



Utilisez la classification BlueXP

BlueXP classification

NetApp
July 22, 2025

Sommaire

Utilisez la classification BlueXP	1
Affichez les détails de gouvernance sur les données stockées dans votre entreprise avec la classification BlueXP	1
Passez en revue le tableau de bord gouvernance	1
Créez le rapport d'évaluation de la découverte de données	4
Créez le rapport de présentation du mappage de données	4
Affichez les détails de conformité sur les données privées stockées dans votre entreprise avec la classification BlueXP	7
Afficher les fichiers contenant des données personnelles	8
Affichez les fichiers contenant des données personnelles sensibles	10
Afficher les fichiers par catégories	12
Afficher les fichiers par type de fichier	13
Catégories de données privées classées par BlueXP	14
Types de données personnelles	14
Types de données personnelles sensibles	19
Types de catégories	20
Types de fichiers	21
Exactitude des informations trouvées	22
Créer une classification personnalisée dans la classification BlueXP	22
Créer une classification personnalisée	22
Analysez les données stockées dans votre entreprise avec la classification BlueXP	24
Filtrez les données dans la page Data Investigation	24
Afficher les métadonnées de fichier	28
Afficher les autorisations des utilisateurs pour les fichiers et les répertoires	29
Vérifiez la présence de fichiers en double dans vos systèmes de stockage	30
Créer le rapport d'enquête sur les données	31
Créer une recherche enregistrée en fonction des filtres sélectionnés	34
Gestion des recherches enregistrées avec la classification BlueXP	35
Afficher les résultats des recherches enregistrées dans la page Investigation	35
Créer des recherches enregistrées personnalisées	35
Modifier les recherches enregistrées	37
Supprimer les recherches enregistrées	39
Recherches par défaut	39
Modifiez les paramètres d'analyse de classification BlueXP pour vos référentiels	40
Afficher l'état d'analyse de vos référentiels	40
Modifier le type de numérisation d'un référentiel	41
Hiérarchiser les acquisitions	42
Arrêter la recherche d'un référentiel	43
Mettre en pause et reprendre l'analyse d'un référentiel	44
Consultez les rapports de conformité à la classification BlueXP	44
Sélectionnez les environnements de travail pour les rapports	45
Rapport de demande d'accès de la personne concernée	46
Rapport conforme à la loi américaine sur la transférabilité et la responsabilité en matière d'assurance	

maladie (HIPAA)	48
Rapport sur la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)	49
Rapport d'évaluation des risques pour la confidentialité	50

Utilisez la classification BlueXP

Affichez les détails de gouvernance sur les données stockées dans votre entreprise avec la classification BlueXP

Maîtrisez les coûts liés aux données sur les ressources de stockage de votre organisation. 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.

C'est là que vous devriez commencer votre recherche. Dans le tableau de bord gouvernance, vous pouvez sélectionner une zone pour une investigation plus approfondie.

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.

Passez en revue le 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.

NetApp BlueXP Demo | Organization: Demo SIM | Project: gruno | Connector: OCCMassDem...

Classification | Governance | Compliance | Investigation | Classification settings | Policies | Configuration

Savings Opportunities

Scale Data

216.2K Items | 227.8 GB

Optimize Storage

Non-Business Data

18.6K Items | 24.3 GB

Optimize Storage

Duplicate Files

159.8K Items | 188.6 GB

Optimize Storage

Policies

[View All](#)

bb1	132.3K Items
Data 3-5 years old	105.9K Items

Data Overview

[Data Discovery Assessment Report](#) |
 [Full Data Mapping Overview Report](#) |
 Scanned: 265.3 GB |
 270.6K Files |
 141 Tables

Top Data Repositories by Sensitivity Level

Repository	Non-Sensitive	Personal	Sensitive	Total Items
CVO	~50%	~30%	~20%	133.8K
Amazon S3	~50%	~30%	~20%	131.5K
File Shares	~50%	~30%	~20%	5.2K
Database	~50%	~30%	~20%	141

Sensitive Data and Wide Permissions

Y-axis: Detected sensitive identifiers (Sensitive to Not sensitive)
X-axis: Users with access (Restrictive to Permissive)

Open Permissions

Legend: 31% - No Open Permissions, 48% - Open to Organization, 11% - Open to Public

Age of Data

Modified | Created | Last Accessed

Y-axis: Number of Files (0 to 120K)
X-axis: Time (30 days to Over 7 years)

Size of Data

Y-axis: Number of Files (0 to 240K)
X-axis: Size (100 bytes to 1GB)

Classification

40 Categories

[View All](#)

Miscellaneous	18.2K Items
Code	18K Items
Bank Statements	13K Items
Miscellaneous Spreadsheets	5.2K Items

127 File Types

[View All](#)

PDF	99.9K Items
TXT	88.9K Items
DOCX	31.4K Items
MXP	16K Items

Classification Documentation | v1.41.0

Étapes

1. Dans le menu BlueXP , sélectionnez **gouvernance > Classification**.
2. Sélectionnez **gouvernance**.

Le tableau de bord gouvernance s'affiche.

Consultez les opportunités d'économies

Le composant « Opportunités d'économie » affiche les données que vous pouvez supprimer ou transférer vers un stockage d'objets moins coûteux. Les données de « Opportunités d'économie » sont mises à jour toutes les deux heures et peuvent être mises à jour manuellement.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **gouvernance**.
2. Dans chaque mosaïque opportunités d'économies du tableau de bord gouvernance, sélectionnez **optimiser le stockage** pour afficher les résultats filtrés dans la page Investigation. Pour découvrir les données que vous devriez supprimer ou transférer vers un stockage moins coûteux, étudiez les *Opportunités d'économie*.
 - **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*.

Examinez les recherches enregistrées avec le plus grand nombre de résultats

Dans l'onglet *saved researchs*, les recherches avec le plus grand nombre de résultats apparaissent en haut de la liste. Ces données sont mises à jour toutes les deux heures.

Pour plus d'informations sur les recherches enregistrées, reportez-vous à "[Créer des recherches enregistrées](#)" la section .

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **gouvernance**.
2. Dans le tableau de bord de gouvernance, recherchez la mosaïque Recherches enregistrées. Sélectionnez le nom d'une recherche enregistrée pour afficher les résultats dans la page Investigation.

3. Sélectionnez **Afficher tout** pour afficher la liste de toutes les recherches enregistrées disponibles. Dans la zone *saved recherchts*, les recherches avec le plus grand nombre de résultats apparaissent en haut de la liste.

Créez le rapport d'évaluation de la découverte de données

Le rapport d'évaluation de la découverte de données fournit une analyse de haut niveau de l'environnement analysé afin 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 :

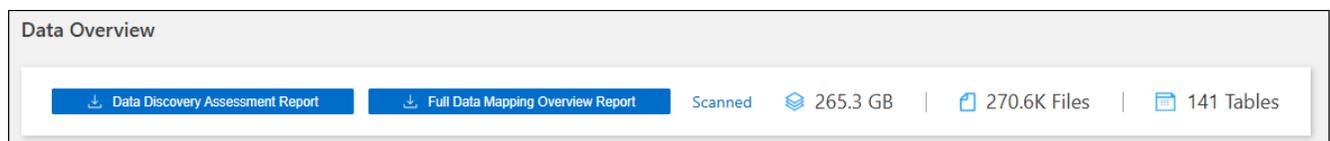
Fonction	Description
Problèmes de gouvernance des données	Une vue d'ensemble détaillée de toutes les données que vous possédez et des zones dans lesquelles vous pouvez réduire la quantité de données pour réduire les coûts.
Risques liés à la sécurité des données	Zones où vos données sont accessibles pour 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).

À l'aide de ce rapport, vous pouvez effectuer les actions suivantes :

- 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

Étapes

1. Dans le menu BlueXP , sélectionnez **gouvernance > Classification**.
2. Sélectionnez **gouvernance**.
3. Sélectionnez **Rapport d'évaluation de la découverte de données**.



Résultat

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

Créez le rapport de présentation du mappage de données

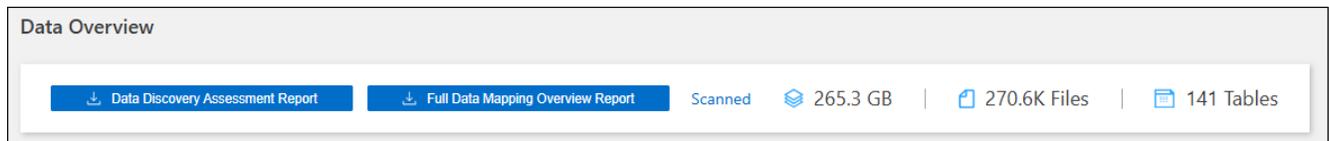
Le rapport de présentation du mappage de données fournit une vue d'ensemble des données stockées dans vos sources de données d'entreprise pour vous aider à prendre des décisions concernant les processus de migration, de sauvegarde, de sécurité et de conformité. Le rapport résume tous les environnements de travail et sources de données. Il fournit également 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.

Étapes

1. Dans le menu BlueXP , sélectionnez **gouvernance > Classification**.
2. Sélectionnez **gouvernance**.
3. Sélectionnez **Rapport de vue d'ensemble de la cartographie de données complètes**.



4. Pour personnaliser le nom de la société qui apparaît sur la première page du rapport, dans le coin supérieur droit de la page de classification BlueXP , sélectionnez  . Sélectionnez ensuite **changer le nom de la société**. La prochaine fois que vous générez le rapport, il inclura le nouveau nom.

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 devrez vous connecter en SSH à l'instance de classification BlueXP pour télécharger le fichier .pdf.

Consultez les principaux référentiels de données répertoriés par sensibilité des données

La section *meilleurs référentiels de données par niveau de sensibilité* du rapport de présentation de la cartographie de données 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

Ces données sont actualisées toutes les deux heures et peuvent être actualisées manuellement.

Étapes

1. Pour voir le nombre total d'éléments dans chaque catégorie, placez votre curseur sur chaque section de la barre.
2. Pour filtrer les résultats qui apparaîtront dans la page Enquête, sélectionnez chaque zone dans la barre et approfondissez vos recherches.

Passez en revue les données sensibles et les autorisations étendues

La zone *données sensibles et autorisations étendues* du rapport vue d'ensemble du mappage de données indique le pourcentage de fichiers contenant des données sensibles et ayant des autorisations étendues. Le graphique montre les types d'autorisations suivants :

- Des autorisations les plus restrictives aux restrictions les plus permissives sur l'axe horizontal.
- Des données les moins sensibles aux données les plus sensibles sur l'axe vertical.

Étapes

1. Pour voir le nombre total de fichiers dans chaque catégorie, placez votre curseur sur chaque case.
2. Pour filtrer les résultats qui apparaîtront dans la page Investigation, sélectionnez une case et recherchez plus loin.

Consultez les données répertoriées par type d'autorisations ouvertes

La zone *Open permissions* du rapport Data Mapping Overview indique le pourcentage pour chaque type d'autorisations existant pour tous les fichiers analysés. Le graphique montre les types d'autorisations suivants :

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

Étapes

1. Pour voir le nombre total de fichiers dans chaque catégorie, placez votre curseur sur chaque case.
2. Pour filtrer les résultats qui apparaîtront dans la page Investigation, sélectionnez une case et recherchez plus loin.

Vérifiez l'âge et la taille des données

Vous pouvez examiner les éléments des graphiques *Age* et *Size* du rapport Data Mapping Overview pour voir s'il y a des données que vous devez supprimer ou mettre en niveau vers un stockage objet moins coûteux.

Étapes

1. Dans le graphique *Age of Data*, pour afficher des détails sur l'âge des données, placez votre curseur sur un point du graphique.
2. Pour filtrer par tranche d'âge ou par plage de taille, sélectionnez cette taille ou cette taille.
 - **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*.

Passez en revue les classifications de données les plus identifiées

La zone *Classification* du rapport vue d'ensemble du mappage de données fournit une liste des données les plus identifiées "**Catégories**" et "**Types de fichiers**" de vos données numérisées.

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 plus d'informations.

Étapes

1. Dans le menu BlueXP , sélectionnez **gouvernance > Classification**.
2. Sélectionnez **Gouvernance** puis 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.

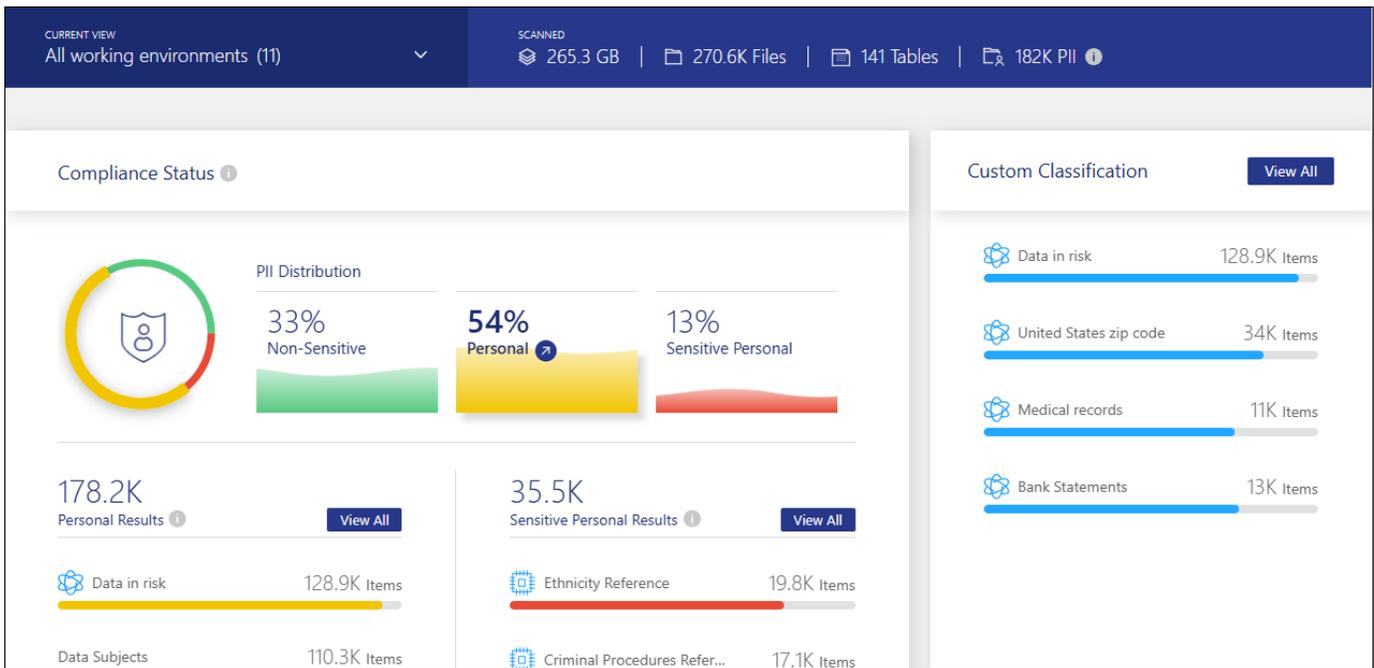
Affichez les détails de conformité sur les données privées stockées dans votre entreprise avec la classification BlueXP

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. Pour afficher les données de certains environnements de travail uniquement, sélectionnez-les.



