Utilisez le sens des données du cloud

Cloud Data Sense

NetApp
January 09, 2023

This PDF was generated from https://docs.netapp.com/fr-fr/cloud-manager-data-sense/task-controlling-governance-data.html on January 09, 2023. Always check docs.netapp.com for the latest.

Table des matières

Utilisez le sens des données du cloud 1
Affichage des détails de gouvernance concernant les données stockées dans votre organisation 1
Affichage des détails de conformité concernant les données stockées dans votre organisation 5
Organiser vos données privées 17
La gestion de vos données privées 34
Affichage des rapports de conformité 47
Réponse à une demande d’accès à un sujet de données 55
Catégories de données privées 57

Utilisez le sens des données du cloud

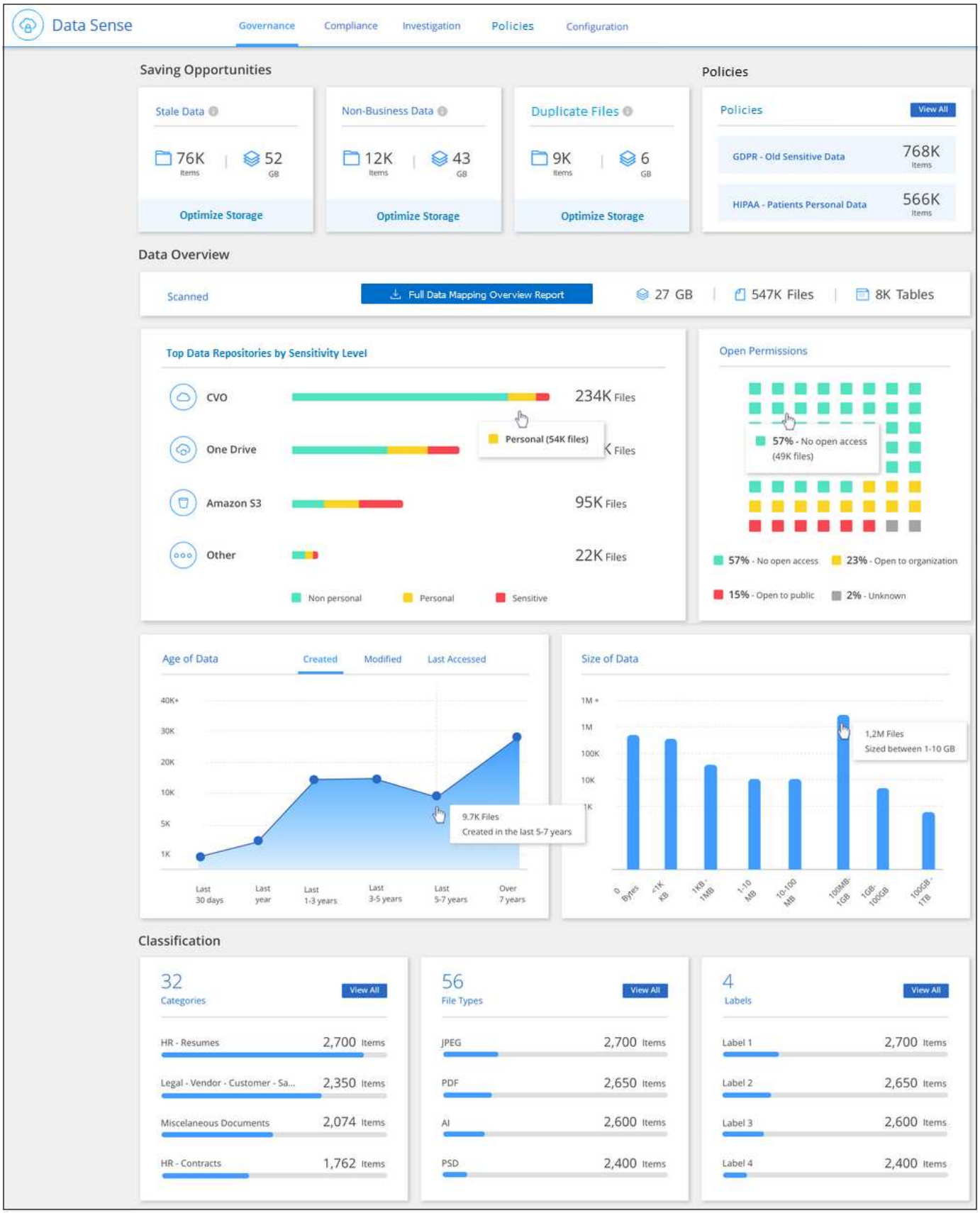
Affichage des détails de gouvernance concernant les données stockées dans votre organisation

Maîtrisez les coûts liés aux données stockées sur les ressources de stockage de votre entreprise. Cloud Data SENSE identifie la quantité de données obsolètes, de données non stratégiques, de fichiers en double et de fichiers très volumineux dans vos systèmes. Vous pouvez ainsi décider si vous souhaitez supprimer ou hiérarchiser certains fichiers dans un stockage objet moins coûteux.

En outre, si vous prévoyez de migrer les données depuis des emplacements sur site vers le cloud, vous pouvez vérifier la taille des données et si chacune d'entre elles contient des informations sensibles avant de les transférer.

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.



Enregistrement d’opportunités

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

afficher les résultats filtrés dans la page Investigation.

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

Règles avec le plus grand nombre de résultats

Cliquez sur le nom d'une police dans la zone *Policy* pour afficher les résultats dans la page Investigation. Cliquez sur **Afficher tout** pour afficher la liste de toutes les stratégies disponibles.

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

Présentation des données

Présentation rapide de toutes les données en cours de numérisation. Cliquez sur le bouton pour télécharger un rapport de mappage de données complet incluant la capacité d'utilisation, l'âge des données, la taille des données et les types de fichiers pour tous les environnements de travail et toutes les sources de données. Voir "Rapport de mappage de données" pour plus d'informations.

Principaux référentiels de données répertoriés par sensibilité des données

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

- Données non personnelles
- Données personnelles
- Données personnelles sensibles

Vous pouvez passer le curseur sur chaque section pour voir le nombre total d'éléments dans chaque catégorie.

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

Données répertoriées par type d'autorisations ouvertes

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

- Aucun accès ouvert
- Ouvert à l'organisation
- Ouvert au public
- Accès inconnu

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

Age des données et taille des données graphiques

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

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

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

Classification des données la plus identifiée

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

Catégories

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

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

Types de fichiers

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

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

Libellés AIP

Si vous vous êtes abonné à Azure information protection (AIP), vous pouvez classer et protéger les documents et les fichiers en appliquant des étiquettes au contenu. La vérification des étiquettes AIP les plus utilisées qui sont attribuées aux fichiers vous permet de voir les étiquettes les plus utilisées dans vos fichiers.

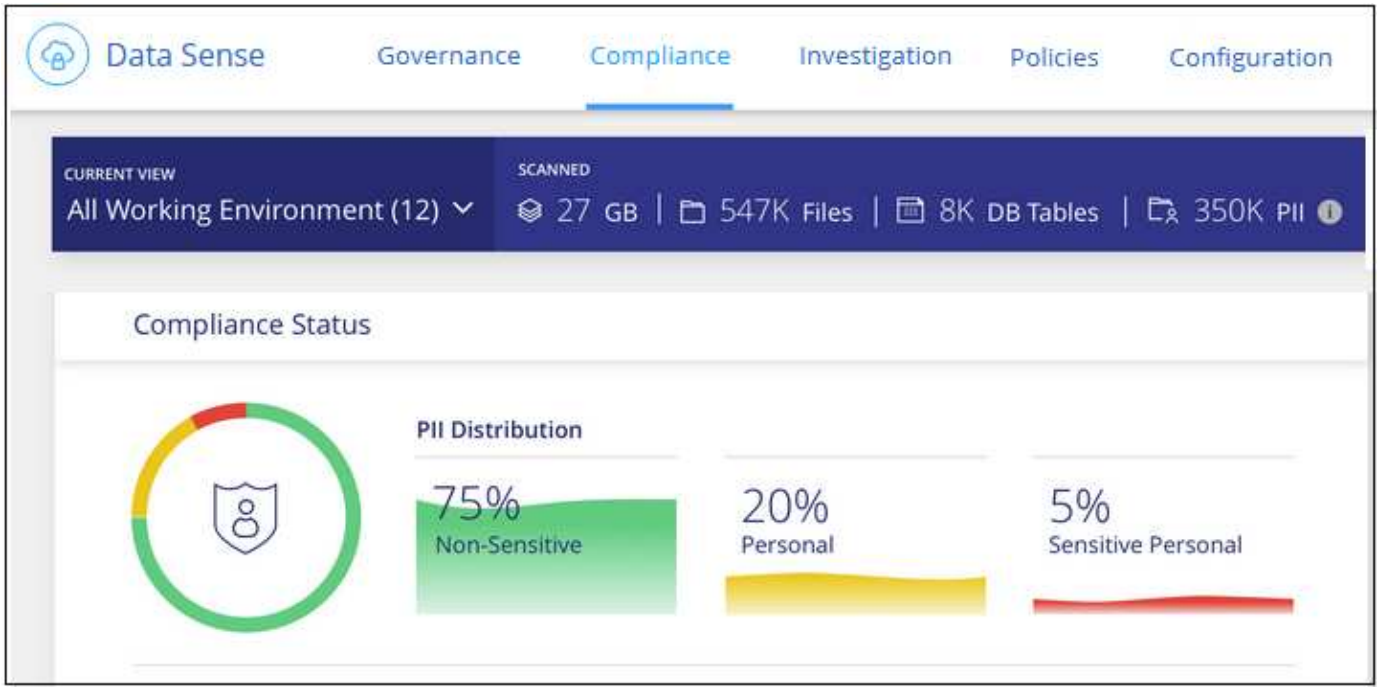
Voir "Etiquettes AIP" pour en savoir plus.

Affichage des détails de conformité concernant les données stockées dans votre organisation

Prenez le contrôle de vos données privées en affichant les détails sur les données personnelles et les données personnelles sensibles de votre organisation. Vous pouvez également consulter les catégories et les types de fichiers que Cloud Data trouve 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 Cloud Data Sense affiche les données de conformité pour tous les environnements et bases de données de travail.



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

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

Affichage des fichiers contenant des données personnelles

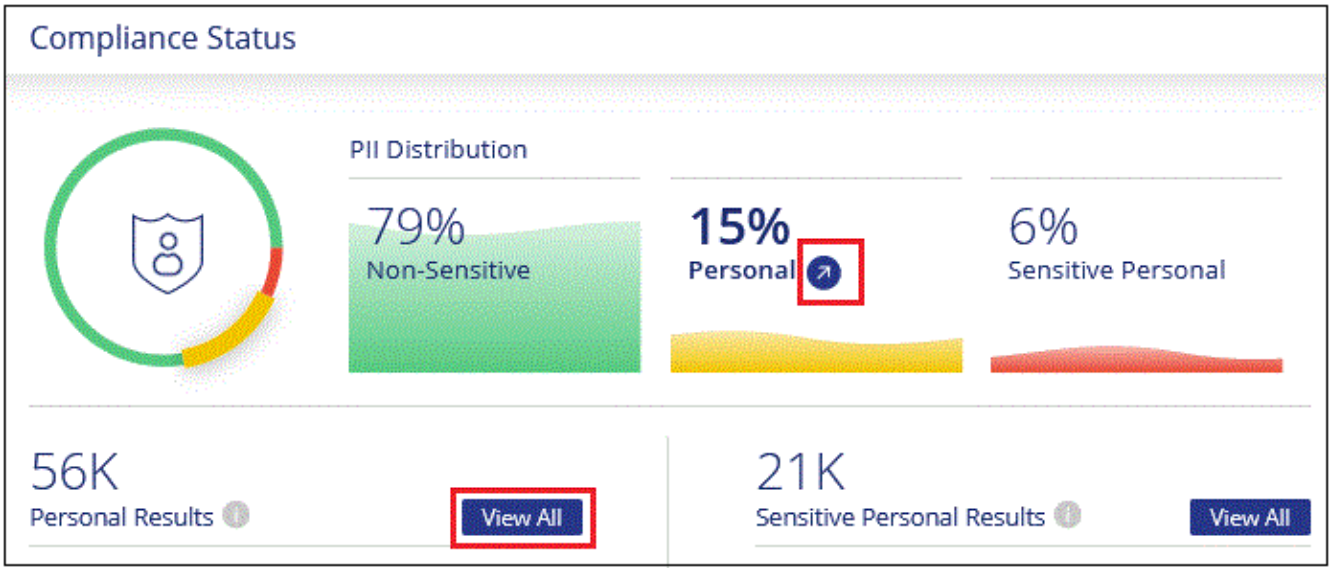
Cloud Data Sense identifie automatiquement des mots, des chaînes et des motifs spécifiques (Regex) dans les données. Par exemple, les renseignements d'identification personnelle (RP), les numéros de carte de crédit, les numéros de sécurité sociale, les numéros de compte bancaire, les mots de passe, entre autres. "Voir la liste complète". Data Sense identifie ce type d'information dans des fichiers individuels, dans des fichiers dans des répertoires (partages et dossiers) et dans des tables de bases de données.

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

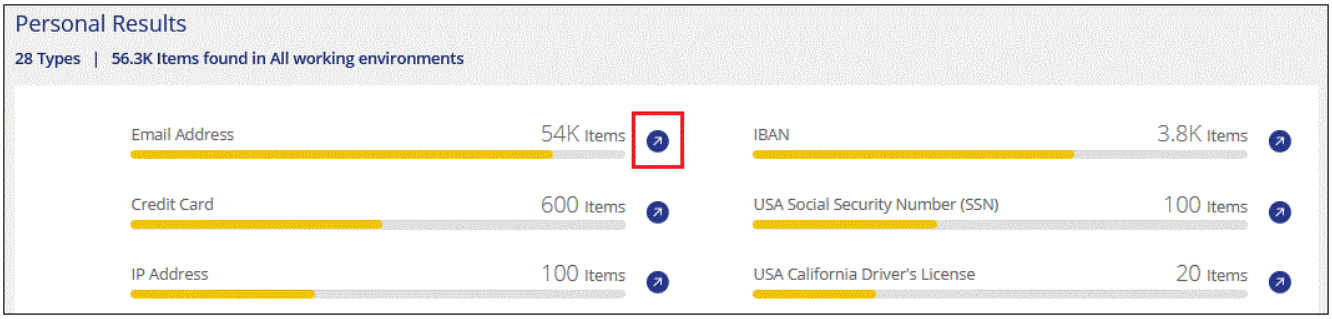
Pour certains types de données personnelles, Data Sense utilise *la validation de proximité* pour valider ses conclusions. La validation se produit en recherchant un ou plusieurs mots clés prédéfinis à proximité des données personnelles trouvées. Par exemple, Data Sense identifie un américain Numéro de sécurité sociale (SSN) comme numéro de sécurité sociale s'il y a un mot de proximité, par exemple, *SSN* ou *social Security*. "Le tableau des données personnelles" Indique quand Data SENSE utilise la validation de proximité.

Étapes

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



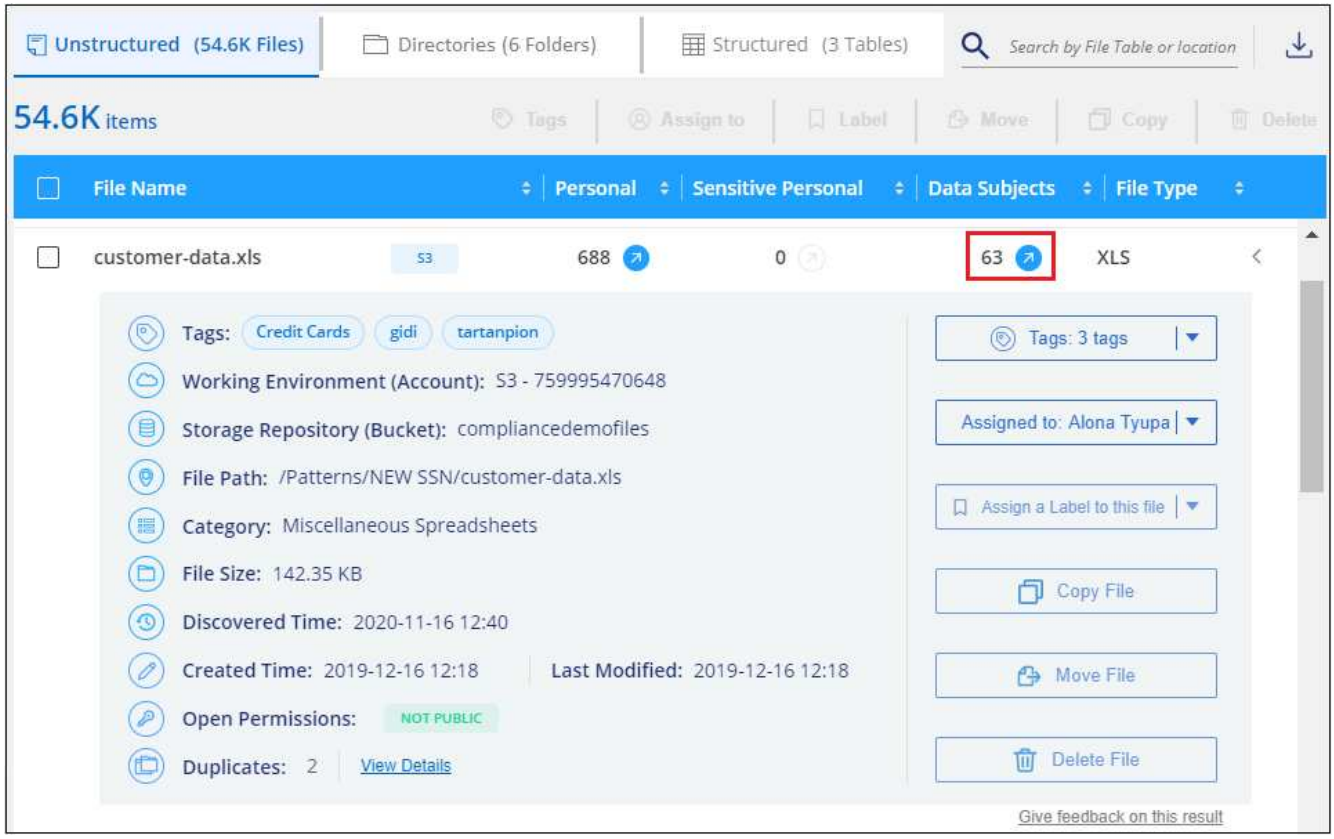
3. Pour examiner les détails d'un type spécifique de données personnelles, cliquez sur **Afficher tout**, puis cliquez sur l'icône **étudier les résultats** pour un type spécifique de données personnelles, par exemple les adresses e-mail.

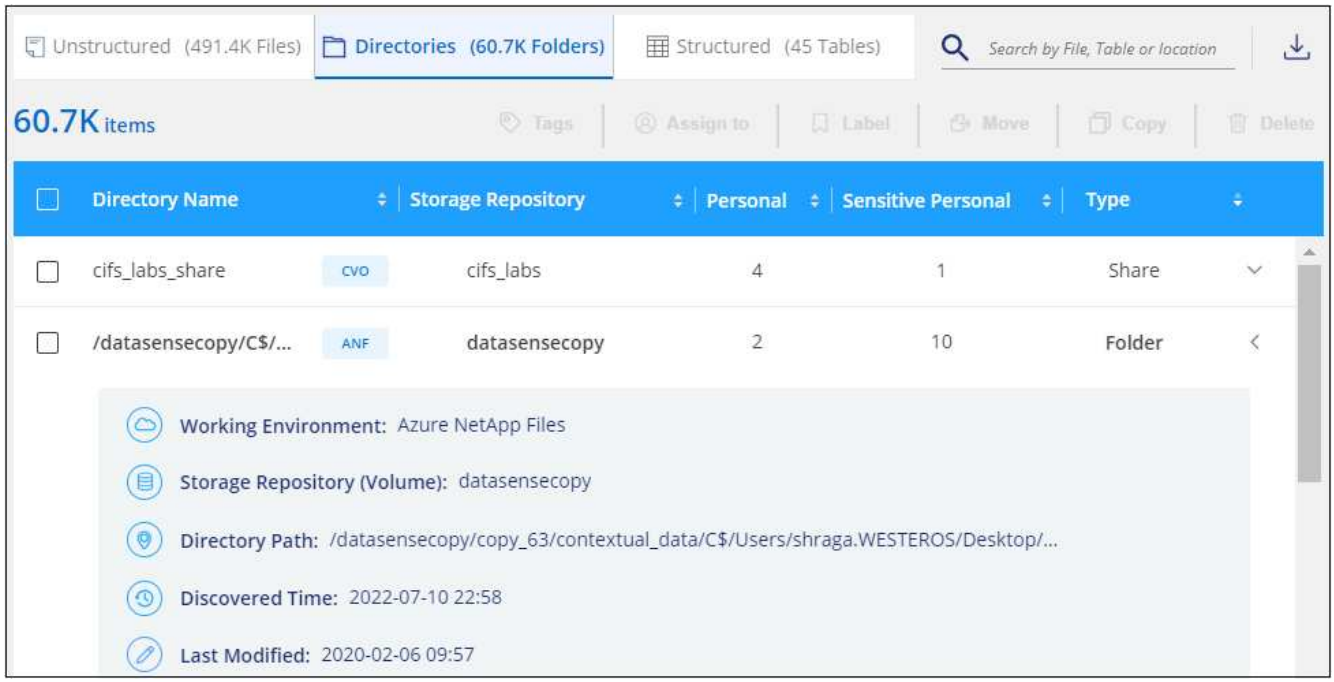


4. Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en cliquant sur **Informez Results** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.

