à 1 Mo, le fichier .PDF est conservé dans l'instance de classification BlueXP et un message contextuel s'affiche pour vous informer de l'emplacement exact. Lorsque la classification BlueXP est installée sur une machine Linux de votre site ou sur une machine Linux que vous

avez déployée dans le cloud, vous pouvez accéder directement au fichier .PDF. Lorsque la classification BlueXP est déployée dans le cloud, vous devez SSH vers l'instance de classification BlueXP pour télécharger le fichier .PDF. "Voir comment accéder aux données sur l'instance de classification".

Notez que vous pouvez personnaliser le nom de l'entreprise qui apparaît sur la première page du rapport en partant du haut de la page de classification BlueXP en cliquant sur ⋮ Puis cliquez sur **changer le nom de l'entreprise**. La prochaine fois que vous générez le rapport, il inclura le nouveau nom.

Rapport d'évaluation de découverte de données

Le rapport d'évaluation de la découverte de données fournit une analyse de haut niveau de l'environnement analysé afin de mettre en évidence les résultats du système et de montrer les points préoccupants et les étapes de correction potentielles. Les résultats sont basés à la fois sur le mappage et la classification de vos données. L'objectif de ce rapport est de sensibiliser les clients à trois aspects importants de leur dataset :

Fonction	Description
Problèmes de gouvernance des données	Une vue d'ensemble détaillée de toutes les données que vous possédez et des zones dans lesquelles vous pouvez réduire la quantité de données pour réduire les coûts.
Risques liés à la sécurité des données	Zones où vos données sont accessibles pour les attaques internes ou externes en raison d'autorisations d'accès étendues.
Lacunes en matière de conformité des données	Où se trouvent vos informations personnelles ou sensibles à des fins de sécurité et pour les DSAR (demandes d'accès des sujets de données).

Après l'évaluation, ce rapport identifie les domaines dans lesquels vous pouvez :

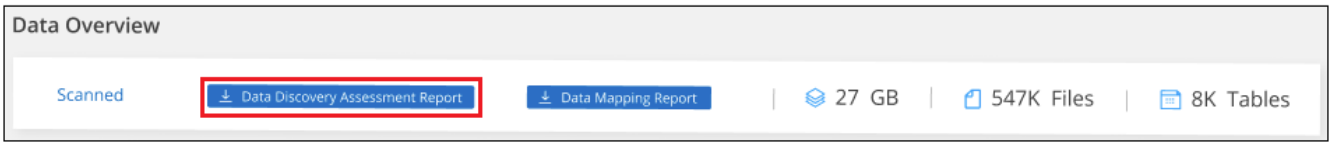
- Réduction des coûts du stockage en modifiant votre règle de conservation, ou en déplaçant ou en supprimant certaines données (obsolètes, dupliquées ou non stratégiques)
- Protégez vos données qui disposent de larges autorisations en modifiant les stratégies de gestion de groupe globales
- Protégez vos données personnelles ou sensibles en déplaçant vos IIP vers des magasins de données plus sécurisés

Générez le rapport d'évaluation de la découverte de données

Ce rapport est généré à partir de l'onglet gouvernance de la classification BlueXP.

Étapes

1. Dans le menu BlueXP, cliquez sur **gouvernance > Classification**.
2. Cliquez sur **gouvernance**, puis sur le bouton **Rapport d'évaluation de la découverte de données**.



Résultat

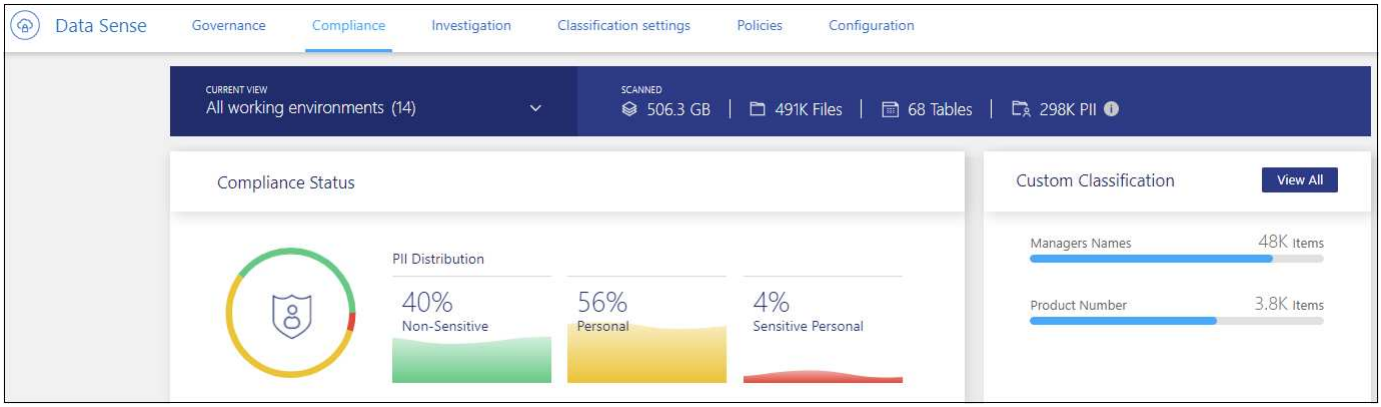
La classification BlueXP génère un rapport au format .PDF que vous pouvez examiner et envoyer à d'autres groupes si nécessaire.

Afficher les détails de conformité des données privées stockées dans votre organisation

Prenez le contrôle de vos données personnelles en consultant les informations relatives aux données personnelles (PII) et aux données personnelles sensibles (SPII) de votre entreprise. Vous pouvez également gagner en visibilité en passant en revue les catégories et les types de fichiers classés par BlueXP dans vos données.

> Les fonctionnalités décrites dans cette section ne sont disponibles que si vous avez choisi d'effectuer une analyse de classification complète sur vos sources de données. Les sources de données qui ont une analyse avec mappage uniquement n'affichent pas de détails au niveau des fichiers.

Par défaut, le tableau de bord de classification BlueXP affiche les données de conformité pour tous les environnements de travail et bases de données.



Si vous ne souhaitez voir des données que pour certains environnements de travail, sélectionnez ces environnements de travail.

Vous pouvez également filtrer les résultats à partir de la page Data Investigation et télécharger un rapport des résultats sous forme de fichier CSV. Voir "Filtrage des données dans la page Data Investigation" pour plus d'informations.

Afficher les fichiers contenant des données personnelles

La classification BlueXP identifie automatiquement des mots, des chaînes et des modèles spécifiques (Regex) à l'intérieur des données. Par exemple, les renseignements d'identification personnelle (RP), les numéros de carte de crédit, les numéros de sécurité sociale, les numéros de compte bancaire, les mots de passe, entre autres. "Voir la liste complète". La classification BlueXP identifie ce type d'informations dans des fichiers individuels, dans des fichiers dans des répertoires (partages et dossiers) et dans des tables de bases de données.

En outre, si vous avez ajouté un serveur de base de données à scanner, la fonction *Data Fusion* vous permet de numériser vos fichiers afin d'identifier si des identificateurs uniques de vos bases de données se trouvent dans ces fichiers ou d'autres bases de données. Voir "Ajout d'identifiants de données personnels à l'aide de Data Fusion" pour plus d'informations.

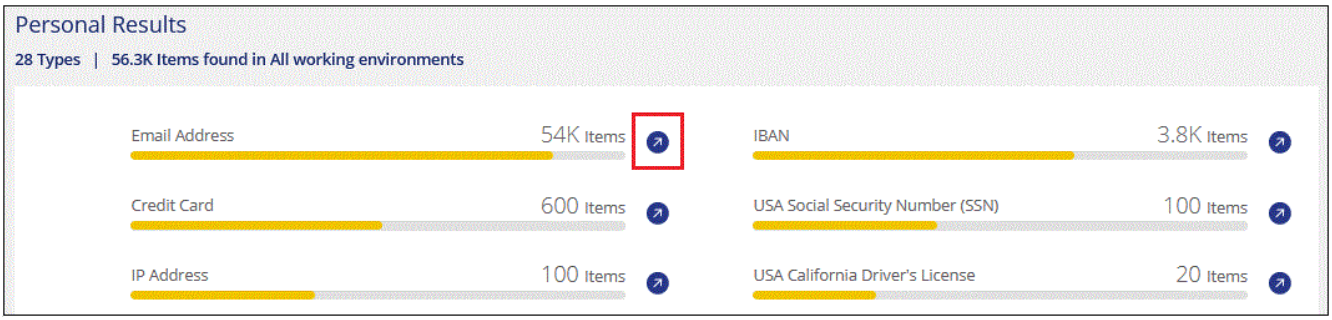
Pour certains types de données personnelles, la classification BlueXP utilise la *validation de proximité* pour valider ses résultats. La validation se produit en recherchant un ou plusieurs mots clés prédéfinis à proximité

des données personnelles trouvées. Par exemple, la classification BlueXP identifie un agent américain Numéro de sécurité sociale (SSN) comme numéro de sécurité sociale s'il y a un mot de proximité, par exemple, *SSN* ou *social Security*. "Le tableau des données personnelles" Indique quand la classification BlueXP utilise la validation de proximité.

Étapes

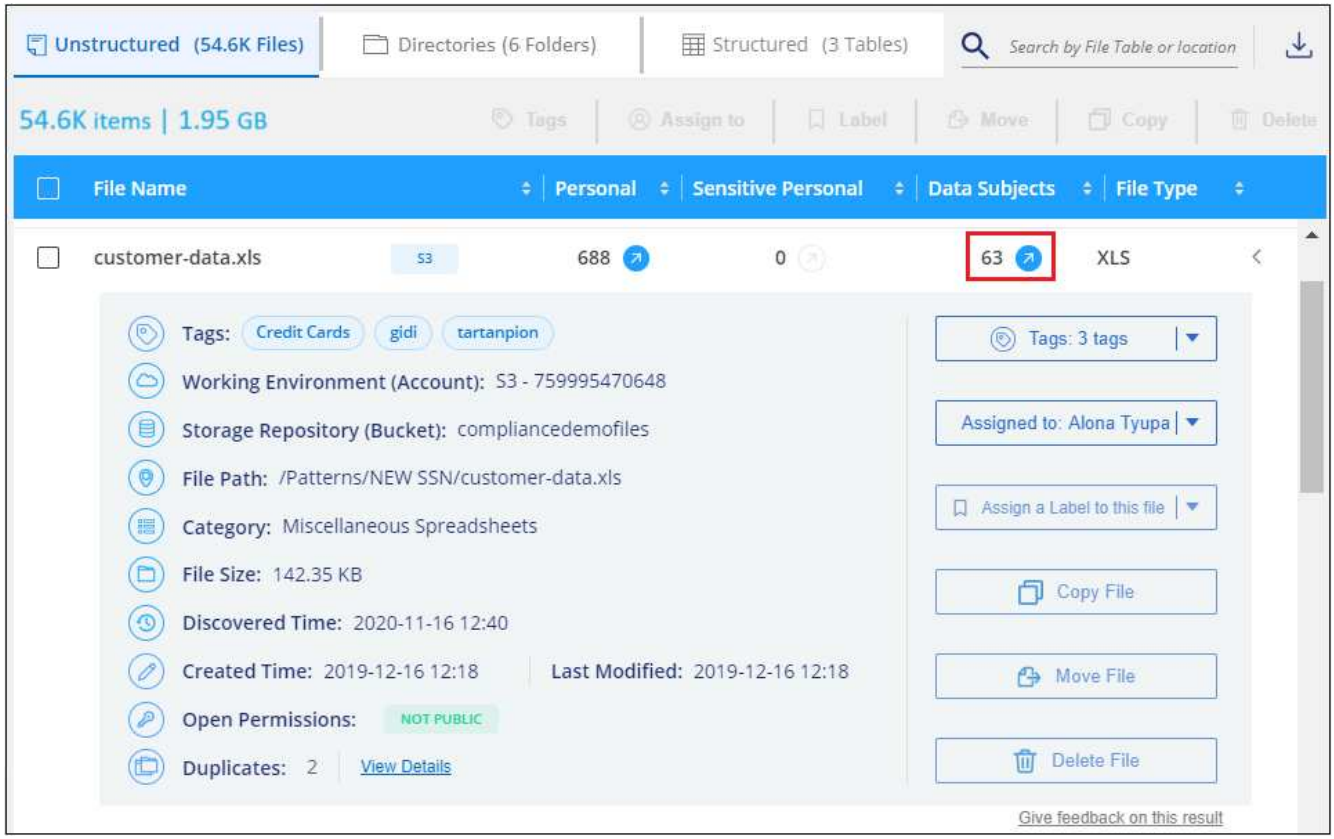
1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > classement**, puis sur l'onglet **conformité**.
2. Pour examiner les détails de toutes les données personnelles, cliquez sur l'icône en regard du pourcentage de données personnelles.

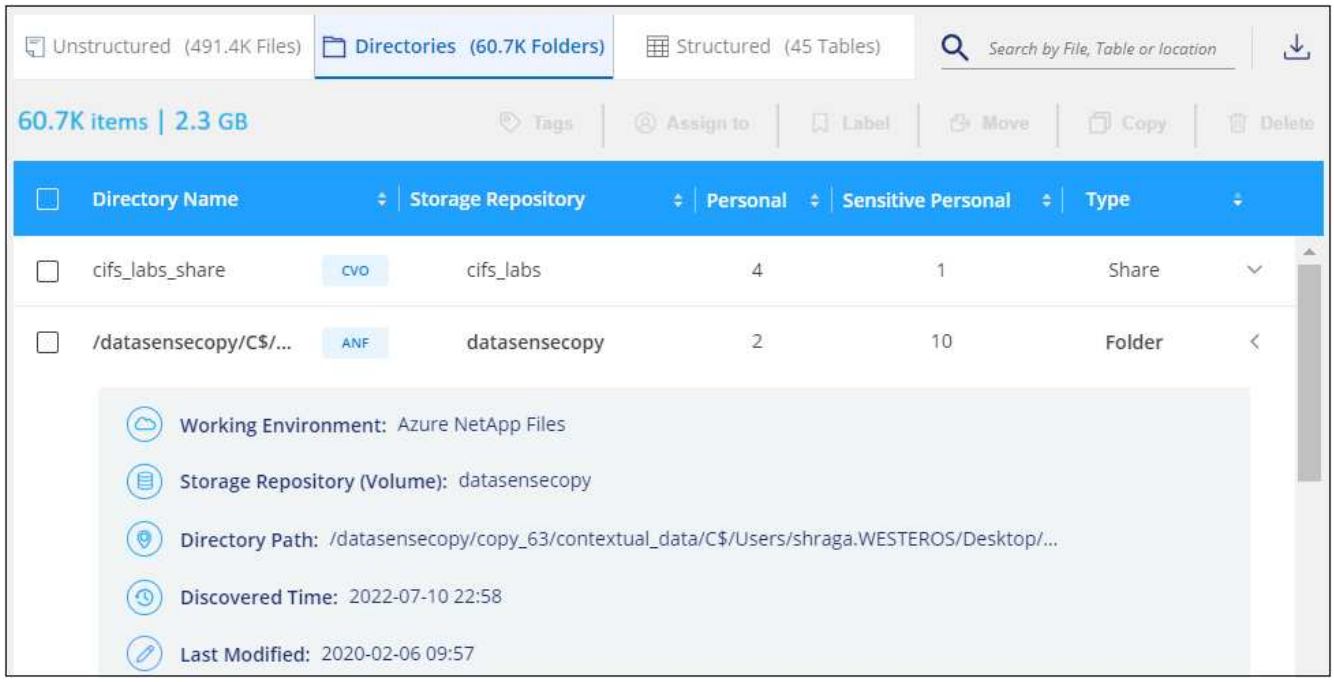
3. Pour examiner les détails d'un type spécifique de données personnelles, cliquez sur **Afficher tout**, puis cliquez sur l'icône **étudier les résultats** pour un type spécifique de données personnelles, par exemple les adresses e-mail.



4. Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en cliquant sur **Informez Results** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.

   Les 2 captures d'écran ci-dessous montrent les données personnelles trouvées dans des fichiers individuels et trouvées dans des fichiers dans des répertoires (partages et dossiers). Vous pouvez également sélectionner l'onglet **Structured** pour afficher les données personnelles contenues dans les bases de données.





Affichez les fichiers contenant des données personnelles sensibles

La classification BlueXP identifie automatiquement des types spéciaux d'informations personnelles sensibles, tels que définis par les réglementations en matière de confidentialité, notamment "Les articles 9 et 10 du RGPD". Par exemple, des renseignements concernant la santé d'une personne, son origine ethnique ou son orientation sexuelle. "Voir la liste complète". La classification BlueXP identifie ce type d'informations dans des fichiers individuels, dans des fichiers dans des répertoires (partages et dossiers) et dans des tables de bases de données.

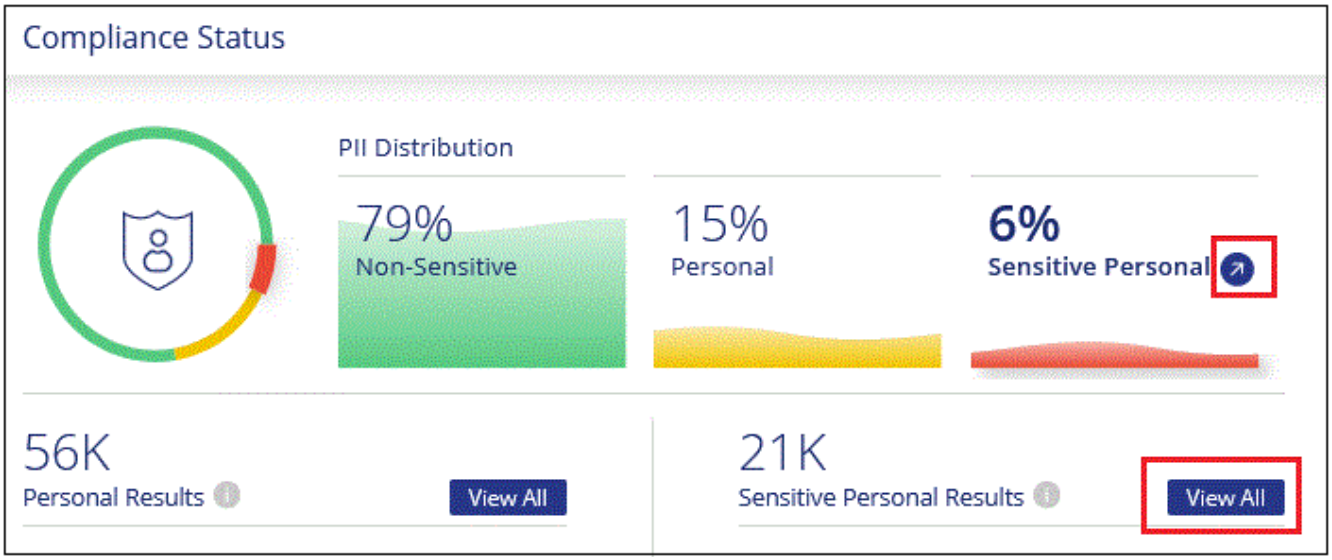
La classification BlueXP utilise l'intelligence artificielle (IA), le traitement du langage naturel (NLP), le machine learning (ML) et l'informatique cognitive (CC) pour comprendre la signification du contenu qu'il analyse afin d'extraire des entités et le catégoriser en conséquence.

Par exemple, une catégorie de données sensibles du RGPD est l'origine ethnique. Du fait de ses capacités NLP, le classement BlueXP peut faire la différence entre la phrase « George est mexicain » (indiquant des données sensibles comme spécifié dans l'article 9 du RGPD) et « George mange mexicain ».

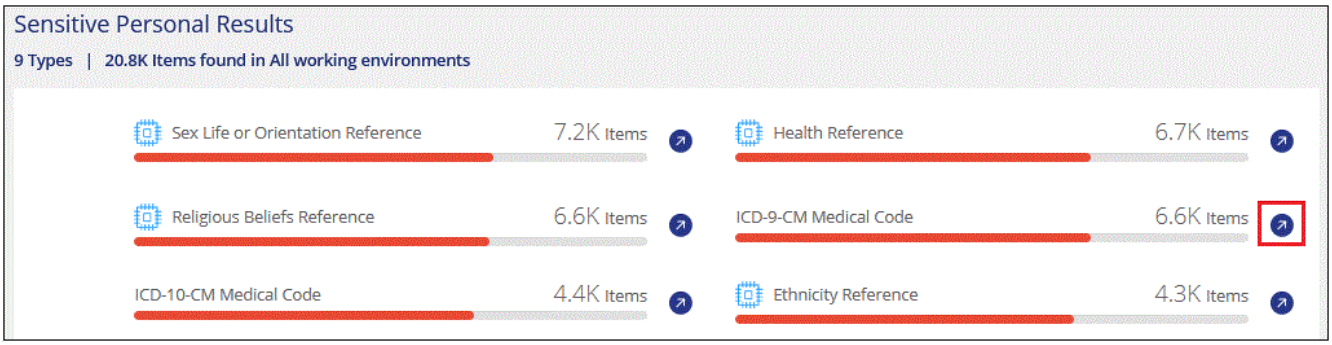
> Seul l'anglais est pris en charge lors de la recherche de données personnelles sensibles. La prise en charge d'autres langues sera ajoutée ultérieurement.

Étapes

1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > classement**, puis sur l'onglet **conformité**.
2. Pour examiner les détails de toutes les données personnelles sensibles, cliquez sur l'icône en regard du pourcentage de données personnelles sensibles.



3. Pour examiner les détails d'un type spécifique de données personnelles sensibles, cliquez sur **Afficher tout**, puis cliquez sur l'icône **enquêter sur les résultats** pour un type spécifique de données personnelles sensibles.



4. Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en cliquant sur **Informez Results** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.

Afficher les fichiers par catégories

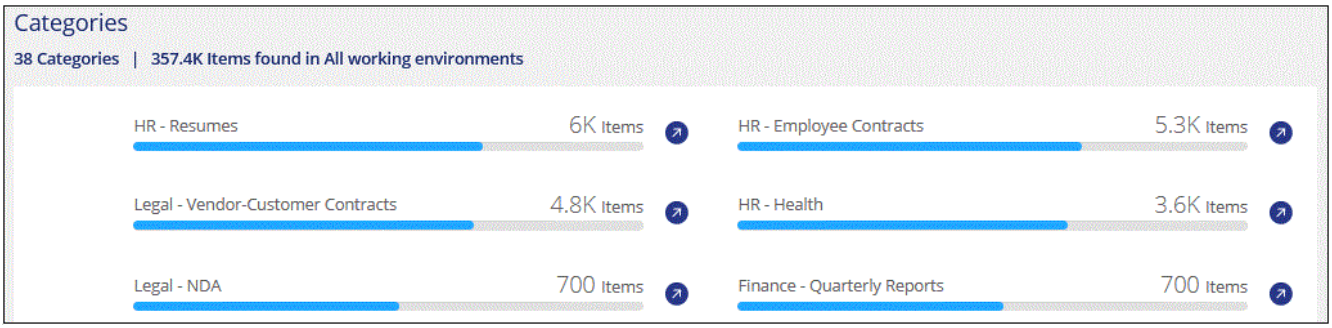
La classification BlueXP récupère les données qu'il a analysées et les divise en différents types de catégories. Les catégories sont des rubriques basées sur l'analyse par IA du contenu et des métadonnées de chaque fichier. "Voir la liste des catégories".

Les catégories peuvent vous aider à comprendre ce qui se passe avec vos données en vous montrant les types d'informations dont vous disposez. Par exemple, une catégorie comme les CV ou les contrats d'employés peut inclure des données sensibles. Lorsque vous examinez les résultats, vous pouvez constater que les contrats d'employés sont stockés dans un emplacement non sécurisé. Vous pouvez ensuite corriger ce problème.

> L'anglais, l'allemand et l'espagnol sont pris en charge pour les catégories. La prise en charge d'autres langues sera ajoutée ultérieurement.

Étapes

1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > classement**, puis sur l'onglet **conformité**.
2. Cliquez sur l'icône **Inquiétude Results** pour l'une des 4 catégories les plus importantes directement à partir de l'écran principal, ou cliquez sur **Afficher tout**, puis cliquez sur l'icône de l'une des catégories.



3. Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en cliquant sur **Informez Results** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.

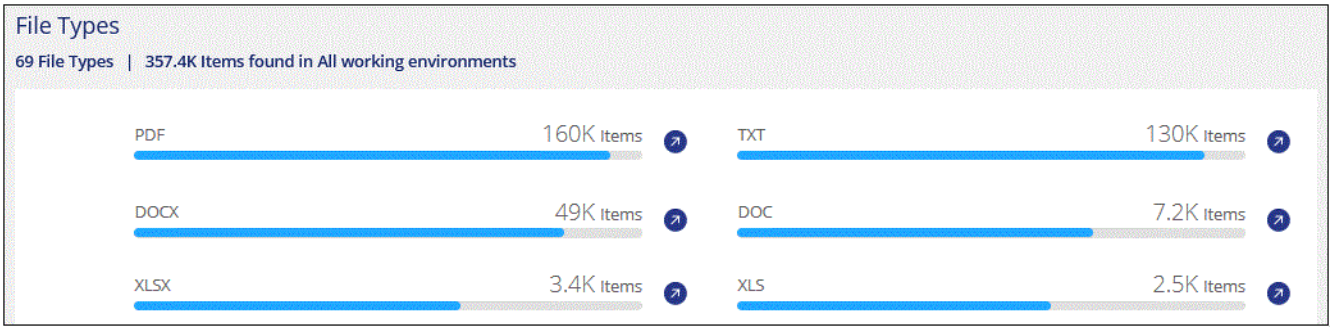
Afficher les fichiers par type de fichier

La classification BlueXP répartit les données analysées par type de fichier. La vérification de vos types de fichiers peut vous aider à contrôler vos données sensibles car il se peut que certains types de fichiers ne soient pas stockés correctement. "Voir la liste des types de fichiers".

Par exemple, vous pouvez stocker des fichiers CAO qui contiennent des informations très sensibles sur votre organisation. S'ils ne sont pas sécurisés, vous pouvez prendre le contrôle des données sensibles en limitant les autorisations ou en déplaçant les fichiers vers un autre emplacement.

Étapes

1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > classement**, puis sur l'onglet **conformité**.
2. Cliquez sur l'icône **étudier les résultats** pour l'un des 4 types de fichiers les plus importants directement à partir de l'écran principal ou cliquez sur **Afficher tout**, puis cliquez sur l'icône correspondant à l'un des types de fichiers.



3. Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en cliquant sur **Informez Results** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.

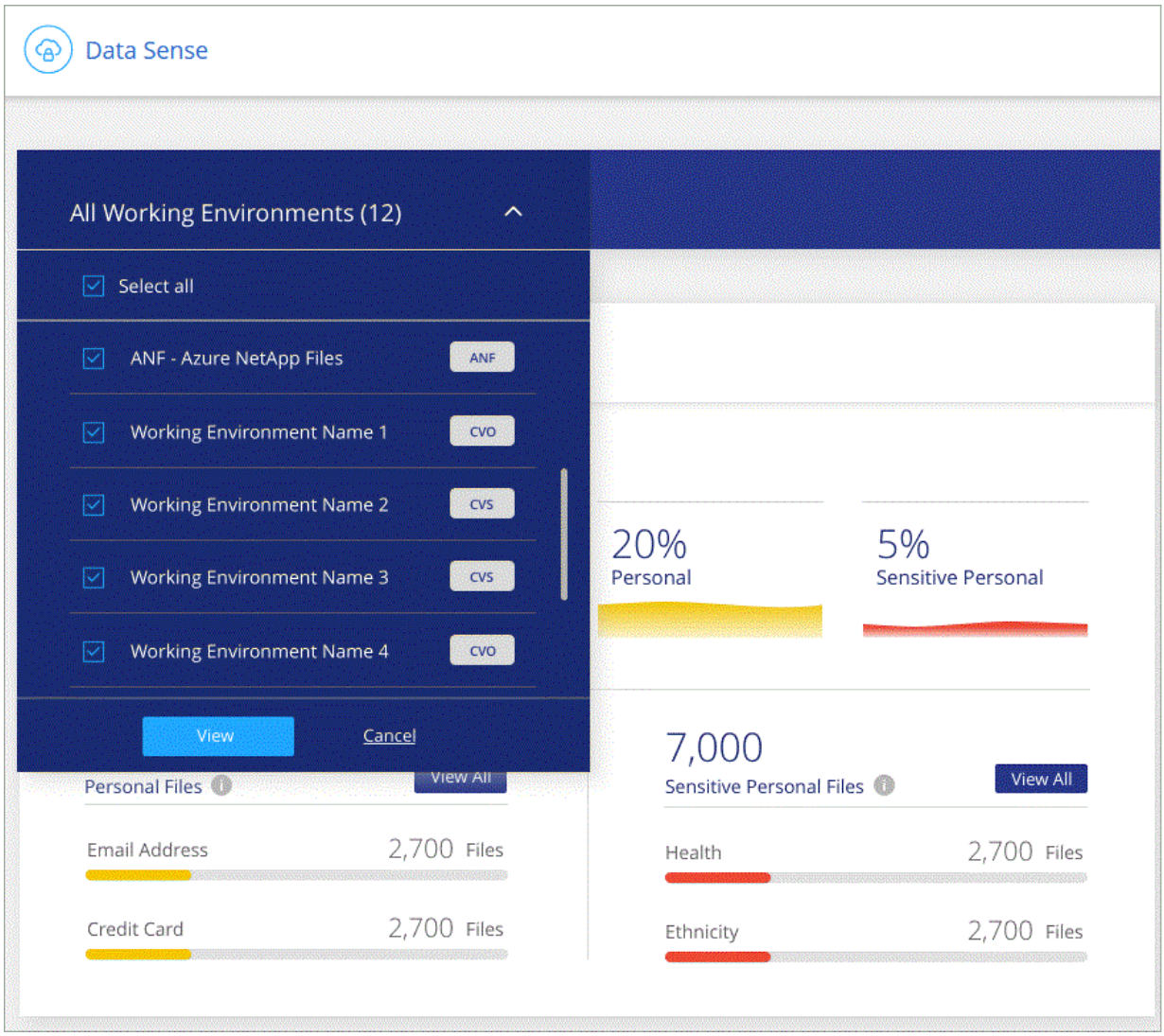
Afficher les données du tableau de bord pour des environnements de travail spécifiques

Vous pouvez filtrer le contenu du tableau de bord de classification BlueXP pour afficher les données de conformité de tous les environnements de travail et bases de données, ou pour seulement des environnements de travail spécifiques.

Lorsque vous filtrez le tableau de bord, la classification BlueXP évalue les données et les rapports de conformité pour les environnements de travail que vous avez sélectionnés.

Étapes

1. Cliquez sur la liste déroulante du filtre, sélectionnez les environnements de travail pour lesquels vous souhaitez afficher les données, puis cliquez sur **Afficher**.



Catégories de données privées

Il existe de nombreux types de données privées que la classification BlueXP peut identifier dans vos volumes et vos bases de données.

La classification BlueXP identifie deux types de données personnelles :

- **Informations personnelles identifiables (PII)**
- **Informations personnelles sensibles (SPII)**

> Si vous avez besoin de la classification BlueXP pour identifier d'autres types de données privées, comme des numéros d'identification nationaux supplémentaires ou des identifiants de santé, envoyez un e-mail à ng-contact-data-sense@netapp.com à votre demande.

Types de données personnelles

Les données personnelles, ou *informations personnelles identifiables* (PII), qui se trouvent dans les fichiers peuvent être des données personnelles générales ou des identificateurs nationaux. La troisième colonne du tableau ci-dessous indique si la classification BlueXP utilise "validation de proximité" pour valider ses résultats

pour l’identificateur.

Les langues dans lesquelles ces éléments peuvent être reconnus sont identifiées dans le tableau.

Type	Identificateur	Validation de proximité ?	Anglais	Allemand	Espagnol	Français	Japonais
Généralités	Numéro de carte de crédit	Non	✓	✓	✓		✓
	Sujets de données	Non	✓	✓	✓		
	Adresse électronique	Non	✓	✓	✓		✓
	Numéro IBAN (numéro de compte bancaire international)	Non	✓	✓	✓		✓
	Adresse IP	Non	✓	✓	✓		✓
	Mot de passe	Oui.	✓	✓	✓		✓

Type	Identificateur	Validation de proximité ?	Anglais	Allemand	Espagnol	Français	Japonais
Identifiants nationaux							

Type	Identificateur	Validation de proximité ?	Anglais	Allemand	Espagnol	Français	Japonais

Type	Identificateur	Validation de proximité	Anglais	Allemand	Espagnol	Français	Japonais
	ID slovène (EMSO)	Oui.	✓	✓	✓		
	Carte d'identité sud-africaine	Oui.	✓	✓	✓		
	Numéro d'identification fiscale espagnol	Oui.	✓	✓	✓		
	Carte d'identité suédoise	Oui.	✓	✓	✓		
	Permis de conduire Texas	Oui.	✓	✓	✓		
	ROYAUME-UNI ID (NINO)	Oui.	✓	✓	✓		
	Permis de conduire de Californie aux États-Unis	Oui.	✓	✓	✓		
	Permis de conduire de l'Indiana des États-Unis	Oui.	✓	✓	✓		
	Permis de conduire New York aux États-Unis	Oui.	✓	✓	✓		
	Numéro de sécurité sociale des États-Unis (SSN)	Oui.	✓	✓	✓		

Types de données personnelles sensibles

La classification BlueXP peut trouver les informations personnelles sensibles suivantes (SPII) dans des fichiers.

Les éléments de cette catégorie ne peuvent être reconnus qu'en anglais pour le moment.

- **Référence pour les procédures pénales** : données concernant les condamnations et les infractions criminelles d'une personne physique.
- **Référence ethnique** : données concernant l'origine raciale ou ethnique d'une personne physique.
- * Référence en matière de santé* : données concernant la santé d'une personne physique.
- **Codes médicaux CIM-9-cm** : codes utilisés dans l'industrie médicale et de la santé.
- **Codes médicaux CIM-10-cm** : codes utilisés dans l'industrie médicale et de la santé.
- **Croyances philosophiques référence**: Données concernant les croyances philosophiques d'une personne physique.
- **Opinions politiques référence**: Données concernant les opinions politiques d'une personne physique.
- **Croyances religieuses référence** : données concernant les croyances religieuses d'une personne physique.
- **Sexe vie ou orientation référence** : données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Types de catégories

La classification BlueXP classe vos données comme suit.

La plupart de ces catégories peuvent être reconnues en anglais, allemand et espagnol.

Catégorie	Type	Anglais	Allemand	Espagnol
Finances	Bilans	✓	✓	✓
	Bons de commande	✓	✓	✓
	Factures	✓	✓	✓
	Rapports trimestriels	✓	✓	✓
RH	Vérifications des antécédents	✓		✓
	Plans de rémunération	✓	✓	✓
	Contrats employés	✓		✓
	Évaluations des employés	✓		✓
	Santé	✓		✓
	Reprend	✓	✓	✓
Légal	NDAS	✓	✓	✓
	Contrats fournisseur-client	✓	✓	✓
Marketing	Campagnes	✓	✓	✓
	Conférences	✓	✓	✓
Exploitation	Rapports d'audit	✓	✓	✓
Ventes	Commandes	✓	✓	
Administratifs	RFI	✓		✓
	RFP	✓		✓
	CAHIER DES CHARGES	✓	✓	✓
	Formation	✓	✓	✓
Assistance	Plaintes et tickets	✓	✓	✓

Les métadonnées suivantes sont également classées en catégories et identifiées dans les mêmes langues prises en charge :

- Données applicatives
- Archiver les fichiers
- Audio
- Fils d'Ariane dans la classification BlueXP
  Données d'applications d'entreprise
- Fichiers CAO
- Code
- Corrompu
- Base de données et fichiers d'index
- Fichiers de conception

- Données d'application de messagerie
- Crypté (fichiers avec un score d'entropie élevé)
- Exécutables
- Données d'applications financières
- Données d'application de santé
- Images
- Journaux
- Documents divers
- Présentations diverses
- Feuilles de calcul diverses
- Divers « Inconnu »
- Fichiers protégés par mot de passe
- Données structurées
- Vidéos
- Fichiers de zéro octet

Types de fichiers

La classification BlueXP analyse tous les fichiers pour rechercher des informations par catégorie et par métadonnées, et affiche tous les types de fichiers dans la section types de fichiers du tableau de bord.

Toutefois, lorsque la classification BlueXP détecte des informations à caractère personnel (PII) ou lorsqu'elle effectue une recherche DSAR, seuls les formats de fichier suivants sont pris en charge :

```
.CSV, .DCM, .DICOM, .DOC, .DOCX, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX,
Docs, Sheets, and Slides
```

Exactitude des informations trouvées

NetApp ne peut pas garantir l'exactitude à 100 % des données personnelles et des données personnelles sensibles identifiées par la classification BlueXP. Vous devez toujours valider les informations en examinant les données.

D'après nos tests, le tableau ci-dessous précise les informations trouvées par la classification BlueXP. Nous la décomposent par *Precision* et *rappel*:

Précision

La probabilité que la classification BlueXP trouve ait été correctement identifiée. Par exemple, un taux de précision de 90 % pour les données personnelles signifie que 9 fichiers sur 10 identifiés comme contenant des renseignements personnels, contiennent en fait des renseignements personnels. 1 fichier sur 10 serait un faux positif.

Rappel

Probabilité que la classification BlueXP trouve ce qu'elle doit. Par exemple, un taux de rappel de 70 % pour les données personnelles signifie que la classification BlueXP peut identifier 7 fichiers sur 10 qui contiennent réellement des données personnelles dans votre entreprise. 30 % des données sont classifiées et n'apparaîtront pas dans le tableau de bord.

Nous améliorons constamment la précision de nos résultats. Ces améliorations seront automatiquement disponibles dans les futures versions de classification BlueXP.

Type	Précision	Rappel
Données personnelles - général	90 à 95 %	60 à 80 %
Données personnelles - identificateurs de pays	30 à 60 %	40 à 60 %
Données personnelles sensibles	80 à 95 %	20 à 30 %
Catégories	90 à 97 %	60 à 80 %

Examinez les données stockées dans votre organisation

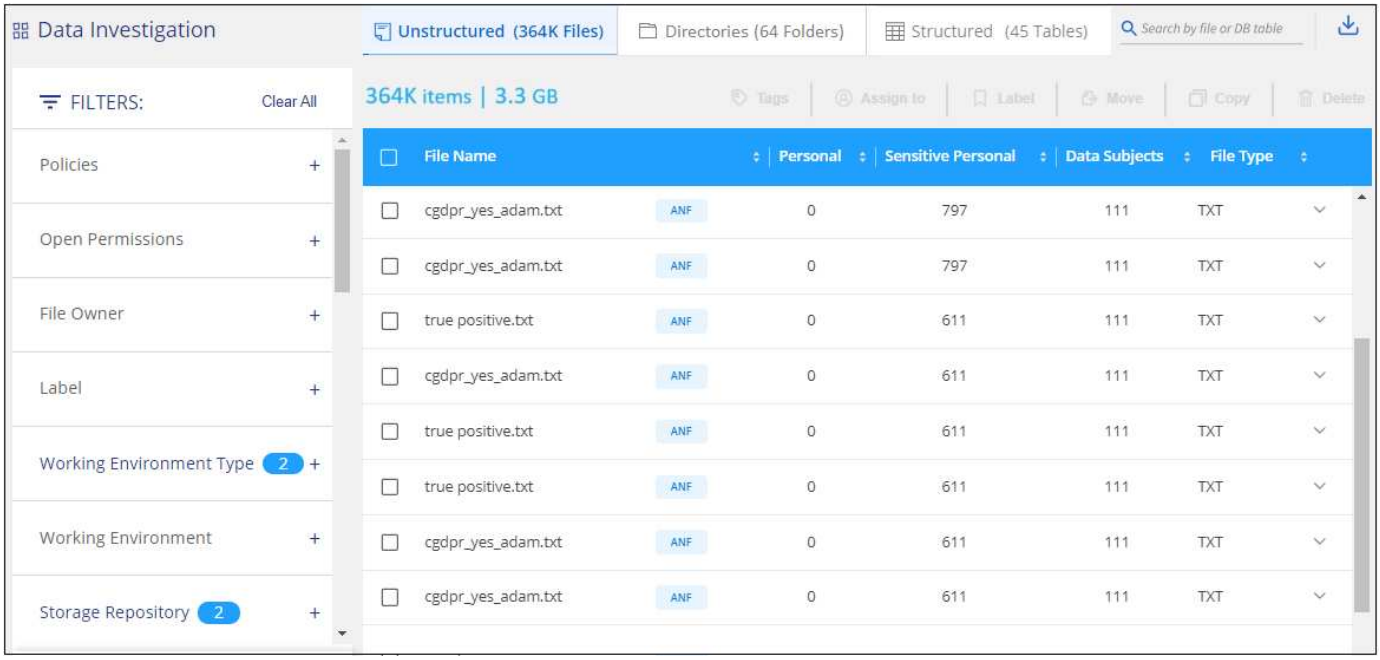
Vous pouvez examiner les données de votre organisation en affichant les détails dans la page recherche de données. Vous pouvez naviguer jusqu'à cette page à partir de plusieurs sections de l'interface de classification BlueXP, y compris les tableaux de bord gouvernance et conformité.

> Les fonctionnalités décrites dans cette section ne sont disponibles que si vous avez choisi d'effectuer une analyse de classification complète sur vos sources de données. Les sources de données qui ont une analyse avec mappage uniquement n'affichent pas de détails au niveau des fichiers.

Filtrez les données dans la page Data Investigation

Vous pouvez filtrer le contenu de la page d'enquête pour n'afficher que les résultats que vous souhaitez voir. Il s'agit d'une fonctionnalité très puissante car une fois les données raffinées, vous pouvez utiliser la barre de boutons en haut de la page pour effectuer diverses actions, notamment copier des fichiers, déplacer des fichiers, ajouter une balise ou une étiquette AIP aux fichiers, et bien plus encore.

Si vous souhaitez télécharger le contenu de la page en tant que rapport après l'avoir affiné, cliquez sur le bouton bouton. Cliquez ici pour plus de détails sur le rapport d'enquête sur les données.



- Les onglets de niveau supérieur vous permettent d'afficher les données issues de fichiers (données non structurées), de répertoires (dossiers et partages de fichiers) ou de bases de données (données structurées).
- Les commandes situées en haut de chaque colonne vous permettent de trier les résultats par ordre numérique ou alphabétique.
- Les filtres du volet gauche vous permettent d'affiner les résultats en sélectionnant les attributs décrits dans les sections suivantes.

Filtrer les données par sensibilité et par contenu

Utilisez les filtres suivants pour afficher la quantité d'informations sensibles contenues dans vos données.

Filtre	Détails
Catégorie	Sélectionner "types de catégories".
Niveau de sensibilité	Sélectionnez le niveau de sensibilité : personnel, personnel sensible ou non sensible.
Nombre d'identificateurs	Sélectionnez la plage d'identificateurs sensibles détectés par fichier. Inclut des données personnelles et des données personnelles sensibles. Lors du filtrage dans les répertoires, la classification BlueXP totalise les correspondances de tous les fichiers de chaque dossier (et sous-dossiers). REMARQUE : la version de décembre 2023 (version 1.26.6) a supprimé l'option permettant de calculer le nombre de données d'informations personnelles identifiables (PII) par répertoires.
Données personnelles	Sélectionner "types de données personnelles".
Données personnelles sensibles	Sélectionner "types de données personnelles sensibles".
Sujet de données	Saisissez le nom complet ou l'identifiant connu d'un sujet de données. "Pour en savoir plus sur les sujets de données, cliquez ici".

Filtrez les données par propriétaire d'utilisateur et par autorisation utilisateur

Utilisez les filtres suivants pour afficher les propriétaires de fichiers et les autorisations d'accès à vos données.

Filtre	Détails
Ouvrez autorisations	Sélectionnez le type d'autorisations dans les données et dans les dossiers/partages.
Autorisations utilisateur/groupe	Sélectionnez un ou plusieurs noms d'utilisateur et/ou de groupe ou entrez un nom partiel.
Propriétaire du fichier	Entrez le nom du propriétaire du fichier.
Nombre d'utilisateurs ayant accès	Sélectionnez une ou plusieurs plages de catégories pour afficher les fichiers et dossiers ouverts à un certain nombre d'utilisateurs.

Filtrez les données par heure

Utilisez les filtres suivants pour afficher les données en fonction des critères de temps.

Filtre	Détails
Heure de création	Sélectionnez une plage horaire au moment de la création du fichier. Vous pouvez également spécifier une plage horaire personnalisée pour affiner davantage les résultats de la recherche.
Heure découverte	Sélectionnez une plage horaire lorsque la classification BlueXP a détecté le fichier. Vous pouvez également spécifier une plage horaire personnalisée pour affiner davantage les résultats de la recherche.
Dernière modification	Sélectionnez une plage horaire pour la dernière modification du fichier. Vous pouvez également spécifier une plage horaire personnalisée pour affiner davantage les résultats de la recherche.
Dernier accès	Sélectionnez une plage horaire lors du dernier accès au fichier ou au répertoire (CIFS ou NFS uniquement). Vous pouvez également spécifier une plage horaire personnalisée pour affiner davantage les résultats de la recherche. Pour les types de fichiers analysés par le système de classification BlueXP, il s'agit de la dernière fois que le fichier a été analysé par le système de classification BlueXP. La classification BlueXP n'extrait pas l'heure du dernier accès des sources de données suivantes : SharePoint Online, SharePoint on-pretlocale (SharePoint Server), OneDrive, Google Drive et Amazon S3.

Filtrage des données par métadonnées

Utilisez les filtres suivants pour afficher les données en fonction de l'emplacement, de la taille et du répertoire ou du type de fichier.

Filtre	Détails
Chemin du fichier	Saisissez jusqu'à 20 chemins partiels ou complets que vous souhaitez inclure ou exclure de la requête. Si vous entrez à la fois les chemins d'inclusion et d'exclusion, la classification BlueXP recherche d'abord tous les fichiers des chemins inclus, puis supprime les fichiers des chemins exclus, puis affiche les résultats. Notez que l'utilisation de "*" dans ce filtre n'a aucun effet et que vous ne pouvez pas exclure des dossiers spécifiques de l'analyse - tous les répertoires et fichiers d'un partage configuré seront analysés.
Type de répertoire	Sélectionnez le type de répertoire : « partager » ou « dossier ».
Type de fichier	Sélectionner "types de fichiers".
Taille du fichier	Sélectionnez la plage de tailles de fichier.
Hachage de fichiers	Entrez le hachage du fichier pour trouver un fichier spécifique, même si le nom est différent.

Filtrer les données par type de stockage

Utilisez les filtres suivants pour afficher les données par type de stockage.

Filtre	Détails
Type d'environnement de travail	Sélectionnez le type d'environnement de travail. OneDrive, SharePoint et Google Drive sont classés dans « applications ».
Nom de l'environnement de travail	Sélectionner des environnements de travail spécifiques.
Référentiel de stockage	Sélectionnez le référentiel de stockage, par exemple un volume ou un schéma.

Filtrer les données par stratégies

Utilisez le filtre suivant pour afficher les données par stratégie.

Filtre	Détails
Stratégies	Sélectionnez une ou plusieurs stratégies. Aller "ici" pour afficher la liste des règles existantes et créer vos propres règles personnalisées.

Filtrez les données par état d'analyse

Utilisez le filtre suivant pour afficher les données en fonction de l'état d'analyse de classification BlueXP.

Filtre	Détails
État de l'analyse	Sélectionnez une option pour afficher la liste des fichiers en attente de première numérisation, terminés en cours de numérisation, en attente de numérisation ou qui n'ont pas pu être numérisés.
Événement d'analyse d'acquisition	Indiquez si vous souhaitez afficher les fichiers non classés car la classification BlueXP n'a pas pu rétablir l'heure du dernier accès ou les fichiers classés même si la classification BlueXP n'a pas pu rétablir l'heure du dernier accès.

"Voir les détails sur l'horodatage de la « dernière heure d'accès »" Pour plus d'informations sur les éléments qui apparaissent dans la page Investigation lors du filtrage à l'aide de l'événement Scan Analysis.