Filtrez les résultats de la page enquête de données et téléchargez un rapport des résultats sous forme de fichier CSV. Voir "[Filtrage des données dans la page Data Investigation](#)" pour plus de détails.

Afficher les fichiers contenant des données personnelles

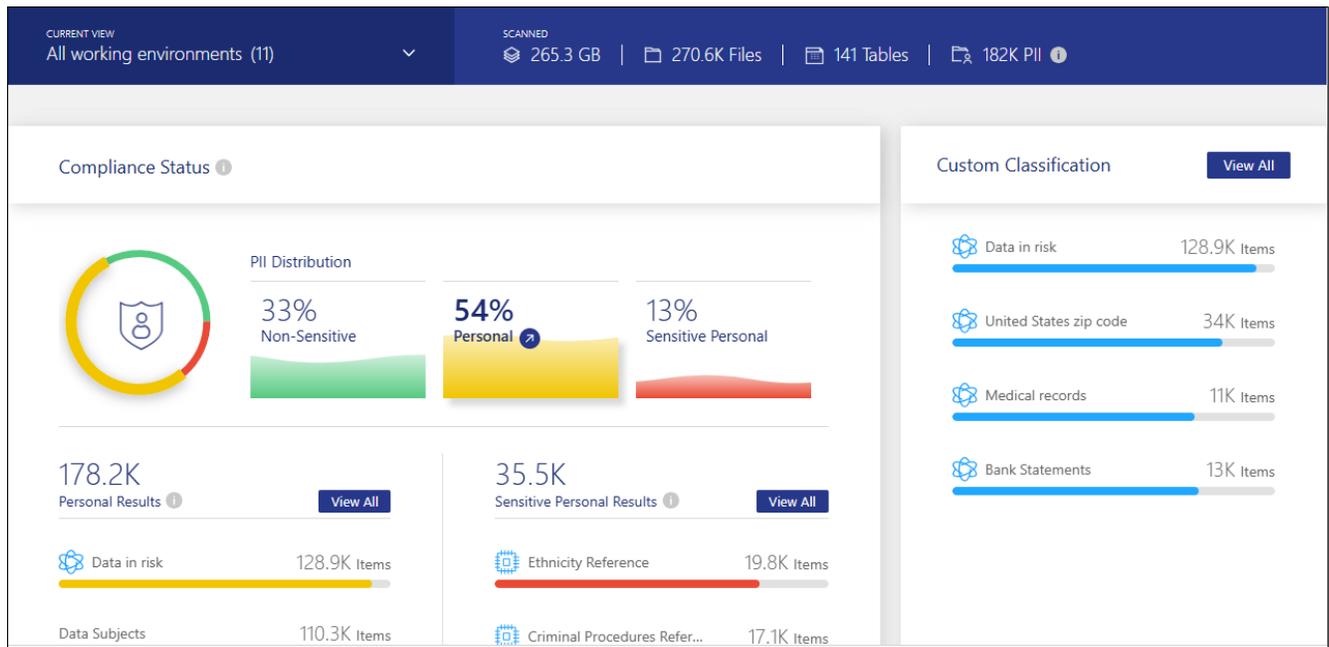
La classification BlueXP identifie automatiquement des mots, des chaînes et des modèles spécifiques (Regex) à l'intérieur des données. Par exemple, les renseignements d'identification personnelle (RP), les numéros de carte de crédit, les numéros de sécurité sociale, les numéros de compte bancaire, les 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.

Vous pouvez également créer des termes de recherche personnalisés pour identifier les données personnelles spécifiques à votre entreprise. Pour plus d'informations, voir "[Créer une classification personnalisée](#)".

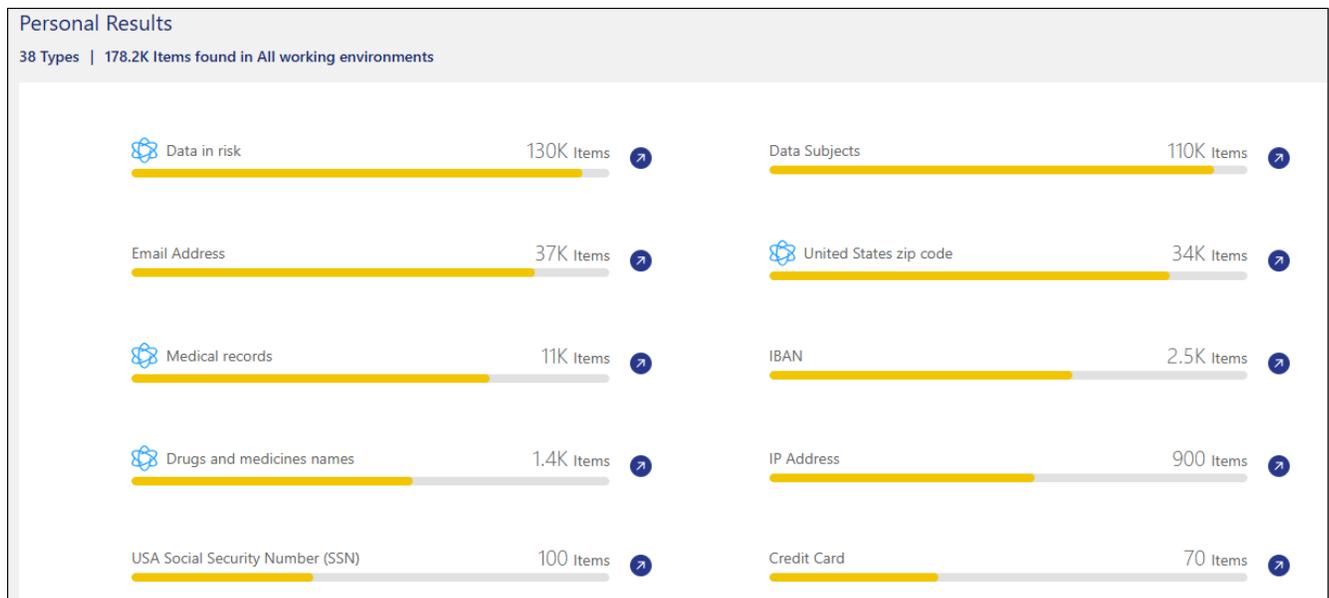
Pour certains types de données personnelles, la classification BlueXP utilise la *validation de proximité* pour valider ses résultats. La validation se produit en recherchant un ou plusieurs mots clés prédéfinis à proximité des données personnelles trouvées. Par exemple, la classification BlueXP identifie un numéro de sécurité sociale américain (SSN) comme un SSN s'il voit un mot de proximité à côté de lui—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 BlueXP Classification, sélectionnez l'onglet **conformité**.
2. Pour examiner les détails de toutes les données personnelles, sélectionnez l'icône en regard du pourcentage de données personnelles.

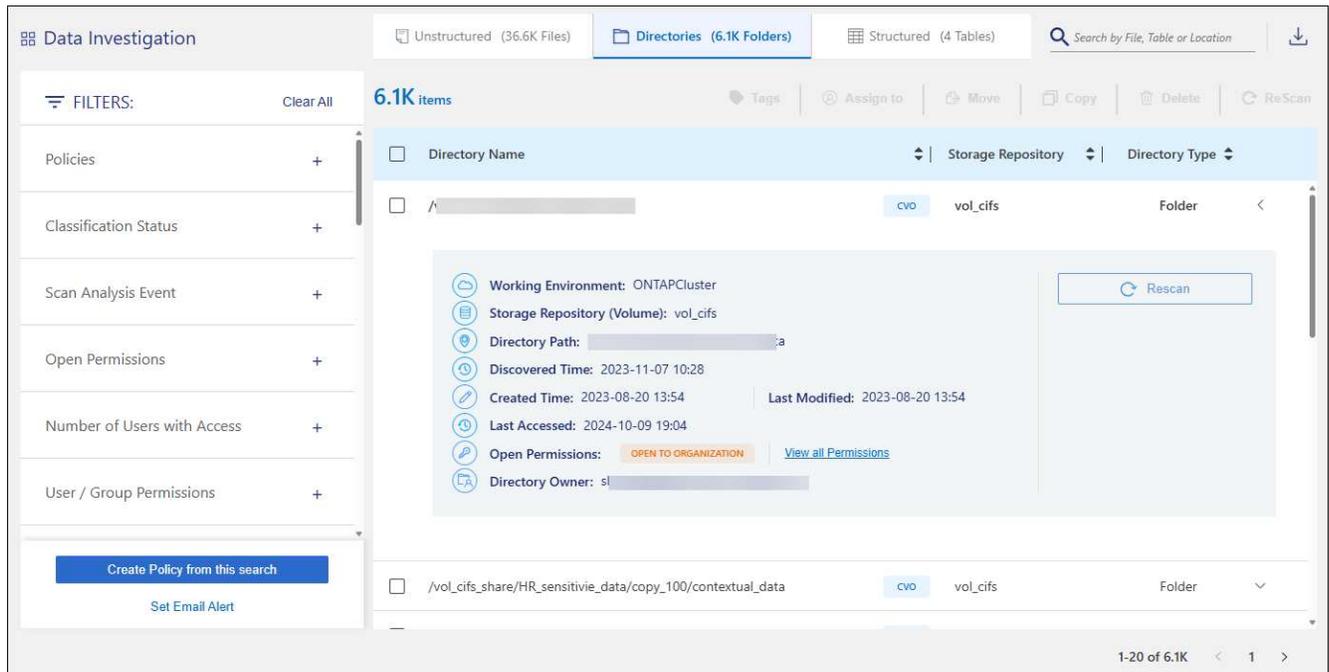
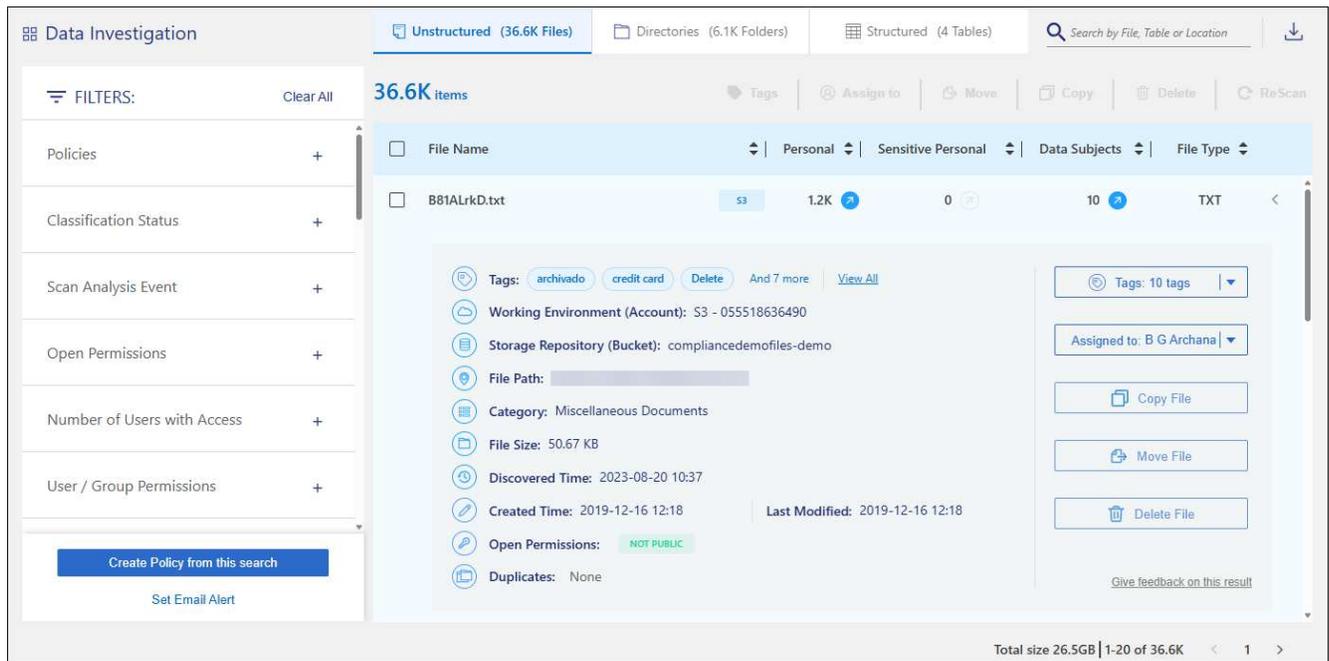


3. Pour examiner les détails d'un type spécifique de données personnelles, sélectionnez **Afficher tout**, puis sélectionnez la flèche **examiner les résultats** pour un type spécifique de données personnelles, par exemple les adresses électroniques.



4. Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en sélectionnant la flèche **examiner les résultats** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.

Les deux 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 les types spéciaux de renseignements personnels sensibles, tels que définis par les réglementations sur la confidentialité telles que "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.