   Les 2 captures d'écran ci-dessous montrent les données personnelles trouvées dans des fichiers

individuels et trouvées dans des fichiers dans des répertoires (partages et dossiers). Vous pouvez également sélectionner l'onglet **Structured** pour afficher les données personnelles contenues dans les bases de données.





Affichage des fichiers contenant des données personnelles sensibles

Cloud Data Sense identifie automatiquement des types spéciaux d'informations personnelles sensibles, comme définis par les réglementations en matière de 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". Data Sense identifie ce type d'information dans des fichiers individuels, dans des fichiers dans des répertoires (partages et dossiers) et dans des tables de bases de données.

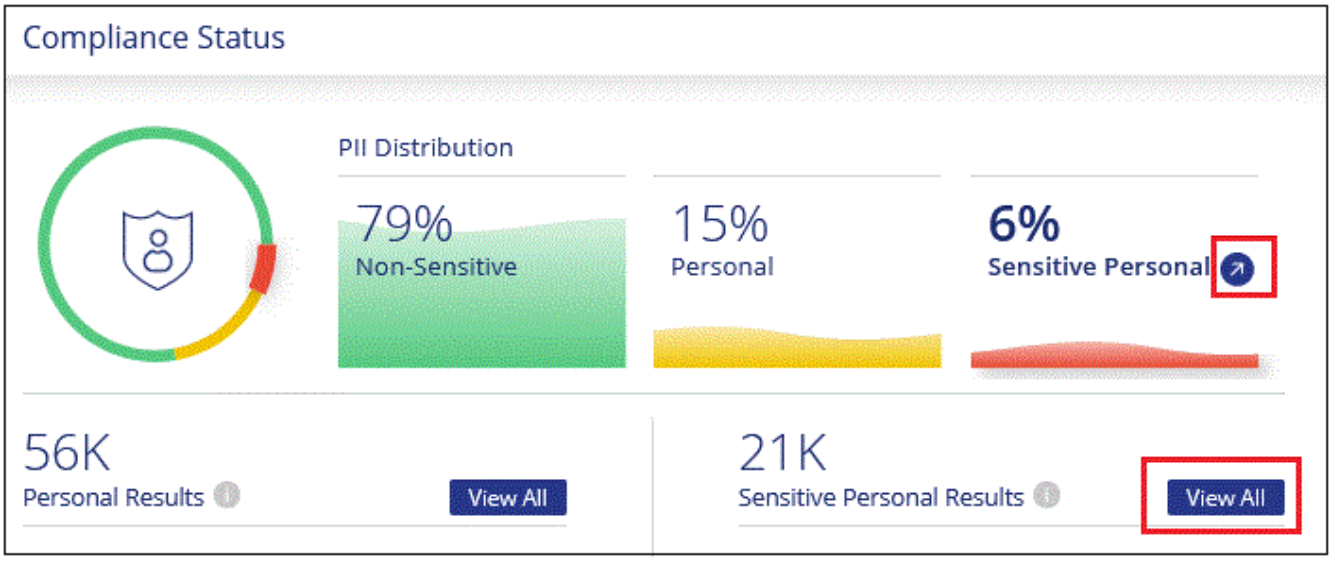
Cloud Data Sense utilise l'intelligence artificielle (IA), le traitement du langage naturel (NLP), l'apprentissage machine (ML) et l'informatique cognitive (CC) pour comprendre la signification du contenu qu'il analyse afin d'extraire des entités et de le catégoriser en conséquence.

Par exemple, une catégorie de données sensibles du RGPD est l'origine ethnique. Du fait de ses capacités NLP, Data Sense peut distinguer une phrase qui lit « George est mexicain » (en indiquant des données sensibles comme indiqué à l'article 9 du RGPD), et « George mange de la nourriture mexicaine ».

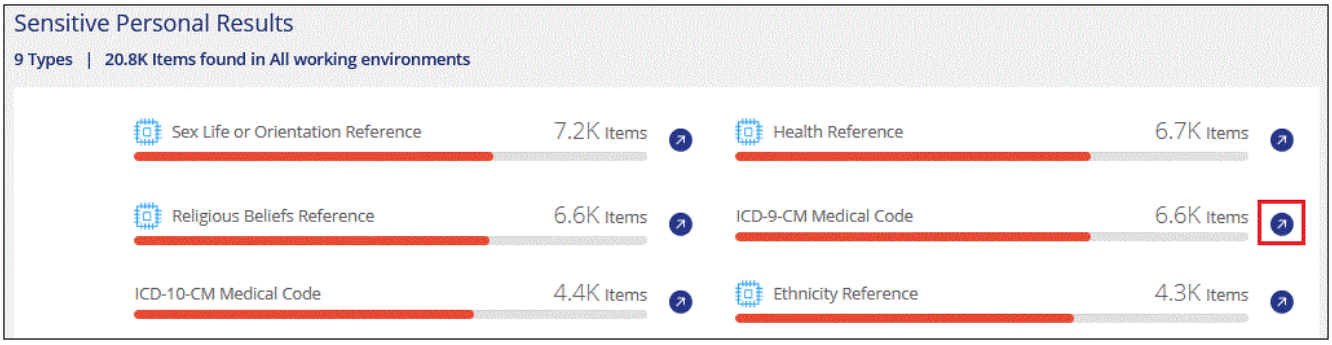
> Seul l'anglais est pris en charge lors de la recherche de données personnelles sensibles. La prise en charge d'autres langues sera ajoutée ultérieurement.

Étapes

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



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



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

Affichage des fichiers par catégories

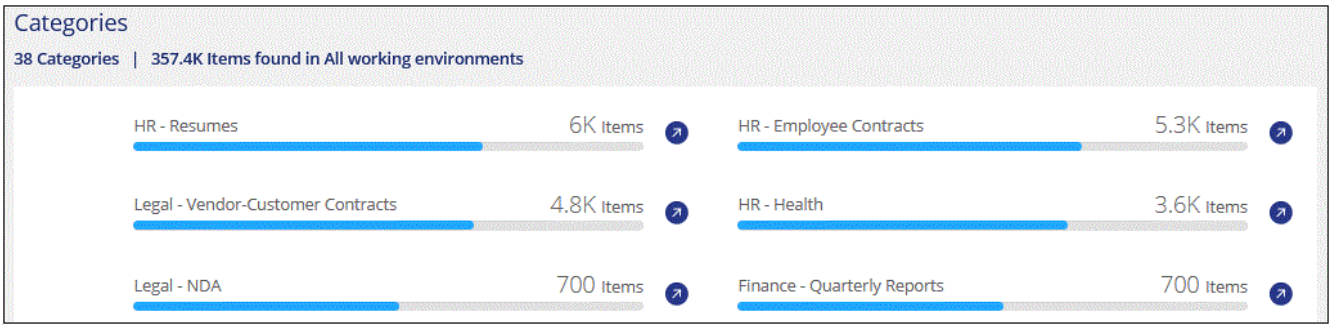
Cloud Data SENSE répartit les données analysées et les divise en différents types de catégories. Les catégories sont des rubriques basées sur l'analyse par IA du contenu et des métadonnées de chaque fichier. "Voir la liste des catégories".

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 étudiez les résultats, vous pouvez constater que les contrats d'employés sont stockés dans un emplacement non sécurisé. Vous pouvez ensuite corriger ce problème.

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

Étapes

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



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

Affichage des fichiers par type de fichier

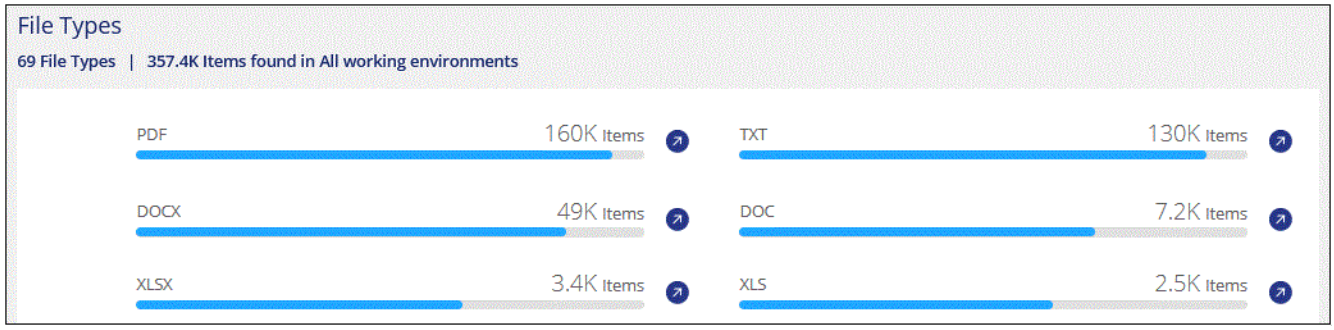
Cloud Data SENSE affecte les données analysées et les divise par type de fichier. La vérification de vos types de fichiers peut vous aider à contrôler vos données sensibles car il se peut que certains types de fichiers ne soient pas stockés correctement. "Voir la liste des types de fichiers".

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

Étapes

1. Dans le menu de navigation de gauche BlueXP, cliquez sur **gouvernance > classement**, puis sur l'onglet **conformité**.

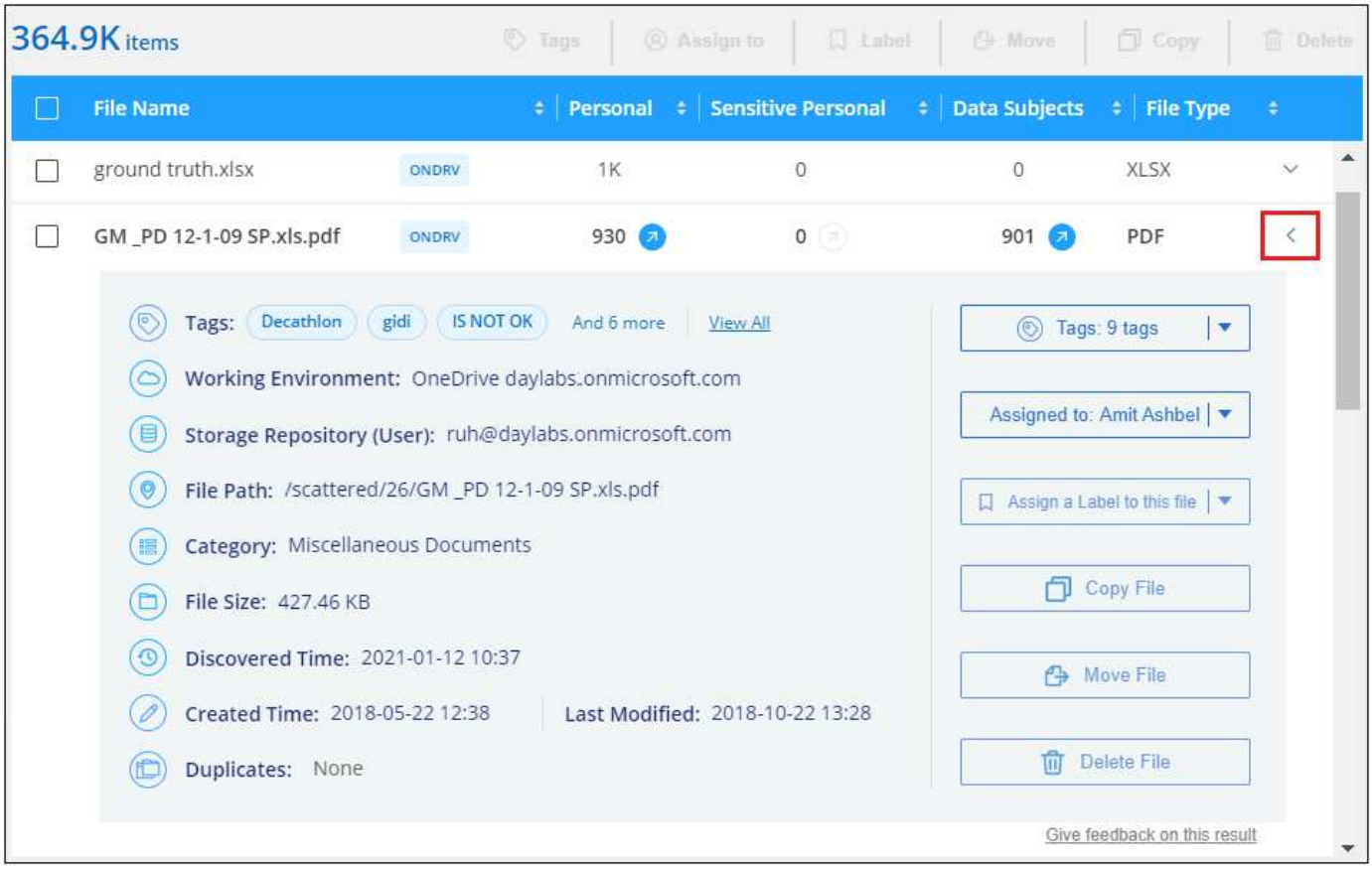
2. Cliquez sur l'icône **étudier les résultats** pour l'un des 4 types de fichiers les plus importants directement à partir de l'écran principal ou cliquez sur **Afficher tout**, puis cliquez sur l'icône correspondant à l'un des types de fichiers.



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

Affichage des métadonnées de fichier

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



En plus de vous indiquer l'environnement de travail et le volume où se trouve le fichier, les métadonnées affichent beaucoup plus d'informations, notamment les autorisations de fichier, le propriétaire du fichier, s'il existe des doublons de ce fichier et l'étiquette AIP attribuée (si vous disposez de "AIP intégré dans le cloud Data SENSE"). Ces informations sont utiles si vous prévoyez de le faire "Créer des règles" car vous pouvez

voir toutes les informations que vous pouvez utiliser pour filtrer vos données.

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

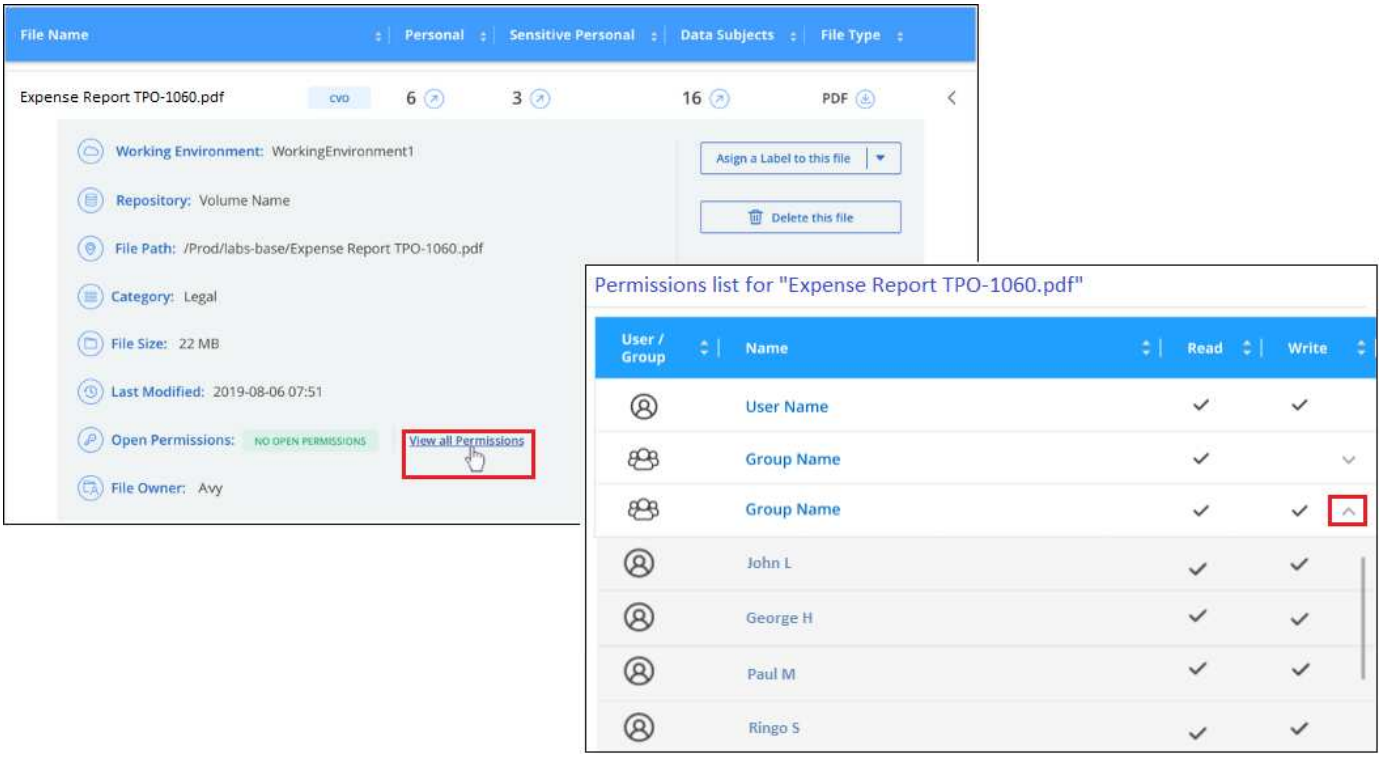
Lors de l'affichage des détails d'un seul fichier, vous pouvez effectuer quelques actions sur le fichier :

- Vous pouvez déplacer ou copier le fichier dans n'importe quel partage NFS. Voir "Déplacement des fichiers source vers un partage NFS" et "Copie des fichiers source vers un partage NFS" pour plus d'informations.
- Vous pouvez supprimer le fichier. Voir "Suppression des fichiers source" pour plus d'informations.
- Vous pouvez affecter un certain état au fichier. Voir "Application de balises" pour plus d'informations.
- Vous pouvez affecter le fichier à un utilisateur BlueXP pour être responsable de toutes les actions de suivi qui doivent être effectuées sur le fichier. Voir "Affectation d'utilisateurs à un fichier" pour plus d'informations.
- Si vous avez intégré des étiquettes AIP avec Cloud Data SENSE, vous pouvez attribuer un libellé à ce fichier ou modifier un libellé différent si celui-ci existe déjà. Voir "Attribution manuelle d'étiquettes AIP" pour plus d'informations.

Affichage des autorisations pour les fichiers et les répertoires

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

Notez que si vous voyez des SID (identificateurs de sécurité) au lieu des noms d'utilisateurs et de groupes, vous devez intégrer Active Directory dans Data Sense. "Découvrez comment faire".



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

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

Recherche de fichiers en double dans vos systèmes de stockage

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

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

Vous pouvez télécharger la liste des fichiers dupliqués et les envoyer à votre administrateur de stockage afin qu'il puisse décider quels fichiers, le cas échéant, être supprimé. Ou vous le pouvez "supprimez le fichier" vous-même si vous êtes sûr qu'une version spécifique du fichier n'est pas nécessaire.

Affichage de tous les fichiers dupliqués

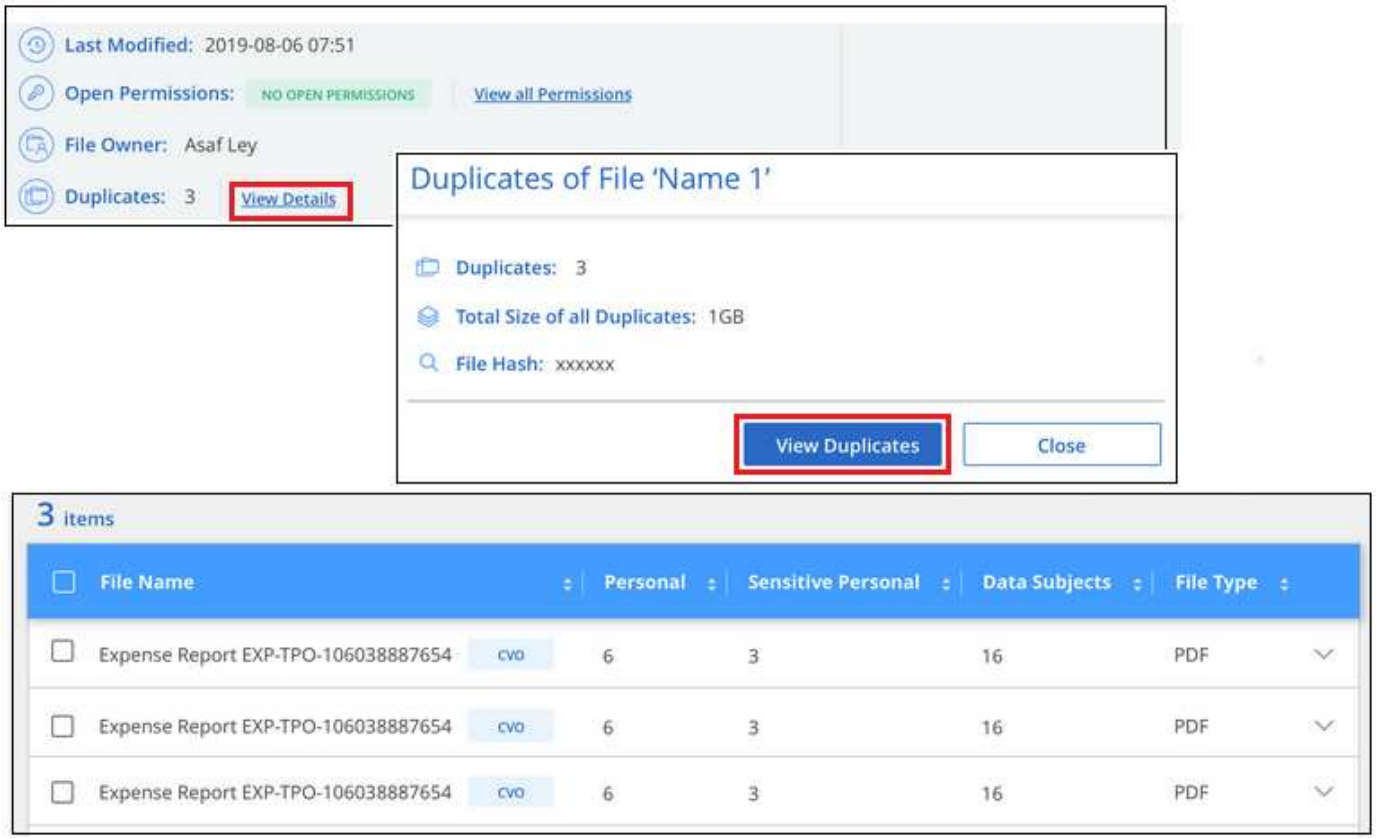
Si vous voulez une liste de tous les fichiers dupliqués dans les environnements de travail et les sources de données que vous scannez, vous pouvez utiliser le filtre **Duplicates > a des doublons** dans la page recherche de données.