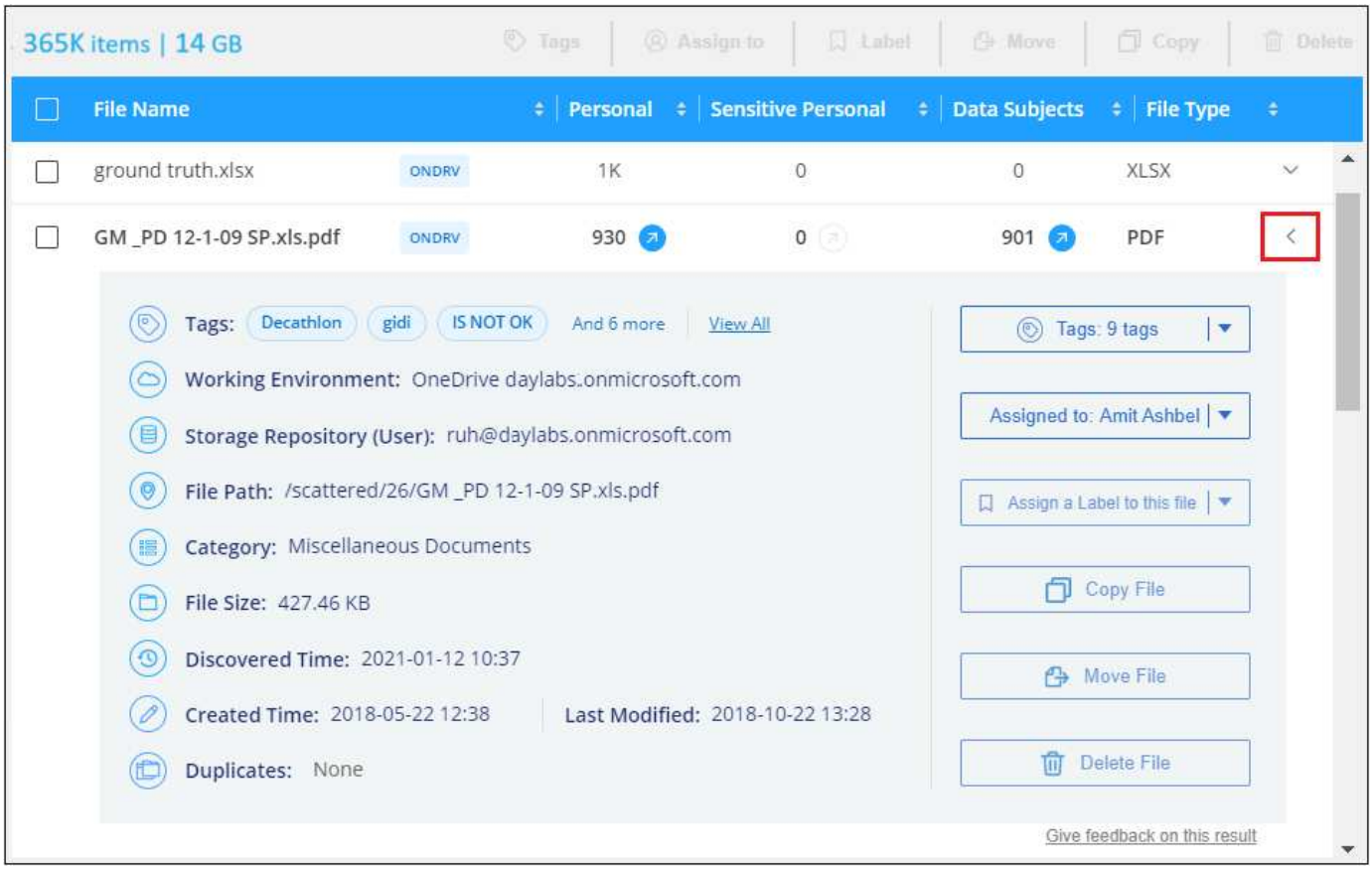
Filtrer les données par doublons

Utilisez le filtre suivant pour afficher les fichiers qui sont dupliqués dans votre espace de stockage.

Filtre	Détails
Doublons	Indiquez si le fichier est dupliqué dans les référentiels.

Afficher les métadonnées de fichier

Dans le volet Résultats de l'enquête de données, vous pouvez cliquer sur ⌄ pour afficher les métadonnées de fichier, quel qu'il soit.



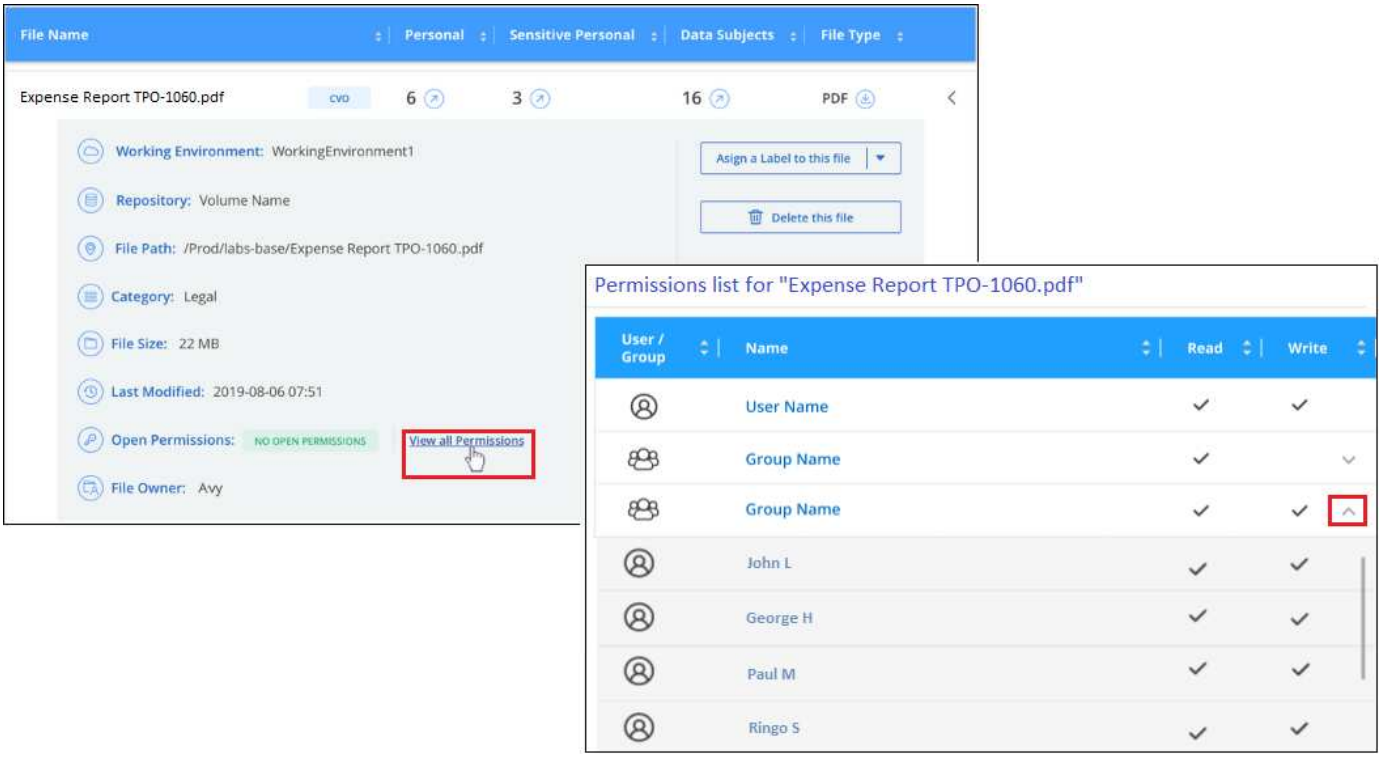
En plus de vous montrer l'environnement de travail et le volume où réside le fichier, les métadonnées affichent beaucoup plus d'informations, y compris les autorisations de fichier, le propriétaire du fichier, et s'il y a des doublons de ce fichier. Ces informations sont utiles si vous prévoyez de le faire "Créer des règles" car vous pouvez voir toutes les informations que vous pouvez utiliser pour filtrer vos données.

Notez que toutes les informations ne sont pas disponibles pour toutes les sources de données, ce qui est juste ce qui est approprié pour cette source de données. Par exemple, le nom du volume et les autorisations ne sont pas pertinents pour les fichiers de base de données.

Afficher les autorisations pour les fichiers et les répertoires

Pour afficher la liste de tous les utilisateurs ou groupes qui ont accès à un fichier ou à un répertoire, ainsi que les types d'autorisations dont ils disposent, cliquez sur **Afficher toutes les autorisations**. Ce bouton est uniquement disponible pour les données des partages CIFS.

Notez que si vous voyez des SID (identificateurs de sécurité) au lieu des noms d'utilisateur et de groupe, vous devez intégrer votre Active Directory dans la classification BlueXP. "Découvrez comment faire".



Vous pouvez cliquer sur ⌄ pour tous les groupes pour voir la liste des utilisateurs qui font partie du groupe.

En outre, Vous pouvez cliquer sur le nom d'un utilisateur ou d'un groupe et la page Investigation s'affiche avec le nom de cet utilisateur ou groupe renseigné dans le filtre "autorisations utilisateur/groupe" pour que vous puissiez voir tous les fichiers et répertoires auxquels l'utilisateur ou le groupe a accès.

Vérifiez la présence de fichiers en double dans vos systèmes de stockage

Vous pouvez afficher si des fichiers dupliqués sont stockés dans vos systèmes de stockage. Cette fonction s'avère utile pour identifier les domaines dans lesquels vous pouvez économiser de l'espace de stockage. Il peut également être utile de s'assurer que certains fichiers possédant des autorisations spécifiques ou des informations sensibles ne sont pas inutilement dupliqués dans vos systèmes de stockage.

Tous vos fichiers (à l'exception des bases de données) de 1 Mo ou plus, contenant des informations personnelles ou sensibles, sont comparés pour voir s'il y a des doublons. Vous pouvez utiliser les filtres de la page Investigation « taille du fichier » ainsi que « doublons » pour voir quels fichiers d'une certaine plage de tailles sont dupliqués dans votre environnement.

La classification BlueXP utilise la technologie de hachage pour déterminer les fichiers en double. Si un fichier a le même code de hachage qu'un autre fichier, nous pouvons être 100 % sûrs que les fichiers sont des doublons exacts, même si les noms de fichier sont différents.

Vous pouvez télécharger la liste des fichiers dupliqués et les envoyer à votre administrateur de stockage afin

qu'il puisse décider quels fichiers, le cas échéant, être supprimé. Ou vous le pouvez "supprimez le fichier" vous-même si vous êtes sûr qu'une version spécifique du fichier n'est pas nécessaire.

Afficher tous les fichiers dupliqués

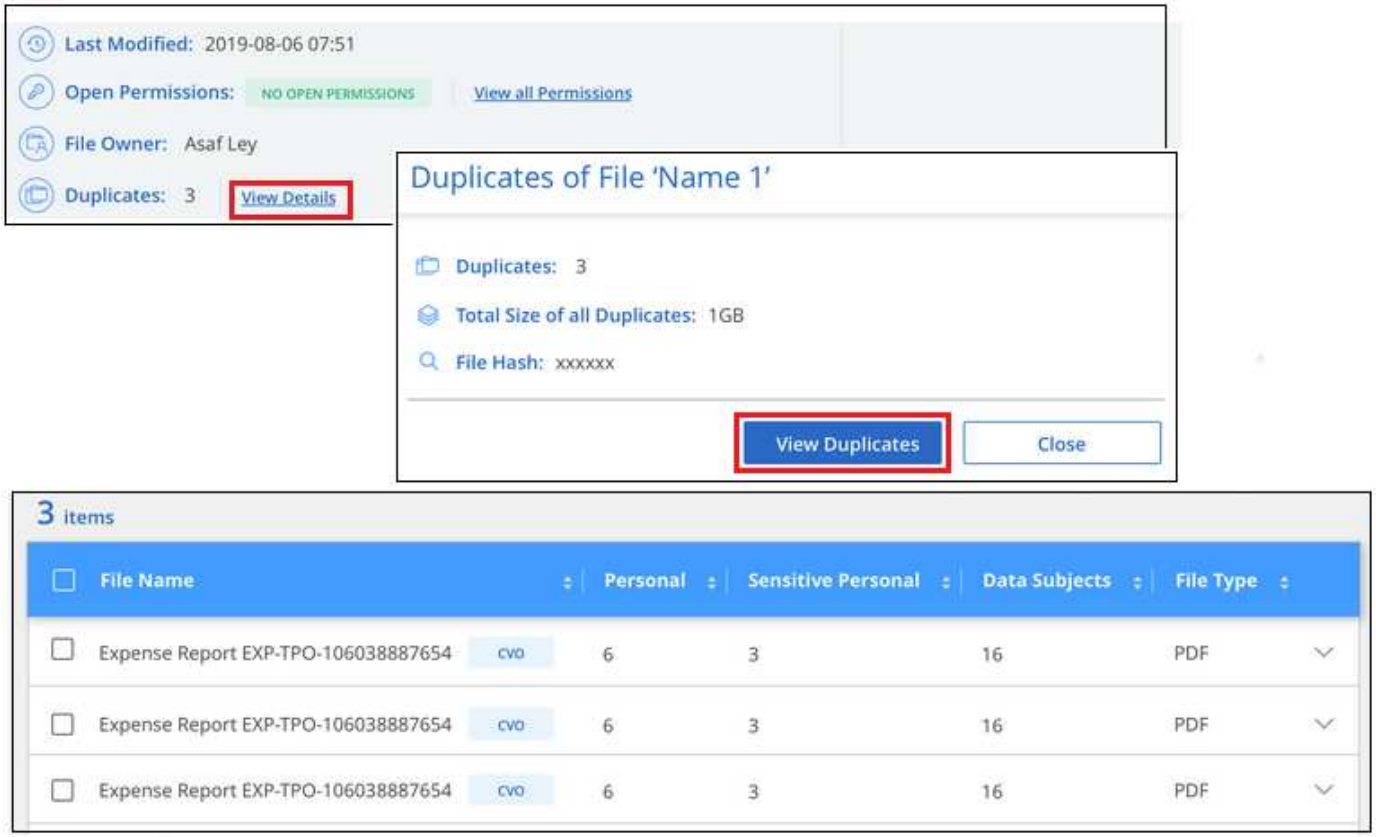
Si vous voulez une liste de tous les fichiers dupliqués dans les environnements de travail et les sources de données que vous scannez, vous pouvez utiliser le filtre **Duplicates > a des doublons** dans la page recherche de données.

Tous les fichiers dupliqués sont affichés dans la page Résultats.

Permet d'afficher si un fichier spécifique est dupliqué

Si vous souhaitez voir si un seul fichier contient des doublons, vous pouvez cliquer sur dans le volet Résultats de l'enquête de données ⌄ pour afficher les métadonnées de fichier, quel qu'il soit. Si un fichier est en double, ces informations apparaissent à côté du champ *Duplicates*.

Pour afficher la liste des fichiers dupliqués et leur emplacement, cliquez sur **Afficher les détails**. Dans la page suivante, cliquez sur **Afficher les doublons** pour afficher les fichiers de la page Investigation.



Vous pouvez utiliser la valeur de hachage de fichier fournie dans cette page et la saisir directement dans la page Investigation pour rechercher un fichier en double spécifique à tout moment, ou vous pouvez l'utiliser dans une police.

Rapport d'enquête de données

Le rapport d'enquête de données est un téléchargement du contenu filtré de la page d'enquête de données.

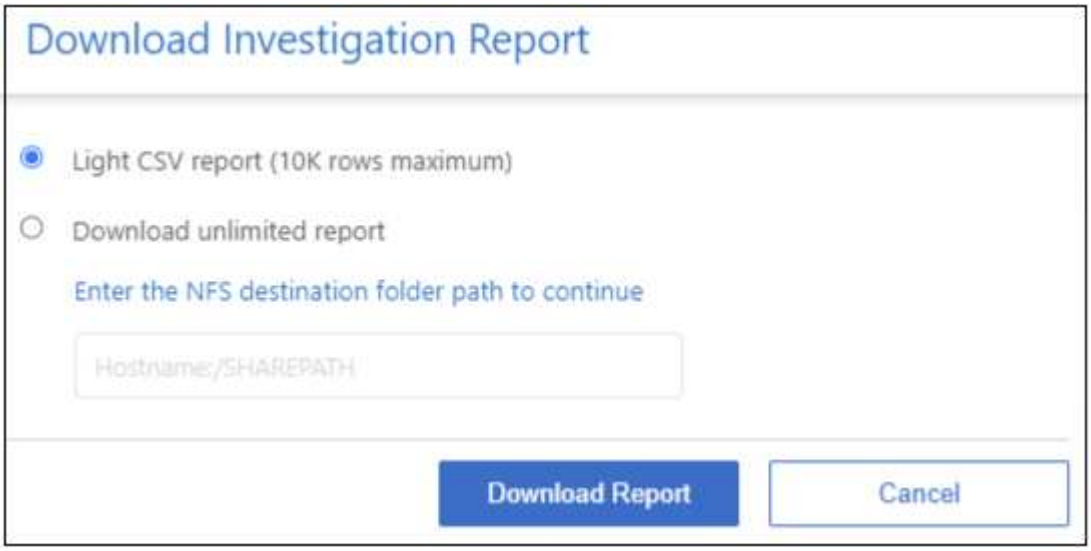
Le rapport est disponible sous la forme . Fichier CSV que vous pouvez enregistrer sur la machine locale.

Vous pouvez télécharger jusqu'à trois fichiers de rapport si la classification BlueXP analyse des fichiers (données non structurées), des répertoires (dossiers et partages de fichiers) et des bases de données (données structurées).

Générer le rapport d'investigation de données

Étapes

1. Dans la page Data Investigation, cliquez sur le bouton en haut à droite de la page.
2. Sélectionnez pour télécharger un . Rapport CSV des données, puis cliquez sur **Télécharger le rapport**.



Résultat

Une boîte de dialogue affiche un message indiquant que les rapports sont en cours de téléchargement.

Ce qui est inclus dans le rapport d'enquête sur les données

Le **non structuré fichier de données** contient les informations suivantes sur vos fichiers :

- Nom du fichier
- Type d'emplacement
- Nom de l'environnement de travail
- Référentiel de stockage (par exemple, un volume, un compartiment, des partages)
- Type de référentiel
- Chemin des fichiers
- Type de fichier
- Taille du fichier (en Mo)
- Heure de création
- Dernière modification
- Dernier accès
- Propriétaire du fichier

- Catégorie
- Informations personnelles
- Informations personnelles sensibles
- Ouvrez les autorisations
- Erreur d'analyse d'acquisition
- Date de détection de suppression

  Une date de détection de suppression identifie la date à laquelle le fichier a été supprimé ou déplacé. Cela vous permet d'identifier le moment où des fichiers sensibles ont été déplacés. Les fichiers supprimés ne font pas partie du nombre de fichiers qui s'affiche dans le tableau de bord ou sur la page Investigation. Les fichiers n'apparaissent que dans les rapports CSV.

Le **Rapport de données de répertoires non structurés** inclut les informations suivantes sur vos dossiers et partages de fichiers :

- Type d'environnement de travail
- Nom de l'environnement de travail
- Nom du répertoire
- Référentiel de stockage (par exemple, un dossier ou des partages de fichiers)
- Propriétaire du répertoire
- Heure de création
- Heure découverte
- Dernière modification
- Dernier accès
- Ouvrez les autorisations
- Type de répertoire

Le **Rapport de données structurées** comprend les informations suivantes sur vos tables de bases de données :

- NOM de la table DB
- Type d'emplacement
- Nom de l'environnement de travail
- Référentiel de stockage (par exemple, un schéma)
- Nombre de colonnes
- Nombre de lignes
- Informations personnelles
- Informations personnelles sensibles

Attribuez des règles à vos données

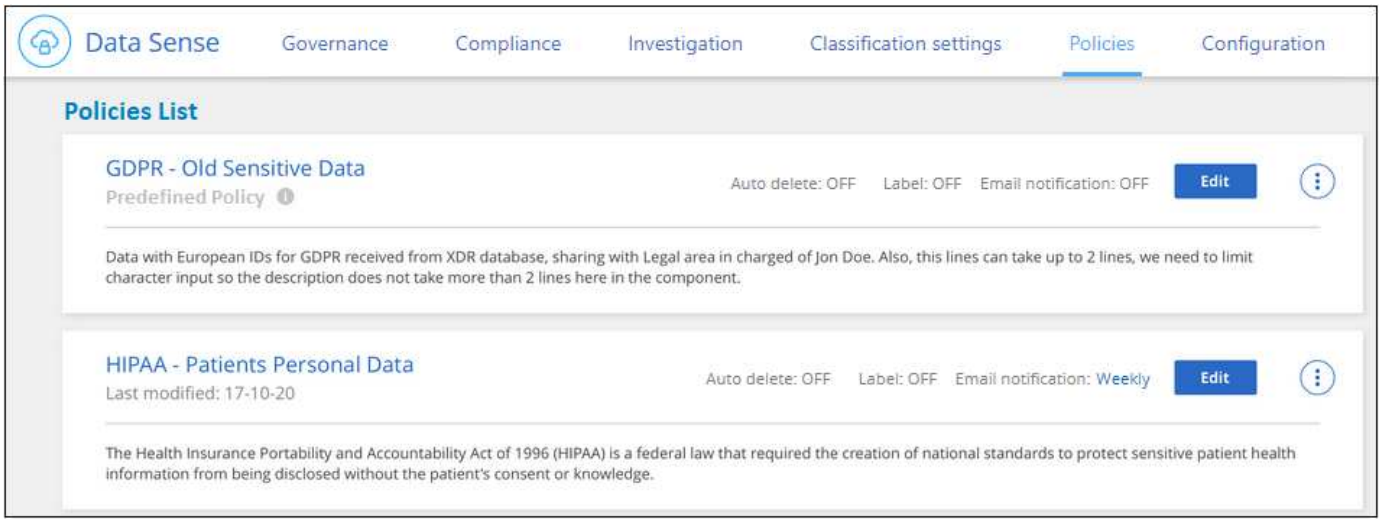
Les stratégies sont comme une liste de favoris de filtres personnalisés qui fournissent des résultats de recherche dans la page Investigation pour les requêtes de conformité les

plus fréquemment demandées. La classification BlueXP offre un ensemble de règles prédéfinies basées sur des demandes client courantes. Vous pouvez créer des stratégies personnalisées qui fournissent des résultats pour des recherches spécifiques à votre organisation.

Les règles offrent les fonctionnalités suivantes :

- Des règles prédéfinies De NetApp en fonction des demandes des utilisateurs
- Possibilité de créer vos propres règles personnalisées
- Lancez la page Investigation avec les résultats de vos polices en un seul clic

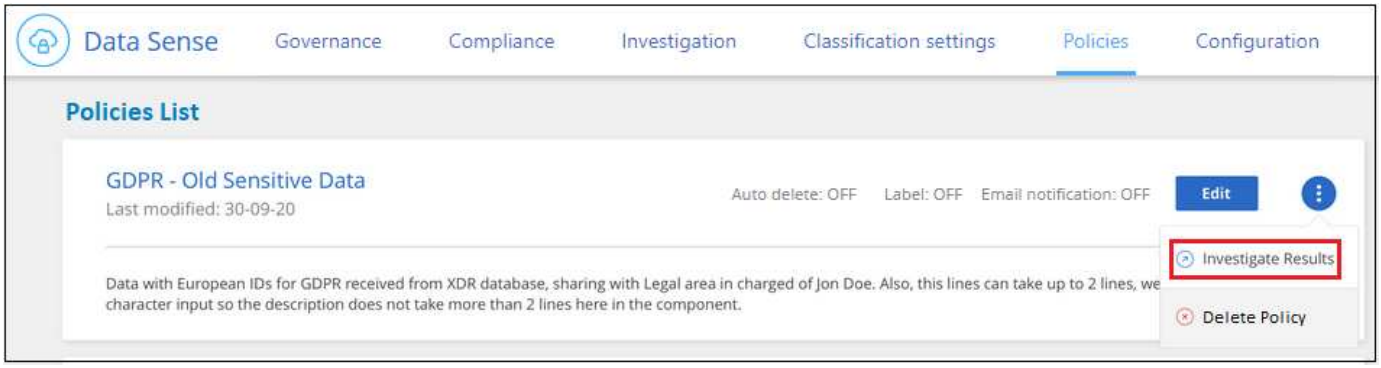
L'onglet **stratégies** du tableau de bord de conformité répertorie toutes les règles prédéfinies et personnalisées disponibles sur cette instance de classification BlueXP.



En outre, les stratégies apparaissent dans la liste des filtres de la page Investigation.

Afficher les résultats de la police dans la page Investigation

Pour afficher les résultats d'une stratégie dans la page Investigation, cliquez sur ⋮ Pour une stratégie spécifique, puis sélectionnez **examiner les résultats**.



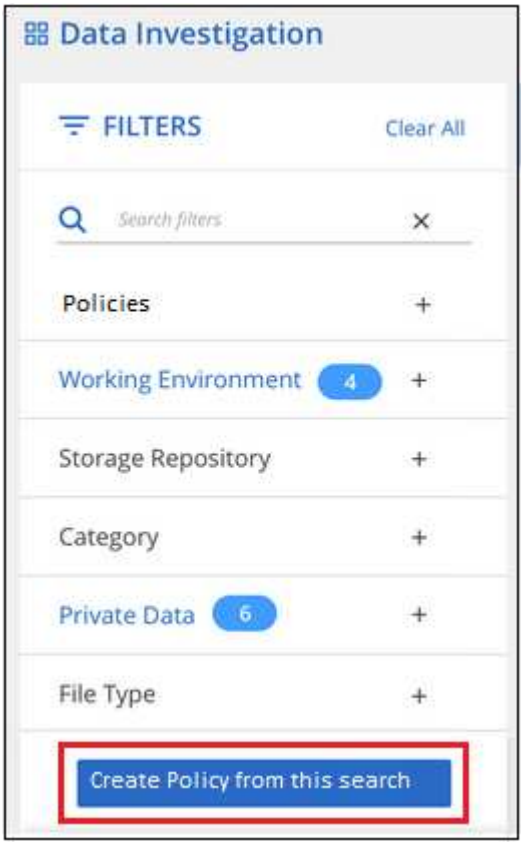
Création de règles personnalisées

Vous pouvez créer vos propres stratégies personnalisées qui fournissent des résultats pour les recherches

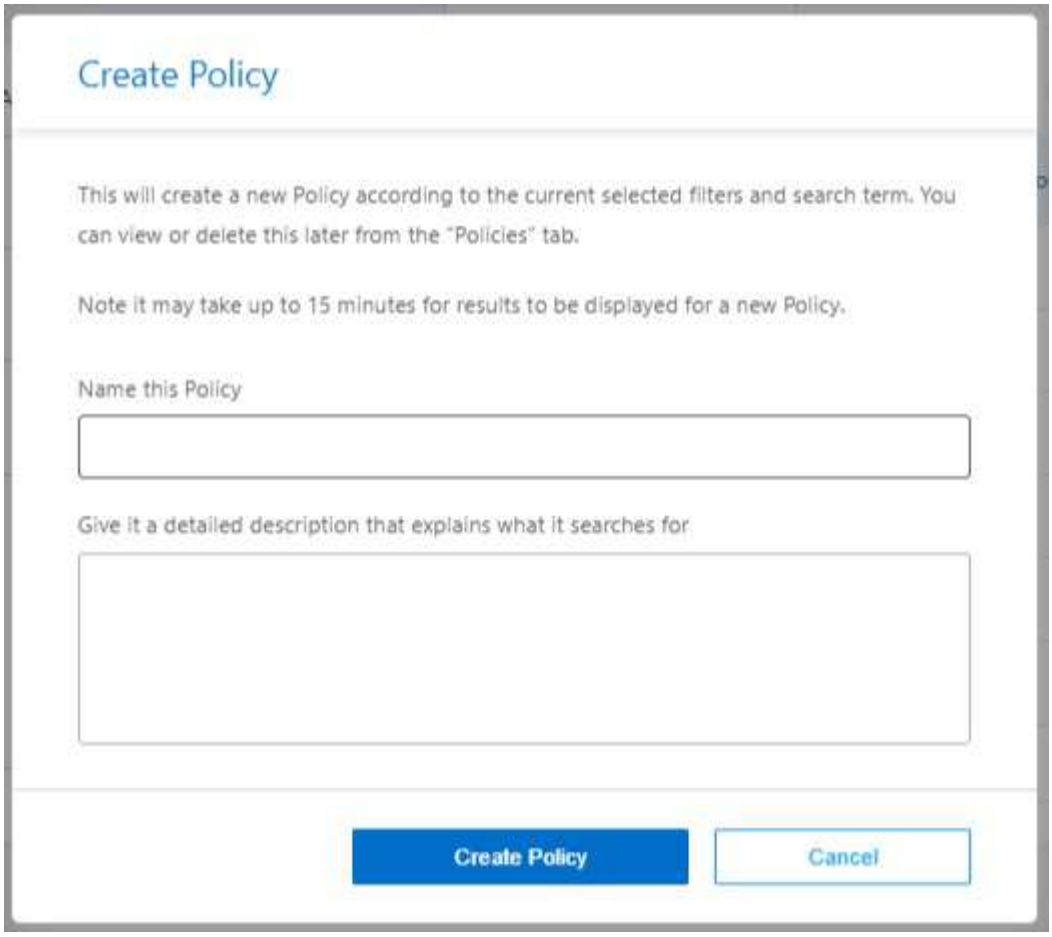
spécifiques à votre organisation. Les résultats sont renvoyés pour tous les fichiers et répertoires (partages et dossiers) qui correspondent aux critères de recherche.

Étapes

1. Dans la page recherche de données, définissez votre recherche en sélectionnant tous les filtres que vous souhaitez utiliser. Voir "Filtrage des données dans la page Data Investigation" pour plus d'informations.
2. Une fois que vous avez toutes les caractéristiques de filtre comme vous le souhaitez, cliquez sur **Créer une stratégie à partir de cette recherche**.



3. Nommez la règle et sélectionnez les autres actions pouvant être effectuées par la règle :
   a. Entrez un nom et une description uniques.
   b. Si vous le souhaitez, cochez la case pour supprimer automatiquement les fichiers correspondant aux paramètres de la stratégie.
   c. Cliquez sur **Créer une stratégie**.



Résultat

La nouvelle stratégie s'affiche dans l'onglet stratégies.

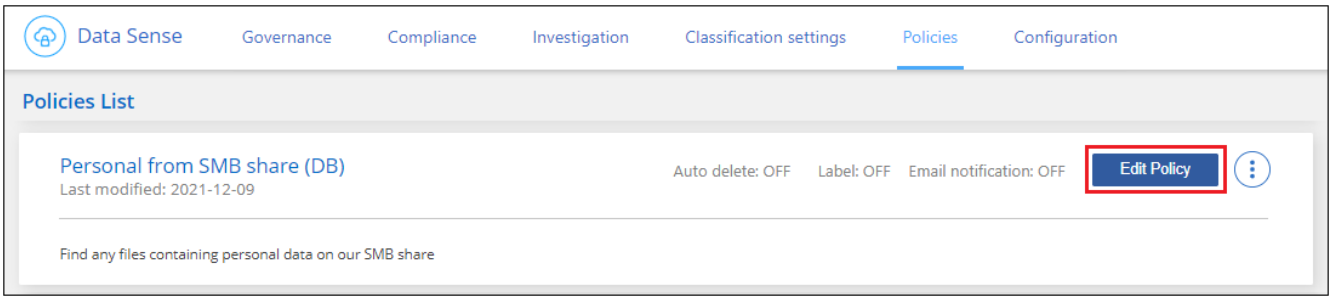
Modifier les règles

Vous pouvez modifier les critères d'une stratégie existante que vous avez déjà créée. Cela peut être particulièrement utile si vous souhaitez modifier la requête (les éléments que vous avez définis à l'aide de filtres) pour ajouter ou supprimer certains paramètres.

Pour les stratégies prédéfinies, vous pouvez uniquement modifier si les notifications par e-mail sont envoyées et si les étiquettes d'AIP sont ajoutées. Aucune autre valeur ne peut être modifiée.

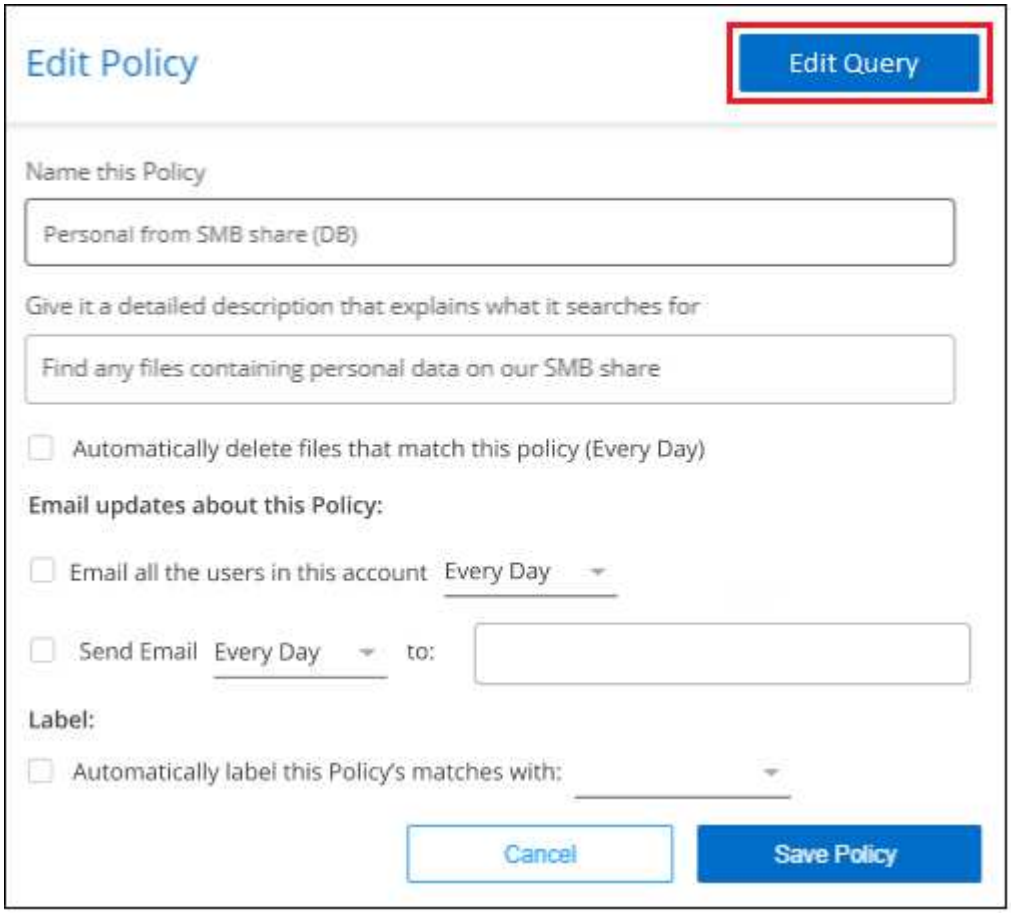
Étapes

1. Dans la page liste des stratégies, cliquez sur **Modifier** pour la stratégie que vous souhaitez modifier.

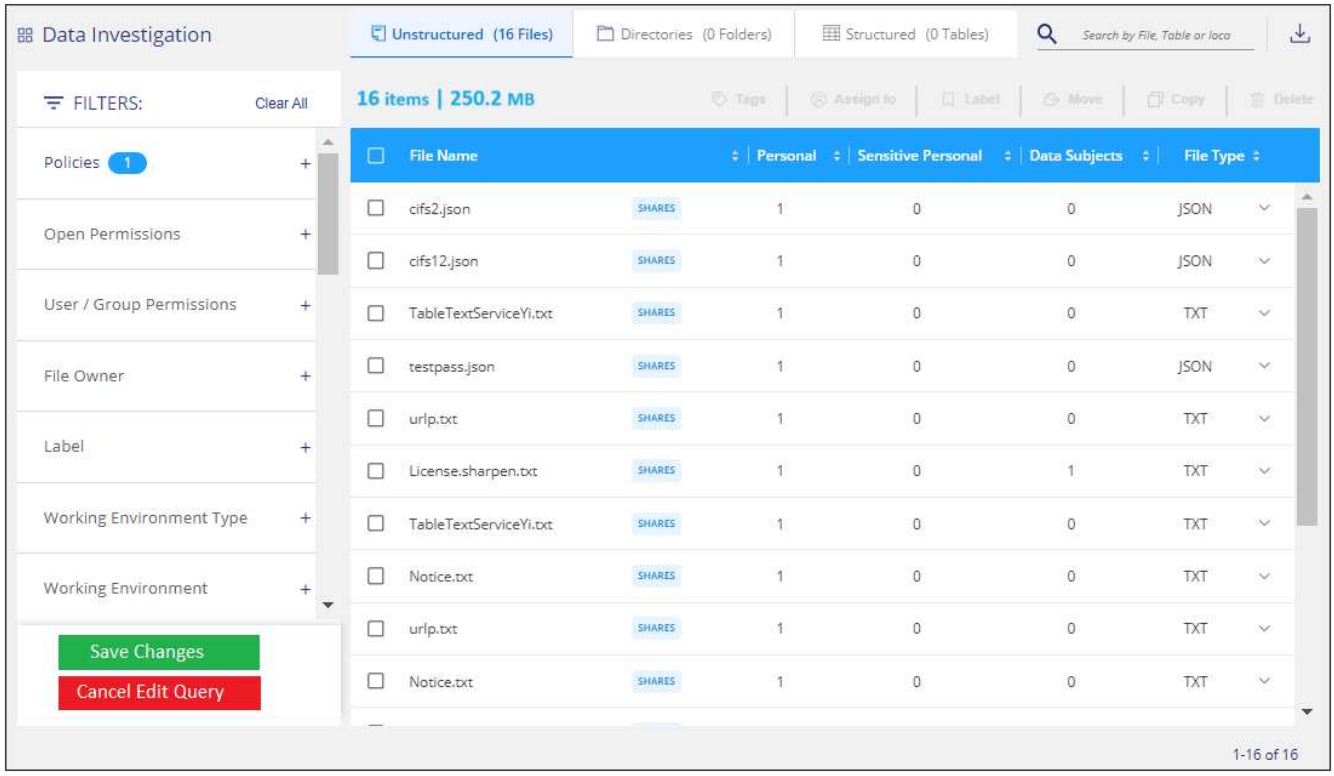


2. Si vous souhaitez simplement modifier les éléments de cette page (le Nom, la Description, si les notifications par e-mail sont envoyées et si des étiquettes AIP sont ajoutées), effectuez la modification et cliquez sur **Enregistrer la stratégie**.

   Si vous souhaitez modifier les filtres de la requête enregistrée, cliquez sur **Modifier la requête**.



3. Dans la page Investigation qui définit cette requête, modifiez la requête en ajoutant, supprimant ou personnalisant les filtres, puis cliquez sur **Enregistrer les modifications** .



Résultat

La police est modifiée immédiatement. Toutes les actions définies pour cette stratégie pour envoyer un e-mail, ajouter des étiquettes AIP ou supprimer des fichiers seront effectuées à l'interne suivant.

Supprimer des règles

Vous pouvez supprimer toute stratégie personnalisée que vous avez créée si vous n'en avez plus besoin. Vous ne pouvez pas supprimer les règles prédéfinies.

Pour supprimer une stratégie, cliquez sur ⋮ Pour une stratégie spécifique, cliquez sur **Supprimer la stratégie**, puis cliquez à nouveau sur **Supprimer la stratégie** dans la boîte de dialogue de confirmation.

Liste des règles prédéfinies

La classification BlueXP fournit les règles définies par le système suivantes :

Nom	Description	Logique
Les données privées ont déjà dépassé les 7 ans	Fichiers contenant des données personnelles ou sensibles, modifié pour la dernière fois il y a plus de 7 ans.	Fichiers contenant des données personnelles ou sensibles, modifié pour la dernière fois il y a plus de 7 ans
Noms des sujets de données - risque élevé	Fichiers avec plus de 50 noms de sujet de données.	Fichiers avec plus de 50 noms de sujet de données
Adresses e-mail - risque élevé	Fichiers contenant plus de 50 adresses électroniques ou colonnes DB contenant plus de 50 % de leurs lignes contenant des adresses électroniques	Fichiers contenant plus de 50 adresses électroniques ou colonnes DB contenant plus de 50 % de leurs lignes contenant des adresses électroniques

Nom	Description	Logique
Données personnelles - risque élevé	Fichiers contenant plus de 20 identificateurs de données personnelles, ou colonnes de bases de données contenant plus de 50 % de leurs lignes contenant des identificateurs de données personnelles.	Fichiers avec plus de 20 colonnes personnelles ou DB avec plus de 50 % de leurs lignes contenant des colonnes personnelles
Données personnelles sensibles - risque élevé	Fichiers contenant plus de 20 identificateurs de données personnelles sensibles, ou colonnes de bases de données contenant plus de 50 % de leurs lignes contenant des données personnelles sensibles.	Les fichiers contenant plus de 20 colonnes personnelles sensibles ou DB contenant plus de 50 % de leurs lignes contenant des données personnelles sensibles

Afficher les rapports de conformité

La classification BlueXP fournit des rapports qui vous permettent de mieux comprendre l'état du programme de confidentialité des données de votre entreprise.

Par défaut, les tableaux de bord de classification BlueXP affichent les données de conformité et de gouvernance pour tous les environnements de travail, bases de données et sources de données. Si vous souhaitez afficher des rapports contenant des données pour certains environnements de travail uniquement, sélectionnez ces environnements de travail.

- Les rapports décrits dans cette section ne sont disponibles que si vous avez choisi d'effectuer une analyse de classification complète sur vos sources de données. Les sources de données qui ont une acquisition avec mappage uniquement peuvent uniquement générer le rapport de mappage de données.
- NetApp ne peut pas garantir l'exactitude à 100 % des données personnelles et des données personnelles sensibles identifiées par la classification BlueXP. Vous devez toujours valider les informations en examinant les données.

Rapport d'évaluation des risques pour la confidentialité

Le rapport d'évaluation des risques pour la confidentialité fournit une vue d'ensemble de l'état des risques pour la confidentialité de votre entreprise, conformément aux réglementations en matière de confidentialité, telles que le Règlement général de l'Union européenne sur la protection des données et la loi CCPA. Le rapport contient les informations suivantes :

Statut de conformité

A indice de gravité et la distribution des données, qu'elles soient non sensibles, personnelles ou sensibles.

Présentation de l'évaluation

Une ventilation des types de données personnelles ainsi que des catégories de données.

Sujets de données dans cette évaluation

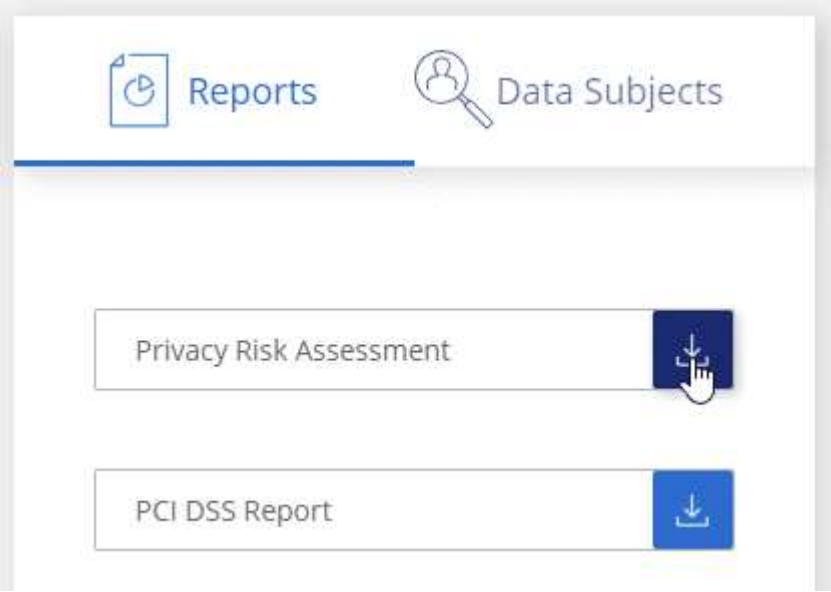
Nombre de personnes, par lieu, pour lesquelles des identificateurs nationaux ont été trouvés.

Générez le rapport d'évaluation des risques en matière de confidentialité

Accédez à l'onglet conformité pour générer le rapport.

Étapes

1. Dans le menu BlueXP, cliquez sur **gouvernance > Classification**.
2. Cliquez sur **conformité**, puis cliquez sur l'icône de téléchargement en regard de **évaluation des risques de confidentialité** sous **Rapports**.



Résultat

La classification BlueXP génère un rapport PDF que vous pouvez examiner et envoyer à d'autres groupes selon les besoins.

Indice de gravité

La classification BlueXP calcule l'indice de gravité du rapport d'évaluation des risques en matière de confidentialité sur la base de trois variables :

- Pourcentage de données personnelles sur toutes les données.
- Le pourcentage de données personnelles sensibles hors de toutes les données.
- Le pourcentage de fichiers qui incluent des sujets de données, déterminé par des identificateurs nationaux tels que les ID nationaux, les numéros de sécurité sociale et les numéros d'identification fiscale.

La logique utilisée pour déterminer le score est la suivante :

Indice de gravité	Logique
0	Les trois variables sont exactement 0 %
1	L'une des variables est supérieure à 0 %
2	L'une des variables est supérieure à 3 %
3	Deux des variables sont supérieures à 3 %
4	Trois des variables sont supérieures à 3 %

Indice de gravité	Logique
5	L'une des variables est supérieure à 6 %
6	Deux des variables sont supérieures à 6 %
7	Trois des variables sont supérieures à 6 %
8	L'une des variables est supérieure à 15 %
9	Deux des variables sont supérieures à 15 %
10	Trois des variables sont supérieures à 15 %

Rapport PCI DSS

Le rapport PCI DSS (Payment Card Industry Data Security Standard) peut vous aider à identifier la distribution des informations de carte de crédit dans vos dossiers. Le rapport contient les informations suivantes :

Présentation

Combien de fichiers contiennent des informations de carte de crédit et dans quels environnements de travail.

Le cryptage

Le pourcentage de fichiers contenant des informations de carte de crédit sur des environnements de travail cryptés ou non cryptés. Ces informations sont spécifiques à Cloud Volumes ONTAP.

Protection contre les ransomwares

Le pourcentage de fichiers contenant des informations de carte de crédit sur des environnements de travail où la protection par ransomware est activée ou non. Ces informations sont spécifiques à Cloud Volumes ONTAP.

La conservation

Délai de la dernière modification des fichiers. Ceci est utile car vous ne devez pas conserver les informations de carte de crédit plus longtemps que vous n'avez besoin de les traiter.

Distribution des informations de carte de crédit

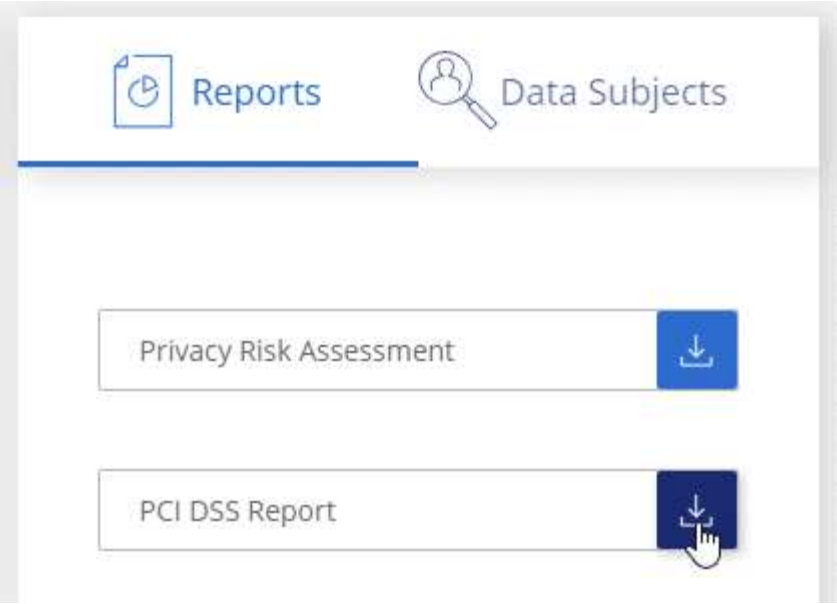
Les environnements de travail où les informations de carte de crédit ont été trouvées et où le chiffrement et la protection contre les ransomwares sont activés.

Générez le rapport PCI DSS

Accédez à l'onglet conformité pour générer le rapport.

Étapes

1. Dans le menu BlueXP, cliquez sur **gouvernance > Classification**.
2. Cliquez sur **Compliance**, puis sur l'icône de téléchargement en regard de **PCI DSS Report** sous **Reports**.



Résultat

La classification BlueXP génère un rapport PDF que vous pouvez examiner et envoyer à d'autres groupes selon les besoins.

Rapport HIPAA

Le rapport HIPAA (Health Insurance Portability and Accountability Act) peut vous aider à identifier les fichiers contenant des informations sur la santé. Il est conçu pour aider votre organisation à respecter les lois HIPAA en matière de confidentialité des données. Voici les informations que recherche la classification BlueXP :

- Modèle de référence de santé
- Code médical ICD-10-cm
- Code médical ICD-9-cm
- RH - Catégorie Santé
- Catégorie données d'application de santé

Le rapport contient les informations suivantes :

Présentation

Combien de fichiers contiennent des informations sur l'état de santé et dans quels environnements de travail.

Le cryptage

Le pourcentage de fichiers contenant des informations de santé sur des environnements de travail chiffrés ou non cryptés. Ces informations sont spécifiques à Cloud Volumes ONTAP.

Protection contre les ransomwares

Le pourcentage de fichiers contenant des informations d'état sur des environnements de travail qui n'ont pas ou qui sont sur lesquels une protection par ransomware est activée. Ces informations sont spécifiques à Cloud Volumes ONTAP.

La conservation

Délai de la dernière modification des fichiers. Ceci est utile parce que vous ne devez pas conserver les renseignements sur la santé plus longtemps que vous n'avez besoin de les traiter.

Distribution des renseignements sur la santé

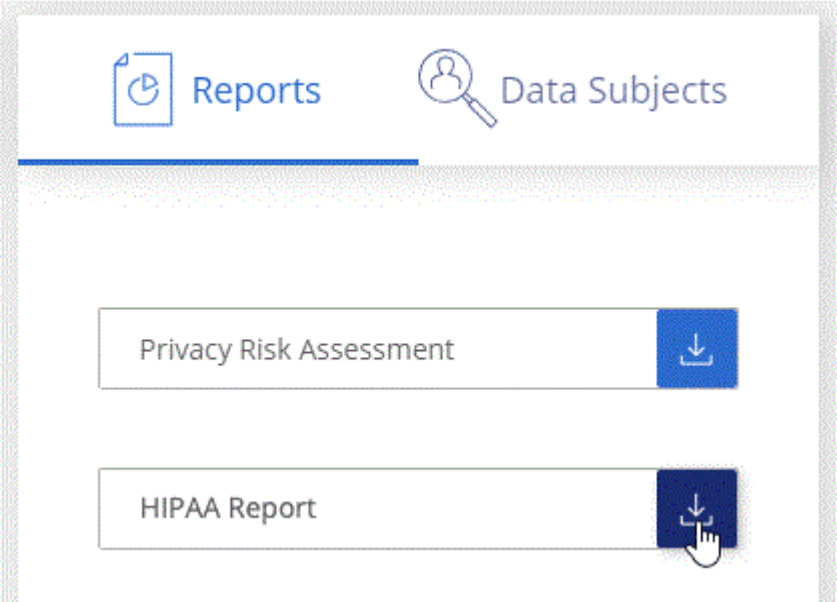
Les environnements de travail dans lesquels les informations de santé ont été trouvées et si le chiffrement et la protection par ransomware sont activés.