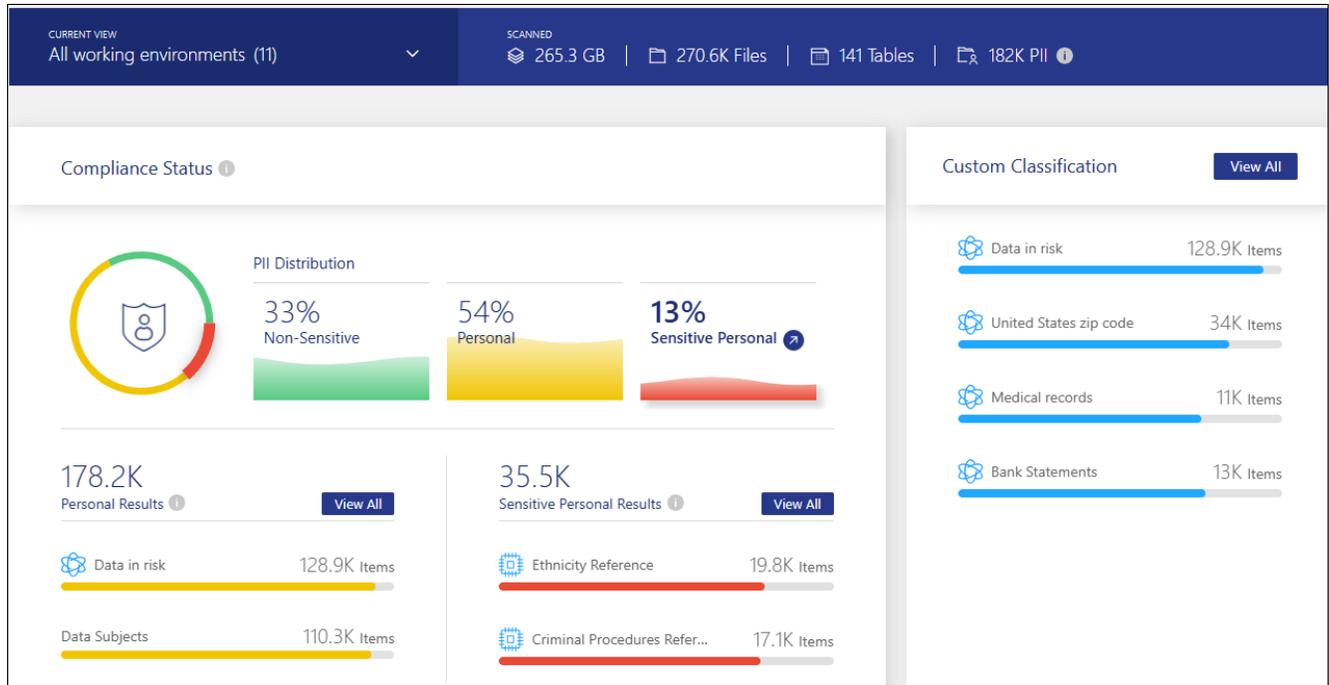
Par exemple, une catégorie de données sensibles du RGPD est l'origine ethnique. Du fait de ses capacités NLP, le classement BlueXP peut faire la différence entre la phrase « George est mexicain » (indiquant des données sensibles comme spécifié dans l'article 9 du RGPD) et « George mange mexicain ».



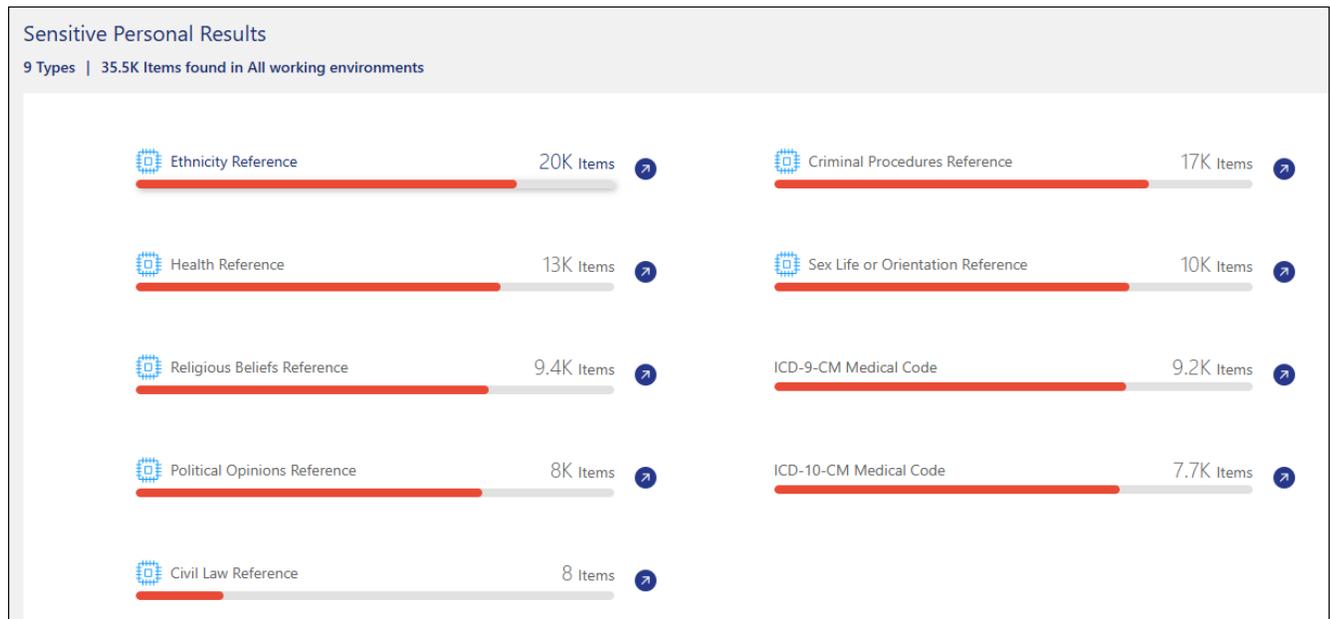
Seul l'anglais est pris en charge lors de la recherche de données personnelles sensibles. La prise en charge d'autres langues sera ajoutée ultérieurement.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **conformité**.
2. Pour examiner les détails de toutes les données personnelles sensibles, sélectionnez l'icône en regard du pourcentage de données personnelles sensibles.



3. Pour examiner les détails d'un type spécifique de données personnelles sensibles, sélectionnez **Afficher tout**, puis sélectionnez la flèche **examiner les résultats** pour un type spécifique de données personnelles sensibles.



- 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](#)".

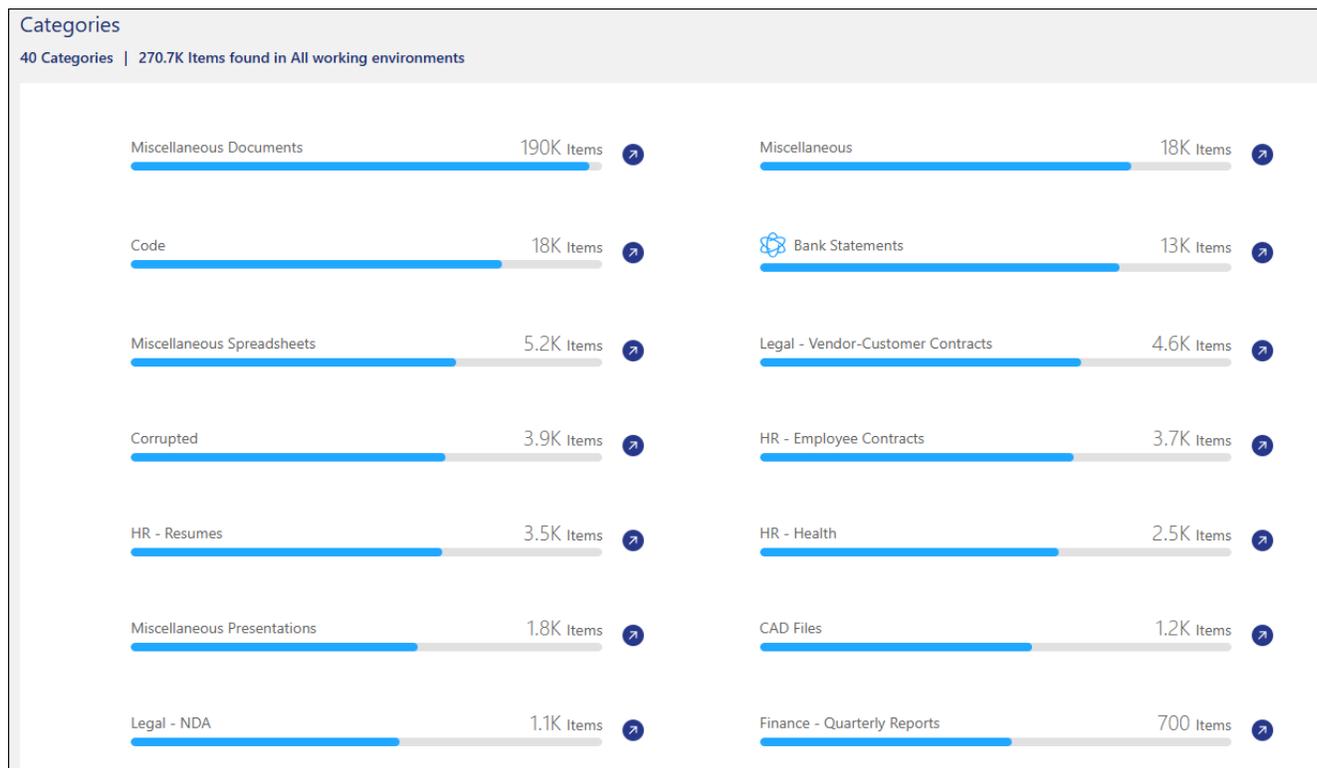
Les catégories peuvent vous aider à comprendre ce qui se passe avec vos données en vous montrant les types d'informations dont vous disposez. Par exemple, une catégorie comme les CV ou les contrats d'employés peut inclure des données sensibles. Lorsque vous examinez les résultats, vous pouvez constater 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

- Dans le menu BlueXP Classification, sélectionnez l'onglet **conformité**.
- Sélectionnez la flèche **examiner les résultats** pour l'une des 4 catégories principales directement à partir de l'écran principal, ou sélectionnez **Afficher tout**, puis sélectionnez l'icône de l'une des catégories.



- Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en sélectionnant la flèche **examiner les résultats** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.

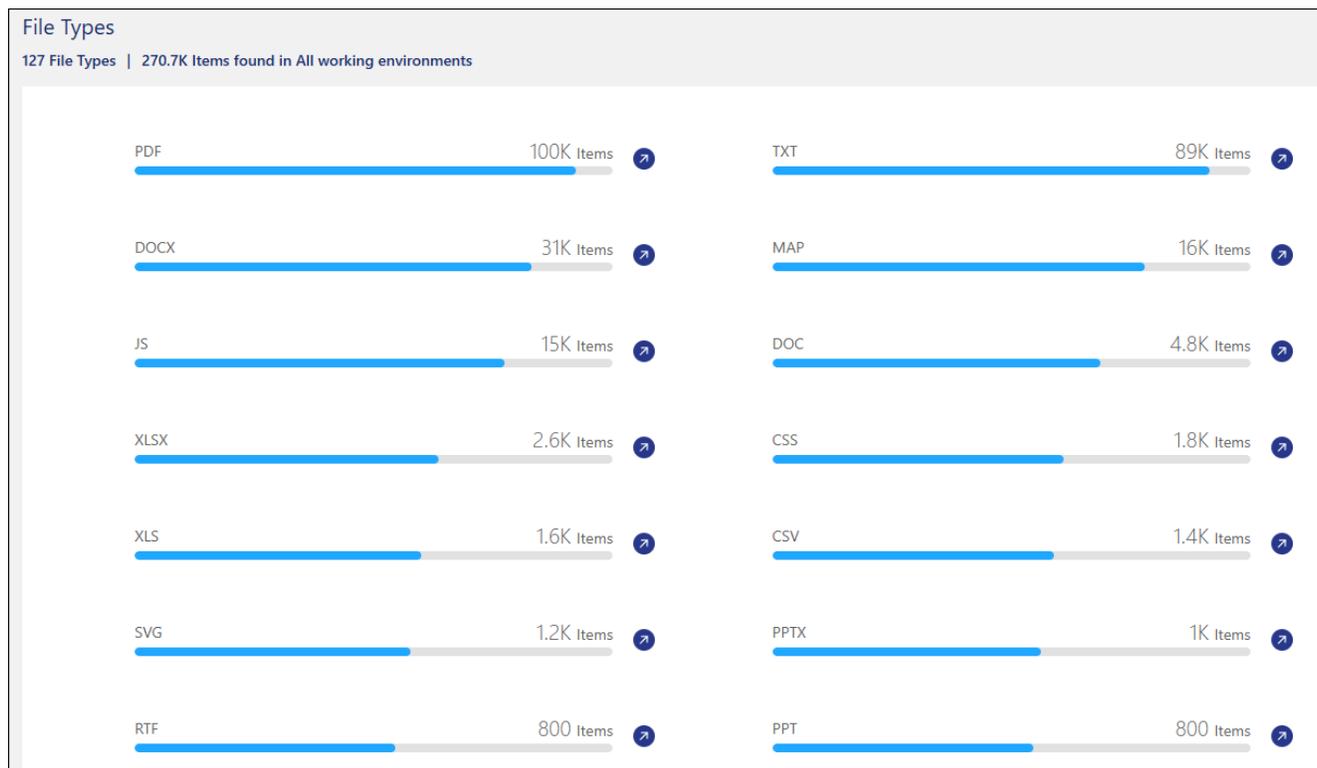
Afficher les fichiers par type de fichier

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

- Dans le mémoire de classification BlueXP, sélectionnez l'onglet **conformité**.
- Sélectionnez la flèche **examiner les résultats** pour l'un des 4 principaux types de fichiers directement à partir de l'écran principal, ou sélectionnez **Afficher tout**, puis sélectionnez 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 sélectionnant la flèche **examiner les résultats** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.

Catégories de données privées classées par BlueXP

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 soins de santé, contactez votre gestionnaire de compte.