Tous les fichiers avec des doublons de tous les types de fichiers (sans les bases de données), d'une taille minimale de 50 Mo et/ou contenant des informations personnelles ou sensibles, s'affichent dans la page Résultats.

Affichage si un fichier spécifique est dupliqué

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

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



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

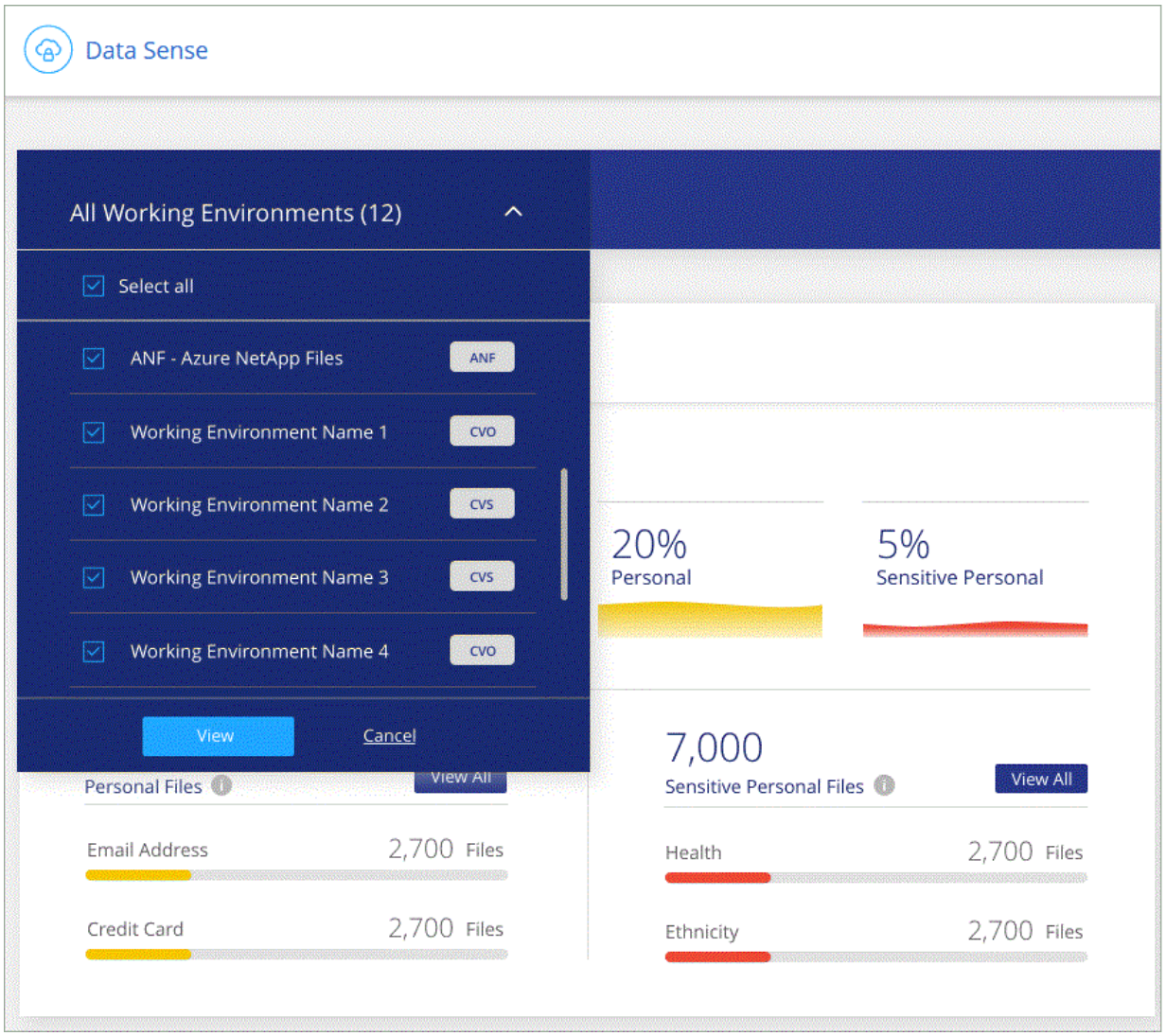
Affichage des données du tableau de bord pour des environnements de travail spécifiques

Vous pouvez filtrer le contenu du tableau de bord Cloud Data Sense afin d'afficher les données de conformité pour tous les environnements de travail et bases de données, ou pour des environnements de travail spécifiques uniquement.

Lorsque vous filtrez le tableau de bord, Data SENSE évalue les données de conformité et les rapports aux environnements de travail que vous avez sélectionnés.

Étapes

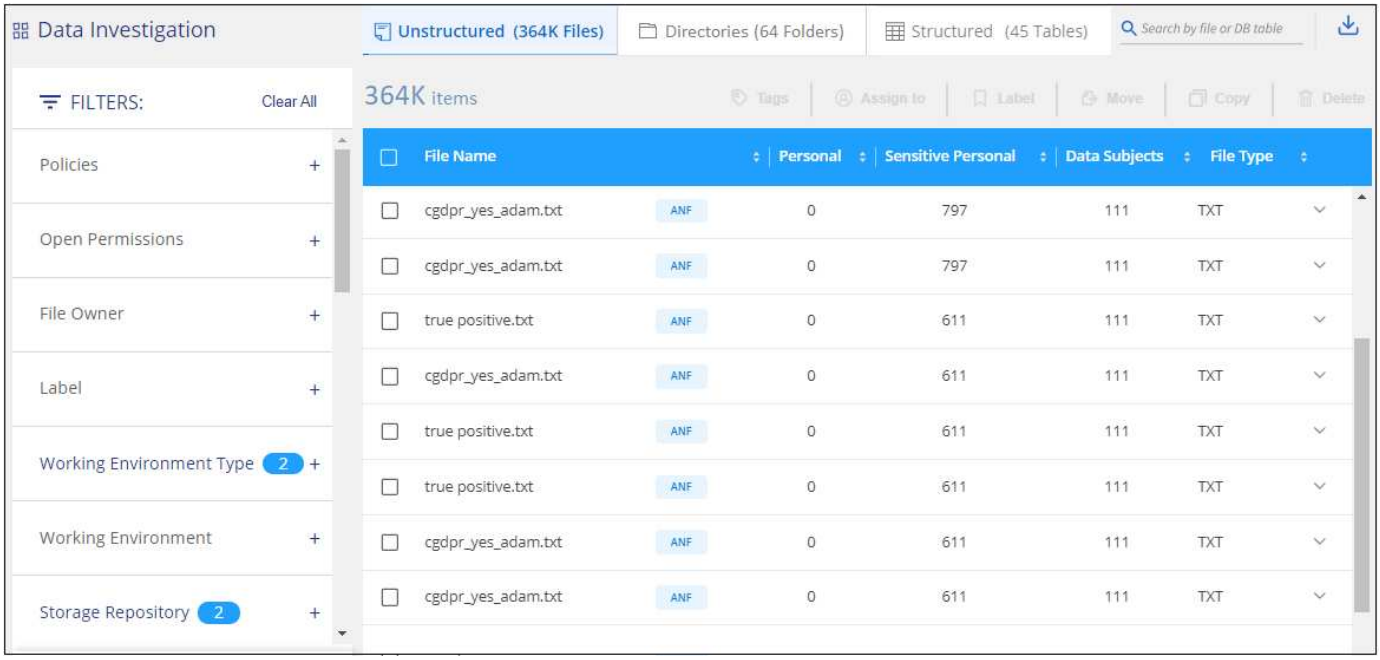
1. Cliquez sur la liste déroulante du filtre, sélectionnez les environnements de travail pour lesquels vous souhaitez afficher les données, puis cliquez sur **Afficher**.



Filtrage des données dans la page Data Investigation

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

Si vous souhaitez télécharger le contenu de la page en tant que rapport après l'avoir affiné, cliquez sur le bouton bouton. Vous pouvez enregistrer le rapport localement sous la forme d'un fichier .CSV (qui peut inclure jusqu'à 5,000 lignes de données) ou sous la forme d'un fichier .JSON que vous exportez vers un partage NFS (qui peut inclure un nombre illimité de lignes). "Cliquez ici pour plus de détails sur les rapports d'enquête de données".



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

Filtre	Détails
Stratégies	Sélectionnez une ou plusieurs stratégies. Aller "ici" pour afficher la liste des règles existantes et créer vos propres règles personnalisées.
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.
Ouvrez autorisations	Sélectionnez le type d'autorisations dans les données et dans les dossiers/partages.
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.
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.
Étiquette	Sélectionnez "Libellés AIP" qui sont affectés à vos fichiers.
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.

Filtre	Détails
Référentiel de stockage	Sélectionnez le référentiel de stockage, par exemple un volume ou un schéma.
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 inclure des chemins d'accès et exclure des chemins, Data Sense recherche d'abord tous les fichiers des chemins inclus, puis supprime les fichiers des chemins exclus, puis affiche les résultats.
Catégorie	Sélectionner "types de catégories".
Niveau de sensibilité	Sélectionnez le niveau de sensibilité : personnel, personnel sensible ou non sensible.
Nombre d'identificateurs	Sélectionnez la plage d'identificateurs sensibles détectés par fichier. Inclut des données personnelles et des données personnelles sensibles. Lors du filtrage dans les répertoires, Data Sense totalise les correspondances de tous les fichiers de chaque dossier (et sous-dossiers).
Données personnelles	Sélectionner "types de données personnelles".
Données personnelles sensibles	Sélectionner "types de données personnelles sensibles".
Sujet de données	Saisissez le nom complet ou l'identifiant connu d'un sujet de données.
Type de répertoire	Sélectionnez le type de répertoire : « partager » ou « dossier ».
Type de fichier	Sélectionner "types de fichiers".
Taille du fichier	Sélectionnez la plage de tailles de fichier.
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 le fichier est détecté par le capteur de données. 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 pour la dernière fois où le fichier a été accédé. Vous pouvez également spécifier une plage horaire personnalisée pour affiner davantage les résultats de la recherche. Pour les types de fichiers analysés par Data Sense, il s'agit de la dernière analyse du fichier par Data Sense.
Doublons	Indiquez si le fichier est dupliqué dans les référentiels.
Hachage de fichiers	Entrez le hachage du fichier pour trouver un fichier spécifique, même si le nom est différent.
Étiquettes	Sélectionnez "la ou les balises" qui sont affectés à vos fichiers.
Affecté à	Sélectionnez le nom de la personne à laquelle le fichier est affecté.

Organiser vos données privées

Avec Cloud Data Sense, vous pouvez gérer et organiser vos données privées de plusieurs façons. Vous pouvez ainsi consulter plus facilement les données qui vous sont les plus importantes.

- Si vous êtes abonné à "Protection des informations Azure (AIP)" Pour classer et protéger vos fichiers, vous pouvez utiliser Cloud Data Sense pour gérer ces étiquettes AIP.
- Vous pouvez ajouter des balises aux fichiers que vous souhaitez marquer pour une organisation ou pour un type de suivi.
- Vous pouvez affecter un utilisateur BlueXP à un fichier spécifique ou à plusieurs fichiers, de sorte que cette personne puisse être responsable de la gestion du fichier.
- Grâce à la fonctionnalité « Stratégie », vous pouvez créer vos propres requêtes de recherche personnalisées afin de pouvoir voir facilement les résultats en cliquant sur un bouton.
- Vous pouvez envoyer des alertes par e-mail à des utilisateurs BlueXP ou à toute autre adresse e-mail lorsque certaines stratégies critiques renvoient des résultats.

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

Dois-je utiliser des étiquettes ou des étiquettes ?

Vous trouverez ci-dessous une comparaison du balisage Data Sense et de l'étiquetage Azure information protection.

Étiquettes	Étiquettes
Les balises de fichier font partie intégrante de Data Sense.	Vous devez vous être abonné à Azure information protection (AIP).
La balise est conservée uniquement dans la base de données de détection des données - elle n'est pas écrite dans le fichier. Il ne modifie pas le fichier, ni les heures d'accès ou de modification du fichier.	Le libellé fait partie du fichier et, lorsque le libellé change, le fichier change. Cette modification modifie également les heures d'accès et de modification du fichier.
Vous pouvez avoir plusieurs balises sur un seul fichier.	Vous pouvez avoir une étiquette sur un seul fichier.
Cette balise peut être utilisée pour une action interne de détection des données, telle que copie, déplacement, suppression, exécution d'une règle, etc	Les autres systèmes qui peuvent lire le fichier peuvent voir l'étiquette, qui peut être utilisée pour une automatisation supplémentaire.
Un seul appel API est utilisé pour voir si un fichier a une balise.	

Catégorisation de vos données à l'aide de libellés AIP

Vous pouvez gérer les étiquettes AIP dans les fichiers que Cloud Data SENSE analyse si vous vous êtes abonné "Protection des informations Azure (AIP)". AIP vous permet de classer et de protéger les documents et les fichiers en appliquant des étiquettes au contenu. Data Sense vous permet d'afficher les étiquettes déjà

affectées aux fichiers, d'ajouter des étiquettes aux fichiers et de modifier les étiquettes lorsqu'une étiquette existe déjà.

Cloud Data SENSE prend en charge les libellés AIP dans les types de fichiers suivants : .DOC, .DOCX, .PDF, .PPTX, .XLS, XLSX.

- Vous ne pouvez pas modifier actuellement les étiquettes dans des fichiers de plus de 30 Mo. Pour OneDrive, SharePoint et Google Drive, la taille maximale de fichier est de 4 Mo.
- Si un fichier a un libellé qui n'existe plus dans AIP, Cloud Data SENSE le considère comme un fichier sans étiquette.
- Si vous avez déployé Data Sense dans une région gouvernementale ou dans un emplacement sur site sans accès à Internet (également connu sous le nom de site sombre), la fonctionnalité AIP label n'est pas disponible.

Intégration des libellés AIP dans votre espace de travail

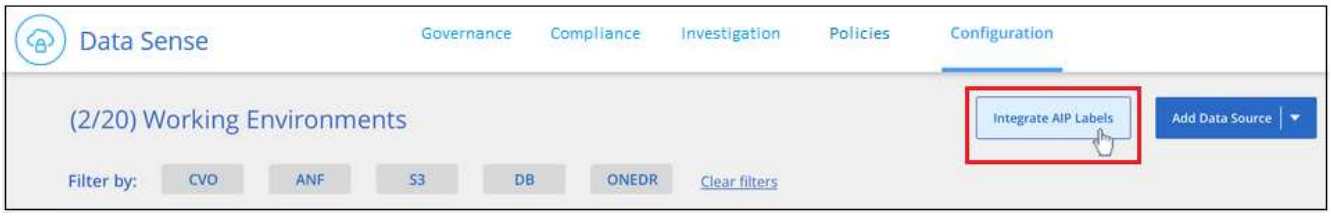
Avant de gérer les étiquettes AIP, vous devez intégrer la fonctionnalité AIP label dans Cloud Data Sense en vous connectant à votre compte Azure existant. Une fois activée, vous pouvez gérer les libellés AIP dans les fichiers pour tous "sources des données" Dans votre espace de travail BlueXP.

De formation

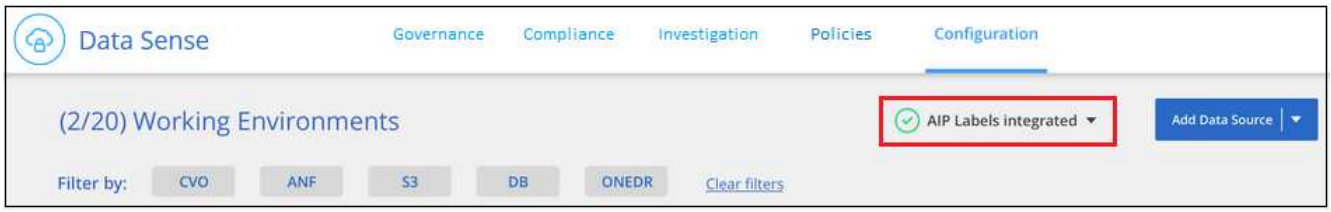
- Vous devez disposer d'un compte et d'une licence Azure information protection.
- Vous devez disposer des identifiants de connexion pour le compte Azure.
- Si vous prévoyez de modifier les étiquettes dans les fichiers qui résident dans les compartiments Amazon S3, assurez-vous que l'autorisation est requise `s3:PutObject` Est inclus dans le rôle IAM. Voir "Configuration du rôle IAM".

Étapes

1. Dans la page Configuration de la détection des données du cloud, cliquez sur **intégrer des étiquettes AIP**.



2. Dans la boîte de dialogue intégrer des libellés AIP, cliquez sur **connexion à Azure**.
3. Sur la page Microsoft qui s'affiche, sélectionnez le compte et saisissez les informations d'identification requises.
4. Revenez à l'onglet Cloud Data Sense et le message «*AIP Labels a été intégré avec succès au compte <Account_name>* ».
5. Cliquez sur **Fermer** et vous verrez le texte *AIP Labels Integrated* en haut de la page.



Résultat

Vous pouvez afficher et affecter des libellés AIP à partir du volet des résultats de la page Investigation. Vous pouvez également attribuer des libellés AIP aux fichiers à l'aide de stratégies.

Affichage des libellés AIP dans vos fichiers

Vous pouvez afficher le libellé AIP actuel attribué à un fichier.

Dans le volet Résultats de l'enquête de données, cliquez sur ⌄ pour que le fichier développe les détails des métadonnées du fichier.

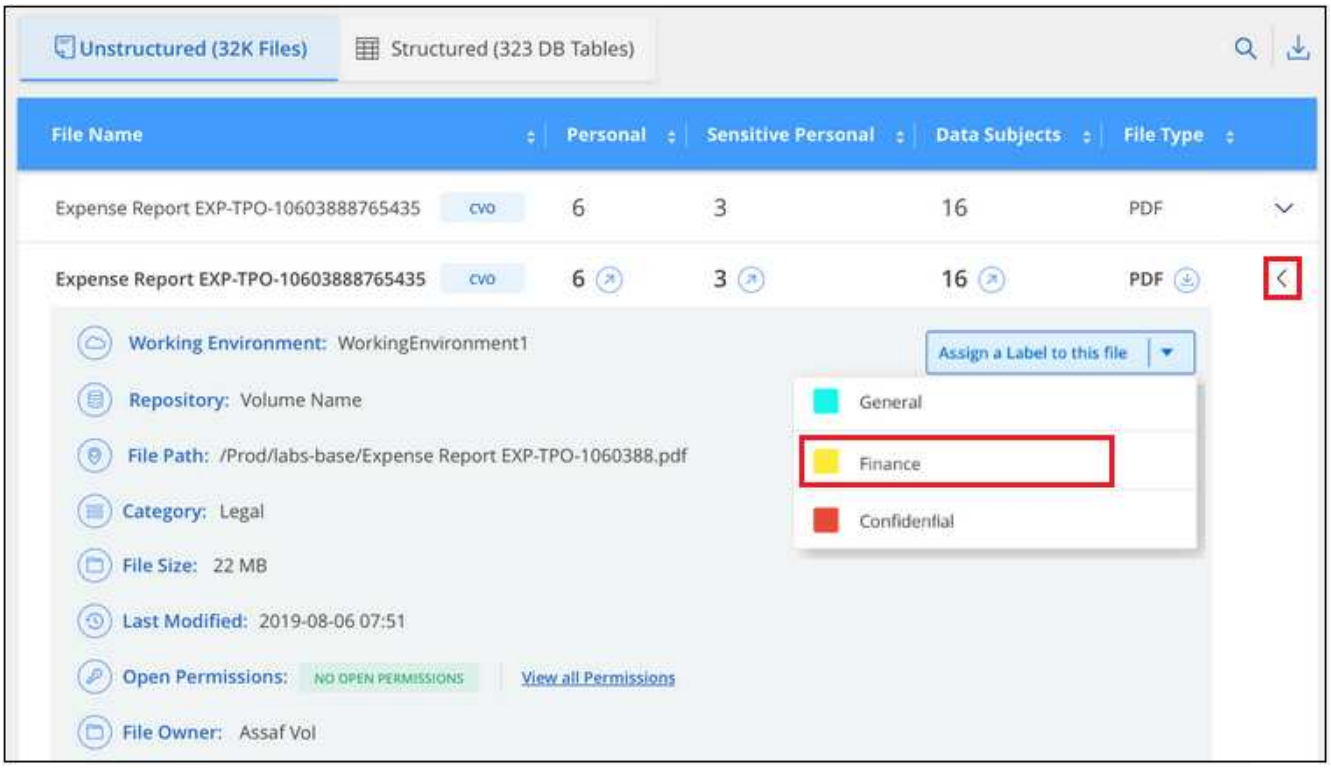
Attribution manuelle d'étiquettes AIP

Vous pouvez ajouter, modifier et supprimer des étiquettes AIP de vos fichiers à l'aide de Cloud Data Sense.

Procédez comme suit pour attribuer un libellé AIP à un seul fichier.