Générez le rapport HIPAA

Accédez à l'onglet conformité pour générer le rapport.

Étapes

1. Dans le menu BlueXP, cliquez sur **gouvernance > Classification**.
2. Cliquez sur **conformité**, puis cliquez sur l'icône de téléchargement en regard de **Rapport HIPAA** sous **Rapports**.



Résultat

La classification BlueXP génère un rapport PDF que vous pouvez examiner et envoyer à d'autres groupes selon les besoins.

Qu'est-ce qu'une demande d'accès aux données ?

Les réglementations en matière de confidentialité, telles que le RGPD européen, accordent à des sujets de données (clients ou employés, par exemple) le droit d'accéder à leurs données personnelles. Lorsqu'un sujet de données demande cette information, elle est appelée DSAR (Data Subject Access request). Les organisations sont tenues de répondre à ces demandes "sans délai excessif" et au plus tard dans un mois suivant la réception.

Vous pouvez répondre à un DSAR en recherchant le nom complet ou l'identifiant connu d'un sujet (par exemple une adresse e-mail), puis en téléchargeant un rapport. Ce rapport est conçu pour aider votre entreprise à respecter le RGPD ou les autres lois similaires sur la confidentialité des données.

Comment la classification BlueXP peut-elle vous aider à répondre à un DSAR ?

Lorsque vous effectuez une recherche relative à une personne concernée, le système de classification BlueXP trouve tous les fichiers, compartiments, OneDrive et comptes SharePoint contenant le nom ou l'identifiant de cette personne. La classification BlueXP vérifie le nom ou l'identifiant des données pré-indexées les plus récentes. Il ne lance pas de nouvelle acquisition.

Une fois la recherche terminée, vous pouvez télécharger la liste des fichiers d'un rapport de demande d'accès aux données. Le rapport rassemble les informations issues des données et les place en termes juridiques que vous pouvez renvoyer à la personne.

> La recherche de sujet de données n'est pas prise en charge actuellement dans les bases de données.

Rechercher des sujets de données et télécharger des rapports

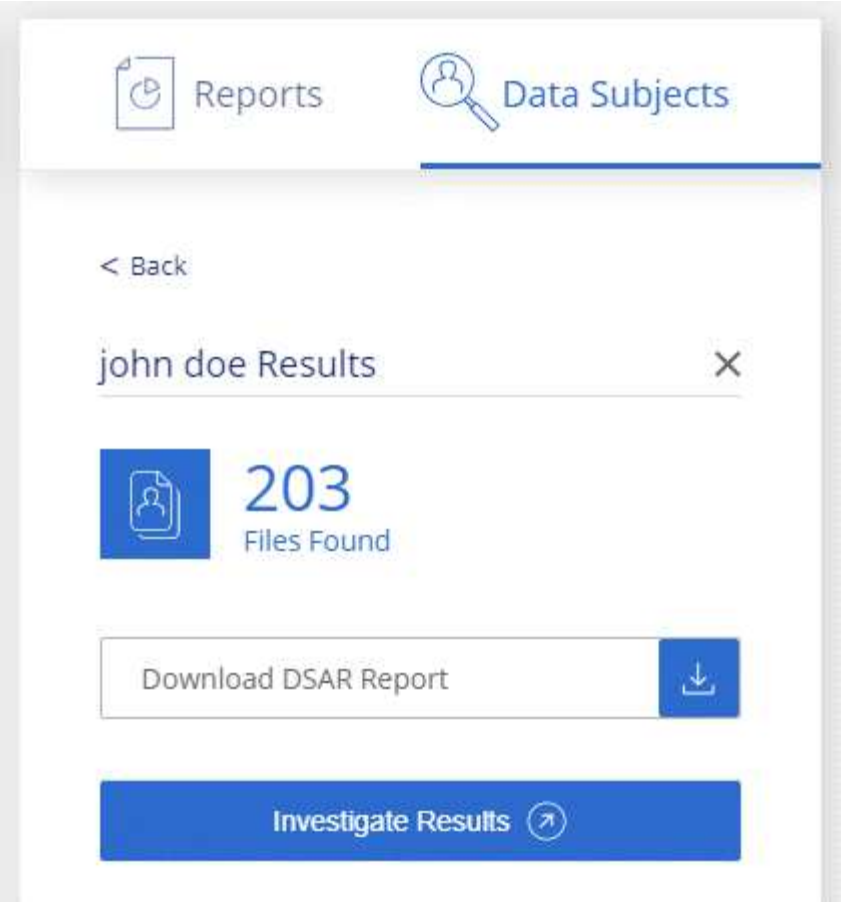
Recherchez le nom complet ou l'identifiant connu du sujet de données, puis téléchargez un rapport de liste de fichiers ou un rapport DSAR. Vous pouvez effectuer une recherche par "tout type d'informations personnelles".

> L'anglais, l'allemand, le japonais et l'espagnol sont pris en charge lors de la recherche des noms des sujets de données. La prise en charge d'autres langues sera ajoutée ultérieurement.

Étapes

1. Dans le menu BlueXP, cliquez sur **gouvernance > Classification**.
2. Cliquez sur **sujets de données**.
3. Recherchez le nom complet ou l'identifiant connu du sujet de données.

   Voici un exemple qui montre une recherche du nom *john Doe*:



4. Choisissez l'une des options disponibles :
   - **Télécharger le rapport DSAR** : réponse officielle à la demande d'accès que vous pouvez envoyer au sujet des données. Ce rapport contient des informations générées automatiquement en fonction des données classées par BlueXP situées sur l'objet des données et qui sont conçues pour être utilisées comme modèle. Vous devez remplir le formulaire et le revoir en interne avant de l'envoyer au sujet des données.
   - **Étudier les résultats** : une page qui vous permet d'examiner les données en recherchant, en triant, en développant les détails d'un fichier spécifique et en téléchargeant la liste de fichiers.

     S'il y a plus de 10,000 résultats, seuls les 10,000 premiers apparaissent dans la liste de fichiers.

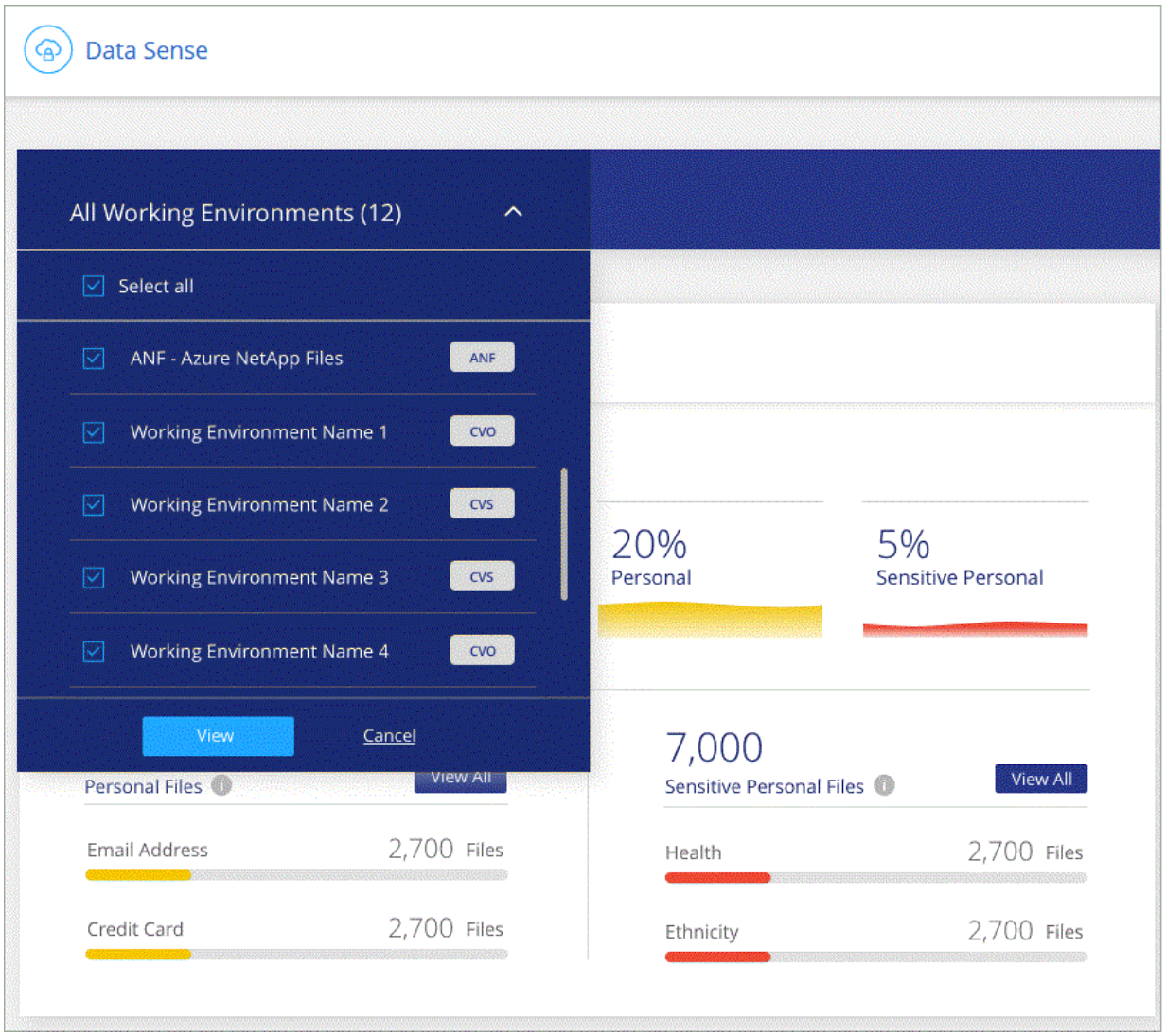
Sélectionnez les environnements de travail pour les rapports

Vous pouvez filtrer le contenu du tableau de bord BlueXP Classification Compliance pour afficher les données de conformité pour tous les environnements de travail et bases de données, ou pour seulement des environnements de travail spécifiques.

Lorsque vous filtrez le tableau de bord, la classification BlueXP évalue les données et les rapports de conformité pour les environnements de travail que vous avez sélectionnés.

Étapes

1. Cliquez sur la liste déroulante du filtre, sélectionnez les environnements de travail pour lesquels vous souhaitez afficher les données, puis cliquez sur **Afficher**.


Data Sense
All Working Environments (12)
Select all
ANF - Azure NetApp Files
ANF
Working Environment Name 1
CVO
Working Environment Name 2
CVS
Working Environment Name 3
CVS
Working Environment Name 4
CVO
View
Cancel
20%
Personal
5%
Sensitive Personal
Personal Files
View All
Email Address
2,700 Files
Credit Card
2,700 Files
7,000
Sensitive Personal Files
View All
Health
2,700 Files
Ethnicity
2,700 Files

Gérer la classification BlueXP

Excluez des répertoires spécifiques des analyses de classification BlueXP

Si vous souhaitez que la classification BlueXP exclut les données d'analyse qui résident dans certains répertoires de sources de données, vous pouvez ajouter ces noms de répertoires à un fichier de configuration. Une fois cette modification appliquée, le moteur de classification BlueXP exclut les données d'analyse de ces répertoires.

Notez que la classification BlueXP est configurée par défaut pour exclure les données de snapshot du volume d'analyse car ce contenu est identique au contenu du volume.

Cette fonctionnalité est disponible dans la classification BlueXP version 1.29 et supérieure (à partir de mars 2024).

Sources de données prises en charge

L'exclusion de répertoires spécifiques des analyses de classification BlueXP est prise en charge pour les partages NFS et CIFS dans les sources de données suivantes :

- ONTAP sur site
- Cloud Volumes ONTAP
- Amazon FSX pour NetApp ONTAP
- Azure NetApp Files
- Partages de fichiers généraux

Définissez les répertoires à exclure de l'analyse

Avant de pouvoir exclure des répertoires de l'analyse de classification, vous devez vous connecter au système de classification BlueXP pour pouvoir modifier un fichier de configuration et exécuter un script. Découvrez comment "Connectez-vous au système de classification BlueXP" Selon que vous avez installé le logiciel manuellement sur une machine Linux ou si vous avez déployé l'instance dans le cloud.

- Vous pouvez exclure un maximum de 50 chemins de répertoire par système de classification BlueXP.
- L'exclusion des chemins de répertoire peut affecter les temps de numérisation.

Étapes

1. Sur le système de classification BlueXP, accédez à «/opt/netapp/config/custom_configuration » et ouvrez le fichier `data_provider.yaml`.
2. Dans la section "Data_providers", sous la ligne "exclude:", entrez les chemins d'accès au répertoire à exclure. Par exemple :

```
exclude:
- "folder1"
- "folder2"
```

Ne modifiez rien d'autre dans ce fichier.

3. Enregistrez les modifications apportées au fichier.
4. Accédez à « /opt/netapp/Datasense/Tools/customer_configuration/Data_providers » et exécutez le script suivant :

```
update_data_providers_from_config_file.sh
```

Cette commande valide les répertoires à exclure de l'analyse vers le moteur de classification.

Résultat

Toutes les analyses ultérieures de vos données excluront l'analyse des répertoires spécifiés.

Vous pouvez ajouter, modifier ou supprimer des éléments de la liste d'exclusion en suivant ces mêmes étapes. La liste d'exclusion révisée sera mise à jour après l'exécution du script pour valider vos modifications.

Exemples

Configuration 1 :

Chaque dossier contenant « folder1 » n'importe où dans le nom sera exclu de toutes les sources de données.

```
data_providers:
   exclude:
   - "folder1"
```

Résultats attendus pour les chemins qui seront exclus :

- /CVO1/folder1
- /CVO1/folder1name
- /CVO1/folder10
- /CVO1/*folder1
- /CVO1/+folder1name
- /CVO1/notfolder10
- /CVO22/folder1
- /CVO22/folder1name
- /CVO22/folder10

Exemples de chemins qui ne seront pas exclus :

- /CVO1/*dossier

- /CVO1/foldername
- /CVO22/*folder20

Configuration 2 :

Chaque dossier qui contient "*folder1" seulement au début du nom sera exclu.

```
data_providers:
   exclude:
   - "\\*folder1"
```

Résultats attendus pour les chemins qui seront exclus :

- /CVO/*folder1
- /CVO/*folder1name
- /CVO/*folder10

Exemples de chemins qui ne seront pas exclus :

- /CVO/folder1
- /CVO/folder1name
- /CVO/NOT*folder10

Configuration 3 :

Tous les dossiers de la source de données "CVO22" qui contiennent "folder1" n'importe où dans le nom seront exclus.

```
data_providers:
   exclude:
   - "CVO22/folder1"
```

Résultats attendus pour les chemins qui seront exclus :

- /CVO22/folder1
- /CVO22/folder1name
- /CVO22/folder10

Exemples de chemins qui ne seront pas exclus :

- /CVO1/folder1
- /CVO1/folder1name
- /CVO1/folder10

Des caractères spéciaux s'échappant dans les noms de dossier

Si vous avez un nom de dossier contenant l'un des caractères spéciaux suivants et que vous souhaitez exclure les données de ce dossier de l'analyse, vous devez utiliser la séquence d'échappement \\ avant le nom du dossier.

```
 ., +, *, ?, ^, $, (, ), [, ], {, }, |
Par exemple :
```

Chemin dans la source : `/project/*not_to_scan`

Syntaxe dans le fichier d'exclusion : `"\\*not_to_scan"`

Afficher la liste d'exclusion actuelle

Il est possible pour le contenu du `data_provider.yaml` le fichier de configuration doit être différent de ce qui a été réellement validé après l'exécution du `update_data_providers_from_config_file.sh` script. Pour afficher la liste actuelle des répertoires que vous avez exclus de l'analyse de classification BlueXP, exécutez la commande suivante depuis « /opt/netapp/Datase/Tools/customer_configuration/data_providers » :

```
get_data_providers_configuration.sh
```

Définissez des ID de groupe supplémentaires comme ouverts à l'organisation

Lorsque des ID de groupe (GID) sont attachés à des fichiers ou dossiers dans des partages de fichiers NFS, ils définissent les autorisations pour le fichier ou le dossier, par exemple s'ils sont « ouverts à l'organisation ». Si certains ID de groupe (GID) ne sont pas initialement configurés avec le niveau d'autorisation « Ouvrir à l'organisation », vous pouvez ajouter cette autorisation au GID pour que tous les fichiers et dossiers auxquels ce GID est rattaché soient considérés comme « ouverts à l'organisation ».

Après avoir effectué cette modification et que la classification BlueXP analyse à nouveau vos fichiers et dossiers, tous les fichiers et dossiers auxquels ces ID de groupe sont associés affichent cette autorisation dans la page Détails de l'investigation et ils apparaissent également dans les rapports où vous affichez les autorisations de fichier.

Pour activer cette fonctionnalité, vous devez vous connecter au système de classification BlueXP afin de modifier un fichier de configuration et d'exécuter un script. Découvrez comment "Connectez-vous au système de classification BlueXP" Selon que vous avez installé le logiciel manuellement sur une machine Linux ou si vous avez déployé l'instance dans le cloud.

Ajoutez l'autorisation « Ouvrir à l'organisation » aux ID de groupe

Vous devez disposer des numéros d'ID de groupe (GID) avant de commencer cette tâche.

Étapes

1. Sur le système de classification BlueXP, accédez à «/opt/netapp/config/custom_configuration » et ouvrez le fichier `data_provider.yaml`.
2. Dans la ligne « id_groupe_organisation : [] », ajoutez les ID de groupe. Par exemple :

```
organization_group_ids: [1014, 1015, 21, 2021, 1013, 2020, 1018, 1019]
```

Ne modifiez rien d'autre dans ce fichier.

3. Enregistrez les modifications apportées au fichier.
4. Accédez à « /opt/netapp/Datasense/Tools/customer_configuration/Data_providers » et exécutez le script suivant :

```
update_data_providers_from_config_file.sh
```

Cette commande valide les autorisations d'ID de groupe révisées au moteur de classification.

Résultat

Toutes les analyses ultérieures de vos données permettront d'identifier les fichiers ou dossiers auxquels ces ID de groupe sont associés comme « ouverts à l'organisation ».

Vous pouvez modifier la liste des ID de groupe et supprimer les ID de groupe que vous avez ajoutés par le passé en procédant de la même manière. La liste révisée des ID de groupe sera mise à jour après l'exécution du script pour valider vos modifications.

Afficher la liste actuelle des ID de groupe

Il est possible pour le contenu du `data_provider.yaml` le fichier de configuration doit être différent de ce qui a été réellement validé après l'exécution du `update_data_providers_from_config_file.sh` script. Pour afficher la liste actuelle des ID de groupe que vous avez ajoutés à la classification BlueXP, exécutez la commande suivante depuis « /opt/netapp/Datase/Tools/customer_configuration/data_providers » :

```
get_data_providers_configuration.sh
```

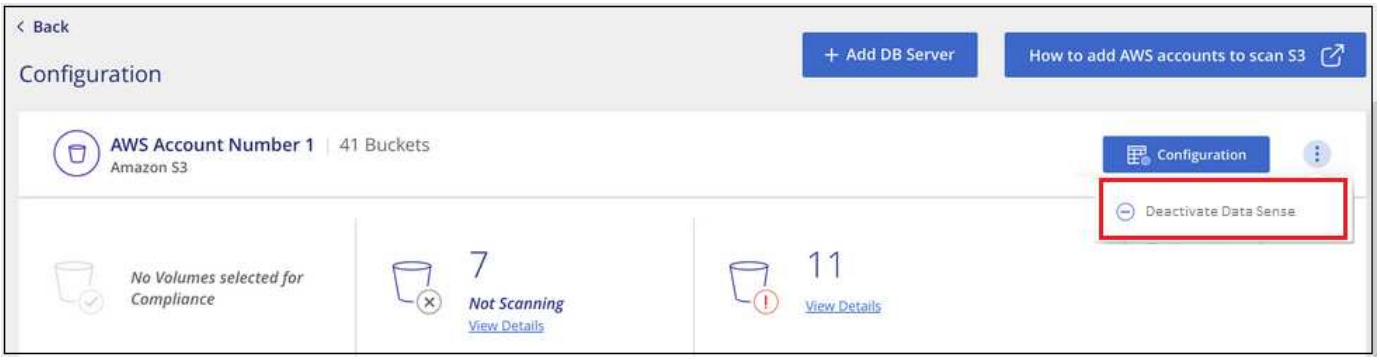
Supprimez les sources de données de la classification BlueXP

Si nécessaire, vous pouvez empêcher la classification BlueXP d'analyser un ou plusieurs environnements de travail, bases de données ou groupes de partage de fichiers.

Désactiver les analyses de conformité pour un environnement de travail

Lorsque vous désactivez des analyses, la classification BlueXP ne analyse plus les données de l'environnement de travail et supprime les informations de conformité indexées de l'instance de classification BlueXP (les données de l'environnement de travail lui-même ne sont pas supprimées).

1. Dans la page *Configuration*, cliquez sur Dans la ligne de l'environnement de travail, puis cliquez sur **Désactiver la détection de données**.



Vous pouvez également désactiver les analyses de conformité pour un environnement de travail à partir du panneau Services lorsque vous sélectionnez l'environnement de travail.

Supprimez une base de données de la classification BlueXP

Si vous ne souhaitez plus analyser une base de données, vous pouvez la supprimer de l'interface de classification BlueXP et arrêter toutes les analyses.

1. Dans la page *Configuration*, cliquez sur Dans la ligne de la base de données, puis cliquez sur **Supprimer serveur DB**.

Supprimez un groupe de partages de fichiers de la classification BlueXP

Si vous ne souhaitez plus analyser les fichiers utilisateur à partir d'un groupe de partages de fichiers, vous pouvez supprimer le groupe de partages de fichiers de l'interface de classification BlueXP et arrêter toutes les analyses.

Étapes

1. Dans la page *Configuration*, cliquez sur Dans la ligne du groupe de partages de fichiers, puis cliquez sur **Supprimer le groupe de partages de fichiers**.

2. Cliquez sur **Supprimer le groupe de partages** dans la boîte de dialogue de confirmation.

Désinstallation de la classification BlueXP

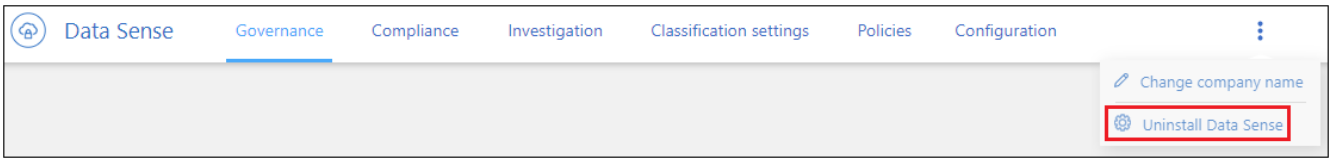
Vous pouvez désinstaller le logiciel de classification BlueXP pour résoudre des problèmes ou supprimer définitivement le logiciel de l'hôte. La suppression de l'instance supprime également les disques associés sur lesquels résident les données indexées. Toutes les informations analysées par BlueXP seront définitivement supprimées.

Les étapes à suivre dépendent du déploiement de la classification BlueXP dans le cloud ou sur un hôte sur site.

Désinstallez la classification BlueXP d'un déploiement cloud

Vous pouvez désinstaller et supprimer l'instance de classification BlueXP de l'environnement du fournisseur cloud si vous ne souhaitez plus utiliser la classification BlueXP.

1. En haut de la page de classification BlueXP, cliquez sur ⋮ Puis cliquez sur **Désinstaller Data SENSE**.



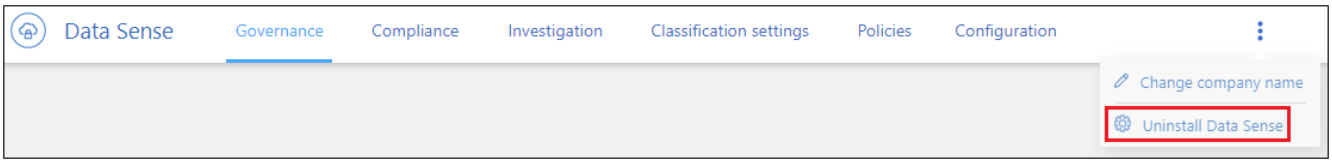
2. Dans la boîte de dialogue *Uninstall Data Sense*, tapez **uninstall** pour confirmer que vous souhaitez déconnecter l'instance de classification BlueXP du connecteur BlueXP, puis cliquez sur **Uninstall**.
3. Accédez à la console de votre fournisseur cloud et supprimez l'instance de classification BlueXP. L'instance s'appelle *CloudCompliance* avec un hachage (UUID) généré concaténé. Par exemple : *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

   Cette opération supprime l'instance et toutes les données associées qui ont été collectées par la classification BlueXP.

Désinstallez la classification BlueXP d'un déploiement sur site

Vous pouvez désinstaller la classification BlueXP d'un hôte si vous ne souhaitez plus utiliser la classification BlueXP ou si vous rencontrez un problème qui nécessite une réinstallation.

1. En haut de la page de classification BlueXP, cliquez sur ⋮ Puis cliquez sur **Désinstaller Data SENSE**.



2. Dans la boîte de dialogue *Uninstall Data Sense*, tapez **uninstall** pour confirmer que vous souhaitez déconnecter l'instance de classification BlueXP du connecteur BlueXP, puis cliquez sur **Uninstall**.
3. Pour désinstaller le logiciel de l'hôte, exécutez `cleanup.sh` script sur la machine hôte, par exemple :

```
cleanup.sh
```

Découvrez comment "Connectez-vous à la machine hôte de classification BlueXP".

Fonctionnalités obsolètes

Fonctionnalités obsolètes de la classification BlueXP

La classification BlueXP est disponible en tant que fonctionnalité clé de BlueXP, sans frais supplémentaires. En incluant la classification BlueXP en tant que fonctionnalité BlueXP clé disponible pour tous les clients, NetApp vous permet d'accéder à une gestion des données personnalisée avec des fonctionnalités principales.

Certaines fonctionnalités sont obsolètes dans la version principale de BlueXP depuis la version 1.31 et ultérieure et sont toujours prises en charge dans les versions 1.30 et antérieures.

Sources de données prises en charge

Source des données	Anciennes versions 1.30 et antérieures	BlueXP core versions 1.31 et ultérieures
Cloud Volumes ONTAP (déployé dans AWS, Azure ou GCP)	Oui.	Oui.
Clusters ONTAP sur site	Oui.	Oui.
StorageGRID	Oui.	Oui.
Azure NetApp Files	Oui.	Oui.
Amazon FSX pour ONTAP	Oui.	Oui.
Google Cloud NetApp volumes	Oui.	Oui.
Cloud Volumes Service pour Google Cloud	Oui.	Oui.
Les bases de données	Oui.	Oui.
Amazon S3	Oui.	Non
Google Cloud Storage	Oui.	Non
OneDrive	Oui.	Non
SharePoint Online	Oui.	Non
SharePoint sur site (SharePoint Server)	Oui.	Non
Google Drive	Oui.	Non

Fonctionnalités de conformité

Fonction	Anciennes versions 1.30 et antérieures	BlueXP core versions 1.31 et ultérieures
Identifier les informations à caractère personnel	Oui.	Oui.
Identifiez les informations personnelles sensibles	Oui.	Oui.

Fonction	Anciennes versions 1.30 et antérieures	BlueXP core versions 1.31 et ultérieures
Répondre aux demandes d'accès aux données (DSAR, Data Subject Access Requests)	Oui.	Oui.
Créez une liste personnalisée des « données personnelles » identifiées	Oui.	Non
Avertissez les utilisateurs par e-mail lorsque des fichiers contiennent certaines PII. (Vous définissez ces critères à l'aide de "Stratégies".)	Oui.	Non
Utilisez des filtres au niveau des répertoires	Oui.	Oui.
Utilisez l'analyse des RP au niveau du répertoire	Oui.	Non

Fonctionnalités de gestion des données

Fonction	Anciennes versions 1.30 et antérieures	BlueXP core versions 1.31 et ultérieures
Déplacer, copier et supprimer des fichiers source	Oui.	Non
Catégorisez les données à l'aide de balises d'état	Oui.	Non
Catégorisez les données à l'aide d'étiquettes AIP	Oui.	Non
Attribuer des fichiers aux utilisateurs	Oui.	Non
Renumériser les données à la demande	Oui.	Non
Créez des classificateurs personnalisés	Oui.	Non
Exclure les répertoires de l'analyse	Oui.	Oui.
Rechercher des noms dans les fichiers	Oui.	Oui.
Exporter les données vers NFS à partir de l'investigation	Oui.	Non
Exporter les données au format CSV à partir de l'investigation	Oui.	Oui.
Prend en charge plusieurs scanners	Oui.	Non
Intégrer Active Directory	Oui.	Oui.
Utilisez l'analyse des autorisations et les filtres	Oui.	Oui.
Utilisez la carte de fichier	Oui.	Oui.
Utilisez la carte thermique	Oui.	Oui.
Utilisez les actions du tableau de bord et de la carte de fichier	Oui.	Non
Utiliser la journalisation des audits d'accès aux fichiers	Oui.	Non
Activez l'accès aux fichiers à partir de la page Configuration	Oui.	Non
Utilisez certaines règles prédéfinies	Oui.	Non

Déployez les dérecommandations de classification BlueXP

Installez la classification BlueXP sur plusieurs hôtes pour les grandes configurations sans accès Internet

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

Dans le cas de configurations très volumineuses qui permettent d'analyser des pétaoctets de données sur des sites sans accès à Internet, vous pouvez inclure plusieurs hôtes pour fournir une puissance de traitement supplémentaire. Lors de l'utilisation de plusieurs systèmes hôtes, le système principal est appelé le *Manager node* et les systèmes supplémentaires qui fournissent une puissance de traitement supplémentaire sont appelés *scanner nodes*.

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

> **REMARQUE** ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP.

Ce dont vous avez besoin

- Vérifiez que tous vos systèmes Linux pour les nœuds Manager et scanner répondent aux exigences de l'hôte.
- Vérifiez que vous avez installé les deux packages logiciels prérequis (Docker Engine ou Podman et Python 3).
- Assurez-vous que vous disposez des privilèges root sur les systèmes Linux.
- Vérifiez que votre environnement hors ligne dispose des autorisations et de la connectivité requises.
- Vous devez disposer des adresses IP des hôtes du nœud de scanner que vous prévoyez d'utiliser.
- Les ports et protocoles suivants doivent être activés sur tous les hôtes :

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

Étapes

1. Suivez les étapes 1 à 8 du "Installation avec un seul hôte" sur le nœud gestionnaire.

2. Comme indiqué à l'étape 9, lorsque le programme d'installation vous le demande, vous pouvez entrer les valeurs requises dans une série d'invites, ou vous pouvez fournir les paramètres requis comme arguments de ligne de commande au programme d'installation.

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

   Par exemple, cette commande ajoute 3 nœuds de scanner :
   `sudo ./install.sh -a <account_id> -c <client_id> -t <user_token> --host <ds_host> --manager-host <cm_host> -n <node_ip1>,<node_ip2>,<node_ip3> --no-proxy --darksite`

3. Avant la fin de l'installation du nœud Manager, une boîte de dialogue affiche la commande d'installation requise pour les nœuds du scanner. Copiez la commande (par exemple : `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF-1-3u69m1-1s35212`) et enregistrez-le dans un fichier texte.
4. Sur **chaque hôte de nœud du scanner** :
   a. Copiez le fichier d'installation de Data Sense (**cc_onsite_installer.tar.gz**) sur la machine hôte.
   b. Décompressez le fichier d'installation.
   c. Collez et exécutez la commande que vous avez copiée à l'étape 3.

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

Résultat

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

Et la suite

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

Ajoutez des nœuds de scanner à un déploiement existant

Vous pouvez ajouter des nœuds scanner à un déploiement existant sur un hôte Linux avec accès Internet.

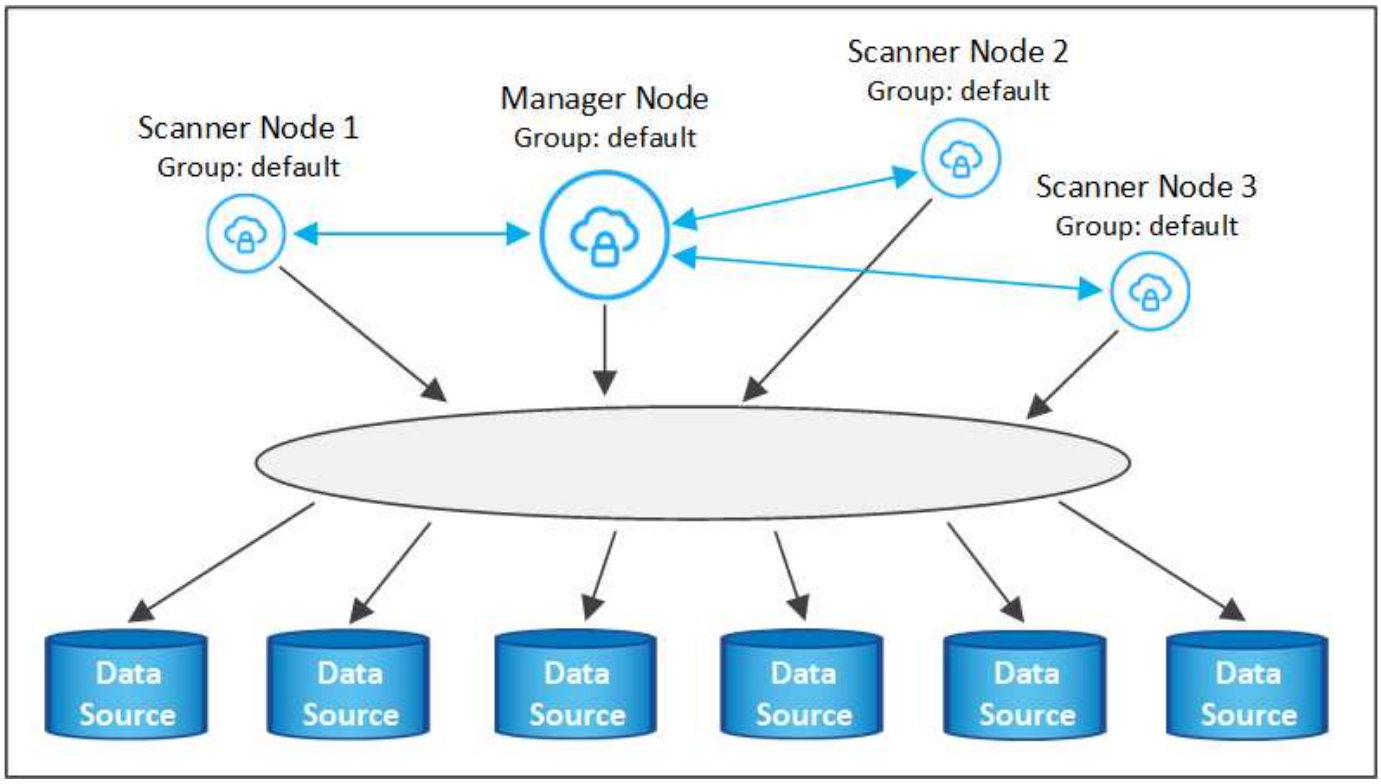
Vous pouvez ajouter d'autres nœuds de numérisation si vous trouvez que vous avez besoin d'une puissance de traitement plus élevée pour numériser vos sources de données. Vous pouvez ajouter les nœuds du scanner immédiatement après avoir installé le nœud du gestionnaire, ou vous pouvez ajouter un nœud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

> **REMARQUE** ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP.

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

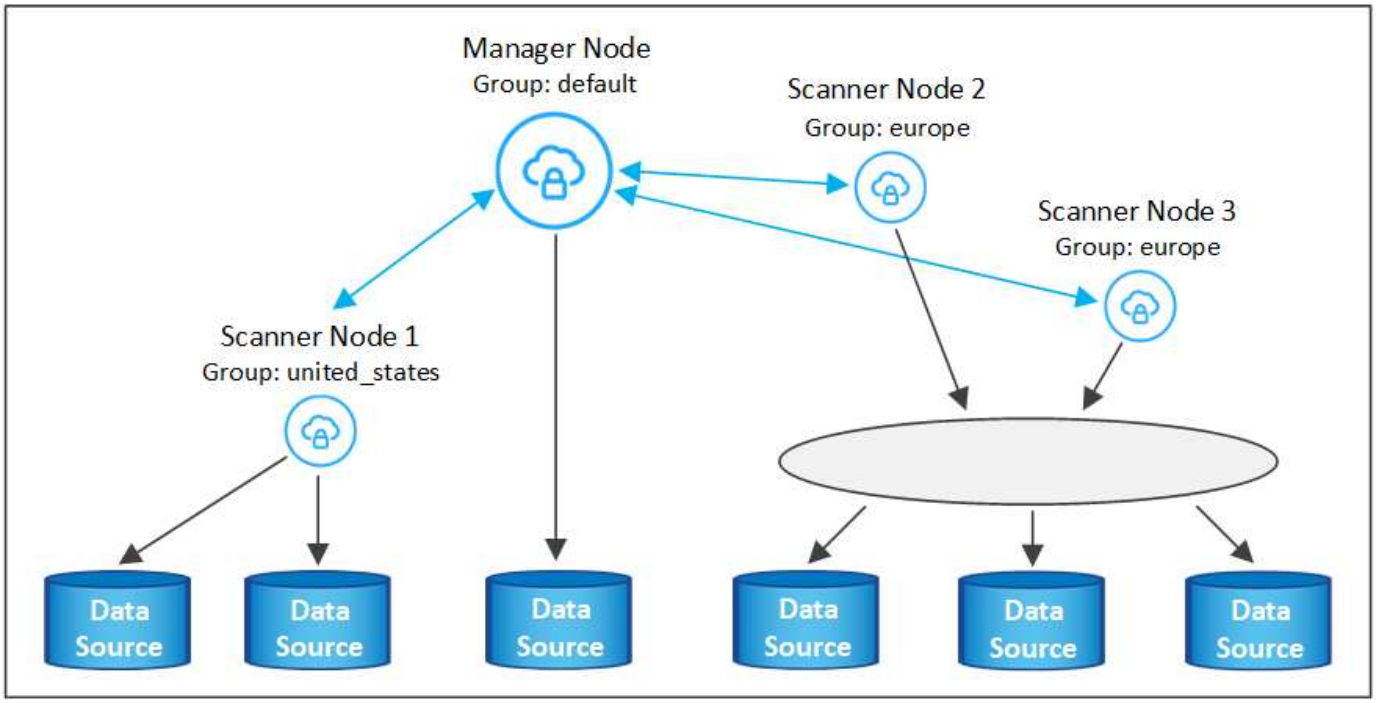
- ajoutez un nœud pour faciliter la numérisation de toutes les sources de données
- ajout d'un nœud pour faciliter l'analyse d'une source de données spécifique ou d'un groupe spécifique de sources de données (généralement basé sur l'emplacement)

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



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

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



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

Vous pouvez choisir les groupes de scanner à ajouter à la classification BlueXP et choisir leur nom. La classification BlueXP n'applique pas qu'un nœud mappé à un groupe de scanner nommé « europe » soit déployé en Europe.

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

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

Ce dont vous avez besoin

- Vérifiez que tous vos systèmes Linux pour les nœuds scanner répondent aux exigences de l'hôte.
- Vérifier que les deux logiciels prérequis sont installés sur les systèmes (Docker Engine ou Podman et Python 3).
- Assurez-vous que vous disposez des privilèges root sur les systèmes Linux.
- Vérifiez que votre environnement dispose des autorisations et de la connectivité requises.

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

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

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

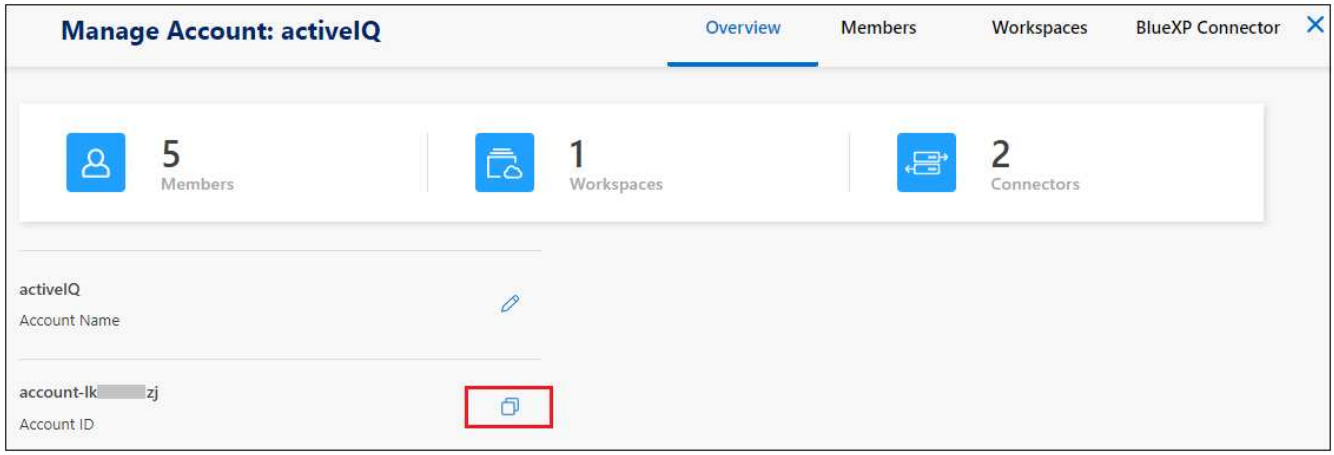
  ```
  firewall-cmd --permanent --add-service=http
  firewall-cmd --permanent --add-service=https
  firewall-cmd --permanent --add-port=80/tcp
  firewall-cmd --permanent --add-port=8080/tcp
  firewall-cmd --permanent --add-port=443/tcp
  firewall-cmd --permanent --add-port=2377/tcp
  firewall-cmd --permanent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

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

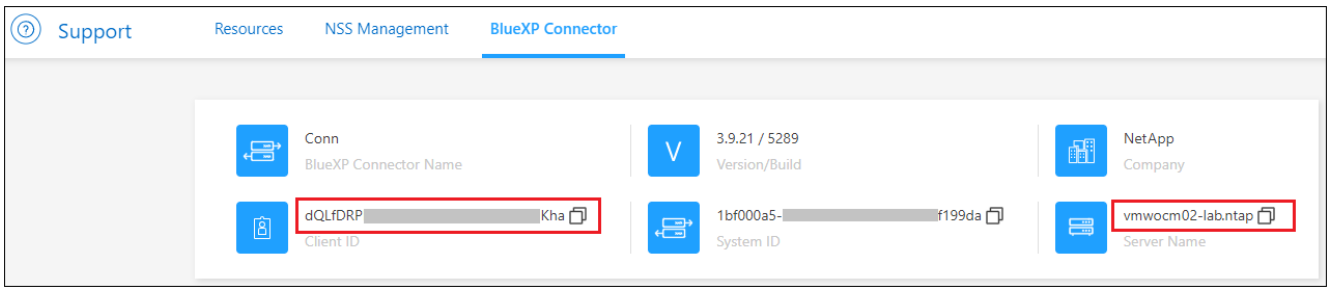
Étapes préalables

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

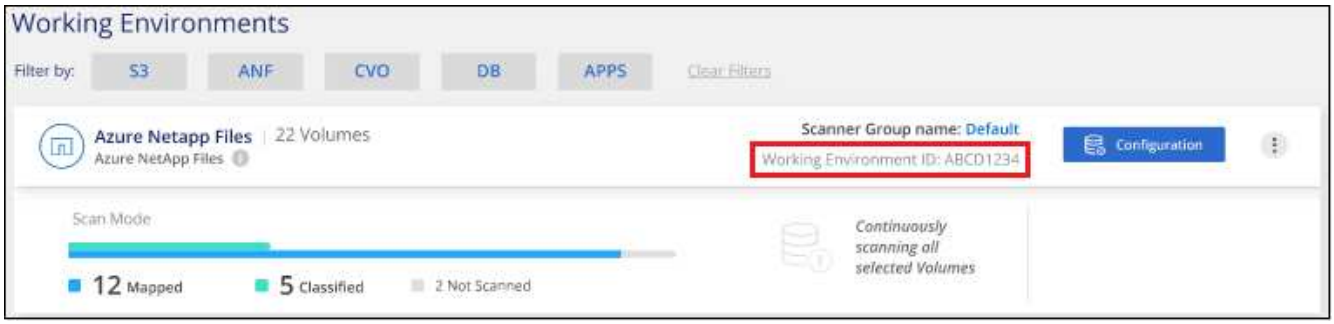
1. Dans la barre de menus BlueXP, cliquez sur **compte > gérer les comptes**.



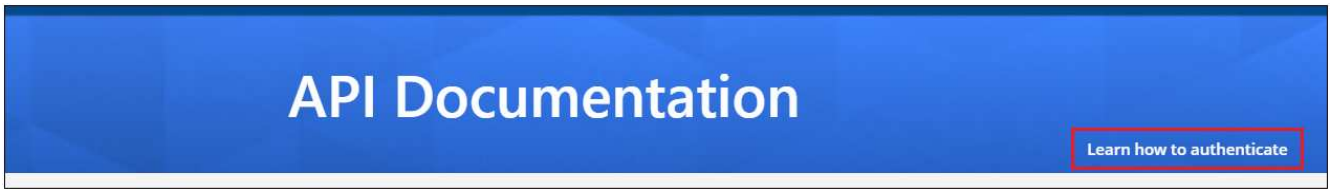
2. Copiez le *ID de compte*.
3. Dans la barre de menus BlueXP, cliquez sur **aide > support > connecteur BlueXP**.



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



6. Accédez au "API Documentation Developer Hub" Et cliquez sur **Apprenez à vous authentifier**.



7. Suivez les instructions d'authentification, en utilisant le nom d'utilisateur et le mot de passe de l'administrateur du compte dans les paramètres "nom d'utilisateur" et "mot de passe".
8. Copiez ensuite le *jeton d'accès* de la réponse.

Étapes

1. Sur le nœud du gestionnaire de classification BlueXP, exécutez le script « add_scanner_node.sh ». Par exemple, cette commande ajoute 2 nœuds de scanner :

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

   Valeurs variables :

   - *Account_ID* = ID du compte NetApp
   - *Client_ID* = connecteur client ID (ajoutez le suffixe "clients" à l'ID client que vous avez copié dans les étapes préalables)
   - *Cm_host* = adresse IP ou nom d'hôte du système de connecteurs
   - *Ds_Manager_ip* = adresse IP privée du système de nœuds BlueXP classification Manager
   - *Node_private_ip* = adresses IP des systèmes de nœuds du scanner de classification BlueXP (les adresses IP de plusieurs nœuds du scanner sont séparées par une virgule)
   - *User_token* = jeton d'accès utilisateur JWT
2. Avant la fin du script add_scanner_node, une boîte de dialogue affiche la commande d'installation requise pour les nœuds du scanner. Copiez la commande (par exemple : `sudo ./node_install.sh -m 10.11.12.13 -t ABCDEF1s35212 -u red95467j`) et enregistrez-le dans un fichier texte.
3. Sur **chaque hôte de nœud du scanner** :
   a. Copiez le fichier d'installation de Data Sense (**DATASENNSE-INSTALLER-<version>.tar.gz**) sur la machine hôte (à l'aide de `scp` ou une autre méthode).
   b. Décompressez le fichier d'installation.
   c. Collez et exécutez la commande que vous avez copiée à l'étape 2.
   d. Si vous souhaitez ajouter un nœud de scanner à un « scanner group », ajoutez le paramètre **-r <scanner_group_name>** à la commande. Sinon, le nœud du scanner est ajouté au groupe « défaut ».

      Une fois l'installation terminée sur tous les nœuds du scanner et qu'ils ont été associés au nœud du gestionnaire, le script « Add_scanner_node.sh » se termine également. L'installation peut prendre entre 10 et 20 minutes.
4. Si vous avez ajouté des nœuds de scanner à un scanner group, revenez au nœud Manager et effectuez les 2 tâches suivantes :
   a. Ouvrez le fichier « /opt/netapp/config/custom_configuration/working_Environment_to_scanner_group_config.yml » et entrez le mappage pour lequel les groupes de scanner vont analyser des environnements de travail spécifiques. Vous devez avoir l'ID *Working Environment* pour chaque source de données. Par exemple, les entrées suivantes ajoutent 2 environnements de travail au groupe de scanner « europe » et 2 au groupe de scanner « united_States » :