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	Oui.	✓	✓	✓		✓
	Sujets de données	Non	✓	✓	✓		
	Adresse électronique	Non	✓	✓	✓		✓
	Numéro IBAN (numéro de compte bancaire international)	Non	✓	✓	✓		✓
	Adresse IP	Non	✓	✓	✓		✓
	Mot de passe	Oui.	✓	✓	✓		✓

Type	Identificateur	Validatio n de proximit é ?	Anglai s	Allema nd	Espag nol	França is	Japon ais
Identifiants nationaux							
16							

Type	Identificateur	Validation de proximité ?	Anglais	Allemand	Espagnol	Français	Japonais
------	----------------	---------------------------	---------	----------	----------	----------	----------

Type	Identificateur	Validation de proximité ?	Anglais	Allemand	Espagnol	Français	Japonais
------	----------------	---------------------------	---------	----------	----------	----------	----------

Type	Identifiant maltais	Oui.	✓	✓	✓		
	Numéro du Service national de santé (NHS) Identificateur	Oui. Validation de proximité ?	✓	✓	✓	Français	Japonais
	Compte bancaire de la Nouvelle-Zélande	Oui.	✓	✓	✓		
	Permis de conduire de la Nouvelle-Zélande	Oui.	✓	✓	✓		
	Numéro IRD de Nouvelle-Zélande (ID taxe)	Oui.	✓	✓	✓		
	Numéro NHI (National Health Index) de la Nouvelle-Zélande	Oui.	✓	✓	✓		
	Numéro de passeport de la Nouvelle-Zélande	Oui.	✓	✓	✓		
	ID polonais (PESEL)	Oui.	✓	✓	✓		
	Numéro d'identification fiscale portugais (FNI)	Oui.	✓	✓	✓		
	ID roumain (CNP)	Oui.	✓	✓	✓		
	Carte d'identité nationale d'enregistrement de Singapour (NRIC)	Oui.	✓	✓	✓		
	ID slovène (EMSO)	Oui.	✓	✓	✓		
	Carte d'identité sud-africaine	Oui.	✓	✓	✓		
	Numéro d'identification fiscale espagnol	Oui.	✓	✓	✓		
	Carte d'identité suédoise	Oui.	✓	✓	✓		
	ID ROYAUME-UNI (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.	✓	✓	✓		
	USA Texas permis de conduire	Oui.	✓	✓	✓		
	Numéro de sécurité sociale des États-Unis (SSN)	Oui.	✓	✓	✓		

Types de données personnelles sensibles

La classification BlueXP peut trouver les renseignements personnels sensibles suivants (SPII) dans les 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	✓	✓	

Catégorie	Type	Anglais	Allemand	Espagnol
Administratifs	RFI	✓		✓
	RFP	✓		✓
	CAHIER DES CHARGES	✓	✓	✓
	Formation	✓	✓	✓
Assistance	Plaintes et tickets	✓	✓	✓

Les métadonnées suivantes sont également catégorisées 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. Lorsque

la classification BlueXP détecte des informations personnelles identifiables (PII) ou lorsqu'elle effectue une recherche DSAR, seuls les formats de fichiers suivants sont pris en charge :

.CSV, .DCM, .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 %

Créer une classification personnalisée dans la classification BlueXP

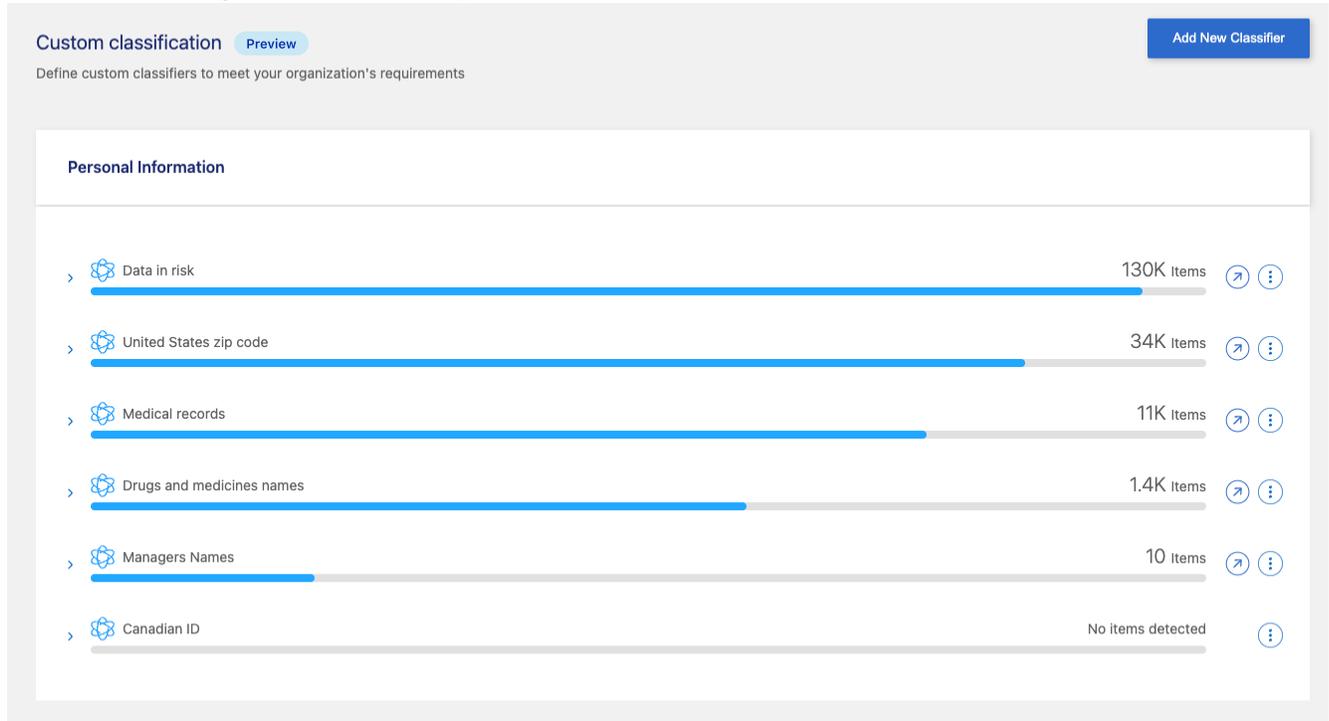
Avec la classification BlueXP , vous pouvez créer une recherche personnalisée pour les informations sensibles. La recherche peut être étendue à une expression régulière (regex).

Créer une classification personnalisée

La classification personnalisée n'est disponible que pour les acquisitions Map & Classify, et non pour les acquisitions de mappage uniquement. Cette fonction est actuellement en aperçu.

Étapes

1. Sélectionnez l'onglet **Classification personnalisée**.



Custom classification Preview Add New Classifier

Define custom classifiers to meet your organization's requirements

Personal Information

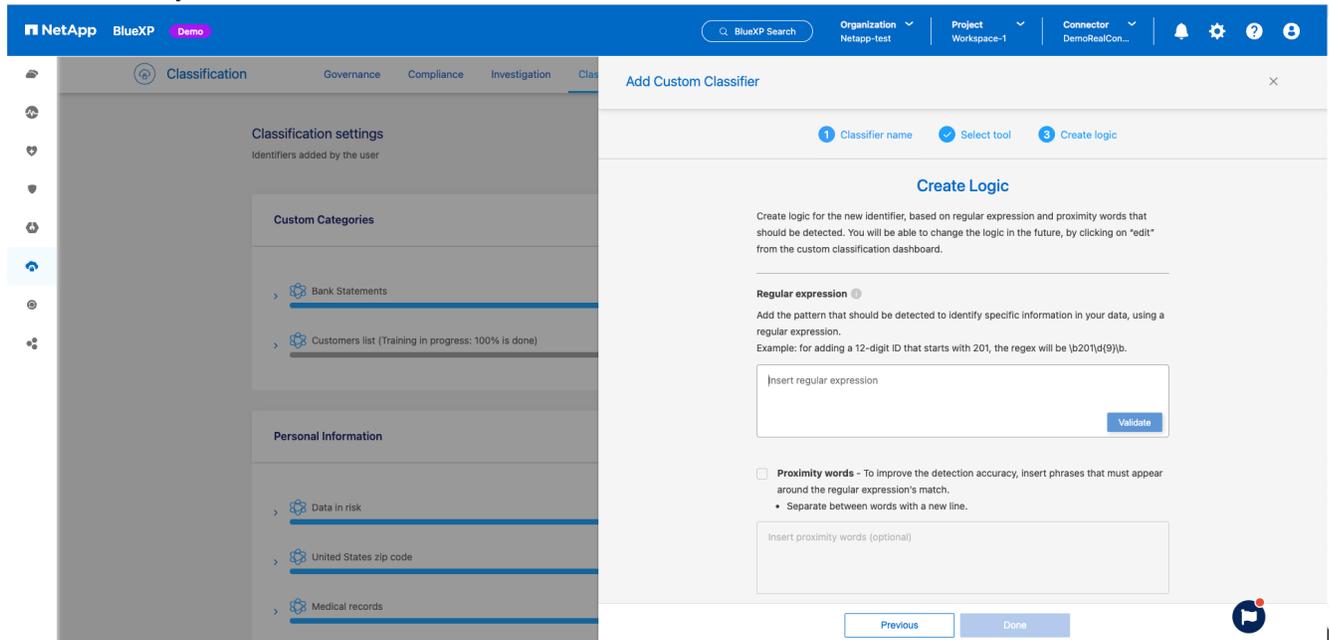
Category	Items
Data in risk	130K Items
United States zip code	34K Items
Medical records	11K Items
Drugs and medicines names	1.4K Items
Managers Names	10 Items
Canadian ID	No items detected

2. Sélectionner le bouton **Ajouter un nouveau classificateur**.

3. Ajoutez un nom et une description pour le nouveau classificateur.

4. Pour ajouter la personnalisation en tant qu'expression régulière, sélectionnez **expression régulière personnalisée** puis **Suivant**.

5. Ajoutez un schéma pour détecter les informations spécifiques de vos données. Sélectionnez **Valider** pour confirmer la syntaxe de votre entrée.



NetApp BlueXP Demo

Classification settings

Identifiers added by the user

Custom Categories

- Bank Statements
- Customers list (Training in progress: 100% is done)

Personal Information

- Data in risk
- United States zip code
- Medical records

Add Custom Classifier

1 Classifier name 2 Select tool 3 Create logic

Create Logic

Create logic for the new identifier, based on regular expression and proximity words that should be detected. You will be able to change the logic in the future, by clicking on "edit" from the custom classification dashboard.

Regular expression

Add the pattern that should be detected to identify specific information in your data, using a regular expression.
Example: for adding a 12-digit ID that starts with 201, the regex will be `{b201}d{9}b`.

Insert regular expression Validate

Proximity words - To improve the detection accuracy, insert phrases that must appear around the regular expression's match.

- Separate between words with a new line.

Insert proximity words (optional)

Previous Done

6. Sélectionnez **terminé** pour créer la classification personnalisée.

La nouvelle personnalisation est capturée lors de la prochaine analyse programmée. Pour afficher les résultats, voir [Générer des rapports de conformité](#).

Analysez les données stockées dans votre entreprise avec la classification BlueXP

Examinez les données de votre organisation en consultant les détails sur la page Enquête sur les données. Voici où vous pouvez poursuivre vos recherches après avoir regardé le tableau de bord gouvernance. Sur la page Investigation, vous pouvez filtrer les données à l'aide de l'un des nombreux filtres pour afficher uniquement les résultats que vous souhaitez voir. Vous pouvez également afficher les métadonnées des fichiers et les autorisations associées aux fichiers et aux répertoires, et rechercher les fichiers dupliqués dans vos systèmes de stockage.

Vous pouvez naviguer jusqu'à cette page à partir de plusieurs zones de l'interface utilisateur de classification BlueXP, y compris les tableaux de bord gouvernance et conformité avec les filtres déjà sélectionnés sur ces pages. Vous pouvez exporter les données dans un fichier CSV ou JSON pour une analyse plus approfondie ou pour les partager avec d'autres.



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.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **Investigation**.
2. Sur la page enquête sur les données, effectuez l'une des opérations suivantes :
3. Pour télécharger le contenu de la page sous forme de rapport après l'avoir affiné, sélectionnez le  bouton.

The screenshot shows the 'Data Investigation' tool interface. At the top, there are tabs for 'Unstructured (270.6K Files)', 'Directories (22K Folders)', and 'Structured (141 Tables)'. A search bar is on the right. On the left, there is a 'FILTERS' panel with options like 'Policies', 'Classification Status', 'Scan Analysis Event', 'Open Permissions', 'Number of Users with Access', 'User / Group Permissions', and 'File Owner'. The main area displays a table of 270.6K items. The table has columns for 'File Name', 'Personal', 'Sensitive Personal', 'Data Subjects', and 'File Type'. The first few rows are:

File Name	Personal	Sensitive Personal	Data Subjects	File Type
BB1A/rkD.txt	1.2K	0	10	TXT
some_live_some_dead.txt	1.1K	0	161	TXT
#opisrael_credit_card_leak.txt	1K	0	8	TXT
aaaa_Unstructured_Report_2025-01-09_12-0...	1K	0	0	CSV
ground_truth.csv	916	0	916	CSV
Customers.xls	911	0	248	XLS
ground_truth.csv	910	0	910	CSV
true positive - 500 - Copy - Copy (2).txt	738	56	496	TXT
true positive - 500 - Copy (7).txt	738	56	496	TXT
true positive - 500 - Copy (9).txt	738	56	496	TXT

At the bottom right, it says 'Total size 265.2GB | 1-20 of 270.6K'.

4. Pour afficher les données issues de fichiers (données non structurées), de répertoires (dossiers et partages de fichiers) ou de bases de données (données structurées), sélectionnez l'un des onglets situés en haut de l'écran.
5. Pour trier les résultats par ordre numérique ou alphabétique, sélectionnez le contrôle en haut de chaque colonne.
6. Pour affiner encore plus les résultats, sélectionnez l'un des filtres dans le volet Filtre.



Vous ne pouvez afficher que les 10,000 premiers résultats (ou les 500 premières pages) d'une analyse sur la page investigation de données.

Filtrer les données par sensibilité et contenu

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

Filtre	Détails
Catégorie	Sélectionnez le " 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	Sélectionnez le " types de données personnelles ".
Données personnelles sensibles	Sélectionnez le " types de données personnelles sensibles ".

Filtre	Détails
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" .

Filterer les données par propriétaire d'utilisateur et autorisations d'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.

Filterer 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-prest (SharePoint Server), OneDrive, Google Drive et Amazon S3.

Filterer les 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	Sélectionnez le "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.

Filter 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.

Filter les données par recherches enregistrées

Utilisez le filtre suivant pour afficher les données des recherches enregistrées.

Filtre	Détails
Recherche enregistrée	Sélectionnez une ou plusieurs recherches enregistrées. Accédez au "onglet recherches enregistrées" pour afficher la liste des recherches enregistrées existantes et en créer de nouvelles.

Filter 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.

Filtre	Détails
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

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 les "[créer des recherches enregistrées](#)" utiliser car vous pouvez afficher toutes les informations que vous pouvez utiliser pour filtrer vos données.