Étapes

1. Dans le volet Résultats de l'enquête de données, cliquez sur ⌄ pour que le fichier développe les détails des métadonnées du fichier.



2. Cliquez sur **attribuer un libellé à ce fichier**, puis sélectionnez le libellé.

   Le libellé apparaît dans les métadonnées du fichier.

Pour attribuer un libellé AIP à plusieurs fichiers :

Étapes

1. Dans le volet Résultats de l'enquête de données, sélectionnez le ou les fichiers que vous souhaitez étiqueter.

   - Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (☑ Volume_1).
   - Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (☑ File Name).

2. Dans la barre de boutons, cliquez sur **Label** et sélectionnez le libellé AIP :

L'étiquette AIP est ajoutée aux métadonnées pour tous les fichiers sélectionnés.

Attribution automatique d'étiquettes AIP à l'aide de stratégies

Vous pouvez affecter un libellé AIP à tous les fichiers qui répondent aux critères de la stratégie. Vous pouvez spécifier l'étiquette AIP lors de la création de la stratégie ou ajouter l'étiquette lors de la modification d'une stratégie.

Les étiquettes sont ajoutées ou mises à jour dans les fichiers en continu lors de l'analyse de vos fichiers par Cloud Data SENSE.

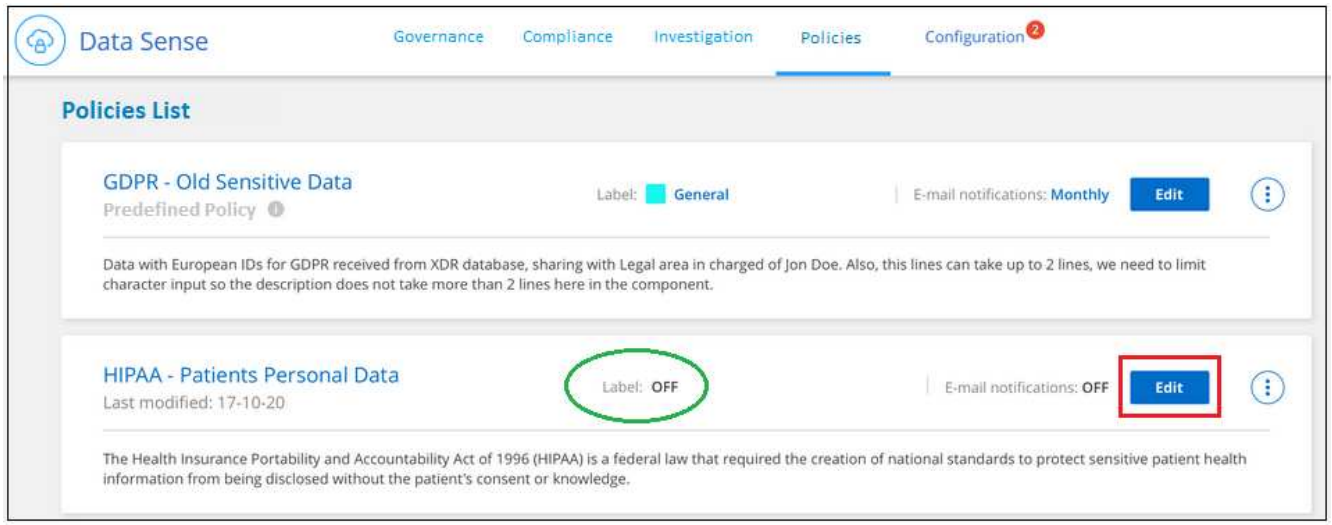
Selon qu'une étiquette est déjà appliquée à un fichier et le niveau de classification de l'étiquette, les actions suivantes sont prises lors de la modification d'une étiquette :

Si le fichier…	Alors…
N'a pas d'étiquette	L'étiquette est ajoutée
Possède une étiquette existante d'un niveau de classification inférieur	L'étiquette de niveau supérieur est ajoutée
Possède un libellé existant d'un niveau de classification supérieur	L'étiquette de niveau supérieur est conservée
Est affectée à une étiquette manuellement et par une police	L'étiquette de niveau supérieur est ajoutée
Deux étiquettes différentes sont attribuées par deux polices	L'étiquette de niveau supérieur est ajoutée

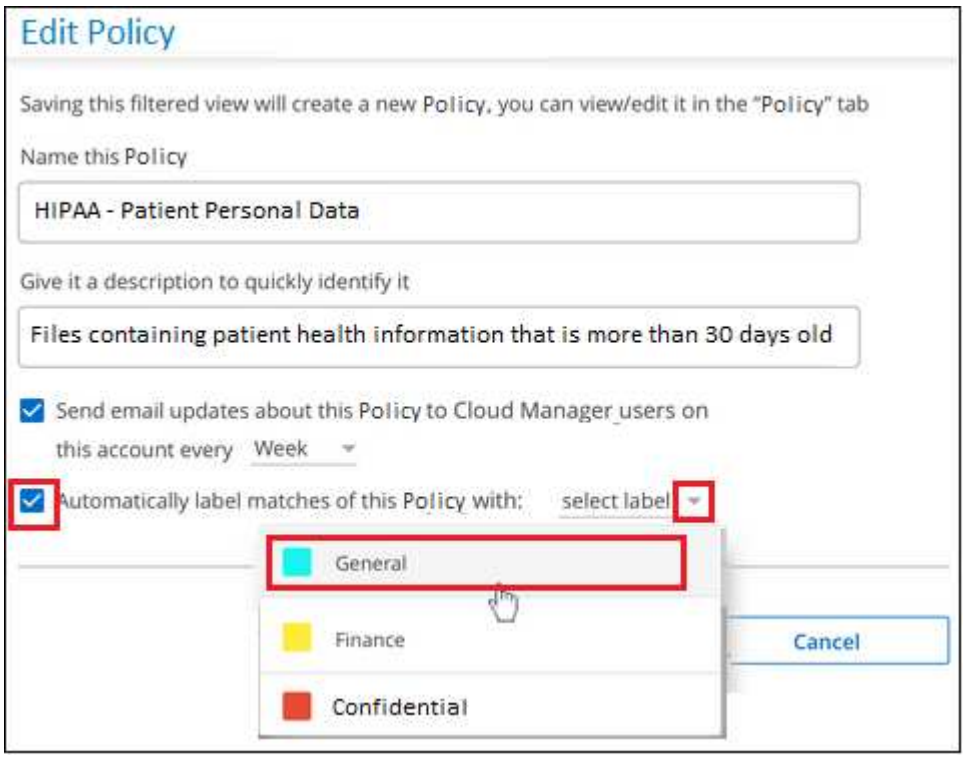
Procédez comme suit pour ajouter une étiquette AIP à une stratégie existante.

Étapes

1. Dans la page liste des stratégies, cliquez sur **Modifier** pour la stratégie dans laquelle vous souhaitez ajouter (ou modifier) l'étiquette AIP.



2. Dans la page Modifier la stratégie, cochez la case pour activer les libellés automatiques des fichiers qui correspondent aux paramètres de la stratégie, puis sélectionnez l'étiquette (par exemple, **général**).



3. Cliquez sur **Enregistrer la stratégie** et le libellé apparaît dans la description de la stratégie.

> Si une stratégie a été configurée avec un libellé, mais que le libellé a depuis été supprimé de l'AIP, le nom de l'étiquette est désactivé et l'étiquette n'est plus affectée.

Suppression de l'intégration AIP

Si vous ne souhaitez plus pouvoir gérer les étiquettes AIP dans des fichiers, vous pouvez supprimer le compte AIP de l'interface Cloud Data SENSE.

Notez qu'aucune modification n'est apportée aux étiquettes que vous avez ajoutées à l'aide de Data Sense. Les étiquettes qui existent dans les fichiers resteront telles qu'elles existent actuellement.

Étapes

1. Dans la page *Configuration*, cliquez sur **libellés AIP intégrés > Supprimer intégration**.

2. Cliquez sur **Supprimer l'intégration** dans la boîte de dialogue de confirmation.

Application de balises pour gérer vos fichiers numérisés

Vous pouvez ajouter une balise aux fichiers que vous souhaitez marquer pour un type de suivi. Par exemple, vous avez peut-être trouvé des fichiers en double et vous voulez en supprimer un, mais vous devez vérifier lequel supprimer. Vous pouvez ajouter une balise « vérifier pour supprimer » au fichier afin que vous sachiez que ce fichier nécessite une recherche et un certain type d'action future.

Data Sense vous permet d'afficher les balises affectées aux fichiers, d'ajouter ou de supprimer des balises des fichiers et de modifier le nom ou de supprimer une balise existante.

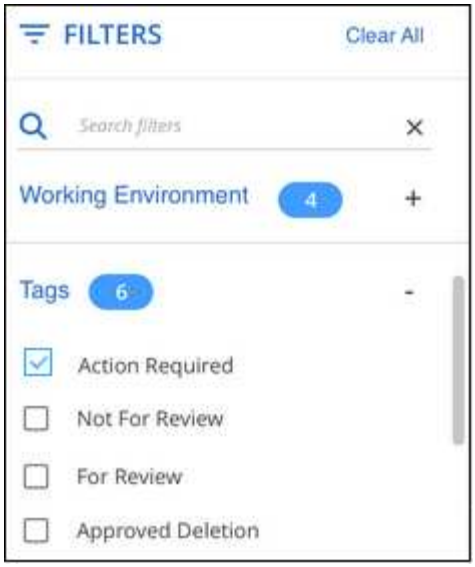
Notez que la balise n'est pas ajoutée au fichier de la même manière que les étiquettes AIP font partie des métadonnées du fichier. La balise vient d'être visible par les utilisateurs de BlueXP à l'aide de Cloud Data SENSE. Ainsi, vous pouvez voir si un fichier doit être supprimé ou vérifié pour un certain type de suivi.

> Les balises attribuées aux fichiers dans Cloud Data SENSE ne sont pas liées aux balises que vous pouvez ajouter aux ressources, telles que des volumes ou des instances de machines virtuelles. Des balises de détection de données sont appliquées au niveau du fichier.

Affichage des fichiers dont certaines balises sont appliquées

Vous pouvez afficher tous les fichiers auxquels des étiquettes spécifiques sont attribuées.

1. Cliquez sur l'onglet **Investigation** dans Cloud Data Sense.
2. Dans la page recherche de données, cliquez sur **balises** dans le volet filtres, puis sélectionnez les balises requises.



Le volet Résultats de l'enquête affiche tous les fichiers auxquels ces balises sont affectées.

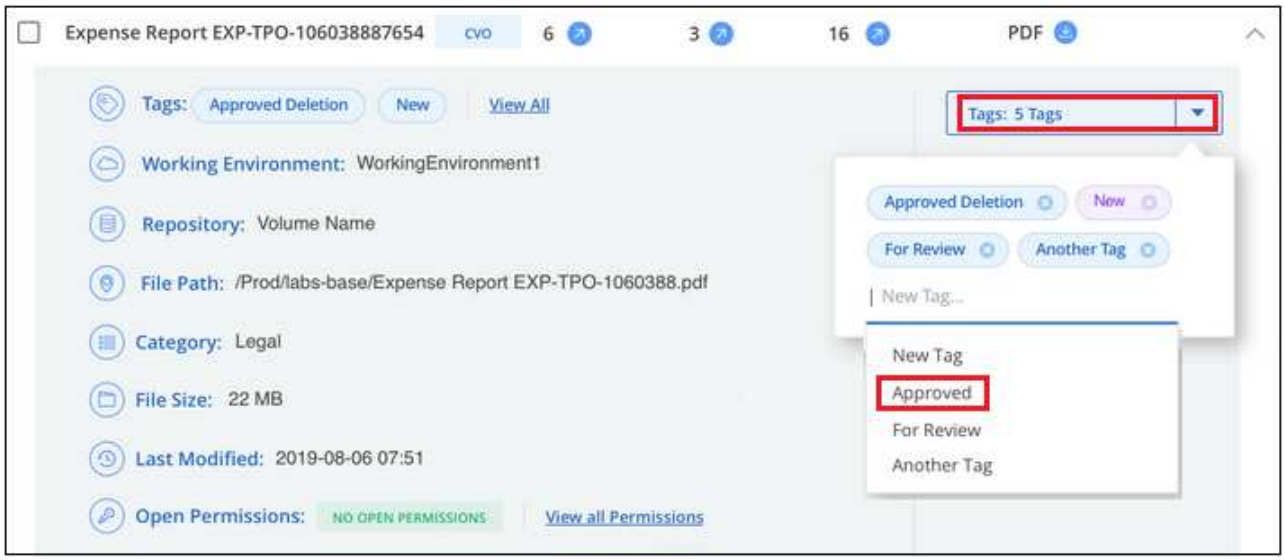
Attribution de balises aux fichiers

Vous pouvez ajouter des balises à un seul fichier ou à un groupe de fichiers.

Pour ajouter une balise à un seul fichier :

Étapes

1. Dans le volet Résultats de l'enquête de données, cliquez sur ⌄ pour que le fichier développe les détails des métadonnées du fichier.
2. Cliquez sur le champ **Tags** pour afficher les balises actuellement affectées.
3. Ajoutez la ou les balises :
   - Pour affecter une balise existante, cliquez dans le champ **Nouvelle balise…** et commencez à taper le nom de la balise. Lorsque la balise que vous cherchez s'affiche, sélectionnez-la et appuyez sur **entrée**.
   - Pour créer une nouvelle balise et l'affecter au fichier, cliquez dans le champ **Nouvelle balise…**, saisissez le nom de la nouvelle balise et appuyez sur **entrée**.



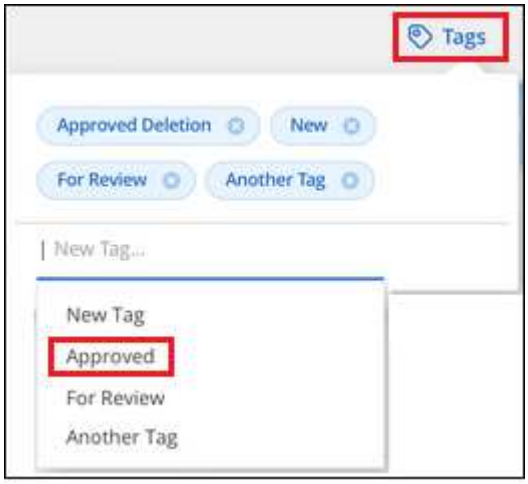
La balise s'affiche dans les métadonnées de fichier.

Pour ajouter une balise à plusieurs fichiers :

Étapes

1. Dans le volet Résultats de l'enquête de données, sélectionnez le ou les fichiers que vous souhaitez marquer.

   - Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (Volume_1).
   - Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (File Name).
2. Dans la barre de boutons, cliquez sur **Tags** et les balises actuellement affectées sont affichées.
3. Ajoutez la ou les balises :
   - Pour affecter une balise existante, cliquez dans le champ **Nouvelle balise…** et commencez à taper le nom de la balise. Lorsque la balise que vous cherchez s'affiche, sélectionnez-la et appuyez sur **entrée**.
   - Pour créer une nouvelle balise et l'affecter au fichier, cliquez dans le champ **Nouvelle balise…**, saisissez le nom de la nouvelle balise et appuyez sur **entrée**.



4. Approuver l'ajout des balises dans la boîte de dialogue de confirmation et les balises sont ajoutées aux métadonnées pour tous les fichiers sélectionnés.

Suppression de balises de fichiers

Vous pouvez supprimer une balise si vous n'avez plus besoin de l'utiliser.

Il vous suffit de cliquer sur **x** pour obtenir une balise existante.

Si vous avez sélectionné plusieurs fichiers, la balise est supprimée de tous les fichiers.

Affectation d'utilisateurs pour gérer certains fichiers

Vous pouvez affecter un utilisateur BlueXP à un fichier spécifique ou à plusieurs fichiers, de sorte que personne puisse être responsable des actions de suivi qui doivent être effectuées sur le fichier. Cette fonctionnalité est souvent utilisée avec la fonction pour ajouter des balises d'état personnalisées à un fichier.

Par exemple, vous pouvez avoir un fichier contenant certaines données personnelles qui autorise un trop grand nombre d'utilisateurs à accéder en lecture et en écriture (autorisations ouvertes). Vous pouvez donc attribuer l'étiquette d'état « Modifier les autorisations » et attribuer ce fichier à l'utilisateur « Joan Smith » afin qu'il puisse décider comment résoudre le problème. Lorsqu'ils ont résolu le problème, ils peuvent changer l'étiquette d'état en « terminé ».

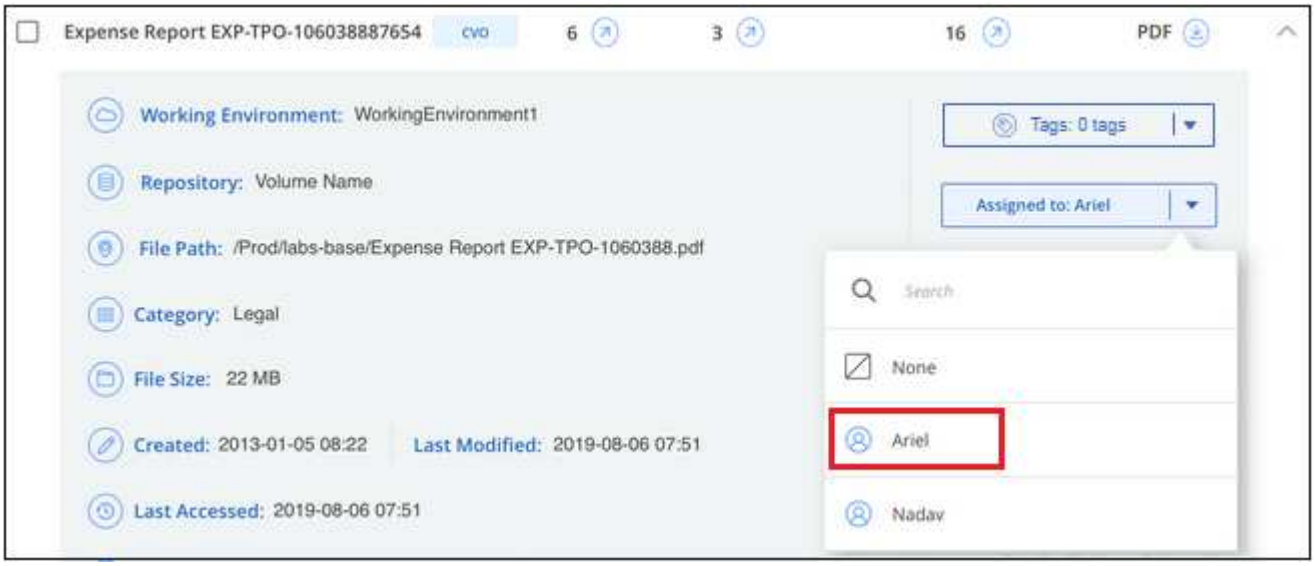
Notez que le nom d'utilisateur n'est pas ajouté au fichier dans le cadre des métadonnées du fichier. Il est simplement visible par les utilisateurs de BlueXP lors de l'utilisation de Cloud Data Sense.

Un nouveau filtre dans la page Investigation vous permet d'afficher facilement tous les fichiers qui ont la même personne dans le champ « assigné à ».

Pour affecter un utilisateur à un seul fichier :

Étapes

1. Dans le volet Résultats de l'enquête de données, cliquez sur ⌄ pour que le fichier développe les détails des métadonnées du fichier.
2. Cliquez sur le champ **affecté à** et sélectionnez le nom d'utilisateur.



Le nom d'utilisateur apparaît dans les métadonnées de fichier.

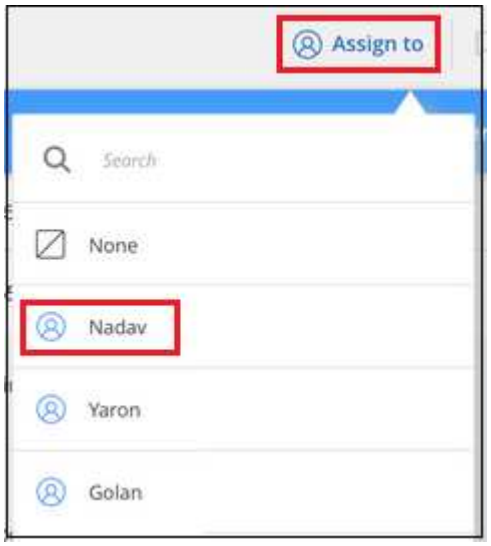
Pour affecter un utilisateur à plusieurs fichiers :

Étapes

1. Dans le volet Résultats de l'enquête de données, sélectionnez le ou les fichiers que vous souhaitez attribuer à un utilisateur.

   - Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (Volume_1).
   - Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (File Name).

2. Dans la barre de boutons, cliquez sur **affecter à** et sélectionnez le nom d'utilisateur :



   L'utilisateur est ajouté aux métadonnées pour tous les fichiers sélectionnés.