```
scanner_groups:
 europe:
   working_environments:
     - "working_environment_id1"
     - "working_environment_id2"
 united_states:
   working_environments:
     - "working_environment_id3"
     - "working_environment_id4"
```

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

b. Exécutez le script suivant pour enregistrer ces informations de mappage avec tous les nœuds du scanner : `/opt/netapp/Datasense/tools/update_we_scanner_group_from_config_file.sh`

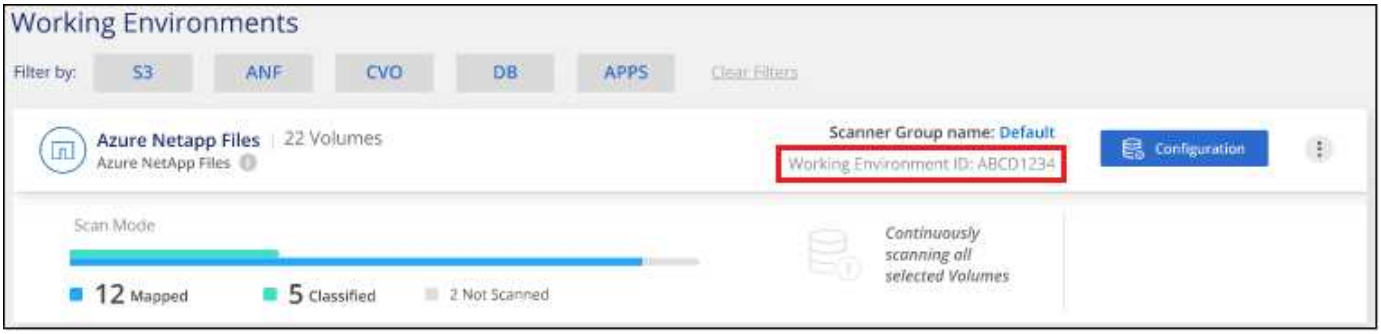
Résultat

La classification BlueXP est configurée avec des nœuds Manager et scanner pour analyser toutes vos sources de données.

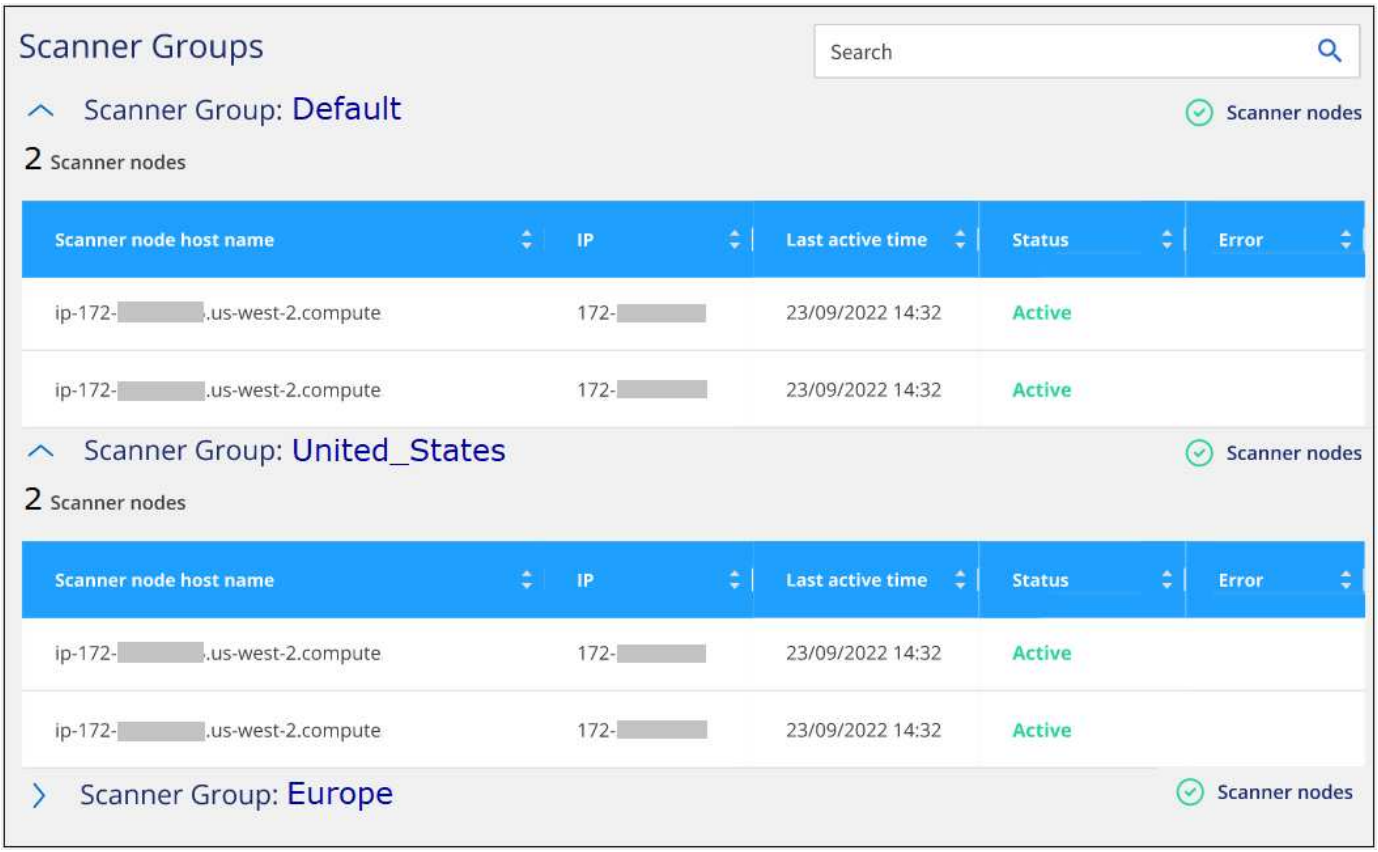
Et la suite

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

Vous pouvez voir le nom du groupe de lecteurs pour chaque environnement de travail dans la page Configuration.



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



Dépercations des données d'acquisition

Analyse des compartiments Amazon S3

La classification BlueXP peut analyser vos compartiments Amazon S3 pour identifier les données personnelles et sensibles qui résident dans le stockage objet S3. La classification BlueXP peut analyser n'importe quel compartiment du compte, qu'il ait été créé pour une solution NetApp.

> **REMARQUE** ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP.

Démarrage rapide

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

1. **Configurez les exigences S3 dans votre environnement cloud**

Assurez-vous que votre environnement cloud répond aux exigences de classification BlueXP, notamment en préparant un rôle IAM et en configurant la connectivité entre la classification BlueXP et S3. Voir la liste complète.

Déployez l’instance de classification BlueXP

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

Activez la classification BlueXP dans votre environnement de travail S3

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

Sélectionnez les compartiments à numériser

Sélectionnez les compartiments que vous souhaitez analyser et la classification BlueXP commencera à les analyser.

Vérification des prérequis S3

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

Configurez un rôle IAM pour l’instance de classification BlueXP

La classification BlueXP nécessite des autorisations pour se connecter aux compartiments S3 de votre compte et les analyser. Configurez un rôle IAM qui inclut les autorisations répertoriées ci-dessous. BlueXP vous invite à sélectionner un rôle IAM lorsque vous activez la classification BlueXP dans l’environnement de travail Amazon S3.

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

Connectivité de la classification BlueXP à Amazon S3

La classification BlueXP doit être connectée à Amazon S3. Pour assurer cette connexion, le meilleur moyen consiste à utiliser un terminal VPC pour le service S3. Pour obtenir des instructions, reportez-vous à la section "Documentation AWS : création d'un terminal de passerelle".

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

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

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

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

Déploiement de l'instance de classification BlueXP

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

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

Remarque : le déploiement de la classification BlueXP dans un emplacement sur site n'est actuellement pas pris en charge lors de l'analyse des compartiments S3.

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

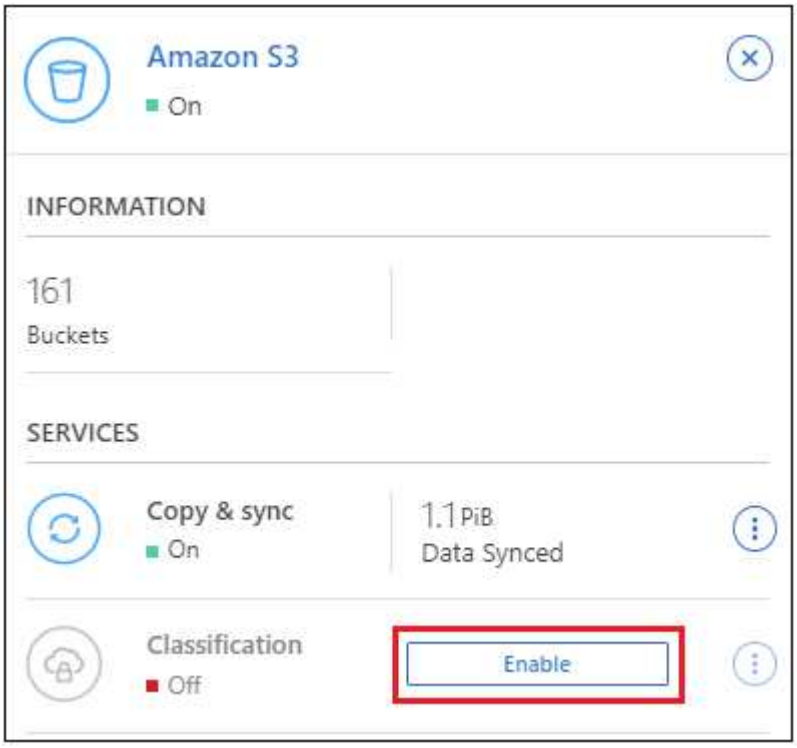
Activation de la classification BlueXP sur votre environnement de travail S3

Activez la classification BlueXP sur Amazon S3 après avoir vérifié les prérequis.

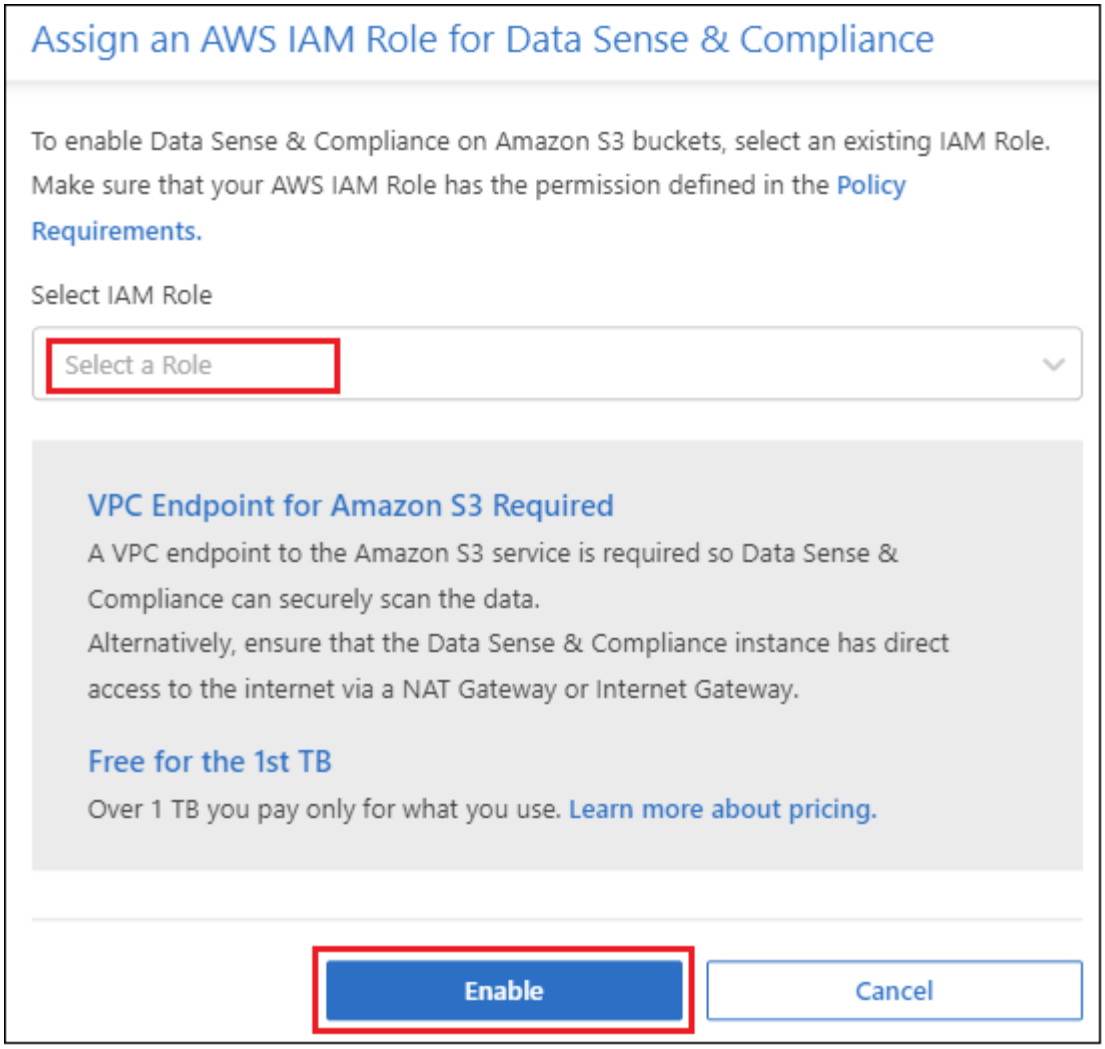
Étapes

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

3. Dans le volet Services à droite, cliquez sur **Activer** en regard de **Classification**.



4. Lorsque vous y êtes invité, attribuez un rôle IAM à l'instance de classification BlueXP qui dispose de les autorisations requises.



5. Cliquez sur **Activer**.

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

Résultat

BlueXP affecte le rôle IAM à l'instance.

Activation et désactivation des analyses de conformité dans les compartiments S3

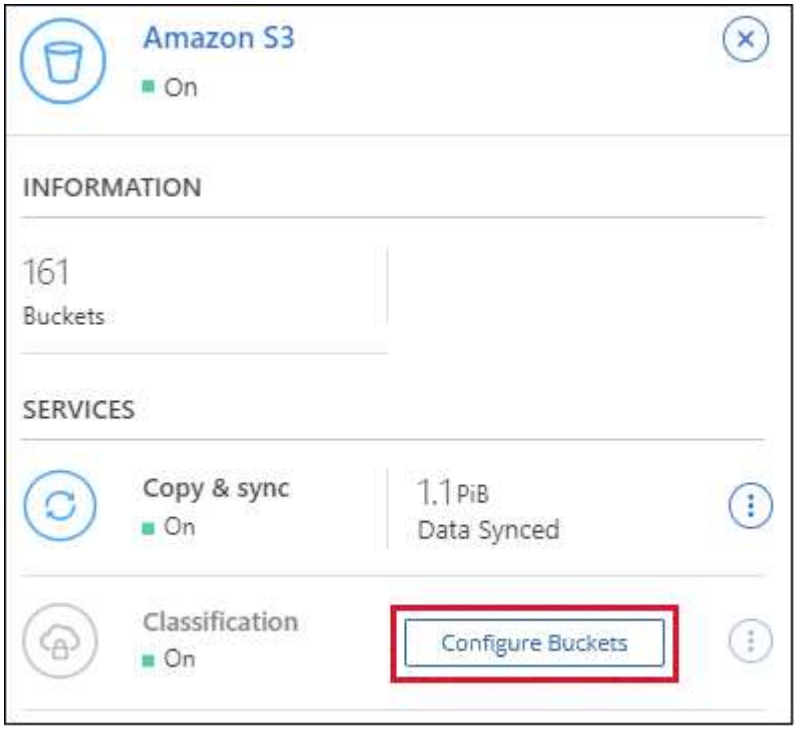
Une fois que BlueXP a activé la classification BlueXP sur Amazon S3, l'étape suivante consiste à configurer les compartiments à analyser.

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

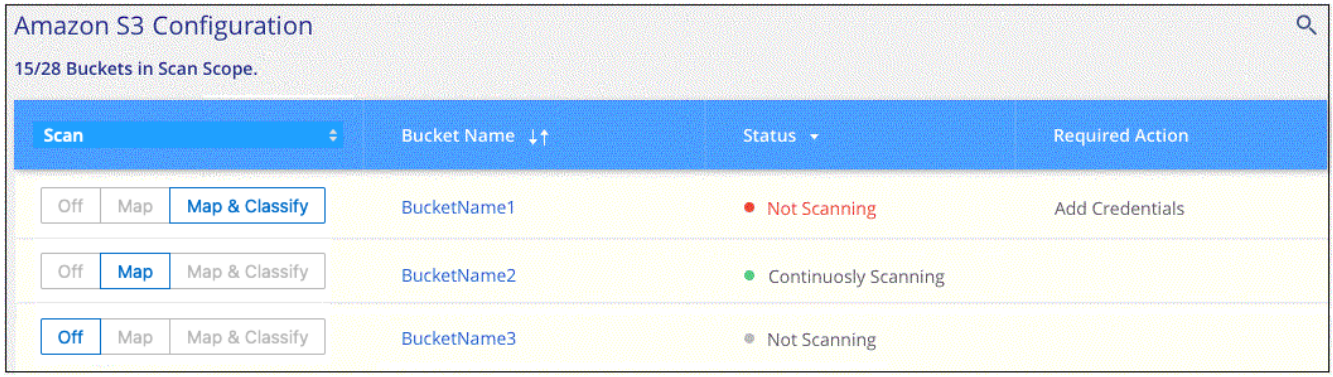
La classification BlueXP peut également être utilisée Analysez les compartiments S3 qui se trouvent dans différents comptes AWS.

Étapes

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



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



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

Résultat

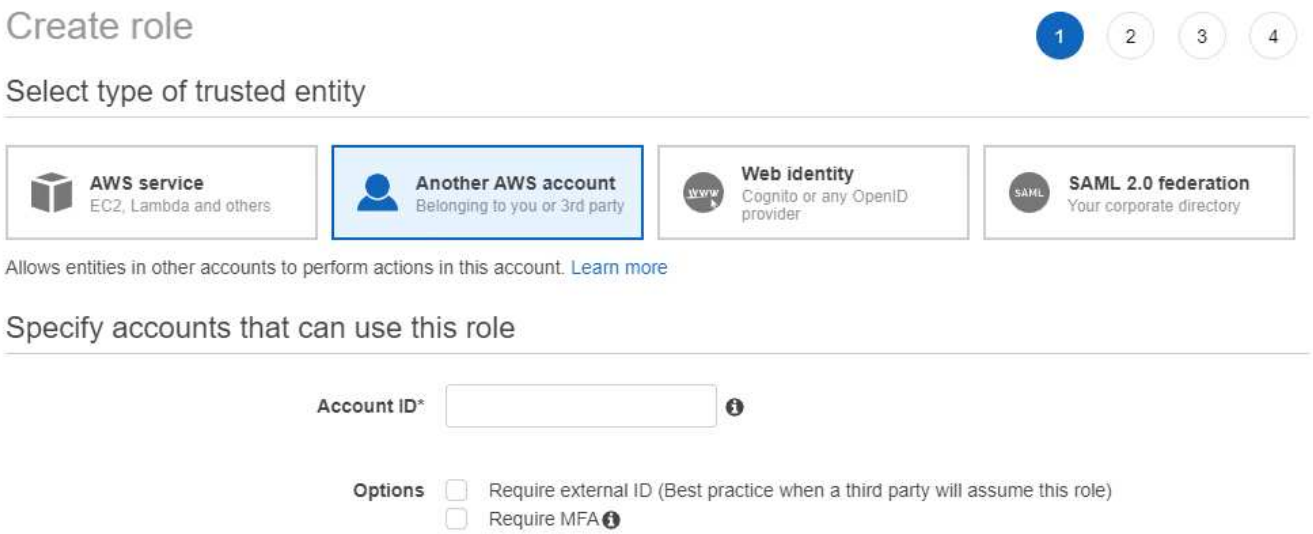
La classification BlueXP commence à analyser les compartiments S3 que vous avez activés. En cas d'erreur, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

Analyse des compartiments à partir de comptes AWS supplémentaires

Vous pouvez analyser les compartiments S3 situés sous un autre compte AWS en attribuant un rôle à partir de ce compte pour accéder à l'instance de classification BlueXP existante.

Étapes

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



   Assurez-vous de faire ce qui suit :

   - Entrez l'ID du compte où réside l'instance de classification BlueXP.
   - Modifiez la durée * maximale de la session CLI/API* de 1 heure à 12 heures et enregistrez cette modification.
   - Reliez la règle IAM de classification BlueXP. Assurez-vous qu'il dispose des autorisations requises.

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

2. Accédez au compte AWS source sur lequel réside l'instance de classification BlueXP et sélectionnez le

rôle IAM qui est associé à l'instance.

a. Modifiez la durée * maximale de la session CLI/API* de 1 heure à 12 heures et enregistrez cette modification.

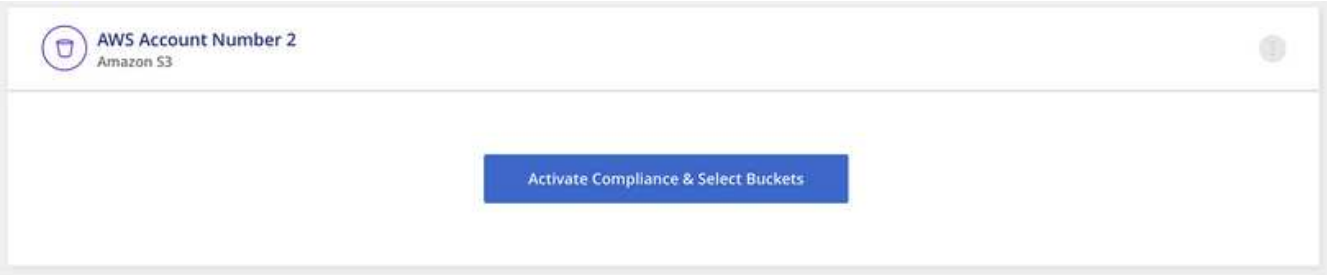
b. Cliquez sur **attacher des stratégies**, puis sur **Créer une stratégie**.

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

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

Le compte de profil d'instance de classification BlueXP a désormais accès au compte AWS supplémentaire.

3. Accédez à la page **Amazon S3 Configuration** et le nouveau compte AWS s'affiche. Notez que la classification BlueXP peut prendre quelques minutes pour synchroniser l'environnement de travail du nouveau compte et afficher ces informations.



4. Cliquez sur **Activer la classification BlueXP et sélectionner les compartiments** et sélectionnez les compartiments à analyser.

Résultat

La classification BlueXP commence à analyser les nouveaux compartiments S3 que vous avez activés.

Analysez les comptes OneDrive

Procédez en quelques étapes pour commencer à analyser les fichiers dans les dossiers OneDrive de votre utilisateur avec la classification BlueXP.

> **REMARQUE** ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP.

Démarrage rapide

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

1 Vérifiez les prérequis OneDrive

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

2 Déployez l'instance de classification BlueXP

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

3 Ajoutez le compte OneDrive

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

4 Ajoutez les utilisateurs et sélectionnez le type de numérisation

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

Vérification des exigences OneDrive

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

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

Déploiement de l'instance de classification BlueXP

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

La classification BlueXP peut l'être "déploiement dans le cloud" ou "dans un emplacement sur site avec accès à internet".

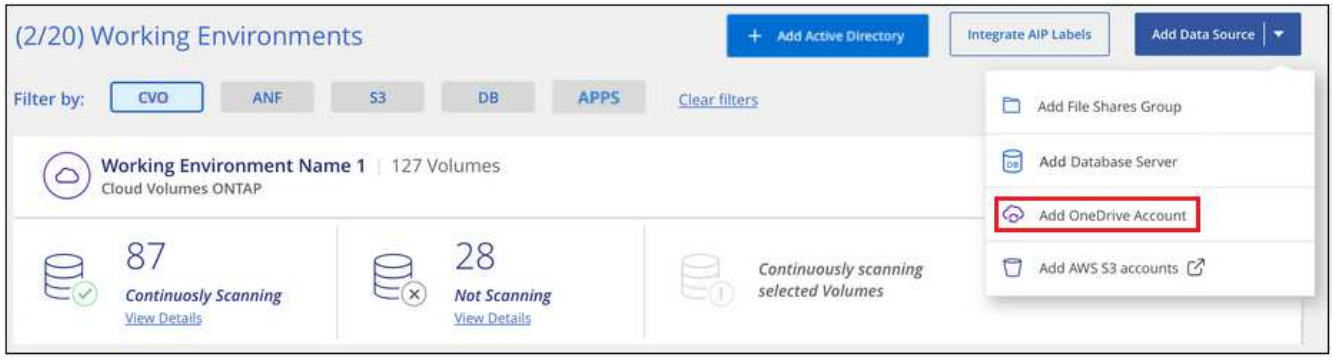
Les mises à niveau du logiciel de classification BlueXP sont automatisées tant que l'instance dispose d'une connectivité Internet.

Ajout du compte OneDrive

Ajoutez le compte OneDrive où résident les fichiers utilisateur.

Étapes

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



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

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

Ajout d'utilisateurs OneDrive aux analyses de conformité

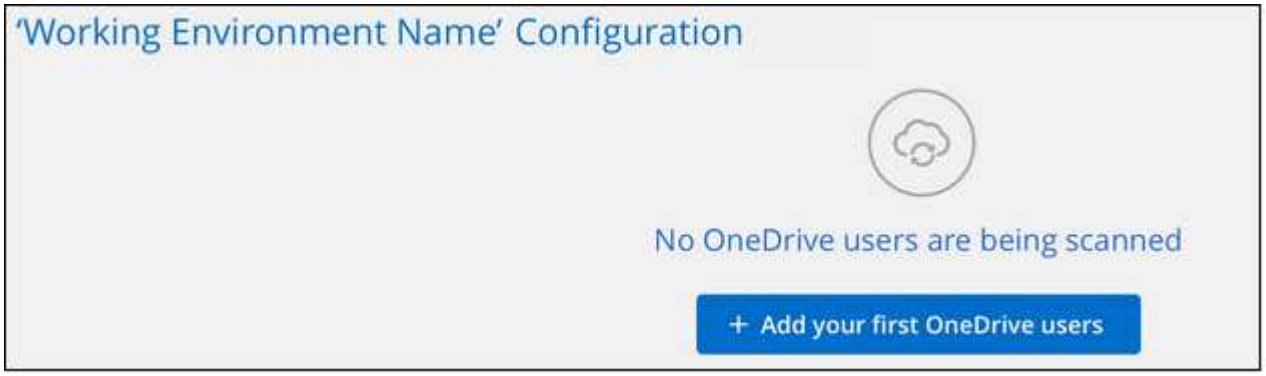
Vous pouvez ajouter des utilisateurs OneDrive individuels ou tous vos utilisateurs OneDrive afin que leurs fichiers soient analysés par la classification BlueXP.

Étapes

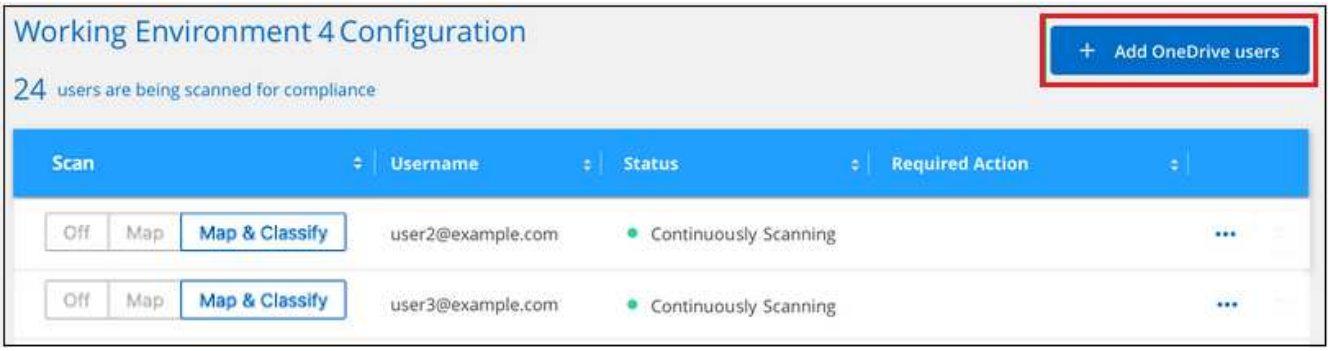
1. Dans la page *Configuration*, cliquez sur le bouton **Configuration** du compte OneDrive.

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

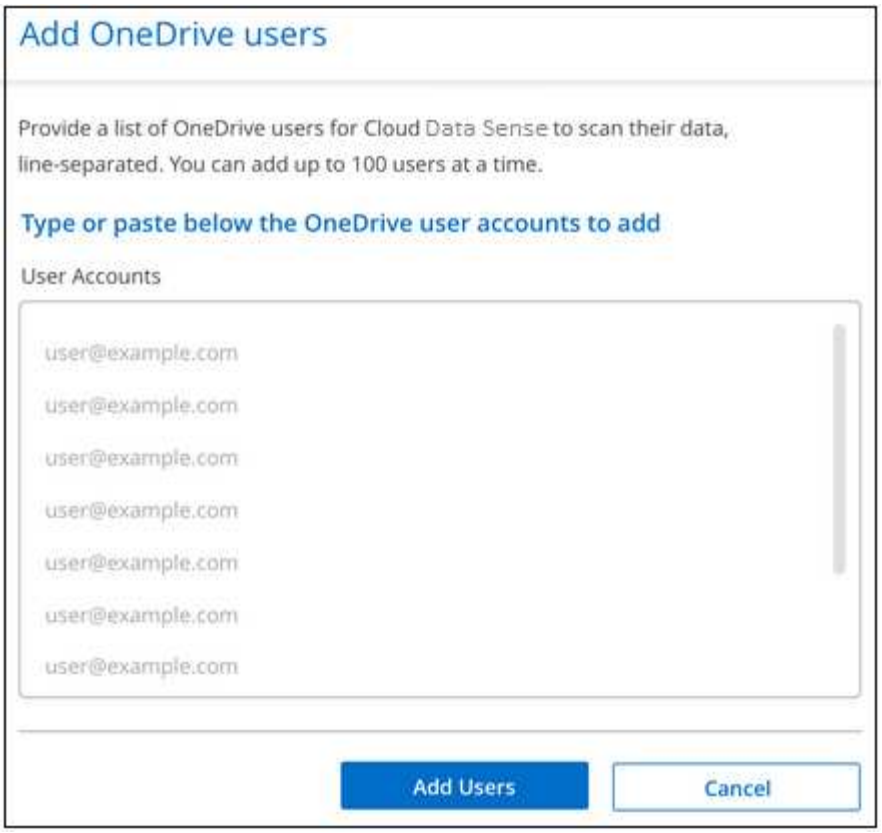
Ajouter vos premiers utilisateurs OneDrive.



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



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



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

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

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

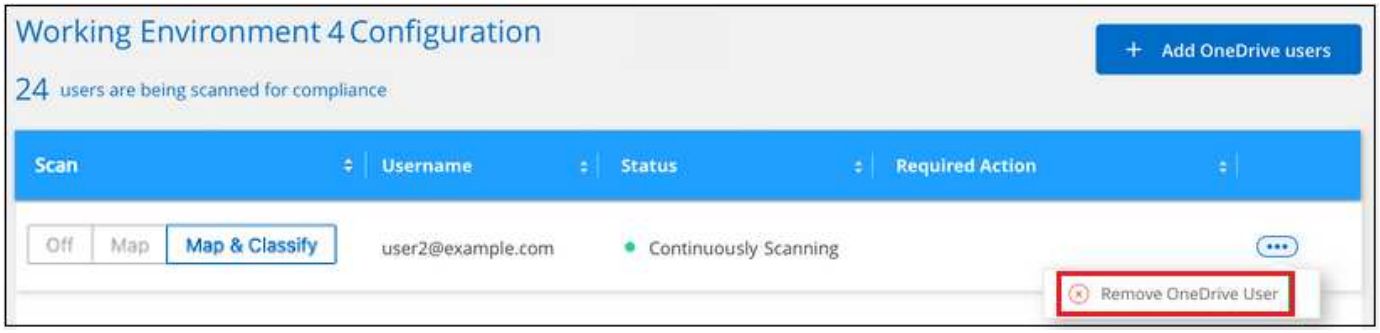
À :	Procédez comme suit :
Activer les analyses de mappage uniquement sur les fichiers utilisateur	Cliquez sur **carte**
Activer les analyses complètes sur les fichiers utilisateur	Cliquez sur **carte et classement**
Désactiver la numérisation sur les fichiers utilisateur	Cliquez sur **Off**

Résultat

La classification BlueXP commence à analyser les fichiers pour les utilisateurs que vous avez ajoutés. Les résultats s'affichent dans le tableau de bord et à d'autres emplacements.

Suppression d'un utilisateur OneDrive des analyses de conformité

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



Analyser les comptes SharePoint

Procédez en quelques étapes pour commencer à analyser les fichiers de vos comptes sur site SharePoint Online et SharePoint avec la classification BlueXP.

> **REMARQUE** ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP.

Démarrage rapide

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

1. **Consultez les prérequis pour SharePoint**

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

2. **Déployez l'instance de classification BlueXP**

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

3. **Connectez-vous au compte SharePoint**

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

4. **Ajoutez les URL du site SharePoint à analyser**

Ajoutez la liste des URL du site SharePoint que vous souhaitez analyser dans le compte SharePoint et sélectionnez le type de numérisation. Vous pouvez ajouter jusqu'à 100 URL à la fois et jusqu'à 1,000 sites au total pour chaque compte.

Passez en revue les exigences liées à SharePoint

Vérifiez les conditions préalables suivantes pour vous assurer que vous êtes prêt à activer la classification BlueXP sur un compte SharePoint.

- Vous devez disposer des identifiants de connexion administrateur pour le compte SharePoint qui fournissent un accès en lecture à tous les sites SharePoint.
  - Pour SharePoint Online, vous pouvez utiliser un compte non administrateur, mais cet utilisateur doit avoir l'autorisation d'accéder à tous les sites SharePoint que vous souhaitez analyser.
- Pour les solutions SharePoint sur site, vous aurez également besoin de l'URL de SharePoint Server.
- Vous aurez besoin d'une liste séparée en plusieurs lignes des URL du site SharePoint pour toutes les données que vous souhaitez analyser.

Déployez l'instance de classification BlueXP

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

- Pour SharePoint Online, la classification BlueXP peut être de "déploiement dans le cloud".
- Pour SharePoint sur site, la classification BlueXP peut être installée "dans un emplacement sur site avec accès à internet" ou "dans un emplacement sur site qui ne dispose pas d'un accès internet".

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

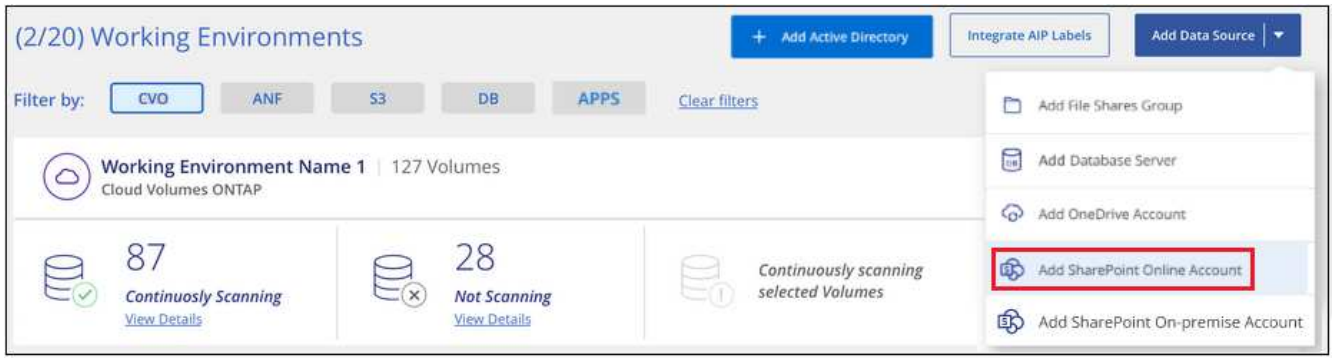
Les mises à niveau du logiciel de classification BlueXP sont automatisées tant que l'instance dispose d'une connectivité Internet.

Ajoutez un compte SharePoint Online

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

Étapes

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



2. Dans la boîte de dialogue Ajouter un compte SharePoint en ligne, cliquez sur **se connecter à SharePoint**.
3. Dans la page Microsoft qui s'affiche, sélectionnez le compte SharePoint et entrez l'utilisateur et le mot de passe (utilisateur Admin ou autre utilisateur ayant accès aux sites SharePoint), puis cliquez sur **accepter** pour permettre à la classification BlueXP de lire les données de ce compte.

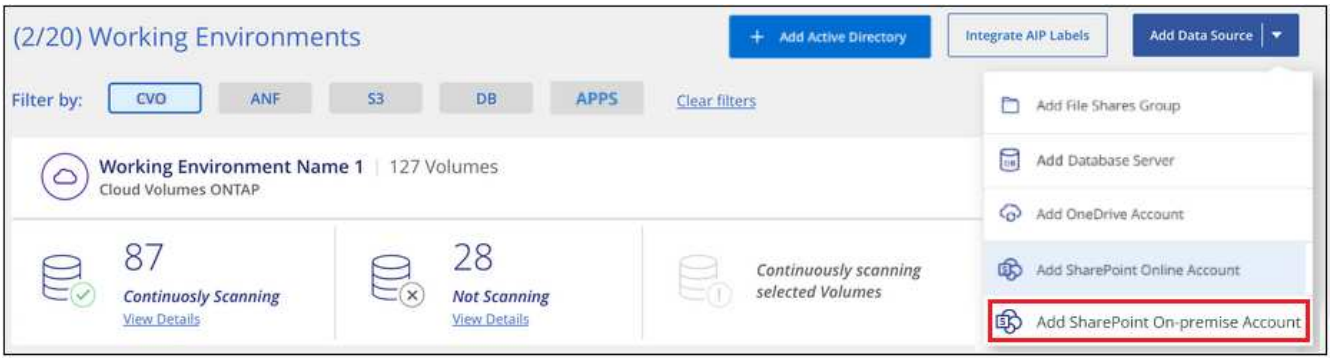
Le compte SharePoint Online est ajouté à la liste des environnements de travail.

Ajoutez un compte SharePoint sur site

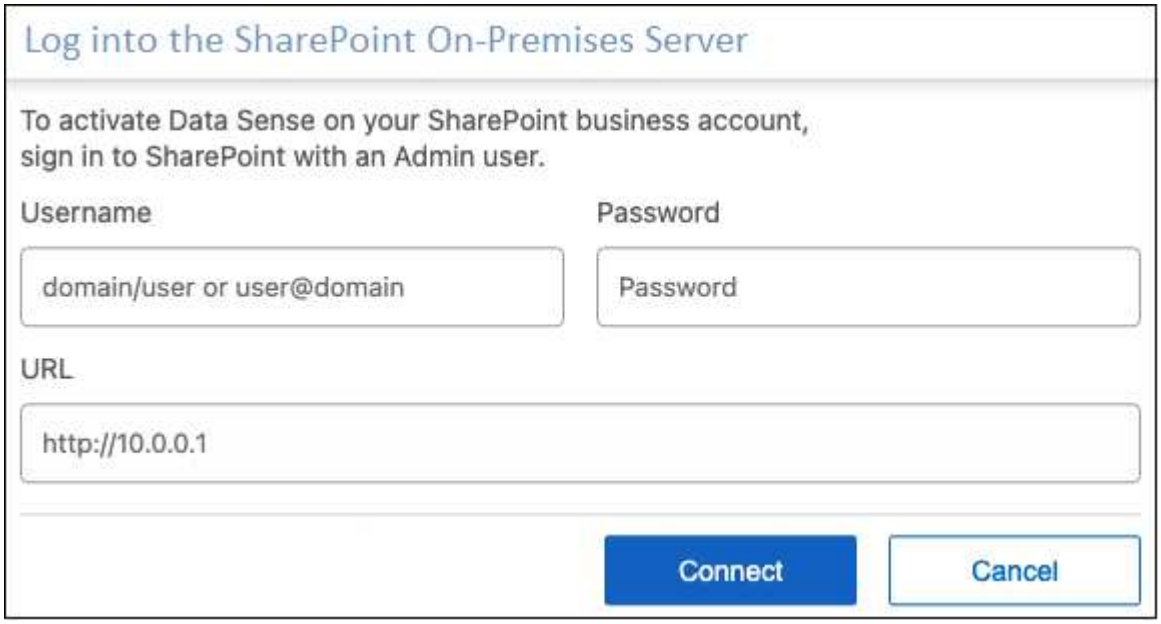
Ajoutez le compte SharePoint sur site où résident les fichiers utilisateur.

Étapes

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



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



3. Cliquez sur **connexion**.

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

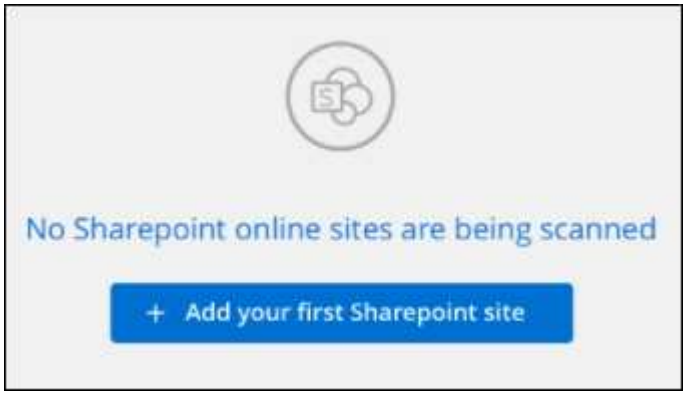
Ajoutez des sites SharePoint aux analyses de conformité

Vous pouvez ajouter des sites SharePoint individuels ou jusqu'à 1,000 sites SharePoint dans le compte, afin que les fichiers associés soient analysés par la classification BlueXP. Les étapes sont les mêmes, que vous ajoutiez des sites SharePoint Online ou SharePoint sur site.

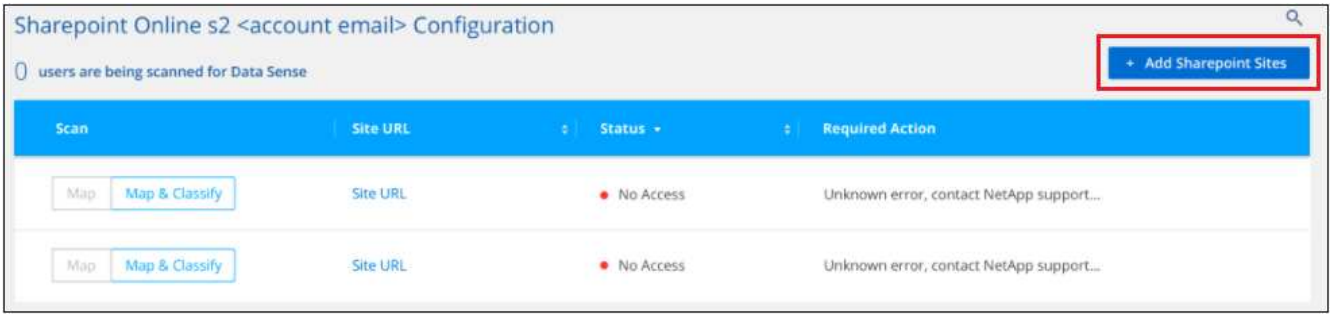
Étapes

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

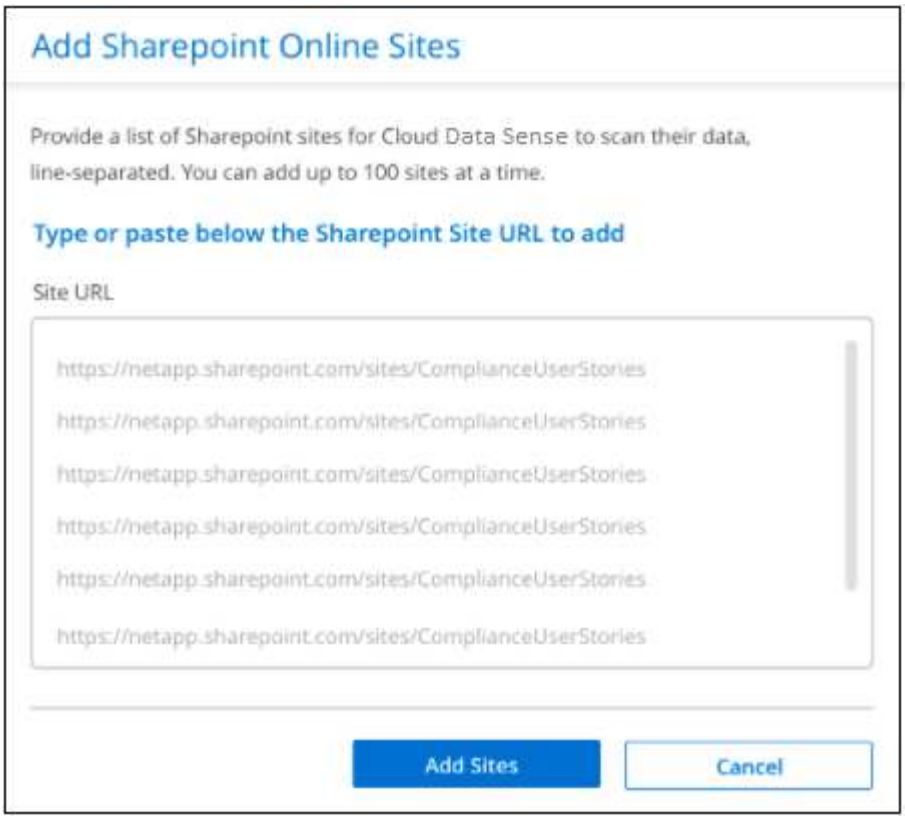
2. Si c'est la première fois que vous ajoutez des sites pour ce compte SharePoint, cliquez sur **Ajouter votre premier site SharePoint**.



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



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



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

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

4. Si vous devez ajouter plus de 100 sites pour ce compte, cliquez à nouveau sur **Ajouter des sites SharePoint** jusqu'à ce que vous ayez ajouté tous vos sites pour ce compte (jusqu'à 1,000 sites au total pour chaque compte).
5. Activez les analyses de mappage uniquement, ou les analyses de mappage et de classification, sur les fichiers des sites SharePoint.

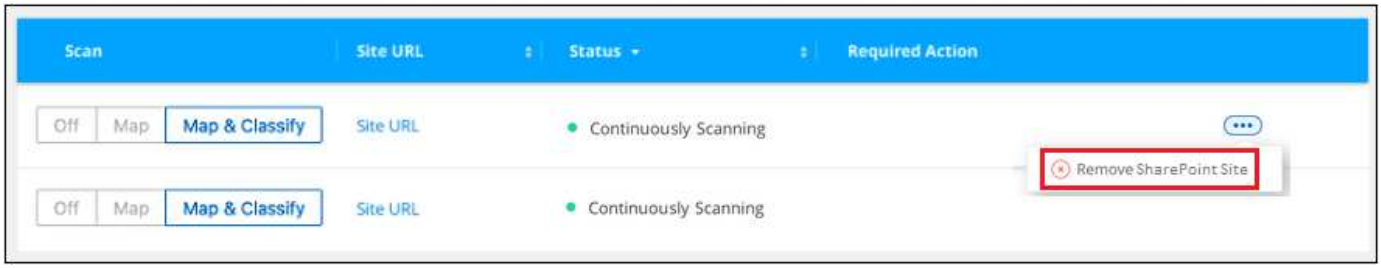
À :	Procédez comme suit :
Activer les analyses de mappage uniquement sur les fichiers	Cliquez sur **carte**
Activez les analyses complètes sur les fichiers	Cliquez sur **carte et classement**
Désactiver la numérisation sur les fichiers	Cliquez sur **Off**

Résultat

La classification BlueXP commence à analyser les fichiers des sites SharePoint que vous avez ajoutés. Les résultats s'affichent dans le tableau de bord et à d'autres emplacements.

Supprimez un site SharePoint des analyses de conformité

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



Notez que vous pouvez "Supprimez le compte SharePoint complet de la classification BlueXP" Si vous ne souhaitez plus analyser les données utilisateur du compte SharePoint.

Analyser les comptes Google Drive

Procédez en quelques étapes pour commencer à analyser les fichiers utilisateur de vos comptes Google Drive avec la classification BlueXP.

> **REMARQUE** ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP.

Démarrage rapide

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

1. **Consultez les conditions préalables à Google Drive**

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

2. **Déployez la classification BlueXP**

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

3. **Connectez-vous au compte Google Drive**

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

4. **Sélectionnez le type de numérisation des fichiers utilisateur**

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

Consultez les exigences relatives à Google Drive

Vérifiez les conditions préalables suivantes pour vous assurer que vous êtes prêt à activer la classification BlueXP sur un compte Google Drive.

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

Restrictions actuelles

Les fonctionnalités de classification BlueXP suivantes ne sont actuellement pas prises en charge par Google Drive Files :

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

Déployez la classification BlueXP

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

La classification BlueXP peut l'être "déploiement dans le cloud" ou "dans un emplacement sur site avec accès à internet".

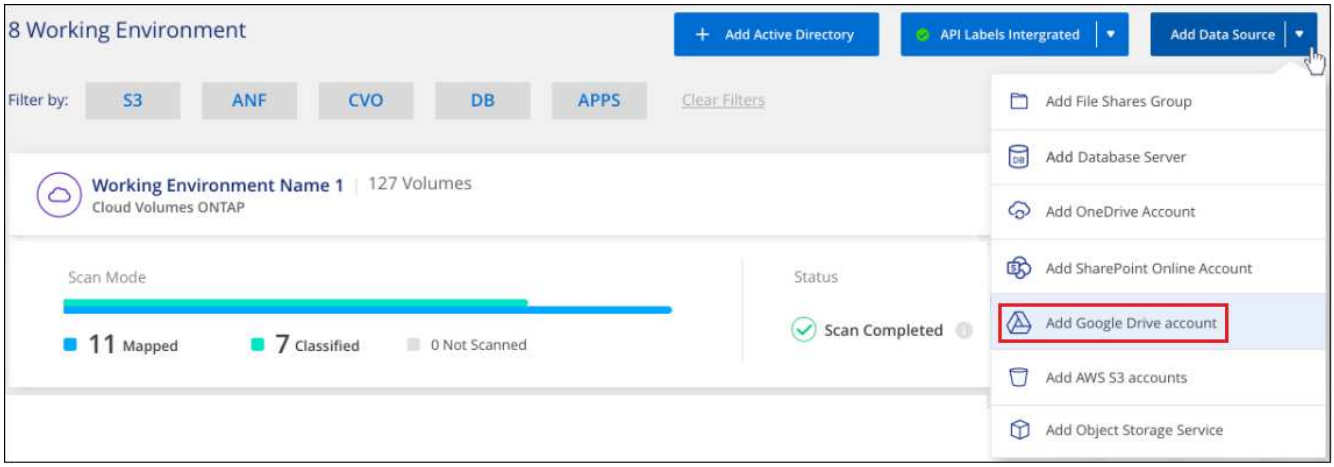
Les mises à niveau du logiciel de classification BlueXP sont automatisées tant que l'instance dispose d'une connectivité Internet.

Ajoutez le compte Google Drive

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

Étapes

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



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

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

Sélectionnez le type de numérisation des données utilisateur

Sélectionnez le type d'analyse que la classification BlueXP effectuera sur les données de l'utilisateur.

Étapes

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

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

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

Résultat

La classification BlueXP commence à analyser les fichiers du compte Google Drive que vous avez ajouté. Les résultats s'affichent dans le tableau de bord et à d'autres emplacements.

Supprimez un compte Google Drive des analyses de conformité

Étant donné que les fichiers Google Drive d'un seul utilisateur font partie d'un seul compte Google Drive, si vous voulez arrêter de numériser des fichiers à partir du compte Google Drive d'un utilisateur, alors vous devriez "Supprimez le compte Google Drive de la classification BlueXP".

Analyser les données StorageGRID

Procédez en quelques étapes pour commencer à analyser les données dans le stockage objet directement avec la classification BlueXP. La classification BlueXP peut analyser les données à partir de n'importe quel service de stockage objet qui utilise le protocole simple Storage Service (S3). Notamment NetApp StorageGRID, IBM Cloud Object Store, Linode, stockage cloud B2, Amazon S3, et bien plus encore.

REMARQUE en utilisant la classification BlueXP qui fait partie du BlueXP principal, vous pouvez maintenant analyser les données StorageGRID. Voir "Analyser les données StorageGRID". Les informations restantes ici ne concernent que les anciennes versions 1.30 et antérieures de la classification BlueXP .

Démarrage rapide

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

1. **Examiner les prérequis en matière de stockage objet**

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

Vous devez disposer de la clé d'accès et de la clé secrète du fournisseur de stockage objet pour que la classification BlueXP puisse accéder aux compartiments.

2. **Déployez l'instance de classification BlueXP**

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

3. **Ajoutez le service de stockage objet**

Ajoutez le service de stockage objet à la classification BlueXP.

4. **Sélectionnez les compartiments à numériser**

Sélectionnez les compartiments que vous souhaitez analyser et la classification BlueXP commencera à les analyser.

Examen des besoins en stockage objet

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 du fournisseur de stockage objet pour que la classification BlueXP puisse accéder aux compartiments.

Déploiement de l'instance de classification BlueXP

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

Si vous analysant des données à partir du stockage objet S3 accessible 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 analysant les données à partir du stockage objet S3 qui a été installé dans un site sombre mais qui n'a pas d'accès à Internet, vous devez "Déployez 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.

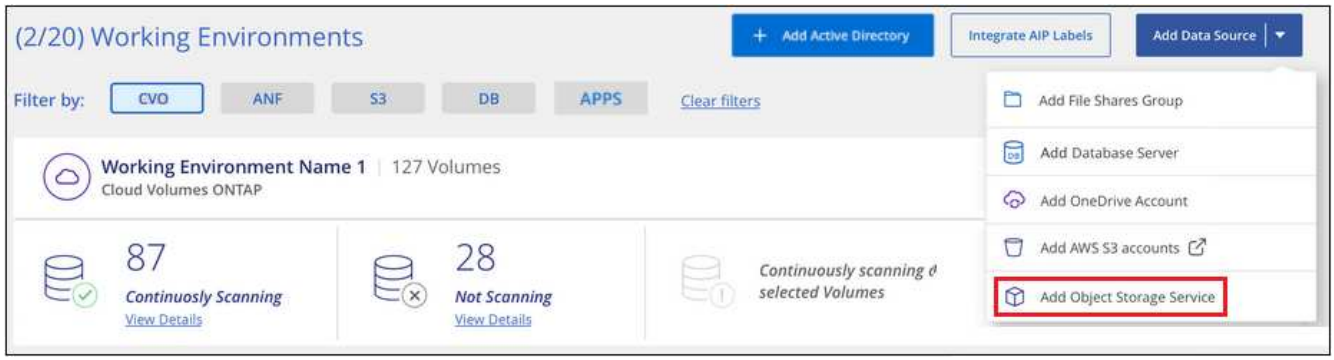
Les mises à niveau du logiciel de classification BlueXP sont automatisées tant que l'instance dispose d'une connectivité Internet.

Ajout du service de stockage objet à la classification BlueXP

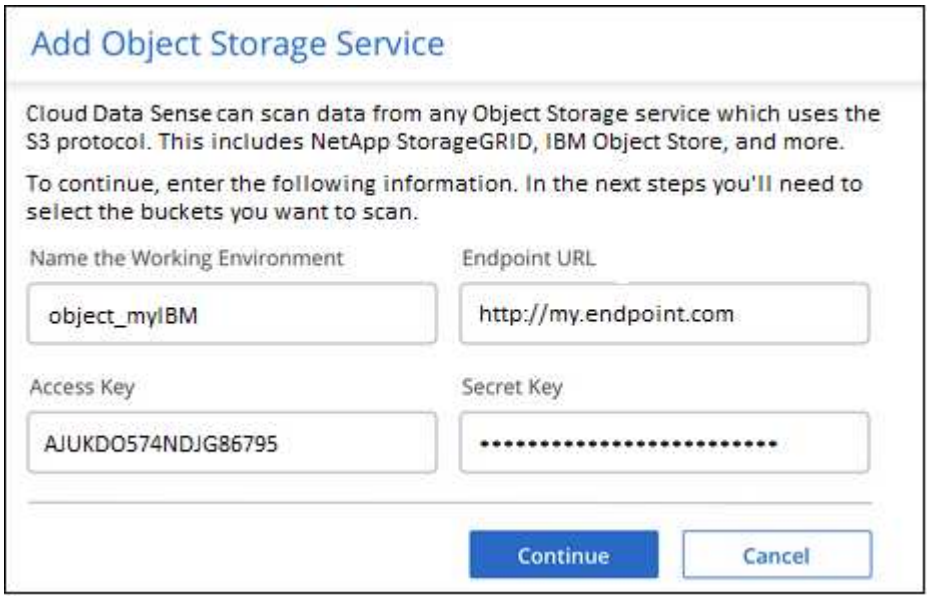
Ajoutez le service de stockage objet.

Étapes

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



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



Résultat

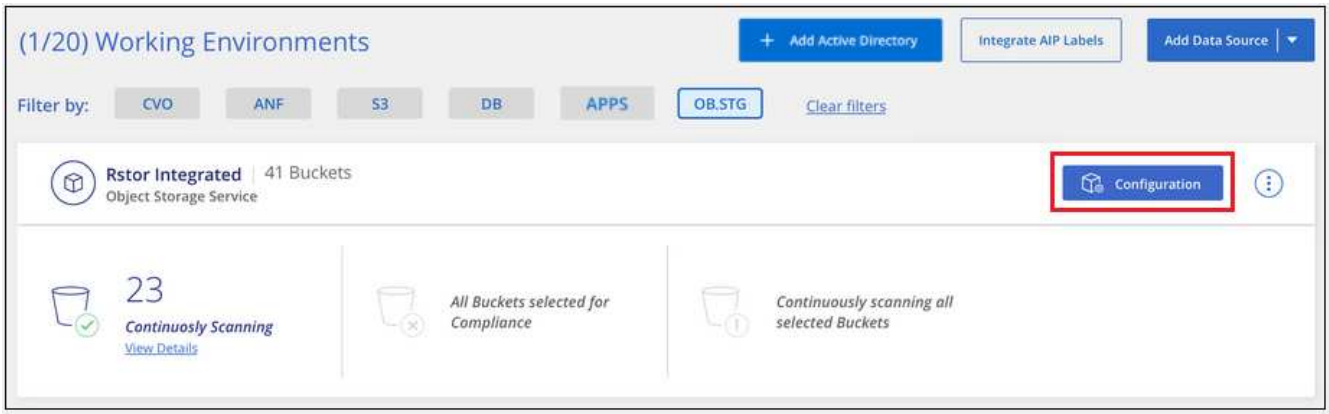
Le nouveau service de stockage objet est ajouté à la liste des environnements de travail.

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

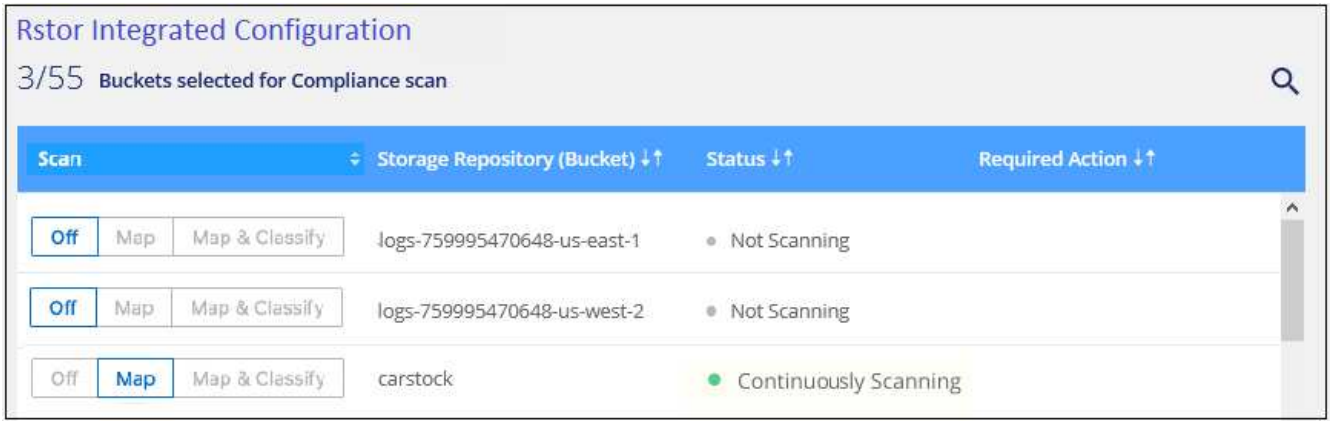
Après avoir activé la classification BlueXP sur votre service de stockage objet, l'étape suivante consiste à configurer les compartiments à analyser. La classification BlueXP détecte ces compartiments et les affiche dans l'environnement de travail que vous avez créé.

Étapes

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



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



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

Résultat

La classification BlueXP commence à analyser les compartiments que vous avez activés. En cas d'erreur, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

Gérer les opérations de données

Affichez les détails de gouvernance de vos données à l'aide du tableau de bord gouvernance

Maîtrisez les coûts liés aux données stockées sur les ressources de stockage de votre entreprise. La classification BlueXP identifie la quantité de données obsolètes, de données non stratégiques, de fichiers en double et de fichiers très volumineux présents dans vos systèmes. Vous pouvez ainsi décider de supprimer ou de déplacer certains fichiers vers un stockage objet moins coûteux.

En outre, si vous prévoyez de migrer des données depuis des emplacements sur site vers le cloud, vous pouvez afficher la taille des données et voir si elles contiennent des informations sensibles avant de les déplacer.

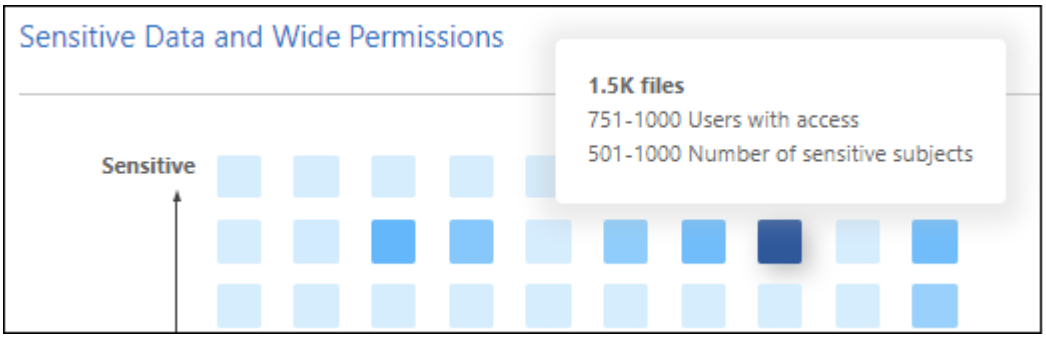
REMARQUE ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP.

Données répertoriées par sensibilité et autorisations étendues dans le tableau de bord de gouvernance

La zone *données sensibles et autorisations étendues* du tableau de bord gouvernance fournit une carte thermique des fichiers contenant des données sensibles (y compris des données personnelles sensibles et sensibles) et qui sont trop permissifs. Cela vous aide à déterminer les risques liés aux données sensibles.

Cela s'applique aux versions 1.30 et antérieures de la classification BlueXP.

Les fichiers sont classés en fonction du nombre d'utilisateurs autorisés à accéder aux fichiers sur l'axe X (le plus bas au plus haut) et du nombre d'identificateurs sensibles dans les fichiers de l'axe y (le plus bas au plus haut). Les blocs représentent le nombre de fichiers correspondant aux éléments des axes X et Y. Le bloc de couleur plus claire est bon, avec moins d'utilisateurs pouvant accéder aux fichiers et avec moins d'identificateurs sensibles par fichier. Les blocs plus sombres sont les éléments que vous pouvez souhaiter examiner. Par exemple, l'écran ci-dessous affiche le texte de l'info-bulle du bloc bleu foncé. Il montre que vous avez 1,500 fichiers où 751-100 utilisateurs ont accès, et où il y a 501-100 identificateurs sensibles par fichier.



Vous pouvez cliquer sur le bloc qui vous intéresse pour afficher les résultats filtrés des fichiers affectés dans la page Investigation afin que vous puissiez en rechercher davantage.

Aucune donnée n'est affichée dans ce panneau si vous n'avez pas intégré de service d'identité avec la classification BlueXP. "Découvrez comment intégrer votre service Active Directory avec la classification BlueXP".

Ce panneau prend en charge les fichiers dans les partages CIFS, les sources de données OneDrive et SharePoint. Actuellement, il n'est pas compatible avec les bases de données, Google Drive, Amazon S3 et le stockage objet générique.

Zone de classification sur le tableau de bord affichant les étiquettes d'AIP

La zone *Classification* du tableau de bord fournit une liste des étiquettes Azure information protection (AIP) les plus identifiées dans vos données numérisées.

Si vous vous êtes abonné à Azure information protection (AIP), vous pouvez classer et protéger les documents et les fichiers en appliquant des étiquettes au contenu. La vérification des étiquettes AIP les plus utilisées qui sont attribuées aux fichiers vous permet de voir les étiquettes les plus utilisées dans vos fichiers.

Voir "Etiquettes AIP" pour en savoir plus.

Organisez vos données privées

La classification BlueXP vous offre de nombreuses façons de gérer et d'organiser vos données privées. Vous pouvez ainsi consulter plus facilement les données qui vous sont les plus importantes.

REMARQUE ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP. La version de décembre 2023 (v1.26.6) a supprimé l'option d'intégration des données à l'aide des étiquettes Azure information protection (AIP).

- Si vous êtes abonné à "Protection des informations Azure (AIP)" Pour classer et protéger vos fichiers, vous pouvez utiliser la classification BlueXP afin de gérer ces étiquettes d'AIP.
- Vous pouvez ajouter des balises aux fichiers que vous souhaitez marquer pour une organisation ou pour un type de suivi.
- Vous pouvez affecter un utilisateur BlueXP à un fichier spécifique ou à plusieurs fichiers, de sorte que cette personne puisse être responsable de la gestion du fichier.
- Grâce à la fonctionnalité « Stratégie », vous pouvez créer vos propres requêtes de recherche personnalisées afin de pouvoir voir facilement les résultats en cliquant sur un bouton.
- Vous pouvez envoyer des alertes par e-mail à des utilisateurs BlueXP ou à toute autre adresse e-mail lorsque certaines stratégies critiques renvoient des résultats.

Les fonctionnalités décrites dans cette section ne sont disponibles que si vous avez choisi d'effectuer une analyse de classification complète sur vos sources de données. Les sources de données qui ont une analyse avec mappage uniquement n'affichent pas de détails au niveau des fichiers.

Dois-je utiliser des étiquettes ou des étiquettes ?

Vous trouverez ci-dessous une comparaison du balisage de classification BlueXP et de l'étiquetage Azure information protection.

Étiquettes	Étiquettes
Les balises de fichier font partie intégrante du classement BlueXP.	Vous devez vous être abonné à Azure information protection (AIP).
La balise n'est conservée que dans la base de données de classification BlueXP, mais pas dans le fichier. Il ne modifie pas le fichier, ni les heures d'accès ou de modification du fichier.	Le libellé fait partie du fichier et, lorsque le libellé change, le fichier change. Cette modification modifie également les heures d'accès et de modification du fichier.
Vous pouvez avoir plusieurs balises sur un seul fichier.	Vous pouvez avoir une étiquette sur un seul fichier.
La balise peut être utilisée pour les actions de classification BlueXP internes, telles que la copie, le déplacement, la suppression, l'exécution d'une règle, etc	Les autres systèmes qui peuvent lire le fichier peuvent voir l'étiquette, qui peut être utilisée pour une automatisation supplémentaire.
Un seul appel API est utilisé pour voir si un fichier a une balise.	

Catégoriser vos données à l'aide d'étiquettes AIP

Si vous vous êtes abonné à, vous pouvez gérer les étiquettes AIP dans les fichiers que la classification BlueXP analyse "Protection des informations Azure (AIP)". AIP vous permet de classer et de protéger les documents et les fichiers en appliquant des étiquettes au contenu. La classification BlueXP vous permet d'afficher les étiquettes déjà attribuées aux fichiers, d'ajouter des étiquettes aux fichiers et de modifier les étiquettes lorsqu'une étiquette existe déjà.

La classification BlueXP prend en charge les étiquettes AIP dans les types de fichiers suivants : .DOC, .DOCX, .PDF, .PPTX, .XLS, .XLSX.

- Vous ne pouvez pas modifier actuellement les étiquettes dans des fichiers de plus de 30 Mo. Pour OneDrive, SharePoint et Google Drive, la taille maximale de fichier est de 4 Mo.
- Si un fichier possède une étiquette qui n'existe plus dans AIP, la classification BlueXP la considère comme un fichier sans étiquette.
- Si vous avez déployé la classification BlueXP dans une région gouvernementale ou dans un emplacement sur site qui n'a pas d'accès à Internet (également appelé site invisible), la fonctionnalité d'étiquette AIP n'est pas disponible.

Intégrez les étiquettes d'AIP dans votre projet ou votre espace de travail

Avant de pouvoir gérer les étiquettes AIP, vous devez intégrer la fonctionnalité d'étiquette AIP dans la classification BlueXP en vous connectant à votre compte Azure existant. Une fois cette option activée, vous pouvez gérer les étiquettes d'AIP dans les fichiers pour tous les "sources des données" éléments de votre projet ou espace de travail BlueXP .

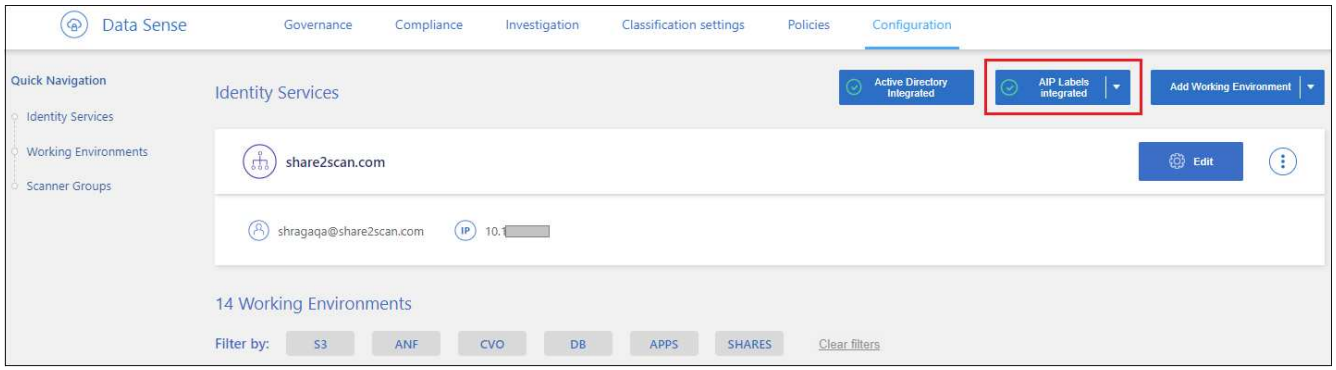
De formation

- Vous devez disposer d'un compte et d'une licence Azure information protection.
- Vous devez disposer des identifiants de connexion pour le compte Azure.
- Si vous prévoyez de modifier les étiquettes dans les fichiers qui résident dans les compartiments Amazon S3, assurez-vous que l'autorisation est requise `s3:PutObject` Est inclus dans le rôle IAM. Voir "Configuration du rôle IAM".

Étapes

1. Sur la page Configuration de la classification BlueXP, cliquez sur **intégrer les étiquettes d'AIP**.

2. Dans la boîte de dialogue intégrer des libellés AIP, cliquez sur **connexion à Azure**.
3. Sur la page Microsoft qui s'affiche, sélectionnez le compte et saisissez les informations d'identification requises.
4. Revenez à l'onglet de classification BlueXP et le message «*AIP Labels ont été intégrés avec le compte <account_name>* » s'affiche.
5. Cliquez sur **Fermer** et vous verrez le texte *AIP Labels Integrated* en haut de la page.



Résultat

Vous pouvez afficher et affecter des libellés AIP à partir du volet des résultats de la page Investigation. Vous pouvez également attribuer des libellés AIP aux fichiers à l'aide de stratégies.

Afficher les étiquettes d'AIP dans vos fichiers

Vous pouvez afficher le libellé AIP actuel attribué à un fichier.

Dans le volet Résultats de l'enquête de données, cliquez sur ⌄ pour que le fichier développe les détails des métadonnées du fichier.

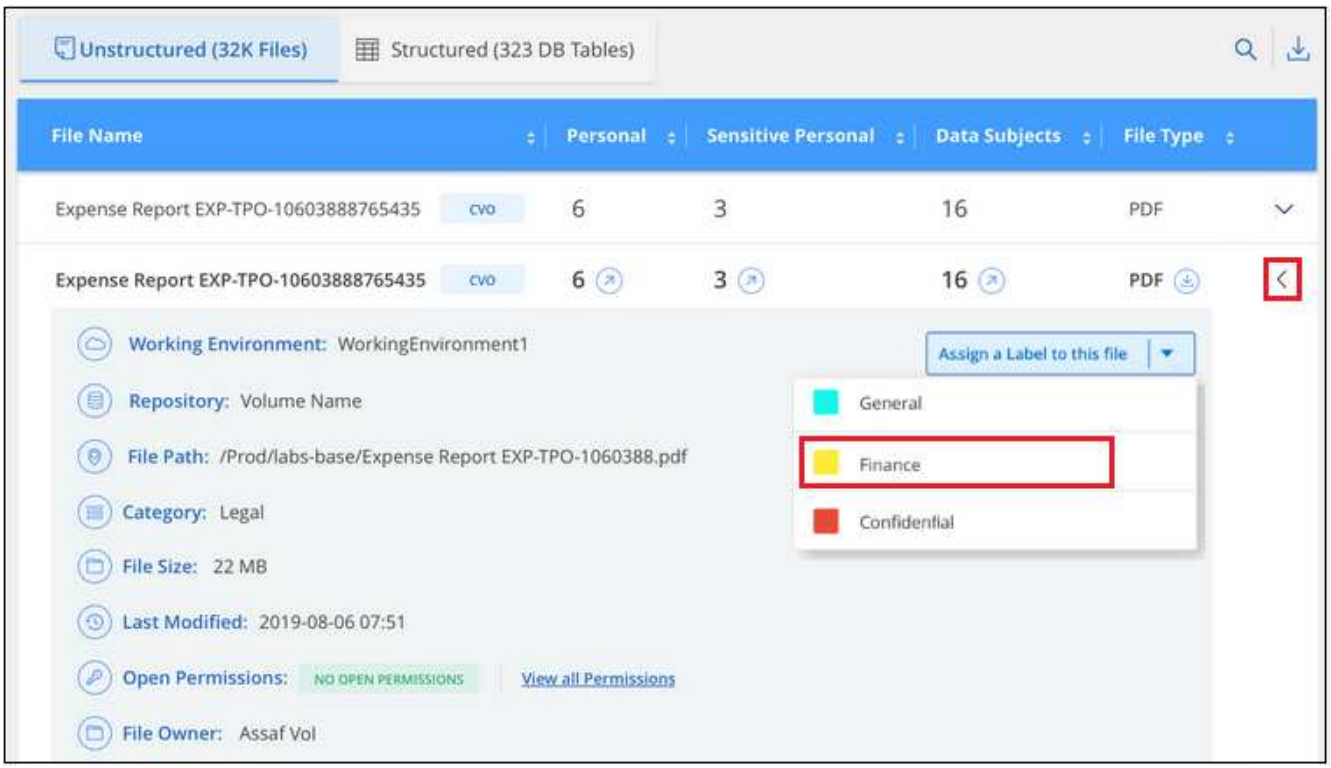
Attribuez manuellement des étiquettes d'AIP

Vous pouvez ajouter, modifier et supprimer des étiquettes d'AIP de vos fichiers à l'aide de la classification BlueXP.

Procédez comme suit pour attribuer un libellé AIP à un seul fichier.

Étapes

1. Dans le volet Résultats de l'enquête de données, cliquez sur ⌄ pour que le fichier développe les détails des métadonnées du fichier.



2. Cliquez sur **attribuer un libellé à ce fichier**, puis sélectionnez le libellé.

   Le libellé apparaît dans les métadonnées du fichier.

Procédez comme suit pour attribuer une étiquette d'AIP à plusieurs fichiers. Notez que vous pouvez attribuer

une étiquette AIP à un maximum de 20 fichiers à la fois (une page dans l'interface utilisateur).

Étapes

1. Dans le volet Résultats de l'enquête de données, sélectionnez le ou les fichiers que vous souhaitez étiqueter.

   - Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (Volume_1).
   - Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (File Name).

2. Dans la barre de boutons, cliquez sur **Label** et sélectionnez le libellé AIP :

   L'étiquette AIP est ajoutée aux métadonnées pour tous les fichiers sélectionnés.

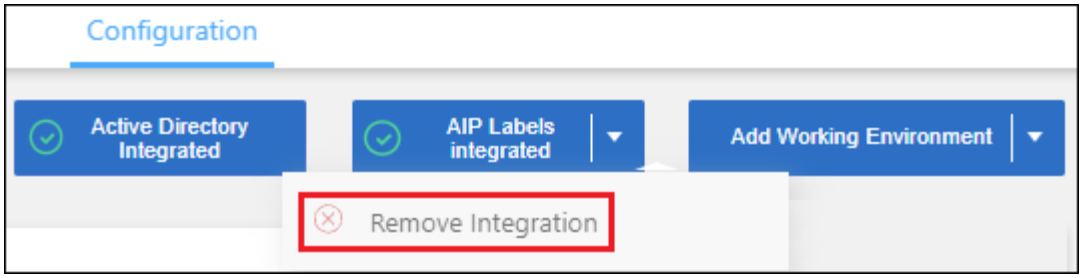
Supprimez l'intégration AIP

Si vous ne souhaitez plus pouvoir gérer les étiquettes AIP dans les fichiers, vous pouvez supprimer le compte AIP de l'interface de classification BlueXP.

Notez qu'aucune modification n'est apportée aux étiquettes que vous avez ajoutées à l'aide de la classification BlueXP. Les étiquettes qui existent dans les fichiers resteront telles qu'elles existent actuellement.

Étapes

1. Dans la page *Configuration*, cliquez sur **libellés AIP intégrés > Supprimer intégration**.



2. Cliquez sur **Supprimer l'intégration** dans la boîte de dialogue de confirmation.

Appliquez des balises pour gérer vos fichiers numérisés

Vous pouvez ajouter une balise aux fichiers que vous souhaitez marquer pour un type de suivi. Par exemple, vous avez peut-être trouvé des fichiers en double et vous voulez en supprimer un, mais vous devez vérifier lequel supprimer. Vous pouvez ajouter une balise « vérifier pour supprimer » au fichier afin que vous sachiez que ce fichier nécessite une recherche et un certain type d'action future.

La classification BlueXP vous permet d'afficher les balises attribuées aux fichiers, d'ajouter ou de supprimer des balises des fichiers, et de modifier le nom ou de supprimer une balise existante.

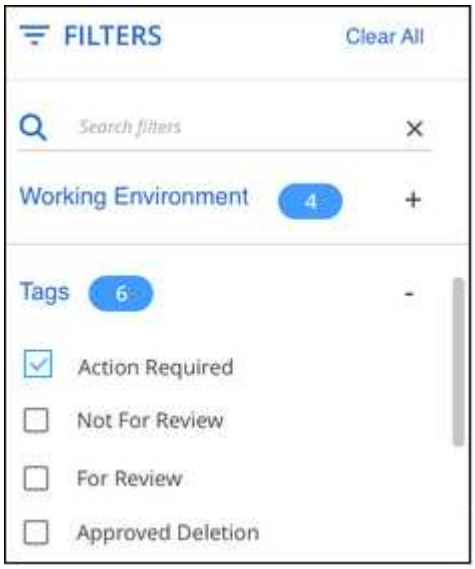
Notez que la balise n'est pas ajoutée au fichier de la même manière que les étiquettes AIP font partie des métadonnées du fichier. La balise est visible par les utilisateurs BlueXP via la classification BlueXP. Vous pouvez ainsi voir si un fichier doit être supprimé ou vérifié pour un certain type de suivi.

> Les balises attribuées aux fichiers de la classification BlueXP ne sont pas liées aux balises que vous pouvez ajouter à des ressources, telles que des volumes ou des instances de machines virtuelles. Les balises de classification BlueXP sont appliquées au niveau des fichiers.

Afficher les fichiers auxquels certaines balises sont appliquées

Vous pouvez afficher tous les fichiers auxquels des étiquettes spécifiques sont attribuées.

1. Cliquez sur l'onglet **Investigation** de la classification BlueXP.
2. Dans la page recherche de données, cliquez sur **balises** dans le volet filtres, puis sélectionnez les balises requises.



Le volet Résultats de l'enquête affiche tous les fichiers auxquels ces balises sont affectées.

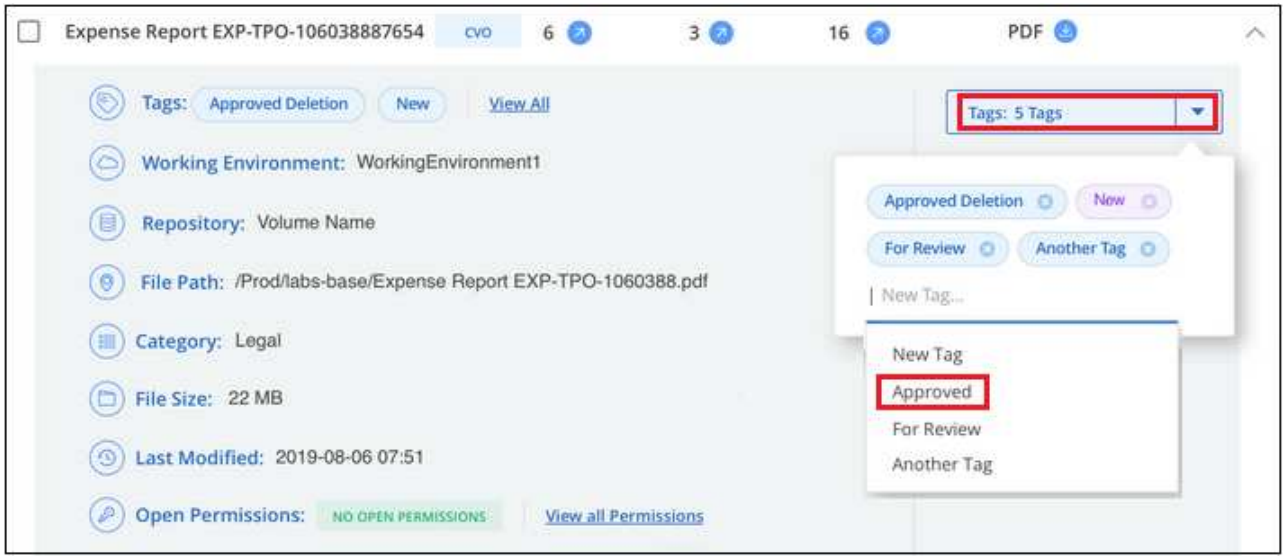
Attribuez des balises aux fichiers

Vous pouvez ajouter des balises à un seul fichier ou à un groupe de fichiers.

Pour ajouter une balise à un seul fichier :

Étapes

1. Dans le volet Résultats de l'enquête de données, cliquez sur ⌄ pour que le fichier développe les détails des métadonnées du fichier.
2. Cliquez sur le champ **Tags** pour afficher les balises actuellement affectées.
3. Ajoutez la ou les balises :
   - Pour affecter une balise existante, cliquez dans le champ **Nouvelle balise…** et commencez à taper le nom de la balise. Lorsque la balise que vous cherchez s'affiche, sélectionnez-la et appuyez sur **entrée**.
   - Pour créer une nouvelle balise et l'affecter au fichier, cliquez dans le champ **Nouvelle balise…**, saisissez le nom de la nouvelle balise et appuyez sur **entrée**.



La balise s'affiche dans les métadonnées de fichier.

Pour ajouter une balise à plusieurs fichiers :

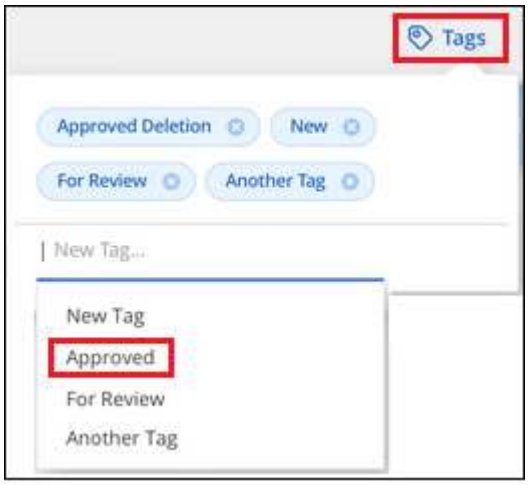
Étapes

1. Dans le volet Résultats de l'enquête de données, sélectionnez le ou les fichiers que vous souhaitez marquer.

- Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (Volume_1).
- Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (File Name).
- Pour sélectionner tous les fichiers sur toutes les pages, cochez la case dans la ligne de titre (File Name), puis dans le message contextuel All **20** Items on this page selected Select all Items in list (63K Items), Cliquez sur **Sélectionner tous les éléments de la liste (xxx items)**.