La disponibilité des informations dépend de la source de données. Par exemple, le nom du volume et les autorisations ne sont pas partagés pour les fichiers de base de données.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **Investigation**.
2. Dans la liste enquête sur les données à droite, sélectionnez la touche de bas ▼ à droite pour afficher les métadonnées du fichier.

The screenshot shows a file management interface with a list of files and a detailed view for a selected file. The file list includes columns for File Name, Personal, Sensitive Personal, Data Subjects, and File Type. The selected file is 'GM_PD 12-1-09 SP.xls.pdf'. The detailed view shows various metadata and actions for the file.

File Name	Personal	Sensitive Personal	Data Subjects	File Type
ground truth.xlsx	ONDRV	1K	0	XLSX
GM_PD 12-1-09 SP.xls.pdf	ONDRV	930	0	PDF

File Details:

- Tags: Decathlon, gidi, IS NOT OK, And 6 more, [View All](#)
- Working Environment: OneDrive daylabs.onmicrosoft.com
- Storage Repository (User): ruh@daylabs.onmicrosoft.com
- File Path: /scattered/26/GM_PD 12-1-09 SP.xls.pdf
- Category: Miscellaneous Documents
- File Size: 427.46 KB
- Discovered Time: 2021-01-12 10:37
- Created Time: 2018-05-22 12:38 | Last Modified: 2018-10-22 13:28
- Duplicates: None

Actions: Tags: 9 tags, Assigned to: Amit Ashbel, Assign a Label to this file, Copy File, Move File, Delete File.

Afficher les autorisations des utilisateurs pour les fichiers et les répertoires

Pour afficher la liste de tous les utilisateurs ou groupes ayant accès à un fichier ou à un répertoire et les types d'autorisations dont ils disposent, sélectionnez **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](#)".

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **Investigation**.
2. Dans la liste enquête sur les données à droite, sélectionnez la touche de bas ▼ à droite pour afficher les métadonnées du fichier.
3. Pour afficher la liste de tous les utilisateurs ou groupes ayant accès à un fichier ou à un répertoire et les types d'autorisations dont ils disposent, dans le champ autorisations ouvertes, sélectionnez **Afficher toutes les autorisations**.



La classification BlueXP affiche jusqu'à 100 utilisateurs dans la liste.

The screenshot shows a file management interface. The top navigation bar includes 'File Name', 'Personal', 'Sensitive Personal', 'Data Subjects', and 'File Type'. The file 'Expense Report TPO-1060.pdf' is selected, with details such as 'Working Environment: WorkingEnvironment1', 'Repository: Volume Name', 'File Path: /Prod/labs-base/Expense Report TPO-1060.pdf', 'Category: Legal', 'File Size: 22 MB', 'Last Modified: 2019-08-06 07:51', 'Open Permissions: NO OPEN PERMISSIONS', and 'File Owner: Avy'. A 'View all Permissions' button is highlighted with a red box. An inset window titled 'Permissions list for "Expense Report TPO-1060.pdf"' shows a table of users and groups with their respective Read and Write permissions. The 'Write' column for the second 'Group Name' entry is highlighted with a red box.

User / Group	Name	Read	Write
👤	User Name	✓	✓
👥	Group Name	✓	⌵
👥	Group Name	✓	✓ ⬆
👤	John L	✓	✓
👤	George H	✓	✓
👤	Paul M	✓	✓
👤	Ringo S	✓	✓

- Sélectionnez le bouton de la touche de direction vers le bas ⌵ de n'importe quel groupe pour afficher la liste des utilisateurs qui font partie du groupe.



Vous pouvez développer un niveau du groupe pour voir les utilisateurs qui font partie du groupe.

- Sélectionnez le nom d'un utilisateur ou d'un groupe pour actualiser la page Investigation afin de 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 vérifier si des fichiers en double sont stockés sur vos systèmes de stockage. Cette fonction s'avère utile pour identifier les domaines dans lesquels vous pouvez économiser de l'espace de stockage. Il est également judicieux de vous assurer que certains fichiers disposant d'autorisations spécifiques ou d'informations sensibles ne sont pas dupliqués inutilement sur vos systèmes de stockage.

Tous vos fichiers (à l'exception des bases de données) de 1 Mo ou plus, ou contenant des informations personnelles ou sensibles, sont comparés pour voir s'il y a des doublons.

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

Étapes

- Dans le menu BlueXP Classification, sélectionnez **Investigation**.
- Dans le volet filtres de la page Investigation, à gauche, sélectionnez « taille du fichier » avec « doublons » (« a des doublons ») pour voir quels fichiers d'une certaine plage de tailles sont dupliqués dans votre environnement.
- Si vous le souhaitez, téléchargez la liste des fichiers dupliqués et envoyez-la à votre administrateur du stockage pour qu'il puisse décider quels fichiers, le cas échéant, peuvent être supprimés.

4. Si vous le souhaitez, "supprimez le fichier" vous-même êtes sûr qu'une version spécifique du fichier n'est pas nécessaire.

Afficher si un fichier spécifique est dupliqué

Vous pouvez voir si un seul fichier contient des doublons.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **Investigation**.
2. Dans la liste enquête sur les données, sélectionnez ▼ à droite un fichier pour afficher les métadonnées de fichier.

Si des doublons existent pour un fichier, ces informations apparaissent en regard du champ *Duplicates*.

3. Pour afficher la liste des fichiers en double et leur emplacement, sélectionnez **Afficher les détails**.
4. Sur la page suivante, sélectionnez **Afficher les doublons** pour afficher les fichiers dans la page Investigation.

The screenshot shows the BlueXP interface. At the top, file metadata is displayed: Last Modified: 2019-08-06 07:51, Open Permissions: NO OPEN PERMISSIONS, File Owner: Asaf Ley, and Duplicates: 3. A 'View Details' button is highlighted with a red box. Below this, a modal window titled 'Duplicates of File 'Name 1'' is open, showing 'Duplicates: 3', 'Total Size of all Duplicates: 1GB', and 'File Hash: xxxxxx'. A 'View Duplicates' button is highlighted with a red box. Below the modal, a table titled '3 Items' displays the following data:

<input type="checkbox"/>	File Name	Personal	Sensitive Personal	Data Subjects	File Type
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654 - cvo	6	3	16	PDF
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654 - cvo	6	3	16	PDF
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654 - cvo	6	3	16	PDF



Vous pouvez utiliser la valeur « 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 recherche enregistrée.

Créer le rapport d'enquête sur les 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 forme de fichier CSV ou JSON que vous pouvez enregistrer sur votre ordinateur local.

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).

Les fichiers sont divisés en fichiers avec un nombre fixe de lignes ou d'enregistrements :

- JSON - 100 000 enregistrements par rapport dont la génération prend environ 5 minutes
- CSV - 200 000 enregistrements par rapport dont la génération prend environ 4 minutes



Vous pouvez télécharger une version du fichier CSV à afficher dans ce navigateur. Cette version est limitée à 10,000 enregistrements.

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
 - Les données du propriétaire du fichier englobent le nom du compte, le nom du compte SAM et l'adresse e-mail lorsque Active Directory est configuré.
- Catégorie
- Informations personnelles
- Informations personnelles sensibles
- Ouvrez les autorisations
- Erreur d'analyse d'acquisition
- Date de détection de suppression

La 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 sont pas comptabilisés dans le nombre de fichiers affichés dans le tableau de bord ni 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

Étapes de génération du rapport

1. Dans la page enquête sur les données, sélectionnez le  bouton en haut, à droite de la page.
2. Choisissez le type de rapport : CSV ou JSON.
3. Entrez un **Nom du rapport**.
4. Pour télécharger le rapport complet, sélectionnez **Environnement de travail** puis choisissez **Environnement de travail** et **Volume** dans les menus déroulants respectifs. Indiquez un chemin d'accès **au dossier de destination**.

Pour télécharger le rapport dans le navigateur, sélectionnez **local** . Remarque cette option limite le rapport aux 10,000 premières lignes et est limitée au format **CSV**. Vous n'avez pas besoin de remplir d'autres champs si vous sélectionnez **local**.

5. Sélectionnez **Télécharger le rapport**.

Download Investigation Report

Report type

CSV file JSON file

Report name

investigation_report

Export destination

Working environment Local (limited to 10K rows)

Working environment i

Working environment ▼

Volume

Type to search... ▼

Destination folder path

/folder/subfolder

Download Report

Cancel

Résultat

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

Créer une recherche enregistrée en fonction des filtres sélectionnés

Vous pouvez créer une recherche enregistrée pour les filtres de recherche fréquemment utilisés dans la page investigation de données pour répliquer facilement ces requêtes de recherche.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **Investigation**.
2. Sur la page investigation de données, sélectionnez les filtres que vous souhaitez utiliser pour créer une recherche enregistrée.
3. En bas du volet filtre, sélectionnez **Créer une recherche enregistrée dans cette recherche**.
4. Entrez un nom et une description pour la recherche enregistrée.
5. Choisissez l'une des options suivantes :
6. Sélectionnez **Créer une recherche enregistrée**.



L'affichage des résultats sur la page recherches enregistrées peut prendre jusqu'à 15 minutes.

Gestion des recherches enregistrées avec la classification BlueXP

La classification BlueXP prend en charge l'enregistrement de vos requêtes de recherche. Avec une recherche enregistrée, vous pouvez créer des filtres personnalisés pour trier les requêtes fréquentes de votre page d'investigation de données. La classification BlueXP inclut également des recherches enregistrées prédéfinies basées sur des demandes courantes.



Dans les versions de la classification BlueXP antérieures à 1.43, les recherches enregistrées étaient appelées **stratégies**.

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

Les recherches enregistrées apparaissent également dans la liste des filtres de la page Investigation.

Classification Governance Compliance Investigation Custom classification **Saved searches** Configuration

Email Addresses – High risk
Default search
Edit search

Files with over 50 Email Addresses, or DB Columns with over 50% of their rows containing Email Addresses.

Financial data
Last modified: 2024-03-04
Edit search

Look for financial data

Afficher les résultats des recherches enregistrées dans la page Investigation

Pour afficher les résultats d'une recherche enregistrée dans la page Investigation, sélectionnez le bouton correspondant à une recherche spécifique,  puis sélectionnez **examiner les résultats**.

Last Access Date Order than 30 days
Last modified: 2025-03-18
Edit search

Last Access Date Order than 30 days

- Investigate results
- Delete search

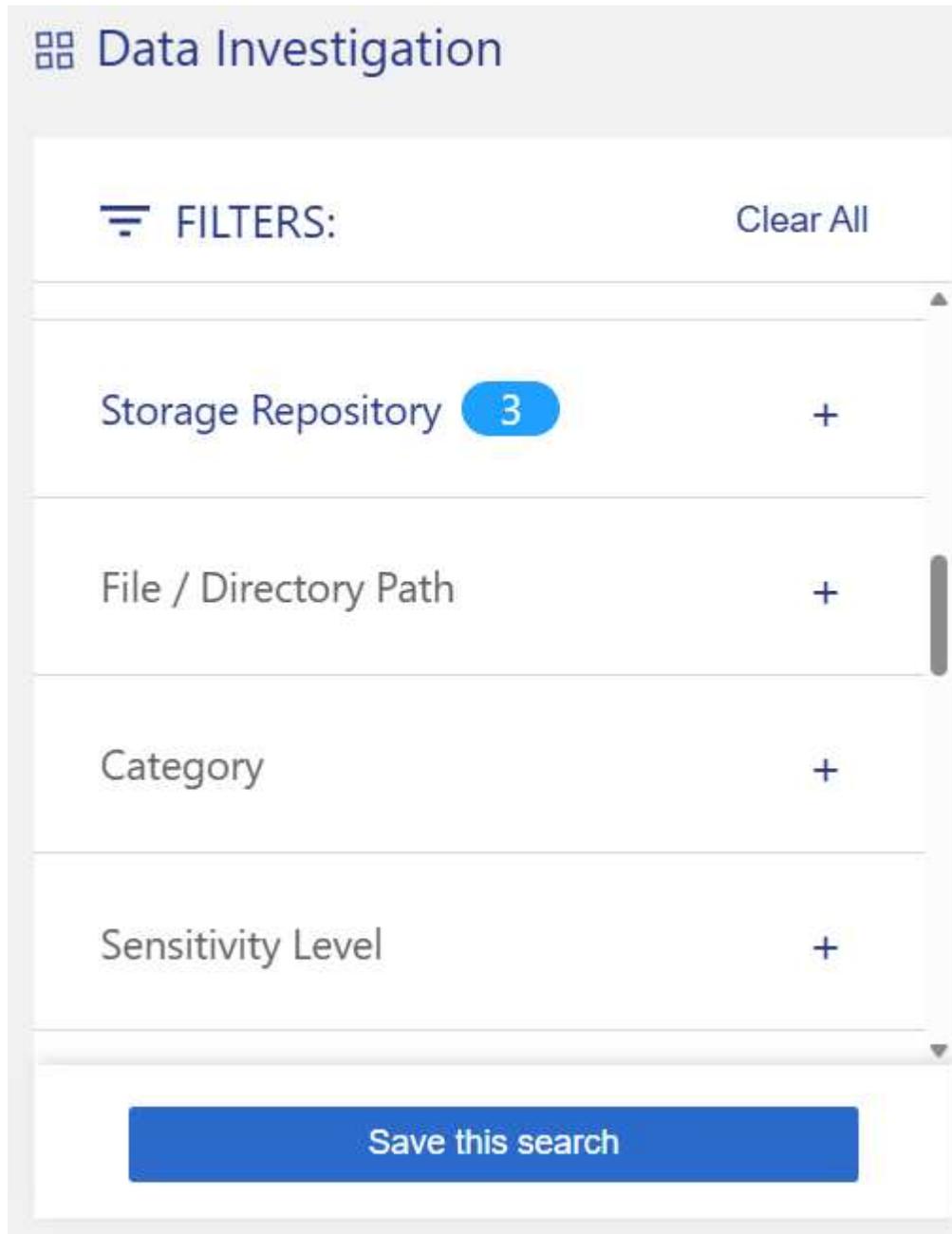
Créer des recherches enregistrées personnalisées

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

requêtes 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 l'onglet Investigation, définissez une recherche en sélectionnant les filtres à utiliser. Voir "[Filtrage des données dans la page Investigation](#)" pour plus de détails.
2. Une fois que vous avez défini toutes les caractéristiques de filtre à votre convenance, sélectionnez **Créer une recherche enregistrée**.