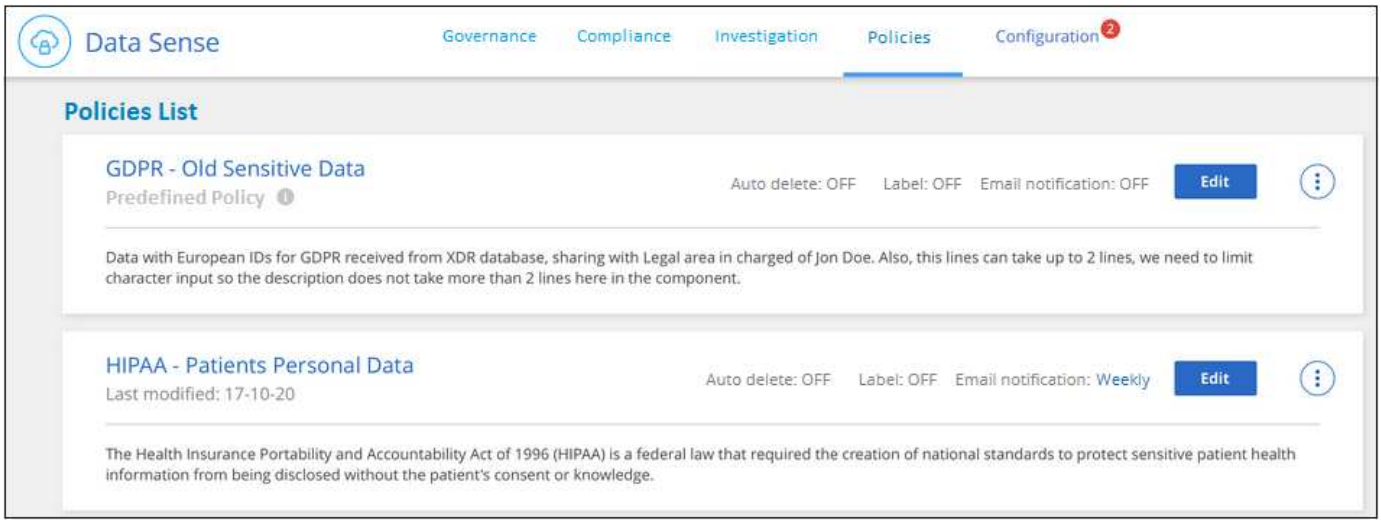
Contrôler vos données à l'aide de règles

Les stratégies sont comme une liste de favoris de filtres personnalisés qui fournissent des résultats de recherche dans la page Investigation pour les requêtes de conformité les plus fréquemment demandées. Cloud Data Sense fournit un ensemble de règles prédéfinies en fonction des demandes courantes des clients. Vous pouvez créer des stratégies personnalisées fournissant des résultats de recherches spécifiques à votre organisation.

Les règles offrent les fonctionnalités suivantes :

- Stratégies prédéfinies De NetApp en fonction des demandes des utilisateurs
- Possibilité de créer vos propres règles personnalisées
- Lancez la page Investigation avec les résultats de vos polices en un seul clic
- Envoyez des alertes par e-mail à des utilisateurs BlueXP lorsque certaines stratégies critiques renvoient des résultats afin que vous puissiez obtenir des notifications pour protéger vos données
- Attribuez automatiquement des étiquettes AIP (Azure information protection) à tous les fichiers qui correspondent aux critères définis dans une stratégie
- Supprimez des fichiers automatiquement (une fois par jour) lorsque certaines stratégies renvoient des résultats pour protéger vos données automatiquement

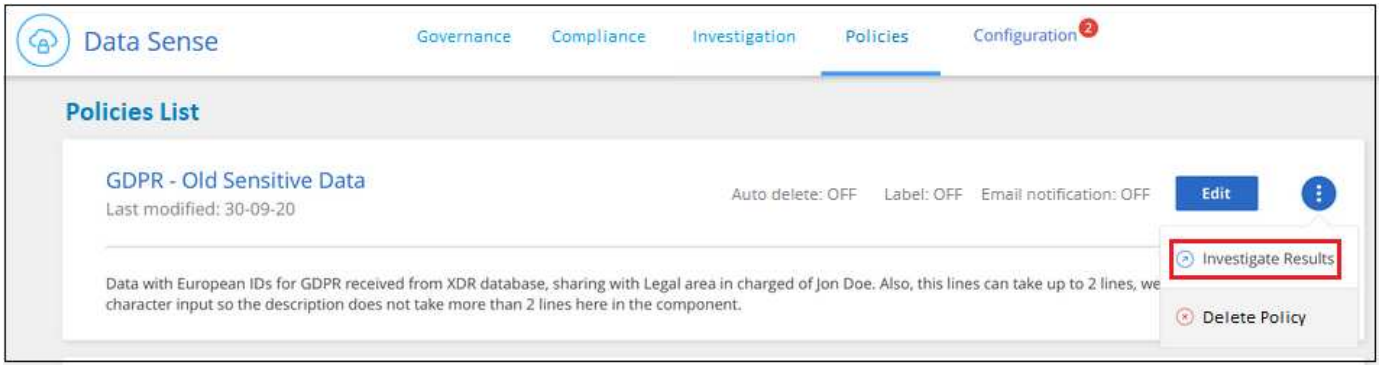
L'onglet **Policies** du tableau de bord de conformité répertorie toutes les stratégies prédéfinies et personnalisées disponibles sur cette instance de Cloud Data Sense.



De plus, les polices apparaissent dans la liste des filtres de la page Investigation.

Affichage des résultats de la police dans la page Investigation

Pour afficher les résultats d'une police dans la page Investigation, cliquez sur le bouton Pour une stratégie spécifique, puis sélectionnez **étudier les résultats**.



Création de stratégies personnalisées

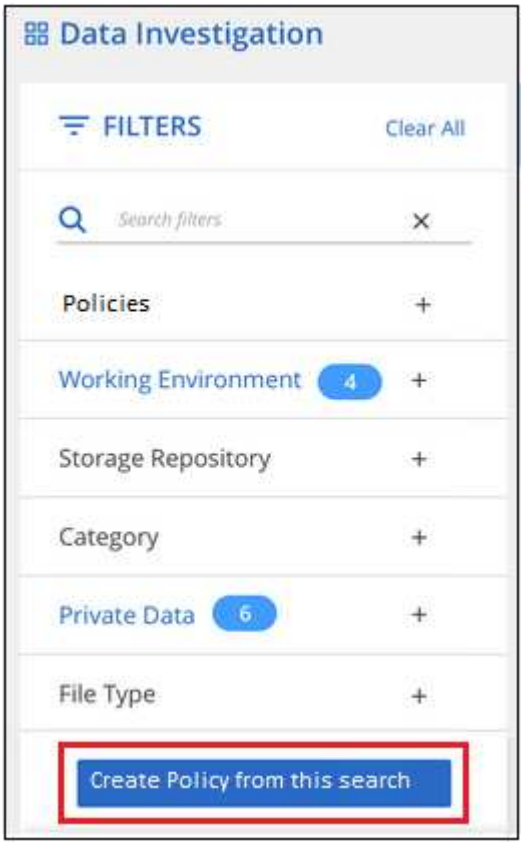
Vous pouvez créer vos propres stratégies personnalisées qui fournissent des résultats pour les recherches spécifiques à votre organisation. Les résultats sont renvoyés pour tous les fichiers et répertoires (partages et

dossiers) qui correspondent aux critères de recherche.

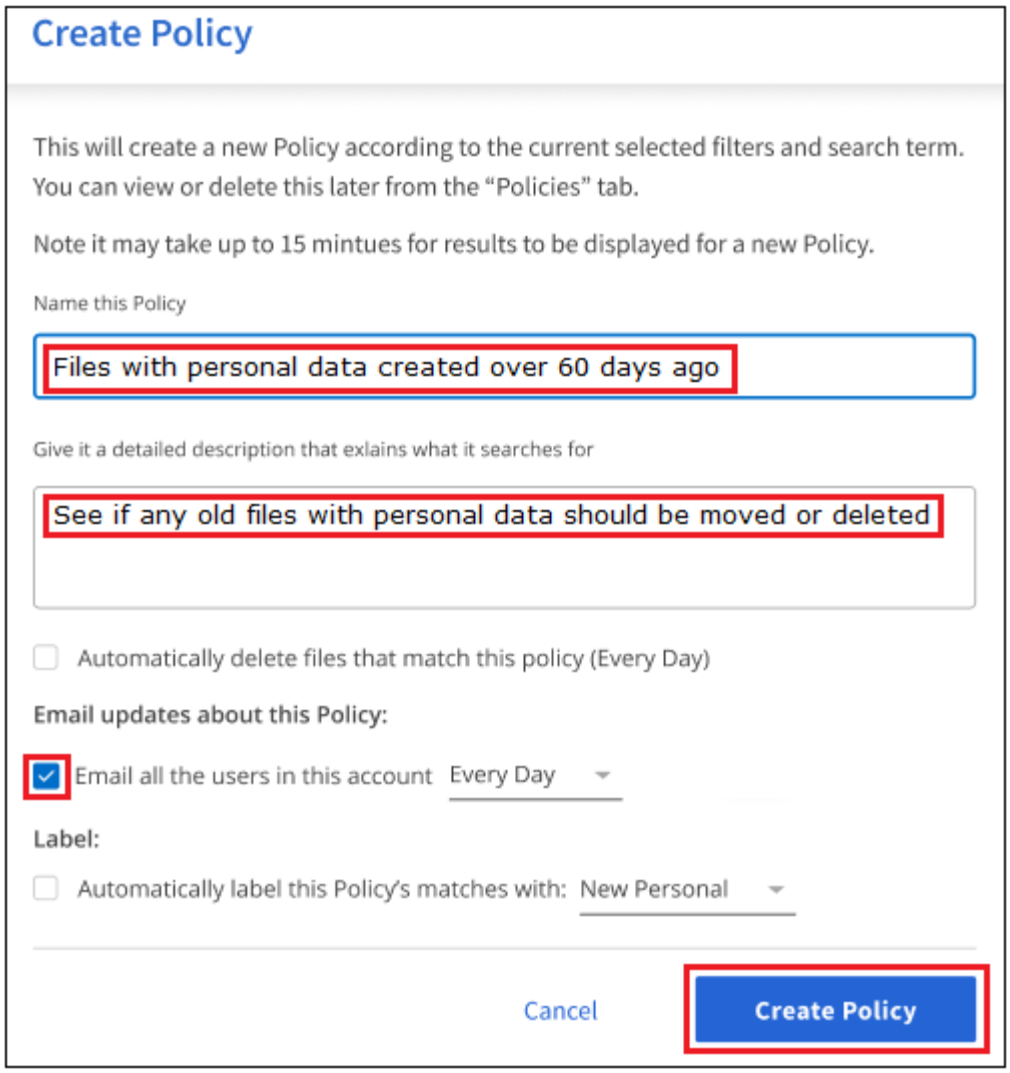
Notez que les actions de suppression de données et d'attribution de libellés AIP basés sur les résultats de la stratégie sont uniquement valides pour les fichiers. Les répertoires qui correspondent aux critères de recherche ne peuvent pas être supprimés automatiquement ou affectés à des libellés AIP.

Étapes

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



3. Nommez la stratégie et sélectionnez d'autres actions pouvant être effectuées par la stratégie :
   a. Entrez un nom et une description uniques.
   b. Si vous le souhaitez, cochez la case pour supprimer automatiquement les fichiers qui correspondent aux paramètres de la stratégie. En savoir plus sur "suppression de fichiers source à l'aide d'une stratégie".
   c. Si vous voulez envoyer des e-mails de notification aux utilisateurs BlueXP de votre compte, cochez la case correspondante et choisissez l'intervalle d'envoi de l'e-mail. En savoir plus sur "envoi d'alertes par e-mail en fonction des résultats de règles".
   d. Si vous le souhaitez, cochez la case pour attribuer automatiquement des libellés AIP aux fichiers qui correspondent aux paramètres de la stratégie, puis sélectionnez le libellé. (Uniquement si vous avez déjà intégré des étiquettes AIP. En savoir plus sur "Libellés AIP".)
   e. Cliquez sur **Créer une stratégie**.



Résultat

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

Envoi d'alertes par e-mail lorsque des données non conformes sont trouvées

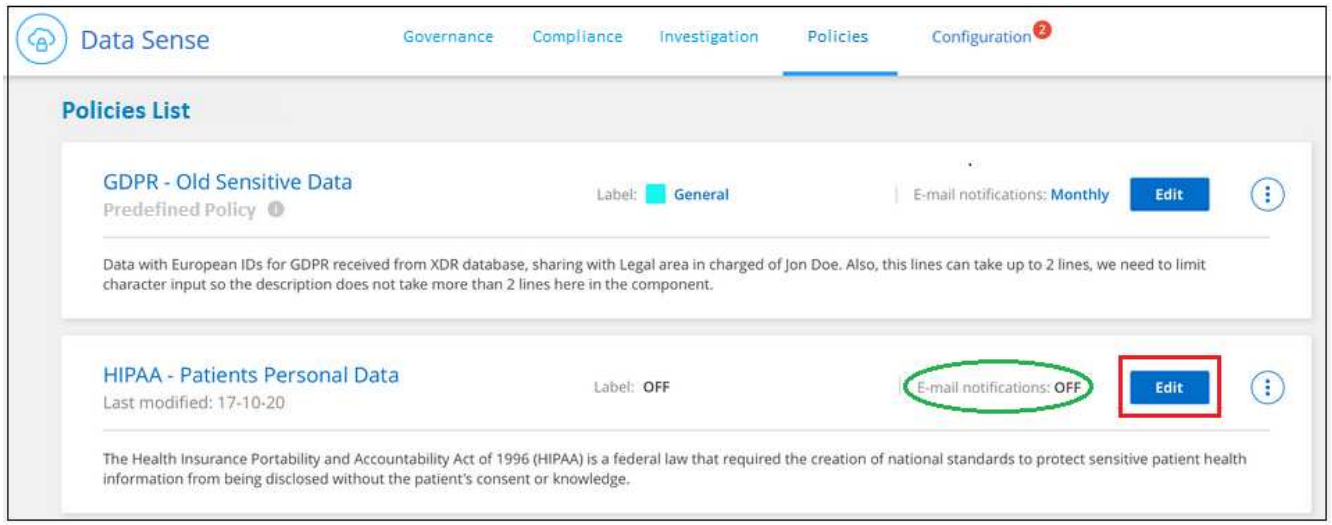
Cloud Data SENSE peut envoyer des alertes par e-mail à des utilisateurs BlueXP de votre compte lorsque certaines stratégies critiques renvoient des résultats afin que vous puissiez obtenir des notifications pour protéger vos données. Vous pouvez choisir d'envoyer les notifications par e-mail tous les jours, toutes les semaines ou tous les mois.

Vous pouvez configurer ce paramètre lors de la création de la stratégie ou lors de la modification d'une stratégie.

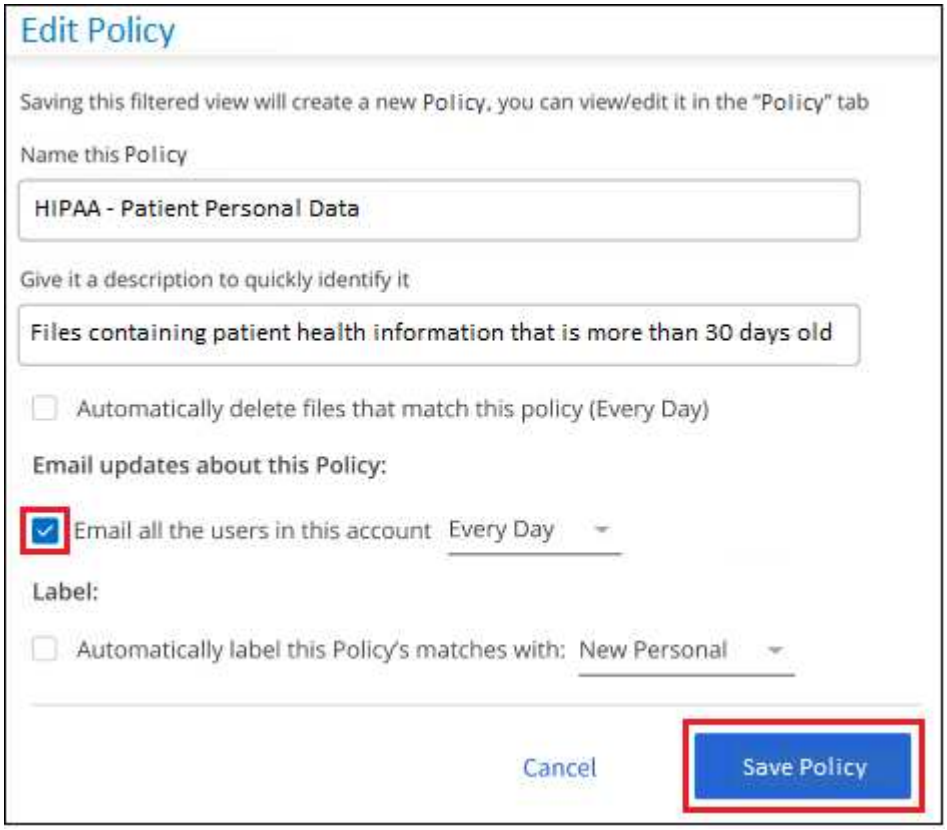
Procédez comme suit pour ajouter des mises à jour par e-mail à une stratégie existante.

Étapes

1. Dans la page liste des stratégies, cliquez sur **Modifier** pour la stratégie dans laquelle vous souhaitez ajouter (ou modifier) le paramètre de messagerie.



2. Dans la page Modifier la stratégie :
   a. Cochez la case « Envoyer tous les utilisateurs dans ce compte » si vous souhaitez envoyer des e-mails de notification aux utilisateurs de votre compte BlueXP, puis choisissez l'intervalle d'envoi de l'e-mail (par exemple, **tous les jours**).



3. Cliquez sur **Enregistrer la stratégie** et l'intervalle auquel l'e-mail est envoyé apparaît dans la description de la stratégie.

Résultat

Le premier e-mail est envoyé dès maintenant s'il y a des résultats de la politique - mais seulement si des fichiers répondent aux critères de police. Aucune information personnelle n'est envoyée dans les e-mails de notification. L'e-mail indique qu'il existe des fichiers qui correspondent aux critères de la police et qu'il fournit un lien vers les résultats de la police.