  Vous pouvez appliquer des balises à un maximum de 100,000 fichiers à la fois.

2. Dans la barre de boutons, cliquez sur **Tags** et les balises actuellement affectées sont affichées.
3. Ajoutez la ou les balises :
   - Pour affecter une balise existante, cliquez dans le champ **Nouvelle balise…** et commencez à taper le nom de la balise. Lorsque la balise que vous cherchez s'affiche, sélectionnez-la et appuyez sur **entrée**.
   - Pour créer une nouvelle balise et l'affecter au fichier, cliquez dans le champ **Nouvelle balise…**, saisissez le nom de la nouvelle balise et appuyez sur **entrée**.



4. Approuver l'ajout des balises dans la boîte de dialogue de confirmation et les balises sont ajoutées aux métadonnées pour tous les fichiers sélectionnés.

Supprimez les balises des fichiers

Vous pouvez supprimer une balise si vous n'avez plus besoin de l'utiliser.

Il vous suffit de cliquer sur **x** pour obtenir une balise existante.

Si vous avez sélectionné plusieurs fichiers, la balise est supprimée de tous les fichiers.

Affecter des utilisateurs à la gestion de certains fichiers

Vous pouvez affecter un utilisateur BlueXP à un fichier spécifique ou à plusieurs fichiers, de sorte que personne puisse être responsable des actions de suivi qui doivent être effectuées sur le fichier. Cette fonctionnalité est souvent utilisée avec la fonction pour ajouter des balises d'état personnalisées à un fichier.

Par exemple, vous pouvez avoir un fichier contenant certaines données personnelles qui autorise un trop grand nombre d'utilisateurs à accéder en lecture et en écriture (autorisations ouvertes). Vous pouvez donc attribuer l'étiquette d'état « Modifier les autorisations » et attribuer ce fichier à l'utilisateur « Joan Smith » afin qu'il puisse décider comment résoudre le problème. Lorsqu'ils ont résolu le problème, ils peuvent changer l'étiquette d'état en « terminé ».

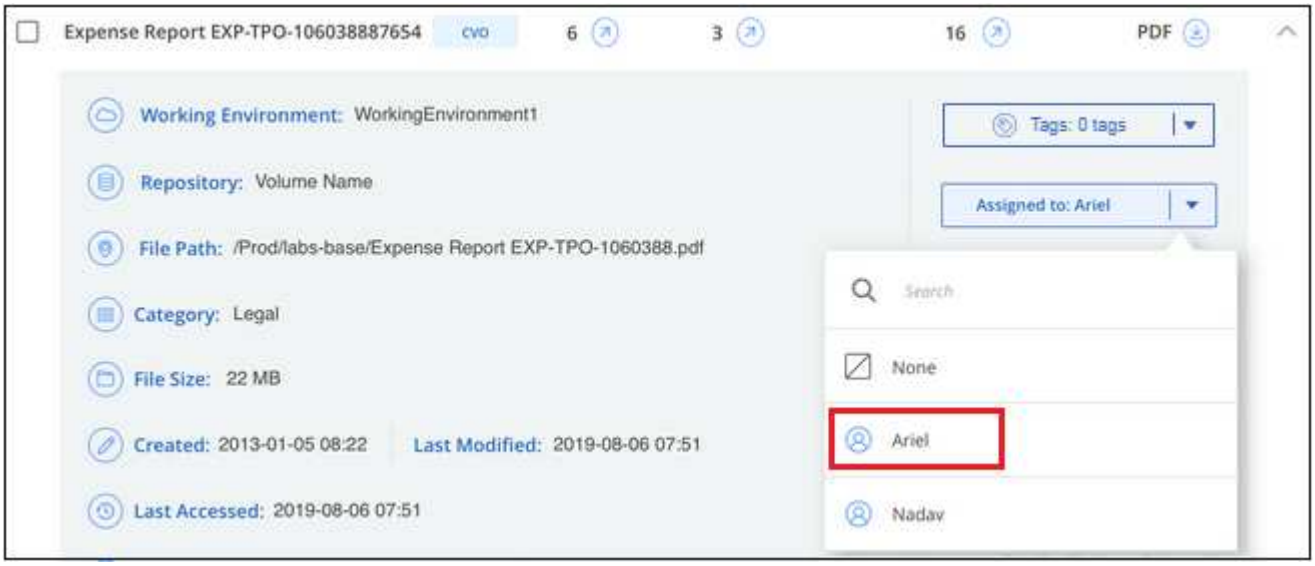
Notez que le nom d'utilisateur n'est pas ajouté au fichier dans le cadre des métadonnées de fichier. Il est vu juste par les utilisateurs BlueXP lors de l'utilisation de la classification BlueXP.

Un nouveau filtre dans la page Investigation vous permet d'afficher facilement tous les fichiers qui ont la même personne dans le champ « assigné à ».

Procédez comme suit pour attribuer un utilisateur à un seul fichier.

Étapes

1. Dans le volet Résultats de l'enquête de données, cliquez sur ⌄ pour que le fichier développe les détails des métadonnées du fichier.
2. Cliquez sur le champ **affecté à** et sélectionnez le nom d'utilisateur.



   Le nom d'utilisateur apparaît dans les métadonnées de fichier.

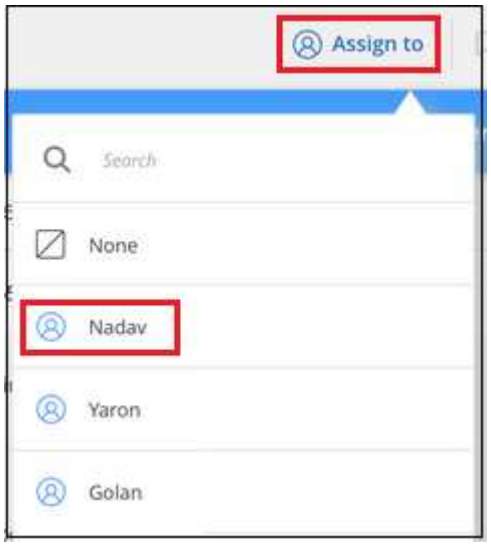
Procédez comme suit pour attribuer un utilisateur à plusieurs fichiers. Notez que vous pouvez affecter un utilisateur à un maximum de 20 fichiers à la fois (une page dans l'interface utilisateur).

Étapes

1. Dans le volet Résultats de l'enquête de données, sélectionnez le ou les fichiers que vous souhaitez attribuer à un utilisateur.

   - Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (Volume_1).
   - Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (File Name).

2. Dans la barre de boutons, cliquez sur **affecter à** et sélectionnez le nom d'utilisateur :



   L'utilisateur est ajouté aux métadonnées pour tous les fichiers sélectionnés.

Gérez vos données privées

La classification BlueXP offre de nombreuses méthodes pour gérer vos données privées. Certaines fonctionnalités facilitent la préparation de la migration des données, tandis que d'autres vous permettent de modifier ces dernières.

> **REMARQUE** ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP.

- Vous pouvez copier des fichiers vers un partage NFS de destination si vous souhaitez effectuer une copie de certaines données et les déplacer vers un autre emplacement NFS.
- Vous pouvez cloner un volume ONTAP sur un nouveau volume, tout en incluant uniquement les fichiers sélectionnés du volume source dans le nouveau volume cloné. Cette fonction est utile lorsque vous migrez des données et que vous souhaitez exclure certains fichiers du volume d'origine.
- Vous pouvez copier et synchroniser des fichiers d'un référentiel source vers un répertoire dans un emplacement de destination spécifique. Cette fonction s'avère utile dans les cas où vous migrez des données d'un système source vers un autre alors que les fichiers source continuent à avoir une activité finale.
- Vous pouvez déplacer les fichiers source numérisés par la classification BlueXP vers n'importe quel partage NFS.
- Vous pouvez supprimer des fichiers qui semblent non sécurisés ou trop risqués pour l'éviter dans votre système de stockage, ou que vous avez identifiés comme doublons.

> - Les fonctionnalités décrites dans cette section ne sont disponibles que si vous avez choisi d'effectuer une analyse de classification complète sur vos sources de données. Les sources de données qui ont une analyse avec mappage uniquement n'affichent pas de détails au niveau des fichiers.
> - Les données des comptes Google Drive ne peuvent pas actuellement utiliser ces fonctionnalités.

Copier les fichiers source

Vous pouvez copier tous les fichiers source numérisés par la classification BlueXP. Il existe trois types d'opérations de copie en fonction de l'objectif que vous essayez d'effectuer :

- **Copier des fichiers** de volumes ou de sources de données identiques ou différentes vers un partage NFS de destination.

  Cette fonction est utile pour effectuer une copie de certaines données et les déplacer vers un autre emplacement NFS.

- **Cloner un volume ONTAP** sur un nouveau volume dans le même agrégat, mais inclure uniquement les fichiers sélectionnés du volume source dans le nouveau volume cloné.

  Cette fonction est utile lorsque vous migrez des données et que vous souhaitez exclure certains fichiers du volume d'origine. Cette action utilise le "NetApp FlexClone ®" fonctionnalité permettant de dupliquer rapidement le volume, puis de supprimer les fichiers que vous avez sélectionnés.

- **Copier et synchroniser des fichiers** à partir d'un référentiel source unique (volume ONTAP, compartiment S3, partage NFS, etc.) vers un répertoire dans un emplacement de destination spécifique (cible).

  Cette fonction est utile lorsque vous migrez des données d'un système source vers un autre. Après la copie initiale, le service synchronise toutes les données modifiées en fonction de la planification que vous avez définie. Cette action utilise le "Copie et synchronisation NetApp BlueXP" fonctionnalité permettant de copier et de synchroniser les données d'une source vers une cible.

Copier les fichiers source vers un partage NFS

Vous pouvez copier les fichiers source numérisés par la classification BlueXP vers n'importe quel partage NFS. Le partage NFS n'a pas besoin d'être intégré à la classification BlueXP, il vous suffit de connaître le nom

du partage NFS où tous les fichiers sélectionnés seront copiés au format `<host_name>:/<share_path>`.

> Vous ne pouvez pas copier les fichiers qui résident dans les bases de données.

De formation

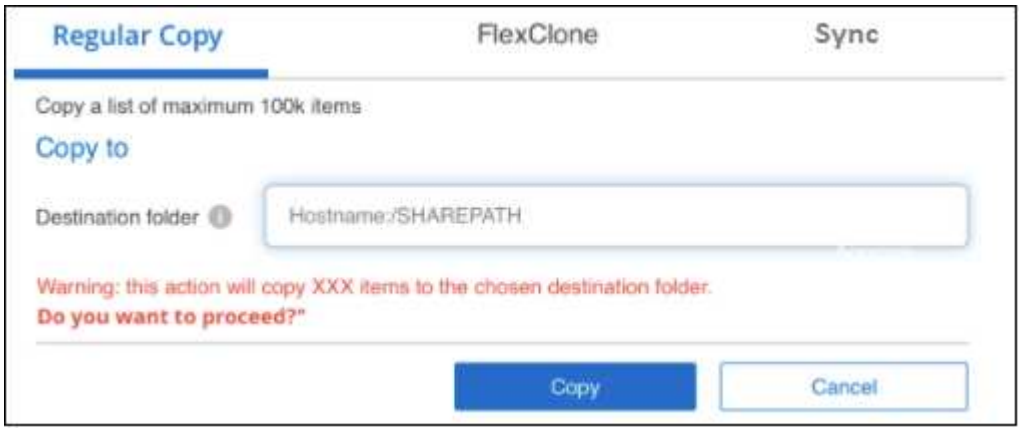
- Vous devez disposer des autorisations nécessaires pour copier des fichiers. "En savoir plus sur l'accès des utilisateurs aux informations de conformité".
- La copie de fichiers nécessite que le partage NFS de destination autorise l'accès à partir de l'instance de classification BlueXP.
- Vous pouvez copier entre 1 et 100,000 fichiers à la fois.

Étapes

1. Dans le volet Résultats de l'enquête de données, sélectionnez le ou les fichiers que vous souhaitez copier, puis cliquez sur **Copier**.

   - Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (Volume_1).
   - Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (File Name).
   - Pour sélectionner tous les fichiers sur toutes les pages, cochez la case dans la ligne de titre (File Name), puis dans le message contextuel All **20** Items on this page selected Select all Items in list (63K Items), Cliquez sur **Sélectionner tous les éléments de la liste (xxx items)**.

2. Dans la boîte de dialogue *Copy Files*, sélectionnez l'onglet **Regular Copy**.



3. Entrez le nom du partage NFS dans lequel tous les fichiers sélectionnés seront copiés au format `<host_name>:/<share_path>`, Puis cliquez sur **copie**.

   Une boîte de dialogue apparaît avec l'état de l'opération de copie.

Vous pouvez afficher la progression de l'opération de copie dans "Volet État des actions".

Notez que vous pouvez également copier un fichier individuel lors de l'affichage des détails de métadonnées d'un fichier. Cliquez simplement sur **Copier fichier**.

Cloner des données de volume vers un nouveau volume

Vous pouvez cloner un volume ONTAP existant que la classification BlueXP analyse à l'aide de la fonctionnalité NetApp *FlexClone*. Cela vous permet de dupliquer le volume rapidement tout en incluant uniquement les fichiers que vous avez sélectionnés. Cela est utile si vous migrez des données et que vous souhaitez exclure certains fichiers du volume d'origine, ou si vous souhaitez créer une copie d'un volume pour le test.

Le nouveau volume est créé dans le même agrégat que le volume source. Assurez-vous de disposer d'un espace suffisant pour ce nouveau volume dans l'agrégat avant de commencer cette tâche. Contactez votre administrateur du stockage si nécessaire.

Remarque : les volumes FlexGroup ne peuvent pas être clonés, car ils ne sont pas pris en charge par FlexClone.

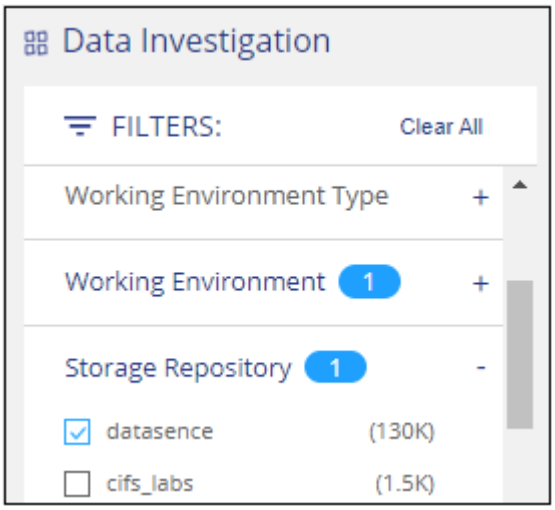
De formation

- Vous devez disposer des autorisations nécessaires pour copier des fichiers. "En savoir plus sur l'accès des utilisateurs aux informations de conformité".
- Vous devez sélectionner au moins 20 fichiers.
- Tous les fichiers sélectionnés doivent se trouver dans le même volume et le volume doit être en ligne.
- Le volume doit correspondre à un système Cloud Volumes ONTAP ou ONTAP sur site. Aucune autre source de données n'est actuellement prise en charge.
- La licence FlexClone doit être installée sur le cluster. Cette licence est installée par défaut sur les systèmes Cloud Volumes ONTAP.

Étapes

1. Dans le volet enquête de données, créez un filtre en sélectionnant un seul **Environnement de travail** et un seul **référentiel de stockage** pour vous assurer que tous les fichiers proviennent du même volume

ONTAP.

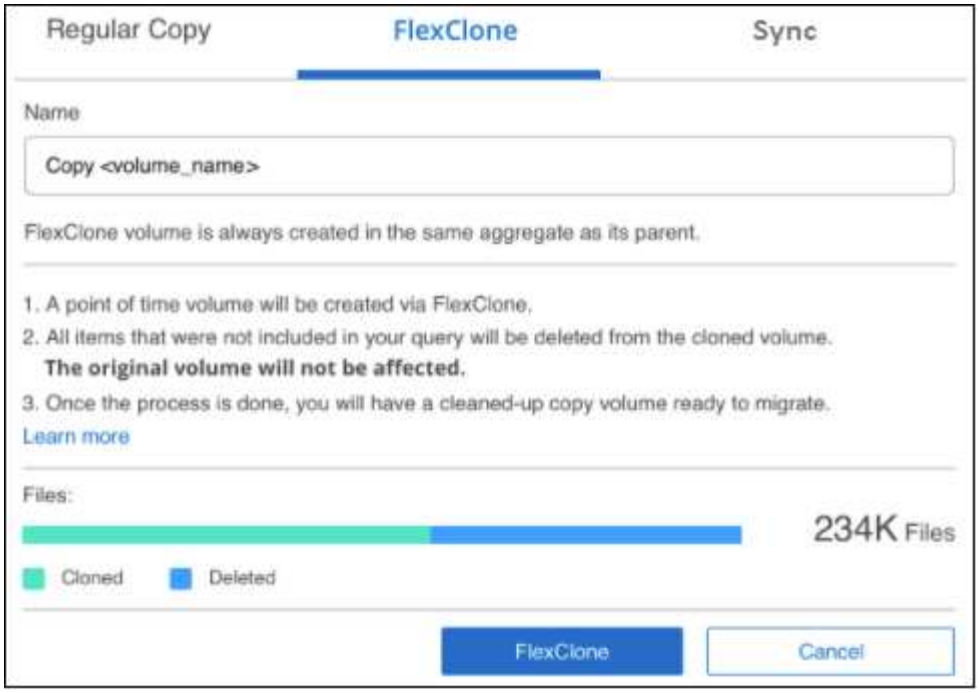


Appliquez tous les autres filtres afin que vous ne voyez que les fichiers que vous souhaitez cloner vers le nouveau volume.

2. Dans le volet Résultats de l'enquête, sélectionnez les fichiers à cloner et cliquez sur **Copier**.

- Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (Volume_1).
- Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (File Name).
- Pour sélectionner tous les fichiers sur toutes les pages, cochez la case dans la ligne de titre (File Name), puis dans le message contextuel All **20** Items on this page selected Select all Items in list (63K Items), Cliquez sur **Sélectionner tous les éléments de la liste (xxx items)**.

3. Dans la boîte de dialogue *Copy Files*, sélectionnez l'onglet **FlexClone**. Cette page affiche le nombre total de fichiers qui seront clonés à partir du volume (fichiers que vous avez sélectionnés) et le nombre de fichiers qui ne sont pas inclus/supprimés (fichiers que vous n'avez pas sélectionnés) du volume cloné.



4. Entrez le nom du nouveau volume et cliquez sur **FlexClone**.

   Une boîte de dialogue affichant l'état de l'opération de clonage s'affiche.

Résultat

Le nouveau volume cloné est créé dans le même agrégat que le volume source.

Vous pouvez afficher la progression de l'opération de clonage dans "Volet État des actions".

Si vous avez initialement sélectionné **Mapper tous les volumes** ou **Mapper et classer tous les volumes** lorsque vous avez activé la classification BlueXP pour l'environnement de travail où réside le volume source, la classification BlueXP analyse automatiquement le nouveau volume cloné. Si vous n'avez pas utilisé l'une ou l'autre de ces sélections au départ, vous devrez effectuer une acquisition pour ce nouveau volume "activer la numérisation sur le volume manuellement".

Copie et synchronisation des fichiers source sur un système cible

Vous pouvez copier les fichiers source numérisés par la classification BlueXP depuis n'importe quelle source de données non structurées prise en charge vers un répertoire situé dans un emplacement cible spécifique ("Emplacements cibles pris en charge par la copie et la synchronisation BlueXP"). Après la copie initiale, toutes les données modifiées dans les fichiers sont synchronisées en fonction du calendrier que vous configurez.

Cette fonction est utile lorsque vous migrez des données d'un système source vers un autre. Cette action utilise le "Copie et synchronisation NetApp BlueXP" fonctionnalité permettant de copier et de synchroniser les données d'une source vers une cible.

> Vous ne pouvez pas copier et synchroniser les fichiers qui résident dans les bases de données, les comptes OneDrive ou les comptes SharePoint.

De formation

- Vous devez disposer des autorisations nécessaires pour copier et synchroniser des fichiers. "En savoir

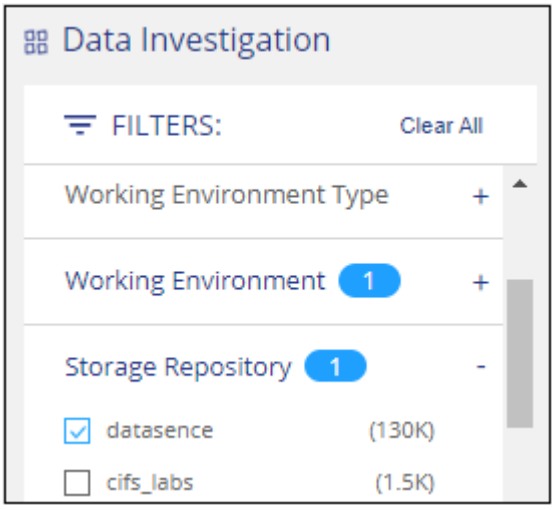
plus sur l'accès des utilisateurs aux informations de conformité".

- Vous devez sélectionner au moins 20 fichiers.
- Tous les fichiers sélectionnés doivent se trouver dans le même référentiel source (volume ONTAP, compartiment S3, partage NFS ou CIFS, etc.).
- Vous devrez activer le service de copie et de synchronisation BlueXP et configurer au moins un courtier de données pouvant être utilisé pour transférer les fichiers entre les systèmes source et cible. Vérifiez les exigences de copie et de synchronisation BlueXP depuis le "Description de Quick Start".

  Notez que le service de copie et de synchronisation BlueXP entraîne des frais de service distincts pour vos relations synchronisées et des frais de ressources si vous déployez le courtier en données dans le cloud.

Étapes

1. Dans le volet investigation de données, créez un filtre en sélectionnant un seul **Environnement de travail** et un seul **référentiel de stockage** pour vous assurer que tous les fichiers proviennent du même référentiel.

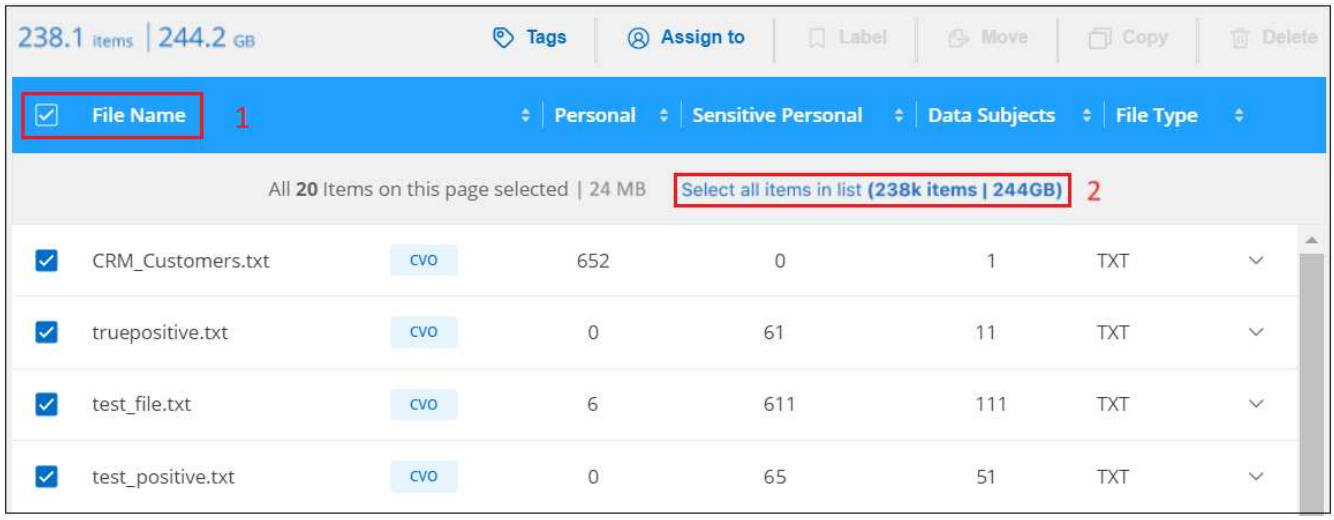


   Appliquez tous les autres filtres de sorte que vous ne voyez que les fichiers que vous voulez copier et synchroniser vers le système de destination.

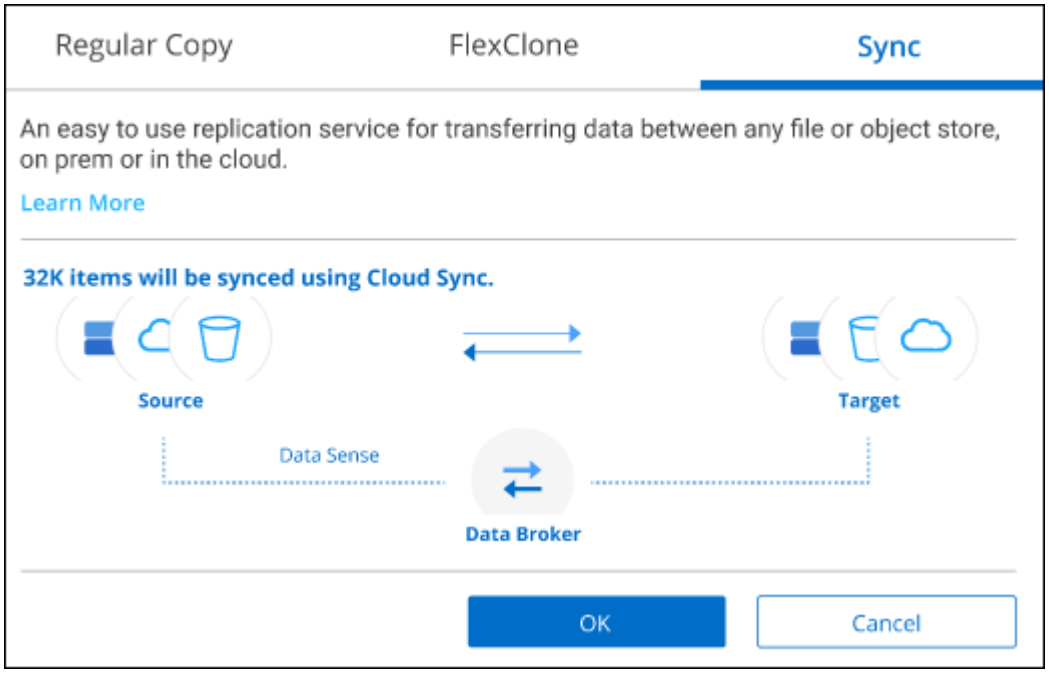
2. Dans le volet Résultats de l'enquête, sélectionnez tous les fichiers sur toutes les pages en cochant la case dans la ligne de titre (

), puis dans le message contextuel 

Cliquez sur **Sélectionner tous les éléments de la liste (xxx items)**, puis sur **Copier**.



3. Dans la boîte de dialogue *Copy Files*, sélectionnez l'onglet **Sync**.



4. Si vous êtes sûr de vouloir synchroniser les fichiers sélectionnés vers un emplacement de destination, cliquez sur **OK**.

   La copie et l'interface de synchronisation BlueXP sont ouvertes dans BlueXP.

   Vous êtes invité à définir la relation de synchronisation. Le système source est pré-rempli en fonction du référentiel et des fichiers que vous avez déjà sélectionnés dans la classification BlueXP.

5. Vous devez sélectionner le système cible, puis sélectionner (ou créer) le courtier de données que vous prévoyez d'utiliser. Vérifiez les exigences de copie et de synchronisation BlueXP depuis le "Description de Quick Start".

Résultat

Les fichiers sont copiés sur le système cible et ils seront synchronisés en fonction du planning que vous définissez. Si vous sélectionnez une synchronisation unique, les fichiers sont copiés et synchronisés une seule fois. Si vous choisissez une synchronisation périodique, les fichiers sont synchronisés en fonction du planning.

Notez que si le système source ajoute de nouveaux fichiers qui correspondent à la requête que vous avez créée à l'aide de filtres, ces *nouveaux* fichiers seront copiés vers la destination et synchronisés ultérieurement.

Notez que certaines des opérations habituelles de copie et de synchronisation BlueXP sont désactivées lorsqu'elles sont invoquées à partir de la classification BlueXP :

- Vous ne pouvez pas utiliser les boutons **Supprimer les fichiers sur la source** ou **Supprimer les fichiers sur la cible**.
- L'exécution d'un rapport est désactivée.

Déplacer les fichiers source vers un partage NFS

Vous pouvez déplacer les fichiers source numérisés par la classification BlueXP vers n'importe quel partage NFS. Le partage NFS n'a pas besoin d'être intégré à la classification BlueXP.

Vous pouvez également laisser un fichier de navigation à l'emplacement du fichier déplacé. Un fichier de navigation permet à vos utilisateurs de comprendre pourquoi un fichier a été déplacé de son emplacement d'origine. Pour chaque fichier déplacé, le système crée un fichier de navigation à l'emplacement source nommé `<filename>-breadcrumb-<date>.txt`. Vous pouvez ajouter du texte dans la boîte de dialogue qui sera ajoutée au fichier de navigation pour indiquer l'emplacement où le fichier a été déplacé et l'utilisateur qui a déplacé le fichier.

Notez que la structure de sous-répertoires du fichier source est recréée sur le partage de destination lorsque le fichier est déplacé, de sorte qu'il est plus facile de comprendre l'emplacement d'où le fichier a été déplacé. Si un fichier du même nom existe dans l'emplacement de destination, le fichier ne sera pas déplacé.

Vous ne pouvez pas déplacer les fichiers qui résident dans les bases de données.

De formation

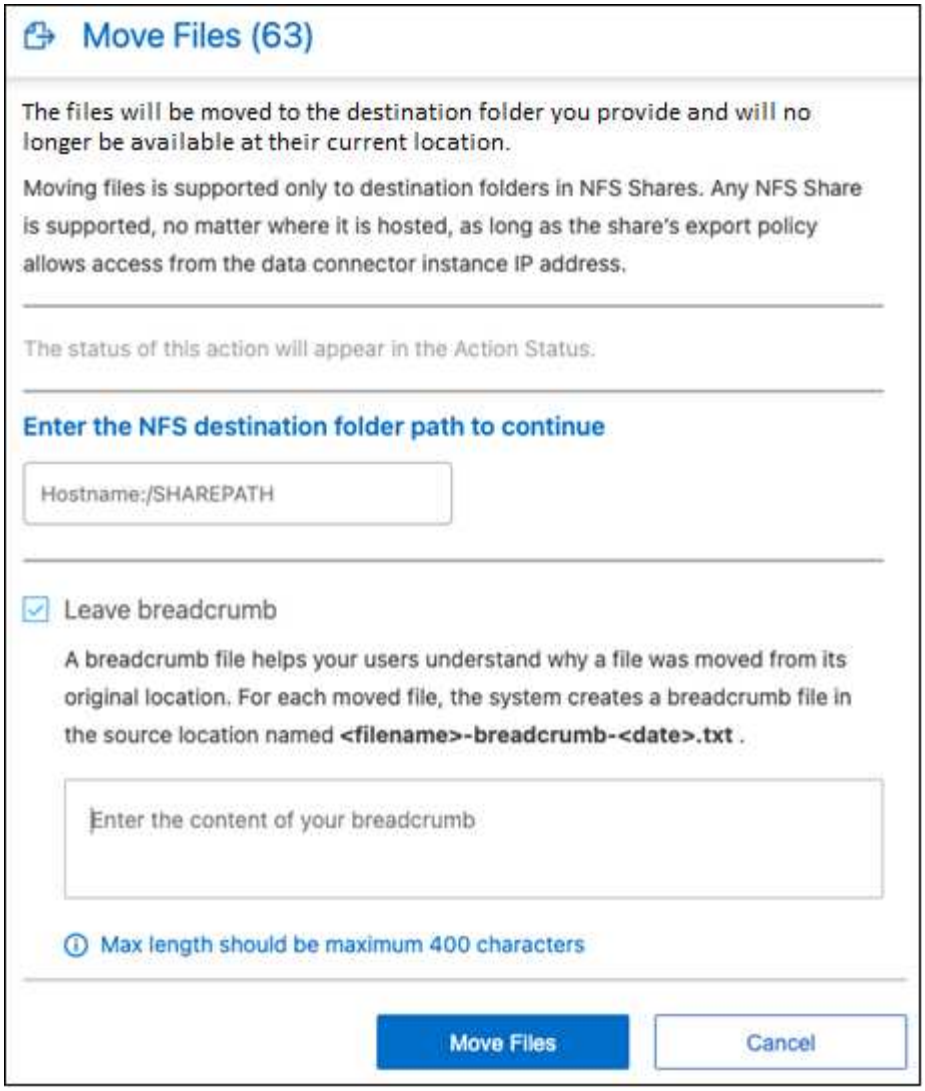
- Vous devez disposer des autorisations nécessaires pour déplacer des fichiers. "En savoir plus sur l'accès des utilisateurs aux informations de conformité".
- Les fichiers source peuvent se trouver dans les sources de données suivantes : systèmes ONTAP sur site, Cloud Volumes ONTAP, Azure NetApp Files, partages de fichiers et SharePoint Online.
- Vous pouvez déplacer jusqu'à 15 millions de fichiers à la fois.
- Seuls les fichiers de 50 Mo ou moins sont déplacés.
- Le partage NFS de destination doit autoriser l'accès à partir de l'adresse IP de l'instance de classification BlueXP.

Étapes

1. Dans le volet Résultats de l'enquête de données, sélectionnez le ou les fichiers que vous souhaitez déplacer.

- Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (Volume_1).
- Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (File Name).
- Pour sélectionner tous les fichiers sur toutes les pages, cochez la case dans la ligne de titre (File Name), puis dans le message contextuel All **20** Items on this page selected Select all Items in list (63K Items), Cliquez sur **Sélectionner tous les éléments de la liste (xxx items)**.

2. Dans la barre de boutons, cliquez sur **déplacer**.



3. Dans la boîte de dialogue *Move Files*, entrez le nom du partage NFS dans lequel tous les fichiers sélectionnés seront déplacés au format `<host_name>:/<share_path>`.
4. Si vous voulez laisser un fichier de navigation, cochez la case *laisser fil fil fil fil fil à fil*. Vous pouvez entrer du texte dans la boîte de dialogue pour indiquer l'emplacement où le fichier a été déplacé et l'utilisateur qui a déplacé le fichier, ainsi que toute autre information, comme la raison pour laquelle le fichier a été déplacé.
5. Cliquez sur **déplacer les fichiers**.

Notez que vous pouvez également déplacer un fichier individuel lors de l'affichage des détails de métadonnées d'un fichier. Cliquez simplement sur **déplacer le fichier**.

Supprimer les fichiers source

Vous pouvez supprimer de manière définitive les fichiers source qui semblent non sécurisés ou trop risqués pour laisser dans votre système de stockage, ou que vous avez identifiés comme un doublon. Cette action est permanente et il n'y a pas d'annulation ou de restauration.

Vous pouvez supprimer des fichiers manuellement à partir du volet Investigation, ou "Utiliser automatiquement des règles".

> Vous ne pouvez pas supprimer les fichiers qui résident dans les bases de données. Toutes les autres sources de données sont prises en charge.

La suppression de fichiers nécessite les autorisations suivantes :

- Pour les données NFS : il est nécessaire de définir la export policy avec les autorisations d'écriture.
- Pour les données CIFS, les identifiants CIFS doivent disposer d'autorisations d'écriture.
- Pour les données S3, le rôle IAM doit inclure les autorisations suivantes : `s3:DeleteObject`.

Supprimez les fichiers source manuellement

De formation

- Vous devez disposer des autorisations nécessaires pour supprimer des fichiers. "En savoir plus sur l'accès des utilisateurs aux informations de conformité".
- Vous pouvez supprimer un maximum de 100,000 fichiers à la fois.

Étapes

1. Dans le volet Résultats de l'enquête de données, sélectionnez le ou les fichiers que vous souhaitez supprimer.

- Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (Volume_1).
- Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (File Name).
- Pour sélectionner tous les fichiers sur toutes les pages, cochez la case dans la ligne de titre (File Name), puis dans le message contextuel All **20** Items on this page selected Select all Items in list (63K Items), Cliquez sur **Sélectionner tous les éléments de la liste (xxx items)**.

2. Dans la barre de boutons, cliquez sur **Supprimer**.
3. Comme l'opération de suppression est permanente, vous devez taper "**définitivement delete**" dans la boîte de dialogue *Delete File* suivante et cliquer sur **Delete File**.

Vous pouvez afficher la progression de l'opération de suppression dans "Volet État des actions".

Notez que vous pouvez également supprimer un fichier individuel lors de l'affichage des détails de métadonnées d'un fichier. Cliquez simplement sur **Supprimer le fichier**.

Ajoutez des identifiants de données personnels à vos analyses de classification BlueXP

La classification BlueXP offre de nombreuses façons d'ajouter une liste personnalisée des « données personnelles » que la classification BlueXP identifiera dans les analyses futures. Vous disposez ainsi d'une vue d'ensemble sur l'emplacement des données potentiellement sensibles dans *tous* les fichiers de votre entreprise.

REMARQUE ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP.

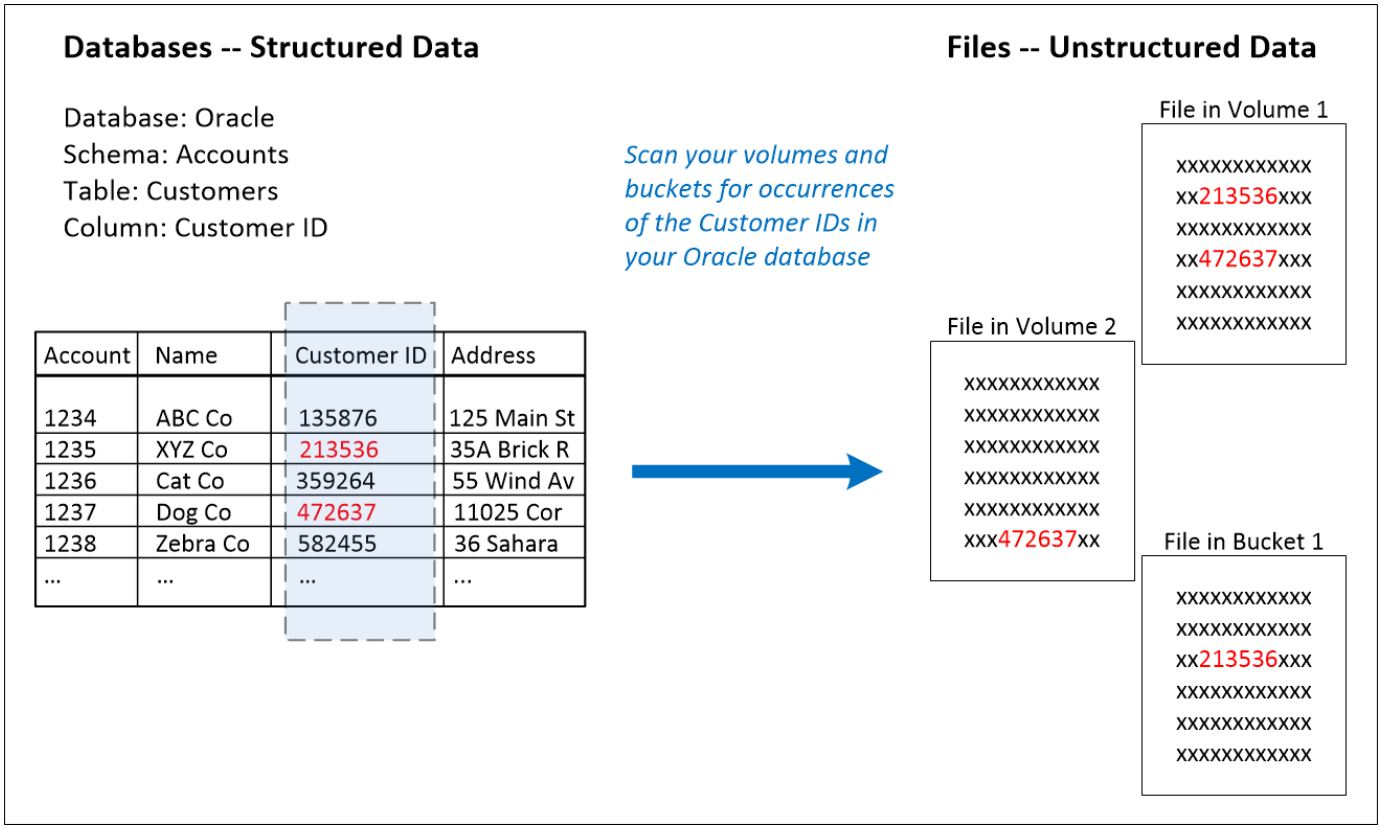
- Vous pouvez ajouter des identificateurs uniques basés sur des colonnes spécifiques dans les bases de données que vous numérisez.
- Vous pouvez ajouter des mots-clés personnalisés à partir d'un fichier texte — ces mots sont identifiés dans vos données.
- Vous pouvez ajouter un motif personnel à l'aide d'une expression régulière (regex) — le regex est ajouté aux motifs prédéfinis existants.
- Vous pouvez ajouter des catégories personnalisées afin d'identifier l'emplacement de catégories d'informations spécifiques dans vos données.

Tous ces mécanismes pour ajouter des critères de numérisation personnalisés sont pris en charge dans toutes les langues.

Les fonctionnalités décrites dans cette section ne sont disponibles que si vous avez choisi d'effectuer une analyse de classification complète sur vos sources de données. Les sources de données qui ont une analyse avec mappage uniquement n'affichent pas de détails au niveau des fichiers.

Ajoutez des identifiants de données personnelles personnalisés à partir de vos bases de données

Une fonctionnalité que nous appelons *Data Fusion* vous permet d'analyser les données de votre organisation pour identifier si des identificateurs uniques de vos bases de données sont trouvés dans l'une de vos autres sources de données. Vous pouvez choisir les identifiants supplémentaires que recherche la classification BlueXP dans ses analyses en sélectionnant une ou plusieurs colonnes spécifiques dans une table de base de données. Par exemple, le diagramme ci-dessous montre comment Data Fusion est utilisé pour analyser vos volumes, compartiments et bases de données pour rechercher les occurrences de tous vos identifiants client à partir de votre base de données Oracle.



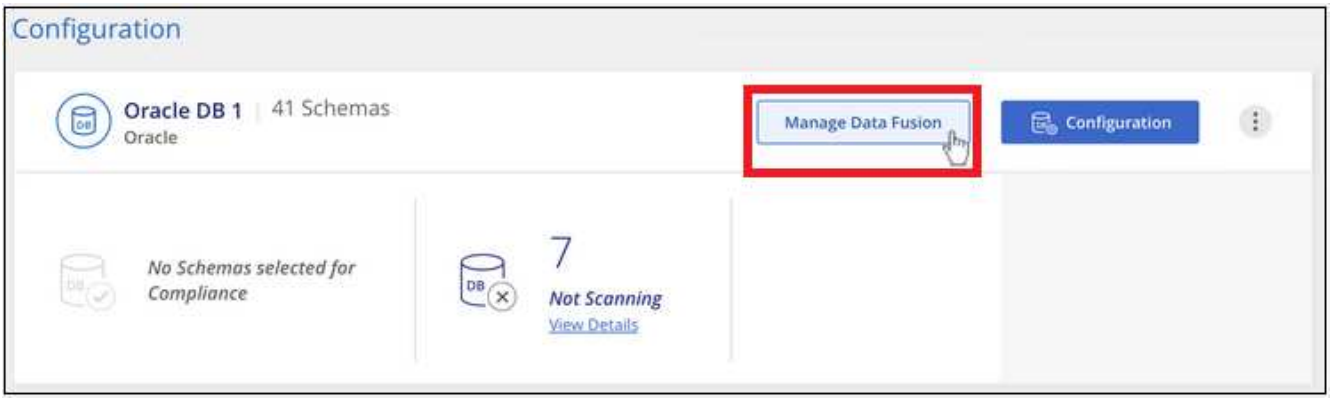
Comme vous pouvez le voir, deux ID de client uniques ont été trouvés sur deux volumes et dans un compartiment S3. Toutes les correspondances dans les tables de base de données seront également identifiées.

Notez que, puisque vous scannez vos propres bases de données, quelle que soit la langue dans laquelle vos données sont stockées, elles seront utilisées pour identifier les données lors des futures analyses de classification BlueXP.

Étapes

Vous devez avoir "ajout d'au moins un serveur de base de données" À la classification BlueXP avant d'ajouter des sources de données Fusion.

1. Dans la page Configuration, cliquez sur **gérer Fusion de données** dans la base de données où résident les données source.



2. Cliquez sur **Ajouter une source de données Fusion** sur la page suivante.

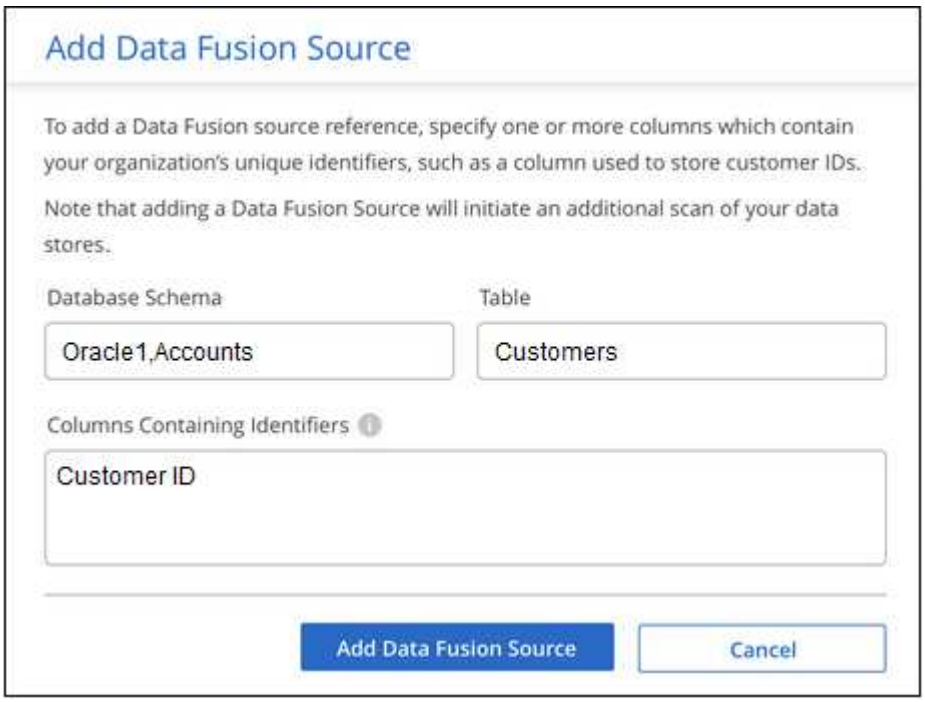
3. Dans la page *Add Data Fusion Source* :

   a. Sélectionnez le schéma de la base de données dans le menu déroulant.

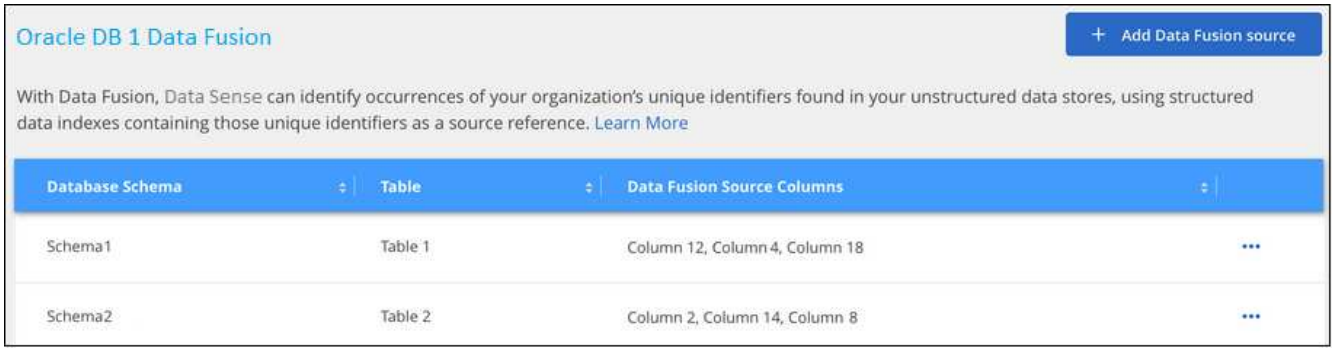
   b. Entrez le nom de la table dans ce schéma.

   c. Entrez la colonne ou les colonnes contenant les identifiants uniques que vous souhaitez utiliser.

      Lors de l'ajout de plusieurs colonnes, entrez chaque nom de colonne ou de vue de table sur une ligne distincte.

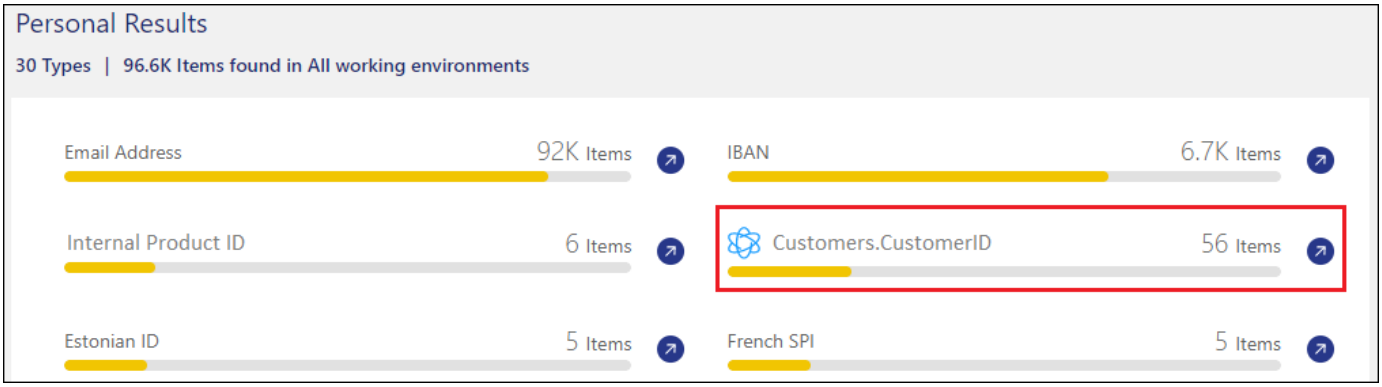


4. Cliquez sur **Ajouter une source de données Fusion**.



Résultats

Après l'analyse suivante, les résultats incluent ces nouvelles informations dans le tableau de bord de conformité sous la section « Résultats personnels » et dans la page Investigation du filtre « données personnelles ». Le nom que vous avez utilisé pour le classificateur apparaît dans la liste de filtres, par exemple `Customers.CustomerID`.



Supprimer une source de Data Fusion

Si vous décidez à un moment donné de ne pas numériser vos fichiers à l'aide d'une source Data Fusion donnée, vous pouvez sélectionner la ligne source dans la page d'inventaire Data Fusion et cliquer sur **Supprimer la source Data Fusion**.

Ajoutez des mots clés personnalisés à partir d'une liste de mots

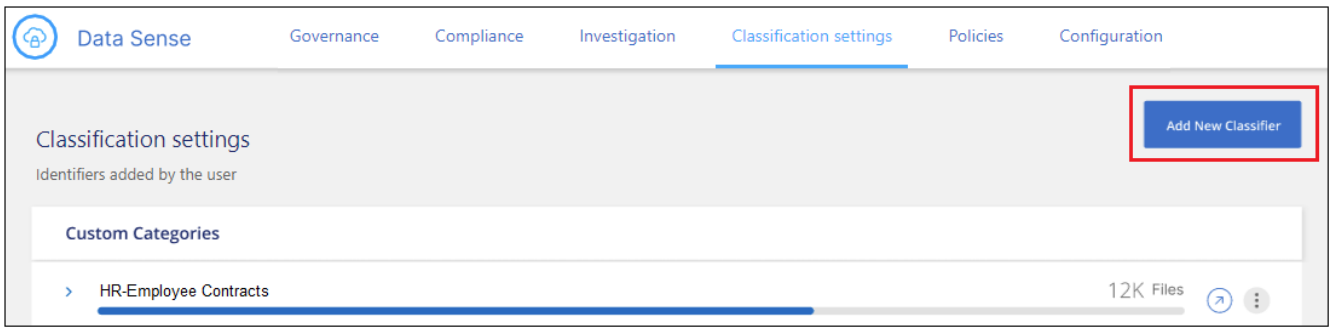
Vous pouvez ajouter des mots-clés personnalisés à la classification BlueXP pour identifier l'emplacement où se trouvent les informations. Pour ajouter ces mots-clés, entrez simplement les mots que vous souhaitez que la classification BlueXP reconnaisse. Les mots-clés sont ajoutés aux mots-clés prédéfinis que la classification BlueXP utilise déjà et les résultats sont visibles dans la section modèles personnels.

Par exemple, vous pouvez voir où les noms de produits internes sont mentionnés dans tous vos fichiers pour vous assurer que ces noms ne sont pas accessibles dans des emplacements qui ne sont pas sécurisés.

Après la mise à jour des mots-clés personnalisés, la classification BlueXP redémarre l'analyse de toutes les sources de données. Une fois l'analyse terminée, les nouveaux résultats apparaissent dans le tableau de bord de conformité de classification BlueXP, dans la section « Résultats personnels », et dans la page Investigation du filtre « données personnelles ».

Étapes

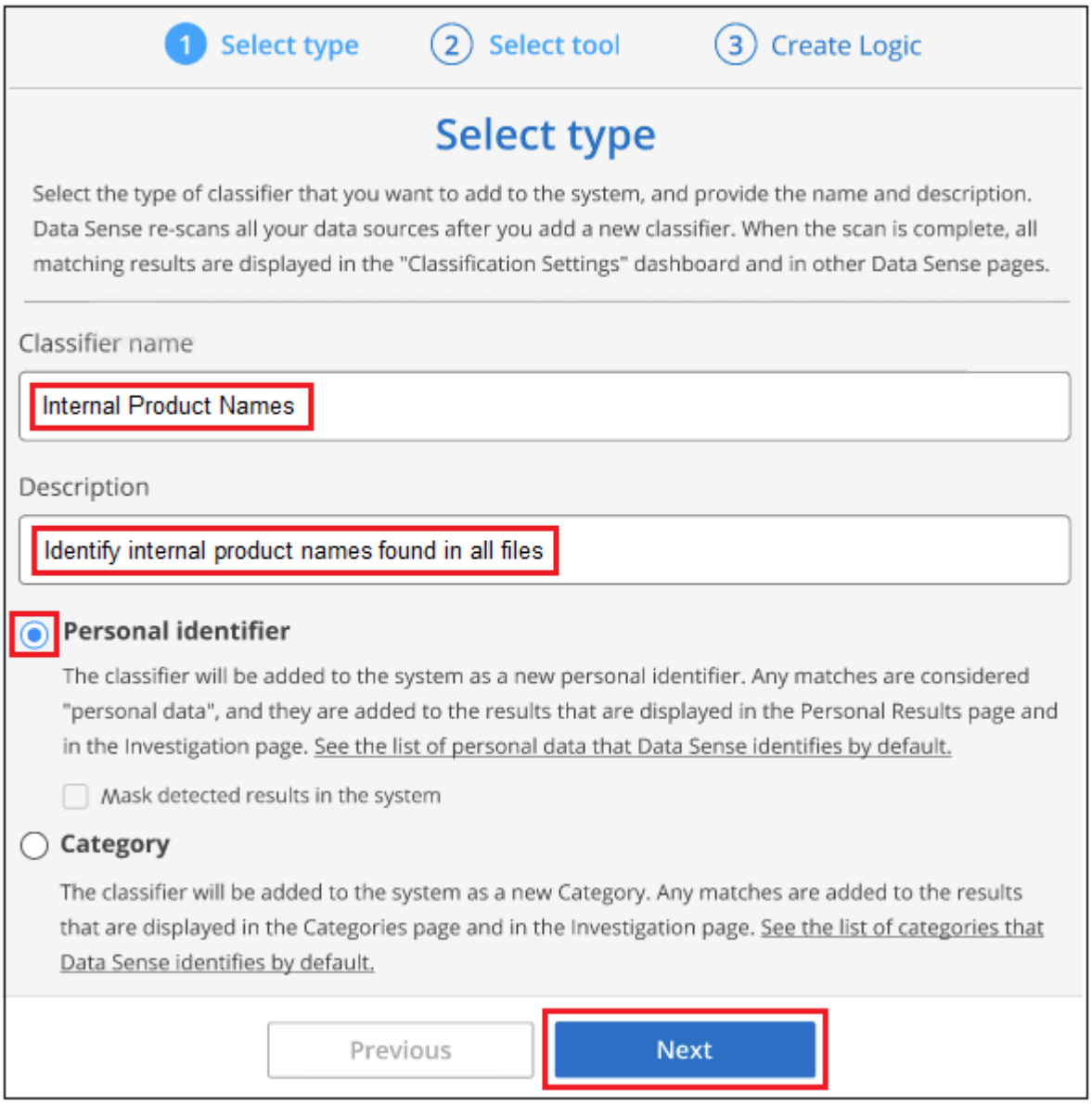
1. Dans l'onglet *Paramètres de classification*, cliquez sur **Ajouter un nouveau classificateur** pour lancer l'assistant *Ajouter un classificateur personnalisé*.



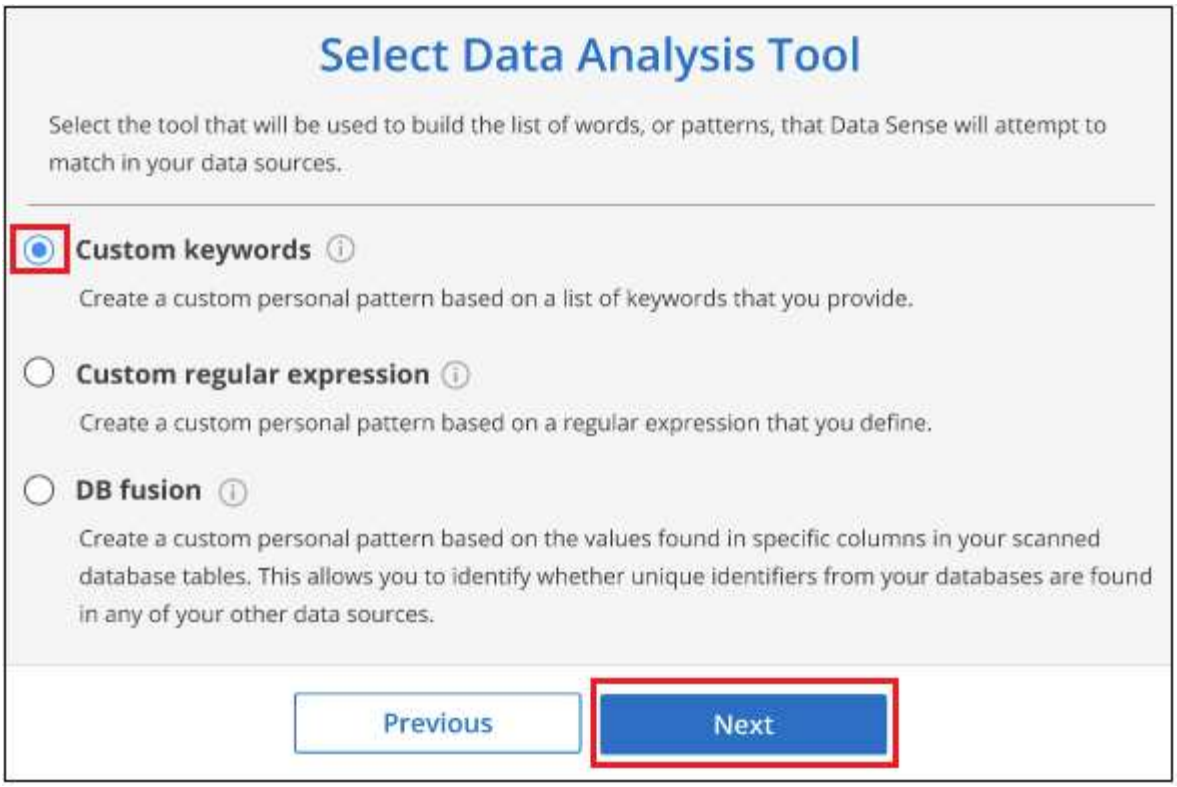
2. Dans la page *Select type*, entrez le nom du classificateur, fournissez une brève description, sélectionnez **Personal identifier**, puis cliquez sur **Next**.

   Le nom que vous entrez s'affiche dans l'interface de classification BlueXP en tant qu'en-tête pour les fichiers numérisés qui correspondent aux exigences du classificateur et en tant que nom du filtre dans la page Investigation.

   Vous pouvez également cocher la case « Masquer les résultats détectés dans le système » pour que le résultat complet n'apparaisse pas dans l'interface utilisateur. Par exemple, vous pouvez vouloir le faire pour masquer les numéros de carte de crédit complets ou des données personnelles similaires (le masque apparaîtra dans l'interface utilisateur comme ceci: "Pass:[**] **** **** ****" 3434).

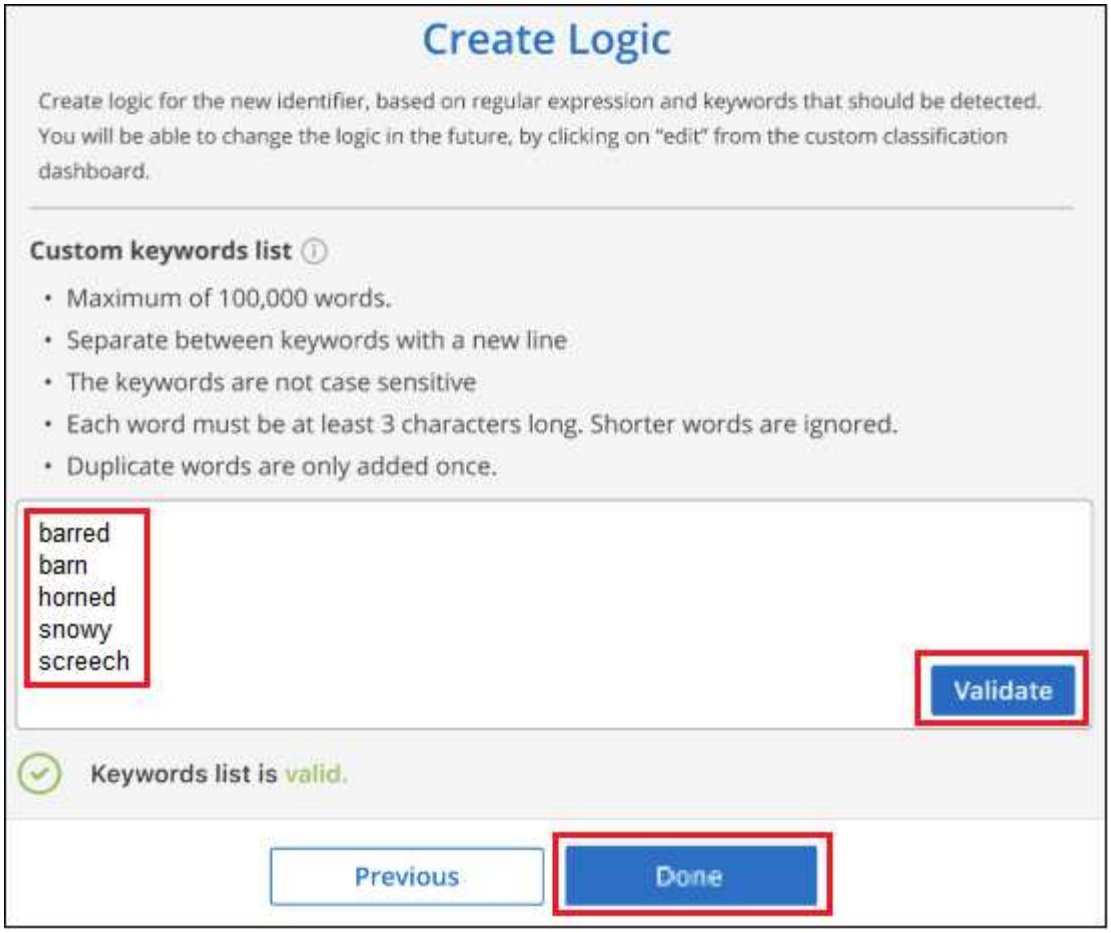


3. Dans la page *Select Data Analysis Tool*, sélectionnez **Custom Keywords** comme méthode à utiliser pour définir le classificateur, puis cliquez sur **Next**.



4. Dans la page *Create Logic*, entrez les mots-clés que vous voulez reconnaître - chaque mot sur une ligne séparée - et cliquez sur **Validate**.

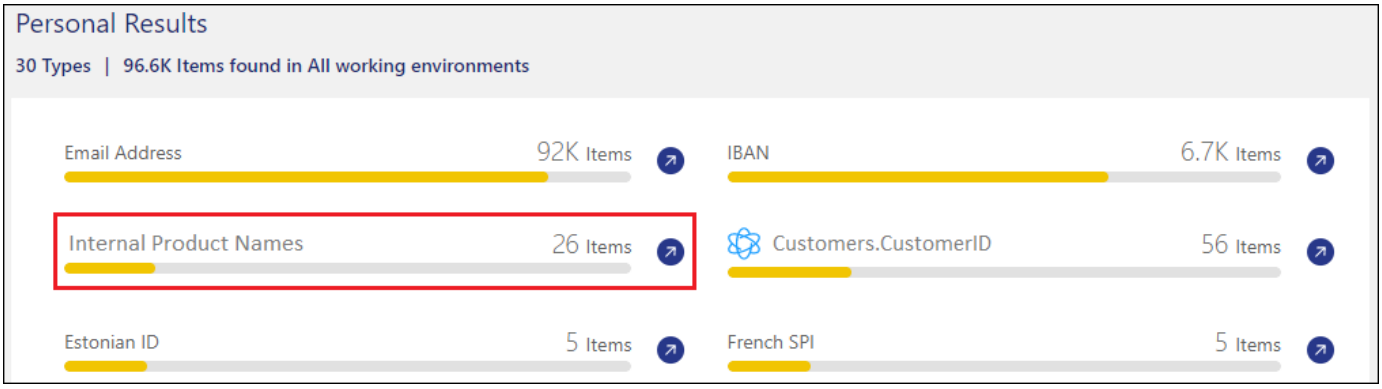
   La capture d'écran ci-dessous montre les noms de produits internes (différents types de wls). La recherche de classification BlueXP pour ces éléments n'est pas sensible à la casse.



5. Cliquez sur **terminé** et la classification BlueXP commence à analyser à nouveau vos données.

Résultats

Une fois l'analyse terminée, les résultats incluront ces nouvelles informations dans le tableau de bord de conformité sous la section « Résultats personnels » et dans la page enquête du filtre « données personnelles ».



Comme vous pouvez le voir, le nom du classificateur est utilisé comme nom dans le panneau Résultats personnels. De cette manière, vous pouvez activer de nombreux groupes de mots-clés et voir les résultats pour chaque groupe.

Ajoutez des identificateurs de données personnelles personnalisés à l'aide d'un regex

Vous pouvez ajouter un modèle personnel pour identifier des informations spécifiques dans vos données à

l'aide d'une expression régulière personnalisée (regex). Cela vous permet de créer un nouveau regex personnalisé pour identifier de nouveaux éléments d'informations personnelles qui n'existent pas encore dans le système. Le regex est ajouté aux modèles prédéfinis existants que la classification BlueXP utilise déjà, et les résultats seront visibles dans la section modèles personnels.

Par exemple, vous pouvez voir où vos ID de produit internes sont mentionnés dans tous vos fichiers. Si l'ID de produit a une structure claire, par exemple, il s'agit d'un numéro à 12 chiffres commençant par 201, vous pouvez utiliser la fonction regex personnalisée pour la rechercher dans vos fichiers. L'expression régulière de cet exemple est **\b201\d{9}\b**.

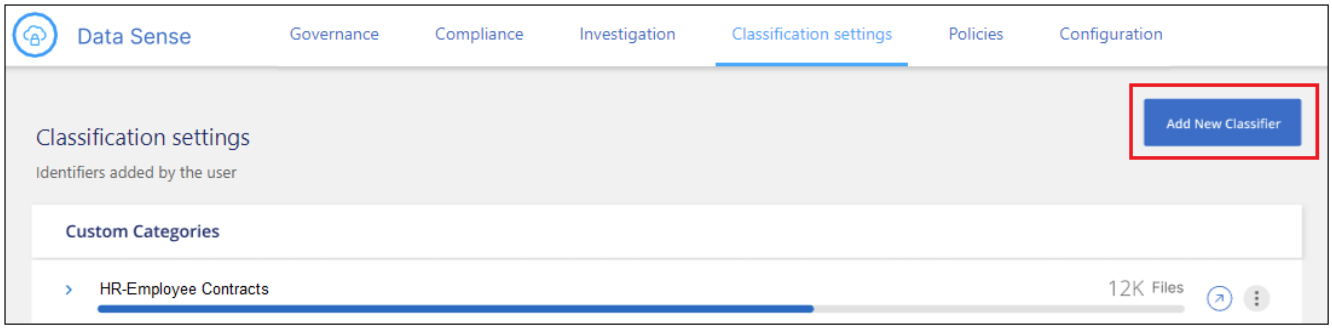
Une fois le regex ajouté, la classification BlueXP redémarre l'analyse de toutes les sources de données. Une fois l'analyse terminée, les nouveaux résultats apparaissent dans le tableau de bord de conformité de classification BlueXP, dans la section « Résultats personnels », et dans la page Investigation du filtre « données personnelles ».

Si vous avez besoin d'aide pour construire l'expression régulière, reportez-vous à la section "Expressions régulières 101". Choisissez **Python** pour que la saveur puisse voir les types de résultats que la classification BlueXP correspond à l'expression régulière. Le "Page Python Regex Tester" est également utile en affichant une représentation graphique de vos répétitions.

> Actuellement, nous n'autorisons pas l'utilisation d'indicateurs de motif lors de la création d'un regex - cela signifie que vous ne devez pas utiliser "/".

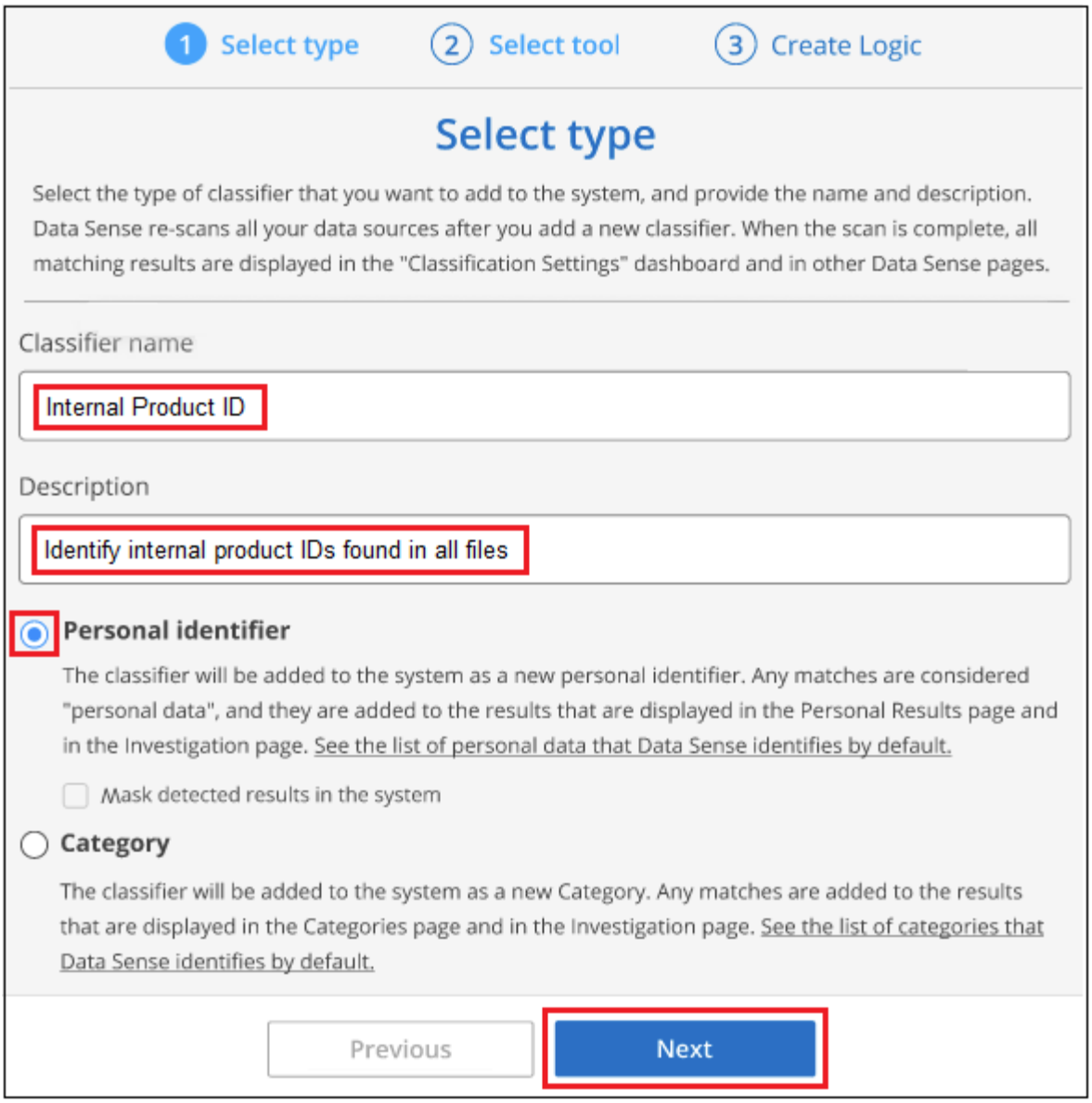
Étapes

1. Dans l'onglet *Paramètres de classification*, cliquez sur **Ajouter un nouveau classificateur** pour lancer l'assistant *Ajouter un classificateur personnalisé*.

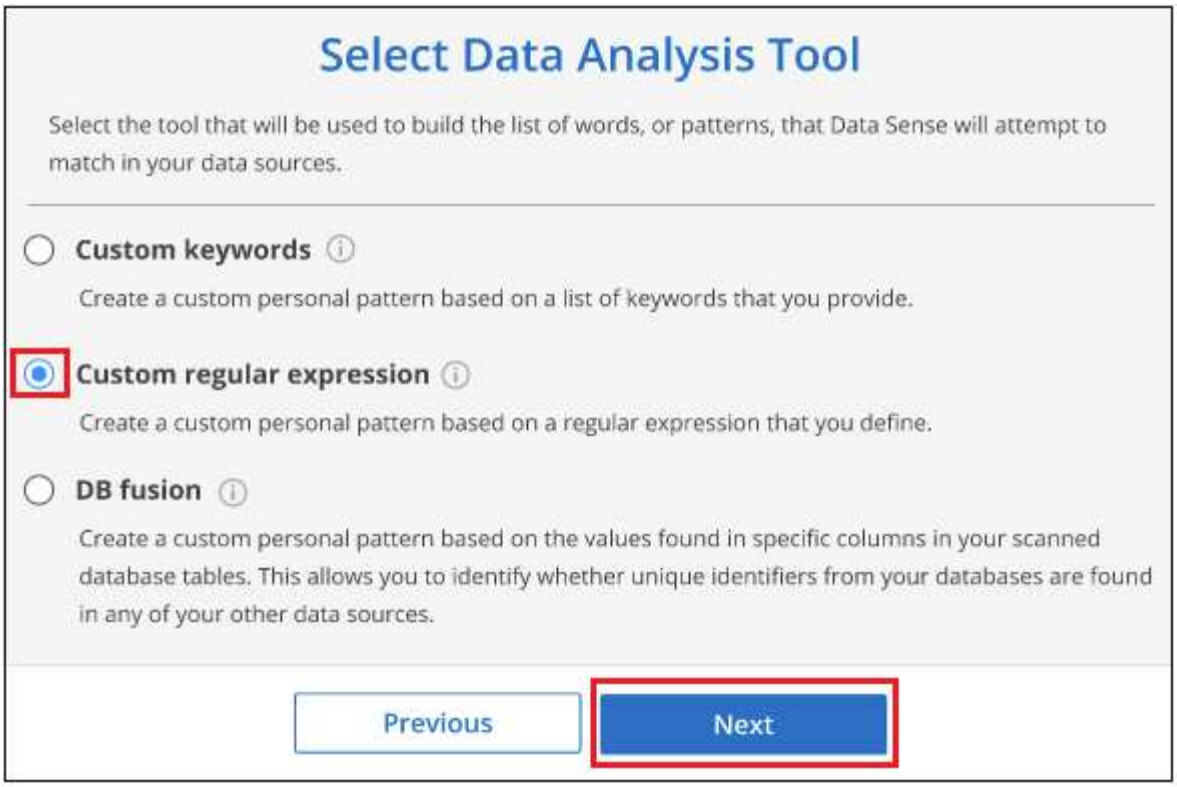


2. Dans la page *Select type*, entrez le nom du classificateur, fournissez une brève description, sélectionnez **Personal identifier**, puis cliquez sur **Next**.

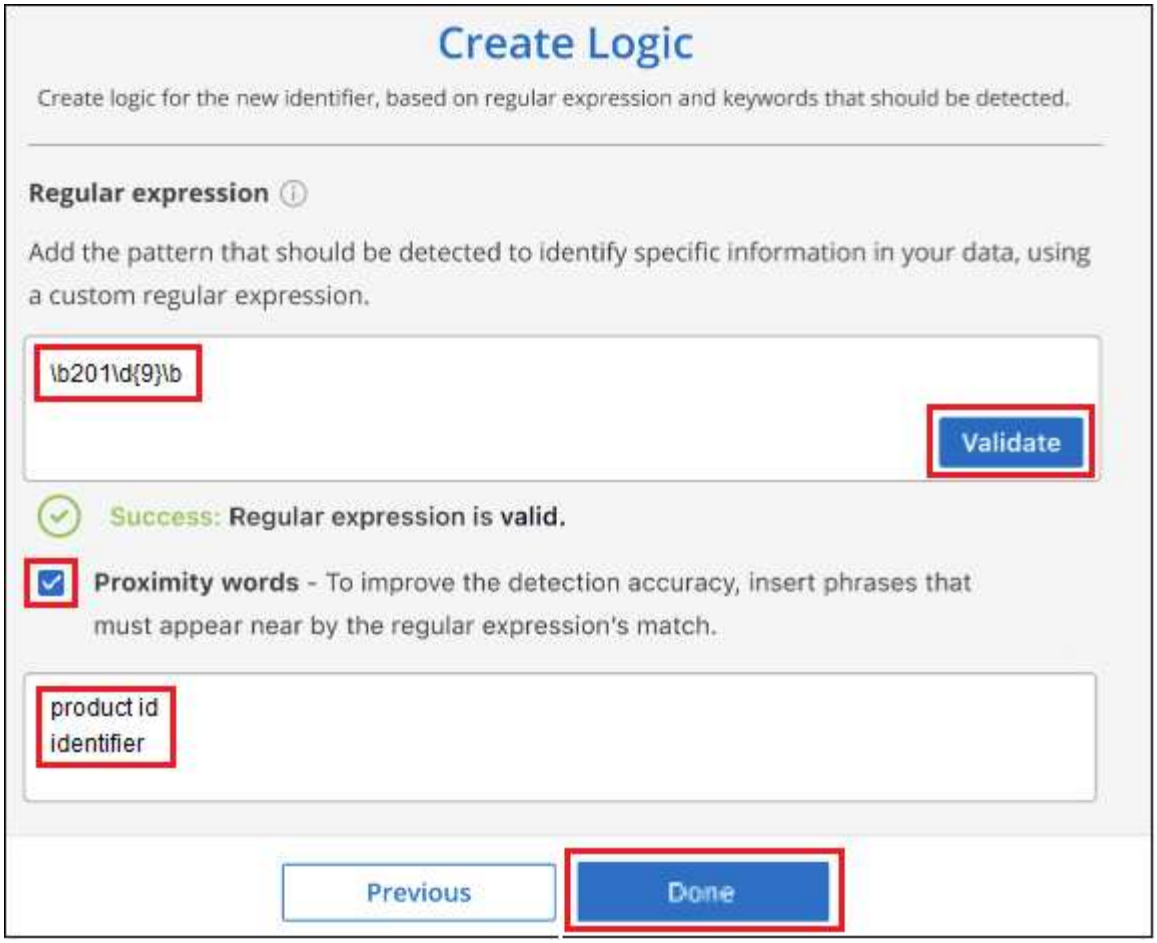
   Le nom que vous entrez s'affiche dans l'interface de classification BlueXP en tant qu'en-tête pour les fichiers numérisés qui correspondent aux exigences du classificateur et en tant que nom du filtre dans la page Investigation. Vous pouvez également cocher la case « Masquer les résultats détectés dans le système » pour que le résultat complet n'apparaisse pas dans l'interface utilisateur. Par exemple, vous pouvez vouloir le faire pour masquer les numéros complets de carte de crédit ou des données personnelles similaires.



3. Dans la page *Select Data Analysis Tool*, sélectionnez **Custom Regular expression** comme méthode à utiliser pour définir le classificateur, puis cliquez sur **Next**.

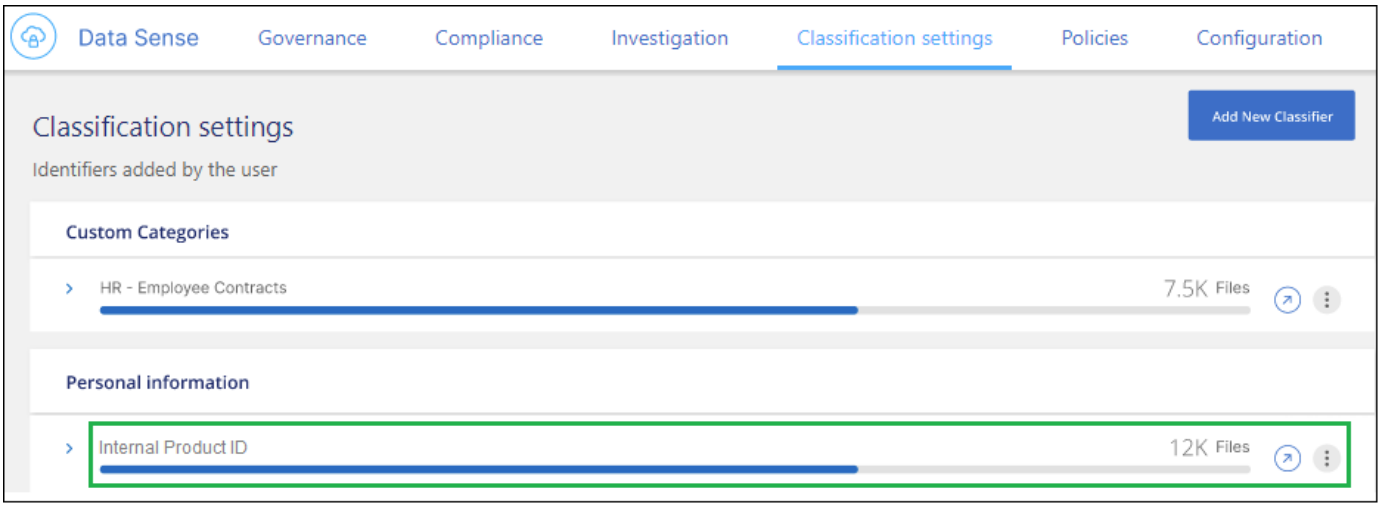


4. Dans la page *Create Logic*, entrez l'expression régulière et les mots de proximité, puis cliquez sur **Done**.
   a. Vous pouvez entrer n'importe quelle expression régulière légale. Cliquez sur le bouton **Valider** pour que la classification BlueXP vérifie que l'expression régulière est valide et qu'elle n'est pas trop large, ce qui signifie qu'elle renvoie trop de résultats.
   b. Vous pouvez également saisir des mots de proximité pour vous aider à affiner la précision des résultats. Il s'agit de mots qui se trouvent généralement dans les 300 caractères du motif que vous recherchez (avant ou après le motif trouvé). Entrez chaque mot ou expression sur une ligne distincte.



Résultats

Le classificateur est ajouté et la classification BlueXP commence à analyser à nouveau toutes vos sources de données. Vous revenez à la page Classificateurs personnalisés où vous pouvez afficher le nombre de fichiers correspondant à votre nouveau classificateur. Les résultats de l'analyse de toutes vos sources de données prennent du temps en fonction du nombre de fichiers à numériser.



Ajouter des catégories personnalisées

La classification BlueXP récupère les données qu'il analyse et les divise en différents types de catégories. Ces catégories sont des thèmes basés sur l'analyse par intelligence artificielle du contenu et des métadonnées de

chaque fichier. "Voir la liste des catégories prédéfinies".

Les catégories peuvent vous aider à comprendre ce qui se passe avec vos données en vous montrant les types d'informations dont vous disposez. Par exemple, une catégorie telle que *CV* ou *contrats d'employés* peut inclure des données sensibles. Lorsque vous étudiez les résultats, vous pouvez constater que les contrats d'employés sont stockés dans un emplacement non sécurisé. Vous pouvez ensuite corriger ce problème.

Vous pouvez ajouter des catégories personnalisées à la classification BlueXP pour identifier où se trouvent les catégories d'informations spécifiques à votre patrimoine de données. Vous ajoutez chaque catégorie en créant des fichiers d'entraînement qui contiennent les catégories de données que vous souhaitez identifier, puis analysez ces fichiers pour les analyser par le biais de l'IA afin qu'il puisse identifier les données dans vos sources de données. Les catégories sont ajoutées aux catégories prédéfinies existantes identifiées par la classification BlueXP et les résultats sont visibles dans la section catégories.

Par exemple, vous pouvez voir où se trouvent les fichiers d'installation compressés au format .gz dans vos fichiers afin que vous puissiez les supprimer, si nécessaire.

Après la mise à jour des catégories personnalisées, la classification BlueXP redémarre l'analyse de toutes les sources de données. Une fois l'analyse terminée, les nouveaux résultats apparaissent dans le tableau de bord de conformité de classification BlueXP sous la section « catégories » et dans la page Investigation du filtre « Catégorie ». "Voir comment afficher les fichiers par catégories".

Ce dont vous avez besoin

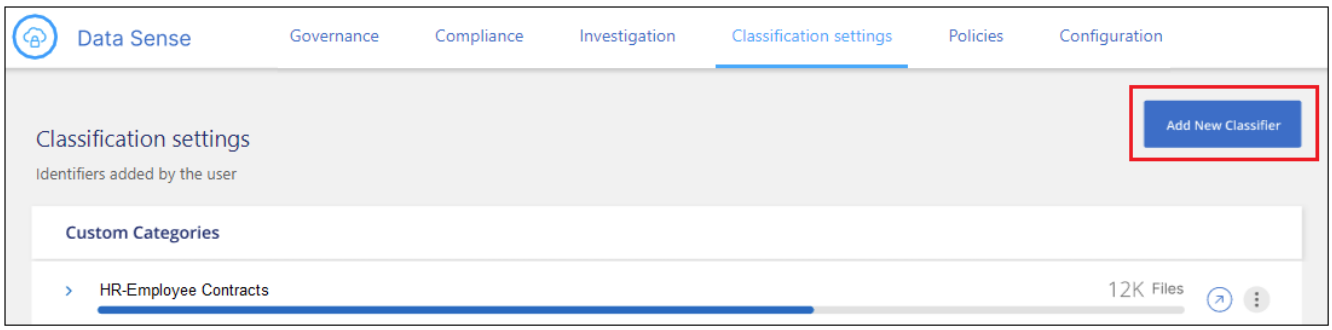
Vous devez créer au moins 25 fichiers d'entraînement contenant des échantillons des catégories de données que vous voulez que la classification BlueXP reconnaisse. Les types de fichiers suivants sont pris en charge :