3. Nommez la recherche enregistrée et ajoutez une description. Le nom doit être unique.
4. Sélectionnez **Créer une recherche enregistrée**.

Create search

This will save the current selected filters and search term as a saved search. You can view or delete this later from the "Saved searches" tab.

Note it may take up to 15 minutes for results to be displayed for a new saved search.

Name this search

Give it a detailed description that explains what it searches for

Create search

Cancel

Une fois la recherche créée, vous pouvez l'afficher dans l'onglet **recherches enregistrées**.

Modifier les recherches enregistrées

Vous pouvez modifier les critères de requête d'une recherche enregistrée (c'est-à-dire les filtres définis) pour ajouter ou supprimer certains paramètres.

Vous ne pouvez pas modifier les recherches enregistrées par défaut.

Étapes

1. Sur la page des recherches enregistrées, sélectionnez **Modifier la recherche** pour la recherche que vous souhaitez modifier.

Sensitive data

Last modified: 2024-03-04

Edit search



Look for sensitive data from 2 years ago

2. Apportez les modifications aux champs Nom et Description. Pour modifier uniquement les champs de nom et de description, sélectionnez **Enregistrer la recherche**.

Pour modifier les filtres de la recherche enregistrée, sélectionnez **Modifier la requête**.

Name this search

Edit query

Name this search

Give it a detailed description that explains what it searches for

Save search Cancel

3. Dans la page Investigation, modifiez la requête. Vous pouvez ajouter, supprimer ou modifier des filtres. Pour terminer vos modifications, sélectionnez **Enregistrer la requête pour cette recherche**.

The screenshot shows the 'Data Investigation' interface. At the top, there are tabs for 'Unstructured (217.3K Files)', 'Directories (0 Folders)', and 'Structured (0 Tables)'. A search bar is visible on the right. On the left, a 'FILTERS:' panel is open, showing 'Last Modified' with a count of 3, 'Last Accessed', 'Duplicates', and 'File Hash'. Below the filters, there are two buttons: 'Save query for search' and 'Cancel edit query'. The main area displays a table with 217.3K items. The table has columns for 'File Name', 'Personal', 'Sensitive Personal', 'Data Subjects', and 'File Type'. The first row is highlighted in blue. The table contains several rows of 'true positive.txt' files with various tags like 'cvo' and 's3'.

File Name	Personal	Sensitive Personal	Data Subjects	File Type	
customers.txt	22	307	0	TXT	
true positive.txt	cvo	107	618	107	TXT
true positive.txt	s3	107	618	107	TXT
true positive.txt	cvo	107	618	107	TXT
true positive.txt	s3	107	618	107	TXT
true positive.txt	s3	107	618	107	TXT
true positive.txt	s3	107	618	107	TXT
true positive.txt	cvo	107	618	107	TXT

Total size 228.6GB | 1-20 of 1

Supprimer les recherches enregistrées

Vous pouvez supprimer toute recherche enregistrée personnalisée si vous n'en avez plus besoin. Vous ne pouvez pas supprimer les recherches enregistrées par défaut.

Pour supprimer une recherche enregistrée, sélectionnez le  bouton correspondant à une recherche spécifique, sélectionnez **Supprimer la recherche**, puis sélectionnez de nouveau **Supprimer la recherche** dans la boîte de dialogue de confirmation.

Recherches par défaut

La classification BlueXP fournit les requêtes de recherche définies par le système suivantes :

- **Noms des sujets de données - risque élevé**

Fichiers avec plus de 50 noms de sujet de données

- **Adresses de courriel - risque élevé**

Fichiers contenant plus de 50 adresses e-mail ou colonnes de base de données contenant plus de 50 % de leurs lignes contenant des adresses e-mail

- **Données personnelles - risque élevé**

Fichiers contenant plus de 20 identificateurs de données personnelles ou colonnes de base de données contenant plus de 50 % de leurs lignes contenant des identificateurs de données personnelles

- **Données privées - périmées sur 7 ans**

Les fichiers contenant des renseignements personnels ou sensibles, modifiés il y a plus de 7 ans

- **Protéger - élevé**

Fichiers ou colonnes de base de données contenant un mot de passe, des informations de carte de crédit, un numéro IBAN ou un numéro de sécurité sociale

- **Protéger - faible**

Fichiers qui n'ont pas été utilisés depuis plus de 3 ans

- **Protéger - Moyen**

Fichiers contenant des fichiers ou des colonnes de base de données avec des identificateurs de données personnels, notamment des numéros d'identification, des numéros d'identification fiscale, des numéros de permis de conduire, des ID médicaux ou des numéros de passeport

- **Données personnelles sensibles - risque élevé**

Fichiers contenant plus de 20 identificateurs de données personnelles sensibles ou colonnes de base de données contenant plus de 50 % de leurs lignes contenant des données personnelles sensibles

Modifiez les paramètres d'analyse de classification BlueXP pour vos référentiels

Vous pouvez gérer le mode d'analyse de vos données dans chacun de vos environnements de travail et sources de données. Vous pouvez effectuer les modifications sur une base de « référentiel », ce qui signifie que vous pouvez apporter des modifications à chaque volume, schéma, utilisateur, etc. En fonction du type de source de données que vous analysez.

Certaines choses que vous pouvez modifier sont si un référentiel est scanné ou non, et si la classification BlueXP exécute un "[acquisition de mappage ou cartographie etamp ; acquisition de classification](#)". Vous pouvez également interrompre et reprendre la numérisation, par exemple si vous devez arrêter la numérisation d'un volume pendant un certain temps.

Afficher l'état d'analyse de vos référentiels

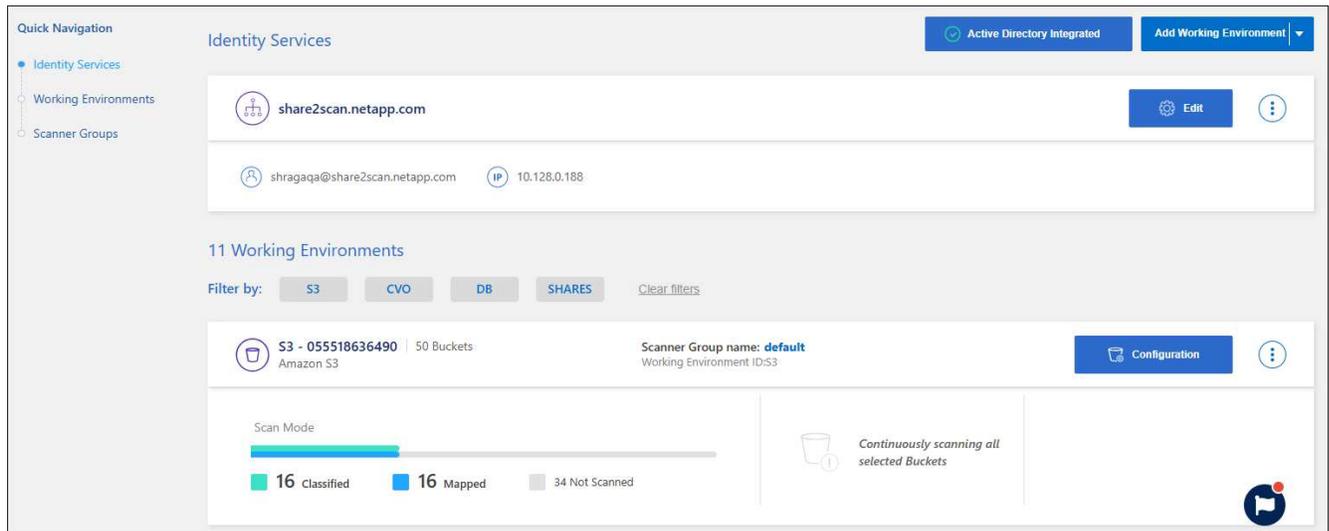
Vous pouvez afficher les référentiels individuels que la classification BlueXP analyse (volumes, compartiments, etc.) pour chaque environnement de travail et source de données. De plus, vous pouvez voir combien ont été « mappés » et combien ont été « classés ». Le classement est plus rapide lorsque l'identification complète de l'IA est effectuée sur toutes les données.

Vous pouvez afficher l'état de numérisation de chaque environnement de travail sur la page Configuration :

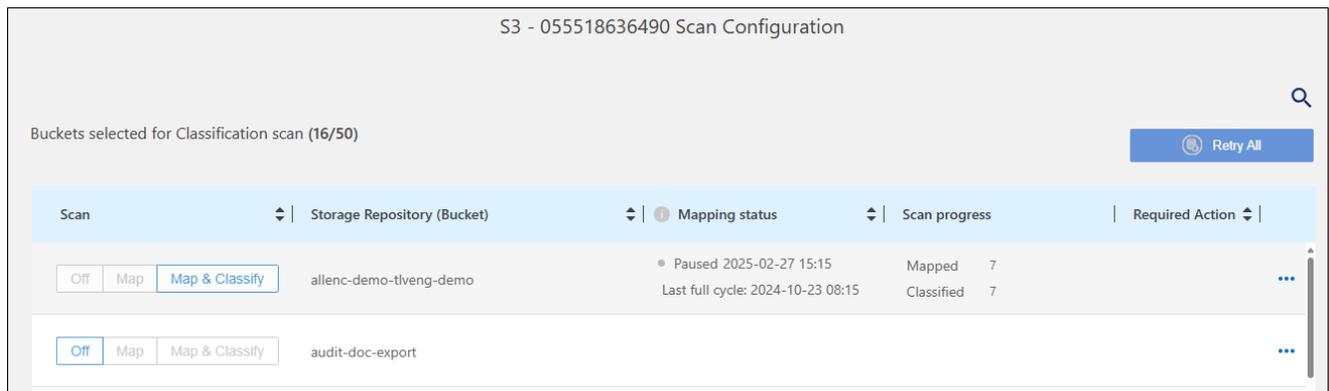
- **Initialisation** (point bleu clair) : la configuration de la carte ou de la classification est activée. Ceci s'affiche pendant quelques secondes avant le démarrage de l'état de la "file d'attente".
- **File d'attente en attente** (point orange) : la tâche de numérisation est en attente d'être répertoriée dans la file d'attente de numérisation.
- **Queued** (point orange) : la tâche a été ajoutée avec succès à la file d'attente de numérisation. Le système démarre le mappage ou la classification du volume à l'arrivée de son tour dans la file d'attente.
- **En cours d'exécution** (point vert) : la tâche de numérisation, qui se trouvait dans la file d'attente, est en cours d'exécution sur le référentiel de stockage sélectionné.
- **Terminé** (point vert) : l'analyse du référentiel de stockage est terminée.
- **Pause** (point gris) : vous avez sélectionné l'option "Pause" pour interrompre la numérisation. Bien que les modifications du volume ne soient pas affichées dans le système, les informations scannées restent affichées.
- **Erreur** (point rouge) : l'analyse ne peut pas se terminer car elle a rencontré des problèmes. Si vous devez effectuer une action, l'erreur s'affiche dans l'info-bulle sous la colonne « action requise ». Dans le cas contraire, le système affiche un état « erreur » et tente de récupérer. Une fois terminé, l'état change.
- **Pas de balayage** : la configuration du volume de "off" a été sélectionnée et le système n'analyse pas le volume.

Étapes

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



2. Dans l'onglet Configuration, sélectionnez le bouton **Configuration** de l'environnement de travail.
3. Dans la page Configuration de la numérisation, affichez les paramètres de numérisation de tous les référentiels.



4. Placez le curseur sur le graphique dans la colonne *Mapping Status* pour voir le nombre de fichiers qui restent à mapper ou à classer dans chaque référentiel (compartiment dans cet exemple).

Modifier le type de numérisation d'un référentiel

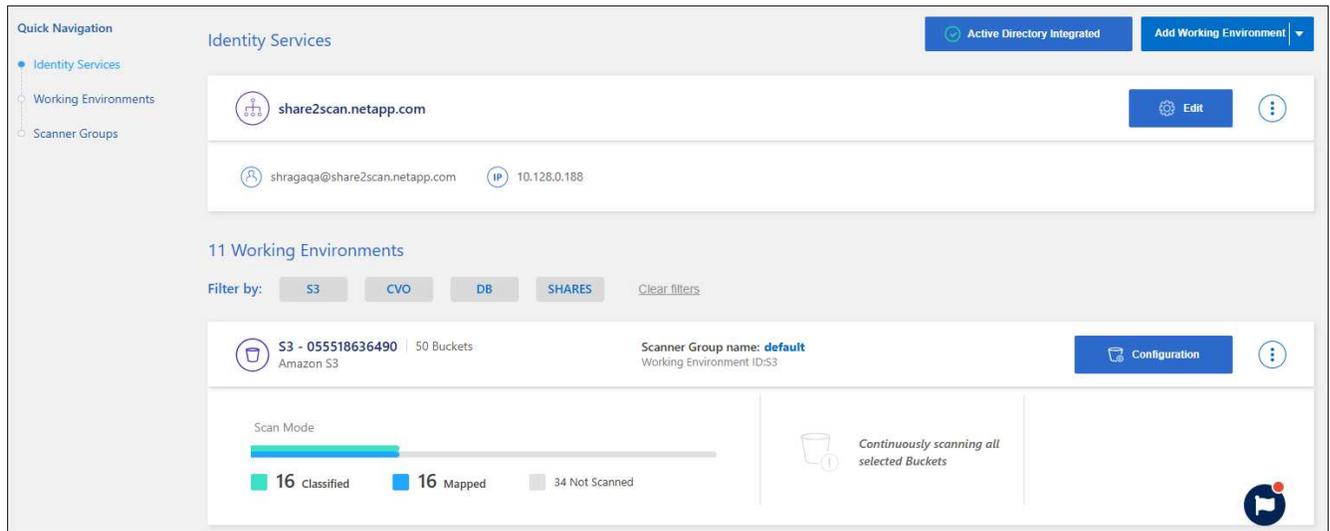
Vous pouvez démarrer ou arrêter des analyses de mappage uniquement, ou des analyses de mappage et de classification, dans un environnement de travail à tout moment à partir de la page Configuration. Vous pouvez également passer des acquisitions avec mappage uniquement à des acquisitions avec mappage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



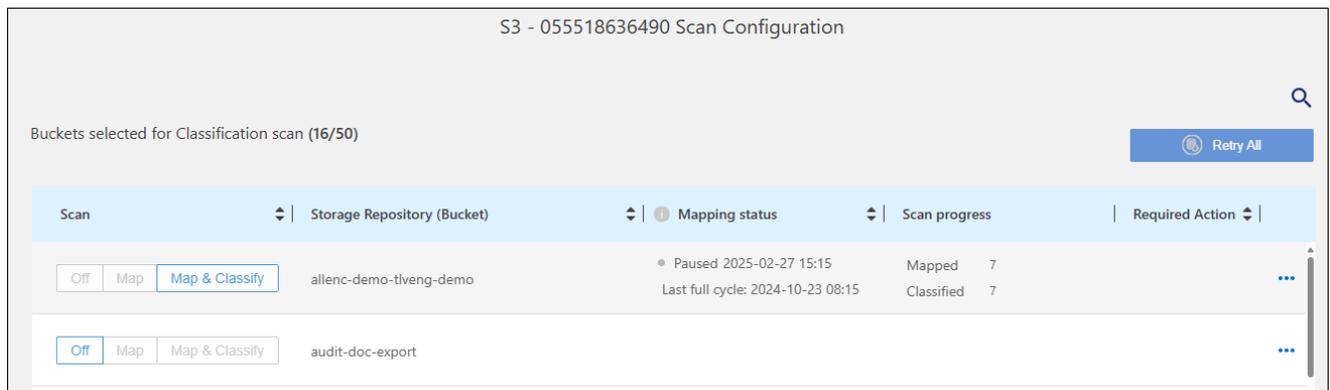
Les bases de données ne peuvent pas être définies pour des analyses de mappage uniquement. L'analyse de la base de données peut être désactivée ou activée, où on équivaut à la cartographie et à la classification.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Dans l'onglet Configuration, sélectionnez le bouton **Configuration** de l'environnement de travail.