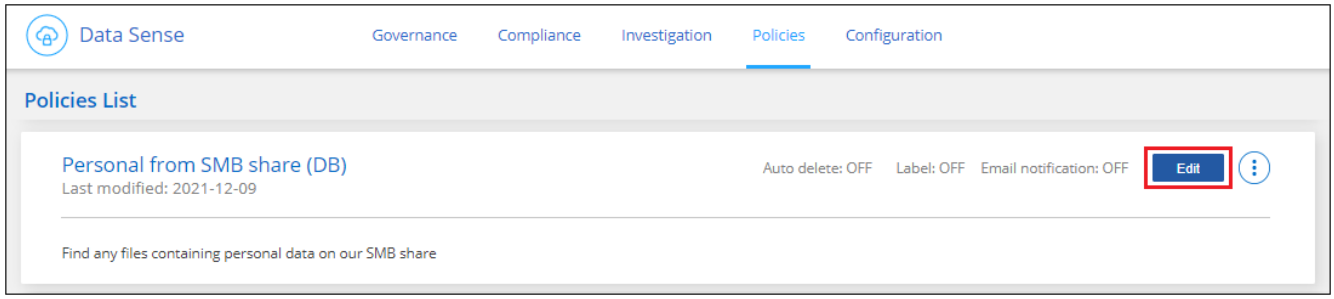
Modification de stratégies

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

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

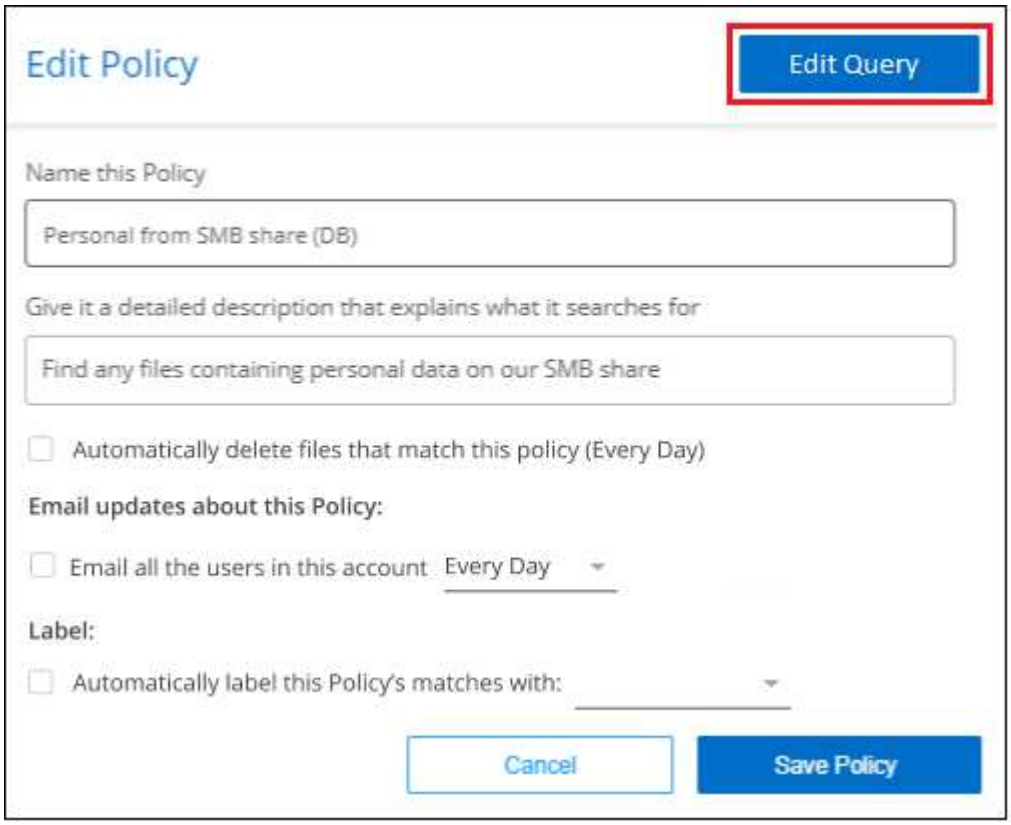
Étapes

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

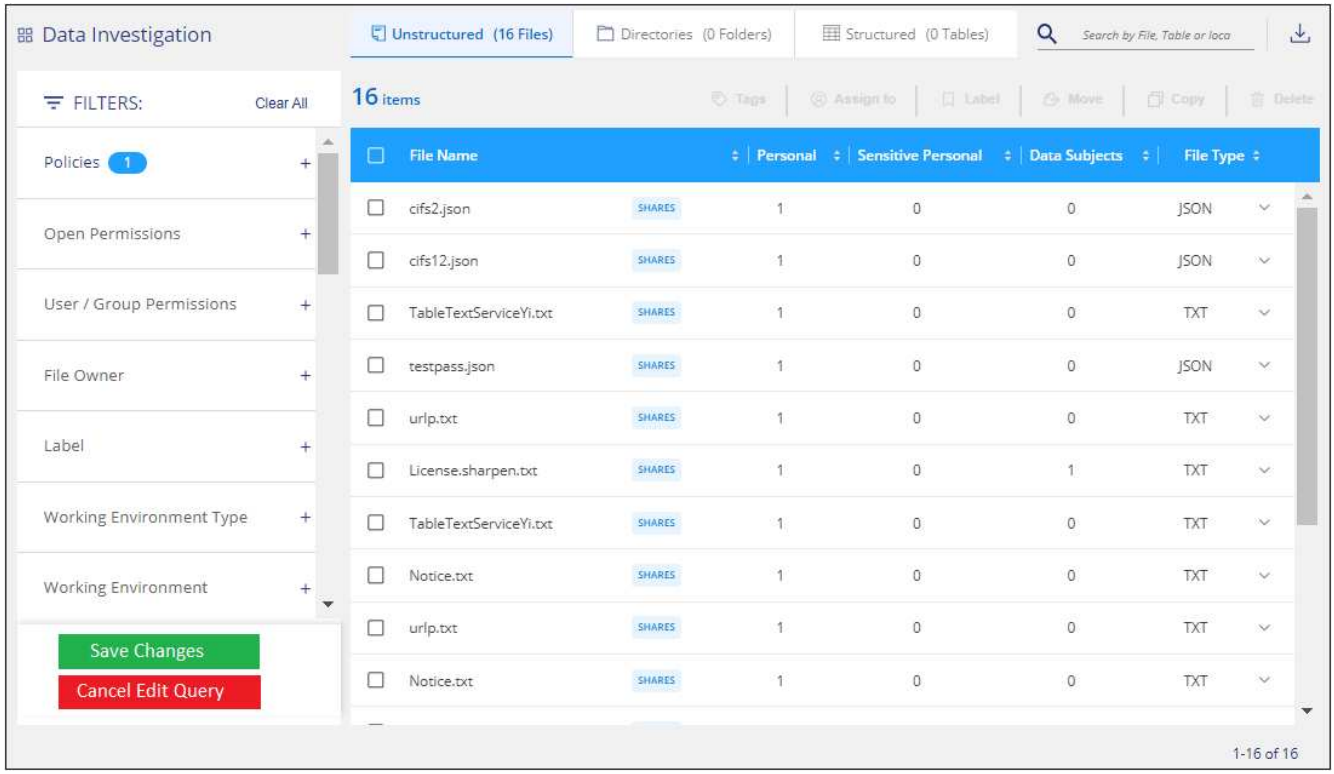


2. Si vous souhaitez simplement modifier les éléments de cette page (le Nom, la Description, si les notifications par e-mail sont envoyées et si des étiquettes AIP sont ajoutées), effectuez la modification et cliquez sur **Enregistrer la stratégie**.

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



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



Résultat

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

Suppression de polices

Vous pouvez supprimer toute stratégie personnalisée que vous avez créée si vous n'en avez plus besoin. Vous ne pouvez supprimer aucune des stratégies prédéfinies.

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

Liste des stratégies prédéfinies

Cloud Data Sense fournit plusieurs règles définies par le système :

Nom	Description	Logique
S3 : données privées exposées publiquement	Objets S3 contenant des informations personnelles ou sensibles, avec un accès public en lecture ouvert.	S3 public ET contient des informations personnelles ou sensibles
PCI DSS : données obsolètes supérieure à 30 jours	Fichiers contenant des informations de carte de crédit, modifié pour la dernière fois il y a plus de 30 jours.	Contient la carte de crédit ET la dernière modification sur 30 jours
HIPAA : données obsolètes sur 30 jours	Fichiers contenant des informations de santé, modifié pour la dernière fois il y a plus de 30 jours.	Contient des données de santé (définies de la même manière que dans le rapport HIPAA) ET modifiées pour la dernière fois sur 30 jours

Nom	Description	Logique
Les données privées ont déjà dépassé les 7 ans	Fichiers contenant des données personnelles ou sensibles, modifié pour la dernière fois il y a plus de 7 ans.	Fichiers contenant des données personnelles ou sensibles, modifié pour la dernière fois il y a plus de 7 ans
RGPD - citoyens européens	Dossiers contenant plus de 5 identificateurs de citoyens d'un pays de l'UE ou tables de BD contenant des identificateurs de citoyens d'un pays de l'UE.	Dossiers contenant plus de 5 identificateurs d'un (un) citoyen de l'UE ou de tables de données contenant des lignes contenant plus de 15% des colonnes avec des identificateurs d'UE d'un pays. (Tout identifiant national des pays européens. N'inclut pas le Brésil, la Californie, le SSN des États-Unis, Israël et l'Afrique du Sud)
CCPA - résidents de Californie	Fichiers contenant plus de 10 identificateurs de permis de conduire californiens ou tables de BD contenant cet identifiant.	Fichiers contenant plus de 10 identificateurs de permis de conduire californiens OU tables de BD contenant la licence du conducteur California
Noms des sujets de données - risque élevé	Fichiers avec plus de 50 noms de sujet de données.	Fichiers avec plus de 50 noms de sujet de données
Adresses e-mail - risque élevé	Fichiers contenant plus de 50 adresses électroniques ou colonnes DB contenant plus de 50 % de leurs lignes contenant des adresses électroniques	Fichiers contenant plus de 50 adresses électroniques ou colonnes DB contenant plus de 50 % de leurs lignes contenant des adresses électroniques
Données personnelles - risque élevé	Fichiers contenant plus de 20 identificateurs de données personnelles, ou colonnes de bases de données contenant plus de 50 % de leurs lignes contenant des identificateurs de données personnelles.	Fichiers avec plus de 20 colonnes personnelles ou DB avec plus de 50 % de leurs lignes contenant des colonnes personnelles
Données personnelles sensibles - risque élevé	Fichiers contenant plus de 20 identificateurs de données personnelles sensibles, ou colonnes de bases de données contenant plus de 50 % de leurs lignes contenant des données personnelles sensibles.	Les fichiers contenant plus de 20 colonnes personnelles sensibles ou DB contenant plus de 50 % de leurs lignes contenant des données personnelles sensibles

La gestion de vos données privées

Avec Cloud Data Sense, vous pouvez gérer vos données privées de plusieurs façons. Certaines fonctionnalités facilitent la préparation de la migration des données, tandis que d'autres vous permettent de modifier ces dernières.

- Vous pouvez copier des fichiers vers un partage NFS de destination si vous souhaitez effectuer une copie de certaines données et les déplacer vers un autre emplacement NFS.
- Vous pouvez cloner un volume ONTAP sur un nouveau volume, tout en incluant uniquement les fichiers sélectionnés du volume source dans le nouveau volume cloné. Ceci est utile dans les situations où vous migrez des données et que vous souhaitez exclure certains fichiers du volume d'origine.

- Vous pouvez copier et synchroniser des fichiers d'un référentiel source vers un répertoire dans un emplacement de destination spécifique. Cela est utile dans les situations où vous migrez des données d'un système source vers un autre alors qu'il y a encore une activité finale sur les fichiers source.
- Vous pouvez déplacer les fichiers source que Data Sense analyse vers n'importe quel partage NFS.
- Vous pouvez supprimer des fichiers qui semblent non sécurisés ou trop risqués pour l'éviter dans votre système de stockage, ou que vous avez identifiés comme doublons.

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

Copie des fichiers source

Vous pouvez copier tous les fichiers source que Data Sense est en cours d'analyse. Il existe trois types d'opérations de copie en fonction de l'objectif que vous essayez d'effectuer :

- **Copier des fichiers** de volumes ou de sources de données identiques ou différentes vers un partage NFS de destination.

  Cette fonction est utile pour effectuer une copie de certaines données et les déplacer vers un autre emplacement NFS.

- **Cloner un volume ONTAP** sur un nouveau volume dans le même agrégat, mais inclure uniquement les fichiers sélectionnés du volume source dans le nouveau volume cloné.

  Cette fonction est utile lorsque vous migrez des données et que vous souhaitez exclure certains fichiers du volume d'origine. Cette action utilise le "NetApp FlexClone ®" fonctionnalité permettant de dupliquer rapidement le volume, puis de supprimer les fichiers que vous avez sélectionnés.

- **Copier et synchroniser des fichiers** à partir d'un référentiel source unique (volume ONTAP, compartiment S3, partage NFS, etc.) vers un répertoire dans un emplacement de destination spécifique (cible).

  Cette fonction est utile lorsque vous migrez des données d'un système source vers un autre. Après la copie initiale, le service synchronise toutes les données modifiées en fonction de la planification que vous avez définie. Cette action utilise le "NetApp Cloud Sync" fonctionnalité permettant de copier et de synchroniser les données d'une source vers une cible.

Copie des fichiers source vers un partage NFS

Vous pouvez copier les fichiers source que Data Sense analyse vers n'importe quel partage NFS. Il n'est pas nécessaire d'intégrer le partage NFS avec Data Sense, il vous suffit de connaître le nom du partage NFS où tous les fichiers sélectionnés seront copiés dans le format `<host_name>:/<share_path>`.

> Vous ne pouvez pas copier les fichiers qui résident dans les bases de données.

De formation

- Vous devez avoir le rôle Administrateur de compte ou Administrateur d'espace de travail pour copier des

fichiers.

- La copie de fichiers requiert que le partage NFS de destination autorise l'accès à partir de l'instance Data Sense.
- Vous pouvez copier un maximum de 100,000 fichiers à la fois.

Étapes

1. Dans le volet Résultats de l'enquête de données, sélectionnez le ou les fichiers que vous souhaitez copier, puis cliquez sur **Copier**.

   - Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (Volume_1).
   - Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (File Name).
   - Pour sélectionner tous les fichiers sur toutes les pages, cochez la case dans la ligne de titre (File Name), puis dans le message contextuel All **20** Items on this page selected Select all Items in list (63K Items), Cliquez sur **Sélectionner tous les éléments de la liste (xxx items)**.

2. Dans la boîte de dialogue *Copy Files*, sélectionnez l'onglet **Regular Copy**.

3. Entrez le nom du partage NFS dans lequel tous les fichiers sélectionnés seront copiés au format `<host_name>:/<share_path>`, Puis cliquez sur **copie**.

   Une boîte de dialogue apparaît avec l'état de l'opération de copie.

Vous pouvez afficher la progression de l'opération de copie dans "Volet État des actions".

Notez que vous pouvez également copier un fichier individuel lors de l'affichage des détails de métadonnées d'un fichier. Cliquez simplement sur **Copier fichier**.

Clonage de données de volume sur un nouveau volume

Vous pouvez cloner un volume ONTAP existant que l'analyse des données est en cours à l'aide de la fonctionnalité NetApp *FlexClone*. Cela vous permet de dupliquer le volume rapidement tout en incluant uniquement les fichiers que vous avez sélectionnés. Cela est utile si vous migrez des données et que vous souhaitez exclure certains fichiers du volume d'origine, ou si vous souhaitez créer une copie d'un volume pour le test.

Le nouveau volume est créé dans le même agrégat que le volume source. Assurez-vous de disposer d'un espace suffisant pour ce nouveau volume dans l'agrégat avant de commencer cette tâche. Contactez votre administrateur du stockage si nécessaire.

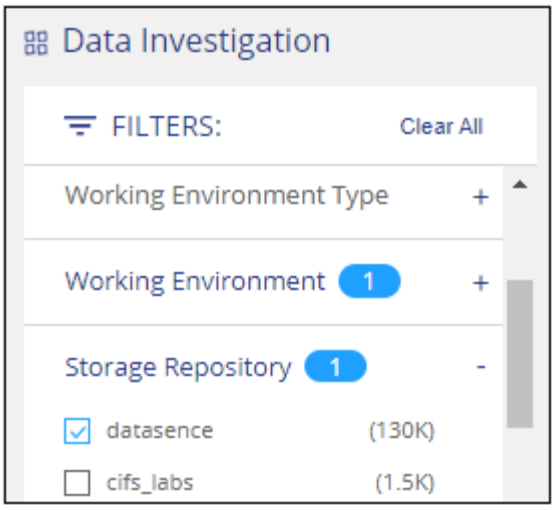
Remarque : les volumes FlexGroup ne peuvent pas être clonés, car ils ne sont pas pris en charge par FlexClone.

De formation

- Vous devez avoir le rôle Administrateur de compte ou Administrateur d'espace de travail pour copier des fichiers.
- Tous les fichiers sélectionnés doivent se trouver dans le même volume et le volume doit être en ligne.
- Le volume doit correspondre à un système Cloud Volumes ONTAP ou ONTAP sur site. Aucune autre source de données n'est actuellement prise en charge.
- La licence FlexClone doit être installée sur le cluster. Cette licence est installée par défaut sur les systèmes Cloud Volumes ONTAP.

Étapes

1. Dans le volet enquête de données, créez un filtre en sélectionnant un seul **Environnement de travail** et un seul **référentiel de stockage** pour vous assurer que tous les fichiers proviennent du même volume ONTAP.

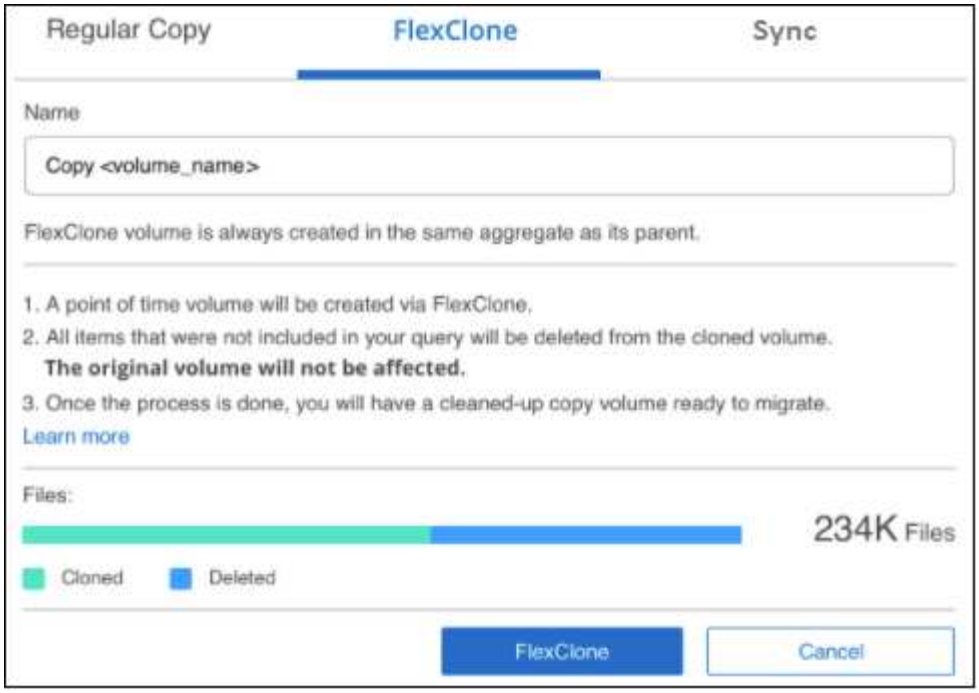


Appliquez tous les autres filtres afin que vous ne voyez que les fichiers que vous souhaitez cloner vers le nouveau volume.

2. Dans le volet Résultats de l'enquête, sélectionnez les fichiers à cloner et cliquez sur **Copier**.

- Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (Volume_1).
- Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (File Name).
- Pour sélectionner tous les fichiers sur toutes les pages, cochez la case dans la ligne de titre (File Name), puis dans le message contextuel All **20** Items on this page selected Select all Items in list (63K Items), Cliquez sur **Sélectionner tous les éléments de la liste (xxx items)**.

3. Dans la boîte de dialogue *Copy Files*, sélectionnez l'onglet **FlexClone**. Cette page affiche le nombre total de fichiers qui seront clonés à partir du volume (fichiers que vous avez sélectionnés) et le nombre de fichiers qui ne sont pas inclus/supprimés (fichiers que vous n'avez pas sélectionnés) du volume cloné.



4. Entrez le nom du nouveau volume et cliquez sur **FlexClone**.

   Une boîte de dialogue affichant l'état de l'opération de clonage s'affiche.

Résultat

Le nouveau volume cloné est créé dans le même agrégat que le volume source.

Vous pouvez afficher la progression de l'opération de clonage dans "Volet État des actions".

Si vous avez initialement sélectionné **mapper tous les volumes** ou **mapper et classer tous les volumes** lorsque vous avez activé Data Sense pour l'environnement de travail où réside le volume source, Data Sense va analyser le nouveau volume cloné automatiquement. Si vous n'avez pas utilisé l'une ou l'autre de ces sélections au départ, vous devrez effectuer une acquisition pour ce nouveau volume "activer la numérisation sur le volume manuellement".

Copie et synchronisation des fichiers source sur un système cible

Vous pouvez copier les fichiers source que Data Sense analyse depuis n'importe quelle source de données non structurées prise en charge vers un répertoire dans un emplacement cible spécifique ("Emplacements cibles pris en charge par Cloud Sync"). Après la copie initiale, toutes les données modifiées dans les fichiers sont synchronisées en fonction du calendrier que vous configurez.

Cette fonction est utile lorsque vous migrez des données d'un système source vers un autre. Cette action utilise le "NetApp Cloud Sync" fonctionnalité permettant de copier et de synchroniser les données d'une source vers une cible.

> Vous ne pouvez pas copier et synchroniser les fichiers qui résident dans les bases de données, les comptes OneDrive ou les comptes SharePoint.

De formation

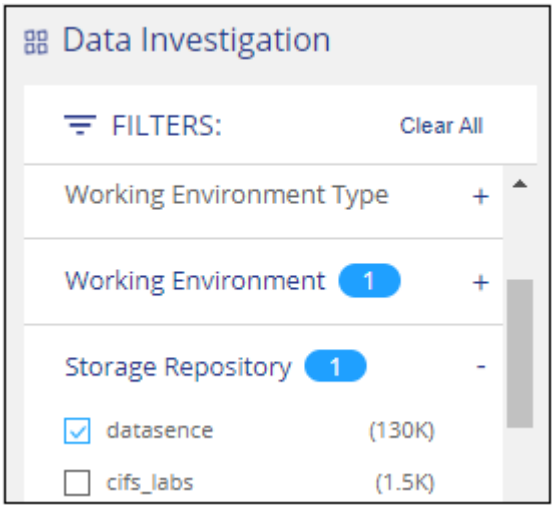
- Vous devez disposer du rôle Administrateur de compte ou Administrateur d'espace de travail pour copier et synchroniser les fichiers.

- Tous les fichiers sélectionnés doivent se trouver dans le même référentiel source (volume ONTAP, compartiment S3, partage NFS ou CIFS, etc.).
- Vous devrez activer le service Cloud Sync et configurer au moins un courtier de données qui peut être utilisé pour transférer des fichiers entre les systèmes source et cible. Vérifiez les exigences Cloud Sync en commençant par le "Description de Quick Start".

  Notez que le service Cloud Sync facture séparément les services de synchronisation et entraîne des frais de ressources si vous déployez le courtier en données dans le cloud.

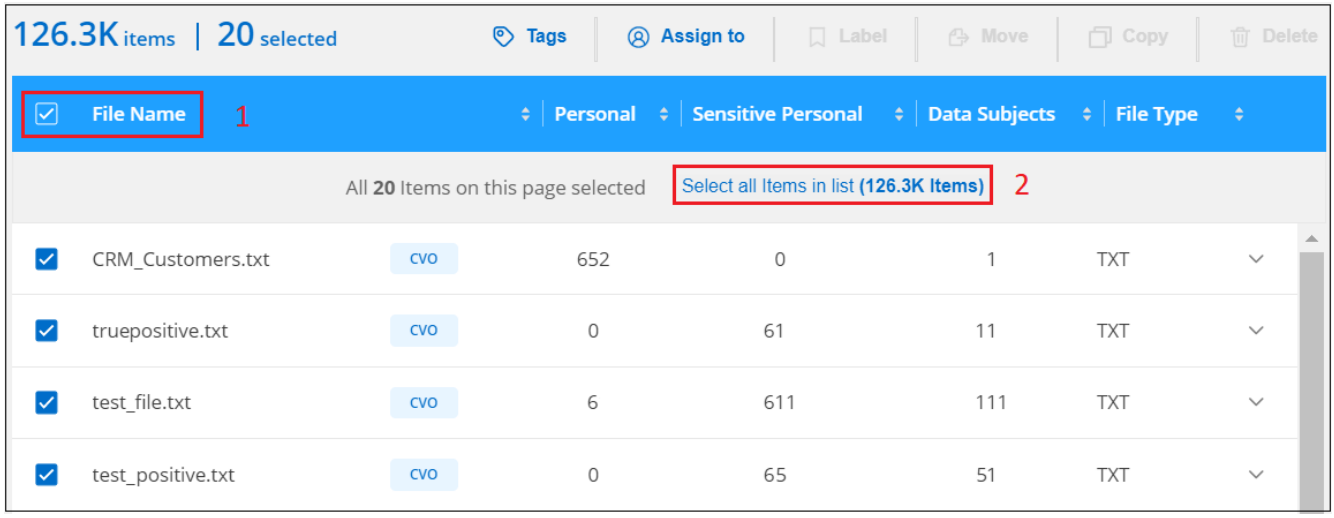
Étapes

1. Dans le volet investigation de données, créez un filtre en sélectionnant un seul **Environnement de travail** et un seul **référentiel de stockage** pour vous assurer que tous les fichiers proviennent du même référentiel.