```
.CSV, .DOC, .DOCX, .GZ, .JSON, .PDF, .PPTX, .RTF, .TXT, .XLS, .XLSX, Docs,
Sheets, and Slides
```

Les fichiers doivent être d'au moins 100 octets et doivent se trouver dans un dossier accessible par la classification BlueXP.

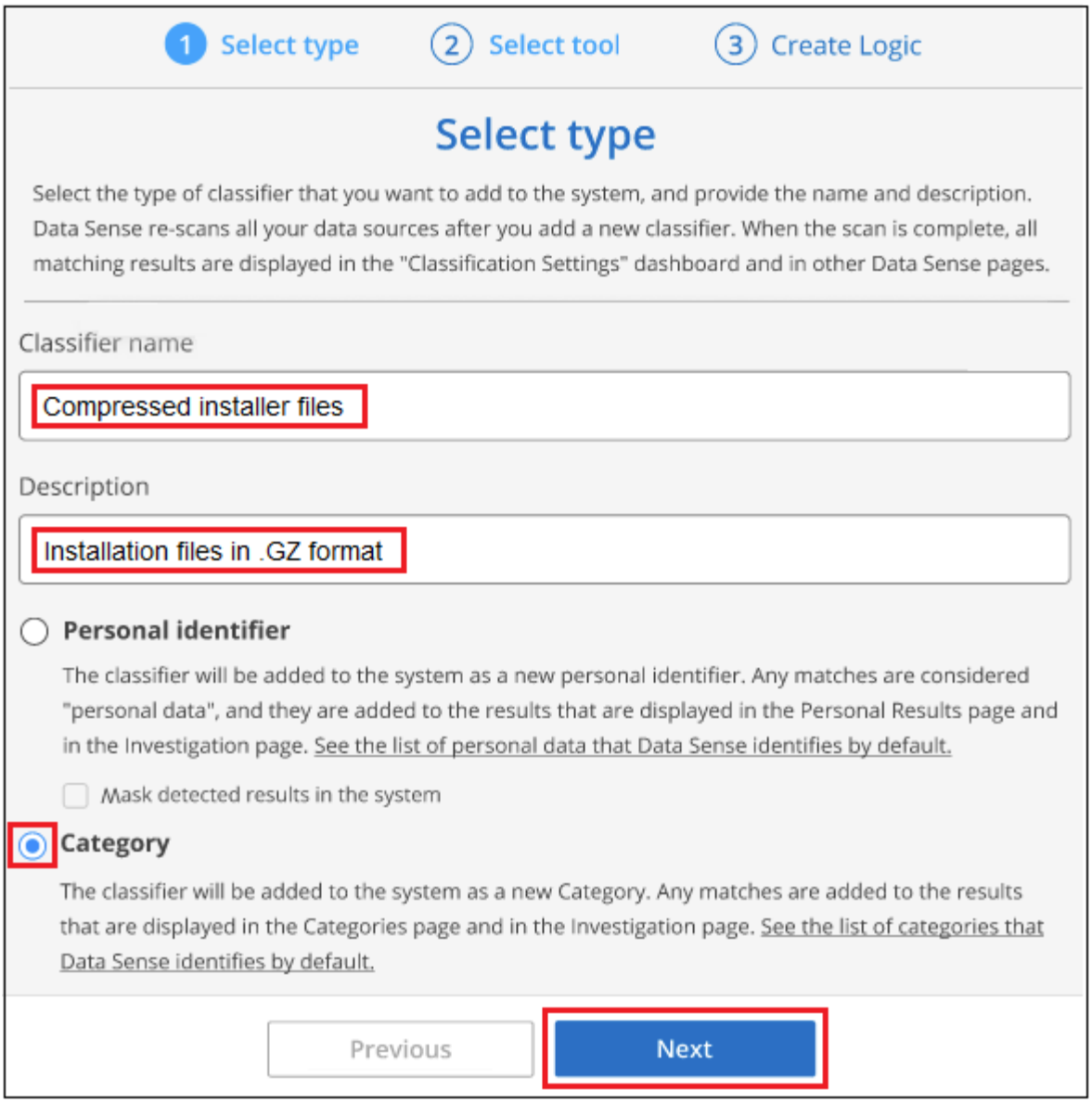
Étapes

1. Dans l'onglet *Paramètres de classification*, cliquez sur **Ajouter un nouveau classificateur** pour lancer l'assistant *Ajouter un classificateur personnalisé*.

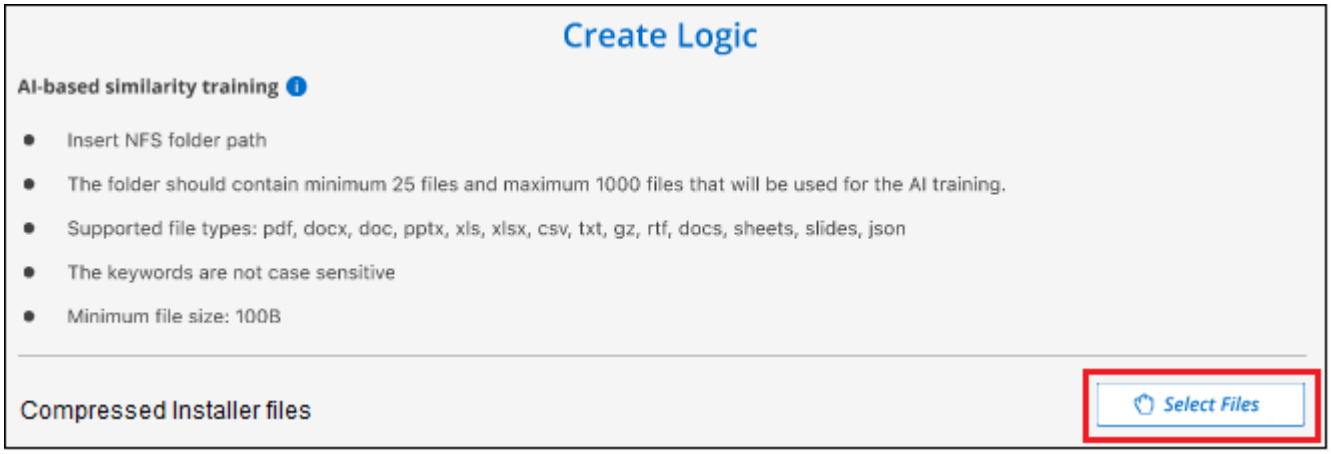


2. Dans la page *Select type*, entrez le nom du classificateur, fournissez une brève description, sélectionnez **Catégorie**, puis cliquez sur **Suivant**.

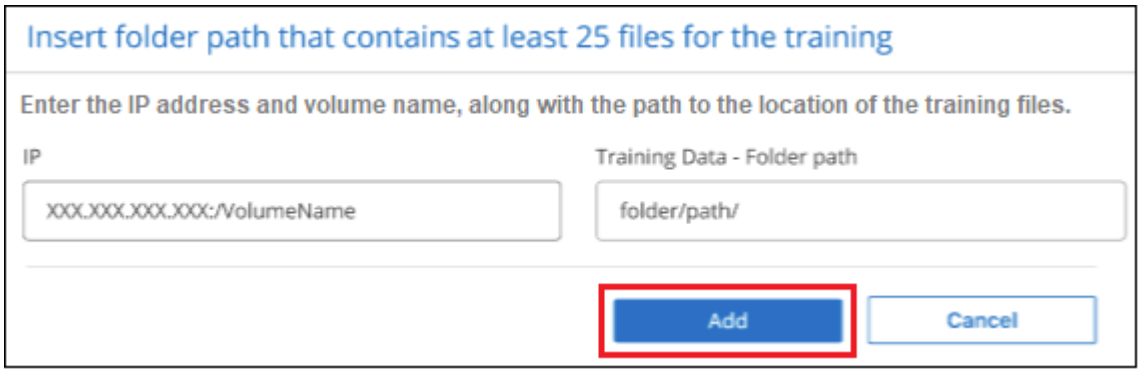
   Le nom que vous entrez s'affiche dans l'interface de classification BlueXP en tant qu'en-tête des fichiers numérisés correspondant à la catégorie de données que vous définissez, et en tant que nom du filtre dans la page Investigation.



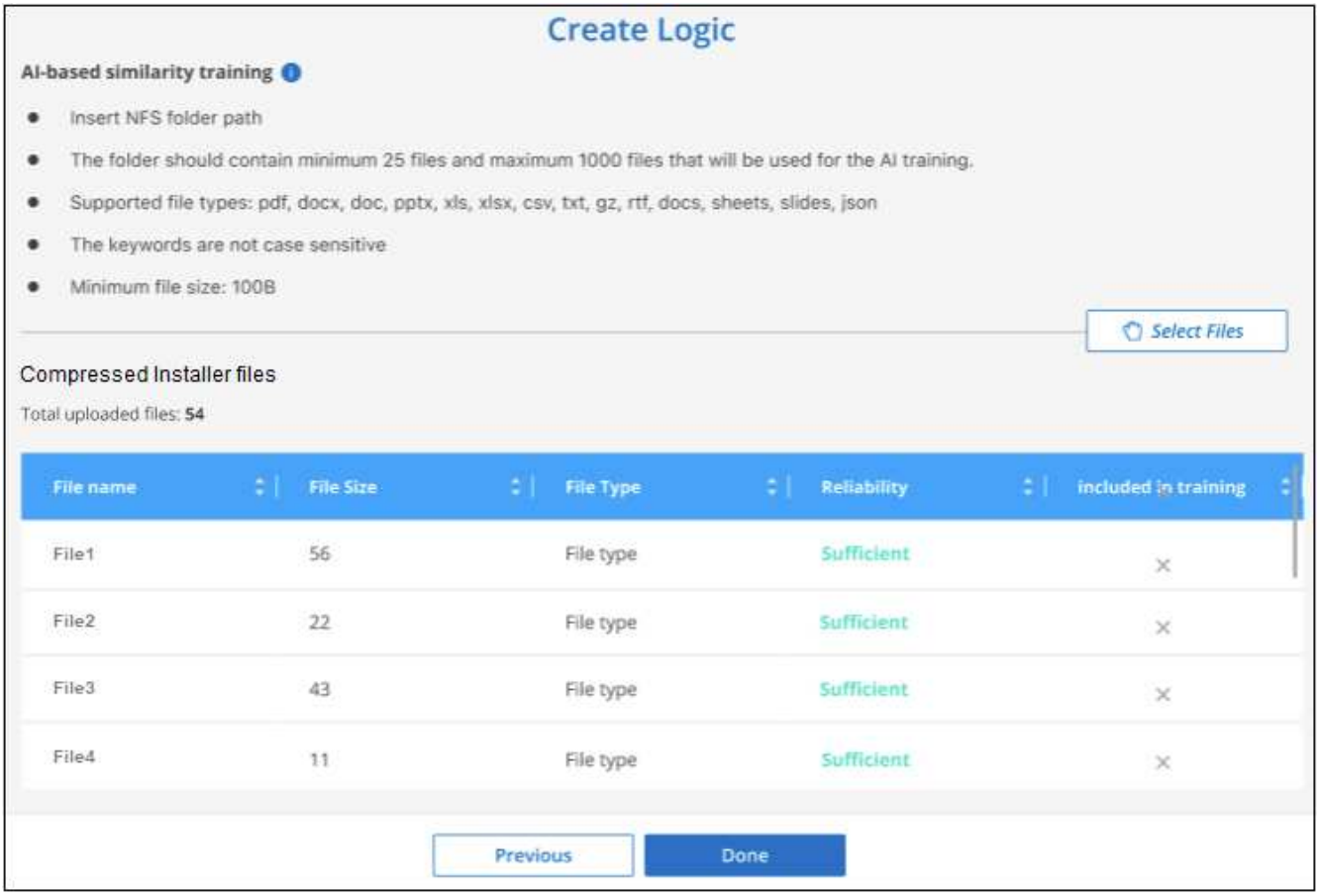
3. Dans la page *Créer logique*, assurez-vous que les fichiers d'apprentissage sont préparés, puis cliquez sur **Sélectionner les fichiers**.



4. Entrez l'adresse IP du volume et le chemin où se trouvent les fichiers de formation, puis cliquez sur **Ajouter**.



5. Vérifiez que les fichiers d'entraînement ont été reconnus par la classification BlueXP. Cliquez sur **x** pour supprimer tous les fichiers de formation qui ne répondent pas aux exigences. Cliquez ensuite sur **terminé**.



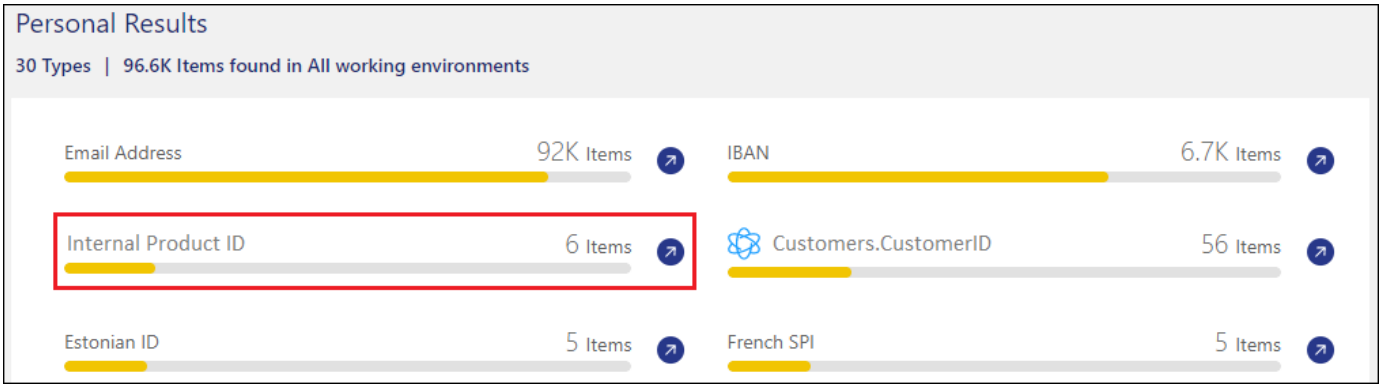
Résultats

La nouvelle catégorie est créée telle que définie par les fichiers d'entraînement et ajoutée à la classification BlueXP. La classification BlueXP commence ensuite à analyser à nouveau toutes vos sources de données pour identifier les fichiers qui s'intègrent à cette nouvelle catégorie. Vous êtes renvoyé à la page Classifications personnalisées où vous pouvez afficher le nombre de fichiers correspondant à votre nouvelle catégorie. Les résultats de l'analyse de toutes vos sources de données prennent du temps en fonction du nombre de fichiers à numériser.

Afficher les résultats de vos classificateurs personnalisés

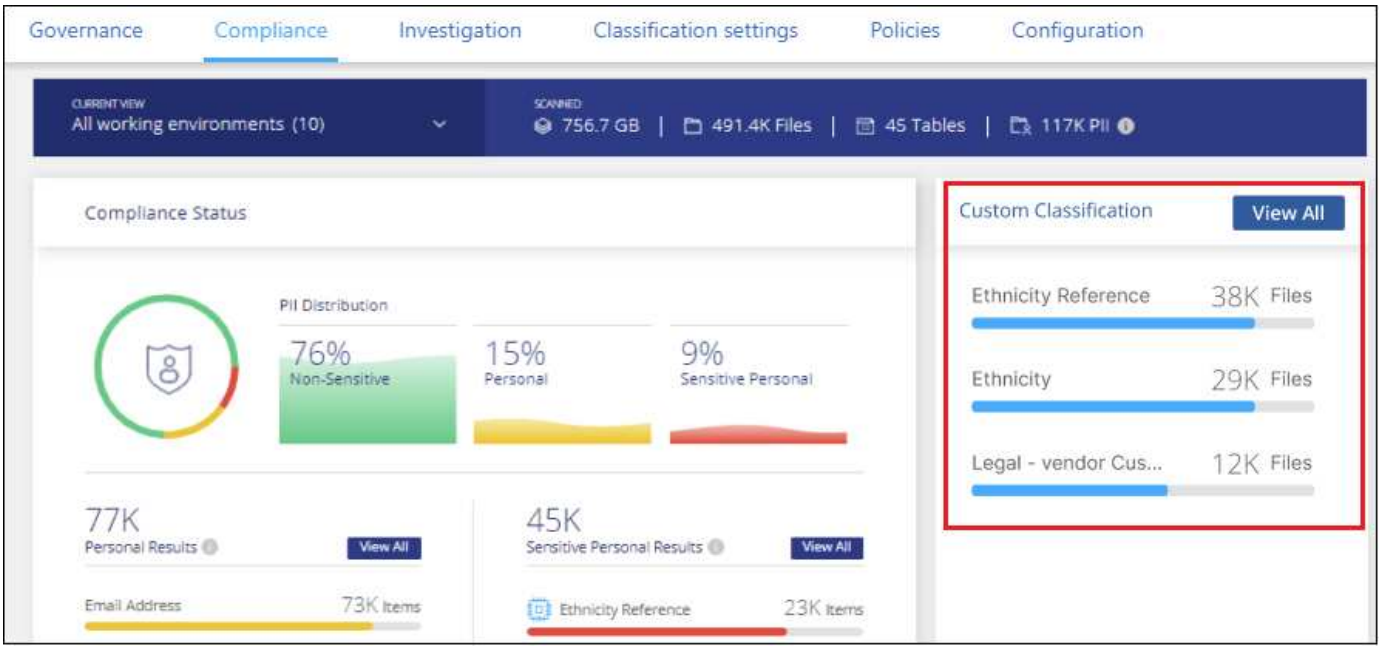
Vous pouvez afficher les résultats de n'importe lequel de vos classificateurs personnalisés dans le tableau de bord de conformité et dans la page Investigation. Par exemple, cette capture d'écran affiche les informations

correspondantes dans le tableau de bord de conformité, sous la section « Résultats personnels ».



Cliquez sur le bouton Pour afficher les résultats détaillés dans la page Investigation.

En outre, tous les résultats de votre classificateur personnalisé apparaissent dans l'onglet Classificateurs personnalisés, et les 6 meilleurs résultats de classificateur personnalisé sont affichés dans le tableau de bord de conformité, comme illustré ci-dessous.

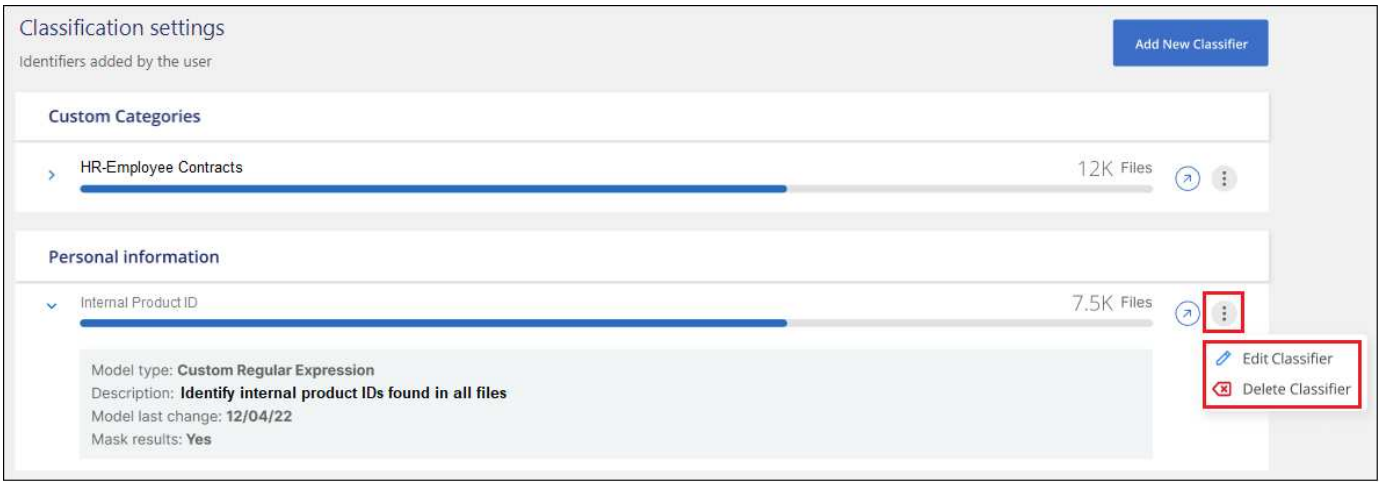


Gérer les classificateurs personnalisés

Vous pouvez modifier n'importe lequel des classificateurs personnalisés que vous avez créés à l'aide du bouton **Edit Classificateur**.

Vous ne pouvez pas modifier les classificateurs Data Fusion pour le moment.

Et si vous décidez ultérieurement que vous n'avez pas besoin de la classification BlueXP pour identifier les modèles personnalisés que vous avez ajoutés, vous pouvez utiliser le bouton **Supprimer le classificateur** pour supprimer chaque élément.



Affichage de l'état de vos actions de conformité

Lorsque vous exécutez une action asynchrone à partir du volet Résultats de l'enquête sur de nombreux fichiers, par exemple le déplacement ou la suppression de 100 fichiers, le processus peut prendre un certain temps. Vous pouvez contrôler l'état de ces actions dans le volet *action Status* pour savoir quand elles ont été appliquées à tous les fichiers.

Cela vous permet de voir les actions effectuées avec succès, celles en cours et celles qui ont échoué pour diagnostiquer et résoudre tout problème. Notez que les courtes opérations qui se sont terminées rapidement, telles que le déplacement d'un seul fichier, n'apparaissent pas dans le volet Statut des actions.

> **REMARQUE** ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP.

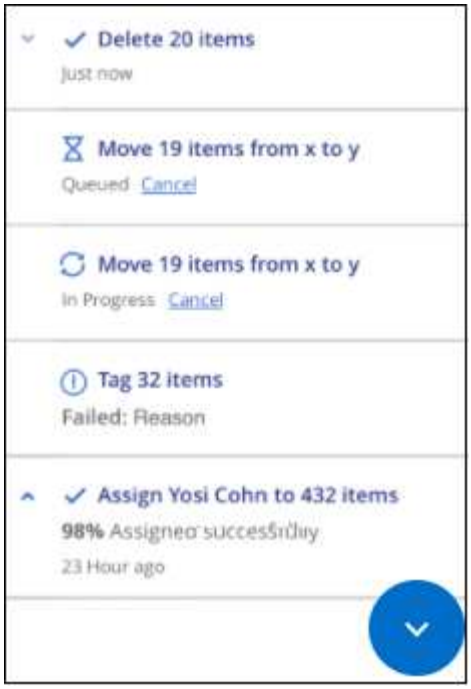
Le statut peut être :

- Réussite : Une action de classification BlueXP est terminée et tous les éléments ont réussi.
- Réussite partielle : Une action de classification BlueXP est terminée, certains éléments ont échoué et d'autres ont réussi.
- En cours - l'action est toujours en cours.
- En file d'attente - l'action n'a pas démarré.
- Annulé : l'action a été annulée.
- Echec - l'action a échoué.

Notez que vous pouvez annuler toutes les actions ayant le statut « en attente » ou « en cours ».

Étapes

1. En bas à droite de l'interface utilisateur de classification BlueXP, vous pouvez voir le bouton **actions Status** .
2. Cliquez sur ce bouton et les 20 actions les plus récentes sont répertoriées.



Vous pouvez cliquer sur le nom d'une action pour afficher les détails correspondant à cette opération.

Vérifiez l'historique des actions de classification BlueXP

Les activités de gestion des journaux de classification BlueXP qui ont été effectuées sur des fichiers depuis tous les environnements de travail et toutes les sources de données que la classification BlueXP analyse. La classification BlueXP consigne également les activités liées au déploiement de l'instance de classification BlueXP.

Vous pouvez afficher le contenu des fichiers journaux d'audit de classification BlueXP ou les télécharger pour voir quelles modifications de fichier ont été apportées et à quelle date. Par exemple, vous pouvez voir quelle demande a été émise, l'heure de la demande et des détails tels que l'emplacement source en cas de suppression d'un fichier ou l'emplacement source et de destination en cas de déplacement d'un fichier.

> **REMARQUE** ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP.

Contenu du fichier journal

Chaque ligne du journal d'audit contient des informations dans ce format :