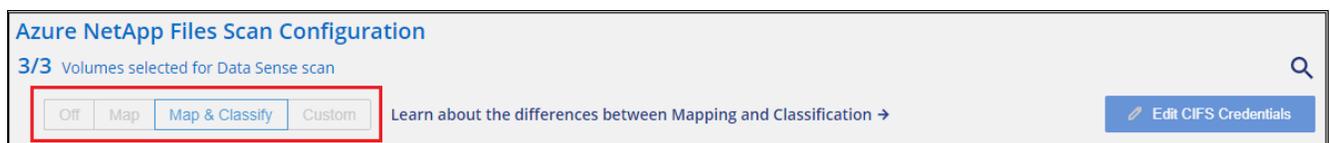


3. Dans la page Configuration de l'analyse, modifiez l'un des référentiels (rubriques dans cet exemple) pour effectuer des analyses **Map** ou **Map & Classify**.



Certains types d'environnements de travail vous permettent de modifier le type de numérisation global pour tous les référentiels à l'aide d'une barre de boutons située en haut de la page. Valable pour les systèmes Cloud Volumes ONTAP, ONTAP sur site, Azure NetApp Files et Amazon FSX pour ONTAP.

L'exemple ci-dessous montre cette barre de boutons pour un système Azure NetApp Files.



Hierarchiser les acquisitions

Vous pouvez hierarchiser les acquisitions de mappage uniquement les plus importantes ou les analyses de mappage et de classification afin de vous assurer que les acquisitions à haute priorité sont effectuées en premier.

Par défaut, les analyses sont mises en file d'attente en fonction de l'ordre dans lequel elles sont initiées. Avec la possibilité de hierarchiser les numérisations, vous pouvez déplacer les numérisations vers l'avant de la file d'attente. Plusieurs acquisitions peuvent être classées par ordre de priorité. La priorité est désignée dans un ordre de premier entrée et de premier sortie, ce qui signifie que la première analyse prioritaire se déplace vers l'avant de la file d'attente ; la deuxième analyse prioritaire devient la deuxième dans la file d'attente, etc.

La priorité est accordée une fois. Les nouvelles analyses automatiques des données de mappage sont effectuées dans l'ordre par défaut.

Étapes

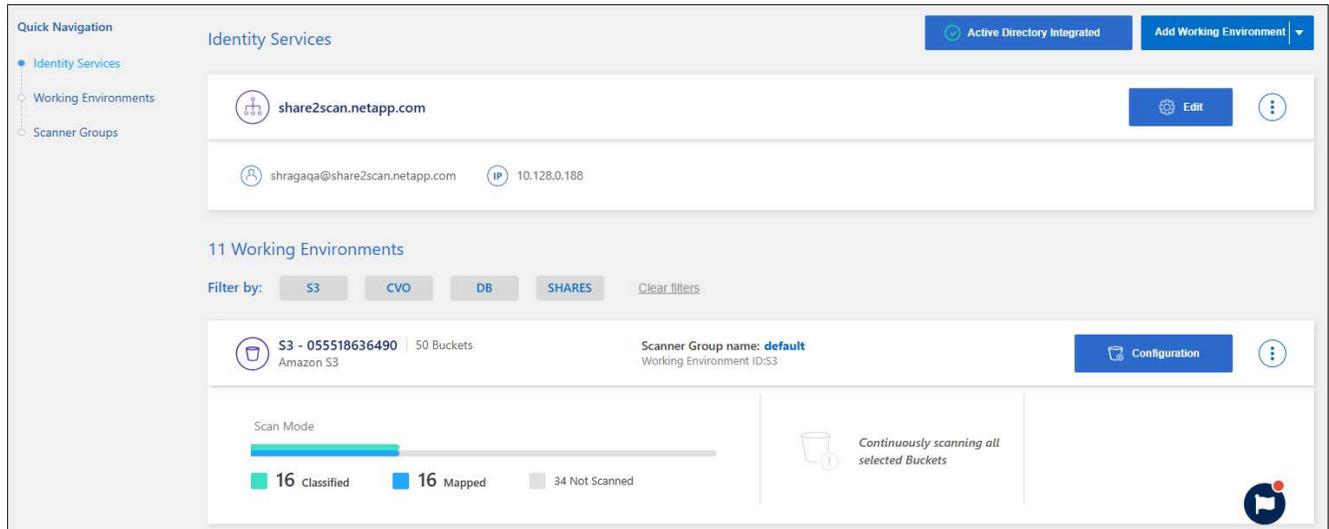
1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Sélectionnez les ressources à hiérarchiser.
3. Dans l'option actions ..., sélectionnez **hiérarchiser l'acquisition**.

Arrêter la recherche d'un référentiel

Vous pouvez arrêter l'analyse d'un référentiel (par exemple, un volume) si vous n'avez plus besoin de le surveiller pour vérifier sa conformité. Pour ce faire, désactivez la numérisation. Lorsque la numérisation est désactivée, l'indexation et les informations relatives à ce volume sont supprimées du système et le chargement pour la numérisation des données est interrompu.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Dans l'onglet Configuration, sélectionnez le bouton **Configuration** de l'environnement de travail.



Quick Navigation

- Identity Services
- Working Environments
- Scanner Groups

Identity Services

Active Directory Integrated | Add Working Environment

share2scan.netapp.com | Edit

shragaa@share2scan.netapp.com | IP 10.128.0.188

11 Working Environments

Filter by: S3 | CVO | DB | SHARES | Clear filters

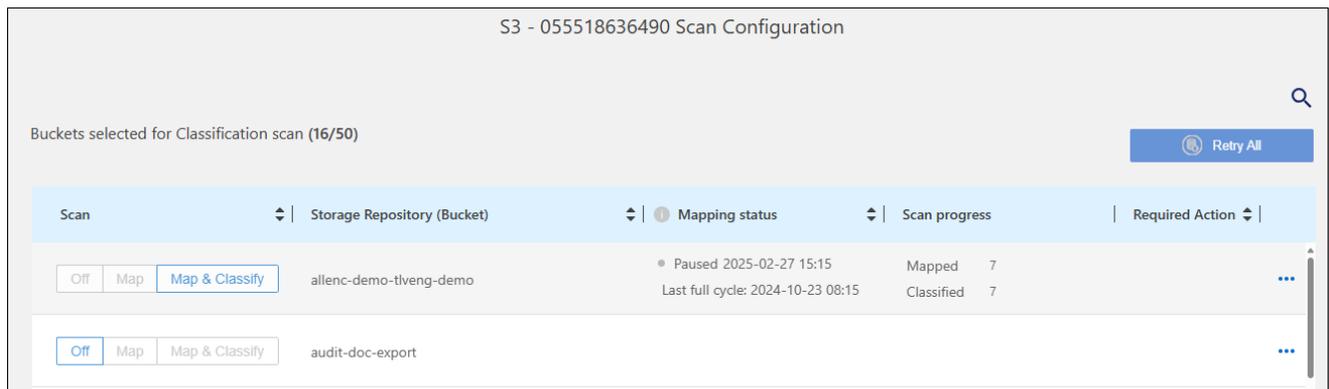
S3 - 055518636490 | 50 Buckets | Amazon S3 | Scanner Group name: default | Working Environment ID:S3 | Configuration

Scan Mode

16 Classified | 16 Mapped | 34 Not Scanned

Continuously scanning all selected Buckets

3. Dans la page Configuration de l'acquisition, sélectionnez **Désactivé** pour arrêter l'analyse d'un compartiment particulier.



S3 - 055518636490 Scan Configuration

Buckets selected for Classification scan (16/50) | Retry All

Scan	Storage Repository (Bucket)	Mapping status	Scan progress	Required Action
Off Map Map & Classify	allenc-demo-tlveng-demo	Paused 2025-02-27 15:15 Last full cycle: 2024-10-23 08:15	Mapped 7 Classified 7	...
Off Map Map & Classify	audit-doc-export			...

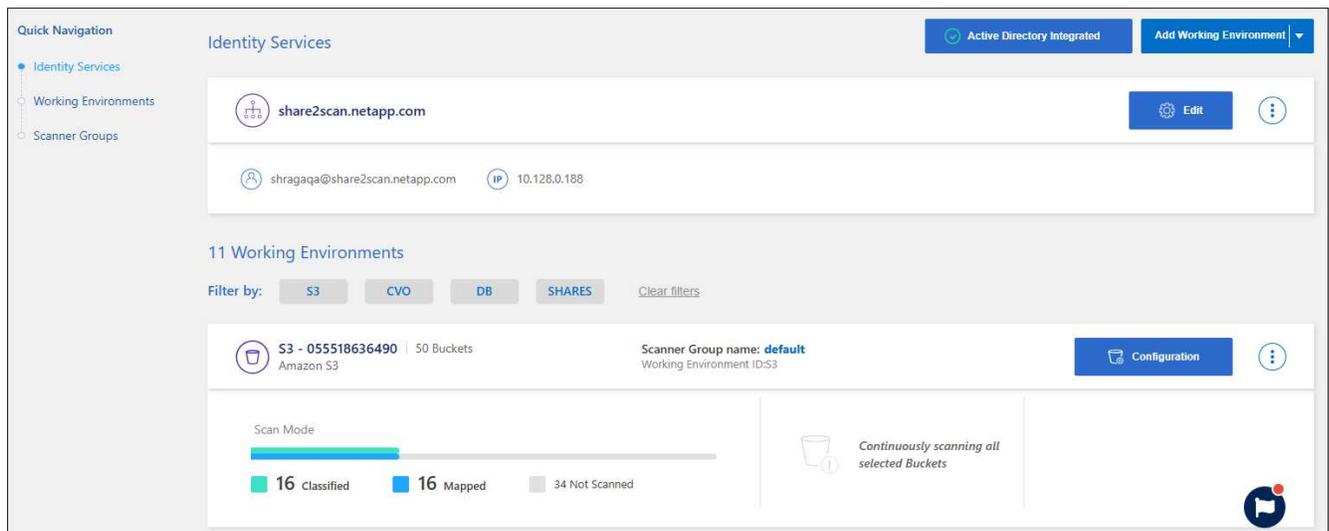
Mettre en pause et reprendre l'analyse d'un référentiel

Vous pouvez interrompre la numérisation dans un référentiel si vous souhaitez arrêter temporairement la numérisation de certains contenus. Avec l'interruption de l'analyse, la classification BlueXP n'effectuera aucune analyse ultérieure en cas de modification ou d'ajout au référentiel, mais tous les résultats actuels seront toujours affichés dans le système. La mise en pause de la numérisation ne cesse pas de charger les données scannées car elles existent toujours.

Vous pouvez reprendre la numérisation à tout moment.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez **Configuration**.
2. Dans l'onglet Configuration, sélectionnez le bouton **Configuration** de l'environnement de travail.



3. Dans la page Configuration de la numérisation, sélectionnez l'icône actions **...**.
4. Sélectionnez **Pause** pour interrompre le balayage d'un volume ou sélectionnez **reprendre** pour reprendre le balayage d'un volume précédemment interrompu.

Consultez les rapports de conformité à la classification BlueXP

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, vous pouvez filtrer pour les voir uniquement.



- 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.

Les rapports suivants sont disponibles pour la classification BlueXP :

- **Rapport d'évaluation de la découverte des données** : fournit une analyse de haut niveau de l'environnement analysé pour mettre en évidence les résultats du système et pour montrer les secteurs préoccupants et les étapes potentielles de la correction.
- **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.
- **Rapport de demande d'accès de la personne concernée** : vous permet d'extraire un rapport de tous les fichiers contenant des informations concernant le nom spécifique ou l'identifiant personnel d'une personne concernée.
- **Rapport HIPAA** : vous aide à identifier la distribution de l'information sur la santé dans vos fichiers.
- **Rapport PCI DSS** : vous aide à identifier la distribution des informations de carte de crédit dans vos fichiers.
- **Rapport sur l'évaluation des risques en matière de confidentialité** : fournit des renseignements sur la confidentialité de vos données et une note sur les risques en matière de confidentialité.
- **Rapports sur un type d'information spécifique**: Des rapports sont disponibles qui comprennent 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.