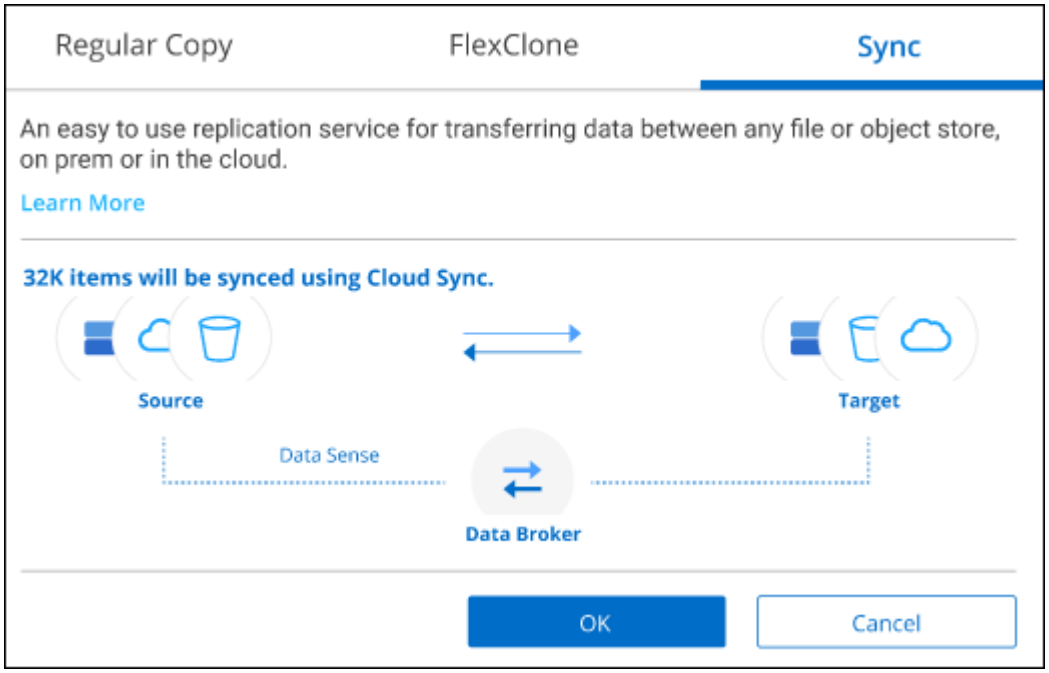


   Appliquez tous les autres filtres de sorte que vous ne voyez que les fichiers que vous voulez copier et synchroniser vers le système de destination.

2. Dans le volet Résultats de l'enquête, sélectionnez tous les fichiers sur toutes les pages en cochant la case dans la ligne de titre (File Name), puis dans le message contextuel All 20 Items on this page selected Select all Items in list (63K Items) Cliquez sur **Sélectionner tous les éléments de la liste (xxx items)**, puis sur **Copier**.



3. Dans la boîte de dialogue *Copy Files*, sélectionnez l'onglet **Sync**.



4. Si vous êtes sûr de vouloir synchroniser les fichiers sélectionnés vers un emplacement de destination, cliquez sur **OK**.

   L'interface utilisateur Cloud Sync est ouverte dans BlueXP.

   Vous êtes invité à définir la relation de synchronisation. Le système source est pré-rempli en fonction du référentiel et des fichiers que vous avez déjà sélectionnés dans le champ logique de données.

5. Vous devez sélectionner le système cible, puis sélectionner (ou créer) le courtier de données que vous prévoyez d'utiliser. Vérifiez les exigences Cloud Sync en commençant par le "Description de Quick Start".

Résultat

Les fichiers sont copiés sur le système cible et ils seront synchronisés en fonction du planning que vous définissez. Si vous sélectionnez une synchronisation unique, les fichiers sont copiés et synchronisés une seule fois. Si vous choisissez une synchronisation périodique, les fichiers sont synchronisés en fonction du planning. Notez que si le système source ajoute de nouveaux fichiers qui correspondent à la requête que vous avez créée à l'aide de filtres, ces *nouveaux* fichiers seront copiés vers la destination et synchronisés ultérieurement.

Notez que certaines des opérations Cloud Sync habituelles sont désactivées lorsqu'elles sont appelées depuis Data Sense :

- Vous ne pouvez pas utiliser les boutons **Supprimer les fichiers sur la source** ou **Supprimer les fichiers sur la cible**.
- L'exécution d'un rapport est désactivée.

Déplacement des fichiers source vers un partage NFS

Vous pouvez déplacer les fichiers source que Data Sense analyse vers n'importe quel partage NFS. Le partage NFS n'a pas besoin d'être intégré avec Data Sense (voir "Analyse des partages de fichiers").

Vous pouvez également laisser un fichier de navigation à l'emplacement du fichier déplacé. Un fichier de navigation permet à vos utilisateurs de comprendre pourquoi un fichier a été déplacé de son emplacement

d'origine. Pour chaque fichier déplacé, le système crée un fichier de navigation à l'emplacement source nommé `<filename>-breadcrumb-<date>.txt`. Vous pouvez ajouter du texte dans la boîte de dialogue qui sera ajoutée au fichier de navigation pour indiquer l'emplacement où le fichier a été déplacé et l'utilisateur qui a déplacé le fichier.

Si un fichier du même nom existe dans l'emplacement de destination, le fichier ne sera pas déplacé.

Vous ne pouvez pas déplacer les fichiers qui résident dans les bases de données.

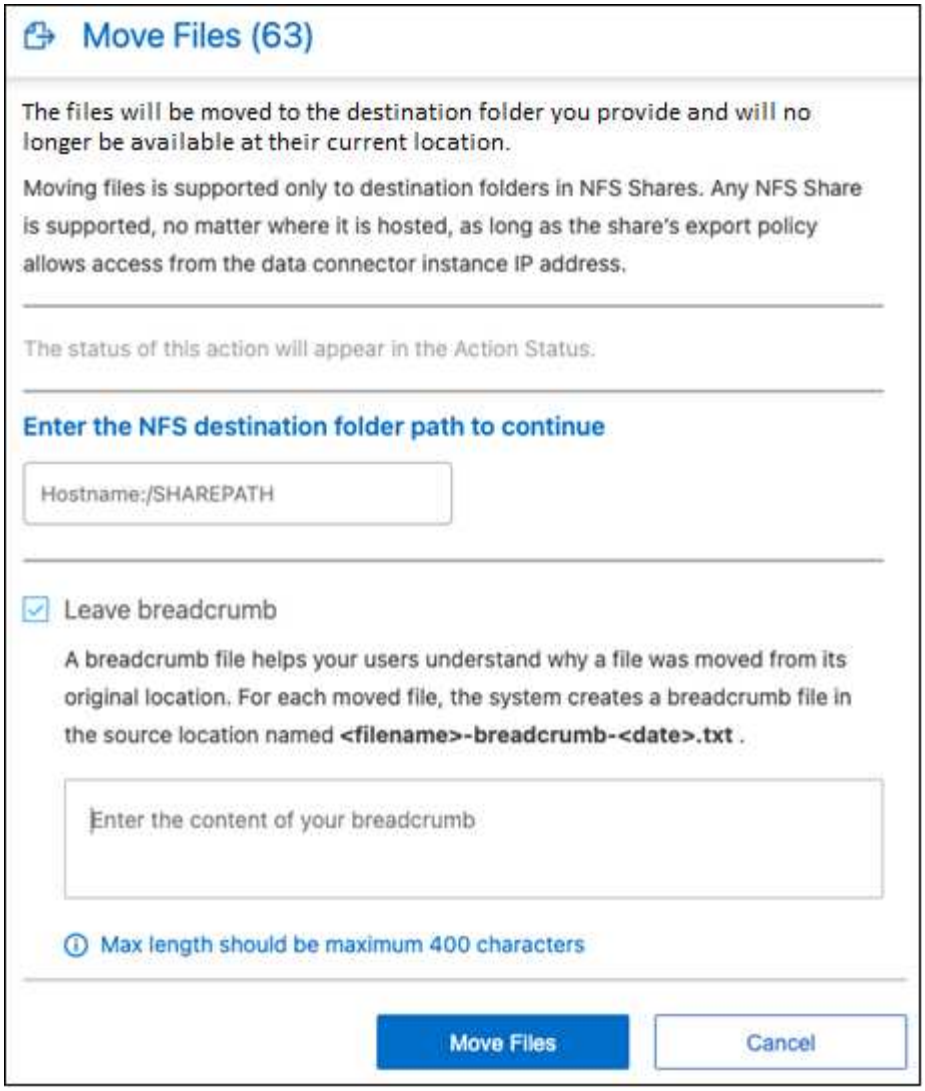
De formation

- Vous devez avoir le rôle Administrateur de compte ou Administrateur d'espace de travail pour déplacer des fichiers.
- Les fichiers source peuvent se trouver dans les sources de données suivantes : systèmes ONTAP sur site, Cloud Volumes ONTAP, Azure NetApp Files, partages de fichiers et SharePoint Online.
- Le déplacement de fichiers nécessite que le partage NFS autorise l'accès à partir de l'adresse IP de l'instance Data Sense.
- Vous pouvez déplacer un maximum de 100,000 fichiers à la fois.

Étapes

1. Dans le volet Résultats de l'enquête de données, sélectionnez le ou les fichiers que vous souhaitez déplacer.

   - Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (Volume_1).
   - Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (File Name).
   - Pour sélectionner tous les fichiers sur toutes les pages, cochez la case dans la ligne de titre (File Name), puis dans le message contextuel All **20** Items on this page selected Select all Items in list (63K Items), Cliquez sur **Sélectionner tous les éléments de la liste (xxx items)**.
2. Dans la barre de boutons, cliquez sur **déplacer**.



3. Dans la boîte de dialogue *Move Files*, entrez le nom du partage NFS dans lequel tous les fichiers sélectionnés seront déplacés au format `<host_name>:/<share_path>`.
4. Si vous voulez laisser un fichier de navigation, cochez la case *laisser fil fil fil fil fil à fil*. Vous pouvez entrer du texte dans la boîte de dialogue pour indiquer l'emplacement où le fichier a été déplacé et l'utilisateur qui a déplacé le fichier, ainsi que toute autre information, comme la raison pour laquelle le fichier a été déplacé.
5. Cliquez sur **déplacer les fichiers**.

Notez que vous pouvez également déplacer un fichier individuel lors de l'affichage des détails de métadonnées d'un fichier. Cliquez simplement sur **déplacer le fichier**.

Suppression des fichiers source

Vous pouvez supprimer de manière définitive les fichiers source qui semblent non sécurisés ou trop risqués pour laisser dans votre système de stockage, ou que vous avez identifiés comme un doublon. Cette action est permanente et il n'y a pas d'annulation ou de restauration.

Vous pouvez supprimer des fichiers manuellement à partir du volet Investigation ou automatiquement à l'aide de stratégies.

Vous ne pouvez pas supprimer les fichiers qui résident dans les bases de données.

La suppression de fichiers nécessite les autorisations suivantes :

- Pour les données NFS : il est nécessaire de définir la export policy avec les autorisations d'écriture.
- Pour les données CIFS, les identifiants CIFS doivent disposer d'autorisations d'écriture.
- Pour les données S3, le rôle IAM doit inclure les autorisations suivantes : `s3:DeleteObject`.

Suppression manuelle des fichiers source

De formation

- Vous devez avoir le rôle Administrateur de compte ou Administrateur d'espace de travail pour supprimer des fichiers.
- Vous pouvez supprimer un maximum de 100,000 fichiers à la fois.

Étapes

1. Dans le volet Résultats de l'enquête de données, sélectionnez le ou les fichiers que vous souhaitez supprimer.

- Pour sélectionner des fichiers individuels, cochez la case de chaque fichier (Volume_1).
- Pour sélectionner tous les fichiers de la page en cours, cochez la case dans la ligne de titre (File Name).
- Pour sélectionner tous les fichiers sur toutes les pages, cochez la case dans la ligne de titre (File Name), puis dans le message contextuel All **20** Items on this page selected Select all Items in list (63K Items), Cliquez sur **Sélectionner tous les éléments de la liste (xxx items)**.

2. Dans la barre de boutons, cliquez sur **Supprimer**.
3. Comme l'opération de suppression est permanente, vous devez taper "**définitivement delete**" dans la boîte de dialogue *Delete File* suivante et cliquer sur **Delete File**.

Vous pouvez afficher la progression de l'opération de suppression dans "Volet État des actions".

Notez que vous pouvez également supprimer un fichier individuel lors de l'affichage des détails de métadonnées d'un fichier. Cliquez simplement sur **Supprimer le fichier**.

Suppression automatique des fichiers source à l'aide de stratégies

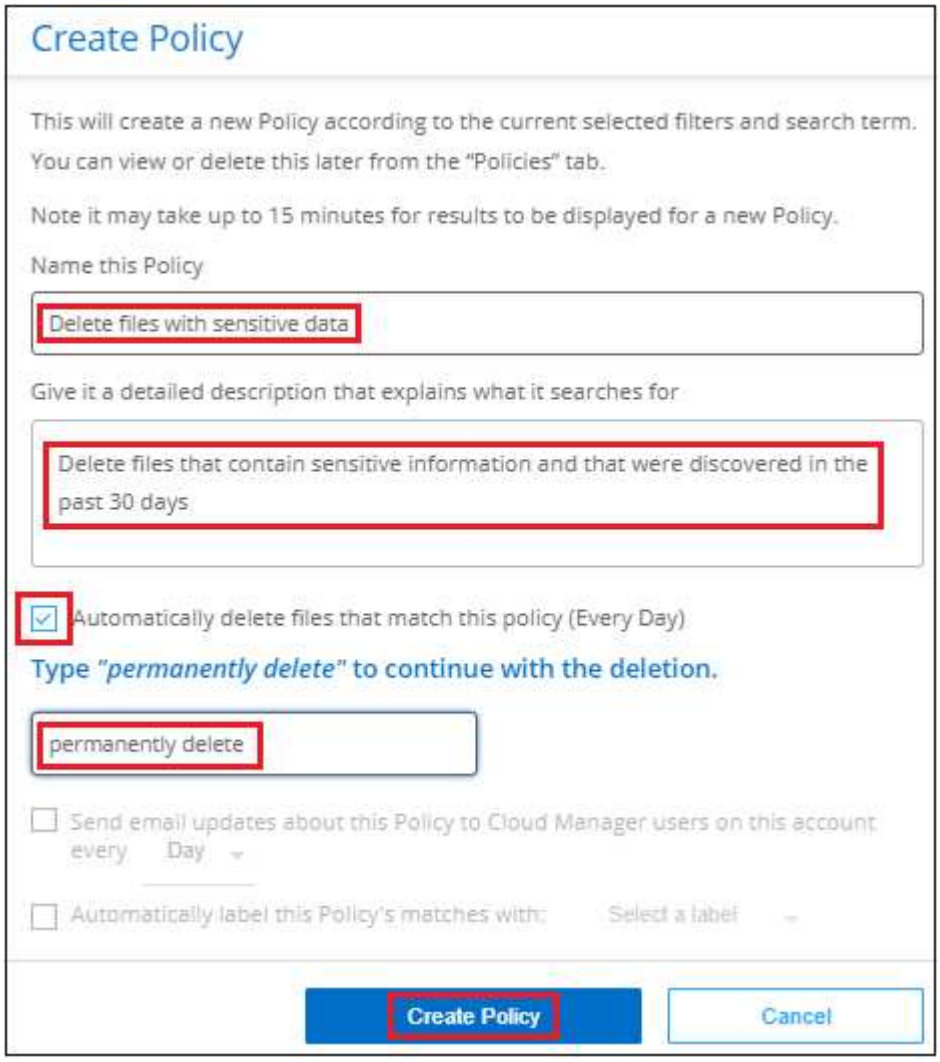
Vous pouvez créer une stratégie personnalisée pour supprimer des fichiers qui correspondent à la stratégie. Par exemple, vous pouvez vouloir supprimer des fichiers contenant des informations sensibles et ayant été découverts par Data Sense au cours des 30 derniers jours.

Seuls les administrateurs de compte peuvent créer une stratégie de suppression automatique des fichiers.

Tous les fichiers qui correspondent à la stratégie seront définitivement supprimés une fois par jour.

Étapes

1. Dans la page recherche de données, définissez votre recherche en sélectionnant tous les filtres que vous souhaitez utiliser. Voir "Filtrage des données dans la page Data Investigation" pour plus d'informations.
2. Une fois que vous avez toutes les caractéristiques de filtre comme vous le souhaitez, cliquez sur **Créer une stratégie à partir de cette recherche**.
3. Nommez la stratégie et sélectionnez d'autres actions pouvant être effectuées par la stratégie :
   a. Entrez un nom et une description uniques.
   b. Cochez la case "Supprimer automatiquement les fichiers qui correspondent à cette stratégie" et tapez **Supprimer définitivement** pour confirmer que vous voulez que les fichiers soient définitivement supprimés par cette stratégie.
   c. Cliquez sur **Créer une stratégie**.



Résultat

La nouvelle stratégie s'affiche dans l'onglet stratégies. Les fichiers qui correspondent à la stratégie sont supprimés une fois par jour au moment de l'exécution de la stratégie.

Vous pouvez afficher la liste des fichiers qui ont été supprimés dans le "Volet État des actions".

Affichage des rapports de conformité

Cloud Data SENSE fournit des rapports qui vous aideront à mieux comprendre l'état du programme de confidentialité des données de votre entreprise.

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

- Les rapports décrits dans cette section ne sont disponibles que si vous avez choisi d'effectuer une analyse de classification complète sur vos sources de données. Les sources de données qui ont une acquisition avec mappage uniquement peuvent uniquement générer le rapport de mappage de données.
- NetApp ne garantit pas une précision de 100 % des données personnelles et des données personnelles sensibles que Cloud Data sens identifie. Vous devez toujours valider les informations en examinant les données.

Rapport d'évaluation des risques pour la confidentialité

Le rapport d'évaluation des risques pour la protection de la vie privée fournit une vue d'ensemble de l'état des risques pour la confidentialité de votre organisation, conformément aux réglementations en matière de confidentialité, telles que le Règlement sur la protection de la vie privée et l'ACFPC. Le rapport contient les informations suivantes :

Statut de conformité

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

Présentation de l'évaluation

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

Sujets de données dans cette évaluation

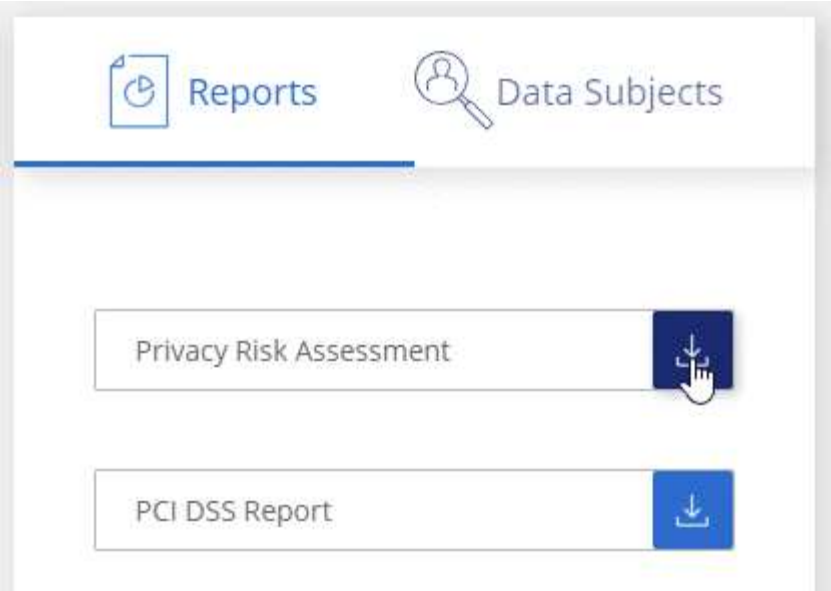
Nombre de personnes, par lieu, pour lesquelles des identificateurs nationaux ont été trouvés.

Génération du rapport d'évaluation des risques pour la confidentialité

Accédez à l'onglet détection de données pour générer le rapport.

Étapes

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



Résultat

Cloud Data SENSE génère un rapport PDF que vous pouvez consulter et envoyer à d'autres groupes, le cas échéant.

Indice de gravité

Cloud Data Sense calcule le score de gravité pour le rapport d'évaluation des risques pour la 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 %

Rapport PCI DSS

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

Présentation

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

Le cryptage

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

Protection contre les ransomwares

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

La conservation

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

Distribution des informations de carte de crédit

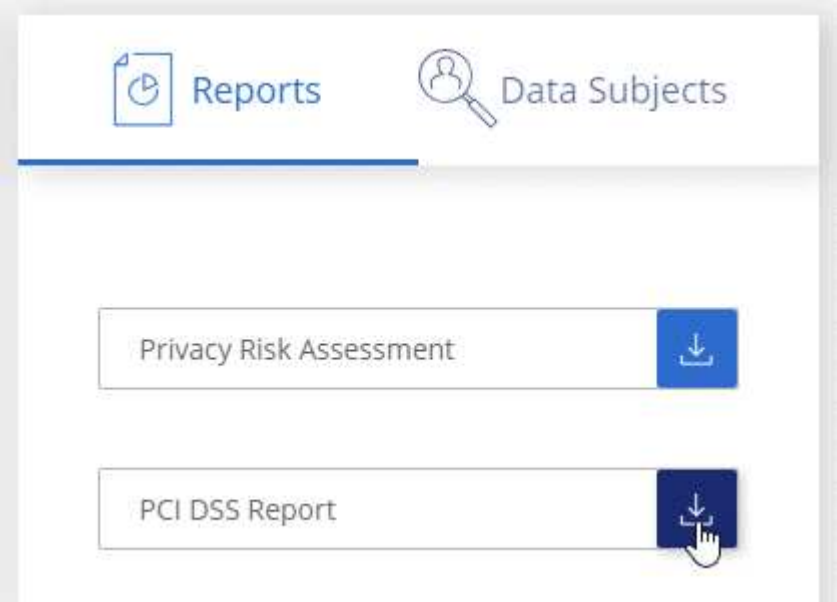
Les environnements de travail où les informations de carte de crédit ont été trouvées et où le chiffrement et la protection contre les ransomwares sont activés.