```
<full date> | <status> | ds_audit_logger | <module> | 0 | 0 | File <full file
path> deleted from device <device path> - <result>
```

- Date et heure : horodatage complet de l'événement
- État - INFO, AVERTISSEMENT
- Type d'action (supprimer, copier, déplacer, créer la stratégie, mettre à jour la stratégie, Analyse des fichiers, téléchargement du rapport JSON, etc.)

- Nom du fichier (si l'action est pertinente pour un fichier)
- Détails de l'action - ce qui a été fait : dépend de l'action
  - Nom de la règle
  - Pour déplacer - Source et destination
  - Pour la copie - Source et destination
  - Pour balise - nom de balise
  - Pour attribuer à - nom d'utilisateur
  - Pour une alerte par e-mail : adresse e-mail/compte

Par exemple, les lignes suivantes du fichier journal indiquent une opération de copie réussie et une opération de copie ayant échoué.

```
2022-06-06 15:23:08,910 | INFO | ds_audit_logger | es_scanned_file | 237 |
49 | Copy file /CIFS_share/data/dop1/random_positives.tsv from device
10.31.133.183 (type: SMB_SHARE) to device 10.31.130.133:/export_reports
(NFS_SHARE) - SUCCESS
2022-06-06 15:23:08,968 | WARNING | ds_audit_logger | es_scanned_file |
239 | 153 | Copy file /CIFS_share/data/compliance-netapp.tar.gz from
device 10.31.133.183 (type: SMB_SHARE) to device
10.31.130.133:/export_reports (NFS_SHARE) - FAILURE
```

Emplacements des fichiers journaux

Les fichiers journaux d'audit de gestion se trouvent sur la machine de classification BlueXP dans : `/opt/netapp/audit_logs/`

Les fichiers journaux d'audit d'installation sont écrits dans `/opt/netapp/install_logs/`

Chaque fichier journal peut avoir une taille maximale de 10 Mo. Lorsque cette limite est atteinte, un nouveau fichier journal démarre. Les fichiers journaux sont nommés « DataSense_audit.log », « DataSense_audit.log.1 », « DataSense_audit.log.2 », etc. Un maximum de 100 fichiers journaux sont conservés sur le système - les anciens fichiers journaux sont automatiquement supprimés une fois le maximum atteint.

Accédez aux fichiers journaux

Vous devez vous connecter au système de classification BlueXP pour accéder aux fichiers journaux. Découvrez comment "Connectez-vous au système de classification BlueXP" Selon que vous avez installé le logiciel manuellement sur une machine Linux ou si vous avez déployé l'instance dans le cloud.

Réduction de la vitesse d'analyse de la classification BlueXP

L'analyse des données a un impact négligeable sur vos systèmes de stockage et sur vos données. Toutefois, si vous êtes préoccupé, même par un très faible impact, vous pouvez configurer la classification BlueXP pour effectuer des analyses « lentes ».

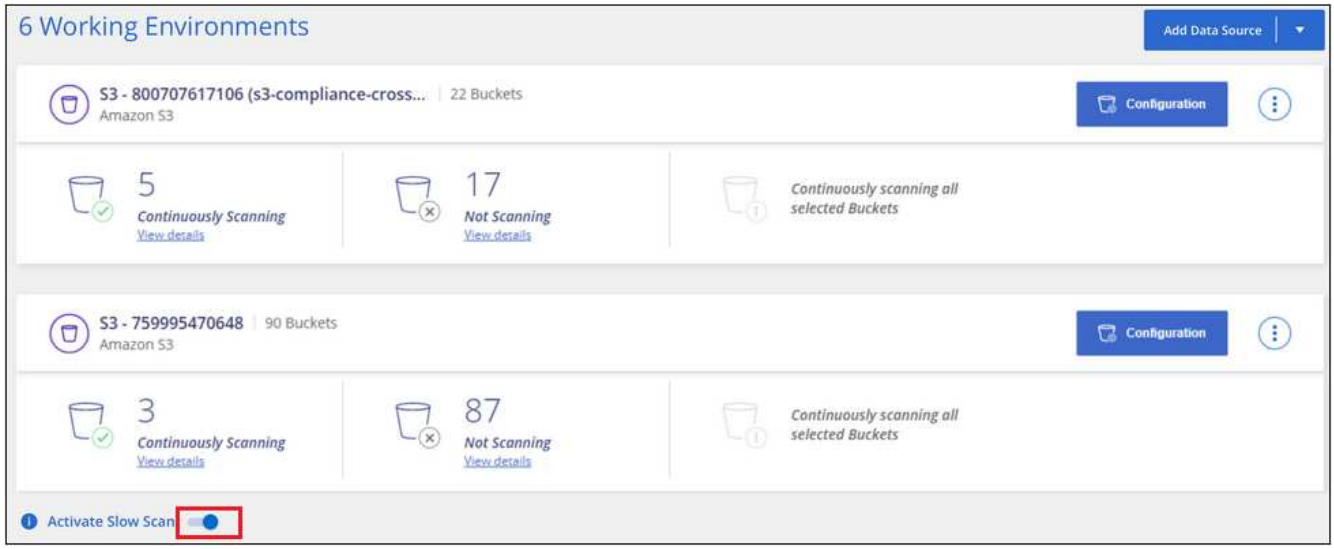
Lorsqu'elle est activée, l'analyse lente est utilisée sur toutes les sources de données ; vous ne pouvez pas configurer la numérisation lente pour un environnement de travail unique ou une source de données.

La vitesse de numérisation ne peut pas être réduite lors de la numérisation de bases de données.

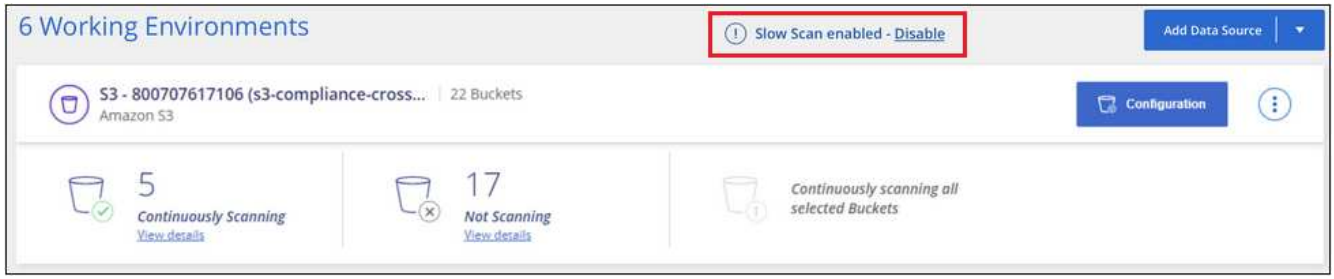
REMARQUE ces informations ne concernent que les versions 1.30 et antérieures de l'héritage de classification BlueXP.

Étapes

1. Depuis le bas de la *Configuration* page, déplacez le curseur vers la droite pour activer la numérisation lente.



Le haut de la page Configuration indique que la numérisation lente est activée.



2. Vous pouvez désactiver la numérisation lente en cliquant sur **Désactiver** dans ce message.

Supprimez un compte OneDrive, SharePoint ou Google Drive de la classification BlueXP

Si vous ne souhaitez plus analyser les fichiers utilisateur à partir d'un compte OneDrive spécifique, d'un compte SharePoint spécifique ou d'un compte Google Drive, vous pouvez supprimer le compte de l'interface de classification BlueXP et arrêter toutes les analyses.

Étapes

1. Dans la page *Configuration*, cliquez sur ⋮ Dans la ligne du compte OneDrive, SharePoint ou Google

Drive, puis cliquez sur **Supprimer le compte OneDrive**, **Supprimer le compte SharePoint** ou **Supprimer le compte Google Drive**.

2. Cliquez sur **Supprimer le compte** dans la boîte de dialogue de confirmation.

Référence

Types d'instances de classification BlueXP pris en charge

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. Lors du déploiement de la classification BlueXP dans le cloud, nous vous recommandons d'utiliser un système présentant les caractéristiques « grandes » pour bénéficier de fonctionnalités complètes.

Vous pouvez déployer la classification BlueXP sur un système avec moins de processeurs et moins de RAM, mais l'utilisation de systèmes moins puissants comporte certaines limitations. "Découvrez ces limites".

Dans les tableaux suivants, si le système marqué comme « par défaut » n'est pas disponible dans la région dans laquelle vous installez la classification BlueXP, le système suivant du tableau sera déployé.

Types d'instances AWS

Taille du système	Caractéristiques	Type d'instance
Très grand	32 processeurs, 128 Go de RAM, 1 Tio de SSD gp3	"m6i.8xlarge" (valeur par défaut)
Grand	16 processeurs, 64 Go de RAM, SSD de 500 Gio	"m6i.4xlarge" (par défaut) m6a.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
Moyen	8 processeurs, 32 Go de RAM, SSD de 200 Gio	"m6i.2xlarge" (par défaut) m6a.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
Petit	8 processeurs, 16 Go de RAM, SSD de 100 Gio	"c6a.2xlarge" (par défaut) c5a.2xlarge c5.2xlarge c4.2xlarge

Types d'instances Azure

Taille du système	Caractéristiques	Type d'instance
Très grand	32 processeurs, 128 Go de RAM, disque OS (2,048 Gio, débit min. De 250 Mo/s) et disque de données (SSD de 1 Tio, débit min. De 750 Mo/s)	"Standard_D32_v3" (valeur par défaut)
Grand	16 processeurs, 64 Go de RAM, SSD de 500 Gio	"Standard_D16s_v3" (valeur par défaut)

Types d'instances GCP

Taille du système	Caractéristiques	Type d'instance
Grand	16 processeurs, 64 Go de RAM, SSD de 500 Gio	"n2-standard-16" (par défaut) n2d-standard-16 n1-standard-16

Métadonnées collectées à partir des sources de données

La classification BlueXP collecte certaines métadonnées lors d'analyses de classification des données à partir de vos sources de données et de vos environnements de travail. La classification BlueXP peut accéder à la plupart des métadonnées dont nous avons besoin pour classer vos données, mais il existe certaines sources où nous ne pouvons pas accéder aux données dont nous avons besoin.

	Métadonnées	CIFS	NFS
Timbres horaires	*Temps de création*	Disponibilité	Non disponible (non pris en charge sous Linux)
	Heure du dernier accès	Disponibilité	Disponibilité
	Heure de la dernière modification	Disponibilité	Disponibilité
Autorisations	*Autorisations d'ouverture*	Si le groupe « TOUT LE MONDE » a accès au fichier, il est considéré comme « ouvert à l'entreprise ».	Si les « autres » ont accès au fichier, il est considéré comme « ouvert à l'entreprise ».
	Accès utilisateurs/groupe	Les informations relatives aux utilisateurs et aux groupes sont extraites du protocole LDAP	Non disponible (les utilisateurs NFS sont généralement gérés localement sur le serveur, par conséquent, la même personne peut avoir un UID différent sur chaque serveur)

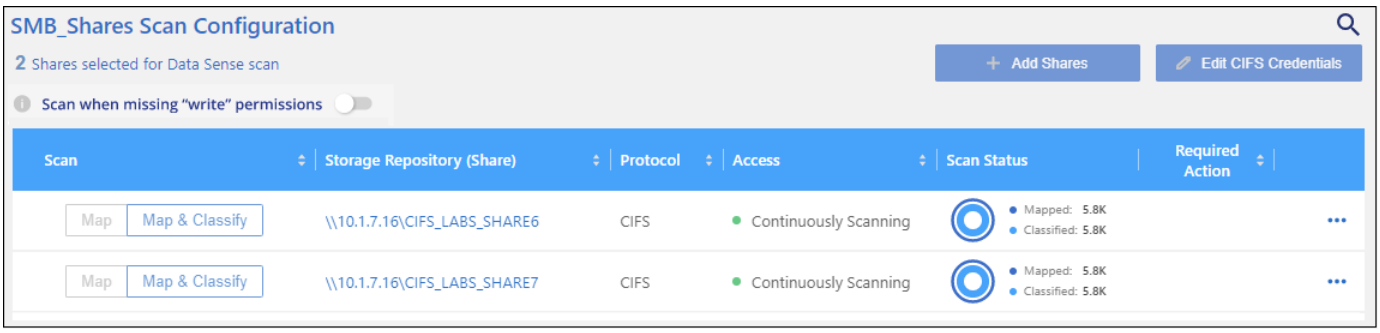
- La classification BlueXP n'extrait pas l'heure du dernier accès des sources de données de la base de données.
- Les versions antérieures du système d'exploitation Windows (par exemple, Windows 7 et Windows 8) désactivent la collection de l'attribut « heure du dernier accès » par défaut car elle peut avoir un impact sur les performances du système. Lorsque cet attribut n'est pas collecté, les analyses de classification BlueXP basées sur « l'heure du dernier accès » sont impactées. Vous pouvez activer la collecte de l'heure du dernier accès sur ces anciens systèmes Windows si nécessaire.

Horodatage du dernier accès

Lorsque la classification BlueXP extrait des données des partages de fichiers, le système d'exploitation les considère comme accédant aux données et modifie l'« heure du dernier accès » en conséquence. Après l'analyse, la classification BlueXP tente de rétablir l'horodatage d'origine pour l'heure du dernier accès. Si la classification BlueXP ne dispose pas d'autorisations d'attributs d'écriture dans CIFS, ou si elle ne dispose pas d'autorisations d'écriture dans NFS, le système ne peut pas rétablir l'heure du dernier accès à l'horodatage d'origine. Les volumes ONTAP configurés avec SnapLock disposent d'autorisations en lecture seule et ne peuvent pas non plus rétablir l'horodatage du dernier accès.

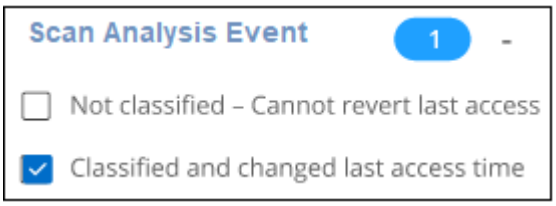
Par défaut, si la classification BlueXP ne dispose pas de ces autorisations, le système n'analyse pas ces fichiers dans vos volumes, car la classification BlueXP ne peut pas rétablir l'heure du dernier accès à l'horodatage d'origine. Cependant, si vous ne vous souciez pas si l'heure du dernier accès est réinitialisée à

l'heure d'origine dans vos fichiers, vous pouvez cliquer sur le commutateur **Scan en cas d'autorisations d'écriture d'attributs manquantes** en bas de la page de configuration pour que la classification BlueXP analyse les volumes indépendamment des autorisations.



Cette fonctionnalité s'applique aux systèmes ONTAP sur site, à Cloud Volumes ONTAP, Azure NetApp Files, FSX pour ONTAP et aux partages de fichiers tiers.

Notez qu'il existe un filtre dans la page Investigation appelé *Scan Analysis Event* qui vous permet d'afficher les fichiers qui n'ont pas été classés car la classification BlueXP n'a pas pu rétablir l'heure de dernier accès, Ou les fichiers classifiés même si la classification BlueXP ne pouvait pas rétablir l'heure du dernier accès.



Les sélections de filtre sont les suivantes :

- « Non classé — Impossible de rétablir l'heure du dernier accès » - affiche les fichiers qui n'ont pas été classés en raison de permissions d'écriture manquantes.
- « Heure du dernier accès classifiée et mise à jour » - affiche les fichiers classés et la classification BlueXP n'a pas pu rétablir l'heure du dernier accès à la date d'origine. Ce filtre n'est pertinent que pour les environnements dans lesquels vous avez activé **Scan lorsque vous ne disposez pas des autorisations d'écriture d'attributs**.

Si nécessaire, vous pouvez exporter ces résultats dans un rapport afin de voir quels fichiers sont ou ne sont pas analysés en raison des autorisations. "En savoir plus sur le rapport d'enquête sur les données".

Connectez-vous au système de classification BlueXP

Il se peut que vous deviez vous connecter au système de classification BlueXP pour pouvoir accéder aux fichiers journaux ou modifier les fichiers de configuration.

Lorsque la classification BlueXP est installée sur une machine Linux de votre site ou sur une machine Linux que vous avez déployée dans le cloud, vous pouvez accéder directement au fichier de configuration et au script.

Lorsque la classification BlueXP est déployée dans le cloud, vous devez établir une connexion SSH avec l'instance de classification BlueXP. Vous vous SSH dans le système en saisissant l'utilisateur et le mot de passe, ou en utilisant la clé SSH fournie lors de l'installation du connecteur BlueXP. La commande SSH est :