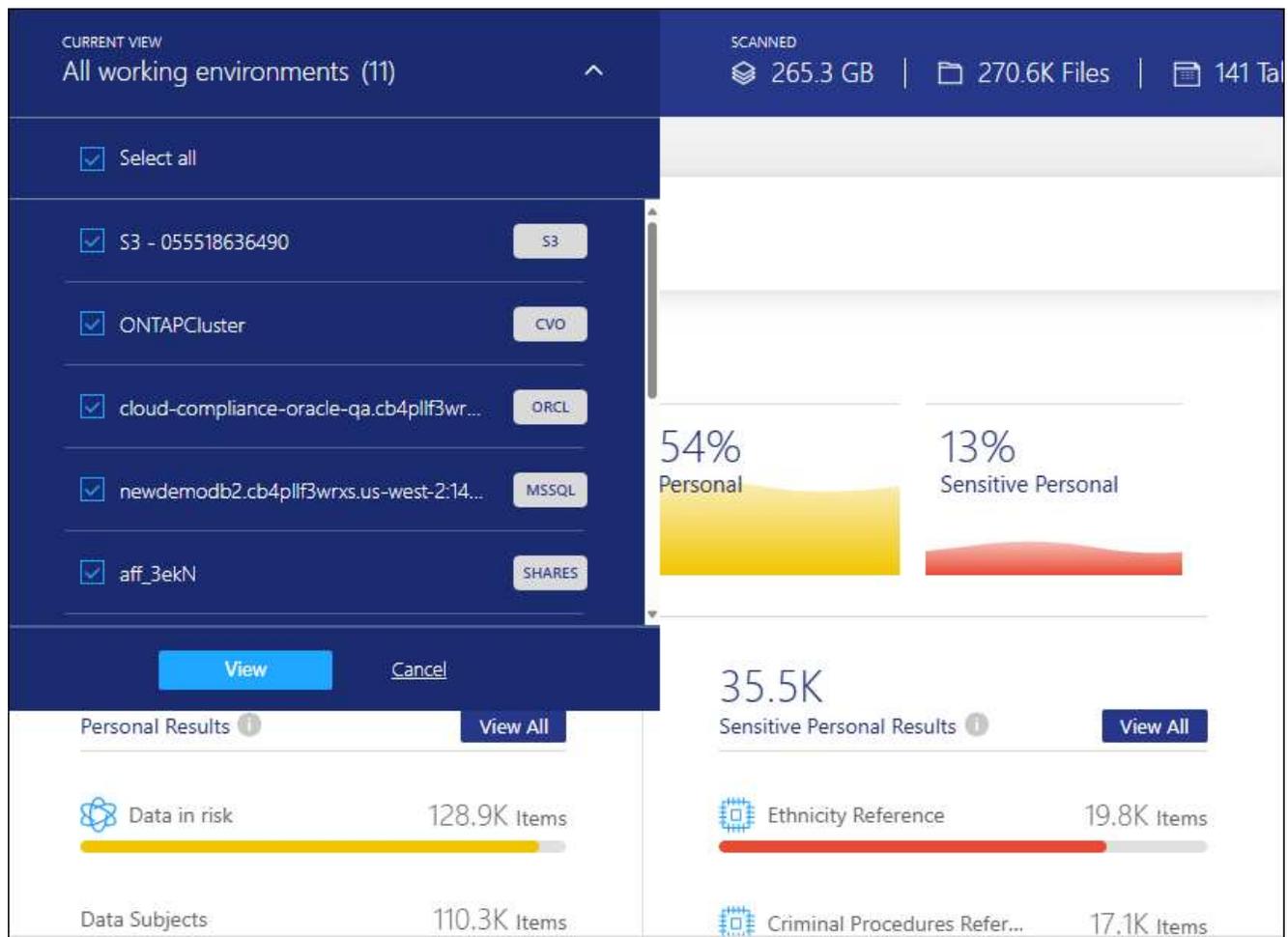
Sélectionnez les environnements de travail pour les rapports

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. Dans le menu BlueXP Classification, sélectionnez "**conformité**".
2. Sélectionnez la liste déroulante filtre environnements de travail et sélectionnez les environnements de travail.
3. Sélectionnez **Afficher**.



Rapport de demande d'accès de la personne concernée

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 RMORCD?

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.

Recherche de sujets de données et téléchargement de 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](#)".

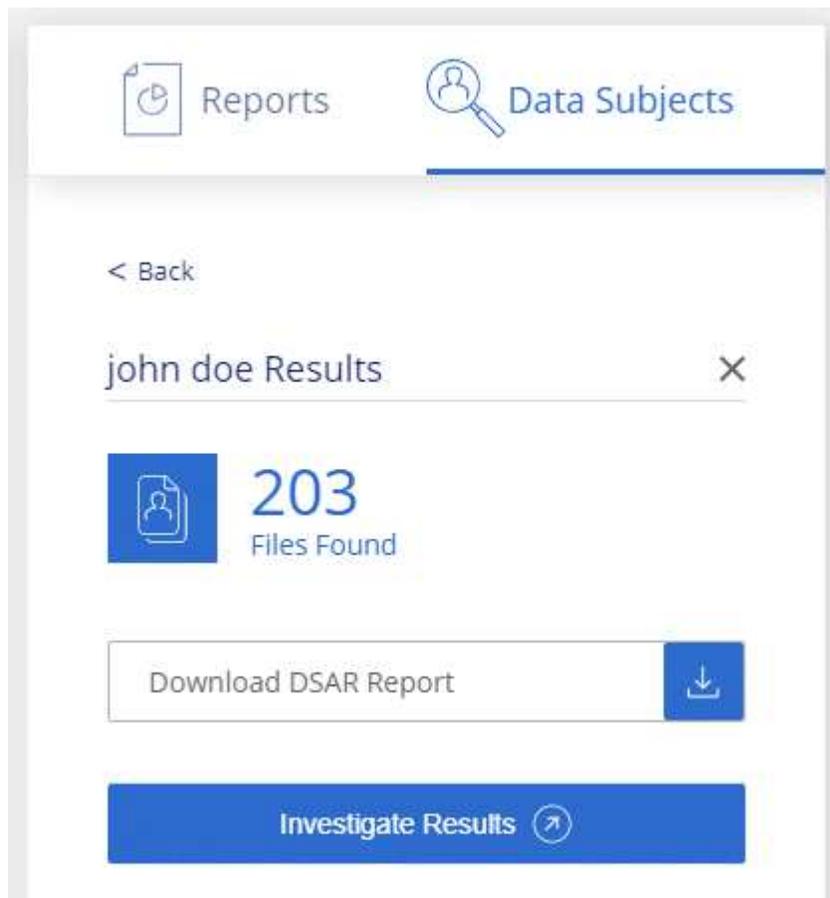


L'anglais, l'allemand, le japonais et l'espagnol sont pris en charge lors de la recherche des noms des sujets de données. La prise en charge d'autres langues sera ajoutée ultérieurement.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez "**conformité**".
2. Dans la page conformité, faites défiler vers le bas et sélectionnez **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.

Rapport conforme à la loi américaine sur la transférabilité et la responsabilité en matière d'assurance maladie (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 :

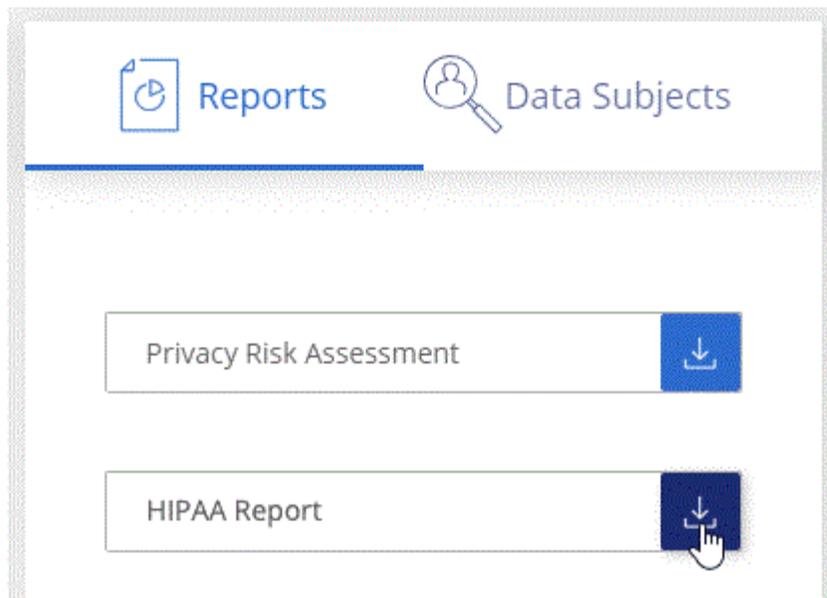
- **Présentation** : nombre de fichiers contenant des informations de santé et dans quels environnements de travail.
- **Chiffrement** : pourcentage de fichiers contenant des informations de santé qui se trouvent dans des environnements de travail chiffrés ou non chiffrés. Ces informations sont spécifiques à Cloud Volumes ONTAP.
- **Protection contre les ransomwares** : pourcentage de fichiers contenant des informations de santé qui se trouvent dans des environnements de travail sur lesquels la protection contre les ransomwares est activée ou non. Ces informations sont spécifiques à Cloud Volumes ONTAP.
- **Conservation** : période de 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 informations de santé** : environnements de travail dans lesquels les informations de santé ont été trouvées et si le chiffrement et la protection contre les ransomware sont activés.

Générer le rapport HIPAA

Accédez à l'onglet conformité pour générer le rapport.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez "**conformité**".
2. Faites défiler vers le bas et localisez le volet **Rapports**.
3. Sélectionnez l'icône de téléchargement en regard de **Rapport HIPAA**.



Résultat

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

Rapport sur la norme de sécurité des données de l'industrie des cartes de paiement (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** : nombre de fichiers contenant des informations de carte de crédit et dans quels environnements de travail.
- **Chiffrement** : pourcentage de fichiers contenant des informations de carte de crédit qui se trouvent dans des environnements de travail chiffrés ou non chiffrés. Ces informations sont spécifiques à Cloud Volumes ONTAP.
- **Protection contre les ransomwares** : pourcentage de fichiers contenant des informations de carte de crédit dans des environnements de travail sur lesquels la protection contre les ransomwares est activée ou non. Ces informations sont spécifiques à Cloud Volumes ONTAP.
- **Conservation** : période de 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** : environnements de travail dans lesquels les informations de carte de crédit ont été trouvées et si le chiffrement et la protection contre les ransomware sont activés.

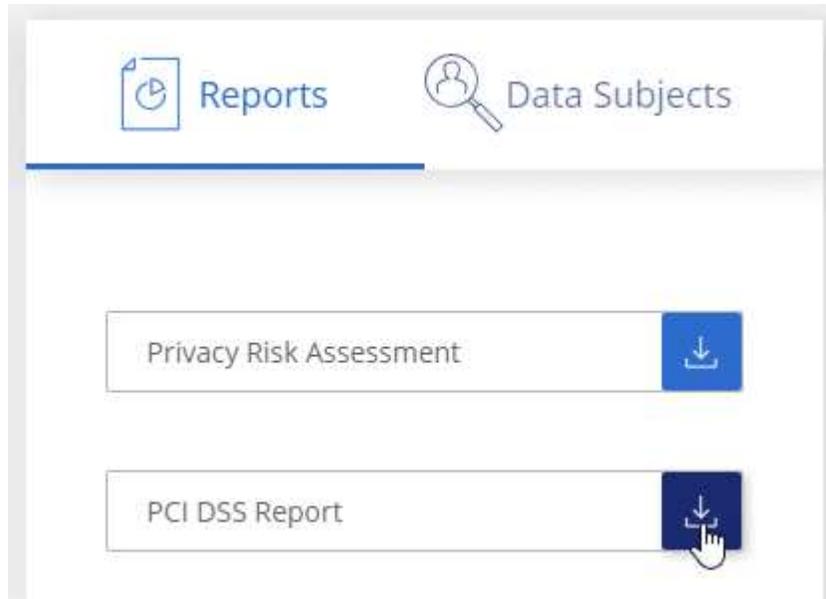
Générer le rapport PCI DSS

Accédez à l'onglet conformité pour générer le rapport.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez "**conformité**".
2. Faites défiler vers le bas et localisez le volet **Rapports**.

3. Sélectionnez l'icône de téléchargement en regard de **PCI DSS Report**.



Résultat

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

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 :

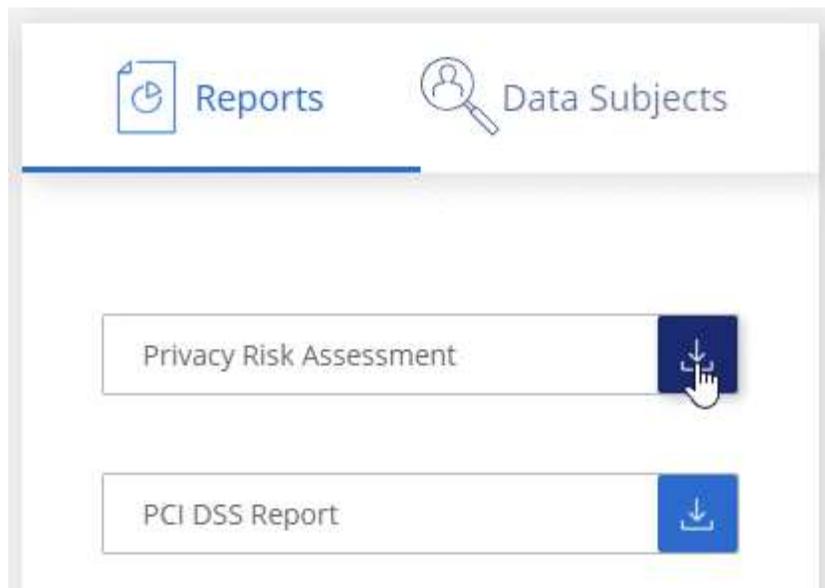
- État de conformité : un score de gravité et la distribution des données, qu'elles soient personnelles ou non sensibles.
- Aperçu de l'évaluation : une ventilation des types de données personnelles trouvées, ainsi que des catégories de données.
- Sujets de données dans cette évaluation : le nombre de personnes, par lieu, pour lesquelles des identificateurs nationaux ont été trouvés.

Générer le rapport d'évaluation des risques pour la protection des renseignements personnels

Accédez à l'onglet conformité pour générer le rapport.

Étapes

1. Dans le menu BlueXP Classification, sélectionnez "**conformité**".
2. Faites défiler vers le bas et localisez le volet **Rapports**.
3. Sélectionnez l'icône de téléchargement en regard de **évaluation des risques liés à la confidentialité**.



Résultat

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

Score 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 %
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 %

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTEUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.