Génération du rapport PCI DSS

Accédez à l'onglet détection de données pour générer le rapport.

Étapes

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



Résultat

Cloud Data SENSE génère un rapport PDF que vous pouvez consulter et envoyer à d'autres groupes, le cas échéant.

Rapport HIPAA

Le rapport HIPAA (Health Insurance Portability and Accountability Act) peut vous aider à identifier les fichiers contenant des informations sur la santé. Il est conçu pour aider votre organisation à respecter les lois HIPAA sur la protection des données personnelles. Le « Cloud Data SENSE » inclut plusieurs aspects :

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

Le rapport contient les informations suivantes :

Présentation

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

Le cryptage

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

Protection contre les ransomwares

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

La conservation

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

Distribution des renseignements sur la santé

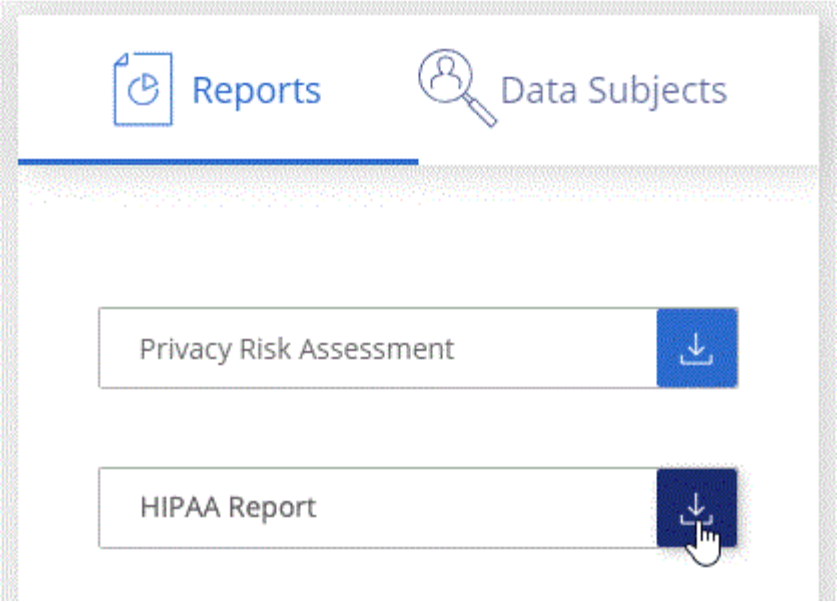
Les environnements de travail dans lesquels les informations de santé ont été trouvées et si le chiffrement et la protection par ransomware sont activés.

Génération du rapport HIPAA

Accédez à l'onglet détection de données pour générer le rapport.

Étapes

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



Résultat

Cloud Data SENSE génère un rapport PDF que vous pouvez consulter et envoyer à d'autres groupes, le cas échéant.

Rapport de mappage de données

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

Le rapport contient les informations suivantes :

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.

Génération du rapport de mappage de données

Accédez à l'onglet détection de données pour générer le rapport.

Étapes

1. Dans le menu BlueXP, cliquez sur **gouvernance > Classification**.
2. Cliquez sur **gouvernance**, puis cliquez sur le bouton **Rapport de la vue d'ensemble de la cartographie de données complète** dans le tableau de bord de gouvernance.

Résultat

Cloud Data SENSE génère un rapport PDF que vous pouvez consulter et envoyer à d'autres groupes, le cas échéant.

Rapport d'enquête de données

Le rapport d'enquête de données est un téléchargement du contenu de la page d'enquête de données. "En savoir plus sur la page Data Investigation".

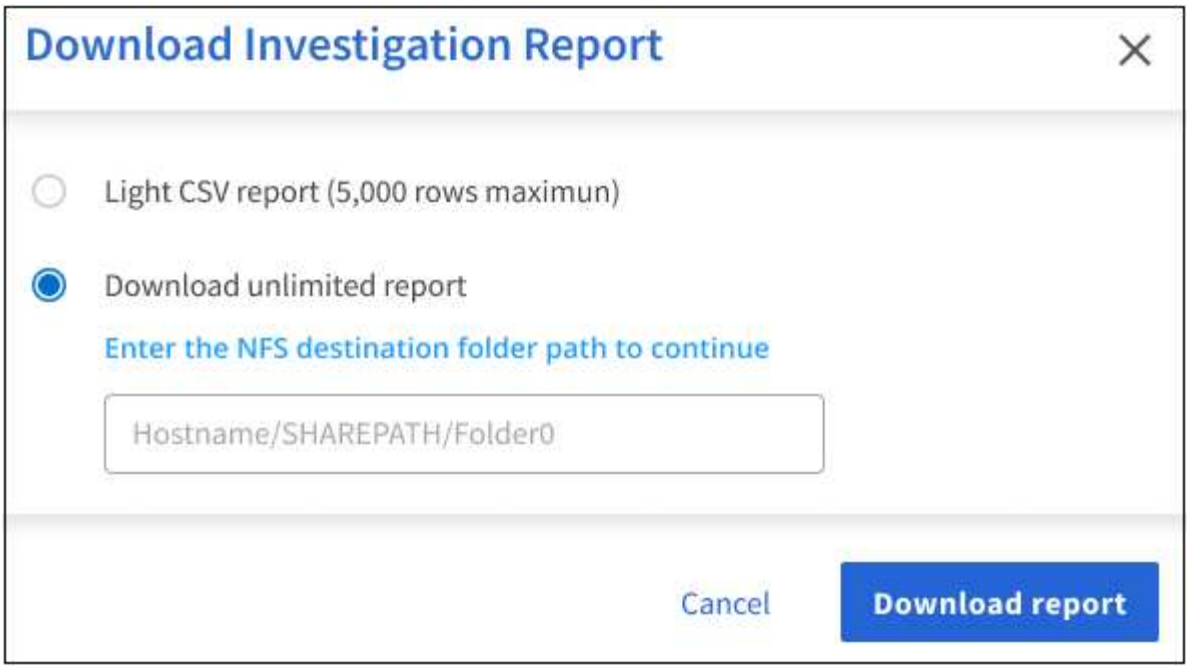
Vous pouvez enregistrer le rapport sur la machine locale en tant que fichier .CSV (qui peut inclure jusqu'à 5,000 lignes de données), ou en tant que fichier .JSON que vous exportez vers un partage NFS (qui peut inclure un nombre illimité de lignes). Si Data Sense analyse des fichiers (données non structurées), des répertoires (dossiers et partages de fichiers) ou des bases de données (données structurées), il peut y avoir jusqu'à trois fichiers de rapports téléchargés.

Lors de l'exportation vers un partage de fichiers, assurez-vous que Data Sense dispose des autorisations appropriées pour l'accès à l'exportation.

Génération du rapport d'investigation des données

Étapes

1. Dans la page Data Investigation, cliquez sur le bouton en haut à droite de la page.
2. Indiquez si vous souhaitez télécharger un rapport .CSV ou .JSON de données, puis cliquez sur **Télécharger le rapport**.



Lors de la sélection d'un rapport .JSON, entrez le nom du partage NFS dans lequel le rapport sera téléchargé au format `<host_name>:/<share_path>`.

Résultat

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

Vous pouvez afficher la progression de la génération du rapport JSON dans le "Volet État des actions".

Ce qui est inclus dans chaque rapport d'enquête de 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 d'environnement de travail
- Chemin des fichiers
- Type de fichier
- Taille du fichier
- Heure de création
- Dernière modification
- Dernier accès
- Propriétaire du fichier
- Catégorie
- Informations personnelles
- Informations personnelles sensibles

- Date de détection de suppression

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

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

- Nom de l'environnement de travail
- Référentiel de stockage (par exemple, un dossier ou des partages de fichiers)
- Type d'environnement de travail
- Chemin du fichier (nom du répertoire)
- Propriétaire du fichier
- 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

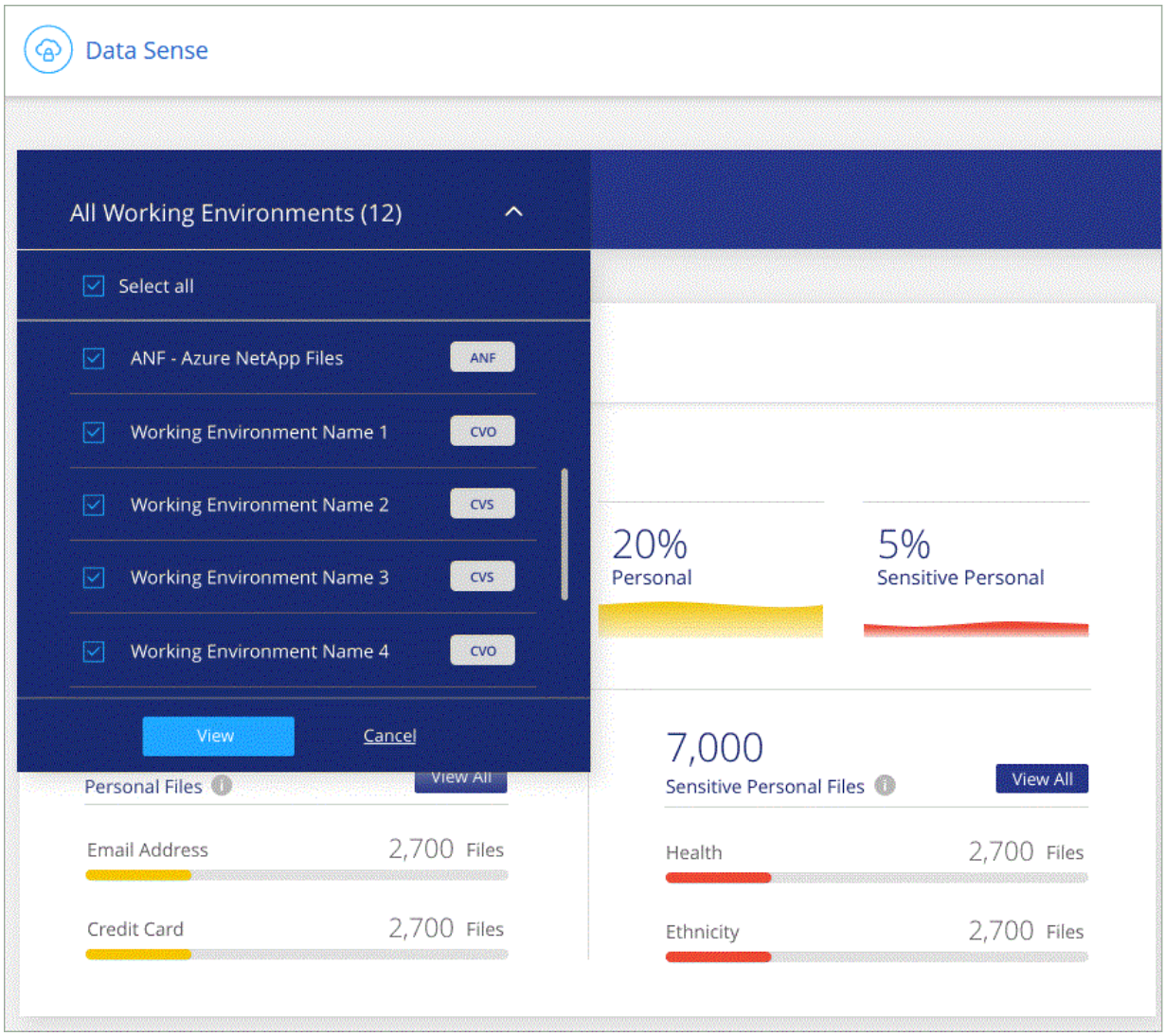
Sélection des environnements de travail pour les rapports

Vous pouvez filtrer le contenu du tableau de bord Cloud Data Sense Compliance pour consulter les données de conformité pour tous les environnements de travail et bases de données, ou pour des environnements de travail spécifiques uniquement.

Lorsque vous filtrez le tableau de bord, Data SENSE évalue les données de conformité et les rapports aux environnements de travail que vous avez sélectionnés.

Étapes

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



Réponse à une demande d’accès à un sujet de données

Répondez à une demande d’accès aux données (DSAR, Data Subject Access Request) 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.

Les capacités DSAR ne sont disponibles que si vous avez choisi d’effectuer une analyse de classification complète sur vos sources de données. Les sources de données ayant une analyse avec mappage uniquement ne fournissent pas de détails au niveau des fichiers.

NetApp ne garantit pas une précision de 100 % des données personnelles et des données personnelles sensibles que Cloud Data sens identifie. Vous devez toujours valider les informations en examinant les données.

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

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

Comment le « Cloud Data SENSE » peut-il vous aider à répondre à un SAR ?

Lorsque vous effectuez une recherche dans l’objet de données, Cloud Data SENSE trouve tous les fichiers, compartiments, OneDrive et comptes SharePoint qui contiennent le nom ou l’identifiant de cette personne. Data Sense vérifie les dernières données pré-indexées pour le nom ou l’identifiant. 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

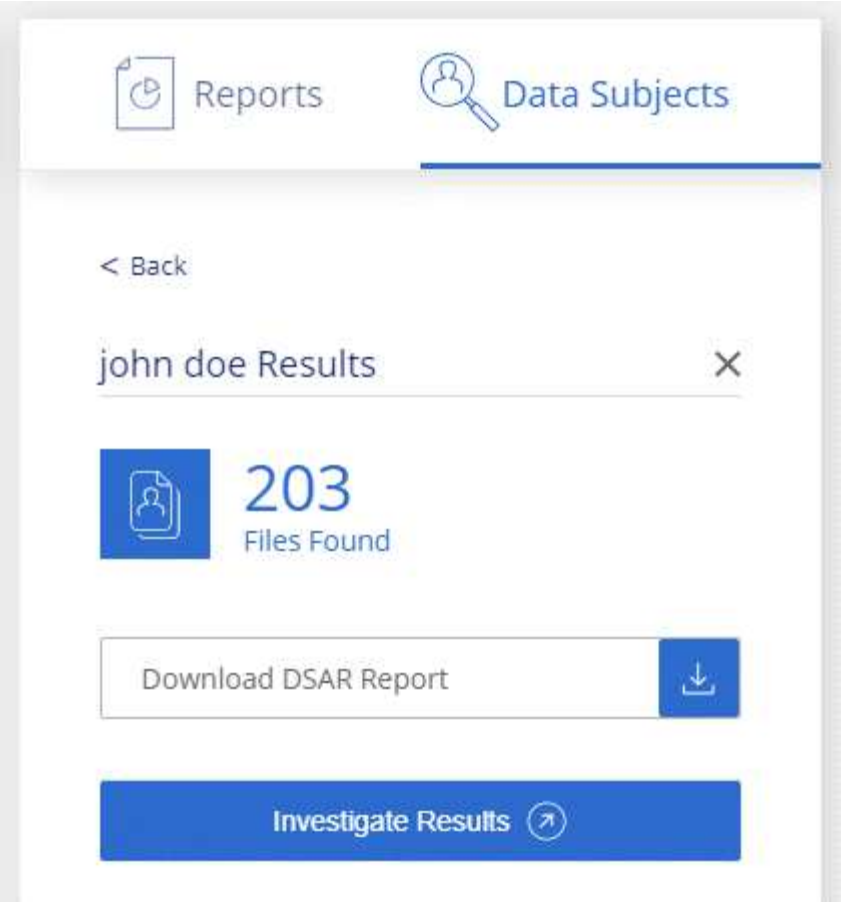
Recherchez le nom complet ou l’identifiant connu du sujet de données, puis téléchargez un rapport de liste de fichiers ou un rapport DSAR. Vous pouvez effectuer une recherche par "tout type d’informations personnelles".

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

Étapes

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

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



4. Choisissez l'une des options disponibles :
   - **Télécharger le rapport DSAR** : réponse officielle à la demande d'accès que vous pouvez envoyer au sujet des données. Ce rapport contient des informations générées automatiquement en fonction des données que Cloud Data SENSE trouve sur le sujet 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.

Catégories de données privées

Il existe de nombreux types de données privées que Cloud Data sens détecte dans vos volumes, compartiments Amazon S3, bases de données, dossiers OneDrive, comptes SharePoint, Et les comptes Google Drive. Voir les catégories ci-dessous.

> Si vous avez besoin que les données cloud soient utiles pour identifier d'autres types de données privées, comme des numéros d'identification nationaux supplémentaires ou des identifiants de santé, envoyez un e-mail à l'adresse ng-contact-data-sense@netapp.com avec votre demande.

Types de données personnelles

Les données personnelles contenues dans les dossiers peuvent être des données personnelles générales ou des identificateurs nationaux. La troisième colonne indique si le logiciel Cloud Data sens utilise "validation de proximité" pour valider ses résultats pour l'identificateur.

Les éléments de cette catégorie peuvent être reconnus dans n'importe quelle langue.

Notez que vous pouvez ajouter à la liste des données personnelles qui se trouvent dans vos fichiers si vous scannez un serveur de base de données. La fonction *Data Fusion* vous permet de choisir les identifiants supplémentaires que Cloud Data SENSE recherche dans ses acquisitions en sélectionnant des colonnes dans une table de base de données. Voir "Ajout d'identifiants de données personnels à l'aide de Data Fusion" pour plus d'informations.

Type	Identificateur	Validation de proximité ?
Généralités	Adresse électronique	Non
	Numéro de carte de crédit	Non
	Sujets de données	Non
	Numéro IBAN (Numéro de compte bancaire international)	Non
	Adresse IP	Non
	Mot de passe	Oui.

Type	Identificateur	Validation de proximité ?
Identifiants nationaux		

Type	Identificateur	Validation de proximité ?
	Numéro d'identification fiscal italien	Oui.
	Carte d'identité lettone	Oui.
	Carte d'identité lituanienne	Oui.
	Luxembourg ID	Oui.
	Identifiant maltais	Oui.
	Numéro du Service national de santé (NHS)	Oui.
	Permis de conduire de New York	Oui.
	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.
	ID slovène (EMSO)	Oui.
	Carte d'identité sud-africaine	Oui.
	Numéro d'identification fiscale espagnol	Oui.
	Carte d'identité suédoise	Oui.
	Permis de conduire Texas	Oui.
	ROYAUME-UNI ID (NINO)	Oui.
	Numéro de sécurité sociale des États-Unis (SSN)	Oui.

Types de données personnelles sensibles

Les données personnelles sensibles que Cloud Data Sense peuvent trouver dans les fichiers incluent la liste suivante. Les éléments de cette catégorie ne peuvent être reconnus qu'en anglais pour le moment.

Référence des procédures pénales

Données concernant les condamnations et infractions pénales d'une personne physique.

Référence ethnique

Données concernant l'origine raciale ou ethnique d'une personne physique.

Référence santé

Données concernant la santé d'une personne physique.

Codes médicaux ICD-9-cm

Codes utilisés dans l'industrie médicale et de la santé.

Codes médicaux ICD-10-cm

Codes utilisés dans l'industrie médicale et de la santé.

Références philosophiques

Données concernant les croyances philosophiques d'une personne naturelle.

Opinions politiques référence

Données concernant les opinions politiques d'une personne physique.

Croyances religieuses

Données concernant les croyances religieuses d'une personne naturelle.

Référence de la vie sexuelle ou de l'orientation

Données concernant la vie sexuelle ou l'orientation sexuelle d'une personne naturelle.

Types de catégories

Il classe les données dans le cloud comme suit. La plupart de ces catégories peuvent être reconnues en anglais, allemand et espagnol.

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

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

- Données applicatives
- Archiver les fichiers
- Audio
- Données d'applications d'entreprise
- Fichiers CAO
- Code
- Corrompu
- Base de données et fichiers d'index
- Fil d'Ariane de détection des données
- 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

Cloud Data SENSE analyse tous les fichiers pour chaque catégorie et chaque métadonnées, et affiche tous les types de fichiers dans la section types de fichiers du tableau de bord.

Mais lorsque Data SENSE détecte des informations à caractère personnel (PII) ou lorsqu'il effectue une recherche DSAR, seuls les formats de fichier suivants sont pris en charge :

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

Exactitude des informations trouvées

NetApp ne garantit pas une précision de 100 % des données personnelles et des données personnelles sensibles que Cloud Data sens identifie. Vous devez toujours valider les informations en examinant les données.

Selon nos tests, le tableau ci-dessous montre la précision des informations que Data Sense trouve. Nous la décomposent par *Precision* et *rappel*:

Précision

La probabilité que le détection de données ait été correctement identifié. 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

La probabilité pour le sens des données de trouver ce qu'il devrait. Par exemple, un taux de rappel de 70 % pour les données personnelles signifie que Data Sense peut identifier 7 fichiers sur 10 qui contiennent réellement des informations personnelles dans votre organisation. 30 % des données semblent manquer le sens où elles ne seront pas affichées dans le tableau de bord.

Nous améliorons constamment la précision de nos résultats. Ces améliorations seront automatiquement disponibles dans les prochaines versions de Data Sense.

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 %

Informations sur le copyright

Copyright © 2023 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 DÉLICTUELLE (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.