```
 ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
* <path_to_the_ssh_key> = emplacement des clés d'authentification ssh
* <machine_utilisateur> :
```

+
Pour AWS : utilisez <utilisateur ec2>
Pour Azure : utilisez l'utilisateur créé pour l'instance BlueXP
** Pour GCP : utilisez l'utilisateur créé pour l'instance BlueXP

- <dataense_ip> = adresse IP de l'instance de la machine virtuelle

Notez que vous devrez modifier les règles entrantes du groupe de sécurité pour accéder au système dans le cloud. Pour plus de détails, voir :

- "Règles de groupe de sécurité dans AWS"
- "Règles de groupe de sécurité dans Azure"
- "Règles de pare-feu dans Google Cloud"

API de classification BlueXP

Les fonctionnalités de classification de BlueXP disponibles via l'interface utilisateur web sont également disponibles via l'API swagger.

Quatre catégories de classification BlueXP correspondent aux onglets de l'interface utilisateur :

- Enquête
- La conformité
- La gouvernance
- Configuration

Les API de la documentation swagger vous permettent de rechercher, d'agréger des données, de suivre vos analyses et de créer des actions telles que la copie, le déplacement, etc.

Présentation

L'API vous permet d'effectuer les fonctions suivantes :

- Informations d'exportation
  - Tout ce qui est disponible dans l'interface utilisateur peut être exporté via l'API (à l'exception des rapports)
  - Les données sont exportées au format JSON (facile à analyser et à envoyer vers des applications tierces, telles que Splunk)
- Créez des requêtes à l'aide des instructions « ET » et « OU », incluez et excluez des informations, etc.

  Par exemple, vous pouvez localiser des fichiers *sans* informations personnelles identifiables (PII) spécifiques (fonctionnalité non disponible dans l'interface utilisateur). Vous pouvez également exclure des champs spécifiques pour l'opération d'exportation.

- Effectuer des actions
  - Mettre à jour les informations d'identification CIFS
  - Afficher et annuler des actions
  - Ré-analyser les répertoires
  - Exporter les données

L'API est sécurisée et utilise la même méthode d'authentification que l'interface utilisateur. Vous trouverez des informations sur l'authentification dans : https://docs.netapp.com/us-en/bluexp-automation/platform/get_identifiers.html

Accès à la référence de l'API swagger

Pour entrer dans swagger, vous devez disposer de l'adresse IP de votre instance de classification BlueXP. Dans le cas d'un déploiement cloud, vous utiliserez l'adresse IP publique. Ensuite, vous devrez entrer dans ce terminal :

https://<classification_ip>/documentation

Exemple d'utilisation des API

L'exemple suivant montre un appel d'API pour copier des fichiers.

Demande d'API

Vous devrez d'abord obtenir tous les champs et options pertinents pour un environnement de travail pour afficher tous les filtres dans l'onglet investigation.

```
curl -X GET "http://{classification_ip}/api/{classification_version}
/search/options?data_mode=ALL_EXTRACTABLE" -H "accept: application/json"
-H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… " -H "x-agent-id:
hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients"
```

Réponse

```
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "string",
      "is_rulable": true,
      "name": "string",
      "operators": [
        "EQUALS"
      ],
      "optional_values": [
        {}
      ],
```

```
      "secondary": {},
      "server_data": false,
      "type": "TEXT"
    }
  ]
}
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "POLICIES",
      "name": "Policies",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "EXTRACTION_STATUS_RANGE",
      "name": "Scan Analysis Status",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "SCAN_ANALYSIS_ERROR",
      "name": "Scan Analysis Event",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "PUBLIC_ACCESS",
```

```
      "name": "Open Permissions",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USERS_PERMISSIONS_COUNT_RANGE",
      "name": "Number of Users with Access",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": true,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "USER_GROUP_PERMISSIONS",
      "name": "User / Group Permissions",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_OWNER",
      "name": "File Owner",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
```

```
      "field": "ENVIRONMENT_TYPE",
      "name": "Working Environment Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ENVIRONMENT",
      "name": "Working Environment",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "SCAN_TASK",
      "name": "Storage Repository",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_PATH",
      "name": "File / Directory Path",
      "operators": [
        "MULTI_CONTAINS",
        "MULTI_EXCLUDE"
      ],
      "server_data": true,
      "type": "MULTI_TEXT"
    },
    {
```

```
      "active_directory_affected": false,
      "data_mode": "ALL_DASHBOARD_EXTRACTABLE",
      "field": "CATEGORY",
      "name": "Category",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_SENSITIVITY_LEVEL",
      "name": "Sensitivity Level",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "NUMBER_OF_IDENTIFIERS",
      "name": "Number of identifiers",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_PERSONAL",
      "name": "Personal Data",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
```

```
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "PATTERN_SENSITIVE",
      "name": "Sensitive Personal Data",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DATA_SUBJECT",
      "name": "Data Subject",
      "operators": [
        "EQUALS",
        "CONTAINS"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "DIRECTORIES",
      "field": "DIRECTORY_TYPE",
      "name": "Directory Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_TYPE",
      "name": "File Type",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
```

```
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "FILE_SIZE_RANGE",
      "name": "File Size",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_CREATION_RANGE_RETENTION",
      "name": "Created Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "DISCOVERED_TIME_RANGE",
      "name": "Discovered Time",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_MODIFICATION_RETENTION",
      "name": "Last Modified",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
```

```
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
      "field": "FILE_LAST_ACCESS_RANGE_RETENTION",
      "name": "Last Accessed",
      "operators": [
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "IS_DUPLICATE",
      "name": "Duplicates",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "FILES",
      "field": "FILE_HASH",
      "name": "File Hash",
      "operators": [
        "EQUALS",
        "IN"
      ],
      "server_data": true,
      "type": "TEXT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "USER_DEFINED_STATUS",
      "name": "Tags",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
```

```
      "type": "SELECT"
    },
    {
      "active_directory_affected": false,
      "data_mode": "ALL_EXTRACTABLE",
      "field": "ASSIGNED_TO",
      "name": "Assigned to",
      "operators": [
        "IN",
        "NOT_IN"
      ],
      "server_data": true,
      "type": "SELECT"
    }
  ]
}
```

Nous utiliserons cette réponse dans nos paramètres de demande pour filtrer les fichiers que nous voulons copier.

Vous pouvez appliquer une action à plusieurs éléments. Les types d'action pris en charge sont notamment : déplacer, supprimer, copier, attribuer à, FlexClone, exporter les données, renumériser et étiqueter.

Nous allons créer l'action de copie :

Demande d'API

Cette API suivante est cette API d'action et elle vous permet de créer plusieurs actions.

```
curl -X POST "http://
{classification_ip}/api//{classification_version}/actions" -H "accept:
application/json" -H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR…… "
-H "x-agent-id: hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients " -H "Content-
Type: application/json" -d "{ \"action_type\": \"COPY\", \"data_mode\":
\"FILES\", \"policy_id\": 0, \"request_params\": { destination_nfs_path:
"{ontap_ip}:/{share_name} " },
\"requested_query\":{"condition":"AND","rules":[{"field":"ENVIRONMENT_TYPE
","operator":"IN","value":["ONPREM"]},{"field":"CATEGORY","operator":"IN",
"value":["21"]}]}}"
```

Réponse

La réponse renvoie l'objet d'action, de sorte que vous pouvez utiliser les API GET et DELETE pour obtenir le statut de l'action ou pour l'annuler.

```
{
  "action_type": "COPY",
  "creation_time": "2023-08-08T12:37:21.705Z",
  "data_mode": "FILES",
  "end_time": "2023-08-08T12:37:21.705Z",
  "estimated_time_to_complete": 0,
  "id": 0,
  "policy_id": 0,
  "policy_name": "string",
  "priority": 0,
  "request_params": {},
  "requested_query": {},
  "result": {
    "error_message": "string",
    "failed": 0,
    "in_progress": 0,
    "succeeded": 0,
    "total": 0
  },
  "start_time": "2023-08-08T12:37:21.705Z",
  "status": "QUEUED",
  "title": "string",
  "user_id": "string"
}
```

Connaissances et support

S’inscrire pour obtenir de l’aide

L’enregistrement au support est requis pour recevoir le support technique spécifique à BlueXP et à ses solutions et services de stockage. L’enregistrement au support est également requis pour activer les principaux workflows des systèmes Cloud Volumes ONTAP.

L’inscription au support n’active pas le support NetApp pour un service de fichiers de fournisseur cloud. Pour obtenir de l’aide concernant un service de fichiers d’un fournisseur cloud, son infrastructure ou toute solution utilisant le service, consultez la section « obtention d’aide » de la documentation BlueXP associée à ce produit.

- "Amazon FSX pour ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service pour Google Cloud"

Présentation de l’inscription au support

Il existe deux types d’inscription pour activer les droits d’assistance :

- Enregistrement du numéro de série de votre compte BlueXP (votre numéro de série 960xxxxxxxxx à 20 chiffres, disponible sur la page des ressources de support de BlueXP).

  Il sert d’ID d’abonnement unique pour tous les services de BlueXP. Chaque abonnement au support BlueXP au niveau du compte doit être enregistré.

- Enregistrement des numéros de série Cloud Volumes ONTAP associés à un abonnement sur le marché de votre fournisseur cloud (numéros de série à 20 chiffres 909201xxxxxxxx).

  Ces numéros de série sont généralement appelés *PAYGO - numéros de série* et sont générés par BlueXP au moment du déploiement de Cloud Volumes ONTAP.

L’enregistrement des deux types de numéros de série offre des fonctionnalités telles que l’ouverture de tickets de support et la génération automatique de tickets. L’inscription est terminée en ajoutant des comptes du site de support NetApp (NSS) à BlueXP, comme décrit ci-dessous.

Enregistrez BlueXP pour bénéficier du support NetApp

Pour vous inscrire au support et activer votre droit de support, un utilisateur de votre entreprise (ou compte) BlueXP doit associer un compte du site de support NetApp à ses identifiants BlueXP . Le fait de vous inscrire au support NetApp dépend de la présence ou non d’un compte sur le site de support NetApp (NSS).

Client existant avec un compte NSS

Si vous êtes client NetApp avec un compte NSS, il vous suffit de vous inscrire pour obtenir du support dans BlueXP.

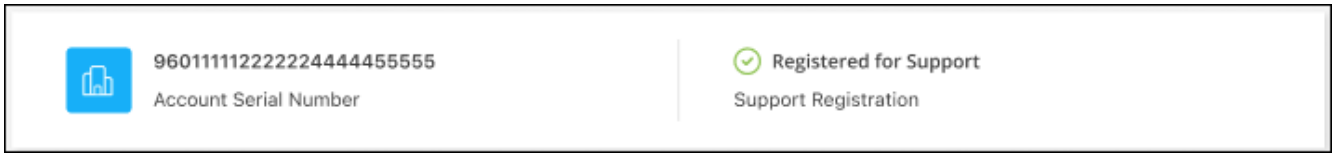
Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l’icône Paramètres, puis sélectionnez

informations d'identification.

2. Sélectionnez **informations d'identification utilisateur**.
3. Sélectionnez **Ajouter des informations d'identification NSS** et suivez l'invite authentification du site de support NetApp (NSS).
4. Pour confirmer que le processus d'enregistrement a réussi, sélectionnez l'icône aide et sélectionnez **support**.

   La page **Ressources** doit indiquer que votre organisation BlueXP est enregistrée pour le support.

   Notez que les autres utilisateurs BlueXP ne verront pas ce même statut d'enregistrement de support s'ils n'ont pas associé de compte sur le site de support NetApp à leur identifiant BlueXP. Cependant, cela ne signifie pas que votre entreprise BlueXP n'est pas enregistrée pour le support. Tant qu'un utilisateur de l'organisation a suivi ces étapes, votre organisation a été enregistrée.

Client existant mais aucun compte NSS

Si vous possédez déjà des licences et des numéros de série NetApp, mais que vous possédez un compte NSS, vous devez créer un compte NSS et l'associer à votre connexion BlueXP.

Étapes

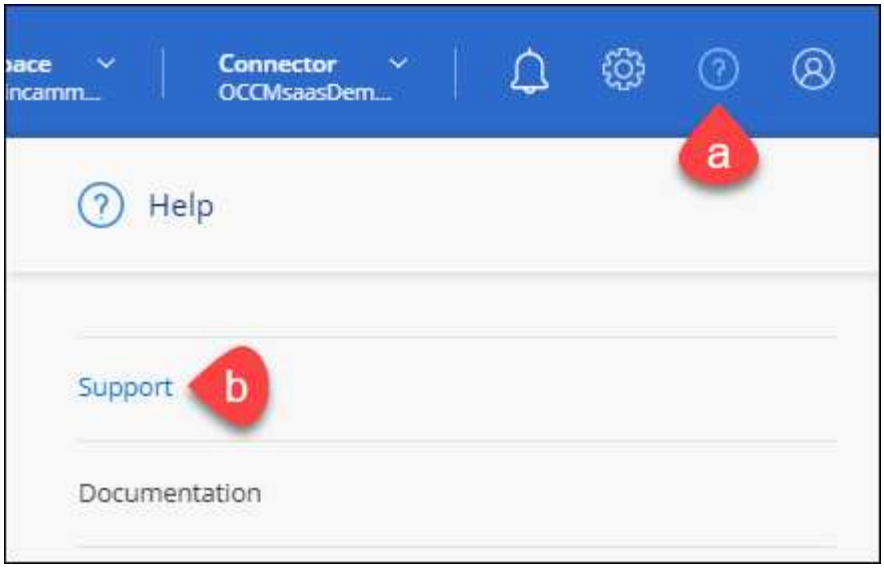
1. Créez un compte sur le site de support NetApp en complétant le "Formulaire d'inscription de l'utilisateur du site de support NetApp"
   a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
   b. Veillez à copier le numéro de série du compte BlueXP (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.
2. Associez votre nouveau compte NSS à votre connexion BlueXP en suivant les étapes décrites sous Client existant avec un compte NSS.

Découvrez la toute nouvelle gamme NetApp

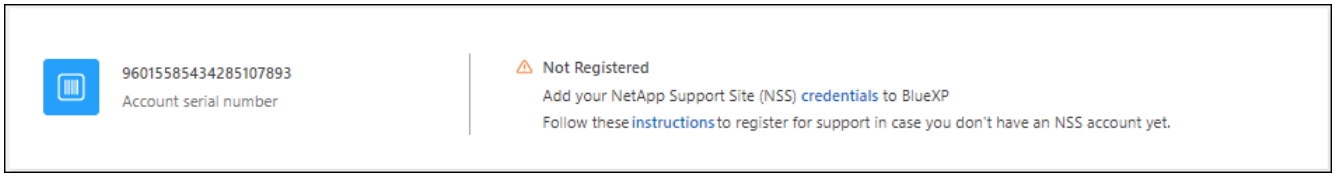
Si vous êtes nouveau chez NetApp et que vous ne disposez pas d'un compte NSS, effectuez chacune des étapes ci-dessous.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône aide, puis sélectionnez **support**.



2. Recherchez le numéro de série de l'ID de compte sur la page d'inscription au support.



3. Accédez à "Site d'inscription au support NetApp" Et sélectionnez **je ne suis pas un client NetApp enregistré**.
4. Remplissez les champs obligatoires (ceux avec des astérisques rouges).
5. Dans le champ **Product Line**, sélectionnez **Cloud Manager**, puis votre fournisseur de facturation applicable.
6. Copiez le numéro de série de votre compte à l'étape 2 ci-dessus, vérifiez sa sécurité, puis lisez la Déclaration de confidentialité des données NetApp.

   Un e-mail est immédiatement envoyé à la boîte aux lettres fournie pour finaliser cette transaction sécurisée. Assurez-vous de vérifier vos dossiers de courrier indésirable si l'e-mail de validation n'arrive pas dans quelques minutes.

7. Confirmez l'action à partir de l'e-mail.

   La confirmation de la soumission de votre demande à NetApp et vous recommande de créer un compte sur le site de support NetApp.

8. Créez un compte sur le site de support NetApp en complétant le "Formulaire d'inscription de l'utilisateur du site de support NetApp"
   a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
   b. Veillez à copier le numéro de série du compte (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Cela accélère le traitement.

Une fois que vous avez terminé

NetApp devrait vous contacter au cours de ce processus. Il s'agit d'un exercice d'intégration unique pour les nouveaux utilisateurs.

Une fois que vous possédez votre compte sur le site de support NetApp, associez-le à votre connexion BlueXP en suivant les étapes décrites sous Client existant avec un compte NSS.

Associer les informations d'identification NSS pour le support Cloud Volumes ONTAP

L'association des informations d'identification du site de support NetApp à votre organisation BlueXP est nécessaire pour activer les flux de travail clés suivants pour Cloud Volumes ONTAP :

- Enregistrement des systèmes Cloud Volumes ONTAP avec paiement à l'utilisation pour bénéficier d'une assistance

  Vous devez fournir votre compte NSS afin d'activer le support pour votre système et d'accéder aux ressources du support technique NetApp.

- Déploiement d'Cloud Volumes ONTAP avec modèle BYOL (Bring Your Own License)

  Il est nécessaire de fournir votre compte NSS afin que BlueXP puisse télécharger votre clé de licence et activer l'abonnement pour la durée que vous avez achetée. Cela inclut des mises à jour automatiques pour les renouvellements de contrats.

- Mise à niveau du logiciel Cloud Volumes ONTAP vers la dernière version

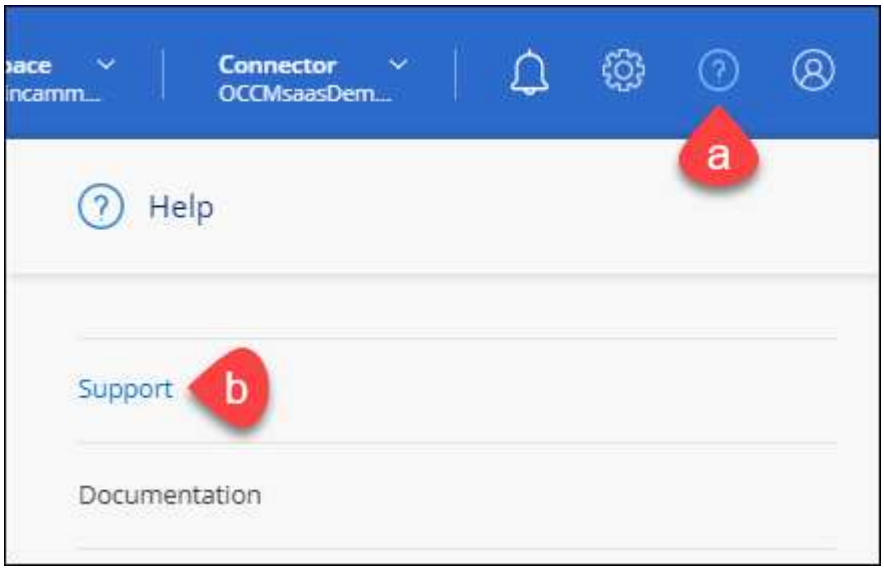
L'association des informations d'identification NSS à votre organisation BlueXP est différente du compte NSS associé à une connexion utilisateur BlueXP .

Ces informations d'identification NSS sont associées à votre identifiant d'organisation BlueXP spécifique. Les utilisateurs qui appartiennent à l'organisation BlueXP peuvent accéder à ces informations d'identification à partir de **support > gestion NSS**.

- Si vous avez un compte au niveau du client, vous pouvez ajouter un ou plusieurs comptes NSS.
- Si vous avez un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés en même temps que les comptes au niveau du client.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône aide, puis sélectionnez **support**.



2. Sélectionnez **gestion NSS > Ajouter un compte NSS**.
3. Lorsque vous y êtes invité, sélectionnez **Continuer** pour être redirigé vers une page de connexion Microsoft.

   NetApp utilise Microsoft Entra ID comme fournisseur d'identité pour les services d'authentification spécifiques à la prise en charge et à l'octroi de licences.

4. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

   Ces actions permettent à BlueXP d'utiliser votre compte NSS pour des opérations telles que le téléchargement de licences, la vérification de la mise à niveau logicielle et les inscriptions de support futures.

   Notez ce qui suit :

   - Le compte NSS doit être un compte de niveau client (pas un compte invité ou temporaire). Vous pouvez avoir plusieurs comptes NSS de niveau client.
   - Il ne peut y avoir qu'un seul compte NSS si ce compte est un compte de niveau partenaire. Si vous essayez d'ajouter des comptes NSS de niveau client et qu'un compte de niveau partenaire existe, le message d'erreur suivant s'affiche :

     "Le type de client NSS n'est pas autorisé pour ce compte car il existe déjà des utilisateurs NSS de type différent."

   Il en va de même si vous possédez des comptes NSS client préexistants et que vous essayez d'ajouter un compte de niveau partenaire.

   - Une fois la connexion établie, NetApp stockera le nom d'utilisateur NSS.

     Il s'agit d'un ID généré par le système qui correspond à votre courrier électronique. Sur la page **NSS Management**, vous pouvez afficher votre courriel à partir du ••• menu.

   - Si vous avez besoin d'actualiser vos jetons d'identification de connexion, il existe également une option **mettre à jour les informations d'identification** dans le ••• menu.

     Cette option vous invite à vous reconnecter. Notez que le jeton de ces comptes expire après 90 jours. Une notification sera publiée pour vous en informer.

Obtenez de l'aide

NetApp prend en charge BlueXP et ses services cloud de différentes manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24 h/24 et 7 j/7, comme des articles de la base de connaissances (KB) et un forum communautaire. Votre inscription au support inclut un support technique à distance via la création de tickets en ligne.

Bénéficiez du support pour les services de fichiers d'un fournisseur cloud

Pour obtenir de l'aide concernant un service de fichiers d'un fournisseur cloud, son infrastructure ou toute solution utilisant le service, consultez la section « obtention d'aide » de la documentation BlueXP associée à ce produit.

- "Amazon FSX pour ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes Service pour Google Cloud"

Pour bénéficier du support technique spécifique à BlueXP et à ses solutions et services de stockage, utilisez les options de support décrites ci-dessous.

Utilisation d'options de support en libre-service

Ces options sont disponibles gratuitement, 24 heures sur 24, 7 jours sur 7 :

- Documentation

  La documentation BlueXP que vous consultez actuellement.

- "Base de connaissances"

  Recherchez dans la base de connaissances BlueXP des articles utiles pour résoudre les problèmes.

- "Communautés"

  Rejoignez la communauté BlueXP pour suivre des discussions en cours ou en créer de nouveaux.

Créez un dossier de demande de support auprès du support NetApp

Outre les options d'auto-support mentionnées ci-dessus, vous pouvez travailler avec un spécialiste du support NetApp pour résoudre tous les problèmes après avoir activé le service de support.

Avant de commencer

- Pour utiliser la fonctionnalité **Créer un cas**, vous devez d'abord associer vos informations d'identification du site de support NetApp à votre connexion BlueXP. "Découvrez comment gérer les identifiants associés à votre connexion BlueXP".
- Si vous ouvrez un dossier pour un système ONTAP doté d'un numéro de série, votre compte NSS doit être associé au numéro de série de ce système.

Étapes

1. Dans BlueXP, sélectionnez **aide > support**.
2. Sur la page **Ressources**, choisissez l'une des options disponibles sous support technique :

   a. Sélectionnez **appelez-nous** si vous souhaitez parler avec quelqu'un au téléphone. Vous serez dirigé vers une page netapp.com qui répertorie les numéros de téléphone que vous pouvez appeler.

   b. Sélectionnez **Créer un cas** pour ouvrir un ticket avec un spécialiste du support NetApp :

      - **Service** : sélectionnez le service auquel le problème est associé. Par exemple, BlueXP lorsqu'il est spécifique à un problème de support technique avec des flux de travail ou des fonctionnalités au sein du service.
      - **Environnement de travail** : si applicable au stockage, sélectionnez **Cloud Volumes ONTAP** ou **sur site**, puis l'environnement de travail associé.

        La liste des environnements de travail s'applique à l'organisation (ou au compte), au projet (ou à l'espace de travail) et au connecteur BlueXP que vous avez sélectionnés dans la bannière

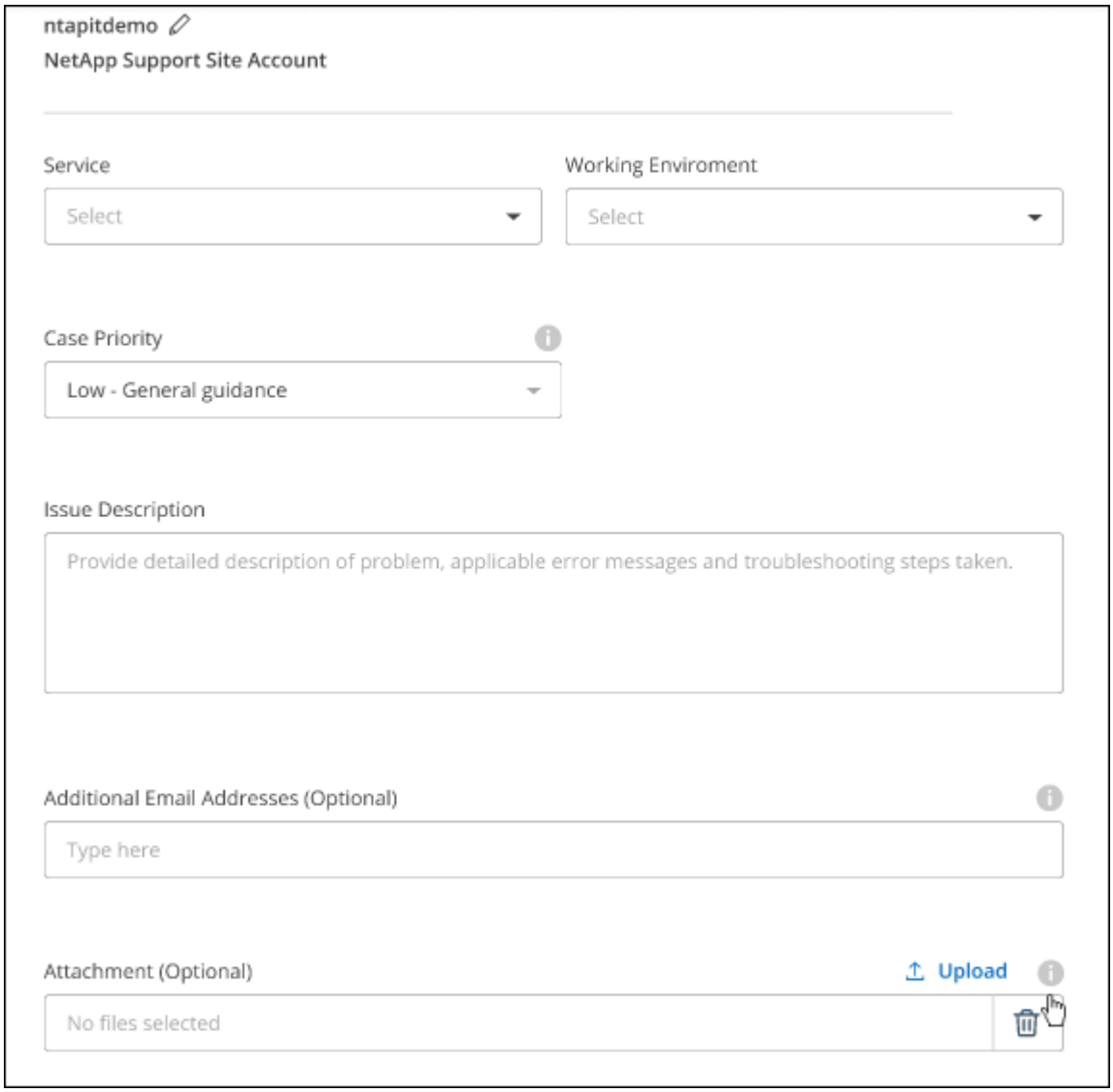
supérieure du service.

- **Priorité du cas** : choisissez la priorité du cas, qui peut être faible, Moyen, élevé ou critique.

  Pour en savoir plus sur ces priorités, passez votre souris sur l'icône d'information située à côté du nom du champ.

- **Description du problème** : fournir une description détaillée de votre problème, y compris les messages d'erreur ou les étapes de dépannage applicables que vous avez effectués.
- **Adresses e-mail supplémentaires**: Entrez des adresses e-mail supplémentaires si vous souhaitez informer quelqu'un d'autre de ce problème.
- **Pièce jointe (facultatif)** : téléchargez jusqu'à cinq pièces jointes, une à la fois.

  Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichier suivantes sont prises en charge : txt, log, PDF, jpg/JPEG, rtf, doc/docx, xls/xlsx et csv.



Une fois que vous avez terminé

Une fenêtre contextuelle contenant votre numéro de dossier de support s'affiche. Un spécialiste du support NetApp va étudier votre dossier et vous recontacterons très rapidement.

Pour un historique de vos dossiers de support, vous pouvez sélectionner **Paramètres > Chronologie** et rechercher les actions nommées "Créer un dossier de support". Un bouton situé à l'extrême droite vous permet de développer l'action pour afficher les détails.

Il est possible que vous rencontriez le message d'erreur suivant lors de la création d'un dossier :

« Vous n'êtes pas autorisé à créer un dossier pour le service sélectionné »

Cette erreur peut signifier que le compte NSS et la société d'enregistrement auquel il est associé n'est pas la même société d'enregistrement pour le numéro de série du compte BlueXP (par exemple 960xxxx) ou le numéro de série de l'environnement de travail. Vous pouvez demander de l'aide en utilisant l'une des options suivantes :

- Utilisez le chat du produit
- Soumettre un dossier non technique à https://mysupport.netapp.com/site/help

Gestion de vos dossiers de demande de support (aperçu)

Vous pouvez afficher et gérer les dossiers de support actifs et résolus directement à partir de BlueXP. Vous pouvez gérer les dossiers associés à votre compte NSS et à votre entreprise.

La gestion des dossiers est disponible en tant qu'aperçu. Nous prévoyons d'affiner cette expérience et d'ajouter des améliorations dans les prochaines versions. Envoyez-nous vos commentaires à l'aide de l'outil de chat In-Product.

Notez ce qui suit :

- Le tableau de bord de gestion des dossiers en haut de la page propose deux vues :
  - La vue de gauche affiche le nombre total de dossiers ouverts au cours des 3 derniers mois par le compte NSS utilisateur que vous avez fourni.
  - La vue de droite affiche le nombre total de dossiers ouverts au cours des 3 derniers mois au niveau de votre entreprise en fonction de votre compte NSS utilisateur.

  Les résultats du tableau reflètent les cas liés à la vue que vous avez sélectionnée.

- Vous pouvez ajouter ou supprimer des colonnes d'intérêt et filtrer le contenu des colonnes telles que priorité et Statut. D'autres colonnes offrent uniquement des fonctions de tri.

  Pour plus d'informations, consultez les étapes ci-dessous.

- Au niveau de chaque dossier, nous offrons la possibilité de mettre à jour les notes de dossier ou de fermer un dossier qui n'est pas déjà à l'état fermé ou en attente fermée.

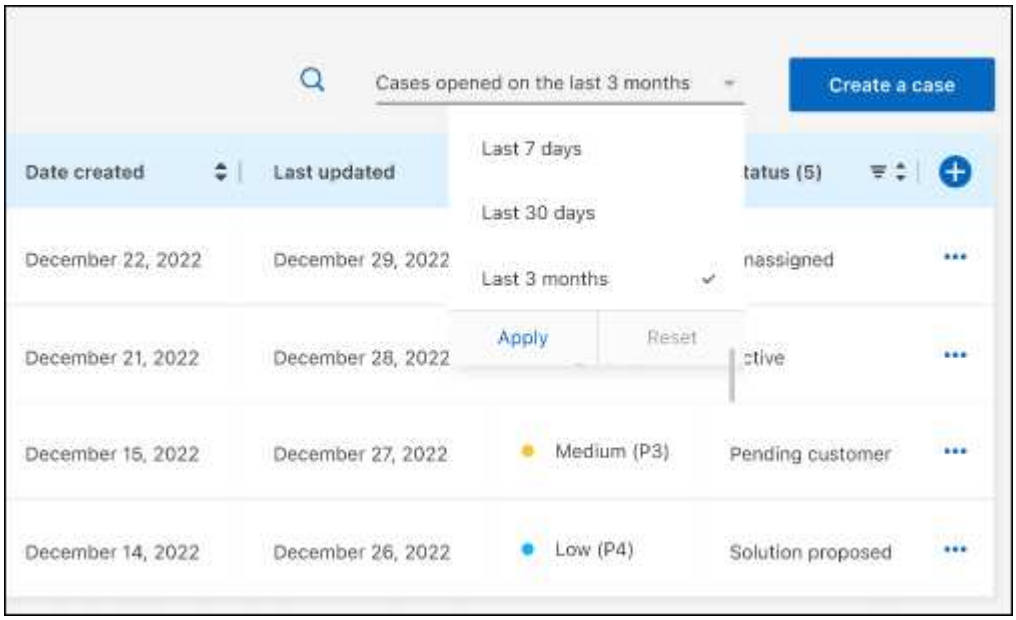
Étapes

1. Dans BlueXP, sélectionnez **aide > support**.
2. Sélectionnez **case Management** et si vous y êtes invité, ajoutez votre compte NSS à BlueXP.

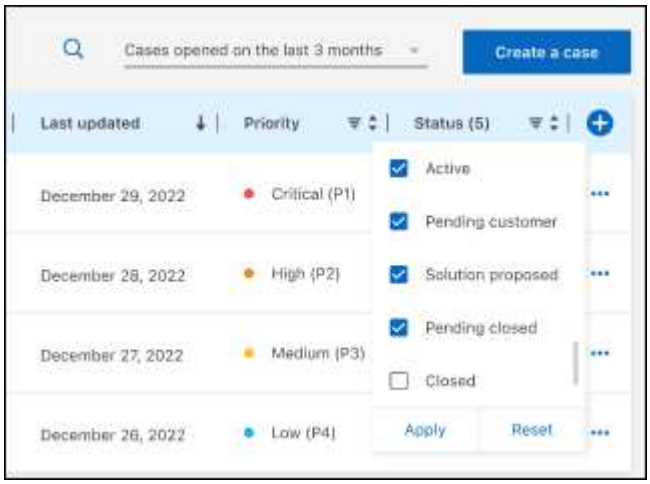
   La page **gestion des cas** affiche les cas ouverts associés au compte NSS associé à votre compte utilisateur BlueXP. Il s'agit du même compte NSS qui apparaît en haut de la page **gestion NSS**.

3. Modifiez éventuellement les informations qui s'affichent dans le tableau :
   - Sous **cas de l'organisation**, sélectionnez **Afficher** pour afficher tous les cas associés à votre société.

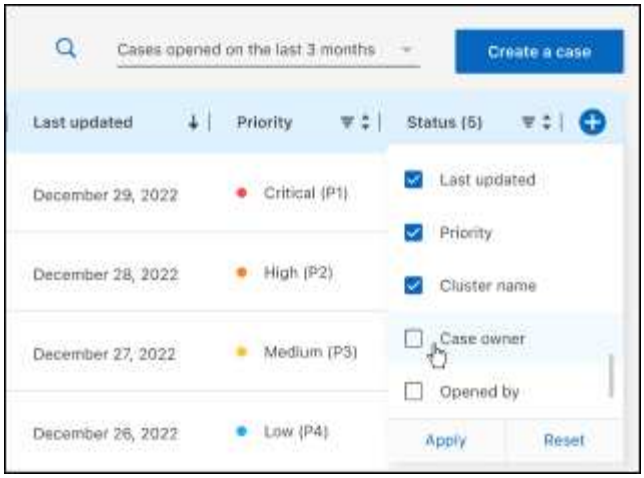
- Modifiez la plage de dates en choisissant une plage de dates exacte ou en choisissant une autre période.



- Filtrez le contenu des colonnes.



- Modifiez les colonnes qui apparaissent dans le tableau en sélectionnant puis choisissez les colonnes que vous souhaitez afficher.

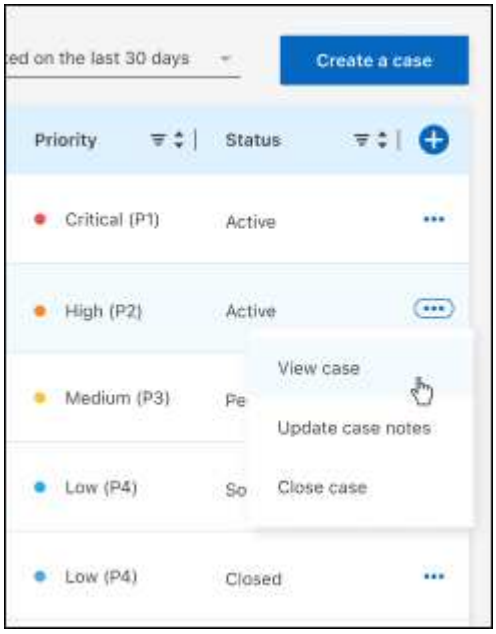


4. Gérer un dossier existant en sélectionnant ••• et en sélectionnant l'une des options disponibles :

   - **Voir cas**: Afficher tous les détails sur un cas spécifique.
   - **Mettre à jour les notes de cas** : fournir des détails supplémentaires sur votre problème ou sélectionner **Télécharger les fichiers** pour joindre jusqu'à cinq fichiers.

     Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichier suivantes sont prises en charge : txt, log, PDF, jpg/JPEG, rtf, doc/docx, xls/xlsx et csv.

   - **Fermer le cas** : fournissez des détails sur la raison pour laquelle vous fermez le cas et sélectionnez **Fermer le cas**.



Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d'auteur

"https://www.netapp.com/company/legal/copyright/"

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

- "Note pour BlueXP"
- "Notez la classification BlueXP"